PAPER *Special Section on Cryptography and Information Security*

A High-Resolution Phase-Based Waveform Matching and Its Application to Side-Channel Attacks

Naofumi HOMMA[†a)], ***Member***, **Sei NAGASHIMA**[†], **Takeshi SUGAWARA**[†], ***Nonmembers***, **Takafumi AOKI**[†], ***and*** **Akashi SATOH**[††], ***Members***

SUMMARY This paper presents an enhanced side-channel attack using a phase-based waveform matching technique. Conventionally, side channel attacks such as Simple Power Analysis (SPA) and Differential Power Analysis (DPA) capture signal waveforms (e.g., power traces) with a trigger signal or a system clock, and use a statistical analysis of the waveforms to reduce noise and to retrieve secret information. However, the waveform data often includes displacement errors, and this degrades the accuracy of the statistical analysis. The use of a Phase-Only Correlation (POC) technique enables to estimate the displacements between the signal waveforms with higher resolution than the sampling resolution. The accuracy of side-channel attacks can be enhanced using the POC-based matching method. Also, a popular DPA countermeasure creating distorted waveforms with random delays can be defeated by our method. In this paper, we demonstrate the advantages of the proposed method in comparison with conventional approaches through experimental DPA and Differential ElectroMagnetic Analysis (DEMA) against DES software and hardware implementations.

key words: *side-channel attacks, DPA, DEMA, cryptographic module, waveform matching, phase-only correlation.*

1. Introduction

Cryptanalysis based on side-channel information is of major concern for designers of smartcards and other embedded cryptosystems. When a cryptographic module performs encryption or decryption, secret parameters correlated to the intermediate data being processed would leak via power dissipation [1], [2], electromagnetic radiation [3], or operating times as side-channel information. These are now essential issues for the evaluation of tamper-resistance devices. Among them, power analysis attacks such as Differential Power Analysis (DPA) [2] are attracting much attention due to their powerful properties.

In general, a side-channel attack requires a statistical analysis of waveforms (e.g., power traces) to reduce noise and to retrieve secret information. The important assumption here is that each waveform is captured by a digital measuring device at the exact moment as the corresponding cryptographic computation. However, it is almost impossible to time exactly when the data was captured for cryptographic modules in actual applications because there is no trigger signal precisely synchronized with the cryptographic computation. Even if a trigger signal is available, it often contains jitter-related deviations from the true timing of the encryption process. Also, some countermeasures creating distorted waveforms with random delays, dummy cycles, or unstable clocking are being proposed for reducing the impact of statistical analysis [4][5]. As a result, the measured waveforms always include displacement errors. The displacement errors would cause significant loss of the secret information when the waveforms are averaged together for the statistical analysis.

Some approaches dealing with the displacements in waveforms were proposed [6], [7]. In a theoretical model, Differential Power Analysis (DPA) with the fast Fourier transform of the power waveforms is introduced to correct the displacement errors [6]. Reference [7], on the other hand, demonstrated a practical approach to analyze Rijndael and ECC on a Java-based wireless PDA. The reported methods were performed in the frequency domain, and thus it would be very difficult to use them in collaboration with other side-channel attacks in the time domain.

Addressing the displacement problem, we propose a high-resolution waveform matching method using a Phase-Only Correlation (POC) function. POC techniques have been successfully applied to high-accuracy image matching tasks [8]-[11]. The POC function employs phase components in the discrete Fourier transforms of waveforms, and makes it possible to determine displacement errors between signal waveforms with high noise tolerance by using the location of the correlation peak. By fitting the analytical model of the correlation peak to the actual numerical data, we can evaluate the displacement errors with a higher resolution than the sampling resolution [12].

This paper presents a high-resolution side-channel attack using POC-based waveform matching. The essence of the proposed method is to use the POC-based waveform matching as a preprocessing step followed by standard analysis. We demonstrate its advan-

Manuscript received January 1, 2003.
Manuscript revised January 1, 2003.
Final manuscript received January 1, 2003.

[†]The authors are with the Department of Computer and Mathematical Sciences, Graduate School of Information Sciences, Tohoku University, 6-6-05, Aramaki Aza Aoba, Sendai, 980–8579 Japan.

[††]The author is with IBM Research, Tokyo Research Laboratory, IBM Japan, Ltd. 1623-14 Shimo-tsuruma, Yamato-shi, Kanagawa, 242-8502, Japan

