# Simulation and Analysis of Negative-Bias Temperature Instability Aging on Power Analysis Attacks

Xiaofei Guo*, Naghmeh Karimi†
* Security Center of Excellence, Intel Corporation
†ECE Department, Rutgers University
xiaofei.rex.guo@intel.com, naghmeh.karimi@rutgers.edu

Francesco Regazzoni‡, Chenglu Jin§, Ramesh Karri§
‡ALaRI - USI, Lugano, Switzerland
§New York University
regazzoni@alari.ch, {cj875, rkarri}@nyu.edu

***Abstract*—Transistor aging is an important failure mechanism in nanoscale designs and is a growing concern for the reliability of future systems. Transistor aging results in circuit performance degradation over time and the ultimate circuit failure. Among aging mechanisms, Negative-Bias Temperature Instability (NBTI) has become the leading limiting factor of circuit lifetime. While the impact of transistor aging is well understood from the device point of view, very little is known about its impact on security, and in particular on power analysis attack. This paper fills the gap by evaluating the effects on power analysis attack. Our experimental results obtained using PRESENT algorithm show that CPA attacks are not significantly affected by aging, while the successful rate of template attack changes significantly.**

## I. Introduction

With the advance of VLSI technology and the continuing decrease in feature size of electronic devices, various robustness concerns continue to arise. Among them, aging effects in CMOS devices are one of the major robustness challenges in nanotechnologies. In practice, aging mechanisms degrade the reliability and performance of CMOS devices over their lifetime. Negative-Bias Temperature Instability (NBTI) is one of most prominent sources of aging mechanisms and induces severe threats to the reliability of nanoscale devices [1]–[3].

NBTI occurs when a negative voltage is applied to PMOS transistors [4]. NBTI increases the threshold voltage of the PMOS transistor under stress and reduces the drain current and hence degrades the delay through the distressed PMOS transistor. At the circuit level, NBTI manifests as circuit timing and functional failures [5]–[7]. Many studies focused on the NBTI effect on circuit life time and schemes to prolong circuit life time. We focus on the impact of NBTI aging effects on the implementation of cryptographic devices complementing studies which discussed the impact of different technology scaling related issues such as process variation [8], [9].

Power analysis attack extracts the secret information by correlating the power consumed by cryptographic devices or their electromagnetic emanations with the data processed by the algorithm [10]. Power analysis uses a divide-and-conquer approach which guesses a small portion of the key and verifies the hypotheses. This process is repeated until the whole key is revealed. The most common ways to carry out power analysis are differential power analysis (DPA) [10], correlation power analysis (CPA) [11], mutual information analysis (MIA) [12], and template attack [13].

Power analysis countermeasures ranges from the algorithm to the cell level [10]. Here we summarize gate-level techniques as they will be the main target of our evaluation. Gate-level countermeasures fall into two major categories: masking techniques such as DRSL [14], gate-level masking [15], which randomize power consumption, and hiding techniques such as WDDL [16], which minimize the data-dependent variations in power consumption. Countermeasures can combine the principles of both categories such as masked dual-rail precharge logic (MDPL) [17] and iMDPL [18].

In a masking circuit, one or more masks are first generated and applied to the input data before the cryptographic algorithm starts. After applying the cryptographic algorithm on the masked data, the mask is removed to generate the output. Since an attacker does not know the random mask value, it is difficult for him to correlate the input data and the power traces. However, glitches can significantly reduce the resistance of masking against power analysis attacks [19].

MDPL combines masking and dual-rail precharge logic styles (DRP). Each operation only processes masked data, i.e., the power consumption of the device only depends on the masked data. Therefore, it is difficult for an attacker to distinguish the key. Moreover, the masking removes the need of routing constraint in the DRP. Ideally, MDPL is safe from glitches and does not have to balance the complementary wires since all data are masked. However, MDPL suffers from early propagation which causes temporary data dependent switching of MDPL gates and reduces the DPA resistance of MDPL [18], [20]. iMDPL improves MDPL by adding an evaluation precharge detection unit that may prevent the occurrence of early propagation [18]. However, the imbalance between the two rails still leaks information [21]

We investigate the impact of NBTI aging on power analysis of cryptographic devices. In particular, we analyze the NBTI aging effect on MDPL and gate-level masking against CPA and template attack. Our main contributions are:

- A simulation framework which integrates the accelerated NBTI aging and the early security evaluation of the design by means of simulation[1].
- The evaluation of gate level masking and MDPL implementations selected as a representative case study to estimate the effect of aging on power analysis using the proposed framework.

