JST: Smart Systems and Devices
Volume 31, Issue 1, May 2021, 017-024

An Efficient Correlation Power Analysis Attack Using Variational Mode Decomposition

Tran Ngoc Quy**, Nguyen Hong Quang
Academy of Cryptography Techniques, Hanoi, Vietnam
**Email: quytn@actvn.edu.vn*

Abstract

Side channel attacks (SCAs) are now a real threat to cryptographic devices and correlation power analysis (CPA) is the most powerful attack. So far, a CPA attack usually exploits the leakage information from raw power consumption traces that collected from the attack device. In real attack scenarios, these traces collected from measurement equipment are usually contaminated by noise resulting in a decrease in attack efficiency. In this paper, we propose a variant CPA attack that exploits the leakage information from intrinsic mode functions (IMFs) of the power traces. These IMFs are the results of the variational mode decomposition (VMD) process on the raw power traces. This attack technique decreases the number of power traces for correctly recovering the secret key by approximately 13% in normal conditions and 60% in noisy conditions compared to a traditional CPA attack. Experiments were performed on power traces of AES-128 implemented in both microcontroller and FPGA by Sakura-G/W side channel evaluation board to verify the effectiveness of our method.

Keywords: Side channel attack, correlation power analysis, variational mode decomposition.

1. Introduction

Side channel attacks (SCAs) are a modern cryptanalysis technique for revealing the secret keys of cryptographic devices by exploiting the physical signals leaked from cryptographic devices during their execution [1]. Typical SCAs contain power analysis attacks, timing attacks, electromagnetic attacks, or combinations of them [2]. Power analysis attacks rely on comparing the distribution of the measured power consumptions (power trace) over a number of encryptions against a theoretical model in order to exploit data-dependent properties of the side-channel leakage. Since its first appearance in [1], many power analysis attack methods have been introduced such as Differential Power Analysis (DPA) [1], Correlation Power Analysis (CPA) [3], Mutual Information Analysis (MIA) [2]. CPA is considered the most common attack and one of the most commonly targeted algorithms in side-channel attacks is the Advanced Encryption Standard (AES), due to its widespread adoption in a number of industrial and ISO standards. We focus on the CPA attack on AES in this paper.

For conducting a CPA attack, an adversary first has to collect the power consumption of cryptographic devices. Then the relationship between hypothetical power consumption and actual power traces is estimated by Pearson's correlation coefficient in order to recovery the correct key. The number of power traces needed for correctly recovering the keys is an important indicator of attack efficiency. In order to improve the attack efficiency, the common approach is denoising of power traces.

There are many methods which are used to denoise power trace before power analysis attack. The most common ones are using linear filters [4 - 5] and wavelet transform [6 - 7] for power trace before power analysis attack. But these methods need signal representation with some prior information. The other one utilizes the property of signal or noise itself, such as averaging [1], high-order cumulant [8], and Kalman filter [9]. Averaging on a number of traces to acquire a clean signal requires that the attacker should have enough traces which cannot always satisfy the realistic requirement.

A recent advance in signal processing and denoising is the variational mode decomposition (VMD) technique. VMD decomposes the signal to intrinsic mode functions or VMD modes. They are amplitude-modulated and frequency modulated signals which represent accurately different components of the original signal in different central frequencies. Therefore, VMD modes contain side channel information of the power trace. Moreover, VMD has more optimality to deal with noisy signals because of the tight connection with the Wiener filter. By these observations, in this paper, we propose a CPA attack method that using IMFs, called the VMD-CPA method, to recovery the secret key of cryptographic devices.

The remainder of the paper is structured as follows: In section 2, we describe the background to

ISSN: 2734-9373
https://doi.org/10.51316/jst.150.ssad.2021.31.1.3
Received: 16 October 2020; accepted: 13 May 2021

this research: the CPA attack, variational mode decomposition. In section 3, we present our proposed VMD-CPA attack. The experiments and their results are presented in section 4. Finally, the main conclusions of our research are presented in the last section.

2. Background

2.1. Correlation Power Analysis Attack

CPA attack is proposed by Brier et al. [4], which uses the linear relationship between real power consumption and hypothesis power consumption of a cryptographic device to achieve the purpose of revealing the secret key. The process of CPA attack is mainly summarized as 4 steps [2]:

Step 1: Choose a model for the target's power consumption. Generally, the model is Hamming weight model or Hamming distance model. The model will focus on specific points in the encryption device. The target point is usually the output of S-box because it calculates the value that relates key value.

