VE-FIDES: Designing Trustworthy Supply Chains Using Innovative Fingerprinting Implementations

Bernhard Lippmann*, Joel Hatsch*, Stefan Seidl*, Detlef Houdeau*,
Niranjana Papagudi Subrahmanyam†, Daniel Schneider†, Malek Safieh†, Anne Passarelli†, Aliza Maftun†,
Michaela Brunner‡, Tim Music‡, Michael Pehl‡, Tauseef Siddiqui‡, Ralf Brederlow‡, Ulf Schlichtmann‡,
Bjoern Driemeyer§, Maurits Ortmanns§, Robert Hesselbarth¶, Matthias Hiller¶
*Infineon Technologies AG, Munich, Germany
†Siemens AG, Munich, Germany
‡Technical University of Munich, TUM School of Computation, Information and Technology, Munich, Germany
§University of Ulm, Ulm, Germany
¶Fraunhofer AISEC, Garching, Germany

***Abstract*—The project VE-FIDES will contribute with a solution based on an innovative multi-level fingerprinting approach to secure electronics supply chains against the threats of malicious modification, piracy, and counterfeiting. Hardware-fingerprints are derived from minuscule, unavoidable process variations using the technology of Physical Unclonable Functions (PUFs). The derived fingerprints are processed to a system fingerprint enabling unique identification, not only of single components but also on PCB level. With the proposed concept, we show how the system fingerprint can enhance the trustworthiness of the overall system. For this purpose, the complete system including tiny sensors, a Secure Element and its interface to the application is considered in VE-FIDES. New insights into methodologies to derive component and system fingerprints are gained. These techniques for the verification of system integrity are complemented by methods for preventing reverse engineering. Two application scenarios are in the focus of VE-FIDES: Industrial control systems and an automotive use case are considered, giving insights to a wide spectrum of requirements for products built from components provided by international supply chains.**

***Index Terms*—trust, security, PUF, electronics supply chain, counterfeit detection**

I. Introduction

Supply chains of electronic goods consist of a large number of steps from the design of the chip over manufacturing, packaging, printed circuit board (PCB) manufacturing to test, integration, and shipping. As these steps are typically performed by many different actors, unintentional vulnerabilities, intended backdoors, counterfeits, defective parts, cheap duplicates, and gray market issues can affect the electronic goods along the supply chain [1]. Additionally, they can bring huge monetary losses to the businesses of trustworthy actors [2]. In parallel, improvements in reverse engineering techniques are making it easier for attackers to steal intellectual property. The present global semiconductor chip shortage crisis and the high demand in electronics that emerged during the COVID-19 pandemic is increasing the number of counterfeit electronic goods in the market [2]. This enhances the need for trust in electronic goods even further.

This work was partly funded by the project VE-FIDES (Knowhow-Schutz und Identifizierbarkeit von Elektronikkomponenten für vertrauenswürdige Produktionsketten), and platform project Velektronik (Velektronik – trustworthy electronics). VE-FIDES and Velektronik receive funding by the German Federal Ministry of Education and Research (grant no. 16ME0257 and grant no. 16ME0217). Project stage: Intermediate

In order to address these issues, we utilize PUFs [3], which enable derivation of unique hardware-based secrets of electronic goods, to protect neuralgic points of the supply chain. We present an innovative multi-level fingerprinting approach, where several component fingerprints are processed to a system fingerprint. In particular, we consider an approach with a Secure Element that utilizes this system fingerprint to enable counterfeit detection [4]. This VE-FIDES approach aims to enhance the trustworthiness of supply chains for a variety of applications, such as industrial control systems and automotive use cases.

The remainder of this paper is organized as follows: Section II presents relevant state-of-the-art and describes the VE-FIDES project vision and structure. Section III describes our approaches for enhancing trust in an electronic system. In Section IV, we present our results. Section V outlines future work and in section VI, we present a conclusion.