[1] In order to evaluate the effect of NBTI aging on the security of a circuit, we first accelerated NBTI aging by generating appropriate input patterns and applying these patterns to the circuit-under-study.

978-1-4673-7421-7/15/$31.00 ©2015 IEEE

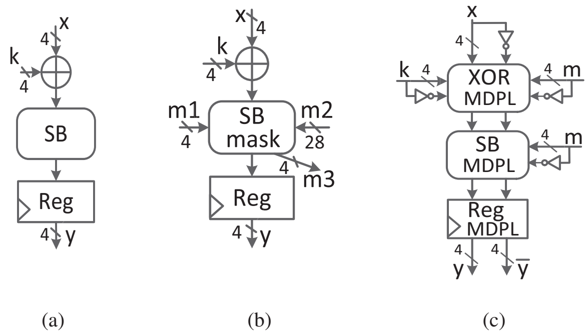


Fig. 1: (a) Simple cipher structure. (b) Simple cipher structure augmented with gate-level masking. (c) Simple cipher structure implemented in MDPL.

## II. Preliminaries

### A. NBTI Effect

NBTI is one of the main factors in decreasing the performance of digital circuits over time. It mostly affects a PMOS transistor when a negative voltage is applied to its gate. In fact, a PMOS transistor experiences two phases of NBTI depending on its operating condition. The first phase, i.e., the stress phase, occurs when the transistor is on, i.e., when a negative voltage is applied to its gate. Positive interface traps are generated at the Si-SiO$_2$ interface. Accordingly, the magnitude of the threshold voltage of the transistor is increased. In the second phase, i.e., recovery phase, a positive voltage is applied to the gate of the transistor. The threshold voltage drift induced by NBTI during the stress phase can partially "recover".

Threshold voltage drifts of a PMOS transistor under stress depend on the stress voltage, temperature, and stress time. The NBTI effect is high in the first few months, but the threshold voltage tends to saturate for long stress times.

To evaluate the impact of NBTI on the performance of a logic circuit under stress, we use the model in [22], which defines the two equations we use to estimate the the change in threshold voltage of a PMOS transistor in stress and recovery modes at a specific instant of time.

### B. PRESENT Cipher

PRESENT is a lightweight block cipher [23]. which encrypts a 64-bit plaintext into a 64-bit ciphertext with an 80-bit key in 31 rounds. Each round consists of a bitwise XOR operation, a non-linear substitution layer and a linear permutation layer.

In the following experiment, we use a reduced version of PRESENT composed by the key addition (XOR) followed by the nonlinear function S-box and then the register as shown in Fig. 1(a). The data value prior to the key addition is obtained from the input. This structure is well accepted by the community as representative of the behaviour of block cipher, with the advantage of being sufficiently small to allow a complete exploration of its characteristics.

### C. Power Analysis Attack

*1) Correlation Power Analysis (CPA):* Power analysis uses power consumption to determine whether the hypothetical value of a portion of the key bits are correct. One way to verify the hypothesis is to use the statistical correlation between power traces and hypothetical power consumption expressed using Pearson's correlation coefficient: one variable representing the hypothetical power consumption (in our case we used the hamming weight) generated with the hypothetical key, while the other is the actual power measurement.

*2) Template Attack:* Template attacks usually consist of two phases: (1) building a template from a device (usually different but identical to the one under attack); (2) template matching to derive the key value of the device under attack. In the first phase, the attacker computes a number of encryption on the "template" device using several pairs of plaintext, key, power traces, and computes the mean vector and the covariance matrix of a multivariate normal distribution (used to characterize the power traces). In the second phase, the adversary collects a power trace from the device under attack and evaluates how probable is that power traces knowing the multivariate normal distribution of the template. The highest probability among all the templates indicates the correct key.

### D. Countermeasures

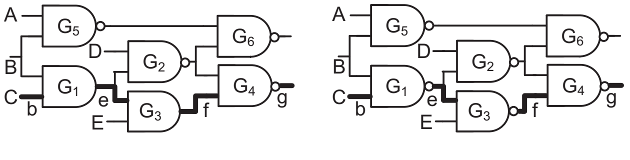
*1) Gate-Level Masking [15]:* Each masking gate computes the masked input and generates the masked output. To implement such systems, we decompose the circuit in simpler gates, i.e., XOR, AND, and NOT. Both AND and XOR gates can be converted into masked gates. XOR is a linear operation and the masked data bits can be easily demasked by XOR-ing the results with the correct mask, while AND operation is slightly more complex because it is a non-linear operation.

