Evaluation of Information Leakage of Cryptographic Chip Based on Variance

Dongyao Zhang, Changlin Zhou, Shuang Li,
Daojie Yu, and Kai He

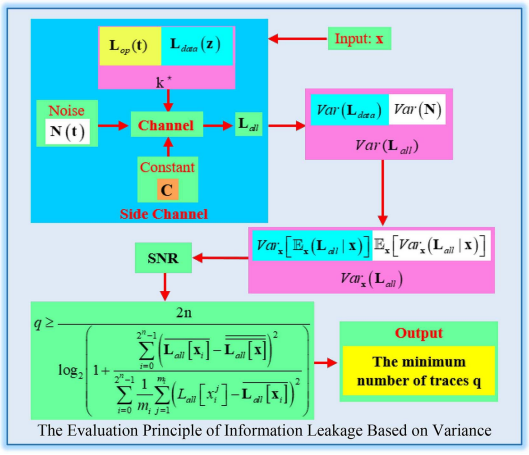
***Abstract*—The cryptographic chip in system must be evaluated for side channel leakage detection before coming into service. However, the existing evaluation technology is too inefficient. This letter decomposes the variance of the traces of power consumption into variance of the sensitive variable and noise to estimate the signal-to-noise (SNR). According to the relationship between the success rate (SR) of the power analysis attack, SNR and conditional mutual information, the minimum number of traces is computable to evaluate the information leakage of the cryptographic chip. This method effectively estimates the minimum number of power traces when the SNR of power consumption is greater than 0.1. When the SNR is less than 0.1, the result calculated by this method is consistent with the change trend of the simulation, which means that the result also evaluates the ability of cryptographic chip to resist power analysis attacks. The method improves the evaluation efficiency by at least 60000 times compared with the simulation of CPA.**

***Index Terms*—Evaluation of information leakage, power analysis attack, conditional mutual information, information security.**

I. Introduction

With the rapid development of information technology, the issues of information security have become increasingly complex and severe. As the core security hardware device in the system, the cryptographic chip is the key unit to achieve information security [1]. As a commonly used encryption algorithm for embedded devices, although the mathematical safe of Advanced Encryption Standard (AES) is provable, adversaries could obtain sensitive information from side channels (such as sound, light, electromagnetic and power consumption) to reduce the key chunk search space combining the information about sensitive variable with the knowledge of the plaintext or ciphertext. By repeating this attack several times, each byte of the secret key separately is recovered thanks to a divide-and-conquer strategy [2]. They could reveal the secret of the AES-128 implementation with only $1,000 cheap equipment [3]. The leakage from side channel has seriously threatened the information security of embedded devices. Therefore, these cryptographic chips must be evaluated for side channel leakage before large-scale commercial use of them.

In present, many papers about the evaluation of information leakage have been put forward. Reference [4] uses SNR to estimate the minimum number of traces according to the sampling distribution of correlation coefficient. Reference [5] uses the sum of difference (SOD) of traces to identify and select the interesting points of traces. Two further improvements are then proposed by Gierlichs *et al.* [6]. The first improvement, called as sum of squared pairwise differences (SOSD), avoids cancellation of positive and negative differences. The second improvement, called as sum of squared pairwise T-differences (SOST), normalizes SOSD by some variance. Normalized Inter-class Variance (NICV) is proposed to estimate the maximum correlation coefficient between sensitive variable and leakage trace [7]. Mutual Information (MI) is introduced to evaluate the information leakage of cryptographic chips by Gierlichs *et al.* [8]. Perceived Information (PI) is proposed to quantify leakage of chips [9]. Those side channel evaluation techniques above



The Evaluation Principle of Information Leakage Based on Variance

Take-Home Messages:

- From the perspective of variance, this paper concludes that the variance of power consumption is mainly composed of the variance of the sensitive variable and the variance of the noise, which correspond to signal and noise respectively.
- The variance of the sensitive variable is equal to the interclass variance, and the variance of the noise is equal to the intraclass variance. The ratio of the interclass variance to the intraclass variance is SNR.
- The conditional mutual information reaches the maximum value n when success rate is equal to 1.
- The evaluator only needs to measure a certain number of traces to estimate the minimum number of traces required for a successful attack.

