On the Impact of Aging on Power Analysis Attacks Targeting Power-Equalized Cryptographic Circuits

Md Toufiq Hasan Anik
University of Maryland Baltimore County
Baltimore, MD 21250, USA
toufiqhanik@umbc.edu

Bijan Fadaeinia
Ruhr University Bochum
Horst Görtz Institute for IT Security, Germany
bijan.fadaeinia@rub.de

Amir Moradi
Ruhr University Bochum
Horst Görtz Institute for IT Security, Germany
amir.moradi@rub.de

Naghmeh Karimi
University of Maryland Baltimore County
Baltimore, MD 21250, USA
nkarimi@umbc.edu

ABSTRACT

Side-channel analysis attacks exploit the physical characteristics of cryptographic chip implementations to extract their embedded secret keys. In particular, Power Analysis (PA) attacks make use of the dependency of the power consumption on the data being processed by the cryptographic devices. To tackle the vulnerability of cryptographic circuits against PA attack, various countermeasures have been proposed in literature and adapted by industries, among which a branch of hiding schemes opt to equalize the power consumption of the chip regardless of the processed data. Although these countermeasures are supposed to reduce the information leakage of cryptographic chips, they fail to consider the impact of aging occurs during the device lifetime. Due to aging, the specifications of transistors, and in particular their threshold-voltage, deviate from their fabrication-time specification, leading to a change of circuit's delay and power consumption over time. In this paper, we show that the aging-induced impacts result in imbalances in the equalized power consumption achieved by hiding countermeasures. This makes such protected cryptographic chips vulnerable to PA attacks when aged. The experimental results extracted through the aging simulation of the PRESENT cipher protected by Sense Amplifier Based Logic (SABL), one of the well-known hiding countermeasures, show that the achieved protection may not last during the circuit lifetime.

1 INTRODUCTION

With the aggressive scaling of VLSI technology and moving towards smaller feature sizes, various design robustness concerns continue to arise. Among them, aging effects in CMOS devices are one of the major challenges in nanotechnologies. Aging mechanisms degrade the reliability and performance of CMOS devices over their lifetime. Due to aging, electrical behavior of transistors deviates from its original intended behavior. This deviation degrades performance; and consequently, the chip fails to meet some of the required specifications [9]. Among aging mechanisms, due to their critical role in urging circuits malfunctions, Bias Temperature-Instability (BTI) and Hot-Carrier Injection (HCI) have received a lot of attention [3].

To address the aging-induced reliability concerns, mitigation schemes have been proposed in different levels of design abstraction ranging from architectural to device level. These schemes prolong device lifetime via guard-banding (i.e., running the device at a lower frequency from the early stage of deployment), gate-sizing, voltage tuning, leveraging partial recovery of BTI aging effects via injecting healing patterns, etc [10, 16]. However, these schemes are either insufficient or otherwise over-pessimistic as the rate of aging degradation depends on operating conditions including temperature, voltage bias, and workload [19]. Thereby, aging effects cannot be thoroughly prevented.

Although aging mechanisms and related mitigation schemes have received the lion's share of attention from reliability perspective in recent years [7, 15], their impact on the security of devices, in particular cryptographic devices, is yet to be investigated [6]. In practice, as the specifications of the transistors embedded in a cryptographic device change during its lifetime, the delay and power consumption of the device deviate from its original values. This in turn affects the success of the attacks built upon exploiting unintentional leakages from the device such as its power consumption or timing characteristics.

Indeed, Side-Channel Analysis (SCA) attacks are known as a serious threat for cryptographic devices. Such an attack can result in recovering their secret data, so-called key. In this attack, the adversary analyzes the physical leakage (e.g., running time, power consumption, electromagnetic radiation) emitted during cryptographic operations in the device and retrieves the key by considering the dependency of this leakage and the key-dependent processed data. In particular, Power-Analysis (PA) attacks (e.g., DPA [14] and CPA [5]) benefit from the dependency of the power traces on the data being processed by the cryptographic device [11].

Hiding and masking are the two main type of countermeasures that cryptographic devices are equipped with to resist PA attacks [18]. While hiding schemes opt to decrease Signal-to-Noise ratio (SNR) in order to hide information leakage below the noise level, masking countermeasures randomize the intermediate values via secret sharing and multi-party computation techniques.

ASPDAC '21, January 18–21, 2021, Tokyo, Japan

ACM ISBN 978-1-4503-7999-1/21/01…$15.00
https://doi.org/10.1145/3394885.3431597

A category of hiding schemes try to equalize the power consumption of the circuit regardless of the data being processed. These schemes are mainly realized as Dual-Rail Pre-Charge (DRP) logic styles in which for each gate, there is a complementary counterpart fed with complement of the original gate's input and generates the complement output. Although such hiding methods are supposed to decrease the success of PA attacks, they fail to consider the aging effects occurring during the device lifetime.

