



**HAL**  
open science

## L'insoutenable légèreté du chiffrement

Anne Canteaut

► **To cite this version:**

Anne Canteaut. L'insoutenable légèreté du chiffrement. Journées Scientifiques Inria 2018, Jun 2018, Bordeaux, France. hal-01955337

**HAL Id: hal-01955337**

**<https://hal.inria.fr/hal-01955337>**

Submitted on 14 Dec 2018

**HAL** is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

# L'insoutenable légèreté du chiffrement

**Anne Canteaut**

Inria Paris, EPI SECRET

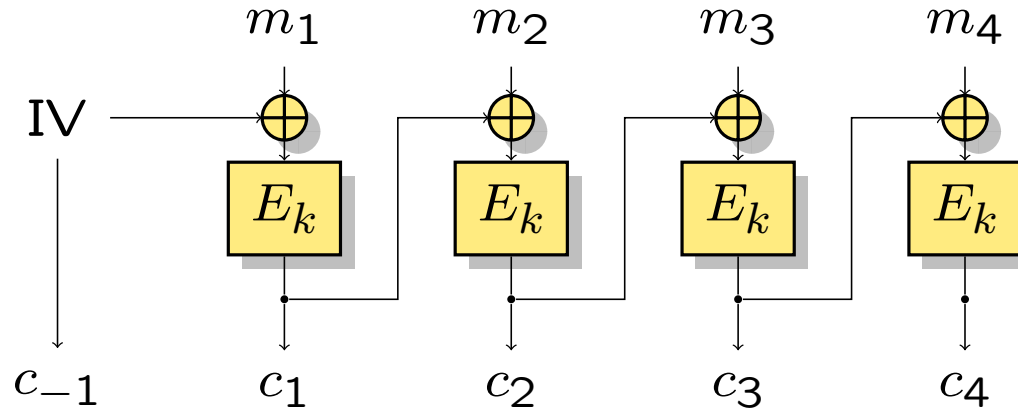
(travaux communs avec C. Beierle, G. Leander et Y. Rotella)

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:

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

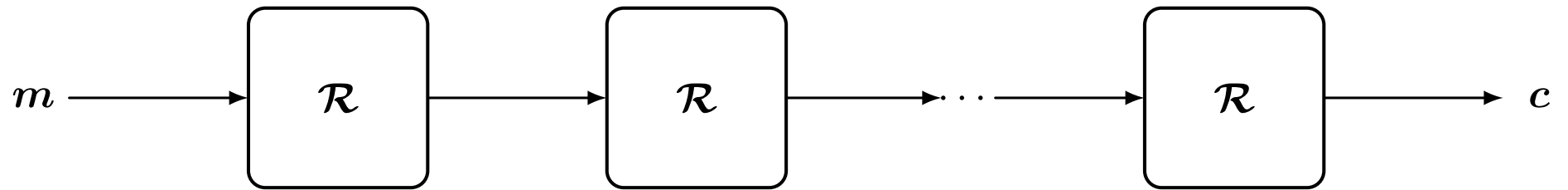
## What is a block cipher?

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

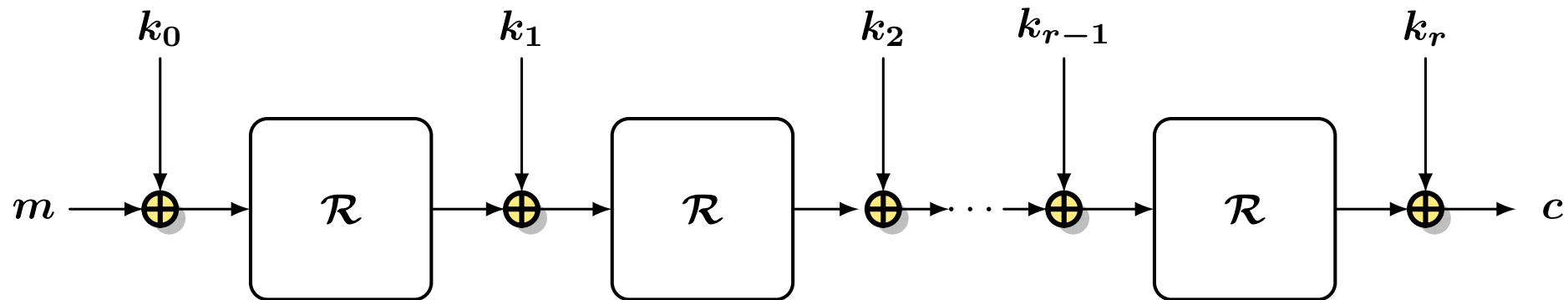
- indistinguishable from a set of randomly chosen permutations of  $\{0, 1\}^n$
- implementable

→ Contradiction!

