Minimalism in Symmetric Cryptography

Anne Canteaut

Inria, Paris

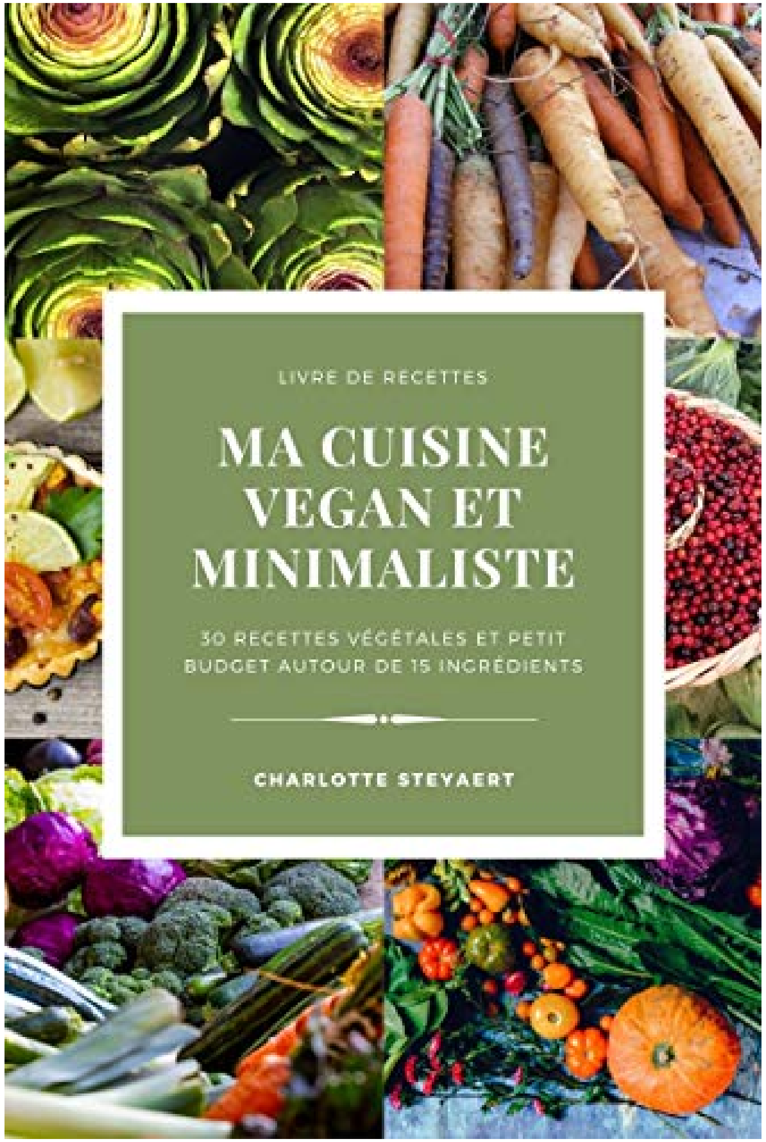
NAC 2024, February 29, 2024

Minimalism

Credit: Hans Peter Schaefer

Maybe less exciting?

Maybe less exciting?



Why is minimalism interesting?

Why is minimalism interesting?

