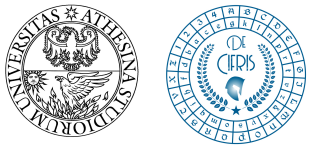
Lightweight symmetric primitives

Anne Canteaut

De Cifris Trends in Modern Cryptography:

the French Magisterium

Lecture 3



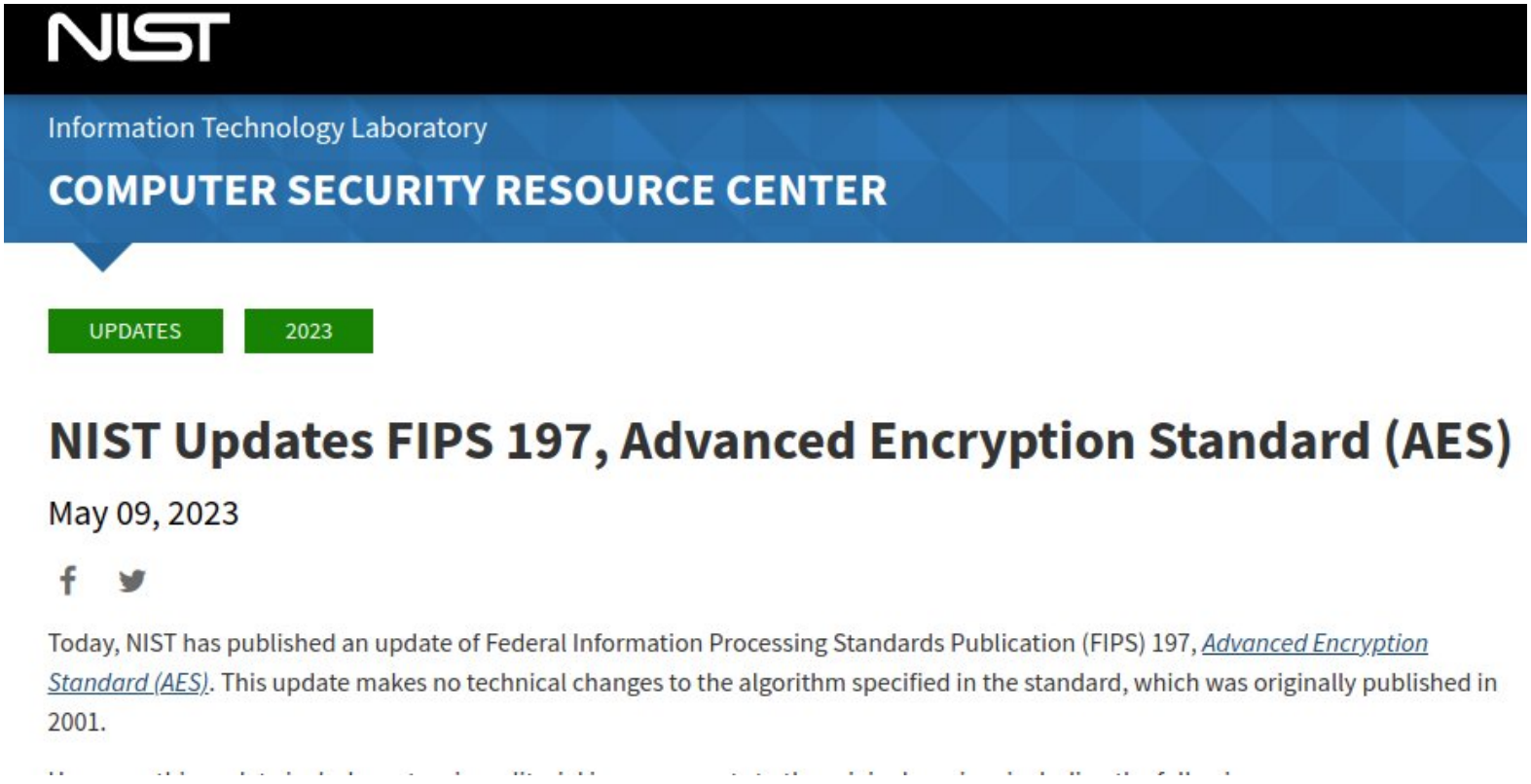
Lightweight Symmetric Primitives

Anne Canteaut

Inria Paris, France


INTRODUCTION

20+ years later, AES is still secure



NIST

Information Technology Laboratory

COMPUTER SECURITY RESOURCE CENTER

UPDATES 2023

NIST Updates FIPS 197, Advanced Encryption Standard (AES)

May 09, 2023

Today, NIST has published an update of Federal Information Processing Standards Publication (FIPS) 197, *Advanced Encryption Standard (AES)*. This update makes no technical changes to the algorithm specified in the standard, which was originally published in 2001.

