An Improved Empirical Mode Decomposition for Power Analysis Attack

Han Gan[1], Hongxin Zhang[1,2,*], Muhammad Saad khan[1], Xueli Wang[3], Fan Zhang[4], Pengfei He[5]

[1] School of Electronic Engineering, Beijing University of Posts and Telecommunications, Beijing, 100876, China
[2] Beijing Key Laboratory of Work Safety Intelligent Monitoring, Beijing University of Posts and Telecommunications, Beijing, 100876, China
[3] School of Science, Beijing University of Posts and Telecommunications, Beijing, 100876, China
[4] College of Information Science and Electrical Engineering, Zhejiang University, Hangzhou, 310027, China
[5] Institute of Science and Technology for Opto-electronic Information, Yantai University, Yantai, 264005,China
[*] The corresponding author, email: hongxinzhang@bupt.edu.cn

Abstract: Correlation power analysis (CPA) has become a successful attack method about crypto- graphic hardware to recover the secret keys. However, the noise influence caused by the random process interrupts (RPIs) becomes an important factor of the power analysis attack efficiency, which will cost more traces or attack time. To address the issue, an improved method about empirical mode decomposition (EMD) was proposed. Instead of restructuring the decomposed signals of intrinsic mode functions (IMFs), we extract a certain intrinsic mode function (IMF) as new feature signal for CPA attack. Meantime, a new attack assessment is proposed to compare the attack effectiveness of different methods. The experiment shows that our method has more excellent performance on CPA than others. The first and the second IMF can be chosen as two optimal feature signals in CPA. In the new method, the signals of the first IMF increase peak visibility by 64% than those of the tradition EMD method in the situation of non-noise. On the condition of different noise interference, the orders of attack efficiencies are also same. With external noise interference, the attack effect of the first IMF based on noise with 15dB is the best.

Keywords: power analysis attack, EMD, IMF, correlation power analysis, RPIs

I. INTRODUCTION

In information security domain, side channel analysis (SCA) attack has become an important direction, which is a big threat for the infor- mation safety of embedded encryption devices. SCA attack can be implemented by physic leakages of cryptographic device that include time consumption, power consumption and electromagnetic leakage. The methods of SCA mainly include differential power analysis (DPA)[1], simple power analysis[2], correlation power analysis (CPA), and mutual information analysis attack[3], etc. Due to the noise caused by random process interrupts (RPIs), a class method is alignment of leakage information, which includes phase-only–correlation[4], am- plitude-only correlation[5], etc. Another is the research for weakening the noise influence by signal processing. It mainly contains filter, four–order cumulant (FOC)[6], wavelet transform(WT)[7], etc. The apply condition of filter is strict, which needs to learn more about the information about traces such as the sample rate. The method of FOC removes Gaussian

Received: Sep. 28, 2016
Revised: Apr. 6, 2017
Editor: Guanglin Zhang

In this paper, an improved empirical mode decomposition method is proposed for Correlation Power Analysis attack.

noise from the whole signals. The WT method restructures the signals in the low and high frequency to realize the noise reduction. Empirical mode decomposition (EMD)[8] is used to decompose and restructure the signals for noise elimination, which is similar with WT about the way of noise reduction. These methods improve the performance on reducing the noise. However, the peaks of the correct curve really need to increase to improve the attack efficiency. The paper proposes a novel method, extracting a class of certain feature signals as the useful information in CPA, sub- tracting others which are considered as noises.

The paper is structured as follows. In Section II, we describe the notations of CPA and previous attacks. In Section III, we introduce the conventional and our improved EMD in detail. Meantime, a new attack assessment is proposed for comparing attack effectiveness. In Section IV, our solution is proved experimentally validated. The attack efficiencies of the experiment are analyzed in the situation with noise and non-noise. Section V is the conclusion part.

