Securing the Internet of Things from the Bottom Up Using Physical Unclonable Functions

Leah Lathrop*, Simon Liebl*, Ulrich Raithel†, Matthias Söllner* and Andreas Aßmuth*

*Technical University of Applied Sciences OTH Amberg-Weiden, Amberg, Germany,
Email: {l.lathrop | s.liebl | m.soellner | a.assmuth}@oth-aw.de
†SIPOS Aktorik GmbH, Altdorf, Germany, Email: ulrich.raithel@sipos.de

***Abstract*—Cyberattacks that target hardware are becoming increasingly prevalent. These include probing attacks that aim at physically extracting sensitive information including cryptographic keys from non-volatile memory. Internet of Things devices that communicate with the Cloud are susceptible to such attacks. Therefore, the integrity of data and ability to authenticate devices are threatened. Physical Unclonable Functions (PUFs) offer a countermeasure to such attacks. A market analysis of products containing PUFs was carried out. An extract of the market analysis and the inferences that were drawn from it is provided. The analysis showed that although many different types of PUFs have been integrated into a variety of devices, most of them are still used in very rudimentary ways.**

Keywords–Cloud; Physical Unclonable Function; Critical Infrastructure; Internet of Things; Hardware Security.

I. INTRODUCTION

The Internet of Things (IoT) has engulfed many aspects of industrial sectors and the lives of private individuals. The number of actively connected IoT devices is forecast to grow to 22 billion by 2025 [1]. The Industrial IoT (IIoT) is the subset of the IoT that is used in industrial applications, e.g., healthcare, energy supply, transportation, and manufacturing. IIoT devices provide many advantages for traditional systems including making their management more efficient. The number of IIoT devices has risen from 3.96 billion in 2018 to 5.81 billion in 2020 [2].

Many IoT devices are constrained by power consumption and computational resources. The role of IoT devices can be leveraged through a symbiotic relationship with cloud computing to carry out data storage, analysis, and monitoring. In healthcare, storage and analysis of patient data collected by IIoT devices in the Cloud can be used to avoid preventable deaths, e.g., by hospital error; real-time monitoring enables emergency response when necessary [3]. Cloud computing is also used for the identification and authentication of actuators according to Molle [4]. The actuators are IIoT devices that can, e.g., be used to open and close valves to control the water supply.

The number of opportunities for cyberattacks grows with the number of IoT devices. The integrity of the data the Cloud and the IIoT device receive from each other is contingent upon the security of these devices. The examples in the previous paragraph showed that IIoT devices are even being used in healthcare and water supply, which are considered critical infrastructures in most countries. Compromise or failure of these systems could harm a society. Attacks that target both hardware and software threaten these devices. Hardware security is becoming increasingly important. An example of a hardware attack is the probing attack, which aims to extract sensitive data from a device's non-volatile memory. Physical Unclonable Functions (PUFs) are a countermeasure to these attacks.

The motivations for the use of PUFs are elaborated in Section II. A detailed explanation of PUF technology is given in Section III. An explanation of the applications for which PUFs can be used in IIoT devices specifically are provided in Section IV. An extract of a market analysis, which was carried out on PUFs, is presented in Section V. The paper is concluded in Section VI.

II. MOTIVATION

Probing attacks can be used to extract sensitive information including cryptographic keys from non-volatile memory. The casing of an Integrated Circuit (IC) is removed, and the internal wires of a security critical module are accessed to retrieve the data. A Focused Ion Beam (FIB) uses ions at high beam currents to remove or deposit chip material with nanometer resolution. The attacker can use a FIB to deposit conducting paths that may serve as electrical probe contacts [5]. Tarnovsky carried out an attack to probe the firmware of the Infineon SLE 66CX680P/PE security/smart chip by probing the buses of the chip using an FIB [5] [6]. An informative introduction on probing attacks can be found in chapter 10 of a book on hardware security by Bhunia and Tehranipoor [5].

Hardware attacks, such as probing attacks, may need more knowledge, time, and monetary resources than software related attacks. However, they must still be considered a valid threat. The attacks are more accessible than some may assume. An FIB can be purchased on the resale market relatively inexpensively or rented at an hourly rate. Furthermore, there are parties for which the above stated factors are not a hindrance. Politically motivated attacks including cyberwarfare must be taken into consideration when evaluating the security of IIoT devices employed in critical infrastructures. Such attacks have occured in the past and may be state-sponsored, eliminating time and financial resources as obstacles. Examples of attacks on critical infrastructures include two attacks that resulted in power outages in the Ukraine. In December 2015, a cyberattack on three Ukrainian energy companies rendered approximately 225,000 people without power for several hours [7]. Ukraine's top law enforcement claimed this was a cyberattack by Russia. Investigations following the attack showed evidence to support the claim [8]. A second attack took place almost exactly a year later [9]. The attacks on the power supply in the Ukraine were

 ISBN: 978-1-61208-778-8

not caused by hardware attacks on IIoT devices. However, IIoT devices are employed to take on various roles in energy supply. If attackers retrieve a cryptographic key from such a device, they may be able to eavesdrop onto the communication with the Cloud. This can help them gain information that will aid them in an attack.

