On the Effect of Aging in Detecting Hardware Trojan Horses with Template Analysis

Naghmeh Karimi*, Jean-Luc Danger†‡ and Sylvain Guilley†‡

*CSEE Department
University of Maryland Baltimore County
Baltimore, MD 21250
naghmeh.karimi@umbc.edu

†Secure-IC S.A.S.
15 Rue Claude Chappe, Bât. B
35510 Cesson-Sévigné, France
firstname.lastname@secure-ic.com

‡LTCI, Télécom ParisTech
Université Paris-Saclay
75013 Paris, France
firstname.lastname@telecom-paristech.fr

***Abstract*—With the outsourcing of design flow, ensuring the security and trustworthiness of integrated circuits has become more challenging. Potential malicious modification of circuits, so-called Hardware Trojans Horses (HTH), has emerged as a major security threat. When triggered, the HTH delivers its payload resulting in denial of service, decreasing the device performance, or leaking sensitive information. Deploying VLSI testing schemes to detect HTH may fail in most cases as HTH are designed such that they are rarely activated. Side-channel analysis schemes have a higher detection coverage. The template analysis is the most powerful side-channel tool from an information theoretic point of view. In this paper, we focus on the template analysis used for detecting HTH in cryptographic devices, and study the effect of device aging on the success of these HTH detection schemes. Due to aging, electrical specifications of transistors, and in turn the power signatures used by template schemes change over time. We focus on Negative-Bias Temperature Instability and Hot-Carrier Injection aging mechanisms. We use the PRESENT cipher as a target, and mount several template attacks at different aging times on target devices and a genuine device used as reference. We deduce the authenticity of the target devices based on the attack success rates obtained by template analysis. Our results show that aging makes template-based HTH detection easier as it needs less traces in old devices compared to the new one (137 traces for a 20-week old device versus 195 traces for a new one).**

I. Introduction

Aggressive scaling of VLSI technology results in more complex systems in a single chip. High complexity and cost of design and fabrication of such circuits has invoked the outsourcing of design and fabrication to different parties across the globe. This globalization has jeopardized the security and trustworthiness of ICs and introduced new security vulnerabilities, among which inserting malicious circuitries, so-called "Hardware Trojan Horses (HTH)" in the original design/circuit has received the lion's share of attention.

A hardware Trojan can be inserted during the design or fabrication phase. It resides in hardware and is activated during the hardware operation. Hardware Trojans may result in denial of service, decreasing the device performance, or leaking sensitive data. Hardware Trojans are mainly stealthy and usually comprise a small fraction of the circuit area to avoid being detected easily [1]–[4].

The harm caused by hardware Trojans is broad and can range from change of performance in game controllers (to motivate customers to buy a new device) to catastrophic consequences in critical applications such as military, space or medical applications. Thereby, detecting HTH is highly crucial. Deploying destructive reverse-engineering schemes to check the genuineness of manufactured chips is highly costly and also cannot guarantee those untested to be Trojan free [5]. Utilizing VLSI testing schemes in detecting Trojans is not highly effective, as the trigger condition of a Trojan rarely appears [6]. The problem is exacerbated for sequential Trojans as they need a sequence of vectors to be triggered.

Side-Channel Analysis (SCA) schemes have been considered as more effective methods to detect hardware Trojans since they do not need to trigger a Trojan to detect it [7]. SCA-based Trojan detection deals with monitoring the device side-channels such as power signatures, path delays, electromagnetic emanation, etc, and comparing the retrieved signatures with those of a reference model to identify abnormal (possibly malicious) behaviors [8]. The success of SCA schemes in detecting Trojans is affected by the Trojan size and the process variations occurring during manufacturing process [9], [10].