In practice, the threshold voltage of the transistors embedded in a cryptographic chip deviates from their original values over time, making the delay of dual rails become unbalanced after the circuit is aged. Such imbalances can be exploited by the adversary to compromise the target chip. Thereby, the effect of device aging on the success of the PA attacks, and in particular the protected chips should be investigated thoroughly. Accordingly, this paper focuses on the success of the PA attacks launched on a dual-rail-logic implementation of the PRESENT cipher [4]. We show how the success rate of the attack increases over time, making the device more vulnerable to the attacks. *To the best of the authors' knowledge, the article in hand is the first work that investigates the impact of device aging on the success of PA attacks launched on the circuits equipped with dual-rail logic.*

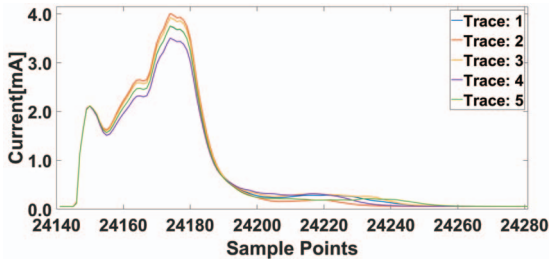
2 MOTIVATION

Hiding schemes are deployed to reduce the information leakage of cryptographic circuits. Power-equalizing hiding countermeasures mainly follow the DRP concept which deals with the source of data-dependent power consumption, i.e., the transitions. Among several such DRP solutions, we can recall Wave Dynamic Differential Logic (WDDL) [30], Masked Dual-rail Pre-charge Logic (MDPL) [22], improved Masked Dual–rail Pre–charge Logic (iMDPL) [21], and Sense Amplifier Based Logic (SABL) [29].

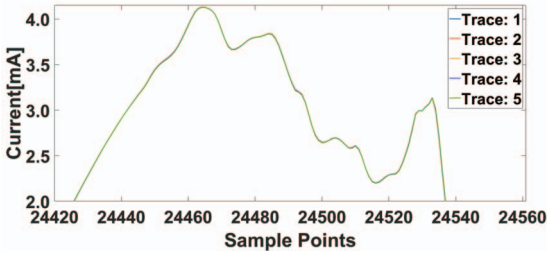
In this paper, we focus on SABL although it necessitates a full-custom design flow. Our choice is due to the data-independent time-of-evaluation of SABL, also known as early propagation effect [18], which is a source of information leakage in most of the other dual-rail logic styles like WDDL and MDPL [27]. More details about SABL is given in Section 3.1. As a side node, iMDPL is also free of early propagation effect, but it combines masking with DRP logic, which is slightly out of our focus.

Below, we give an example to motivate the research conducted in this paper. Figure 1(a) depicts five current traces (corresponding to five different plaintexts, but the same key) obtained by simulating the unprotected implementation of the PRESENT cipher. For the sake of clarity, the shown traces belong to a single clock cycle, when a PRESENT S-Box is computed. As expected, the current traces are deviating from each other in different points of time; this can be easily exploited by an adversary to recover the key. In contrast, Fig. 1(b) shows the traces for the same plaintexts when encrypted by the SABL circuit of the PRESENT cipher. As depicted, in this case, the current traces have been highly equalized. This makes the device compromising highly difficult (if not impossible).

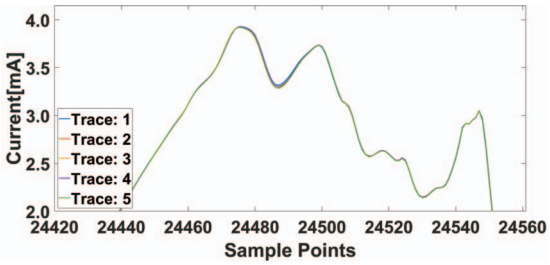
Both Fig. 1(a) and Fig. 1(b) relate to new circuits, i.e., when the target circuits have not been aged. However, Fig. 1(c) shows how the SABL circuit deviates its primary mission of power equalization when the circuit is aged. This figure shows the traces when applying



(a) Unprotected circuit (Age=0)



(b) SABL-protected circuit (Age=0)



(c) SABL-protected circuit (Age=8 weeks)

Figure 1: Current traces of PRESENT cipher circuitry when being fed with five different plaintexts.

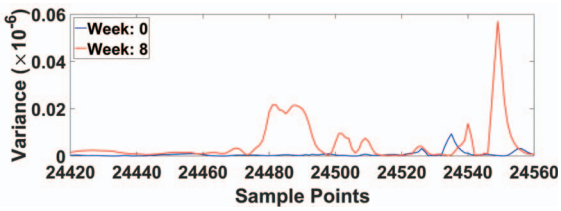
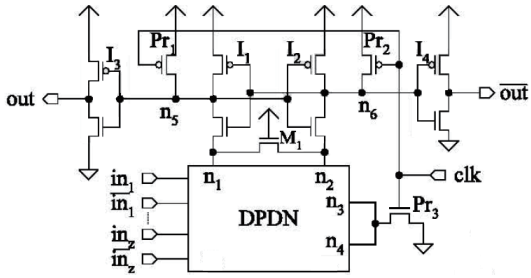


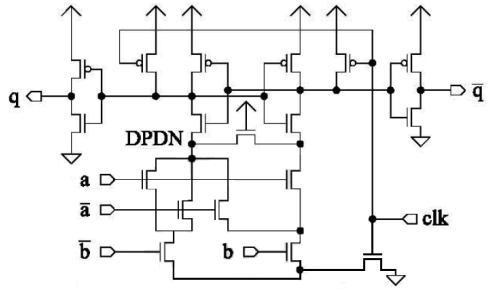
Figure 2: Variance traces of the SABL-protected circuit.

the same set of plaintexts (as the other two figures) to the 8-week old circuit. Such deviations are expected to be exploited by the adversary to extract the key.

