THRESHOLD CRYPTOGRAPHY AGAINST COMBINED ATTACKS

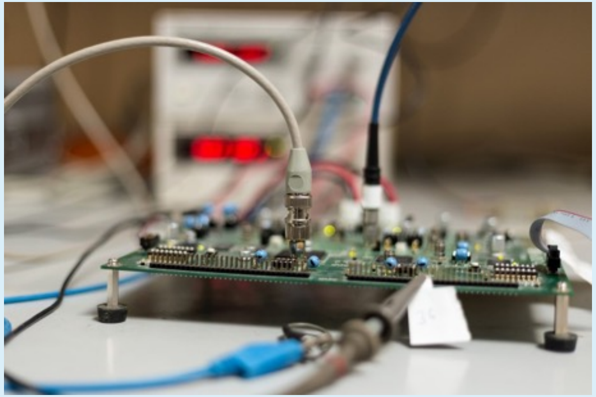
Lauren De Meyer

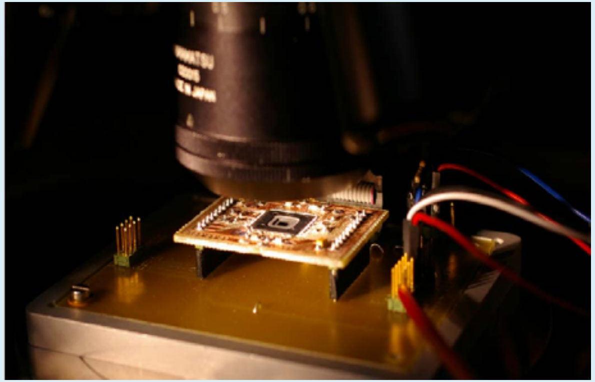
Joint work with Oscar Reparaz, Victor Arribas, Begül Bilgin, Svetla Nikova, Ventzi Nikov, Vincent Rijmen, Nigel Smart

NIST

fwo

KU LEUVEN





Back to the 90’s

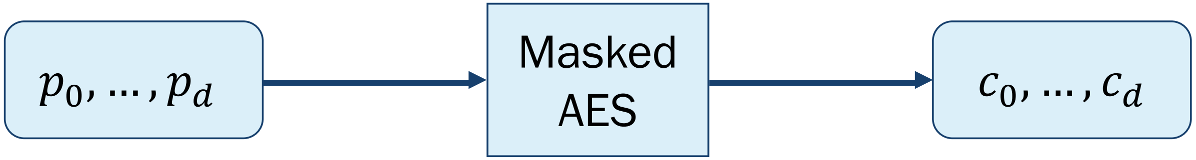
- Differential Power Analysis (DPA) - Paul Kocher 1999 [1]

- Differential Fault Analysis (DFA) - Biham and Shamir 1997 [2]

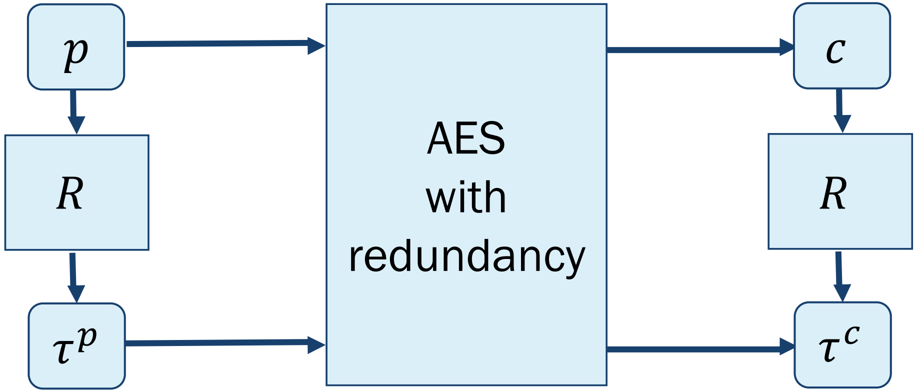
[1] Paul C. Kocher, Joshua Jaffe, Benjamin Jun: Differential Power Analysis. CRYPTO 1999: 388-397
[2] Eli Biham, Adi Shamir: Differential Fault Analysis of Secret Key Cryptosystems. CRYPTO 1997: 513-525

Countermeasures

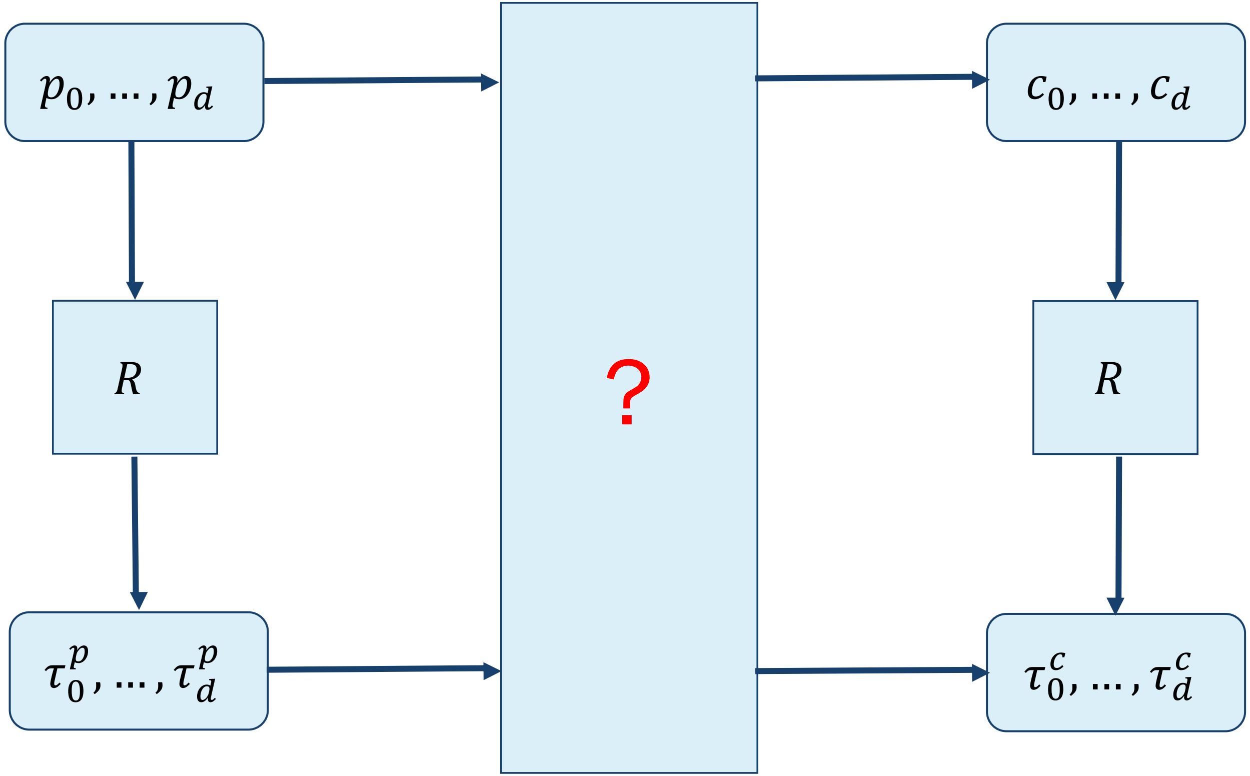
- Against side-channel attacks:
  - *Hiding*
  - ***Masking***



