Does Aging Matter? The Curious Case of Fault Sensitivity Analysis

Mohammad Ebrahimabadi*, Bijan Fadaeinia†, Amir Moradi†, Naghmeh Karimi*
*University of Maryland Baltimore County, United States
†Ruhr University Bochum, Germany
Email:{e127@umbc.edu, bijan.fadaeinia@rub.de, amir.moradi@rub.de, naghmeh.karimi@umbc.edu}

***Abstract*—An adversary with physical access to a cryptographic device may place the device under an external stress such as over-clocking, and under-volting in order to generate erroneous outputs based on which the keys can be retrieved. Among fault-injection attacks, Fault Sensitivity Analysis (FSA) has received considerable attention in recent years as in this attack the adversary does not need to know the faulty output; rather he/she only needs to know whether the injected fault has led to an error or not. Although fault-injection attacks, and in particular FSA, have been extensively studied in literature and a number of countermeasures have been proposed to mitigate these attacks, the impact of device aging on the success of these attacks is still an open question. Due to aging, the specifications of transistors deviate from their fabrication-time specification, leading to a change of circuit's delay over time. In this paper, we focus on the impact of aging in collision timing attacks (one of the strongest variant of FSA attacks). The corresponding results, realized by extensive HSpice simulations, show that the aging-induced impacts can facilitate such an attack. This calls for aging-resilient countermeasures that sustain the security over the lifetime of the cryptographic devices.**

I. Introduction

As the process technology paves its way to very-deep sub-micron technologies, time-dependent degradation of the electrical properties in CMOS circuits becomes more severe. This phenomenon, so-called device aging, results in performance degradation of circuits over time and eventually leads to functional failures [1]. Among aging mechanisms, Bias Temperature-Instability (BTI) and Hot Career Injection (HCI) have received the lion's share of attention considering their dominant effect [2].

Aging jeopardizes device reliability by leading the device to early malfunctions. To address such reliability concerns, different aging-mitigation schemes have been proposed in literature [3, 4, 5]. These schemes mainly prolong device lifetime and postpone aging-related malfunctions via running the device at a lower frequency from the early stage of deployment (guard-banding), enlarging transistors (gate-sizing), leveraging partial recovery of BTI aging effects via injecting healing patterns when the device is idle [6], and so on.

Albeit enhancing the reliability of circuits against aging mechanisms, the aforementioned schemes cannot thoroughly protect the device against aging-induced security threats such as information leakage [7]. In practice, aging mitigation schemes increase the device's Mean Time To Failure (MTTF) but still different parts of the device may experience small, yet different aging-induced change of specification even in the presence of such aging mitigation schemes. This deviation may facilitate leaking sensitive information, in particular in cryptographic devices which face the attacks making use of timing deviations. One such example is Fault Sensitivity Analysis (FSA) proposed in [8]. As another example we can point to the power analysis attacks that benefit from aging-induced imbalances in the supposed-to-be-balanced paths.

The impact of aging on the success of power analysis attacks, in particular in the circuits equipped with dual-rail countermeasures have been studied in recent literature [9], and countermeasures to enhance the security of such circuits when device aging comes into account have been proposed in [10]. However, to the best of the authors' knowledge, there is no study in the open literature that quantitatively discusses how the security of cryptographic devices, that are under fault-injection attacks, can be affected by device aging. Accordingly in this paper, we fill the gap and focus on fault-injection attacks, and in particular FSA. In short, we demonstrate that the attacker can benefit from device aging when revealing the secret key of cryptographic devices via FSA. More precisely, among the FSA attacks we use the Collision Timing Attack (CTA) [8] and investigate how its success is affected when the device is aged.

In general, FSA attacks rely on the dependency between the secret intermediate values and the fault sensitivity of the device, where fault sensitivity refers to a critical condition (e.g., clock frequency or supply voltage) at which faulty outputs begin to appear [11, 12]. As we show in this paper, due to the change of transistors' specifications and in turn the propagation delay of the corresponding gates over the lifetime of the underlying device, the success of the FSA attacks can be affected over time. We discuss this impact in more details in Section III.

In sum, the contributions of this paper are as follows:

- Investigating the impact of aging on the vulnerability of cryptographic devices against FSA attacks, in particular against collision timing attack;
- Developing a simulation framework which integrates device aging into the feasibility assessment of the collision timing attack;
- Conducting detailed HSpice MOSRA simulations to evaluate the effect of BTI and HCI degradation on the success of the launched attacks.