For the sake of clarity and illustrating the leakage points, Fig. 2 shows the corresponding variance of several traces for the new and 8-week old circuits. As shown, the maximum variance increases around times, when the device has been deployed for 8 weeks. This observation confirms that the leakage is increased via aging.



(a) Overall-view of an SABL gate



(b) Representation of SABL AND/NAND gate

Figure 3: Block diagram of SABL structure [29].

3 PRELIMINARY BACKGROUNDS

3.1 SABL

SABL, first proposed by Tiri et al. in 2002 [29] and later improved in [32], is a Dual-Rail Pre-charge (DRP) logic style using a pair of wires to carry a signal and its complementary. It includes two phases, pre-charge and evaluation, to avoid glitches.At every clock cycle while *clk* signal is LO, first the entire circuit goes to the pre-charge phase, where the output of all gates set to LO. Then, at the start of the evaluation phase, i.e., positive edge of the *clk* signal, the gates start to evaluate their outputs, by turning only one of their dual rails to HI. This guarantees only one LO-to-HI transition at every gate output during the evaluation phase, thereby avoiding glitches and making the power consumption independent of the data processed. Note that the efficiency of dual-rail circuits and in particular the SABL relies on several factors including the early propagation effect [27] and symmetry between the complimentary rails [18]. Otherwise, the power consumption of a LO-to-HI toggle at different rails of a signal would be recognizable.

Due to their special design, SABL cells need a full custom design flow, i.e., standard cell libraries cannot be used. Figure 3 shows the overall view of an SABL gate (and that of an AND/NAND gate), where DPNP denotes the Differential Pull Down Network. Through the transistor M_1, all internal nodes and capacitances are predischarged during the pre-charge phase. This charge and discharge of the same capacitances in every clock cycle makes the power consumption of the SABL circuit independent of its workload; hence, providing protection against PA attacks.

The area of an SABL gate is more than twice of its original circuit counterpart, its clock rate is almost half, and it consumes more power compared to the original circuit. However, it can significantly harden PA attacks. We should highlight that the success of SABL depends on avoiding early-propagation effect (as explained in [32]) and balancing the dual-rail routes (as suggested in [31]).

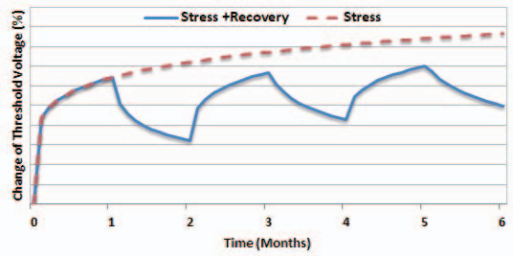


Figure 4: NBTI-induced Threshold-voltage shift of a PMOS transistor over time [2]. Y-axis values are not shown to make the graph generic for different technologies.

3.2 Aging Mechanisms

Device aging results in performance degradation and eventual failure of digital circuits over time [13]. Aging mechanisms include Negative Bias Temperature-Instability (NBTI), Positive Bias Temperature-Instability (PBTI), Hot Carrier Injection (HCI), Time Dependent Dielectric Breakdown (TDDB), and Electro-Migration (EM). In fact, among all aging mechanisms, BTI and HCI are two leading factors in degradation of digital circuits [8, 20].

The BTI (including NBTI and PBTI effects) mechanism is one of the major causes of threshold voltage increase in transistors during their lifetime. NBTI and PBTI occur in PMOS and NMOS transistors, respectively. The impact of NBTI is more dominant than PBTI beyond the 45 nm technology node. However, with the introduction of high-k gate dielectrics and metal gate transistors, PBTI effects have also received significant attention [12].

A PMOS transistor experiences two phases of NBTI depending on its operating condition. The first phase (i.e., *stress*) occurs when the transistor is on ($V_{gs} < V_t$). Here, positive interface traps are generated at the Si-SiO_2 interface which leads to an increase of the threshold voltage. The second phase (i.e., *recovery*) occurs when the transistor is off ($V_{gs} > V_t$). In this phase, the threshold voltage drift occurred during the stress phase is partially recovered. The BTI-induced threshold voltage drifts depend on the physical parameters of the transistor under stress, supply voltage, temperature, and stress time [12]. The last three parameters (so-called external parameters) are generally used to accelerate the aging process. Note that PBTI affects NMOS transistors in a similar way that NBTI affects PMOS transistors.

