Karlsruhe Institute of Technology

Key Exchange at the Physical Layer

zur Erlangung des akademischen Grades eines

Doktors der Ingenieurwissenschaften

der Fakultät für Informatik
des Karlsruher Instituts für Technologie (KIT)

genehmigte

Dissertation

von

Antonio Pedro Sobreira de Almeida

aus Porto, Portugal

Tag der mündlichen Prüfung:	10. Juli 2015
Erster Gutachter:	Prof. Dr. Jörn Müller-Quade
Zweiter Gutachter:	Prof. Dr. Ralf Reussner

Ich versichere wahrheitsgemäß, diese Dissertation bis auf die angegebenen Hilfen selbstständig angefertigt, alle benutzten Hilfsmittel vollständig und genau angegeben und als kenntlich gemacht zu haben, was aus Arbeiten anderer und eigenen Veröffentlichungen unverändert oder mit Änderungen entnommen wurde.

Karlsruhe, 21. Mai 2015

Antonio Sobreira de Almeida

Acknowledgements

Several people have contributed in many different and valuable ways to the conclusion of this work. First and foremost, I would thank my research advisor, Prof. Dr. Jörn Müller-Quade, whose guidance was of utmost importance during all my happy years at the Institute of Cryptography and Security. Under his supervision, I was able to learn many aspects of cryptography, including various methodologies for dealing with interesting problems. Our conversations about a large variety of subjects have given me a good amount of knowledge and many entertaining hours. I would also like to offer my gratitude to Prof. Dr. Ralf Reussner, who took interest in my research and accepted to co-referee this thesis.

I am truly indebted to Prof. Dejan Lazich. With his precious support, I was able to dig into the essence, mysteries and beauty of cryptographic hardware, where a small detail can make a big difference. His large expertise and insights on how to analyze the hardware in detail was of paramount importance during the experimental part of this work. I will certainly never forget the experience of our participation in the 2008/09 DPA Contest. We spent countless hours on trying to find out a better way of performing a more efficient DPA attack. We started late, but we still made it into the top 13. If there had been an award for the team who had the most fun, we surely would have received it.

I owe a special thanks to all my colleagues at the Institute. In particular, I want to thank Bernhard Löwe, my office roommate, for his friendship and continuous support. His skills with photography and digital drawing were always of great value for my work. I also want to thank Brandon Broadnax for carefully proofreading several chapters, as well as for our healthy jogging afternoon sessions. Year after year, we became older but never slower.

I would also like to thank *Fundação para a Ciência e Tecnologia*, which financially supported me through the first years of my PhD studies under the PhD Grant *SFRH/BD/27858/2006*.

Last, but by no means the least, I am infinitely grateful to all of those who, either close or far away, were always there for me.

Abstract

At its core, cryptography is focused on establishing secret communication between two parties. Traditionally, this goal required both legal parties to share some kind of common information which had to be kept secret from an eavesdropper - the so-called *private key*. One major problem consists of finding a way to generate and establish a shared secret key between two parties without the availability of a secure channel. One can tackle this problem using established key exchange methods. Techniques from public-key cryptography can be employed to solve this problem. Still, they rely on unproven assumptions, namely the problem of $\mathcal{NP} \neq \mathcal{P}$. Moreover, these methods are strongly time and energy consuming, which can be critical for low-energy applications, such as wireless sensor networks. One of the most promising techniques for the key exchange problem makes use of the properties of the physical layer, namely of the wireless channel. In this approach, emitted radio signals are scattered and reflected from various physical obstacles such as cars, buildings, trees, and many others. Thus, a receiver will receive the original signal superposed with several echoes caused by reflections, as stated by the multipath interference property. The reciprocity property of the channel ensures that both parties receive the same echo pattern when the exchange is performed fast enough. The shared randomness therefore results from unknown and dynamic electromagnetic characteristics of the common physical environment. This method also contributes to avoid a mass surveillance scenario, as, for this purpose, an attacker would have to be continuously able to reproduce this protocol between the communicating parties exactly at the same time they perform it, which requires physical presence. In this thesis, we consider key exchange at the physical layer in the following three aspects:

Vulnerabilities and Attacks. The conditions under which this method is secure are not totally clear. What if the environment is too simple, e.g. a desert, where the entropy is almost non-existent? Are there any kind of side-channel attacks against this method, i.e. attacks based on the physical properties of the device or on implementation details? We demonstrate that indeed this protocol is not totally secure if the environment is too simple and propose an attack called *environment reconstruction attack*. We thereby draw attention to an aspect of reciprocity-based key exchange that has so far been neglected. More precisely, we provide a model scenario for fading channels in which a passive eavesdropping adversary can reconstruct a key

generated by the protocol parties. Furthermore, we present a side-channel attack against the implementation. This attack is based on the fact that antennas reradiate all the signals they receive. We called this attack the *reradiation leakage attack*. We develop an exhaustive analysis and we characterize the conditions under which this attack can be mounted. Upper theoretical bounds for the feasibility of this attack are derived. We experimentally validated this attack.

Improvements to the Protocol. We explain how we can *extend the source of entropy to the hardware* using the example of a direct-conversion receiver. For this purpose, we utilize the properties of some hardware components, namely those of the transceivers' local oscillators, as an additional source of randomness shared by the legitimate parties. Reciprocity will still hold, allowing shared key extraction. This method has the additional advantage of being more resistant to the reradiation leakage side-channel attack on reciprocity-based wireless key exchange. Simulation results that seek to validate our new protocol are presented.

Experimental Validation. We developed a prototype which served as a *proof-of-concept* for this method and experimentally validated our novel protocol. Several experiments under different environments were performed in order to prove the feasibility of this method. Our studies also address some limitations and propose solutions.

Zusammenfassung

Im Kern der Kryptographie steht die sichere Kommunikation zwischen zwei Parteien. Für gewöhnlich kann dieses Ziel erreicht werden, indem ein sogenannter *geheimer Schlüssel* zwischen beiden Kommunikationspartnern geteilt wird. Etwaigen Mithörern ist dieser jedoch unbekannt. Eines der Hauptprobleme besteht darin, den Schlüssel ohne einen sicheren Kanal zu generieren und zwischen beiden Parteien zu teilen. Verschiedene Methoden im Rahmen der Public-Key-Kryptographie können zur Lösung dieses Problems Anwendung finden. Diese beruht jedoch auf einigen unbewiesenen Annahmen, wie dem $\mathcal{NP} \neq \mathcal{P}$-Problem. Ein Nachteil dieser Methoden ist zudem der hohe Aufwand an Energie und Zeit, welcher besonders bei Anwendungen mit geringem Energieverbrauch, wie etwa drahtlosen Netzwerken, kritisch zu bewerten ist. Eines der erfolgversprechendsten Verfahren zum Teilen eines kryptographischen Schlüssels beruht auf den Eigenschaften der physikalischen Schicht, genauer gesagt dem drahtlosen Kanal. In diesem Fall wird die ausgestrahlte Radiostrahlung an verschiedenen Hindernissen, wie etwa Autos, Gebäuden oder Bäumen, gestreut und reflektiert. Es kommt zur Überlagerung der Wellen, in deren Folge zusätzlich zum ursprünglich ausgesendeten Signal verschiedene Echos empfangen werden. Die Reziprozitätseigenschaft eines Kanals gewährleistet, dass beide Parteien dasselbe Muster des Echos empfangen, wenn der Austausch schnell genug abläuft. Die Zufälligkeit, mit der dieses Muster entsteht, resultiert aus der unbekannten und sich ständig ändernden physischen Umwelt. Diese Methode sorgt zudem dafür, dass ein Szenario der Massenüberwachung verhindert werden kann. Ein Angreifer müsste nämlich das Protokoll zwischen den beiden kommunizierenden Parteien kontinuierlich mithören, was seine physische Präsenz bedingen würde. In dieser Arbeit wird der Austausch eines kryptographischen Schlüssels über die physikalische Schicht hinsichtlich folgender drei Aspekte bewertet:

Verwundbarkeit und Angriffe. Die Bedingungen, unter denen diese Methode sicher ist, sind noch nicht vollkommen bekannt. Was passiert, wenn die Umgebung kaum Merkmale mit Informationsgehalt, wie es etwa in Wüsten der Fall ist, aufweist? Existieren Seitenkanalangriffe gegen diese Methode, beispielsweise Angriffe basierend auf den physikalischen Eigenschaften der Apparatur oder bei der Umsetzung? Es wird aufgezeigt, dass es tatsächlich keine hundertprozentige Sicherheit gibt, wenn die Umgebung zu einfach aufgebaut ist. Es wird ein Angriff auf das System model-

liert, der in diesem Zusammenhang als *environment reconstruction attack* bezeichnet werden soll. Dabei soll der Fokus auf einem Aspekt des wechselseitigen Austausches des Schlüssels liegen, welcher bislang vernachlässigt wurde. Konkret wird ein Szenario *fading Kanäle* modelliert, welches einem passiven Abhörer ermöglicht, den kryptographischen Schlüssel zwischen zwei kommunizierender Parteien nachzubilden. Des Weiteren wird ein Seitenkanalangriff unter der Bezeichnung *reradiation leakage attack* modelliert. Grundlage hierfür ist die Rückstrahlung der von Antennen empfangenen Signale. Es wurde eine gründliche Analysemethode entwickelt. Außerdem wurden die Bedingungen charakterisiert, unter denen ein solcher Angriff abläuft. Die Obergrenze für die Durchführbarkeit dieses Angriffs werden abgeleitet, eine experimentelle Durchführung soll zur Validierung dienen.

Fortschritte beim Protokoll. Es wird ausgeführt, wie man die Quellen der Entropie bis zur Hardware erweitern kann, indem beispielsweise ein Direktmischempfänger eingesetzt wird. Zu diesem Zweck werden Eigenschaften einiger Hardwarekomponenten, die *lokalen Oszillatoren* des Transceivers, eingesetzt, um weitere Zufälligkeiten bei der Kommunikation zweier autorisierter Kommunikationspartner zu erhalten. Die Reziprozitätseigenschaft bleibt erhalten, was die gemeinsame Schlüsselerzeugung ermöglicht. Die Anwendung dieser Strategie bietet einen zusätzlichen Vorteil, da die Verwundbarkeit gegenüber dem *reradiation leakage side-channel*-Angriff so geringer ist. Simulationen, welche die Funktionsfähigkeit des neu gestalteten Protokolls bestätigen, werden abschließend vorgestellt.

Experimentelle Validierung. Es wurde ein Prototyp entwickelt, welcher die theoretischen Überlegungen belegt und zur experimentellen Validierung des Protokolls dienen soll. Eine Vielzahl an Experimenten wurde in verschiedenen Umgebungen durchgeführt, um die Realisierbarkeit dieser Methode zu prüfen. Die Studie befasst sich außerdem mit verschiedenen Einschränkungen und schlägt Lösungsansätze vor.

Contents

Acknowledgements v

Abstract vii

Zusammenfassung ix

1. Introduction 1
- 1.1. General Aspects of Cryptography . . . 1
  - 1.1.1. Private-Key Cryptography . . . 2
  - 1.1.2. Public-Key Cryptography . . . 3
- 1.2. Motivation for Wireless Key Exchange . . . 4
- 1.3. Our Contribution . . . 6

2. Preliminaries 9
- 2.1. Antenna Theory . . . 9
  - 2.1.1. Antenna Radiation Pattern and Directivity . . . 9
  - 2.1.2. Antenna Reradiation . . . 10
    - 2.1.2.1. Transmitting Mode . . . 10
    - 2.1.2.2. Receiving Mode . . . 12
- 2.2. The Wireless Channel . . . 14
  - 2.2.1. Physical Models . . . 14
    - 2.2.1.1. Free Space Propagation and Fixed Antenna . . . 15
    - 2.2.1.2. Free Space Propagation and Moving Antenna . . . 16
    - 2.2.1.3. Reflecting Wall and Fixed Antenna . . . 17
    - 2.2.1.4. Reflecting Wall and Moving Antenna . . . 18
    - 2.2.1.5. Remarks . . . 19
  - 2.2.2. Channel as a Linear Time-Varying System . . . 19
  - 2.2.3. Important Parameters for Channel Characterization . . . 20
  - 2.2.4. Reciprocity Theorem . . . 22
- 2.3. Information Reconciliation and Privacy Amplification . . . 23

3. Related Work 25
- 3.1. Noise-based Methods . . . 25
- 3.2. Reciprocity-&-Fading-based Methods . . . 27
- 3.3. Antenna-based Methods . . . 34
  - 3.3.1. Time-Varying Radiation Pattern Antennas . . . 34
  - 3.3.2. Multiple Antennas . . . 37
- 3.4. Jamming-based Methods . . . 39
- 3.5. Device-based Methods . . . 40

3.6. Other Interesting Wireless Security Schemes and Applications 42

4. Vulnerabilities and Attacks 45
4.1. Environment Reconstruction Attacks 45
4.2. Side-Channel Attack: Reradiation Leakage 49
4.2.1. Theory 58
4.2.2. Experimental Setup 58
4.2.3. Hardware 58
4.2.4. Results 60
4.3. Discussion 60
4.4. Conclusion 61

5. Improvements to the Protocol 63
5.1. Based on Radiation Pattern 63
5.2. Based on Differences in the Local Oscillators 64
5.2.1. Channel 64
5.2.2. Hardware 65
5.2.2.1. Direct-Conversion Receivers 65
5.2.3. Basic Protocol 66
5.3. Key Extraction 67
5.3.1. Features Extraction 67
5.3.2. Quantizer 68
5.4. Simulation 69
5.4.1. Channel 69
5.4.2. Hardware 69
5.4.3. Protocol 69
5.4.4. Experiments 70
5.4.4.1. Experiment I 70
5.4.4.2. Experiment II 71
5.4.5. Key Agreement Rate 71
5.4.6. Results 71
5.5. Discussion 72
5.6. Conclusion 74

6. Experimental Validation 75
6.1. Hardware and Software 75
6.2. Experiment: Differences in the Frequencies 76
6.2.1. Location 76
6.2.1.1. Laboratory 76
6.2.1.2. Between Rooms 76
6.2.2. Results 78
6.2.2.1. Laboratory 78
6.2.2.2. Between Rooms 78
6.2.3. Discussion 79
6.3. Experiment: Key Exchange Evaluation 79
6.3.1. Protocol 79
6.3.2. Experimental Variables 81
6.3.2.1. Environments 81
6.3.2.2. Quantization Bits 87

6.3.2.3. Key Extractors 87
6.3.3. Quality Criteria 88
6.3.3.1. Key Agreement Rate (KAR) 89
6.3.3.2. Bit Generation Rate 89
6.3.3.3. Randomness - the NIST Statistical Test Suite 89
6.3.4. Results 91
6.3.4.1. Extractor Amplitudes (X) 93
6.3.4.2. Extractor Zeros (Z) 95
6.3.4.3. Extractor Product of Amplitudes and Zeros (XZ) . . 97
6.3.4.4. Extractor Square of Both ($(XZ)^2$) 99
6.3.4.5. Extractor Trimmed Mean (trm) 101
6.3.4.6. Extractor Division Amplitudes by Zeros (X/Z) . . . 103
6.3.5. Discussion 105
6.3.5.1. Dependency of KAR and Randomness on Q 105
6.3.5.2. Choice of the Extractor 105
6.3.5.3. Bit Generation Rate 106
6.3.5.4. Drawbacks 106
6.3.5.5. Other Observations 107
6.3.5.6. Strategy for a Practical Implementation 107
6.4. Conclusion 108

7. Conclusion **109**

A. Appendix **111**
A.1. Extractor XZ: Single Configuration 112
A.2. Extractor XZ: All Configurations 123

Bibliography **135**

1. Introduction

The modern world is inconceivable without considering the *security* of systems. The challenges of this new technological era have strongly increased the need for secure communications. Message secrecy has played a prominent role in historical events and helped to shape the world as it is today. It seems indisputable that this is becoming even more important in recent years and so will continue to be in the future.

The definition of cryptography is intrinsically connected with the notion of security, specifically the security of information systems. Nowadays, cryptography can be defined as the science concerned with the design and analysis of *secure information systems*, i.e. systems able to withstand any kinds of *manipulation attempts* [Gol00]. It is a broad discipline involving the knowledge of different fields, like mathematics, theoretical and applied informatics, even telecommunications engineering or, in very specific cases, quantum physics. Developing a holistic approach to the design of secure communication systems is by no means a trivial task.

In this chapter, we briefly give an overview of the main ideas of cryptography and introduce the scope of our research.

1.1. General Aspects of Cryptography

As in some other branches of science, cryptography progressed from a kind of art into a well established science which is part of the field of computer science. This process took a few centuries. Modern cryptography demands a rigorous treatment and clear *proofs of security*.

Originally, cryptography was more concerned with establishing secret communication between two parties. This goal required legal parties sharing secret information - the so called *private key*. This was the basic scenario of *private-key cryptography* (also called symmetric cryptography), which we will explain more in detail in Section 1.1.1. Nevertheless, this approach still presented a few drawbacks, namely the need of a different key for each two-party communication and a means for establishing a shared secret key between two parties via an untrusted channel.

In 1976, Diffie and Hellman proposed in their seminal work [DH76] the usage of two mathematically related keys in order to exchange messages secretly. This marks

the beginning of a new area of cryptography, namely the *public-key cryptography* (or asymmetric cryptography), as we will see in Section 1.1.2. These developments brought cryptography and complexity theory together. The scope of cryptography was extended by digital signatures and message authentication codes.

Fault-tolerant protocols were developed in order to ensure that a protocol is executed correctly by the involved parties. This lead to the construction of so-called Zero-Knowledge Protocols. This *cryptographic primitive* (a basic cryptographic construction block) plays an important role in proving the security of cryptographic protocols.

Another problem for which cryptography provides elegant solutions is the problem of calculating the output of a certain function whose inputs are kept secret by one of each parties. The first problem that raised this question was the famous Yao's Millionaires' Problem [Yao82]. Here two millionaire's want to know which one is richer without revealing the value of their fortune and without the help of a third party.

In 1996, a new kind of attack was introduced. Rather than mathematically attacking the protocol itself, these attacks used physical properties of the devices or implementation details in order to break the system. They were called *side-channel attacks*. The first one was a timing attack first introduced by Paul Kocher in [Koc96]. A major breakthrough occurred in this area when Kocher showed in [KJJ99] how to extract the secret key from a device by merely analyzing the electric current consumption during a decryption (resp. encryption) phase and by knowing the processed ciphertext (resp. plaintext). This discovery forced researchers to look for countermeasures. Nowadays these measures are taken into consideration when implementing industrial and commercial security solutions.

Advances in technology and new requirements will certainly make sure that cryptography will be full of new interesting problems waiting to be solved in the years to follow.

1.1.1. Private-Key Cryptography

The oldest and more basic scenario in cryptography raises when two legitimate parties (usually called Alice and Bob) intend to secretly exchange a message in a public channel, without an eavesdropper (commonly referred to as Eve) being able to understand its content. Private-key cryptography focuses on the study of cryptographic systems such that Alice and Bob somehow (as we will be able to see later) already share a secret key, obviously kept secret from Eve. Symmetric cryptography develops algorithms using this secret key (usually called *ciphers*) in order to transform the plain message (usually called *plaintext*) into a string - the *ciphertext* - which cannot be understood without the knowledge of the secret key.

Let Enc_k and Dec_k be the encryption and decryption algorithms using the secret key k, respectively, x the plaintext, and $y := Enc_k(x)$ the ciphertext. The basic property that an encryption system has to fulfill is the following: $Dec_k(Enc_k(x)) = x$. Clearly, this means that encryption and decryption are inverse operations and that one can therefore recover the plaintext given the ciphertext, as long as the secret key is provided.

Claude Shannon developed a mathematical framework in his 1948 famous work [Sha48] for the analysis of the *information* and established that a *perfect secret* or *information-theoretically secure* encryption would be one where the ciphertext

provides no information about the plaintext. In other words, this means that the entropy of the messages (related to the idea of randomness) is kept constant even after the knowledge of the ciphertext. In Shannon's theory, it is proven that this is only possible if the secret key is as long as the plaintext, which makes it impractical for daily applications. The perfectly secure encryption scheme Shannon proposed is the so-called *one-time pad*, where the ciphertext y is given by $y := Enc_k(x) = x \oplus k$. In practice, however, keys are shorter than the plaintext and must be reused several times. This implies that the encryption and decryption ciphers should be carefully designed in order not to *leak* any information about the secret key.

Historically, several ciphers have been successively developed and constantly been broken. Prominent examples are the Shift Cipher, Substitution Cipher, Affine Cipher, Vigenère Cipher, Hill Cipher and Permutation Cipher. In our days, the available computational power is enough to easily break this kind of ciphers. Not only statistical properties can be used to break the systems, but also the small amount of possible keys (i.e., the entropy of the key) makes it feasible to perform exhaustive search. All these ciphers belong to the group of so-called *block ciphers*. The ciphertext y is constructed by breaking the plaintext x into several blocks of equal length, i.e., $x := x_1x_2...$, and encrypting each block separately with the same key k, i.e., $y := y_1y_2... = Enc_k(x_1)Enc_k(x_2)....$ In *stream ciphers*, plaintext blocks are encrypted using a keystream $z := z_1z_2....$ The ciphertext will be constructed as $y = Enc_{z_1}(x_1)Enc_{z_2}(x_2)....$ A detailed description of each of one of these ciphers can be found in [Sti02].

Cryptography is primarily concerned with finding possible secure ciphers. The design of appropriate block ciphers is not a trivial task. In 1977, the *Data Encryption Standard (DES)* (see [DES77] and [BA81]) was adopted as a standard cryptographic cipher. This cipher is a block cipher, where each block has a length of 64 bits. The key is also 64-bit long, including 8 parity bits. While providing a good level of security during several years, modern computers can perform an exhaustive search on the DES key space. As a result, the block cipher Rijndael [DR98] was adopted as the new standard and renamed *Advanced Encryption Standard (AES)* in the year 2000. The AES key is usually 128, 192 or 256 bit long, depending on the number of rounds employed in its structure. This cipher has so far resisted all breaking attempts and is still vastly employed.

1.1.2. Public-Key Cryptography

Public-key cryptography requires the existence of two possibly different but somehow related keys - one *secret key* and one *public key*. The idea is that Alice generates a pair of public and private keys which are mathematically related. Then she publishes her public key. Bob uses this key in order to encrypt the message and sends the ciphertext to Alice. Alice is the only party who knows her private key enabling her to decrypt the ciphertext. Eve will not be able to decrypt the ciphertext, as she has no knowledge about the private key. When considering public-key cryptography, one mainly refers to the *computational security* of the systems. Some assumptions need to be made about the computational power of an adversary and about its possibility of inverting a so-called *one-way function*. These functions are *hard to invert* unless some knowledge (called *trapdoor*) is available. Most public-key cryptosystems are based on number-theoretical problems. This is also the case for the RSA cryptosystem [RSA78]. In this cryptosystem, modular operations (specifically expo-

nentiations) are used in order to encrypt and decrypt the messages. The modulus is the product of two big prime numbers that just one of the parties knows. The security of this method relies on the fact that an opponent cannot *efficiently* factorize this modulus into two primes number. The security of other ciphers relies on the *discrete logarithm (DL)* problem. Basically, given a multiplicative group (G,·), an element $\alpha \in G$ having order n and an element $\beta \in \langle\alpha\rangle$, this problem asks to find an integer $a, 0 \leq a \leq n-1$, such that $\alpha^a = \beta$. Several public-key cryptosystems are based on the DL problem, like the ElGamal Cryptosystem. Other public-key cryptosystems are based in elliptic curves over finite fields. Its application to cryptography was proposed independently in 1985 by Koblitz [Kob87] and Miller [Mil85].

But public-key cryptosystems are useful not only for message encryption. Public-key cryptography also comprises *digital signatures*, a means for providing authentication and integrity of a message.

As one particular example of the application of public-key cryptography, we would like to focus on the key exchange problem, the main topic of our work. Key exchange can be performed using basically any public-key cryptosystem. One of the most deployed methods is the so-called *Diffie-Hellman (DH) Key Exchange protocol* [DH76]. This protocol is also based on the DL-problem. In this case, given a cyclic group $\mathbb{G}$ with order q and a generator g of $\mathbb{G}$, Alice chooses randomly $x \in_R \mathbb{Z}_q$ and sends $h_1 := g^x$ to Bob. Bob performs very similarly, i.e., Bob chooses randomly $y \in_R \mathbb{Z}_q$ and sends $h_2 := g^y$ to Alice. Alice calculates $k_A := h_2^x$ and Bob calculates $k_B := h_1^y$. Assuming that the DL-problem is *computational hard*, Eve should not be able to calculate the shared key $k_A = k_B$.

Public-key techniques require extensive computational power. As a result, *hybrid systems* were developed, combining public key techniques merely for the purpose of key exchange (as RSA or Elliptic Curve Cryptography) with private cryptography methods (e.g., AES) for the encryption and decryption of the transmitted messages.

A detailed introduction to these topics can be found in any textbook, e.g. in [KL07] or [Sti02].

1.2. Motivation for Wireless Key Exchange

Pre-sharing and manually configuring symmetric keys is one of most used methods for key establishment in modern wireless devices. This solution is clearly not practical and flexible enough, as a reset of the key would require physical presence.

As explained in Section 1.1.2, public-key techniques can be employed to solve the problem of key exchange. However, public-key cryptography relies on still unproven assumptions, namely the problem of $\mathcal{NP} \neq \mathcal{P}$. Moreover, these methods are strongly time and energy consuming, which can be critical for low-energy applications and resource-constrained platforms, such as wireless sensor networks (WSN). This is, in particular, the case for ZigBee and Bluetooth specifications, where very weak security mechanisms have been implemented in order to perform the key exchange and have therefore already been cracked. Due to energy constraints, public-key methods are not implemented in their standard form. Other known security issues have also been observed in WiFi Protected Setup (WPS) and other wireless standards.

Up until recently, cryptographic functionality has been solely implemented in the upper layers of the protocol stack (see Figure 1.1).

For example, admission control, like WiFi Protected Access (WPA), is imple-

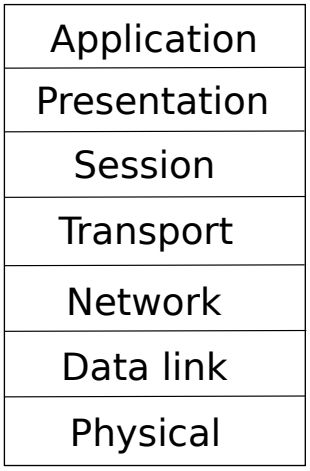


Figure 1.1.: OSI Model layers.

mented at the *link layer*, Internet Protocol Security (IPSec) at the *network layer* or Secure Sockets Layer (SSL) at the *transport layer*. With the increasing popularity of the wireless interconnection of small embedded systems, the so-called Internet of Things (IoT), new challenges regarding security and privacy awareness have emerged. Nevertheless, using the *physical layer* for security purposes was not considered. Lower levels simply seemed not to offer any properties that could be useful for security. In recent years, a few authors have been proposing methods for exploring the lower levels of the stack, namely the *physical layer (PHY)*, for improving the security of the overall system, as described in [BB11].

Lately, the ubiquitous presence of wireless networks has renewed the interest in key exchange schemes at the physical layer. One of the most promising techniques to generate cryptographic keys at the physical layer is based on the concept of *reciprocity* of wireless channels. Wireless channels exhibit a phenomenon called *multipath interference* (or multipath fading). The key extraction is simply performed from the physical structure of the environment where the wireless transmission takes place. The *shared randomness* is created by sounding the channel between both legitimate parties and results from unknown and dynamic electromagnetic characteristics of the physical environment. In such channels, emitted radio signals are scattered and reflected from various physical obstacles. Thus a receiver will receive the original signal superposed with several echoes caused by different reflections. Reciprocity, in turn, states that the channel between two parties, characterized by its channel impulse response, will remain the same if the roles of sender and receiver are exchanged. Therefore, a sender-receiver system consisting of two physically separated transceivers, Alice and Bob, can extract joint randomness by measuring the impulse response of the wireless channel between them. Since the measured channel impulse response is the same for Alice and Bob during the coherence time of the channel, it can be processed to a common secret key. For the security of this method, it is crucial that any further eavesdropper, who is sufficiently distant from the legitimate protocol parties, will receive uncorrelated measurements.

Therefore, in this work, we studied the feasibility of replacing public-key techniques by physical layer methods for the purpose of key exchange.

One other important motivation for *key exchange on the physical layer* is the possibility of avoiding mass surveillance. By using physical-layer security, an attacker

would have to continuously be able to reproduce the physical layer key exchange protocol between each communicating parties exactly at the same time they perform it, which requires him to be physically present. As it is not feasible to have one surveillance agency per communicating party, this is impossible to realize.

The usage of this kind of key exchange may be eventually combined with other conventional systems (like the DH key exchange protocol) in order to increase the computational resources needed to break a system. This can be an interesting subject for further work.

1.3. Our Contribution

A few methods used to extract a shared key (a binary sequence) from the received signals have been proposed by different authors. These techniques basically aim at generating a secret key having as much entropy as possible, while being reliable and efficient. They are suited for key extraction and key agreement in wireless and mobile settings, such as wireless sensor networks.

However, the conditions under which they are secure are not totally clear. The possibility of dealing with environments which are not complex enough should also be considered. Besides, as in other areas of cryptography, one should consider implementation issues.

In this work, we demonstrate that indeed this protocol is not totally secure if the environment is too simple and propose an attack we named *environment reconstruction attack*. Moreover, we present a side-channel attack against its implementation. This attack is based on the fact that antennas reradiate all the signals they receive. We called this attack the *reradiation leakage attack*. We establish under which circumstances this attack is feasible and define a region outside of which an attacker must be in so he cannot collect significant information from the reradiated signal.

We additionally propose a new method to extract raw information from the environment. Our technique explores the characteristics of the channel in different frequencies. Our main contribution consists in leveraging the properties of some hardware components for the purpose of generating a shared key containing more entropy. We use the local oscillators of the transceivers as the additional source of randomness shared by the legitimate parties. This is done without affecting the overall symmetry of the system. Consequently, reciprocity will still hold, which further allows for common secret key extraction. This method has the advantage of being more resistant to the reradiation leakage side-channel attack on reciprocity-based wireless key exchange, as an attacker should somehow know the exact frequency Alice and Bob's oscillators are tuned to in order to mount an attack.

Finally, we develop a radio prototype in order to serve as a *proof-of-concept* and experimentally validate our protocol. We perform a variety of experiments under different environments. We address some limitations and propose solutions.

Thesis Outline After introducing the necessary background knowledge needed to understand our work, we put forward our main achievements: we present new methods for breaking the fading-based key exchange protocols proposed up until now in Chapter 4 and introduce and experimentally validate a novel technique to cope with these new attacks in Chapters 5 and 6. Our work is divided into the following chapters:

Chapter 2. Preliminaries In this chapter, we introduce the basic notions necessary for fully understanding the methods we have implemented. More precisely, we expound some topics concerning antenna theory, wireless channels and information reconciliation. No original contribution by the author is put forward here.

Chapter 3. Related Work We give a rundown of the literature and methods employed for the transmission of a secret (like a bitstring that might be later used as a secret key) or for authentication purposes implemented in the physical layer. We classify them as noise-based, reciprocity-&-fading-based, antenna-based, jamming-based and device-based methods. The main principles of reciprocity-&-fading-based methods, against which we have mounted attacks in our work, are described in more detail. We explain some known methods for key extraction and we summarize previous results about wireless key exchange.

Chapter 4. Vulnerabilities and Attacks We demonstrate an aspect of reciprocity-based key exchange that has so far been neglected. A model for fading channels is described under which a passive eavesdropping adversary can reconstruct a key generated by two protocol parties. We introduce some vulnerabilities of the fading-based key exchange protocol and mount an attacked we named *environment reconstruction attack*. Additionally, a new side-channel attack is presented. This side-channel attack is based on the phenomenon of passive signal reradiation that occurs in receiving antennas. We called it *reradiation leakage attack*. An experimental test of this attack is described and the results are analyzed. The exact conditions under which this attack can be mounted are identified in detail. Upper theoretical bounds for the feasibility of this attack are derived. The results are published in [DLMdA10].

Chapter 5. Improvements to the Protocol We introduce a *countermeasure* against the *environment reconstruction attack*. This measure also helps against the reradiation side-channel attack, introducing a new variable for the entropy generation, namely the unavoidable and unpredictable *difference in the frequencies* between Alice and Bob's transceivers' local oscillators. For a perfect attack, the attacker would also need to estimate both these frequencies with a very high degree of precision, which, in reality, is not easy to perform with common receivers. Simulations illustrating these ideas are presented. The main results are published in [MdA14] and [DLMQdA10].

Chapter 6. Experimental Validation We present an experimental study that validates the above mentioned *countermeasure*. A measurement campaign has been undertaken and information has been collected under different environments, both indoor and outdoor. The goal was to make sure that our method is stable and applicable under different environment conditions. We also seek to find the better way of combining the effects from fading with those due to different oscillation frequencies. The results are analyzed in detail.

Chapter 7. Conclusion We conclude our work and point out new directions for further research.

2. Preliminaries

In this chapter, we introduce the underlying concepts that are required to understand this work. Note that we do not intend to put forward a fully detailed introduction of the presented subjects, but only introduce the strictly necessary notions. Some important concepts are constantly mentioned throughout this work, namely some notions about antenna theory, wireless channels and channel reciprocity, as well as some ideas about information reconciliation. For the sake of self-containedness of this work, we will briefly describe these concepts. Most of the content is based on the sources referenced in the text. We refer the interested reader to those references.

2.1. Antenna Theory

Since key exchange based on fading channels depend upon the transmission of electromagnetic waves using transceivers equipped with any kind of antennas, we show some important ideas related to this topic. This theory is also important in order to fully understand the reradiation leakage attack presented in Section 4.2. For a thorough understanding of this subject, refer to [Bal97].

2.1.1. Antenna Radiation Pattern and Directivity

A very important notion when characterizing an antenna is the so-called *radiation pattern*. The radiation patters (also called antenna pattern) of an antenna refers to the spatial dependence of the emitted or received radiation. It can be described as a mathematical function (usually calculated from electromagnetic theory) or as a graphical representation (usually measured through experimentation). It is a measure for how strong an antenna emits or receives in a certain direction.

Some types of antennas have very peculiar radiation patterns: an *isotropic antenna* is an antenna which reradiates equally in all directions; an *omnidirectional antenna* is an antenna having a constant radiation in a certain plane; finally, a *directional antenna* is able to transmit or receive signals differently in different directions. Therefore, it is able to transmit and receive better in some directions than others. Figure 2.1 shows an example of a directional antenna radiation pattern. This radiation pattern corresponds to a Yagi antenna, which is an antenna mainly used for the reception of TV signals. It is clear that this antenna radiates stronger in

one direction (usually the 0° direction), corresponding to the so-called main lobe. Opposite to this lobe, we can observe a very small back lobe (in the 180° direction). In other directions, one can clearly recognize some minor or side lobes.

This antenna covers a relatively small area for sending and receiving information signals. In practice, only the signals incoming from the directions between 20° and −20° will be captured by the antenna.

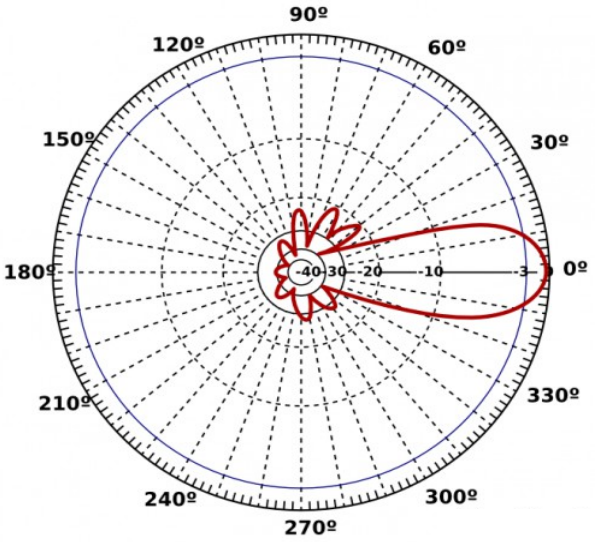


Figure 2.1.: Radiation Pattern of a Yagi antenna (source: [Mor11]).

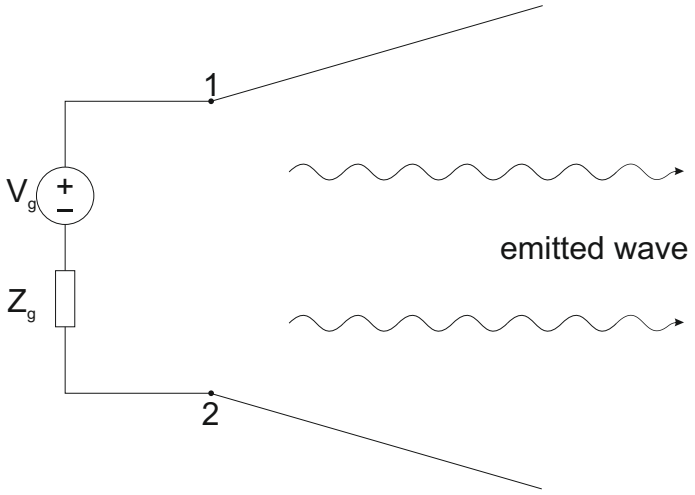
One important parameter of an antenna is its *directivity*. It is defined as *the ratio of the radiation intensity in a given direction from the antenna to the radiation intensity averaged over all directions* [Bal97]. In case the direction is not explicitly mentioned, one usually refers to the direction of maximum radiation intensity. This is also called *maximum directivity*. This is an expression of the extension of the main lobe of the radiation pattern. The bigger its directivity, the higher the capability of an antenna to send or receive in a certain direction in comparison with the other directions. By visual inspection of the radiation pattern shown in Figure 2.1, we can say that the corresponding antenna has a relatively high directivity. The *gain* of an antenna is proportional to its directivity. Furthermore, the antenna radiation patterns of the emitter and receiver are of utmost importance, a fact that plays an important role in our experiments.

2.1.2. Antenna Reradiation

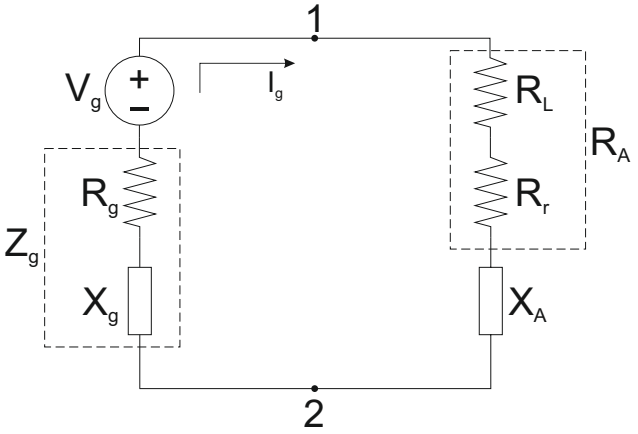
We will now briefly describe the fundamentals about antenna models. Antennas can work either in the *receiving mode* or in the *transmitting mode*. For both modes, the used models are quite similar and explained next.

2.1.2.1. Transmitting Mode

Consider the following model of an antenna in the transmitting mode (Figure 2.2). The ratio of the voltage to the current at its terminals, 1 and 2, is called the impedance of the antenna, and is given by



2.2.1: Antenna Model.



2.2.2: Antenna Model Circuit.

Figure 2.2.: Antenna in transmitting mode.

$$Z_{\mathrm{A}} = R_{\mathrm{A}} + jX_{\mathrm{A}}, \tag{2.1}$$

where R_{A} is the antenna resistance at its terminals, and X_{A} its reactance. R_{A} can be expressed as

$$R_{\mathrm{A}} = R_{\mathrm{r}} + R_{\mathrm{L}}, \tag{2.2}$$

where R_{r} is the radiation resistance of the antenna and R_{L} its loss resistance.

If we consider its Thévenin equivalent and the antenna connected to a wave generator with impedance Z_{g},

$$Z_{\mathrm{g}} = R_{\mathrm{g}} + jX_{\mathrm{g}}, \tag{2.3}$$

where R_{g} and X_{g} are the resistance and reactance of the generator, respectively, we have that the power delivered to the antenna for radiation is given by

$$P_r = \frac{1}{2}|I_{\mathrm{g}}|^2 R_r = \frac{|V_{\mathrm{g}}|^2}{2}\frac{R_{\mathrm{r}}}{(R_{\mathrm{r}}+R_{\mathrm{L}}+R_{\mathrm{g}})^2+(X_{\mathrm{A}}+X_{\mathrm{g}})^2}, \tag{2.4}$$

the power dissipated as heat by

$$P_{\mathrm{L}} = \frac{1}{2}|I_{\mathrm{g}}|^2 R_{\mathrm{L}} = \frac{|V_{\mathrm{g}}|^2}{2}\frac{R_{\mathrm{L}}}{(R_{\mathrm{r}}+R_{\mathrm{L}}+R_{\mathrm{g}})^2+(X_{\mathrm{A}}+X_{\mathrm{g}})^2}, \tag{2.5}$$

and the rest of the energy dissipated as heat on the internal resistance R_g of the generator by

$$P_{\mathrm{g}} = \frac{|V_{\mathrm{g}}|^2}{2}\frac{R_{\mathrm{g}}}{(R_{\mathrm{r}}+R_{\mathrm{L}}+R_{\mathrm{g}})^2+(X_{\mathrm{A}}+X_{\mathrm{g}})^2} \tag{2.6}$$

From elementary computations, it readily follows that one can maximize the power delivered to the antenna when we have the case of conjugate matching[1], i.e., when

$$Z_{\mathrm{A}} = Z_{\mathrm{g}}^* \tag{2.7}$$

From this expression, it appears clear that:

$$P_{\mathrm{r}} = \frac{|V_{\mathrm{g}}|^2}{8}\frac{R_{\mathrm{r}}}{(R_{\mathrm{r}}+R_{\mathrm{L}})^2} \tag{2.8}$$

$$P_{\mathrm{L}} = \frac{|V_{\mathrm{g}}|^2}{8}\frac{R_{\mathrm{L}}}{(R_{\mathrm{r}}+R_{\mathrm{L}})^2} \tag{2.9}$$

$$P_{\mathrm{g}} = \frac{|V_{\mathrm{g}}|^2}{8}\frac{1}{R_{\mathrm{r}}+R_{\mathrm{L}}} \tag{2.10}$$

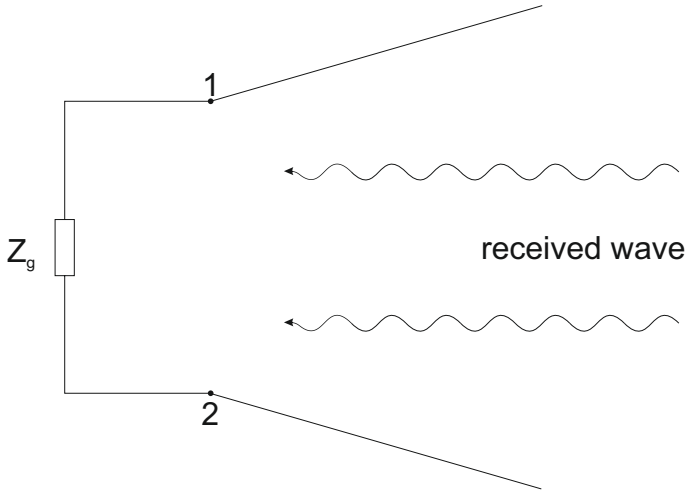
From expressions (2.8) to (2.10), it is obvious that $P_{\mathrm{g}} = P_{\mathrm{r}} + P_{\mathrm{L}}$.

This means that of the total power that is provided by the generator, one half is dissipated as thermal energy (heat) in the internal resistance of the generator and the other half is delivered to the antenna. Part of the power delivered to the antenna is *radiated*, represented here by the radiation resistance, R_{r}, and the other part is dissipated as heat. In the case of a perfect lossless antenna, a maximum of 50% of the total power given to the antenna is radiated.

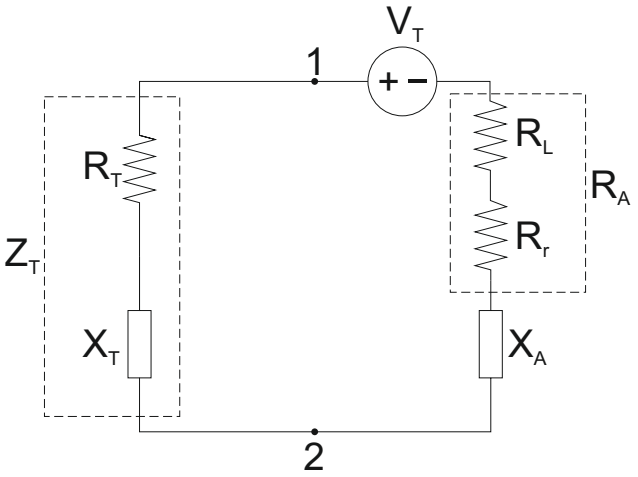
2.1.2.2. Receiving Mode

Consider now an antenna in the receiving mode (Figure 2.3). The incident wave reaches the antenna and it induces a voltage V_{T} very similar to the voltage V_{g} induced by the generator in the transmitting mode (cf. 2.1.2.1). Therefore, as the similarities are obvious, we can replace V_{g} by V_{T} in the previous expressions (2.8 to 2.10) under conjugate matching

[1] $z^* = x - jy$ stands for the conjugate operator of a given complex quantity $z = x + jy$.



2.3.1: Antenna Model.



2.3.2: Antenna Model Circuit.

Figure 2.3.: Antenna in receiving mode.

$$Z_{\mathrm{A}} = Z_{\mathrm{T}}^{*} \tag{2.11}$$

to conclude that the power delivered to the resistors P_{r}, P_{L} and P_{T} are:

$$P_{\mathrm{r}} = \frac{|V_{\mathrm{T}}|^2}{8} \frac{R_{\mathrm{r}}}{(R_{\mathrm{r}} + R_{\mathrm{L}})^2} \tag{2.12}$$

$$P_{\mathrm{L}} = \frac{|V_{\mathrm{T}}|^2}{8} \frac{R_{\mathrm{L}}}{(R_{\mathrm{r}} + R_{\mathrm{L}})^2} \tag{2.13}$$

$$P_{\mathrm{T}} = \frac{|V_{\mathrm{T}}|^2}{8} \frac{1}{R_{\mathrm{r}} + R_{\mathrm{L}}} \tag{2.14}$$

The *collected power*, P_c is given by

$$P_{\mathrm{c}} = \frac{|V_{\mathrm{T}}|^2}{4} \frac{1}{R_{\mathrm{r}} + R_{\mathrm{L}}} \tag{2.15}$$

The power P_{r} will play a very important role in our work in Section 4.2. This power is called *scattered or reradiated power*. Half of the total collected power is delivered to the load R_{T} and the other half is reradiated through R_{r} and dissipated as heat through R_{L}. In a lossless antenna ($R_{\mathrm{L}} = 0$), half of the collected power is delivered to the load and the other half is reradiated. We use this fact to mount a side-channel attack against a key exchange protocol.

In general, we define the *reradiating factor*, ρ, as the fraction of the incoming power, P_i, reaching an antenna that is reradiated, i.e., $\rho := \frac{P_{\mathrm{r}}}{P_{\mathrm{i}}}$.

Under conjugate matching, $P_i = P_c$ and, therefore,

$$\rho = \frac{P_{\mathrm{r}}}{P_{\mathrm{c}}} = \frac{1}{2} \frac{R_{\mathrm{r}}}{R_{\mathrm{r}} + R_{\mathrm{L}}}. \tag{2.16}$$

2.2. The Wireless Channel

The wireless channel plays a fundamental role for the subject of this thesis, namely for generating and sharing a symmetric cryptographic key between two communicating parties. For the sake of self-containedness, we present in this section the necessary notions for understanding our work. An extensive study on this subject can be found in [TV05]. We use the same notation throughout this section.

It seems obvious that the broadcast nature of the wireless channel makes it prone to eavesdropping. In this section, we will introduce the basic notions related with this transmission medium and its basic physical parameters.

The variations of the channel strength over time and over frequency constitute two of its basic properties, which clearly do not occur in a cabled medium, like a coaxial cable or an optical fiber. These variations can be divided in two large classes, namely

1. Large-scale fading: path loss over large distances and shadowing by large objects in the environment (like buildings) are the main cause of this type of fading. It is frequency independent;

2. Small-scale fading: consequence of wave interference (constructive and/or destructive) over small distances, due to the fact that there are multiple paths between the transmitter and the receiver. Its influence is in the order of the carrier wavelength. It is frequency dependent. It is commonly known as *multipath interference* and is of paramount importance to our work.

In order to better understand the wireless channel, some models have been created.

2.2.1. Physical Models

This section is based on the textbook by Tse [TV05]. The interested reader should refer to this work. Electromagnetic waves are explained and described by the famous Maxwell's equations. These equations can be expressed in differential and

integral form and are usually not easy to solve analytically or even using numerical methods. In certain complex environments, solving these equations might be even a practically impossible task. Therefore, stochastic models for describing the wireless channel have been proposed. To model the wireless channels, one divides the complex environment in simpler cases. Four main cases of increasing complexity will be considered for modeling the wireless channel.

1. Free space propagation and fixed antennas;
2. Free space propagation and moving antenna;
3. Reflecting wall and fixed antenna;
4. Reflecting wall and moving antenna.

Free space propagation is not very common in the real world, except for the cases of communication in space or in a desert. The last two cases are the ones that appear more often, either in static (none or reduced movement) or dynamic environments.

2.2.1.1. Free Space Propagation and Fixed Antenna

Let us start with the following basic scenario. Consider a fixed antenna and the electromagnetic waves propagating freely in space (Figure 2.4).

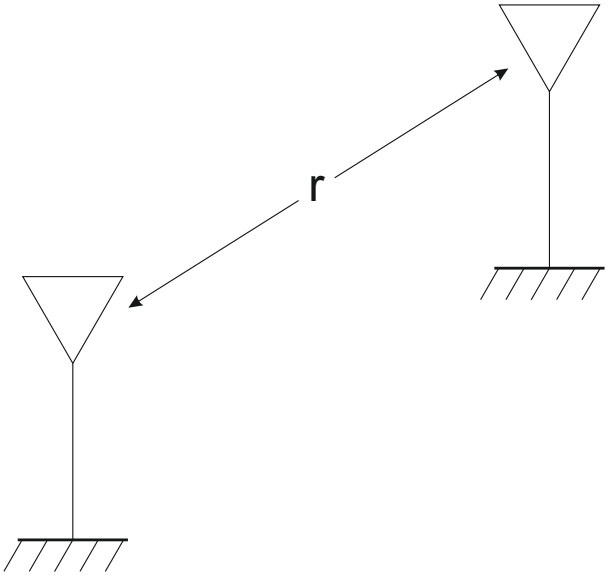


Figure 2.4.: Free space and fixed antennas.

We know from electromagnetic theory that the electric and magnetic fields are perpendicular to each other and to the direction of propagation from the antenna. For this reason, it is sufficient to consider and describe the electric field. Given that the transmitter has sent a sinusoidal wave, say $s(t) = cos(2\pi ft)$, the electric far-field at instant t is given by the following expression:

$$\begin{aligned} E(f,t,(r,\theta,\psi)) =& \frac{\alpha_S(\theta,\psi,f)s(t-r/c)}{r} \\ =& \frac{\alpha_S(\theta,\psi,f)\cos(2\pi f(t-r/c)}{r}, \end{aligned} \tag{2.17}$$

where (r, θ, ψ) are the spherical coordinates of a point in space and $s(t - r/c)$ a delayed replica of the original signal $s(t)$. We consider the transmitter antenna placed at the origin of the coordinate axis, which means that r is the distance between transmitter and receiver antennas. c is the speed the radiation propagates freely at, and $\alpha_{\mathrm{S}}(\theta, \psi, f)$ is the radiation pattern of the sending antenna at frequency f in the direction (θ, ψ). The radiation pattern of an antenna basically indicates how much radiation an antenna can send and receive in each direction and has already been described in detail in the Section 2.1.1. Electromagnetic theory states that the amplitude of the electric fields depends on $1/r$, and its power changes with $1/r^2$ in free propagation. A receiver antenna will therefore receive

$$E_{\mathrm{r}}(f, t, (r, \theta, \psi)) = \frac{\alpha(\theta, \psi, f)\cos(2\pi f(t - r/c)}{r}, \tag{2.18}$$

where $\alpha(\theta, \psi, f)$ is the aggregate product of the radiation patterns of the sender, α_{S}, and receiver antennas, α_{R}, i.e., $\alpha := \alpha_{\mathrm{S}} \cdot \alpha_{\mathrm{R}}$.

2.2.1.2. Free Space Propagation and Moving Antenna

Now consider the case where the receiving antenna is moving with constant speed v (Figure 2.5).

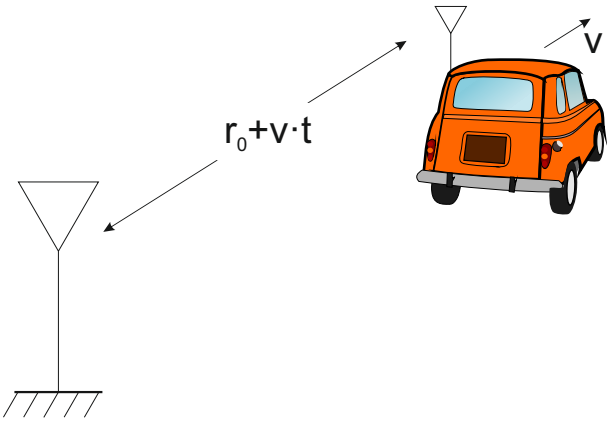


Figure 2.5.: Free space and moving antennas.

