Reflection Ciphers (Extended abstract)

Christina Boura[1,3], Anne Canteaut[2,3], Lars R. Knudsen[3], and Gregor Leander[4,3]

[1] Université de Versailles Saint-Quentin, France
christina.boura@prism.uvsq.fr
[2] Inria, France
anne.canteaut@inria.fr
[3] DTU, Denmark
lrkn@dtu.dk
[4] Ruhr-Universitt Bochum, Germany
gregor.leander@rub.de

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 show that this coupling permutation must be an involution without fixed points. 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. In particular, we show that, for affine coupling permutations, the resistance to related-key distinguishers is given by some trade-off between the dimension and the covering-radius of some linear codes. Finally, as an illustration, we provide new variants of the block cipher PRINCE with key schedules corresponding to several coupling permutations.

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

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. $\mathrm{Rev}(k_1, \ldots, k_r) = (k_r, \ldots, k_1)$. Feistel ciphers with independent round-keys are the most prominent examples of this construction [10]. 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 [4] 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. 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.

Our Contribution. In this work we study the properties of reflection ciphers and derive 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). 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 focus on key-alternating block ciphers by emphasizing on ciphers with n-bit block size and $2n$-bit key size. The block cipher PRINCE [4] is an example of this family of ciphers. In the approach followed by its designers, the key size is a priori limited to the block size, and the solution chosen for doubling the key size is not optimal and raises security questions [7]. We try here to answer this question by presenting some variants that offer a better security, corresponding to different coupling permutations.

Because of the limited number of pages, most proofs are omitted in this extended abstract.

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

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

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 [11, Page 596]. This weakness is well-known and has been exhibited in several works, including [18]. 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 [6], 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 [3, 15]. This construction (aka the Even-Mansour construction [8]) 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 [4]).

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. By elementary linear algebra, we obtain the following simple characterization of affine involutions without fixed points. 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, P is an involution without any fixed points if and only if $\phi : x \mapsto P(x) + P(0) + x$ satisfies $\operatorname{Im}\phi \subset \operatorname{Ker}\phi$ and $P(0)$ belongs to $\operatorname{Ker}\phi \setminus \operatorname{Im}\phi$.*

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 [17, 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 $\operatorname{Im}\phi \subseteq \operatorname{Ker}\phi$.

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.

Proposition 2. *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 [4] 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 Proposition 2. Indeed, the bit permutation π in the above coupling mapping is only composed of cycles of length 2.

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 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 [4], 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 [2, 13, 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 [2]. 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 p, since they are all cosets of $\operatorname{Ker}\phi$. Therefore, the minimal possible dimension for the key classes is $(\kappa+1)/2$ (see Prop. 1). Moreover, the second quantity, the minimum weight of $\{x + P(x)\} = P(0) + \operatorname{Im}\phi$ is equal to the Hamming distance between $P(0)$ and $\operatorname{Im}\phi$, where $P(0) \notin \operatorname{Im}\phi$. The highest possible value for $d_H(P(0), \operatorname{Im}\phi)$ then corresponds to the covering radius of $\operatorname{Im}\phi$, 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 for example Proposition 2 in [5]. We then deduce the following result.

Proposition 3. *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*

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

Moreover, the affine involutions for which the previous upper-bound is tight can be characterized.

Proposition 4. *Let κ and p be two integers, $\kappa < 2p$. The permutation P is an affine involution over $\mathbb{F}_2^\kappa$ such that*

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

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 $\operatorname{rank} M = \kappa - p$, $\mathbf{1}B + \mathbf{1}C = 0$ 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.

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. 3 is not tight. However, we can precisely determine the minimal (and maximal) weight of $\{k + P(k),\ k \in \mathbb{F}_2^\kappa\}$.

Proposition 5. *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.

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 3 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.

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 $(k + P(k))$ 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 nonlinear permutations permits to obtain a better idea of the bounds that can be in general achieved by coupling permutations.

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 6. *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 $\mathrm{Tr}(\left[\psi^{-1}(\delta)\right]^{-1}) = 0$. 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 $\mathrm{Tr}(\left[\psi^{-1}(x)\right]^{-1}) = 1$. 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 [9] (see also [14, Theorem 2.20]) that such an element always exists for $\kappa \geq 5$. □

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 $a \neq 0$ [16].

Proposition 7. *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

$$\max_{\delta \in \mathbb{F}_2^\kappa} \#\{x : x+P(x) = \delta\} \leq \delta(S) \text{ and } \min_{x \in \mathbb{F}_2^\kappa} wt(x+P(x)) \geq \min\left\{ wt(x),\ x \in \mathrm{Im}(D_\alpha S) \right\}.$$

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 2. 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 6. 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

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

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) [16]. 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 6, 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 $D_{x_0}S$.

4 Some variants of PRINCE

We will see now how the coupling permutations investigated in the previous section can be used for constructing some variants of the block cipher PRINCE. Indeed, the design of PRINCE raised several questions. 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 satisfactory because the resulting security level does not correspond to what is usually expected from the key size [7]. We then analyze alternative solutions for constructing a key-alternating reflection cipher whose key is twice as long as the block size.

Recall that the structure used in PRINCE is as follows: the cipher is composed of a number of round permutations, $R_1, \ldots, R_r$ (and their inverses) along with an unkeyed involution M in the middle of the structure. Now, we construct coupling permutations for reflection ciphers following this structure for the special situation of an n-bit block cipher with a $2n$-bit key.

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:

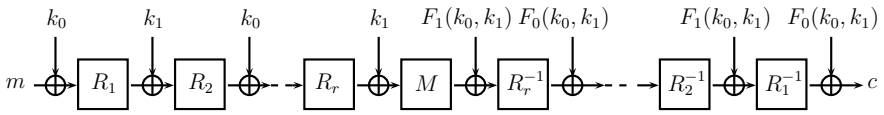

Fig. 1. Construction 1: a reflection cipher with $2n$-bit key and n-bit block with coupling mapping $P(k_0, k_1) = (F_0(k_0, k_1), F_1(k_0, k_1))$.

- 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 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 [12, 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 $\mathbb{F}_2^n$.

Construction 2. 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.

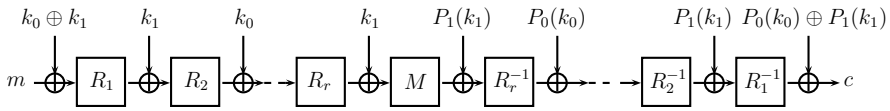

Fig. 2. Construction 2: a reflection cipher with $2n$-bit key and n-bit block with coupling mapping $P(k_0, k_1) = (P_0(k_0), P_1(k_1))$.

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 8. *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*

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

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 9. *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*

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

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 $\nu = \operatorname{rank}(P_0 + P_1)$. 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 2). 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.

Lemma 1. *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 5, this comes at the price that $(k + P(k))$ may have a low Hamming weight.

Based on the previous results, we can then define some variants of PRINCE which differ from their key schedule only. All these variants operate on 64-bit inputs with a 128-bit key, and follow Construction 2 with 5 rounds R_i, $1 \leq i \leq 5$, an unkeyed middle round M, and then the inverses of the five R_i (see Figures 1 and 2). We define three different coupling mappings: a nonlinear permutation of the form $P(k_0, k_1) = (P_0(k_0),\ P_0(k_1))$ where P_0 is defined by the construction presented in Section 3.3; an affine coupling mapping of the form $P(k_0, k_1) = (P_0(k_0), P_1(k_1))$ where both affine involutions P_0 and P_1 are obtained as in Example 1 in Section 3; a coupling mapping based on a bit permutation. The respective properties of these three key-schedules are given in Table 1. 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.

