1. Introduction

Recently, the security of constrained hardware environments such as RFID tags and sensor nodes is major topic in cryptography [1, 2]. The research on lightweight block ciphers suitable for the efficient implementation in constrained hardware environments such as RFID tags and sensor nodes has been studied. As a result, PRESENT [3], LED [4], HIGHT [5], PRINTcipher [6], and Piccolo [7] were proposed.

PRINTcipher is a 48/96-bit block cipher proposed in CHES 2010 which supports the 80/160-bit secret keys. According to the block size, they are denoted by PRINTcipher-48 and PRINTcipher-96, respectively. The attractive properties of PRINTcipher are that all rounds use the same round key and differ only by a round counter and that the linear layer is partially key-dependent. Because of these properties, most known cryptanalytic results on PRINTcipher are based on weak keys (see Table 1). The best attack results on PRINTcipher are invariance subspace attacks on the full PRINTcipher-48/96 [8]. In detail, the attack on the full PRINTcipher-48 is applicable to $2^{52}$ weak keys and requires 5 chosen plaintexts with a negligible computational complexity. In the case of the full PRINTcipher-96, it is applicable to $2^{102}$ weak keys and requires 5 chosen plaintexts with a negligible computational complexity.

In this paper, we find weakness of PRINTcipher-48/96 on related-key attacks. To construct related-key differential characteristics, we focus on related keys that have different values in the part related to a key-dependent permutation. Thus, we can construct $t$-round related-key differential characteristics with a probability of $2^{-t}$. By using these characteristics, we can recover the secret keys of PRINTcipher-48/96. Our results are summarized in Table 1. In detail, to recover the 80-bit secret key of PRINTcipher-48, our attack requires 4 related keys, $2^{47}$ related-key chosen plaintexts, and a computational complexity of $2^{60.62}$. In the case of PRINTcipher-96, we require 4 related keys, $2^{95}$ related-key chosen plaintexts, and a computational complexity of $2^{107}$. These results are the first known related-key cryptanalytic results on them.

This paper is organized as follows. In Section 2, we describe briefly the structure of PRINTcipher. In Section 3, we explain how to construct related-key differential characteristics on PRINTcipher. Related-key attacks on PRINTcipher-48 and PRINTcipher-96 are proposed in Sections 4 and 5, respectively. Finally, we give our conclusion in Section 6.
Table 1: Summary of cryptanalytic results on PRINTcipher.

| Target algorithm | Attack method | Attack rounds | Number of weak keys | Complexity Data | Complexity Computation | Reference |
|------------------|---------------|---------------|---------------------|-----------------|-------------------------|-----------|
| PRINTcipher-48   | DC            | 22            | -                   | 2^48            | 2^48                    | [9]       |
|                  | LC *          | 29            | 2^5                | 2^48            | 2^73                    | [10]      |
|                  | CDLC *        | 31            | 2^68.56            | 2^46.92         | 2^28.92                 | [11]      |
|                  | ISA *         | Full (48)     | 2^52               | 5               | Negligible              | [8]       |
|                  | RKDC          | Full (48)     | -                  | 2^47            | 2^66.62                 | This paper |
| PRINTcipher-96   | ISA *         | Full (96)     | 2^62               | 5               | Negligible              | [8]       |
|                  | RKDC          | Full (96)     | -                  | 2^92            | 2^107                   | This paper |

* Attack results based on weak keys.
CDLC: combined differential and linear cryptanalysis.
ISA: invariant subspace attack.
RKDC: related-key differential cryptanalysis.

2. Description of PRINTcipher

PRINTcipher-48/96 are 48/96-bit block ciphers supporting the 80/160-bit secret keys. Note that PRINTcipher uses the same round key \( SK^1 \) and \( SK^2 \) for all rounds. In detail, the secret key \( K \) is divided into \( SK^1, SK^2 \). \( SK^1 \) is used to XORing with an intermediate value, and \( SK^2 \) controls a key-dependent permutation.

Figure 1 presents a single round of PRINTcipher-b, where \( b \in \{48, 96\} \). The encryption process of PRINTcipher-b is as follows. Here, the number of rounds is \( b \). A \( b \)-bit round key \( SK^1 = (sk^1_0, \ldots, sk^1_{b-1}) \) and a \( (2b/3) \)-bit round key \( SK^2 = (sk^2_0, \ldots, sk^2_{2b/3-1}) \); hence, \( sk^1_0 \) is the most significant bit of \( SK^1 \).

\[ sk^1_j \]

\[
\text{XOR SK}^1
\]

\[
\text{BP}
\]

\[
\text{XOR RC}_i
\]

\[
\text{...}
\]

Figure 1: A single round of PRINTcipher-b.

(1) A \( b \)-bit plaintext \( P = (p_0, p_1, \ldots, p_{b-1}) \) is loaded to a \( b \)-bit intermediate value \( X = (x_0, x_1, \ldots, x_{b-1}) \).

(2) For \( i = 1, \ldots, b \), do the following steps.