New implementation constraints

COMPUTERWORLD UK

THE VOICE OF IT MANAGEMENT

IT Topics | News | In Depth | IT Management | Profe

Home > Mobile & Wireless > News

Questions raised about Oyster card security

Its RFID chip is cracked by researchers

By Network World and Computerworld UK staff | Published 12:20, 07 March 08

Smartcards with encrypted RFID chips, including London's Oyster fare card, might not be as secure as previously thought.

New research at the University of Virginia is causing a major stir in Boston, because it raises question over the smart "CharlieCards" used by commuters on the city's 'T' metro system.

However, London's Oyster card uses similar RFID technology – the Mifare Classic made by Philips spinoff NXP Semiconductors.

Also in this channe

- News
- In Depth
- How-Tos
- Blogs
- Slideshows

New implementation constraints

HOME SECTIONS SEARCH NEW YORK POST

NEWS

Cheney feared terrorists would 'hack' pacemaker

By Bob Fredericks October 19, 2013 | 4:11am

Lightweight Competitions

CAESAR for authenticated encryption (2014-2019):

`https://competitions.cr.yp.to/caesar.html`

Use case 1: Lightweight (resource-constrained) applications

1. Ascon [Dobraunig, Eichlseder, Mendel, Schläffer 16]
2. Acorn [Wu 14]

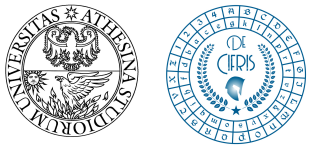
NIST Lightweight Cryptography standardization (2015-23):

Ascon family (announced in Feb. 2023)

Why is minimalism interesting?

Tretyakov Gallery

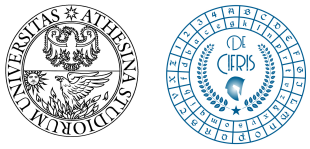
Besides (niche) application needs, it helps us understand where security comes from.



Outline

1. Symmetric encryption
2. How to make it lightweight?
3. Ascon
4. Possible weaknesses coming from "minimal" building-blocks:
   - Simple key-schedule
   - ...


