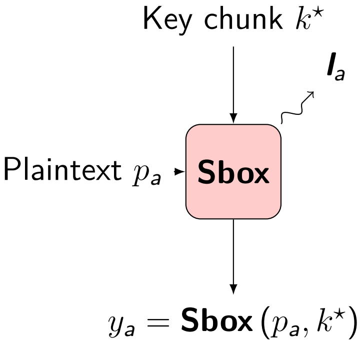
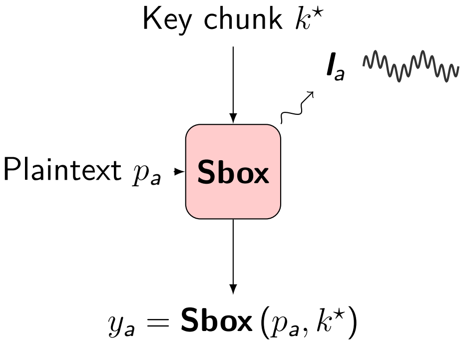
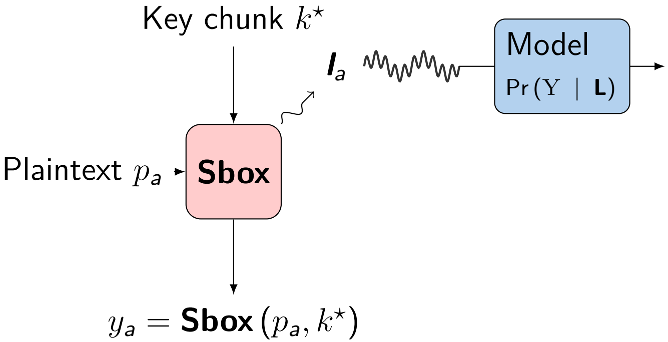
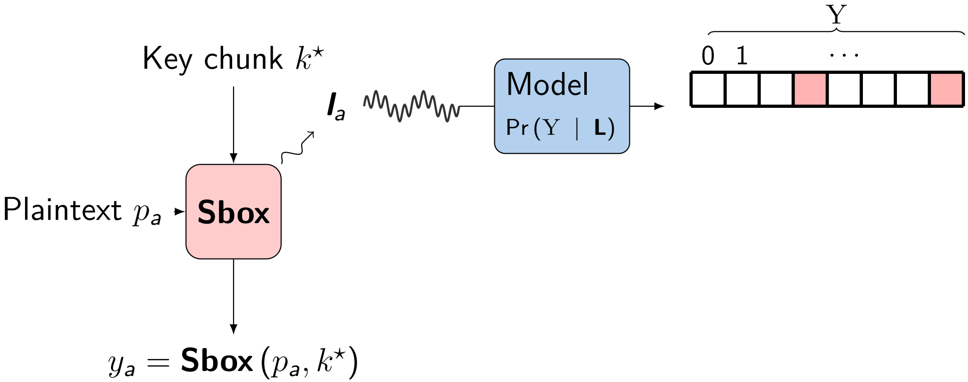
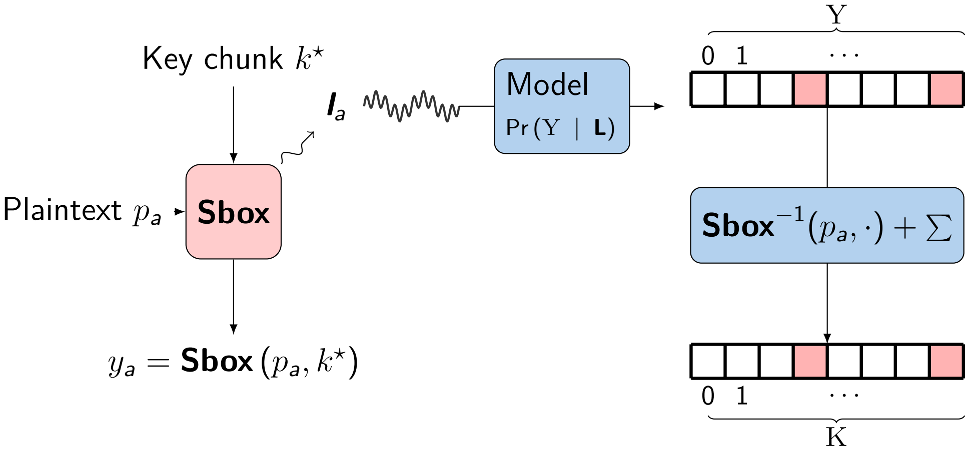

