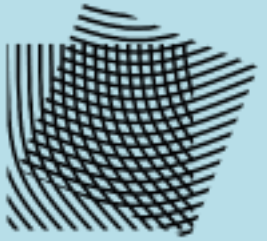


SYMMETRIC KEY TECHNIQUES IN SIDE-CHANNEL COUNTERMEASURES: IMPLEMENTING A NEW THRESHOLD

Svetla Nikova

COSIC, KU Leuven

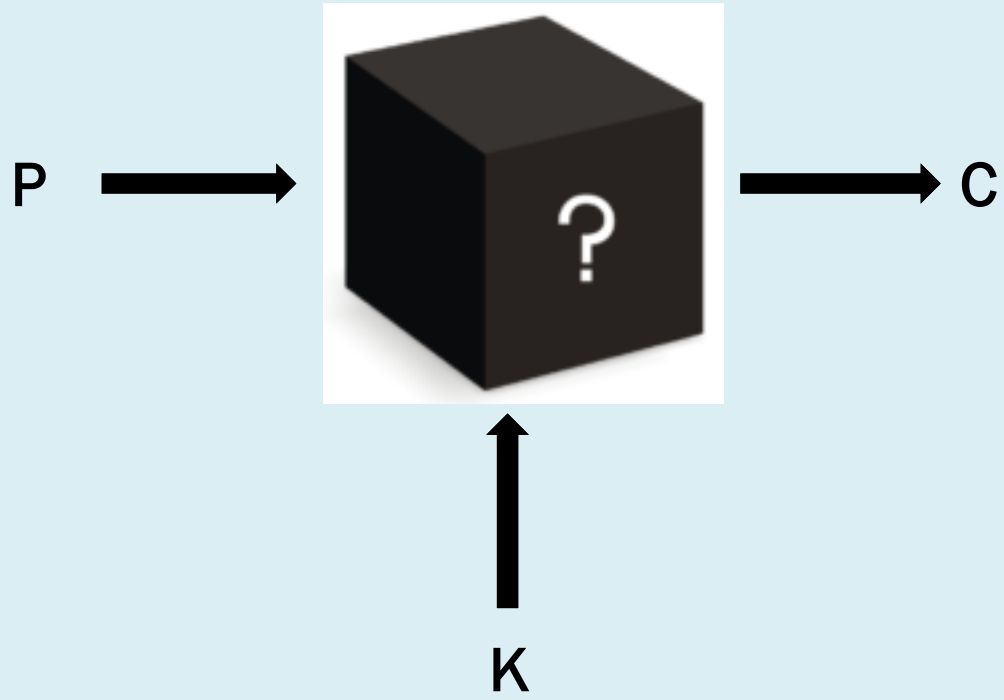
Based on joint work with colleagues from COSIC, KU Leuven and NXP among which: B. Bilgin, K. Varici, V. Rijmen, S. Dhooghe, V. Nikov, etc.

KU LEUVEN

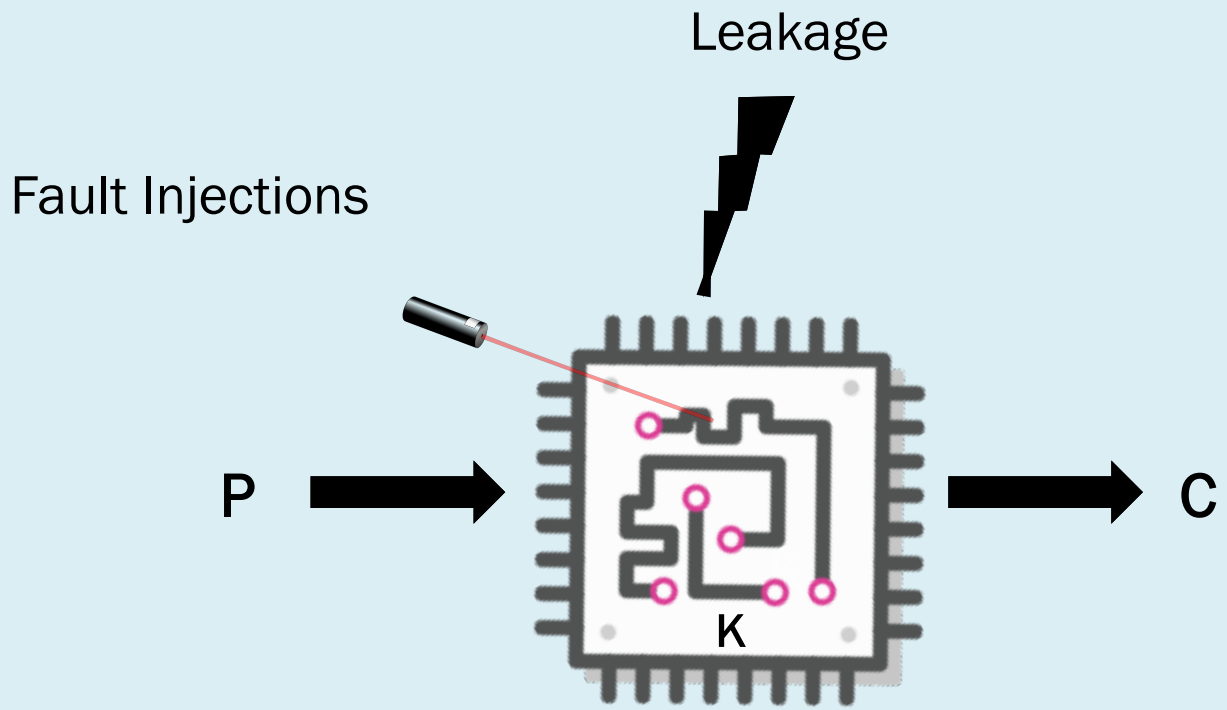
Thanks to Siemen Dhooghe for part of the slides

INTRODUCTION

The black box setting



The grey box setting



Masking

Basic idea: Split the data in shares and operate on them

To compute $y = f(x)$, we split $x = x_1 + x_2$

think of x_1 as one-time pad encryption of x with a key x_2

Then y can be recovered from $y_1 = f_1(x_1)$ and $y_2 = f_2(x_2)$

note that $f_1(x_1)$ reveals nothing about x

Even if an adversary compromises an entire part of the chip ($f_1(x_1)$)

no sensitive data is leaked

This is (essentially) a variant of the wire probe model of Ishai, Sahai and Wagner

