M&M: Masks and Macs against Physical Attacks

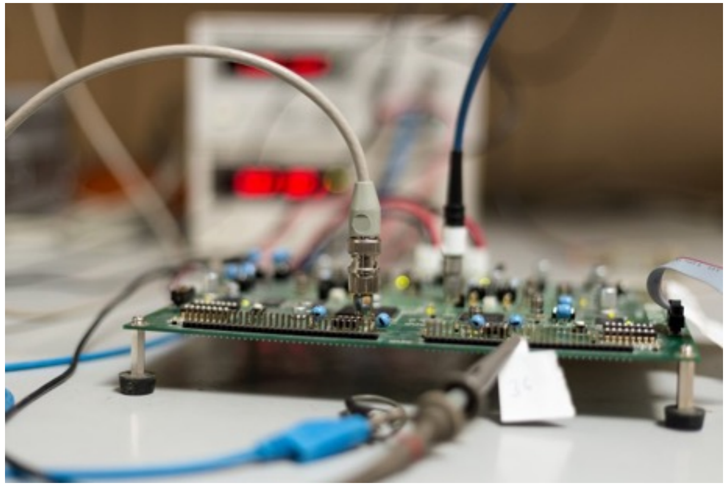
CHES 2019

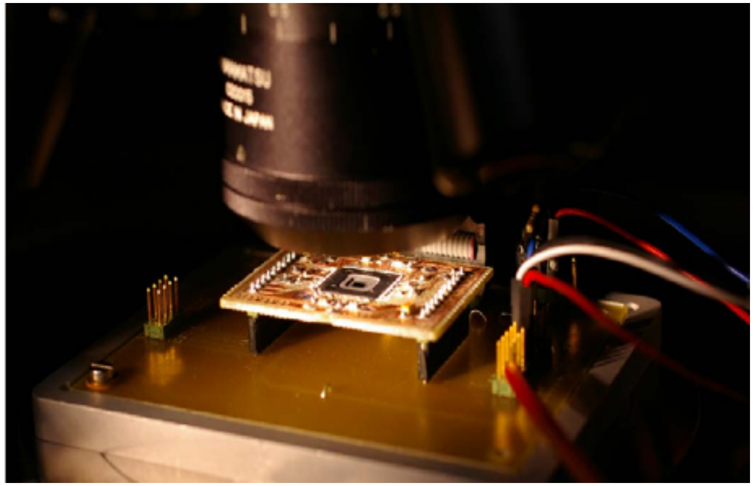
Lauren De Meyer, Victor Arribas
Svetla Nikova, Ventzislav Nikov, Vincent Rijmen

BACK TO THE 90'S

- Differential Power Analysis (DPA) – Paul Kocher et al. 1999 [KJJ99]

- Differential Fault Analysis (DFA) – Biham and Shamir 1997 [BS97]



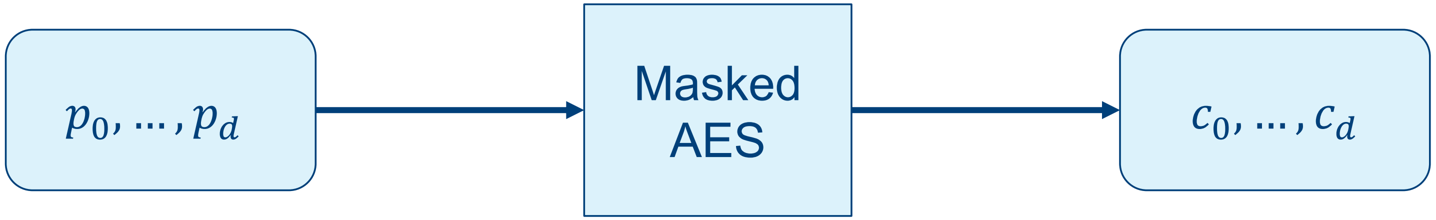


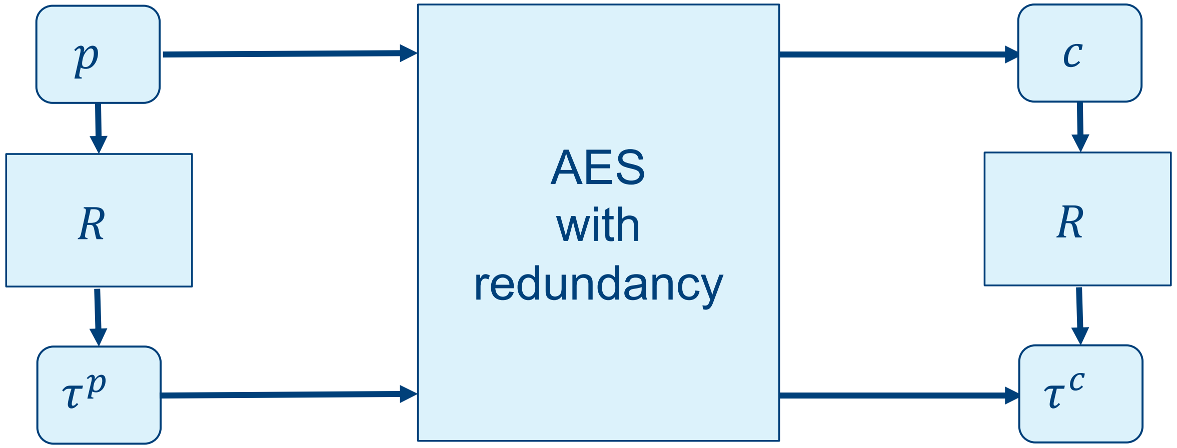
[KJJ99] Paul C. Kocher, Joshua Jaffe, Benjamin Jun: Differential Power Analysis. CRYPTO 1999: 388-397
[BS97] Eli Biham, Adi Shamir: Differential Fault Analysis of Secret Key Cryptosystems. CRYPTO 1997: 513-525

