Impact of Aging on Template Attacks

Naghmeh Karimi
CSEE Department
University of Maryland Baltimore County
nkarimi@umbc.edu

Sylvain Guilley
Secure-IC S.A.S.
LTCI, Télécom ParisTech & ENS
sylvain.guilley@secure-ic.com

Jean-Luc Danger
LTCI, Télécom ParisTech
Secure-IC S.A.S.
danger@telecom-paristech.fr

ABSTRACT

Template attack is the most powerful side-channel attack from an information theoretic point of view. This attack is launched in two phases. In the first phase (training) the attacker uses a training device to estimate leakage models for targeted intermediate computations, which are then exploited in the second phase (matching) to extract secret information from the target device. Process variation and discrepancy of operating conditions (e.g., temperature) between training and matching phases adversely affect the success probability of the attack. Attack-success degradation is exacerbated when device aging comes into account. Due to aging, electrical specifications of transistors change over time. Thereby, if the training and target devices have experienced different usage time, the attack will be more difficult. Aging alignment between training and target devices is difficult as aging degradation is highly affected by operating conditions and technological variations. This paper investigates the effect of aging on the success rate of template attacks. In particular, we focus on NBTI and HCI aging mechanisms. We mount several attacks on the PRESENT cipher at different temperatures and aging times. Our results show that the attack is more difficult if there is an aging-duration mismatch between the training and target devices.

ACM Reference Format:
Naghmeh Karimi, Sylvain Guilley, and Jean-Luc Danger. 2018. Impact of Aging on Template Attacks. In *GLSVLSI '18: 2018 Great Lakes Symposium on VLSI, May 23–25, 2018, Chicago, IL, USA.* ACM, New York, NY, USA, 4 pages. https://doi.org/10.1145/3194554.3194638

1 INTRODUCTION

With the aggressive scaling of VLSI technology, various design robustness concerns continue to arise. Among them, aging effects in CMOS devices are one of the major challenges in nanotechnologies. Due to aging, electrical behavior of transistors deviates from its original behavior. This deviation degrades performance; and consequently, the chip fails to meet some of the required specifications [1]. Among aging mechanisms, due to their critical role in urging circuits malfunctions, Negative-Bias Temperature-Instability (NBTI), Hot-Carrier Injection (HCI), and gate Oxide Breakdown (OB) have received the lion's share of attention [2]. Guard-banding, gate-sizing, and voltage tuning are among the methods used in industry to reduce the aging effects. 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 [3]. Thereby, aging effects cannot be thoroughly prevented.

Aging mitigation is critical not only from device reliability point of view but also regarding device security perspectives. With the increasingly reliance on integrated circuits, it is essential to assure the security of the sensitive tasks performed by these circuits and to guarantee the security of information stored within these devices. In practice, any device that contains a secret data such as a cryptographic key can be targeted by an adversary. Cryptographic cores are used to protect various devices but their physical implementation can be compromised by adversaries via observing dynamic circuit emanations in order to extract the secrets they conceal [4].

Breaking cryptographic secrets by exploiting physical information while a device is processing sensitive data is known as side-channel attack [4]. 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 secret information by considering the dependency of this leakage and the secret data. In particular, power analysis attacks analyze the device power consumption to extract the secret information.

Differential power analysis (DPA), correlation power analysis (CPA), mutual information analysis (MIA), and template attacks are the most common power analysis attacks [4–7]. The first three are categorized as non-profiling attacks, as they do not need device characterization before launching the attack, while template attack is a profiling attack that includes a characterization step in which the templates are computed on a training device, and an attack step in which the templates are used to extract the secret data of the target device.

Due to the strength of template attacks in leaking information, in this paper we focus on these attacks and investigate the effect of device aging on their success. As mentioned, due to the aging, electrical specifications of transistors such as their threshold voltage deviate from their original one and thereby power traces change accordingly. If the power traces deployed in the profiling phase of the template attack have been extracted from a new (non-aged) device while the attacker tries to retrieve the secret key of a used device, the aging-related deviation of device parameters may result in modeling mismatch. A similar scenario occurs when the profiled and attack devices experience different usage time (aging). Accordingly, for the first time in the scientific literature, we investigate the effect of aging on the success of template attacks launched on cryptographic devices. The contributions of this paper are as follows:

- A simulation framework which integrates device aging and its security evaluation against template attacks;
- Detailed HSpice MOSRA simulations to evaluate the effect of NBTI and HCI degradations on the success rate of template attacks launched on the PRESENT cipher.

