Hindawi
Security and Communication Networks
Volume 2017, Article ID 5098626, 8 pages
https://doi.org/10.1155/2017/5098626

Research Article

RFA: *R*-Squared Fitting Analysis Model for Power Attack

An Wang,[1,2] Yu Zhang,[1] Liehuang Zhu,[1] Weina Tian,[3] Rixin Xu,[1] and Guoshuang Zhang[4]

[1]*The School of Computer Science, Beijing Institute of Technology, Beijing 100081, China*
[2]*State Key Laboratory of Cryptology, P.O. Box 5159, Beijing 100878, China*
[3]*The College of Bioengineering, Beijing Polytechnic, Beijing 100176, China*
[4]*The Science and Technology on Information Assurance Laboratory, Beijing 100072, China*

Correspondence should be addressed to Liehuang Zhu; liehuangz@bit.edu.cn

Received 4 January 2017; Accepted 27 February 2017; Published 18 April 2017

Academic Editor: Xiaojiang Du

Correlation Power Analysis (CPA) introduced by Brier et al. in 2004 is an important method in the side-channel attack and it enables the attacker to use less cost to derive secret or private keys with efficiency over the last decade. In this paper, we propose *R*-squared fitting model analysis (RFA) which is more appropriate for nonlinear correlation analysis. This model can also be applied to other side-channel methods such as second-order CPA and collision-correlation power attack. Our experiments show that the RFA-based attacks bring significant advantages in both time complexity and success rate.

1. Introduction

With the development of information technology, information security plays an important role in medical system [1, 2], communications [3], finance [4], and other fields. Side-channel analysis [5, 6] which focuses on exploiting the implementation or some measurable nonmathematical property of a cryptographic system, was introduced by Kocher et al. in 1996. It marks the outbreak of this new research field in the applied cryptography area, so it has advanced quickly such as power analysis [7, 8] and electromagnetic analysis [9–11] in recent two decades. At the same time, many relational techniques have been published which can easily get the secret key by the information leakage.

When using statistical methods to analyze encryption devices, there are several common methods which can be observed. The first one is differential power analysis [5] which was introduced by Kocher. Another is Correlation Power Analysis (CPA) which is introduced by Brier et al. in 2004 [12]. CPA is more efficient than others as it significantly reduces the quantities of the power traces needed for recovering the secret key. Therefore, there are lots of researches in this field.

CPA uses two main models for relating the instantaneous power consumption and the data being manipulated. One is Hamming weight model and the other is Hamming distance model [12]. Then the correct key will be got by calculating the relationship between the changes of the specific register and the power consumption with Pearson's Correlation Coefficient (PCC). Because of the efficiency and operability of CPA, it has been widely studied and applied on various cryptographic algorithms, such as DES and AES.

In 2008, Gierlichs et al. proposed mutual information analysis which used information theory to develop a powerful attack without any device characterization [13]. With the development of artificial intelligence technology, differential cluster analysis was introduced in 2009 [14]. This technique could use cluster analysis to detect internal collisions and it combines features from previously known collision attacks and differential power analysis. In 2013, a new second-order side-channel attack based on linear regression was proposed by Dabosville et al. [15]. The authors introduced a linear regression model and analyzed the second-order attacks by this technique. In 2016, Bos et al. presented differential computation analysis to assess the security of white-box implementations which required neither knowledge about the look-up tables used nor any reverse engineering effort [16].

At the same time, several countermeasures have been proposed to secure those algorithms from first- and high-order attacks. The first practical evaluation was performed

on one additive and one multiplicative masking scheme of AES [4]. An enhancement of this method was proposed [17] which improved the CPA by restricting normalization factor. In 2011, Clavier et al. proposed collision-correlation power analysis on first-order protected AES.

However, to implement the power attack, each collection contains random noise in the process of power consumption. Overall, the noise is normally distributed for the whole traces. But it is also discrete distribution for each power trace. And the PCC cannot describe the correlation better because it is a statistical measure of the strength of a linear relationship between two variables. Therefore, the efficiency and accuracy may be affected.

In this paper, we propose a new method to operate the side-channel attack. The main contributions are as follows:

(1) A concept of R-squared fitting analysis (RFA) model for power analysis is proposed. This method can describe the correlation of the data better than CPA. In suitable experimental environment, the success rate of RFA is the same as CPA. But, in the poor environment, the result of RFA is better than CPA.

(2) RFA can improve the efficiency compared with the classic CPA which is used PCC. A model of the power traces with different Hamming weight from 0 to 8 is set up. In the case of more key points, it can effectively remove the interference of extra random noise so as to improve the success rate and shorten the operation time.

(3) RFA method has wide applicability, which is verified by simulation experiments in the different test scenarios. Its efficiency is similar to or better than that of the CPA.

In this paper, the organization is as follows. The Hamming weight model, R-squared model, and the classic CPA are given in Section 2. In Section 3, we introduce the basic idea and the R-squared fitting model analysis. Then, in Section 4, we introduce the application on the traditional CPA and comparison between the RFA and CPA on AES. In Section 5, we apply the RFA to the other attack methods. Finally, we conclude the paper in Section 6.

2. The Preliminaries

In this section, we first discuss the Hamming weight model. Second, the CPA steps are shown. And, finally, the basic principle of R-squared is introduced.

