Reflection Cryptanalysis of PRINCE-Like Ciphers

Hadi Soleimany[1(✉)], Céline Blondeau[1], Xiaoli Yu[2,3], Wenling Wu[2], Kaisa Nyberg[1], Huiling Zhang[2], Lei Zhang[2], and Yanfeng Wang[2]

[1] Department of Information and Computer Science, Aalto University School of Science, Espoo, Finland
{hadi.soleimany,celine.blondeau}@aalto.fi
[2] TCA, Institute of Software, Chinese Academy of Sciences, Beijing, People's Republic of China
[3] Graduate University of Chinese Academy of Sciences, Beijing, People's Republic of China
{yuxiaoli,wwl}@is.iscas.ac.cn

Abstract. PRINCE is a low-latency block cipher presented at ASIACRYPT 2012. The cipher was designed with a property called α-reflection which reduces the definition of the decryption with a given key to an encryption with a different but related key determined by α. In the design document, it was shown that PRINCE is secure against known attacks independently of the value of α, and the design criteria for α remained open.

In this paper, we introduce new generic distinguishers on PRINCE-like ciphers. First, we show that, by folding the cipher in the middle, the number of rounds can be halved due to the α-reflection property. Furthermore, we investigate many classes of α and find the best differential characteristic for the folded cipher. For such α there exist an efficient key-recovery attack on the full 12-round cipher with the data complexity of $2^{57.98}$ known plaintexts and time complexity of $2^{72.39}$ encryptions. With the original value of α we can attack a reduced six-round version of PRINCE. As a result of the new cryptanalysis method presented in this paper, new design criteria concerning the selection of the value of α for PRINCE-like ciphers are obtained.

Keywords: Block cipher · α-reflection property · PRINCE · Statistical attack · Reflection attack

1 Introduction

Recently, important applications in special constrained environments such as RFID tags and sensors have received a lot of attention by the cryptographic community. The new secure primitives should provide the best security possible while under tight constraints. Traditionally, cryptographic algorithms have been designed with large security margin to be on the secure side even when exposed

S. Moriai (Ed.): FSE 2013, LNCS 8424, pp. 71–91, 2014.
DOI: 10.1007/978-3-662-43933-3_5,

to new and unknown vulnerabilities. Since lightweight ciphers must be as small and power-efficient as possible, it is of utmost importance to analyze and understand the security of cryptographic designs to reduce the superfluous margins. New innovative and unconventional designs pose new challenges. For instance, to reduce the power consumption of the encryption algorithm, new cipher proposals, such as PRINTcipher [7] and LED [5] with very simple key-schedule or even without key-schedule, have been developed. With the emergence of such constructions, new attacks have emerged.

PRINCE is a low-latency block cipher proposed at ASIACRYPT 2012 [2]. In order to reduce the cost of implementation of decryption, this iterated cipher uses a property called α-reflection. As the key-schedule of the encryption is almost non-existent, the round constants play crucial role in preventing self-similarity attacks like slide attacks. The α-reflection property is built in the cipher by selecting the round constants in pairs. The constants that form a pair have a difference equal to α, and if one of them is used on round r then the other one is used on round $2R-r+1$, where $r = 1, 2, \ldots, 2R$, and $2R$ is the total number of rounds of the cipher. As the round functions at round r and $2R-r+1$, $r < R$, are selected to be inverses of each other, it follows that decryption with round key K is identical to encryption with round key $K \oplus \alpha$.

In the original proposal, the security of PRINCE and the effects of the α-reflection were studied extensively. In particular, it was shown that the cipher is secure against known attacks with reasonable security margin. For instance, it was shown that any differential or linear characteristic over 4 consecutive rounds has at least 16 active S-boxes. This holds independently of the selection of the non-zero parameter α.

In this paper, we study PRINCE in a more general setting of PRINCE-like ciphers by allowing freedom in the selection of the value of α and of some other components of the cipher. We identify new types of relations over the cipher, and show that they can be used as distinguishers over PRINCE, but that their effectivity depends crucially on the properties of α. We call these new relations *reflection characteristics*. They are constructed by feeding input data of round r, $r \leq R$, forward over $2(R-r+1)$ rounds and comparing it with the corresponding output data of round $2R-r+1$ by exclusive-or differences. We investigate distributions of these reflection differences. Their non-uniformity properties crucially depend on the relationships between the differential properties of the round function, fixed points of the middle linear layer and the reflection parameter α.

The starting point of the reflection cryptanalysis is a probabilistic relation on the middle rounds of the cipher. The extracted relations starting from the middle of the cipher share some similarities with some attacks on Feistel ciphers. Self-similarity properties can be used to determine classes of weak keys as for instance for the DES [8]. The reflection attack [6] and its modifications for hash functions [3] take advantage of involution properties when classes of fixed points exist in some intermediate rounds. In this paper, the involution property is replaced by the α-reflection property, and the resulting reflection characteristics are not

necessarily deterministic, but evaluated in terms of differential probabilities. The resulting attacks require known plaintext only.

In sharp contrast to differential and linear characteristics on PRINCE-like ciphers, the number of active S-boxes in a reflection characteristic strongly depends on the value of α. In particular, we show that for some values of α the key-recovery attack using reflection characteristic works for the full cipher. We present a known-plaintext single-key attack with the data complexity of $2^{57.95}$ plaintexts and time complexity of $2^{72.37}$. For the original α specified in [2], the key recovery attack using a reflection distinguisher found in this paper breaks reduced-round versions of the cipher only up to 6 rounds and hence does not threaten the security of full 12-round version of PRINCE. Nevertheless, we believe that the introduction of the new distinguishers will shed light on the security of PRINCE-like ciphers and can be taken into consideration when designing ciphers according to the model of PRINCE.

The paper is organized as follows. In Sect. 2, we define a family of ciphers called PRINCE-like ciphers. In Sect. 3, different characteristics for the ciphers in this family are described and their probabilities determined. Concatenations of these characteristics are also studied in order to provide characteristics on a larger number of rounds. In Sect. 4, we show how reflection characteristics over $2R-2$ rounds of the cipher can be converted to distinguishers and used for key recovery attacks on the full $2R$ rounds of the cipher. In Sect. 5, we evaluate the complexity of the best reflection attacks and identify classes of the weakest α using the original S-layer and M-layer of PRINCE.

2 Brief Description of PRINCE

Distinguishers and attacks presented in this paper focus not only on the original PRINCE but are more general and can be applied to all ciphers with similar reflection structure. To this aim, let us start by describing what we call a PRINCE-like cipher.

2.1 PRINCE-Like Cipher

A PRINCE-like cipher encrypts messages of n-bit blocks by iterating $2R$ times a round function. We denote by E_k^α the encryption function parametrized with a $2n$-bit key $k = (k_0||k_1) \in \mathbb{F}_2^{2n}$ and the reflection parameter $\alpha \in \mathbb{F}_2^{n*}$.

The key schedule of a PRINCE-like cipher is simple. The $2n$-bit key is split into two n-bit parts k_0 and k_1. From k_0, a key k_0' is derived using a rotation and a shift as follows

$$k_0' = (k_0 \ggg 1) \oplus (k_0 \gg (n-1)). \tag{1}$$

The keys k_0 and k_0' are used as whitening keys in the encryption operation that follows the FX structure. The n-bit key k_1 is added to the state in the $2R$ rounds of the cipher.

The core function $G_{k_1}^\alpha$ of this cipher (denoted by PRINCE$_{core}$ in the original proposal) is defined as an iteration of the $2R$ rounds. To keep it as general

as possible, we assume that we have a non-linear S-layer composed of a set of parallel Sboxes and two different linear layers, defined by $n \times n$ matrices M' and M, where M' is an involution matrix.

The first $R-1$ rounds $\mathfrak{R}_r : \mathbb{F}_2^n \to \mathbb{F}_2^n$, $1 \leq r \leq R-1$, are identical and are composed (in this order) of addition of the round constant RC_r and the key k_1, the non-linear layer S and the linear permutation layer M. The $R-1$ last rounds $\mathfrak{R}_r : \mathbb{F}_2^n \to \mathbb{F}_2^n$, $R+2 \leq r \leq 2R$ are, in the reverse order, equal to inverses of the first $R-1$ rounds except that the round constants are modified by α so that the following holds:

$$RC_{2R-r+1} = RC_r \oplus \alpha, \text{ for all } r = 1, \ldots, 2R. \tag{2}$$

We call these rounds with $r \leq R-1$ or $r \geq R+2$ the external rounds of the PRINCE-like cipher.

