J. Cryptol. (2015) 28: 718–744
DOI: 10.1007/s00145-013-9175-4

Journal of
CRYPTOLOGY

Reflection Cryptanalysis of PRINCE-Like Ciphers

Hadi Soleimany and Céline Blondeau

Department of Information and Computer Science, School of Science, Aalto University, Espoo, Finland
hadi.soleimany@aalto.fi; celine.blondeau@aalto.fi

Xiaoli Yu

TCA, Institute of Software, Chinese Academy of Sciences, Beijing, P.R. China
yuxiaoli@is.iscas.ac.cn
and
University of Chinese Academy of Sciences, Beijing, P.R. China

Wenling Wu

TCA, Institute of Software, Chinese Academy of Sciences, Beijing, P.R. China
wwl@is.iscas.ac.cn

Kaisa Nyberg

Department of Information and Computer Science, School of Science, Aalto University, Espoo, Finland
kaisa.nyberg@aalto.fi

Huiling Zhang, Lei Zhang, and Yanfeng Wang

TCA, Institute of Software, Chinese Academy of Sciences, Beijing, P.R. China

Communicated by Vincent Rijmen.

Received 27 April 2013
Online publication 13 December 2013

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 decryption with a given key to 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 distinguishers on PRINCE-like ciphers by constructing probable or impossible relations from the cipher data located at layers that are symmetric around the middle of the cipher. We show that the probabilities of such relations, called reflection characteristics in this paper, depend crucially on the choice of the reflection parameter α. Several classes of α are investigated. As a result we show that there exist values of α which, if used in the otherwise original PRINCE, would allow a key-recovery attack on the full 12-round cipher with the data complexity of $2^{57.98}$ known plaintexts and the time complexity of $2^{72.39}$ encryptions. While this attack is not better than the generic attack on the complete cipher, where the core cipher

is protected by the whitening key, the same reflection distinguisher, when applied on the core cipher without the whitening key, yields a key-recovery attack with time complexity less than exhaustive key search and data complexity of $2^{56.21}$ known plaintexts. 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.

Key words. Block cipher, α-Reflection property, PRINCE, Statistical attack, Reflection attack.

1. Introduction

Applications in special constrained environments such as RFID tags and sensors have recently received a lot of attention by the cryptographic community. The new secure primitives should provide the best possible security under tight constraints. Traditionally, cryptographic algorithms have been designed with large security margins to be on the secure side even when exposed to new and unknown vulnerabilities. Since lightweight ciphers must be optimized with respect to several performance criteria, such as chip size, power consumption, and energy efficiency, it is of utmost importance to analyze and quantify the cryptographic security of lightweight ciphers to reduce the superfluous security margins. New innovative and unconventional designs pose new challenges. For instance, new cipher proposals, such as PRINTcipher [24] and LED [18] with very simple key-schedule or even without key-schedule, have been developed to reduce the power consumption of the encryption algorithm. With the emergence of such constructions, new attacks have been developed.

PRINCE is a low-latency block cipher proposed at ASIACRYPT 2012 [7,8]. It is an iterated block cipher structured as a substitution-permutation network (SPN). PRINCE has a new, original feature called the α-reflection property that involves a specific fixed parameter α. Because of this property, decryption with round key K is identical to encryption with round key $K \oplus \alpha$, which significantly reduces the cost of implementation of decryption. The cipher has even number of rounds, say $2R$, and the round functions at round r and $2R - r + 1$, $r < R$, are selected to be the inverse of each other up to the round constant addition. Each round function is parameterized by a fixed round constant and a key, which are added to the round data by exclusive-or operation. The key is the same at all rounds. The round constants are selected 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 $2R - r + 1$, $r \leq R$.

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, and they have received due attention by the designers. Obviously, due to its similarity with the Even–Mansour construction [16], the cipher is vulnerable to a trivial related-key distinguishing attack. Although, it is not clear how to convert it to a key-recovery attack since the distinguisher holds for any numbers of rounds with probability one.

In the original proposal document, the security of PRINCE and the effects of the α-reflection were studied extensively and the cipher was shown to be secure against several known attacks with reasonable security margins. 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.

The purpose of this paper is to investigate the security of PRINCE against reflection attacks. Even if naturally suggested by the structure of the cipher, such attacks were not covered by the designers in the original proposal. The notion of reflection attack was coined by O. Kara, who presented a general framework of reflection attacks on iterated cryptographic functions [21]. The idea itself is much older and dates back to 1985, when D. Coppersmith explained the existence of short cycles in repeated encryptions with the DES using, in an alternating manner, the all-zero key and the all-one key [11]. According to Coppersmith, if a fixed point occurs at some point, the encryptions after the fixed point will revert the state back to the starting point. The idea was subsequently investigated in depth for weak and semi-weak keys of DES [26]. The contemporary reflection attacks apply this same idea, not to the full encryption function, but instead, to the round functions of an iterated cryptographic function. The recent works on generic cryptanalysis of Even–Mansour cipher also exploit the fact that distributions of differences between input and output are not completely random even for an ideal permutation [13,15]. Moreover, there is some similarity in the process of key search between the generic attack on Even–Mansour cipher and our key-recovery attacks developed in the concrete setting of PRINCE-like ciphers presented in [28] and this paper.

In contrast to the other previously known and widely exploited attacks, such as related-key attacks and slide attacks that exploit self-similarity properties of the encryption round functions (see [4] and [5] and applications for hash functions [9]), reflection attacks are based on similarities between the encryption and decryption round functions. Hence Feistel structures with involutory round functions are natural targets of reflection cryptanalysis and they have been studied extensively [14,19,21,22]. While reflection attacks are well known for Feistel ciphers, their applications on SPN ciphers cannot be found in the literature. To the best of our knowledge, the cryptanalysis of PRINCE presented in this paper is the first application of reflection cryptanalysis on SPN block ciphers.

The starting point of a reflection attack is a non-uniform distribution of fixed points on some layer of intermediate rounds of the iterated cipher. Then the fixed points are propagated backwards using decryption from this intermediate layer and, simultaneously, forwards using encryption. Due to the similarity of the corresponding encryption and decryption round functions, the endpoints resulting from this process are expected to have some relation with a biased distribution. Depending on the conditions that are imposed on the key-schedule by the similarity of encryption and decryption, the attack works for some class of weak keys, or even for all keys [21].

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, show how they can be used as distinguishers over PRINCE, and examine how 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 functions, the reflection parameter α and the fixed points of the middle linear layer.

In sharp contrast to differential and linear characteristics on PRINCE-like ciphers, the number of active Sboxes 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 12-round version of the cipher with less data complexity than the whole code book. We present a known-plaintext single-key attack with the data complexity of $2^{57.98}$ plaintexts and time complexity of $2^{72.39}$. This attack comes close but does not surpass the generic attack on the FX-construction of PRINCE. By applying the same reflection characteristic to the core of the cipher, without the whitening key, we give a key-recovery attack with time complexity less than exhaustive key search and data complexity of $2^{56.21}$ known plaintexts.

