Frontiers in Computing and Intelligent Systems
ISSN: 2832-6024 | Vol. 3, No. 1, 2023

Research on group distribution leakage analysis method for RSM

Yiqin Feng*, Yi Wang

School of Cyberspace Security, Chengdu University of Information Technology, Cheng Du, 610225, China
* **Corresponding author**: Yiqin Feng (Email: 924077458@qq.com)

Abstract: Side channel attack is a new and simple attack idea, and its proposal has created a significant threat to the security of cryptographic devices. With the continuous development of deep learning techniques, deep learning-based side channel attacks have enabled the attack techniques to reach new heights, but the attack efficiency and training time have become new problems. In order to improve the attack efficiency, researchers have proposed a large number of leakage analysis methods, which can effectively extract the intervals with significant leakage in the energy consumption curve and reduce the training parameters and data volume. In order to deal with side channel attacks, researchers have proposed various resistance strategies, among which masking protection is the simplest and widely used way. RSM rotating S-box masking scheme is a particularly important masking protection scheme, which uses a first-order masking scheme to randomize the leakage energy consumption of sensitive information using random masks, thus making the algorithm resistant to first-order side channel attacks. For this type of masking algorithm, this paper proposes a new leakage analysis algorithm, namely "Group Distribution Difference" (GDD). This algorithm is based on the distribution difference of energy consumption, and the energy consumption frequency in the group is calculated instead of the probability distribution. The KL distance is used to calculate the difference between groups and find out the leakage interval, so as to achieve an efficient attack.

Keywords: Leakage Analysis, RSM Rotaing S-box; KL distance.

1. Introduction

In 1996, Kocher [1] first introduced the concept of side-channel attacks, and then a large number of studies on side-channel attacks against cryptographic devices followed. In 1999, Kocher [2] and others first introduced the concept of DPA attack, which exploits the connection between the energy change generated by a cryptographic device during the encryption operation and its corresponding intermediate value to restore the key. In 2003, Chari [3] et al. proposed the template attack (TA). This attack first mathematically models the power consumption curves of all keys completing the encryption process to obtain the energy consumption templates generated by all elements performing encryption, and then performs template matching on the energy consumption curves collected by the device to be attacked to find the most suspicious key based on statistical principles. Compared with the non-modeling class of side channel attacks, the template attack has a more accurate portrayal of the leakage and a more efficient attack, but its huge computation is still a problem. In 2015, Gilmore [4] proposed a neural network-based template attack that accelerates the construction of templates and makes the construction of templates more accurate.

With the continuous development of side-channel attacks, the security of cryptographic devices has been greatly tested, and a series of countermeasures have been proposed to resist side-channel attacks, of which masking technique is one of the most effective and widely used. In 1999, Chari [5] et al. proposed an S-box mask protection scheme for power analysis attacks. In 2001, Akkar [6] et al. proposed a multiplication-based masking scheme to add a multiplicative mask to the S-box inverse of the AES algorithm. In the same year, Itoh [7] et al. proposed a fixed-value mask scheme with the same random mask for each round of encryption, but the scheme is not resistant to higher-sorder attacks. In 2012, Nassar [8] et al. proposed the RSM (Rotating S-box Mask) low-entropy mask scheme, which is the focus of this paper, and a more detailed introduction can be found in Section 2.1.

At present, the attacks generally used against cryptographic algorithms implemented by add-masking are higher-order DPA attacks. After kocher et al. first proposed the concept of DPA, in 2000, for the masked cryptographic algorithm, Messages [9] refined the definition of nth-order DPA from various aspects and first proposed the concept of second-order DPA and its implementation method, taking the masked DES algorithm as an example, and confirmed the feasibility of the method through experiments. Based on these theories, more practical schemes and optimization methods have been proposed for masking strategies. 2004, Jason [10] et al. proposed their attack model and corresponding algorithm for second-order DPA, which can achieve better results when the energy traces are short and the correlation coefficients are large. 2013, Belgarric [11] et al. proposed a preprocessing method for time-frequency analysis of energy traces, which can effectively improve the attack efficiency. The method can effectively improve the attack efficiency and avoid the preprocessing of cross-combination of leaked energy sources. The method is applicable to soft encryption implementations with first-order protection.

Template attack is an energy analysis attack with learning that is also used to attack cryptographic algorithms with masking. Template attack uses known information about the training device to build an accurate noise model of the leaked information in the learning phase, thus greatly improving the efficiency of the attack. in 2006, Oswald et al [12-13] proposed the first template-based DPA attack by combining the template attack. in 2007, Lemke-Rust et al [14] proposed to use the template attack directly to mask method for encryption algorithms. This method uses a training device to

learn a comprehensive template about the leaked intermediate value and the mask, and attacks both the mask and the key of the device during the attack.In 2015, Lerman et al [15] proposed to use support vector machines to build templates about the mask and the intermediate value after demasking. In the attack using the template of the mask first attack the mask and after the demasking then attack the key. In the same year, Gilmore et al [16] proposed the same idea of attack but with a template using a neural network. The methods proposed in these studies all require the attacker to learn the random mask used by the device in each encryption during the learning phase this requirement is very demanding and is not available in all attacks.

2. Common Leakage Analysis Techniques

One of the safety-critical devices that need to be certified before going to market is the test side channel attack. This attack exploits unintentional leakage of the device, such as power consumption, electromagnetic radiation or timing, to pose a threat to the physical implementation. The certification process is expensive and time-consuming, especially when the desired level of security is increased. For example, the ISO draft standard 17825 requires resistance to side-channel analysis with 10,000 traces (level 3) and 100,000 traces (level 4). To speed up the evaluation process, a method should be used to compress a large number of traces into a small set of correlation points.

Before the template attack, feature extraction of the target energy traces is required to select the points with higher correlation for the attack, which helps to improve the efficiency of template construction as well as the accuracy of the attack. Seven main feature selection methods are described below.

2.1. SOD (Sum of Pairwise Differences)

Chair [3] proposed the SOD method in 2003 as a basic feature point selection method, which is simpler to calculate. The calculation of the SOD method is shown in Equation (1):

$$s = \sum_{j>i=1}^{N} (t_i - t_j) \tag{1}$$

t denotes the energy trace curve in the data set, N is the number of energy traces (not described subsequently), and s is the sum of the difference curves. The principle of this method is to obtain the difference curve by making a difference between two of the collected energy traces. Then, the data corresponding to the same moments on the difference curve are summed up, and the moments corresponding to the points with larger values are the locations of the feature points with higher correlation to be extracted. However, this scheme has a problem that there are positive and negative differences in the collected energy traces, which may cause some feature points to be ignored in the calculation and thus have a great impact on the selection of feature points.

2.2. SOSD (Sum of Squar-ed Pairwise Differences)

Christian et al. proposed an improved method called SOSD for the inability of SOD to better handle the positive and negative energy traces, i.e., the square operation is added to the SOD method, and the calculation is shown in Equation (2):

$$s = \sum_{j>i=1}^{N} (t_i - t_j)^2 \tag{2}$$

As in the first method, the moment of the larger value point is selected as the location for feature point selection.

2.3. SOST (Sum of Squar-ed Pairwise T-Differences)

Gierlichs [17] et al. proposed a t-test-based feature selection method SOST, which optimized the SOSD method. The details of the calculation are shown in Eqs. (3) and (4):

$$T = \frac{m_i - m_j}{\sqrt{\frac{\sigma_i^2}{N_i} + \frac{\sigma_j^2}{N_j}}} \tag{3}$$

$$s = \sum_{j>i=1}^{n} \left(\frac{m_i - m_j}{\sqrt{\frac{\sigma_i^2}{N_i} + \frac{\sigma_j^2}{N_j}}} \right)^2 \tag{4}$$

Equation (3) is the formula of T-test, and Equation (4) is the formula of SOST's feature point extraction, which is the combination of T-test and SOSD. m denotes the corresponding energy trace curve mean vector, and N denotes the number of corresponding curves. When the number of samples is small, the relative SOSD is more resistant to noise, and it is easier to find out the feature points with obvious leakage.