(a) \( X \) is XORed with a \( b \)-bit round key \( SK^1 \). Consider

\[
x_j \leftarrow x_j \oplus sk^1_j \quad (j = 0, 1, \ldots, b - 1). \tag{1}
\]

(b) Consider \( X \leftarrow BP(X) \), where \( BP \) is a bit permutation.

(c) Consider \( X \leftarrow X \oplus RC_i \), where \( RC_i \) is a round constant.

(d) For \( i = 0, \ldots, b/3 - 1 \), \( (x_{3i}, x_{3i+1}, x_{3i+2}) \leftarrow KP_i((x_{3i}, x_{3i+1}, x_{3i+2})) \), where \( KP_i \) is the \( i \)th key-dependent permutation based on a 2-bit \( SK^2_i = (sk^2_{i,0}, sk^2_{i,1}) \) (see Figure 1).

(e) Consider that \( X \) is mixed by using \( b/3 \) identical \( 3 \times 3 \) S-boxes.

\[ C = (c_0, \ldots, c_{b-1}) \leftarrow X. \]

With a bit permutation \( BP \), a value of the bit position \( i \) is moved to the bit position \( j \), where

\[
j = \left\lfloor \frac{3i \mod (b - 1)}{b - 1} \right\rfloor, \quad \text{for } 0 \leq i \leq b - 2, \quad \text{for } i = b - 1. \tag{2}
\]

In a key-dependent permutation \( KP \), an intermediate value \( X \) is arranged in \( b/3 \) blocks of 3 bits each, which are permuted individually according to a 2-bit \( SK^2_i \). Out of 6 possible permutations on 3 bits, only four permutations are valid for PRINTcipher. In detail, as shown in Table 2, a 3-bit input value \( (y_0, y_1, y_2) \) is permuted to the corresponding output value according to a 2-bit \( (sk^2_{i,0}, sk^2_{i,1}) \). Here, \( KP^m \) means \( KP_i \) in the case that \( (sk^2_{i,0}, sk^2_{i,1}) = (m, n) \).

3. Construction of Related-Key Differential Characteristics on PRINTcipher

In this section, we present how to construct \( t \)-round related-key differential characteristics on PRINTcipher-48/96 by using properties of a key-dependent permutation \( KP \) and S-box.

3.1. Related-Key Properties on Key-Dependent Permutation and S-Box. We consider a 3-bit input value \( (y_0, y_1, y_2) \) of
Table 2: Key-dependent permutation $K_P_i$.

(a) Notation $(s(k_{i}^{2}, k_{i}^{2}))$ $K_P_i(y_0, y_1, y_2)$
| $K_P_i^{00}$ | (0, 0) | $(y_0, y_1, y_2)$ |
| $K_P_i^{01}$ | (0, 1) | $(y_0, y_1, y_2)$ |
| $K_P_i^{10}$ | (1, 0) | $(y_0, y_2, y_1)$ |
| $K_P_i^{11}$ | (1, 1) | $(y_2, y_1, y_0)$ |

(b) $x$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | $S(x)$ | 0 | 1 | 3 | 6 | 7 | 4 | 5 | 2

a key-dependent permutation $K_P_i$ (i = 0, ..., 15). If a 2-bit round key $(s(k_{i}^{2}, s(k_{i}^{2}))$ is equal to (0, 0) or (0, 1), from Table 2, the corresponding output value is computed as follows:

(i) $(0, 0): (y_0, y_1, y_2) \xrightarrow{K_P_i^{00}} (y_0, y_1, y_2)$;
(ii) $(0, 1): (y_0, y_1, y_2) \xrightarrow{K_P_i^{01}} (y_0, y_2, y_1)$.

In the above relations, if $y_0$ is equal to $y_1$, each permutation outputs the same value and vice versa. That is, the following equation holds:

$y_0 = y_1 \iff K_P_i^{00}((y_0, y_1, y_2)) = K_P_i^{01}((y_0, y_1, y_2))$. (3)

In total, we can obtain the following six properties of $K_P$.

Property 1. Consider $y_0 = y_1 \iff K_P_i^{00}((y_0, y_1, y_2)) = K_P_i^{01}((y_0, y_1, y_2))$.

Property 2. Consider $y_1 = y_2 \iff K_P_i^{00}((y_0, y_1, y_2)) = K_P_i^{10}((y_0, y_1, y_2))$.

Property 3. Consider $y_0 = y_2 \iff K_P_i^{00}((y_0, y_1, y_2)) = K_P_i^{11}((y_0, y_1, y_2))$.

Property 4. Consider $y_0 = y_1 = y_2 \iff K_P_i^{01}((y_0, y_1, y_2)) = K_P_i^{10}((y_0, y_1, y_2))$.

Property 5. Consider $y_0 = y_1 = y_2 \iff K_P_i^{11}((y_0, y_1, y_2))$.

Property 6. Consider $y_0 = y_1 = y_2 \iff K_P_i^{10}((y_0, y_1, y_2)) = K_P_i^{11}((y_0, y_1, y_2))$.

Furthermore, from the definition of $S$-box $S$, we can obtain the following property.