The symmetry is broken by specifying the two middle rounds R and $R+1$ to be different from each other and from the external rounds. Below we summarize the definitions for all rounds.

$$\begin{array}{ll} \mathfrak{R}_r(x) = M(S(x \oplus RC_r \oplus k_1)) & \text{if } 1 \leq r \leq R-1 \\ \mathfrak{R}_r(x) = M'(S(x \oplus RC_r \oplus k_1)) & \text{if } r = R \\ \mathfrak{R}_r(x) = S^{-1}(x) \oplus RC_r \oplus k_1 & \text{if } r = R+1 \\ \mathfrak{R}_r(x) = S^{-1}(M^{-1}(x)) \oplus RC_r \oplus k_1 & \text{if } R+2 \leq r \leq 2R \end{array} \tag{3}$$

The function $G_{k_1}^{\alpha}(x)$ is then defined as the composition of these $2R$ round functions. The structure of the cipher is depicted in Fig. 1. The family of PRINCE-like ciphers have been designed, like for the original cipher, such that decryption can be obtained from encryption with a different key. If we denote by P a plaintext, the corresponding ciphertext is computed as $C = E_k^{\alpha}(P)$ with $k = (k_0||k_0'||k_1)$. Decryption of C can be obtained by computing the encryption over a related key: $D_k^{\alpha}(C) = E_{k'}^{\alpha}(C)$ with $k' = (k_0'||k_0||k_1 \oplus \alpha)$.

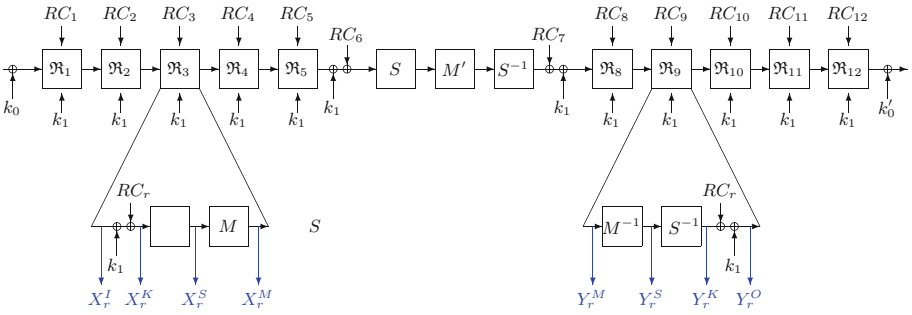


Fig. 1. Description of a $2R = 12$ rounds PRINCE-like cipher

2.2 Description of PRINCE

The full specification of PRINCE is given in [2]. It is a PRINCE-like cipher with $n = 64$ and $R = 6$. The reflection constant is defined as $\alpha =$ `C0AC29B7C97C50DD`. The function $G_{k_1}^{\alpha}$ is called PRINCE$_{core}$. The S-layer is a non-linear layer where each nibble is processed by the same Sbox. The action of this Sbox is given in Table 5, in Appendix A.1. To construct the linear layers, first two 16×16 binary involution matrices $\hat{M}_0, \hat{M}_1$ are defined. Definition of these components can be found in Appendix A.1. Then the 64×64 block diagonal matrix M' is generated by setting its diagonal equal to $(\hat{M}_0, \hat{M}_1, \hat{M}_1, \hat{M}_0)$. Then M' is an involution. The second linear matrix M for PRINCE is obtained by composition of M' and a permutation SR of nibbles by setting $M = SR \circ M'$. The permutation SR is analogous to the AES shift row operation, but instead of bytes, it operates on nibbles.

Definition of the original round constants can be found in [2]. Exact values of these round constants are not used in the analysis presented in this paper. However, our attacks exploit the α-reflection of the round constants RC_r, $r = 1, \ldots, 12$, given in (2).

The description of the round functions given in Sect. 2.1 differs slightly from the original. Nevertheless, it is easy to see that both descriptions are equivalent.

3 Distinguishers for PRINCE-Like Ciphers

In this section, different reflection characteristics on PRINCE-like ciphers are constructed and investigated. The necessary notations for describing these characteristics are depicted in Fig. 1 and explained next in more detail.

Given the round number r, $1 \leq r \leq R$, we denote by X_r^I the input state of the round number r, and by X_r^K, X_r^S and X_r^M, the states *after* the key and round constant addition, the S-layer, and the M-layer, respectively. In order to exploit the symmetry of the cipher, we give different definitions for $R + 1 \leq r \leq 2R$. For these rounds, we denote by Y_r^O the output state of the round number r, and by Y_r^K, Y_r^S and Y_r^M, the states *before* the key and round constant addition, the S-layer, and the M-layer, respectively.

To build a distinguisher on a PRINCE-like cipher, we introduce two types of characteristics. First we focus on the middle rounds of the cipher which are different from the external ones. Characteristics on the middle rounds depend on the property of the matrix M'. Then by using a folded view of the cipher and the α-reflection property, we extend these characteristics to the external rounds of the cipher.

3.1 Characteristics on the Middle Rounds

We identify two kinds of characteristics on 2 or 4 middle rounds of the cipher. The first characteristic on the 2 midmost rounds is independent of the reflection parameter. The second one is defined on 4 rounds and extends over one round

before and one round after the midmost rounds. It behaves differently depending of the reflection parameter. Probability of both of these characteristics is related to the number of fixed points of the matrix M'.

Definition 1. *Let $f : A \to A$ be a function on a set A. A point $x \in A$ is called a fixed point of the function f if and only if $f(x) = x$.*

In [2] it is stated based on the result of [4] that the number of fixed points of an involution $f : \mathbb{F}_2^n \to \mathbb{F}_2^n$ is on the average equal to $2^{n/2}$. While the result of [4] holds in general, restricting to the case of linear involutions f over $\mathbb{F}_2$ gives the following result.

Lemma 1. *Let $f : \mathbb{F}_2^n \to \mathbb{F}_2^n$ be a linear involution. Then the number of fixed points of f is greater than or equal to $2^{n/2}$.*

Proof. Let us denote $B = f \oplus I$, where I is the $n \times n$ identity matrix over $\mathbb{F}_2$. Then $B^2 = 0$, which means that $\mathrm{Im}(B) \subset \mathrm{Ker}(B)$. As $\dim(\mathrm{Ker}(B)) + \dim(\mathrm{Im}(B)) = n$, we have $\dim(\mathrm{Ker}(B)) \geq \frac{n}{2}$. As $\mathrm{Ker}(B)$ is the set of fixed points of f, the claim follows.

In what follows, we denote by $F_{M'}$, the set of fixed points of the matrix M' and by $|F_{M'}|$ the size of this set, which by Lemma 1 is larger than or equal to $2^{n/2}$.

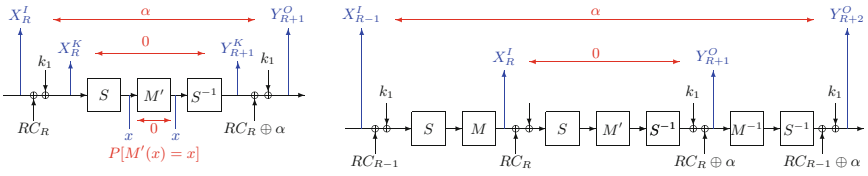
Characteristic $\mathcal{I}_1$. The characteristic

$$Y_{R+1}^O \oplus X_R^I = \alpha$$

over two rounds $\mathfrak{R}_{R+1} \circ \mathfrak{R}_R$ of a PRINCE-like cipher holds with probability

$$\mathcal{P}_{\mathcal{I}_1} = \mathcal{P}_{F_{M'}} = \frac{|F_{M'}|}{2^n}.$$

Characteristic $\mathcal{I}_1$ is depicted in Fig. 2(a). By Lemma 1 we have that $\mathcal{P}_{\mathcal{I}_1} \geq 2^{-n/2}$. As the matrix M' of PRINCE has exactly $2^{32} = 2^{n/2}$ fixed points, it minimizes the probability of characteristic $\mathcal{I}_1$.



