Normalized Differential Power Analysis - for ghost peaks mitigation

Chen, Juncheng; Ng, Jun-Sheng; Kyaw, Nay Aung; Lwin, Ne Kyaw Zwa; Ho, Weng-Geng;
Chong, Kwen-Siong; Lin, Zhiping; Chang, Joseph Sylvester; Gwee, Bah-Hwee

2021

Chen, J., Ng, J., Kyaw, N. A., Lwin, N. K. Z., Ho, W., Chong, K., Lin, Z., Chang, J. S. & Gwee, B. (2021). Normalized Differential Power Analysis - for ghost peaks mitigation. 2021 IEEE International Symposium on Circuits and Systems (ISCAS).
<https://dx.doi.org/10.1109/ISCAS51556.2021.9401487>

<https://hdl.handle.net/10356/151136>

<https://doi.org/10.1109/ISCAS51556.2021.9401487>

© 2021 IEEE. Personal use of this material is permitted. Permission from IEEE must be obtained for all other uses, in any current or future media, including reprinting/republishing this material for advertising or promotional purposes, creating new collective works, for resale or redistribution to servers or lists, or reuse of any copyrighted component of this work in other works. The published version is available at:
<https://doi.org/10.1109/ISCAS51556.2021.9401487>

Downloaded on 26 Apr 2023 20:53:46 SGT

Normalized Differential Power Analysis - For Ghost Peaks Mitigation

Juncheng Chen*, Jun-Sheng Ng, Nay Aung Kyaw, Ne Kyaw Zwa Lwin, Weng-Geng Ho,
Kwen-Siong Chong, Zhiping Lin, Joseph Sylvester Chang, Bah-Hwee Gwee

School of Electrical and Electronic Engineering

Nanyang Technological University

50 Nanyang Avenue, Singapore 639798

Email: *juncheng002@e.ntu.edu.sg

Abstract—The attack efficacy of Differential Power Analysis (DPA), a popular side channel evaluation technique for key extraction, is compromised by the false highest Difference Of Means (DOMs) value (‘ghost peaks’) in the DOMs matrix produced in a conventional DPA. The ghost peak is generated by the wrong key guess and always occurs in the conventional DPA when the number of side channel traces is not enough. In this paper, an improved version of the conventional DPA termed as Normalized DPA (NDPA) is proposed to circumvent the ghost peak. With the analysis on the generation of ghost peaks in the conventional DPA, we observed that by normalizing the DOMs matrix, the ghost peaks can be greatly suppressed. We model the proposed NDPA mathematically and show that it performs better than the conventional DPA. We further provide the experimental validations on a set of 200k power simulation traces on AES S-Box and 500 EM traces from ASCAD dataset. Based on the attack results of these datasets, our proposed NDPA requires (up to 68%) lesser number of traces to reveal a correct key when compared to the conventional DPA.

Index Terms—Differential Power Analysis (DPA), Normalized Differential Power Analysis (NDPA), ghost peaks, Advanced Encryption Standard (AES)

I. INTRODUCTION

Side channel attack (SCA) has been a non-negligible threat to hardware devices with confidential information [1], [2]. SCA targets on the side channel where the physical leakage information is generated. Compared to other invasive and semi-invasive attacks, SCA is a comparatively ‘easier’ and ‘cheaper’ way to extract confidential information. SCAs include non-profiling SCA [3], [4], [5], [6] and profiling SCA [7], [8], [9]. Profiling SCA features the most powerful leakage detection capability but requires a copy of the targeted device for building a template before the attack. This makes profiling SCA not applicable when the copy of the targeted device is not available. The non-profiling SCA, including differential power analysis (DPA) [10], correlation power analysis (CPA) [4], etc., is more popular due to its applicability with or without the copied device.

