

# Hybrid low-voltage physical unclonable function based on inkjet-printed metal-oxide transistors

Alexander Scholz<sup>1,2,6</sup>, Lukas Zimmermann<sup>3,6</sup>, Ulrich Gengenbach<sup>4</sup>, Liane Koker<sup>4</sup>, Zehua Chen<sup>4</sup>, Horst Hahn<sup>1</sup>, Axel Sikora<sup>3</sup>, Mehdi B. Tahoori<sup>5</sup> & Jasmin Aghassi-Hagmann<sup>1,2</sup>✉

Modern society is striving for digital connectivity that demands information security. As an emerging technology, printed electronics is a key enabler for novel device types with free form factors, customizability, and the potential for large-area fabrication while being seamlessly integrated into our everyday environment. At present, information security is mainly based on software algorithms that use pseudo random numbers. In this regard, hardware-intrinsic security primitives, such as physical unclonable functions, are very promising to provide inherent security features comparable to biometrical data. Device-specific, random intrinsic variations are exploited to generate unique secure identifiers. Here, we introduce a hybrid physical unclonable function, combining silicon and printed electronics technologies, based on metal oxide thin film devices. Our system exploits the inherent randomness of printed materials due to surface roughness, film morphology and the resulting electrical characteristics. The security primitive provides high intrinsic variation, is non-volatile, scalable and exhibits nearly ideal uniqueness.

<sup>1</sup>Institute of Nanotechnology, Karlsruhe Institute of Technology, Hermann-von-Helmholtz-Platz 1, Eggenstein-Leopoldshafen 76344, Germany. <sup>2</sup>Institute for Applied Research, Offenburg University of Applied Sciences, Badstraße 24, Offenburg 77652, Germany. <sup>3</sup>Institute of Reliable Embedded Systems and Communication Electronics, Offenburg University of Applied Sciences, Badstraße 24, Offenburg 77652, Germany. <sup>4</sup>Institute for Automation and Applied Informatics, Karlsruhe Institute of Technology, Hermann-von-Helmholtz-Platz 1, Eggenstein-Leopoldshafen 76344, Germany. <sup>5</sup>Chair of Dependable Nano Computing, Karlsruhe Institute of Technology, Haid-und-Neu-Straße 7, Karlsruhe 76131, Germany. <sup>6</sup>These authors contributed equally: Alexander Scholz, Lukas Zimmermann. ✉email: [jasmin.aghassi@kit.edu](mailto:jasmin.aghassi@kit.edu)

The term Internet of Things (IoT) describes the ubiquitous presence of interconnected devices exchanging sensitive data, often through open communication channels, which can be compromised. In this era of digitization, device identity and encryption techniques are more than ever vital factors for ensuring data security, proper authentication, and secure communication<sup>1–8</sup>. Many security solutions, such as the asymmetric key establishment methods<sup>9,10</sup>, are based on mathematically proven foundations and significantly rely on random numbers. The trustworthiness of the encryption depends on the quality of the random number generators (RNGs) used for the generation of public and private keys. Ideally, the generation of random numbers uses the entropy of a high-quality randomness source. Various software-based computational or hardware-based methods exist for RNGs, each more or less satisfying the requirements for cryptographic applications. Fast symmetric cryptographic algorithms, such as the Advanced Encryption Standard (AES)<sup>11</sup>, have also been used and offer a high level of security, if the established private key is truly secret. As a consequence, inter-linked security solutions in software as well as in hardware are increasingly in demand. Especially for IoT-enabled devices, which are often subject to strict design and performance constraints, hardware-based security is essential.

To tackle the aforementioned challenges, hardware-intrinsic security solutions based on unique device parameters are deployed. These security primitives are referred to as physical unclonable functions (PUFs), which are used for identification, authentication, and cryptographic key generation<sup>12–15</sup>. Among the main advantages of PUFs to be used as root of trust in the IoT, is their unique and unclonable response as well as their memory-less circuit architecture making them less vulnerable to invasive attacks. Historically, initial studies regarding PUFs were carried out by exploiting imperfect surface speckle patterns<sup>16</sup> as an entropy source. One major drawback is the high equipment overhead for key generation and readout, making this PUF approach inapplicable for most application fields. In the next step, silicon-based PUFs (Si-PUFs), leveraging intrinsic manufacturing-induced variations of integrated circuits (ICs), were studied and present a well-established PUF implementation<sup>5,12–14,17,18</sup>. Si-PUFs can be further classified as bi-stable<sup>19–21</sup>, delay-based<sup>22</sup>, or analog PUFs<sup>23,24</sup>, depending on the underlying variation source, such as dopants, defects, and geometrical device dimensions. Furthermore, Si-PUFs often suffer from reduced entropy<sup>25</sup>, compared with additive manufacturing techniques. Also, IC fabrication is limited to a few foundries worldwide. In many application domains where the entire design and fabrication are sensitive, globalization of foundries is a major risk. This invites counterfeiting and tampering of the IC or readout of the Si-PUF-specific keys by third parties before the official deployment by the end user. In general, lithography-based silicon technologies face a cost barrier for many envisioned applications and devices in the scope of the IoT. Furthermore, with the ever-increasing demand in electronic devices for the IoT, electronic waste (e-waste), that presents a substantial ecological problem up to now<sup>26–28</sup>, is even expected to increase<sup>27,28</sup>.

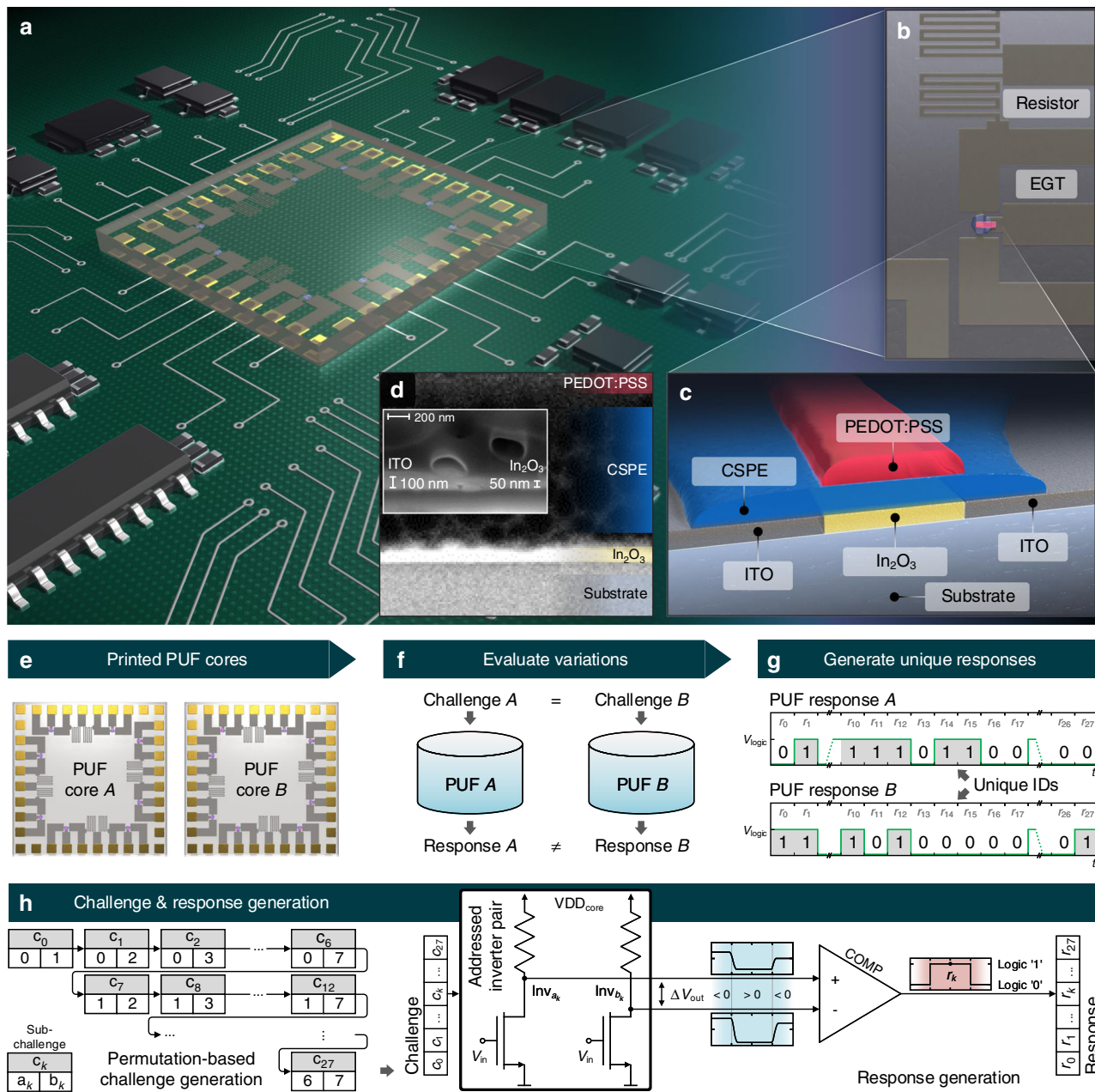
In the near future, emerging technologies such as printed electronics (PE) will further expand the IoT by enabling features like new form factors, flexible substrates, stretchability of the hardware circuits, transparency, and large-area sensing while providing low-cost fabrication<sup>29–31</sup>. PE can help to tackle e-waste by efficient use of non-toxic, and bio-degradable materials to empower a sustainable future regarding “green electronics”<sup>32,33</sup>. Recently, PUFs based on novel materials, such as quantum dots (Liu et al.<sup>34</sup>), biological human T cells (Wali et al.<sup>25</sup>) were presented, mostly utilizing optical inspections for key generation. Other works on promising novel materials and methods