a) E-mail: homma@aoki.ecei.tohoku.ac.jp

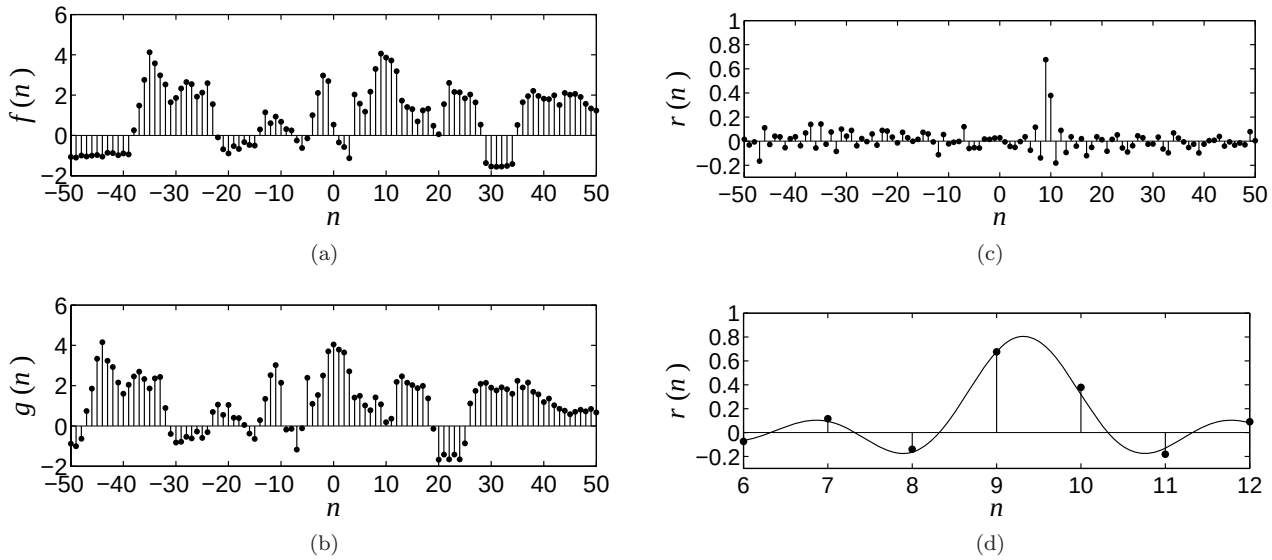


Fig. 1 Displacement estimation using POC function: (a) Original waveform, (b) Displaced version of the original waveform, (c) POC function, and (d) Function fitting for estimating peak position.

tages over conventional methods through experimental analysis of DPA and Differential ElectroMagnetic Analysis (DEMA) against DES software and hardware implementations. In this experiment, the POC-based matching successfully improves the DPA and DEMA even if the measure waveforms include the noise components of -5 dB signal-to-noise ratio. In addition, our method can defeat a popular countermeasure creating distorted waveform with random delays.

2. High-resolution waveform matching using Phase-Only Correlation

2.1 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) $R(k)$ is defined as

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

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

$$r(n) = \frac{1}{N} \sum_{k=-M}^{M} R(k) W_N^{-kn}. \tag{4}$$

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 measure for waveform matching, and the location of the peak shows the translational displacement between the two waveforms. Fig. 1 shows an example of the 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

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

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

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 $R(k)$ and the POC

function $r(n)$ between $f(n)$ and $g(n)$ will be given by

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

$$r(n) = \frac{1}{N}\sum_{k=-M}^{M} R(k)W_N^{-kn} \simeq \frac{\alpha}{N}\frac{\sin\{\pi(n+\delta)\}}{\sin\left\{\frac{\pi}{N}(n+\delta)\right\}}, \tag{8}$$

where $\alpha = 1$. The above Eq. (8) represents the shape of the peak for the POC function between the same waveforms that are slightly displaced with 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 $r(n)$ 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 $r(n)$. We use Eq. (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. Note here that we can use other types of functions, such as a Gaussian function or a quadratic function, for the function fitting.

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 [12].

2.2 Preliminary evaluation

Consider two waveforms $f(n)$ and $g(n)$, and an estimated displacement δ. The waveform matching finally calculates $g'(n)$ by shifting $g(n)$ by an amount corresponding to δ. For example, this waveform shifting is done by the phase rotation of the waveform in the frequency domain. Let $G'(k)$ denotes the DFT of $g'(n)$. $G'(k)$ will be given by

$$G'(k) \simeq G(k)e^{j\frac{2\pi}{N}k\delta}. \tag{9}$$

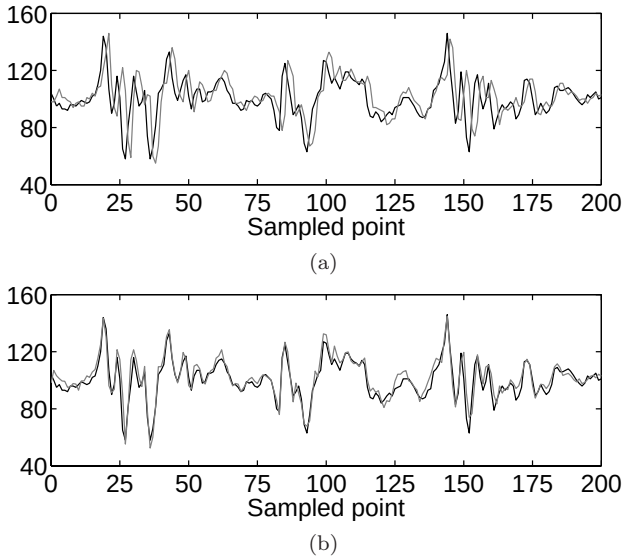


Fig. 2 Example of POC-based waveform matching: (a) input waveforms $f(n)$ and $g(n)$, (b) $f(n)$ and displacement-normalized waveform $g'(n)$.