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

Outline

1. Designing a practical PRP
2. How to make it lightweight?
3. Possible weaknesses coming from “minimal” Sboxes

Designing a Practical PRP

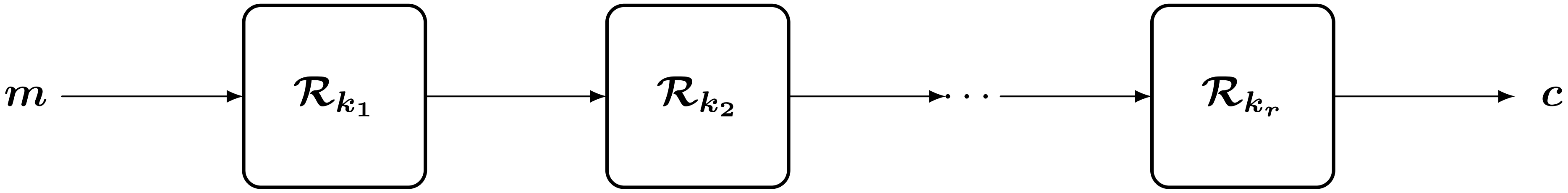
Practical PRP

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

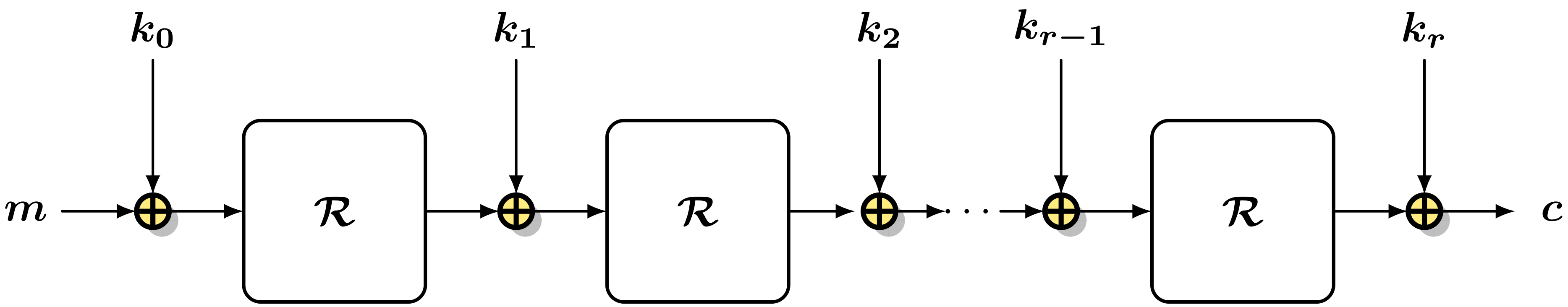
- indistinguishable from randomly chosen permutations of $\{0,1\}^n$ with $n \in \{64, 128\}$
- implementable

$\rightarrow$ Contradiction!

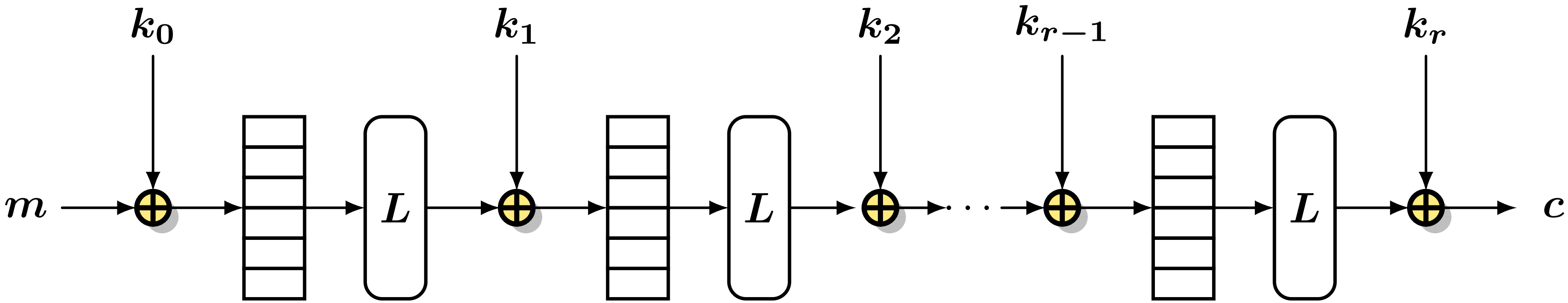
Iterated construction



Iterated construction



Iterated construction



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

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

How to make it lightweight?