Using Equation (2.17) and substituting $r(t)$ by $r(t) = r_0 + vt$, where r_0 is the initial position, we get the following equation:

$$\begin{aligned} E(f, t, (r_0 + vt, \theta, \psi)) =& \frac{\alpha_{\mathrm{S}}(\theta, \psi, f)\cos(2\pi f(t - r_0/c - vt/c)}{r_0 + vt} \\ =& \frac{\alpha_{\mathrm{S}}(\theta, \psi, f)\cos(2\pi f(t(1 - v/c) - r_0/c))}{r_0 + vt}. \end{aligned} \tag{2.19}$$

By other words, the sinusoid at frequency f has been transformed into a sinusoid of frequency $f(1 - v/c)$. There exists a shift of frequency of value $-v/c$. This shift of frequency is called *Doppler shift* and is due to the relative motion of transmitter and receiver.

The received electromagnetic wave will be given, analogously to (2.18), by

$$E_{\mathrm{r}}(f,t,(r_0+vt,\theta,\psi)) = \frac{\alpha(\theta,\psi,f)\cos(2\pi f(t(1-v/c)-r_0/c))}{r_0+vt}.. \tag{2.20}$$

2.2.1.3. Reflecting Wall and Fixed Antenna

We will now introduce the case where objects are to be found in the environment (Figure 2.6). Let's consider we have a direct path between a sender antenna and a receiver antenna, but also a reflected path in a wall.

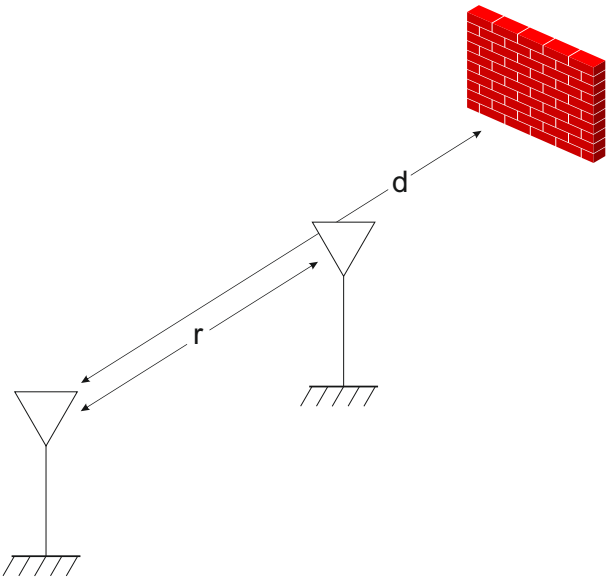


Figure 2.6.: Reflecting wall and fixed antennas.

The received waveform will be the result of the sum of the free space wave from the transmitter and the reflected free space waves from each of the reflecting objects, namely the wall. In the literature, this method is called *ray tracing*. Electromagnetic theory tells us that if a very large wall or object is located at a position d from the transmitter antenna, the reflected wave at a given point is the same as a wave that would exist on the symmetric side of the wall in the case there weren't any wall, which means at a distance of $2d-r$. According to (2.18), we have the received signal given by

$$\begin{aligned} E_{\mathrm{r}}(f,t,(r,\theta,\psi)) = &\frac{\alpha(\theta,\psi,f)\cos(2\pi f(t-r/c)}{r} \\ &-\frac{\alpha(\theta,\psi,f)\cos(2\pi f(t-(2d-r)/c)}{2d-r}. \end{aligned} \tag{2.21}$$

The phase difference between both waves (direct and reflected) has the value of

$$\Delta\theta = \left(\frac{2\pi f(2d-r)}{c}+\pi\right) - \left(\frac{2\pi fr}{c}+\pi\right) = \frac{4\pi f}{c}(d-r)+\pi.$$

Wave theory says that two waves can interact

- *constructively*: phase difference is an integer multiple of 2π; or
- *destructively*: phase difference is a odd integer multiple of π.

Thus, a very important parameter is the so-called *coherence distance*, which is the distance from a peak to a valley of an electromagnetic field:

$$\Delta x_{\mathrm{c}} = \lambda/4,$$

where $\lambda = c/f$ is the wavelength of the transmitted signal.

A change in the distance that is much smaller than Δx_c will not result in a significantly different received signal at a certain instant.

Another important parameter is called the *delay spread* and is defined as

$$T_{\mathrm{d}} = \frac{2d - r}{c} - \frac{r}{c}.$$

This corresponds to the difference between the propagation delays along both paths. The value $1/T_d$ is called the *coherence bandwidth* of the channel. In situations when the frequency changes by an amount much smaller than this value, the interference pattern does not change significantly.

2.2.1.4. Reflecting Wall and Moving Antenna

This is the case that better models the majority of the real-world environments. Consider that the receiving antenna is moving at a velocity v along the pattern of constructive an destructive interference induced by the two waves (Figure 2.7).

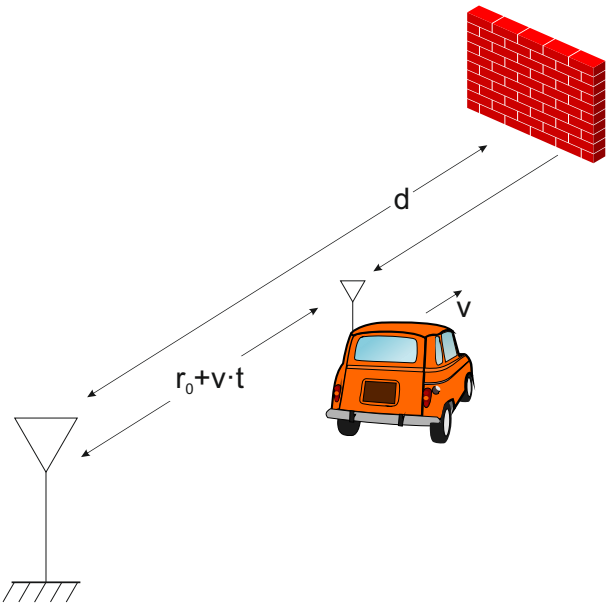


Figure 2.7.: Reflecting wall and moving antennas.

The strength of the received signal will increase and decrease accordingly. This is the origin of the *multipath fading*. To travel from a peak to a minimum of an electromagnetic wave, it is necessary the time of $(\lambda/4)/v = c/(4fv)$. This value is called *coherence time* of the channel.

The parameter $D_s = 2fv/c$ is called the *Doppler spread*. The resulting signal will be approximately the product of two sinusoids, which is a also a sinusoid of frequency f and envelope with frequency $D_s/2$.

Most of the times, wireless channels are time-variant. Their appropriate models depend on the observed time-scales of interest.

2.2.1.5. Remarks

Another important factor in studying wave propagation in wireless channels is the the reflection from an "object" which is almost always present: the ground plane. In particular, this plays an important role in rural areas as reflection objects are scarce in these areas. It can be shown that the electric wave at the receiver is in this case attenuated proportionally to r^{-2} and the received power to $(r^{-2})^2 = r^{-4}$.

Similarly, due to the presence of obstacles in the environment, one expects the power decay to be much faster than r^{-2}. Experimentation suggests that while power decay near the transmitter changes proportionally to r^{-2}, at large distances it can even decay exponentially with distance.

By modeling the density of obstacles and their absorption behavior as random numbers, one can simulate this randomness of the environment; the overall phenomenon is called *shadowing*. This stands in contrast to multipath fading. Its effects can last for multiple seconds or even minutes, occurring at a much slower time-scale.

Scattering is another type of reflection and occurs in the atmosphere or in reflections from very rough objects.

As previously stated, simulating the electromagnetic properties of a real environment is not a trivial task and might be practically impossible to perform in most real-world situations.

2.2.2. Channel as a Linear Time-Varying System

Due to the additive nature of electromagnetic waves, wireless channels can be modeled as a linear time-varying system. Consequently, the response of the system (the wireless channel) to a sinusoidal signal $A\cos(2\pi ft)$ of amplitude A and frequency f will be of the type

$$\sum_{i=1}^{n} \rho_i(f,t) A \cos(2\pi f(t - \tau_i(f,t)), \tag{2.22}$$

where $\rho_i(f,t)$ and $\tau_i(f,t)$ are the overall attenuation and propagation delay at time t in the path $i = 1, ..., n$. Let's now assume that these values do not depend on the frequency. In this case, the received signal $y(t)$ after a given signal $s(t)$ is sent in the path will be expressed by

$$y(t) = \sum_{i=1}^{n} \rho_i(t) \cdot s(t - \tau_i(t)). \tag{2.23}$$

If we consider transmission over narrow bands relative to the used carrier frequency, f, the individual attenuations and delays are assumed to be independent of the frequency. However, the overall channel response will vary with frequency due to

the fact that different paths have different delays. We can therefore state that the impulse response for a fading multipath channel, i.e., the response of a channel to a Dirac impulse $\delta(t)$ is given by

$$h(t,\tau) = \sum_{i=1}^{n} \rho_i(t) \cdot \delta(t - \tau_i(t)). \tag{2.24}$$

The Doppler shift for path i is then contained in the expression having the value $-f\tau_i'(t)$, where $\tau_i'(t) = v_i/c$ and v_i the velocity with which the ith path is being modified.

If one considers that the time-scale a channel changes is much bigger than the delay spread value (in the extreme case, transmitter, receiver and environment are all stationary), the values of $\rho_i(t)$ and $\tau_i(t)$ do not depend on t. The electromagnetic channel characteristics are therefore reduced to those of a linear time-invariant (LTI) filter. Shortly, a LTI system is a system whose output $y(t)$ to an input $s(t)$ is given by the convolution of the input $s(t)$ with its impulse response $h(t)$, i.e.,

$$y(t) = s(t) * h(t) := \int_{-\infty}^{+\infty} s(t-\tau)h(\tau)\, d\tau. \tag{2.25}$$

Simplifying (2.24), the impulse response of the channel is simply given by

$$h(\tau) = \sum_{i=1}^{n} \rho_i \delta(\tau - \tau_i). \tag{2.26}$$

Usually, one tends to use the variable t instead of τ when describing an impulse response. Replacing in Equation (2.26), we finally have the expression we will use in Section 4.1 for mounting an attack against the fading-based key exchange protocol:

$$h(t) = \sum_{i=1}^{n} \rho_i \delta(t - \tau_i). \tag{2.27}$$

Considering the wireless channel as a LTI system, the received signal (or output) $y(t)$ when sending a signal $s(t)$ would be thus

$$y(t) = \sum_{i=1}^{n} \rho_i s(t - \tau_i), \tag{2.28}$$

a sum of attenuated and delayed version of the input $s(t)$.

2.2.3. Important Parameters for Channel Characterization

The *coherence time* of a wireless channel, denoted by T_C, is defined as the time interval over which the channel impulse response does not change considerably (in what order of magnitude is concerned). Basically, this means that the impulse response for a certain time instant t may be considered constant. A channel is considered *fast fading* if the coherence time is much shorter than the time required for a certain application and *slow fading* if the opposite occurs. This value depends

mainly on the Doppler shifts for different paths. The Doppler spread can be defined as $D_S := 1/(4T_c)$. Other definitions are $D_S = 1/T_c$, if we consider only the order of magnitude to be important for the channel characterization. Typical values for T_c and D_S are 2.5 ms and 100 Hz, respectively (cf. [TV05]).

The multipath delay spread, T_d, is defined as the difference in propagation time between the longest and the shortest path, when only the main paths, i.e., the paths with significant energy, are considered. The value of the received signal $E_r(f, t)$ does not only change when t changes by T_c, but also when f chances by $1/(2T_d)$. Therefore we define the *coherence bandwidth*, W_c, as $W_c := 1/(2T_d)$. Concerning multipath time delay, if the bandwidth of the input is much less than W_c, then the channel is said to be *flat fading*. If the opposite occurs, the channel is said to be *frequency-selective*. Typical values for T_d and W_c are 1 µs and 500 kHz. More typical values for these parameters and a detailed explanation of channels and how to model them can be found in [TV05].

Moreover, several studies based on experimentation and simulation have been performed in order to evaluate the physical layer parameters for specific situations. E.g., in [TMB01], the authors use several simulation tools in order to check how the physical layer affects the performance of a wireless protocol. Curiously enough, they showed that different simulation tools for the evaluations of wireless network protocols yield different results, particularly due to different assumptions made at the physical layers, which they were able to simulate.

Other more complicated models, like the wide-sense stationary-uncorrelated scattering (WSSUS) channel model, commonly employed for the multipath channel experienced in mobile communications, are investigated in more detail in [SK98].

Braun et al. present in [BD91] a model for the time and frequency selective outdoor mobile radio channel. According to the authors, their method allows a classification of real environments into several classes and the extraction of the relevant parameters. They performed extensive experimentation in urban, suburban and rural regions, in hilly and mountainous regions in Switzerland. They experimentally measured complex impulse responses using two types of correlation receiver equipment: a narrow-band receiver and a broadband receiver. Furthermore, they showed that the impulse response contained one big peak corresponding to the direct path and a few, weak scattered components caused by small scatterers.

There are several other studies that try to characterize the wireless channels through experimental setups. One important characterization is based on the power delay profile of a channel, which can be performed in an easy way.

The *power delay profile (PDP)* (usually expressed in dB) plots the intensity power of a signal received through a multipath channel as a function of time delay. This time delay is the difference in travel time between multipath arrivals. This means that the highest peak will correspond to the main path, possible the line-of-sight (LOS) path. It is easily measured empirically and can be used to extract certain channel parameters such as the delay spread. There are expensive devices allowing this kind of measurements.

In [ZW99], the authors present power delay profile measurements gathered for the indoor radio propagation channel in the 2.4 GHz ISM Band. This is the band we will use later in our experiments. From the obtained PDP, they subsequently derived time dispersion parameters for this channel, namely the mean excess delay, RMS delay spread and maximum excess delay spread, as also defined in that work. Additionally, they also calculated the coherence bandwidth, W_c, of this channel.

Interesting values with mean excess delays of around 50 ns and coherence bandwidth about 700 kHz have been shown.

In their work [ZBN05], Zwick et al. characterized the wireless channel in several different rooms in four different buildings, from a small office to a library or laboratory by making broad multipath channel propagation measurements at 60 GHz. The measured RMS delay spread ranged between 3 ns and 9 ns.

Similarly, Choi et al. [CGR05] realized a measurement campaign for the characterization at 60 GHz of the indoor channel at three different corridors. The RMS delay spreads were about 10 ns.

Traditional methods like signal analyzers and oscilloscopes can be very expensive. In [MFZ+12], the authors show a very interesting and low-cost method to measure the channel impulse response (CIR) using less expensive devices, namely Universal Software Radio Peripheral (USRP) devices. We will in Section 5.2.2 describe this radio devices in detail, as they were used in our experiments. RMS delay spread were about 7 ns for a residential area, 6.5 ns for a commercial area and 30.2 ns for downtown urban areas. These values were obtained in several measurement campaigns.

In [AM94], the authors used a ray-tracing propagation model, as explained in Section 2.2.1.3, to compute the coherence bandwidth of an urban environment and the channel's RMS delay spread.

For more details about modeling the wireless channels as a LTI system, please refer to Hashemi's very interesting tutorial-survey paper [Has93]. They present the theory and a vast set of measurements for indoor systems, as well as an extensive bibliography about this subject.

As seen before, the channel is responsible for distortion in the original input signals. This distortion may cause bad effects in the telecommunications systems, like intersymbol interference (ISI), which may lead to high error rates in digital communications. Usually, equalizers are designed to compensate for this. In order to design such an equalizer, one may need to estimate the channel and its corresponding introduced distortion. The problem of channel estimation or sounding is also very important in our method for key exchange. Extensive literature has been written on this subject. In [TTD00], the authors propose a single-user channel estimation and equalization for LTI channels. Designing an optimal detector or receiver requires the knowledge of the channel response. Its parameters must therefore be carefully estimated from training sequences. However, there are channel estimation techniques which do not require training sequences. Therefore, they were given the name of *blind channel estimation* methods. Using these techniques, the channel estimation is performed while information signals are being transmitted. The intermediate case is called *semi-blind channel estimation*, where known symbols and unknown information data are contained in the same transmitted signal.

2.2.4. Reciprocity Theorem

This theorem requires sophisticated skills in the field of electromagnetics. We will just briefly mention it in order to get an intuition. The interested reader should refer to [Bal97] for more details.

Already in [Car29], Carson makes reference to a work from Sommerfeld from the year 1925 stating that: *If A_1 and A_2 are two antennas located at 0_1 and 0_2 respectively, and have arbitrary orientations, and signals are first sent from A_1 and*

received by A_2 and then sent with the same average power from A_2 and received by A_1, then the intensity and phase of the electric field at the receiver A_1 will be equal to that previously produced at A_2, regardless of the electrical properties and geometry of the intervening media and the form of the antennas.

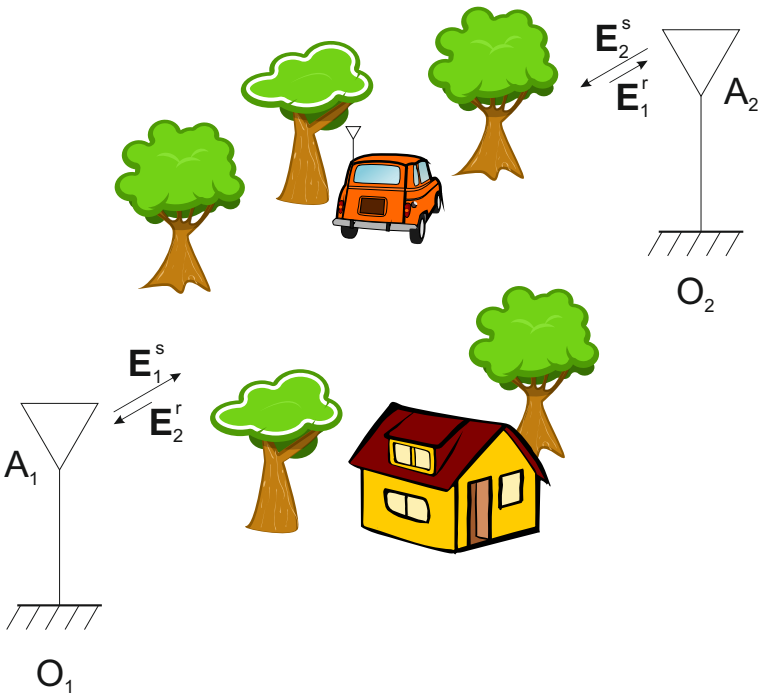


Figure 2.8.: Illustration of the Reciprocity Property.

Mathematically, if $|\mathbf{E_1^s}| = |\mathbf{E_2^s}|$ and $\angle\mathbf{E_1^s} = \angle\mathbf{E_2^s}$, then $|\mathbf{E_1^r}| = |\mathbf{E_2^r}|$ and $\angle\mathbf{E_1^r} = \angle\mathbf{E_2^r}$.

Its derivation comes from the Lorentz Reciprocity Theorem. Briefly, this theorem basically states the following: suppose a current density $\mathbf{J_1}$ produces an electric field $\mathbf{E_1}$ and a magnetic field $\mathbf{H_1}$. Similarly, a current density $\mathbf{J_2}$ produces an electric field $\mathbf{E_2}$ and a magnetic field $\mathbf{H_2}$. All these vectors are considered to be periodic with the same frequency.

For an arbitrary surface S enclosing a volume V, we have that

$$\int_V [\mathbf{J_1} \cdot \mathbf{E_2} - \mathbf{E_1} \cdot \mathbf{J_2}]\, \mathrm{d}V = \oint_S [\mathbf{E_1} \times \mathbf{H_2} - \mathbf{E_2} \times \mathbf{H_1}]\, \mathrm{d}\mathbf{S}.$$

This is the expression in the integral form. In its differential form, we would have

$$\mathbf{J_1} \cdot \mathbf{E_2} - \mathbf{E_1} \cdot \mathbf{J_2} = \nabla \cdot [\mathbf{E_1} \times \mathbf{H_2} - \mathbf{E_2} \times \mathbf{H_1}].$$

This theorem has several applications. It is used, e.g., for proving the reciprocity for two antennas and for radiation patterns (see [Bal97]).

2.3. Information Reconciliation and Privacy Amplification

Reciprocity itself may not ensure that the received signals of both parties are totally equal. Noise, small synchronization errors, differences in the used hardware or

even manufacture difference in similar hardware will be responsible for differences in the received signals. Therefore, the bitstring generated by these signals on both communicating parties may be slightly different, as we will show later in Chapter 6, where the results of our experimental validation are presented.

The problem of generating an equal bitstring from two marginally different strings in both legitimate parties has been already considered in the domain of the quantum key agreement and it has been given the name of *information reconciliation*. In the case that an attacker knows more than Alice and Bob about each other's secret random variable, there is the need, even before the information reconciliation step, to perform the so-called *advantage distillation* step, where Alice and Bob, by using the public channel, can get an advantage over the attacker. We didn't foresee the usage of this step in our prototype because, as we will show later in Chapter 6, Alice and Bob's information about each other's generated key, given by their key agreement rate, has virtually always been higher than Eve's information.

In order to cope with this issue in our prototype, an implementation of an information reconciliation phase has been suggested at the end of the protocol. Since this step is performed interactively in the public channel, some information is leaked to a passive eavesdropper.

We straightforwardly used one method for performing information reconciliation, namely the practical protocol described in detail in [BS93], called CASCADE. This protocol consists in exchanging parity bits between both parties in the public channel. This method can be better described as a kind of interactive binary search. As a drawback of this protocol, it is clear that the more parity bits are exchanged, the more information an attacker can collect about the secret key. The more bits Alice's and Bob's original bitstring differ in, the more parity bits have to be exchanged in order to correct this error.

The usage of information reconciliation protocols, namely of CASCADE, in the context of secret key agreement using antennas, namely with ESPAR Antenna, has already been suggested in [SIS09]. A detailed study on CASCADE can be found in [SY00]. More protocols about advantage distillation and information reconciliation and an analysis of CASCADE can be found in [LvTvD03].

Maurer and Wolf's 2003 three-part seminal paper on this subject, [MW03a], [MW03b] and [MW03c], give a deeper and formal insight on this problem.

These authors also studied a similar problem in key distribution, namely the problem of reducing the partial information that an attacker could have gained about the key during its generation process. This is achieved by creating a shorter key with information retrieved from the original key and reducing the information that the attacker would have gained before. This process is called *privacy amplification* and is based on the usage of a universal hash function. Since this technique is not original, we have not implemented it in our prototype. More details on these kind of functions can be found in [CW79]. Information reconciliation can also be performed by using decoders, as done e.g. in [HHY95].

3. Related Work

The possibility of using the intrinsic properties of the wireless channels for implementing security solutions in wireless communication systems was recently discovered and triggered an increasing interest about this subject. Several studies have been recently elaborated and some different approaches have been presented.

Wireless key exchange can be based on several principles and different approaches for security at the physical layer have been proposed by different authors.

These methods are considered to provide information-theoretical (unconditional) security, as no computational assumptions are required for their security.

In this chapter, we present an extensive survey on the distinct approaches for generating and/or transmitting a shared secret key by leveraging the properties of lower layers. We will refer to some studies who were elaborated in other contexts than security, but whose results are used when showing the security of some of the methods described here, like a few works studying the properties of different wireless environments.

3.1. Noise-based Methods

Most works mentioned here are predominantly based on the notion of information-theoretic secrecy capacity of the channels, defined as the maximum achievable secure rate of communication with a weak secrecy constraint. A deep survey of this subject can be found, e.g., in [BB11] and [BBRM08].

In 1975, in his seminal paper [Wyn75], Wyner introduced the famous *wiretap channel model*. Unlike the most accepted *Shannon's Model* for communication proposed in his work [Sha48], where the channel is assumed to be noiseless, the Wyner's wiretap channel ponders the realistic assumption of a noisy channel. Wyner's wiretap channel model consists of two legitimate parties (a transmitter and a receiver) and an eavesdropper. The channel between the transmitter and the receiver is called the *main channel*, whereas the channel between the transmitter and the eavesdropper is called the *eavesdropper's channel*. The signal the eavesdropper receives is a noisy version of the signal received at the legitimate receiver. These methods rely on the assumption that the noise of the legitimate user's channel and the noise of the eavesdropper's channel are uncorrelated. This gives an opportunity for secret

communication which will be explored by several other authors, as described in this section.

This model was extended to a *gaussian wiretap channel* in [LYCH78]. It considered an additive white-Gaussian noise channel. Hereby the noisy processes over the main and wiretap (or eavesdropper) channels are independent and identically distributed (i.i.d.) Gaussian over different channel users, with zero mean and variances σ_1 and σ_2. If we consider the average power limited to the value P over the transmitted symbols, the secrecy capacity of the Gaussian wiretap channel was shown to be $C_M - C_{MW}$, where C_M is the capacity of the main channel and C_{MW} is the capacity of the eavesdropper's channel, which is a concatenation of the main and wiretap channels. More specifically, the secrecy capacity, C_S, was found to be given by the fundamental expression

$$C_S = \frac{1}{2}log(1 + P/\sigma_1^2) - \frac{1}{2}log(1 + P/(\sigma_1^1 + \sigma_2^2)).$$

In [AC91], Ahlswede and Csiszar proposed a source-type and channel-type model where Alice and Bob share common randomness.

Other information-theoretic approaches extending Maurer's paper [Mau93] considered the secrecy capacity of the wireless channels by exchanging information over the public authenticated feedback channel. It is shown that such a secret key agreement is possible for a scenario in which all three parties receive the output of a binary symmetric source over independent binary symmetric channels, even when the enemy's channel is superior to the other two channels.

In [BR06], Barros and Rodrigues consider the transmission of confidential data over wireless channels with several communicating parties. First, these authors define the secrecy capacity in terms of outage probability. Based on this definition, they provide a complete characterization of the maximum transmission rate at which the eavesdropper is incapable of reliably decoding any information. The channels are considered to be quasi-static fading. The keystone is that the channel between both legitimate parties is independent from the the eavesdropper channel. Their results are stronger as they require less assumptions about the channel. Contrary to the results regarding Gaussian wiretap channels (without feedback), Barros shows that information-theoretic security is achievable even when the eavesdropper has a better average signal-to-noise ratio (*SNR*) than the legitimate receiver, as long as fading is present. In [BBRM08], the authors prove that information-theoretic security is achievable even when the eavesdropper's channel has a better average signal-to-noise ratio (*SNR*) than the main channel, given quasi-static Rayleigh fading channels. They summarize this property with the sentence: in what security is concerned, *fading thus turns out to be a friend and not a foe.* The key point here is to design secrecy capacity-achieving channel codes. One thus focuses on finding suitably long codes that get close to perfect secrecy.

In [CDK11], the authors present what they call a *Wireless Information-Theoretic Security (WITS)* scheme. They experimentally confirmed the suitability of their scheme for an outdoor topology with obstacles in two different situations: Obstructed-Line-of-Sight (OLOS) and Non-Line-of-Sight (NLOS). They explicitly ignored Doppler spread arguing that only a low-speed user movement was considered, i.e., in practice, a static environment. They claim that the lack of experimental measurements and empirical results threats the reliability of information-theoretic schemes and their robustness when submitted to real-life conditions and actual wave pro-

pagation environments. The authors set up an *ad hoc* network to test their technique. They used three laptops equipped with embedded 802.11n wireless adapters. The *netSumbler* software [net] was employed for the acquisition of average received power levels.They found an expression for the probability of nonzero secrecy capacity and outage secrecy capacity. Particularly, they concluded, among other interesting observations, that dense plantation shadowing leads to strong signal attenuation. Moreover, they confirmed some intuitional assumptions, namely that a degeneration of the channel topology and characteristics does not totally compromise the WITS scheme in terms of probability of nonzero secrecy capacity, given that this degeneration applies for both legitimate receivers and for the eavesdropper. They claim that the most important aspect in their method is the relative positions of both users and the attacker.

3.2. Reciprocity-&-Fading-based Methods

Some experimental studies about the correlation of the received signals depending on the distance of the receiving antennas and on the existence of several scatterers have been performed by Lee [Lee73]. Assuming a Rayleigh distribution for the receiver signal amplitude and uniform distribution of its phase, a simplified theoretical model has been proposed. The experimental results confirmed the theoretical underpinnings and the intuition that the correlation of the received signal clearly decreases with the insertion of scatterers and the distance between the antennas. This study is about antenna diversity and multipath interference and tries to explain the conditions under which there is significant advantage of using several antennas for a more efficient message transmission. Accordingly, a correlation of 0.7 or less is needed to obtain an advantage of antenna diversity. We can extrapolate for our case of fading-based key exchange and conclude that an attacker would receive, under certain conditions detailed in [Lee73], an uncorrelated signal from the one the legitimate parties receive. The theoretical prediction, including noisy signals, still agrees with the experiments. This noise is mainly due to the receivers. It is mentioned that in a city with tall buildings, the correlation between the signals obtained would be expected to be much lower.

Generally, *channel sounding* techniques have been already proposed in [RM93] for other purposes than security systems. Usually, the channel is described in terms of average delay, delay spread and coherence bandwidth. All these parameters give relevant information needed for the design of communication system. Channel sounding is a method for collecting this information for a communication's path and frequency range. In this paper, experiments under different environments were performed in order to calculate the path loss. The path loss was even determined for different moments in time. The difference between the results for April and May were clear. This was supposedly due to the development of new leaves and full foliage. Losses were determined to increase with frequency. This should be due to the fact that the dimensions of the leaves were very close to the value of a wavelength at the used frequency of 2.0 GHz.

However, the very first idea of using reciprocity combined with multipath interference as an opportunity for creating and sharing a cryptographic secret key first came up in 1995 in Hershey, Hassan and Yarlagadda's landmark paper [HHY95] on keying variable management. They basically suggested to use the characteristics of

an urban UHF radio channel, which could be determined by what they called *mutual sounding*. This is basically a way of measuring the impulse response of a channel, which they designated as *cryptovariable*. More concretely, the authors proposed a protocol where Alice and Bob send each other a suite of tones with a certain phase and amplitude. The relative phase information is then quantized. The usage of decoders on both parties is considered in order to get the agreement in slightly different keys, as mentioned in the section about information reconciliation (see Section 2.3). The security of this protocol refers to detailed investigations by Jakes [Jak74] on the probability distributions of the phase difference at two frequencies. This depends on the environment and an attacker should, accordingly, receive uncorrelated tone phases if its distance to the legitimate parties is large enough.

This idea was extended in [HSHC96]. In this work, the authors also propose to use the reciprocity of the channel and the rapid spatial decorrelation of phase in the radio channel as the main features for the purpose of key exchange. The presence of thermal noise as a source of errors between the generated keys was also analyzed. Again, the authors proposed the usage of a channel decoder to deal with this problem. A simulation was presented in order to evaluate the performance of a Golay code in establishing a 64-bit long secret key.

In [KHC00], the authors propose to probe the response of the channel. Accordingly, the sender of the message should adapt the sending phases in order to compensate for the difference in phases introduced by the channel and measured by the sender. This technique makes no use of a secret key to ensure secrecy. They claimed again that two receivers located far enough away from each other in a complex enough environment receive uncorrelated signals [OOKF68] due to reflections and interference of signals propagating through different paths. As stated previously, rapid spatial decorrelation is the basis of a few schemes used for key exchange. Some rules-of-thumb were established in order to characterize how far both receivers should be separated from each other and how complex the environmental conditions should be. Keeping this in mind, unconditional security from fading channels is exploited further in [TM01]. The authors present the first practical unconditionally secure system for a key exchange over a wireless link. They claim that statistical independence between Bob and Eve's signals occurs when these parties are separated by more than 10 to 100 wavelengths, depending on the fading channel characteristics. If Eve is not able to examine the changing channel attenuation between Alice's antenna and Bob's antenna, then she won't be able find the secret key. It was assumed in this work that fading is characterized only by lognormal shadowing. The authors claim however that their method should work also with other kinds of fading models. It is also mentioned that Eve's correlation depends on how close her antenna is to the legitimate parties' antennas, the RF band employed and the multipath characteristics of the channel. Their three-way handshake protocol has the disadvantage of requiring a RNG for the first step. Also a Forward Error Correction (FEC) coder is employed, as well as *cryptographically secure hash functions*. This clearly makes it unsuitable for light-weight applications. It is mentioned that the protocol lacks authentication, which makes it vulnerable to man-in-the-middle attacks. They also firstly identified the possibility of Eve, although unlikely, influencing or manipulating the environment in such a way that she could deduce the secret key. We explore this subject in our work in more detail later. Thermal noise is also mentioned. It is stated that in addition to unconditionally secure protocols, one may think about also employing conventional public-key methods, in order to

achieve secure communication.

In [SP08], the authors suggest that there is an optimum transmit power, and an optimum quantization strategy, that minimizes the energy consumption for a given key size. The emphasis is on exploiting the wideband wireless channels for generation of large secret keys. An important parameter is introduced, namely the probability $p(SINR, M)$, that both Alice and Bob originate the same quantization index for a particular phase as a function of the signal-to-interference-and-noise ratio ($SINR$) and the number of quantization levels (M). This variable is then used in order to calculate the minimum energy consumption for a successful key acquisition.

In [LDS12], the authors compare a few key extraction methods based both on entire channel state information (CSI) and on single channel parameter such as the received signal strength indicator (RSSI). They claim that the reduction in the degree-of-freedom when going from CSI to RSSI decreases the rate of the key extraction. They therefore suggest to make CSI information available to higher layers, where security is normally managed. They also identify the random amplitudes and phases of the channel response of wireless multipath fading channels as a source of naturally occurring randomness that would satisfy three important properties: easily and widely accessible, high level of randomness and difficult for Eve to observe. In a rich multipath environment wireless channels have high spatial and temporal variation, meaning there is a constant surge of new randomness that one can use to extract new and independent key bits. An Orthogonal Frequency Division Multiplexing (OFDM) system is explored from the perspective of key generation. Moreover, it is mentioned that the frequency generated by local oscillators continuously fluctuates (or drifts) around its center frequency, originating a time dependent phase drift. For their purposes, the authors considered the phase offset caused by oscillator frequency drift as negligible during each channel sounding. However, in our work, we used this drift as a source of common randomness (see Chapter 5).

After a couple of theoretical studies in this area, there was still a lack of an implementation of radio reciprocity-based key exchange schemes. This drew the attention of the community to the implementation of a few practical setups performing this protocol. In all of them, the authors present different *key extractors* (see Section 5.3) for generating the key from the received signal, given that some *non-reciprocities* (like different hardware employed or additive noise) strongly influence the final result ([MTM+08]). At this point, these non-reciprocities were seen as a problem for a perfect key establishment. In our work, we use instead the opportunity arising from this new source of randomness to augment the extracted entropy. Hence, most of the recent research focuses on finding stable and efficient key quantizers that deal with these impairments ([CPK10] and [PJC+13]).

One of the first practical implementation of key establishment schemes have been proposed in the seminal work by Lee et al. ([LXMT06]). Apart from their implementation, they additionally claim to reach confidentiality and authenticity of protocol parties, which therefore allows to detect spoofing attacks by using the characteristics of the physical channel. They called this technique the *channel-based authentication*. The principle is basically the same as the one employed for key exchange purposes: it is assumed that Alice and Bob had previously sounded the channel and subsequently both know the channel responses $h_{\mathrm{AB}}(t)$ and $h_{\mathrm{BA}}(t)$. This initial link is assumed to be established using traditional higher-layer authentication procedures. Later, Eve tries to masquerade as Alice. Bob asks Eve to send the signal and compares the received signal $\tilde{h}(t)$ with $h_{\mathrm{AB}}(t)$. If Eve is located somewhere else, $\tilde{h}(t)$ will be

different enough from $h_{AB}(t)$. This way, Bob realizes that this party is not Alice. Two methods for channel sounding were proposed: Temporal (Pulse-type) probing, where the usage of probing methods are suggested to construct channel estimates for authentication, as RF pulsing or spread spectrum methods; and Multiple Tone Probing, where different multiple, simultaneous carrier waves are sent, being the carrier frequencies f_i by an amount bigger than the channel coherence bandwidth to ensure independent fading across them. Finally, they proposed the keys to be given by $K_A = f(h_{BA})$ and $K_B = f(h_{AB})$, where f is a cryptographic one-way function. Another solution would be to use these two values as a mask for the distribution of some chosen random bitstring chosen to be the private key. Simultaneously, they present experimental results using a USRP [USR] device deployed in the 400 MHz band interacting with the GNU Radio software [gnu]. The oscillator drift has once again been mentioned as a negative effect forcing the authors to use merely the magnitude of the gains. As previously mentioned, by exploiting this drift, we were able to harvest more common randomness (see Chapter 5) in our work .

In [ASKMY07], Azimi-Sadjadi et al. use signal envelope as the source from which to extract the cryptographic key. They explore the deep fades of the signal to extract correlated bitstrings and introduce a new method called *secure fuzzy information reconciliators* to generate a robust key. They present a study based on the simulation of the wireless channel that confirms their approach. The authors also proposed to make practical measurements in the frequency domain. An experiment has been done in line-of-sight (LOS) and the reciprocity property has been confirmed. They claim that the fact of considering only the deep fades instead of the entire envelope allows this method to be more resistant to interference. Error-correction techniques are applied to correct noise errors and filtering to correct chattering.

Consequently, searching better algorithms for bit extraction became the main research direction. In their seminal paper, Mathur et al. [MTM+08] presented a new algorithm to extract shared secret bits from the environment. They use a technique combining level-crossings and quantization. They achieved an error-free key establishment rate of approximately **1 bit/sec** using off-the-shelf 802.11 hardware in a indoor wireless environment. These hardware platforms use coarse per-packet RSSI information. To the best of our knowledge, the authors were the first to evaluate the randomness of the bit-sequences produced by their method, showing they are suitable for the use as cryptographic keys. They used for this purpose the NIST test suite [BRS+10] and Maurer's universal statistical test for checking the entropy of the obtained sequences. The deployed radios are *half-duplex* due to hardware constraints. It was observed that in the time between two successive probes, the channel slightly changes. The channel estimates are quite correlated if the difference in time for different probings is very small. The authors firstly present the properties of a good key: *suitably long* and *statistically random* - accordingly, the bits should not show any statistical patterns that could be explored by an attacker. They first introduced the idea of studying the randomness of the generated bits and proposed the usage of statistical tests to test for various defects. They address the problem of estimating the trade-off between probability of error and rate of generation of secret bits using the level-crossings method. An important conclusion arising from their studies was that the order of secret-bit rate should not be expected to be great than the order of the maximum Doppler frequency for a certain threshold method. They also pointed out that in practice this value of key generation rate also depends on the channel probing rate, i.e. how quick both legitimate parties are able to send each

other probing signals. For experimental validation, the authors used the **magnitude of the tallest peak in the CIR**, which corresponds to the *dominant multipath* as the parameters of interest. The practical results showed that the algorithm performs very well both in static as in mobile setups. One of the drawbacks of this method is that the variation in average signal power produces long strings of ones and zeros, which basically means that the extracted entropy of the algorithm is too low and, subsequently, that an adversary would be able to easily guess the key and break the system. The authors explained this fact by saying that they are trying to include the effect of shadow fading (large-scale fading), which produces large but slow changes in the average signal power, used in the key extraction method. In order to cope with this problem, they subtracted an average of each trace from the original trace, which leaves only the small scale fading (see Section 2.2), corresponding to faster variations of the signal. The authors also explained how to act in the case where interference is present. According to them, this problem could be obviated by reducing the quantization levels in order to achieve improved robustness in the key generation process at the cost of lowering the key generation rate. We also deal with this issue in our work (see Chapter 6).

The idea of *joint randomness not shared by others* (JRNSO), where the communicating entities generate JRNSO bits from a channel impulse response (CIR) estimate using the JRNSO-bits for the generation of an encryption key, has already been presented [YMR+09]. Theoretical models have been proposed and the secret key rate has been indicated for different values of the signal-to-noise (*SNR*) ratio for a basic scenario. An improved system based on over-quantization has been introduced. The authors experimentally achieved the value on the order of **10 bit/sec** of key generation rate.

Other authors, like Premnath et al. [PJC+13], focused their efforts on evaluating the effectiveness of secret key extraction using RSS intensity values for the channel characteristics. Again, they used the idea that the time variation of the RSS values can be measured using off-the-shelf equipment on a per frame basis and later quantized. They showed that, under certain environments, the entropy might be too low due to lack of dynamic variations of the wireless channel, which is also a problem that we developed later in our work in Section 4.1. Moreover, they also observed that an adversary can cause predictable key generation in these environments. They sustained that high entropy is reached easily in a dynamic environment or when the devices are mobile. The NIST test suite is used for the randomness tests of the conducted experiments. We also used this suite in our work for similar purposes (see Section 6.3.3.3). They also implemented their extraction method in hand-held devices phones and in a MIMO-like sensor network. This last case gave raise to a high bit mismatch. In this work, the asymmetry and limited capabilities of the wireless hardware are mentioned as a drawback to the key generation process under real settings. The attacker is assumed to be only passive and is not able to jam the communication. Moreover the man-in-the-middle attack is not considered. Also very interesting is mentioning the possibility of authenticating the wireless devices by using certain physical and radiometric properties. The authors observe that different RSS quantizers have been proposed in the existing literature. They claim that the main difference among them consists in the number of thresholds and their value. The authors point out some causes for the mismatch in the obtained key bitstrings, such as presence of *noise* and *interference*, *hardware limitations*, *manufacturing variations*, *vendor-specific differences*, including differences in implementing automatic

gain control, and the *lack of sampling at the same time*, i.e., synchronization issues due to the half-duplex mode of communication in commercial transceivers. The CASCADE protocol is used for information reconciliation (cf. Section 2.3). The authors firstly present three performance metrics for the quality of the key:

1. Entropy: estimated using the NIST test suite's approximate entropy test;
2. Bit Mismatch Rate: ratio of different bits extracted from RSS quantization between Alice and Bob to the the total number of extracted bits;
3. Secret Bit Rate: average number of secret bits extracted per collected measurement after considering bit losses due to information reconciliation and privacy amplification.

Once again, it is mentioned that there is a trade-off between extracted entropy and bit rate. Their extractor algorithm, called Adaptive Secret Big Generation (ASBG), basically builds upon the one described in [MTM+08]. The main difference resides in the fact that the RSS measurements are divided into smaller blocks, for which the mean values and the thresholds are calculated separately. This allows the quantizer to adapt to the slow variations of RSS. Experiment validation was performed using wireless network cards operating in the 802.11g mode. Once again, RSS on a per frame basis was used to measure the variation of the wireless channel. The wireless card drivers report the RSS values as integers, and it is known that the calculation of RSS is vendor dependent. Each of the RSS measurements is quantized into one or more bits for secret key extraction. The environments tested were of three different types: stationary, mobile and intermediate. In a stationary environment, the authors found out that the variations of Alice and Bob's signals are primarily due to the hardware imperfections and thermal effects, as both effects aren't symmetric. Moreover, they claim RSS measurements in this type of environment contain very low inherent entropy. It is not possible, according to them, to extract secret bits at a fast rate in this type of setting. They achieved a rate of 7 to 8 minutes to generate a 256-bit secret key, which is very inefficient. In a mobile setting, a high degree of reciprocity was observed. The same satisfying degree of reciprocity and entropy was achieved in a place with several mobile intermediate objects. They proposed an attack on stationary environments. They called it the *predictable channel* attack. In a certain way, this attack has some common points with the one we had proposed in our 2010 paper [DLMdA10] and presented in Chapter 4. They claim that an adversary can cause *predictable* changes in a stationary environment and therefore inducing certain predictable values to the generated key. Moreover, the authors perform experiments with heterogeneous devices. They showed that despite bigger mismatching rate, secret key extraction is still reasonably possible due to the information reconciliation step. The authors benchmark their results in a comparison between the results in [ASKMY07],[MTM+08], [TM01] and [AHT+05b].

In [CPK10], Croft et al. extracted a secret key from a wireless environment despite the existence of *real-world non-reciprocities*. They further studied the trade-off between bit generation rate and bit disagreement rates. They presented a scheme using a ranking method to remove the non-reciprocities due specially to the transceiver hardware characteristics. Their method makes up for the difference in the transmit powers and RSSI circuit variations. Variations of scale are observed even with identical hardware. This is even more true with different hardware. This method

allows the extraction of **40 bits/second** for the key generation. Some of the non-reciprocities sources mentioned are the additive noise and differences in hardware, and they are the cause of bit disagreement. They propose a method they called adaptive ranking-based uncorrelated bit extraction (ARUBE), which consists of two stages: *interpolation*, which removes non-reciprocities caused by the half-duplex nature of the channel; and *ranking*, during which the non-reciprocities caused by differences in the hardware characteristics are reduced. Each receiver actually measures the RSSI, as many of the off-the-shelf equipment available in the market. This value has known to present an affine relationship with the channel gain, CG, i.e., $\text{RSSI} = c_1\text{CG} + c_0$, where c_1 and c_0 depend on the two nodes, and they originate on the difference between hardware brands or manufacturing differences in identical hardware. Such values are considered to be constant over the short periods of time required to generate a key from the channel (tens of seconds). In the quantization step, the authors also reinforce the notion that there is a trade-off between the probability of bit disagreement and the number of bits generated. Some experiments were performed in order to test their setup. Additionally, a very interesting study on the computational complexity of this method was performed and it was shown that is significantly smaller than that of the Diffie-Hellman traditional key exchange method, which requires the repetitive use of modular exponentiation. An entropy rate above 0.97 was achieved.

Wilson, Tse and Scholtz in [WTS07] put forward an idea to use the ultrawideband (UWB) channel pulse response between two transceiver as a source of common randomness using UWB channel models. They presented simulation results in order to determine the feasible key lengths and success rates of channel identification for UWB indoor channels. Indoor experiments have been performed and the timing synchronization error is pointed as a source of error. They claim that empirical studies of correlation between channel impulse responses under different conditions are critical in understanding how secure the system is. More study of the potential ability of enemy terminals to break the system is required. They also used the bit mismatch as a measure of the quality of their method. They obtained values from 50% up to 70% for the eavesdropper.

The problem of analyzing the physical layer in more detail has also been approached in [AP09]. The main goal of their work was to study the effect of shadowing. For this purpose, they employed a channel measurement system in a set of different environments. Path losses are extensively modelled and experimentally tested. They claim that the probability of path failure is strongly underestimated: a factor of two or higher in the current shadowing models is estimated for the underestimation. Measurements take place using *Crossbow TelosB* wireless sensor devices [cro] and are performed in open air environment characterized by having dense vegetation. RSS values are used for referring to the intensity of the signal. The devices operated in the 900 MHz and 2.4 GHz bands.

In [ZCP+14], the authors proposed a new system architecture for the secret key establishment problem which is also suitable for resource-constrained platforms. It is clear that a random number generator is a critical component in every cryptographic device. Therefore, an important security feature of the entire system design is a statistical test to provide entropy testing. Again, the authors proposed a method for *online entropy estimation* using NIST tests as in [BRS+10]. They identify and clarify potential failure sources in reciprocal channel estimations, such as bad synchronization, noise, nonlinearities, and too rapid movement. The authors conclude

that, unlike CASCADE [BS93], no information of the key material would be revealed if one uses the transmission of syndromes of binary codes during the information reconciliation phase of the protocol. Particularly, they applied BCH syndrome decoding for this purpose.

Further, the authors extended this idea by combining physical layer techniques and asymmetric cryptography [ZAW+14] in order to strengthen the overall system.

3.3. Antenna-based Methods

Other methods for key establishment have been proposed. The following methods are based on antenna diversity. They can be classified into Time-Varying Radiation Pattern Antennas, where the radiation pattern is technically manipulated in order to change with time, and variation in the number of used antennas.

3.3.1. Time-Varying Radiation Pattern Antennas

Other solutions were developed in order to achieve a secure key exchange even in the case when the *environment is not complex enough* or does not change sufficiently with time. The core idea is to create an artificial change in the environment by changing the radiation pattern in a controlled way during the transmission and reception of the probing signals.

In this context, the use of a very peculiar time-varying radiation pattern antennas was reported, as described in [AHT+05a, Ohi05, SHOK04]. The working principle of these antennas is presented in more detail in [SHOK04]. They are based on the *Harrington's Reactively Controlled Array*. This kind of antenna consists of an active dipole surrounded by six parasitic dipoles loaded with reactances. It has been first presented in 1978 [Har78].

The *Electrically Steerable Parasitic Array Radiator (ESPAR)* is a modified version of the Harrington Array in the sense that monopoles, instead of dipoles, are used, and the variable reactive loads (also called varactors) are integrated in the ground plane. These antennas have been thoroughly investigated for low-cost and small analog adaptive beamforming purposes.

We can define a m-Element ESPAR as an antenna with one active monopole and $m - 1$ passive or parasitic elements. These parasites are not directly connected to the transceiver circuit but simply terminated with independent variable reactors or varactors. Some control logic, using a microcontroller, is associated with the varactors, which allows to control their capacities. These varactors are a type of tunable load. A varactor diode, also known as varicap, has a variable capacity depending on the voltage applied across its terminals. This has, of course, influence on the radiation pattern produced by the array.

In [KO05] Kawakami et al. give deeper details about the functioning of this antenna. Radiation patterns are presented for different adjustable characteristics of these kind of antennas. A passive element located around an active element is loaded by a varactor, implemented with a reverse-bias varactor diode. Different configurations for the ground plane are studied. It is shown that the maximum gain in the horizontal direction is obtained for a radius of the circular ground plane about 0.5λ, where λ is the wavelength of the electromagnetic wave, and the length of the skirt about 0.25λ for the monopole variant and for seven-element ESPAR antennas, where each passive element is 0.25λ length.

In [SHOK04], Shun et al. further developed the subject of ESPAR antennas. They claim that its low-power consumption attributes, ease of fabrication and its fast beamforming ability makes them quite suitable for mass deployment. The theory of ESPAR antennas is presented in detail, its signal model and its adaptive beamforming algorithm performance is analyzed with simulation and experimental methods. They showed that ESPAR antennas are suitable for ad hoc networks or WLAN applications, where the performance is mainly influenced by the interferences from the neighboring mobile terminals, like laptops.

Taillefer et al. in [TC07] describe in detail the functioning of the ESPAR antennas and specifically how to electronically steer beams and nulls of the radiation pattern in different directions. The usage of Direction of Arrival (DoA) methods allowing high precision and resolution estimation of an incoming source are explained and a signal model for this purpose is presented.

In [HHO05], the authors present a technique for designing a miniature of the conventional ESPAR antenna, being used as a direction finder. They employ a special technique consisting in immersing the central active element in a dielectric cylinder, being the parasitic element at the circumference of the cylinder, and decreasing the radius of the ground plane to that of the circumference. Measurements results are shown for a frequency of 2.484 GHz. Measured and simulation results were shown to be identical. An improvement of the performance in comparison with traditional antennas was obtained.

In [Ohi05], Ohira proposes the usage of ESPAR antennas in order to achieve time variation in the transmitted (or received) signal amplitudes for the purpose of establishing a common secret key between two parties. He claims that this antenna increases the spatial randomness that can never be predicted in practice by any other party and presents some proof-of-concept experiments in an indoor environment. The eavesdropper is even given the possibility of having a high-gain antenna to pick up the wave leakage. In [Ohi05], the idea of leakage is unfortunately not explored deeper and it is not totally clear if it is meant the reradiation or simply the signal that both legitimate parties send. In Chapter 4, we focus on the detailed study of how to use the passive reradiation by both Alice and Bob to recover the key. The ESPAR antenna is considered to equip an access point (AP), whereas the user terminal (UT) has a simple omnidirectional antenna. The AP and UT emit constant-amplitude waves. The same frequency is used in both directions, using time division multiplexing (TDD). In detail, the AP transmits a constant amplitude wave not carrying any key information while simultaneously controlling the varactors randomly. The RF signal source excites the main radiator, which induces a coherent current on each parasite element through electromagnetic mutual coupling among them. The antenna therefore works as a phased array. Next, the UT transmits back a signal. Important here is that the AP receives the incoming signal while controlling the varactors again in the same way. This means that the radiation diagram variation is the same during transmission and reception of the channel probe signal. Experiments were performed in a metal-walled room causing different multipath reflections. The body of the person in charge of measurements provides a time-varying condition. Thermal noise is mentioned already a a source of discrepancy. To cope with this, a threshold of 2 dB range was considered, inside of which the generated bits would be ignored, in a signal with approximately 20 dB span. A drawback of this method is that the microcontroller randomly steering the varactors should be able to generate randomness by itself in the chip.

In their seminal work [AHT+05a], Aono et al. proposed to explicitly use ESPAR antenna and its *beam-forming capabilities* in order to increase the fluctuation of the radio channel characteristics. Experimental validation was performed and they were able to extract robust secret keys from the received signal strength indicator (RSSI) profile. As a motivation, they postulate that it would be easy to break the secret keys under an environment with a small fluctuation of the channel characteristics and propose the usage of smart antennas in order to vary electronically the fluctuation of channel characteristics. They mentioned that digital beam-forming array antennas require elaborate control circuits and a considerable amount of power, making them not suitable for commercial solutions. The gain of an ESPAR antenna is about 6 dBi. For a 8-bit resolution control voltage, the number of radiation patterns that an m-element ESPAR antenna can form is, according to the authors, $(2^8)^{m-1} = 2^{48}$, with $m = 7$. The key generation process is described in detail: the ESPAR antenna access point (AP) fixes a beam pattern during a certain period of time where she transmits a series of packets. Bob (user terminal - UT) receives these packets and calculates their RSSI values. Bob will send some packets back while Alice keeps the beam pattern constant. She also calculates the RSSI profile. Alice changes the beam pattern and the procedure is repeated. The binary quantization is quite simple: a threshold value is defined and all values *under* this threshold are considered to be 0; all values *over* this threshold are considered to be 1. It is mentioned that a small number of beam patters will allow an eavesdropper located near the access point to be able to deduce information by near-field probing of the ESPAR antenna, which allows him to find out the beam pattern. The number of beam patterns, 2^{48}, and the presence time of a beam pattern of few milliseconds makes it much difficult for an eavesdropper to deduce this information. Experiments with 1 mW power and a frequency of 2.4 GHz were performed. The bit disagreement has been used as a quality measure of this technique. A low disagreement rate was observed between the AP and the UT, whereas between the UT and the eavesdropper the opposite happens. It is shown that the technique also works under a dynamic environment and also under different heights for the AP to the other parties. The keys between the UT and the eavesdropper were observed to be sufficiently independent.