A malevolent faction may go about an incursion on critical infrastructures with so much exertion because of the considerable amount of damage that can be caused. Denial of Service (DoS) attacks on power supply, which is usually also considered a critical infrastructure, can have detrimental effects on the economy. The authors of [10] created blackout-simulator.com, a tool that provides an estimate of the economic damage caused by power outages in Europe. The user can specify the start time, date, and the length of a power outage, and the region in which the power outage is taking place and receives an estimate of the economic damage. For example, the tool estimated the damages caused by a hypothetical six hour power outage in the state of Bavaria starting at 8 am on February 24th, 2020 to be approximately 660 million euro [11]. Furthermore, other critical infrastructures, such as healthcare, would also break down, causing deaths. This provides another reason why it is important to defend against all cyberattacks on IIoT devices, especially those that are used in critical infrastructures.

Some may also consider the shrinking size of integrated circuits with time a limiting factor. However, FIBs are also used for the failure analysis in ICs and will therefore continue to be developed and researched to accommodate the size of hardware [5].

A recent study shows that hardware- and silicon level security are becoming a reality for many companies. Forrester Consulting was commissioned to carry out a study to evaluate the needs of companies managing breaches to their hardware- and silicon-level devices and supply chains. The survey was carried out recently — between March 2019 and May 2019 — and included decision makers in 307 companies. The study showed that 63% of companies had experienced data compromise or breach due to an exploited vulnerability in hardware or silicon level security at least once within the last 12 months; 70% of the surveyed companies consider silicon-level security as critically important or very important [12]. The broad spectrum of invasive and non-invasive hardware attacks were implied by this study. These also include probing attacks.

IIoT devices are particularly susceptible to hardware attacks for several reasons. Man-At-The-End (MATE) attacks happen from the inside when an adversary gains "physical access to a device and compromises it by inspecting or tampering with the hardware itself or the software it contains" [13]. Several different third parties, some of which are trusted, have unhampered access to IIoT devices at various points in their life cycle. Companies have their IC designs manufactured in semiconductor fabrication plants. There are some cases in which the manufacturer must place information including cryptographic keys into non-volatile memory during production. The manufacturers may try to extract the information and keep it. During operation, (I)IoT devices are often employed in remote areas without supervision giving attackers unlimited access to the device.

III. Physical Unclonable Functions

PUFs offer a countermeasure against probing attacks. Analogous to biometrics, such as fingerprint detection or a retinal scan, a probabilistic characteristic of a physical object is used to derive a unique cryptographic secret. Semiconductor components in electrical devices contain production tolerances, which are usually unwanted and cannot be controlled. Although these tolerances are only visible on a microscopic level, they manifest themselves in small differences in physical sizes, e.g., two voltages may be slightly different. Therefore, devices which are constructed in exactly the same way can be individualized. PUFs that derive their fingerprints from tolerances from the semiconductor production process, e.g., random fluctuations in the dopant concentration or doping profiles, are called silicon PUFs.

A wide variety of different PUFs have emerged including the arbiter PUF. Figure 1 shows how a single bit can be derived to illustrate the principle of the arbiter PUF. A chain of electrical components, each having two inputs and outputs, is formed resulting in two race tracks for electrical signals. When applying an electrical signal to both inputs at exactly the same time, the signals should theoretically arrive synchronously. Contrary to what might be expected, the arrival times of the electrical signals are minutely different, due to tolerances from the semiconductor production process. The outputs are encoded as a "0" or a "1," and the bits for the keys can be derived based on which output the signal arrived at first. The output of a PUF is called the response [14]. A third input allows for configuration of the paths; each electrical component can either be configured as straight or switched. Different configurations for PUFs are called challenges. Pairs of challenges and responses are called Challenge-Response Pairs (CRPs).

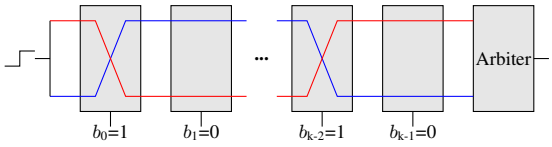

Figure 1. Arbiter PUF [14].