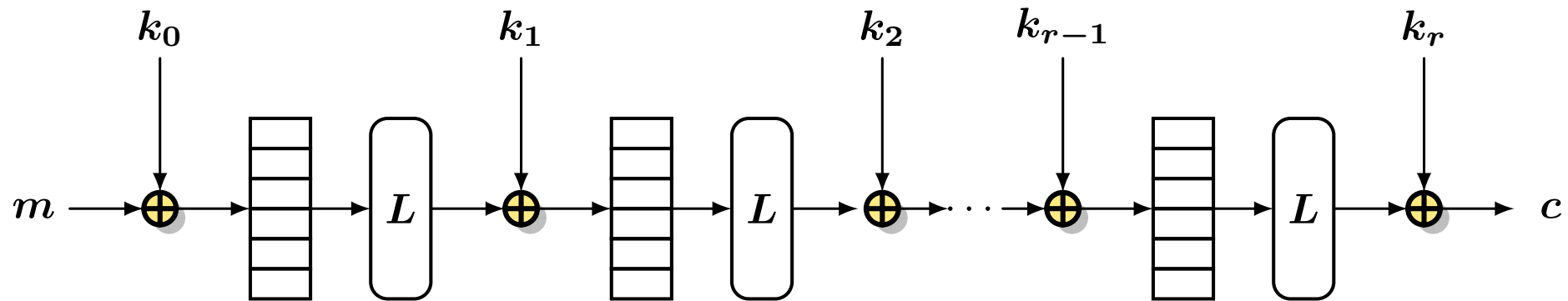
## Iterated block ciphers



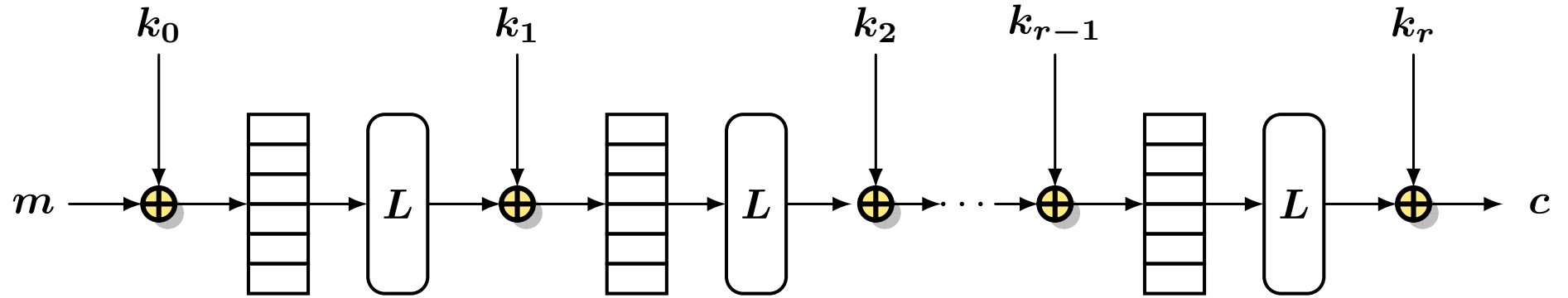
# Iterated block ciphers



# Iterated block ciphers



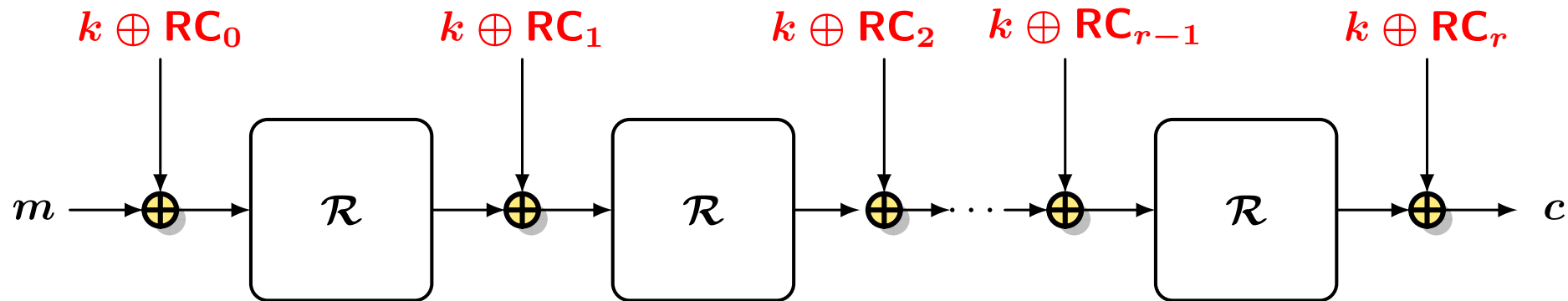
## Lightweight block ciphers



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



## Lightweight key schedules



where  $\text{RC}_0, \text{RC}_1, \dots, \text{RC}_r$  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  $\mathcal{X}$  of inputs **invariant under  $E_k$**  for many weak keys.

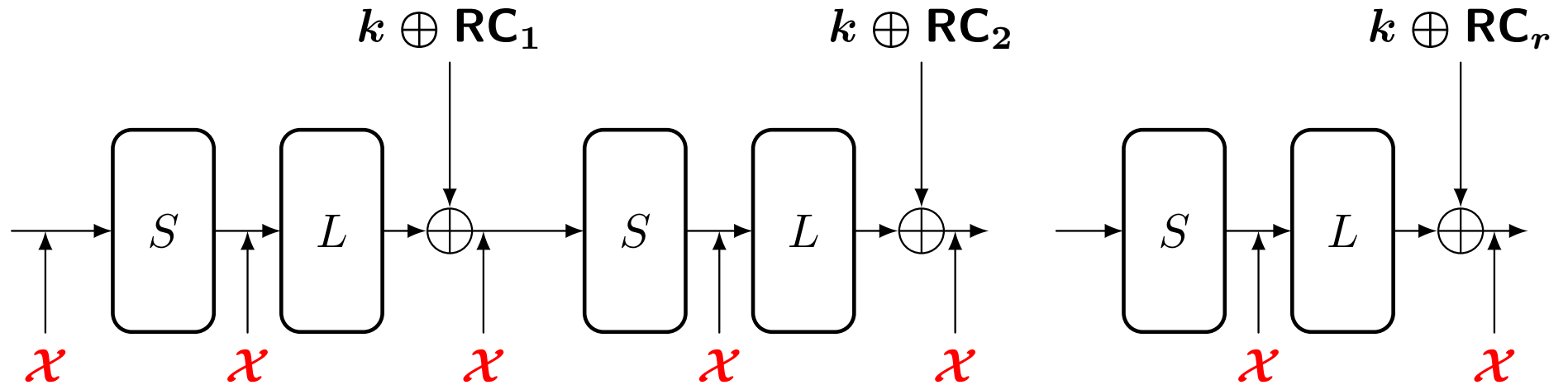
### Ex: Invariant subspace for Midori-64 [Guo et al. 16]

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

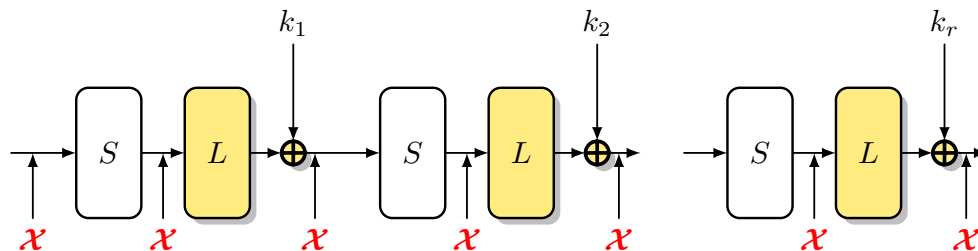
For  $k = (1100110011001100, 0011001100110011)$ ,

$m = 9999999999999999$  leads to the ciphertext  $c = 89999999988988989$

# 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

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

$W_L(D) :=$  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  $W_L(D)$ ?

## Condition on the existence of invariant sets

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

$W_L(D) :=$  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.

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

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

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

### Prince.

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

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

### 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  $L$ .

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



## 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.