concentrate on fingerprint-like intrinsic counterfeit protection using random surface patterns<sup>25,34–41</sup>. These approaches need high-cost equipment such as microscopes, image processing, and optical readout for reliable key generation. Also, optical PUFs may face challenges when integrated into signal- and software-layers, which are mainly realized as electronic systems. Another direction in PUF research is to use novel materials and methods and adapt the concepts of Si-PUF architectures<sup>42–50</sup>. Emerging technologies, such as PE, enable decentralized, customizable manufacturing of small and mid-size volumes, which can help to establish “root of trust” in the manufacturing supply chain. Furthermore, owing to the manifold possibilities in design, materials, and substrates it offers a core complexity with many sources of entropy, which can be exploited for hardware-based security. Owing to the additive manufacturing process of printed active devices, larger device variations are expected, compared with lithographically structured devices. The source of variations can be numerous, reaching from the discrete droplet size of the printed ink, the surface roughness of printed layers and the quality of interfaces between layers in general, up to scaling errors in the channel width-to-length ratio due to the manufacturing process and physical layout of a design, to name but a few<sup>51–56</sup>.

In this work, we leverage the sources of entropy in printed devices to generate a unique unclonable response function. We develop unclonable, unique PUF security primitives by combining the advantages of PE and Si-based technologies. The security primitives are fabricated through inkjet-printing of the PUF core using electrolyte-gated transistors (EGTs). The surrounding control logic that harvests the intrinsic variations of the printed PUF core is composed of Si-based technology. So far, related printed PUF implementations remain limited to standalone, often single device implementations, neither addressing the system level integration nor including statistical validity. With this work, we overcome the existing limitations with an integrated hybrid PUF implementation for 28-bit, which is scalable to arbitrary key bit width and shows superior security features. We have further performed a statistical analysis based on experimental large-scale characterization for important PUF security metrics, such as uniqueness, bit aliasing, reliability, and bit errors. In addition, the design has the potential in the near future of being fully printed, including the Si-based logic periphery circuits, once inkjet-printed circuit technology evolves further. To the best of our knowledge, designing, fabricating, and embedding a printed PUF core into a system level environment as well as the experimental analysis of PUF security metrics has not been presented before.

## Results

**Full fabrication of hybrid PUF security primitive.** The hybrid (i.e., Si-based control logic and printed PUF core) PUF system and its components are shown in Fig. 1a–d. The printed PUF core, as an intrinsic variation source, is embedded into an addressing and readout environment, as shown in Supplementary Fig. 1. The hybrid PUF evaluation and unique response generation principle is shown in Fig. 1e–h and Supplementary Fig. 2. The PUF core circuit consists of an inkjet-printed inverter array realized with EGTs and resistive indium-tin oxide (ITO) meander structures as load resistors, as shown in Fig. 1b. EGTs operate at low voltages ( $\leq 2.0$  V) and show circuit performances ranging from several hundreds of Hz until kHz<sup>57–60</sup>. Studies on EGT variations and device variation modeling have also been studied prior to this work<sup>61,62</sup>. In our hybrid PUF approach, we exploit the implicit random variations caused by the material composition, layer thickness and roughness, as well as interface properties between several printed layers as a source of randomness for hardware security (see Fig. 1d). These variations are reflected in

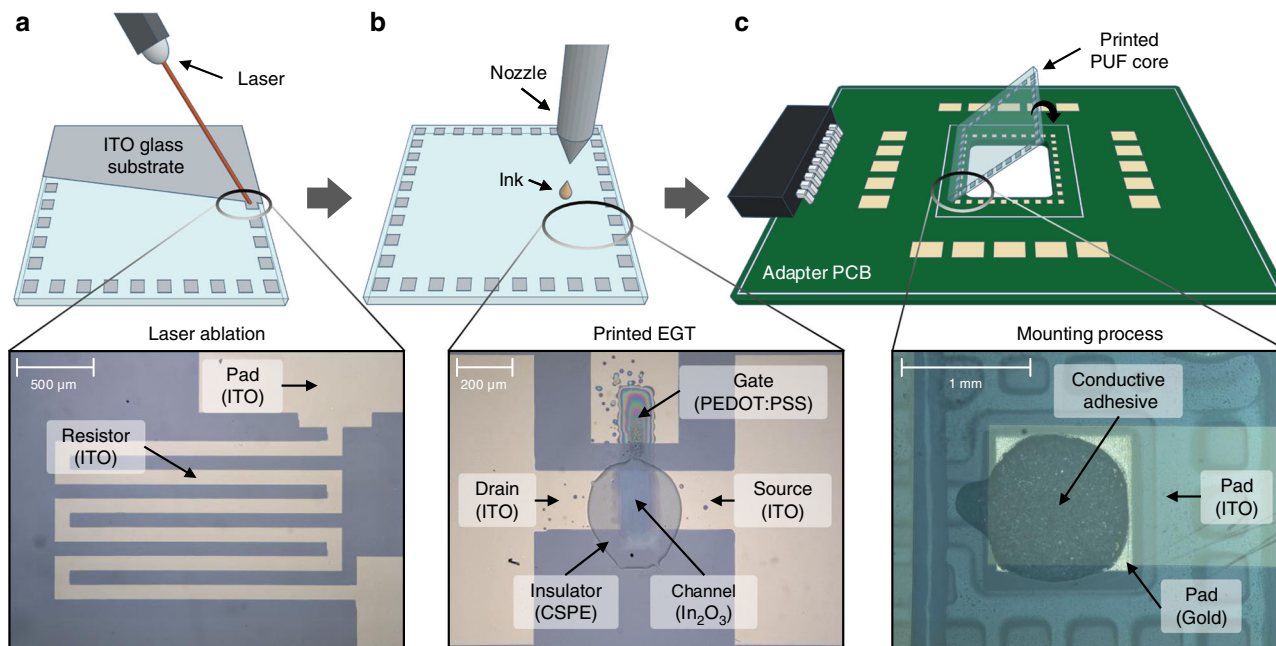


**Fig. 1** Integrated hybrid PUF circuit and corresponding challenge-response mechanism. **a** Schematic illustration of the hybrid PUF with the printed core substrate mounted onto the control logic printed circuit board (PCB). **b** Zoom in of one PUF core inverter consisting of a resistor-electrolyte-gated transistor-pair. **c** Schematic EGT top-gate bottom-contact stack structure. **d** Scanning electron microscopy (SEM) image of a printed EGT, which shows the non-uniform semiconductor-/electrolyte interface. The small inset picture shows the ITO film thickness with the known 100 nm layer thickness as a reference. The inkjet-printed ( $\text{In}_2\text{O}_3$ ) layer is determined to be  $\approx 50$  nm. On the ITO layer, also an ( $\text{In}_2\text{O}_3$ ) film can be seen. **e** Two examples of printed PUF cores A and B fabricated with equal processes. **f** Evaluation of the random variations caused by the fabrication process in terms of applying the same challenge to the PUFs A and B and extracting their unique responses. **g** Digital timing diagram representation of the unique PUF responses  $\{r_0r_1\dots r_{27}\}$  for two PUF cores A and B, respectively. **h** High-level schematic of the challenge and response generation procedure. The inverter pair ( $\text{Inv}_{a_k}, \text{Inv}_{b_k}$ ) addressing is provided by the permutation-based sub-challenge  $c_k$ . The comparator output generates the corresponding sub-response  $r_k$ , based on the voltage difference  $\Delta V_{\text{out}}$  between  $\text{Inv}_{a_k}$  and  $\text{Inv}_{b_k}$ .

the electrical characteristics of our printed EGTs and corresponding inverter structures. By addressing two inverters ( $\text{Inv}_{a_k}, \text{Inv}_{b_k}$ ) simultaneously and comparing their output voltages, one output bit is generated based on the voltage difference  $\Delta V_{\text{out}}$ . To enable a comprehensive understanding of the challenge-response mechanism and the corresponding effects that lead to the response bits, we also track the individual inverter

output voltages at the comparator input with an analog-to-digital converter (ADC). The full mechanism of the challenge-response generation is shown in Fig. 1h. The exact challenge configuration to generate a 28-bit response is further described in the Supplementary Fig. 2.