*2) MDPL [17]:* MDPL combines DRP with masking. MDPL represents a logic-1 and a logic-0 with a differential pairs (1, 0) and (0, 1), respectively. Additionally, the pair (0, 0) is used during the pre-charge phase. MDPL can be implemented in compact way using majority-gates. The basic MDPL AND gate takes six dual-rail inputs ($a_m$, $\overline{a_m}$, $b_m$, $\overline{b_m}$, $m$, $\overline{m}$) and produces two output values ($q_m$, $\overline{q_m}$). The MDPL NAND can be built by swapping the complementary wires of the output signals of MDPL AND, while the the MDPL XOR gate is built from three MDPL NAND gates.

## III. The NBTI Acceleration

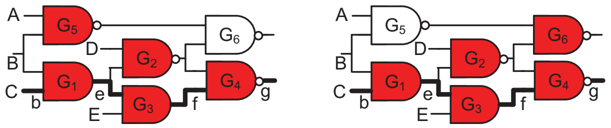
To investigate the effect of NBTI aging on power analysis, we developed a framework to accelerate NBTI aging, i.e., by having access to the circuit netlist, we find input patterns that when applied to the circuit, accelerates the NBTI effects.

We describe the NBTI-related performance degradation of a circuit using the simple combinational circuit shown in Fig. 2(a). Assume that path $b$-$e$-$f$-$g$ (including $G_1$, $G_3$, and $G_4$) is the critical path. By holding the primary inputs constant at $V_1(ABCDE)$="dd0dd" (where $d$ stands for don't-care), the PMOS transistors of each gate in this path are kept on and accordingly these gates experience NBTI aging. However, it is not always possible to stress all the gates in the critical path of a circuit simultaneously. Let us consider the



(a) (b)

Fig. 2: Two sample circuits (the longest paths are in bold). (a) One input pattern “ABCDE=dd0dd” can put all the gates of the critical-path under NBTI stress. (b) Two input patterns “dd0d1;d11dd” can put all the gates of the critical-path under NBTI stress. To stress path $b$-$e$-$f$-$g$, apply $V_1$ =“d10d1” at time $t_0$ and $V_2$ =“d11d1” at time $t_1$. Lines $b$ and $f$ get “0” in the first time slot and $e$ gets “0” in the second time slot. $V_1$ stresses gates $G_1$ and $G_4$ and $V_2$ stresses gate $G_3$.



(a) (b)

Fig. 3: (a) $G_2$, $G_5$, $G_1$, $G_3$, and $G_4$ are aged after applying pattern “10011” (b) $G_2$, $G_6$, $G_1$, $G_3$, and $G_4$ are aged after applying pattern “11011”

circuit in Fig. 2(b). Holding the primary inputs constant at $V_1(ABCDE)$=“dd0d1” accelerates aging of $G_1$ and $G_4$, while holding the primary inputs constant at $V_2(ABCDE)$=“d11dd” accelerates aging of $G_3$.

We find a minimal set of input patterns that when are applied to the circuit collectively result in a maximal NBTI stress. For the circuit in Fig. 2(a), this set includes only one input pattern, i.e., $ABCDE$=“dd0dd”, while for the circuit depicted in Fig. 2(b), this set includes two patterns, i.e., $ABCDE$=“dd0d1;d11dd”.

To generate the minimal set of patterns that results in a maximal NBTI effect in a circuit, we target the critical path of that circuit and identify the input patterns that put each gate on this path under NBTI stress. Then, we select a minimal subset of patterns such that by applying the selected patterns all the gates in the critical path are put under NBTI stress.

Table I shows the input patterns that put each individual gate of the circuit in Fig. 2(a) under stress. By applying input pattern “dd0dd” all gates of the critical path are stressed. Table II shows the similar results for the circuit in Fig. 2(b). For this circuit, the minimal set of patterns required to target all the gates of the critical path includes “dd0d1; d11dd” patterns.

If by applying the generated patterns, the PMOS transistors of other gates which are not in the critical path get zero as input, those gates get aged as well. For instance, for the circuit in Fig. 2(a), by applying “10011”, $G_2$ and $G_5$ are aged besides the gates in the critical path, i.e., $G_1$, $G_3$, and $G_4$ as shown by the shaded gates in Fig. 3(a). Fig. 3(b) shows the case where pattern “11011” is applied to the circuit. In this case, $G_2$ and $G_6$ are aged besides the gates in the critical path.

