A NOBEL KEY-SEARCH METHOD FOR SIDE CHANNEL ATTACKS BASED ON PATTERN RECOGNITION

You-Seok Lee[*], *Yong Je Choi*[**], *Dong-Guk Han*[**], *Ho Won Kim*[**], *Hyoung-Nam Kim*[*]

[*]Dept. of Electronics and Electrical Engineering
Pusan National University, Busan, Korea {hnkim@pusan.ac.kr}
[**]Electronics and Telecommunication Research Institute (ETRI), Daejeon, Korea

ABSTRACT

Differential Power Analysis (DPA) has been known as an efficient attack for finding secret keys of cryptosystems but its efficiency may be lowered due to the misalignment of the acquired signals. Though the misalignment problem has been now solvable by various successful approaches in DPA, a lot of power traces are still required to find correct keys. Since the required number of power traces is directly connected with the efficiency of SCAs, we propose a key-search method even with relatively reduced number of power traces based on recognizing special patterns of the signal caused by cryptographic operations. Experimental results show that the proposed method is able to search correct keys with much smaller number of traces than the minimum number of traces with which the conventional methods of the energy-based DPA and frequency-based DPA succeed in finding keys.

Index Terms— Correlation, cryptography, power consumption, security, signal detection.

1. INTRODUCTION

Side channel Attacks (SCAs), which exploit physical information leaked during the operation of a secured device, seem to be implementation attacks against cryptographic algorithms, rather than attacks for theoretical weaknesses. The physical parameters include timing, power consumption, and electromagnetic emanations. Power consumption information has been commonly used for SCAs, such as in Simple Power Analysis (SPA) [1], Differential Power Analysis (DPA) [2] and Correlation Power Analysis (CPA) [3]. Electromagnetic radiation signals can be also used instead of power dissipations, the corresponding methods to which are Simple ElectroMagnetic Analysis (SEMA) and Differential ElectroMagnetic Analysis (DEMA) [4], [5].

Although SCAs are powerful cryptanalysis techniques, the attack efficiency can be degraded by noise added to side channel signals and misalignment mainly caused by measurements. The misalignment is a crucial problem for successful SCAs. To overcome this misalignment problem, the energy-based DPA [6] and the frequency-based DPA [7] have been proposed. While these methods provide efficient solutions, lots of power traces are still required to detect correct keys. Because the power traces depend on diverse operations which constitute complex devices as well as the cryptographic operations, the increase of the required number of traces is unavoidable to suppress the effects associated with the operations unrelated to encryption. As a result, the attack efficiency cannot but degrade. To cope with such undesirable degradation and improve the efficiency of the attacks in terms of required minimum number of traces, we find special patterns of the signal caused by cryptographic operations and then propose a key-search method based on the signal patterns.

This paper is organized as follows. In section 2, DPAs, which recently have drawn much interest in SCAs, are introduced. Section 3 describes a proposed key-search method of using special signal patterns associated with cryptographic operations to improve the efficiency of SCAs. Experimental results are shown in section 4 to verify the superiority of the proposed method over the original energy-based DPA and frequency-based DPA. Section 5 concludes the paper.

2. DIFFERENTIAL POWER ANALYSIS

The differential power analysis (DPA) attack, which was originally proposed by Kocher et al. [2], is one of the most popular attacks associated with power analysis. The basic idea of the DPA is that the power consumption for manipulating one bit to "1" is different from the power consumption for manipulating it to "0."

To implement the DPA attack, an attacker first observes M encryption operations and captures M power traces comprising of N samples per each operation. In addition, the attacker records M ciphertexts or M plaintexts. To test whether the guessing key K_S is correct, the attacker

This work was supported by the IT R&D program of MIC/IITA. [2005-S-088-03, Development of Security technology for Secure RFID/USN Service] and the 2nd-Phase Brain Korea (BK) 21 Program funded by the Ministry of Education, Korea.

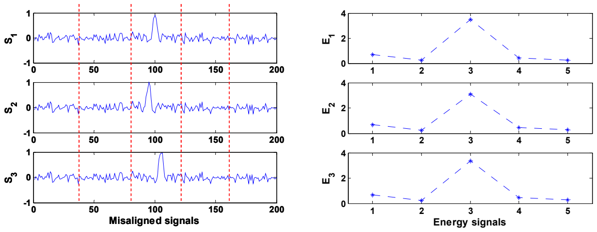

Fig. 1. Misaligned signals (left) and energy signals (right).

computes an N-sample differential trace $\Delta_D[1,\ldots,N]$ by calculating the difference between the average of the traces for which the DPA selection function $D(P,b,K_S)$ is 1 and the average of the traces for which $D(P,b,K_S)$ is 0, where P is the plaintext and b denotes handling bit position. When the guessing key is correct, a peak is appeared in the differential traces at one instant τ, which is called as a DPA peak. For incorrect keys, all N values of the differential trace tend to be 0 or no significant peak appears. One should note that the DPA peak clearly appears only when the power traces handled at the same instant τ for all tested keys. If the traces are not aligned, the magnitude of the DPA peak can be reduced and the attack must be disturbed.