II. State of the Art and VE-FIDES Project Organisation

Over the last two decades, PUFs matured from first research papers to a technology that is deployed in selected commercial products. In particular, silicon PUFs such as the SRAM, ring oscillator or arbiter PUF which evaluate manufacturing variation inside CMOS circuits [3] on chip level, are utilized. However, by evaluating only manufacturing variation on the die they only allow to address limited supply chain aspects. At the other end of the scale, envelopes can protect entire embedded systems from physical tampering under a high technical effort [5], but do not address the authenticity of the components *before* the envelope is applied.

However these technologies fall short to address a wider range of supply chain issues such as vulnerabilites, backdoors and gray-markets [1]. So far, mostly analysis and fingerprinting techniques, e.g. discussed in [6], were incorporated to address them.

978-3-9819263-7-8/DATE23/© 2023 EDAA

Therefore, current technologies lack an end-to-end approach that allows to integrate different types of electronic components along the supply chain, link them and evaluate them in a stand-alone fashion on the device.

A. VE-FIDES Project Vision and Targets

To establish trust in global markets and given global supply chains, authentication of every product as well as every component in a system should be ensured not only during manufacturing but over the whole life cycle. VE-FIDES focuses on systems like electronic control boards with a broad spectrum of different components from lightweight sensors to complex microcontrollers. VE-FIDES aims to protect such systems against threats in the supply chain discussed above. To achieve this goal, we equip critical and costly components with individual fingerprints. We identified the PUF technology as a suitable solution, which we develop further to fit the needs for system fingerprinting even better. Therefore, VE-FIDES not only integrates PUFs into critical components but also investigates how the intrinsic variations of analog sensors could be used directly for identification and fingerprinting without requiring a dedicated PUF as part of such sensors, thereby raising challenging research questions regarding the levels of reliability and trustworthiness achievable with this approach. Across different manufacturing steps, VE-FIDES derives a unique system fingerprint from these components. The fingerprint allows for attesting the integrity of a system with its integrated components, to detect gray market components and also physical tampering. To ultimately prevent highly sophisticated counterfeiting or tampering techniques, reverse engineering techniques come into play: while hardware obfuscation hinders IP theft, physical verification aims to increase trust by comparing a physical design to a golden model for finding unexpected deviations. By answering the different research questions, VE-FIDES helps to improve the trustworthiness of systems built with electronic components from a global supply chain.

B. VE-FIDES Project Structure

As shown in Figure 1, the project VE-FIDES targets fingerprinting on a system level. Work package 1 is dedicated to the fundamental analysis of trust and the requirements to implement solutions into products. Process variation during the chip production process are used for the generation of fingerprints on a chip level and are evaluated in work package 2. In work package 3, variations during the PCB production process as well as the evaluation of individual electrical properties of components and sensors are used for fingerprinting on a board level and of small devices without specific security features. Finally, system trust over the product life time covering production, maintenance, and operation requires the easy to use integration of a system fingerprint into the software stack. The planned demonstrator in work package 4 will combine the individual contributions.

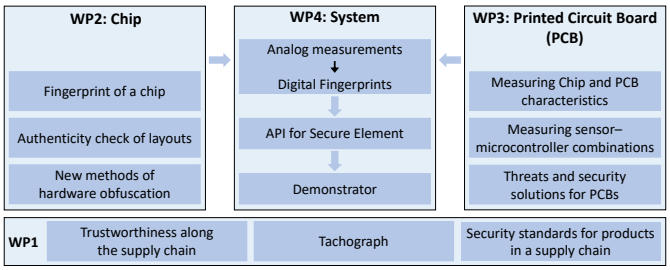

Fig. 1. VE-FIDES work package structure.

III. Methods

A. System Level Fingerprinting and Counterfeit Detection

Industrial control systems consist of complex compositions of a large number of electronic components. In order to enhance the trustworthiness for such systems, our concept validates fingerprints of multiple components, in particular critical and costly components. For this purpose, our multi-level fingerprinting approach combines PUF-based raw fingerprints of components into one representative system fingerprint. Raw fingerprints have diverse characteristics. Some sensors might provide only a few noisy bits while more complex devices like microcontrollers might provide the capability to run complete cryptographic protocols. These different kinds of fingerprints require different processing steps, and the fingerprinting system must provide the capability to handle all of them. Therefore, the technique to derive a fingerprint must be carefully selected and an elaborate concept for fingerprint derivation is needed.

In our concept, a Secure Element (SE) serves as the root of trust collecting and combining raw fingerprints. It allows fingerprint verification at runtime as well as modifying or replacing components by authorized parties. In order to simplify the use of different SEs and to orchestrate these, the Generic Trust Anchor API (GTA API) [7] will be used in our implementation. Our concept is depicted in Fig. 2 and it is described in the following.

1) Generation of Reference Fingerprint: During production, the manufacturer builds a system, e.g., an industrial device, in a trusted environment by integrating components, including a SE, from different suppliers. The manufacturer starts a user application on the device to trigger the measurement application on the SE via the GTA API. The SE records fingerprints of components, and generates the reference fingerprint. The integrity of the stored reference fingerprint is ensured by the SE. This enables offline verification on the device. Only the manufacturer should be able to trigger generation or modification of the reference fingerprint, which is realized with authentication measures. In order to enable authorized component replacement by the manufacturer, also a public key corresponding to the manufacturer's signing key is provisioned into the SE.

2) Establishing Trust and Fingerprint Verification: The process of fingerprint verification is visualized in Fig. 2. After procurement, the customer obtains the device attestation certificate (purple) and the manufacturer certificate (green). By verifying these certificates against public keys, secured in the SE, the

customer can anchor trust in the device. During operation, the fingerprint of the device is re-measured by the SE and compared to the stored reference fingerprint for offline verification of integrity. We refer to this process as the device self-check, where verification is triggered internally and periodically within the device.

Additionally, an attestation request to check the device integrity can be triggered by a remote backend, as shown in Fig. 2. In this case, the SE prepares and sends a signed response in the form of an attestation report, using the attestation key (purple). The customer backend verifies the signature on the report and acknowledges the integrity of the device.

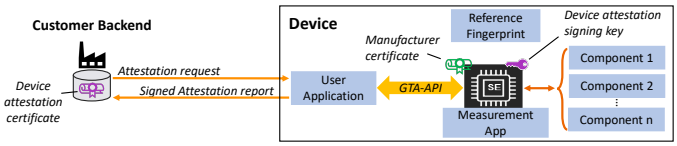

Fig. 2. Fingerprint verification

3) Component Repair and Replacement: If a component needs replacement, the entire reference fingerprint is recomputed. For this purpose, the manufacturer sends a signed fingerprint generation request to the SE. The SE verifies the signature with the securely stored public key (green certificate) and authenticates the manufacturer to generate a new reference value.

B. Sensor- and PCB-Manufacturing-Variation-Based PUF Design

Automotive and industrial applications often require sensors to be a critical part of such infrastructure which drives the need for securing also the sensor itself. To fingerprint sensors we are looking for unique and random features within each sensor by exploring the inherent randomness and deviations originating from silicon manufacturing variations. With such goal in mind in chapter 4 we analyze Hall sensors as available on the market. More generally, typical sensor architectures are designed to counter these random effects. While such design techniques are beneficial to stabilize the sensor output with respect to temperature, supply voltage and aging changes, initial datasheet studies and measurements have clearly shown that it is almost impossible to get lifetime and environmentally stable, but random information from the sensor outputs because of them. Access to raw offset characterization data used for internal sensor calibration in test modes, however, is more promising for this purpose and an example from VE-FIDES will be shown in Section IV-B using a Hall sensor test mode.

In addition to such PUF structures, data converters can also be used for fingerprint generation. This has the advantage of gaining identification and trustworthiness without realizing dedicated fingerprint circuitry. One approach, which is pursued in VE-FIDES is to use unique data converters' non-idealities as source of entropy. Analog-to-Digital converter (ADC) based fingerprints were found to be particularly suitable for this purpose, since ADCs have well measurable non-idealitites, ADCs are widely used, and the suitability of ADCs for fingerprint generation over varying environmental influences has already been demonstrated [8].

Existing components or interfaces can also be used for PCB identification [9], [10]. The common weakness of most PCB-based methods is the resilience to varying environmental influences and noise, which plays a subordinate role in the state of the art. In VE-FIDES, special focus is therefore on the extraction of robust PCB fingerprints.

