Correlation power analysis for AES encryption device

Zhang Xiaoyu[a]，Chen Kaiyan，Zhang Yang，Gui Weilong, Li Lei

Department of information Engineering, Ordnance Engineering College, Shijiazhuang 050003, China

[a]18811785953@163.com

Keywords：side channel attacks; correlation coefficient; advance encryption standard; *Hanmming weight model*

Abstract. This paper introduces the realization of correlation power analysis attack to decrypt the encryption equipment for AES encryption system. On the basis of analysis power leakage principle power models and data correlation to build the power information collection and data processing platform. Introducing the CPA simulation attack in S-box about AT89S52 then analysis and compare the difference. As a result, practical experiment has shown that an attacker can obtain the exact key quickly.

Introduction

Cryptography is the foundation of information security theory. The traditional method of cryptanalysis mainly researches on stability of the algorithm which the cryptographic algorithm or protocol vulnerabilities are expected to find. However, there are some problems with this method like it's difficult to decipher passwords and needs a long time to analysis. Side-channel attack[1] uses the physical information[6] (power, electromagnetic, time, etc.) leaked from the running device rather than complex mathematical analysis of Cryptographic algorithm to decipher the key.

Power analysis attack uses the effective signals leaked from the running device to decipher the key. Depending on the method of analysis, it can be divided into a few categories like Differential Power Analysis[2,4](DPA) and Correlation Power Analysis (CPA). Correlation Analysis needs a smaller number of samples than Differential Analysis, avoids the occurrence of false peaks, and is accurate and efficient when decipher the key.

Based on the AES algorithm and Correlation Analysis Attack, this paper completes the CPA attack simulation pre and post S box, provides theoretical basis and experimental data for subsequent experiments and indirectly verify the nonlinear variation of S-box. we set up the experimental platform on the basis of the simulation to realize the CPA attack about AES cryptographic algorithm and encryption sub-key in first round of AES was successfully obtained.

Advanced Encryption Standard encryption algorithm

In Secret-key cryptography, the Advanced Encryption Standard(AES), also known as Rijndael, is a famous block-cipher too, which is designed by Joan Daemen and Vincent Rijndael. AES is a U.S. encryption standard that is developed essentially to be an alternative to the Data Encryption Standard DES. AES processes data using blocks of 128 bits length, and a variable secret key length(128,192or256 bits).Hence, as specified by the standard, three different block-ciphers can be used:AES-128,AES-192,AES-256. From the structural point of view, AES operates on a 4*4 matrix of bytes, usually referred to as the state. Each round of AES is composed of four stages, The structure of AES is shown as Fig. 1

Sub-byte: The Sub-byte modifies each byte in the state using an 8-bit substitution box, often called S-box. From the mathematical view point, Sub-byte function is a non linear operation.

Shift-Rows: The Shift-Rows rotates the bytes in each row of the state.

Mix-Columns: The Mix-Columns is a linear transformation that operates on the column of the state. Note that this transformation is omitted for the last round.

AddRoundKey: The AddRoundKey mixes the state with a sub-key. The sub-key is basically generated from the initial key (or the input key) using what we call key generator module.

Power point in this paper is Sub-byte in first round of AES, code as shown below.

```
void ByteSub( uint8 *state )
{ int i;
        for (i = 0; i < 16; i++)
   {
     state[ i ] = FSb[ state[ i ] ];
         }
   }
```