As substrate, we have used ITO-covered 20 mm  $\times$  20 mm glass (PGO CEC020S) with a layer thickness of 100 nm. After laser



**Fig. 2** Fabrication and integration process of the printed PUF core into the PCB. **a** Structuring by laser ablation of the PUF core circuit including routing strips, resistors, I/O and transistor terminals. **b** Inkjet-printing of the EGT layers, such as  $\text{In}_2\text{O}_3$  (channel), electrolyte (gate insulation), and top gate (PEDOT:PSS). **c** Flip-chip adopted mounting process of the inkjet-printed PUF core onto the adapter PCB using conductive adhesive.

ablation, the resulting ITO structures present the electrodes and resistor structures used in the PUF core design, employing eight inverters. In general, the scalable design of the hybrid PUF is not limited to eight PUF core inverters and can be extended if needed. The placement of the components follows a symmetrical alignment, where the input–output (I/O) terminals of all core inverters are connected to bonding pads. This design approach eliminates the need for printed crossovers by shifting this complexity to the Si-based system. A large width of the I/O terminal wiring was chosen to reduce the resistivity of the ITO strips. Also, this increases the manufacturing yield for the printed PUF cores. The EGT transistor stack is designed as a top-gate bottom-contact structure, as displayed in Fig. 1c. Fig. 1d displays the corresponding scanning electron microscopy (SEM) image of a printed EGT, showing the non-uniform semiconductor/electrolyte interface as intrinsic variation source. The smaller inset picture shows the layer thickness as a reference. Fig. 2 shows the manufacturing process and integration workflow for the printed PUF core. In the first step, an ITO glass substrate is structured via laser ablation, using a Trumpf TruMicro 5000 picosecond laser. The structured ITO layer includes the full electrical signal routing of the PUF core such as I/O terminal routing strips, resistive meander structures and the drain, gate, and source terminals of the printed EGTs, respectively.

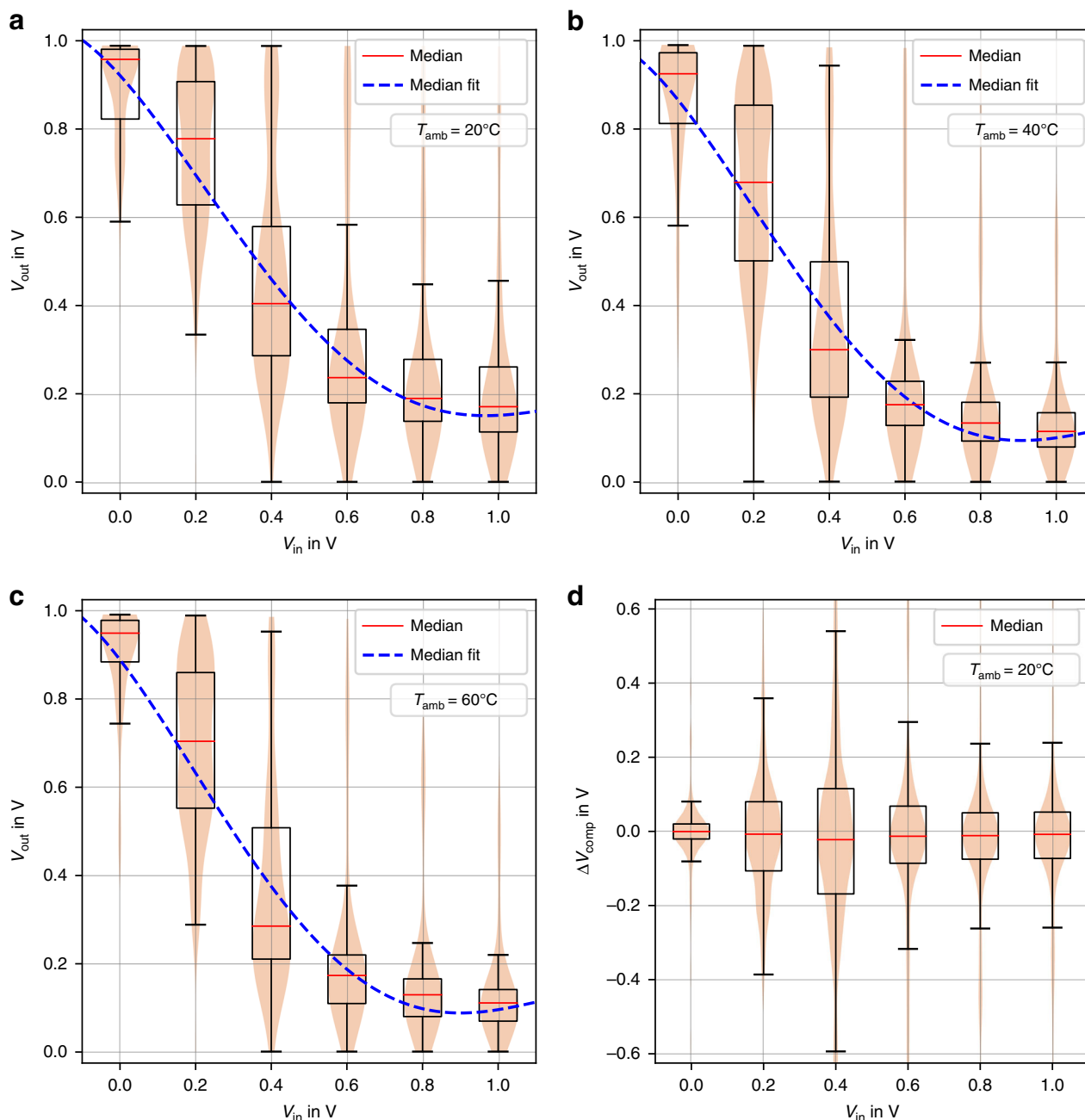
After cleaning the structured glass substrate in an ultra-sonic bath with acetone and isopropanol (1:1) for 1 hour, an indium (III) nitrate hydrate ( $\text{H}_2\text{InN}_3\text{O}_{10}$ )-based precursor is inkjet-printed between the transistors' drain and source electrodes. Following an annealing step at  $400^\circ\text{C}$ , the indium-oxide ( $\text{In}_2\text{O}_3$ ) semiconductor thin-film channel is formed<sup>63</sup>, and a composite-solid-polymer-electrolyte (CSPE) is inkjet-printed as a gate insulator. In a final step, poly(3,4-ethylenedioxythiophene):poly(styrenesulfonate) (PEDOT:PSS) is inkjet-printed as the top-gate electrode material. The precursor and ink formulations can be seen in the Methods section. All inkjet-printing steps are performed with a Fujitsu Dimatix DMP-2850 inkjet-printer. The hybrid PUF's control logic includes the addressing and readout circuitry for the printed PUF core and is assembled with

discrete Si-based components (see Supplementary Fig. 1 and Supplementary Note 1). To enable large-scale characterization, an adapter PCB has been designed that allows printed PUF cores with a fixed control logic to be interchanged (see Supplementary Figs. 1 and 8). The integration process of the printed PUF cores onto Si-based adapter PCBs is derived from the silicon flip-chip mounting process<sup>64</sup>. Conductive interconnection between the ITO-based printed PUF core conductive layer I/O terminals and the gold-coated contact pads on the adapter PCB is implemented by a low-temperature curing conductive adhesive. This approach allows mounting at ambient room temperature, thereby diminishing potential negative impact on the printed devices during the integration process. Automated integration includes adhesive dispensing on the adapter PCBs and precise alignment and mounting of the PUF core substrates on the PCBs. The proposed framework allows for various different technology nodes to be seamlessly integrated, in our case printed EGTs and discrete Si-based CMOS circuitry. The standardized interface between printing technology and PCB also permits the evaluation PCB to be interchanged, enabling large-scale automated characterization of several printed PUF cores, for example, for statistical evaluation in a real system environment.