The SRAM PUF, first introduced by Guajardo in [15], offers another method of deriving a cryptographic key from a stochastic process. SRAM cells are constructed in a way that enables easy writing making them prone to intrinsic fluctuations. This does not affect the SRAM cells in any way during normal operation when an externally exerted signal is applied to them. However, when the memory cells are in an undefined state, they take on disparate values. Since SRAM is a form of volatile memory, such a state is achieved during power-up. The cryptographic secret can be extracted from the device during that time. The response is retrieved from the states of the memory cells of the SRAM.

The SRAM and arbiter PUFs can both be considered silicon PUFs. Although they share this similarity, these PUF types can also be distinguished in several different ways. The nature of the probabilistic behavior is different. PUF principles that are derived from similar processes can be separated into different categories. The SRAM PUF belongs to the category of memory-based PUFs which are derived from a type of memory. The arbiter PUF belongs to a category of PUFs that

 ISBN: 978-1-61208-778-8

rely on delays of signals called delay-based PUFs. The second large difference lies in the amount of challenges which can be applied to a PUF instance. A PUF which has very few or only one challenge is called a Physically Obfuscated Key (POK) in PUF literature. A PUF that has many challenges is called a PUF or strong PUF. The SRAM PUF is an example of a POK because it only has one challenge whereas the arbiter PUF has many challenges and can therefore be considered a strong PUF. The difference is important when considering how they are integrated into security protocols.

Many formal definitions have been introduced in literature. The definitions provided by Rührmair are best suited for IIoT devices because of the consideration that the adversary has access to the device for a long time [16]. The source provides formal definitions for both POKs and strong PUFs. Assuming an adversary has access to a PUF for a set amount of time and can retrieve CRPs from it. A PUF is strong if the adversary can not collect enough CRPs, to deliver the correct response to a randomly chosen challenge with a probability greater than 90%. The probability must be greater than 50% to allow systems with binary outputs to be strong PUFs. However, whether that value is 90% or 75% is somewhat arbitrary. The key derived from a system may be called obfuscating PUF or POK if it derived at least in part from random, uncontrollable manufacturing variations. It must also be infeasible for an attacker to guess each digit in the key with a probability greater than 90% when given the device for a specified amount of time [16].

IV. Applications of PUFs

A PUF key can be used to hide a cryptographic key, thereby eliminating the risk of a probing attack. PUF keys are not stored in the device but are generated on demand when they are needed and subsequently deleted. A cryptographic secret can be derived from a PUF and used directly to substitute one which was stored in non-volatile memory. The PUF response can alternatively be used as a Key Encryption Key (KEK) to encrypt sensitive information stored in non-volatile memory including cryptographic keys. In the former scenario, an attacker would no longer find the cryptographic secret in the device when it is powered off. A probing attack in the latter scenario would be futile because the data is encrypted. A POK is well-suited for this because there is no need to store a challenge. Security protocols that are not specifically designed for PUFs can then be used.

Several protocols that harness the specific advantages offered by PUFs have also been designed that offer improvements upon traditional security protocols. These include protocols for authentication and authenticated execution for a variety of different devices on a spectrum of capabilities regarding power consumption and computing power. A protocol, which is based on the principle of the Controlled PUF (CPUF), was introduced by Gassend in [17]. A CPUF can only be accessed through an algorithm that is physically linked to the PUF in an inseperable way. The algorithm can be used to restrict challenges or limit information about responses. The algorithms with which the PUF can be accessed in this particular protocol are shown in Figure 2. The owner of the PUF has one CRP that was extracted from the PUF before it was employed. This CRP was extracted by applying a pre-challenge to get a response. The actual challenge can then be computed by calculating the hash value of the combination of the pre-challenge and a hash

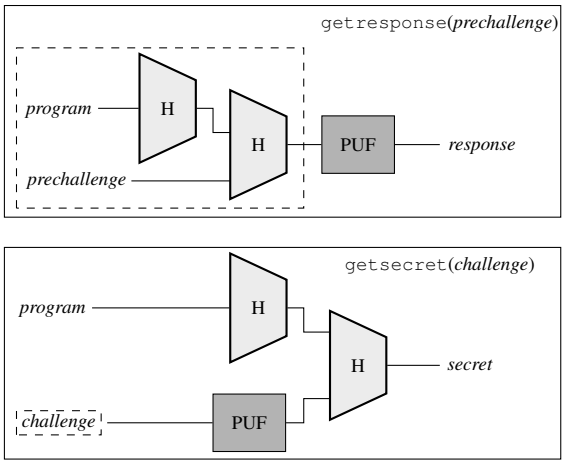

Figure 2. Algorithms to access the CPUF [17].