Step 2. Get some different plaintexts of the target. Record every power trace of the target's power consumption during each of the encryption devices. This step results in D power traces, each has T data points, to form a matrix $\mathbf{T}_{D\times T}$.

Step 3. For all possible options for the key, use the plaintexts of step 2 and the key to calculate the intermediate value of target and then the power consumption according to the model. This step results in a hypothesis power consumption in form of a matrix $\mathbf{H}_{D\times K}$, where K is the number of all possible hypothesis keys.

Step 4. Calculate the Pearson correlation coefficient (Equation 1) between the modeled power consumption of step 3 and the real power consumption of step 2. Then the key results in maximum Pearson coefficient are considered as the correct key of the target device. In equation (1), $h_{d,i}$ is an element of hypothesis power consumption matrix $\mathbf{H}_{D\times K}$, and $t_{d,j}$ is an element of real power consumption matrix $\mathbf{T}_{D\times T}$.

$$r_{i,j}=\frac{\sum_{d=1}^{D}[(h_{d,i}-\bar{h}_i)(t_{d,j}-\bar{t}_i)]}{\sqrt{\sum_{d=1}^{D}\left(h_{d,i}-\bar{h}_i\right)^2\sum_{d=1}^{D}\left(t_{d,j}-\bar{t}_j\right)^2}} \quad (1)$$

where $i=1,..,K; j=1,\ldots,T$

2.2. Variational Mode Decomposition

VMD decomposes a signal $x(t)$ into a small number of K narrowband intrinsic mode functions (IMFs) or the VMD modes for simply as given [10] by equation (2).

$$x(t)=\sum_{k=1}^{K}u_k(t) \quad (2)$$

VMD modes have characteristics: (1) each mode $u_k(t)$ is an amplitude and frequency modulated signal of the form: $u_k(t)=A_k(t)\cos(\phi_k(t))$, where $\phi_k(t)$ is the phase of the mode and $A_k(t)$ is its envelopes; (2) The modes have positive and slowly varying envelopes; (3) Each VMD mode has an instantaneous frequency $\phi_k'(t)$ that is nondecreasing, varies slowly, and is concentrated around a central value f_k.

The VMD method simultaneously calculates all the mode waveforms and their central frequencies. For a real value signal $x(t)$, the algorithm to search each mode can be described as follows: (1) For each mode function, compute the associated analytic signal using the Hilbert transform to obtain a unilateral frequency spectrum; (2) Shift the frequency spectrum of each mode function to baseband by mixing with an exponential tuned to the respective estimated center frequency; (3) Estimate the bandwidth through the H^1 Gaussian smoothness of the demodulated signal, i.e. the squared 2 -norm of the gradient. Then the process of finding a set of $u_k(t)$ and $f_k(t)$ that minimize the constrained variational problem is given by expression (3). The solution to (3) is equivalent to finding an optimum of the augmented Lagrangian $\mathcal{L}$ as given by (4). The second and third terms in (4) enforce the constraint $x(t)=\sum_{k=1}^{K}u_k(t)$ by imposing a quadratic penalty and incorporating a Lagrange multiplier. The penalty factor α measures the relative importance of the first term compared to the second and third terms in (4).

$$\min_{u_k,f_k}\left\{\sum_k\frac{d}{dt}\left[\left(\delta(t)+\frac{j}{\pi t}\right)*u_k(t)\right]e^{-j2\pi f_k t}{}_2^2\right\} \quad (3)$$

Subject to: $\sum_k u_k(t)=x(t)$

$$\mathcal{L}\{u_k(t),f_k,\lambda(t)\}=\alpha\sum_{k=1}^{K}\frac{d}{dt}\left[\left(\delta(t)+\frac{j}{\pi t}\right)*u_k(t)\right]e^{-j2\pi f_k t}{}_2^2+x(t)-\sum_{i=1}^{K}u_k(t)_2^2+\lambda(t),x(t)-\sum_{k=1}^{K}u_k(t) \quad (4)$$

