Reflection ciphers

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

WCC 2015, Paris, France

April 15, 2015

Motivation

One way of reducing the implementation cost of a cipher:

> Minimize the **overhead of decryption** on top of encryption.

The ENIGMA case (when such a feature was essential):

- Use of a reflector.
- $E_k = F_k^{-1} \circ M \circ F_k$, with $M = M^{-1}$.
- E_k is an **involution**.

Why E_k should not be an involution

Fixed points. [Youssef-Tavares-Heys 96]

- A random **permutation** of $\mathbf{F}_2^n$ has 1 fixed point on average.
- A random **involution** of $\mathbf{F}_2^n$ has $2^{\frac{n}{2}} + \mathcal{O}(1)$ fixed points.

In particular, for $E_k = F_k^{-1} \circ M \circ F_k$

E_k has the same cycle structure and the same number of fixed points as M.

- ENIGMA: the reflector has no fixed points.
- DES with a weak key : M is the swapping of the two branches.
  - 2^{32} points [Coppersmith 85]

Use involutional building blocks

$$E_{(k_1,\ldots,k_r)} = F_{k_r} \circ \cdots \circ F_{k_2} \circ F_{k_1},$$

where all F_{k_i} are **involutions**.

Decryption under $(k_1, \ldots, k_r)$ = Encryption under $(k_r, \ldots, k_1)$.

Examples : Feistel ciphers, involutional SPNs, Khazad, ANUBIS, NOEKEON, ICEBERG...

The sequence $k_1, \ldots k_r$ is derived using a **key schedule**.

- Designing a good key schedule is a difficult task.
- Important implementation overhead or extra memory required.

Reflection ciphers

Definition: A cipher E is a reflection cipher if there exists a permutation P, called the coupling permutation such that, for all k

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

Examples

- Feistel cipher with independent round keys

$$P(k_1, \ldots, k_r) = (k_r, \ldots, k_1)$$

- RSA

$$P = \text{inversion modulo } (p-1)(q-1).$$

General properties of the coupling permutation

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

implies that

$$E_k = E_{P^2(k)}$$

Choice of P:

- P should be an involution.
- Fixed points should be avoided.

Example:

$$P(k) = k \oplus \alpha$$

Affine coupling mappings

Proposition: Let P be an affine function of $\mathbf{F}_2^\kappa$. Then, P is an involution without fixed points iff

$$\phi : x \mapsto P(x) + P(0) + x$$

satisfies $\mathsf{Im}(\phi) \subset \mathsf{Ker}(\phi)$ and $P(0)$ belongs to $\mathsf{Ker}(\phi) \setminus \mathsf{Im}(\phi)$.

Bit permutations

Proposition: Les π be a permutation of $\{1, \ldots, \kappa\}$ and M the corresponding permutation matrix. Then, there exists α such that

$$x \mapsto xM + \alpha$$

is an involution without fixed points iff π is an involution with at least one fixed point.

Impact of related-key distinguishers for reflection ciphers

Trivial related-key distinguishers : not considered.

Related-key distinguishers: may have an impact in the single-key model.

A related-key distinguisher for E_k involving two keys k and k', related by $k' = P(k)$ is a distinguisher in the single-key model.

- In scenarios where the attacker has access to both encryption and decryption, related-key distinguishers may have a real impact on the security of the cipher.

Differential related-key distinguishers

Distinguishers involving k and $k' = P(k)$ should be avoided.

Two different approaches:

- Choose P such that the existence of such distinguishers is very unlikely, e.g., such that $k \oplus P(k)$ has always a high weight.
- Choose P such that related-key distinguishers can be exploited for a few k only, e.g., almost $k \oplus P(k)$ differ when k varies.

Trade-off between

$$\min_k wt(k \oplus P(k)) \text{ and } \max_\delta \#\{k \oplus P(k) = \delta\}$$

Different classes for P

We investigated both quantities for the following coupling permutations P:

- affine
- non-linear
- general construction combining both

When P is affine

$$\phi : x \mapsto P(x) + P(0) + x$$

Dimension of key-classes

- All non-empty key classes $K_\delta = \{k : k + P(k) = \delta\}$ are affine subspaces of $\mathbb{F}_2^\kappa$ of the same dimension.
- Minimal possible dimension for the key classes is $\dfrac{\kappa + 1}{2}$.

