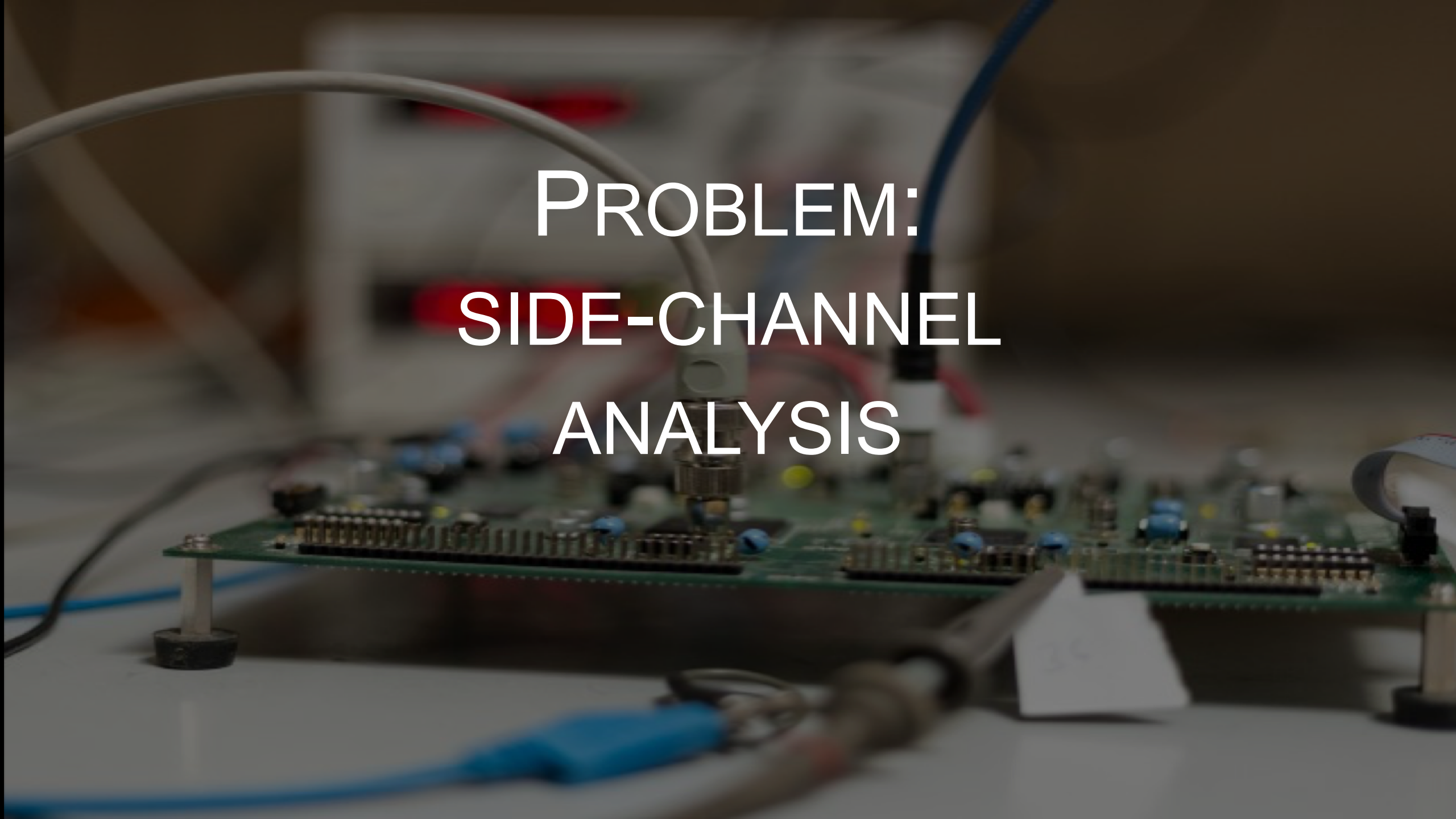
KU LEUVEN

fwo

Consolidating Security Notions in Hardware Masking

CHES 2019

Lauren De Meyer, Begül Bilgin, Oscar Reparaz



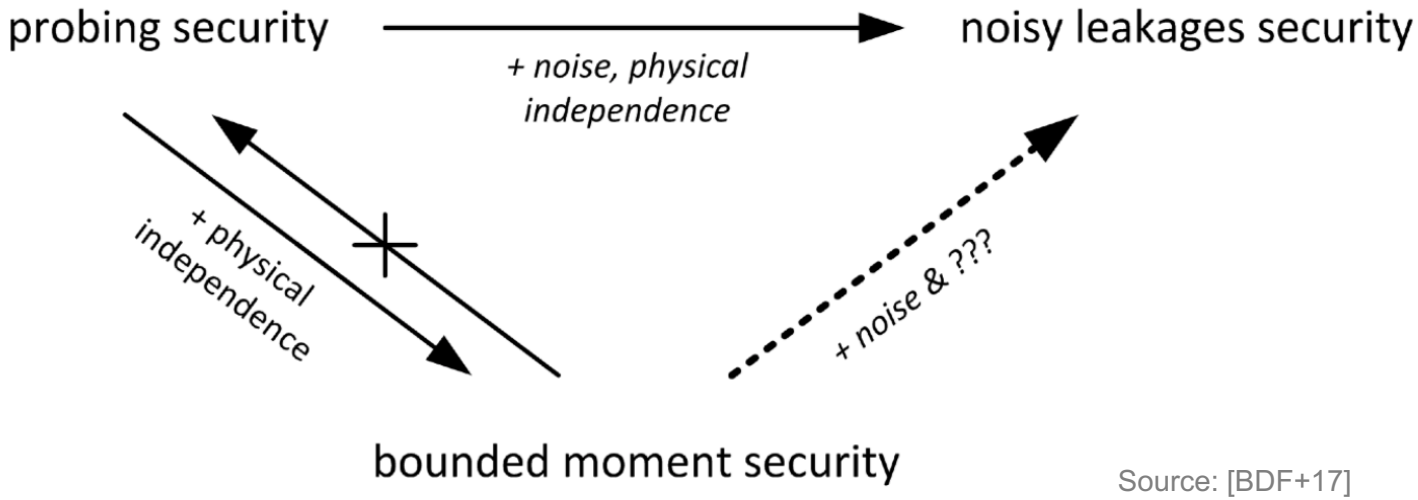
Problem: side-channel analysis

Solution: Masking

PROBING MODEL [ISW03]