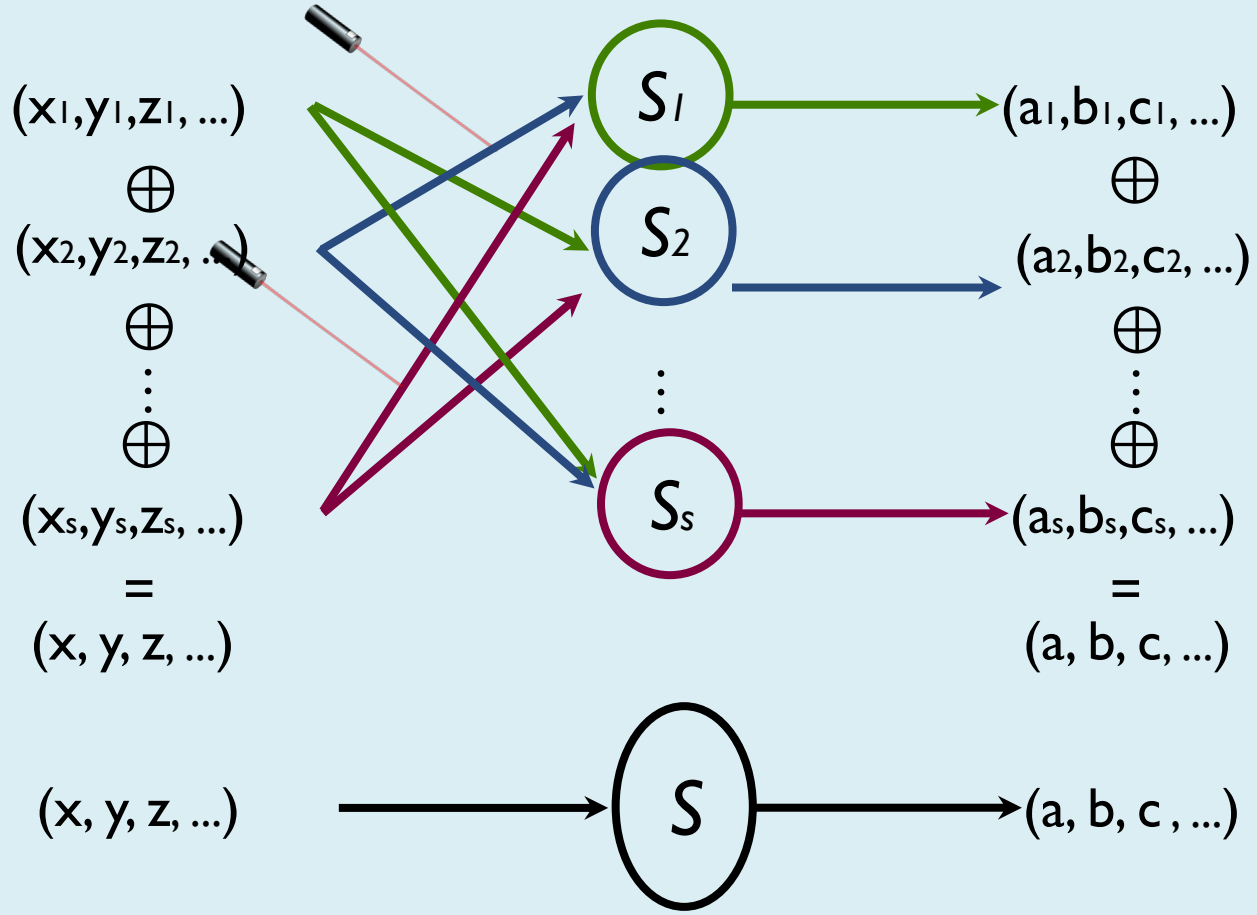
TI & BOOLEAN FUNCTIONS

Threshold Implementations (TI) in a nutshell

- Secure implementations in HW are more challenging than in SW because of physical effects like **glitches** which cause additional leakage

- TI is a provably secure masking scheme based on SSS and MPC
- Initially proposed for 1st order SCA [NRR06] extended to any order [BGNNR14]
- The first countermeasure secure in circuits with physical defaults like glitches
- Efficient (area, performance, latency, power, energy) in HW
- Any HW technology

TI conditions



Correctness, Non-completeness, Uniformity

Higher-order Threshold Implementations

- d-th order Non-completeness [BGNNR14]

Property 2 (d^{th}-order non-completeness). Any combination of up to d component functions f_i of F must be independent of at least one input share.

- d+1 TI always leads to a sharing which is expansion: $s_{in} = d + 1, s_{out} \geq (d + 1)^t$
- Higher-order td+1 TI also can lead to expansion

Theorem 2. *There always exist a d^{th}-order TI of a function of degree t that requires $s_{in} \geq t \times d + 1$ input and $s_{out} \geq \binom{s_{in}}{t}$ output shares.*