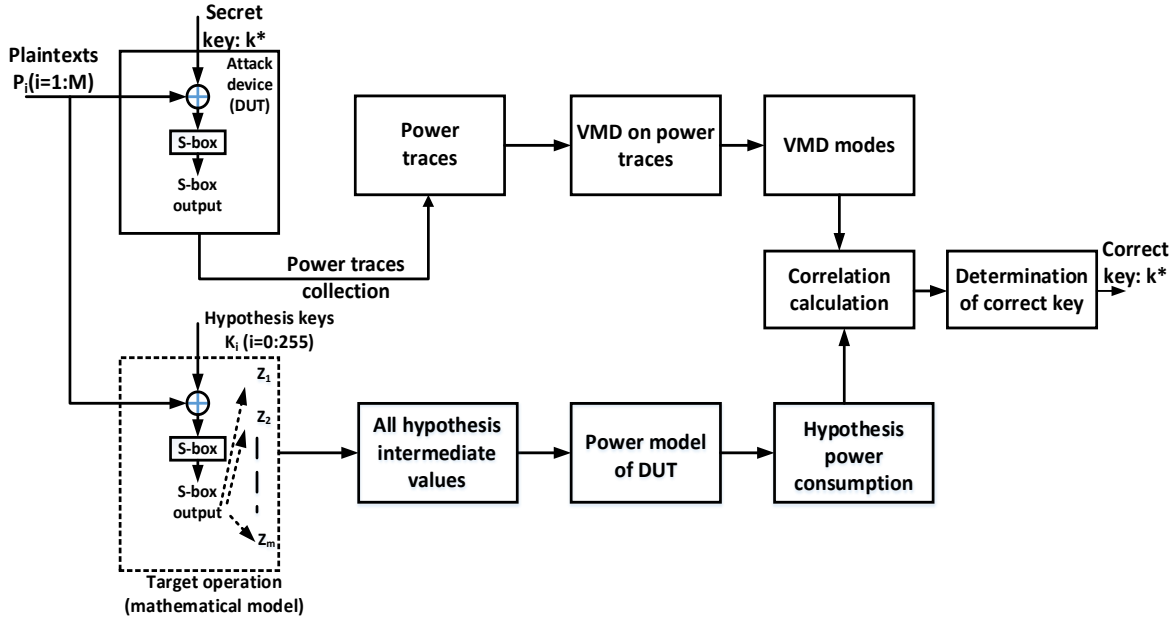


Fig. 1. VMD based Correlation Power Analysis Attack Framework

Then the alternate direction method of multipliers (ADMM) is used for solving the original minimization problem (11) by finding the saddle point of the augmented Lagrangian $\mathcal{L}$ in a sequence of iterative sub-optimizations. Each VMD modes are directly optimized in frequency domain by iteratively updating the modes until condition $\sum_k \frac{u_k^{n+1}(t)-u_k^n(t)_2^2}{u_k^n(t)_2^2} < \epsilon$ is met, where τ is the update rate of the Lagrange multiplier

3. The Proposed Attack Methodology

Fig.1 demonstrates the framework of our proposed VMD-CPA attack. The process of VMD-CPA attack is based on CPA attack with addition VMD decomposition step to preprocess power traces. For traditional CPA attacks, power traces are directly used in statistical analysis to conduct a guess of secret key. In our VMD-CPA attack, power traces are first transformed to VMD modes and then a statistical analysis utilizes these VMD modes to conduct a guess of secret key. We will present the reason that VMD modes can be used for CPA attacks as follows.

The electric circuits that perform the computation in the processor are designed from a technology known as CMOS (Complementary Metal Oxide Semiconductor). The power trace collected during the operation of a CMOS circuit represents its power consumption. It consists of many components in which dynamic power dissipation is the most important. This component depends on the processed data of the circuit and is useful information leakage for power analysis attack. The dynamic power dissipation is mainly caused by the switching activity of logic gates in a circuit which is controlled by the operating clock frequency so the dynamic power consumption is driven by the clock frequency of circuit [2]. Therefore, in spectrum of power trace, it is expected that the clock frequency component has significant magnitude compared to the other components. The information leakage is nearly in the form of an amplitude modulation signal and the central frequency of its spectrum is the clock frequency. Generally, in a device, the different parts of its circuit are controlled by different operating frequencies through the clock division system, so the dynamic power dissipation is the combination of some amplitude modulation signals with different center frequencies. So, it is reasonable to assume that the eviction of signal components which are unrelated to the useful computation will yield a signal denser in informative content related to the key manipulation, due to the elimination of polluting noise.

Because of the separation of VMD modes in frequency range, it is possible to select a VMD mode that relates to operation clock of target circuit part and remove the other VMD modes that represent power consumption generated by other parts of circuits. Moreover, VMD modes are robust to noise so we expect that correlation power attack on VMD modes works effectively with noisy power traces. In real attack scenario, the attacker has no knowledge of operation clock of target circuit, CPA attacks are conducted on all VMD modes for determining the VMD mode that contains most of leakage information from power traces.