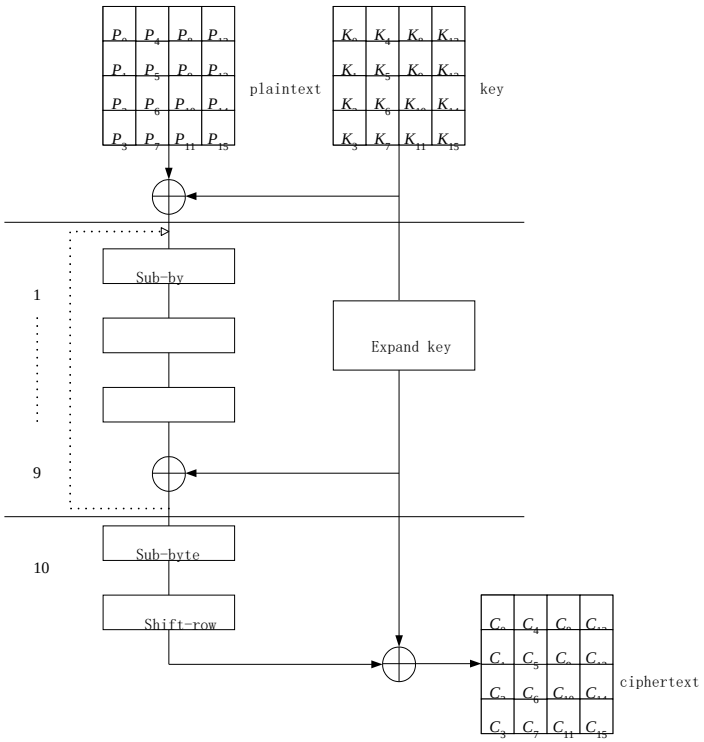

Fig. 1Encryption process of AES-128

Correlation power Analysis

A. Physical basis of CPA

CMOS has been widely used in integrated circuits, MCU. External manifestation of CMOS is encryption device need steady power supply during operation and result in power consumption; internal performance is flip between 0 and 1 of logic gates. Flipping cause charging and discharging of the load capacitance what result in power consumption of CMOS logic circuit. Getting in touch with key-related information via the power track during the operation. Establishing contact between Hamming-weight model and key then crack the key.

B. Power leakage model.

In the power analysis attacks ,It is need to establish energy leakage model. In this paper Hamming weight model is used to converted the intermediate value into energy consumption. In Hamming weight model, energy consumption and the current status of the CMOS integrated circuit are considered to be related directly. There is power consumption when the circuit is in a high state,

while in a low level there is not power consumption. In this case using Eq. 1 indicates the energy consumption:

$$E = aHW(x) + b \tag{1}$$

Where E represents the energy consumption of the circuit, X is a CMOS gate status, HW (x) is the Hamming weight of x, *a* represents the coefficient between energy consumption and Hamming weight, b stands for energy consumption of others processing and noise [5].

C. Correlation power analysis

In the Side-channel attack, we usually capture the power track when the cryptographic device is in the operation and crack the key information by using the latter statistical analysis. Based on the correlation power analysis[7] the ghost peaks can be effectively avoided which the mean difference method cannot. Therefore CPA is commonly used to get the key information. CPA has been recently proposed as innovative technique for watermarks detection mainly used for Intellectual Properties protection. Obviously, CPA continues to outsmart its competitors, and one can fear the excesses of this powerful tool in the context of Side-channel analysis.

The correlation coefficient is the most common method to determine the linear relationship between data. First, measure the cryptographic chip's actual energy consumption value when cryptographic is in the encryption status; Second, calculate the assumption power consumption based on the energy leakage model; Third calculate the correlation coefficients of both energy consumption and speculate critical information of the key based on the maximum correlation coefficient. The Formula is Eq. 2 r is the correlation coefficient between X and Y , Which ranges between -1 and 1. E and Var represent respectively the mean and variance. A lager value of $|r|$ means stronger linear relationship.

$$r_{x,y} = \frac{E(X \bullet Y) - E(X)E(Y)}{\sqrt{Var(X)Var(Y)}} \tag{2}$$

CPA attack can be divided into the following four steps:

step 1: Measure the leakage energy. Do cryptographic operations for multiple sets of plaintext and measure the actual leak energy of encryption devices. Using matrix T to presents the measured results. T=t_1,t_2,…,$t_{N,,}$ which N is the number of plaintext, t_i indicates the ith power track.