Property 7. If $K_P_i^{00}$ and $K_P_i^{01}$ have the same input value $Y$, the output difference of $S$-box, $S((K_P_i^{00}(Y)) \oplus S(K_P_i^{01}(Y)))$, should be included in a set $\{0, 2, 4\}$.

3.2. Related-Key Differential Characteristics on PRINTcipher-48. Among the above seven properties, we focus on Properties 1, 2 and 3. To apply these properties on the proposed attack, we first consider the following related-key pairs $(K = (SK_1^1, SK_2^2), K^* = (SK_1^{1*}, SK_2^{2*})$. Here, $l = 0, \ldots, 15$.

Case 1 (l). Consider the following:

(i) $SK_1^1 = SK_1^{1*}$;
(ii) $SK_2^2 = (0, 0), SK_2^{2*} = (0, 1)$;
(iii) $SK_2^2 = SK_2^{2*}$ where $i \neq l$.

Case 2 (l). Consider the following:

(i) $SK_1^1 = SK_1^{1*}$;
(ii) $SK_2^2 = (0, 0), SK_2^{2*} = (1, 0)$;
(iii) $SK_2^2 = SK_2^{2*}$ where $i \neq l$.

Case 3 (l). Consider the following:

(i) $SK_1^1 = SK_1^{1*}$;
(ii) $SK_2^2 = (0, 0), SK_2^{2*} = (1, 1)$;
(iii) $SK_2^2 = SK_2^{2*}$ where $i \neq l$.

We assume that the input difference of the target round is zero. If a related-key pair $(K, K^*)$ satisfies Case 1 (0), $K_P_0$ has a nonzero related-key difference. Here, from Property 1, it can be easily shown that the output difference of $K_P_0$ is zero with a probability of $2^{-1}$ (i.e., the probability that $y_0$ is equal to $y_1$). Since the output differences of other $K_P$’s except $K_P_0$ are zero, as shown in Figure 2, we can construct a 1-round related-key differential characteristic $0 \xrightarrow{\text{Case 1 (0)}} 0$ with a probability of $2^{-1}$ under Case 1 (0). Since PRINTcipher-48 uses the same round key for all rounds, we can easily extend this result to a $t$-round related-key differential characteristic. That is, we can construct a $t$-round related-key differential characteristic $0 \xrightarrow{\text{Case 1 (0)}} 0$ with a probability of $2^{-t}$. The other cases of Case 1 (l) are explained in a similar fashion. Moreover, in Case 2 (l) and Case 3 (l), we can construct $t$-round related-key differential characteristics $0 \xrightarrow{\text{Case 2 (l)}} 0$ and $0 \xrightarrow{\text{Case 3 (l)}} 0$ with a probability of $2^{-t}$, respectively.

Note that we cannot control the exact values of the related-key pair $(K, K^*)$ under a related-key attack scenario. In other words, we cannot apply the above related-key differential characteristics to our attack directly. To solve this problem, for each $K_P$, we consider the following four related keys simultaneously. Here, $K$ means the right secret key of PRINTcipher-48.

(i) Consider $K_{(00)}^1 = [SK_1^1, SK_2^2, \ldots, SK_2^2 \oplus (0, 0), \ldots, SK_{15}^2]$ = $K$.
(ii) Consider $K_{(01)}^1 = [SK_1^1, SK_2^2, \ldots, SK_2^2 \oplus (0, 1), \ldots, SK_{15}^2]$.
(iii) Consider $K_{(10)}^1 = [SK_1^1, SK_2^2, \ldots, SK_2^2 \oplus (1, 0), \ldots, SK_{15}^2]$.
(iv) Consider $K_{(11)}^1 = [SK_1^1, SK_2^2, \ldots, SK_2^2 \oplus (1, 1), \ldots, SK_{15}^2]$. 
From these four related keys, we can combine six related-key pairs. For each value of SK$_j^2$, a related-key pair is satisfied one among three cases, Case 1 ($l$), Case 2 ($l$), and Case 3 ($l$) (see Table 3). For example, we assume that SK$_j^2$ is equal to (1, 0). Then, four related keys are computed as follows.

(i) Consider $K_j^{0,0} = [SK_1^1, (SK_0^2, SK_2^2, \ldots, (1, 0) \oplus (0, 0), \ldots, SK_{15}^2)].$

(ii) Consider $K_j^{0,1} = [SK_1^1, (SK_0^2, SK_2^2, \ldots, (1, 0) \oplus (0, 1), 1, 1)], \ldots, SK_{15}^2]).$

(iii) Consider $K_j^{1,0} = [SK_1^1, (SK_0^2, SK_2^2, \ldots, (1, 0) \oplus (1, 0), 0, 0)], \ldots, SK_{15}^2]).$

(iv) Consider $K_j^{1,1} = [SK_1^1, (SK_0^2, SK_2^2, \ldots, (1, 0) \oplus (1, 1), 0, 1)], \ldots, SK_{15}^2]).$

Recall that the condition of Case 1 ($l$) is that SK$_j^2 = (0, 0)$ and SK$_j^{2*} = (0, 1)$. Thus, $(K_j^{1,0}, K_j^{1,1})$ satisfies this condition. Similarly, the condition of Case 2 ($l$) is that SK$_j^2 = (0, 0)$ and SK$_j^{2*} = (1, 0)$. Thus, $(K_j^{1,0}, K_j^{0,0})$ satisfies this condition.

