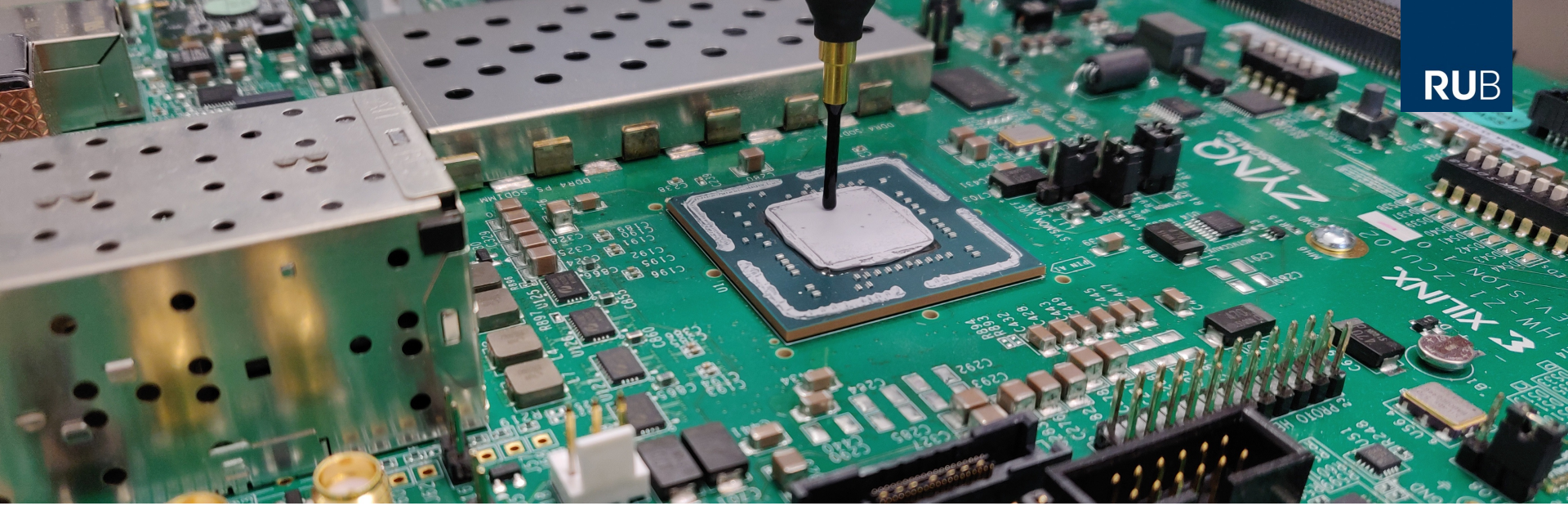


RUHR-UNIVERSITÄT BOCHUM

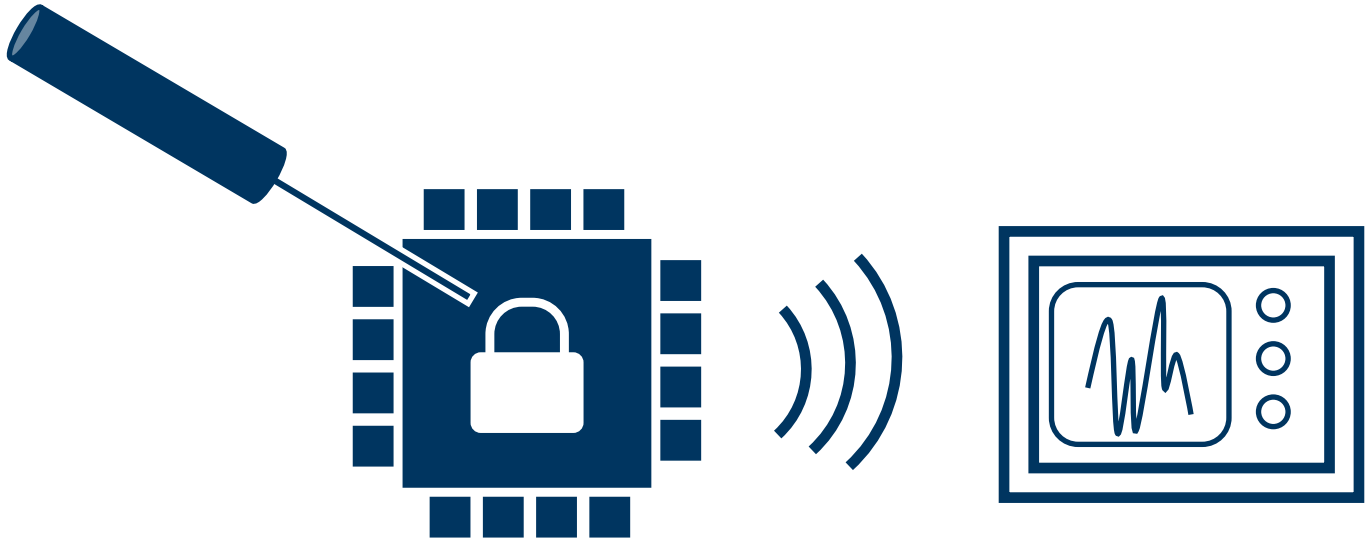
Computer-Aided Verification of Countermeasures against Physical Attacks

