A Novel Points of Interest Selection Method for SVM-based Profiled Attacks

Tran Ngoc Quy, Nguyen Hong Quang

***Abstract*—Currently, one of the most powerful side channel attacks (SCA) is profiled attack. Machine learning algorithms, for example support vector machine (SVM), are currently used to improve the effectiveness of the attack. One issue of using SVM-based profiled attack is extracting points of interest (POIs), or features from power traces. Our work proposes a novel method for POIs selection of power traces based on the combining variational mode decomposition (VMD) and Gram-Schmidt orthogonalization (GSO). VMD is used to decompose the power traces into sub-signals (modes) and POIs selection process based on GSO is conducted on these sub-signals. As a result, the selected POIs are used for SVM classifier to conduct profiled attack. This attack method outperforms other profiled attacks in the same attack scenario. Experiments were performed on a trace data set collected from the Atmega8515 smart card with AES-128 run on the Sakura-G/W side channel evaluation board and the DPA Contest v4 dataset to verify the effectiveness of our method in reducing number of power traces for the attacks, especially with noisy power traces.**

***Tóm tắt*—Hiện nay, tấn công mẫu được xem là một trong những tấn công kênh kề (SCA) mạnh. Các thuật toán học máy, ví dụ như máy vector hỗ trợ (SVM), thường được sử dụng để nâng cao hiệu quả của tấn công mẫu. Một thách thức đối với tấn công mẫu sử dụng SVM là cần phải tìm được các điểm thích hợp (POI) hay các đặc trưng từ vết điện năng tiêu thụ. Công trình nghiên cứu này đề xuất một phương pháp mới để tìm POI của vết điện năng tiêu thụ bằng cách kết hợp kỹ thuật phân tích mode biến phân (VMD) và quá trình trực giao hóa Gram-Schmidt (GSO). Trong đó, VMD được sử dụng để phân tách vết điện năng tiêu thụ thành các tín hiệu con còn gọi là VMD mode và việc lựa chọn POIs trên VMD mode này được thực hiện dựa trên quá trình GSO. Dựa trên phương pháp lựa chọn POIs này, chúng tôi đề xuất phương pháp tấn công mẫu sử dụng SVM có hiệu quả tốt hơn các tấn công mẫu khác ở cùng kịch bản tấn công. Các thí nghiệm tấn công được thực hiện trên tập dữ liệu được thu thập từ thẻ thông minh Atmega8515 cài đặt AES-128 chạy trên nền tảng thiết bị tấn công kênh kề Sakura-G/W và tập dữ liệu DPA Contest v4, để chứng minh tính hiệu quả của phương pháp của chúng tôi, trong việc giảm số lượng vết điện năng tiêu thụ cần cho cuộc tấn công, đặc biệt trong trường hợp các điện năng tiêu thụ có nhiễu.**

Keywords—side channel attack, profiled attack, points of interest, variational mode decomposition.

Từ khóa—tấn công kênh kề, tấn công mẫu, POI, phân tích mode biến phân.

I. INTRODUCTION

Side channel attack is one of the most powerful cryptanalysis techniques for revealing secret key or sensitive information stored on cryptographic devices. The conduct of SCA is based on the analysis of unintended side channel leakages observed from the devices during cryptographic algorithms run on. There are so many forms of the observed leakages, but the time of operation, the power consumption of the devices, or electromagnetic radiation are the most common uses. SCAs based on the power consumption are known as the power analysis attacks first proposed by Kocher et al. in the late 1990s [1]. These attacks rely on the physical nature of instantaneous power consumption of a cryptographic device depending on the data being processed and the operation being executed. This dependency can be used to expose the data that contains secret key of a cryptographic device. Most power analysis attacks fit into one of the following categories:

Non-profiled attacks techniques aim to recover the secret key by performing statistical calculations on power measurements of the device under attack regarding a hypothesis of the device's leakage. Typical examples are Differential Power Analysis (DPA) [1],

This manuscript is received on November 11, 2020. It is commented on Decemeber 4, 2020 and is accepted on Decemeber 4, 2020 by the first reviewer. It is commented on Decemeber 15, 2020 and is accepted on Decemeber 25, 2020 by the second reviewer.

Correlation Power Analysis (CPA) [2] and Mutual Information Analysis (MIA) [3].

Profiled attacks assume a stronger adversary who is in possession of a profiling device. It is an open copy of the attacked device which the adversary can manipulate to characterize the leakages very precisely in a first step. Once this has been done, the built model can be used to attack the actual target device in the key extraction phase. So far, there has been a lot of attention on profiled attack in the SCA research community. The first profiled attack is called template attack, as proposed in [4] by Chari et. al, relies on the assumption that power consumption characteristics follows multivariate Gaussian distribution. However, in general, this assumption should not be met, so machine learning techniques are introduced to conduct profiled attacks. Consequently, several works have applied machine learning techniques to profiled SCA attacks [5]–[8]. All these works indicate that machine learning based profiled attacks are more efficient and SVM is commonly used as a machine learning algorithm.

Machine learning based profiled attacks relax the need for probability distributions of side channel leakage traces but still require specific extraction techniques to identify POIs on the traces or feature selection in machine learning domain. In SCA, POIs are time sample points from the power traces that correspond to the calculation of the sensitive variables being targeted and their values change according to those variables [9]. The POIs selection, as input features to machine learning algorithms, is critical for two main reasons as follows: (1) the power traces are usually acquired by measurement equipment with high sampling rates and so consist of a large amount of time samples. However, often only a relatively small range of these time samples are informative or statistically dependent on a sensitive target variable; (2) power traces are considered as highly multi-dimensional data that results in the curse of dimensionality issues with machine learning algorithms. Computational and runtime complexity for them to solve a task increase. Indeed, POIs are critical to the effectiveness of profiled attacks. The more precisely the POIs are selected, the better the ability to characterize the power consumption of the profiled device, resulting in increased attack efficiency and vice versa. Our work focuses on a method for finding POIs for SVM-based profiled attacks.

The remainder of the paper is structured as follows: In *Section II*, the related works are presented. The *Section III* describes the background of this work: profiled attacks, SVM-based profiled attack, variational mode decomposition, Gram-Schmidt Orthogonalization and SVM. In *Section IV*, we present our proposed POIs selection method. The experiments and results are presented in *Section V*. Finally, the main conclusions of our paper are presented in last section.

II. RELATED WORKS

Some studies in the side channel community focus on methods of finding POIs for profiled attacks, which can be classified into four classes: filter methods, dimensionality reduction method, wrapper and hybrid methods, and machine learning based methods. In filter methods, POIs selection process operates on the basis of computation of some sample-wise statistics, whose aim is to quantify a sort of signal strength. The signal-strength estimates are derived from classical side channel attack distinguishers computed under the right key hypothesis, such as the Difference of Means [4] or Correlation Power Analysis (CPA) [10]. Other deployed estimates are the Sum of Squared Differences [11], the Signal-to-Noise Ratio [12], [13], and the Sum of Squared t-differences, corresponding to the t-test [11]. Once the chosen signal-strength estimate is computed, all time samples for which the signal strength is higher than a certain threshold are selected as POIs. Of these, the POIs selection method based on CPA estimates is the most common use.