**Printed PUF core analog signal level characteristics.** In general, a full readout of the hybrid PUF includes all PUF core inverter address pair permutations. For eight inverters, the maximum bit-width  $L_{\text{max}} = 28$  for a single PUF response is calculated by the binomial coefficient without repetitions according to Eq. (1). In the approach used here, we apply all inverter address permutations subsequently in sub-challenges, thereby generating the corresponding sub-response bits, and concatenate them to obtain the full PUF response as a digital bit sequence.

$$L_{\text{max}} = \frac{M \cdot (M - 1)}{2} \Big|_{M=8} \quad (1)$$

To obtain more PUF responses, the number of inverter address combinations in the challenge could be decreased, which splits the



**Fig. 3 Printed PUF core voltage characteristics.** **a** Inverter voltage transfer curve including all 120 fabricated inverters at a relative humidity of 50%, a PUF core supply voltage of 1 V and at 20 °C. The maximum output voltage variation is reached around  $V_{in} = 0.4$  V. **b** Inverter voltage transfer curve including all 120 fabricated inverters at a relative humidity of 50%, a PUF core supply voltage of 1 V and at 40 °C. **c** Inverter voltage transfer curve including all 120 fabricated inverters at a relative humidity of 50%, a PUF core supply voltage of 1 V and at 60 °C. **d** Voltage difference levels  $\Delta V_{comp}$  at the comparator input terminals including all PUF core inverter pair combinations at the ambient temperature 20 °C. The data shown in **a-d** is visualized as box plot as well as violin plot (light red shaded area). The red line in the box plot marks the median value for  $V_{out}$ . The upper end of the box in the box plot represents the 75 percentile of the  $V_{out}$  distribution and the bottom side the 25 percentile. The maximum is at the 95 percentile, whilst the minimum is at the respective five percentile. The violin plot includes the full data range for  $V_{out}$  and helps to visualize the data distribution more clearly. The blue dashed line in **a-c** is a fit over the corresponding median values with a fourth-degree polynomial.

challenge-response pair (CRP) space into various units. However, it must be noted that this approach also decreases the bit-width of the single PUF responses. For the following investigations of the fabricated hybrid PUFs on the analog signal level, we apply different test cases in defined by temperatures in the range of  $T_{amb} = \{20\text{ }^\circ\text{C}, 40\text{ }^\circ\text{C}, 60\text{ }^\circ\text{C}\}$  as well as controlled relative humidity (RH) and PUF core supply voltage conditions ( $VDD_{core}$ ). This allows to visualize the temperature dependencies of the PUF core inverter

voltage transfer curves. All measurements were performed in a Weiss WK3 climatic chamber to obtain a controlled operational environment.

Fig. 3a–c show the voltage transfer curves  $V_{out} = f(V_{in})$  of 120 inverters taken from 15 fabricated printed PUF cores as statistical violin and box plot with different temperature conditions, (a)  $T_{amb} = 20\text{ }^\circ\text{C}$ , (b)  $T_{amb} = 40\text{ }^\circ\text{C}$ , and (c)  $T_{amb} = 60\text{ }^\circ\text{C}$ , a stable relative humidity at  $RH = 50\%$ , and PUF core supply voltage at

$VDD_{core} = 1$  V. For an ambient temperature of  $20$  °C, the inverters' maximum output voltage variation is at  $V_{in} = 0.4$  V, as shown in Fig. 3a. With increasing temperature, an increase in the transistor drain current  $I_D$  is expected, which leads to a reduction of  $V_{out}$  as can be seen in Fig. 3b and 3c. The light red shaded violin plots at each  $V_{in}$  cover the complete  $V_{out}$  measurement data. The plots indicate that some inverters do not show the expected voltage transfer curves. Nonetheless, such potential malfunctioning of single inverter cells does not affect PUF operation in a negative manner as long as the PUF responses can be reproduced, which is verified experimentally later in this paper.

Furthermore, Fig. 3d shows the corresponding voltage differences at the comparator input terminals ( $\Delta V_{comp}$ ) over the test case  $P_1$  as violin and box plot. At  $V_{in} = 0.4$  V the median value for  $V_{out}$  is  $-48$  mV, and the measured samples interquartile range is at  $284.1$  mV, respectively. We can conclude that biasing the hybrid PUF around this  $V_{in}$  is beneficial, as most probably a high-voltage difference  $\Delta V_{comp}$  can be expected. This satisfies the constraint that the inverter voltage difference levels  $\Delta V_{out}$  are much larger than the control logic's systematic error  $\Delta V_e$  ( $\Delta V_{out} \gg \Delta V_e$ )<sup>65</sup>.

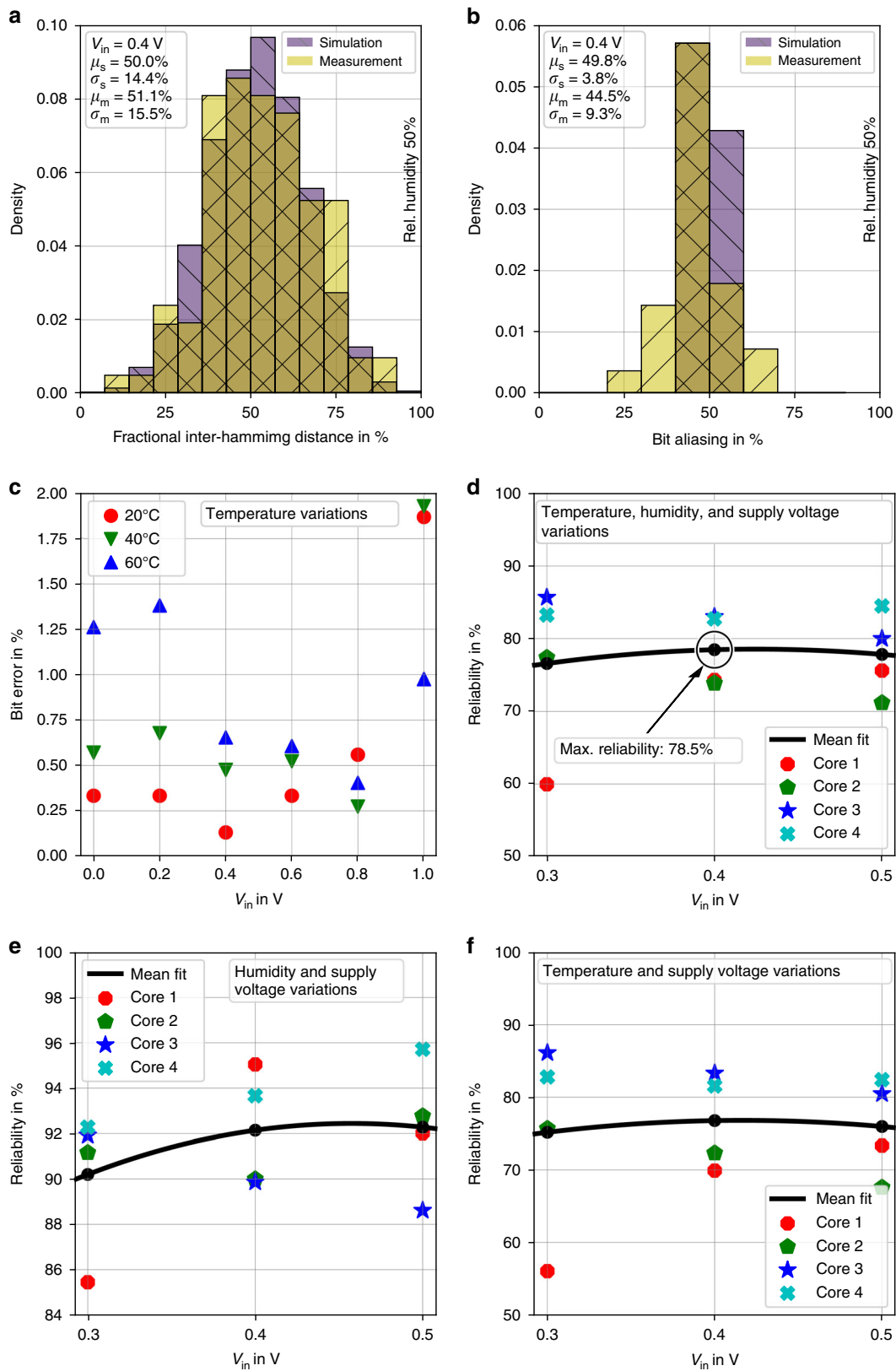
**Security metrics.** We evaluate the security metrics of our fabricated hybrid PUFs by using the uniqueness, bit aliasing, and reliability metrics proposed by Maiti et al.<sup>66</sup>. To investigate the uniqueness and reliability metrics further, we evaluate the bit errors in the PUF responses that occur over time. Detailed definitions of these security metrics can be found in the section Methods. In the following discussion, we apply various test cases for evaluation. These test cases compromise various temperatures with  $T_{amb} = \{20$  °C,  $40$  °C,  $60$  °C}, relative humidity conditions  $RH = \{45\%$ ,  $50\%$ ,  $55\%\}$  and different PUF core supply voltages  $VDD_{core} = \{0.9$  V,  $1.0$  V,  $1.1$  V}. A tabular overview of all resulting test case combinations can be found in the Supplementary Table 1. We consider changes in  $RH$  in our evaluations, because it impacts the functionality of the EGTs<sup>67</sup>. In the following, nominal conditions are defined at an ambient temperature of  $T_{amb} = 20$  °C, relative humidity  $RH = 50\%$ , and  $VDD_{core} = 1.0$  V, and used as a reference in security metrics evaluation. All measurements are repeated 20 times under controlled environmental conditions.

