Biasing power traces to improve correlation in power analysis attacks

Yongdae Kim†, Takeshi Sugawara †, Naofumi Homma †, Takaafumi Aoki †, Akashi Satoh †

†Graduate School of Information Sciences, Tohoku University
6-6-05 Aramaki Aza Aoba Aoba-ku Sendai-shi 980-8579 Japan
Email: {kimyd, sugawara, homma}@aoki.ecei.tohoku.ac.jp
aoki@ecei.tohoku.ac.jp

‡National Institute of Advanced Industrial Science and Technology
1-18-13 Sotokanda Chiyoda-ku Tokyo 101-0021 Japan
Email: akashi.satoh@aist.go.jp

Abstract—In this paper, we present a selection method of power traces to improve the efficiency of power analysis attacks. The proposed method improves the correlation factor by biasing distribution of power traces. The biasing is to select a subset from many traces. We demonstrate our method through correlation power analysis (CPA) experiments using two different devices. The results clearly show that the selection of power traces has a significant impact on the results of CPAs. Based on the selection method, an evaluation method to detect such biasing in power traces is also proposed. The method can be used to achieve fair comparison of statistical distinguishers for power analysis attacks.

I. INTRODUCTION

Power analysis attacks [1] have been serious threats to cryptographic devices. The attacks usually exploit a set of power traces measured from a target device which are correlated to internal data/operations. The assumption here is that the measured power traces have different statistical distributions depending on the operands/operations. An adversary can recover secret keys when the distributions are distinguishable.

Since the difference-of-means method was presented as a distinguisher in the primary article on Differential Power Analysis (DPA) [1], a lot of efforts have been devoted to find effective distinguishers [2]–[7]. We note that the correlation coefficient in Correlation Power Analysis (CPA) [4] is one of the most common distinguishers.

In contrast, we take an approach of changing the statistical distribution of power traces, rather than working on distinguishers. In the previous works, it is implicitly assumed that the statistical distributions are fixed and mainly determined by physical characteristics of the target device. However, they can be biased when particular subset of traces are selected from a larger set. As a result, the efficiencies of conventional power analysis attacks are improved when the biased traces are used. The idea of selecting power traces was firstly proposed in [8]. In the article, masking countermeasure is compromised by selected traces to bias the statistical distribution of a random mask.

On the other hand, we introduce a selection method that can be used to reduce the number of power traces to reveal keys. Our method is as a pre-processing technique to improve the performance of the following conventional analysis. In addition, we present a method to evaluate such biasing in the set of power traces since the selected sets potentially cause an unfair comparison between distinguishers.

Our preliminary result was posted to the DPA Contest 2008/2009 [9]. This paper focuses on the selection method tailored to CPA, yet the same strategy can be extended to other distinguishers. The advantage of the proposed method is examined through actual experiments on two different cryptographic devices: (i) FPGA implementation of AES (Advanced Encryption Standard) and (ii) ASIC implementation of DES (Data Encryption Standard). The results show that the selection of power traces achieves a significant reduction in the value of measurement to disclosure (MTD).

II. FORMALIZATION OF POWER TRACES

This section describes our power consumption model and derives the equation of correlation coefficient for CPAs. The basic characteristics of power traces are discussed from the viewpoint of correlation which is used in CPA. Then, we mention how to improve the correlation factor.

A. Power Consumption

Let $P_{total}$ be a power consumption observed from a cryptographic device. $P_{total}$ is represented as a sum of two components, $P_{data}$ and $P_{noise}$, that is

$$P_{total} = P_{data} + P_{noise},$$

(1)

where $P_{data}$ is the power consumption depending on the processed data, and the remaining $P_{noise}$ is the noise component (i.e., electronic noise in the measurement setup). The relationship between $P_{data}$ and the processed data is determined by a power model (e.g., Hamming weight model and Hamming distance model). On the other hand, $P_{noise}$ is approximated by a normal distribution in most cases.
B. Correlation Coefficient

One of the improved power analysis attacks is Correlation Power Analysis (CPA), which employs Pearson’s correlation coefficient $\rho$ to evaluate the linear relationship between $P_{\text{total}}$ and the processed data.

Assume that we have $N$ power consumptions corresponding to $N$ different inputs and $N$ is large enough. Let $g_i$ ($1 \leq i \leq N$) denote a power consumption at the $i$-th input, which is given by

$$g_i = s_i + w_i,$$  

(2)

where $s_i$ is the data-dependent component corresponding to $P_{\text{data}}$, and $w_i$ is the data-independent component corresponding to $P_{\text{noise}}$. The assumption considered here is that $s_i$ is perfectly correlated to the processed data and $w_i$ is subjected to a normal distribution with a mean of 0 and a standard deviation of $\sigma_{\text{noise}}$ described as

$$w_i \sim N(0, \sigma_{\text{noise}}).$$  

(3)

