Available online at www.sciencedirect.com

SciVerse ScienceDirect

Procedia Engineering 15 (2011) 2108 – 2112

Procedia Engineering

www.elsevier.com/locate/procedia

Advanced in Control Engineering and Information Science

Correlation Power Analysis with Companding Methods

Hongying Liu[a,*], Satoshi Goto[a], Yukiyasu Tsunoo[b]

[a]*Graduate School of Information, Production and Systems, Waseda University,Kitakyushu-shi,8080135, Japan*
[b]*Information and Media Processing Laboratories, NEC Corp., Kawasaki, 2118666, Japan*

Abstract

Companding methods have been profoundly applied in signal processing for quantization. And various companding schemes have been proposed to improve the PAPR (Peak to Average Power Ratio) of OFDM systems. In this paper, based on the exploration of the features of μ-law functions, we propose Correlation Power Analysis (CPA) with μ-law companding methods. μ-law expanding function is used to preprocess the power traces collected during AES encryption on ASIC and FPGA respectively. Experiments show that it reduces the number of power traces to recover all the key bytes as much as 25.8% than the conventional CPA.

Selection and/or peer-review under responsibility of [CEIS 2011]
Keywords: AES; CPA; Hamming Distance; Side channel attacks (SCA)

1. Introduction

Power analysis (PA) attacks are based on analyzing the power consumption of the unit while it performs the encryption operation. By either simple or differential analysis of the power the unit consumes, attacker can learn about the processes that are occurring inside the unit and gain some information, when combined with other cryptanalysis techniques, recover the secret key. Simple Power Analysis (SPA) attacks rely on detailed knowledge of the cryptographic algorithm being implemented and visual inspection of the power consumption curve, to extract the cryptographic key. Differential Power Analysis (DPA) attacks are more powerful based on SPA. It adds the power of statistical techniques to separate signal from noise, and requires less detailed knowledge of the implementation of the cryptographic algorithm. In 2004, Brier et al. [1] proposed the correlation power analysis (CPA) attack which uses the correlation factor between Hamming Distance and measured power to guess keys. The

* *E-mail*: liuhongying@fuji.waseda.jp.

1877-7058 © 2011 Published by Elsevier Ltd. Open access under CC BY-NC-ND license.
doi:10.1016/j.proeng.2011.08.394

work was based on the Hamming Distance leakage model, which was more advanced than Hamming Weight model. Then Le et al. [2] improved the performance of CPA by restricting the normalization factor in the proposed Partitioning Power Analysis method.

Unlike the conventional CPA attacks, we propose that the CPA with power trace preprocessing, which takes advantage of the μ-law expanding functions to strengthen the critical points of the power trace while weaken the unrelated parts. The experiments show its effectiveness. The remainder of this paper is organized as follows. Section 2 describes related research work. Section 3 presents the proposed companding methods in detail. Section 4 shows the CPA experiments and results. Section 5 draws conclusions and suggests future research.

2. Related Work

So far, there are a few previous works that address the preprocessing techniques for the power traces.In the work[3], the authors propose a preprocessing method based on the fourth-order cumulant to remove the effects due to Gaussian noise coupled into side channel signals. The experiment of analyzing electromagnetic signals during DES operation shows a decrease of power traces to detect the encryption key. But this high order statistic method leads to considerable computational cost. In another work [4], the authors select the expander of the A-law companding function, which is a non-linear transformation function to preprocess the power traces. The performance of the method is evaluated by analyzing the power consumption signals of micro-controller chip during DES operations. However the applications based on this equipment is limited.

To further explore the preprocessing techniques with companding methods, we evaluated μ-law function with the power traces collected from AES encryption on ASIC and FPGA. We found that the number of power traces to recover the encryption keys can be further decreased after μ-law preprocessing.