value of the program, as shown in the box with the dotted line. This allows the owner to calculate the same secret the PUF calculates using `getsecret`(*prechallenge*) later on. In IoT devices this protocol could, e.g., be used to authenticate a measurement taken by a sensor. The execution program is sent to the PUF. The first instruction of the program is to calculate `getsecret`(*prechallenge*). The secret can then be used by the device to generate a Message Authentication Code (MAC). The owner of the PUF can also generate the secret because he has the CRP and can use it to verify the result. Even if attackers extract the challenge from the program, they will still not be able to use it because they need the pre-challenge to calculate the response. This is impossible because it would require them to reverse the hash functions.

Although this paper focuses on the use of PUFs to secure (I)IoT devices communicating with a cloud, there are also many other cloud applications in which PUFs can be used. A Field-Programmable Gate Array (FPGA) can be used to accommodate hardware to accelerate certain algorithms, e.g., in cryptography. They can be reprogrammed offering flexibility. There are services that offer their customers to carry out their work on FPGA boards in the Cloud. These services include Amazon Web Service's EC2 F1 Instances and services offered by the company reconfigure.io. The CPUF could be used to authenticate the results of the computations of the FPGA boards.

V. Available PUF Technologies

Several PUF technologies have emerged on the market. An extensive analysis of available PUF technologies was carried out. An extract of the results of the market analysis is provided below. The PUF technologies that were included in the extract were chosen because they best illustrate the insights gained in the market analysis. Most companies that integrate a PUF into their products buy the technology from a vendor as Intellectual Property (IP). The IP vendors were researched and mapped to the companies that integrate them into their products. In this way, a better idea could be gained of all available PUF technologies because not all IPs have been integrated into products that are available for public purchase. An insight could also be gained into what companies license their technologies from the same vendor.

When contemplating the integration of technologies with PUFs into IIoT devices, there are several challenges that

 ISBN: 978-1-61208-778-8

must be considered. For example, IIoT devices can sometimes have longer lifespans in comparison to regular IoT devices. Therefore, it is even more important that these can be flexibly updated because it is far more likely that changes in security may occur over a span of ten years than over a span of two to three years.

The IP vendor Intrinsic ID designs a PUF IP that uses the SRAM PUF technology as described in Section III. The technology can either be integrated into a product as a hardware IP (QuiddiKey) [18] or software IP (BroadKey) [19]. BroadKey can even be integrated into devices that have already been employed such as IoT devices [20]. The company Renesas has a family of Microcontroller Units (MCUs) called Synergy. Renesas offers a free version of BroadKey called DemoKey which can be tested on Synergy MCUs [21]. Several vendors of electrical components have integrated the hardware IP QuiddiKey into their products. These include NXP's LPC5500 series of MCUs [22] and the LPC540XX family of MCUs [23]. NXP also includes the PUF in two families of i.MX RT crossover processors — the i.MX RT600 [24] and the i.MX RT1170 [25]. Crossover processors combine the advantages of high end MCUs and application processors to meet the needs of IoT devices [26]. The NXP products use the PUF to encrypt data in memory and as a KEK to secure cryptographic keys in non-volatile memory [24] [27]. Microsemi also uses the SRAM PUF technology in several products including the PolarFire FPGA Boards to secure non-volatile memory [28].

Two different PUF technologies are based on the principle of the current mirror circuit shown in Figure 3, the current mirror PUF by Invia and ChipDNA by Maxim Integrated. The black portion of the circuit shows a current mirror as it can be found in many electrical circuits as a constant current source. The gate and the drain of MOSFET M_1 are connected. Therefore, the MOSFET stays in saturation and the current I_1 will stay constant.

The gates of M_1 and M_2 are connected causing their potentials to be equal. Equation (1) can be used to calculate the drain current of a MOSFET [29]. W and L are the width and length of the channel of the MOSFET, V_{Th} is the threshold voltage, V_{GS} is the gate-source voltage, C_{ox} is the gate oxide capacitance per unit area, and μ_n is the charge carrier effective mobility. If the MOSFETs that are used for M_1 and M_2 are of the same type and from the same manufacturer, the values of these variables should theoretically be the same. Therefore, I_{ref} and I_1 should also be the same. In practice, there will be small tolerances from the production process, that can affect any of the variables in (1) and cause miniscule differences between the two currents. The blue part of the circuit shows, that a second constant current source can simply be added by including another MOSFET M_3. Small production tolerances in the MOSFETs will also affect the currents I_1 and I_2.