2.1. The Hamming Weight Model. In many ways, Hamming weight model is the simplest method which is proposed in [5, 18] to analyze the correlation between power consumption and the register switching from one state to the other. In CPA, it is generally assumed that the leakage from the power side-channel depends on the number of bits switching 0 to 1 or 1 to 0 at a given time. And the register is modeled as a state transition which is triggered by some events such as the edge of a clock signal. In an m-bit register, binary data $D = [d_0, d_1, \ldots, d_{m-1}]_2$ is coded as $D = \sum_{i=0}^{m-1} d_i 2^i$, with the bit values $d_i = 0$ or 1. And its Hamming weight is the number of 1, $H(D) = \sum_{i=0}^{m-1} d_i$.

The Hamming weight model neglects some factors which have an influence on the power consumption, for example, parasitic capacities, glitches, and transition events. When using the Hamming weight model for analysis, we assume that the power consumption is proportional to the number of bits set to logic 1 of the processed sensitive variable. In reality, we need to use the Hamming weight model only if the previous state is all 0.

The linear relationship between the power consumption W and $H(D)$ is limited. But considering a chip as a large set of elementary electrical components, the linear relationship does not represent the entire consumption of a chip but only the data-dependent part. In addition to the previously mentioned state changes, the power consumption of a chip also contains other variable consumption. It would be assigned to a term denoted by b which is assumed independent from the other variables: b encloses offsets, time dependent components, and noise. Therefore, the basic model for the data dependency can be written as follows:

$$W = aH(D) + b, \tag{1}$$

where a is a scalar gain between the value of Hamming weight of D and the power consumption W.

2.2. The Correlation Power Analysis. When processing sensitive intermediate values, side-channel leakage brings data-dependent power consumption or other physical behaviors. In [7], we can see the power consumption is related to the status of the register. In this paper, we use the Hamming weight model to analyze the correlation between the power consumption and intermediate values.

The connection of the devices is shown in Figure 1. The computer sends the ciphertexts to the cryptographic device, for example, chips, smart cards, and microcontrollers. The attacker connects the resistor with the power line of the cryptographic device and acquires the traces of the power consumption by the oscilloscope, which are transmitted to the computer.

CPA is a useful attack method proposed by Brier et al. [12]. First, the attacker should acquire a set of n power consumption traces corresponding to n different plaintexts. Let t_i denote the ith power trace and T denote the set of traces. Second, the attacker will recover the correct key by guessing the key from 0 to 255. Assume that the handled value is the result of an XOR operation between a secret key byte k and a known plaintext byte p, $d_i = p_i \oplus k$. The attacker can predict the value of Hamming weight h_i of d_i in time for each acquired traces t_i. Equation (2) can compute the PCC between these predictions of Hamming weight h_i and the instantaneous power consumption of the set of acquired traces t_i. The maximum PCC corresponds to the correct key. This formula can also be calculated to deduce the leakage position on the trace:

$$\rho_{h,t} = \frac{\mathrm{Cov}(h,t)}{\sigma_h \sigma_t}. \tag{2}$$

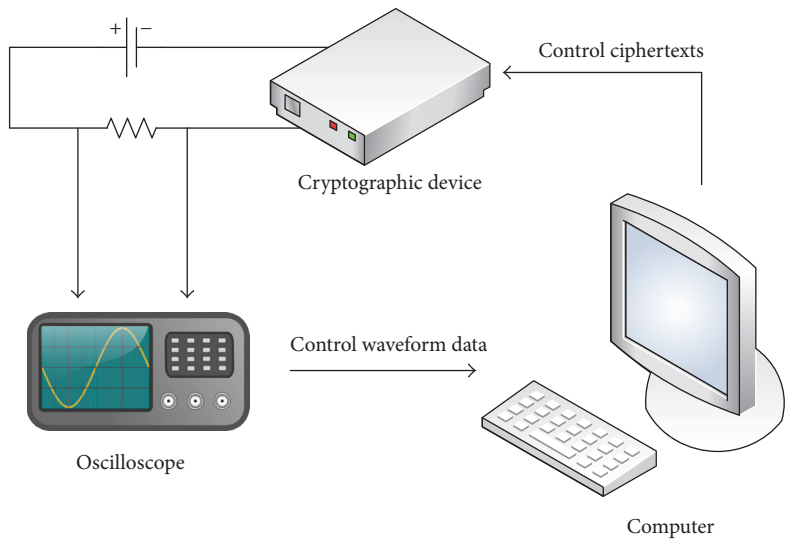

Figure 1: CPA connection of the devices.

2.3. The R-Squared Introduction. R-squared is a statistical method to evaluate how close the data are to the fitted regression line. It is also known as the coefficient of determination or the coefficient of multiple determination for multiple regression.

The definition of R-squared is fairly straightforward. It is the percentage of the response variable variation that is explained by a linear model. R-squared is always between 0% and 100%.

Here, 0% indicates that the model explains none of the variabilities of the response data around its mean. 100% indicates that the model explains all the variabilities of the response data around its mean.

