Reflective-Physically Unclonable Function based System for Anti-Counterfeiting

Zur Erlangung des akademischen Grades eines

DOKTOR-INGENIEURS

von der Fakultät für
Elektrotechnik und Informationstechnik
des Karlsruher Institut für Technologie (KIT)
genehmigte

DISSERTATION

von

M.Sc. Harsha Umesh Babu

geb. in: Bangalore

Tag der mündlichen Prüfung:	10. Dezember 2013
Hauptreferent:	Prof. Dr. rer. nat. Wilhelm Stork
Korreferent:	Prof. Dr. rer. nat. Cornelius Neumann

Karlsruhe, den January 20, 2014

To my friends and family.

Declaration

I hereby declare that I wrote my doctoral dissertation on my own and that I have followed the regulations relating to good scientific practice of the Karlsruhe Institute of Technology (KIT) in its latest form. I have not used any unacknowledged sources or means and I have marked all references I used literally or by content. This work has not previously been presented in an identical or similar form to any other university or examination board.

Karlsruhe, 12. November 2013

_____

Harsha Umesh Babu

Acknowledgments

Although this appears at the beginning of the document, I would like to emphasize that it was written at the very end of this wonderful journey. The simple reason, for why I had put off writing this section is - I do not know how to appropriately express my gratitude to all the people who have helped me reach this stage in life. I do not want to sound obligatory in acknowledging the help and influence while at same time inadvertently forget mentioning names.

I would like to express my sincere thanks to Prof. Wilhelm Stork and my master thesis supervisor Prof. K.-D. Müller-Glaser, for giving me the opportunity to pursue graduate studies at Institut für Technik der Informationsverarbeitung (ITIV). The German equivalent of a PhD Supervisor is 'Doktorvater', and it literally translates into 'Doctoral father'. Prof. Wilhelm Stork or Willy as he is known to everybody, is my 'Doktorvater'. His infectious philosophy towards learning and teaching - *Man lernt fürs Leben* has been constant source of encouragement over the years. I would like to explicitly thank him for the propitious working relationship, where I had the room for making my own mistakes and learning from them.

My thanks to Prof. Cornelius Neumann for agreeing to be the co-referent and encouragement for the successful defence of my dissertation.

The impact of colleagues cannot be understated. There have been many a times when work was not bearing fruit but the inspiration to keep going can be solely attributed to *it is a joy to work with* colleagues. Thanks to all my colleagues at ITIV, for your patience, encouragement and many times, for simply 'putting up' with cranky me! A special mention to the ITIV-Optics members, for helping me with project reports, technical reviews, checking (and rechecking) my results and brainstorming everything under the sun!

A substantial part of the work for my dissertation was done in co-operation with Informium AG, who were our industrial partners. Over the years and many visits to Leverkusen and Bergisch Gladbach, I have come to appreciate the efforts that go into creating a product from a mere technology. I wish acknowledge the help and co-operation that I have received from all the people at Informium.

A part of my graduate studies were supported by Karlsruhe School of Optics and Photonics (KSOP). The concept of graduate studies supplemented with management modules and mentor has had a positive influence in my pursuit of PhD. Assistance and advice provided by KSOP is greatly appreciated and acknowledged.

My parents underwent significant hardships and made sacrifices to their quality of life so as to enable me to receive a good education. This got translated into a me being taught by wonderful teachers throughout my academic life. I wish to thank my parents and all my teachers who have helped me reach this juncture in life.

My friends, with whom I have studied, learned, worked, trekked, travelled, engaged in hobbies with, lived with (and currently living with) and shared life, have all endured me and encouraged me to come this far. Thank you all, and I hope I can express my returns in kind.

Harsha

January 2014

Abstract

Product security techniques, in particular those targeting counterfeit goods, are under increased focus due to proliferation of supply and distribution chains across the world. Counterfeit goods are not restricted to specific product categories but pose problems across the board. In addition to loss of revenue, the usefulness of the product, functionality and safety are undermined by counterfeit products. A security technique that can be harmoniously applied across product categories as an anti-counterfeiting measure is explored in this dissertation.

Physically unclonable functions (PUFs) are physical security mechanisms, which utilize inherent randomness in processes used to instantiate physical objects. In this dissertation, an extensive overview of both, the state of the art in implementations and the accompanying literature dealing with definition and analysis is provided. Although this is a relatively new domain, one can find established methods and metrics that can be applied in analysis of PUFs. We review these, while presenting our priorities in the framework of anti-counterfeiting application. Focus on experimental verification of unclonability, is a marked difference in our approach when compared with other implementations and analyses in this domain.

The concept of the reflective physically unclonable function (r-PUF) is presented as a product security solution. The viability of the concept, while evaluating and defining the requirements of such a system is explored. The evolution process of the system design is elaborated, which allows for understanding of the compromises that were reached. The anti-counterfeiting system is a combination of physical modules –instantiation, registration, verification and software modules –data extraction, algorithms for processing the data and application layers to provide functionality. During the dissertation, end-to-end functionality of an anti-counterfeiting system using r-PUF was verified.

The system variables in the r-PUF instantiation process were identified and their influence in the system was studied. Experiments were designed to understand the impact of individual variables and results were analysed. We were able to conclusively prove the unclonability of r-PUFs in an anti-counterfeiting scenario.

Zusammenfassung

Methoden zur Produktsicherheit, besonders diejenigen die auf die Unterbindung von Produktfälschungen abzielen werden zunehmend wichtiger, da die Versorgungs- und Verteilungsketten weltweit wachsen. Das Problem der Produktfälschung existiert nicht nur in einigen wenigen Produktkategorien sondern über alle Produktbereiche hinweg. Es gefährdet die unternehmerischen Gewinne, den Produktnutzen und die Sicherheit für den Anwender. Eine Technik welche einfach für alle Produktgruppen verwendet werden kann um dies zu unterbinden wird im Rahmen dieser Doktorarbeit untersucht. Physically unclonable functions (PUFs) sind physikalische Sicherheitsmechanismen, welche Zufallskomponenten ausnutzen, die prozessinhärent ohnehin auftreten.

In Rahmen dieser Dissertation wird ein umfassender Überblick über den Stand der Technik im Bereich der Implementierung und die zugehörigen Definitionen und Analysen gegeben. Obwohl dies ein recht neuer Forschungsbereich ist, gibt es bereits etablierte Methoden und Beurteilungskriterien welche für die PUF Analyse verwendet werden. Diese werden vorgestellt und die relevanten Punkte für das Umfeld der Produktfälschung herausgearbeitet. Der Fokus liegt dabei auf der experimentellen Verifizierung der Nicht-Reproduzierbarkeit, was die vorliegende Arbeit zu anderen Implementierungen und Analysen in diesem Bereich abgrenzt.

Das Problem der Produktsicherheit wird dann unter Verwendung einer konkreten Implementierungsoption, der reflektierenden PUFs (r-PuFs), gelöst. Dafür wird zuerst die Machbarkeit dieses Konzepts untersucht indem die Rahmenbedingungen für ein System festgelegt und Anforderungen abgeleitet werden. Die Systemanforderungen während des Entwicklungsprozesses werden dabei schrittweise beschrieben und die entsprechend resultierenden Designparameter diskutiert. Anschließend wird das Konzept in einen Laboraufbau umgesetzt. Es besteht dabei aus physikalischen Teilen sowie der zugehörige Software. Ersteres umfasst die Instanziierung, Registrierung und Verifizierung, während letzteres die Datenextraktion, Algorithmen zur Datenprozessierung und die Anwendungsschicht umfasst.Innerhalb dieser Arbeit wurde damit die End-to-End Funktionalität eines Systems zur Produktsicherheit unter Verwendung der r-PUFs verifiziert.

Die Systemvariablen im r-PUF Instanziierungs-Prozess wurden identifiziert und deren Einfluss auf das System untersucht. Es wurden Experimente geplant und durchgeführt welche den Einfluss der einzelnen Variablen auf die Ergebnisse untersuchen. Außerdem war es möglich die Fälschungssicherheit dieser r-PUFs in tatsächlichen Produktsicherheitsszenarien zu beweisen.

Contents

1 Introduction

The focus of this dissertation is to explore a variant of the optical physically unclonable function (PUF) implementation for use in anti-counterfeiting and product security applications and evaluate its claim to *unclonability*.

Product security has become an essential component across all industries and significant research is under way in both development of new technology and policy to implement them. Loss of revenue, reputation and safety are some of the issues which have brought product security into the limelight. According to recent published studies [1], the share of counterfeit and pirated goods was $\sim 1.95\%$ of the world trade amounting to US$250 billion annually. It is slated to grow to more than 1000 billion dollars according to a report from International Chamber of Commerce [2]. The numbers gain significance, when looked at over a period of time. The growth in supply, distribution and market for finished products spread across the globe, has magnified the problems posed by counterfeiting. Figure 1.1 shows the estimates of counterfeit trade from year 2000 to 2015 (projected). At the first glance this may seem to be a small percentage but then counterfeiting is prevalent across product categories like pharmaceuticals, electrical goods, foods and beverages. The implications arising out of compromises in safety, efficiency and functional failures are hard to compute but can be safely assumed to have significant impact.

One can get a grasp of the significance of product security by looking into what it is composed of and what are the factors that are influenced by it. In a broad sense, product security is the application of cryptological primitives or tools to any product or commodity with an intention of proving its authenticity, integrity or both. Product security entails three aspects in general - a) ownership, b) functionality assurance and logistical assistance.

a) Ownership and Counterfeiting

In the context of product security, proving ownership and originality are the primary objectives (can be equated to cryptographic objectives of authentication and identification). For any product, establishing the ownership is important for the manufacturer, the user or any other entity which may be involved in the life cycle of the product. Ownership for the manufacturer comprises of protection of trademarks, copyrights, intellectual property rights and any other legal claims thereof. Usually the ownership is represented or claimed with the use of trademarks, statements explicitly claiming rights, special identification markings and/or inherent design or functionality features. These representations establish trust between users and manufacturers which could bear influence on its usage, functionality, safety etc. Counterfeiting is a scenario where the ownership of a product is misrepresented or hijacked for either commercial gain or any other ulterior motive. Counterfeited products therefore cause harm in two ways - the user or the customer is exposed to an untrusted product in terms of safety and functionality, while the manufacturer has to deal with loss of revenue, reputation and any other negative outcomes arising out of functionality and safety issues. Examples of techniques targeting these issues are holograms, emblems, trademark symbols etc.

b) Functionality assurance

Product security plays a significant role in ensuring and delivering promised functionality or the means to cover the lack of it. It also covers the safety aspect whereby the manufacturer vouches for the safety under stated circumstances. Product security for functionality assurance covers two grounds

- Counterfeiting - Counterfeit products do not have functionality or safety assurance.
- Tamper-resistance - Products that may be exposed to tampering with an intention of causing harm or loss during its life cycle.

Examples of Product Security Techniques (PST) in this front include tamper-resistant seals, self-diagnostic algorithms etc.

c) Logistics assistance

Product security features could also be used in logistics assistance. This is usually a secondary or less significant aspect of the security technique. Usually techniques used in product security are optimized for product life cycle and the market. Nevertheless one could exploit any epiphenomena of the security solution for logistical purposes. Two-dimensional (2D) barcodes are a classic example on this front.

There are several other factors such as performance and implementation complexity which influence the use of any given PST. There have been significant efforts put into research and development of PSTs over the years to address the above. There is no one PST solution that could work for all product types and applications. It can be said that most security techniques are optimised for the product that they are being applied to and targeted to address one or more specific high probability risks in a security scenario.

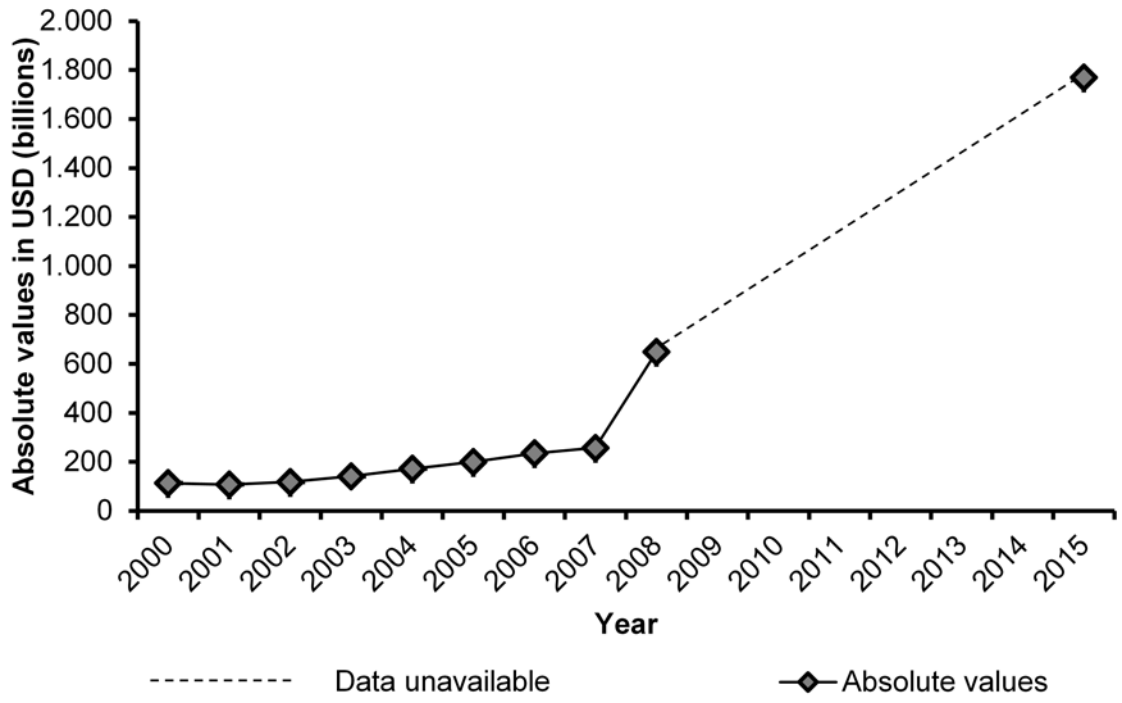


Figure 1.1: Growth of counterfeit trade in absolute and projected value. Sources - [1] and [2]

1.1 Motivation

In 1883, Auguste Kerckhoffs put forward a core set of desiderata for cryptographic systems [3] (Petitcolas provides an translation of the same on the website [4]). A paraphrasing of the principles as applicable to a cryptographic system can be listed as -

- The system should be practically indecipherable, if not mathematically.
- The existence or functioning of system must not be a secret.
- It must be easy to communicate, retain and change (when required) the key involved in the operation.
- The system ought to be compatible with telegraphic communication systems.
- The system must be portable.
- The system must be user friendly - where the operation/interaction with the system does not entail significant skill acquisition or effort.

The second point is popularly referred to as *Kerckhoffs principle*. It was further expounded into a maxim by Claude Shannon as '*the enemy knows the system*'. In literature, one can find reference to this context, in the form of *security by obscurity*.

In this dissertation, we derive inspiration from principles put forth by Kerckhoffs and aim to fulfil them in most respects. In a marked departure from current approach in analysis of security in cryptographic systems, we focus on experimentally proving physical unclonability rather on mathematical modelling. This effort, encapsulates the first two points in the above list. The third point is closely bound to protocol used in the application and will be elaborated in the relevant sections. The use of mobile phone camera and the real-time verification in the anti-counterfeiting solution in intended to cover the last three aspects of the desiderata by Kerckhoffs.

State of the art product security is continually compromised at different levels due to easy access to high-end technology, that is used in security solutions. Currently the security for high-value products is fairly well established due to a combination of inaccessible technology and lower volume, examples include - bank notes, engravings on diamonds etc. When it comes to day-to-day products of moderate value such as medicines, accessories and machinery parts, the security solutions are found to be inadequate (can be inferred from the counterfeit trade information in figure 1.1). This research aims to provide a sustainable solution for product security which is simple, easy to implement and uses minimal resources. We present the concept of *Reflective Physically Unclonable Function* (r-PUF) based anti-counterfeiting system. The work here follows the trail in literature on cryptographic needs for such a system and explores how our solution fits into it.

Cryptographic primitives are tools mainly used to achieve secrecy, authentication/identification and data integrity in a given information exchange scenario. Examples of primitives include signatures, encryption/ decryption algorithms, hash functions etc. A cryptographic protocol is a set of steps which uses one or more primitives to achieve the above stated goals in a given context. *One time pad* is the only foolproof encryption scheme [5] that is currently known while all other primitives are subject to either known failures or unprovable (but widely accepted) security guarantees. However this is not much of an issue when it comes to practice, since different primitives provide different levels of security and one could pick and choose what

suits the application. A good primitive is one where the cost of the data/message/product is less than the cost involved in breaking the cryptographic system.

Modern cryptography is based on computational difficulty and one-way functions are central to this approach[6]. The basic principle is, such a function is *easy* to compute but *hard* to invert. When the underlying principle of such a security technique is based on its physical implementation or exploits any of the physical phenomena in its implementation, it can be labelled as a *Physically Unclonable Function* (PUF). The mathematical definitions or the *easy* and *hard* are presented along with the formal treatment of PUFs in chapter 2. The use of PUF as a security primitive, specifically as a security tag, which can be used with physical objects and not just algorithms has been around for quite some time now. The works [7, 8] have brought it the much deserved attention in academia and industry in 2002-03. They explored the mathematical basis for a PUF, starting from the existing one way functions in cryptography. However, these compromise just one facet - the optical PUF, of a wide variety of PUFs that are out there currently. The earliest reference to an optical PUF is [9] from 1992. Since then many more physical effects have been explored for application in a PUF. A compiled study is provided in chapter 3 dealing with the state of the art. The current implementations are fairly complex in terms of practical realisation, when burdened with providing acceptable security [10]. It can be noted that, despite advances in many techniques, there is room for a simple and effective solution.

Our goal is to explore a variant of the optical PUF inspired by [8, 9], which aims to provide reasonable amount of security at a nominal cost both in terms of money and technology involved. In this endeavour only one application scenario i.e., anti-counterfeiting is explored. This is a conscious decision, since most implementations so far, compromise their achievable goals in an effort to provide a traditional cryptography equivalent panacea using PUFs. The conceived anti-counterfeiting system is further expounded in chapter 4.

1.2 Research objective

This thesis deals with the concept, implementation and the application framework in which the r-PUF can be used. We are restricting ourselves to the case of product security, thereby not providing detailed analyses for authentication and identification aspects. However, there have been various studies that have explored the use of PUF in key-exchange and session security as well (referenced in chapter 2).

We put forth a concept for a PUF which is based on random distribution of micro particles with reflective properties in a three dimensional area. The random distribution along with the selective illumination (angle based) of the micro particles is the core security feature. This volume or it 2D projection area is designated as a 'tag'. The tag shall usually be embedded on a product packaging or product surface is imaged at the production facility and stored in a secured database. This dissertation presents the system design and implementations in a developmental chronology detailing the pits, falls and bridges that we encountered along the way.

The system is analysed for its effectiveness within the anti-counterfeiting perspective. Evaluation is carried out using the standard metrics that are relevant in PUF field to validate our implementation, notably the uniqueness and robustness criteria. Most of the PUF implementations rely on theoretical analysis for proving the *unclonability* aspect of the PUF while experimental evaluation itself is an inference. Experiments were constructed with focus on analysing the effect of various system variables on the final outcome of the

r-PUF within the anti-counterfeiting application scenario. Using these, we provide a simple yet concrete proof of unclonability of the r-PUFs.

1.3 Layout of the dissertation

Definitions and mathematical concepts starting from one-way functions to PUF are presented in chapter 2. Formalization of PUFs is an ongoing process, we follow the method based on properties described in chapter 1 of [11]. This chapter also covers background theory on applications scenarios and security frameworks in which a PUF can be evaluated.

Chapter 3 has a compilation of the state of the art in product security techniques. Several current solutions well as PUFs are discussed. Effort is made to bring about distinction between various solutions based on their emphasis to either security or logistical assistance. Descriptions of various PUF instantiations are compiled and compared.

It is not the intention of this dissertation to serve as a reference compilation of the PUF techniques, however an effort is made to include a comprehensive overview in the interest of positioning the new technique among the state of the art. In chapters 2 and 3, while dealing with the cryptographic background to PUFs and various efforts in formalization, some clichés relevant to the subject will crop in. In case of scientific relevance all efforts are made to reference them appropriately.

Chapter 4 gives details regarding the concept and implementation of the PUF we are proposing. System overview, followed by properties of individual particles and the tag as whole are discussed here along with their relevance to the implementation and performance of the PUF.

System design comprising of three different parts, registration, verification and hashing algorithms are presented in chapter 5. The registration system is usually at a manufacturing facility, integrated with the assembly line. The requirements and complexity of such systems are discussed and their implementations are presented. The verification device is a cellphone equipped with a camera and some add-on optics. The magnification and illumination criteria for imaging the micro-particles is analysed and different versions of solutions are presented.

Experimental results are presented in chapter 6. Discussions are focussed on ease of implementation and our efforts in overcoming the constraints of system design. Performance evaluation measures which affect the usability of the system such as robustness and uniqueness are elaborated here. We also provide proof unclonability from experimental evaluation of the system variables involved in the generation and usage of r-PUFs. Summary, future work and outlook are considered in chapter 7.

2 PUF: Concepts and Definitions

In this chapter, the concept of PUF is elaborated with a historical glance , keeping in mind it's development. There have been many efforts to provide precise and unambiguous definitions for PUFs and an overview of these is provided here. There exists a strong inclination to peg PUF into standard algorithmic definitions of cryptography. While the cryptographic primitives are well understood and have withstood the scrutiny, the pegging of PUF into these cryptographic holes does not necessarily yield fool proof advantages. To address the inconsistencies arising from this exercise, there have been many attempts to formalize the definition of PUF, given that each PUF can have a different underlying technology and may be closely entwined to one application/protocol/solution than others, this effort is still on going. In this dissertation, various formalization efforts will be acknowledged and analysed, though an effort to fit into one or any of them will not be attempted. However, during the analysis the relevant definitions which are applicable will be emphasized.

In chapter 1 of [12], Goldreich provides a neat overview of how the perspective of the cryptography has changed over time. The classical or historical view of cryptography was mainly encryption with some emphasis on signatures. Primitives per say were not evaluated in isolation but only in conjunction with these two applications. While the effort of analysing the primitives in conjunction with applications scenarios/ protocols is still valid today, modern cryptography has moved on from plain encryption to accommodate the growing need for different techniques based on technological and application requirements of the ever connected world that we live in. The figure 2.1 captures the change in perspective from historical to the modern view of cryptography. Modern cryptography, as expressed by [12] is explicitly related to complexity theory. In simple words, it is more important to analyse the primitives and protocols with a view on how much effort is required to break it rather than any absolute measure of security. As long as the effort involved in breaking it is considered infeasible within reasons of limit considering technology available and time required, the cryptographic primitives/protocols are considered secure.

2.1 One way functions

A one-way function (OWF) is a function that is easy to compute in the forward direction but hard/infeasible to invert. The hardness or infeasibility involved in inverting the function is enumerated in terms of computational complexity. The ease of forward computation in addition to the hardness in inverting is used in cryptographic primitives to construct various protocols. To go one step further, one can also bring into account the existence of auxiliary information which enables the fast/easy forward computation and without which the inversion is hard. These kind of functions are used in secure encryption message transmission where, auxiliary informations is shared only with intended receiver. Anybody else who has access to this encrypted message will not be able to decrypt without auxiliary information. Such functions are called trap-door functions (public key encryption is one popular protocol using trapdoor functions).

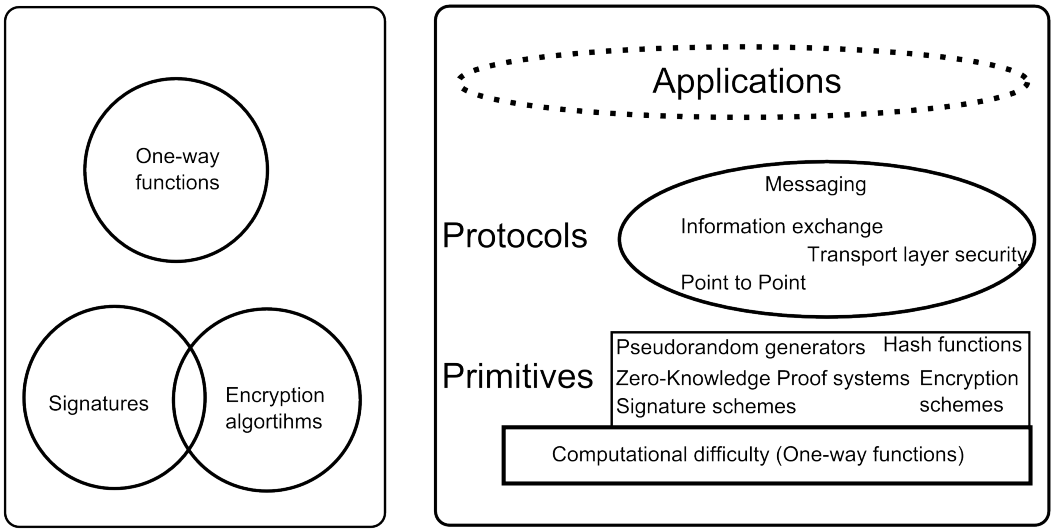


Figure 2.1: Perspective of cryptography [12]

2.1.1 Algorithmic OWF

There are many definitions for OWFs in literature and they vary slightly in notation and assumptions. In this dissertation, the definitions are based on [12, 13]. In its simplest and abstract form, an one way function can be defined as any function f that is easy to compute meaning there exists a polynomial time algorithm which takes an input x and outputs $f(x)$. It is infeasible to find a pre-image of this function, i.e., given $f(x)$ there exists no algorithm to find x. This can be formally encapsulated as -

Definition 2.1 (One-way function, as in [12])**.** A function $f : \{0,1\}^* \rightarrow \{0,1\}^*$ is one way if

(i) Easy to compute
There exists a probabilistic polynomial time (PPT) algorithm A, such that on input x, algorithm A outputs $f(x) \quad \forall x \in \{0,1\}^*$, and

(ii) Hard to invert
There is no adversarial algorithm or function A' such that $\forall x$
$$Pr[A'(f(x)) \in f^{-1}(f(x))] = 1$$

This definition is quite stringent in the sense that any given algorithm must fail to invert $f(x)$ for infinite number of input x. It is plausible that such a function exists but it is not verifiable. For cryptographic purposes, a stable and practical function is required and this can be achieved if one lowers the stringency. A workable definition for hard inversion would be that, for a randomly chosen x, the probability that inversion is achieved is very small or negligible. The concept of negligible is well defined in cryptographic world and below is a standard form of it.

Definition 2.2 (Negligible probability, as in [12])**.** A function $\xi(n)$ is negligible in n if for every positive polynomial $p()$ there exists an n_0 such that for all $n > n_0$,
$$\xi(n) \leq \frac{1}{p(n)}.$$

In plain words, one can say that a negligible function is asymptotically smaller than the inverse of any fixed polynomial. However, there is a bit more subtlety to this definition coming from implementation perspective; a function/algorithm if deemed negligible if as a function of its input-length, the success probability is bounded by every polynomial fraction. This clause of the input-length dependency comes from implementation perspective since all modern computing is done with binary representation and that the length of the binary representation is inherently related to computational costs. The polynomial fraction bound can be understood as follows - if an event/outcome has negligible probability in n, then repeating the experiment polynomially does not improve the probability. [12] captures the relationship between polynomial fraction of computational infeasibility as follows

> *The definition of negligible success rate as 'occurring with probability smaller than polynomial fraction' is naturally coupled with defining feasible computation as 'computed within polynomial time'*

Having described the notion of negligibility, we can proceed to define a less stringent definition of one-way functions.

Definition 2.3 (Strong One-Way Function, as in [12])**.** A function $f : \{0,1\}^* \to \{0,1\}^*$ is a strong one-way function if it is

(i) Easy to compute
There exists a probabilistic polynomial time (PPT) algorithm A, such that on input x, algorithm A outputs $f(x) \quad \forall x \in \{0,1\}^*$, and

(ii) Hard to invert
For any adversarial algorithm or function A' there exists a negligible function ξ such that for any input length n,

$$Pr[A'(f(x), 1^n) \in f^{-1}(f(x))] < \xi(n)$$

From the definition of negligibility, we know that $\xi(n)$ is bounded by inverse of polynomial $p(n)$, therefore the above equation can be rewritten as

$$Pr[A'(f(x), 1^n) \in f^{-1}(f(x))] < \frac{1}{p(n)}$$

In this definition, the requirement on x is that, it is a random variable distributed uniformly over $\{0,1\}^n$. The auxiliary input 1^n is mainly to ensure that any non-length preserving functions are not wrongly classified as one-way functions. In the event when functions are length preserving in nature, the auxiliary input 1^n can be done away with. Further more, if the one-way function outputs a fixed-length output irrespective of the length of the input then such functions are called one-way hash functions. These functions are abundantly used in cryptographic primitives.

It has been observed that even this definition is strict in the sense many useful candidates for one-way functions will fail to meet this strong definition. In order to accommodate more functions, a further weakened definition (titled likewise - weak one-way function) is put forth. This relaxed definition requires that all efficient (computational resources and time) attempts at inverting will fail with some non-negligible probability.

Definition 2.4 (Weak One-Way Function, as in [12])**.** A function $f : \{0,1\}^* \to \{0,1\}^*$ is a weak one-way function if it is

(i) Easy to compute
There exists a probabilistic polynomial time(PPT) algorithm A, such that on input x, algorithm A outputs $f(x) \quad \forall x \in \{0,1\}^*$, and

(ii) Hard to invert
There exists a polynomial $p()$ for any adversarial algorithm or function A', for sufficiently large n,

$$Pr[A'(f(x),1^n) \notin f^{-1}(f(x))] > \frac{1}{p(n)}$$

There exists proof on how weak one-way functions can be used to construct strong one-way functions[12].

2.1.2 Physical One-Way Function(POWF)

Pappu in [7] makes a smooth extension of the algorithmic definition of one-way function to the physical medium and refers to it as *physical one-way functions* (POWF). Below is an extract of the definition of POWF from [7], it is presented here in its **primordial form** keeping in mind the simplicity and succinctness of the original definition. POWF was one of the first formal definitions in this domain and the authors have put it forth, in a form that is as generic as possible without any direct restrictions coming from their own implementation, i.e., optical PUF.

Let Σ be a physical system in an unkown state $X \in \{0,1\}^l$. X is a random variable representing the state of the physical system which in turn may be dependent on physical properties of the system. l is a polynomial function of some physical resource relevant to the system in consideration.

Let $z \in \{0,1\}^k$ be a specific state of the physical probe P such that k is a polynomial function of some physical resource. The probe P in a state z will be denoted by P_z.

Let $y = f(X,P_z) \in \{0,1\}^n$ be the output of the interaction between system Σ in the state X and the probe P_z.

Definition 2.5 (POWF, as in [7])**.** A function $f : \{0,1\}^l \times \{0,1\}^n$ is a physical one-way function if

- $\exists$ a deterministic physical interaction between P and $\exists$ which outputs y in constant time.
- Inverting f using either computational or physical means requires n queries to the system Σ, where $n \propto some_expression^l$
  In other words, the probability of any PPT algorithm or a physical procedure A', when applied on $y = f(X,P_r)$, where $y \in \{0,1\}^n$ is drawn from a uniform distribution is able to output X or P_r is negligible. Equation wise, it can be represented as
  $$Pr[A'(f(X,P_r)) \rightarrow XorP_r] < \frac{1}{p(l)}$$
  where $p()$ is any positive polynomial. P_r notation covers the probability taken over several instantiations of r in the definition.
- Simulating y, given X and P, requires either $O(poly(l))$ or $O(exp(l))$ in time/space resources depending on whether f is a weak or a strong physical one-way function.
- Replicating the physical system to get Σ' such that its unknown state $X' = X$ is hard.

This definition uses the concepts of asymptotic notation of expressing the complexity involved in evaluating functions/procedures. Since this is no detailed analysis of the definition per say, one can safely ignore the details while still appreciating the scope of the meaning. The bulk of the focus in this definition is on

the non-invertability or one-wayness. However, the analysis presented in [14, 15] identify the shortcomings of this definition. The one-wayness in itself is not a sufficient security criteria for most cryptographic protocols. The variable space for the input and output as indicated in the definition to be very large, such that it is *hard* for adversaries to simulate or register all possible states of the physical system in conjunction with the probe with ill-intention was argued to be false. In [14, 16] authors present the bounds for variable space, and argue that though the numbers are big, they are finite in nature. [15] notes that the definition lacks the notion of noise, since measurement of any physical system involves dealing with some amount of noise.

Another early work in this field was [17], which espoused the concept of *physical random functions* (PRF). In this definition the stringent one-wayness or the non-invertability is replaced with a probabilistic measure of unpredictability. The definition is in association with a implementation of PUF based on time delays in silicon circuits. There have been works [18] which have proved that the unpredictability factor can be overcome quite easily with machine learning methods.

2.2 Physically unclonable functions

The works of the [7, 19] have inspired many new implementations where the unreliable behaviour of the physical functions were encapsulated to form basis of cryptographic primitives. Chapter 3 provides a brief overview of most of them. Before more complex definitions of PUFs can be presented, it is helpful to have an understanding of the background notation, terms used in describing PUFs and their operational scheme.

Challenge-Response space

In the broad scheme of PUF applications, there exists always an outside interaction with the PUF device/implementation. This interaction usually characterised by applying a stimuli to the PUF (can be seen as an input to the function), which is then acted upon by the PUF to produce a response (analogous to function output). The stimuli are usually called *challenge* in PUF parlance. An applied input (*challenge*) and its corresponding output *response* is generally called a *challenge-response pair (CRP)*. A set of all possible *CRPs* for a given PUF is called the *challenge-response space* of the PUF.

In literature, there are many more related terms used, and we shall describe them as and when we come across them. For almost all PUFs there is a basic set of operations, *enrolment and verification* which are independent of application or protocol that they are being used in.

- **Enrolment :** A predetermined set of challenges are issued to the PUF and their responses recorded. This step is carried out at the PUF manufacturer, before the PUF is commissioned (a fancy term for putting it out in the real world for usage). The entire set of CRPs is stored in a database for use later.

- **Verification :** This step is carried out either by a some kind of user (not necessarily end-user) of PUF. In its simplest manifestation, one would want to verify the authenticity of the PUF. One of the challenges from the pre-recorded and stored set of CRPs is applied to the PUF and its response is compared to the response stored, if they match then the verification step is deemed successful.

There are variety of complex protocols constructing manifestations of these steps depending on the application. In this dissertation, we are solely focussed on anti-counterfeiting and shall elaborate only those relevant to our objective, while mentioning others in passing.

The evaluation of PUFs is a hotly debated topic, there are research papers dealing solely about the objective method of PUF evaluation. These will covered in detail in next sections but for now, the concept of

inter and intra distance measures shall be explained. Inspired from classification theory, these serve as a first estimate metric in evaluating or comparing the different types/implementation of PUFs.

- **Inter-Distance -** The distance between two responses when a particular challenge is applied to two different instantiations is called *inter-distance*.
- **Intra-Distance -** The distance between two responses obtained by two evaluations of a given PUF instantiation when a particular challenge is applied is called *intra-distance*.

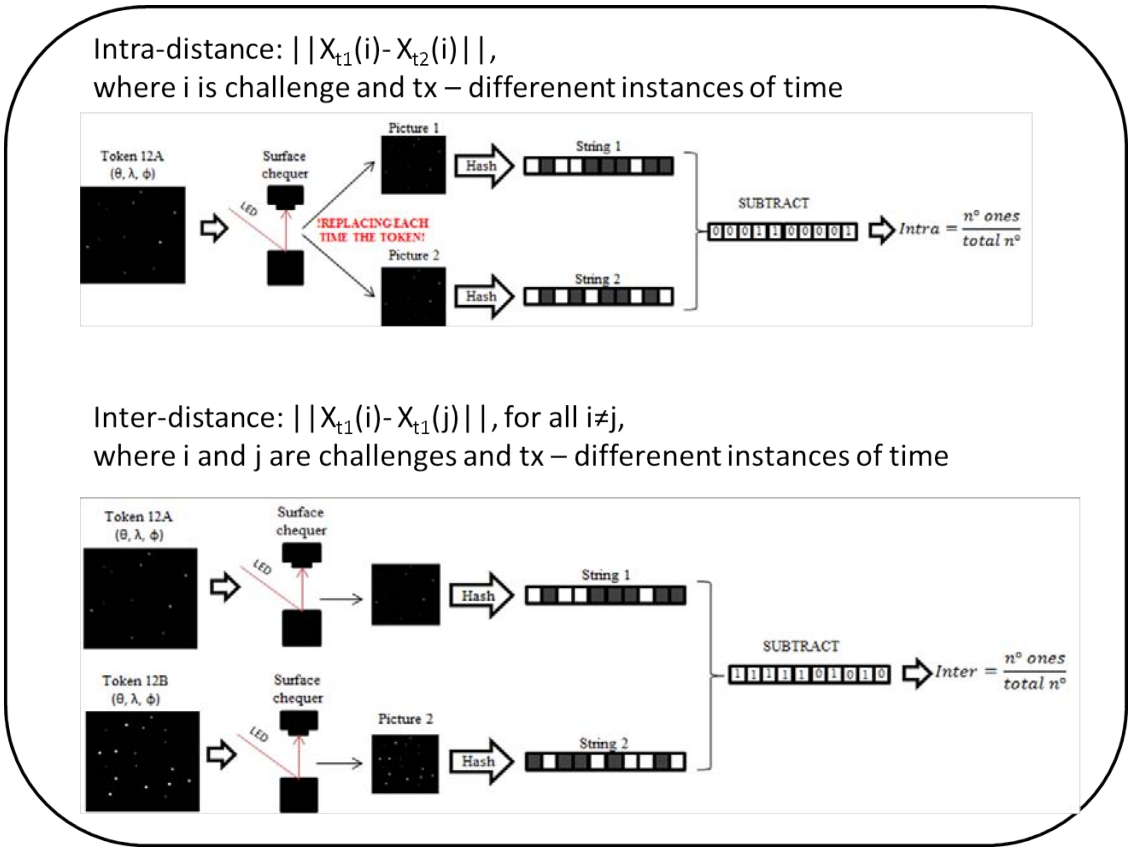


Figure 2.2: Intra- and inter-distance computation using Hamming distances for a generic set of PUF tokens

In figure 2.2, an example computation of intra- and inter-distances are shown using r-PUF. The working of the same will be covered in next chapters but one can understand the concept by abstracting the exact measurement techniques used. The most obvious application of PUF is authentication/identification and these two metrics provide a means for an effective evaluation. It must be noted that in both these definitions, the challenge remains the same, thus the distance measure characterizes the nature of the response and in turn the PUF characteristics. In practice, the distances are computed using normalized Hamming distances. Intra-distance captures the notion of average noise in measurement, or in simpler words the reproducibility of the measurement for a given PUF instantiation and challenge. The notion of uniqueness can be represented as a measure of responses from two instantiations to the same challenge, this difference in measures is encapsulated by inter-distance.

With these preliminaries in place, we can present the rest of the definitions for PUF which are built upon POWF to cover many further implementations and proposals in this domain.

2.2.1 Review of definitions

In this section, we aim to capture the core essence of a host of definitions in the field of PUFs found in literature over the last years. With a view of keeping scholastic integrity, a conscious effort is made to reproduce most of the definitions in this section in their original form with references, however some paraphrasing may creep in inadvertently.

In [20], authors give an inclusive specification (when compared to previous works thus far) for PUF but refrain from formalizing it as a definition. However, a lot of later works treat this description as quasi-definition and include it the list of definitions of PUF.

Definition 2.6 (PUF from [20])**.** Physical unclonable functions are composed from inherently unclonable physical constructions. The unclonability can be attributed to the random components or steps in the manufacturing process and thus, by definition cannot be controlled. On being subjected to a challenge, the system interacts with the challenge and outputs a response. Thus a PUF can be considered as a function that maps challenges to response.

The assumptions made on the PUF are -

- There is negligible amount of mutual information between any two responses R_i (corresponding to a challenge C_i) and R_j (for a different challenge C_j) where $i \neq j$.
- Without access to a given PUF, it is impossible to arrive at response R_i corresponding to a challenge C_i, except with negligible probability.
- The PUF instantiation has inherent tamper evidence characteristics. Any attempt to investigate the PUF with intent to analyse or destabilize it renders the PUF void leaving the challenge-response behaviour altered significantly.

The authors use the size of the CRP space to distinguish strong PUFs from weak PUFs. For strong PUFs the size of the CRP space, say N is so large that a probability of success using exhaustive search is less than $1/N \approx 2^{-k}$ for large $k \approx 100$. Smaller N are categorized as weak PUFs.

[14] points out that this definition too suffers from lack of clarity in dealing with asymptotic concepts as POWF. The definition hints at finite function leading to finite CRP space, however the negligible probability arising out of vastness of CRP space is contradictory. PUFs with limited or small output are excluded by definition of large CRP space. Thus all PUFs based on delay in silicon with one bit outputs are exempted. However as [15] notes, this definition acknowledges the fact that all interactions with the physical system or PUFs in general have an element of noise associated with them.

As a wrap around for these issues Rührmair et. al[14] propose two definitions strong PUFs and obfuscating PUFs. The following two definitions avoid asymptotic concepts and use finite time bounds. But what sets these two definitions apart from previous ones is the concept of an experiment in the definition. The outcome of the experiment is tightly encapsulated in the definition. The authors use the following notation in their definitions -

- Let M be a measurement apparatus which is used to interact with the physical system S, which incorporates the PUF instance.

- C_i denotes the stimulus or challenge which is applied by M to S. C_M denotes the finite set of all possible challenges C_i which M can apply to S.
- M_{C_i} or $M^S_{C_i}$ denotes the response of output from the physical system S that is measured by M.

Definition 2.7 (Strong t-PUF from [14])**.** Let S be a physical system and M a measuring apparatus which may be integrated into the system. S is called a *strong t-PUF* with respect to M if the following conditions hold :

- **Unclonability :** It is practically infeasible to clone or reproduce another system S', even by the original manufacturer of S such that
$$M^S_C = M^{S'}_C \qquad for \quad all\, C \in C_M \quad .$$
- **Security experiment :** It is practically infeasible for any cryptographic adversary Eve (borrowed personality from conventional cryptographic contexts), who may utilize any methods or means allowed by current state of the technology and any practically feasible Turing machine to succeed in the following experiment with probability greater than 90 % :
  (a) Eve is given the system S and the measurement apparatus M for a time period t.
  (b) Eve is also granted access for a time t to a 'time-faithful' oracle O, which outputs M^S_C n input C. Time-faithful means that O produces its output in the same time span that would be required for measuring the response M^S_C on the real system S via use of M.
  (c) At the end of the period of length t, Eve must output a physical system S', and access to O is withdrawn from her.
  (d) Subsequently, a measurement parameter C_0 is chosen uniform at random from the set C_M, and is given to Eve. After that she must output a numerical value V_{Eve}.

  The experiment is deemed successful if the following hold :
  (i) $V_{Eve} = M^S_{C_0}$.
  (ii) For all $C \in C_M$ it holds that
  $$M^S_C = M^{S'}_C \quad .$$
  The probability is taken over the uniformly distributed challenges C_M, and the random choices and procedures that Eve may employ during experiment as described above.

The authors propose a finite time bound in terms of $t \geq 1 \quad day$, for a physical system S to be called a strong PUF. The figure 2.3 captures the essence of the security experiment that is used in defining the strong t-PUF.

In order to cater to PUFs where the unique internal structure resulting from random variations in manufacturing processes can be used a input to traditional cryptographic primitives[20, 21], the authors propose new definition called *obfuscating-PUFs*. [17] has proposed Physically Obfuscated Keys (POKs) which is similar to definition here.

Definition 2.8 (Obfuscating t-PUFs from [14])**.** Let S be a physical system and M be a measuring apparatus with only **one** measurement parameter, $C_M = \{C^*\}$. S is called and *obfuscating t-PUF* for a binary key K_S relative to M if the following conditions hold :

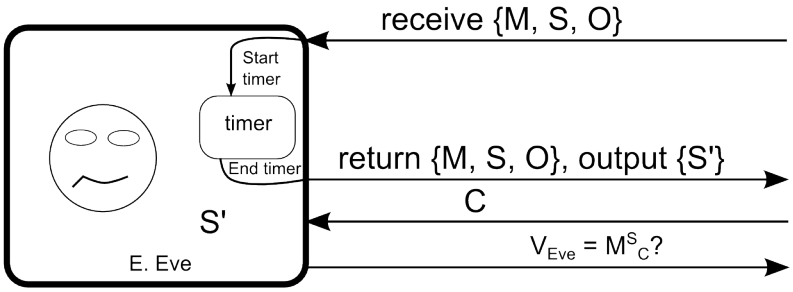


Figure 2.3: Security experiment for strong t-PUF [14]

- **Key storage :** $M^S_{C^*} = K_S$.
- **Unclonability :** The value of K_S is influenced at least in part, from random, uncontrollable manufacturing variations.
- **Security experiment :** It is infeasible for Eve to succeed in the following experiment with a probability greater than $(0.9)|K_S|$:
  (i) Eve is given S and M for a time period t. She is allowed to utilize any means allowed by current state of technology on $S and M$.
  (ii) At the end of the period, Eve must output a binary value V_{Eve}.

  The experiment shall be deemed successful if $V_{Eve} = K_S$. The probability is taken over the random choices or procedures that Eve employed during the experiment as described above.

The figure 2.4 captures the essence of the security experiment that is used in defining the obfuscated t-PUF.

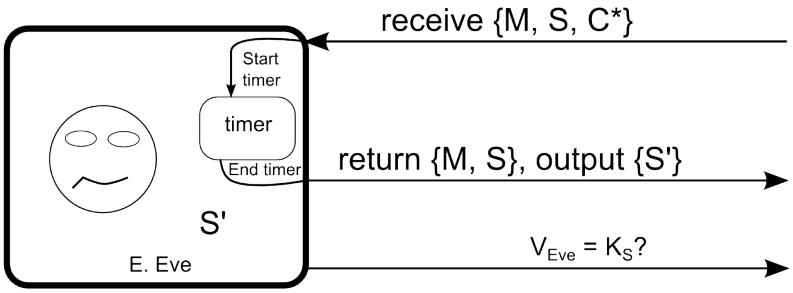


Figure 2.4: Security experiment for obfuscated t-PUF [14]

These definitions were proposed at a time when the PUF terrain was abundant in implementations which involve silicon based on delay, memory initializations and unpredictability in junction bias (voltage). We are not suggesting that this definition is not suited for other PUFs but looking back at development of this

research area in the last 10 years; other than the early implementation of optical PUF[8] and print based approaches[22], most of the others have been FPGA, silicon (IC based security) implementations.

The finite time bound of 1 day and the probability of 90% seems arbitrary since the authors propose the adversary to have access to any means supported by current state of technology. Moreover, the probability and time bound is generic in nature as are the definitions but we believe such bounds will be effective only when they are application or protocol specific. However this negates the scope of definition and we admit that it cannot be a justifiable criticism. The concept of the *oracle O* and the limitation posed by 'current state of technology' seems to make the definition ambiguous and weak depending on the actual implementation. However, the authors support the worthiness of such definitions by proving various cryptographic protocols in [23, 24].

The authors themselves note that weak PUFs receive quasi representation under the obfuscating t-PUFs. However in this definition only one challenge is allowed while there exists a score of PUFs with multiple challenges that do not qualify the strong t-PUF definition. The focus of the obfuscating t-PUF is on the *obfuscation* while unclonability and uniqueness are dealt with a short hand.

Armknecht et al. in [25] make progress on how PUFs can be defined based on the properties. They make a distinction between the algorithmic and the physical properties of the PUF, while defining the PUF. The concept of the noise in PUF measurement is formally encapsulated at the outset.

Definition 2.9 (Noisy functions as per [25])**.** For three positive integers $l, m, \delta \in \mathbb{N}$ with $0 \leq \delta \leq m$, a (l, m, δ)-noisy function f^* is a probabilistic algorithm which accepts input or challenges $x \in \{0,1\}^l$ and generates responses $y \in \{0,1\}^m$ such that the Hamming distance between two outputs to the same input is at most δ. The same definition can be extended in plurality to a family of functions.

Definition 2.10 (PUFs as per [25])**.** A $(l, m, \delta; q_{puf}, \varepsilon_{puf})$ - family of PUFs P is a set of physical realizations of a family of probabilistic algorithms that fulfils the following algorithmic and physical properties.
Algorithmic properties

- **Noise :** is a (l, m, δ)-noise family of functions with $\delta < \frac{m}{2}$.
- **Non-uniform output and independence :** There exists distributions $\mathbb{D}$ on $\{0,1\}^m$ such that for any input $x \in \{0,1\}^l$, the following two distributions on $(\{0,1\}^m)^{q_puf}$ can be distinguished with advantage at most ε_{puf}.
  (i) $(\Pi_1(x) \ldots \Pi_{q_puf}(x))$ for adaptively chosen $\Pi_i \in P$.
  (ii) $(y_i, \ldots y_{q_puf})$ with $y_i \leftarrow \mathbb{D}$.

  For a practical PUF, $q_{puf} \approx |P|, \varepsilon_{puf}$ is negligible and minimum entropy is greater than zero, denoted by $H_\infty(\mathbb{D}) > 0$.

Physical properties

- **Unclonability :** It is infeasible to physically clone any member $\Pi \in P$.
- **Tamper evidence :** For any PUF instance $\Pi \in P$, any attempt to externally obtain its responses or investigates its parameters will significantly alters its functionality or destroy it.

This definition marks breakaway from previous attempts in distinguishing algorithmic and physical properties separately, however significant contribution is the emphasis on *physical unclonability* as opposed merging it with mathematical clonability. Armknecht et al. go further in [15] to describe a framework with which PUF can be defined and analysed (figure 2.5). Here they propose a clear separation of physical function, interaction in terms of applying challenge, measuring response and extraction module to remove noise and give a usable output.

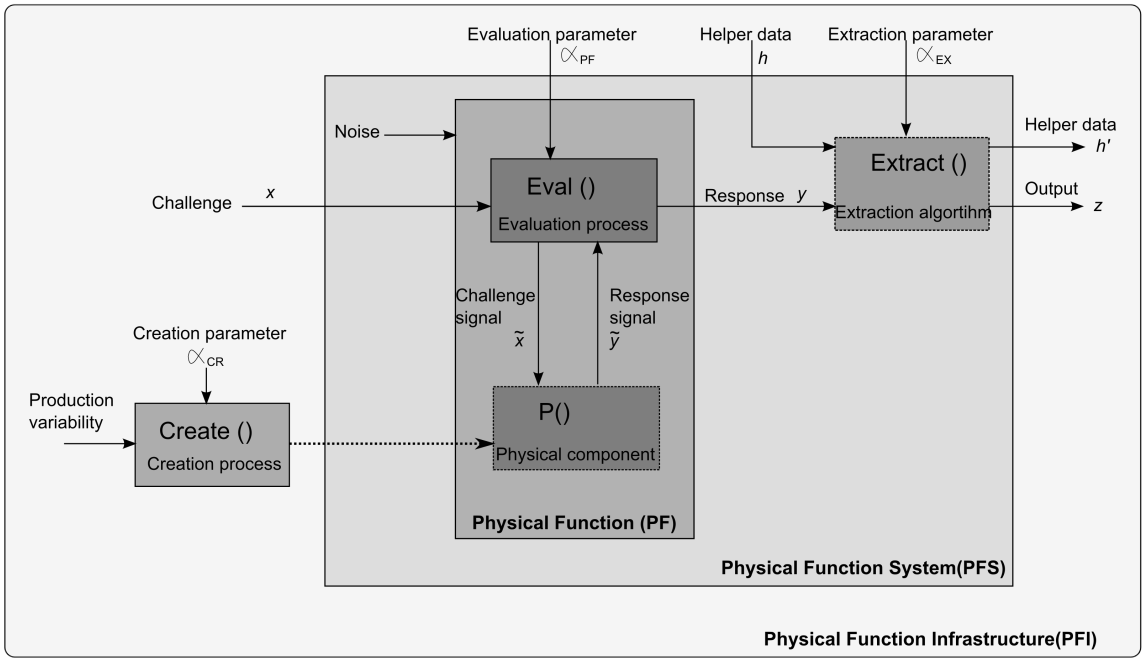


Figure 2.5: Formal model for PUF by [15]

A brief description (as opposed to definition) of the framework is as follows -

- **Physical Function(PF) :** It is the most significant part representation of the PUF in this framework and is described as probabilistic function that maps a set of challenges to responses. It comprises of a physical component $p()$, which responds to a stimulation with some output. There exists an evaluation procedure(module) $Eval()$ which handles the interaction with the physical component $p()$ and external interfaces(usually digital I/O). The challenge-response behaviour of the PF is dependent on both the physical component and the evaluation procedure. The separation of entities allows modelling of PUF where more than one type of physical property can be harnessed for PUF functionality by using different $Eval()$ modules. The uncertainties in measurement such as noise, quantizations errors can be modelled in evaluation procedure.