Jan Richter-Brockmann, Jakob Feldtkeller, Pascal Sasdrich, Tim Güneysu

Chair for Security Engineering
Faculty of Computer Science
Ruhr University Bochum

16. Januar 2025

Physical Attacks

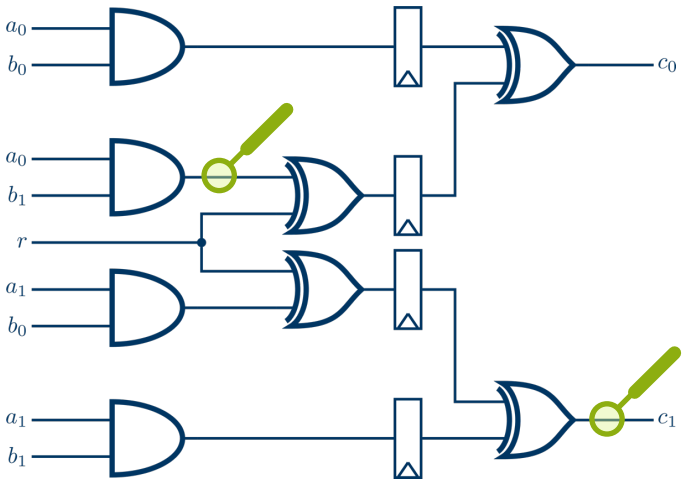


Fault-Injection Attacks

Side-Channel Attacks

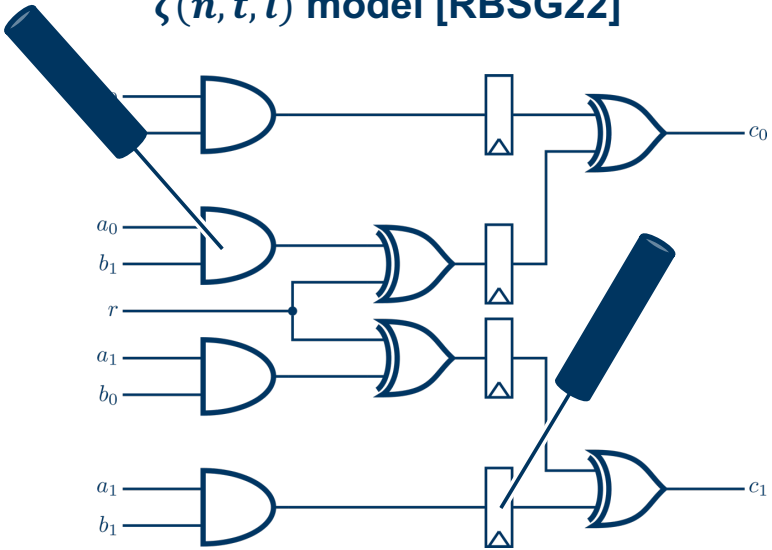
Model Physical Attacks

d-probing model [ISW03]



An adversary is given the exact values of up to d wires of a circuit C.

$\zeta(n, t, l)$ model [RBSG22]



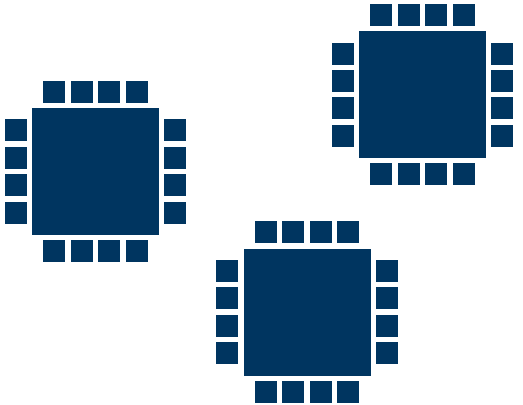
An adversary can inject up to n faults assuming a fault type t and locations l.