Lightweight block ciphers

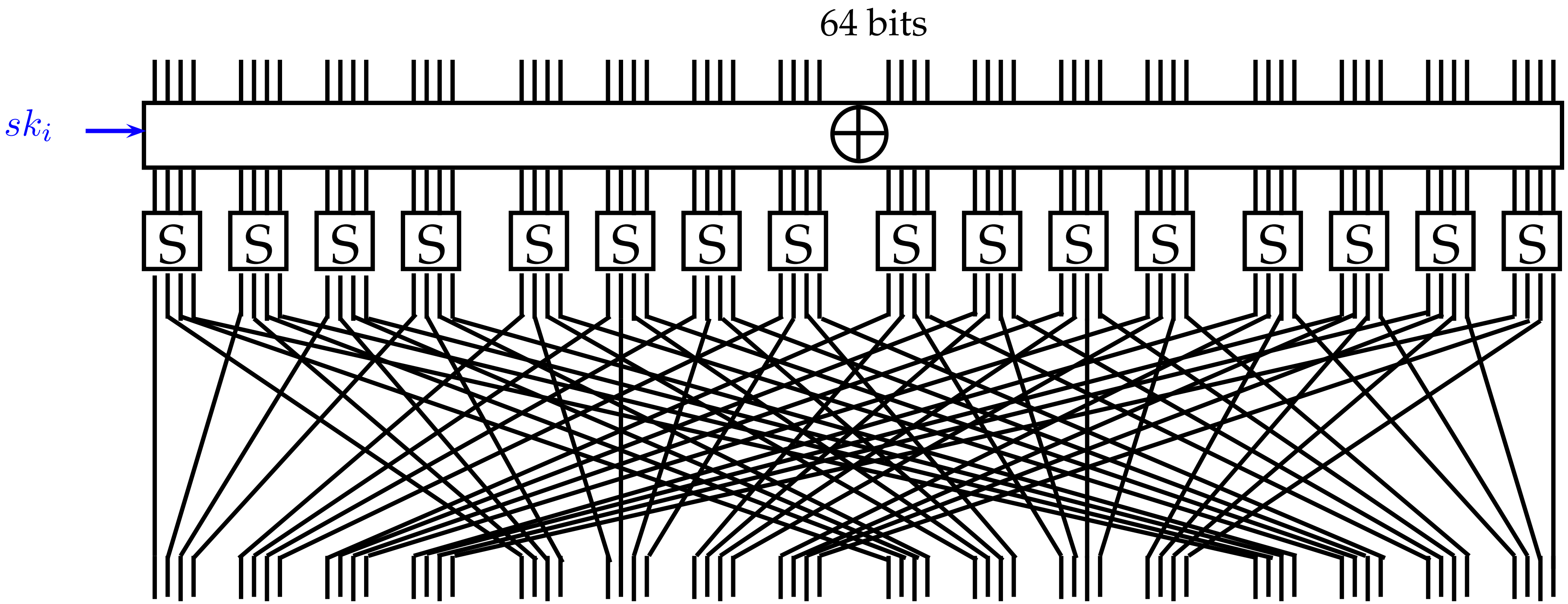
AES [Daemen-Rijmen 98][FIPS PUB 197]

- blocksize: 128 bits
- Sbox operates on 8 bits
- diffusion layer is linear over $\mathbf{F}_{2^8}$

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

The usual design strategy: 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]

Lightweight Competitions

CAESAR for authenticated encryption (2014-2019) :

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

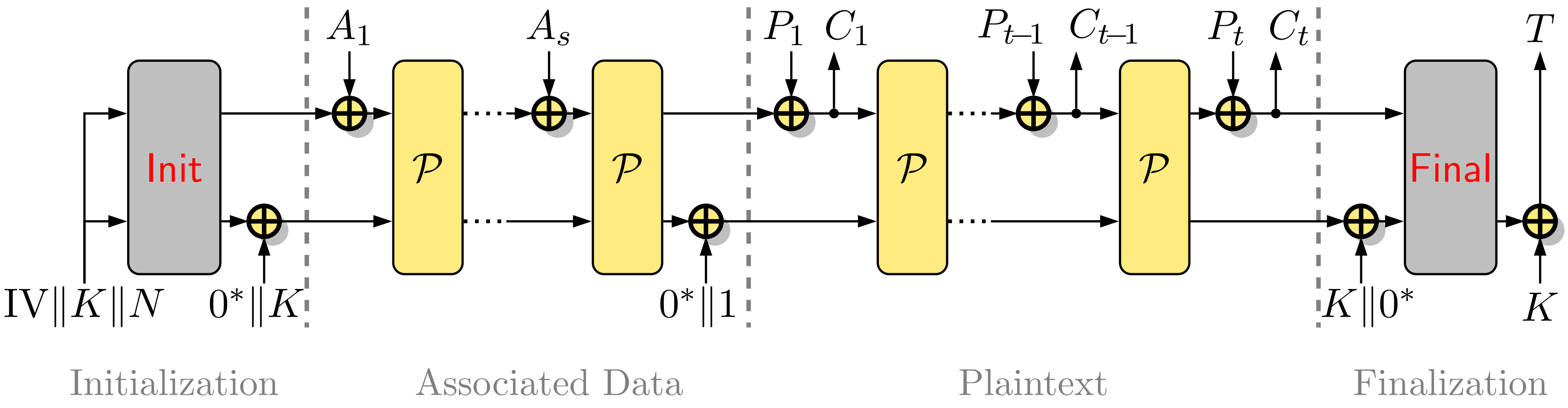
Use case 1: Lightweight applications (resource constrained environments)