**Uniqueness.** The uniqueness metric shows the ability to differentiate PUF instances from each other. When applying the same challenge to different PUF instances, all responses are expected to be unique. The ideal value for the uniqueness metric is 50%, which means that all PUF responses are distinguishable. For our evaluation, we use 15 fabricated hybrid PUF core instances and operate them under nominal conditions. The inverter input-biasing voltage is set to  $V_{in} = 0.4$  V, as explored in our prior simulations, to be the best operating point for our PUF design<sup>65</sup>. The experimental results, together with the outcome of the simulations, are shown in Fig. 4a. The mean value and standard deviation of the uniqueness for the measured responses are  $\mu_m = 51.1\%$  and  $\sigma_m = 15.5\%$ , respectively. These values are in good agreement with both the simulation and the theoretical ideal value of the uniqueness metric, which is 50% and means that the PUF entities can be distinguished.

**Bit aliasing.** Bit aliasing (BA) will occur if various PUF instances produce the same response when stimulated with the same challenge. In this case, PUF authentication results in false positives, which degrades the operational capabilities of a PUF for use in applications such as secure device identification. In general, bit

aliasing is caused by internal biases, which lead to fixed bits that in the worst case never change their binary values. In general, the bit aliasing metric is associated with the uniqueness metric, as internal bitwise biases lead to multiple appearances of PUF responses for different challenges. As a result, the uniqueness of the CRPs degrades. To evaluate the bit aliasing metric, we utilize the same CRP data obtained from our uniqueness tests under nominal conditions. The inverter input-biasing voltage remains at the theoretically best operating point achieved at  $V_{in} = 0.4$  V<sup>65</sup>. Fig. 4b shows the distribution of the calculated bit aliasing values obtained separately for each response bit position. The mean value of the bit aliasing calculated using the measured PUF responses is  $\mu_m = 44.5\%$  with a standard deviation of  $\sigma_m = 9.3\%$ . The plot also proves the statistical coverage with the simulation results obtained in our prior work<sup>65</sup>. The experimentally obtained mean bit aliasing value of  $\mu_m = 44.5\%$  indicates a bias of the PUF responses towards logic '0'. However, the simulated theoretical bit aliasing for the presented hybrid PUF is  $\mu_s = 49.8\%$ . This shows that the bit aliasing can be improved to provide a close to true random bit sequence, suitable for cryptographic applications with the presented approach. The hybrid PUF's response entropy and its capabilities regarding identification is shown in Supplementary Fig. 4 and Supplementary Note 1.

**Bit errors and reliability.** To verify the robustness of our fabricated PUFs regarding their response stability, extensive testing under various controlled environmental conditions in a climatic chamber is executed. Standard reliability measures consider PUF responses generated at certain operating conditions and calculate their bitwise deviations to a fixed reference response, extracted under nominal conditions by utilizing the hamming distance (HD). The HD of two binary strings of equal length is the number of positions with different bit values. This evaluation procedure assumes that the response bits remain stable, if the operational conditions, such as ambient temperature, relative humidity, and supply voltage do not change over time/iterations. Therefore, noise-inflicted, time-dependent operational effects such as flipping bits are not further evaluated. However, this is not the case for circuits, whose internal characteristics might change slightly during operation because of non-ideal devices and other factors, such as aging. We measure in the ambient temperature range  $T_{amb} = \{20$  °C,  $40$  °C,  $60$  °C}, fixed relative humidity  $RH = 50\%$ , and inverter supply voltage  $VDD_{core} = 1.0$  V. For our evaluations, we increase the inverter input-biasing voltage in the range of  $V_{in} = \{0.0$  V, . . . ,  $1.0$  V} in  $0.2$  V steps. In Fig. 4c, the markers show the calculated mean bit error values. The plot shows that the bit errors strongly increase between  $V_{in} = (0.8$  V,  $1.0$  V). This effect appears because the PUF core inverters have already reached their logical low levels, where variations are small. Nonetheless, a single flipped bit in a 28-bit PUF response has a relative impact of  $\approx 3.6\%$ . As the measured relative bit errors of the 28-bit responses are  $\leq 2\%$ , in average there is less than one bit flip per response. In the following the reliability metric is discussed. In total, we operate four fabricated hybrid PUFs in a climatic chamber under all previously defined operating conditions. The inverter input-biasing voltage is consecutively set to the values  $V_{in} = \{0.3$  V,  $0.4$  V,  $0.5$  V}, in order to investigate the robustness around the best operating point determined in our prior simulations. We repeat the response extraction 20 times for each test case to achieve expressive statistics. Fig. 4d shows the reliability values for each of the tested PUF cores. The thick black line represents a second-degree regression model fit of the calculated mean reliability values that reaches its maximum of  $78.5\%$  at  $V_{in} = 0.4$  V. It should be noted that no



passivation layer for active component protection from environmental impacts was available at the time of fabrication. We expect the reliability values to be higher, once proper passivation is introduced for EGTs. To further investigate the reliability of our fabricated devices without the impact of changing

ambient temperatures, we create the plot shown in Fig. 4e. The mean reliability is above 90%, which indicates that values close to ideal can be achieved for our hybrid PUF. Furthermore, the impacts of altered relative humidity and inverter supply voltage  $VDD_{core}$  in the range of  $\pm 10\%$  are low, respectively.

**Fig. 4 Security metrics for the hybrid PUF.** **a** Uniqueness at  $V_{in} = 0.4$  V, visualized as histogram over the fractional inter-hamming distance for measurement and simulation data. The mean value of the simulated uniqueness is  $\mu_s = 50\%$  with a standard deviation of  $\sigma_s = 14.4\%$ . The measured uniqueness mean value is  $\mu_m = 51.1\%$  with a standard deviation of  $\sigma_m = 15.5\%$ . **b** Bit aliasing at  $V_{in} = 0.4$  V, visualized as histogram for measurement and simulation data. The mean value of the simulated bit aliasing is  $\mu_s = 49.8\%$  with a standard deviation of  $\sigma_s = 3.8\%$ . The measured mean value of the bit aliasing is  $\mu_m = 44.5\%$  with a standard deviation of  $\sigma_m = 9.3\%$ . **c** Bit errors for various ambient temperatures over  $V_{in} = \{0$  V, 0.2 V, . . . , 1.0 V $\}$  and test cases including temperature variations. Each data point displays the mean bit error value of 15 measurement samples. **d** Reliability metric including temperature, humidity, and supply voltage variations. **e** Reliability metric including humidity and voltage variations. **f** Reliability including temperature and supply voltage variations. **d–f** The mean value curve fit is done with a second-degree polynomial.

Fig. 4f shows that the reliability values are not heavily influenced by the tested relative humidity variations. This plot shows the reliability values for the four tested PUF cores with fixed relative humidity at 50%. The data points and curves are almost equal to Fig. 4d.

## Discussion

In conclusion, we have presented a hybrid PUF incorporating an inkjet-printed core circuit as an intrinsic source of entropy, integrated into a silicon-based CMOS system environment. The embedded system can generate 28-bit PUF responses and enables large-scale characterization as well as error tracking on both the digital and analog signal levels. In contrast to other PE-based PUF approaches, the hybrid PUF design presented here covers the full system level integration and breaks through the limitations of former device level-only implementations. Potential target applications in the security domain as well as benchmarking security metrics span the full range from conventional electronics to emerging technology fields, as PE, which enables low-cost manufacturing. Digitally controlled additive and solution-processed manufacturing techniques provide a high degree of flexibility in materials and unique intrinsic variation properties beneficial for fabricating PUF circuits. Flexible substrates in the future also enable new design patterns and integration capabilities, which pave the way for favorable applications in the IoT.

To investigate the security metrics of the hybrid PUF system and to assess the performance of our fabricated hybrid PUFs, we operated and characterized them in the controlled environment of a climatic chamber. In detail, we tested the hybrid PUFs under the impact of temperature, humidity, and supply voltage variations. With a mean uniqueness value of 51.1% and a mean bit aliasing value of 44.5%, the proposed hybrid PUFs generate unique responses that are distinguishable. The bit error evaluation shows that the PUF responses remain stable when regenerated successively at various ambient temperatures, with bit errors  $\leq 2\%$ . To show the robustness around the best operating point obtained from simulations in our prior work, we have shown reliability evaluation for the inverter input-biasing voltages  $V_{in} = \{0.3$  V, 0.4 V, 0.5 V $\}$ . The mean reliability value at the best operating point is at 78.5%. However, the reliability score can be expected to be higher once passivation to protect the EGTs from environmental influences has been introduced. Even with this figure of merit, it is still a major advance compared with the state-of-the-art research. We also investigated the reproducibility of the PUF challenge-response mechanism by calculating the bit errors that occur over time of operation.