Principal component analysis, as dimensionality reduction method, is another technique for POIs selection. The time samples on traces having the maximum variability in the projection space of PCA are remained as POIs. So far, the effectiveness of PCA-based profiled attack is not clear, as reported in [14]–[16]. Indeed, selecting the number of retained components as well as the threshold of determination in PCA process is also not an easy task.

Profiled attacks presented in [17] used wrapper method for finding POIs. In the wrapper method, subsets of time samples on the power traces are evaluated by the prediction performance of a classifier and the subset that has the best performance is selected as POIs. As claimed in [17], wrapper and hybrid methods gave slightly better results. The issue with this approach is that computational complexity and search space increase exponentially as the length of trace increases.

Ideally, an attacker wants to avoid all the manual feature engineering usually needed for SCAs. For this, ML algorithms that are capable of automatically determining the most important sample points become interesting. The normal-based POIs selection mechanism tailored for SVMs was the first work suggested in this regard [18] in terms of a machine learning-based POIs selection method.

Previous works have only focused on finding POIs from raw traces and to our knowledge there are only a few works on finding POIs with noisy traces. Furthermore, there have been no further studies on feature engineering in the machine learning domain as applied to profiled attacks. For noisy traces, the authors in [9] claim that the goodness of POIs selections depends significantly on the noise level: as noise level increases the goodness of POIs selection decreases, while at the same noise level, CPA based POIs selection method is the best. This drawback of the POIs selection method is confirmed by the authors in [17] regarding the wrapper and embedded method. Therefore, this paper presents a new POIs selection method based on the other representation of power trace and evaluates the effectiveness of the proposed method with the noisy traces.

In the literature, VMD [19] is used to process noisy signals, extract features from original signals for machine learning applications, and GSO [20] could select the best features from the set of given features. To the best of out knowledge, no study has been conducted to investigate the VMD and GSO for POIs selection in side channel attacks. So, our POIs selection method is a combination of VMD and GSO. VMD as a new tool decomposes power traces in different sub-signals and one of them is selected as the features of raw power trace. In order to avoid large dimensions of feature vector, GSO-based feature selection method is used for elimination of redundant features. The best features selected by GSO are considered as POIs of power traces. These POIs are then used for SVM-based profiled attack. We denote SVM_{VMD} for our proposed attack. To demonstrate the efficiency of our proposed attack method, we compare our method to two other SVM-based profiled attacks using the SVM classifier. One uses CPA as the POIs selection method as in [5], so called SVM_{CPA} and it is currently considered to be the best method, and the other uses a normal-based POIs selection method as in [18], so called SVM_{NB}. We also investigate the effectiveness of our method with noisy power traces, which often happens in real attack scenarios. Our main contribution is a novel method for feature selection of the power traces that is used for SVM-based profiled attacks in the real scenarios.

III. BACKGROUND

A. Profiled attack

Profiled SCAs are considered the most powerful type of SCAs and are divided into two phases. In the first step, the adversary takes advantage of a profiling device on which he can fully control input and secret key parameters of the cryptographic algorithm. He uses that to acquire a set of N_p profiling side-channel traces $X \in \mathbb{R}^D$, where D denotes the number of sample points in the measurements. Let $Z = g(t, k)$ be a random variable representing the result of an intermediate operation of the target cipher which depends partly on public information p (plaintext or ciphertext chunk) and secret key $k \in K$, where K is the set of possible key values. Z is assumed to have an influence on the deterministic part of the side-channel measurements. The ultimate goal of the attacker during the profiling phase is then to estimate the probability:

$$\Pr(X|Z = z) \quad (1)$$

for every possible value $z \in Z$ from the profiling base $\{X_i, z_i\},\ i = 1, \dots, \mathbb{N}_p$. In template attacks [4] for example, the Probability Density

Function (PDF) of (1) is assumed to be multivariate Gaussian and can be described by the parameter pairs (μ_z, Σ_z), depicting the mean values and covariance matrices for the corresponding values of z [4].

During the attack phase, the adversary generates a new set of N_a attack traces from the actual target device (which is structurally identical to the profiling device) whereby the secret key k^* is fixed and unknown. In order to retrieve it, estimations for all possible key candidates $k \in K$ are made and combined following the *maximum likelihood* strategy such that:

$$k^* = \underset{k \in K}{argmax} \prod_{i=1}^{N_a} \Pr(Z = z_i | X_i) \qquad (2)$$

where the probabilities on the right are retrieved with the help of the built profile and public information which is also available for the attack traces.

In general, the PDF of the power trace is not known upfront, machine learning algorithms are used to estimate the probability distribution function of (1) on the basis of data. Two well-known examples are Random Forest (RF) and a Support Vector Machine (SVM). These two techniques allow to remove the Gaussian assumption and to infer in a data driven manner the model which best fits the stochastic dependency between target value and power consumption.

B. SVM-based profiled attack

The SVM-based profiled attack, shown in Fig. 1, is carried out in two phases: a profiling phase and an attack phase. In the profiling phase, power traces are collected from the profiled device while it is executing a cryptographic algorithm to form a trace data set. This trace data set is labeled according to the Hamming weight of targeted value of the algorithm that needs to be profiled $Z_1, \ldots, Z_m$. Usually, these targeted values are taken at the output of the S-box. Because they are 8-bit values that result in 9 Hamming weight classes from 0 to 8 denoted as: $c_0, c_1, \ldots, c_8$. This labeled set of traces is fed into the feature extraction and selection block for mapping traces into feature space and the best features are selected. These selected features are considered POIs of the power trace in feature space that should describe the statistical dependency of the Hamming weight of the targeted value Z_i with the power consumption. In the final step of the profiled phase, POIs of all traces are used to train SVM to model the power consumption characteristic of the profiled device.