Manuscript received July 21, 2020; revised October 30, 2020; accepted December 7, 2020. Date of publication December 15, 2020; date of current version January 18, 2021. This work was supported in part by the National Natural Science Foundation of China under Project 61871405. *(Corresponding author: Dongyao Zhang.)*

The authors are with the School of Systems Engineering, Strategic Support Force Information Engineering University, Zhengzhou 450001, China (e-mail: zdy.01@foxmail.com).

Digital Object Identifier 10.1109/LEMCPA.2020.3044212

all are divided into parameter estimation methods and non-parametric estimation methods. The parameter estimation methods assume that the leakage follows a normal distribution when the number of power traces is large enough according to the central limit theorem [4]–[7]. Those methods become increasingly time-consuming and laborious as the number of power traces increases. The non-parametric estimation methods assume the leakage follows a special distribution. Evaluate efficiency of those methods is faster, but the error is larger.

This letter decomposes the variance of the traces of power consumption into the variance from the sensitive variable and the variance from noise to estimate the SNR of side channel. According to the estimated value of SNR, the upper bound of the conditional mutual information between the all power consumption and the power consumption from the sensitive variable for the given plaintext is also computable, which is related to the minimum number of traces required to perform a successful attack. Evaluators use the minimum number of traces to evaluate the information leakage of the encryption chip. This method improves the efficiency of evaluation, which is verified by the simulation.

This letter is organized as follows. Section II describes the variance of traces and the estimation of SNR. The evaluation of side-channel leakage is introduced in Section III. The result is verified by the simulation in Section IV. We summarize this letter in Section V.

II. Power Analysis

A. Mathematical Model of Power Consumption

The attacked target of a cryptographic primitive $\mathbf{F}$ is the sensitive variable $\mathbf{z} = \mathbf{F}(\mathbf{x}, \mathbf{k}, \mathbf{t})$, where $\mathbf{x} \in (0, 2^n - 1)$ denotes some public variable (e.g., plaintext or ciphertext), $\mathbf{k} \in (0, 2^n - 1)$ denotes the part of secret key the attacker aims to retrieve, and $\mathbf{t}$ denotes time series of execution of encryption algorithm or sampling time series. Among all the possible value $\mathbf{k}$ may take, $k^\star$ refers to the right key hypothesis. The power consumption $\mathbf{L}_{all}(\mathbf{x}, \mathbf{t})$ from cryptographic chips includes the operation-dependent component $\mathbf{L}_{op}(\mathbf{t})$ consumed by the execution of instructions, the data-dependent component $\mathbf{L}_{data}(\mathbf{z})$ from the target sensitive data variable $\mathbf{z}(\mathbf{x}, k^\star, \mathbf{t})$, the inherent noise $\mathbf{N}(\mathbf{t})$ of the electronic system and the fixed power consumption $\mathbf{C}$. So the power consumption satisfies formula (1), when using the secret $k^\star$ to encrypt the plaintext $\mathbf{x}$.

$$\mathbf{L}_{all}(\mathbf{x}, \mathbf{t}) = \mathbf{L}_{op}(\mathbf{t}) + \mathbf{L}_{data}(z) + \mathbf{N}(t) + \mathbf{C} \tag{1}$$

B. Variance of Power Consumption

According to formula (1), the total variance of the power trace consists of 4 parts as shown in formula (2), where *Var* refers to the variance.

$$Var(\mathbf{L}_{all}) = Var\big(\mathbf{L}_{op}\big) + Var(\mathbf{L}_{data}) + Var(\mathbf{N}) + Var(\mathbf{C}) \tag{2}$$

$Var_{\mathbf{x}}(\mathbf{L}_{op})$ is equal to 0, because $\mathbf{L}_{op}$ has nothing to do with plaintext $\mathbf{x}$. Because $\mathbf{C}$ is constant, $Var(\mathbf{C})$ is also equal to 0. So, the variance of power consumption is mainly composed of the variance of the sensitive variable and the variance of the noise, as shown formula (3).