Symmetric encryption

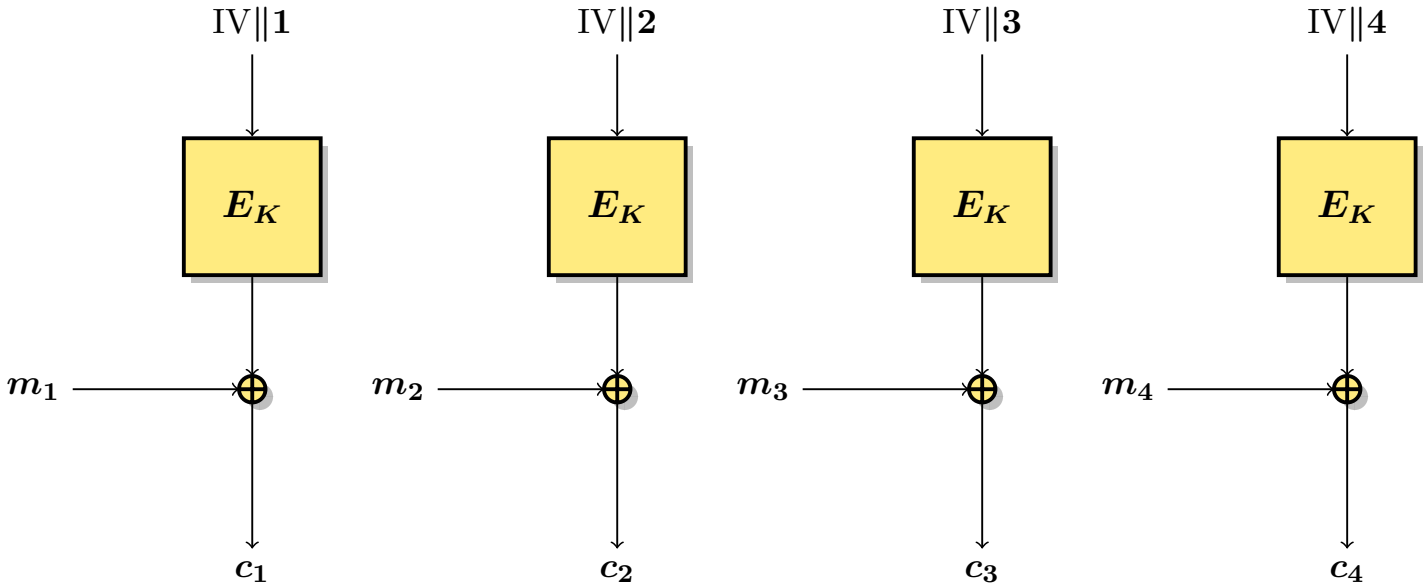


Encryption scheme

Two steps for encrypting plaintexts of an arbitrary length:

1. design a permutation, or a family of permutations, operating on $\{0,1\}^n$.
2. design a mode of operation describing how this primitive can used for encrypting messages of any length (e.g. CTR, CBC).

CTR mode for encryption



where E_K = family of permutations of $\{0,1\}^n$ indexed by the key.

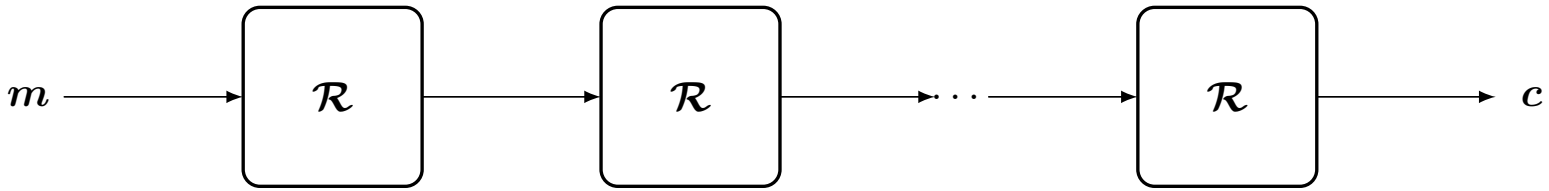
Practical Pseudo-Random Permutation

$$E_K : \{0,1\}^n \longrightarrow \{0,1\}^n$$

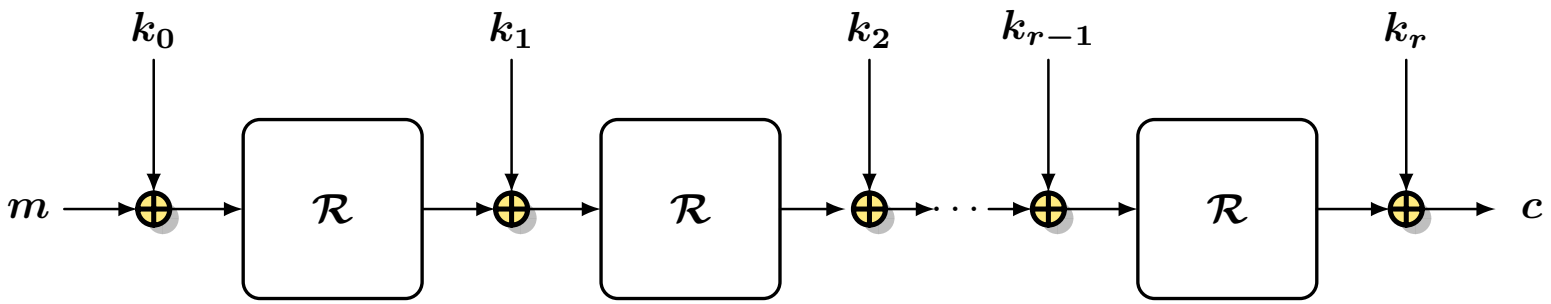
- indistinguishable from randomly chosen bijections of $\{0,1\}^n$ with $n \in \{64, 128\}$
- implementable

$\rightarrow$ Contradiction!