As DPA performs attack based on a bit model, it is very effective when the device leaks information only at certain bits instead of the entire byte of data [11]. This type of devices is most vulnerable to DPA which extracts secret keys by comparing the DOMs based on a bit model. However,

the so-called “ghost peaks” [12] restricts the efficacy of the conventional DPA. Unlike CPA which gives a normalized result (correlations range from -1 to 1), the conventional DPA compares the absolute values of DOMs at different sample points. This means that the non-uniform side channel signals strength at different sample points could influence the result significantly in the presence of ghost peaks. A conventional approach to overcome it, is by using more side channel traces to reveal the correct key. In this paper, we propose a Normalized Differential Power Analysis (NDPA) which can suppress the ghost peaks by normalizing the DOMs matrix generated in the conventional DPA. The contributions of this paper can be summarized as follows:

- We investigate the cause of ghost peaks by modelling the whole DPA attack process.
- We propose the NDPA to increase the attack efficacy by suppressing ghost peaks and model the NDPA mathematically.
- We perform two experiments to validate the attack efficacy improvement based on the proposed NDPA - first involves the power dissipation attack of 200k simulated power traces and the second involves the attack of EM traces from the ASCAD dataset [8].

The remainder of the paper is organized as follows. Section II reviews the conventional DPA and summarizes the attack process. Section III provides the investigation on the generation of the ghost peaks. Section IV proposes the NDPA and models it mathematically to show it be more efficient than the conventional DPA. Section V presents the attack results of the conventional DPA and the proposed NDPA on the simulated power traces and ASCAD dataset. Section VI concludes the paper.

II. REVIEW OF CONVENTIONAL DIFFERENTIAL POWER ANALYSIS

The conventional DPA was reported in 1998 [3]. Subsequently, several variants of DPAs were reported which include Differential Electromagnetic Analysis (DEMA) [13] to exploit the electromagnetic emanation instead of power dissipation. The conventional DPA and DEMA are based on the assumption that the mean of the power used to compute a logic ‘0’ and a logic ‘1’ are different at any bit position from a

intermediate circuit node. The formulation of the conventional DPA is elaborated as follows.

Conventional DPA starts with the collection of data. First, Set $\mathcal{T} = \{T_i \mid i \in [0, N-1]\}$ containing N side-channel traces and its corresponding plaintext set $\mathcal{PT} = \{PT_i \mid i \in [0, N-1]\}$ containing N plaintext PT_i are recorded. Every T_i includes M sample points. The side channel signal of the j^{th} sample point in a side channel trace T_i is $T_i[j]$. With an n -bit secret key k belonging to $\mathcal{K} = \{k \mid k \in [0, 2^n - 1]\}$, and an n -bit plaintext PT_i belonging to $\mathcal{PT} = \{PT_i \mid i \in [0, N-1]\}$ as inputs. For completeness, should the last round of block ciphers be targeted, a ciphertext set $\mathcal{CT} = \{CT_i \mid i \in [0, N-1]\}$ should be used instead. A selection function $f(k, PT_i) = b$ is defined to partition all the side channel traces into the first sub-set that has $b = 0$, and the second sub-set that has $b = 1$. b is a bit logic value computed at the targeted intermediate circuit node, which is expressed in (1). With 2^n different key guesses, 2^n different partitions could take place with each partition producing two sub-sets $\mathcal{T}^{k_0}$ and $\mathcal{T}^{k_1}$.

$$\begin{aligned} \mathcal{T}^{k_0} &= \{T_i \mid f(k, PT_i) = 0\} \\ \mathcal{T}^{k_1} &= \{T_i \mid f(k, PT_i) = 1\} \end{aligned} \quad (1)$$

where $i \in [0, N-1], k \in [0, 2^n - 1]$.

For each sub-set $\mathcal{T}^{k_b}$, a mean trace A^{k_b} computed in a pointwise sense is expressed in (2).

$$\begin{aligned} A_{mean}^{k_0} &= \frac{1}{|\mathcal{T}^{k_0}|} \sum_{T_i \in \mathcal{T}^{k_0}} T_i \\ A_{mean}^{k_1} &= \frac{1}{|\mathcal{T}^{k_1}|} \sum_{T_i \in \mathcal{T}^{k_1}} T_i \end{aligned} \quad (2)$$

where $|\mathcal{T}^{k_0}| + |\mathcal{T}^{k_1}| = N$.