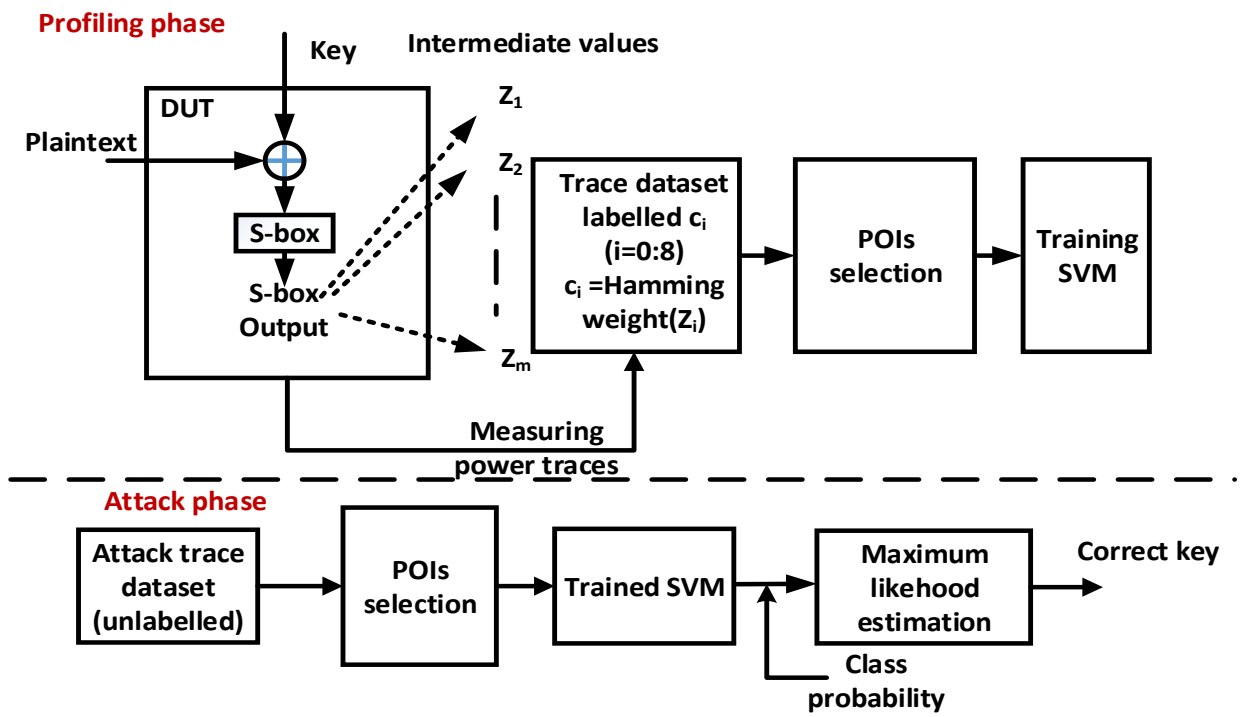

Fig. 1. SVM-based profiled attack framework.

During the attack phase, unlabeled traces collected from the attack device are fed into the feature extraction and selection block to select POIs and they are next classified by the trained SVM model to determine the probabilities of the traces for classes $c_0, \dots, c_8$. Finally, we compute the log likelihood for each hypothesis value of the key byte that is used by the attack device as follows:

$$\log L_k \equiv log \prod_{i=1}^{N_a} P_{SVM}(X_i|c_i) = \sum_{i=1}^{N_a} \log P_{SVM}(X_i|c_i) \quad (3)$$

where k is a hypothesis key byte value, $c_i = Hamming\ weight(Sbox(p_i, k))$, p_i is the plaintext associated with trace X_i, and the number of attack traces is N_a. The key k_c that maximizes the log likelihood in (4), as given below, is predicted to be the correct key.

$$k_c = \underset{k_c}{argmax} \log L_k \quad (4)$$

C. Variational mode decomposition

VMD decomposes a signal $x(t)$ into a small number of *K* narrowband sub-signals, called intrinsic mode functions (IMFs) or the VMD modes for simplcity as given [19] equation (5).

$$x(t) = \sum_{k=1}^{K} u_k(t) \quad (5)$$

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 (6).

$$\min_{u_k, f_k} \left\{ \sum_k \left\| \frac{d}{dt} \left[\left(\delta(t) + \frac{j}{\pi t} \right) * u_k(t) \right] e^{-j2\pi f_k t} \right\|_2^2 \right\} \quad (6)$$

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

The formula can be transformed into an unconstrained problem which can be solved by an alternate direction method of multipliers (ADMM) by introducing a quadratic penalty term and a Lagrangian multiplier factor. More details about VMD can be found in [19].

D. GSO-based feature selection

The GSO process is a simple forward selection method which can be effectively used for features ranking. Suppose the k^{th} feature of M patterns is denoted by vector $X_k = [x_{k1}, x_{k2}, \dots, x_{kM}]$ and $Y = [y_1, y_2, \dots, y_M]^T$ representing the vector of output target. In order to select the best correlated feature with output, the cosine of angle between each input feature X_k and target Y is calculated as an evaluation criterion [20].

$$\cos(\varphi_k) = \frac{\langle X_k . Y \rangle}{\|X_k . Y\|} \quad (7)$$

Where φ_k is the angle between input k^{th} feature vector X_k and output target Y, N is the number of all features and $\langle X_k . Y \rangle$ denotes the inner product between X_k and Y. If the output is fully proportional to input, the φ_k is zero, and inversely if the output is fully uncorrelated to

input, the φ_k is $\pi/2$ [19]. So, in an iterative procedure, the feature that maximizes the above-mentioned evaluation criterion is selected as the most correlated feature to target. For selection of the next feature, the output vector and all other candidate features are mapped to null space of the selected feature and then input features and output vectors are updated with new data. The ranking procedure is repeated until all candidate features are ranked, or when a predetermined stopping condition is met [19].

IV. THE PROPOSED POIS SELECTION METHOD

Features or POIs selection is critical to the effectiveness of profiled attacks. The more precisely the features are selected, the better the ability to characterize the power consumption of a profiled device, resulting in increasing attack efficiency and vice versa. This section presents a new method for finding POIs of power traces for SVM-based profiled attack. The inspiration of our method is based on power trace characteristics are discovered as follows:

The power trace collected during the operation of a cryptographic device describes its power consumption. It consists of many components in which dynamic power dissipation is the most important [12]. 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. Therefore, in the 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 both amplitude and frequency modulation signal and the central frequency of its spectrum is 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 - frequency modulation signals with different center frequencies. So, if it is possible to separate the dynamic power dissipation drom amplitude - frequency modulation signals with different center frequencies, one of these signals contains significant information leakage related to the target circuit part while the other does not.

As a result, the feature extraction process from power trace should ensure: (1) the remaining features contain the most important information of the trace which is the dynamic power dissipation caused by the target circuit; (2) it could remove the other component of traces; (3) it could reduce noise in the power traces. Fortunately, these requirements can be fulfilled by using the VMD method. That is because VMD decomposes a trace into different components and it is robust to noise.

In our proposed method, VMD is used to extract features from power traces. VMD decomposes the signal into sub-signals, called VMD mode in this paper, which are amplitude-modulated frequency-modulated signals so each mode contains a specific frequency spectrum with different center frequency. So, the VMD mode which has center frequency relates to clock frequency could be used as a feature of the power trace. Indeed, VMD can discover signal changes more accurately so that features of power traces can be recognized more accurately. Moreover, VMD is robust to noise because of using Wiener filter technique. Thus, VMD should be useful for using noisy traces.

Unfortunately, the VMD mode still contains redundant features which are not related to the target variable that has been profiled. Therefore, they must be eliminated to increase increasing the generalization capability of the classifier and reduce the volume of training data. The elimination of redundant features is known as the feature selection. In previous related works, all features that are higher than a certain threshold are selected. For this purpose, GSO-based feature selection is used in this work.

To sum up, there are three phases in the proposed POIs selection method as follows: VMD decomposition of power traces, VMD mode determination, and GSO for POIs selection (Figure 2). In first phase, VMD is used to decompose original traces to VMD modes. In the VMD process, it is necessary to set parameters. The number of decomposed modes *K*: VMD needs to preset the number of decomposed 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 traces by the VMD, the number of VMD modes (K) and the quadratic penalty factor (a) should be determined beforehand. In this study, the parameters K and a, were determined according to the following steps:

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

Step 2. Add up the modes for each of the K and a value 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 value for maximum Pearson correlation coefficient.

For other input parameters of VMD: update rate, τ and convergence condition ϵ are selected by standardization values in range $0: 1e-6$ [19].