Figure 4 shows the threshold voltage drift of a PMOS transistor that is continuously under stress for 6 months and a PMOS that alternates stress/recovery phases every other month. As shown, NBTI effect is high in the first couple of months but the threshold voltage tends to saturate for long stress times.

HCI occurs when hot carriers are injected into the gate dielectric during transistor switching and remain there. HCI is a function of switching activity and degrades the underlying circuit by shifting the threshold voltage and the drain current of transistors under

stress [23]. HCI has a dependency on temperature, clock frequency, usage time, and activity factor of the transistor under stress, i.e., the percentage of cycles in which the transistor is switching [20]. Note that, unlike BTI mechanisms, HCI is not recovered.

4 TARGET CIRCUIT

In this paper, we target the SABL model of the PRESENT cipher. PRESENT is an SPN-based ultra-lightweight ISO-standardized block cipher with 64-bit blocks deployed in ubiquitous computing environments with extremely constrained resources [4]. PRESENT includes 31 rounds and supports two different key lengths, 80 and 128 bits. Each round consists of a bitwise XOR operation, a non-linear substitution layer (S-Box) and a linear permutation layer.

We build our SABL circuit based on an implementation of the 80-bit encryption function following the serialized architecture presented in [25]. This implementation is claimed to be area-optimized, and its data paths are serialized to 4-bit words (one nibble). It includes only one 4-bit S-Box which thus needs to be shared between the data path and the key schedule. It requires 563 clock cycles to finish an encryption of one plaintext. Figure 5 depicts the block diagram of this serialized architecture.

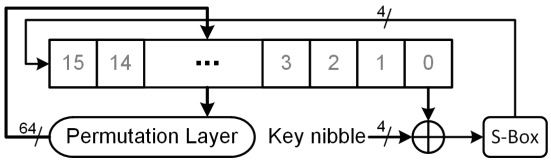


Figure 5: The Block diagram of the target PRESENT cipher.

In order to obtain the SABL circuit, we first synthesized an RTL description of the aforementioned PRESENT encryption function by Synopsis Design Compiler using a custom library including only (2-input) AND/NAND, OR/NOR, XOR/XNOR, NOT, and FlipFlop cells. Then, we converted the resulting verilog netlist to a Spice netlist including the corresponding SABL gates (as shown in Section 3.1), where the single-rail signals are turned to dual rails. The achieved Spice netlist is a transistor-level simulation file of the SABL model of the nibble-serial PRESENT-80 encryption function. We suppose that the dual-rails are routed by some techniques (like wire-fat approach [31]) to make them as balanced as possible. Therefore, we did not consider any routing imbalances in our SABL circuit. For the sake of completeness, we report that the netlist includes 21,980 NMOS and 13,838 PMOS transistors.

5 EXPERIMENTAL RESULTS

In this section we give the details of our experimental analyses including the setup and conducted attacks and evaluations.

5.1 Experimental Setup

We used Synopsys HSpice for the transistor-level simulations using 45-nm NANGATE technology [1], and the HSpice built-in MOSRA Level 3 model to assess the effect of NBTI and HCI aging [28]. Current values were extracted for the new (original) circuit as well as the aged ones. The effect of aging was evaluated for 8 weeks of device operation in time steps of one week. We considered the operating temperature as 80°C and the supply voltage (Vdd) was set to 1.2V during the original and the aging simulation.

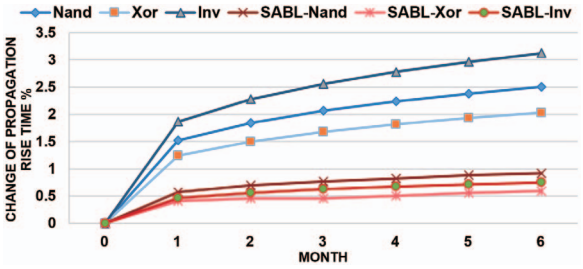


Figure 6: Change of propagation rise time (%) of basic gates with different aging conditions.

To extract the current values, we simulated the first round of the SABL circuit for the total of 22 clock cycles. The circuit was operated at 300 MHz, and we sampled the current signal with the accuracy of 2 ps, i.e., 1665 sample points in each clock cycle. Note that the first round of the cipher makes use of the first 64 bits of the 80-bit key [4]. Hence, conducting an attack at the first round would reveal only the first 64-bit part of the key.

The SABL PRESENT netlist was fed with randomly generated plaintexts and a fixed key. We used the same fixed key and the same set of plaintexts for both original (no aging) and aging simulations during the measurements, where each measurement corresponds to one randomly-generated plaintext and the fixed key.

Our HSpice simulations include 90 traces associated to simulating 90 different plaintexts. The simulation of each plaintext took around 3 hours for the new circuit (week: 0) and around 51 hours for aging simulations (all 8 weeks together) using a single core of a machine with 24 CPU cores and 320 GB of RAM. To reduce the computation time, we conducted each 24 simulations in parallel. In total, we required around 8.5 days to collect 90 traces from both new and aged circuits.

