A Survey of Combined Countermeasures against Passive and Active SCAs

Weijia Wang

Outline

- Backgrounds
- Problem description
- Security models
  - State-of-the-arts
  - Challenges
- Schemes
  - State-of-the-arts
  - Challenges

Backgrounds

- Passive side-channel attacks: Read ‘hidden’ signals
  - timing, power consumption, electromagnetic emission, …
  - masking (most investigated countermeasure) :
    - Sensitive variable *x* is encoded into *d* shares, and any d-1 shares are independent of x
- Active side-channel attacks: Insertion of faults
  - power glitches, laser, ...
- Combined side-channel attacks
  - Attackers have the ability to mount both passive and active attacks

Problem description

- How to defend against the passive and active attacks:
  - Focus:
    - Protection of the algorithm (without relying on e.g. shields or detectors on the chip)
    - In a formal security model
  - Only masking does not work (and even enlarge the attack surface to insert a fault in the computation)

Security Models

Security models: state-of-the-arts

Active \ Passive		Probing security		Tile-probe-and-fault-model (MPC)
		SW.	HD.	
Fault coverage (detectable faults number / possible faults number)			[SMG16]	
k-order active secure	**Reset attacks**	[IPS06]		
	General attacks	[IPS06] [DN19]		
Tile-probe-and-fault-model (MPC)				[RMB18]

[DN19] Dhooghe, S., Nikova, S. My Gadget Just Cares For Me-How NINA Can Prove Security Against Combined Attacks.. IACR Cryptology ePrint Archive, 2019

[RMB18] Reparaz, O., De Meyer, L., Bilgin, B., Arribas, V., Nikova, S., Nikov, V., Smart, N.. CAPA: the spirit of beaver against physical attacks. CRYPTO 2018.

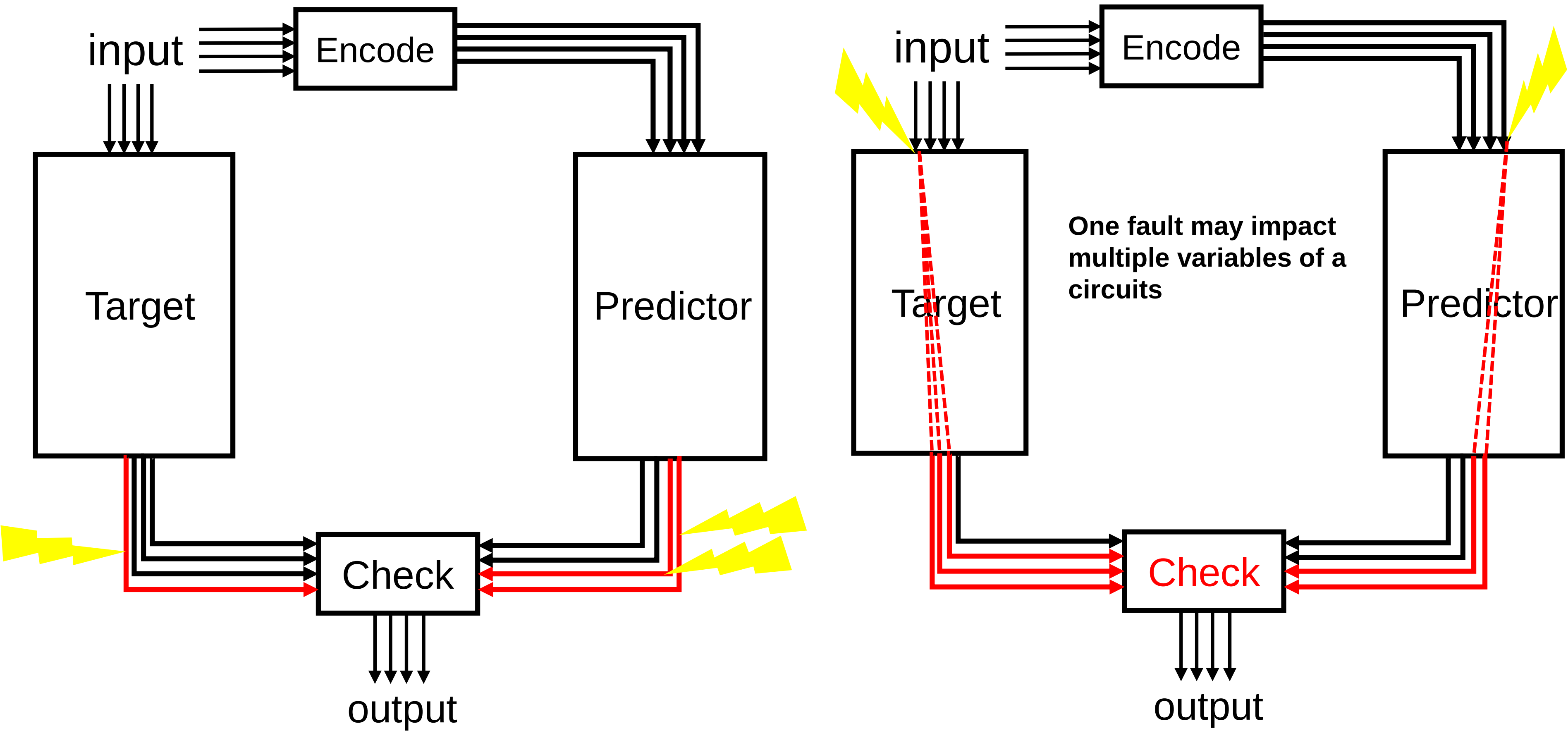
[IPS06] Ishai, Y., Prabhakaran, M., Sahai, A., & Wagner, D.. Private circuits II: keeping secrets in tamperable circuits. EUROCRYPT 2006