(a) $\mathcal{I}_1$ (b) $\mathcal{I}_2$

Fig. 2. Middle-round characteristics

Characteristic $\mathcal{I}_2$. The characteristic

$$Y_{R+2}^{O} \oplus X_{R-1}^{I} = \alpha$$

over four rounds $\mathfrak{R}_{R+2} \circ \mathfrak{R}_{R+1} \circ \mathfrak{R}_R \circ \mathfrak{R}_{R-1}$ of a PRINCE-like cipher holds with probability

$$\mathcal{P}_{\mathcal{I}_2} = 2^{-n} \# \left\{ x \in \mathbb{F}_2^n \mid S^{-1}\Big(M'\big(S(x)\big)\Big) \oplus x = \alpha \right\}.$$

Characteristic $\mathcal{I}_2$ is depicted in Fig. 2(b). Next we show that $\mathcal{P}_{\mathcal{I}_2}$ can be computed efficiently. We write

$$\mathcal{P}_{\mathcal{I}_2} = 2^{-n} \sum_{\Delta \in \mathbb{F}_2^n} \# \left\{ x \in \mathbb{F}_2^n \mid M'\big(S(x)\big) \oplus S(x) = \Delta, S(x \oplus \alpha) \oplus S(x) = \Delta \right\}.$$

The set on the right hand side of the equality is not empty only if $\Delta \in \mathrm{Im}(M' \oplus I)$. We then deduce as in the proof of Lemma 1 that $\Delta \in F_{M'}$, and obtain

$$\mathcal{P}_{\mathcal{I}_2} = 2^{-n} \sum_{\Delta \in F_{M'}} \# \left\{ x \in \mathbb{F}_2^n \mid M'(S(x)) \oplus S(x) = \Delta, S(x \oplus \alpha) \oplus S(x) = \Delta \right\}.$$

Assuming that the fixed point properties of M' and differential properties of S are independent we obtain

$$\mathcal{P}_{\mathcal{I}_2} \approx \mathcal{P}_{F_{M'}} \sum_{\Delta \in F_{M'}} \Pr_{\mathbf{X}} \left[S(\mathbf{X}) \oplus S(\mathbf{X} \oplus \alpha)) = \Delta \right]. \tag{4}$$

The exact expression of the probability can be efficiently evaluated as the summation is taken over the fixed points only. In the case where M' is a block-diagonal matrix, the probability $\mathcal{P}_{\mathcal{I}_2}$ can be computed by decomposing the probabilities over the different blocks, and will be shown in detail in the case of PRINCE in Sect. 5.

This characteristic is useful for building a distinguisher if $\mathcal{P}_{\mathcal{I}_2} > 2^{-n}$. But depending on M' and the value of α, it is also possible that $\mathcal{P}_{\mathcal{I}_2} = 0$. In this case we get an *impossible reflection characteristic*. We will show in Sect. 4.2 how characteristic $\mathcal{I}_2$, even if impossible, can be used for a distinguisher. Such a situation occurs if $S(x \oplus \alpha) \oplus S(x)$ is never equal to a fixed point of M'.

3.2 External Characteristic

When the probabilities $\mathcal{P}_{\mathcal{I}_1}$ and $\mathcal{P}_{\mathcal{I}_2}$ are large, it is useful to extend the characteristics $\mathcal{I}_1$ and $\mathcal{I}_2$ to more rounds. In what follows, we denote these characteristics by $\mathcal{I}_v$, $v = 1, 2$. The structure of PRINCE-like ciphers is such that the first and the last external rounds are symmetrical. One of the main ideas in this paper is to use this specific property to extend the distinguishers $\mathcal{I}_v$, which cover $2v$ middle rounds, to external rounds. This idea is illustrated in Fig. 3, which gives another view of the cipher. In this representation, the $2R$-round cipher can be viewed as composed of two parallel copies of a $(R-v)$-round cipher connected together by $2v$ rounds. Then characteristics on $2u$ external rounds, $1 \leq u \leq R-v$, are built as ordinary related key differential characteristics with input data difference equal to α and the key difference or round constant difference equal to α.

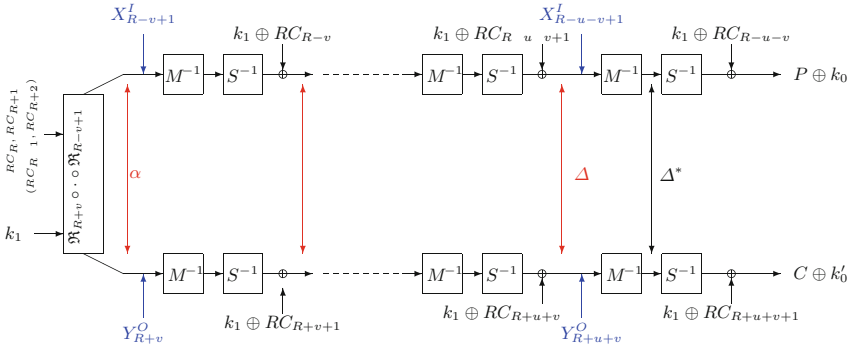


Fig. 3. A folded view of a PRINCE-like cipher: the external characteristic

Characteristic $\mathcal{C}_u$. Suppose that the characteristic $Y^O_{R+v} \oplus X^I_{R-v+1} = \alpha$ holds. The characteristic

$$Y^O_{R+u+v} \oplus X^I_{R-u-v+1} = \Delta$$

on the $2u$ external rounds is denoted by $\mathcal{C}_u$. It holds with probability

$$\mathcal{P}_{\mathcal{C}_v} = \Pr_{\mathbf{X}} \left[F^u_0(x) \oplus F^u_\alpha(x \oplus \alpha) = \Delta \right],$$

where $F^u_0 = \mathfrak{R}^{-1}_{R-v-u+1} \circ \cdots \circ \mathfrak{R}^{-1}_{R-v}$ and $F^u_\alpha = \mathfrak{R}^{-1}_{R+v+u} \circ \cdots \circ \mathfrak{R}^{-1}_{R+v+1}$.

The probability of this characteristic can be computed by using techniques similar to the ones used in classical differential cryptanalysis. In particular, using the Branch and Bound algorithm, it is possible to find the best characteristics for a fixed reflection parameter α. Description of this method for PRINCE is detailed in Sect. 5.

In comparison with differential cryptanalysis, the characteristic $\mathcal{C}_u$ benefits from the related constant α. Similarly to related key differential attacks, zero differences between states are possible. Then two parallel rounds, say $\mathfrak{R}_{R-z+1}$ and $\mathfrak{R}_{R+z}$, can for some characteristics be passed with probability equal to 1. This happens when the data difference is cancelled by the key or round constant difference. Examples of such situations will be given in Sect. 5. Even when the difference is non-zero, two rounds of the cipher can be passed at the cost of one non-linear layer, where the classical differential cryptanalysis on PRINCE-like ciphers must consider differential probabilities over two non-linear layers.

Distinguishers over several rounds of the cipher, can then be built using a combination of the external characteristic $\mathcal{C}_u$ with $\mathcal{I}_v$, $v = 1, 2$. If $\mathcal{P}_{\mathcal{I}_v} \times \mathcal{P}_{\mathcal{C}_u} > 2^{-n}$, then $2v + 2u$ rounds of the cipher are distinguishable from random. In Sect. 5 we identify classes of parameters α such that 4, 6, 8 and 10 rounds of a PRINCE-like cipher can be distinguished from random.

4 Key Recovery

The characteristics constructed in the previous section can be used to build either a probabilistic or a deterministic distinguisher. The combination of $\mathcal{I}_v$

and $\mathcal{C}_u$ gives a *probabilistic reflection distinguisher*. Then the relation

$$Y^O_{R+i} \oplus X^I_{R-i+1} = \Delta, \tag{5}$$

for some $i = u + v$, holds with a positive probability p.

A deterministic distinguisher over 4 rounds exists for those values of α such that $\mathcal{P}_{\mathcal{I}_2} = 0$. Then we have an *impossible reflection distinguisher* such that the relation

$$Y^O_{R+2} \oplus X^I_{R-1} \neq \alpha, \tag{6}$$

holds with probability 1.

