Efficient Key Detection Method in the Correlation Electromagnetic Analysis Using Peak Selection Algorithm

You Sung Kang, Doo Ho Choi, Byung Ho Chung, Hyun Sook Cho, and Dong-Guk Han

Abstract: **A side channel analysis is a very efficient attack against small devices such as smart cards and wireless sensor nodes. In this paper, we propose an efficient key detection method using a peak selection algorithm in order to find the advanced encryption standard secret key from electromagnetic signals. The proposed method is applied to a correlation electromagnetic analysis (CEMA) attack against a wireless sensor node. Our approach results in increase in the correlation coefficient in comparison with the general CEMA. The experimental results show that the proposed method can efficiently and reliably uncover the entire 128-bit key with a small number of traces, whereas some extant methods can reveal only partial subkeys by using a large number of traces in the same conditions.**

Index Terms: **Correlation power analysis (CPA), cryptanalysis, electromagnetic analysis, peak selection, side channel attack (SCA).**

I. INTRODUCTION

Commercial availability of ubiquitous computing devices now provides numerous attractive applications to consumers. Many researchers have developed small digital devices contributing to the realization of a ubiquitous computing era. Some of representative devices are smart cards, radio frequency identification (RFID) tags, and wireless sensor nodes. However, the ubiquity of computing devices increases the number of security challenges which a system designer must cope with. Since such devices will be used in hostile environments and often include sensitive information such as identity related tokens, it is important for devices to endure the threat of attack. Initial efforts to protect these digital devices have mainly focused on traditional security mechanisms such as data encryption, access control, and privacy protection. However, complicated and physical attacks on cryptographic devices have recently become a very powerful threat.

A side channel analysis (SCA) is a kind of physical attacks that infer the internal operation and data of small digital devices. The SCA attack usually uses some measurable non-mathematical properties of a cryptographic device, such as power consumption [1] or electromagnetic (EM) emanations [2]. These information-leakage signals are called the side channel signals (or information). In [1], the measured side channel signals are called traces. For example, a trace is a set of EM emanation measurements taken through a cryptographic operation of a smart card or a wireless sensor node. A general side channel analysis method is a simple power analysis (SPA), whereby the internal cryptographic operation is identified [3]. There are more powerful SCA attack methods such as the differential power analysis (DPA) and the correlation power analysis (CPA). The former is introduced in [1] and well formalized in [4] and the latter is reported in [5] as an alternative to the former. When these methods are applied to electromagnetic signals, they are referred to as the simple electromagnetic analysis (SEMA), differential electromagnetic analysis (DEMA), and correlation electromagnetic analysis (CEMA), respectively [6], [7].

Many research results have shown that these attacks can reveal the secrets of the block cipher algorithm operated in smart cards [1]–[12]. Mangard *et al*. published the SCA techniques on smart cards in book form [13]. However, research so far has largely focused on smart card security. Recently, security analyses of RFIDs [14], [15] and personal digital assistants (PDAs) [16] have been proposed.

In comparison with smart cards, performing SCA attacks against PDAs and wireless sensor nodes presents more challenging problems, since there could be a temporal misalignment of traces due to unstable trigger, unstable clock, non-constant time implementation, and some countermeasures. In general, the temporal misalignment of signals is a very crucial problem that decreases the SCA efficiency because misaligned signals affect other normal signals as if unintentional noises [17], [18]. The misalignment sources can be categorized into two groups. The first one is unintentionally caused by the device or measurements [19] and the second one is due to intentional works of device developers, for example, the random process interrupts [20]. Because the side channel information depends on a variety of operations that include complicated control on the device as well as cryptographic operations, the SCA attack on a wireless sensor node using intentional implementation techniques is more difficult than that on a PDA with misalignment signals [21].

In [19], a new SCA attack method called the differential frequency analysis (DFA) was proposed to overcome the misalignment problem caused in PDAs. Due to the severer misalignment of traces obtained from wireless sensor nodes than that from PDAs, a general CEMA fails to find the secret information stored in the wireless sensor node and the DFA can reveal only partial secret information with a large number of traces, as determined from our experimental results. The motivation of this paper is to solve the severe temporal misalignment problem in the SCA attack on a wireless sensor node and develop a means of finding all the secret information by using a small number of

Manuscript received April 29, 2009.

This work was supported by the IT R&D program of MKE/KEIT. [2009-F-055-01, Development of the Technology of Side Channel Attack Countermeasure Primitives and Security Validation].

Y. S. Kang, D. H. Choi, B. H. Chung and H. S. Cho are with the Knowledge-based Information Security Research Department, ETRI, Daejeon, 305-700, Korea, email: {youskang, dhchoi, cbh, hscho}@etri.re.kr.

D.-G. Han is with the Mathematics Department, Kookmin University, Seoul, 136-702, Korea, email: christa@kookmin.ac.kr.

traces.

In this paper, we propose an efficient key detection method using a peak selection algorithm to overcome the temporal misalignment on EM traces. And we apply the proposed method to a wireless sensor node and analyze related experimental results. Our approach using the proposed peak selection algorithm results in increase in the correlation coefficient in comparison with the general CEMA. The experimental results show that the proposed peak selection algorithm can address a temporal misalignment problem and detect the entire 128-bit key of the advanced encryption standard (AES) used in a wireless sensor node with fewer than 500 traces.

This paper is organized as follows. In Section II, related works are briefly reviewed. Our proposed peak selection algorithm and key-decision metric are then explained in Section III. In addition, an attack against a wireless sensor node is described and the experimental results are analyzed in Section IV. Finally, Section V draws a conclusion.

II. RELATED WORKS

The first phase of a normal SCA attack is to acquire information-leakage signals which are called traces. In the case of CEMA, an EM emanation can be treated as a trace and expressed as $T_{1\cdots m}[1\cdots n]$, where m is the number of encryption operations and n is the number of samples per encryption operation [1]. Because one encryption operation creates one trace, m becomes the number of traces. We use the term EM traces hereafter.

A. Correlation Electromagnetic Analysis

CEMA exploits the relation between the EM trace of the attacked device and a hypothetical model. The representative models used in correlation approaches are the Hamming weight model and the Hamming distance model. Brier *et al*. used the Hamming distant model and obtained good results [5].

In [5], the basic model for the measured traces is defined as follows:

$$W = cH(D \oplus R) + b \tag{1}$$

where D is p independent and uniformly distributed bits and R is a reference state that is an unknown constant machine word. In the leakage model based on state transitions triggered by the edges of a clock signal, the number of flipping bits to go from R to D is the Hamming distance, that is, $H(D \oplus R)$. c is a scalar gain between the Hamming distance $H(D \oplus R)$ and the measured traces W. A term denoted b includes offsets, time dependent components and noise, which are caused during collecting traces. We denote $H(D \oplus R)$ by H hereafter.

The measured EM trace W and the Hamming distance D have a linear relationship. Therefore, the guessed key which maximizes their correlation coefficient becomes the correct key. In other words, if the correlation coefficient is very high, i.e., it is close to $+1$ or -1, it is usually assumed that the key hypothesis is correct.

B. Forced Alignment of Traces

The simplest way to alleviate the effect of the temporal misalignment is to compulsorily align traces. In general, a good approach to align two traces is to use cross-correlation [22]. The forced alignment method using cross-correlation first defines a window size, and then cross-correlation between two traces is performed only in this window. It is therefore necessary to decide a basis trace, i.e., the first trace or the middle trace among all measured traces, to align many traces. In the case of usual traces except for the basis trace, data in the defined window is shifted to the left or right as necessary after cross-correlation is calculated. Next, the window is moved forward by a given amount, and the procedure is repeated up to the last point of the trace. While this method can mitigate the temporal misalignment, it unavoidably requires complex computations and long attack time.

C. Differential Frequency Analysis

Another solution to reduce the effect of the trace misalignment is to use a frequency-based differential analysis [19]. This method is called a differential frequency analysis (DFA) and is based on signal processing techniques, especially fast Fourier transform (FFT). The main feature of the DFA is the analysis of traces in the frequency domain and it is essentially based on the time shifting property of the discrete fourier transform for periodic signals. This property means that a shift in the time domain leaves the magnitude unchanged but causes a linear phase shift in the frequency domain. Although most traces are not exactly periodic signals, the frequency contents of most traces are less vulnerable to the effects of time shifts. Therefore, by analyzing traces in the frequency domain, the effect of the temporal misalignment can be reduced without perfect alignment. However, this method requires large memory and long attack time, because the FFT is complicated computation.

III. PROPOSED METHODS

In this section, we propose and explain a peak selection algorithm to eliminate the effect of the temporal misalignment as well as a key-decision metric to improve the reliability of key-decision.

A. Peak Selection Algorithm

It is necessary for an attacker to know which points of the EM traces contain useful information. It is widely accepted that exploitable signals are present in several peaks of the power consumption in the case of a power trace analysis [13]. However, this is not always true. In particular, the temporal misalignment of traces tends to affect the analysis of the leakage signals for a single point.

In this paper, we propose a peak selection algorithm using peak points of the EM traces and some neighboring points of each peak. As this method realigns the EM traces with selected peaks and neighboring points, it can efficiently reconstruct the condensed EM traces such that they are similar to well-aligned traces. An example of the realignment using the proposed peak selection algorithm is illustrated in Fig. 1. In this example, only 9 points are selected among the 24 sampling points which is a window size. If 9 points from each window are selected around the peak point in the other traces, the realigned traces will be well-aligned traces. Algorithm 1 describes the proposed peak

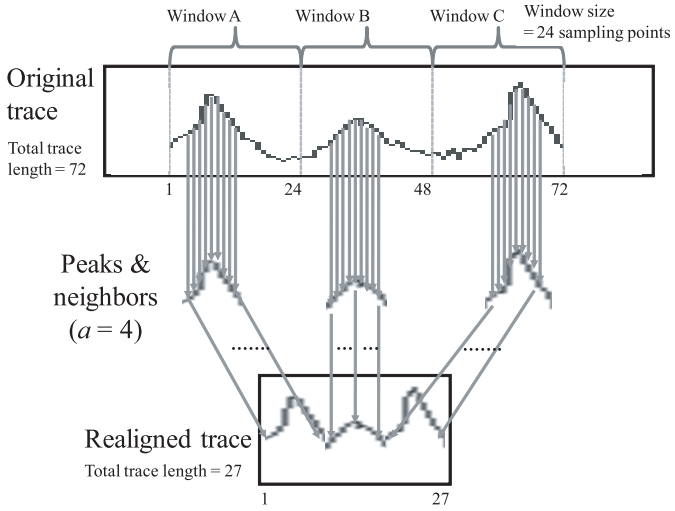

Fig. 1. Realignment using the proposed peak selection algorithm.

Algorithm 1 Peak selection method

1: INPUT: Measured EM traces $T_{1\cdots m}[1\ldots n]$, neighboring point of the peak position a, window size s
2: OUTPUT: Realigned EM traces $T'_{1\cdots m}[1\ldots n']$
3: $index \leftarrow 1$;
4: $flag \leftarrow 1$;
5: **for** $i \leftarrow 1$ to m **do**
6: $[peakval, peakpos] \leftarrow max(T_i(index : index + s))$;
7: $T'_i(flag : flag + a \times 2) \leftarrow T_i(index + peakpos - a : index + peakpos + a)$;
8: $index \leftarrow index + s$;
9: $flag \leftarrow flag + a \times 2$;
10: **end for**
11: Return $T'_{1\cdots m}[1\ldots n']$

selection algorithm. This algorithm is described by means of the MATLAB coding style, and thus it can help the reader visualize our experiment. We use the following variables for Algorithm 1.