Among SCA schemes, template analysis is considered as the most powerful tool from an information theoretic point of view [11]. Although template analysis is mainly used by adversaries to leak sensitive data from crypto cores, it can be adapted for detecting HTH in crypto devices. To investigate the genuineness of a *crypto device*, a template attack is launched on the target device as well as a genuine device used as a reference. Then, the authenticity of the target device is deduced based on the success rate of the launched attacks. Template analysis attacks include two steps: a characterization step in which the templates are computed on a training device, and a matching step in which the templates are used to extract the secret data of the target device. The efficiency of the template-based Trojan-detection schemes depends on the alignment between the training device (genuine reference device) and the device-under-investigation. *In this paper, we focus on the template-analysis based HTH detection schemes in crypto devices. In particular, we study the effect of device aging on the success of HTH detection schemes as due to aging, electrical specifications of transistors, and in turn the power signatures used by template schemes change over time.*

Aging effects in CMOS devices are one of the major challenges in nanotechnologies. Due to aging, electrical specifications of transistors embedded in the device such as their threshold voltage, deviate from their original intended specification. This deviation degrades performance; and consequently, the chip fails to meet some of the required specifications [12].

978-1-5386-5992-2/18/$31.00 ©2018 IEEE

Due to the aging-related deviations, power traces of the device change during the time [13]. This change can be different for genuine versus Trojan-infested devices. Thereby, when these devices are under template analysis using a similar profiling device (which is a new genuine device), the success rate of the launched attacks can be different. *In this paper, we investigate if by launching a template attack on an aged target crypto device, we can deduce that it is Trojan infested or not given that we have access to a genuine device. Note that, the aim of this paper is not discussing the efficiency/weakness of template analysis in Trojan detection versus other existing schemes (e.g. process-variation related weakness of Template attacks). The paper only investigates if aging affects the success of the template-analysis based Trojan-detection schemes.*

Among aging mechanisms, the effect of Negative-Bias Temperature-Instability (NBTI) and Hot-Carrier Injection (HCI) are more dominant than other mechanisms [13]. Thereby, in this paper, we focus on these two aging mechanisms. We use the PRESENT cipher as a target, and mount several template attacks on genuine and target devices with different aging durations to investigate how the template-based Trojan detection schemes are affected by aging. To the best of the authors' knowledge this is the first study on this topic. The contributions of this paper are as follows:

- A simulation framework which integrates device aging and the success evaluation of template-analysis based Trojan detection schemes;
- Detailed HSpice MOSRA simulations to evaluate the impact of NBTI/HCI aging on the success of Trojan detection in the PRESENT cipher using template analysis.

The rest of this paper is organized as follows. Section II discusses the Trojan-detection scenario considered in this paper. Section III presents the backgrounds on aging mechanisms and template attacks. Section IV discusses the impact of aging on detecting Trojans via template analysis. Simulation results are presented in Section V. Conclusions are drawn in Section VI.

II. Trojan Detection Scenario

We target the hardware implementation of cryptographic devices, and in particular we show our findings for the PRESENT cipher [14]. We utilize Template analysis methods and investigate how device aging affects the success rate of attacks launched on Trojan-infested circuits versus genuine circuits. In our scenario, the trusted facility investigates if a device is Trojan-infested or genuine. We assume that the facility has access to a reference genuine circuit, but has no information about the age of the target device, i.e., the device-under-investigation. The facility launches template analysis attacks on both genuine and target devices and based on the evolution of success rates, determines if the device is genuine or Trojan-infested. Section IV and the results presented in Section V extensively show how such distinction can be made.

III. Preliminaries

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

NBTI affects PMOS transistors. It includes two phases depending on the operating condition of the transistor. The first phase (*stress*) occurs when the transistor is "on". In this phase, the positive traps generated at the Si-SiO$_2$ interface 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 occurred during the stress phase partially recovers. Physical parameters of a transistor, supply voltage, temperature, and stress time all affect the magnitude of its threshold voltage drift [12]. Fig. 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.

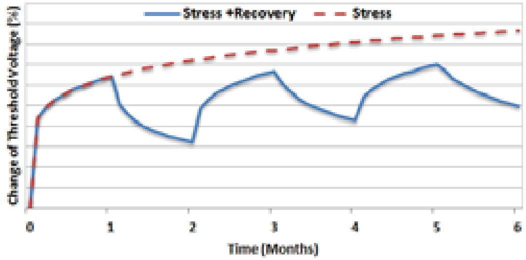


Fig. 1. The effect of NBTI aging on a PMOS Transistor.

