Electromagnetic Analysis Attack for a lightweight cipher PRINCE

Masaya Yoshikawa and Yusuke Nozaki
Dept. of Information Engineering
Meijo University
Nagoya, Japan

***Abstract*— Ensuring the security of built-in apparatuses has become an important task because of advancements in Internet of Things (IoT) technology. Therefore, lightweight ciphers that are available in built-in apparatuses have attracted the attention of many researchers. However, the danger of electromagnetic analysis attacks against cryptographic circuits has been pointed out. Electromagnetic analysis attacks illegally analyze confidential information using the electromagnetic waves that are generated during the operation of a cryptographic circuit. Many studies have reported on power analysis attacks against the advanced encryption standard (AES). However, as far as we know, no study has reported on electromagnetic analysis attacks against PRINCE, which is one of the most popular lightweight ciphers. The present study proposes a method for electromagnetic analysis attacks against PRINCE in order to evaluate the tamper resistance of PRINCE. The present study also verifies the validity of the proposed method by performing an evaluation experiment using a field-programmable gate array (FPGA).**

Keywords—Security; Electromagnetic analysis attack; PRINCE; Internet of Things; Lightweight cipher

I. INTRODUCTION

The security of built-in apparatuses, such as automobile-mounted sensors and the in-vehicle equipment that is used in in-vehicle systems, has become more important than ever due to the development of the Internet of Things (IoT). In built-in apparatuses, the circuit scale, power consumption, and processing time are strictly restricted. Therefore, the current literature includes studies on lightweight ciphers[1]–[3] that are available under strict conditions. The safety of lightweight ciphers, including PRINCE[1], is computationally secured.

However, attacks of illegally analyzing confidential information against a cipher, the safety of which is computationally secured, have been reported[4]–[10]. These attacks include side-channel attacks[4]–[10], which illegally analyze secret keys using physical information, such as power consumption and the electromagnetic waves that are generated during the operation of a cryptographic circuit. In particular, electromagnetic analysis attacks[6]–[10] using electromagnetic waves are considered to be extremely dangerous.

Several studies on electromagnetic analysis attacks against the AES[11] have been reported. However, as far as we know, no study has reported on electromagnetic analysis attacks against lightweight ciphers. To secure the safety of lightweight ciphers in the future, it is extremely important to examine electromagnetic analysis attacks against lightweight ciphers.

The present study proposes a method for conducting electromagnetic analysis attacks against PRINCE, a lightweight cipher and an encryption standard. The present study also verifies the validity of the proposed method by performing an evaluation experiment using a field-programmable gate array (FPGA).

II. PRELIMINARIES

A. PRINCE

PRINCE[1] is a lightweight cipher proposed by J. Borghoff et.al. in 2012. The block size of PRINCE is 64 bits, and its key size is 128 bits. The 128-bits secret key is divided into two 64-bits partial keys. Fig.1 shows the outline of PRINCE. As shown in Fig.1, encryption processing consists of addition of constant value, round function R, middle processing, and inverse round function R^{-1}. These processing are repeated 12 times.

Addition of constant value performs exclusive-OR using partial key and round constant value RC. As shown in Fig.2, in round function R, S processing, M' processing, SR processing, and addition of constant value are repeated. Middle processing consists of S processing, M' processing, and S^{-1} processing. As shown in Fig.3, in inverse round function R^{-1}, addition of constant value, SR^{-1} processing, M' processing, and S^{-1} processing are repeated.