- $index$: original index for sampling points
- $flag$: realigned index for points
- $peakval$: peak value of points in window size
- $peakpos$: position of peak value

The measured EM traces, $T_{1\cdots m}[1\cdots n]$, can be treated as an n by m matrix, where n is the number of sampling points and m is the number of the measured EM traces. Similarly, the output EM traces, $T'_{1\cdots m}[1\cdots n']$, are an n' by m matrix, where n' is the reduced number of sampling points after preprocessing for realignment. One peak position is selected in each block of window size s, which is a disjoint block. The neighboring point a affects both sides of the peak position, and hence the number of points for the output EM traces is $(a \times 2) + 1$ including the peak position in each block of window size s.

We apply the well-aligned EM traces to a CEMA attack. A general correlation analysis attack first acquires a set of m EM traces while a given algorithm is being computed (w_i for $1 \leq i \leq m$, where m is the number of traces, as mentioned above), and attempts to predict the Hamming distance during an internal state transition (h_i for $1 \leq i \leq m$). The correlation coefficient between the instantaneous sampling points of the set of measured traces W and these Hamming distance predictions H can be calculated as follows [5], [23]:

$$\rho_{1\cdots k}[1\cdots n] = \rho_{WH} = \frac{cov(W,H)}{\sigma_W \sigma_H}. \quad (2)$$

Using (1), Equation (2) can be replaced with (3) under the uncorrelated noise assumption [5].

$$\rho_{WH} = \frac{cov(W,H)}{\sigma_W \sigma_H} = \frac{cov((cH+b),H)}{\sigma_W \sigma_H} = \frac{c\sigma_H}{\sigma_W}. \quad (3)$$

From (3), we can know that the correlation coefficient is affected by the standard deviation of the measured traces W, σ_W. In other words, the correlation coefficient at a certain sampling point is improved if σ_W at that point is decreased.

The proposed peak selection algorithm reduces σ_W by realigning the measured traces around each peak. This feature leads to the increase of the correlation coefficient and makes the efficient key detection possible.

B. Key-Decision Metric

We define a new metric to evaluate the success of an attack. The metric is based on correlation coefficients and reflects the key detection possibility. In other words, if a guessed key satisfies the condition of the proposed key-decision metric, we can guarantee that it is the correct key. Algorithm 2 describes the proposed key-decision metric. This is also described by means of the MATLAB coding style. We use the following variables for Algorithm 2.

- k : guessed key value
- $maxval$: maximum value of original correlation coefficients
- $maxidx$: position of maximum value
- $corrmean\_a$: mean of correlation coefficients in the first step
- $newcorr\_a$: new correlation coefficients subtracting $corrmean\_a$ from original correlation coefficients in the first step
- $maxval\_a$: new maximum value of new correlation coefficients in the first step
- $maxidx\_a$: position of new maximum value in the first step
- $newmean\_a$: new mean of new correlation coefficients in the first step
- hmr_a : new maximum value divided by new mean in the first step
- $corrhmr\_a$: maximum values of original correlation coefficients passing the threshold of the first step, which is a vector of 1 by 256
- $keycorr$: maximum value of $corrhmr\_a$
- $keyval$: position of maximum value of $corrhmr\_a$, which is a guessed key value
- $zeropos$: position with zero value of $corrhmr\_a$
- $corrmean\_b$: mean of $corrhmr\_a$ without zero value
- $newcorr\_b$: new values subtracting $corrmean\_b$ from $corrhmr\_a$
- $maxval\_b$: new maximum value of new values in the second step
- $maxidx\_b$: position of new maximum value in the second step

Algorithm 2 Key-decision metric

1: INPUT: Correlation coefficients $\rho_{1\ldots k}[1\ldots n]$
2: OUTPUT: Ratio of highest value to mean value of correlation coefficients HMR, detected key d
3: **for** $i \leftarrow 0$ to k, where, $k = 255$ **do**
4: $[maxval, maxidx] \leftarrow max(\rho_i)$;
5: $corrmean\_a \leftarrow mean(\rho_i)$;
6: $newcorr\_a \leftarrow (\rho_i - corrmean\_a)$;
7: $[maxval\_a, maxidx\_a] \leftarrow max(newcorr\_a)$;
8: $newmean\_a \leftarrow mean(newcorr\_a)$;
9: $hmr\_a \leftarrow maxval\_a/newmean\_a$;
10: **if** $hmr\_a \geq 7$ **then**
11: $corrhmr\_a_i \leftarrow maxval$;
12: **else**
13: $corrhmr\_a_i \leftarrow 0$;
14: **end if**
15: **end for**
16: $[keycorr, keyval] \leftarrow max(corrhmr\_a)$;
17: $zeropos \leftarrow find(corrhmr\_a == 0)$;
18: $corrhmr\_a(zeropos) \leftarrow [\,]$;
19: $corrmean\_b \leftarrow mean(corrhmr\_a)$;
20: $newcorr\_b \leftarrow (corrhmr\_a - corrmean\_b)$;
21: $[maxval\_b, maxidx\_b] \leftarrow max(newcorr\_b)$;
22: $newmean\_b \leftarrow mean(newcorr\_b)$;
23: $hmr\_b \leftarrow maxval\_b/newmean\_b$;
24: **if** $hmr\_b \geq 7$ **then**
25: $HMR \leftarrow hmr\_b; d \leftarrow keyval$;
26: **else**
27: $HMR \leftarrow null; d \leftarrow null$;
28: **end if**
29: Return HMR and d

- $newmean\_b$: new mean of new values in the second step
- hmr_b : the final maximum value divided by new mean in the second step
- HMR : the final metric passing the threshold of the second step, the correct key can be obtained from positions of the surviving HMRs

The input correlation coefficients $\rho_{1\cdots k}[1\cdots n]$ of Algorithm 2 can be treated as an n by k matrix, where n is the number of sampling points and k denotes an 8-bit guessed key, i.e., 0x00 to 0xFF. The outputs of Algorithm 2 are the detected key d and the ratio of the highest value to the mean value HMR, which is a new metric defined in this paper. The HMR is an abbreviation for the ratio of the highest value of correlation coefficients to the mean value of correlation coefficients. The final key is decided one by one on each byte, because the input matrix of correlation coefficients is related to a byte-based analysis in the case of the AES-128 block cipher algorithm.

The existing correlation analysis attack usually considers a guessed key corresponding to the maximum correlation coefficient as a correct key. The correlation analysis attack is well explained in [5]. In the case of well-aligned traces, if a correct key is found from the highest correlation coefficient at a certain number of traces, the correct key can be always detected by using more than the amount of traces. However, the severe temporal misalignment of the EM traces obtained from the wireless sensor node cause an unsteady key-decision as the number of traces increases. Therefore, a reliable key-decision metric that is not affected by the temporal misalignment is needed.

A high HMR implies that the correlation coefficient related to the correctly guessed key is comparatively high and the others are low. According to Algorithm 2, there are two-step calculations. The first step is to remove the effect of an abnormal peak value among correlation coefficients; this step is pertinent to the operation of line 5 to line 9. It calculates a HMR for sampling points per each guessed key, thus a set of correlation coefficients after line 15, $corrhmr\_a$, becomes a vector of 1 by 256. Here each component denotes the maximum correlation coefficient for each key or 0. The second calculation step is for providing the reliability to the attacker; this step is related to the operation of line 19 to line 23. It counts a HMR between the correlation coefficient corresponding to the correct key and the others. The final output successfully passing the threshold of the HMR becomes the detected key d. The threshold of the HMR should be searched by a heuristic method; 7 is used as the threshold in this paper. Our experiments show that a steep slope rises at about 320 traces with more than neighboring point of 3 and the value of 7 is the most adequate to the threshold for our experimental environment as described in Fig. 7. If this key-decision metric is applied to a CPA or CEMA attack, the correct key can be rapidly and reliably obtained, because two-step examinations of the HMR can filter the effects of the correlation coefficient peaks that result from incorrect keys.

Table 1. Experimental conditions.

Category	Contents
Target sensor note	*Telos* mote
Target processor	MSP 430 (8 MHz, 16-bit RISC)
Cipher algorithm	AES-128 encryption algorithm
Oscilloscope sampling rate	200 MHz
Trace source	Electromagnetic traces
Acquired traces	5,000
Analysis method	Correlation analysis
Analysis model	Hamming distance model

IV. EXPERIMENTAL RESULTS AND ANALYSIS

The purpose of the experiment is to demonstrate that the proposed peak selection algorithm and key-decision metric can efficiently discover the 128-bit AES secret key from misaligned EM traces of a wireless sensor node. Fig. 2 shows the CEMA attack procedure using the proposed peak selection algorithm and key-decision metric. The attack procedure consists of three parts; the EM traces acquisition phase, the EM traces analysis phase, and the result checking phase, which are explained in Subsections *B*, *C*, and *D*, respectively.

A. Experiment Environment

In order to evaluate the performance of the proposed method and metric, we prepared a high sample rate oscilloscope, an EM probe of *Near Field Probe Set LF1* [24], a power supply, and a wireless sensor node of *Telos*, in which the AES-128 encryption is performed. Fig. 3 is a photograph of the actual experimental setup and Table 1 summarizes the experimental conditions.

B. EM Traces Acquisition

Using the setup shown in Fig. 3 and outlined in Table 1, we first recorded EM traces of the target sensor node with 200 MHz

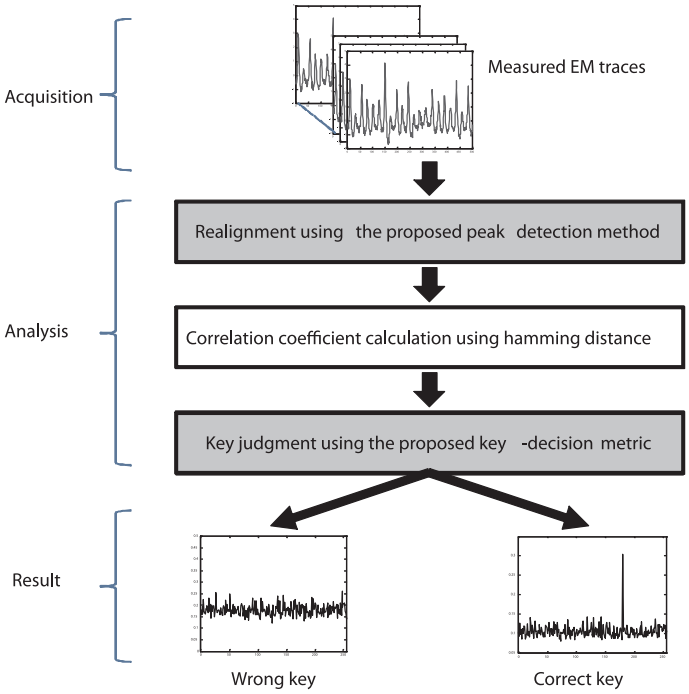

Fig. 2. CEMA attack procedure using the proposed peak selection algorithm and key-decision metric.

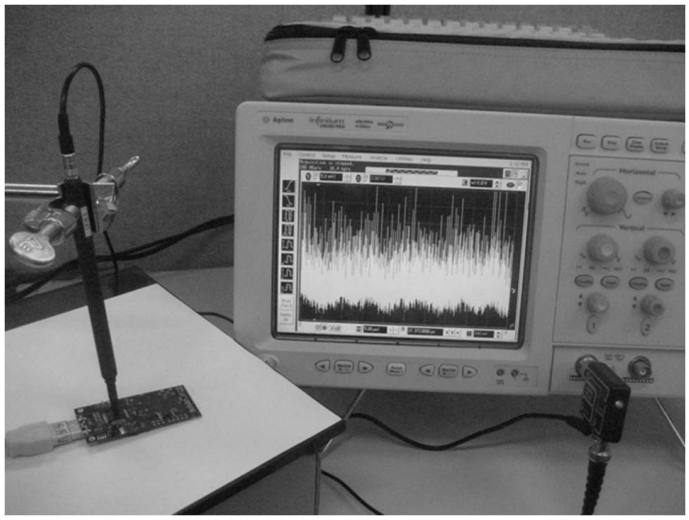

Fig. 3. Experimental setup for measuring EM traces from a wireless sensor node.

sampling frequency while the node has encrypted 5,000 random plaintexts. The EM traces are acquired at the next point of S-Box passing of the first round of AES-128 encryption. Fig. 4 shows a portion of the 1,000 EM traces which are measured in the experiment. The figure shows the actual temporal misalignment of the EM traces.