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 [13].

Background on PRESENT Cipher: PRESENT is a lightweight block cipher with 64-bit blocks and a bit oriented permutation layer. 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 applied 16 times in parallel in each round [14].

Background on Template Attacks: SCA attacks are mainly launched by adversaries to obtain secret information of a device, e.g., a cryptographic key. These attacks retrieve the key by analyzing the physical leakage emitted during operation of a device (e.g., its running time, power consumption, etc), as this leakage is statistically dependent on the secret key. Profiled SCAs (e.g. template analysis) are the most powerful type of SCAs in which an attacker is able to characterize the leakage of an additional similar device and use this information to break the target 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. In the attack phase, the recorded traces are classified based on the value of the key and template matching is performed to derive the key value of the target device [15]. If traces are represented as a matrix X of $D \times Q$ elements (Q traces of D samples), and the learned model Y_k is also a $D \times Q$ matrix, then the attack guesses the key as below where Σ is the $D \times D$ noise covariance matrix, tr is the trace operator, and $argmin$ selects the value of k that results in the minimum value of its following function [16]:

$$\hat{k} \;=\; \underset{k\in\{0,1\}^4}{\operatorname{argmin}} \; \mathsf{tr}\big((X - Y_k)^{\mathsf{T}} \Sigma^{-1} (X - Y_k)\big) \,. \qquad (1)$$

Template attack can be adapted for detecting HTH. To do so, first the template is built by using a genuine device operating under normal conditions (room temperature, no aging, etc). Then, to investigate the authenticity of a target device, an attack is launched on the target device as well as a genuine device and the success rate of the attacks are utilized to deduce whether or not the target device is Trojan-infested. In this paper, we investigate how aging can affect the success rate of the template-based Trojan-detection schemes.

IV. Effect of Aging on Trojan Detection via Template Analysis

Template attacks are mainly used for leaking secret keys from crypto devices. In practice, the accuracy of the leakage models used in these attacks to retrieve the keys highly affects the success of such attacks. Thereby, one of the main challenges in these attacks is to avoid being biased by an incorrect model [17]. However, in practice, it is hard to reproduce exactly the same operating conditions (e.g., temperature) in both profiling and matching phases. Process variations occurring during the manufacturing process may also result in discrepancies between profiling and matching chips.

Template analysis schemes can be deployed to detect HTH in crypto devices via launching attacks on the device-under-investigation as well as a reference genuine device and deducing the authenticity of the target device based on the success rate of these attacks. In this paper, we focus on the effect of device aging on template-based Trojan-detection schemes. In fact, when a target device is investigated in terms of Trojan, it may have been used (aged) previously, and hence its specification and in turn its power signatures may have been changed based on its usage time and operating conditions. Thus, ignoring aging effects can be misleading and may not result in an accurate HTH detection. In fact, the target device should be compared with a genuine device of the same age regarding attack success. However, *we cannot estimate the exact age of the target device as aging effects depend on external factors such as workload, operating temperature, etc*.

To make the genuine reference device and the target device comparable in terms of aging, and to increase the accuracy of the Trojan detection scheme, we suggest to place an embedded Ring-Oscillator (RO) in the crypto chip during the design phase. As ring-oscillators are highly prone to aging [18], by measuring the frequency of this RO, we can estimate the *age level* of the target chip. After the age level estimation, we investigate the effect of the template attack on the target chip along with a genuine chip of the same age level. For aging estimation, we do not need to (and cannot) extract the exact age of the device, as it depends on operating conditions of the target device which is not known during the investigation.

To investigate if a device is Trojan-infested, we compare the frequency of its embedded RO with the frequency of the RO embedded in a reference new genuine chip and find the frequency ratio ($= \gamma$). Then, we will place the genuine chip under aging stress (by placing it in a climate chamber under high temperature) and periodically measure its frequency change due to such aging. We continue the process till we get the same frequency ratio (γ) for the genuine under-stress chip (compared to the genuine new chip). Thereby, without information on the exact age of the device-under-investigation, we will have a genuine and a target device with the same age level. We will mount template attacks on both devices, and based on the relative success rates of the launched attacks (as will be discussed in Section V-B1) deduce the authenticity of the target device. Note that *as we balance age levels (not exact age times) we do not need information about the usage time and operating temperature of the target device (if not new)*.

V. Experimental Results and Discussions

A. 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 [19, §3]. Fig. 2 shows the gate-level netlist of this circuit. Though the gate-level netlist is of minimal size, it includes a long critical path with several XOR gates, which makes it highly amenable to glitches that complexify the link between input data and leakage. Thereby, this circuit is highly suitable as a case study for Template analysis.

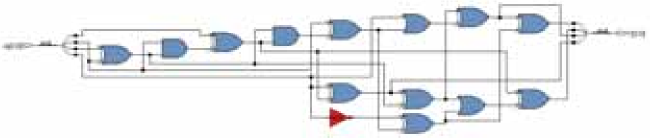


Fig. 2. Netlist of the genuine PRESENT S-box considered in this study.

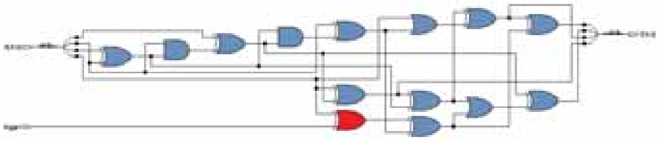
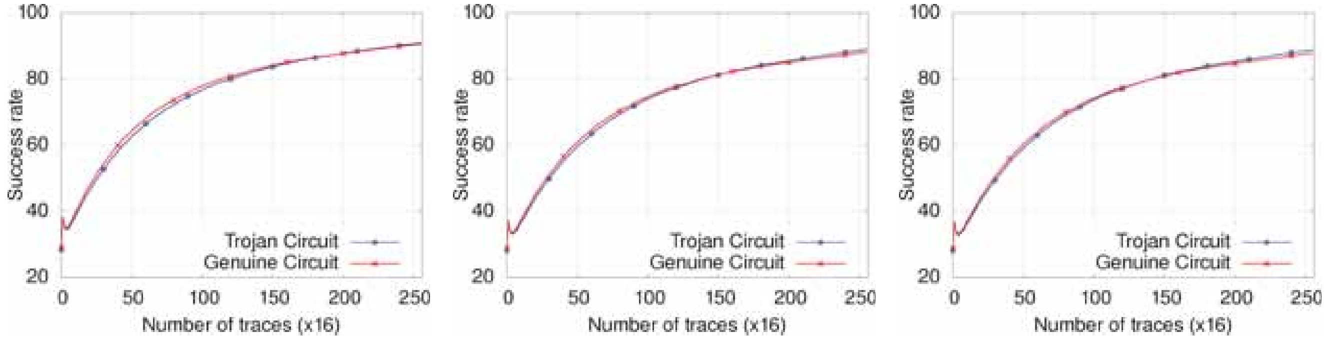


Fig. 3. Netlist of the Trojan-infested PRESENT S-box targeted in this study.

Fig. 3 shows our Trojan-infested circuit. The only difference between this circuit and the genuine circuit (Fig. 2) is replacing the INVERTER gate in the genuine circuit with an XOR gate whose second input is fed by the *trigger* signal. *In our experiments, the trigger signal is connected to VDD. Thereby,*



(a) Age: 0 week

(b) Age: 10 weeks

(c) Age: 20 weeks

Fig. 4. SR after $100,000$ attacks (attack temperature=105°C, $\sigma = 0.032$) on devices with different ages.

the Trojan is never triggered. The reason for not triggering the Trojan is that the Trojans are mainly designed such that they rarely affect the output since otherwise they can be detected easily during manufacturing testing or via simple power observation. Though detecting untriggered Trojans is more difficult than triggered ones, it is more realistic. *To highlight the effect of aging and avoid the obvious power changes caused by triggering a Trojan, in our experiments, the Trojan is not triggered.*

The genuine and Trojan-infested circuits have been implemented in the transistor level using 45-nm NANGATE technology [20]. 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 [21]. Power traces were extracted for genuine and Trojan-infested devices with different age duration. The effect of aging was evaluated for 20 weeks of device operation in time steps of one week in 105°C operating temperature.

