Advanced Science and Technology Letters
Vol.38 (Embedded Ubiquitous 2013), pp.40-43
http://dx.doi.org/10.14257/astl.2013.38.09

An Experimental CPA Attack for Arduino Cryptographic Module

Young Jin Kang[1], Jung Bok Jo[2], Tae Yong Kim[2], Hoon Jae Lee[2]
[1]Department of Ubiquitous IT, Graduate School of Dongseo University,
Sasang-Gu, Busan 617-716, Korea
rkddudwls55@gmail.com,
[2]Division of Computer and Engineering Dongseo University
Sasang-Gu, Busan 617-716, Korea
hjlee@dongseo.ac.kr

Abstract. The importance of this emerging information security and u-Korea or ubiquitous IT era, and the information security is more important. Especially, the small core device password encryption algorithm is an important part of the secure side channel attack cryptographic algorithms. However, it can provide high level of security, an adversary can attack small core device through implementation of cryptographic algorithms. In this paper, we explain about the correlation power analysis attack, which is the most dangerous type of side channel attack. Also, we implemented and experiment this attack. In our experiment, we used ATmega cryptographic module to configure and the oscilloscope to obtain the experimental result, and MATLAB program for the verification process.

Keywords: Side-Channel Attack, AES, CPA, Arduino module

1 Introduction

The Side-Channel Attacks method proposed by P.Kocher encryption algorithm, the encryption process is not a theoretical vulnerability from leaking timing information, power, and electromagnetic signals to use the method of attack. Also Small device password and encryption algorithms can be the core, and the password is an important part of the security of the algorithm. By attacking the encryption algorithm key value is to steal sensitive information, such as exposure to acts, especially one of the most powerful side channel attack, power analysis attacks, which are under threat in attack [1].

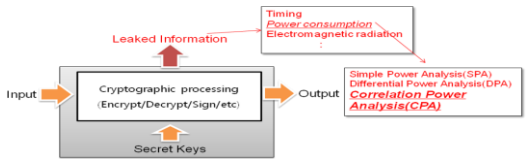

Fig. 1. The side channel for general encryption processing.

ISSN: 2287-1233 ASTL

Encryption / decryption in hardware signatures, and to perform any action, saying the leaked information; the information that is leaked by the attack technique is called side channel attacks [2].

2 Experimental and analytical CPA attack

Connect with Pc to collect the signal of estimated power consumption. And then connect the Pc also with small size of crypto graph to operate it.

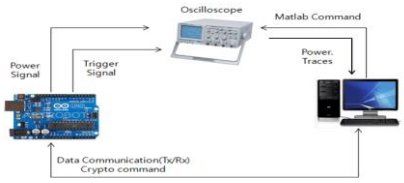

Fig. 2. Test device configuration

2.1 Measuring power consumption signal and Key generation guess

By using over one thousand of different plaintext, we measure consumption of the power signal that is over one thousand. A picture above is measured trigger signal that is indicating the moment of operation of the AddRoundKey function.

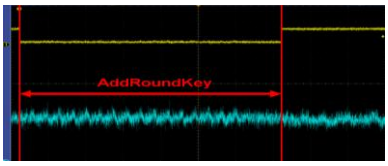

Fig. 3. Perform AddRoundKey function at this point, the power consumption of the signal

Using a plaintext with speculation is to generate the key. P_{ji} is called the plaintext, j is number of plaintext, i is its byte position, P_j for each of the i(th) value of the key AddRoundKey if at all possible, operation by performing a guess that generated the key table [3].

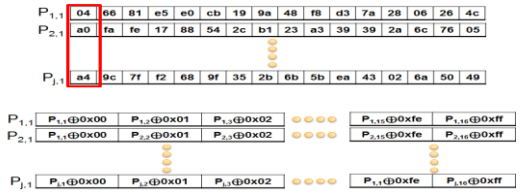

Fig. 4. Guess key generation process

Generated guess key table Hamming weight model estimated using a table of values to generate electric power. Hamming weight power model is a model that has different size of power depending on the number of 0 and 1 of certain value that passes data bus. It has higher power consumption according to the number of 1 and also has smaller signal as it has more 1. The following figure represents the Hamming weight model, equation (1) to guess key in order to change the equation represents the Hamming weigh model [4].