Now, we assume that the parallel implementation of a cryptographic algorithm with $M$ S-boxes processed simultaneously. When the contribution of the $j$-th S-box at the $i$-th input is represented as $h_{ij}$ ($1 \leq i \leq N, 1 \leq j \leq M$), $s_i$ is given as

$$s_i = \sum_{j=1}^{M} h_{ij}.$$  

(4)

The mean $E(h_{ij})$ and the variance $\text{var}(h_{ij})$ are represented as

$$E(h_{ij}) = \frac{1}{N} \sum_{i=1}^{N} h_{ij} = \mu,$$  

(5)

$$\text{var}(h_{ij}) = \frac{1}{N} \sum_{i=1}^{N} (h_{ij} - \mu)^2 = \sigma^2,$$  

(6)

respectively. This is because the $N$ data are truly at random, and processed independently in $M$ S-boxes. The mean and the variance of $s_{ij}$ are provided by a sum of those of $h_{ij}$ as

$$E\left(\sum_{j=1}^{M} h_{ij}\right) = \sum_{j=1}^{M} E(h_{ij}) = M\mu,$$  

(7)

$$\text{var}\left(\sum_{j=1}^{M} h_{ij}\right) = \sum_{j=1}^{M} \text{var}(h_{ij}) = M\sigma^2,$$  

(8)

respectively. The Pearson’s correlation coefficient $\rho_j$ between $g_i$ and $h_{ij}$ is defined as

$$\rho_j = \frac{\text{cov}(g_i, h_{ij})}{\sqrt{\text{var}(g_i)\text{var}(h_{ij})}}.$$  

(9)

(8) as follows:

$$\text{cov}(g_i, h_{ij}) =$$  

$$= E((g_i - E(g_i))(h_{ij} - E(h_{ij})))$$  

(10)

$$= E((s_i + w_i - E(s_i) - E(w_i))(h_{ij} - \mu))$$  

(11)

$$= E((s_i + w_i - M\mu)(h_{ij} - \mu))$$  

(12)

$$= E((s_i - M\mu)(h_{ij} - \mu)) + E(w_i)(h_{ij} - \mu))$$  

(13)

$$= E\left(\sum_{k=1}^{M} h_{ik} - M\mu\right)(h_{ij} - \mu)$$  

(14)

$$+ E(w_i)(h_{ij} - \mu)$$  

$$= E\left(\sum_{k=1}^{M} (h_{ik} - \mu)\right)(h_{ij} - \mu)$$  

(15)

$$= E((h_{ij} - \mu)^2) (\text{only if } k = j, \text{ otherwise } 0)$$  

(16)

$$= \sigma^2$$  

(17)

Also, $\text{var}(g_i)$ can be simplified using Eq. (8) as

$$\text{var}(g_i) = \text{var}\left(\sum_{k=1}^{M} h_{ik} + w_i\right)$$  

(18)

$$= \sum_{k=1}^{M} \text{var}(h_{ik}) + \text{var}(w_i)$$  

(19)

$$= M\sigma^2 + \sigma^2_{\text{noise}}.$$  

(20)

Using Eqs. (17) and (20), therefore, $\rho_j$ is represented as

$$\rho_j = \frac{\text{cov}(g_i, h_{ij})}{\sqrt{\text{var}(g_i)\text{var}(h_{ij})}}$$  

(21)

$$= \frac{\sigma}{\sqrt{(M\sigma^2 + \sigma^2_{\text{noise}})\sigma^2}}$$  

(22)

$$= \frac{1}{\sqrt{\left(M + \frac{\sigma^2_{\text{noise}}}{\sigma^2}\right)}}$$  

(23)

$$= \frac{1}{\sqrt{\left(M + \frac{1}{N}\right)}},$$  

(24)

where $\text{SNR}$ represents the signal-to-noise ratio given by the variance of $h_{ij}$ and $w_i$.

III. BIASING POWER TRACES

This section presents a method of selecting a biased subset of power traces from a larger set of power traces. An evaluation method to detect the bias in power traces is also presented.

A. Method of choosing biased power traces

To improve the correlation coefficients, many papers have been only focused on finding efficient distinguishers [5], [6]. In this paper, however, we focus on a pre-processing technique choosing biased power traces to improve the correlation coefficient. As shown in Eq. (24), the SNR should be increased
to achieve the higher correlation coefficient, \( \rho \). However, the noise component \( \sigma_{\text{noise}}^2 \) is uncontrollable and determined by the target device and the measurement. On the other hand, the variance \( \sigma^2 \) can be changed to have a higher correlation coefficient. It can be achieved by intentionally choosing a subset of measured traces so that \( \sigma^2 \) is maximized. According to Eq. (20), the maximization of \( \sigma^2 \) is equivalent to that of \( \text{var}(q_i) \). Therefore, the subset can be chosen by the following method.

First, let \( N_1 \) and \( N_2 \) denote the number of chosen power traces and total power traces, respectively.