- Against fault attacks:
  - *Repetition, redundancy (error detecting codes), **tags**,...*
  - ***Detection**, correction or **infection***



Combined Attacks



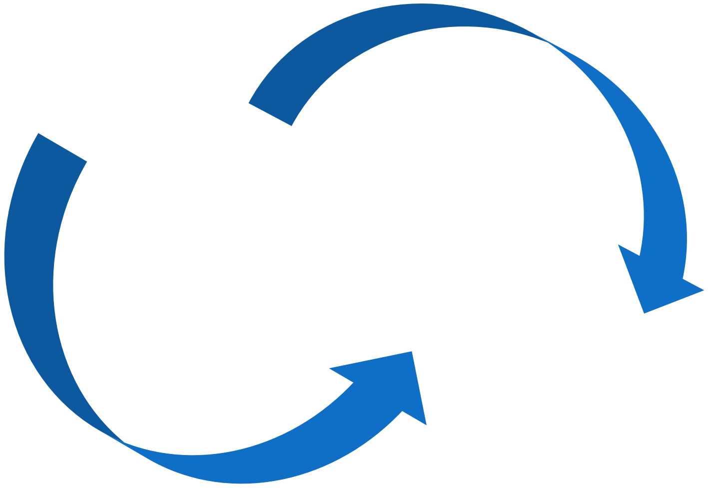
Threshold Cryptography

	MPC	Embedded Systems	
Passive	Shamir's Secret Sharing [1]	Masking TI [3], ...	SCA
Active	SPDZ [2], ...	....	SCA+FA

[1] Adi Shamir: How to Share a Secret. Commun. ACM 22(11): 612-613 (1979)
[2] Ivan Damgård, Valerio Pastro, Nigel P. Smart, Sarah Zakarias: Multiparty Computation from Somewhat Homomorphic Encryption. CRYPTO 2012: 643-662
[3] Svetla Nikova, Vincent Rijmen, Martin Schläffer: Secure Hardware Implementation of Nonlinear Functions in the Presence of Glitches. J. Cryptology 24(2): 292-321 (2011)

Two Proposals:

- M&M:
  - To be presented at CHES 2019 [2]
  - Extension of Masking schemes (TI,...)

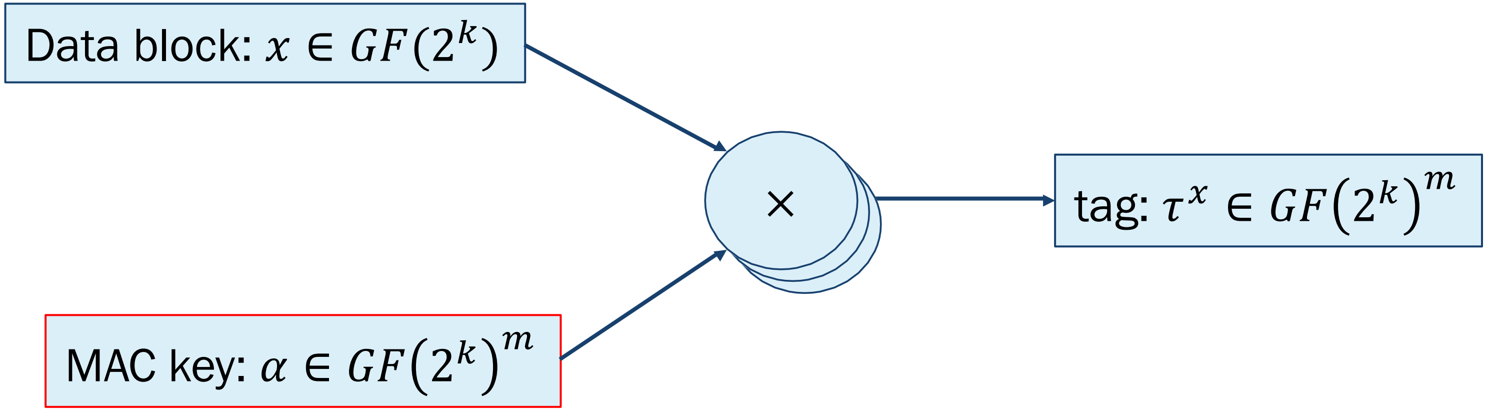


- CAPA:
  - Presented at Crypto 2018 [1]
  - Based on active MPC protocol SPDZ

[1] 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

[2] Lauren De Meyer, Victor Arribas, Svetla Nikova, Ventzislav Nikov, Vincent Rijmen: M&M: Masks and Macs against Physical Attacks. IACR Trans. Cryptogr. Hardw. Embed. Syst.2019(1): 25-50 (2019)

Information-theoretic MAC tags

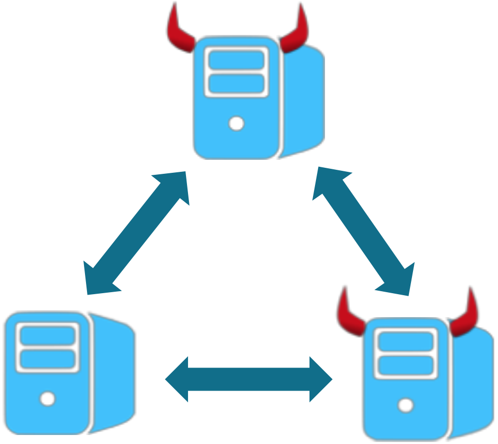


Used 1x!

