

Correlation Photonic Emission Attacks Against AES Algorithm

Hong-sheng Wang^{1,a}, Zi-yan Xu^{1,b}, Yang Zhang¹, Kai-yan Chen¹, Ling-an Wu²

¹Department of Information Engineering, Ordnance Engineering College, Shijiazhuang 050003, China;

²Institute of Physics and Beijing National Laboratory for Condensed Matter Physics, Chinese Academy of Sciences, Beijing 100190, China.

^b1508785745@qq.com

Keywords: Correlation photonic emission attacks; AES; signal-noise ratio; correlation coefficient.

Abstract. Cipher chips, such as microprocessors, are playing the important role in most cryptosystems, and protecting the data which is important. But since Side Channel Analysis is put forward, the security of cipher chip was met a severe challenge. Correlation photonic emission attacks (CPEA) is a new kind of method against cipher chips. Operating steps and the simulation result is given in the paper. First, A typical CPEA process is given, which is important for the simulation experiment. Then, the concept of correlation coefficient is given, and introduces a estimated method for correlation coefficient. There is a certain relationship between signal-noise ratio (SNR) and the correlation coefficient of CPEA. The last, the simulation results of CPEA against AES algorithm is given.

1. Introduction

Cipher Chip plays an increasingly important role with the rapid development of microelectronics and computer techniques in people's lives. During operation, cipher chip releases some information, called side channel information. Since Kocher has been published groundbreaking articles in 1996 and 1999, side channel become an important area of research on cryptanalysis [1]. Correlation attacks (such as power analysis attacks [2], the electromagnetic radiation attacks [3], fault injection attacks [4], etc.) and a variety of analytical methods (such as templates attacks [5], differential analysis [6], etc.) have been studied. Compared with the traditional power and electromagnetic side-channel attacks, whose mainly against information leakage analysis of the entire system, photonic emission analysis attacks [7] be proposed allows you to select a specific part of the hardware cryptographic chip optical radiation analysis, so that photonic emission analysis attack selective attack even more than power, electromagnetic analysis attacks. A good signal noise ratio (SNR) can be obtained by choosing the specific location / area attack. However, due to the huge cost and complexity of the necessary equipment used in [6], the photonic side channel was not regarded as a realistic threat at that time. Since then, new research has introduced new applications and demonstrated that photonic side channel attacks can be realized with low-cost equipments [8].

This work gives a thorough overview on the photonic side channel, describes correlation photonic emission attacks against cipher chip in detail and also discusses data dependence of the optical radiation trace of cipher chip by a experimental verification.

2. Background

2.1 AES algorithm

AES is a 128-bit block cipher ratified as a standard by NIST, AES operates on a 4×4 matrix of bytes, called state matrix. Depending on the length of the key, which is 128, 192 or 256 bit, called AES-128, AES-192 or AES-256. Except for the last one is not included among MixColumns, each cycle has four distinct steps [9] (SubBytes, ShiftRows, MixColumns, AddRoundKey), in addition to, before the first round AddRoundKey is carried out. For AES-128, the original key which is 128 bits is used for AddRoundKey in the first round behind the 128-bit key is obtained from the initial round key derivation.

2.2 photonic emission composition of cipher chip

If the optical time domain signal recording technology is used, photonic emission, according to the literature [9], refers to a function between the intensity of photonic emission signal and time, which is the photon-number distribution in the time domain of single photon detection technology [8] and time-correlated single-photon counting (TCSPC) technology [8] sampled. Photonic emission reflects photon leaks at each point in time of running cipher chip. Photonic emission contains both the useful information to crack a key, but also includes some of the noise signal. For noise signal processing largely determines the efficiency and accuracy of key analysis. Photonic emission a point in time following composition:

$$P = P_{op} + P_{da} + P_{co} + P_{no} \quad (1)$$

In the equation (1), where P is the total amount of a point of photonic emission, P_{op} is the operation dependent component, P_{da} is the data dependent component, P_{no} is electronic noise, P_{co} is a constant component. Wherein, P_{op} and P_{da} is the most important component of the photonic emission analysis, especially P_{da} , it is because the photonic emission analysis attacks depends on data processing operations and the implementation of its runtime. Executing different operating and handling different data will result in a different photonic emission. Electronic noise P_{no} mainly composed by quantization noise, external environmental interference, power supply and clock noise and other components, P_{no} leads to the photonic emission of cipher chip to run the program under the same circumstances and processing of data collected will still be different. In order to improve the signal to noise ratio and to reduce the influence of electronic noise analysis of efficiency, on the one hand, TCSPC (time-correlated single photon counting, the same below) photon recording technology can be used, which has a smaller quantization noise than analog recording technology; On the other hand, because P_{no} submits to normal distribution $N(0, \sigma^2)$, such that the expected value goes to zero, multiple optical signal acquisition can be used with the averaging method for reducing electronic noise. P_{co} mainly composed by the switching of the transistor, which is no associated with operational procedures and processes data, considered to be a constant generally.

3. CEPA methods and processes

CPEA principle is to analyze the dependence of light leakage trace between a fixed time of the light leakage and processed data, the main purpose is to calculate the correlation coefficient of light leakage simulation model to calculate the actual position of each light leakage tracks(each sampling time points),simulation model and the actual light leak light leakage trace at each position (each sampling time points) polish leaks related coefficient, if correlation coefficient at some point is maximum, we can guess the key of the position is the actual value.

3.1 A typical CPEA process

1) Cryptographic algorithm intermediate results performed. The intermediate result is a function $f(d, k)$, d is very aware of the amount of data that is not expressly ciphertext; k is a small part of the key.

2) Measurement D different data packets leak when cryptographic chip encrypt or decrypt a light, and sequentially records each encryption or decryption corresponding plaintext or ciphertext d , forming vectors $d = (d_1, \dots, d_D)'$. Encryption or decryption data d_i corresponding light leakage track record is $t_i = (t_{i,1}, \dots, t_{i,T})'$, where T represents the length of the light leakage track (i.e. the number of sampling time points), therefore, the light leakage can be written as $D \times T$ order matrix T .

3) For all possible key values k (key candidates), according to the function $f(d, k)$ calculated hypothetically intermediate results. All possible assumptions values of k recorded as vector $k = (k_1, \dots, k_K)$, K is the number of all possible values of k . An attacker is based on the data vector d and key assumptions k to calculate the assumed median $f(d, k)$, obtained hypothetical median matrix V , which is done as follows.

$$V = \begin{pmatrix} f(d_1, k_1) & \dots & f(d_1, k_K) \\ \vdots & \ddots & \vdots \\ f(d_D, k_1) & \dots & f(d_D, k_K) \end{pmatrix} \quad (2)$$

$$v_{i,j} = f(d_i, k_j) \quad i = 1, \dots, D \quad j = 1, \dots, K$$

Cryptographic algorithm used an element of K when encrypt or decrypt, denoted this element k_{ck} , which is the correct key. The goal of CPEA: in D encryption or decryption process, simply find the column of V has been processed, k_{ck} we can get.

4) By assuming that the matrix of intermediate values V , applying some light leakage simulation model, it will be assumed intermediate value matrix V analog mapping assumption light leakage value matrix H , i.e. every hypothetically intermediate value $v_{i,j}$ is mapped to a hypothetical light leaking value $h_{i,j}$.

5) Compared the hypothetical light leakage value matrix H and the actual light leakage trace matrix T . according to correlation, compared each column and row of the matrix H and T to get a correlation coefficient matrix R which is $K \times T$ ranks. The greater the value of the element $r_{i,j}$ of R , the greater the correlation between the column h_j and the column t_j . Thus, an attacker can find out the correct key by looking up the maximum of correlation coefficient matrix R . Referred the location of the light leakage trace as ct , the corresponding column t_{ct} contains all of the light leakage which is dependent on intermediate values.