A data set has n values marked by $y_1, \ldots, y_n$ (collectively known as y_i or as a vector $y = \{y_1, \ldots, y_n\}$), each associated with a predicted (or modeled) value $f_1 \cdots f_n$ (known as f_i, as a vector f). Define the residuals as $e_i = y_i - f_i$ (forming a vector e). If $\overline{y}$ is the mean of the observed data: $\overline{y} = (1/n)\sum_{i=1}^{n} y_i$, then the variability of the data set can be measured using three sums of squares formulas:

(i) The total sum of squares (proportional to the variance of the data) is

$$\mathrm{SS}_{\mathrm{tot}} = \sum_i (y_i - \overline{y})^2. \tag{3}$$

(ii) The regression sum of squares, also called the explained sum of squares, is

$$\mathrm{SS}_{\mathrm{reg}} = \sum_i (f_i - \overline{y})^2. \tag{4}$$

(iii) The sum of squares of residuals, also called the residual sum of squares, is

$$\mathrm{SS}_{\mathrm{res}} = \sum_i (y_i - f_i)^2 = \sum_i e_i^2. \tag{5}$$

(iv) The most general definition of the coefficient of determination is

$$R^2 = 1 - \frac{\mathrm{SS}_{\mathrm{res}}}{\mathrm{SS}_{\mathrm{tot}}} = \frac{\mathrm{SS}_{\mathrm{reg}}}{\mathrm{SS}_{\mathrm{tot}}}. \tag{6}$$

In general, the higher the value of the R-squared is, the better the model fits the data.

However, PCC is used to describe the linear relationship between the two variables, but the scope of application of the R-squared is more extensive. R-squared can be used to describe the nonlinear or have two or more independent variables. Because of the random noise of the energy traces which are measured, the correlation between the energy traces and the template cannot be well reflected by the PCC. So we can be more accurate to determine the relationship between the power traces and the Hamming weight by R-squared method.

3. The R-Squared Fitting Analysis for Power Attack

As we know, it is assumed that the attacker has two capabilities. First, the attacker can operate the chosen-plaintexts attack. Second, the attacker can acquire the power consumption from the device under attack.

The proposed approach is based on the Hamming weight model [7]. The leakage position is the AES first round's S-box output value y which is stored in a specific register. Figure 2 shows the position under attack.

3.1. The Basic Idea. In the template construction phase, we first model 9 templates corresponding to $H(y) = 0, 1, \ldots, 8$; for example, the template corresponding to $H(y) = 0$ is defined as $\overline{t}_0 = (1/m)\sum_{i=1}^{m} t_{i,0}$. The template set $\overline{T} = \{\overline{t}_0, \overline{t}_1, \ldots, \overline{t}_8\}$ can reflect the characteristics of the 9 kinds of power traces well.

Input: n random plaintexts $P = \{p_i \mid i \in [1, n]\}$,
template $\overline{T} = \{\overline{t}_0, \overline{t}_1, \ldots, \overline{t}_8\}$.
Output: k_{correct}.
(1) Encrypt P and acquire n traces $T = \{t_i \mid i \in [1, n]\}$
(2) **for** $k_{\text{guess}} = 0, 1, \ldots, 255$ **do**
(3) **for** $i = 1, 2, \ldots, n$ **do**
(4) $H_i = H(S(p_i \oplus k_{\text{guess}}))$
(5) $\widehat{t}_i = \overline{t}_{H_i}$
(6) **end for**
(7) Compute the $R^2_{k_{\text{guess}}}$ between $T_{\text{guess}} = \{\widehat{t}_1, \widehat{t}_2, \ldots, \widehat{t}_n\}$ and T
(8) **end for**
(9) **return** $k_{\text{correct}} = \arg\max_{k_{\text{guess}}} R^2_{k_{\text{guess}}}$

Algorithm 1: R-squared fitting analysis steps on S-box output.

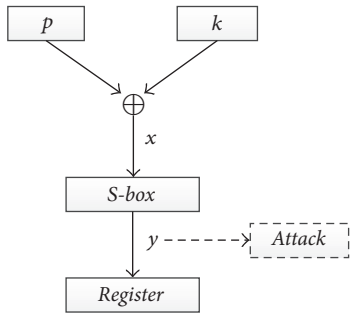

Figure 2: The position under attack.

In order to recover the secret key byte k, we product n random plaintext bytes $\{p_i \mid i \in [1, n]\}$. At the same time, we can get power traces $T = \{t_i,\ i \in [1, n]\}$ corresponding to n plaintexts.

In the key recovery phase, the attacker first guesses k_{guess} from 0 to 255, so the Hamming weight of y can be calculated by $H_i = H(S(p_i \oplus k_{\text{guess}}))$. According to each H, we choose the corresponding $\overline{t}_i$ from $\overline{T}$ to build T_{guess} which can reflect the leakage of the register. We call it $\widehat{t}$. Then the R-squared between T_{guess} and T can be calculated:

$$R^2_{k_{\text{guess}}} = 1 - \frac{\text{SS}_{\text{res}}}{\text{SS}_{\text{tot}}} = 1 - \frac{\sum_{i=1}^{n} \left(t_i - \widehat{t}_i\right)^2}{\sum_{i=1}^{n} \left(t_i - t_{\text{average}}\right)^2}. \quad (7)$$

The k_{guess} corresponding to the maximum R-squared value is the correct key.