TABLE I: Input patterns that put each gate of the critical path of Fig. 2(a) under NBTI stress.

| Gates | Input patterns (ABCDE) to put a gate under stress |
|---|---|
| $G_1$ | “dd0dd” |
| $G_3$ | “d0ddd”, ‘dd0dd” |
| $G_4$ | “d0ddd”, ‘dd0dd”, “dddd0” |

TABLE II: Input patterns that put each gate of the critical path of Fig.2(b) under NBTI stress.

| Gates | Input patterns (ABCDE) to put a gate under stress |
|---|---|
| $G_1$ | “dd0dd” |
| $G_3$ | “d11dd” |
| $G_4$ | “d0dd1”, ‘dd0d1” |

The amount of aging is determined by the duration for which the generated vector are continuously applied to the circuit. The type of gates in the targeted path also determines the magnitude of aging. Fig. 4 shows the propagation delay changes of primitive logic gates over time when these gates are under NBTI stress. It shows the case where the gates are continuously under NBTI stress and they do not experience recovery. For various gate types and aging times, the increase of propagation delay ranges from 14-43%. Although the propagation delay of each gate increased over time, the increase is the most in the first couple of months.

To evaluate the effect of NBTI on the propagation delay of primitive gates, we conducted a series of HSpice simulations using 45nm technology with high-k dielectric, at a nominal supply voltage (Vdd) of 1.1 V and a nominal temperature of 80°C. We first extracted the nominal propagation delay of each primitive gate. Then, we evaluated the change in threshold voltage using the model discussed in [25] assuming that the gate is subjected to NBTI stress for different time durations. Finally, using the degraded threshold voltage values, we ran HSpice simulations to extract the propagation delay of each gate under NBTI stress.

## IV. Experimental Results

### A. Aging Effect on Standard Cells

Fig. 5(a) shows a circuit with three AND gates. The primary inputs are $A_0$, $A_1$, $A_2$, and $A_3$. The primary outputs of the baseline and aged circuits are $X_n$ and $X_a$, respectively.

The initial input pattern is $A_0$=$A_1$=$A_2$=$A_3$=1 in Fig. 5(a). When $A_0$ falling transition (1→0) occurs, $X_n$(1→0) occurs with a delay of three gates. We aged the AND gate inputs that connect to $A_0$, $G_0$, and $G_1$ by setting $A_0$=$A_1$=$A_2$=$A_3$=0 for six months[2]. After aging, we apply the same input patterns. When $A_0$(1→0) transition occurs, it excites (turns on) the aged PMOS transistor in the leftmost AND gate. Similarly, $G_0$(1→0) and $G_1$(1→0) occur one after another. In this case, all aged AND gates are excited shown by the burst symbol. Therefore, after aging, the primary output transition $X_a$(1→0) happens with a delay increase $\Delta_{t1}$=0.028ns-0.020ns=0.008ns. The delay of the aged circuit is 40% more than that of the baseline. With this input pattern, the aged PMOS transistor in all three AND gates are excited.

[2] The PMOS transistor directly connecting to $A_0$ is aged.

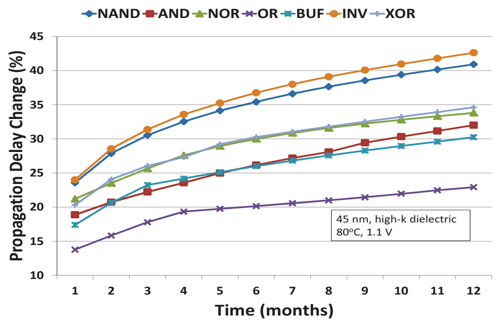
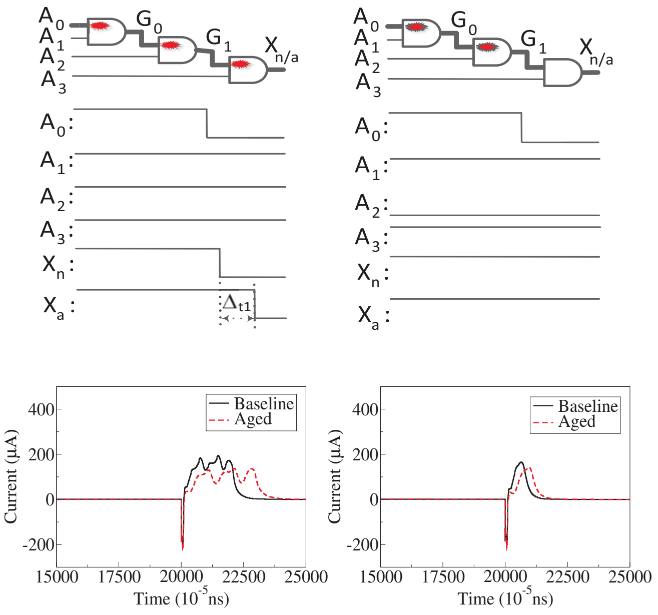


Fig. 4: Percentage change in propagation delay of primitive logic gates as a function of stress time.

