Key-Recovery Attacks on ASASA

Brice Minaud[1], Patrick Derbez[2], Pierre-Alain Fouque[3], Pierre Karpman[4]

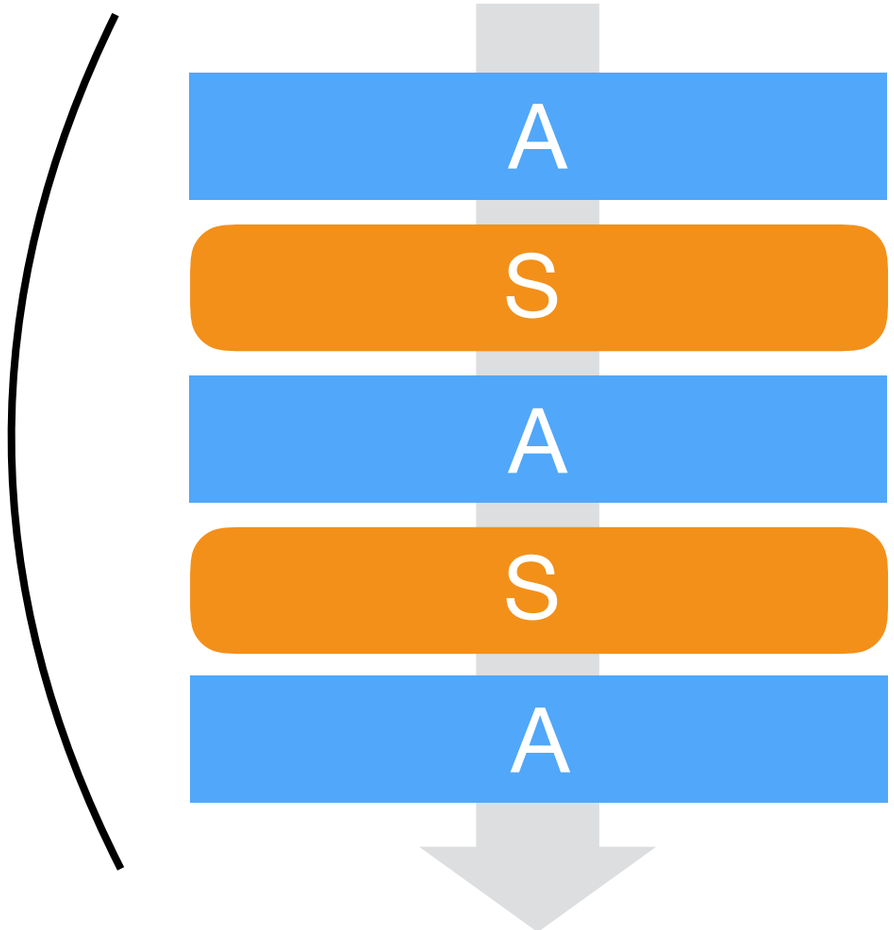
[1] Université Rennes 1
[2] Université du Luxembourg
[3] Université Rennes 1 et Institut Universitaire de France
[4] Inria et Nanyang Technological University, Singapour

ASIACRYPT 2015

ASASA Structure

At Asiacrypt 2014, Biryukov, Bouillaguet and Khovratovich considered various applications of the **ASASA** structure.

F = **A**○**S**○**A**○**S**○**A**



Affine layer

Nonlinear layer
e.g. **S**-boxes

ASASA

Three uses cases were proposed in [BBK14]:

- 1 "black-box" scheme ≈ block cipher ✘ this paper
- 2 "strong whitebox" schemes ≈ public-key encryption scheme
  - "Expanding S-box" scheme ✘ Crypto'15 [GPT15]
  - "χ-based" scheme ✘ this paper
- 1 "weak whitebox" scheme ✘ this paper & [DDKL15]

same attack!

Plan

1. Public-key χ-based **ASASA** scheme.
2. Cryptanalysis.
3. Secret-key **ASASA** scheme.
4. Cryptanalysis (same).

Public-key **ASASA**

Multivariate Cryptography

Hard problem: solving a system of random, say, quadratic, equations over some finite field.

→ How to get an encryption scheme $\mathbb{F}_q^n \to \mathbb{F}_q^n$:

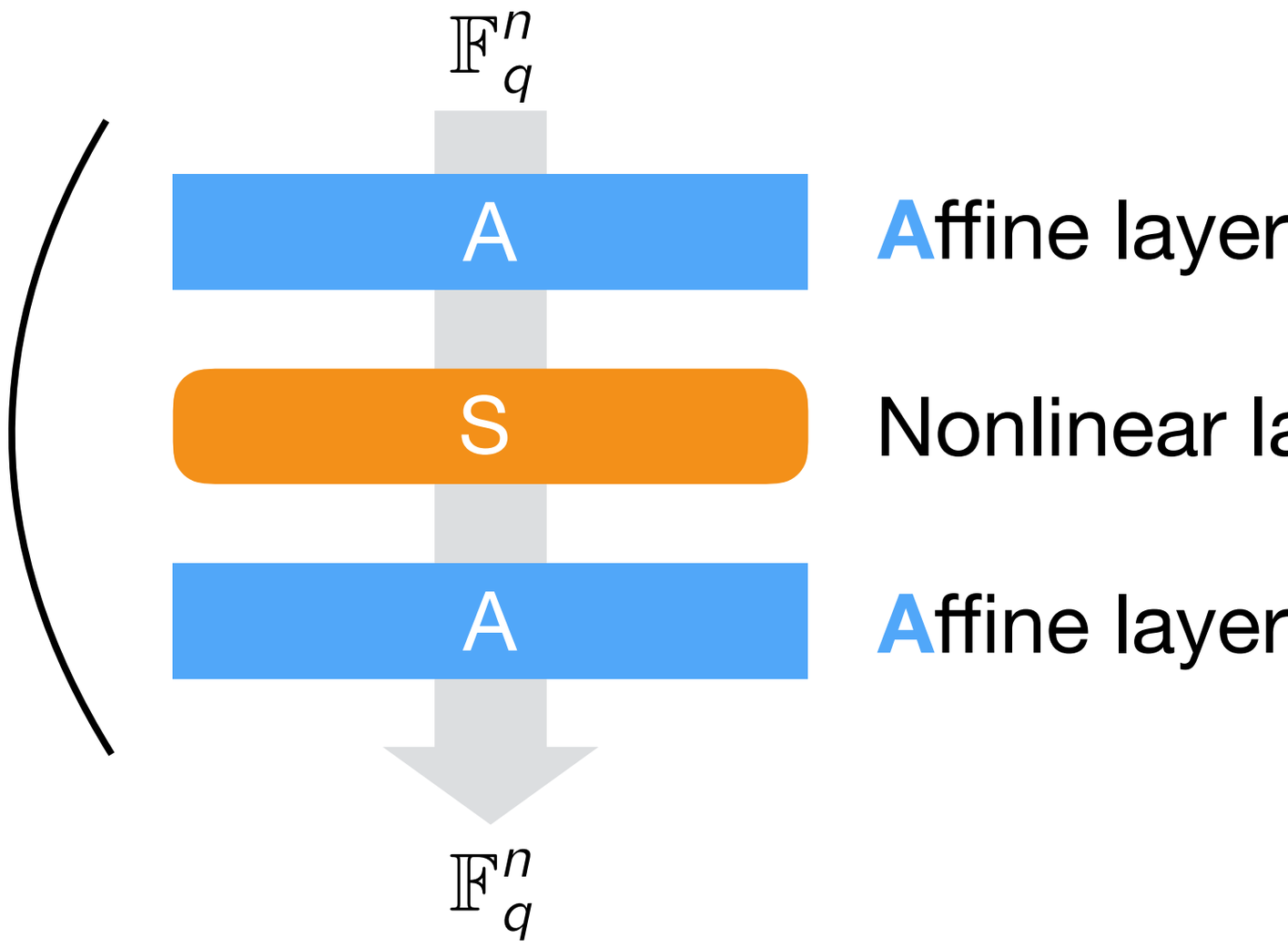
Public key: encryption function **F** given as sequence of *n* quadratic polynomials in *n* variables.