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

NIST Lightweight Cryptography standardization process (2019-2023)

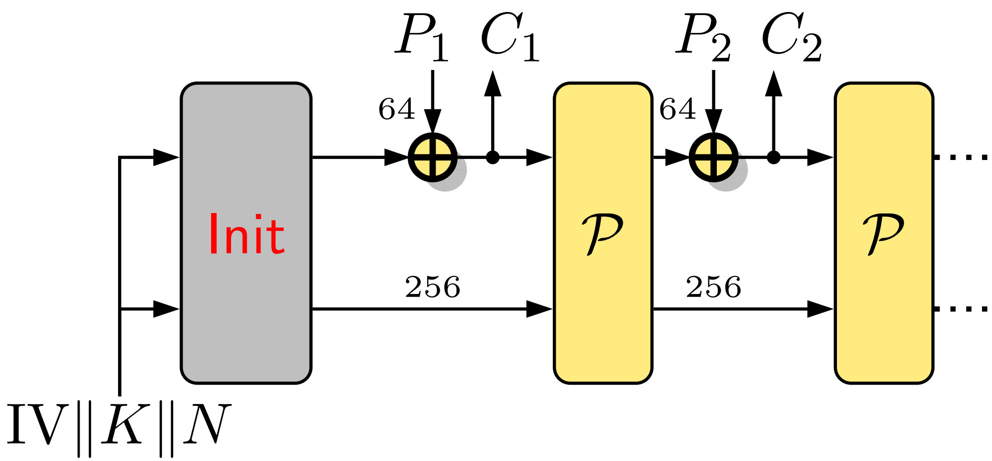
Ascon family (announced in Feb. 2023)

Duplex-Sponge mode for AEAD encryption [Bertoni et al. 12]



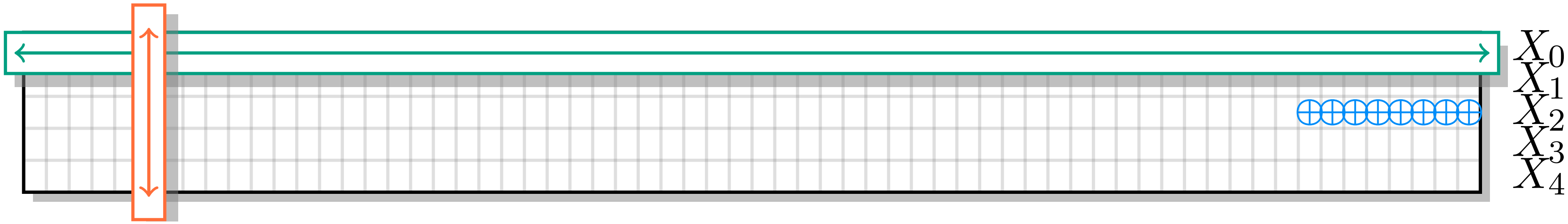
where $\mathcal{P}$ is a permutation of $\{0,1\}^n$.

Duplex-Sponge mode in Ascon



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

$\mathcal{P}$ in Ascon [Dobraunig, Eichlseder, Mendel, Schläffer 16]



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

Use low-cost Sboxes

Algebraic Normal Form of $f : \mathbf{F}_2^n \rightarrow \mathbf{F}_2$:

unique polynomial representation in $\mathbf{F}_2[x_1, \ldots, x_n]/(x_1^2 - x_1, \ldots, x_n^2 - x_n)$.

$$f(x_1, \ldots, x_n) = \bigoplus_{u \in \mathbb{F}_2^n} c_u x^u \text{ with } c_u \in \mathbb{F}_2$$

Evaluation of a monomial:

Evaluation of $x^{(0101)}$ at $x = (0011)$:

$$0^0 0^1 1^0 1^1 = 1011 = 0$$

$$x^u = 1 \text{ if and only if } u \preceq x$$

i.e., $u_i \leq x_i$ for all $1 \leq i \leq n$.