3. Proposed Preprocessing Method

3.1. μ-law companding

Originally, μ-law is companding scheme used in telephone network to get more dynamics to the 8 bit samples. OFDM (Orthogonal Frequency Division Multiplexing) system uses the companding transform for PAPR reduction.The expression of μ-law companding functions, which including compressing function and expanding function are shown as (1) and (2) respectively,

$$Y = \frac{\log(1 + UX / V)}{\log(1 + U)} V \operatorname{sgn}(X) \quad (1)$$

$$Y = (e^{X \log(1+U)/V} - 1)\frac{V}{U}\operatorname{sgn}(X) \quad (2)$$

where X is the vector of input signal, V is the maximum value of X, U is an adjustable parameter, log is natural logarithm operation, and *sgn* is the mathematical sign function. Y is the output signal.

The feature of μ-law compressing and expanding functions are shown in Fig.1 and Fig.2 respectively. Both of them are central symmetry with center (0,0). Compared with compressing function, the output signal is magnified using expanding function when the input signal is between 0 and 2. This is the case for power trace. The range of power consumption is between 1.21 volt and 1.35 volt.

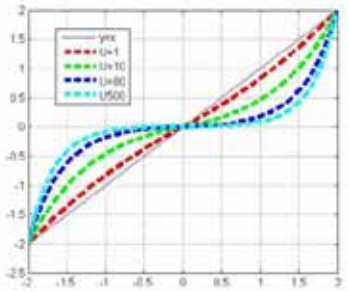

Fig.1 μ-law compressing feature

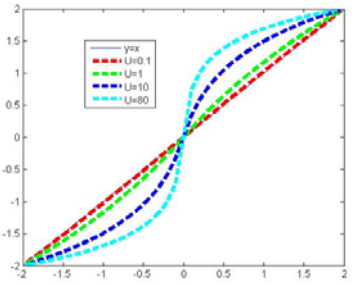

Fig.2 μ-law expanding feature

3.2. CPA with μ-law companding

The process of CPA with μ-law companding method is similar to conventional CPA, but with an additional preprocess of power trace.

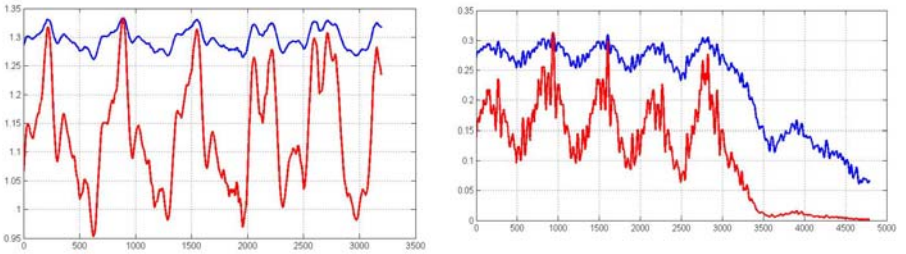

Fig.3 (a) Sampling power traces from AES ASIC implementation. (b) Sampling power traces from AES FPGA implementation. The vertical axis denotes sampling voltage in volt.

Secret key analysis is based on the side channel signals. The signal-to-noise ratio (SNR) of the collected signals influences the effect of secret key detection decisively. It is impossible, though, to arbitrarily change the SNR of the collected signals. We observe that the crypto-operation energy is concentrated on a region of particular amplitude, which is on the lower amplitudes.

Take the power traces collected from AES on Side-channel Attack Standard Evaluation Board (SASEBO-R)[5] as an example. The original power traces of AES encryption is on the bottom of Fig.3, while the μ-law preprocessed power traces are on the top of the figure. The waveforms which have lower altitude are expanded, while the waveforms which are near to the peaks are remained to be similar to the original curve. This exponential weight depending on the side channel signal amplitudes produces a more efficient signal, which enhances the performance of CPA. To further verify the effectiveness of μ-law expanding, we adopt it to preprocess the power traces collected during the AES encryption on SASEBO-G, shown in Fig. 3(b). The communication interface is the same, but the implementation is on FPGA. The bottom curves are the original power traces and the top curves are the ones with μ-law expanding. The architecture of AES implementation is shown in Appendix(Fig.6). The relevant waveforms are stretched out over larger range.

4. Experiments And Results

4.1. Measurement setup

Firstly, one specific point for the attack is selected. We choose the output of the final round of encryption function “add round key” as a target. Secondly, the encryption process is measured.

Experimental environment is shown in Appendix (Fig.7.). The connection between devices is shown in Fig.4. Computer randomly generates 128-bit plaintext in 10 thousand groups, which are transmitted to the FPGA through RS-232 serial ports, and then upon receipt of the plaintext, the FPGA control the ASIC to implement AES encryption program. At the same time, the execution signal on ASIC triggers the digital oscilloscope to start sampling, and thus the oscilloscope obtains power signals through its probe. The sampled data is transmitted to computer through LAN. When encryption is finished, the cipher text is transmitted to computer. So we obtain 10 thousand groups of plaintext, corresponding cipher text as well as 10 thousand power traces.

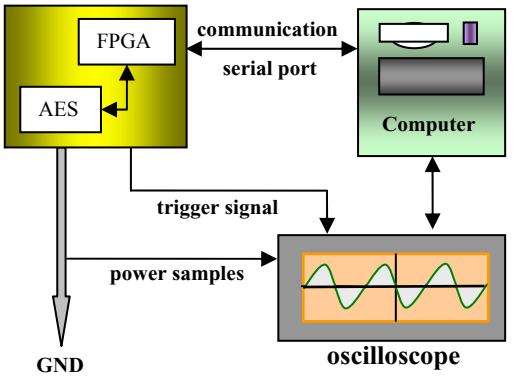

Fig.4 The connection between devices.

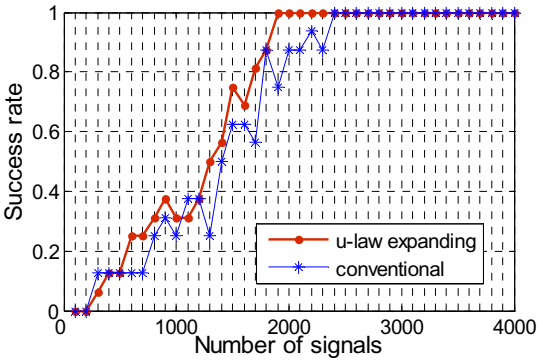

Fig. 5 Comparison of success rates

Then Hamming Distance[1] $H_{i,R}$ between the ciphertext C_i and the reference state R which is prior to "add round key" is calculated according to (3), where HW denotes the Hamming weight, i is the number of samplings.

$$H_{i,R} = HW(R \oplus C_i) \tag{3}$$

$$\rho = \frac{N\sum P(C_i)H_{i,R} - \sum P(C_i)\sum H_{i,R}}{\sqrt{N\sum P(C_i)^2 - (\sum P(C_i))^2}\sqrt{N\sum H_{i,R}{}^2 - (\sum H_{i,R})^2}} \tag{4}$$

Finally, the correlation coefficient is calculated. For a correct key, the operation is data dependent. Thereby, the leakage $P(C_i)$ from EM signal has a linear relationship with Hamming Distance $H_{i,R}$, and the correct key is the one that maximizes the correlation coefficient ρ, given by(4).

4.2. Experimental Results

The results of the CPA with μ-law expanding function is shown in Table 1. The numbers of power traces for each key byte are listed. The 10th key byte needs the most signals. For conventional CPA, 16 bytes of keys are recovered within 2604 power traces, while for expanding method, the power traces have been decreased to 1785. 25.8% reduction has been achieved. The success rate of CPA via the number of power traces are also compared in Fig.5. It shows that the correct keys appear faster with μ-law expanding, which means the accuracy of key detection is improved.

Table 1. The number of needed signals for revealing each key byte.

No.	**K1**	**K 2**	**K 3**	**K 4**	**K 5**	**K 6**	**K 7**	**K 8**
conventional	2,058	795	1,414	607	1,621	1,812	1,293	853
expanding	1,103	763	1,121	562	1,018	1,707	1,299	846
No.	**K 9**	**K 10**	**K 11**	**K 12**	**K 13**	**K 14**	**K 15**	**K16**
conventional	431	**2,406**	1,809	2,125	1,536	934	1,418	1,548
expanding	407	**1,785**	1,514	1,619	841	492	1,207	1,233

In order to confirm the effectiveness of μ-law expanding, the experiment is repeated on SASEBO-G, the number of signals is reduced by 21.9%. But it takes 3514 power traces to recover all the key bytes. This may result from the lower SNR in the collected waveforms, which is less smooth than the signal from ASIC implementation.

We also compared the results of the other settings of the parameter U (in equation (2)). When U is larger than 1, the number of power traces is reduced as much as 30%, when it is smaller than 1, the number of power traces remain the same as conventional CPA.

5. Conclusions

CPA with μ-law expanding methods is proposed in this paper. The experiments against AES implementations on ASIC and FPGA confirm its effectiveness. Compared with conventional CPA, it reduces the number of power traces as much as 25.8%. The performance of CPA is enhanced. There is several works to do in future. Other companding functions or signal processing techniques will be explored and compared to find the optimal to further reduce the power traces.

Acknowledgements

This work was supported by Waseda University "Global COE program" and CREST of JST in Japan.

References

[1] E. Brier, C. Clavier, F. Olivier, Correlation Power Analysis with a Leakage Model, proceedings of CHES 2004, LNCS 3156, pp. 16-29, 2004.

[2] T. Le, J. Clédière, C. Canovas, A proposition for correlation power analysis enhancement, LNCS 4249, pp.174, 2006.

[3] T.-H. Le, C. Servière, J. Cledière, and J.-L. Lacoume, Noise reduction in the side channel attack using fourth order cumulants, IEEE Trans. Inf. Forensic Security, vol. 2, no. 4, pp. 710-720, 2007.

[4] J.Ryoo, D.G. Han, S.K.Kim, and S.Lee, Performance Enhancement of Differential Power Analysis Attacks with Signal Companding Methods, IEEE signal processing letters, 2008.

[5] Research Center for Information Security (RCIS) of AIST, Side-channel Attack Standard Evaluation Board(SASEBO). http://www.rcis.aist.go.jp/special/SASEBO/index-en.html.

Appendix

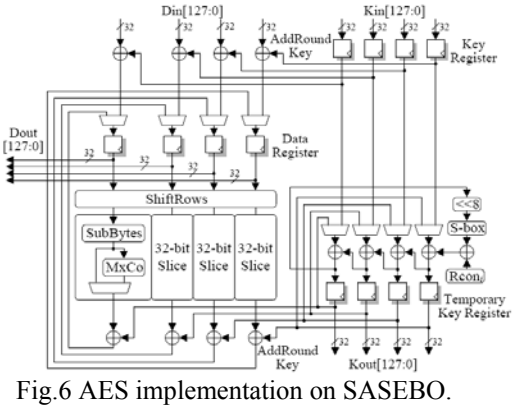

Fig.6 AES implementation on SASEBO.

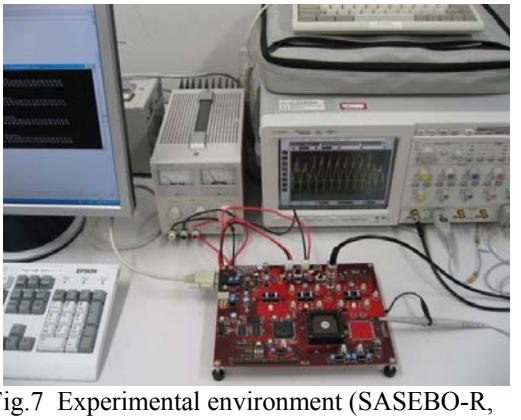

Fig.7 Experimental environment (SASEBO-R, oscilloscope, etc.)