- Adversary can probe up to d intermediate values
- ”Ideal circuit”: probes are exact and instantaneous and independent

- Basis for many proofs in SCA

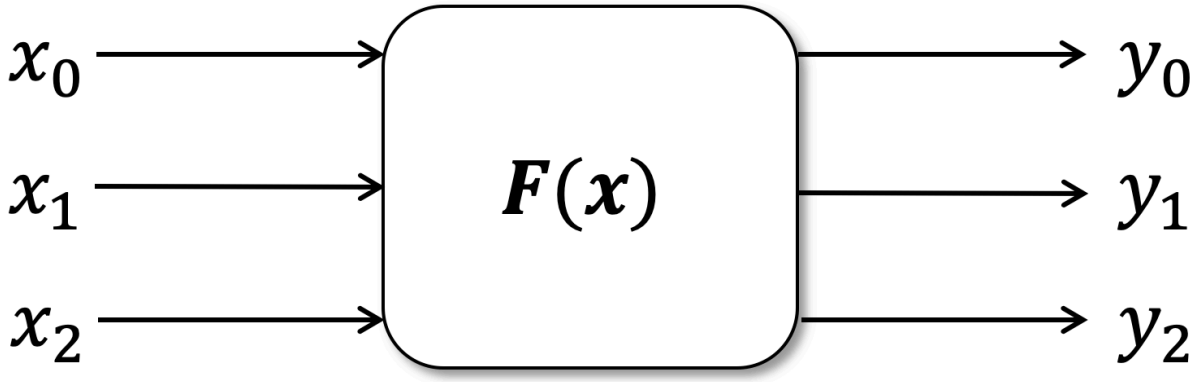


Source: [BDF+17]

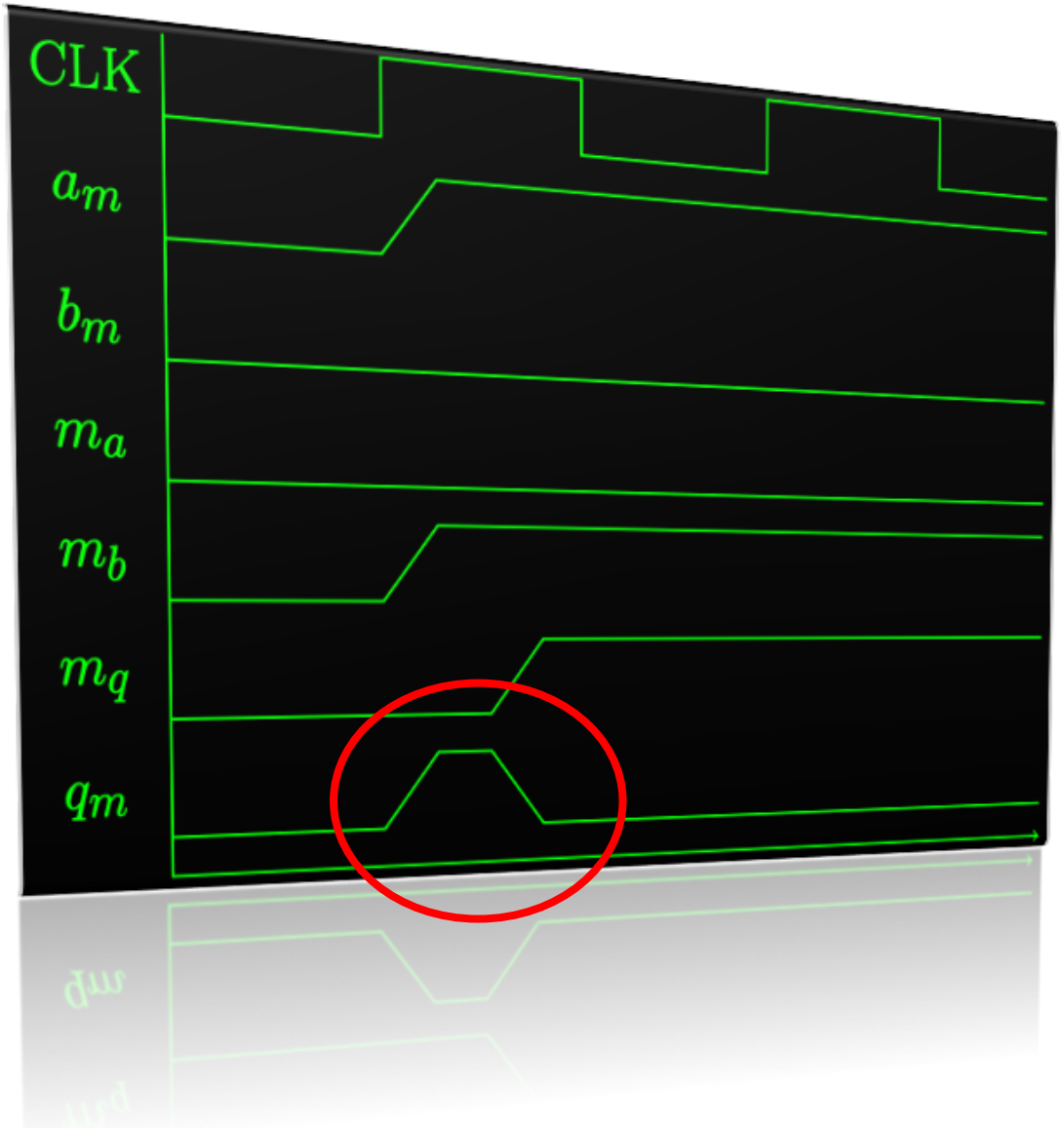
[ISW03] Yuval Ishai, Amit Sahai, David A. Wagner: Private Circuits: Securing Hardware against Probing Attacks. CRYPTO 2003: 463-481
[BDF+17] Gilles Barthe, François Dupressoir, Sebastian Faust, Benjamin Grégoire, François-Xavier Standaert, Pierre-Yves Strub: Parallel Implementations of Masking Schemes and the Bounded Moment Leakage Model. EUROCRYPT (1) 2017: 535-566