3.2. Attack Scene. Algorithm 1 shows R-squared fitting analysis steps on S-box output. When using R-squared fitting method to analyze AES, there are two steps which must be completed. First, a template of traces $\overline{T}$ must be set up according to different Hamming weight, which can reflect the trace of each Hamming weight. For example, we randomly select m different plaintexts and keys, so that $H(S(p_i \oplus k)) = 0$. And we can get m traces. The average of the m traces is t_0. By repeating the above steps, we change $H(S(p_i \oplus k))$ from 1 to 8, and $t_1 \cdots t_8$ can be obtained. The template $\overline{T}$ is $\{\overline{t}_0, \overline{t}_1, \ldots, \overline{t}_8\}$. Second, R^2 as a distinguisher identifies the correct key. According to the value of R^2 between the real traces T and T_{guess} which reflect k_{guess}, we can judge the correct key. The formula of R^2 is (7).

By selecting the maximum value of the R^2, we can judge which k_{guess} is the most possible secret key.

4. Comparisons with Pearson's Correlation Coefficient

In order to evaluate R^2 between the traces of power consumption and T_{guess}, we use the software simulation so the test on AES can emerge, as shown in Figure 2. The parameters of simulating the traces of the register are that standard deviation σ is 3 and the number of key points of the trace is 10. Based on the descriptions of Section 3, we try to use the R-squared fitting model to analyze the leakage of power consumption and compare RFA with the classic CPA. The part under attack is the register which saves the output value of the S-box.

Figure 3 shows the fitting traces of the power consumption. We assume that the noise is Gauss random noise. And the traces are simulated on the computer. And then, we compute the correlation by R-squared fitting model analysis and compare it with the classic CPA. The relationship between guessed key and correlate coefficient is shown in Figure 4. From Figure 4, we can see that the RFA can distinguish the correct key clearly which is 150.

We do the simulation experiments on the computer. When the standard deviation $\sigma = 2$ and the number of key points of the trace is 5, we can find that we only need 12 plaintexts to get the correct key by RFA with the success rate 91%, while CPA is about 65% (as shown in Figure 5).

Figure 6 also shows the contrast between CPA and RFA in the case of different number of plaintexts and the standard deviation $\sigma = 4$. Some similar contrasts are shown in Figures 7 and 8. From Figures 5–8, we can see that as the standard deviation increases, more plaintexts are required to recover the correct key in the same conditions. However, the efficiency of RFA is still better than that of CPA.

By comparing the success rate of RFA with CPA in different conditions, we get a conclusion that the RFA can judge the correct key the same as CPA, and the efficiency is slightly better than CPA. When the number of plaintexts is 5, the success rate of RFA is double the PCC. In the RFA, only 86 seconds are spent in the calculation process, and it is better than CPA by nearly 20%. This is because R^2 costs lower computation complexity than PCC [19].

5. Application on the Other Attack Methods

In Section 4, we can see that the RFA is efficient compared to CPA. In this section, we will show that this method still can be widely used in the other attack models. We choose the second-order CPA attack [20] and collision-correlation power analysis on first-order protected AES [21] to compare the success rate between RFA and CPA in simulation scenario.

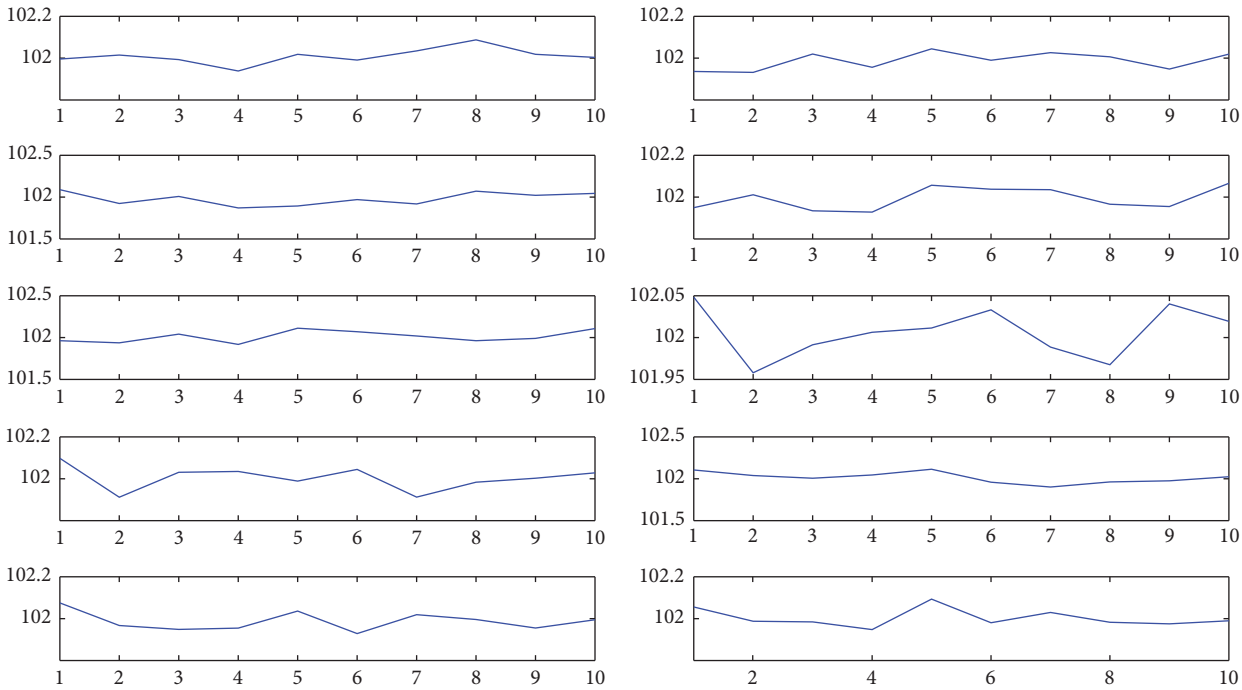

Figure 3: The fitting traces of the power consumption when Hamming weight is 2.