Compared with other printed PUFs, our current system shows the largest PUF response bit-width and sufficient statistics to experimentally evaluate security metrics based on characterization results. The hybrid PUF presented here as a scalable, fully integrated system is a promising approach for future utilization in emerging security-related application fields such as identification, multi-factor authentication, and cryptographic key

generation. In addition, inkjet-printing technology enables a root of trust to be established in the PUF supply chain through decentralized manufacturing, which implies a substantial progress in providing trustworthy security primitives. Regarding future work in the area of printed PUFs several points need to be further investigated. As shown in our results, temperature stability needs to be improved to increase reliability and to enable bit-stable PUF responses.

## Methods

**Materials.** As a printing substrate, a commercially available 20 mm  $\times$  20 mm ITO glass (PGO CEC020S) with a layer thickness of 100 nm and a sheet resistance of  $R_{\square} = 20 \Omega$  is used. The materials used for the EGTs are as follows: Indium (III) nitrate hydrate (99.9% trace metal basis, MW = 300.83, Sigma-Aldrich), Glycerol (MW = 92.09 g mol<sup>-1</sup>, Merck KGaA), Dimethyl sulfoxide anhydrous (DMSO, 99.9%, MW = 78.13 g mol<sup>-1</sup>, Sigma-Aldrich) Propylene carbonate anhydrous (PC, 99.7%, MW = 102.09 g mol<sup>-1</sup>, Sigma-Aldrich), Poly(vinyl alcohol) hydrolysed (PVA, 98%, Sigma-Aldrich), Lithium perchlorate (LP, 99.99% trace metal basis, MW = 106.39 g mol<sup>-1</sup>, Sigma-Aldrich), Poly(3,4-ethylenedioxythiophene) polystyrene sulfonate (PEDOT:PSS, 3.0–4.0% in H<sub>2</sub>O, Sigma-Aldrich), Ethylene glycol anhydrous (99%, MW = 62.07 g mol<sup>-1</sup>, Sigma-Aldrich). The conductive adhesive, used to contact the core substrates to the adapter PCB is the two-component silver-filled adhesive Elecolit 325 by Panacol.

**Substrate preparation.** The substrates are structured via laser ablation with a Trumpf TruMicro 5000 picosecond laser with a laser wavelength of 1030 nm, set at 2.5 W average power.

**PUF fabrication.** For all printing operations, print heads of the type Fujitsu Dimatix DMC-11610 with an average droplet volume of 10 pl are used. The annealing of the substrate for the indium channel formation is done in a box furnace. The temperature is ramped up to 400 °C for 2 hours and is kept at this temperature level for further 2 hours. For cooling, the substrate is kept in the box furnace over night. It should be mentioned, that other possibilities for channel formation can be utilized, such as photonic or chemical curing, to lower processing temperature<sup>68,69</sup>.

**Ink preparation.** The inkjet-printable precursor ink for the indium-oxide channel is based on dissolved 0.05M (H<sub>2</sub>InN<sub>3</sub>O<sub>10</sub>) in double-deionized water and glycerol with a ratio of 4:1<sup>67</sup>. The solution is stirred for 2 hours and filtered with a 0.2  $\mu$ m polyvinylidene fluoride (PVDF) filter before usage. The CSPE is prepared with 1 wt % LiClO<sub>4</sub>, dissolved in 9 wt% PC and stirred for 2 h at ambient room temperature. In addition, 4.29 wt% PVA is dissolved in 85.71 wt% DMSO and stirred at 90 °C for 2 hours. The two solvents are mixed together and stirred until a clear solution is obtained<sup>67</sup>. Before inkjet-printing, the solution is filtered using a 0.2  $\mu$ m polytetrafluoroethylene filter. In the last step, 70 wt% PEDOT:PSS is dissolved in 30 wt % ethylene glycol and stirred for 2 hours, then filtered with a 0.2  $\mu$ m PVDF membrane before printing.

**Mounting inkjet-printed PUF core substrate onto adapter PCB.** A mounting process derived from flip-chip-technology has been selected for integrating the inkjet-printed PUF core onto the Si-based adapter PCB. The I/O terminals of the PUF core have to face the contact pads of the adapter PCB. The electrically conductive interconnection is realized with conductive adhesive. The integration process is based upon a mounting process for surface-mounted devices on low-temperature flexible substrates<sup>70</sup> that is adapted to the present application. The four axis cartesian handling platform applied for the mounting process is equipped with an application-specific carrier for the 20 mm  $\times$  20 mm PUF core glass substrates, a top camera to identify the fiducials on the PCB, a bottom camera to capture the fiducials on the PUF core glass substrates, a vacuum gripper, and a pressure time-controlled dispenser tool that is adapted to apply small amounts of conductive adhesive.

The silver-filled two-component adhesive Elecolit 325 from Panacol is applied as a conductive adhesive. A small amount of adhesive of 1 g per session is mixed



manually. In the present application, it has a pot time of  $\approx 90$  minutes and is used to contact four PUF cores with 28 I/O terminals each to the respective adapter PCBs. The area of the ITO-based conductive layer I/O terminals as well as the gold-coated contact pads on the adapter PCB are  $1\text{ mm} \times 1\text{ mm}$ , respectively. This dimensioning allows the positioning tolerances of the dispenser needle, the PCB and the PUF core glass substrates to be compensated. As examples, 56 contact points were evaluated based upon optical acquisition and image processing, showing that the diameters of the conductive adhesive in the final setup with the assembled glass substrate vary between  $\approx 570\text{ }\mu\text{m}$  and  $970\text{ }\mu\text{m}$ .

The integration process starts by manually placing the glass substrates with the printed PUF cores and one adapter PCB in the handling platform. The machine is initialised and an automated image processing-based routine is used to identify the exact position of the PCB. The conductive adhesive is then filled into the dispenser and the position of the dispenser needle is also identified by image processing. After a pre-dispensing step executed as a precondition for enabling reliable and reproducible adhesive flow, the adhesive is automatically dispensed onto the PCB contact pads. The first PUF core is automatically gripped and orientated into the correct mounting position. In order to orientate the glass substrate, the fiducials of the PUF core are acquired by the lower camera and identified based upon an image processing routine. After the glass PUF core has been mounted, the assembled device is manually removed and the next PCB is placed in the machine. The mounting process is then rerun with the next PUF core. Assembling one PUF core on the adapter PCB takes  $\sim 10$ – $15$  minutes. Final mechanical stability and electrical conductivity of the interconnection is achieved after 16 hours when curing at room temperature. Curing can be accelerated at elevated temperatures.

**Measurement setup and characterization.** A computer-driven automatic challenge-response readout and measurement system was custom-built for hybrid PUF characterization. The hybrid PUF platform design was split into the three functional units (a) microcontroller development board, (b) control logic, and (c) PUF core adapter, as further explained in Supplementary Fig. 8. and Supplementary Note 1. This setup enables the printed PUF core instances to be interchanged, as well as large-scale characterization. The custom-built software implementation allows challenges to the PUF to be applied automatically and the internal analog signals measured with a 12-bit MAX1237EUA ADC that lead to response bit generation. The microcontroller development board is connected to a personal computer (PC) and powered via USB. The control logic's components are powered using the microcontroller development board's internal 5 V and 3.3 V supply pins. For dynamic voltage generation of  $V_{in}$  and  $VDD_{core}$ , two internal 12-bit digital-to-analog converter channels of the microcontroller board are utilized. All our PUF response measurements were performed in a Weiss WK3 climatic chamber under controlled ambient temperature and humidity conditions. For PUF bit error and reliability measures, the ambient temperature was divided into three sections in the range of  $20\text{ }^{\circ}\text{C}$  to  $60\text{ }^{\circ}\text{C}$ . The relative humidity was varied in three sections from 45% and 55%.