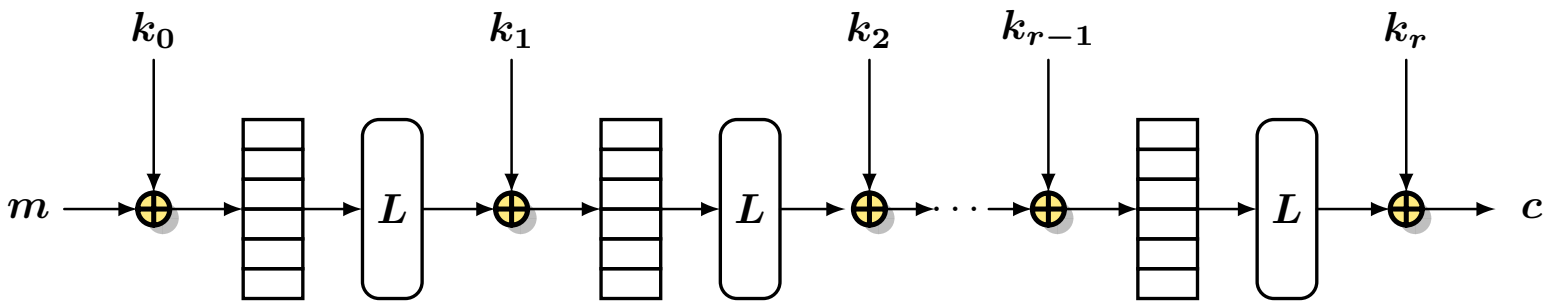
Iterated construction



Iterated construction



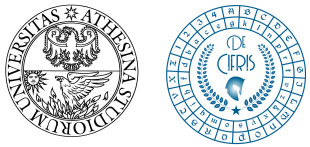
Iterated construction



AES [Daemen-Rijmen 98][FIPS PUB 197]

- blocksize: 128 bits
- 10 rounds for the 128-bit key version
- Sbox operates on 8 bits
- diffusion layer is linear over F_{2^8}
- nonlinear key schedule.


How to make it lightweight?



Lightweight block ciphers

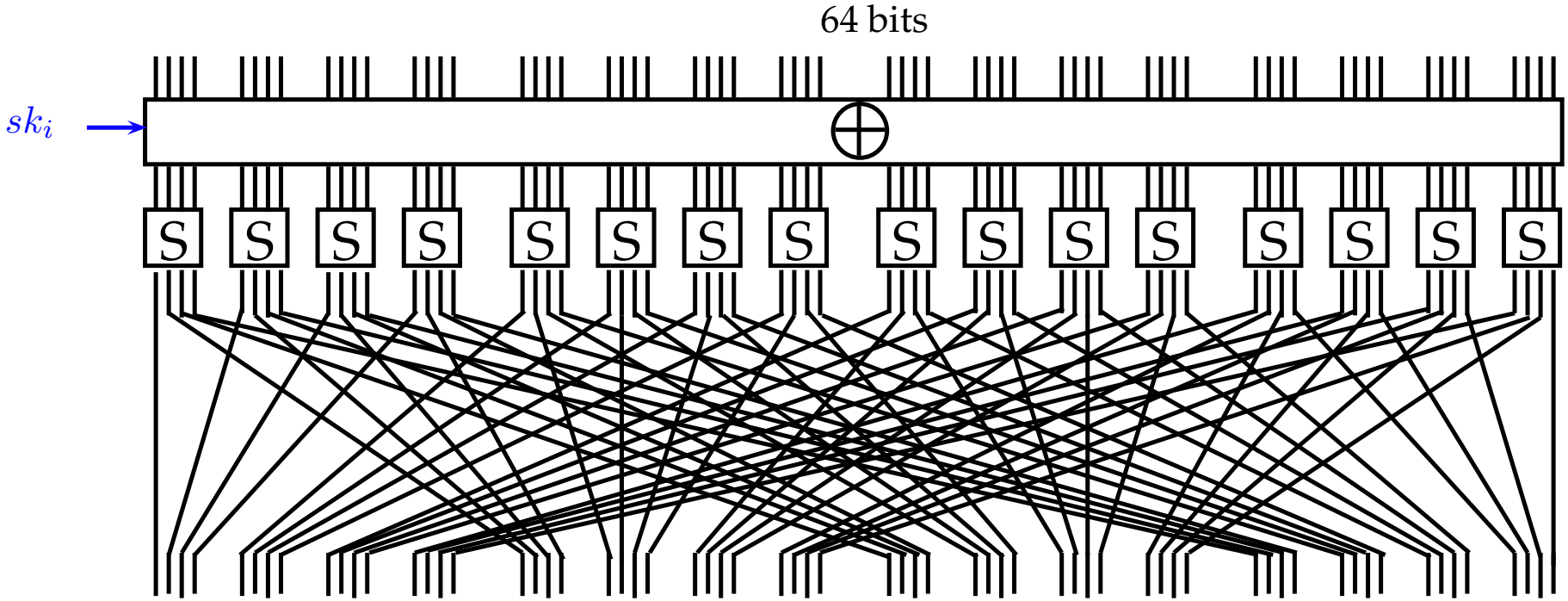
AES [Daemen-Rijmen 98][FIPS PUB 197]