- **Extraction Algorithm :** The output from the PF can be still described as raw (although it is a digital representation of the measured signal). This is because, by definition the $p()$ is a function that is built on uncontrollable random noise. There exists a possibility that the response of the PF when queried with the same challenge twice results in slightly varied output. This, combined with the fact that outputs of PF may not be uniformly distributed can be overcome by employing an extraction algorithm. The extraction algorithm $Extract()$ is modelled as a separate module from PF so that it could customized based on PUF application.

- **Creation :** The authors also provide for a creation process which enables modelling of various parameters which influence the instantiation of the PUF. At the outset this may seem contradictory since PUF are supposed to be manufactured with non controllable parameters. However, in reality there always exist few parameters(size, ambient temperature etc.) which can be set but their subsequent influence on PUF behaviour is uncontrollable or non-existent.

A more detailed view is provided in the later sections, where our PUF is discussed based on the adaptation of this framework. The advantage of this formalization is that the unclonability, robustness and the effect of noise in output can be analysed in isolation. The different implementations of PUF with varying underlying technologies can be accommodated since the definition is actually a set of different modules. The authors provide an example in terms of SRAM based PUF analysis. Shariati et al. in [26] too base their analysis of image based PUF on this framework.

Plaga and Koob in [27] go a step further in adding intricacies to the definition of PF to overcome the generic formulation of Armknecht et. al. They break up the PF from Armknecht et. al's framework into three modules - $PF_1(), PF_2()andPF_3()$ as seen in the figure below. C is the challenge, R is the response and $\{S, S_r\}$ are intermediate outputs.

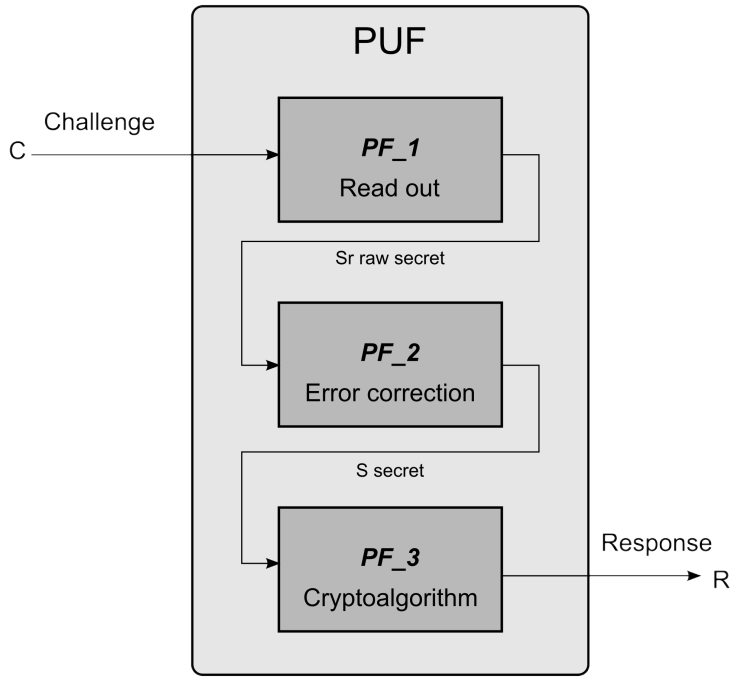


Figure 2.6: Formal model for PUF by [27]

(i) In response to a challenge C, the first or the innermost physical readout $PF_1 = S_r$ is obtained.

(ii) In a optional step $PF_2(S_r) = S$, error correction result from measurement noise and/or privacy amplification is performed.

(iii) In the last step $PF_3(S) = R$, some additional algorithm is applied with S as input to compute final response R. Typically this step is cryptographic protocol which proves the possession of S without exposing it.

Using these sub-functions, they define a PUF as -

Definition 2.11 (PUF as per [27])**.** A piece of hardware is called a PUF if:

- A physical function $PF_2(PF_1())$ is deterministic for a set of challenges $\mathbb{C}$, and can be evaluated with each challenge at least once.
- The value $S = PF_2(PF_1(C))$ is dependent on challenge $C \in \mathbb{C}$ and is not a constant function.

This definition leaves out the unclonability in PUF while trying to be inclusive for all previous implementations of PUF candidates. The authors opine that the security aspect associated with PUF is more important than unclonability, since that is what matters at the end (application wise). In its simplest formulation, the security of the PUF stems from the fact that secret S cannot be **predicted** by an attacker for a given challenge C. They propose two attack scenarios where the security can be defined. The first scenario, the existential unclonability proposed by Armknecht et. al, the attacker is not able to clone the PUF despite given access to it. This does not cover the malicious manufacturer who might generate two equivalent PUFs. In the second scenario, they take into account the parameters that are at disposal of the manufacturer of the PUF and access to PUF. They go ahead and define security criteria for a PUF using the same set of sub-functions.

Definition 2.12 (PUF-security objective from [27])**.** A PUF is secure against existential clonability if the attacker can mathematically or physically clone the function $PF_2(PF_1(C)) = S$ for not more than a negligible fraction L of challenges from the set of all possible challenges $\mathbb{C}$

This definition starts out well in trying to address fundamental issues such as definition of properties that enable a piece of hardware to be called PUF and criteria for piece of hardware to be unclonable. However, their definition ends up trying to be all inclusive and leaves out the unclonable part of the PUF as a part of security analysis.

2.2.2 Protocol based definitions

All the definitions covered so far have been more or less constructed with identification, authentication and anti-counterfeiting in mind. There are works which have made attempts to go beyond this and adapt PUFs in traditional cryptographic protocols such as key storage, key-exchange (KE) etc. Rührmair et al. in [23] provide one of the first constructions and proofs related to oblivious transfer (OT) using PUFs. This in turn spurred interest in utilizing PUFs in other advanced protocols apart from OT. Brzuska et al. in [28] present an adaptation of universal composition (UC) framework [29] to work with PUFs and prove OT, bit commitment (BC) and KE to be secure in their adapted UC setting. This approach of using PUFs in UC framework allows abstraction of the exact implementation of PUF and enables exploration of various application specific protocols. The authors in [28] liken the PUF to a non-programmable random oracle, which is explained as combination of the physical function and a fuzzy extractor leading to properties of unpredictability and unclonability in PUF. Ostrovsky et al. in [30] extend this while negating the assumptions of PUF to be unclonable and restrictions with access for the adversary. They propose a more inclusive setting where malicious PUFs can also take part in protocols. Rührmair and Van Dijk take another approach to overcome the limitations of UC framework adaptation of [28] and propose two new models - posterior access model and bad PUF model which deal with access restrictions and malicious PUF (or adversarial actions on PUF).

In taking a broader perspective of PUFs, Cheong in [31] defines a concept of generic physically unclonable objects (PUO) without explicit verification means. When verification process is included in the definition, independent of the type of PUO, a subset of objects called physically unclonable verifiable objects (PUVO) can be defined. Cheong further goes on to state that PUFs are a subset of PUVO while exploring the strictness of definitions which allow for BC and OT.

The adaptation of PUFs in UC framework, proofs and constructions for PUFs in advanced cryptographic protocols such as OT, BC etc. are out of scope for this dissertation, and hence will not be analysed in depth. However, a closer look at protocols related to identification, authentication and anti-counterfeiting will be presented in next sections. Conventional definitions of PUFs as seen in previous section are sufficient to analyse them.

2.2.3 Properties of PUF

After going through a host of definitions in previous sections it is clear that the field of PUF could be analysed from different perspectives. To take this discussion forward, it is necessary to understand the characteristics or properties of a system which qualifies it as a PUF or is desirable in a system as described. Differentiating the properties of a system from its definitions allows one to analyse the dependency of the application/interaction of the system to its properties. It is also useful in evaluation and/or comparison of PUF systems across technologies and applications scenarios.

Starting with the earliest works Pappu et.al in [8], Gassend in [17] to Armknecht et.al in [15] and Maes and Verbauwhede in[11], all of them include `easy to evaluate` as a necessary property and also bind it to definition of PUFs. At the outset this seems trivial but they construct their definitions of PUF in such a way that properties such as `unpredictability` and `unclonability` is dependent on effort of computation involved in interacting with PUFs. Another implicit property that propagates through most definitions and implementations is the `reproducibility` - this loosely represents security aspect arising from possibility of malicious PUF manufacturer who may produce more than one PUF with identical properties. In our opinion, this is encapsulated in the definition of PUF (no reference to any particular definition, but a general understanding that underlying concept for PUF involving random physical processes). `Unclonability and unpredictability` are two most important properties and many definitions are built around them. Rührmair et.al[14] and others who deal with mainly silicon based PUFs rely more on `unpredictability` while Pappu[7] and Armknecht et al [15] focus on `unclonability`. Maes & Verbauwhede[32] bind `uniqueness` with `physical unclonability` and `unpredictability` with `mathematical unclonability`. Then there are others like Plaga & Koob [27], who dismiss `unclonability` altogether as a property that is aimed for, rather than achieved by definition. This sounds rational from one perspective, as there exists many PUF candidates who are easily cloned mathematically but can still be useful under certain protocols [27]. Armknecht et. al use a reduced criteria for `unclonability` by optional inclusion of *existential unclonability* where by no attacker can physically clone the PUF. Another property which is omnipresent in all PUF related words is the `one-way`. This is straight forward to perceive, given the *challenge-response* scheme under which PUF operates, it should not be possible for any function to map *responses* to *challenges*. `Tamper evidence` is another property which is useful in the context of PUFs, though this has been claimed as a additional benefit right from the first implementation of optical PUFs[7].

Maiti et.al in [33] present a comprehensive review of previous works and provide detailed analysis of the different properties that should be considered when analysing a PUF. They provide a final set of seven prop-

erties - `Uniformity, Reliability, Steadiness, Uniqueness, Diffuseness, Bit-aliasing and probability of misidentification`. However, in our opinion `uniformity` cannot be guaranteed by the underlying physical process of the PUF and there exist extraction/ privacy amplifying algorithms as a part of definition to address this aspect. Terms such as `reliability and steadiness` (though defined to exactness) can be considered as implicit requirements for any practical implementation. Another closely defined parameter `robustness` can be used for the same purposes. `Diffuseness` as defined by authors is useful when dealing with protocols/PUF systems extracting more than one identifier from a single instance of PUF. To a certain extent this property can be covered by `uniqueness` and hence does not qualify as a necessary property. `Bit aliasing and probability of misidentification` are defined almost exclusively in the context of silicon based PUFs and hence will not be further elaborated.

We present a minimum set of properties that are necessary for analysis and comparison of PUFs in general. These properties need not necessarily be bound to the definition of PUF or to a particular protocol. They are generic in nature and should applicable to all PUF implementations irrespective of definition and application. Let p_i be an instance of PUF family P, the challenge this instance is defined as $c_i \in C$ which results in a response $r_i \in R$. The $\{c_i, r_i\}$ is called a $Challenge - Response$ Pair(CRP), a set of all valid CRPs is called the $Challenge - Response\,(CR)$ space. The PUF can also be represented by a function $p_i(c_i) = r_i$.

- **Unclonability :** Given a PUF instance p_i, it is not possible for any attacker or the manufacturer to produce another instance of PUF p_j, such that $p_i(c_i) = p_j(c_i) \quad \forall c_i \in C$. This may seem to be a strict definition, while there exists many definitions which lower the impossibility criteria with a negligible probability. The reason we avoid negligible probability is that we are referring to physical cloning of a device; even if one succeeds in cloning a PUF for one *CRP* then its still no harm since the PUF is characterised by numerous CRPs. One could extend this to cases where more than one *CRP* is compromised, but there would have to be a line drawn to say that p_j is not a clone of p_i. To address this issue, negligible probability is proposed by few, however in our opinion this is a weakening of the PUF concept since the application protocol has to take into consideration this weakened definition. In case the PUF has only one valid *CRP* then it can be categorized as a unique object (section 3.4). In case negligible probability is included as a criteria for unclonability the it should defined as a function of the cardinality of *CR* space.

- **Unpredictability :** Given a PUF instance p_x and a $CRP - \{c_x, r_x = p_x(c_x)\}$, it is possible to predict another $CRP - \{c_y, r_y\} \mid c_y \in C \, and \, r_y \in R$ with negligible probability. Here again the negligible probability should be a function of the cardinality of *CR* space and the number of bits in response $r \in R$. We believe that negligible probability is a necessity here since the *CR* space is finite in many PUF implementations.

- **Uniqueness :** This captures the notion of how different one individual instance of a PUF is from other instances. Given a challenge c_x and two instances of PUFs, $p_i \, and \, p_j$, the fractional/normalized Hamming distance (FHD/NHD) between the responses is recorded. For a set of PUFs, the average of the FHD taken pairwise gives the notion of uniqueness. In PUF parlance this is usually represented by $inter - distance$.

- **Robustness :** When a given instance of PUF p_i is stimulated by a challenge c_x multiple times, the variance in the response has be bounded for any practical application. The lower this bound is, we

say that the system is more robust. Fractional/normalized Hamming distance(FHD/NHD) can also be used for evaluating and setting this bound. In PUF parlance this is represented by the $intra-distance$.

- **One-wayness :** Given a PUF instance p_i and one of its responses r_x, it is infeasible to compute or arrive at $c_x \mid p_i(c_x) = r_x$.
- **Tamper-evidence :** We include this with some reservation, since there are many PUF implementations where `tamper-evidence` cannot be reasonably evaluated and some implementations claim to be `tamper-proof`. Tampering, as interpreted here, is making changes to the physical entity(PUF) with malicious intent. This can be represented as $p_i \rightarrow p_i'$. However, in case a PUF claims `tamper evidence` property then, for any challenge $c_x \in C$,
$$p_i(c_x) \neq p_i'(c_x).$$

2.3 Classification and pigeonholing of PUF

The classification of the PUFs does not qualify as a step in scientific study of PUFs, since most of the PUFs differ in implementation technology but are tied to each other in application scenarios. However, almost all texts on PUF contain a section or two on classification, we shall include it here as an exercise in literature study. There have been many attempts at categorisation of PUFs and we shall cover a few of the more pronounced efforts here.

2.3.1 Intrinsic versus Extrinsic

By definition all PUFs are based on intrinsic random physical processes [34], hence it seems that extrinsic PUFs will take some explaining before PUFs can be categorised into it. Guajardo et al. in [20] define intrinsic PUFs as

> *A PUF that is inherently present in a device due to its manufacturing process and no additional hardware has to be added for embedding the PUF.*

Maes and Verbauwhede in [11], give their perspective on what PUF implementations qualify as intrinsic by splitting this definition into two parts - the PUF and any measurement equipment that is required to interact with the PUF must be integrated and the complete PUF construction is self sufficient such that all primitives and procedures required for operation are built in at the time of manufacturing. This definition is clear on what constitutes an intrinsic PUF and anything that does not fulfil these can be classified as extrinsic.

Going by this definition, only silicon based PUFs qualify as intrinsic PUFs. Most of the implementations on ICs (both memory based as well as delay based) can query and read out the embedded PUF and use the results with inbuilt software or hardware routines too. There is no overhead in terms of extraction of usable data for security primitives since everything is integrated. On the other hand, implementations such as optical PUF, coating PUF (though this is an IC) and image based PUF need external evaluation mechanisms followed by some computational overhead in terms of extraction to retrieve usable data from PUFs. The works of [15] too espouse similar view on categorization of intrinsic and extrinsic PUFs. As mentioned before, getting the classification intrinsic and extrinsic is a fruitless exercise in itself and we shall not delve further into merits of the same. It must however be noted (will become more obvious in next chapters) that reflective PUF (r-PUFs) will fall into extrinsic PUF category by almost all the definitions in literature.

2.3.2 Electronic versus Non-Electronic

This is a very simple exercise, since the PUF implementation details will directly lead us into putting each PUF in its basket based on underlying technology.

Electronic PUFs : A host of implementations which use some form of electrical signal in their PUF function can be categorized here. In literature, they have been further sub-classified as digital and analog.

- **Delay based PUFs** These PUFs use the non-deterministic but characteristic delay for every implementation experienced by signal that flows through a chip as the underlying PUF principle. Two most important implementations in this category are the Arbiter PUF and the Ring Oscillator PUF. Both these are covered in quite some detail in section 3.3.1 and section 3.3.10. There has been extensive research on this category since the applications arising out of this range from not just IC protection but also includes growing field of trusted hardware based applications. Recent implementations have explored the phenomena on FPGAs as well as ASICs. The Glitch PUFs [35, 36] too can be counted under this branch.

- **Memory based PUFs** Another IC based PUF but with different underlying technology. Digital memory works by storing bits in individual cells which are capable to two stable states (usually). In case the cells are driven to unstable state momentarily, the next stable state they take is non-deterministic. Using this basic premise there exists a host of PUF implementations as described in section 3.3.8.

- **Analog PUFs** All PUFs which do not fall under either delay based or memory PUFs can be grouped here. One could make an argument that even delay based PUF and memory PUF are analog in nature. However, the subtle distinction can be appreciated when implementations such as coating PUF (section 3.3.2), LC PUF (section 3.3.5), Magnet PUFs (section 3.3.7), Resistance PUFs (section 3.3.9), RF-DNA PUFs (section 3.3.11), and Threshold PUFs (section 3.3.13) are encountered. The readout in most of these cases is still an analog signal which is then quantized and converted to a digital signal (since most of modern world lives digitally). Thus the subtle distinction one could attribute to analog PUF is that the read out has to be in analog form as opposed to digital.

Non-Electronic PUFs : Some of the earliest PUF proposals - reflective tokens [9] and optical PUFs [8] fall into this category. The focus is on using some form of physical signal that is non-deterministic in nature. Fiber structure PUF (section 3.3.3), Laser marking based PUFs (section 3.3.4) and the PUF implementation based on randomly distributed micro-structures, which is the focus of this thesis, too fall into this basket of classification.

2.3.3 Definition based classification

This a fairly complex task, given that there are many variations in the definitions as seen in section 2.2.1. We shall not attempt to classify PUF implementations as per each of or for that matter any of the definitions since they serve us no purpose. For the sake of completeness however, one can generalize the definitions to consist of *Weak PUFs, Strong PUFs, Unique objects and others*. This classification can be attributed to [37] where a clear distinction is proposed between unique objects and PUFs. And any implementation which does not fit into either of the two can be left out as *others*. Within PUFs, one can make a further sub-classification as weak and strong PUF based on any of the definitions (from section 2.2.1), as one sees fit.

Unique objects have been covered in section 3.4, while implementations that are close to PUF in functionality but are classified as PUF in literature can be grouped under others.

2.4 Application scenarios

Examples of PUF implementations will be presented in chapter 3 and definitions covering different perspectives in section 2.2.1. Here we present a brief survey of various application scenarios and protocols that have been proposed in the literature. The focus of this dissertation is anti-counterfeiting using PUFs and protocols related to this are elaborated in more detail. Historically, PUFs have come about as a result of search into methods to achieve strong anti-counterfeiting. Anti-counterfeiting encompasses a wide array of notions, broadly speaking, it is a protection mechanism against piracy and counterfeit products. Protection is usually some form of verification or authentication about the legitimacy of the product in question. Usually products are attached with some form of identity tag, which can be verified. In this domain the terms identification, authentication and authorization take differing meanings in different works of literature. For clarity, we present our understanding of these terms before further discussion on protocols.

Identification - Let us assume that an entity has been assigned an identity (preferably unique or in some closed space). Then a simple act of stating or presenting its identity upon query, followed by acknowledgement is defined as an identification process. For example, reading an identity tag on conference delegate to ascertain if he/she were attending the conference. This is a simple process and does not require too much details to determine if the tag were a counterfeit or the person were impersonating someone by using a legitimate tag or whether the tag was tampered to indicate wrong identity. Thus identification only answers the question - who is the person? But makes no check to ascertain the real identity of the person that he/she claims to be. There exist many scenarios where there are no strong security requirements and a mere identification suffices.

Authentication - Identification when combined with a verification process is defined as authentication for purposes of this dissertation. The verification can involve verifying the identity of the entity bearing identification as well as authority making the verification. In cryptography, authentication is usually studied in reference to message communication between parties and one can find *message authentication* as a subject of various protocols. In Handbook of Applied Cryptography [38], the authors put in a further condition for active presence of the party being authenticated. To summarize, authentication can be described as a exercise involving two parties where one party presents its identity and seeks to be authenticated. The other party verifies this identity using some prior knowledge or by acquiring some corroborative evidence to support the claim of the first party's identity. The authenticating party also has to make sure that a party presenting it's identity is actively engaged during the authentication process.

The need for active engagement can be easily understood in the context of biometric authentication. If finger prints are used in verification of a person's identity, one must be sure that a person is present during the process and the system is not duped by a synthetic fingerprint in front of its scanner. Worst case scenarios, include people cutting off fingers to beat the system. To discourage such macabre settings, *liveness detection* is mandated for biometric authentication. In the world of PUFs, one is spared such gruesomeness but care has to be taken that entity bearing PUF is actively engaged during the authentication process.

Authorization - Usually identification and authentication are part of a larger story. In cases where exchange of services are involved, authorization comes into picture. Authorization can be defined as process

of empowering someone/something to act or providing access to controlled entities. Taking forward the fingerprint example, let us assume that a person has been authenticated using fingerprint and is now seeking access to some physical facility or data in a system. Authorization is a process controlling this access. Since authorization is usually an application specific step succeeding identification and authentication, we shall not elaborate further.

In almost all application scenarios involving PUFs - the *enrolment* and *verification* form the core of operations. We describe the basic notion here, while many protocols will define these steps in further detail which are application specific. Let us consider two parties, a manufacturer and a verifier.

- **Enrolment :** The manufacturer creates a PUF and tags it with a product. An identity (*ID*) associated with it and a set of CRPs measured on the PUF is stored on the database indexed by the identity. The product tagged with the PUF is deployed i.e., sent out into real world.

- **Verification :** When somebody wants to authenticate a product, they take on the role of verifier. The verifier sends the product *ID* to the manufacturer seeking authentication.The manufacturer checks if the *ID* exists in the database, if it exists, they choose a random *challenge* from the set of stored CRPs and sends it to the verifier. The verifier stimulates the PUF instance at hand with the *challenge* received from the manufacturer and returns the *response* of the PUF function to the manufacturer. The manufacturer compares the response received with the one stored and responds to the verifier whether the PUF that in question is authentic or not.

2.4.1 Anti-Counterfeiting

In simple words, identification combined with verification forms authentication. Anti-counterfeiting solutions basically consist of authentication of a product or an entity. Use of PUFs in anti-counterfeiting is done usually in two ways - embed or attach the PUF device to the product (mostly extrinsic PUFs) or the PUF is a part of the product manufacturing process (intrinsic PUFs usually fall into this category). Pappu et al. in [8] propose a simple scheme where the optical PUF tag is embedded or attached to the product. Every time an authentication is carried out, one *CRP* is used up. Reusing a *CRP* makes the scheme susceptible to replay attack, thus PUF should have an infinite or sufficiently large set of *CRPs*. There are further shortcomings of this basic protocol, the *challenge* and *response* are transmitted without encryption between the two parties which leaves it open to attack. To overcome this Tuyls et al in [16] propose a more advanced scheme using message authentication codes (MAC), where response of the PUF is never transmitted. There is some overhead in this protocol in terms of generation of a secret key from the PUF response and computation of MAC at both ends but it is secure too.

Despite the improvement in security in the method proposed by Tuyls et al, the requirement of large CRP is a disadvantage for many PUF implementations. Then there are attacks where the manufacturer can be impersonated and the verifier gets an unreliable authentication. To address these issues, Herrewege et al. [39] propose a mutual authentication scheme inspired by the classic cryptographic $challenge - response$ authentication protocols which use symmetric keys and one-way hash functions, where one party demonstrates to the other that it has access to secret key without revealing it. To overcome the uncertainty involved in repeated PUF evaluations (intra distance is never 0 %), they propose to use the secure sketches [40] in reverse. Instead of sending the response of PUF, they send a projection of the response on linear block code.

To avoid attacks based on recording and guessing PUF response, the length of the projection should always be lesser than the entropy of the PUF response.

Inspired by error handling in communication theory, Voloshynovski et al. [41] provide an ID generation, comparison algorithm called reference list decoding. Beekhof et al. [22] use the reference list decoding along with microscopic print variations as a PUF to construct an anti-counterfeiting protocol.

Chong et al. in[42] present a similar protocol which uses the helper data from the fuzzy extractor scheme[40]. However the random pattern due to phosphorous particles does not qualify as a PUF since there is only one CRP. There are many works ([24], [37], [43] and others) where slightly varying versions of the basic protocol are presented in the context of strong PUF verification.

Shariati et al. in [26] propose an anti-counterfeiting solution using images of random laser markings. The PUF in this case would be a plastic token with laser markings. The inherent random noise in laser results in non-uniformity of the edges of laser marking, which is imaged and used as a PUF. They too propose a model which uses the auxiliary data from [40] to generate a secret key or uniformly distributed PUF response.

2.4.2 Session Key Management

In classical cryptography, encrypting communication between two parties is a widely researched topic. Usually such encryption is done with a secret key, if only one shared key is used then its symmetric cryptography and if a pair of them are used for encryption and decryption then it called asymmetric cryptography (eg: Public Key crypto-systems). Establishing a key and initiating a secure session is well described in standard cryptographic protocols. The generation of the secret key is usually done with the help of a (pseudo) random number generator, and this could be replaced with PUFs. This approach has been proposed and analysed with many varying details in [44, 45, 34, 46, 47] among others.

Another variation of the secure communication problem is an ad hoc network. The characteristics of PUFs allow them to be bound to individual nodes in a network and communication within the network can be encrypted using keys generated from PUF responses. This throws up further complexities on how to distribute a key to secure communications. Key deployment has been researched in the context of PUFs by [43].

Tuyls et al. in [47] extend the notion of authentication from the context of anti-counterfeiting to authentication of bank card embedded with an optical PUF followed by session key management. The goal of session key management is that PUF is used to derive a secret key with which all communication between two parties can be encrypted. The protocol proposed by Tuyls first authenticates the bank care with an optical PUF and establishes a secure communication channel for further interaction between a remote bank terminal or an automated teller machine (ATM) and the bank. Busch et al. in [48] point out the shortcomings in Tuyls's approach and propose two further variations of the protocol using Bloom filters and Hash trees. Most of the authentication protocols mentioned in literature point towards session key management ([47, 49, 43] among others). The bank ATM scenario is an attractive application scenario and Frikken et al. in[50] analyse this in greater depth along with attack scenarios.

2.4.3 Extension of classical primitives

Buoyed by the key generation protocols using PUFs, people have tried to extend the PUF into traditional cryptographic settings. Pappu in [7], proposed one of the first attempts of bit-commitment (BC) using PUF

but proofs were provided much later by other works. Starting with tamper evident seals (which are not technically PUFs themselves but can be considered a weak definition since tamper evidence is a property that is shown by most PUF implementations) Moran et al. [51] explore the possibility of their use in OT and BC.

Rührmair in [23] provides one of the first proofs for OT using PUFs. Brzuska et al. engage in a more complete effort to fit PUFs under UC framework and provide proofs for OT, BC and KE within UC framework. Ostrovsky et al. in [30] take this approach further by considering malicious PUFs in their proofs. van Dijk et al. in [52] improve upon these protocols by removing some restrictions related to access and malicious PUFs and provide proofs of their own to all PUF based OT, BC and KE protocols. The proofs from UC adaptation are quite attractive, as it opens up opportunities where PUFs can be exchanged with existing cryptographic modules within larger application frameworks.

2.4.4 Integrated Hardware Cryptography

Taking a step further from using PUFs in classical cryptographic primitives, there have been efforts to integrate the PUF into fully functional cryptographic hardware. The first such proposal called *controlled PUF* (C-PUF) was proposed by Gassend et al. [53] way back in 2002. During those times most of PUF implementations were dealing with limited CRP space; C-PUF were proposed to overcome arbitrary or ill-intentioned access to CRPs. The authors proposed constructions where the PUFs were embedded along with required hardware for PUF interaction and a controlling module such as a microprocessor in a physical casing that is tamper proof. The micro processor controlled the interactive hardware and in turn the PUF. The response of the PUF were abstracted by this construction to the outside world, thus limiting/controlling the exposure of CRPs. Over the years there have been works which have used optical PUFs, coating PUFs and acoustic PUFs and other silicon based PUF implementations to construct C-PUFs. The following works propose and analyse different protocols associated with C-PUFs - [44, 34, 47]. The abstraction of PUFs has been treated as something less than PUF in some works, where they classify this as a physically obfuscated token (POK) [14].

Frikken et al. in [25] propose a more radical approach to integrated PUF. In their construction, a key is no longer generated from PUF response but instead they propose a new primitive where the PUF is treated as a pseudo random functions (PRF) calling it *PUF-PRFs*. The authors present a complete case study involving SRAM PUFs instantiated as PRF-PUFs. The motivation for this approach comes from the fact that keys derived from PUF when stored tend to leak or can be harnessed by various methods. To overcome this PRF-PUFs construction avoids storage of keys at all stages and aims replicate the classical PRF generator.

One-Time-Pad (OTP)is considered by far the most secure protocol for secure message communication [5]. The drawbacks include the length of the key and requirement of pre shared keys apart from the obvious *one-time* restriction. In a novel approach, [54] propose to use the PUF responses as OTP. They go ahead and prove that the same can be extended to asymmetric protocols too.

2.5 Summary

In this chapter, the background on existing literature related to PUFs were reviewed. We tried to focus our attention to understand what constitutes a PUF, in terms of properties, characteristics, its instantiation and usage. We surveyed the literature for definitions of PUFs and made observations to suit our needs. Starting

with one-way functions, their translation into physical domain where both one-wayness and unclonability can be exploited in tandem were described. Existing work in the field of PUFs in terms of their definition, treatment and application were reviewed. We also presented our perspective on the bucket list of properties that can be attributed to a PUF. This will be cross-referenced in later chapters while presenting results for r-PUF. Many PUF implementations have strong associations with end application or usability scenarios. We reflect on some of the most common ones found in literature. It must be noted here, that r-PUF too, has a strong association with anti-counterfeiting application scenario.

3 State of the art

Security devices and techniques have been used with products and commodities from time immemorial. However, the use of product security techniques has gained momentum after the second world war with the growth in retail industry clubbed with globalised supply and delivery chains. The simplest of them all to pop into memory would be the wax seals. These were used for securing communications, marking/authenticating messages and as a proof of originality on products. However, in the face of technological advancement today, wax seals serve as a fond remembrance of a bygone era. With the invention of printing, security markings gained a leg up since replication was standardized. Along with printing, variety of inks and papers were developed which opened up the use of these for secure markings. This field of secure printing has continued to evolve till today with advancements in more than one dimensions. Next important scientific input which has contributed to the product security techniques is the understanding of light and its interaction with matter. Despite most of the basic phenomenon like refraction, diffraction and interference being understood by early 1800s, these were not applied to security devices (not at least for products). Denis Gabor discovered holography as we know it today in 1947. Still it did not find mass application until 1960s when lasers came around. Thereafter it established itself as one of the most preferred and recognized security techniques. However in the late 1990s a new technology - radio frequency identification (RFID) has challenged the hologram with its ease of use and cost effectiveness.

The underlying reason for any these technologies to succeed is that the initial cost and the complexity of the technology is quite high but cost per instantiation is cheap. This acts as a deterrent for people with intention of counterfeiting.

In this chapter a brief compilation study the state of the art techniques is presented. We discuss the core technical phenomenon and its implementation scope. The advantages and disadvantages are briefly touched upon with adequate references. However, a detailed analysis of each of the technique is not in the scope of this work.

3.1 Conventional techniques

In this section, only non optical techniques are covered while optical techniques deserve their own space and are menioned in later sections.

3.1.1 RFIDs

Radio frequency identification (RFID) has its origins in the spy world, where Léon Theremin of the 'theremin' fame devised an ingenious passive listening device. It was essentially a cavity resonator containing a diaphragm connected to a quarter wave antenna, which was activated only when exposed to radio wave of a particular frequency, these were then modulated by the sound vibrations from the diaphragm and sent back. Modern RFID tags are based on similar passive activation techniques.

An RFID tag is composed of an antenna which responds to a particular frequency and it is tied to a code. When queried by a reader with a given radio frequency, it responds with a signal modulated by the code that is embedded in the tag. The reader then decodes this code and sends it to the software or any other system which was seeking the information. Figure 3.1 shows a schematic of a basic setup for the operation of RFID technology.

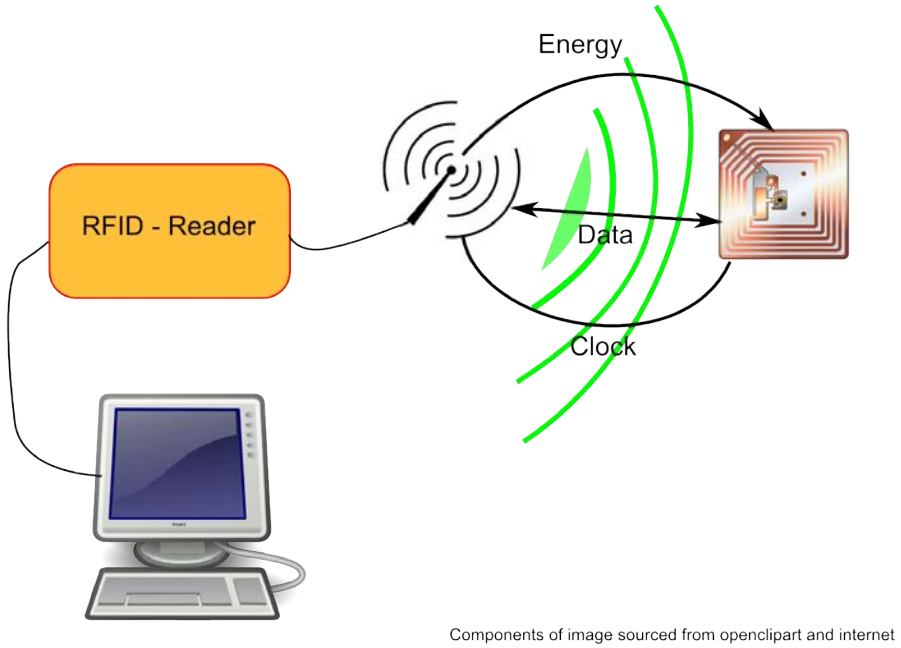


Figure 3.1: Schematic of a basic setup for the operation of RFID technology.

Standardization of the tags, readers, protocols for exchanging information and general frameworks are in place to a large extent. Currently there exist a host of international standards organisation (ISO) standards that oversee the RFID technology. The Auto-ID labs is a consortium of universities and companies across the world[1] which is responsible for the current development of RFID technology standards and policy. The most important outcome in the RFID story is the development of electronic product code (EPC). The EPC is a universal identifier or a unique number which combines the Global Trade Item Number (GTIN) which identifies the Stock Keeping Unit (SKU) along with a serial number to identify the particular instance of the product. The EPCs are defined by the standard instituted by EPCglobal[2] [55]. The adoption of the EPCs are closely related to RFIDs and one could remark that they are designed to be stored on it. However, they are carrier independent and could be adopted with other technologies too[55].

As with any technology, the adoption has continued to pose challenges. RFID as a technology has uses in secure access applications in addition to its namesake identification applications. The European central bank explored the possibilities of using RFIDs in Euro notes to aid anonymous verification[56] but it has not been implemented so far. Product identification has been the most attractive application domain for RFIDs. GS1 [57] is a non-profit association with members from over 100 countries and is dedicated to development of standards for improving the efficiency of supply chain systems. Electronic product code (EPC) is a universal identifier or a unique number which combines the Global Trade Item Number (GTIN) which identifies the

[1] http://www.autoidlabs.org/
[2] http://www.epcglobalinc.org/

Stock Keeping Unit (SKU) along with a serial number to identify the particular instance of the product [58]. EPCglobal is leading the development of industry-driven standards for the EPC to support the use of RFID in product security applications [57]. There are efforts to bring in the EPCglobal standards within the ambit of ISO. Table 3.1 summarizes the different standards and their security features.

Technical standard	Band	Range (meters)	Data	Security Features
EPC Class 0/0+ (supply chain)	Ultrahigh frequency (UHF)	3	64 or 96 bit with read/write (R/W) block	• Parity bit • CRC error detection
EPC Class 1 Generation 1 (supply chain)	UHF	3	64- or 96 bit with R/W block	• 5 bit parity commands • CRC error detection
EPC Class 1 Generation 2 (supply chain) also ISO 18000-6C	UHF	3	R/W block	• CRC error detection
ISO/IEC18000-2 (item management)	Low frequency (LF)	$<$0.010	Up to 1Kbyte R/W	• CRC error detection • Permanent, factory set 64 bit ID • Optional, lockable identifier code
ISO/IEC18000-3 (item management)	High frequency(HF)	$<$2	R/W	• CRC error detection • Two modes of operation, with write protection in one of them
ISO 14223 (animal tracking)	LF	$<$0.010	64-bit identifier	• Re-tagging counter • CRC error detection
ISO/IEC 15693 (vicinity smart cards)	HF	$<$1.5	Up to 1Kbyte R/W	• Optional protection on write command • Error checking on air interface

Table 3.1: Summary of RFID related standards

RFID technology has been adopted across different industrial domains right from US armed forces, retail chains such as Walmart, contact-less smart cards for secure access to credit cards. The adoption of the EPCs are closely related to RFIDs and one could remark that as they are designed to be stored on it. According to [59] the highest adoption was in the track and trace application as against anti-counterfeiting and mobile payment applications that are usually mentioned. It was also noted that the factors influencing the adoption of the RFID were compatibility, costs, support from the top management and external pressure (from clients, suppliers, logistics handlers etc) in the order of their importance [59].

The compatibility issues are linked to the technical challenges. However the components of the RFID such as low power transceivers, on-chip computation units, encryption-enabled memory units are all state of the art and have been understood very well individually. This notion has been substantiated to a certain extent in [59], where two different hypotheses are analysed. The hypothesis that positive influence of the technical know-how on the decision to adopt RFID was rejected as well as the negative influence of the possible resistance arising out of employee perceptions.

Different applications scenarios warrant different security scenarios. However most of them are based on exploiting one of the tag properties such as integrity of data (both its intrinsic nature and its observability), confidentiality of the tag owners' identity and importantly indistinguishability of the tag identity and clonability. There exist many protocols and attacks that are documented in the literature [60]. In addition to the attacks on the RFID security protocols, the most popular issue (if not the most important) is the privacy concern. Everything from the simple pickpocketing aid, skimming of data, tracking and hijacking of identity scenarios have been discussed. Privacy has been a significant factor that hinders the adoption of RFID technology.

3.1.2 Barcodes

In today's world, barcodes have become ubiquitous. The history and development of barcodes have been well documented in [61]. The primary application of barcodes has almost remained the same since its inception i.e., classification and identification to increase the speed of product or material handling. As with RFIDs, the catalyst for large scale adoption of barcodes was the adoption/use of Code 39[62] by United States Department of Defence for marking all products sold to the United States military[63]. There exists a variety of designs and shapes for barcodes but the most popular are the linear barcodes and off late, the two dimensional (2D) barcodes. Linear barcodes are basically a set of black bars against white or other hight contrast background. The number of bars and the width of them vary according to different standards. There were multiple approaches to standardisation mainly separated by geographical influence. In the North American countries the Universal Product Code (UPC) was widely adopted. The European Article Number (EAN) was developed as a super set of UPC and is currently known as International Article Number (though the acronym EAN has been retained). Both UPC and EAN encode the GTIN identifier conforming to the GS1 standards [64]. The simplistic nature of one dimensional linear barcodes presents both its advantage as well as it's constraints. Easy readability, simple encoding schemes have made linear barcode adoption attractive while limited data is its drawback. For use in product information domain this is overcome by use of GTIN which is linked to a database having more information about the particular product.

With decreasing cost of imaging chips and camera units, 2D barcodes (also called matrix codes) are becoming popular. They a have distinct advantage over 1D barcodes in terms of data content that can be stored on them. In the case of 2D barcodes there are many symbologies and standards associated with them, some of the popular ones are -

PDF417 This code was developed by Symbol Technologies, and is a high capacity 2D barcode capable of encoding more than 2000 characters [65]. It is represented by ISO/IEC 15438 standard. PDF stands for 'portable document format', and is popular with applications in transport industry along with the other printing intensive applications. PDF417 is essentially a stacked 1D code thereby constricting the full use of 2D features enjoyed by other symbologies.

Data Matrix International Data Matrix, Inc invented Data Matrix in 1995. It is a 2D barcode composed of black and white cells arranged in either a square or rectangular pattern. It can theoretically encode up to 2335 alphanumeric characters. However it is a variable size barcode i.e., it can be of any size between 8x8 to 144x144 cells. Two solid adjacent borders in an 'L' shape and two other borders in alternating black and white cells form the characteristic of a Data Matrix. The solid edges are called the 'finder' pattern and is used for finding and orienting the Data Matrix. While the alternating black

and white celled edges are called 'timing' pattern which are used as a count for number of rows and columns in the data matrix. The latest version is Data Matrix ECC 200 and is standardized by ISO / IEC 16022 [66].

QR Code Denso Wave, a subsidiary of Denso Corporation developed this symbolism to aid in logistics handling of automotive parts. The QR code is an acronym for 'quick response' code. It is optimised to be easily detected with a 2D image sensor, the image is then analysed by a software to decode the information. The QR code is characterised by three distinctive squares in three corners which help in estimating the scale and orientation of the code. Being invented in Japan it can encode Kanji characters (max. 1800) along with standard numeric (max. 7000) and alphanumeric characters (max. 4000) [67]. It has been standardized in ISO/IEC 18004:2006 Information technology – Automatic identification and data capture techniques – QR Code 2005 bar code symbology specification.

Aztec Code Aztec Code was invented by Andrew Longacre of Welch Allyn Inc. in 1995 and is currently in public domain. The code is built on a square grid with a bulls eye pattern at its center followed by a ring of pixels containing encoding information forming the core. The corners of this core contain orientation marking in form of specific dark and white pixels. Data is encoded in further rings of pixels around the core. Aztec code is a variable code with the largest code capable of encoding upto 3000 alphanumeric characters. It has been standardized by ISO/IEC 24778:2008 Information technology – Automatic identification and data capture techniques – Aztec Code bar code symbolism specification. Currently this code is very popular because of it's use in travel industry. The airline industry (IATA's BCBP standard) uses Aztec code for the electronic boarding passes. Several airlines use Aztec Codes in digital form on passengers' mobile phones or other electronic devices for ticketing purposes. Several European train companies like Deutsche bahn, Eurostar etc. also use Aztec codes in their tickets [68].

Maxicode United Parcel Service created this matrix code and is its biggest user. Maxicode is built on a hexagonal grid with a characteristic bulls eye in the center. Currently Maxicode is in public domain and is standardized under ISO/IEC 16023.

EZCode With the growth of camera equipped mobile phones, combined with customizable apps there exists ample opportunity to extend the adoption of matrix codes. ETH Zurich invented a low density matrix code specifically designed for mobile phone cameras called EZ code. It is a 11x11 code with 76 data bits. The idea is that these 76 bits are a handle for some information stored on a server and the software on the mobile phone contacts the server with this handle for further instructions. Currently the company 'Scanbuy' is exclusively licensed to handle such transactions [69]. It is currently not standardized but the operation principle dictates that there be a central server and this is controlled by Scanbuy.

Tag Barcode Microsoft jumped in to the barcode pool with a centralized operating model like EZcode. These barcodes are called 'tags' and they are no longer black and white matrices but are the capability to have bright colours in various shapes. The software for generating these tags, managing existing tags and reading them from different mobile phones are provided by Microsoft [70].

Table 3.2 contains concise summary of some of the most common 2D barcodes that are in use today. The

cost of desktop printing has continually decreased in the last 30 years, while the quality of printing has improved. This has in a way inspired the use of barcodes in various industries and application domains. Many customizations have been worked out for specific use in different application scenarios like logistics handling and e-ticketing. The amount of data that can be encoded in a barcode increased with 2D barcodes, there exist complimentary technology to encrypt the data and error-correcting encoding to add value in it's application. Easy implementation, specialised encoding combined with availability of easy hand-held devices to interact has boosted the use of barcodes for many applications. However, the lack of security features notwithstanding the encryption of the data stored in a barcode is a constraint when compared to other technologies. Any code no matter how strongly it is encrypted, can be easily cloned by reprinting the label with the code.

3.1.3 Secure printing

Secure printing is an umbrella term for various technologies that serve different domains such as currency, bond papers, stock certificates (in the olden days), personal identity papers/cards - passports along with identification labels for products. There are many modules or blocks of processes where the security aspect of the secure printing can be handled. In its simplest form they comprise of the special papers used in currencies, the characteristics of the paper or the material substrate is exploited as a security feature [71, 72, 73, 74, 75, 76]. One can further combine watermarks for authentication purposes.

The next major contributor to secure printing are the special inks, which are used to print special patterns or regular prints but stand out under careful examination. As long as the security lies in an obfuscated feature it is less secure. The next section 3.2 cover these to some detail when the features involves any optical phenomenon and are applicable to product security. Another feature exploited for security is the printing process itself in combination with the special inks. There exists a body of literature which deals with fingerprinting a particular instance of document or printed matter for the purposes of authentication [77, 78, 79]. Despite promising claims there are no standards for implementation in product security for the secure printing technologies. They have however found their use in the currency notes, legal documents and label markers for packaging.

3.2 Optical techniques

This section delves into 2D, 3D diffractive structures and volume renderings such as holograms used as security techniques. There exists various claims for the *first steps* is this field[80]. Some of the earliest works which have significant influence on the progress of holography include the Lippman's photography plate, where multiple wavelengths could be recorded on a single surface. The formal beginnings of this field can be traced back to Gabor who coined the term *hologram*. With the maturing of laser technology, significant improvements were made in the field of holography in 60s and 70s in form of off-axis holography, volume holography and white light transmission holography (also called Rainbow holograms). During the efforts to commercialize this technology, the technology moved from photographic plates to diffractive micro structures driven by replication needs. In this phase various different 2D and 3D diffractive structures were realized. Today there are many more such diffractive structures in security application as compared to the conventional volume hologram. However, one can group them together under the broad umbrella

term of optically variable devices (OVD). A definitive text on this subject by van Renesse [81] gives a clear understanding of the different types of holograms, optical techniques and categorization of OVDS.

3.2.1 Diffractive Optically Variable Image Devices - DOVID

Optically variable devices are characterized by iridescent display of colours based on the angles of observation[81]. The variation in observable colours forms the core of the security aspect of OVDs. Solutions where diffractive structures are the means to realize this, are called *diffractive optically variable image devices (DOVID)*. These devices are usually realized using light interference between two beams incident from different angles to form relief patterns on a photo resist layer ([82, 83]). This relief pattern can be transferred to a master relief which can then be used for replication. Relief patterns created by light interference usually result in symmetrical, sinusoidal cross sections. These sinusoidal relief patterns diffract light mostly in first order, thereby giving the name *first order optically variable devices* [81].

Most holograms in this type are the rainbow holograms. The single plane holograms like the VISA logo are very popular. There exist multiple plane holograms which increase the complexity and information content but displaying separate images in different planes. The instances where the holograms are transmissive, are made reflective by having a mirrored surface behind. With the advanced lithographic techniques such as e-beam (electron beam) lithography one can create complex patterns of diffractive structures resulting in specific visible features. Kinegram, Pixelgram, 2D dot-matrix tags are some of the implementations which can be categorized here. Figure 3.2 shows examples of DOVIDs in application.

Figure 3.2: Examples of DOVID. Source - Internet images.

The colourful representation of the inherent patterns from the first order DOVIDs do not add value to the security aspect of the devices, but mainly assist in ease of inspection. Devices that exhibit sensitiveness to colour representation about the plane of the rotation of the device, when observed in zero order are called Zero Order Devices (ZODs). These devices have a defined behaviour for the specular reflections related to the plane of rotation. The ZODs are usually composed of sub wavelength features (< wavelength of visible light) that result in large angles for first order diffractions [81].

3.2.2 Interference security image structure - ISIS

Volume holograms, lustre inks made of high refractive index (RI) micro particles, multiple layer structures ([84]) with each layer having different refractive index among others can be categorised here. These security structures have different layers contributing in a specific interference behaviour forming the core of the security feature. The optically variable inks (OVI) with defined colour shifts are usually due to a combination of two separate layers with different RI. Figure 3.3 shows some examples of ISIS structures in application.

Figure 3.3: Examples of ISIS implementations. Source - Internet images.

3.2.3 Security features in OVDs

The security features of OVDs vary across different techniques and their applications. The ease of observability/inspectability, has been the most important characteristic of OVDs, security not withstanding. In the beginning when these were first introduced in the market as a security feature, they were to a large extent true to their claims. OVDs could neither be photocopied, nor tampered due to easy verification procedures. They were also popular since the technolgy was complex and costly for easy counterfeiting. Technological breakthroughs in lasers, optical material processing and overall accessibility of technology has lowered the expectations of security characteristics from an OVD. However there exist many variations which exploit application specific needs and new techniques are researched and developed all the time. Many a time, a combination of OVDs will satisfy most security requirements, for example the currency notes usually

have OVI markings, volume holograms, diffractive structures in patterns-all combine to give better security against counterfeiting.

3.3 PUF - implementations

This thesis deals with a specific instantiation of physically unclonable function (PUF) and hence it is of interest to analyse the state of the art in this domain. An in-depth definition of PUF as a concept and analysis of its properties is presented in chapter 3 along with the formalized model of PUF and the different ways of classifying the various implementations. In the current section, various instantiations of the PUFs are listed with brief details and commentary. Two words - implementation and instantiation in conjunction with PUF will be used frequently through out this thesis. For the purposes of clarity, implementation refers to a particular PUF technology or a method while instantiation refers to the individual instance/ device / tag of a given given PUF implementation. A brief qualitative excerpt on PUF evaluation protocol and evaluation metrics presented here to facilitate understanding the commentary on each of the PUF implementation. A more detailed and quantitative analysis will be presented in the next chapter.

Evaluation protocol The generalized protocol seen in literature in conjunction with PUF is usually composed of a *challenge-response pair* (CRP). The principle notion is that the output of a PUF is a random variable and is unique for a given set of input conditions. In practice, the environmental conditions for operation are kept constant and the PUF evaluation is carried out by issuing a single controlled source of stimulus (challenge) and the resulting response is recorded. By definition of PUF, one cannot invert the response to compute the challenge. This defined relationship between the challenge and the response forms the core of the PUF. There are many kinds of PUFs - for which there exist only one CRP or, a finite set of CRPs or, an infinite set of CRPs and PUFs which have a predefined set of valid-invalid CRPs.

Evaluation metrics The way to compare and evaluate the performance of the different PUF technologies is inspired from information theory. The notional distance between two responses for the same instantiation of the PUF for a given challenge is called the intra distance measure. Similarly the distance measure between two response from two different instantiations for a given challenge is inter distance. The use of distance measure, by the way of Hamming distance (or fractional Hamming distances) for intra- and inter-distance measure for a given PUF implementation is common in PUF literature . The intra-distance measure helps in understanding the robustness or the environmental factors influencing a given PUF, where as the inter distance measure brings about the uniqueness associated with the random variable in the PUF output. The inter- and intra-distances were also covered in previous chapter 2.2. When a PUF is used for authentication or identification, the use standard definitions of *false acceptance rate* (FAR) and *false rejection rate* (FRR) are also prevalent. For some PUF implementations, the entropy in bits is also used as a metric [85, 86], since this is helpful in cases when a PUF technology is susceptible to predictive analysis and the inter-distance measure no longer conveys the uniqueness information effectively.

3.3.1 Arbiter PUF

Arbiter PUF was conceptualized by Gassend et al. [17, 19] for exploiting the random variations in the silicon fabricating process of integrated circuits (ICs). The delay along the data flow path has some inherent randomness owing to the silicon fabrication process and is bound to a particular instantiation. The term *switch blocks* was coined by [17], it contains two inputs and two outputs representing two different channels of data flow and a control bit. In its simplest implementation, it consists of two 2:1 multiplexers. The measurement of delay and its binding with the IC can be used in identification and authentication protocols. To increase the security one could process a vector of bits instead of just one bit. The accurate measurement of the delay usually needs a long observation duration[17]. If one considers a vector of bits then the measurement times are almost unacceptable for practical use.