The rest of this paper is organized as follows. Section 2 presents the backgrounds on aging mechanisms and template attacks. Section 3 motivates this research and argues how the template attack is affected by various mismatch of training and attack devices. Experimental results are presented in Section 4. Conclusions are drawn in Section 5.

GLSVLSI '18, May 23–25, 2018, Chicago, IL, USA

ACM ISBN 978-1-4503-5724-1/18/05…$15.00
https://doi.org/10.1145/3194554.3194638

2 PRELIMINARIES

Background on Aging Mechanisms: Device aging results in performance degradation and eventual failure of digital circuits over time. Among other aging mechanisms, NBTI and HCI are two leading factors in performance degradation of digital circuits. Both mechanisms result in increasing switching and path delays in the circuit under stress, and eventually lead to faster wearout of the system.

NBTI occurs in PMOS transistors. A PMOS transistor experiences two phases of NBTI depending on its operating condition. The first phase (*stress*) occurs when the transistor is "on". In this phase, positive interface traps are generated at the Si-SiO$_2$ interface which lead to an increase of the threshold-voltage (V_{th}) of the transistor. The second phase (*recovery*) occurs when the transistor is "off". In this phase, the V_{th} drift that occurred during the stress phase will partially recover. Physical parameters of a transistor, supply voltage, temperature, and stress time all affect the magnitude of its threshold voltage drift [3]. Figure 1 shows the V_{th} drift of a PMOS transistor that is continuously under stress for 6 months and a transistor that alternates stress/recovery phases every other month. The values on Y axis are not shown to make the graph generic for different technologies.

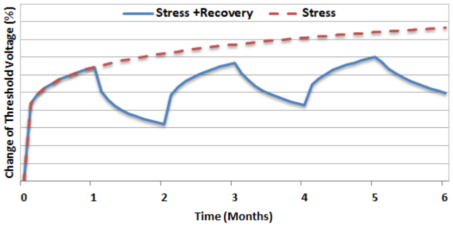

Figure 1: The effect of NBTI aging on a PMOS Transistor.

HCI mainly occurs in NMOS transistors 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 circuit by shifting the threshold-voltage and drain current of transistors under stress. HCI-induced threshold-voltage drift is sensitive to the number of transitions occurring in the gate input of the transistor under stress. HCI effects also depend on the operating temperature [8].

Background on PRESENT Cipher: PRESENT is a lightweight block cipher with 64-bit blocks and a bit oriented permutation layer [9]. It includes 31 rounds and supports two key lengths of 80 and 128 bits. Each encryption round consists of a bitwise XOR operation, a non-linear substitution layer and a linear permutation layer. The non-linear layer uses a single 4-bit S-box which is applied 16 times in parallel in each round [9].

Background on Template Attacks: Side-Channel Attacks (SCA) are mainly launched by adversaries to obtain secret information of a device, e.g., a cryptographic key. These attacks retrieve the secret key by analyzing the physical leakage emitted during operation of a device (e.g., its running time, and power consumption), as this leakage is statistically dependent on the secret key [4]. Profiled SCAs (e.g., template attacks) are the most powerful type of SCAs in which an attacker is able to characterize the leakage of an additional similar device and use the extracted information to break the targeted device.

Template attacks are launched in two phases: training and attack. During training, the attacker has a full control on another copy of the device, and records a large number of traces of the cloned device, corresponding to random values of inputs (plaintexts and keys). These traces are utilized to build a template y_k from the device, using key k. Then, in the attack phase, the recorded traces are classified according to the value of the key and template matching is performed to derive the key value of the target device [7].

In this paper, we aim at studying template attacks in terms of success rate, by analyzing how factors such as aging, temperature and process variation affect them. We consider an ideal setup (for the attacker) where training and attacked devices are otherwise equal, but different in terms of aging, process variations, and temperature. In practice, the actual discrepancy results from a combination of those three (or even more) mismatch factors. We will quantify how these factors contribute in decreasing the success rate of template attacks.