Since we developed our attack, other related cryptanalytic studies on PRINCE have appeared. In [1] a truncated attack on the original α was presented. We show the existence of a general truncated attack, which demonstrates that not only α with small number of active nibbles should be avoided when designing a PRINCE-like cipher but also other properties should be analyzed. Also related-key key-recovery attacks have appeared [20]. Note that while there exists a trivial related-key distinguisher on PRINCE, it cannot be used for key recovery as it holds with probability one independently of the number of rounds. In this paper we construct another non-trivial related-key distinguisher, which can be turned to a single-key distinguisher, if the attacker is given access to the decryption oracle. Based on this distinguisher we present a key-recovery attack over the 12-round core function of PRINCE for some specific choices of α.

The original α specified in [7] is not in the set of weak α found in this paper. 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 PRINCE-like ciphers. 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. In Sect. 6 we describe the truncated attacks and the related-key key-recovery attacks. To conclude in Sect. 7 we discuss restrictions made in this work and potential other directions for finding new and better reflection attacks.

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.

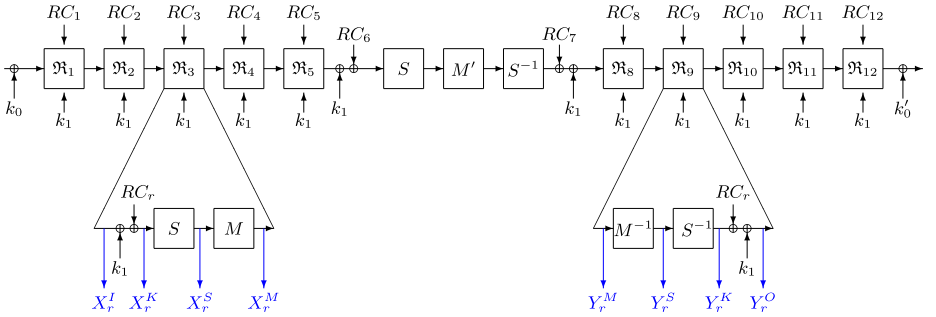


Fig. 1. Description of a $(2R = 12)$-round PRINCE-like cipher.

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 parameterized with a $2n$-bit key $k = (k_0 \parallel k_1) \in \mathbb{F}_2^{2n}$ 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

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

The keys k_0 and k_0' are used as pre- and post-whitening keys in the encryption operation that follows the FX-construction. The exclusive-or of the plaintext and k_0 is encrypted using the core function of the cipher under the key k_1, and to this result the key k_0' is added using the exclusive-or operation.

The core function of this cipher (denoted by $\text{PRINCE}_{\text{core}}$ in the original proposal) is defined as an iteration of the $2R$-round functions. The n-bit key k_1 is added to the state at each of the $2R$ rounds of the cipher. The building blocks of the round functions are a non-linear layer S 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 involutory matrix. The structure of the cipher is depicted in Fig. 1.

The descriptions of the first $R-1$ rounds $\mathfrak{R}_r : \mathbb{F}_2^n \to \mathbb{F}_2^n$, $1 \le r \le R-1$, are identical. Each of them is composed, in this order, of an 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 $\mathfrak{R}_r : \mathbb{F}_2^n \to \mathbb{F}_2^n$, $R+2 \le r \le 2R$ 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:

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

In what follows, these rounds with $r \le R-1$ or $r \ge R+2$ will be called the external rounds of the PRINCE-like cipher.

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

Table 1. Sbox of PRINCE.

x	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
Sbox(x)	B	F	3	2	A	C	9	1	6	7	8	0	E	5	D	4

all rounds.

$$\begin{aligned}
&\mathfrak{R}_r(x) = M\big(S(x \oplus RC_r \oplus k_1)\big) && \text{if } 1 \le r \le R-1,\\
&\mathfrak{R}_r(x) = M'\big(S(x \oplus RC_r \oplus k_1)\big) && \text{if } r = R,\\
&\mathfrak{R}_r(x) = S^{-1}(x) \oplus RC_r \oplus k_1 && \text{if } r = R+1,\\
&\mathfrak{R}_r(x) = S^{-1}\big(M^{-1}(x)\big) \oplus RC_r \oplus k_1 && \text{if } R+2 \le r \le 2R.
\end{aligned} \tag{3}$$

The PRINCE-like ciphers have the property that decryption can be obtained from encryption with a different key. If we denote by P a plaintext, the corresponding ciphertext is computed as $C = E_k^{\alpha}(P)$, where $k = (k_0 \parallel k_0' \parallel k_1)$. Then C can be decrypted by encrypting it using a related key as $P = E_{k'}^{\alpha}(C)$, where $k' = (k_0' \parallel k_0 \parallel k_1 \oplus \alpha)$.

2.2. *Description of PRINCE*

The full specification of PRINCE is given in [7]. It is a PRINCE-like cipher with $n = 64$ and $R = 6$. The reflection constant is set to $\alpha =$ C0AC29B7C97C50DD. Throughout this paper, we use the same convention as in the original proposal and use hexadecimal notation in typewriter type fonts to denote numerical values of bit strings. The nonlinear layer S consists of 16 copies of a 4-to-4-bit Sbox given in Table 1 and each nibble is processed by the same Sbox.

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

$$M_0 = \begin{bmatrix} 0&0&0&0\\ 0&1&0&0\\ 0&0&1&0\\ 0&0&0&1 \end{bmatrix}, \qquad M_1 = \begin{bmatrix} 1&0&0&0\\ 0&0&0&0\\ 0&0&1&0\\ 0&0&0&1 \end{bmatrix},$$

$$M_2 = \begin{bmatrix} 1&0&0&0\\ 0&1&0&0\\ 0&0&0&0\\ 0&0&0&1 \end{bmatrix}, \qquad M_3 = \begin{bmatrix} 1&0&0&0\\ 0&1&0&0\\ 0&0&1&0\\ 0&0&0&0 \end{bmatrix}.$$

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

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

Finally, a 64×64 block-diagonal and involutory matrix M' over $\mathbb{F}_2$ is generated by setting its diagonal equal to $(\hat{M}_0, \hat{M}_1, \hat{M}_1, \hat{M}_0)$. The second linear matrix M for

PRINCE is obtained by composition of M' and a permutation SR of nibbles, that is, $M = SR \circ M'$. The permutation SR is analogous to the shift row operation of the AES, but instead of bytes, it operates on nibbles.

The definition of the original round constants can be found in [7]. Exact values of the round constants are not relevant to the analysis presented in this paper. Only the α-reflection property (2) of the round constants will be exploited in the attacks discussed in this paper.

One of the goal of this paper is to study the effect of the value α on the security of this cipher. For clarification, we denote respectively by PRINCE^{α} and $\text{PRINCE}^{\alpha}_{\text{core}}$ the cipher and its core function when PRINCE is defined with a different but specific value α.

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 notation for describing these characteristics is 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, after the S-layer, and after the M-layer, respectively. In order to exploit the symmetry of the cipher, we give different definitions if $R + 1 \leq r \leq 2R$. 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, before the S-layer, and before the M-layer, respectively.