To overcome the delay measurement problem, Lim et al.[87, 88] proposed a arbiter which measures the difference in two data paths, giving rise to the term *Arbiter PUF*. There are many candidates for implementation of such an arbiter, but Lin et al. in [89] conclude that a SR-Latch (set-reset latch) is the best candidate. Figure 3.4 shows the implementation scheme of the arbiter PUF consisting of a series of switcher blocks followed by an arbiter module. The initial results by Lim et al. [88, 88] show a better performance of this method when implemented on ASICs (application specific integrated circuit) as against FPGA (field programmable gate arrays) with inter distances being 23% and $\sim$1% while intra-distances being $< 5\%$ and $< 0.5\%$ respectively. The unusually high intra distance of 5% for ASIC implementation was observed as a result of variation in operating environment (increase in temperature). This exposes the system's fallibility in terms of robustness. However the cause for concern lay elsewhere. It was noted fairly early in the de-

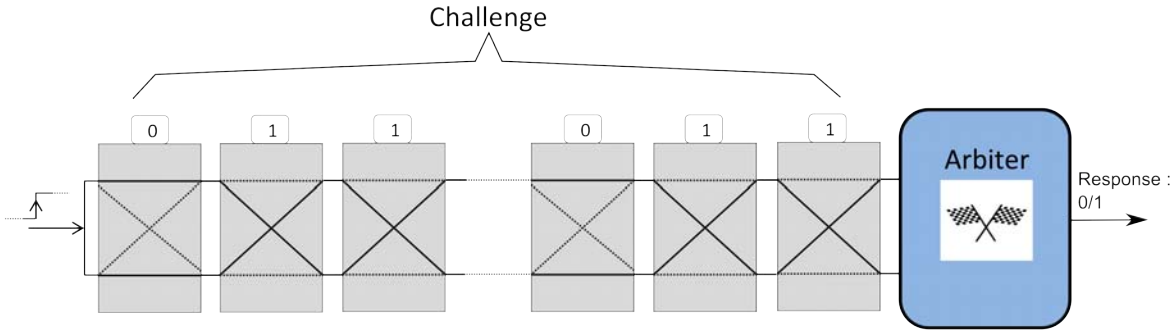


Figure 3.4: Schematic of Arbiter PUF from [87]

velopment of this technology [19], that the overall delay is additive in nature and can be attributed to the various elements in the data path. This linear relationship between the input and the output brings about a deterministic outlook to the system (although not complete but susceptible to predictive analysis), thereby rendering it less secure. To avoid this linearity problem, a variable delay element was introduced in the data flow path and in another version a one-way hash function was used to generate a random vector as the input to the delay line. These techniques, to some extent, strengthened the system. There exists body of work dealing with estimating/understanding the data flow path elements where delay elements are modelled

mathematically and are used in predicting the outcomes of arbiter PUFs[17, 90, 88, 87]. The prediction error of 3.5% was achieved after observance of 5000 CRPs for ASIC implementation and 0.6% error for FPGA implementation after observing 90,000 CRPs. Subsequently [87] introduced *feed forward* design to incorporate some non-linearity in the data flow path. The use of an arbiter component in between two switching blocks realises this effect. This intermediate arbiter increased the inter- and intra-distance measures to 38% and 9.8 %. for the ASIC implementation. However, more advanced modelling attacks were developed [14, 18] and the predictive error was shown to be < 5% after observing over 49,000 CRPs in a simulated environment.

The implementation of arbiter PUFs on FPGAs is also a hotly pursued topic in research circles, [91, 92] and many others have tried to optimize the conditions for PUF on a FPGA, while utilizing innovative feed forward architectures and non-inverting functions to control the input/output to the PUFs. All these approaches are focussed on increasing the non linearity in the PUF implementation as a counter to the modelling attacks. At the same time, there are contemporary works [14, 18], which provide designs for sophisticated modelling attacks.

3.3.2 Coating PUF

Trusted hardware is a big market and protection of intellectual property in terms of chip design, on baord algorithms, security enabling ICs, hardware license keys etc. fall into this category. It is given, that players in this hightech field have access to advanced technical know-how and tools. Some exploits, debunking the security of the hardware key dongles, chips with write protection can be seen on websites like these [93]. One can observe that security by obscurity principle is still a bad idea even when dealing with hightech, micro-nano features based techniques. Tuyls et al. [21] propose a capacitive PUF, which does not only takes advantage of the variations due to manufacturing random processes but explicitly introduces some random elements into the structure, that play a vital part in the functionality.

The cross section of the coating PUF as shown in Figure 3.5, consists a layer of randomly distributed particles with varying dielectric constant. This layer is sandwiched between two metal layers to enable the measurement of capacitance. One of these layers is shaped as a comb which helps in localized measurement of capacitances. Thus the entire measurement mechanism is integrated on the chip. Any tampering by the way of etching or reading using a focussed ion beam will destroy the random structure of the dielectric particles thereby invalidating the capacitance reading. The coating is opaque in nature (absorbs all light from infrared to UV frequencies), which thwarts any direct observation of the pattern. The coating PUF does not use the measurements of the capacitances directly as a secure key, but instead it uses it to generate a set of public and private keys which will be stored on the IC along with a signature scheme. The results reported by [21] show impressive inter- and intra-distances of $\sim 50\%$ and < 5 % respectively.

3.3.3 Fiber structure PUF

There are many works which can be mentioned under the fiber structure unclonability. In the security printing section 3.1.3, methods based on print process variations and inherent material properties were mentioned. The use of these variations and building of an authentication system while proving the physical unclonability of the process was presented in [22]. This work details a complete authentication system in the

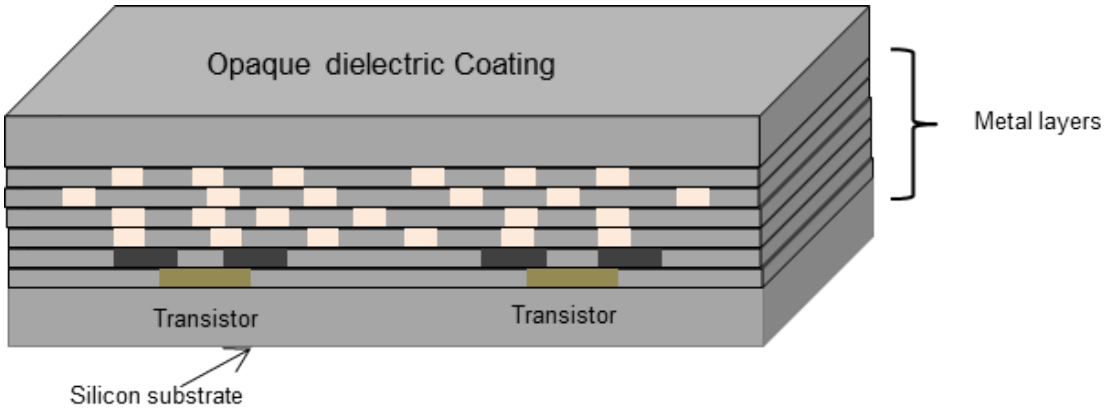


Figure 3.5: Cross section of a Coating PUF.

PUF framework based on the random distribution of fiber structures on the surface of a paper or a packaging material.

The strength of this approach lies in its simplicity. Since the fibers are in the micro meter range, a low powered microscope is sufficient for visualizing them. A small designated area of $0.4cm \times 0.4cm$ is used as the tag and the scanning resolution requirement is computed to be in the order of 1200 (dots per inch) . The authors propose a camera equipped cellphone in addition to a macro lens attachment to capture these fiber structures. The image obtained is hashed and stored during enrolment. During verification process, the same process is repeated and the server is queried to verify the stored hash against the computed value. The authors present results with 0% error rate in the measures samples.

3.3.4 Laser-marking PUF

The growth in laser technology and miniaturization has allowed for it to be incorporated in consumer devices since late 80's. A vast range of optical storage devices such as the compact disc (CD), digital versatile disc (DVD), blue-ray disc etc. have found their way into most homes and offices in some form or the other. More often than not, the distributors of content on these mediums feel the need to assert it's authenticity either for security purposes or protection of intellectual property.

CD Fingerprinting

Hammouri et al. in chapter 9 of [11] put forward a method which helps in binding an identity to each instance of a CD and coined the term *CD fingerprinting*. The authors present a full case study for CDs but in theory this can be extended to all other optical storage media. Information is stored on a CD using *lands and pits*, markings made by a laser on a polymer substrate, and is read by noting the variations in reflections when queried by a laser beam. Hammouri et al. exploit the random variations in laser writing process which is caused by unstable CD writing speed. A variation in the order of $\pm$ 0.1m/s writing speed, results in tens of nanometres variation in lands and pits. This can be measured fairly accurately by the varying strength of the photo detector dielectric signal while reading process. The authors present a scheme which utilize the fuzzy extractor principle from [40] to overcome the noise issues while reading to construct a hash code. The results presented are fairly impressive at $> 50\%$ and < 10 % for average inter- and intra-distances respectively. The attractive feature of this method is that it is fully integrated into the current technology and probably only requires some low level drivers to read the photo detector output in the verification application.

Image based PUF

Shariati et al. [94] propose another laser marking system, based on the random laser instability and the properties of the material that is being used as a tag. They explicitly target the anti-counterfeiting problem and the markings can be made on packaging material or embedded tags to the products themselves. The security markings are essentially small features such as dots and lines in the order of 60μm. Each instance of these markings will have a random variation in the sub micron range. The markings are read using white light interferometry and the random variations extracted to build a hash code which can be verified with successive readings. The exact scheme and its validity for using these marking as a anti-counterfeiting solution are presented in [26]. The authors report highly impressive results with mean inter and intra distances at $\sim$ 41 % and $\sim$ 16 % respectively [95]. The robustness, uniqueness and conformance to the concept of a PUF notwithstanding, only the practicality of the method is complex prone. While the PUF carrier or the tag itself come at low cost, the use of white light interferometry as a verification mechanism brings in complexity in terms of both operation and higher costs.

3.3.5 LC PUF

Guajardo et al. [43] present another PUF scheme based on variable capacitance similar to the coating PUF discussed earlier. The LC-PUF, as it's name suggests is an inductor capacitor resonator with a characteristic response curve. It is basically a capacitor where a a randomized dielectric is sandwiched between two metal surfaces and an inductor connected to one of the metal contacts. The authors report that some properties of the inductor too may be subjected to random manufacturing process variations. Thus every LC resonator produced will have a different resonant frequency and a unique frequency response curve. The authors report robustness in terms of test for over 500 instances and accurate reproducibility of frequency response curves up to 1Mhz frequency scan with entropy between 9 and 11 bits per resonator.

3.3.6 Speckle based PUF

Optical PUF

Pappu et al. in [8] and the PhD thesis [7] were probably the first works to define the physically unclonable functions while extending the one way functions concept from cryptography. The solution presented by them is popularly referred to as an optical PUF, since this happens to be one of the few PUF technologies which is optics based. The PUF token as the authors put it, consists of an epoxy plate which has micrometer sized glass balls randomly embedded in them. When a laser is passed through this token it creates a speckle pattern that is uniquely bound to the angle of the illumination, position on the token where the beam hits and the token itself (owing to random distribution of the refractive micro spheres). The speckle pattern is recorded and hashed to produce a 1D vector which serves as a code that can be stored for verification purposes. A schematic depiction of the proposed setup is shown in figure 3.6.

The angle of illumination and the position on the token is treated as challenge and resulting speckle pattern as the response. Pappu in [7] details the hashing algorithm based on Gabor hash functions [96] which yield a unique hash vector for every token and every angle of illumination. The average inter- and intra-distance measures were computed for the Gabor hashes and were reported to be $\sim$ 50 % and $\sim$ 25 % respectively. Extensive theoretical analysis was carried out for the proposed technology by [85, 16, 44] and the entropy was calculated to be about 0.3 bits per pixel of the captured speckle pattern.

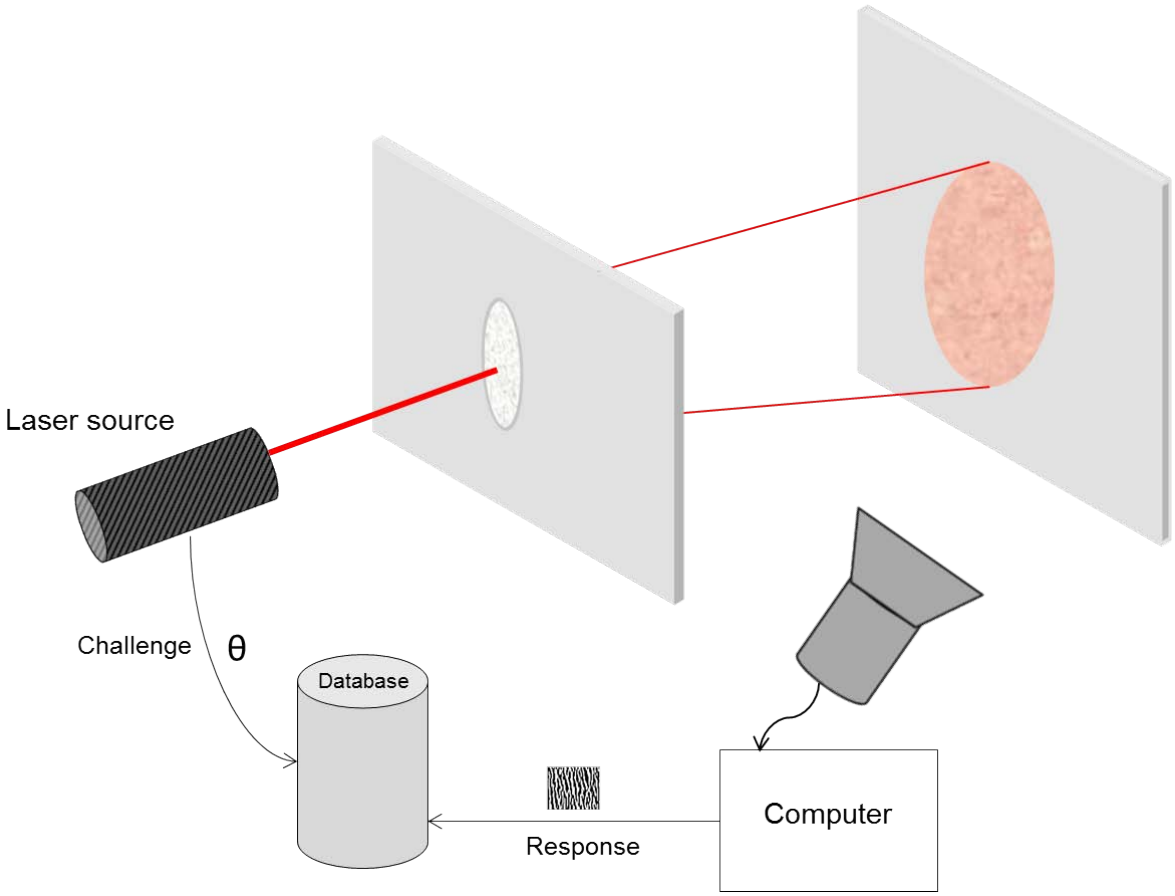


Figure 3.6: Schematic of the Optical PUF.

Optical PUF has in many ways been considered as a bench mark for the further development of the PUF. This was one of the first works which established the *one-wayness* associated to physical phenomenon and it's use for security purposes. There were many prior works which proposed such technical solutions but did not bring forward a complete frame work with both theory and implementation. The discussions in [7] on matters related to complexity associated with clonability, tamper evidence and well defined registration/ verification protocols have a set a standard for presenting the results for later PUF technologies. However in the absence of any lack of standards in this domain, it can be safely said that [7] and Section 6 of chapter 1 in [11] form a comprehensive guideline for presenting, comparing and evaluating PUF solutions.

Paper Speckle

The optical PUF while setting the trend for extensive research in the field of PUF, was noted for its lack of implementation simplicity. Sharma et al. in [97] propose a speckle based technique which used bench top, consumer electronics in its implementation. Extending the concept that the speckle pattern is unique for a given set of conditions to the microscopic structures and the printed matter on a paper, a paper based PUF is built. A partially coherent source illuminates a selected region on the paper which may contain printed material or some markings, a microscope is used to image the resulting speckle pattern on to a imaging device. This speckle pattern is then processed with the Gabor hash algorithms to produce a unique vector which can be stored for later verification. The authors report that the imaging and the illumination can be accomplished using off-the-shelf components such as an USB microscope and a laser diode.

The effects of printing, writing/marking with different inks is discussed and use of insoluble inks seem to positively increase identification. The main application is document security and various aspects of it such as ageing and water soaking is explored and the results are found to be consistent. The envisaged set up for this technique is shown in figure 3.7.

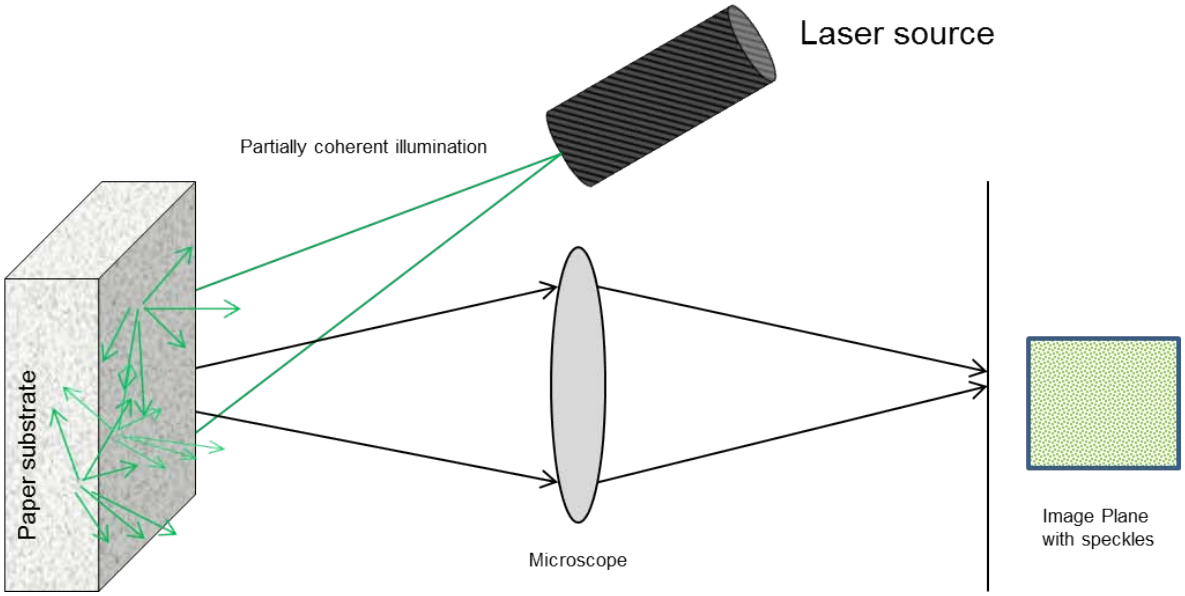


Figure 3.7: Setup for PaperSpeckle PUF.

3.3.7 Magnet PUF

The random distribution and orientation of the ferrous oxide particles in a magnetic layer gives rise to a distinct and unique magnetic response. This is encoded and used in identification and security of magnetic swipe cards and is currently offered as a commercial solution [98]. The concept was first disclosed in a patent by [99].

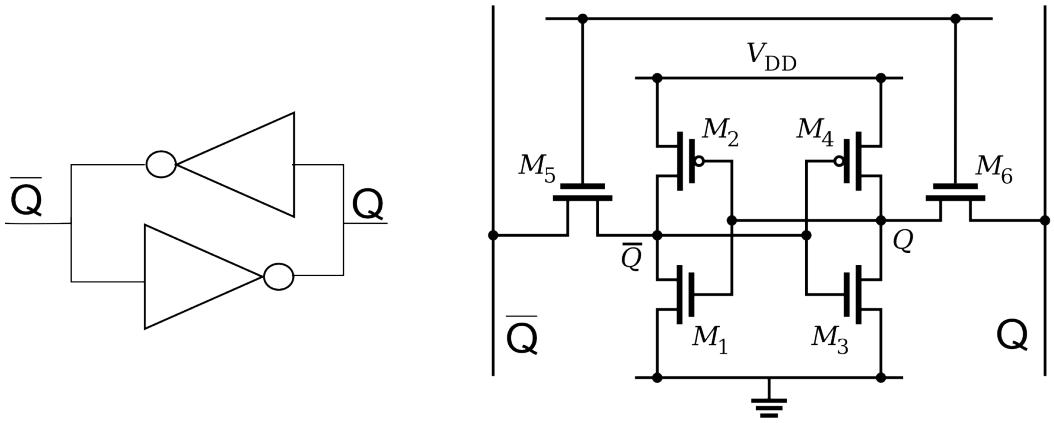
3.3.8 Memory PUF

The variation in silicon manufacturing processes during IC fabrication, incorporates a random element which has been exploited in different ways. One such manifestation of this uncertainty is the settling state of a digital memory element. The simplest digital memory element has two stable states representing 0 and 1. On power up, voltage is applied to a memory cell and there is no certainty that the memory cell will take a either 0 or 1 stable state. Each memory element has a unique preference for its stable state based on microscopic variations in the threshold voltages for the transistors that make up the memory cell. There exist many variants of PUF that exploit these phenomenon, some of the well documented approaches in literature using static memory, latches and flip flops are recorded here.

SRAM PUF

Static random access memory (SRAM) was found to exhibit a random behaviour on power up. In chapter 2 of [11], the authors report an intensive study exploring SRAM memory elements by different companies,

fabrications technologies from 180nm to 65nm, from different foundries and were able to confirm random behaviour across the board. Holcomb et al. in [100] propose the use of this technique to extract a secure fingerprint in a RFID, to be used as seeds to true random number generators. In one of their later papers [101] they provide results from use of these SRAM finger prints in intermittently powered devices used as identification with success rates between 96 % and 100 % for different types of SRAM memories. In terms of average distance measures, the authors report $\sim 43\%$ and $< 4\%$ for inter- and intra-distance respectively for commercial SRAM chips. For SRAM block of micro-controllers an average distance of $\sim 49\%$ and 6.5% for inter- and intra-distance measure respectively. The use of SRAM fingerprints in true random number generators were impressive too with the approximate entropy levels passing the standard NIST (National institute of standards and technology) test suite. In an extensive testing [20] that was done in FPGA implementation of SRAMs and the average inter distance was ~ 50 % while the intra distance measure varied from < 4 % to < 12 % for conditions with fixed temperature to large deviations in temperature. Figure 3.8 shows both the logical circuit as well as a schematic of the SRAM cell that forms the basic component of the SRAM PUF. Recently the same concept has been extended for secure identification of



a) Logical circuit of SRAM cell

b) 6-Transistor electrical circuit of an SRAM cell in CMOS Technology

Figure 3.8: a) Logical circuit of SRAM cell, b) Schematic of 6 transistor SRAM cell

wireless sensor nodes (WSN). In [102], the commercial 90nm 6T RAMs were evaluated for application as a PUF. Different tests related to variation in voltage (important since the application is in WSN, usually used in low power environments), ageing and changing temperature conditions were studied while proving the validity for use of this technique as a PUF.

In a slightly different variation of the SRAMs for PUF, Fujiwara et al. in [103] propose to use the addresses of the failed individual memory cells in a SRAM array as the PUF. The SRAM are susceptible to static noise which can be induced with voltage variations. There exists a figure of merit called static noise

margin (SNM) which is a measure of the memory cell failure leading to deletion of the information it is holding. The authors define a *ID generation* procedure, during which the SRAM is first initialized and the voltage noise in the array is increased to a predefined level, at which some memory cells undergo failure. The addresses of the failed cells are recorded to form a PUF response. The static noise margin of each of the cells is different and is dependent on the manufacturing process variations. In the world of SRAM failure models, one could categorize this as a *hold failure*. The performance of these kind of PUFs are reported in terms of average inter- and intra-distance measures of ~ 64 % and < 1 % for an experiment involving 53 ASICs and 128 bit PUF IDs. In [104], the authors discuss another variation of SRAM failure - the *write failure* to generate the PUF response. Here, the duty cycle of the line voltage is altered to induce a write failure and the addresses of the failed bits are recorded as a PUF response. The authors present a simulation based analysis with high uniqueness based on average inter-distance of ~ 50 %.

Butterfly PUF

Though [20] reports results with SRAMs in FPGAs, the use of the SRAM PUF technique is limited in ASICs due to the fact that it is a common practice to hard rest the SRAM memory cells after power up. In [105], Kumar et al. propose a new configuration of latches in FPGA which mimic the behaviour of the SRAM cell during power up. Figure 3.9 shows the basic component of Butterfly PUF. The output of the two data latches are cross coupled, the preset of one latch and the clear of the other are permanently held at 'zero' state while the excitation signal is simultaneously fed to the remaining preset and clear of the two latches. The latches are driven to unstable state by making the excitation signal high, To start the PUF functionality, the excitation signal has to be set low, which then forces the latches to take either of the stable states. This choice of stable states is dependent on delays in the inter connections between the two latches and cannot be determined beforehand. The authors report average inter and intra distance measures of 50% and $< 5\%$ respectively which include operation in environment with large temperature changes. Additional advantage of the butterfly PUF is that, it does not require a power up which means that the verification function can be called any time during the application.

3.3.9 Resistance based PUF

A PUF technique based on variations in resistance in the power handling circuitry of a chip was proposed in [106]. Equivalent resistance values computed using voltage drops in the power distribution circuits, were found to be varying across different chips owing to variations in the manufacturing process. One drawback of this technique is that external measurement techniques need to be employed to capture the precise voltage drops in the circuitry.

3.3.10 Ring Oscillator PUF

The delay based PUF introduced by [19, 17] can take another form apart from the arbiter PUF discussed earlier. It was noted by the authors that precise delay measurements were difficult and the arbiter was introduced to compare the delays instead. In the same work, authors propose another method to overcome the need to measure delay, they propose to introduce a negative feedback giving rise to an oscillator circuit. The frequency of the oscillations are directly dependent on the random delay present in the given circuit instance. The measurement problem is overcome since an edge detector followed by a counter at the end of

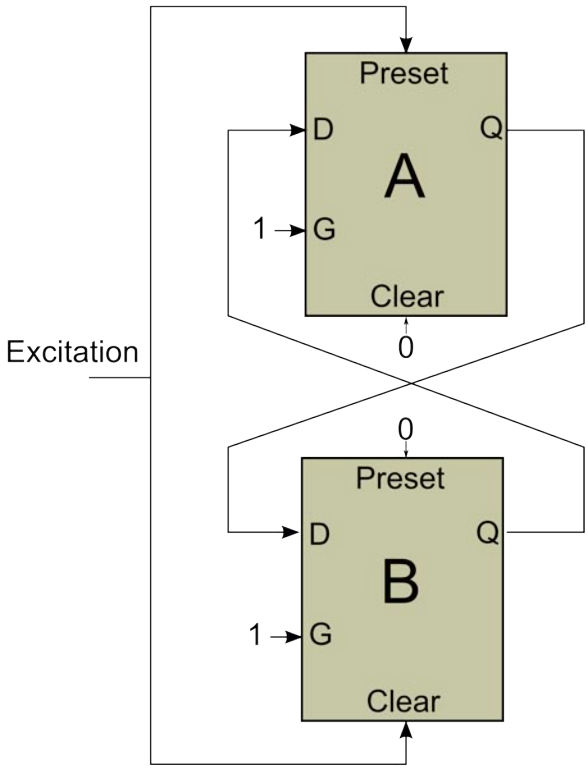


Figure 3.9: Basic component of Butterfly PUF.

the oscillator which measures the frequency. The basic scheme as envisaged the [19, 17] is shown in figure 3.10 and is known as *Ring Oscillator PUF* (RO-PUF) in literature. As noted in case of the arbiter PUFs,

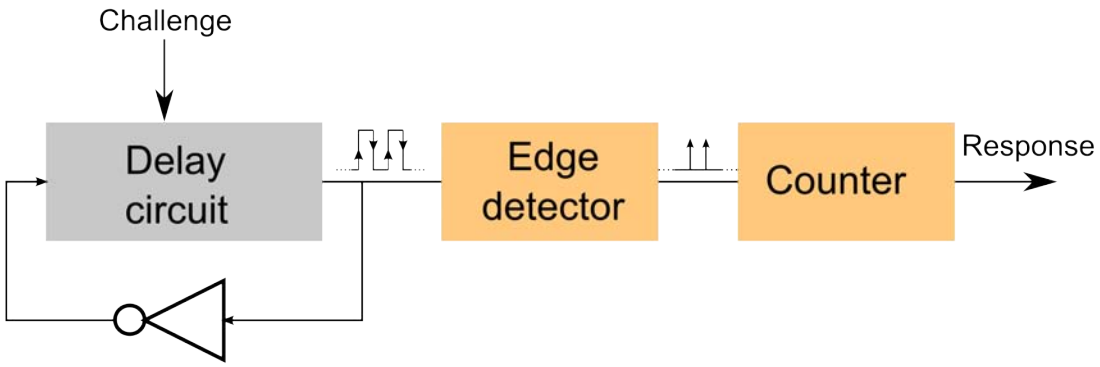


Figure 3.10: Basic configuration of RO-PUF.

the environmental conditions affect the delay measurements, which is manifested in terms of frequency in RO-PUF. In arbiter PUF, the differential was measured which negated the effect of environment. Similarly, in RO-PUF a divider is used which gives a ratio of two frequencies from two different oscillators in par-

allel (figure 3.11). Gassend et al in [19, 17] use the term *compensated measuring* for this. The authors in [46] propose another measurement compensation technique with a *n*-set of ring oscillators in parallel connected to two n-to-1 multiplexers followed by two frequency counters. The multiplexer select signals can be construed as a challenge set for the PUF. In its simplified form, only two oscillators paths can be used in conjunction with a comparator which outputs 1 or 0 based on which oscillator has higher frequency count. The challenge can be parametrized as the input to the oscillator then one could get a string of random 0 or 1 bits as output which would serve as the response from the PUF. The schematic for the both these scenarios are shown in figure 3.12. In the case of n-ring oscillator implementation, there could be a problem of bias owing to the fact that some oscillator paths may be much faster than others. This would reduce the challenge-response set. Suh and Devadas in [46], propose two different methods to resolve this issue. First, a fixed pair of ring oscillators could be compared resulting in $\frac{n}{2}$ bit output response from a n-set of ring oscillators. Alternatively they apply a *1 out of K* compensation technique, where only a specific set of *K* ring oscillators are evaluated and only the result from the pair of oscillators which have the highest difference in frequency is output. This highly selective method for outputs results in a spectacular average intra distance measure of < 0.5 % in the light of temperature variation of 120deg centigrade, while the average inter distance measure was found to be $\sim$46 % when, tested across 15 FPGAs.

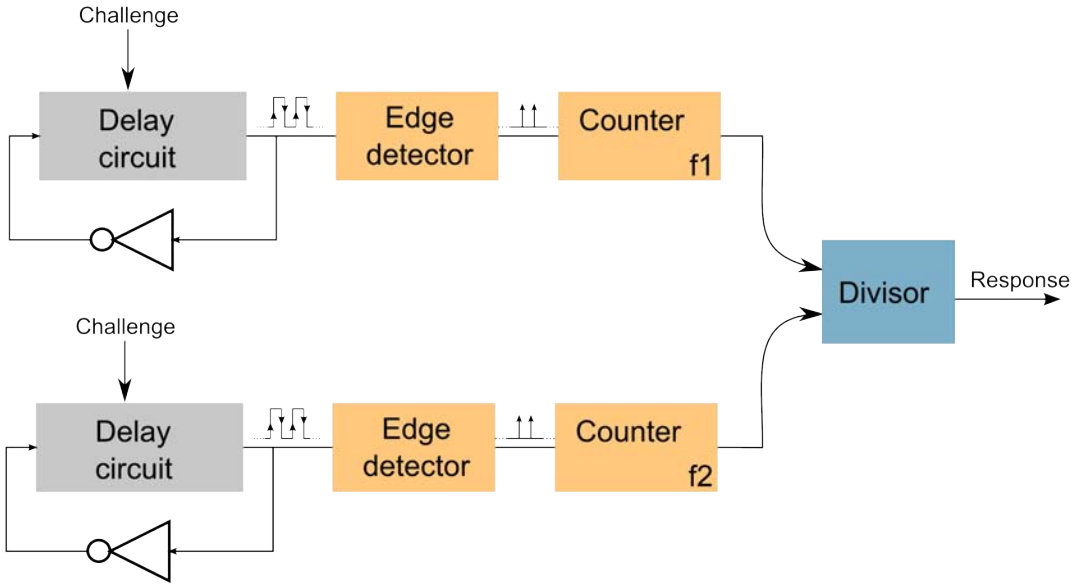


Figure 3.11: RO-PUF with Divisor

In [107, 108], Maiti et al. analyse the causes of the systematic bias in RO-PUF and propose various methods to reduce or overcome them. In an improvement over the *1 out of K* compensation mechanism of [46], the authors propose the selection of ring oscillators based on configurability instead of frequency difference. Maiti et al. in [109] conduct large scale analysis, large to the tune of 125 FPGAs with a slightly different compensation measurement technique. They compare each of the neighbouring ring oscillators giving rise to *n-1* bit output for a n-set of ring oscillators. The average inter- and intra-distance measures were reported to be $\sim$ 47 % and $<$ 1 % respectively. In the face of change in environmental conditions

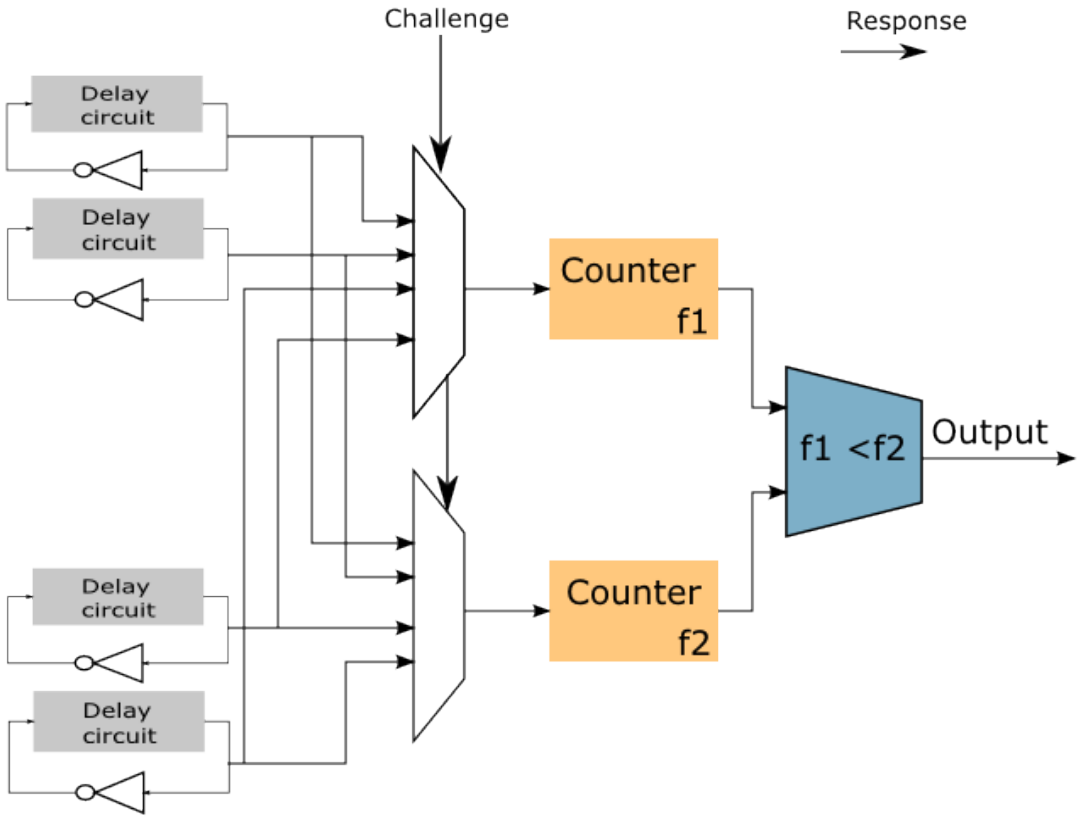


Figure 3.12: n-to-1 comparator RO PUF

owing to reduced supply voltage, the intra-distance goes up to $\sim$ 15 %. In other works by Maiti et al. [110], they propose an identity mapping function along with test statistics for the frequency differential measures to increase the challenge-response set. In the light of reduced number of bits from technique aiming to mitigate the system bias or the cost involved in building a PUF system which is capable of generating longer keys, this approach throws up interesting possibilities. However they are resource and time intensive in nature.

Yin et al. in [111, 112] propose variations to the *1 out of K* method by [46] in form of grouping the ring oscillators, which ensure that most of them are used in output as opposed to the few selected in the previous methods. In [111], a mutually exclusive grouping based on minimal frequency variation is proposed. The minimum frequency variation is kept above a given threshold, which ensures that comparison between oscillators within the same group is stable. More detailed analysis of this grouping and further variations are presented in the dissertation of Yin [112], all of which are focussed on maximizing the resource utilization of the ring oscillators while not compromising on the mitigation of the systematic bias.

Merli et al. in [113] propose a different approach to improve the quality of the output from RO-PUF. They show that the resulting frequency of a ring oscillator is strongly influenced by its neighbouring circuits. Thus by controlling the ON/OFF state of the neighbouring ring oscillators, they claim an improved PUF response. In addition, they also exploit the dependence of the RO frequency on it's run time. Two different

configurations for ring oscillators are explored - random and chain. The average inter- and intra- distance measures for random configuration was ~ 44 % and < 5 % while for the chain configuration was found to be ~ 49 % and ~ 6 % respectively. The reliability in both the cases was found to be > 98 %.

Chen et al. in [114] propose another variation called the *Bistable Ring PUF*. A ring of even number of inverters having two stable states and which are individually addressable, form the core of the PUF. In its implementation, the authors replace the individual inverter with a set of NOR/NAND gates sandwiched between a multiplexer (MUX) and demultiplexer (DEMUX). The select signals of the MUX and DEMUX is the challenge bit and this selects either of the NOR/NAND gate as the active ring component. In a 64 component ring, the challenge signal is a 64 bit vector and the challenge set will be 2^{64}, since either of NOR/NAND gates are selectable. The ring is initialized using a reset signal to all NOR/NAND components, after the reset signal is removed the ring is unstable and each of the selected NOR/NAND component (based on the challenge vector) shall then try to attain a stable state. This stabilization process is based on inherent manufacturing variations and is random, thereby giving rise to a PUF. The authors present a 64 ring implementation on eight FPGAs with impressive average inter- and intra-distance measures of ~ 50 % and < 3 % with settling times in the order of 50 μs for each of the inverting gates. The authors also remark on ageing and environmental conditions, but do not provide any details of possible modelling attacks or other failure scenarios.

3.3.11 RF-DNA

The radio frequency identification tag based on random distribution of components was proposed in [115, 116]. A small token made of silicon rubber sealant is used as base and thin copper wires are randomly embedded within. This near field scattering pattern of the electromagnetic waves is dependent on the random pattern of the copper wires in the tag. A matrix of antennae can be used for scanning/measuring the RF response of the tag.

3.3.12 Glitch behaviour PUF

Another propagation delay based PUF was first proposed by Anderson in [35]. However Anderson does not utilize the delay effect directly in his proposal, but instead makes use of glitches. In combinational networks, the delay between the input and the output can propagate to neighbouring circuits causing the output to hold wrong or invalid value at certain instants of time. In digital circuit design, there is sufficient emphasis on understanding design issues which could overcome this unwanted behaviour. Anderson proposes an FPGA specific solution which uses this glitch behaviour in combinational logic. In its simplest construction, the PUF cell consists of two look up tables (LUT), configured as shift registers tied to two carry chain multiplexers. There are four inputs and two select signals for both these multiplexers. One input to both these multiplexers are tied to 'zero'. The output of one carry multiplexer is fed as the input to the following multiplexer, while the remaining input for the other multiplexer is tied to 'one'. The outputs from the LUTs are fed as the select signals to the carry multiplexers. A schematic showing this arrangement is shown in figure 3.13.

When this setup is fed with two vectors (can be considered challenge), the final output is determined by the delay variations in the data flow path of the two LUTs and the propagation delay from the carry-on multiplexers. Combining a chain of such circuits one could generate a string of PUF vector. Anderson

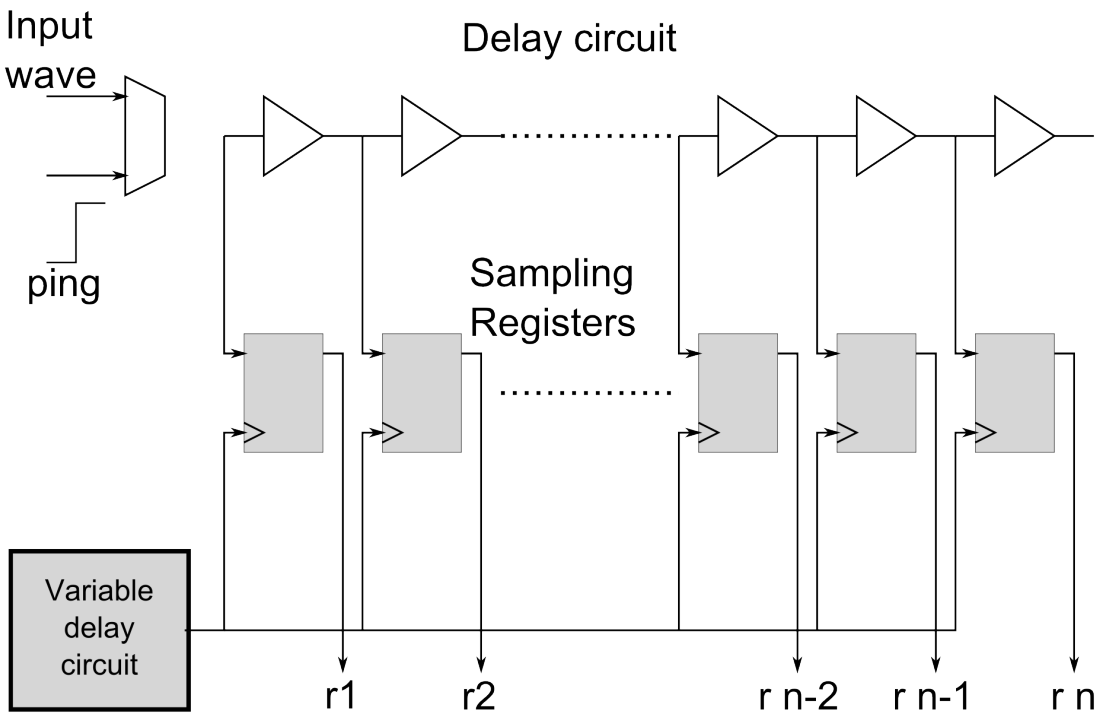


Figure 3.13: Schematic of Glitch PUF.

reports an experiment, where 128 bits were generated with the average intra- and inter-distance measures being ~ 48 % and < 4 % respectively.

The term *Glitch PUF* was however coined by Shimizu et al. in [117]. They propose a more in-depth analysis of the glitch behaviour, where they sample the glitch waveform with high frequency and quantize the sampled data to produce a PUF response vector. The rationale being the parity of the glitch detection being a random number. In a later work [36], they present the details of their proposed implementation, followed by results.

3.3.13 Threshold voltage PUF

One of the earliest works in identification of integrated circuits was presented by Lofstrom et al.[118]. The authors propose a non-alterable identification (in later works, this comes under PUF) based on random variations in MOSFET (Metal Oxide Semiconductor Field Effect Transistor) threshold voltages due to manufacturing process. A set of addressable MOSFETs array with common gate and source and sequentially connected drain terminals are used to drive a resistive load. The current through the load will slightly vary depending on which MOSFET is driving it. The voltage across the load is measured and quantized to produce a random bit output. A sequential reading with different addressing (serving as a challenge) will provide a random bit vector, which can be used in identification of the IC. The technique was verified in 55 ASIC implementations with average inter- and intra-distance measures of 1.3 % and ~ 50 % respectively.

There exists another implementation based on the variation of the threshold voltages, but more along the line of cross coupled elementary combinatorial circuits. In [119, 120] a cross coupled pair of NOR gates forming a latch are used to achieve this effect. The variations in the threshold voltages of the two different NOR gates are dependent on the manufacturing process instabilities which brings about uncertainty in the

latch output. The background concept is to drive a latch into instability and wait for it to stabilize and settle into one of it's known stable states. The authors report a study of over 128 latches implemented on 19 ASICs using 0.13 μm technology with average inter- and intra- distance measures of $\sim$ 50 % and $\sim$ 3 % respectively.

The random output behaviour due to manufacturing variations can also be seen in flip-flops, since the underlying structures in an flip-flop are the latches. In [121], Maes et al. explore the possibility in a FPGA implementation with average inter- and intra-distance measures of 50 % and $<$ 5 %. In [122], van der Leest et al. extend the same concept to a larger implementation on ASICs and report average inter- and intra-distances of 36 % and 13 %.

3.3.14 Buskeeper PUFs

The PUF implementations with latches and flip-flops take in significant resources in terms of circuit area on a FPGA or an ASIC. Simons et al.[123] while exploring cheaper options, propose the buskeeper circuit as a possible PUF candidate. The buskeeper is a weak latch used to keep the bus lines from floating. If the bus lines have multiple drivers and if there is an idle state, the bus line tends to go into a floating state, where power consumption is higher. To avoid this, a weak pull-up latch is used to maintain the bus in its last driven state. Figure 3.14 shows the buskeeper cell and its most common usage in weak latches. The advantages

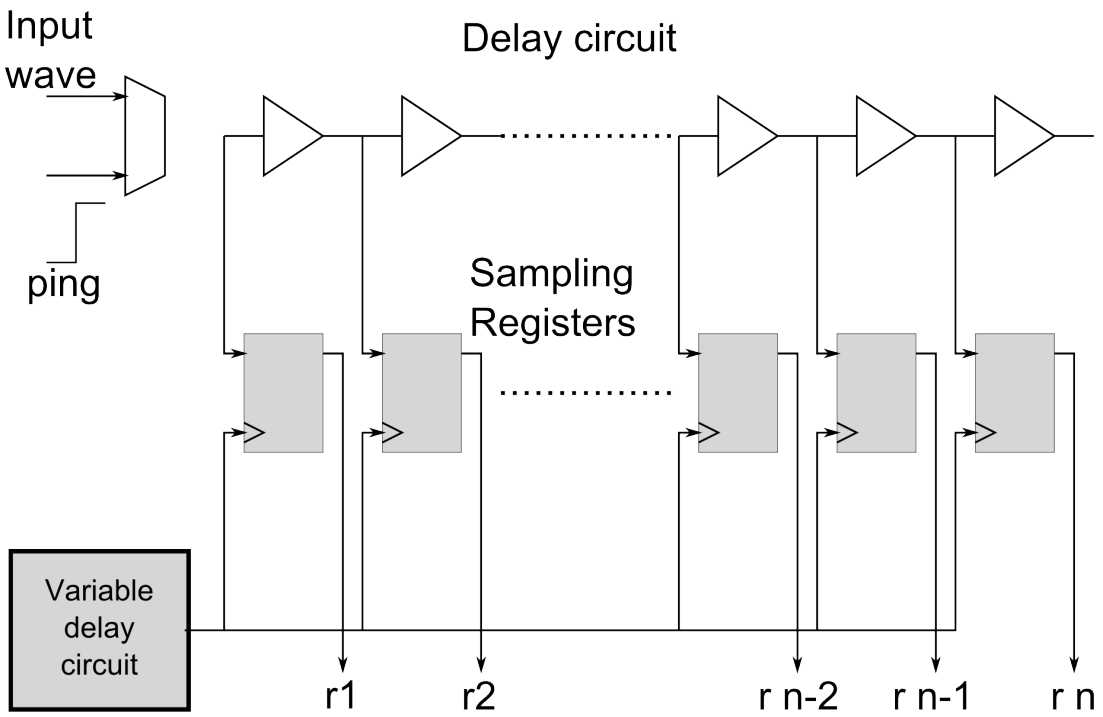


Figure 3.14: a) Buskeeper cell, b) Usage of the buskeeper cell in weak latches.

of the buskeeper over the latch or flip-flop implementation are the small circuit areas and reduced power consumption. The authors also note that placement of the buskeepers as well as latch based PUFs on a chip is less critical as compared to SRAMs, where they cannot be freely distributed across the circuit.

3.3.15 SHIC PUFs

SHIC is an acronym for *Super High Information Content* and in [124], the authors propose a new PUF implementation based on it. The idea is that a large storage of data combined with low read out speed will deter any attacker to model or attack the PUF response. The authors propose storage of data in the order of 10 Giga bits and a read out speed of 100 bits/s, which leads to a total read out time in the order of 3 years. In addition to this, if the data stored is random in nature, it becomes all the more difficult for the attacker. They propose to use a crossbar implementation based on diodes to generate this random data. In [125], the authors propose a distribution of diode array (individually addressable) which has a random variation in current-voltage characteristics. They propose to implement this using Aluminium-Induced Layer Exchange (ALILE) technology. The end implementation looks similar to the coating PUF, but with diode characteristics.

3.4 Other relevant approaches

In the last section, we have presented an exhaustive list of PUF implementations. However, we cannot claim that this effort is all inclusive. Our goal was to survey the PUF grounds with as much cover as possible so as to gain a perspective on where reflective PUFs stand in comparison to other solutions. With this, we would like to bring an end to this exercise, while making a fleeting mention of few other approaches that don't make the cut for generally accepted PUF definitions, but are close to it. The works of [11, 37, 126] provide a more elaborate listing and classification of PUFs.

Vrijaldenhoven in a master thesis [127] explores the possibility of using delay lines as acoustic noise signatures which may qualify as a PUF by some definitions. A group of researchers from Simon Fraser university have commercialized a technology where nano sized structures are used to create iridescence patterns to be used as security features. They call their platform **N.O.t.E.S** [3](Nano-Optic Technology for Enhanced Security). Ruhrmair et al. in [37] present another classification called Unique Objects (UNO), basically to account for biometric and other naturally occurring unique features which can be exploited in security applications. Their definitions can be easily extended to include the paper structure based tokens, print irregularity based tokens and even our concept of reflective PUF.

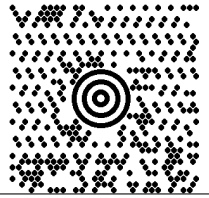
3.5 Summary

This chapter contains a fairly exhaustive (but incomplete) literature review of the state of the art solutions in product security. Starting with conventional techniques, which have mainly served logistical purposes but were further overloaded with security features in systems such as RFIDs and barcodes. The combination is very attractive for most common application scenarios and has served the manufacturing industry well over last few decades with reasonably good solution for both logistics handling and retail-shop level security. Optical methods for product security are very effective and attractive due to their visual appeal and ease of verification. PUFs are a relatively new field with less success in commercial terms as compared to conventional techniques. We take a look at various approaches, while observing the salient features in each of them. An objective comparison cannot be made since there is no level playing field and many of the

[3]Nanotech security - http://nanosecurity.ca/

implementations are endemic to certain application scenarios. Their study is nevertheless helpful in both devising usage strategy and building application level protocols relevant to anti-counterfeiting.

Table 3.2: Summary of 2D barcodes. The barcodes contain the encoded text : `Reflective PUF`

Name	PDF417	DataMatrix	QR Code	Aztec Code	MaxiCode	EZCode	Tag Barcode
Example image						Proprietary	Proprietary
Developed/ Invented by	Symbol technologies	International Data Matrix, Inc	Denso Wave a subsidiary of Denso Corporation	Welch Allyn Inc.	United Parcel Service	ETH Zurich	Microsoft
Capacity	about 2000 characters at maximum	up to 2335 alphanumeric characters	maximum 4000 alphanumeric characters	upto 3000 alpanumeric characters	about 93 characters	76 data bits	upto 3,500 characters per square inch
Standard	ISO/ IEC 15438	ISO/ IEC 16022	ISO/ IEC 18004:2006	ISO/IEC 24778:2008	ISO/IEC 16023	Proprietary	Discontinued

4 Concept and Realization

4.1 System overview

In this chapter, the motivation for the implementation of *reflective PUFs* is presented. An overview, on how we envisage the system to work as a anti-counterfeiting solution is presented. This implementation bears stark resemblance to the solution proposed by [9]. The advancement of technology, which enables cell phone cameras with sufficiently high resolution and ability to run programs to process the image captured, has opened up interesting scenarios. Then, there is the work of Pappu et al.[8], which also focussed on randomly distributed micro-spheres to generate a speckle pattern. A significant contribution of Pappu's work is related to simplicity and elegance of implementation, thereby reducing the cost factor. However, the state of the technology then, forced the read out equipment to be not so cost effective as the solution itself. Nevertheless, there have been (not very successful) efforts to bring this implementation to mainstream in the form of ATM card embedding [16]. In this scheme of operation, the high cost of reading equipment can be off-loaded onto a small number of verifiers (ATM providers) and the PUF solution itself will be cost-effective in relatively large numbers. The scheme has remained in proposal stage itself, since there has been no documented solution in the market today. Having gone through various implementations in the last years, it is evident that there are other factors affecting the adoption of the technology, in addition to the proof that technology itself is worthy.

These were the issues in mind, when a PUF technique based anti-counterfeiting solution was being formulated. The important criteria, that were considered are - the implementation must be technically *simple*, *elegant* (from the perspective of the user, can also be described as user-friendliness) , *cost-effective* and *harmonious* with the existing processes. At first these may seem more like aesthetic requirements than technical! Lets take a more descriptive view of the intended meaning of these terms here.

- **Simplicity -** We are of the opinion, that a PUF implementation is less effective if it hides behind the screen of complexity. One can call it the engineering equivalent of the *Kerckhoffs-principle*, which undervalues security by obscurity. The heart of PUF implementation is a physical process with some inherent randomness, which in most cases, people can easily relate to but not always analyse them to the last detail. This reduced notion should be sufficient for building the PUF implementation. One could construct a security principle based on many number of simple physical processes, running them in complex loops, feeding ones output to others input such a way that it is discouraging (both time and effort wise) for people trying to unravel it. In a gist, the complexity of the implementation should not be the core of security principle, because complexity is a relative term. It must be made clear that the argument against complexity, is not related to the algorithmic complexity which forms the core of modern cryptography.

- **Elegant -** Drawing reference to the sixth principle in Kerckhoffs desiderata section 1.1, any process or procedure that is cumbersome to use or its interaction is unwieldy, loses appeal and applicability

irrespective of its technological superiority. This aspect is well studied and practised in product design teams. For our purposes, as an anti-counterfeiting solution - it should be put forth as an easy interaction for people using it, provide clear and consistent results from evaluation (can be construed as robustness too).

