Cloning Physically Unclonable Functions

Clemens Helfmeier*, Christian Boit
Semiconductor Devices,
Dept. of High-Frequency and Semiconductor System Tech.,
Technische Universität Berlin,
Berlin, Germany
{clemens.helfmeier,christian.boit}@.tu-berlin.de

Dmitry Nedospasov*, Jean-Pierre Seifert
Security in Telecommunications,
Dept. of Software Eng. and Theoretical Computer Science,
Technische Universität Berlin,
Berlin, Germany
{dmitry,jpseifert}@sec.t-labs.tu-berlin.de

* These authors contributed equally to this work

***Abstract*—As system security demands continue to evolve, Physically Unclonable Functions (PUFs) are a promising solution for secure storage on Integrated Circuits (ICs). SRAM PUFs are among the most popular types of PUFs, since they require no additional circuitry and can be implemented with on-die memories such as caches and data memory that are readily available on both ASICs and FPGAs. This work demonstrates that SRAM PUFs are not well suited as PUFs, as they do not meet several requirements that constitute an ideal PUF. The compact nature of SRAM, standard interconnects and resiliency to environmental effects make SRAM PUFs particularly easy to clone. We consider several ways in which SRAM PUFs can be characterized and demonstrate a Focused Ion Beam circuit edit with which we were able to produce a physical clone of our Proof-of-Concept SRAM PUF implementation. As a result of the circuit edit, when challenged, the physical clone produced an identical physical response to the original device. To the best of our knowledge, this is the first work in which a physical clone of a Physically Unclonable Function was produced.**

I. Introduction

Secure storage is a critical component of any secure system and is often delegated to dedicated hardware. In many cases dedicated security Integrated Circuits (IC) are incorporated into the designs of secure systems specifically to take care of such tasks. Secret data can be programmed into a secure IC during production by the vendor or personalization by the end-user [1]. In systems lacking Non-Volatile Memory (NVM), key storage and distribution can be particularly difficult.

However, even with NVM, an attacker can utilize any number of techniques to read-out on-die memories [2]. One especially promising avenue to solve the problems of key storage are Physically Unclonable Functions (PUFs) since intrinsic process variations can be used to implement unique challenge/response pairs for every IC [3], [4]. When implemented correctly, a key does not have to be stored at all, but is instead derived from the characteristic response of a PUF. Ideally, the characteristic response changes whenever the IC is altered, i.e. when the device is depackaged. Such behavior provides an additional layer of tamper-resistance [5].

One of the most researched and popular classes of PUFs are memory-based PUFs [6]. Such PUFs utilize the settling state of volatile memory, such as Static Random Access Memory (SRAM), to implement unique challenge/response pairs. Such memories are already present on secure ICs and offer hardware vendors substantial flexibility during manufacturing. Memories can be partially or completely re-purposed to temporarily or permanently act as a PUF at startup. SRAM is commonly included in such solutions, making SRAM-based PUFs especially popular [7]. SRAM and SRAM-based PUFs are also particularly resilient to temperature variations and are generally more compact than many other memory-based PUFs [8].

Though several works to date have described the characteristics of an ideal PUF, this work focuses on the original definitions introduced in [3]. This work demonstrates that SRAM PUFs violate at least the following characteristics of an ideal PUF:

- **Manufacturer resistant -** It should be infeasible to create a second PUF that generates the same response.
- **Hard to characterize -** It should be infeasible to characterize the response of a PUF.
- **Controlled -** The PUF should be difficult to access for the attacker and implement some tamper-resistance.

The main contributions of this paper are: (1) *First successful physical clone.* We successfully reproduced the "unique" response of our Proof of Concept (PoC) SRAM PUF implementation in a second identical device. We used a Focused Ion Beam (FIB) circuit edit (CE) to produce a fully-functioning second instance of the device with an identical physical response to that of the target device. To the best of our knowledge this is the first successful hardware-based cloning attack against a PUF. (2) *Several strategies to read out SRAM.* If the entire contents of the SRAM can be extracted, an SRAM PUF can be fully-characterized. We review several techniques with which the contents of SRAM at startup can be extracted allowing an attacker to recover the unique response of the IC. (3) *Discussion and Countermeasures.* We discuss several inherent weaknesses of memory-based PUFs as compared to other classes of PUFs. We also introduce several mitigation techniques with which hardware vendors can make our attack significantly less cost-effective for the attacker.