Private key: hidden structure (decomposition) of **F** that makes it easy to invert.

+: small message space, fast with private key.
-: slow public-key operations, large key, no reduction.

ASA

F = **A**○**S**○**A**

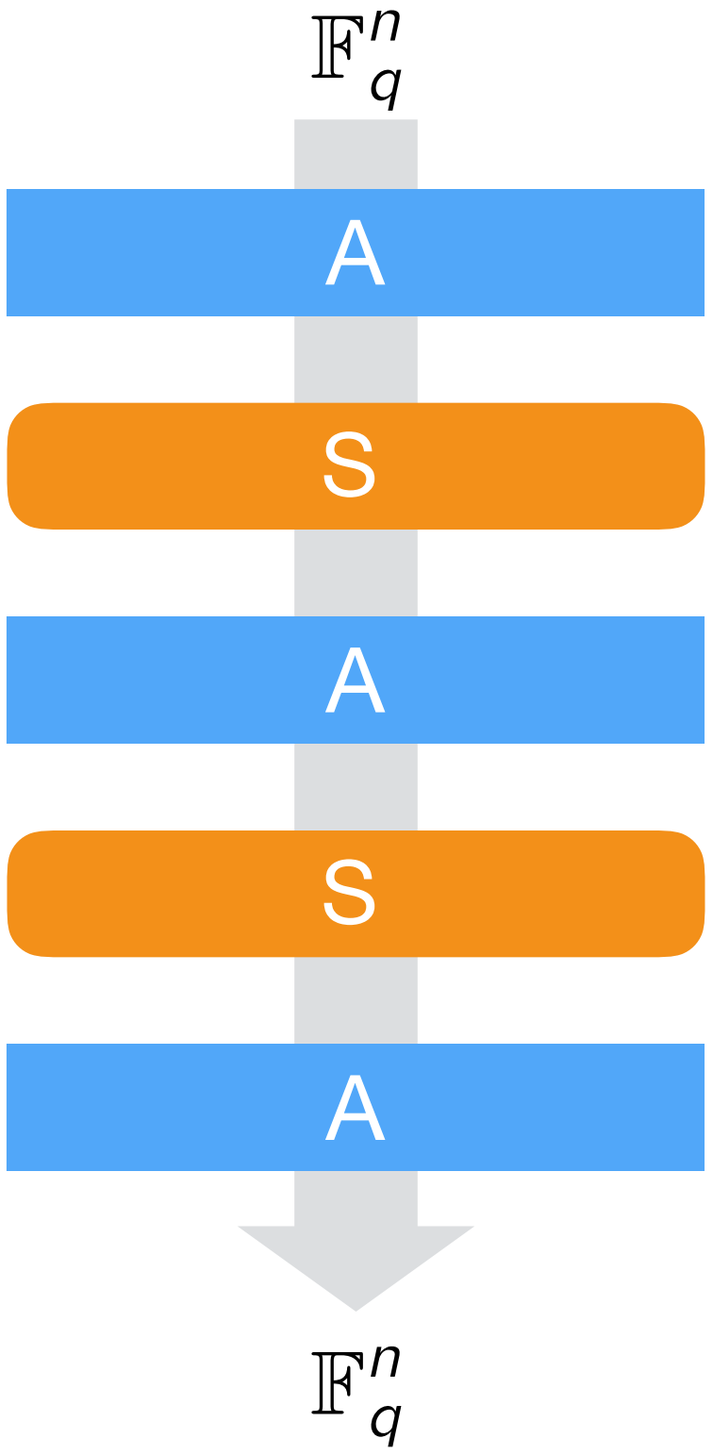


Many proposed scheme follow an ASA structure.

Matsumoto-Imai, Hidden Field Equations, Oil and Vinegar…

Almost all have been broken.

ASASA



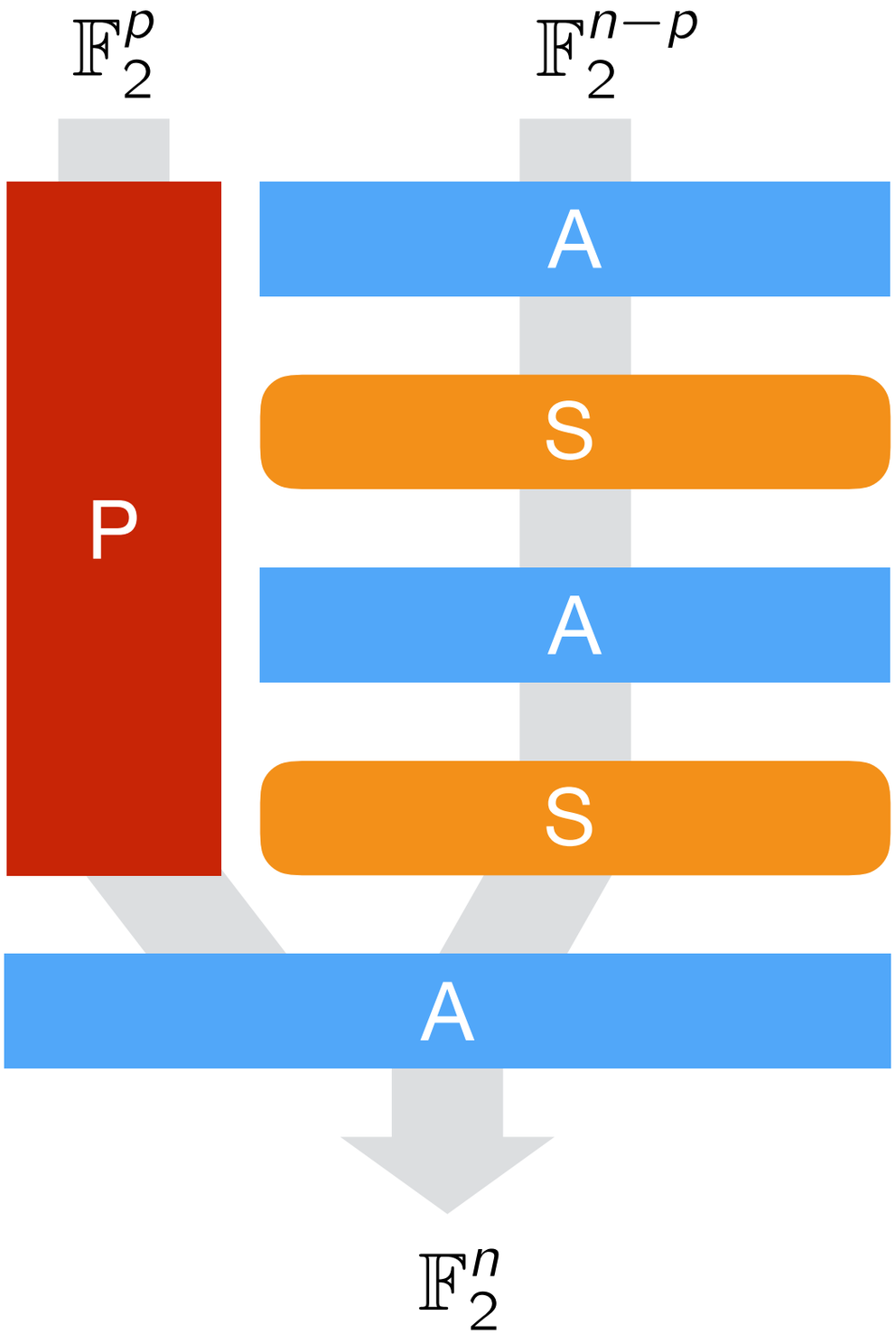
History of ASASA

Idea already proposed by Goubin and Patarin: “2R” scheme (ICICS’97).

Broken by **decomposition** attacks.

- Introduced by Ding-Feng, Lam Kwok-Yan, and Dai Zong-Duo.
- Developped in a general setting by Faugère et al.