MASKING

- Goal: no correlation between any d wires and the secret
- Split sensitive intermediates into $d + 1$ shares
- $x = x_0 \blacksquare x_1 \blacksquare x_2 \Rightarrow y = F(x) = y_0 \blacksquare y_1 \blacksquare y_2$

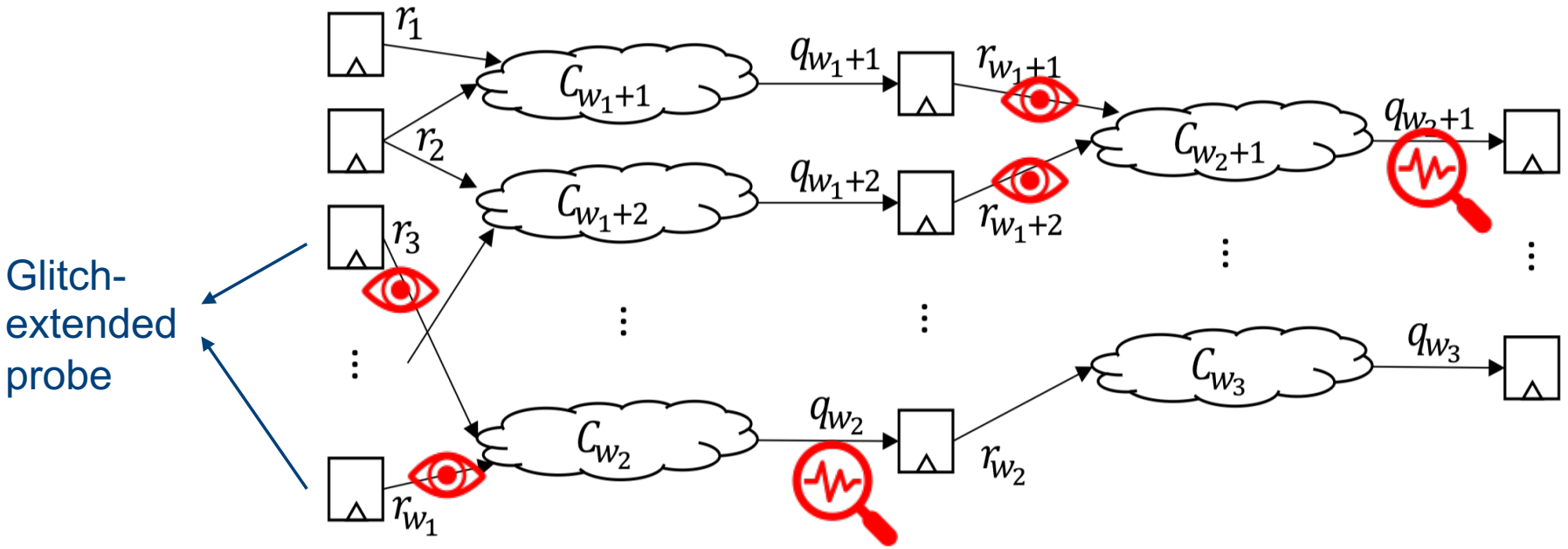


Extra Problem in HW: Glitches!



GLITCH-EXTENDED PROBING MODEL [RBN+15]

- d probes
- Assume a glitch on combinational logic C_i can reveal any of it inputs
- → Includes worst-case glitch



[RBN+15] Oscar Reparaz, Begül Bilgin, Svetla Nikova, Benedikt Gierlichs, Ingrid Verbauwhede: Consolidating Masking Schemes. CRYPTO (1) 2015: 764-783