- **Cost-effective -** This aspect need not be stressed upon. There are different categories of products with varying anti-counterfeiting solutions based on complexity and costs. The more *secure* ones, tend to be less cost effective in nature. Our target is day-to-day usage consumables which need sufficiently high degree of security but not necessarily infallible. Products like pharmaceuticals, food items and consumer electronics and other consumables with short shelf life can be grouped as our targets which do not have high individual value but significant market value in volume.

- **Harmonious -** This aspect cannot always provided with valid arguments. There have been technologies which have radically changed the ways people perceive and use them. However, in our view the global supply and distribution chain for products has enough complexities in itself and we do not aim to address any of them through our solution. The goal is to come up with an anti-counterfeiting solution that is in harmony with existing processes. Thus, the intended PUF based anti-counterfeiting solution will not bring about any drastic changes in current processes but will serve as a add-on module. This aspect is elaborated in next the sections.

4.1.1 Reflective PUF

The reflective PUF is the core of the anti-counterfeiting solution that we present. A mixture of reflective micro-structures in the size of $10\mu m$ to $100\mu m$ in transparent adhesive is applied on the product packaging or on the product surface directly followed by a protective lacquer layer. The application of the particles[1] on to the surface entails some physical processes, which results in particles being randomly distributed in *three dimensional* (3D) volume. The process of the applying this mixture onto the surface can be achieved in a different ways - the most simplest would be to utilize any of the digital printing mechanisms (ink-jet, laser etc.). The existence of inherent randomness in the printing process was explored by [128] and Zhu et al. used this to build signature and authentication of printed documents in [78]. There have also been works which use printed surface individualities alone and also in a combined configurations with print process variance to generate security schemes for printed material (covered in 3.1.3). Thus using the inherent randomness in the printing process, one can apply the mixture of transparent ink and reflective micro-structures. This is referred to as an instance of *reflective-PUF tag* (r-PUF tag)or simply *tag*[2] from here on.

It must be clarified here that the exact nature of the micro-structures and their manufacturing is the intellectual property of *Informium AG*. Also the specific process of applying the reflective micro-structures onto the surface to is a protected process of the same firm. The patents related to these two aspects are - [129, 130]. For the purposes of this thesis, it is sufficient to consider the micro-structures as being reflective in nature; in practice there exists small variations in terms for planar reflector and first order gratings which will elaborated in the next sections. This abstraction does not in any way hamper the analysis of the PUF application to anti-counterfeiting scenario. Similarly, the process of applying the micro-structures

[1] Micro-structures, micro-particles and particles will be used interchangeably but all refer to the reflective micro-structures used in realization of the r-PUF (reflective PUF).

[2] Any reference to 'tag' is intended to an instance of the r-PUF, in case the context demands reference to instances of other PUFs, then it shall be explicitly mentioned.

and the transparent ink can be abstracted to a digital printing process which has been proved to have inherent randomness, thus protecting the intellectual property of *Informium AG*. Having this aspect in the clear, the contribution of this author has been in using, this reflective PUF in the implementation of an anti-counterfeiting solution along with authentication protocols, conception and development of verification optics, rigorous analysis of effectiveness of the technique and unclonability analysis of the tag-generation using digital printing process.

The size of the particles in the tag are beyond the resolution of the naked eye and one requires a microscope objective to view them. When the tag is illuminated with incoherent light, the reflection pattern of the micro-structures can be observed and captured with the help of a microscope objective and a camera. The resulting reflection pattern is dependent on the angle of illumination and the angle of observation. Assuming that angles of observation is fixed to the normal of the surface containing the tag, the angle of illumination will have two degrees of freedom that can be varied. The figure below shows the set-up as explained here. Figure 4.1 shows the illumination degrees of freedom and angle of observation in a typical r-PUF readout set-up.

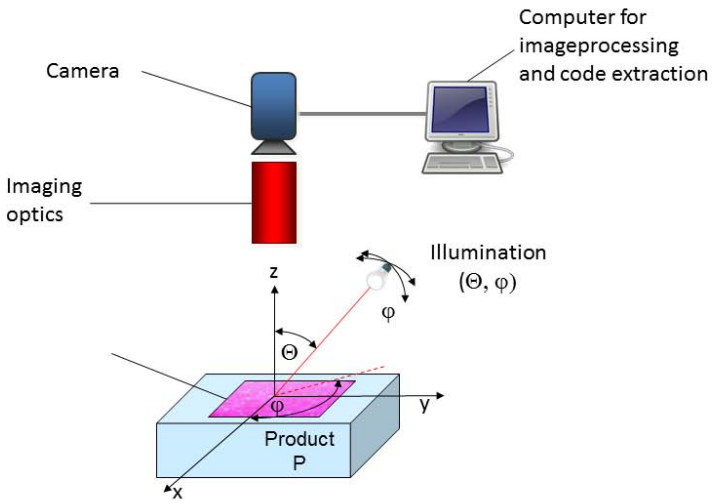


Figure 4.1: Schematic representation of the reflective PUF readout.

Given a fixed set of angles for illumination, the image of reflection pattern accounts for reflections from only those particles that have their reflections in the cone of observance. The random distribution of the micro-structures in 3D volume accounts for this relationship between illumination angle and the reflection pattern. Thus, every reflection pattern image is unique for a given set of illumination angles. There are some other considerations such as specular reflection from the lacquer layer and contrast from the background reflections. These factors are related to illumination intensity and corresponding variations are not unique to individual tag, but can be calibrated in a solution setting. In the next chapter, these factors are considered, while the illumination design is presented. Switching to PUF parlance, the set of illumination angles is the *challenge* and the corresponding image of the reflection pattern is the *response*.

4.1.2 Installation or Registration

Any manufacturer or product handler who wants to use this anti-counterfeiting solution will have to add this *r-PUF (reflective PUF) installation* module in the assembly line (usually at the end, in case of packaging), where they intend to attach the r-PUF to the product. The PUF installation module consists of printing equipment, which applies mixture of transparent ink and micro-structures onto the surface and then a lacquer layer is applied for protection. This is then imaged with a given set of illumination angles and the resulting image along with the product identification data (ID) is stored in a database. The response image cannot be used in its raw format and will have to undergo processing as explained before. The processing of the image shall extract usable unique code which can be associated with the *product ID*. This process is called *registration*.

The image of the reflection pattern by itself cannot be used as a secure key or a code for identification, since such a code would have to be a unique member of a set, corresponding to every item which incorporates the PUF. For the purposes of overall security, such a set must be uniformly distributed, which reduces the possibility of prediction. Depending on the service provider, the number of unique codes can run into very large number and thus the cardinality of set also grows, bringing about additional implementation issues. For now, only one outline of procedure for generating the unique code is considered. Other alternatives and a discussion on what qualifies as a best solution will be provided in next the chapter 5.3.

The image of the reflection pattern is first resized to a predetermined value and passed through a low pass filter to avoid aliasing in future steps. Two-dimensional (2D) Gabor transform is then applied with multiple frequency scales. Implementation-wise scaling is a form of sub-sampling carried out on the input image rather than the Gabor filters. The level of sub-sampling is decided in such a way that it results in a usable set of coefficients after the Gabor filtering. These coefficients can be used directly as a unique code [8] or can be put through further steps. There have been works [97], where *singular value decomposition* (SVD) is applied on the resulting coefficient matrix to compute a set of unique singular values or fed to hash function as an input. For now, it would suffice to proceed with any of the above methods as an example - say a predetermined level of sub-sampled input is used and passed through Gabor filters. The resulting Gabor coefficients are then fed to a hash function which outputs a uniformly distributed unique code. This is stored in a database along with other product identification data such as serial number, batch reference or any of the specific parameters from EPC standards.

The solution provider takes care of the appropriate interfaces required by the manufacturer to register the product and any maintenance of the registration thereafter. The schematic 4.2 captures the registration process.

4.1.3 Verification

Interfaces for the end user/verifier who intends to interact with the database to verify the product at hand, has to be made available by the solution provider. The verification is carried out with a camera equipped mobile phone with some add-on optics consisting of a magnification lens and an illumination module. Beekhof et at. in [22] point out that usually PUF related security schemes involve some form of special devices to stimulate and capture the response. Such requirements for extra equipments and devices usually bring in hesitation for users when it comes to adoption of a new technology. In our PUF based anti-counterfeiting solution we intend to use smart phone capable of running independent and dedicated applications for verification

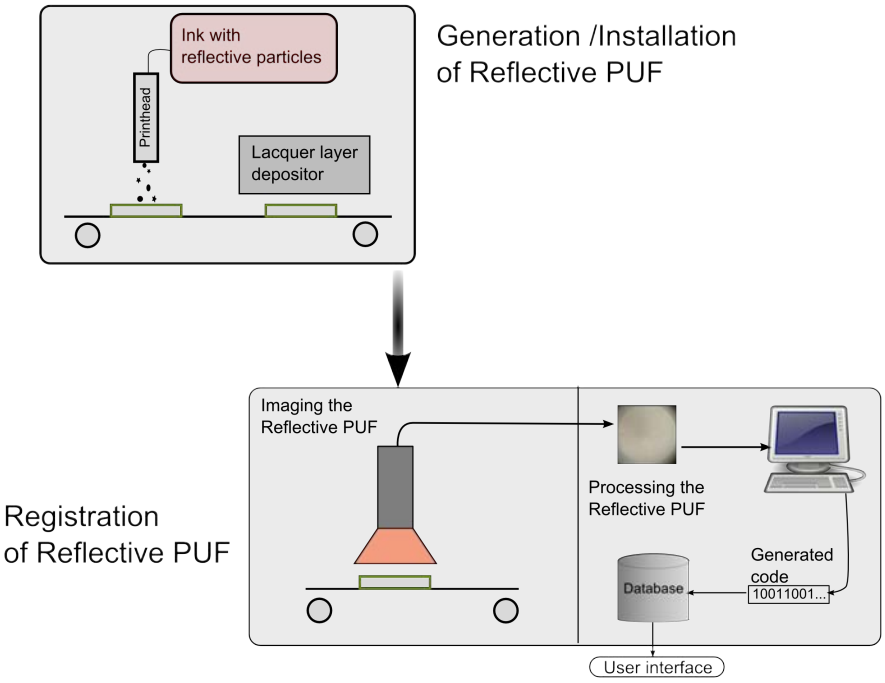


Figure 4.2: Registration of r-PUF

process; currently the system has a solution with Android™operating system. The possible protocols which can be used in verification could be -

- A secure session established with the server using `username/password`, which is then used for getting challenges from the server to be used for eliciting a response.
- A single fixed predetermined CRP in an authentication protocol, which uses a random nonce in every interaction.
- Device-specific public key cryptography using signed certificates at both server and client ends to secure the session, over which *challenges* and *responses* can be exchanged.

In any of the protocols, the steps starting from the registration stage - to generate a unique code from the reflection pattern image is repeated. The resulting code is checked against the one stored in the database at the time of registration. The PUF solution provider shall provide interfaces to the databases to complete this verification exercise. Irrespective of the protocol being used, there is one other detail which influences the computational load and security. The response can be either processed at the server end or at the client itself. In the former case the amount of data being exchanged will be significantly higher, assuming high speed data connection it may turn out to faster option since processing the image at server is easy as opposed to processing on mobile phone. Given that current mobile phones come with sufficiently powerful hardware with $< 1\,gigabyte$ of ram and multi core processors ($\sim$ 200 MFLOPS reported in media), the option of doing image processing at client side may seem sweeter in some circumstances. This has the added advantage of having very little data load on communication. We refer to these two possibilities as `Config 1 and Config 2` in this dissertation. The choice between the two configurations is a trade-off between amount of data transmissions and computational speed. Figure 4.3 show a schematic representation of the verification process.

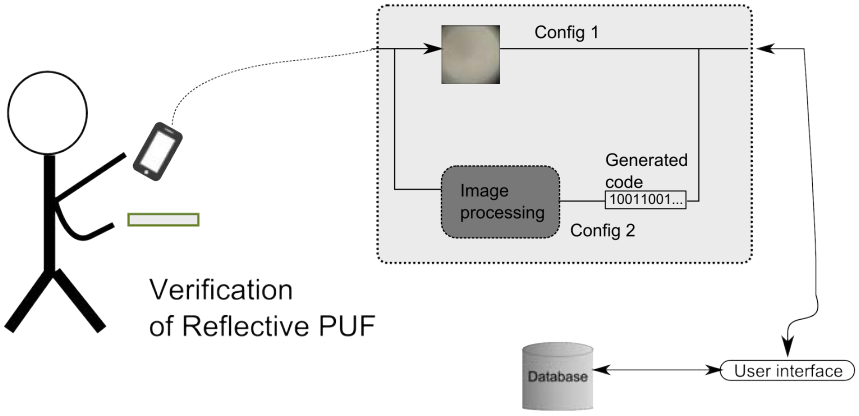


Figure 4.3: Verification of r-PUF

4.2 Realization of optical tags

In this section, we delve a bit deeper into the realization of the r-PUFs - structural and shape requirements for micro-particles in reflective PUF. The focus is more pn the motivation for the current manifestation and possible alternatives, while avoiding details, which breach the IP from *Informium AG*. We would like to explicitly credit the previous work in this area such as a [9, 7, 78] and others as a motivation for our approach. However, most of the effort in this dissertation is focussed on building a practical/ready to market anti-counterfeiting solution based on PUFs with experimental validation of unclonability. One can notice that most of the PUF implementations are fairly complex when it comes to user interaction, thereby rendering large scale adoption of the technology with difficulties. An exception to this observation can be made in case of some silicon-based PUFs which have an application layer built into the IC in form of both hardware and software.

Since the objective here is general purpose anti-counterfeiting, silicon-based PUFs can be ruled out; the most attractive solution thereafter are the optical PUFs. In their original implementation, PUFs are transmissive in nature. This imposes certain requirements on the PUF implementation and application in terms of material used. The transmission loss in the material plays a significant role. Use of visible range implies transparent PUFs, which may not always be possible. Else, Infra-Red(IR) or higher frequencies such as Ultra-Violet(UV) or X-Rays will have to used, which brings about the need for more specialised equipment, thereby driving the complexity of the system higher. Keeping these issues in mind, we decided to use reflection-based implementation. Furthermore, the requirement of coherent illumination implies a laser which brings about its own portability issues. Beekhof et al. in [22] also propose a reflective solution using partially coherent illumination from cheap and fast becoming ubiquitous laser diodes. The differentiating factor is that Beekof et al. and others use the inherent micro-structures on the surface, which in other words can be termed as substrate irregularities, whereas we intend to explicitly use additive micro-structures with multiple faces. This enables us to further lighten the constraints on the illumination and use simple LEDs instead for capturing reflections instead of coherence requirements for speckle effect. In the final configuration, incoherent light from LEDs are used to elicit the reflections from the micro-particles and the same is captured with a mobile phone camera using magnifying lens.

4.2.1 Requirements for micro-structures

An outline of requirements for the micro-structures is presented here and elaborated further in the next sections. They will be back referenced to this section whenever the choices seem arbitrary but are actually design/implementation constraints.

Optical characteristics - Since we have set out to implement PUF based on optical techniques, the micro-structures have to be sensitive to some form of optical stimulation. Reflection is our choice due to the simplicity in both stimulation and capturing the resultant effect. This translates to a requirement that the micro-structures must have at least one strongly reflecting surface. In the next section, we discuss the possibilities for stimulation in the visible range wavelengths and UV light.

Shape - This takes two connotations. Since the micro-structures are three dimensional objects, shape can refer to the geometrical shape or the shape of the polygon in 3D geometry. We postpone the discussion of the latter's reference to the next section. It is a straight forward need for the polygons with 3D geometry that are non-uniform across different particles. This enhances the entropy because of the difference in reflections from individual particles. However, this is a weak requirement since much of the entropy contribution is achieved by the 3D geometrical shape in combination with random orientation and distribution of the particles in a tag.

Size - There are two factors affecting the size of the particles. When looked at from the point of view of instantiation, the size of the particles must not pose any hindrance to the devices or the processes involved in realization of PUFs. On the other hand, once the PUF tag consisting of these micro-particles is in place, they will be stimulated with incident light and reflections will be captured by imaging the tag. The resolution of the image, sets the lower limit on the size of the micro-particles. There are two scenarios where imaging is carried out - first, during registration of the tag at the manufacturer's facility and again at the time of verification. In the registration system, the size of the optics is not an issue, however the working distance might be. It would be fair to consider that the verification stage which involves the use of mobile phone camera has a stronger bearing on resolution limitations. Most of the mobile cameras today have pixel sizes in the range $1.2\mu m$ to $1.8\mu m$. True imaging would mean 1 : 1 magnification which is not practical due to the lens complexity and reduced field of view (at $1.4\mu m$, the field of view would be $\sim 3mm \times 3mm$). Thus the imaging requirements are set lower at the start. The lens characteristics as shown in table 4.1 are used as guidelines. The motivation for the lens characteristics are - comfortable working distance which can accommodate illumination modules, sufficient depth of focus which enables capture of 2D projection of 3D structures and reasonable magnification of the particle reflections in the image. These aspects are discussed in more detail in the next chapter, section 5.2.1.

Cost efficiency - The requirements noted down so far can be easily fulfilled by using diamond dust in r-PUFs. They are reflective, come in variety of sizes, they have an established supply chain, know-how in handling it and are non-reactive chemically to be used in most of the inks. However, the choice reeks of asininity due to cost considerations. Thus, a cheap source of micro-structures which are inherently reflective or can be coated to achieve the same effect is needed. There are multitude of options in the form of metal coated micro-spheres, metal dust or coated polymer structures with diffractive structures ([131]). This aspect of the cost efficient particles for use in r-PUF will not be

elaborated in this dissertation for the reasons of scope but our partners in the project [132] assure us that they have developed a cost-effective process of manufacturing the particles to fulfil all other requirements.

4.2.2 Types of micro-structures

Visual markers

Having set the outline of requirements for reflective micro-structures, we explore different possible solutions for the geometry of the markers in this section.

- **Type 1 :** A direct extension of the optical PUF is to use reflective micro-spheres in a transparent ink, which is then applied onto a packaging surface to serve as a PUF. This solution is quite attractive due to easy availability of metal coated micro-spheres, which have sufficiently high reflectivity. The surface area responsible for reflection is a fraction of the total surface area of a sphere; considering that we are using micro-spheres, the reflection will be very weak. There are two aspects to this - one is the resolution, which is a direct consequence of the reduced surface area responsible for reflection and amount of light that is reflected. Using a higher intensity illumination, one could increase the amount of reflected light in general and overcome the resolution limit posed by surface normal reflection only. Consider a $100\mu m$ diameter micro-sphere used in a reflective PUF. Assuming a viewing distance of $25mm$ and resolution of $10\mu m$, one could theoretically image the entire face ($100\mu m$) of the sphere, if the contrast is sufficient. Thus, the limiting factor in effective utilization of reflections from micro-spheres, is good contrast. One can attribute contrast to the properties of underlying material such as reflectivity, scattering and colour, on which the reflective PUF is applied. Another drawback of reflections from micro-spheres is the folding of dimension or loss of orientation information. This translates as inability to differentiate between varying 3D orientations and a mere 2D positioning of the micro-spheres. In simple words, a sphere is a still sphere when viewed from any angle in a 3D volume since it has no face[3]. This results in identical reflection pattern from any viewing angle, given a constant relationship between angle of illumination and observance. Thus, one cannot derive any advantage from the random distribution of the sphere in a 3D volume, since it is equivalent to distribution in a 2D.

- **Type 2 :** The spherical nature reduces dimensionality from a 3D distribution to a 2D in the reflections and can be overcome by using multifaceted micro-structures with at least one face being highly reflective. Since there exists more than one face with differing shapes, a random distribution in 3D results in different faces of the micro-structure being responsible for reflections. Consider a micro-structure as shown in the figure with two reflective faces - both perpendicular to the object normal. Depending on the orientation of the micro-structure, one face or both of them are responsible for reflections. The angle of reflection is too now dependent on both the face normal and the angle of illumination. Figure 4.4a below captures the description in a schematic, where the dark blue surfaces are reflective and light blue surface are non-reflective.

  One can set a minimum requirement on the number of faces for the micro-structure. To avoid the dimension folding as in case of the sphere, any micro-structure with more than one face and at least

[3] In three-dimensional object geometry, a face usually describes a two-dimensional polygon bound by the edges of the object.

one of must be reflective in nature can be set as requirement. A simple manifestation of such a structure can be flakes which are very thin. Figure 4.4b has non-exhaustive list of different possible geometries in 3D. To summarize, the reflection pattern is dependent on

- Random position of the micro-structure.
- Random orientation of the micro-structure in three dimensional geometry.
- The angle(s) of the illumination - both the angle of the inclination (θ) and angle of rotation (ϕ).

Any random distribution of these micro-structures in a 3D volume will be hard to clone by manual placement in such a way that all micro-structures are having identical orientation and the resulting reflection patterns are faithfully replicated. The *hard* aspect in cloning such a PUF tag can be attributed to dependency of response to both the micro-structure itself and the illumination specification. The unclonability analysis considering different system parameters involving digital printing process will be covered in chapter 6.

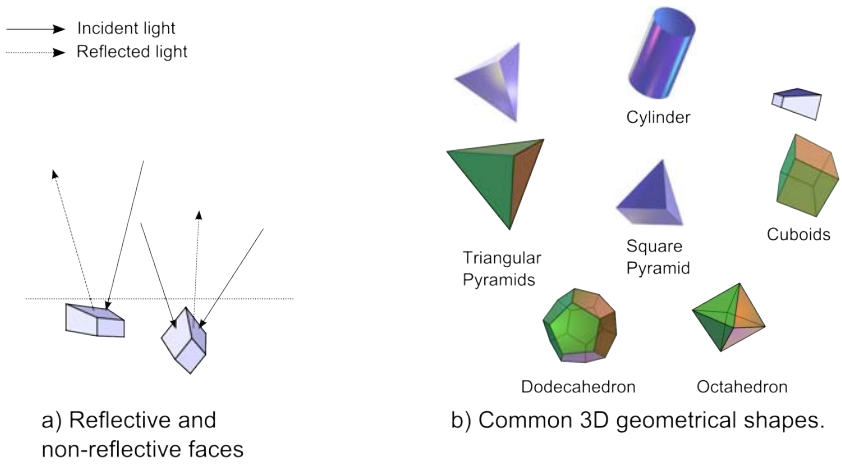


Figure 4.4: Different possible three dimensional geometries of micro-structures

Fluorescence markers

One could forego the requirement of a multifaceted 3D geometry by using particles, which are stimulated only by non-visible light, thus making a direct copy virtually impossible. Chong et al. in [42] use phosphorous micro-particles stimulated by UV light. A random distribution of these particles is then imaged under UV illumination and used to extract an unique code. This technique has only one *CRP* which is wavelength dependent, and the reflection pattern does not depend on the geometry and orientation of the micro-structure, but only on the random positions. One could imagine a scenario where such a reflection pattern can be printed off normal printer to substitute the actual PUF tag with micro-structures in them. This argument discounts the effect of wavelength dependency, which is not very substantive, but the effort is directed at pointing out that one independent *CRP* is the weak link in this implementation (irrespective of how many *CRPs* are actually used in an application scenario).

4.2.3 Instantiation methods

The behavior of the PUF is not only influenced by the choice of the markers, but also the mechanism by which they are brought together to form a PUF tag. In our implementation, we use multifaceted visual markers due the advantages as mentioned in previous section. However, this choice does not impact the analysis of the print process by which a tag is instantiated. In this section, the basis on which the instantiation of reflective PUFs is elaborated. We reiterate here that the specific process of instantiation used in commercialization of this technology is an IP of our partner firm Informium AG. Nevertheless, we base our arguments on the established digital printing process, which can be used alternatively, without the loss of generality.

Oliver et al. in [133] show that the analysis of pre-determined shapes or text printed from different printers can reveal the printer technology used. They provide results where ink-jet printers can be differentiated from the laser printers based on a statistical analysis of print quality. Zhu et al. in [78] use a laser printer and print out pre-determined shapes to create sample set of documents. They extract feature vectors in terms of averaged radii in different segments on the circumference of dot, which is then used as a unique code or a print signature to identify the specific sample. In [77], the authors present a PCA based analysis of printed characters to achieve both printer and document level identification. They use only laser printers, but have included both solid ink and dry toner technology based printers in their analysis. The most interesting aspect from their work is the influence of the toner level as a variable on the final outcome. According to the authors, the influence of the toner level as a variable, is restricted to loss of information related to document level security but printer identification remains valid. Mikkilineni et al. in [128] use the banding artefacts in the laser print process as an intrinsic feature of the printer to tie the documents to the printer which printed them. The authors also propose methods to embed extrinsic information in the text or material that is being printed, which could be later used for authenticating the document itself. In an another publication [134], the same group provides comprehensive review of the causes, means and ways to profile both printed documents and printers themselves encompassing the entire range of ink-jet and laser printing technology. This establishes the basis for using the digital printing process as a method for instantiating the r-PUF.

The core requirement of the instantiation process of reflective PUF is distribution of the micro-structures in a three dimensional volume. This can be achieved by adding the micro-structures to a transparent ink, which is then applied onto the required surface. Ink-jet printers are ideal for this purpose since one can mix micro-structures in a variety of inks and as long as the size of the nozzle is larger that the micro-structures, the ink flow is not hampered. The resulting print shall have all the characteristics arising out of the inherent randomness or errors of the digital printing process. Three principal components of the ink-jet printer technology are the printhead, the carriage and the paper-advance mechanism. The printing in the two dimensional space is carried out by moving the paper in one direction (usually referred to as process direction) and scanning in the perpendicular direction by the printhead with the help of a carriage return(referred to as scan direction). Printheads are usually equipped with multiple set of nozzles for different colours or types of ink which are connected to respective reservoir/container of ink. The nozzles on the printhead are usually set in a pattern; for example, a single column of seven or a set of two staggered columns with four and three nozzles respectively. A given pattern will be printed differently based on the nozzle configuration on the print head. Figure 4.5 shows the basic architecture of an ink-jet printer along with the two main scan directions. Drops of ink are fired on the paper by a set of nozzles in the printhead. By controlling the firing in a given column of the nozzles, several rows of pixels can be printed simultaneously in one pass

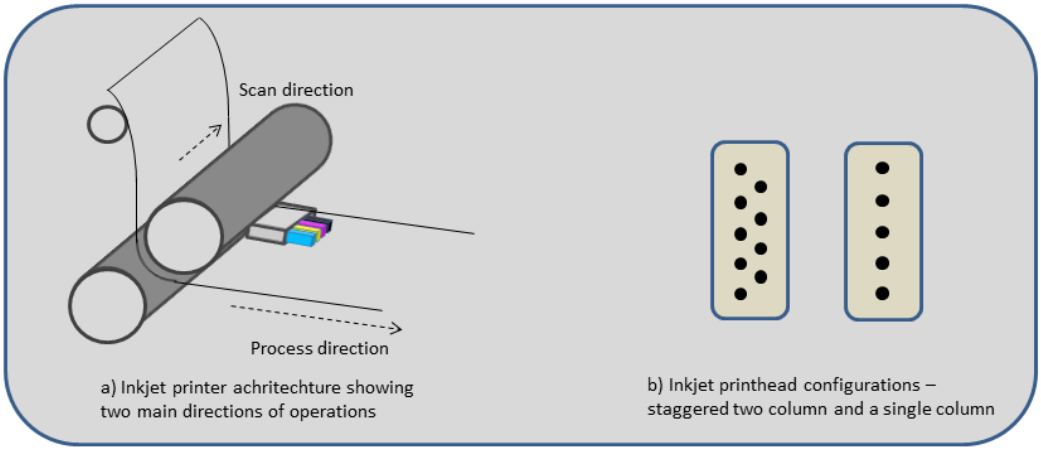


Figure 4.5: Basic architecture of the ink-jet printer and nozzle configurations

of the printhead in scan direction. After completion of one pass, the paper is moved in process direction and followed by printhead scanning in perpendicular direction. This is repeated until the entire document is printed.

The critical considerations of ink-jet printers are the way the firing is done and the type of ink that a technology can handle. Ink-jet printers are classified broadly as continuous ink-jet (CIJ) and drop-on-demand (DOD) printers. There exists further sub-classification in the DOD type printers. A brief overview of the classification and the underlying principles is excerpted from Handbook of print media[135].

- **Continuous ink-jet :** As the name suggests, it is a continuous stream of ink droplets generated by a high pressure pump and passed through a nozzle. A piezoelectric crystal is used to create pressure waves, which break the continuous stream into individual droplets. These droplets are charged by a charging electrode before they pass through an electrostatic field, which deflects the drops either onto the printing substrate or into a collection sink, which is then recycled into the reservoir. The electrostatic field can be controlled to position the droplets on the printing surface. The advantages of this technology are - high velocity of the printing that can be achieved and the use of volatile solvents along with ink which enables printing on variety of substrates. CIJ has low resolution when compared many other techniques due to which it is mainly used in marking applications, where resolution requirements are lower. CIJ is also not energy efficient due to the continuous generation of the droplets irrespective of the information content that is being printed.

- **Drop-on-demand :** Droplets are generated and ejected on demand as opposed to continuous generation based on the information content that is being printed. In general the drops are formed using pressure pulse in the printhead, which can be achieved by either thermal processes or piezoelectric effect. There have also been developments in technology where droplets are generated by electrostatic means.

  Thermal DOD - Rapidly heated resistive element in a small chamber in the print head containing the ink creates drops. The heated resistive element causes a thin film of ink above the heater to vaporise into a rapidly expanding bubble. This creates a pressure pulse that forces a drop of ink through the nozzle. The advantages of this method is that very small drop sizes can be achieved, which results in high resolution printing. The range of inks that can be used with this

technology is limited, since the inks have to withstand the cyclic heating. It also requires the ink to be composed of materials, which are easily vaporized.

Piezoelectric DOD - The mechanical distortion in the piezocrystal on application of electric field, is used to create a pressure wave in the ink chamber, resulting in release of a drop through the nozzle. Piezoelectric DOD is an isothermal process which allows the use of wide range of inks. The relative high cost of the technology is the only limiting factor.

Electrostatic DOD - Droplets are formed using a complex interaction of surface tension difference between ink and nozzle using a controlled electrostatic field. This technology is relatively new in development and still maturing, which translates into higher costs and complexities in operation.

Chiang et al. in [134] identify user controlled options in the form of print resolution, speed, directionality, number of printing passes, which introduce artefacts and affects the quality of print. Further, there are few system inconsistencies in the form of carriage positioning errors resulting from gear backlash, paper-advance errors and spur marks. The printhead by itself is the source for variety of artefacts due to dot placement errors and varying drop geometry. The misaligned nozzles in the printhead are one of the main causes of dot placement errors. According to [134], minute variations in the structural characteristics of the print head cause the nozzles to fire differently resulting in characteristic patterns in printed content. Further more, the fluid dynamics of the ink-jet nozzle, ink properties and missed jets can be treated as causes for intrinsic randomness in the resulting print pattern which can be exploited for generating secure print signatures. Pollard et al. present a very similar approach of generating the signatures from printed documents, using inherent randomness in digital printing followed by feature extraction by 2D Gabor demodulation in [136]. Once again, the noticeable difference to the proposed solution, is the use of additive micro-structures which are affected by the irregularities in print process.

For the purposed solution, since the PUF is instantiated on a product/packaging surface, one can do away with the paper advance mechanism, as the underlying conveyor belt on the assembly line serves the same purpose. On the assembly line, it is efficient to print without going through passes, since only spatially-restricted content is of interest. These can be achieved with more nozzles on the printhead. In case there is a need for printing along an extended space, then it would serve better if the process is restricted to a single pass of the printhead. In brief, only a set of nozzles is sufficient and the carriage return can also be done away with. Thus the set-up is reduced to a conveyor belt for moving the products and an overhead ink-jet printhead followed by lacquer lamination module. We choose the REA JET™printhead with seven nozzles for generating the samples used in this dissertation. Minimum nozzle size is $80\mu m$, but can be extended up to $500\mu m$ and the print height is $3mm$ to $27mm$. This augurs well with our requirements since we have micro-structures in the range of $10\mu m$ to $50\mu m$ and tag area is $5mm \times 5mm$ in size.

Having done away with the paper-advance mechanism and the carriage based scan, the options are limited to exploiting the irregularities arising from the use of printhead, density of the particles and print control options such as speed, print pattern and dot size resolution.

4.3 Characteristics of Reflective PUF

The crux of the implementation of r-PUF and its use in anti-counterfeiting scenario is based on two dimensional projection of three dimensional object geometry using the reflections. In the 2D projection image,

one can treat every pixel as a switch with `ON-OFF` behaviour. `ON` when reflected light is present and `OFF` when no reflections can be recorded. The representation of the image pixels as matrix of switches allows for abstraction of underlying object geometry and its dependence on illumination specifications. In its simplest form, the contents of the matrix (*response*) itself serves as the unique code which can be tied to illumination specification (*challenge*). However, as mentioned before, one has to make allowance for noise in read-outs from the underlying physical interaction - both from manifestation point of view and due to the measurement procedure. The measurement procedure involves fairly standard image capture devices along with controlled illumination, where one can determine the noise factors forehand. This leaves us the uncertainty or noise considerations arising from the manifestation process. In the following sections, we shall present an analysis of the interaction of the individual micro-structure with illumination and constraints of the measurement system, while capturing this interaction.

Before we delve into further details, a definition of framework for considering object geometry is presented. A generic scheme which can be applicable to both registration and verification scenarios is elaborated here. Below is the description and an accompanying schematic 4.6 of the various components of this framework.

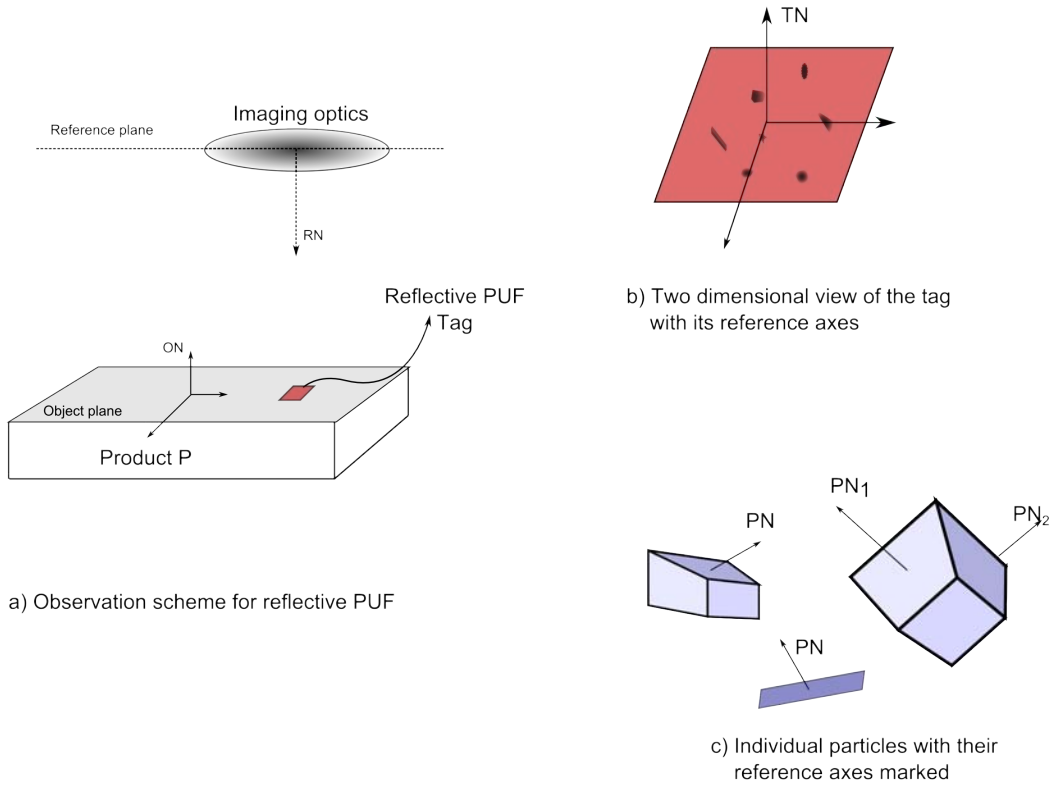


Figure 4.6: r-PUF tag geometry - frame of reference

Reference Plane The observation plane is defined as a system wide reference. In the proposed scheme of things, imaging micro-particles always requires some form of magnification which is achieved using a lens. The normal to the reference plane (*RP*) is designated as *RN* and everything else in the system is positioned and referenced with respect to this plane and its normal (*RN*). Consider the lens to be lying in the reference plane, thus justifying the equivalence of observation and reference planes. The

optical axis of the lens coincides with the normal to the reference plane, and will be discounted from future analysis unless there is an explicit need for the lens to be shifted out of its position.

Object Any product on which the r-PUF tag is applied, is referred to as an object in this section. The object can be either a product or its packaging, but what is important for this analysis is the plane/surface on which the tag is present. This plane is referred to as object plane (*OP*) and the normal to this surface as the object normal (*ON*[4]). Since object is being imaged, it makes easier for analysis for the reference plan and the object plane to be co-axial (although in figure 4.6a it is not depicted as such).

Tag An instance of the r-PUF that is applied onto the object. The normal to the outwards surface of the tag is denoted as tag normal (TN) . In most cases when only one tag is present on the object, the *ON* and TN are coincident and either of the can be used in analysis without the loss of information. In case the object has more than one tag on its surface the explicit reference will have to be made to *ON* and TN for individual tags and the displacement from the *ON*.

Particle Every tag is composed of a multitude of micro-particles of varying geometry. These particles can have more than one active surface - responsible for reflections. Consider a hemisphere, where the planar surface is the active surface or a cuboid, which has six active surfaces. Each of the surfaces can have a normal defined and is designated as particle normal (*PN*), followed by a subscript denoting the relevant surface. The orientation of the particle can then be described using the *PN* in relation to the TN or *ON*. This in addition with the position of the particle in the tag can be used to analyse the contribution of the particle to the *CR* behaviour of the tag as a whole.

Illumination Let us assume that the source of illumination can be abstracted to a point, denoted by *IPS* - illumination point source. This point in turn can be referenced in the scheme above, using the distance (r) from the origin of the tag, angle of inclination (Θ) from the *ON* and the rotational angle (Φ). The exact nature of the illumination is not much of importance here and requirement for the same will be considered in the next chapter while dealing with illumination design. For now, we assume that it is some form of incoherent or partially coherent illumination.

Lens The position of the lens and the optical axis are already stated above. That leaves out the characteristics of the lens from the imaging perspective. The working distance or the distance between the reference plane and the object plane is the most important parameter in deciding the resolution and the numerical aperture(NA) of the lens. For the purposes of analysis, relevant parameters are listed in the table 4.1. The reasoning for these will be covered in the next chapter, whilst dealing with system requirements and design.

Lens diameter	$16mm$
Working distance	$25mm$
optical resolution	$10\mu m$
Field of View	$10mm \times 10mm$

Table 4.1: Characteristics of imaging lens - derived from requirements

[4]The object normal *ON* must not be confused with the state of a switch `ON`, the variation in the font is aimed to maintain the difference. Also explicit references are made when the context demands.

4.3.1 Particle characteristics

In this section, the analysis of interaction between the illumination and the individual particle is considered in isolation. For the sake of simplicity, lets consider that the micro-structure under consideration is a cuboid with its $thickness(T) \ll \{length(L) or breadth(B)\}$, with one of the faces being reflective in nature. This surface will be referred to as the active surface. In the elementary configuration, the particle lies in the centre of the tag plane facing outwards, such that the *PN*, defined with respect to this surface, and the *TN* or *ON* are coincident. The reflections captured from this particle is dependent not only on the illumination parameters, but also on the lens characteristics (as described in table 4.1). Let us make a further assumption that the size of the particle in question, is equal to the resolution of the lens. Thus the reflection from this particle influences one pixel in the captured image. In case the particles are smaller, the reflections cannot be captured to due resolution limit of the lens and in the case when particles are larger in size, more than one pixel is influenced by the reflections from the particle. This assumption is a more inclusive case, where every pixel is accounted by an individual particle. Figure 4.6b and 4.6c show the schematic representation of the reference framework used here.

Considering the particle surface to be planar in nature, one can arrive at the relation between incident illumination and reflection using *Snell's Law*, where both the incident angle(θ_i) and reflection angle (θ_r) are defined with respect to *ON*.

$$n_1 sin(\theta_i) = n_2 sin(\theta_r) \tag{4.1}$$

With the above assumptions, when the *PN* is coincident with *TN*, the rotational angle (Φ) of the illumination source(*IPS*) can be discounted and only the vertical inclination(Θ) can be considered for the analysis. The reflections from the particle can be captured only if they are in the cone of acceptance (equivalent to numerical aperture). The cone of acceptance for the given lens parameters is about 35.48° as shown in the figure. Figure 4.7 shows the cone of acceptance for various illumination conditions.

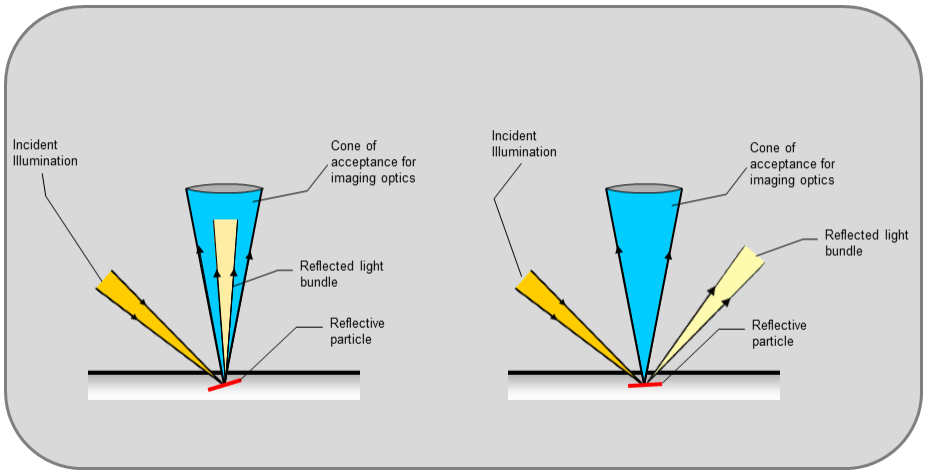


Figure 4.7: Cone of acceptance for planar reflector micro-structures

Since the arrangement is symmetric about the co-axial normals when seen on a two dimensional schematic as above, we can reduce the analysis to $0° to 90°$. The edge of the lens subtends an angle of 17.74° from the *ON* to the object center. In our experiments, for small angles of inclination (up to $\simeq 10°$) of the *IPS*, the specular reflection from the protective lacquer layer was so strong that the particle reflection could not be differentiated. In this case, it's a given that the object surface(background of the tag) offers sufficient

contrast to detect reflection from the particles in the tag. Thus, for successful imaging of the reflections, the angle of inclination of the *IPS* has to be in the range 10° and $\sim$ 18°. Currently, the lens diameter is 16*mm* and by increasing it to 25*mm*, one can increase the useful range of angle on inclination from 10° to 24°. This leaves a lot of unused illumination angles, which can be interpreted as reduction of the *CRP* space. Below figure 4.8 shows the useful range of the illumination variable Θ for planar reflectors.

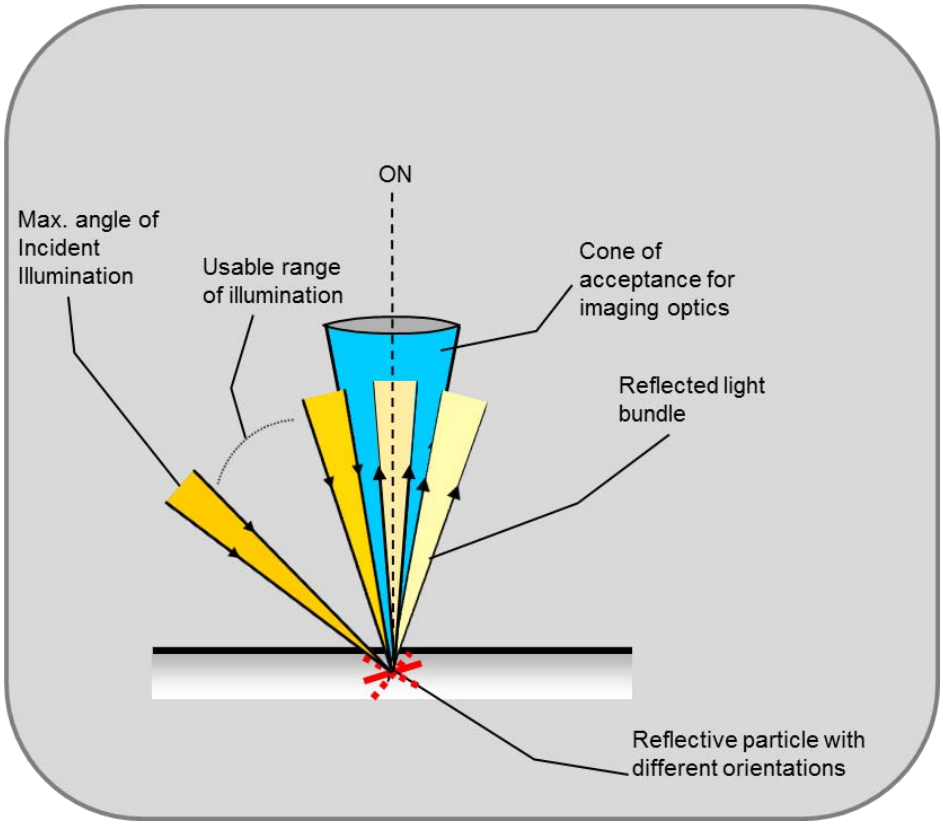


Figure 4.8: Usable range of Θ for planar micro-structures

Further more, having *IPS* within the angle subtended by the lens will interfere with the imaging, especially at the edge of the fields - where the cone of acceptance (NA) is smaller than at the center of the tag. This forms a major constraint of planar reflectors. In the following analysis, the different orientations of the particle have been omitted for simplicity. In any orientation, the relation between the angles of incidence and reflection remain the same, and thus the size of useful range is also constant. With change in the orientation, this useful range gets shifted by an amount equal to the difference between *PN* and *OB*, when it is still located at the center of the tag. In the case when the particle is not at the center of the tag, the displacement of the particle origin from the tag center also needs to be taken into account, in addition to the angle difference between *PN* and *ON*, while computing the shift of the useful range of the incidence angles.

To overcome the constraint posed by planar reflectors, diffraction gratings were explored. The planar reflector with particles which have either ruled grating or blazed grating on the active surface. Continuing the simplistic analysis, this particle, which has only one reflective principle surface is positioned at the center of the tag with the grating normal (*GN*), coincident with the *ON*. The size of the particle is so large as to influence just one pixel in the captured image. The choice of either the ruled grating or the blazed grating does not bear much significance in the proposed case, since a polychromatic source is used and reflection in all wavelengths in the visible range are of interest.

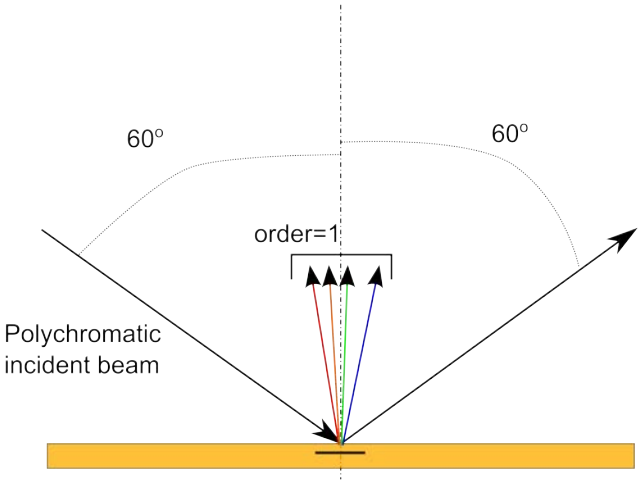


Figure 4.9: Usable range of Θ for illumination settings

The figure 4.9 shows the increased range of the Θ for diffractive micro-structures. The relation between the incidence angle and the reflection (actually diffraction!) angle is given by the grating equation, where both the incident angle θ_i and reflection angle θ_r are defined with respect to the ON. The order of diffraction is denoted by m , the wavelength by λ and the line/groove spacing by d.

$$m\lambda = d(sin\theta_i \quad + \quad sin\theta_r) \tag{4.2}$$

Let us consider an indicative example, where the active surface on the particle consists of 1500 lines per millimetre (lpmm). This is a high density grating and not necessarily the design, which is used in our system, but is only for explorative purposes. We are interested in the entire range of visible wavelengths thus, our illumination in this example will be a polychromatic white light source. If the angle of incidence is 60°, the entire visible wavelength range is diffracted in the first order between $-10°$ and $10°$. In the case of planar reflectors, the rotational angle of the illumination (Φ) and the orientation of the particle in the object plane can be omitted without loss of any information. Extending the assumptions to diffractive gratings mean that plane of illumination is perpendicular to the grating lines, which allows us to use the grating equation 4.2 directly. However, we would have to consider the other angles as well, since both the illumination angle Φ and the orientation of the grating in the object plane will influence the resultant diffraction. The modified equation which can be used take in to account the Φ and orientation uses ε, the angle between the incident light path and the plane perpendicular to the grating lines at the tag center. The modified grating equation is as below -

$$m\lambda = d\,cos\,\varepsilon(sin\theta_i + sin\theta_r) \tag{4.3}$$

Microscopic images of the diffractive micro-structures are shown in figure 4.10. It can be observed that not all of them are in focus, which is due to the distribution of the particles in the tag at different depths. In the analysis so far, a simple case of cuboid with one active surface was considered, since in terms of realization one can approximate it to a very thin flake with one side reflective. In reality the 3D geometry of an object can have many more active surfaces, and this only increases the entropy in terms of individual pixels in the image being affected by the reflection from these particles. We also made an assumption about the size of particles corresponding to the state of only one pixel. If the sizes are bigger and the surface is non-uniform

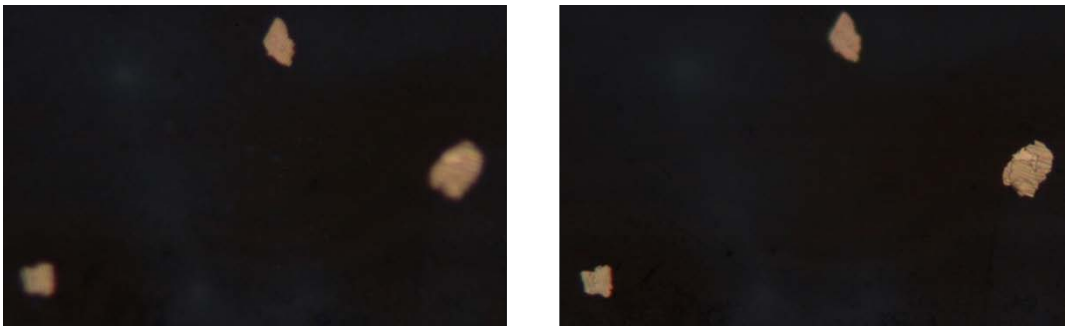


Figure 4.10: Microscope images of the diffractive micro-structures

shape, then the orientation of the surface in the object plane also bears influence on which pixels and how many of them are influenced. The rigorous computation of the contribution from different orientations for both planar and diffractive surface are presented in chapter 7, while computing entropy.

4.3.2 Tag characteristics

With the understanding of the interaction between incident light and reflection due to individual particles, we can now proceed to the tag instance, where many such particles are present. The analysis so far was carried out in isolation on an individual particle, while analysis in this section focusses on the interaction of the incident light and its image, which captures the combined effect of individual particles in a given instance of the tag. This tag is a manifestation of the different random processes that are involved in applying these micro-particles on a background surface (which can be a product or its packaging). The combined effect of the particles is a result of the random distribution of the individual particles in three dimensions. The field of view of the verification lens sets the constraint on the size of the r-PUF tag in two dimensions. The thickness is kept as small as possible (in the range $\sim 100\mu m$) , so that the tag does not stand out from the surface, but can be perceived to be embedded into it. In the analysis so far, the field of view of the lens is about $10mm \times 10mm$, and the tag size should be smaller or equal to this value. If the size is equal to the field of view, the sensitivity to translational errors during measurement will be high. By keeping the tag size smaller ($\sim 5mm \times 5mm$), one can relax the positioning requirements during image capture and ensure that the tag stays in the field of view of the lens.

For the purposes of this analysis, size of tag is set to $5mm \times 5mm$. This, in combination with the lens resolution of $10\mu m$ means that the reflection pattern will be a 500×500 image. As mentioned before, the image can be treated as a matrix of 500×500 switches, and the state of these switches can be used to generate a security code. This state of the matrix is deemed to be unique and corresponds to a gives set of illumination specifications and the instance of the tag. The next logical step would be to analyse factors, which affect the number of particles and their distribution in a given instance of the tag. We continue using the digital printing scheme to account for the application of the micro-particles on the product/packaging surface as opposed to process developed by our partners *Informium AG*. The factors that influence the print process variances in an ink-jet printing process were covered in previous section 4.2.3. However, not all user controlled variables are applicable in our implementation. The important factors for analysing the tag properties can be split into two categories.