S and S^{-1} processing perform nonlinear processing using S-BOX table in Table I. M' processing multiples with 64 × 64 matrix M' defined in Formula (1). In Formula (1), M' consists of $\hat{M}^{(0)}$ and $\hat{M}^{(1)}$.

$$M' = \begin{pmatrix} \hat{M}^{(0)} & 0 & 0 & 0 \\ 0 & \hat{M}^{(1)} & 0 & 0 \\ 0 & 0 & \hat{M}^{(1)} & 0 \\ 0 & 0 & 0 & \hat{M}^{(0)} \end{pmatrix} \quad (1)$$

978-1-5090-6096-2/16/$31.00 ©2016 IEEE

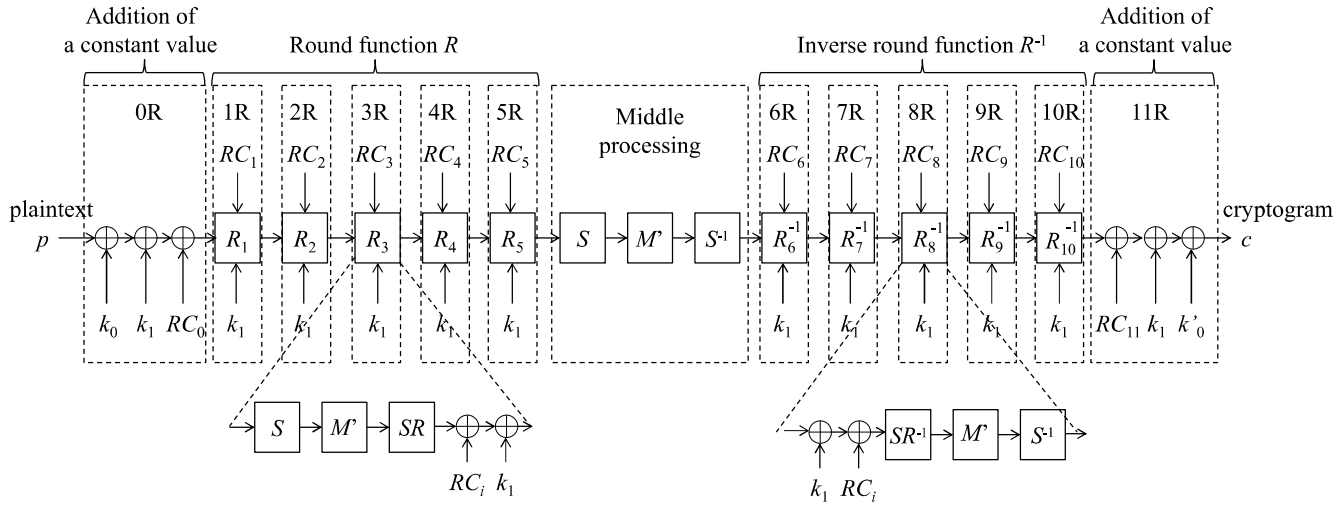

Fig. 1. The outline of PRINCE

TABLE I. S-BOX

x	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
$S(x)$	B	F	3	2	A	C	9	1	6	7	8	0	E	5	D	4
$S^{-1}(x)$	B	7	2	3	F	D	8	9	A	6	4	0	5	E	C	1

$\hat{M}^{(0)}$ and $\hat{M}^{(1)}$ are defined in Formulae (2)(3).

$$\hat{M}^{(0)} = \begin{pmatrix} M_0 & M_1 & M_2 & M_3 \\ M_1 & M_2 & M_3 & M_0 \\ M_2 & M_3 & M_0 & M_1 \\ M_3 & M_0 & M_1 & M_2 \end{pmatrix} \tag{2}$$

$$\hat{M}^{(1)} = \begin{pmatrix} M_1 & M_2 & M_3 & M_0 \\ M_2 & M_3 & M_0 & M_1 \\ M_3 & M_0 & M_1 & M_2 \\ M_0 & M_1 & M_2 & M_3 \end{pmatrix} \tag{3}$$

$\hat{M}^{(0)}$ and $\hat{M}^{(1)}$ are involution defined in Formula (4).

$$\begin{cases} \hat{M}^{(0)} = \left(\hat{M}^{(0)}\right)^{-1} \\ \hat{M}^{(1)} = \left(\hat{M}^{(1)}\right)^{-1} \end{cases} \tag{4}$$

$\hat{M}^{(0)}$ and $\hat{M}^{(1)}$ multiply with 4 × 4 matrix M_0, M_1, M_2, and M_3 defined in Formulae (5)–(8).

$$M_0 = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \tag{5}$$

$$M_1 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \tag{6}$$

$$M_2 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \tag{7}$$

$$M_3 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \tag{8}$$

SR and SR^{-1} processing perform left shift processing and right shift processing, as shown in Fig.4 and Fig.5. In these shift processing, 64-bit intermediate value are divided into 16 4-bit data. Then, 16 4-bit data are represented 4 × 4 matrix.

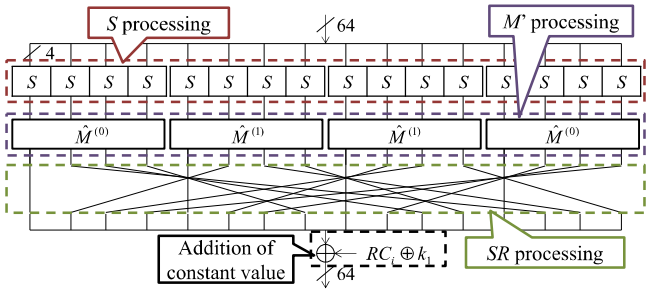

Fig. 2. Round function *R*

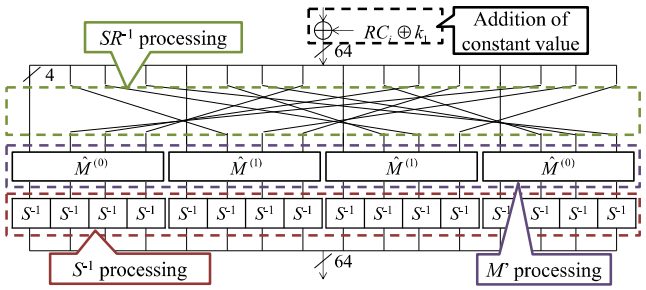

Fig. 3. Inverse round function R^{-1}

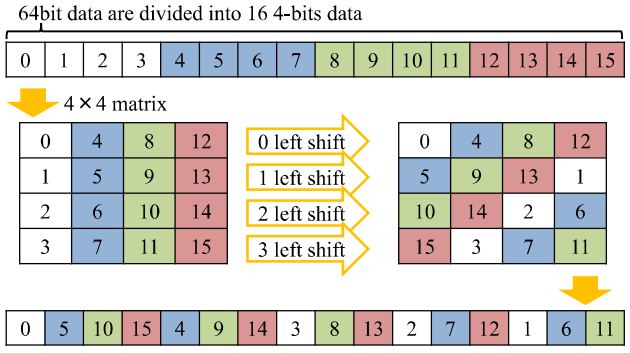

Fig. 4. *SR* processing

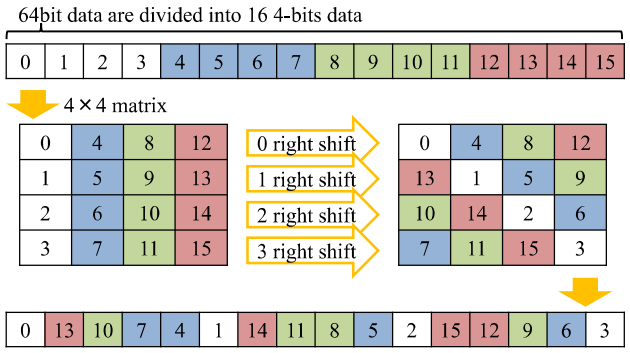

Fig. 5. SR^{-1} processing

B. *Electromagnetic Analysis Attack*

Electromagnetic analysis attacks obtain waveforms using a magnetic field or electric field probe, and use the obtained waveforms for attacks.

In an actual analytical method in electromagnetic analysis attacks, the electromagnetic fields at two points near LSI, such as a place just above the LSI chip and a power-supply pattern were measured. Since a measurement method of approaching a small loop antenna to the LSI chip for probing reflects the effects due to the difference in cell location, this method can directly measure the conditions inside LSI. In other words, the menace of electromagnetic analysis attacks may be more serious than that of power analysis attacks from the viewpoint of tamper resistance.

C. *Related Work*

Papers [4][5] are the most popular power analysis attacks. A principle of almost all side-channel attacks is based on papers [4] and [5] .Although the number of studies on electromagnetic analysis attacks is smaller than that on power analysis attacks, several studies have been performed [8]–[10]. Paper [8] embedded countermeasure dual-rail circuits in field-programmable gate array (FPGA), and conducted attacks while noticing the gap between two embedded circuits, which performed a complementary operation. Paper [9] also reported experimental results regarding the locality of layout in detail. Paper [10] reported the differences in attack results when the direction of a magnetic field probe was changed.

III. Proposed Analysis

The proposed analysis method analyzes secret keys using the waveform data obtained by observing the radiated electromagnetic wave during the operation of a cryptographic circuit. Fig. 6 shows the outline of the proposed analysis method. The proposed analysis method assumes that a linear relationship exists between the intra-data resister Hamming distance (HD) and the electromagnetic wave. As shown in Fig.6, the HD is calculated using an already known cryptogram and the predicted value of a key.

Then, the Pearson's correlation coefficient ρ between the calculated HD h and the electromagnetic wave w, is obtained using Formula (9). In this formula, $w_{i,t}$ represents the electromagnetic wave, h_i represents the HD, $\overline{w_t}$ represents the mean value of the electromagnetic wave $w_{i,t}$, $\overline{h}$ represents the mean value of the HD h_i, and D represents the number of waveform data sets used for the analysis.

$$\rho = \frac{\sum_{i=1}^{D}\left(w_{i,t}-\overline{w_t}\right)\left(h_i-\overline{h}\right)}{\sqrt{\sum_{i=1}^{D}\left(w_{i,t}-\overline{w_t}\right)^2\sum_{i=1}^{D}\left(h_i-\overline{h}\right)^2}} \qquad (9)$$

In the proposed analysis method, the predicted value of a key with the maximum value of the Pearson's correlation coefficient, ρ, is presumed to be the correct key.

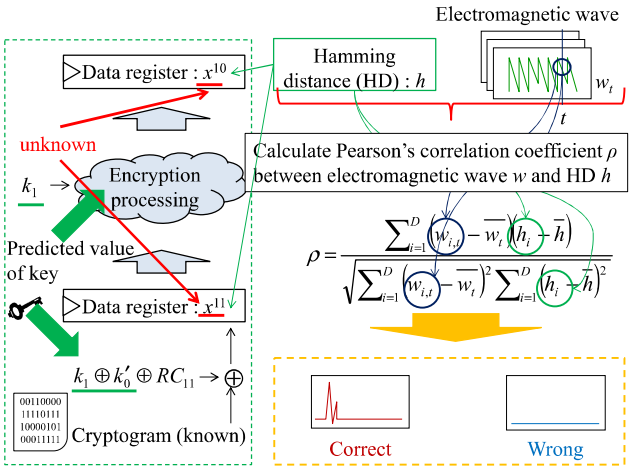

Fig. 6. Outline of the proposed analysis method

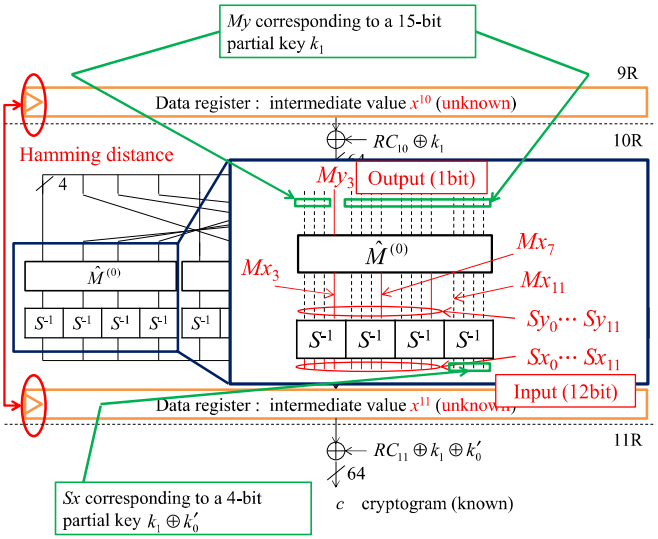

Fig. 7. Deriving method of HD

Next, the detail of deriving of HD are explained. As shown in Fig.6, the proposed method utilizes HD between intermediate value x^{10} of 9th round and intermediate value x^{11} of 10th round. This HD is derived one by one. Since x^{10} and x^{11} are unknown, the proposed analysis method estimates these values using Formulae (10) and (11). In Formula (10), intermediate value x^{11} can be calculated using a known cryptogram c, the predicted value of partial key $k_1 \oplus k'$, and the round constant value RC_{11}.

$$x^{11} = c \oplus RC_{11} \oplus k_1 \oplus k_0' \qquad (10)$$

Then, the proposed analysis method performs a reverse calculation of inverse round function R_{10}^{-1} processing using both x^{11} and the predicted value of partial key k_1 to calculate the intermediate value x^{10}. In other words, that can calculate x^{11} using an only inverse round function R. Here, addition of constant value uses the round constant value RC_{10}. This calculation is represented using Formula(11). In Formula(11), $S(\ )$ represents S processing, $M'(\ )$ represents M' processing, and $SR(\ )$ represents SR processing.

$$x^{10} = SR\left(M'\left(S\left(x^{11}\right)\right)\right) \oplus RC_{10} \oplus k_1 \qquad (11)$$

Since the proposed analysis method calculates HD one by one, it derives the intermediate value x^{10} one by one, as shown in Fig7. In deriving of x_3^{10} (fourth bit of x^{10}), My_3 (fourth bit of My) is calculated using Formulae (12)(13). Formula (12) are derived by Formulae (2)(5)–(8). In Formula (12), Mx represents input value of $\hat{M}^{(0)}$ processing and My represents output value of $\hat{M}^{(0)}$ processing.

$$My_3 = Mx_3 \oplus Mx_7 \oplus Mx_{11} \qquad (12)$$

$$My_3 = Sy_3 \oplus Sy_7 \oplus Sy_{11} \qquad (13)$$

In Formula (13), Sy represents output value of S processing and Sy equals to Mx. Then, Sy are calculated using S processing. This calculation is expressed as Formula (14). In this formula, Sx represents input value of S processing.

$$\begin{cases} Sy_0 \| Sy_1 \| Sy_2 \| Sy_3 = S(Sx_0 \| Sx_1 \| Sx_2 \| Sx_3) \\ Sy_4 \| Sy_5 \| Sy_6 \| Sy_7 = S(Sx_4 \| Sx_5 \| Sx_6 \| Sx_7) \\ Sy_8 \| Sy_9 \| Sy_{20} \| Sy_{11} = S(Sx_8 \| Sx_9 \| Sx_{10} \| Sx_{11}) \end{cases} \qquad (14)$$

Then, intermediate value x_3^{10} can be obtained using My_3, RC_{10}, and the predicted value of partial key k_1. The proposed analysis method utilizes HD between x_3^{10} and x_3^{11}.

As shown in Fig.7, My_3 can be calculated using a 12-bits input value $Sy_{0,\cdots}$, Sy_{11}. This calculation requires the predicted value of partial key $k_1 \oplus k'$. Moreover, it requires a 1-bit predicted value of partial key k_1 to derive intermediate value x_3^{10}. Therefore, this calculation requires a 13-bits predicted value of partial key to calculate a 1-bit HD.

In example of Fig.7, deriving of secret key K requires a 19-bits partial key (a 4-bits partial key k_1 and a 15-bits partial key $k_1 \oplus k'$). This calculation is as follows :

Step1: Derive a 5-bits partial key related to 4-bits input value and 1-bit output value.

Step2: Derive a remaining of 14-bits partial key.

In Step1, it utilizes the already known 13-bits partial key. Then, 16-bits partial key $k_1 \oplus k'$ can be obtained. In Step2, it utilizes the already known 16-bits partial key $k_1 \oplus k'$, and can

estimate the partial key k_1 one by one. Therefore, the computational complexity is 8,252 ways ($2^{13} + 2^5 + 2^1 \times 14 = 8{,}252$), as shown in Fig.8. Moreover, in deriving of the 128-bits secret key K, 33,008 ways ($8{,}254 \times 4 = 33{,}008$) of calculation are required as well as paper [12] of power analysis for PRINCE. This is less than 2^{128} ways which are computational complexity of brute force.

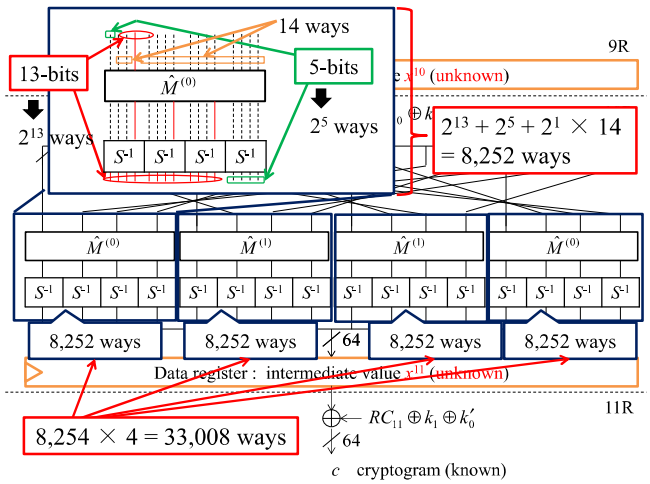

Fig. 8. Computational complexity of the proposed analysis method

IV. Evaluation Experiment

To verify the validity of the proposed method, the present study performed an evaluation experiment using a FPGA.

A. Experimental Environment

In the experiment, PRINCE was embedded into a FPGA, and FPGA Spartan-6 on the side-channel attack standard evaluation board (SASEBO)-W[13] was used. PRINCE is implemented with a round based architecture as well as the paper [1], as shown in Fig.9. To measure the radiated electromagnetic wave, a shielded loop antenna was used. Table II and Fig.10 show the experimental environment.

TABLE II. Experimental Environment

Encryption algorithm	PRINCE
Block size	64 bit
Key size	128 bit
Evaluation board	SASEBO-W
FPGA	Spartan-6 XC6SLX150
Implementation tool	Xilinx ISE Design Suite 14.7
Magnetic field probe	Shielded loop antenna
Oscilloscope	Agilent DSO-X 3104A
Sampling rate	5 Gsa/sec
Power supply	USB supply from PC
Number of waveforms	20,000
Plaintext	Random

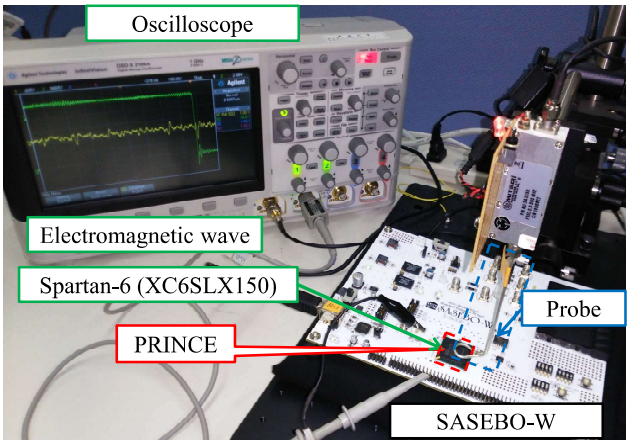

Fig. 10. Experiment environment

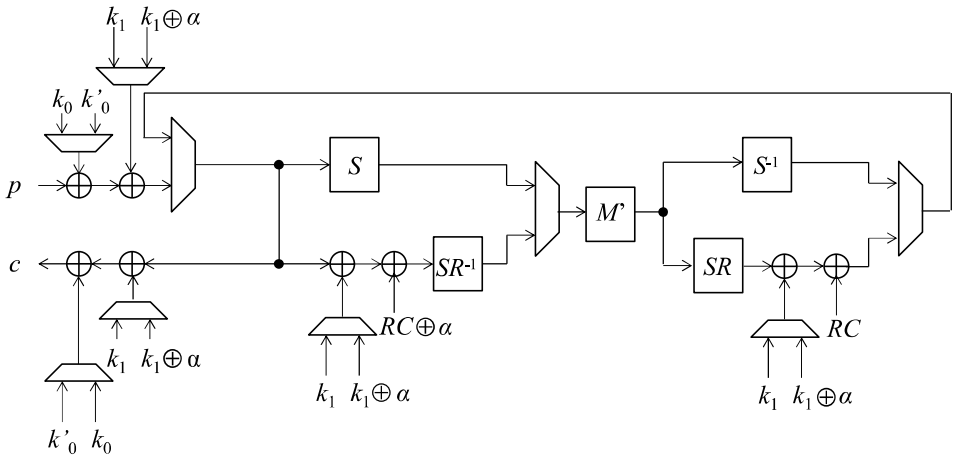

Fig. 9. Implementation architecture of PRINCE[1]

B. *Experimental Results*

In the evaluation experiment, the analysis was performed for PRINCE using the proposed analysis method against 11th round to estimate partial key $k_1 \oplus k'$. Fig.11 shows the analytical results.

In the analysis, a round key at one round was derived. Since the round key consisted of 64 bits, the total number of the correct keys was 64 bits.

As shown in Fig.11, all the round keys could be analyzed using 6,000 waveforms. Thus, the proposed method successfully analyzed the round keys of PRINCE, a typical lightweight cipher. Therefore, PRINCE was found to be vulnerable to electromagnetic analysis attacks.

Next, experiments compared the correlation coefficient with a correct key and wrong keys. Fig.12 shows the comparison results. The vertical axis shows the correlation coefficient and the horizontal axis shows processing time. As shown in Fig.12, the peak appears in 11th round in the correlation coefficient with a correct key. By contrast, in wrong keys, the peak does not appear.

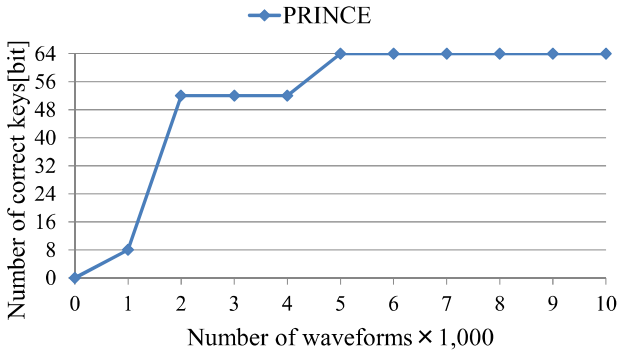

Fig. 11. Experimental result

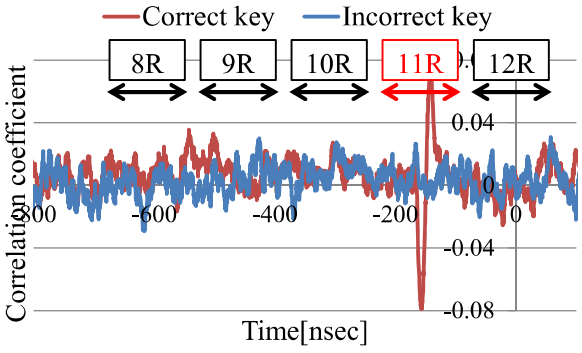

Fig. 12. Comparison result of correlation coefficient

V. Conclusion

To secure the safety of a device to which a lightweight cipher is applied, measures against electromagnetic analysis attacks must be developed. To examine the measures taken to prevent electromagnetic analysis attacks, it is important to first evaluate and verify the vulnerability of a lightweight cipher against those types of attacks. The present study proposed a method for electromagnetic analysis attacks against PRINCE. The present study also verified the validity of the proposed method by performing an evaluation experiment using a FPGA. The future works include to examine measures to prevent the proposed electromagnetic analysis attack.