Therefore, $g'(n)$ is given by

$$g'(n) = \frac{1}{N}\sum_{k=-M}^{M} G'(k)W_N^{-kn}. \tag{10}$$

We can also implement the waveform shifting with various interpolation techniques, such as bicubic interpolation.

Fig. 2 shows an example of the POC-based waveform matching, where the two waveforms are power traces from a microprocessor captured by using a trigger signal at the times of the same computation. Due to the trigger jitter, there is a displacement error between these waveforms as shown in Fig. 2 (a). Using the POC-based waveform matching, we can obtain the displacement $\delta = 1.5555$. Fig. 2 (b) shows two waveforms after the waveform shifting. Thus, the proposed method can be used to match waveform positions with higher resolution than the sampling resolution.

Fig. 3 shows examples of the POC functions, where we use the two waveforms shown in Fig. 2. For comparison, the waveforms include additive Gaussian noise components. The signal-to-noise ratio (S/N) = -10db when the noise energy is about 3.2 times larger than the signal energy. We observe that the POC function provides a sharp peak even if the noise level increases. This suggests that the POC function exhibits much higher discrimination than the ordinary correlation function. Ideally, we can detect the peak position even at the -20 dB setting.

x

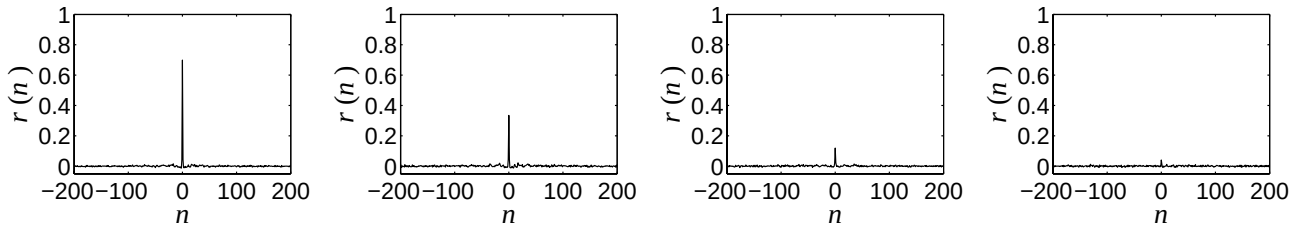


Fig. 3 POC functions with Gaussian noise components: (a) S/N = 10dB, (b) S/N = 0dB, (c) S/N = -10dB, and (d) S/N = -20dB.

3. Side-channel attacks with POC-based waveform matching

3.1 Basic concept

The proposed waveform matching is used as a preprocessing step followed by standard analysis. The overview of our proposed DPA with the POC-based waveform matching described in Section 2 is shown in Fig. 4. 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. Finally, we resample each waveform according to the evaluated displacement.

After the waveform matching, the standard analysis is performed. We first guess at some of the secret key, and calculate a bit value for each waveform by using a selection function. Then we divide the waveforms into two groups according to the selection bit value 0 and 1, average each group, and subtract one averaged waveform from the other. If a peak appears in the averaged waveform, the guess about the secret key is correct. If there is no obvious peak signal, another candidate key is tested.

In the following experiment, we used a trigger signal as in the conventional DPAs for simplicity, and the measured waveforms are initially aligned at the trigger. Note here that the proposed method can get the same alignment of the waveforms without using a trigger signal. At any rate, the waveforms always contain jitter-related deviations from the true timing of the cryptographic computation.

3.2 Experimental conditions

We applied the POC-based matching technique to DPAs against a DES software implementation on a Zilog Z80 processor (8 MHz). For the selection functions, we focus on the S-box computation in the 16-th (final) round. DES has eight 6-bit-input and 4-bit-output S-boxes, and thus $4 \times 8 = 32$ selection functions using the S-box output can be formed. For each selection function, we have $2^6 = 64$ key candidates derived from the 6-bit S-box input.

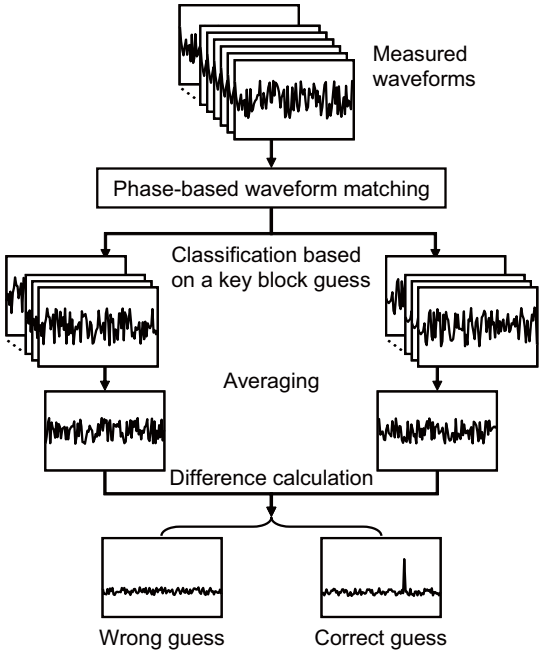


Fig. 4 Proposed differential analysis with POC-based waveform matching.

Fig. 5 shows the INSTAC-8 evaluation board [13] designed for the side-channel attack experiment, and the measurement point on the board. 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 board. We used a trigger signal synchronized with the beginning of round 15, and obtained four sets of waveforms at sampling rates of 100 MSa/s (millions of samples per second), 200 MSa/s, 400 MSa/s, and 1 GSa/s. Fig. 6 is the measured waveform at 400 MSa/s. The capture range of waveforms is from 4.22 ms to 4.24 ms after the trigger signal, which contains all of the operations of S-box S_1 to S-box S_8. A set of 1,000 waveforms was measured during encryption of 1,000 random plaintexts with a fixed key. The subkey values from S_1 to S_8 at

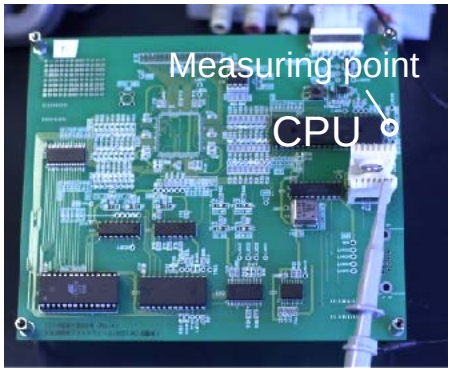


Fig. 5 Evaluation board (INSTAC-8).

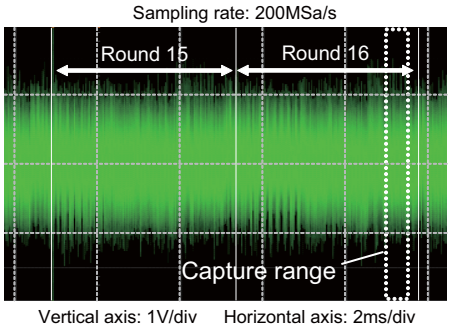


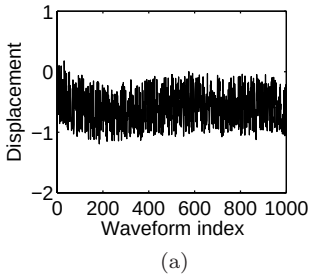
Fig. 6 Example of measured waveform.

the round 16 were fixed as 21, 16, 31, 35, 9, 51, 51, and 48 in decimal, respectively.

3.3 Experimental results

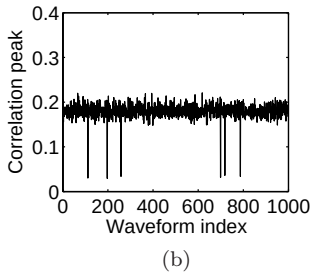
Fig. 7 shows the evaluated displacements for the 1,000 waveforms sampled at 200 MHz (5 ns/point), where the horizontal and vertical axes indicate the waveform index and the displacement value, respectively. The waveforms contain relatively large displacement errors even though they were captured by using a trigger signal synchronized to the system clock, which was generated by the board. Fig. 8 shows the correlation peaks between each waveform and a reference. The peak between two waveforms was about 0.2 due to the different plaintexts and noise. (The peak between identical waveforms is 1.) However, we can identify the peak position clearly since the POC function gives a distinct sharp peak as shown in Fig. 9 (a). Fig. 8 also shows that there are some small peaks among the waveforms. Fig. 9 (b) shows one of the corresponding POC functions. We found that the waveforms at a low peak value were quite different in shape from the reference waveform. The proposed POC-based analysis can easily detect this kind of inaccurately measured waveform, and thus adverse effects on the statistical analysis can be prevented by removing them in an averaging process.

Fig. 10 illustrates the results of the conventional DPA and the proposed DPA, where both DPAs have



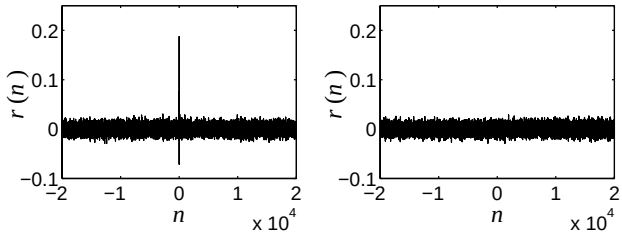
(a)

Fig. 7 Displacement values.



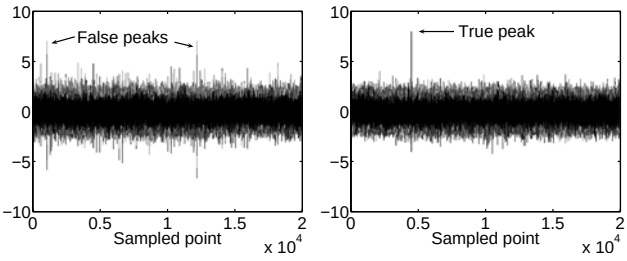
(b)

Fig. 8 Correlation peak values.



(a) (b)

Fig. 9 POC functions: (a) for the case $\alpha \approx 0.2$, (b) for the case $\alpha \approx 0.02$.