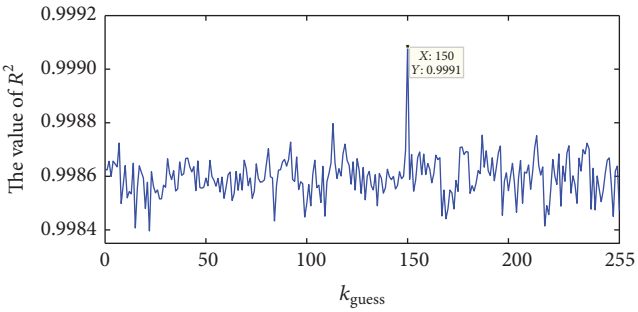

Figure 4: The result of k_{guess} correlation by RFA.

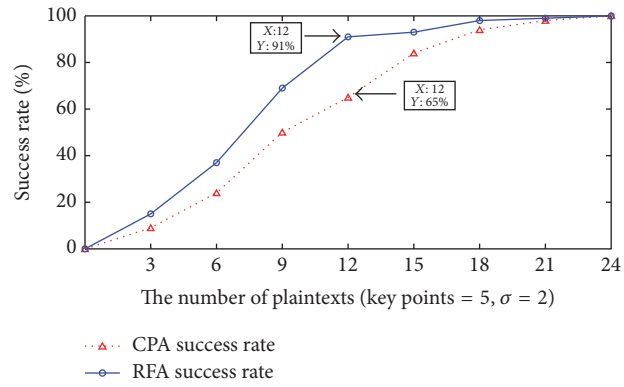

Figure 5: The comparison between RFA and CPA.

5.1. Implementation with Collision-Correlation Power Analysis. Collision-correlation power analysis on first-order protected AES [21] is proposed in CHES 2011. This attack is more powerful and practicable than previous second-order power analyses and increases the risk that these implementations are broken in practice. The contrast of success rate of RFA and CPA is shown in Figure 9.

In Figure 9, we can see that the mask protection scheme is used to mask the first round before S-box in AES. And the attack steps are introduced in Algorithm 2. For each p_2, we encrypt it for n times, and we can find the relationship between k_1 and k_2 by detecting the collision between t_1 and t_2 so as to recover the correct key. In Figure 10, the success rate of RFA on collision-correlation attack is higher than CPA clearly, and the RFA also has more obvious advantages in operation time.

5.2. Implementation with Practical Second-Order CPA Attacks. If the attacker can get the relationship between the power consumption and the intermediate value of cryptographic algorithms, the secret key can be recovered easily. In order to change this relationship, the designer puts the mask m into the intermediate value. In 2006, Oswald et al. proposed the mask protection scheme and its attack methods [20].

In Figure 11, RNG means the random number generator. This module can output random numbers which are called masks. These random numbers are involved in the encryption process. We can see that the information leakage of power consumption has been masked by the random masking of the operation, so the trace which we have held seems to be masked randomly and we cannot directly recover the correct

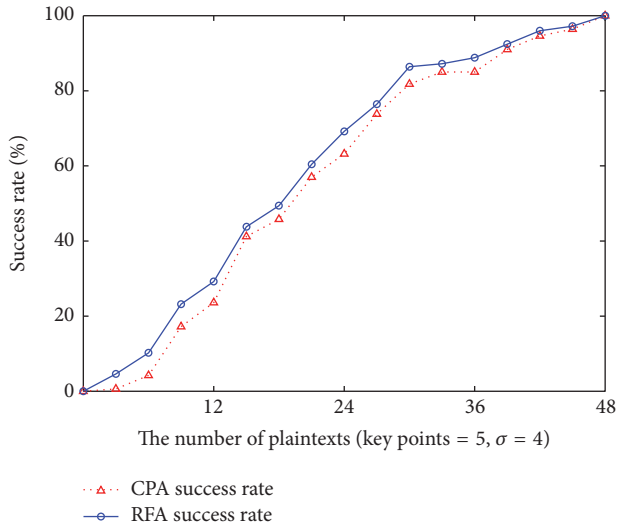

Figure 6: The comparison between RFA and CPA.

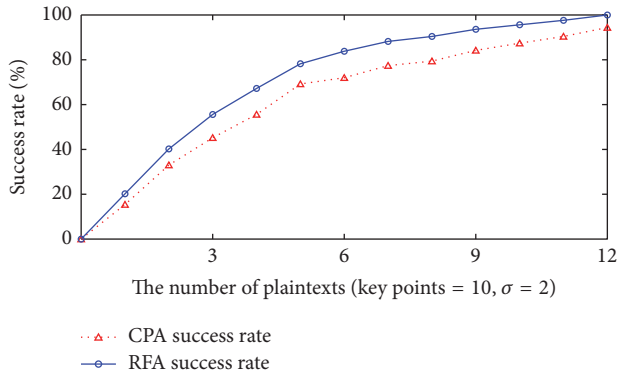

Figure 7: The comparison between RFA and CPA.