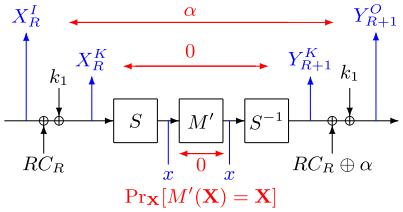
To build a distinguisher on a PRINCE-like cipher, we introduce two types of characteristics. First we focus on the middle rounds of the cipher which are different from the external ones. Characteristics on the middle rounds depend on the property of the matrix M'. Then by using a folded view of the cipher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

3.1. *Characteristics on the Middle Rounds*

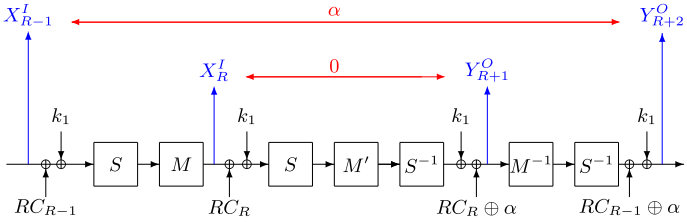
We identify two kinds of characteristics on 2 or 4 middle rounds of the cipher. The first characteristic on the 2 midmost rounds is independent of the reflection parameter. The second one is defined on 4 rounds and extends over one round before and one round after the midmost rounds. It behaves differently depending of the reflection parameter. The probability of each of these characteristics depends on 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 [7] it is stated based on the result of [17] 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 [17] holds in general, restricting to the case of linear involutions f over $\mathbb{F}_2$ gives the following result.



(a) $\mathcal{I}_1$



(b) $\mathcal{I}_2$

Fig. 2. Middle-round characteristics.

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 $\mathcal{I}_1$. Also the probability of the characteristic $\mathcal{I}_1$ is then $\mathcal{P}_{\mathcal{I}_1} = \frac{2^{32}}{2^{64}} = 2^{-32}$.

Characteristic $\mathcal{I}_2$ 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

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

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

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

The set under summation is non 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 the following equation

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

The expression on the right hand side can be efficiently evaluated as the summation is taken over the fixed points only.

As M' in PRINCE 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:

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

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

$$\mathcal{P}_{\mathcal{I}_2} = \mathcal{P}^{(\alpha_0)}_{\hat{M}_0} \times \mathcal{P}^{(\alpha_1)}_{\hat{M}_1} \times \mathcal{P}^{(\alpha_2)}_{\hat{M}_1} \times \mathcal{P}^{(\alpha_3)}_{\hat{M}_0}. \tag{4}$$

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

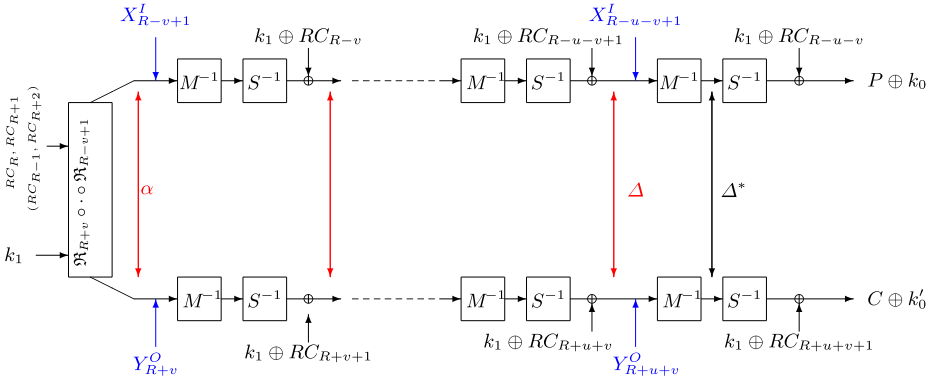


Fig. 3. A folded view of a PRINCE-like cipher: The external characteristic.

cipher connected together by $2v$ rounds. Then characteristics on $2u$ external rounds, $1 \le u \le R - v$, are built as ordinary related-key differential characteristics with an input data difference equal to α and a key difference or a round constant difference equal to α.

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

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

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

The probability of this characteristic can be computed using techniques similar to the ones used in classical differential cryptanalysis. In Sect. 5, two methods to compute the probability of such characteristics are described. For some reflection parameters α, an iterative characteristic on 4 rounds can be constructed by hand. For other values of α, an automatic search based on a Branch and Bound algorithm can be used for finding the best possible characteristics for different number of rounds.

In comparison with differential cryptanalysis, the characteristic $\mathcal{C}_u$ potentially 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 $2v + 2u$

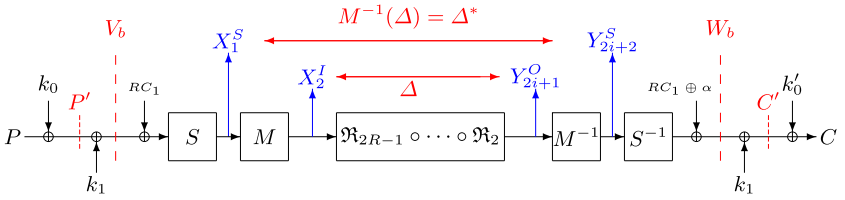


Fig. 4. Key-recovery principle when $2R = 2i + 2$.

rounds of the cipher are distinguishable from random. In Sect. 5 we identify classes of parameters α such that up to 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

$$Y_{R+i}^O \oplus X_{R-i+1}^I = \Delta, \tag{5}$$

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

$$Y_{R+2}^O \oplus X_{R-1}^I \neq \alpha, \tag{6}$$

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_2^I and Y_{2i+1}^O 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 [6]. Given the false alarm probability $p_{\text{fa}} = 2^{-a}$, the quantity a is called the advantage of the attack.

Key-Recovery Attack for $2R = 2i + 2$ Rounds Let us assume that a characteristic $Y_{2i+1}^O \oplus X_2^I = \Delta$ 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 $Y_{2i+2}^S \oplus X_1^S = M^{-1}(\Delta) = \Delta^*$ depicted in Fig. 4.

To find the values of X_1^S and Y_{2i+2}^S for all pairs (P, C), the whole key $(k_0 \parallel k_1)$ 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 jth 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^*.

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

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

We denote the number of nibbles of Δ^* that are equal to zero by $\ell = n/4 - w(\Delta^*)$ where $w(\Delta^*)$ is the number of non-zero nibble of Δ^*. 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
   $$\begin{aligned}S\big(P(j) \oplus K_1(j) \oplus RC_1(j)\big) \oplus S\big(C(j) \oplus K_1'(j) \oplus RC_{2R}(j)\big) \\ \neq \Delta^*(j).\end{aligned}$$
   1.2.2 Count the number of remaining pairs.
   Store this number to a counter indexed by $(K_0 \parallel K_1)$.
2. Keep a list of $(K_0 \parallel K_1)$ 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 $(k_0 \parallel k_1)$.

For each j in Step 1.1, only 4 bits out of $2^{4\ell}$ of key K_0 are involved. At the first iteration, 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

$$2^{4\ell} \sum_{z=\ell+1}^{n/4} 2^{m-4z+4} \cdot 2^{8(z-\ell)} = 2^{m-4\ell+4} \sum_{z=\ell+1}^{n/4} 2^{4z} \simeq 2^{m+n+4-4\ell} = 2^{m+4\omega+4}$$

times where $\omega = w(\Delta^*)$. 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 $1 \le a \le 2n-4\ell$. As Step 2 is negligible compared to Steps 1 and 3 the total complexity of key-recovery attack on $2R$ rounds corresponds to

$$2^{2n-a} + \frac{1}{nR} \cdot 2^{m+6+4w(\Delta^*)}$$

full encryptions. Note that when the advantage $1 \le a \le n+4w(\Delta^*)$ is large, the second term dominates.