3 AGING-RELATED MISMATCH BETWEEN TEMPLATE AND ATTACK DATA

In side-channel attacks to retrieve the secret data, key-dependent leakage models are compared with actual measurements of the target chip. Thereby, the accuracy of the utilized models highly affects the success of the attack. Although profiling attacks, include an offline learning phase to estimate the leakage model, the profiling method is based on some assumptions (such as Gaussian noise models) or even model estimation can be bounded by the number of measurements during the characterization. Thereby, one of the main challenges in these attacks is to avoid being biased by an incorrect model [10]. In practice, it is hard to reproduce an exact similar operating condition (e.g., temperature) in both profiling and matching phases. Process variations occurring during the manufacturing process also result in discrepancies between profiling and matching chips.

In this research, we focus on a discrepancy that cannot be avoided, i.e., device aging. In practice, it is difficult (if not impossible) to align the age of the profiling and the target devices. One option could be to "accelerate aging" in the younger device (whether it is the profiling or the target one) by artificial aging (e.g., placing the chip in a climate chamber to accelerate aging). However, as aging degradation rate changes exponentially with the drift of operating conditions [3], a slight deviation in the input parameters strongly impacts the acceleration rate. Thereby, it is interesting to quantify how much the security is impacted by the unavoidable effect of aging. In this paper, we study the impact of aging on the success of the template attack.

4 RESULTS AND DISCUSSIONS

4.1 Experimental Setup

We implemented the add-round-key and S-box operations in the first round of the PRESENT cipher with 80-bit keys. Our implementation represents the most compact S-box architecture presented in [11, §3].

The circuit has been implemented in the transistor level using 45-nm NANGATE technology [12]. We used Synopsys HSpice for the transistor-level simulations and deployed the HSpice built-in MOSRA Level 3 model to assess the effect of NBTI and HCI aging [13]. Power traces were extracted for a new device as well as aged devices. The effect of aging was evaluated for 20 weeks of device operation in time steps of one week, in different operating temperatures. As each S-box module in the PRESENT cipher has $n = 4$ input bits, we have a total of $2^{2n} = 256$ input transitions in the S-box. All of these transitions were considered in the profiling phase of the template attacks. The simulated traces contain two parts: the results of key addition and S-box outputs for each initial n-bit value as well as its following n-bit value. For the attack, we considered only the second clock cycle, when the cryptographic circuit transitions from *initial* to *final* value. Cryptographic functions, by essence, randomize the data they manipulate. Therefore, it is natural that in "steady cruising

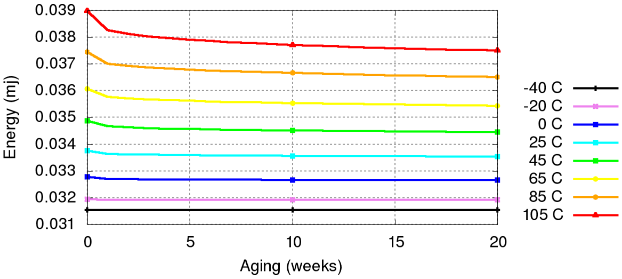

Figure 2: Average energy of S-box for different temperatures and aging.

speed" all possible transitions are considered with equal probability of 2^{-2n} ($1/256$ when $n=4$). The actual order of the transitions has no real impact as long as all transitions are asymptotically equiprobable.

4.2 Experimental Results

4.2.1 Impact of aging on the average energy consumption in S-box. The first set of results deals with the effect of aging on the energy consumed to compute S-box outputs. In this experiment, we first performed HSpice simulations using all 256 input transitions and recorded the instantaneous power consumption related to each input transition over time. We repeated the simulations for different temperatures and aging times. Then, we evaluated the average energy consumption of S-box using the recorded values. Fig. 2 depicts the distribution of average energy consumption in S-box for different temperatures. As expected, the average energy consumption decreases over time. This is because aging results in the increase of the threshold-voltage of transistors under stress and thus in the decrease of the drain current through them. The degradation is more visible in the first few weeks of device operation. Moreover, the increase of temperature results in more energy consumption. The take away points of this observation is that due to the aging the power traces change over time and accordingly, profiling attacks such as template attacks need to consider aging effects while profiling/matching is conducted.