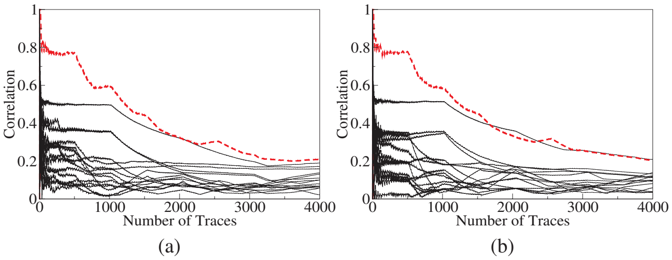


(c) (d)

Fig. 5: (a) One input pattern and the excited aged gates. (b) Another input pattern and the excited aged gates. (c) The instant current with three aged PMOS transistors excited (c) The instant current with two aged PMOS transistors excited.

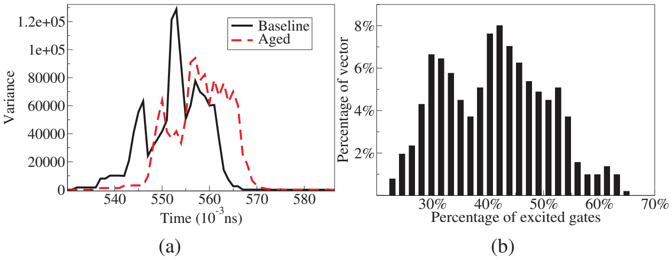
The initial input pattern is $A_0$=$A_1$=$A_3$=1 and $A_2$=0 in Fig. 5(b). When $A_0(1\rightarrow0)$ transition occurs, $X_n$ does not change. After aging, we apply the same input patterns. When $A_0(1\rightarrow0)$ occurs, it turns on the aged PMOS transistor and the aging effect increases the propagation delay of the left AND gate. The input of the other two AND gates are logic low, therefore the aged PMOS transistor in the middle AND gate is also excited. However, the aging effect does not have any impact on the delay since the output does not change.

Fig. 5(c) and Fig. 5(d) show the comparison between the current of the baseline and the aged circuit when applying the test patterns to the left and right circuits of Fig. 5(a), respectively. The current of the baseline circuit is shown in the bold line and that of the aged circuit is shown in the dotted line. In Fig. 5(c), The current of the aged circuit has a significant shift in time and reduction in the magnitude. The time shift correlates with the delay effect, because the aged PMOS transistor has higher threshold voltage (in magnitude) and thus it takes more time to pull enough current to the fanout. The reduction of the current after aging is a result of the higher threshold voltage. In Fig. 5(d), the difference between the baseline and aged circuits are smaller because less aged PMOS transistors are excited.



(a) (b)

Fig. 6: CPA on the baseline and aged masked circuit (a) baseline (b) aged



(a) (b)

Fig. 7: Variance of the power traces for PRESENT S-box with masking.

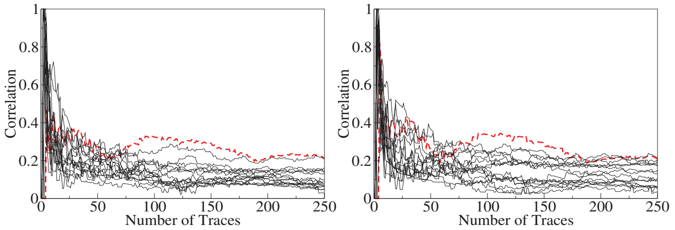
We also characterize the aging effect on other standard cells. The general observations when the aged gates are excited are:

- NBTI aging creates a time shift and a reduction of peak magnitude in the current consumption.
- NBTI aging effect on the current is proportional to the ratio between the excited aged PMOS transistors and the total number of transistors.