In (3), D_{mean}^k is defined as the DOMs trace representing the absolute value of the difference between A^{k_0} and A^{k_1} .

$$D_{mean}^k = |A_{mean}^{k_0} - A_{mean}^{k_1}| \quad (3)$$

With all the DOMs traces D_{mean}^k , produced by 2^n different key guess k , a maximum leakage detection function $l(k)$ is defined to detect and return the maximum value $D_{mean}^k[j]$ in D_{mean}^k . By comparing 2^n different output of $l(k)$, the key guess associated with the largest output of $l(k)$ is considered to be the correct key guess k_c , which can be described by (4) and (5).

$$l(k) = \max\{D_{mean}^k[j] \mid j \in [0, M-1]\} \quad (4)$$

$$k_c = \arg \max_{k \in \mathcal{K}} l(k) \quad (5)$$

III. ANALYSIS ON GHOST PEAKS

The conventional DPA presented in Section II can reveal the correct key guess successfully at the sample points associated with the targeted intermediate circuit node. We group the location of these sample points as the leaky region. The locations of the rest of the sample points can then be grouped as non-leaky region. However, it is always difficult for an

Fig. 1. DOMs with Ghost peaks for conventional DPA

adversary to identify where the exact leaky region is. In practice, when all sample points are attacked together, the peaks associated with the correct key guess in the leaky region could be lower than the false peaks associated with the wrong key guesses in the non-leaky region. Those false peaks that are higher than the peaks associated with the correct key guess are termed as ‘ghost peaks’. As shown in Fig. 1, the ghost peaks in the non-leaky region have higher DOMs than those generated by the correct key guess. Even though the correct key guess produces the highest peak at point j_1 in the leaky region, this peak could still be lower than the peaks produced by some wrong key guesses at point j_2 in the non-leaky region. In this section, we will analyse the cause of ghost peaks.

We define a model of side channel signal including linear, constant and Gaussian noise components at sample point j as:

$$P_j = a_j H + C_j + w \quad (6)$$

where H represents a hypothesis power model (such as Hamming Weight and Hamming Distance) and it correlates to the linear component of the side channel signals through a coefficient a_j at sample point j . C_j and w represent the constant and the Gaussian noise components of the side channel signal at sample point j respectively. All the sample points are assumed to process the same level of Gaussian noise. Based on (6), side channel signal at sample point j in T_i from $\mathcal{T}^{k_b}$ can be represented as:

$$P_j^{k_b} = a_j H^{k_b} + C_j + w \quad (7)$$

In a conventional DPA once the data collection is done, side channel traces need to be partitioned based on $f(PT_i, k) = b$ ($b = 0$ or $b = 1$). According to (3) and (7), the DOMs signal $D_{mean}^k[j]$ generated by any key guess k at sample point j is expressed in (8):

$$\begin{aligned} D_{mean}^k[j] &= |A_{mean}^{k_0}[j] - A_{mean}^{k_1}[j]| \\ &= |E\{P_j^{k_0}\} - E\{P_j^{k_1}\}| \\ &= |E\{a_j H^{k_0}\} - E\{a_j H^{k_1}\}| \\ &= |a_j \Delta_k| \end{aligned} \quad (8)$$