- Number of particles in a given tag and their indirect influence on the security code (reflection pattern is directly influenced).

- Influence of printer process variables on the random distribution of the particles and subsequently their influence on final security code.

The selection of the variables in the print process which are exposed to user control and their influence the above mentioned factors in analysis of the tag properties are listed below.

- **Density -** This is a measure of the proportion(volume wise) of the particles that is mixed with the transparent ink used for printing. This has a direct impact on the number of particles that will be present on the tag.
- **Dot size -** The size of dot influences both the amount of ink that is ejected from the nozzle and its spread on the tag surface. Thus, both the number of particles in the tag and the distribution are affected by the dot size parameter.
- **Print pattern -** The goal of printing is only random deposition of particles. However, in the absence of actual data to be printed, we have to supply the print head with some known pattern that can be used for printing. The choice of this pattern will influence how close the dots are printed and how much ink is used for generation of one tag. Thus, this parameter also influences both the number of particles and the spatial distribution of the particles in the tag.
- **Speed of printing -** The speed of printing has a direct effect on the movement of the tag surface, which is used for printing and thereby influencing the spread of the dots on it. The shape of the ink drops that are released from the nozzles are also influenced by the speed of the printing. Thus, both these factors can be understood have a bearing distribution of the particles.
- **Viscocity -** The viscosity of the transparent base ink in which the particles are mixed, affects the flow of the ink through the nozzles and its spread on the tag surface. Variation of this parameter can influence the spatial distribution of the particles on the tag.

These user control options in combination with inherent randomness in digital printing process is at the heart of the proposed PUF manifestation. We propose some experiments to determine whether any bias exists for these variables in the final outcome. In an ideal case, there is no bias discernible and the outputs are truly random and unclonable. In case any bias is noticeable for any of the variables either individually or in combination, then care has to be taken to nullify this effect by keeping them constant across all instantiations. The results of the experiments related to this are provided in chapter 6.

Illumination angle sensitivity

Realization of the tags forms one half of the story, evaluating their relationship with illumination specification is the next step. As mentioned before, there are two variables related to illumination at our disposal - the angle of inclination (Θ) and the rotational angle (Φ). One could consider the wavelength of the incident light as a parameter too, but LEDs are used for practical convenience, wavelength is not regarded as a variable. It would be of interest to know the sensitivity of these two variables on the resulting reflection pattern. To this end, we take a set of reflective PUFs instantiated using the above described methods and evaluate them under varying illumination conditions. The normalized correlation give a good impression of the sensitivity of the illumination parameters. At the outset, this may seem as a reduction of the $Challenge - Response$ space, but this factor can be alleviated by judicious choice of authentication protocol fitting to our application scenario.

4.4 Formalization of Reflective PUF

The optical PUF [7, 8] implementation in 2002 spurred the growth of the PUF field and since then, a host of different implementations have been reported. The use of these PUFs in a variety of settings ranging from traditional cryptographic protocols to specialized applications is being explored. It is generally well understood what a PUF stands for, but there is no agreement on a formal definition in this field. Some prefer using the traditional cryptographic settings while other have come up with more characteristic definitions. In the chapter 2 under sections 2.2.1 and 2.2.2 provide an exhaustive review of existing definitions and formalizations. Almost every approach has some or the other advantages and disadvantages, and it is clear that standalone definitions do not help in evaluating competing implementations. Therefore, a definition framework is needed, which

- sets minimum requirements to include as many PUF implementations as possible
- inculcates the essence of the physical unclonability in a modular way, where they can be compared with other manifestations
- includes provisions for capturing the interaction of the PUF with the application protocol
- incorporates representation for factors affecting the instantiation and operation of the PUF.

In our opinion, there are three relevant works which fit the bill - the framework of Armknecht et al. [15], PUFs in UC [28] and work[27] by Plaga and Koob. Putting PUFs in the context of UC goes a long way in bringing PUFs into mainstream cryptographic solutions space, but since this dissertation deals with a very specific application scenario of anti-counterfeiting, we shall not be exploring reflective PUFs in UC context. The definition of Plaga and Koob place reduced emphasis on physical unclonability, while focussing on overall security. This approach is motivated by the 'ends justify the means' philosophy, since the unclonability is exploited in some or the other security protocol. Finally, it is the notion of security that the PUF brings to the table that matters rather than the underlying principle. In our opinion, the physical unclonability is what sets apart this field of work from the rest and any definition or framework serving this field should include this aspect unambiguously. Therefore, we adapt the framework from Armknecht et al. [15] to define and formalize the implementation of reflective PUFs.

The authors use this framework to espouse the properties of the PUF such as robustness, unclonability and unpredictability. We however, restrict the usage of the framework to the definition of the r-PUF and use it to bring about the notion of unclonability. Other properties - robustness and unpredictability included, can be clearly defined independent of the framework. The definitions of unclonability, which encapsulates the uniqueness aspect, together with unpredictability, robustness and application protocol that wraps the PUF in itself, all contribute to the notion of security of the PUF. This approach loosely binds different properties of the PUF to the overall security as opposed to clear and precise condition as seen in classical cryptography. It has been observed that any direct approach to define security involves use of probabilistic polynomial time limits on processes/resources or the concept of negligible probability in one or more variables involved in PUF operation. As sound as the argument may be, we restrict ourselves to proving security in the isolation of application scenario rather than making a general case.

4.4.1 Overview of the framework

A brief overview of the framework is presented before the adaptation, and for an in-depth description we refer to [15]. The framework(figure 2.5) consists of five constituents involving both components and procedures that will cover all aspects from instantiation, registration up to the evaluation of the PUF.

Creation process The instantiation of the physical component p is achieved by incorporating some random physical process or irregularities represented by `CREATE`. Only the manufacturer has access to this process and all controllable parameters involved are represented by α_{CR}.

Physical Function A PUF instance is represented as a *physical component* p, which can be stimulated with a challenge $\tilde{x}$ to elicit a response $\tilde{y}$; there exists a module(`EVAL`) to carry out this interaction with the physical component. This evaluation module `EVAL` together with the PUF instance p is called the *Physical Function* (PF). `EVAL` receives the user input x, which is usually a digital representation of challenge and translates it into $\tilde{x}$. It stimulates p with $\tilde{x}$ and captures the resulting response $\tilde{y}$. The received response is again translated into digital representation y and returns it to the user. Any external factors affecting this interaction can be defined with the help of α_{PF}, the evaluation parameter. The separation of the `EVAL` procedure and the PUF instance p, allows one to model settings where more than one `EVAL` procedures exist for a given type of PUF with varying results.

Extraction module Due to the underlying physical processes, the responses of the PUF have a noticeable noise quotient. When stimulated with the same challenge $\tilde{x}$ multiple times, the responses may be different. This can be addressed with an extraction module `EXTRACT`, which eliminates or reduces the noise in the output y, such that slightly varying responses to the same challenge can be mapped to a unique output z. All external factors or settings involved in this process are represented by α_{EX}. `EXTRACT` module can contain one or more algorithms to realize this one-to-one mapping between challenge and unique response. Armknecht et al. in [15] also make room for different mode of operations for this module - *registration* and *verification*. The authors propose to utilize the concept of fuzzy extractors[137] in this context and go on to define the helper data h' and h to be used during *registration* and *verification* modes respectively[5]. The helper data in our scheme can be visualized as the logical data from application scenario which can be bound to the unique output of the PUF.

Physical Function System The combination of the physical function PF and the `EXTRACT` module is represented as the *Physical Function System*(PFS). This abstracts the implementation details to the user, who only sees the challenge x and the unique output z.

Physical Function Infrastructure This is a further abstraction constituting all the components and processes described above. Within a *Physical Function Infrastructure*(PFI), the creation, evaluation and extraction parameters are maintained as constants. Thus, one can define an entire PUF implementation by PFI.

[5] Although we are not using the fuzzy extractor in our scheme of working, we include it in different places for the sake of completeness in adaptation of the framework. Later on, we find use for it in representation of logical identity that is bound to the PUF

Notation

Let A be a probabilistic procedure, then $y \leftarrow A(x)$ denotes an event where the procedure A outputs y on input x. Since A is a probabilistic procedure, there can be more than one output for a given input x. Such a set of all possible outputs is represented by $[A(x)]$. An empty set is denoted by ϵ.

4.4.2 Definition of r-PUF (reflective PUF)

The concept of the r-PUF was covered in section 4.1.1, here we provide concise definitions of various components in the framework of Armknecht et al.[15], when adapted to r-PUFs. Adapted framework for r-PUF is shown in figure 4.11.

Creation process

The digital printing process has some inherent random irregularities[78], which are unique for a given instance of print. The creation process `CREATE` involves mixing reflective micro-structures with the ink and printing them on designated surface areas. The inherent random variations manifest themselves by randomly distributing and causing non-uniform orientations of the micro-structures in 3D space on the tag. This is followed by application of a protective lacquer layer. Thus produced r-PUF, is denoted by p (physical component). The user controllable settings for this process such as - density of the particles in the ink, dot size, speed of printing and print pattern are represented the process parameter α_{CR}.

Physical Function A *physical function PF* is a probabilistic procedure, which captures the *challenge-response* behaviour of the r-PUF. The physical component p and the `EVAL` procedure are the constituents of PF and their interaction can be represented as

$$y \leftarrow PF_{p,\alpha_{PF}}(x) = \mathtt{Eval}_p(\alpha_{PF}, x) \tag{4.4}$$

Let $\mathbb{X}$ be a set of all challenges in the form of various illumination angles, α_{PF} is a set of parameters which help in system implementation and $\mathbb{Y}$ is a set of all reflection patterns for a given instance of r-PUF. At one higher level of abstraction, the PF can be described without any reference to its constituents as

$$PF_{p,\alpha_{PF}} : \mathbb{X} \rightarrow \mathbb{Y} \tag{4.5}$$

The `EVAL` process is implemented in a micro-controller which interacts with the mobile phone (in the case of verification) or a computer (during registration phase) to receive the challenge x, it translates it into control signals $\tilde{x}$ for the LED illumination module. The resulting reflection pattern is imaged by digital camera through a magnification lens. In our implementation, the factors affecting the imaging of the reflection patterns such as the intensity of the LED, distance to the tag, number of pixels in the image and the magnification of the lens, all form the part of the evaluation parameter α_{PF}.

Physical Function System A *physical function system* (PFS)is a probabilistic procedure defined as

$$PFS_{p,\alpha_{PF},\alpha_{EX}} : \mathbb{X} \times (\mathbb{H} \cup \{\epsilon\}) \rightarrow \mathbb{Z} \times \mathbb{H} \tag{4.6}$$

where, $\mathbb{X}$ is a set of all challenges, α_{EX} reflects the set of parameters of the PF, ϵ represents null set, $\mathbb{H}$ is a set of helper data values and $\mathbb{Z}$ is the set of all outputs for a given instance of r-PUF p. As mentioned before,

the PFS is a logical combination of the PF and the EXTRACT process. Thus, PFS can also be elaborated as

$$(z, h') \leftarrow PFS_{p,\alpha_{PF},\alpha_{EX}}(x, h)$$
$$\texttt{Extract}_{\alpha_{EX}}(PF_{p,\alpha_{PF}}(x), h) \tag{4.7}$$

When the EXTRACT is executed in the registration mode, the $h = \epsilon$, and new helper data is generated for a given challenge x. If $h \neq \epsilon$, then EXTRACT is executed in verification mode, where z is computed with the help of helper data h. It must be noted here that $h = h'$, where the notation h' is the helper data that is returned by EXTRACT. The authors in [15] use the difference in notation for the sake of consistency, which we are faithfully replicating here. The images of the reflection pattern y vary slightly on multiple measurements for the same challenge x. The measurement noise is related to positioning of the tag, angular accuracy of the illumination and quantization of the image sensors. The active physical process irregularity is not much of an issue in r-PUF as opposed to silicon based PUF. Nevertheless, this is undesirable and using an EXTRACT process, we can remove the noise component to arrive at an unique output z.

In our implementation, we are using 2D Gabor demodulation or Gabor hashing, where the image of reflection pattern is sub-sampled and passed through Gabor filters to arrive at a set of coefficients which form the basis for unique code z. The EXTRACT procedure implements this part. The level of sub-sampling, Gabor filter coefficients and any quantization threshold used will be represented by the extraction parameter α_{EX}.

Physical Function Infrastructure The ensemble of all the components defined so far forms the *physical function infrastructure PFI*. Within a given PFI, the processes CREATE, EVAL and EXTRACT and the related parameters α_{CR}, α_{PF} and α_{EX} are fixed. It is denoted by

$$\mathsf{PFI}_{\alpha_{CR}} = (\texttt{CREATE}, \{PFS_{p,\alpha_{PF},\alpha_{EX}} : p \leftarrow \texttt{CREATE}(\alpha_{CR})\}) \tag{4.8}$$

As seen from the figure 4.11, the framework can be split into two parts - *registration* and *verification*. While most of the adaptations do this for the sake of clarity, it becomes essential in our adaptation since the constituent modules are different. The *registration* is more or less consistent with original framework, but in the *verification* framework, we break up the logical binding of *physical function PF*. As explained before, the verification is done using a mobile phone camera with some add-ons in the form of imaging optics and illumination. This hand-held device serves as a common verification device for many instances of r-PUFs. The parameters α_{PF} and α_{EX} can be programmed into the mobile phone application. This makes it possible to handle reflective PUFs that are not be from the same *PFI* too.

In chapter 3, section 2.2.3 a review of the different properties that are desirable in any PUF implementation was presented. We now elaborate on their application to the implementation of reflective PUFs. The framework from [15] has been used in defining unclonability, robustness and unpredictability by implementation using the formalization [15, 95]. We however, restrict its use to unclonability only and instead use simple formulations consistent in literature for other properties. The number of *CRPs* for a given instance of r-PUF is finite (but large, in the order of $\sim 180 \times 90$). Thus theoretically one could capture all the *CRPs* and build a mathematical clone of the instance. This we shall not try to circumvent this, since it is not in the scope of the work. The PUF implementation was done with anti-counterfeiting and product security in mind, and focussing on physical unclonability is sufficient in this context.

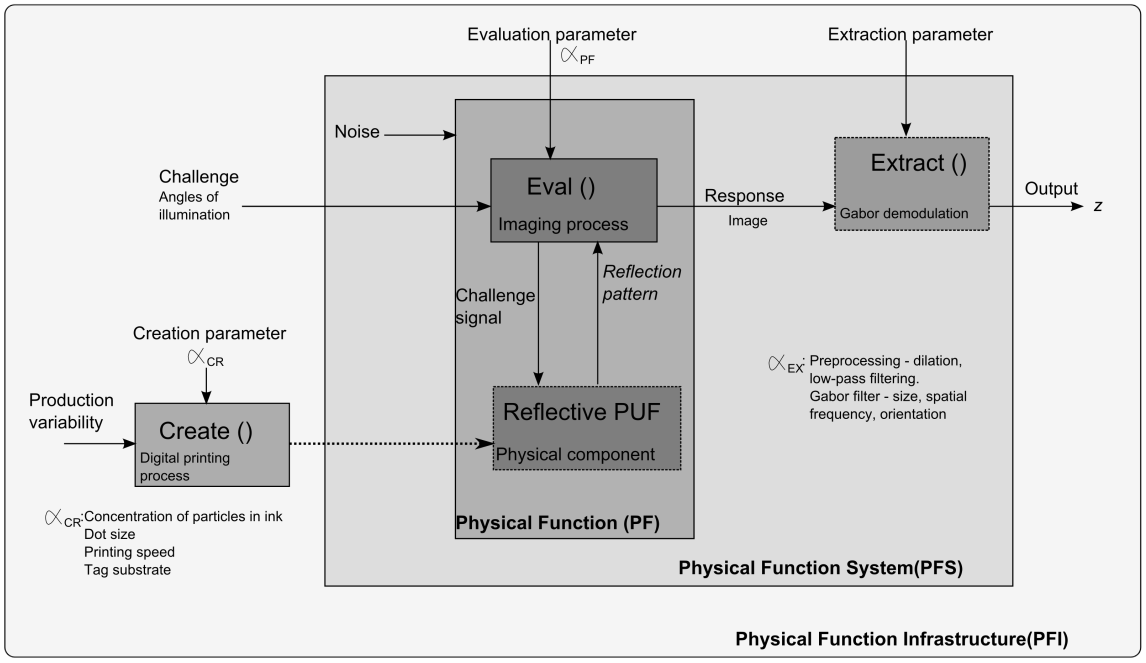


Figure 4.11: Adapted framework for formalization of r-PUFs

Physical Unclonability

Most of the works in PUF domain define unclonability with negligible probability or processes that cannot be completed in polynomial time. By using the above framework, one can arrive at a more practical bound what constitutes as unclonable in a given PUF implementation. It must be noted here, that mathematical cloning is excluded by definition. The authors in [15] explicitly target *physical unclonability* by the following statement -

> *A PFS' is a physical clone of another PFS if both PF systems show identical CR behaviour and deploy the same* `EXTRACT` *algorithm.*

In the proposed solution, physical cloning is restricted to the instance p, since other components may be common, as seen from the verification framework. The inclusion of CR behaviour in the definition of *physical unclonability* opens up the possibility to verify claims. We have already mentioned that, a given PUF instance p, when stimulated with challenge x multiple times the response y varies slightly each time due to the inherent randomness present in the PUF. The maximum variance of such responses for a given PUF instance is a measure of the robustness denoted by ρ_{PFS}. We have described this as the $intra-distance$ in previous chapters. This has to be taken into consideration, while designing the `EXTRACT` module. However, for the purposes of unclonability, this robustness measure serves as an upper bound on how identical any two instances of PUF can be. Armknecht et al. in [15] further break down the physical unclonability into

Selective cloning refers to the case, where for a given r-PUF instance p and PFS another p' can be constructed where $PFS \equiv PFS'$.

Existential cloning refers to the generic case, where the manufacturer can produce two reflective PUFs p and p' such that $PFS \equiv PFS'$.

We put forth proposition that the concept of existential cloning is all encompassing in nature and covers the selective cloning scenarios as well. If we can prove that existential cloning is not possible under certain conditions, then one cannot achieve selective cloning too within the same bounds. A physical clone of a reflective PUF is be defined by [15] as

Definition 4.1 (Physical clone)**.** Let evaluation parameter α_{PF} and extraction parameters α_{EX}, be fixed in two PF systems such that they are identical except for $p \neq p'$. This can be written as $PFS = PFS_{p,\alpha_{PF},\alpha_{EX}}$ and $PFS' = PFS_{p',\alpha_{PF},\alpha_{EX}}$. The PFS' is defined as a δ clone of PFS w.r.t $\mathbb{X}' \subseteq \mathbb{X}$ if for all $x \in \mathbb{X}'$, if

$$Pr[(z,h) \leftarrow PFS'(x,h) : (z,h) \leftarrow PFS(x,\epsilon)] \geq \delta \cdot \rho_{PFS} \tag{4.9}$$

Using this definition, we can construct the definition for *existential cloning*. As defined before the physical instance p implicitly extends its self to the definition of $PFS = PFS_{p,\alpha_{PF},\alpha_{EX}}$, where α_{PF} andα_{EX} are fixed. Let $\mathbb{A}_{CR}$ be the set of all possible creation process parameters α_{CR}. We allow the adversary counterfeiter to choose any $\alpha_{CR} \in \mathbb{A}_{CR}$ for producing a physical clone of p and run the `CREATE` process a finite number q times(this bound is necessary to rule out infinite trials scenario). We define a family of PUF instantiations or the *physical function infrastructurePFI* to be (γ, δ, q) resistant to existential cloning w.r.t $\mathbb{X}' \subseteq \mathbb{X}$, if

$$\begin{aligned} Pr[PFS'_{p',\alpha_{PF},\alpha_{EX}} \overset{\delta,\mathbb{X}'}{\equiv} PFS_{p,\alpha_{PF},\alpha_{EX}} : \\ (p,p') \leftarrow \texttt{CREATE}^{run\,by}_{counterfeiter}(q, \alpha_{CR}, \alpha'_{CR} \in \mathbb{A}_{CR})] \leq \gamma \end{aligned} \tag{4.10}$$

This definition covers both scenarios, where an honest manufacturer creates a clone by coincidence and the case, where a manufacturer creates a clone with deliberate malicious intent. The limit γ for the *existential cloning* will also serve as a upper bound for *selective cloning* scenario and hence will not be analysed separately. The quantization of γ for a given set of creation parameters α_{CR} will be represented by distance measures of final outcome (chapter 6).

4.5 Anti-Counterfeiting with Reflective PUFs

In section 4.1, while dealing with system overview, the utilization reflective PUF was outlined. Also, a review of different approaches was included in section 2.4.1. In this section, the analysis, reasoning and choice of the protocols are elaborated.

Reflective PUFs are extrinsic by nature, where the readout/ measurement mechanisms are not integrated within the actual PUF instance. In our system, a common platform or device is used in verification mode, which has the capability to verify PUF tags from any of the PFI families of the r-PUF. Thus, one needs to add the user-access and the operation of this device to the notion of system security. The r-PUF tag is meant to be attached to a product or embedded on product surface/packaging. During registration of the PUF, there has to be a logical binding of the identity of the specific product to the unique code of the PUF tag. This identity of the product can be a serial number, product ID or anything which helps in identification of the product. This product identity information can be stored as auxiliary information along with the unique code from PUF. Since product handling and supply-chain management systems are very mature, there exists an effective way to search through a database of products using their identification details. Associating the unique code from the PUF to this product detail entry is a more harmonious solution, where searching through database during verification can be done faster. This removes the burden of identification from

PUFs while focussing only on anti-counterfeiting (verification) aspect. Since, there exists more than one *CRP* for a given reflective PUF tag, it is assumed that the during registration process many *CRPs* (if not all) are recorded and stored. These aspects of registration can be assumed to be common across schemes for anti-counterfeiting.

Anybody who wants to check the product for its authenticity has to run the verification process on the PUF tag that is attached to the product. It must be noted here that during a verification procedure involving PUFs, it is only the PUF tag that gets verified or authenticated and not the actual product or entity. It is assumed that the PUF and its physical association with the product/entity is a given thing. In case of anti-counterfeiting using r-PUFs, one can visualize the actors involved as

Product/entity (TAG) This is the actual instance of the product that is to be verified. It usually has an instance of r-PUF tag attached or embedded, which can be used for verification.

Trusted Authority (TA) This is an application on a server, which houses the database of the registered PUFs along with their product details. It provides an interface, through which anybody can place a query requesting for the verification of a PUF tag.

Verifier (vDEVICE)This is verification device[6] which interacts with the PUF and checks with the TA about the authenticity of the PUF. With reference to the above framework, it includes the EVAL and EXTRACT processes.

The basic verification protocol for anti-counterfeiting has been included while reporting almost all implementations of PUFs. The verifier vDEVICE queries the trusted authority TA for challenges relevant to the given product or entity. The TA randomly selects one *CRP* and communicated the corresponding challenge x to the vDEVICE. The verifier stimulates the TAG with the challenge x, records the response, computes the unique code z and conveys the same to the TA. The TA checks the received unique code with the stored value, if they are identical then the product is verified as authentic. The TA communicates the finding from the comparison to the verifier. To increase the security, the process can be repeated with more than one *CRP*.

The drawbacks of this basic approach and various efforts to overcome it were reviewed in section 2.4.1 and the three most promising methods were listed in section 4.1.3. The mutual authentication protocols are ruled out due to the fact that the EVAL and EXTRACT are in one module here (vDEVICE) and can be used to verify PUF instances from more than one PFI. We focus only on authenticating/verifying of the PUF tags and review two efforts which have been implemented for anti-counterfeiting using r-PUFs.

4.5.1 Verification using public key cryptography

This is a device specific solution, where two pairs of public-private keys, one each for the verifier vDEVICE and TA are used. The public-private key pair(TA_{pk}, TA_{sk})[7] generated for the trusted authority TA and can be used by all verifiers in all transactions. Every verifier vDEVICE will have its own public-private key pair(V^i_{pk}, V^i_{sk}). All verification devices will have the public key TA_{pk} of the trusted authority stored in them, so that they can initiate communication. The public key of the vDEVICE can either be registered with the TA or can be sent at the beginning of the exchange.

[6] Verifier could also be a reference to the user who is operating the verification device. In the course our analysis, this distinction will be highlighted if necessary.

[7] the subscript *pk* stand for public key and *sk* for private key

When a verifier wants to verify a given PUF, it sends the product ID(any other auxiliary data) and an identifier for the vDEVICE(since there can be many verifiers) or its own public key(V^i_{pk}) encrypted by TA_{pk}. The trusted authority on receiving the message, decrypts it using its own private key, selects a random *CRP* for the given product and sends the challenge x encrypted using V^i_{pk}. The verifier decrypts challenge using the V^i_{sk} and stimulate the PUF tag with x. The resulting unique code z is again encrypted using TA_{pk} and sent to the trusted authority for verification. The TA compares the received unique code with the stored *CRP* and communicates the status of verification to vDEVICE. This exchange is captured in the schematic below 4.12. In the actual implementation, a pre-signed certificate for the public key of the verifier was stored on the vDEVICE(a mobile phone) and the public key of the verifier was not actually made public but sent during first exchange under encryption. This rules out the need for authentication of both TA and vDEVICE.

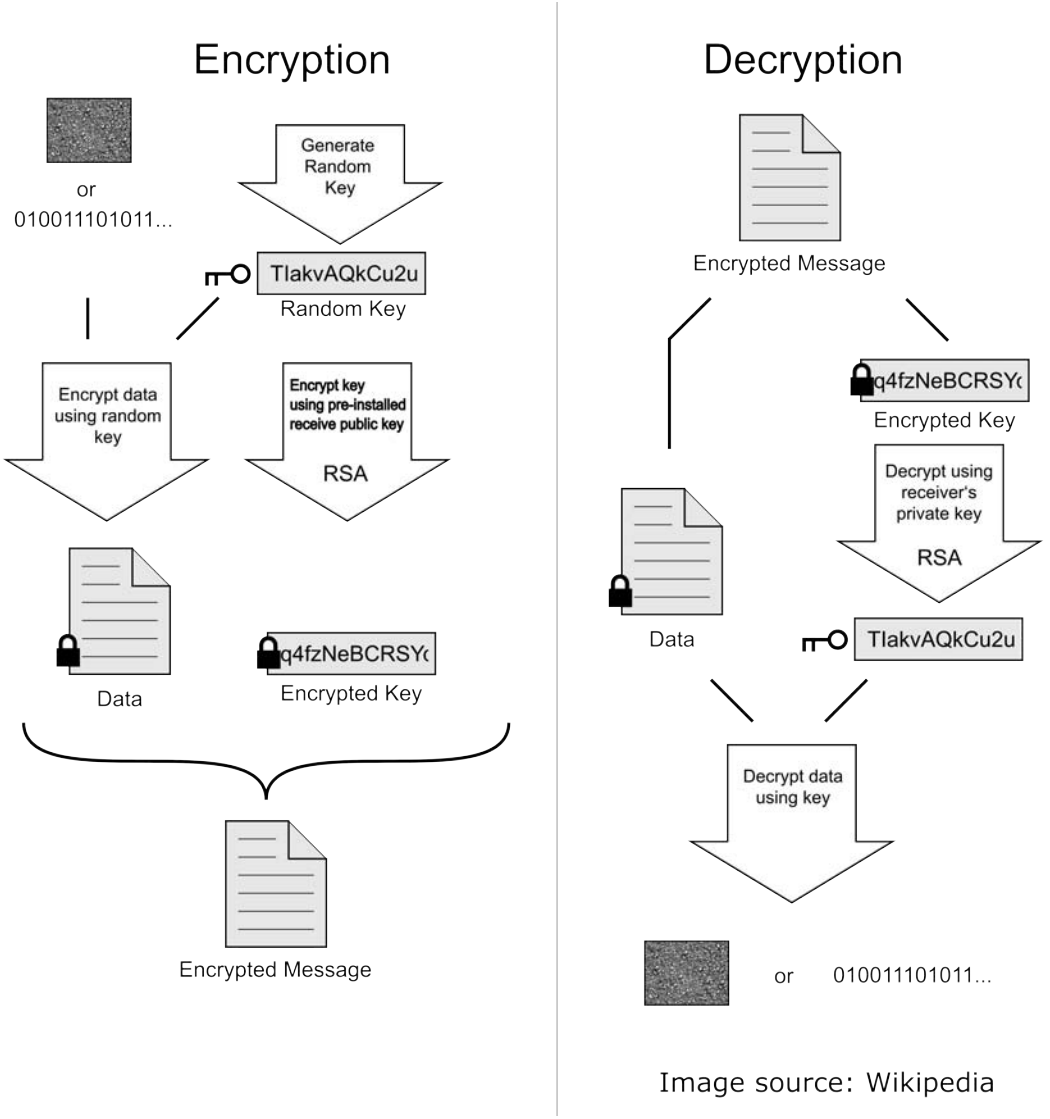


Figure 4.12: Schematic showing the transaction of the public key cryptography based verification

4.5.2 Username/Password based verification

There exists possibility that vDEVICE itself can be misused. To verify the actual person who is operating the vDEVICE, we implemented a conventional username/password based verification protocol using standard

HTTPS protocol. All users must be registered with the TA with a username/password. The access to the vDEVICE application is controlled by login. On successful login, a secure session is established on which challenges and responses are exchanged. After verification is completed, the session ends and the user is logged out. In actual implementation, the entire transaction was done using Secure Sockets Layer(SSL) to avoid the leak of username/password information. It must be observed here that in both the methods described above, there is no restriction on the number of *CRPs* that can be used. It has been pointed out that repetition of *CRP* leads to replay attacks and hence, the need for large set of *CRPs*. In both our implementations the challenges and responses are sent across under encryption, thus only one *CRP* may be sufficient for any number of verifications.

4.6 Summary

In this chapter, we have presented the concept of r-PUF, its realization, analysis of characteristics along with a system overview on how it can be used in an anti-counterfeiting solution. We omit the pegging of r-PUFs into one of the definitions presented in chapter 2 on purpose. Instead we use the formalization framework from [15] as a base for explaining the workings for r-PUF.

Notable omission has been the discussion on security provided by r-PUF. In most of definitions related to PUF, the security is quantified using PPT algorithm and its runtime or by effort required to break codes measured in bits (usually in 2^k, denoting *k-level* security). Comparison in either forms is not suitable for r-PUFs, not withstanding the underlying hardware technology dependence for either of them. Most common example is the comparable security provided by 1024-bit RSA (76-bit security) and 160-bit elliptic curve cryptography (86-bit security) due the difference in algorithms involved [138]. Lenstra et al. in [139] propose a common basis for comparing the security in cryptography based on energy. We however, choose to bypass the security quantification and instead choose to rely on unclonability which is satisfactory in the context of anti-counterfeiting. The equivalent bit-level security in cryptography hash algorithms are reported in chapter 6 for the sake of completeness.

5 System Design

Having covered the concept of r-PUF and its realization, the aspects involving its system design will be presented in this chapter. This will be split into three major portions - the instantiation/registration system, verification device and the algorithms used in extraction of unique code. The instantiation of the r-PUF was covered to a large extent in the previous chapter and any other remaining aspects will be dealt with here. For each of the sections, requirements are outlined first, followed by current state-of-the-art that can be used or tailored to our needs and in the end, the details of the designs that were implemented along with their analyses. Most of the work in this chapter has been guided by the severe constraint, that it must be practically feasible technology which can be rolled out as a valid anti-counterfeiting solution. In a lot of ways this work has drawn on previous existing research in this domain of PUFs and we aim to overcome the last mile barriers while keeping the underlying scientific principles intact.

We envisage the anti-counterfeiting solution to be built on the foundation of r-PUFs. The registration system and the verification device form the two pillars of the solution, while the code extraction/ hashing module as a common roof resting on pillars (but may be split or replicated at both ends implementation-wise). Anti-counterfeiting using r-PUF can be described by the figure 5.1 with reflective PUF as the foundation, registration and verification as pillars and hashing as common roof. The section dealing with registration will be less detailed, since it was not the focus of work for this dissertation. Nevertheless, the system will be presented along with requirements matching but no in-depth analysis of the system design itself is included. The verification device is basically a mobile phone running a custom application along with some add-on optics and illumination module. This, along with the extraction algorithms and the unclonability analysis form a core of the work done for this dissertation and all efforts will be done to faithfully capture their design and development.

5.1 Registration system

Once the PUFs are instantiated, they need to be attached to a given product (if they are not already embedded in the product/packaging), followed by extraction of the unique code and storing it in a data base along with relevant product identity information. This system will be installed at the product manufacturer's site or at the PUF solution provider, who in turn arranges for the PUF tags to be integrated with the products. For the purposes of clarity, lets assume that the PUF instantiation and registration module will be placed on the product assembly line at the manufacturer's facility. Since, the PUF tagging needs to be done on either the surface or packaging of the finished product, the position of the registration systems is usually near the end of the assembly line. Figure 4.2 shows the scheme of operation.

5.1.1 Requirements

One of the main design goals is to make the r-PUF solution as harmonious as possible with the existing product manufacturing and logistical set-ups (section 4.1). The registration system forms the first entry step

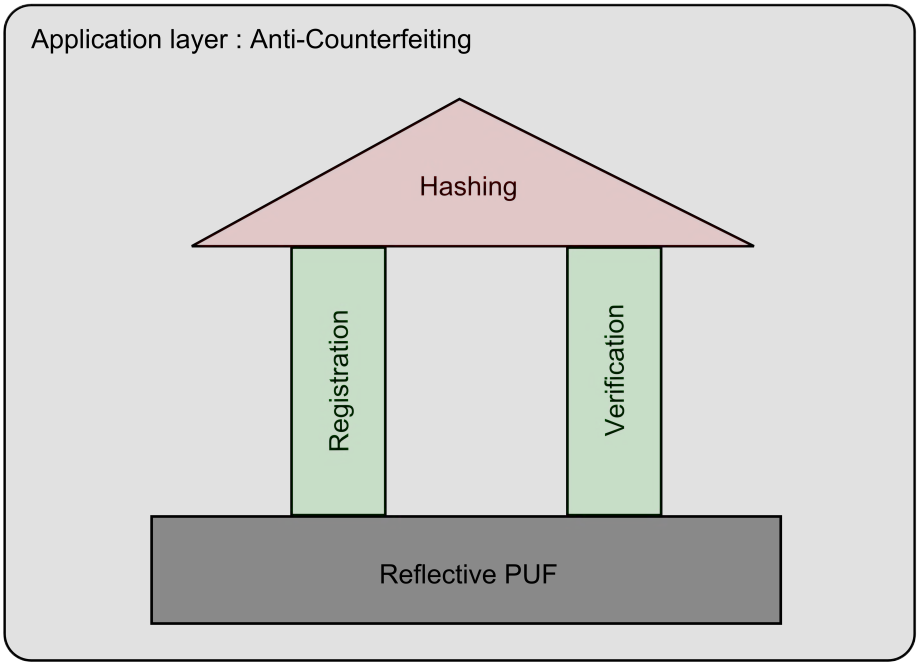


Figure 5.1: Anti-counterfeiting based on r-PUF

of the r-PUF in the solution's scheme. The requirements for this system are -

(a) The entire system must be modular, so that it fits on different assembly lines.

(b) The speed of operation must be comparable to rest of the assembly line. This means fast imaging and processing of the data. While processing may itself not be a constraint since computational power is more accessible these days, it is the fast imaging which has to be considered. To keep the requirements low, up to 20 registrations per minute is the target to begin with.

(c) Illumination module must be capable of fast switching both spatially and temporally. Since the reflection pattern depends on the angles of illumination, spatially switching is required. Moving around the illumination module mechanically is not a good solution, since we aim to complement at least 20 registrations per minute and each registration will involve more than one image capture ($\simeq$ no. of CRPs). Therefore, the design must allow different angles of illumination to be achieved by non-mechanical means.

(d) The optics must be able to image resolutions in the order of $10\mu m$ with sufficient working distances. The exact amount of working distance will be hard to set out explicitly. The goal is to keep it as large as possible, while placing priority on resolution and speed of imaging higher. One other factor which could influence the working distance is the placement of the illumination module. For now, $50mm$ working distance is used as a starting point in design (which is sufficient from the illumination module point of view).

The machine vision industry is quite mature and a host of technical solutions already available in the market, which can be tailored to our needs. There was some designing involved in realization of this system but since they were not the work of this author, we shall delve into it.

The system realized, uses a object side telecentric optics with a working distance $\sim 195mm$ and a resolution of $10\mu m$. The camera itself can capture images up to 30 images per second at two megapixel resolution.

5.1.2 Implementation

The actual assembly line system cannot be shown here as it is out of the scope of this thesis and developed by our project partners Informium AG. Instead another construction was used to implement the registration system with the moniker *Surface Checker*. This *SurfaceChecker* implements all the functionality of an actual registration system as a desktop unit. It has a fire-wire camera, equipped with telecentric optics for imaging the r-PUF tags. The illumination system can be rotationally positioned along two axes (Θ, Φ) using a combination of stepper motor and servo motor. The entire system is controllable using a serial intercase from a computer with an Labview based application. The system implementation is shown in figure 5.2.

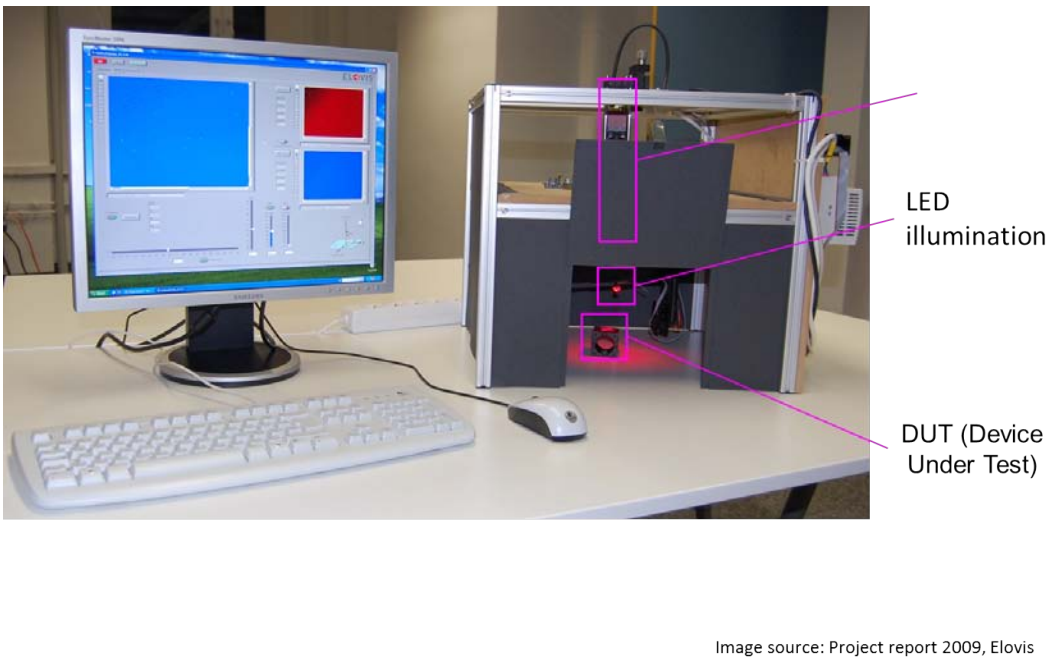


Figure 5.2: Registration system

5.2 Verification device

The verification device is functionally identical to the registration system, however the constraints are different. The use of the mobile phone camera for image acquisition and the fact that the entire device must be hand-held (signifying size requirements) are the main contributors. This section covers the design effort of all the components in a more or less evolutionary format - starting with crude proof of concept implementations to final designs.

5.2.1 Requirements

We bring forward the assumptions made in section 4.3.2 about the size of the r-PUF tag. It is a $5mm \times 5mm$ tag with cross-section dimensions as shown in the figure 5.3. The sizes of the micro-structures are in the range of $10\mu m - 60\mu m$. These two values set the specifications for field of view(FoV) and resolution. The mobile phone lens is not capable of imaging such small resolutions and we need to attach some additional optics to achieve this. This additional optics is usually called a macro lens or magnification optics, and in this work it is referred to as imaging optics or simply lens (when the context provides disambiguation). The

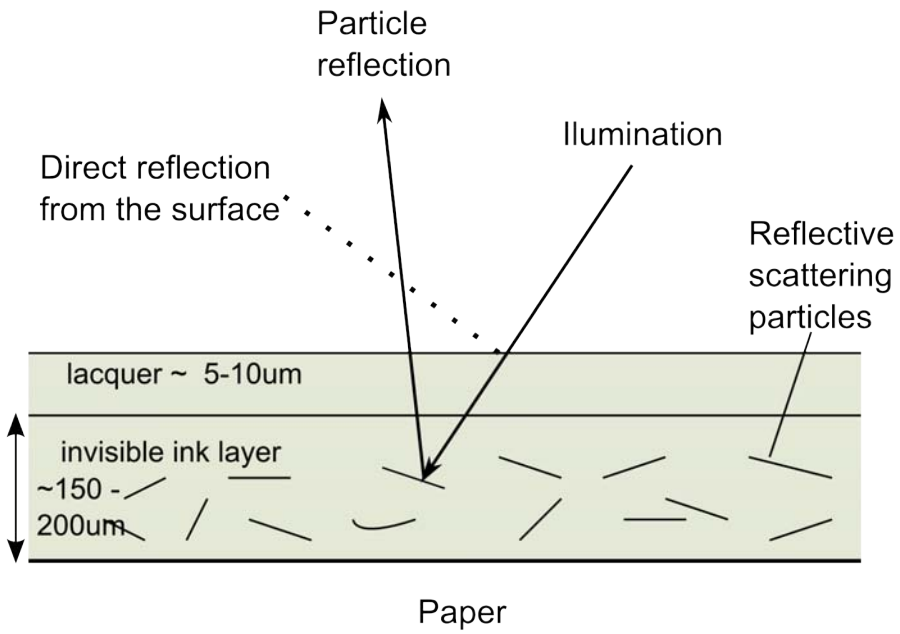


Figure 5.3: Cross-section of r-PUF

depth-of-field must be greater than the thickness of the r-PUF layers in the tag, so that only 2D projection of the reflection from 3D micro-structures are captured, i.e., $\sim 200\mu m$. The working distance or the distance between the lens and the PUF tag is also important, since the illumination module will be fitted into this space. As a starting point, $25mm$ working distance is considered, keeping in mind the overall size of the device. Schematic in figure 5.4 represents all the requirements for a verification system.

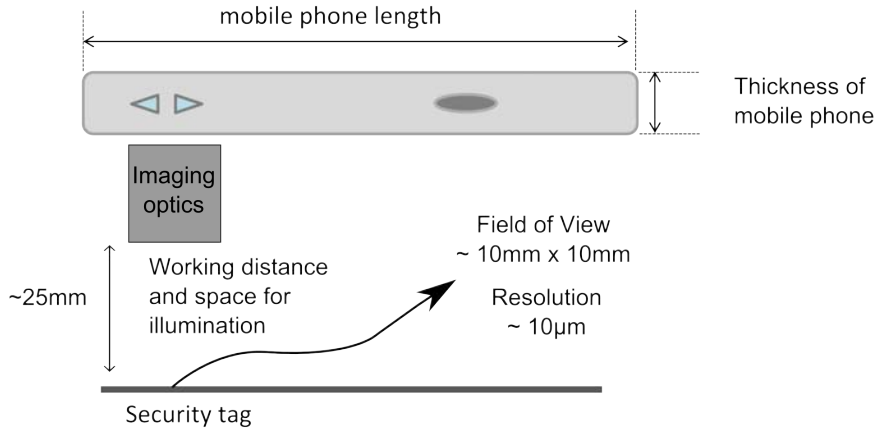


Figure 5.4: Requirements for verification device

5.2.2 Probable solutions

The use of mobile phone camera as a digital microscope is an interesting prospect. This was first explored by [140] as an add-on for mobiles phones with integrated illumination modules. This is almost a perfect solution for the problem at hand. The resolution reported by the authors, fall marginally short of requirements specified. But, that is an issue which can be handled easily by redesigning within the same principle. The illumination requirements and the smaller FoV in r-PUF verification are the only aspects which stops us from incorporating this design as a solution in verification device. This is currently marketed as an off the shelf solution for portable microscopes ([141]).

In a similar application to r-PUFs, Adams in [142] presents a readout device for print-pattern based identification of documents. The readout design consists of a modified Dyson lens with 1 : 1 magnification. The configuration of the Dyson lens mandates no further lens requirement on the camera side. In [142], the authors use a 3.2 mega pixel CMOS OEM camera with any additional lens fittings. However, in r-PUF verification since it is intended to serve as an add-on for mobile phones, the base lens of mobile phone prevent us from adopting this technique. Moreover, first versions of lenses in a different setting were already developed, by the time the modified Dyson lens appeared in literature.

5.2.3 Imaging optics design

Before embarking on designing of a lens system, we wanted to confirm whether one can achieve imaging with a mobile phone for the given resolutions and FoV. A camera objective was used in reverse configuration with image and object sides changed. The PUF tag was placed in the plane of image sensor and the mobile phone camera on the front lens. Since both the camera objective and the mobile phone lens are usually designed for infinity focus, the pupil matching is simple. Figure 5.5 shows the schematic of the arrangement. A sample set of images captured using this configuration are shown in figure 5.6. The reflection of the particles are seen clearly with sufficiently large FoV. A Nokia N82 mobile phone and incoherent illumination from a slit lamp were used for this imaging. This sets the proof of concept basis for imaging micro particles using mobile phone cameras. A straight forward design to meet the requirements stated above would be

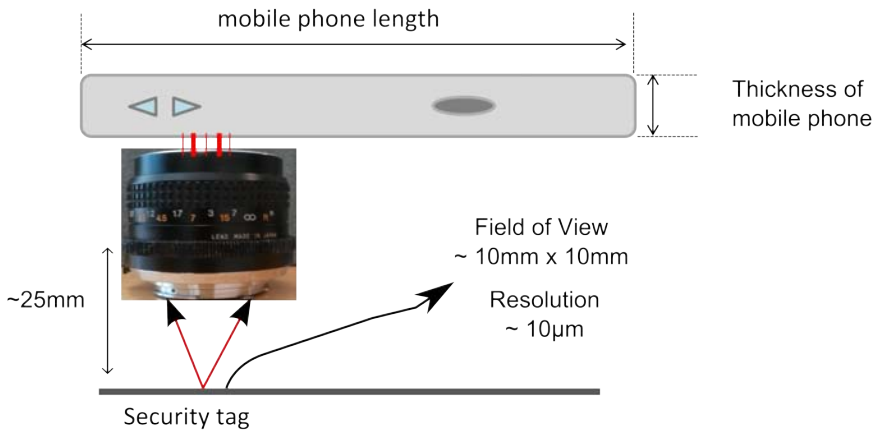


Figure 5.5: Camera objective in reverse configuration

Figure 5.6: Images from camera objective in reverse configuration - taken using a N82 Nokia phone

to use a telecentric lens system (which includes the lens of the mobile phone camera). A simple telecentric system with no magnification can be considered as a $4f$ imaging set up(figure 5.7). Although this design

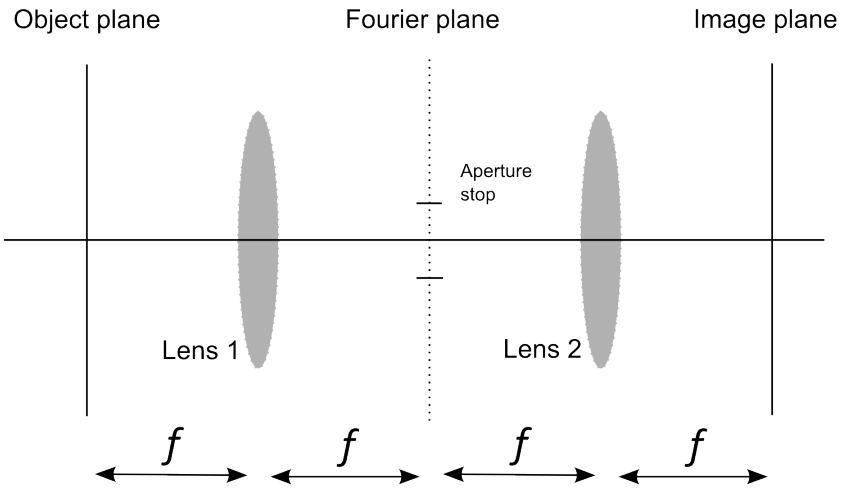


Figure 5.7: 4f-imaging concept

works flawlessly, the size of the optics not very convenient. Considering a lens with focal length of $15mm$, the overall size of the optics would be in the order of $60mm$ which would not easy to fit into a hand-held device. Therefore, the desired system uses a single lens solution.

Version 1 - Aspheric Singlet

A single lens design is envisaged as shown in the schematic 5.8. Although it is a derivation from the telecentric system, it cannot be called telecentric lens in the true sense. The working distance provides the starting point for the first order design with focal length of the lens $\sim 25mm$. The design was carried out using ZEMAX software with poly-methyl-methacrylate (PMMA) as the glass substrate. The choice of the material is influenced by possibility of low cost manufacturing using diamond turning, where even aspheric surfaces can be realized. In all, five iterations of design and fabrication were carried out. The final design was an aspheric singlet, which met all of the requirement specifications outlined in table 4.1. Figure 5.9 shows some of the performance graphs of the final design. Figure 5.10 shows the theoretical modulation transfer (MTF) curves along the with measured MTF curves.

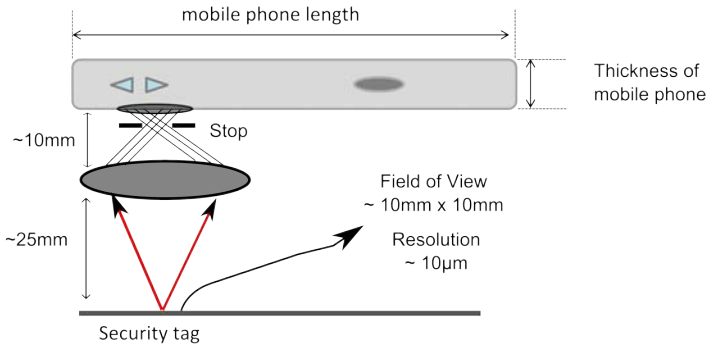


Figure 5.8: Schematic showing a single lens solution in combination with mobile phone lens

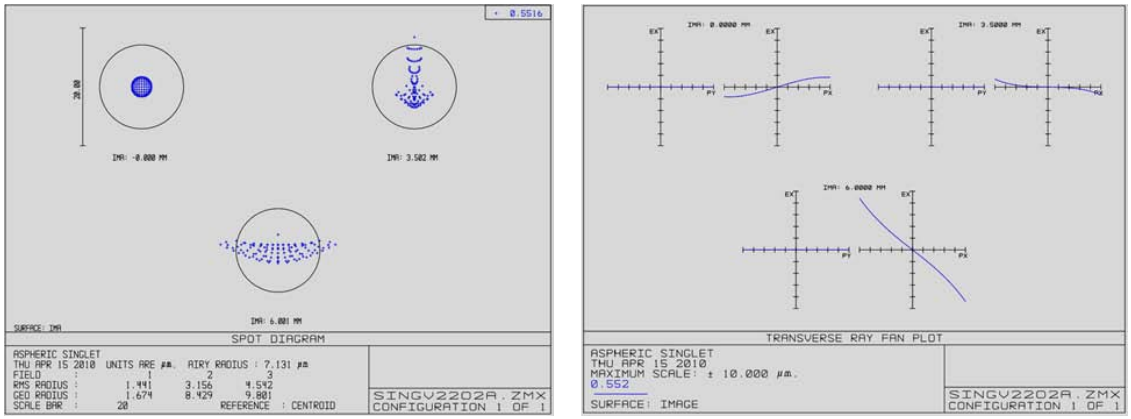


Figure 5.9: Performance graphs - spot diagrams and ray fan plots for the aspheric singlet

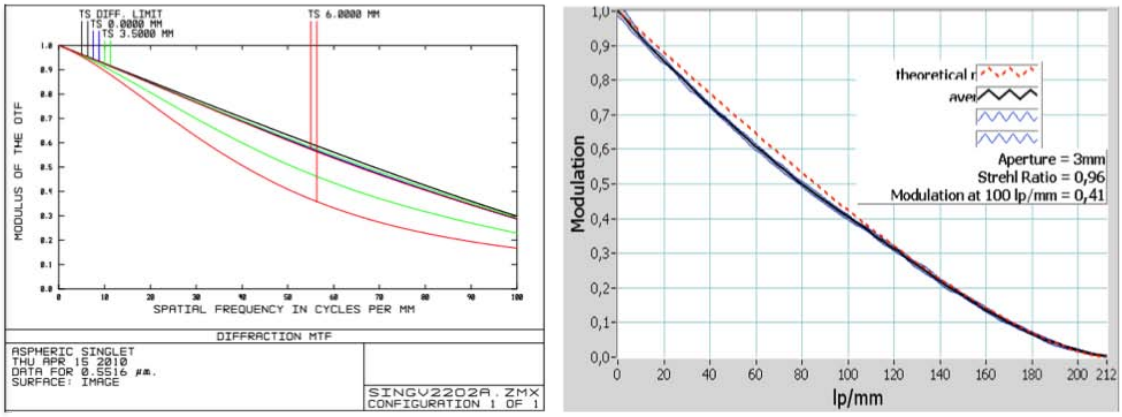


Figure 5.10: MTF theoretical vs. measured

Version 2 - Diffractive Bifocal

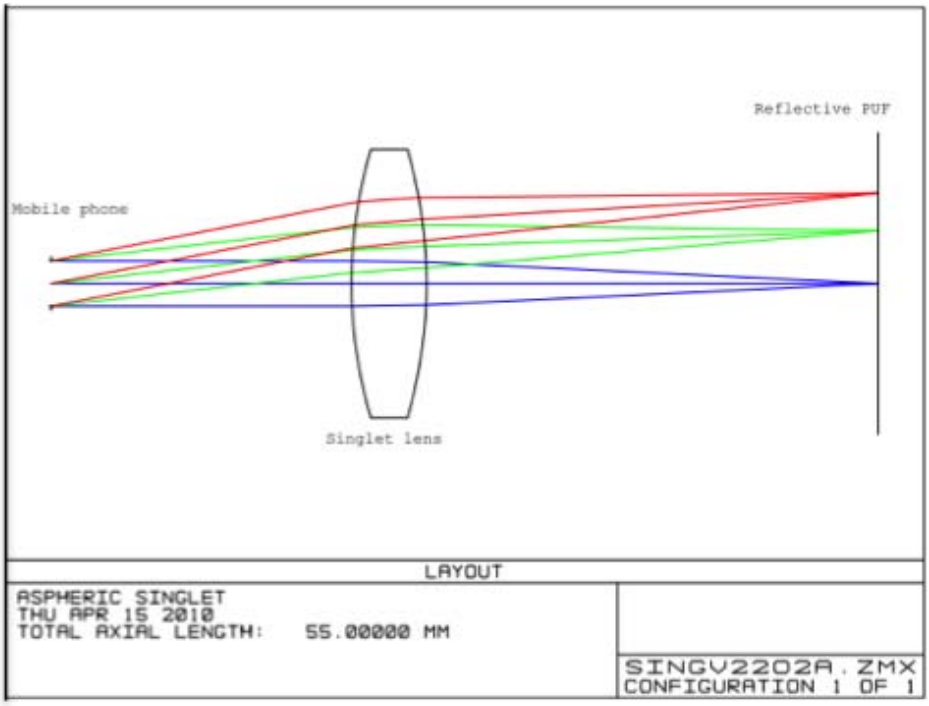


Figure 5.11: Layout for the design of aspheric singlet

The singlet design presented above, has some drawbacks despite its elegance. The depth of field i.e., the range in the object space (where tag is placed) in focus is quite small. The analysis of this can be done using the depth of focus measure due to the configuration of the design. In figure 5.11, the pupil stop can be considered as the entrance pupil diameter (EPD) and the tag to be lying in the image plane. In this configuration, the depth of focus is given by

$$DoF = 2 \times f/\# \times cc \tag{5.1}$$

Where, cc is the diameter of circle of confusion and one can estimate it as the resolution limit of the lens. The $f/\#$ is called image space f-number, defined as a ratio of the EPD to effective focal length (EFL).

$$f/\# = \frac{EPD}{EFL} \tag{5.2}$$

For the aspheric singlet, the image space f-number is $f/\# = 0.04715$ and the resolution limit is in the order of $\sim 10\mu m$, which leads to a depth of focus of

$$\begin{aligned} DoF &= 2 \times 0.04715 \times 10\mu m \\ &= 211.8448\mu m \end{aligned} \tag{5.3}$$

This satisfies one of the requirements, where the DoF has to be comparable to the thickness of the tag. The lens is to be used as an add-on to mobile phone camera, which will be operated as a hand-held. During the course of our testing, we found that the $\sim 200\mu m$ focussing range is not very user friendly to operate.