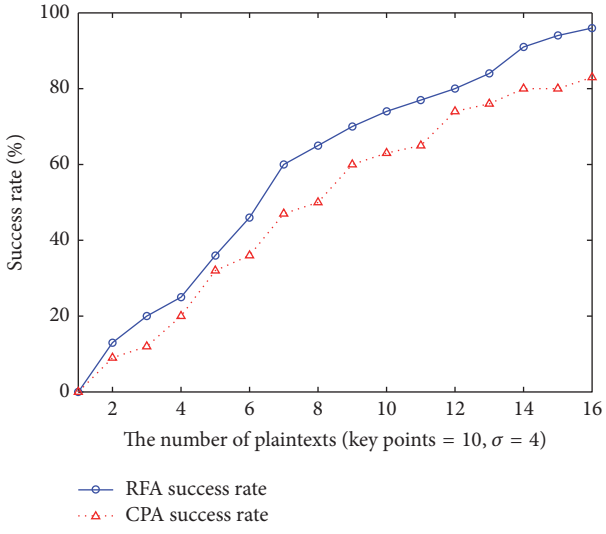

Figure 8: The comparison between RFA and CPA.

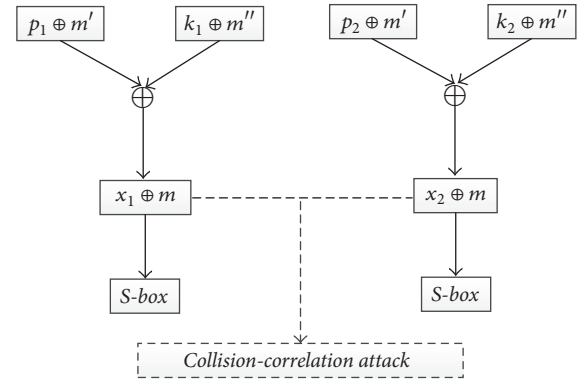

Figure 9: Mask protection scheme and collision-correlation power analysis.

Input: Fixed plaintext bytes $p_1 = 0$.
Output: $k_1 \oplus k_2$.
(1) **for** $p_2 = 0, 1, \ldots, 255$ **do**
(2) **for** $i = 1, 2, \ldots, n$ **do**
(3) Encrypt p_1 and acquire $t_{1,i}$
(4) Encrypt p_2 and acquire $t_{2,i}$
(5) **end for**
(6) Compute the $R^2_{p_2}$ between $\{t_{1,i} \mid i \in [1, n]\}$ and $\{t_{2,i} \mid i \in [1, n]\}$
(7) **end for**
(8) $p_2 = \arg\max_{p_2} R^2_{p_2}$
(9) **return** $k_1 \oplus k_2 = p_1 \oplus p_2 = p_2$

Algorithm 2: RFA on collision-correlation power attacks.

key. For these mask protection schemes, we use the attack method in [20] with the RFA. In Algorithm 3, we show the attack steps. And the comparison with the success rate of CPA is in Figure 12.

In the above second-order attack scenario, we replace the CPA with RFA to recover the secret key. We can see the success rate of RFA is nearly the same as the CPA in Figure 12. But the time cost of RFA is also 20% less than CPA, as we explained in Section 4.

5.3. Discussion. From formulas (7) and (8), we can see that the R-squared used in this paper is equivalent to the Least Squared Method (LSM). Therefore, we try to study the LSM, Least Absolute Deviation (LAD) and LAD's variants in the application of RFA. In order to study the superiority of RFA, we experiment with LSM and LAD to evaluate the distance between T and T_{guess} so as to see whether RFA is more appropriate than LAD:

$$D_{\text{LSM}} = \frac{1}{n}\sum_{i=1}^{n}\left(t_i - \hat{t}_i\right)^2, \tag{8}$$

$$D_{\text{LAD}^\alpha} = \frac{1}{n}\sum_{i=1}^{n}\left|t_i - \hat{t}_i\right|^\alpha. \tag{9}$$

Input: n random plaintexts $P = \{p_i \mid i \in [1, n]\}$,
template $\overline{T}$.
Output: k_{correct}.
(1) Encrypt P and acquire $T_{y \oplus w} = \{t_{y \oplus w, i} \mid i \in [1, n]\}$,
$T_w = \{t_{w,i} | i \in [1, n]\}$
(2) $T = |T_{y \oplus w} - T_w|$
(3) **for** $k_{\text{guess}} = 0, 1, \ldots, 255$ **do**
(4) **for** $i = 1, 2, \ldots, n$ **do**
(5) $H_i = H(S(p_i \oplus k_{\text{guess}}))$
(6) $\widehat{t}_i = \overline{t}_{H_i}$
(7) **end for**
(8) Compute the $R^2_{k_{\text{guess}}}$ between $T_{\text{guess}} = \{\widehat{t}_1, \widehat{t}_2, \ldots, \widehat{t}_n\}$
and T
(9) **end for**
(10) **return** $k_{\text{correct}} = \arg\max_{k_{\text{guess}}} R^2_{\text{guess}}$

Algorithm 3: RFA on second-order CPA attacks.