### PUF security metrics

**Uniqueness.** The uniqueness metric measures the correlation of the PUF responses from different instances of the same type, by applying the same challenge. The lower the correlation, the greater the uniqueness. Ideally, all PUF responses should differ due to the random intrinsic variations, which implies a uniqueness value of 50%. For two different PUF instances  $i$  and  $j$ , each with  $L$ -bit responses  $R_i$  and  $R_j$ , the uniqueness for  $N$  PUFs in total is defined as:

$$U = \frac{2}{N(N-1)} \sum_{i=1}^{N-1} \sum_{j=i+1}^N \frac{\text{HD}(R_i, R_j)}{L} \times 100\% \quad (2)$$

**Bit aliasing.** The bit aliasing metric is a measure of the 0's and 1's distribution across different PUF entities of the same type. Ideally, both binary values occur with the same probability of 50%. If the  $l$ -th bit of the tested PUF responses has the same bit value across all PUF entities, the inter-HD of this bit will be zero. As a result, various PUFs may produce the same responses, which degrades the uniqueness and leads to false positives in device authentication. The bit aliasing for  $N$  PUF entities at the  $l$ -th bit position is calculated as:

$$\text{BA} = \frac{1}{N} \sum_{n=1}^N R_{n,l} \times 100\% \quad (3)$$

**Bit errors.** Bit errors are bit flips that may occur over time when generating the same PUF response multiple times. Owing to changing operating conditions, the regenerated challenge-response pairs might differ, which degrades both the uniqueness and the reliability scores. We calculate the bit errors ( $\text{BE}_n$ ) for PUF instance  $n$  by using the  $L$ -bit reference response  $R_{\text{ref},n}$  at nominal conditions, and the  $L$ -bit response  $R'_{n,w}$  regenerated  $W$ -times:

$$\text{BE}_n = \frac{1}{W} \sum_{w=1}^W \frac{\text{HD}(R_{\text{ref},n}, R'_{n,w})}{L} \times 100\% \quad (4)$$

**Reliability.** The reliability metric is a measure of the stability of PUF responses under the impact of varying operating conditions when applying the same challenge. The ideal value is 100%, which means that PUF responses are not affected by any environmental impacts such as noise, temperature, humidity, or unstable

voltage supply. The reliability  $\text{REL}_n$  for PUF instance  $n$  is calculated by using the  $L$ -bit reference response  $R_{\text{ref},n}$  measured at nominal conditions, and the  $L$ -bit test response  $R'_{n,t}$  for  $T$  different operating conditions:

$$\text{REL}_n = 100\% - \frac{1}{T} \sum_{t=1}^T \frac{\text{HD}(R_{\text{ref},n}, R'_{n,t})}{L} \times 100\% \quad (5)$$

### Data availability

The data sets generated and/or analyzed during the current study are available from the corresponding author on reasonable request.

### Code availability

The codes used for data analysis are available from the corresponding author on reasonable request.

Received: 22 April 2020; Accepted: 28 September 2020;

Published online: 02 November 2020

### References

- Atzori, L., Iera, A. & Morabito, G. The internet of things: a survey. *Comput. Netw.* **54**, 2787–2805 (2010).
- Sfar, A. R., Natalizio, E., Challal, Y. & Chtourou, Z. A roadmap for security challenges in the internet of things. *Digit. Commun. Netw.* **4**, 118–137 (2018).
- Wurm, J., Hoang, K., Arias, O., Sadeghi, A.-R. & Jin, Y. Security analysis on consumer and industrial IoT devices. in *2016 21st Asia and South Pacific Design Automation Conference*, 519–524 (IEEE, 2016).
- Lee, J.W. et al. A technique to build a secret key in integrated circuits for identification and authentication applications. in *2004 Symposium on VLSI Circuits. Digest of Technical Papers*, 176–179 (IEEE, 2004).
- Cortese, P.F., Gemmiti, F., Palazzi, B., Pizzonia, M. & Rimondini, M. Efficient and practical authentication of PUF-based RFID tags in supply chains. in *2010 IEEE International Conference on RFID-Technology and Applications*, 182–188 (IEEE, 2010).
- Mosenia, A. & Jha, N. K. A comprehensive study of security of internet-of-things. *IEEE Trans. Emerg. Top. Comput.* **5**, 586–602 (2016).
- Akmandor, A. O. & Jha, N. K. Smart health care: an edge-side computing perspective. *IEEE Consum. Electron. Mag.* **7**, 29–37 (2017).
- Zhang, M., Raghunathan, A. & Jha, N. K. Trustworthiness of medical devices and body area networks. *Proc. IEEE* **102**, 1174–1188 (2014).
- Diffie, W. & Hellman, M. New directions in cryptography. *IEEE Trans. Inf. Theory* **22**, 644–654 (1976).
- Merkle, R. C. Secure communications over insecure channels. *Commun. ACM* **21**, 294–299 (1978).
- National Institute of Standards and Technology Specification for the ADVANCED ENCRYPTION STANDARD (AES). *Fed. Inf. Process Stand. Publ.* **197** (2001).
- Gassend, B., Clarke, D., Van Dijk, M. & Devadas, S. Silicon physical random functions. in *Proceedings of the 9th ACM Conference on Computer and Communications Security*, 148–160 (ACM, 2002).
- Gassend, B., Lim, D., Clarke, D., Van Dijk, M. & Devadas, S. Identification and authentication of integrated circuits. *Concurr. Comput.* **16**, 1077–1098 (2004).
- Suh, G.E. & Devadas, S. Physical unclonable functions for device authentication and secret key generation. in *2007 44th ACM/IEEE Design Automation Conference*, 9–14 (ACM/IEEE, 2007).
- Herder, C., Yu, M.-D., Koushanfar, F. & Devadas, S. Physical unclonable functions and applications: a tutorial. *Proc. IEEE* **102**, 1126–1141 (2014).
- Pappu, R., Recht, B., Taylor, J. & Gershenfeld, N. Physical one-way functions. *Science* **297**, 2026–2030 (2002).
- Bhargava, M. *Reliable, Secure, Efficient Physical Unclonable Functions*, Pittsburgh Carnegie Mellon University (2013).
- Gao, Y., Al-Sarawi, S. F. & Abbott, D. Physical unclonable functions. *Nat. Electron.* **3**, 81–91 (2020).
- Chen, Q., Csaba, G., Lugli, P., Schlichtmann, U. & Rührmair, U. The bistable ring PUF: a new architecture for strong physical unclonable functions. in *2011 IEEE International Symposium on Hardware-Oriented Security and Trust*, 134–141 (IEEE, 2011).
- Garg, A. & Kim, T. Design of SRAM PUF with improved uniformity and reliability utilizing device aging effect. in *2014 IEEE International Symposium on Circuits and Systems*, 1941–1944 (IEEE, 2014).
- Kumar, S.S., Guajardo, J., Maes, R., Schrijen, G.-J. & Tuyls, P. The butterfly PUF protecting IP on every FPGA. in *2008 IEEE International Workshop on Hardware-Oriented Security and Trust*, 67–70 (IEEE, 2008).
- Morozov, S., Maiti, A. & Schaumont, P. An analysis of delay based PUF implementations on FPGA. in *Proceedings of the 6th International Symposium on Applied Reconfigurable Computing*, 382–387 (Springer, 2010).

