International Journal of Security and Its Applications
Vol.8, No.2 (2014), pp.261-270
http://dx.doi.org/10.14257/ijsia.2014.8.2.27

An Experimental CPA attack for Arduino Cryptographic Module and Analysis in Software-based CPA Countermeasures

Young Jin Kang[1], Tae Yong Kim[2], Jung Bok Jo[3] and Hoon Jae Lee[4]

[1]*Department of Ubiquitous IT, Graduate School of Dongseo University, Sasang-Gum Busan 617-716, Korea*
[2,3,4]*Division of Computer and Engineering, Dongseo University, Sasang-Gum Busan 617-716, Korea*
[1]*rkddudwls55@gmail.com,* [4]*hjlee@dongseo.ac.kr*

Abstract

Side channel attacks are attacks that are based on "Side Channel Information". Side channel information is information that can be retrieved from the encryption device that is neither the plaintext to be encrypted nor the cipher text resulting from the encryption process. Side-channel attacks are easy-to-implement whilst powerful attacks against cryptographic implementations and their targets range from primitives, protocols, modules, and devices to even systems. These attacks pose a serious threat to the security of cryptographic modules. In consequence, cryptographic implementations have to be evaluated for their resistivity against such attacks and the incorporation of different countermeasures has to be considered. 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 using ATmega cryptographic module for configuration and the oscilloscope to obtain the experimental result, and MATLAB program for the verification process and design technology to analyze countermeasures.

Keywords: *Side-Channel Attack, Software Based Countermeasure, CPA attack, Masking*

1. Introduction

Side-Channel Attacks The proposed method of attack by P.Kocher encryption algorithm encryption process and not a theoretical vulnerability from leaking timing information, power, electromagnetic signals to use the method of attack. Also be magnified the importance of information security is being, era of u-Korea or ubiquitous IT the information security is more important, and popularization of the small cryptographic device is in the trend. 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 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 [2].

ISSN: 1738-9976 IJSIA

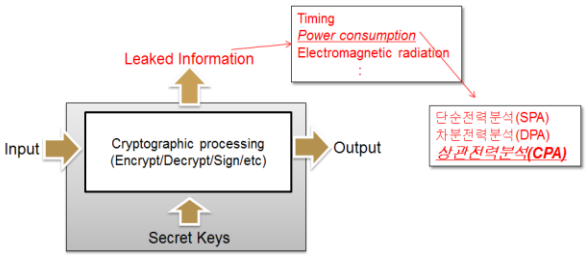

Figure 1. The Side Channel for General Encryption Processing

The information leaked by power consumption of the simple power analysis attacks (SPA), Differential Power Analysis (DPA), correlation power analysis (CPA) technique, and correlation power analysis technique that is 8 bits at a time, one resulted by adding 1 byte attacks, and these attacks have been implemented or how the algorithm can be applied, depending on the environment is an attack technique [4, 10]. In the recent research in the technology to correspond to the encryption device and the unit of data processed by the correlation between the channel signal, Removing Masking, Blinding, Randomization and Hiding Technique are implemented.

This paper presents the review of small channel attacks on security devices which are classified as the most threatening attacks in the correlation power analysis (CPA: Correlation Power Analysis) techniques, and also for the actual attack ATmega (ATmega328P-PU). This paper also present the review of the password used by the cryptographic module algorithm which is the AES-128 (AES: Advanced Encryption Standard) with a MATLAB program and it is configured by the oscilloscope's correlation power analysis which is used experimentally that verify the vulnerabilities, and attacks against the corresponding response technology software.