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 its S-box. All of these transitions were considered to build the template. Cryptographic functions, by essence, randomize the data they manipulate. Thereby, it is natural that in "steady cruising 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.

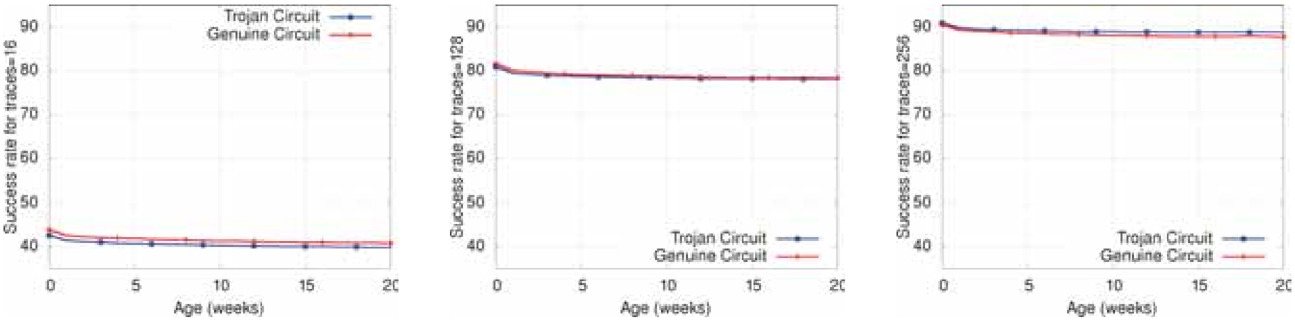
B. Experimental Results

1) Impact of aging on the success rate of template analysis: The first set of results shows the impact of aging on the success of the template attacks mounted on Trojan-infested versus genuine devices. The training traces were gathered from a fresh (not-aged) genuine device operating in 25°C. Attacks were mounted on genuine and Trojan-infested circuits aged between 0 and 20 weeks in 105°C. Assuming different temperatures for training and attack phases makes the experiments more realistic. As our HSpice simulations with MOSRA do not consider any noise, to realize the experiments, we artificially added some level of Gaussian noise in our analysis.

Fig. 4 shows the Success Rate (*SR*) of attacks for different aging durations when temperature is 105°C and $\sigma = 0.032$ where σ denotes the standard deviation of the noise. We considered a large amount of noise compared to the signals (with standard deviation ≈ 150 μW), resulting in signal-to-noise ratio of ≈ 0.005. As Fig. 4 shows the genuine and Trojan-interested circuits behave differently when the number of traces is increased. Fig. 4a shows the success rate of the attacks lunched on new devices, i.e., both genuine and Trojan-infested circuits are fresh. As shown, by increasing the number of traces, SR of attacks mounted on each device increases albeit with different rates. The attack is more successful in a genuine device compared to a Trojan-infested device when lower number of traces are deployed for the attack. This trend is changed with increasing the number of traces such that with $\approx$ 190 (x16) traces, the genuine device is more difficult to attack compared to the Trojan-infested device. Figures 4b-4c depict the attack outcomes for aged devices. As shown, similar to new devices, for the aged devices the attack is more successful in genuine circuits when lower number of traces are used, while it is more effective in Trojan-infested devices with increasing the number of traces. The take-away point from this observation is that to deduce the authenticity of a crypto device, a tester can launch a template attack on that device as well as a genuine device used a reference, and then based on the relative success rate of the attacks when different number of traces are deployed, we can classify the device as genuine or Trojan-infested.