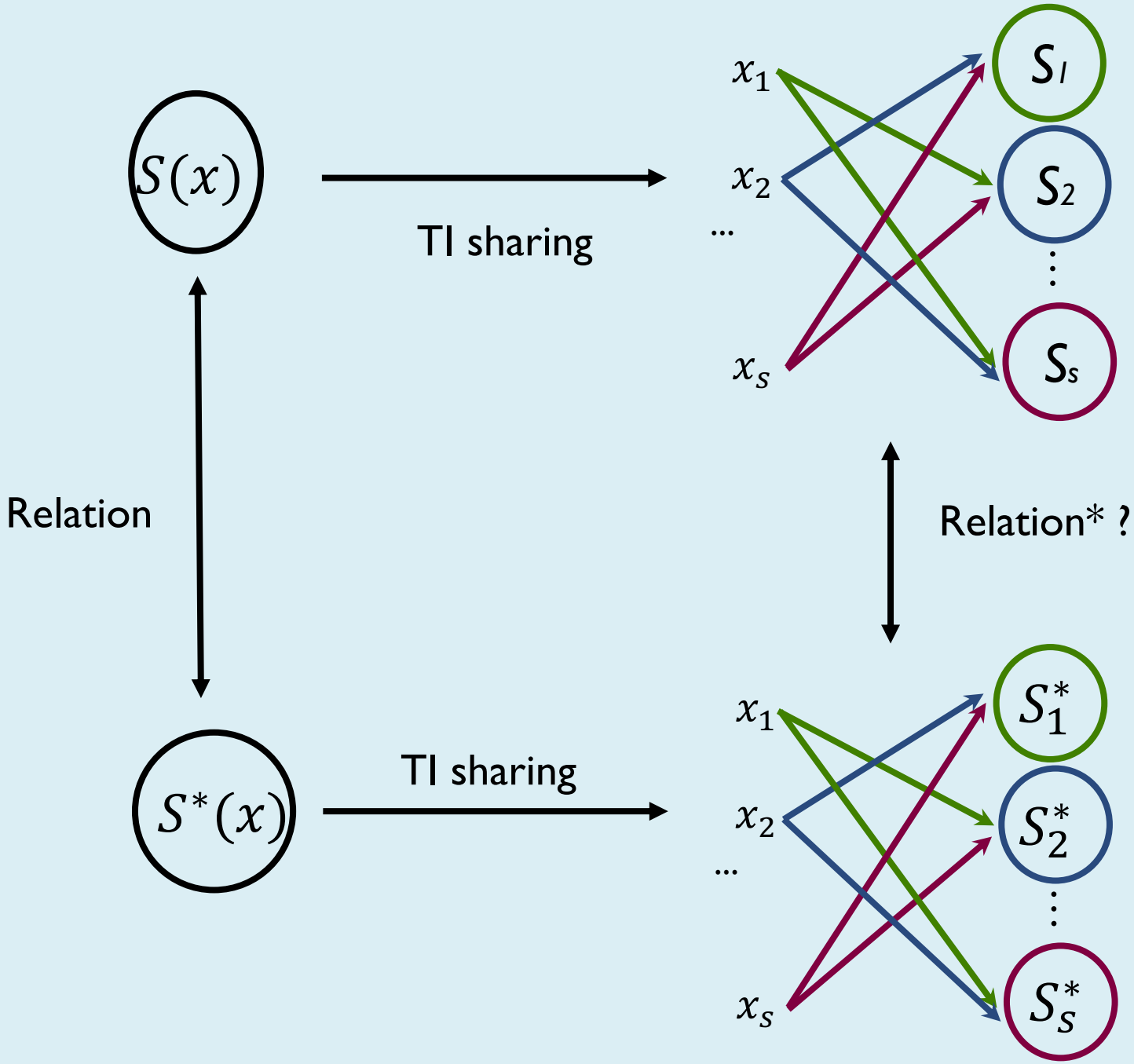
Sharings for higher-order Threshold Implementations

Definition 2 ([Pet19]). *A d^{th}-order non-complete set covering $\mathcal{C}^{nc}(s,t,d)$ is a set of subsets from the universe of the inputs, $\mathcal{U}_s = \{1,\ldots,s\}$, such that:*

1. *each t-subset of $\mathcal{U}_s$ is a subset of at least one element of $\mathcal{C}^{nc}(s,t,d)$,*
2. *each element of $\mathcal{C}^{nc}(s,t,d)$ has size at least t, and*
3. *a minimum of $d+1$ elements of $\mathcal{C}^{nc}(s,t,d)$ are needed to cover $\mathcal{U}_s$.*

Example of a set covering: $\mathcal{C}^{nc}(3,2,1) = \{\{1,2\},\{2,3\},\{1,3\}\}$

Lemma 27 ([Pet19]) *If $s \geq td+1$ then for every $\mathcal{C}^{nc}(s,t,d)$ there exists $\mathcal{C}^{nc}(s+1,t,d)$ of equal cardinality.*


$S(x)$
TI sharing
x_1
x_2
...
x_s
S_1
S_2
S_s
Relation
Relation* ?
$S^*(x)$
TI sharing
x_1
x_2
...
x_s
S_1^*
S_2^*
S_s^*

Affine equivalence (1)

- 302 affine equivalent classes of 4x4 S-boxes - S'=AoSoB [BNNRS12]
- There are 1 affine, 6 quadratic and 295 cubic 4x4 classes
- Half of the 4x4 S-boxes belong to A_{16}

- The affine and the quadratic S-boxes can be shared with 3 shares
- The cubic are shared with 4 or 5 shares or using decomposition

remark	unshared	3 shares				4 shares			5 shares
		1	2	3	4	1	2	3	1
affine	1	1				1			1
quadratic	6	5	1			6			6
cubic in A_{16}	30		28	2			30		30
cubic in A_{16}	114			113	1			114	114
cubic in $S_{16} \setminus A_{16}$	151					4	22	125	151

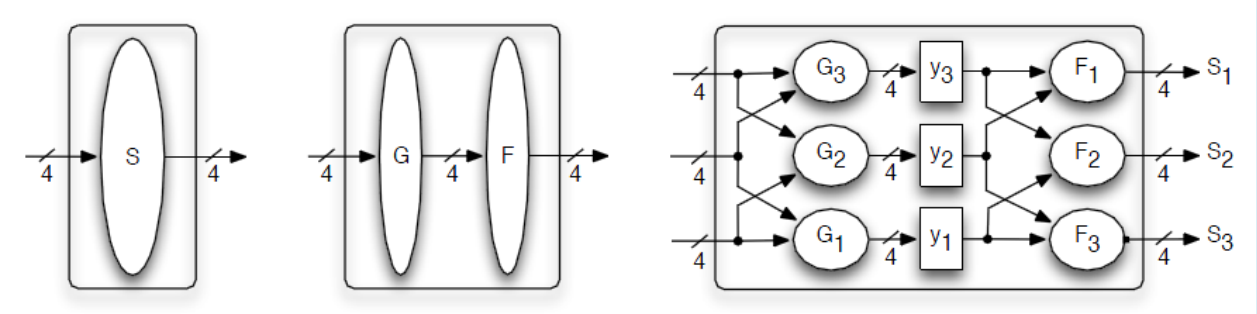
Affine equivalence (2)

- 4 affine equivalent classes of 3x3 S-boxes (Bilgin et al. [BNNRS12])
- There are 1 affine and 3 quadratic 3x3 classes – shared with 3 and 4 shares

- 75 quadratic classes for 5-bit permutations classified by Bozilov et al. [BBS17]
- 30 of them have sharing with 3 shares, all of them have sharing with 4 shares