1. Determine a time index \( t_{ct} \) which is the most relevant time index to the processed data using \( N_2 \) power traces.
2. Calculate a mean, \( \mu_p \) and a variance, \( \sigma_p^2 \) of power consumption at \( t_{ct} \) using \( N_2 \) power traces.
3. Describe the normal distribution of power consumption (see Fig. 1(a)) by the probability density function with parameters \( \mu_p \) and \( \sigma_p^2 \) as given by:

\[
f(x) = \frac{1}{\sqrt{2\pi \sigma_p^2}} \exp\left(-\frac{(x - \mu_p)^2}{2\sigma_p^2}\right) .
\]

4. Sort \( N_2 \) power traces by the probability density function.
5. Extract \( N_1 \) power traces from \( N_2 \) power traces in order for increasing the probability (see Fig. 1(b)).

This method assumes that the power consumption \( q_i \) is approximated by a normal distribution. The assumption is based on the fact that each bit of in the processed data is changed independently with a probability of 0.5, and follows the binomial distribution. Thus, the sum of transitions for all the bits can be approximated by the normal distribution. This approximation is reasonable since the bit-length \( L \) is large enough in practice (e.g., \( L = 64 \) in DES).

Figure 1(b) shows that the extracted power traces are away from the mean. It is intuitive that the variance of these traces is high. Such a distribution is well investigated in statistics and referred to as a truncated distribution [10]. The variance of the truncated distribution is higher than that of the original distribution.

### B. Evaluation of power traces

The use of the above biased power traces would happen intentionally or unintentionally, resulting in an unreliable evaluation of cryptographic modules. In other words, a set of power traces based on a normal distribution would be preferable for evaluation. Thus, we can evaluate the set of power traces by the distribution. Such evaluation is achieved by testing normality of the traces. For the quantification of normality, one of the well-known test methods is a modification of the Kolomogorov-Smirnov test, which is generally referred to as the Lilliefors test [11]. If the Lilliefors test statistic is small enough, it can be said that the set of power traces follows a normal distribution.

### IV. EXPERIMENTAL RESULTS

This section demonstrates the effectiveness of biasing power traces through CPA experiments. In addition, we show a method of evaluating whether the power traces are selected to improve the results of power analysis attacks.

Our experiments employed power consumption traces from (i) DES and (ii) AES circuits. The experiment (i) was conducted on the DES crypto-processor implemented on an ASIC called SecmatV3 SoC in 2008/2009 DPA contest [9]. The experiment (ii) is performed on the AES circuit implemented in a Xilinx FPGA on the Side-channel Attack Standard Evaluation Board (SASEBO) [12]. The total numbers of measured traces are (i) 80,000 and (ii) 150,000, respectively. Figures 2(a) and (b) show the measured power trace of DES and AES, respectively.

In order to choose the biased set of power traces, we determined a point \( t_{ct} \) by computing the correlation coefficients between the power consumption and the processed data of DES and AES. The determined points are 724 ns and 593 ns for DES and AES, respectively.

Using the values at the point, we selected the biased set of power traces according to the method described in the previous section. We also selected the same number of power traces at random for comparison. In this procedure, 300 and 3,000 traces are selected for the experiments (i) and (ii), respectively.

Figures 3 and 4 show the transitions of correlation coefficient values (MTD : measurement to disclosure) in CPAs on DES and AES, respectively. In each figure, the black line

---

1The point can also be determined by SPA. For example, we can determine the point of AES in the experiment since the unique pattern of 10th round (i.e. the target round) is observed by SPA. Another possible method is to utilize a reference device. In this case, such point would be found by the selection method for Template Attacks. However, we do not discuss the efficient method of selecting of the point in this paper.
indicates the transition of the correct key and the gray lines indicate those of wrong keys. Figures 3(a) and 4(a) are the results of power traces selected at random, and Figs. 3(b) and 4(b) are those of biased power traces selected by our method. It is obvious that the correlation results were improved using the biased power traces. More precisely, the MTDs of the biased power traces in Figs 3 and 4 are 2.5 and 8.0 times smaller than those of the randomly-selected power traces, respectively.

Figure 5 shows the classification rates of CPAs using the two types of power traces. The vertical axis indicates the classification rate representing the number of S-boxes where we could distinguish a correct key from all possible key candidates. If all correct keys were obtained, the classification rate is 100. The horizontal axis is the number of traces used in the CPA. We can confirm from Fig. 5 that the characteristics of power-trace sets have a significant impact on the results of power analysis attacks independently of cryptographic algorithms and implementation platforms.

Table I shows the variance $\sigma^2$ and the Lilliefors test statistic $D$ used in the above experiments. We present the product of $\sigma^2$ and $D$ as an evaluation matrix of power trace sets. The biased power traces have a specific property of increasing both the components. As the value of $\sigma^2D$ increases, the probability that the power traces were biased for the improvement of power analysis attacks increases.

**V. CONCLUSION**

In this paper, we presented a method of selecting a biased set of power traces for the improvement of power analysis attacks. The selection method can also be available for examining power traces for the fair evaluation of attacks. We confirmed that the significant MTD improvements in CPAs were achieved by the selection method for two different algorithms and platforms. The results suggest that the characteristics of power traces should be fairly considered for evaluating power analysis attacks.

**REFERENCES**