3.2 The method of calculating correlation coefficient

In CPEA, according to the correlation coefficient to get the linear relationship between column h_i of matrix H and column t_j of matrix T , where $i = 1, \dots, K$; $j = 1, \dots, T$. According to the following formula can obtain each $r_{i,j}$ of matrix R , where \bar{h}_i and \bar{t}_j represent the mean of column h_i of the matrix H and the mean of column t_j of the matrix T .

$$r_{i,j} = \frac{\sum_{d=1}^D (h_{d,i} - \bar{h}_i) \cdot (t_{d,j} - \bar{t}_j)}{\sqrt{\sum_{d=1}^D (h_{d,i} - \bar{h}_i)^2 \cdot \sum_{d=1}^D (t_{d,j} - \bar{t}_j)^2}} \quad (3)$$

4. The correlation coefficient estimation and simulation based on a single point of photonic emission

In CPEA, based on the correlation coefficient to estimate a linear relationship of the column between matrix T and matrix H , the spikes appears in the correlation coefficient matrix R can reveal the key.

The following describes the correlation coefficient estimation techniques, the estimates do not need to implement the actual attack. Estimation of the correlation coefficient for the attacker to attack the AES cryptographic chip has great value and can help estimate the effect of attacks.

4.1 The estimated method for correlation coefficient

We first need to establish a relationship between signal-noise ratio (SNR) and the correlation coefficient of correlation analysis attacks [10].

For the SNR of position j of light leakage track, how to calculate the correlation of columns h_i of the hypothetical light leakage matrix H and columns t_j of the actual light leakage trace matrix T ? According to the equation $P(X) = P_{ef}(X) + P_{sw} + P_{co} + P_{no}$, establishes model for photonic emission, where P is the light leakage at the time position j of cryptographic chip, random variable H_i represents hypothetical light leakage value of the column i . So, each element of h_i is a sample of random variable H_i . Use $\rho(H_i, P)$ represents the correlation, AS can be seen in equation (4). Because of the public component P_{co} does not affect correlation coefficient, transition noise $P_{sw} = 0$, statistically, P_{no} independent of P_{ef} .

$$\rho(H_i, P) = \rho(H_i, P_{ef} + P_{sw} + P_{no} + P_{co})$$

$$\begin{aligned}
&= \rho(H_i, P_{ef} + P_{sw} + P_{no}) \\
&= \rho(H_i, P_{ef} + P_{no}) \\
&= \frac{E(H_i \cdot (P_{ef} + P_{no})) - E(H_i) \cdot E(P_{ef} + P_{no})}{\sqrt{\text{Var}(H_i) \cdot (\text{Var}(P_{ef}) + \text{Var}(P_{no}))}} \\
&= \frac{E(H_i \cdot P_{ef} + H_i \cdot P_{no}) - E(H_i) \cdot (E(P_{ef}) + E(P_{no}))}{\sqrt{\text{Var}(H_i) \cdot \text{Var}(P_{ef})} \cdot \sqrt{1 + \frac{\text{Var}(P_{no})}{\text{Var}(P_{ef})}}} \\
\rho(H_i, P) &= \frac{\rho(H_i, P_{ef})}{\sqrt{1 + \frac{1}{\text{SNR}}}} \tag{4}
\end{aligned}$$

This conclusion is very important. SNR describes the information leak of cryptographic chip at a given attack scenario, the attacker uses light leakage model to take advantage of this information leakage, how to use the information leakage at the specific attack can be characterized by $\rho(H_i, P_{ef})$, it is the correlation between light leakage which is hypothesized by the attacker with the value of light leakage which can be used of cipher chip. It should be noted that this correlation characterization depends on f light leakage simulation model used by the attacker to process the described accuracy which caused by attacked median.