23. Sehwag, V. & Saha, T. TV-PUF: a fast lightweight analog physical unclonable function. in *2016 IEEE International Symposium on Nanoelectronic and Information Systems*, 182–186 (IEEE, 2016).
24. Yang, K., Dong, Q., Blaauw, D. & Sylvester, D. 2-transistor amplifier-based physically unclonable function (PUF) with 1.67% native instability. in *2017 IEEE International Solid-State Circuits Conference*, 146–147 (IEEE, 2017).
25. Wali, A. et al. Biological physically unclonable function. *Commun. Phys.* **2**, 39 (2019).
26. Ogunseitan, O. A., Schoenung, J. M., Saphores, J.-D. M. & Shapiro, A. The electronics revolution: from e-wonderland to e-wasteland. *Science* **326**, 670–671 (2009).
27. Forti, V., Baldé, C.P., Kuehr, R. & Bel, G. *The Global E-waste Monitor 2020: Quantities, flows and the circular economy potential*. (United Nations University/United Nations Institute for Training and Research, International Telecommunication Union, and International Solid Waste Association, Bonn/Geneva/Rotterdam, 2020).
28. Ferreira, G. et al. Touch-interactive flexible sustainable energy harvester and self-powered smart card. *Adv. Funct. Mater.* **30**, 1908994 (2020).
29. Street, R. A. et al. From printed transistors to printed smart systems. *Proc. IEEE* **103**, 607–618 (2015).
30. Suganuma, K. *Introduction to Printed Electronics* (Springer, New York, 2014).
31. Chang, J. S., Facchetti, A. F. & Reuss, R. A circuits and systems perspective of organic/printed electronics: review, challenges, and contemporary and emerging design approaches. *IEEE J. Emerg. Sel. Top. Circuits Syst.* **7**, 7–26 (2017).
32. Barras, R. et al. Printable cellulose-based electroconductive composites for sensing elements in paper electronics. *Flex. Print. Electron.* **2**, 014006 (2017).
33. Hoeng, F., Denneulin, A. & Bras, J. Use of nanocellulose in printed electronics: a review. *Nanoscale* **8**, 13131–13154 (2016).
34. Liu, Y. et al. Inkjet-printed unclonable quantum dot fluorescent anti-counterfeiting labels with artificial intelligence authentication. *Nat. Commun.* **10**, 2409 (2019).
35. Horstmeyer, R., Judkewitz, B., Vellekoop, I. M., Assaworarith, S. & Yang, C. Physical key-protected one-time pad. *Sci. Rep.* **3**, 3543 (2013).
36. Kim, J. et al. Anti-counterfeit nanoscale fingerprints based on randomly distributed nanowires. *Nanotechnology* **25**, 155303 (2014).
37. Smith, A. F., Patton, P. & Skrabalak, S. E. Plasmonic nanoparticles as a physically unclonable function for responsive anti-counterfeit nanofingerprints. *Adv. Funct. Mater.* **26**, 1315–1321 (2016).
38. Mesaritis, C. et al. Physical unclonable function based on a multi-mode optical waveguide. *Sci. Rep.* **8**, 9653 (2018).
39. Carro-Temboury, M. R., Arppe, R., Vosch, T. & Sørensen, T. J. An optical authentication system based on imaging of excitation-selected lanthanide luminescence. *Sci. Adv.* **4**, e1701384 (2018).
40. Leem, J. W. et al. Edible unclonable functions. *Nat. Commun.* **11**, 1–11 (2020).
41. Gu, Y. et al. Gap-enhanced Raman tags for physically unclonable anticounterfeiting labels. *Nat. Commun.* **11**, 1–13 (2020).
42. Hu, Z. et al. Physically unclonable cryptographic primitives using self-assembled carbon nanotubes. *Nat. Nanotechnol.* **11**, 559 (2016).
43. Rahman, F., Shakya, B., Xu, X., Forte, D. & Tehranipoor, M. Security beyond CMOS: fundamentals, applications, and roadmap. *IEEE Trans. Integr. Syst.* **25**, 3420–3433 (2017).
44. Nili, H. et al. Hardware-intrinsic security primitives enabled by analogue state and nonlinear conductance variations in integrated memristors. *Nat. Electron.* **1**, 197 (2018).
45. Gao, Y., Ranasinghe, D. C., Al-Sarawi, S. F., Kavehei, O. & Abbott, D. Memristive crypto primitive for building highly secure physical unclonable functions. *Sci. Rep.* **5**, 12785 (2015).
46. Roberts, J. et al. Using quantum confinement to uniquely identify devices. *Sci. Rep.* **5**, 16456 (2015).
47. Kuribara, K. et al. Organic physically unclonable function on flexible substrate operable at 2V for IoT/IoE security applications. *Org. Electron.* **51**, 137–141 (2017).
48. Ogasahara, Y., Kuribara, K., Shintani, M. & Sato, T. Feasibility of a low-power, low-voltage complementary organic thin film transistor buskeeper physical unclonable function. *Jpn. J. Appl. Phys.* **58**, SBBG03 (2019).
49. Moon, D.-I. et al. Physically unclonable function by an all-printed carbon nanotube network. *ACS Appl. Electron. Mater.* **1**, 1162–1168 (2019).
50. Erozan, A. T. et al. Inkjet-printed EGFET-based physical unclonable function - design, evaluation, and fabrication. *IEEE Trans. Integr. Syst.* **26**, 2935–2946 (2018).
51. Noh, J. et al. Key issues with printed flexible thin film transistors and their application in disposable RF sensors. *Proc. IEEE* **103**, 554–566 (2015).
52. Bartzsch, M., Kempa, H., Otto, M., Huebler, A. & Zielke, D. Device and circuit simulation of printed polymer electronics. *Org. Electron.* **8**, 431–438 (2007).
53. Lau, P. H. et al. Fully printed, high performance carbon nanotube thin-film transistors on flexible substrates. *Nano Lett.* **13**, 3864–3869 (2013).
54. Sowade, E. et al. All-inkjet-printed thin-film transistors: manufacturing process reliability by root cause analysis. *Sci. Rep.* **6**, 33490 (2016).
55. Zhang, X., Ge, T. & Chang, J. S. Fully-additive printed electronics: transistor model, process variation and fundamental circuit designs. *Org. Electron.* **26**, 371–379 (2015).
56. Zhou, J., Ge, T., Ng, E. & Chang, J. S. Fully additive low-cost printed electronics with very low process variations. *IEEE Trans. Electron Devices* **63**, 793–799 (2015).
57. Marques, G. C. et al. Electrolyte-gated FETs based on oxide semiconductors: fabrication and modeling. *IEEE Trans. Electron Devices* **64**, 279–285 (2016).
58. Marques, G. C. et al. Digital power and performance analysis of inkjet printed ring oscillators based on electrolyte-gated oxide electronics. *Appl. Phys. Lett.* **111**, 102103 (2017).
59. Marques, G.C., Rasheed, F., Aghassi-Hagmann, J. & Tahoori, M.B. From silicon to printed electronics: a coherent modeling and design flow approach based on printed electrolyte gated FETs. in *2018 23rd Asia and South Pacific Design Automation Conference*, 658–663 (IEEE, 2018).
60. Feng, X. et al. Impact of intrinsic capacitances on the dynamic performance of printed transistor-based inorganic field effect transistors. *IEEE Trans. Electron Devices* **66**, 3365–3370 (2019).
61. Rasheed, F., Golanbari, M. S., Marques, G. C., Tahoori, M. B. & Aghassi-Hagmann, J. A smooth EKV-based DC model for accurate simulation of printed transistors and their process variations. *IEEE Trans. Electron Devices* **65**, 667–673 (2018).
62. Rasheed, F., Hefenbrock, M., Beigl, M., Tahoori, M. B. & Aghassi-Hagmann, J. Variability modeling for printed inorganic electrolyte-gated transistors and circuits. *IEEE Trans. Electron Devices* **66**, 146–152 (2018).
63. Garlapati, S. K. et al. Electrolyte-gated, high mobility inorganic oxide transistors from printed metal halides. *ACS Appl. Mater. Interfaces* **5**, 11498–11502 (2013).
64. Baldwin, D. F. & Higgins, L. M. *Electronic Packaging and Interconnection Handbook* (McGraw-Hill Handbooks, New York, 2007).
65. Zimmermann, L., Scholz, A., Tahoori, M. B., Aghassi-Hagmann, J. & Sikora, A. Design and evaluation of a printed analog-based differential physical unclonable function. *IEEE Trans. Integr. Syst.* **27**, 2498–2510 (2019).
66. Maiti, A., Gunreddy, V. & Schaumont, P. A systematic method to evaluate and compare the performance of physical unclonable functions. in *Embedded Systems Design with FPGAs*. (Springer, New York, 2013).
67. Marques, G. C. et al. Influence of humidity on the performance of composite polymer electrolyte-gated field-effect transistors and circuits. *IEEE Trans. Electron Devices* **66**, 2202–2207 (2019).
68. Garlapati, S. K. et al. High performance printed oxide field-effect transistors processed using photonic curing. *Nanotechnology* **29**, 235205 (2018).
69. Baby, T. T. et al. A general route toward complete room temperature processing of printed and high performance oxide electronics. *ACS Nano* **9**, 3075–3083 (2015).
70. Gengenbach, U. et al. Automated fabrication of multi-layer printed electronic circuits using a novel vector ink-jet printing process control and surface mounting of discrete components. *IFAC-Papers OnLine* **52**, 609–614 (2019).

## Acknowledgements

This work was supported by the Ministry of Science, Research, and Arts of the state of Baden-Wuerttemberg, Germany through the Modellierung, Entwurf, Realisierung und Automatisierung von gedruckter Elektronik und ihren Materialien (MERAGEM) Doctoral Program. J.A.-H. acknowledges support by the German Research Foundation (DFG) under Germany's Excellence Strategy via the Excellence Cluster 3D Matter Made to Order (EXC-2082/1 – 390761711). Special thanks go to Dr. Torsten Scherer and Vanessa Wollersens of the Karlsruhe Nano Micro Facility (KNMF) for providing the SEM images of our printed transistors (proposal ID: 2019-023028029).

## Author contributions

A.Sc., L.Z., A.Si., M.B.T., and J.A.-H., conceived the project. A.Sc. designed the circuits and fabricated the inkjet-printed devices. L.Z. designed the printed circuit boards hosting the control logic and implemented the software for automated large-scale characterization and security metric evaluation. U.G., L.K., and Z.C. developed the mounting process to integrate the printed into the silicon-based electronics. A.Sc. and L.Z. performed the electrical experiments. A.Sc., L.Z., and J.A.-H. analyzed the simulations and experimental results. J.A.-H. supervised the project. All authors have participated in analyzing the results and contributed to writing the manuscript.

## Funding

Open Access funding enabled and organized by Projekt DEAL.

## Competing interests

The authors declare no competing interests.

**Additional information**

**Supplementary information** is available for this paper at <https://doi.org/10.1038/s41467-020-19324-5>.

**Correspondence** and requests for materials should be addressed to J.A.-H.

**Peer review information** *Nature Communications* thanks Derek Abbott and Meng-Day Yu for their contribution to the peer review of this work. Peer reviewer reports are available.

**Reprints and permission information** is available at <http://www.nature.com/reprints>

**Publisher's note** Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.



**Open Access** This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this license, visit <http://creativecommons.org/licenses/by/4.0/>.

© The Author(s) 2020