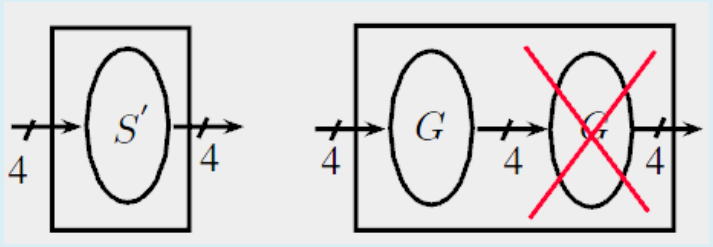
- 2263 quadratic classes for 6-bit permutations classified by De Meyer and Bilgin [DB18]

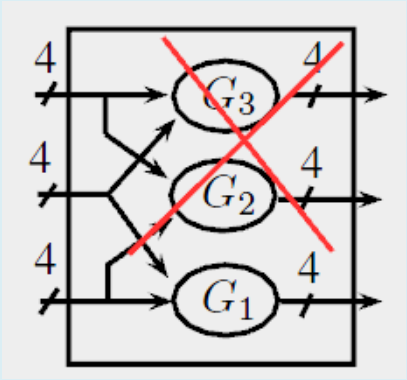
Decomposition – reduces the degree

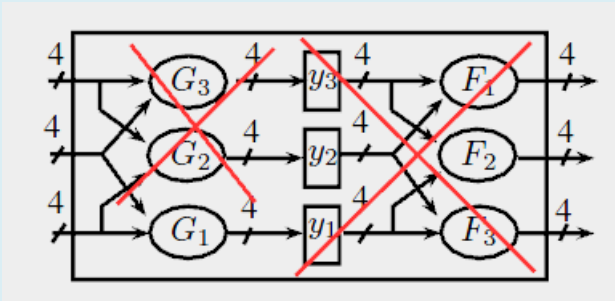


- Poschmann et al. [PMKLWL11] for the Present S-box
- Classification and decomposition of all 3x3 and 4x4 S-boxes, [BNNRS12]
- A cubic 4 bit S-box can be decomposed on 2 or more quadratic S-boxes in this way only if it belongs to the Alternative group.
- What are the conditions for an n-bit permutation to have a decomposition?

Decomposition – optimizations

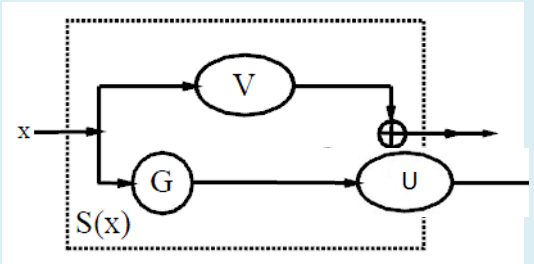


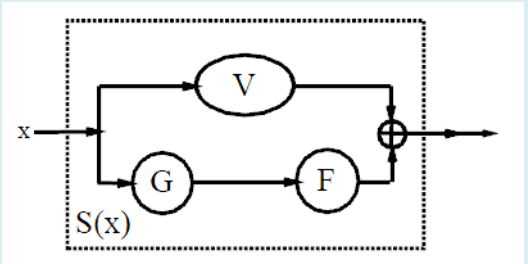


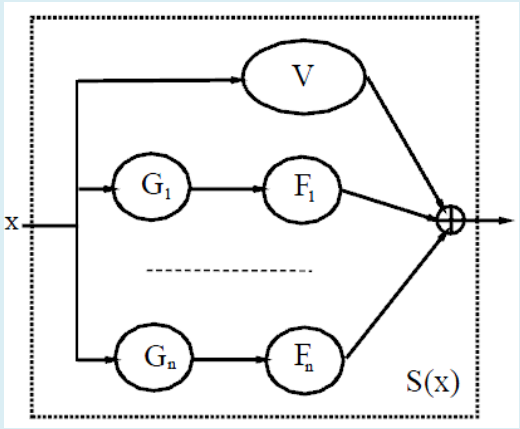


- Kutzner et al. [KHPW12] again for the Present S-box
- Implemented with 3 shares S' = G(G(.))
- $G_1 = G_2 = G_3$

Decomposition – factorization







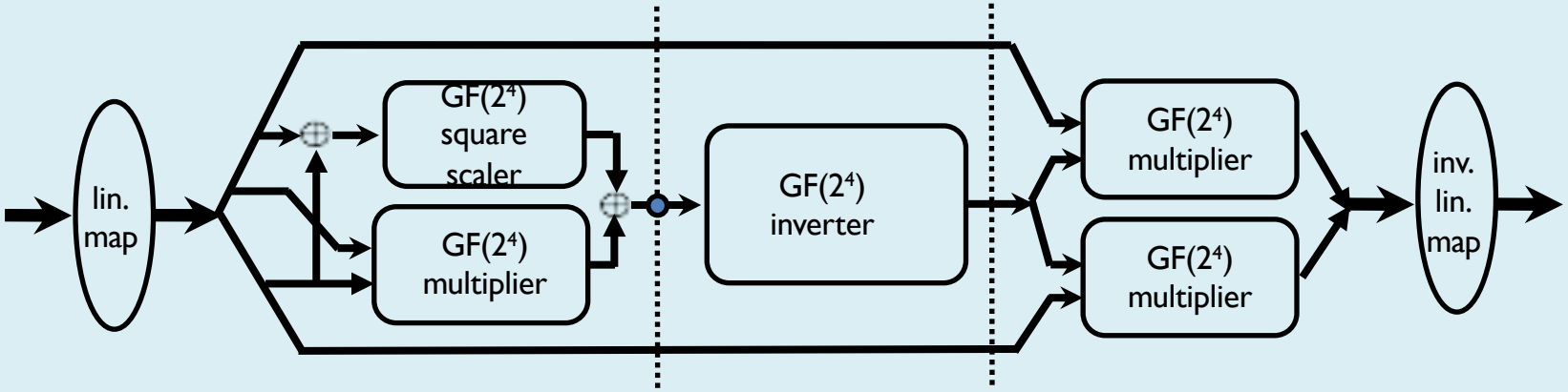
For cubic s-boxes S(.) can be used the following approach proposed by Kutzner et al. [KNP12]

- Factorization S(.) = U(.) + V(.)
- U(.) contains all the cubic terms, V(.) quadratic
- U(.) = F(G(.)) is decomposed with quadratic F(.) and G(.)