$$I(\quad ; \quad) = 0$$

KU LEUVEN

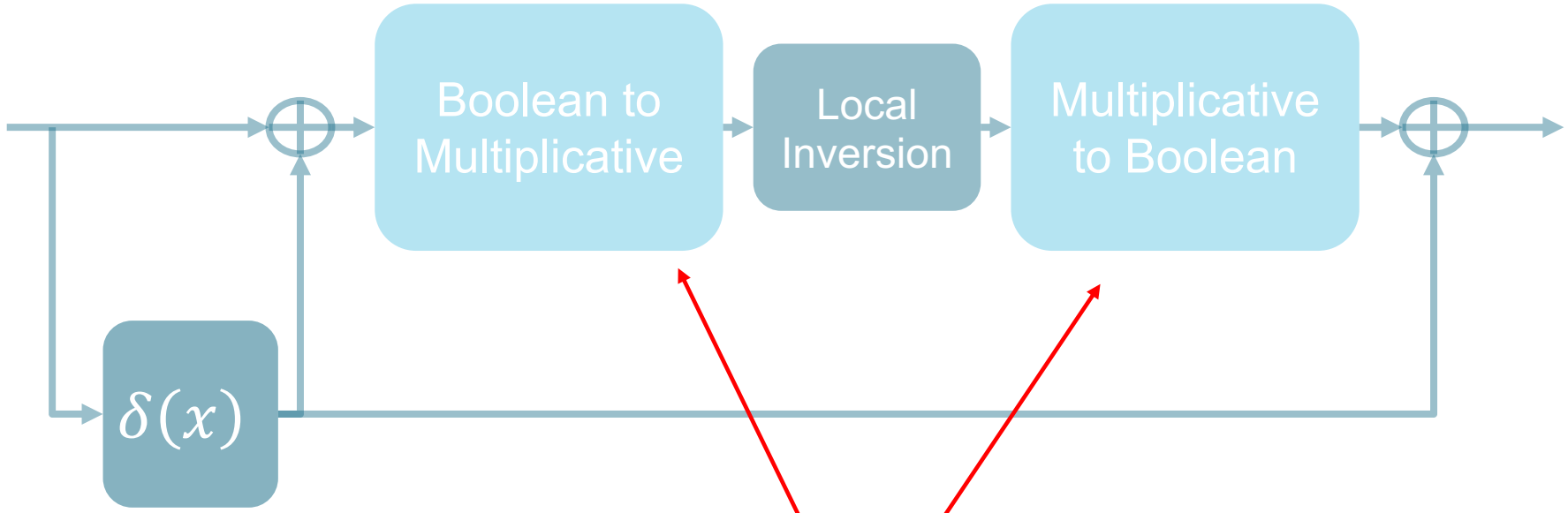
$$I(\quad ; \quad) = 0$$

- Simple
- Versatile
  - Probing/NI/SNI
  - Different models (with/without glitches, …)
  - Any type of masking (Boolean, multiplicative, arithmetic, …)
  - Non-uniformity possible
  - Information-theoretic vs practical security
  - Leakage functions (identity, Hamming, …)

THE STORY

KU LEUVEN

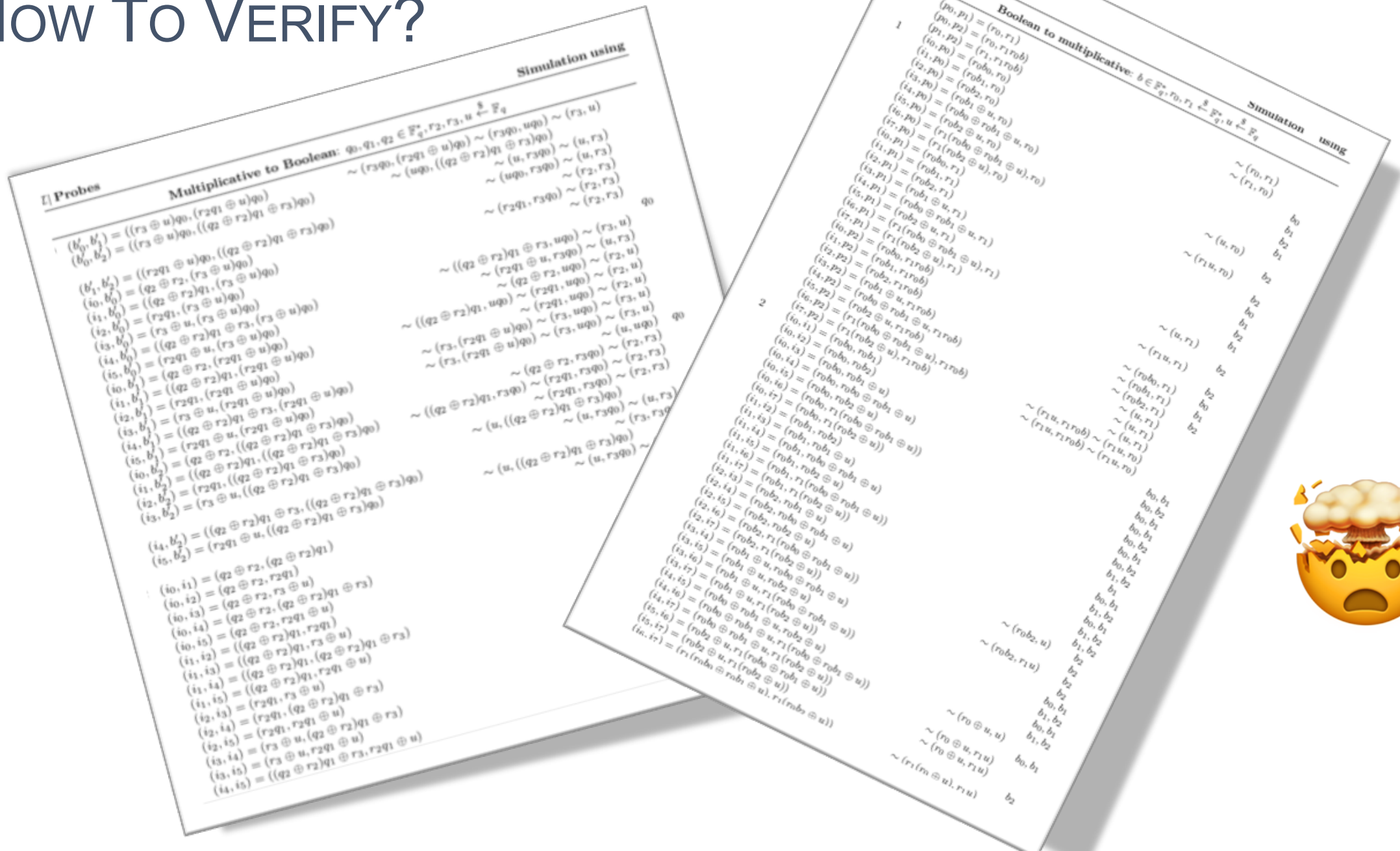
CHES '18: Multiplicative Masking



Verification?