Fig. 5 shows the difference between Trojan-infested and genuine devices from a different perspective. It depicts how the SR of the template attack decays with aging, as the target device becomes older and older w.r.t. the clone used to build the template. For instance, Fig. 5b shows that the SR of the attack mounted on a genuine device decreases $\approx 4.1\%$ after 20 weeks of aging when 128 (x16) traces are used. As shown, the SR of the attack mounted on both circuits drops fast after one week, and then continues to decrease, though at a slower rate. Figures 5a-5c depict that for any constant number of traces, attack would be more difficult for old devices, regardless of including a Trojan or not. But as expected, with increasing the number of traces, attacks would be more successful, e.g., for a 20-week old genuine device by increasing the traces from 16 (x16) to 256 (x16), SR increases $\approx 115\%$. This increase is around $\approx 122\%$ for a 20-week old Trojan-infested device.

The third set of results deals with the relative change in



(a) Number of Traces: 16 (x16)

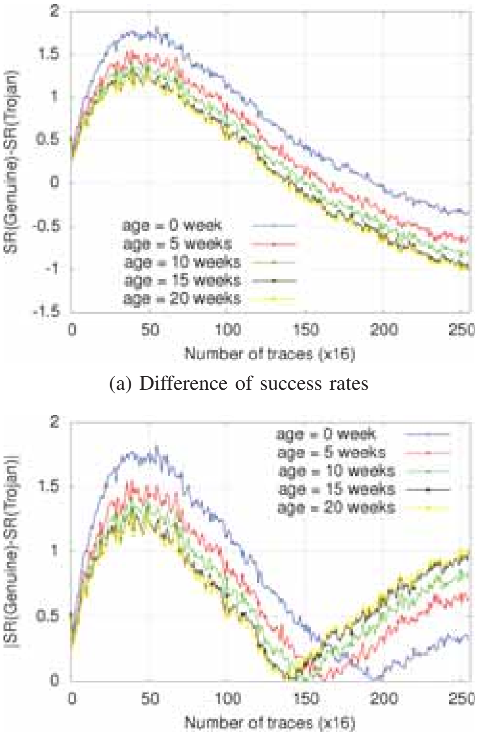
(b) Number of Traces: 128 (x16)

(c) Number of Traces: 256 (x16)

Fig. 5. SR after $100,000$ attacks (attack temperature=105°C, $\sigma = 0.032$) with different number of traces.

the SR of a template attack mounted on a genuine versus a Trojan-infested device. Fig. 6a shows the difference of the SR of the attacks mounted on these devices (ΔSR), and Fig. 6b shows the absolute value of this difference for various aging durations. As depicted ΔSR decreases with aging, i.e., ΔSR is 1.74%, 1.51%, 1.41%, 1.34%, and 1.31% for 0, 5, 10, 15, and 20 weeks of aging, respectively, when 50 (x16) traces are utilized. For each aging duration, with low number of traces, genuine device is easier to attack than the Trojan-infested device, i.e., ΔSR is positive. The value of ΔSR increases for $\approx$ 50 traces but afterwards with deploying more traces, ΔSR starts decreasing (i.e., Trojan and genuine circuit behaviors become more similar in terms of power consumption). However, as these figures show, with more and more increase in traces (more than $\approx$ 137 (x16) for 20 week age and $\approx$ 195 (x16) for a fresh device) the relative behavior of genuine and Trojan-infested devices diverge again ($|\Delta SR|$ increases), and beyond this point, Trojan-infested circuit is easier to attack than the genuine one. As depicted, $|\Delta SR|$ increases with aging after the convergence points (the point where ΔSR is 0).

The take-away point from these observations is that by mounting a template attack on a target device and a genuine device, and comparing their behaviors (in terms of the relation of SR and number of traces used), we can deduce if the target device is genuine or not. Fig. 6b shows that such investigation needs more traces when both devices are new. As shown, ΔSR reaches to "0" with $\approx$ 195 (x16) traces for new devices while for 20-week old devices $\approx$ 137 (x16) traces are needed to get "0" on ΔSR. Thereby, *aging makes the Trojan detection easier*.



(a) Difference of success rates

(b) Absolute value of success rate differences

Fig. 6. Difference of SR in genuine and Trojan-infested circuits after $100,000$ attacks (temperature=105°C, $\sigma = 0.032$).

