L'insoutenable légèreté du chiffrement

Anne Canteaut

L’insoutenable légèreté du chiffrement

Anne Canteaut

Inria Paris, EPI SECRET

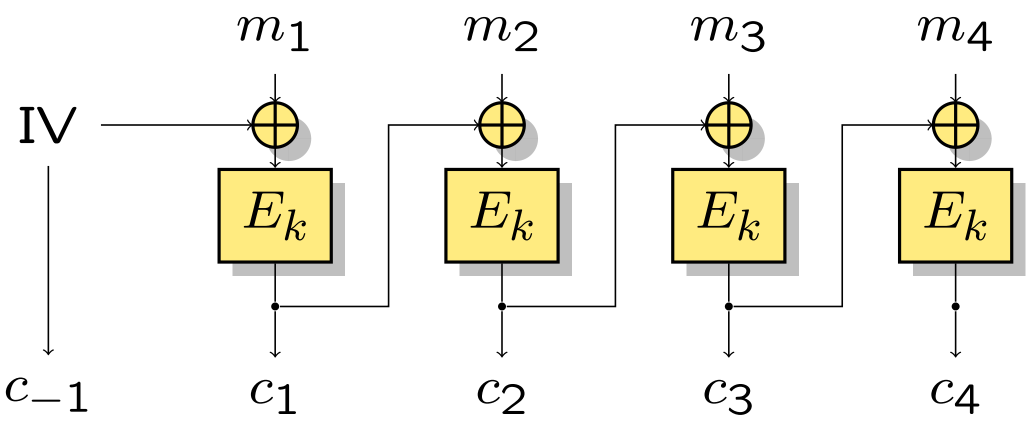
(travaux communs avec C. Beierle, G. Leander et Y. Rotella)

Journées Scientifiques 2018, Bordeaux

Symmetric Encryption Schemes

For encrypting messages of an arbitrary length:

- use a transformation operating on n-bit blocks (block cipher)
- chain the blocks with a mode of operation (CBC, CTR...)



Typical block size:

$$n \in \{128, 64\}$$

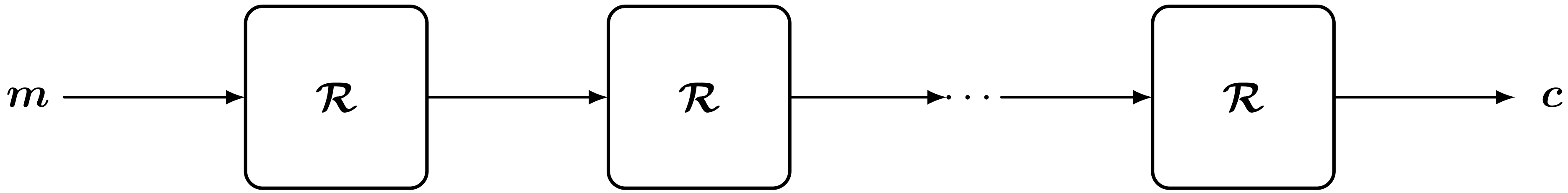
What is a block cipher?

$$E_k : \{0,1\}^n \longrightarrow \{0,1\}^n, \quad n \in \{64, 128\}$$

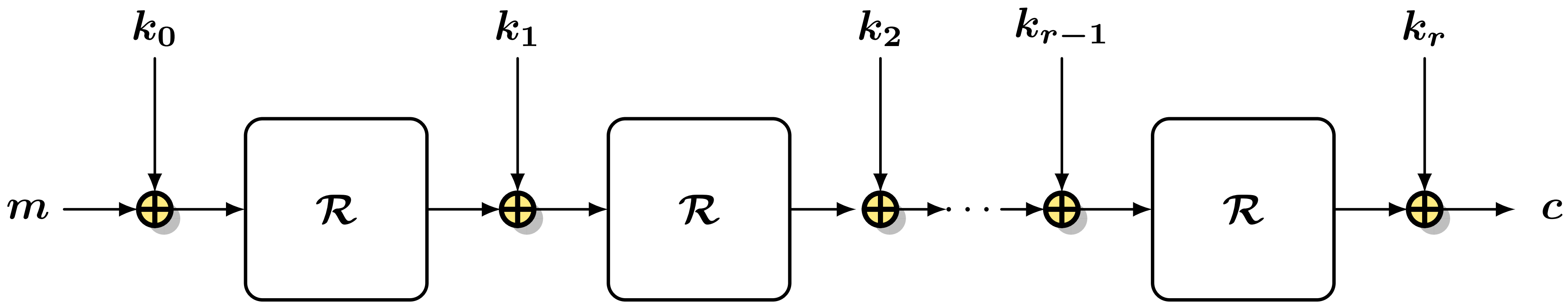
- indistinguishable from a set of randomly chosen permutations of $\{0,1\}^n$
- implementable

$\rightarrow$ Contradiction!

