Reflection ciphers

Christina Boura, Anne Canteaut, Lars R. Knudsen, Gregor Leander

Noname manuscript No.
(will be inserted by the editor)

Reflection Ciphers

Christina Boura · Anne Canteaut · Lars R. Knudsen · Gregor Leander

Abstract This paper investigates ciphers where the set of encryption functions is identical to the set of decryption functions, which we call *reflection ciphers*. Equivalently, there exists a permutation P, named the coupling permutation, such that decryption under k corresponds to encryption under $P(k)$. We study the necessary properties for this coupling permutation. Special care has to be taken of some related-key distinguishers since, in the context of reflection ciphers, they may provide attacks in the single-key setting. We then derive some criteria for constructing secure reflection ciphers and analyze the security properties of different families of coupling permutations. Finally, we concentrate on the case of reflection block ciphers and, as an illustration, we provide concrete examples of key schedules corresponding to several coupling permutations, which lead to new variants of the block cipher PRINCE.

Keywords Reflection ciphers · Involutions · Related-key distinguishers, · PRINCE

Mathematics Subject Classification (2000) 94A60

This work has been initiated when the four authors were with DTU, Denmark.

Christina Boura
Université de Versailles Saint-Quentin, France
E-mail: christina.boura@prism.uvsq.fr

Anne Canteaut
Inria, France
E-mail: anne.canteaut@inria.fr

Lars R. Knudsen
DTU, Denmark
E-mail: lrkn@dtu.dk

Gregor Leander
Ruhr-Universität Bochum, Germany
E-mail: gregor.leander@rub.de

1 Introduction

Among all design strategies used for reducing the implementation cost of a cipher, one option consists in minimizing the overhead of decryption on top of encryption. This feature was essential when encryption was performed by heavy cipher machines since having two different machines, one for encryption and a different one for decryption was unthinkable. This issue was then solved a century ago by Arthur Scherbius who introduced a reflector into the Enigma machine, that means an involutive transformation M which is applied to the initial permutation and which is followed by the inverse permutation. Then, for any key, the encryption function has the form $E_k = F^{-1} \circ M \circ F$, implying that it is an involution. However, involutive ciphers present serious flaws, including the fact that any involution can be easily distinguished from a randomly permutation by the number of its fixed points. This type of weaknesses has been exploited for cryptanalyzing Enigma. Instead, a classical solution consists in constructing a cipher based on involutive building-blocks. For instance, the different round permutations can be chosen within a family of involutions parameterized by a round key, i.e., $E_{(k_1,\ldots,k_r)} = F_{k_r} \circ \ldots \circ F_{k_2} \circ F_{k_1}$ where all F_x are involutions. Then, the decryption function under the round-key sequence $(k_1, \ldots, k_r)$ is equal to the encryption function under the same round-key sequence but in reverse order, i.e. $\mathrm{Rev}(k_1, \ldots, k_r) = (k_r, \ldots, k_1)$. Obviously, Feistel ciphers are the most prominent examples of this construction [13]. But, since the round key sequence is usually derived from a master key, i.e., $(k_1, \ldots, k_r) = \mathrm{KS}(k)$, the choice of the key expansion KS has a major influence both on the security and on the implementation cost of the cipher. Indeed, KS should obviously be chosen such that $\mathrm{KS}(k)$ does not provide any palindromic round-key sequence. Otherwise, the cipher would have some weak keys under which the encryption is an involution. Moreover, computing $\mathrm{Rev}(\mathrm{KS}(k))$ requires either the storage of the whole round-key sequence, or the implementation of the reverse key expansion function, like in the DES, for instance.

The implementation overhead due to the reverse key schedule can be avoided by designing a cipher such that the family of decryption functions obtained for all master keys is exactly the same as the family of all encryption functions. In other words, for any master key k, there exists another key k' such that decryption with key k corresponds to encryption with k'. This has been used in [6] for the block cipher PRINCE, more precisely for its core cipher PRINCE_{core}, where $k' = k \oplus \alpha$ for some constant α. However, we could think of a more general setting where there exists some permutation P of the key space such that, for any key k,

$$(E_k)^{-1} = E_{P(k)} \tag{1}$$

Such ciphers will be called *reflection ciphers* and the permutation P the *coupling permutation*. As previously explained, reflection ciphers obviously include all constructions with involutive round functions, like Feistel ciphers. In this case, the coupling permutation is $P = \mathrm{Rev}$. RSA is also a reflection cipher and in this case, the coupling permutation is secret: P is the permutation of the set $\{x \in \{2, \ldots, (p-1)(q-1)-1\} \ : \gcd(x, (p-1)(q-1)) = 1\}$ corresponding to inversion modulo $(p-1)(q-1)$, where p and q are two distinct prime numbers.

One of the main motivations of this general setting is to improve the key-schedule of the block-cipher PRINCE. Indeed, the core cipher of PRINCE follows

the general construction depicted on Figure 1, which leads to a reflection cipher with coupling permutation $P(k) = k \oplus \alpha$.

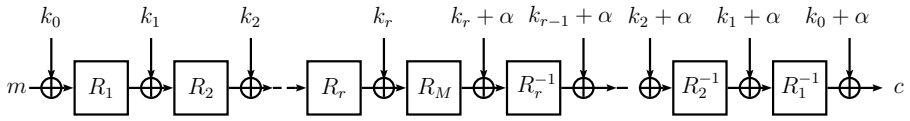

Fig. 1 Construction used in PRINCE$_{core}$ where the middle round R_M is an involution. The resulting cipher is a reflection cipher with coupling permutation $P(k) = k \oplus \alpha$.

But in this construction the key size is limited to the block size (which is 64 bits only). The solution chosen by the designers of PRINCE to increase the key size consists in adding an independent whitening key at the beginning and at the end of the cipher. However this construction is not optimal and raises security questions [7, 15, 10]. Designing a secure key-schedule for reflection ciphers with n-bit block size and $2n$-bit key size is therefore an open issue which is addressed in this paper.

Our Contribution.

This work mainly aims at studying the properties of reflection ciphers and at deriving several universal conditions on how the coupling permutation P should be constructed. We start by exhibiting very general properties, showing for example that a coupling permutation should be an involution and that fixed points should be avoided (cf. Section 2). A class of coupling permutations of particular interest is the class of affine permutations as such functions permit in general very efficient implementations. We study therefore this case and describe criteria that should be verified so that the general properties exhibited before hold for these functions.

Obviously, reflection ciphers are not ideal in the related-key setting since the relation $(E_k)^{-1} = E_{P(k)}$ allows to easily distinguish them from an ideal cipher. We therefore explicitly exclude related-key attacks here. However, an important observation is that some related-key distinguishers may have a practical impact since they provide attacks in the single-key model, in a scenario where an attacker has access to both the encryption and the decryption operations. Therefore we study the influence of the choice of P on such attacks, in particular on differential related-key distinguishers. We elaborate on the trade-off between the size of (possibly weak) key classes and the minimal Hamming weight of the difference $P(k) \oplus k$ introduced by comparing the encryption with the decryption process. We investigate different kinds of coupling permutations such as affine permutations, including functions based on bit permutations, nonlinear permutations and some combinations of those by analyzing for each case the impact of related-key distinguishers (cf. Section 3). We show in particular, that each family of functions can offer different trade-offs between the two above quantities.

In Section 4 we narrow down the scope and focus on key-alternating block ciphers by emphasizing on ciphers with n-bit block size and $2n$-bit key size, like PRINCE. We present two specific constructions for such ciphers. We then derive

from the previous theoretical results several examples of key-schedules corresponding to different coupling permutations for the case $n = 64$, which provide alternative key-schedules to the cipher PRINCE [6].

2 General Criteria For the Coupling Mapping

In this section we derive criteria for the coupling mapping P. These criteria are general and can be applied to different settings. For the rest of this paper, κ denotes the key size and n the block size of the cipher. Therefore, the coupling mapping is a function from $\mathbb{F}_2^\kappa$ into $\mathbb{F}_2^\kappa$.

2.1 Cycle structure of the coupling mapping

It is clear that Relation (1) makes sense only when the coupling mapping P is a permutation: otherwise, there exists a subset of the key space which leads to the same family of encryption functions. Moreover, Relation (1) implies that

$$E_k = E_{P^{2^i}(k)}, \ \forall i \geq 1,$$

for any key k. Then, if P is not an involution, several keys again lead to the same encryption function, implying that the effective size of the key space is reduced. Therefore, we focus on the case where P is an involution.

Fixed points of the coupling mapping. Fixed points of P correspond to weak keys for the cipher, since the corresponding encryption functions are involutive. Indeed, random involutions can be distinguished from random permutations by using the fact that such involutions over $\mathbb{F}_2^\kappa$ have $2^{\frac{\kappa}{2}} + \mathcal{O}(1)$ fixed points, whereas a randomly chosen permutation has $\mathcal{O}(1)$ fixed points [14, Page 596]. This weakness is well-known and has been exhibited in several works, including [26]. It is worth noticing that, in the particular case of an iterative construction of the form $E_k = F^{-1} \circ M \circ F$, E_k has exactly the same number of fixed points as the middle round M (and more general the exact same cycle structure). This fact has been exploited for weak keys in DES where the middle round is the swapping of the two halves, which has exactly 2^{32} fixed points [9], and also in Enigma where the reflector has no fixed points.

Fixed points of the coupling mapping also introduce weaknesses when E is not used directly as an encryption function, but is modified by the FX-construction [5, 21]. This construction (aka the Even-Mansour construction [11]) extends a block cipher E with a κ-bit key to a block cipher with a $(\kappa + 2n)$-bit key by XORing two n-bit secret whitening keys to the input and the output of the cipher respectively. If the reflection cipher E is used as inner cipher in the FX-construction, fixed points in the coupling mapping can be exploited by the attacker to recover some information on the whitening keys (see Section 4.2 in [6]).

2.2 Affine coupling mappings

In this section, we focus on the case where P is an affine mapping, which is of particular interest as affine functions permit efficient implementations. We provide here some simple characterizations of affine involutions without fixed points, based on elementary algebra. To avoid any ambiguity, we draw attention to the fact that elements in $\mathbb{F}_2^\kappa$ are seen as row vectors, and that linear permutations are written $x \mapsto xM$ for some matrix M.

Proposition 1 *Let P be an affine function of $\mathbb{F}_2^\kappa$. Then, the following statements are equivalent:*

(i) P is an involution without any fixed points.
(ii) $L : x \mapsto P(x) + P(0)$ is an involution and $P(0)$ belongs to $\operatorname{Ker}\phi \setminus \operatorname{Im}\phi$, where $\phi = L + \mathrm{Id}$.
(iii) $\phi : x \mapsto P(x) + P(0) + x$ satisfies $\operatorname{Im}\phi \subset \operatorname{Ker}\phi$ and $P(0)$ belongs to $\operatorname{Ker}\phi \setminus \operatorname{Im}\phi$.