4.2.2 Impact of aging on the attack success rate. This set of results investigates the effect of aging on the success of the template attack. In this experiment, profiling and attack temperatures were equal. However, the training traces were gathered from a fresh device (i.e., 0 week aging shown as 0w in Fig. 3), while attack was mounted on an aged device. We extracted the results for the devices that experienced aging in the range of 0 and 20 weeks (shown as 0w to 20w in the figure). As our HSpice simulations with MOSRA do not consider any noise, to realize the experiments, we added some level of noise in our analysis.

Figure 3 shows the Success Rate (SR) of attacks when the temperature is 105°C and $\sigma = 0.032$ where σ denotes the standard deviation of the noise considered in our analysis. Note that we considered a large amount of noise compared to the signals (with standard deviation $\approx 150\ \mu$W), resulting in signal-to-noise ratio of ≈ 0.005 (typical value, see [14, Fig. 8 in App. A]). As Fig. 3 shows, the success rate slightly decays with aging, as the attacked circuit becomes older and older with respect to the clone used to build the templates. A zoom around 80% of success rate is shown in Fig. 4(a). As depicted, SR drops fast after one week, and then continues to decrease, albeit at a slower rate.

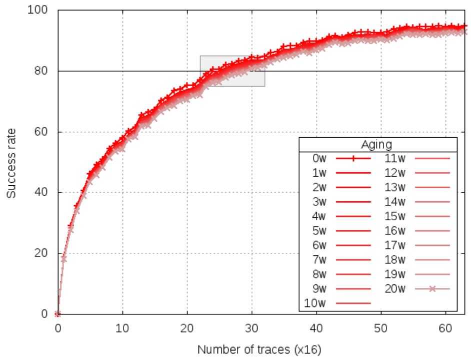

Figure 3: SR after 1000 attacks (Temperature=105°C, $\sigma = 0.032$).

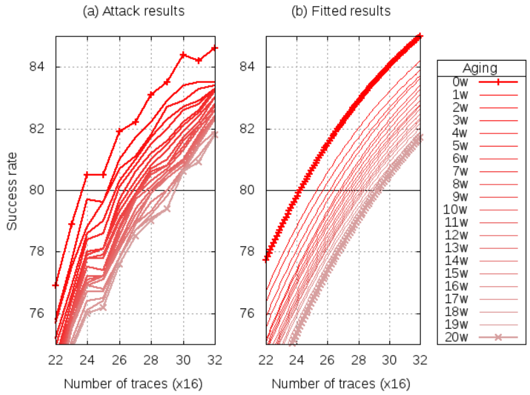

Figure 4: Zoom on the window around SR=80% displayed in Fig. 3, (a) raw data, and (b) fitted data on Eqn. (1).

The value of SR in Fig. 4(a) seems noisy as simulating success rates are prone to estimation errors (though we resorted to 1000 attacks). One common practice in side-channel analysis is to *smooth* the SR curve. However, for more sensible approximation, we consider that empirical SR (Fig. 4(a)) can be fitted by the exponential law shown in Eqn. (1), where q is the number of traces (X-axis in Fig. 3 and 4) and the constant e is the *first order success rate exponent* [15] whose theoretical value can be expressed as a linear function of the signal-to-noise ratio and algorithmic confusion coefficient [16]. In practice, the value of $e \in \mathbb{R}^+$ is extracted by fitting Eqn. (1) to the experimental data.

$$\mathrm{SR} = 1 - \exp(-e \times q) \tag{1}$$

The law (1) can be interpreted as follows: to increase the success rate of an attack from 90% to 99% (resp. from 99.0% to 99.9%), twice number of traces is needed. Fig. 4(b) shows the result of fitting to Eqn. (1), using linear regression.

Fig. 5 compares the number of traces needed to reach the success rate of 80% for the attacks launched in 65°C and 105°C. In both cases the number of traces to attain 80% success is increasing fast in the first week of aging, and then it grows with a slower rate. The results depict that temperature increase makes the attack more difficult. In particular, **the number of traces required to break the key with probability of 80% in 105°C will increase $\approx 25\%$ after 20 weeks.** Note that in each case, the number of traces is 16 times of the Y-ordinate. To highlight the effect of aging and avoid mismatches caused by process variation, we do not consider process variation in this figure.