Countermeasures

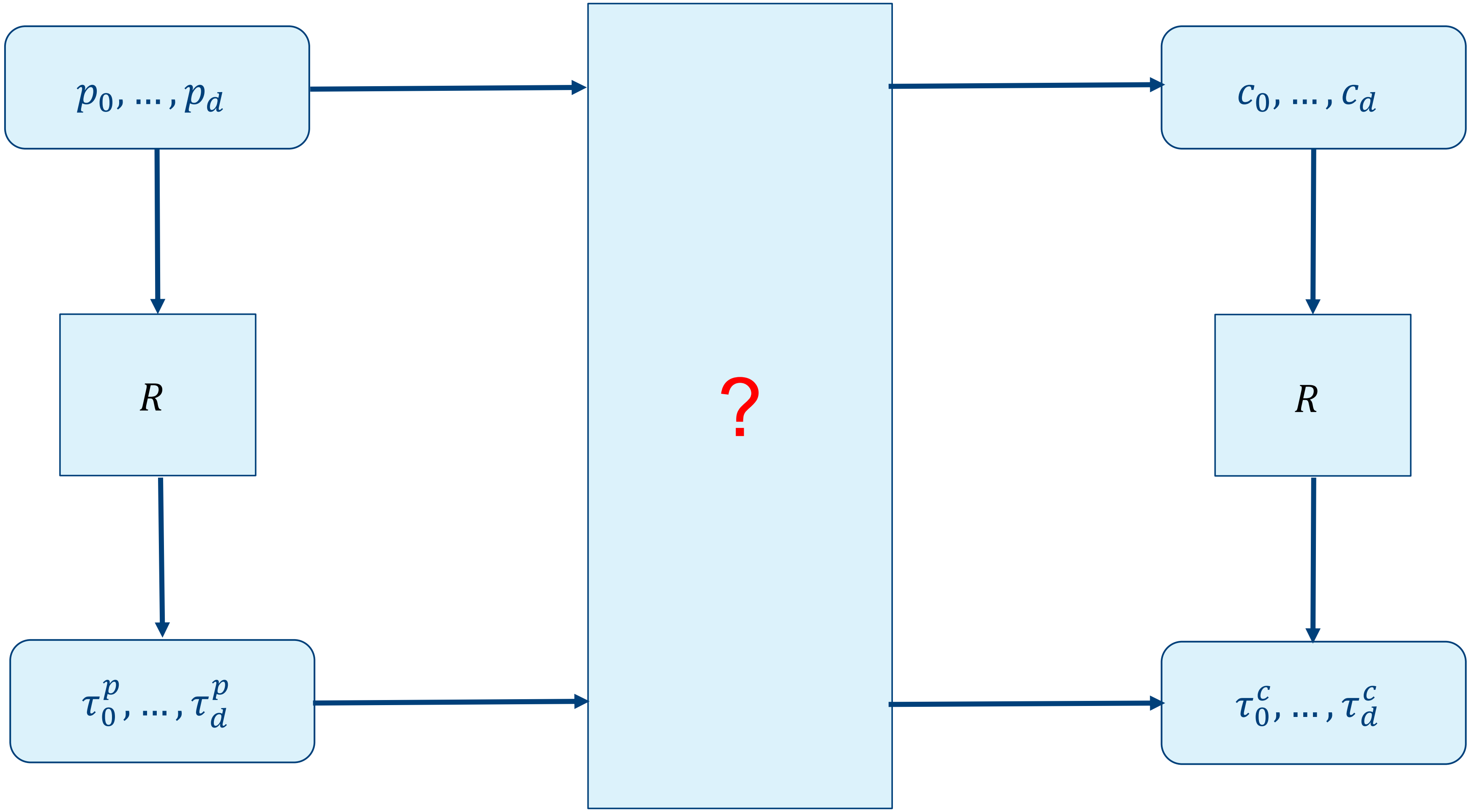
- Against side-channel attacks:
  - Hiding
  - **Masking**

- Against fault attacks:
  - Repetition, redundancy (EDC, **tags**), …
  - Detection, correction or **infection**





Combined Countermeasures

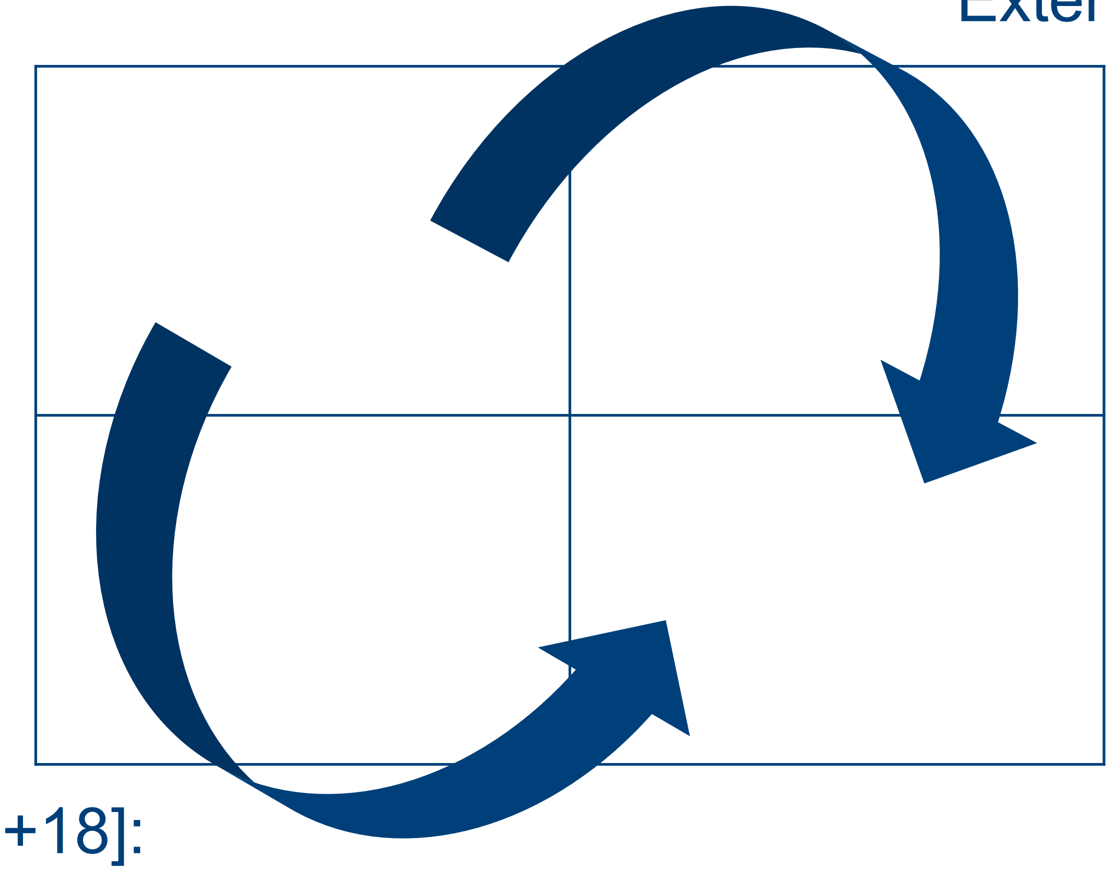


THRESHOLD CRYPTO

	MPC	Embedded Systems	
Passive	Shamir’s Secret Sharing [Sha79]	Masking ([ISW03],[NRS11], …)	SCA
Active	SPDZ [DPS+12], …	….	SCA+FA

[Sha79] Adi Shamir: How to Share a Secret. Commun. ACM 22(11): 612-613 (1979)
[DPS+12] Ivan Damgård, Valerio Pastro, Nigel P. Smart, Sarah Zakarias: Multiparty Computation from Somewhat Homomorphic Encryption. CRYPTO 2012: 643-662
[NRS11] Svetla Nikova, Vincent Rijmen, Martin Schläffer: Secure Hardware Implementation of Nonlinear Functions in the Presence of Glitches. J. Cryptology 24(2): 292-321 (2011)
[ISW03] Yuval Ishai, Amit Sahai, David A. Wagner: Private Circuits: Securing Hardware against Probing Attacks. CRYPTO 2003: 463-481

TWO ROUTES



Extension of masking schemes:

- ParTI [SMG16]
- [SFE+18]
- New: M&M

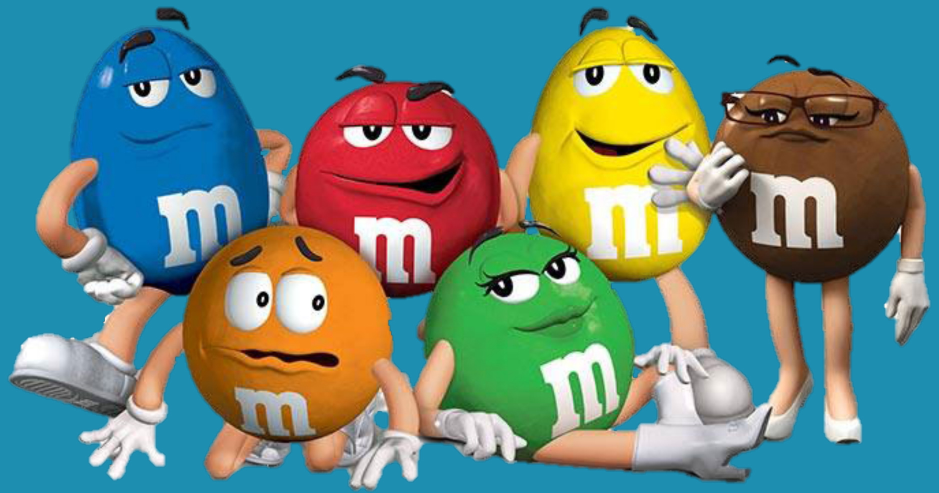
CAPA [RDB+18]:

Based on active MPC protocol SPDZ

[RDB+18] Oscar Reparaz, Lauren De Meyer, Begül Bilgin, Victor Arribas, Svetla Nikova, Ventzislav Nikov, Nigel P. Smart: CAPA: The Spirit of Beaver Against Physical Attacks. CRYPTO (1) 2018: 121-151
[SMG16] Tobias Schneider, Amir Moradi, Tim Güneysu: ParTI - Towards Combined Hardware Countermeasures Against Side-Channel and Fault-Injection Attacks. CRYPTO (2) 2016: 302-332
[SFE+18] Okan Seker, Abraham Fernandez-Rubio, Thomas Eisenbarth, Rainer Steinwandt: Extending Glitch-Free Multiparty Protocols to Resist Fault Injection Attacks. IACR Trans. Cryptogr. Hardw. Embed. Syst. 2018(3): 394-430 (2018)

M&M

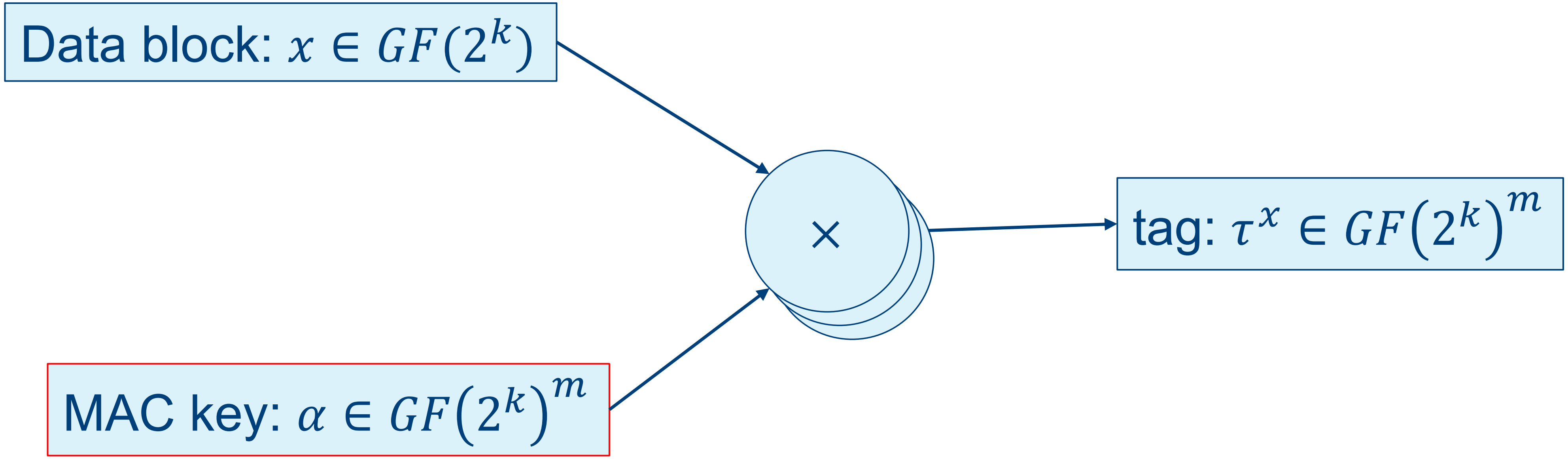
The essentials



ADVERSARY MODEL

- Side-Channel Adversary:
  - d-probing model
- Faulting Adversary:
  - Fault = stochastic additive error
    - Unlimited # bits
  - Fault = exact
    - Limited to d shares
- Combined Adversary

INFORMATION-THEORETIC MAC TAGS



Data block: $x \in GF(2^k)$

$\times$

tag: $\tau^x \in GF\left(2^k\right)^m$

MAC key: $\alpha \in GF\left(2^k\right)^m$

- Used 1x!
- Secret!

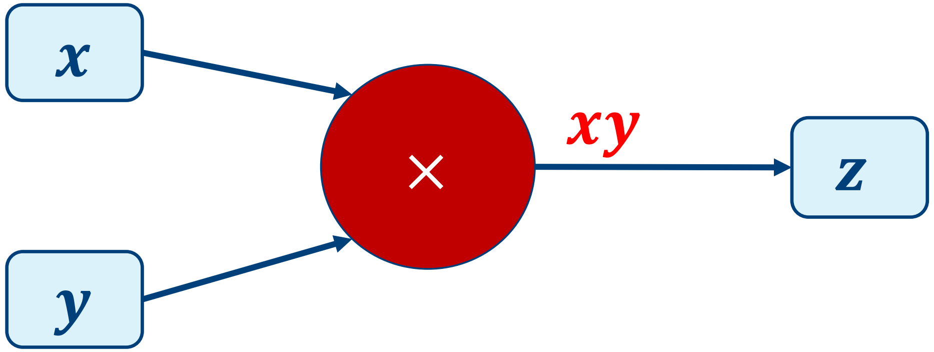
$\Pr$[compromised (x, τ^x) = consistent] $= 2^{-km}$

Information-Theoretic MAC tags Motivation

- Suppose α=fixed (not secret)
  - ~ linear code
  - ~ ParTI [SMG16]
  - Fault model: limited in HW
- Combined Attacks
  - Adversary has “some” side-channel information
  - $x \rightarrow x \oplus \Delta \quad \Rightarrow \quad \tau^x \rightarrow \tau^x \oplus \ ?$
  - make α secret

[SMG16] Tobias Schneider, Amir Moradi, Tim Güneysu: ParTI - Towards Combined Hardware Countermeasures Against Side-Channel and Fault-Injection Attacks. CRYPTO (2) 2016: 302-332

