Let's Tessellate: Tiling for Security Against Advanced Probe and Fault Adversaries

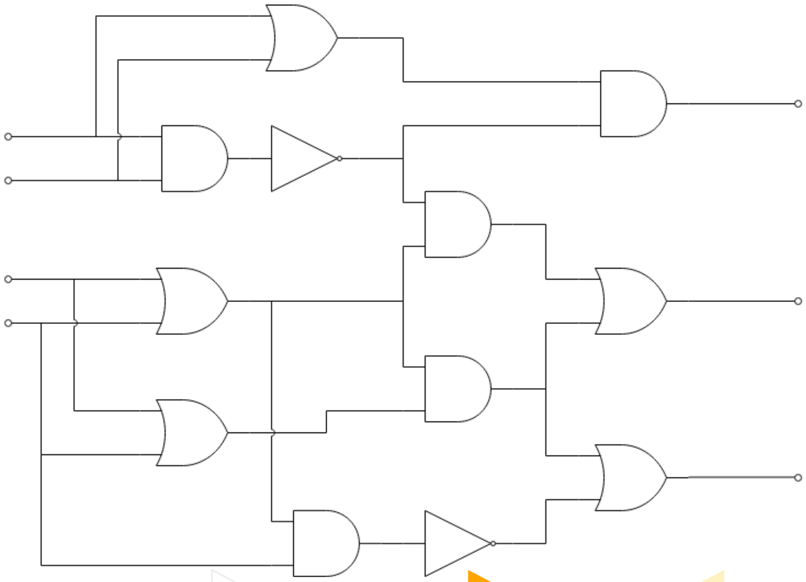
Joint work with

Siemen Dhooghe and Svetla Nikova

Security models: what do we need?

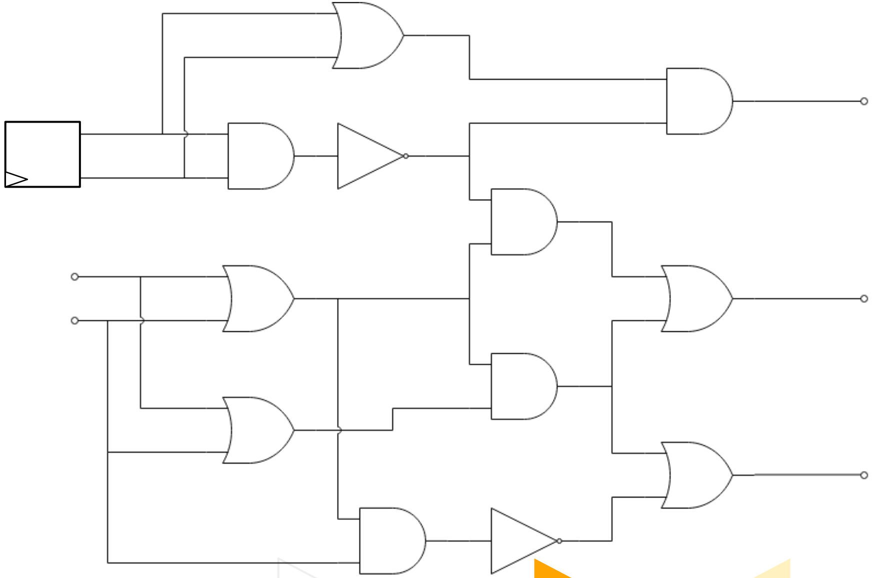
- Easy verification: composable security
- Capture of leakage effects
- Allows for efficient countermeasures