II. Related Works

2.1 Notations

In the paper, the expression of the random variables as follows. The mean of x is denoted by $\mathrm{E}(x)$, its variance by $\mathrm{V}(x)$. The latter equals to $\mathrm{V}(x) = \mathrm{E}(x - E(x))^2$. The covariance of variables X and Y are denoted by Cov. It can be expressed as follows:

$$\mathrm{Cov} = \mathrm{E}((X - E(X))(Y - \mathrm{E}(Y))) \quad (1)$$

The correlation of $X$and Y is shown as follows. If ρ is larger, the greater the correlation will be.

$$\rho = \frac{\mathrm{E}(X \times Y) - E(X) \cdot E(Y)}{\sqrt{\mathrm{V}(X) \cdot V(Y)}} (0 \leqslant \rho \leqslant 1) \quad (2)$$

In the encryption algorithm (EA), different plaintexts P_i are encrypted with the same key. The key is composed of sixteen segments. We take one key segment K as an example. After the calculation of SubBytes S, we get the result D_i ($\mathrm{D}_i = \mathrm{S}(\mathrm{K} \oplus \mathrm{P}_i)$). Power traces T_{ij} are obtained when EA is encrypted. And i and j are random variables; n and m represent the number of sample points and the number of traces separately; x_{11} and x_{21} represent the values of first sample points of the first and second trace separately.

$$\mathrm{T}_{ij} = \begin{bmatrix} \mathrm{x}_{11} & \mathrm{x}_{12} & \cdots & \mathrm{x}_{1n} \\ \mathrm{x}_{21} & \mathrm{x}_{22} & \cdots & \mathrm{x}_{2n} \\ \vdots & \vdots & \cdots & \vdots \\ \mathrm{x}_{m1} & \mathrm{x}_{m2} & \cdots & \mathrm{x}_{mn} \end{bmatrix} \quad (3)$$

In conventional CPA (CPA-Covt), we adopt the strategy of 'divide and conquer' to combine the guess key segment to recovery the whole key.

For one key segment, we traverse all possible key segments to get intermediate values, the hamming weight of the SubBytes results. Then we get a correlation matrix of hamming weight HW and power traces. After that, we find the maximum peak of correlation matrix to get the corresponding key segment which will be considered as the right one. The correlation formulation is expressed as follows:

$$C = \frac{\sum_{i=1}^{m} T_i * HW - \sum_{i=1}^{m} T_i * \sum_{i=1}^{m} HW}{\sqrt{V(T_i)} * \sqrt{V(HW)}} \quad (4)$$

where C is correlation coefficient.

2.2 Previous attacks

Youssef Souissi proposed adapt KALMAN FILTER[9,10] for the CPA optimization, which is a recursive filter for time-varying linear systems. And the mentioned method makes the past error estimation into new to estimate the future error and to realize the noise filtering. It proved the mentioned method reduced the number of traces in the situation of same attack result.

CHARVET Xavier et al proposed a kind of improving power analysis attack by wavelet transform. By the reconstruction of the information with low and high frequency, the method smoothed the signals in the situation of asynchrony and improved the attack effect.

Thanh-Ha Le et al proposed to use FOC to improve the attack performance. The mentioned method is assumed that the noise is Gauss noise which will be removed to produce

new signals. It proved the time shift of asynchrony signals was eliminated by the superposition of new signal with FOC.

These methods are proposed for power traces processing. They have different ways of dealing with noise, and their attack effects are different.

III. Proposed Method

EMD is used for time-frequency analysis of signal process[11], which extracts the local signals of different frequency bands from the original data, to reconstruct the data for noise elimination. Its decomposition steps are shown as follows.

1 Find all the extreme points of original signals $\mathrm{y}(t)$.

2 Calculate the mean $m_1(t)$ of the upper and lower envelopes and remove it from the original signals to get a variable $h_1(t)$. The expression is as follows:

$$\mathrm{y}(t) - m_1(t) = h_1(t) \tag{5}$$

3 Repeat the second step for k times until the first intrinsic mode function (IMF) $h_{1k}(t)$ satisfies the condition. The expression is as follows:

$$\mathrm{h}_{1(k-1)}(t) - m_{1k}(t) = h_{1k}(t) \tag{6}$$

4 Remove the first IMF from the original signal to get the new signal, and repeat the second and the third step to generate a plurality of intrinsic mode functions (IMFs).

In conventional EMD (EMD-Covt) method, $\widetilde{x}(t)$ is reconstructed signals containing IMF $I_p(t)$ $(p = 1, 2, \ldots \mathrm{L})$ and a remainder $d(t)$. The express is shown as follows:

$$\widetilde{x}(t) = \sum_{p=\mathrm{M}}^{\mathrm{L}} I_p(t) + d(t) \tag{7}$$

where L and L are the minimum and maximum number of IMFs. In the phase of signal reconstruction, not all the IMFs are selected. If IMF is selected that depends on its actual and theoretical energies. If the comparison has significant distinction, the IMF will be chosen.