To mitigate deviations between profiling and matching phases, template normalization has been proposed in literature [17] where both 2^n templates $\hat{p}$ (for all the values of the key) and 2^n online distributions $\tilde{p}$ are transformed by homothety such that they have the same *zero mean* and *unit variance*. The next set of results shows how normalization affects the success of template attack when there is an aging mismatch between profiling and matching devices. In Fig. 6 the template device is new while the target device is 20 week old. As shown, normalization slightly helps to improve the attack via reducing the number of traces, but does not impact our conclusions.

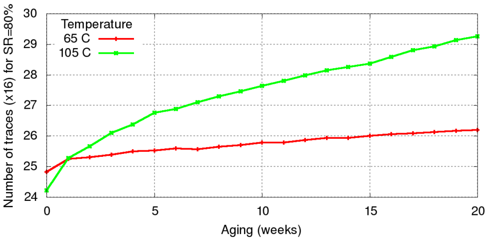

Figure 5: Mean number of traces to reach SR=80% **(**$\sigma = 0.032$**).**

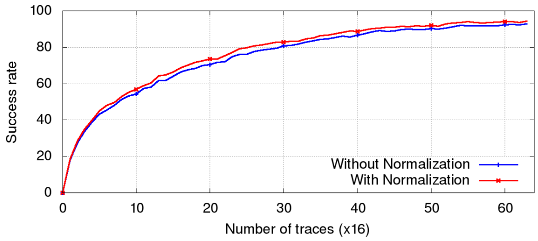

Figure 6: SR after 1000 attacks with and without applying normalization [17] (Temperature=105°C, $\sigma = 0.032$**).**

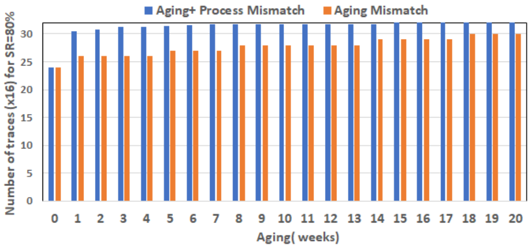

Figure 7: Mean number of traces to reach SR=80% **with and without process variations (temperature:** 105°C**,** $\sigma = 0.032$**).**

In particular, **via normalization, the number of traces required to break the key with probability of 80% decreases** ≈ 16% **when there is a 20 week aging mismatch and temperature is 105°C**.

4.2.3 Impact of process mismatch. Figure 7 compares the number of traces required to attain 80% success when both aging and process variations are considered with the case when only aging is considered. Simulations were carried out using a Gaussian distribution: transistor gate length L: $3\sigma = 10\%$; threshold voltage V_{TH}: $3\sigma = 30\%$, and gate-oxide thickness t_{OX}: $3\sigma = 3\%$. As expected, the attack is more difficult when both aging and process variation mismatches occur. As shown in Fig. 7, **process plus aging mismatch results in 11% increase of the number of traces after** 20 **weeks on top of the aging mismatch increase of 25% to attain 80% success.**

4.2.4 Impact of temperature mismatch. Figure 8 depicts the effect of temperature mismatch. In this experiment, profiling was conducted in 0°C and attack was performed in different temperatures. Both profiling and attack were conducted on new devices. As shown, the number of traces for attacks in −40°C, −20°C and 0°C are approximately similar. (Minor deviations are due to the estimation error of the experiments.) By increasing the number of samples in our experiments, we expect to see a global minimum in this graph at 0°C (profiling temperature). As depicted, the attack is more difficult when there is a temperature mismatch between profiling and attack process. **The impact of temperature is to increase the number of traces required to attain** 80% **success by** ≈ 166%**, considering the corners** −40°**C &** +105°**C required in commercial applications.**

The difficulty of the attack (in terms of number of traces) is exacerbated when both temperature and aging time are not aligned between the profiling and target device. The take away point of the results shown in Fig. 5 and Fig. 8 is that to decrease the number of traces, first, the temperature must be the same for the training and matching devices. Then, ideally, aging should be balanced. However, this is not always possible as activity of trainee and attacker are not similar.