If SK$_j^2$ is equal to (0, 0), three related-key pairs $(K_j^{0,0}, K_j^{0,1})$, $(K_j^{0,0}, K_j^{1,0})$, and $(K_j^{0,0}, K_j^{1,1})$ satisfy Case 1 ($l$), Case 2 ($l$), and Case 3 ($l$), respectively (see Table 3). It means that $t$-round related-key differential characteristics 0\(\xrightarrow{\text{Case 1 (l)}}\) 0, 0\(\xrightarrow{\text{Case 2 (l)}}\) 0, and 0\(\xrightarrow{\text{Case 3 (l)}}\) 0 are satisfied with a probability of $2^{-t}$, respectively. However, if SK$_j^2$ is not equal to (0, 0), only one of related-key pairs satisfies the corresponding condition. For example, it is assumed that the right SK$_j^2$ is (1, 0). Only one key pair, $(K_j^{0,0}, K_j^{1,0})$, among three related-key pairs is satisfied Case 2 ($l$) from Table 3. It means that the corresponding differential characteristic 0\(\xrightarrow{\text{Case 2 (l)}}\) 0 is satisfied with a probability of $2^{-t}$ and that the other differential characteristics 0\(\xrightarrow{\text{Case 1 (l)}}\) 0 and 0\(\xrightarrow{\text{Case 3 (l)}}\) 0 are satisfied with a random probability ($= 2^{-2t}$), respectively.

3.3. Related-Key Differential Characteristics on PRINTcipher-96. In the case of PRINTcipher-96, we can construct 96($= 3 \cdot 32$) $t$-round related-key differential characteristics with a probability $2^{-t}$ by using the similar method on PRINTcipher-48. In detail, for each $K_{P_i}$, we can obtain the same six properties and three cases, Case 1 ($l$), Case 2 ($l$), and Case 3 ($l$). Thus, we get three $t$-round related-key differential characteristics for each $K_{P_i}$ ($l = 0, \ldots, 31$).

4. Related-Key Cryptanalysis on PRINTcipher-48

We are ready to propose related-key cryptanalysis on PRINTcipher-48. Recall that we can construct $t$-round related-key differential characteristics on PRINTcipher-48 with a probability of $2^{-t}$. These related-key differential characteristics depend on the concrete key value. However, the attacker did not control the exact key value under a related-key attack scenario.

To solve this, we use 4 related keys $(K_0^{0,0}, K_0^{0,1})$, $(K_0^{0,0}, K_0^{1,0})$, and $(K_0^{0,0}, K_0^{1,1})$ are considered. Then, among two key pairs, only one should satisfy Case 1 ($l$). Thus we first apply the related-key pair $(K_0^{0,0}, K_0^{0,1})$ to our attack. After that, we repeat the same procedure using the other related-key pair $(K_0^{0,0}, K_0^{1,1})$. For the convenience of description, we assume that the key pair $(K_0^{0,0}, K_0^{0,1})$ satisfies Case 1 ($l$).

4.1. Basic Related-Key Attack on PRINTcipher-48. To attack the full PRINTcipher-48, we consider 44-round related-key differential characteristic 0\(\xrightarrow{\text{Case 1 (l)}}\) 0 (from round 2 to round 45) with a probability of $2^{-44}$.

Our attack procedure mainly consists of the following steps. First, we consider plaintext structures which are composed of 4 plaintexts each. Second, we discard the wrong ciphertext pairs from the difference between ciphertexts. Finally, we guess the partial secret key and determine related-key pairs satisfying Case 1 ($l$).
4.1. Collection of Ciphertexts. First, we consider the following plaintext structures $\delta^{x_{p_{i,j}}}$ which are composed of 4 plaintexts each (see Figure 3).

(i) Consider $\delta^{x_{p_{i,j}}}$, where
(a) $s_{i,j}^{x_{p_{i,j}}} = (||x_j|| ||x_i||)$;
(b) $i, j \in \{0, 1\}$;
(c) $x_0$: arbitrary 15-bit value;
(d) $x_1$: arbitrary 31-bit value.