C. EM Traces Analysis

C.1 Realignment of EM Traces

The forced alignment method, a traditional alignment method, has some troubles in achieving the desired effect in the case of a serious misalignment such as that shown in Fig. 4.

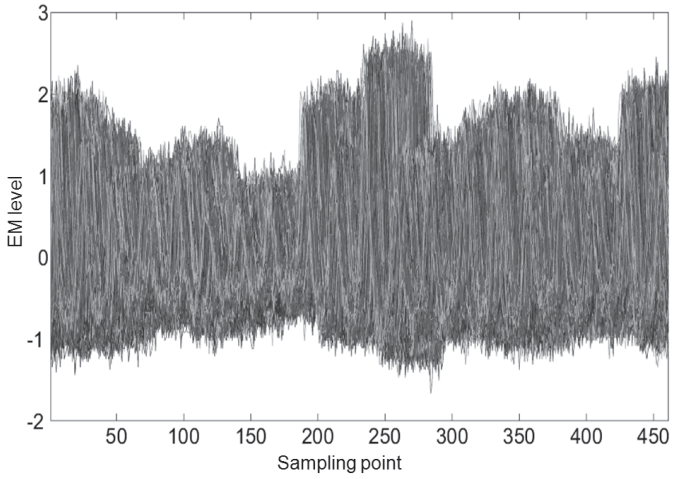

Fig. 4. Misaligned EM traces.

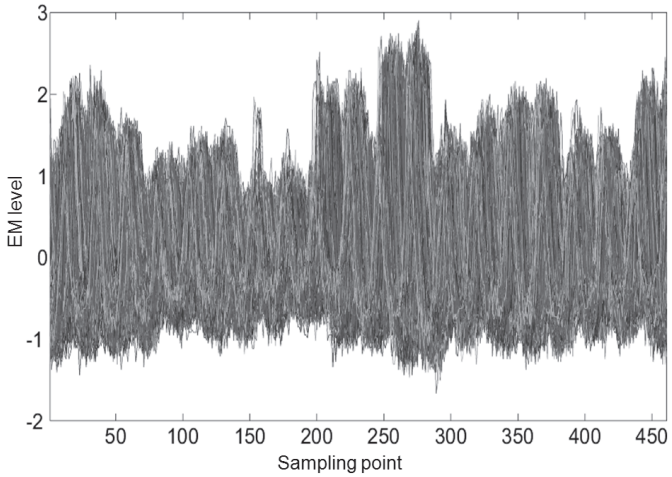

Fig. 5. Realigned EM traces using the forced alignment method.

Fig. 5 depicts the realigned EM traces for the traces of Fig. 4 using the forced alignment method.

Before correlation coefficient calculation for the measured EM traces, we realigned the EM traces using Algorithm 1 to remove the effect of the temporal misalignment. We first selected 25 as the window size s because the oscilloscope sampling frequency of 200 MHz is 25 times larger than the processor clock frequency (i.e., 8 MHz). But the window size of 24 provided excellent results in the real test, and hence was chosen as the window size s. The main processor clock signal of the target sensor node is generated from a digitally controlled oscillator and is configured by the software [25]. Some variations ($\sim 9ns$) on one period of the clock signal were found in the experiment. This is why the window size of 24 is better than the window size of 25. We applied 0, 1, 2, 3, 4, 5, 6, and 7 to the neighboring point a, and thereby obtained 1, 3, 5, 7, 9, 11, 13, and 15 points every 24 sampling points, respectively. Fig. 6 shows the realigned EM traces for the traces of Fig. 4 using the proposed peak selection algorithm with $a = 4$, which means extraction of 9 points among 24 sampling points. From the visual inspection, it is readily apparent that the proposed method is superior to the forced alignment method.

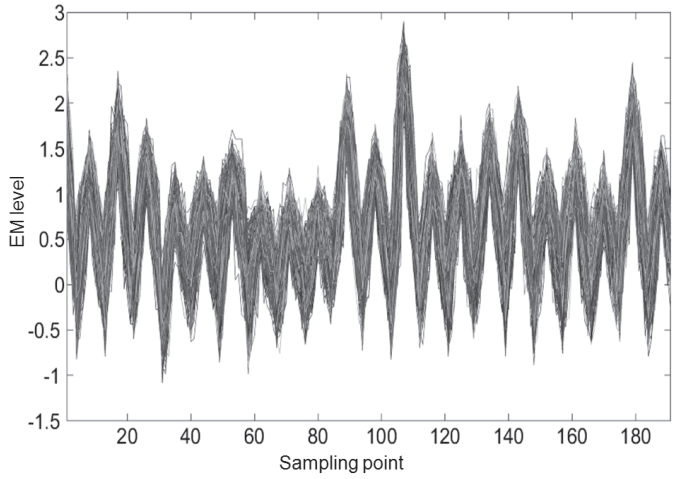

Fig. 6. Realigned EM traces using the proposed peak selection algorithm (Neighboring point a = 4.)