The rest of the paper is structured as follows. Section II discusses the preliminaries on aging mechanisms and their impact on transistors' electrical specification. Fault-injection attacks and their success when device aging comes into account are discussed in Section III. Section IV presents the circuitries

we target in this paper. The setup used for our practical investigations is introduced in Section V followed by the simulation results and discussions. Finally, Section VI concludes the paper and draws the future directions of this research.

II. Aging Mechanisms

Aging mechanisms including Bias Temperature-Instability (BTI), Hot Carrier Injection (HCI), Time Dependent Dielectric Breakdown (TDDB), and Electro-Migration (EM) result in performance degradation and eventual failure of digital circuits over time. The first three mechanisms deal with the gate oxides of transistors, while EM occurs in the interconnect metal lines [13]. Among all aging mechanisms, BTI and HCI are two leading factors in degradation of digital circuits [14].

BTI refers to NBTI (Negative BTI) and PBTI (Positive BTI) mechanisms; both result in 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 can also be considerable.

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-SiO2 interface leading 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 [15]. 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 1 shows the NBTI-induced change of threshold voltage in a PMOS transistor that was under continuous stress during 6 months (always ON) and the one that is alternatively ON and OFF every other month.

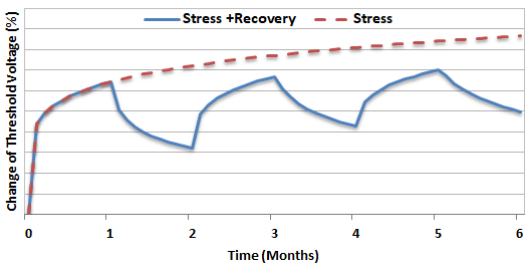


Fig. 1: Threshold-voltage shift of a PMOS transistor under NBTI effect [13]. Values on Y axis are not shown to make the graph generic across different silicon foundries and technological nodes.

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 [16]. HCI is impacted by 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 [14]. HCI, unlike BTI, does not have any recovery phases.

III. Fault Injection Attacks

To recover the secret key of cryptographic devices, an adversary may benefit from injecting transient faults in the target circuit by over-clocking, under-volting, electromagnetic perturbation or laser exposure. In this paper, we target the faults injected by over-clocking the circuit. Such faults can result in setup-time violations; generating erroneous outputs.

Fault-injection attacks can be categorized into two main groups. The first group includes the attacks that rely on the value of the erroneous outputs. Differential Fault Analysis (DFA) [17] is among such attacks. However, for the second group, e.g., FSA [18], the faulty output value is not required, and the adversary only needs to know whether the injected fault has led to an error or not. Indeed, in FSA attacks the adversary exploits the dependency between the secret intermediate values and the time requires by a combinational circuit to compute the output with respect to the given input.

Device aging is not expected to change the effect of over-clocking-injected faults on erroneous results of the circuit. Thereby, the success of DFA attacks should not be impacted by aging. However, the situation is different for FSA attacks, as the success of such threats highly depends on the delay measurements carried out during the attack, and these delays in turn are subject to change by device aging over the device lifetime. As the magnitude of the aging-induced delay change for each gate depends on its type and workload, different gates embedded in the underlying circuit may experience different aging degradation. This, in turn, can affect the success of the FSA attacks, on which we mainly focus in this paper.

Collision Timing Attack (CTA): This attack, presented in [8], is based on linear collision concept. This refers to the case in which two instances of the same block in a circuit process the same value. The underlying idea lies on the fact the propagation time of different S-Box instances embedded in the circuit are very similar when they are fed with the same inputs. The propagation time refers to the time required for the S-Box output to get stable since its inputs changed. This attack reveals the linear difference between the keys associated to two different S-Boxes; thus, after successfully accomplishing this attack, by guessing the key of one S-Box, the other key portions can be recovered.

Assume that a round-based implementation of Advanced Encryption Standard (AES-128) encryption function is attacked at the 10-th cipher round. As this round does not include MixColumns, the propagation time between its input and output is mainly the propagation time of the S-Boxes followed by last Key-XOR. To perform CTA at this round exemplary targeting S-Box$_1$ and S-Box$_2$, first the timing characteristic of S-Box$_1$ is extracted as $T_1^o = \langle PT_1^0, \ldots, PT_1^{255} \rangle$ where PT_1^y denotes the propagation time of S-Box$_1$ followed by a Key-XOR with k_1 when producing the value y at its output. Similarly,

$T_2^o = \langle PT_2^0, \ldots, PT_2^{255} \rangle$ represents the timing characteristics of S-Box$_2$ followed by a Key-XOR with k_2, where PT_2^y stands for propagation time when the corresponding output is y. Then, CTA applies the correlation between T_1^o and different permutations of and $T_2^{o \oplus \Delta k}$ for all possible value guesses of $\Delta k = k_1 \oplus k_2$. When propagation times are measured with enough accuracy, Δk with maximum correlation should denote the most probable keys difference.

