World Academy of Science, Engineering and Technology
International Journal of Mathematical and Computational Sciences
Vol:9, No:9, 2015

Round Addition Differential Fault Analysis on Lightweight Block Ciphers with On-the-Fly Key Scheduling

Hideki Yoshikawa, Masahiro Kaminaga, Arimitsu Shikoda, Toshinori Suzuki

***Abstract*—**Round addition differential fault analysis using operation skipping for lightweight block ciphers with on-the-fly key scheduling is presented. For 64-bit KLEIN, it is shown that only a pair of correct and faulty ciphertexts can be used to derive the secret master key. For PRESENT, one correct ciphertext and two faulty ciphertexts are required to reconstruct the secret key. Furthermore, secret key extraction is demonstrated for the LBlock Feistel-type lightweight block cipher.

***Keywords*—**Differential Fault Analysis (DFA), round addition, block cipher, on-the-fly key schedule.

I. Introduction

DIFFERENTIAL FAULT ANALYSIS (DFA) using operation skipping is an effective technique for attacking cipher-implemented microcontrollers [1]-[3]. Round addition DFA can be achieved by skipping an increment or decrement command. We have previously demonstrated that round addition DFA can be used to derive secret keys for some ciphers that employ Feistel or substitution-permutation network (SPN) block ciphers [4]-[6].

In recent years, several lightweight block ciphers have been proposed for low-resource devices, such as sensor networks, smartcards, and radio-frequency identification systems. These block ciphers are suitable for hardware environments and are expected to be used in software platforms, such as the software in 8-bit microcontrollers [7]-[9], [13], [15]. Thus, to maintain hardware security, their vulnerability to DFA using operation skipping must be evaluated. In recent years, several reports have presented methods for attacking several cipher-implemented hardware [10]-[12], [14]. However, these methods require a number of fault injections to obtain many faulty ciphertexts. Our attack method uses a power supply with an abnormal voltage glitch or a clock signal with a clock glitch to targeted ICs without de-packaging and microscopic operations [10], [11]; thus, this technique costs less than other methods.

In this study, a secret-key-extraction method for lightweight block ciphers with an on-the-fly key schedule is presented. The method is essentially identical to that used for block ciphers with either Feistel or SPN structures [5], [6]; however, those methods do not assume an on-the-fly key schedule. This means that both the original and added rounds use identical round keys. Here, we have shown that a secret key can be reconstructed using only a pair of correct and faulty ciphertexts to derive the secret master key for 64-bit KLEIN. For PRESENT, it is shown that one correct ciphertext and two faulty ciphertexts are required to reconstruct the secret key. These results indicate that our attack method is effective for a block cipher with an 'add round key' operation. Furthermore, the secret key extraction is demonstrated for the LBlock Feistel-type lightweight block cipher [13].

Hideki Yoshikawa, Masahiro Kaminaga, Arimitsu Shikoda, and Toshinori Suzuki are with the Faculty of Engineering, Tohoku Gakuin University, Tagajo, Miyagi 985-8537, Japan (e-mail: hyoshi@ mail.tohoku-gakuin.ac.jp).

II. Round Addition DFA Model for Block Cipher with On-the-Fly Key Schedule

Fig. 1 shows the pseudocode of a round addition DFA attack for a block cipher with an on-the-fly key schedule. In the figure, P is plaintext, C is ciphertext derived from P, X is round data, and RK_i (i = 1,…,r) is the i-th round subkey. Each round comprises an F-function $F(\ ,\ )$ and a swap permutation $SW(\ )$. For a block cipher algorithm with an on-the-fly key schedule, a round key update $UD(\ )$ is also included in the round operation. A faulty ciphertext can be obtained if the increment instruction, denoted i++, is bypassed.

```
X = P; i = 1;
while (i ≤ r) {
   X ← F(X, RK_i);
   X ← SW(X);
   RK_{i+1} ← UD(RK_i);
   i++;                    /* Attack Point * /
}
C ← X;
```

Fig. 1 Pseudocode of a round addition DFA attack for a block cipher with an on-the fly key schedule