(a) (b)

Fig. 10 Example of DPAs using 1,000 waveforms sampled at 200 MHz: (a) conventional DPA, (b) proposed DPA.

used the same set of waveforms sampled at 200 MHz. These results were obtained by evaluating 64 possible keys with one out of the four selection functions of S-box 1. When the DPA succeeds, the highest peak appears in the averaged waveform indicating the correct key, but the conventional DPA in Fig. 10 (a) gives many high false peaks for incorrect keys. In contrast, the proposed DPA clearly indicates the true peak with the correct key as shown in Fig. 10 (b). In this experiment, we confirmed that the proposed DPA consistently increased the peak signal and reduced the noise at all four of the sampling rates.

Fig. 11 compares the error rates of the conventional DPA and those of the proposed DPA for different numbers of waveforms, where the vertical axis indicates the number of error bits. In other words, Fig. 11 shows the number of selection functions that could not distinguish a correct key from the incorrect keys by investigating the highest peak. If no secret key bit was obtained, the number of errors is 32 bits. The sam-

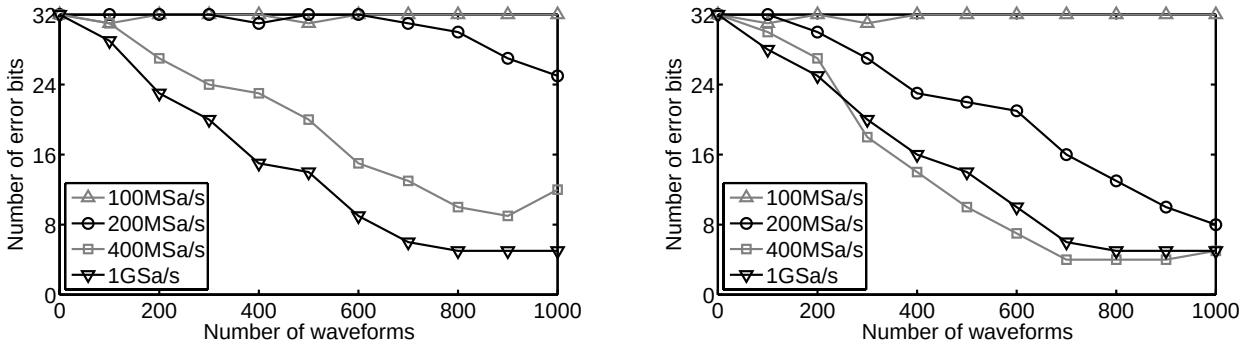


Fig. 11 Error rates for various sampling rates: (a) conventional DPA, (b) proposed DPA.

Table 1 DPA results at 200 MSa/s

Conventional DPA							
S_1	S_2	S_3	S_4	S_5	S_6	S_7	S_8
21	16	31	35	5	51	51	48
51	5	44	33	27	54	32	11
15	22	43	58	33	13	26	60
8	45	54	14	11	11	60	20

Proposed DPA							
S_1	S_2	S_3	S_4	S_5	S_6	S_7	S_8
21	16	31	35	9	51	51	48
38	16	31	21	12	49	51	48
11	25	53	58	2	26	8	7
10	16	31	14	50	51	19	20

Table 2 DPA results at 400 MSa/s

Conventional DPA							
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	53	47	51	51	39
11	25	31	35	9	26	8	51
55	16	31	14	9	32	51	36

Proposed DPA							
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
21	25	31	35	9	26	8	48
21	16	31	14	9	51	51	48

pling rate of 1 GSa/s is high enough to attack the slow 8-MHz processor by using conventional DPA, but the proposed method has clear computational advantages at the sampling rates of 200 MSa/s and 400 MSa/s as shown in Figs. 11.

Tables 1 and 2 show the DPA results using 1,000 waveforms at 200 MSa/s and 400 MSa/s, respectively. The 4-bit output from each S-box S_i was used for four selection functions, and thus four estimations were made for each 6-bit subkey that was XORed to 6 bits of S-box input data. Therefore, four 6-bit possible keys were obtained for each S-box in the tables, and the shaded boxes indicate the correctly guessed keys. If two or more of the values in an S-box column are the same, then there is a very high probability that we can obtain the correct subkey by majority vote. As shown in Table 1, the proposed DPA found five out of eight subkeys at 200 MSa/s while the conventional approach found none. In the 400 MSa/s measurements, the proposed DPA determined all of the subkeys, as shown in Table 2. It is important to note that both DPAs used exactly the same waveform data, and the POC preprocess is simply applied to the captured waveforms before statistical analysis.

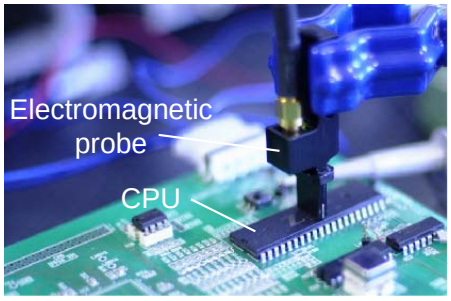


Fig. 12 Electromagnetic probing.

4. Further studies

The proposed matching method in the above section can be easily applied to other types of side-channel information and different implementation, such as electromagnetic radiation and an FPGA hardware implementation. Also, our method can be used for practical DPAs even when cryptographic modules include some popular countermeasures based on random delay or noise jamming. This section examines these advantages through further experiments.