In our proposed EMD method, we consider that signals with different frequency range have different effects on CPA attack. So we intend to apply the first, second, and third IMF as three kinds of new signals which will be used in CPA.

3.1 Attack assessment

Commonly the way to recover the secret key is to find the maximum peak from the correlation curves. However, if the maximum peak is not obvious, it will increase the difficulty of the attack. To effectively evaluate the attack effectiveness of our proposed method, this paper presents a new assessment for CPA attack.

We find the correct correlation curve and select a segment of the curve which has no obvious larger peak. The number of peaks for this segment is denoted by q(q=1,2,...N). Get the mean of these peak values to be benchmark amplitude w. Then calculate the ratio R of the maximum peak value H and w, named peak visibility (PV).

$$w = \frac{\sum_{q=1}^{N} C(q)}{N} \tag{8}$$

$$\mathrm{R} = \frac{\mathrm{H}}{w} \tag{9}$$

IV. Experiment and Analysis

4.1 Analysis in non-noise environment

We select a set of traces about Advanced Encryption Standard with RPIs and assume that the traces are collected in the external environment of non-noise. To evaluate the effectiveness of our proposed method, CPA- Covt attack, EMD-Conv and our proposed EMD methods are compared.

We compress the traces firstly by summing the values of traces [12]. After the signal processing of EMD-Covt and our proposed method, we get the new signals for CPA attack. With the number of traces increase, these attack results present rising trend. In figure 1, it can be seen that the first and second IMFs show excellent performances on attack effects, which are better than EMD-Covt, which will be considered as new effective signals to attack. The