[SMG16] Schneider, T., Moradi, A., & Güneysu, T.. ParTI–towards combined hardware countermeasures against side-channel and fault-injection attacks. CRYPTO 2016.

[CN16] De Cnudde, T., Nikova, S.. More efficient private circuits II through threshold implementations. FTDC 2016.

Security models: state-of-the-arts

Composable security model for combined attacks
-- The issue of fault propagation



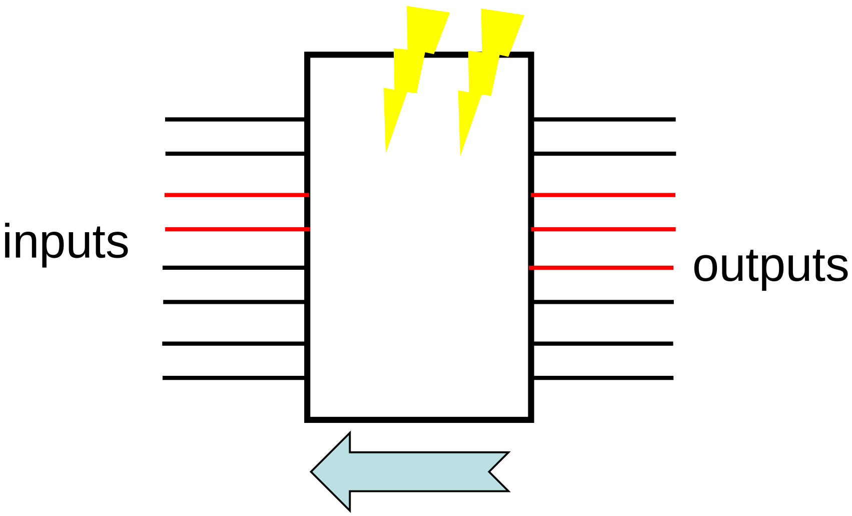
Basic Structure of code-based concurrent error detection schemes

Security models: state-of-the-arts

Composable security model for combined attacks [DN19]

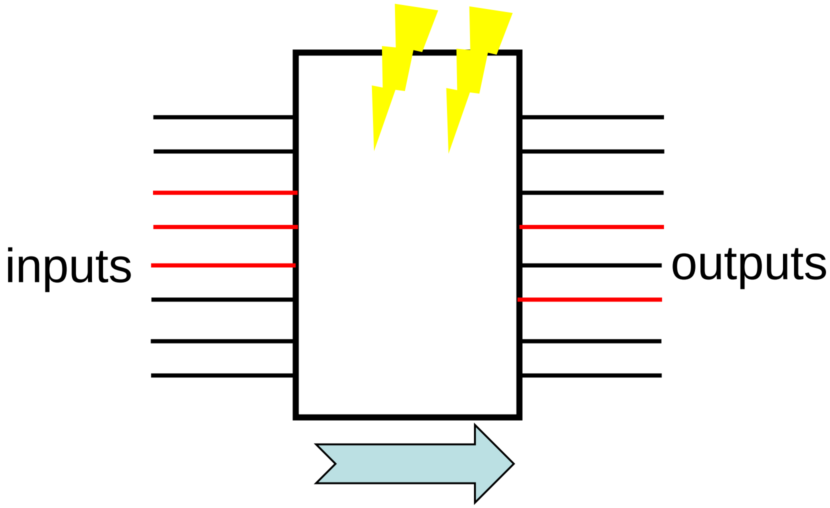
- Strong Non-Interference and Non-Accumulation (SNINA) = SNI + SNA

Two probes



Strong Non-Inference (SNI)

Two faults



Strong Non-Accumulative (SNA)