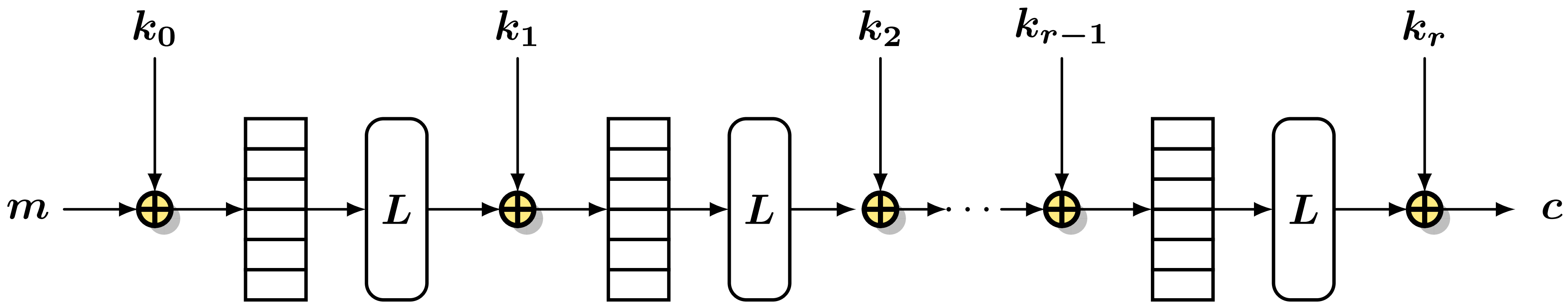
Iterated block ciphers



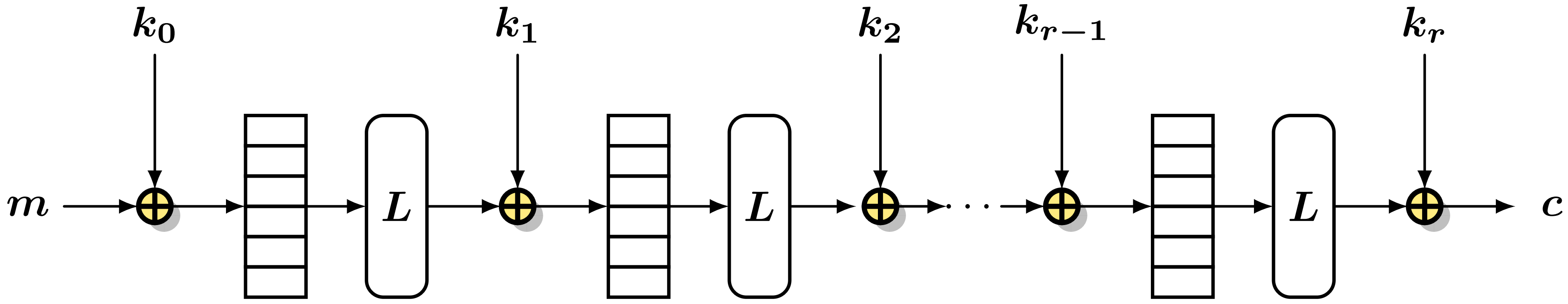
Iterated block ciphers



Iterated block ciphers

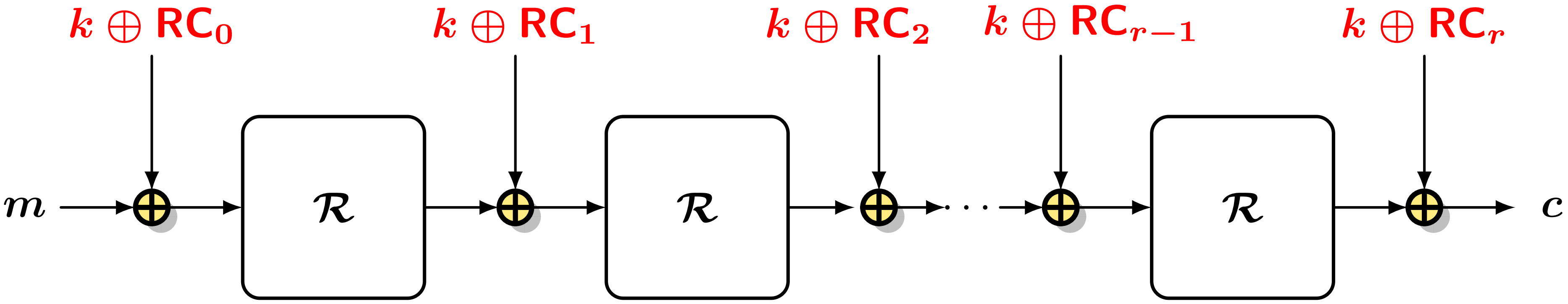


Lightweight block ciphers



- lighter nonlinear functions
- lighter diffusion layers
- simpler key schedules

Lightweight key schedules



where $\mathbf{RC}_0, \mathbf{RC}_1, \ldots, \mathbf{RC}_r$ are fixed round-constants.

Examples:

- PrintCipher [Knudsen et al. 10]
- LED [Guo et al. 11]
- Prince [Borghoff et al. 12]
- Scream and iScream [Grosso et al. 14]