In the VMD process, it is necessary to set parameters. The number of decomposed modes *K*: VMD needs to preset the number of decompose modes *K.* If *K* is too small, the decomposed modes are too few, and all the decomposition modes cannot be captured; while if the value of *K* is too large, the

interfering signal will be over decomposed such that the center frequencies of modes will be mixed. The penalty factor, α affects the bandwidth of the decomposed signal. To decompose input and target time series by the VMD, the number of decomposed modes (K) and the quadratic penalty factor (α) should be determined beforehand. In this study, the parameters, K and α, were determined according to the following steps:

Step 1. Decompose a power trace into modes for different $K = [1, 20]$ and $\alpha = [5, 2000]$.

Step 2. Add up the modes for each of the K and α values to obtain the reconstructed power trace and estimate the values of Pearson correlation coefficient for the reconstructed and original power trace.

Step 3. Select the sets of K and a values for maximum of Pearson correlation coefficient.

For other input parameters of VMD: update rate, τ and convergence condition ϵ are selected by standardization values in range $0 - 10^{-6}$ [10].

4. Experiments

In this section, we present experiments for conducting CPA and VMD-CPA attacks on the first key byte of AES-128. The offline key recovery is implemented in MATLAB 2017b. The parameters used to evaluate the effectiveness of the attack method are as follows: (1) The ability to reveal the correct key: To confirm that our VMD-CPA attacks can reveal the correct key used by AES-128, we figure out the probability of the correct key over all keys. The key with the highest probability is the best one; (2) The number of traces for attack successfully, N_a: Pearson coefficient for all hypothesis keys are figured out according to the number of attack traces. N_a is the number of traces that attack can be discriminated between the correct key and the other keys.

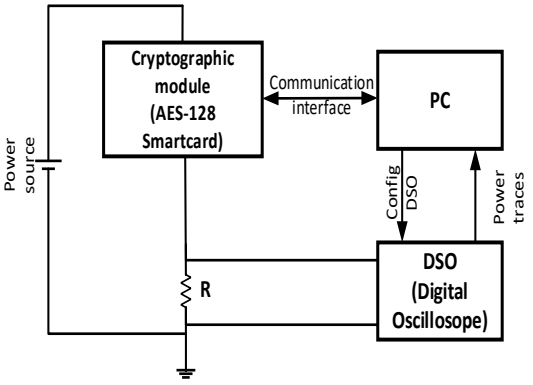
4.1. Power Traces Measurement Setup

To measure the power leakage of cryptographic devices, the side-channel attack standard evaluation board (SAKURA-G/W) is served as our main experiment platform (Fig.2). The AES-128 is implemented in the Atmega8515 microcontroller inside a smartcard. In addition, an oscilloscope (Tektronix DPO-3052) is used to collect the power traces whose bandwidth is 500 MHz and the maximum sampling frequency is 5 GSa/s. Here 1000 power traces are collected with 10000 time-samples. An example of power trace is depicted in Fig.3 with titled as '*Original trace'*.

4.2. Experiments Results and Analysis

4.2.1. Investigation of CPA attack on VMD modes.

In this section, we investigated the key recovery ability of CPA attack on VMD modes. First, VMD is used to decompose original traces to VMD modes. For VMD, two main parameters (K, α) are determined by the procedure as presented in section 3. This results in $K = 5$ and $\alpha = 1000$. The VDM modes of AES-128 traces are depicted in Fig.3. As expected, VMD modes contain the different components of the original signal at different central frequencies. In order to determine which VMD mode contained maximum leakage information of power trace, we conduct correlation power analysis (CPA) attacks on all the VMD modes. The results of VMD-CPA attacks on all VMD modes are presented in Fig.4.



(a)

(b)

Fig.2. (a) Measurement framework. (b) Experimental environment with SAKURA-G/W.

In an attack, for a key hypothesis k^*, if there is a visible peak of correlation coefficient, it can be concluded that k^* is the most likely key of AES using for encryption. As depicted in Fig.5, there are two VMD modes that CPA attack is successful for key recovery. It can be concluded that VMD modes can be used for power analysis attack. The CPA attack on VMD mode 1 has the maximum correlation coefficient, so VMD mode 1 contains most of leakage information of power trace. We will use VMD mode 1 for further investigation of the effectiveness of VMD-CPA attack when compare with CPA attack on the original power traces.