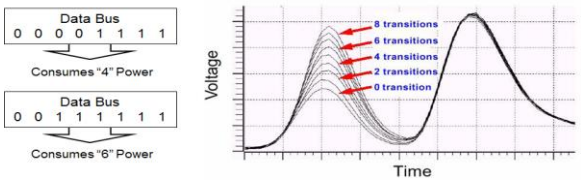

Fig. 5. Hamming weigh model

$$HW(P_{j,i} \oplus (00...255)) \tag{1}$$

2.2 Correlation coefficient calculation

2.1 With the measurements and using the value generated by the corrcoef operation to perform the correlation coefficient. Equation (2) shows the corrcoef arithmetic expression.

$$R(i,j) = \frac{C(i,j)}{\sqrt{C(i,i)C(j,j)}} \tag{2}$$

2.2 corrcoef operation power generated by the estimated value of H, the table, the h_j i votes can be present. h_j, i is 1 if the i plaintext 0x00, P_j, 1 and the XOR operation is the value, i guess that the attack can be called key values. Collected for each I dissipation power signal for the entire operation is performed, and corrcoef calculate the correlation coefficient.

2.3 CPA attack experimental results

Through the calculated Correlation coefficients, we can check the result of experiment of mock attack. As you can see the picture below, peak has occurred that means there is a correct key. If we check the key when the peak has been occurring, we would be able to find which key is the secret key.

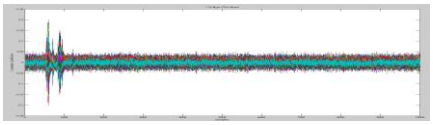

Fig. 6. The first 1 bytes of all of the key values of attack

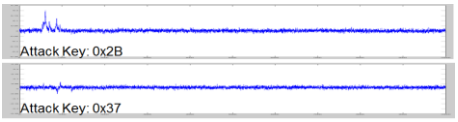

Fig. 7. The first 1 bytes in the attack on key 0x2B, 0x37 the result of an attack

Among the true secret key of which made up small cryptographic module, the value of first byte is 0x2B. Same as the second picture above, if the attacking key is 0x2B, we can see the Peak, if is 0x37, we cannot see the Peak. Also Peak can be seen some other values though, the possibility is lower that key is the true one.

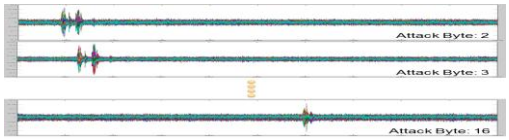

Fig. 8. 2 – 16bytes the correlation coefficient graph

3 Conclusion

Current side-channel attacks, the vulnerability of the system to find the attack has been recognized as a realistic attacks, such as a secure password-based system which is used as a good tool for building. In this paper, AES [5] cryptographic algorithm used in a small crypto device is vulnerable to CPA attacks was proved. The study of software-based countermeasure for CPA attack is expected for the future work.

Acknowledgement: This work was supported by the Brain Busan 21 Project in 2013, and this research was also supported by Basic Science Research Program through the National Research Foundation of Korea(NRF) funded by the Ministry of Education, Science and Technology. (grant number: 2013-071188).

References

1. Young-Jin Kang, Jeong-Bok Jo, Hoon-Jae Lee, “Technical Analysis for the corresponding side-channel attacks”, proceeding on domestic conference of KIICE, vol. 17, 2013.
2. HoonJae Lee et al., “A Study of attack prevention techniques for Crypto-processor”, Technical report of NSRI, 2011
3. Wiliam Hnath, “Differential Power Analysis Side-Channel Attacks in Cryptography”, April 29 2010
4. Young Goo Park, “Power Analysis Attack on Secure Devices using Time Alignment”, Doctoral Thesis, 2012
5. AES cryptographic algorithm @http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf