DPA Using Phase-Based Waveform Matching against Random-Delay Countermeasure

Sei Nagashima*, Naofumi Homma*, Yuichi Imai*, Takafumi Aoki* and Akashi Satoh†
* Graduate School of Information Sciences, Tohoku University
6-6-05, Aramaki Aza Aoba, Aoba-ku, Sendai-shi, Miyagi, 980-8579, Japan
Phone: +81-22-795-7169, Fax: +81-22-263-9308,
E-mail: {nagasima, homma}@aoki.ecei.tohoku.ac.jp
† IBM Research, Tokyo Research Laboratory
1623-14, Shimo-tsuruma, Yamato-shi, Kanagawa, 242-8502, Japan
E-mail: akashi@jp.ibm.com

***Abstract*— We propose Differential Power Analysis (DPA) with a phase-based waveform matching technique. Conventionally, a trigger signal and a system clock are used to capture the waveform traces, but the signals always contain jitter-related deviations, and this degrades the accuracy of the statistical analysis. Our method can adjust for this timing deviation with a higher resolution than the sampling rate by post-processing on the measured waveforms. Therefore, no modification of the measuring equipment is required. Our method can also defeat DPA countermeasures creating distorted waveforms with random delays or dummy cycles. We implemented Data Encryption Standard (DES) software with and without the countermeasure on a Z80 microprocessor, and demonstrated the advantages of our method in comparison with a conventional attack.**

I. Introduction

Side-channel attacks that use information leaked from a cryptographic module are attracting great attention, both for research and in industry. When the cryptographic module performs encryption or decryption its power dissipation and electromagnetic radiation contain secret information correlated to the internal data and operations. However, if taken as a signal the leaked information is usually very weak, and thus it is hard to obtain the secret key directly from one power or electromagnetic waveform. Therefore Differential Power Analysis (DPA) [1] uses thousands of waveforms to amplify very weak signals related to the secret key operations. For such statistical analysis, it is very important for signal enhancement to capture the waveforms exactly synchronized with the target operations. Therefore, waveform-distortion countermeasures against DPA were proposed to interfere with the timing by inserting random delays or dummy cycles, or by using an unstable clock [2], [3].

We propose a high-resolution DPA to adjust for the misalignments between waveforms for high-accuracy analysis and to defeat such DPA countermeasures. Our approach uses a Phase-Only Correlation (POC) function capable of evaluating the displacements between the waveforms with higher resolution than the sampling clock [4]. Then the displacements caused by measurement error or DPA countermeasures can be canceled out before the statistical analysis. In this paper, we also demonstrate the advantages of the proposed method through experimental DPA for DES software on a Z80 microprocessor with a waveform-distortion countermeasure.

II. DPA with waveform matching

A. Phase-based waveform matching

Consider two signal waveforms, $f(n)$ and $g(n)$, where we assume that the index range is $n = -M, \cdots, M$ for mathematical simplicity, and hence the length of waveforms $N = 2M+1$. Let $F(k)$ and $G(k)$ denote the Discrete Fourier Transforms (DFTs) of the two waveforms. $F(k)$ and $G(k)$ are given by

$$F(k) = \sum_{n=-M}^{M} f(n) W_N^{kn} = A_F(k) e^{j\theta_F(k)}, \tag{1}$$

$$G(k) = \sum_{n=-M}^{M} g(n) W_N^{kn} = A_G(k) e^{j\theta_G(k)}, \tag{2}$$

where $W_N = e^{-j\frac{2\pi}{N}}$, $A_F(k)$ and $A_G(k)$ are amplitude components, and $e^{j\theta_F(k)}$ and $e^{j\theta_G(k)}$ are phase components.

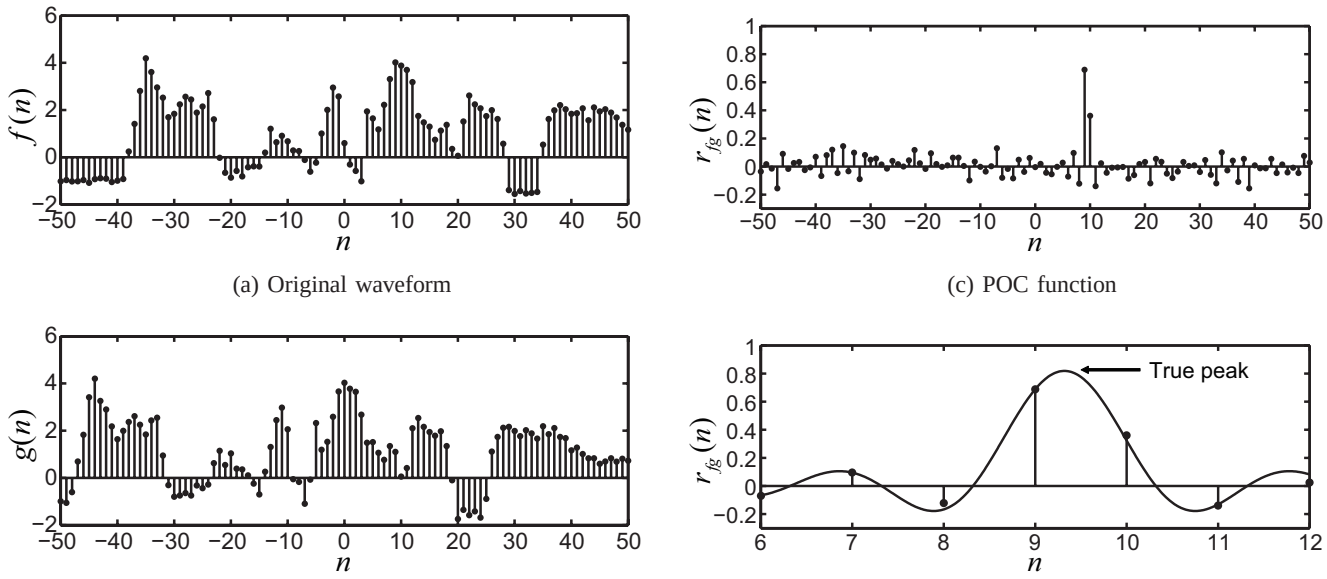
The cross-phase spectrum (or normalized cross spectrum) $R_{FG}(k)$ is defined as

$$R_{FG}(k) = \frac{F(k)\overline{G(k)}}{\left|F(k)\overline{G(k)}\right|} = e^{j\theta_{FG}(k)}, \tag{3}$$

where $\overline{G(k)}$ denotes the complex conjugate of $G(k)$ and $\theta_{FG}(k) = \theta_F(k) - \theta_G(k)$. The POC function $r_{fg}(n)$ is the Inverse Discrete Fourier Transform (IDFT) of $R_{FG}(k)$ and is given by

$$r_{fg}(n) = \frac{1}{N} \sum_{k=-M}^{M} R_{FG}(k) W_N^{-kn}. \tag{4}$$

If there is a similarity between two waveforms, the POC function gives a distinct sharp peak. (When $f(n) = g(n)$, the POC function becomes the Kronecker delta function.) If not, the peak drops significantly. The height of the peak can be used as a good similarity metric for the waveform matching, and the location of the peak shows the translational displacement between the two waveforms. Fig. 1 shows an example of the



(a) Original waveform

(c) POC function

(b) Displaced version of the original waveform

(d) Function fitting for estimating peak position

Fig. 1. Displacement estimation using POC function.

POC function, where (a) and (b) are an example waveform and a displaced version of the waveform, respectively. Fig. 1 (c) is the corresponding POC function.

Now consider $f_c(t)$ as a waveform defined in continuous space with a real number index t. Let δ represents a displacement of $f_c(t)$, so the displaced waveform can be represented as $f_c(t-\delta)$. Assume that $f(n)$ and $g(n)$ are spatially sampled waveforms of $f_c(t)$ and $f_c(t-\delta)$, and are defined as

$$f(n) = f_c(t)|_{t=nT}, \quad (5)$$

$$g(n) = f_c(t-\delta)|_{t=nT}, \quad (6)$$

where T is the sampling interval and the index range is given by $n = -M, \cdots, M$. For simplicity, we assume $T = 1$. The cross-phase spectrum $R_{FG}(k)$ and the POC function $r_{fg}(n)$ between $f(n)$ and $g(n)$ will be given by

$$R_{FG}(k) = \frac{F(k)\overline{G(k)}}{\left|F(k)\overline{G(k)}\right|} \simeq e^{j\frac{2\pi}{N}k\delta}, \quad (7)$$

$$r_{fg}(n) = \frac{1}{N}\sum_{k=-M}^{M} R_{FG}(k)W_N^{-kn} \simeq \frac{\alpha}{N}\frac{\sin\{\pi(n+\delta)\}}{\sin\left\{\frac{\pi}{N}(n+\delta)\right\}}, \quad (8)$$

where $\alpha = 1$. The above Eqn. (8) represents the shape of the peak for the POC function between the corresponding waveforms that are slightly displaced relative to each other. This equation gives a distinct sharp peak. The peak position δ of the POC function corresponds to the displacement between the two waveforms. We can prove that the peak value α decreases (without changing the shape of the function itself), when small noise components are added to the original waveforms. Hence, we assume $\alpha \leq 1$ in practice. For the waveform matching task, we evaluate the similarity between the two waveforms by the peak value α, and estimate the displacement by the peak position δ.

By calculating the POC function for two waveforms $f(n)$ and $g(n)$, we can obtain a numerical value of $r_{fg}(n)$ for each discrete index n, where $n = -M, \cdots, M$. Fig. 1 (d) shows the POC function around the correlation peak, where the black dots indicate the discrete data values from $r_{fg}(n)$. We use Eqn. (8) (the closed-form peak model of the POC function) directly to estimate the peak position by function fitting. The solid line in Fig. 1 (d) represents the estimated shape of the POC function. Thus, it is possible to find the location of the peak that may exist between sampling intervals by fitting the peak model to the calculated data around the correlation peak, where α and δ are fitting parameters.

In addition to the function fitting, we employ advanced techniques for high-accuracy estimation of displacement: (i) windowing to reduce boundary effects, and (ii) spectral weighting to reduce aliasing and noise effects [4].

B. Proposed DPA

The overview of our proposed DPA with the POC-based waveform matching described in Section II-A is shown in Fig. 2. We first collect a number of power traces by repeating encryption or decryption with different plaintexts for each iteration. Then we use the POC-based matching for the precise alignment between the waveforms. For the matching, we select any one of the waveforms as a reference, and then evaluate and adjust the displacement errors between this reference and the other waveforms.

After the waveform matching, a statistical analysis is performed. We first guess at some of the bits of the secret key, and calculate a bit value for each waveform by using a selection

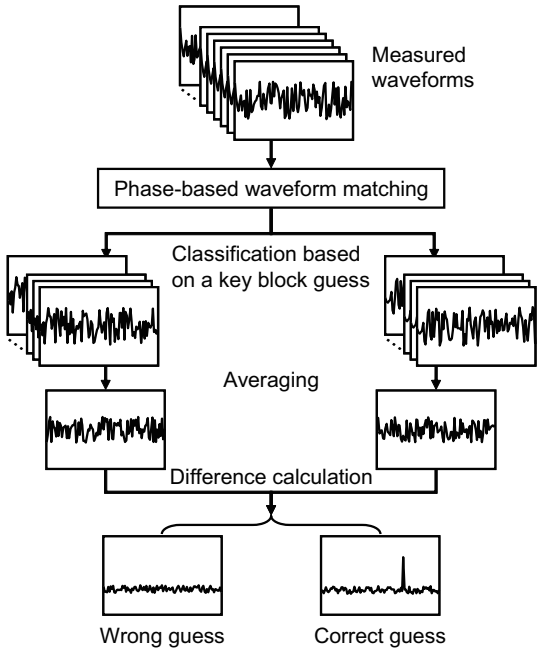


Fig. 2. Proposed differential analysis using phase-based waveform matching.

function. Then we divide the waveforms into two groups according to the selection bit value 0 and 1, and average each group, subtracting one averaged waveform from the other. If a peak appears in the averaged waveform, the guess about the secret key was correct. If there is no obvious peak signal, another candidate key is tested.

III. Experimental DPA on DES software with countermeasure

A. Experimental conditions

Our method was applied to DES software on a Zilog Z80 processor (8 MHz). The software used a countermeasure inserting NOPs (No OPerations) at random after the trigger signal [2]. The number of NOPs was normally distributed with mean 3 and variance 1. The random number was generated in advance. A single NOP operation takes 0.02 msec, and the maximum delay time is about 0.10 msec.

We used S-box outputs at the 16-th (final) round as selection functions. DES has eight 6-bit-input and 4-bit-output S-boxes $\mathrm{S}_1 \sim \mathrm{S}_8$, and thus $4 \times 8 = 32$ selection functions can be formed. For each selection function, we have $2^6 = 64$ key candidates derived from the 6-bit S-box input.

The power consumption of the processor was monitored as the voltage drop caused by a resistor inserted between the Z80 ground pin and the ground plane of the evaluation board (INSTAC-8 as shown in Fig. 3) [5]. We used a trigger signal synchronized with the beginning of round 15, and obtained 1,000 waveforms at each sampling rates of 100 MSa/s (millions of samples per second), 200 MSa/s, 400 MSa/s, and 1 GSa/s. The capture range of waveforms is from 4.433 ms to 4.783 ms after the trigger signal, which contains all of the operations of eight S-boxes (Fig. 4). During the measurements,

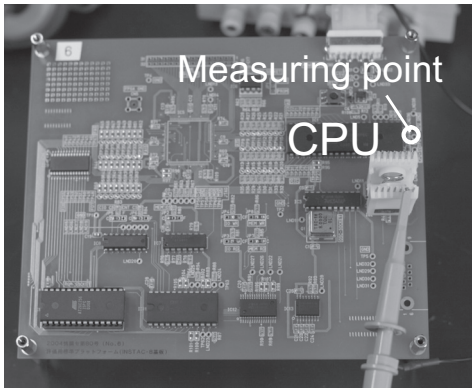


Fig. 3. Evaluation board (INSTAC-8).

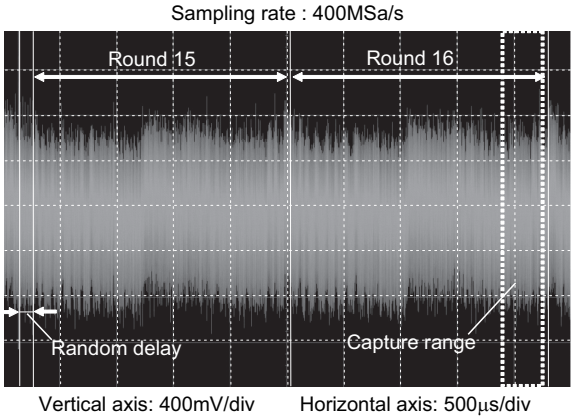


Fig. 4. Example of measured waveform.

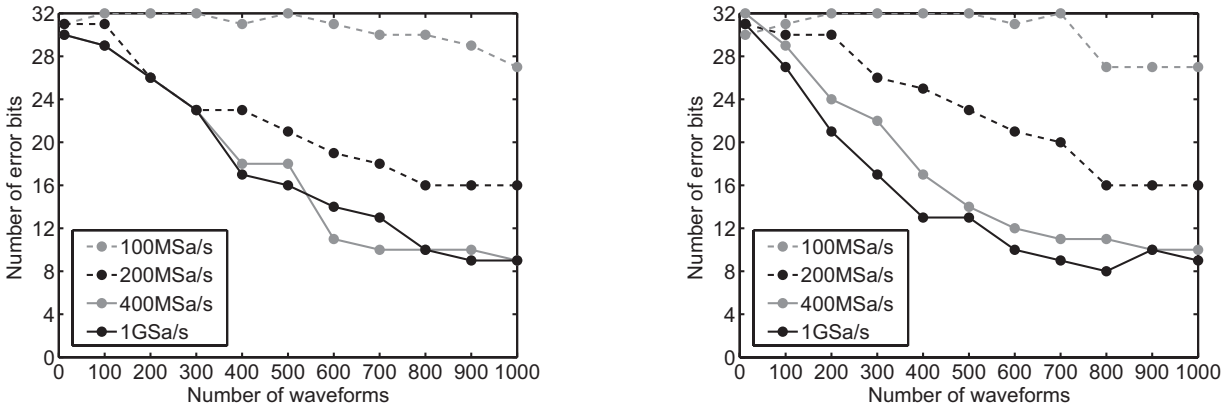
the plaintexts were randomly changed, but the sub-key values used for eight S-box inputs at the 16-th round were fixed as 21, 16, 31, 35, 9, 51, 51, and 48 in decimal.

B. Experimental results

Fig. 5 shows the results DPA for both the conventional and the proposed method at 400 MSa/s against DES with the random-delay countermeasure. These results were obtained by testing all of the possible sub-keys ($1 \sim 64$) on one of the four selection functions of S-box S_1. The conventional DPA in Fig. 5 (a) gives no peak signal even for the correct key. In contrast, the proposed DPA in Fig. 5 (b) shows a significant peak with the correct key. Note here that the increase of computation time is only 5%.

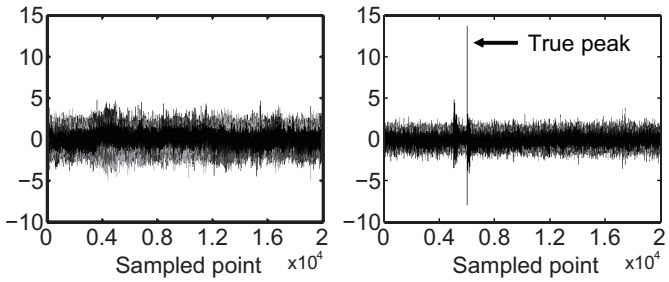
Fig. 6 shows error rates for the proposed method applied to DES software (a) with and (b) without the countermeasure for various sampling rate and number of waveforms. The vertical axis indicates the number of incorrect bits. In other words, this shows the number of selection functions that did not reveal the correct key. If no secret key was obtained, the number of errors is 32 bits. The error rates between two graphs are almost the same, which means our proposed DPA can completely defeat the random-delay countermeasure.

Table I shows the DPA results using 1,000 waveforms at 400 MSa/s. The four selection functions were used to recover the



(a) Conventional DES (b) DES with random delays

Fig. 6. Error rate of proposed DPA.



(a) Conventional DPA (b) Proposed DPA

Fig. 5. DPAs against DES implementation with random delays.

TABLE I
DPA results at 400 MSa/s

Conventional DES							
S_1	S_2	S_3	S_4	S_5	S_6	S_7	S_8
21	16	31	35	9	51	51	48
21	16	31	35	47	51	51	48
11	25	24	35	9	26	8	48
55	16	31	14	9	51	51	26

DES with random delays							
S_1	S_2	S_3	S_4	S_5	S_6	S_7	S_8
21	16	31	35	9	51	51	48
21	16	31	35	47	9	51	48
11	25	12	35	9	26	8	51
55	16	31	14	9	51	51	48

6-bit sub-key for each S-box, and thus four estimations were made for each S-box, as shown in the table, where shaded boxes indicate the correct keys. Even though some estimation errors occurred, correct keys could be obtained by majority decisions. Therefore, the numbers of error bits are not zero with 1,000 waveforms in Fig. 6, but all the correct keys were obtained with about 500 waveforms at 400 MSa/s regardless of whether countermeasures were used.

IV. Conclusions

We proposed a high-resolution DPA using phase-based waveform matching, and demonstrated its advantages through experimental DPA attacks against DES software on a Z80 microprocessor. The phase-based matching method makes it possible to evaluate the displacements between signal waveforms with higher resolution than the sampling rate. Our method can efficiently enhance the key-related weak signal for the statistical analysis phase by precisely adjusting the displacements of the waveforms without modifying the measuring equipment. The DPA countermeasures that interfere with the sampling timing by inserting random delays can also be defeated completely by using our method with only 5 % additional computation time.

We focus on DPA in this paper, but our waveform matching can be applied to any kind of side-channel attack to enhance its precision, algorithms (symmetric-key and public-key ciphers), implementations (software and hardware), leakage sources (power dissipation and electromagnetic radiation), and analysis methods (simple analysis and differential analysis). Conventional work usually captured operational waveforms by using a trigger signal and a system clock for a cryptographic module. In contrast, the experimental results showed that our method has the potential to attack cryptographic modules even though no trigger signal nor internal clock can be observed.

References

[1] P. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," *CRYPTO 1999, Lecture Notes in Computer Science*, vol. 1666, pp. 388 – 397, Aug. 1999.

[2] C. Clavier, J. Coron, and N. Dabbous, "Differential power analysis in the presence of hardware countermeasures," *CHES 2000, Lecture Notes in Computer Science*, vol. 1965, pp. 252 – 263, Aug. 2000.

[3] O. Kommerling and M. G. Kuhn, "Design principles for tamper-resistant smartcard processors," *Proc. of the USENIX Workshop on Smartcard Technology, Chicago*, pp. 9 – 20, May 1999.

[4] N. Homma, S. Nagashima, Y. Imai, T. Aoki, and A. Satoh, "High-resolution side-channel attack using phase-based waveform matching," *CHES 2006, Lecture Notes in Computer Science*, Oct. 2006 (to be published).

[5] T. Matsumoto, S. Kawamura, K. Fujisaki, N. Torii, S. Ishida, Y. Tsunoo, M. Saeki, and A. Yamagishi, "Tamper-resistance standardization research committee report," *The 2006 Symposium on Cryptography and Information Security*, pp. 1 – 6, Jan. 2006.