Cryptanalysis of Masked Ciphers

A not so Random Idea

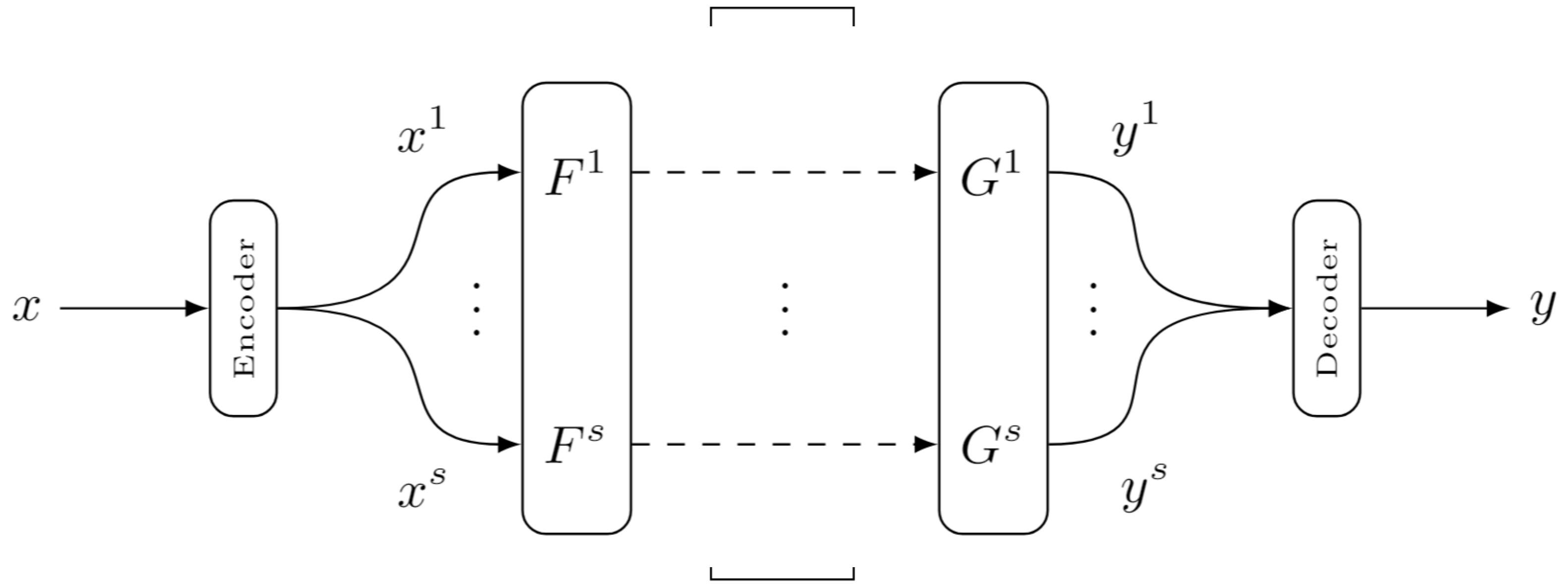
Tim Beyne, **Siemen Dhooghe**, Zhenda Zhang
imec-COSIC, ESAT, KU Leuven, Belgium

The Work in a Nutshell

- Side-channel analysis, masking, and probing security
- A security analysis based on cryptanalysis
  - Bounded-query security
  - Higher-order threshold implementations
  - The analysis includes the randomness generation
- Importance of cryptanalytic properties
  - Linear activity patterns caused by diffusion
  - Nonlinearity of the masked S-box