The rest of this paper is structured as follows: In Section II we provide additional necessary background information on the 6T-SRAM cell circuit as well as SRAM PUF implementations. The FIB CE is explained in Section III. In Section IV we

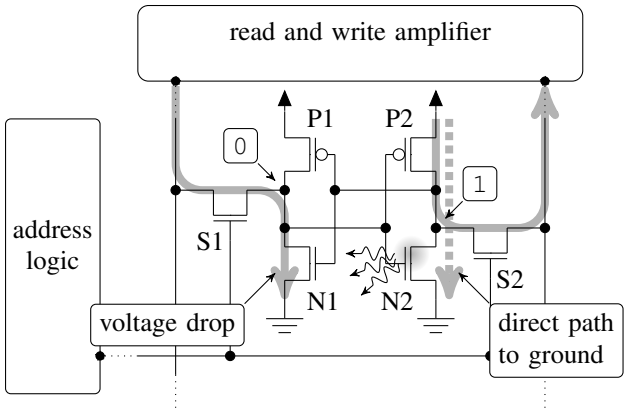


Fig. 1: Schematic and read operation of a 6T SRAM. The solid arrows depict the current injected by the read amplifiers for the specified states. The dotted arrows correspond to the resulting current to ground. During this process, transistor N2 is in saturation and emits light.

provide details of the Device Under Test (DUT) as well as the PoC implementation and experimental setup. We present the results of our experiments including all the necessary steps to reproduce the attack in Section V. Finally we evaluate the impact of our findings and propose several potential countermeasures in Section VI.

II. Background

This section introduces terminology used throughout the work and reviews several characteristics of SRAM and SRAM-based PUFs. The process of cloning a PUF consists of two main steps:

- **Chacterization** - a process in which the attacker gains knowledge of the challenge/response behavior of a PUF.
- **Emulation** - the process of recreating or modeling the unique response of a PUF, i.e. creating a PUF with identical challenge/response pairs.

If an attacker is able to fully *characterize* the unique PUF response, the response can be *emulated* or modeled. The authors of [9] successfully applied machine learning to create a software model of an arbiter PUF and generate correct responses. However, software modeling is often impractical, especially in high-security applications. Such scenarios may require an identical form factor, i.e. a smartcard, or additional functionality present on the IC that is outside the scope of the PUF itself. By directly characterizing the physical response of the *target device*, an identical physical response can be reproduced in a second instance of the device. We refer to a modified device exhibiting an identical physical response as a *physical clone* of the target device. The physical clone remains fully functional and retains any additional capabilities implemented on the IC.

A. SRAM and SRAM PUFs

An SRAM consists of an array of cells connected by bitlines and wordlines where each cell stores a single bit of information. The cells of an SRAM array can be read or written by the corresponding logic interface, depending on the status of the bitlines and wordlines. During a read of an SRAM cell, the corresponding wordline is asserted and the status of the bitlines is read [10]. The cell needs to drive the read amplifiers inputs during this read access, see Figure 1. Depending on the drive strength of a given cell, the voltages at the drains of the cell's four inverter transistors are elevated and reduced, respectively.

As the SRAM is powered up, each cell takes on either the logical state of `0` or `1` [6], [11]. A PUF response is generated simply by challenging or addressing an SRAM array, i.e. reading out a particular location within the array. This also has the advantage of requiring no additional logic to generate challenge/response pairs since existing memory access logic can be used.

B. SRAM Characterization Techniques

Since SRAM PUF responses are produced simply by challenging certain addresses within the SRAM, reading out the entire SRAM after startup is sufficient to fully characterize the IC. There are a number of ways in which an attacker can achieve this goal. SRAM PUF challenges utilize standard on-chip memory interfaces and buses. If an attacker gains control of such interfaces, any memory contents stored on the IC can be accessed.

With the exception of Read Only Memory (ROM), which can be extracted from optical images of the die, the IC must be actively stimulated in order to extract memory contents. Fully-invasive decapsulation in conjunction with microprobing can provide an attacker access to any memory circuitry. However, probing embedded memories directly is infeasible in practice because of the number of data and address lines. Instead, the data can exfiltrated over multiple measurements of the individual lines [2]. Arbitrary access to embedded memories can also be achieved by directly manipulating the opcodes executed by the IC. Such attacks circumvent all on-die countermeasures and sensors and are not impeded by bus encryption, since data must be deobfuscated and decrypted before reaching the core of the IC [12].