To perform the described attack, the storage of the 2^m plaintext-ciphertext pairs is necessary, as well as the storage of all the $2^{n+4w(\Delta^*)}$ counters, one per each 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.

Generic Attack on PRINCE-Like Ciphers A PRINCE-like cipher is based on the generalized Even–Mansour or FX construction and does not provide the same security level than an ideal block cipher primitive with a $2n$-bit master-key [7,15,23]. Given 2^m pairs of plaintexts and corresponding ciphertexts, the time complexity of the generic attack of a PRINCE-like cipher corresponds to 2^{2n-m-2} encryptions as explained recently by the designers of PRINCE, e.g. in [25]. It means that for the original PRINCE, the correct number for the data and time complexity of the generic attack is 2^{126}. Due to the existence of the generic attack, it is very hard to build an efficient key-recovery attack on 12 rounds of the cipher even if for some α an efficient reflection distinguisher over 10 rounds could be found.

Therefore, to illustrate the effect of the non-randomness of the SPN primitive, we omit the pre- and post-whitenings and consider key-recovery attack on $\text{PRINCE}^{\alpha}_{\text{core}}$. $\text{PRINCE}^{\alpha}_{\text{core}}$ is parameterized with the n-bit key k_1 and hence all attacks with data complexity and time complexity less than 2^{n-1} can be considered better than any generic attack.

The key-recovery algorithm for this attack is similar to the previous one. If the number of active nibbles of Δ^* is small, a sieving process can be performed to discard

all plaintext-ciphertext pairs such that $P(j) \oplus C(j) \oplus \alpha(j) \neq 0$ for all $j \in L$. Using the previous notation and setting $K_0 = 0$, $K_1 = K_1' = k_1$, only about $2^{m-4\ell}$ pairs of plaintext-ciphertext will help us to determine $2^{4w(\Delta^*)}$ bits of k_1. Then as described in Step 1.2, we should nibble by nibble, for all $j \notin L$, guess the value of $k_1(j)$ and discard the pairs such that

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

These checks take

$$2 \cdot \sum_{z=\ell+1}^{n/4} 2^{m-4z+4} \cdot 2^{4z-4\ell-4} \cdot 2^4 = w \cdot 2^{m-4\ell+5}.$$

Sbox evaluations and 2^{n-a} full encryptions over $2R = 2i + 2$ rounds of $\text{PRINCE}_{\text{core}}^{\alpha}$. The time complexity of this attack corresponds to

$$\frac{1}{nR} \cdot 2^{m+6-n+4w(\Delta^*)} + 2^{n-a}$$

full encryptions, where the advantage a can be up to $4w(\Delta^*)$. It is negligible when the number of non-zero nibbles of Δ^* is small. So the overall complexity of this attack is dominated by the sieving process consisting in the preparation and evaluation of the 2^m known plaintexts.

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. As for this attack the full code book (or almost) is necessary, we describe the attack on $2R = 2i + 2$ rounds for the family of PRINCE-like cipher without whitening keys. Like in some generic attacks [12,13] on Even–Mansour construction, our key-recovery attack take advantage of the fact that the first and last keys are identical.

Key Recovery for 6 *Rounds of* $\text{PRINCE}_{\text{core}}^{\alpha}$ 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 pre-compute certain values from the states of the second round and the second to last round of the cipher. We denote by P' and C' the plaintext and ciphertext of the cipher without whitening keys. For all $0 \leq b \leq 2^n - 1$, we denote by (V_b, W_b) the following values:

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

Then, as depicted in Fig. 4, for each pair (P', C') and the unknown key k_1 there exist V_b and W_b such that the following equations hold:

$$P' \oplus V_b = k_1,$$
$$P' \oplus C' = V_b \oplus W_b.$$

Store the value V_b in a hash table T of 2^{64} rows indexed by $V_b \oplus W_b$. On average, each row of T contains only one V_b. By assuming that we have 2^m known pairs (P', C'), the goal is to find for as many key candidates k_1 as possible a pair (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

1. Consider a list of all keys k_1.
2. For each of the 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_1 as a key candidate.

By using 2^m known plaintexts and by considering the collisions, the number of remaining wrong keys k_1 is about $2^n(1-2^{-n})^{2^m} = 2^n(1-2^{-n})^{2^n 2^{m-n}} \approx 2^n e^{-2^{m-n}} = 2^{n-1.44\times 2^{m-n}}$. 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. 5.3, we show that this attack can be applied for many more values of α.

5. Various Classes of α-Reflection

In [7], 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 [7] are recalled in Sect. 2.2. In this section, we compute the probabilities of the distinguishers proposed in Sect. 3 and their combinations for various classes of values of α, and determine the maximum number of rounds which can be attacked.

As presented in Sect. 3.2, characteristics on the external rounds can be seen as a differential characteristic with input difference α and related constant difference α, see Fig. 3. As PRINCE$^\alpha$ 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 a Branch and Bound algorithm. Finding the weakest α for such a characteristic

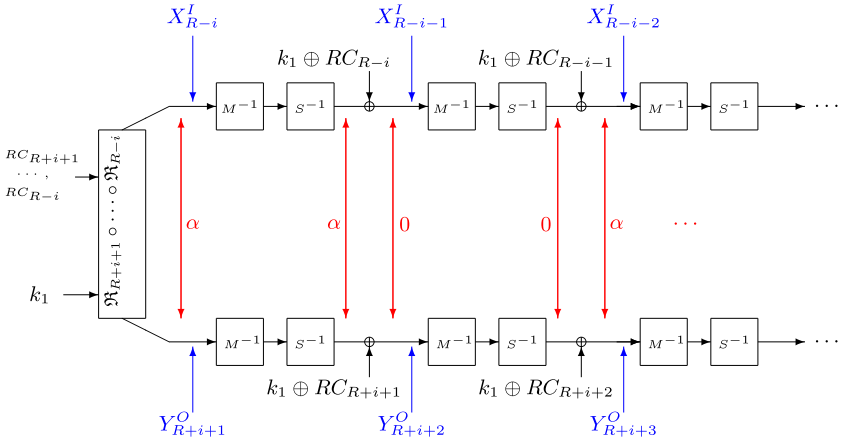


Fig. 5. Iterative characteristic.

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 $\text{PRINCE}^{\alpha}_{\text{core}}$ is possible.

5.1. *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 $\mathcal{P}_{\mathcal{C}_4}$. In this section, two methods to maximize $\mathcal{P}_{\mathcal{C}_u}$ are described. The first one inspired from the cancellation property can be performed for particular α. For the other values of α, we describe a more systematic method based on a Branch and Bound algorithm.

Cancellation Property In classical differential and linear cryptanalysis the idea of iterative characteristic have been used in the past to derive manually good characteristics. In some settings—for instance, when some component are not balanced or when considering related-key characteristics—cancellation of the differential characteristic allow to extend deterministically a characteristic to more rounds. For some α, we observe in the case of PRINCE^{α} that a cancellation of the differential characteristic is possible for two "symmetric" rounds with input difference the reflection parameter α. In the following, we describe this characteristic model for the family of PRINCE-like cipher. Illustration of this particular type of characteristic is given in Fig. 5.