Probe Model



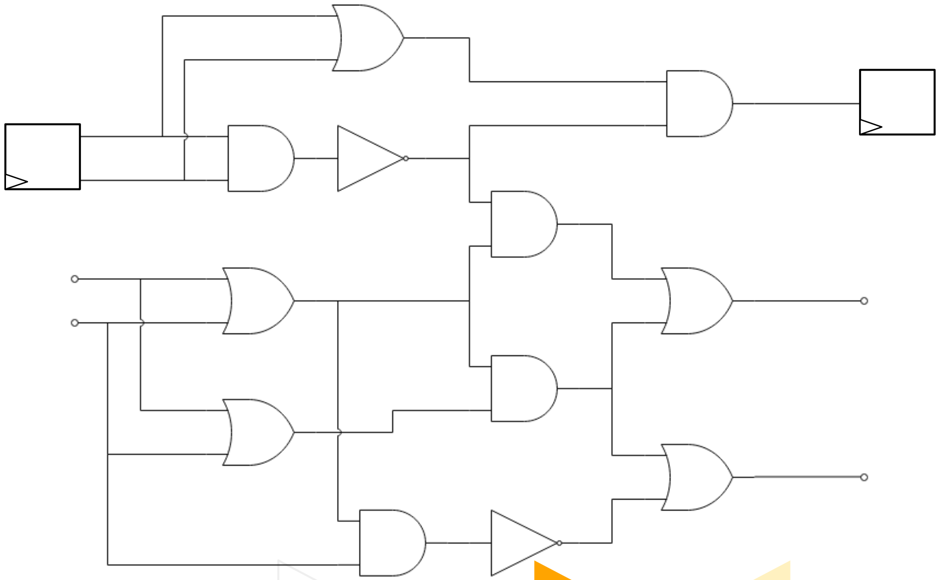
* Private Circuits: Securing Hardware against Probing Attacks: Yuval Ishai, Amit Sahai, David Wagner

Robust Probe Model: Glitches



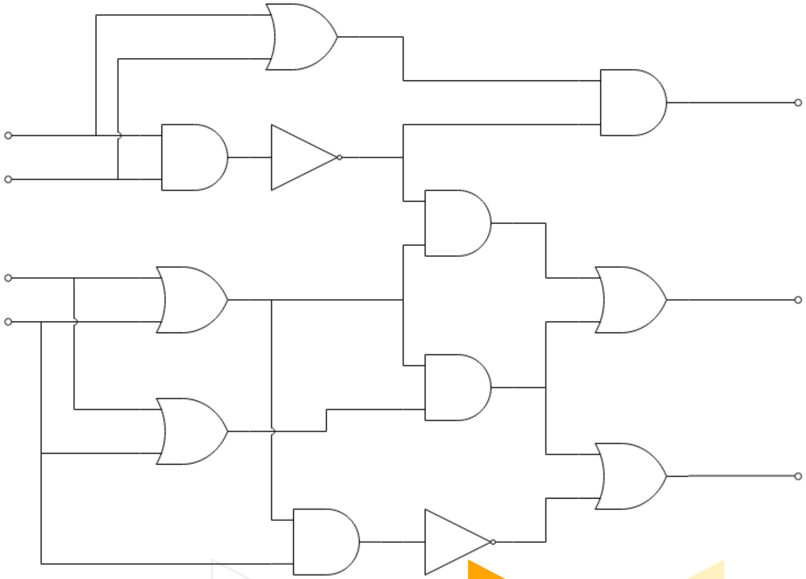
* Composable Masking Schemes in the Presence of Physical Defaults and the Robust Probing Model, Sebastian Faust, Vincent Grosso, Santos Merino Del Pozo, Clara Paglialonga, François-Xavier Standaert

Robust Probe Model: Transitions



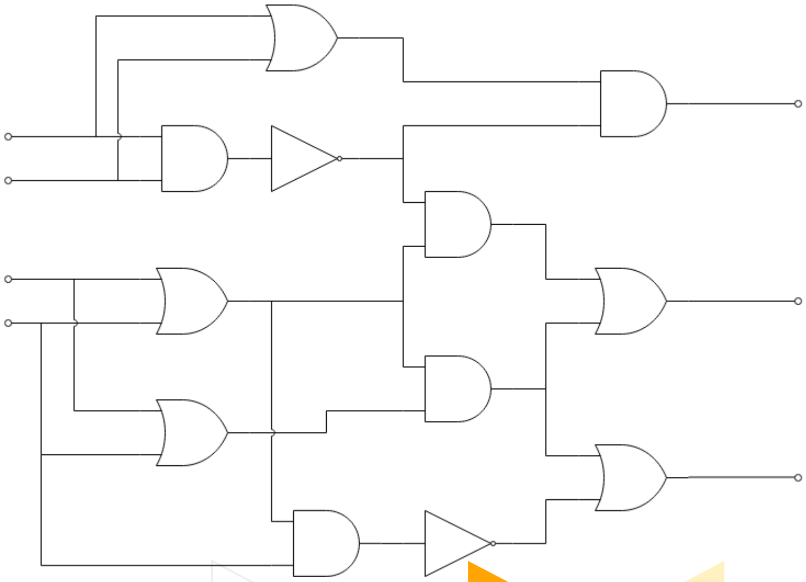
* Composable Masking Schemes in the Presence of Physical Defaults and the Robust Probing Model, Sebastian Faust, Vincent Grosso, Santos Merino Del Pozo, Clara Paglialonga, François-Xavier Standaert