Through the implementation of simulation CPEA, the correlation $\rho(H_i, P_{ef})$ can be determined. The basic method is as follows:

- 1) Generate vector d , the vector contains all possible input data which be attacked of middle values.
- 2) Based on data input d , key which cryptographic chip uses and a suitable light leakage simulation model, making simulation about light leaking P_{ef} , the simulation result is a matrix S , which each row contains an available light leakage track simulation of password chip.
- 3) Using the matrix S implement CPEA attack, based on the light leakage simulation model to generate all hypothetic light leakage values of the key.
- 4) Calculating the correlation coefficients between each column of matrix H and matrix S , to generate the correlation matrix R .

Each element $r_{i,j}$ of the correlation coefficient matrix R which is got by this method is equal to $\rho_{i,j}$, when based on all of the data the input to calculate the correlation coefficient r , $r = \rho$. Therefore, the simulation results corresponding to the CPEA attacks also occurred in a real attack correlation $\rho(H_i, P_{ef})$.

It should be noted that the hypostatic role of CPEA simulation attacks often switch between designers and attackers. For the first step (i.e. generated light leakage simulation trace S), if the key is known, it is considered from the perspective of the designer. In order to quickly identify $\rho(H_i, P_{ef})$ in different scene, simulation CPEA attacks are very useful because the entire attack is a simulation, so the light leakage characteristics and attacker's light leakage model can be changed easily and various changes resulting consequences can be analyzed immediately.

Next, the paper using simulation CEPA attack and formulas (4) to estimate the correlation coefficient against AES cipher chip.

4.2 The correlation coefficient simulation

The target of attacking against AES cipher chip is S-box outputs of the first round, using Hamming-weight model to implement the simulation of CPEA attack.

- 1) Generating a vector d , which contains all input values of S-boxes that is attacked, i.e. $d = (0, 1, 2, \dots, 255)'$.
- 2) These input values are mapped to the simulation of light leakage values, according to $s_{i,ct} = HW(S(d_i \oplus k_{ck}))$.

In the current simulation CPEA attack, only the light leakage of the S-box output is emulated, i.e. light leakage at the location ct . Therefore, the matrix S is composed of the column s_{ct} . The available information at the location ct is maximum. Therefore, there is a position having the maximum correlation of the light leakage track.

3) After the s_{ct} simulation, we can implement CPEA attacks on this column. Hamming-weight model generate hypothetical light leakage value matrix H for all possible key assumptions, calculating the correlation between each column of matrix H and s_{ct} . The simulation CPEA attack generated a matrix R which size is 256×1 .

4) See Fig. 1, the CPEA Attack Simulation results are shown for S-box output of the first round of AES encryption, actual key is 255, the correlation coefficient corresponding to the column s_{ct} is 1.

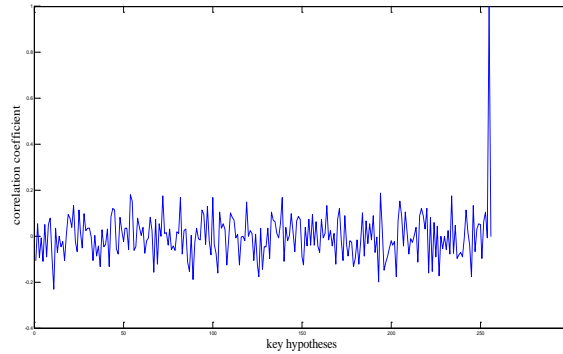


Fig. 1 Attack simulation of CPEA on AES algorithm for the first S-box output

As can be seen in Fig. 1, when key assumptions is the 255, $\rho(h_i, t_{ct}) = 1$. In order to map these correlations for the actual correlations $\rho(h_i, t_{ct})$, the noise appearing in the actual attack must be considered.