Minimum Hamming-weight $k + P(k)$

- The minimum Hamming weight of $\{k + P(k)\} = P(0) + \mathrm{Im}(\phi)$ equals the Hamming distance between $P(0)$ and $\mathrm{Im}(\phi)$.
- Equals the covering radius of $\mathrm{Im}(\phi)$ which is a linear code of length κ and dimension $\kappa - p$:

$$\kappa - (\kappa - p) = p.$$

When P is non-linear

If using a linear P, the size of all key classes is relatively high.

Question : How to reduce the size of all key classes for guaranteeing that any related-key distinguisher defines only a very few weak classes?

Study non-linear permutations.

Remark: The implementation cost of some of these mappings is too high for having a practical interest in a lightweight context.

However, it permits to get a better idea of the bounds that can be achieved.

The inverse mapping

Proposition

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

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

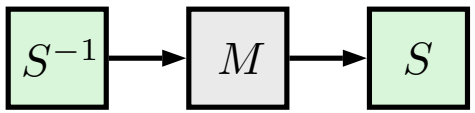
Then, P is an involution without fixed points over $\mathbb{F}_2^\kappa \setminus \{0, x_0\}$, and for any δ, the set $\mathcal{K}_\delta = \{k : k + P(k) = \delta\}$ has size either 0 or 2. Moreover, for any $\kappa \geq 5$, there exists some ψ such that

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

A general construction

$$P = S \circ M \circ S^{-1}$$

where M is an affine involution without fixed points and S is a nonlinear permutation with good differential properties.



If $\dim \mathrm{Im}(M + \mathrm{Id}) = p$, then P is an involution without fixed points with

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

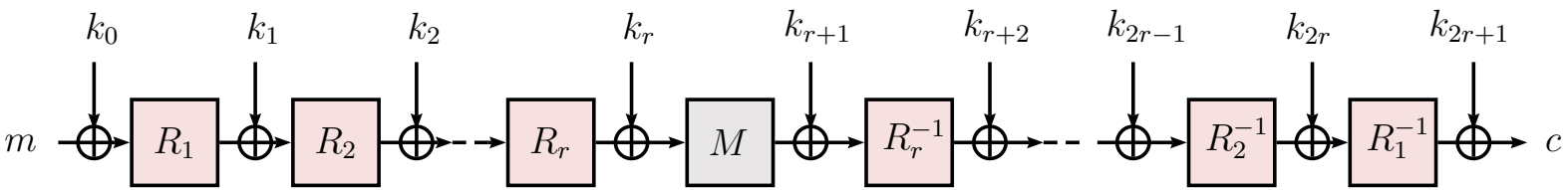
and

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

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

The key-alternating block cipher case

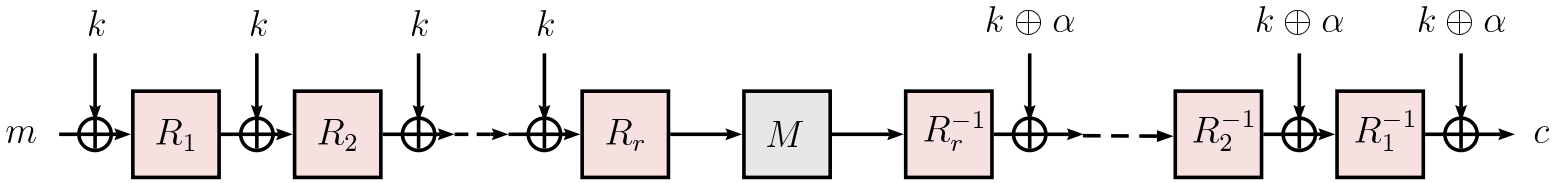
Reflection block ciphers for constraint environments.



PRINCE block cipher

Designed by Borghoff et al. in 2012.

Reflection cipher with $P(k) = k \oplus \alpha$.