Countermeasures

Side-Channel Attacks

Masking

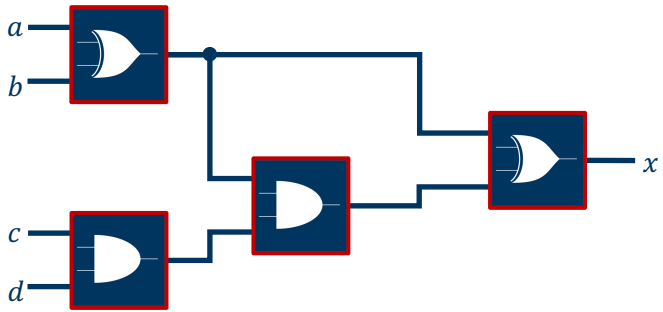
Fault-Injection Attacks

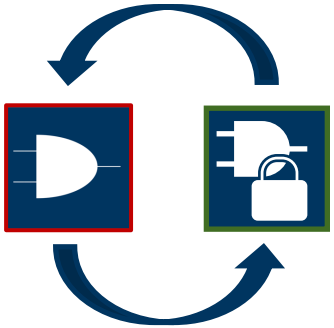


Redundancy

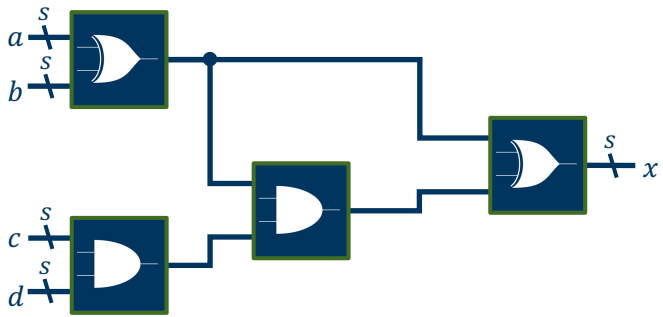
Secure Gadgets

Insecure Circuit





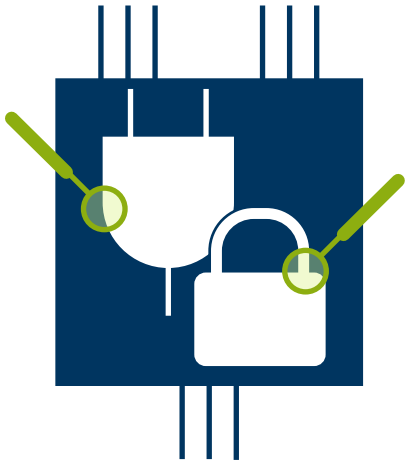
Protected Circuit



Composability Notions

RUB