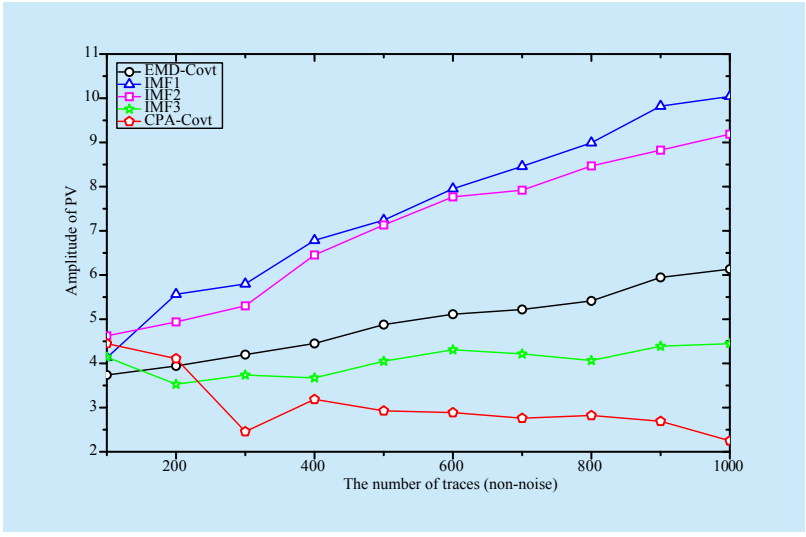

Fig. 1 *The results of different methods (non-noise)*

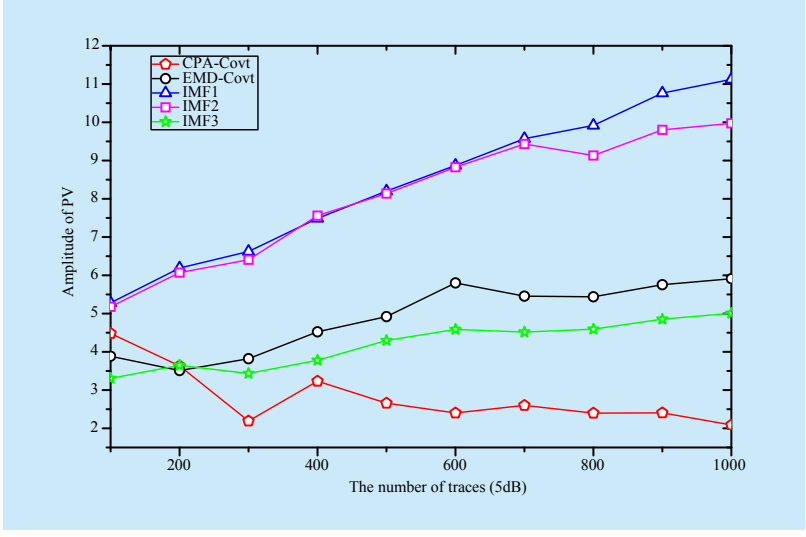

Fig. 2 *The results of different methods (SNR-5dB)*

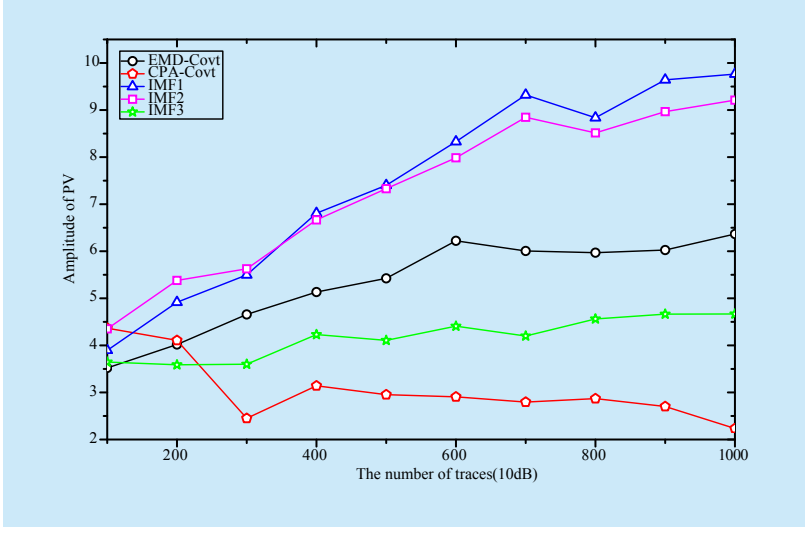

Fig. 3 *The results of different methods (SNR-10dB)*

third IMF is second-to-last, but better than CPA-Covt.

As the traces to attack is 1000, the maximum value of PV of the first IMF is 10.04, increasing by 64% than EMD-Covt. And it also increases by 3.46 times than CPA-Covt (shown in figure 1).

4.2 Analysis in noise environment

In order to research the influence of the external environment on the power traces, we analyze the attack effect of the proposed method on the conditions of signal-to-noise ratio (SNR) of 5dB, 10dB, 15dB and 20 dB.

On condition of the SNR of 5dB, except the PV of CPA-Covt, the others' show tendency to ascend. The first and second IMFs still show better performance than EMD-Covt and CPA-Covt. As the number of traces is 1000, the value of PV for the first IMF is 11.12, increasing by 88.2% than EMD-Covt, and also increasing by 4.32 times than CPA-Covt (shown in figure 2).

With the SNR is increased to 10dB (shown in figure 3), the attack results show similar tendency with the non-noise environment. The order of the results is also same. As the number of traces is 1000, the value of PV for the first IMF is 9.76, increasing by 53% than EMD-Covt, and also increase by 3.33 times than CPA-Covt.

The attack results of these methods with SNR of 15dB tend to increase slowly (shown in figure 4). As the number of trace is 1000, for EMD-Covt, its value of PV is closed to 6.73. For the first IMF, its value of PV increases by 65.4% than EMD-Covt, and also increases by 4.48 times than CPA-Covt.

V. Conclusion

In this paper, an improved EMD method is proposed for CPA attack, whose result shows better than EMD-Covt and CPA-Covt. To test the effect of new method, the paper proposes a new attack assessment. The new method is tested in the environment of noise and non-noise. In the absence of noise interference, the

attack effect of the first IMF is optimal, and the second IMF is the second choice. In the case of noise interference, the orders of attack effects are still the same. But the noise has impact on the value of PV. The attack effect of the first IMF shows excellent performance on the condition of noise with 15dB.

Acknowledgments

This work has been supported by The National Natural Science Foundation of China under Grants 61571063, 61501100 and 61472357.