Suppose that the characteristic $Y^O_{R+i+1} \oplus X^I_{R-i} = \alpha$ holds. Then with probability

$$\Pr_{\mathbf{X}}\left[S(\mathbf{X}) \oplus S(\mathbf{X} \oplus \alpha) = M^{-1}(\alpha)\right]$$

a cancellation of the difference occurs and we have $Y^O_{R+i+2} \oplus X^I_{R-i-1} = 0$. So the next folded round can be passed with probability one and finally based on the round constant

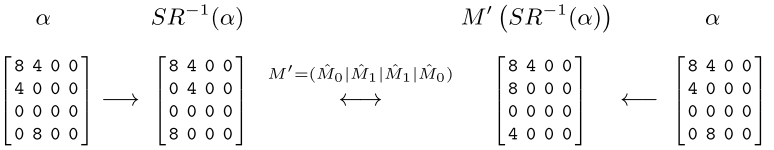


Fig. 6. Example of α for which we can derive an iterative characteristic.

Table 2. The weakest α with attack on 12 rounds using $\mathcal{C}_4 \circ \mathcal{I}_1$ and the iterative characteristic based on the cancellation idea.

α	Δ^*	$w(\Delta^*)$	$\mathcal{P}_{\mathcal{C}_4}$	$\text{PRINCE}^{\alpha}_{\text{core}}$	PRINCE^{α}	
				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. Differential probabilities of the inverse Sbox for single-bit input and output 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}

property we have $Y^O_{R+i+3} \oplus X^I_{R-i-2} = \alpha$. This characteristic can be applied iteratively. Such characteristics 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. In Fig. 6, we provide an illustration of this phenomenon for $\alpha = 8400400800000000$.

For the α in Table 2 with $w(\alpha) = 4$, the cancellation property leads to an attack on 12 rounds of $\text{PRINCE}^{\alpha}_{\text{core}}$. The probability of the characteristic has been computed from the difference table of the Sbox, see Table 3. In this table, complexity 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 $a = 4w(\Delta^*)$ for $\text{PRINCE}^{\alpha}_{\text{core}}$ and $a = 64 + 4w(\Delta^*)$ for PRINCE^{α}. The success probability is taken equal to 95 %. The data complexity is derived using Algorithm 1 of [6] and the time complexity is derived as for the key-recovery attack presented in Sect. 4.1.

No α with less than 4 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.

Table 4. Example of α with attack on 12 rounds using $\mathcal{C}_4 \circ \mathcal{I}_1$.

α	Δ^*	$w(\Delta^*)$	$\mathcal{P}_{\mathcal{C}_4}$	$\text{PRINCE}^{\alpha}_{\text{core}}$	PRINCE^{α}	
				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.

Automatic Search As the number of rounds of the folded cipher is small, the existence of iterative characteristic is, for many α, hard to determine. A Branch and Bound algorithm can then be used for searching the best reflection characteristics for a fixed α. Nevertheless, this method does not allow searching for the best α directly. Therefore, we must make guesses of the potentially best α to reduce the search space.

We start by analyzing the properties of the Sbox and the linear layer M of PRINCE in order to identify those values of α for which the number of active Sboxes at each round is minimal and the differential probabilities of the Sboxes 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 is a 4-bit value, $a_i \in \{0, 1, 2, 4, 8\}$, $i = 1, 2, 3, 4$. Differential probabilities of the inverse Sbox for single-bit differences are given in Table 3. Based on this table and experiments, we assume that α with some nibbles 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 the following procedure:

1. For $\alpha = (a_1, a_2, \ldots, a_{15}, a_{16})$, where $a_i \in \{0, 1, 4, 8\}$ (2^{32} values).
2. 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).
3. Among the remaining ones, check if there is a characteristic $\mathcal{C}_4$ with $\mathcal{P}_{\mathcal{C}_4} \geq 2^{-28}$.

Using this method the best derived α are the one of Table 2, with iterative characteristics.

In Table 4, we give other example of α derived from this automatic search, 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. We notice that different characteristics for the same α can be derived. Table 4 presents one of the best characteristic for 4 example of α with different probability and different time complexity.

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 constraints of the Branch and Bound algorithm.

Table 5. Example of α with attack on 10 rounds and $w(\alpha) = 2$ using $C_2 \circ \mathcal{I}_2$, computed for $P_S = 95\ \%$ and $a = 16$.

α	Δ^*	$w(\Delta^*)$	$\mathcal{P}_{\mathcal{C}_2}$	$\mathcal{P}_{\mathcal{I}_2}$	$\text{PRINCE}^{\alpha}_{\text{core}}$ Data/Time	PRINCE^{α} Data	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}

5.2. *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. 3.1. 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 $\mathcal{P}^{0}_{\hat{M}_\epsilon} \leq 2^{-8}$, computation for $\hat{M}_0$ and $\hat{M}_1$ gives us respectively 63 and 73 16-bit values and 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 $\alpha = \texttt{0000111100000000}$ and $\alpha = \texttt{0000000011110000}$.

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 $\alpha = \texttt{0000408000008040}$ given in Table 2 we have a characteristic with $\mathcal{P}_{\mathcal{C}_3} = 2^{-19}$ and $\mathcal{P}_{\mathcal{I}_2} = 2^{-40}$ while using $\mathcal{C}_4$ and $\mathcal{I}_1$ the best characteristic has probability 2^{-54}. 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 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 5.

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

5.3. *Impossible Attack*

If $\mathcal{P}_{\mathcal{I}_2} = 0$, a deterministic distinguisher on 4 rounds of the cipher can be built. It leads to the key-recovery attack described in Sect. 4.2 for a 6-round cipher without whitening keys. The time complexity of this attack correspond to $2^{62.56}$ encryptions and a storage of 2^{67} bytes of the hash table is needed. This attack is efficient, in particular, for $\alpha = \texttt{C0AC29B7C97C50DD}$ of PRINCE. But we can find many more values of α with $\mathcal{P}_{\mathcal{I}_2} = 0$.

As specified by (4), 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 $\mathcal{P}^{(\beta)}_{\hat{M}_0} = 0$ is 5940. For $\hat{M}_1$, the number of β for which $\mathcal{P}^{(\beta)}_{\hat{M}_1} = 0$ 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 $\mathcal{P}_{\mathcal{I}_2} = 0$, 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 the security or insecurity against the reflection attacks discussed in this paper.

6. Other Types of Attacks and Related Work

Due to its innovative structure, PRINCE has received a lot of attention from the cryptographic community as soon as it was released. In parallel works [1,20], the authors studied many types of attacks on PRINCE with its original parameter value α including biclique attacks [1] and different time-memory trade-offs [20]. These attacks are not better than the generic attacks as pointed out in [25]. Recently, using an advanced meet-in-the-middle technique, the authors of [10] have provided an attack on PRINCE reduced to 8 rounds with large time complexity requiring only one plaintext-ciphertext pair.

The integral distinguisher on the 4 middle rounds of PRINCE built in [20] allows to recover the key of a 6-round reduced version of PRINCE and thus improves on our attack presented in Sect. 5.3, which is efficient only on $\text{PRINCE}_{\text{core}}$.

Next, in Sect. 6.1, we take a detailed look at an attack based on a truncated characteristic proposed in [1]. Then we describe another attack of ours based on a similar truncated characteristic in Sect. 6.2.

In Sect. 6.3, we discuss related-key key-recovery attacks on $\text{PRINCE}^{\alpha}_{\text{core}}$. Since there is a trivial related-key distinguisher with probability one, the designers of PRINCE do not claim resistance against related-key attacks. On the other hand, the trivial distinguisher cannot be used for key recovery. Hence related-key attacks on PRINCE-like ciphers that can be used for key recovery are of interest. Moreover, the related-key attack presented in Sect. 6.3 can be turned to an efficient single-key attack assuming access to both encryption and decryption oracles.