2. AES Algorithm Model CPA Attack

AES [7] as the U.S. federal standard algorithm is a symmetric key block cipher method. Block length of 128 bits and key length is used with a choice of 128,192,256 bits, Belgium in 2000 by adopting cryptologist developed Rijindeal has been used. AES algorithm is AddRoundKey, SubBytes, ShiftRows, MixColumns function consists of plain text is entered, as shown in Figure 2, the function is performed AddRoundKey SubBytes, ShiftRows, MixColumns, AddRoundKey the function being performed 9 times 9 rounds after operation ShiftRows, MixColumns, AddRoundKey first-round action function operates a total of 10 rounds. The key used in the operation through the Key Schedule will be used at the next plaintext block to generate a key.

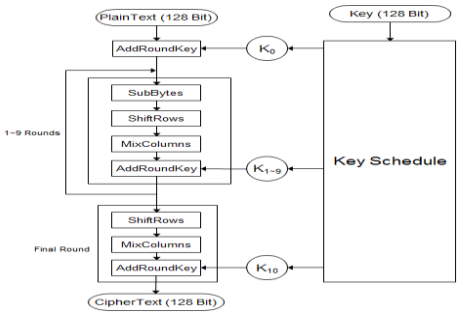

Figure 2. AES Algorithm

2.1. Time of the Attack Function

In this Section, We set the moment of attacking as AddRoundKey is started running. AddRoundKey is fulfill Plaintext and secret key it is set as a model of attacking because when XOR is started to operate, Plaintext P, a secret key K, AddRoundKey results S, Byte of the i, can be expressed.

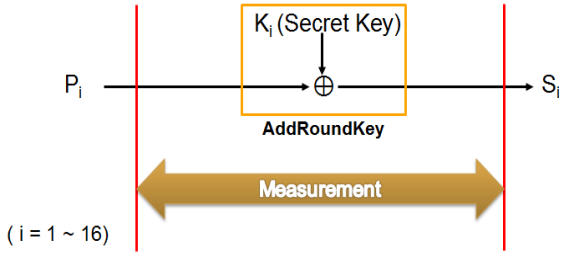

Figure 3. AddRoundKey Function

The display of the measurement XOR operation occurs, the power consumption and the result of an operation is stored as S_i that occurs when power consumption P_i K_i, depending on the state of the consumes much less power at this point because they have different models of attack using the model.

3. Using ATmega Cryptographic Module Configuration

For the actual attack ATmega (ATmega 328 P – PU) [8] Arduino Uno [9] equipped with a password using the modules, and AES algorithm applies. I saw this in the paper, the test for when an attack AddRoundKey functions to implement and behave, first round. To measure the power consumption consumed by ATmega in Arduino Uno board, connect friction R additionally between No 8 pin (GND) and Arduino Uno board as a picture shows above. The resistance value is ATmega needed to work voltage limit is not possible in the large values. We can use Oscilloscope to measure probe at the location of ②. ① is trigger signal that will be generation while AddRoundKey is running, to measure it, we connect probe at the location of ①.

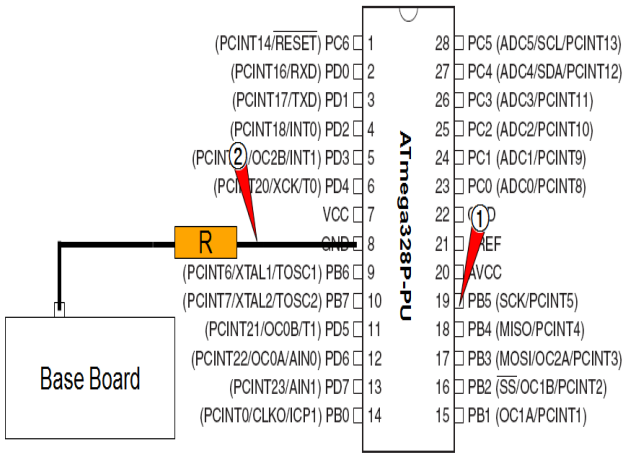

Figure 4. ATmega P-PU GND Power in the Signal Extraction

4. Experimental and Analytical CAP Attack

We connect cryptographic module as the picture above. 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.