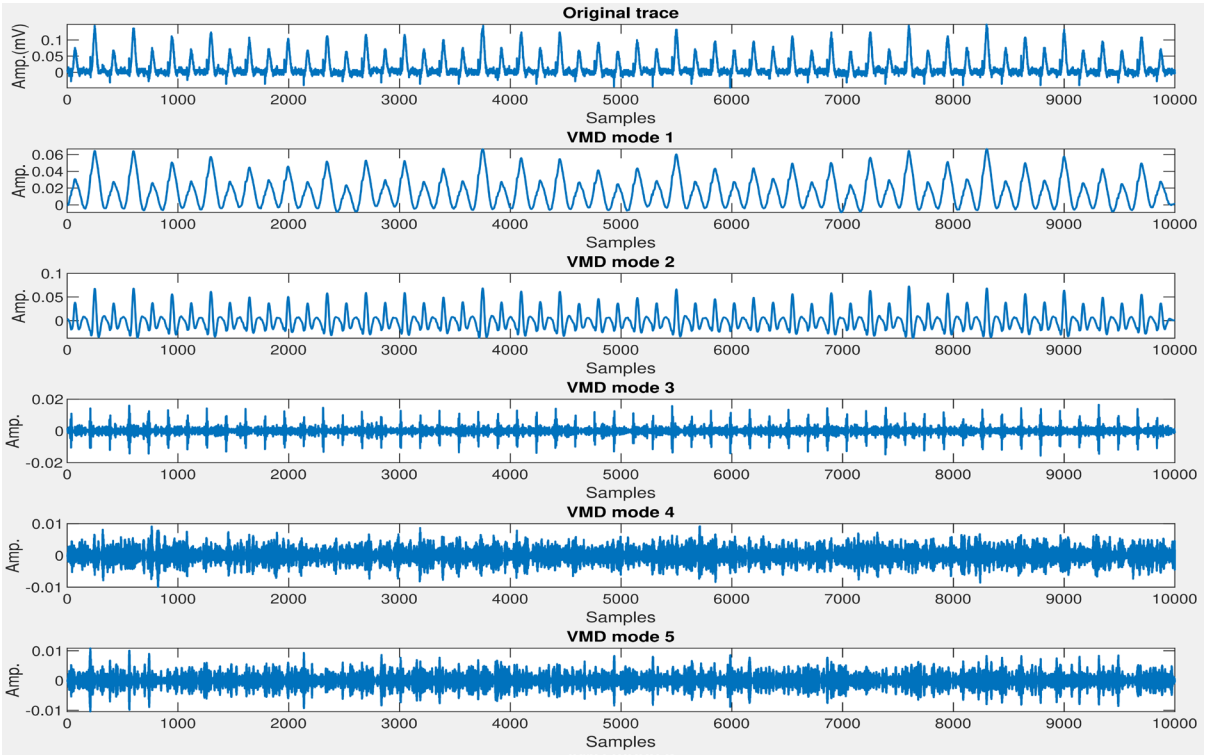


Fig. 3. VMD modes of power traces with $K = 5$ and $\alpha = 1000$.