step 2: Calculate the value of hypothetic energy leakage. Select an intermediate value of the attacked device which must meet function $f(d,k)$ which *d* is known and *k* is a part of the key. For each possible k, calculate the corresponding intermediate value. According to D encryption operations and all the assume keys, we can obtain a matrix of size D*K. Finally, according to the energy leakage model, map the intermediate value matrix to the assuming energy consumption value matrix H.

step 3: Correlation statistical analysis. Compare the assuming energy consumption of each hypothesis key with the energy of each position then calculate the correlation. And obtain a matrix of correlation coefficient. r is calculated by the Eq. 3 $i = 1,2,\cdots,M;\ j = 1,2,\cdots,L$, $\overline{h_i}$, $\overline{h_i}$ is on behalf of the column means respectively.

$$r_{i,j} = \frac{\sum_{d=1}^{D}(h_{d,i} - \overline{h_i}) \bullet (t_{d,j} - \overline{t_j})}{\sqrt{\sum_{d=1}^{D}(h_{d,i} - \overline{h_i})^2 \bullet \sum_{d=1}^{D}(t_{d,j} - \overline{t_j})^2}} \tag{3}$$

step 4: Determine the correctness of the key. Plot with the correlation coefficient matrix R and obtain correlation coefficient curve of each key assumptions. The energy leakage assumptions of the correct key has the strongest linear relationship with certain column of actual energy consumption matrix and result the maximum.

D. Valuation techniques of correlation coefficients

Take the output of S-box as an attack target In the first round of AES , and simulate the energy consumption at that moment, which is the energy consumption in the position ct . Energy consumption is represented by the matrix consisting by column S_{ct} . All input(vector $d=(0,1,\cdots,255)'$ represents all the input)of attacked S-boxes mapped into the energy consumption of simulation which Energy consumption value of simulation is represented by the matrix H. According to the correlation formula，calculate correlation coefficients between each column of matrix H and S_{ct} then generate a matrix R. Lager value of r means better suitability between column of H_i and S_{ct} Based on the relationship recover the device's key. Figure 2 shows the effect of the attack.

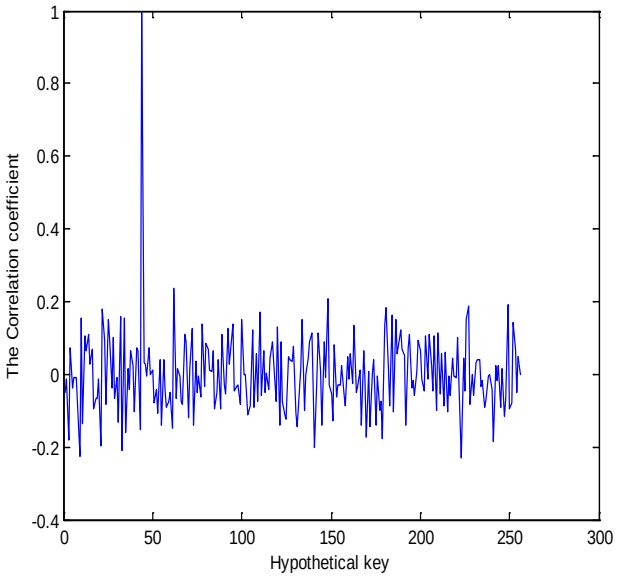

Fig. 2 CPA attack simulation in S-box of AES’s first round

In Fig. 2, The correlation coefficient of correct key assumption (k_{ct}=43) is 1 While other correlation coefficients are less than 0.2. There is no need to do actual attack on the correlation coefficient estimates which have research value to cryptographic equipment designers and attackers. Designers can evaluate the anti-attack capability of the device by estimating the correlation coefficients while attackers can use this technique to evaluate the attack effect and learn more about the internal structure of device.

Deformation on the basis of this attack, chose the input of S-box as the attack point.. Let $d=(0,1,\cdots,255)'$,using Hamming weight model generate simulation energy consumption then implement the CPA attack. Attack effect is as shown in Fig. 3 There is only one distinct peak in

Fig. 2and correlation coefficients are inversely proportional with the key and the Hamming distance in Fig. 3 There is only a little difference between the correlation coefficient of the correct key and the wrong one. Therefore, there needs amounts of energy traces if we want to find the difference in the actual experiments.

