Research Article

A Highly Effective Data Preprocessing in Side-Channel Attack Using Empirical Mode Decomposition

ShuaiWei Zhang^{1,2}, XiaoYuan Yang¹, Lin Chen,¹ and Weidong Zhong¹

¹Key Laboratory of Network and Information Security Under the People's Armed Police, Engineering University of People's Armed Police, Xi'an 710086, China

²Academy of People's Armed Police, Beijing 100012, China

Correspondence should be addressed to XiaoYuan Yang; yxyangyxyang@163.com

Received 5 February 2019; Revised 24 September 2019; Accepted 8 October 2019; Published 30 October 2019

Guest Editor: Giovanni Agosta

Copyright © 2019 ShuaiWei Zhang et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Side-channel attacks on cryptographic chips in embedded systems have been attracting considerable interest from the field of information security in recent years. Many research studies have contributed to improve the side-channel attack efficiency, in which most of the works assume the noise of the encryption signal has a linear stable Gaussian distribution. However, their performances of noise reduction were moderate. Thus, in this paper, we describe a highly effective data-preprocessing technique for noise reduction based on empirical mode decomposition (EMD) and demonstrate its application for a side-channel attack. EMD is a time-frequency analysis method for nonlinear unstable signal processing, which requires no prior knowledge about the cryptographic chip. During the procedure of data preprocessing, the collected traces will be self-adaptably decomposed into sum of several intrinsic mode functions (IMF) based on their own characteristics. And then, meaningful IMF will be reorganized to reduce its noise and increase the efficiency of key recovering through correlation power analysis attack. This technique decreases the total number of traces for key recovering by 17.7%, compared to traditional attack methods, which is verified by attack efficiency analysis of the SM4 block cipher algorithm on the FPGA power consumption analysis platform.

1. Introduction

A safe encryption system must be reliably realized for every section from the initial design to the final implementation. In the last decades of 20th century, cryptologists emphasized their research studies on the safety of mathematic structures and characteristics for encryption algorithms. However, the safety of implementation was omitted until Paul Kocher proposed a side-channel attack technique in 1996 [1]. Keys were successfully acquired through measuring the leaked physical information from the encrypted device or chip while they were running encryption algorithms. Since then, the page for encryption attack and defense has been turned. Side-channel attack embraced a rapid development in the past decades; many new techniques have emerged, such as timing attack [1], power

consumption attack [2], electromagnetic attack [3], fault attack [4, 5], template attack [6], combinational attack [7–9], and machine learning attack [10–14], resulting in significant safety hazards to encryption system implementations.

Due to limitations of technology, developing new methods for a side-channel attack has reached the bottleneck. More research studies have turned their focus onto improving the attack efficiency. As we know, the amount of the traces needed for correctly recovering the keys is an important indicator for attack efficiency. The higher the signal-to-noise ratio (SNR), the less the amount of traces is needed, leading to higher efficiency. In detail, not only higher SNR for a single trace is needed, but also the noise introduced between the traces, such as alignment, should also be eliminated. This work takes the abovementioned two requirements into consideration and comes up with a

thorough method for data preprocessing to increase attack efficiency.

The remainder of this paper is arranged as follows. In Section 2, the state of the art for data preprocessing including raising SNR and alignment is briefly reported. Section 3 describes the preliminaries of power analysis and EMD algorithm. The proposed scheme of a highly effective data preprocessing in a side-channel attack using EMD is illustrated in Section 4. Then, the measurement setup and result of demonstrating experiments are shown in Section 5. At last, Section 6 concludes the paper.

2. Related Works

Data preprocessing is normally applied to collected traces in the real side-channel attack scenario by the attacker, to reduce the noise and increase attack efficiency. The existence of noise within the traces is significant, including artificially introduced noise [15] (e.g., unstable clock, random delay, and inaccurate triggering) and intrinsic noise of the signal as two main sources.