Key chunk $k^\star$
$\boldsymbol{l}_a$
Plaintext p_a
Sbox
$y_a = \textbf{Sbox}\,(p_a, k^\star)$

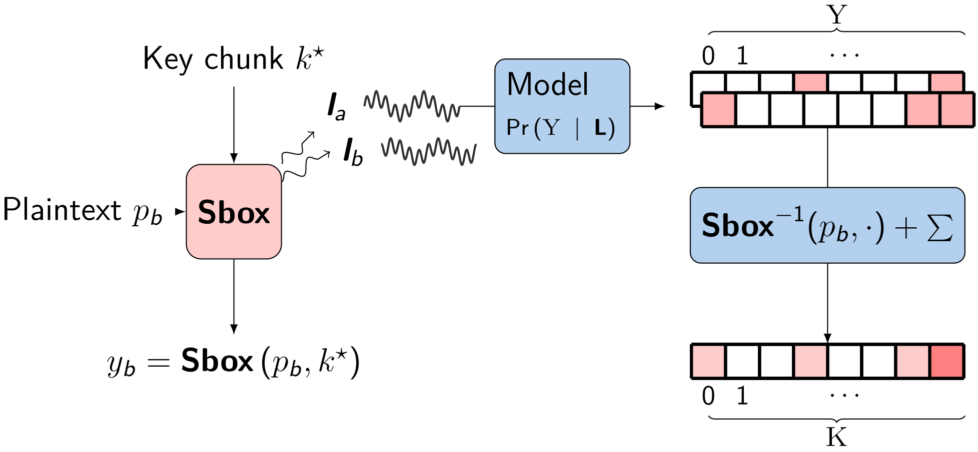

Key chunk $k^\star$
$\boldsymbol{l}_a$
Plaintext p_a
Sbox
$y_a = \textbf{Sbox}\,(p_a, k^\star)$


Key chunk $k^\star$
$\boldsymbol{l}_a$
Model
$\Pr(\mathrm{Y} \mid \mathbf{L})$
Plaintext p_a
Sbox
$y_a = \mathbf{Sbox}(p_a, k^\star)$

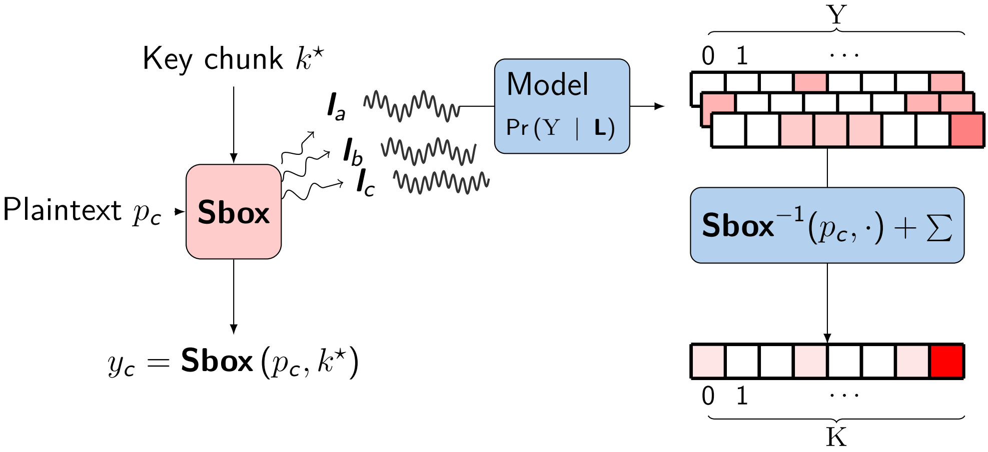


Key chunk $k^\star$
$\boldsymbol{l}_a$
Model
$\Pr(\mathrm{Y} \mid \mathbf{L})$
Y
0 1 ...
Plaintext p_a
Sbox
$y_a = \mathbf{Sbox}(p_a, k^\star)$