2) Deploying an embedded RO for aligning template-based HTH detection: The results presented earlier depict that one can identify a Trojan-infested crypto chip by placing that chip as well as a genuine chip under a template attack and comparing the relative change of success rates. However, as discussed earlier, the Trojan and genuine circuits should be of the same *age level* so that the results of the attacks be comparable. To be able to make these devices comparable, as discussed in Section IV, we embed a RO inside each chip in the design phase. Then, during the Trojan investigation process, we first extract the aging-induced change of the frequency of the RO embedded in the device-under-investigation. Then, we place the genuine circuit under stress in order to bring it to the same age level as the device-under-investigation, and then launch a template attack on both devices and analyze the outcome. Fig. 7 quantifies the effect of aging on the clock period of a ring oscillator (composed of 21 cascaded INVERTERS) in different operating temperatures. As expected, ring oscillators are highly sensitive to aging (even in temperatures close to room temperature) and thereby are suitable candidates for estimating the age-level of a target device. *Note that to detect HTH, we do not need to know the temperature under which the target device may have been deployed previously as we try to equalize the age level of the target and genuine devices.*

3) Impact of process mismatch on Trojan detection: Due to process variations that occur during the manufacturing process, the specifications of the training and target devices can be slightly different. To quantify the effect of process variations in our method, we conducted Monte Carlo simulations using

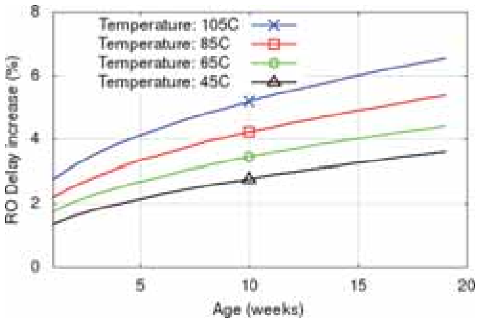


Fig. 7. Effect of aging on the delay of a RO in different temperatures.

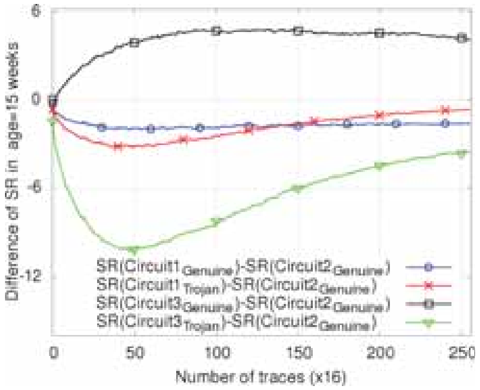


Fig. 8. The effect of process variation on the SR of genuine and Trojan-infested circuits (aging: 15 weeks).

a Gaussian distribution: transistor gate length L: $3\sigma = 10\%$; threshold voltage V_{TH}: $3\sigma = 30\%$, and gate-oxide thickness t_{OX}: $3\sigma = 3\%$. Parameters reflect a 45-nm process in commercial use today [22]. In this experiment, we considered *Circuit2* as our genuine device and *Circuit1* and *Circuit3* as target devices. All three are 15 weeks old. Fig. 8 shows the difference of *SR* of the mounted attacks on genuine circuit (*Circuit2*) and the other 2 devices when they are genuine or Trojan-infested. First observation is that this figure confirms our previous finding regarding the trend of the SR change in Trojan-infested circuits, i.e., with few traces a genuine circuit has a higher SR compared to its Trojan-infested counterpart while this trend is changed with increasing the number of traces.

In this experiment, the genuine device (*Circuit2*) is different from target devices (*Circuit1*/*Circuit3*) to reflect the effect of process variations in real silicon. Thereby, the values shown in Fig. 8 can be negative even when a few traces are deployed. Moreover, Fig. 8 shows that the SR in genuine circuits does not change significantly after 100 traces, i.e., it almost saturates for both genuine circuits. However, for the Trojan-infested circuits, a significant slope is observed after deploying 100 (x16) traces. In particular, the slope of changes in Fig. 8 for genuine model of *Circuit1* and *Circuit3* is 0.00007 and -0.0003, respectively when the traces increase from 100 (x16) to 255 (x16). While, this slope is 0.0007 and 0.002 for the Trojan-infested models of *Circuit1* and *Circuit3*, respectively. The take-away point from this observation is that we can deduce that an aged device is Trojan-infested based on the shape of the success rate which has much higher slopes in case of HTH presence.