- blocksize: 128 bits
- Sbox operates on 8 bits
- diffusion layer is linear over F_{2^8}

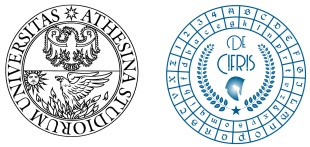
To make it smaller in hardware:

- blocksize: 64 bits
- smaller Sbox, on 3 or 4 bits
- linear diffusion layer over a smaller alphabet
- simplified key-schedule

PRESENT [Bogdanov et al. 07]



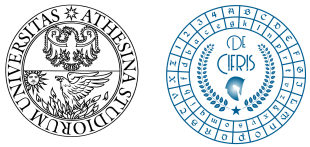
31 rounds (+ a key addition)



Lightweight but secure...

Increase the number of rounds!

- PRESENT [Bogdanov et al. 07]: 31 rounds
- LED [Guo et al. 11]:
  LED-64: 32 rounds, LED-128: 48 rounds
- SPECK [Beaulieu et al. 13]:
  SPECK64/128: 27 rounds, SPECK128/256: 34 rounds
- SIMON [Beaulieu et al. 13]:
  SIMON64/128: 44 rounds, SIMON128/256: 72 rounds

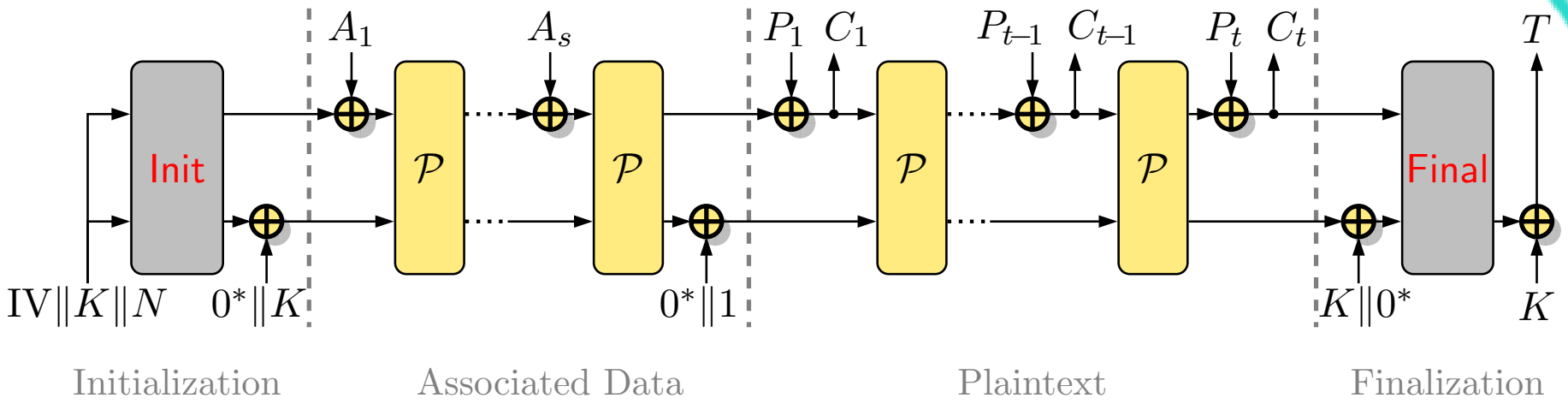


Does lightweight mean "light + wait"?