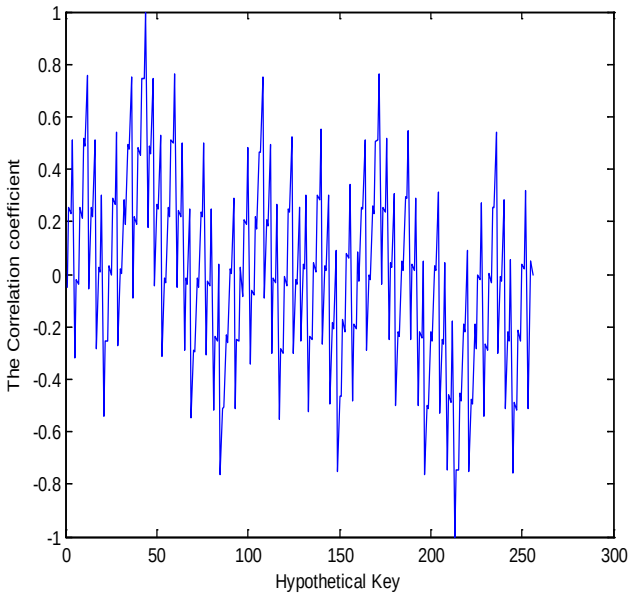

Fig. 3CPA attack simulation in xor of AES's first round

Through experimental comparison, it can be found that S-box makes the attack effect more distinct. This is because the S-box transformation is nonlinear. One different bit of input can result in more different bits of output. Even if the wrong key assumption only has one bit different with correct key, the output of S-box has a number of different bits values. Therefore the correlation coefficient of wrong key assumption is much smaller than the correct key assumption's correlation coefficient. Hence, the most effective point of CPA is selected in S-box of the first round or the last round.

CPA experiment for AES encryption algorithm

A. Experimental configuration

Platform mainly consists of four parts: Cryptographic chip, Digital oscilloscopes, personal computer and power supply. Figure 4 is the circuit diagram. Experiment realized on the AT89S52 microcontroller which crystal is 11.0592MHz. Use Tektronix DPO4032 oscilloscope (passive probe P6139A) to collect the leakage track. Random plaintext is provided to AT89S52 via RS232 interface and use LabView to write the virtual oscilloscope. Digital storage oscilloscope is control by the virtual oscilloscope to transport waveform data for pc and realize data collection automation.

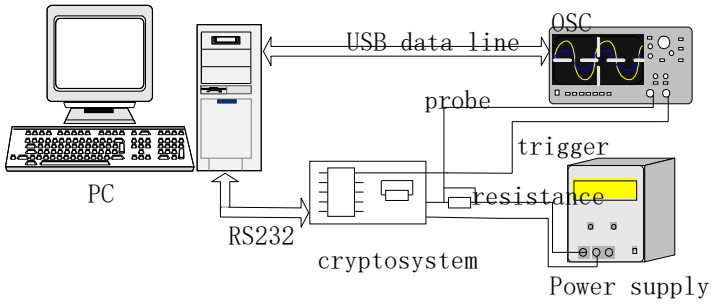

Figure 4 configuration of experimental platform

B. Attack Experiment for AES cryptographic algorithm

With the above power information collection platform, based on statistical analysis of the correlation method, AES encryption algorithm running microcontroller implementation of the CPA attack. Choose the first output of S-box of AES encryption algorithm in the first round as an intermediate value which is a function of the former eight of Plaintext and eight of key .To obtain the key, we need to guess 256 keys. Meanwhile, according to Hamming weight model, we take the Hamming weight which is assumed as the median value as the assumed power leakage.