### *B. Aging Effect on Classical CPA*

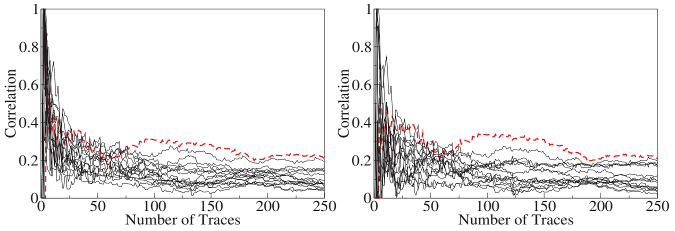
*1) Gate-level Masking:* The masking S-box with XOR and register circuit is shown in Fig. 1(b). The masking S-box has two additional input masks and one output mask. Mask $m_1$ is for the input values and mask $m_2$ is for the intermediate value of AND gates. Mask $m_3$ is for the output values.

The circuit has 57 gates and 37 gates were aged by using our NBTI acceleration framework. We performed 4096 simulations with all possible values of input $x$, mask $m_1$ and $m_3$. We generate random values $m_2$ in each simulation. The attack results of the baseline circuit is shown in Fig. 6(a) The correlation of the correct key in dotted line is clearly higher than the wrong key hypotheses. Fig. 6(b) shows the attack results on the aged masked S-box, which is slightly lower than a wrong key hypothesis.



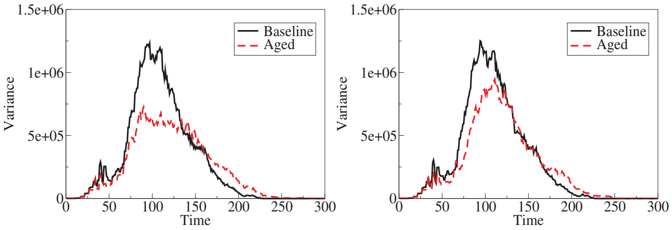
(a) (b)

Fig. 8: CPA on the MDPL PRESENT S-box ($m$,$\overline{m}$)=(0,1) (a) baseline (b) aged



(a) (b)

Fig. 9: CPA on the MDPL PRESENT S-box. ($m$,$\overline{m}$)=(1,0) (a) baseline (b) aged



(a) (b)

Fig. 10: The variance of the traces of the baseline and aged MDPL PRESENT S-box (a) ($m$,$\overline{m}$)=(0,1) (b) ($m$,$\overline{m}$)=(1,0)

TABLE III: The number of failed and successful template attack with baseline and aged designs as templates.

| Design | Baseline as template | | Aged as template | |
|---|---|---|---|---|
| | Fail | Success | Fail | Success |
| Unprotected | 236 | 20 | 244 | 12 |
| Masking | 238 | 18 | 232 | 24 |
| MDPL($m$,$\overline{m}$)=(0,1) | 239 | 17 | 237 | 19 |
| MDPL($m$,$\overline{m}$)=(1,0) | 243 | 13 | 241 | 15 |

Fig. 7(b) shows the relationship between the percentage of the vectors and the percentage of the excited aged gates (number of excited aged gates divided by the total number of gates). The input vectors excites around 25-65% percent of the aged gates and most of the input vectors excites 30-55% of the aged gates among all the gates, each of these gates reduces the data-dependent power consumption of the circuit. NBTI aging increases the $V_{th}$ of the PMOS transistors. As a result, the variance of the aged circuit decreases compared to the baseline (as it can be seen from Fig. 7(a)) This has a negative impact on the data-dependent leakage, and make the CPA slightly more difficult.

*2) MDPL:* We perform CPA on the MDPL implementation shown in Fig. 1(c). The input of the circuit is key $k$, data $x$, and mask $m$. The circuit first generates the complementary values of $k$, $x$, and $m$. Then, each signal and its complement are computed by the MDPL XOR and MDPL S-box. The results stored in the registers are complementary to each other.

In our first attack, we set ($m$, $\overline{m}$)=(0, 1). We simulated 256 all possible input data transitions. The attack results of the baseline and the aged circuits are shown in Fig. 8(a) and Fig. 8(b), respectively. The correlation of the correct key is the dotted line. In our second attack, we set ($m$, $\overline{m}$)=(1, 0). We simulated 256 all possible input data transitions. The attack results of the baseline and the aged circuits are shown in Fig. 9(a). and Fig. 9(b), respectively.

The decrease in the correlation in both attacks seems counter-intuitive because NBTI aging on the cirtical path can increase the imbalance between the delays of the two rails. In fact, the delay variation between the aged and the baseline designs under the same input transitions shows that the delay variation for different input values and mask values is more significant after aging, and that the imbalance between the rails is significantly larger after NBTI aging. Both effect should increase the leakage of MDPL exploitable by classical CPA.