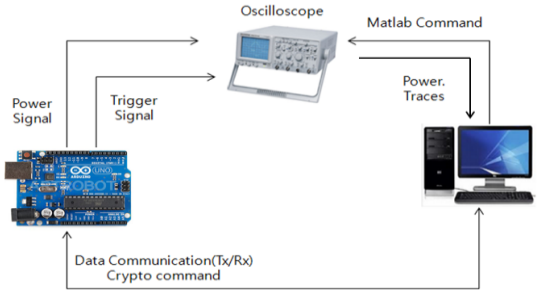

Figure 5. Test Device Configuration

4.1. 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.

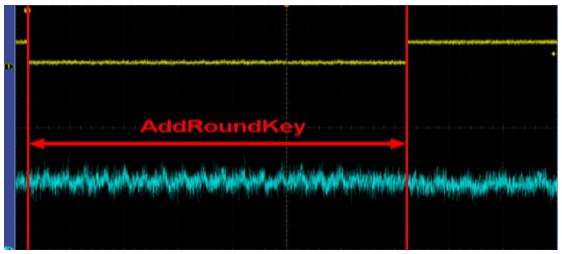

Figure 6. Perform AddRoundKey Function at This Point, the Power Consumption of the Signal

Using a plain text with speculation is to generate the key. P_{ji} is called the plaintext, j is number of plaintext, i say 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].

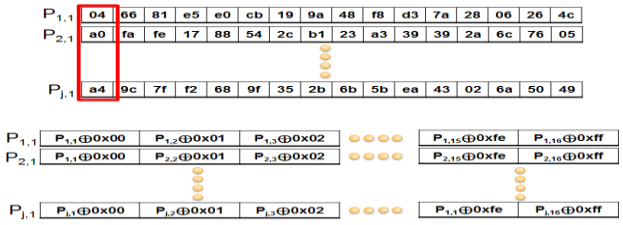

Figure 7. Guess Key Generation Process

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 depends on the number of 0 and 1 of certain value that passes data bus. It has bigger power consumption according to the number of 1 and also has smaller signal as it has more 1. The following represents the Hamming weight model, equation (1) to guess key to change the equation represents the Hamming weigh model [5].

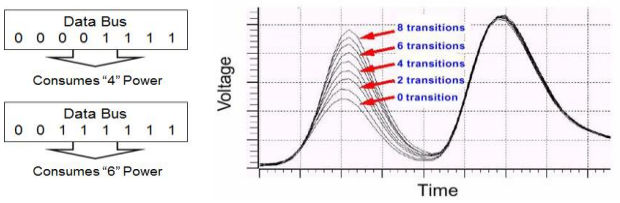

Figure 8. Hamming Weigh Model

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

4.2. Correlation COEFFICIENT CALCULATION

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

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

4.2 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.

4.3. 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.

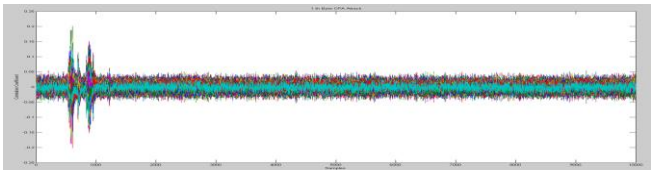

Figure 9. The First Bytes of all of the Key Values of Attack

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.