$$Var(\mathbf{L}_{all}) = Var(\mathbf{L}_{data}) + Var(\mathbf{N}) \tag{3}$$

According to variance decomposition formula, the total variance is decomposed into intraclass variance $Var_{\mathbf{x}}[\mathbb{E}(\mathbf{L}_{all}|\mathbf{x})]$ and interclass variance as shown (4), where $\mathbb{E}$ refers to the mean.

$$Var_{\mathbf{x}}(\mathbf{L}_{all}) = Var_{\mathbf{x}}[\mathbb{E}_{\mathbf{x}}(\mathbf{L}_{all}|\mathbf{x})] + \mathbb{E}_{\mathbf{x}}[Var_{\mathbf{x}}(\mathbf{L}_{all}|\mathbf{x})] \tag{4}$$

putting (3) into $Var_{\boldsymbol{x}}(\mathbf{L}_{all}(\mathbf{x}, \mathbf{t})\mathbf{x})$, we get

$$Var_{\mathbf{x}}[\mathbf{L}_{all}|\mathbf{x}] = Var_{\mathbf{x}}[\mathbf{L}_{data}|\mathbf{x}] + Var_{\mathbf{x}}[\mathbf{N}|\mathbf{x}] \tag{5}$$

When $\mathbf{x}$ is known, $\mathbf{L}_{data}$ is a certain value, and the conditional variance$\mathrm{Var}_{\mathbf{x}}[\mathbf{L}_{data}|\mathbf{x}]$ is equal to 0. Then:

$$\mathbb{E}_{\mathbf{x}}(\mathrm{Var}_{\mathbf{x}}[\mathbf{L}_{all}|\mathbf{x}]) = \mathrm{Var}(\mathbf{N}) \tag{6}$$

According to (6), the intraclass variance $Var_{\mathbf{x}}[\mathbb{E}_{\mathbf{x}}(\mathbf{L}_{all}|\mathbf{x})]$ is equal to the noise variance $Var_{\mathbf{x}}x(\mathbf{N})$. The estimation of the noise variance is calculated by estimating intraclass variance as shown (7), where $\mathbf{L}_{all}[x_i^j]$ is the power consumption of the j-th encryption of plaintext x_i, $\overline{\mathbf{L}_{all}[\mathbf{x}_i]}$ refers to the average power consumption corresponding to the plaintext x_i, and m_i is the times that the plaintext x_i is encrypted.

$$\begin{aligned}\widehat{Var}(\mathbf{N}) &= \widehat{\mathbb{E}}_{\mathbf{x}}(\mathrm{Var}_{\mathbf{x}}[\mathbf{L}_{data}|\mathbf{x}]) \\ &= \frac{1}{2^n}\sum_{i=0}^{2^n-1}\frac{1}{m_i}\sum_{j=1}^{m_i}\Big(\mathbf{L}_{all}\Big[x_i^j\Big] - \overline{\mathbf{L}_{all}[\mathbf{x}_i]}\Big)^2\end{aligned} \tag{7}$$

Combining (3), (4) and (6), We obtain (8).

$$Var_{\mathbf{x}}[\mathbb{E}_{\mathbf{x}}(\mathbf{L}_{all}|\mathbf{x})] = Var_{\mathbf{x}}(\mathbf{L}_{data}) \tag{8}$$

According to (8), the interclass variance $Var_{\mathbf{x}}[\mathbb{E}_{\mathbf{x}}(\mathbf{L}_{all}|\mathbf{x})]$ is equal to the variance of the sensitive variable $Var_{\mathbf{x}}(\mathbf{L}_{data})$. The estimation of the data-dependent variance is calculated by estimating interclass variance as shown (9), Where $\overline{\overline{\mathbf{L}_{all}}}$ refers to the means of all power consumption.

$$\begin{aligned}\widehat{\mathrm{Var}}_{\mathbf{x}}[\mathbf{L}_{data}] &= \widehat{\mathrm{Var}}_{\mathbf{x}}[\mathbb{E}_{\mathbf{x}}(\mathbf{L}_{all}|x)] \\ &= \frac{1}{2^n}\sum_{i=0}^{2^n-1}\Big(\overline{\mathbf{L}_{all}[\mathbf{x}_i]} - \overline{\overline{\mathbf{L}_{all}}}\Big)^2\end{aligned} \tag{9}$$