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

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 doesn't seem optimal and its impact on the cipher's security is 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. M. R. Albrecht, P. Farshim, K. G. Paterson, and G. J. Watson. On Cipher-Dependent Related-Key Attacks in the Ideal-Cipher Model. In *Fast Software Encryption - FSE 2011*, volume 6733 of *Lecture Notes in Computer Science*, pages 128–145. Springer, 2011.
2. M. Bellare and T. Kohno. A Theoretical Treatment of Related-Key Attacks: RKA-PRPs, RKA-PRFs, and Applications. In *Advances in Cryptology - EUROCRYPT 2003*, volume 2656 of *Lecture Notes in Computer Science*, pages 491–506. Springer, 2003.
3. A. Biryukov. DES-X (or DESX). In Henk C. A. van Tilborg and Sushil Jajodia, editors, *Encyclopedia of Cryptography and Security (2nd Ed.)*, page 331. Springer, 2011.
4. J. Borghoff, A. Canteaut, T. Gneysu, E. B. Kavun, M. Kneevi, L. R. Knudsen, G. Leander, V. Nikov, C. Paar, C. Rechberger, P. Rombouts, S. S. Thomsen, and T. Yaln. PRINCE - A Low-latency Block Cipher for Pervasive Computing Applications. In *Advances in Cryptology - ASIACRYPT 2012*, volume 7658 of *LNCS*, pages 208–225. Springer, 2012.
5. G. D. Cohen, M. G. Karpovsky, H. F. Mattson Jr., and J. R. Schatz. Covering Radius - Survey and Recent Results. *IEEE Transactions on Information Theory*, 31(3):328–343, 1985.
6. D. Coppersmith. The Real Reason for Rivest's Phenomenon. In *Advances in Cryptology - CRYPTO'85*, volume 218 of *LNCS*, pages 535–536. Springer, 1985.
7. I. Dinur. Cryptanalytic Time-Memory-Data Tradeoffs for FX-Constructions with Applications to PRINCE and PRIDE. In *Advances in Cryptology - EUROCRYPT 2015*, LNCS. Springer, 2015. To appear.
8. S. Even and Y. Mansour. A Construction of a Cipher From a Single Pseudorandom Permutation. In *Advances in Cryptology - ASIACRYPT '91*, volume 739 of *Lecture Notes in Computer Science*, pages 210–224. Springer, 1993.
9. S. Fan and X. Wang. Primitive Normal Polynomials with the Specified Last Two Coefficients. *Discrete Mathematics*, 309(13):4502 – 4513, 2009.
10. H. Feistel, W.A. Notz, and J.L. Smith. Some Cryptographic Techniques for Machine-To-Machine Data Communications. *Proceedings of the IEEE*, 63(11):1545–1554, 1975.
11. P. Flajolet and R. Sedgewick. *Analytic Combinatorics*. Cambridge University Press, 2009.

12. J. Guo, T. Peyrin, A. Poschmann, and M. J. B. Robshaw. The LED Block Cipher. In B. Preneel and T. Takagi, editors, *CHES*, volume 6917 of *Lecture Notes in Computer Science*, pages 326–341. Springer, 2011.
13. D. G. Harris. Critique of the Related-Key Attack Concept. *Des. Codes Cryptography*, 59(1-3):159–168, 2011.
14. S. Huczynska. Existence Results for Finite Field Polynomials with Specified Properties. In *Finite Fields and Their Applications - Character sums and polynomials*, volume 11 of *RSCAM*, pages 65–87. De Gruyter, 2013.
15. J. Kilian and P. Rogaway. How to protect DES against exhaustive key search (an analysis of DESX). *J. Cryptology*, 14(1):17–35, 2001.
16. K. Nyberg. Differentially Uniform Mappings For Cryptography. In *Advances in Cryptology - EUROCRYPT'93*, volume 765 of *LNCS*, pages 55–64. Springer, 1993.
17. H. Soleimany, C. Blondeau, X. Yu, W. Wu, K. Nyberg, H. Zhang, L. Zhang, and Y. Wang. Reflection Cryptanalysis of PRINCE-like Ciphers. In *Fast Software Encryption - FSE 2013*, volume 8424 of *LNCS*, pages 71–91. Springer, 2014.
18. A.M. Youssef, S.E. Tavares, and H.M. Heys. A New Class of Substitution-Permutation Networks. In *Selected Areas in Cryptography - SAC'96*, pages 132–147, 1996.