Evaluating an S-box

If we have an n-bit permutation we can either:

- Work with the Boolean functions
- Use the tower field approach, i.e. work in the sub-field(s) e.g. Canright
- Work in GF(2^n): Polynomial presentation of the S-box [RP10]
- Nikova et al. [NNR18]: Decomposition of the inverse power function in GF(2^n) for n up to 16 on quadratic functions



How to construct “good” S-boxes (1)

- Shannon-expansion
- S_i n-bit permutations
- F_i, G_i Boolean functions

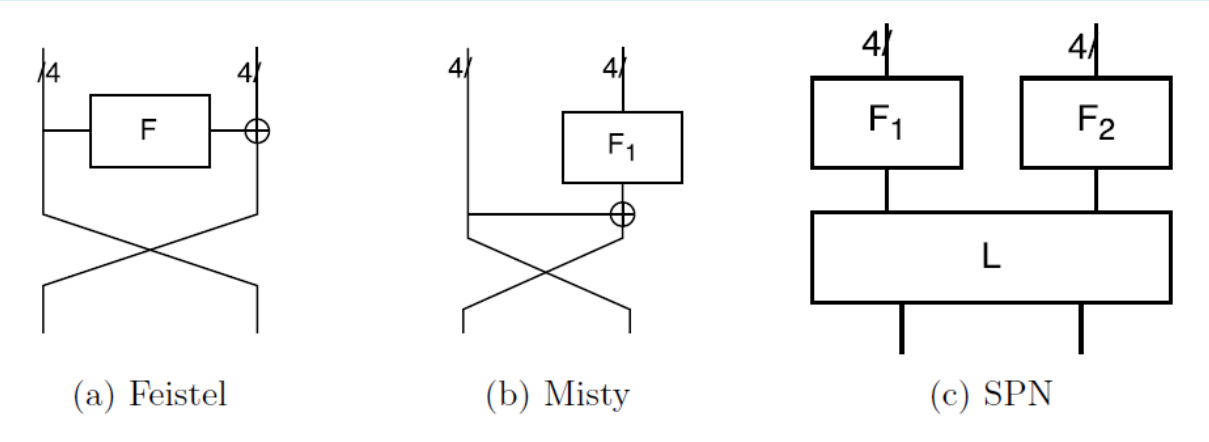
$(\bar{x}, x_{n+1} = 0)$	$(\bar{x}, x_{n+1} = 1)$
$(S_2(\bar{x}), G(\bar{x}))$	$(S_1(\bar{x}), F(\bar{x}))$

$(\bar{x}, x_{n+1} = 0, x_{n+2} = 0)$	$(\bar{x}, x_{n+1} = 0, x_{n+2} = 1)$	$(\bar{x}, x_{n+1} = 1, x_{n+2} = 0)$	$(\bar{x}, x_{n+1} = 1, x_{n+2} = 1)$
$(S_4(\bar{x}), G_2(\bar{x}), G_4(\bar{x}))$	$(S_3(\bar{x}), F_2(\bar{x}), F_4(\bar{x}))$	$(S_2(\bar{x}), G_1(\bar{x}), G_3(\bar{x}))$	$(S_1(\bar{x}), F_1(\bar{x}), F_3(\bar{x}))$

- S is an (n+1)-bit permutation or an (n+2)-bit permutation when certain relations between the functions hold, Varici et al. [VNNR18]

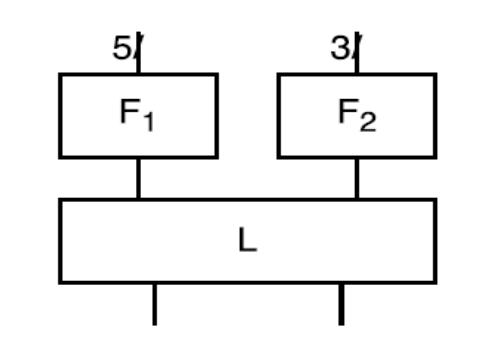
How to construct “good” S-boxes (2)

- Boss et al. [BGGLMS17],

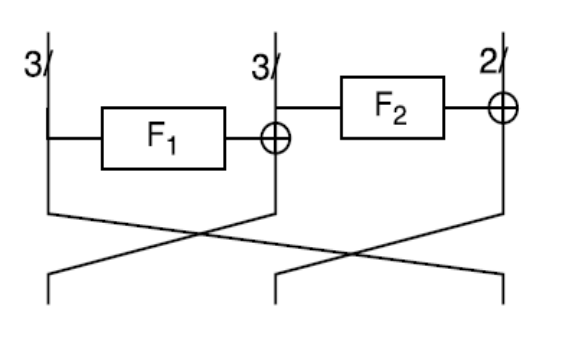


(a) Feistel (b) Misty (c) SPN

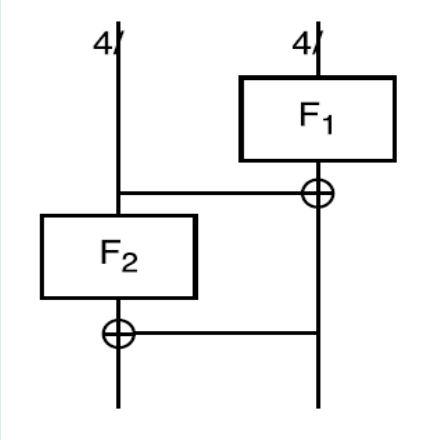
- De Meyer and Varici [DV17]