6.1. *Truncated Attack for Original α*

The work reported in [1] also includes an attack for the original α which has been built upon similar reflection ideas than our attacks. But their distinguisher is a probabilistic one, while we considered only the impossible characteristic $\mathcal{I}_2$ which in the case of the original α is impossible as α is not among the fixed points of M'. To bypass this situation they construct a truncated characteristic, see Sect. 3.2 of [1]. This characteristic is depicted in Fig. 7 using our notation.

As α' can take 2^{16} values, the probability that $X_2^S \oplus Y_5^S$ is equal to one of these α' is 2^{-48}. Using $2^{56.08}$ plaintext-ciphertext pairs, the key k_1 of a 6-round version of $\text{PRINCE}^{\alpha}_{\text{core}}$ is derived using similar key-recovery technique than in Sect. 4. This probabilistic distinguisher allows a more powerful attack on a 6-round reduced version of $\text{PRINCE}^{\alpha}_{\text{core}}$ in terms of complexity than the one described in Sect. 5.3.

In the next section, we present a different attack based on another similar truncated characteristics which allows to recover the full key of a 8-round reduced version of PRINCE^{α}. The attack is efficient for 2^{18} values of α which do not include the original one.

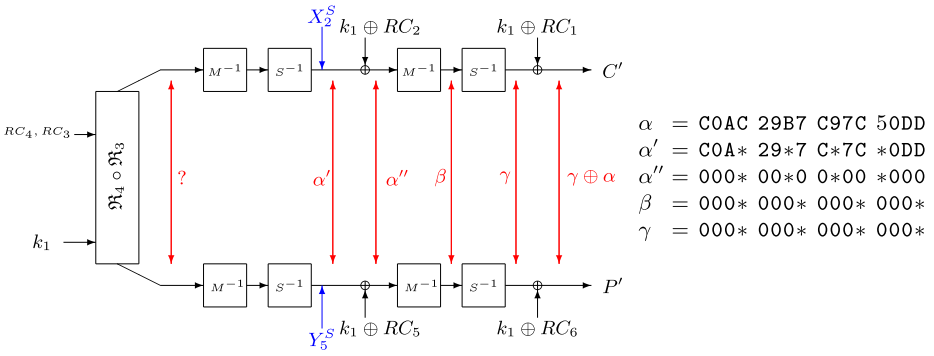


Fig. 7. The truncated characteristic of Sect. 3 of [1].

6.2. *Stronger Truncated Attack for Some Other α*

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

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*

$$Y^O_{R+3} \oplus X^I_{R-2} = \begin{bmatrix} * & 0 & 0 & 0 \\ * & 0 & 0 & * \\ * & 0 & * & 0 \\ * & * & 0 & 0 \end{bmatrix} \oplus \alpha, \tag{8}$$

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*:

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

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

Proof. The four 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 $\mathcal{I}_1$, the probability that $X_R^I \oplus Y_{R+1}^O = \alpha$ is equal to $P_{F_{M'}}$ ($= 2^{-32}$ for PRINCE$^\alpha$). 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

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

□

In all four cases of the characteristics, nine nibbles of the data difference are equal to those of α. Hence the uniform probability of such a truncated characteristic is 2^{-36} while the proposed characteristic has probability $P_{F_{M'}} = 2^{-32}$.

By the previous lemma, such truncated characteristics exist for $4 \times (2^{16} - 1) \approx 2^{18}$ values of α. While the distinguishers of Sect. 5.1 and Sect. 5.2 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

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

This truncated distinguisher enables a key-recovery attack for a cipher without whitening keys reduced to eight rounds in the same way that the key-recovery attack described in Sect. 4.2. In the following we describe the key-recovery attack for this truncated characteristic.

Key-Recovery Attack on PRINCE$^\alpha_{\text{core}}$ For simplicity, we restrict to the characteristic given by (8). 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 (8). 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 of $\text{PRINCE}^{\alpha}_{\text{core}}$. 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_1. It means that only up to 48 bits of k_1 can be obtained in a similar way to the attack of Sect. 4 ($1 \leq a \leq 48$). 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 $2^{48} \times 2^{12} = 2^{60}$ pairs $(a, b) \in (\mathbb{F}_2^{48} \times \mathbb{F}_2^{48})$ such that $a \oplus b$ is equal to the truncated state of the three most right columns in $\begin{bmatrix} * & 0 & 0 & 0 \\ * & 0 & 0 & * \\ * & 0 & * & 0 \\ * & * & 0 & 0 \end{bmatrix} \oplus \alpha$ compute the pair $(\nu_a, \omega_b) \in (\mathbb{F}_2^{48} \times \mathbb{F}_2^{48})$ (see Fig. 4) 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 has $\frac{2^{60}}{2^{48}} = 2^{12}$ values.

Attack Procedure

1. Allocate a counter D_{k_1} for each 2^{48} values of k_1.
2. For each 2^m pairs (P_t, C_t)

   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.

3. Consider a list of 2^{48-a} of the keys k_1 with highest counter values. Do an exhaustive search on the remaining $64 - a$ bits of key.

Assuming that α does not have any zero nibble, the time complexity of Step 2 corresponds to 2^{m+12} memory accesses. The exhaustive search described in Step 3, required 2^{64-a}. We need $2^{60} \times 48/8 \times 2 \simeq 2^{63.6}$ bytes for the storage of the hash table T and $2^{48-a} \times 48/8 = 2^{50.6-a}$ bytes for the storage of the list of key candidates.

When considering only the most probable key ($a = 48$), this attack can be performed using $2^{36.82}$ known plaintext-ciphertext in time corresponding to $2^{48.8}$ memory accesses and 2^{16} full encryptions. The memory complexity is dominated by the storage of $2^{63.6}$ bytes for the hash table.

Extension of this attack on a 8-round reduced version of PRINCE^{α}, will require a data complexity of $2^{36.85}$, a time complexity of $2^{97.8}$ memory accesses and 2^{80} full encryptions and the storage of $2^{63.6}$ bytes.

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.

$$0 \xrightarrow{\text{key-add}} \alpha \xrightarrow{S} \gamma \xrightarrow{M} \alpha \xrightarrow{\text{key-add}} 0 \xrightarrow{S} 0 \xrightarrow{M} 0 \xrightarrow{\text{key-add}} \alpha \xrightarrow{S} \gamma \xrightarrow{M} \alpha \xrightarrow{\text{key-add}} 0 \xrightarrow{S} 0 \xrightarrow{M} 0$$
$$\xrightarrow{\text{key-add}} \alpha \xrightarrow{S} \gamma \xrightarrow{M} \alpha \xrightarrow{\text{key-add}} 0 \xrightarrow{S} 0 \xrightarrow{M'} 0 \xrightarrow{S^{-1}} 0 \xrightarrow{\text{key-add}} \alpha \xrightarrow{M^{-1}} \gamma \xrightarrow{S^{-1}} \alpha$$
$$\xrightarrow{\text{key-add}} 0 \xrightarrow{M^{-1}} 0 \xrightarrow{S^{-1}} 0 \xrightarrow{\text{key-add}} \alpha \xrightarrow{M^{-1}} \gamma \xrightarrow{S^{-1}} \alpha \xrightarrow{\text{key-add}} 0 \xrightarrow{M^{-1}} 0 \xrightarrow{S^{-1}} 0 \xrightarrow{\text{key-add}} \alpha \xrightarrow{M^{-1}} \gamma$$

Fig. 8. A related-key characteristic.