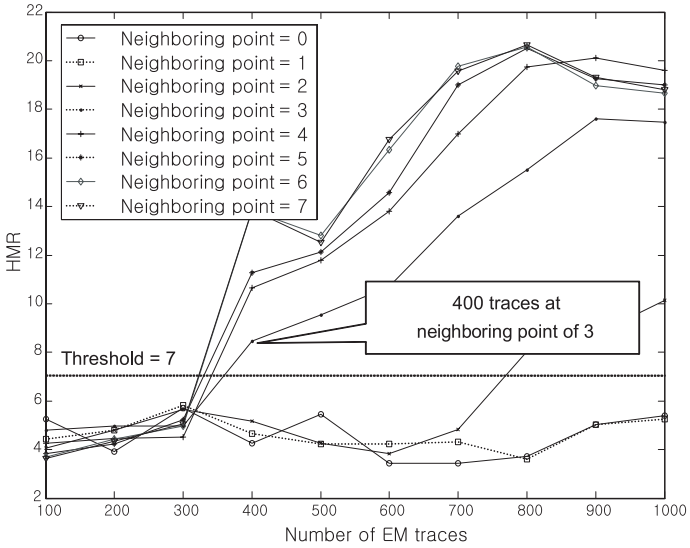

Fig. 7. HMR variation according to number of EM traces (in the case of the second subkey).

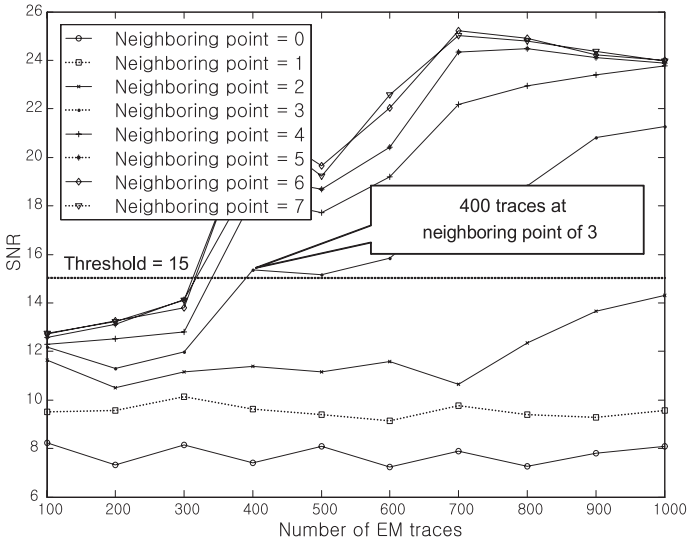

Fig. 8. SNR variation according to number of EM traces (in the case of the second subkey).

C.2 Calculation of Correlation Coefficients

In the experiment, we used the correlation electromagnetic analysis and the Hamming distance model to identify the secret key from the leakage traces. The correlation coefficient was calculated from the realigned EM traces and the Hamming distance for each S-Box in accordance with (2). Because we acquired the EM traces at the next point of S-Box passing of the first round, we could make use of a byte-based analysis. The byte-based analysis is only performed on each of the 8-bit S-Boxes. Therefore, the key search space is only $4,096 (= 2^8 \times 16)$ in the case of the AES-128 algorithm with 16 S-Boxes in total.

D. Result Checking

After calculating correlation coefficients, we applied a set of correlation coefficients to the key-decision metric described in Algorithm 2.

Fig. 7 shows HMR variation for the second subkey when the number of EM traces varies from 100 to 1000. The more traces are used, the better HMR is obtained overall. In addition, the HMR increases somewhat as the more neighboring points are used. Therefore, it can be ascertained that the discovered key is correct if the HMR increases in proportion to the number of traces and has a sufficient value, i.e., more than 7 in the case of our target sensor node. We selected 7 as the HMR threshold for the experiment as mentioned before. On the whole, the HMR increased analogously to the number of EM traces and the threshold of 7 showed satisfactory results.

E. Discussion

We use the HMR as a key-decision metric, while Le *et al*. use the signal-to-noise ratio (SNR) of the differential power analysis (DPA) curve corresponding to the correct key. In other words, the DPA peak is defined as the signal and the other parts are considered as noise [18]. The generalized SNR is defined as follows.

$$\mathrm{SNR} = \frac{\text{height of the detection peak}}{\text{standard deviation of noise}}. \tag{4}$$

The SNR evaluation of the CEMA curve for our target sensor node is depicted in Fig. 8, which varies according to the number of EM traces. It shows a similar pattern to the HMR evaluation. According to Figs. 7 and 8, we can know that the correct second subkey is able to be detected by using minimum 400 EM traces at more than the neighboring point 3. These observations for the second subkey are compatible with the experimental result shown in Table 2.

Table 2 provides the required minimum number of traces to find the correct keys. It compares the proposed methods with those of the previous works. We used 100 as the step size of the number of EM traces. Although the forced alignment method and the frequency-based differential analysis are good solutions to overcome the temporal misalignment, they failed to detect the AES-128 secret key even after 5,000 EM traces. However, the efficiency and the reliability of the key detection are enhanced when the proposed method is adopted with some neighboring

Table 2. Required number of EM traces for successful key detection.

S-Box	Forced Align [22]	DFA [19]	Proposed $(a=0)^a$	Proposed $(a=1)^a$	Proposed $(a=2)^a$	Proposed $(a=3)^a$	Proposed $(a=4)^a$	Proposed $(a=5)^a$	Proposed $(a=6)^a$	Proposed $(a=7)^a$
1	Fail	1300	1700	1600	800	600	500	500	500	500
2	Fail	Fail	2700	1100	800	400	400	400	400	400
3	Fail	1100	4000	3900	1000	500	500	500	500	500
4	Fail	700	2100	1400	800	500	300	200	200	200
5	Fail	1900	Fail	Fail	1100	700	300	300	300	300
6	Fail	Fail	700	900	700	300	200	200	200	200
7	Fail	1300	600	400	400	400	400	400	400	400
8	Fail	1100	2200	1800	700	300	300	200	200	200
9	Fail	1500	3700	500	400	300	300	300	300	300
10	Fail	1200	1900	2700	500	300	300	300	300	300
11	Fail	Fail	4300	1200	700	300	200	200	200	200
12	Fail	1100	2100	1500	800	300	200	100	100	100
13	Fail	300	3800	1800	600	300	300	200	200	200
14	Fail	2700	2200	2200	700	400	300	300	300	300
15	Fail	Fail	1900	1400	700	300	200	200	100	100
16	Fail	3800	2900	1700	900	600	500	400	400	400

[a] (a=0), (a=1), (a=2), (a=3), (a=4), (a=5), (a=6), and (a=7) of the proposed method mean 1, 3, 5, 7, 9, 11, 13, and 15 point(s) per 24 sampling points, respectively.

points. Furthermore, we confirmed that all the keys could be successfully detected with fewer than 500 EM traces in the case of neighboring point of 4 and upward.