III. Key Reconstruction Method Using Round Addition DFA for KLEIN SPN Block Cipher

In this section, we present the key reconstruction method for the KLEIN lightweight SPN block cipher [6] with on-the-fly key scheduling. The key reconstruction method for 64-bit KLEIN is illustrated in Fig. 2. This is a 12-round operation lightweight block cipher [8]. The i-th round keys Ki are generated by a 64-bit master key $\boldsymbol{K}$, which is divided into two byte-oriented tuples as $\boldsymbol{K} = \boldsymbol{A}|\boldsymbol{B} = sk_0 \ldots sk_7$, i.e., $\boldsymbol{A} = sk_0 \ldots sk_3$ and $\boldsymbol{B} = sk_4 \ldots sk_7$, where | denotes concatenation. The initial

round key is $K_0 = \boldsymbol{K}$, and, for i = 1,…, 12, the key update operation is as follows:

- $[sk_0 \cdots sk_7] \leftarrow (B <<< 1) \mid (A <<< 1) \oplus (B <<< 1)$
- $[sk_0 \cdots sk_7] \leftarrow [sk_0 sk_1 (sk_2 \oplus i) sk_3 sk_4 S(sk_5) S(sk_6) sk_7]$
- $K_i \leftarrow A \mid B \leftarrow [sk_0 \cdots sk_7], \quad i \leftarrow i+1$

where <<< means left shift by one byte position and S( ) is S-box substitution. The encryption process of 64-bit KLEIN is shown in Fig. 2. In the figure, C denotes the correct round output. Each encryption operation includes SubNibble, Rotate Nibble, MixNibble, and round key addition. Here, "Update" means the round operation of the key schedule. A faulty ciphertext can be obtained if a final round is added. The generation process is shown in Fig. 3. In the figure, C' denotes faulty round output, including the addition of a final round, and K'_{11} is the new round key for the added round operation. In this case, the final round key K_{12} is the same as K'_{11} obtained from the key updation algorithm. The following relation can be derived from Fig. 3. For 64-bit KLEIN, the 80-bit secret key can be extracted from K'_{12}.

$$\mathrm{Mix}(\mathrm{Rot}(\mathrm{Sub}(C))) \oplus C' = K'_{12} \tag{1}$$

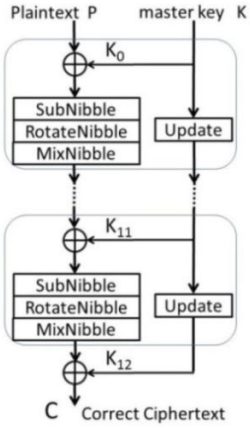

Fig. 2 64-bit KLEIN encryption process

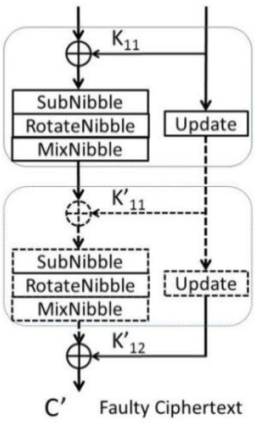

Fig. 3 Faulty ciphertext generation process by final round addition with 64-bit KLEIN

The same approach can be applied to 64-bit LED in a straightforward manner since all round keys are identical [6], [9].

IV. Key Reconstruction Method Using Round Addition DFA for PRESENT

In this section, the key reconstruction method for PRESENT-80 is described. PRESENT-80 is a 31-round SPN lightweight block cipher with a block size of 64 bits and an 80-bit secret key [7]. The round keys Ki are generated by 80-bit master key $\boldsymbol{K} = k_{79} \ldots k_0$, where $K_0 = k_{79} \ldots k_{16}$. For i = 1,…,31, the update operation is as follows:

- $[k_{79} k_{78} \cdots k_1 k_0] = [k_{18} k_{17} \cdots k_{20} k_{19}]$
- $[k_{79} k_{78} k_{77} k_{76}] = S[k_{79} k_{78} k_{77} k_{76}]$
- $[k_{19} k_{18} k_{17} k_{16} k_{15}] = [k_{19} k_{18} k_{17} k_{16} k_{15}] \oplus i$
- $K_i = k_{79} \cdots k_{16}$ is output as the i-th 64-bit round key and $i \leftarrow i+1$

where $S[x]$ is a 4-bit S-box.