Imai et al. [IKM06] build upon the work of Aono [AHT+05a]. They claim Aono's method still lacks a rigorous security analysis. In order to cope with this issue, they present a complete security analysis for the scheme. Only passive attacks are considered. However, their setup works under the condition that an attacker does not obtain more information on the data exchanged by the legitimate parties than a certain threshold. They recommend only to use this technique in a protected environment, such as offices with restricted access. The attacker would be assumed to be out of that room. They point out that an attacker could get enough information in the case that the environment is a simple cube made of some material with known electromagnetic properties and containing just the parties and himself inside. He could be able to simulate the wave propagation in this environment and guess the key. Though, the environment was very simple and no objects were considered. Still, in the case that an ESPAR with a true random generation is used, this attack will not work.

In [KYL08], Hashimoto et al. recall the usage of the ESPAR antenna and give a detailed description of the protocol for key exchange. They present a few experiments in an indoor environment and use the results of the experiments and also computer simulation in order to compare the error-correcting codes concerning key

disagreement using the mutual information extracted from the environment.

3.3.2. Multiple Antennas

Other methods for secret key establishment are based on the simultaneous usage of several antennas. Antenna diversity is a technique employed in telecommunications to mitigate the lateral effects of the multipath channel. Due to deep fade, as previously explained in Section 2.2, it can happen that the incoming signal may be too low. The usage of a set of multiple antennas allows that at least one antennas receives a copy of the signal with enough energy to be correctly demodulated.However, lately, their usage for the purpose of key establishment has also been seriously considered. Thorough information about antenna diversity can be found in [VA87].

A complete introduction to the theory of MIMO (*multiple-input multiple-output*) can also be found in [TV05] and [GSS+03]. MIMO systems make use of many antennas and is explored by 4G technologies and IEEE 802.11n for most recent standards in LANs and cellular networks. In [LCR05] and [LR05], Li et al. explore the redundancy of array transmissions using MIMO to make sure that Eve cannot perform blind identification. The sender is assumed to have several antennas and the propagation channel to be Rayleigh flat fading. An attacker is also given the possibility of using multiple receiving antennas. Multipath interference is assumed to be available and the channel difference is exploited, rather than the noise difference, in order to achieve information-theoretic secrecy.

Other methods using MIMO systems were proposed to enhance security [KV08]. The usage of the inherent properties of MIMO channels has been suggested, as well as some characteristics from the different parties, to ensure security under certain conditions, as described in detail in [GN05] and [KV08].

In [LHR06] and, in more detail, in [LHR07], Li, Hwu and Ratazzi suggest to use an array redundancy-based approach with low probability of interception (LPI) as an approach for physical-layer security. Accordingly, spread spectrum techniques are the most widely used techniques for low probability of interception/detection (LPI/LPD). Using J antennas, Alice sends to Bob a symbol sequence $b(n)$ assumed to be independent identically and uniformly distributed with zero-mean and unit variance. Alice wants to transmit a symbol sequence $b(n)$ to Bob. $\mathbf{h}$ is the channel response for the channel between Alice and Bob and $(.)^H$ represents the Hermitian of the matrix. With a transmit-beamforming-like scheme, Alice transmits $\mathbf{s}(n) = \mathbf{w}(n)b(n)$, where $w_i(n)$ denotes the weighting coefficient of the i-th transmit antenna during the symbol interval n. Bob, equipped with one antenna, will receive $x(n) = \mathbf{h}^H\mathbf{s}(n)$ whereas Eve, equipped with M antennas, gets $\mathbf{x}_e(n) = \mathbf{H}_e\mathbf{s}(n) + \mathbf{v}_e(n)$, with $\mathbf{h}$ being a $J \times 1$ channel vector, $\mathbf{H}_e$ of $M \times J$. $\mathbf{h}$ and $\mathbf{H}$ are assumed to be different, due to multipath interference, and Eve is assumed not to know these values. In order to prevent Eve from estimating the channel between Alice and Bob, no training sequence should be transmitted. A strategy for the transmission and receiving procedure from Alice to Bob is explained. The goal is to calculate $\mathbf{w}(n)$ from the estimation of the channel $\mathbf{h}$ in order to prevent Eve from performing blind deconvolution. A strategy for this is presented in their paper, as well as some simulations and experiments.

Some authors extended the ideas of Section 3.1 to the case of multiple antennas.

In [LP07], Liu and Poor made a similar approach to secrecy as the one explained in Section 3.1. They propose outer and inner bounds on the secrecy capacity region

of a generally *non-degraded Gaussian broadcast channel* with confidential messages for two users, where the transmitter has t antennas and each user has one single antenna. They proposed to use the so-called dirty-paper secure coding strategy in order to achieve the secrecy capacity region of this particular channel.

In [NG05], Negi and Goel proposed an ingenious method for secret communication. The idea is to introduce artificial noise in the message such that the receiver's channel is not affected. This could be done when the transmitter has several antennas or one single antenna, but a few so-called "helper" nodes are available. The knowledge about the eavesdropper's location is not assumed and the secrecy of this scheme does not depend on the secrecy of the channel characteristics. In all situations, it is assumed that the eavesdropper has only one antenna. The idea is to transmit artificial noise in the null space of the intended receiver's channel, thus not affecting the legitimate receiver, rather only the eavesdropper's channel. For the case of several helper nodes, the key point is that the helper nodes transmit a weighted signal whose contribution will cancel just at the intended receiver while the transmitter is transmitting the secret signal.

This work has been extended to the case where there are several colluding eavesdroppers, which can be modeled has an adversary with multiple antennas. In [GN05], it is assumed that the channel state information (CSI) is publicly available and cannot be used to obtain a secret key. Furthermore, it is also not required that the eavesdropper's channel is worse than the legitimate channel. The key idea is quite similar to the one presented in [NG05]: add artificial noise to the information signal such that it lies in the null space of the receiver's channel. The effect of the number of antennas at the receiver, N_R, and at the eavesdropper, N_E, is considered, and the number of transmit antennas, N_T, is taken constant. For the case when $N_R = N_E$, the secrecy capacity attains a maximum at a value of $N_R < N_T$. In this case, it is shown that even if the eavesdropper comes closer to the transmitter, secret communication is still possible.

In [KV08], the authors develop the previous studies by pondering the case where $N_R = N_T = N_E$. The eavesdropper's channel is even consider to have a higher signal to noise ratio (*SNR*) than the legitimate channel. Hereby it is proposed that the transmitter uses a singular value decomposition of the legitimate channel matrix, perform a low density parity check (LDPC) encoding of the date and add artificial noise. The single column vectors of the channel matrix seen by the eavesdropper are not orthogonal to one another; therefore, the received signal corresponding to each transmitted signal is corrupted by the channel noise and by the projections of the other transmitted signals. This is called *interchannel interference*. This effect increases with the number of used antennas.

Methods to decorrelate two closely spaced monopoles for MIMO can be found in [DBR05].

In [KWWE07], Khisti et al. generalize the Wyner's wiretap channel [Wyn75] for secret-key distribution over wireless links to the case when the sender, the receiver and the eavesdropper have multiple antennas and an upper-bound on secrecy-capacity for any *SNR* for the MISO case (when the receiver has only one antenna) is calculated.

The case of SIMO (single input, multiple output) is analyzed by Khisti et al. in [PB05]. They conclude that the use of multiple receive antennas provides an advantage with respect to a single-antenna channel. The authors extend this work and analyze the MIMOME (multiple input, multiple output, multiple eavesdropper)

wiretap channel in [KW10]. In these cases, all parties are equipped with an array of antennas. The secrecy capacity of the MIMOME channel is found and analyzed. They characterize the case when an eavesdropper oppose the possibility of secure communication by making the secrecy capacity to be zero.

3.4. Jamming-based Methods

Jamming is usually considered to be a malicious technique developed to destroy a legitimate communication between two parties by lowering their *SNR*. The opponents basically introduce noise in the same frequency band that the communicating parties are using. Spread spectrum is a common technique employed by the users to avoid or reduce the influence of jamming, as an attacker would have to emit signals in much broader bands. Lately, the possibility of using jamming for the purpose of key establishment has been pondered. *Jamming-based* methods make use of this usually "bad intentional" technique in order to obtain secrecy. The main idea is to try to degrade the eavesdropper's channel in order to achieve a higher *SNR* for the legitimate users than for the eavesdropper.

In [TY07], the authors consider the general *gaussian multiple access wire-tap channel*. Achievable rates and outer bounds on secrecy capacity for certain scenarios have been established and it has been shown that the multiple-access nature of the channel can be used for secrecy purposes. A method called *cooperative jamming* has been introduced in order to increase the achievable secret rate. This is done by enforcing some users to jam the eavesdropper's channel.

The key idea of [JYK+07] is to make the eavesdropper incapable of decoding the secret wireless message. The scenario uses two access points that are assumed to be connected through a secure (e.g. wired) connection. This method has been given the name *Shout to Secure*. The intentional induction of noise-like interference has been proposed. One more legitimate party is needed in this scenario - usually called Carol. Consider that Bob and Carol are connected via a wired communication. Alice wants to transmit securely, while Eve is trying to eavesdrop the signal. Carol should firstly give Bob a random sequence and then "shout out" that same signal, while Alice is transmitting. While interference is created, Bob is the only party capable of extracting Alice's signal. There has been a shift of the problem of key distribution between Alice and Bob to a problem between Bob and Carol. Quantum cryptography could be used for the alternative secure connection. However, it is pointed out that this scheme has a problem when Eve is equipped with a high directional antenna (see Section 2.1.1). She could point it directly to Alice, avoiding the interferences.

Further *jamming-based* techniques are presented in [XTZW05]. It is claimed that no single measurement is sufficient for reliably classifying the presence of a jammer. This requires enhanced detection schemes that can remove ambiguity when detecting a jammer. Several attack strategies that a jammer can perform have been introduced and some models have been proposed. A few statistics for detecting this jamming attacks have been presented. They are based on detecting anomalies regarding the normal behavior in the channel based on different features of the signal:

- signal strength: based on RSSI measurements;
- carrier sensing time: the time the channel seems to be busy is measured;

- packet delivery ratio: the ratio of packets that are successfully delivered to a destination compared to the total number of packets sent. It can be computed at the receiver by calculating the ratio of the number of packets that pass the CRC check, or at the sender by having the receiver send back an acknowledgment packet.

More approaches to jamming-based methods can be found in [XWTZ04] and [WSS03].

3.5. Device-based Methods

Most authors use these methods for the purpose of *party/device authentication*. When a radio device receives a signal coming from a transmitter, there are several factors that influence the received signal at the receiver. Radio Frequency (RF) features can be classified into *channel-specific* ones, as already explained in Section 2.2, and *transmitter-specific* or *device-dependent* ones. We shall here say that we employed device-dependent resources in order to extend the source of entropy of *our secret key establishment method*, as we will see later in more detail in Chapter 5.

Due to its nature, wireless networks are specially vulnerable to many identity-based attacks. E.g., an attacker might set his device to use forged MAC addresses to impersonate a specific client or to create any false identity.

In order to cope with this problem, some authors pondered the possibility of using device-dependent data, i.e. information that depends on the transmitter hardware, for the purpose of transmitter authentication. This area is called device identity management.

In Brik et al. [BBGO08], this property is referred to as *radiometric identity* or *RF fingerprinting: minor variations in the analog hardware of transmitters are manifested as idiosyncratic artifacts in their emitted signals*. Consequently, they can be used to unequivocally identify a signal's device-of-origin. It is a property of the devices similar to biometric characteristics in humans. Both define identity as the collection of observable properties depending on the individual's constitution. The authors developed an interesting technique to identify the source network interface card (NIC) through passive radio-frequency analysis. The method they proposed uses tiny imperfections of the transmitter hardware (acquired during the manufacturing) which are transmitter-specific and whose consequence is observable in the emitted signals. In this case, RF identification is possible because of benign hardware imperfections inherent to the analog component of a NIC's transmitter. These imperfections are also called *impairments*. The authors pointed out the following impairments sources: quadrature errors, self-interference, *frequency offset* (which we used later in Section 5.2) and amplitude clipping. Machine-learning tools are used for classification. The authors developed a method they called PARADIS (Passive RAdiometric Device Identification System). PARADIS defines a signal's signature in terms of structure related to the properties of the used modulation types. PARADIS uses a classifier used to convert signatures to NIC MAC addresses. Like in all classification methods, there must be a training stage, where a wireless NIC signatures is extracted and recorded in a data bank. An identification stage is then implemented, where the features of the device-under-test is compared with the features saved in a data bank. Experimentation results confirmed the feasibility of this technique.

In [FC06], Faria and Cheriton proposed a new method for device identification. Their method uses signal strength information (RSSI levels) reported by access points as identification feature. Therefore, a signalprint is the signal strength characterization of a packet transmission. As already explained thoroughly in Section 2.2, these are strongly correlated with the physical location of clients. Experimental results confirming the theory are provided.

Device fingerprinting has been used in [BRC07] and [KBC05]. The main goal of radio fingerprinting is the detection of signal features that form a valid fingerprint valid for each single radio device. In [BRC07], Rasmussen and Capkun presented a study showing the feasibility of radio fingerprinting for wireless sensor nodes using a hardware device.Through fingerprinting, one can make associations between observed messages and their senders. Therefore, replay attacks might be avoided by using device identification. Five different features extracted out of the radio signal transient were used for the creation of the device fingerprints.

In [KBC05], Kohno et al. introduced the new area of remote physical device fingerprinting, using a certain small, microscopic deviation in the device hardware, called *clock skews*. It exploits the fact that modern computer chips all show this kind of characteristic. The techniques do not require any modification to the fingerprinted devices. The attackers exploited the device's *TCP timestamps option clock* or *TSopt clock* through wired connections.

Later, this idea has been extended for the identification of GSM Mobile Phones in a recent paper by Hasse et al. [HGB13]. Their findings fall in the domain of *mobile forensics*. They introduced *time-based patterns of modulation error* as a unique device-dependent feature and carefully removed random effects of the wireless communication channel on GSM devices. They used two USRP N210 devices operating in synchronized MIMO mode to collect the signals with a 900/1800 MHz GSM antenna. Machine learning methods have, as usually in this field, been utilized. Therefore, there is a training stage, during which the phones were placed close to the receiver; it follows then a test stage, when the mobile phones were placed at a different location. The main question is basically what makes a good feature. For the purpose of device identification, it seems clear that the priority should lay in extracting characteristics which remain stable over different dimensions and especially over time. It is of utmost importance to identify and remove all aspects that introduce random behavior. The signatures were given to a linear Support Vector Machine (SVM) for classification. The used features were based on the modulation information (I/Q signals - see Section 6.3), namely the magnitude error (ME), phase difference (PE), Error Vector (EV) and the length the Error Vector Magnitude (EVM). These were the common error metrics describing the precision of a modulated signal. Given the high precision of GSM systems, they proposed to use characteristic error pattern over the time of a normal burst as a device-dependent, still non-environment dependable, feature. The RF hardware introduces stable deterministic deviations at specific times of a burst, being a consequence of, e.g., fluctuations of the power amplifier. According to the authors, the results were quite encouraging.

3.6. Other Interesting Wireless Security Schemes and Applications

The methods presented in this section are designed to operate alongside other wireless security protocols, adding *defense in depth*. They are not meant to be methods for generating a key or transmitting a secret message.

In [XJ10], the authors propose to use multi-antenna APs to determine the directions from which an incoming signal arrives. They use this information - called angle-of-arrival (AoA) - to construct signatures that identify each client in a multipath indoor environment. This allows the AP to drop packets coming from clients physically located outside a building or office. In order to test their setup, the authors make experiments using USRP2 devices and equipped them with several antennas. They claim that while readily available from commodity hardware, RSS is very coarse compared to physical-layer information, making it very prone to error if few packets are available. They also claim that their method could be as accurate as GPS for client location.

They extended their work in [XJ13]. They use their AoA information to construct an AoA signature unique to each client and very hard to reconstruct. An attacker would need to know the location of all obstacles in the vicinity of the AP and client or to be located under five centimeters of the client's antennas. This is again the application of the multipath principle. The combined direct path and reflection path AoAs form the unique signature for each client. They developed their method in order to mitigate WiFi spoofing attack attempts. The literature about determining AoA for multipath signals is extensive, mostly based on the MUSIC (Multiple Signal Classification) algorithm, as explained in [VBBH05].

Multipath channel models can be even used for the spatial location of movement using the signal strength on a wireless link, like explained in [WP11].

There is still the problem of *identity* in cryptography. In [CGMO09], the authors launch the study of cryptographic protocols where the identity of a party is derived from its geographic location. They lay a solid foundation for the problem of *secure positioning* and even show how to realize secure multiparty computation using their method. The question is now how to achieve secure positioning in the real-world scenario using, e.g., wireless networks. This was done in [CH06]. The authors suggest a mechanism for the secure position computation and verification of positions of wireless devices, based on the measurements of the time of radio signal propagation. However, no experimentation was provided in this work.

In some cases, estimating the WiFi signal strength of several AP can allow to build a WiFi signal strength mapping inside a building that can give precious information about the current location of an object measuring this intensity. This WiFi signature map is used for a robot in the building to estimate its own location according to the signal strength he is measuring at a certain position. They observed that the bigger the number of visible access points, the small the localization error. For more details, see Biswas et al's paper [BV10]. It uses techniques from the above mentioned *secure positioning*.

There is an extensive literature on the subject of wireless sensor networks routing protocols. However, security issues in this field tend to be ignored or postponed. A complete analysis of the security of these networks is presented in [KW03]. Attacks and countermeasures have been listed. The same topic is also considered in [ABV06].

Here, a formal security model based on the simulation paradigm has been proposed.

In [FC04], Faria et al. propose a technique providing location-based access control. The main goal of the so-called authentication handshake is to limit wireless coverage to the intended service area, imposing a maximum distance for authentication, which is a function of the density and placement of access points. In other words, one seeks that clients located outside a certain area should not be allowed to successfully complete the handshake. Accordingly, an attacker located outside the intended coverage area would need impractical amounts of antenna gain.

Similarly, in [CCH06], the authors propose three methods for authentication before employing the Diffie-Hellman (DH) Protocol for key exchange over a radio link. One of these methods is based on the interesting idea of using the distance between the parties to authenticate them. It was called DH with distance bounding (DH-DB). This protocol ensures that the DH protocol is performed only in case that there are no other parties that are closer to A or to B than themselves.

4. Vulnerabilities and Attacks

In this chapter, we propose and analyze two types of attacks on fading-based key exchange protocols: an attack on the protocol (Section 4.1), where we explore the scarce entropy in the environment in order to reconstruct the signals that both legitimate parties receive; and an attack on the implementation (Section 4.2), where we focus on an inevitable property of all antennas: their reradiation leakage. The results in this chapter are published in [DLMdA10].

4.1. Environment Reconstruction Attacks

In this section, we describe an attack where an adversary, Eve, can precisely reconstruct simple environments by using the signals she passively collects during the execution of fading-based key exchange protocols between two parties. Knowing the exact position of the reflecting objects, she can then calculate the signals Alice and Bob receive.

In order to understand this attack, we shortly review the necessary concepts about channel modeling, as described in detail in Section 2.2.2. Radio channels are usually represented by their impulse response. As fading-based key exchange protocols take place in a short period of time, we can realistically assume that the channels we examine are *static* or *quasi-static*. Therefore, we have the time-invariant multipath fading channel between a sender Alice and a receiver Bob given by the impulse response

$$h_{\mathrm{AB}}(t) = \sum_{i=1}^{n} \rho_i \delta(t - \tau_i),$$

an impulse train, where the τ_i and ρ_i are the latencies and phasors of the direct and scattered signal components, respectively. The scattered components are assumed to arise by reflections of the sent signal. Reciprocity states that the channel characteristics are the same during the coherence time of the channel if the roles of the sender and the receiver are exchanged (cf. Section 2.2.4), thus

$$h_{\mathrm{BA}}(t) = h_{\mathrm{AB}}(t) =: h(t).$$

Typical coherence times for fading channels take values around 2.5 ms [TV05]. It was observed in [HHY95] that the shared entropy that can be extracted from the common channel impulse response $h(t)$ might be used to generate a common secret between Alice and Bob. Some practical implementations have already been designed (see Section 3.2).

The elementary requirement for reciprocity-based key exchange to be secure is the presence of a fading channel that quickly decorrelates in space due to multipath interference. More precisely, the channel responses $h_{\mathrm{AE}}(t)$ and $h_{\mathrm{BE}}(t)$ an eavesdropper measures should be uncorrelated to $h_{\mathrm{AB}}(t)$ and $h_{\mathrm{BA}}(t)$, respectively. Generally, the spatial decorrelation is implicitly assumed in models describing fading channels (cf. Section 3.2). The most common stochastic processes used to model the randomness of fading channels are the Rayleigh and Rician processes. They have been shown to be appropriate to model fading channels in urban or rural areas [OOKF68]. Such models are utilized to analyze and estimate typical error patterns in wireless communication.

To the best of our knowledge, the issue of the amount of uncorrelated randomness that can be extracted from multipath fading channels [MTM+08, YMR+09] has so far failed to model *how much* uncorrelated randomness can be extracted from multipath fading channels.

It seems infeasible to provide security guarantees for reciprocity-&-fading-based key exchange. We illustrate this by providing a model that instantiates a fading channel for which the reciprocity-based key exchange protocols become insecure under reasonable assumptions. Even though this model is overly idealized, it demonstrates the fundamental intricacies of wireless key exchange. Our model exhibits the following properties:

- the environment is planar and there is only a finite and small number of point-shaped specular reflectors (objects). They show isotropic reflection characteristics, i.e., they reflect equally in all the directions. Each reflector R_i has its distinct attenuation factor α_i, which is the portion of the incident power that is reflected. These values are chosen uniformly from $(0, 1]$;

- there are two parties, Alice (A) and Bob (B), each sending and receiving one signal, and a passive eavesdropper, Eve (E), who can merely listen to the signals that Alice and Bob inject in the environment. Each of the parties has one antenna;

- we consider only the first-order reflections of signals. Furthermore, in order to simplify the analysis, we neglect the interference of other signals and noise.

We assume that Eve knows the geographical positions $p_{\mathrm{A}} = (x_{\mathrm{A}}, y_{\mathrm{A}})$ of Alice and $p_{\mathrm{B}} = (x_{\mathrm{B}}, y_{\mathrm{B}})$ of Bob relative to her own position $p_{\mathrm{E}} = (x_{\mathrm{E}}, y_{\mathrm{E}})$. This might, for instance, be the case if Alice is an access point and Bob is a static user terminal [HIU+08]. However, she has no further information about the environment. Figure 4.1.1 is an example of such an elementary environment containing five objects, represented by small circles, whose positions are unknown to Eve. If just one signal $s(t)$ is sent from Alice to Bob and vice versa, Alice and Bob will measure $h_{\mathrm{BA}}(t) * s(t)$ and $h_{\mathrm{AB}}(t) * s(t)$, respectively, whereas Eve will measure $h_{\mathrm{AE}}(t) * s(t)$ and $h_{\mathrm{BE}}(t) * s(t)$ (cf. Section 2.2.2). To simplify our analysis, we assume that $s(t)$ is an impulse, i.e. $s(t) := \delta(t)$, and that Eve can recover $h_{\mathrm{AE}}(t)$ and $h_{\mathrm{BE}}(t)$ such that the peaks can

still be separated. In Figure 4.1, we consider the channel and the corresponding power delay profiles measured by the Alice, Bob and Eve.

The information Eve learns from $h_{\mathrm{AE}}(t)$ is, at the first glance, insufficient to retrieve significant information about Bob's measurement, i.e. $h_{\mathrm{AB}}(t)$, since, from her view, Bob's measurement is undetermined by several degrees of freedom. So, Bob's measurement is subject to a significant amount of uncertainty seen as randomness by Eve.

The bottom line, however, is that, in this model, given the channel impulse responses $h_{\mathrm{AE}}(t)$ between Alice and Eve and $h_{\mathrm{BE}}(t)$ between Bob and Eve, Eve is enabled to uniquely recover the channel impulse response $h_{\mathrm{AB}}(t)$ within the scope of her measuring accuracy. We will briefly describe how this attack works.

Let

$$h_{\mathrm{AE}}(t) = \sum_{i=1}^{n} \rho_i \delta(t - \tau_i)$$

be the impulse response of the channel A-E, i.e., the signal Eve receives when Alice sends an impulse $s(t)$. Without loss of generality, we assume that the first peak, $\rho_1\delta(t-\tau_1)$ represents the direct path between Alice and Eve. All further multipath components $\rho_i\delta(t-\tau_i)$, $i > 1$, have traversed a distance

$$d_i = d(p_{\mathrm{A}}, p_{\mathrm{E}}) + (\tau_i - \tau_1) \cdot c,$$

where c is the vacuum speed of light. So,

$$d_i = d(p_{\mathrm{A}}, p_{R_i}) + d(p_{R_i}, p_{\mathrm{E}}) \tag{4.1}$$

defines an equation for some reflector R_i that accounts for this multipath component. The set of solutions for Equation (4.1) with respect to p_{R_i} defines an ellipse. Likewise, every multipath component of h_{BE} provides an ellipse equation. The possible loci of the reflectors lie at the intersections of the ellipses obtained from $h_{\mathrm{AE}}(t)$ and $h_{\mathrm{BE}}(t)$ and given by

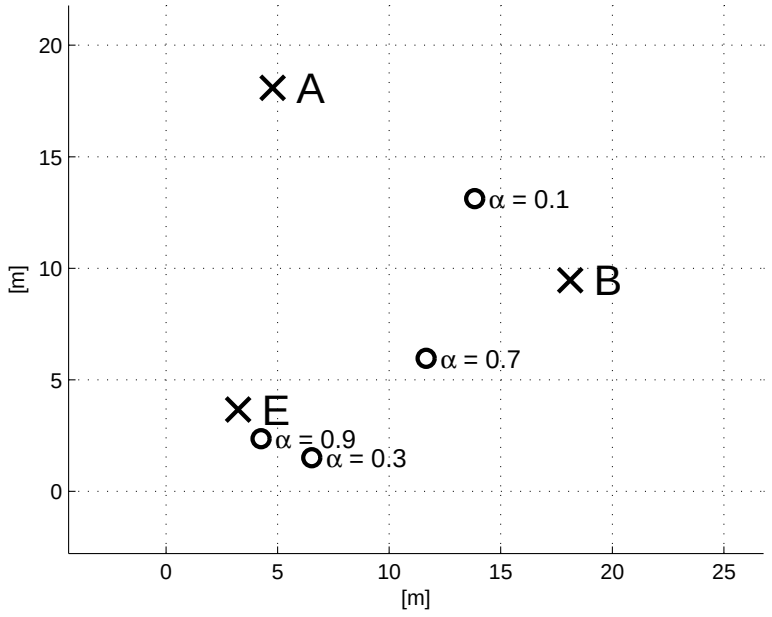
$$\begin{cases} d_{i_{\mathrm{A}}} = c \cdot \tau_{i_{\mathrm{AE}}} = d(p_{\mathrm{A}}, p_{R_i}) + d(p_{R_i}, p_{\mathrm{E}}) \\ d_{i_{\mathrm{B}}} = c \cdot \tau_{i_{\mathrm{BE}}} = d(p_{\mathrm{A}}, p_{R_i}) + d(p_{R_i}, p_{\mathrm{E}}). \end{cases} \tag{4.2}$$

This system of equations has at most $4n^2$ solutions, where n is the number of reflectors in the environment. This is due to the fact that the maximum number of intersections between two families of k and l confocal ellipses, i.e, ellipses having common focal points, is $4kl$.

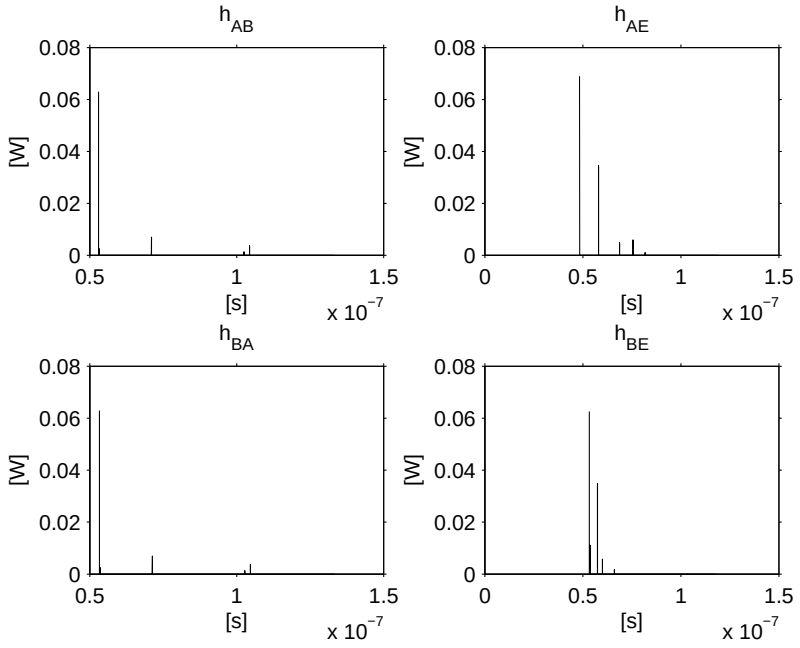
Alice and Bob transmit the same sounding signal $s(t)$. Bob measures $h_{\mathrm{AB}}(t)$, Alice $h_{\mathrm{BA}}(t)$ and Eve the two channel responses $h_{\mathrm{AE}}(t)$ and $h_{\mathrm{BE}}(t)$. An example of the power delay profiles of the channels is shown in Figure 4.1.2.

When a direct path is present, the primary peak represents this path in each impulse response. Using the delay times between the primary peak and the reflected components, Eve can estimate the lengths of the signal paths of the reflected components.

Until now, Eve has just used information from the power delay profile's horizontal axis (time). Nevertheless, she can also use the information provided by the vertical axis (power) in order to reduce the degrees of freedom for the solutions. She knows the transmitted power P_{t} and receives a power P_{r}, which is attenuated by:



4.1.1: Randomly generated environment with reflectors. The circles indicate the positions of the reflectors. The numbers next to the reflectors are their attenuation factors.



4.1.2: Power delay profiles at A (upper left), B (lower left) and E (right side, upper from A and lower from B).

Figure 4.1.: Example of an environment and corresponding received signals by Alice (A), Bob (B) and Eve (E).

- free space propagation by a factor of $\alpha \cdot d^{-2}$, where α is the free-space propagation attenuation constant and d the traversed distance;
- reflection in object R_i by the reflector attenuation factor α_i.

She can now check for each point of intersection if it is a valid position for a reflector by testing whether it has approximately the same α_i on both assumed paths, i.e., solving (4.3) in relation to α_i and searching for similar values.

$$P_\mathrm{r} = P_\mathrm{t} \cdot \underbrace{\alpha \cdot d(p_\mathrm{A}, p_{R_i})^{-2}}_{\text{propagation}} \cdot \underbrace{\alpha_i}_{\text{reflection}} \cdot \underbrace{\alpha \cdot d(p_{R_i}, p_\mathrm{E})^{-2}}_{\text{propagation}} \tag{4.3}$$

If this is the case, it means that the objects are in the positions denoted by a square in Figure 4.2.1. In a final step, knowing each α_i, Eve simulates the signal propagation from Alice to Bob in her reconstructed environment to obtain an estimated $h^*_\mathrm{AB}(t)$ of $h_\mathrm{AB}(t)$, as illustrated in Figure 4.3.

We have implemented this model in MATLAB® and run simulations with several parameter sets.

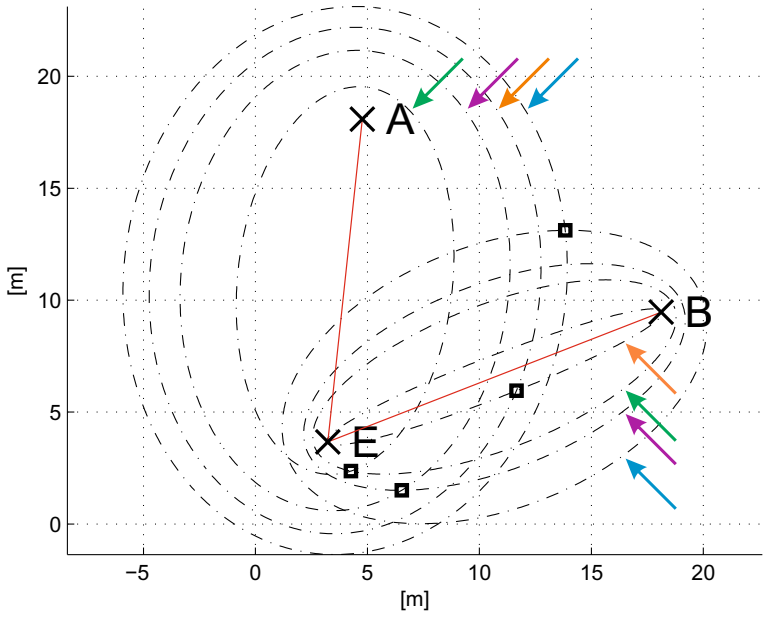
4.2. Side-Channel Attack: Reradiation Leakage

This attack targets side effects that appear in the implementation of the protocol in real devices. A new attack against the wireless key exchange on the physical layer, called *reradiated wireless side-channel (RRW-SC)* attack, is presented and analyzed.

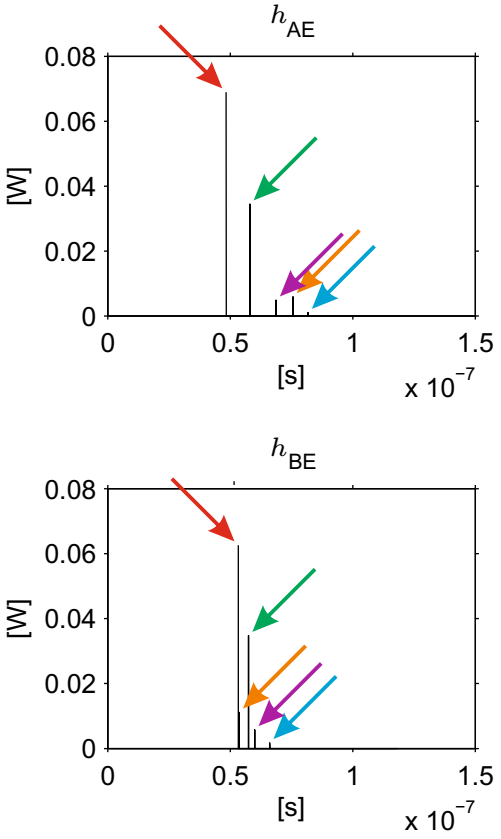
First, we will review some concepts which are necessary for obtaining a method for the derivation of *upper bounds* on the distance to a receiving antenna where it is still practically possible for an adversary to recover a useful amount of information by considering only the reradiation of the receiving antenna in use.

The general model for an antenna in the receiving mode is described in Section 2.1.2.2. Accordingly, its Thévenin equivalent model consists of a simple electrical circuit with the antenna impedance $Z_\mathrm{A} = R_\mathrm{A} + jX_\mathrm{A}$ and the input impedance of the receiver $Z_\mathrm{T} = R_\mathrm{T} + jX_\mathrm{T}$ serially connected to the voltage generator V_T representing the induced voltage by the incident wave. In general, the resistive part $R_\mathrm{A} = R_\mathrm{r} + R_\mathrm{L}$ of Z_A consists of two components, where R_r represents the reradiation resistance and R_L the loss resistance of the antenna. In a conjugate matching condition, i.e. $R_\mathrm{r} + R_\mathrm{L} = R_\mathrm{T}$ and $X_\mathrm{A} = -X_\mathrm{T}$, between the antenna and the receiver, the maximum amount of power is transmitted to the receiver. In this case, expressions for powers P_T, P_r, and P_L delivered to R_T, R_r, and R_L, respectively, as well as the collected (induced) power P_c can be simply calculated. From these expressions follows that from the total amount of power P_c induced in the antenna, one half is transmitted to the receiver (P_T) and the other half is partly reradiated (P_r) and partly dissipated as heat (P_L). The *reradiating factor*, ρ, as defined in Section 2.1.2.2, usually ranges between 0.4 and 0.8.

Thus, the power reradiated is an important phenomenon that can leak information about the received signal. Let us consider the following example: Eve is equipped with a receiver with a high-gain antenna (see Section 2.1) directed towards Bob's receiver in line-of-sight. The signal wave Bob receives from Alice (containing information about the secret key) will be partially reradiated. Eve will try to capture this signal in order to recover the key. Therefore, Bob and Alice should make Eve's intentions more difficult to achieve by implementing appropriate countermeasures.



4.2.1: Environment estimated by Eve by performing the attack in the environment depicted in Figure 4.1.1.



4.2.2: Power delay profiles, $h_{\mathrm{AE}}(t)$ and $h_{\mathrm{BE}}(t)$, measured by Eve. Using the information on both axis (time and power), she can find the location of the objects in the environment.

Figure 4.2.: Environment reconstruction attack performed by Eve. The red arrows point to the signals which correspond to the direct paths. All other arrows associate two peaks in the power delay profile with the respective possible locations (an ellipse), indicated by the same color.

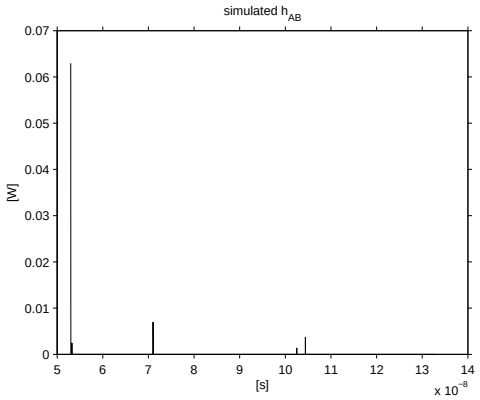


Figure 4.3.: Power delay profile, $h^*_{\mathrm{AB}}(t)$, between Alice an Bob as estimated by Eve. For comparison, see Figure 4.1.2 (upper left).

In order to estimate the threat of the RRW-SC, we introduce the concepts of *attacking region*, *intermediate region* and *secure region*. Figure 4.4 illustrates these regions. The attacking region is defined as the area around Bob's antenna where Eve, equipped with receiver equipment, needs to be located such that she still has a *practical chance*, given by an acceptable bit error rate, *BER*, or word (symbol) error rate, *WER*, of recovering the secret key coming from Alice by using solely the passive reradiation from Bob's receiving antenna, i.e. the RRW-SC. It is bounded by the *maximal attacking range*, D_{attack}. This distance corresponds to the distance where a receiver would demodulate a M-ASK signal with a *BER* equal to a certain threshold. We define the threshold of $BER = 0.2$ as a good practical limitation for recovering the key. Note, however, that an attacker knowing that a bitstring of length $L = 128$ has a number $BER \cdot L$ of bit errors, still has to try $\binom{L}{\lceil BER \cdot L \rceil}$ combinations. If $L = 128$ and $BER = 20\,\%$, this corresponds to $\binom{128}{26} \approx 2^{90}$ keys.

The *secure region* is the region where Eve has no practical advantage of analyzing the reradiation signals for finding the secret key. The *minimal distance of (complete) security*, D_{secure}, is the distance such that $BER = 0.5$, which gives Eve as much possibility of getting the key by analyzing the reradiation signal as she would have by randomly guessing the key. Therefore, this area is defined as the area where $d_{\mathrm{BE}} > D_{\mathrm{secure}}$.

The *intermediate region* is defined as the region around Bob where it is still realistically feasible for Eve to recover the key. Thus, this area is defined for all values d_{BE} such that $D_{\mathrm{attack}} < d_{\mathrm{BE}} < D_{\mathrm{secure}}$.

For the estimation of D_{attack} and D_{secure}, we employ an *energy budget* procedure. This technique uses the variation of the energy propagated in the environment. The first step is the expression of the average energy per bit at the receiver, denoted by E_{bR}, which is caused by free space propagation of electromagnetic waves. In terms of the average energy per bit at the transmitter, denoted by E_{bT}, this *range equation* (cf. [Bla90]) has the following form:

$$E_{\mathrm{bR}} = aE_{\mathrm{bT}} = \frac{G_{\mathrm{T}}}{4\pi}\frac{\lambda^2 G_{\mathrm{R}}}{4\pi}\frac{E_{\mathrm{bT}}}{d^2} = \frac{\alpha A_{\mathrm{R}} E_{\mathrm{bT}}}{d^2}. \tag{4.4}$$

Here, G_{T} and G_{R} are the gains of the transmitting and receiving antennas in the direction of propagation, d is the range from transmitter (Tx) to receiver (Rx) and λ the wavelength of the electromagnetic radiation (EMR). The equation (4.4) can

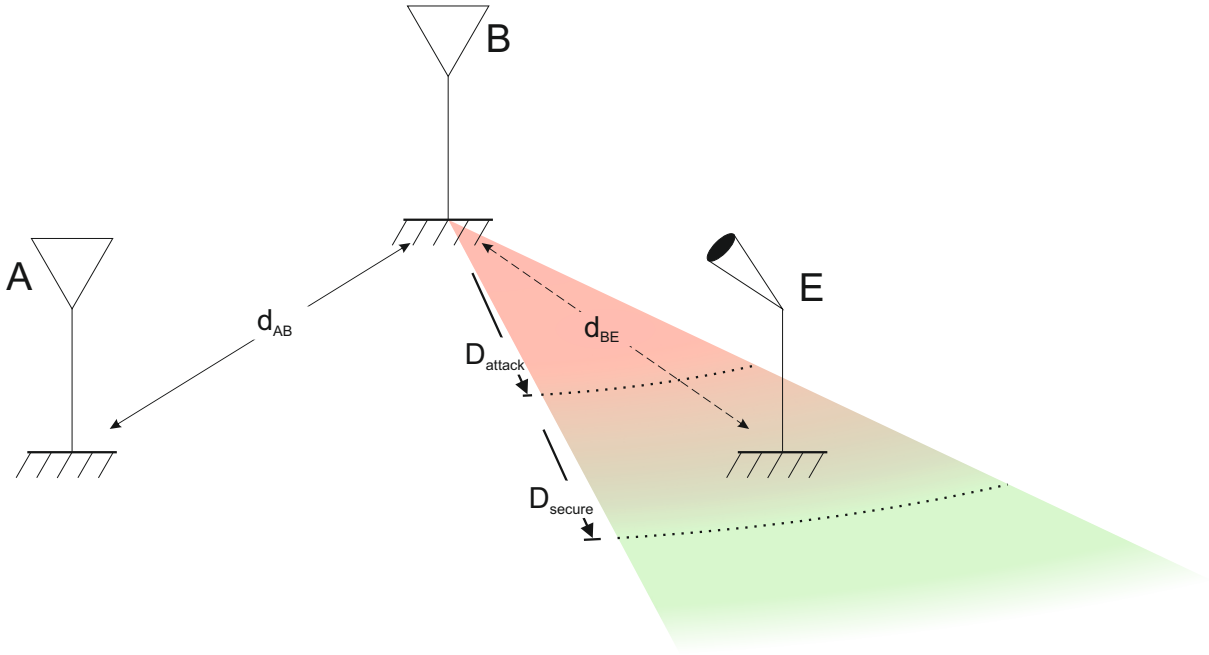


Figure 4.4.: Illustration of *maximal attacking range* (D_{attack}) and *minimal distance of security* (D_{secure}). Alice sends a signal which is reradiated by Bob. Eve collects the reradiated signal. She can reconstruct with good quality the signal that Bob receives if she is inside the circle of radius D_{attack}. This quality degenerates with the distance. For a distance bigger than D_{secure}, it is virtually impossible for Eve to reconstruct that signal.

also be expressed in terms of average power, S, rather than of average energy, by replacing E_{bR} and E_{bT} by S_{bR} and S_{bT}, respectively. The factor a in (4.4) represents the *energy (power) attenuation* of EMR between Rx and Tx, which can be expressed by the product of the effective area of the receiving antenna $A_{\text{R}} = \frac{\lambda^2 G_{\text{R}}}{4\pi}$ and the spherical density of the transmitting antenna gain $\alpha = \frac{G_{\text{T}}}{4\pi}$.

Any receiver at absolute temperature T_{R} will always contaminate the received signal with additive white Gaussian noise (AWGN) of power spectral density $N_0 = kT_{\text{R}}$, where k is the Boltzmann constant ($k = 1.38 \times 10^{-23}$ [J/K]). This thermal noise is due to unavoidable thermal fluctuations of electrons in the first stage of amplification at electronic receivers. Actual receivers will have a somewhat larger value of thermal noise power spectral density, N_0, expressed as

$$N_0 = FkT_{\text{R}}, \tag{4.5}$$

where F is a number known as the noise figure of the receiver. Ideally, $F = 1$, but it happens to be larger in practice. For a high-quality receiver, it is comprised in the range of 2 to 5.

Generally, the quality of digital communication can be expressed by the average *BER* in the received data. In wireless communication systems, its value depends on numerous influencing factors. The most important are: implemented modulation/demodulation and error control encoding/decoding techniques, the information bit rate R_{b}, the average power S_{T} of Tx, the occupied frequency bandwidth W around the carrier frequency f_{c}, as well as EMR interferences, obstacles and reflectors in the zone of influence around Tx and Rx. By considering only the ubiquitous

influencing factors, the *signal-to-noise ratio* (*SNR*) in the presence of additive white gaussian noise (AWGN), given by $\frac{S_\mathrm{R}}{S_\mathrm{AWGN}}$, can be expressed as

$$SNR = \frac{S_\mathrm{R}}{WN_0} = \frac{aS_\mathrm{T}}{WN_0}, \tag{4.6}$$

where $S_R = aS_\mathrm{T}$ is the average signal power and $S_\mathrm{AWGN} = WN_0$ the thermal noise power at the input of Rx. By inserting (4.4) and (4.5) in (4.6), we have

$$SNR = \frac{\alpha A_\mathrm{R}}{FkT_\mathrm{R}} \frac{S_\mathrm{T}}{Wd^2} = Q\frac{S_\mathrm{T}}{Wd^2}, \tag{4.7}$$

where $Q = \frac{\alpha A_\mathrm{R}}{FkT_\mathrm{R}}$ represents the *basic quality* of the wireless AWGN channel. In practice, there are many other influencing factors that degrade Q, like the conduction and dielectric efficiency of antennas, taking in account losses at the input terminals and within the structure of the antenna. Such degradation factors are very difficult to model and compute, but they can be determined experimentally. Thus, the practical basic quality Q_p of a wireless channel has always a smaller value than Q and can be expressed by the experimental corrective factor $e < 1$ as $Q_\mathrm{p} = eQ$.

For example, the basic quality of an omnidirectional wireless channel ($G_\mathrm{R} = G_\mathrm{T} = 1$) in the 433 MHz ISM-band (*Industrial, Scientific, and Medical* radio bands) with the carrier signal wavelength $\lambda = 0.7\,\mathrm{m}$ and a receiver at room temperature (20 K) and noise figure $F = 2$ amounts $Q = 0.384 \times 10^{18}\,[\mathrm{m^2/J}]$. The basic quality of the wireless channel decreases with the growing carrier frequency. For example, in the 2.4 GHz ISM-band an omnidirectional wireless channel ($G_\mathrm{R} = G_\mathrm{T} = 1$) with the carrier signal wavelength $\lambda = 0.125\,\mathrm{m}$ and a receiver at room temperature and noise figure F = 2 has a basic quality of $Q = 1.223 \times 10^{16}\,[\mathrm{m^2/J}]$. When using a transmitter with average power of $S_\mathrm{T} = 100\,\mathrm{mW}$ and a bandwidth $W = 1\,\mathrm{MHz}$ in the 433 MHz ISM-band, the dependence of *SNR* on the Tx – Rx distance d can be, according to Equation (4.7), expressed as $SNR = 3.84 \times 10^{10}\,\mathrm{d}^{-2}d^{-2}$. For a channel in the 2.4 GHz ISM-band and the same values of S_T and W, this dependency is given by $SNR = 1.22 \times 10^{9}\,\mathrm{d}^{-2}$.

The most adequate detection technique for modeling the secret key extraction in the wireless key exchange on the physical layer is the detection of an M-ary amplitude shift keying signal (M-ASK, also called pulse amplitude modulation M-PAM). The exact average word (symbol) error probability (*WER*) in dependence of *SNR* for the M-ASK detection is given by [Pro02]

$$WER = \frac{(M-1)}{M}\,\mathrm{erfc}\left(\sqrt{\frac{3SNR}{2(M^2-1)}}\right), \tag{4.8}$$

where $\mathrm{erfc}(x)$ denotes the complementary error-function[1] and M the number of chosen amplitude levels in a signal sample labeled by $Q = log_2 M$ key bits. For example, from (4.7) and (4.8) and for the values of S_T, W, λ, F, G_R and G_T chosen above, the value $WER = 1 \times 10^{-2}$ will be attained at the distance of $d = 17\,\mathrm{km}$ in the 433 MHz ISM-band, whereas in the 2.4 GHz GHz ISM-band the same value of *WER* will be attained at the distance $d = 1\,\mathrm{km}$, if the number of detected amplitude levels is $M = 8$. We can rewrite Equation (4.8) as

[1] $\mathrm{erfc}(x) = \frac{2}{\sqrt{\pi}} \int_x^\infty e^{-t^2}\,\mathrm{d}t$

$$SNR(WER) = \frac{2}{3}(M^2 - 1)\left(\mathrm{erfc}^{-1}\left[\frac{M}{M-1}\,WER\right]\right)^2. \tag{4.9}$$

Under the above mentioned conditions, the $SNR(d_{\mathrm{AB}})$ at Bob's receiver for the signal coming from Alice is, according to Equation (4.7)

$$SNR(d_{\mathrm{AB}}) = Q_{\mathrm{AB}}\frac{S_{\mathrm{TA}}}{W_{\mathrm{AB}}d_{\mathrm{AB}}^2}, \tag{4.10}$$

where Q_{AB} is the basic quality of the wireless channel between Alice and Bob, S_{TA} the average power of Alice's transmitter, and W_{AB} the bandwidth used on this channel. The $SNR(d_{\mathrm{BE}})$ at Eve's receiving antenna for the signal reradiated from Bob's receiving antenna with a reradiating factor $\rho = 1$ (for a worst-case scenario estimation) is, according to Equation (4.7),

$$SNR(d_{\mathrm{BE}}) = \rho Q_{\mathrm{BE}}\frac{S_{\mathrm{RB}}}{W_{\mathrm{BE}}d_{\mathrm{BE}}^2}, \tag{4.11}$$

where Q_{BE} is the basic quality of the wireless channel between Bob and Eve, S_{RB} the average power of Alice's signal at Bob's antenna, and W_{BE} the bandwidth used on the *RRW-SC*. Using (4.6) and some other expressions defined above, the term S_{RB} in (4.11) can be replaced by $SNR(d_{\mathrm{AB}})W_{\mathrm{AB}}N_{0\mathrm{AB}}$ so that

$$SNR(d_{\mathrm{BE}}) = \rho\frac{G_{\mathrm{TA}}G_{\mathrm{RB}}G_{\mathrm{rrB}}G_{\mathrm{RE}}}{F_{\mathrm{E}}kT_{\mathrm{R}}}\left(\frac{\lambda}{4\pi}\right)^4\frac{S_{\mathrm{TA}}}{W_{\mathrm{BE}}d_{\mathrm{AB}}^2d_{\mathrm{BE}}^2}, \tag{4.12}$$

where G_{TA} is the gain of Alice's transmitting antenna, G_{RB} the gain of Bob's receiving antenna, G_{rrB} the reradiating gain of Bob's receiving antenna, G_{RE} the gain of Eve's receiving antenna, F_{E} the noise figure of Eve's receiver, and T_{R} the absolute temperature of the first stage amplification circuit in Eve's receiver. Finally, (4.12) can be written as

$$SNR(d_{\mathrm{BE}}) = Q_{\mathrm{rr}}\frac{S_{\mathrm{TA}}}{W_{\mathrm{BE}}}\frac{1}{d_{\mathrm{AB}}^2d_{\mathrm{BE}}^2}, \tag{4.13}$$

where Q_{rr}, which is a function of the frequency, represents the basic quality of the *RRW-SC*.

Alice and Bob's interest will be to reduce Q_{rr}, while Eve will try to improve it. Eve can increase G_{RE} of her antenna connecting it to a high quality receiver (with small noise figure F_{E}) whose first stage of amplification is cooled. The best possible practical improvement of Q_{rr} in this way can be attained by choosing the following *best quality parameters* of a RRW-SC: highest reradiating factor of $\rho = 1$, receiving antenna gain of $G_{\mathrm{RE}} = 1000$ obtained using a high quality reflector antenna connected to the perfect receiver with $F_{\mathrm{E}} = 2$ (a typical value for a very good receiver), whose first stage of amplification is cooled in liquid helium up to $T_{\mathrm{R}} = 4\,\mathrm{K}$. Since Alice and Bob usually do not know each other's position, they will use omnidirectional antennas, which means that the following values of $G_{\mathrm{TA}} = G_{\mathrm{RB}} = G_{\mathrm{rrB}} = 1$ can be assumed for best quality parameters. On the other hand, Eve will be confronted with some unavoidable disturbances. The coincidental radiation of Alice's transmitter as well as other ubiquitous EMR interferences will more or less decrease the basic quality Q_{rr} of the RRW-SC. By replacing the best quality parameters in Equation (4.12) and by omitting the influences of all degradation

factors on Q_{rr}, the best *SNR* value, SNR^*, on the RRW-SC, for given λ, S_{TA}, W_{BE}, d_{AB} and d_{BE} can be calculated. Replacing the SNR^* in (4.8) directly gives the word error probability with which Eve recovers the secret key under best achievable conditions above assumed.