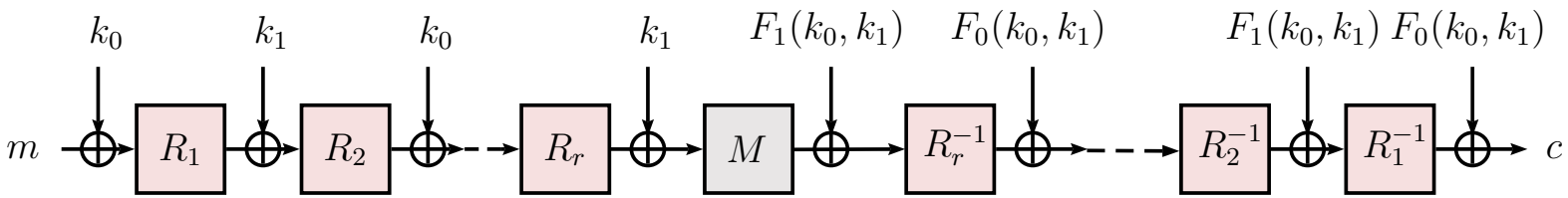
Question raised : How to design such a cipher without limiting the key size to the block size.

The PRINCE approach: Use a whitening key which is independent of the inner cipher key.

A first construction with $2n$-bit key and n-bit block

Split the $2n$-bit master key into two halves $k = (k_0, k_1)$ and use

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



Important security parameter: Number of information bits corresponding to the first and the last round-keys.

Number of information bits of the first and last round-keys

Question: What is the number of different values of

$$(k_0, F_0(k_0, k_1))$$

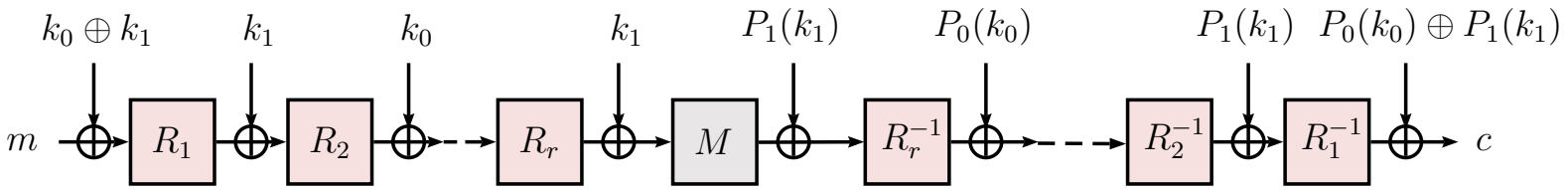
when (k_0, k_1) takes all the possible 2^{2n} values?

The amount of key guessing equals

- $2n$ bits iff $k_1 \mapsto F_0(k_0, k_1)$ is a permutation of $\mathbb{F}_2^n$ for every $k_0 \in \mathbf{F}_2^n$.
- n bits iff F_0 is independent from k_1.
  - $P(k_0, k_1) = (P_0(k_0), P_1(k_1))$

Increase the amount of key guessing

A second construction



The amount of key-guessing is $> n$ in the following two cases:

- If $P_0 = P_1$ and P_0 is non-linear.
- If P_0 and P_1 are two distinct affine permutations.

The case of bit permutations

Let the linear parts L_0 and L_1 of P_0 and P_1 be defined by two bit-permutations π_0 and π_1.

- The amount of key-guessing is related to the number of fixed points of π_0 and π_1.

The rank of $L_0 \circ L_1 + \mathrm{Id}$ is upper bounded by

$$n - \frac{f_0 + f_1}{2}$$

where f_i is the number of fixed points of π_i.

Alternative key schedules for PRINCE

	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 of active Sboxes		≥ 24	≥ 72	≥ 48

Summary

- Analysis the general properties of a coupling permutation.
- Investigation of different families of coupling permutations.
- Investigation of reflection key alternating block ciphers with $2n$-bit key and n-bit block.
- Proposal of alternative key schedules for the PRINCE block cipher.

Summary

- Analysis the general properties of a coupling permutation.
- Investigation of different families of coupling permutations.
- Investigation of reflection key alternating block ciphers with $2n$-bit key and n-bit block.
- Proposal of alternative key schedules for the PRINCE block cipher.

Thanks for your attention!