References

[1] J. Borghoff, A. Canteaut, T. Güneysu, E.B. Kavum, M. Knežević, L.R. Knudsen, G. Leander, V. Nikov, C. Paar, C. Rechberger, P. Rombouts, S.S. Thomsen, and T. Yalçin, "PRINCE — A Low-latency Block Cipher for Pervasive Computing Applications," Proc. of ASIACRYPT 2012, LNCS 7658, pp.208–225 , Dec. 2012.

[2] A. Bogdanav, L.R. Knudsen, G. Leander, C. Paar, A. Poschmann, M.J.B. Robshaw, Y. Seurin, and C. Vikkelsoe, "PRESENT: An Ultra-Lightweight Block Cipher," Proc. of 9th Int. Workshop on Cryptographic Hardware and Embedded Systems (CHES 2007), LNCS 4727, pp.450–466, Springer-Verlag, Sept. 2007.

[3] T. Suzaki, K. Minematsu, S. Morioka and E. Kobayashi, "TWINE: A Lightweight, Versatile Blockcipher," Proc. of ECRYPT Workshop on Lightweight Cryptography (LC11), pp.146–149, Nov. 2011.

[4] P. Kocher, J. Jaffe, and B. Jun, "Differential Power Analysis," Proc. of CRYPTO'99, LNCS 1666, pp.388–397, Springer-Verlag, Dec. 1999.

[5] E. Brier, C. Clavier, and F. Olivier, "Correlation Power Analysis with a Leakage Model," Proc. of 6th Int. Workshop on Cryptographic Hardware and Embedded Systems (CHES 2004), LNCS 3156, pp.16–29, Springer-Verlag, Aug. 2004.

[6] K. Gandolfi, C. Mourtel, and F. Olivier, "Electromagnetic Analysis: Concrete Results," Proc. of 3rd Int. Workshop on Cryptographic Hardware and Embedded Systems (CHES 2001), LNCS 2162, pp.251–261, Springer-Verlag, May 2001.

[7] O. Meynard, S. Guilley, J.-L. Danger, and L. Sauvage, "Far Correlation-based EMA with a Precharacterized Leakage Model," Proc. of Design, Automation and Test in Europe Conference and Exhibition (DATE 2010), pp.977–980, March 2010.

[8] T.Syouji, Y.Tsunoo, and Y.Itakura, "Local Electromagnetic Analysis against FPGA," Proc. of Symposium on Cryptography and Information Security (SCIS 2010), 3B3-2, pp.1–6, Jan. 2010. (in Japanese)

[9] H.Morita, T.Matsumoto, Y.Takahashi, and J.Shikata, "Electro Magnetic Analysis and Local Information of Cryptographic Hardware -Part 3-," Proc. of Symposium on Cryptography and Information Security, 2D3-2, pp.1–7, Jan. 2011. (in Japanese)

[10] T.Ochiai, D. Yamamoto, K. Itoh, M. Takenaka, N. Torii, D. Uchida, T. Nagai, S. Wakana, M. Iwamoto, K. Ohta, and K. Sakiyama, "Locality of Electromagnetic Analysis and Anisotropy of Magnetic Emanation," Proc. of Symposium on Cryptography and Information Security (SCIS 2011), 2D3-3, pp.1–8, Jan. 2011. (in Japanese)

[11] Federal Information Processing Standards (FIPS) Publication 197 "Advanced Encryption Standard (AES)," U. S. Department of Commerce/National Institute of Standard and Technology (NIST) , 2001.

[12] R. Selvam, D. Shanmugam, and S. Annadurai. "Side Channel Attacks: Vulnerability Analysis of PRINCE and RECTANGLE using DPA," Cryptology ePrint Archive: Report 2014/644, Aug. 2014.

[13] Research Center for Information Security, "Evaluation Environment for Side-channel Attacks," National Institute of Advanced Industrial Science and Technology, http://www.risec.aist.go.jp/project/sasebo/