Robust Probe Model: Couplings

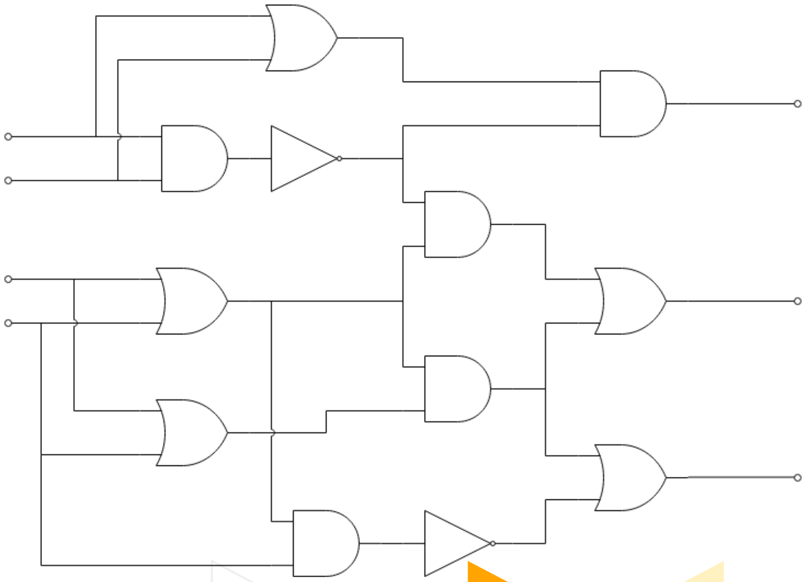


* Composable Masking Schemes in the Presence of Physical Defaults and the Robust Probing Model, Sebastian Faust, Vincent Grosso, Santos Merino Del Pozo, Clara Paglialonga, François-Xavier Standaert