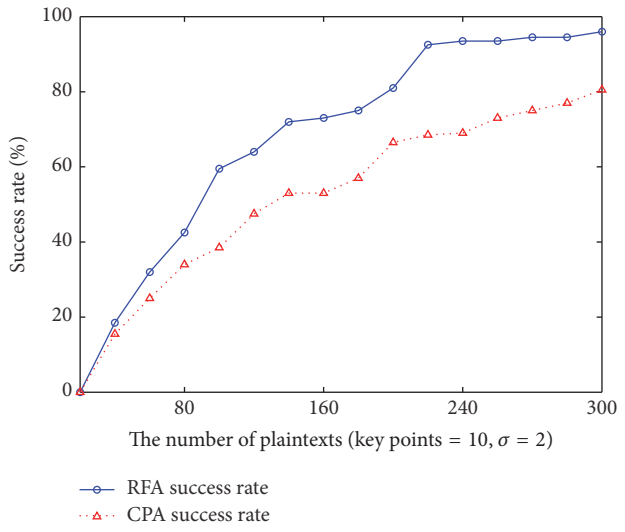

Figure 10: The comparison of the RFA and CPA in first-order protected AES.

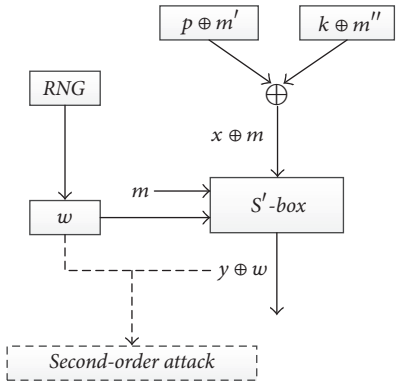

Figure 11: Mask protection scheme and second-order attack.

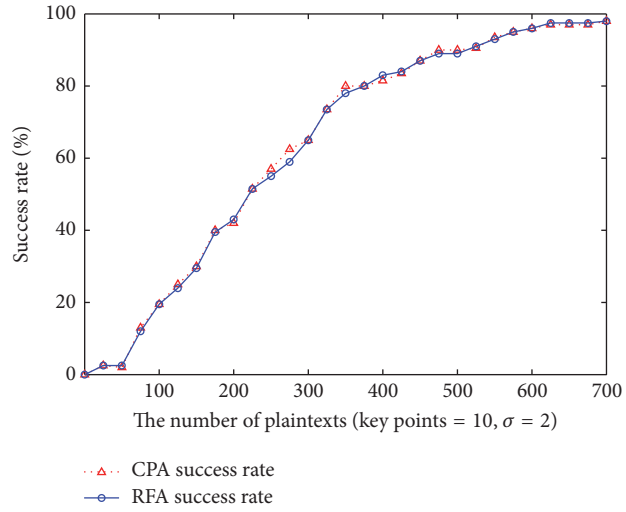

Figure 12: The comparison of the RFA and CPA in second-order attack.

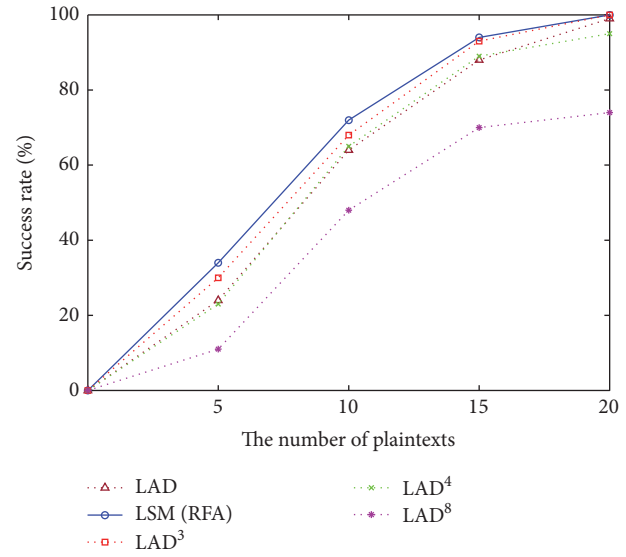

Figure 13: The comparison of the LSM and LAD.

In Figure 2 scenarios, we operate the experiments, respectively, with the LSM and LAD. The comparison of success rate is shown in Figure 13. We can see that the success rate of LSM is higher than LAD. So RFA method is more efficient than the LAD.

6. Conclusion

We present a new correlation analysis method which is called R-squared fitting model analysis. Through the simulation with different experiment scenes, we can see that this method is better for the nonlinear correlation analysis. At the same time, we can see that RFA has the same success rate as the CPA in recovering the secret keys. And in some case, the performance is even better. Because of the ease of operation, the time complexity of RFA is more superior.

Through practical results from software implementations, this technique may also be a threat for hardware coprocessors. Moreover, we can use this method in other areas, for example, electromagnetic analysis which needs to use the correlation analysis. Therefore, the R-squared fitting analysis may be promoted in a wider range of application scenarios.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

Acknowledgments

This paper is supported by National Natural Science Foundation of China (nos. 61402252 and 61402536), Beijing Natural Science Foundation (no. 4162053), Foundation of Science and Technology on Information Assurance Laboratory (no. KJ-15-005), Beijing Institute of Technology Research Fund Program for Young Scholars, and DNSLAB, China Internet Network Information Center, Beijing 100190.