where error $\Delta_k = E\{H^{k_0}\} - E\{H^{k_1}\}$. When $k = k_c$ (correct key), $|\Delta_k| = |E\{H^{k_{c0}}\} - E\{H^{k_{c1}}\}| = |E\{1bit\} \cdot \#(untargeted\ bits) + 0(b=0) - E\{1bit\} \cdot \#(untargeted\ bits) + 1(b=1)| = 1$, which is the maximum of $|\Delta_k|$. When $k = k_w$ (wrong key), the value of b is not calculated correctly. Thus, $\mathcal{T}^{k_{w0}}$ and $\mathcal{T}^{k_{w1}}$ both contain side channel traces corresponding to $b=0$ and $b=1$, making $|\Delta_{k_w}| < 1$. The DOMs matrix of DPA contains $|\mathcal{K}| \times M$ different $|a_j \Delta_k|$ to be compared to determine the correct key guess in (4) and (5). The key guess k corresponding to the largest $|a_j \Delta_k|$ assumes to be the correct key. The comparison among different $|a_j \Delta_k|$ will involve a_j from different sample point. If the values of a_j are very different across the whole side channel trace, the correct key guess determined by comparing these DOMs may not be correct as these values are not normalized. In short, the difference among $|a_j|$ from different sample points is the major cause for ghost peaks generation which compromises the extraction of correct.

IV. PROPOSED NORMALIZED DIFFERENTIAL POWER ANALYSIS

To circumvent the ghost peaks issue caused by the significant change of a_j at different sample points, normalized DPA (NDPA) is proposed. Before comparing the DOMs in the raw DOMs matrix, the proposed NDPA requires one additional step to sum all the DOMs signals in every column of the DOMs matrix, followed by further calculating the contribution of each DOMs signal. We then compare the normalized DOMs signals instead of comparing the raw DOMs signals. Intuitively, this process can be considered as bringing all the peaks as shown in Fig. 1 to the same scale for comparison. In this section, an analysis of this process will be performed. The 2^n DOMs traces calculated from (3) with 2^n different key guesses k yields a $|\mathcal{K}| \times M$ DOMs matrix D as:

$$D = \begin{pmatrix} D^0[0] & \dots & D^0[j] & \dots & D^0[M-1] \\ D^1[0] & \dots & D^1[j] & \dots & D^1[M-1] \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ D^{|\mathcal{K}|-1}[0] & \dots & D^{|\mathcal{K}|-1}[j] & \dots & D^{|\mathcal{K}|-1}[M-1] \end{pmatrix} \quad (9)$$

Fig. 1 is plotted from a DOMs matrix. As discussed, we can normalize the summation of $D^k[j]$ in each column j , $\sum_{k \in \mathcal{K}} D^k[j]$, to 1 and calculate what percentage each $D^k[j]$ contributes. In the non-leaky region, or non-leaky columns, although some wrong key guesses could produce a large $D^{k_w}[j]$, each $D^{k_w}[j]$ will contribute only a small percentage of $\sum_{k \in \mathcal{K}} D^k[j]$ since many wrong key guesses could produce similar scale of $D^{k_w}[j]$ at the same column. Whereas in the leaky columns, only the correct key is likely to produce a comparably larger $D^{k_c}[j]$, meaning a bigger share among all the $D^k[j]$. After normalization, the DOMs matrix becomes:

$$D' = \begin{pmatrix} \frac{D^0[0]}{\sum_{k \in \mathcal{K}} D^k[0]} & \dots & \frac{D^0[j]}{\sum_{k \in \mathcal{K}} D^k[j]} & \dots & \frac{D^0[M-1]}{\sum_{k \in \mathcal{K}} D^k[M-1]} \\ \frac{D^1[0]}{\sum_{k \in \mathcal{K}} D^k[0]} & \dots & \frac{D^1[j]}{\sum_{k \in \mathcal{K}} D^k[j]} & \dots & \frac{D^1[M-1]}{\sum_{k \in \mathcal{K}} D^k[M-1]} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ \frac{D^{|\mathcal{K}|-1}[0]}{\sum_{k \in \mathcal{K}} D^k[0]} & \dots & \frac{D^{|\mathcal{K}|-1}[j]}{\sum_{k \in \mathcal{K}} D^k[j]} & \dots & \frac{D^{|\mathcal{K}|-1}[M-1]}{\sum_{k \in \mathcal{K}} D^k[M-1]} \end{pmatrix} \quad (10)$$

As shown in Fig. 1, we perform the NDPA, on points j_1 and j_2 , where the targeted byte has n bits and the number

of key guess is 2^n . Suppose the correct key guess is k_c , the $2^n - 1$ wrong key guesses are $k_{w_1} \dots k_{w_{2^n-1}}$, then the DOMs signals produced by all the key guesses at point j_1 and point j_2 are shown in Table I.