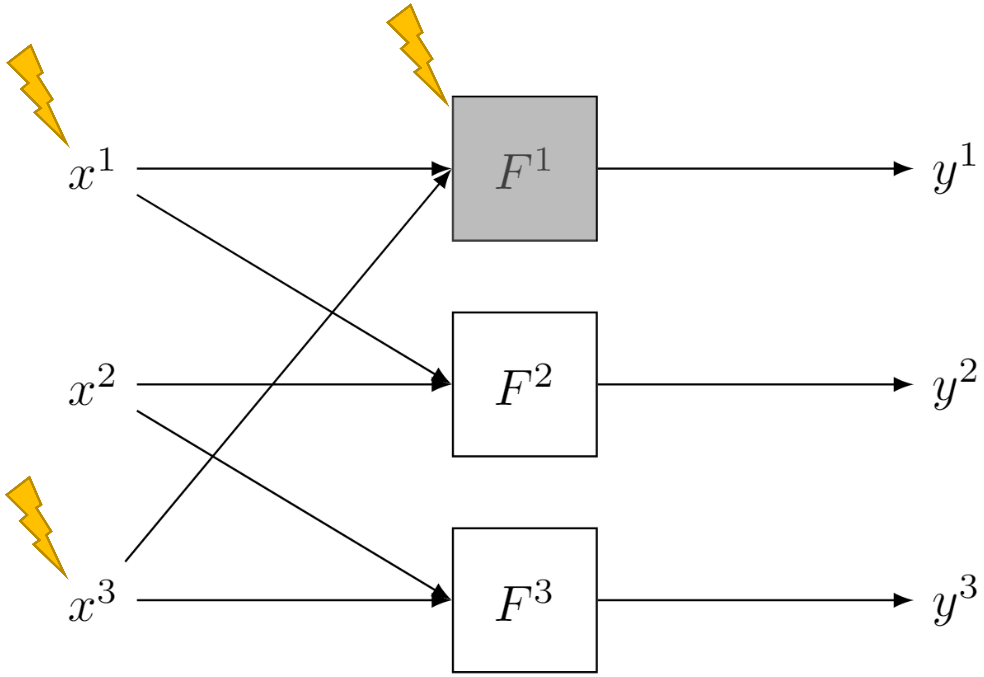
Threshold Implementations

- Correctness
- Non-completeness
- Uniformity



Glitch-Extended Probing

- Using a probe an adversary views the inputs of a function
- The number of probes is called the order of security



Bounded-Query Security

- Moving from perfect security to bounded-query security

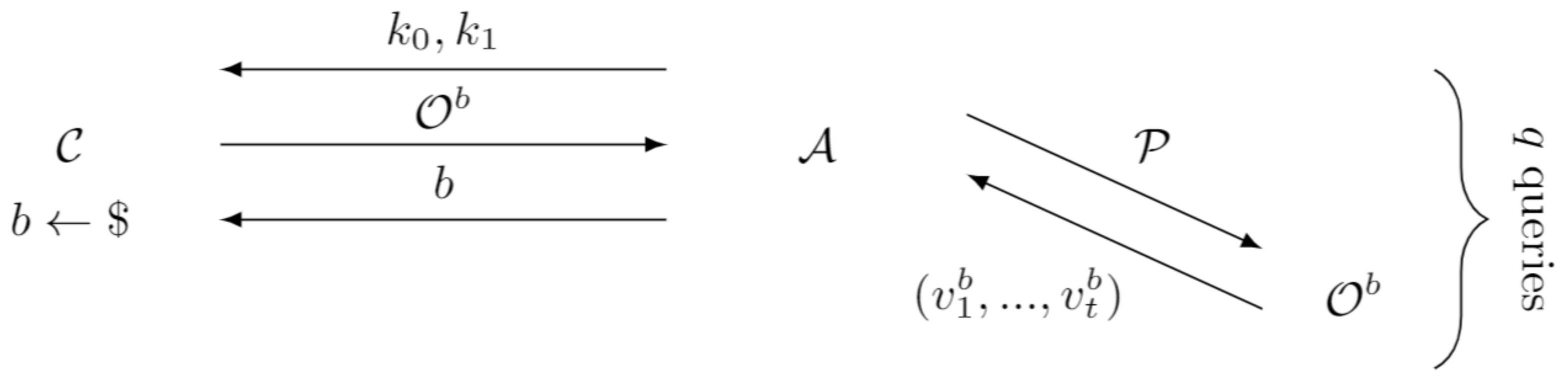
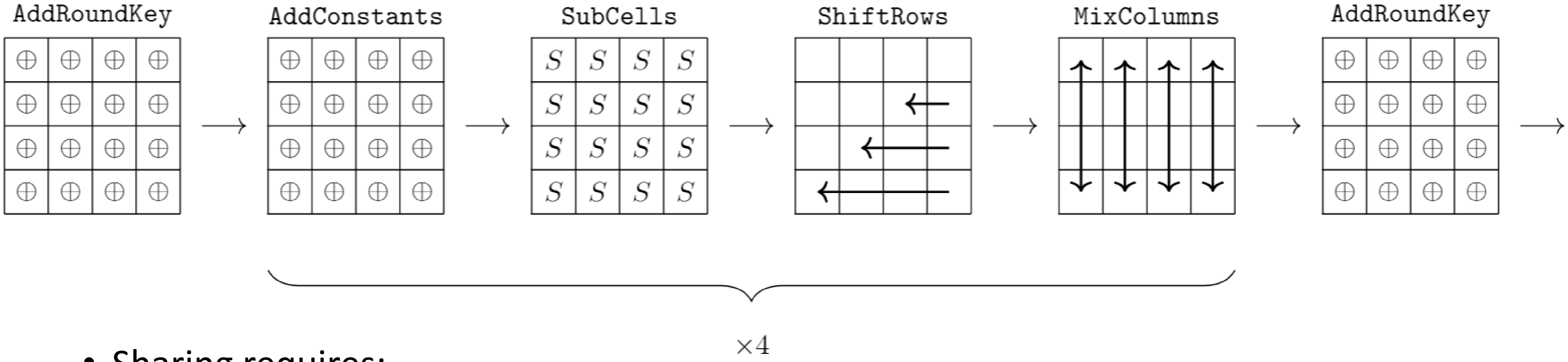