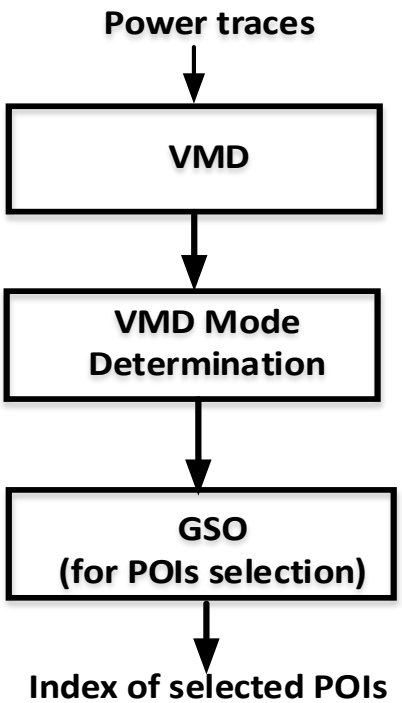

Fig. 2. VMD-GSO based features selection method.

In the second phase, VMD mode determination phase, in order to determine which VMD mode has frequency range that relates to frequency of operating clock our attack device and this mode can be used as features of the power trace, we conduct correlation power analysis (CPA) attacks on all the VMD modes. Based on the results of CPA attacks, the VMD mode that has the largest correlation coefficient is selected.

The last phase, named GSO for POIs or feature selection phase, it is necessary to set number of selected POIs, called N. Our principle of finding the value of N is to find a trade-off between the accuracy and the computation cost or execution time. The selected POIs are put to SVM classifier for the training process and the value of N that SVM has the highest accuracy together with the lowest execution time is selected.

V. EXPERIMENTS

In this section, we show the experimental results of implementing the profiled attacks with our proposed POIs selection method, called SVM_{VMD}. We compare the effectiveness of the proposed method with the two profiled attacks SVM_{CPA} and SVM_{NB}. The following parameters are used to evaluate the effectiveness of an attack: (1) The ability to reveal the correct key: To confirm that our profiled attacks can reveal the correct key used by AES-128, we figure out the probability of each key being the actual key used. The key with the highest probability is the most likely one; (2) Guessing Entropy [21]: This score is also known as the average rank of correct key that is widely used to rate the effectiveness of side channel attack according to the number of attack traces. Guessing entropy is the index of correct in list all ranked keys.

A. Dataset

DataSet 1: The set consists of 60000 traces collected while AES-128 processed intermediate values at S-box output. AES-128 was implemented on a Smartcard Atmega8515 run on Sakura G/W. A sample of one of the collected power traces has 2500 time-samples which is titled ‘Original trace’ in Fig. 2.

DataSet 2: This dataset was published by DPA contest v4 at http://www.dpacontest.org/ v4. The set consists of 100000 traces, each one consists of 4000 features, of a masked AES implementation. However, the traces leak first-order data and this dataset is only used as an unprotected dataset after unmasking the S-box output. The targeted sensitive variable is the output of S-box, $Sbox(P_i + k^*) \oplus M$, where M is the known mask.

B. Results

1. POIs selection phase

In this section, we investigated the effect of POIs selection on the classification accuracy of the proposed method. First, VMD is used to decompose original traces to VMD modes. For VMD, two main parameters: the number of VMM modes (K) and penalty factor (α) must be initialized in advance and in our experiments, they are set according to the suggestion of Dragomiretskiy and Zosso [22] with $K = 5, \alpha = 1000$. The VDM modes of both Dataset 1 and Dataset 2 are depicted in Figures 3 and 4. As expected, VMD modes contain the different components of the original signal at different central frequencies. Second, in order to determine which VMD mode has frequency range that relates to the frequency of operating clock of our attack device and this mode can be used as a feature of the power trace, we conduct correlation power analysis (CPA) attacks on all the VMD modes. Based on the results of CPA attacks, the VMD mode that has the largest correlation coefficient is selected as the feature of the power trace. As the results given in Table 1, VMD mode 1 is selected as an extraction feature of power trace in Dataset 1 and with Dataset 2 is VMD mode 2.

Table 2 and Table 3 represent the classification accuracy of SVM on Dataset 1 and Dataset 2 when the extracted features are VMD mode 1 and the selected POIs are chosen by GSO. The selected POIs are put into an SVM classifier for the training phase. As the POIs dimension increases, so does the accuracy of the classification, but with too many POIs the accuracy decreases because the features do not generalize the power consumption characteristic well when used by the classifier. Therefore, the subset of POIs with the highest accuracy and lowest POIs dimensions are selected and shown in bold font.

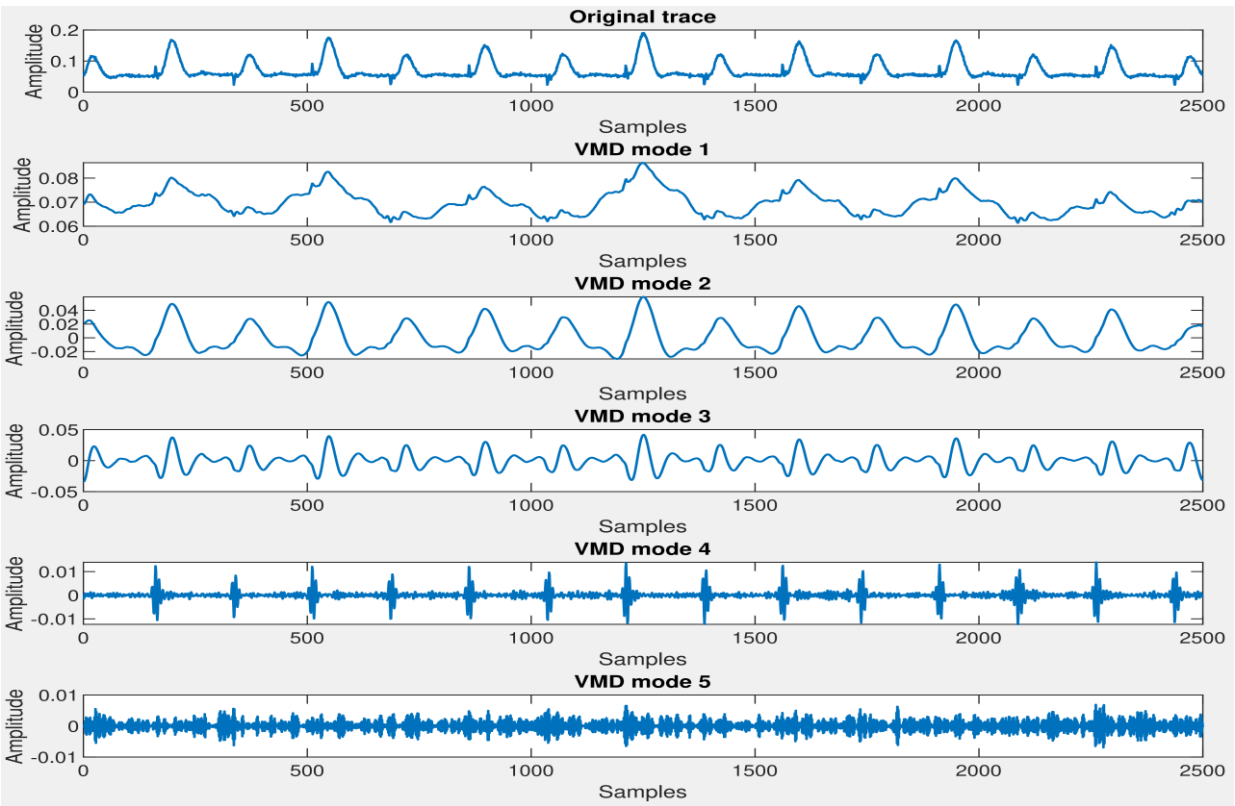

Fig. 3. VDM mode of the power trace on Dataset 1.