Combining (8) and (9), We obtain (10).

$$\widehat{SNR} = \frac{\widehat{\mathrm{Var}}_{\mathbf{x}}(\mathbf{L}_{data})}{\widehat{\mathrm{Var}}(\mathbf{N})} = \frac{\sum_{i=0}^{2^n-1}\Big(\overline{\mathbf{L}_{all}[\mathbf{x}_i]} - \overline{\overline{\mathbf{L}_{all}}}\Big)^2}{\sum_{i=0}^{2^n-1}\frac{1}{m_i}\sum_{j=1}^{m_i}\Big(\mathbf{L}_{all}\Big[x_i^j\Big] - \overline{\mathbf{L}_{all}[\mathbf{x}_i]}\Big)^2} \tag{10}$$

According to (10), we estimate the SNR of the side channel by measuring the power consumption of the cryptographic chip.

III. Evaluation of Side Channel Leakage

A. Threshold of Leaked Information

This letter treats side channel as communication channel and uses mutual information theory to evaluate the leakage. The average conditional mutual information $\mathbf{I}(\mathbf{L}_{all}; \mathbf{L}_{\mathrm{data}}|\mathbf{x})$ between the all power consumption and the leakage of sensitive variable refers to the reduction in uncertainty of $\mathbf{L}_{data}$ due to the knowledge of $\mathbf{L}_{all}$ when x is known.

According to [10], the relationship between conditional mutual information and success rate of an attack is

$$n - \big(1 - \mathbb{P}_{\mathrm{sr,t}}(\mathbf{k})\log_2(2^n - 1) - H_2\big(\mathbb{P}_{\mathrm{sr,t}}(\mathbf{k})\big)\big) \le \mathbf{I}(\mathbf{L}_{all}; \mathbf{L}_{data}|\mathbf{x}), \tag{11}$$

where $\mathbb{P}_{sr,t}(\mathbf{k})$ refers to the success rate, and $H_2(\mathbb{P}_{sr,t}(\mathbf{k}))$ is its binary entropy

$$\begin{aligned}H_2\big(\mathbb{P}_{\mathrm{sr,t}}(\mathbf{k})\big) = &-\big(1 - \mathbb{P}_{\mathrm{sr,t}}(\mathbf{k})\big)\log_2\big(1 - \mathbb{P}_{\mathrm{sr,t}}(\mathbf{k})\big) \\ &- \mathbb{P}_{\mathrm{sr,t}}(\mathbf{k})\log_2\big(\mathbb{P}_{\mathrm{sr,t}}(\mathbf{k})\big).\end{aligned} \tag{12}$$

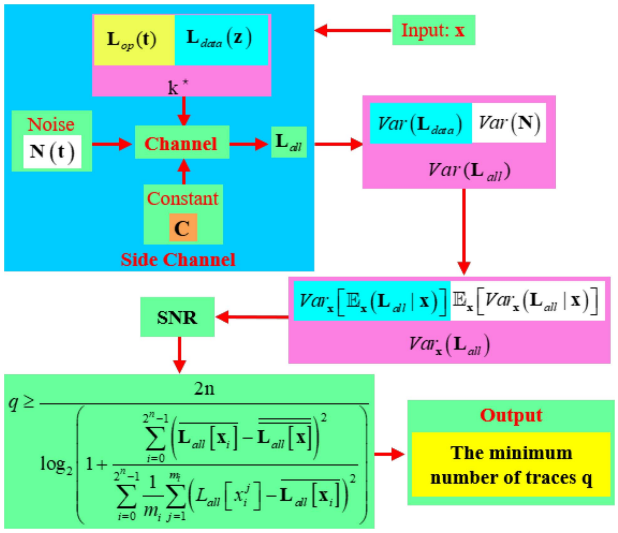


Fig. 1. The evaluation principle of information leakage based on variance.