Hence, the need for extended depth of field optics, this is achieved by using a diffractive bifocal lens instead of a singlet.

The field of intra-ocular lenses have made huge strides in increasing depth of field. Taking inspiration from them, a bifocal with two focal lengths ($\sim 2mm$ apart) was designed. The approach was to individually design two lenses with given focal lengths with the constraint that one surface of each lens is identical (say the lens front). Now, both these lenses were combined in such a way that the identical surface was retained as the lens front. The back surface was diffractive with one of the lenses providing the base curvature and the other as a diffractive add-on. The figure 5.12 explains the design principle. The phase profiles are a

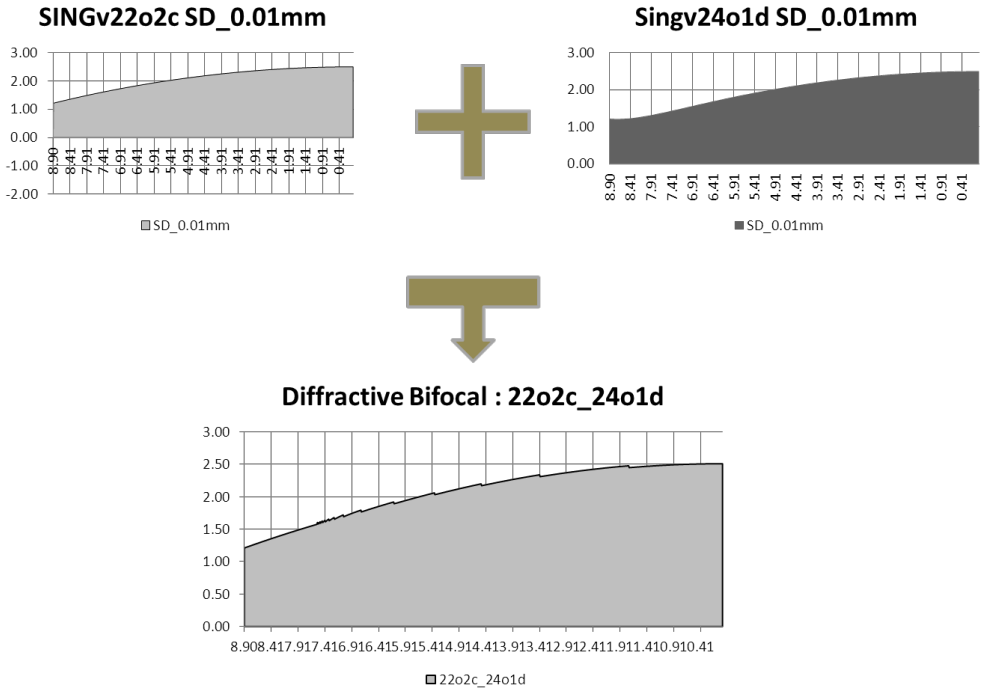
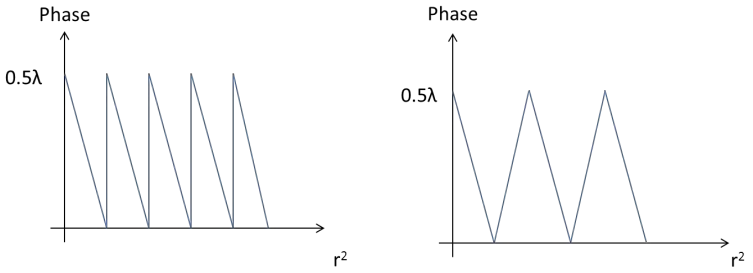


Figure 5.12: Principle for the design of diffractive bifocal

characteristic of the diffractive surfaces. In the first effort, a simple saw-tooth profile (5.13a) for the lens shown in figure 5.12 was fabricated. The profile height was in the order of $3\mu m$, and the corresponding angles between the groves proved very costly for fabrication. The next design used a triangular profile (5.13b), where the angles between profile faces doubled. Figure 5.14 shows the profile of the triangular profile diffractive surface along with a magnified view of the section. The bifocal lens does not completely



(a) Sawtooth profile (b) Triangular profile

Figure 5.13: Types of profiles that can be used in diffractive surfaces

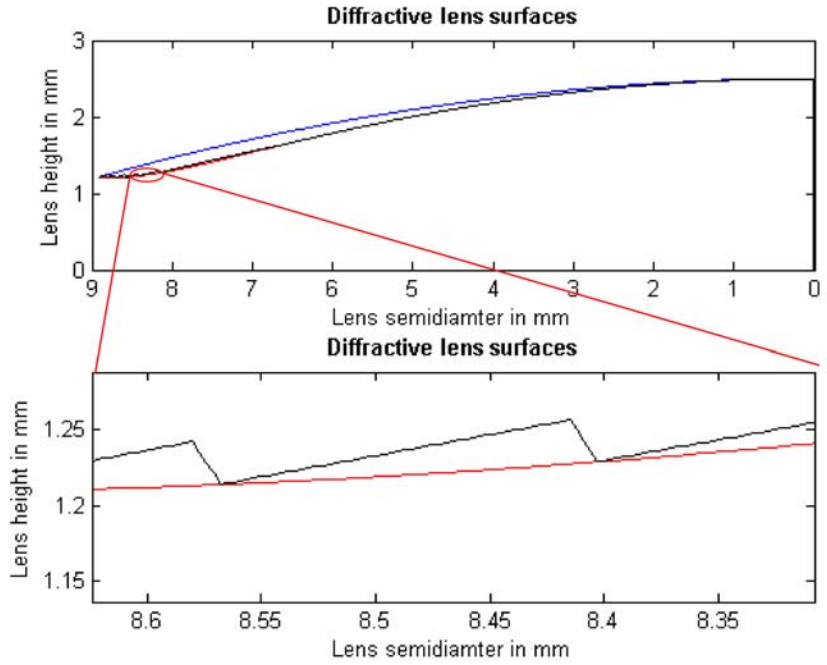


Figure 5.14: Surface profile of the diffractive bifocal

alleviate the problems associated with depth of field and its impact on user friendliness is minimum, since by definition, it can focus on two distinct planes and continual medium. The extended field of view also results in a marginal loss of resolution. The figure 5.15 shows the images captured by the diffractive focal lens at two focal planes and an intermediate plane. The loss of resolution in the intermediate plane is clearly visible. The use of this lens is a trade-off; if we can design the hand-held in such a way that the PUF tags can be exactly placed in the focal plane without much difficulty, then singlet is a better choice.

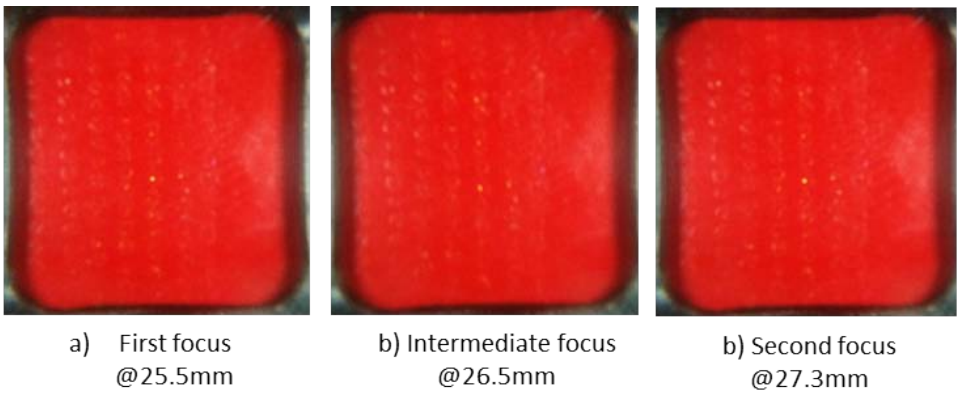


Figure 5.15: Images of r-PUF taken with diffractive bifocal

Magnification or resolution

The issues of magnification is closely related to resolution. When discussing an closed digital imaging system, magnification does not hold as much significance as resolution. What matters is the object resolution that being captured and how that is translated onto camera sensor pixels. Thus captured image, can

be viewed on a any form of display, which then determines the end magnification. In case of the verification device, the object side resolution (responsible for capturing reflections from micro-structures) of the singlet lens as well as the imaging side resolution (responsible for imaging onto camera sensor) have to be considered to characterize the system resolution.

The specifications for objective lens was set at $\sim 10\mu m$. The designed objective has a theoretical diffraction limited resolution of $\sim 7\mu m$ (see figure 5.9), which is well within the desired specification. The characterisation was done by image a matrix of $1mm$ dots, followed by imaging actual PUF tag (figure 5.16). The

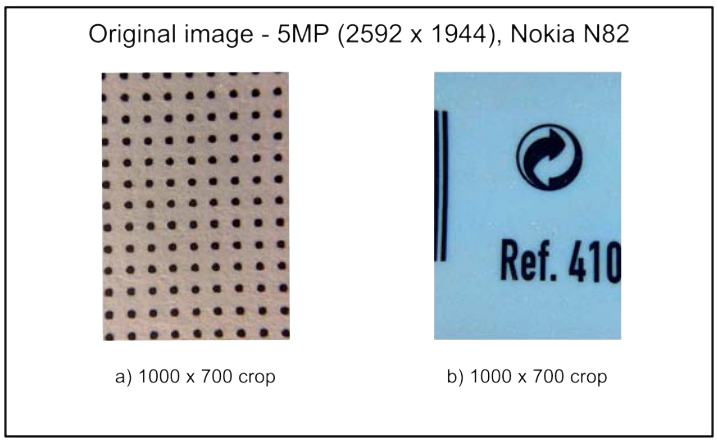


Figure 5.16: Characterization of magnification

resulting magnification works out to $1:4$, in other words $1mm^2$ of object area is imaged onto $200\mu m^2$ on the camera sensor. This theoretically translates to about $12.5\mu m^2$ of object imaged by one pixel. However, this is does not reveal much information about actual resolution. The definitive indicator on the resolution would the MTF curve, the spatial frequency cut-off in figure 5.10 is around $\sim 5\mu m$ which is an aberration since the theoretical limit was $\sim 7\mu m$ and can be attributed to errors in measurement in combination with manufacturing artefacts. Nevertheless the resulting resolution is sufficient to capture the reflections from micro-structures as seen from figure 5.16. The micro-structures are in the range of $10-25\mu m$, which fits well with estimated resolution. The low pixel count for every particle can bring about a stability issue, but is a trade off with larger pixel size and better optics that comes with Nokia N82.

Towards end of 2011, Nokia reorganized their product portfolio, which left Symbian based phones in limbo (N82 included). Xperia S from Sony (released 2012) was selected as an alternative which had $12MP$ at $1.4\mu m$ pixel pitch. This works out similar magnification as in the case of Nokia N82. $1mm^2$ of object area is imaged onto $224\mu m^2$. Resolution wise, one pixel images $\sim 6.25\mu m^2$. This is at the theoretical limit of the objective lens. In reality, the smaller pixel pitch along aberrations, make it possible to image only above $10\mu m$. Thus the final images do not vary much, except that pixel count is higher with Xperia S.

5.2.4 Illumination design

With the imaging optics sorted out, the focus is now on the illumination techniques. Although this section comes after imaging optics, the work carried out was more or less in parallel and therefore, the tone of the text will take the liberty of this presumption. The size of the particles combined with the low numerical aperture (which is due to large working distance) makes it difficult to image reflections from micro-particles.

In the section 4.3.1 the physical characteristics of the micro-structures and their reflection properties were analysed. There is only so much that can be optimized by using grating structures in the micro-structures. The random orientation of the particles allows for capture of reflection of only a few of them. In one of the first approaches, the goal was to increase the number of particles, whose reflections could be captured.

Version 1 - Ring illumination

The relationship between the two angles of illumination and the reflections they cause based on the orientation of the micro-structures was covered in previous chapter. To increase number of particle reflections, illumination from multiple angles was envisaged. This of course reduces the *CRP* space, but still can be used in some anti-counterfeiting protocols, where only one *CRP* is required. Instead of arbitrarily using more number of illumination sources from different angles, we go for the maximum with ring illumination. The schematic for the setup is as shown in figure 5.17. The ring illumination can be implemented using

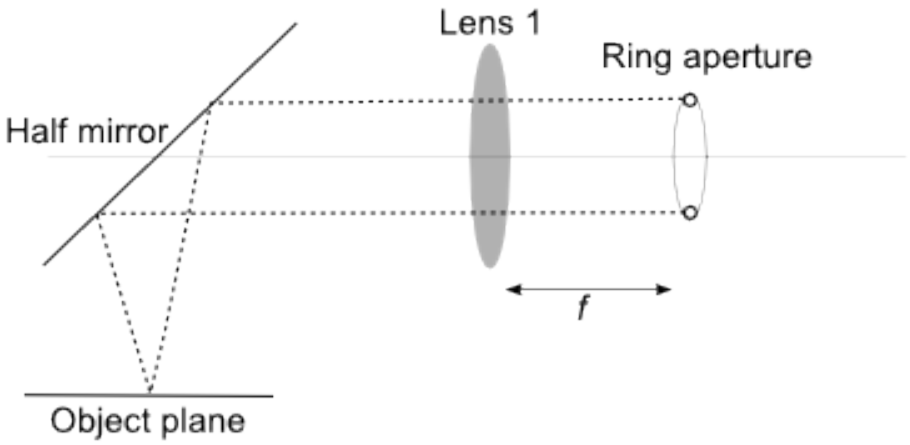


Figure 5.17: Concept of ring illumination

different ways, and the most simple construction would be a ring of LEDs. This arrangement however, does not serve much purpose since only a portion of light is incident on the PUF tag. In our implementation, a ring aperture is placed in the focal plane of a lens which in turn focusses the light from the aperture onto the tag. The r-PUF tag need not necessarily be placed in the back focal plane of the illumination focussing lens, since the incident angle is dependent on only the lens properties - focal length and the diameter of the ring aperture. The incidence angle can be calculated as

$$tan\Theta = \frac{D_{ring}}{f} \tag{5.4}$$

where, D_{ring} is the diameter of the ring aperture and f is the focal length of the lens. If D_{lens} is the diameter of the lens then the field(D_{field}) that can be covered by such an illumination is given by

$$D_{field} = D_{lens} - D_{ring} \cdot \frac{f}{Tag_{distance}} \tag{5.5}$$

The ring illumination can be coupled into the system either by placing it in a half mirror arrangement or as an on-axis set-up where the ring is placed in the telecentric plane. It has been observed that the contrast achieved is inversely proportional to the area of the illumination. This means that the ring's aperture should be as thin as possible. The figure 5.18 and 5.19 shows the ring illumination in combination with the $4f$ imaging optics. In the actual set-up, the ring is implemented using two concentric circular plates - with one of them having a hole in it slightly bigger than the diameter of the other ring, held together by a transparent adhesive tape.

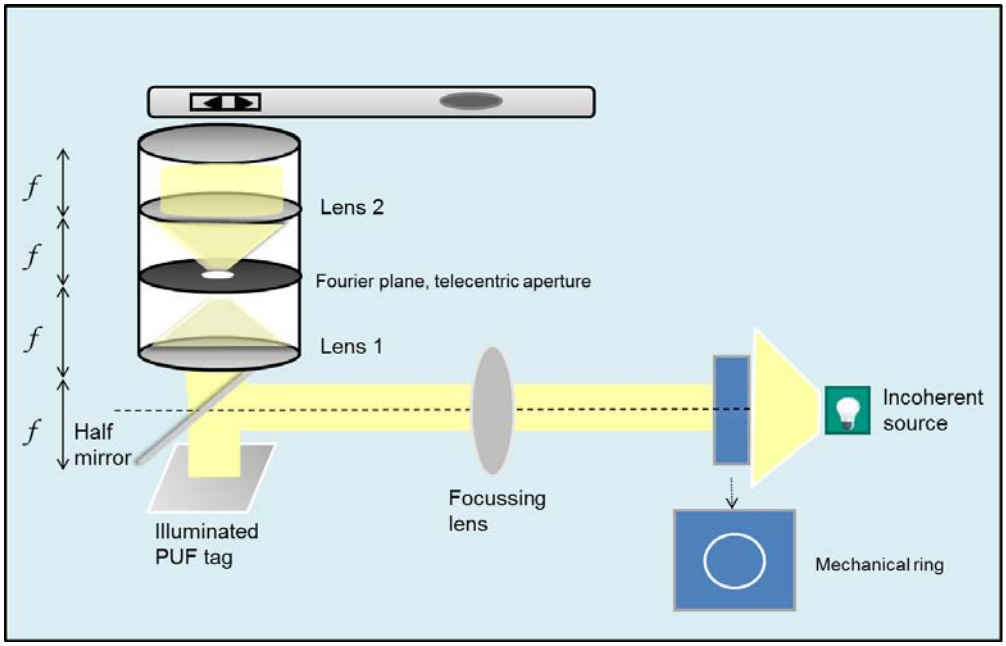


Figure 5.18: Schematic of ring illumination with 4f imaging

The mechanical ring illumination works fairly well, but it serves only as a proof of concept and cannot be used in final implementations simply because of size constraints and use of mechanical rings. It would rather be effective in terms of cost and size if we could redesign the illumination with lesser components. This is achieved using an axicon. An axicon is a term coined by J.H. Mcleod in 1954 [143] for an optical device that images a point source into a line focus. One can express axicon as a form of conical lens formed on a plane surface and a rotationally symmetric conical surface. The intensity distribution of an axicon in the plane perpendicular to the optical axis is described by a first order Bessel function, when an infinite axicon is illuminated with a uniform plane wave . This intensity distribution (transverse) is constant along the optical axis (property of axicon by definition). The Bessel's function is characterized by an intense central part, encircled by rings of lesser intensity (figure 5.20). The transverse intensity distribution is an integration of the interference effects of beams from different rotationally symmetric sections of an axicon. At any given position, the resultant intensity is created by interference from a small annulus of rays coming from the corresponding annulus in the axicon. The propagation distance increases with the increase in

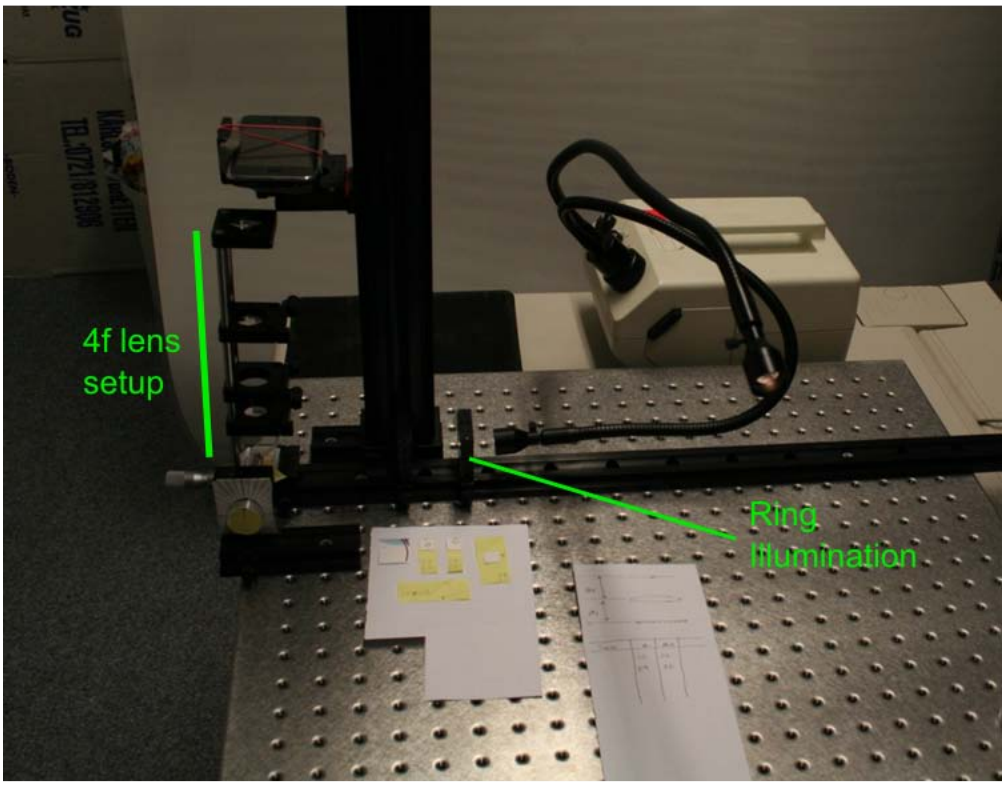


Figure 5.19: Implementation of ring illumination with 4f imaging

diameter of the annulus on axicon that are responsible for interference, thus the intensity of an ideal Bessel beam increases indefinitely with propagation. But then in reality we don't have ideal uniform plane waves or infinite axicons, so what's realizable, is only an approximation Bessel beams. The configuration of the axicon is represented in figure 5.21. The region of uniform intensity after the axicon is optically transferred to illuminate the object by a combination of two lenses and a half mirror.

Let n be the refractive index of the axicon material, Θ_{axicon} be the axicon angle, $\Theta_{deviation}$ be the angle of the deviation of the beams from the optical axis and λ is the wavelength of the light that is incident on the axicon. Equation 5.6 and equation 5.7 give the beam width and the relation between the axicon angle the beam angle deviation. These quantities are graphically represented in figure 5.20. The corresponding design quantities from figure 5.21 are shown in table 5.1.

ISO cone slope	-0.413469
Φ	$22.46\,\text{deg}$
Θ	$12.73\,\text{deg}$
Illumination area	$Ø = 15mm$
Illumination plane	$51mm$ from last lens surface
Lens 1	$FL = 40mm, Ø = 50mm$
Lens 1	$FL = 75mm, Ø = 45mm$

Table 5.1: Design parameters for ring illumination with axicon

$$r_0 = \frac{0.383 \cdot \lambda}{\Theta_{deviation}} \tag{5.6}$$

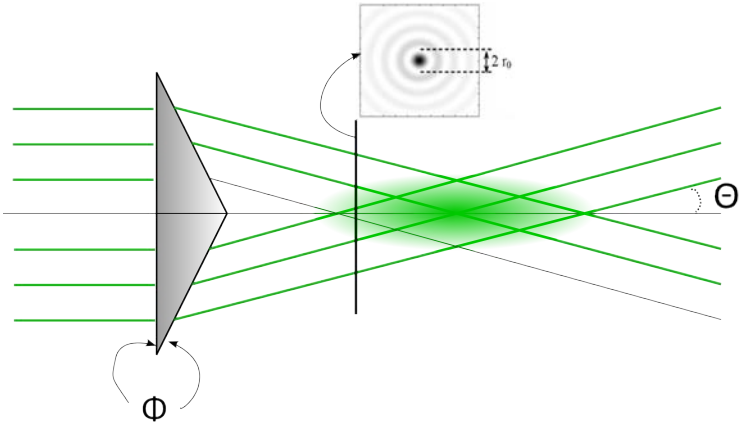


Figure 5.20: Axicon and its basic functionality

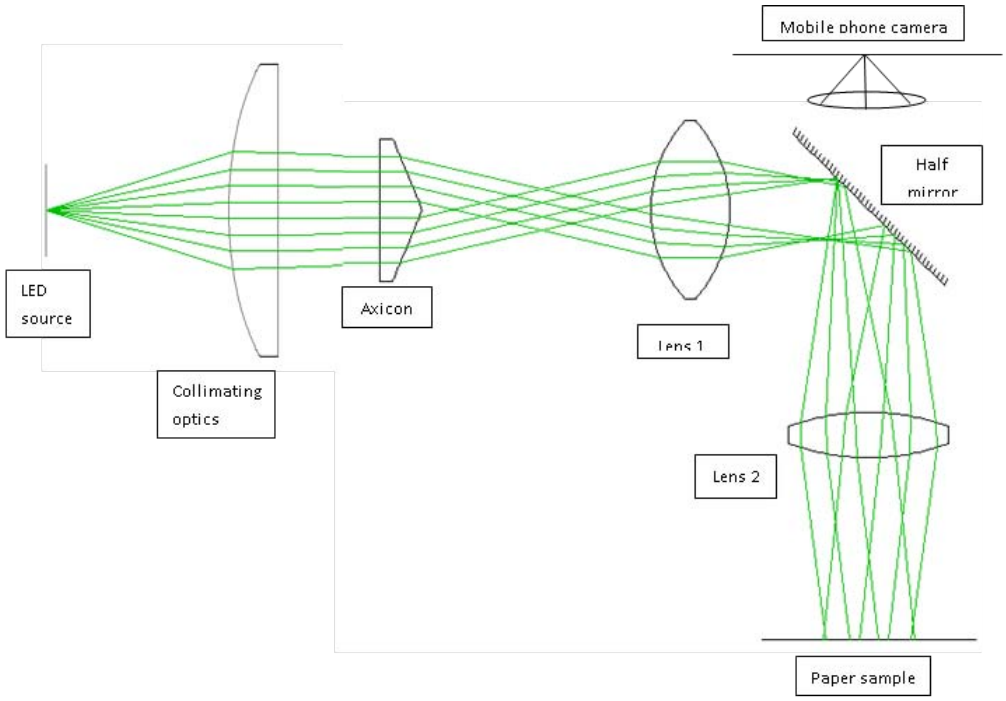


Figure 5.21: Ring illumination using axicon

$$\Theta_{deviation} = sin^{-1}(n \cdot sin(\Theta_{axicon})) - \Theta_{axicon} \tag{5.7}$$

From the illustration above, it can be seen that the space constraints are not effective as the design itself. As is evident from the figure 5.21 above, that the design requires close to $130mm \times 80mm$ space in the vertical plane. The use of two lenses to transform the axicon spot and the collimation lens add complexity to the design. If these can be done away with then some of cost and space can be saved. With this in mind a new design, where axicon and the imaging lens are inline is designed (figure 5.22).

The size constraints from previous design are easily overcome and since only the axicon is used for illumination optics in the modified inline design. It must be noted here that we are using a ring of LEDs instead of a laser for Gaussian source. Though this design provides fairly good rotationally invariant illumination, the performance is not ideal, but is just satisfactory with respect to uniformity of intensity distribution. One could improve performance by using more LED sources in the ring or by using a diffuser between LEDs and

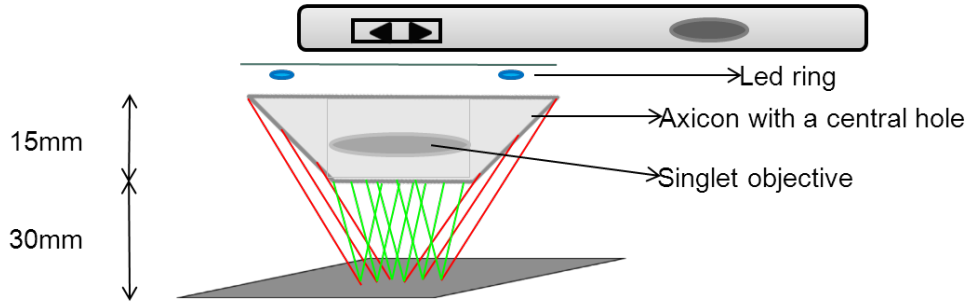
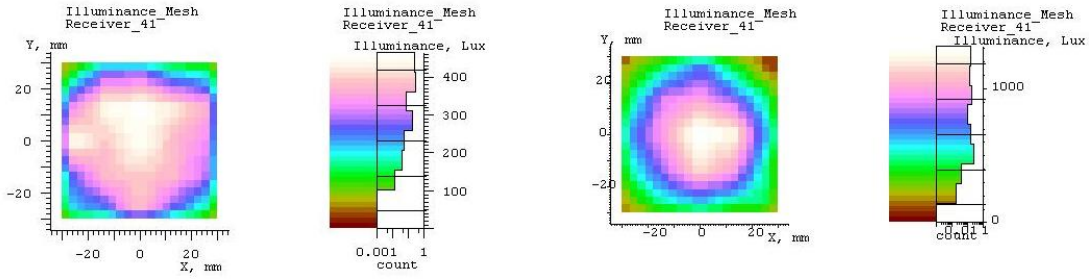


Figure 5.22: Ring illumination using axicon in inline configuration

axicon. The intensity analyses for both cases are shown in figure 5.23. The red square marks the region of interest, where illumination is uniform. The design of the imaging lens used in this configuration is detailed in the previous section. One other advantage of the ring illumination is that it is rotationally invariant, which eases positioning constraints on imaging optics. The non-uniformity in the illumination across the field is



(a) With diffuser (b) Without diffuser

Figure 5.23: Illumination analysis for ring illumination

due to the non-continuous nature of the light sources used here (LEDs are discrete sources). There are other possibilities where a ring of LEDs can be strung together or a use a circular cavity which uses fiber coupled illumination as an input source to give an impression of continuous source but this just increases system complexity in trying to fit them into a hand held.

Version 2 - Simple LED illumination

The advantages of the ring illumination in terms of increased number of particle reflections and the rotationally invariant imaging that it aided are definitely positive, but the lack of uniform illumination across the FoV is its biggest drawback. We decided to re-investigate the possibility of using simple LED driven illumination, with added constraint of uniform illumination across the FoV. We used LW67C white LEDs from OSRAM catalog with an illumination distance of 26.5*mm* as the source. Simulations were carried out using the CAD models and ray data files provided by the manufacturer in ZEMAX. Three simple scenarios were simulated with over five million rays for each LED source -

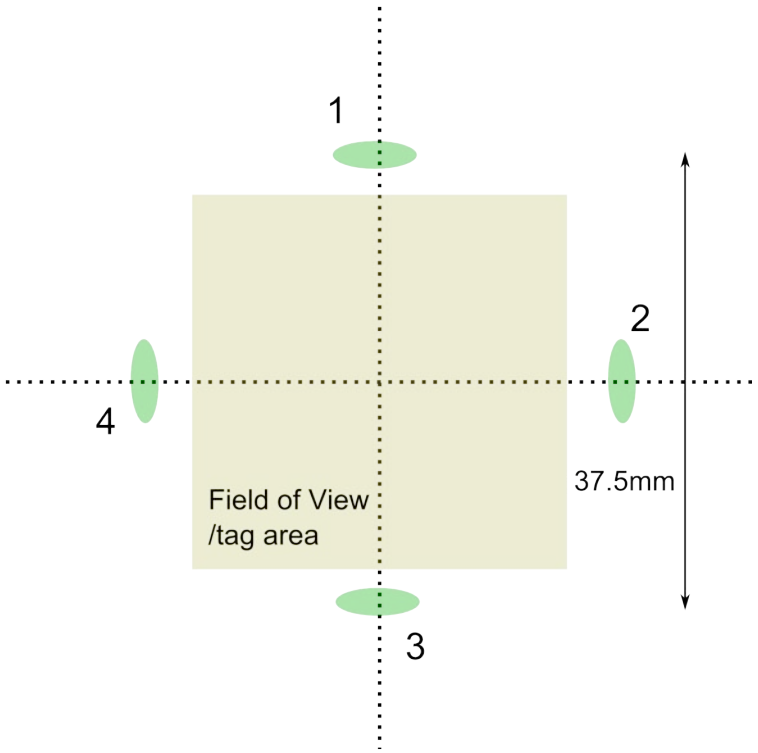


Figure 5.24: Setup for LED illumination

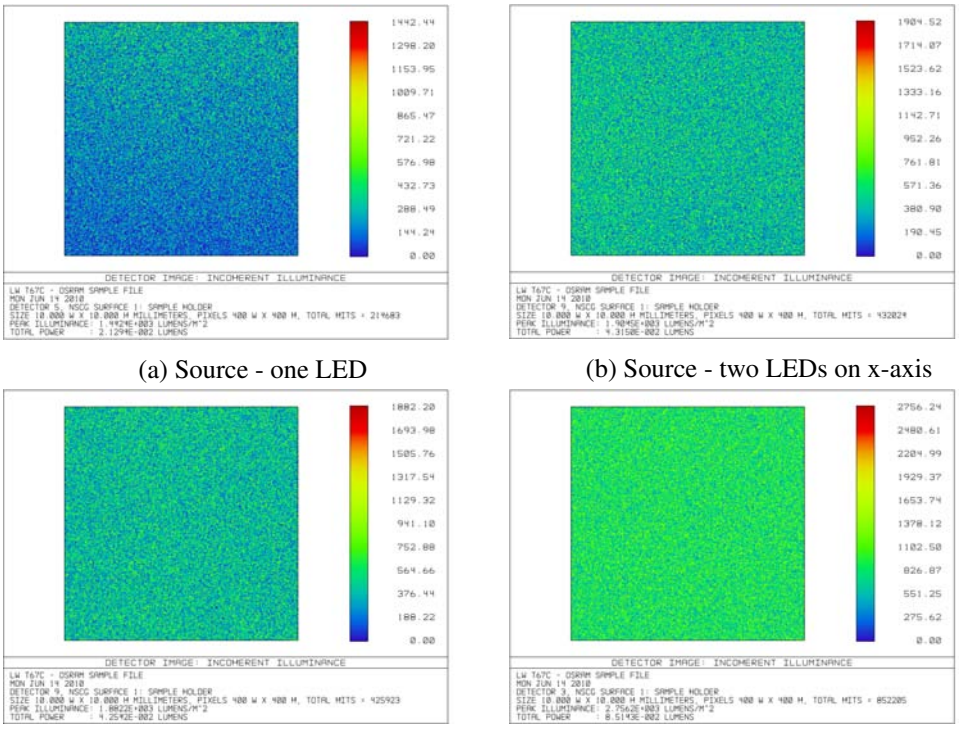
(i) Single LED on Y axis: This scenario presents more or less oblique illumination and the distribution is uneven as seen from the illumination chart in Fig L1.

(ii) Two LEDs on Y axis: To overcome the uneven illumination, two opposite LEDs were used for illumination and the field becomes noticeably even. This case was repeated with two LEDs on X axis which led to results similar to case LEDs on Y-axis. The simulation geometries and the results from the simulation are shown in figures 5.24 and 5.25.

(iii) Four LEDs, with two LEDs on each of the X-axis and Y-axis. Figure L4 shows the arrangement and the illumination analysis of the same.

The objective of these simulations was to check if a single LED is sufficient for illumination. While illumination is possible over entire field of view (FoV), it is not uniform and different particles may react differently. This aspect can be utilized to get variant illumination for different particles but then we would also need marker for image alignment. In case (ii), the effect of illumination by two opposite LEDs was simulated and we could check if there is a difference in illumination w.r.t Y-axis and X-axis LEDs. It was observed that no noticeable differences in illumination were recorded, when the illumination LEDs were shifted by 90 degrees. The illumination in the last case is fairly uniform as expected, since there are 4 LEDs along both X-Y axis. Experiments with real LEDs yield similar results except that when imaged by a mobile phone camera, the imaged tends to get saturated with specular reflection of LED from the lacquer layer.

Though we are not aware of how the micro-particles achieve their reflective property, we experimented with polarization filters in front of the imaging optics to check if they made any difference. Apparently, the micro-particles are metallic in nature (at least when it comes to reflection properties) and the contrast between reflection from particles and specular reflection from the lacquer layer was enhanced. The use of two LEDs to achieve uniform illumination reduces the *CRP* space by half, since Θ can take values from



(a) Source - one LED

(b) Source - two LEDs on x-axis

(c) Source - two LEDs on y-axis

(d) Source - four LEDs

Figure 5.25: Intensity distributions from LED illuminations

$0 - 180\,\text{deg}$ as opposed to full range up to $360\,\text{deg}$. Using two LEDs for illumination and the resulting reduction in *CRP* space is an implementation trade-off. However, in the lab setup(figure 5.26), only one LED was used, with contraptions for varying the angle on illumination in both Θ and Φ. For the anti-counterfeiting application scenario involving consumable goods, a limited number of *CRPs* is still good as compared to having only one *CRP*.

Figure 5.26: Lab set-up used for verification

5.3 Feature extraction and hashing

In the last two sections, the design and development of imaging optics and illumination modules were presented. The next step in the scheme of utilization of r-PUFs is feature extraction and hashing to arrive at a unique code which is associated with the r-PUF. The image of the reflection pattern consists of a set of bright spots due to reflections from the micro-structures against the background of the packaging material. Figure 5.27 shows an example image for the r-PUF at two mega pixel resolution. Feature extraction and hashing of images is used in many different applications and there exists a vast body of research. We started

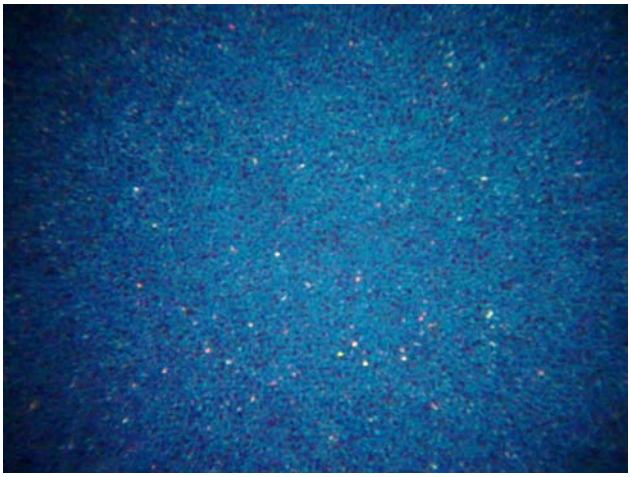


Figure 5.27: Example of reflection pattern from r-PUF, FoV $\sim 10mm \times 8mm$

out with over optimistic expectations in search of algorithms which are rotationally invariant, invariant to scaling and translation, optimal speed (such that it can be implemented on a mobile phone) and those that, possess inherent qualities which translate the unique reflection pattern to a low density fixed code, while preserving it's one-way qualities. Soon, we realized that we are on a beaten track and need to identify our priorities, before settling on an algorithm.

5.3.1 Background and history

Verification and authentication of images is an old topic of research. This process usually involves either an explicit addition of security data to the images or some characteristics of the image content, later extracted and used in computing a security parameter. The exact choice of mechanism is based on a given application. In case of image transfers, the verification would involve not only the source of the image, but also its authenticity, in terms of tampering or corruption of data during handling. The field of research dealing with this is usually referred to as image hashing. But image authentication goes beyond image hashing. A survey of various techniques in the field of image authentication can be found in [144]. In our application, authentication of the image is a secondary goal as opposed to building a unique code from it. It is a given thing that, in case the image authenticity fails, then the generated code is invalid too. The images that concerns our interest have distinct spots - or technically speaking contrast localizations. We began with algorithms which can be used to extract the information about these spots. This has traditionally referred to as a blob detection problem.

The most simple and common operator for blob detection is based on Gaussian kernels - Laplacian of Gaussian (LoG), difference of Gaussian (DoG) and determinant of Hessian. The simplest of them all the

LOG - first applies a Gaussian filter at a given spatial scale to smoothen the image, where noise or details in the image lower than the selected spatial scale are removed. Then applying a Laplacian filter, produces an output with marked variations (zero-crossings) at edges of details present in the image. This technique was first proposed by [145]. Applying thresholds while measuring the zero-crossings can further eliminate effects of noise. The LoG can be approximated using difference between two separate passes of Gaussian on the input image. This approach is called the Difference of Gaussian (DoG). The DoG is essentially a difference operation which is better at restricting the detection to the chosen scale since any artefacts from other scales will be removed in the difference operation. The Laplacian operator can be replaced by a Hessian matrix - which is essentially a matrix representation of the second order partial derivatives of any given function. Such an approach is called the difference of Hessian (DoH).

All the approaches have some dependency on the scale selection, to detect features with different scales, the filters have to be applied multiple times with varying scales. Furthermore, all of them use luminance contrast in some way or the other in their use of derivatives and thresholding of local extrema (minima-maxima). It is well established that a digital representation suffers loss at every step of manipulation due to quantization and averaging. In the proposed application since we are dealing with two separate but identical images, it brings about tight constraints on illumination settings. There are Gaussian based methods which go beyond blob detection to more complex feature extraction such as scale-invariant feature transform (SIFT) and speeded up robust features (SURF). The utility of these algorithms lie more in realm of object detection/recognition than secure hashing of images for authentication. If we use any of these techniques for feature extraction, then there would be a need for another algorithm to hash the extracted feature data to generate a unique code.

Images can be represented using a variety of descriptors - in colour-space, shape, texture or spatial (-temporal in case of video) domains. In addition, one can transform any given image into a mathematical domain such as Fourier, Laplace (as mentioned before), Zernike etc., where feature extraction can be applied. Image hashing goes one step further in using these extracted features in generating a unique hash value, which can be used for verification purposes. Inspired by cryptographic hashing algorithms, efforts were made where images are directly fed to algorithms such as SHA for hashing. The downside of this is that the these hashing algorithms are very sensitive to even bit level changes in input. A digital representation of the image undergo various minute changes at bit level which do not affect the content perceptually such as compression while saving or transformation during change in format, spatial averaging, reduction sub-sampling etc. Images altered by such processes would result in a different hash as opposed to the original image when run through standard cryptographic hash algorithms. Thus came about the need for perceptual hashing, where hashing algorithms are impervious changes which are not perceptible to a given application context.

Monga in [146] provides one of the earliest classifications of perceptual hashing algorithms while Hadmi et al in [147] and other add to it, to include later works in this field.

Statistical analysis based schemes Algorithms in this group extract features, using image statistics in either spatial domain or in some mathematical transform domain. Schneider and Chang [148] was one of the early works, where histograms of images were used as features. Similar approaches have been proposed where statistical characteristics of an image such as mean, variance (computed over blocks in an image) are used as features. One of the main drawbacks of such approaches is that the content of the image can be altered without altering the statistics that are used to represent them. Venkatesan

et al. in [149] propose decomposing an image using wavelet transforms and the randomly tiling of them before taking statistical measurement from them.

Transform domain relation based schemes In [150], Lin and Chang show that there exists invariant relationships between coefficients in the transformed image space. In [151], they show that their method works even when images are put through standard compression processes. While Lin and Chang used DCT coefficients in Fourier domain for their analysis, Lu et al. in [152] use DWT coefficients to achieve similar results.

Coarse representation schemes This approach extends the notion from image compression, where it is established that most of the information is present in the low frequency component, as opposed to high frequencies. [153], [154] and [155] present various methods, which make use of the coarse information(low frequency content) to derive hashes. The content itself may not very attractive, but their spatial distribution and relative densities could be exploited in arriving at a robust hash algorithm.

Low level feature based schemes This category caters to most of other implementations where hashes are computed using pixel level information individually from the images either in the spatial domain or in the transform space. [156], [157], [158], [159], [160], [161] and others have proposed various approaches that can be categorized under here.

Most of these algorithms are not suitable for our application. The reflection of a single particle accounts for $\approx 20 \times 20$ pixel area in a 2 mega pixel image. Thus, changes in reflection pattern due to different *CRP* or token shall yield a very low number of pixels. These changes might be easily missed by naked eye and hence perceptual definition is not applicable here. However, the approaches using Radon transform ([159], [161] and others), Fourier-Mellin transform ([158] and others) and other low level feature based approaches are attractive at first sight. Both Radon and Fourier-Mellin use some form of projection of the spatial data onto linear space, followed by some form of statistical operation to arrive at features, which can be either treated as components of hash or fed into a standard cryptographic hash functions. There have been implementation where such projections are applied in transform space such as Fourier and wavelet decomposition other than spatial domain. After some thought and checking, it turns out that since the features in our image are not uniform in size and contrast, it will be difficult to achieve the level of security as reported by the authors for regular images. Although these transforms have relatively high invariance to rotational errors, their tolerance to translational effects are low. This forms one of the key criteria in our application since there will be some translational errors when imaging using a mobile phone.

Taking inspiration from other optical and image based PUF implementations, the Gabor demodulation for hash generation was evaluated. This technique was first proposed by Daugman et al. in [96] for use in iris recognition algorithms. Pappu adapted the same in his optical PUF implementation ([7]). Shariati et al. [95] too, use a version of Gabor kernel in their implementation. Gabor transform belongs to a broader category of image processing tools - multi resolution analysis. The advantages of this approach is that the residue from the Gabor demodulation can directly be used as hash and there is no need for further processing. However, there remain some factors, which can be tuned using the Gabor demodulation, and these are presented in the next section.

5.3.2 Desirable features

After a careful study of the existing body of work related to image hashing, our notions regarding non existence of any single solution which fulfils are requirements across applications were further strengthened. Moreover, any algorithm mentioned above will have to be adapted and tailored to suit individual application scenarios. To this end, we identify the desirable features for our application in two parts.

First, the properties related to capturing features in the reflection pattern effectively:

a) All the information in the reflection pattern is the spatial distribution of the reflections and their relative intensities. The ability to encapsulate this information from spatial distribution of the reflections from the micro-structures is essential for any algorithm to be applicable in our scenario.

b) Effective across different scales, this translates to its ability to detect features with varying sizes. As mentioned before, although the reflection patterns in our application fall within a small ranges of sizes, it is necessary that most of them are accounted for and contribute to the hash code generation.

c) The tolerance to positional errors is very important with respect to any feature extraction algorithm. In our application, we aimed initially for rotational and translation invariance. During system development, it became evident that rotational invariance is contrary to our objectives. Since the reflection pattern is dependent on the illumination angles, any tolerance to rotational invariance will render the image to be associated with the wrong *CRP*. This aspect was handled in the hardware - device handling was designed with a L-shaped holder such that there will be very less rotational variation in positioning of the tag. However, the L-shaped holder brings about possibility of translational errors, which is not addressed. Thus, algorithm should be invariant to translational errors to a reasonable extent.

Second come the properties related to the hasing aspect and these can be directly referenced from text books on cryptography and has already been treated to a large extent in 2.2.3. Recapping them in brief, they can be described as -

a) One-way or pre-image resistance is a quality of the algorithm which makes it infeasible to reverse compute the input, given an output from the algorithm.

b) Second pre-image resistance - Given a pair of input and output for an algorithm, it is computationally infeasible to find another input which produces the same output.

c) Collision resistance - This is a more strict definition of previous definition, it must be computationally infeasible to find any two valid inputs for a given algorithm which hash to the same output.

d) Size of the hash output be reasonably smaller than the reflection pattern image.

For now, the requirements related to speed of computation and memory costs are left out. Once an algorithm is found suitable, the computational cost factor can be revisited.

5.3.3 Selected implementations

We implemented two standard algorithms, but made requisite adaptations to fulfil our criteria. In this section, we present them and explain the various variables that were tuned to achieve acceptable results.

Algorithm 1 - Laplacian of Gaussian

It was rather a simple choice to start with LoG approach to detect the bright spots - reflections from the micro-particles. Once these reflections are identified as blobs, we note down the spatial distribution details along with mean intensity and area of the blobs. A subset of this information is then fed to standard cryptographic hashing algorithms such as SHA to obtain a unique hash code. The LoG is a straight forward algorithm as its name. First, a Gaussian kernel is built, which can be represented by

$$g(x,y,a) = \frac{1}{2\pi a} e^{-\frac{(x^2+y^2)}{2a}} \tag{5.8}$$

where, x and y are variables in the two-dimensional plane and a is a scale factor which is also known as spread of Gaussian function. The Gaussian kernel is then convolved with the input image $I(x,y)$ and the Laplacian operator is applied on it[1].

$$\begin{aligned} L(x,y,t) =& g(x,y,t) * I(x,y) \\ \nabla^2 L =& L_{xx} + L_{yy}, \text{where the Laplacian can be described as} \\ \nabla^2 L =& \frac{\partial^2 L}{\partial x^2} + \frac{\partial^2 u}{\partial y^2} \end{aligned} \tag{5.9}$$

The Laplacian is a simple second partial derivative operator, which helps to localize the blobs from the change in contrast of the pixel values. Only blobs with a correlation to the spread of the Gaussian are identified by this operation. Therefore, the spread is called the scale factor. To be able to capture blobs of different sizes we need to rerun the operator on the image with kernels using different scale factors. For our application, since the sizes of the spots were within a known range, we did not need a too many scale factors. The effect of scale factors is achieved using sub-sampling of the image rather than varying the scale factor in the Gaussian kernel.

Once the blobs were identified, we went one step further and overlapped the blob data on to the original image. Then, computed the centroid, area and average intensity for each of the blobs. In the final analysis, only a subset containing about ten of the brightest were fed into SHA-256 algorithm to generate a 256 bit hash associated with the tag. An example of the algorithm result is shown in figure 5.28. It can be seen, that our filtering of scale space for blobs needs more teeth since lot of small bright spots (seen clearly in 5.28c), which were due to specular reflections being identified as particle reflections. This aspect can be addressed by following the methods proposed by Damerval and Meignen in [163]. They mainly put forth a method to normalize the scale space and select the blobs based on the maximal lines in the transformed domain. In order to test the effectiveness of the selection based on maximal lines and robustness against noise, we generated images with circular blobs randomly distributed along with pepper noise to simulate specular reflection. The results were much better than before. Figure 5.29 shows the results of the modified algorithm on synthetic images, since the effect of noise rejection is more pronounced. Although this algorithm performs what is set out to do, but as indicated before there are shortcomings. Relying purely on intensity does not augur well, since we are usually dealing with two images of the same object, where intensity levels may be different due to operating conditions. The fact that not all blobs may be true reflections from micro-structures but specular noise, makes us select only the strongest subset of such blobs for

[1] For the sake of simplicity and clarity, the notation used in the explanation of this algorithm is consistent with the wikipedia article on blob detection ([162]) and other literature on scale-space analysis using Gaussian kernels.