Proof First, it is clear that P has a fixed point x_0 if and only if $\phi(x_0) = P(0)$, i.e., $P(0)$ belongs to $\operatorname{Im}\phi$. Moreover, by writing $P(x) = \phi(x) + x + P(0)$, we deduce that $P(P(0)) = 0$ if and only if $\phi(P(0)) = 0$, i.e., $P(0) \in \operatorname{Ker}\phi$. Then, $P(0) \in \operatorname{Ker}\phi \setminus \operatorname{Im}\phi$ if and only if P has no fixed points and $P(P(0)) = 0$.

Let us now show that the other conditions in (ii) and (iii) are equivalent to the fact that $P^2(x) = x$ for all nonzero x. For any x, we have

$$P(P(x)) = L(L(x) + P(0)) + P(0) = L(L(x)) + (L + \mathrm{Id})(P(0)) = L(L(x)).$$

Since $L(L(0)) = 0$ by definition of L, we deduce that $P(P(x)) = x$ for all nonzero x if and only if L is an involution. Similarly, we have

$$P(P(x)) = \phi(L(x)) + L(x) = \phi(\phi(x)) + \phi(x) + \phi(x) + x = \phi(\phi(x)) + x.$$

Then, for any nonzero x, $P^2(x) = x$ if and only if $\phi^2(x) = 0$. This is equivalent to $\operatorname{Im}\phi \subseteq \operatorname{Ker}\phi$, but equality does not hold since $P(0) \in \operatorname{Ker}\phi \setminus \operatorname{Im}\phi$. □

It is worth noticing that the condition $\operatorname{Im}\phi \subset \operatorname{Ker}\phi$ implies that $\dim \operatorname{Ker}\phi > \kappa/2$. Also, the previous proposition recovers the result from [24, Lemma 1]: any linear involution over $\mathbb{F}_2^\kappa$ has at least $2^{\kappa/2}$ fixed points, since we have proved that P is a linear involution if and only if $\operatorname{Im}\phi \subseteq \operatorname{Ker}\phi$.

Coupling mappings based on bit permutations.

When $L : x \mapsto P(x) + P(0)$ corresponds to a bit permutation, we can derive a very simple characterization of the mappings which satisfy the conditions of the previous proposition.

Lemma 1 *Let π be a permutation of $\{1, \ldots, \kappa\}$ and M the corresponding $\kappa \times \kappa$ permutation matrix, i.e., $M_{ij} = 1$ if and only if $j = \pi(i)$. Then, the dimension of $\operatorname{Ker}(M + \mathrm{Id})$ is equal to the number of cycles of π. Moreover, there exists some $\alpha \in \operatorname{Ker}(M + \mathrm{Id}) \setminus \operatorname{Im}(M + \mathrm{Id})$ if and only if π has a cycle of odd length.*

Proof We number the positions in a way that all positions within a cycle of π are consecutive. More precisely, if π has c cycles, $\{1, \ldots, \kappa\}$ is partitioned into c intervals $\{\ell_i, \ldots, \ell_{i+1} - 1\}$, $1 \leq i \leq c$, where $\ell_1 = 1$, $\ell_{c+1} = \kappa + 1$ and

$$\pi(j) = \begin{cases} j+1 & \text{if } j \in \{\ell_i, \ldots, \ell_{i+1} - 2\} \\ \ell_i & \text{if } j = \ell_{i+1} - 1 \end{cases}$$

Then, $(M + \mathrm{Id})$ is a block matrix

$$M' = \begin{bmatrix} A_1 & 0 & \ldots & \ldots & 0 \\ 0 & A_2 & 0 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & \ldots & \ldots & 0 & A_c \end{bmatrix} \text{ with } A_i = \begin{bmatrix} 1 & 1 & 0 & \ldots & 0 \\ 0 & 1 & 1 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ 1 & 0 & 0 & \ldots & 1 \end{bmatrix}$$

where each A_i is a $(\ell_{i+1} - \ell_i) \times (\ell_{i+1} - \ell_i)$ matrix if $\ell_{i+1} - \ell_i \geq 2$, and $A_i = [0]$ if $\ell_{i+1} = \ell_i + 1$. It follows that $\mathrm{Ker}(M + \mathrm{Id})$ is the subspace of dimension c such that all bits within $\{\ell_i, \ldots, \ell_{i+1} - 1\}$ with $\ell_{i+1} - \ell_i \geq 2$ are identical. Moreover, $\mathrm{Im}(M + \mathrm{Id})$ is the subspace formed by all vectors x such that

$$x_{\ell_i - 1} = \bigoplus_{j=\ell_{i-1}}^{\ell_i - 2} x_j, \ \forall 1 \leq i \leq c \text{ with } \ell_{i+1} - \ell_i \geq 2 \, .$$

In other words, the last bit in each cycle of length at least 2 is a parity bit. By using that a cycle composed of identical bits has a valid parity bit if and only if its length is even, we deduce that there exists some element in $\mathrm{Ker}(M + \mathrm{Id})$ and not in $\mathrm{Im}(M + \mathrm{Id})$ if and only if π has a cycle of odd length. □

By combining the previous lemma with the second characterization in Proposition 1, we derive the following.

Corollary 1 *Let π be a permutation of $\{1, \ldots, \kappa\}$ and M the corresponding $\kappa \times \kappa$ permutation matrix. Then, there exists α such that $x \mapsto xM + \alpha$ is an involution without fixed points if and only if π is an involution with at least one fixed point.*

In Section 4.2 of [6] the authors explain that the coupling mapping $P(k_1, k_2) = (k_2, k_1) + (\alpha, \alpha)$ should be avoided for any choice of the constant α. Indeed, this mapping presents an obvious class of weak keys, that can be easily detected: all keys (k_1, k_2) with $k_2 = k_1 + \alpha$ are fixed points of P. Then, the corresponding encryption function is an involution. This unwanted behavior can now be explained by Corollary 1. Indeed, the bit permutation π in the above coupling mapping is only composed of cycles of length 2.

All affine involutions P analysed in the rest of the paper are assumed without fixed points.

3 Impact of related-key distinguishers

The class of ciphers considered here has trivial related-key distinguishers. However, any class of related-key distinguishers for a reflection cipher involving both E_k and its inverse, *i.e.*, $E_{P(k)}$, provides a distinguisher in the single-key setting. So, at least in scenarios where an attacker can be assumed to have access to both the

encryption and the decryption operations, the existence of some related-key distinguisher must be investigated with care. There are at least two different approaches (and a trade-off between both):

- The coupling mapping P can be designed in such a way that the relation between k and $P(k)$ is so complicated that any good related-key distinguisher can only be exploited for a very small number of keys. For instance, if almost all values $k + P(k)$ differ when k varies, then any good related-key differential distinguisher (involving keys which differ by a constant) defines very few weak keys only.
- The coupling mapping P can be designed in such a way that, for any k, a distinguisher involving both k and $P(k)$ is unlikely to exist. For instance, choosing $P(x) = x + \alpha$ as in [6], where α is a randomly chosen constant with a high Hamming weight, follows this approach. One may expect that there are no related-key distinguishers involving two keys with difference α, but, on the other hand, if such a distinguisher exists, then all keys will be weak.

3.1 Related-key differential distinguishers

It is well-known that a given block cipher cannot be secure against all types of related-key distinguishers. Indeed, there exist some sets of related-key derivation functions which allow to build a distinguisher with overwhelming advantage for any cipher [4,17,1]. Here, we focus on the set of additions with a constant, which is one of the most relevant and sound families of related-key derivation functions [4]. In other words, we investigate the existence of related-key distinguishers involving keys k and $k' = k + \delta$.

In this context, the mapping $\phi : x \mapsto P(x) + x + P(0)$ and the set $\mathrm{Im}(\phi) = \{x + P(x) + P(0), x \in \mathbb{F}_2^\kappa\}$ play an important role. Let N denote the size of this set. We have $N \leq 2^{\kappa-1}$ since both x and $P(x)$ have the same image under ϕ and are distinct because P has no fixed points. Then, ϕ defines an equivalence relation on the keys, namely the key space is partitioned into N equivalence classes $\mathcal{K}_\delta := \{k \ : k + P(k) = \delta\}$. Each of these classes corresponds to a potential class of weak keys that may result from the existence of a related-key distinguisher involving keys k and $k' = k + \delta$. All these key classes have size at least 2, and their average size is $2^\kappa/N$.

So, there is a trade-off between two quantities: the maximal size of a key class $\mathcal{K}_\delta$ and the minimum weight of the set $\{\delta : \mathcal{K}_\delta \neq \emptyset\}$. In the following, the relation between these two quantities is investigated from a theoretical point of view, first when P has degree 1, and then for some particular nonlinear mappings. Later, in Section 4, some concrete constructions of key-alternating reflection ciphers will be presented in which the minimum weight of $\{\delta : \mathcal{K}_\delta \neq \emptyset\}$ affects the existence of efficient related-key distinguishers.

3.2 When P is affine

When P has degree 1, all non-empty key classes $\mathcal{K}_\delta$ are affine subspaces of $\mathbb{F}_2^\kappa$ of the same dimension, since they are all cosets of $\mathrm{Ker}\,\phi$. Therefore, the minimal

possible dimension for the key classes is $(\kappa+1)/2$ (see Prop. 1). But, we can also show that the minimum weight of $\{x+P(x)\}$ is upper-bounded by the dimension of the non-empty $\mathcal{K}_\delta$. Moreover, it is possible to characterize all involutions P which achieve this bound.

Proposition 2 *Let P be an affine involution over $\mathbb{F}_2^\kappa$ without fixed points. Let p denote the dimension of the non-empty sets $\mathcal{K}_\delta = \{x \ : x + P(x) = \delta\}$. Then, $p > \kappa/2$, and*

$$\min_{x \in \mathbb{F}_2^\kappa} wt(x + P(x)) \leq p \ .$$

Proof Let $\phi : x \mapsto P(x)+x+P(0)$ and $\mathcal{C}$ be the code corresponding to $\mathrm{Im}(\phi)$. Then, all sets $\mathcal{K}_\delta = \{x \ : x+P(x) = \delta\}$ are cosets of $\mathrm{Ker}\,\phi$, implying that $p = \dim \mathrm{Ker}\,\phi = \kappa - \dim \mathcal{C}$. Moreover, the minimum weight of $\{(x + P(x)), x \in \mathbb{F}_2^\kappa\} = P(0) + \mathcal{C}$ is equal to the Hamming distance between $P(0)$ and $\mathcal{C}$, where $P(0) \notin \mathcal{C}$. The highest possible value for $d_H(P(0), \mathcal{C})$ corresponds to the covering radius of $\mathcal{C}$, which is a linear code of length κ and dimension $(\kappa - p)$. And, it is well-known that the covering radius of a linear code of length κ and dimension $(\kappa - p)$ does not exceed $\kappa - (\kappa - p) = p$, see *e.g.* Proposition 2 in [8]. □

The following proposition now characterizes the affine involutions for which the previous upper-bound is tight.