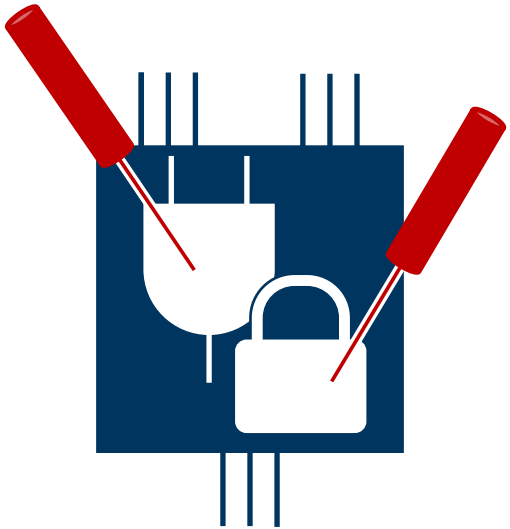
Side Channel



PNI, PSNI

PINI

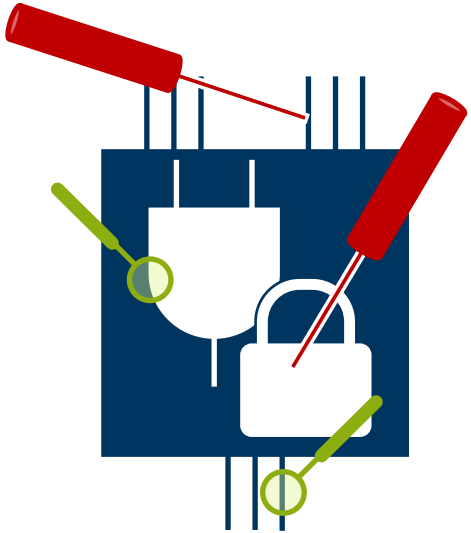
Fault Injection



FNI, FSNI

FINI

Combined



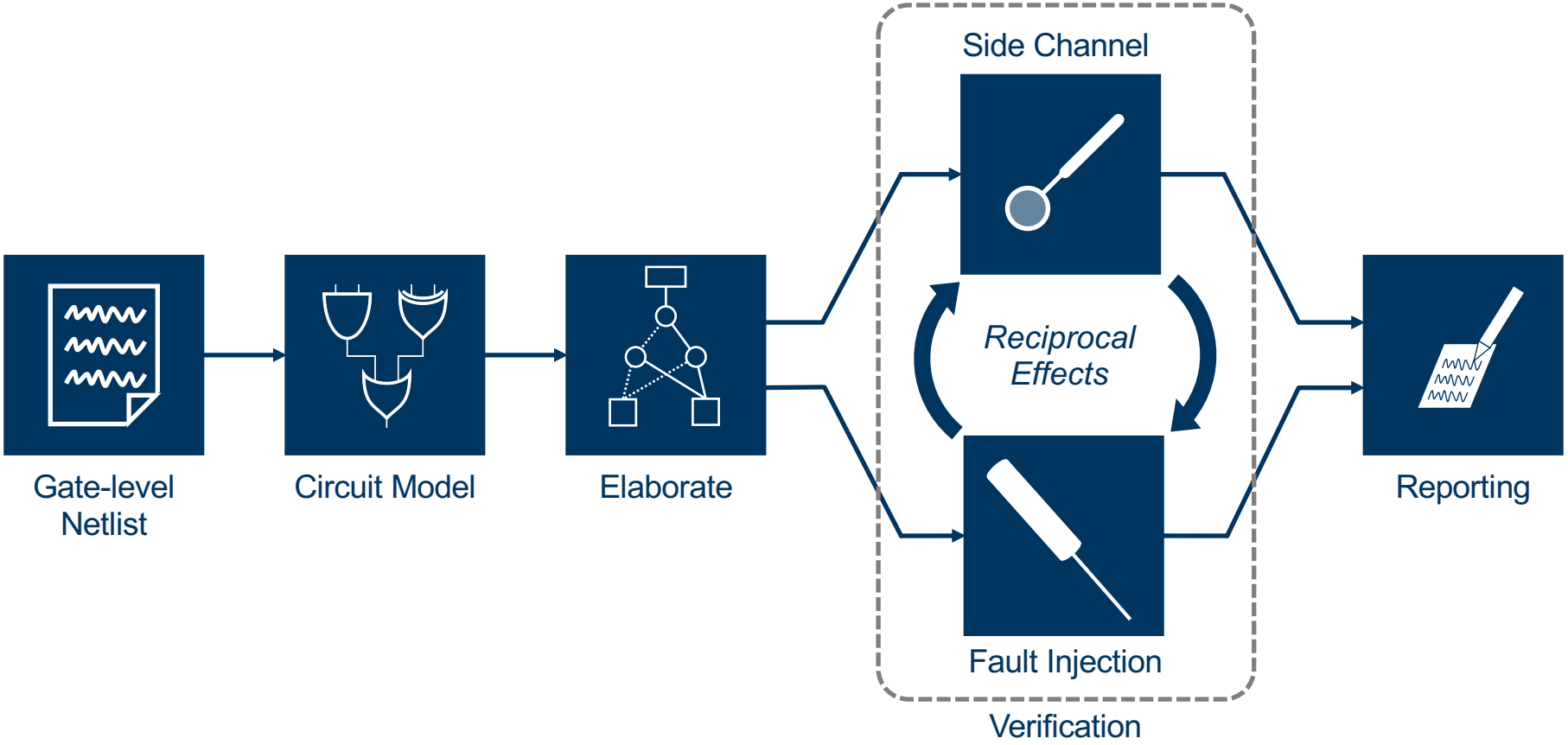
CNI, CSNI, ICSNI

CINI, ICINI

Research Questions

How to efficiently apply computer-aided verification to evaluate countermeasures against physical attacks?