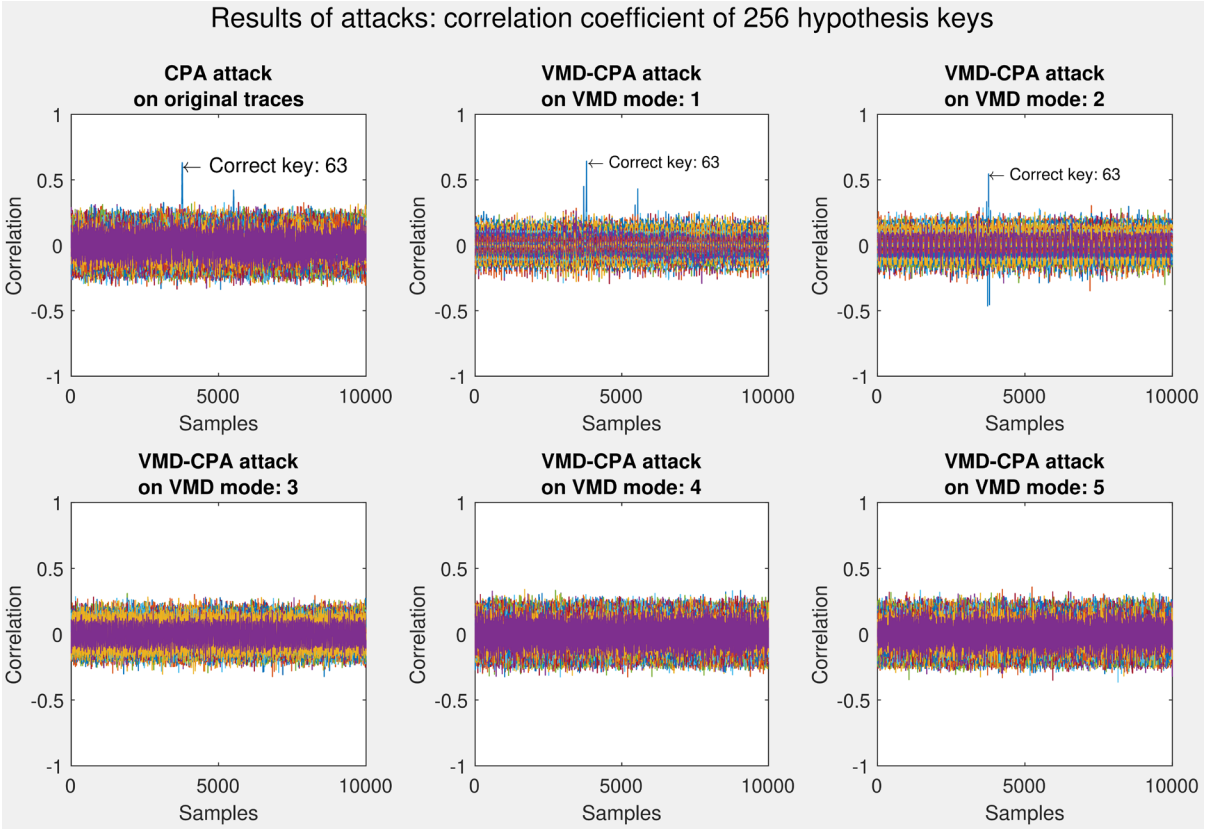


Fig. 4. Results of VMD-CPA attack on original traces and VMD modes

4.2.2. Performance comparison to CPA attack on original traces.

Fig. 5 shows the relationship between the correlation coefficient and the number of power traces obtained by performing CPA on original traces and VMD-CPA on VMD mode 1 of power traces. The correlation coefficient is significantly larger than the rest when the number of power traces is 91 for CPA and for VMD-CPA is 79 (Table 1). This means that the number of power traces for VMD-CPA to recover the correct key decreased approximately by 13%. These results prove that VMD mode contains more leakage information than amplitude in original power traces.

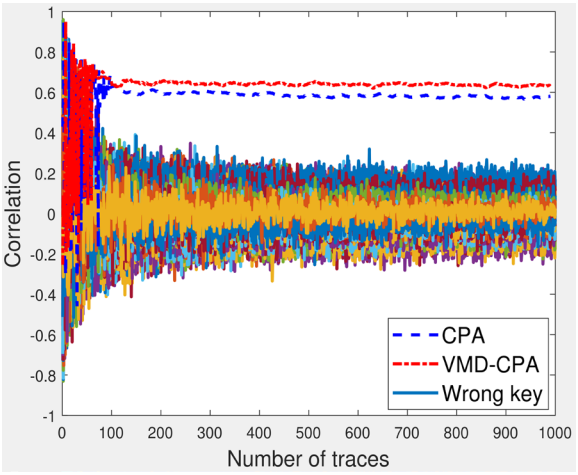


Fig. 5. Correlation of correct key and wrong key versus number of attack traces.

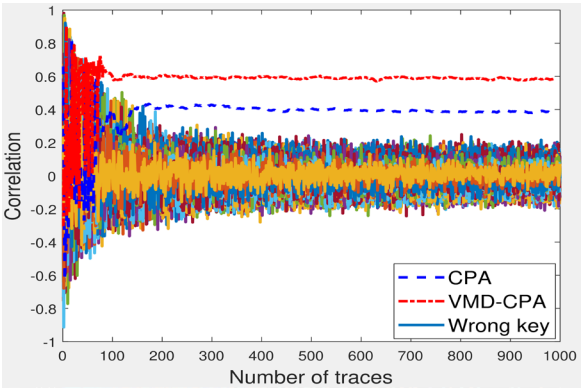


Fig. 6. Correlation of correct key and wrong key versus number of attack traces with $SNR_1 = 10\,dB$.

Table 1. Number of traces (N_a) for attack to recover the secret key of AES-128.