Structure ASASA + P [BBK14]



Perturbation: random polynomials of degree 4

Quadratic layer

Quadratic layer

Note : this is slightly different from BBK14.

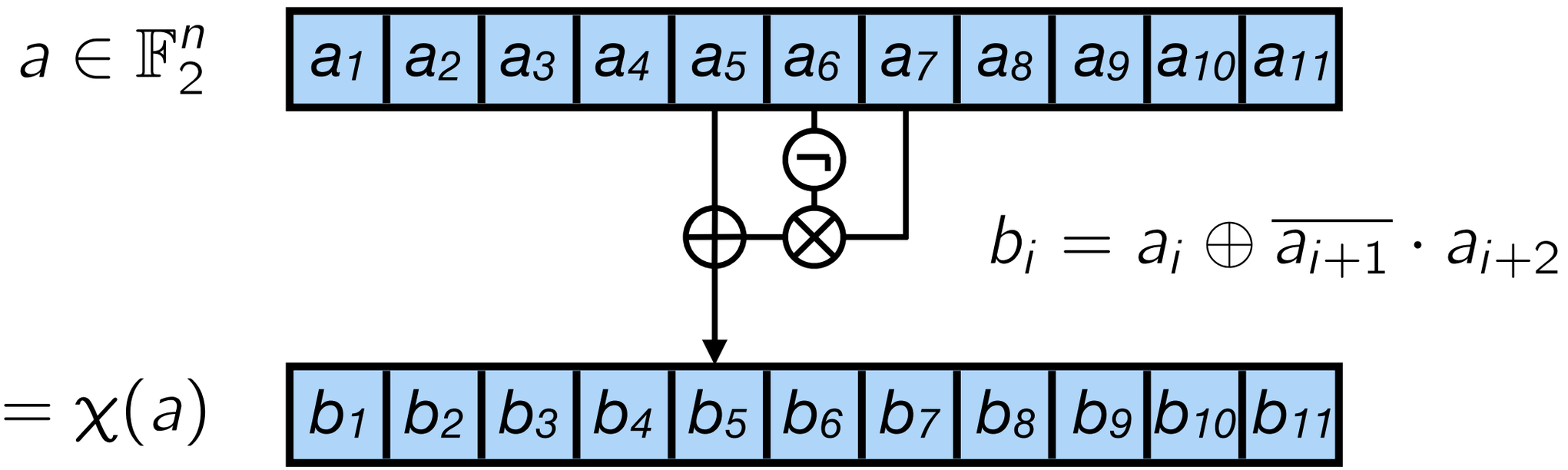
Instances of ASASA + P

Two instances were proposed in BBK14 :

- "Expanding S-boxes" : decomposition attack by Gilbert, Plût and Treger, Crypto'15.

- χ-based scheme: using the χ function of Keccak.

χ function of Keccak

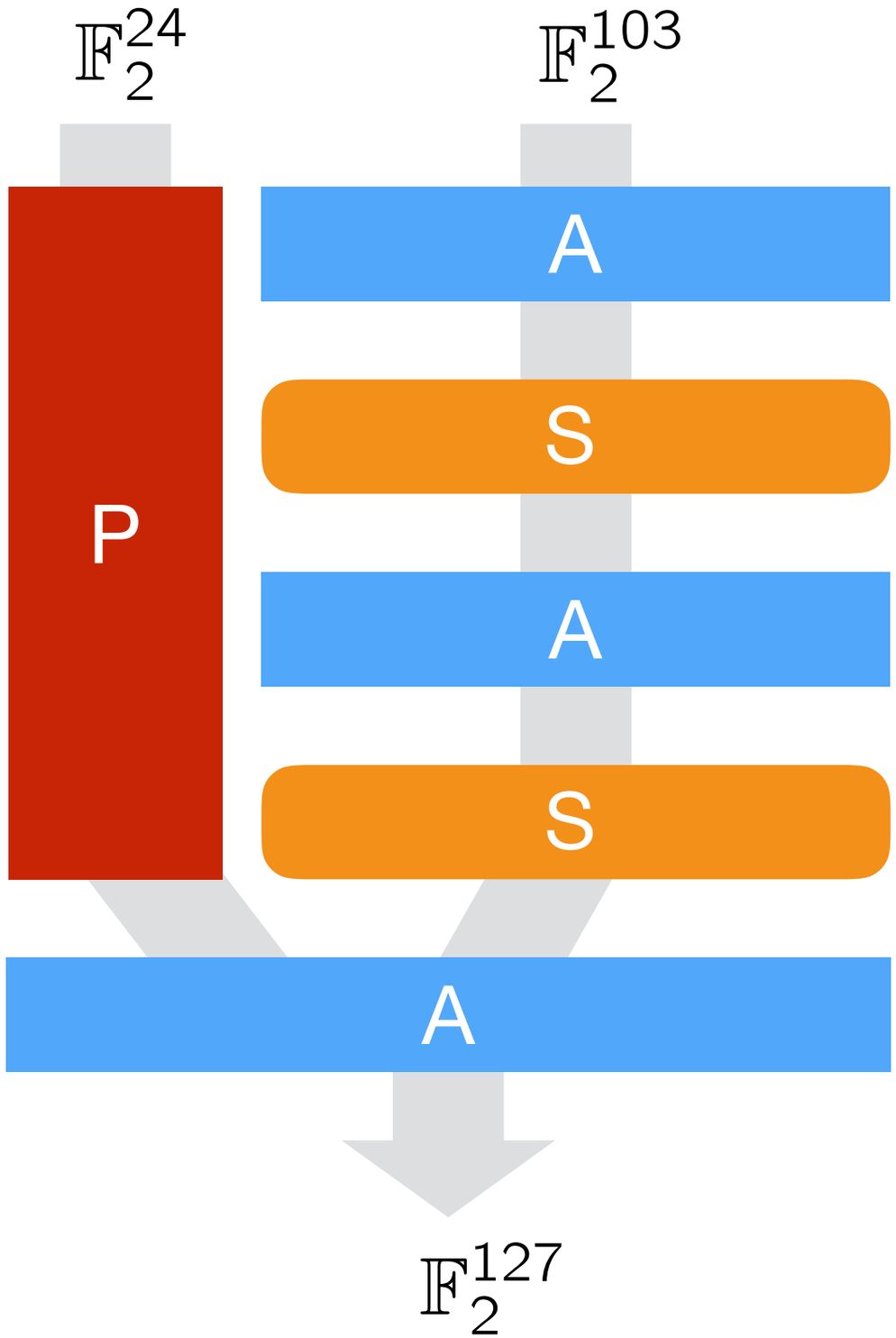


Introduced by Daemen in 1995, known for its use in Keccak.

Invertible for odd number of bits.