C. Digitally Dominated PUF Design

Digitally dominated PUF designs, as opposed to PUF structures that require analog circuits to operate (like the ADC PUF mentioned in Section III-B), are based on regular logic devices, which have the advantage that they can be implemented in any foundry technology without need for special process steps.

Examples of digital implementations are arbiter PUFs that compare signal propagation along (theoretically) identical delay lines, or ring-oscillator PUFs that compare the oscillation frequencies of two identical ring oscillators. While the area footprint is typically much smaller, the downside is that foundries focus on getting semiconductor devices manufactured with the lowest possible variations, which is counter-productive for a PUF implementation.

Hence PUF circuitry needs to be designed in such a way that it amplifies the small remaining fluctuations in device characteristics. Furthermore, the circuits shall be stable and provide identical output over a broad temperature and voltage range, which is typical for industrial and automotive applications, but makes the circuit implementation more difficult.

Besides temperature and voltage, many other environmental factors should be considered that can have a negative influence on the stability of the bit generation, like electromagnetic fields, power supply ripples, local IR drop, humidity, etc.

Realistically, 100%-perfectly stable circuitry cannot be designed at acceptable costs of development and manufacturing. Error Correction Codes (ECCs) are used to cope with a certain number of unstable bits. Designs must then balance the overhead in the PUF circuitry vs. the implementation of ECC logic to find the best economical compromise. Finally, the aging of the circuitry over lifetime has to be taken into consideration, too. One approach is to accept a small degradation of the bit error rate and use error correction to compensate the aging. Another one is to build and operate the circuitry in modes where aging is prevented or where the aging leads to the circuit becoming more stable.

D. Design for Test (DfT) Aspects

For productive use, an important topic is the aspect of DfT. For security reasons, PUFs are typically built in such a way that their data is protected from external access. Furthermore, their data is expected to be as well random as also chip-individual, which means that there actually is no reference value that it can be compared against. New methods must therefore be considered in order to perform hardware validation after fabrication. New metrics must be investigated to qualify the cryptographical properties of the generated bits.

For some of the considerations, methodology can be derived from Random Number Generators (RNGs), which partly have similar requirements and issues. However, while RNGs are just generating "infinite" bitstreams of data, PUFs must as well combine randomness and repeatability, which both must be assessed. Furthermore, the results obtained by many RNG tests strongly depend on the arrangement of data when applying tests to them. As a consequence, results from tests not dedicated to PUFs must be taken with care.

E. Hardware Obfuscation

Error correction is an important element of many fingerprinting methods, such as digitally dominated PUF designs, see Section III-C. ECCs usually come with a control logic which can be an interesting target for attackers. To prevent an end user from performing reverse engineering attacks, finite state machine (FSM) obfuscation can be applied [11], [12]. In VEFIDES, we developed a new FSM obfuscation method, timing camouflage enabled FSM obfuscation, and presented a beneficial combination with logic locking [13]. Timing camouflage introduces wave-pipelining paths, i.e. paths with two signal waves at the same time, by removing flip-flops without changing the original functionality [14]. This approach increases the complexity of physical reverse engineering, likely resulting in a gate-level netlist with missing flip-flops. We developed two FSM redesign approaches to apply timing camouflage also on flip-flops of an FSM, i.e. state flip-flops. By removing an appropriately selected state flip-flop with timing camouflage, the FSM extraction can only rely on the remaining state flip-flops, leading to an obfuscated extracted FSM. Additionally, a correct circuit unrolling is practically impossible. This reduces the probability of a successful sequential SAT-based attack which targets the extraction of the correct locking key in sequential circuits [15]. Summarizing, this obfuscation again shows the potential of combining different techniques, like FSM obfuscation, camouflaging, and logic locking.