Measuring the Propagation Time: In order to extract the propagation time of the targeted S-Box to fill e.g., T_1^o, first a nominal clock period at which the circuit operates properly is considered. Then, the clock period is gradually decreased (by means of a clock glitch) until an erroneous value on the corresponding output is observed. The minimum clock period leading to a correct output is then taken as the propagation time for the corresponding fault-free output value. This process is repeated for all 256 possible output values to fully fill T_1^o. Note that the same processes should be conducted for all targeted S-Boxes, i.e., all $T_{1 \leq i \leq 16}^o$. Figure 2 shows an example leading to the conclusion that the corresponding propagation time is 12.4 ns.

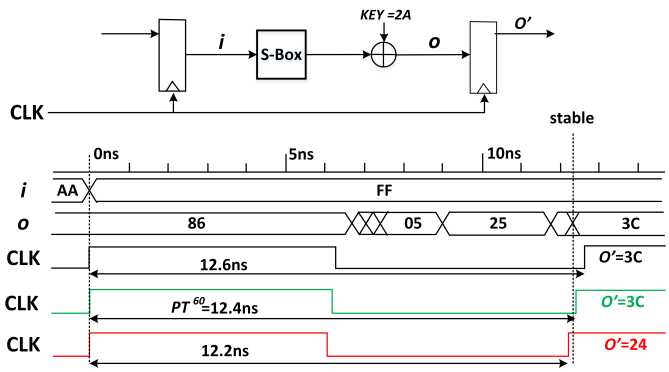


Fig. 2: A sample of extracting propagation time [8].

IV. Targeted Architectures

The AES is a block cipher with 128-bit blocks and three different key lengths of 128, 192, and 256 bits. AES-128 includes 10 rounds where all rounds except the last one consists of four operations: SubBytes (S-Box), ShiftRows, MixColumns, and AddRoundKey. The last round (round 10) misses MixColumns but includes the other three operations.

Here, we mainly target the S-Box module, since it is the most interesting target for the adversaries due to its high algebraic degree and the involvement of the secret key right before and right after its application, at the first and last encryption rounds respectively. In particular, we target three implementations of S-Box explained below.

Normal S-Box: We refer to the implementation proposed by Canright in [20] as "Normal S-Box". This is a compact implementation of AES S-Box realized through multi-level representation of arithmetic in $GF(2^8)$. The low-area overhead of this implementation makes it a suitable option specially for ASIC applications.

PPRM1 S-Box: Morioka et al. proposed a low-power architecture for the AES S-Box called Positive Polarity Reed-Muller (PPRM) at CHES 2002 [21]. Their basic structure consists of a leading AND plane (an array of AND gates) followed by an XOR plane as depicted in Figure 3. To reduce the power consumption, this implementation tries to avoid dynamic hazards as much as possible. To do so, the circuit is implemented such that all gates receive their entire inputs simultaneously (more precisely, as close as possible in time). This can be achieved if all inputs of each gate are in the same logical depth with respect to the primary inputs.

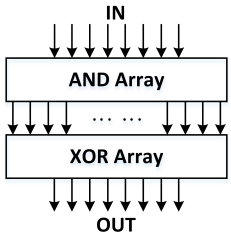


Fig. 3: Structure of PPRM1 S-Box [18].

PPRM3 S-Box: To reduce the large area overhead of PPRM1; owing to its 2-level circuitry, PPRM3 has been proposed in [21]. The PPRM3 S-Box, shown in Figure 4, is a multi-stage PPRM that is compact has low-power consumption. As shown, the three sub-components are included in PPRM3 (i.e., pre-inversion, inversion, and post-inversion), each of which is built upon an AND plane followed by an XOR plane.

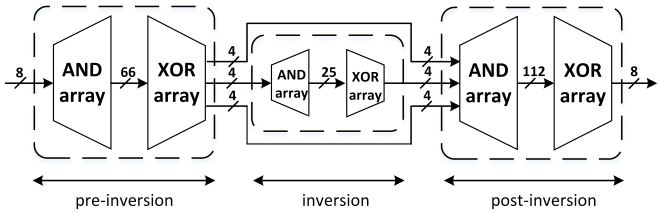


Fig. 4: Structure of PPRM3 S-Box [21].