2.4. Pearson correlation coefficient

The Pearson correlation coefficient method can be used when the data are linearly correlated with each other and the data obey normal distribution, and the selection area of feature points can be determined by calculating the location of the points with higher correlation. The calculation is shown in Equation (5).

$$\rho(i) = \frac{Cov(t_i, v)}{\sqrt{Var(t_i) \bullet Var(v)}} \tag{5}$$

Where t denotes the vector composed of the corresponding points of i at a certain moment of the energy trace curve and v denotes the corresponding intermediate value. It can only represent the degree of correlation of the data and cannot be used for direct causal determination.

2.5. PCA (Principal Component Analysis)

Principal component analysis (PCA) is a common leakage analysis technique that is typically used to process large amounts of data to find the main patterns and features in the data. In side-channel attacks, PCA can be used to analyze the main features in energy consumption leaked data to infer the secret key. The basic idea of PCA is to transform high-dimensional data into low-dimensional data while retaining most of the information of the data. PCA obtains the principal components of the data and the corresponding eigenvalues by calculating the covariance matrix of the data and then decomposing the covariance matrix into eigenvalues. Principal components are linear combinations of the data that explain most of the variance in the data. By using principal components, the data can be mapped from a high-dimensional space to a low-dimensional space, while retaining most of the information of the data.

2.6. SNR (Signal-To-Noise Ratio)

Signal-to-noise ratio (SNR) is a common leakage analysis technique used to analyze the ratio between signal and noise in energy consumption leakage data. In side-channel attacks, SNR can be used to evaluate the quality of energy consumption leakage data and extract from it the points with high signal-to-noise ratios as the characteristic points where leakage is evident. The calculation is shown in Equation (6).

$$\mathrm{SNR} = Var\left(E\left(signal\right)\right) / E\left(Var\left(signal\right)\right) \quad (6)$$

2.7. NICV（Normalized Inter-Class Variance）

Shivam Bhasin [18] et al. in 2014 proposed a better analysis technique namely regularized inter-group variance NICV.A key advantage of NICV is that neither cloning of devices nor obtaining key information of encrypted devices in advance is required. As a univariate ANOVA F-test, NICV is relatively low computational effort, using only publicly available data such as plaintext input or ciphertext output to detect leaks, and calculating the variance as the ratio between the group mean variance and the total leak variance. The results show that NICV is related to two standard metrics, Pearson correlation coefficient and signal-to-noise ratio (SNR). NICV can be used to theoretically calculate the minimum number of tracks required for an attack to be realized. The theoretical basis of NICV is given, and some practical applications are performed on real cryptosystems.

The above common leakage analysis methods have differences and advantages and disadvantages among them, but they all basically utilize all linear leaks associated with variables to perform the analysis, and all of them are inhibited to some extent if the resistance strategy eliminates all linear leaks associated with X.We used a method based on the fitting of a Gaussian mixture distribution using the GMM-EM algorithm, using the distribution of the theoretical Hamming weight as the initial centroid of the fit, in order to achieve a fast and accurate fit.

3. Leak Analysis Solution For RSM

For existing first-order SCA attacks, Nassar et al. proposed an AES-RSM (rotating S-box) encryption scheme in 2012, which has almost the same performance and complexity as unprotected AES, and also has strong resistance to first-order DPA and CPA as well as hardware protection-based defense strategies.

3.1. AES-RSM encryption scheme

In this section, the AES-RSM masking strategy is briefly introduced theoretically, and its core lies in the construction of add-masked S-boxes, which are preconfigured and calculated as follows.

Sixteen 8-bit fixed masks of fixed order m = {0x00, 0x0f, 0x36, 0x39, 0x53, 0x5c, 0x65, 0x6a, 0x95, 0x9a, 0xa3, 0xac, 0xc6, 0xc9, 0xf0, 0xff}. The random start positions in the above order will be applied sequentially to construct the corresponding S-boxes. Fixed mask set M= {moffset, moffset+1, moffset+2, moffset+3, moffset+4, moffset+5, ..., moffset+15mod (16)}, offset is the random initial position.

The S-box as a new construction should satisfy S'j (x') =S(x)+mj+1(mod 16), x is 8-bit plaintext, $x' = x \oplus m_j$. That is, Sin is masked with addition and the value Sout after the output S-box is protected by mj+1 (mod 16).