In this section we describe how to convert these distinguishers on $2i$ rounds to a key recovery attack on a cipher of $2R = 2i + 2$ rounds.

4.1 Probabilistic Reflection Setting

Assuming a probabilistic distinguisher on $2i$ rounds of a PRINCE-like cipher as described in Sect. 3, a key recovery attack can be derived by counting the number of plaintext-ciphertext pairs such that the difference between X^I_2 and Y^O_{2i+1} is equal to Δ.

In what follows, we denote by 2^m the data complexity of the attack. This value can be computed using Algorithm 1 of [1]. If we denote by a the advantage of this attack, the corresponding false alarm probability is $p_{\text{fa}} = 2^{-a}$.

Key Recovery Attack for $2R = 2i + 2$ Rounds. Let us assume that a characteristic $Y^O_{2i+1} \oplus X^I_2 = \Delta$ over the midmost $2i$ rounds holds with probability p, $0 < p \leq 1$. Without modification of the probability, this characteristic can be extended in both sides over linear layer M^{-1} to obtain a characteristic $Y^S_{2i+2} \oplus X^S_1 = M^{-1}(\Delta) = \Delta^*$ depicted in Fig. 4.

To find the values of X^S_1 and Y^S_{2i+2} for all pairs (P, C), the whole key $(k_0||k_1)$ needs to be guessed. The procedure makes use of the word-oriented structure of the non-linear layer. We assume that the S-layer is nibble-oriented like in the original PRINCE.

We present the n-bit state with $n/4$ nibbles and number them from 1 to $n/4$. The j-th nibble of any n-bit word X is denoted by $X(j)$. The complexity of the attack depends of the number of non-zero nibbles of Δ^*. In what follows, we denote by $w(\Delta^*)$, the number of non-zero nibbles of the difference Δ^*.

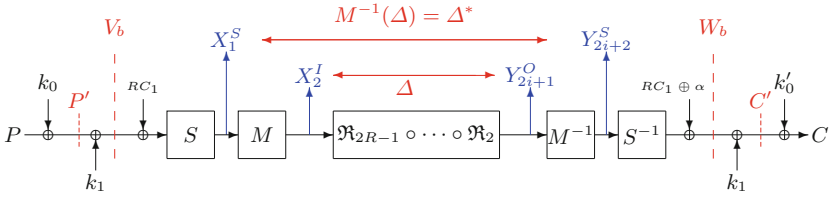


Fig. 4. Key recovery principle when $2R = 2i + 2$

As depicted in Fig. 4, the following property holds for all $1 \leq j \leq n/4$:

$$\Delta^*(j) = S\big(P(j) \oplus k_0(j) \oplus k_1(j) \oplus RC_1(j)\big) \oplus S\big(C(j) \oplus k_0'(j) \oplus k_1(j) \oplus RC_{2R}(j)\big).$$

We denote the number of nibbles of Δ^* that are equal to zero by $\ell = n/4 - w(\Delta^*)$. Indices of these nibbles are stored in a list L. Hence $|L| = \ell$. Then the property

$$P(j) \oplus k_0(j) \oplus C(j) \oplus k_0'(j) \oplus \alpha(j) = 0,$$

holds for all $j \in L$, and can be used to reduce the time complexity of the attack. For these nibbles, the value of $k_1(j)$ need not be guessed. Guessing $k_0 \oplus k_0'$ and computing $P(j) \oplus k_0(j) \oplus C(j) \oplus k_0'(j)$ allows us to discard already a large number of (P, C) pairs.

Let us assume that the attacker has 2^m plaintexts with corresponding ciphertexts. Then the attack proceeds as follows:

1. For $2^{4\ell}$ values of K_0 such that $K_0(j) = k_0(j) \oplus k_0'(j)$ holds for all $j \in L$
   - 1.0 Take all 2^m plaintext ciphertext pairs
   - 1.1 For all $j \in L$
     Among the remaining pairs discard the ones such that $P(j) \oplus C(j) \oplus K_0(j) \oplus \alpha(j) \neq 0$.
   - 1.2 For $2^{4w(\Delta^*)} = 2^{n-4\ell}$ values of K_1 such that $K_1(j) = k_0(j) \oplus k_1(j)$ holds for all $j \notin L$ and for all $2^{n-4\ell}$ completions of K_0
     - 1.2.1 For all $j \notin L$
       Compute $K_1'(j) = K_0(j) \oplus K_1(j) = k_0'(j) \oplus k_1(j)$
       Among the remaining pairs discard the ones such that $S\left(P(j) \oplus K_1(j) \oplus RC_1(j)\right) \oplus S\left(C(j) \oplus K_1'(j) \oplus RC_{2R}(j)\right) \neq \Delta^*(j)$.
     - 1.2.2 Count the number of remaining pairs.
       Store this number to a counter indexed by $(K_0||K_1)$.
2. Keep a list of $(K_0||K_1)$ ordered according to the counter values with the highest value on top. Compute the corresponding keys k_0 from K_0 according to the key expansion. Also compute $k_1(j)$ for $j \notin L$.
3. For the $2^{2n-4\ell-a}$ top candidates of k_0 on the list and the $2^{4\ell}$ remaining bits of k_1, do an exhaustive search to find the whole key $(k_0||k_1)$.

For each j in Step 1.1, only 4 bits out of $2^{4\ell}$ of key K_0 are involved. The first time we do this loop, we have to check the equality of 2^m plaintexts, among which 2^{m-4} pairs are expected to remain. After z iterations of the loop in Step 1.1, for each $4z-4$ key bits guessed in the previous steps and the 4 key bits of the current iteration, we should guess a nibble of the key and check the property for all remaining $2^{m-4(z-1)}$ plaintext-ciphertext pairs. The time complexity of Step 1.1 is $\sum_{z=1}^{\ell} 2^{m-4z+4} \cdot 2^{4z} = \ell \cdot 2^{m+4}$ simple operations.

Using the same arguments, Step 1.2 is iterated $2^{4\ell} \sum_{z=\ell+1}^{n/4} 2^{m-4z+4} \cdot 2^{8(z-\ell)} = 2^{m-4\ell+4} \sum_{z=\ell+1}^{n/4} 2^{4z} \simeq 2^{m+n+4-4\ell} = 2^{m+4\omega(\Delta^*)+4}$ times. If we denote $\omega = w(\Delta^*)$, the total time complexity of Step 1 corresponds to $2^{m+4\omega+4}$ double S-box evaluations, which is equivalent to $\frac{2^{m+5+4\omega}}{(n/4)\cdot(2R)} = \frac{2^{m+6+4\omega}}{n \cdot R}$ full encryptions.

Step 3 corresponds to 2^{2n-a} full encryptions, where $0 \leq a \leq 2n - 4\ell$. Step 2, is negligible compared to Step 1 and 3 and the total complexity of the algorithm is $2^{2n-a} + \frac{1}{n \cdot R} \times 2^{m+6+4w(\Delta^*)}$ full encryptions. When the advantage is large, the second term dominates.

To perform the described attack, storage of the 2^m plaintext-ciphertext pairs is necessary, as well as storage of all the 2^{2n-l} counters, one per guessed key. Nevertheless, the memory complexity can be reduced by keeping only keys for which the number of remaining pairs is above some fixed bound.

4.2 Impossible Reflection Setting

In this attack we make use of $\mathcal{I}_2$ and assume that the parameter α is such that $\mathcal{I}_2$ holds with probability equal to zero. Then a deterministic reflection distinguisher with probability equal to one can be built. A guessed key can be discarded if it gives a data pair such that the difference is equal to α.

Key Recovery for $2R = 2i + 2$ Rounds. In the case of $\mathcal{I}_2$ we have $i = 2$, but the attack works for any i, if an impossible characteristic over $2i$ rounds can be built. To reduce the time complexity, we precompute certain values from the states of the second round and the second to last round of the cipher. We denote by $P' = P \oplus k_0$ and $C' = C \oplus k'_0$ the states after modification of the plaintext and ciphertext by the whitening keys. For all $0 \leq b \leq 2^n - 1$, we denote by (V_b, W_b) the following values:

$$\begin{aligned} V_b &= S^{-1}(b) \oplus RC_1, \\ W_b &= S^{-1}(b \oplus M^{-1}(\alpha)) \oplus RC_{2R}. \end{aligned} \tag{7}$$

Then, as depicted in Fig. 4, the following properties hold for the pairs (P', C') and the corresponding (V_b, W_b):

$$\begin{aligned} P' \oplus V_b &= k_1, \\ P' \oplus C' &= V_b \oplus W_b. \end{aligned}$$

Assume again we have 2^m known pairs (P, C) of plaintexts with corresponding ciphertexts. The goal is to find for as many key candidates k_1 as possible a (P', C') such that $(P' \oplus k_1, C' \oplus k_1)$ is equal to some pair (V_b, W_b). Then we can conclude that the key k_1 is a wrong key and discard it. After pre-computation, the attack works as follows.

Attack Procedure when (k_0, k'_0) is known

1. Consider a list of all keys k_1.
2. For each 2^m pairs (P', C')
   Compute $\Lambda = P' \oplus C'$.
   For all V_b in the row Λ in the hash table T compute the value $k_1 = P' \oplus V_b$ and discard it from the list.

3. If there is still a key in the list of key k_1, consider $k = (k_0||k_1)$ as a key candidate.

On average, there is one V_b in each row of T. So by using 2^m known plaintexts and by considering the collisions, the number of remaining wrong keys k_1 is about $2^n(1-2^{-n})^{2^m} = 2^n(1-2^{-n})^{2^n 2^{m-n}} \approx 2^n e^{-2^{m-n}} = 2^{n-1.44\times 2^{m-n}}$, for each fixed k_0. The remaining keys are then searched exhaustively.

The impossible characteristic $\mathcal{I}_2$ holds for the involution matrix M', the non-linear layer S and the reflection parameter value α specified for the original PRINCE. In Sect. 5.4, many more such values of α are shown to exist. For all these α, by using the full codebook, the right key can be found after $2^{126.56}$ encryptions. In total 2^{67} bytes are necessary for the storage of the hash table. Considering only PRINCE$_{core}$, using the full codebook, the right key k_1 can be found after $2^{62.56}$ encryptions.

5 Various Classes of α-Reflection

In [2], the security of PRINCE and the effects of the α-reflection were studied extensively. In particular, it was shown that the cipher is secure against known attacks with reasonable security margin. For instance, it was shown that any differential or linear characteristic over 4 consecutive rounds has at least 16 active Sboxes. This holds independently of the selection of the non-zero parameter α.

In this section, we focus on a sub-family of PRINCE-like ciphers using the same S-layer and the same linear layers M and M' as in the original PRINCE. Definition of these components as given in [2] are recalled in Sect. A.1. We compute the probabilities $\mathcal{P}_{\mathcal{I}_1}$, $\mathcal{P}_{\mathcal{I}_2}$, and $\mathcal{P}_{\mathcal{C}_u}$ $(1 \leq u \leq 4)$ of the distinguishers proposed in Sect. 3, for various classes of values of α. Then we use these distinguishers for key-recovery attacks on PRINCE presented in Sect. 4, determine the maximum number of rounds that can be attacked, and give complexities of these attacks. The key-recovery attacks in Sect. 4, can be modified to apply on PRINCE$_{core}$, in which case their complexities will be reduced. We will give these complexities for comparison, but omit the descriptions of the actual attacks on PRINCE$_{core}$ due to lack of space.

5.1 Probability of the Characteristics: Computation

The difference between $\mathcal{I}_1$ and $\mathcal{I}_2$ is noticeable, since the probability of the former is independent of the value of α, which is not the case for $\mathcal{I}_2$ on the 4 midmost rounds. Next we describe how to compute the probability of these characteristics for PRINCE.

Characteristic $\mathcal{I}_1$. The involution matrix M' of the original PRINCE is such that $|F'_M| = 2^{32}$. The probability of the characteristic $\mathcal{I}_1$ is then $\mathcal{P}_{\mathcal{I}_1} = \frac{2^{32}}{2^{64}} = 2^{-32}$.

Characteristic $\mathcal{I}_2$. As M' is a block-diagonal matrix constructed from the 16×16 matrices $\hat{M}_0$ and $\hat{M}_1$, probability $\mathcal{P}_{\mathcal{I}_2}$ can be computed exactly by computing the following probabilities:

$$\mathcal{P}^{(\beta)}_{\hat{M}_0} = 2^{-16} \# \left\{ x \in \mathbb{F}_2^{16} | S^{-1}\left(\hat{M}_0\big(S(x)\big)\right) \oplus x = \beta \right\}$$
$$\mathcal{P}^{(\beta)}_{\hat{M}_1} = 2^{-16} \# \left\{ x \in \mathbb{F}_2^{16} | S^{-1}\left(\hat{M}_1\big(S(x)\big)\right) \oplus x = \beta \right\}$$

where β is a 16-bits word and S is the application of 4 Sboxes. Then if $\alpha = (\alpha_0, \alpha_1, \alpha_2, \alpha_3)$, we have

$$\mathcal{P}_{\mathcal{I}_2} = \mathcal{P}^{(\alpha_0)}_{\hat{M}_0} \times \mathcal{P}^{(\alpha_1)}_{\hat{M}_1} \times \mathcal{P}^{(\alpha_2)}_{\hat{M}_1} \times \mathcal{P}^{(\alpha_3)}_{\hat{M}_0}. \tag{8}$$

Characteristic $\mathcal{C}_u$. As presented in Sect. 3.2, characteristics on the external rounds can be seen as a differential characteristics with input difference α and related constant difference α, see Fig. 3. As PRINCE is a 64-bit cipher with 12 rounds, only 3 or 4 external rounds must be considered, and therefore computation of the best characteristics for a fixed α is possible by the Branch and Bound algorithm. Finding the weakest α for such a characteristic remains nevertheless a challenging task. When aiming at a combination with $\mathcal{I}_2$, focusing on the best α for $\mathcal{I}_2$ gives a good starting point, whereas $\mathcal{I}_1$ is independent of α, a more complex analysis should be done to find the values of α for which an attack on the full 12 rounds of PRINCE$_{core}$ is possible.

5.2 Maximizing $\mathcal{P}_{\mathcal{C}_u}$ for Combination of $\mathcal{C}_u$ with $\mathcal{I}_1$

We describe here the method we use to derive the α for which 12 rounds of the cipher can be attacked using a combination of $\mathcal{I}_1$ and $\mathcal{C}_4$. As we have seen in Sect. 4, a key-recovery attack on 12 rounds can be derived using a distinguisher on 10 rounds. Hence we are interested in finding values of α which maximize $\mathcal{P}_{\mathcal{C}_4}$.

Maximizing $\mathcal{P}_{\mathcal{C}_4}$. We start by the analysis of the properties of the S-box and permutation layer M of PRINCE. Indeed, the values of α for which a minimal number of Sboxes are active (that is, have non-zero differences) at each round and the differential probabilities of the Sbox are maximal. To this aim, we first express some properties of the matrices $\hat{M}_0$ and $\hat{M}_1$.

To maximize $\mathcal{P}_{\mathcal{C}_u}$, we want to minimize the weight of $\alpha = (\alpha_0, \alpha_1, \alpha_2, \alpha_3)$ and $M^{-1}(\alpha)$. Since $\hat{M}_\epsilon$, $\epsilon = 0, 1$, have a branch number 4, $w(\beta) + w(\hat{M}_\epsilon(\beta)) \geq 4$ and we have only 61 out of the total of 2^{16} values β such that $w(\beta) + w(\hat{M}_\epsilon(\beta)) = 4$ for both $\epsilon = 1$ and $\epsilon = 2$. Among these 61 values, 57 are such that $\beta = (a_1, a_2, a_3, a_4)$, where $a_i \in \{0, 1, 2, 4, 8\}$. Differential probabilities of the inverse Sbox for single-bit differences are given in Table 1. Based on this table and experiments, we assume that α with some nibble equal to 2 is not likely to maximize $\mathcal{P}_{\mathcal{C}_4}$. To find the best distinguisher on 10 rounds, we reduce the search space of α using

Table 1. Differential probabilities of the inverse Sbox for single-bit differences.