However, the situation is similar to that of gate-level masking. Fig. 10(a) and 10(b) show the variance of the power traces for ($m$,$\overline{m}$)=(0,1) and ($m$,$\overline{m}$)=(1,0), respectively. For both cases, the variance of the aged design decreases compared to the baseline one. This has a negative impact on the data-dependent leakage. Therefore, after aging, the degradation of the data-dependent power consumption seems to overshadow the delay variation effect.

### C. Template Attack

In the typical scenario, the template is built from one device to attack the identical one or a different device when process variation was not determinant, the information leakage of the device used to create the template were suitable for attacking another device. This was not true already at 65nm [9]. However, it was shown that using a sufficient number of chip, the template constructed could still be used. We analyze the effect of aging on template attacks. Similar to process variations, aging causes that chips supposed to be identically have, in reality, differences in the power profile as well as in timing. Therefore the template constructed using aged devices might not be suitable to carry out successful the attack. In the rest of the session, we will discuss the results we obtained mounting template attacks on aged devices.

The template attack is significantly affected by aging, as shown in Table III. We first build template using the baseline circuit and attack the aged circuit, using the approach proposed in [13]. Then we build template using the aged circuit and attack the baseline circuit. For each design, we performed all possible 256 attacks. When the baseline is used as template to attack the aged circuit, the success rate is between 5.3-8.5%. When the aged circuit is used as template to attack the baseline circuit, the success rate is between 4.9-10.3%. Both results are significantly lower than the 100% success rate when the baseline template is applied to the baseline circuit and when the aged template is applied to the aged circuit. This results shows that while building a template, the adversary has to consider the potential aging which could have happened to the circuit under attack or to the circuit used to build the template.

## V. Discussion

**NBTI effect and process variation.** The effect of process variation for 65nm devices on power analysis was studied in [9]. It is shown that the traditional way of evaluating the resistance against power analysis is not sufficient at the presence of process variation. Besides process variation, NBTI is another important concern in advanced technology nodes. While process variation is determined right after chip fabrication, NBTI aging is an effect that impacts the chip during its life time. Moreover, our study focuses on the impact of NBTI aging for a certain chip before and after aging and process variation will not affect a certain chip during this experiment. In summary, one should consider both effects while evaluating the resistance against power analysis and analyze them depending on the attacker model.

**NBTI effect on other block ciphers.** The experimental results were obtained from PRESENT which is a lightweight block cipher in ISO/IEC 29192-2:2012 standard [24]. Its structure is similar to other block ciphers based on substitution and permutation networks such as AES. The results presented can thus be considered sufficiently general and representative of the aging effect on block ciphers in general.

## VI. Conclusion

Power analysis is a serious threat to cryptographic device. In this paper, we analyzed the effect of NBTI aging on power-based side channel attack. Our experiments, carried out using PRESENT implementation with gate-level masking and MDPL shows that the power model used for baseline circuit is not immediately suitable for the aged one, especially when using template attacks. Additionally, although NBTI aging increases the imbalance among different paths, it also reduces the short-circuit power consumption, affecting slightly negatively the classical CPA attacks. We showed the impact of NBTI on side channel attacks. As a continuation of this work, we extend the scope of aging effects and we investigate the effect of other aging mechanisms including Hot Carrier Injection, Oxide Breakdown, and Positive Bias Temperature Instability on the effectiveness of power side channel attacks.

## Acknowledgment and Disclaimer

We thank the reviewers' comments and Rui Yang for his help in the experiments. We thank Prof. Christof Paar for the discussions. This material is based upon work supported by the NSF CNS program under grant 0831349. The views expressed in this paper solely belong to the authors and do not in anyway reflect the views of Intel Corporation. The countermeasures described in this paper were implemented in experimental hardware and software environments. The authors of this paper have not explored the potential applicability of these countermeasures to commercially available hardware and software.

## References

[1] S. Chakravarthi, A. Krishnan, V. Reddy, C. F. Machala, and S. Krishnan, "A comprehensive framework for predictive modeling of negative bias temperature instability," *In Proc. Reliability Physics Symp.*, pp. 273–282, Apr. 2004.

[2] H. Kufluoglu and M. A. Alam, "A generalized reaction-diffusion model with explicit h-h2 dynamics for negative-bias temperature-instability (nbti) degradation," *IEEE Trans. on Electron Devices*, vol. 54, no. 5, pp. 1101–1107, 2007.

[3] S. Wang, G. Duan, C. Zheng, and T. Jin, "Combating nbti-induced aging in data caches," *In Proc. GLSVLSI*, pp. 215–220, May 2013.