When success rate is equal to 1, formula (11) is rewritten as

$$\mathbf{I}(\mathbf{L}_{all};\mathbf{L}_{data}|\mathbf{x}) \geq n. \tag{13}$$

Due to

$$\mathbf{I}(\mathbf{L}_{all};\mathbf{L}_{data}|\mathbf{x}) \leq \mathbf{I}(\mathbf{L}_{all};\mathbf{L}_{data}) \leq n, \tag{14}$$

the conditional mutual information is equal to n when the attack is successful.

$$\mathbf{I}(\mathbf{L}_{all};\mathbf{L}_{data}|\mathbf{x}) = n \tag{15}$$

Formula (15) shows that the leakage information from side channel reaches the maximum value when success rate is equal to 1.

B. The Minimum Number of Traces

Because the side channel is memoryless, the conditional mutual information satisfies (16), where $\mathcal{C}$ refers to the Shannon channel capacity of the side channel.

$$\mathbf{I}(\mathbf{L}_{all};\mathbf{L}_{data}|\mathbf{x}) \leq \sum_{\mathrm{i}=0}^{q} I(L_{all};L_{data}|x_i) = q\cdot\mathcal{C} \tag{16}$$

Formula (17) is obtain according to the Shannon channel capacity.

$$\mathcal{C} = \frac{1}{2}\log_2(1+SNR) \tag{17}$$

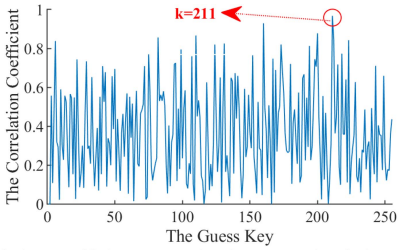
Combining (10), (15), (16) and (17), the minimum number of power traces is calculated according to formula (18).

$$q \geq \frac{2n}{\log_2\left(1+\frac{\sum_{i=0}^{2^n-1}\left(\overline{\mathbf{L}_{all}[\mathbf{x}_i]}-\overline{\mathbf{L}_{all}[\mathbf{x}]}\right)^2}{\sum_{i=0}^{2^n-1}\frac{1}{m_i}\sum_{j=1}^{m_i}\left(\mathbf{L}_{all}[x_i^j]-\overline{\mathbf{L}_{all}[\mathbf{x}_i]}\right)^2}\right)} \tag{18}$$

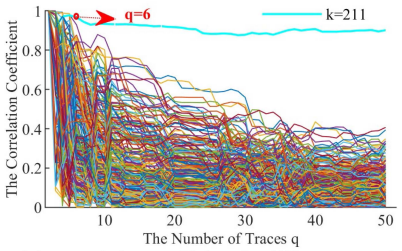
The evaluator only needs to measure a certain number of traces to estimate the minimum number of traces required for a successful attack, which is treated as an indicator to evaluate the ability of cryptographic chips to resist side-channel attacks. The specific principle of evaluation of information leakage is shown in Fig. 1. This method improves the efficiency of evaluation. For example, when the means of CPA is used, we need to calculate repeatedly the correlation coefficient between power traces and sensitive intermediate variables corresponding to each candidate secret (2^n candidate secrets) until the correct key is distinguished, which is becoming more time-consuming and laborious as the number of traces are increasing. Our method does not need to calculate the correlation coefficient repeatedly, which takes much less time.

TABLE I
THE SPECIFIC PARAMETERS FOR SIMULATION

t	$\mathbf{L}_{op}(\mathbf{t})$+C	σ_t^2	$Var_{\mathbf{x}}[H_W(\mathbf{z})]$	SNR
1	-2057	0.5302	2.6545	5.0069
2	1999	11.5693	2.3809	0.2058
3	-1497	14.0681	2.3022	0.1636
4	-6420	3.0709	1.8634	0.6068
5	-2964	8.4709	2.2909	0.2704
6	-3222	0.1427	2.1778	15.2648
7	-3136	2.6422	2.2395	0.8476
8	2728	12.7389	2.3629	0.1855
9	4886	12.2820	1.9744	0.1608
10	-5631	10.4315	2.1437	0.1858



(a) The correlation coefficients occurring in a CPA simulation using the HW model to attack an S-box output in the first round when the number of traces is equal to 6.



(b) Evolution of the correlation coefficient for different guess key over an increasing number of traces. Key hypothesis 211 is plotted with a bold blue curve.