Fig. 4 shows the PRESENT encryption process, and Figs. 5 and 6 show faulty encryption processes that include single and double round addition, respectively. Each round of PRESENT includes three stages, i.e., round key addition, a non-linear substitution layer (sBoxLayer), and a bit-wise permutation layer (pLayer). Note that the added round operation is depicted by dashed lines. If the final round is added, the final round key K_{32} is the same as K'_{31}. Thus, the following relation can be derived from Figs. 2 and 3 along with the key scheduling algorithm.

$$\mathrm{pLayer}(\mathrm{sBoxLayer}(C)) \oplus C' = K'_{32} \tag{2}$$

$$\mathrm{pLayer}(\mathrm{sBoxLayer}(C')) \oplus C'' = K''_{32} \tag{3}$$

From (2), the 64-bit secret information in the 80-bit key register in key scheduling can be derived. If the second faulty ciphertext C'' is obtained by a double round attack, all key register secret information can be obtained since K'_{32} is the same as K''_{31}. Thus, the 80-bit secret key can be extracted by an inverse operation of the key scheduling algorithm.

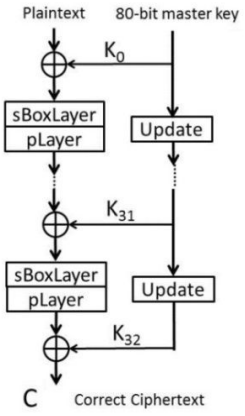

Fig. 4 PRESENT-80 encryption process

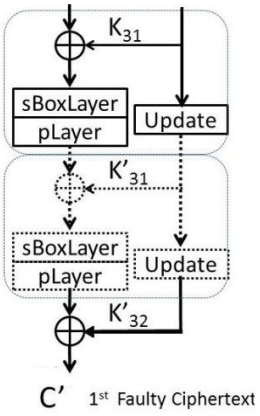

Fig. 5 Single round addition attack on PRESENT-80

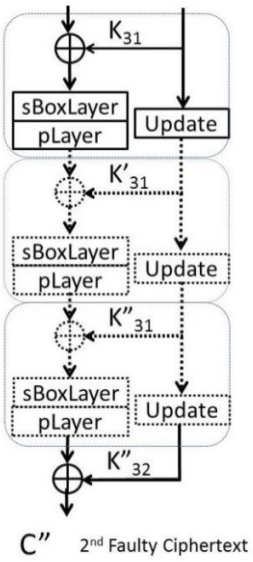

Fig. 6 Double round addition attack on PRESENT-80

V. Secret Key Reconstruction of Feistel Block Cipher LBLOCK with On-the-Fly Key Schedule

In this section, an application for key reconstruction of the LBlock lightweight Feistel block cipher is demonstrated. This cipher algorithm has a 32-round Feistel structure with a 64-bit block size and an 80-bit key size [13]. The encryption procedure is illustrated in Fig. 7. In the figure, a 64-bit ciphertext denoted $C = X_{32}|X_{33}$ is generated by a 64-bit plaintext denoted $P = X_1|X_0$. The output data of the round operation can be expressed as:

$$X_i = F(X_{i-1}, K_{i-1}) \oplus (X_{i-2} <<< 8), \ i = 2,3,\ldots,33 \qquad (4)$$

where $F(\ )$ and K_i denote a round function and the i-th 32-bit round key, respectively, and $(a <<< b)$ indicates that b bits remain in the left cyclic shift operation in binary sequence a.

The round keys K_1, K_2, ..., K_{32} are generated by the 80-bit master secret key $\mathbf{K} = k_{79}\ldots k_0$. For $i = 1, 2,\ldots,31$, the updation operation is given as:

- $\mathbf{K}$ is updated as $\mathbf{K} \leftarrow (\mathrm{K} <<< 29)$.
- $k_{79}\cdots k_0 \leftarrow s_9[k_{79}k_{78}k_{77}k_{76}] \,|\, s_8[k_{75}k_{74}k_{73}k_{72}] \,|\, k_{71}\cdots k_0$
- $k_{79}\cdots k_0 \leftarrow k_{79}\cdots k_{51} \,|\, [(k_{50}k_{49}k_{48}k_{47}k_{46} \oplus i)] \,|\, k_{45}\cdots k_0$
- $\mathbf{K}_i \leftarrow k_{79}\cdots k_{48}$ is output as the (i+1)-th round key and $i \leftarrow i+1$.

where $s_9[\ ]$ and $s_8[\ ]$ are two 4 × 4 S-boxes.