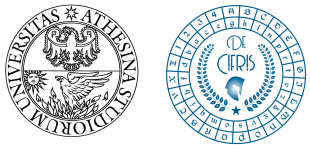
[Knežević et al. 12]

Duplex-Sponge mode for AEAD encryption

[Bertoni et al. 12]



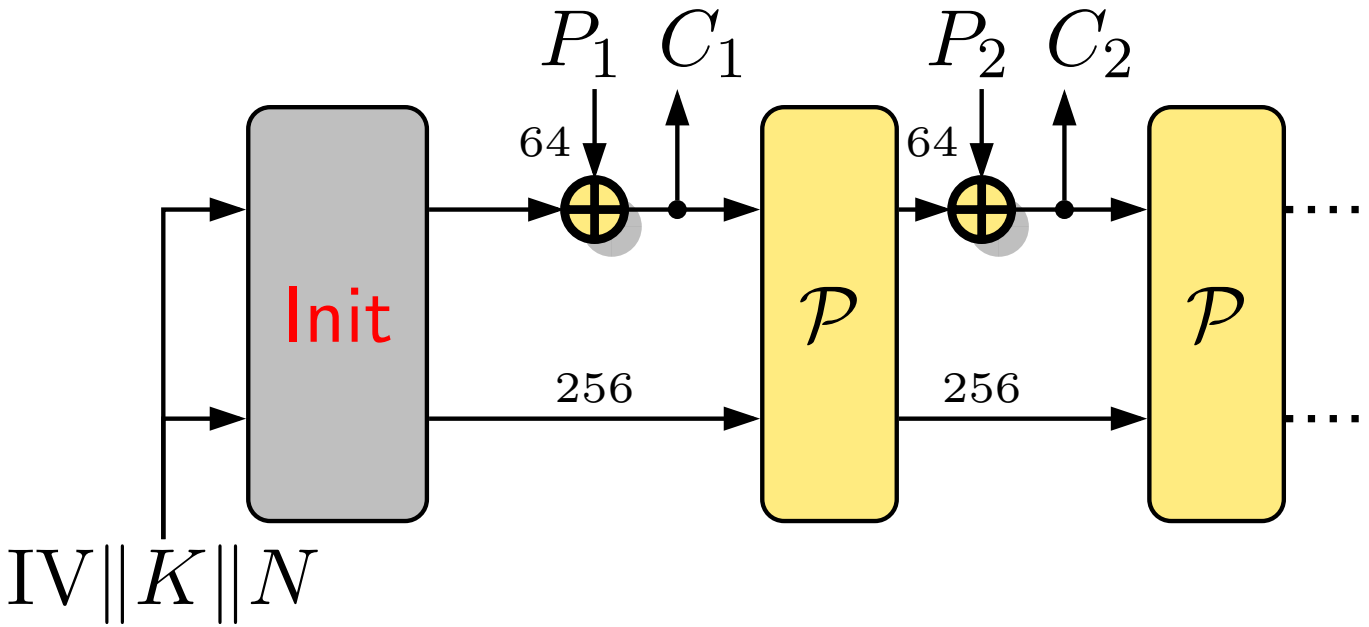
where $\mathcal{P}$ is a permutation of $\{0,1\}^n$.



Ascon

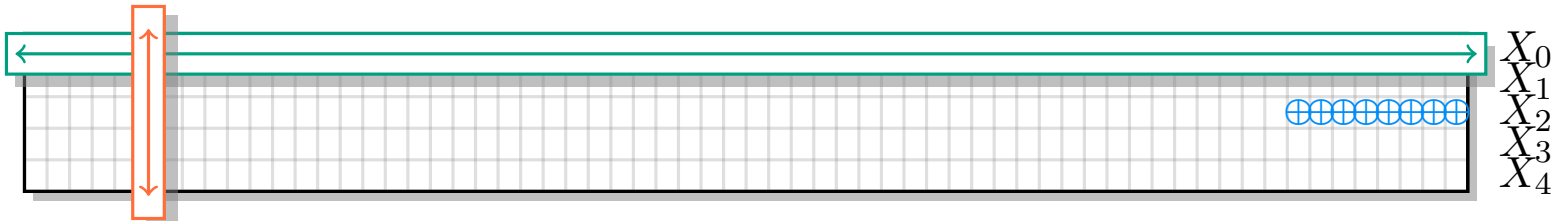
Duplex-Sponge mode in Ascon

[Dobraunig, Eichlseder, Mendel, Schläffer 16]