Fig. 2. Partial Results of the Simulation.

IV. SIMULATION VERIFICATION

A. Settings of the Simulation

This letter simulate the leakages from a n = 8 bits sensitive variable to verify the method above. It is assumed that the leakage function of sensitive variables is the Hamming weight function H_W. The traces are defined such that for every $\mathbf{t} = (1,\ldots,10)$, $\mathbf{x} = (0,\ldots,255)$

$$\mathbf{L}_{all}(\mathbf{x},\mathbf{t}) = \mathbf{L}_{\mathrm{op}}(\mathbf{t}) + H_W\big(\mathbf{z}(\mathbf{x},k^{\star},\mathbf{t})\big) + \mathbf{N}(\mathbf{t}) + \mathbf{C}, \tag{19}$$

where $\mathbf{z}(\mathbf{x},k^{\star},\mathbf{t})$ refers to the outputs of the ten rounds of SubBytes in AES algorithm, $\mathbf{N}(\mathbf{t})$ follows normal distribution $\mathcal{N}(0,\acute{o}_t^2)$, and the real key is equal to 211. The specific parameters are shown in Table I.

B. Comparison Estimation and Simulation

We repeat the CPA simulation 500 times for each set of parameters to ensure the reliability of the results. The partial results are shown in Fig. 2. The correlation coefficient $\tilde{n}(H_W(\mathbf{z}),\mathbf{L}_{all})$ along the y-axis characterizes the linear correlation between the leakage power traces and the

TABLE II
TIME-CONSUMING COMPARISON BETWEEN CPA AND OUR METHOD

t	1	2	3	4	5	6	7	8	9	10
CPA (s)	68.61	493.03	643.12	239.18	369.63	55.15	158.49	566.67	648.25	534.73
Our method (ms)	1.08	1.10	1.29	1.05	1.16	0.90	1.00	1.10	1.12	1.09

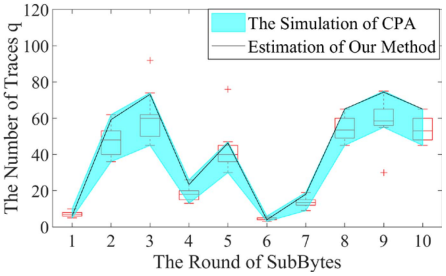


Fig. 3. Comparison Estimation and Simulation. The red boxplot shows the distributions of the minimum numbers of traces required to conduct 500 CPA simulations. The red crosses refer to outliers of the boxplot. The blue area indicates the reasonable distribution range of the boxplot. The black curve represents the minimum numbers of traces estimated by our method.

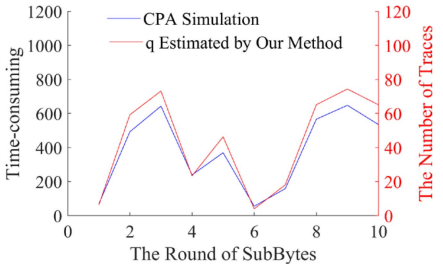


Fig. 4. Relationship between the time-consuming of CPA and the minimum number of traces estimated by our method. The blue curve shows the time-consuming of CPA simulation, and the red curve refers to the minimum number of traces estimated by our method.

Hamming weight of the sensitive variables depending to the input plaintext and the guess key. Fig. 2(a) shows the correlation coefficient is the largest when the guessed key is equal to the real key. Fig. 2(b) reveals that the correct key hypothesis is distinguished from the incorrect key hypotheses when the number of traces is greater than 6.

Fig. 3 shows the comparison between estimation and simulation. The probability of outliers from box-and-whisker plot is particularly small, showing the reliability of the experimental results. The estimated values are all within the range of the CPA simulation results, which proves the correctness of our method.

The Table II shows the time-consuming comparison, which shows that our method improves the efficiency of the evaluation by at least 60000 times compared with the simulation of CPA. Fig. 4 shows the comparison between the time-consuming of CPA simulation and the minimum number of traces estimated by our method. There is an interesting phenomenon that they are linearly related, which indirectly proves the correctness of our method because the time-consuming of CPA simulation is proportional to the number of traces required to perform CPA simulation.