V. Practical Results and Discussions

A. Setup

In this research, we implemented round 10 of the AES-128 encryption function with three different S-Box architectures whose details are given in Section IV. Each implementation includes 16 S-Box modules, while each one contributes in computation of a ciphertext byte.

These circuits are implemented at the transistor level using 45 nm Nangate technology [22]. For transistor-level simulations, we used Synopsys HSpice and the built-in HSpice MOSRA Level 3 model to evaluate the impact of NBTI and HCI aging In order to realize process variations in our target circuits, we considered Gaussian distribution for transistor gate length L: $3\sigma = 10\%$, threshold voltage V_{TH}: $3\sigma = 30\%$, and gate-oxide thickness t_{OX}: $3\sigma = 3\%$. The circuits are then simulated for the supply voltage of 1.2 V and at the temperature of $105\,^{\circ}C$ for different aging durations up to 7

years of operation in steps of one year. During the course of aging, all 16 S-Boxes are fed with randomly generated inputs, thus experiencing different aging-induced stress rate.

At each aging stage, following the procedure explained in Section III, we extracted the propagation time of each S-Box module followed by a Key-XOR for all possible output values. More precisely, we collected PT_i^o for possible output values $o \in \{0, \ldots, 255\}$ and all S-Box modules $1 \leq i \leq 16$ as the minimum clock period required to generate the correct output. In our simulations with Vdd=1.2 V, we considered logical value of '1' for the signals with the voltages beyond 1 V, and the logical value of '0' for the signals with the voltages below 0.2 V. The value is considered as unstable if its voltage is in the range of (0.2 V, 1 V). Figure 5 shows an example where the correct output is '1'. Here, the propagation time is 300 ps.

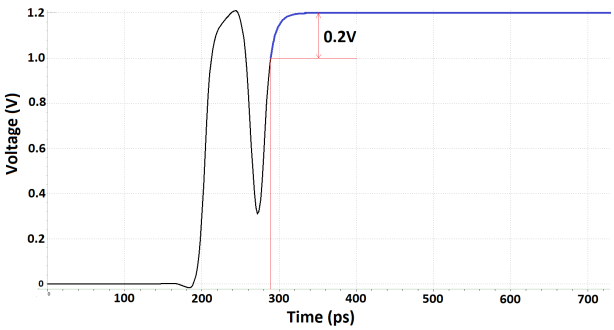
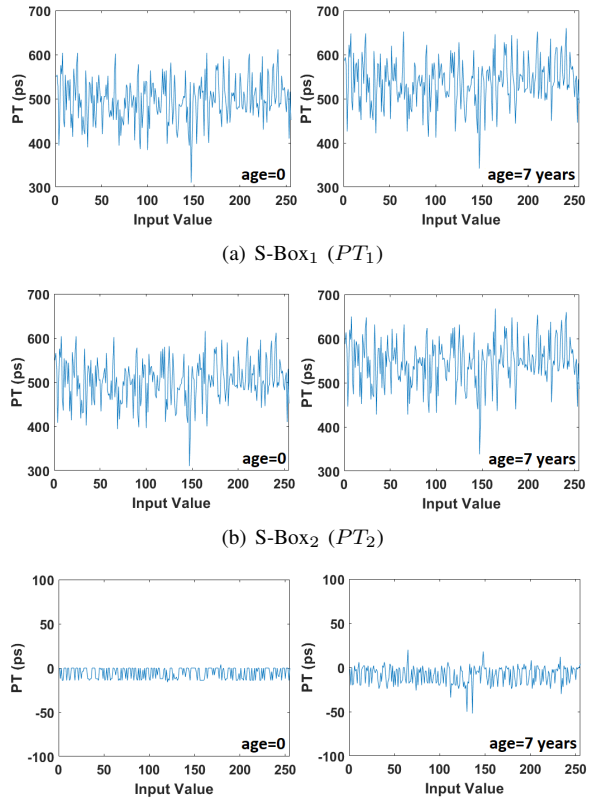


Fig. 5: Propagation time of the S-Box's LSB output when the S-Box is fed with 0xA9.