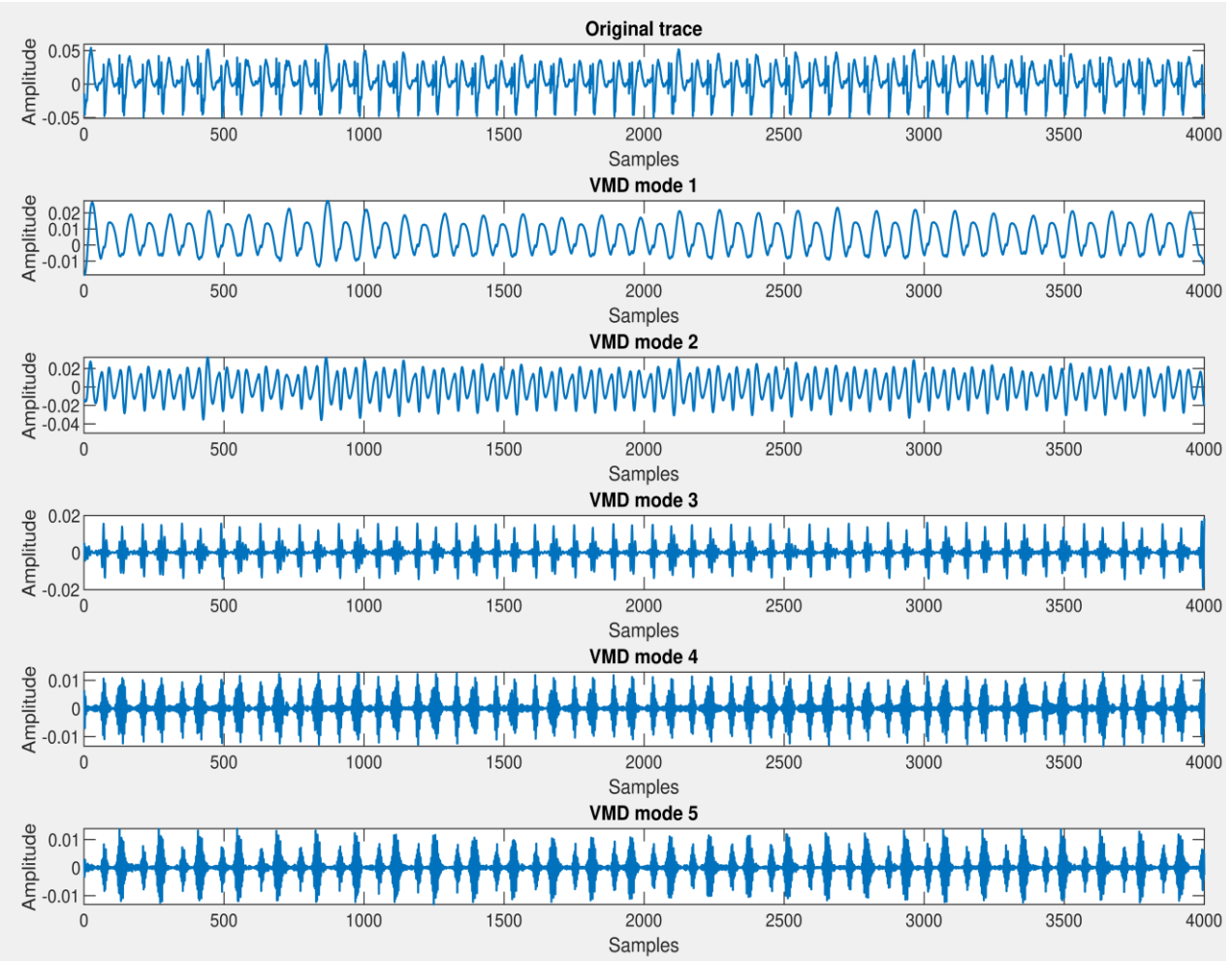

Fig. 4. VDM mode of the power trace on Dataset 2.

TABLE 1. RESULTS OF CORRELATION POWER ATTACK ON VMD MODES

	Dataset 1		Dataset 2	
	Max correlation	**Key found**	**Max correlation**	**Key found**
VMD mode 1	0.64	63 (correct)	0.52	108 (correct)
VMD mode 2	0.62	63 (correct)	0.87	108 (correct)
VMD mode 3	0.54	63 (correct)	0.80	108 (correct)
VMD mode 4	0.37	255 (wrong)	0.37	188 (wrong)
VMD mode 5	0.35	246 (wrong)	0.34	135 (wrong)

TABLE 2. ACQUIRED RESULTS CONSIDERING POIS SELECTION ON DATASET 1

Dimensions	**Selected POIs**	**Classification accuracy (%)**
2	1036 509	18.2
4	1036 509 2261 2262	30.12
6	1036 509 2261 2262 2263 2260	50.31
8	1036 509 2261 2262 2263 2260 2264 2265	81.56
10	1036 509 2261 2262 2263 2260 2264 2265 2259 861	81.78
12	1036 509 2261 2262 2263 2260 2264 2265 2259 861 2267 1038	89.22
14	**1036 509 2261 2262 2263 2260 2264 2265 2259 861 2267 1038 411 577**	**95.03**

16	1036 509 2261 2262 2263 2260 2264 2265 2259 861 2267 1038 411 577 886 1687	95.02
18	1036 509 2261 2262 2263 2260 2264 2265 2259 861 2267 1038 411 577 886 1687 1211 1670	94.27
20	1036 509 2261 2262 2263 2260 2264 2265 2259 861 2267 1038 411 577 886 1687 1211 1670 1576 216	92.84

TABLE 3. ACQUIRED RESULTS CONSIDERING POIS SELECTION ON DATASET 2.