χ-based instance

Random degree-4 polynomials

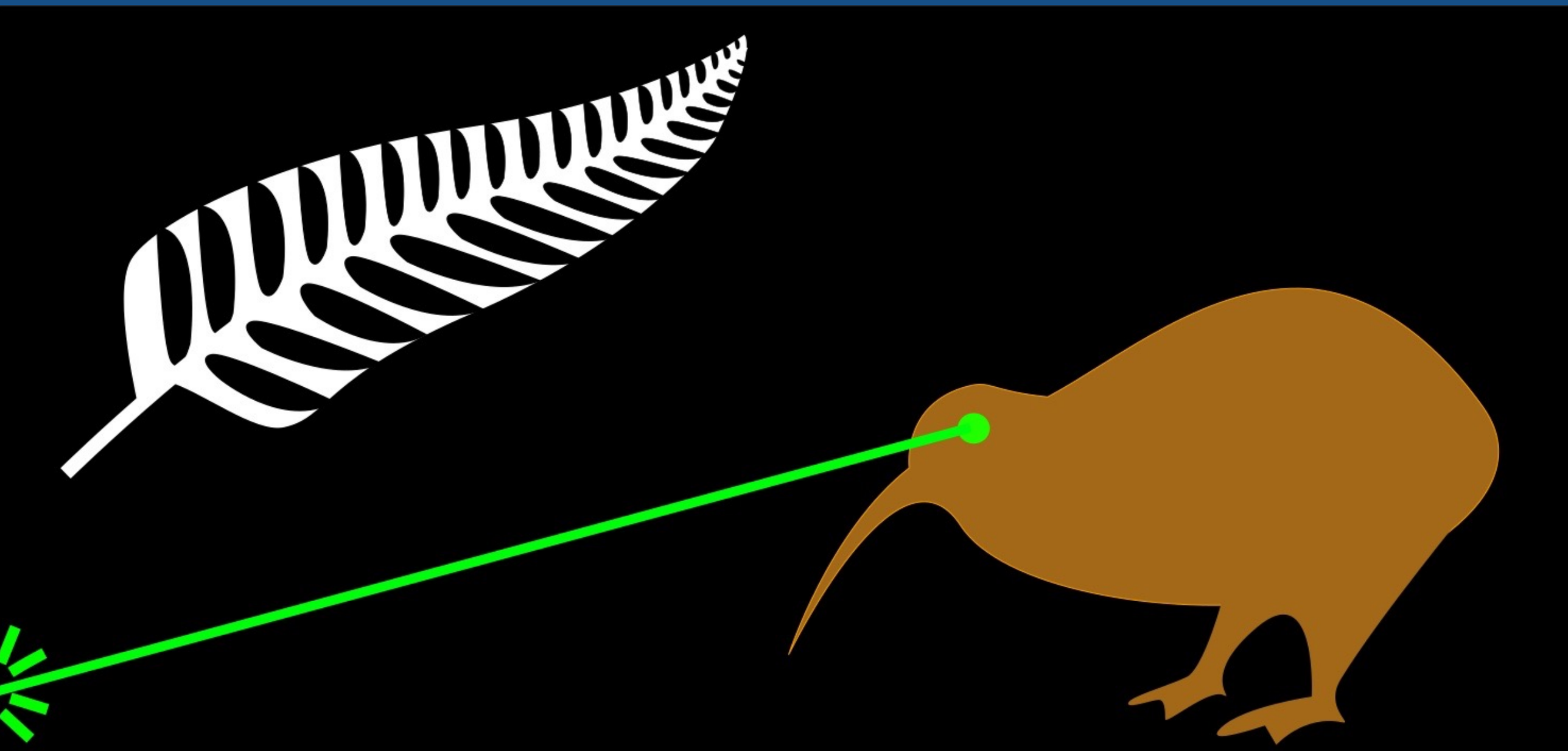


χ

χ

Random invertible affine layers

Attack!



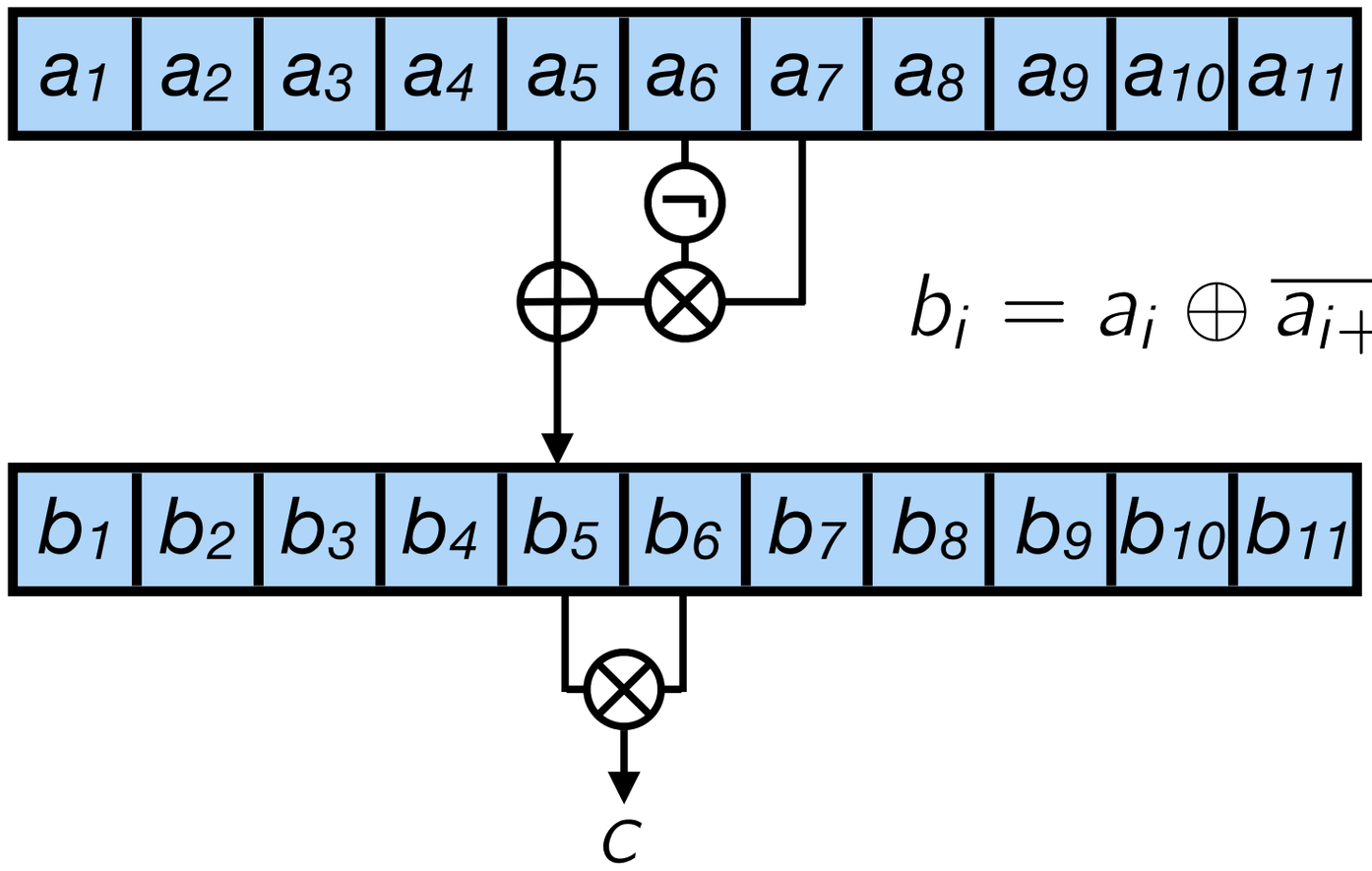
Cubes

A **cube** is an affine subspace [DS08].

Property : Let *f* be a degree-*d* polynomial over binary variables. If *C* is a cube of dimension *d+1*, then :