MASKED MULTIPLIER



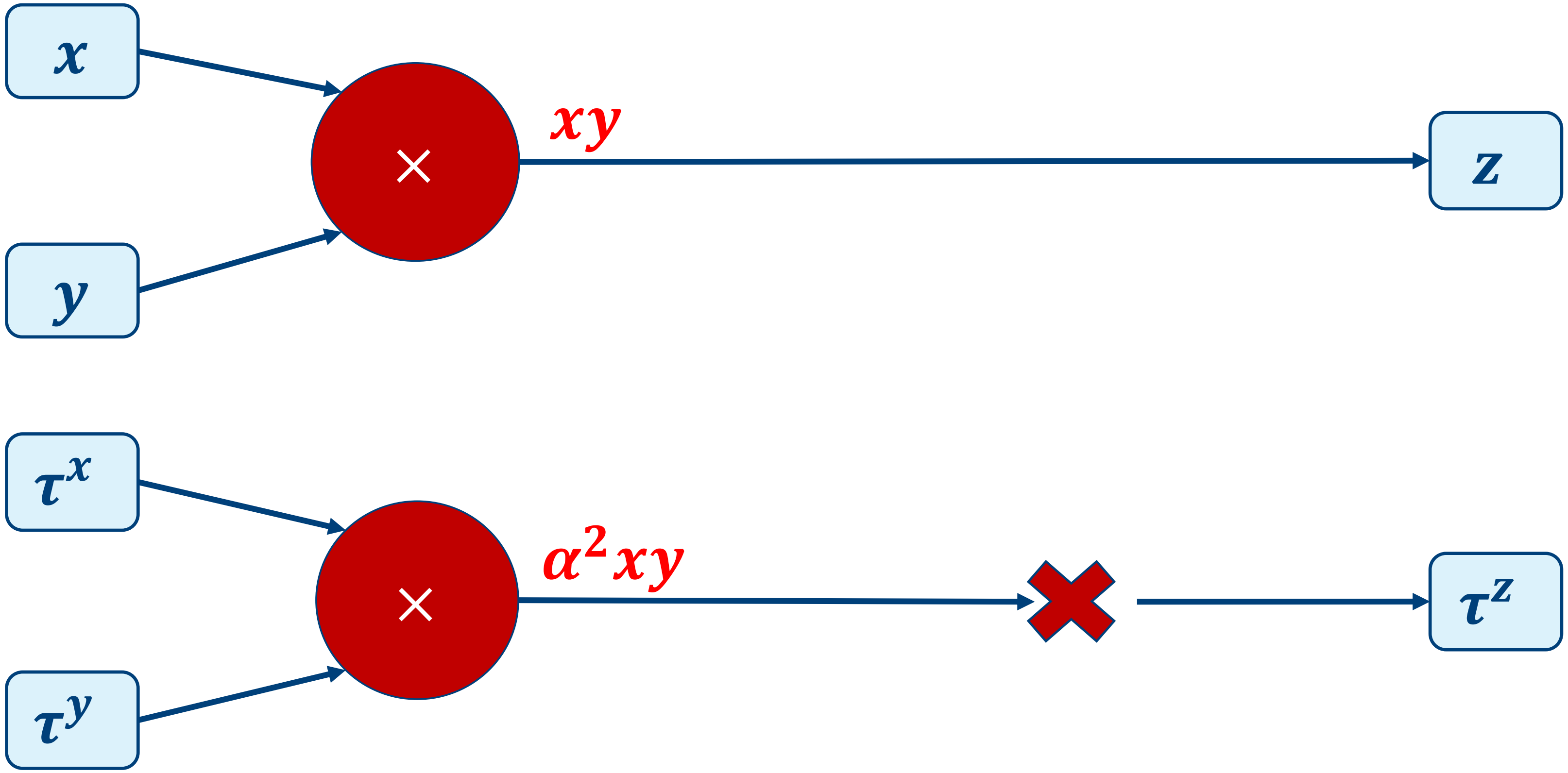
- ISW, TI, DOM, CMS, …
- Example ($d = 1$):

$$z_0 = [x_0 y_0] \oplus [x_0 y_1 \oplus r]$$
$$z_1 = [x_1 y_1] \oplus [x_1 y_0 \oplus r]$$

M&M Multiplication

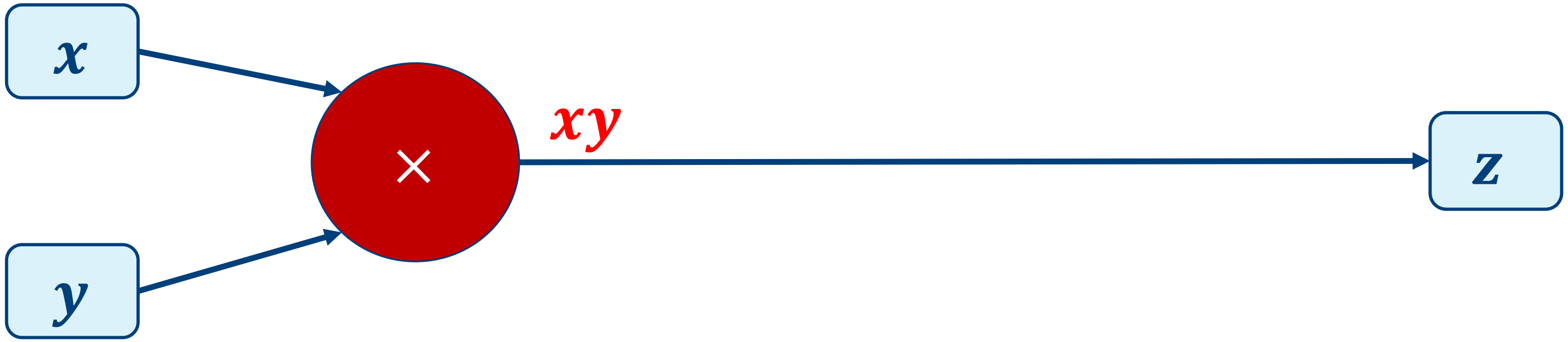
Masks:

MACs:

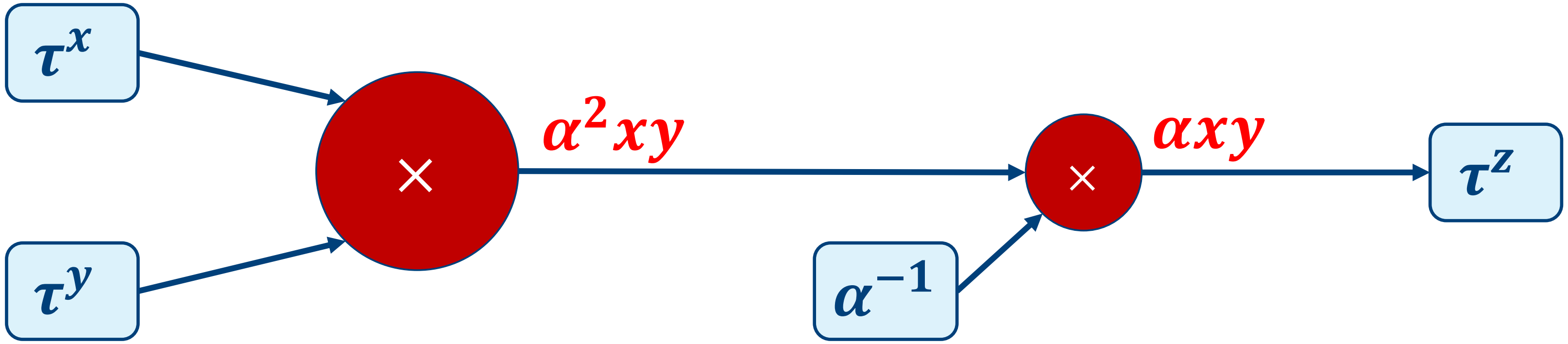


M&M Multiplication

Masks:



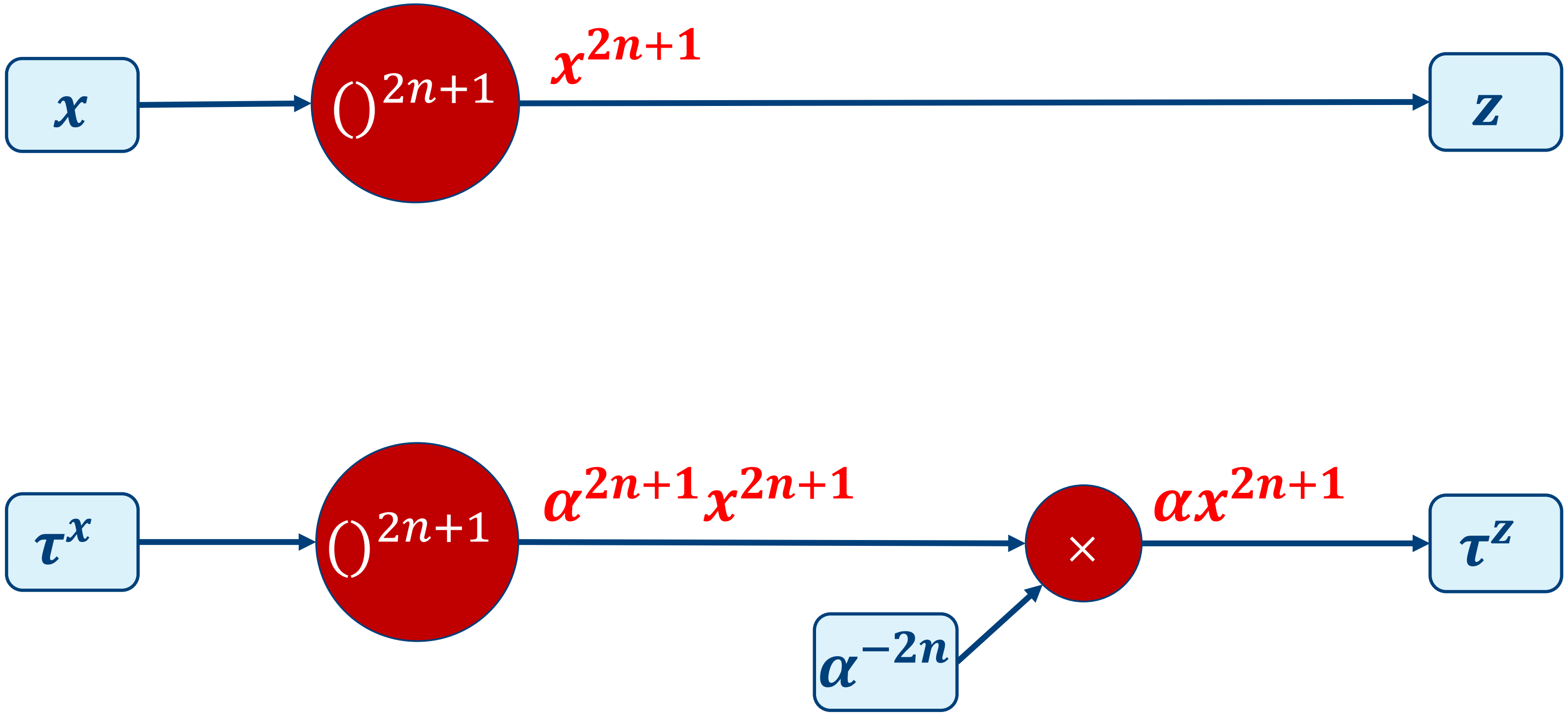
MACs:



Or other operations …

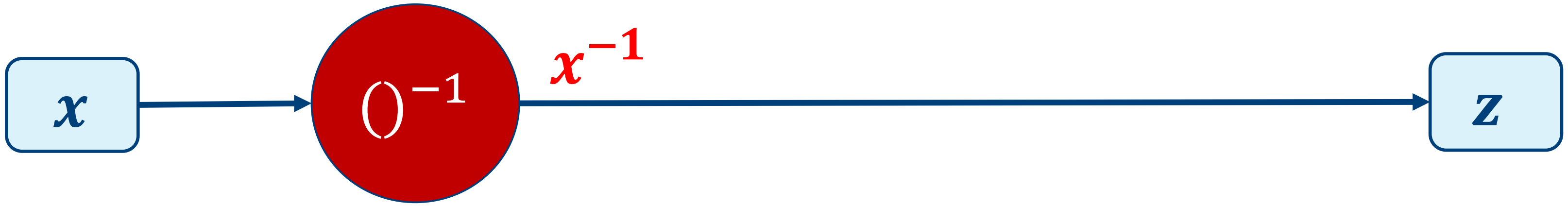
Masks:

MACs:

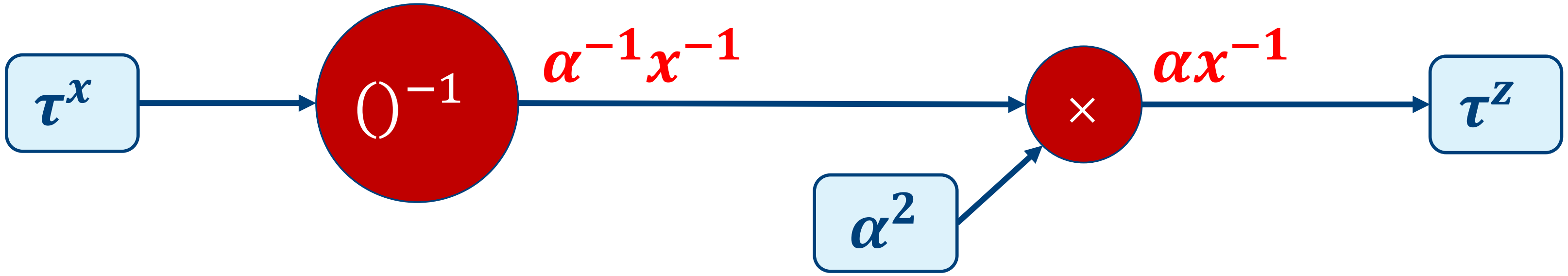


AND EVEN …

Masks:



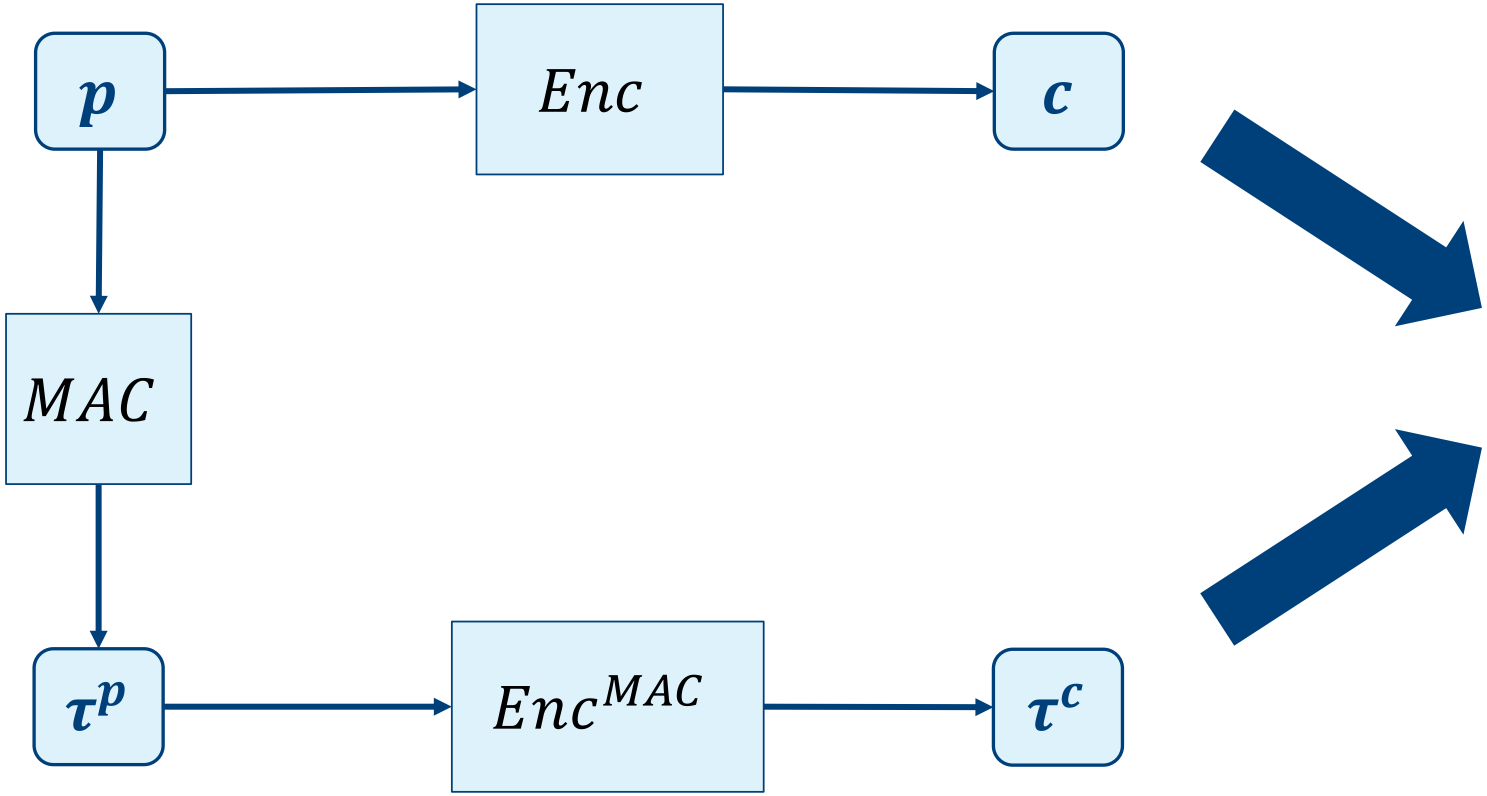
MACs:



Building blocks for ANY algorithm

Many flavors of Masking → many flavors of M&M

Masked Encryption Datapath



p

Enc

c

MAC

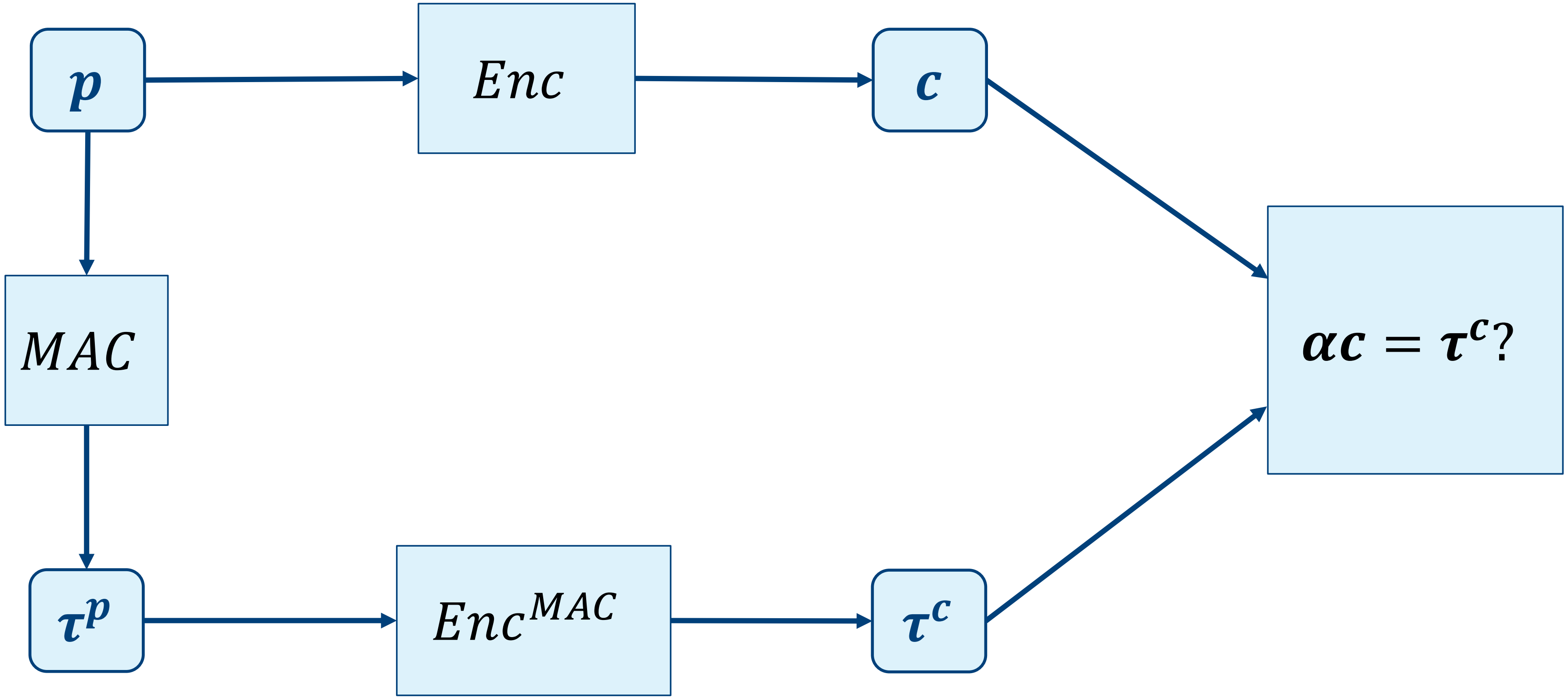
τ^p

Enc^{MAC}

τ^c

Masked Tag Datapath

Now what?