Dimensions	**Selected POIs**	**Classification accuracy (%)**
2	1804 3201	22.6
4	1804 3201 1664 2389	31.89
6	1804 3201 1664 2389 689 3231	60.38
8	1804 3201 1664 2389 689 3231 1524 1556	80.24
10	1804 3201 1664 2389 689 3231 1524 1556 3093 3192	86.66
12	1804 3201 1664 2389 689 3231 1524 1556 3093 3192 2766 2282	90.35
14	1804 3201 1664 2389 689 3231 1524 1556 3093 3192 2766 2282 1244 852	95.68
16	**1804 3201 1664 2389 689 3231 1524 1556 3093 3192 2766 2282 1244 852 2392 1797**	**96.62**
18	1804 3201 1664 2389 689 3231 1524 1556 3093 3192 2766 2282 1244 852 2392 1797 2251 3113	94.58
20	1804 3201 1664 2389 689 3231 1524 1556 3093 3192 2766 2282 1244 852 2392 1797 2251 3113 3108 1095	90.28

2. Key recovery phase

In order to verify our proposed SVM_{VMD} profiled attack has the ability to reveal secret key of attack device, In the attack phase, SVM_{VMD} is used to reveal the secret key when classifying 9 hamming weight classes of S-box output. Instead of predicting the class HW of each trace, we gave the posterior conditional probability $P_{SVM}(X_i|c)$. The estimated probability of hypothetical keys is determined by the maximum likelihood estimation. The correct key is defined as the key with the highest probability. For Dataset 1, which was collected in this experiment, the first byte of the AES-128 key is 63, and that is indeed assigned the largest probability value, as depicted in Fig. 5. With Dataset 2, the recovery key is 108, identical to the key used to install AES in the DPA contest v4 (Fig. 6). These results prove that our attack method was able to correctly recover the key used by AES-128.

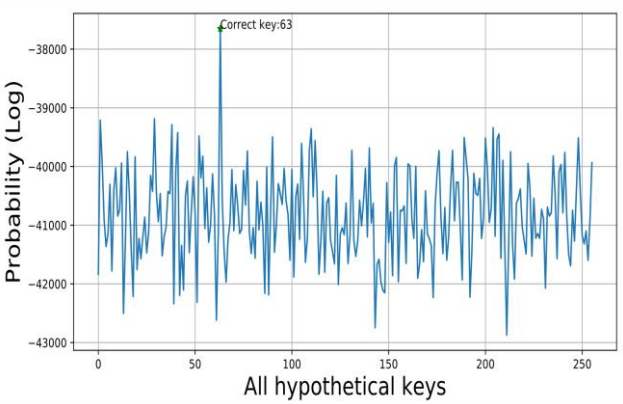

Fig. 5. Probability of all hypothetical keys on Dataset 1.

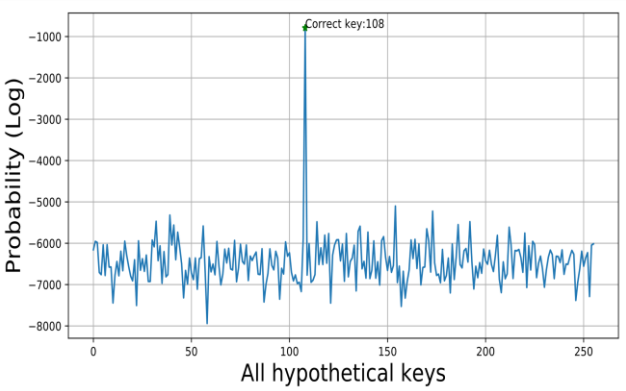

Fig. 6. Probability of all hypothetical keys on Dataset 2.

Fig. 7 and Fig. 8 report the GE corresponding to different numbers of traces used for attacks with Dataset 1 when SVM_{VMD}, SVM_{CPA} and SVM_{NB} are used to predict hamming weight classes. As expected, the GEs of all attacks decrease as the number of traces increases. Moreover, the larger the size of the training set, the lower the GE. The reason for this is that the performance of SVM is determined by its parameters, and the size of the training set is critical to finding the best parameters for the SVM. With Dataset 2, we performed the same experiments as for Dataset 1, and the GE calculated in the attack phases are presented in Figures 9 and 10. The overall performance of all the attacks is the same as those for Dataset 1. Again, SVM_{VMD} achieves the best GE values.

In Table 4, for each dataset we give the number of traces required by the profiled attacks based on SVM for guessing entropy to reach 0. SVM_{VMD} requires the minimum number of traces to recover the key, 10.2 and 5.3 traces on average, corresponding to 100 and 200 profiling traces respectively. These empirical results indicate that the SVM-based profiled attack with our proposed POIs selection method is more effective than the attacks with the CPA and normal-based POI selection method. This can be explained by the combining of VMD and GSO for POI selection allowing more effective selection of trace characteristics than the CPA and normal-based POI selection methods.

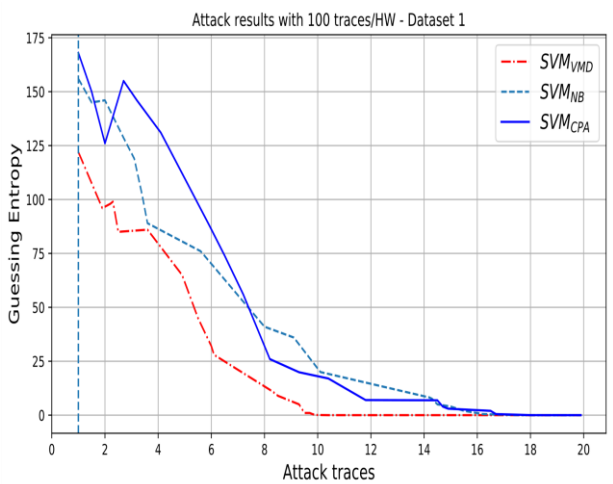

Fig. 7. Attack performance with 100 traces/HW class on Dataset 1.

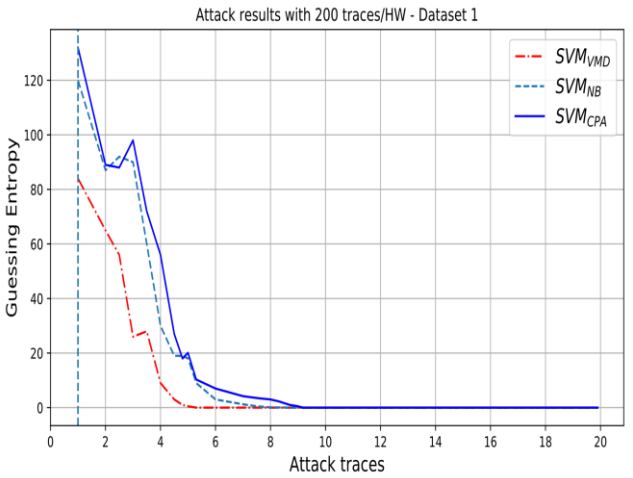

Fig. 8. Attack performance with 200 traces/HW class on Dataset 1.

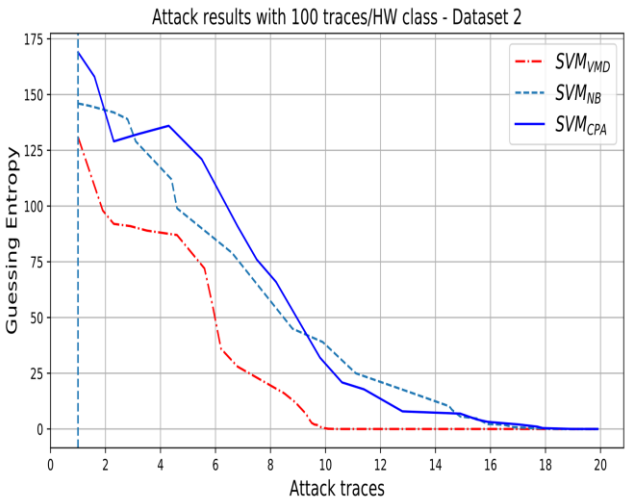

Fig. 9. Attack performance with 100 traces/HW class on Dataset 2.