Proposition 3 *Let κ and p be two integers, $\kappa < 2p$. The permutation P is an affine involution over $\mathbb{F}_2^\kappa$ such that*

$$\min_{x \in \mathbb{F}_2^\kappa} wt(x + P(x)) = p \text{ and } \dim\{x \ : x + P(x) = \delta\} = p, \ \forall \delta \in \mathrm{Im}(P + \mathrm{Id})$$

if and only if, up to a permutation of the coordinates of x and of $P(x)$,

$$P(x) = x + xM + P(0) \text{ with } M = \begin{pmatrix} ZB & ZBZ & 0 \\ B & BZ & 0 \\ C & CZ & 0 \end{pmatrix}$$

where Z is a $(\kappa - p) \times t$ matrix, $0 \leq t \leq \kappa - p$, having t distinct nonzero rows, all of weight 1, B is a $t \times (\kappa - p)$ matrix, C is a $(p - t) \times (\kappa - p)$ matrix such that $\mathrm{rank}\, M = \kappa - p$, $\mathbf{1}B + \mathbf{1}C = 0$ and $P(0) = \left(u, \overline{Zu}, \mathbf{1}\right)$ with $u \in \mathbf{F}_2^{\kappa-p}$, and $\mathbf{1}$ denotes the all-one word.

Proof First, we prove that M and $P(0)$ should have the prescribed form. Let $\phi : x \mapsto P(x) + x + P(0)$. Since $\dim\{x \ : x + P(x) = \delta\} = p$, $\mathcal{C} = \mathrm{Im}\,\phi$ is a linear subspace of $\mathbb{F}_2^\kappa$ of dimension $(\kappa - p)$. Let G be a $(\kappa - p) \times \kappa$ matrix whose rows form a basis of $\mathcal{C}$. Up to a permutation of the coordinates, we can assume that the first $(\kappa - p)$ columns of G are linearly independent. Thus we can choose

$$G = (\mathrm{Id}_{\kappa-p}, R) \ ,$$

for some $(\kappa-p)\times p$ matrix R. Then, $\mathcal{C}$ corresponds to all words x such that $xH = 0$, for

$$H = \begin{pmatrix} R \\ \mathrm{Id}_p \end{pmatrix} \ .$$

Now, by hypothesis, there exists some element $x_0 = P(0) \in \mathbb{F}_2^\kappa$ such that the minimum weight of $(x_0 + \mathcal{C})$ equals p. This equivalently means that there exists

some $s_0 \in \mathbb{F}_2^p$ such that, for all $y \in \mathbb{F}_2^\kappa$ with $wt(y) < p$, we have $yH \neq s_0$. Indeed, by setting $s_0 := x_0 H$, we have that for each $x \in \mathbb{F}_2^\kappa$, $xH = s_0$ if and only if $x \in x_0 + \mathcal{C}$. Then, if $y \in \mathbb{F}_2^\kappa$, with $wt(y) < p$, we have $y \notin x_0 + \mathcal{C}$, or equivalently $yH \neq s_0$. Clearly, s_0 should be the all-one vector. If not, i.e. if $wt(s_0) < p$, then $y = (0, \ldots, 0, s_0)$, satisfies $wt(y) < p$ and $yH = s_0$. Moreover, all rows of R should have weight at most 1. Otherwise, if there is a row of weight $w > 1$ in R, then s_0 can be obtained by summing this row and $(p - w)$ rows from the lower part of H, implying that $yH = s_0$ for some y of weight $(p - w + 1) < p$. Let now t denote the number of nonzero distinct rows in R, $0 \leq t \leq \kappa - p$. Since each row has weight 1, R has exactly $(p - t)$ columns which vanish. Then, we can rearrange the last p columns of matrix G such that $R = (Z, 0)$ where Z is a $(\kappa - p) \times t$ matrix whose rows have weight one. By definition of M, $\mathcal{C} = \operatorname{Im} \phi$ is the linear subspace spanned by the rows of M. We then deduce that each row of M is of the form $(u, uZ, 0)$, $u \in \mathbb{F}_2^{\kappa - p}$. Therefore, we can decompose

$$M = \begin{pmatrix} A & AZ & 0 \\ B & BZ & 0 \\ C & CZ & 0 \end{pmatrix} ,$$

where each row and each column in the matrix is decomposed as an element in $\mathbb{F}_2^{\kappa-p} \times \mathbb{F}_2^t \times \mathbb{F}_2^{p-t}$. Moreover, P is an involution without fixed points if and only if $\operatorname{Im} \phi \subset \operatorname{Ker} \phi$ and $P(0) \in \operatorname{Ker} \phi \setminus \operatorname{Im} \phi$. Any element in $\operatorname{Im} \phi$, i.e., any word $x = (u, uZ, 0)$ must then satisfy $xM = 0$. We have

$$(u, uZ, 0)\, M = (uA + uZB, (uA + uZB)Z, 0) ,$$

implying that $A + ZB = 0$. Moreover, $P(0)$ should be such that $P(0)H$ is the all-one vector. Thus, $P(0)$ belongs to the coset of $\mathcal{C}$ defined by the vector having its first $(\kappa - p)$ coordinates equal to 0 and its last p coordinates equal to 1, i.e.,

$$P(0) = (u, uZ + \mathbf{1}, \mathbf{1}) .$$

The condition $P(0) \in \operatorname{Ker} \phi$ corresponds to $uZB + (uZ + \mathbf{1})B + \mathbf{1}C = \mathbf{1}B + \mathbf{1}C = 0$. Then, P has the prescribed form. Finally, it is easy to check that any M and $P(0)$ with the prescribed form define an involution having the required properties. Indeed, P is an involution without fixed points since $\operatorname{Im} \phi \subset \operatorname{Ker} \phi$ due to the structure of M, and $P(0) \in \operatorname{Ker} \phi \setminus \operatorname{Im} \phi$. Moreover, any element $y \in \{x + P(x),\ x \in \mathbb{F}_2^\kappa\}$ can be written as $y = (u, uZ + \mathbf{1}, \mathbf{1})$. Its weight equals $wt(y) = wt(u) + (t - wt(uZ)) + p - t$. Since uZ corresponds to the sum of $wt(u)$ rows of Z and each row of Z has weight 1, we deduce that $wt(uZ) \leq wt(u)$, implying that $wt(y) \geq p$. □

Example 1 Let κ and p be two integers with $p > \kappa/2$. We consider the mappings defined in the previous proposition with parameter $t = 0$. Then, we have

$$M = \begin{pmatrix} 0 & 0 \\ C & 0 \end{pmatrix}$$

where C is a $p \times (\kappa - p)$ matrix of full rank and with columns of even Hamming weight (*i.e.*, $\mathbf{1}C = 0$). Let γ_i be the i-th column of C. Then, up to a permutation of the coordinates of x and z, P is defined by $P(x_1, \ldots, x_\kappa) = (z_1, \ldots, z_\kappa)$ with

$$z_i = \begin{cases} x_i + \gamma_i \cdot (x_{\kappa-p+1}, \ldots, x_\kappa) + \alpha_i & \text{for } 1 \leq i \leq \kappa - p \\ x_i + 1 & \text{for } \kappa - p < i \leq \kappa \end{cases} ,$$

where $\alpha_i \in \mathbb{F}_2$ for $1 \leq i \leq \kappa - p$. It can be checked that, for any linearly independent vectors $\gamma_i \in \mathbb{F}_2^p$, $1 \leq i \leq \kappa - p$, of even Hamming weight, this mapping is an involution, that all non-empty sets $\{x : x + P(x) = \delta\}$ have dimension p and all elements $x + P(x)$ have Hamming weight at least p.

Coupling mappings based on bit permutations.

In the particular case where the coupling mapping is defined by $P(k) = kM + \alpha$, where M is a permutation matrix, we can show that the bound of Prop. 2 is not tight. However, we can precisely determine the minimal (and maximal) weight of $\{k + P(k),\ k \in \mathbb{F}_2^\kappa\}$.

Proposition 4 *Let π be an involution of $\{1, \ldots, \kappa\}$ with $f \geq 1$ fixed points and M the corresponding $\kappa \times \kappa$ permutation matrix. Let $\alpha \in \mathrm{Ker}(M + \mathrm{Id})$. Then,*

$$\forall k \in \mathbb{F}_2^\kappa,\ \ wt(\alpha_{FP}) \leq wt(k + kM + \alpha) \leq \kappa - f + wt(\alpha_{FP})$$

where α_{FP} denotes the f-bit binary word equal to the restriction of α to the coordinates corresponding to the fixed points of π.

Proof Let us number the positions as in the proof of Lemma 1 and such that the first f positions correspond to the fixed points of π. Let $p' = \frac{\kappa}{2} - \frac{f}{2}$ be the number of cycles of length 2 of π. Then, from Lemma 1, we have

$$\mathrm{Im}(M + \mathrm{Id}) = \{(0, \ldots, 0, x_1, x_1, x_2, x_2, \ldots, x_{p'}, x_{p'}),\ (x_1, \ldots, x_{p'}) \in \mathbb{F}_2^{p'}\}$$

and $\mathrm{Ker}(M + \mathrm{Id})$ is the subspace of dimension $f + p' = \frac{\kappa + f}{2}$ of all words

$$(b_1, \ldots, b_p, a_1, a_1, a_2, a_2, \ldots, a_{p'}, a_{p'})\ .$$

Thus, for any k, $k(M + \mathrm{Id}) + \alpha$ has weight $wt(\alpha_{FP})$ on its first f positions, and weight between 0 and $(\kappa - f)$ on the other ones, with both bounds being tight. □

Then, when $k \mapsto kM$ is a bit permutation with $f \geq 1$ fixed points, all key classes have size $2^{\frac{\kappa+f}{2}}$, and the minimum weight of $k + kM + \alpha$ is equal to $wt(\alpha_{FP}) \leq f$. Therefore, the bound of Proposition 2 is not tight (except when $\pi = \mathrm{Id}$ and $\alpha = \mathbf{1}$): the optimal trade-off between the two quantities cannot be achieved by bit permutations. However, the values of the two quantities obtained for some bit permutations may be considered as reasonable when a lightweight coupling mapping is required (such examples will be provided in Section 4.2).

3.3 When P is nonlinear

If we want to reduce the size of all key classes to guarantee that any related-key distinguisher defines a very few weak keys only, we need to choose a nonlinear coupling mapping since the key classes for an affine coupling mapping have size at least $2^{\frac{\kappa+1}{2}}$. We then study the trade-offs between the maximal size of a key class and the minimal weight of $(k + P(k))$ which are achieved by some particular families of nonlinear coupling mappings. As we will see, some of these mappings are of theoretical interest only since their implementation cost is too high for a practical use within a lightweight block cipher. However, investigating non-linear permutations permits to obtain a better idea of the bounds that can be in general achieved by coupling permutations.