Hence the misalignment of the traces may be a lethal problem to the use of the DPA. If peaks are slightly out of alignment in time, they will be cancelled out rather than be reinforced when averaging in DPA. To solve the misalignment problem in DPA signals, the energy-based DPA [6] and the frequency-based DPA [7] have been established.

2.1. Energy-based DPA

The misalignment of side channel signals can be observed by distinct peaks in the mean curve of captured traces. If the range of the dispersed peaks is so small that can be included in one segment, the energy of the signal in the same segment does not vary with the peak position. The energy-based DPA uses this remarkable point to perform a “resistant-misalignment” DPA attack. The energy-based DPA consists of dividing the original signal into same-length segments and computing the energy of the signal corresponding to each segment as described in Fig. 1. Then, these energy signals are used for the DPA signals instead of the original ones [6].

2.2. Frequency-based DPA

The frequency-based DPA uses a frequency-domain signal instead of a time-domain one. Analyzing the side channel signals in frequency domain solves the problem of misalignment in traces since the time-shift of the time-domain signal is not appeared in the magnitude of the frequency-domain signal. A frequency-domain threshold is used for acquiring the important part of the DPA peaks in the differential signal. Only the differential peaks that exceed a constant multiple of the threshold are used for finding keys. [7].

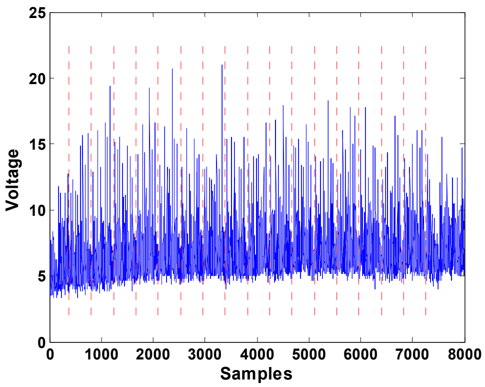

Fig. 2. Power trace measured during 16 S-box operations.

3. REDUCION OF THE REQUIRED NUMBER OF POWER TRACES

Cryptographic operation has been commonly performed in various systems with complicated components, such as a personal digital assistant (PDA) or network devices. The power signals measured from these systems depend on diverse operations as well as the cryptographic processing. As the power caused by other operations unrelated to the cryptographic operation becomes large, the efficiency of SCAs may be more disturbed. Even though the noise and temporal misalignment problems can be solved by some successful methods [6], [7], SCAs still require a lot of power traces to diminish the effects associated with the unwanted operations. Since the required minimum number of power traces is directly related to the attack efficiency, how to reduce the number of power traces has been a hot issue in improving the attack efficiency. As one of methods to achieve this goal, we propose a key-search method even with relatively small number of power traces based on recognizing special signal patterns associated with cryptographic operations.

Fig. 2 is one example of power traces captured during the encryption by 16 S-boxes in the sensor network device based on the Advanced Encryption Standard (AES). One can find easily 16 discernable parts corresponding to 16 S-box operations. To find each key used in each S-box, it is reasonable to employ respective corresponding portion of the power consumption signals. Unfortunately, since each portion includes impure ingredients caused by unrelated operations to the encryption, it is inevitable to increase the number of traces to minimize the effects of the unwanted operations. It may be therefore effective, if possible, to extract the signal component associated only with each S-box operation. One possibility lies with the 16 discernable parts which may include a special signal pattern caused by

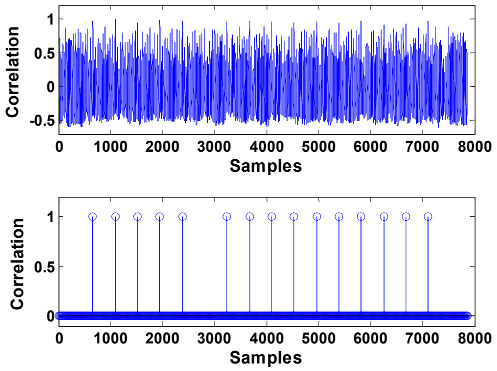

Fig. 3. 16 S-box operation points obtained by correlation.