References

[1] B. Mazumdar and D. Mukhopadhyay, "Construction of Rotation Symmetric S-Boxes with High Nonlinearity and Improved DPA Resistivity". *IEEE Transactions on Computers*, vol. 66, no. 1, pp. 59-72, 2017.

[2] AA. Zadeh, HM. Heys. "Simple power analysis applied to nonlinear feedback shift registers". *IET Information Security*, vol. 9, no. 1, pp. 90-90, 2015.

[3] D. Bellizia, S. Bongiovanni, P. Monsurro, G. Scotti, A. Trifiletti, "Univariate Power Analysis Attacks Exploiting Static Dissipation of Nanometer CMOS VLSI Circuits for Cryptographic Applications". *IEEE Transactions on Emerging Topics in Computing*, vol.PP, no.99, pp.1-1, 2016.

[4] Catherine H. Gebotys and Brian A. White. "A Sliding Window Phase-Only Correlation Method for Side- Channel Alignment in a Smartphone". *ACM Trans. Embed. Comput*. vol.14, no 4, pp.80, 2015.

[5] N. Debande, Y. Souissi, M. Nassar. "Re-synchronization by Moments: an efficient solution to align Side-Channel traces". *IEEE International Workshop on Information Forensics & Security*. pp.1 - 6 2011.

[6] T. Ha Le, J. Clédière, C. Servière, and J.L. Lacoume. "Noise Reduction in Side Channel Attack Using Fourth-Order Cumlant". *IEEE Transaction on In- Formation Forensics and Secu-Rity*, vol. 2, no. 4, pp. 710- 720, 2007.

[7] H Patel and R Baldwin. "Differential Power Analysis Using Wavelet Decomposition". *Military Communica- tions Conference*, pp. 1-5, 2012.

[8] M.L. Feng, Y.B. Zhou, Z.M Yu. "EMD- Based Denoising for Side-channel Attacks and Relationships between the Noises Extracted with Different Denoising Methods". *ICICS 2013, LNCS* 8233, pp. 259- 274, 2013.

[9] Y Souissi, S Guilley, JL Danger, S Mekki, G Duc. "Improvement of Power Analysis Attacks Using Kalman Filter". *ICASSP*, pp.1778-1781, 2010.