In terms of the tradeoff between the proposed method and the general CEMA attack, the proposed method needs processing time for selecting peaks and neighbors and calculating key-decision metric. But, it takes a shorter time to execute the proposed method than the general CEMA attack because the proposed method uses fewer sampling points for calculating correlation coefficients. For example, if the neighboring point of 4 is selected, the time to calculate correlation coefficients can be reduced up to 37.5% because only 9 points every 24 sampling points are used for the calculation. The proposed method shows very good results in case that the distinguished information exists in the peak signal. We can consider some mitigation approaches. Some approaches, such as the insertion of timing variations in processing and the use of random clock jittering, can be countermeasures against our method because they scatter the distinguished information and increase noises. That is, the proposed method is efficient and reliable in case of peaks and neighbors related to cryptographic operations, on the other hand, it does not work well in case that peaks and neighbors have little information related to cryptographic operations.

V. CONCLUSION

We presented conclusive electromagnetic analysis results on wireless sensor nodes. We proposed an efficient peak selection algorithm to eliminate the effect of temporal misalignment of EM traces of a wireless sensor node as well as a key-decision metric to improve the reliability of key-decision. The proposed method makes it possible to detect a correct key even when temporal misalignment of the measured traces is very serious.

In order to evaluate the performance of the suggested method and key-decision metric, we prepared an experiment environment for an electromagnetic analysis attack and attacked a *Telos* mote in which AES-128 encryption is performed. The experimental results showed that the entire 128-bit secret key was successfully detected with fewer than 500 EM traces in the case of neighboring point of 4 and upward. As a result, it was confirmed that the proposed method can be efficiently and reliably used for a correlation analysis attack without any tradeoffs. In further research, we will attempt to apply the proposed techniques to various cryptographic devices such as a wireless LAN access point and a PDA. In addition, we will study some suitable mitigation approaches for the proposed method and apply our technique to the studied approaches.

ACKNOWLEDGMENT

We gratefully acknowledge Prof. Howon Kim for his helpful comments on the EM analysis. Special thanks also go to Mr. Yong-Je Choi for his assistance with this work.

REFERENCES

[1] P. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," in *Proc. Advances in Cryptology*, CA, 1999, pp. 388–397.

[2] K. Gandolfi, C. Mourtel, and F. Oliver, "Electromagnetic analysis: Concrete results," in *Proc. Cryptographic Hardware and Embedded Syst.*, Paris, France, 2001, pp. 251–261.

[3] P. Kocher, J. Jaffe, and B. Jun, "Introduction to differential power analysis and related attacks," Cryptography Research, San Francisco, CA, White Paper, 1998.

[4] T. Messerges, E. Dabbish, and R. Sloan, "Examining smart-card security under the threat of power analysis attacks," *IEEE Trans. Comput.*, vol. 51, no. 5, pp. 541–552, May 2002.

[5] E. Brier, C. Clavier, and F. Oliver, "Correlation power analysis with a leakage model," in *Proc. Cryptographic Hardware and Embedded Syst.*, Cambridge, MA, 2004, pp. 16–29.

[6] J. Quisquater and D. Samyde, "Electromagnetic analysis (EMA): Measures and countermeasures for smart cards," in *Proc. Research in Smart Cards*, Sophia Antipolis, Greece, 2001, pp. 200–210.

[7] E. De Mulder, P. Buysschaert, S. B. Ors, P. Delmotte, B. Preneel, G. Vandenbosch, and I. Verbauwhede, "Electromagnetic analysis attack on an

FPGA implementation of an elliptic curve cryptosystem," in *Proc. EUROCON 2005*, 2005, pp. 1879–1882.

[8] K. Schramm, G. Leander, P. Felke, and C. Paar, "A collision-attack on AES combining side channel- and differential-attack," in *Proc. Cryptographic Hardware and Embedded Syst.*, Cambridge, MA, 2004, pp. 163–175.

[9] S. Chari, C. Jutla, J. R. Rao, and P. Rohatgi, "A cautionary note regarding evaluation of AES candidates on smart cards," in *Proc. the Second Advanced Encryption Standard (AES) Candidate Conf.*, 1999.

[10] T. Kim, D.-G Han, K. Okeya, and J. Lim, "Differential power analysis on countermeasures using binary signed digit representations," *ETRI J.*, vol. 29, no. 5, pp. 619–632, Oct. 2007.

[11] J. Kim, S. Hong, D.-G Han, and S. Lee, "Improved side-channel attack on DES with the first four rounds masked," *ETRI J.*, vol. 31, no. 5, pp. 625–627, Oct. 2009.

[12] C. Kim, M. Schlaffer, and S. Moon, "Differential side channel analysis attacks on FPGA implementations of ARIA," *ETRI J.*, vol. 30, no. 2, pp. 315–325, Apr. 2008.

[13] S. Mangard, E. Oswald, and T. Popp, *Power Analysis Attacks: Revealing the Secrets of Smart Cards*, Springer, ISBN-13:978-0-387-30857-9, 2007.

[14] Y. Oren and A. Shamir, "Remote password extraction from RFID tags," *IEEE Trans. Comput.*, vol. 56, no. 9, pp. 1292–1296, Sept. 2007.

[15] M. Hutter, S. Mangard, and M. Feldhofer, "Power and EM attacks on passive 13.56 MHz RFID devices," in *Proc. Cryptographic Hardware and Embedded Syst.*, Vienna, Austria, 2007, pp. 320–333.