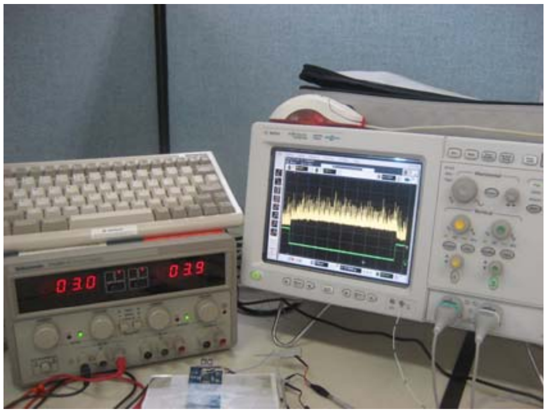

Fig. 4. Experimental setup with an oscilloscope, a power supply and a wireless sensor network device of mote IV.

each S-box operation. Noticing that all the discernable parts have almost the same length, the periodicity buried in the signal can be easily found by performing correlation. This is a basic idea to trigger our proposed method.

To detect the special signal pattern in the power traces, it is required to find an appropriate reference template. The starting point of the template can be determined as follows. At first, we select one in 16 discernable parts and assign it as a reference template with *L*-length samples. Then, we compute the correlation between the power trace and the selected template. We find the points of which correlation values have more than 90 % similarity and check the periodicity of those points. If any periodicity is not found, we repeat the above checking process with the reduced-length reference template. The reduced length is determined by the sampling frequency and the data bus speed. A realistic example for these procedures will be given in section 4. To reduce the computational complexity, further checking with the more reduced-length template may be useful even when we already find the periodicity because the shortened template is also related with the computation of correlation in other traces. The correlation results obtained with the 144-length template are shown in the top of Fig. 3 and the correlation values which pass over 0.9 are appeared in periodically in the bottom. Through these procedures, we can detect the operation points caused by each 16 S-box. Although the detected operation points are only 15, the blank point can be estimated by using the periodicity of the S-box operation. Then, we employ only a portion of the power traces with the same length of the final template corresponding to each S-box operation for SCAs to find the correct keys instead of full length of traces including unrelated operation to the S-box operation. Since only S-box operation-dominant peaks inside the signal is involved in SCAs, we may find secret keys with much smaller number of power traces than the conventional DPAs.

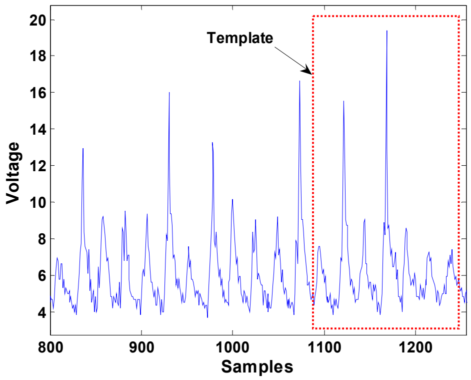

Fig. 5. A power trace of the second S-box operation and the template used in experiment.

4. EXPERIMENTAL RESULTS

In order to evaluate the efficiency of the proposed method, we measured the power consumptions of a wireless sensor network device of “mote IV” during the first round of an AES operation. The experimental setup is shown in Fig. 4. We acquired power-consumption traces with a sampling frequency of 200 MHz corresponding to each random plaintext input. Since the bus speed is 8 MHz, peaks are to appear every 25 samples. In our experiment, however, the peaks appeared every 24 samples because of the inaccuracy of the devices used in our experiment. Fig. 2 shows one example of captured power traces. The number of the samples comprising one S-box operation was about 430. Accordingly, the length of the first template was 432 which is the nearest multiple of 24 to 430 and the step-size of the template length was 24. The length of the template was determined by a minimum value satisfying the periodicity with the given starting point which correlation values at that point are over 0.9. In our experiments, since the correlation values which pass over 0.9 periodically appeared when the lengths of the template were 264, 240, 216, 192, 168, and 144, we selected a 144-length template. The starting point obtained by the template is shown in Fig. 5. With this template we found the starting point corresponding to each S-box operation, which is given in Fig. 3 and Table I. The special signal patterns similar to the selected template

TABLE I
STARTING POINTS CORRESPONDING TO EACH S-BOX OPERATION OBTAINED BY THE PROPOSED METHOD

S-box	Starting Points	S-box	Starting Points
1	659	9	4096
2	1087	10	4530
3	1521	11	4958
4	1949	12	5387
5	2377	13	5815
6	(2807)	14	6249
7	3239	15	6677
8	3688	16	7106