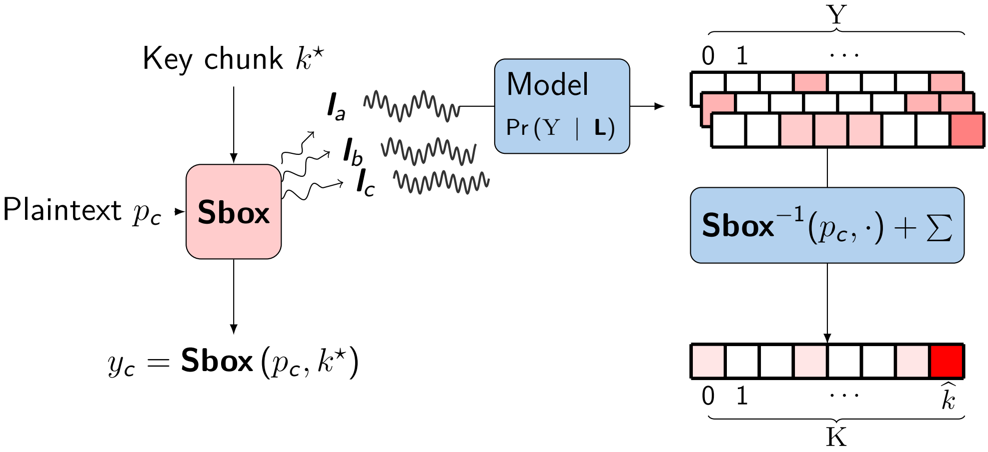

Key chunk $k^\star$
$\boldsymbol{l}_a$
Model
$\Pr(\mathrm{Y} \mid \mathbf{L})$
Y
0 1 $\cdots$
Plaintext p_a
Sbox
$\mathbf{Sbox}^{-1}(p_a, \cdot) + \sum$
$y_a = \mathbf{Sbox}(p_a, k^\star)$
0 1 $\cdots$
K



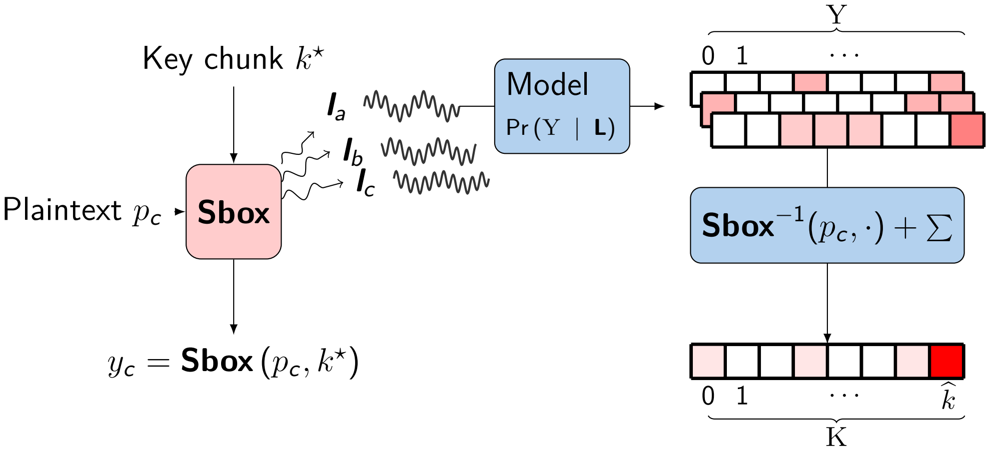
Key chunk $k^\star$
Plaintext p_b
Sbox
$y_b = \textbf{Sbox}\,(p_b, k^\star)$
$\boldsymbol{l}_a$
$\boldsymbol{l}_b$
Model
$\Pr(\mathrm{Y} \mid \mathbf{L})$
Y
0 1 ...
$\textbf{Sbox}^{-1}(p_b, \cdot) + \sum$
0 1 ...
K



Key chunk $k^\star$
Plaintext p_c
Sbox
$y_c = \textbf{Sbox}(p_c, k^\star)$
$\boldsymbol{l}_a$
$\boldsymbol{l}_b$
$\boldsymbol{l}_c$
Model
$\Pr(\mathrm{Y} \mid \mathbf{L})$
Y
0 1 $\cdots$
$\textbf{Sbox}^{-1}(p_c, \cdot) + \sum$
0 1 $\cdots$
K

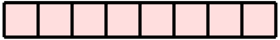


Key chunk $k^\star$
Plaintext p_c
Sbox
$y_c = \textbf{Sbox}(p_c, k^\star)$
$\boldsymbol{l}_a$
$\boldsymbol{l}_b$
$\boldsymbol{l}_c$
Model
$\Pr(\mathrm{Y} \mid \mathbf{L})$
Y
0 1 ...
$\textbf{Sbox}^{-1}(p_c, \cdot) + \sum$
0 1 ... $\hat{k}$
K

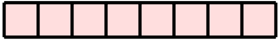


Successful attack iff $\hat{k} = k^\star$

If, the adversary gets:



If, the adversary gets:

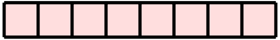


Sensitive computation unpredictable

SCA not more powerful than cryptanalysis

Device fully secure

If, the adversary gets:



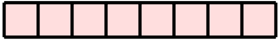
If, the adversary gets:

Sensitive computation unpredictable

SCA not more powerful than cryptanalysis

Device fully secure

If, the adversary gets:



Sensitive computation unpredictable

SCA not more powerful than cryptanalysis

Device fully secure

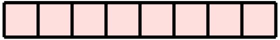
If, the adversary gets:

Exact prediction of the sensitive computation

Success rate of 100% with *one* trace

Device not secure at all

If, the adversary gets:

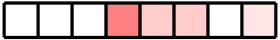


Sensitive computation unpredictable
SCA not more powerful than cryptanalysis
Device fully secure

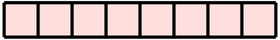
If, the adversary gets:

Exact prediction of the sensitive computation
Success rate of 100% with *one* trace
Device not secure at all

In general, the adversary gets:



If, the adversary gets:



Sensitive computation unpredictable

SCA not more powerful than cryptanalysis

Device fully secure

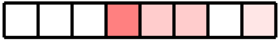
If, the adversary gets:

Exact prediction of the sensitive computation

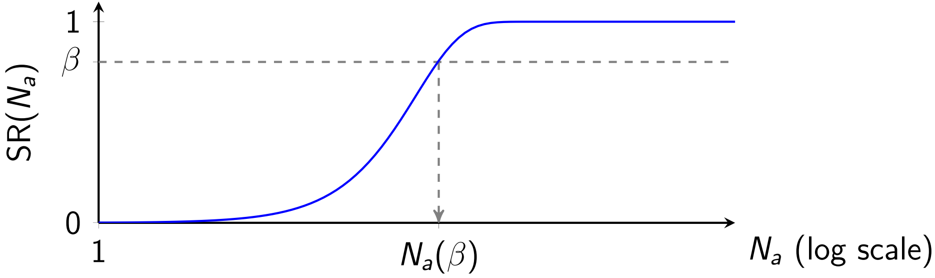
Success rate of 100% with *one* trace

Device not secure at all

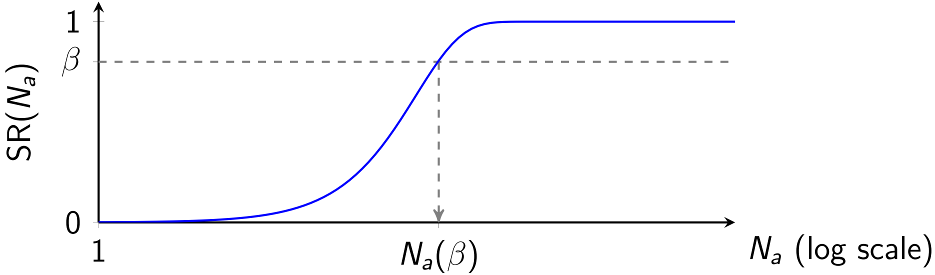
In general, the adversary gets:



How does this translate into SCA security metrics ?

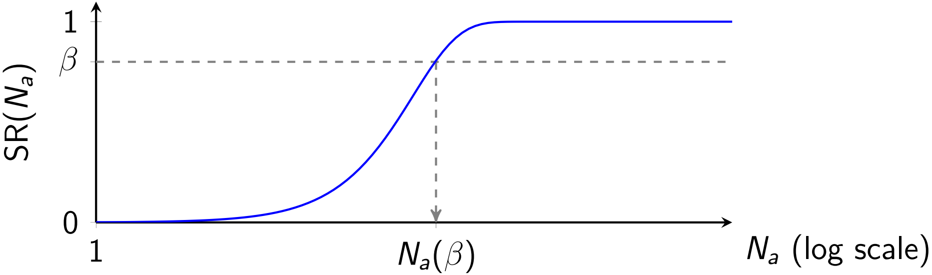


SR: probability to succeed the attack within N_a queries to the target



SR: probability to succeed the attack within N_a queries to the target

Secured device with prob. $\geq 1 - \beta$, $\implies$ refresh secret every $N_a(\beta)$ use ✓



SR: probability to succeed the attack within N_a queries to the target

Secured device with prob. $\geq 1-\beta$, $\implies$ refresh secret every $N_a(\beta)$ use ✓

Naive est. of $N_a(\beta)$ is expensive: complexity depends on $N_a(\beta)$ itself ✗

Can we find surrogate metrics characterizing $N_a(\beta)$?