[4] S. Bhardwaj, W. Wang, R. Vattikonda, Y. Cao, and S. Vrudhula, "Predictive modeling of the nbti effect for reliable design," *In Proc. Custom Integrated Circuits Conference*, pp. 189–192, Sept. 2006.

[5] S. Khan, N. Z. Haron, S. Hamdioui, and F. Catthoor, "Nbti monitoring and design for reliability in nanoscale circuits," *In Proc. DFT*, pp. 68–76, Oct. 2011.

[6] M. A. Alam and S. Mahapatra, "A comprehensive model of pmos nbti degradation," *Microelectronics Reliability*, vol. 45, no. 1, pp. 71–81, 2005.

[7] M. A. Alam, H. Kufluoglu, D. Varghese, and S. Mahapatra, "A comprehensive model for pmos nbti degradation: Recent progress," *Microelectronics Reliability*, vol. 47, no. 6, pp. 853–862, 2007.

[8] L. Lin and W. P. Burleson, "Analysis and mitigation of process variation impacts on power-attack tolerance," *In Proc. DAC*, pp. 238–243, Jul. 2009.

[9] M. Renauld, F.-X. Standaert, N. Veyrat-Charvillon, D. Kamel, and D. Flandre, "A formal study of power variability issues and side-channel attacks for nanoscale devices," *In Proc. EUROCRYPT*, pp. 109–128, May 2011.

[10] P. Kocher, J. Jaffe, B. Jun, and P. Rohatgi, "Introduction to differential power analysis," *J. Crypto. Engineering*, vol. 1, no. 1, pp. 5–27, 2011.

[11] E. Brier, C. Clavier, and F. Olivier, "Correlation Power Analysis with a Leakage Model," *In Proc. CHES*, pp. 16–29, Sept. 2004.

[12] B. Gierlichs, L. Batina, P. Tuyls, and B. Preneel, "Mutual information analysis," *In Proc. CHES*, pp. 426–442, Aug. 2008.

[13] S. Chari, J. Rao, and P. Rohatgi, "Template attacks," *In Proc. CHES*, pp. 13–28, Sept. 2003.

[14] Z. Chen and Y. Zhou, "Dual-rail random switching logic: A countermeasure to reduce side channel leakage," *In Proc. CHES*, pp. 242–254, Oct. 2006.

[15] E. Trichina, "Combinational logic design for aes subbyte transformation on masked data," Cryptology ePrint Archive, Report 2003/236, 2003, http://eprint.iacr.org/.

[16] K. Tiri and I. Verbauwhede, "A logic level design methodology for a secure dpa resistant asic or fpga implementation," *In Proc. DATE*, pp. 246–251, Feb. 2004.

[17] T. Popp and S. Mangard, "Masked dual-rail pre-charge logic: Dpa-resistance without routing constraints," *In Proc. CHES*, pp. 172–186, Aug. 2005.

[18] T. Popp, M. Kirschbaum, T. Zefferer, and S. Mangard, "Evaluation of the masked logic style mdpl on a prototype chip," *In Proc. CHES*, pp. 81–94, Sept. 2007.

[19] S. Mangard, T. Popp, and B. M. Gammel, "Side-channel leakage of masked cmos gates," *In Proc. CT-RSA*, pp. 351–365, Feb. 2005.

[20] M. G. K. K. J. Kulikowski, , and A. Taubin, "Power attacks on secure hardware based on early propagation of data," *In Proc. IOLTS*, pp. 131–138, Jul. 2006.

[21] A. Moradi, M. Kirschbaum, T. Eisenbarth, and C. Paar, "Masked dual-rail precharge logic encounters state-of-the-art power analysis methods," *IEEE Trans. on VLSI*, vol. 20, no. 9, pp. 1578–1589, 2012.

[22] W. Wang, S. Yang, S. Bhardwaj, S. Vrudhula, F. Liu, and Y. Cao, "The impact of nbti effect on combinational circuit: Modeling, simulation, and analysis," *IEEE Trans. on VLSI*, vol. 18, no. 2, pp. 173–183, 2010.

[23] A. Bogdanov, L. Knudsen, G. Leander, C. Paar, A. Poschmann, M. Robshaw, Y. Seurin, and C. Vikkelsoe, "PRESENT: An ultra-lightweight block cipher," *In Proc. CHES*, pp. 450–466, Sept. 2007.

[24] I. 29192-2:2012, "Information technology – security techniques – lightweight cryptography," http://www.iso.org/iso/iso_catalogue /catalogue_tc/catalogue_detail.htm?csnumber=56552, 2012.