- Midori [Banik et al. 15]
- Skinny and Mantis [Beierle et al. 16]...

Invariant attacks [Todo-Leander-Sasaki 16]

Principle:

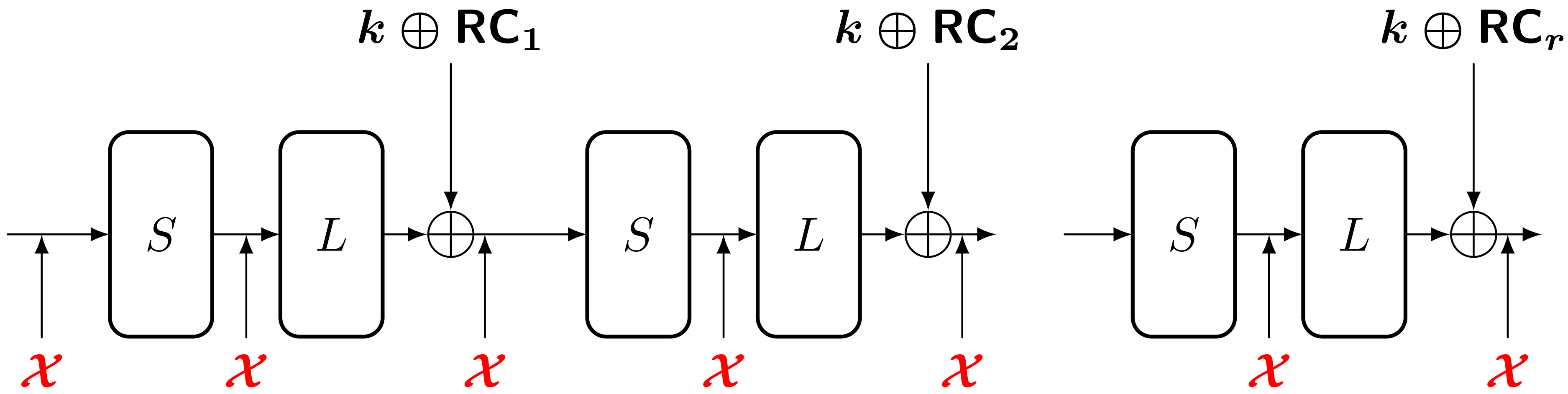
Exhibit a set $\boldsymbol{\mathcal{X}}$ of inputs invariant under $\boldsymbol{E_k}$ for many weak keys.

Ex: Invariant subspace for Midori-64 [Guo et al. 16]

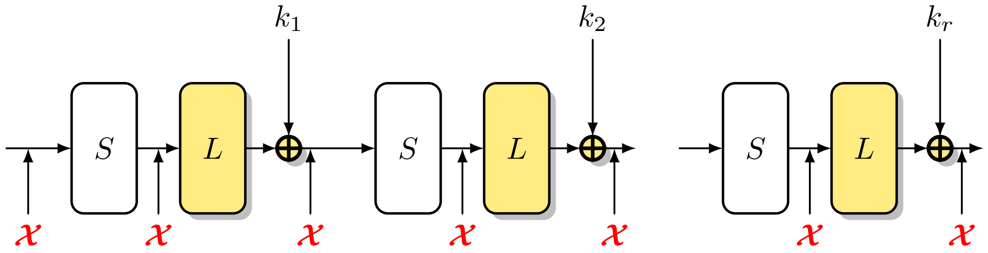
$\boldsymbol{\mathcal{X}} = \{\mathbf{8}, \mathbf{9}\}^{\mathbf{16}}$ is invariant under $\boldsymbol{E_k}$, for any 128-bit key $\boldsymbol{k} \in \{\mathbf{0}, \mathbf{1}\}^{\mathbf{32}}$.