[DRB18] Lauren De Meyer, Oscar Reparaz, Begül Bilgin: Multiplicative Masking for AES in Hardware. IACR Trans. Cryptogr. Hardw. Embed. Syst.2018(3): 431-468 (2018)

How To Verify?

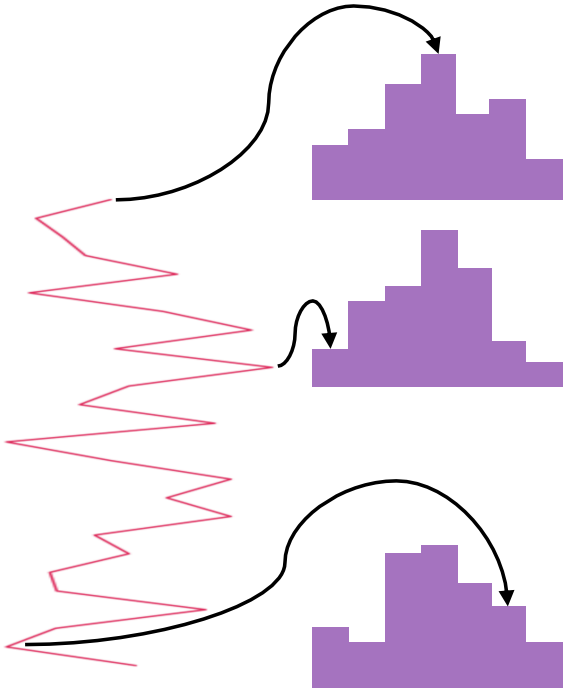


TOOL FROM [REP16]

```
u8 m1 = nonzero_rnd()&bitmask;  add_timesample(m1);
u8 b1 = crypto_input_shares[0]; add_timesample(b1);
u8 b2 = crypto_input_shares[1]; add_timesample(b2);

u8 b1m1 = mult_log(b1, m1);     add_timesample(b1m1);
u8 b2m1 = mult_log(b2, m1);     add_timesample(b2m1);
u8 m2 = b1m1 ^ b2m1;            add_timesample(m2);
```

0x31
0x9A
0xF5
0x3F
0xB5
0x8A



- Simulated traces of intermediates
- Random inputs
- → TVLA (t-test) to detect flaws
- Higher orders: combine probes (e.g. centered product)
- Only for software (no glitches ☹)

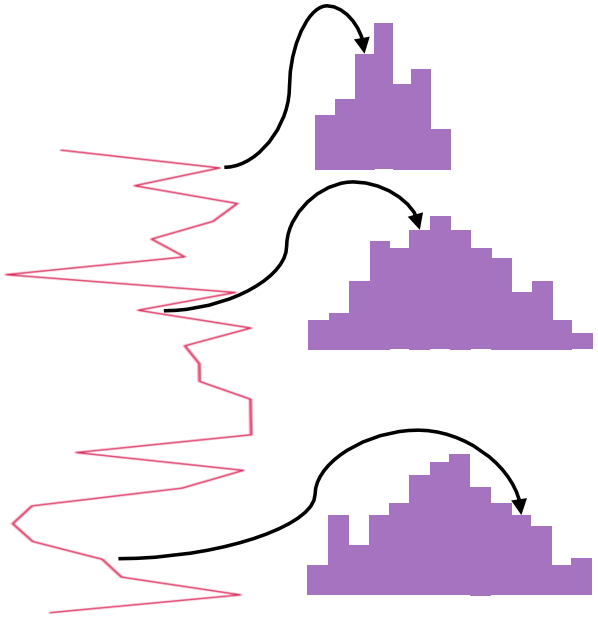
[Rep16] Oscar Reparaz: Detecting Flawed Masking Schemes with Leakage Detection Tests. FSE 2016: 204-222

IDEA: GLITCH-EXTENDED PROBES

```
u8 m1 = nonzero_rnd()&bitmask;  add_timesample(m1);
u8 b1 = crypto_input_shares[0]; add_timesample(b1);
u8 b2 = crypto_input_shares[1]; add_timesample(b2);

u8 b1m1 = mult_log(b1, m1);     add_timesample(b1,m1);
u8 b2m1 = mult_log(b2, m1);     add_timesample(b2,m1);
u8 m2 = b1m1 ^ b2m1;            add_timesample(b1m1,b2m1);
```

0x31
0x9A
0xF5
0x319A
0x31F5
0x3FB5



- Replace regular probes with glitch-extended probes
- → TVLA to detect flaws
- Higher orders: ?

IDEA: GLITCH-EXTENDED PROBES

- Higher orders: concatenate extended probes
- → χ^2 test to detect flaws

```
u8 m1 = nonzero_rnd()&bitmask;  add_timesample(m1);
u8 b1 = crypto_input_shares[0]; add_timesample(b1);
u8 b2 = crypto_input_shares[1]; add_timesample(b2);

u8 b1m1 = mult_log(b1, m1);     add_timesample(b1,m1);
u8 b2m1 = mult_log(b2, m1);     add_timesample(b2,m1);
u8 m2 = b1m1 ^ b2m1;            add_timesample(b1m1,b2m1);
```

ESSENTIALLY:

$$I(\mathcal{R}\ ;\ x\ ) = 0$$

[BBF+18] Gilles Barthe, Sonia Belaïd, Pierre-Alain Fouque, Benjamin Grégoire: maskVerif: a formal tool for analyzing software and hardware masked implementations.IACR Cryptology ePrint Archive 2018: 562 (2018)

PROBING SECURITY WITH/WITHOUT GLITCHES

KU LEUVEN

PROBING SECURITY [GM10]