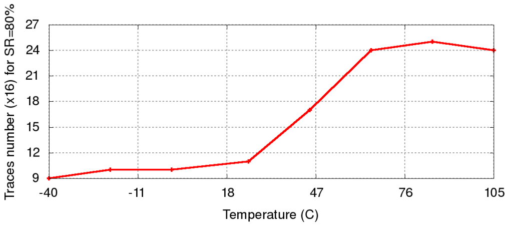

Figure 8: Mean number of traces to reach SR=80% in different attack temperatures (profiling temperature=0°**C,** $\sigma = 0.032$**).**

5 CONCLUSION

In this paper we showed the outcome of mounting the template attack on the PRESENT cipher in different temperatures and aging duration mismatches. The results show that the impact of aging on the attack is in the order of 10% after 5 weeks of usage in 105°C. As the impact of temperature mismatch is also highly significant (about 166% change in number of traces to recover the key with probability 80%, between -40°C and 105°C cases), to increase the success rate of the attack, the temperature (in general, the operational environment, including supply voltage, clock signal shape, etc.) must be the same for the training and matching devices. Then, as the secondary factor, aging should be balanced to fine-tune the attack. The technological dispersion (when training and matching devices are not the same) accounts for 11% more traces needed to break the device in 20 weeks on top of 25% more traces needed due to aging mismatches. Those quantitative results are of interest to designers, who can apply simple **derating factors** when estimating the practical strength of cryptographic designs against side-channel attacks.

REFERENCES

[1] O. Sinanoglu, N. Karimi, J. Rajendran, and R. Karri et al., "Reconciling the IC test and security dichotomy," in *ETS*, 2013, pp. 1–6.

[2] Y. Lu et al., "Statistical reliability analysis under process variation and aging effects," in *DAC*, 2009, pp. 514–519.

[3] S. Wang, J. Chen, and M. Tehranipoor, "Representative critical reliability paths for low-cost and accurate on-chip aging evaluation," in *ICCAD*, 2012, pp. 736–741.

[4] P. C. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," in *Int'l Conf. on Advances in Cryptology (CRYPTO)*, 1999, pp. 789–789.

[5] E. Brier, C. Clavier, and F. Olivier, "Correlation power analysis with a leakage model," in *CHES*, 2004, pp. 16–29.

[6] B. Gierlichs, L. Batina, P. Tuyls, and B. Preneel, "Mutual information analysis," in *CHES*, 2008, pp. 426–442.

[7] S. Chari, J. R. Rao, and P. Rohatgi, "Template attacks," in *CHES*, 2002, pp. 13–28.

[8] F. Oboril and M. B. Tahoori, "Extratime: Modeling and analysis of wearout due to transistor aging at microarchitecture-level," in *DSN*, 2012, pp. 1–12.

[9] A. Bogdanov et al., "Present: An ultra-lightweight block cipher," in *CHES*, 2007, pp. 450–466.

[10] F. Durvaux, F.-X. Standaert, and N. Veyrat-Charvillon, "How to certify the leakage of a chip?" in *EUROCRYPT*, 2014, pp. 459–476.

[11] N. Courtois, D. Hulme, and T. Mourouzis, "Solving circuit optimisation problems in cryptography and cryptanalysis," *IACR Cryptology ePrint Archive*, p. 475, 2011.

[12] "Nangate 45nm open cell library," "http://www.nangate.com" (accessed May 2016).

[13] Synopsys, "HSPICE User Guide: Basic Simulation and Analysis," 2016.

[14] C. Carlet et al., "Achieving side-channel high-order correlation immunity with leakage squeezing," *J. Cryptographic Engineering*, vol. 4, no. 2, pp. 107–121, 2014.

[15] S. Guilley et al., "A key to success - success exponents for side-channel distinguishers," in *INDOCRYPT*, 2015, pp. 270–290.

[16] S. Bhasin et al., "Side-channel leakage and trace compression using normalized inter-class variance," in *HASP*, 2014, pp. 7:1–7:9.

[17] M. A. Elaabid and S. Guilley, "Portability of templates," *J. Cryptographic Engineering*, vol. 2, no. 1, pp. 63–74, 2012.