Secret!

$\Pr[\text{faulted tag=consistent}] = 2^{-km}$

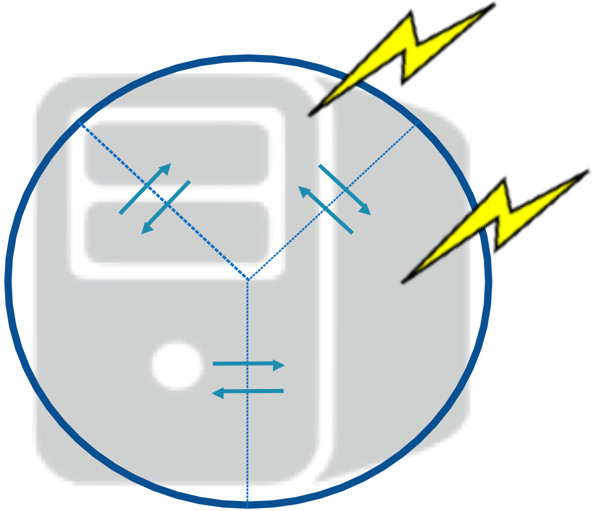
CAPA: from MPC to Embedded Security



- Expensive communication
- Local memory relatively cheap
- Adversaries ⊂ Parties (internal)
- Rushing adversary

- Active Adversary
- Dishonest Majority

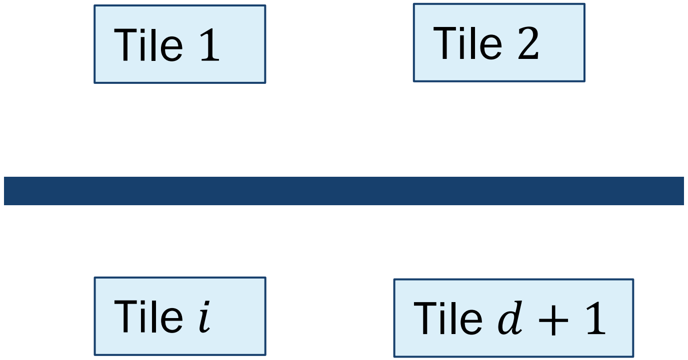
Tile-probe-and-fault-model



- Communication = wiring
- Restricted Storage
- External Adversary
- Zero propagation delay ~ synchronized parties

Tile-probe-and-fault Model

- Static Adversary
- Side-Channel Adversary:
  - *Probe ALL intermediates within d tiles*
  - *Correct value disclosed with probability 1*
- Faulting Adversary:
  - *Exact and known (~very precise laser)*
    - In up to d tiles
    - Probability 1
  - *Random (~clock glitching)*
    - No tile restriction
- Combined Adversary:
  - *Combination and interaction of faults and probes within d tiles*



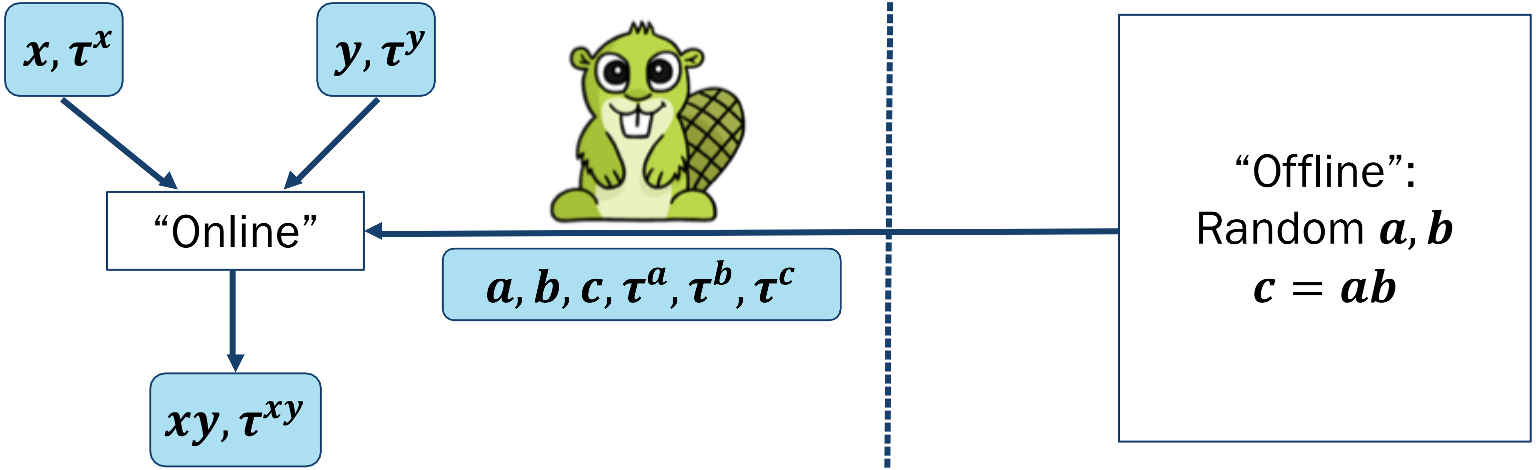
CAPA: Beaver Multiplications

"Online" phase:

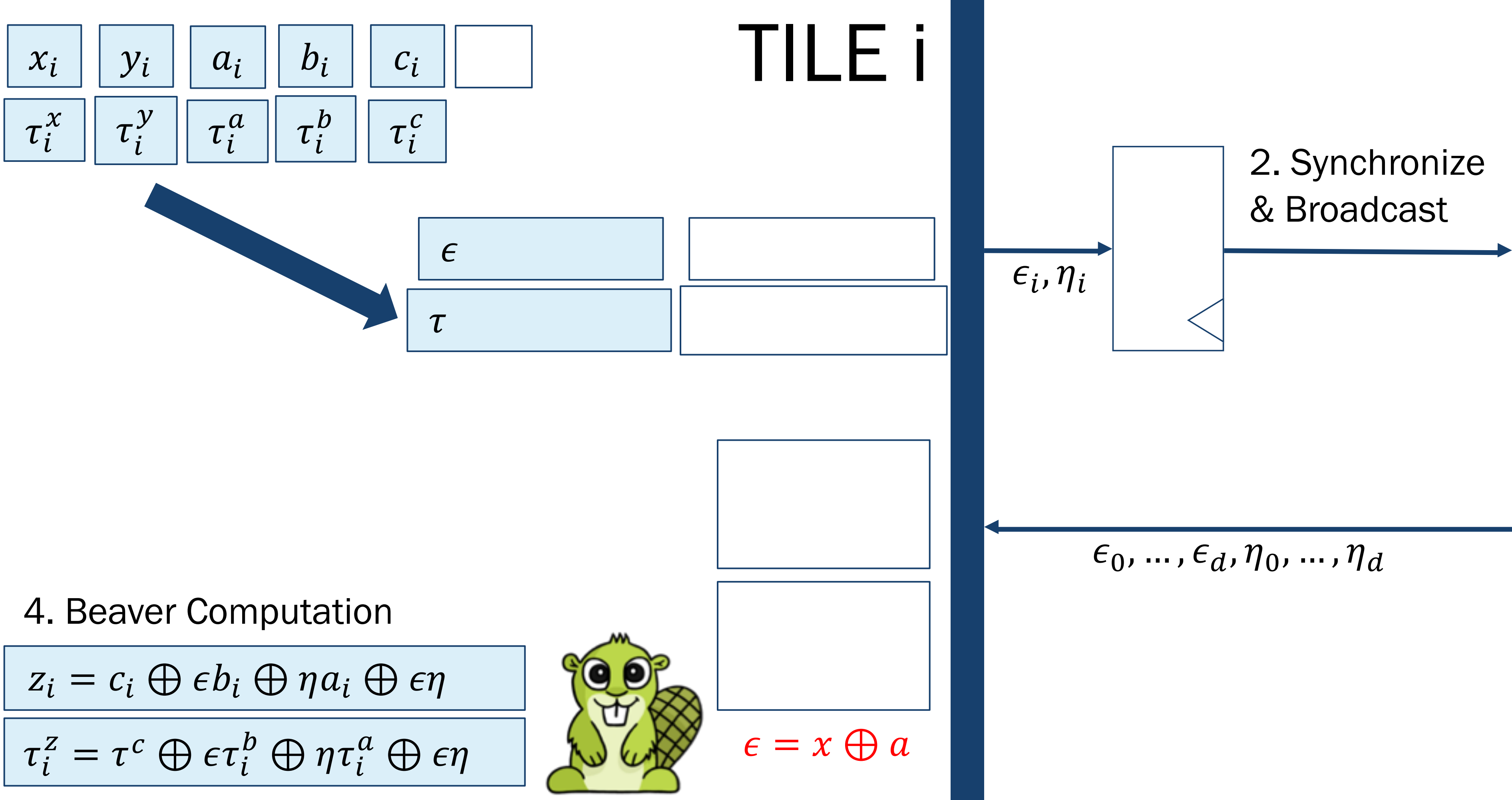
- Beaver multiplications: "Blind" the inputs
- MAC tag check of "Blinded" values

"Offline" phase:

- Generate auxiliary data
- Independent of key/inputs



Donald Beaver: Precomputing Oblivious Transfer. CRYPTO 1995: 97-109


TILE i
x_i y_i a_i b_i c_i
τ_i^x τ_i^y τ_i^a τ_i^b τ_i^c
ϵ
τ
2. Synchronize & Broadcast
ϵ_i, η_i
$\epsilon_0, \ldots, \epsilon_d, \eta_0, \ldots, \eta_d$
4. Beaver Computation
$z_i = c_i \oplus \epsilon b_i \oplus \eta a_i \oplus \epsilon\eta$
$\tau_i^z = \tau^c \oplus \epsilon\tau_i^b \oplus \eta\tau_i^a \oplus \epsilon\eta$
$\epsilon = x \oplus a$

TILE i

x_i | y_i | a_i | b_i | c_i

τ_i^x | τ_i^y | τ_i^a | τ_i^b | τ_i^c

ϵ

τ

2. Synchronize & Broadcast

ϵ_i, η_i

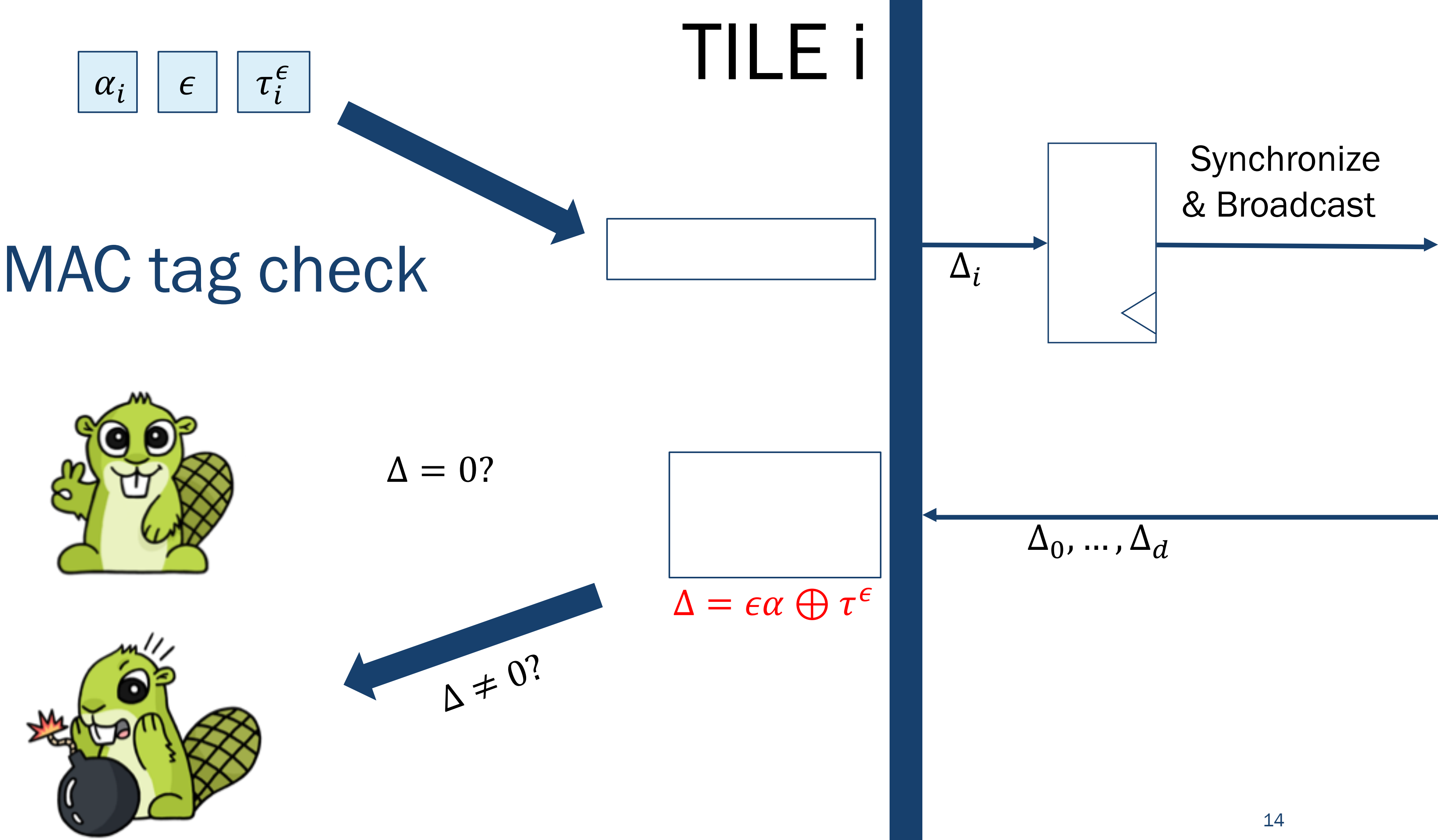
$\epsilon_0, \dots, \epsilon_d, \eta_0, \dots, \eta_d$