3.3.1 Inverse mapping.

The inverse mapping over the field with 2^κ elements provides a nice example of an involution where the size of the key classes is minimal. However, it has two fixed points (0 and 1) which must be excluded.

Proposition 5 *Let ψ be any isomorphism from $\mathbb{F}_{2^\kappa}$ into $\mathbb{F}_2^\kappa$, and $x_0 = \psi(1)$. Let P be the permutation of $\mathbb{F}_2^\kappa$ defined by*

$$P(x) = \psi\left[\left(\psi^{-1}(x)\right)^{2^\kappa-2}\right] .$$

Then, P is an involution without fixed points over $\mathbb{F}_2^\kappa \setminus \{0, x_0\}$, and for any δ, the set $\mathcal{K}_\delta = \{x : x + P(x) = \delta\}$ has size either 0 or 2.

Moreover, for any $\kappa \geq 5$, there exists some ψ such that

$$\min_{x \neq 0, x_0} wt(x + P(x)) \geq 2 .$$

Proof P is an involution since $(2^\kappa - 2)^2 \equiv 1 \bmod (2^\kappa - 1)$ (*i.e.*, the inverse function is an involution). Moreover, any nonzero fixed point x of P should be such that $y = \psi^{-1}(x)$ satisfies $y^{2^\kappa-2} = y$ which is equivalent to $y^2 = 1$. This equation does not have any solution when $y \notin \mathbb{F}_2$ (*i.e.*, when $x \notin \{0, x_0\}$).

Similarly, any nonzero element x in the key class $\mathcal{K}_\delta = \{x : x + P(x) = \delta\}$ should be such that $y = \psi^{-1}(x)$ satisfies

$$y + y^{2^\kappa-2} = \psi^{-1}(\delta) .$$

Since $y \neq 0$, this is equivalent to $y^2 + \delta' y + 1 = 0$ where $\delta' = \psi^{-1}(\delta)$. Moreover, δ' is nonzero because the class $\{x : x + P(x) = 0\}$ is equal to $\{0, x_0\}$. Then, this quadratic equation has 2 solutions if $\mathrm{Tr}(\delta'^{-1}) = 0$, and no solution otherwise.

It follows that the minimal weight of $x + P(x)$ when $x \in \mathbb{F}_2^\kappa \setminus \{0, x_0\}$ corresponds to the minimum weight of $\delta \neq 0$ such that $\mathrm{Tr}(\left[\psi^{-1}(\delta)\right]^{2^\kappa-2}) = 0$. Then, we have that this minimum weight is at least 2 if and only if all vectors $x \in \mathbb{F}_2^\kappa$ of weight 1 are such that $\mathrm{Tr}(\left[\psi^{-1}(x)\right]^{2^\kappa-2}) = 1$. An equivalent condition is that there exists a basis $\{b_1, \ldots, b_\kappa\}$ of $\mathbb{F}_{2^\kappa}$ such that $\mathrm{Tr}(b_i^{-1}) = 1$ for all $1 \leq i \leq \kappa$. In particular, if $\{b_1, \ldots, b_\kappa\}$ is a normal basis, *i.e.*, $b_i = b^{2^{i-1}}$, then $\mathrm{Tr}(b_i^{-1})$ takes the same value for all elements in the basis. Therefore, any normal basis $\{b, \ldots, b^{2^{\kappa-1}}\}$ of $\mathbb{F}_{2^\kappa}$ such that $\mathrm{Tr}(b^{-1}) = 1$ leads to an isomorphism ψ for which the minimal weight of $x + P(x)$ is at least two.

For any element $\alpha \in \mathbb{F}_{2^\kappa}^*$, $\mathrm{Tr}(\alpha)$ is the sum of all conjugates of α. Since the minimal polynomial m_α of α is the product of all $(X - \alpha^{2^i})$, it is clear that $\mathrm{Tr}(\alpha)$ is the coefficient of the monomial of degree $(\deg(m_\alpha) - 1)$ in m_α. Moreover, the minimal polynomial of α^{-1} is the reciprocal of the minimal polynomial of α. We then deduce that $\mathrm{Tr}(\alpha^{-1})$ is the coefficient of the monomial of degree 1 in m_α. The existence of a normal basis satisfying the requirements is equivalent to the existence of a normal element b in $\mathbb{F}_{2^\kappa}$ such that the coefficient of degree 1 of its minimal polynomial is equal to 1. It has been proved in [12] (see also [18, Theorem 2.20]) that such an element always exists for $\kappa \geq 5$. □

Example 2 For $\kappa = 8$, we define ψ by $x = \sum_{i=0}^{7} x_i \alpha^{2^i} \mapsto (x_0, \ldots, x_7)$ where α is a root of the primitive polynomial $X^8 + X^7 + X^6 + X^5 + X^2 + X + 1$. Indeed, $\{\alpha^{2^i}, 0 \leq i \leq 7\}$ is a basis of $\mathbb{F}_{2^8}$. Then, it can be checked that the minimum weight of $(x + P(x))$, for $P(x) = \psi\left[\left(\psi^{-1}(x)\right)^{254}\right]$ is equal to 2.

3.3.2 A general construction.

Another technique consists in constructing an appropriate nonlinear involution by $P = S \circ M \circ S^{-1}$ where M is an affine involution without fixed points as described in the previous section, and S is a nonlinear permutation with good differential properties. More precisely, we focus on the differential uniformity of S, which is the maximal number of solutions $x \in \mathbb{F}_2^\kappa$ for an equation $S(x + a) + S(x) = b$, $a, b \in \mathbb{F}_2^\kappa$ and $a \neq 0$ [23].

Proposition 6 *Let M be an affine involution of $\mathbb{F}_2^\kappa$ without fixed points with* $\dim \mathrm{Im}(M + \mathrm{Id}) = p$. *Let S be a permutation of $\mathbb{F}_2^\kappa$ with differential uniformity $\delta(S)$. Then, $P = S \circ M \circ S^{-1}$ is an involution without fixed points and satisfies*

$$\max_{\delta \in \mathbb{F}_2^\kappa} \#\{x : x + P(x) = \delta\} \leq 2^p \delta(S)$$

and

$$\min_{x \in \mathbb{F}_2^\kappa} wt(x + P(x)) \geq \min\left\{wt(x) : x \in \bigcup_{a \in \mathrm{Im}(M+\mathrm{Id})} \mathrm{Im}(D_a S)\right\},$$

where $D_a S : x \mapsto S(x + a) + S(x)$.

Most notably, if $M(x) = x + \alpha$ for some $\alpha \in \mathbb{F}_2^\kappa \setminus \{0\}$, we have

$$\max_{\delta \in \mathbb{F}_2^\kappa} \#\{x : x + P(x) = \delta\} \leq \delta(S)$$

and

$$\min_{x \in \mathbb{F}_2^\kappa} wt(x + P(x)) \geq \min\left\{wt(x) : x \in \mathrm{Im}(D_\alpha S)\right\}.$$

Proof It is clear that P is an involution without fixed points if and only if M is an involution without fixed points. Moreover, there is a one-to-one correspondence between both sets $\{x : x + P(x) = \delta\}$ and $\{y : S(y) + S \circ M(y) = \delta\}$. The set $\{y : S(y) + S \circ M(y) = \delta\}$ is included within the set

$$\bigcup_{a \in \mathbb{F}_2^\kappa} \left\{y : (M + \mathrm{Id})(y) = a \text{ and } S(y) + S(y + a) = \delta\right\}.$$

Then, we directly deduce the bounds on the cardinality of $\{y : S(y) + S \circ M(y) = \delta\}$, and on the minimal weight of $(S(y) + S \circ M(y))$. □

Example 3 We choose

$$S(x) = \psi\left[\left(\psi^{-1}(x)\right)^{2^\kappa - 2}\right]$$

where ψ is the isomorphism from $\mathbb{F}_{2^\kappa}$ into $\mathbb{F}_2^\kappa$ defined by a normal basis $\{a, a^2, \ldots, a^{2^{\kappa-1}}\}$ with $\mathrm{Tr}(a^{-1}) = 1$. Such a basis exists for any $\kappa \geq 5$ as detailed in the proof of Proposition 5. For $x_0 = \psi(1)$,

$$P(x) = S\left(S(x) + x_0\right)$$

is an involution over $\mathbb{F}_2^\kappa$ without fixed points and satisfies

$$\max_{\delta \in \mathbb{F}_2^\kappa} \#\{x : x + P(x) = \delta\} = \begin{cases} 2 & \text{if } \kappa \text{ is odd} \\ 4 & \text{if } \kappa \text{ is even} \end{cases} \quad \text{and} \quad \min_{x \in \mathbb{F}_2^\kappa} wt(x + P(x)) \geq 2 \; .$$

The fact that P is an involution without fixed points and the maximal size of a key class are derived from the previous proposition, since the inverse function over $\mathbb{F}_{2^\kappa}$ is differentially 2-uniform (resp. 4-uniform) if κ is odd (resp. even) [23]. Moreover, this bound is tight since there is a one-to-one correspondence between the elements in $\{x : x + P(x) = x_0\}$ and the solutions z of $(z+1)^{2^\kappa - 2} + z^{2^\kappa - 2} = 1$. The number of solutions of this last equation is 2 if κ is odd and 4 if κ is even.

Also, the minimal weight of $(x + P(x))$ is the minimal weight of any element in the image set of the derivative $D_{x_0}S$. Then, it corresponds to the minimal weight of $\psi(y)$ for $y \in \{(z+1)^{2^\kappa - 2} + z^{2^\kappa - 2},\ z \in \mathbb{F}_{2^\kappa}\}$. By using the same technique as in the proof of Proposition 5, we get that

$$\{(z+1)^{2^\kappa - 2} + z^{2^\kappa - 2}\} = \{x \in \mathbb{F}_{2^\kappa} : \mathrm{Tr}(x^{-1}) = 0\} \; .$$

By definition of ψ, the elements δ of weight 1 in $\mathbb{F}_2^\kappa$ satisfy $y = \psi^{-1}(\delta) = a^{2^i}$ for some $0 \leq i \leq \kappa - 1$, implying that $\mathrm{Tr}(y^{-1}) = \mathrm{Tr}(a^{-1}) = 1$. Therefore, these elements $y = \psi^{-1}(\delta)$ do not belong to $\{(z+1)^{2^\kappa - 2} + z^{2^\kappa - 2},\ z \in \mathbb{F}_{2^\kappa}\}$, which equivalently means that the elements δ of weight 1 do not belong to the image set of the derivative $D_{x_0}S$.

We will see now how the coupling permutations investigated in this section can be used inside some cryptographic primitives. We will focus in particular on the case of key-alternating block ciphers.