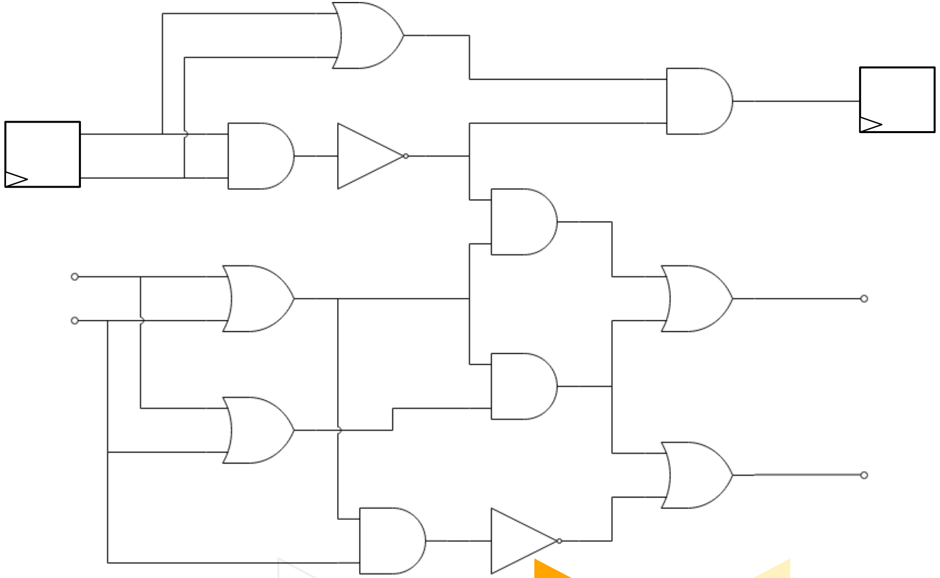
Wire Fault Model



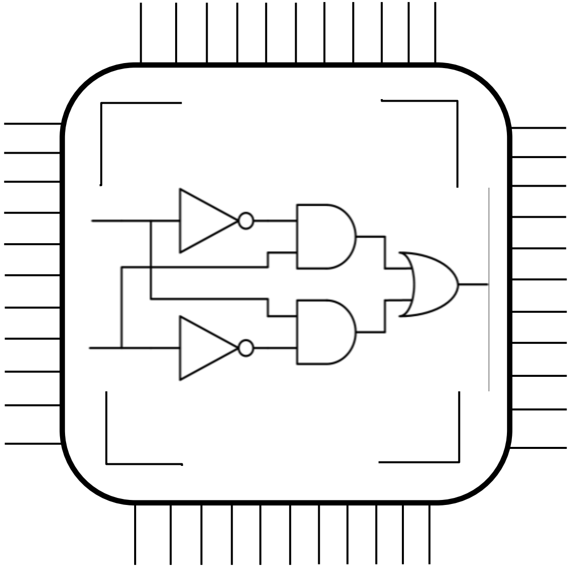
Extended Fault Model: Area Faults



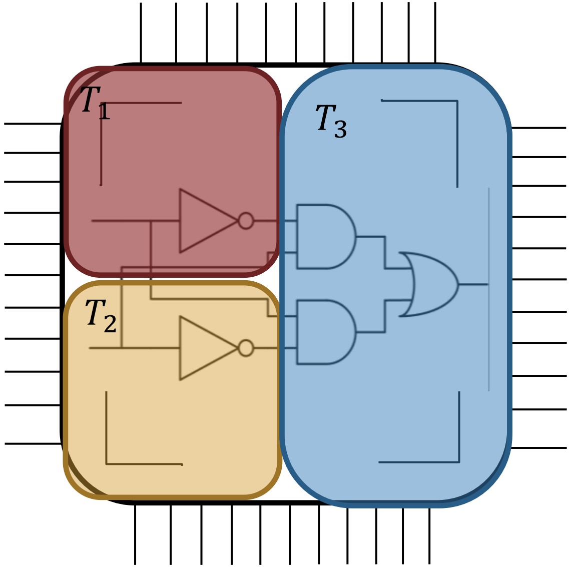
Extended Fault Model: Permanent Faults



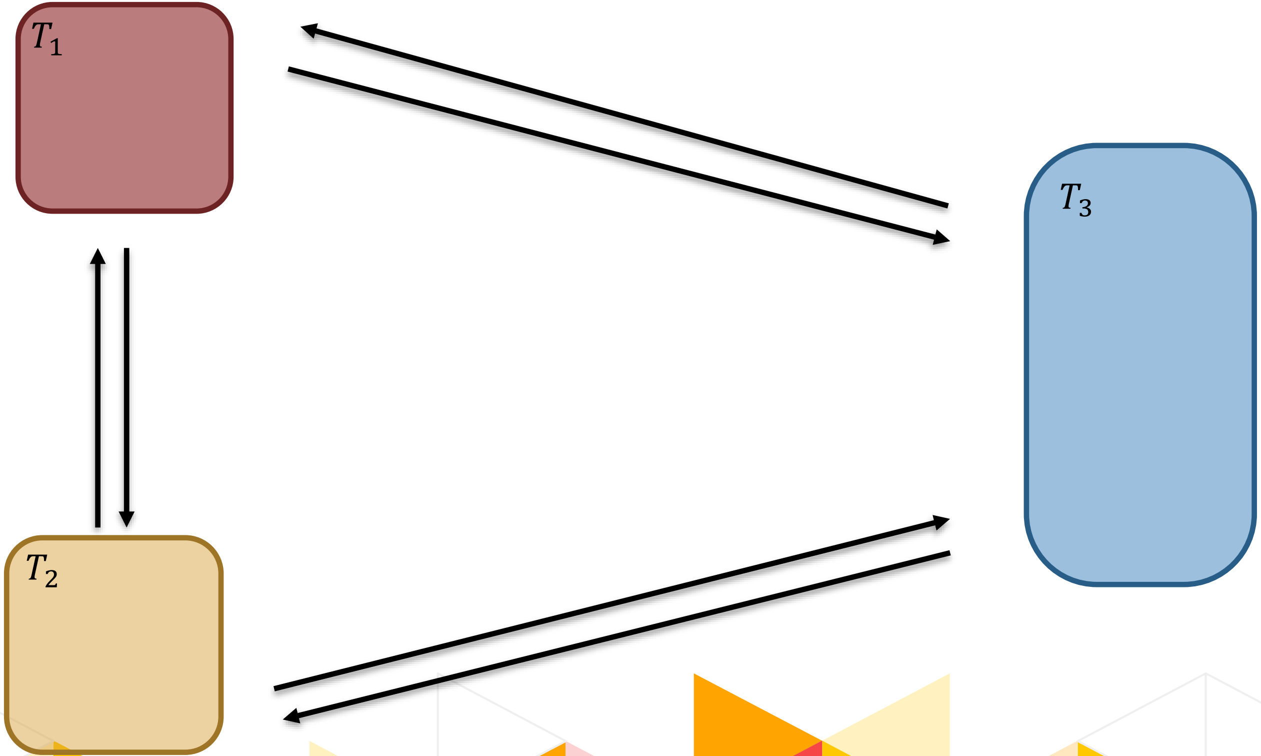
Tile Model and CAPA



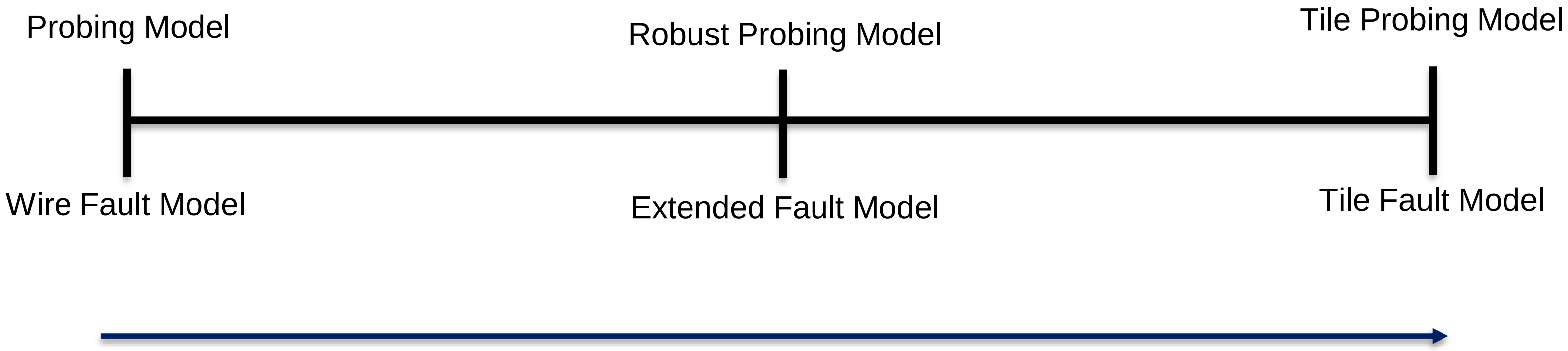
Tile Model and CAPA



Tile Model and CAPA



Relation Between Probe and Fault Models



Probing Model

Robust Probing Model

Tile Probing Model

Wire Fault Model

Extended Fault Model