4. Beaver Computation

$$z_i = c_i \oplus \epsilon b_i \oplus \eta a_i \oplus \epsilon\eta$$

$$\tau_i^z = \tau^c \oplus \epsilon\tau_i^b \oplus \eta\tau_i^a \oplus \epsilon\eta$$

$\epsilon = x \oplus a$

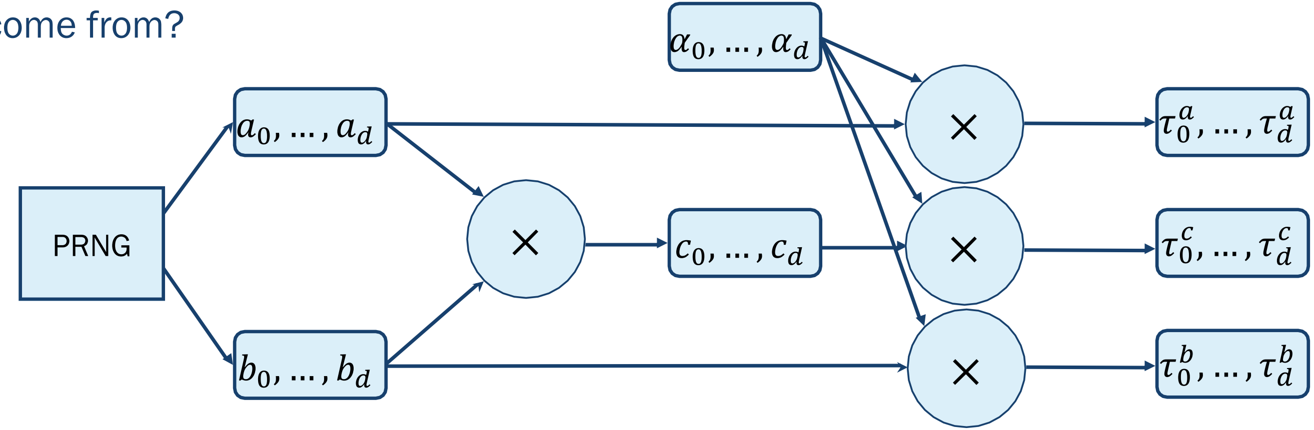

TILE i
MAC tag check
α_i
ϵ
τ_i^ϵ
Δ_i
Synchronize & Broadcast
$\Delta_0, \ldots, \Delta_d$
$\Delta = 0?$
$\Delta = \epsilon\alpha \oplus \tau^\epsilon$
$\Delta \neq 0?$

CAPA Preprocessing Phase

- Where do Beavers come from?

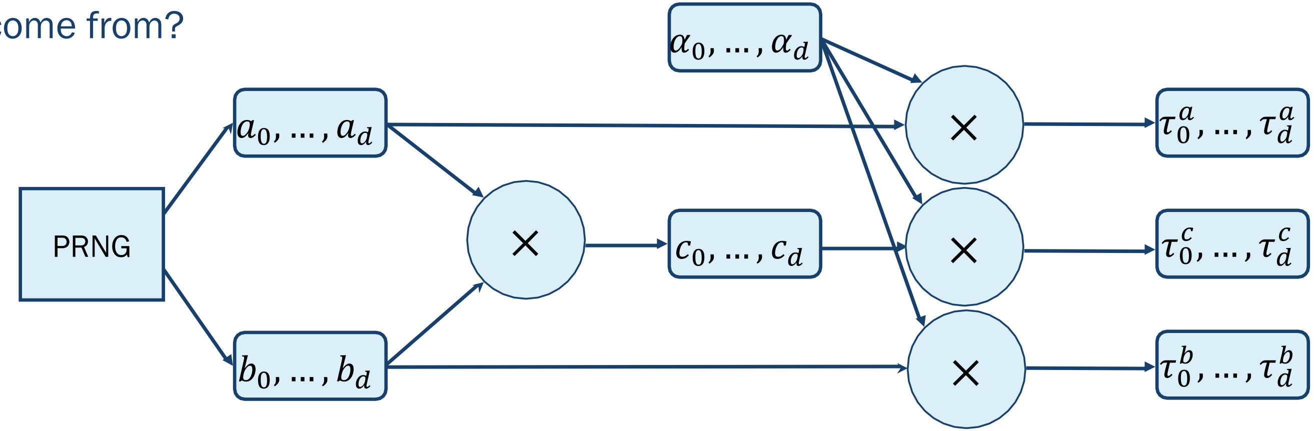
CAPA Preprocessing Phase

- Where do Beavers come from?



CAPA Preprocessing Phase

- Where do Beavers come from?