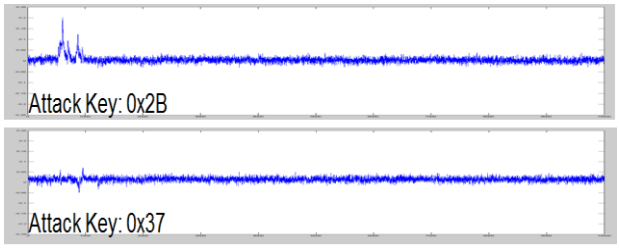

Figure 10. The First Bytes in the Attack on Key 0x2B, 0x37 the Result of an Attack

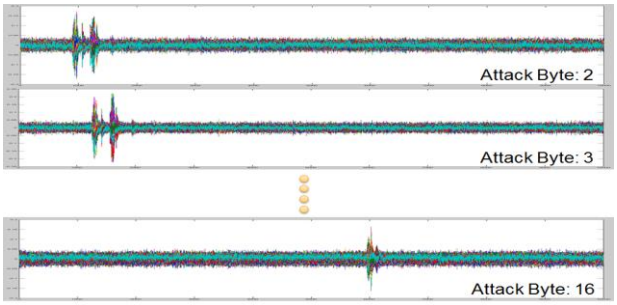

Figure 11. 2 – 16bytes the Correlation Coefficient Graph

5. Software-based Countermeasures

Until recently the corresponding techniques research password on your device data and side-channel signals are processed to remove the correlation between the measures and Goubin the following general strategy was introduced.

- Run time to move randomly, waiting to put the command to insert fake, randomly running operations in the execution of cryptographic algorithms, such as the value of the correlation of the output trace is removed.
- Important to analyze the assembler instructions to make it harder to replace it with another command, Shem and memory circuit redesign is an important move.
- Data or the key to have a different value each time it is used the password that is used to modify the algorithm of the primitive attacks are made that difficult [6].

In general function of AES AddRoundKey 0-15, to witr 1-16 bytes sequentially perform the operation. However, the random sequence of operations performed by a large number of plaintext using statistical power analysis attacks more difficult this will be. Next create array that saved the location of each byte.

INDEX[1]	8	6	3	5	12	2	16	4	7	10	13	1	15	9	11	14
INDEX[2]	15	2	3	5	7	12	14	16	11	8	10	4	6	9	11	1
INDEX[3]	4	5	6	8	2	1	3	12	15	13	16	11	10	9	7	14

Figure 12. Sequence Table of the Location of Byte

After selecting sequence table randomly by using the function, operate in order of value in the table. For instance, as you can see a picture below, if INDEX (1) is selected, the following operating sequence will be made

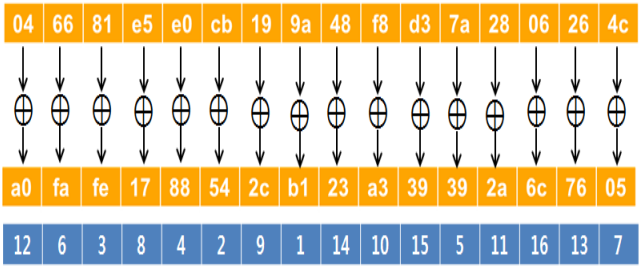

Figure 13. Random Sequence of Operations Illustrated

This and the following pictures are coded.

```
void addRoundKey() {
  randomSeed(analogRead(0));
  index = (int)random(0,2);
  int i2 = 0;
  for(int i=0; i<16 ;i++) {
    i2 = RandomIndex[index][i];
    state[i2] = PText[i2] ^ Key[i2];
  }
}
```

Figure 14. Apply Random Operation Code

```
void shiftRandomIndex() {
  int temp;
  temp = RandomIndex[index][0];
 for(int i = 0;i<14;i++) {
  RandomIndex[index][i] = RandomIndex[index][i+1];
 }
 RandomIndex[index][15] = temp;
}
```

Figure 15. Sequence Shift Function Code Table

The corresponding technology is the same in other functions, can be applied. In addition, when used with other functions do not need to continue to generate random values from an array to get the hours of operation time, except for the change that has the advantage. Only by changing the order of operations only, the corresponding cipher text and the difference between the previous techniques do not apply the transmit and receive side, all without the use of the corresponding technology using one side only, even if the problem does not occur.