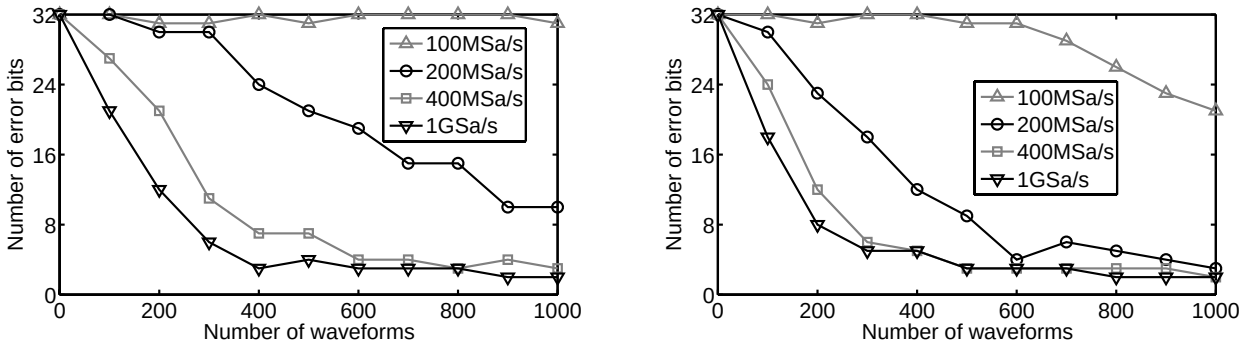


Fig. 13 Error rates for various sampling rates: (a) conventional DEMA, (b) proposed DEMA.

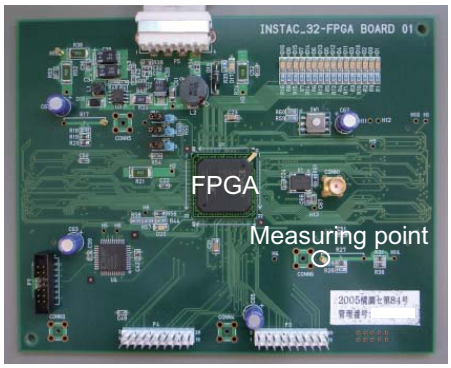


Fig. 14 Evaluation board (INSTAC-32).

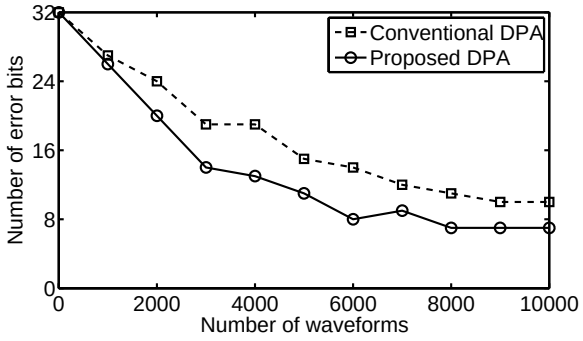


Fig. 15 Error rates on DES hardware.

4.1 DEMA on DES software

The POC-based method was applied to DEMA against the same DES software as described in Section 3. The electromagnetic radiation was monitored over the Z80 processor as illustrated in Fig. 12. The experimental condition was the same as in the DPA described in the previous section.

Fig. 13 shows the error rate comparisons between the conventional and proposed DEMA. The proposed method shows lower error rates at the sampling rates of 100 MSa/s and 200 MSa/s. For example, the proposed DEMA at 200 MSa/s requires less than half the number of waveforms used by the conventional method to achieve the 50 % error rate.

4.2 DPA on DES hardware

In addition to DES software, we also implemented DES hardware on a Xilinx Virtex-II and applied our method to it. The DES hardware has a loop architecture where one round function block is iteratively repeated [14]. Fig. 14 shows the experimental FPGA board INSTAC-32 [13], and the measurement point where a register is inserted between the FPGA ground pin and the ground plane of the board. The power traces were monitored with an oscilloscope (Agilent MSO 6104A) as voltage drops caused by the resistor, and the sampling rate of the oscilloscope was 1 GSa/s. The DES operations were performed at a 2-MHz operating frequency (0.5-μs clock cycle). For simplicity, we used a positive edge trigger at the beginning of round 1.

Fig. 15 shows the error rate comparisons between the conventional and proposed DPA. This result clearly shows that the proposed method is also very effective for the FPGA implementation. For other sampling rates, such as 100 MSa/s, 200 MSa/s, and 400 MSa/s, we would have almost the same results as 1 GSa/s in this condition.

4.3 DPA on DES software with random delay

We implemented a DES software with a random-delay countermeasure inserting NOPs (No OPerations) at random after the trigger signal [4]. 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. As a result, the conventional DPA never gives any true peak for all the sampling rates (100 MSa/s, 200 MSa/s, 400 MSa/s and 1GSa/s) by 1,000 waveforms.