$$\sum_{c \in C} f(c) = 0$$

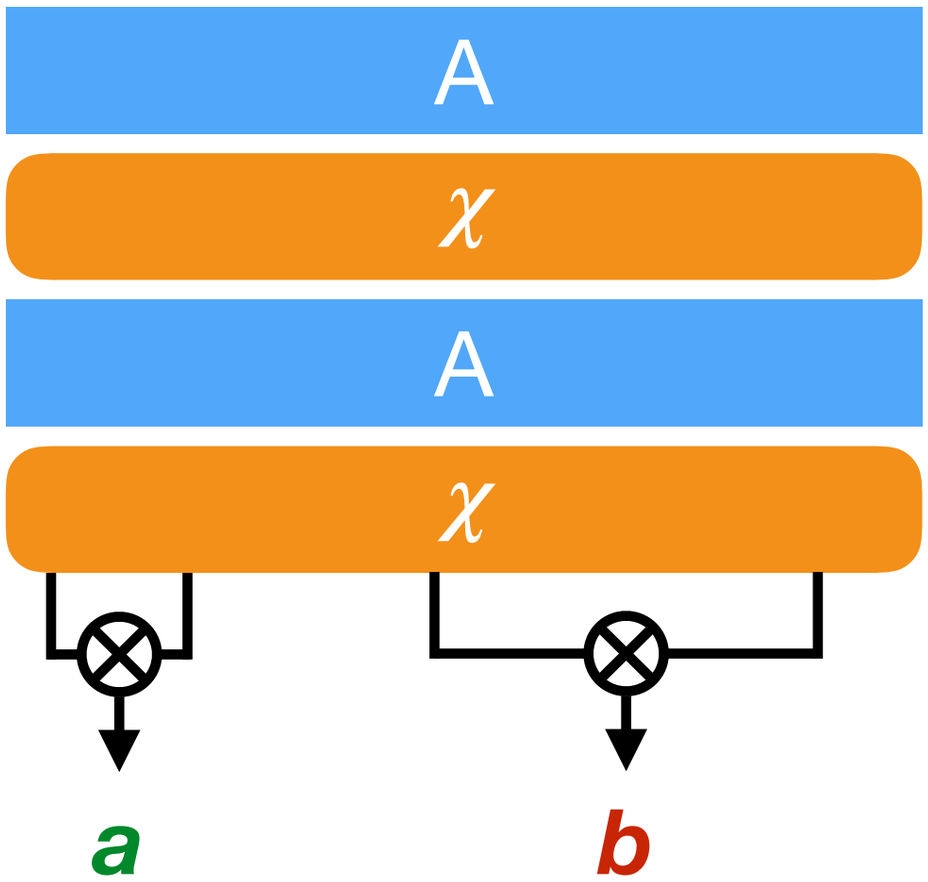
Degree deficiency



$$c = b_i \cdot b_{i+1}$$
$$= (a_i \oplus \overline{a_{i+1}} \cdot a_{i+2}) \cdot (a_{i+1} \oplus \overline{a_{i+2}} \cdot a_{i+3})$$

→ c has degree 3. Sums up to 0 over cube of dim 4.

ASASA Cryptanalysis



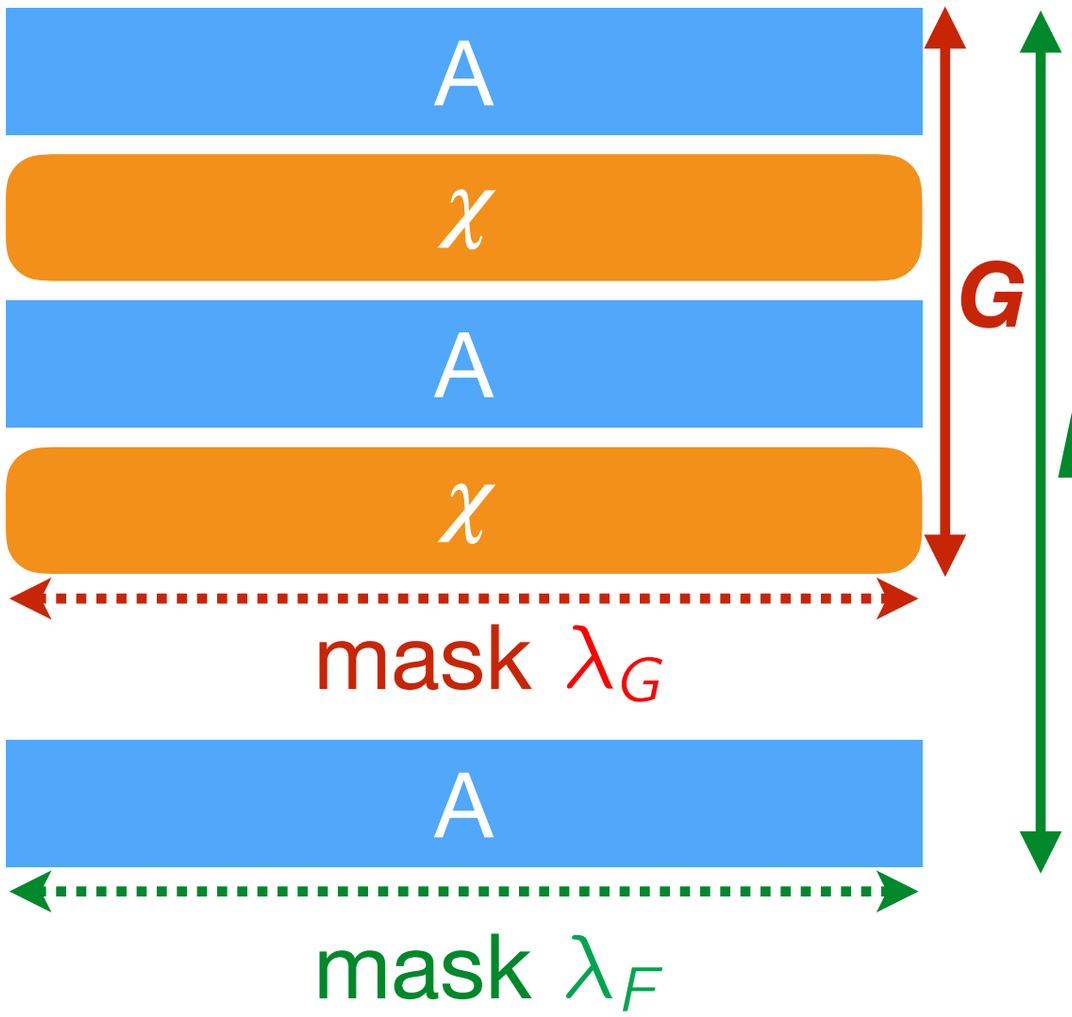
- Let ***a*** = product of 2 **adjacent** bits at the output of χ.

  Then ***a*** has degree 6.

- Let ***b*** = product of 2 **non-adjacent** bits at the output of χ.

  Then ***b*** has degree 8.