After each round of AES calculation, the offset value is added by one, i.e., the mask area is rotated down one turn in the previous round, M={moffset+1, moffset+2, moffset+3, moffset+4, moffset+5, ...moffset+15mod(16), moffset }, Therefore, it is called a rotating S-box.

The specific encryption process is shown in the following figure.

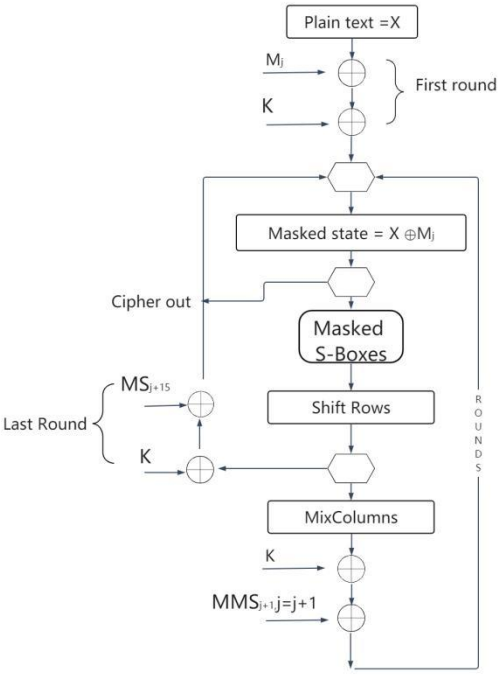

Figure 1. Encryption Flow

3.2. First-order leakage of RSM

Based on the Hamming weight model, the RSM plus mask approach appears to have no first-order leakage, but according to our experiments, it actually has leakage under other models, which is the focus of this paper, based on the difference in energy consumption distribution.

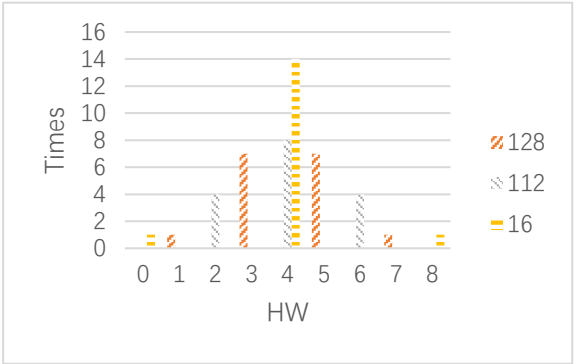

Figure 2. Frequency Distribution

The Hamming weight after each s_{out} has been heterodyned with 16 fixed masks is shown in Figure 2 above, Counter ({'{1: 1, 3: 7, 5: 7, 7: 1}': 128, '{2: 4, 4: 8, 6: 4}': 112, '{0: 1, 4: 14, 8: 1}': 16}).

Although the mean variance of a deterministic X with all masked heterogeneous post-band masked values Y is constant, so that the commonly used leakage analysis methods cannot build an effective leakage model, the distribution of Y values after different plaintexts are masked is different, and it is still possible to distinguish different Xs by the difference of

energy consumption frequency distribution through the joint attack of multiple energy traces.

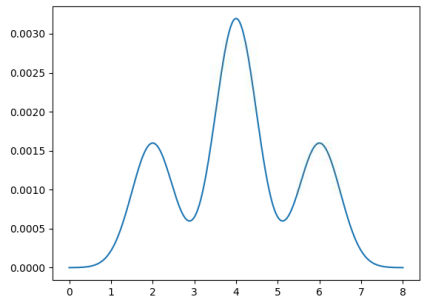

Figure 3. Gaussian mixture distribution

The numerical calculation methods of leakage metrics include methods that directly use energy consumption frequencies in groupings instead of probability distributions, methods based on kernel density estimation, and methods based on fitting Gaussian mixture distributions.

4. Experiment and Analysis

4.1. Experimental data

The experimental data are divided into real data and simulated energy traces, where the real data are used to test the effectiveness of the method. The simulated energy traces, on the other hand, have different signal-to-noise ratios and can be used to observe the tolerance of the method to noise.