If the attacker is able to introduce one or more deterministic transient faults into the SRAM PUF, Differential Fault Analysis (DFA) can be applied to recover the SRAM contents [13]. An attacker could use laser stimulation to induce transient faults and perform DFA or to increase the leakage current of the system [14], [15]. Such attacks could however be thwarted on systems with optical sensors. Moreover, many modern security ICs have additional passive and/or active layers of shielding that obstruct any light from reaching the surface of the IC [1].

Several Side-Channel Analysis (SCA) techniques are capable of dynamically extracting contents of embedded memories. However, in many cases SCA can only extract part of the secret data and secure memory architectures, such as inspection resistant memory, can make extraction of the full secret data infeasible [16]. Nevertheless, certain forms of SCA such as

Photonic Emission Analysis (PEA) can be used to dynamically extract the full contents of the SRAM [17], [18]. In this work, we chose to use PEA for its passive, non-destructive, semi-invasive nature and the relatively simple sample preparation required.

C. Photon emission of 6T SRAM cells

Metal Oxide Semiconductor (MOS) transistors have three modes of operation, off, triode or linear region, and saturation or active mode. Photon emission only occurs in saturation region for high drain-source voltages $V_{\mathrm{DS}} > V_{\mathrm{GS}} - V_{\mathrm{TH}}$. In saturation, the channel does not fully extend to the drain forcing carriers to travel through a space charge region. The acceleration of carriers in the high electric field of the space charge region is accompanied by light emission [19]. Both types of transistors emit photons, but since holes have a smaller impact ionization probability, PMOS emissions occur less frequently. In CMOS logic, devices only operate in saturation for a very short time during transition between logic states. When driving long interconnects, the output voltage of a logic cell degrades from the nominal voltage for a logical state of `0` and `1`. This process increases the time spent in saturation by subsequent cells. Integration over many cycles is necessary in order to capture an acceptable image.

Addressed SRAM cells drive long bitline capacitances and the current from read amplifiers for enhancement of read performance. This loading of the SRAM cell leads to a strong degradation of the voltage at the drains of the SRAM cells transistors, see Figure 1, and an increase in time spent in saturation region. Additionally, NMOS transistors connected to the bitline at their gate operate in saturation due to the degraded bitline signal. As shown in Figure 1, this leads to a significant current through two transistors of the SRAM cell and thus to substantial emissions.

D. Focused Ion Beam Circuit Edit

Modern security ICs have multiple mechanisms to detect attacks [1]. In order to eliminate any potential attack detection and subsequent self-destruction of the target IC, attackers may first disable on-die countermeasures and subsequently modify the IC [12]. Note, that all countermeasures deployed to date seek to detect malicious modifications from the frontside. In this work, we instead use a backside approach to clone the SRAM startup behavior and thus are not impeded by any frontside countermeasures implemented on the IC.

In a process known as FIB trenching, a FIB is used to mill the backside of the device down to the n-wells. This leaves an approximate substrate thickness of 2 µm while the circuit remains fully functional. At locations where an SRAM cell is to be modified, the device is further thinned down to shallow trench isolation (STI) level, as can be seen in Figure 2. This leaves only a few hundred nanometers of thickness at the active devices. At this point, the STI layer provides an excellent reference for sample alignment allowing precise access to all circuit nodes inside the SRAM. Circuit modification can now be conducted with accurate precision. Though the main application of this technique is cutting or rewiring for static modification, this approach also allows the modification of dynamic behavior characteristics like increasing the speed of individual cells [20]. Due to the relatively small trenching areas, overall system performance is unaffected.

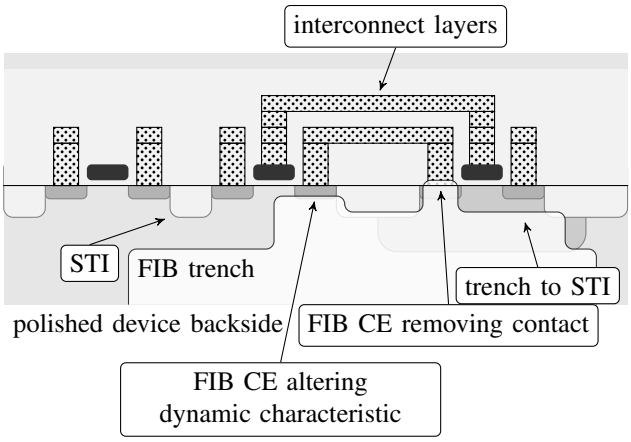


Fig. 2: Cross section of a backside-prepared device thinned down to STI. The first FIB CE shown (right) has removed the drain connection of the PMOS transistor rendering the PMOS transistor non-functional and forcing the output of the inverter to ground. The second FIB CE shown (left) has thinned the bulk silicon into the transistors drain diffusion altering the transistors dynamic performance and introducing dynamic bias into the corresponding gate. Either one of the two possible modifications is sufficient to bias the startup behavior of SRAM cells.

III. Cloning SRAM PUFs using FIB CE

In this work, we present two techniques for modifying the startup behavior of SRAM cells using a FIB CE. 1) To achieve a deterministic startup behavior, individual transistors can be removed completely. This CE yields a cell incapable of storing a particular logical state. 2) The transistors can be trimmed individually to alter their dynamic performance and leakage characteristics. As the symmetry of an 6T SRAM cell is corrupted by this CE, the startup behaviour of the cell is biased. The SRAM cell remains fully-functional as only the dynamic behavior changes.

FIB workstations can be programmed to raster the CE position using individual patterns. This makes it possible to mill or etch arbitrary surface reliefs up to a certain degree of accuracy[21], [22], [23]. The binary nature of the physical response of SRAM means that a simple bitmap generated during the PUF characterization can be utilized for the FIB CE with high success probability. Such a bitmap makes it possible to edit tens of cells simultaneously, making it possible to clone the response of an SRAM array of several kilobits in size.

IV. Experimental Setup

In this Section we describe the DUT and the equipment used for SRAM characterization and emulation of the target

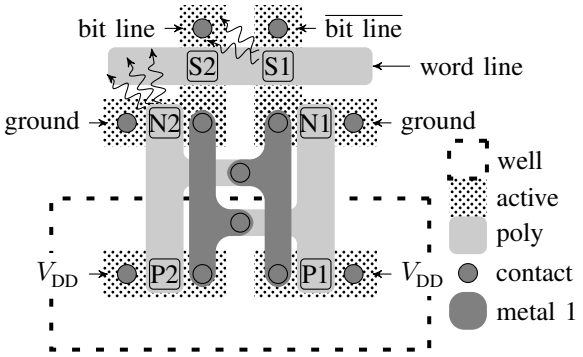


Fig. 3: Layout of the target's SRAM cells. As explained in Figure 1, either N1/S2 or N2/S1 produce emissions during read out. The two logical states of the inverters can be distinguished based on the emissions.

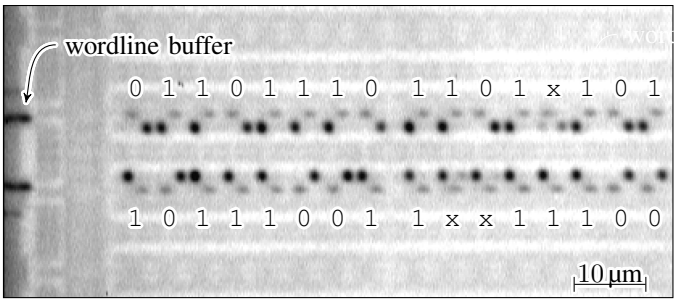


Fig. 4: Reflected image of the SRAM array with overlaid emission image. Bits 9, 10 in the bottom row and bit 12 in the top row are marked "don't care" `x`. These cells started up with both logical states `0` and `1` during integration. Assuming a fuzzy extractor algorithm is used on the PUF response, these bits potentially do not need to be modified [11].

device. In our work we used only standard equipment which can generally be found in every failure analysis laboratory.

A. Sample Preparation and Device Under Test

For our experiments we chose to use an industry standard microcontroller, the Atmel ATmega328P. The IC came in an industry standard TQFP package. The samples were prepared using the Ultratec ASAP-1 automated mechanical polishing machine. The machine removed the package and excess bulk silicon of the device backside. The bulk silicon was thinned to an approximate substrate thickness of 20 µm. This step could potentially be omitted, but it saves significant milling time in the FIB.

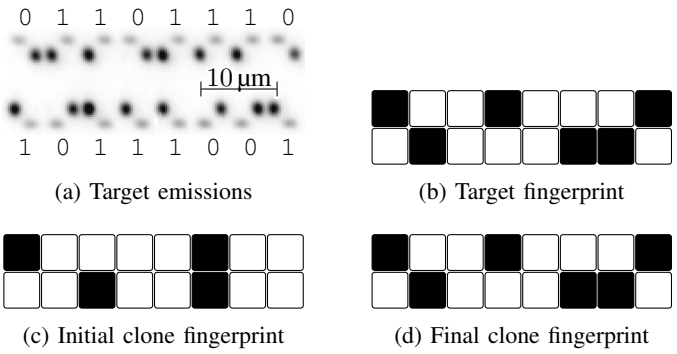
The DUT was inversely mounted on a custom printed circuit board. This allowed for the DUT to be electrically stimulated in the Hamamatsu Phemos, as well as in the FIB vacuum chamber. The ATmega328P has a total of 2 kilobytes of SRAM with an SRAM feature size of approximately 600 nm. For verification, the contents of the SRAM was transmitted over a serial interface.

B. SRAM Characterization

To characterize the SRAM of the IC, the Near Infrared (NIR) photonic emissions of the DUT were captured using the Hamamatsu Phemos 1000 NIR-CCD. The program on the DUT was executed with a high loop frequency so that sufficient photonic emissions could be generated, reducing the overall required integration time. To ensure that bit flips could also be detected, the supply voltage was occasionally disconnected from the DUT for several seconds. This ensured that startups were independent of the previous value stored within memory and that certain SRAM cells could attain the opposite bistable value on subsequent startups.

C. FIB Circuit Edit

The CEs were performed on the DCG Systems OptiFIB. This system has a coaxial optical path integrated into the ion column that makes navigation possible using near-infrared light on backside-prepared devices. As silicon is transparent



(a) Target emissions

(b) Target fingerprint

(c) Initial clone fingerprint

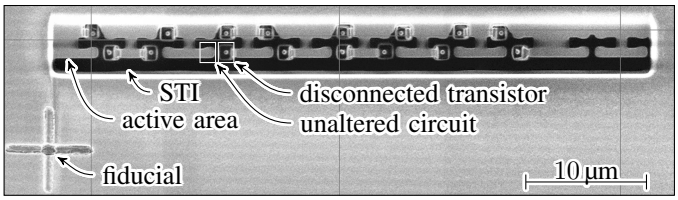
(d) Final clone fingerprint

Fig. 5: SRAM fingerprints of the target device and physical clone. The photonic emission correspond to the target fingerprint, see Figure 5a and 5b, respectively. The initial fingerprint of the physical clone differed from the fingerprint of the target device, see Figure 5c and 5b, respectively. The final fingerprint of the clone matched the fingerprint of the target, see Figure 5d.

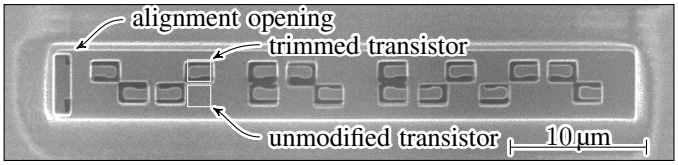
for near-infrared light, the target site can easily be found. During the trenching procedure, the process inside the OptiFIB is assisted by XeF_2 to enhance the etch process. By observing the optical image, slope and thickness of the silicon material can be estimated. With this method, trenches covering an area of 300 µm × 300 µm can be created in under one hour.

V. Results

Our experiments determined that the SRAM of the ATmega328P lost the information stored in it after approximately 30 ms of off-time. In order to ensure independent SRAM startup behavior following two consecutive start-ups, the off-time threshold was set significantly higher, namely 3 s. To reduce integration times, the SRAM was read out continuously at memory locations containing the target's PUF response. An integration time of 10 s was sufficient for recovering the logical state of the SRAM. To produce high contrast images a 300 s



(a) Secondary electron image of the destructive FIB CE



(b) Secondary electron image of the non-destructive FIB edit

Fig. 6: Secondary electron images of the DUT. The first FIB edit shows the exposed contact plugs of the SRAM cells PMOS drains, see Figure 6a. Since the PMOS drains were only trimmed in the second edit, the memory remained fully functional, see Figure 6b.

integration time was used, see Figure 4. The corresponding bit values can be decoded as explained in Section II-C. Figure 3 illustrates the emission for the first bit of the first row in the emission image, see Figure 4. Using this emission image information, two different FIB CEs were performed on a second device. The results of the successful CEs are clearly visible in the secondary electron image produced by the ion beam in Figures 6a and 6b. In the first FIB CE, the PMOS transistors drain contacts opposite the emitting NMOS transistors were removed in the first FIB CE. The exposed remains of the round drain connection contact plugs are clearly visible in Figure 6a. In contrast, the die contacts were not removed completely in the second FIB CE. Instead, the transistors were trimmed leaving the remaining drain diffusion as can be seen in Figure 6b. The modification of 16 bits was completed in approximately 5 minutes for both edits. If a mask was applied, this process could be sped up significantly.

To determine if the FIB edit was successful, the SRAM contents were subsequently verified by the UART output of the DUT. After the FIB edit the target device and the physical clone exhibited an identical SRAM fingerprint, see Figure 5. Both circuit edits produced physical clones that continued to operate nominally in our laboratory environment. Since the contacts were completely removed in the first CE, the SRAM was no longer bistable. In contrast, the SRAM of second FIB CE remained fully-functional.

VI. Disussion

Characterization of PUFs by modeling is different to physical cloning. The physical response of the PUF itself is an invariable part of the PUF protocol. Hence, an in-depth understanding of any additional parameters applied to the PUF response is unnecessary. As demonstrated in this work, even low cost analysis techniques can yield sufficient information for the characterization of the physical response and for the production of a physical clone [24]. An attacker can remain completely oblivious to any countermeasures and/or obfuscation implemented on the device, as well as any post-processing performed on the PUF response [1], [3]

SRAM PUFs do not meet the three characteristics outlined in Section I. In contrast to delay-based PUFs, SRAM PUFs have a huge amount of independent bits of information, making modeling attacks hard. Nevertheless, even such PUFs are not necessarily *hard to characterize* as we were successful in characterizing the physical response of the SRAM array. Characterization of SRAM PUFs is even simpler in part due to the high spatial density of the response. When SRAM PUFs are powered-up the full physical response is present within the SRAM. Thus, SRAM PUFs are not *controlled* because an attacker can apply standard IC analysis techniques to read out the SRAM at startup and recover the full unique physical response. *Manufacturer resiliency* is also difficult to achieve with SRAM PUFs. The array structure of SRAM means that FIB trenching can be performed extremely efficiently on adjacent cells at the same time, greatly reducing time required for producing a clone.

Though our PoC implementation utilized an SRAM PUF many of these observations hold true for other types of PUFs as well. For example, ring oscillator based PUFs can be trimmed individually using a very similar method. The work of Schlangen et al. [20] presents such a CE, where individual logic cells can be trimmed accordingly to produced the desired physical response. In light of tools like the FIB, *manufacturer resiliency* is particularly difficult to guarantee. Emphasis should instead be placed on the *hard to characterize* the property of PUFs. Two promising approaches to this problem have already been introduced by Plaga and Koob [25] as “strong PUFs” and Lugli et. al. [26] as “Super High Information Content PUFs”.

A. Impact

By modifying a second instance of the device we were able to immensely reduce the cost and effort necessary for producing physical clone. All the tools used in this work are readily available in university failure analysis labs. The machines could be acquired used for 100 k$ to 200 k$ or rented on an hourly basis in any failure analysis laboratory. The amount of lab time necessary to produce an initial clone was about twenty hours, whereas subsequent clones can easily be produced in under three hours. Nevertheless, producing a physical clone with these techniques remains economically infeasible for devices of limited monetary value. Moreover, sample preparation and PUF characterization would be more difficult in a real-world scenario. However, the Pay-TV industry in particular is fraught with examples of devices that were compromised using similar IC analysis techniques [27]. Such techniques also pose a threat to use-cases where damages can accumulate over a long period of time, such as identification where the validity of digital documents is measured in decades.