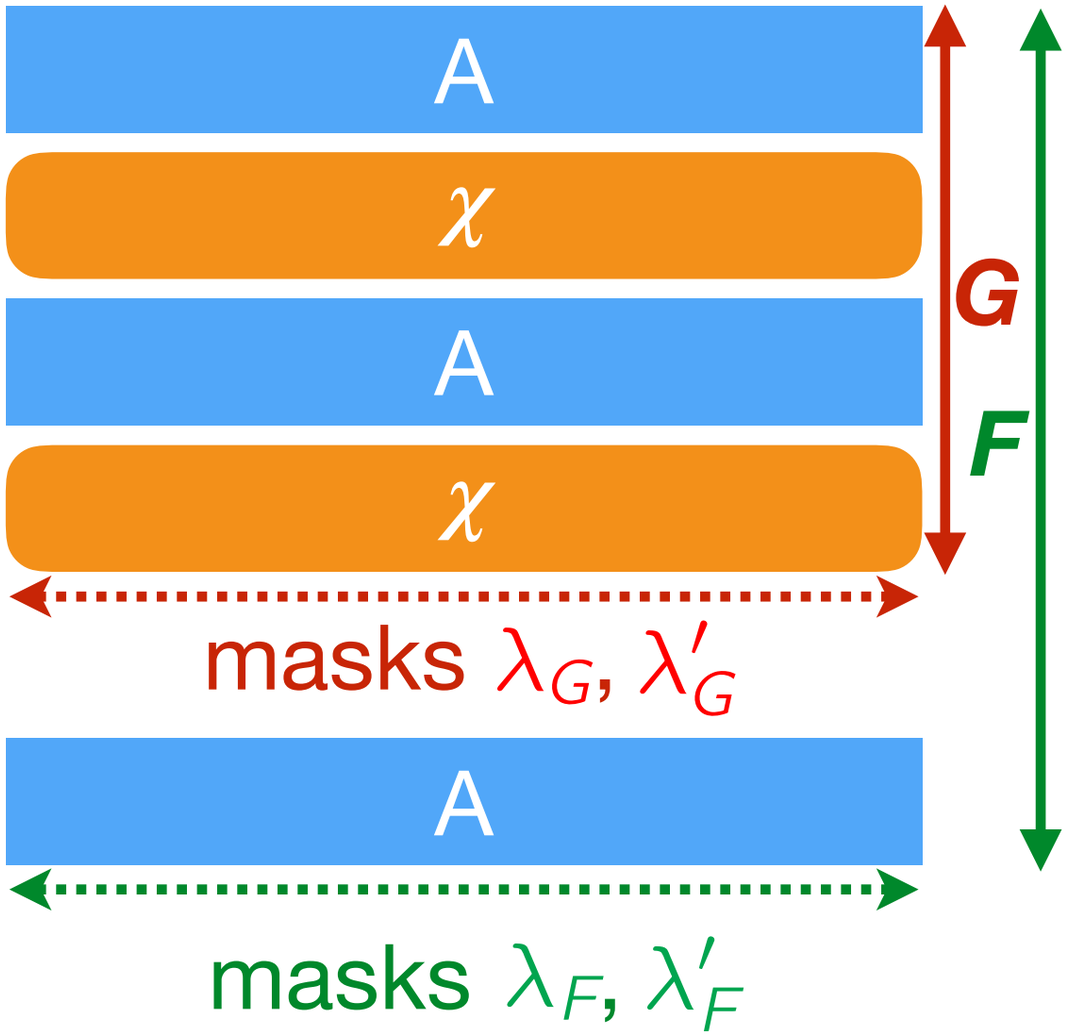
ASASA Cryptanalysis



Let λ_F be an output mask, i.e. we look at $\langle F|\lambda_F\rangle = x \mapsto \langle F(x)|\lambda_F\rangle$.

Then there exists a mask λ_G s.t. $\langle F|\lambda_F\rangle = \langle G|\lambda_G\rangle$.

ASASA Cryptanalysis

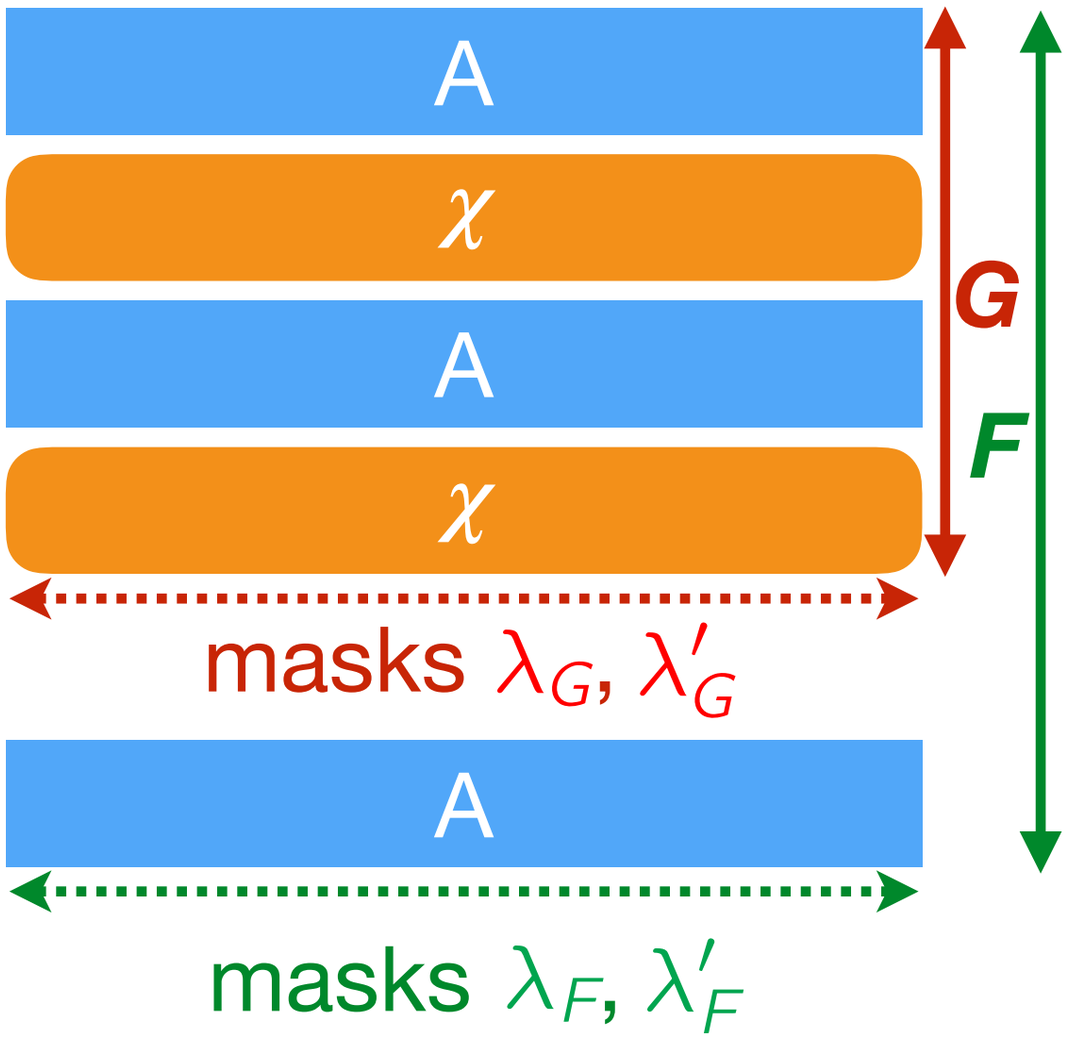


Let λ_F, λ'_F be two output masks, and λ_G, λ'_G the associated masks.

- If λ_G and λ'_G activate **single adjacent** bits, $\langle F|\lambda_F\rangle \cdot \langle F|\lambda'_F\rangle$ has degree 6.

- Otherwise $\langle F|\lambda_F\rangle \cdot \langle F|\lambda'_F\rangle$ has degree 8.

ASASA Cryptanalysis



Goal : Find λ_F, λ'_F such that

$$\deg(\langle F|\lambda_F\rangle \cdot \langle F|\lambda'_F\rangle) = 6$$

Let C be a dimension-7 cube. Then :

$$\Sigma_{c\in C}\langle F(c)|\lambda_F\rangle \cdot \langle F(c)|\lambda'_F\rangle = 0$$

→ we get an equation on λ_F, λ'_F.

ASASA Cryptanalysis

View λ_F, λ'_F as two vectors of n binary unknowns: $(\lambda_0, \ldots, \lambda_{n-1})$ and $(\lambda'_0, \ldots, \lambda'_{n-1})$. Then:

$$\begin{aligned}\sum_{c\in C}\langle F(c)|\lambda\rangle\langle F(c)|\lambda'\rangle &= \sum_{c\in C}\sum_{i<n}\lambda_i F_i(c)\sum_{j<n}\lambda'_j F_j(c)\\ &= \sum_{i,j<n}\left(\sum_{c\in C}F_i(c)F_j(c)\right)\lambda_i\lambda'_j\\ &= 0\end{aligned}$$

$\Rightarrow$ We get a quadratic equation on the λ_i, λ'_i's.

ASASA Cryptanalysis

Each cube yields 1 quadratic equation on the λ_i, λ'_i's.