TABLE I
DOMS SIGNAL FOR DIFFERENT KEY GUESS AT SAMPLE POINT j_1 AND j_2

	point j_1	point j_2
k_c	$ a_{j_1} $	$ a_{j_2} \Delta_{j_2}^0 $
k_{w_1}	$ a_{j_1} \Delta_{j_1}^1 $	$ a_{j_2} \Delta_{j_2}^1 $
$\dots$	$\dots$	$\dots$
k_{w_q}	$ a_{j_1} \Delta_{j_1}^q $	$ a_{j_2} \Delta_{j_2}^q $
$\dots$	$\dots$	$\dots$
$k_{w_{2^n-1}}$	$ a_{j_1} \Delta_{j_1}^{2^n-1} $	$ a_{j_2} \Delta_{j_2}^{2^n-1} $

Where $\Delta_{j_1}^q$ and $\Delta_{j_2}^q$ are the DOMs of the hypothesis model produced by a wrong key guess k_{w_q} at point j_1 and j_2 respectively. Note that since the targeted intermediate circuit node is not located at point j_2 , there is no 'correct' key at point j_2 . Since point j_1 is located in the leaky region, $|a_{j_1}|$ is greater than any $|a_{j_1} \Delta_{j_1}^q|$ ($\Delta_{j_1}^q < 1$). However, $|a_{j_1}|$ could still be smaller than $|a_{j_2} \Delta_{j_2}^q|$ if $|a_{j_2}|$ is large enough in a conventional DPA. Whereas in the proposed NDPA, a normalization is applied at the DOMs matrix. The normalized DOMs signal $D_{mean}^{k_c}[j_1]$ produced by the correct key k_c at point j_1 is:

$$D_{mean}^{k_c}[j_1] = \frac{|a_{j_1}|}{|a_{j_1}|(|\Delta_{j_1}^1| + \dots + |\Delta_{j_1}^{2^n-1}|) + |a_{j_1}|} \quad (11)$$

At point j_2 , the DOMs signal $D_{mean}^{k_{w_q}}[j_2]$ produced by k_{w_q} , $|a_{j_2} \Delta_{j_2}^q|$ is also normalized in (12).

$$D_{mean}^{k_{w_q}}[j_2] = \frac{|a_{j_2} \Delta_{j_2}^q|}{|a_{j_2}|(|\Delta_{j_2}^0| + \dots + |\Delta_{j_2}^{2^n-1}|)} \quad (12)$$

To be able to extract the correct key, $D_{mean}^{k_c}[j_1]$ must be greater than $D_{mean}^{k_{w_q}}[j_2]$. This being the case, the error threshold $|\Delta_{j_2}^q|$ for any wrong key guess k_{w_q} not to generate ghost peaks in at point j_2 in the proposed NDPA is:

$$|\Delta_{j_2}^q| < \frac{|\Delta_{j_2}^0| + |\Delta_{j_2}^1| + \dots + |\Delta_{j_2}^{2^n-1}|}{|\Delta_{j_1}^1| + |\Delta_{j_1}^2| + \dots + |\Delta_{j_1}^{2^n-1}| + 1} = \frac{(|\Delta_{j_2}^0| + \dots + |\Delta_{j_2}^{q-1}| + |\Delta_{j_2}^{q+1}| + \dots) + |\Delta_{j_2}^q|}{(|\Delta_{j_1}^1| + |\Delta_{j_1}^2| + \dots) + 1} \quad (13)$$