VI. Conclusion

This paper investigated the impact of transistor aging on detecting Hardware Trojans Horses (HTH) via template analysis schemes. We addressed how aging-related change of device specifications during the time, facilitates detecting HTH. To detect HTH via template analysis, we can mount several template attacks on the target device as well as a reference genuine device, and deduce the authenticity of the target device based on the attack outcomes, notably by taking advantage of the success rate curve. In this paper, we targeted the hardware implementation of the PRESENT cipher and launched several attacks on genuine and Trojan-infested devices that have been aged for different duration. The experimental results show that aging makes template-based HTH detection easier as it needs less traces in old devices compared to the new ones. Moreover it was shown that process variation does not impact the effectiveness of our HTH detection scheme in aged devices.

References

[1] S. Bhunia, M. S. Hsiao, M. Banga, and S. Narasimhan, "Hardware Trojan attacks: Threat analysis and countermeasures," *Proceedings of the IEEE*, vol. 102, no. 8, pp. 1229–1247, Aug 2014.

[2] M. Tehranipoor and F. Koushanfar, "A survey of hardware Trojan taxonomy and detection," *IEEE Design and Test of Computers*, vol. 27, no. 1, pp. 10–25, Jan 2010.

[3] J. Dubeuf, D. Hély, and R. Karri, "Run-time detection of hardware Trojans: The processor protection unit," in *ETS*, 2013, pp. 1–6.

[4] M. Banga and M. S. Hsiao, "A region based approach for the identification of hardware Trojans," in *HOST*, 2008, pp. 40–47.

[5] Y. Jin and Y. Makris, "Hardware Trojan detection using path delay fingerprint," in *HOST*, 2008, pp. 51–57.

[6] R. Rad et al., "Power supply signal calibration techniques for improving detection resolution to hardware Trojans," in *ICCAD*, 2008, pp. 632–639.

[7] D. Agrawal et al., "Trojan detection using IC fingerprinting," in *IEEE Symp. on Security and Privacy*, 2007, pp. 296–310.

[8] X. T. Ngo et al., "Hardware Trojan detection by delay and electromagnetic measurements," in *DATE*, 2015, pp. 782–787.

[9] T. Hoque et al., "Golden-free hardware Trojan detection with high sensitivity under process noise," *Journal of Electronic Testing*, vol. 33, no. 1, pp. 107–124, 2017.

[10] J. Zhang, H. Yu, and Q. Xu, "HTOutlier: hardware trojan detection with side-channel signature outlier identification," in *HOST*, 2012, pp. 55–58.

[11] S. Picek, A. Heuser, and S. Guilley, "Template attack vs bayes classifier," in *Workshop on Security Proofs for Embedded Systems (PROOFS)*, 2016.

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

[13] N. Karimi, S. Guilley, and J.-L. Danger, "Impact of aging on template attacks," in *GLSVLSI*. ACM, May 23-25 2018, Chicago, Illinois, USA.

[14] A. Bogdanov et al., "PRESENT: An Ultra-Lightweight Block Cipher," in *CHES*, ser. LNCS, vol. 4727. Springer, 2007, pp. 450–466.

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

[16] N. Bruneau et al., "Optimal side-channel attacks for multivariate leakages and multiple models," *J. Cryptographic Engineering*, vol. 7, no. 4, pp. 331–341, 2017.

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

[18] 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.

[19] N. Courtois et al., "Solving circuit optimisation problems in cryptography and cryptanalysis," *IACR Cryptology ePrint Archive*, p. 475, 2011.

[20] "NANGATE 45nm Open Cell Library," "http://www.nangate.com".

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

[22] N. Karimi and K. Chakrabarty, "Detection, diagnosis, and recovery from clock-domain crossing failures in multiclock SoCs," *IEEE Trans. on CAD*, vol. 32, no. 9, pp. 1395–1408, 2013.