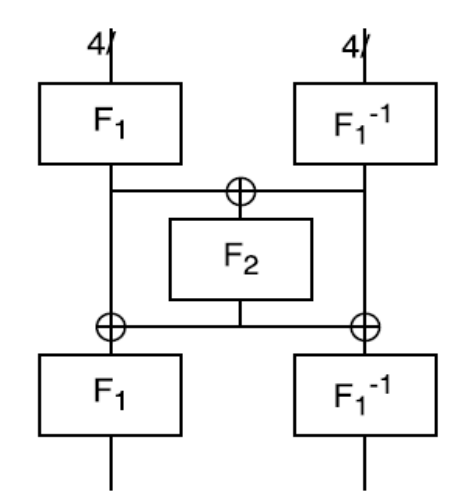
Asymmetric SPN



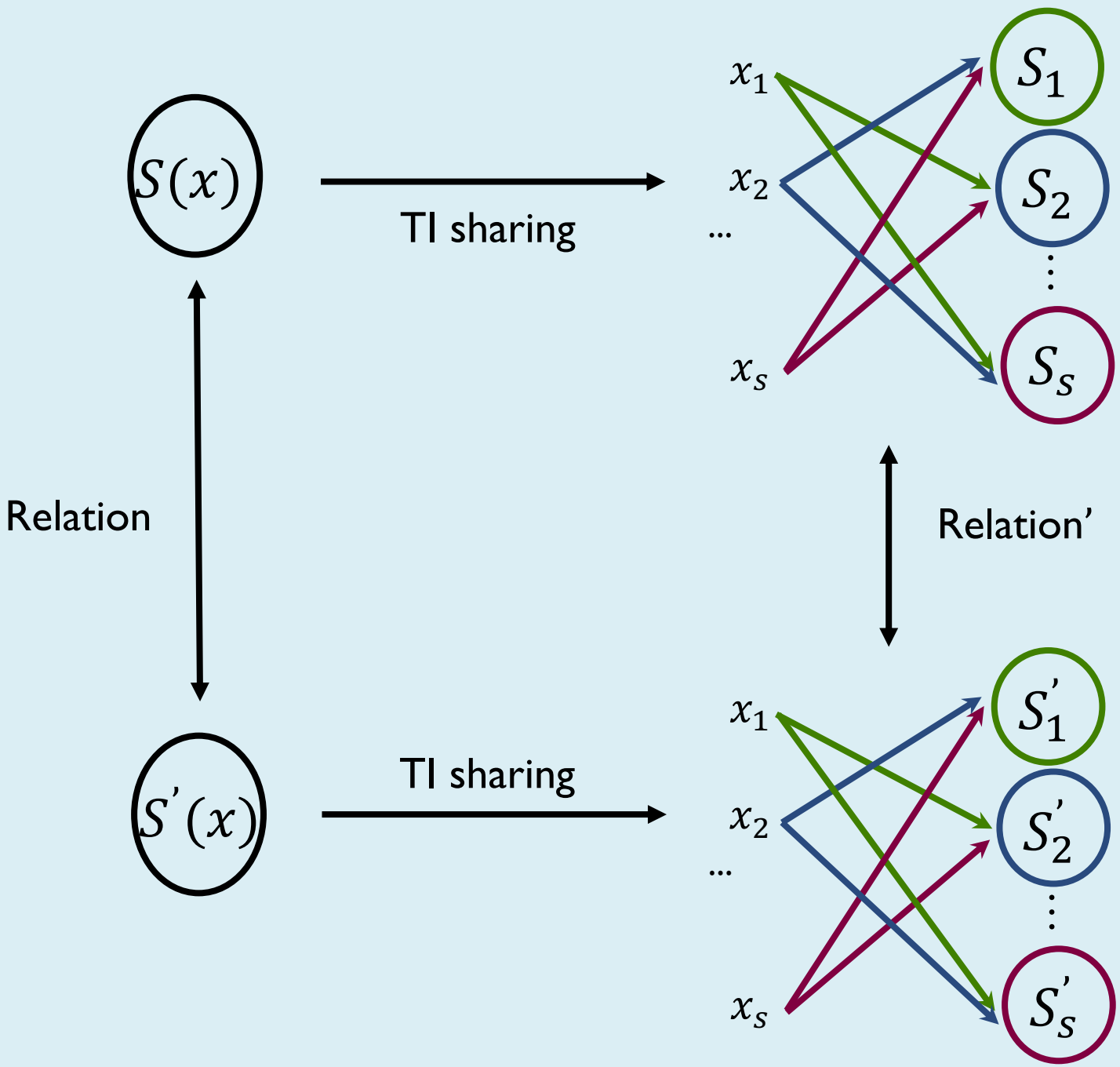
3-bit Feistel



Double Misty



Whirlpool



Open question:

Under what conditions
the inverse of the TI sharing is
a **TI sharing of the inverse S-box**?

RECENT RESULTS

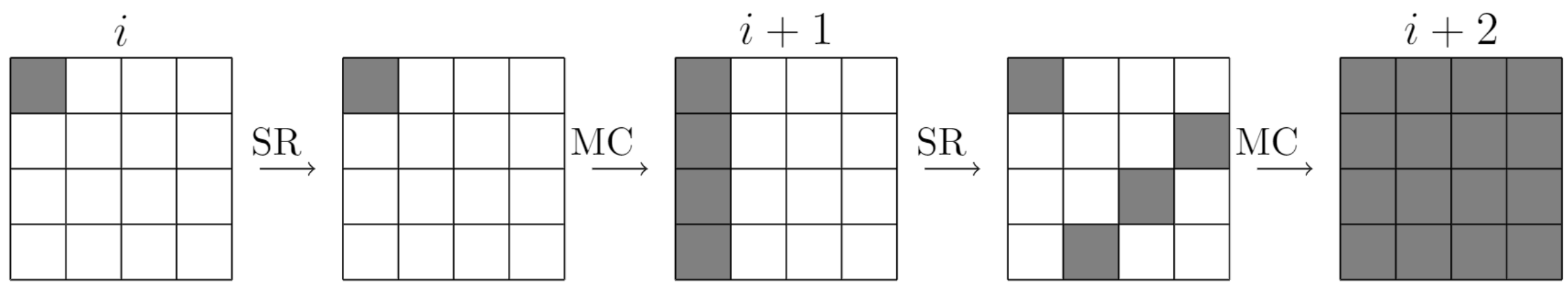
Cryptanalysis of masked ciphers

- The entropy of observed shared values can be bounded in terms of the nontrivial Fourier coefficients of its distribution
- We can use linear cryptanalysis (where the secret is fixed)
- We need sharings with low maximum absolute correlation
  - *High nonlinearity of the sharing (without considering the last component function of a share)*
- This reduces the need for extra randomness

Tim Beyne and Siemen Dhooghe and Zhenda Zhang, “Cryptanalysis of Masked Ciphers: A not so Random Idea”, to appear at AsiaCrypt 2020.

Why nonlinearity provides security

- AES Diffusion Pattern



- Strong diffusion guarantees security of power samples which are “close” together
- Further rounds activate many strong S-boxes

Open problems

- Is it possible to give bounds for the maximum absolute correlation of the sharing given the correlation of the S-box?
- Since shared S-boxes are large, can we speed up verification techniques?
- How to construct strong nonlinear sharing?