In terms of analyzing artificially introduced noise, Clavier et al. utilized the method of sliding window DPA [16] to counter the noise problem introduced by random process interrupts. Charvet and Pelletier implemented the wavelet transform [17] to improve the attack efficiency by analyzing clock frequency randomization of the encrypted circuit and resynchronizing the clock. Homma et al. proposed a high-resolution waveform matching method using a phase-only correlation (POC) function to address the displacement problem between waveforms [18]. And Plos et al. discovered DFA, a powerful, fast, and time-invariant analysis which even works in harsh environments with misaligned traces caused by noise and randomization [19]. While regarding minimizing intrinsic noises, van Woudenberg et al. applied the elastic alignment algorithm onto the encrypted power consumption traces to diminish the effect of intrinsic noise and improve attack efficiency [20]. And Le et al. generalized all the noises as Gaussian white noises, and by using the fourth-order cumulant, the noises have been reduced [21].

Nevertheless, most of the abovementioned data-preprocessing methods for noise reduction approximately assume the side-channel traces and their noises as linear stable signals, performing time-frequency analysis with Fourier transform to decrease noises. Since Fourier transform is a global transform, sectional time-frequency characteristics cannot be highlighted, leading to negligence of meaningful encryption information.

This work proposed a data-preprocessing method based on EMD algorithm, separating and reorganizing meaningful traces at different frequencies in the time domain. It simply depends on characteristics of the input traces without any prior knowledge of the encryption devices, which is completely independent of base function. Experimental results of the block cipher algorithm (SM4) with FPGA power consumption analysis platform are reported to have higher efficiency than the traditional attacks without our scheme.

3. Preliminaries

3.1. Power Analysis. Power analysis includes simple power analysis (SPA), differential power analysis (DPA), and correlation power analysis (CPA).

Simple power analysis directly measures power consumption of encryption devices or chips while they are running encryption algorithms and then corresponds the power consumption data with related execution instructions and operands to recover keys with a small amount or even a single power consumption trace. SPA requires fewer experimental conditions and has simple operations; however, the application is limited because it requests prior knowledge of the target's algorithm, specifically, its branches, conditional statements, and sequence of execution instructions.

Differential power analysis is a side-channel attack method, proposed by Paul Kocher et al. in 1999 with the model based on Hamming weight. The method is built on the fact that power consumption for storing "0" is different from that of "1" in the registers, resulting in leakage of power consumption information. DPA employs the statistical difference technique to recover keys, without having any prior knowledge of the algorithm, at a cost of collecting and analyzing more power consumption traces.

Correlation power analysis is published by Brier et al. on CHES conference in 2004 [22]. Its main background for attack is having sufficient plaintext and able to acquire corresponding power consumption traces with different plaintexts. Intermediate state can be calculated by the known plaintext and assumed encryption key after exhausting part of the key. According to the Hamming weight model, the corresponding power consumption is proportional to the Hamming weight of the intermediate state. Function (1) is used to calculate the correlation coefficient of power consumption and its Hamming weight:

$$W = aH(W) + b, \quad (1)$$

where a is the fixed scalar parameter, $H(W)$ is the Hamming weight of the intermediate state, b is the noise independent of the signal, and W is the power consumption of the intermediate state. Finally, correct key is obtained as the correlation coefficient reaches maximum.

3.2. EMD Algorithm. Fourier transform is a signal processing method widely used for linear stable signals in the field of signal analyzing and processing. Overall spectrum of the signal can be obtained through Fourier transform; characteristic spectrum of the target signal is analyzed to help filter out noises from the overall spectrum to achieve noise reduction. But, Fourier transform is not suitable for the side-channel attack because the physical information generated during the processing of encryption devices or chips, such as power consumption and electromagnetic fields are nonlinear unstable signals, and signal frequencies related to key are not fixed as well.

Hereafter, signal processing methods, such as short-time Fourier transform, bilinear time-frequency distribution, and wavelet transform, have been raised to describe nonlinear unstable signals in different aspects, which greatly make up for the shortcomings of Fourier transform. And yet, these methods still belong to global analysis; their analysis capabilities of these methods are directly influenced by the selection of base functions, specifically, the more compatible between the signal and the selected base function, the better analysis result there will be.

While in reality, signal profile varies from one to another; it is extremely difficult to find one base function compatible to all the signals. Under the circumstances, in 1998, Huang et al. from NASA put forward an empirical mode decomposition algorithm [23], a new adaptive time-frequency signal analysis method, which extracts intrinsic mode functions from the signal depends on its own characteristics. This method can be applied to effectively analyze nonlinear unstable encryption signals, which is considered to be a breakthrough in the traditional linear stable time-frequency signal analysis method, as we mentioned before.

4. Our Scheme

In this section, detailed description of the proposed power consumption data-preprocessing method based on the EMD algorithm is given below, together with the power consumption analysis of the SM4 block cipher algorithm, applying chosen plaintext attack introduced in [24, 25].

4.1. Data Preprocessing Based on EMD. Since EMD algorithm assumes that any signal consisted of several finite intrinsic mode functions (IMF), the single signal $x_1(t)$ of the first acquired encryption power consumption trace can be decomposed into intrinsic mode functions by steps (1) to (5):

- (1) Finding out all the maximum points of $x_1(t)$ and obtaining the envelope of them ($e_+(t)$) by fitting with the cubic spline function. Similarly, search for all the minimum points of $x_1(t)$ and also obtain the envelope of them ($e_-(t)$) by fitting with the cubic spline function. $m_1(t)$ is the average of two envelopes:

$$m_1(t) = \frac{e_+(t) + e_-(t)}{2}. \quad (2)$$

- (2) Subtracting $m_1(t)$ from $x_1(t)$ and removing low frequency signal, $h_1^1(t)$ can be acquired:

$$h_1^1(t) = x_1(t) - m_1(t). \quad (3)$$

- (3) In general, $h_1^1(t)$ is an unbalanced signal, which does not satisfy the definition of the intrinsic mode function. Thus, repeat the first two steps for K times, until $h_1^K(t)$ satisfies the definition of the intrinsic

mode function. Component of the first-order intrinsic mode function:

$$c_1(t) = \text{imf}_1(t) = h_1^K(t). \quad (4)$$

- (4) Subtracting $c_1(t)$ from $x_1(t)$ and removing high-frequency signal, $r_1(t)$ can be acquired:

$$r_1(t) = x_1(t) - c_1(t). \quad (5)$$

- (5) Repeat the similar steps of achieving $c_1(t)$ from $h_1^1(t)$ to calculate the component of the second-order intrinsic mode function $c_2(t)$ from $r_1(t)$. These processes are continued Until two conditions followed: firstly, component of the n^{th} order intrinsic mode function $c_n(t)$ or its residue $r_n(t)$ is less than the predefined value; secondly, the residue $r_n(t)$ is a monotonic function or a constant. $x_1(t)$ will be decomposed by EMD into

$$x_1(t) = \sum_{i=1}^n c_i(t) + r_n(t), \quad (6)$$

where $c_1(t), c_2(t), \dots, c_n(t)$ are components of the 1st to n^{th} order intrinsic mode functions, respectively.

Workflow of finding IMF is shown in Algorithm 1.

Moreover, to perform noise reduction on $x_1(t)$, reconstruct components of the 1st to n^{th} order intrinsic mode functions depending on their correlations with the encryption device. Those ones having higher correlations are selected to generate the new trace $x_1(t)'$:

$$x_1(t)' = \sum_{i=\text{select}} c_i(t) + r_n(t), \quad (7)$$

in which select is the set of components having high correlation with the encryption device and $x_1(t)'$ is the first power consumption trace preprocessed by the EMD algorithm.

Finally, iterate the steps from (1) to (6) for all the collected power consumption traces to have $x_1(t)', x_2(t)', \dots, x_m(t)'$.

4.2. Correlation Power Analysis in the Chosen Plaintext Attack. SM4 block cipher algorithm is one of the standard commercial encryption algorithm designed independently in China. Selected as an analysis object, SM4 algorithm is analyzed in this section with correlation power analysis in the chosen plaintext attack, combining the proposed EMD data-preprocessing method.

Structure diagram of the SM4 algorithm is illustrated in Figure 1. Linear transformation L spreads round key into multiple digits of round output, connecting round input and key with every bit of round output, which makes the output become intermediate data of the attack.

However, during power consumption analysis attack, all the 32 bits of round output will be used as intermediate data, leading to a $[0, 2^{32} - 1]$ round key search domain. The

ALGORITHM 1: Workflow of finding IMF.

FIGURE 1: Structure diagram of the SM4 algorithm.

minimum number of power consumption traces needed to be collected and processed is 2^{32} , which makes the idea of using round output as attack intermediate data and performing power consumption analysis attack impractical, considering the attack complexity and data processing difficulty. Consequently, the chosen plaintext attack method introduced in [24, 25] is employed in this work for power consumption analysis on SM4 encryption key. The analysis procedures are demonstrated as follows.

First of all, $(X_0, X_1, X_2, X_3) = (00000000h, 00000000h, 00000000h, XX000000h)$ is the particularly chosen plaintext, in which X represents variable data. Performing encryption operation and collecting power consumption signal data, the intermediate calculation expression is

$$X_4 = F(X_0, X_1, X_2, X_3, rk_0) = T(XX000000h \oplus rk_0). \quad (8)$$

In function (8), since T transformation is the series of τ transformation and L transformation, τ transformation needs to be calculated beforehand, which is depicted in

$$\begin{aligned} B_0 &= \tau(A_0) = \tau(XX000000h \oplus rk_0) = \tau(a_{0,0} \| a_{0,1} \| a_{0,2} \| a_{0,3}) \\ &= (b_{0,0}, b_{0,1}, b_{0,2}, b_{0,3}), \end{aligned} \quad (9)$$

$b_{0,1}$, $b_{0,2}$, and $b_{0,3}$ are fixed constants, but $b_{0,0}$ is a variable. Then, calculate L transformation, which is demonstrated in Figure 2 with X representing variable data and other characters standing for fixed data.

In Figure 3,

$$\begin{aligned} c_{0,0} &= b_{0,0} \oplus (b_{0,0} \ll 2) \oplus (b_{0,1} \gg 6) \oplus (b_{0,1} \ll 2) \oplus (b_{0,2} \gg 6) \\ &\quad \oplus (b_{0,2} \ll 2) \oplus (b_{0,3} \gg 6) \oplus b_{0,3}, \end{aligned} \quad (10)$$

FIGURE 2: Process diagram of L linear transformation for the SM4 algorithm.

FIGURE 3: Architecture diagram of the power analysis system.

in which $(b_{0,1} \gg 6) \oplus (b_{0,1} \ll 2) \oplus (b_{0,2} \gg 6) \oplus (b_{0,2} \ll 2) \oplus (b_{0,3} \gg 6) \oplus b_{0,3}$ are fixed values and marked as $\text{Mask}_{0,0}$; similarly, $\text{Mask}_{0,i}$ stands for the fixed value operation result of $c_{0,i}$ in L transformation. $c_{0,i}$ can be written as $b_{0,0} \oplus (b_{0,0} \ll 2) \oplus \text{Mask}_{0,0}$, and the intermediate data calculation expression of the attack changes into equation (11). During the attack, higher byte ($rk_{0,0}$) of round key in the first round can be acquired with the power consumption model, which is built based on Hamming weight and Hamming distance of $X_{4,0}$ and the principle of power consumption analysis attack.

$$X_{4,0} = c_{0,0} = b_{0,0} \oplus (b_{0,0} \ll 2) \oplus \text{Mask}_{0,0}. \quad (11)$$

5. Measurement Setup and Experimental Results

5.1. Measurement Setup. Power analysis system based on FPGA was designed and implemented to verify the proposed EMD data-preprocessing method in our lab. The overall architecture mainly includes a PC for analyzing power consumption data, an oscilloscope, signal acquisition module, power supply, and other miscellaneous equipment, such as a serial cable used for interconnection, MMCX power consumption signal transport cable, electromagnetic probe, internet cable, power cable, and so on. Detailed structure is shown in Figure 3.

The platform of the power analysis system is organized by Labview on host PC. Oscilloscope and signal acquisition module are controlled through internet and serial cables to collect power consumption traces generated by the encryption chip. Then, the recorded data are transferred back

TABLE 1: Implementation environment.

Experimental equipment and instruments	Model
PC	Lenovo Thinkpad X240s
Oscilloscope	Tektronix MSO5204B, 2GHz
Power supply	DH1719A-3
FPGA	ALTERA Cyclone IV EP4CE115F2317N

to host PC and analyzed by the signal processing module using the side-channel attack method to recover the key. An overview of all the equipment used and their models are listed in Table 1.

5.2. Experiments and Results. In this section, we show the results of the proposed EMD data-preprocessing method compared with the state-of-the-art attack method as in [24, 25] through SM4 power consumption attack experiments.

Firstly, SM4 block cipher encryption algorithm was implemented in FPGA, obtaining m power consumption traces with the power consumption analysis method as explained in Section 4.1. All traces are presented in Figure 4.

In Figure 4, depending on the algorithm design, one complete encryption is composed of 33 setup rounds (1 data input round and 32 encryption key generation rounds) and 33 encryption rounds (1 data input round and 32 encryption iteration rounds). It is obvious that the key generation domain is from around 1500 to 4800 unit-time-points, while encryption iteration domain falls at around 5500 to 8800 unit-time-points.

Each power consumption trace undergoes the process of the proposed EMD data-preprocessing method. One of the processed trace's intrinsic mode components are illustrated in Figure 5.

There are 14 power consumption traces in Figure 5, among which the first trace is the original encrypted single power consumption trace $x(t)$, traces 2–13 are 1st–12th order intrinsic mode components $[c_1(t), c_2(t), \dots, c_{12}(t)]$ of $x(t)$, respectively, and the last one is the residue $r_{12}(t)$. It can be concluded that the frequency of the intrinsic mode component trace decreases if the order of it increases, which matches with the theory in Section 4.1. Besides, it is shown in the figure that, among the traces of the 1st order intrinsic mode component IMF1, the high-frequency noise discontinuously occurs with time. Thus, the encrypted signals are proven to be nonlinear unstable signals.

Based on experiences, lower order of intrinsic mode components correspond to high-frequency noises. Thus, after a large amount of simulation verifications, the 1st and 2nd order intrinsic mode components are removed for noise reduction, and the 3rd to 12th order intrinsic mode components are recovered by function (7). Comparison of the single power consumption trace in the first 5 rounds (1 data input round and 4 encryption iteration rounds) before and after EMD decomposition are shown in Figures 6 and 7.

High-frequency noises exist at the peaks of the trace after each round of encryption (Figure 6); however, after

FIGURE 4: Power consumption traces encrypted once with SM4.

(a)

(b)

FIGURE 5: Intrinsic mode components of one power consumption trace processed with the EMD data-preprocessing method.

FIGURE 6: Single power consumption trace before EMD decomposition.

FIGURE 7: Single power consumption trace after EMD decomposition.

FIGURE 8: Efficiency of original correlation power analysis.

removing 1st and 2nd order intrinsic mode components with the EMD process, the high-frequency noises at the peaks of trace are absent (Figure 7).

Next, higher bytes ($rk_{0,0}$) of round keys in the first round of SM4 algorithm are recovered from both with and without EMD processed power consumption traces using the chosen plaintext power consumption attack method mentioned in

Section 4.2. Analysis of both efficiencies is explicated in Figures 8 and 9.

From above, to separate correct key from incorrect ones, 252 power consumption traces are needed for the data without EMD data preprocessing, while only 195 power consumption traces are required for the data preprocessed by the EMD method. Therefore, the proposed

FIGURE 9: Efficiency of correlation power analysis after the EMD process.

TABLE 2: Comparison of analysis efficiencies.

	rk_0	rk_1	rk_2	rk_3	Total
Before data preprocessing	894	911	921	922	3654
After data preprocessing	711	753	745	798	3007

TABLE 3: Comparison between EMD and other methods of analysis efficiencies.

	rk_0	rk_1	rk_2	rk_3	Total
Before data preprocessing	894	911	921	922	3654
After FIR filter	798	811	865	846	3320
After analog filter	786	792	871	893	3342
After EMD	711	753	745	798	3007

EMD data-preprocessing method increases the analysis efficiency, reducing the required power consumption traces by 22.6%.

Applying the abovementioned method to recover all bytes of keys for the first four rounds are recovered as rk_0, rk_1, rk_2 , and rk_3 ; the required amount of power consumption traces is all listed in Table 2. For the power consumption analysis of the data without EMD data preprocessing, in total, 3,654 traces are needed to recover round keys of the first four rounds (i.e., master key). Comparing to the analysis with proposed EMD data preprocessing, only 3,007 power consumption traces are expected, which have reduced the amount by 17.7%, indicating higher efficiency of the proposed method.

5.3. Comparison. To fully demonstrate the high efficiency of the proposed data-preprocessing method based on the EMD algorithm, two traditional solutions of noise reduction filtering have been selected for comparison. Results of the experiments have been analyzed, and the conclusions are illustrated below:

5.3.1. Data-Preprocessing Method Based on the FIR Filter. FIR filter (finite impulse response filter), also known as the nonrecursive filter, is the most fundamental element of the digital signal processing system. Not only does it keep

amplitude-frequency characteristics but also has strict linear phase-frequency characteristics with a finite length of unit sampling response, which makes it a stable system. In this section, a FIR filter is designed in Matlab to reduce the high-frequency noise in the encrypted signals.