Among all possible sixteen plaintext pairs for each plaintext structure, we consider only the following 8 plaintext pairs:

\[
\begin{align*}
\delta^{x_{p_{0,0}}} = (s_{0,0}^{x_{p_{0,0}}}, s_{0,1}^{x_{p_{0,0}}}), \\
\delta^{x_{p_{0,1}}} = (s_{0,0}^{x_{p_{0,1}}}, s_{0,1}^{x_{p_{0,1}}}), \\
\delta^{x_{p_{1,0}}} = (s_{0,0}^{x_{p_{1,0}}}, s_{1,1}^{x_{p_{1,0}}}), \\
\delta^{x_{p_{1,1}}} = (s_{0,0}^{x_{p_{1,1}}}, s_{1,1}^{x_{p_{1,1}}}), \\
\delta^{x_{p_{1,2}}} = (s_{1,0}^{x_{p_{1,2}}}, s_{1,1}^{x_{p_{1,2}}}), \\
\delta^{x_{p_{1,3}}} = (s_{1,0}^{x_{p_{1,3}}}, s_{0,0}^{x_{p_{1,3}}}).
\end{align*}
\]

Recall that $(K^{(0,0)}, K^{(0,1)})$ is assumed to satisfy Case 1 (0). Thus, for only four plaintext pairs in each plaintext structure, the input difference of round 2 is zero. Here, when we use $2^{44}$ plaintext structures, the expected number of right pairs is $4(= 4 \cdot 2^{44} \cdot 2^{-44})$. Note that our related-key differential characteristics hold with a probability of $2^{-44}$.

4.1.2. Filtering the Wrong Pairs. We discard the wrong ciphertext pairs by checking the difference between ciphertexts. For the right ciphertext pair, the output difference of round 45 should be zero as shown in Figure 3.

In round 46, from Property 7, the possible output difference of the first S-box is 0 or 2 or 4. The differential propagation in round 47–48 is shown in Figure 3. Then, we discard the wrong ciphertext pairs by checking the following three checkPoints.

(i) **CheckPoint**. The difference between the rightmost 30 bits of ciphertext is zero.

(ii) **CheckPoint**. The output difference of $KP_1, KP_2, \ldots, KP_4$ in round 48 should be included in a set $\{0, 1, 2, 4\}$.

(iii) **CheckPoint**. The input difference of $KP_0$ should be included in a set $\{0, 4\}$.

Since the filtering probability of this step is $2^{-37}(= 2^{-30} \cdot 2^{-15} \cdot 2^{-2})$, $2^{15}(= 8 \cdot 2^{44} \cdot 2^{-37})$ ciphertext pairs are survived.

4.1.3. Recovery of the Secret Key of PRINTcipher-48. For each ciphertext pair passing the above steps, we guess the following 16-bit key:

\[
(SK_1, SK_2, SK_3, SK_4, sk_0, sk_1, sk_2, sk_3, sk_4, sk_5, sk_6, sk_7). \quad (5)
\]

Then we recover 16-bit key by checking the following checkPoints (see Figure 3).

(i) **CheckPoint**. Input differences of $KP_1, KP_2, KP_3, KP_4, and KP_5$ in round 48 should be 0 or 4.

(ii) **CheckPoint**. Input differences of $KP_0$ and $KP_1$ in round 47 should be 0 or 4.

(iii) **CheckPoint**. Output difference of the first S-box in round 46 should be 0 or 2 or 4.

First, we check **CheckPoint**. In this step, we guess a 10-bit key $(SK_2^0, SK_2^1, SK_2^2, SK_2^3, SK_3^0, SK_3^1, sk_0^0, sk_1^0, sk_2^0, sk_3^0, sk_4^0)$. Since the filtering probability of this step is $2^{-7}, 2^5(= 2^{10} \cdot 2^{-5})$ ciphertext pairs remained for each guessed key. Then, we guess an additional 6-bit key $(sk_0^1, sk_1^1, sk_2^1, sk_3^1, sk_4^1)$ and check **CheckPoint** and **CheckPoint**. Since the filtering probabilities of this step are $2^{-4}$ (**CheckPoint**) and 0.75 (**CheckPoint**), the expected number of the remaining ciphertext pairs is 1.5 for each guessed key. Finally, we determine the guessed key with the maximal number of remaining ciphertext pairs as the right key.

Until now, we introduced the attack procedure with a related-key pair $(K_0^{(0,0)}, K_0^{(0,1)})$. In case of the related-key pair $(K_0^{(1,0)}, K_0^{(1,1)})$, the attack procedure can be explained in a similar fashion. Our attack procedure on the full PRINTcipher-48 is summarized as follows.

(1) Select $2^{44}$ plaintext structures which are composed of 4 plaintexts each and obtain the corresponding ciphertexts under four related keys $K_0^{(0,0)}, K_0^{(0,1)}, K_0^{(1,0)}, and K_0^{(1,1)}$, respectively.

(2) Considering the related-key pair $(K_0^{(0,0)}, K_0^{(0,1)})$, we have the following.

(a) Discard wrong pairs which do not satisfy **CheckPoint**, **CheckPoint**, and **CheckPoint**.

(b) Guess 16-bit key $(SK_2^0, SK_2^1, SK_2^2, SK_2^3, SK_3^0, SK_3^1, sk_0^0, sk_1^0, sk_2^0, sk_3^0, sk_4^0, sk_5^0, sk_6^0, sk_7^0, sk_8^0)$ and count the ciphertext pairs satisfying **CheckPoint**, **CheckPoint**, and **CheckPoint**.

(3) Considering the related-key pair $(K_0^{(1,0)}, K_0^{(1,1)})$, we have the following.

(a) Discard wrong pairs which do not satisfy **CheckPoint**, **CheckPoint**, and **CheckPoint**.