[1] Mangard, Oswald, and Popp, *Power analysis attacks - revealing the secrets of smart cards*

[2] Chérisey et al., "Best Information is Most Successful: Mutual Information and Success Rate in Side-Channel Analysis"

Can we find surrogate metrics characterizing $N_a(\beta)$?

CPA [1]

Using correlation coeff.

$$N_a(\beta) \approx \frac{f(\beta)}{\rho^2}$$

Easy to estimate ρ ✓
Only for univariate, linear ✗

---

[1] Mangard, Oswald, and Popp, *Power analysis attacks - revealing the secrets of smart cards*

[2] Chérisey et al., "Best Information is Most Successful: Mutual Information and Success Rate in Side-Channel Analysis"

Can we find surrogate metrics characterizing $N_a(\beta)$?

CPA [1]

Using correlation coeff.

$$N_a(\beta) \approx \frac{f(\beta)}{\rho^2}$$

Easy to estimate ρ ✓

Only for univariate, linear ✗

General case [2]

Using the Mutual Information (MI),

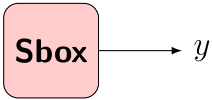
$$N_a(\beta) \geq \frac{f(\beta)}{\mathrm{MI}\,(\mathrm{Y}; \mathbf{L})}$$

MI generalizes ρ ✓

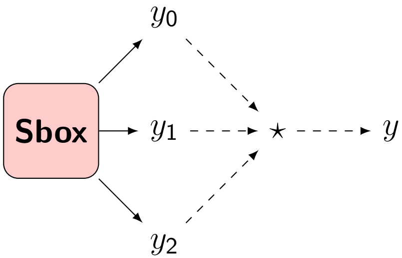
MI hard to estimate ✗

[1] Mangard, Oswald, and Popp, *Power analysis attacks - revealing the secrets of smart cards*

[2] Chérisey et al., "Best Information is Most Successful: Mutual Information and Success Rate in Side-Channel Analysis"