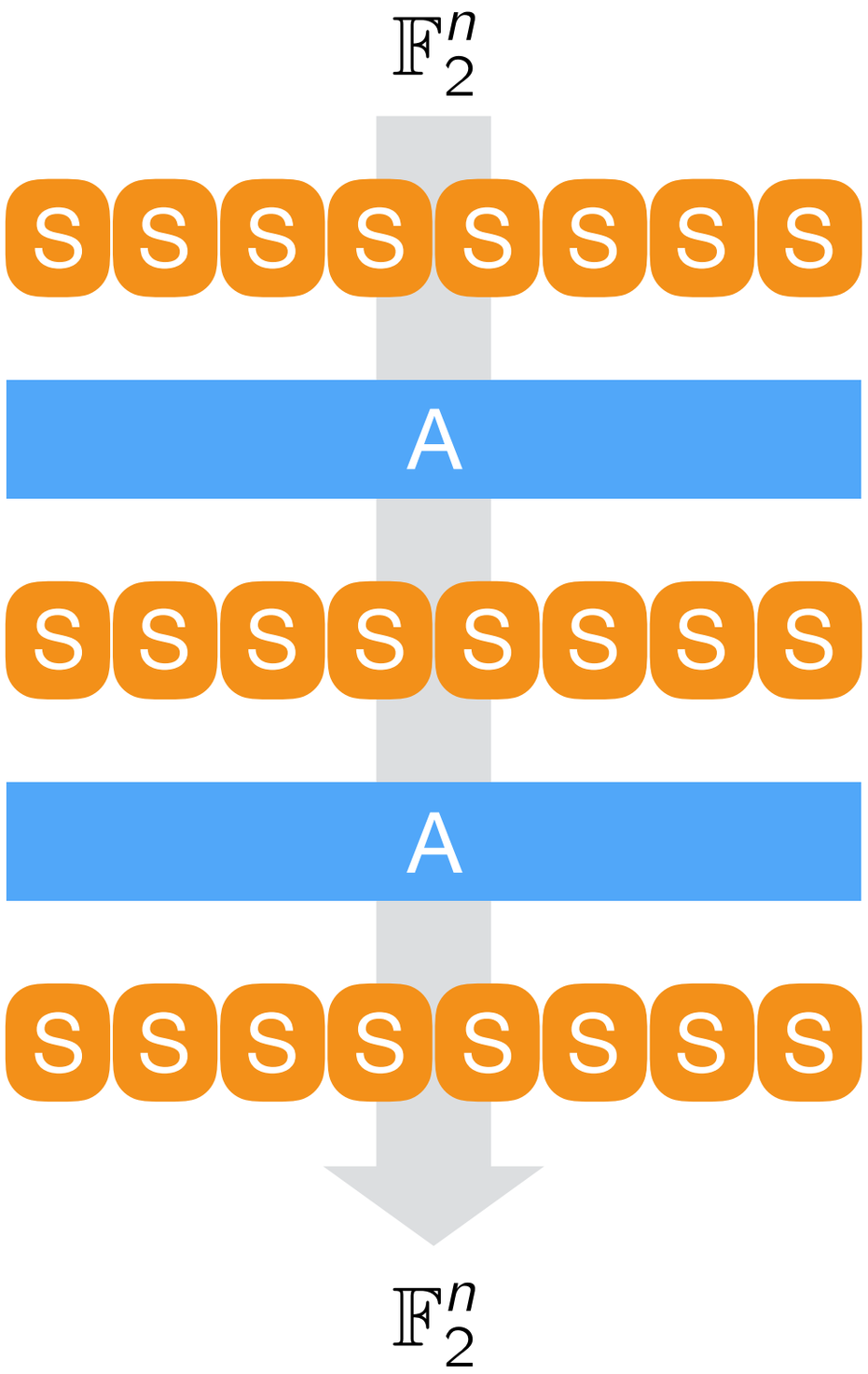
Using relinearization, there are $127^2 \approx 2^{14}$ terms $\lambda_i \lambda'_j$
→ we need 2^{14} cubes of dimension 7.

Resolving the system yields solution masks.
The last **A** layer is peeled off.
The rest (**ASAS**) can be broken in negligible time.

Conclusion: the scheme is broken using 2^{21} CP, and time complexity $\approx 2^{39}$ (for inverting a binary matrix of size 2^{13}).

“Black-box” ASASA

SASAS structure



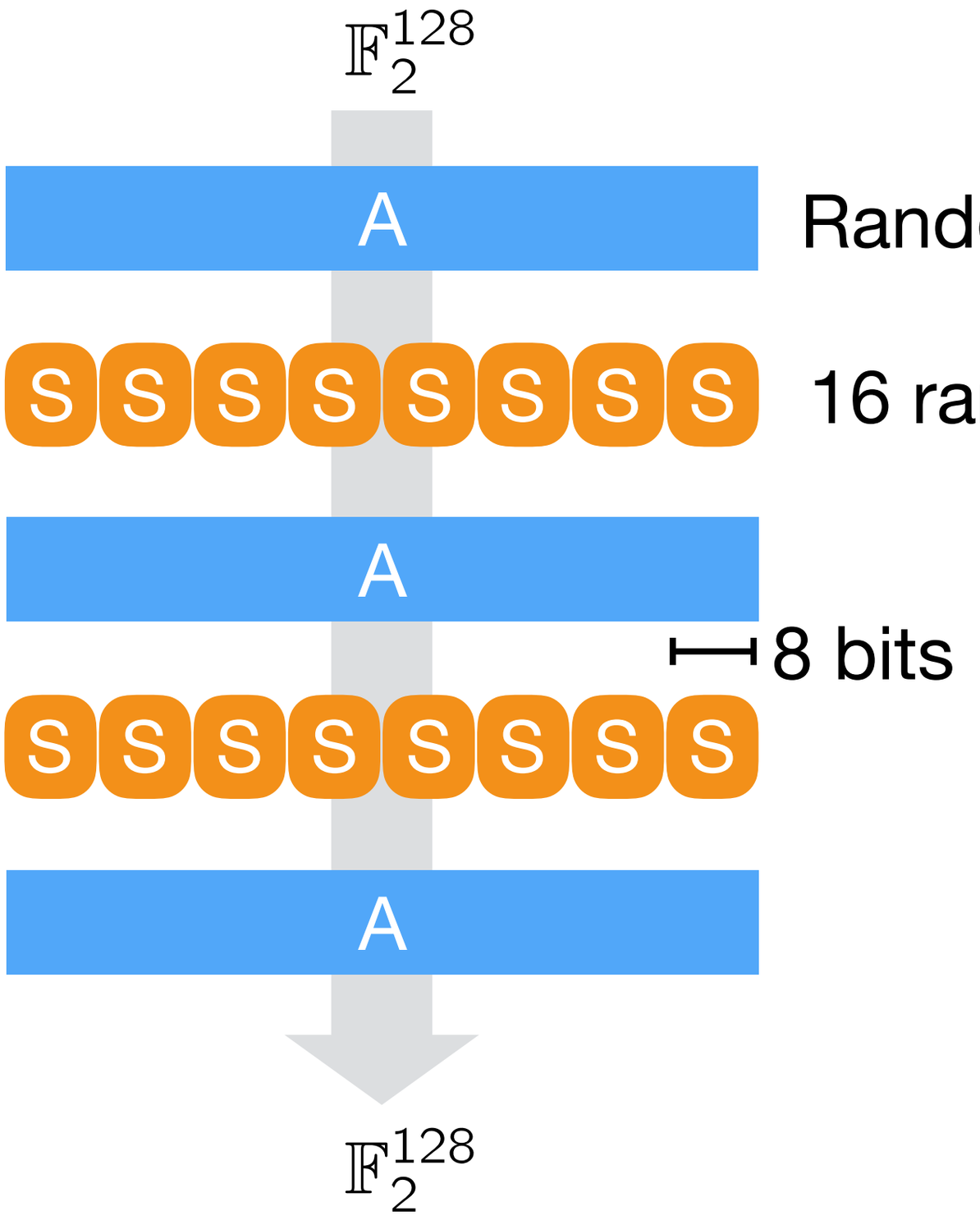
Analyzed by Biryukov and Shamir at Eurocrypt 2001.

Random **A**ffine layer over *n* bits.

Random independent **S**-boxes over *k* bits each.

→ **Goal**: recover all internal components (affine layers **A** and **S**-boxes) with only “black-box” access (KP/CP/CC).