Figure 2. The privacy model for t-threshold-probing security for a challenger $\mathcal{C}$, an adversary $\mathcal{A}$, a left-right oracle $\mathcal{O}^b$, two inputs k_0, k_1, a set of probes $\mathcal{P}$, and a set of probed wire values $(v_1^b, ..., v_t^b)$ of the circuit $C(k_b)$.

Bounding the Advantage (Simplified)

- The advantage is bounded in terms of the Shannon entropy of the probed values
- The entropy of probed values can be bounded in terms of the nontrivial Fourier coefficients of its distribution
- The bounding of these Fourier coefficients is done using standard linear cryptanalysis

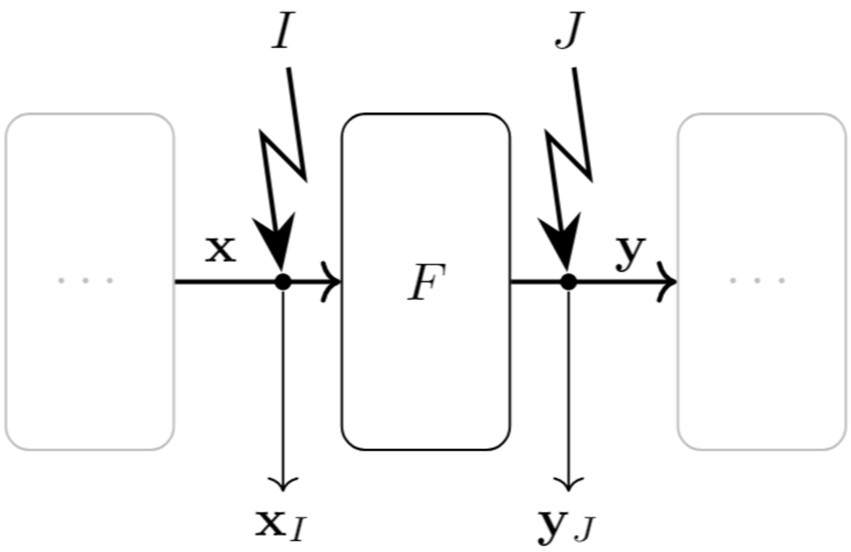
Case Study: Second-Order Masked LED



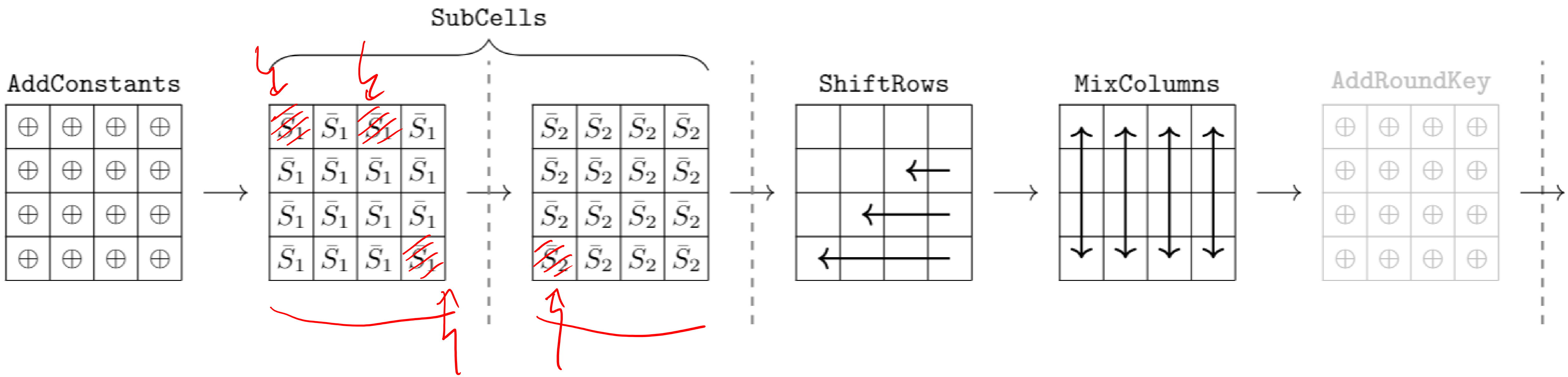
- Sharing requires:
  - 664 bits of randomness
  - 7 shares per state bit
  - 3 shares per key bit

Security Analysis in Three Steps

- S-box level: probing security
- Nearby rounds: zero-correlation
- Distant rounds: small absolute correlation

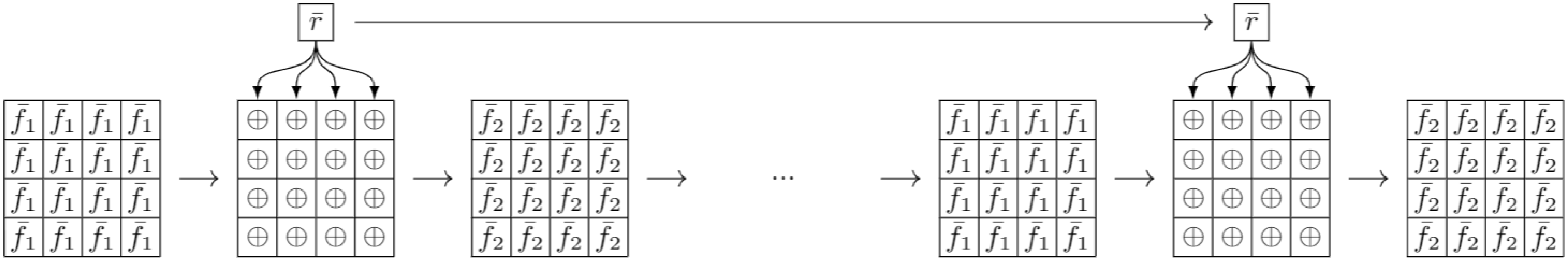


S-Box Level: Threshold Implementations



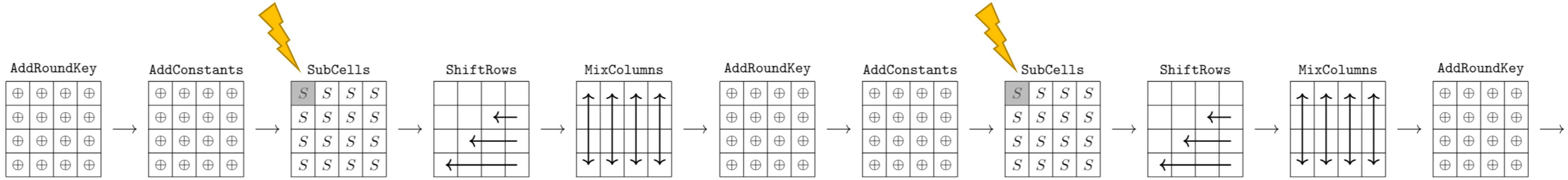
- $\bar{S}_1, \bar{S}_2$ are
  - Correct
  - Second-order non-complete
  - Uniform