From the above key scheduling algorithm, it is evident that that the 80-bit secret master key $\mathbf{K}$ can be extracted by three consecutive round keys. In addition, the key scheduling algorithm is similar to that of PRESENT.

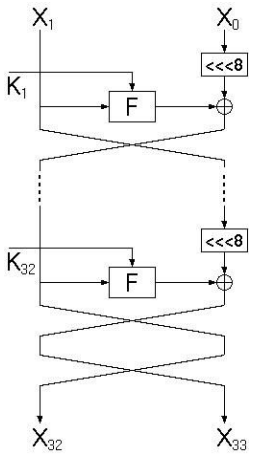

Fig. 7 Encryption procedure of LBlock

For a Feistel block cipher with an on-the-fly key schedule, the attack point is set to the final round, and a double and triple round addition is applied. The double round addition can be applied for the secret key derivation of 128-bit CLEFIA or 128-bit AES [4], [6]. To reconstruct the secret master key, three faulty ciphertexts are required (Figs. 8–10). In this case, half of the correct ciphertext and half of the faulty ciphertext are identical. Thus, the derivation of the round key is easy. Using correct ciphertext $C = X_{32}|X_{33}$ and three faulty ciphertexts $C' = X_{33}|X_{34}$, $C'' = X_{34}|X_{35}$, and $C''' = X_{35}|X_{36}$, the three consecutive round subkeys K'_{32}, K''_{32}, and K'''_{35} are derived as:

$$X_{34} = F(X_{33}, K'_{32}) \oplus (X_{32} <<< 8) \qquad (5)$$

$$X_{35} = F(X_{34}, K''_{32}) \oplus (X_{33} <<< 8) \qquad (6)$$

$$X_{36} = F(X_{35}, K'''_{32}) \oplus (X_{34} <<< 8) \ . \qquad (7)$$

This attack method can be easily applied for another block cipher with the same Feistel structure, e.g., DES, MIBS [15], etc.

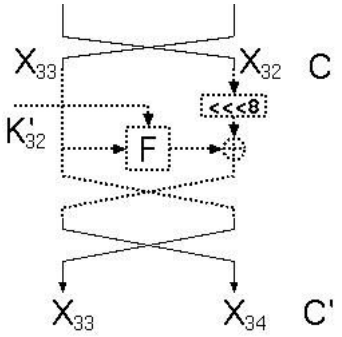

Fig. 8 Generation process with on-the-fly key schedule of a faulty ciphertext by single round addition

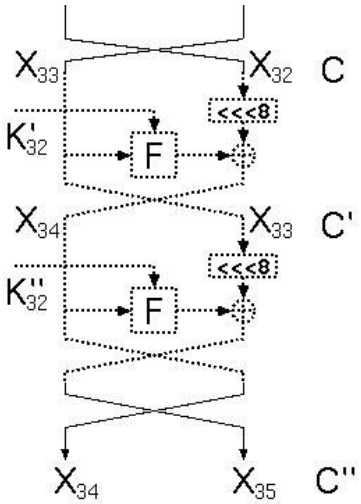

Fig. 9 Generation process with on-the-fly key schedule of a faulty ciphertext by double round addition

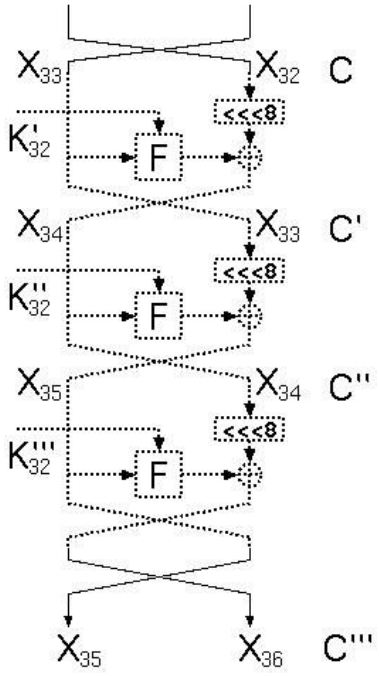

Fig. 10 Generation process with on-the-fly key schedule of a faulty ciphertext by triple round addition

VI. Conclusion

In this study, we have demonstrated round addition DFA as key extraction method for lightweight block ciphers with on-the-fly key scheduling. This attack method is effective for such block ciphers as they include an 'add round key' operation, and a secret cipher key can be extracted from the final round key. Therefore, we must consider countermeasure techniques against round addition DFA for microcontrollers implemented using such lightweight block ciphers. In future, we plan to demonstrate the DFA attack using AES because this block cipher includes the 'add round key' operation and the secret master key can be reconstructed from a final round key, similar to KLEIN.

Acknowledgment

This work was supported by the Japan Society for the Promotion of Science (JSPS), KAKENHI Grant Number 25330157.

References

[1] H. Choukri and M. Tunstall, "Round Reduction Using Faults," *Proc. of FDTC*, pp.13-24, 2005.
[2] J. Park, S. Moon, D. Choi, Y. Kang, and J. Ha, "Differential Fault Analysis for Round-Reduced AES by Fault Injection," *ETRI Journal*, Vol.33, No.3, pp.434-442, 2011.
[3] M. Kaminaga, A. Shikoda, and H. Yoshikawa, "Development and evaluation of a microstep DFA vulnerability estimation method," *IEICE Electronics Express,* vol. 8, no.22, pp.1899-1904, Nov. 2011.
[4] H. Yoshikawa, M. Kaminaga, and A. Shikoda, "Round Addition Using Faults for Generalized Feistel Network," *IEICE Trans. Info. & Syst.*, Vol.E96-D, No.1, pp.146-150, Jan. 2013.
[5] H. Yoshikawa, M. Kaminaga, A. Shikoda, and T. Suzuki, "Round Addition DFA on 80-bit Piccolo and TWINE," *IEICE Trans. Info. & Syst*., Vol.E96-D, No.9, pp.2031-2035, Sept. 2013.
[6] H. Yoshikawa, M. Kaminaga, A. Shikoda, and T. Suzuki, "Round Addition DFA on SPN block ciphers," *IEICE Trans. Fundamentals*., Vol.E97-A, No.12, pp.2671-2674, Dec. 2014.
[7] A. Bogdanov, 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. CHES 2007*, Springer LNCS 4727, pp. 450–466, 2007.
[8] Z. Gong, S. Nikova, and Y. W. Law, "KLEIN: A new family of lightweight block cipher," http://doc.utwente.nl/73129/.
[9] J. Guo, T. Peyrin, A. Poschmann, and M. Robshaw, "The LED block cipher," *Proc. CHES 2011,* Springer. LNCS 6917, pp.326-341, 2011.
[10] N. Bagheri, R. Ebrahimpour, and N. Ghaedi, "New differential fault analysis on PRESENT," EURASIP J. Advances in Signal Processing 2013, 2013:145.
[11] J-M. Dutertre, A-P. Mirbaha, D. Naccache, A-L. Ribotta, A. Tria, and T. Vaschalde, "Fault round modification analysis of the advanced encryption standard," IEEE Int. Synp. Hardware-Oriented Security and Trust (HOST), pp.140-145, 2012.
[12] A. Dehbaoui, J-M. Dutertre, B. Robisson, and A. Tria, "Electromagnetic transient faults injection on a hardware and a software implementations of AES," 2012 Workshop on Fault Diagnosis on Tolerance in Cryptography (FDTC), pp.7-15, 2012.
[13] Wu, and L. Zhang, "LBlock: A lightweight block cipher," Proc. ACNS 2011, LNCS 6715, pp.327-344, 2011.
[14] K. Jeong, C. Lee, and J. I Lim, "Improved differential fault analysis on lightweight block cipher LBlock for wireless sensor networks," EURASIP Journal on Wireless Communications and Networking 2013, 2013:151.
[15] M. Izadi, B. Sadeghiyan, S. Sadeghian, H. Khanooki, "MIBS: A new lightweight block cipher," CANS 2009. LNCS, vol. 5888, pp. 334-348. Springer, 2009.