5.2 Aging-induced Delay Change

The first set of results illustrates the effect of NBTI aging on the propagation delay of primitive logic gates. Figure 6 shows the change in propagation delay of each classic (i.e., unprotected) primitive logic gate as well as their SABL-protected counterpart over time when these gates are fed with randomly generated inputs between 1 and 6 months. As shown, each primitive gate, both unprotected and SABL-protected, experiences different amount of delay change related to its transistor level topology. This observation confirms that each path in a cryptographic device may degrade with a different rate based on the type of its underlying gates, and the input values feeding it. The takeaway point from this observation is that aging can result in imbalances in the power consumption of each gate, each path, and in sum in the total power consumption of a device during the time even if the device is equipped with power-equalization schemes. These imbalances can improve the success of the PA attacks on such protected devices.

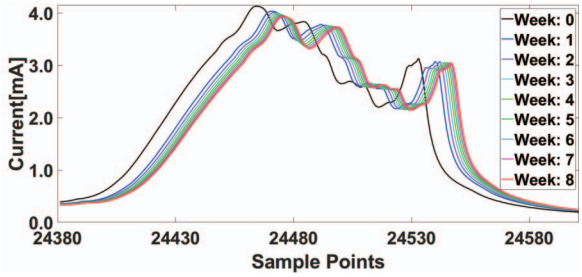


Figure 7: Current traces during the computation of an S-Box for the same input in different aging conditions.

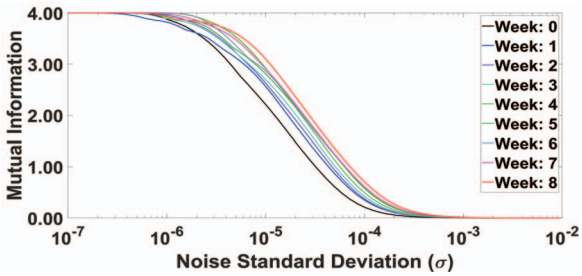


Figure 8: Mutual Information curves associated to an S-Box input for different aging conditions.

5.3 Power Analysis Attacks

5.3.1 Aging-Induced Dynamic Power Change. Figure 7 depicts the simulation result representing the dynamic power change during the computation of an S-Box for one randomly generated plaintext (the same time frame as in Fig. 1) when the circuit is new versus when it was deployed between 1 and 8 weeks. As expected, the magnitudes of the current trace changes during the device lifetime.

5.3.2 Mutual Information. In the simulation environment, the SCA traces are free of noise. Hence, even extremely small differences between the amount of energy consumption associated to different processed data lead to successful key recovery. Therefore, the goal of a proper SCA evaluation in the simulation domain is to assess the susceptibility of attacks on the underlying circuit to the noise level, since the SCA measurements are always affected by noise originating from the measurement setup and environmental parameters. To this end, an analysis scheme (so-called IT analysis) based on the concept of Information Theory has been introduced in [26] and applied, e.g., in [17, 24]. Following the nature of environmental noise, it considers noise with Gaussian distribution centered to each simulated SCA value associated to a processed data, and estimates mutual information by means of conditional entropy as

$$\mathrm{I}(S;L) = \mathrm{H}[S] - \mathrm{H}[S|L],$$

where L denotes the SCA leakages and S the selected intermediate value (in our case is the S-Box input). The conditional entropy can be estimated by means of integral over l as

$$\mathrm{H}[S|L] = -\sum_{s} \Pr[s] \int \Pr[l|s] \cdot \log_2 \Pr[s|l]\, dl.$$

Such an analysis extracts a curve for mutual information (between current traces and the S-Box input) over the standard deviation of a Gaussian noise. It actually reveals how much noise is required to avoid the exploitability of leakages. This technique is mainly used to compare two circuits simulated under the same conditions in order to understand which one exhibits more information, or which one needs more noise to avoid the information leakage.

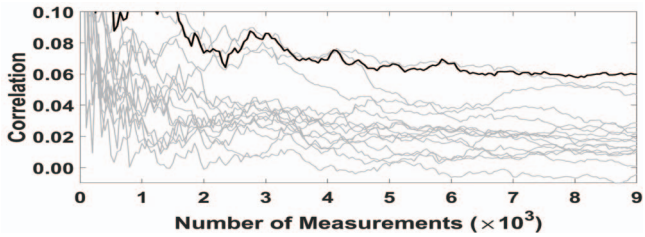
In our analysis, we considered nine cases of the simulated current traces: the new (not aged) SABL circuit and 8 SABL aged circuits corresponding to 8 weeks of deployment. To this end, we focused on a single clock cycle, where an S-Box is computed (including both evaluation and precharge phases), and extracted the mean traces associated to the S-Box input, i.e., 16 mean traces (to remove the switching noise [18]). Then, the maximum estimated mutual information at all sample points has been taken while increasing the noise standard deviation σ. The resulting nine mutual information curves are shown in Fig. 8.

It can be seen that mutual information drops with a higher amount of noise when the circuit is aged. In other words, information leakage is increased and a higher amount of noise is required to hide the leakage in case of the aged SABL circuits.