(b) Guess 16-bit key $(SK_2^0, SK_2^1, SK_2^2, SK_2^3, SK_3^0, SK_3^1, sk_0^0, sk_1^0, sk_2^0, sk_3^0, sk_4^0, sk_5^0, sk_6^0, sk_7^0)$ and count the ciphertext pairs satisfying **CheckPoint**, **CheckPoint**, and **CheckPoint**.

(4) Output the guessed key with the maximal count as the right key.

(5) Do an exhaustive search for the remaining secret key by using trial encryption.
4.2. Complexities of Basic Related-Key Attack on PRINTcipher-48. This attack considers 4 related keys \( K_0^{(0,0)}, K_0^{(0,1)}, K_0^{(1,0)}, \) and \( K_0^{(0,0)} \). And \( 2^{48} \) plaintexts are used for each related-key. Hence, a data complexity of our attack is \( 2^{48} \) related-key chosen plaintexts.

A computational complexity of Step 1 is \( 2^{48} \) PRINTcipher-48 encryptions. In Step 2(a) and Step 3(a), \( 2^{10} (= 8 \cdot 2^{44} \cdot 2^{-37}) \) ciphertext pairs are survived. Thus computational complexities of Step 2(b) and Step 3(b) do not exceed \( 2^{28} \) PRINTcipher-48 encryptions, respectively. From Step 2 and Step 3, we can recover the 17-bit information on the 80-bit secret key of PRINTcipher-48. Thus, a computational complexity of Step 5 is \( 2^{63} \) PRINTcipher-48 encryptions. Hence, a total computational complexity of our attack is \( 2^{63} \).

4.3. Improved Related-Key Attack on PRINTcipher-48. In this subsection, we improve the basic related-key attack on the full PRINTcipher-48. To improve the basic attack, we consider 43-round related-key differential characteristic \( 0 \rightarrow 0 \) (from round 2 to round 44) with a probability of \( 2^{-43} \). The overall attack procedure is similar to the basic attack procedure.

(1) Select \( 2^{43} \) plaintext structures which are composed of 4 plaintexts each and obtain the corresponding ciphertexts under four related keys \( K_0^{(0,0)}, K_0^{(0,1)}, K_0^{(1,0)}, \) and \( K_0^{(0,1)} \), respectively.

(2) Considering the related-key pair \( (K_0^{(0,0)}, K_0^{(0,1)}) \), we have the following.
(a) Discard wrong pairs which do not satisfy CheckPoint7, CheckPoint8, and CheckPoint9.
(b) Guess 30-bit key \((SK^1, \ldots, SK^{15})\) and remain the ciphertext pairs satisfying CheckPoint10 and CheckPoint11.
(c) Guess 18-bit key \((sk^1, \ldots, sk^{17})\) and count the ciphertext pairs satisfying CheckPoint12, CheckPoint13, and CheckPoint14.

(3) Considering the related-key pair \((K^{(0)}, K^{(1)})\), we have the following.
(a) Discard wrong pairs which do not satisfy CheckPoint7, CheckPoint8 and CheckPoint9.
(b) Guess 30-bit key \((SK^1, \ldots, SK^{15})\) and remain the ciphertext pairs satisfying CheckPoint10 and CheckPoint11.
(c) Guess 18-bit key \((sk^1, \ldots, sk^{17})\) and count the ciphertext pairs satisfying CheckPoint12, CheckPoint13 and CheckPoint14.

(4) Output the guessed key with the maximal count as the right key.
(5) Do an exhaustive search for the remaining secret key using trial encryption.

4.4. Complexities of Improved Related-Key Attack on PRINTcipher-48. The improved attack uses 4 related keys \((K^{(0)}, K^{(1)}, K^{(0)}, K^{(0)})\) and 247 related-key chosen plaintexts. Hence, a data complexity of our attack is 247 related-key chosen plaintexts.

A computational complexity of Step 1 is 247 PRINTcipher-48 encryptions.

In Step 2(a) and Step 3(a), similar to the basic attack, we discard wrong ciphertext pairs by checking the following three checkPoints (see Figure 4).

(i) CheckPoint2. The output difference of \(KP_2, KP_3, \ldots, KP_{15}\) in round 48 should be included in a set \([0, 1, 2, 4]\).
(ii) CheckPoint6. Input difference of \(KP_0\) in round 48 should be included in a set \([0, 2, 4, 6]\).
(iii) CheckPoint8. The output difference of \(KP_1\) in round 48 should be included in a set \([0, 1, 2, 3, 4, 5, 6]\).

The filtering probability of this step is computed as follows:

\[
\frac{7}{2^{18}} \left( = 2^{-114} \cdot \frac{7}{8} \right). \tag{6}
\]

Thus, \(7 \cdot 2^{18} = 8 \cdot 2^{13} \cdot 7/2^{18}\) ciphertext pairs remained on average. So, computational complexities of Step 2(b) and 3(b) are computed as follows:

\[
2^{55.22} \left( \approx 7 \cdot 2^{28} \cdot 2^{30} \cdot \frac{1}{48} \right). \tag{7}
\]

For each remaining ciphertext pair, we guess total 48-bit key \((SK^1, \ldots, SK^9, sk^1, \ldots, sk^7)\). Then we recover 16-bit key by checking the following checkPoints.