Given d wires $Q = (q_1, \ldots, q_d)$

$$I(Q ; x) = 0$$

[GM10] Berndt M. Gammel, Stefan Mangard: On the Duality of Probing and Fault Attacks. J. Electronic Testing 26(4): 483-493 (2010)

GLITCH-EXTENDED PROBING SECURITY

Given d wires $Q = (q_1, \ldots, q_d)$
with glitch-extended probes $\mathcal{R} = (\mathcal{R}_1, \ldots, \mathcal{R}_d)$

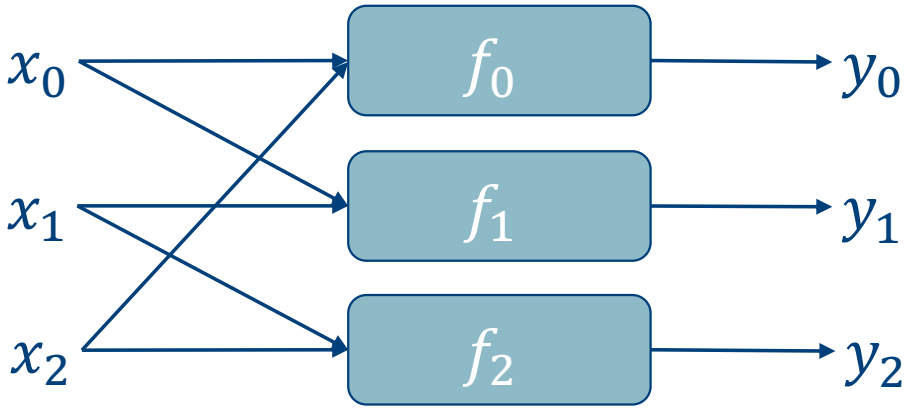
$$I(\mathcal{R}; x) = 0$$

Threshold Implementations

KU LEUVEN

Threshold Implementations [NRS11]

- Non-Completeness



- Uniformity

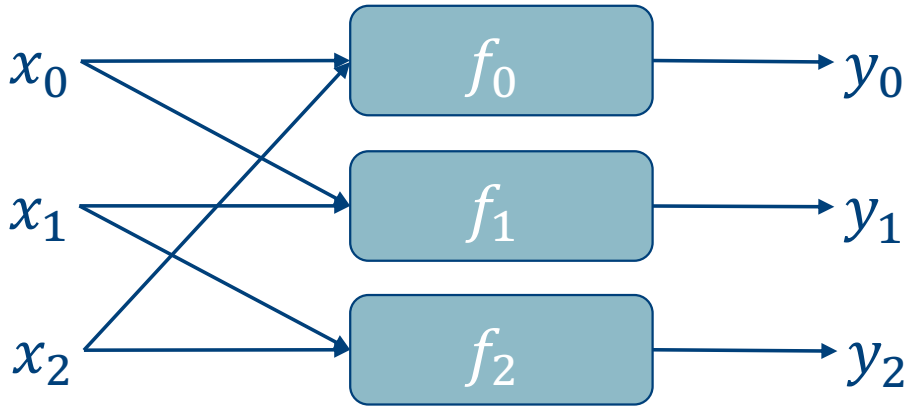
$\forall(x_0, x_1, x_2)$ s.t. $x_0 \oplus x_1 \oplus x_2 = x$:

$$\Pr[(x_0, x_1, x_2)|x] = p$$

[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)

Threshold Implementations [NRS11]

- Non-Completeness



- Uniformity

$\forall(x_0, x_1, x_2)$ s.t. $x_0 \oplus x_1 \oplus x_2 = x$:
$\Pr[(x_0, x_1, x_2)|x] = p$

1-Glitch Extended Probing Security

$I(\ \mathcal{R}\ ;\ x\ ) = 0$

(Not sufficient for higher-order probing security [RBN+15])

[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)
[RBN+15] Oscar Reparaz, Begül Bilgin, Svetla Nikova, Benedikt Gierlichs, Ingrid Verbauwhede: Consolidating Masking Schemes. CRYPTO (1) 2015: 764-783

Threshold Implementations [NRS11]

	Non-Completeness	Uniformity	$I(\mathcal{R}; x) = 0$
Sufficient	☹	☹	☺
Necessary	☺	☹	☺
Efficient Verification	☺ [ANR18]	☹	😐
Multi-variate	☹	☹	☺
Knowledge required	☹	☹	☺