4 The Key-Alternating Block Cipher Case

In the rest of the paper we will concentrate on block ciphers and more precisely on key-alternating ciphers. Having block ciphers with the reflection property has obvious interest for some cryptographic applications running in constraint environments. The recent design of the block cipher PRINCE raised several questions about the design principles of such ciphers. One such question is related to the key size of the cipher. In particular, the coupling mapping chosen in PRINCE limits the key size to the block size, which is too small in most lightweight ciphers. The approach used in PRINCE for doubling the key length consists in using a whitening key which is independent from the key of the inner cipher. However, this solution is not completely satisfactory because the resulting security level does not correspond to what is usually expected from the key size. In this section we analyze alternative solutions for constructing a key-alternating reflection cipher whose key is twice as long as the block size.

We start by introducing a general construction for key-alternating reflection ciphers, which is used in PRINCE. This structure is shown below. It is composed of a number of round permutations, $R_1, \ldots, R_r$ (and their inverses) along with an unkeyed involution R_M in the middle of the structure. We furthermore assume that all the round-keys k_i are derived from a master key k.

Not only PRINCE follows this structure, but also several other block ciphers. For instance, some alternating-key ciphers with involutive round permutations are

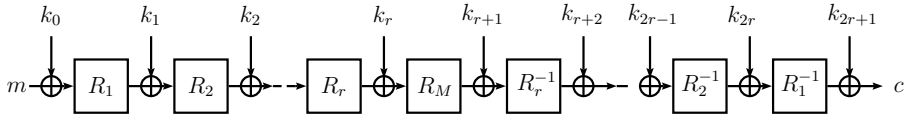

Fig. 2 General construction for a key-alternating reflection cipher.

of the previous form. Examples include Anubis [2] and Khazad [3] with an even number of rounds (the middle involutive transformation M then corresponds to the function named θ in both ciphers), and also ICEBERG [25] with an even number of rounds (in this case M corresponds to the linear layer). It is worth noticing that, although they follow the construction depicted in Figure 2, these three block ciphers are not reflection ciphers because of their key schedule. Only their variants with independent round keys can be seen as reflection ciphers.

Compared to the classical case where all round permutations are involutive, the general construction depicted in Figure 2 requires both R_i and R_i^{-1} to be implemented. Therefore, this generalization is of practical interest in the case of an unrolled implementation only, in particular when a low latency is needed, which is for example the case of all applications with real-time requirements [22]. The fact that the round permutations are not similar does not then affect the implementation cost of the cipher. In this context, there is no reason to limit ourselves to involutive round permutations.

4.1 Two constructions with $2n$-Bit Key and n-Bit Block

In the following we consider the structure depicted in Figure 2 for the special situation of an n-bit block cipher with a $2n$-bit key. In the rest of the paper, involutions are denoted by P (or P_i for some integer i) while mappings with no particular property are denoted with an F. Moreover, when the involution P is affine, we denote by L its linear part.

4.1.1 Construction 1.

We split the $2n$-bit master key into two halves $k = (k_0, k_1)$ and use as a coupling mapping the permutation

$$P(k_0, k_1) = (F_0(k_0, k_1), F_1(k_0, k_1)) \ .$$

In other words, F_0 and F_1 denote the restrictions of P to the first and second half of the output respectively. Then, we define the subkeys as follows:

- for $0 \leq i \leq r$, $k_i = k_0$ if i is even and $k_i = k_1$ if i is odd;
- for $r + 1 \leq i \leq 2r + 1$, $k_i = F_1(k)$ if i is even and $k_i = F_0(k)$ if i is odd.

An important security parameter of this construction is the number of information bits corresponding to the first and the last-round keys: this is the number of key bits which need to be guessed in order to peel off one round at both ends. Then, a strategy for attacking the $(2r + 1)$-round cipher consists in guessing the first and last round keys and in attacking the $(2r - 1)$ middle rounds in order

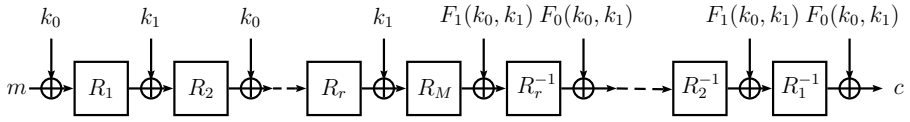

Fig. 3 Construction 1: a reflection cipher with $2n$-bit key and n-bit block with coupling mapping $P(k_0, k_1) = (F_0(k_0, k_1), F_1(k_0, k_1))$.

to recover the remaining key bits. Therefore, if the amount of key guessing corresponding to the extremal rounds is much smaller than the overall key size, we must ensure that attacking $(2r - 1)$ rounds is infeasible. Such a situation usually imposes to increase the number of rounds compared to the n-bit key variant, which is highly unsuitable in the context of unrolled implementations, for instance for low-latency ciphers. An example of such a situation is the lightweight cipher LED-128 for which the first and last round keys are similar and cover half of the key size. For this reason, LED-128 has 16 more rounds (i.e., four steps) than its 64-bit variant, as explained by the designers [16, Section 3.1].

We need therefore to determine the number of different values of the pair $(k_0, F_0(k_0, k_1))$, when the vector (k_0, k_1) takes all the possible 2^{2n} values. This number corresponds to

$$\sum_{k_0 \in \mathbb{F}_2^n} \#\,\mathrm{Im}(F_0(k_0, .))$$

where $F_0(k_0, .)$ is the mapping $k_1 \mapsto F_0(k_0, k_1)$. In particular, the amount of key-guessing for this pair of subkeys is maximal and equals to $2n$ bits if and only if $k_1 \mapsto F_0(k_0, k_1)$ is a permutation of $\mathbb{F}_2^n$ for every possible $k_0 \in \mathbb{F}_2^n$. At the other extreme, the amount of key-guessing is only n bits if and only if F_0 is independent from k_1. This situation occurs for instance when the coupling mapping P operates on the two halves of its input separately:

$$P(k_0, k_1) = (P_0(k_0), P_1(k_1)) \,,$$

where P_0 and P_1 are two permutations of $\mathbb{F}_2^n$.

4.1.2 Construction 2.

As previously explained, if $P(k_0, k_1) = (P_0(k_0), P_1(k_1))$, the amount of key-guessing for the first and last round keys corresponds to n bits only. But, the previous construction can be slightly modified in order to increase this number: the first subkey is replaced by $(k_0 + k_1)$ and the last one is now replaced by $(P_0(k_0) + P_1(k_1))$, as depicted below.

Then, we can prove that this second construction increases the amount of key-guessing, which is strictly greater than n bits in the following two cases: if $P_0 = P_1$ and P_0 is nonlinear, or if P_0 and P_1 are two distinct affine permutations. This is detailed in the following two propositions.

Proposition 7 *Let P_0 be an involution of $\mathbb{F}_2^n$. Then, the number of different values of the pair $(k_0 + k_1, P_0(k_0) + P_0(k_1))$, when (k_0, k_1) takes all the possible 2^{2n} values is*

$$\sum_{a \in \mathbb{F}_2^n} \#\,\mathrm{Im}(D_a P_0) \,,$$

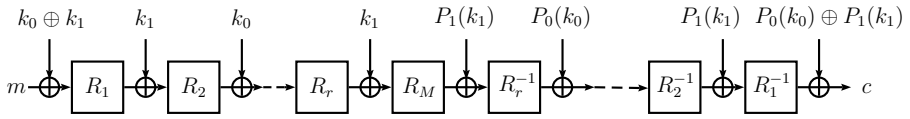

Fig. 4 Construction 2: a reflection cipher with $2n$-bit key and n-bit block with coupling mapping $P(k_0, k_1) = (P_0(k_0), P_1(k_1))$.

where $D_a P_0 : x \mapsto P_0(x + a) + P_0(x)$. *This number is strictly greater than* 2^n *if and only if* $\deg P_0 > 1$.

Proof Let $a = k_0 + k_1$. Then, we need to determine the number of different values of $(a, P_0(k_1 + a) + P_0(k_1)) = (a, D_a P_0(k_1))$ where (a, k_1) takes all possible values in $\mathbb{F}_2^{2n}$. For each $a \in \mathbb{F}_2^n$, the number of values taken by $D_a P_0(k_1)$ when k_1 varies is the cardinality of the image set of $D_a P_0$. Moreover, this number equals 2^n if and only if each $D_a P_0$ is a constant function. It is well-known that a function having all its derivatives constant is a function of degree at most 1. □

When both P_0 and P_1 are affine but distinct, the amount of key-guessing is given by the following proposition.

Proposition 8 *Let* P_0 *and* P_1 *be two affine involutions of* $\mathbb{F}_2^n$. *Then, the number of different values of the pair* $(k_0 + k_1, P_0(k_0) + P_1(k_1))$, *when* (k_0, k_1) *takes all the possible* 2^{2n} *values is* $2^{n+\nu}$ *where*

$$\nu = \mathrm{rank}(P_0 \circ P_1 + \mathrm{Id}) = \mathrm{rank}(P_0 + P_1) \ .$$

Proof Obviously, the number of different values of the quantity $(k_0 + k_1, P_0(k_0) + P_1(k_1))$ is equal to the number of different values of its linear part, that is of $(k_0 + k_1, L_0(k_0) + L_1(k_1))$ where $L_i(x) = P_i(x) + P_i(0)$. Let $a = k_0 + k_1$. The previous couple can then be written as $(a, L_0(a + k_1) + L_1(k_1)) = (a, L_0(a) + (L_0 + L_1)(k_1))$. The number of values taken by this pair then corresponds to $2^{n+\nu}$ where $\nu = \mathrm{rank}(P_0 + P_1)$. Equivalently, it corresponds to the rank of

$$k_1 \mapsto P_0(P_0(k_1) + P_1(k_1)) = k_1 + P_0(P_1(k_1)) \ .$$

□

We now consider the particular case where the linear parts of P_0 and P_1 are defined by two bit permutations π_0 and π_1. In order to guarantee that P is an involution, we need π_0 and π_1 to be involutions (cf. Corollary 1). Then, the amount of key-guessing is related to the number of fixed points of π_0 and of π_1, as stated in the following lemma (the proof is given in Appendix A).

Lemma 2 *Let* π_0 *and* π_1 *be two involutions of* $\{1, \ldots, n\}$ *and* L_0 *and* L_1 *be the corresponding permutations of* $\mathbb{F}_2^n$. *Then, the rank of* $L_0 \circ L_1 + \mathrm{Id}$ *is upper bounded by* $n - (f_0 + f_1)/2$ *where* f_i *is the number of fixed points of* π_i.

Thus, in order to ensure a high cost for guessing the first and the last round keys, the number of fixed points of π_0 and of π_1 has to be minimal. However, given Proposition 4, this comes at the price that $(k + P(k))$ may have a low Hamming weight.

For these two constructions, it can be shown that the minimum Hamming weight of $(k+P(k))$ has a practical impact on the security of the cipher. First, this parameter affects the success probability of the so-called reflection attack [20]. Such an attack has been presented in [24] against PRINCE, but it can be easily generalized to both constructions. It consists in constructing some particular differential characteristics starting from the middle round. Indeed, a differential characteristic with probability 1 is exhibited in [24] for the middle round, as well as another simple characteristic for the three middle rounds (see Figure 5). Extending any of these characteristics to one round involves then a differential of the round function whose output difference corresponds to one of the two halves of $(k + P(k))$, i.e., with the notation used in Construction 1, either to $(k_0 + F_0(k_0, k_1))$ or to $(k_1 + F_1(k_0, k_1))$. In the particular case of PRINCE, the round permutation cor-

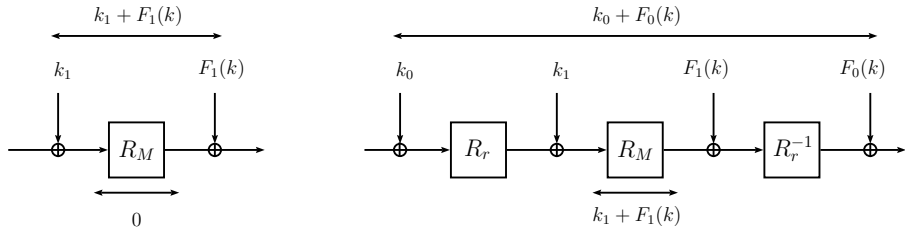

Fig. 5 Middle differential characteristics exploited in the attack of [24] on reduced-round PRINCE.

responds to the concatenation of four smaller permutations operating on 16 bits. Therefore, the number of 16-bit words which are not zero in $(k_0+F_0(k_0, k_1))$ (or in $(k_1 + F_1(k_0, k_1))$) corresponds to the number of active 16-bit permutations for the considered differential and gives a lower bound on the number of active Sboxes in this round. This explains why, in the particular case of PRINCE with coupling permutation $P(k) = k+\alpha$, the attack presented in [24] works much better for some α which has a lower weight than for the value proposed by the designers of PRINCE. The minimum weight of $(k_0 + F_0(k_0, k_1))$ and $(k_1 + F_1(k_0, k_1))$ has also an impact on the probability of related-key differential characteristics in both constructions. This will be discussed in more details in the next section, in the particular case of the PRINCE round function.

4.2 PRINCESSes

In this section we define some variants of PRINCE which differ from their key schedule only. The focus of this work is on the reflection property and not on the round function itself. We therefore chose to simply adopt the round function of PRINCE. Then, a cipher is said to follow the PRINCESS construction if it operates on 64-bit inputs with a 128-bit key, and follows Construction 2 with 5 rounds R_i, $1 \leq i \leq 5$, an unkeyed middle round R_M, and then the inverses of the five R_i (see Figures 3 and 4). More precisely, the internal state of the cipher is represented by a 4×16 binary matrix. Each row of this matrix can be seen as a 4-tuple of nibbles. Each of the five round functions R_i is composed of a nonlinear layer S, a linear

layer L, and the addition of a round-constant RC_i. The nonlinear layer S applies the same 4-bit Sbox to the 16 nibbles of the state. Then, the first part L' of the linear layer corresponds to the application of 16 involutive 4-bit transformations, applied in parallel to the 16 columns of the state. This is then followed by a ShiftRows permutation SR of the 16 nibbles, and by the addition of a round-constant. The middle round R_M is equal to $S^{-1} \circ L' \circ S$. We refer to [6] for the complete description of all these building-blocks.

Before presenting our proposals for the key schedule, we first show that, in the reflection cipher obtained by the PRINCESS construction, the probability of a related-key differential distinguisher involving keys k and $P(k)$ is upper-bounded by a quantity which is related to the minimal weight of $SR^{-1}(k_1 + F_1(k_0, k_1))$.

Proposition 9 *Let us consider any cipher following the* PRINCESS *construction. For $\delta \in \mathbb{F}_2^{64}$, $\mathcal{L}_\delta$ denotes the code of length 128 and size 2^{64} formed by all $(x, L(x)+\delta), x \in \mathbb{F}_2^{64}$, where L is the linear layer. Let ω_4 be the smallest possible minimum weight over $\mathbb{F}_2^4$ of all $\mathcal{L}_\delta$ when δ varies in $\{k_1 + F_1(k), k \in \mathbb{F}_2^{128}\}$. Then, any related-key differential characteristic involving keys k and $P(k)$ for this cipher has at least $6\omega_4$ active Sboxes.*

In particular, if any element in $\{SR^{-1}(k_1 + F_1(k)), k \in \mathbb{F}_2^{128}\}$, seen as a 4×4 matrix of nibbles, has no zero column, then any such differential characteristic has at least 24 active Sboxes.

Proof Let $\mathcal{F}_x = S \circ \mathrm{Add}_x \circ L \circ S$ denote two rounds in the PRINCESS construction without the second linear layer and key addition. Then, PRINCESS can be decomposed as a succession of 3 such functions, and of their inverses, all separated by an affine transformation, namely:

$$\mathcal{F}^{-1}_{F_1(k)+RC_1} \circ A_1^{-1} \circ \mathcal{F}^{-1}_{F_1(k)+RC_3} \circ A_2^{-1} \circ \mathcal{F}^{-1}_{F_1(k)+RC_5} \circ L' \circ \mathcal{F}_{k_1+RC_5} \circ A_2 \circ \mathcal{F}_{k_1+RC_3} \circ A_1 \circ \mathcal{F}_{k_1+RC_1} .$$

In this description, the two Sbox-layers composing the middle round of the cipher are involved in two different $\mathcal{F}_x$.

Then, the total number of active Sboxes in the whole related-key differential characteristic is lower bounded by 6 times the minimum number of active Sboxes within a related-key differential characteristic for a single function $\mathcal{F}_x$ (or $\mathcal{F}_x^{-1}$). Therefore, for a fixed k, this number corresponds to the minimum distance over $\mathbb{F}_2^4$ between two words of the form $(x, L(x) + k_1 + RC)$ and $(y, L(y) + F_1(k) + RC)$, or equivalently to the minimum weight over $\mathbb{F}_2^4$ of the word $(x+y, L(x+y)+k_1+F_1(k))$ which belongs to the code $\mathcal{L}_{k_1+F_1(k)}$. By taking the minimum over all possible keys, we obtain that any such related-key differential characteristic for $\mathcal{F}_x$ has at least ω_4 active Sboxes. It is worth noticing that this property holds even if the input (resp. the output) of $\mathcal{F}_x$ is zero. Indeed, the number of active Sboxes then corresponds to the weight of $(0, k_1 + F_1(k))$ (resp. to the weight of $(L^{-1}(k_1 + F_1(k)), 0)$), which belongs to the code $\mathcal{L}_{k_1+F_1(k)}$. It follows that $\omega_4 = 0$ if and only if there exists a key k such that $k_1 + F_1(k) = 0$.

In the particular case of PRINCESS, L consists of a first permutation L', composed of 4 parallel 16-bit transformations $L_0, \ldots, L_3$, and followed by the nibble permutation SR. Since the permutation SR commutes with the nonlinear layer S, we obtain that

$$\mathcal{F}_x = S \circ \mathrm{Add}_x \circ SR \circ L' \circ S = SR \circ S \circ \mathrm{Add}_{SR^{-1}(x)} \circ L' \circ S.$$

Then, ω_4 is the sum of the corresponding values $\omega_4^{(i)}$, $0 \leq i \leq 3$, for the four 16-bit transformations $\mathrm{Add}_{\delta_i} \circ L_i$ where δ_i is the i-th column of nibbles in $SR^{-1}(k_1 + F_1(k))$. It follows that $\omega_4^{(i)} \geq 1$ unless the corresponding code contains the all-zero codeword, or equivalently unless $\delta_i = 0$. We directly deduce that $\omega_4 \geq 4$ if all δ_i are nonzero. □

As an illustration of our results, we now present several key-schedules, corresponding to different coupling mappings, one in each of the three categories studied in the previous sections. They lead to different trade-offs between the three quantities studied in the paper: the amount of key-guessing for the first and last round keys, the minimal number of active Sboxes in a related-key differential characteristic involving k and $P(k)$, and the maximal size of a key equivalence class $\mathcal{K}_\delta = \{k : k + P(k) = \delta\}$, i.e. of a class of weak keys coming from such a distinguisher. The three different trade-offs we obtain are summarized in Table 1.

Table 1 Summary of the studied quantities for the proposed alternative key-schedules.

	PRINCE	nonlinear	affine $p = 33$	bit permutation
key-guessing	128	119.9	126	112
max size of $\mathcal{K}_\delta$	2^{128}	2^{32}	2^{66}	2^{80}
minimum number of active Sboxes		≥ 24	≥ 72	≥ 48

As a comparison, we recall that in PRINCE the amount of key-guessing is maximal (128 bits) and all keys belong to the same key class. This last property has been exploited in the reflection attack on round-reduced versions of PRINCE presented in [24], as well as on the multiple-differential attack described in [7]. Moreover, since all rounds in PRINCE except the first and last ones depend on a 64-bit key only, the security level of the cipher is limited by the security offered by the FX construction. In particular, there exist generic attacks with time complexity T and data complexity D such that $DT = 2^{126}$ [6,19]. Moreover, in some variants of these attacks, the main computational effort corresponds to a precomputation phase [15]. The memory complexity can also be reduced as shown in [10]. We aim then at achieving a higher security with some alternative key schedules.

4.2.1 A nonlinear coupling mapping.

We use a coupling mapping of the form $P(k_0, k_1) = (P_0(k_0),\ P_0(k_1))$, and the key-schedule then corresponds to Construction 2, i.e., the first round-key equals $k_0 + k_1$ and the last one equals $P_0(k_0) + P_0(k_1)$. The permutation P_0 is defined by the construction presented in Section 3.3: $P_0 = S' \circ M' \circ S'^{-1}$ where M' is an affine involution of $\mathbb{F}_2^{64}$ without fixed points and S' is a nonlinear permutation with a low differential uniformity. In order to reduce the implementation cost of the nonlinear layer, we choose for S' the function corresponding to 8 parallel applications of the inverse function over $\mathbb{F}_{2^8}$, and $M'(x) = x + \alpha$ where $\alpha = (x_0, \ldots, x_0)$ with $x_0 = \texttt{0xff} = \psi(1)$ and ψ is the isomorphism from $\mathbb{F}_{2^8}$ into $\mathbb{F}_2^8$ defined as in Example 2. More precisely, each of the 8-bit permutations defining S' is applied to two nibbles

of the internal state belonging to the same right-leaning diagonal, i.e., on two nibbles whose images by SR^{-1} belong to the same column.

Since S' consists of 8 copies of the inverse function over $\mathbb{F}_{2^8}$, its differential uniformity is $\delta(S') = 4^8 = 2^{16}$. From Proposition 6, the corresponding coupling mapping P is an involution without fixed points and satisfies

$$\max_{\delta \in \mathbb{F}_2^{128}} \#\{x : x + P(x) = \delta\} = (2^{16})^2 = 2^{32} .$$

This is much smaller than what we can obtain with any affine involution, since any affine involution over $\mathbb{F}_2^{128}$ leads to key classes of size at least 2^{65} (see Prop. 2).

P_0 is composed of eight copies of the same permutation σ of $\mathbb{F}_2^8$, where $\sigma(x) = s(s(x) + \texttt{0xff})$ and s corresponds to the inversion over $\mathbb{F}_{2^8}$. Then, we have

$$\min_{x \in \mathbb{F}_2^8} wt(x + \sigma(x)) = 2 ,$$

as discussed in Example 3. In particular, this implies that any byte in a right-leaning diagonal of $x + P_0(x)$ is non-zero for all $x \in \mathbb{F}_2^{64}$, or equivalently any byte in a column of $SR^{-1}(x + P_0(x))$ is non-zero. We then deduce from Proposition 9 that any related-key differential distinguisher for the cipher has at least 24 active Sboxes. The amount of key-guessing corresponding to the first and last round keys is given by Proposition 7. We have checked that $\sum_{a \in \mathbb{F}_2^8} \#\,\mathrm{Im}(D_a\sigma) = 2^{14.98}$, implying that the total amount of key-guessing is $8 \times 14.98 = 119.84$ bits.

4.2.2 An affine coupling mapping.

In this example we use a coupling mapping of the form $P(k_0, k_1) = (P_0(k_0), P_1(k_1))$ and follow equally Construction 2. We construct both affine involutions P_0 and P_1 by following Example 1 in Section 3. More precisely, we number the bits of the internal state as depicted in Figure 6.

63	59	55	51	47	43	39	35	31	27	23	19	15	11	7	3
62	58	54	50	46	42	38	34	30	26	22	18	14	10	6	2
61	57	53	49	45	41	37	33	29	25	21	17	13	9	5	1
60	56	52	48	44	40	36	32	28	24	20	16	12	8	4	0

Fig. 6 Bit numbering of the internal state.

For this numbering, we define P_0 by $P_0(x_1, \ldots, x_{64}) = (z_1, \ldots, z_{64})$ with

$$z_i = \begin{cases} x_i + x_{i+8} + x_{i+9} & \text{if } 0 \leq (i \bmod 16) \leq 6 \\ x_i + x_{i+8} + x_{i+17} & \text{if } (i \bmod 16) = 7 \text{ and } i \neq 55 \\ x_i + 1 & \text{if } 8 \leq (i \bmod 16) \leq 15 \text{ or } i = 55 \end{cases}$$

and P_1 by $P_1(x_1, \ldots, x_{64}) = (z'_1, \ldots, z'_{64})$ with

$$z'_i = \begin{cases} x_i + 1 & \text{if } 0 \leq (i \bmod 16) \leq 7 \text{ or } i = 8 \\ x_i + x_{i-8} + x_{i-17} & \text{if } (i \bmod 16) = 8 \text{ and } i \neq 8 \\ x_i + x_{i-8} + x_{i-9} & \text{if } 9 \leq (i \bmod 16) \leq 15 \end{cases}$$

Up to a reordering of the bit positions, both constructions P_i, $i = 0, 1$, correspond to Example 1: P_0 and P_1 are involutions without fixed points with

$$\#\{x : x + P_i(x) = \delta\} = \{0, 2^{33}\} \text{ for all } \delta \in \mathbb{F}_2^{64} \text{ and } \min_{x \in \mathbb{F}_2^{64}} wt(x + P_i(x)) = 33.$$

Let now compute the value $\omega_4^{(i)}$ defined in the proof of Proposition 9, i.e., the minimum weight of $(x, L_i(x) + \delta_i), x \in \mathbb{F}_2^{16}$ where $L_0, \ldots, L_3$ are the four 16-bit involutions defining L', and δ_i is the i-th column of nibbles in $SR^{-1}(k_1 + P_1(k_1))$. By definition, the first two bits of any nibble in $k_1 + P_1(k_1)$ are equal to 1. Since SR^{-1} is a nibble-wise operation, the same property holds for $SR^{-1}(k_1 + P_1(k_1))$. It follows that the first two binary columns of δ_i correspond to the all-one vector. Then, $(0, \delta_i)$ and $(L_i(\delta_i), 0)$ have always 4 nonzero nibbles because L_i maps an all-one column to an all-one column. This implies that $\omega_4^{(i)} \geq 2$. Moreover, if x has a single nonzero nibble, then its binary columns are either the all-zero column or one fixed column of weight 1. The columns of $L_i(x)$ are then either the all-zero column or a column of weight 3 but all these columns of weight 3 must be different. Since δ_i has two all-one columns, it follows that $L_i(x) + \delta_i$ cannot have a single nonzero nibble, implying that $\omega_4^{(i)} > 2$. From Proposition 9, we deduce that $\omega \geq 12$, and then that any related-key differential characteristic involving k and $P(k)$ has at least 72 active Sboxes.

Finally it can be verified that $\nu = \text{rank}(P_0 + P_1) = 62$, thus from Proposition 8 the amount of key-guessing is equal to $64 + 62 = 126$ bits.

4.2.3 A coupling mapping based on a bit permutation.

We propose here a coupling mapping $P(k_0, k_1) = (P_0(k_0), P_1(k_1))$ based on a bit permutation that offers a different trade-off among the three quantities investigated in this section. As proved in Section 3.2, bit permutations do not achieve the bound of Proposition 2: for a given dimension of the key classes, the minimum weight of $(x + P(x))$ is much smaller than the one we can obtain with a general affine mapping. However, their low implementation cost makes them very attractive for lightweight designs.

In this variant, P_0 and P_1 are affine mappings $P_i(x) = xM_i + \alpha_i$ where the M_i are the permutation matrices corresponding to two bit permutations π_0 and π_1 with at least one fixed point (see Corollary 1).

We choose

$$\begin{aligned}
\pi_1 = {} & (0)(1)(2)(3)(4,8)(5,12)(6,10)(7,14)(9,13)(11,15) \\
& (16)(17)(18)(19)(20,24)(21,28)(22,26)(23,30)(25,29)(27,31) \\
& (32)(33)(34)(35)(36,40)(37,44)(38,42)(39,46)(41,45)(43,47) \\
& (48)(49)(50)(51)(52,56)(53,60)(54,58)(55,62)(57,61)(59,63) \\
\pi_0 = {} & (0,63)(1,9)(2,13)(3,11)(4)(5)(6)(7)(8,12)(10,14) \\
& (15,16)(17,25)(18,29)(19,27)(20)(21)(22)(23)(24,28)(26,30) \\
& (31,32)(33,41)(34,45)(35,43)(36)(37)(38)(39)(40,44)(42,46) \\
& (47,48)(49,57)(50,61)(51,59)(52)(53)(54)(55)(56,60)(58,62)
\end{aligned}$$

where the bits are numbered as in Figure 6. The bit permutation π_1 (resp. π_0) has exactly 16 fixed points corresponding to the first bit (resp. second bit) of each nibble in the state.

We have

$$\begin{aligned}\pi_0 \circ \pi_1 = &(0,63,51,59)(1,9,2,13)(3,11,16,15)(4,12,5,8)(6,14,7,10)\\ &(17,25,18,29)(19,27,32,31)(20,28,21,24)(22,30,23,26)\\ &(33,41,34,45)(35,43,48,47)(36,44,37,40)(38,46,39,42)\\ &(49,57,50,61)(52,60,53,56)(54,62,55,58)\end{aligned}$$

which implies according to Lemma 2 that $\text{rank}(M_0 \circ M_1 + \text{Id})$ equals 48. Thus, guessing the first and the last-round keys corresponds to guessing $64 + 48 = 112$ information bits of the 128-bit key.

We furthermore have to specify the two constants α_i such that $\alpha_i \in \text{Ker}(M_i + \text{Id})$ and $\alpha_i \notin \text{Im}(M_i + \text{Id})$. These constants are given below, where the rightmost bit is the bit number 0. All these constants are chosen such that the first bit of each nibble of α_1 and the second bit of each nibble of α_0 is equal to 1.

$$\alpha_1 = (1001110001101111110010011001111101100011100111110101010111111111)$$
$$\alpha_0 = (0011100111111101111001001111010110100010111101100001101111111010$$

We can easily show that each $\omega_4^{(i)}$, i.e., the minimum weight of $\{(x, L_i(x) + \delta_i), x \in \mathbb{F}_2^{16}\}$, is at most 2 for any $\delta = SR^{-1}(k_1 + P_1(k_1))$. Indeed, $(0, \delta_i)$ and $(L_i(\delta_i), 0)$ have always four nonzero nibbles because the first bit of each nibble in δ_i equals 1, implying that this also holds for $L_i(\delta_i)$. Then, $\omega_4^{(i)} \geq 2$, implying that $\omega_4 \geq 8$. From Proposition 9, we deduce that any related-key differential characteristic involving k and $P(k)$ has at least 48 active Sboxes.

Finally, the size of the key classes is here larger than in the previous variants. Indeed, all key classes are of size $(2^{\frac{64+16}{2}})^2 = 2^{80}$.

From the properties of these three different proposals which are summarized in Table 1, we observe that the variant with the nonlinear key-schedule has much smaller key classes. But this variant is not realistic when a low-cost implementation is required. The two other key-schedules can be implemented with very few resources since they correspond to very sparse affine permutations over $\mathbb{F}_2^{64}$. In particular, the key-schedule based on bit permutations appears to be very efficient. These two key-schedules then provide interesting variants of PRINCE at a marginal implementation overhead. In particular, their security level is not limited by the generic attack against the FX-construction (in other words the attacks presented in [15,10] do not apply). Moreover, based on our theoretical results, we are able to exhibit some lower bounds on the complexity of some attacks, e.g., on the probability of any related-key differential characteristic obtained by comparing the encryption and the decryption functions.

5 Conclusion

In this work, we tried to answer some open questions related to the design of a family of ciphers, for which the set of encryption functions is identical to the

set of decryption functions. In particular, we focused on the design of what we called the coupling permutation. A coupling permutation P applied to a master key k, makes, in our context, encryption with $P(k)$ identical to decryption with k. Questions on the design of the coupling permutation of reflection block ciphers were raised after the design of the lightweight block cipher PRINCE. Indeed, in PRINCE, the coupling permutation chosen by the designers does not seem optimal and its impact on the security of the cipher has been questioned. After presenting some general properties of coupling permutations, we analyzed the case of PRINCE and came up with some alternative key-schedules for this cipher. Each key schedule presents a different trade-off of the studied security properties and the choice of which one to choose should depend on the security requirements settled by the designers and the target implementation cost.