$\boldsymbol{p}$

Enc

$\boldsymbol{c}$

MAC

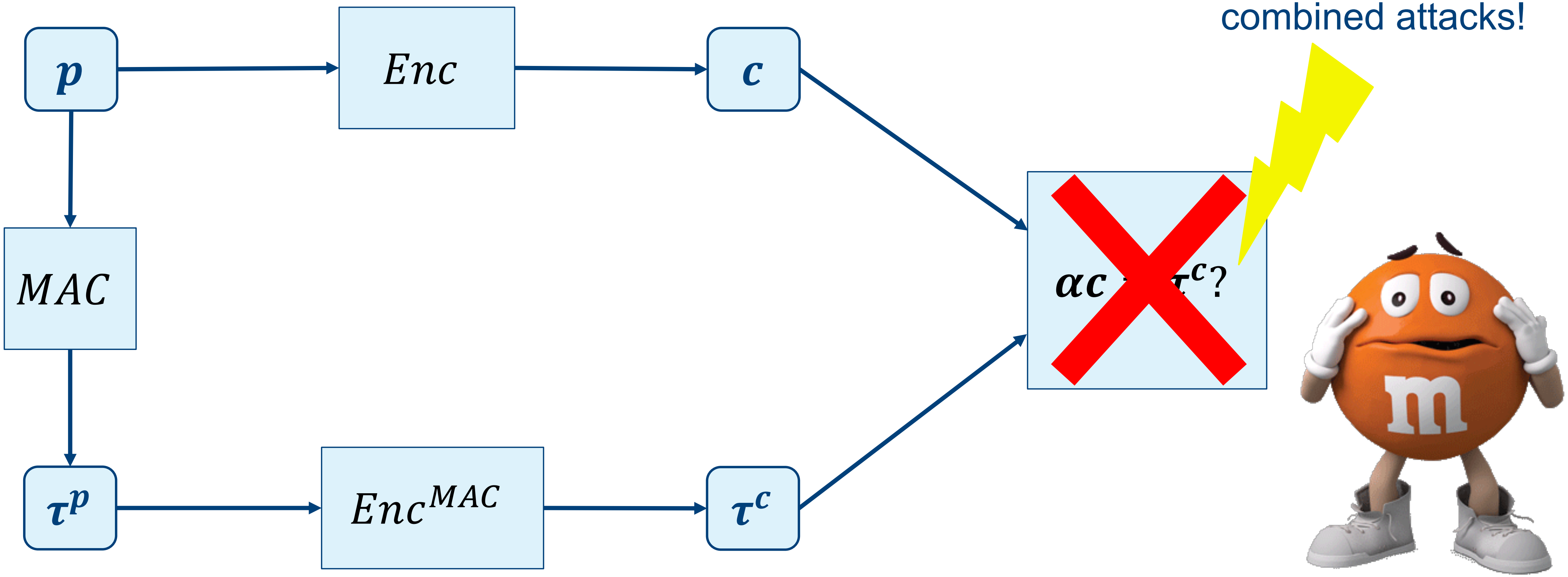
$\boldsymbol{\tau^p}$

Enc^{MAC}

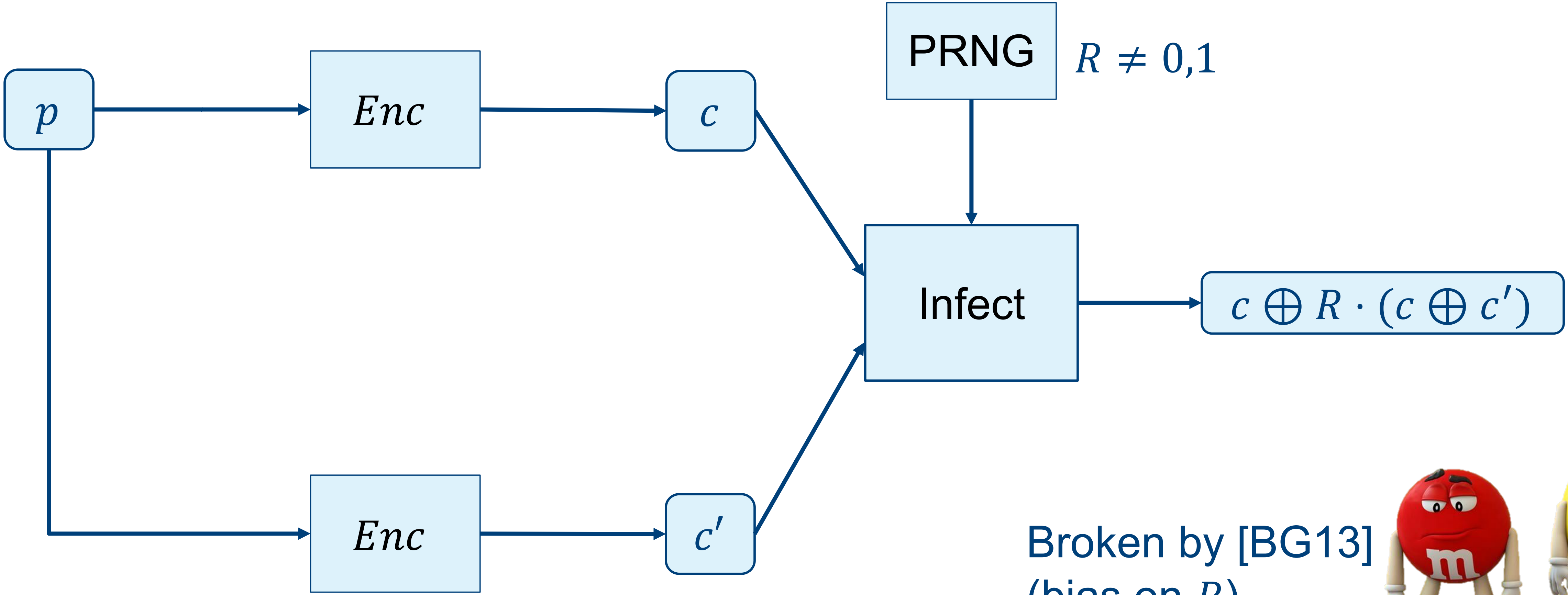
$\boldsymbol{\tau^c}$

$\boldsymbol{\alpha c = \tau^c}?$

Vulnerable to combined attacks!

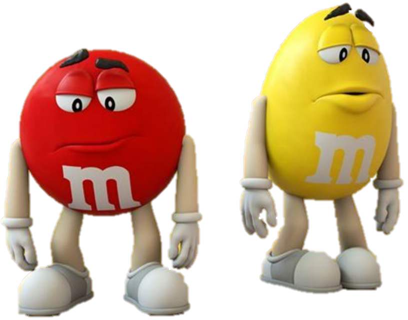


Infective Computation [LRT12]



$R \neq 0,1$

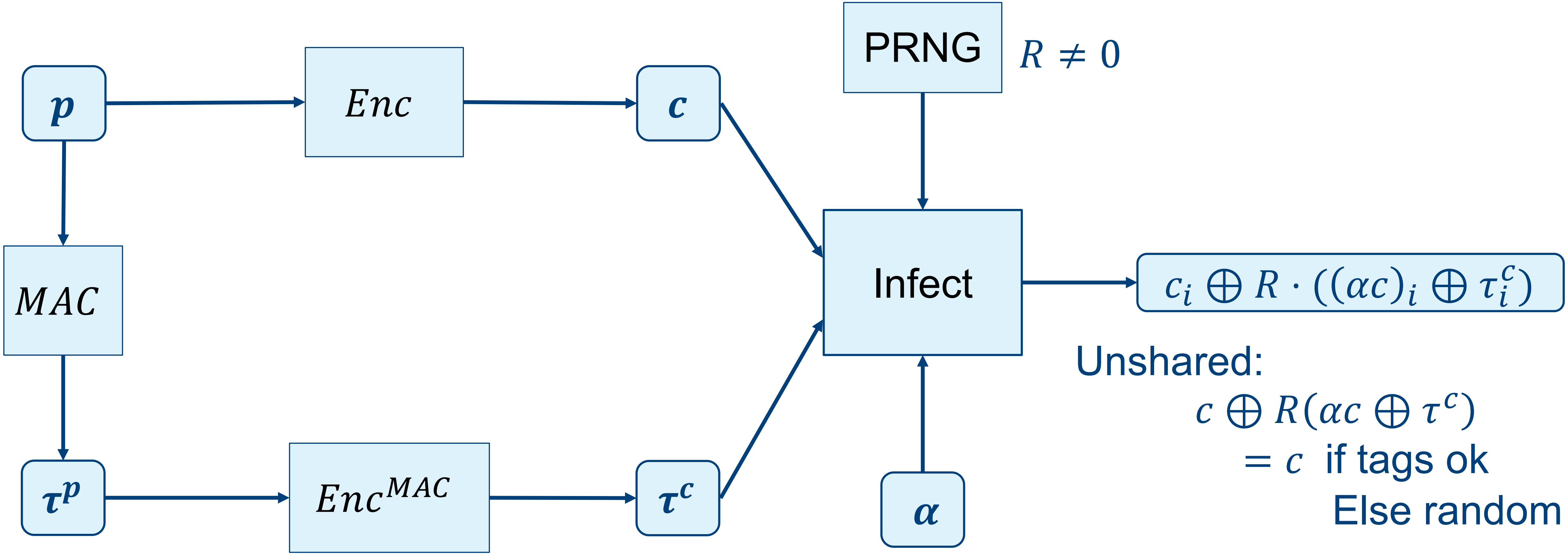
Broken by [BG13]
(bias on R)



[LRT12] V. Lomné, T. Roche, and A. Thillard. On the need of randomness in fault attack countermeasures - application to AES. In G. Bertoni and B. Gierlichs, editors, FDTC 2012, pages 85–94. IEEE Computer Society, 2012.

[BG13] A. Battistello and C. Giraud. Fault analysis of infective AES computations. In W. Fischer and J. Schmidt, editors, FDTC 2013, pages 101–107. IEEE Computer Society, 2013.

PROPOSAL



Unshared:

$c \oplus R(\alpha c \oplus \tau^c)$

$= c$ if tags ok

Else random

No Bias?