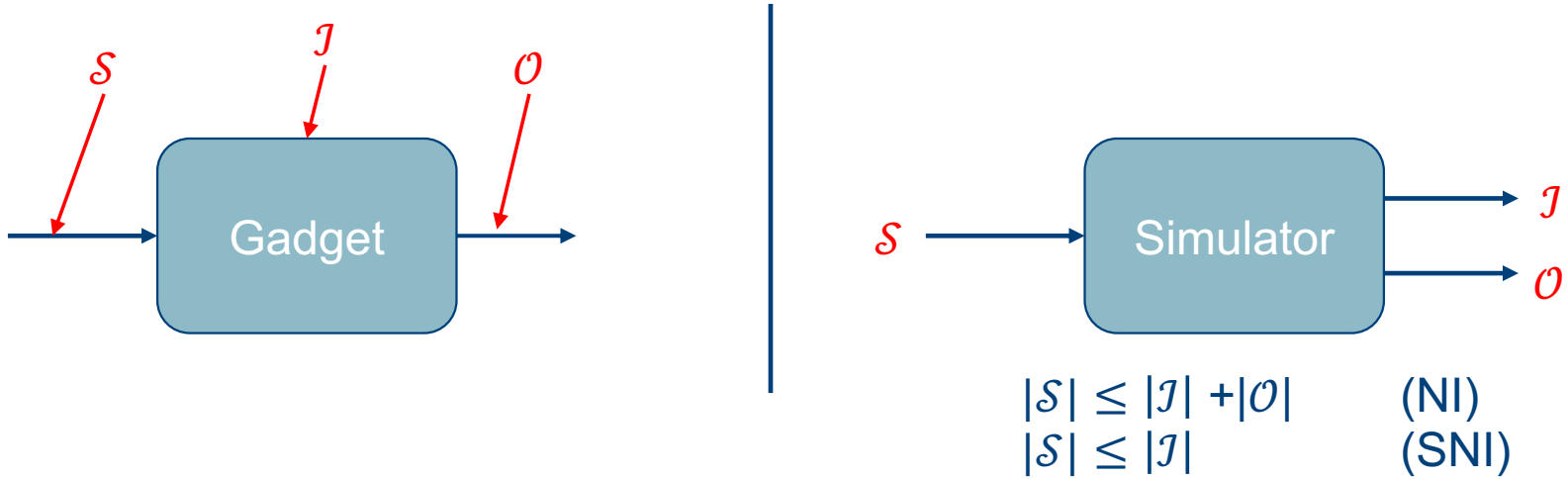
[NRS11] Svetla Nikova, Vincent Rijmen, Martin Schläffer: Secure Hardware Implementation of Nonlinear Functions in the Presence of Glitches. J. Cryptology 24(2): 292-321 (2011)
[ANR18] Victor Arribas, Svetla Nikova, Vincent Rijmen: VerMI: Verification Tool for Masked Implementations. ICECS 2018: 381-384

(STRONG) NON-INTERFERENCE

KU LEUVEN

(Strong) Non-Interference [BBD+16]

- Notions introduced for composable security
- More efficient verification (MaskVerif [BBF+18])
- Based on simulatability:

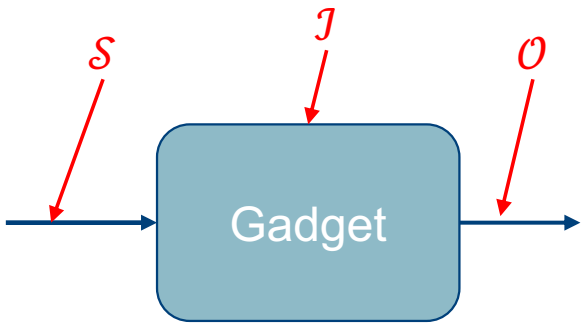


- Implies t-probing security

[BBD+16] Gilles Barthe, Sonia Belaïd, François Dupressoir, Pierre-Alain Fouque, Benjamin Grégoire, Pierre-Yves Strub, Rébecca Zucchini: Strong Non-Interference and Type-Directed Higher-Order Masking. ACM Conference on Computer and Communications Security 2016: 116-129
[BBF+18] Gilles Barthe, Sonia Belaïd, Pierre-Alain Fouque, Benjamin Grégoire: maskVerif: a formal tool for analyzing software and hardware masked implementations.IACR Cryptology ePrint Archive 2018: 562 (2018)

(Strong) Non-Interference [BBD+16]

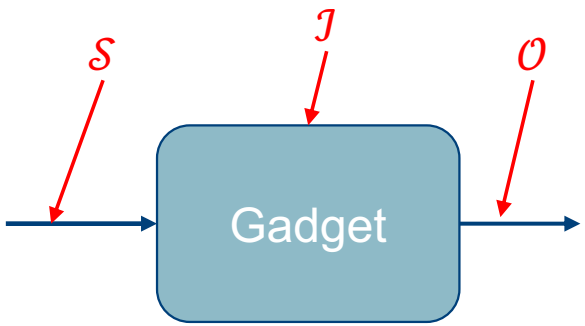
- Originally without glitches
- Extended by robust probing model [FGD+18]
- Unify with mutual information framework:



[FGD+18] Sebastian Faust, Vincent Grosso, Santos Merino Del Pozo, Clara Paglialonga, François-Xavier Standaert: Composable Masking Schemes in the Presence of Physical Defaults & the Robust Probing Model. IACR Trans. Cryptogr. Hardw. Embed. Syst. 2018(3): 89-120 (2018)

(Strong) Non-Interference [BBD+16]

- Originally without glitches
- Extended by robust probing model [FGD+18]
- Unify with mutual information framework:

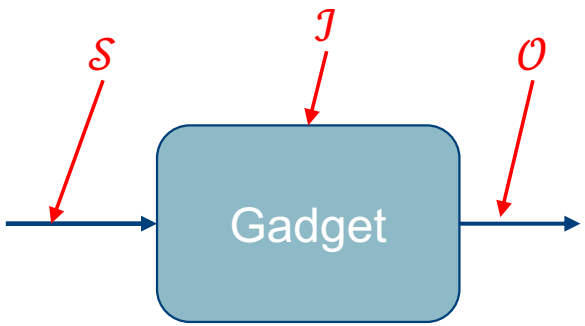


$$I\left((\mathcal{I},\mathcal{O});\boldsymbol{x}_{\bar{\mathcal{S}}}\,\middle|\,\boldsymbol{x}_{\mathcal{S}}\right)=0$$

[FGD+18] Sebastian Faust, Vincent Grosso, Santos Merino Del Pozo, Clara Paglialonga, François-Xavier Standaert: Composable Masking Schemes in the Presence of Physical Defaults & the Robust Probing Model. IACR Trans. Cryptogr. Hardw. Embed. Syst. 2018(3): 89-120 (2018)

(Strong) Non-Interference [BBD+16]

- Originally without glitches
- Extended by robust probing model [FGD+18]
- Unify with mutual information framework:



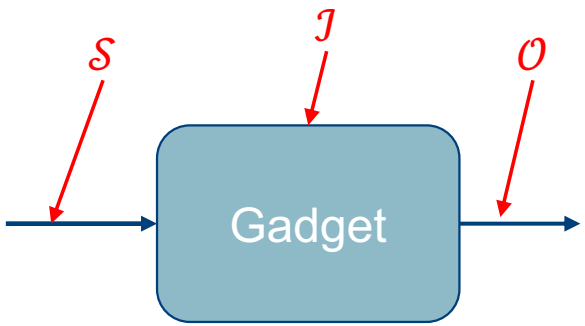
$$I\left((\mathcal{I},\mathcal{O});\boldsymbol{x}_{\bar{\mathcal{S}}}\,\middle|\,\boldsymbol{x}_{\mathcal{S}}\right)=0$$

  - Example: output probes & SNI: $|\mathcal{S}|=0 \Rightarrow I(\mathcal{O};\boldsymbol{x})=0$

[FGD+18] Sebastian Faust, Vincent Grosso, Santos Merino Del Pozo, Clara Paglialonga, François-Xavier Standaert: Composable Masking Schemes in the Presence of Physical Defaults & the Robust Probing Model. IACR Trans. Cryptogr. Hardw. Embed. Syst. 2018(3): 89-120 (2018)

(Strong) Non-Interference [BBD+16]

- Originally without glitches
- Extended by robust probing model [FGD+18]
- Unify with mutual information framework:



$$I\left((\mathcal{I},\mathcal{O});\boldsymbol{x}_{\bar{\mathcal{S}}}\,\middle|\,\boldsymbol{x}_{\mathcal{S}}\right)=0$$

  - Example: output probes & SNI: $|\mathcal{S}|=0 \Rightarrow I(\mathcal{O};\boldsymbol{x})=0$

- Glitches?→ replace probes with glitch-extended probes

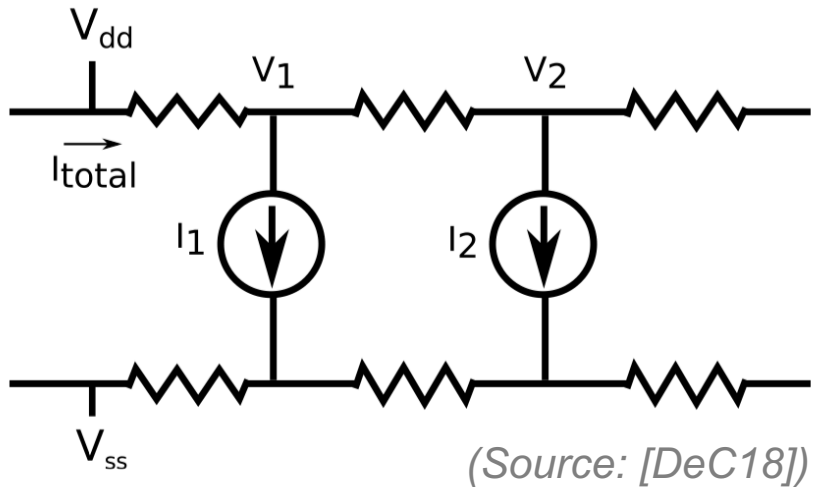
[FGD+18] Sebastian Faust, Vincent Grosso, Santos Merino Del Pozo, Clara Paglialonga, François-Xavier Standaert: Composable Masking Schemes in the Presence of Physical Defaults & the Robust Probing Model. IACR Trans. Cryptogr. Hardw. Embed. Syst. 2018(3): 89-120 (2018)

EXTENDING THE MODELS

KU LEUVEN

Beyond Glitches

- Gap between theory and practice
  - Coupling [DEM18]
  - CPU leaks [PV17]
  - …
- Robust Probing Model [FGD+18]
- In the same framework: $I(\ ;\ ) = 0$
  - New probe definitions: X-extended probes
  - Same tools!!



(Source: [DeC18])

[DEM18] Thomas De Cnudde, Maik Ender, Amir Moradi: Hardware Masking, Revisited. IACR Trans. Cryptogr. Hardw. Embed. Syst. 2018(2): 123-148 (2018)
[DeC18] T. De Cnudde: Cryptography Secured Against Side-Channel Attacks. PhD thesis, KU Leuven, S. Nikova, and V. Rijmen (promotors): 168 pages (2018)
[PV17] Kostas Papagiannopoulos, Nikita Veshchikov: Mind the Gap: Towards Secure 1st-Order Masking in Software. COSADE 2017: 282-297
[FGD+18] Sebastian Faust, Vincent Grosso, Santos Merino Del Pozo, Clara Paglialonga, François-Xavier Standaert: Composable Masking Schemes in the Presence of Physical Defaults & the Robust Probing Model. IACR Trans. Cryptogr. Hardw. Embed. Syst. 2018(3): 89-120 (2018)

Advantages

$$I(\ ;\ ) = 0$$

- Simple
  - No difference uni-variate or multi-variate
  - No knowledge required on variables
- Any type of masking (Boolean, multiplicative, arithmetic, …)
- Non-uniformity possible (low entropy masking)
- Versatile
  - Probing/NI/SNI
  - Different models (X-extended probes)
  - Information-theoretic vs practical security (noiseless TVLA)
  - Leakage functions (identity, Hamming, …)

CONCLUSION

consolidate verb

con·sol·i·date | \ kən-ˈsä-lə-ˌdāt \

consolidated; **consolidating**

Definition of *consolidate*

transitive verb

1 : to join together into one whole : UNITE
// *consolidate* several small school districts

2 : to make firm or secure : STRENGTHEN
// *consolidate* their hold on first place
// He *consolidated* his position as head of the political party.

[MW] https://www.merriam-webster.com/dictionary/consolidate

Thank You

KU LEUVEN