When $k = k_w$ (wrong key guess), all the side channel traces are partitioned based on a wrongly calculated b . All the $|\Delta_{j_1}^q|$ and all the $|\Delta_{j_2}^q|$ can be considered two sample sets from a same population. If we define the population mean as Δ ($\Delta \geq 0$), Δ will be very close to the sample means of the two sample sets when the number of the side channel traces is large enough. Then (13) becomes (14).

$$\begin{aligned} |\Delta_{j_2}^q| &< \frac{(\Delta + \Delta + \dots + \Delta) + |\Delta_{j_2}^q|}{(\Delta + \Delta + \dots + \Delta) + 1} \\ &= \frac{(2^n - 1)\Delta + |\Delta_{j_2}^q|}{(2^n - 1)\Delta + 1} \end{aligned} \quad (14)$$

If we define this error threshold as Δ_{norm} , we can obtain:

$$|\Delta_{j_2}^q| < \Delta_{norm} \quad (15)$$

Since $|\Delta_{j_2}^q|$ is smaller than 1, (14) implies that (15) will not be violated, which means no ghost peak exists. The error threshold Δ_{norm} is now independent of a_j .

V. EVALUATION OF THE PROPOSED NORMALIZED DIFFERENTIAL POWER ANALYSIS

As depicted in Fig. 2, we first show the attack results of the conventional DPA and the proposed NDPA on the bit 6 of an AES S-Box with 200k simulated power traces. The power traces are obtained from the simulation run in Synopsys PrimeTime using 65nm CMOS process library cells.

Fig. 2. DOMs obtained by attacking bit 6 of an AES S-Box with 200k simulated power traces for (a) Conventional DPA and (b) Proposed NDPA

The red curves in Fig. 2(a) and Fig. 2(b) indicate the DOMs traces generated by the correct key. With 200k traces, the conventional DPA fails to reveal the correct key while the proposed NDPA reveals the correct key with a very high confidence level. Here, the confidence level is estimated by difference between the peak produced by the correct key guess and the highest peak produced by a wrong key guess. The ghost peaks in Fig. 2(a) are effectively removed in Fig. 2(b).

In the second experiment, the conventional Differential Electro-Magnetic Analysis (DEMA) and the proposed Normalized Differential Electro-Magnetic Analysis (NDEMA) are performed on the byte 0 and byte 1 in the ASCAD dataset. Byte 0 and byte 1 in ASCAD dataset have first order leakage because their mask values are forced to 0 during encryption as reported in [8]. The Measure To Disclosure (MTD) plots for byte 0 and byte 1 are shown in Fig. 3 and Fig. 4 respectively. MTD shows the relationship between the number of traces and difference of means for all the key guesses.

The red curves in Fig. 3 and 4 indicates the MTD curves generated by the correct key guess. Fig. 3(a) and Fig. 3(b) show the MTD plots for the conventional DEMA and the proposed NDEMA on byte 0 respectively. For byte 0, the proposed NDEMA reduces the minimum number of traces to reveal the correct key by 14% from 430 traces to 370 traces when compared to the conventional DEMA. Fig. 4(a) and Fig. 4(b) show the MTD plots for the conventional DEMA and the proposed NDEMA on byte 1 respectively. For byte 1, the proposed NDEMA reduces the minimum number of traces to

Fig. 3. MTD obtained by attacking MSB of byte 0 in ASCAD dataset with 500 traces for (a) Conventional DPA and (b) Proposed NDEMA.

Fig. 4. MTD obtained by attacking MSB of byte 1 in ASCAD dataset with 500 traces for (a) Conventional DPA and (b) Proposed NDPA.

reveal the correct key by 68% from 370 traces to 120 traces when compared to the conventional DEMA. In both power simulation traces and the ASCAD dataset, the proposed NDPA and NDEMA demonstrates a significant increase on the attack efficacy.

VI. CONCLUSIONS

In this work, we have proposed the Normalized Differential Power Analysis (NDPA) or the Normalized Differential Electro-Magnetic Analysis (NDEMA) through normalizing the Difference Of Means (DOMs) matrix produced in a conventional DPA or DEMA. We have provided both theoretical proof as well as experimental validation. For the designs with first order leakage as in the case of AES, the proposed NDEMA outperforms the conventional DEMA using as few as 68% of traces collected for conventional DEMA, when the model of side-channel signal is accurate.