6.3. *Related-Key Key-Recovery Attacks*

Recently a related-key key-recovery attack for 240 values of α in the boomerang setting was presented in [20]. It makes use of a characteristic which is similar to the iterative characteristics we exploited in our analysis and uses adaptively chosen plaintext. It is also interesting to note that this related-key attack is efficient for the values of α such that α is block diagonal, while our attack based on truncated characteristic in Sect. 6.2 is applicable to α such that $M^{-1}(\alpha)$ is block diagonal.

Next we present a related-key attack on $\text{PRINCE}^{\alpha}_{\text{core}}$, which is applicable to the values of α given in Table 2. Let us assume that the attacker obtains encryptions C and C' of the same, but possibly unknown plaintext P using $\text{PRINCE}^{\alpha}_{\text{core}}$ under keys k_1 and $k_1 \oplus \alpha$, respectively. Note that due to the α-reflection property, the related-key encryption oracle with the key $k_1 \oplus \alpha$ can be replaced by the decryption oracle with the original key k_1, and in this manner, this attack can be turned to an attack in a single-key model. Also note that the difference is introduced only in the key and not in the plaintext.

Based on the iterative characteristic presented in Sect. 5, we define a related-key characteristic. Using this 11.5-round distinguisher the full $\text{PRINCE}^{\alpha}_{\text{core}}$ is vulnerable for some reflection parameters including the α given in Table 2, for which this attack is particularly effective. Let $\gamma = M^{-1}(\alpha)$, this distinguisher is built on the following characteristic over 11.5 rounds (see Fig. 8).

This related-key characteristic is deterministic on the midmost rounds, while in all other attacks presented in this paper for α in Table 2, the midmost rounds are the most expensive for the characteristics and can be passed over with small probabilities $\mathcal{P}_{\mathcal{I}_1} = 2^{-32}$ and $\mathcal{P}_{\mathcal{I}_2} \leq 2^{-32}$. Moreover, the related-key characteristic cancels every two rounds, and can be efficient for the α such that $\gamma = M^{-1}(\alpha)$ is non-zero on the same nibble positions. The probability of this characteristic is

$$\Pr_{\mathbf{X}}\left[S(\mathbf{X}) \oplus S(\mathbf{X} \oplus \alpha) = M^{-1}(\alpha)\right]^5 = 2^{-55},$$

for the first four α of Table 2.

The most expensive part of this attack, similarly to any last-round key-recovery attack in the differential context, is the sieving process. It consists of discarding all ciphertext pairs (C, C') such that $C \oplus C'$ is non-zero on the zero nibble positions of α. For the remaining pairs, up to $4w(\alpha)$ bits of k_1 can be found by partially deciphering the last round. The remaining bits of k_1 can be found using exhaustive search. The time complexity of this attack is dominated by the sieving process, which is roughly equivalent to the data complexity.

To achieve the full advantage of $4w(\alpha)$ key bits, this related-key attack on $\text{PRINCE}^{\alpha}_{\text{core}}$ takes $2^{57.89}$ known plaintexts and corresponding ciphertexts encrypted with two differ-

ent keys. The attack requires the storage of $2^{4w(\alpha)} = 2^{16}$ counters and its time complexity is $2^{57.89}$.

7. Conclusion and Open Questions

In this paper, we presented results of the first application of reflection cryptanalysis on PRINCE-like ciphers. Since the characteristics $\mathcal{I}_1$ and $\mathcal{I}_2$ are naturally suggested by the α-reflection structure of the cipher, we restricted our attention to them as starting points for the reflection characteristics. In addition to studying the structural extensions of $\mathcal{I}_1$ and $\mathcal{I}_2$ by the characteristics $\mathcal{C}_u$ and finding the weakest α for such combinations, we also performed automatic searches and found many weak α values directly. The weakest values of α were found when starting from $\mathcal{I}_1$, and they allow an efficient key-recovery attack on 12 rounds of the core cipher.

Our 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. This attack which requires $2^{56.08}$ known plaintext-ciphertext pairs is, however, not better than the generic attack. It would also be possible to perform similar analysis starting from some other characteristics over the midmost rounds of the cipher. The question, whether such an approach can be successfully used to find new distinguishers that are more efficient for the original α, remains to be studied.

One of the main goals of this work was to investigate how the choice of the reflection parameter influences the security of a PRINCE-like cipher. For this reason, in all concrete examples presented in this paper, the other components of the cipher were kept as specified in the original design. Based on their analysis of resistance against differential and linear attacks in [7,8], the designers suggested that also other non-linear layers ensuring the same differential and linear properties could have been chosen. Encouraged by one of the anonymous reviewers, we experimented on S-boxes obtained from the original one using affine transformations and observed that such changes could significantly weaken the resistance of the cipher against reflection attack. Our experiments on the characteristics $\mathcal{C}_4$ and the values of α in Table 2 showed that there are affine transformations such that, when applied to the original Sbox, the differential probabilities in Table 3 will be changed in such a way that the probabilities $\mathcal{P}_{\mathcal{C}_4}$ can be increased significantly. For example, for some α, the probability $\mathcal{P}_{\mathcal{C}_4}$ can be increased from 2^{-24} to 2^{-16}. Using the otherwise same setting as in Sect. 5.1, we obtain an attack requiring $2^{51.41}$ plaintext/ciphertext pairs and performing in time $2^{65.82}$ which is better than the generic attack over the complete 12-round cipher. This example demonstrates that resistance against reflection attack depends strongly on the properties of the combinations of the linear layer, the non-linear layer and the reflection parameter, and opens up the need for more research to achieve better understanding of this complex issue.

In this work we developed and applied probabilistic reflection distinguishers for a cipher with SPN structure. We see at least two directions as potential future applications of our ideas. First, it would be interesting to revisit deterministic reflection distinguishers that are previously known to exist on several Feistel ciphers and investigate if they have probabilistic extensions that could be used for attacking more rounds of those

ciphers. A second direction would be look at other involutional SPN ciphers like ICEBERG [29], KHAZAD [3] or ANUBIS [2] as possible targets of probabilistic reflection distinguishers. More generally, cryptanalysis on specific Even–Mansour designs, such as our work on PRINCE presented here and the recent attacks on the LED cipher [27], may serve as sources of inspiration for future research on the general Even–Mansour scheme.

Acknowledgements

We wish to thank the anonymous reviewers of FSE 2013 and Journal of Cryptology for their helpful suggestions for improving the paper. The authors from Aalto University wish to acknowledge useful discussions with Gregor Leander during his visits in 2012 and 2013 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 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 (Nos. 61272476, 61232009, 61202420).