Fig. 16 shows error rates for the proposed method

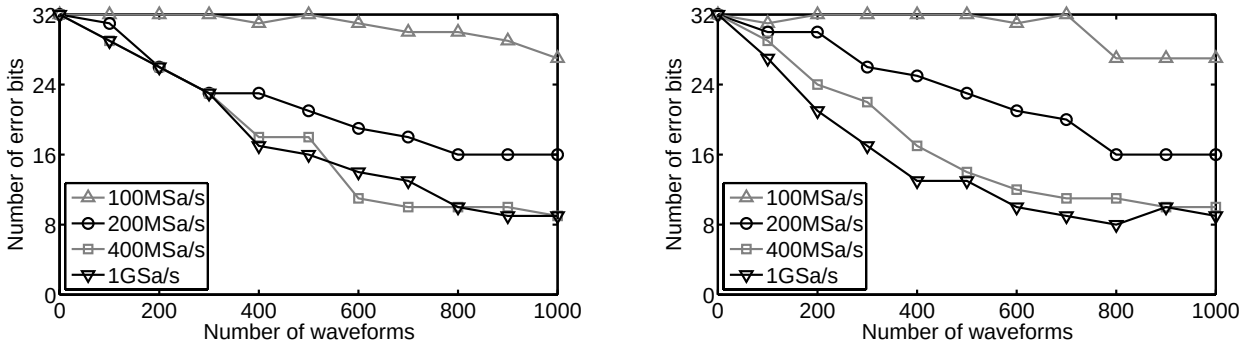


Fig. 16 Error rate of proposed DPA: (a) Conventional DES, and (b) DES with random delays.

Table 3 Proposed DPAs 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

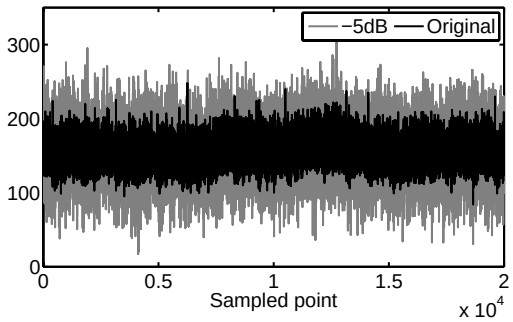


Fig. 17 Experimental waveforms (original waveform and noisy waveform at -5dB S/N ratio).

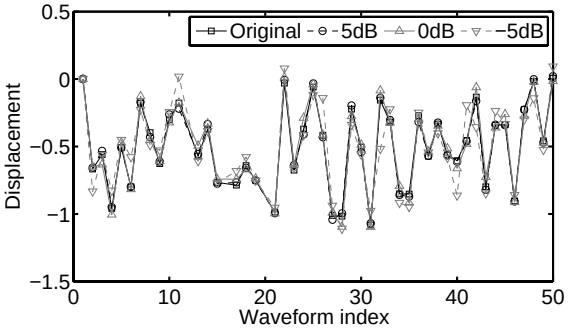


Fig. 18 Displacement errors for noisy waveforms.

applied to DES software (a) without and (b) with the random-delay countermeasure for various sampling rate and number of waveforms. The error rates between two graphs are almost the same, which means our proposed DPA can completely defeat the random-delay countermeasure. Table 3 shows the DPA results using 1,000 waveforms at 400 MSa/s. Even though some estimation errors occurred, correct keys could be obtained by majority decisions. The result shows that all the correct keys were obtained with about 500 waveforms at 400 MSa/s regardless of whether countermeasures were used or not.

4.4 DPA on DES software with noise injection

We evaluated the noise tolerance of the proposed matching using waveforms with Gaussian noise components. Assuming that the measured waveforms in the above experiment do not have any noise component, we generated three sets of 1,000 waveforms for signal-to-noise (S/N) ratios of 5dB, 0dB, and -5dB. The noise components were added on Matlab software. Fig. 17 shows an example of the waveforms at -5dB S/N ratio.

Fig. 18 shows a part of the evaluated displacements for the waveforms sampled at 400 MHz, where the horizontal and vertical axes indicate the waveform index and the displacement value, respectively. The result shows that the POC-based matching can be useful for aligning the waveforms even at -5dB S/N ratios. Fig. 19 shows the results of DPA for both the conventional and the proposed method at 400 MSa/s against the noisy waveforms. The proposed DPA can reduce the error rate clearly for all of the waveform sets.

5. Conclusions

In this paper we proposed a POC-based waveform matching method and its application to side-channel attacks. The proposed matching method makes it possible to evaluate the displacement between signal wave-

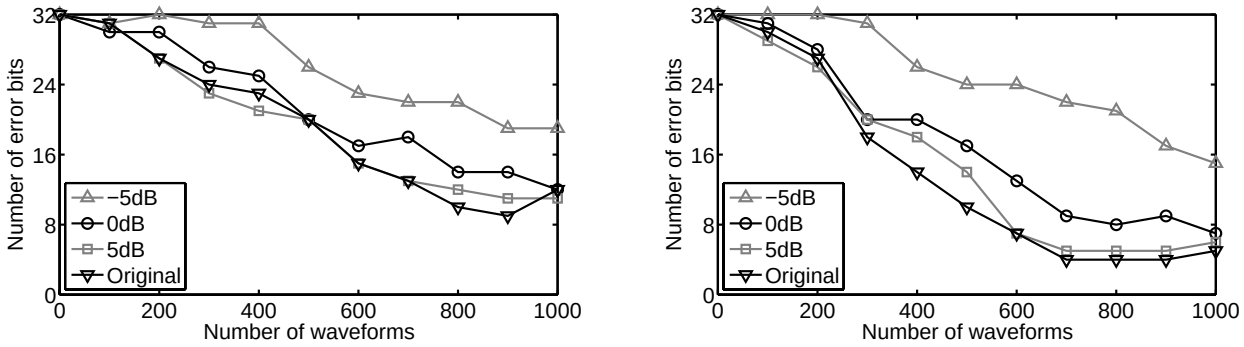


Fig. 19 Error rates for various noise levels: (a) conventional DPA, (b) proposed DPA.