$a\backslash b$	1	2	4	8
1	2^{-2}	2^{-3}	2^{-3}	0
2	0	0	2^{-3}	2^{-3}
4	2^{-3}	0	2^{-3}	2^{-2}
8	2^{-2}	2^{-3}	2^{-3}	2^{-3}

the following procedure: For $\alpha = (a_1, a_2, \cdots, a_{15}, a_{16})$, where $a_i \in \{0, 1, 4, 8\}$ (2^{32} values), we select the ones such that there exists a characteristic $\mathcal{C}_2$ with $\mathcal{P}_{\mathcal{C}_2} \geq 2^{-12}$ (there are more than 300 values of α of this sort). Among the remaining ones, check if there is a characteristic $\mathcal{C}_4$ with $\mathcal{P}_{\mathcal{C}_4} \geq 2^{-28}$.

In Tables 2 and 3, we present some values of α, for which we obtain a distinguisher on 10 rounds. Estimated time and data complexities of a key recovery attack on the 12-round cipher are also shown in the same tables. These estimates have been computed under the assumption that the right key maximizes the number of remaining pairs in Step 4 of the key recovery attack, meaning that the advantage is $a = n + 4w(\Delta^*)$. The success probability is taken equal to 95 %. The data complexity is derived using Algorithm 1 of [1] and the time complexity is derived as for the key recovery attack presented in Sect. 4.1.

Iterative Characteristic. For the α in Table 2, which maximize the probability $\mathcal{P}_{\mathcal{C}_4} \times \mathcal{P}_{\mathcal{I}_1}$, the characteristic $\mathcal{C}_4$ is particular since a cancellation of the difference occurs every second round. For instance, we can have $Y^O_{R+1} \oplus X^I_R = \alpha$, $Y^O_{R+2} \oplus X^I_{R-1} = 0$, $Y^O_{R+3} \oplus X^I_{R-2} = \alpha$, $Y^O_{R+4} \oplus X^I_{R-3} = 0$, and $Y^O_{R+5} \oplus X^I_{R-4} = \alpha$. Then every second folded round can be passed with probability one, and it can be applied iteratively to minimize the probability of the characteristic. Such characteristic are easily found even by hand. We just look for α such that α and $M^{-1}(\alpha)$ are non-zero on exactly the same nibble position. Such a cancellation property occurs for some particular values of α. When $w(\alpha) = 4$, the cancellation property leads to an attack on 12 rounds of the cipher. No α with less than 4

Table 2. The weakest α with attack on 12 rounds (using $C_4 \circ \mathcal{I}_1$). Iterative characteristic based on the cancellation idea.

α	Δ^*	$w(\Delta^*)$	$\mathcal{P}_{\mathcal{C}_4}$	PRINCE$_{core}$	PRINCE	
				Data/Time	Data	Time
8400400800000000	8800400400000000	4	2^{-22}	$2^{56.21}$	$2^{57.98}$	$2^{72.39}$
8040000040800000	8080000040400000	4	2^{-22}	$2^{56.21}$	$2^{57.98}$	$2^{72.39}$
0000408000008040	0000404000008080	4	2^{-22}	$2^{56.21}$	$2^{57.98}$	$2^{72.39}$
0000000048008004	0000000044008008	4	2^{-22}	$2^{56.21}$	$2^{57.98}$	$2^{72.39}$
0000440040040000	0000440040040000	4	2^{-24}	$2^{58.72}$	$2^{60.28}$	$2^{74.69}$
8008000000008800	8008000000008800	4	2^{-24}	$2^{58.72}$	$2^{60.28}$	$2^{74.69}$

Table 3. Example of α with attack on 12 rounds (using $C_4 \circ \mathcal{I}_1$).

α	Δ^*	$w(\Delta^*)$	$\mathcal{P}_{\mathcal{C}_4}$	PRINCE$_{core}$	PRINCE	
				Data/Time	Data	Time
0108088088010018	0000001008000495	5	2^{-26}	$2^{61.22}$	$2^{62.80}$	$2^{79.21}$
0088188080018010	00000100C09D0008	5	2^{-26}	$2^{61.22}$	$2^{62.80}$	$2^{79.21}$
0108088088010018	000000100800D8CC	6	2^{-26}	$2^{61.42}$	$2^{62.86}$	$2^{83.27}$
0001111011010011	1101100110000100	7	2^{-28}	$2^{63.57(\dagger)}$	$2^{63.57(\dagger)}$	2^{112}

†: complexities computed for an advantage of $a = 16$ bits.

active nibbles or with $w(\alpha) = 5$ can satisfy the cancellation property. Nevertheless some α with 6 active nibbles have characteristic which cancel the difference after two rounds. As for these α, $Y^O_{R+3} \oplus X^I_{R-2} = \alpha$ with probability $\mathcal{P}_{\mathcal{C}_2} \leq 2^{-16}$, the iterative characteristic $\mathcal{C}_u$ can be applied only once and a distinguisher on 6 rounds with probability p, where $2^{-49} \leq p \leq 2^{-48}$, leads to a key-recovery attack on 8 rounds.

Non-Iterative Characteristic. In Table 3, we give other values of α, which allow an attack on 12 rounds. While the list is not exhaustive, this table illustrates that also α with larger weight can lead to an attack on 12 rounds. Different characteristic for the same α can be derived. While the weight of Δ^* is larger for these characteristics, the time complexity of this attack is still reasonable. While the list of α with a key recovery attack on 12 rounds is already quite large, the number of α such that attacks on 6, 8, or 10 rounds are possible is even larger. Search for α of this sort can be done by adjusting the constraint of the Branch and Bound algorithm.

5.3 Maximizing $\mathcal{P}_{\mathcal{I}_2}$ for Combination with $\mathcal{C}_u$

Finding the values of α which maximize $\mathcal{P}_{\mathcal{I}_2}$ can be done exhaustively by decomposing over the matrices $\hat{M}_\epsilon$, $\epsilon = 0, 1$, see Sect. 5.1. Computation for 2^{16} values of β gives us the list of best α regarding to this characteristic. In what follows, we focus on $\beta \neq 0$ such that $2^{-12} \leq \mathcal{P}^{(\beta)}_{\hat{M}_\epsilon} \leq 2^{-10.54}$. As $\mathcal{P}^0_{\hat{M}_\epsilon} \leq 2^{-8}$, we obtain a list of $63^2 \times 73^2 \approx 2^{24.33}$ values of α for which $2^{-48} \leq \mathcal{P}_{\mathcal{C}_2} \leq 2^{-34.54}$. Two values of α reach this upper bound. They are $\alpha =$ 0000111100000000 and $\alpha =$ 0000000011110000.

The values α which maximize $\mathcal{I}_2$ and for which 10 rounds of a PRINCE-like cipher can be distinguished from random also allow a combination of $\mathcal{C}_4$ and $\mathcal{I}_1$. For instance, for $\alpha =$ 0000408000008040 we have a characteristic with $\mathcal{P}_{\mathcal{C}_3} = 2^{-19}$ and $\mathcal{P}_{\mathcal{I}_2} = 2^{-40}$. None of these characteristics give a better cryptanalysis results than the ones given in Table 2. While for the attacks on 12 rounds all values of α are such that $w(\alpha) \geq 4$, we can find α of smaller nibble weight which

Table 4. Example of α with attack on 10 rounds and $w(\alpha) = 2$ (using $C_2 \circ \mathcal{I}_2$). Computation done for $P_S = 95\,\%$ and $a = 16$.

α	Δ^*	$w(\Delta^*)$	$\mathcal{P}_{\mathcal{C}_2}$	$\mathcal{P}_{\mathcal{I}_2}$	PRINCE$_{core}$ Data/Time	PRINCE Data	PRINCE Time
0000000001100000	1000111011011101	10	2^{-20}	2^{-36}	$2^{58.17}$	$2^{58.17}$	2^{112}
0000000008040000	9189505500008991	11	2^{-24}	2^{-36}	$2^{63.57}$	$2^{63.57}$	2^{112}
0000000000000804	4C0C18998C0C0000	10	2^{-24}	2^{-36}	$2^{63.57}$	$2^{63.57}$	2^{112}

allow a key recovery attack on a 10-round cipher using a combination of $\mathcal{C}_2$ and $\mathcal{I}_2$ as illustrated in Table 4.