F. Physical Verification of Chip Individual Features

Physical inspection can be applied to verify sample originality during the product life time. The physical verification workflow ends with a comparison of the recovered design M against the golden reference design G. On a chip level the technology verification contains the individual comparisons of measured layer thicknesses and minimal structure width. The layout comparison evaluates the difference between the physical layout and the available reference layout. The method of comparing recovered layouts and manufacturing parameters can be extended to the process development kit and on the PCB level [16] and described with the similarity $S(M,G)$ using dedicated comparators as shown in Equation (1).

$$S(M,G) = \frac{1}{N}\big(PackCom(M,G) + DFCom(M,G) + TFCom(M,G) + PolyCom(M,G)\big) \quad (1)$$

Each comparator (package, process design kit, technology, and polygon layout) consists of a number N_i of single feature comparisons and will return the measured correlation in a range 0..1. For normalising the complete similarity function $S(M,G)$ we need to add the factor $\frac{1}{N}$ with $N = \sum_i N_i$. The generated trust $T(M,G)$ through a physical inspection is described as a sum of the weighted comparator results, with CT giving the number of used comparator types.

$$T(M,G) = \frac{1}{N}\Big(\sum_{j=0}^{CT}\sum_{i=0}^{N_j} \underbrace{w_j(i)}_{weights} \cdot Comparator_{(i,j)}(M_i, G_i)\Big)$$

The computation of numerical values for the weights, representing the impact of a single comparison, is far from trivial. We will connect our approach to already existing frameworks like CRESS [17] and CVSS [18]. The final challenge exists in the analysis of chip individual features and analysis tasks where no adequate and effective tool and method is known as of today. A solution path could be based on integrating electrical analysis in a combination with layout recovery and increasing the recovery yield and accuracy in dedicated local areas containing chip individual features.

IV. RESULTS

A. ADC-Based Fingerprints

ADC-based fingerprints PUFs render the unique non-idealitites of Data Converters as source of entropy. The general extraction-flow is presented in Fig. 3 by using ADC non-idealities for fingerprint generation. The non-idealities (static or dynamic) of an already existing ADC are determined and post processed, resulting in the ADC fingerprint. Former work has shown the suitability of static ADC/DAC errors given by the differential non-ideality (DNL) converted into ADC fingerprints [8], [19]. The stability of the generated fingerprints over noise, temperature and supply voltage variation is investigated in great detail in [8], [19] and motivates further investigations using ADC as source of entropy for fingerprinting. To further increase the uniqueness of given ADC fingerprints, longer fingerprints are required. The approach taken in VEFIDES tries to use dynamic ADC errors as an additional source for ADC fingerprints. For this, a dynamic ADC error estimation technique is required. It has been shown in [20] that one can determine static and dynamic ADC non-idealities, given by Intersymbol-Interference (ISI), simultaneously with reduced complexity compared to the state of the art. In addition, it was shown in [21] that the determined ISI errors are an excellent source for the randomness of a PUF. With the help of linear error correction polynomials as sole post processing, the PUF could be stabilised over variation of supply voltage and temperature - with a higher yield of bits per ADC error compared to the state of the art.

B. Hall Sensor-Based Fingerprints

For sensors, concepts similar to the ADC-based fingerprints can be used. To study different environmental conditions on the stability of the sensor offsets we were using a test mode of a 3D Hall sensor to measure the Hall plate's offset. Figure 4

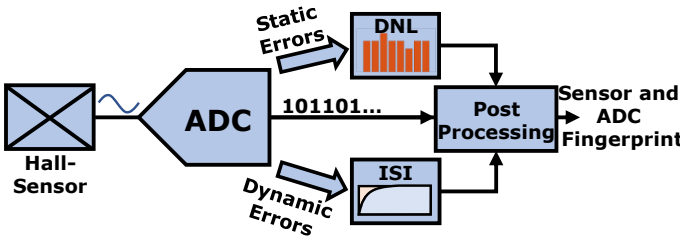

Fig. 3. Extraction flow of ADC and Hall-Sensor non-idealities towards fingerprints.

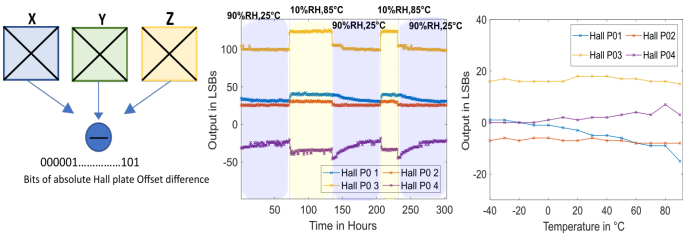

Fig. 4. Concept of differential X-Z offset for 4 sensors (left), measurement of humidity (center) and temperature (right) effect on sensor offset values.