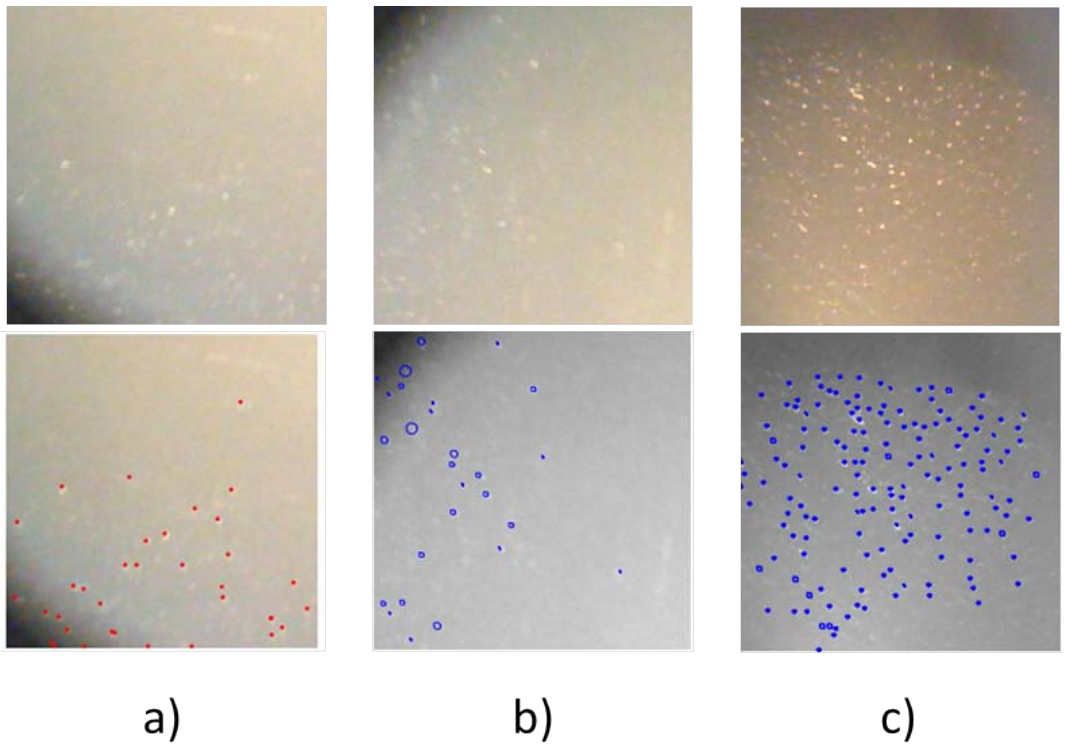


Figure 5.28: Sample results from applying LoG on r-PUF reflection patterns

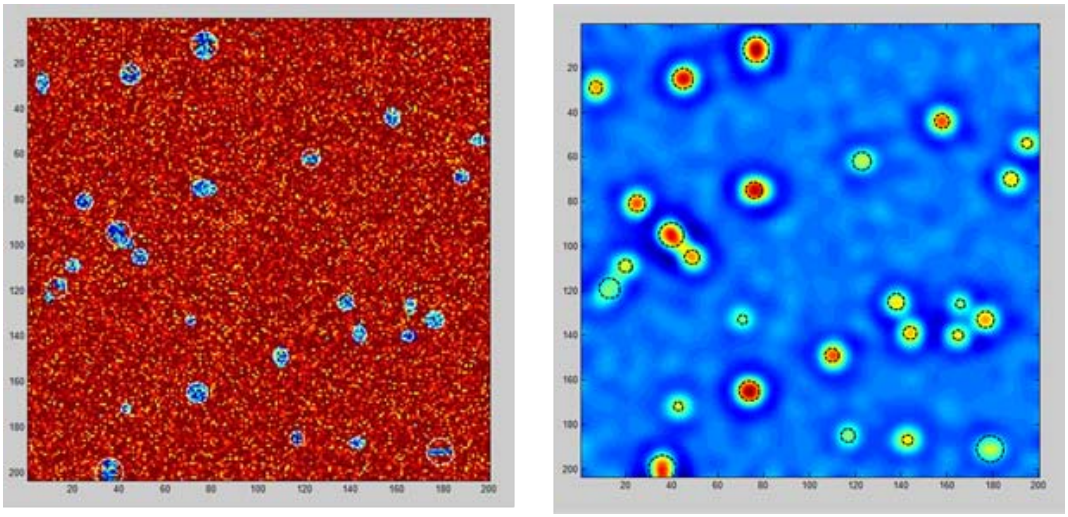


Figure 5.29: Results from applying modified LoG on synthetic images

further processing. The disadvantages brought about by this factor offsets any tolerance related worries that we may have to encounter further on.

Algorithm 2 - Gabor Demodulation

Gabor transforms are used for image representation in many applications, from image coding, compression, texture analysis, motion estimation to modelling image representation in visual cortex[164]. Originally proposed by Gabor in 1946 as a 1-D filter [165], it was adapted to 2-D version by Daugman, who evaluated its properties related to faithfully capturing features across scale and their spatial distribution information in 2-D plane [164]. Daugman further utilized this for encoding the iris image to a unique hash code serving identification applications in humans[166]. In PUF domain, there have been many works which use Gabor demodulation and have reported fruitful results ([8, 97, 95, 136] and others).

Although Gabor filter proposal is more than 50 years old, it is only in last 30 years that significant work has been accomplished. With the growth in multi-resolution representation and analysis of signals, a lot of text books and technical articles have been published on this subject. Gabor transforms belong to general field of wavelet based analysis that are used in many applications. In this thesis, we follow the syntax and formulation of the Gabor demodulation from [167] (a lucid reading catering to beginners as well as advanced users). A two dimensional Gabor function can described as a product of a 2D Gaussian function ($w_r(x,y)$) and a complex sinusoid ($s(x,y)$).

$$g(x,y) = s(x,y) \cdot w_r(x,y) \tag{5.10}$$

The Gaussian function can be expanded as below. Figure5.30a shows a plot of Gaussian function, while Figure5.30b shows another Gaussian function with 45 deg rotation. In the depictions here, the spatial frequencies along two axes were different so that the rotation effect can be visualized.

$$w_r(x,y) = K \cdot e^{\left(-\pi\left(a^2(x-x_0)_r^2 + b^2(y-y_0)_r^2\right)\right)} \tag{5.11}$$

The function is centred on (x_0, y_0), a and b are the scaling factors of the Gaussian function. The r subscript in the above equation indicates a rotation of the Gaussian function, which can be computed as below.

$$\begin{aligned}(x-x_0)_r &= (x-x_0)cos\theta + (y-y_0)sin\theta \\ (y-y_0)_r &= -(x-x_0)sin\theta + (y-y_0)cos\theta\end{aligned} \tag{5.12}$$

In our analysis, we shall neither be using the rotation nor two different scale factors in $xy-$ directions of Gaussian envelope. Therefore, $a = b$ and the r subscript can be dropped. The scaling and direction of the kernel is handled by the complex sinusoid that is to follow. The complex sinusoid in rectangular coordinates is given by

$$s(x,y) = e^{(j(2\pi(xu_0+yv_0)+P))} \tag{5.13}$$

where, the spatial frequencies in x and y directions are given by u_0 and v_0 respectively, and phase by P. In literature, this sinusoid is usually represented in polar form since it is easy to comprehend the effect of filter

(a) Gaussian envelope at 0° (b) Gaussian envelope at 45°

Figure 5.30: Gaussian envelope at different angles

orientation and scale. To arrive at the polar form, we separate the real and imaginary parts first.

$$\begin{aligned} Re(s(x,y)) =& cos(2\pi(xu_0+yv_0)+P) \\ Im(s(x,y)) =& sin(2\pi(xu_0+yv_0)+P) \end{aligned} \tag{5.14}$$

The spatial frequency F_0 and orientation θ_0 in polar form is given by

$$\begin{aligned} F_0 =& \sqrt{u_0^2+v_0^2} \\ \theta_0 =& tan^{-1}\left(\frac{v_0}{u_0}\right) \end{aligned} \tag{5.15}$$

The reverse notation for rectangular coordinate variables using the polar form is

$$\begin{aligned} u_0 &= F_0 cos\theta_0 \\ v_0 &= F_0 sin\theta_0 \end{aligned} \tag{5.16}$$

Thus, the complex sinusoid in polar form can be written as

$$s(x,y) = exp\left(j\left(2\pi F_0(xcos\theta_0+ysin\theta_0)+P\right)\right) \tag{5.17}$$

Combining both the complex sinusoid and the Gaussian envelope gives us the 2D Gabor function.

Rectangular form

$$\begin{aligned} g(x,y) =& K\, e^{\left(-\pi\left(a^2\left[(x-x_0)^2+(y-y_0)^2\right]\right)\right)} \\ & e^{(j(2\pi(xu_0+yv_0)+P))} \end{aligned} \tag{5.18}$$

Polar form

$$\begin{aligned} g(x,y) =& K\, e^{\left(-\pi\left(a^2\left[(x-x_0)^2+(y-y_0)^2\right]\right)\right)} \\ & e^{(j(2\pi F_0(xcos\theta_0+ysin\theta_0)+P))} \end{aligned} \tag{5.19}$$

Design parameters

We present both the rectangular and polar forms for the sake of clarity. We fix zero phase P for both Gaussian envelope as well as complex sinusoid. In the above equation, it is easy to pick out scale factor of the Gaussian a, spatial frequency component F_0 and the orientation θ_0 of the Gabor function. The scale factor for the Gaussian is fixed according to [168], which corresponds to one octave bandwidth of spatial frequency. The other two parameters are carefully selected based on our needs.

We shall denote the spatial frequency in terms of its inverse ($\lambda-$ wavelength), which can be easily expressed in pixels. The orientation parameter can be imagined as convolution of Gabor filter with an image at a given angle. In multi-resolution representation and analysis images there is defined need for faithful reconstruction of the image from the demodulated (filtered) data. This brings about the need for multi-resolution - filtering with various spatial frequencies. In our application, we are not concerned with reconstruction the image but are interested in finding out which filters (spatial frequency) capture most of the information from the reflection pattern. To this end we shall experiment with set of filters having a spatial frequency of $2-10$ pixels and pick out the most useful for our needs. In addition to tuning the spatial frequency of the Gabor function, we also use a set of sub-sampled input images. Usually, only one of the two ways - either varying the spatial frequency or sub-sampling of the input image is sufficient, since they are computationally identical. Since we will be using the complete output of the Gabor demodulation as our hash code, the size is an important criteria and hence, we try and find a sweet spot by varying both spatial frequency and input image size to serve our purpose.

Technically speaking, the orientation parameter θ_0 is not much of relevance and can be set arbitrarily. However, it would be not wise to waste a variable in any analysis. Thus, we first evaluated the possibility of using the filter orientation as a part of the challenge. This would amplify the PUF output during the processing stage. On the other hand, it can be used to give a bit more leeway while designing hardware with constraints. In our application, we image the reflective PUF twice - first for registration and second time for verification. The imaging optics and the operating conditions are different each time. During registration, the tags are attached to products, which are moving along an assembly line. Thus, the positional errors are usually along the direction of motion. If we use a filter which is orthogonal to this direction, then the effect from positional errors can be mitigated. Figure 5.31 shows the scenario, where the tag is imaged during registration process. The directions along which the probability of translation error is marked, along with best choice for filter orientation to mitigate it.

In the verification stage, the tags are imaged under fixed focus with the help of physical holder. In all our analyses, we used a square holder cut out from cardboard to position tag before imaging. In final product design, a square holder may not be feasible since tags can be placed any where on the surface of the product. But, relaxation could be made where a L-shaped holder is used for positioning the tags. This is usually sufficient for mitigating translational error in the x and y directions. In case of any residual positioning errors, they will be restricted to two orthogonal directions along the L-shape. The choice of filter orientation, which bisects the L-shape will be ideal in mitigating the effects from residual translational errors. Figure 5.31 shows the imaging scenario in the verification stage along with marked directions have propensity for placement errors and the best choice of orientation for filters. As a compromise for both the imaging scenarios, the filter orientations of 45° and 135° were selected. It must be noted here that the exact values are arbitrary and one could choose any angles other than the marked directions in the figure 5.31.

Gabor Demodulation

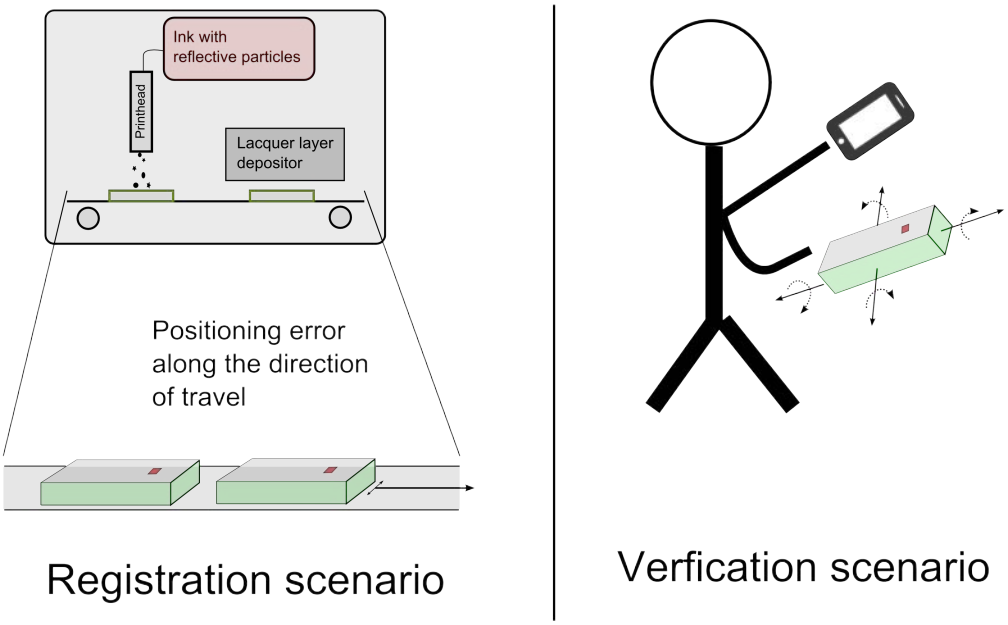


Figure 5.31: Positioning errors in both registration and verification scenarios

Gabor demodulation or filtering is achieved by convolving the Gabor function with the input image. The resulting output in complex in nature and we are interested only the phase part. As pointed out by [8], the odd basis functions of the imaginary part of the Gabor filter are unaffected by the average intensity of illumination. This helps us to relax the illumination requirements while imaging with different hardware systems.

$$I_{Gabor}(x,y) = \mathbf{Im}\left(\iint I(x,y)g\left((x-x_0),(y-y_0),F_0,\theta_0\right)dxdy\right) \tag{5.20}$$

Nestares et al. in [168] propose a separable form of Gabor function using one-dimensional filter banks which results in efficient computation. Since we are interested only in the imaginary part of the filter, we follow a similar approach and construct separable filters for the Gabor function described before as

Even filter

$$\begin{aligned}\mathbf{G_{EVEN}} = & K\,e^{\left(-\pi\left(a^2\left[(x-x_0)^2+(y-y_0)^2\right]\right)\right)} \\ & cos(2\pi F_0(xcos\theta_0 + ysin\theta_0) + P)\end{aligned} \tag{5.21}$$

Odd filter

$$\begin{aligned}\mathbf{G_{ODD}} = & K\,e^{\left(-\pi\left(a^2\left[(x-x_0)^2+(y-y_0)^2\right]\right)\right)} \\ & sin(2\pi F_0(xcos\theta_0 + ysin\theta_0) + P)\end{aligned} \tag{5.22}$$

Figure 5.32 and Figure 5.33 show the even and odd filters for various spatial frequencies and orientations. Using only the odd filter, the Gabor coefficients are computed. To generate a unique code from this, the resulting coefficients are binarized using a threshold. This is converted to 1D vector to form the unique code.

As mentioned before, we can have different orientation of the filer, each generating a set of Gabor coefficients. Pappu et al in [8] propose to concatenate outputs of two filters to generate a hash code. We evaluated this aspect as a follow-up to our idea of incorporating the filter choices as a part of the challenge. In case, we use more than one filter orientation, the exact order of concatenation of the various filter outputs could also be a included in the challenge space. This, however brings about increased computation time and storage requirements for every code. We have explored this in our experiments with the aim of evaluating any advantages of using more than one filter orientation in our outputs.

5.4 Summary

A detailed overview of the system design was covered in this chapter. Requirements were defined for each of the modules along with the rationale. Various constraints related to both functionality as well as system implementation were analysed before finalizing a design. A evolutionary view of the system design was presented which closely captures the effort and the choices that go into the final system.

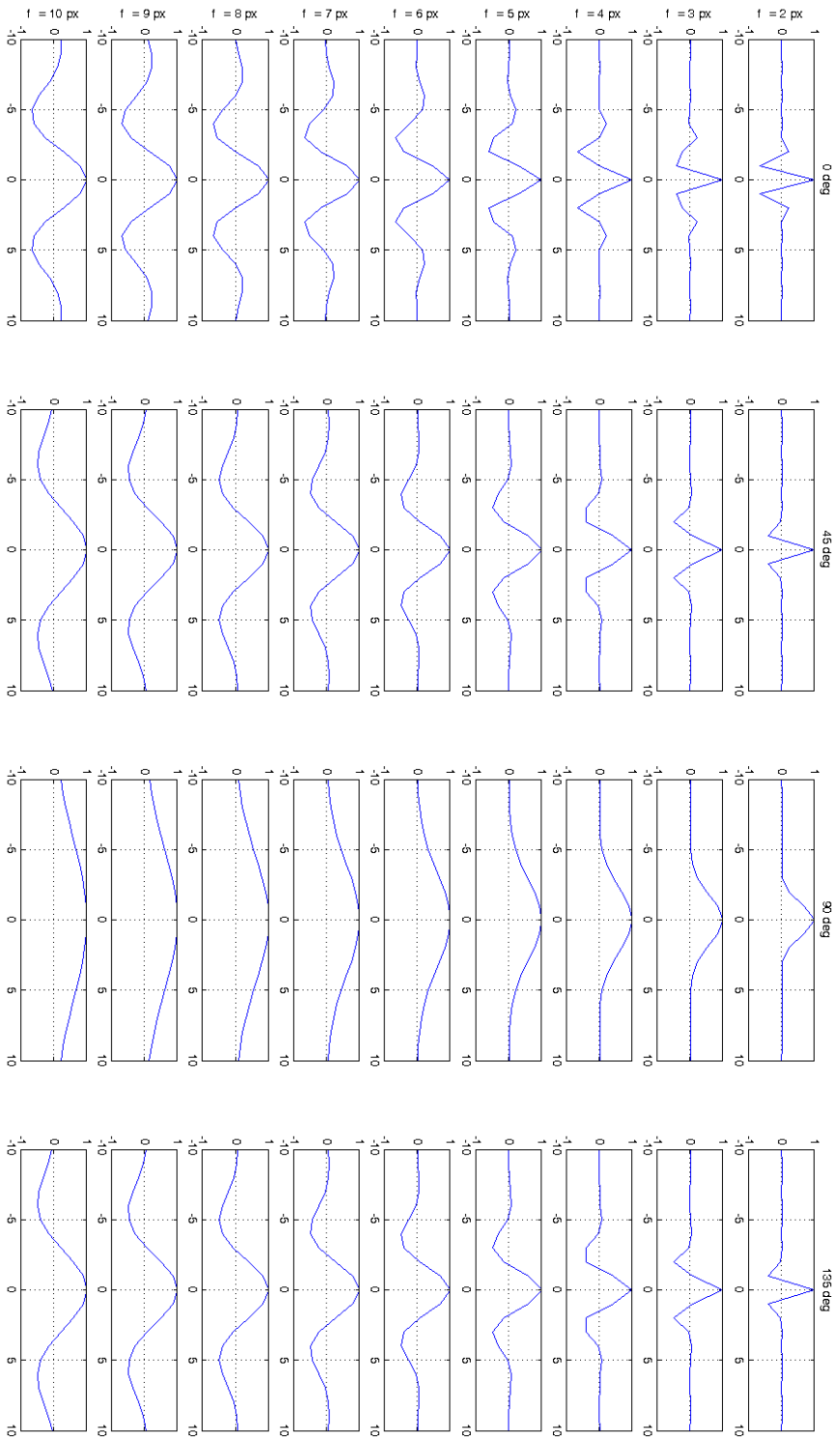


Figure 5.32: Cross section of 2D Gabor even filters at different spatial frequencies and orientations

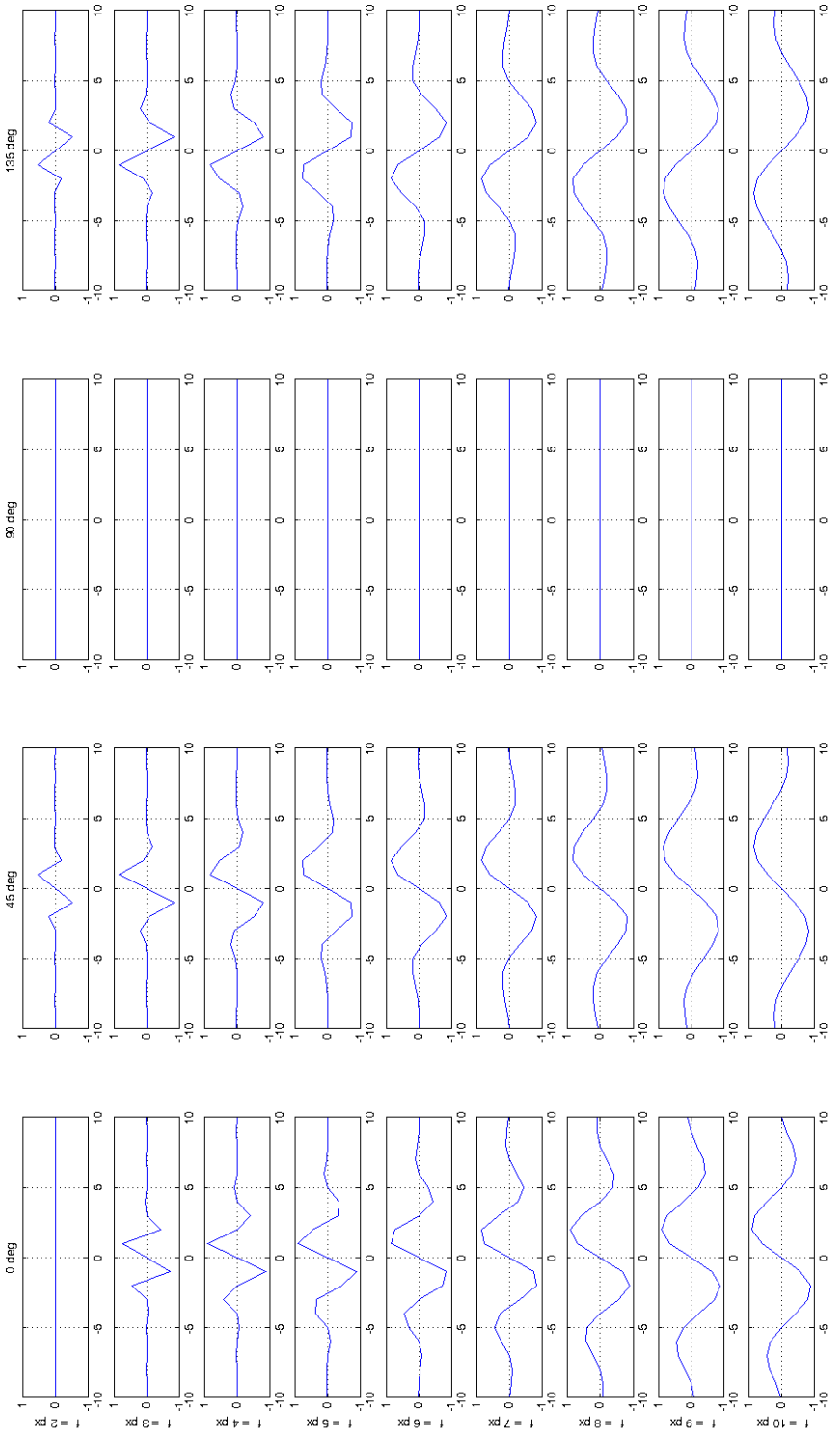


Figure 5.33: Cross section of 2D Gabor odd filters at different spatial frequencies and orientations

6 Experimental results and discussion

In this chapter, details of the experiments are provided along with results and analysis. Having covered the concept of reflective PUF and system design in previous chapters, the goal of this chapter in elaborating the effectiveness of the technique. We have mentioned it in passing while covering the state of the art that there are no standards for reporting results, and hence we shall keep it simple and make an effort to espouse the core qualities of the r-PUF as applicable to anti-counterfeiting scenario. There are mainly three aspects that have to considered while evaluating the r-PUFs - the generation of the r-PUFs, system design of the readout mechanisms and the algorithms that are used in converting the readout from r-PUF to usable codes for anti-counterfeiting application.

6.1 Evaluation grounds

6.1.1 r-PUF generation process

An evaluation or in-depth analysis of the generation process of the r-PUF is contradictory to the PUF principle, since we started off by stating that they contain an inherently random process. However, there are other system variables which have to be explored and checked for any influence on the PUF generation process. Identifying a bias due to a system variable and exploring ways of negating it, is the goal of this evaluation. This forms the basis for the unclonability claims of reflective PUFs. In an effort to understand the effect of system variables on final outcome, system variables are split along the lines of influence related to -

1. The number of micro-particles in an individual tag and their effect on end code.
2. Influence of the print process on the end code.

We realise that it would not be possible to both qualitatively and quantitatively reach a conclusion on both these questions given that there is an inherent random process involved. Experiments were designed to address these two questions, while splitting the system variables along their probable influence domains. This exercise may seem arbitrary at first but it is based on a qualitative analysis done by studying the literature on the specific printhead that is used in our system and discussions with the manufacturer.

Number of Particles : The number of particles in a given tag is influenced by

- Density of micro-particles in the ink, this can also be termed as concentration.
- Printing speed, in our system it translated to the speed of the conveyor belt.
- Print pattern determines how much ink is used in printing and consecutively the number of particles that end up on the tag.
- Dot size. Since we are using an ink-jet printer where printing is achieved using a series of dots, the dot size plays an important role in determining the amount of ink that is used on a given tag. This in turn influences the number of particles in the tag.

Print process influence : The system variables which form the critical core of the printing process itself are

• Dot size. The reasoning for inclusion of this under print process influence is same as above.

• Turn of printhead - this is one factor which bears importance due to the way we use the printhead in our system. The products or substrates on which reflective PUFs will be installed are moving on a conveyor belt in an assembly line with an ink-jet printhead. The placement of the substrate can be altered due variety of environmental and operational factors. We assume that extreme care is taken to avoid any discrepancy but nevertheless, we will have to determine if there is any influence on final outcome due to small artefact in positioning errors.

• Print pattern. The reasoning for including this in this section is same as above.

• Substrate type - we explore the effect of different type of substrates on end code. The spread of dots, drying time and contrast while imaging are some of the factors which are affected by type of substrate.

Experiment design

In both the sections one variable is chosen as a primary, based on experimental convenience and all other variables are pivoted on the primary variable. In the first section, the concentration of the micro-particles is chosen as a primary variable since varying concentration is time consuming and effort intensive. We plan to experiment with three different densities of particles in base ink, starting with highest concentration. At each concentration, the dotsize, print pattern and speed of printing is varied iteratively and a print run is carried out. At the end of one print run we shall have strips of printed material which are then cut up into individual tokens in the size of $5mm \times 5mm$. Thus in first experiment - we end up with three densities, three dot sizes, three speeds of printing and two print patterns; resulting in a total of $3 \times 3 \times 3 \times 2 = 54$ print runs. Each of these print runs consists of four tokens, in all 216 tokens are generated for analysis with this experiment.

In the second experiment, the turn of the printhead is designated as primary variable, again out of operational convenience. We start of with the prinhead in a position where its nozzles are aligned perpendicular to the direction of the motion of the conveyor belt and test two other positions of $+5°$ and $-5°$. At each setting of the turn of the printhead, the dot size(3 different values), printing speed(3 different values), print pattern (two different patterns) and substrate material(three types - blue, white and glossy surface) are varied iteratively and print runs are carried out. A total of $3 \times 3 \times 3 \times 2 = 54$ print runs were done resulting in 216 tokens.

There exists a possibility to realise more than four tokens from each print run and it came in handy on occasions when we had to replace a token due to damage. In each of the experiments, one can analyse the effect of a system variable by selecting sets of tokens where the variable is constant and comparing them with the rest. We call this effort as clustering analysis, where effect of individual variable is depicted as a cluster of comparisons. Details on analysis and results are explained in section 6.5.

6.1.2 System design factors

Imaging system

The reflective PUF brings about a unique requirement when it comes to read-out robustness due the fact that registration and verification are two separate systems but identical in configurations. The critical factors which affect the imaging of the reflection pattern effectively are -

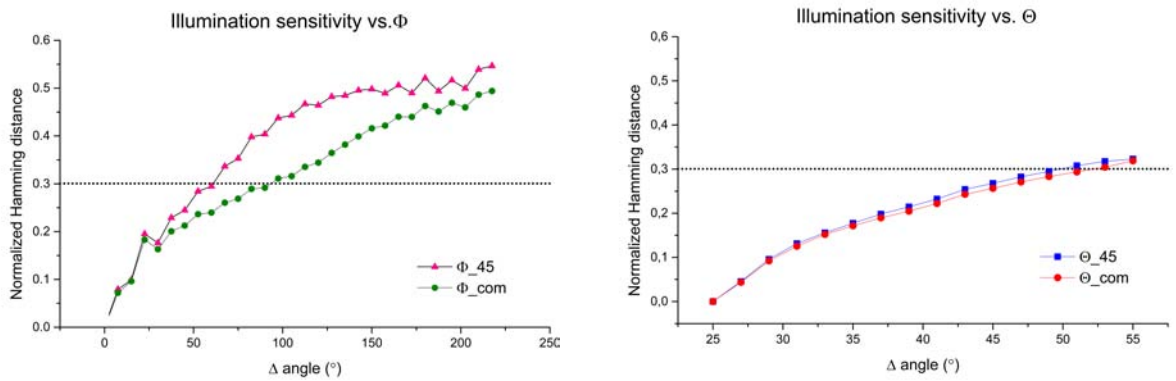
- **Sensitivity to translation :** This one aspect of the positioning errors that was discussed in previous chapter both while considering device design and orientation of the filters in Gabor demodulation. There is very little that can be achieved by trying to compensate translation errors algorithmically. However with some planning, it can be incorporated into system design to minimize translation errors.
- **Sensitivity to rotation :** This is more applicable to verification scenario since the hand held is prone to errors of rotational alignment. To overcome this we incorporate a L-shaped holder where the reflective tag can be placed for imaging. There is still some room for artefacts to creep in at the registration system due to the movement of the products on the assembly line. The resulting positional difference with reference to turn head may cause some bias in the behaviour of the r-PUFs. We explore this aspect, by varying the orientation of the filters in Gabor demodulation phase.
- **Sensitivity to depth of focus :** As with previous two criteria, this also affects the verification system more as compared to registration system. It is relatively easy to handle depth of focus issues at registration end since we can make use of more complex telecentric optics. It is the verification stage where a singlet is used in combination with mobile phone where depth of focus is in the order of $200\mu m$. This aspect too should be handled in device design where reflective PUF is placed in image plane always.

In the registration system, one can work up system complexity - using telecentric optics for depth of focus issues, guide lines along assembly line for controlling effects of translation and rotation errors. All the above factors have greater impact on design constraints in the verification system. Instead of increasing design effort both in terms of hardware and algorithms to deal with these issues, we decided to take the easy way out. The add-on for the cellphone is designed with an L-shaped wedge at the bottom where the package can be positioned. This fixes all the issues highlighted above at the cost of increased user effort in holding the package while it is being verified. Figure 6.1 shows one of the early versions of the add-on in operation, where the fixed positioning is clearly visible.

Illumination system

Having covered the imaging constraints, we turn out focus to illumination. Here again the size and system complexity issues in verification stage override the troubles at registration end. We decided to reduce the complexity of the system by implementing a LED ring where individual LEDs can be controlled corresponding the Φ variable. The size of ring was kept a constant thereby fixing the Θ variable which in turn resulted in the *CRP* space being reduced significantly. Apart from design complexity, the analysis carried out to find the sensitivity of the final outcome to the illumination angles revealed that Θ is less sensitive to final outcome as opposed to Φ. The x-axis in the figure 6.2 refers the difference in illumination angles for which the Hamming distances between final codes are plotted. In the conception of the r-PUF, we had estimated that for each of the illumination angle there would be a unique reflection pattern(overall

Figure 6.1: One of the early version of add-on in operation showing the positioning of the package for verification. Source: Informium AG



(a) (b)

Figure 6.2: Illumination sensitivity of final codes vs. angles of illumination (Φ, Θ). Dotted lines indicate possible threshold values.

$CRP-(\Theta=180°,\Phi=360°)$). The LEDs we are using for illumination are hardly the point sources that we had envisaged and the actual physical geometry brings about some redundancy in the reflection patterns reducing the *CRP* space. In figure 6.2a, the illumination sensitivity is plotted against Φ, the minimum resolution that was used in computation was $7.5°(\Delta_\Phi)$. It is evident that the reflection patterns from any two illumination angles with Δ_Φ difference differ from each other $<\approx 10\%$. Similar analysis for Θ with minimum resolution $2°(\Delta_\Theta)$, shows that the r-PUF is more sensitive to changes in illumination in Θ when compared to Φ. However, the variation due to Φ continues to reach maximum possible $\approx 50\%$, where as with Θ it peters out to maximum difference of $\approx 30\%$. The illumination at the verification device is implemented using LEDs, when put together as a ring of individually controllable LEDs the Φ variation is achieved down to the resolution of the physical size of the LED. With this arrangement, the diameter of the LED ring corresponds to Θ settings. Considering the maximum difference that can be achieved by variation of Θ is about $\approx 30\%$, it was deemed justifiable to drop it as a variable in the illumination design, i.e., the diameter of the LED ring was fixed.

Influence on CRP space

In the section dealing with robustness, it can observed that threshold for deciding the likeness of the pattern can be set at Hamming distance 0.3 (figure 6.4). Using this as a reference, we can compute the cardinality of the *CRP* space.

Starting with Θ the minimum angle separation required for two *CRPs* is $\sim 50°$ (see dotted line in figure 6.2b). Let us denote this using Θ_{th} referring to the threshold. The imaging lens diameter is about $20mm$, which translates to $\sim 22°$ of subtended angle (Θ_{min}). It has been observed during experiments that maximum illumination angle in this domain is $\sim 70°$ (Θ_{max}), any illumination after this will only result in specular reflection from the surface masking the particle reflections. Assuming symmetry about optical axis for the moment, the usable range of the illumination in Θ is given by

$$\begin{aligned}\Theta_{usable} &= \Theta_{max} - \Theta_{min} \\ \Theta_{usable} &= 70° - 22° = 48°\end{aligned} \tag{6.1}$$

It can be seen that $\Theta_{usable} < \Theta_{th}$, thus only one *CRP* can be defined using Θ for angles between $0° - 90°$. If symmetry about optical axis is considered then we can define *CRPs*, on either side of optical axis ($0°$ to $90°$ and $0°$ to $-90°$). The total number of *CRPs* for a given $Phi, with Θ as a variable can be computed to be 48×48 (denoted by $\Theta_{cardinality}$).

Similarly, the cardinality of the Φ component in *CRP* space can be computed. There is no boundaries for Φ in terms of maximum and minimum usable angles but only separation threshold. The threshold value of $\Phi_{th} = 60°$ can be ascertained from figure 6.2a. Thus, the maximum number of illumination sources ($iSource_max$) that can be used in a single *CRP* will be

$$iSource_{max} = \frac{360°}{\Phi_{th}} = \frac{360°}{60°} = 6 \tag{6.2}$$

To proceed further, we need to define some physical dependencies - the diameter (D_{iRing}) of the illumination ring (hypothetical along which the source can be placed) and the physical dimensions of the illumination source. Considering LEDs are our sources, only the significant dimension (say length) corresponding to two dimensional plane containing the ring is required (denoted by $Size_{source}$). The total number of sources that

can be accommodated on the illumination ring (*iRing*) is given by

$$iSource_{total} = \lfloor \frac{\pi \times D_{iRing}}{Size_{source}} \rfloor \tag{6.3}$$

The total number of *CRPs* for a given Θ, Φ as a variable is given by

$$\Phi_{cardinality} = \sum_{n=1}^{iSource_{max}} \begin{pmatrix} iSource_{total} \\ n \end{pmatrix} \tag{6.4}$$

For a given practical implementation, where the $D_{iRing} = 50mm$ and $Size_{source} = 5mm$, $iSource_{max}$ can be computed to be 30. Using these, the $\Phi_{cardinality}$ can be calculated to be equal to 768211.

Now, if we combine the cardinalities of both Θ and Φ variables, we arrive at the cardinality of the entire *CRP* space. For a given threshold of 0.3 used to define likeness of the patterns and the physical dimension assumptions for the example case above, the overall cardinality of the *CRP* space is given by

$$\begin{aligned} CRP_{total} &= \Theta_{cardinality} \times \Phi_{cardinalty} \\ &= (48 \times 48) \times 768211 \\ &= 1769958144 \end{aligned}$$

This is a huge number, indicative of the vastness of *CRP* space. Theoretically, one could capture all possible patterns to override the security of the system but this aspect is explicitly not covered by the definition of security for r-PUFs. In reality, just a few *CRPs* are sufficient in the anti-counterfeiting solution, when used in combination with other identity protocols.

The selection of the threshold 30% or 0.3 in normalized Hamming distance scale can be interpreted as the quantization of the γ as used in the definition of r-PUFs (section4.4.2).

6.1.3 Algorithmic factors

Since most of the device design parameters cannot be tested quantitatively, in the next main focus is on controlling the variables in the Gabor demodulation process and their effect on their final outcome. Spatial frequency(λ), orientation of the filter and level of sub-sampling are the variables that can be tailored.

Sub-sampling level is more of an operational efficiency issue. The input image is 1280×960 pixels in size, on undergoing Gabor demodulation they would generate equally large output. Since we intend to use to output of Gabor demodulation directly as a unique code, the size of 1280×960 is unwieldy. Processing issues apart, the input contains more redundancy at this scale which would result in large intra-distances. Therefore, we explore sub-sampling the image to an extent where the features from reflective micro-structures are not lost. Considering that individual reflection feature has an average size of $\sim 20 \times 20$ pixels in the original scale image, we can sub-sample the input image upto four or five times. This would reduce the features, to about $\sim 2 \times 2$ pixels at level four[1] (L4 sub-sampling : 80×60) and $\sim 1 \times 1$ pixel at level five (L5 sub-sampling : 40×30). This also has a bearing on the choice of spatial frequency.

Spatial frequency determines how effective does the filter interact with the content in the image it is convolved with. Considering level of sub-sampling that we are likely to use (L4 or L 5), the spatial frequency

[1] Sub-sampling level is indicated by the letter L followed by an integer representing the level of sub-sampling.

should also be comparable to the size of the features present at that level of sub-sampling. We explore a range of values for spatial frequency while building the Gabor filter kernels and process a set of image to find the optimal choice. This part is included under section 6.3 and section 6.4 to allow for consistency in dealing with explanations related to inter and intra distances.

6.2 Sample generation

The samples were generated using an REA ink-jet printhead fed by ink containing reflective micro-structures on a short haul assembly line at the facilities of Informium AG. Unused packaging material was used as substrate, which was fastened to the assembly line using adhesive tapes (since they were empty, they were light to be held down). A longish print pattern (at least $10cm$)was carried out instead of individual tags to save on material. The width of the print pattern depends on the actual pattern that is being printed, but in all our prints it was more than $5mm$. After each print run, the printed material was cut up into individual tokens of $5mm \times 5mm$ size. These tokens were then pasted on paper supports measuring $4cm \times 4cm$. We used three different substrates with - blue, white and red backgrounds in five print runs.

Samples were generated in two batches. In the first batch, six print runs were conducted using arbitrary settings for system variables and tokens were realised. From each of the print run, five more tokens were cut up leading to thirty tokens in all. Figure A1 shows examples of such tokens. The send batch was focussed on unclonability experiment or clustering analysis, in which a total of 432 tokens were generated as explained previously.

To tune the filters used in Gabor demodulation, a random selection of five tokens were drawn from the both the batches. We shall refer to these as *config-tokens* henceforth.

6.3 Robustness

We define robustness as the ability of a system to consistently produce a output given the same input over a period of time or at different time instances. Although this is a generic statement, the *system* here entails both the registration as well as verification set-up. Unlike most other PUF implementations, we have different set-ups for registration and verification, which makes the robustness a more acute criteria. The inter-distance measure provides a very accurate representation of robustness.

6.3.1 Algorithm tuning

In the figure 6.3, intra distances computed with five different tokens at nine different spatial frequencies($2-10$ pixels) and five sub-sampling levels are plotted. It can be seen that lower levels of sub-sampling have a lot of redundancy in data which give rise to high intra distance values. At higher levels of sub-sampling the intra distances drop off. We choose level four(L4) of sub-sampling(80×60 pixels), where we believe that particle reflection features are still significantly represented. The output of Gabor demodulation will also be 80×60 pixels, which is then converted into a column vector and stored as the unique code.

The variation of intra-distance with spatial frequency is also to be noted here since at higher spatial frequencies where particle reflection features are smaller than the spatial frequency, the intra-distances are low. This is due the fact that particles features are not contributing to the final code only background content is used for intra-distance computation. A spatial frequency of 7 or more can be ruled out since the particle

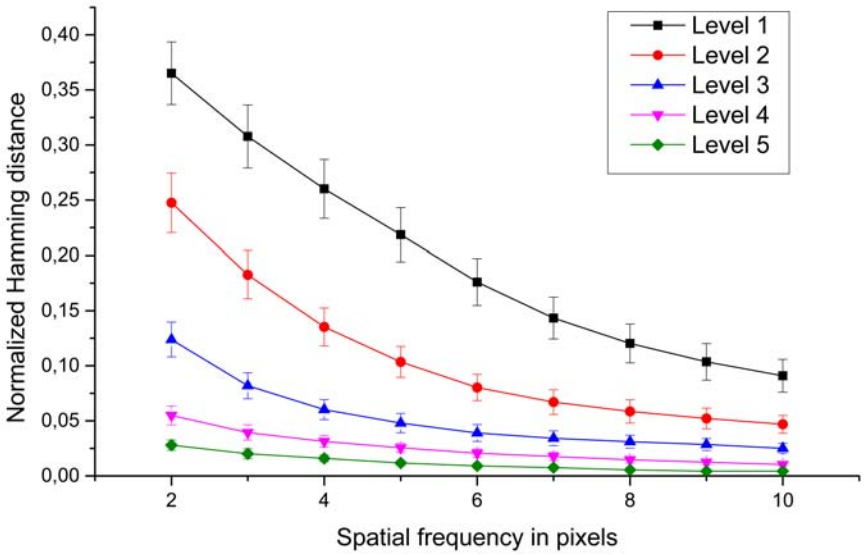


Figure 6.3: Intra-distance summary for all values of spatial frequency and levels of sub-sampling

reflection feature sizes $\sim 2 \times 2$ pixel at this sub-sampling level will cannot be effectively captured. We choose 4 pixels as spatial frequency since it is a mid-point among contenders($2-6$ pixels).

The intra-distances computed for *config-tokens* at spatial frequency $4-pixels$ are shown below in table 6.1. The values in the table are averages of intra-distances using 15 different CRPs for each token. We are currently using only 45° orientation of the Gabor filter. The values for L4 are sufficiently small for all to support our choice of sub-sampling level.

Table 6.1: Intra distances for *config-tokens* at $\lambda = 4 pixels$ spatial frequency

Token/Level	**13A001**	**13B006**	**D2B43S6**	**D2B83S6**	**GK4006**
L1	0,2904	0,2872	0,24988	0,23831	0,2354
L2	0,1524	0,1557	0,12539	0,12037	0,1225
L3	0,0624	0,0734	0,0503	0,05298	0,0619
L4	0,032	0,0371	0,02431	0,02818	0,0351
L5	0,0134	0,0191	0,01343	0,01413	0,0195

6.3.2 Overall robustness

System wise robustness can only be proved by taking large number of samples and testing their intra-distance measures. In all 216 tokens were tested for intra-distances at sub-sampling level four and spatial frequency $4-pixels$. Figure 6.4 shows the histogram of all the intra-distance measures from 216 tokens. It can be seen that most of them are restricted to less than $<\approx 10\%$, which means that our system is very robust.

6.4 Uniqueness measure

We define the uniqueness of a PUF as a variation in the output of different tokens in response to a same challenge. As long as the outputs are distinguishable across the tokens and challenge space, one can con-

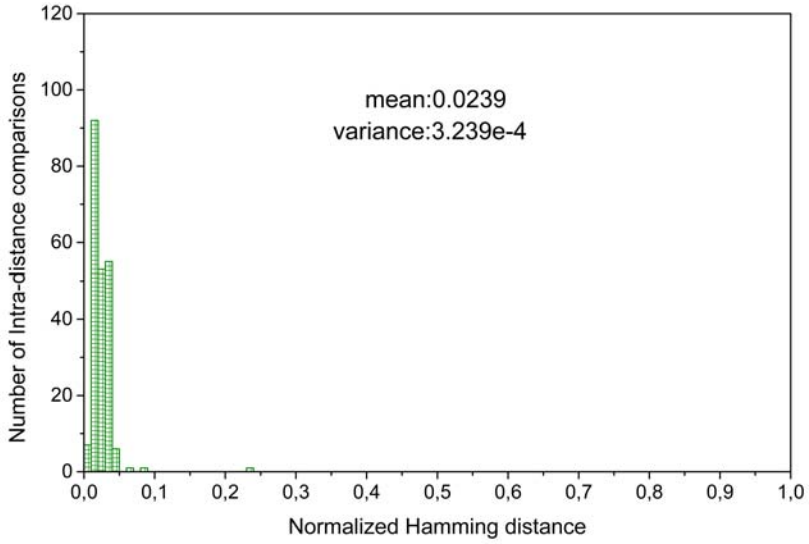


Figure 6.4: Intra-distances for estimating overall robustness at $\lambda = 4$ pixels and L4 sub-sampling

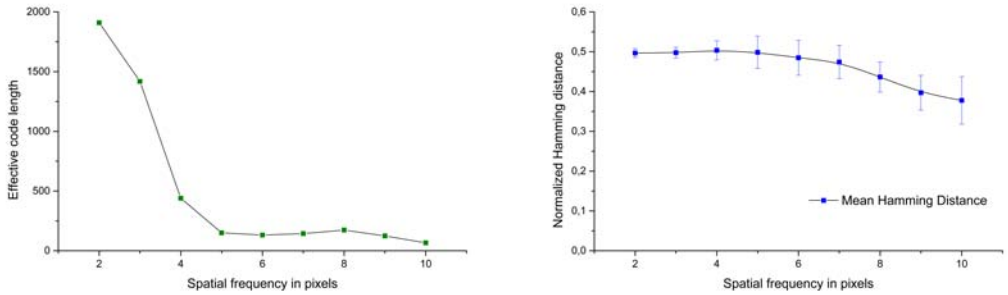
clude that the r-PUFs are unique. Our definition of uniqueness is borrowed from inter-distance measure and therefore, uniqueness is evaluated using inter-distance measure.

6.4.1 Algorithmic tuning

The intra-distance was critical in determining the sub-sampling level. As mentioned before, we proceed at level four sub-sampling resulting in 4800 bit final code. The histogram of inter-distances can be approximated by probability distribution function of a binomial distribution. Using this, the number of effective bits (ECL-effective code length, a term coined by [136]) in the final code can be determined.

$$ECL = \frac{\mu(1-\mu)}{\sigma^2} \tag{6.5}$$

The mean of the distribution is represented by μ and the variance by σ^2. The choice of the spatial frequency



(a) Effective code length (b) Mean Hamming distance

Figure 6.5: ECL and Mean Hamming distance plots at sub-sampling level four for varying spatial frequencies

is influenced by both the intra-distance and inter-distance measures. Figure 6.5a shows the effective code length as a function of spatial frequency. At spatial frequencies $2-pixels$ and $3-pixels$ the ECL is high

but undergoes a significant drop at $4-pixels$. The high values of ECL at $\lambda-(2,4)pixels$ can be attributed to noise that is picked up by very sensitive filters. At $4-pixels$, the filter performs better by ignoring background noise and capturing only particle reflections which are comparable in size. In Figure 6.5b the mean Hamming distance (MHD) is plotted against spatial frequency. There is not much to be gained by analysis of this plot, since at almost all spatial frequencies the MHD is ~ 0.5. The choice of $\lambda-4pixels$ also has a desirable MHD of ~ 0.5, which can be confirmed from the figure.

6.4.2 Overall uniqueness

The figure 6.6 show the inter-distance values computed using config-tokens with filter parameters - $\lambda = 4$ pixels and 45° orientation. Two CRPs were used in computation without averaging. The mean of inter-distances is around 0.5, which means that outputs of any two randomly selected tokens vary by 50% for a given input.

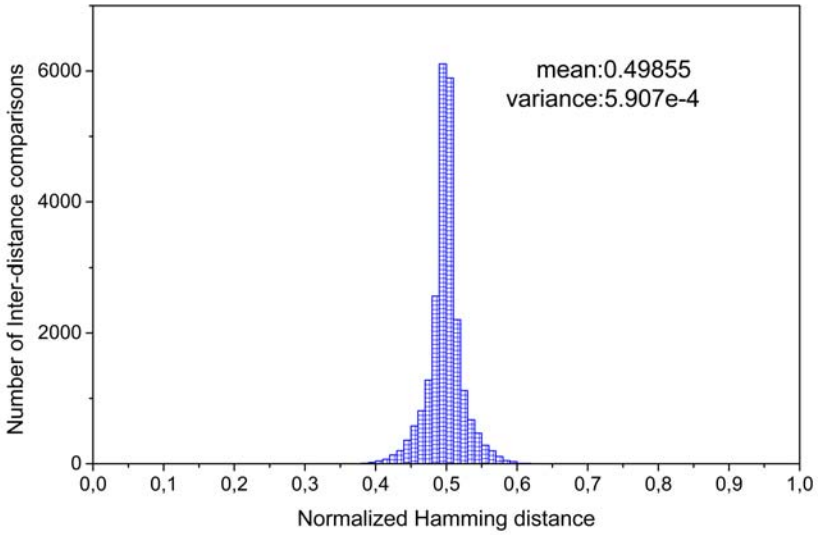


Figure 6.6: Histogram of inter-distance using $\lambda = 4$ pixels and L4 sub-sampling

6.5 Unclonability

We look at system variables in the token generation process and analyse their influence on final outcome. We look for any kind of bias that a variable can cause in the generated tag, which can be exploited to clone the reflective PUF. To analyse a influence of a variable, we sort all the generated tokens into sets where the given variable is a constant. For example, consider print pattern - in both experiments we use two different print patterns. We sort out all tokens only based on the print patterns (pattern-1 and pattern-2), neglecting other variables. We end up with two sets of tokens (if we are using tokens from experiment 1, then each set will have 108 tokens). Since we are interested in finding the effect of print pattern, we have to define one as a reference and check for similarities in end code with tokens bearing same pattern and tokens with other pattern. Let us define pattern-1 as a reference. We shall then select a set of tokens from pattern-1 as reference tokens. We check for inter-distances between the reference set of tokens and tokens from both

pattern-1 and pattern-2. In case the print pattern induces a bias then the inter-distances between reference set and pattern-1 will be significantly different when compared to inter-distances between reference set and pattern-2 tokens.

The selection of reference tokens is as follows. Within the segregation based on print pattern, we know that tokens can be further divided based on other variables. For every combination of variables, we have four tokens, thus 27 subsets within a given set. We select the first token in every set as reference token. Thus final output is always a cluster of the averages of inter-distances from each subset. The evaluation process is explained schematically in figure 6.7.