For all the α presented in this section, also other characteristics can be derived. Complexities of our attacks are based on the best characteristic.

5.4 Impossible Attack

If $\mathcal{P}_{\mathcal{I}_2} = 0$, a deterministic distinguisher on 4 rounds of the cipher can be built. It leads to a key-recovery attack for a 6-round cipher described in Sect. 4.2. The time complexity of this attack correspond to $2^{126.56}$ encryptions and 2^{67} bytes are necessary for the storage of the hash table. This attack is efficient, in particular, for $\alpha =$ C0AC29b7C97C50DD of PRINCE. But we can find many more values of α with $\mathcal{P}_{\mathcal{I}_2} = 0$.

As specified by Eq. (8), the computation of $\mathcal{P}_{\mathcal{C}_2}$ can be decomposed over $\hat{M}_0$ and $\hat{M}_1$. For $\hat{M}_0$, the number of $\beta \in \mathbb{F}_2^{16}$ for which $\mathcal{P}_{\hat{M}_0}^{(\beta)} = 0$ is 5940. For $\hat{M}_1$, the number of β for which $\mathcal{P}_{\hat{M}_1}^{(\beta)} = 0$ is 6914. In total, we deduce that the impossible distinguisher is valid for approximately $2 \cdot (2^{12.54}) \times 2^{48} + 2 \cdot (2^{12.76}) \times 2^{48} = 2^{62.65}$ values of α.

Using the fact that $\hat{M}_0$ and $\hat{M}_1$ have no fixed points of weight 1, we conclude that $\mathcal{P}_{\mathcal{C}_2} = 0$, for all α with only 1 or 3 non-zero nibbles. Also a large number of α with 2, 4 and 5 non-zero nibbles allow this impossible distinguisher. We also found that for some α with 4 active nibbles we have an attack on 12 rounds, while for some other α the best attack we found is on 6 rounds only. Hence the weight of α alone does not prove anything about security or insecurity against the reflection attacks discussed in this paper.

5.5 Truncated Attack

When the linear layer is defined as in the original proposal, using the shift row operation of the AES, truncated reflection distinguishers can be derived for α such that $M^{-1}(\alpha)$ has a small number of active nibbles. Proof of the characteristic presented below can be found in Appendix A.2.

Lemma 2. *Assume* α *is such that* $M^{-1}(\alpha) = \begin{bmatrix} * & 0 & 0 & 0 \\ 0 & 0 & 0 & * \\ 0 & 0 & * & 0 \\ 0 & * & 0 & 0 \end{bmatrix}$, *where* $*$ *can be any 4-bit value. Then the following truncated characteristic*

$$Y^O_{R+3} \oplus X^I_{R-2} = \begin{bmatrix} * & 0 & 0 & 0 \\ * & 0 & 0 & * \\ * & 0 & * & 0 \\ * & * & 0 & 0 \end{bmatrix} \oplus \alpha, \tag{9}$$

holds on 6 rounds $\mathfrak{R}_{R-2} \circ \cdots \circ \mathfrak{R}_{R+3}$ *of the cipher with probability* $\mathcal{P}_{F_{M'}} = 2^{-32}$. *Similar characteristics can be obtained for* α *such that:*

$$M^{-1}(\alpha) = \begin{bmatrix} 0 & * & 0 & 0 \\ * & 0 & 0 & 0 \\ 0 & 0 & 0 & * \\ 0 & 0 & * & 0 \end{bmatrix} \quad or \quad M^{-1}(\alpha) = \begin{bmatrix} 0 & 0 & * & 0 \\ 0 & * & 0 & 0 \\ * & 0 & 0 & 0 \\ 0 & 0 & 0 & * \end{bmatrix} \quad or \quad M^{-1}(\alpha) = \begin{bmatrix} 0 & 0 & 0 & * \\ 0 & 0 & * & 0 \\ 0 & * & 0 & 0 \\ * & 0 & 0 & 0 \end{bmatrix}.$$

In all four cases of the characteristics, nine nibbles of the data difference are equal to those of α. Hence the probability of such a truncated characteristic is 2^{-36}.

By the previous lemma, such truncated characteristics exist for $4 \times (2^{16} - 1) \approx 2^{18}$ values of α. While distinguisher of Sects. 5.2 and 5.3 focused on α with a small number of active nibbles, this distinguisher is targeted on α, for which $M^{-1}(\alpha)$ has a small number of active nibbles, but α itself can have any number of non-zero nibbles. As an example, we give

$$\alpha = \begin{bmatrix} 7 & 1 & C & B \\ 9 & 5 & 9 & 3 \\ 9 & A & 5 & 9 \\ 3 & 6 & 8 & D \end{bmatrix}, \quad M^{-1}(\alpha) = \begin{bmatrix} 7 & 0 & 0 & 0 \\ 0 & 0 & 0 & B \\ 0 & 0 & D & 0 \\ 0 & 9 & 0 & 0 \end{bmatrix}.$$

This truncated distinguisher enables a key-recovery attack for a cipher reduced to eight rounds in the same way that the key recovery attack described in Sect. 4. The keys k_0 and k_1 can then be recovered independently. In Appendix A.2 details of this key recovery attack are explained. This key recovery attack has data complexity $2^{36.85}$, time complexity of $2^{97.8}$ memory accesses and 2^{80} full encryptions. The memory complexity is dominated by the storage of $2^{63.6}$ bytes for the hash table.

Several other kinds of truncated reflection characteristics can be derived for different configuration of $M^{-1}(\alpha)$. For instance, in some configurations, where $M^{-1}(\alpha)$ has up to eight non-zero nibbles a key-recovery attack on a 6-round cipher can be done using a distinguisher on 4 rounds.

6 Conclusion

In this paper, we investigated the security of a family of ciphers, which includes the new design PRINCE. This family is characterized by the α-reflection property. We constructed new types of characteristics for such ciphers starting from

a probabilistic or impossible relation on the midmost rounds of the cipher. By using properties of the constant α and the symmetry of the cipher, such reflection characteristics can be considered as differential characteristics over a half of the cipher, and in particular, their probabilities can be computed efficiently using ordinary differential probabilities over the non-linear components of the cipher. In the security analysis of PRINCE given in [2] the properties of α did not receive much attention. In this paper, we show that the security of PRINCE-like ciphers depends strongly on the choice of the value of α. By keeping the other components of PRINCE as in the original design, and by varying the value of α, we identified special classes of α for which reduced-round versions of the cipher can be distinguished from random. The values of α in the weakest class allow an efficient key-recovery attack on 12 rounds of the cipher. These results show that the security of PRINCE is not independent of the value of α. On the other hand, the best attack we could construct using this technique on PRINCE with the original value of the reflection parameter α, was a key recovery attack on a reduced 6-round version of the cipher. While the new technique, which exploits the special reflection structure of the cipher, did not reveal any vulnerabilities in the original design, it provided new information about the security criteria for the selection of the reflection parameter as well as other componenets of the cipher.

Acknowledgments. We wish to thank the anonymous reviewers for helpful comments. The authors from Aalto University wish to acknowledge useful discussions with Gregor Leander during his visits funded by the Aalto Science Institute. The work of Hadi Soleimany is supported by Helsinki Doctoral Program in Computer Science - Advanced Computing and Intelligent Systems (HECSE). The work of Hadi Soleimany and Céline Blondeau is partly supported by European Commission through the ICT program under contract ICT-2007-216676 ECRYPT II. The work of Xiaoli Yu, Wenling Wu, Huiling Zhang, Lei Zhang and Yanfeng Wang is partly supported by the National Basic Research Program of China (No. 2013CB338002) and the National Natural Science Foundation of China (No. 61272476, 61232009, 61202420).