References

[1] X. Hei and X. Du, "Biometric-based two-level secure access control for implantable medical devices during emergencies," in *Proceedings of the 30th IEEE International Conference on Computer Communications (IEEE INFOCOM '11)*, pp. 346–350, Shanghai, China, April 2011.

[2] X. Hei, X. Du, J. Wu, and F. Hu, "Defending resource depletion attacks on implantable medical devices," in *Proceedings of the 53rd IEEE Global Communications Conference (GLOBECOM '10)*, Seattle, Wash, USA, December 2010.

[3] X. Du, M. Guizani, Y. Xiao et al., "Defending DoS attacks on broadcast authentication in wireless sensor networks," in *Proceedings of the IEEE International Conference on Communications (ICC '08)*, pp. 1653–1657, IEEE, 2008.

[4] S. Mangard, N. Pramstaller, and E. Oswald, "Successfully attacking masked AES hardware implementations," in *Proceedings of the International Workshop on Cryptographic Hardware and Embedded Systems*, pp. 157–171, Springer, Edinburgh, UK, 2005.

[5] P. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," in *Proceedings of the 19th Annual International Cryptology Conference*, pp. 388–397, Springer, Santa Barbara, Calif, USA, 1999.

[6] S. Mangard, E. Oswald, and T. Popp, *Power Analysis Attacks: Revealing the Secrets of Smart Cards*, Springer Science Business Media, Berlin, Germany, 2008.

[7] M. L. Akkar, R. Bevan, P. Dischamp et al., "Power analysis, what is now possible," in *Proceedings of the International Conference on the Theory and Application of Cryptology and Information Security*, pp. 489–502, Springer, 2000.

[8] C. Herbst, E. Oswald, and S. Mangard, "An AES smart card implementation resistant to power analysis attacks," in *Proceedings of the International Conference on Applied Cryptography and Network Security*, pp. 239–252, Springer, 2006.

[9] D. Agrawal, B. Archambeault, J. R. Rao et al., "The EM side-channel(s)," in *Proceedings of the International Workshop on Cryptographic Hardware and Embedded Systems*, pp. 29–45, Springer, Redwood Shores, Calif, USA, August 2002.

[10] K. Gandolfi, C. Mourtel, and F. Olivier, "Electromagnetic analysis: concrete results," in *Proceedings of the 3rd International Workshop on Cryptographic Hardware and Embedded Systems*, pp. 251–261, Paris, France, 2001.

[11] J. Quisquater and D. Samyde, "ElectroMagnetic analysis: measures and counter-measures for smart cards," in *Proceedings of the International Conference on Research in Smart Cards: Smart Card Programming and Security*, pp. 200–210, Springer, Cannes, France, September 2001.

[12] E. Brier, C. Clavier, and F. Olivier, "Correlation power analysis with a leakage model," in *Proceedings of the International Workshop on Cryptographic Hardware and Embedded Systems*, pp. 16–29, Springer, Cambridge, Mass, USA, August 2004.

[13] B. Gierlichs, L. Batina, P. Tuyls et al., "Mutual information analysis," in *Proceedings of the International Workshop on Cryptographic Hardware and Embedded Systems*, pp. 426–442, Springer, Washington, DC, USA, August 2008.

[14] L. Batina, B. Gierlichs, and K. Lemke-Rust, "Differential cluster analysis," in *Proceedings of the 11th International Workshop on Cryptographic Hardware and Embedded Systems (CHES '09)*, pp. 112–127, Springer, Lausanne, Switzerland, September 2009.

[15] G. Dabosville, J. Doget, and E. Prouff, "A new second-order side channel attack based on linear regression," *IEEE Transactions on Computers*, vol. 62, no. 8, pp. 1629–1640, 2013.

[16] J. W. Bos, C. Hubain, W. Michiels et al., "Differential computation analysis: hiding your white-box designs is not enough," in *Proceedings of the International Conference on Cryptographic Hardware and Embedded Systems*, pp. 215–236, Springer, Santa Barbara, Calif, USA, August 2016.

[17] T. H. Le, J. Clédière, C. Canovas, B. Robisson, C. Servière, and J.-C. Lacoume, "A proposition for correlation power analysis enhancement," in *Proceedings of the International Workshop on Cryptographic Hardware and Embedded Systems*, pp. 174–186, Springer, Yokohama, Japan, October 2006.

[18] T. S. Messerges, A. E. Dabbish, and R. H. Sloan, "Investigations of power analysis attacks on smartcards," *Smartcard*, vol. 99, pp. 151–161, 1999.

[19] D. E. Knuth, *The Art of Computer Programming, Volume 2: Seminumerical Algorithms*, Pearson Education, Upper Saddle River, NJ, USA, 1997.

[20] E. Oswald, S. Mangard, C. Herbst, and S. Tillich, "Practical second-order DPA attacks for masked smart card implementations of block ciphers," in *Proceedings of the Cryptographers' Track at the RSA Conference on Topics in Cryptology*, pp. 192–207, Springer, San Jose, Calif, USA, February 2006.

[21] C. Clavier, B. Feix, G. Gagnerot et al., "Improved collision-correlation power analysis on first order protected AES," in *Proceedings of the International Workshop on Cryptographic Hardware and Embedded Systems*, pp. 49–62, Springer, 2011.