To study the influence of the SNR on the experimental results, 500 CPA simulations are conducted on the S-box output of the first round at different SNR respectively. The results are shown in Fig. 5. When the SNR is greater than 0.1, the red curves are all inside the red boxplot, and our method is dependable. However, when the SNR is less than 0.1, the deviation between estimation and the CPA simulation

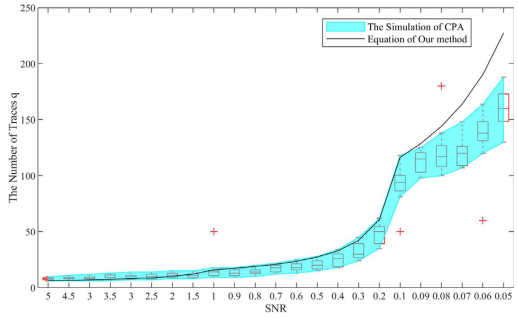


Fig. 5. Evolution of the minimum number of traces over an increasing SNR.

begins to appear, which becomes larger as the SNR decreases. However, the result calculated by this method is consistent with the change trend of the simulation, which means that the result also evaluates the ability of cryptographic chip to resist power analysis attacks.

V. CONCLUSION

From the perspective of variance, this letter concludes that the variance of power consumption is mainly composed of the variance of the sensitive variable and the variance of the noise, which correspond to signal and noise respectively. The variance of the sensitive variable is equal to the interclass variance, and the variance of the noise is equal to the intraclass variance. The ratio of the interclass variance to the intraclass variance is SNR. According to the relationship between the success rate (SR) of the power analysis attack, SNR and conditional mutual information, the minimum number of traces is computable to evaluate the information leakage of the cryptographic chip. The method improves the evaluation efficiency.

REFERENCES

[1] L. Zhang, D. Mu, W. Hu, and Y. Tai, "Machine-learning-based side-channel leakage detection in electronic system-level synthesis," *IEEE Netw.*, vol. 34, no. 3, pp. 44–49, May/Jun. 2020.
[2] L. Masure, C. Dumas, and E. Prouff, "A comprehensive study of deep learning for side-channel analysis," *IACR Trans. Cryptogr. Hardw. Embedded Syst.*, vol. 2020, no. 1, pp. 348–375, 2019.
[3] A. Wang, J. Ge, N. Shang, F. Zhang, and G. S. Zhang, "Practical cases of side-channel analysis," *J. Cryptol. Res.*, vol. 5, no. 4, pp. 383–398, 2018.
[4] S. Mangard, *Hardware Countermeasures Against DPA—A Statistical Analysis of Their Effectiveness*. Berlin, Germany: Springer, 2004, pp. 222–235.
[5] S. Chari, J. R. Rao, and P. Rohatgi, "Template attacks," in *Proc. Cryptogr. Hardw. Embedded Syst.*, 2002, pp. 13–28.
[6] B. Gierlichs, K. Lemke-Rust, and C. Paar, "Templates vs. Stochastic methods," in *Proc. Cryptogr. Hardw. Embedded Syst.*, 2006, pp. 15–29.
[7] S. Bhasin, J.-L. Danger, S. Guilley, and Z. Najm, "Side-channel leakage and trace compression using normalized inter-class variance," in *Proc. 3rd Workshop Hardw. Archit. Support Security Privacy*, Minneapolis, MN, USA, 2014, p. 7.
[8] B. Gierlichs, L. Batina, P. Tuyls, and B. Preneel, "Mutual information analysis," in *Proc. Cryptogr. Hardw. Embedded Syst.*, 2008, pp. 426–442.
[9] F. Durvaux, F.-X. Standaert, and N. Veyrat-Charvillon, *How to Certify the Leakage of a Chip?* Berlin, Germany: Springer, 2014, pp. 459–476.
[10] E. de Chérisey, S. Guilley, O. Rioul, and P. Piantanida, "Best information is most successful: Mutual information and success rate in side-channel analysis," *IACR Trans. Cryptogr. Hardw. Embedded Syst.*, vol. 2019, no. 2, pp. 49–79, 2019.