Protecting PRESENT

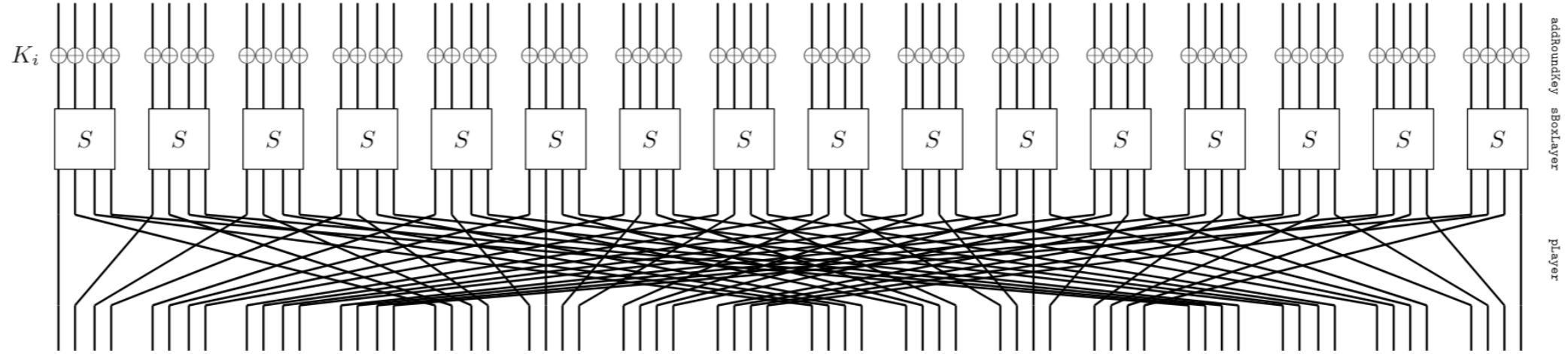
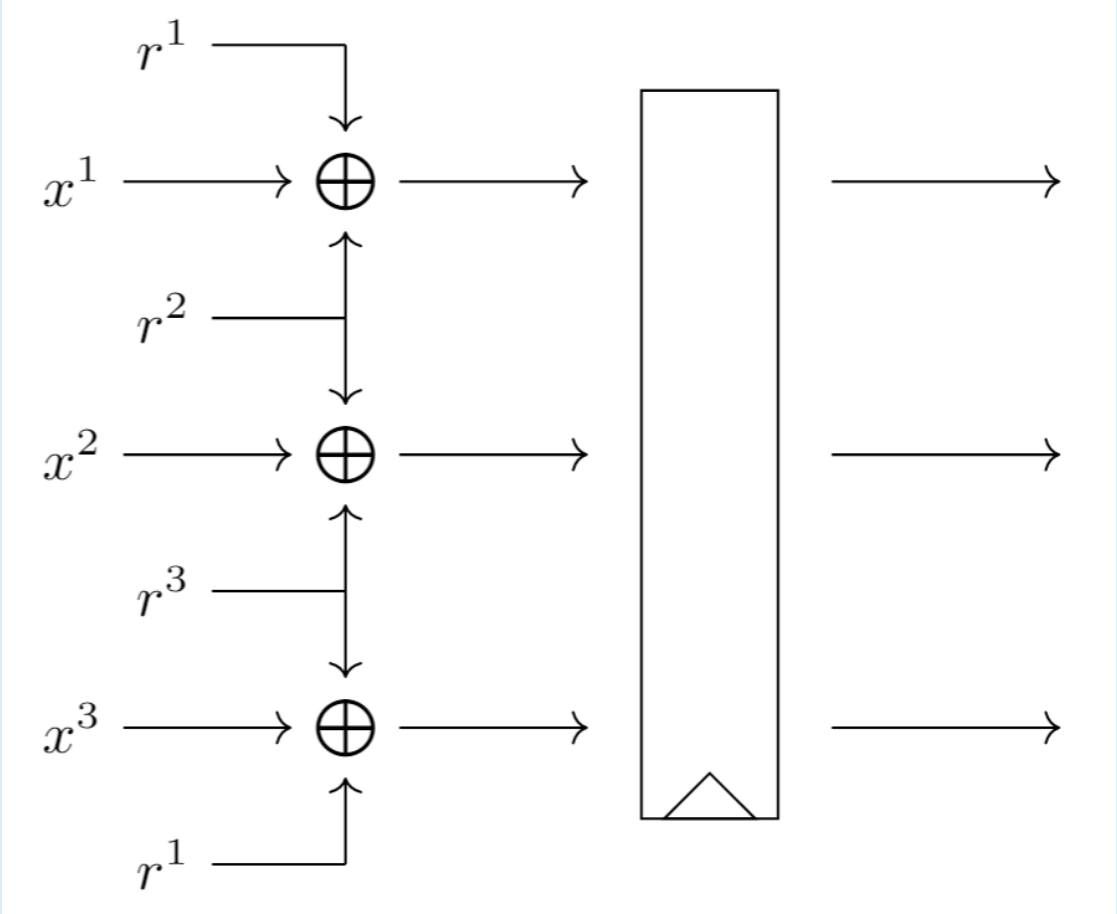


Figure 4: A round of PRESENT.