4.1.1. Real Data

We measured the running process of AES128-RSM encryption algorithm executed on a smart card. The experimental equipment includes an oscilloscope, a smart encryption card, a card reader, and a computer. The computer is responsible for sending commands to the card reader to control the encryption algorithm running on the encryption card, and sending plaintext messages to the smart card via USB. At the same time, the oscilloscope is triggered to perform the energy consumption curve acquisition. The oscilloscope sends the collected energy consumption profiles to the computer, and then performs some pre-processing, resulting in the final data set. The raw energy traces include 100,000 sample points with a total of 40,000 curves.

4.1.2. Simulation of energy traces

The intermediate values to be leaked are calculated according to the encryption algorithm, and the energy consumption is summed by bit conversion bit. Finally, the leaked diverse instincts are superimposed on a base energy consumption curve afterwards. If the signal-to-noise ratio needs to be reduced, white noise with different variance values is added. 40,000 simulated energy traces each with signal-to-noise ratios of 0.9 and 0.7 were generated, of which 30,000 were used for training and 10,000 for testing.

4.2. Experimental indicators

In this paper, the custom leakage analysis method GDD (Group Distribution Difference) is used as the experimental index. The frequencies of each curve at different voltages with the same intermediate values are counted and normalized, the frequency distribution p is used instead of the probability distribution, the mean value of the frequency distribution for all intermediate values is used as the average distribution q, and the KL distance of pq is found as the size of leakage.

$$D_{KL}(p \| q) = \sum_{i=1}^{n} p(x_i) \log\left(\frac{p(x_i)}{q(x_i)}\right) \quad (7)$$

4.3. Experiments on simulated energy traces

4.3.1. Use of common leak analysis methods

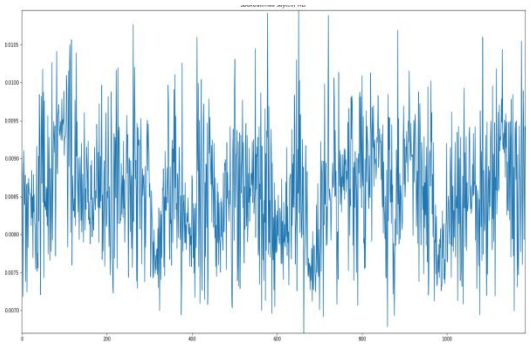

Figure 4. Leakage analysis of SNR on simulated energy traces

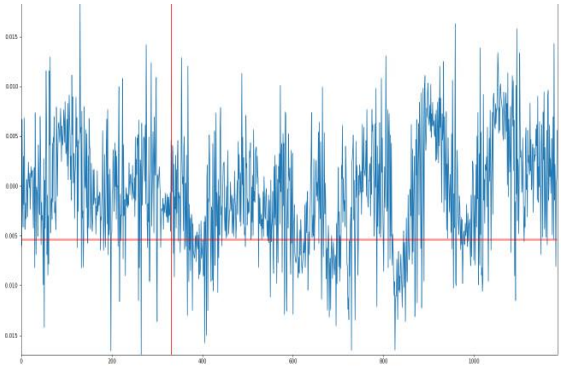

Figure 5. Leakage analysis of NICV on simulated energy traces

As can be seen from Figures 4,5 above, ordinary leakage analysis methods do not reflect the leakage situation.

4.3.2. Using GDD

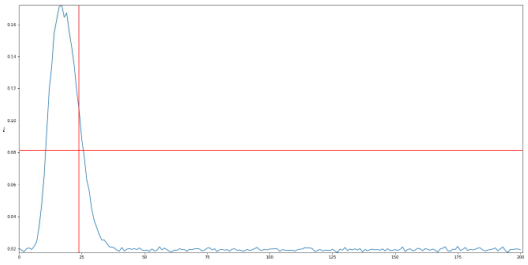

Figure 6. GDD's analysis of 0.9

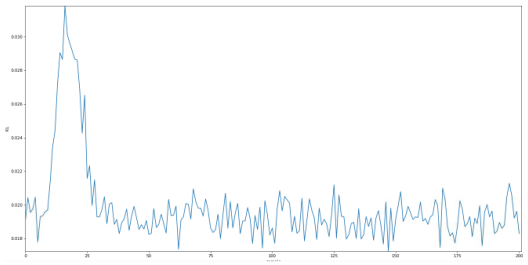

Figure 7. GDD's analysis of 0.7

According to the above figure 6,7, we can see that the leakage analysis using GDD can find the leakage points of the energy consumption curve. However, when the intensity of the noise increases, the value of the leakage indicator will become smaller. When the noise reaches a certain level, the leakage indicator may become invalid.