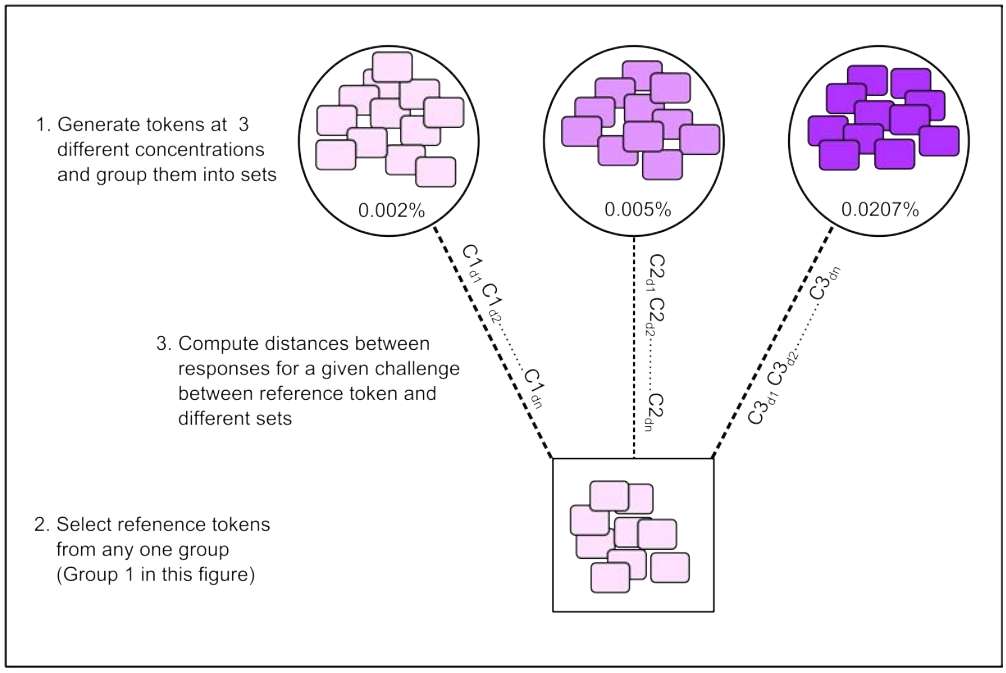
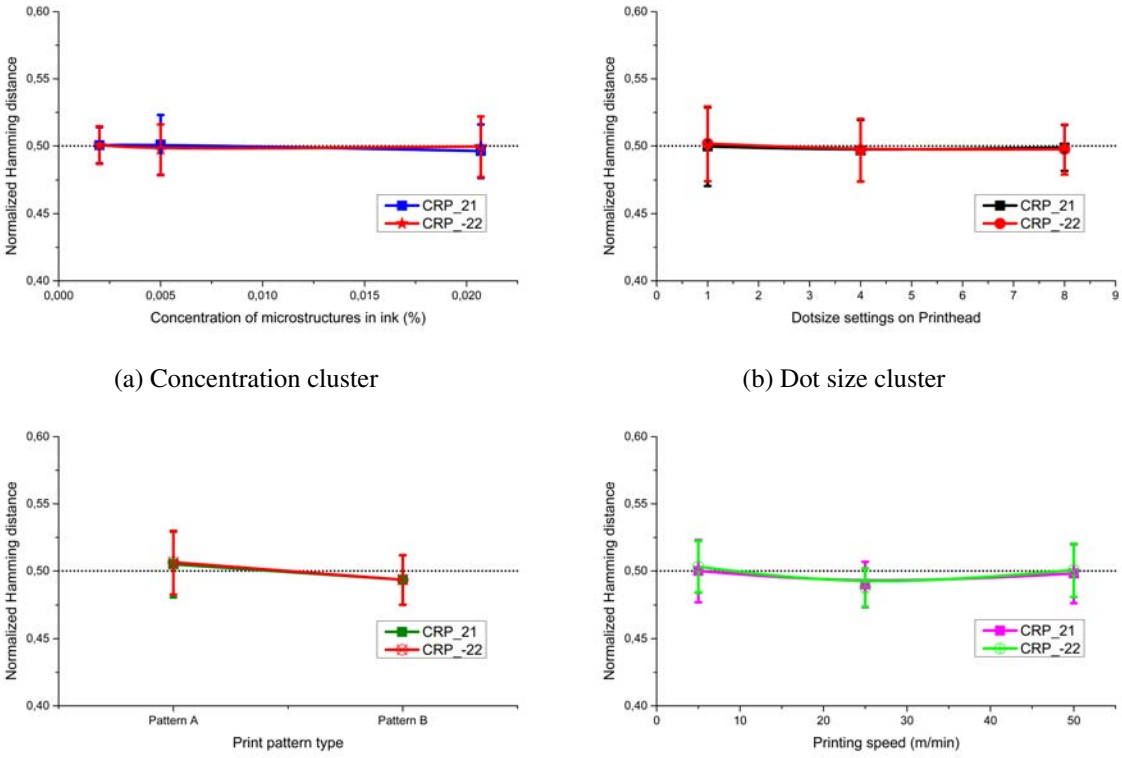


Figure 6.7: Clustering principle with concentration as the choice of system variable

6.5.1 Experiment 1

In this experiment we look at system variables which influence the number of particles on given PUF tag. We identified four variables - concentration of particles, dotsize, print pattern and speed of printing. In the figure 6.8 the results from clustering analysis is presented for every system variable. It can observed that all the inter-distance values are close to 0.5 and there is no significant difference between values of various clusters. Thus it can be concluded that none of the four system variables - concentration of particles, dot size, print pattern and speed of printing introduce a bias into the generation of tokens.

The bias that was verified in this experiment accounts for only the random distribution of the particles, but leaves out the possibility of non-uniform distribution. One can extend the interpretation of the results from this experiment to exclude distribution bias too. We went about this issue in a simple manner where large number of tags were printed with spaced out dots - average dot spacing $2mm$ and average dot diameter $1mm$. It was found the number of particles per dot varied between 3 and 4. Thus, one can conclude that the instantiation process does not introduce any distribution bias.



(a) Concentration cluster

(b) Dot size cluster

(c) Print pattern cluster

(d) Print speed cluster

Figure 6.8: Results from cluster analysis in experiment 1

6.5.2 Experiment 2

In experiment 2, we focus on effect of turn of print head and substrate material as dot size and print pattern were already analysed in previous experiment. Substrate material analysis is straight forward. We grouped tokens into three sets based on substrate - blue, white and glossy paper(72 tokens in each set). With blue as the reference variable, we selected reference tokens among the blue set from each subset of tokens where all the other variables were constant(18 subsets with constant variables resulting in 18 reference tokens). Inter-distances were computed between the reference tokens and tokens from the blue, white and glossy set. The results are plotted as clusters in figure 6.9.

To analyse the effect of turn of print head, we used two different orientations of the Gabor filter. In addition to the usual 45°, we used 90° kernel too. Since the turn head orientation was with reference to the direction of motion(of conveyor belt), 90° orientation of the kernel should be sensitive to any bias introduced by the rotation of printhead. In figure 6.10 the results from clustering analysis using both the filter orientations are presented. It must be noted that there is not significant variation in the clusters across the different turn of print head positions when analysed by both 45° and 90° filter kernels. Thus we can conclude that turn of print head does not introduce any bias in the generation of the tokens.

6.6 Summary

The results of the evaluation of the r-PUF are presented in this chapter. Factors affecting the performance and usability of r-PUFs were discussed. Experiments to validate the PUF properties such as robustness,

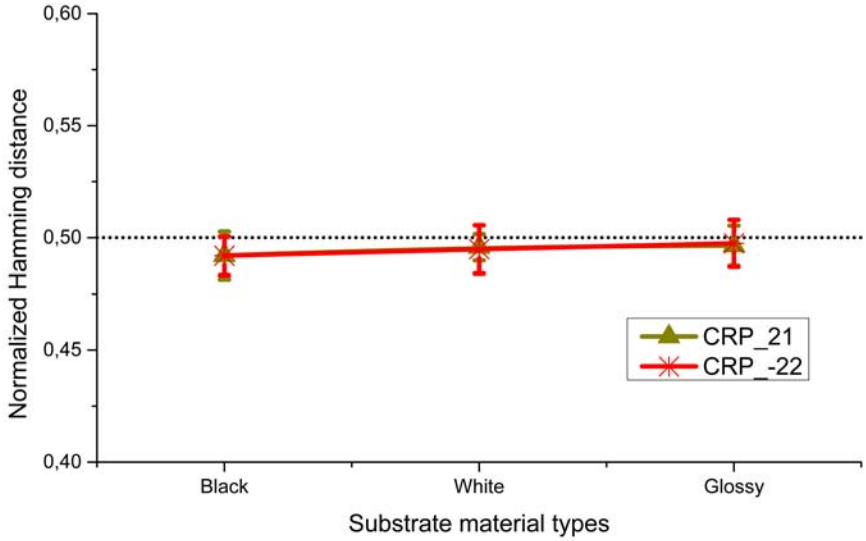
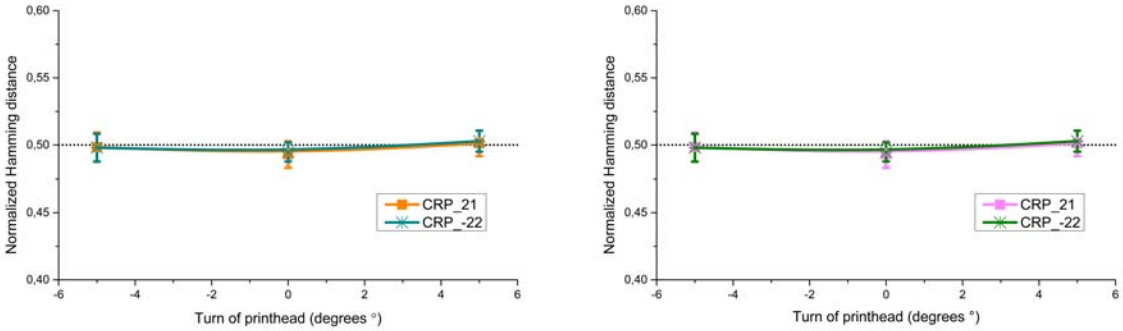


Figure 6.9: Substrate cluster



(a) Turn of Print head analyzed with Gabor transform at 45° rotation

(b) Turn of Print head analyzed with Gabor transform at 90° rotation

Figure 6.10: Results from turn of print head cluster analysis in experiment 2

uniqueness and unclonability were carried out and the corresponding results were presented and analysed here.

7 Conclusions and outlook

In this chapter, we summarize the work carried out in the dissertation and provide conclusions by reflecting on what we set out to achieve and what has been accomplished. The PUF domain over the years has had numerous implementations catering to a variety of application scenarios either individually or in multitude. Our motive was to design a PUF based system for anti-counterfeiting. We excluded theoretical analysis of the security and discounted the usual approach of fitting PUFs in conventional cryptography protocol/ primitive moulds. Instead we choose to rely on existing frameworks, narrowed our attention to one application and experimentally verify the core aspects of the PUF. The focus was on of system design in our chosen application domain and exploring the *unclonability* aspect in r-PUF, such that the technology can see the light of the day instead of being confined to lab set-ups and theoretical proofs. To this end, the crux of this dissertation lies in two parts -

- Design, development and validation of the anti-counterfeiting system using r-PUFs.
- Experimental verification of the PUF in terms of robustness, uniqueness and unclonability.

The notion of unclonability in physical systems and their evolutions was presented in chapter 2. Definitions, frameworks and other formal structures associated with PUF in particular and security in general were explored. We presented a simplistic approach to evaluating the PUF implementations using a minimal set of characteristics which are independent of the underlying technology. The effort of developing PUF domain along the lines of conventional cryptography has its limitations. This aspect was observed and we limit our contribution to application specific definitions while still presenting results in a simple and effective (in terms of comparison, evaluation possibilities) templates.

Chapter 3 covered state of the art in security technologies related to product security and PUF implementations. A sincere effort was made to capture the as much as possible of the huge canvass (in term of technologies) in this field along with brief commentaries where applicable. The detail in chapter 2 and 3 at times may seem out of place in a dissertation; the motivation was to make this a comprehensive reading as far as background was concerned.

7.1 System design

- Requirements analysis was carried out for the specific application of anti-counterfeiting based on r-PUFs. The final system design involved two separate parts related to registration and verification.
- System was implemented end-to-end, with both registration and verification modules. Requirements at each stage were validated. Verification system was the focus in the system design phase. A chronological description involving design and development was presented. This approach is more intuitive to understand the influences that go into design while being constrained by requirements.

- The feature extraction algorithm which is common to both registration and verification was designed/ tuned. Probable solutions were explored and their shortcomings were presented during the algorithm selection phase. Thereafter, the selected algorithm was tuned to fit the requirements of the system and validated with small sample set of five r-PUF tokens.
- Modular implementation of the system provides means for further application level customizations in terms of protocol. For example - the unique code extraction can be run on a centrally server which interacts with the database after receiving the raw data(in form of image) for the reflection pattern from the verification device.

7.2 Experiments and analysis

The lack of consistent reporting standards for the PUF implementations was already commented upon in previous chapters. We propose a simple bucket list of characteristics on which each of the implementation can be compared. Experiments were designed and carried out to obtain results for each of these characteristics. Below is a brief summary of the result for r-PUF.

- Robustness of the system was verified using the intra-distance measure. In all 216 r-PUF tokens were tested for two different CRPs and the mean intra-distance was found to be $< 3\%$.
- Uniqueness of the r-PUF is an important measure since it signifies its utility when used to identify a product instance. Inter-distance measure is used to quantify uniqueness. Out of 216 r-PUF tested for uniqueness, the mean inter-distance was found to be ~ 0.49 with a variance $\sim 5\%$. The information content in the final code is $\sim 10\%$, i.e., ~ 500 bits out of 4800 bits.
- Unpredictability property of the r-PUFs was analysed across the CRP space for a large set of tokens. Ideally, the knowledge of one CRP for a given r-PUF token should not reveal any useful information where one could predict another CRP for the same token. This validation was carried out using distance measures between various CRPs for a given token. The reduction in CRP space (Θ is constant, while only Φ is used in CRP space) owing to design constraints imposed by illumination setting in verification device also bring about reduced notion of unpredictability. For the r-PUF, the unpredictability can be guaranteed only for a finite number of CRPs - where $\Delta\Phi \sim 20^\circ$ for a given value of Θ.
- Unclonability analysis was carried out for six different system variables involved in r-PUF instantiation. The scope of the experiments included concentration of the micro-structures, type of the substrate material on which r-PUF is embedded and printer specific variables such as dotsize, printing speed, printed pattern. The alignment settings were also explored where the printhead is skewed with reference to the normal operating axes.

  For each of the variables, ~ 210 r-PUF tokens were generated with at least three different variable settings (~ 70 for each setting). Results were collated and a clustering analysis was carried out. It was conclusively proved that there is no bearing of the system variables on te final outcome.
- One-wayness can be inferred by the extension of the unclonability analysis. One cannot gain any knowledge about the system variables by analysing the final outcomes statistically. This forms a experimental validation of the one-wayness property of the PUF.

Tamper evidence is the only characteristic, for which we are not providing explicit proof. However, the combination of uniqueness, unpredictability and unclonability analysis provide an insight into relationship between the reflection pattern and final code, which can be extended to infer tamper evidence. The access to limited number of tokens was the main cause for not carrying out studies in this area. It would be possible to tamper few tokens and confirm the inferences but it would not be comparable to sample sets used in deriving results for other characteristics. Then again r-PUF was presented as a extended primitive for anti-counterfeiting application, where there is scope for implementing a customized protocol. This provides an opportunity to abstract the 'tamper evidence' property to the application protocol.

7.3 Outlook

Two important factors are required for r-PUFs to be used in product security. Firstly, the r-PUFs can only be used on conducive packaging surfaces or if they can be embedded to the product surface itself. Second, a communication medium is required, so that the verification device can query the database for authenticity of the r-PUF at hand. At the outset these do not seem to be very restrictive, but if there are ways to find alternatives then the relevant applications can be expanded.

Counterfeit drugs is one of the major problems which impacts not just the manufacturer economically but also consumers. Extending r-PUF solution to pharmaceutical products seemed a natural path to effort. Reflective PUFs in its current form can be readily used as tag on medicine packaging and this would not merit a mention in the outlook section. However if the same can be applied to individual tablets then it would mean that we are targeting the core of the counterfeit medicine problem. According to figure 7.1, the false packaging constitutes about $\sim 68\%$ of the overall counterfeit medicines that were reported, while false active ingredient with legitimate packaging forms the next highest cause ($\sim 18\%$). Thus by extending the r-PUF principle to table level instantiation, one could effectively address $\sim 90\%$ of the counterfeit trade in medicines.

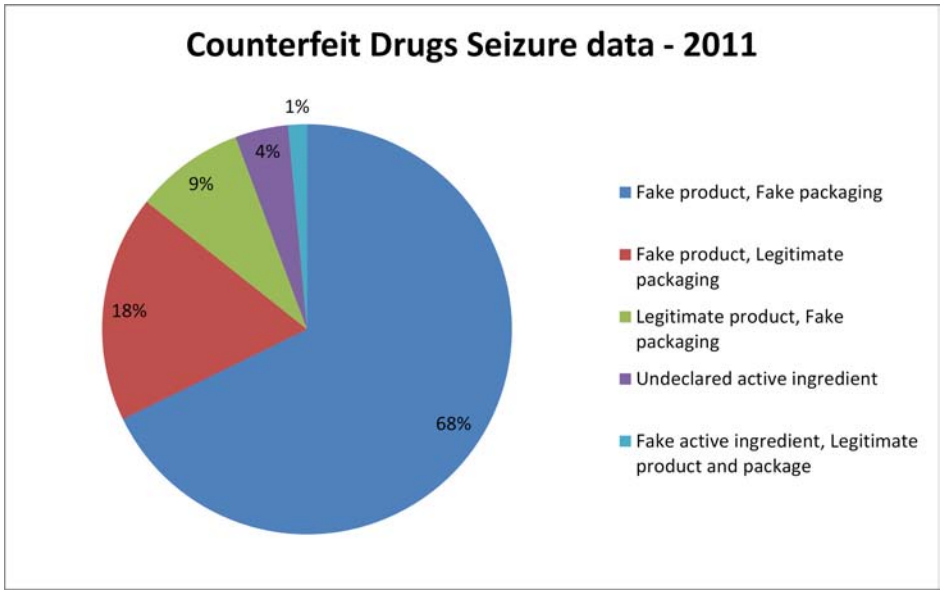


Figure 7.1: Types of counterfeiting seen in medicines, data from 2011. Source: [169]

To instantiate a r-PUF on the tablet surface, the micro-particles should be certified for consumption by relevant regulatory agencies. The micro-particles that was used in r-PUF do not fit this bill and hence efforts were made to search for alternatives. It was reported that there exists a possibility for obtaining micro-particles which would qualify for embedding into tablets but they would be much smaller ($\sim 1 - 3\mu m$) that the ones used currently. This increases the resolution requirements for imaging them. A series of macro-lenses were designed as an add-on for the mobile phone which could image at this resolution (Refer Appendix). This turned out to a classic 'chasing the tail' kind of an exercise where the design feasibility and requirements kept defining each other, eclipsing the application needs. At the moment there is no significant scientific outcome that is worth reporting.

The need for communication medium to verify authenticity is a burden in certain locations. If r-PUF could be integrated with an off-line verification technique in addition to existing capabilities, then the chances of technology adoption would be higher.

7.4 Summary

A new kind of PUF (r-PUF) was designed and implemented as a part of this dissertation. The entire work was carried out within the boundaries of a specific application - anti-counterfeiting. The motivation for a new security technique and requirements were built up from scratch after surveying the state of the art. PUF as a domain and its many implementations were studied and their applicability to anti-counterfeiting scenario was discussed. Experimental validation has been provided for the usability of the r-PUF in anti-counterfeiting application. Unclonability analysis was done by designing experiments where effect of system variables on final outcomes were tested.

List of Figures

List of Tables

Bibliography

[1] OECD. *Magnitude of counterfeiting and piracy of tangible products - an update*. Tech. rep. Organisation for Economic Co-operation and Development (OECD), 2009.

[2] ICCWBO. *Estimating the global economic and social impacts of counterfeiting and piracy*. Tech. rep. International chamber of commerce world business organisation, 2011.

[3] Auguste Kerckhoffs. "Desiderata de La cryptographie militaire". In: *Journal des sciences militaires* IX (1883), pp. 5–83.

[4] Fabien Petitcolas. *la cryptographie militaire*. 2012. URL: `http://www.petitcolas.net/fabien/kerckhoffs/index.html`.

[5] B. Schneier. *Applied cryptography: protocols, algorithms, and source code in C*. John Wiley & Sons Inc, 1996.

[6] O. Goldreich. "Foundations of cryptography: a primer". In: *Foundations and Trends® in Theoretical Computer Science* 1.1 (2005), pp. 1–116.

[7] R. Pappu et al. "Physical one-way functions". PhD thesis. 2003.

[8] R. Pappu et al. "Physical one-way functions". In: *Science* 297.5589 (2002), p. 2026.

[9] KM Tolk. *Reflective particle technology for identification of critical components*. Tech. rep. Sandia National Labs., Albuquerque, NM (United States), 1992.

[10] H. Busch et al. "The PUF promise". In: *Trust and Trustworthy Computing* (2010), pp. 290–297.

[11] A.R. Sadeghi and D. Naccache. *Towards Hardware-Intrinsic Security: Foundations and Practice*. Springer-Verlag New York Inc, 2010.

[12] Oded Goldreich. *Foundations of Cryptography: Volume 1, Basic Tools*. Vol. 1. Cambridge university press, 2003.

[13] O. Goldreich. "On the foundations of modern cryptography". In: *Advances in Cryptology-CRYPTO'97* (1997), pp. 46–74.

[14] U. Rührmair, J. Sölter, and F. Sehnke. *On the foundations of physical unclonable functions*. Tech. rep. Cryptology ePrint Archive, Report 2009/277, 2009.

[15] F. Armknecht et al. "A formal foundation for the security features of physical functions". In: *IEEE Symposium on Security and Privacy*. 2011, pp. 397–412.

[16] P. Tuyls et al. "Information-theoretic security analysis of physical uncloneable functions". In: *Financial Cryptography and Data Security* (2005), pp. 578–578.

[17] B.L.P. Gassend. "Physical random functions". MA thesis. Massachusetts Institute of Technology, 2003.

[18] U. Rührmair et al. “Modeling attacks on physical unclonable functions”. In: *Proceedings of the 17th ACM conference on Computer and communications security*. ACM. 2010, pp. 237–249.

[19] B. Gassend et al. “Silicon physical random functions”. In: *Proceedings of the 9th ACM conference on Computer and communications security*. ACM. 2002, pp. 148–160.

[20] J. Guajardo et al. “FPGA intrinsic PUFs and their use for IP protection”. In: *Cryptographic Hardware and Embedded Systems-CHES 2007* (2007), pp. 63–80.

[21] P. Tuyls et al. “Read-proof hardware from protective coatings”. In: *Cryptographic Hardware and Embedded Systems-CHES 2006* (2006), pp. 369–383.

[22] F. Beekhof et al. “Secure surface identification codes”. In: *Security, Forensics, Steganography, and Watermarking of Multimedia Contents X* (2008), pp. 27–31.

[23] U. Rührmair. “Oblivious transfer based on physical unclonable functions”. In: *Trust and Trustworthy Computing* (2010), pp. 430–440.

[24] U. Rührmair, H. Busch, and S. Katzenbeisser. “Strong PUFs: models, constructions, and security proofs”. In: *Towards Hardware-Intrinsic Security* (2010), pp. 79–96.

[25] Frederik Armknecht et al. “Memory leakage-resilient encryption based on physically unclonable functions”. In: *Advances in Cryptology–ASIACRYPT 2009*. Springer, 2009, pp. 685–702.

[26] Saloomeh Shariati, François Koeune, and François-Xavier Standaert. “Security Analysis of Image-based PUFs for Anti-Counterfeiting”. In: *Communications and Multimedia Security*. Springer. 2012, pp. 26–38.

[27] R. Plaga and F. Koob. “A formal definition and a new security mechanism of physical unclonable functions”. In: *Measurement, Modelling, and Evaluation of Computing Systems and Dependability and Fault Tolerance* (2012), pp. 288–301.

[28] C. Brzuska et al. “Physically uncloneable functions in the universal composition framework”. In: *Advances in Cryptology–CRYPTO 2011* (2011), pp. 51–70.

[29] R. Canetti. “Universally composable security: A new paradigm for cryptographic protocols”. In: *Foundations of Computer Science, 2001. Proceedings. 42nd IEEE Symposium on*. IEEE. 2001, pp. 136–145.

[30] Rafail Ostrovsky et al. *Universally composable secure computation with (malicious) physically uncloneable functions*. Tech. rep. Cryptology ePrint Archive, Report 2012/143, 2012.

[31] K.Y. Cheong. “A Survey of Cryptography Based on Physically Unclonable Objects”. In: (2011).

[32] R. Maes and I. Verbauwhede. *A Discussion on the Properties of Physically Unclonable Functions*. 2010.

[33] A. Maiti, V. Gunreddy, and P. Schaumont. “A systematic method to evaluate and compare the performance of physical unclonable functions”. In: *IACR ePrint* 657 (2011).

[34] Pim Tuyls and Boris Škorić. “Secret key generation from classical physics: Physical uncloneable functions”. In: *AmIware Hardware Technology Drivers of Ambient Intelligence*. Springer, 2006, pp. 421–447.

[35] J.H. Anderson. “A PUF design for secure FPGA-based embedded systems”. In: *Proceedings of the 2010 Asia and South Pacific Design Automation Conference*. IEEE Press. 2010, pp. 1–6.

[36] K. Shimizu, D. Suzuki, and T. Kasuya. “Glitch PUF: Extracting Information from Usually Unwanted Glitches”. In: *IEICE TRANSACTIONS on Fundamentals of Electronics, Communications and Computer Sciences* 95.1 (2012), pp. 223–233.

[37] U. Rührmair, S. Devadas, and F. Koushanfar. “Security based on physical unclonability and disorder”. In: *Introduction to Hardware Security and Trust* (2011).

[38] Alfred J Menezes, Paul C Van Oorschot, and Scott A Vanstone. *Handbook of applied cryptography*. CRC press, 2010.

[39] Anthony Van Herrewege et al. “Reverse fuzzy extractors: Enabling lightweight mutual authentication for PUF-enabled RFIDs”. In: *Financial Cryptography and Data Security*. Springer, 2012, pp. 374–389.

[40] Y. Dodis et al. “Fuzzy extractors: How to generate strong keys from biometrics and other noisy data”. In: *SIAM Journal on Computing* 38.1 (2008), pp. 97–139.

[41] S. Voloshynovskiy et al. “Unclonable identification and authentication based on reference list decoding”. In: *Proceedings of the conference on Secure Component and System Identification*. 2008, pp. 17–18.

[42] C.N. Chong et al. “Anti-counterfeiting with a random pattern”. In: *Emerging Security Information, Systems and Technologies, 2008. SECURWARE’08. Second International Conference on*. IEEE. 2008, pp. 146–153.

[43] J. Guajardo et al. “Anti-counterfeiting, key distribution, and key storage in an ambient world via physical unclonable functions”. In: *Information Systems Frontiers* 11.1 (2009), pp. 19–41.

[44] B. Škorić, P. Tuyls, and W. Ophey. “Robust key extraction from physical uncloneable functions”. In: *Applied Cryptography and Network Security*. Springer. 2005, pp. 99–135.

[45] D. Lim et al. “Extracting secret keys from integrated circuits”. In: *Very Large Scale Integration (VLSI) Systems, IEEE Transactions on* 13.10 (2005), pp. 1200–1205.

[46] G.E. Suh and S. Devadas. “Physical unclonable functions for device authentication and secret key generation”. In: *Proceedings of the 44th annual Design Automation Conference*. ACM. 2007, pp. 9–14.

[47] P. Tuyls and B. Škorić. “Strong authentication with physical unclonable functions”. In: *Security, Privacy, and Trust in Modern Data Management* (2007), pp. 133–148.

[48] H. Busch, S. Katzenbeisser, and P. Baecher. “PUF-Based Authentication Protocols–Revisited”. In: *Information Security Applications* (2009), pp. 296–308.

[49] J. Guajardo et al. “Brand and IP protection with physical unclonable functions”. In: *Circuits and Systems, 2008. ISCAS 2008. IEEE International Symposium on*. IEEE. 2008, pp. 3186–3189.

[50] K. Frikken, M. Blanton, and M. Atallah. “Robust authentication using physically unclonable functions”. In: *Information Security* (2009), pp. 262–277.

[51] T. Moran and M. Naor. “Basing cryptographic protocols on tamper-evident seals”. In: *Automata, Languages and Programming* (2005), pp. 61–61.

[52] Marten van Dijk and Ulrich Rührmair. *Physical Unclonable Functions in Cryptographic Protocols: Security Proofs and Impossibility Results*. Tech. rep. Cryptology ePrint Archive, Report 228/2012, 2012.

[53] Blaise Gassend et al. "Controlled physical random functions". In: *Computer Security Applications Conference, 2002. Proceedings. 18th Annual*. IEEE. 2002, pp. 149–160.

[54] Roarke Horstmeyer et al. "Physical key-protected one-time pad". In: *arXiv preprint arXiv:1305.3886* (2013).

[55] *EPCIS Standard v. 1.0.1*. 2007.

[56] D. Kügler. "On the anonymity of banknotes". In: *Privacy Enhancing Technologies*. Springer. 2005, pp. 786–789.

[57] GS1. *GS1 Overview*. URL: http://www.gs1.org/about/overview.

[58] Wikipedia. *EPC - Wikipedia*. URL: http://en.wikipedia.org/wiki/Electronic_Product_Code.

[59] P. Schmitt and F. Michahelles. "Status of RFID/EPC adoption". In: *AutoID Labs* (2009).

[60] A. Juels. "RFID security and privacy: A research survey". In: *Selected Areas in Communications, IEEE Journal on* 24.2 (2006), pp. 381–394.

[61] Wikipedia.org. *History of Barcodes*. URL: http://en.wikipedia.org/wiki/Barcode#History.

[62] Wikipedia. *Code 39 - Wikipedia*. URL: http://en.wikipedia.org/wiki/Code_39.

[63] Russ Adams. *A Short History Of Bar Code*. URL: http://www.adams1.com/history.html.

[64] GS1. *An Introduction to the Global Trade Item Number (GTIN)*. URL: http://www.gs1.org.

[65] Morovia. *PDF417 Specification*. URL: http://www.morovia.com/education/symbology/pdf417.asp.

[66] GS1. *GS1 DataMatrix - An introduction and technical overview of the most advanced GS1 Application Identifiers compliant symbology*. URL: http://www.gs1.org.

[67] DensoWave. *QR code*. URL: http://www.qrcode.com/en/qrfeature.html.

[68] Wikipedia. *Aztec Code - Wikipedia*. URL: http://en.wikipedia.org/wiki/Aztec_Code.

[69] Scanbuy. *EZ code*. URL: http://www.scanbuy.com/web/index.php?option=com_content&view=article&id=55&Itemid=15.

[70] Microsoft. *Tag Barcodes*. URL: http://tag.microsoft.com/home.aspx.

[71] J.D.R. Buchanan et al. "Forgery: fingerprinting documents and packaging". In: *Nature* 436.7050 (2005), pp. 475–475.

[72] J. Brosow and E. Furugard. "Method and a system for verifying authenticity safe against forgery". Pat. US Patent 4,218,674. 1980.

[73] R.N. Goldman. "Verification system for document substance and content". Pat. US Patent 4,689,477. 1987.

[74] T. Tel. "System and method of verifying the legitimacy of a product against forgery". Pat. US Patent 5,719,939. 1998.

[75] S. Denenberg et al. “System for verification of unique items”. Pat. US Patent 5,673,338. 1997.

[76] E. Metois et al. “FiberFingerprint identification”. In: *Proc. 3rd Workshop on Automatic Identification*. 2002, pp. 147–154.

[77] E. Kee and H. Farid. “Printer profiling for forensics and ballistics”. In: *Proceedings of the 10th ACM workshop on Multimedia and security*. ACM. 2008, pp. 3–10.

[78] B. Zhu, J. Wu, and M.S. Kankanhalli. “Print signatures for document authentication”. In: *Proceedings of the 10th ACM conference on Computer and communications security*. ACM. 2003, pp. 145–154.

[79] I. Amidror. “A new print-based security strategy for the protection of valuable documents and products using moire intensity profiles”. In: *Proc. SPIE: Optical Security and Counterfeit Deterrence Technique IV* 4677 (2002), pp. 89–100.

[80] S.F. Johnston. “Reconstructing the history of holography”. In: *Electronic Imaging 2003*. International Society for Optics and Photonics. 2003, pp. 455–464.

[81] Rudolf L. van Renesse. “A Review of Holograms and other Microstructures as Security Features”. In: *Holography, The first 50 years*. Springer series in Optical Sciences Vol.78, Springer Verlag(2003), 2003.

[82] Wilhelm Stork. “OPTICALLY DIFFRACTIVE STRUCTURE”. Pat. EP0826191. 2002. URL: `http://www.freepatentsonline.com/EP0826191B1.html`.

[83] Wilhelm Stork. “STRUCTURAL ARRANGEMENT, ESPECIALLY FOR A SECURITY COMPONENT”. Pat. EP0785874. 1998. URL: `http://www.freepatentsonline.com/EP0785874B1.html`.

[84] Wilhelm Stork. “Beugungsoptisch wirksame Strukturanordnung”. Pat. DE19516741. 1997. URL: `http://www.freepatentsonline.com/DE19516741.html`.

[85] T. Ignatenko et al. “Estimating the secrecy-rate of physical unclonable functions with the context-tree weighting method”. In: *Information Theory, 2006 IEEE International Symposium on*. IEEE. 2006, pp. 499–503.

[86] B.. Škorić et al. “Information-theoretic analysis of capacitive physical unclonable functions”. In: *Journal of Applied physics* 100.2 (2006), pp. 024902–024902.

[87] D. Lim. “Extracting secret keys from Integrated Circuits”. MA thesis. Massachussets Institute of Technology, 2004.

[88] Jae W. Lee et al. “A technique to build a secret key in integrated circuits with identification and authentication applications”. In: *In Proceedings of the IEEE VLSI Circuits Symposium*. 2004, pp. 176–179.

[89] L. Lin et al. “Low-power sub-threshold design of secure physical unclonable functions”. In: *Low-Power Electronics and Design (ISLPED), 2010 ACM/IEEE International Symposium on*. IEEE. 2010, pp. 43–48.

[90] B. Gassend et al. “Identification and authentication of integrated circuits”. In: *Concurrency and Computation: Practice and Experience* 16.11 (2004), pp. 1077–1098.

[91] M. Majzoobi, F. Koushanfar, and M. Potkonjak. “Techniques for design and implementation of secure reconfigurable PUFs”. In: *ACM Transactions on Reconfigurable Technology and Systems (TRETS)* 2.1 (2009), p. 5.

[92] Y. Lao and K.K. Parhi. “Reconfigurable architectures for silicon Physical Unclonable Functions”. In: *Electro/Information Technology (EIT), 2011 IEEE International Conference on*. IEEE. 2011, pp. 1–7.

[93] FlyLogic Inc. *Flylogic Blog*. URL: `http://www.flylogic.net/blog/`.

[94] S. Shariati et al. “Random profiles of laser marks”. In: *WIC Symposium on Information Theory in the Benelux*. 2010, pp. 27–34.

[95] S. Shariati et al. “Analysis and Experimental Evaluation of Image-based PUFs”. In: *Journal of Cryptographic Engineering* 2 (2012). DOI: `10.1007/s13389-012-0041-3`.

[96] J.G. Daugman. “Complete discrete 2-D Gabor transforms by neural networks for image analysis and compression”. In: *Acoustics, Speech and Signal Processing, IEEE Transactions on* 36.7 (1988), pp. 1169–1179.

[97] A. Sharma, L. Subramanian, and E.A. Brewer. “PaperSpeckle: microscopic fingerprinting of paper”. In: *Proceedings of the 18th ACM conference on Computer and communications security*. ACM. 2011, pp. 99–110.

[98] MagnetPrint. *Magnet Fingerprint*. URL: `http://www.magneprint.com`.

[99] R.S. Indeck, M.W. Muller, and R.E. Morley Jr. “Method and apparatus for fingerprinting and authenticating various magnetic media”. Pat. US Patent 5,920,628. 1999.

[100] D.E. Holcomb, W.P. Burleson, and K. Fu. “Initial SRAM state as a fingerprint and source of true random numbers for RFID tags”. In: *Proceedings of the Conference on RFID Security*. Vol. 7. 2007.

[101] D.E. Holcomb, W.P. Burleson, and K. Fu. “Power-up SRAM state as an identifying fingerprint and source of true random numbers”. In: *Computers, IEEE Transactions on* 58.9 (2009), pp. 1198–1210.

[102] G. Selimis et al. “Evaluation of 90nm 6T-SRAM as Physical Unclonable Function for secure key generation in wireless sensor nodes”. In: *Circuits and Systems (ISCAS), 2011 IEEE International Symposium on*. IEEE. 2011, pp. 567–570.

[103] H. Fujiwara et al. “A Chip-ID generating circuit for dependable LSI using random address errors on embedded SRAM and on-chip memory BIST”. In: *VLSI Circuits (VLSIC), 2011 Symposium on*. IEEE. 2011, pp. 76–77.

[104] A. Krishna et al. “MECCA: a robust low-overhead PUF using embedded memory array”. In: *Cryptographic Hardware and Embedded Systems–CHES 2011* (2011), pp. 407–420.

[105] S.S. Kumar et al. “The butterfly PUF protecting IP on every FPGA”. In: *Hardware-Oriented Security and Trust, 2008. HOST 2008. IEEE International Workshop on*. IEEE. 2008, pp. 67–70.

[106] R. Helinski, D. Acharyya, and J. Plusquellic. “A physical unclonable function defined using power distribution system equivalent resistance variations”. In: *Design Automation Conference, 2009. DAC’09. 46th ACM/IEEE*. IEEE. 2009, pp. 676–681.

[107] A. Maiti and P. Schaumont. “Improving the quality of a physical unclonable function using configurable ring oscillators”. In: *Field Programmable Logic and Applications, 2009. FPL 2009. International Conference on*. IEEE. 2009, pp. 703–707.

[108] A. Maiti and P. Schaumont. “Improved ring oscillator PUF: an FPGA-friendly secure primitive”. In: *Journal of cryptology* 24.2 (2011), pp. 375–397.

[109] A. Maiti et al. “A large scale characterization of RO-PUF”. In: *Hardware-Oriented Security and Trust (HOST), 2010 IEEE International Symposium on*. IEEE. 2010, pp. 94–99.

[110] A. Maiti, I. Kim, and P. Schaumont. “A Robust Physical Unclonable Function With Enhanced Challenge-Response Set”. In: *Information Forensics and Security, IEEE Transactions on* 7.1 (2012), pp. 333–345.

[111] C.E.D. Yin and G. Qu. “LISA: Maximizing RO PUF’s secret extraction”. In: *Hardware-Oriented Security and Trust (HOST), 2010 IEEE International Symposium on*. IEEE. 2010, pp. 100–105.

[112] C.E. Yin. “A group-based ring oscillator physical unclonable function”. PhD thesis. UNIVERSITY OF MARYLAND, COLLEGE PARK, 2012.

[113] D. Merli, F. Stumpf, and C. Eckert. “Improving the quality of ring oscillator PUFs on FPGAs”. In: *Proceedings of the 5th Workshop on Embedded Systems Security*. ACM. 2010, p. 9.

[114] Q. Chen et al. “The bistable ring puf: A new architecture for strong physical unclonable functions”. In: *Hardware-Oriented Security and Trust (HOST), 2011 IEEE International Symposium on*. IEEE. 2011, pp. 134–141.

[115] G. Dejean and D. Kirovski. “RF-DNA: Radio-frequency certificates of authenticity”. In: *Cryptographic Hardware and Embedded Systems-CHES 2007* (2007), pp. 346–363.

[116] G. DeJean and D. Kirovski. “Radio frequency certificates of authenticity”. Pat. US Patent 7,677,438. 2010.

[117] D. Suzuki and K. Shimizu. “The glitch PUF: a new delay-PUF architecture exploiting glitch shapes”. In: *Cryptographic Hardware and Embedded Systems, CHES 2010* (2010), pp. 366–382.

[118] K. Lofstrom, W.R. Daasch, and D. Taylor. “IC identification circuit using device mismatch”. In: *Solid-State Circuits Conference, 2000. Digest of Technical Papers. ISSCC. 2000 IEEE International*. IEEE. 2000, pp. 372–373.

[119] Y. Su, J. Holleman, and B. Otis. “A 1.6 pJ/bit 96process variations”. In: *Solid-State Circuits Conference, 2007. ISSCC 2007. Digest of Technical Papers. IEEE International*. IEEE. 2007, pp. 406–611.

[120] Y. Su, J. Holleman, and B.P. Otis. “A digital 1.6 pJ/bit chip identification circuit using process variations”. In: *Solid-State Circuits, IEEE Journal of* 43.1 (2008), pp. 69–77.

[121] R. Maes, P. Tuyls, and I. Verbauwhede. “Intrinsic PUFs from flip-flops on reconfigurable devices”. In: *3rd Benelux workshop on information and system security (WISSec 2008)*. Vol. 17. 2008.

[122] V. van der Leest et al. “Hardware intrinsic security from D flip-flops”. In: *Proceedings of the fifth ACM workshop on Scalable trusted computing*. ACM. 2010, pp. 53–62.

[123] P. Simons, E. van der Sluis, and V. van der Leest. “Buskeeper PUFs, a promising alternative to D Flip-Flop PUFs”. In: *Hardware-Oriented Security and Trust (HOST), 2012 IEEE International Symposium on*. IEEE. 2012, pp. 7–12.

[124] U. Rührmair et al. “Applications of high-capacity crossbar memories in cryptography”. In: *Nanotechnology, IEEE Transactions on* 10.3 (2011), pp. 489–498.

[125] U. Rührmair et al. “Security applications of diodes with unique current-voltage characteristics”. In: *Financial Cryptography and Data Security* (2010), pp. 328–335.

[126] Roel Maes. “Physically Unclonable Functions: Constructions, Properties and Applications”. PhD thesis. Arenberg Doctoral School of Science, Katholieke Universiteit Leuven., 2012.

[127] S. Vrijaldenhoven. “Acoustical Physical Uncloneable Functions”. MA thesis. Technische Universiteit Eindhoven, 2005.

[128] Aravind K Mikkilineni et al. “Signature-embedding in printed documents for security and forensic applications”. In: *Electronic Imaging 2004*. International Society for Optics and Photonics. 2004, pp. 455–466.

[129] N. Biermann and H. Rauhe. “METHOD FOR PRODUCING SECURITY MARKINGS”. Pat. WO/2004/070667. 2004. URL: www.wipo.int/patentscope/search/en/WO2004070667.

[130] Nils Biermann. “Sicherheitskennzeichnung”. DE. Pat. DE102008015466. 2009.

[131] Wilhelm Stork and Heinrich Wild. “METHOD OF PRODUCING PRINTING OR EMBOSSING CYLINDERS HAVING A PATTERNED SURFACE”. Pat. EP0904569. 2000. URL: http://www.freepatentsonline.com/EP0904569B1.html.

[132] BMBF. *HandyProve - BMBF report*. 2010. URL: http://www.pt-it.pt-dlr.de/_media/Infoblatt_HandyProve.pdf.

[133] John Oliver and Joyce Chen. “Use of signature analysis to discriminate digital printing technologies”. In: *International Conference on Digital Printing Technologies*. 2002, pp. 218–222.

[134] Pei-Ju Chiang et al. “Printer and scanner forensics”. In: *Signal Processing Magazine, IEEE* 26.2 (2009), pp. 72–83.

[135] Helmut Kipphan. *Handbook of print media: technologies and production methods*. Springer, 2001.

[136] Stephen Pollard, Steven Simske, and Guy Adams. “Print biometrics: Recovering forensic signatures from halftone images”. In: *Pattern Recognition (ICPR), 2012 21st International Conference on*. IEEE. 2012, pp. 1651–1654.

[137] Y. Dodis, L. Reyzin, and A. Smith. “Fuzzy extractors: How to generate strong keys from biometrics and other noisy data”. In: *Advances in cryptology-Eurocrypt 2004*. Springer. 2004, pp. 523–540.

[138] Joppe W Bos et al. “On the Security of 1024-bit RSA and 160-bit Elliptic Curve Cryptography”. In: *ePrint Archive for Int. Assc. for Cryptologic Research* (2009).

[139] Emmanuel ThomÃl’ Arjen K. Lenstra Thorsten Kleinjung. “Universal security; from bits and mips to pools, lakes – and beyond”. In: (2013). URL: http://eprint.iacr.org/.

[140] Jukka-Tapani Mäkinen et al. “Inmould integration of a microscope add-on system to a 1.3 Mpix camera phone”. In: *International Congress on Optics and Optoelectronics*. International Society for Optics and Photonics. 2007, pp. 658507–658507.

[141] Keeploop. *KeepLoop. Microscope for mobile*. 2012. URL: http://www.keeploop.com/.

[142] Guy Adams. "Hand held Dyson relay lens for anti-counterfeiting". In: *Imaging Systems and Techniques (IST), 2010 IEEE International Conference on*. IEEE. 2010, pp. 273–278.

[143] John H McLeod. "The axicon: a new type of optical element". In: *JOSA* 44.8 (1954), pp. 592–592.

[144] Adil Haouzia and Rita Noumeir. "Methods for image authentication: a survey". In: *Multimedia Tools and Applications* 39 (1 2008). 10.1007/s11042-007-0154-3, pp. 1–46. ISSN: 1380-7501. URL: http://dx.doi.org/10.1007/s11042-007-0154-3.

[145] David Marr and Ellen Hildreth. "Theory of edge detection". In: *Proceedings of the Royal Society of London. Series B. Biological Sciences* 207.1167 (1980), pp. 187–217.

[146] V. Monga. "Perceptually based methods for robust image hashing". PhD thesis. Faculty of the Graduate School of The University of Texas at Austin, 2005. URL: http://repositories.lib.utexas.edu/bitstream/handle/2152/2001/mongav59809.pdf?sequence=2.

[147] Brahim Ait Es Said Azhar Hadmi William Puech and Abdellah Ait Ouahman. *Perceptual Image Hashing*. Ed. by Mithun Das Gupta. Vol. 2. Watermarking. InTech, 2012. URL: http://www.intechopen.com/books/watermarking-volume-2/perceptual-image-hashing.

[148] Marc Schneider and Shih-Fu Chang. "A robust content based digital signature for image authentication". In: *Image Processing, 1996. Proceedings., International Conference on*. Vol. 3. IEEE. 1996, pp. 227–230.

[149] R. Venkatesan et al. "Robust image hashing". In: 3 (2000), 664 –666 vol.3. DOI: 10.1109/ICIP.2000.899541. URL: http://dx.doi.org/10.1109/ICIP.2000.899541.

[150] Ching-Yung Lin and Shih-Fu Chang. "Generating robust digital signature for image/video authentication". In: *Multimedia and Security Workshop at ACM Multimedia*. Vol. 98. Citeseer. 1998, pp. 94–108.

[151] Ching-Yung Lin and Shih-Fu Chang. "A robust image authentication method distinguishing JPEG compression from malicious manipulation". In: *Circuits and Systems for Video Technology, IEEE Transactions on* 11.2 (2001), pp. 153–168.

[152] Chun-Shien Lu and H-YM Liao. "Structural digital signature for image authentication: an incidental distortion resistant scheme". In: *Multimedia, IEEE Transactions on* 5.2 (2003), pp. 161–173.

[153] Jiri Fridrich and Miroslav Goljan. "Robust hash functions for digital watermarking". In: *Information Technology: Coding and Computing, 2000. Proceedings. International Conference on*. IEEE. 2000, pp. 178–183.

[154] S.S. Kozat, R. Venkatesan, and M.K. Mihcak. "Robust perceptual image hashing via matrix invariants". In: 5 (2004), 3443 –3446 Vol. 5. ISSN: 1522-4880. DOI: 10.1109/ICIP.2004.1421855. URL: http://dx.doi.org/10.1109/ICIP.2004.1421855.

[155] M Kıvanç Mıhçak and Ramarathnam Venkatesan. "New iterative geometric methods for robust perceptual image hashing". In: *Security and privacy in digital rights management*. Springer, 2002, pp. 13–21.

[156] V. Monga and B.L. Evans. “Robust perceptual image hashing using feature points”. In: *Image Processing, 2004. ICIP ’04. 2004 International Conference on*. Vol. 1. 2004, 677–680 Vol. 1. DOI: 10.1109/ICIP.2004.1418845.

[157] V. Monga and B.L. Evans. “Perceptual Image Hashing Via Feature Points: Performance Evaluation and Tradeoffs”. In: *Image Processing, IEEE Transactions on* 15.11 (2006), pp. 3452 –3465. ISSN: 1057-7149. DOI: 10.1109/TIP.2006.881948. URL: http://dx.doi.org/10.1109/TIP.2006.881948.

[158] A. Swaminathan, Y. Mao, and M. Wu. “Robust and secure image hashing”. In: *Information Forensics and Security, IEEE Transactions on* 1.2 (2006), pp. 215–230.

[159] Frédéric Lefebvre, Benoit Macq, and Jean-Didier Legat. “RASH: Radon soft hash algorithm”. In: *Proceedings of EUSIPCO-European Signal Processing Conference*. 2002.

[160] D. Guo X.C. und Hatzinakos. “Content Based Image Hashing Via Wavelet and Radon Transform”. In: *Lecture Notes in Computer Science* 4810.2007 (2007), pp. 755–764. DOI: 10.1007/978-3-540-77255-2_91. URL: http://dx.doi.org/10.1007/978-3-540-77255-2_91.

[161] F. Ahmed, MY Siyal, and V. Uddin Abbas. “A secure and robust hash-based scheme for image authentication”. In: *Signal Processing* 90.5 (2010), pp. 1456–1470.

[162] Wikipedia.org. *Blob detection*. URL: http://en.wikipedia.org/wiki/Blob_detection.

[163] Christophe Damerval and Sylvain Meignen. “Blob detection with wavelet maxima lines”. In: *Signal Processing Letters, IEEE* 14.1 (2007), pp. 39–42.

[164] John G Daugman et al. “Uncertainty relation for resolution in space, spatial frequency, and orientation optimized by two-dimensional visual cortical filters”. In: *Optical Society of America, Journal, A: Optics and Image Science* 2.7 (1985), pp. 1160–1169.

[165] D Gabor. “Theory of communication”. In: *J. of the Institute of Electrical Engineers Part III* 93 (1946), pp. 429–457.

[166] John G Daugman. “Biometric personal identification system based on iris analysis”. Pat. US Patent 5,291,560. 1994.

[167] Javier R Movellan. *Tutorial on Gabor filters*. In: 2002.

[168] O. Nestares et al. “Efficient spatial-domain implementation of a multiscale image representation based on Gabor functions”. In: *Journal of Electronic Imaging* 7.1 (1998), pp. 166–173.

[169] Committee on Understanding the Global Public Health Implications of Substandard Falsified and Counterfeit Medical Products. *Countering the Problem of Falsified and Substandard Drugs*. Ed. by Lawrence O. Gostin. Ed. by Gillian J. Buckley. Board on Global Health; Institute of Medicine. The National Academies Press, 2013. ISBN: 9780309269391. URL: http://www.nap.edu/openbook.php?record_id=18272.

Supervised Student Research

[1] Andreas Bohn. “Integration statisher Thorax-MRT-Aufnahmen und dynamischer Cardio-MRT-Aufnahmen mit Hilfe zeitlich veränderlicher, nicht rigider Abbildungen”. Diploma thesis, ID-1622. Trimesh Simulations GmbH, Karlsruhe: Institut für Technik der Informationsverarbeitung (ITIV), Karlsruhe Institute of Technology, 2012.

[2] Leyre Medina. “Algorithms for Image Recognition using Blob Analysis”. Bachelor thesis, ID-871. Institut für Technik der Informationsverarbeitung (ITIV), Karlsruhe Institute of Technology, 2009.

[3] Mortada Mouazzen. “Development of a test platform for HandyProve”. Diploma thesis, ID-1515. Institut für Technik der Informationsverarbeitung (ITIV), Karlsruhe Institute of Technology, 2012.

[4] Andres Arriaga Perez. “Development of hashing algorithms for PUF verification”. Bachelor thesis, ID-1680. Institut für Technik der Informationsverarbeitung (ITIV), Karlsruhe Institute of Technology, 2013.

[5] Max Sirkin. “Vermessung einer Gesichsoberfläche mit Hilfe einer Low Cost kamera zur Resistrierung eines dreidimensionalen Gesichtsdatensatzes”. Diploma thesis, ID-1630. Stryker Leibinger GmbH, Freiburg: Institut für Technik der Informationsverarbeitung (ITIV), Karlsruhe Institute of Technology, 2012.

[6] Jia Ye. “Entwicklung einer HW/SW Plattform fü den Einsatz in Add-on Anwendungen auf dem Handy”. Diploma thesis, ID-1517. Institut für Technik der Informationsverarbeitung (ITIV), Karlsruhe Institute of Technology, 2012.

Publications

[1] *Fast scan-fail device for class 1 operation of scanning micromirrors at a high laser power in the near-infrared region*. Vol. 8512. 2012, 85120E–85120E–9. DOI: 10.1117/12.929717. URL: http://dx.doi.org/10.1117/12.929717.

[2] Stiftungslabor für Grundlagenforschung, Tübingen Universitäts-Augenklinik, and Sektion Experimentelle Ophthalmo-Chirurgie. "Optimierung von Strom-und Beleuchtungsquelle des indirekten binokularen Brillenophthalmoskops nach Foerster". In: *Klin Monatsbl Augenheilkd* 230.8 (2013), pp. 825–828.

[3] *Thermodynamic finite-element-method (FEM) eye model for laser safety considerations*. Vol. 8579. 2013, 85790J–85790J–8. DOI: 10.1117/12.2004594. URL: http://dx.doi.org/10.1117/12.2004594.

[4] *A coherent laser Doppler wind profiler for the active control of wind turbines*. Vol. 8235. 2012, pp. 823519–823519–12. DOI: 10.1117/12.908759. URL: http://dx.doi.org/10.1117/12.908759.

[5] *A simulation environment for assisting system design of coherent laser doppler wind sensor for active wind turbine pitch control*. Vol. 8789. 2013, pp. 87890V–87890V–10. DOI: 10.1117/12.2020594. URL: http://dx.doi.org/10.1117/12.2020594.

[6] H. Umesh Babu, W. Stork, and H. Rauhe. "Anti-counterfeiting using reflective micro structures-Based on random positioning of microstructures". In: *Advances in Optoelectronics and Micro/Nano-Optics (AOM), 2010 OSA-IEEE-COS*. IEEE. 2010, pp. 1–5.