Resilient uniformity



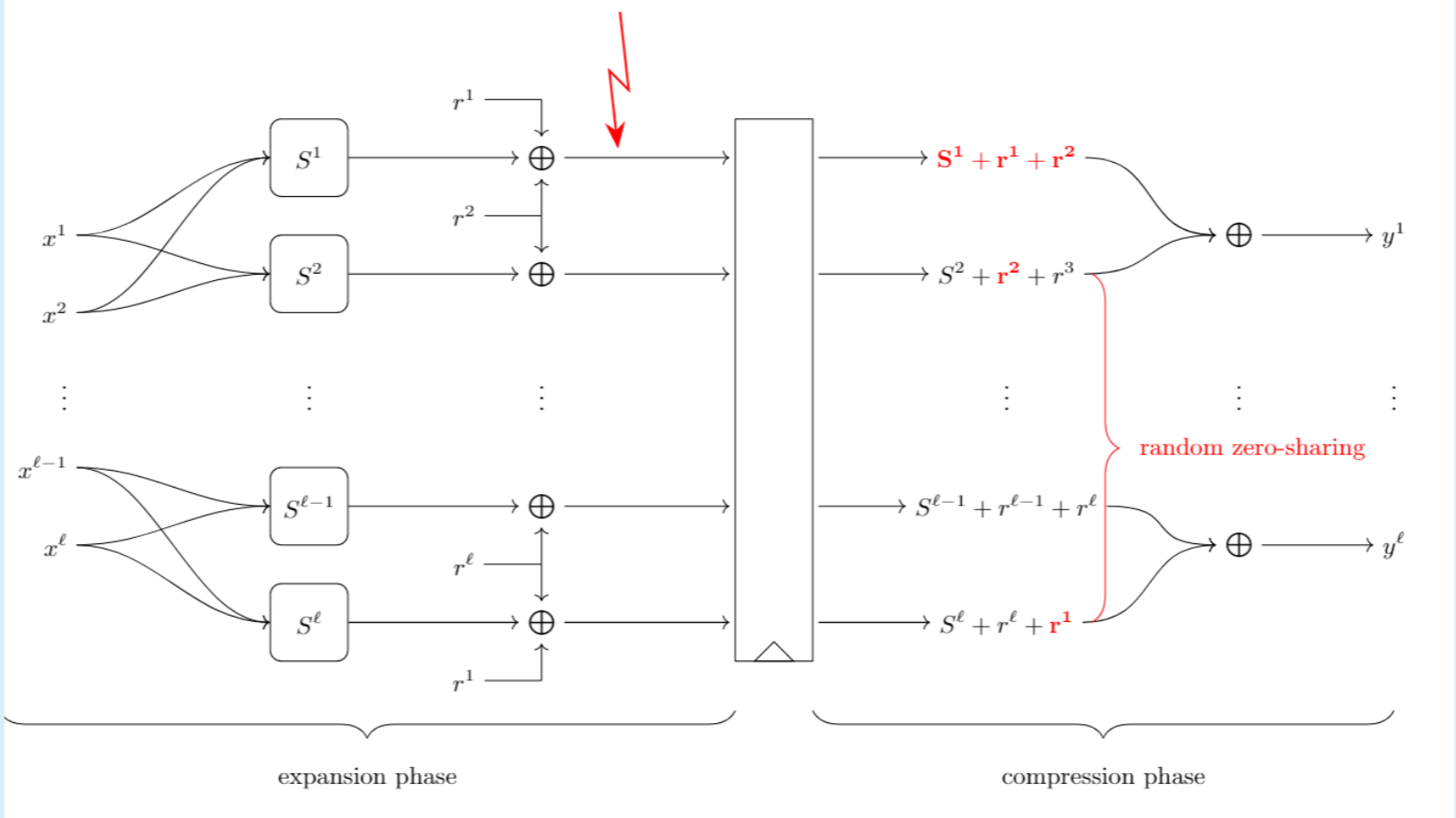
Resilient uniformity

Definition 2 (Δ resilient). *Let $f(x) = f(x^1, ..., x^n)$ be a Boolean function on $\mathbb{F}_2^n$ and Δ be a monotone decreasing set. Then $f(x)$ is called Δ resilient if any of its restrictions obtained by fixing an input set $A \in \Delta$ of inputs coordinates is balanced.*

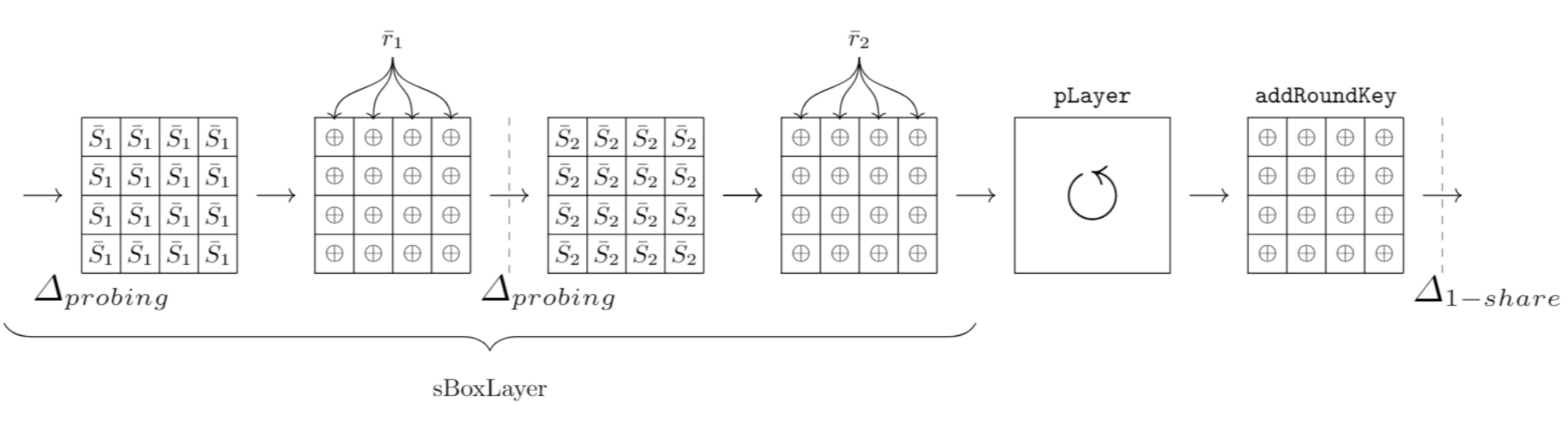
Definition 4 (Δ resilient uniformity). *A function $\bar{F}(\bar{x}) = \bar{y}$ is Δ resilient uniform if for all $I \in \Delta$ there exists a set $J \in \Delta$ such that for all realizations $\bar{x}_I^*, \bar{y}_J^*$ there exists a constant c such that for all secrets x and outputs $\bar{y} \in Sh(F(x))$ with $\bar{y}_J = \bar{y}_J^*$:*

$$\left| \left\{ \bar{x} \in Sh(x) \text{ with } \bar{x}_I = \bar{x}_I^* \,\middle|\, \bar{F}(\bar{x}) = \bar{y} \right\} \right| = c\,.$$

“Consolidating Masking Schemes” [RBNGV15]



Application to PRESENT



Symmetric key design
open problems

- Can we design a TI sharing-friendly cipher?
- What would its diffusion layer be?
- Can we design S-boxes with specifically good properties when shared?
- Can the cipher be designed so that allows for higher-order protection?