(a) S-Box$_1$ (PT_1)

(b) S-Box$_2$ (PT_2)

(c) PT_1 - PT_2

Fig. 6: The effect of aging on the propagation time of S-Box$_1$ and S-Box$_2$ when device is fresh and 7-year old.

B. Results and Discussions

1) Effect of Aging on the Propagation Time: The first set of the results depicts the impact of aging on the propagation time of the S-Boxes. We compare two PPRM3 S-Boxes (among the 16 instances); so-called S-Box$_1$ and S-Box$_2$. Figure 6(a) shows the measured propagation time of S-Box$_1$ when it is fresh (not aged) as well as when it has been used for 7 years. As expected, the S-Box propagation time increases during the course of aging. A similar trend, yet with a slight different rate, is observed in Figure 6(b) for S-Box$_2$, e.g., for the input value of 0x93, the propagation time of S-Box$_1$ and S-Box$_2$ are increased from 310 ps and 309 ps to 342 ps and 338 ps, hence 10.3% and 9.3% increase, respectively.

Another observation that can be made from this set of experiment is the deviation of propagation delays of different paths in these S-Boxes from each other after the course of aging. As will be shown in the next set of results, such deviation will ease the CTA attack. Figure 6(c) shows the difference in propagation delays of S-Box$_1$ and S-Box$_2$ in a new device (left) versus a 7-year old device(right). As depicted, such difference is in the range of [-16ps,4ps] and [-52ps,20ps] for new and 7-year old devices, respectively.

Note that the difference in the propagation delay of different S-Box instances for a fresh device is due to the intra-die process variations occurring in the manufacturing process. This difference between propagation times is augmented during the course of aging as each S-Box module may receive a different set of inputs and the workload during the aging period (usage time) in turn affecting the aging rate.

2) Mutual Information: In this research the propagation times are captured in simulation environment, i.e., noise free measurements. To mimic a real-silicon experimental setup, we artificially added noise with Gaussian distribution to the extracted propagation time values, and assessed the susceptibility of attacks on the underlying circuit to the noise level using the Mutual Information (MI) metric; an information theoretic analysis scheme presented in [23] and applied, e.g., in [24, 25]. In this analysis, it is supposed that the noise follows a Gaussian distribution centered to each extracted propagation time. Hence, MI is estimated by means of conditional entropy using Equation (1) where L denotes the leakages (propagation time of S-Box) and S is the selected intermediate value (in our case: the S-Box output). The conditional entropy (i.e., H[$S|L$]) can be estimated using Equation (2).

$$I(S;L) = H[S] - H[S|L] \tag{1}$$

$$H[S|L] = -\sum_s Pr[s] \int Pr[l|s] \times \log_2 Pr[s|l] dl \tag{2}$$

This analysis extracts a curve for mutual information between propagation delays and the S-Box output over the standard deviation of a Gaussian noise. It estimates the amount of noise required to avoid the exploitability of leakages. To perform such analysis, we targeted a single S-Box of each

architecture, and obtained the estimated MI while increasing the noise standard deviation.

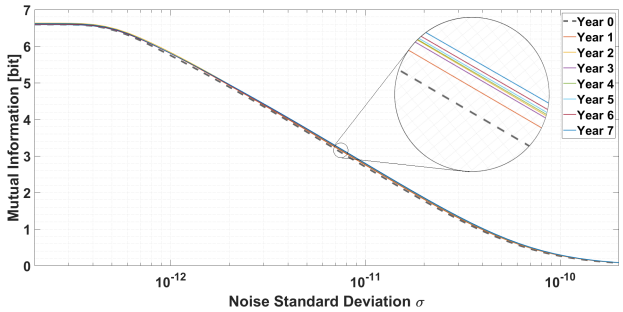


Fig. 7: Mutual Information curves associated to normal S-Box output for different aging durations.

Figure 7 demonstrates the MI for normal S-Box. As depicted, the MI drops with higher amount of noise when the circuit is aged. We highlight a zoomed part of the figure for the sake of clarity. As shown, the aged circuits have higher mutual information compared to a fresh device; thereby, higher amount of noise is required to hide the leakage in case of the aged circuits. The mutual information associated to PPRM1 and PPRM3 S-Boxes are shown in Figure 8 and Figure 9, respectively. Both circuits follow the same trend as described for the normal S-Boxes, i.e., aging is expected to increase the susceptibility of devices to FSA attacks.