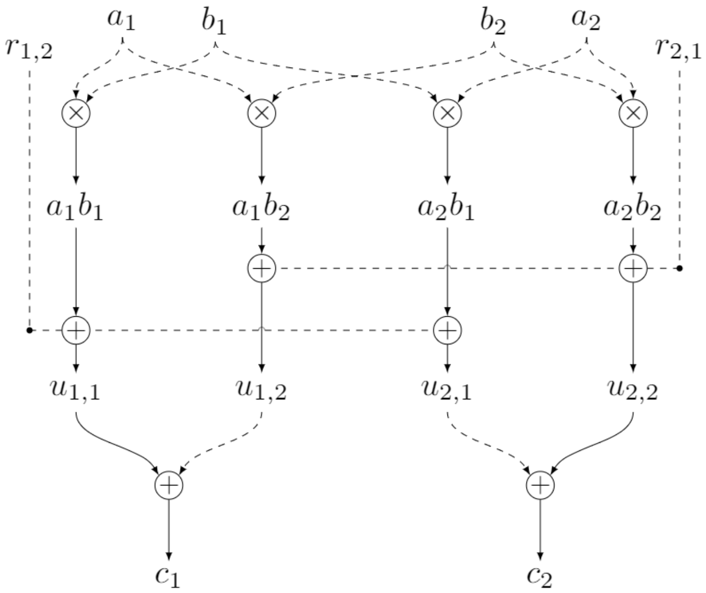
Tile Fault Model

Stronger Model:
Providing security against more leakage effects

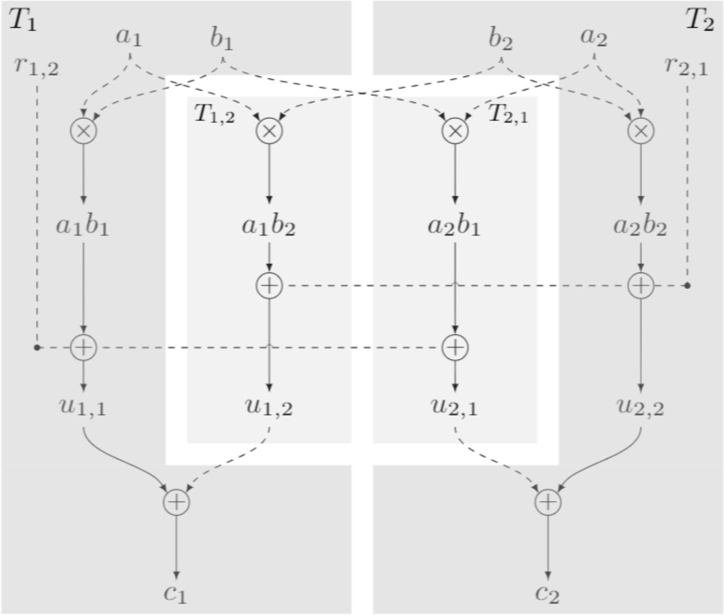
Comparing Compositional Notions
# shares/duplicates required for (d,k)th-order security

	NI & NA	Standalone
Glitches	d+1	d+1
Transitions	2d+1	d+1
Couplings	d+1	d+1
Area Faults	k+1	k+1
Permanent Faults	2k+1	k+1

A Tiled ISW Method



A Tiled ISW Method



Some Numbers

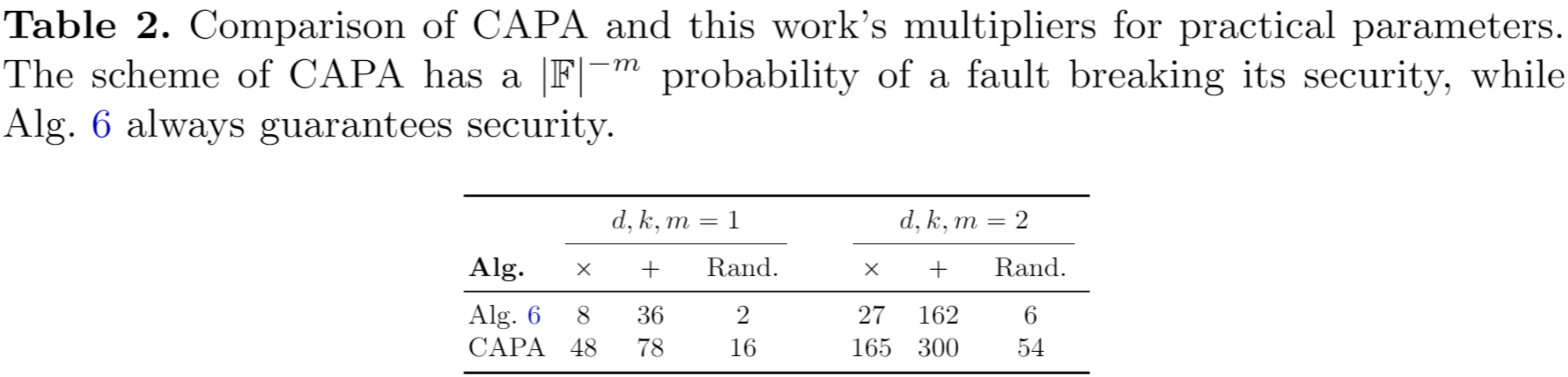


Table 2. Comparison of CAPA and this work's multipliers for practical parameters. The scheme of CAPA has a $|\mathbb{F}|^{-m}$ probability of a fault breaking its security, while Alg. 6 always guarantees security.

	$d, k, m = 1$			$d, k, m = 2$		
Alg.	×	+	Rand.	×	+	Rand.
Alg. 6	8	36	2	27	162	6
CAPA	48	78	16	165	300	54

* CAPA: The Spirit of Beaver Against Physical Attacks, Oscar Reparaz, Lauren De Meyer, Begül Bilgin, Victor Arribas, Svetla Nikova, Ventzislav Nikov, Nigel P. Smart

Conclusion

- Extension of the fault model
- Comparison with the tile model
- Proposal of tiled ISW method

Thanks!