TABLE II
MINIMUM NUMBER OF THE TRACES FOR SUCCESSFUL ATTACK

S-box	Energy-based DPA		Frequency-based DPA	
	Original	Proposed	Original	Proposed
1	Fail	1300	Fail	400
2	Fail	1000	800	200
3	3100	300	Fail	100
4	2500	600	1000	300
5	Fail	600	Fail	400
6	Fail	1100	Fail	400
7	Fail	300	Fail	200
8	Fail	400	1300	300
9	Fail	300	Fail	500
10	Fail	400	Fail	400
11	Fail	400	Fail	200
12	2700	200	900	300
13	Fail	500	Fail	500
14	Fail	800	Fail	300
15	Fail	200	Fail	200
16	1500	400	500	300

periodically appeared every about 430 samples. The sixth point was estimated by adding 430 to the value of the fifth point. In each S-box operation interval of 430 sample, the starting point appeared at about 280th sample in each S-box interval. This means that the useful information for SCA exists between about 280th sample and 423th sample. Therefore we used only these 144 samples corresponding to each S-box in all traces for attack.

The energy-based attack and the frequency-based differential analysis were employed to verify the efficiency of the proposed method with 4,000 power consumption traces based on the AES. For the AES, there are eight output bits of b available for the selection function of $D(P,b,K_S)$. We chose a final key among eight keys corresponding to the eight-output bits by the majority voting rule. To adopt the energy-based DPA, we manually realigned the peaks using the correlation as described in [6]. The segment for computing energy signal was composed of 24 samples. For the frequency-based DPA, FFT size was 512 and the multiple number of the threshold value to acquire the significant peak was 4, which was obtained by extensive experiments.

Table II provides the required minimum traces to find the correct keys based on the energy-based attack and the frequency-based attack with and without the proposed method. The step-size of the number of the traces was 100. Although the energy-based DPA and the frequency-based DPA may be efficient solutions for misalignment, they failed to search the keys even when 4,000 power traces were used. Adopting the proposed method, however, dramatically improved the efficiency of the attack. The proposed method reduced the required number of traces to find all the keys by 1,300 traces for the energy-based DPA and 500 traces for the frequency-based DPA. The result that the minimum number of traces required to detect the correct keys for the energy-based DPA was larger than that of the frequency-based DPA is because that segment energy is sensitive to how to divide segments and it was not clear to assign a starting point of one segment in our experimental data.

5. CONCLUSIONS

We proposed a novel key-search method to improve the efficiency of side channel attacks (SCAs) based on differential power analysis (DPA) by finding a special pattern of the power signals associated with the cryptographic operations. The DPA based on the proposed method finds the correct keys with much smaller number of side channel signals than the conventional attacks do.

While SCAs have not been studied in the field of signal processing, we opened a new possibility to improve security techniques even with a very simple idea of finding a special signal pattern. In further research, we will try to introduce diverse signal-processing methods in this security area and contribute to the improvement of the efficiency and the reliability of SCAs.

6. REFERENCES

[1] P. Kocher, J. Jaffe, and B. Jun, “Introduction to differential power analysis and related attacks,” 1998, White Paper, Cryptography Reasearch.

[2] P. Kocher, J. Jaffe and B. Jun, “Differential Power Analysis,” *in Proceedings of CRYPTO 1999*, LNCS 1666, pp. 388-397, Springer-Verlag, 1999.

[3] E. Brier, C. Clavier, and F. Olivier, “Correlation power analysis with a leakage model,” *in Proceedings of CHES 2004*, LNCS 3156, pp. 16-29, 2004.

[4] K. Gandolfi, C. Mourtel, and F. Oliver, “Electromagnetic Attacks: Concrete Results,” *in Proceedings of CHES 2001*.

[5] J.J. Quisquater and D. Samyde, “Electromagnetic Analysis (EMA): Measures and Countermeasures for Smart Cards,” *in Proceedings of e-Smart 2001*.

[6] T-H. Le, J. Clédière, C. Servière, J-L. Lacoume, “Efficient Solution for Misalignment of Signal in Side Channel Analysis,” *in Proceedings of ICASSP 2007*. vol. 2, pp. II-257-II-260, April 2007.

[7] C. Gebotys, S. Ho. And C.C. Tiu, “EM Analysis of Rijndael and ECC on a Wireless Java-Based PDA,” *in Proceedings of CHES 2005*, LNCS 3659, pp. 350-264, Springer-Verlag, 2005.