For $\boldsymbol{k} = (\mathbf{1100110011001100}, \mathbf{0011001100110011})$,
$\boldsymbol{m} = \mathbf{9999999999999999}$ leads to the ciphertext $\boldsymbol{c} = \mathbf{8999999988988989}$

Using the same invariant for all layers in an iterated cipher



Finding an $\mathcal{X}$ invariant under all linear layers



$$L(\mathcal{X}) \oplus k_i = \mathcal{X} \text{ and } L(\mathcal{X}) \oplus k_j = \mathcal{X} \Rightarrow \mathcal{X} \oplus k_i = \mathcal{X} \oplus k_j$$

$\mathcal{X}$ is invariant under addition of any $(\mathbf{RC}_i \oplus \mathbf{RC}_j)$

Proposition.

$$\mathbf{LS}(\mathcal{X}) = \{a \in \{0,1\}^n \ : \ (a \oplus \mathcal{X}) = \mathcal{X}\}$$

- $\mathbf{LS}(\mathcal{X})$ is a linear space
- $\mathbf{LS}(\mathcal{X})$ is invariant under L
- $\mathbf{LS}(\mathcal{X})$ contains all $(\mathbf{RC}_i \oplus \mathbf{RC}_j)$

Condition on the existence of invariant sets

$$D := \{(\mathsf{RC}_i \oplus \mathsf{RC}_j),\ \ 0 \le i < j \le r\}$$

$W_L(D) :=$ smallest subspace invariant under L which contains D .

Problem.

Is there a set $\mathcal{X} \subset \{0,1\}^n$ such that $S(\mathcal{X}) = \mathcal{X}$ and
$\mathcal{X}$ is invariant under addition of any element in $W_L(D)$?

Condition on the existence of invariant sets

$$D := \{(\mathsf{RC}_i \oplus \mathsf{RC}_j),\ \ 0 \leq i < j \leq r\}$$

$W_L(D) :=$ smallest subspace invariant under L which contains D .

Problem.

Is there a set $\mathcal{X} \subset \{0,1\}^n$ such that $S(\mathcal{X}) = \mathcal{X}$ and $\mathcal{X}$ is invariant under addition of any element in $W_L(D)$?

No if $W_L(D) = \{0,1\}^n$

Some lightweight ciphers with $n = 64$

Skinny-64-64.

$$D = \{\mathsf{RC}_1 \oplus \mathsf{RC}_{17},\ \mathsf{RC}_2 \oplus \mathsf{RC}_{18},\ \mathsf{RC}_3 \oplus \mathsf{RC}_{19},\ \mathsf{RC}_4 \oplus \mathsf{RC}_{20},\ \mathsf{RC}_5 \oplus \mathsf{RC}_{21}\}$$

$$\dim W_L(D) = 64$$

The round-constants and L guarantee that the attack does not apply.

Prince.

$$D = \{\mathsf{RC}_1 \oplus \mathsf{RC}_2,\ \mathsf{RC}_1 \oplus \mathsf{RC}_3,\ \mathsf{RC}_1 \oplus \mathsf{RC}_4,\ \mathsf{RC}_1 \oplus \mathsf{RC}_5,\ \alpha\}.$$

$$\dim W_L(D) = 56$$

Midori-64.

$$\dim W_L(D) = 16$$

Maximizing the dimension of $W_L(d)$

$$W_L(d) = \langle L^t(d), t \in \mathbb{N} \rangle \ .$$

Theorem. There exists d such that $\dim W_L(d) = k$ if and only if k is the degree of a divisor of the minimal polynomial of L.

$$\Rightarrow \max_{d \in \mathbb{F}_2^n} \dim W_L(d) = \deg \mathsf{Min}_L$$

For some lightweight ciphers

LED.

$$\text{Min}_L(X) = (X^8 + X^7 + X^5 + X^3 + 1)^4 (X^8 + X^7 + X^6 + X^5 + X^2 + X + 1)^4$$

There exist some d such that $\dim W_L(d) = 64$

Prince.

$$\text{Min}_L(X) = X^{20} + X^{18} + X^{16} + X^{14} + X^{12} + X^8 + X^6 + X^4 + X^2 + 1$$

$$\max_d \dim W_L(d) = 20$$

Midori.

$$\text{Min}_L(X) = (X+1)^6 \Rightarrow \max_d \dim W_L(d) = 6$$

Some conclusions on lightweight cryptography

- standardization process launched by NIST in December
- risky
- clarifies the design criteria.