4.4. Experiments on real energy traces

Leakage analysis of real energy traces using GDD results in the following figure.

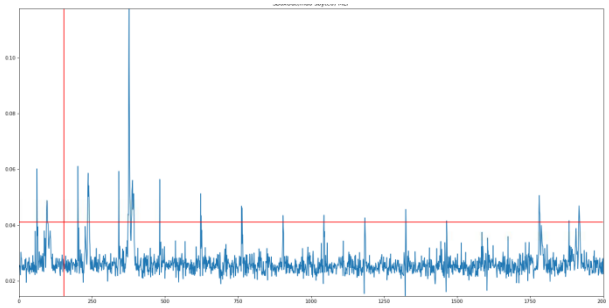

Figure 8. GDD's analysis of real trace

As can be seen in Figure 8 above, there are significant spikes at certain locations in the curve, which means that there may be significant leakage at these locations. By using the leakage analysis metrics, we can use MLP to train on these points where there is significant leakage, so that we can quickly and efficiently complete the training of the model and implement the attack. The specific effect of the attack is as follows.

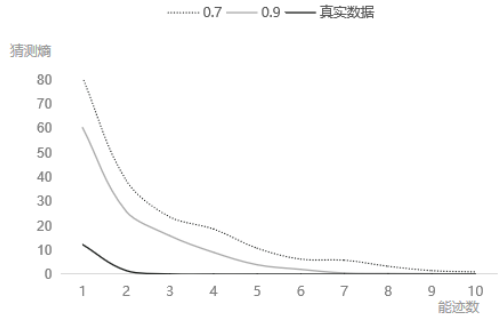

Figure 9. The effect of the attack after the leakage of different data with GDD

From the figure 9, we can see that the noise still has some influence on the final attack effect, the larger the noise, the worse the attack effect, but still can train an effective model. The attack effect on real data is better, and only 4 energy traces are needed to achieve the attack.

5. Conclusion

In this study, we explored the use of energy consumption frequency distribution to implement a method for leakage analysis in side channel attacks and verified the effectiveness of the method through experiments. By using GDD, we were able to identify the location of the leaks implemented by the cryptographic algorithm, and then attack the algorithm and complete the training of the model. In addition, we also explored the effect of noise on the leakage analysis results, and although noise has some influence on the results, it still has good results in real data. The contribution of this study is to provide an effective method to identify and solve the leakage problem of cryptographic algorithm implementations in side channel attacks, which is important to protect the security of cryptographic algorithms. In the future, we can further explore how to combine GDD with other methods to further improve the accuracy and practicality of the attack algorithm. We believe that the results of this study will have a positive impact on the development of the information security field.

Acknowledgment

This work was supported in part by the Sichuan Science and Technology Program (No. 2021ZYD0011)

References

[1] Kocher P C. Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems[C]//Advances in Cryptology—CRYPTO'96: 16th Annual International Cryptology Conference Santa Barbara, California, USA August 18–22, 1996 Proceedings 16. Springer Berlin Heidelberg, 1996: 104-113.

[2] Kocher P, Jaffe J, Jun B. Differential power analysis[C]//Advances in Cryptology—CRYPTO'99: 19th Annual International Cryptology Conference Santa Barbara, California, USA, August 15–19, 1999 Proceedings 19. Springer Berlin Heidelberg, 1999: 388-397.

[3] Chari S, Rao J R, Rohatgi P. Template attacks[C]//Cryptographic Hardware and Embedded Systems-CHES 2002: 4th International Workshop Redwood Shores, CA, USA, August 13–15, 2002 Revised Papers 4. Springer Berlin Heidelberg, 2003: 13-28.

[4] Gilmore R, Hanley N, O'Neill M. Neural network based attack on a masked implementation of AES[C]//2015 IEEE International Symposium on Hardware Oriented Security and Trust (HOST). IEEE, 2015: 106-111.