In addition, making CEPA simulation for S-box input of the first round of AES encryption algorithm (i.e. the result of AddRoundKey of the first round), ditto, get the result shown in Fig.4-2.

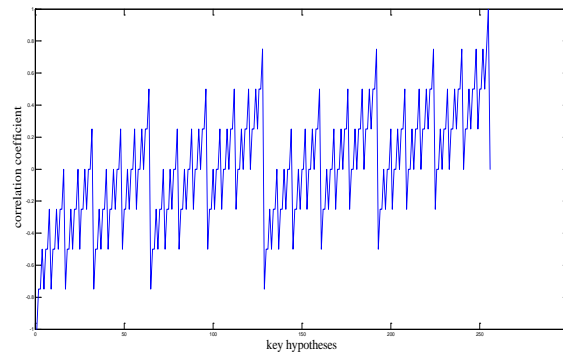


Figure 4-3 Attack simulation of CPEA on AES algorithm for the first S-box input

It can be seen in Fig. 1, there is only one distinct peak, and the differences of the correlation coefficient of correct key and correlation coefficients of other key in Fig. 2 is much smaller than it in Fig. 1.

Therefore, to obtain the correct key in the actual attack, more light leakage tracks are needed. This is due to the S-boxes belonging to non-linear transformation, a different input bit will cause a plurality of different output bits. Therefore, CPEA attack against AES cipher chip recommended to choosing the output of the first round of AES (or the final round of the S-box input) as the intermediate value.

5. Conclusions

Based on the analysis of the composition of photonic emission, correlation coefficients estimation method is introduced, to establish the relationship of the correlation coefficient between

the SNR and correlation analysis, to achieve a CPEA experimental result of simulation analysis which is useful to research CPEA and lay a good foundation for comparing with other PEA, at the same time, the conclusion which the correlation coefficient of actual attack can be get only need to compute is proved.

References

- [1] Kocher P, Jaffe J, Jun B. Differential power analysis[C]. //Wiener M. Advances in Cryptology - CRYPTO 1999 , LNCS, vol. 1666, Springer-Verlag, 1999: 388-397.
- [2] Hnath W. Differential Power Analysis Side-Channel Attacks in Cryptography[D]. Dissertation for the Doctoral Degree, Worcester Polytechnic Institute, 2010.
- [3] Mulder E D. Electromagnetic Techniques and Probes for Side-Channel Analysis on Cryptographic Device[D]. Dissertation for the Doctoral Degree, Katholieke Universiteit Leuven, 2010.
- [4] Biham E, Shamir A. Differential fault analysis of secret key cryptosystems[C]. CRYPTO '97, volume 1294 of Lecture Notes in Computer Science, Springer-Verlag, 1997:513-525.
- [5] Wang T, Zhao X J, Guo S Z, Zhang F, Liu H Y, Zheng T M. Cache timing template attack research against AES. Chinese Journal of Computers, 2012,35(2):325-341.
- [6] Schlosser A, Nedospasov D, Kramer J, Orlic S, Seifert J P. Differential Photonic Emission Analysis[C]. COSADE 2013, 2013: 1-16.
- [7] Ferrigno, J., Hlavac, M.: When AES blinks: introducing optical side channel[J]. Information Security, IET 2(3), 2008, 94 -98.
- [8] Wang H S, Ji D G, Gao Y L, Zhang Y, Chen K Y, Chen J G, Wu L A, Wang Y Z. Photonic Emission Analysis of Cipher Chips Based on Time-Correlated Single-Photon Counting[J]. Acta Phys. Sin. 64(5) 058901-1.
- [9] Mangard S, Oswald E, Popp T (translated by Feng D G, Zhou Y B, Liu J Y). *Power Analysis Attacks* (Beijing: Science Press) 2010, pp1-129.
- [10] Wang H S. Research on Optical Side Channel Attacks against AES Cipher Chips[D]. Dissertation for the Doctoral Degree, Department of Information Engineering, 20.