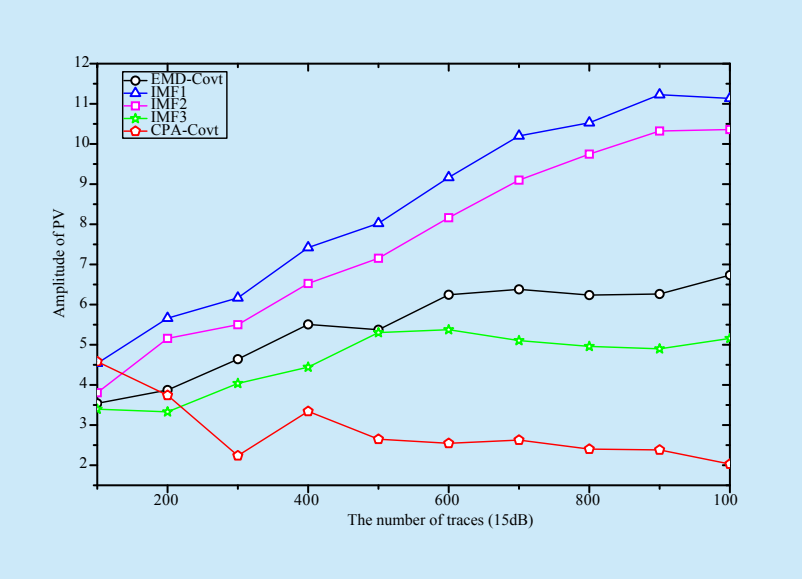

Fig. 4 *The results of different methods (SNR-15dB)*

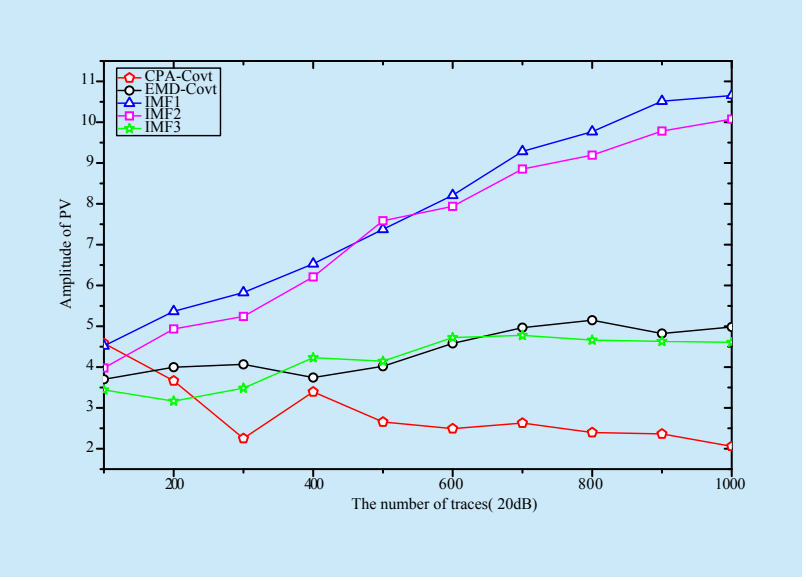

Fig. 5 *The results of different methods (SNR-20dB)*

[10] JY Wang, Y Wang, BY Jing, X Gao. "Maximum correntropy Kalman filter". *Automatica*. Vol. 76, pp.70- 77, 2017

[11] X. Wang, Z. Chen, J. Luo, J. Meng and Y. Xu, "ECG compression based on combining of EMD and wavelet transform". *Electronics Letters*, vol.52, no.19, pp. 1588 -1590, 2016.

[12] S Mangard, E Oswald, T Popp. Power Analysis Attacks [M]. Dengguo Feng, YB. Zhou, JY. Liu. Beijing: Science Press, 100-109, 2010.

Biographies

Han Gan, was born in 1986 in Hebei province of China. She is percuing her Ph.D Degree at the School of Electronic Engineering, Beijing University of Posts and Telecommu- nications. Her research interests are Information security, signal processing, electro- magnetic field, machine learning and pattern recognition. Email: ganhanamy @163. com

Hongxin Zhang, was born in 1969 in Shandong province of China. He is the professor of Electrical Engi- neering Institute of Beijing university of posts and tele- communications, and also the Doctoral tutor. He is the director of the Broadband communications and microwave technology center. He is the review expert of the national natural science fund project. He is also the evaluation expert of Education degree and graduate education development center. Email: hongxinzhang@ bupt.edu.cn.

Muhammad Saad Khan, was born in 1984 in Pakistan. He received his M.Sc Elec- trical Engineering Degree from Blekinge Institute of Technology, Karlskrona, Sweden. He was a Lecturer in Electrical Engineering Department BahauddinZakariya University Pakistan. He is percuing his Ph.D Degree at the School of Electronic Engineering, Beijing University of Posts and Telecommu- nications. His research interests are VLSI design, Microwave and antenna Propagation, RFIC design, Wireless and Optical communications, Low noise amplifiers and Power Amplifiers. Email: saadkhan9@gmail. com.

Xueli Wang, was born in 1973 in Shandong province of China. She achieved the Ph.D degree from School of mathe- matical Sciences, Peking University, now She is the associate professor of Beijing university of posts and telecommunications, and also the graduated tutor. Her major is statistical inference and machine learning. She is also a member of the Chinese Association for Probability and Statistics, a director member of the Computation Statistics. Email: wangxl @bupt. edu.cn.

Fan Zhang, was born in 1978, Zhejiang, China, acquired his Ph.D degree from department of computer science and engineering in University of Connecticut, America. Now he is a profess of college of information and Electrical engineering, Zhejiang University, and his interesting research filed includes information security, computer architecture, human-com- puter interaction, and sensor networks. Email: fanzhang@zju.edu.cn.

Pengfei He, was born in 1980 in Shandong province of China, received his Ph.D. degree in electromagnetic field and microwave tech- nology from Beijing Univer- sity of Posts and Telecommunications, Now he is an associate professor of the Institute of Science and Technology for Opto-electronic Information, Yantai University. His current research areas include Short-range Wireless Communication Technology, Wireless Body Area Network, Broadband Access Network and Electromagnetic Compatibility. Email: hpf_ 972 @163.com.