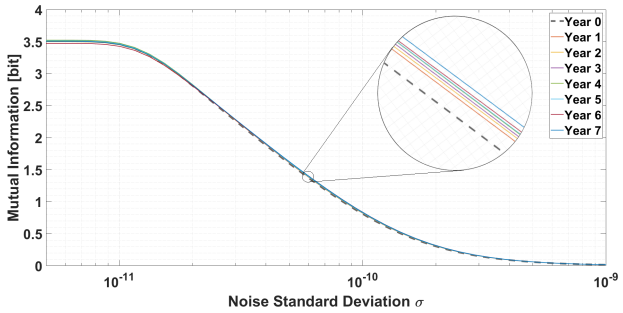


Fig. 8: Mutual Information curves associated to PPRM1 S-Box output for different aging durations.

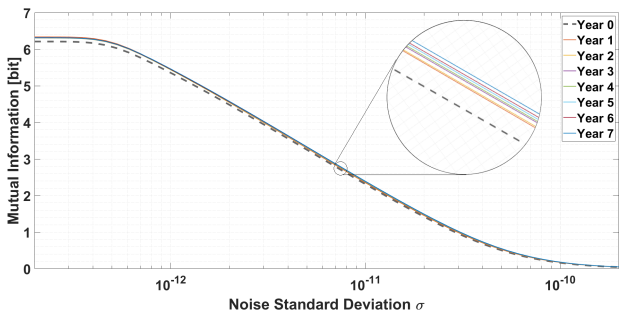
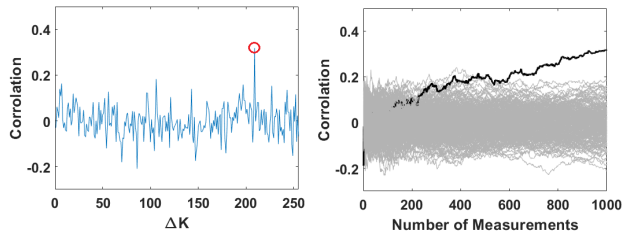
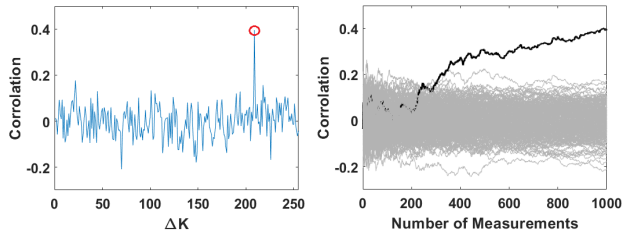


Fig. 9: Mutual Information curves associated to PPRM3 S-Box output for different aging durations.

3) Attack: The next set of results shows the effect of aging and noise on the required number of measurements to reveal the correct Δk. Similar to real-silicon attacks where we need to repeat a measurement several times to mitigate noise effects, in our simulations we artificially added Gaussian noise to each extracted propagation time value 1000 times, hence generating 1000 noisy measurements per S-Box output followed by a Key-XOR (totally 256,000 values). We performed this process on the propagation time of the fresh PPRM3 circuit as well as the 7-year old one. After performing the CTA attack (as explained in Section III) on such noisy measurements of two S-Box modules, we obtained the correlation curves presented in Figure 10. The other designs (i.e., normal and PPRM1 S-Boxes) show a very similar result; all confirming that aging can help the adversary in attacking the device via CTA. In particular, as Figure 10 depicts, for a fresh device it takes around 600 measurements to recover the secret. This number is decreases to 350 for a 7-year old device. This confirms that less effort is required to attack aged devices compared to the fresh ones.



(a) Age = 0



(b) Age = 7 years

Fig. 10: Result of the attack on the last round of AES recovering Δk between key bytes of the targeted S-Box modules on a fresh and a 7-year old circuit; (left) using 1000 measurements and (right) over the number of measurements.

4) Success Rate: This set of results investigates the success rate of CTA attack targeting our three S-Box architectures in different aging durations. We have conducted the above explained attack while artificially adding Gaussian noise with 4 different standard deviations σ. We further repeated each experiment 100 times for each of the considered noise level and report the average corresponding success rates, i.e., the number of key bytes which are correctly revealed. Figure 11 shows the results targeting all key bytes for the normal S-Box architecture. As depicted, in lower noise levels ($\sigma = 36 \times 10^{-12}$ and $\sigma = 72 \times 10^{-12}$), the success rate is 100% regardless of aging duration. However, the aging effect is observable in higher noise levels, i.e., the attack has a higher success rate in aged devices compared to the fresh one. For example, as shown in Figure 11, when $\sigma = 144 \times 10^{-12}$, the success rate is dropped drastically in both new and aged devices, yet with different rates, i.e., the success rate is 47% for a fresh device, while 60% when the device is aged for 7 years.