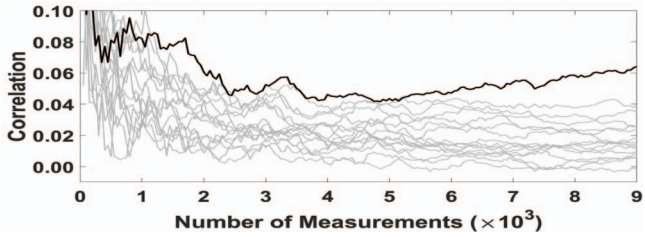
5.3.3 State-of-the-art Attack. The next set of evaluation results deals with the side-channel leakage of the target cipher via the state-of-the-art Correlation Power Analysis (CPA) attack. In this attack, the adversary considers a hypothetical power model for each recorded trace, by applying a hypothetical model to an intermediate value that depends on a known input as well as (part of) the unknown key. Then, by correlating the predicted hypothetical power values (depending on the guessed key) to the measured leakage traces, the key can be recovered. This is true if the hypothetical power model (at least partially) fits to the actual power consumption of the device, and enough number of measured leakage traces are used to accurately-enough estimate the correlation by Pearson correlation coefficient.

To resemble the real silicon implementation, in our experiments we artificially added noise to the current traces extracted from HSpice simulations. The added noise follows a Gaussian distribution with standard deviation σ of 10^{-3}. The noise was added to the current traces of the original (no aging) as well as aged simulations. We added the noise to each trace 100 times, resulting in a set of 9,000 traces and used this set for each attack and evaluation. To remove the effect of randomness, we repeated each attack and evaluation 50 times, i.e., making 50 current profiles each including 9,000 noisy traces, and used them to launch the attacks. Below, we report the attack results based on the mean of the gathered results for each current profile.

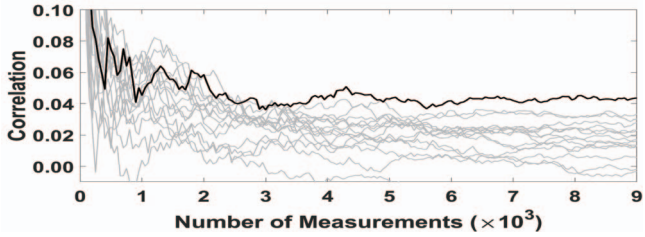
By means of a Hamming weight (HW) model on the S-Box output, we conducted the attack on all nine differently-aged SABL circuits. Note that since the SABL circuit follows a precharge-evaluation fashion, the values stored in registers (correspondingly seen by the combinatorial gates) are preset to 0 before every evaluation phase. Therefore, the common Hamming distance model used to attack hardware cryptographic devices are equivalent to Hamming weight in this case. Figure 9 depicts a couple of exemplary correlation curves over the number of measurements (for the most informative points). In the graphics, the curve associated to the correct key



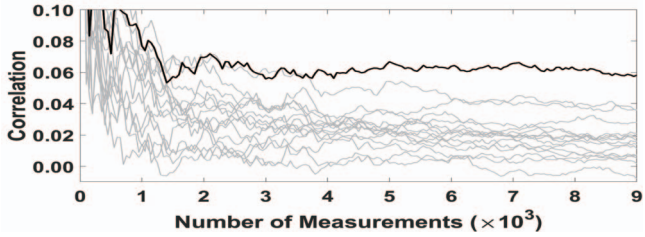
(a) Age=0



(b) Age=2 weeks



(c) Age=5 weeks



(d) Age=8 weeks

Figure 9: CPA results on simulated traces when the device is aged for 0, 2, 5, and 8 weeks. Target: a key nibble in the first cipher round. Model: Hamming weight of the S-Box output.

candidate is marked by black color. As shown, the more the device is aged, the higher is the correlation of the correct key, i.e., the attack becomes easier. The takeaway point from this observation is that by aging, the SABL-protected circuit experiences imbalances in its dual rails and thereby it would be more susceptible to attacks.

Another observation taken from the set of experiment shown in Fig. 9 is that to find the correct key candidate, we need ≈ 7200 traces for the new circuit while this number is decreased to 5200, 4900, and 3700 when the circuit has been used for 2, 5, and 8 weeks, respectively. This observation necessitates revisiting the security of power-equalized cryptographic devices with respect to aging.

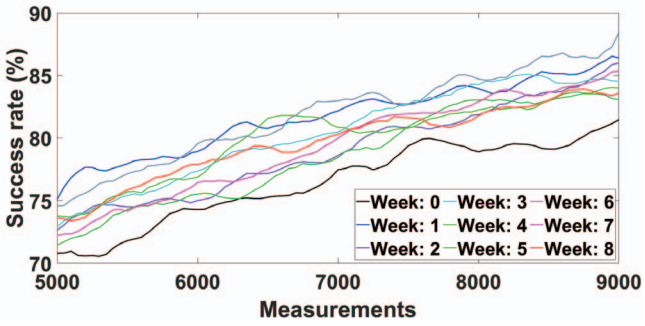


Figure 10: Attack success rate in different aging conditions.