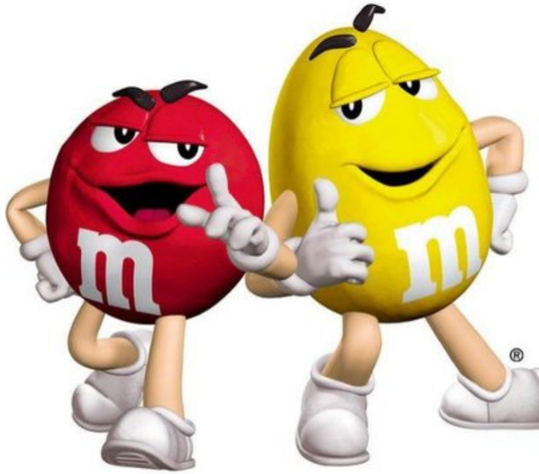
- Faulty evaluation gives $\tilde{c} = c \oplus \Delta$

- Output:

$$\begin{aligned} c \oplus \Delta \oplus R \cdot (\alpha(c \oplus \Delta) \oplus \tau^c) &= c \oplus \Delta \oplus R \cdot (\cancel{\alpha c} \oplus \alpha\Delta \oplus \cancel{\tau^c}) \\ &= c \oplus \Delta(1 \oplus R\alpha) \end{aligned}$$

- Is $\Delta(1 \oplus R\alpha)$ uniformly random?

- Yes if α uniform in $\mathbb{F}_q$ and R uniform in $\mathbb{F}_q^*$



Case Study

EXAMPLE: AES

- Using S-box from [DRB+16]

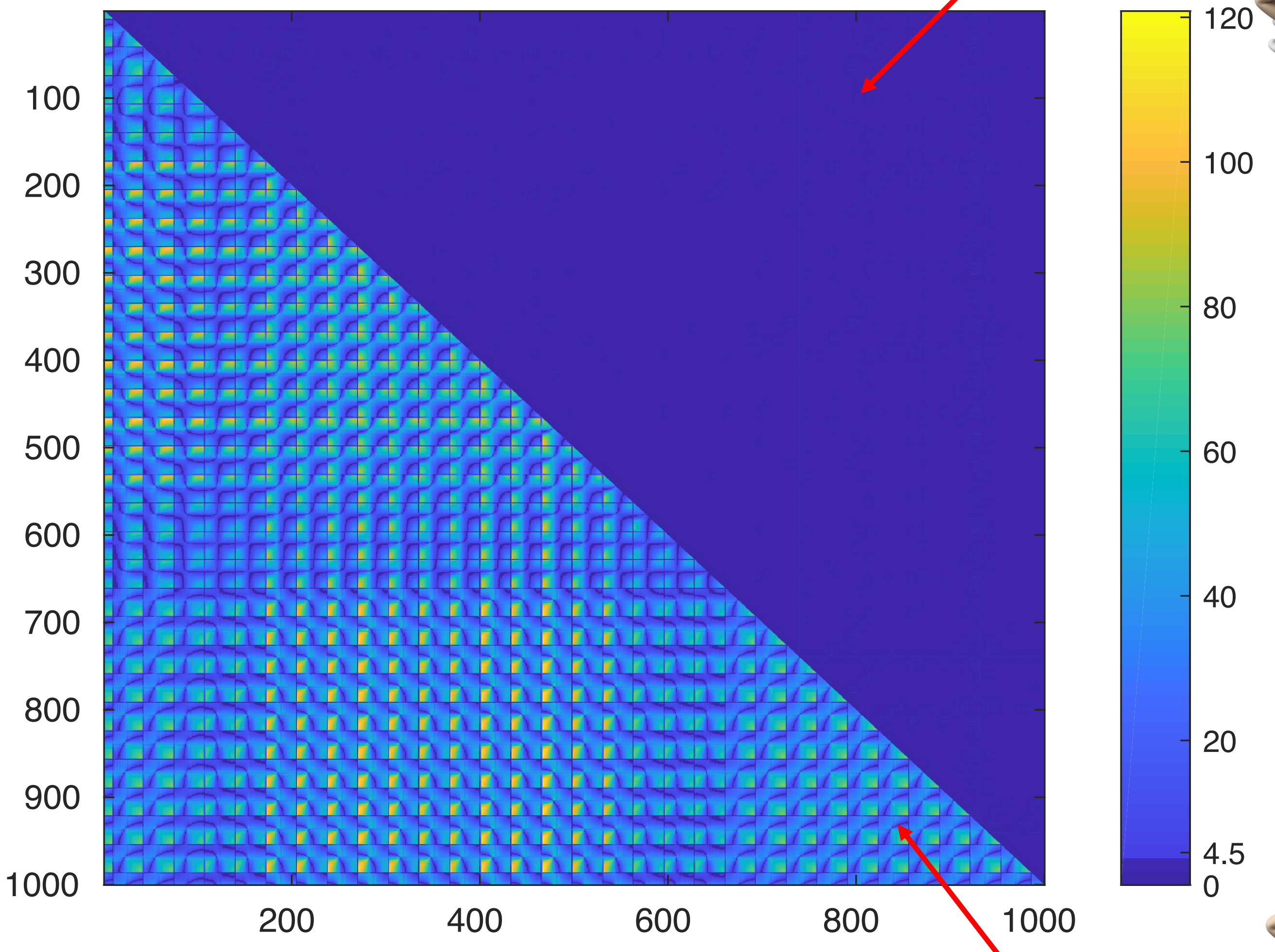
- Comparing area-overhead to state-of-the-art:

	Scheme	SCA-only [kGE]	Combined [kGE]	Overhead factor
$d = 1$	CAPA [RDB+18]	3.6	30.5	8.47
	ParTI [SMG16]	7.9	20.2	2.56
	M&M	7.6	19.2	$\mathbf{2.53}$
$d = 2$	CAPA [RDB+18]	5.9	55.2	9.35
	M&M	12.6	33.2	$\mathbf{2.63}$

[DRB+16] Thomas De Cnudde, Oscar Reparaz, Begül Bilgin, Svetla Nikova, Ventzislav Nikov, Vincent Rijmen: Masking AES with d+1 Shares in Hardware. CHES 2016: 194-212
[RDB+18] Oscar Reparaz, Lauren De Meyer, Begül Bilgin, Victor Arribas, Svetla Nikova, Ventzislav Nikov, Nigel P. Smart: CAPA: The Spirit of Beaver Against Physical Attacks. CRYPTO (1) 2018: 121-151
[SMG16] Tobias Schneider, Amir Moradi, Tim Güneysu: ParTI - Towards Combined Hardware Countermeasures Against Side-Channel and Fault-Injection Attacks. CRYPTO (2) 2016: 302-332

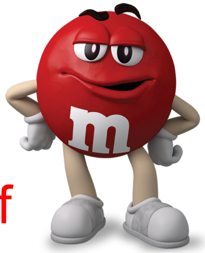
SIDE-CHANNEL EVALUATION

- Spartan6 on SAKURA-G
- TVLA [BCD+13] (t-test)
- 50 million traces



Masks on

Masks off



[BCD+13] G. Becker, J. Cooper, E. De Mulder, G. Goodwill, J. Jaffe, G. Kenworthy, T. Kouzminov, A. Leiserson, M. Marson, P. Rohatgi, et al. Test vector leakage assessment (tvla) methodology in practice. In International Cryptographic Module Conference, volume 1001, page 13, 2013.

Fault Evaluation

- No “standard” methods of verification
- Adapt HDL with possibility to inject randomized faults (XOR)
- Experiment: 50 000 iterations, 189 faulty ciphertexts not infected
  → experimental rate of detection/infection = 0.9962
- Theoretical rate of detection/infection: $1 - 2^{-8} = 0.9961$
- Verification methodology extended and automized in VerFI
  (see poster session)

Take-Away

TAKE AWAY TAKE AWAY

TAKE AWAY

- Cheaper than CAPA and stronger adversary than ParTI
- Super versatile: use any existing or future(?) masking scheme
- Infective computation can be combined with detection result (see paper)
- Future work:
  - provable security against combined attacks?
  - Verification tools for combined countermeasures?
  - Optimization: don’t update tags: $\alpha x \rightarrow \alpha^{-1} y \rightarrow \cdots \rightarrow \alpha z$

Thank You