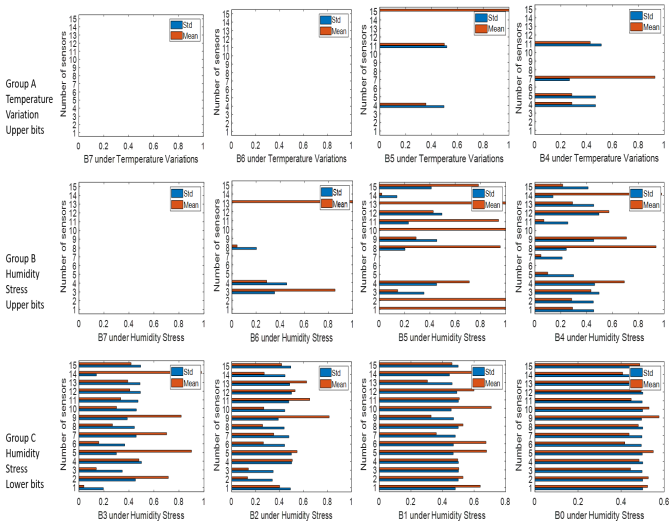

Fig. 5. Reliability analysis: standard deviation and mean of bits for differential X-Z offset with humidity and temperature effects, for 15 sensors.

shows the difference in the offset of two plates (here x- and z-direction) over temperature and in a humidity experiment for 4 different sensors with digital output. By building this difference first order temperature and humidity are canceled. The remaining offset shows different effects for these two parameters: from the graphs it can be seen, that while temperature effects cause fast offset changes, humidity effects take longer time to settle - making them more difficult to correct. In Figure 5, a more detailed analysis of the stability of those values shows 15 different sensors on a bit level: For the lowest bits (B0 and B1) noise causes unreliability. For the first 4 bits (B0-B3) also temperature drifts effects the quality. But for the more significant bits (up to B5) cases of humidity drift related flips make these bits not fully reliable. Therefore we have to use digital correction techniques as indicated in Fig. 3 and which are further discussed in the next section. Finally, based on such characterization data it is clear, that without design effort we can only get a small number of unique, reliable bits from the sensor's entropy to get a good fingerprint here.

C. Fingerprinting Solutions

Three algorithms satisfying the requirements and constraints for VE-FIDES have been analyzed for their applicability to derive system fingerprints from raw fingerprints.

1) Direct Correlation: This denotes the process of comparing noisy raw fingerprint with a reference stored during an enrollment process. Reference fingerprints are captured and stored in a list, from which a system fingerprint can be derived. During verification, the list is traversed and each reference is compared to the corresponding raw fingerprint newly measured for verification. Components are evaluated as authentic if the correlation between reference and measurement reaches a threshold defined by the noise level to be accepted. This approach is favorable if few components are to be verified in a system or if the fingerprint size does not allow for using ECCs. Please note, that – due to measurement noise – direct correlation in the described form does not allow for associating additional metadata, like enrollment time or manufacturer, through hashing.

2) Bloom Filter: Bloom filters are probabilistic data structures allowing for efficient membership testing. Applied to our scenario, the filter's underlying data structure is directly usable as fingerprint. The approach features distinct advantages and disadvantages: Whilst the basic filter construction does not allow exchanging elements they are easily extended to fit this requirement of VE-FIDES [22]. Bloom filters allow for efficient evaluation of large amounts of component fingerprints. However, due to their probabilistic nature, false positive and negative rates need to be fixed. Error correction is needed to allow for reliable reproduction of a Bloom filter based fingerprint. The association of metadata with raw fingerprints is hard to achieve.