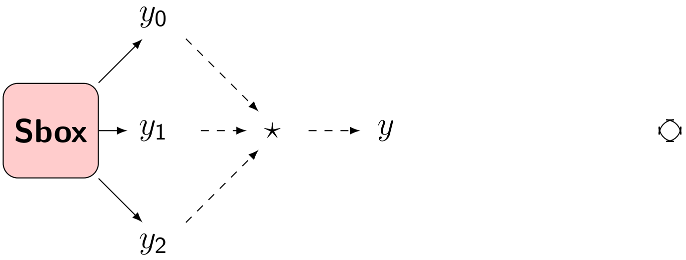


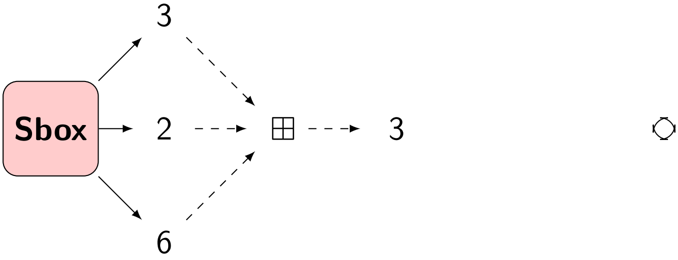
(a) Unprotected

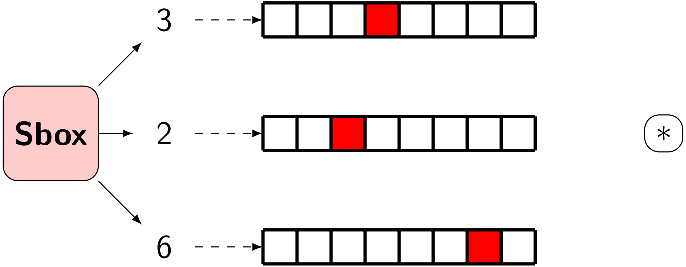


(b) Masking with $d + 1 = 3$ shares

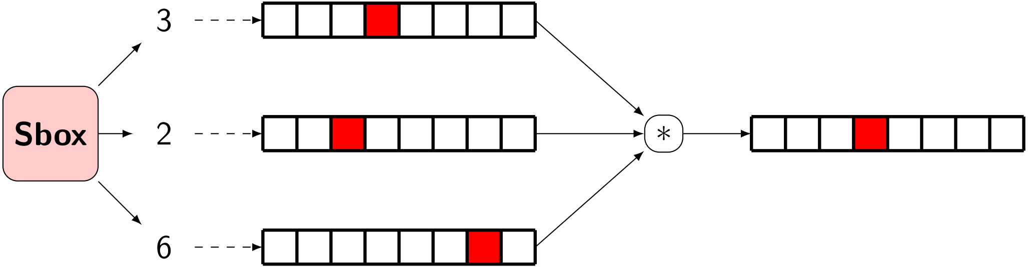
Each share y_i drawn uniformly, such that $y = y_0 \star \ldots \star y_d$

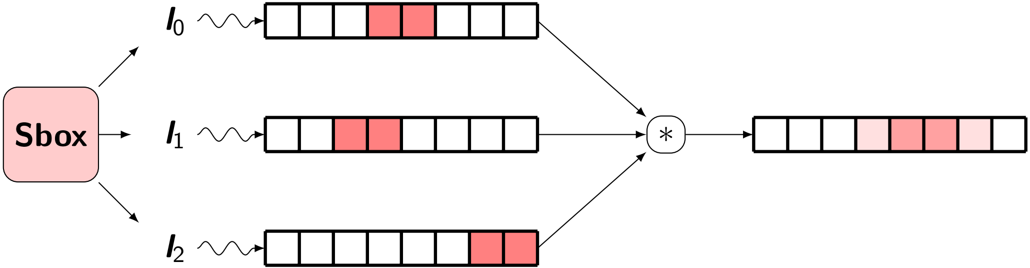

Sbox
y_0
y_1
y_2
$\star$
y

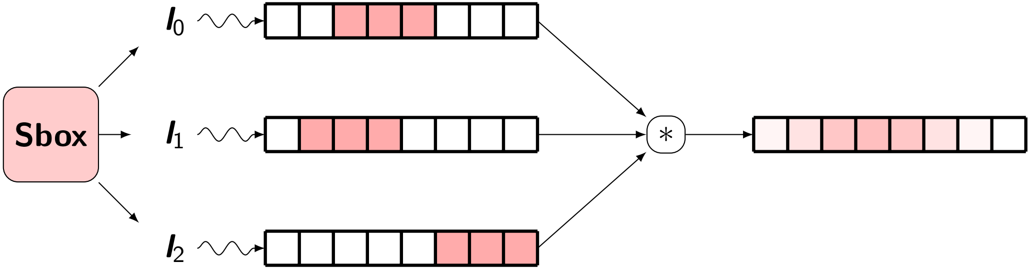

3
Sbox
2
3
6



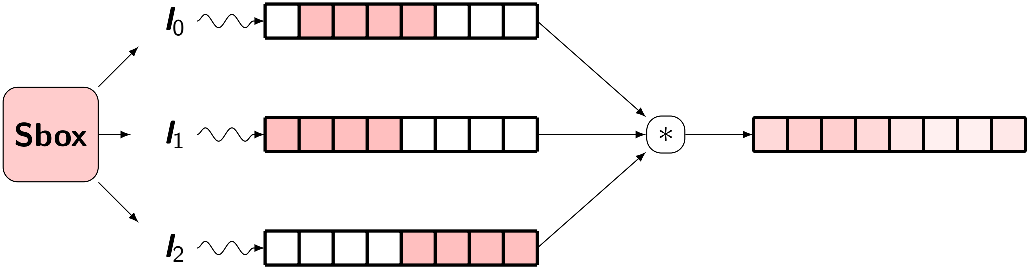
Sbox
3
2
6
*


Sbox
3
2
6
*


Sbox
l_0
l_1
l_2
$*$



Sbox
l_0
l_1
l_2
$*$



Masking amplifies the noise . . . exponentially with #shares

MI *very* hard to compute naively with masking

- Curse of dimensionality increases with #shares
- Higher #shares $\implies$ lower MI $\implies$ harder est.