$$I_D = \frac{1}{2}\mu_{\mathrm{n}} C_{\mathrm{ox}} \frac{W}{L}(V_{\mathrm{GS}} - V_{\mathrm{Th}})^2 \qquad (1)$$

The company Invia has developed a PUF as a hardware IP that utilizes the principle of the current mirror. The PUF consists of a matrix of cells that each contain two MOSFETs producing two constant current sources. The matrix consists of 128 elements — 8 rows and 16 columns. Figure 4 shows how the value of each element is evaluated; only the first row of the matrix is depicted. The two resulting currents are compared. The result will depend on which current is larger. There are

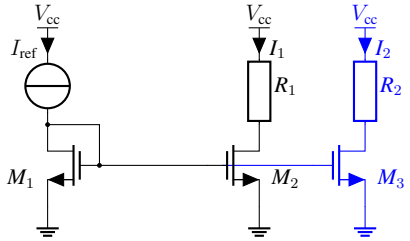

Figure 3. Current mirror as a constant current source.

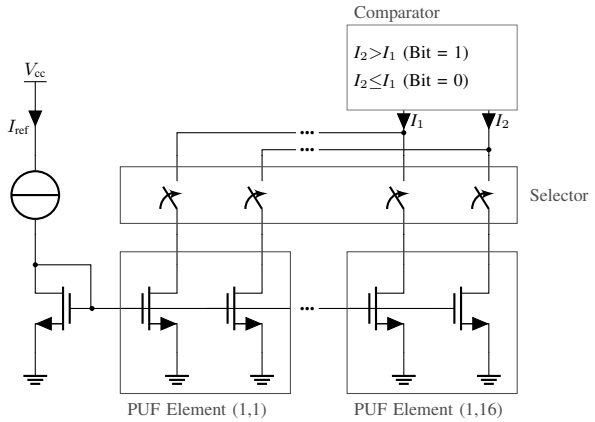

Figure 4. Current mirror PUF by Invia [30].

currently no products available for purchase to the public that contain this hardware IP.

Maxim Integrated is a vendor of electrical components. Rather than purchasing their PUF as a hardware IP, they have designed their own technology called ChipDNA, shown in Figure 5. The PUF also makes use of the principle of the current mirror. It consists of a matrix of 256 elements — 16 rows and 16 columns. As Figure 5 shows, each cell contains two MOSFETs, a p-channel MOSFET M_1 and an n-channel MOSFET M_2. The left part of the circuit and M_1 of each element of the matrix form a current mirror, providing a constant current source. The gate and the drain of MOSFET M_2 are connected causing the MOSFET to stay in the saturation region and switched on. When a MOSFET is switched on, it conducts current but has a resistance $R_{\mathrm{DS,on}}$ so there is a voltage drop across the component. These voltages will vary slightly depending on production tolerances of the MOSFETs used for the current mirror and for the voltage drop. Therefore, they can be compared in order to derive a value. In a diagram of the PUF provided by Maxim Integrated, the gate and drain of M_{ref} are not connected [31]. The assumption is made that this is a mistake because the circuit would cease to function if this would not be the case. The 256 elements of the array are combined into 128 pairs to achieve higher stability [31]. Maxim Integrated is the assignee of a patent that describes an algorithm in which matrix elements are paired [32]. It is likely that this algorithm is used to create the pairs mentioned in [31].

ChipDNA has been integrated into several electrical components, including the DS2477 [33] and DS28E50 [34], which can be used for authentication. Authentication is carried out using a challenge-response protocol. The shared secrets needed for the challenge-response protocol can be stored on the components. Only one secret can be stored on the DS28E50,

 ISBN: 978-1-61208-778-8

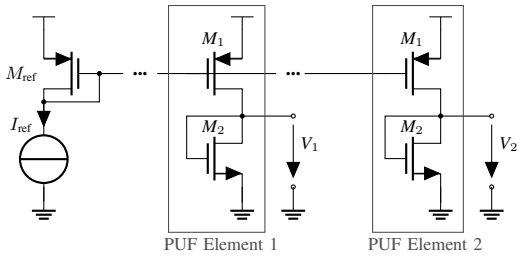

Figure 5. ChipDNA PUF Technology by Maxim Integrated [31].