A Appendix

A.1 Components of PRINCE

The linear layer of PRINCE is defined using four 4×4 matrices M_0, M_1, M_2, M_3 given as follows:

$$M_0 = \begin{pmatrix} 0\,0\,0\,0 \\ 0\,1\,0\,0 \\ 0\,0\,1\,0 \\ 0\,0\,0\,1 \end{pmatrix}, \quad M_1 = \begin{pmatrix} 1\,0\,0\,0 \\ 0\,0\,0\,0 \\ 0\,0\,1\,0 \\ 0\,0\,0\,1 \end{pmatrix}, \quad M_2 = \begin{pmatrix} 1\,0\,0\,0 \\ 0\,1\,0\,0 \\ 0\,0\,0\,0 \\ 0\,0\,0\,1 \end{pmatrix}, \quad M_3 = \begin{pmatrix} 1\,0\,0\,0 \\ 0\,1\,0\,0 \\ 0\,0\,1\,0 \\ 0\,0\,0\,0 \end{pmatrix}.$$

Then the two 16×16 matrices $\hat{M}_0$ and $\hat{M}_1$ are defined as:

$$\hat{M}_0 = \begin{pmatrix} M_0 & M_1 & M_2 & M_3 \\ M_1 & M_2 & M_3 & M_0 \\ M_2 & M_3 & M_0 & M_1 \\ M_3 & M_0 & M_1 & M_2 \end{pmatrix}, \quad \hat{M}_1 = \begin{pmatrix} M_1 & M_2 & M_3 & M_0 \\ M_2 & M_3 & M_0 & M_1 \\ M_3 & M_0 & M_1 & M_2 \\ M_0 & M_1 & M_2 & M_3 \end{pmatrix}.$$

The non-linear layer S consists of 16 copies of a 4-to-4-bit Sbox given in Table 5.

Table 5. Sbox of PRINCE

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

A.2 Truncated Reflection Characteristic

Proof of Lemma 2. The 4 types of truncated characteristics given in Lemma 2 differ only by the position of the completely undetermined column of the difference. We present here the proof for the first column. Proofs for the other types are similar.

As described by the characteristic $\mathcal{C}_1$, the probability that $X_R^I \oplus Y_{R+1}^O = \alpha$ is equal to $P_{F_{M'}}$ ($= 2^{-32}$ for PRINCE). For the previous and the next round, we have

$$Y_{R+2}^O \oplus X_{R-1}^I = S^{-1}\left(M^{-1}(\alpha)\right) \oplus \alpha = \begin{bmatrix} * & 0 & 0 & 0 \\ 0 & 0 & 0 & * \\ 0 & 0 & * & 0 \\ 0 & * & 0 & 0 \end{bmatrix} \oplus \alpha.$$

Since $M^{-1} = M' \circ SR^{-1}$ is linear and

$$M^{-1}\left(\begin{bmatrix} * & 0 & 0 & 0 \\ 0 & 0 & 0 & * \\ 0 & 0 & * & 0 \\ 0 & * & 0 & 0 \end{bmatrix}\right) = \begin{bmatrix} * & 0 & 0 & 0 \\ * & 0 & 0 & 0 \\ * & 0 & 0 & 0 \\ * & 0 & 0 & 0 \end{bmatrix},$$

we have

$$Y_{R+3}^O \oplus X_{R-2}^I = S^{-1}\Big(M^{-1}(\alpha) \oplus \begin{bmatrix} * & 0 & 0 & 0 \\ * & 0 & 0 & 0 \\ * & 0 & 0 & 0 \\ * & 0 & 0 & 0 \end{bmatrix}\Big) \oplus \alpha = \begin{bmatrix} * & 0 & 0 & 0 \\ * & 0 & 0 & * \\ * & 0 & * & 0 \\ * & * & 0 & 0 \end{bmatrix} \oplus \alpha.$$

Key Recovery Attack. For simplicity, we restrict to the characteristic given by Eq. (9). As this characteristic is completely undetermined in the first column, and will stay completely undetermined in the same column after application of the inverse of shift row, it is sufficient to focus on the 12 nibbles corresponding

to the three most right columns of the matrix of (9). For a state Z, we denote the truncation of the state to the last three columns by Z_t. Let (P, C) be a plaintext-ciphertext pair. The distinguisher involves only partial encryption of 48 bits of the plaintext P_t and partial decryption of the ciphertext C_t with the key k_0, k_0' and k_1. It means that only up to 49 bits of k_0 and 48 bits of k_1 can be obtained in a similar way to the attack of Sect. 4. An exhaustive search on the remaining bits is then necessary to recover the full key.

The attack procedure is as follows:

Pre-computation

For each possible 2^{60} pairs $(a, b) \in (\mathbb{F}_2^{48})^2$ such that $a \oplus b$ is equal to the truncated state of $\begin{bmatrix} * & 0 & 0 & 0 \\ * & 0 & 0 & * \\ * & 0 & * & 0 \\ * & * & 0 & 0 \end{bmatrix} \oplus \alpha$ compute the pair $(\nu_a, \omega_b) \in (\mathbb{F}_2^{48})^2$ such that

$$\nu_a = S^{-1}\big(M^{-1}(a)\big) \oplus RC_1,$$
$$\omega_b = S^{-1}\big(M^{-1}(b)\big) \oplus RC_8.$$

Store ν_a in the row $\Lambda = \nu_a \oplus \omega_b$ of the hash table T. The hash table T has 2^{48} rows and on average each row have $\frac{2^{60}}{2^{48}} = 2^{12}$ values.

Attack Procedure

1. Guess 49 bits of the key k_0 and extract 48 bits of k_0 and of k_0'.
   (i) Allocate a counter D_{k_1} for each 2^{48} values of k_1.
   (ii) For each 2^m pairs $(P_t', C_t') = (P_t \oplus k_0, C_t \oplus k_0')$
   Compute $\Lambda = P_t' \oplus C_t'$.
   For all ν_a in the row Λ of the hash table T increase the counter $D_{(P_t' \oplus \nu_a)}$ by one.
   (iii) Consider a list of 2^{48-a} of the keys k_1 with highest counter values.
2. Do an exhaustive search on the remaining $128 - a$ bits of key.

The time complexity of the attack without whitening keys (Steps (i) to (iii)) corresponds to 2^{m+12} memory accesses. To obtain k_0, the attack should be repeated for 2^{49} keys k_0. So the time complexity to find the whole key corresponds to 2^{61+m} memory accesses in addition to 2^{128-a} full encryptions. We need $2^{60} \times 48/8 \times 2 \simeq 2^{63.6}$ bytes for the storage of the hash table T and $2^{49+48-a} \times 48/8 = 2^{99.6-a}$ bytes for the storage of the list of keys candidates.

References

1. Blondeau, C., Gérard, B., Tillich, J.-P.: Accurate estimates of the data complexity and success probability for various cryptanalyses. Des. Codes Crypt. **59**(1–3), 3–34 (2011)
2. Borghoff, J., et al.: PRINCE – a low-latency block cipher for pervasive computing applications (extended abstract). In: Wang, X., Sako, K. (eds.) ASIACRYPT 2012. LNCS, vol. 7658, pp. 208–225. Springer, Heidelberg (2012)

3. Bouillaguet, C., Dunkelman, O., Leurent, G., Fouque, P.-A.: Another look at complementation properties. In: Hong, S., Iwata, T. (eds.) FSE 2010. LNCS, vol. 6147, pp. 347–364. Springer, Heidelberg (2010)
4. Flajolet, P., Sedgewick, R.: Analytic Combinatorics. Cambridge University Press, New York (2009)
5. Guo, J., Peyrin, T., Poschmann, A., Robshaw, M.: The LED block cipher. In: Preneel, B., Takagi, T. (eds.) CHES 2011. LNCS, vol. 6917, pp. 326–341. Springer, Heidelberg (2011)
6. Kara, O.: Reflection cryptanalysis of some ciphers. In: Chowdhury, D.R., Rijmen, V., Das, A. (eds.) INDOCRYPT 2008. LNCS, vol. 5365, pp. 294–307. Springer, Heidelberg (2008)
7. Knudsen, L., Leander, G., Poschmann, A., Robshaw, M.J.B.: PRINTcipher: a block cipher for IC-printing. In: Mangard, S., Standaert, F.-X. (eds.) CHES 2010. LNCS, vol. 6225, pp. 16–32. Springer, Heidelberg (2010)
8. Moore, J.H., Simmons, G.J.: Cycle structure of the DES with weak and semi-weak keys. In: Odlyzko, A.M. (ed.) CRYPTO 1986. LNCS, vol. 263, pp. 9–32. Springer, Heidelberg (1987)