If, in (4.8), the *WER* is determined by some chosen value WER^* and d_{BE} is taken as a free variable, the upper bounds D_{attack} or D_{secure} on a RRW-SC can be obtained. The value of WER^* determines the capacity of the digital communication channel using ASK signaling (without using of any kind of error control codes). *WER* defines the amount of symbols which are received incorrectly, i.e., which have *at least* one bit error per block of $log_2(M)$ bits. If we assume a uniform distribution of bit errors between the minimum and maximum amount of bit errors in a string of length $N\log_2(M)$ for a given *WER* value, we can define the bit error rate, *BER*, as the average between these values. For N blocks of $\log_2(M)$ symbols, the minimum amount of errors would happen if just one bit is wrong per wrong symbol, i.e. a total of $N \cdot WER$ wrong bits. On the other hand, the maximum amount of errors would happen if all bits in a symbol are wrong, i.e. a total of $N \cdot \log_2(M) \cdot WER$ wrong bits.

Taking the average of both, we get the following relation, which we use to relate *BER* and *WER*:

$$BER = \frac{1+\log_2(M)}{2\log_2(M)}\,WER. \tag{4.14}$$

Inserting (4.14) in (4.9) , we have

$$SNR(BER) = \frac{2}{3}(M^2-1)\left(\mathrm{erfc}^{-1}\left[\frac{M}{M-1}\cdot\frac{2\log_2(M)}{1+\log_2(M)}BER\right]\right)^2. \tag{4.15}$$

Combining Equations (4.13) and (4.15), one has

$$D_{\mathrm{attack}} := d_{\mathrm{BE}}\Big|_{BER=0.2} = \sqrt{Q_{\mathrm{rr}}(f)\frac{S_{\mathrm{TA}}}{W_{\mathrm{BE}}}\cdot\frac{1}{d_{\mathrm{AB}}^2 SNR(BER)|_{BER=0.2}}} \tag{4.16}$$

and, by making $BER = 0.5$,

$$D_{\mathrm{secure}} := d_{\mathrm{BE}}\Big|_{BER=0.5} = \sqrt{Q_{\mathrm{rr}}(f)\frac{S_{\mathrm{TA}}}{W_{\mathrm{BE}}}\cdot\frac{1}{d_{\mathrm{AB}}^2 SNR(BER)|_{BER=0.5}}} \tag{4.17}$$

In order to illustrate the magnitude of D_{attack} and D_{secure} in practice, a few examples are evaluated for different parameters. For all the cases, we take $S_{\mathrm{TA}} = 100\,\mathrm{mW}$, $W_{\mathrm{AB}} = W_{\mathrm{BE}} = 1\,\mathrm{MHz}$, and best quality parameters of the RRW-SC. Typical values for D_{attack} and D_{secure} are shown in Table 4.1.

Because of symmetry in (4.13), d_{AB} and D_{attack} (or d_{AB} and D_{secure}) can be exchanged. For example, in the 433 MHz ISM-band, if d_{AB} amounts 700 m, than $D_{\mathrm{attack}} = 471\,\mathrm{m}$ for $M = 8$. If, for the same conditions, we make $d_{\mathrm{AB}} = 471\,\mathrm{m}$, than $D_{\mathrm{attack}} = 700\,\mathrm{m}$.

In Figures 4.5 and 4.6, we depict the dependency of D_{attack} and D_{secure} on several parameters we can control, namely frequency and M. It is clear that Eve will have an advantage if lower frequencies are used and smaller number quantization levels are considered, since, for the same distance between Alice and Bob, d_{AB}, she would

f [MHz]	d_{AB} [m]	M	D_{attack} [m]	D_{secure} [m]
433	1000	4	1400	9260
433	1000	8	666	3507
433	1000	16	330	1697
433	700	8	471	2425
2400	1000	4	46	301
2400	1000	8	21	114
2400	100	4	456	3014
2400	100	8	217	1142
2400	100	16	107	553

Table 4.1.: Typical values of D_{attack} and D_{secure}.

be able to reconstruct the key from larger distances, $d_{\mathrm{BE}} < D_{\mathrm{attack}}$, from Bob's antennas. This is due to the fact that, as already mentioned, the quality of the wireless channels declines with the frequency.

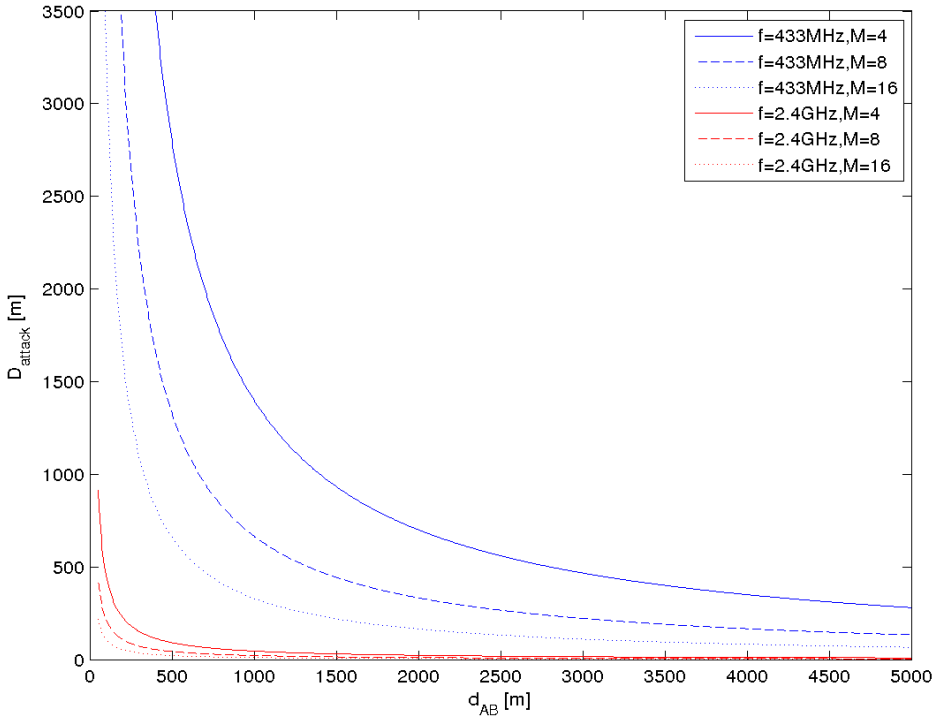


Figure 4.5.: D_{attack} dependency on d_{AB}, f and M.

In Figure 4.7, we visualize the radius of each regions for a certain d_{AB}, for both 433 MHz and 2.4 GHz bands.

The analysis of the figures and expressions above clearly shows that the passive reradiation side-channel represents a serious threat for the wireless key exchange on the physical layer. The reradiation side-channel can be always improved by using many synchronized receivers placed at different positions around Bob's receiver. This kind of attack will not be considered here. The development of effective countermeasures against reradiation side-channel attacks remains an open problem. Possible

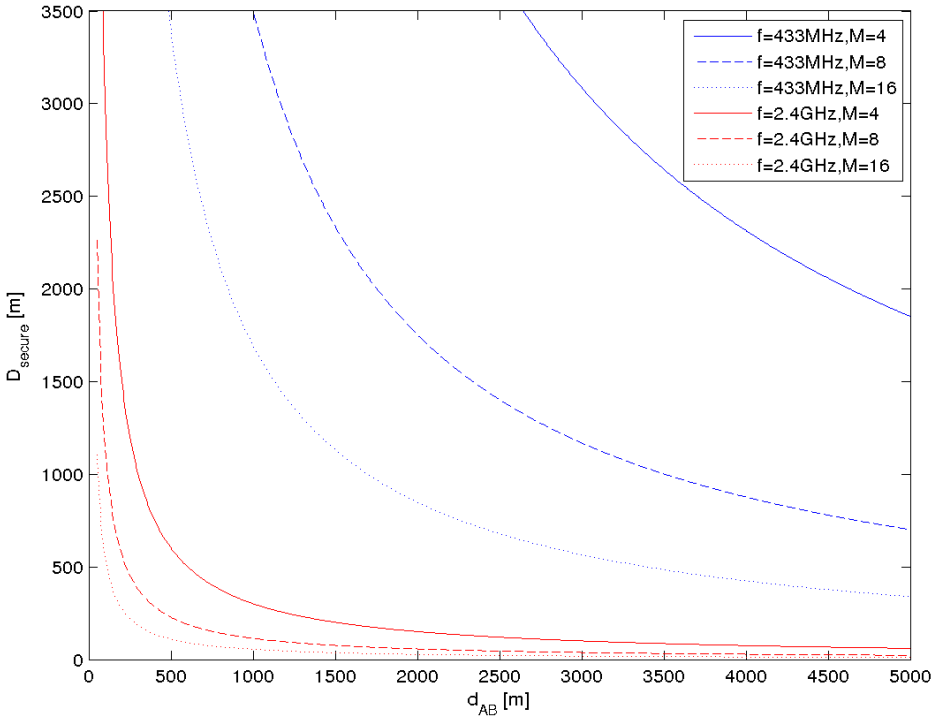


Figure 4.6.: D_{secure} dependency on d_{AB}, f and M.

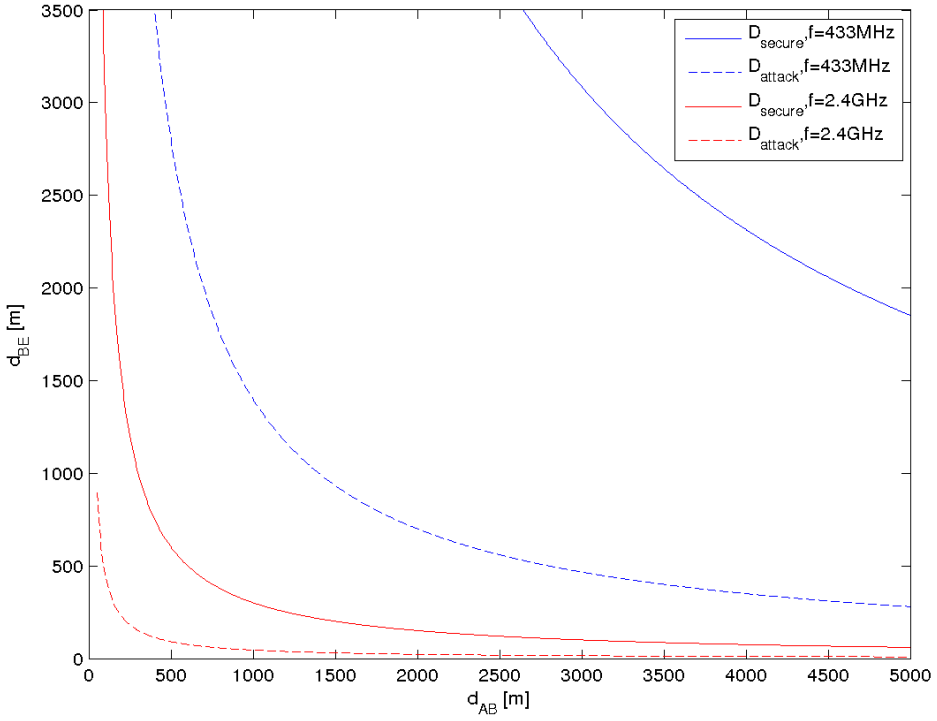


Figure 4.7.: D_{attack} and D_{secure} for $M = 4$.

candidate countermeasures include the use of reradiation suppressing electrical and opto-electrical antennas or even different jamming techniques.

4.2.1. Theory

4.2.2. Experimental Setup

In this section, our experimental efforts to measure the reradiation side-channel are described. We tried to confirm in practice that Bob's antenna leaks enough information that can be captured and properly used by Eve. Due to the fact that the energy of the reradiated signal is predictably very low, an experimental setup that maximizes the reradiated power and minimizes all other signals' interferences is designed. This means that our setup must basically satisfy two conditions:

- minimize the power of the signals arriving to Eve originated in sources other than Bob's antenna, i.e. the signal coming from Alice in line-of-sight and all signals coming from Alice through reflections or scattering;
- maximize the energy of Alice's signal reradiated by Bob's antenna, which means that the pairs Alice and Bob, as well as Bob and Eve, should be in line-of-sight positions.

In order to fulfill these requirements, we performed our experiments using an anechoic chamber as described in Section 4.2.3. This chamber is made of ferrite walls, which have the property of absorbing the incident electromagnetic waves within a certain frequency range, strongly reducing the reflection and scattering components [FRA].

4.2.3. Hardware

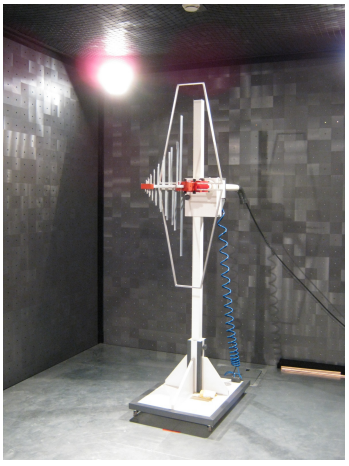
In our experimental setup, Alice consisted of a USRP2 transmitter [USR] and a corresponding controlling laptop, as shown in Figure 4.8.1. Eve was equipped with a directional antenna [Ant] (Figure 4.8.2) pointed towards Bob's antenna (Figure 4.8.3). In order to collect the measurement traces, Eve's antenna was connected to an oscilloscope with 2.5 GSamples/s of sampling rate.

Three experiments were performed:

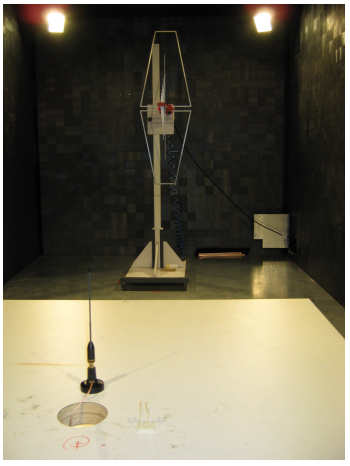
1. Alice was placed inside the anechoic chamber in position A' (Figure 4.9); nothing was placed in position B (Figure 4.9); Eve just measured the received signal;
2. Alice was placed outside the anechoic chamber in position A; nothing was placed in position B and Eve's antenna (point E) was pointed towards point B. This way, points A and B are in line-of-sight position, as well as points B and E; however, A and E have no line-of-sight between them;
3. a $\lambda/4$ dipole antenna (Figure 4.8.3) was placed at point B without any other Bob's receiver components (i.e. antenna in open circuit). Alice and Eve remained as described in the previous item.

For all the experiments, we collect the signals measured by Eve when Alice emitted a 430 MHz sinusoidal signal of 100 mW power. This frequency value is within the

4.8.1: Alice's USRP2 transmitter with laptop (outside the chamber).



4.8.2: Eve's directional antenna (inside the chamber).



4.8.3: Eve measuring Bob's omnidirectional antenna (on the table inside the chamber) reradiation.

Figure 4.8.: Alice, Bob and Eve's experimental setup.

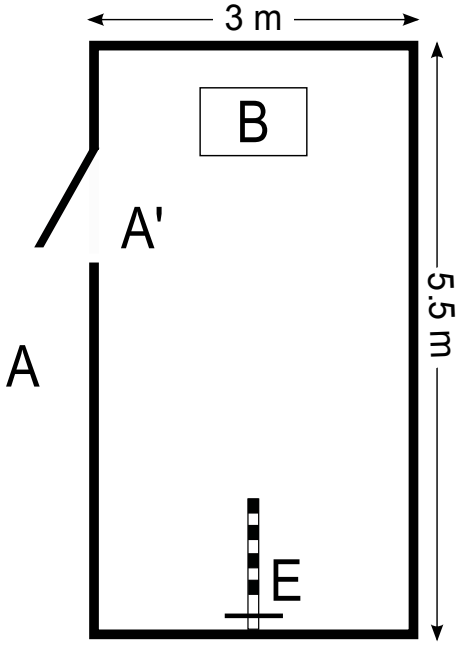


Figure 4.9.: Schematics of the anechoic chamber with positions of Alice (A or A'), Bob (B) and Eve (E).

range where ferrite absorbent material is more effective. Each trace measurement had a duration of 50 µs. Assuming that the ferrite walls absorbs the majority of the energy, Eve would be able to detect Bob's reradiated signal superimposed with unavoidable residual reflection and diffraction components. For each experiment, we gathered a set of traces. With those traces, the resulting average signal was calculated. It is worth noting that all traces were aligned in both axis, due to the uprising trigger set up (x-axis alignment) and due to the DC component extraction (y-axis alignment).

4.2.4. Results

Firstly, we eliminated the DC component (or average value), $x_{\mathrm{DC}}(t)$, of the signal $x(t)$ limited in to the interval T. This component can be expressed as

$$x_{\mathrm{DC}}(t) = \frac{1}{T}\int_{T} x(t)\mathrm{d}t. \tag{4.18}$$

The AC component $x_{\mathrm{AC}}(t)$ is given by $x_{\mathrm{AC}}(t) = x(t) - x_{\mathrm{DC}}(t)$. The discrete case is quite similar, with the respective changes. The DC-component, or average value, $x_{\mathrm{DC}}[n]$ of a signal $x[n]$ limited to N samples is given by

$$x_{\mathrm{DC}}[n] = \frac{1}{N}\sum_{i=1}^{N} x[i]. \tag{4.19}$$

The AC-component $x_{\mathrm{AC}}[n]$ is therefore given by $x_{\mathrm{AC}}[n] = x[n] - x_{\mathrm{DC}}[n]$.

We discarded the DC component of the signals since we were only interested in the supposed small variations due to the change in the environment. Afterwards, we calculated the energy of the signal. The energy of a continuous signal $x(t)$, represented by $E\{x_{\mathrm{AC}}(t)\}$, during a certain period T is given by

$$E\{x_{\mathrm{AC}}(t)\} = \int_{T} x_{\mathrm{AC}}^2(t)\mathrm{d}t. \tag{4.20}$$

Since the oscilloscope gives us the discrete measured trace of a signal, represented here by $x[n]$, we used the following expression for the computation of the energy:

$$E\{x_{\mathrm{AC}}[n]\} = \sum_{i=1}^{n} x_{\mathrm{AC}}^2[i]. \tag{4.21}$$

The value of the energy measured from those traces and given by the Equation (4.21) is shown in Table 4.2 for all the experiments.

4.3. Discussion

The *environment reconstruction attack* demonstrates the principal unreliability of implicitly assuming spatial uncorrelatedness of joint measurements: using the reconstructed environment, Eve can now simulate the key exchange between Alice and Bob and, thereby, recover the *secret* impulse response $h_{\mathrm{AB}}(t)$.

Exp.	Alice	Bob	Energy
1	A'	None	3.9675
2	A	None	2.436×10^{-3}
3	A	Antenna	2.950×10^{-3}

Table 4.2.: Measured energy by Eve.

Concerning the *reradiation leakage attack*, according to Table 4.2, when comparing the results for the experiments 1 and 2, it can be concluded that, as expected, the anechoic chamber absorbs a great part of the signal energy coming from Alice. From the experiments 2 and 3, it becomes clear that the insertion of an antenna at point B (the extreme case of a reradiating receiving antenna in open circuit) is responsible for a significant increase (about 17 %) of the energy received by Eve. Thus, we also experimentally demonstrated that reradiation is a side-channel that must be taken into consideration in the development of key exchange protocols based on the channels' physical properties.

4.4. Conclusion

In certain applications, key exchange on the physical layer seems to be a promising and viable alternative to key exchange protocols whose security is based solely on computational assumptions. However, the conditions under which it can be securely implemented are still to be rigorously defined. In this chapter, the security of such schemes was examined in detail and two new attacks against this physical primitive were presented. The first attack is strictly based on the potential simplicity of the wireless channel. Under too simple environment conditions, an eavesdropper can reconstruct the environment and, therefore, extract the common secret key established between the two legitimate parties. The other attack is based on the wireless systems physical properties and is considered to be a side-channel attack to reciprocity-based schemes. We theoretically established under which conditions an eavesdropper equipped with a receiver system has some chance to recover a common key from the observation of the reradiated signal emitted from one of the protocol parties. We concluded that, in order to avoid leakage by reradiation, higher frequencies for channel sounding should be used, as this considerably reduces Eve's power to extract the key. We also presented the results of our efforts to experimentally prove the feasibility of this attack.

5. Improvements to the Protocol

Insufficient entropy in the environment and unavoidable antenna reradiation leakage convey important information about the received signals that can be used by an attacker, as explained in Chapter 4. Both attacks may, however, be hardened by introducing a new source of entropy in the system. In Section 3.6, we have seen how one can use the intrinsic and irreproducible hardware properties of the devices for authentication purposes. In this chapter, we present a new method consisting of combining the small differences in the clocks of both legitimate parties' devices with the fading properties of the wireless channel for the purpose of generating a shared secret key. This method tackles the challenge of increasing the difficulty involved in reconstructing the secret key for an adversary. The problem of harvesting more randomness, even when the fading-based key exchange protocol is performed in static environments, is mentioned by several authors (e.g. [CPK10]). In this setting, we explain a novel technique that enables us to achieve this goal. The main results of this chapter are published in [MdA14].

5.1. Based on Radiation Pattern

In order to make it more difficult to perform the environment reconstruction and reradiation leakage attacks, one can employ a special kind of antennas in at least one of the legitimate parties. These antennas have radiation patterns which change randomly with time. This technique builds upon the fact that the change of the reradiation diagram cannot be predicted easily by any attacker. This method can be implemented using the so-called ESPAR antennas. As a consequence, the generated entropy lies not only in the channel, but also in random modification of the radiation pattern. This method has been described in detail in Section 3.3.1 and does not contain any original contribution by the author. As a drawback, we point out that at least the party (or parties) having such an antenna needs an internal random number generator and some memory for controlling the beamforming and saving the settings for later reuse when receiving the signal.

5.2. Based on Differences in the Local Oscillators

In this section, we will describe in detail how our novel technique *combining channel fading effects with hardware impairments* in the transceiver's devices can be implemented.

We considered a special type of receivers, namely the *direct-conversion receivers*, which we introduce later in detail. We point out that there might be other ways of using the impairments in the receivers for the purpose of augmenting the entropy of the generated key. We leave this subject for further research.

5.2.1. Channel

As described extensively in Chapter 2, it is usual to characterize the radio channels through their impulse response. Recalling, the impulse response $h_{\mathrm{AB}}(t)$ of the multipath fading channel between Alice and Bob in a time-invariant channel (during the short time period of the protocol execution) can be represented by an impulse train

$$h_{\mathrm{AB}}(t) = \sum_{i=1}^{n} \rho_i \delta(t - \tau_i), \tag{5.1}$$

where the τ_i are the propagation delays and the coefficients ρ_i the amplitudes of different signal components arriving to Bob through n different paths. Because of reciprocity, we can state that in theory

$$h_{\mathrm{BA}}(t) = h_{\mathrm{AB}}(t), \tag{5.2}$$

which means that the channel characteristics are the same in both directions. Hershey et al. [HHY95] propose to use this common characteristic in order to generate a secret key between Alice and Bob, as this signal corresponds to the *signature* of the channel between these parties. Because of the spatial decorrelation of signals in a fading channel, the channel responses, $h_{\mathrm{AE}}(t)$ and $h_{\mathrm{BE}}(t)$, that Eve receives are uncorrelated to $h_{\mathrm{AB}}(t)$ and $h_{\mathrm{BA}}(t)$, respectively. This guarantees the secrecy of the key.

Some practical implementations of this protocol have been described in detail in [MTM+08], [LXMT06], [ASKMY07] and [CPK10]. However, the measured values might be influenced by several imparities, like additive noise, differences in hardware [CPK10], interference, manufacturing variations and the fact that the channel is not sounded in both directions at the same time [PJC+13]. Some issues related to synchronization are also addressed in [CPK10]. This can affect the channel state information and induce *asymmetries* in the system. In real-world application, we have therefore $h_{\mathrm{BA}}(t) \approx h_{\mathrm{AB}}(t)$. In order to cope with this issue, an information reconciliation step should be performed at the end of the protocol to ensure that both parties possess the same key (cf. Section 2.3).

Fading-based key exchange protocols only account for passive attackers. This means that it is assumed that Eve is not able to jam the probing signals. Additionally, Eve is supposed to be sufficiently separated (at least a few wavelengths) from Bob.

Now let $s_{\mathrm{A}}(t) = A\cos(2\pi f_{\mathrm{A}} t)$ be the channel probing carrier signal sent by Alice. According to Equation (5.1), Bob receives the signal $r_{\mathrm{B}}(t)$ changed by the channel given by

$$r_{\mathrm{B}}(t) = \sum_{i=1}^{n} \rho_i s(t - \tau_i) \tag{5.3}$$

$$= A \sum_{i=1}^{n} \rho_i \cos(2\pi f_A (t - \tau_i)), \tag{5.4}$$

which is the sum of n attenuated and delayed replicas of the original wave $s_A(t)$.

5.2.2. Hardware

One important type of common receivers are the so-called *direct-conversion receivers*. This kind of receivers is often used by the *software-defined radio* community [USR, gnu].

5.2.2.1. Direct-Conversion Receivers

Unlike superheterodyne receivers, a direct-conversion receiver (DCR) uses no intermediary frequency for performing the demodulation stage. Instead, it uses a local oscillator with a similar frequency to that of the carrier signal. A simplified diagram of a DCR can be seen in Figure 5.1.

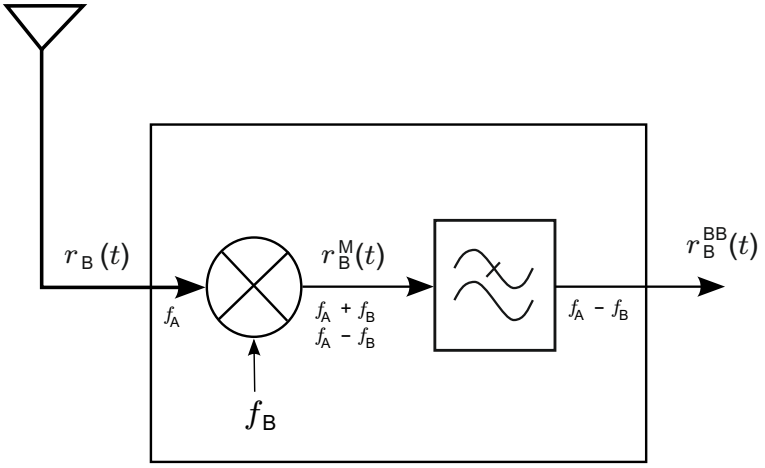


Figure 5.1.: Direct-Conversion Receiver (simplified) at Bob.

The received signal $r_{\mathrm{B}}(t)$ (cf. Equation 5.3) will be downconverted in the mixer with local oscillator with frequency f_{B}. The resulting signal is therefore

$$r_{\mathrm{B}}^{\mathrm{M}}(t) = A \sum_{i=1}^{n} \rho_i \cos(2\pi f_{\mathrm{A}}(t - \tau_i)) \cos(2\pi f_{\mathrm{B}} t) \tag{5.5}$$

Applying well-known trigonometric identities to Equation (5.5), we obtain

$$r_{\mathrm{B}}^{\mathrm{M}}(t) = \sum_{i=1}^{n} C_i [\cos(2\pi(f_{\mathrm{A}} - f_{\mathrm{B}})t + \phi_i) + \underbrace{+ \cos(2\pi(f_{\mathrm{A}} + f_{\mathrm{B}})t + \phi_i)}_{\text{filtered out}}], \tag{5.6}$$

where C_i are amplitude coefficients depending on A, ρ_i and τ_i, and ϕ_i phases depending on τ_i.

As we can see from Equations (5.5) and (5.6), due to the mixing of different frequencies, new signal components with frequencies $f_\mathrm{A} - f_\mathrm{B}$ and $f_\mathrm{A} + f_\mathrm{B}$ are created in this process. Therefore, a filtering stage is applied in order to clean the signal from its undesirable higher frequency components. This removes the $f_\mathrm{A} + f_\mathrm{B}$ component. Applying a low-pass filter to $r_\mathrm{B}^M(t)$, we obtain the baseband signal

$$r_\mathrm{B}^\mathrm{BB}(t) = \sum_{i=1}^{n} C_i \cos(2\pi(\underbrace{f_\mathrm{A} - f_\mathrm{B}}_{\delta f})t + \phi_i). \tag{5.7}$$

This means that the DCR receiver outputs a signal whose amplitude is basically defined by the channel characteristics and whose frequency, δf, is exclusively due to the sender and receiver local oscillators' frequencies. Combining these two factors, we develop the protocol described next.

5.2.3. Basic Protocol

Taking into consideration what has been explained in the previous sections and ideally assuming total precision of the local oscillators, we developed the following basic protocol for common key generation:

1. Alice and Bob agree on a set of n frequencies, say $\mathcal{F} = \{f_k\}_{k=1}^n$. These frequencies can be, without loss of generality, equally spaced, as illustrated in Figure 5.2;

2. Alice and Bob *randomly* choose a frequency from $\mathcal{F}$, i.e., $f_\mathrm{A} \xleftarrow{R} \mathcal{F}$ and $f_\mathrm{B} \xleftarrow{R} \mathcal{F}$;

3. Alice probes the channel with a frequency f_A signal;

   This means that Alice injects a probing signal $s_\mathrm{A}(t)$ with frequency f_A in the environment. This wave propagates through the wireless medium. Bob receives the incoming wave, $r_B(t)$, by tuning his local oscillator for the frequency f_B. After filtering, he finally obtains the baseband signal $r_\mathrm{B}^\mathrm{BB}(t)$ given by Equation (5.7);

4. Bob and Alice exchange roles. This means that Bob generates and sends a probing signal, $s_\mathrm{B}(t)$, with frequency f_B, whereas Alice collects the channel response to Bob's signal, $r_\mathrm{A}(t)$, with local oscillator tuned for f_A;

5. Repeat the previous steps a certain number, N, of iterations and save the respective channel responses in baseband, $r_i^\mathrm{BB}(t)$, $i = 1, ..., N$.

Because of the difference in the oscillators, a new signal with frequency $\delta f = |f_\mathrm{B} - f_\mathrm{A}|$ will be generated. As seen before, this signal combines information about hardware oscillators in its frequency and about the environment in its amplitude. Afterwards, this signal must be processed, as explained in the next section, in order to obtain a binary sequence - the secret key.

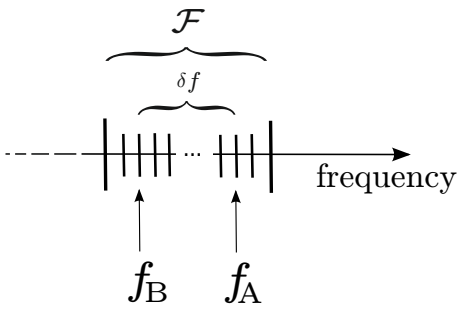


Figure 5.2.: Set of signal frequencies randomly sampled.

5.3. Key Extraction

In this section, a novel method for generating the key extracted from the surrounding environment is described in detail.

Basically, all *key extractors* consist of two components (see Figure 5.3):

1. Features Extraction block (filter): selects and processes some selected features of the incoming signal;

2. Quantizer: transforms the signal coming out of the filter into a binary sequence.

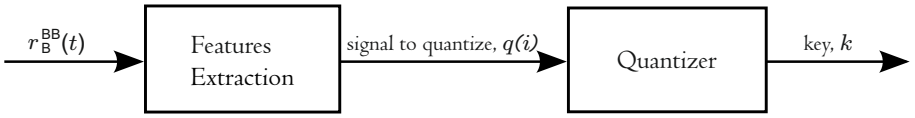


Figure 5.3.: Key Extractor Block Diagram.

In the next sections, we extensively describe how we implemented these two blocks.

5.3.1. Features Extraction

Most experimental studies on this subject use the time variation of the signals' RSSI (*Received Signal Strength Indicator*) values as input of the quantization block. The values are then processed in a way such that the system imparities are minimized and the entropy rate of the secret keys is maximized (cf. [MTM+08],[CPK10] and [PJC+13]).

We consider the baseband signal demodulated by the transceiver in iteration i, represented as $r_i^{\mathrm{BB}}(t)$. As previously explained, we do not restrict ourselves to the amplitude values due to *fading*, but we also consider the effect of the frequency of this signal due to differences in the *local oscillators* as a new source of common entropy. Keeping this in mind, a simple Features Extraction Block is developed. For each iteration i of the protocol, each party computes the output of this block as:

$$q(i) := \underbrace{\frac{1}{N}\sum_{k=1}^{N}|X_k|}_{\text{fading}} \cdot \underbrace{\frac{1}{M}\sum_{l=1}^{M}(Z_l - Z_{l-1})}_{\text{local oscillators}}, \tag{5.8}$$

where X_k are the local maxima and minima, and Z_l the zero crossings, respectively, of the signal $r_i^{\mathrm{BB}}(t)$, as depicted in Figure 5.4. This equation corresponds to the *product of the averages* of the main characteristics: the amplitude (contained in the values $|X_k|$) and the frequency (translated in the values Z_l, being the interval between two zero crossings approximately half of the period of the wave). The *averaging* process tends to minimize the influence of the signals and measurements' associated noise.

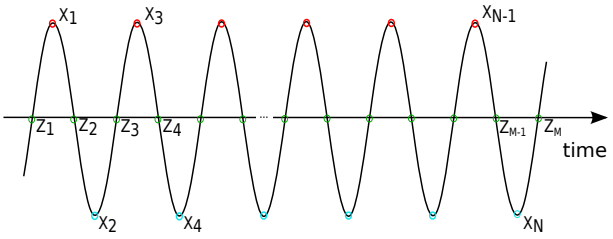


Figure 5.4.: Baseband signal with local extrema and zero crossings.

Basically, the effects of fading are being *rescaled* by the frequency of the signal generated by the difference of the local oscillators' frequencies. These values are unknown to an adversary at the time the channel is sounded.

This technique is quite efficient since the number of performed calculations needed for the key generation is small: for each sent frequency, one just needs to calculate the peaks and the zero crossings of the signal. This is easy to implement in both software and hardware.

5.3.2. Quantizer

Our quantizer performs a *uniform* discretization of the output of the Features Extraction block.

Firstly, we plot the output of this block, $q(i)$. We then proceed to make a quantization of this signal according to a predefined number of quantization bits, Q, in the following way:

1. The amplitude of the signal is divided in $M = 2^Q$ equally spaced intervals and we assign to each of these intervals a binary sequence of Q bits;

2. For each iteration i, the Q-bit binary sequence, k_i, corresponding to the interval in which the value $q(i)$ is located, is selected and appended to the extracted key. Therefore, we obtain the secret key $k_e = k_1||k_2||...||k_i||...||k_N$;

   Moreover, a gray code grid (i.e., such that adjacent quantization intervals just differ in 1 bit) was used, in order to deal with slight imparities in the received values, which minimizes the bit mismatches and consequently allows to obtain better key agreement results (as in [PJC+13]).

Due to the fact that the quantization step was conducted taking into consideration the minimum and maximum values of the signal, $q(i)$ will be normalized in amplitude by the Quantizer, which accounts for possible differences in the received gains or properties of the hardware. This way, the influence of amplitude *imparities* in the quality of the key, due to different gains at the receivers (cf. [CPK10]), is reduced.

5.4. Simulation

Since in the real world it is virtually impossible to totally control the environment and the hardware conditions, we firstly performed a simulation using MATLAB®. The main goal is to try to understand how big the advantages we gain by using the hardware as a new source of entropy are and how much considering the difference in the local oscillators frequencies can make it more difficult for an attacker to reconstruct the signal obtained by Alice and Bob. In the simulation we can easily separate the components influencing the received signal - the environment and the hardware.

5.4.1. Channel

The environment was modeled as a simple *discrete set* of finite objects similarly to Chapter 4. Under this model, the transmitted signal propagates along the physical wireless environment and is reflected by each of these objects. Since the main goal of the simulation is to seek to understand the effect of the oscillators, we considered a very simple environment made of five different reflecting objects like in Section 4.1. We have been pessimistic, since real-world applications usually deal with more complex channels, which clearly implies more entropy in the final key.

We considered a propagation path passing through each of these objects and connecting two transceivers (Alice-Bob, Alice-Eve and Bob-Eve). According to Equation (5.1), each path is characterized by an *attenuation factor*, ρ_i, (it encompasses the influence of path attenuation, object absorption and reflection coefficients) and *delay* τ_i introduced to the signal by the propagation distances traveled by the electromagnetic wave. We also consider a certain amount of unavoidable *AWGN noise* in the channel, characterized by the signals' *SNR*. All these factors will interfere in the quality of the generated key. In our simulation, we introduced a dominant path (as observed in [MTM+08]). This corresponds to the lowest value of attenuation for this path and highest *SNR*. We also considered the channel not changing the frequency of the signals. Channel reciprocity was ensured by giving very similar values to *Alice-Bob* and *Bob-Alice* channels parameters. Nevertheless, the values were not exactly equal, since there are always some imparities to be taken into account in the real world: small changes of the channel due to synchronization issues, interferences and measurement imparities.

On the other hand, fading was translated into our model by setting different values for the *Alice-Eve* and *Bob-Eve* channels of those given to the *Alice-Bob* channel. In all channels, a much stronger direct path component is considered, as observed in [MTM+08].

5.4.2. Hardware

We ideally consider that Alice, Bob and Eve have identical transceivers. Each transceiver was modeled as being a mixer and a simple low-pass filter with cut-off frequency set to 500 kHz (cf. Section 5.2.2.1).

5.4.3. Protocol

We consider a small variation of the basic protocol described in Section 5.2.3. For each iteration i, new sets $\mathcal{F}_{\mathrm{A}_i}$ and $\mathcal{F}_{\mathrm{B}_i}$ are created by Alice and Bob, respectively.

Both sets are shifted a certain value Δf to the right in each iteration (see Figure 5.5). This seeks to exploit in the real world the channel frequency characteristics and is similar to the protocol we implemented in our prototype (see Chapter 6). In the simulation, we considered both set of frequencies to have the same number of elements. We established $|\mathcal{F}_{\mathrm{A}_i}| = |\mathcal{F}_{\mathrm{B}_i}| = 20$. This means that the difference in the oscillation frequencies belong to a *discrete set of values*.

We also guarantee a minimal frequency distance between $\mathcal{F}_{\mathrm{A}_i}$ and $\mathcal{F}_{\mathrm{B}_i}$, denoted by ν, in order to ensure that there are at least two zero-crossings and one peak (maximum or minimum) in the received signal.

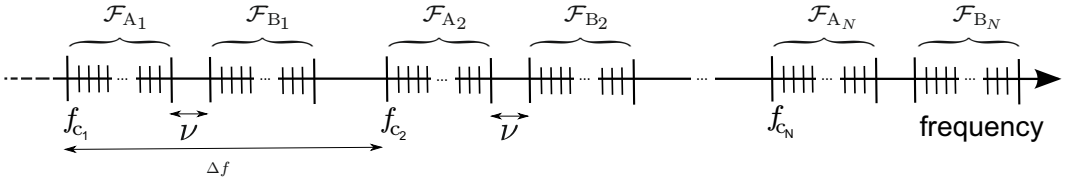


Figure 5.5.: $\mathcal{F}_{\mathrm{A}_i}$ and $\mathcal{F}_{\mathrm{AB}_i}$: set of frequency values Alice and Bob, respectively, tune their local oscillator in iteration $i, i = 1, ..., N$.

In our case, we set $\Delta f = 1\,\mathrm{MHz}$ and $\nu = 800\,\mathrm{Hz}$, starting at $f_{c_1} = 2.43\,\mathrm{GHz}$. The range of the $\mathcal{F}$ sets was of 100 kHz. Typical values for the coherence bandwidth, W_c, are usually around 500 kHz (cf. [WTS07] and [ZW99]), depending on the environment. Therefore, for each iteration, $\delta f < W_c$ and, thus, reciprocity still holds.

For each iteration i, Eve randomly guesses a value from $\mathcal{F}_{\mathrm{A}_i}$ and $\mathcal{F}_{\mathrm{B}_i}$ and tunes her local oscillator for those frequencies when receiving a wave from Bob and Alice, respectively.

5.4.4. Experiments

In order to investigate the influence of the frequency oscillations in the quality of the generated key and to separate the influence of the two factors (channel and hardware) in the key quality, we design two experiments. Since we want to evaluate the influence of the difference of frequencies in the generated key, we consider a very simple wireless channel, consisting of only five reflectors, which are responsible for attenuating and phase shifting the original signal. As mentioned before, in order to simulate the reciprocity property, the attenuation parameters for the channels A-B and B-A are, of course, very similar. They are not totally equal in order to simulate some differences due to other kind of asymmetries (e.g., due synchronization issues), as already mentioned. Those parameters are different from the ones for the eavesdropper's channels due to multipath interference.

5.4.4.1. Experiment I

In this case, we are interested in checking how very simple channels influence the shared key. This is the case when *Eve knows the oscillation frequencies*, but has no knowledge about the channel *Alice-Bob* at all. This would happen in the ideal case when Eve has a perfect clone of Alice and Bob's hardware.

Here, the *source of entropy* is restricted to the *channel*. Therefore, $h_{\mathrm{BE}} \neq h_{\mathrm{BA}}$ and $h_{\mathrm{AE}} \neq h_{\mathrm{AB}}$, whereas $f_{\mathrm{E}}^{\mathrm{B}} = f_{\mathrm{B}}$ and $f_{\mathrm{E}}^{\mathrm{A}} = f_{\mathrm{A}}$ (see Figure 5.6).

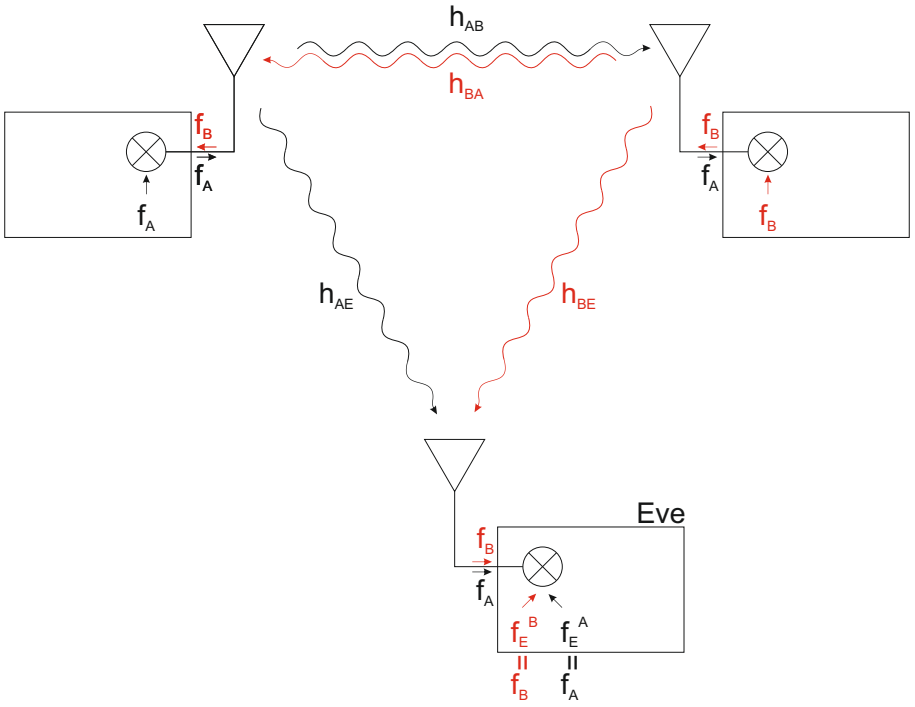


Figure 5.6.: Exp. I: *Eve knows the oscillation frequencies (but not the channels).*

5.4.4.2. Experiment II

This experiment corresponds to the real-world scenario (though in a very rudimentary environment), i.e., when *Eve knows nothing* about the *environment* or about the *hardware*.

Therefore, under this scenario, there are simultaneously two *sources of randomness* - the *channel* and the *hardware oscillators*.

Thus, $h_{\mathrm{BE}} \neq h_{\mathrm{BA}}$ and $h_{\mathrm{AE}} \neq h_{\mathrm{AB}}$ and $f_{\mathrm{E}}^{\mathrm{B}} \neq f_{\mathrm{B}}$ and $f_{\mathrm{E}}^{\mathrm{A}} \neq f_{\mathrm{A}}$ (see Figure 5.7).

5.4.5. Key Agreement Rate

As a figure of merit for the quality of our method, we define the *key agreement rate*, KAR, as being the relative amount of equal bits on both generated keys, i.e., the ratio of the Hamming-Distance, HD, between the generated keys, k_{P_1} and k_{P_2}, on parties P_1 and P_2, respectively, and the length of the keys, $L = |k_{P_1}| = |k_{P_2}|$. Mathematically,

$$KAR(P_1, P_2) = \frac{HD(k_{P_1}, k_{P_2})}{L} \tag{5.9}$$

Ideally, we expect KAR values around 100% between Alice and Bob; and around 50% for the Alice-Eve and Bob-Eve channels. This would be for Eve as good as by simply performing a random guess of the key, which means that she would gain no advantage from the received signal.

5.4.6. Results

The obtained values for KAR for both experiments are shown in Table 5.1. The shown values are an average over five runs of the Experiments.

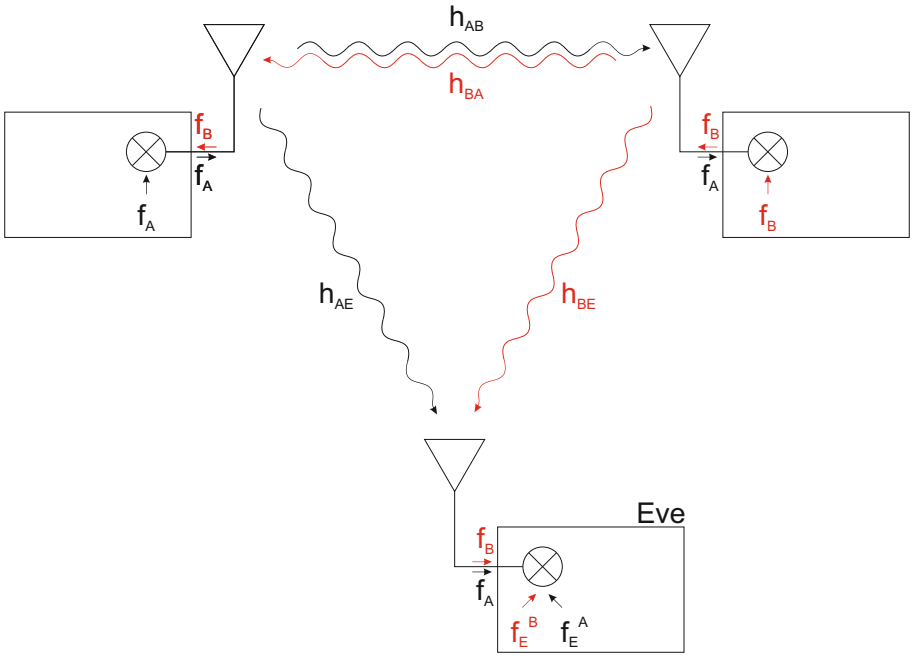


Figure 5.7.: Exp. II: *Eve knows nothing.*

Exp.	A-B	E-A	E-B
I	99.6	99.5	97.3
II	99.8	72.4	72.9

Table 5.1.: KAR (%) values for all experiments.

Another way of illustrating the quality of the key extraction method is to check simultaneously the *profiles* of the quantizer's output of all the parties. Figures 5.8 and 5.9 show these profiles for the experiments I and II respectively. For each experiment, the upper two graphs in each figure correspond to the output of Alice (left) and Bob's (right) quantizers, i.e., the left graph shows the key extraction output from the signal received by Alice coming from Bob and the right one from the signal received by Bob coming from Alice. The downer plots present the signal received by Eve from Bob (left) and Alice (right).

5.5. Discussion

On the one hand, both upper graphs of Figures 5.8 and 5.9 are similar, which is a straightforward consequence of the *reciprocity* of the wireless channels. On the other hand, it is clear that the signal transmitted by Bob received by Alice (upper left corner) and by Eve (lower left corner) and the signals received by Bob sent by Alice (upper right corner) and by Eve (lower right corner) are different, which is due to the *multipath* properties of these channels and/or different oscillation frequencies. Therefore, it seems accurate to say that the performed simulations confirm our theoretical underpinnings. The profile is however very flat, which can be explained by the fact that we considered a channel with very simple characteristics, i.e., low entropy.

Table 5.1 and the quantizers' outputs show that the differences in the oscillation

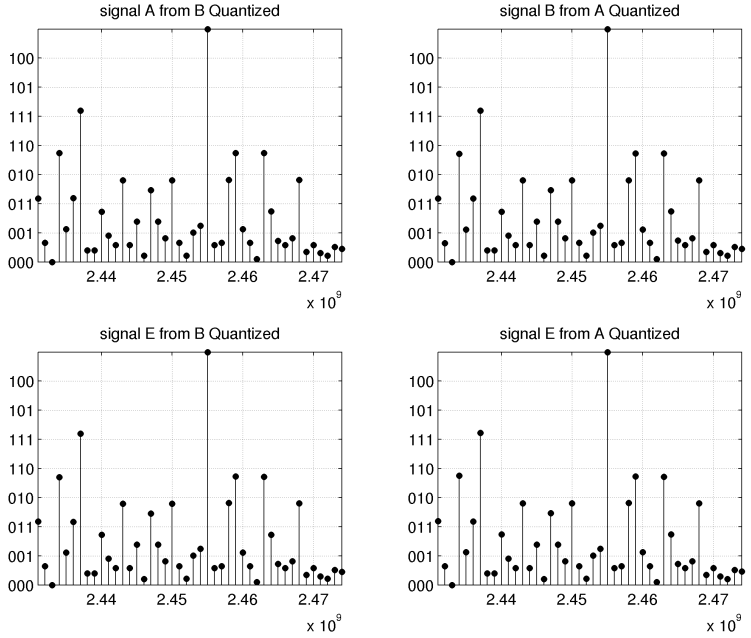


Figure 5.8.: Exp. I: *Eve knows the oscillation frequencies (but not the channels).*

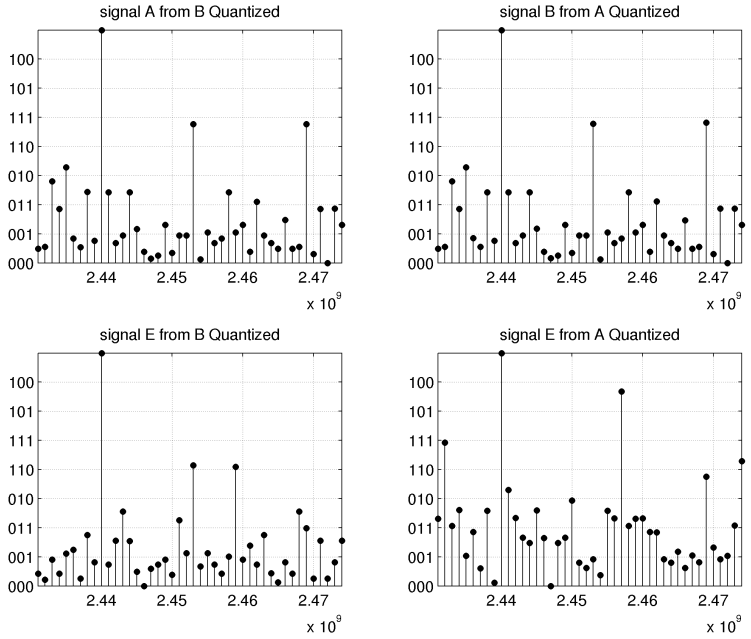


Figure 5.9.: Exp. II: *Eve knows nothing.*

frequencies play an important role in protecting the system from an eavesdropper. For our purposes, we consider an idealized simple environment, where the reflections influence is small in the received signal.

However, while the KAR values for the *Alice-Bob* channel are similar for both experiments, significant differences in the values for the eavesdropper channels reflect the fact that the oscillation frequencies differences contribute decisively for the security of this method.

These results suggest that the usage of hardware-based "asymmetries" act like amplifying the multipath property of the channel, in the same way as the usage of ESPAR antennas do by changing the radiation pattern during the execution of the channel sounding ([AHT+05b] and [SHOK04]).

5.6. Conclusion

We extend the source of randomness in order to include also the unavoidable imparities in the transmitter and receiver hardware by leveraging the differences in the oscillation frequencies of the local oscillators, which may vary with temperature or manufacturing process. This technique enables us to increase the security of the wireless key exchange method. We demonstrate how the spurious signals created by mixing signals with different frequencies can be used in order to augment the security of the key exchange system based on wireless fading, even when the environment is static.

A simulation showing that small differences in the oscillation frequencies can induce different quantizers' profiles and, therefore, cause disparities in the resulting keys, was developed. We acknowledge, though, that the simulation is only a simplification of the real-world conditions. It only takes into account a finite degree of randomness in the frequency values. However, in practice, these values can be continuous (as we will see in the next chapter) and therefore hardly predictable by an attacker.

The experiments suggest that the oscillation differences due to imparities in the local oscillators act in the same way as the ESPAR antennas. In this case, the adversary is not able to easily find the time-varying beamforming characteristic of these antennas. Similarly, in our novel method for key generation, the adversary is unable to predict the oscillation frequencies resulting from the unavoidable impairments in the legitimate parties' local oscillators. By taking this into account, we introduce another source of entropy when generating the key, which allows us to harvest more randomness in total.

The eventuality of a very simple environment, providing too low entropy, or even the existence of side-channel attacks on fading-based key exchange protocols, has been mostly neglected. One advantage of extending the source of randomness to the hardware components lies in the fact that these attacks against these protocols will be hardened. The environment may have almost no entropy or Eve might be able of measuring the reradiation from the antennas; however, as long as she doesn't know which frequency to tune precisely her receiver to, she will no longer have enough information to correctly reconstruct the baseband signal.

Our method is easy to implement, both in software as in hardware and can, thus, be deployed in off-the-shelf equipment.

6. Experimental Validation

In this chapter, we describe our efforts to experimentally validate the key generation method we proposed in the previous chapter. This method combines the environment and the hardware properties for the generation and sharing of a secret bitstring between two parties. We design and conduct two main experiments. In the first experiment, we show that the originated frequencies are only a result of the devices and not due to other overseen phenomena. In order to isolate the possible causes for the difference in the frequencies of the originated signals, we perform a series of smaller experiments under controlled conditions. Moreover, we evaluate the validity of our method under *real-world indoor and outdoor conditions*. For this purpose, we develop a prototype with which we perform a second main experiment. We conducted different data collection campaigns in different outdoor environments with different characteristics: a static (rural) environment, a semi-dynamic (semi-urban) environment and a dynamic (urban) environment. We introduce a set of parameters used as a *metric for the quality* of the results. The practical aspects of the experiments were carried out in collaboration with Simon Dreher. Finally, we analyze the obtained results and draw conclusions. This was done during the preparation of Michael Markus *Studienarbeit*. Further, we identify quality criteria for key extraction techniques and we seek, according to those, the best way, for different types of environments, of combining the information from the environment with the information due to the hardware.

6.1. Hardware and Software

We use one USRP1 device per party (Alice, Bob and Eve) as a transceiver front end for generating the channels' probing signals and for measuring the corresponding echoes (cf. Section 3.2). Each USRP1 device is equipped with a *direct conversion* RFX2400 daughterboard. They provide superior performance in the 2.4 GHz -2.483 GHz band and have 50 mW of output power. Two of these devices are connected to an omnidirectional antenna, whereas the third one is linked to a logpad-antenna (detailed description about all hardware components, including data sheets, can be found in [USR]). Since all parties receive and send the probing signals through the same antennas, the fact of using different types of antennas will not affect

the global reciprocity of the system (cf. Section 2.2.4).

Our implementation uses the GNU Radio software platform [gnu] installed in similar laptops running Linux-OpenSUSE distributions for the interaction with the transceivers. Synchronization was performed by sending and receiving packets through the 802.11 Ethernet cards installed in the laptops. Our software is written in Python programming language and also includes the implementation of the synchronization and sounding parts of the protocol, as well as the CASCADE protocol (cf. Section 2.3) for information reconciliation. It is flexible and easily allows the implementation of different methods for the key extraction. Bash scripts were also used in order to automatize the experiments, namely the exchange of parties in each device, as shown later in the Table 6.1.

The thorough analysis of the experimental results and the generation of the key were processed offline in MATLAB®.

6.2. Experiment: Differences in the Frequencies

In this section, we describe our experiments laid out to confirm that the different frequencies we observe are solely due to inherent properties of the hardware devices. For that purpose, we had to isolate the potential causes of this behavior. A few possible causes were identified: equipment (i.e., the combination of *laptops* (L_1, L_2, L_3) and transceiver *hardware* (H_1, H_2, H_3)), *positions* (X,Y,Z), *party* (A, B or E) and *location* (laboratory or between walls).

6.2.1. Location

We perform our experiments in two different locations at our Institute: in our *laboratory* (Section 6.2.1.1) and *between two different rooms* (Section 6.2.1.2).

6.2.1.1. Laboratory

As depicted in Figure 6.1, all parties are placed on an octagon shaped table located at our laboratory. The positions X, Y and Z are defined to be approximately one meter apart from each other. The equipment is placed on these positions. It consists of three pairs of laptops together with the transceiver hardware devices, denoted by L_1/H_1, L_2/H_2 and L_3/H_3.

We performed three experiments. For each of them, we tried all possible combinations of parties for each pair laptop/hardware (see Table 6.1):

1. inter-exchange the hardware positions, i.e., place L_1/H_1 at position Z, L_2/H_2 at position Y and L_3/H_3 at position X;
2. increase the distance between X and Z;
3. rotate the positions X, Y and Z 45° clockwise .

6.2.1.2. Between Rooms

In order to collect more evidence for our results and to prove that such a difference in the frequency is not due to the location, we repeated the same experiments between two different rooms, as depicted in Figure 6.2. The distance between points X, Y, Z was, necessarily, increased. Point X was also tested for two different positions: in positions X and X' (behind a concrete pillar).

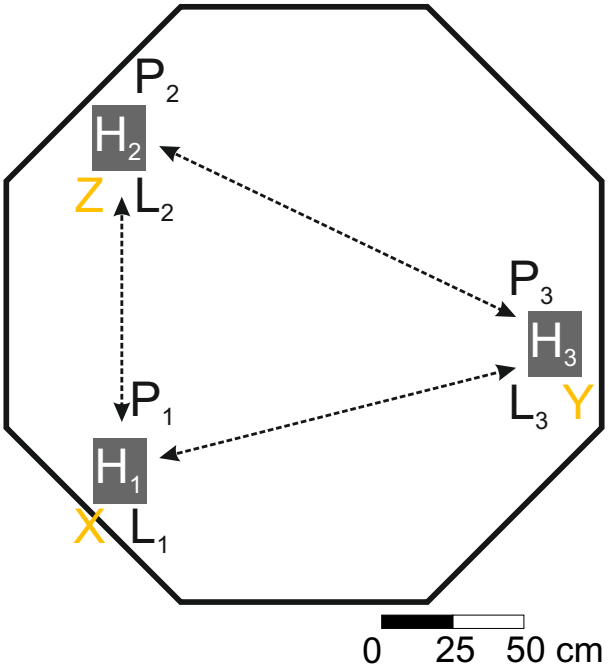


Figure 6.1.: Laboratory: laptops and transceivers were placed on a table in positions X, Y and Z.

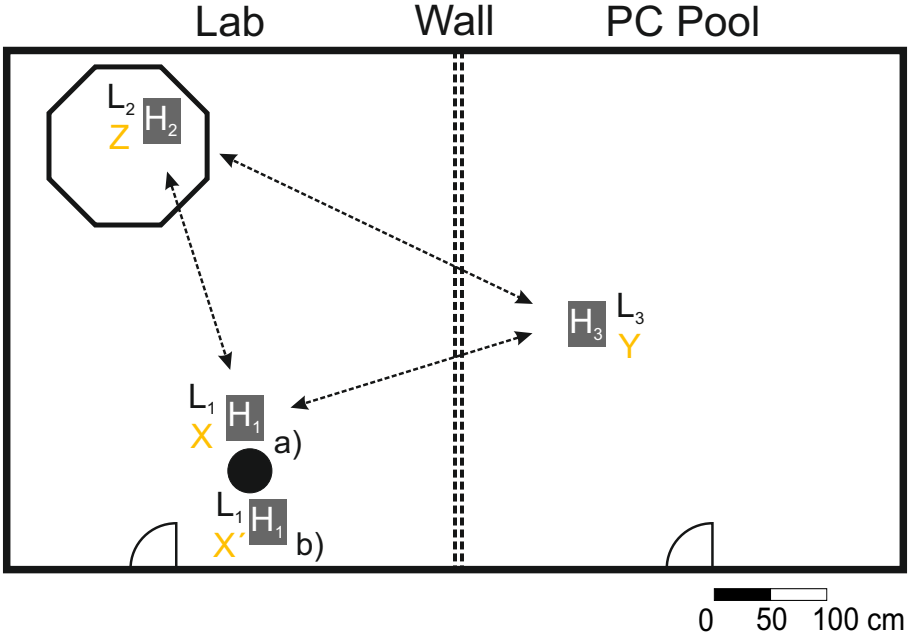


Figure 6.2.: Between rooms: Floor plan of both rooms.

6.2.2. Results

In this section, we present and analyze the received baseband signals (as described in Section 5.2.2).

6.2.2.1. Laboratory

Figure 6.3 shows a typical sample of the baseband signals (cf. Section 5.2.2) received by H_1 coming from H_3, by H_3 coming from H_1, by H_2 coming from H_3 and by H_2 coming from H_1. Without loss of generality, this figure corresponds to the situation where Alice is placed at position X equipped with hardware H_1, Bob at position Y using hardware H_3 and Eve at position Z equipped with hardware H_2. However, we tried all possible configurations.

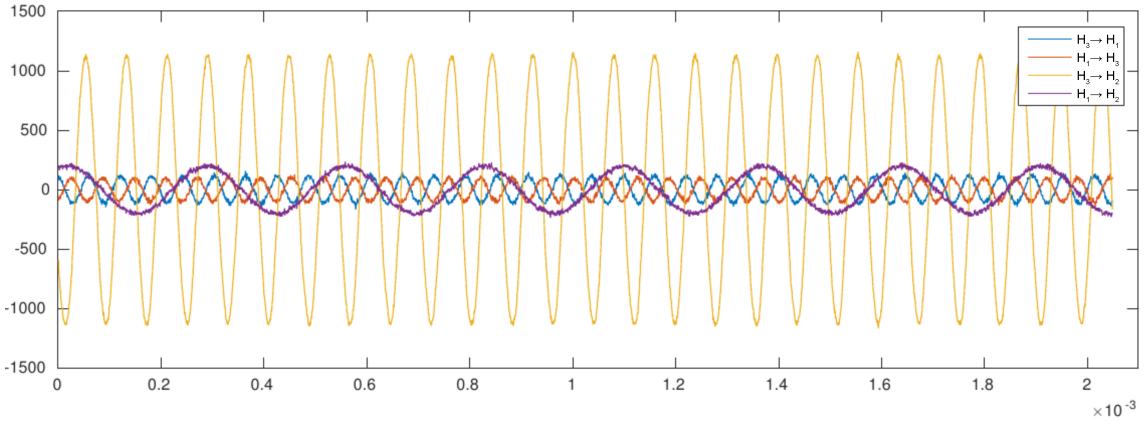


Figure 6.3.: Received baseband signals: we observe that the signals $H_3 \to H_1$ and $H_1 \to H_3$ have the same frequency, which is different from the frequencies of the signals $H_3 \to H_2$ and $H_1 \to H_2$.

By visual inspection, one can easily confirm in Figure 6.3 that one wave clearly shows a smaller frequency ($H_1 \to H_2$). We extensively test for the influence of the *location*, *hardware* and *role* assumed by each party on these results.

We permanently observe that the signal showing a remarkable difference in the frequency always appears between hardware H_1 and hardware H_2, irrespective of the role, position in the room or location.

We conclude therefore that a significant difference between the oscillation frequencies of the local oscillators of both hardware devices H_1 and H_2 is the cause of such frequency. The differences in the frequencies between the pairs of hardware H_1 and H_3 and H_2 and H_3 are lower, as one can see in Figure 6.3. E.g., in this case, the signal between H_2 and H_1 had a frequency of approximately 4 kHz, the signal between H_3 and H_1 and H_1 and H_3 the frequencies of 16 kHz (sometimes there are small variations between these two values) and H_3 and H_2 of 12 kHz, as we show schematically in Figure 6.4. All these values are significantly smaller than a coherence bandwidth $W_c = 500$ kHz (cf. [WTS07]).

6.2.2.2. Between Rooms

No significant differences in frequency were observed between the layout containing the position X and the one containing X'. However, it was observed that the

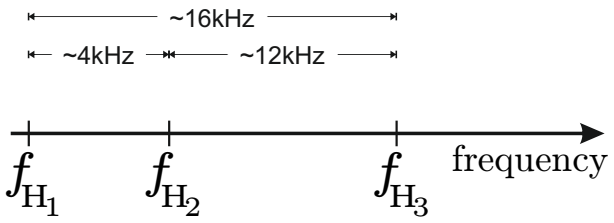


Figure 6.4.: Approximate frequencies of the generated signals ($f_{H_2} - f_{H_1}$, $f_{H_3} - f_{H_1}$ and $f_{H_3} - f_{H_2}$) resulting from differences in the frequencies in the local oscillators of the devices H_1, H_2 and H_3.

magnitude of the received signal was weaker when position X' was examined. This is clearly due to the massive concrete pillar in front of one of the transceivers, which is responsible for a stronger attenuation of the incoming and outgoing waves. Once again, the wave showing a larger period was the one corresponding to the pair H_1 and H_2, irrespective of the roles (Alice, Bob or Eve). This supports our theoretical considerations stating that the originated signals are due to some *imparities* in the devices' local oscillators.

6.2.3. Discussion

By isolating the different possible causes of the generated signals, we confirmed that the hardware is the only possible cause for the origin of signals with different frequencies. We use this fact in our novel key exchange technique as proposed in Chapter 5. We experimentally consolidate this idea in the next section.

6.3. Experiment: Key Exchange Evaluation

In order to check the feasibility of using frequency information for generating a shared secret key under different real environments, we perform an experimental data collection campaign for testing our key exchange protocol. We implement several extractors (as defined later in Section 6.3.2.3) and we present the obtained results in several graphs.

6.3.1. Protocol

We use a slightly different protocol than the one presented in Sections 5.2.3 and 5.4.3. Instead of creating new sets $\mathcal{F}_{A_i}$ and $\mathcal{F}_{B_i}$ for each iteration i, we assume that the transceivers' local oscillators *inherently* contain unavoidable frequency errors, as shown in Section 5.2.2.1, i.e., small unpredictable variations of the oscillation frequency, ϵ, due to manufacturing issues, temperature or other differences, as mentioned, e.g., in [BBGO08]. It is virtually impossible to tune exactly to a certain oscillation frequency. As an example, the signal of approximately 15 kHz originated between H_2 and H_3 in an oscillation frequency of 2.4 GHz accounts for an error of 6.2×10^{-4} %. Actually, when we intend to tune the local oscillator to a certain frequency f_{c_i}, the device gets tuned for $f_{c_i} \pm \epsilon$. The difference in the actual tuned frequencies by the devices A and B will be responsible for the creation of a new signal baseband component, as explained in detail in Section 5.2.2.1. Therefore, this difference, $\delta f = |f_A - f_B| = |\epsilon_A - \epsilon_A|$, *naturally* takes values in a *continuous interval*.

As illustrated in Figure 6.5, the implemented protocol runs the following way:

1. Alice starts sending an analog *sounding signal*, e.g., a carrier wave with a certain frequency $f_{c_1}(\pm\epsilon_A)$;

2. using a TCP packet transmission, *sync signal*, Alice signalizes Bob that she already started sending a signal with frequency f_{c_1};

3. Bob saves the incoming signal during a certain period of time, Δt, tuning his local oscillator for the same frequency value $f_{c_1}(\pm\epsilon_B)$;

4. Bob informs Alice that she can already stop sending the analog probing signal and Alice interrupts the transmission of the wave;

5. Alice and Bob exchange their roles and perform the previous steps accordingly;

6. Repeat this procedure for all other central frequency values $f_{c_i}, i = 1, ..., N$, where N is the total number of central frequencies previously agreed between both parties.

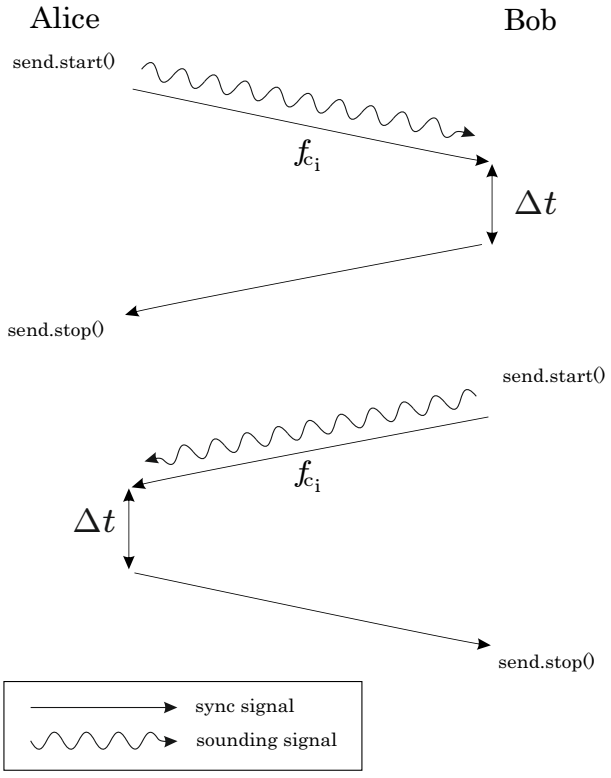


Figure 6.5.: Protocol for channel sounding in iteration i.

Several runs (between 5 and 30) for each central frequency, f_{c_i}, were performed while collecting the data. 4096 points were saved for each central frequency f_{c_i}. Each run takes around 19 seconds to be executed using USRP devices. In order to avoid any interferences between the *sounding signal* sent by the USRP1 and the *synchronization (sync) signal* around 2.4 GHz being sent by the laptop's Ethernet cards (Figure 6.5), the starting *sounding carrier* frequency was chosen to be slightly

higher than 2.4 GHz, namely $f_{c_1} = 2.43$ GHz. The sounding frequencies were separated by $\Delta f = 1$ MHz (as in Section 5.4.3), until reaching the value of 2.473 GHz, which corresponds to $N = 44$ probing bands. These values lie within the 2.4 GHz ISM band and within the range allowed by the RFX2400 daughterboards.

The signal traces were saved in the laptop and later transferred to a PC, where the analysis and processing steps of the different *key extractors* (described later in Section 6.3.2.3) were performed offline using MATLAB®.

Each USRP receiver measures an in-phase (or real) component (I) and a quadrature (Q) component for each received signal $R^{BB}(t)$, say $R^{BB}(t) = R_I^{BB}(t) + \jmath R_Q^{BB}(t)$. As input of our signal transformation block (Figure 5.3), we considered only the in-phase component of the signal, i.e., $r^{BB}(t) = R_I^{BB}(t) = \mathrm{Re}(R^{BB}(t))$, since the quadrature component brings no further information about the channel or local oscillator frequencies.

The main purpose of the experiments is to test for the suitability of our technique in different kinds of real-world channels. A role *configuration* corresponds to the allocation of a role (Alice, Bob or Eve) to a certain spatial position. In all performed experiments, all six possible role *configurations* were tested, as presented in Table 6.1.

Config./Position	X	Y	Z
I	Alice	Bob	Eve
II	Bob	Alice	Eve
III	Alice	Eve	Bob
IV	Bob	Eve	Alice
V	Eve	Alice	Bob
VI	Eve	Bob	Alice

Table 6.1.: Set of all possible *role configurations*.

6.3.2. Experimental Variables

When generating a new secret key, it is of utmost importance that this key looks as *as-random-as-possible*, similar on both legitimate parties and different to the key estimated by an eavesdropper. We conduct several experiments in order to evaluate the feasibility of our method under different conditions or experimental variables: environment, key extractors, quantization levels and key agreement rate.

6.3.2.1. Environments

We tested our protocol under different kind of environments concerning their dynamic, namely *rural (R)*, *semi-urban (SU)* and *urban (U)* environments.

Indoor In this section, our experimental efforts to measure the feasibility of our technique in a typical indoor environment are described. We conducted the indoor experiments in October 2013.

The experiments were performed during an inactivity time period at our Institute. This guarantees that the environment is static and minimizes the interference of other signals.

In order to test the feasibility of our method, we test at different distances, namely along the corridor at our Institute. For this group of experiments, two transceiver platforms (a set of USRP, laptop and antenna) are placed constantly at positions X and Y, whereas the movable platform is subsequently placed at eleven different positions, represented as $Z = a, b, c, ..., k$ (see Figures 6.6 and 6.7). Each position Z defines a certain layout. We performed a number of runs $N_r = 5$ for all role *configurations* for each *layout*.

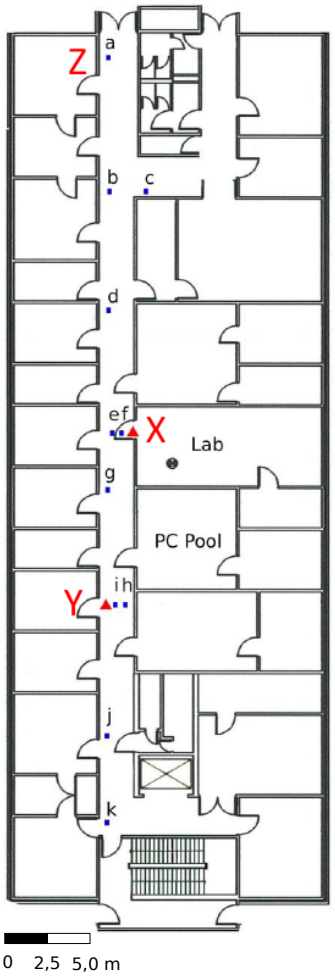


Figure 6.6.: Corridor: All Layouts (Z = a,...,k).

Figure 6.7.: Inside the Corridor.

Figure 6.8.: Indoor Environment (hallway in the Institute).

We have implemented a script that sets the configurations automatically (i.e. automatically changes the roles of each transceiver platform after a certain number of runs of the same experiment) for each layout. The platform is manually moved to the next position after the script finishes executing. Then, the script is restarted. This procedure is repeated for each one of the layouts $Z = a, ..., k$.

Outdoor All the outdoor experiments were conducted in spots located around the *KIT-Campus Süd* area, as depicted in Figure 6.9, during the summer of 2014.

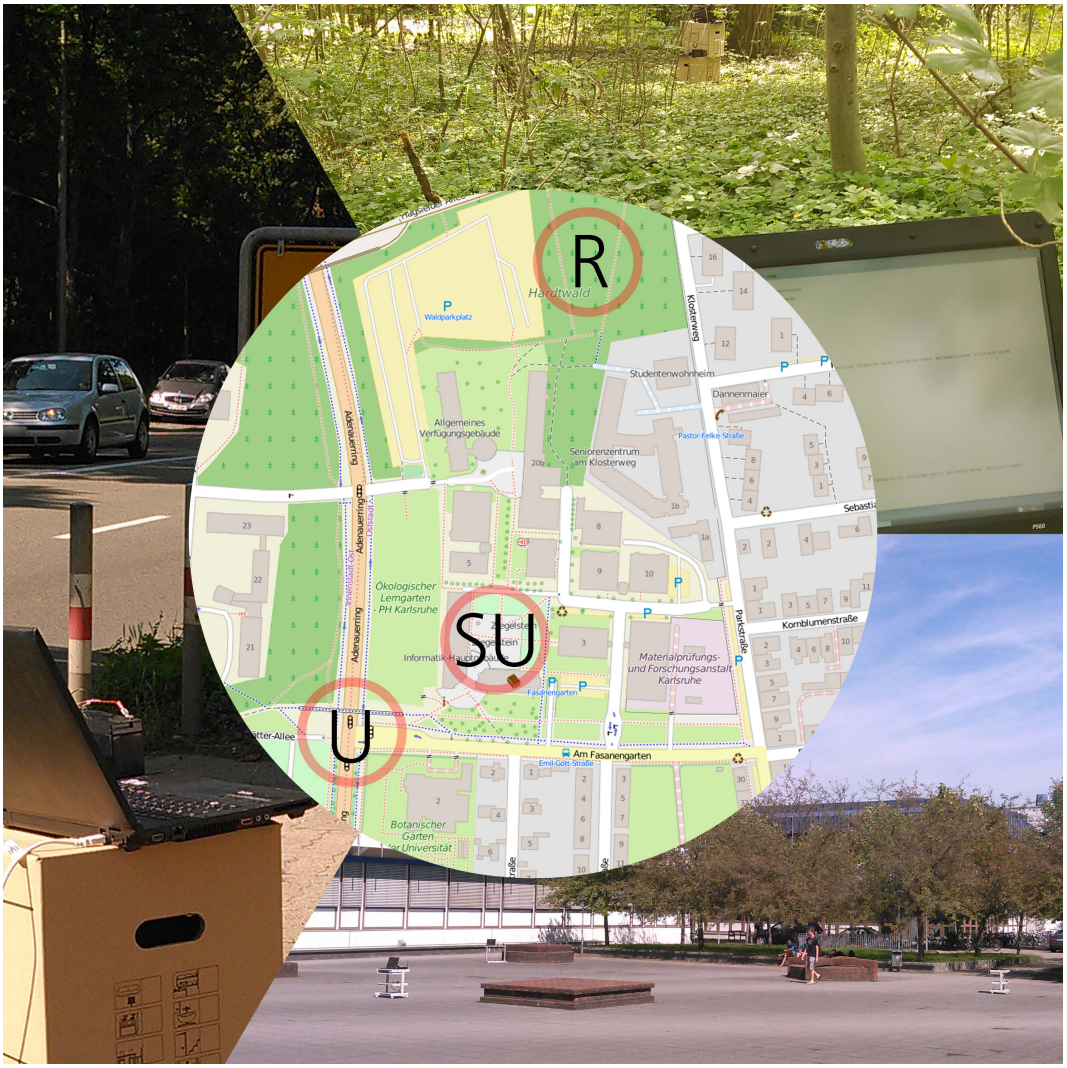


Figure 6.9.: Outdoor Environment (*KIT-Campus Süd*): Places where the experiments were conducted. R: Rural; SU: Semi-Urban; U: Urban.

Rural The experiments for this kind of environment were performed in a *forest environment*. This environment is quite static, however still shows complex characteristics. It is typically characterized by the presence of static and dense obstacles, namely trees and other kinds of vegetation, as shown in Figure 6.10. Vegetation is known to have a big impact on the results of outdoor tests [AP09].

The antennas were placed in a triangular pattern approximately 15 meters apart from each other.

Figure 6.10.: Outdoor Environment (Rural). X, Y and Z mark the positions where the antennas were placed.

Semi-Urban We conducted the experiments in the *courtyard* in front of the Informatics Department building. This location is a typical example of a semi-urban environment, where one can find different kind of static obstacles (like buildings) and some smaller moving objects (like bicycles or even people). In order to consider a variety of possible different situations, four different cases were considered, as schematically presented in Figure 6.11:

a. **Line-of-sight (LOS)** between all parties, X_a, Y and Z (Exp. SU a);

b. **LOS between all parties**, Position X_b **close to a wall** (SU b);

c. one party at position X_c has **LOS** contact to another party (SU c);

d. one party at position X_d has **no LOS** contact with any other party (SU d).

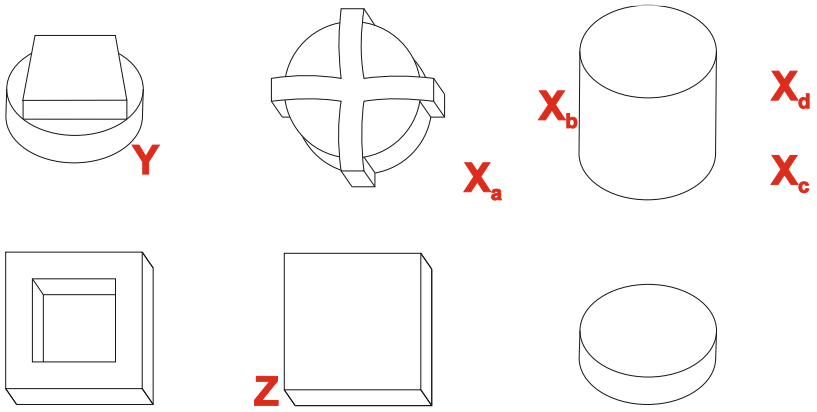
Figure 6.11 shows the three parties placed in a triangle configuration, also approximately 15 meters apart from each other. The antenna placed in position X had its position changed a few times to obtain the configurations (X_a, X_b, X_c and X_d).

Urban We chose the *road junction* in the area around the Informatics Department building as representative of a dynamic environment. This environment is characterized by intensive movement of objects. Particularly, it consists of a road with four lanes and intensive traffic. There is also a bridge used by pedestrians and bikes, as seen in Figure 6.12. Two different scenarios were considered:

1. All parties located at the same height in the road;

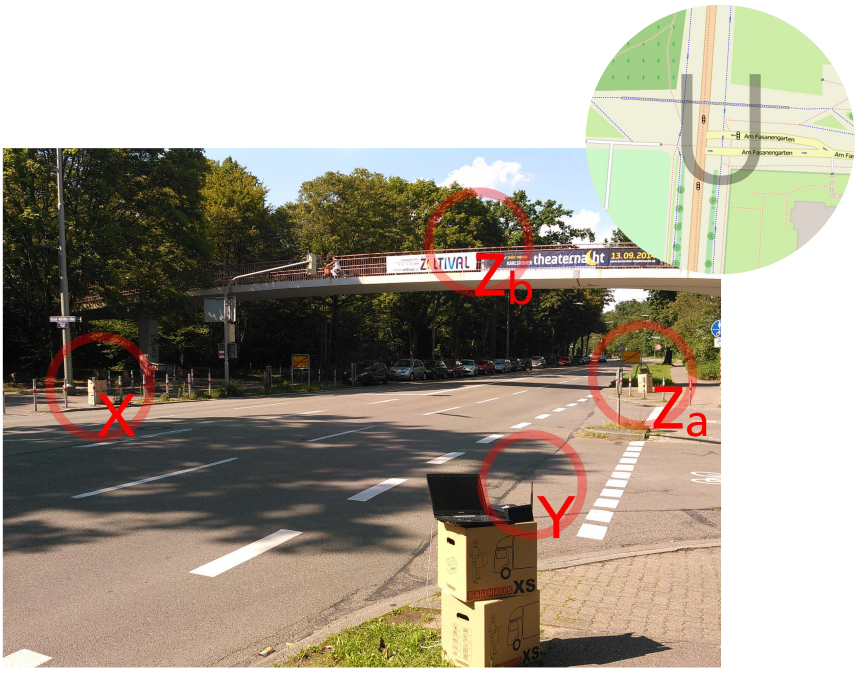
2. Party Z placed at a different height, namely on the bridge at a higher level (position Z_b).

6.11.1: Picture of the Courtyard.

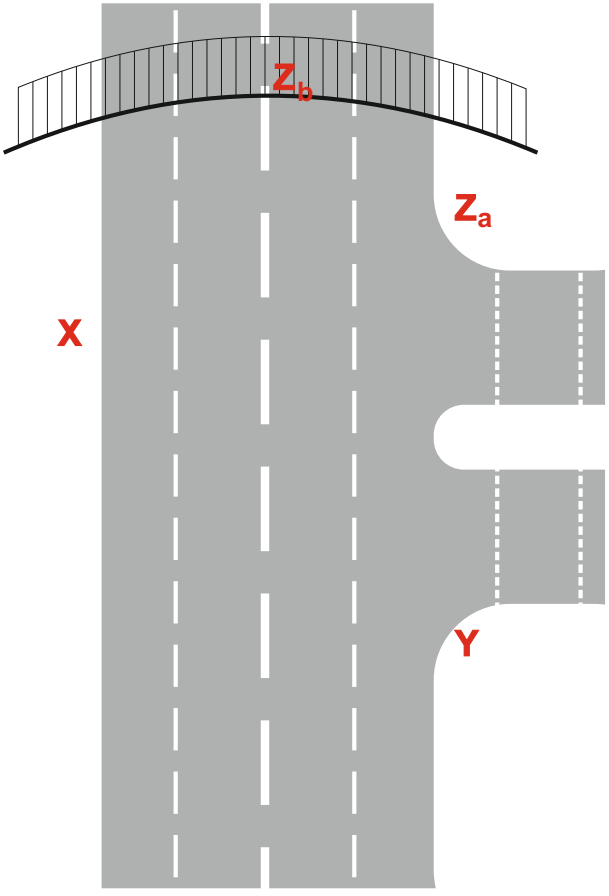


6.11.2: Scheme of the positions where the antennas were placed.

Figure 6.11.: Outdoor Environment (Semi-Urban): Courtyard located next to the Informatics Department Building. Antennas were placed in positions X, Y and Z.



6.12.1: Picture of the road junction.



6.12.2: Scheme of the positions where the antennas were placed.

Figure 6.12.: Outdoor Environment (Urban): Road junction located immediately next to the Informatics Department building.

6.3.2.2. Quantization Bits

An important parameter that needs to be considered when developing the extractor is the number of quantization bits, Q, used to perform the quantization step (cf. Section 5.3.2). Therefore, we study the influence of this parameter on the key agreement rate, KAR, and on the randomness of the key. Recalling, using the notation of Section 4.2, the number of quantization levels, M, is given by $M = 2^Q$.

6.3.2.3. Key Extractors

In Section 5.3, we define *key extractors* as a means of extracting different features of a signal and combining them. One of the main challenges of fading-based key exchange is to find out *what* features to extract and *how* to combine them. Thus, we can also designate the key extractors by *key combiners*. In Chapter 5, we explained in detail how to combine the frequencies with the amplitudes. Nevertheless, we only introduced one simple extractor, namely the *product of averages* key extractor, where the average of the magnitude of the amplitudes is multiplied by the average of the interval between zero-crossings (which depends on the frequency of the signal). Next, we present other combiners. For the sake of simplicity of notation, let us define X as the average of the amplitudes magnitude of the received signal, as shown in Figure 5.4, i.e.,

$$X := \frac{1}{N} \sum_{k=1}^{N} |X_k|,$$

where N is the total number of extreme points, and let Z be the average of the size of the interval between two zero crossings, i.e.,

$$Z := \frac{1}{M} \sum_{k=1}^{M} (Z_l - Z_{l-1}),$$

where M is the total number of zeros. The averaging process is introduced in order to reduce the influence of the noise from the measurements of these two quantities - amplitude and zeros. Note that the zero-crossings are directly related to the frequency, f, of the signal by $f = 1/(2Z)$.

Keeping this notation in mind, we define the following *combiners*:

Amplitudes (X) This extractor mainly considers the effects of fading in the signals, which is reflected in the amplitude of the signals. It is the *basic extractor* and ignores any signal's frequency information.

$$q(i) := X \tag{6.1}$$

Zeros (Z) This extractor only takes the effects of the hardware into consideration. It does not contemplate any information about the fading. It only serves as a reference for comparison to the results of the other extractors.

$$q(i) := Z \tag{6.2}$$

Product of Amplitudes and Zeros (XZ) This extractor is the basic combiner of amplitudes and zeros that we consider. It combines the effects of fading and local oscillators (hardware) together by multiplying the (average of) amplitudes with the (average of) zeros. This combiner was already introduced in Section 5.3.1, under the designation of *Product of Averages*.

$$q(i) := XZ \tag{6.3}$$

Square of Both ((XZ)^2) In this extractor both effects of fading and local oscillators by squaring the product of the averages with the amplitudes are combined. By introducing this extractor, we study how the square operation affects the results.

$$q(i) := (XZ)^2 \tag{6.4}$$

Division of Amplitudes by Zeros (X/Z) This extractor is similar to the XZ-Extractor. The only difference resides in the mathematical operation connecting these effects, namely a *division*.

$$q(i) := X/Z \tag{6.5}$$

Trimmed Means (trm) This extractor is similar to the XZ-Extractor (cf. Section 6.3.2.3). The difference resides in the fact that the 10 % outlier values are excluded (also called truncated mean), i.e., the 5 % lower and the 5 % values do not count for the calculation of the average. By using this extractor, we search for excluding any atypical values that may occur due to unforeseen reasons: wireless interference, bad measurement and noise. Mathematically, this combiner is defined the following way:

$$q(i) := X'Z', \tag{6.6}$$

where X' and Z' stand for the trimmed (or truncated) average of the amplitudes, i.e.,

$$X' := \frac{1}{N'} \sum_{k=1}^{N'} |X_k|,$$

and

$$Z' := \frac{1}{M'} \sum_{k=1}^{M'} (Z_l - Z_{l-1}),$$

where N' and M' stand for the number of amplitude ($|X_k|$) and zero ($|Z_l - Z_{l-1}|$) elements excluding the 5 % lower and the 5 % higher values.

6.3.3. Quality Criteria

After the execution of the fading-based key exchange protocol, we hope that Alice and Bob share as many similar bits as possible before the information reconciliation step takes place, whereas Eve is able to guess only around 50 % of the secret bits. This idea is captured by the concept of *key agreement rate*, which is defined in Section 5.4.5.

At the same time, it is very important that the key exhibits *random* characteristics, e.g. by avoiding long strings of 1s and 0s. As in [PJC+13, YMR+09], we employ an often used test suite for the evaluation of the randomness of the generated bitstring, namely the NIST test suite, as described in Section 6.3.3.3.

6.3.3.1. Key Agreement Rate (KAR)

The *key agreement rate* was already defined in Section 5.4.5. This parameter is used also in [PJC+13]. The authors use the terminology *bit mismatch rate (BMR)*, which is $BMR = 1 - KAR$.

Ideally, due to the reciprocity property of the wireless channels, we predict to achieve values around 100 % for $KAR(A, B)$. Due to multipath interference of fading channels, values around 50 % for $KAR(A, E)$ and $KAR(B, E)$ are expected. Again, this means that Eve has no further advantage for reconstructing the key by analyzing the signals she receives compared to when she merely tries to randomly guess the bits of the secret key (i.e., having no information at all).

6.3.3.2. Bit Generation Rate

We define the *bit generation rate* BGR as the number of *shared secret bits generated per time unit*. In our setup, BGR can be given by

$$BGR := \frac{KAR \times N \times Q}{\Delta T}, \tag{6.7}$$

where KAR is the key generation rate, N the number of iterations according to the protocol shown in Section (cf. Section 6.3.1), Q the number of quantization bits and ΔT the time needed to perform the protocol.

6.3.3.3. Randomness - the NIST Statistical Test Suite

Calculating *a priori* the randomness associated to the physical characteristics of an environment proved to be a very difficult task, if not even impossible. Accordingly, we consider measuring the randomness *a posteriori*, i.e., after the key extraction process. As in other works [PJC+13, YMR+09, MTM+08], we employ the *NIST Statistical Test Suite*. This suite was developed by the *Random Number Generation Technical Working Group (RNG-TWG)* of the *National Institute of Standards and Technology (NIST)*. According to the documentation, the purpose of this group was *to develop a battery of statistical tests to detect non-randomness in binary sequences constructed using random number generators and pseudo-random number generators utilized in cryptographic applications* (cf. [BRS+10]). Therefore, these tests intend to detect any *deviations of a binary sequence from randomness*. In regular cryptographic applications, this may have origin in a bad random generator design or some other anomalies. For the sake of self-containedness of this work, we briefly introduce the notions of Random Number Generators (RNG) and Pseudorandom Number Generators (PRNGs). The interested reader should refer to [BRS+10].

Random Number Generators (RNGs) These generators extract their randomness from an entropy source using some processing function (the entropy distillation process). This function should be implemented in such a way that no long strings of 0s or 1s appear. A frequent entropy source is the electronic noise originated in an electronic circuit, the timing of user processes (e.g., movements with the mouse or

keystroking speed) or even quantum effects in a semiconductor. The output of RNGs may be used directly in cryptographic operations or may be used as the input of a Pseudorandom Number Generators (see under). If used directly, one should test the string for randomness, as some *irregular patterns* may not necessarily have origin in some random process, but rather be the superposition of deterministic effects. Statistical tests help to detect this regularities and test for randomness. Under some circumstances, usual RNGs have the drawback that the string generation rate might be too low. This justifies the use of a PRNG.

We should note that the key exchange methods based on the physical properties of the environment are methods for the physical generation of randomness, where the entropy source is the unknown physical channel between the parties. However, since the channel is reciprocal, it allows for *common (or shared) randomness*. Using this method, we simultaneously achieve *generation* and *sharing* of randomness.

Pseudorandom Number Generators (PRNGs) PRNGs may be more suitable to produce large quantities of random numbers, However, they need an input value, called *seed*. The output of a PRNG is a deterministic function of this value. This means that a PRNG needs a RNG for the generation of this seed, containing all the randomness. Generally, the outputs of a PRNG have better statistical properties than those of the RNGs. Pseudorandom functions also rely on the existence of one-way functions, since the seed should be kept hidden for an adversary knowing the output of the generator (see [Gol00] and [KL07] for details). The NIST statistical tests aim at *finding some pattern showing non-randomness*.

Implementations of the NIST suite can be found freely available in the Internet. The NIST itself provides a C-implementation, with an awkward interface and does not allow to be called from any outside scripts. Since we deal with more than 8000 generated keys, it is not reasonable to proceed manually. For this reason, we use a Python implementation of these specifications [Ger]. Curiously enough, the results of the reference implementation are different from those presented in the documentation. The results of the Python implementation seem to be much more in agreement (until the fifth decimal number) with those from the documentation.

The output of all these tests is a so-called *P-value*. This value corresponds to the *probability that a perfect random number generator would have produced a sequence less random than the sequence that was tested, given the kind of non-randomness assessed by the test* [BRS+10]. A *P-value* ≥ 0.01 means that the sequence would be considered to be random with a confidence of 99%, whereas a *P-value* ≤ 0.01 means that the conclusion was that the sequence is non-random with a confidence of 99%. *P-value* $= 1.0$ would correspond to perfect randomness, whereas *P-value* $= 0.0$ to a perfect deterministically generated sequence.

This suite defines fifteen possible tests, which check if the input test sequence fulfill conditions that a random sequence should meet. Next, we introduce these tests in a nutshell. Details can be found in [BRS+10]. Some of these tests are also briefly described in [PJC+13].

Used Tests Since other tests require too long strings, not available to us, we only used six of tests presented in [BRS+10], namely the *Cumulative Sums Test (C)*, *Frequency (monobit) Test (F)*, *Runs Test (R)*, *Discrete Fourier Transform Test (D)*, *Serial Test (S)*, and the *Approximate Entropy Test (A)*.

For the sake of self-containedness of this work, we shortly explain these tests. For more details, refer to [BRS+10].

Cumulative Sums Test Also known as *cumsum test*. For each bit, it calculates the difference of the number of 0s appearing up to a certain point with the number of 1s. In other words, it calculates the position of a random walk whose variable is the bits of the sequence: to bit 1, it corresponds to a movement to the right (+1); to bit 0, a movement to the left (−1). If this value diverges strongly from zero (the initial position), then we talk of a non-random teststring;

Frequency (monobit) Test This test focuses on counting the number of 0s and 1s in the test sequence. It checks whether the number of 0s and ones are approximately the same, as it is expected in a random sequence;

Runs Test This test checks the number of runs of 0s and 1s of several lengths and compare to the values of a random sequence. It basically tests if the change from 0s to 1 or vice-versa are too slow or too fast;

Serial Test This test checks if every m-bit pattern has the same probability of appearing as every other m-bit pattern, which happens in a random sequence;

Approximate Entropy Test This test compares the frequency of overlapping blocks of two consecutive lengths (lengths m and $m + 1$) against the expected result for a random sequence.

Discrete Fourier Transform (Spectral) Test Hereby the spikes of a Fourier Transformation are used for testing periodicity. If too many spikes appear, it means there is a periodic repetition in the teststring;

6.3.4. Results

After collecting the data, we performed a thorough analysis of the results. For all runs and environments, we generated quantizer profiles for all extractors and for different values of Q. As an example, the typical output of the quantizer for the extractor XZ for $Q = 3$ for an indoor environment is depicted in Figure 6.13. The reciprocity property is reflected in the fact that both upper plots are similar, whereas the multipath interference becomes clear when we compare the upper with the downer plots in each column.

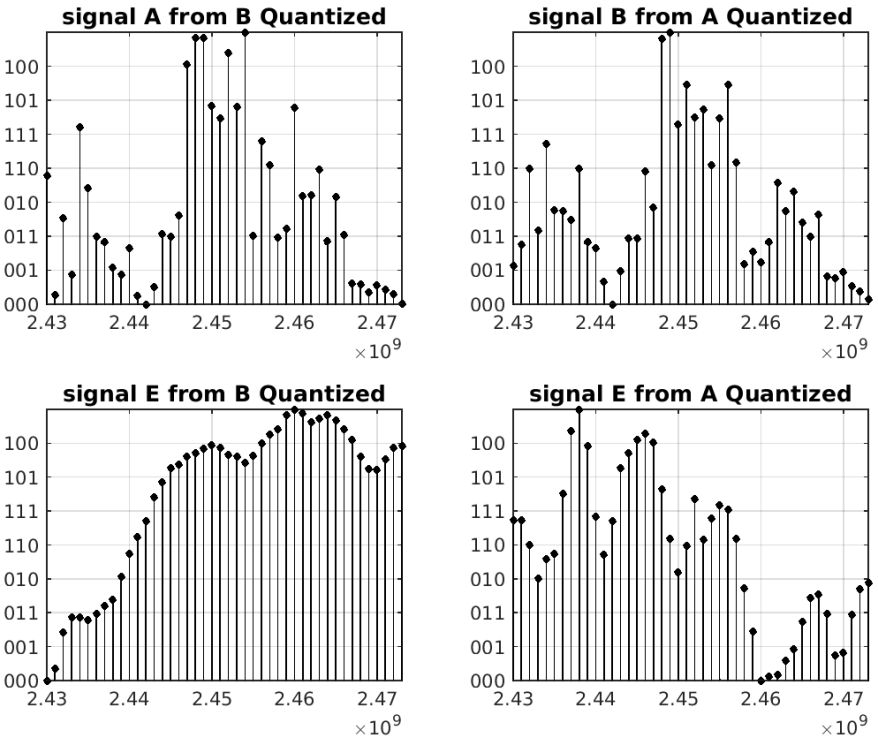


Figure 6.13.: Typical output of the quantizer for $Q = 3$. Upper left: signal received by Alice when Bob sends; Upper right: signal received by Bob when Alice sends; downer left: signal received by Eve when Bob sends; downer right: signal received by Eve when Alice sends.

In A.1, we show the dependency on Q of KAR and min-entropy (cf.[BK12]) of the generated keys at Alice and Bob (before the information reconciliation step) for the extractor XZ, which is the one showing best results (as we describe later in Section 6.3.5.2). We present the results of the NIST tests for the extracted key. The results are taken on all five runs, i.e., for a data set containing five elements. For the sake of simplicity and w.l.o.g., we only present the plots for four indoor positions, namely $Z = a$, $Z = d$, $Z = g$ and $Z = k$, and for all seven outdoor positions (R, SU a, SU b, SU c, SU d, U a, U b). Afterwards, we combine the data of all six configurations (see Table 6.1) results for each position. In Appendix A.2, we plot the results for the KAR values depending on Q in a box plot. We also put forward the results of the NIST tests for 5 runs/configuration $\times$ 6 configurations/position, i.e., for a total of 30 data points. We restrict ourselves to show the results for the positions already mentioned in Appendix A.1. Next, we present the results for the KAR values depending on Q in a box plot and the number of tests passed for each test in a bar chart, where C, F, R, D, S and A in each bar stand for **C**umsums test, **F**requency (monobit) test, **R**uns test, **D**iscrete Fourier Transform test and **A**pproximate entropy test, respectively. As we seek the best extractor for indoor and for outdoor environments separately, we divide the data in indoor and outdoor data elements. Since we performed 5 runs per configuration, 6 configuration per position, 11 positions for indoor ($Z = a, ..., k$) and 7 positions for outdoor experiments (R, SU a, SU b, SU c, SU d, U a, U b), we have a total of $5 \times 6 \times 11 = 330$ data points for indoor and $5 \times 6 \times 7 = 210$ for outdoor, which we analyze separately.

6.3.4.1. Extractor Amplitudes (X)

Indoor

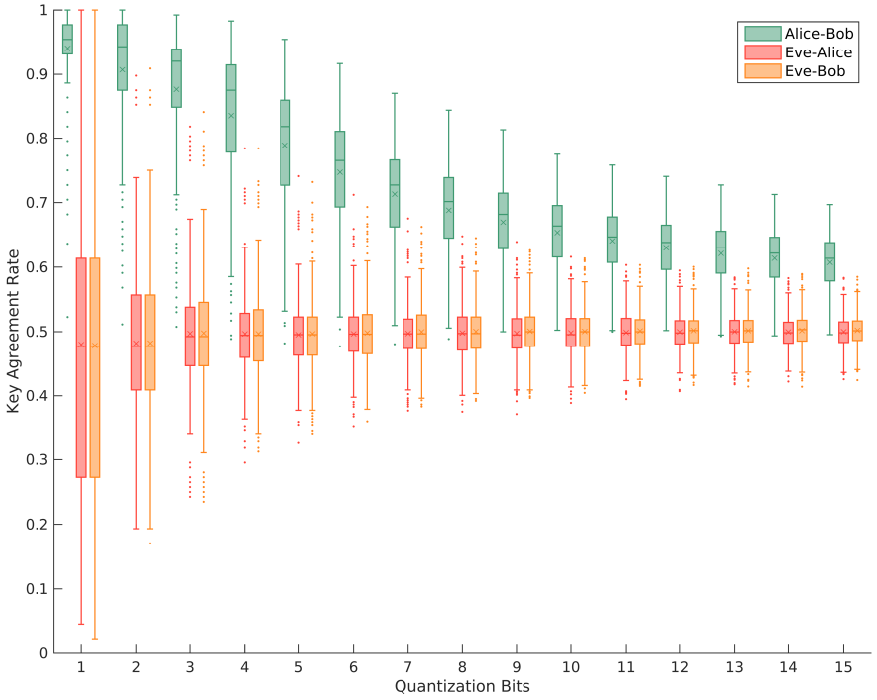


Figure 6.14.: Key Agreement Rate vs Quantization Bits.

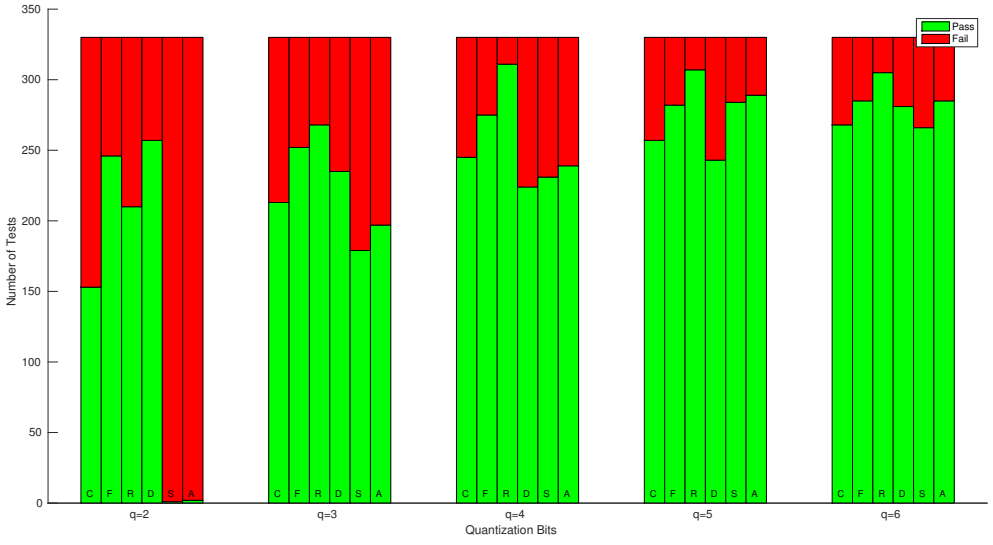


Figure 6.15.: Result of the NIST tests.

Outdoor

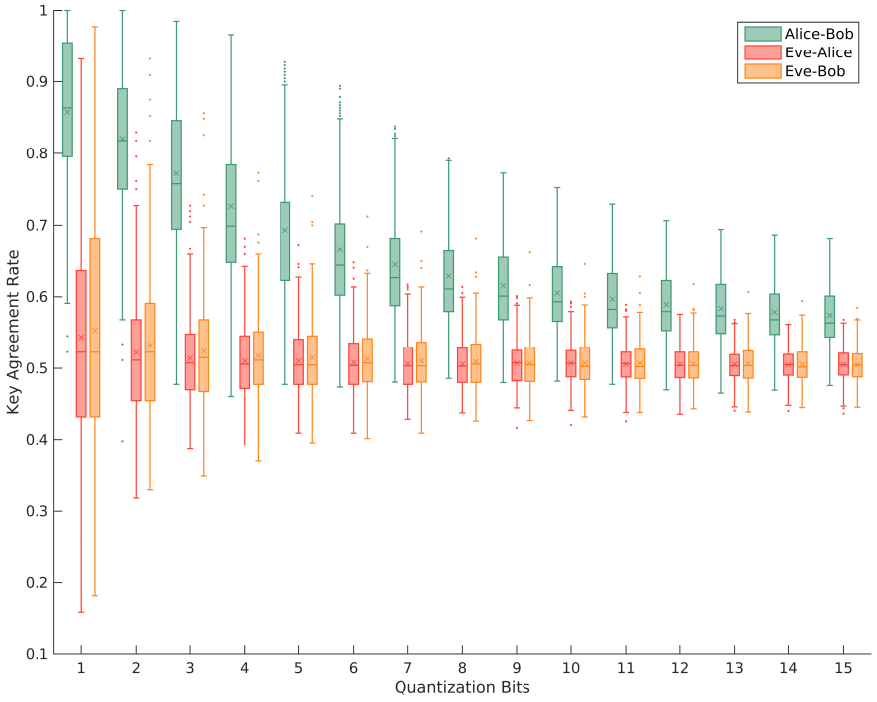


Figure 6.16.: Key Agreement Rate vs Quantization Bits.

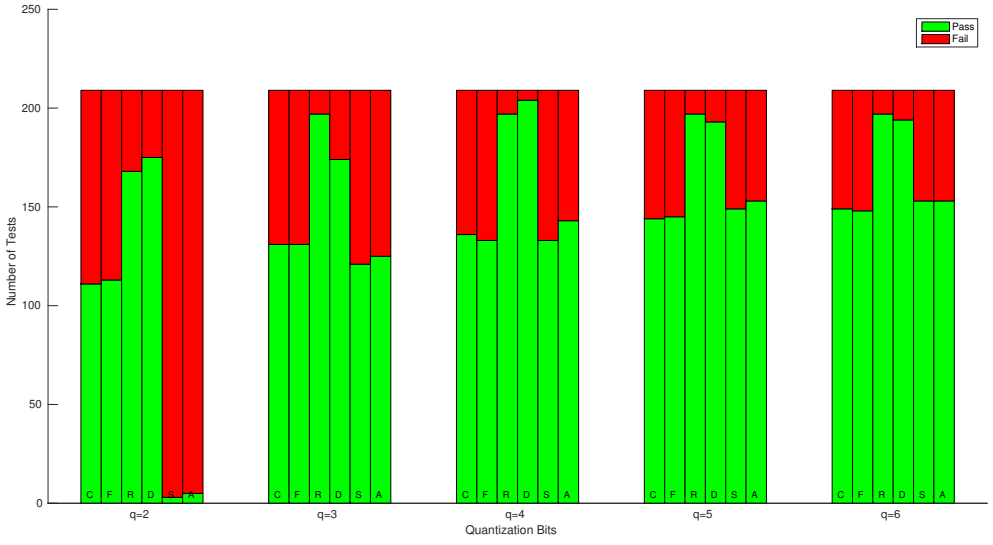


Figure 6.17.: Result of the NIST tests.

6.3.4.2. Extractor Zeros (Z)

Indoor

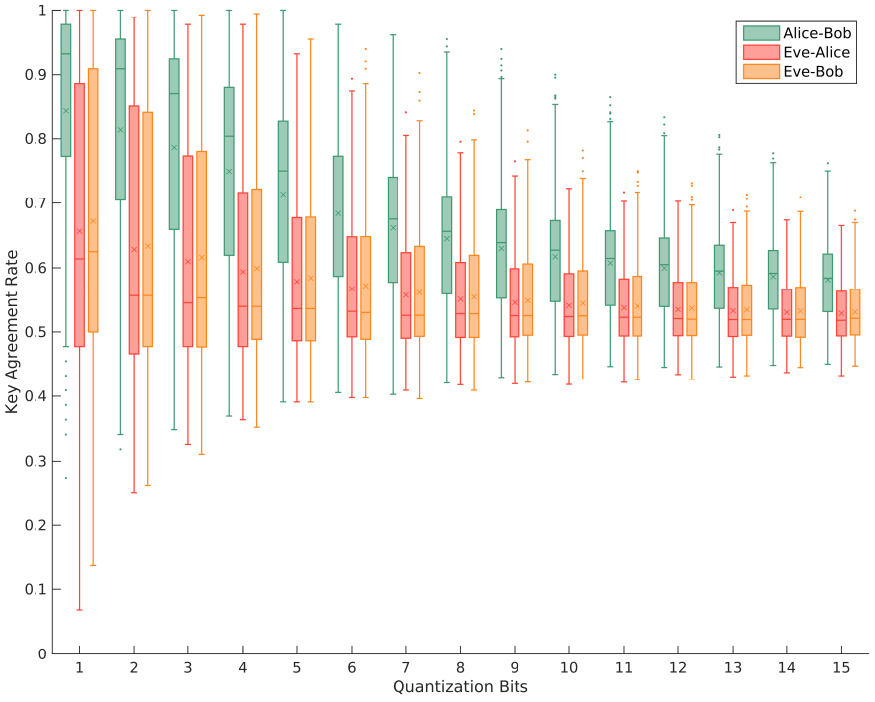


Figure 6.18.: Key Agreement Rate vs Quantization Bits.

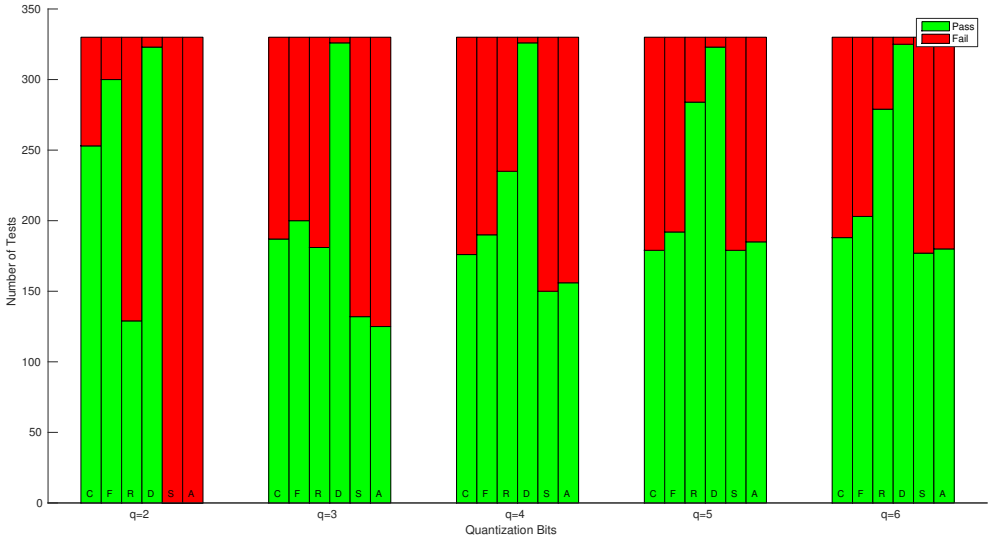


Figure 6.19.: Result of the NIST tests.

Outdoor

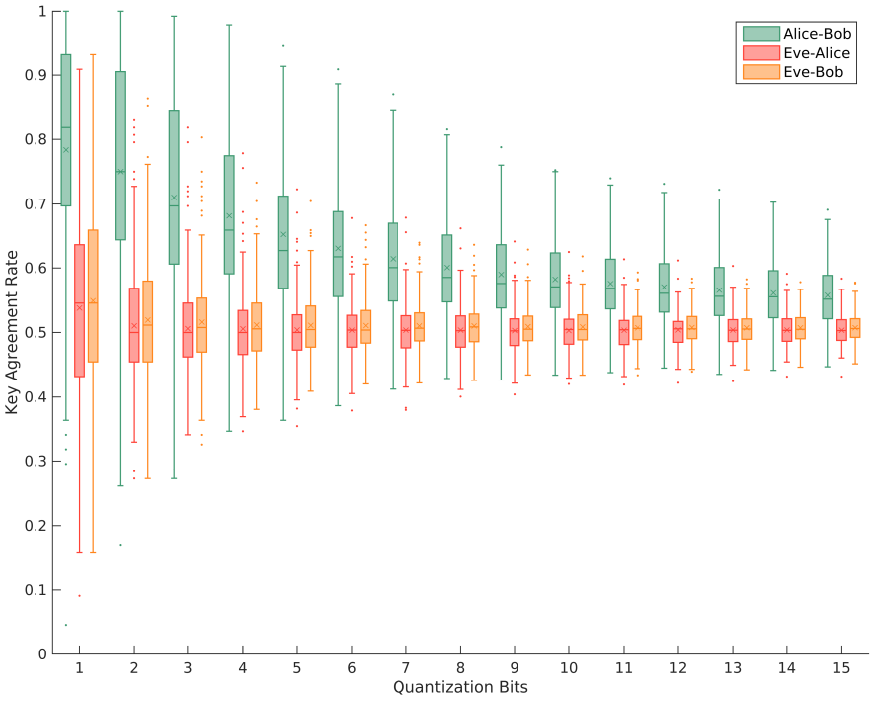


Figure 6.20.: Key Agreement Rate vs Quantization Bits.

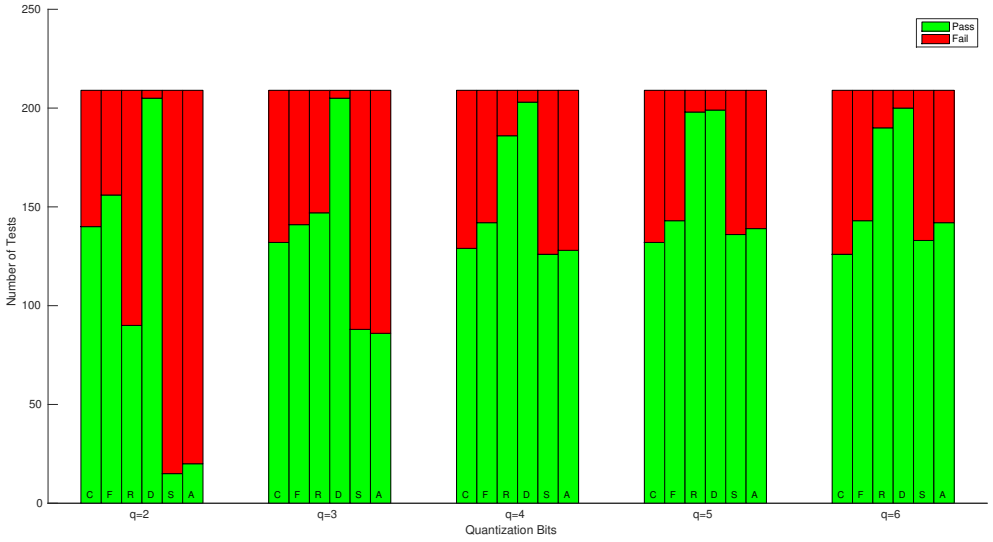


Figure 6.21.: Result of the NIST tests.

6.3.4.3. Extractor Product of Amplitudes and Zeros (XZ)

Indoor

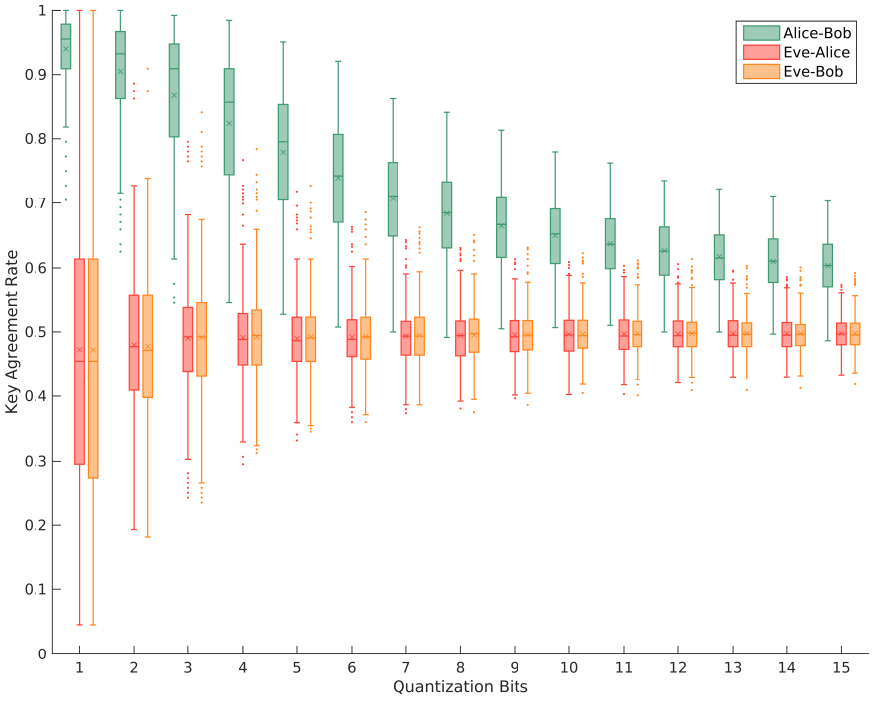


Figure 6.22.: Key Agreement Rate vs Quantization Bits.

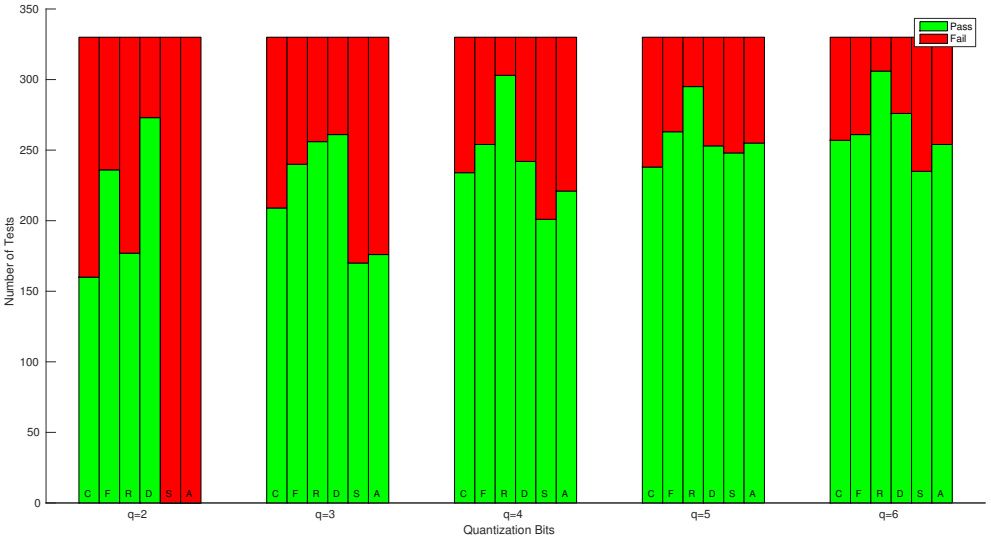


Figure 6.23.: Result of the NIST tests.

Outdoor

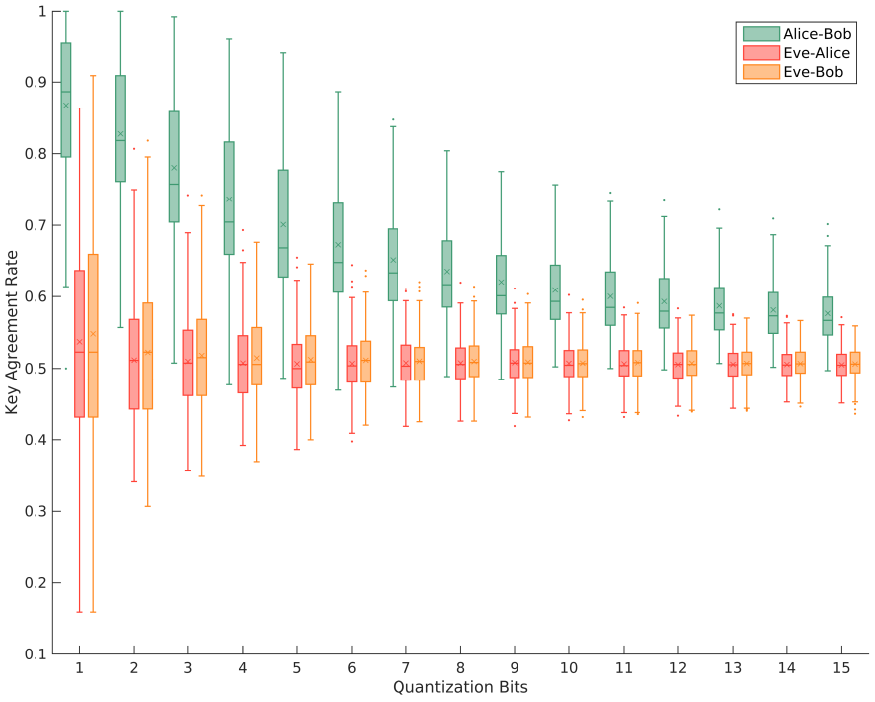


Figure 6.24.: Key Agreement Rate vs Quantization Bits.

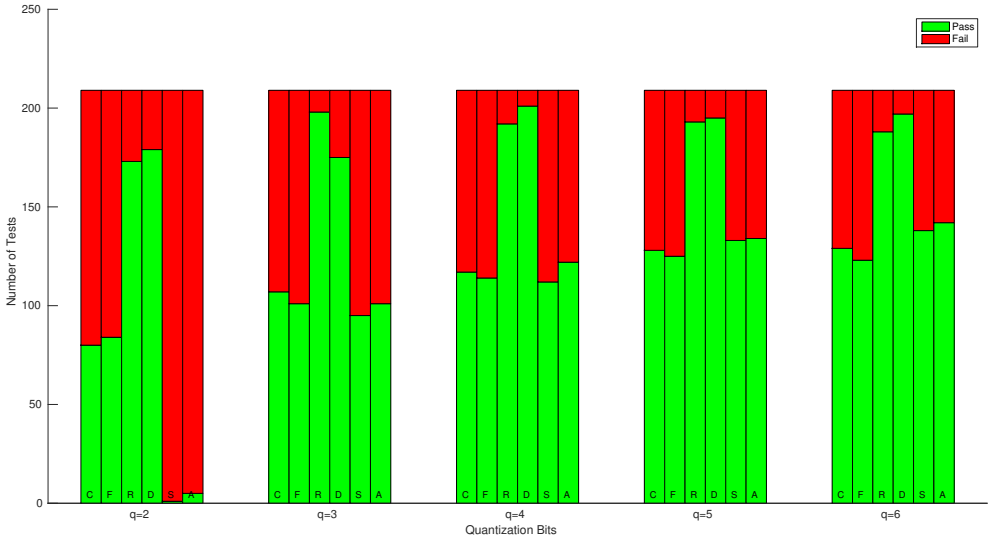


Figure 6.25.: Result of the NIST tests.

6.3.4.4. Extractor Square of Both ((XZ)^2)

Indoor

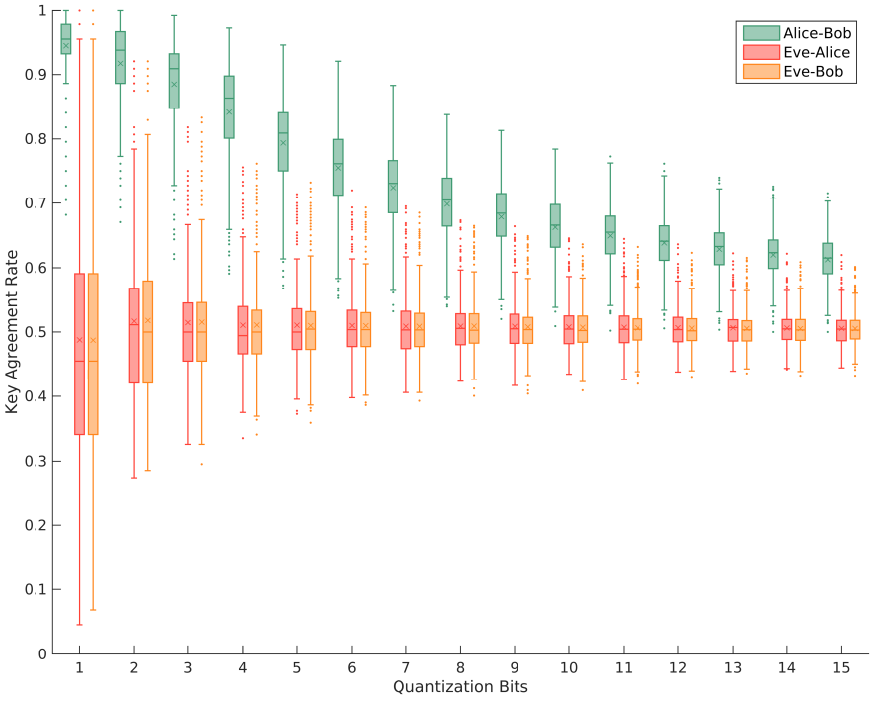


Figure 6.26.: Key Agreement Rate vs Quantization Bits.

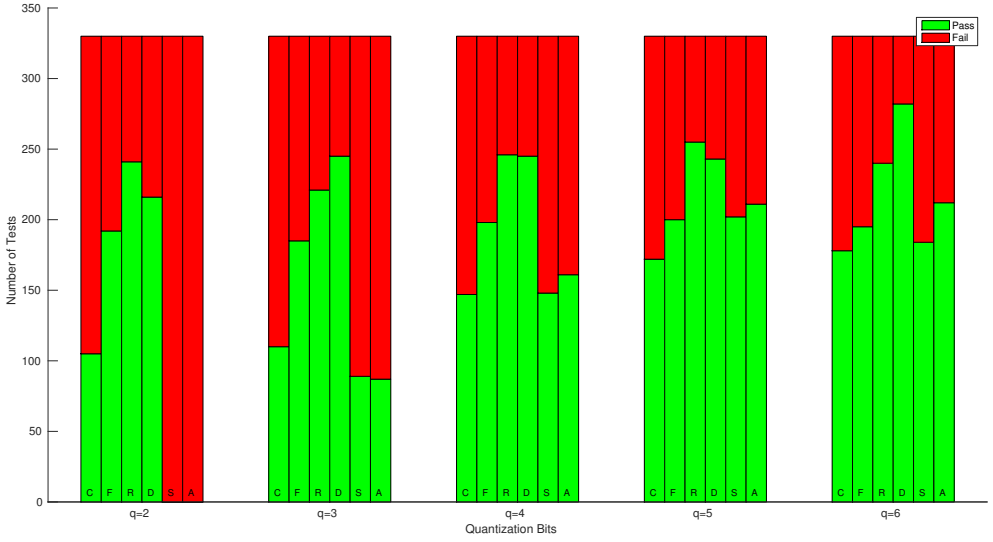


Figure 6.27.: Result of the NIST tests.

Outdoor

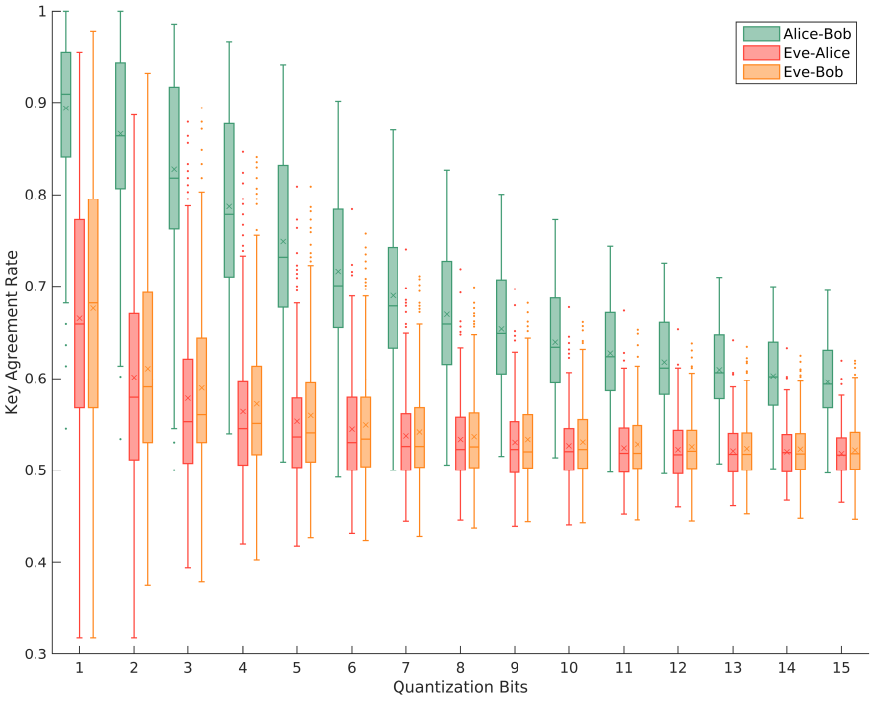


Figure 6.28.: Key Agreement Rate vs Quantization Bits.

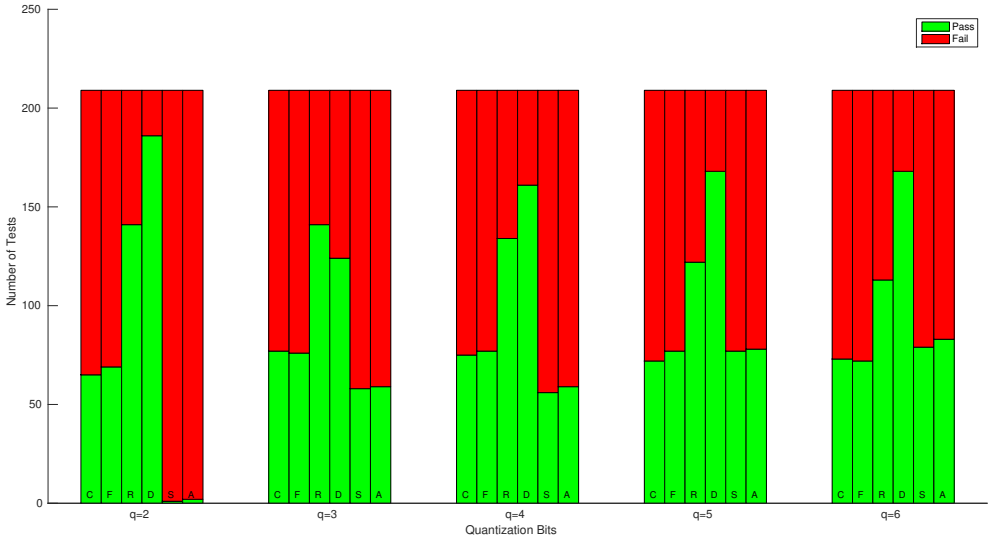


Figure 6.29.: Result of the NIST tests.

6.3.4.5. Extractor Trimmed Mean (trm)

Indoor

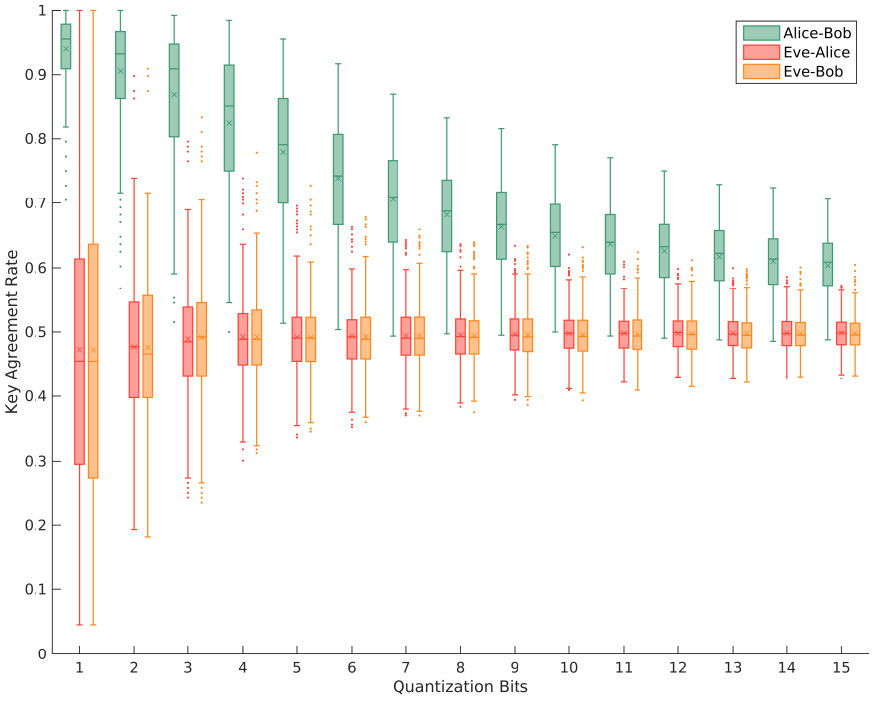


Figure 6.30.: Key Agreement Rate vs Quantization Bits.

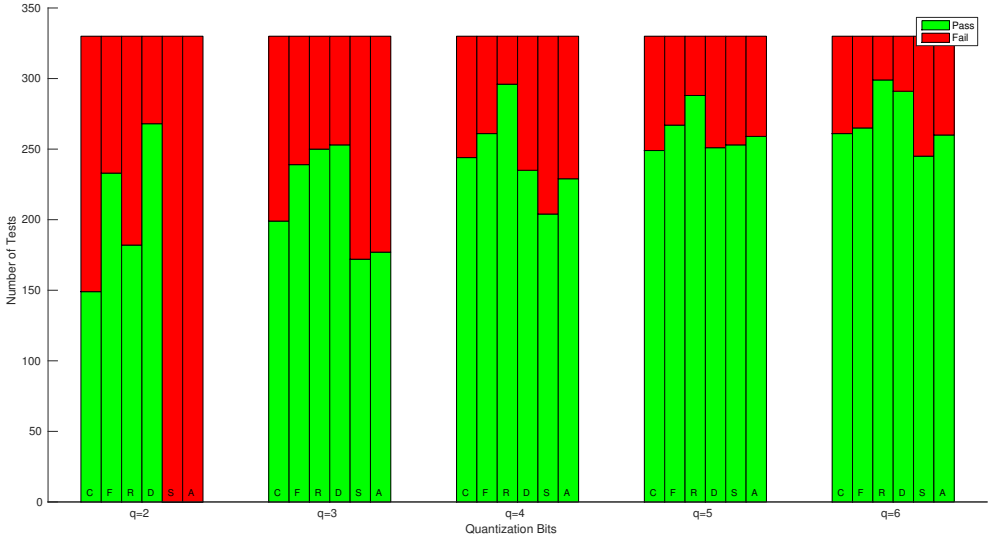


Figure 6.31.: Result of the NIST tests.

Outdoor

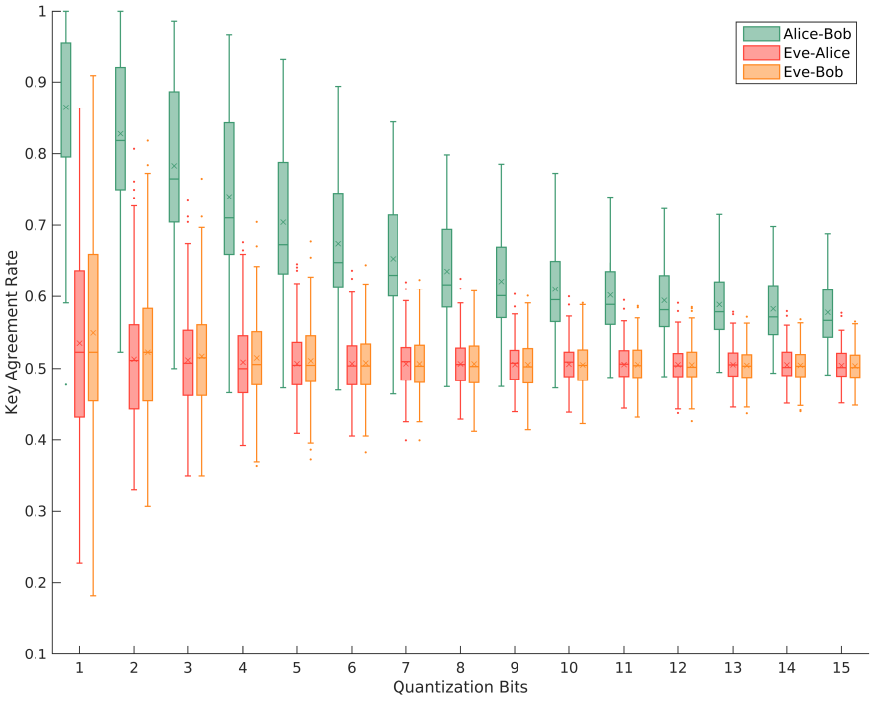


Figure 6.32.: Key Agreement Rate vs Quantization Bits.

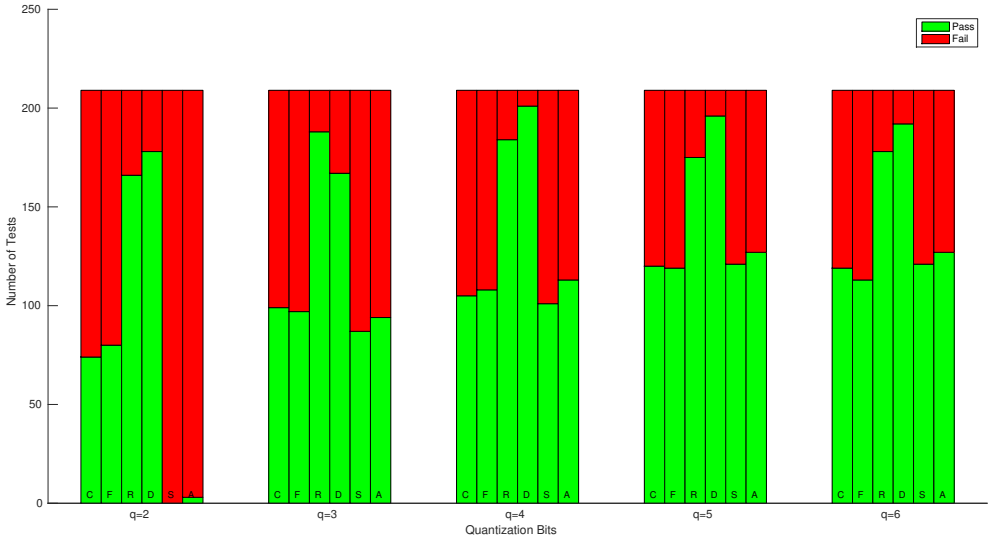


Figure 6.33.: Result of the NIST tests.

6.3.4.6. Extractor Division Amplitudes by Zeros (X/Z)

Indoor

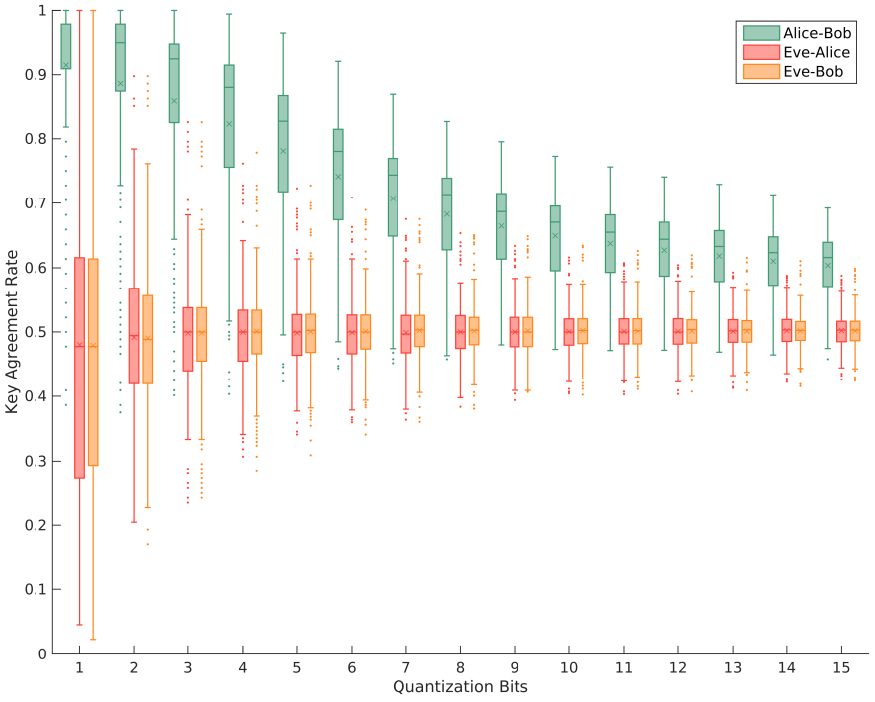


Figure 6.34.: Key Agreement Rate vs Quantization Bits.

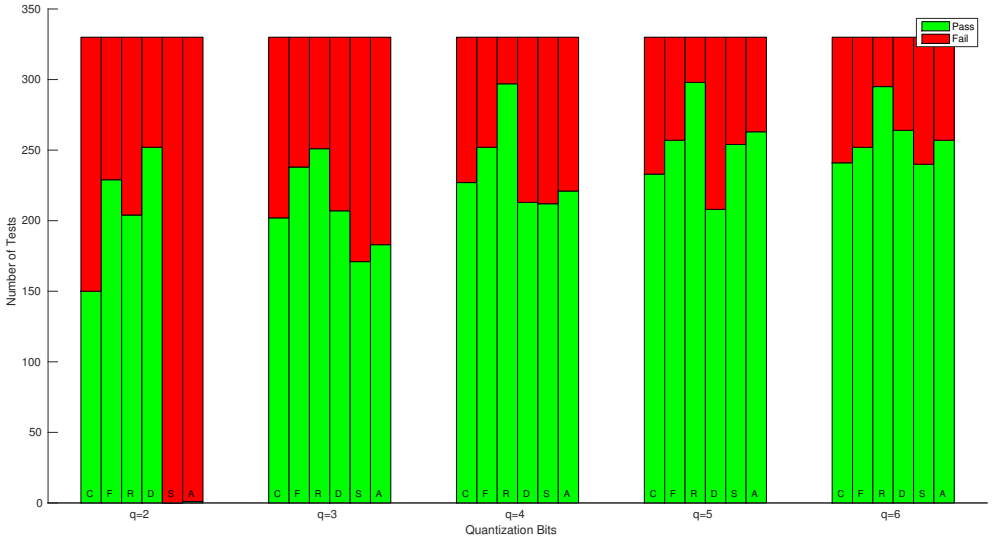


Figure 6.35.: Result of the NIST tests.

Outdoor

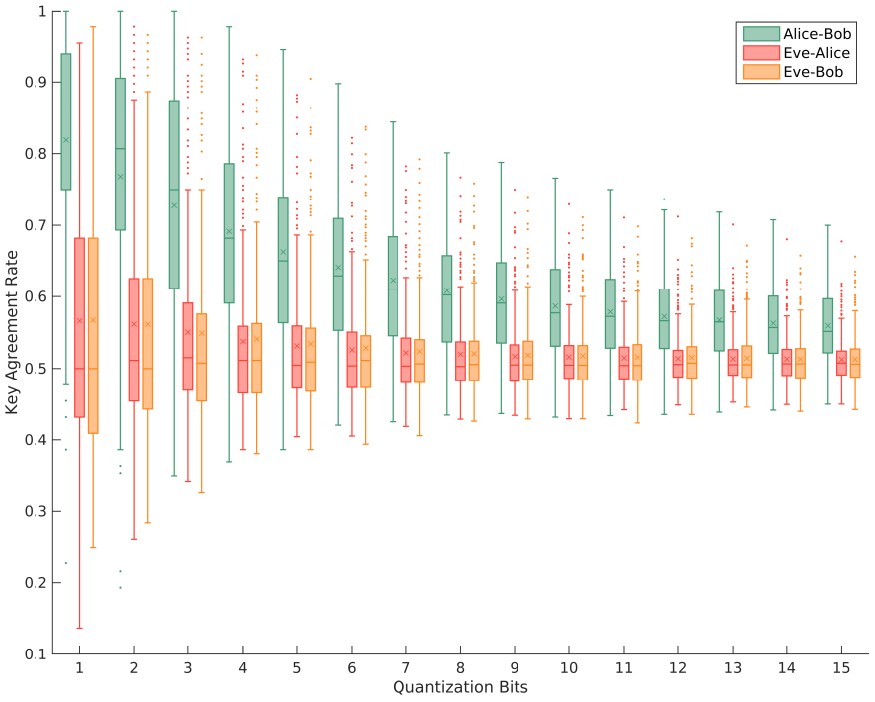


Figure 6.36.: Key Agreement Rate vs Quantization Bits.

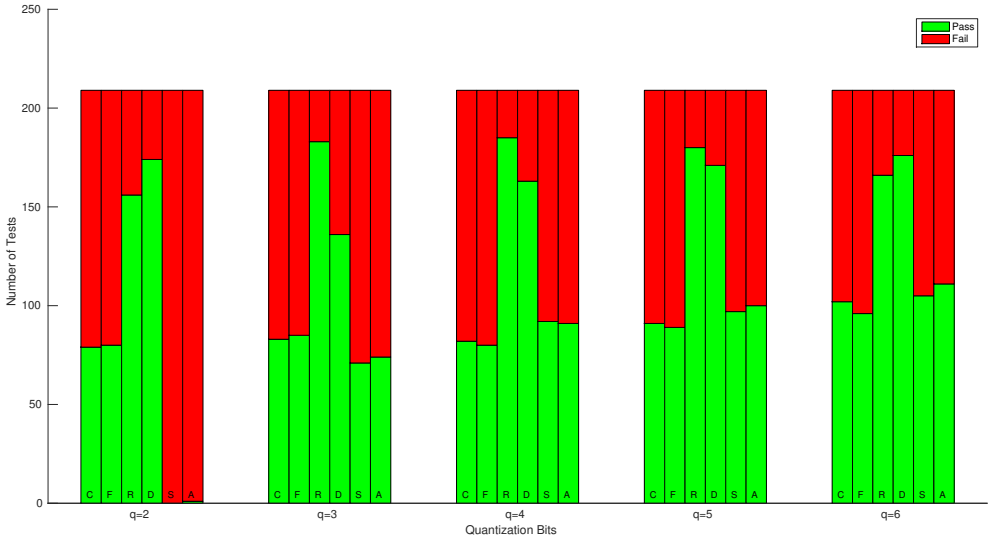


Figure 6.37.: Result of the NIST tests.

6.3.5. Discussion

The conducted experiments for validating our novel key exchange method in real-world indoor and outdoor scenarios allow us to make interesting empirical observations and deduce useful relations between the different protocol parameters and its performance.

Combining this information, we are able to choose the best extractors for indoor and outdoor environments among the described extractor candidates. We described a dependency between the evolution of KAR and the number of quantization bits, Q, as well as between *quality of randomness* associated with the key bitstring and Q.

Finally, we estimate the secret key bit generation rate and identify some shortcomings associated with this technique.

6.3.5.1. Dependency of KAR and Randomness on Q

The plots in Section 6.3.4 indicate that the *quality of randomness* increases with Q. This is given by the increasing value of the min-entropy (see Appendix A.1) and by the number of NIST tests passed (see the bar charts for the latter, e.g. in Section 6.3.5).

KAR vs Q. The key agreement rate decreases with the number of quantization bits Q. An increase of Q leads to closer quantization levels, which means that the noise plays an important role in defining the secret key bits. Therefore, since noise is random and not shared by Alice and Bob, it is responsible for "asymmetries" in the system, which are reflected in the KAR values. The chances that the same point in the quantizer profile (see Figure 6.13) of Alice and Bob are in different intervals increase with Q. Therefore, with only few exceptions, KAR values decrease for the channel A-B. If interpreted as a measure of the system's symmetry, the results confirm our expectations. Likewise, the values of KAR for the E-A and E-B channels, reflecting the multipath properties of the channel, are around 50%.

***Randomness* vs Q.** On the other hand, the bigger the value of Q, the bigger the amount of the quantization levels, as $M = 2^Q$. Thus, the intervals corresponding to a block of Q bits during the quantization process become much thinner, which implies that the quantization process becomes more sensitive to small variations of the signal. These small variations have unpredictable causes, such as noise or other hardware imparities. If the influence of noise is much bigger (equivalently, we can say that the signal-to-noise ratio, SNR, during the quantization is much lower), the randomness coming from noise increases. The probability that blocks of Q bits repeat in consecutive frequencies also diminishes, which explains why the random tests perform better for higher values of Q. More noise means more randomness. As a consequence, the number of passed tests increase. In our analysis, a given test is considered to be passed if and only if the same test is passed for both Alice and Bob's secret key bitstrings.

6.3.5.2. Choice of the Extractor

Since KAR decreases with Q and the randomness (higher *min-entropy* values and number of NIST tests passed) increases with Q, we have to find a compromise

between key agreement and key security. We define the *optimal value of Q for a certain extractor* as being the maximal value of Q such that the following two conditions hold:

- on the one hand, $KAR(A, B)$ values are bigger than a certain threshold. We define this threshold to be 80 %. The lower the values of KAR, the more information is revealed to an eavesdropper about the key during the information reconciliation phase [PJC+13]. On the other hand, $KAR(E, A)$ and $KAR(E, B)$ should be as close as possible to 50 %;
- all the NIST tests should pass at least once.

Next, we determine the value of Q that is best suited for a given extractor in a certain environment, denoted by Q^*. These values can be read found in Figures 6.14 - 6.37 and are given in Table 6.2.

Extractor	Indoor	Outdoor
X	4	2
Z	3	2
XZ	4	3
$(XZ)^2$	4	3
trm	4	2
X/Z	4	2

Table 6.2.: Values for Q^* for each extractor depending on the environment.

In general, the extractor XZ shows the best results for both inside and outside conditions. All results concerning this extractor are shown in detail in the Appendices A.1 and A.2. Stability can be deduced by observing the amount of the outliers in the box plots, i.e., points outside the main box, and the limited span of the data points. This extractor has also shown to be the most *stable*, as we can conclude by visual inspection of the KAR box plots (see the figures in Section 6.3.4.3).

6.3.5.3. Bit Generation Rate

In our implementation of the key exchange protocol using USRP devices, each run takes around $\Delta T \approx 19\,\text{s}$ to be executed. As, in our case, we have $N = 44$ frequency iterations, for a $KAR \approx 80\,\%$, we have, according to Equation (6.7), $BGR = 5.5\,\text{bits/s}$ and $BGR = 7.4\,\text{bits/s}$ for $Q = 3$ and $Q = 4$, respectively.

6.3.5.4. Drawbacks

In this section, we describe a few issues arising from the implementation of our protocol. First, from our experimental results, we acknowledge that no significant improvements in the *bit generation rate* is achieved, since its value is similar to the values obtained in [YMR+09]. However, our setup is implemented in hardware that is not dedicated to this specific application, and therefore requires intensive communication between the transceiver devices and the laptop. We believe that each run would be processed much faster in a dedicated hardware experimental setup. We claim, however, that our method provides a higher degree of security against reconstruction and side-channel attacks than previous fading-based key exchange

techniques. The main reason for this is that we include the hardware asymmetries during the secret key generation process.

Another drawback of our technique lies in the unavoidable *interference* with other WLAN networks. This is however an unavoidable problem for all the wireless systems operating in the same frequency ranges. We observed a more intensive interference especially in a semi-urban environment, due to the several WLAN access points and packet traffic around the Informatics Department building. As a workaround, we propose to use other bands of the spectrum, not occupied by other WLAN signals. We acknowledge that our technique is not jamming-resistant (cf. Section 3.4), unless frequency hopping techniques [TV05] are employed.

Checking the results for SU c (Single Configuration – Figures A.8.1 and A.8.2) and SU d (Single Configuration – Figures A.9.1 and A.9.2), one can see that they still have a big $KAR(E, A)$ value and a *min-entropy* of zero for low values of Q. One can also see that the bar charts indicate several failed tests (red color), which shows low randomness. This clearly means that when there is no line-of-sight, a large number of long series of 1s or 0s might appear due to the massive obstructing obstacle, since the direct path component is predominant (as in [MTM+08]).

We have observed that a few runs show a low level of reciprocity for urban environments, which can be confirmed by the values for $KAR(A, B)$. This is due to *synchronization issues*. We realized that the traffic of cars often interrupted the TCP packet delivery responsible for the synchronization (see Figure 6.5). Therefore, due to several retries, the synchronization time is much bigger than the coherence time of the channel. Thus, there is a big time gap between the moments when the channel is sounded by both parties. Since this environment is very dynamic and, therefore, the coherence time short, both parties will receive different channel responses.

We also discovered an issue concerning the reference extractor Z. In the box plot (in Figure 6.3.4.2), we can see that the green boxes and the yellow and red boxes partially superpose in the KAR-axis. This means that the values of $KAR(E, A)$ and $KAR(E, B)$ are too large for indoor, which makes it unsuitable for practical applications. A reason for this might be similar frequency oscillations. This extractor only serves as a reference, as the influence of fading is not taken into consideration for the features extraction.

6.3.5.5. Other Observations

The results obtained for the cases of different heights do not show significant differences, as one can see by comparing the results for *Outdoor: Urban a* and *Outdoor: Urban b experiments* presented in the Appendix. We confirmed that the most important factor influencing the reciprocity is the dynamic behavior of the environment.

6.3.5.6. Strategy for a Practical Implementation

First, both parties start, as usually, by sounding the channel and extracting its main characteristics as explained in Section 5.3.1. Since the environment conditions are unpredictable at the moment of the protocol execution and given our experimental results shown before, we suggest to use the extractor XZ and $Q = 4$ and $Q = 3$ for indoor and outdoor, respectively (or simply $Q = 3$ for both environments (see Table 6.2)). Afterwards, each party applies the NIST tests to the originated bitstring and informs his counterpart of the result (*failed*, if at least one of the tests failed; or *passed*, otherwise). If at least one party has *failed*, both parties should restart the

protocol and repeat the sounding channel process expecting that, meanwhile, the channel has changed sufficiently to contain enough randomness (entropy). If both parties *passed*, they proceed to the information reconciliation step (cf. Section 2.3). Subsequently, if they determine that the condition "$KAR >$ threshold $= 80\%$" is satisfied, they set their common secret key as the bitstring generated after the reconciliation procedure. If this condition is not satisfied, meaning that Eve received too much information during the execution of the information reconciliation protocol, the key exchange protocol should be restarted.

6.4. Conclusion

In this chapter, we experimentally demonstrate the surge of a baseband signal as a result of differences in the hardware of the sender and emitter. In order to enhance the total security of fading-based key exchange, we combine these hardware effects with channel fading effects. We proposed a new *fading-&-hardware*-based key exchange protocol and experimentally validated this novel technique. We conducted a series of experiments in order to find an optimal way of combining the information from the environment with hardware-dependent signals. We presented several methods for performing this combination and we make extensive studies to confirm its feasibility under real-world conditions. For that purpose, we identify some quality criteria and check if our method meets them under different constraints.

This chapter confirms that there are several factors that can influence the quality of the generated key. The type of the surrounding environment and the number of quantization bits, Q, play an important role. We showed that this parameter determines the quality of the key and therefore must be chosen carefully: a larger value of Q makes this technique more sensitive to small variations in the channel or to hardware noise. The trade-off between a high KAR and randomness must be taken into account in the choice of Q.

Our experimental results evidence that our new technique seems to be a promising method for secret key generation, especially when executed in an indoor environment. Due to the nature of the wireless medium, its performance still needs improvement when applied in outdoor environments.

We estimate that combining a previously known secret using conventional cryptographic methods with our technique can improve the overall security of the system. That would be the case, e.g., when the known secret would be used to encode a different sequence of central frequencies for sounding the channel, using a method similar to frequency-hopping. Since an adversary would not know the frequency of the current signal sounding the channel, he would have to sound the channel in a very wide band of the spectrum, increasing the interferences and the noise associated with the measurements. Besides, if only equipped with a narrowband receiver, it could be unfeasible for an attacker to measure the signal received by Alice or Bob, even if located near their nodes.

7. Conclusion

We conclude our work by listing some open problems and suggesting new topics for further research. The usage of the physical properties of the wireless channels for the key agreement problem has become a fast-growing research topic in the wireless security community. This method provides several advantages over traditional key-exchange techniques in terms of time and energy consumption. Few implementations aiming to extract a secret key from shared randomness contained in the wireless channel have been proposed and thoroughly explored in the literature.

Being dependent on the variable *surrounding environment*, these methods still lacked precise security guarantees. Therefore, a security evaluation based on the complexity of the environment had yet to be done. In Chapter 4, we presented some shortcomings of the fading-based key exchange protocols and, by doing so, highlighted the importance of a security evaluation. We modeled a simple channel and showed how a passive eavesdropper is able to reconstruct the information that both legitimate parties extract from the environment by using merely the signals received from both parties. This raises the question whether it is possible to conduct a formal evaluation of the complexity of this attack depending on the constitution of the environment.

Furthermore, the study of side-channel attacks is a very lively topic in cryptographic research. Such attacks can partially or totally reveal the secret key by analyzing *uncommon* sources of information of any cryptographic system, such as electric current consumption, time or even the frequencies pattern of the sound waves emanated by a processor. We introduced a new attack based on the reradiation effect that every antenna displays and determined the precise conditions and physical boundaries under which this attack can be mounted. The question of whether there are other side-channels that can be explored against this protocol is an open topic.

As a countermeasure against these attacks, we introduced in Chapter 5 a new method for increasing the security of fading-based key exchange techniques by leveraging the inherent and single properties of the hardware components, namely the local oscillators, during the channel sounding process. Specifically, we harvested another source of randomness by also considering the *symmetrical* differences in the oscillation frequencies of the sender's and receiver's local oscillators. We combined this information with the environment entropy in order to enhance the total security of the key exchange system. The security of this measure depends not only

on the environment complexity, but also on the precision of the receiver oscillators. An attacker would need extreme precise oscillators in order to reconstruct the legitimate signal accurately. In Section 3.5, several hardware imparities have been described. The usage of some kind of other imparities than frequency oscillations for the purpose of key exchange is a topic for further research.

We experimentally validated our method under real-world constraints, both in indoor and outdoor environments. In Chapter 6, we showed that our method seems to be a promising technique for key extraction. However, we were able to identify some drawbacks of our method under outdoor conditions. The interferences of waves coming from other WLAN sources operating in the same frequency bands and some synchronization issues contribute to the degeneration of the quality of the results. As future work, we suggest conducting experiments in other spectral bands in order to check how much the results are improved and if these shortcomings have been overcome. Indoor results were more satisfactory, though. For our experimental setup described in Chapter 6, we used similar transceivers. The question of how our method performs if the parties have different hardware is also a very interesting subject to explore. Specifically, testing the performance of our method when implemented in dedicated hardware would also be an interesting topic for further analysis. In particular, it would be interesting to study how much the oscillation frequencies vary in different hardware, and if we would achieve a better key agreement rate. We identified a drawback concerning the extracted secret bit rate in our experiments. Still, we achieved values comparable to some of the systems proposed by other authors. We presented different methods for combining device-generated randomness with the randomness provided by the multipath channel. The question of finding better combination strategies remains open.

We point out that one has to integrate a solution for guaranteeing the authenticity of the parties before the key exchange takes place. This can be based on radiometric signatures as shown by other authors and described in Section 3.5. Combining such authentication methods with our key exchange technique would allow a complete wireless solution for key management.

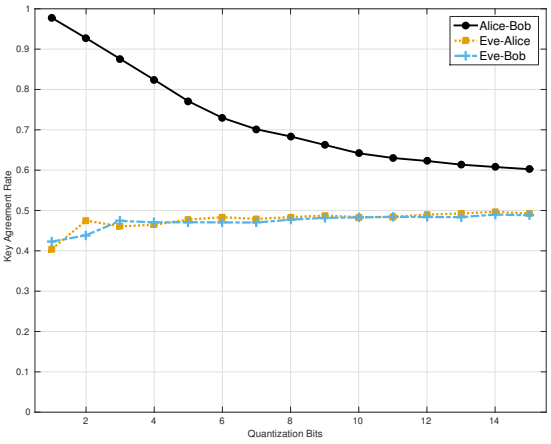
The possibility of combining lightweight information-theoretical key exchange methods (like the one we proposed) with traditional methods (like the Diffie-Hellman key exchange protocol) for achieving a significant security advantage is a challenging problem still left open for future research.

A. Appendix

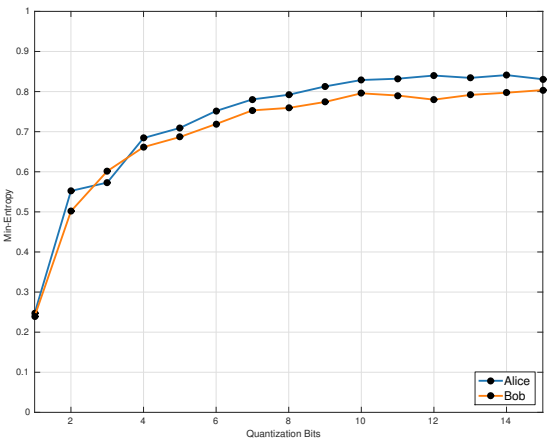
A.1. Extractor XZ: Single Configuration

Only the results for Configuration I (5 runs) are shown - see Table 6.1.

Indoor: Position Z = a



A.1.1: Key Agreement Rate vs Quantization Bits.



A.1.2: Min-Entropy vs Quantization Bits.

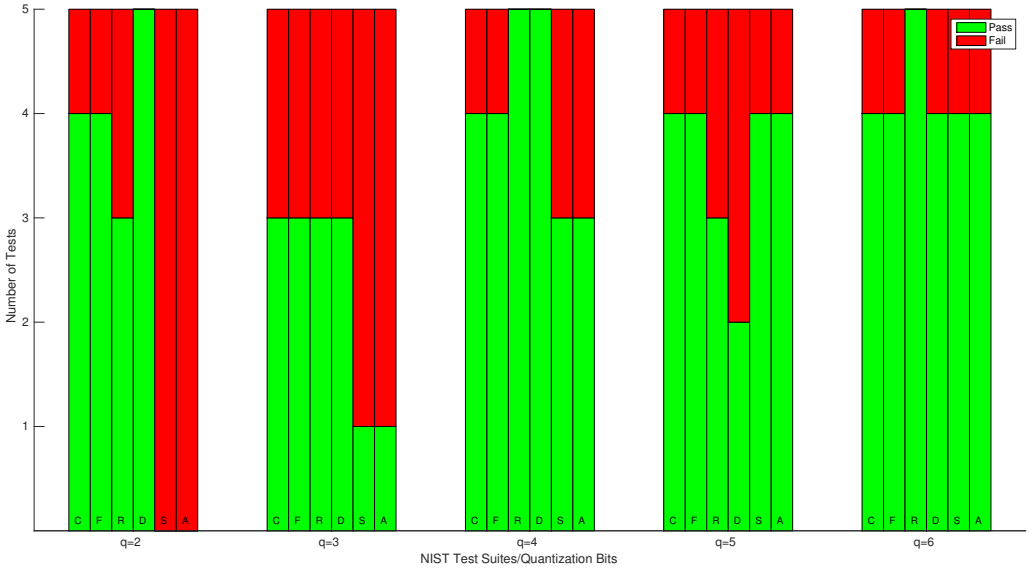
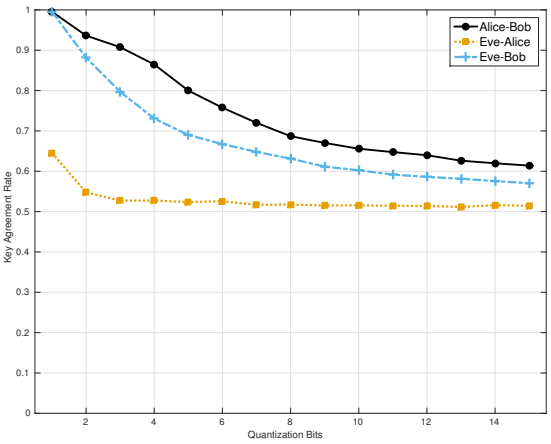
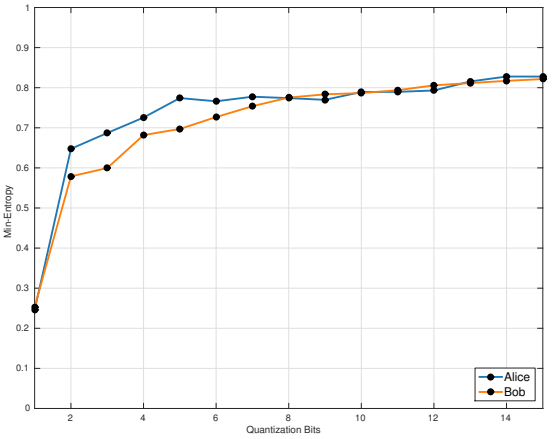


Figure A.1.: Result of the NIST tests.

Indoor: Position Z = d



A.2.1: KAR vs Q.



A.2.2: Min-Entropy vs Q.

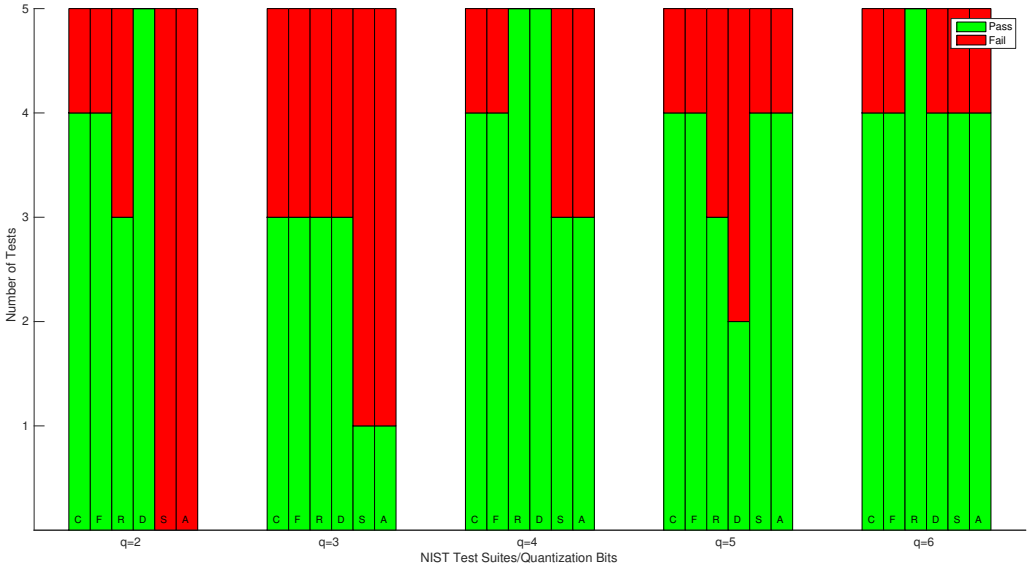
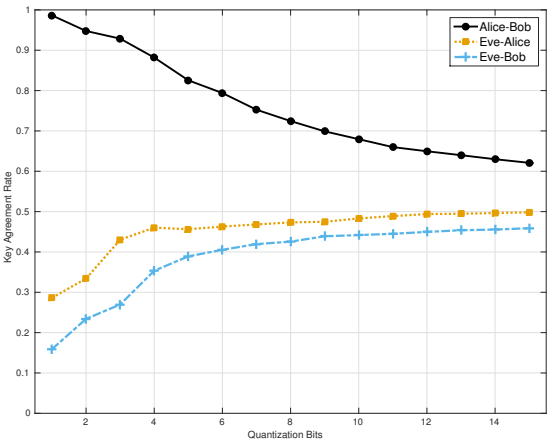
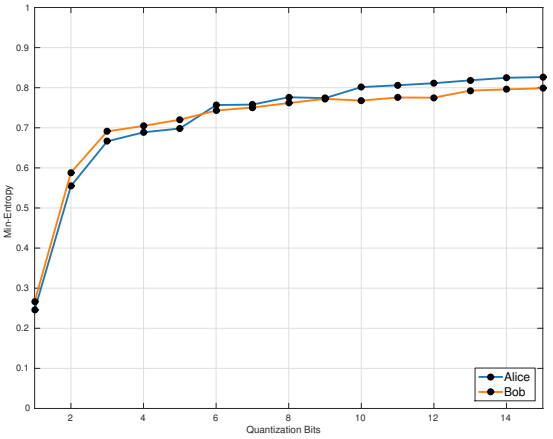


Figure A.2.: Result of the NIST tests.

Indoor: Position Z = g



A.3.1: KAR vs Q.



A.3.2: Min-Entropy vs Q.

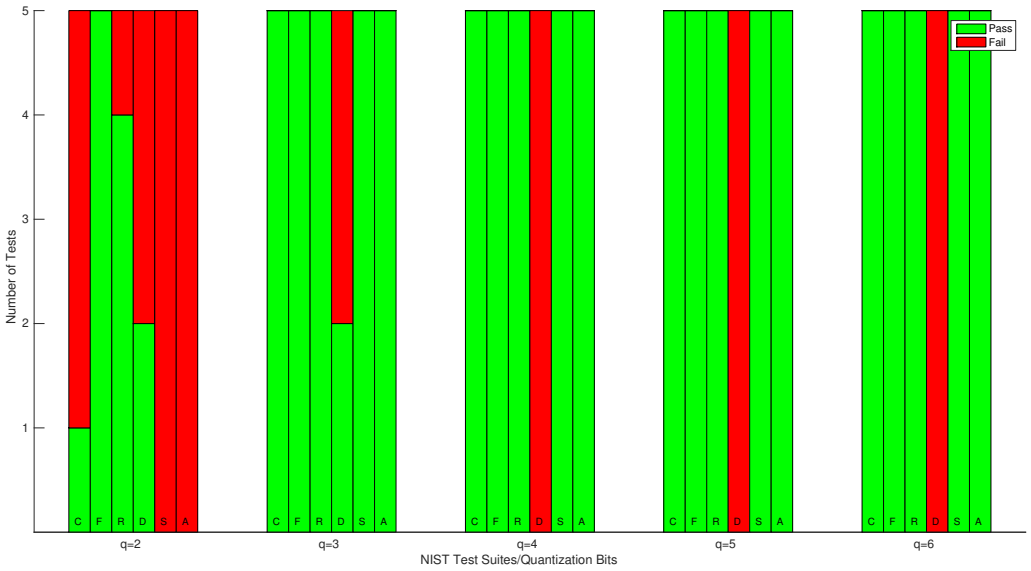
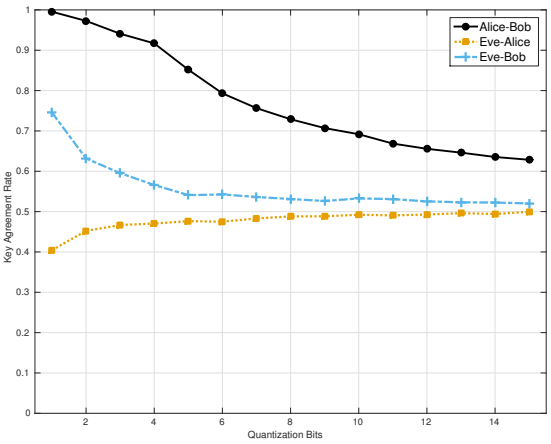
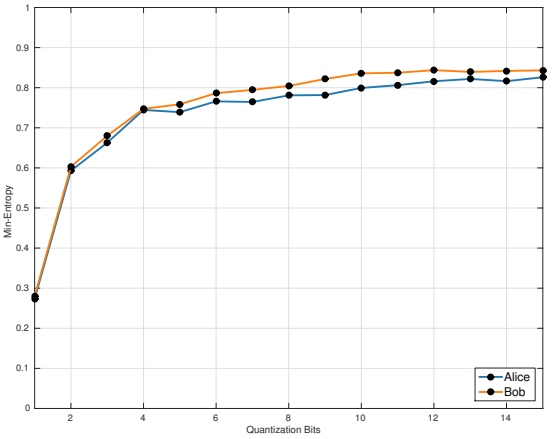


Figure A.3.: Result of the NIST tests.

Indoor: Position Z = k



A.4.1: KAR vs Q.



A.4.2: Min-Entropy vs Q.

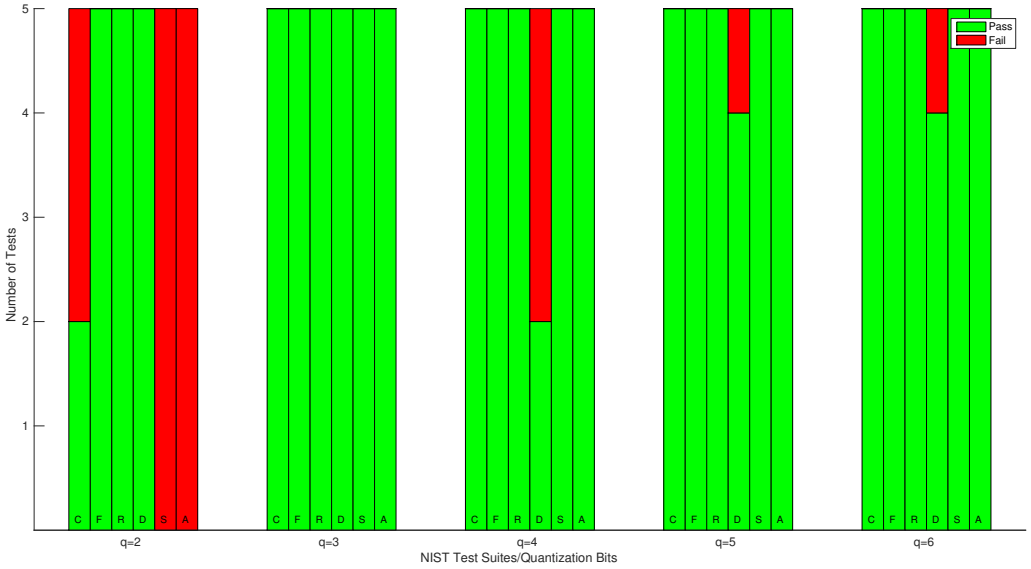
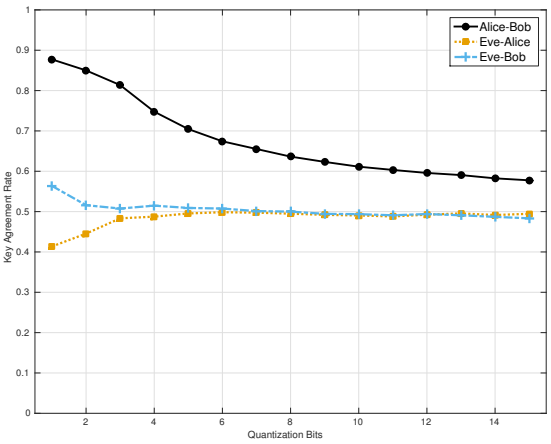
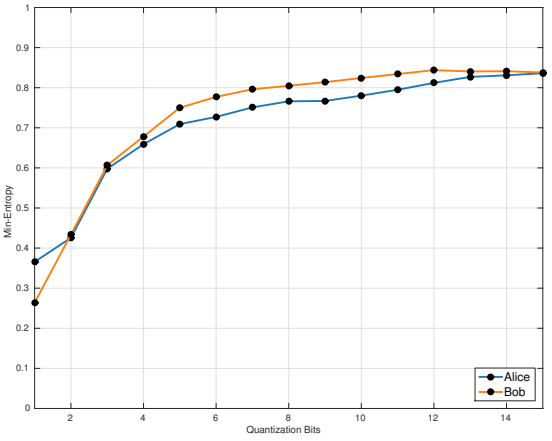


Figure A.4.: Result of the NIST tests.

Outdoor: Rural



A.5.1: KAR vs Q.



A.5.2: Min-Entropy vs Q.

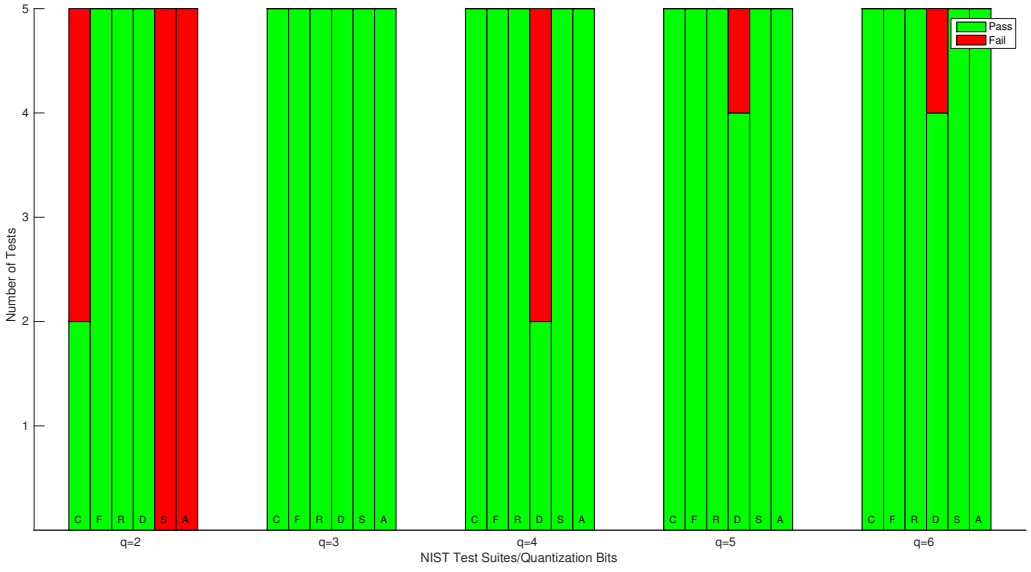
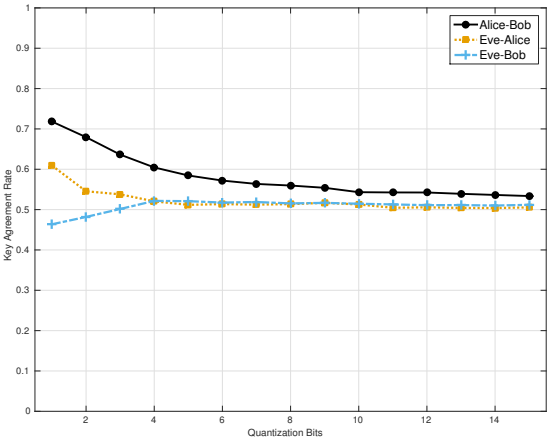
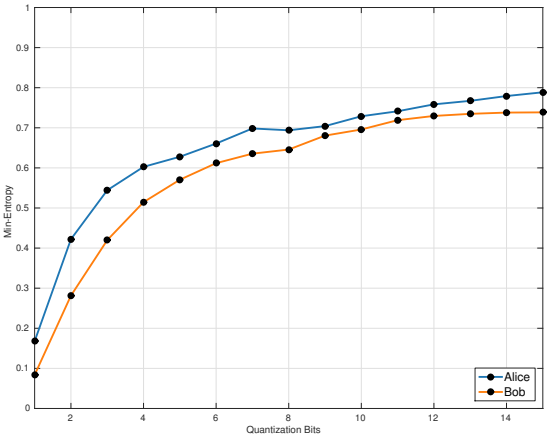


Figure A.5.: Result of the NIST tests.

Outdoor: Semi Urban a



A.6.1: KAR vs Q.



A.6.2: Min-Entropy vs Q.

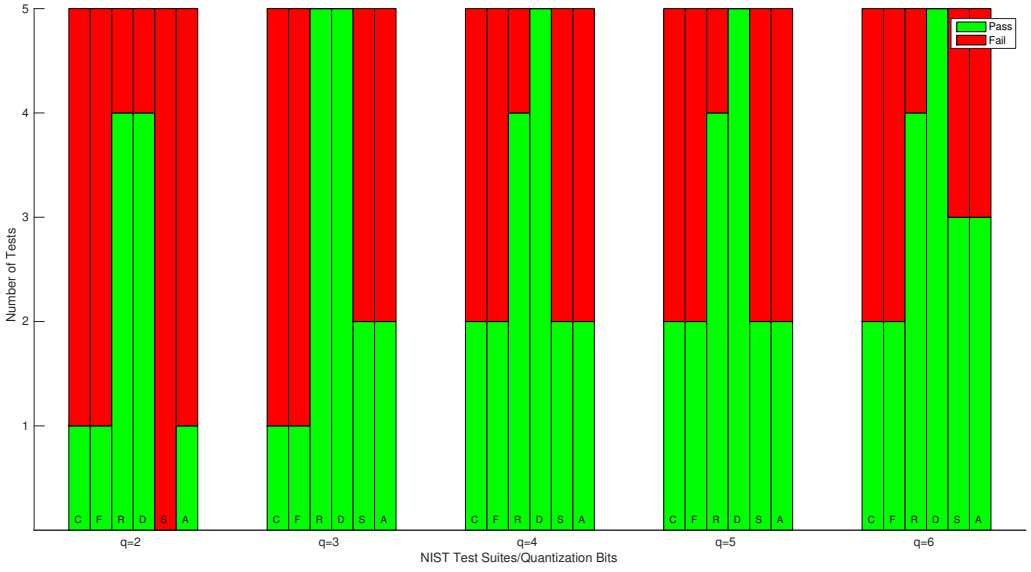
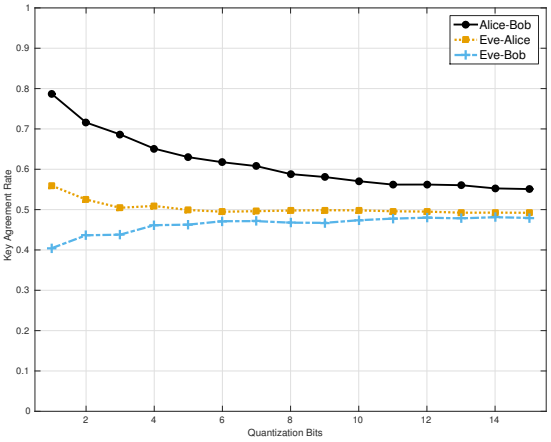
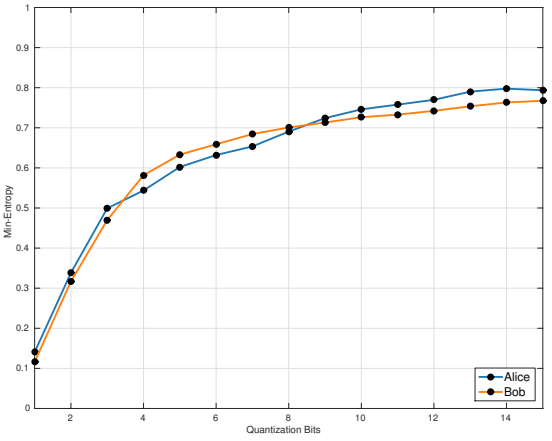


Figure A.6.: Result of the NIST tests.

Outdoor: Semi Urban b



A.7.1: KAR vs Q.



A.7.2: Min-Entropy vs Q.

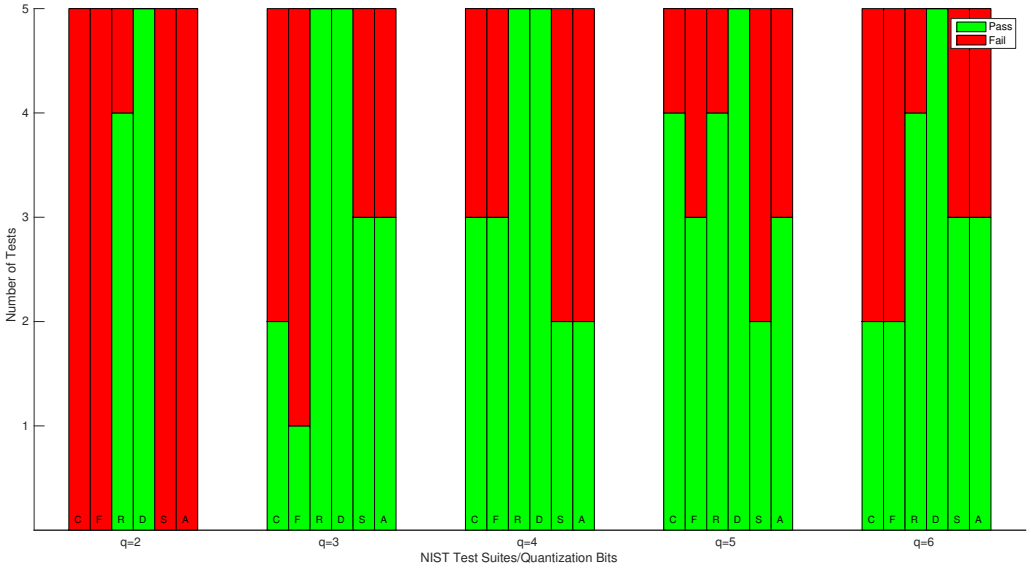
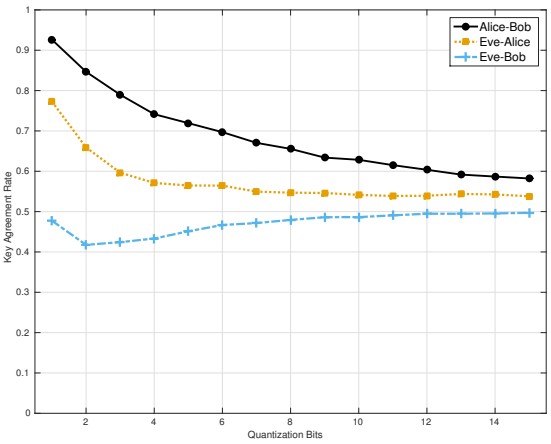
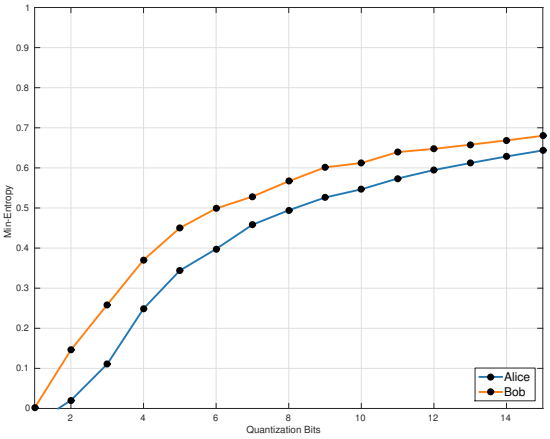


Figure A.7.: Result of the NIST tests.

Outdoor: Semi Urban c



A.8.1: KAR vs Q.



A.8.2: Min-Entropy vs Q.

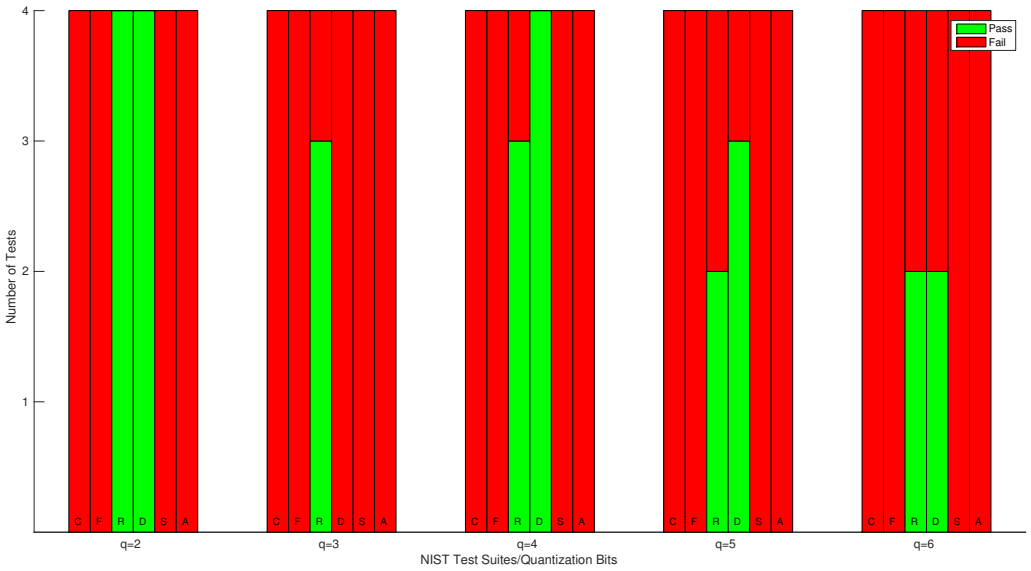
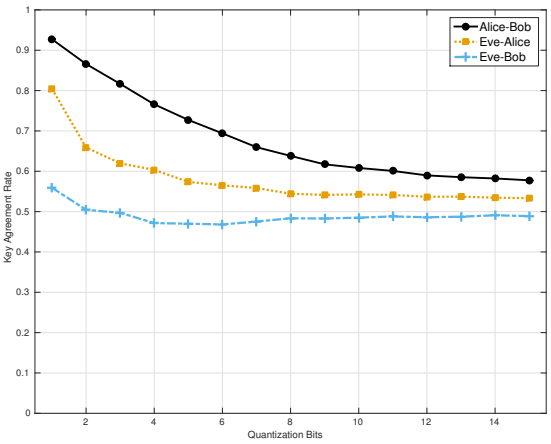
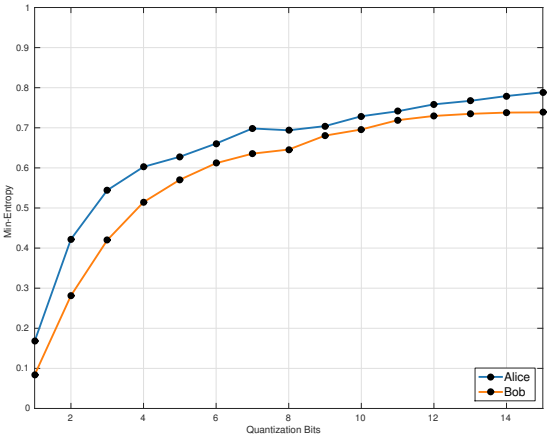


Figure A.8.: Result of the NIST tests.

Outdoor: Semi Urban d



A.9.1: KAR vs Q.



A.9.2: Min-Entropy vs Q.

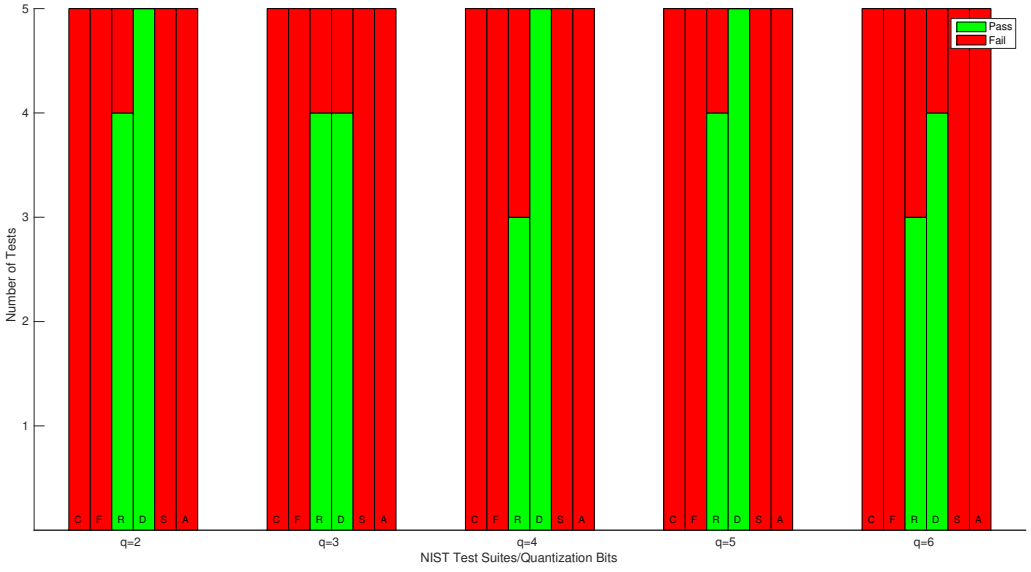
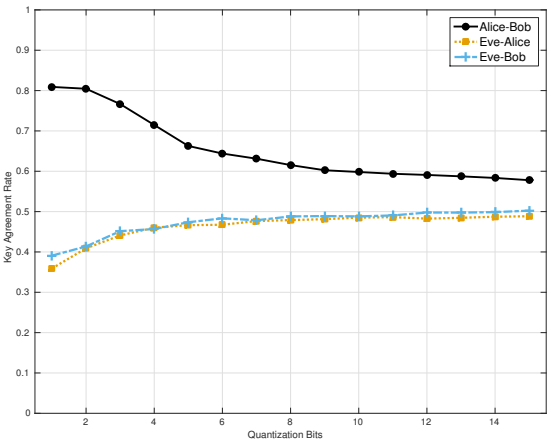
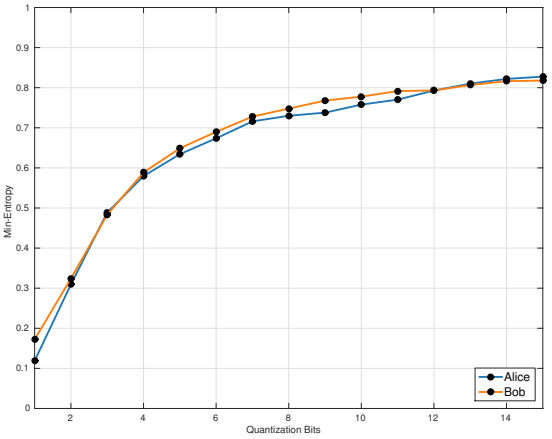


Figure A.9.: Result of the NIST tests.

Outdoor: Urban a



A.10.1: KAR vs Q.



A.10.2: Min-Entropy vs Q.

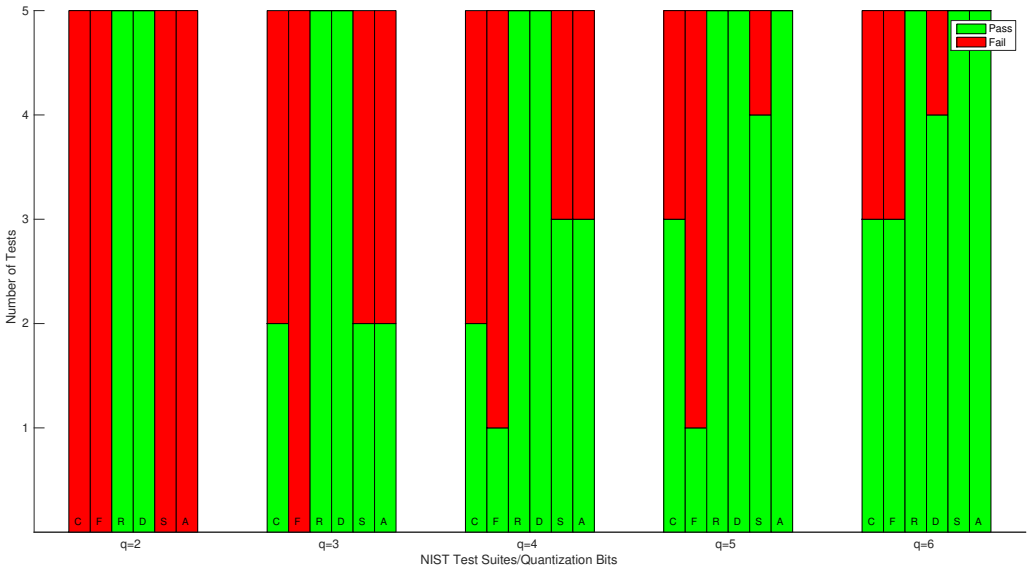
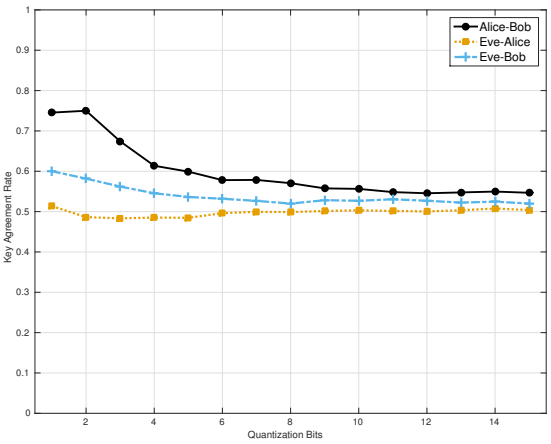
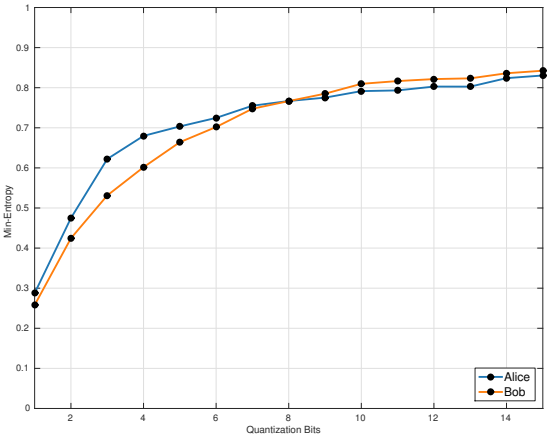


Figure A.10.: Result of the NIST tests.

Outdoor: Urban b



A.11.1: KAR vs Q.



A.11.2: Min-Entropy vs Q.

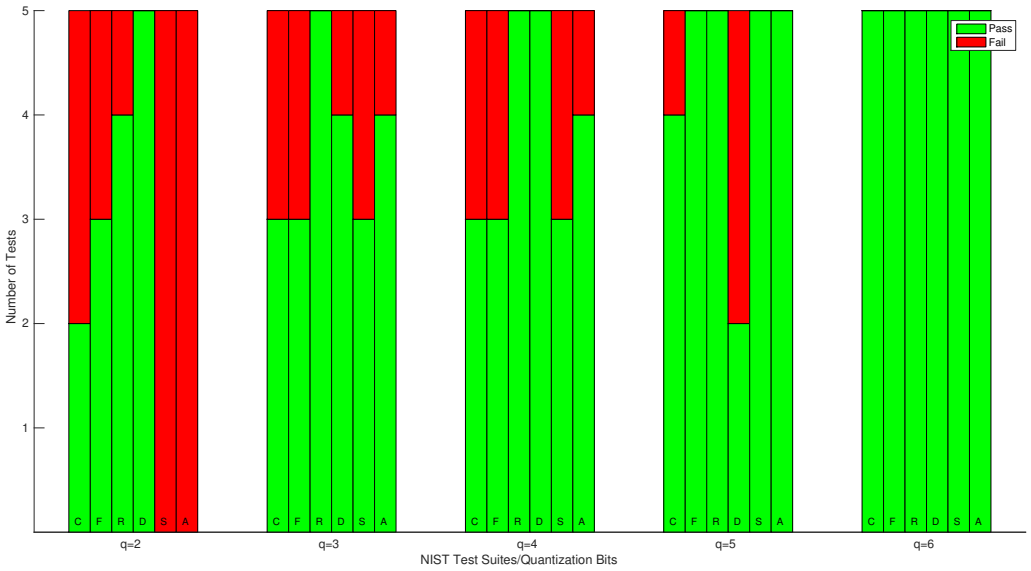


Figure A.11.: Result of the NIST tests.

A.2. Extractor XZ: All Configurations

These plots correspond to Configurations I-VI, a total of 30 runs (= 6 configurations × 5 runs/configuration, see Table 6.1).

Indoor: Position Z = a

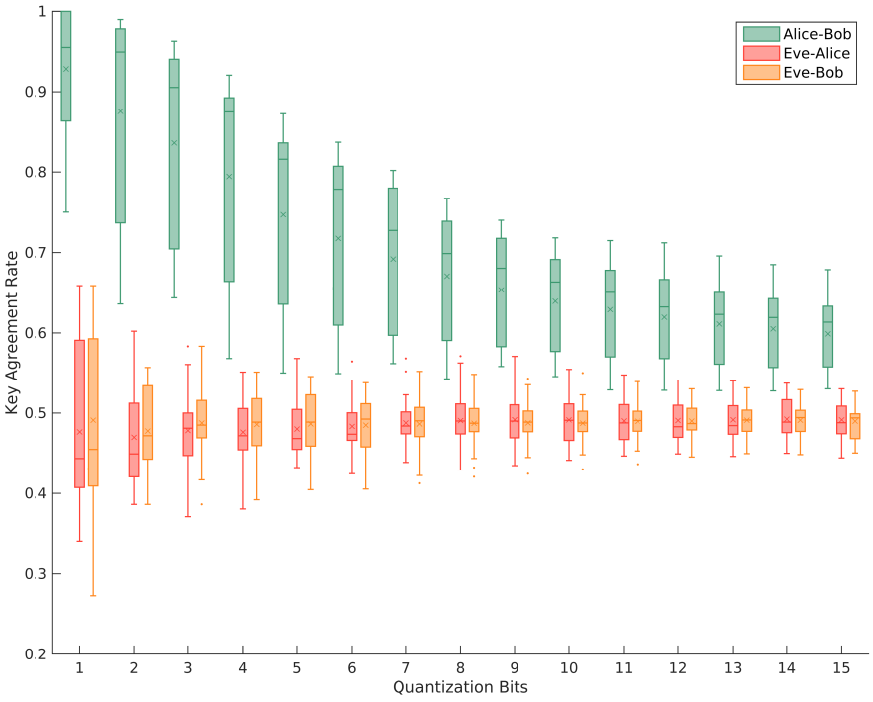


Figure A.12.: Key Agreement Rate vs Quantization Bits.

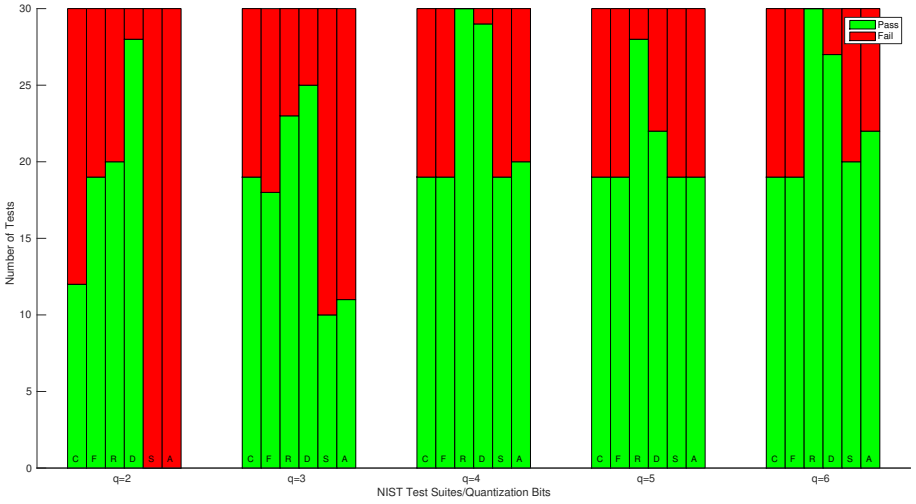


Figure A.13.: Result of the NIST tests.

Indoor: Position Z = d

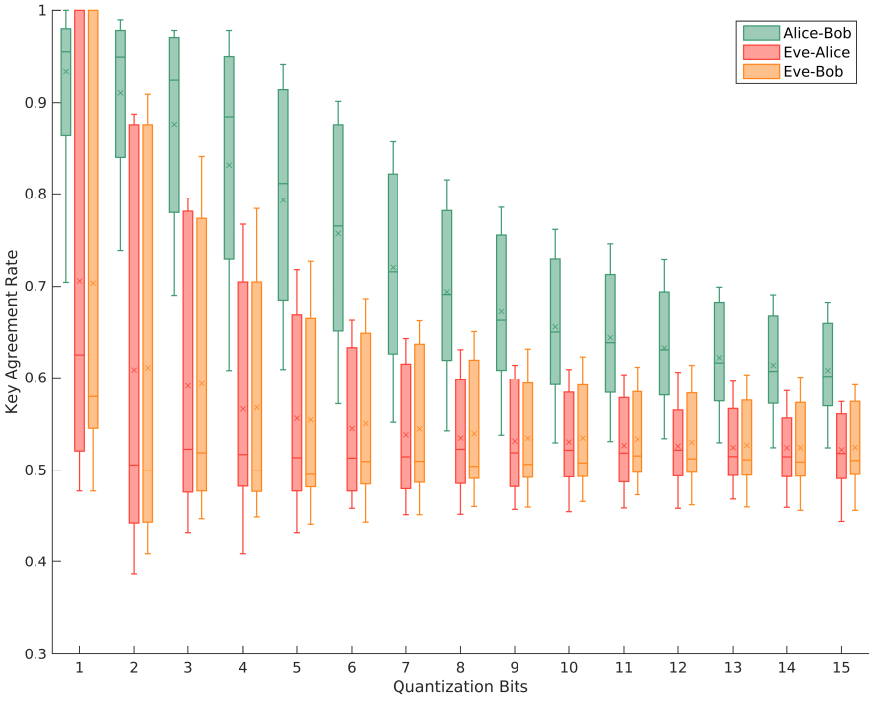


Figure A.14.: Key Agreement Rate vs Quantization Bits.

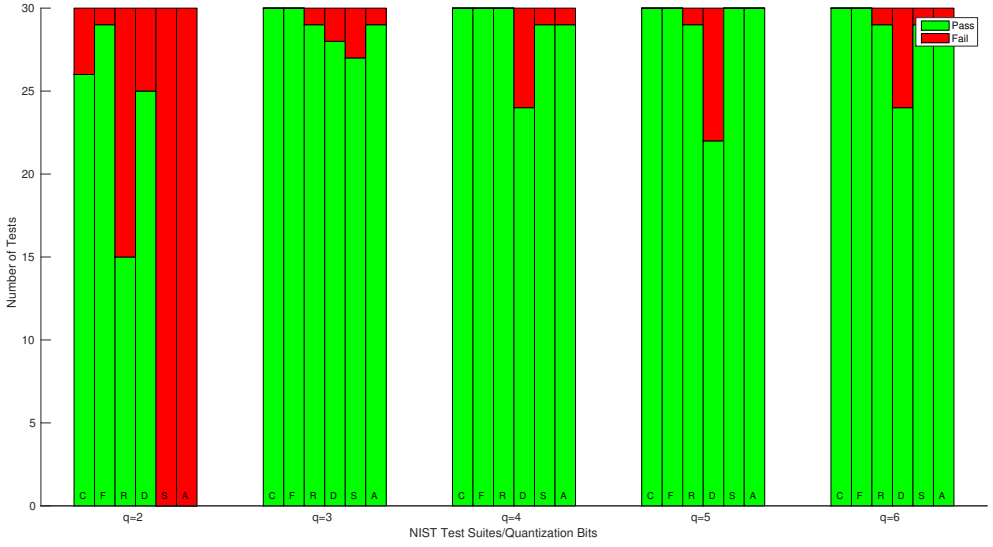


Figure A.15.: Result of the NIST tests.

Indoor: Position Z = g

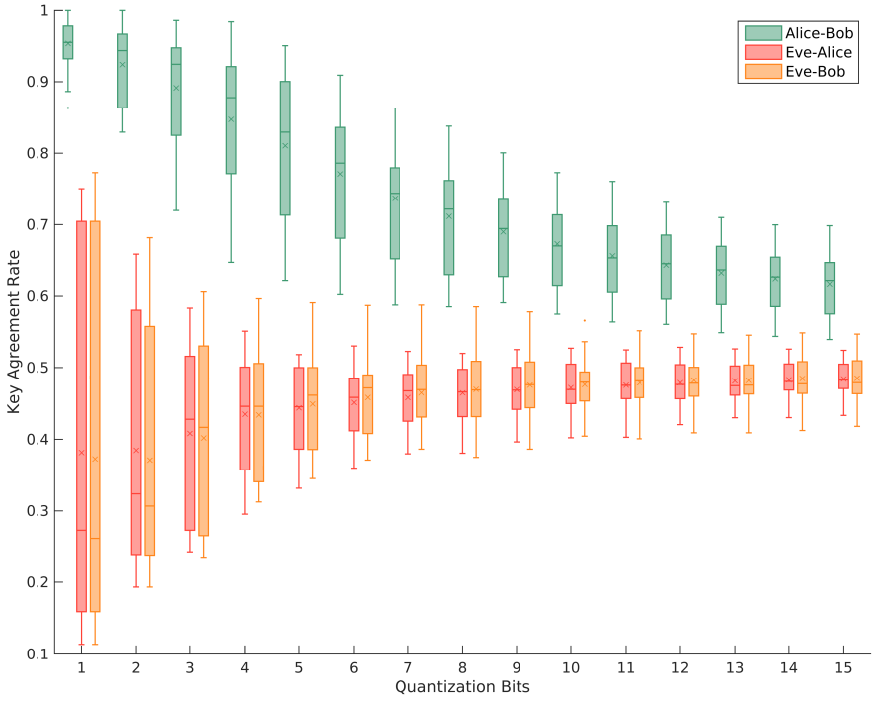


Figure A.16.: Key Agreement Rate vs Quantization Bits.

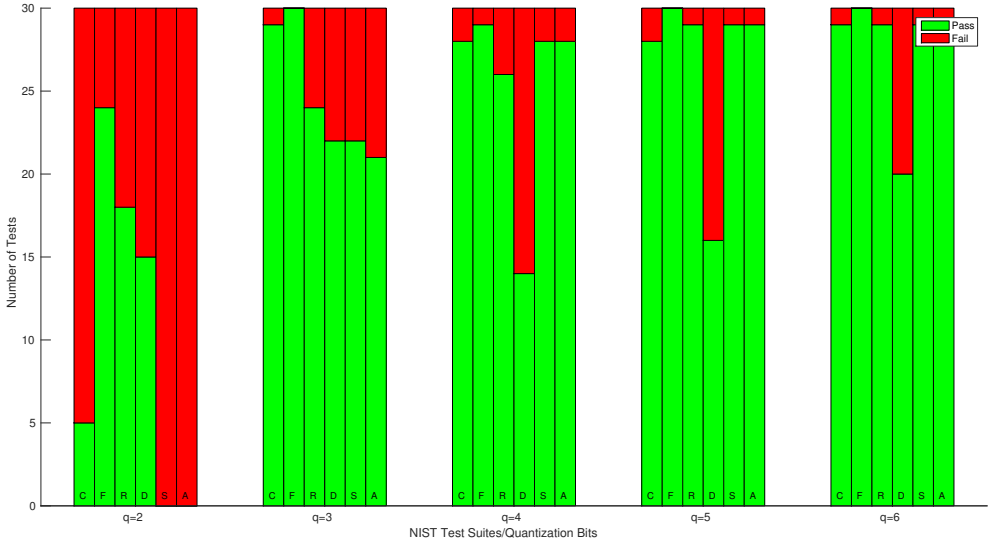


Figure A.17.: Result of the NIST tests.

Indoor: Position Z = k

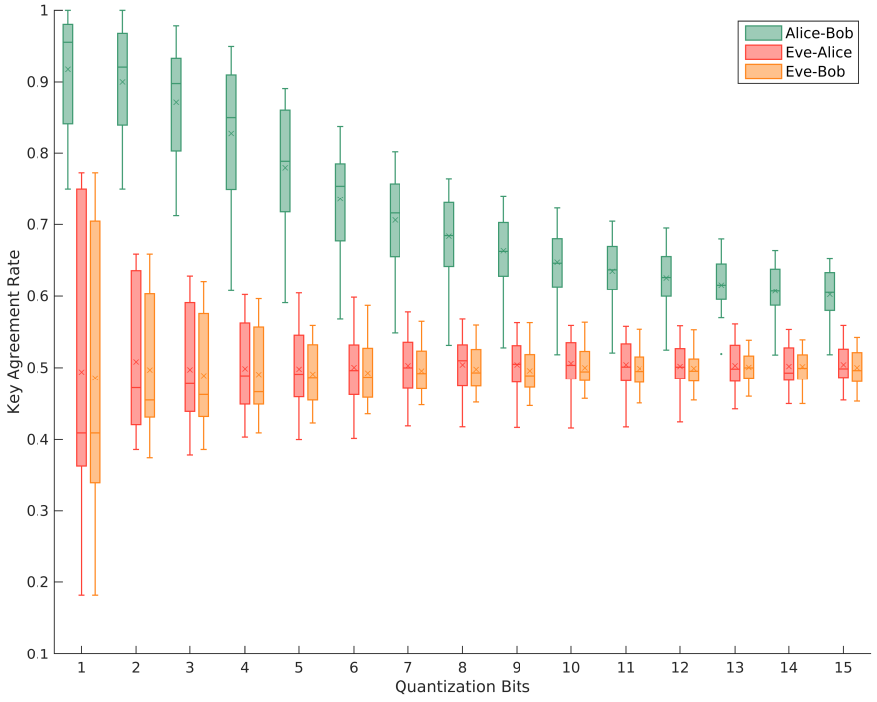


Figure A.18.: Key Agreement Rate vs Quantization Bits.

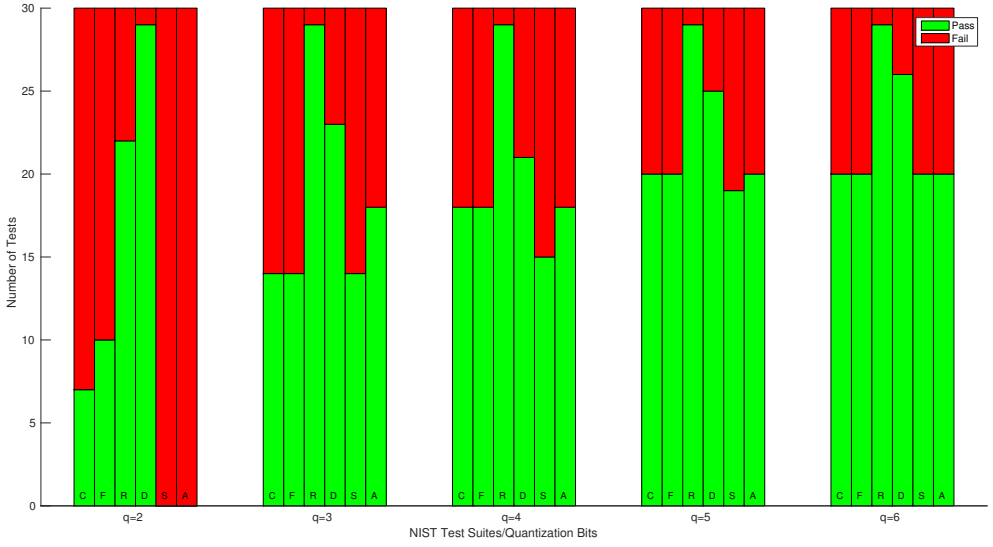


Figure A.19.: Result of the NIST tests.

Outdoor: Rural

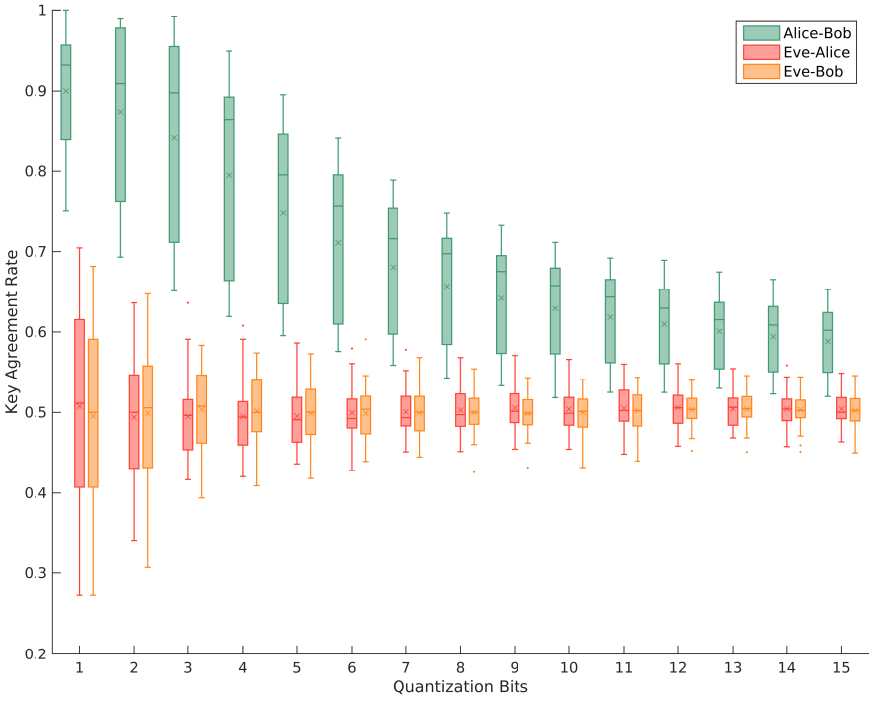


Figure A.20.: Key Agreement Rate vs Quantization Bits.

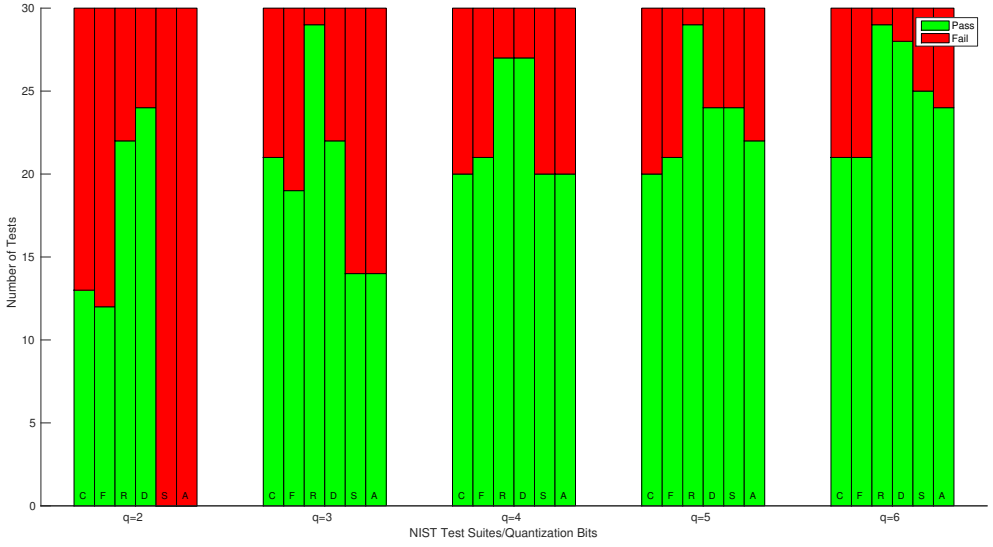


Figure A.21.: Result of the NIST tests.

Outdoor: Semi Urban a

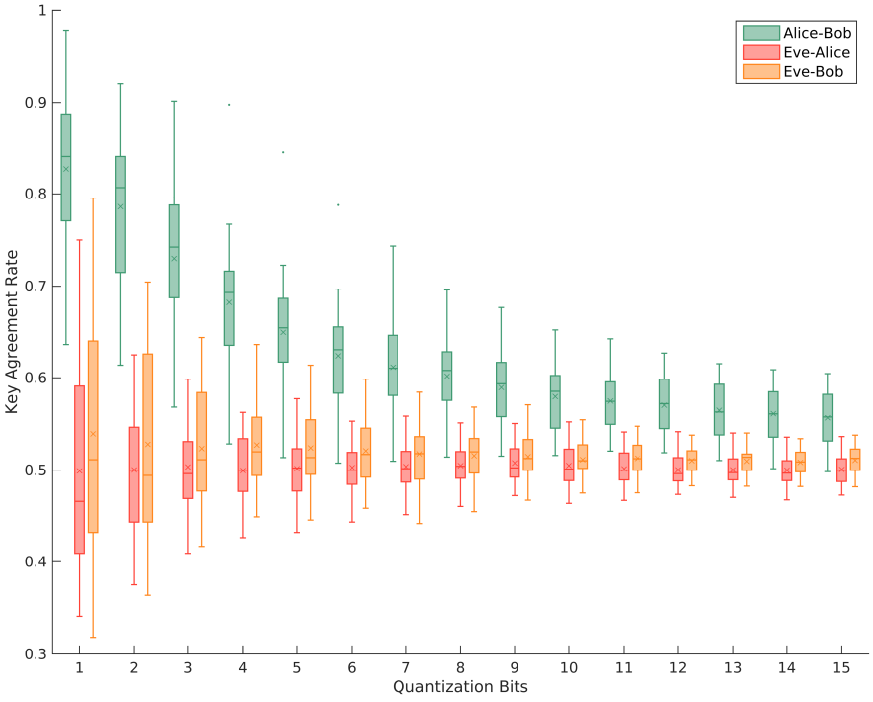


Figure A.22.: Key Agreement Rate vs Quantization Bits.

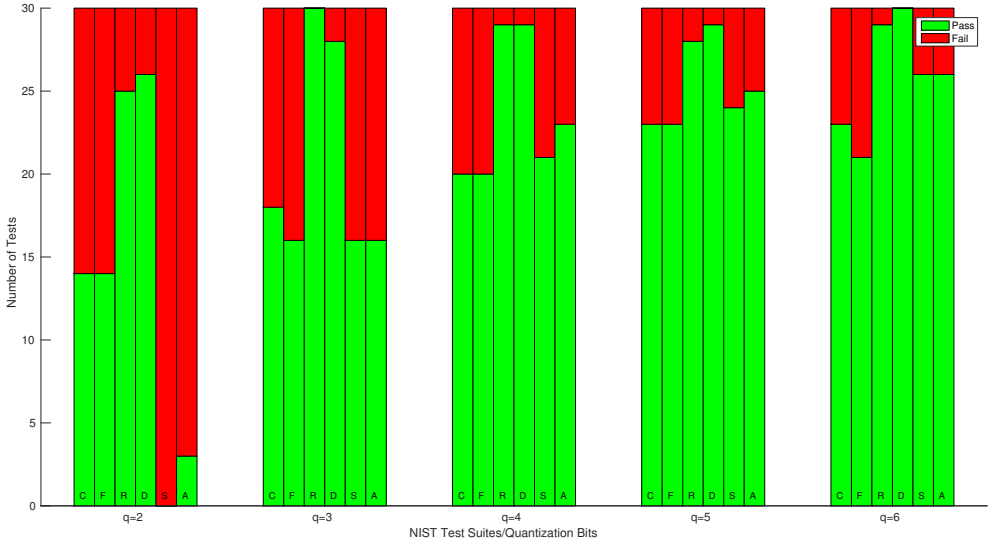


Figure A.23.: Result of the NIST tests.

Outdoor: Semi Urban b

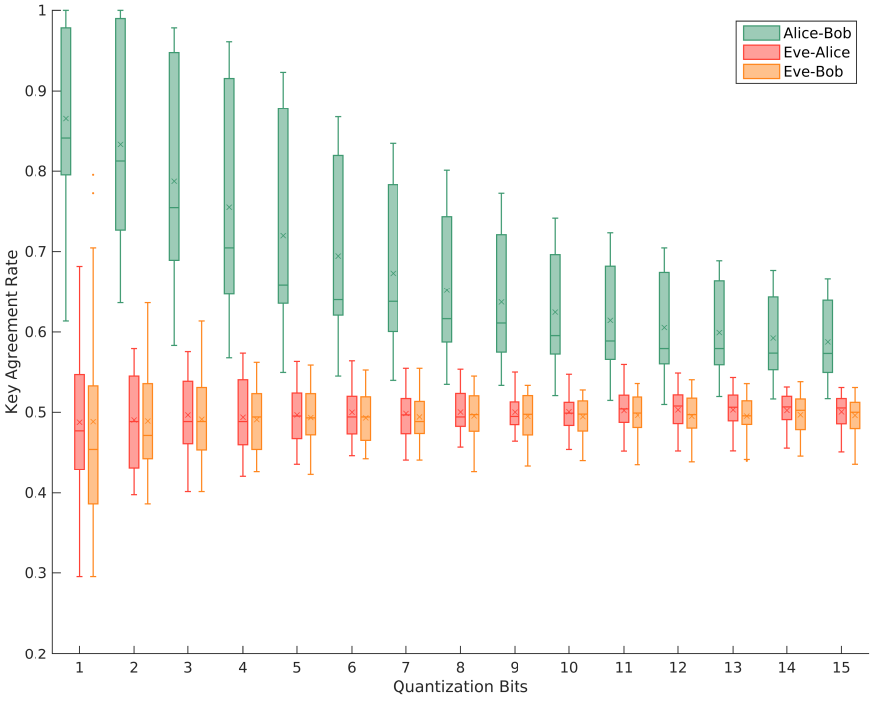


Figure A.24.: Key Agreement Rate vs Quantization Bits.

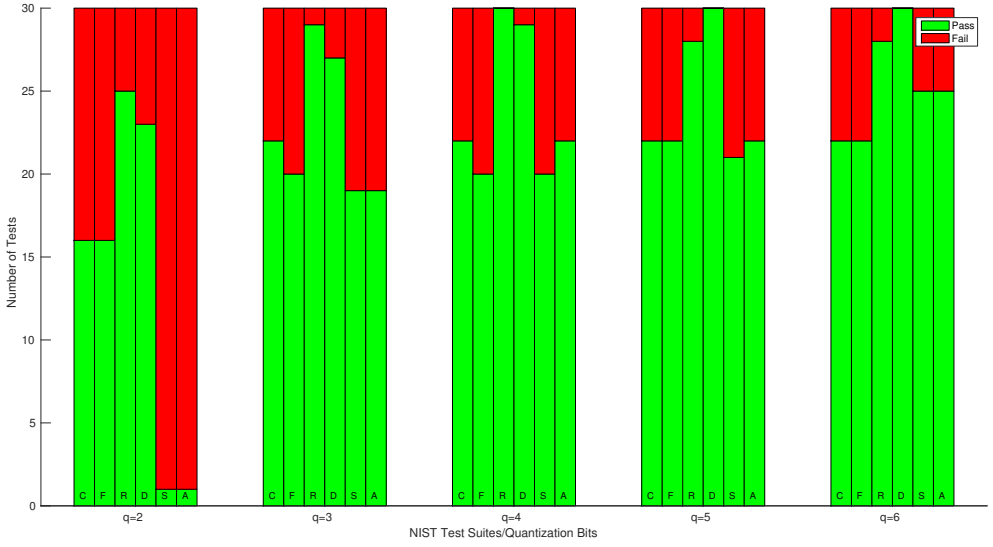


Figure A.25.: Result of the NIST tests.

Outdoor: Semi Urban c

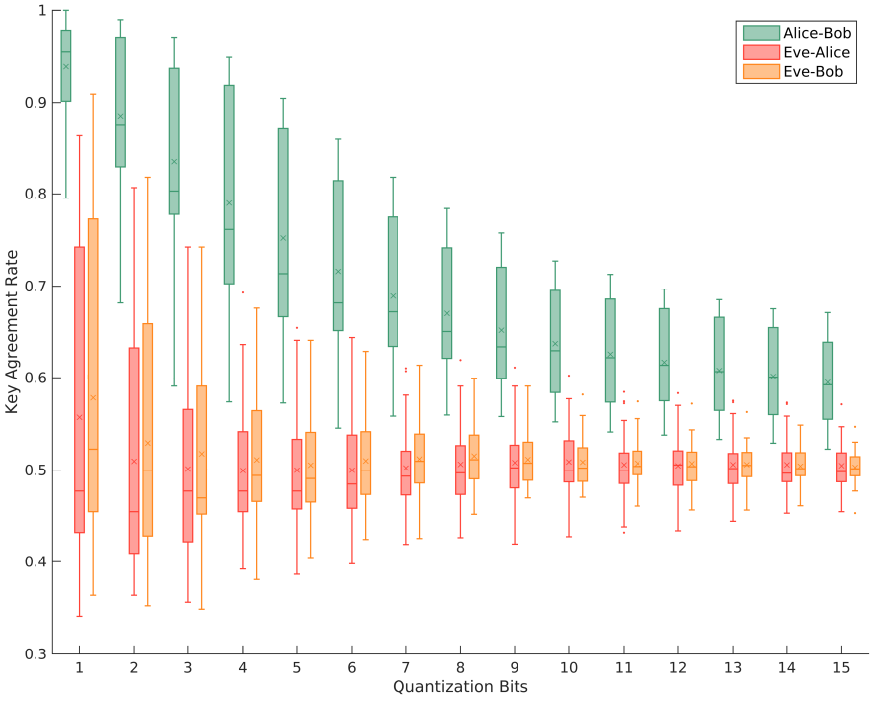


Figure A.26.: Key Agreement Rate vs Quantization Bits.

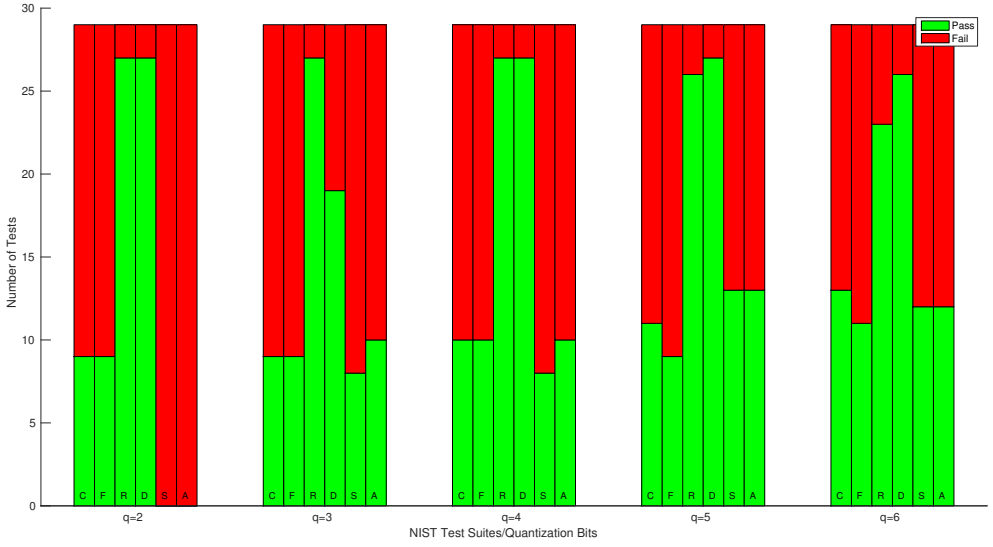


Figure A.27.: Result of the NIST tests.

Outdoor: Semi Urban d

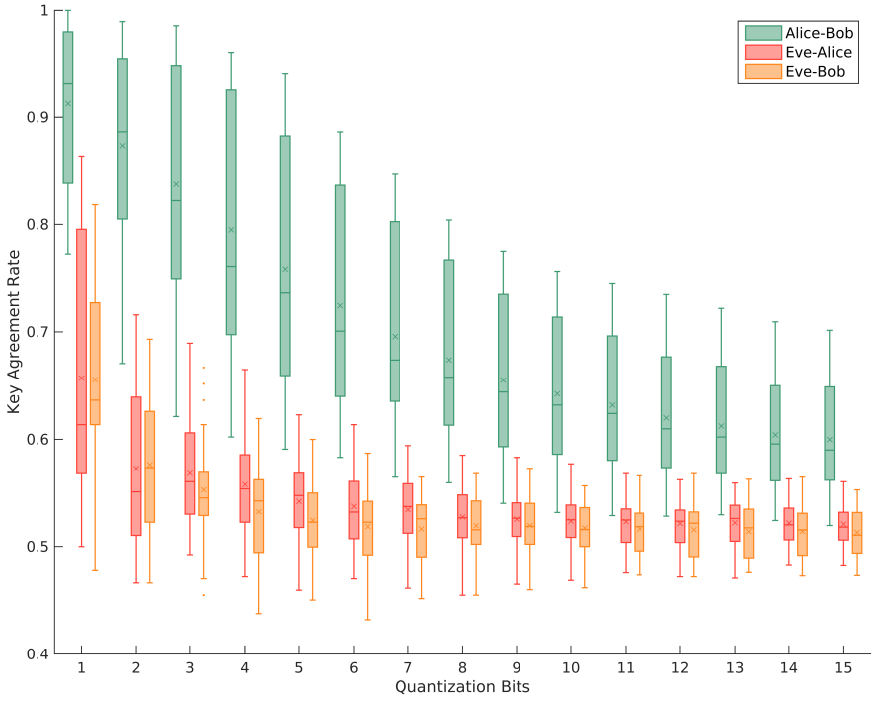


Figure A.28.: Key Agreement Rate vs Quantization Bits.

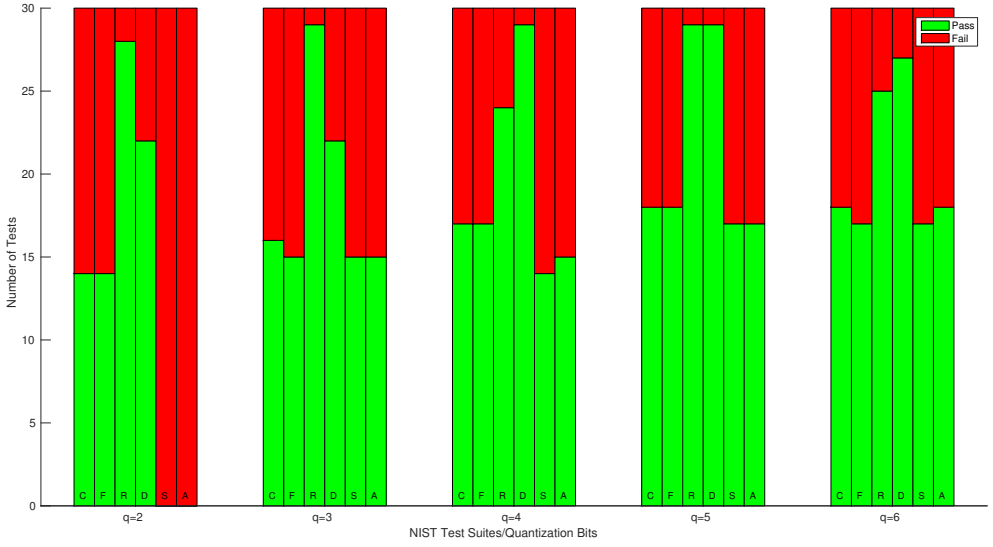


Figure A.29.: Result of the NIST tests.

Outdoor: Urban a

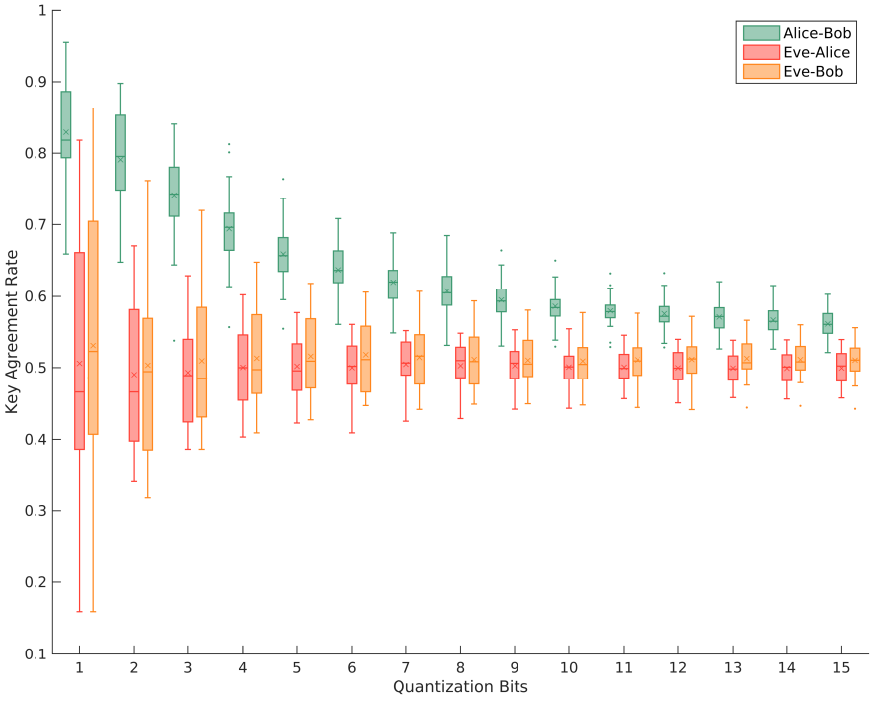


Figure A.30.: Key Agreement Rate vs Quantization Bits.

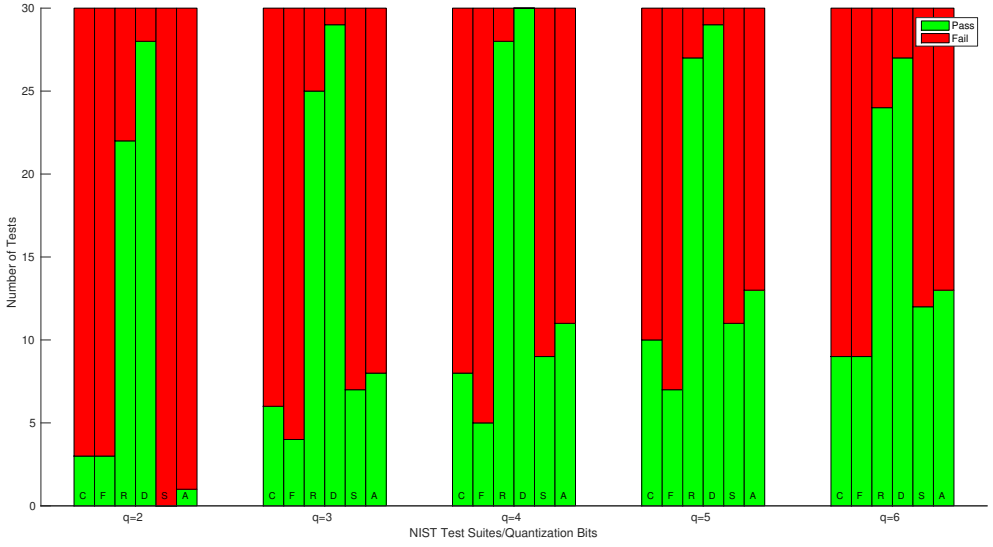


Figure A.31.: Result of the NIST tests.

Outdoor: Urban b

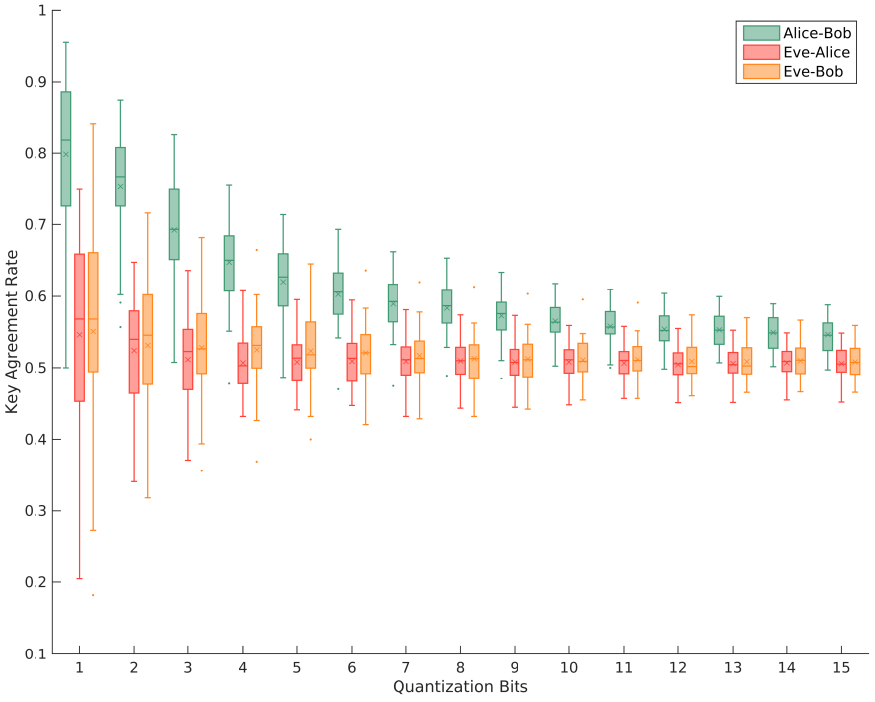


Figure A.32.: Key Agreement Rate vs Quantization Bits.

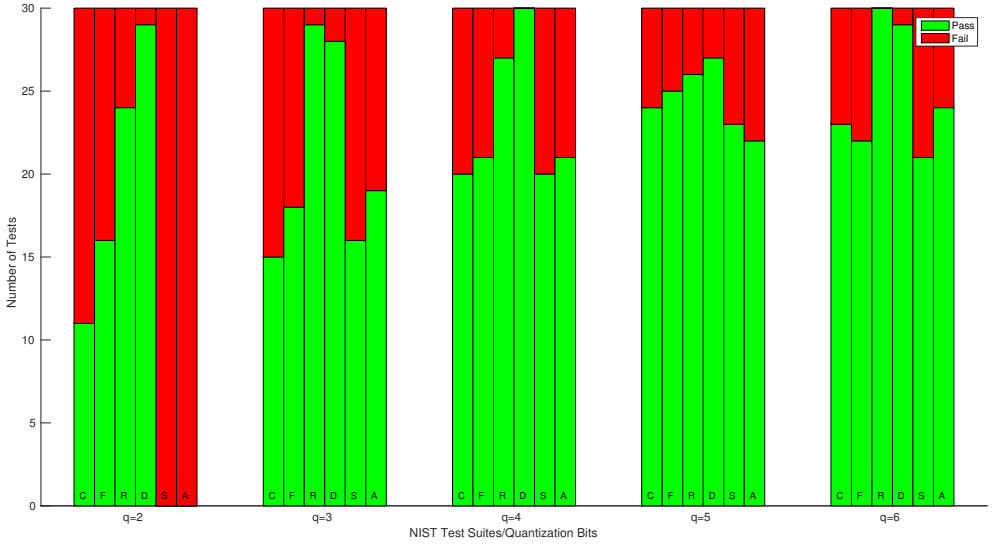


Figure A.33.: Result of the NIST tests.

Bibliography

[ABV06] G. Ács, L. Buttyán, and I. Vajda. Modelling adversaries and security objectives for routing protocols in wireless sensor networks. In *ACM Workshop on Security of Ad Hoc and Sensor Networks*, pages 49–58, New York, NY, USA, 2006. ACM.

[AC91] R. Ahlswede and I. Csiszar. The role of common randomness in information theory and cryptography, Part 1: Secrecy constraints. In *IEEE International Symposium on Information Theory*, pages 265–265, June 1991.

[AHT+05a] T. Aono, K. Higuchi, M. Taromaru, T. Ohira, B. Komiyama, and H. Sasaoka. Wireless secret key generation exploiting the reactance-domain scalar response of multipath fading channels. In *IEEE Transactions on Antennas and Propagation*, pages 3776–3784. November 2005.

[AHT+05b] T. Aono, K. Higuchi, M. Taromaru, T. Ohira, and H. Sasaoka. Wireless secret key generation exploiting the reactance-domain scalar response of multipath fading channels: RSSI interleaving scheme. In *The European Conference on Wireless Technology*, pages 173–176. October 2005.

[AM94] H.R. Anderson and J.P. McGeehan. Direct calculation of coherence bandwidth in urban microcells using a ray-tracing propagation model. In *IEEE International Symposium on Indoor and Mobile Radio Communications. Wireless Networks - Catching the Mobile Future*, volume 1, pages 20–24, September 1994.

[Ant] Frankonia BTA Antennas. Ultra-broadband antennas. `http://www.emcia.org/documents/ECMPartner/BTAAntenna.pdf`. Accessed 2015-05-08.

[AP09] P. Agrawal and N. Patwari. Correlated link shadow fading in multi-hop wireless networks. *IEEE Transactions on Wireless Communications*, 8(8):4024–4036, August 2009.

[ASKMY07] B. Azimi-Sadjadi, A. Kiayias, A. Mercado, and B.t Yener. Robust key generation from signal envelopes in wireless networks. In *ACM Conference on Computer and Communications Security*, pages 401–410. October 2007.

[BA81] M. Baldridge and E. Ambler. Guidelines for implementing and using the NBS Data Encryption Standard. 1981.

[Bal97] C. A. Balanis. *Antenna Theory: Analysis and Design*. John Wiley & Sons, 1997.

[BB11] M. Bloch and J. Barros. *Physical-Layer Security: From Information Theory to Security Engineering*. Cambridge University Press, 2011.

[BBGO08] V. Brik, S. Banerjee, M. Gruteser, and S. Oh. Wireless device identification with radiometric signatures. In *ACM International Conference on Mobile Computing and Networking*, pages 116–127, New York, NY, USA, 2008. ACM.

[BBRM08] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin. Wireless information-theoretic security. *IEEE Transactions on Information Theory*, 54(6):2515–2534, 2008.

[BD91] W. Braun and U. Dersch. A physical mobile radio channel model. *IEEE Transactions on Vehicular Technology*, 40(2):472–482, May 1991.

[BK12] E. Barker and J. Kelsey. *SP 800-90 B. Recommendation for the Entropy Sources Used for Random Bit Generation*. National Institute of Standards & Technology, Gaithersburg, MD, United States, 2012.

[Bla90] Richard E. Blahut. *Digital Transmission of Information*. Addison-Wesley, 1990.

[BR06] J. Barros and M.R.D. Rodrigues. Secrecy capacity of wireless channels. In *International Symposium on Information Theory*, pages 356–360, 2006.

[BRC07] K. B. Rasmussen and S. Capkun. Implications of radio fingerprinting on the security of sensor networks. In *Security and Privacy in Communications Networks and the Workshops*, pages 331–340, 2007.

[BRS+10] L. E. Bassham, A. L. Rukhin, J. Soto, J. R. Nechvatal, M. E. Smid, E. B. Barker, S. D. Leigh, M. Levenson, M. Vangel, D. L. Banks, N. A. Heckert, J. F. Dray, and S. Vo. *SP 800-22 Rev. 1a. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications*. National Institute of Standards & Technology, Gaithersburg, MD, USA, 2010.

[BS93] G. Brassard and L. Salvail. Secret-key reconciliation by public discussion. In *Advances in Cryptology - EUROCRYPT '93, Workshop on the Theory and Application of of Cryptographic Techniques, Lofthus, Norway, May 23-27, 1993, Proceedings*, pages 410–423, 1993.

[BV10] J. Biswas and M. Veloso. WiFi localization and navigation for autonomous indoor mobile robots. In *International Conference on Robotics and Automation (ICRA)*, pages 4379–4384, May 2010.

[Car29] J. R. Carson. Reciprocal theorems in radio communication. *Proceedings of the Institute of Radio Engineers*, 17(6):952–956, June 1929.

[CCH06] M. Cagalj, S. Capkun, and J. Hubaux. Key agreement in peer-to-peer wireless networks. In *Proceedings of the IEEE (Special Issue on Security and Cryptography)*, pages 467–478, 2006.

[CDK11] T. Chrysikos, T. Dagiuklas, and S. Kotsopoulos. Wireless information-theoretic security in an outdoor topology with obstacles: Theoretical analysis and experimental measurements. *EURASIP J. Wirel. Commun. Netw.*, 2011:4:1–4:7, January 2011.

[CGMO09] N. Chandran, V. Goyal, R. Moriarty, and R. Ostrovsky. Position based cryptography. In *Advances in Cryptology - CRYPTO 2009, 29th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 16-20, 2009. Proceedings*, pages 391–407, 2009.

[CGR05] M. Choi, G. Grosskopf, and D. Rohde. Statistical characteristics of 60 GHz wideband indoor propagation channel. In *International Symposium on Indoor and Mobile Radio Communications*, volume 1, pages 599–603, 2005.

[CH06] S. Capkun and J. Hubaux. Secure positioning in wireless networks. *IEEE Journal on Selected Areas in Communications*, 24(2):221–232, February 2006.

[CPK10] J. Croft, N. Patwari, and S. K. Kasera. Robust uncorrelated bit extraction methodologies for wireless sensors. In *International Conference on Information Processing in Sensor Networks, IPSN 2010, April 12-16, 2010, Stockholm, Sweden*, pages 70–81, 2010.

[cro] Moog-crossbow. `http://www.moog-crossbow.com/`. Accessed 2015-05-08.

[CW79] L. Carter and M. N. Wegman. Universal classes of hash functions. *J. Comput. Syst. Sci.*, 18(2):143–154, 1979.

[DBR05] S. Dossche, S. Blanch, and J. Romeu. Three different ways to decorrelate two closely spaced monopoles for MIMO applications. In *IEEE/ACES International Conference on Wireless Communications and Applied Computational Electromagnetics*, pages 849–852, April 2005.

[DES77] Data encryption standard (DES). In *FIPS PUB 46, Federal Information Processing Standards Publication*, pages 46–2, 1977.

[DH76] W. Diffie and M. E. Hellman. New directions in cryptography. *IEEE Transactions on Information Theory*, 22(6):644–654, 1976.

[DLMdA10] N. Döttling, D. Lazich, J. Müller-Quade, and A. S. de Almeida. Vulnerabilities of wireless key exchange based on channel reciprocity. In *Information Security Applications - 11th International Workshop, WISA 2010, Jeju Island, Korea, August 24-26, 2010, Revised Selected Papers*, pages 206–220, 2010.

[DLMQdA10] N. Döttling, D. Lazich, J. Müller-Quade, and A. S. de Almeida. Wireless key exchange using the GNU-Radio platform. In *European Reconfigurable Radio Technology Workshop (ERRT)*, 2010.

[DR98] J. Daemen and V. Rijmen. The block cipher Rijndael. In *Smart Card Research and Applications, CARDIS '98*, pages 277–284, 1998.

[FC04] D. B. Faria and D. R. Cheriton. No long-term secrets: Location-based security in overprovisioned wireless LANs. In *ACM Workshop on Hot Topics in Networks*, 2004.

[FC06] D. B. Faria and D. R. Cheriton. Detecting identity-based attacks in wireless networks using signalprints. In *ACM Workshop on Wireless Security*, pages 43–52, New York, NY, USA, 2006. ACM.

[FRA] Frankonia EMC test-systems. `http://www.frankoniagroup.com/cms/en/products/emc-test-equipment/`. Accessed 2015-05-08.

[Ger] I. Gerhardt. NIST-testsuite. implementierung in python. `http://gerhardt.ch/random.php`. Accessed 2015-05-08.

[GN05] S. Goel and R. Negi. Secret communication in presence of colluding eavesdroppers. In *IEEE Military Communication*, volume 3, pages 1501–1506. October 2005.

[gnu] GNU Radio. `http://www.gnuradio.org`. Accessed 2015-05-08.

[Gol00] O. Goldreich. *Foundations of Cryptography: Basic Tools*. Cambridge University Press, New York, NY, USA, 2000.

[GSS+03] D. Gesbert, M. Shafi, D. Shiu, P.J. Smith, and A. Naguib. From theory to practice: an overview of MIMO space-time coded wireless systems. *IEEE Journal on Selected Areas in Communications*, 21(3):281–302, April 2003.

[Har78] R.F. Harrington. Reactively controlled directive arrays. *IEEE Transactions on Antennas and Propagation*, 26(3):390–395, May 1978.

[Has93] H. Hashemi. The indoor radio propagation channel. *Proceedings of the IEEE*, 81(7):943–968, July 1993.

[HGB13] J. Hasse, T. Gloe, and M. Beck. Forensic identification of GSM mobile phones. In *ACM Workshop on Information Hiding and Multimedia Security*, pages 131–140, New York, NY, USA, 2013. ACM.

[HHO05] Q. Han, B. Hanna, and T. Ohira. A compact ESPAR antenna with planar parasitic elements on a dielectric cylinder. *IEICE Transactions*, 88-B(6):2284–2290, 2005.

[HHY95] J. E. Hershey, A. A. Hassan, and R. Yarlagadda. Unconventional cryptographic keying variable management. In *IEEE Transactions on Communications*, volume 43, pages 3–6. January 1995.

[HIU+08] T. Hashimoto, T. Itoh, M. Ueba, H. Iwai, H. Sasaoka, K. Kobara, and H. Imai. Comparative studies in key disagreement correction process on wireless key agreement system. In *Information Security Applications*, pages 173–187. January 2008.

[HSHC96] A. A. Hassan, W. E. Stark, J. E. Hershey, and S. Chennakeshu. Cryptographic key agreement for mobile radio. In *Digital Signal Processing*, pages 207–212. November 1996.

[IKM06] H. Imai, K. Kobara, and K. Morozov. On the possibility of key agreement using variable directional antenna. In *Joint Workshop on Information Security, Seoul, Korea*. September 2006.

[Jak74] W.C. Jakes. *Microwave Mobile Communications*. John Wiley & Sons, 1974.

[JYK+07] M. Jørgensen, B. Yanakiev, G. Kirkelund, P. Popovski, Hiroyuki Yomo, and T. Larsen. Shout to secure: Physical-layer wireless security with known interference. In *IEEE Global Telecommunications Conference*, pages 33–38. November 2007.

[KBC05] T. Kohno, A. Broido, and K.C. Claffy. Remote physical device fingerprinting. *IEEE Transactions on Dependable and Secure Computing*, 2(2):93–108, April 2005.

[KHC00] H. Koorapaty, A. A. Hassan, and S. Chennakeshu. Secure information transmission for mobile radio. In *IEEE Communication Letters*, volume 4, pages 52–55. February 2000.

[KJJ99] P. C. Kocher, J. Jaffe, and B. Jun. Differential power analysis. In *Advances in Cryptology - CRYPTO '99, 19th Annual International Cryptology Conference, Santa Barbara, California, USA, August 15-19, 1999, Proceedings*, pages 388–397, 1999.

[KL07] J. Katz and Y. Lindell. *Introduction to Modern Cryptography*. Chapman & Hall/CRC, 2007.

[KO05] H. Kawakami and T. Ohira. Electrically steerable passive array radiator (ESPAR) antennas. *IEEE Antennas and Propagation Magazine*, 47(2):43–50, April 2005.

[Kob87] N. Koblitz. Elliptic curve cryptosystems. *Mathematics of Computation*, 48(177):203–209, 1987.

[Koc96] P. C. Kocher. Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems. In *Advances in Cryptology - CRYPTO '96, 16th Annual International Cryptology Conference, Santa Barbara, California, USA, August 18-22, 1996, Proceedings*, pages 104–113, 1996.

[KV08] H. Kim and J. D. Villasenor. Secure MIMO communications in a system with equal number of transmit and receive antennas. In *IEEE Communication Letters*, volume 12, pages 386–388. May 2008.

[KW03] C. Karlof and D. Wagner. Secure routing in wireless sensor networks: attacks and countermeasures. In *IEEE International Workshop on Sensor Network Protocols and Applications*, pages 113–127, May 2003.

[KW10] A. Khisti and G. W. Wornell. Secure transmission with multiple antennas; Part II: The MIMOME wiretap channel. *IEEE Transactions on Information Theory*, 56(11):5515–5532, November 2010.

[KWWE07] A. Khisti, G. Wornell, A. Wiesel, and Y. Eldar. On the Gaussian MIMO wiretap channel. In *IEEE International Symposium on Information Theory*, pages 2471–2475, June 2007.

[KYL08] S. Kim, M. Yung, and H. Lee, editors. *Information Security Applications, 8th International Workshop, WISA 2007, Jeju Island, Korea, August 27-29, 2007, Revised Selected Papers*, volume 4867 of *Lecture Notes in Computer Science*. Springer, 2008.

[LCR05] X. Li, M. Chen, and E. P. Ratazzi. Space-time transmissions for wireless secret-key agreement with information-theoretic secrecy. In *IEEE 6th Workshop on Signal Processing Advances in Wireless Communications*, pages 811–815. June 2005.

[LDS12] Y. Liu, S. C. Draper, and A. M. Sayeed. Exploiting channel diversity in secret key generation from multipath fading randomness. *IEEE Transactions on Information Forensics and Security*, 7(5):1484–1497, 2012.

[Lee73] W.C.Y. Lee. Effects on correlation between two mobile radio base-station antennas. *IEEE Transactions on Communications*, 21(11):1214–1224, November 1973.

[LHR06] X. Li, J. Hwu, and E. P. Ratazzi. Array redundancy and diversity for wireless transmissions with low probability of interception. In *IEEE International Conference on Acoustics, Speech and Signal Processing, ICASSP Proceedings*, volume 4, pages 525–528. May 2006.

[LHR07] X. Li, J. Hwu, and E. P. Ratazzi. Using antenna array redundancy and channel diversity for secure wireless transmissions. In *Journal of Communications*, volume 2, pages 24–32. May 2007.

[LP07] R. Liu and H. V. Poor. Multiple antenna secure broadcast over wireless networks. *CoRR*, arXiv:0705.1183, 2007.

[LR05] X. Li and E. P. Ratazzi. MIMO transmissions with information-theoretic secrecy for secret-key agreement in wireless networks. In *IEEE Military Communications Conference*, volume 3, pages 1353–1359. October 2005.

[LvTvD03] S. Liu, H. C. A. van Tilborg, and M. van Dijk. A practical protocol for advantage distillation and information reconciliation. *Des. Codes Cryptography*, 30(1):39–62, 2003.

[LXMT06] Z. Li, W. Xu, R. Miller, and W. Trappe. Securing wireless systems via lower layer enforcements. In *5th ACM Workshop on Wireless Security*, pages 33–42, New York, NY, USA, 2006. ACM.

[LYCH78] S.K. Leung-Yan-Cheong and M. E. Hellman. The Gaussian wiretap channel. In *IEEE Trans. Inform. Theory*, volume 24, pages 451–56. July 1978.

[Mau93] U. M. Maurer. Secret key agreement by public discussion from common information. *IEEE Transactions on Information Theory*, 39(3):733–742, 1993.

[MdA14] J. Müller-Quade and A. S. de Almeida. Wireless key exchange using frequency impairments. In *Information Security Applications - 15th International Workshop, WISA 2014, Jeju Island, Korea, August 25-27, 2014. Revised Selected Papers*, pages 283–294, 2014.

[MFZ+12] D. Maas, M.H. Firooz, J. Zhang, N. Patwari, and S.K. Kasera. Channel sounding for the masses: Low complexity GNU 802.11b channel impulse response estimation. *IEEE Transactions on Wireless Communications*, 11(1):1–8, January 2012.

[Mil85] V. S. Miller. Use of elliptic curves in cryptography. In *Advances in Cryptology - CRYPTO '85, Santa Barbara, California, USA, August 18-22, 1985, Proceedings*, pages 417–426, 1985.

[Mor11] C. E. Morimoto. Guia do hardware. `http://www.hardware.com.br/guias/redes-wireless/antenas.html`, November 2011. Accessed 2015-05-08.

[MTM+08] S. Mathur, W. Trappe, N. Mandayam, C. Ye, and A. Reznik. Radiotelepathy: Extracting a secret key from an unauthenticated wireless channel. In *ACM International Conference on Mobile Computing and Networking*, pages 128–139, New York, NY, USA, 2008. ACM.

[MW03a] U. M. Maurer and S. Wolf. Secret-key agreement over unauthenticated public channels I: definitions and a completeness result. *IEEE Transactions on Information Theory*, 49(4):822–831, 2003.

[MW03b] U. M. Maurer and S. Wolf. Secret-key agreement over unauthenticated public channels II: the simulatability condition. *IEEE Transactions on Information Theory*, 49(4):832–838, 2003.

[MW03c] U. M. Maurer and S. Wolf. Secret-key agreement over unauthenticated public channels III: privacy amplification. *IEEE Transactions on Information Theory*, 49(4):839–851, 2003.

[net] Netstumbler. `http://www.netstumbler.com/`. Accessed 2015-05-08.

[NG05] R. Negi and S. Goel. Secret communication using artificial noise. In *Vehicular Technology Conference*, volume 3, pages 1906–1910, 2005.

[Ohi05] T. Ohira. Secret key generation exploiting antenna beam steering and wave propagation reciprocity. In *European Microwave Conference*, volume 1. October 2005.

[OOKF68] Y. Okumura, E. Ohmori, T. Kawano, and K. Fukuda. Field strength and its variability in VHF and UHF land mobile radio services. 1968.

[PB05] P. Parada and R. Blahut. Secrecy capacity of SIMO and slow fading channels. In *International Symposium on Information Theory*, pages 2152–2155. September 2005.

[PJC+13] S. N. Premnath, S. Jana, J. Croft, P. L. Gowda, M. Clark, S. K. Kasera, N. Patwari, and S. V. Krishnamurthy. Secret key extraction from wireless signal strength in real environments. *IEEE Trans. Mob. Comput.*, 12(5):917–930, 2013.

[Pro02] J. Proakis. *Communication Systems Engineering*, chapter 7.6. Prentice Hall, 2002.

[RM93] R. Rood and F. Morehouse. Channel sounder testing for tactical communications. In *Military Communications Conference*, volume 2, pages 369–373 vol.2, October 1993.

[RSA78] R. L. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Commun. ACM*, 21(2):120–126, February 1978.

[Sha48] C. E. Shannon. A mathematical theory of communication. *Bell System Technical Journal*, 27(3):379–423, 1948.

[SHOK04] C. Sun, A. Hirata, T. Ohira, and N. C. Karmakar. Fast beamforming of electronically steerable parasitic array radiator antennas: Theory and experiment. In *IEEE Transactions on Antennas and Propagation*, pages 1819–1832. July 2004.

[SIS09] T. Shimizu, H. Iwai, and H. Sasaoka. Information reconciliation using reliability in secret key agreement scheme with ESPAR antenna. In *Security and Privacy in Mobile Information and Communication Systems, First International ICST Conference, MobiSec 2009, Turin, Italy, June 3-5, 2009, Revised Selected Papers*, pages 148–159, 2009.

[SK98] J.S. Sadowsky and V. Kafedziski. On the correlation and scattering functions of the WSSUS channel for mobile communications. *IEEE Transactions on Vehicular Technology*, 47(1):270–282, February 1998.

[SP08] A. M. Sayeed and A. Perrig. Secure wireless communications: Secret keys through multipath. In *IEEE International Conference on Acoustics, Speech, and Signal Processing*, pages 3013–3016, 2008.

[Sti02] D. Stinson. *Cryptography: Theory and Practice*. Chapman & Hall/CRC, 2nd edition, 2002.

[SY00] T. Sugimoto and K. Yamazaki. A study on secret key reconciliation protocol "cascade". *IEICE Trans. Fundamentals*, E83-A(10):1987–1991, October 2000.

[TC07] E. Taillefer and J. Cheng. Reactance-domain signal processing for adaptive beamforming and direction-of-arrival estimation: An overview. *Radio Science Bulletion*, (323):14–25, December 2007.

[TM01] M. A. Tope and J. C. McEachen. Unconditionally secure communications over fading channels. In *Military Communications Conference. Communications for Network-Centric Operations: Creating the Information Force*, volume 1, pages 54–58. 2001.

[TMB01] M. Takai, J. Martin, and R. Bagrodia. Effects of wireless physical layer modeling in mobile ad hoc networks. In *ACM International Symposium on Mobile Ad Hoc Networking & Computing*, pages 87–94, New York, NY, USA, 2001. ACM.

[TTD00] J.K. Tugnait, L. Tong, and Z. Ding. Single-user channel estimation and equalization. *IEEE Signal Processing Magazine*, 17(3):16–28, May 2000.

[TV05] D. Tse and P. Viswanath. *Fundamentals of Wireless Communication*. Cambridge University Press, 2005.

[TY07] E. Tekin and A. Yener. The gaussian multiple access wire-tap channel: wireless secrecy and cooperative jamming. In *Information Theory and Applications Workshop, 2007*, pages 404–413. February 2007.

[USR] Ettus research. `http://www.ettus.com/`. Accessed 2015-05-08.

[VA87] R.G. Vaughan and J.B. Andersen. Antenna diversity in mobile communications. *IEEE Transactions on Vehicular Technology*, 36(4):149–172, November 1987.

[VBBH05] V. Y. Vu, J. Braga, X. Begaud, and B. Huyart. Direction of arrival and time delay measurements for multi-path signals using five-port reflectometers. In *Antennas and Propagation Society International Symposium*, volume 1B, pages 735–738 vol. 1B, 2005.

[WP11] J. Wilson and N. Patwari. See-through walls: Motion tracking using variance-based radio tomography networks. *IEEE Transactions on Mobile Computing*, 10(5):612–621, May 2011.

[WSS03] A. Wood, J.A. Stankovic, and S.H. Son. JAM: a jammed-area mapping service for sensor networks. In *Real-Time Systems Symposium*, pages 286–297, December 2003.

[WTS07] R. Wilson, D. Tse, and R.A. Scholtz. Channel identification: Secret sharing using reciprocity in ultrawideband channels. In *IEEE International Conference on Ultra-Wideband*, pages 270–275, 2007.

[Wyn75] A.D. Wyner. The wire-tap channel. In *Bell Syst. Tech. J.*, volume 54, pages 1355–87. October 1975.

[XJ10] J. Xiong and K. Jamieson. SecureAngle: improving wireless security using angle-of-arrival information. In *ACM Workshop on Hot Topics in Networks., Monterey, CA, USA - October 20 - 21, 2010*, page 11, 2010.

[XJ13] J. Xiong and K. Jamieson. SecureArray: Improving wifi security with fine-grained physical-layer information. In *Annual International Conference on Mobile Computing & Networking*, pages 441–452, New York, NY, USA, 2013. ACM.

[XTZW05] W. Xu, W. Trappe, Y. Zhang, and T. Wood. The feasibility of launching and detecting jamming attacks in wireless networks. In *ACM international symposium on Mobile ad hoc networking and computing*, pages 46–57. 2005.

[XWTZ04] W. Xu, T. Wood, W. Trappe, and Y. Zhang. Channel surfing and spatial retreats: Defenses against wireless denial of service. In *Proceedings of the 3rd ACM Workshop on Wireless Security*, pages 80–89, New York, NY, USA, 2004. ACM.

[Yao82] A. Yao. Protocols for secure computations (extended abstract). In *Symposium on Foundations of Computer Science, Chicago, Illinois, USA, 3-5 November 1982*, pages 160–164, 1982.

[YMR+09] C. Ye, S. Mathur, A. Reznik, Y. Shah, W. Trappe, and N. B. Mandayam. Information-theoretically secret key generation for fading wireless channels. arXiv:0910.5027, 2009.

[ZAW+14] C. T. Zenger, A. Ambekar, F. Winzer, T. Pöppelmann, H. D. Schotten, and C. Paar. Preventing scaling of successful attacks: A cross-layer security architecture for resource-constrained platforms. In *International Conference on Cryptography and Information Security*, 2014.

[ZBN05] T. Zwick, T.J. Beukema, and H. Nam. Wideband channel sounder with measurements and model for the 60 ghz indoor radio channel. *IEEE Transactions on Vehicular Technology*, 54(4):1266–1277, July 2005.

[ZCP+14] C. T. Zenger, M. Chur, J. Posielek, C. Paar, and G. Wunder. A novel key generating architecture for wireless low-resource devices. In *International Workshop on Secure Internet of Things*, pages 26–34, 2014.

[ZW99] H.-J. Zepernick and T.A. Wysocki. Multipath channel parameters for the indoor radio at 2.4 GHz ISM band. In *Vehicular Technology Conference*, volume 1, pages 190–193 vol.1, July 1999.