S-Box Level: Static Randomness



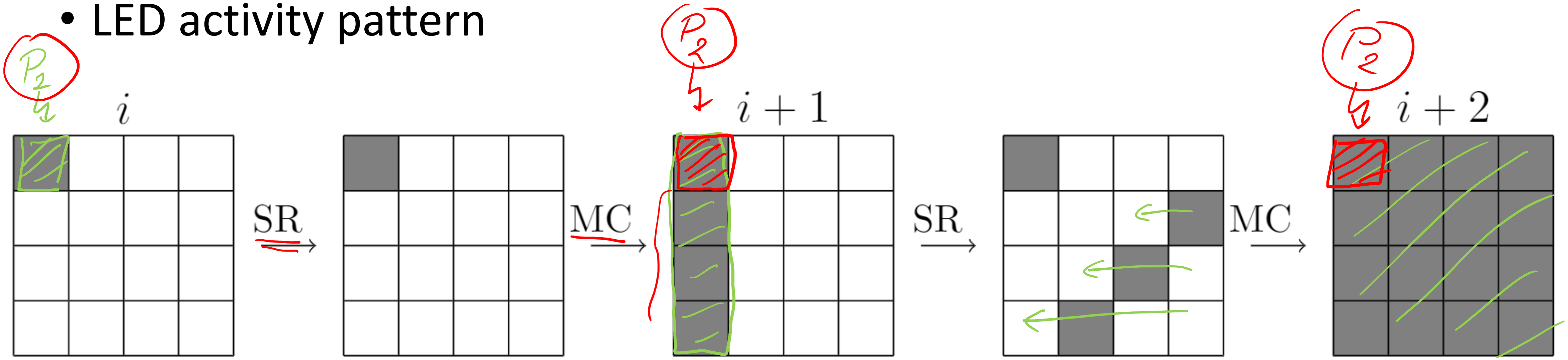
- Randomness $\bar{r}$ is added in the shared S-box
- This randomness is re-used every round, every cell

Nearby Rounds



Nearby Rounds

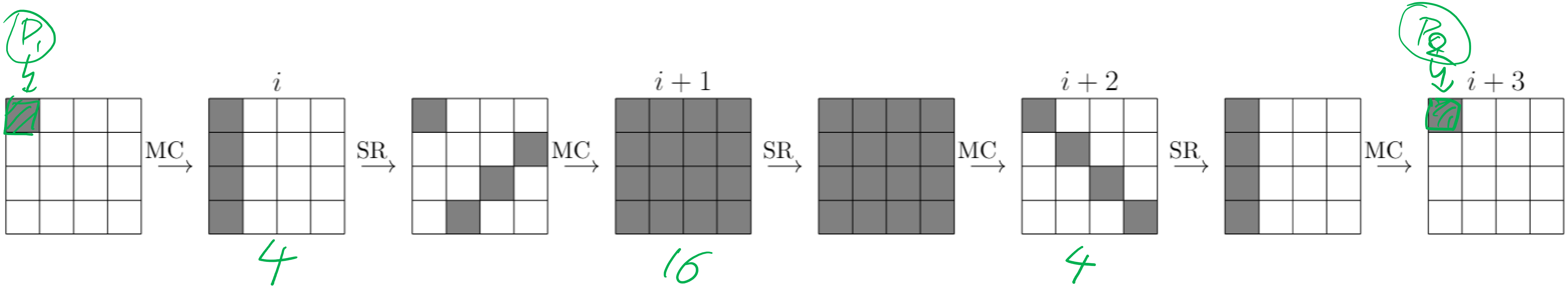
- LED activity pattern



- Zero-correlation linear approximation(s):
  - Any pair of measurements from probes which are at most three rounds apart is uniformly distributed

Distant Rounds (Wide-Trail Strategy)

- LED activity pattern



- Bounds on (absolute) correlation of linear approximations/trails:
  - Probes at least four rounds apart activate at least 24 shared S-boxes
  - Each shared S-box has maximum absolute correlation 2^{-3}
  - The distribution of any pair of measurements from probes which are at least four rounds apart is close to uniform

Security of Masked LED

Security Claim 1. *For the masked LED described in this section, the following bound on the advantage of the adversary (assuming piling-up) in the probing model is claimed:*

$$\mathrm{Adv}_{\textsf{2-thr}}(\mathcal{A}) \leq \sqrt{\frac{q}{2^{120}}}\,.$$

To Conclude

- Linear cryptanalysis can be used to analyze the probing-security of masked primitives
- Fresh randomness is not needed for second-order security
- Some symmetric primitives are easier to secure than others
  - AES S-box has no known uniform sharing
  - PRESENT has slow diffusion

- Future work:
  - Find cryptanalytically good sharings
  - Application to other security models
  - Investigate the effect of RNGs in the design