References

[1] F. Abed, E. List, S. Lucks, On the Security of the Core of PRINCE Against Biclique and Differential Cryptanalysis. Cryptology ePrint Archive, Report 2012/712 (2012). http://eprint.iacr.org/

[2] P.S.L.M. Barreto, V. Rijmen, The ANUBIS Block Cipher. Submission to the NESSIE project (2000). http://www.larc.usp.br/~pbarreto/AnubisPage.html

[3] P.S.L.M. Barreto, V. Rijmen, The KHAZAD Legacy-level Block Cipher. Submission to the NESSIE project (2000). http://www.larc.usp.br/~pbarreto/KhazadPage.html

[4] E. Biham, New types of cryptanalytic attacks using related keys. *J. Cryptol.* **7**(4), 229–246 (1994)

[5] A. Biryukov, D. Wagner, Slide attacks, in *FSE 1999*, ed. by L.R. Knudsen. Lecture Notes in Computer Science, vol. 1636 (Springer, Berlin, 1999), pp. 245–259

[6] C. Blondeau, B. Gérard, J.-P. Tillich, Accurate estimates of the data complexity and success probability for various cryptanalyses. *Des. Codes Cryptogr.* **59**(1–3), 3–34 (2011)

[7] J. Borghoff, A. Canteaut, T. Güneysu, E. Bilge Kavun, M. Knezevic, L.R. Knudsen, G. Leander, V. Nikov, C. Paar, C. Rechberger, P. Rombouts, S.S. Thomsen, T. Yalçin, PRINCE—a low-latency block cipher for pervasive computing applications—extended abstract, in *ASIACRYPT 2012*, ed. by X. Wang, K. Sako. Lecture Notes in Computer Science, vol. 7658 (Springer, Berlin, 2012), pp. 208–225

[8] J. Borghoff, A. Canteaut, T. Güneysu, E. Bilge Kavun, M. Knezevic, L.R. Knudsen, G. Leander, V. Nikov, C. Paar, C. Rechberger, P. Rombouts, S.S. Thomsen, T. Yalçin, PRINCE—A Low-latency Block Cipher for Pervasive Computing Applications (Full version). Cryptology ePrint Archive, Report 2012/529 (2012). http://eprint.iacr.org/

[9] C. Bouillaguet, O. Dunkelman, G. Leurent, P.-A. Fouque, Another look at complementation properties, in *FSE 2010*, ed. by S. Hong, T. Iwata. Lecture Notes in Computer Science, vol. 6147 (Springer, Berlin, 2010), pp. 347–364

[10] A. Canteaut, M. Naya-Plasencia, B. Vayssière, Sieve-in-the-middle: improved MITM attacks, in *CRYPTO 2013*, ed. by R. Canetti, J.A. Garay. Lecture Notes in Computer Science, vol. 8042 (Springer, Berlin, 2013), pp. 222–240

[11] D. Coppersmith, The real reason for rivest's phenomenon, in *CRYPTO 1985*, ed. by H.C. Williams. Lecture Notes in Computer Science, vol. 218 (Springer, Berlin, 1986), pp. 535–536

[12] I. Dinur, O. Dunkelman, N. Keller, A. Shamir, An Improved Attack on 4-Round Even–Mansour with 2 Alternating Keys. Rump session of CRYPTO 2013 (2013)

[13] I. Dinur, O. Dunkelman, N. Keller, A. Shamir, Key Recovery Attacks on 3-round Even–Mansour, 8-step LED-128, and Full AES^2. Cryptology ePrint Archive, Report 2013/391 (2013). http://eprint.iacr.org/, extended version of ASIACRYPT 2013

[14] I. Dinur, O. Dunkelman, A. Shamir, Improved attacks on full GOST, in *FSE 2012*, ed. by A. Canteaut. Lecture Notes in Computer Science, vol. 7549 (Springer, Berlin, 2012), pp. 9–28

[15] O. Dunkelman, N. Keller, A. Shamir, Minimalism in cryptography: the even–mansour scheme revisited, in *EUROCRYPT*, ed. by D. Pointcheval, T. Johansson. Lecture Notes in Computer Science, vol. 7237 (Springer, Berlin, 2012), pp. 336–354

[16] E. Shimon, Y. Mansour, A construction of a cipher from a single pseudorandom permutation, in *ASIACRYPT*, ed. by H. Imai, R.L. Rivest, T. Matsumoto. Lecture Notes in Computer Science, vol. 739 (Springer, Berlin, 1991), pp. 210–224

[17] P. Flajolet, R. Sedgewick, *Analytic Combinatorics* (Cambridge University Press, Cambridge, 2009)

[18] J. Guo, T. Peyrin, A. Poschmann, M.J.B. Robshaw, The LED block cipher, in *CHES 2011*, ed. by B. Preneel, T. Takagi. Lecture Notes in Computer Science, vol. 6917 (Springer, Berlin, 2011), pp. 326–341

[19] T. Isobe, A single-key attack on the full GOST block cipher, in *FSE 2011*, ed. by A. Joux. Lecture Notes in Computer Science, vol. 6733 (Springer, Berlin, 2011), pp. 290–305

[20] J. Jean, I. Nikolic, T. Peyrin, L. Wang, S. Wu, Security analysis of PRINCE, in *FSE 2013* ed. by S. Moriai (2013 to appear)

[21] K. Orhun, Reflection cryptanalysis of some ciphers, in *INDOCRYPT 2008*, ed. by D.R. Chowdhury, V. Rijmen, A. Das. Lecture Notes in Computer Science, vol. 5365 (Springer, Berlin, 2008), pp. 294–307

[22] O. Kara, C. Manap, A new class of weak keys for blowfish, in *FSE 2007*, ed. by A. Biryukov. Lecture Notes in Computer Science, vol. 4593 (Springer, Berlin, 2007), pp. 167–180

[23] J. Kilian, P. Rogaway, How to protect DES against exhaustive key search, in *CRYPTO 1996*, ed. by N. Koblitz. Lecture Notes in Computer Science, vol. 1109 (Springer, Berlin, 1996), pp. 252–267

[24] L.R. Knudsen, G. Leander, A. Poschmann, M.J.B. Robshaw, PRINTcipher: a block cipher for IC-printing, in *CHES 2010*, ed. by S. Mangard, F.-X. Standaert. Lecture Notes in Computer Science, vol. 6225 (Springer, Berlin, 2010), pp. 16–32

[25] G. Leander, Design and analysis of block cipher—Links to Boolean functions and coding theory (invited talk), in *WCC 2013* (2013)

[26] J.H. Moore, G.J. Simmons, Cycle structures of the DES with weak and semi-weak keys, in *CRYPTO 1986*, ed. by A.M. Odlyzko. Lecture Notes in Computer Science, vol. 263 (Springer, Berlin, 1987), pp. 9–32

[27] I. Nikolic, L. Wang, S. Wu, Cryptanalysis of round-reduced LED, in *FSE 2013*, ed. by S. Moriai. Lecture Notes in Computer Science (2013 to appear)

[28] H. Soleimany, C. Blondeau, X. Yu, W. Wu, K. Nyberg, H. Zhang, L. Zhang, Y. Wang, Reflection cryptanalysis of PRINCE-like ciphers, in *FSE 2013*, ed. by S. Moriai. Lecture Notes in Computer Science (Springer, Berlin, 2013 to appear).

[29] F.-X. Standaert, G. Piret, G. Rouvroy, J.-J. Quisquater, J.-D. Legat, ICEBERG: an involutional cipher efficient for block encryption in reconfigurable hardware, in *FSE*, ed. by B.K. Roy, W. Meier. Lecture Notes in Computer Science, vol. 3017 (Springer, Berlin, 2004), pp. 279–299