5.3.4 Success rate. We have conducted the above experiment (CPA attack with HW model) on all key nibbles of the cipher, and repeated it 50 times with different sets of 9,000 noisy traces. Figure 10 shows the average success rate of the attack targeting all key nibbles over number of traces. As shown, the new device (shown as week:0) in Fig. 10 is more difficult to attack, e.g., in average success rate ≈ 81.4% with 9,000 traces. However, the success rate of the attack on the 1-week old counterpart with the same number of traces is ≈ 86.4%. These results also confirm that device aging makes the attack easier on SABL circuits.

6 CONCLUSIONS AND FUTURE DIRECTIONS

This paper investigated the impact of transistor aging on the success of power analysis attacks launched on the SABL-protected circuitry of the encryption function of the PRESENT cipher. The SABL scheme, as a dual-rail precharge logic, is a countermeasure used to protect the cryptographic chips against power analysis attacks by equalizing the power consumption of the target circuit regardless of the data being processed. However, as shown in this paper, device aging defeats the purpose of the SABL countermeasure, and results in power consumption imbalances originated from the change of transistor's threshold voltage over time. In this paper, for the first time, we illustrated that such deviation of transistors specification over time can ease the attacks launched on SABL-protected circuits. The experimental results corresponding to CPA attacks with Hamming weight model show that on average the attack's success rate increased over 6.1% (from 81.4% to 86.4%) when targeting a 1-week old device compared to a new one. This observation calls for proper secure implementations of cryptographic circuits that are resilient against power analysis attack over the circuit lifetime regardless of its age.

This paper focused on the dynamic power consumption of the chip to launch the attacks. We will extend this study and focus on the impact of device aging when the attacker exploits the static power of the target SABL-protected circuit for key recovery. As the continuation of this work, we have plans to validate our findings on real silicon by fabricating ASIC chips of SABL-protected circuits and conducting practical experimental investigations.

ACKNOWLEDGMENT

The work described in this paper has been supported in part by the National Science Foundation CAREER Award (NSF CNS-1943224),

and in part by the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation) under Germany's Excellence Strategy - EXC 2092 CASA - 390781972 and through the project 418658052 "Aged but Fit: Long Lasting Security for Trusted Platforms".

REFERENCES

[1] [n.d.]. Nangate 45nm Open Cell Library. "http://www.nangate.com" (accessed May 2019).

[2] Md Toufiq Hasan Anik, Jean-Luc Danger, Sylvain Guilley, and Naghmeh Karimi. 2020. Detecting Failures and Attacks via Digital Sensors. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems (TCAD)* (2020). https://doi.org/10.1109/TCAD.2020.3020921

[3] Md Toufiq Hasan Anik, Sylvain Guilley, Jean-Luc Danger, and Naghmeh Karimi. 2020. On the Effect of Aging on Digital Sensors. In *2020 33rd International Conference on VLSI Design and 2020 19th International Conference on Embedded Systems (VLSID)*. 189–194.

[4] Andrey Bogdanov, Lars Knudsen, Gregor Leander, Christof Paar, Axel Poschmann, Matthew J. B. Robshaw, Yannick Seurin, and C. Vikkelsoe. 2007. PRESENT: An ultra-lightweight block cipher. In *Cryptographic Hardware and Embedded Systems (CHES)*. 450–466.

[5] Éric Brier, Christophe Clavier, and Francis Olivier. 2004. Correlation Power Analysis with a Leakage Model. In *Cryptographic Hardware and Embedded Systems (CHES)*. 16–29.

[6] Daniël Kraak et al. 2018. Device aging: A reliability and security concern. In *European Test Symposium (ETS)*. 1–10.

[7] Anteneh Gebregiorgis, Mojtaba Ebrahimi, Saman Kiamehr, Fabian Oboril, Said Hamdioui, and Mehdi B Tahoori. 2015. Aging mitigation in memory arrays using self-controlled bit-flipping technique. In *Asia and South Pacific Design Automation Conf. (ASP–DAC)*. 231–236.

[8] Naghmeh Karimi, Jean-Luc Danger, Sylvain Guilley, and Florent Lozac'h. 2016. Predictive aging of reliability of two delay PUFs. In *Security, Privacy, and Applied Cryptography Engineering (SPACE)*. 213–232.

[9] Naghmeh Karimi, Sylvain Guilley, and Jean-Luc Danger. 2018. Impact of Aging on Template Attacks. In *Great Lakes Symp. on VLSI (GLSVLSI)*. 455–458.

[10] Naghmeh Karimi, Arun Karthik Kanuparthi, Xueyang Wang, Ozgur Sinanoglu, and Ramesh Karri. 2015. MAGIC: Malicious Aging in Circuits/Cores. *ACM Trans. on Architecture and Code Optimization (TACO)* 12, 1 (2015), 5:1–5:25.

[11] Naghmeh Karimi, Thorben Moos, and Amir Moradi. 2019. Exploring the Effect of Device Aging on Static Power Analysis Attacks. *Cryptographic Hardware and Embedded Systems (CHES)* 2019, 3 (2019), 233–256.