References

1. Albrecht, M.R., Farshim, P., Paterson, K.G., Watson, G.J.: On Cipher-Dependent Related-Key Attacks in the Ideal-Cipher Model. In: Fast Software Encryption - FSE 2011, *Lecture Notes in Computer Science*, vol. 6733, pp. 128–145. Springer (2011)
2. Barreto, P., Rijmen, V.: The ANUBIS Block Cipher. Submission to the NESSIE project (2000). URL https://www.cosic.esat.kuleuven.be/nessie/workshop/submissions.html
3. Barreto, P., Rijmen, V.: The Khazad Legacy-level Block Cipher. Submission to the NESSIE project (2000). URL https://www.cosic.esat.kuleuven.be/nessie/workshop/submissions.html
4. Bellare, M., Kohno, T.: A Theoretical Treatment of Related-Key Attacks: RKA-PRPs, RKA-PRFs, and Applications. In: Advances in Cryptology - EUROCRYPT 2003, *Lecture Notes in Computer Science*, vol. 2656, pp. 491–506. Springer (2003)
5. Biryukov, A.: DES-X (or DESX). In: H.C.A. van Tilborg, S. Jajodia (eds.) Encyclopedia of Cryptography and Security (2nd Ed.), p. 331. Springer (2011)
6. Borghoff, J., Canteaut, A., Güneysu, T., Kavun, E.B., Knežević, M., Knudsen, L.R., Leander, G., Nikov, V., Paar, C., Rechberger, C., Rombouts, P., Thomsen, S.S., Yalçın, T.: PRINCE - A Low-latency Block Cipher for Pervasive Computing Applications. In: Advances in Cryptology - ASIACRYPT 2012, *Lecture Notes in Computer Science*, vol. 7658, pp. 208–225. Springer (2012)
7. Canteaut, A., Fuhr, T., Gilbert, H., Naya-Plasencia, M., Reinhard, J.: Multiple differential cryptanalysis of round-reduced PRINCE. In: Fast Software Encryption - FSE 2014, *Lecture Notes in Computer Science*, vol. 8540, pp. 591–610. Springer (2014)
8. Cohen, G.D., Karpovsky, M.G., Jr., H.F.M., Schatz, J.R.: Covering Radius - Survey and Recent Results. IEEE Transactions on Information Theory **31**(3), 328–343 (1985)
9. Coppersmith, D.: The Real Reason for Rivest's Phenomenon. In: Advances in Cryptology - CRYPTO'85, *Lecture Notes in Computer Science*, vol. 218, pp. 535–536. Springer (1985)
10. Dinur, I.: Cryptanalytic Time-Memory-Data Tradeoffs for FX-Constructions with Applications to PRINCE and PRIDE. In: Advances in Cryptology - EUROCRYPT 2015, Part I, *Lecture Notes in Computer Science*, vol. 9056, pp. 231–253. Springer (2015)
11. Even, S., Mansour, Y.: A Construction of a Cipher From a Single Pseudorandom Permutation. In: Advances in Cryptology - ASIACRYPT '91, *Lecture Notes in Computer Science*, vol. 739, pp. 210–224. Springer (1993)
12. Fan, S., Wang, X.: Primitive Normal Polynomials with the Specified Last Two Coefficients. Discrete Mathematics **309**(13), 4502 – 4513 (2009)
13. Feistel, H., Notz, W., Smith, J.: Some Cryptographic Techniques for Machine-To-Machine Data Communications. Proceedings of the IEEE **63**(11), 1545–1554 (1975)
14. Flajolet, P., Sedgewick, R.: Analytic Combinatorics. Cambridge University Press (2009). URL http://algo.inria.fr/flajolet/Publications/book.pdf
15. Fouque, P., Joux, A., Mavromati, C.: Multi-user Collisions: Applications to Discrete Logarithm, Even-Mansour and PRINCE. In: Advances in Cryptology - ASIACRYPT 2014, Part I, *Lecture Notes in Computer Science*, vol. 8873, pp. 420–438. Springer (2014)

16. Guo, J., Peyrin, T., Poschmann, A., Robshaw, M.J.B.: The LED Block Cipher. In: Cryptographic Hardware and Embedded Systems - CHES 2011, *Lecture Notes in Computer Science*, vol. 6917, pp. 326–341. Springer (2011)
17. Harris, D.G.: Critique of the Related-Key Attack Concept. Des. Codes Cryptography **59**(1-3), 159–168 (2011)
18. Huczynska, S.: Existence Results for Finite Field Polynomials with Specified Properties. In: Finite Fields and Their Applications - Character sums and polynomials, *RSCAM*, vol. 11, pp. 65–87. De Gruyter (2013)
19. Jean, J., Nikolic, I., Peyrin, T., Wang, L., Wu, S.: Security Analysis of PRINCE. In: Fast Software Encryption - FSE 2013, *Lecture Notes in Computer Science*, vol. 8424, pp. 92–111. Springer (2014)
20. Kara, O.: Reflection Cryptanalysis of Some Ciphers. In: Progress in Cryptology - INDOCRYPT 2008, *Lecture Notes in Computer Science*, vol. 5365, pp. 294–307. Springer (2008)
21. Kilian, J., Rogaway, P.: How to protect DES against exhaustive key search (an analysis of DESX). J. Cryptology **14**(1), 17–35 (2001)
22. Kneževic, M., Nikov, V., Rombouts, P.: Low-Latency Encryption - Is "Lightweight = Light + Wait"? In: CHES 2012, *Lecture Notes in Computer Science*, vol. 7428, pp. 426–446. Springer (2012)
23. Nyberg, K.: Differentially Uniform Mappings For Cryptography. In: Advances in Cryptology - EUROCRYPT'93, *Lecture Notes in Computer Science*, vol. 765, pp. 55–64. Springer (1993)
24. Soleimany, H., Blondeau, C., Yu, X., Wu, W., Nyberg, K., Zhang, H., Zhang, L., Wang, Y.: Reflection Cryptanalysis of PRINCE-like Ciphers. In: Fast Software Encryption - FSE 2013, *Lecture Notes in Computer Science*, vol. 8424, pp. 71–91. Springer (2014)
25. Standaert, F.X., Piret, G., Rouvroy, G., Quisquater, J.J., Legat, J.D.: ICEBERG : An Involutional Cipher Efficient for Block Encryption in Reconfigurable Hardware. In: Fast Software Encryption - FSE 2004, *Lecture Notes in Computer Science*, vol. 3017, pp. 279–299. Springer (2004)
26. Youssef, A., Tavares, S., Heys, H.: A New Class of Substitution-Permutation Networks. In: Selected Areas in Cryptography - SAC'96, pp. 132–147 (1996)

A Proof of Lemma 2

Lemma 3 *Let π_0, π_1 be two involutions of $\{1, \ldots, n\}$. Then, each cycle of $\pi_0 \circ \pi_1$ contains either zero fixed points of π_0 and π_1 or exactly two.*

Proof Suppose that a cycle c of $\pi_0 \circ \pi_1$ of length λ contains a fixed point of π_0, say x_0. The proof holds equally for x_0 being a fixed point of π_1. Let us number the successive elements in c by x_i with $-\ell \leq i \leq \ell$ if λ is odd, and with $-\ell < i \leq \ell$ if λ is even, where $x_{i+1} = \pi_0 \circ \pi_1(x_i)$ for all $i \neq \ell$ and $\pi_0 \circ \pi_1(x_\ell) = x_{-\ell}$ if λ is odd and $\pi_0 \circ \pi_1(x_\ell) = x_{-(\ell-1)}$ if λ is even.

Then, we can prove by induction on i that $\pi_0(x_i) = x_{-i}$ for all $0 \leq i \leq \ell$ if λ is odd, and for all $0 \leq i < \ell$ if λ is even. Indeed, this property obviously holds for $i = 0$. Then, the induction step is as follows: from $\pi_0(x_i) = x_{-i}$, we deduce that $x_{-(i+1)} = \pi_1 \circ \pi_0(x_{-i}) = \pi_1(x_i)$. Then, $x_{i+1} = \pi_0 \circ \pi_1(x_i) = \pi_0(x_{-(i+1)})$.

Now, if λ is odd, we have $\pi_0 \circ \pi_1(x_\ell) = x_{-\ell}$, implying that $\pi_1(x_\ell) = \pi_0(x_{-\ell}) = x_\ell$, i.e., x_ℓ is a fixed point of π_1. If λ is even, we use that $\pi_0 \circ \pi_1(x_\ell) = x_{-(\ell-1)}$, implying that $\pi_1(x_\ell) = \pi_0(x_{-(\ell-1)}) = x_{\ell-1}$. Then, it follows that $x_\ell = \pi_0 \circ \pi_1(x_{\ell-1}) = \pi_0(x_\ell)$, i.e. x_ℓ is a fixed point of π_0.

Eventually, we can prove that there is no other fixed point of π_0 or π_1 within the cycle. Indeed, if there exists some $i \neq \{0, \ell\}$ such that $\pi_0(x_i) = x_i$, then we deduce that $x_{-i} = x_i$ which contradicts that all the x_i are distinct. If $\pi_1(x_i) = x_i$ for some $i \neq \{0, \ell\}$, then $x_{i+1} = \pi_0 \circ \pi_1(x_i) = \pi_0(x_i) = x_{-i}$, a contradiction. □

Now, we can prove the following proposition.

Proposition 10 *Let π_0 and π_1 be two involutions of $\{1, \ldots, n\}$ and L_0 and L_1 be the corresponding permutations of $\mathbb{F}_2^n$. Then, the rank of $L_0 \circ L_1 + \mathrm{Id}$ is upper bounded by $n - (f_0 + f_1)/2$ where f_i is the number of fixed points of π_i.*

Proof According to Lemma 1, the rank of $L_0 \circ L_1 + \mathrm{Id}$ is $n - c$, where c is the number of cycles of the permutation $\pi_0 \circ \pi_1$. We know from Lemma 3 that there are four different possibilities for a cycle of $\pi_0 \circ \pi_1$. The first one is that it has exactly two fixed points of π_0, the second one that it has two fixed points of π_1, the third possibility is that it contains a fixed point of π_0 and a fixed point of π_1, and the last one that it contains no fixed points at all. Let us denote by x, y and z the number of cycles of $\pi_0 \circ \pi_1$ in the first three categories. Then, we have

$$2x + z = f_0 \text{ and } 2y + z = f_1 \ .$$

It follows that the number of cycles c of $\pi_0 \circ \pi_1$ satisfies

$$c \geq x + y + z = \frac{f_0 - z}{2} + \frac{f_1 - z}{2} + z = \frac{f_0 + f_1}{2} \ .$$