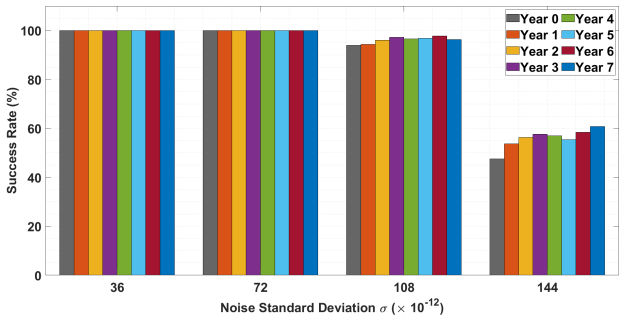


Fig. 11: Attack success rate in different aging durations for normal S-Box.

We repeated the above experiment for PPRM1 and PPRM3 S-Box architectures. As shown in Figure 12, the success rate of the attack on PPRM1 is 100% for all new and aged devices for $\sigma = 100 \times 10^{-12}$. However, for higher noise levels aged devices are more vulnerable to CTA than the fresh one. Here, the success rate of CTA targeting a 7-year old PPRM1 circuit is 18.2% for $\sigma = 400 \times 10^{-12}$ yet 14.2% for a fresh device. PPRM3 module follows a very similar trend where the CTA success rate is increased by aging for higher noise levels. The takeaway point from these observations is that aging can facilitate the CTA attack, increasing the success of the attack through its course of usage.

Note that – compared to the other 2 architectures – different noise levels have been considered for PPRM1 circuit. This is due to the difference in their critical path delay that results in different range of propagation times. In our experiments the critical path delay for PPRM1 is approximately 2500 ps while it is 7 00ps for both normal S-Box and PPRM3 architectures.

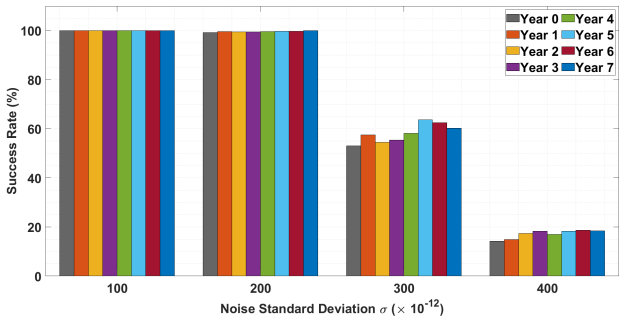


Fig. 12: Attack success rate in different aging durations for PPRM1 S-Box.

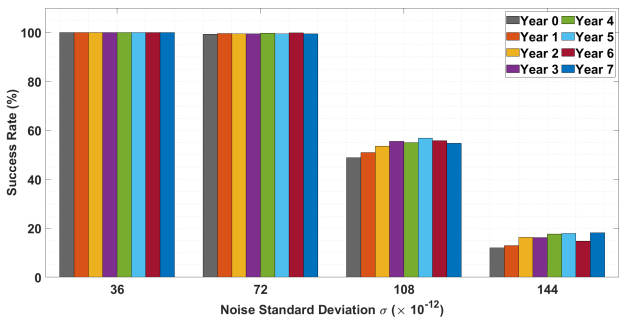


Fig. 13: Attack success rate in different aging durations for PPRM3 S-Box.

VI. Conclusions and Future Directions

In this paper, we investigated the impact of device aging on the success of fault sensitivity analysis attacks, and in particular collision timing attacks, launched on three known implementations of the AES S-Box. By means of HSpice simulations, we quantitatively showed that the aging-induced deviation of the transistors' specification over time can be beneficial when recovering the secrets by collision timing attacks. We plan to extend this study by real-silicon experiments and develop aging-resilient countermeasures that remain secure during the course of usage.

Acknowledgments

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) through the Germany's Excellence Strategy under Grant EXC 2092 CASA-390781972 and the Project "Aged but Fit" under Grant 418658052.