Black-box ASASA [BBK14]



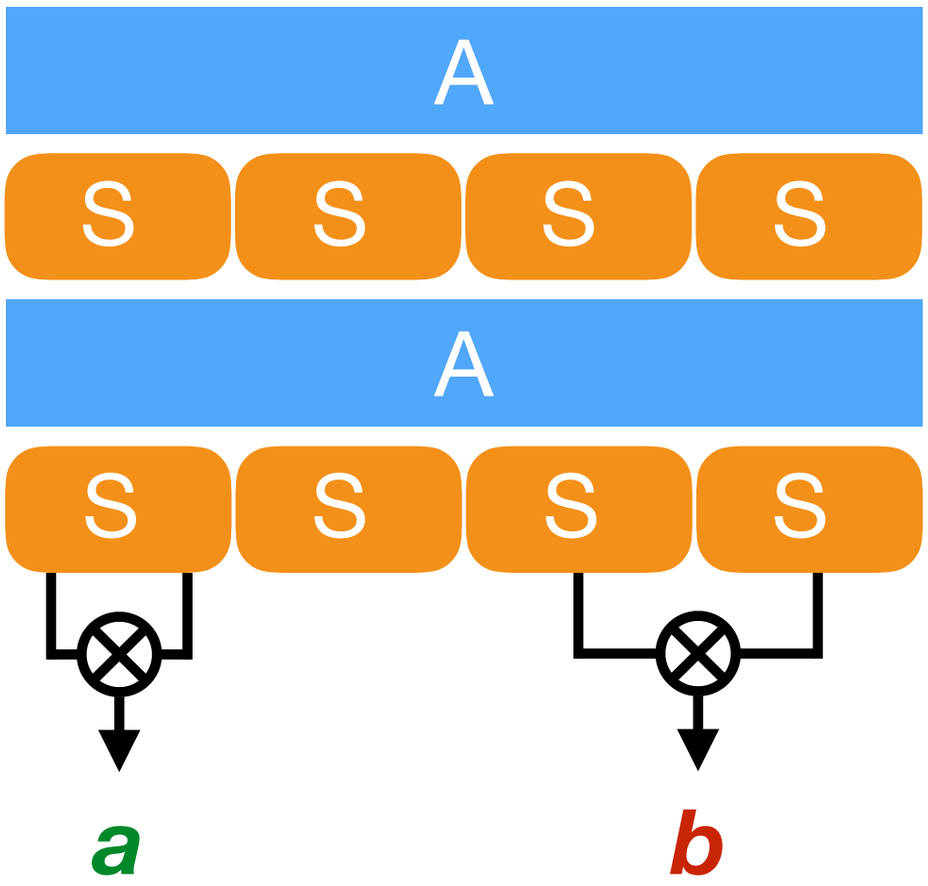
Random **A**ffine layer over 128 bits.

16 random independent **S**-boxes

Goal : recover all internal components.

Note: degree ≤ 49
⇒ distinguisher w. 2^{50} CP

ASASA cryptanalysis



Degree of an S-box = 7.

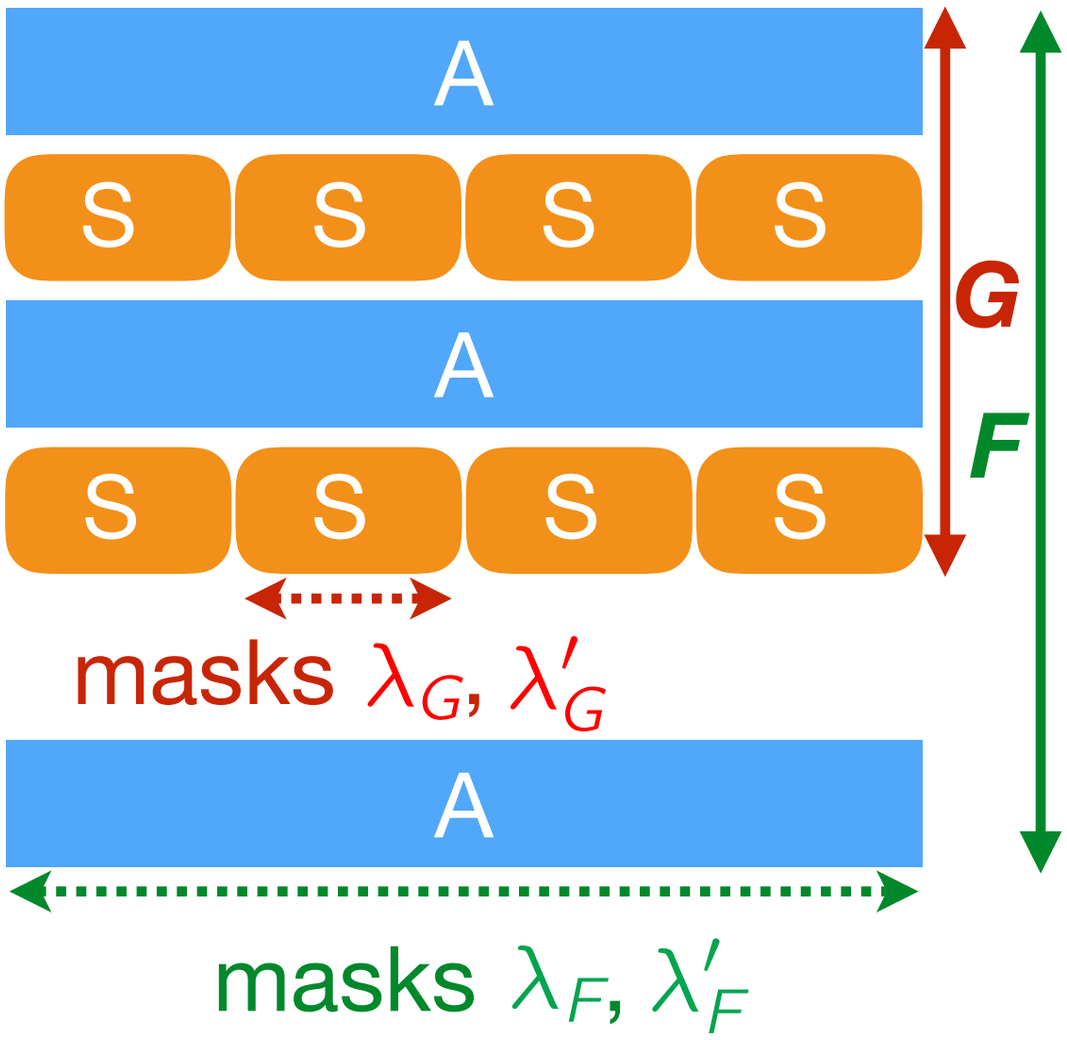
- Let ***a*** = product of 2 output bits of a **single common** S-box.

  Then ***a*** has degree 7x7 = 49.

- Let ***b*** = product of 2 output bits of two **distinct** S-boxes.

  Then ***b*** has max degree (127).

Cryptanalyse de ASASA



Goal : Find λ_F, λ'_F such that

$$\deg(\langle F|\lambda_F\rangle \cdot \langle F|\lambda'_F\rangle) = 49$$

Let C be a dimension-50 cube. Then:

$$\Sigma_{c\in C}\langle F(c)|\lambda_F\rangle \cdot \langle F(c)|\lambda'_F\rangle = 0$$

→ we get an equation on λ_F, λ'_F.

Conclusion : All internal components are recovered in time and data complexity 2^{63}. In general: $n^2 2^{(m-1)^2}$.
For comparison: the distinguisher is in 2^{50}. In general $2^{(m-1)^2+1}$.

Cryptanalysis de SASASASAS

Recent work by Biryukov et Khovratovich: the same attack extends ASASASA and even SASASASAS (ePrint, june 2015).

Indeed the main obstacle is that the overall function must not be full degree (→ use results by Boura, Canteaut and Cannière on the degree of composite boolean functions).

Conclusion

- A new attack on ASASA-type structures.

- Not presented: LPN-based attack on the χ-based scheme, heuristic attack on white-box scheme.

- Regarding multivariate ASASA proposals, [GPT15] and our result are somewhat complementary.

- Open problems:

  Other applications of this type of attack.

  Secure white-box scheme.

Conclusion

Thank you for your attention!

Questions ?