5.3.2. Data-Preprocessing Method Based on the Mini-Circuit Analog Filter. Analog filtering is achieved by running the signals through filters made of analog circuits before sampling, to improve the signal quality and reduce the workload and difficulty of data preprocessing. A 50 MHz low pass filter is used in the experiments (BLP-50+, Mini-Circuits, ISO9001).

Results of the experiments are shown in Table 3.

In Table 3, as for the power consumption analysis with FIR filter data preprocessing, 3,320 power consumption traces are needed to recover the round keys of the first four rounds (i.e., master key), 9.1% less compared to analysis without the data-preprocessing algorithm. And for the power consumption analysis with the analog filter, 3,342 power consumption traces are required to perform the same task, and it is only 8.5% less. However, the proposed EMD data-preprocessing algorithm uses much less power consumption traces (3,007) than these two methods. Thus, according to the comparison, the EMD data-preprocessing algorithm is proven to have a much higher efficiency for

power consumption analysis. In addition, both data-preprocessing methods of the FIR filter and Mini-Circuit analog filter require the clock frequency of the encrypted chip (50 MHz FPGA in this work) in advance to perform the targeted data preprocessing. However, the proposed method does not require that; this is why EMD is advantageous over other techniques.

6. Conclusion

In this paper, we have explored a general technique to reduce high-frequency noise of power consumption traces produced from our laboratory platform in CPA attack. This technique is a data-preprocessing method based on the EMD algorithm, which is one of the most profound time-frequency analysis methods for nonlinear unstable signals. It adaptively decomposes the collected encryption traces, based on their own characteristics, into the sum of several intrinsic mode functions without having any prior knowledge of the encryption chip. Then, it reorganizes the trace with meaningful intrinsic mode components selected by simulation verifications to reduce signal noises. The proposed technique is verified by experimentations of the SM4 block cipher algorithm, proving to have a 17.7% reduction on the number of power consumption traces for recovery of the master key, compared to the original CPA method.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work was supported by the National Key R&D Program of China (grant no. 2017YFB0802000), the National Natural Science Foundation of China (grant nos. U1636114, 61772550, and 61572521), and the National Cryptography Development Fund of China (grant no. MMJJ20170112).