3) Hash Tree: Hash trees are widely used to verify integrity of data structures. In VE-FIDES, the top hash poses as system fingerprint. Nodes in the hash tree reflect critical components. The nesting level corresponds to the hierarchical position in subsystems. Hash trees allow for efficient binding of reference fingerprints with associated metadata. Associating helper data, needed to correct measurements for verification, with fingerprint is possible and prevents helper data manipulation attacks. On the down side, error correction is needed in this approach to allow for hashing fingerprints. By constructing the hash tree and computing each node's value not only during enrollment but also for verification, permanently storing reference fingerprints can be avoided.

Overall, our evaluation has shown that for systems as in VE-FIDES hash trees are the best fit. This is mainly due to their flexibility and capability to associate data with individual components.

D. Error Correction

For most fingerprinting systems error correction is needed. Methods like fuzzy extraction are used to map a random raw fingerprint to a codeword that can be corrected. This step requires helper data which is typically large in size. For an efficient design, recent papers suggest using polar codes. However, the feasibility of implementing polar codes with sufficiently low hardware overhead was not clear. In VE-FIDES we developed – together with partners – a hardware implementation of a corresponding decoder [23]. The inputs to the decoder are log-likelihood ratios, derivable for all PUFs providing digitized analog values as an output. The results show that a corresponding decoder can be implemented with twice the area of competing codes but saves for the considered use case approx. 57% of helper data bits for fuzzy extraction. This makes polar codes an interesting candidate for future research in VE-FIDES, since in case of a large fingerprinting system, helper data need to be stored for many raw fingerprints.

V. Demonstrator and Future Work

A multi-layered security solution at all stages of the value chain allows not only to trust the supply chain of digital elements, such as semiconductor-chips, but also the final electronic product and system. The previous chapters have shown the strategy of VE-FIDES to root the trust in hardware. First results summarized in this work indicate the feasibility of our approach and highlight first findings. Measurement of trust through physical verification has been proposed, as well. However, additional research will be carried out in VE-FIDES. For instance, protecting transmissions between the fingerprinted component and the SE is an issue to be solved. Future research may also asses the increase on trust through the individual measures introduced in VE-FIDES.

To show the feasibility of VE-FIDES's concepts and improvements, we aim to integrate these into a modular demonstration system including a top level device, a Secure Element, sensors and other components to show-case their interactions and capabilities. The modularity allows us to demonstrate threats as well as newly contributed mitigation capabilities in different situations throughout the lifetime of the system including assembly steps along the supply chain as well as the (un-)authorized replacement of subsystems after deployment in the field.

From a supply chain perspective the demonstration will represent a wide range of applications, e.g., from industrial, automotive, automation, aerospace or medical domains. During hypothetical manufacturing, components as well as multiple PCBs are incrementally added to the demonstration system. Before handing off to the next stop in the supply chain, the system is powered on and the new components are attested and integrated. In this manner, the system fingerprint is gradually built and allows to attest the secured integration of different components. It finally allows to verify that *only* the expected, authentic components are part of the assembled product.

VI. Conclusion

Trusted supply chain is more and more needed for products, which are built with digital elements. Electronic products, such as sensors, microcontrollers or communication modules for example in IoT- IIoT-, IoTT- and IoMT-products are often characterized by supply chains around the globe. Electronic products allow intrinsic security technologies to verify the origin of the product and the production facility. The approach is also usable for spare parts and the repair process along the lifecycle of the product. This article reflects some technologies and shows some use cases.

References

[1] J. Heyszl, G. Sigl, A. Seelos-Zankl, and M. Hiller, "Referenzpapier Vertrauenswürdige Elektronik," 2022.

[2] EUIPO and Europol, "Intellectual Property Crime Threat Assessment 2022," 2022.

[3] C. Herder, M.-D. Yu, F. Koushanfar, and S. Devadas, "Physical unclonable functions and applications: A tutorial," *Proceedings of the IEEE*, vol. 102, no. 8, 2014.

[4] J. Boyens *et al.*, "Validating the Integrity of Computing Devices," National Institute of Standards and Technology, Tech. Rep., 2022.

[5] V. Immler *et al.*, "B-TREPID: Batteryless tamper-resistant envelope with a PUF and integrity detection," in *2018 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*, IEEE, 2018.

[6] N. Asadizanjani, M. T. Rahman, and M. Tehranipoor, *Physical Assurance*. Springer, CHAM, 2021.