- Detecting bad Beavers

Like SPDZ: Sacrificing

CAPA Results

- Implementation = very costly!
  - *Example: AES with detection probability 0.996*

	$d = 1$	$d = 2$
Area (kGE)	**122**	**215**
- Evaluation	28	42
- Preprocessing	94	173
Randomness/S-box (bytes)	64	156

- *Superstrong* security:
  - *Adversary is **very** powerful*
  - *~internal adversary (MPC)*
  - *realistic?*

- The alternative route to combined countermeasures:
  - *Start from masking*
  - *Add fault countermeasure*

M&M Adversary Model

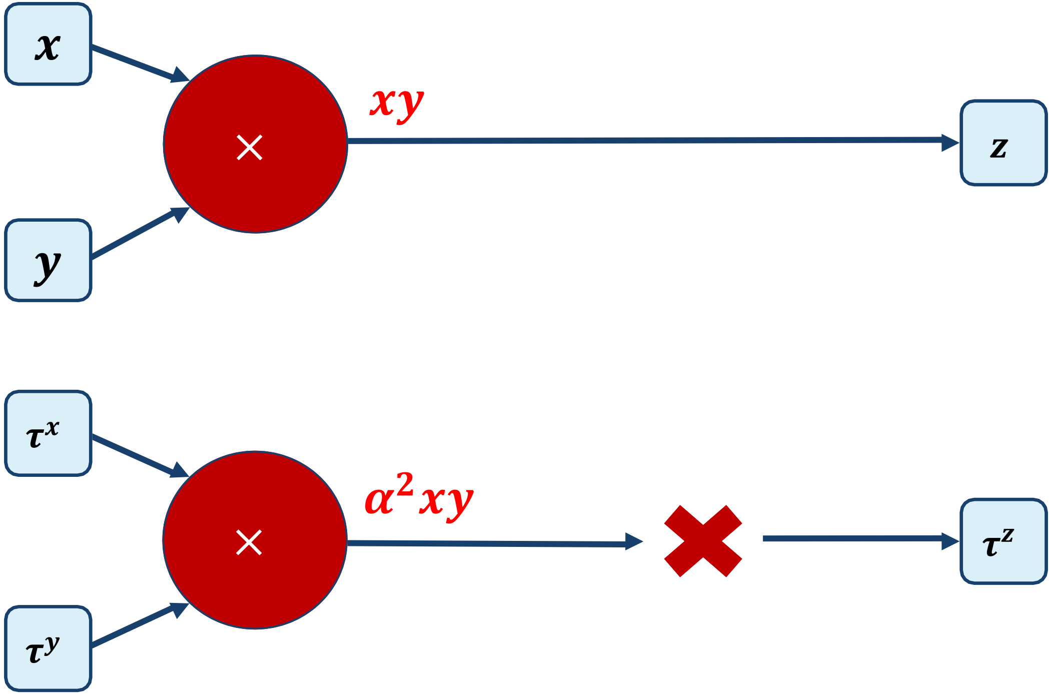
- Side-Channel Adversary:
  - *d-probing model*
  - *Noisy leakage model*
- Faulting Adversary:
  - *Fault = stochastic additive error*
    - Unlimited # bits
  - *Fault = exact*
    - Limited to d shares
- NOT tile-probe-and-fault

M&M Multiplication

TI
DOM
CMS
...

Masks:

MACs:

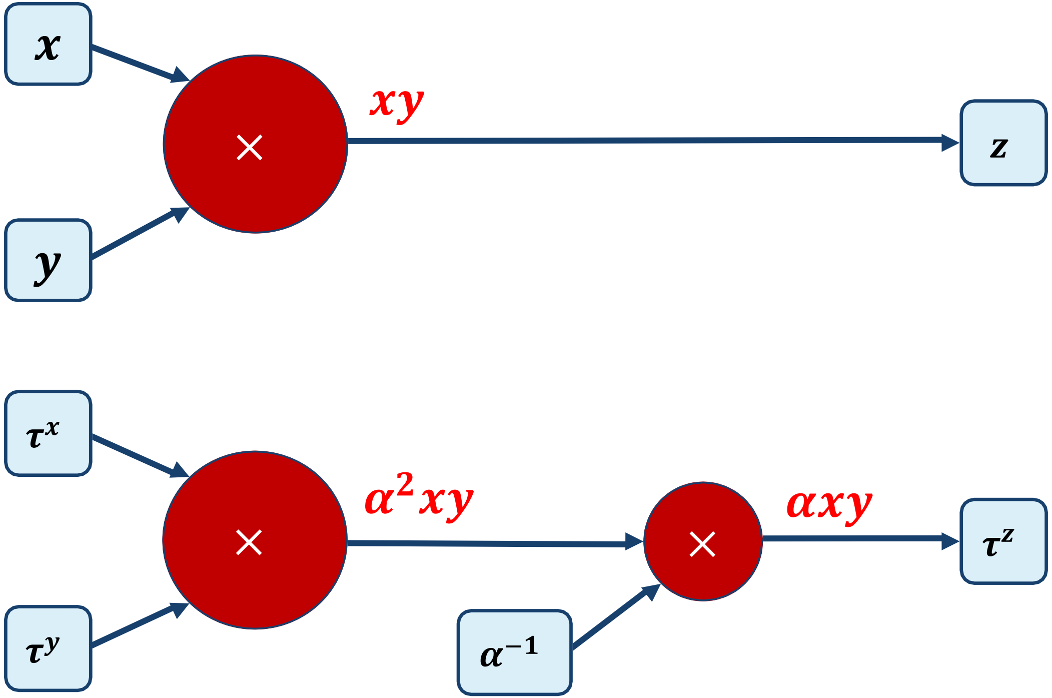


M&M Multiplication

TI
DOM
CMS
...