Verification Concept



Verification of Countermeasures against Fault Injections [RBRSS+21]

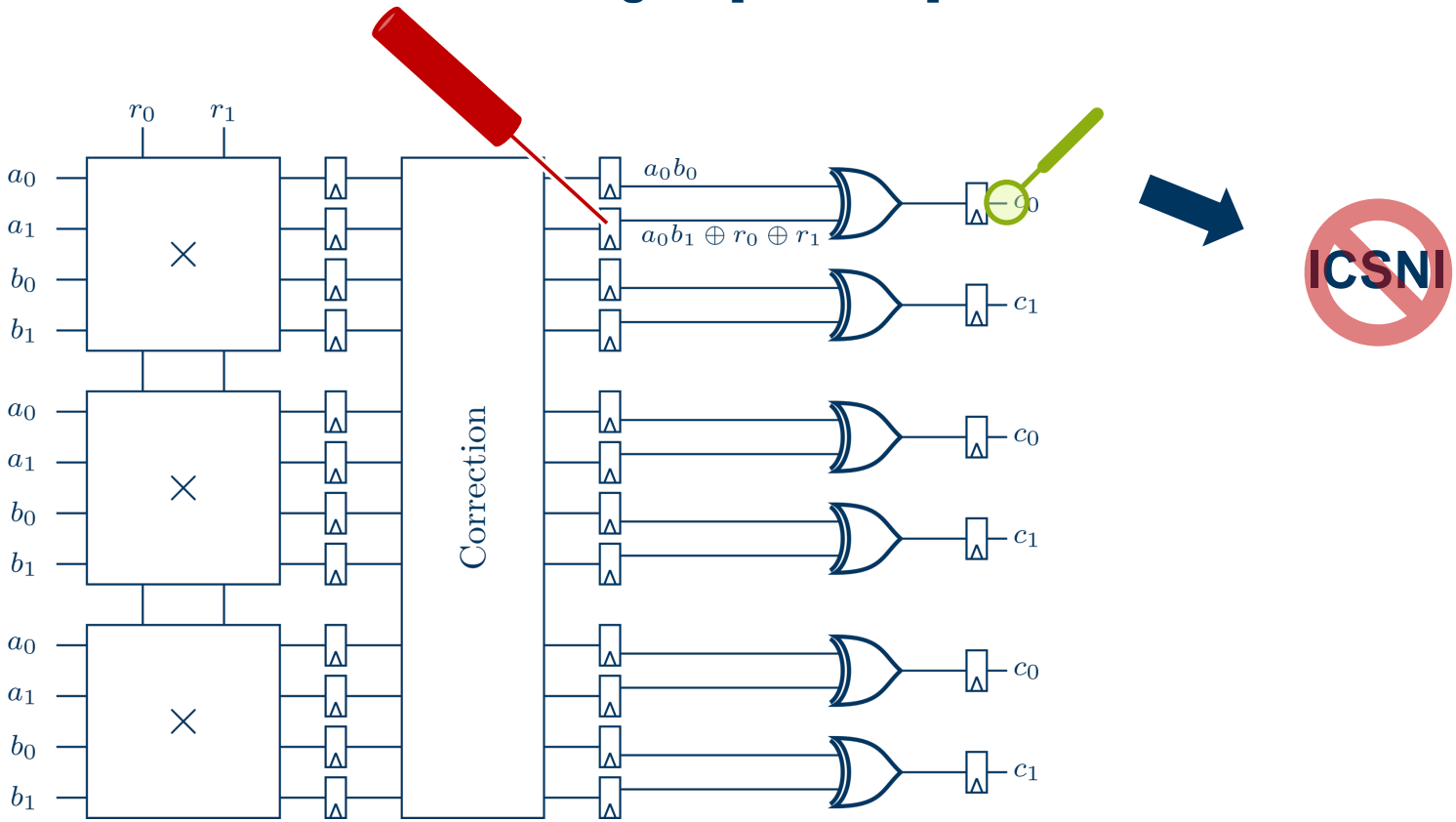
RUB

Single round of CRAFT protected by linear error correcting codes

$$t = \tau_{bf} \qquad l = \mathrm{mc}_{\infty}$$

1-bit Protection	2-bit Protection	3-bit Protection
 925	 1 490	 1 807
$\binom{n}{k}$ 766	$\binom{n}{k}$ 329 730	$\binom{n}{k}$ 91 737 144
 0.021 s	 1.496 s	 2 937 s

Verification of Combined Gadgets [RFSG22]