[7] *ISO/IEC TS 30168 ED1, Internet of Things (IoT) - Generic Trust Anchor Application Programming Interface for Industrial IoT Devices, JTC1-SC41/314/CD (COMMITTEE DRAFT)*, Oct. 2022.

[8] A. Herkle, J. Becker, and M. Ortmanns, "Exploiting Weak PUFs From Data Converter Nonlinearity—E.g., A Multibit CT $\Delta\Sigma$ Modulator," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 63, no. 7, 2016.

[9] A. Hennessy, Y. Zheng, and S. Bhunia, "JTAG-based robust PCB authentication for protection against counterfeiting attacks," in *2016 21st Asia and South Pacific Design Automation Conference (ASP-DAC)*, 2016.

[10] J. R. Hamlet, M. T. Martin, and N. J. Edwards, "Unique signatures from printed circuit board design patterns and surface mount passives," in *2017 International Carnahan Conference on Security Technology (ICCST)*, 2017.

[11] K. Juretus and I. Savidis, "Time Domain Sequential Locking for Increased Security," in *2018 IEEE International Symposium on Circuits and Systems (ISCAS)*, IEEE, 2018.

[12] M. Hoffmann and C. Paar, "Doppelganger Obfuscation — Exploring the Defensive and Offensive Aspects of Hardware Camouflaging," *IACR Transactions on Cryptographic Hardware and Embedded Systems*, vol. 2021, no. 1, Dec. 2020.

[13] M. Brunner *et al.*, "Timing Camouflage Enabled State Machine Obfuscation," in *2022 IEEE Physical Assurance and Inspection of Electronics (PAINE)*, 2022.

[14] G. L. Zhang *et al.*, "TimingCamouflage+: Netlist Security Enhancement With Unconventional Timing," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 39, no. 12, 2020.

[15] K. Shamsi, M. Li, D. Z. Pan, and Y. Jin, "KC2: Key-Condition Crunching for Fast Sequential Circuit Deobfuscation," in *Design, Automation & Test in Europe Conference & Exhibition (DATE)*, IEEE, 2019.

[16] B. Lippmann, M. Ludwig, and H. Gieser, "5. Generating Trust in Hardware through Physical Inspection," EAI Workshop Milan 2022, Sep. 2022.

[17] M. Ludwig, A. Hepp, M. Brunner, and J. Baehr, "CRESS: Framework for Vulnerability Assessment of Attack Scenarios in Hardware Reverse Engineering," in *2021 IEEE Physical Assurance and Inspection of Electronics (PAINE)*, (Dec. 2021), preprint: https://dx.doi.org/10.36227/techrxiv.16964857, Washington, DC, USA: IEEE, Dec. 2021.

[18] FIRST.Org, Inc. "Common Vulnerability Scoring System version 3.1: Specification Document." (Aug. 21, 2022), https://www.first.org/cvss/specification-document.

[19] M. Danesh *et al.*, "Unified Analog PUF and TRNG Based on Current-Steering DAC and VCO," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 28, no. 11, 2020.

[20] B. Driemeyer, J. Spiess, J. G. Kauffman, and M. Ortmanns, "Complexity Reduced LUT-Based DAC Correction in Continuous-Time Delta-Sigma Modulators," in *2022 IEEE International Symposium on Circuits and Systems (ISCAS)*, 2022.

[21] B. Driemeyer *et al.*, "PUF-Entropy Extraction of DAC Intersymbol-Interference using Continuous-Time Delta-Sigma ADCs," in *2022 29th IEEE International Conference on Electronics, Circuits and Systems (ICECS)*, 2022.

[22] S. Tarkoma, C. E. Rothenberg, and E. Lagerspetz, "Theory and Practice of Bloom Filters for Distributed Systems," *IEEE Communications Surveys & Tutorials*, vol. 14, no. 1, 2012.

[23] C. Kestel, C. Frisch, M. Pehl, and N. Wehn, "Towards More Secure PUF Applications: A Low-Area Polar Decoder Implementation," in *2022 IEEE 35th International System-on-Chip Conference (SOCC)*, 2022.