where $\mathcal{P}$ is a permutation on 320 bits
of which 64 are known/controlled.

$\mathcal{P}$ in Ascon



Permutation operating on a 320-bit state:

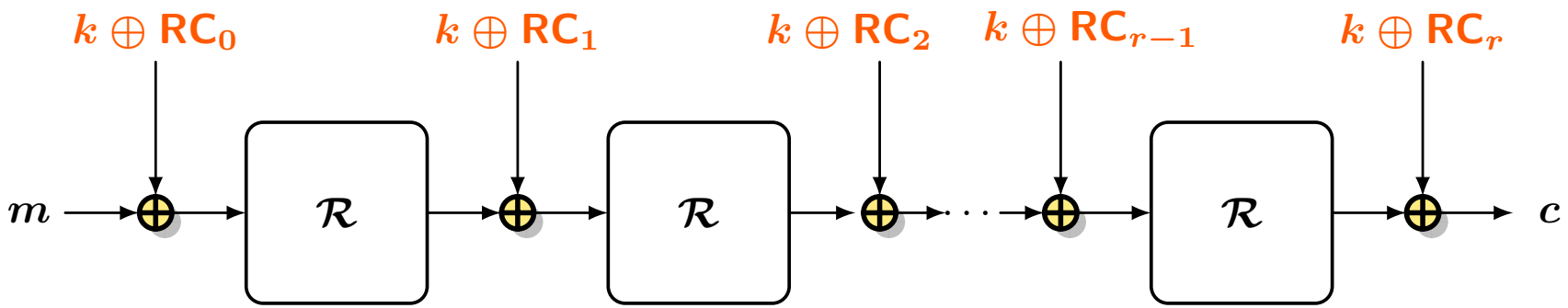
- 8-bit constant addition;
- Nonlinear Sbox on 5 bits of degree 2 (on the 64 columns);
- 5 simple linear transformations on 64 bits

$$\Sigma_i(X_i) = X_i \oplus (X_i \ggg a_i) \oplus (X_i \ggg b_i)$$

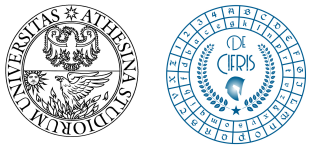
$\rightarrow$ 6 rounds


Possible weaknesses coming from minimal building-blocks

Lightweight key schedules



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



Invariants for Midori-64

[Guo et al. 16][Todo et al. 16]

Midori-64 [Banik et al. 15]:

$$E_K : \left(\{0,1\}^4\right)^{16} \longrightarrow \left(\{0,1\}^4\right)^{16}$$

with $K = (k_0, k_1, k_0 \oplus \mathrm{RC}_2, k_1 \oplus \mathrm{RC}_3, k_0 \oplus \mathrm{RC}_4, \ldots)$

Invariant set for Midori-64:

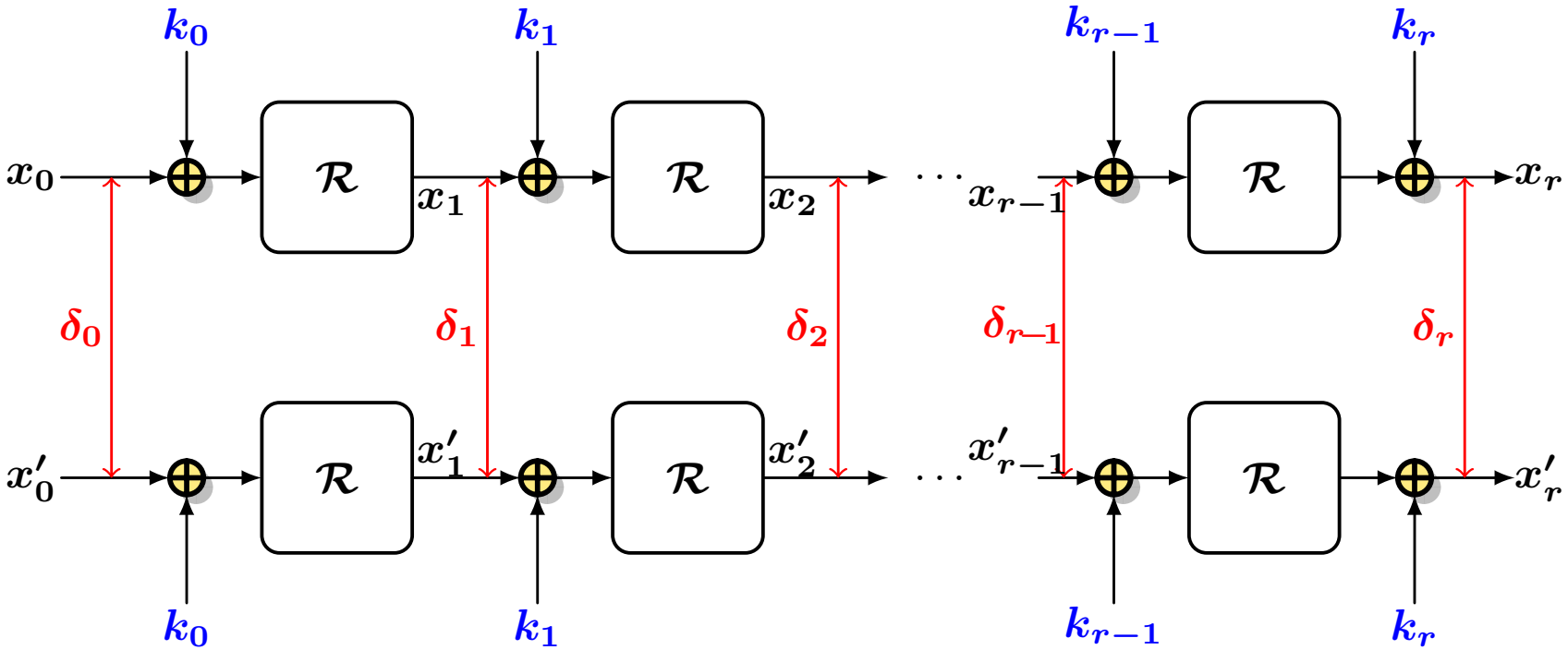
If $k_0, k_1 \in \{\mathtt{0x0}, \ \mathtt{0x1}\}^{16}$, then $\{\mathtt{0x8}, \ \mathtt{0x9}\}^{16}$ is invariant under E_K.

Example :

For $(k_0, k_1) = (\mathtt{0x1100110011001100}, \mathtt{0x0011001100110011})$,
$m = \mathtt{0x9999999999999999} \mapsto c = \mathtt{0x8999999988988989}$

Probability of a differential path

[Biham,Shamir 90]



Fixed-key differential paths for r iterations of Midori-64

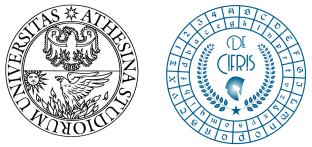
Differential path $(\delta, \delta, \ldots, \delta)$ with $\delta = (\mathtt{0x1})^{16}$

- **On average over all key sequences**

$$\mathrm{EDP}(\delta, \ldots, \delta) = 2^{-48r}$$

- **For a fixed key**

$$\mathrm{DP}(\delta, \ldots, \delta) = \begin{cases} 2^{-48} & \text{if } \forall i, k_i \in \{\mathtt{0x0}, \mathtt{0x1}\}^{16} \\ 0 & \text{otherwise.} \end{cases}$$



Where does this come from?

- The key schedule is compatible with the fact that each k_i lies in a (affine) subspace.
- The linear diffusion function is defined by an orthogonal matrix.

Takeaway

Minimalism helps us understand where security comes from.
It motivates new attacks, and new design criteria.

De Componendis Cifris

https://www.decifris.it