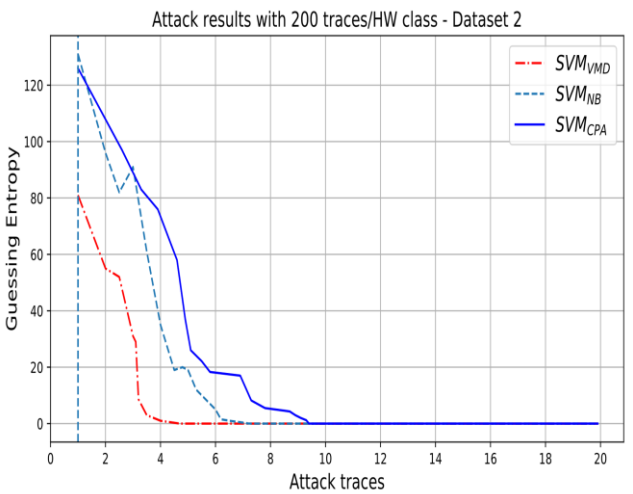

Fig. 10. Attack performance with 200 traces/HW class on Dataset 2.

3. Results in the case of noisy traces

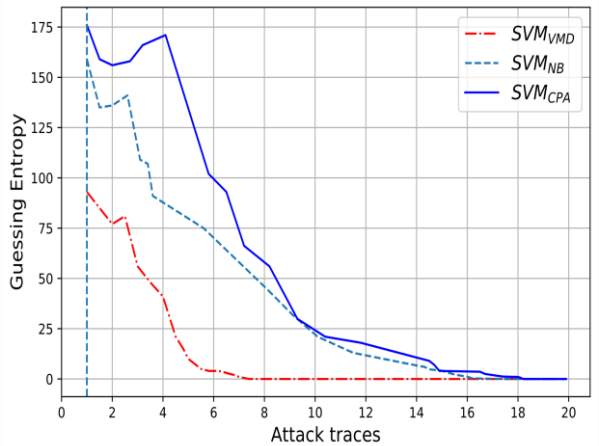

Fig. 11. Attack results on Dataset 1 with $SNR_1 = 20$ noise added to power traces.

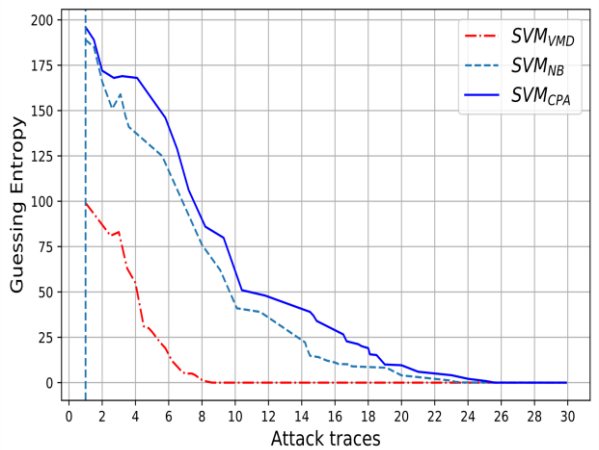

Fig. 12. Attack results on Dataset 1 with $SNR_2 = 10$ noise added to power traces.

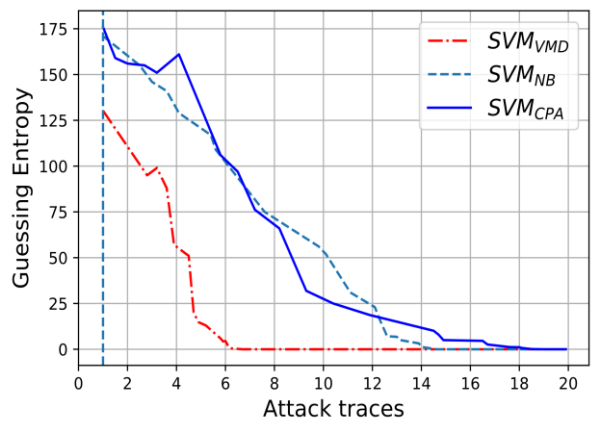

Fig. 13. Attack results on Dataset 2 with $SNR_1 = 20$ noise added to power traces.

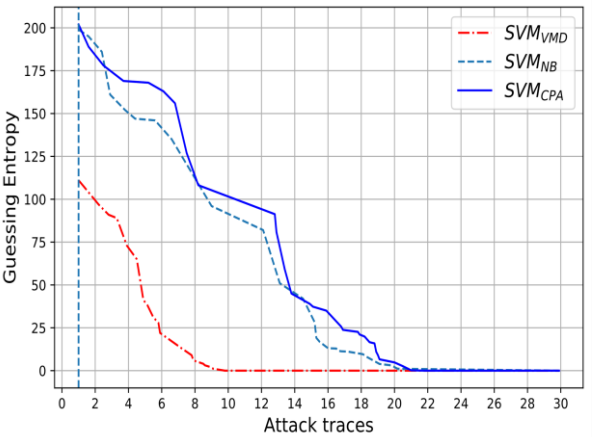

Fig. 14. Attack results on Dataset 2 with $SNR_2 = 10$ noise added to power traces.

The power traces are usually polluted with noise in practice. To examine the effectiveness of our proposed SVM_{VMD} profiled attack in noisy condition, additive Gaussian noise is added to the power traces. In our experiments, two noise levels of standard deviation $SNR_1 = 20$ and $SNR_2 = 10$ are added to both Dataset 1 and Dataset 2. In addition, different feature extraction techniques were used for the SVM-based profiled attacks to investigate their effects on the efficiency of the attacks in the presence of noise. Overall, the guessing entropy of all the attacks increase with the level of noise, but the attack based on SVM with combining of VMD and GSO is the least sensitive to noise. The results of our attacks with 200 profiling traces per Hamming weight class, presented in Fig. 11, 12, 13 and 14 and Table 5, show that out of SVM_{CPA}, SVM_{NB} and SVM_{VMD}, the proposed method, SVM_{VMD}, has the best performance at both noise levels while SVM_{CPA} and SVM_{NB} are comparable to each other. After adding noise to the power trace, the number of traces required for GE to reach 0 increased by only 25% approximately with the proposed attack, while it increased by over 100% for the other methods. This proves that the VMD signal is insensitive to noise so the SVM_{VMD} attack should work well under noisy conditions. This property is very useful in real attack scenarios where collected measurement traces invariably contain noise.