(i) CheckPoint10. Input difference of \(KP_2, KP_3, \ldots, KP_{15}\) in round 48 should be included in a set \([0, 4]\).
(ii) CheckPoint11. Input difference of \(KP_1\) in round 48 should be included in a set \([0, 2, 4, 6]\).
(iii) CheckPoint12. Input difference of \(KP_0, KP_1\) in round 47 should be included in a set \([0, 4]\).
(iv) CheckPoint13. Input difference of \(KP_0\) and \(KP_1\) in round 46 should be included in a set \([0, 4]\).
(v) CheckPoint14. Output difference of the first S-box in round 45 should be included in a set \([0, 2, 4]\).

In Step 2(b) and Step 3(b), we guess 30-bit key \((SK^1, \ldots, SK^{15})\) and check CheckPoint10 and CheckPoint11. The filtering probability of this step is computed as follows:

\[
\frac{6}{7} \cdot 2^{14} \left( = 2^{-114} \cdot \frac{6}{7} \right). \tag{8}
\]

Thus, \(3 \cdot 2^{15} = 7 \cdot 2^{28} \cdot 6/(7 \cdot 2^{14})\) ciphertext pairs remained for each guessed key. Since \(3 \cdot 2^{15}\) ciphertext pairs remained in Step 2(b) and Step 3(b) for each guessed key, computational complexities of Step 2(c) and Step 3(c) are \(3 \cdot 2^{59} = 3^{15} \cdot 2^{48} \cdot 3/48\) PRINTcipher-48 encryptions.

In Step 2(c) and Step 3(c), we guess 15-bit key \((sk^1, \ldots, sk^7)\) in order to check CheckPoint12, CheckPoint13 and CheckPoint14. Similar to the basic attack, the expected number of the remaining ciphertext pairs is 1.5 for each guessed key. Note that the expected number of right pairs is 4 similar to the basic attack.

Since we can recover the 49-bit information on the 80-bit secret key of PRINTcipher-48, a computational complexity of Step 5 is \(2^{31}\) PRINTcipher-48 encryptions. Hence, a total computational complexity of our attack is computed as follows:

\[
2^{60.62} \left( = 2^{47} + 2^{55.22} + (3 \cdot 2^{59}) + 2^{31} \right). \tag{9}
\]

5. Related-Key Cryptanalysis on PRINTcipher-96

The overall attack procedure on the full PRINTcipher-96 is similar to that on the full PRINTcipher-48. Thus, we explain the attack procedure on the full PRINTcipher-96 briefly. In this attack, we consider 91-round related-key differential characteristics \(0 \xrightarrow{X_{01}} 0\) (from round 2 to round 92) with a probability of \(2^{-91}\). The checkPoints used in this attack are as follows (see Figure 5).

(i) CheckPoint15. The rightmost 40-bit of ciphertext does not have difference.
(ii) CheckPoint16. The output difference of \(KP_1, KP_2, \ldots, KP_{15}\) in round 48 is included in a set \([0, 1, 2, 4]\).
(iii) CheckPoint17. The input difference of \(KP_0\) is included in a set \([0, 4]\).
(iv) CheckPoint$_{18}$. Input difference of $KP_1$, $KP_2$, \ldots, $KP_{17}$ in round 96 should be included in a set $\{0, 4\}$.

(v) CheckPoint$_{19}$. Input difference of $KP_0$, \ldots, $KP_5$ in round 95 should be included in a set $\{0, 4\}$.

(vi) CheckPoint$_{20}$. Input difference of $KP_0$ and $KP_1$ in round 94 should be included in a set $\{0, 4\}$.

(vii) CheckPoint$_{21}$. Output difference of the first $S$-box in round 93 should be included in a set $\{0, 2, 4\}$.

The attack procedure on the PRINTcipher-96 is summarized as follows.

(1) Select $2^{31}$ plaintext structures which are composed of 4 plaintexts each and obtain the corresponding
Figure 5: Related-key differential attack on PRINTciper-96.

ciphertexts under four related keys \( K_0^{(0,0)}, K_0^{(0,1)}, K_0^{(1,0)}, \) and \( K_0^{(1,1)} \), respectively.

2) Considering the related-key pair \( (K_0^{(0,0)}, K_0^{(0,1)}) \), we have the following.

(a) Discard wrong pairs which do not satisfy CheckPoint\(_{15}\), CheckPoint\(_{16}\), and CheckPoint\(_{17}\).
(b) Guess 34-bit key \( (SK_1^2, \ldots, SK_{17}^2) \) and remain the ciphertext pairs satisfying CheckPoint\(_{18}\).
(c) Guess 18-bit key \( (sk_0^1, \ldots, sk_{17}^1) \) and count the ciphertext pairs satisfying CheckPoint\(_{19}\), CheckPoint\(_{20}\), and CheckPoint\(_{21}\).