ANF and values:

$$f(a) = \bigoplus_{u \preceq a} c_u \text{ and } c_u = \bigoplus_{a \preceq u} f(a)$$

Cube-like attacks [Dinur-Shamir 09]

$$\begin{array}{rccc} f: & \mathbb{F}_2^{64} \times \mathbb{F}_2^{256} & \to & \mathbb{F}_2 \\ & (x, k) & \mapsto & f(x, k) \end{array}$$

$$f(x, k) = \bigoplus_{u \in \mathbb{F}_2^{64}} \underbrace{\left(\bigoplus_{u \in \mathbb{F}_2^{256}} \alpha_{u,v} \; k^v \right)}_{A_u(k)} x^u$$

Attack:

- Offline: determine the polynomial expression of $A_u(k)$ for a given u.
- Online: for the key used k^*, compute the value

$$A_u(k^*) = \bigoplus_{v \preceq u} f(v, k^*)$$

Cube-like attacks on Ascon [Rohit et al. 21][Baudrin-C.-Perrin 22]

$$S(x, a, b, c, d) = \begin{cases} (a \oplus 1)x & \oplus \quad ab \oplus ad \oplus a \oplus b \oplus c \\ x & \oplus \quad ab \oplus ac \oplus bc \oplus a \oplus b \oplus c \oplus d \\ & \quad\;\; cd \oplus a \oplus b \oplus d \oplus 1 \\ (c \oplus d \oplus 1)x & \oplus \quad a \oplus b \oplus c \oplus d \\ ax & \oplus \quad ad \oplus a \oplus c \oplus d \end{cases}$$

→ The degree in x after r rounds is 2^{r-1}, for $r \leq 6$.

After two rounds:

The coefficient of $x_0 x_i$ is

$$(a_0 \oplus 1)P \oplus Q \oplus (c_0 \oplus d_0 \oplus 1)R \oplus a_0 S.$$

For some well-chosen i, it equals $(a_0 \oplus 1)P$ or $(c_0 \oplus d_0 \oplus 1)R$.

Cube attack on Ascon [Baudrin-C.-Perrin 22]

After six rounds:

For all 64 outputs, the coefficient of some monomials of degree $\mathbf{2^5}$ containing x_0 can be written as

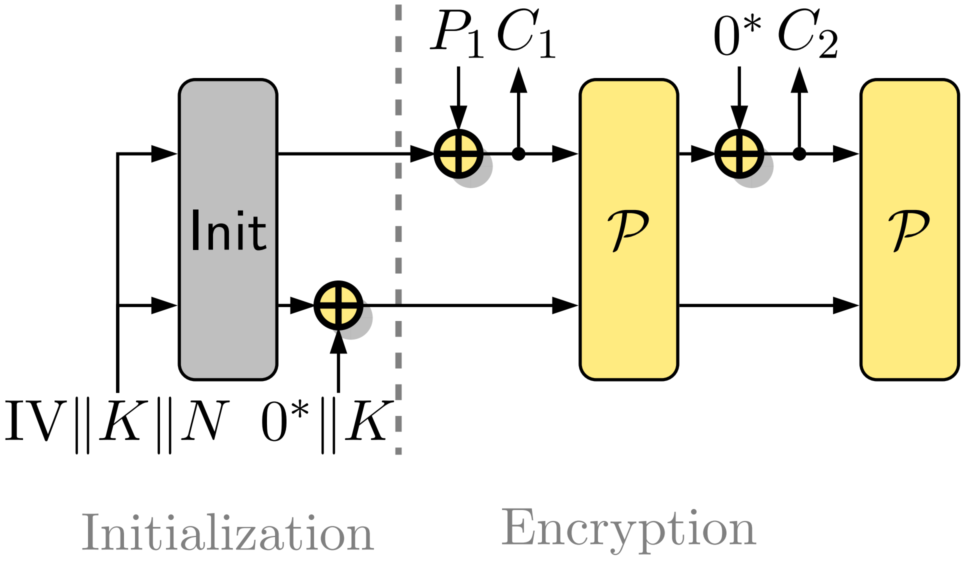
$$(a_0 \oplus 1)P \oplus (c_0 \oplus d_0 \oplus 1)R$$

$\rightarrow$ If these 64 coefficients do not all vanish, then

$$a_0 = 0 \text{ or } c_0 \oplus d_0 = 0$$

$+$ The converse also holds in practice.

Practical attack in the nonce-misused scenario [Baudrin-C.-Perrin 22]



Recover the full initial state from less than $\mathbf{2^{39.6}}$ ciphertexts obtained from the same $(\boldsymbol{K}, \boldsymbol{N})$ with time complexity $\mathbf{2^{40}}$.

Minimalism in cryptography is more fun than in cooking