B. Potential Countermeasures

Both characterization and emulation can be made significantly more difficult if PUFs with synthesized logic are used instead. These would ideally be distributed over large areas of the die. Such countermeasures can ensure that multiple measurements are necessary during characterization and increase the amount of effort required to produce a clone. Industry standard obfuscation techniques such as memory scrambling can also achieve a lower PUF response density and better distribution in SRAM [1]. Moreover, this also makes certain characterization techniques far more tedious, requiring an attacker to first understand the memory layout. However, with techniques such as PEA, an attacker can simply characterize the start-up behavior for all the cells and non-destructively edit the entire memory using a FIB mask.

VII. Conclusion

In this work we successfully produced a physical clone of a PUF in an identical form factor. Only standard university failure analysis equipment was used allowing for cost-effective production of the physical clone. The high-density of SRAM cells within an array makes characterization of the PUF response and production of the physical clone particularly efficient. The standard interfaces through which SRAM PUFs are challenged make them susceptible to numerous well documented semi-invasive and invasive attacks against on-die memories. Most importantly our experiments show that such structures are extremely resilient to environmental effects meaning that the device function is not compromised during characterization and production of the physical clone. In light of our results, SRAM-PUF implementations and memory-based PUFs in general offer little additional protection over industry standard programmable NVM memories such as flash and EEPROM. Such attacks pose a real threat to high-security applications utilizing PUFs as comparable equipment can be found in failure analysis labs around the world.

VIII. Acknowledgements

This research was supported by the Helmholtz Research School on Security Technologies. We would like to thank colleagues Andreas Eckert and Carlo Pagano for their support.

References

[1] W. Rankl and W. Effing, *Smart Card Handbook*, 4th ed. Wiley Publishing, 2010.

[2] O. Kömmerling and M. Kuhn, "Design Principles for Tamper-Resistant Security Processors," *USENIX Workshop on Smartcard Technology, Chicago, IL (10–11 May 1999) http://www. cl. cam. ac. uk/Research/Security/tamper*, 1999.

[3] B. Gassend, D. Clarke, M. van Dijk, and S. Devadas, "Silicon physical random functions," *Proceedings of the 9th ACM conference on Computer and communications security*, pp. 148–160, 2002.

[4] R. Pappu, B. Recht, J. Taylor, and N. Gershenfeld, "Physical one-way functions," *Science*, vol. 297, no. 5589, pp. 2026–2030, 2002.

[5] P. Tuyls, G. J. Schrijen, B. Škorić, J. van Geloven, N. Verhaegh, and R. Wolters, "Read-proof hardware from protective coatings," *Cryptographic Hardware and Embedded Systems-CHES 2006*, pp. 369–383, 2006.

[6] A.-R. Sadeghi and D. Naccache, Eds., *Towards Hardware-Intrinsic Security: Foundations and Practice*, 1st ed. New York, NY, USA: Springer-Verlag New York, Inc., 2010.

[7] "NXP Strengthens SmartMX2 Security Chips with PUF Anti-Cloning Technology," NXP Semiconductors N.V, Feb. 2013.

[8] S. Katzenbeisser, Ü. Kocabaş, V. Rožić, A. Sadeghi, I. Verbauwhede, and C. Wachsmann, "PUFs: Myth, Fact or Busted? A Security Evaluation of Physically Unclonable Functions (PUFs) Cast in Silicon," *Cryptographic Hardware and Embedded Systems–CHES 2012*, pp. 283–301, 2012.

[9] U. Rührmair, F. Sehnke, J. Sölter, G. Dror, S. Devadas, and J. Schmidhuber, "Modeling attacks on physical unclonable functions," in *CCS '10: Proceedings of the 17th ACM conference on Computer and communications security*. ACM Request Permissions, Oct. 2010.

[10] N. H. E. Weste and D. M. Harris, *CMOS VLSI Design*, 4th ed., ser. A Circuits and Systems Perspective. Addison-Wesley, Mar. 2010.

[11] J. Guajardo, S. Kumar, G. J. Schrijen, and P. Tuyls, "FPGA intrinsic PUFs and their use for IP protection," *Cryptographic Hardware and Embedded Systems-CHES 2007*, pp. 63–80, 2007.

[12] C. Tarnovsky, "Hacking the Smartcard Chip," in *Blackhat DC 2010*. Arlington, VA: Flylogic Engineering, LLC, Feb. 2010.