3) Considering the related-key pair \( (K_0^{(1,0)}, K_0^{(1,1)}) \), we have the following.

(a) Discard wrong pairs which do not satisfy CheckPoint\(_{15}\), CheckPoint\(_{16}\), and CheckPoint\(_{17}\).
(b) Guess 34-bit key \( (SK_1^2, \ldots, SK_{17}^2) \) and remain the ciphertext pairs satisfying CheckPoint\(_{18}\).

4) Output the guessed key with the maximal count as the right key.

5) Do an exhaustive search for the remaining secret key using trial encryption.

Since 4 related keys \( (K_0^{(0,0)}, K_0^{(0,1)}, K_0^{(1,0)}, \) and \( K_0^{(0,1)} \) \) are used in our attack, the data complexity of our attack is \( 2^{95} \) related-key chosen plaintexts. And a total computational complexity of our attack is about \( 2^{107} \) PRINTcipher-96 encryptions.

6. Conclusion

In this paper, we proposed related-key cryptanalysis of PRINTcipher. Our attack results are summarized in Table 1. To recover the 80-bit secret key of PRINTcipher-48, our
attack required $2^{47}$ related-key chosen plaintexts with a computational complexity of $2^{60.62}$. In the case of PRINTcipher-96, $2^{25}$ related-key chosen plaintexts with a computational complexity of $2^{107}$ are required. These results are the first known related-key cryptanalytic results on them.

**Conflict of Interests**

The authors declare that there is no conflict of interests regarding the publication of this paper.

**Acknowledgment**

This research was supported by the MSIP (Ministry of Science, ICT & Future Planning), Korea, under the C-ITRC (Convergence Information Technology Research Center) Support Program (NIPA-2013-H0301-13-3007).

**References**

[1] A. Grover and H. Berghel, “A survey of RFID deployment and security issues,” *Journal of Information Processing Systems*, vol. 7, no. 4, pp. 561–580, 2011.

[2] D. Seo and I. Lee, “A study on RFID system with secure service availability for ubiquitous computing,” *Journal of Information Processing Systems*, vol. 1, no. 1, pp. 96–101, 2005.

[3] A. Bogdanov, L. R. Knudsen, G. Leander et al., “PRESENT: an ultra-lightweight block cipher,” in *Cryptographic Hardware and Embedded Systems—CHES 2007*, vol. 4727 of *Lecture Notes in Computer Science*, pp. 450–466, Springer, Berlin, Germany, 2007.

[4] J. Guo, T. Peyrin, A. Poschmann, and M. Robshaw, “The LED block cipher,” in *Cryptographic Hardware and Embedded Systems—CHES 2011*, vol. 6917 of *Lecture Notes in Computer Science*, pp. 326–341, Springer, Berlin, Germany, 2011.

[5] D. Hong, J. Sung, S. Hong et al., “HITE: a new block cipher suitable for low-resource device,” in *Cryptographic Hardware and Embedded Systems—CHES 2006*, vol. 4249 of *Lecture Notes in Computer Science*, pp. 46–59, Springer, Berlin, Germany, 2006.

[6] L. Knudsen, G. Leander, A. Poschmann, and M. J. B. Robshaw, “PRINTcipher: a block cipher for IC-printing,” in *Cryptographic Hardware and Embedded Systems, CHES 2010*, vol. 6225 of *Lecture Notes in Computer Science*, pp. 16–32, Springer, Berlin, Germany, 2010.

[7] K. Shibutani, T. Isobe, H. Hiwatari, A. Mitsuda, T. Akishita, and T. Shirai, “Piccolo: an ultra-lightweight blockcipher,” in *Cryptographic Hardware and Embedded Systems—CHES 2011*, vol. 6917 of *Lecture Notes in Computer Science*, pp. 342–357, Springer, Berlin, Germany, 2011.

[8] G. Leander, M. A. Abdelaheem, H. Alkhzaimi, and E. Zenner, “A cryptanalysis of PRINTcipher: the invariant subspace attack,” in *Advances in Cryptology—CRYPTO 2011*, vol. 6841 of *Lecture Notes in Computer Science*, pp. 206–221, Springer, Berlin, Germany, 2011.

[9] M. A. Abdelaheem, G. Leander, and E. Zenner, “Differential cryptanalysis of round-reduced PRINTcipher: computing roots of permutations,” in *Fast Software Encryption*, vol. 6733 of *Lecture Notes in Computer Science*, pp. 1–17, Springer, Berlin, Germany, 2011.

[10] M. Ågren and T. Johansson, “Linear cryptanalysis of PRINTcipher—trails and samples everywhere,” in *Progress in Cryptology—INDOCRYPT 2011*, vol. 7107 of *Lecture Notes in Computer Science*, pp. 114–133, Springer, Berlin, Germany, 2011.

[11] F. Karaço, H. Demirci, and A. E. Harmanç, “Combined differential and linear cryptanalysis of reduced-round PRINTcipher,” in *Selected Areas in Cryptography*, vol. 7118 of *Lecture Notes in Computer Science*, pp. 169–184, Springer, Berlin, Germany, 2012.