References

[1] M. Ebrahimi and Z. Navabi, "Selecting representative critical paths for sensor placement provides early FPGA aging information," *TCAD*, vol. 39, no. 10, pp. 2976–2989, 2019.
[2] D. Sengupta and S. S. Sapatnekar, "Estimating circuit aging due to BTI and HCI using ring-oscillator-based sensors," *TCAD*, vol. 36, no. 10, pp. 1688–1701, 2017.
[3] M. S. Mispan, M. Zwolinski, and B. Halak, "Ageing mitigation techniques for SRAM memories," in *Ageing of Integrated Circuits*, 2020, pp. 91–111.
[4] B. Khaleghi et al., "Estimating and mitigating aging effects in routing network of FPGAs," *TVLSI*, vol. 27, no. 3, pp. 651–664, 2019.
[5] C.-L. Hsu, "Layout-dependent aging mitigation for critical path timing," in *ASP-DAC*, 2018, pp. 153–158.
[6] N. Karimi, A. K. Kanuparthi, X. Wang, O. Sinanoglu, and R. Karri, "Magic: Malicious aging in circuits/cores," *ACM Trans. on Architecture and Code Optimization (TACO)*, vol. 12, no. 1, pp. 1–25, 2015.
[7] D. K. et al., "Device aging: A reliability and security concern," in *European Test Symp. (ETS)*, 2018, pp. 1–10.
[8] A. Moradi, O. Mischke, and C. Paar, "One attack to rule them all: Collision timing attack versus 42 AES ASIC cores," *TCOMP*, vol. 62, no. 9, pp. 1786–1798, 2012.
[9] M. T. H. Anik, B. Fadaeinia, A. Moradi, and N. Karimi, "On the impact of aging on power analysis attacks targeting power-equalized cryptographic circuits," in *ASP-DAC*, 2021, pp. 414–420.
[10] B. Fadaeinia, M. T. H. Anik, N. Karimi, and A. Moradi, "Masked SABL: A long lasting side-channel protection design methodology," *IEEE Access*, vol. 9, pp. 90 455–90 464, 2021.
[11] S. Endo et al., "A silicon-level countermeasure against fault sensitivity analysis and its evaluation," *TVLSI*, vol. 23, no. 8, pp. 1429–1438, 2015.
[12] A. Moradi, O. Mischke, C. Paar, Y. Li, K. Ohta, and K. Sakiyama, "On the Power of Fault Sensitivity Analysis and Collision Side-Channel Attacks in a Combined Setting," in *CHES*, 2011, pp. 292–311.
[13] N. Karimi, J.-L. Danger, and S. Guilley, "Impact of aging on the reliability of delay PUFs," *Journal of Electronic Testing*, vol. 34, no. 5, pp. 571–586, 2018.
[14] F. Oboril and M. B. Tahoori, "Extratime: Modeling and analysis of wearout due to transistor aging at microarchitecture-level," in *Dependable Systems and Networks*, 2012, pp. 1–12.
[15] S. Khan, N. Z. Haron, S. Hamdioui, and F. Catthoor, "NBTI monitoring and design for reliability in nanoscale circuits," in *DFTS*, 2011, pp. 68–76.
[16] M. T. Rahman, D. Forte, J. Fahrny, and M. Tehranipoor, "ARO-PUF: An aging-resistant ring oscillator PUF design," in *DATE*, 2014, pp. 1–6.
[17] E. Biham and A. Shamir, "Differential Fault Analysis of Secret Key Cryptosystems," in *CRYPTO*, vol. 1294, 1997, pp. 513–525.
[18] Y. Li et al., "Fault Sensitivity Analysis," in *CHES*, vol. 6225, 2010, pp. 320–334.
[19] Y. Fei et al., "A statistics-based success rate model for DPA and CPA," *Journal of Cryptographic Engineering*, vol. 5, no. 4, pp. 227–243, 2015.
[20] D. Canright, "A very compact s-box for AES," in *CHES*, 2005, pp. 441–455.
[21] S. Morioka and A. Satoh, "An optimized s-box circuit architecture for low power AES design," in *CHES*, 2002, pp. 172–186.
[22] "Nangate 45nm open cell library," "http://www.nangate.com", last accessed: Sep. 10, 2021.
[23] F.-X. Standaert, T. G. Malkin, and M. Yung, "A unified framework for the analysis of side-channel key recovery attacks," in *Theory and Applications of Cryptographic Techniques*, 2009, pp. 443–461.
[24] F. Macé, F.-X. Standaert, and J.-J. Quisquater, "Information theoretic evaluation of side-channel resistant logic styles," in *CHES*, 2007, pp. 427–442.
[25] M. Renauld et al., "Information theoretic and security analysis of a 65-nanometer DDSLL AES s-box," in *CHES*, 2011, pp. 223–239.