[13] E. Biham and A. Shamir, "Differential fault analysis of secret key cryptosystems," *Advances in Cryptology—CRYPTO'97*, pp. 513–525, 1997.

[14] S. Skorobogatov and R. Anderson, "Optical fault induction attacks," *Cryptographic Hardware and Embedded Systems, CHES 2002*, pp. 31–48, 2003.

[15] S. Skorobogatov, "Optically Enhanced Position-Locked Power Analysis," *Cryptographic Hardware and Embedded Systems-CHES 2006*, pp. 61–75, 2006.

[16] J. Valamehr, M. Chase, S. Kamara, A. Putnam, D. Shumow, V. Vaikuntanathan, and T. Sherwood, "Inspection resistant memory: architectural support for security from physical examination," in *ISCA '12: Proceedings of the 39th Annual International Symposium on Computer Architecture*. IEEE Computer Society, Jun. 2012, pp. 130–141.

[17] D. Nedospasov, A. Schlösser, J.-P. Seifert, and S. Orlic, "Functional integrated circuit analysis," *Hardware-Oriented Security and Trust (HOST), 2012 IEEE International Symposium on*, pp. 102–107, 2012.

[18] A. Schlösser, D. Nedospasov, J. Krämer, S. Orlic, and J. Seifert, "Simple Photonic Emission Analysis of AES," *Cryptographic Hardware and Embedded Systems–CHES 2012*, pp. 41–57, 2012.

[19] C. Boit, "Fundamentals of Photon Emission (PEM) in Silicon – Electroluminescence for Analysis of Electronic Circuit and Device Functionality," in *Microelectronics Failure Analysis: Desk Reference*. ASM International, 2004, p. 356 ff.

[20] R. Schlangen, R. Leihkauf, T. Lundquist, P. Egger, and C. Boit, "Rf performance increase allowing ic timing adjustments by use of backside fib processing," in *Proceedings of the 16th International Symposium on the Physical and Failure Analysis of Integrated Circuits (IPFA 2009)*, vol. 1. IEEE Press, 2009, pp. 33–36.

[21] P. Scholz, U. Kerst, C. Boit, C.-C. Tsao, and T. Lundquist, "Creation of Solid Immersion Lenses in Bulk Silicon Using Focused Ion Beam Backside Editing Techniques," in *ISTFA '08: Proceedings of the 34st International Symposium for Testing and Failure Analysis*. ASM International, 2008, pp. 157–162.

[22] R. K. Jain, T. R. Lundquist, M. E. Antolik, and M. Thompson, "Novel and Practical Method of Through Silicon FIB Editing of SOI Devices," in *ISTFA '05: Proceedings of the 31st International Symposium for Testing and Failure Analysis*. ASM International, 2005, pp. 70–77.

[23] J. Siebert, L. Johri, D. McCarty, S. Voong, M. Sengupta, and H. Wang, "Enhanced Scanning Control of Charged Particle Beam Systems," US Patent US 7,230,240, 06 12, 2007.

[24] A. Schlösser, D. Nedospasov, J. Krämer, S. Orlic, and J.-P. Seifert, "Simple Photonic Emission Analysis of AES," *Journal of Cryptographic Engineering*, vol. 3, no. 1, pp. 3–15, 2013. [Online]. Available: http://dx.doi.org/10.1007/s13389-013-0053-7

[25] R. Plaga and F. Koob, "A Formal Definition and a New Security Mechanism of Physical Unclonable Functions," in *Measurement, Modelling, and Evaluation of Computing Systems and Dependability and Fault Tolerance*, ser. Lecture Notes in Computer Science, J. Schmitt, Ed. Springer Berlin Heidelberg, 2012, vol. 7201, pp. 288–301. [Online]. Available: http://dx.doi.org/10.1007/978-3-642-28540-0_24

[26] P. Lugli, A. Mahmoud, G. Csaba, M. Algasinger, M. Stutzmann, and U. Rührmair, "Physical Unclonable Functions based on Crossbar Arrays for Cryptographic Applications," *International Journal of Circuit Theory and Applications*, 2012.

[27] N. Chenoweth, *Murdoch's Pirates: Before the Phone Hacking, There Was Rupert's Pay-TV Skullduggery*. Allen & Unwin, 2012.