References

- [1] P. C. Kocher, "Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems," in *Proceedings of the Annual International Cryptology Conference*, pp. 104–113, Springer, Santa Barbara, CA, USA, August 1996.
- [2] P. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," in *Proceedings of the Annual International Cryptology Conference*, pp. 388–397, Springer, Santa Barbara, CA, USA, August 1999.
- [3] J. J. Quisquater and D. Samyde, "Electromagnetic analysis (EMA): measures and counter-measures for smart cards," in *Smart Card Programming and Security*, pp. 200–210, Springer, Berlin, Heidelberg, 2001.
- [4] G. Piret and J. J. Quisquater, "A differential fault attack technique against SPN structures, with application to the AES and Khazad," in *Proceedings of the International Workshop on Cryptographic Hardware and Embedded Systems*, pp. 77–88, Springer, Cologne, Germany, September 2003.
- [5] C. H. Kim and J. J. Quisquater, "Faults, injection methods, and fault attacks," *IEEE Design & Test of Computers*, vol. 24, no. 6, pp. 544–545, 2007.
- [6] S. Chari, J. R. Rao, and P. Rohatgi, "Template attacks," in *Proceedings of the International Workshop on Cryptographic Hardware and Embedded Systems*, pp. 13–28, Springer, Redwood Shores, CA, USA, August 2002.
- [7] F. X. Standaert and C. Archambeau, "Using subspace-based template attacks to compare and combine power and electromagnetic information leakages," in *Proceedings of the International Workshop on Cryptographic Hardware and Embedded Systems*, pp. 411–425, Springer, Washington, DC, USA, August 2008.
- [8] W. Schindler, "A combined timing and power attack," in *Proceedings of the International Workshop on Public Key Cryptography*, pp. 263–279, Springer, Paris, France, February 2002.
- [9] S. W. Zhang, X. Y. Yang, W. D. Zhong et al., "An improved combinational side-channel attack on S-box in block cipher," *Journal of Internet Technology*, vol. 17, no. 1, pp. 157–166, 2016.
- [10] G. Hospodar, B. Gierlichs, E. De Mulder, I. Verbauwhede, and J. Vandewalle, "Machine learning in side-channel analysis: a first study," *Journal of Cryptographic Engineering*, vol. 1, no. 4, pp. 293–302, 2011.
- [11] E. Cagli, C. Dumas, and E. Prouff, "Convolutional neural networks with data augmentation against jitter-based countermeasures," in *Proceedings of the International Conference on Cryptographic Hardware and Embedded Systems*, pp. 45–68, Springer, Taipei, Taiwan, September 2017.
- [12] S. Hou, Y. Zhou, H. Liu, and N. Zhu, "Wavelet support vector machine algorithm in power analysis attacks," *Radio-engineering*, vol. 26, no. 3, pp. 890–902, 2017.
- [13] L. Lerman, Z. Martinasek, and O. Markowitch, "Robust profiled attacks: should the adversary trust the dataset?," *IET Information Security*, vol. 11, no. 4, pp. 188–194, 2016.
- [14] W. Shan, S. Zhang, and Y. He, "Machine learning based side-channel-attack countermeasure with hamming-distance redistribution and its application on advanced encryption standard," *Electronics Letters*, vol. 53, no. 14, pp. 926–928, 2017.
- [15] S. Mangard, E. Oswald, and T. Popp, *Power Analysis Attacks: Revealing the Secrets of Smart Cards*, Springer Science & Business Media, Berlin, Germany, 2008.
- [16] C. Clavier, J. S. Coron, and N. Dabbous, "Differential power analysis in the presence of hardware countermeasures," in *Proceedings of the International Workshop on Cryptographic Hardware and Embedded Systems*, pp. 252–263, Springer, Worcester, MA, USA, August 2008.
- [17] X. Charvet and H. Pelletier, "Improving the DPA attack using wavelet transform," in *Proceedings of the NIST Physical Security Testing Workshop*, vol. 46, Honolulu, HI, USA, 2005.
- [18] N. Homma, S. Nagashima, Y. Imai et al., "High-resolution side-channel attack using phase-based waveform matching," in *Proceedings of the International Workshop on Cryptographic Hardware and Embedded Systems*, pp. 187–200, Springer, Yokohama, Japan, October 2006.
- [19] T. Plos, M. Hutter, and M. Feldhofer, "Evaluation of side-channel preprocessing techniques on cryptographic-enabled HF and UHF RFID-tag prototypes," in *Proceedings of the Workshop on RFID Security*, pp. 114–127, Budapest, Hungary, 2008.

- [20] J. G. J. van Woudenberg, M. F. Witteman, and B. Bakker, "Improving differential power analysis by elastic alignment," in *Proceedings of the Cryptographers' Track at the RSA Conference*, pp. 104–119, Springer, San Francisco, CA, USA, February 2011.
- [21] T.-H. Le, J. Clediere, C. Serviere, and J.-L. Lacoume, "Noise reduction in side channel attack using fourth-order cumulant," *IEEE Transactions on Information Forensics and Security*, vol. 2, no. 4, pp. 710–720, 2007.
- [22] E. Brier, C. Clavier, and F. Olivier, "Correlation power analysis with a leakage model," in *Proceedings of the International Workshop on Cryptographic Hardware and Embedded Systems*, pp. 16–29, Springer, Cambridge, MA, USA, August 2004.
- [23] N. E. Huang, Z. Shen, S. R. Long et al., "The empirical mode decomposition and the Hilbert spectrum for nonlinear and non-stationary time series analysis," *Proceedings of the Royal Society of London. Series A: Mathematical, Physical and Engineering Sciences*, The Royal Society, vol. 454, no. 1971, pp. 903–995, 1998.
- [24] S. Wang, D. Gu, J. Liu et al., "A power analysis on SMS4 using the chosen plaintext method," in *Proceedings of the 2013 9th International Conference on Computational Intelligence and Security (CIS)*, pp. 748–752, IEEE, Leshan, China, December 2013.
- [25] Z. Du, Z. Wu, M. Wang, and Js. Rao, "Improved chosen-plaintext power analysis attack against SM4 at the round-output," *Journal on Communications*, vol. 36, no. 10, pp. 85–91, 2015.