[16] C. Gebotys, S. Ho, and C. Tiu, "EM analysis of Rijindael and ECC on a wireless Java-based PDA," in *Proc. Cryptographic Hardware and Embedded Syst.*, Edinburgh, U.K., 2005, pp. 250–264.

[17] T.-H. Le, J. Clediere, C. Serviere, and J.-L. Lacoume, "Efficient solution for misalignment of signal in side channel analysis," in *Proc. Int. Conf. on Acoustics, Speech, and Signal Proess.*, 2007, pp. II-257-II-260.

[18] T.-H. Le, J. Clediere, C. Serviere, and J.-L. Lacoume, "Noise reduction in side channel attack using fourth-order cumulant," *IEEE Trans. Inf. Forens. Security*, vol. 2, no. 4, pp. 710–720, Dec. 2007.

[19] C. C. Tiu, "A New frequency-based side channel attack for embedded systems," M.Eng. thesis, Dept. Elect. Comput. Eng., Univ. Waterloo, Waterloo, ON, Canada, 2005.

[20] C. Clavier, J. Coron, and N. Dabbous, "Differential power analysis in the presense of hardware countermeasures," in *Proc. Cryptographic Hardware and Embedded Syst.*, Worcester, MA, 2000, pp. 252–263.

[21] Y.-S. Lee, Y. Choi, D.-G. Han, H. Kim, and H.-N. Kim, "A novel key-search method for side channel attacks based on pattern recognition," in *Proc. Int. Conference on Acoustics, Speech, and Signal Proess.*, 2008, pp. 1773–1776.

[22] R. Junee, "Power Analysis Attacks: A Weakness in Cryptographic Smart Cards and Microprocessors," B.E. thesis, Dept. Comput. Eng., Univ. Sydney, Sydney, Australia, 2002.

[23] N. Hanley, R. McEvoy, M. Tunstall, C. Whelan, C. Murphy and W. Marnane, "Correlation power analysis of large word sizes," in *Proc. IET Signals and System Conference*, Derry, Ireland, 2007, pp.145–150.

[24] Langer EMV-Technik GmbH, *Near Field Probe Set LF1*, Available: http://www.langer-emv.de/index_en.htm.

[25] M. Mitchell, "Implementing a real-time clock on the MSP 430", Texas Instruments, Application Report SLAA076A, 2001.

You Sung Kang received his B.S. and M.S of Engineering degree in Electronics Engineering from the College of Engineering, Chonnam National University, Gwangju, Korea in 1997 and in 1999, respectively. He is now pursuing his Ph.D. in Electrical and Electronic Engineering from Korea Advanced Institute of Science and Technology (KAIST). In November 1999 he joined Electronics and Telecommunications Research Institute (ETRI), and he is now a senior member of engineering staff. Since 2004, he has been the IT international standard expert of Telecommunications Technology Association (TTA). He is a member of the IEEE and the Korea Institute of Information Security & Cryptology (KISC) and now on the editorial staff of Journal of KISC. He is an editor of the ISO/IEC 29176 and a co-editor of the ISO/IEC 29167. His research interests include the areas of RFID/USN security, wireless LAN security, cryptographic protocol and side channel analysis.

Doo Ho Choi received his B.S. degree in Mathematics from Sungkyunkwan University, Seoul, Korea in 1994, and the M.S. and Ph.D. degrees in Mathematics from Korea Advanced Institute of Science and Technology (KAIST), Daejeon, Korea in 1996 and 2002, respectively. He is currently a Senior Researcher in Electronics and Telecommunications Research Institute (ETRI), Daejeon, Korea from Jan. 2002. His current research interests are side channel analysis and its resistant crypto design, security technologies of RFID and wireless sensor network, lightweight cryptographic protocol/module design, and cryptography based on non-commutativity. He was an editor of the ITU-T Rec. X.1171.

Byung Ho Chung received the B.S. degree from Chonnam National University in 1988 and the M.S. and Ph.D. degrees in Computer Science from Chungnam National University in 2000 and 2005, respectively. He joined Agency for Defense Development (ADD), Korea, as a research engineer in 1988. After about twelve years in 2000, he moved into Electronics and Telecommunications Research Institute (ETRI), at which he is currently working as a principle researcher. His current research concerns are all aspects of modeling & analysis, protocol design, and implementation of information security specially relating to wireless Internet, multimedia contents, and software based tamper-resistant systems.

Hyun Sook Cho received the B.S. degree in Mathematics from Chonnam National University, Korea, in 1979, and the M.S. and Ph.D. degree in computer science from Chungbuk National University, Korea in 1989 and 2001, respectively. She joined ETRI in 1982 and has worked for the development of information security technologies especially key management mechanism and cryptographic algorithm. She served as director of Information Security Research Division (1999–2001) and worked at University of Science and Technology (UST), Korea, as an adjunct professor (2004–2007). She served also as director of Future Technology Research Group (2007–2008), and currently she is director of Knowledge Information Security and Safety Research Department. Her current research interests include cryptographic algorithm, lightweight security protocol design, network security, digital ID authentication, and their deployment into the real world. She is also serving the role of Board Member in Korea Information and Communication Society (KICS) since 2001 and in Korea Institute of Information Security & Cryptology (KISC) since 1999.

Dong-Guk Han received his B.S. degree in Mathematics from Korea University in 1999, and his M.S. degree in Mathematics from Korea University in 2002, respectively. He received Ph.D. of Engineering in Information Security from Korea University in 2005. He was a Post. Doc. in Future University-Hakodate, Japan. After finishing the doctor course, he had been an exchange student in Dep. of Computer Science and Communication Engineering in Kyushu University in Japan from Apr. 2004 to Mar. 2005. He was a Senior Researcher in Electronics and Telecommunications Research Institute(ETRI), Daejeon, Rep. of Korea. He is currently working as an Assistant Professor with the Department of Mathematics of Kookmin University, Seoul, Rep. of Korea. He is a Member of KIISC, IEEK, and IACR.