forms with higher resolution than the sampling resolution. In addition to the waveform alignment, we can remove inaccurately measured waveforms by detecting significant drops of correlation peaks, eliminating their adverse effects on the statistical analysis.

The advantage of proposed method over the conventional methods was demonstrated by experimental DPAs and DEMAs against DES software and hardware implementation. The results showed that the proposed method can enhance the effectiveness of the side-channel attacks. A high success rate of finding correct subkeys was obtained even at a low sampling rate while the conventional attacks failed. At higher sampling rates, the proposed analysis requires fewer plaintexts to obtain the same error rate as the conventional analysis. As a result, we confirmed that the POC-based waveform matching can be used efficiently for both DPA and DEMA without any drawbacks. In the experiments with INSTAC-8/32 boards, we used a trigger signal synchronized with the cryptographic operations for simplicity, but the POC-based matching does not require this for aligning a number of power traces. Therefore, we are very confident that our approach is efficient for attacking cryptographic modules in actual applications, where no trigger signal or no internal clock can be observed.

The unique feature of the proposed method is its capability to enhance any side-channel analysis independently of the cryptographic algorithms, implementations (software or hardware), and kind (power or electromagnetic) of side-channel information. In addition, the proposed method can defeat the countermeasures creating distorted waveforms with random delays, dummy cycles, or unstable clocking. The proposed waveform matching clearly defeated a random-delay countermeasure that interferes with the timing-synchronization by inserting NOP operations. We are now conducting research to develop advanced matching techniques and to investigate their utility in attacks against other waveform-distortion countermeasures.

References

[1] P. Kocher, J. Jaffe, and B. Jun, "Introduction to differential power analysis and related attacks," IEEE Trans. electron devices, vol.50, no.2, pp.462–470, Feb. 1998.
[2] P. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," *CRYPTO 1999*, Lecture Notes in Computer Science, vol.1666, pp.388 – 397, Aug. 1999.
[3] K. Gandolfi, C. Mourtel, and F. Olivier, "Electromagnetic analysis: Concrete results," *CHES 2001*, LNCS, vol.2162, pp.251 – 261, May 2001.
[4] C. Clavier, J. Coron, and N. DabbousGoubin, "Differential power analysis in the presence of hardware countermeasures," *CHES 2000*, Lecture Notes in Computer Science, vol.1965, pp.252–263, Aug. 2000.
[5] 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.
[6] J. Waddle and D. Wagner, "Towards efficient second-order power analysis," *CHES 2004*, LNCS, vol.3156, pp.1 – 15, Aug. 2004.
[7] H.C. Gebotys, S. Ho, and C.C. Tiu, "EM analysis of Rijndael and ECC on a wireless Java-based PDA," *CHES 2005*, LNCS, vol.3659, pp.250 – 264, Aug. 2005.
[8] Q. Chen, M. Defrise, and F. Deconinck, "Symmetric phase-only matched filtering of Fourier-Mellin transforms for image registration and recognition," IEEE Trans. Pattern Analysis & Machine Intelligence, vol.16, no.12, pp.1156 – 1168, Dec. 1994.
[9] K. Takita, T. Aoki, Y. Sasaki, T. Higuchi, and K. Kobayashi, "High-accuracy subpixel image registration based on phase-only correlation," IEICE Trans. on Fundamentals, vol.E86-A, no.8, pp.1925 – 1934, Aug. 2003.
[10] K. Ito, H. Nakajima, K. Kobayashi, T. Aoki, and T. Higuchi, "A fingerprint matching algorithm using phase-only correlation," IEICE Trans. on Fundamentals, vol.E87-A, no.3, pp.682 – 691, Mar. 2004.
[11] K. Takita, A.M. Muquit, T. Aoki, and T. Higuchi, "A sub-pixel correspondence search technique for computer vision applications," IEICE Trans. on Fundamentals, vol.E87-A, no.8, pp.1913 – 1923, Aug. 2004.
[12] N. Homma, S. Nagashima, Y. Imai, T. Aoki, and A. Satoh, "High-resolution side-channel attack using phase-based waveform matching," *CHES 2006*, LNCS, vol.4249, pp.187–200, May 2006.
[13] 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*, no.25, pp.1–6, Jan. 2006.

[14] Cryptographic Hardware Project. http://www.aoki.ecei.tohoku.ac.jp/crypto/

[15] A.M. Muquit, T. Shibahara, and T. Aoki, "A high-accuracy passive 3D measurement system using phase-based image matching," IEICE Trans. on Fundamentals, vol.E89-A, no.3, pp.686 – 697, Mar. 2006.