Masks:

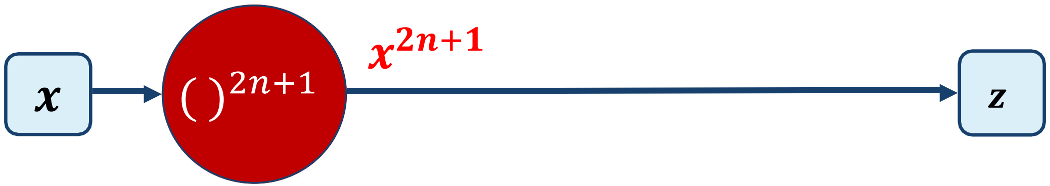
MACs:



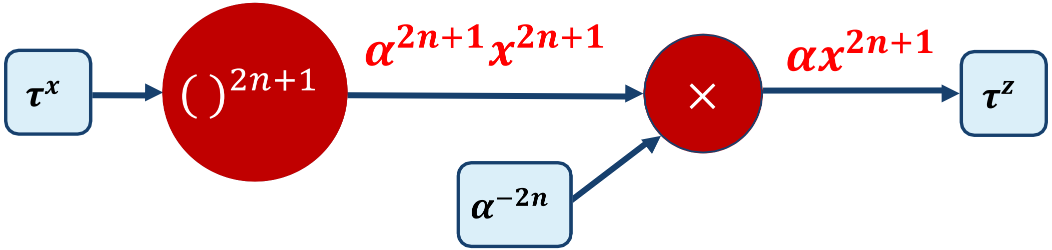
Or other operations....

TI
DOM
CMS
...

Masks:



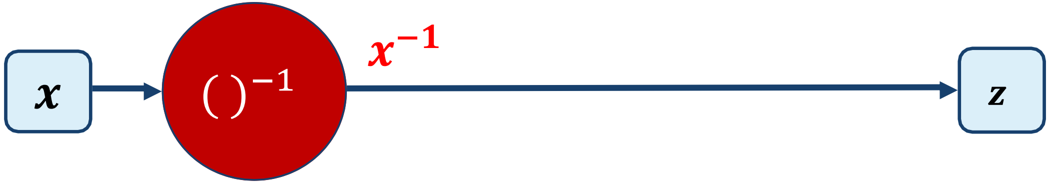
MACs:



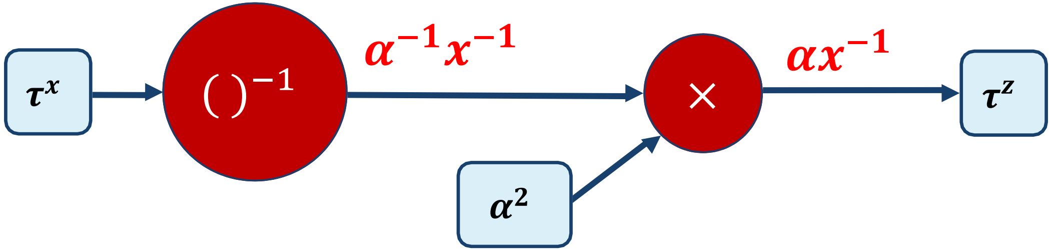
And even...

TI
DOM
CMS
...

Masks:



MACs:

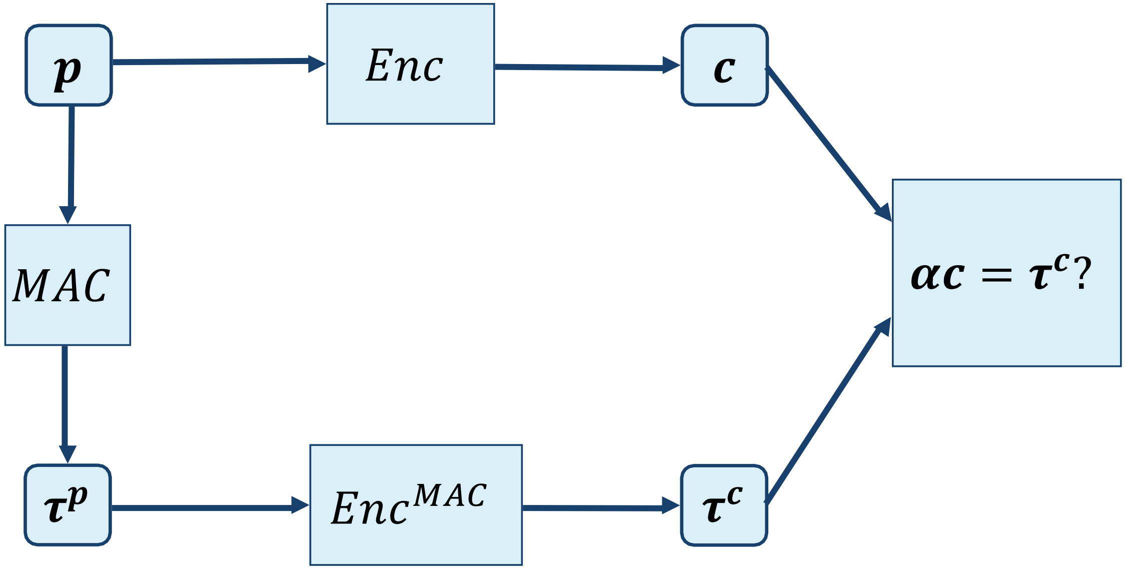


Building blocks for any algorithm

Many flavors of masking

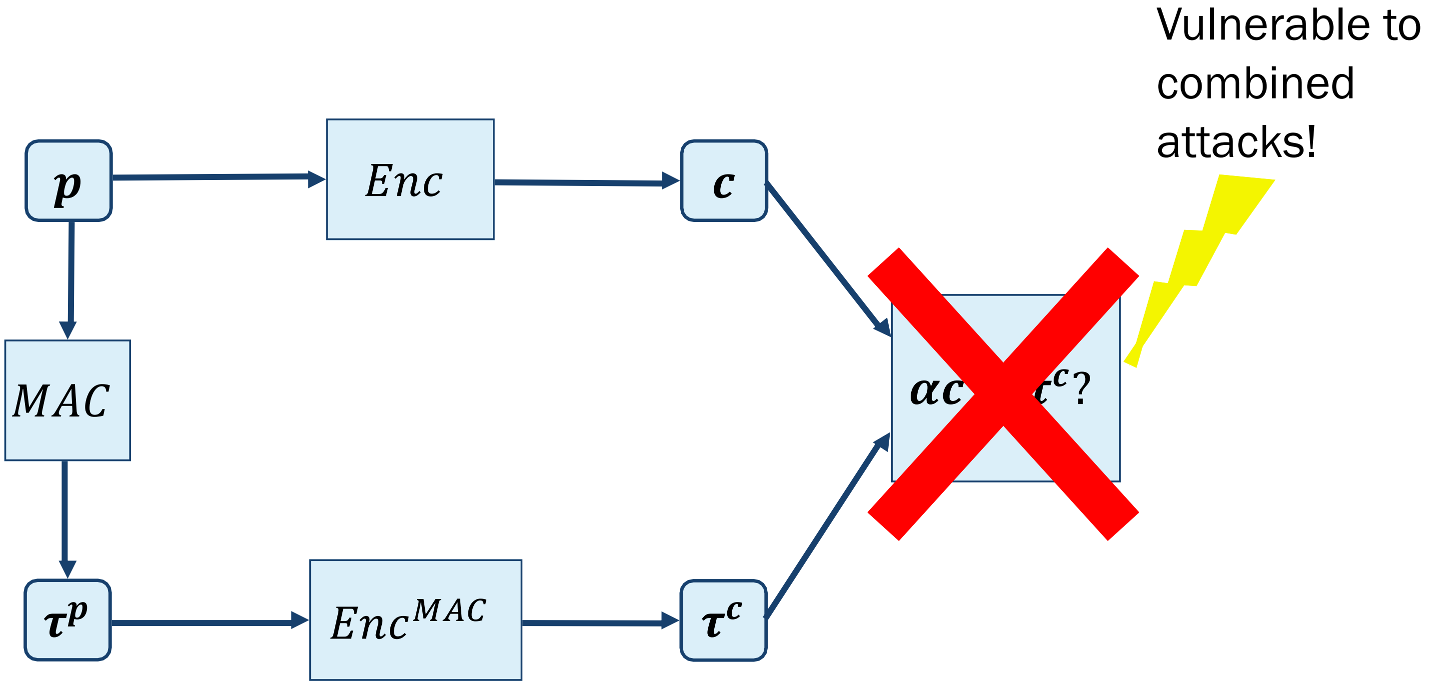
→ many flavors of M&M

How to check?

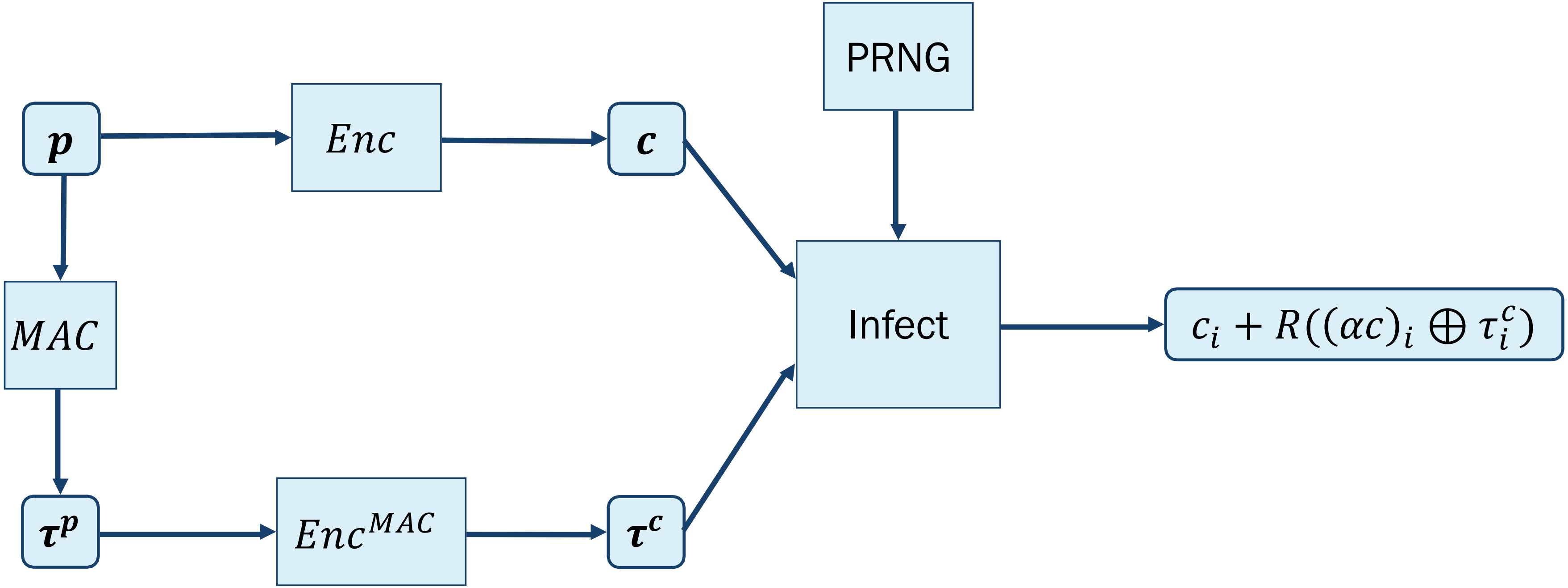


$\boldsymbol{p}$
Enc
$\boldsymbol{c}$
MAC
$\boldsymbol{\alpha c = \tau^c?}$
$\boldsymbol{\tau^p}$
Enc^{MAC}
$\boldsymbol{\tau^c}$

How to check?



Infective Computation



M&M Results

- Much Lower cost
  - *Example: AES with detection probability 0.996*

	$d = 1$	$d = 2$
Area (kGE)	$\mathbf{19.2}$	$\mathbf{33.2}$
Randomness/S-box (bits)	116	348

  - *Overhead factor ~2.53-2.63!*
- Adversary model weaker but more realistic
- BUT combined attacks….
  - *Not vulnerable to state-of-the-art attacks*
  - *But not provably secure since not derived from MPC*

Face-off

d-th order DPA		
- #probes	d	Unlimited in d tiles
- Coupling	✗	✓
- Glitches	✓	✓
d-shot DFA		
- Detection probability	$1-2^{-km}$	$1-2^{-km}$
- Exact faults	Unlimited in d shares	Unlimited in d tiles
- Stochastic faults	Unlimited	Unlimited
- Safe Errors	✗	✓
Combined Attacks		
- Resist PACA [1]	✓	✓
- Provable security	✗	✓

[1] Frédéric Amiel, Karine Villegas, Benoit Feix, Louis Marcel: Passive and Active Combined Attacks: Combining Fault Attacks and Side Channel Analysis. FDTC2007: 92-102

What’s next?

- Cheaper generation of Beaver triplets?
- Relaxing CAPA adversary?
- Provable security against combined attacks at lower cost?
- Verification tools for combined attacks?

QUESTIONS?