[12] Seyab Khan, Nor Zaidi Haron, Said Hamdioui, and Francky Catthoor. 2011. NBTI Monitoring and Design for Reliability in Nanoscale Circuits. In *2011 IEEE International Symposium on Defect and Fault Tolerance in VLSI and Nanotechnology Systems (DFTS)*. 68–76.

[13] K. K. Kim. 2015. On-Chip Delay Degradation Measurement for Aging Compensation. *Indian J. of Science and Technology* 8, 8 (2015), 777–782.

[14] Paul Kocher, Joshua Jaffe, and Benjamin Jun. 1999. Differential Power Analysis. In *Int'l Cryptology Conf. (CRYPTO)*. 388–397.

[15] Daniël Kraak, Innocent Agbo, Mottaqiallah Taouil, Said Hamdioui, Pieter Weckx, Stefan Cosemans, and Francky Catthoor. 2019. Hardware-based aging mitigation scheme for memory address decoder. In *European Test Symposium (ETS)*. 1–6.

[16] Yongho Lee and Taewhan Kim. 2011. A fine-grained technique of NBTI-aware voltage scaling and body biasing for standard cell based designs. In *Asia and South Pacific Design Automation Conf. (ASP–DAC)*. 603–608.

[17] François Macé, François-Xavier Standaert, and Jean-Jacques Quisquater. 2007. Information Theoretic Evaluation of Side-Channel Resistant Logic Styles. In *Cryptographic Hardware and Embedded Systems (CHES)*. Springer, 427–442.

[18] Stefan Mangard, Elisabeth Oswald, and Thomas Popp. 2006. *Power Analysis Attacks: Revealing the Secrets of Smart Cards*. Springer. ISBN 0-387-30857-1.

[19] Iraj Moghaddasi, Arash Fouman, Mostafa E Salehi, and Mehdi Kargahi. 2018. Instruction-Level NBTI Stress Estimation and Its Application in Runtime Aging Prediction for Embedded Processors. *IEEE Trans. on Computer-Aided Design of Integrated Circuits and Systems (TCAD)* 38, 8 (2018), 1427–1437.

[20] Fabian Oboril and Mehdi B. Tahoori. 2012. ExtraTime: Modeling and analysis of wearout due to transistor aging at microarchitecture-level. In *Dependable Systems and Networks (DSN)*. 1–12.

[21] Thomas Popp, Mario Kirschbaum, Thomas Zefferer, and Stefan Mangard. 2007. Evaluation of the Masked Logic Style MDPL on a Prototype Chip. In *Cryptographic Hardware and Embedded Systems (CHES)*. 81–94.

[22] Thomas Popp and Stefan Mangard. 2005. Masked Dual-Rail Pre-charge Logic: DPA-Resistance Without Routing Constraints. In *Cryptographic Hardware and Embedded Systems (CHES)*. 172–186.

[23] Md Tauhidur Rahman, Domenic Forte, Jim Fahrny, and Mohammad Tehranipoor. 2014. ARO-PUF: An aging-resistant ring oscillator PUF design. In *Design, Automation Test in Europe (DATE)*. 1–6.

[24] Mathieu Renauld, Dina Kamel, François-Xavier Standaert, and Denis Flandre. 2011. Information Theoretic and Security Analysis of a 65-Nanometer DDSLL AES S-Box. In *Cryptographic Hardware and Embedded Systems (CHES)*. 223–239.

[25] Carsten Rolfes, Axel Poschmann, Gregor Leander, and Christof Paar. 2008. Ultra-lightweight implementations for smart devices–security for 1000 gate equivalents. In *Int'l Conf. on Smart Card Research and Advanced Applications*. 89–103.

[26] François-Xavier Standaert, Tal Malkin, and Moti Yung. 2009. A Unified Framework for the Analysis of Side-Channel Key Recovery Attacks. In *EUROCRYPT*. 443–461.

[27] Daisuke Suzuki and Minoru Saeki. 2006. Security Evaluation of DPA Countermeasures Using Dual-Rail Pre-charge Logic Style. In *Cryptographic Hardware and Embedded Systems (CHES)*. 255–269.

[28] Synopsys. 2016. HSPICE User Guide: Basic Simulation and Analysis.

[29] Kris Tiri, Moonmoon Akmal, and Ingrid Verbauwhede. 2002. A dynamic and differential CMOS logic with signal independent power consumption to withstand differential power analysis on smart cards. In *European solid-state circuits Conf.* 403–406.

[30] Kris Tiri and Ingrid Verbauwhede. 2004. A logic level design methodology for a secure DPA resistant ASIC or FPGA implementation. In *Design, Automation Test in Europe (DATE)*. 246–251.

[31] Kris Tiri and Ingrid Verbauwhede. 2004. Place and route for secure standard cell design. In *Smart Card Research and Advanced Applications VI*. 143–158.

[32] Kris Tiri and Ingrid Verbauwhede. 2005. Design Method for Constant Power Consumption of Differential Logic Circuits. In *Design, Automation and Test in Europe (DATE)*. 628–633.