Noise level	CPA	VMD-CPA
No artificial noise added	91	79
$SNR_1 = 10dB$	203	81
$SNR_2 = 5dB$	N/A	165

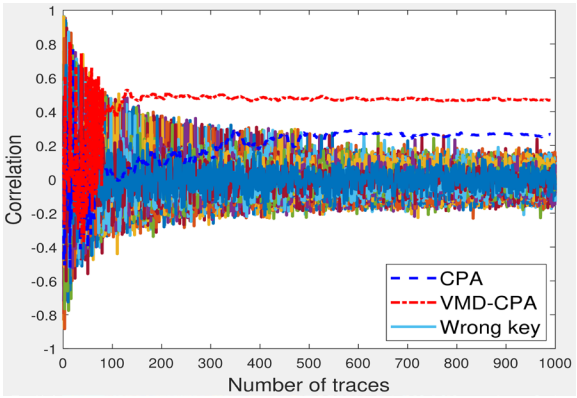


Fig. 7. Correlation of correct key and wrong key versus number of attack traces with $SNR_1 = 5\,dB$

4.2.3. Robustness to the noise of VMD-CPA attack

The power traces are usually contaminated with noise. To consider noisy conditions, additive white Gaussian noise (AWGN) is added to the power traces. In our experiments, two noise levels of $SNR_1 = 10dB$ and $SNR_2 = 5dB$ are added to original power traces. The results of CPA and VMD-CPA attack are presented in Fig.6, Fig.7 and Table 1. With $SNR_1 = 10dB$, both CPA and VMD-CPA attack can recover the secret key of AES but the number of power traces reduces from 203 to 91, equivalent to a 60% reduction. With $SNR_2 = 5dB$, VMD-CPA can be able to recover the secret key while CPA does not. This proves that the VMD modes have an impact on noise reduction so the VMD-CPA attack should work well under noisy conditions. This property is very useful in real attack scenarios where collected measurement traces invariably contain noise.

4.2.4. Investigation of VMD-CPA on hardware implementation of cryptographic algorithms.

To investigate the potential of VMD-CPA against hardware implementation of cryptographic algorithms, we have attacked power traces of AES-128 that implemented on Xilinx Spartan-6 on Sakura-G board. Fig.8 shows an example of the power trace and three VMD modes. The results of CPA attacks on all VMD modes and the original traces are presented in Fig.9. It can be seen that the attack on the original power traces and VMD mode 1 can recover the correct key of AES-128 while not for other VMD modes. This can be explained by that VMD mode 1 contains the most information of the original power traces and other VMD mode can be considered as the noise components of the power traces. Fig.10 shows the attack results with noisy power traces ($SNR = 5dB$), VMD-CPA can be able to recover the secret key while CPA does not. This result again confirms the ability of VMD in reducing noise for improving attack efficiency.

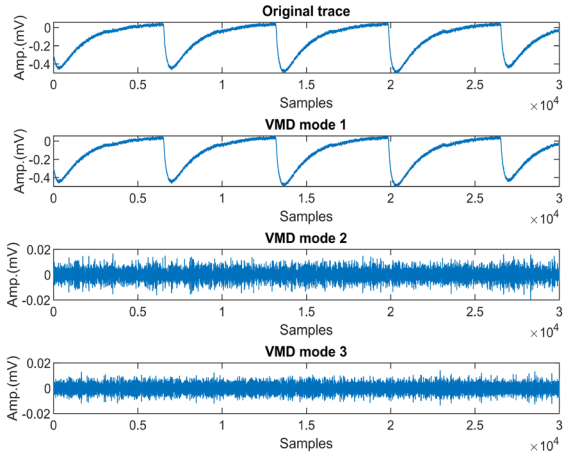


Fig. 8. A power trace of FPGA-implemented AES-128 and its VMD modes.