Security models: challenges

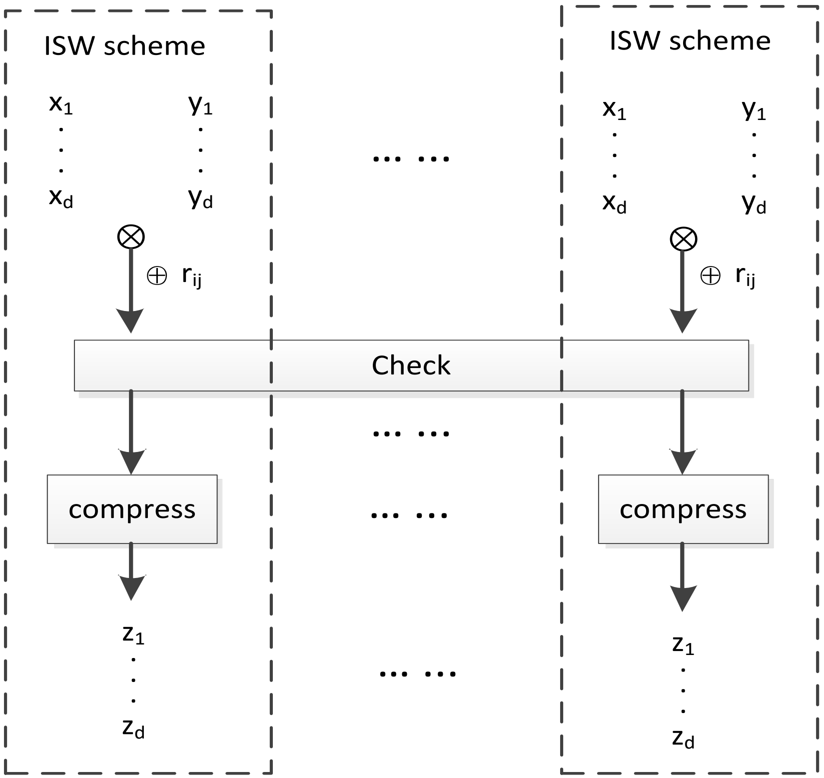
- Challenges are mainly on active security
  - What type of security we need for active attacks?
    - Fault coverage? k order fault security? or in between?
    - It is important to realistically estimate the power of potential FI attackers
  - Composable combined security model
    - Formal verification
    - More efficient

Schemes

Schemes: state-of-the-arts

Duplicated Boolean masking [IPS06] [DN19]

- This scheme is secure in SNINA
- But suffers from symmetric errors
- Complexity for the multiplication:
  - Computation: $O(kd^2)$
  - Randomness: $d^2/2$
    - k: fault security order
    - d: probing security order



[IPS06] Ishai, Y., Prabhakaran, M., Sahai, A., & Wagner, D.. Private circuits II: keeping secrets in tamperable circuits. EUROCRYPT 2006

[DN19] Dhooghe, S., Nikova, S. My Gadget Just Cares For Me-How NINA Can Prove Security Against Combined Attacks.. IACR Cryptology ePrint Archive, 2019

Schemes: state-of-the-arts

Combined secure polynomial masking [DN19]

- Based on polynomial masking
- Needs (k+d+1) shares for d and k orders security for passive and active attacks (better than duplication)
- This scheme is secure in SNINA
- Complexity for the multiplication: $O((k+d)^2)$
  - For both computation and randomness

[DN19] Dhooghe, S., Nikova, S. My Gadget Just Cares For Me-How NINA Can Prove Security Against Combined Attacks.. IACR Cryptology ePrint Archive, 2019

Schemes: state-of-the-arts

ParTI [SMG16]

- Hardware
  - First-order secure Threshold Implementation (TI)
  - Code-based concurrent error detection scheme
    - The fault security is assessed by fault coverage
    - Suffer from the fault propagation issue
- LED instance: 12% bigger of area than TI + simple duplication
- Leaving out a formal adversary model

[SMG16] Schneider, T., Moradi, A., & Güneysu, T.. ParTI–towards combined hardware countermeasures against side-channel and fault-injection attacks. CRYPTO 2016.

Schemes: state-of-the-arts

CAPA [RMB18]

- Draws inspiration from MPC protocol SPDZ
- More secure: all the wires in a partition can be probed and fault
- Both software and hardware
- Cost: heavy (for both computation and randomness)

- Recent improvement: M & M [MAN19]
  - More efficient
  - Leaving out the high security property

[RMB18] Reparaz, O., De Meyer, L., Bilgin, B., Arribas, V., Nikova, S., Nikov, V., Smart, N.. CAPA: the spirit of beaver against physical attacks. CRYPTO 2018.

[MAN19] De Meyer, L., Arribas, V., Nikova, S., Nikov, V., & Rijmen, V.. M&M: Masks and Macs against physical attacks. CHES 2019.

Schemes: challenges

- How to improve the efficiency (without degrading the security)?
  - Randomness Complexity
  - Computational Complexity
- Mode of operation: leakage + fault resilient?

Thanks for your attention

Q & A ?