10. Conclusion

Current side-channel attacks are being used in the academic research to exploit the vulnerability of the system. Those attacks have been recognized as realistic attacks, when it comes to break a secure password-based system. In this paper, we have used AES cryptographic algorithm implemented in a small crypto device. The experiment has revealed that, this kind of device is vulnerable to CPA attacks by applying technologies corresponding CPA where proofs have been given that the software attack was difficult. Therefore the corresponding technologies have been applied without increasing hardware cost of cryptographic algorithms. Thus, an implementation of that method of attack without significant performance degradation in a small crypto device based defense power analysis attacks can be applied. However, the current techniques in response to one of the main problems of response technique, when encryption algorithms for safety assurance, and response techniques when applied to two or more existing password encryption algorithm is applied to a module of performance than might actually impossible to use. In the near future, corresponding method of the performance degradation that can prevent a new side-channel for securing the core technology is thought to be urgent

Acknowledgements

This research was 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) and it also supported by the BB21 project of Busan Metropolitan City.

References

[1] Y. Jin Kang, J. Bok Jo, T. Yong Kim and H. Jae Lee, "An Experimental CPA Attack for Arduino Cryptographic Module", Proceedings of International Workshop, Embedded and Ubiquitous Engineering, Jeju Island, Korea, (**2013)** December 11-13.
[2] Y.-J. Kang, J.-B. Jo and H.-J. Lee, "Technical Analysis for the corresponding side-channel attacks", Proceedings on domestic conference of KIICE, Korea, vol. 17, **(2013)**.
[3] W. Hnath, "Differential Power Analysis Side-Channel Attacks in Cryptography", **(2010)** April 29.
[4] H. Jae Lee, "A Study of attack prevention techniques for Crypto-processor", Technical report of NSRI, **(2011)**.
[5] Y. G. Park, "Power Analysis Attack on Secure Devices using Time Alignment", Doctoral Thesis, **(2012)**.
[6] L. Goubin, "A Refined Power-Analysis Attack on Elliptic Curve Cryptosystems", PKC LNCS 2567, **(2003)**, pp. 199-211.
[7] AES cryptographic algorithm @http://csrc.nist.gov/publications/fips/fips/fips197/fips-197.pdf.
[8] ATmega128 microprocessor @www.atmel.com/Images/doc2467.pdf.
[9] Arduino module @http://www.arduino.cc/.
[10] P. Kocher, J. Jaffe and B. Jun, "Differential Power Analysis", Proceedings of Advances in Cryptology, CRYPTO '99, Springer-Verlag, **(1999)**, pp. 388-397.

Authors

Young Jin Kang, received the B.S in Electrical Engineering from Dongseo University in Korea 2013. His research interests are in the security topics of Side-Channel Attack (SCA) and Network Security.

Tae Yong Kim, received the B.S in Electrical Engineering from Fisheries University in 1993. And M.S, Ph.D in Electrical Engineering from Okayama University in 1997, 2001. Since 2002 he has been working for Department of Computer Engineering of Dongseo University as an associate professor, and now he is a full professor.

Jung Bok Jo, received his B.S in Electrical Engineering from Kyungpook national University in 1978 and received M.S in Electrical Engineering from Yeungnam University in 1986 and received ph.D in Electrical Engineering form Tokyo Metropolitan Science and Technology University in 1996. And Since 1993 he has been working for Department of Computer Engineering of Dongseo University as an associate professor, and now he is a full professor.

Hoon Jae Lee, received the B.S., M.S. and Ph.D. degree in Electrical Engineering from Kyungpook national university in 1985, 1987 and 1998, respectively. He had been engaged in the research on cryptography and network security at Agency for Defense Development from 1987 to 1998. Since 2002 he has been working for Department of Computer Engineering of Dongseo University as an associate professor, and now he is a full professor. His current research interests are in security communication system, side-channel attack, USN & RFID security. He is a member of the Korea institute of Information security and cryptology, IEEE Computer Society, IEEE Information Theory Society and etc.