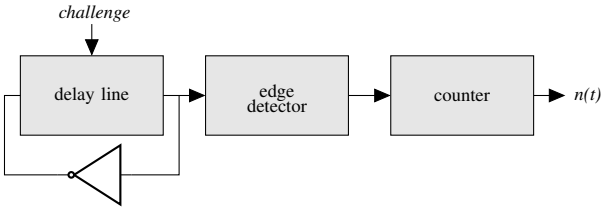

Figure 6. Ring Oscillator PUF [41].

and multiple secrets can be stored on the DS2477. The key generated by the ChipDNA is used to "cryptographically secure" all data stored on the device including the secret for the challenge-response protocol. The electrical components both contain a True Random Number Generator (TRNG) and a SHA-3 engine, which can be used to create a Hash-based Message Authentication Code (HMAC) for the challenge-response protocol. Maxim Integrated sees great potential in the integration of these devices into medical equipment among other applications. They also offer an MCU with a PUF — MAX32520 [35]. The PUF can be used for internal flash encryption, device authentication, and to generate a public and private key pair. The associated public key can be exported and signed by a certification authority.

According to several sources, the PUF that is integrated into Xilinx products is sourced from the IP designer Verayo [36]. The PUF technology that Xilinx integrates into their Zync UltraScale+ products is a Ring Oscillator PUF (ROPUF) [37]. It can therefore be deduced that Verayo develops an ROPUF. Srini Devadas who founded Verayo supervised the masters thesis in which the ROPUF was introduced [38] and was involved in a publication in which a variation of the ROPUF is proposed [39]. In the Zync UltraScale+ products, the PUF is utilized as a KEK to encrypt a user key. The user key can be used to encrypt the boot image [37] [40, pg. 270]. The Zync UltraScale+ products include multi processor system on chips (MPSoC).

Figure 6 shows a diagram of the ROPUF. An asynchronously oscillating loop is formed by inverting the output of a digital delay line and feeding it back to the input. The frequency of the oscillator is determined by the delay line, which is influenced by the manufacturing tolerances of the electrical components. Consequently, the instances of the circuit have distinct frequencies. The edges of the signal are counted using a digital counter to derive a PUF response. The function $n(t)$ is the edge count as a function of time. The input *challenge* can be used to configure the delay line [41]. In [39], a variation of the ROPUF is introduced to reduce the influence of environmental variations like temperature. The counters of two instances of the ROPUF circuit are compared to derive the bit, instead of using the counter as a response directly. The exact version of the ROPUF that is used in the Zync UltraScale+ products is not specified in the datasheet. It is safe to assume that a variation of the ROPUF is used that does not require a challenge as there is no mention of this in the data sheet [40].

Several important insights were gathered from the market analysis. A variety of different PUF technologies (e.g., current mirror PUF, SRAM PUF, ROPUF) are incorporated into a diverse group of devices (e.g., FPGA, MCU, MPSoC). PUFs contribute to the security of a diversity of applications, e.g., flash encryption and secure boot processes. However, most are used in a similar way: to encrypt data on the device or replace a cryptographic key stored in non-volatile memory. Most of the technologies still use the PUF in a very rudimentary way, not taking advantage of the specific PUF properties such as the CPUF protocol. All of the technologies, which were found in the analysis, were POKs. Although the ROPUF can potentially have multiple challenges, no mention of these were made in the datasheet of the product leading to the assumption that the ROPUF was implemented without them [40].

VI. Conclusion and Future Work

Hardware attacks including probing attacks are a surging problem to which PUFs offer an attainable countermeasure. Many different PUF technologies have been integrated into a variety of products on the market. Most PUF technologies available on the market are only used to secure keys which are then used in traditional security protocols. Based on all the sources found in the market analysis, most products currently available on the market for public purchase do not leverage a protocol that exploits the specific advantages offered by PUFs and all used PUF technologies are POKs. It will be interesting to observe the future developments of the PUF market.

Acknowledgement

The research project "Intelligent Security for Electrical Actuators and Converters in Critical Infrastructures (iSEC)" is a collaboration of SIPOS Aktorik GmbH, Grass Power Electronics GmbH and OTH Amberg-Weiden. It is supported and funded by the Bavarian Ministry of Economic Affairs, Regional Development and Energy.

References

[1] K. L. Lueth, "State of the IoT 2018: Number of IoT devices now at 7B – Market accelerating," 2018, URL: https://iot-analytics.com/state-of-the-iot-update-q1-q2-2018-number-of-iot-devices-now-7b/ [accessed: 2020-07-27].

[2] "Gartner Says 5.8 Billion Enterprise and Automotive IoT Endpoints Will Be in Use in 2020," 2019, URL: https://www.gartner.com/en/newsroom/press-releases/2019-08-29-gartner-says-5-8-billion-enterprise-and-automotive-io [accessed: 2020-07-27].

[3] M. S. Hossain and G. Muhammad, "Cloud-assisted industrial internet of things (iiot) - enabled framework for health monitoring," *Computer Networks*, vol. 101, pp. 192–202, 2016.

[4] M. Molle, U. Raithel, D. Kraemer, N. Graß, M. Söllner, and A. Aßmuth, "Security of cloud services with low-performance devices in critical infrastructures," in *The Tenth International Conference on Cloud Computing, GRIDs, and Virtualization – CLOUD COMPUTING 2019*, 2019, pp. 88–92.

[5] M. Tehranipoor and S. Bhunia, *Hardware Security A Hands-On Learning Approach*. Elsevier, 2019.

[6] C. Tarnovsky, "Security Failures in Secure Devices," 2008, URL: https://www.blackhat.com/presentations/bh-dc-08/Tarnovsky/Presentation/bh-dc-08-tarnovsky.pdf [accessed: 2020-07-27].

 ISBN: 978-1-61208-778-8

[7] "Analysis of the Cyber Attack on the Ukrainian Power Grid," 2016, URL: https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf [accessed: 2020-07-27].

[8] J. Pagliery, "Scary questions in Ukraine energy grid hack," 2016, URL: https://money.cnn.com/2016/01/18/technology/ukraine-hack-russia/ [accessed: 2020-07-27].

[9] P. Polityuk, O. Vukmanovic, and S. Jewkes, "Ukraine's power outage was a cyber attack: Ukrenergo," 2017, URL: https://www.reuters.com/article/us-ukraine-cyber-attack-energy-idUSKBN1521BA [accessed: 2020-07-27].

[10] M. Schmidthaler and J. Reichl, "Assessing the socio-economic effects of power outages ad hoc," *Computer Science - Research and Development*, vol. 31, pp. 157–161, 03 2016.

[11] "Blackout Simulator 2.0," URL: http://blackout-simulator.com/ [accessed: 2020-07-27].

[12] "BIOS Security – The Next Frontier for Endpoint Protection," 2019, URL: https://www.dellemc.com/ja-jp/collaterals/unauth/analyst-reports/solutions/dell-bios-security-the-next-frontier-for-endpoint-protection.pdf [accessed: 2020-07-27].

[13] M. Jakubowski, P. Falcarin, C. Collberg, and M. Atallah, "Software protection," *IEEE Software*, vol. 28, pp. 24–27, 03 2011.

[14] D. Lim, "Extracting secret keys from integrated circuits," Master's thesis, Massachusetts Institute of Technology, May 2004.

[15] J. Guajardo, S. S. Kumar, G.-J. Schrijen, and P. Tuyls, "Fpga intrinsic pufs and their use for ip protection," in *Cryptographic Hardware and Embedded Systems - CHES 2007*, P. Paillier and I. Verbauwhede, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2007, pp. 63–80.

[16] U. Rührmair, J. Sölter, and F. Sehnke, "On the foundations of physical unclonable functions," *IACR Cryptology ePrint Archive*, June 2009, 2009/277 URL: ia.cr/2009/277 [accessed: 2020-07-29].

[17] B. Gassend, D. Clarke, M. van Dijk, and S. Devadas, "Controlled physical random functions," in *18th Annual Computer Security Applications Conference, 2002. Proceedings.*, 01 2002, pp. 149–160.

[18] "QuiddiKey," URL: https://www.intrinsic-id.com/products/quiddikey/ [accessed: 2020-07-27].

[19] "Bk software," URL: https://www.intrinsic-id.com/products/bk-software/ [accessed: 2020-07-27].

[20] "Intrinsic ID's BROADKEY Secures IoT with Key Management Software Powered by SRAM PUF," 2017, URL: https://www.intrinsic-id.com/intrinsic-ids-broadkey-secures-iot-key-management-software-powered\\-sram-puf/ [accessed: 2020-07-27].

[21] "Secure Key Management Software," URL: https://www.renesas.com/us/en/products/synergy/gallery/partner-projects/intrinsic-id-secure-key-management-software.html [accessed: 2020-07-27].

[22] "LPC5500 Series: World's Arm Cortex-M33 based Microcontroller Series for Mass Market, Leveraging 40nm Embedded Flash Technology," URL: https://www.nxp.com/products/processors-and-microcontrollers/arm-microcontrollers/general-purpose-mcus/lpc5500-cortex-m33:LPC5500_SERIES [accessed: 2020-07-27].

[23] "LPC540XX: Power-Efficient Microcontrollers (MCUs) with Advanced Peripherals Based on Arm Cortex-M4 Core," URL: https://www.nxp.com/products/processors-and-microcontrollers/arm-microcontrollers/general-purpose-mcus/lpc54000-cortex-m4-/power-efficient-microcontrollers-mcus-with-advanced-peripherals-based\\-on-arm-cortex-m4-core:LPC540XX [accessed: 2020-07-27].

[24] "RT600 (Datasheet)," URL: https://www.nxp.com/docs/en/data-sheet/DS-RT600.pdf [accessed: 2020-07-27].

[25] "i.MX RT1170 Crossover MCU Family - First Ghz MCU with Arm Cortex-M7 and Cortex-M4 Cores," URL: https://www.nxp.com/products/processors-and-microcontrollers/arm-microcontrollers/i.mx-rt-crossover-mcus/i.mx-rt1170-crossover-mcu-family-first-ghz-mcu-with-arm-cortex-m7\\-and-cortex-m4-cores:i.MX-RT1170 [accessed: 2020-07-27].

[26] "Crossover Embedded Processors – Bridging the gap between performance and usability," URL: https://www.nxp.com/docs/en/white-paper/I.MXRT1050WP.pdf [accessed: 2020-07-27].

[27] "LPC55S6x (Datasheet)," URL: https://www.nxp.com/docs/en/data-sheet/LPC55S6x.pdf [accessed: 2020-07-27].

[28] "UG0753 User Guide PolarFire FPGA Security," URL: https://www.microsemi.com/document-portal/doc_download/136534-ug0753-polarfire-fpga-security-user-guide [accessed: 2020-07-27].

[29] M. T. Thompson, *Intuitive Analog Circuit Design*. Newnes, 2014, URL: https://www.elsevier.com/books/intuitive-analog-circuit-design/thompson/978-0-12-405866-8 [accessed: 2020-07-27].

[30] V. Telandro and C. Tremlet, "Why should your next secure design be PUF based," 2019, URL: https://www.design-reuse-embedded.com/ipsocdays/ipsocdays2019/china2019/slides/1-Invia%20-%20Why_should_your_next_PUF_based.pptx [accessed: 2020-07-27].

[31] "How ChipDNA Physically Unclonable Function Technology Protects Embedded Systems (Application Note 6767)," URL: https://pdfserv.maximintegrated.com/en/an/ChipDNA-Unclonable-Protects-Embedded-Systems.pdf [accessed: 2020-07-27].

[32] P. Parvarandeh and S. Ung Kwak, "Systems and Methods for Stable Physically Unclonable Functions (US Patent 9,485,094)," 2016.

[33] "DeepCover Secure SHA-3 Coprocessor with ChipDNA PUF Protection," URL: https://www.maximintegrated.com/en/products/embedded-security/secure-authenticators/DS2477.html/tb_tab0 [accessed: 2020-07-27].

[34] "DeepCover Secure SHA-3 Authenticator with ChipDNA PUF Protection," URL: https://www.maximintegrated.com/en/products/embedded-security/DS28E50.html [accessed: 2020-07-27].

[35] "ChipDNA Secure Arm Cortex M4 Microcontroller," URL: https://datasheets.maximintegrated.com/en/ds/MAX32520.pdf [accessed: 2020-07-27].

[36] Design&Reuse, "Verayo puf ip on xilinx zynq ultrascale+ mpsoc devices addresses security demands," URL: https://www.design-reuse.com/news/40875/verayo-puf-ip-xilinx-zynq-ultrascale-mpsoc.html?utm_campaign=40875&utm_content=1&utm_medium=rss&utm_source=designreuse [accessed: 2020-07-27].

[37] E. Peterson, "Developing Tamper-Resistant Designs with Zynq UltraScale+ Devices (XAPP1323)," 2018, URL: https://www.xilinx.com/support/documentation/application_notes/xapp1323-zynq-usp-tamper-resistant-designs.pdf [accessed: 2020-07-27].

[38] B. Gassend, "Physical random functions," Master's thesis, Massechusetts Institute of Technology, February 2003.

[39] G. Suh and S. Devadas, "Physical unclonable functions for device authentication and secret key generation," in *Proc 44th ACM/IEEE Design Automation Conference*, 07 2007, pp. 9–14.

[40] "Zynq UltraScale+ Device Technical Reference Manual," 2019, URL: https://www.xilinx.com/support/documentation/user_guides/ug1085-zynq-ultrascale-trm.pdf [accessed: 2020-07-27].

[41] R. Maes and I. Verbauwhede, "Physically unclonable functions: A study on the state of the art and future research directions," in *Information Security and Cryptography*. Springer Berlin Heidelberg, 2010, pp. 3–37, URL: https://doi.org/10.1007%2F978-3-642-14452-3_1 [accessed: 2020-04-10].

 ISBN: 978-1-61208-778-8