At last, transmit the power track of digital storage oscilloscope to PC processing module and analysis correlation between the assumed power leakage and the actual leak value. The results of the statistical analysis is shown in Fig. 5.

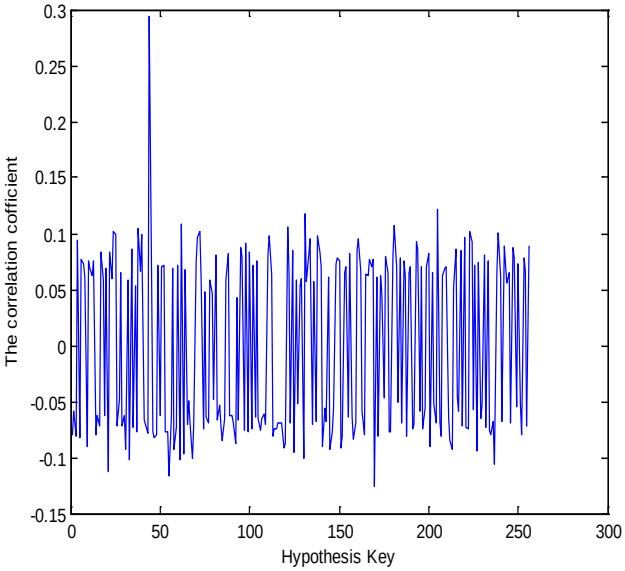

Fig. 5CPA attack in S-box of AES's first round

Fig. 5 shows the correlation coefficients of each key. There is a large number of electronic noise during the attack, so correlation coefficient is unlikely to be 1. There is a clear peak when k_{ck}=43 and the corresponding correlation coefficient is much larger than the other keys which is 0.2796. According to the principle of CPA attack， the key guess which is corresponding to an obvious peak is the right guess.

Conclusion

The results of CPA in Cryptographic chip AT89S52 showed that there is information disclosure running the Cryptographic chip. We got 5000 energy trajectory through the design capture platform and analyzed the leak of information with correlation analysis method. We got the correct key accurately and compared the difference between S-box and XOR. It confirmed the nonlinear transformation of S-box and analyzed the most advantageous power point of CPA attack. The next stage is started mainly from the XOR operation. Added noise signal on the basis of the simulation, compare coefficients at different points under different noise.

References

[1] KOCHER P C. Timing attacks on implementations of Diffie-Hell man, RS A,D SS, and other system[A]. N Koblitz, editor,CRYPTO[C].1996.104-113.

[2] Kocher P, Jaffe J, Jun B. Differential power analysis [G].LNCS 1666:Proceeding of CRYPTO(),Santa Bartara, California,USA, Springer, 1999:388-397.

[3] Stefan Mangard, Elisabeth Oswald, Thomas Popp. Power Analysis Attacks Revealing the Secrets of Smart Cards [M]. Springer,2007:97-100.

[4] Sauvage L, Guilley S, Mathieu Y. Elect romagnetic raditions of FPGAs: high spatial resolution cartography and attack of a cryptographic module[J]. ACM Transactions on Reconfigurable Technology and Systems,2009,2(1): 1-24.

[5] Canovas C, Clédière J J. What do S-boxes say in differential side channel attacks [EB/OL]. http://eprint.iacr.org/, Report 20085/311,2005.

[6] L. Batina, B. Gierlichs, E. Prouff, et al. Mutual Information Analysis: a Comprehensive Study[J]. Journal of Cryptology 24, 269-291, 2011.

[7] DPA Contest[EB/OL], http://www.dpacontest.org

[8] T. Eisenbarth, T. Kasper, A. Moradi, et al. On the Power of Power Analysis in the Real World: A Complete Break of the KeeLoq Code Hopping Scheme[C]. In CRYPTO 2008, volume 5157 of LNCS, pages 203-220. Springer, 2008.

[9] P.C. Kocher, J. Jaffe, B. Jun. Differential Power Analysis[C]. In CRYPTO 1999, volume 1666 of LNCS, pages 388-397. Springer, 1999.