TABLE 4. NUMBER OF TRACES USED BY THE ATTACKS TO ATTAIN GE=0

Num. of. profiling traces	Dataset 1			Dataset 2		
	SVM_{VMD}	**SVM_{CPA}**	**SVM_{NB}**	**SVM_{VMD}**	**SVM_{CPA}**	**SVM_{NB}**
100	**10.2**	18.1	17.6	**10.3**	19.2	18.3
200	**5.3**	9.2	8.7	**4.7**	9.4	7.3

TABLE 5. NUMBER OF NOISY TRACES USED BY THE ATTACKS TO ATTAIN GE=0

Noise level	Dataset 1			Dataset 2		
	SVM_{VMD}	**SVM_{CPA}**	**SVM_{NB}**	**SVM_{VMD}**	**SVM_{CPA}**	**SVM_{NB}**
$SNR_1 = 20$	**7.4**	19.0	17.0	**6.7**	18.8	14.6
$SNR_2 = 10$	**8.6**	25.7	23.6	**9.8**	21.6	20.2

VI. CONCLUSION

In this work, the combining of variational mode decomposition and Gram-Schmidt orthogonalization was proposed as a POIs selection method of power traces. The VMD mode that has central frequency related to clock operation frequency of the attack device can be used as features of power traces and GSO can be used as a POIs selection method. Experimental results show that an acceptable classification accuracy can be achieved when SVM classifier uses these selected features as its input. Compared to other SVM-based profiled attacks, the SVM_{VMD} required the minimum number of traces for successful key recovery. Furthermore, SVM_{VMD} is less sensitive to noise so can be used well with noisy power traces. In our opinion, this work suggests a new approach for feature extraction from power traces using variational mode decomposition, and this method should also be tested in combination with other feature selection methods and learning algorithms for profiled attacks.

REFERENCES

[1] Kocher P., Jaffe J., Jun B. "Differential Power Analysis". In Proceedings of the 19th Annual International Cryptology Conference on Advances in Cryptology. London (UK), 1999, pp. 388–397.

[2] Brier E., Clavier C., Olivier F. "Correlation Power Analysis with a Leakage Model". In: Joye M., Quisquater JJ. (eds) Cryptographic Hardware and Embedded Systems - CHES 2004. CHES 2004. Lecture Notes in Computer Science, vol 3156. Springer, Berlin, Heidelberg.

[3] Gierlichs B., Batina L., Tuyls P., Preneel B. "Mutual Information Analysis". In: Oswald E., Rohatgi P. (eds) Cryptographic Hardware and Embedded Systems – CHES 2008. CHES 2008. Lecture Notes in Computer Science, vol 5154. Springer, Berlin, Heidelberg.

[4] Chari S., Rao J.R., Rohatgi P. "Template Attacks". In: Kaliski B.S., Koç .K., Paar C. (eds) Cryptographic Hardware and Embedded Systems - CHES 2002. CHES 2002. Lecture Notes in Computer Science, vol 2523. Springer, Berlin, Heidelberg.

[5] Heuser A., Zohner M. "Intelligent Machine Homicide." In: Schindler W., Huss S.A. (eds) Constructive Side-Channel Analysis and Secure Design. COSADE 2012. Lecture Notes in Computer Science, vol 7275. Springer, Berlin, Heidelberg.

[6] Hospodar, G., Gierlichs, B., De Mulder, E. et al. "Machine learning in side-channel analysis: a first study." J Cryptogr Eng 1, 293. 2011.

[7] Hospodar, G., De Mulder, E., Gierlichs, B., Vandewalle, J., Verbauwhede, I. "Least Squares Support Vector Machines for Side-Channel Analysis". In: COSADE 2011. CASED, Darmstadt.

[8] S. Picek et al. "Side-channel analysis and machine learning: A practical perspective". 2017 International Joint Conference on Neural Networks (IJCNN), Anchorage, AK, 2017, pp. 4095-4102.

[9] Zheng, Y., Zhou, Y., Yu, Z., Hu, C., Zhang, H. "How to compare selections of points of interest for side-channel distinguishers in practice?" Information and Communications Security: 16th International Conference, ICICS 2014, Hong Kong, China.

[10] Rechberger C., Oswald E. "Practical Template Attacks." Information Security Applications. WISA 2004.

[11] Gierlichs B., Lemke-Rust K., Paar C. "Templates vs. Stochastic Methods". In Goubin L., Matsui M. (eds) Cryptographic Hardware and Embedded Systems - CHES 2006. Lecture Notes in Computer Science, vol 4249, Springer, Berlin, Heidelberg, 2006, pp. 15-29.

[12] Stefan Mangard, Elisabeth Oswald, and Thomas Popp. "Power Analysis Attacks:Revealing the Secrets of Smart Cards". Springer US, 2007.

[13] Lomné V., Prouff E., Roche T. "Behind the Scene of Side Channel Attacks". In Sako K., Sarkar P. (eds) Advances in Cryptology - ASIACRYPT 2013. ASIACRYPT 2013. Lecture Notes in Computer Science, vol 8269, Springer, Berlin, Heidelberg, 2013, pp. 506-525.

[14] Lerman, L., Bontempi, G., Markowitch, O. "Side channel attack: an approach based on machine learning". In COSADE 2011 - Second International Workshop on Constructive Side-Channel, 2011.

[15] Liu, J., Zhou, Y., Han, Y., Li, J., Yang, S., Feng, D. "How to characterize side-channel leakages more accurately?". In ISPEC 2011 - Information Security Practice and Experience:7th International Conference, Guangzhou, China, 2011.

[16] Houssem Maghrebi, Thibault Portigliatti, and Emmanuel Prouff. "Breaking cryptographic implementations using deep learning techniques". In Claude Carlet, M. Anwar Hasan, and Vishal Saraswat, editors, Security, Privacy, and Applied Cryptography Engineering, Springer International Publishing. ISBN 978-3-319-49445-6, 2016, pp. 3-26.

[17] Picek, S., Heuser, A., Jovic, A., Legay, A. "On the relevance of feature selection for profiled side-channel attacks". Cryptology ePrint Archive, Report 2017/1110, https://eprint.iacr.org/2017/, 2017.

[18] Bartkewitz, T., Lemke-Rust, K. "Efficient template attacks based on probabilistic multi-class support vector machines". In Mangard, S. (ed.) Smart Card Research and Advanced Applications:11th International Conference, CARDIS 2012, Graz, Austria, 2012.

[19] Dragomiretskiy K and Zosso D. "Variational Mode Decomposition". IEEE Transactions on Signal, vol. 62, pp. 513-544, 2014.

[20] H. Stoppiglia, G. Dreyfus, R. Dubois, Y. Oussar. "Ranking a random feature for variable and feature selection". J. Mach. Learn, vol. 3, pp. 1399-1414, 2003.

[21] Standaert FX., Malkin T.G., Yung M. "A Unified Framework for the Analysis of Side-Channel Key Recovery Attacks". In In: Joux A. (eds) Advances in Cryptology - EUROCRYPT 2009. EUROCRYPT 2009. Lecture Notes in Computer Science, vol 5479, Springer, Berlin, Heidelberg, 2009.

ABOUT THE AUTHORS

Tran Ngoc Quy

Workplace: Academy of Cryptography Techniques

Email: quyhvm@gmail.com

Education: Master's degree in Electronic and Communication Techniques.

Recent research direction: hardware attack, side channel attack, IoT security.

Nguyen Hong Quang

Workplace: Academy of Cryptography Techniques

Email: quangnh@actvn.edu.vn

Education: Received Master's degree in 2003 and Assoc. Professor title in 2016.

Recent research direction: cryptographic design, side channel attack, hardware security.