[5] Chari S, Jutla C S, Rao J R, et al. Towards sound approaches to counteract power-analysis attacks[C]//Advances in Cryptology—CRYPTO'99: 19th Annual International Cryptology Conference Santa Barbara, California, USA, August 15–19, 1999 Proceedings 19. Springer Berlin Heidelberg, 1999: 398-412.

[6] Akkar M L, Giraud C. An implementation of DES and AES, secure against some attacks[C]//Cryptographic Hardware and Embedded Systems—CHES 2001: Third International Workshop Paris, France, May 14–16, 2001 Proceedings 3. Springer Berlin Heidelberg, 2001: 309-318.H. Poor, An Introduction to Signal Detection and Estimation. New York: Springer-Verlag, 1985, ch. 4.

[7] Itoh K, Takenaka M, Torii N. DPA countermeasure based on the "masking method"[C]//Information Security and Cryptology—ICISC 2001: 4th International Conference Seoul, Korea, December 6–7, 2001 Proceedings 4. Springer Berlin Heidelberg, 2002: 440-456.

[8] Nassar M, Souissi Y, Guilley S, et al. RSM: A small and fast countermeasure for AES, secure against 1st and 2nd-order zero-offset SCAs[C]//2012 Design, Automation & Test in Europe Conference & Exhibition (DATE). IEEE, 2012: 1173-1178.

[9] Messerges T S. Using second-order power analysis to attack DPA resistant software[C]//Cryptographic Hardware and Embedded Systems—CHES 2000: Second International Workshop Worcester, MA, USA, August 17–18, 2000 Proceedings. Berlin, Heidelberg: Springer Berlin Heidelberg, 2002: 238-251.

[10] Waddle J, Wagner D. Towards efficient second-order power analysis[C]//Cryptographic Hardware and Embedded Systems-CHES 2004: 6th International Workshop Cambridge, MA, USA, August 11-13, 2004. Proceedings 6. Springer Berlin Heidelberg, 2004: 1-15.

[11] Belgarric P, Bhasin S, Bruneau N, et al. Time-frequency analysis for second-order attacks[C]//Smart Card Research and Advanced Applications: 12th International Conference, CARDIS 2013, Berlin, Germany, November 27-29, 2013. Revised Selected Papers 12. Springer International Publishing, 2014: 108-122.

[12] Oswald E, Mangard S, Herbst C, et al. Practical second-order DPA attacks for masked smart card implementations of block ciphers[C]//Topics in Cryptology–CT-RSA 2006: The Cryptographers' Track at the RSA Conference 2006, San Jose, CA, USA, February 13-17, 2005. Proceedings. Springer Berlin Heidelberg, 2006: 192-207.

[13] Oswald E, Mangard S. Template attacks on masking—resistance is futile[C]//Topics in Cryptology–CT-RSA 2007: The Cryptographers' Track at the RSA Conference 2007, San Francisco, CA, USA, February 5-9, 2007. Proceedings. Springer Berlin Heidelberg, 2006: 243-256.

[14] Lemke-Rust K, Paar C. Gaussian mixture models for higher-order side channel analysis[C]//Cryptographic Hardware and Embedded Systems-CHES 2007: 9th International Workshop, Vienna, Austria, September 10-13, 2007. Proceedings 9. Springer Berlin Heidelberg, 2007: 14-27.

[15] Lerman L, Bontempi G, Markowitch O. A machine learning approach against a masked AES: Reaching the limit of side-channel attacks with a learning model[J]. Journal of Cryptographic Engineering, 2015, 5: 123-139.

[16] Gilmore R, Hanley N, O'Neill M. Neural network based attack on a masked implementation of AES[C]//2015 IEEE International Symposium on Hardware Oriented Security and Trust (HOST). IEEE, 2015: 106-111.

[17] Gierlichs B, Lemke-Rust K, Paar C. Templates vs. stochastic methods: A performance analysis for side channel cryptanalysis[C]//Cryptographic Hardware and Embedded Systems-CHES 2006: 8th International Workshop, Yokohama, Japan, October 10-13, 2006. Proceedings 8. Springer Berlin Heidelberg, 2006: 15-29.

[18] JBhasin S, Danger J L, Guilley S, et al. NICV: normalized inter-class variance for detection of side-channel leakage[C]//2014 International Symposium on Electromagnetic Compatibility, Tokyo. IEEE, 2014: 310-313.