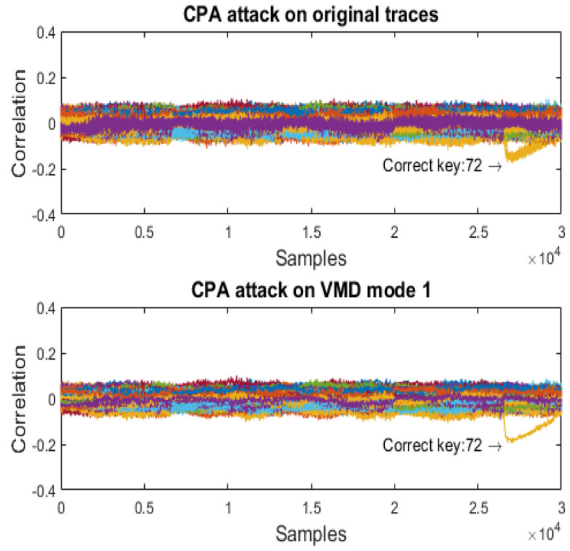


Fig. 9. Results of CPA attack on original traces and VMD mode 1

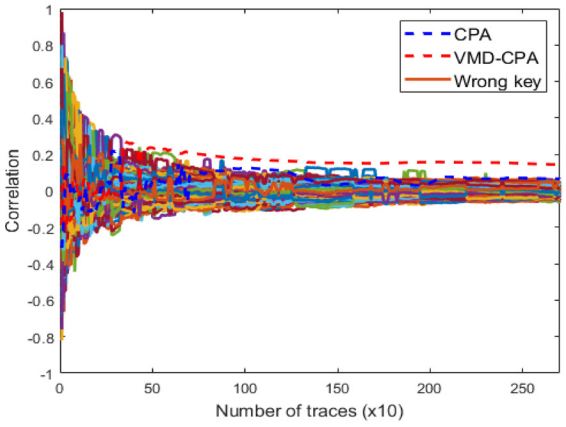


Fig. 10. Attack performance with noisy traces of FPGA-implemented AES-128.

4.3. Discussion

The proposed VMD-CPA attack framework takes advantage of the noise reduction capability of VMD so it can improve the efficiency of the secret key recovery on AES-128 that is implemented by software on a microcontroller and FPGA. Like power analysis attacks, VMD-CPA is based on the dependence between power consumption and processed values of attack devices, not cryptographic algorithms so this method can be used to attack other cryptographic algorithms when they are implemented on a specific device.

5. Conclusion

In this paper, an efficient correlation power analysis attack, VMD-CPA, is proposed that using VMD as a preprocessing step for power traces. The research shows that VMD separates the power trace into VMD modes and there exists one VMD mode containing maximum useful information for power analysis attacks. VMD-CPA attack is more effective than traditional CPA attack in reducing the number of power traces. Furthermore, VMD-CPA is less sensitive to noise so it can be used well with noisy power traces. In our opinion, this work suggests a new approach for power analysis attacks on other representations of power traces using variational mode decomposition, and this method should also be tested with other power analysis attacks.

References

[1] P. Kocher, J. Jaffe, B. Jun, Differential Power Analysis, CRYPTO 1999, LNCS 1666. Springer: Heidelberg, p. 388–397, 1999. https://doi.org/10.1007/3-540-48405-1_25

[2] S. Mangard, E. Oswald, and T. Popp, Power Analysis Attacks: Revealing the Secrets of Smart Cards, New York: USA: Springer, 2010.

[3] E. Brier, C. Clavier, F. Olivier, Correlation power analysis with a leakage model, in Proceedings of the International Workshop on Cryptographic Hardware and Embedded Systems, Cambridge (USA), 2004. https://doi.org/10.1007/978-3-540-28632-5_2

[4] D. Oswald and C. Paar, Improving side-channel analysis with optimal linear transforms, in Tnternational Conference on Smart Card Research and Advanced Applications, 2012. https://doi.org/10.1007/978-3-642-37288-9_15

[5] A. Barenghi, G. Pelosi, and Y. Teglia, lnformation leakage discovery techniques to enhance secure chip design, in International Workshop on information Security Theory and Practices, 2011. https://doi.org/10.1007/978-3-642-21040-2_9

[6] Y. Souissi, M. A. Elaabid, N. Debande, S. Guilley, and J.-L. Danger, Novel applications of wavelet transforms based side-channel analysis, in Non-Invasive Attack Testing Workshop, 2011

[7] A. Park, D.-G. Han, and J. Ryoo, CPA performance comparison based on Wavelet Transform, in Security Technology (ICCST), 2012 IEEE International Carnahan Coriference, 2012. https://doi.org/10.1109/CCST.2012.6393559

[8] T-H. Le, J. Cl6diere, C. Serviere, and J.-L. Lacoume, Noise reduction in side channel attack using fourth-order cumulant, in IEEE Transactions on Information Forensics and Security, 2007.

[9] Y. Souissi, S. Guilley, J.-1. Danger, S. Mekki, and G. Duc, Improvement of power analysis attacks using Kalman filter, in IEEE International Conference on Acoustics, Speech and Signal Processing, 2010. https://doi.org/10.1109/ICASSP.2010.5495428

[10] K. Dragomiretskiy and D. Zosso, Variational Mode Decomposition, IEEE Transactions on Signal Processing, vol. 62, no. 3, pp. 531-544, 2014. https://doi.org/10.1109/TSP.2013.2288675.