ACKNOWLEDGMENT

This research project is supported by the National Research Foundation, Singapore under its National Cybersecurity R&D (NCR) Research Programme in Assuring Hardware Security by Design in Systems on Chip, SOCure (NRF2018NCR-NCR002-001).

REFERENCES

- [1] K. Tiri, "Side-channel attack pitfalls," in *Proc. 2007 44th ACM/IEEE Design Automation Conference*, 2007, pp. 15–20.
- [2] Y. Xiang, Y. Xu, Y. Li, W. Ma, Q. Xuan, and Y. Liu, "Side-channel gray-box attack for dnnns," *IEEE Transactions on Circuits and Systems II: Express Briefs*, pp. 1–1, 2020.

- [3] P. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," in *Proc. Advances in Cryptology — CRYPTO' 99*, M. Wiener, Ed. Berlin, Heidelberg: Springer Berlin Heidelberg, 1999, pp. 388–397.
- [4] E. Brier, C. Clavier, and F. Olivier, "Correlation power analysis with a leakage model," in *Proc. Cryptographic Hardware and Embedded Systems - CHES 2004*, M. Joye and J.-J. Quisquater, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2004, pp. 16–29.
- [5] B. Gierlichs, L. Batina, P. Tuyls, and B. Preneel, "Mutual information analysis," in *Proc. Cryptographic Hardware and Embedded Systems - CHES 2008*, E. Oswald and P. Rohatgi, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2008, pp. 426–442.
- [6] J. S. Ng, J. Chen, N. A. Kyaw, N. K. Z. Lwin, W. G. Ho, K. S. Chong, and B. H. Gwee, "A highly efficient power model for correlation power analysis (cpa) of pipelined advanced encryption standard (aes)," in *Proc. 2020 IEEE International Symposium on Circuits and Systems (ISCAS)*, 2020, pp. 1–5.
- [7] S. Chari, J. R. Rao, and P. Rohatgi, "Template attacks," in *Proc. Cryptographic Hardware and Embedded Systems - CHES 2002*, B. S. Kaliski, ç. K. Koç, and C. Paar, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2003, pp. 13–28.
- [8] E. Prouff, R. Strullu, R. Benadjila, E. Cagli, and C. Canovas, "Study of deep learning techniques for side-channel analysis and introduction to ascad database," *IACR Cryptol. ePrint Arch.*, vol. 2018, p. 53, 2018.
- [9] B. Gierlichs, K. Lemke-Rust, and C. Paar, "Templates vs. stochastic methods," in *Cryptographic Hardware and Embedded Systems - CHES 2006*, L. Goubin and M. Matsui, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2006, pp. 15–29.
- [10] T. Messerges, E. Dabbish, and R. Sloan, "Investigations of power analysis attacks on smartcards," in *Proc. USENIX Workshop Smartcard Technology*, 1999, pp. 151–161.
- [11] S. Mangard, N. Pramstaller, and E. Oswald, "Successfully attacking masked aes hardware implementations," in *Proc. Cryptographic Hardware and Embedded Systems - CHES 2005*, J. R. Rao and B. Sunar, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2005, pp. 157–171.
- [12] S. Guilley, P. Hoogvorst, and R. Pacalet, "Differential power analysis model and some results," in *Smart Card Research and Advanced Applications VI*, J.-J. Quisquater, P. Paradinas, Y. Deswarte, and A. A. El Kalam, Eds. Boston, MA: Springer US, 2004, pp. 127–142.
- [13] G. Ding, Z. Li, X. Chang, and Q. Zhao, "Differential electromagnetic analysis on aes cryptographic system," in *Proc. 2009 Second Pacific-Asia Conference on Web Mining and Web-based Application*, 2009, pp. 120–123.