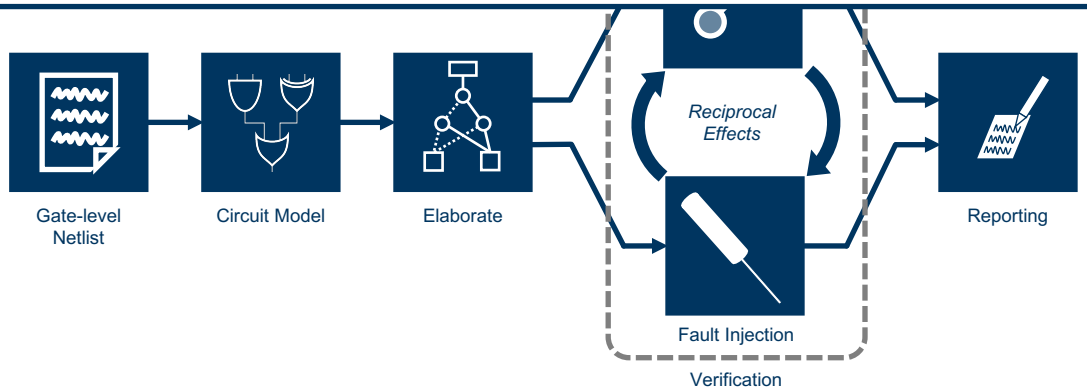


The gadget has been originally proposed in [DN20] and should be $(1,1)$-ICSNI.

Summary

Code and paper are publicly available

https://github.com/Chair-for-Security-Engineering/VERICA



Modeling of Physical Attacks

Verification of Countermeasures against Physical Attacks

RUB

Thank you!

jan.richter-brockmann@rub.de

HG SECURITY ENGINEERING

References

[BBD+15] Gilles Barthe, Sonia Belaïd, François Dupressoir, Pierre-Alain Fouque, Benjamin Grégoire, and Pierre-Yves Strub. *Verified Proofs of Higher-Order Masking.* In EUROCRYPT, pages 457–485, 2015.

[BBD+16] Gilles Barthe, Sonia Belaïd, François Dupressoir, Pierre-Alain Fouque, Benjamin Grégoire, Pierre-Yves Strub, and Rébecca Zucchini. *Strong Non-Interference and Type-Directed Higher-Order Masking.* In SIGSAC, pages 116–129, 2016.

[CS20] Gaetan Cassiers and Fran¸cois-Xavier Standaert. *Trivially and Efficiently Composing Masked Gadgets With Probe Isolating Non-Interference.* IEEE Trans. Inf. Forensics Secur., 15:2542–2555, 2020.

[DDE+20] Joan Daemen, Christoph Dobraunig, Maria Eichlseder, Hannes Groß, Florian Mendel, and Robert Primas. *Protecting against Statistical Ineffective Fault Attacks.* IACR Trans. Cryptogr. Hardw. Embed. Syst., 2020(3):508–543, 2020.

[DN20] Siemen Dhooghe and Svetla Nikova. *My Gadget Just Cares for Me – How NINA Can Prove Security Against Combined Attacks.* In CT-RSA, volume 12006 of Lecture Notes in Computer Science, pages 35–55. Springer, 2020.

[FGP+18] Sebastian Faust, Vincent Grosso, Santos Merino Del Pozo, Clara Paglialonga, and Fran¸cois-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.

[FRSG22] Jakob Feldtkeller, Jan Richter-Brockmann, Pascal Sasdrich, and Tim Güneysu. *CINI MINIS: Domain Isolation for Fault and Combined Security.* CCS, 2022

[HPB21] Vedad Hadzic, Robert Primas, and Roderick Bloem. *Proving SIFA protection of masked redundant circuits.* In Automated Technology for Verification and Analysis, volume 12971 of Lecture Notes in Computer Science, pages 249–265. Springer, 2021.

[ISW03] Yuval Ishai, Amit Sahai, and David A. Wagner. *Private Circuits: Securing Hardware against Probing Attacks.* In Dan Boneh, editor, CRYPTO, volume 2729 of Lecture Notes in Computer Science, pages 463–481. Springer, 2003.

[KSM20] David Knichel, Pascal Sasdrich, and Amir Moradi. *SILVER – Statistical Independence and Leakage Verification.* In ASIACRYPT, volume 12491 of Lecture Notes in Computer Science, pages 787–816. Springer, 2020.

[RBRSS+21] Jan Richter-Brockmann, Aein Rezaei Shahmirzadi, Pascal Sasdrich, Amir Moradi, and Tim Güneysu. *FIVER – Robust Verification of Countermeasures against Fault Injections.* IACR Trans. Cryptogr. Hardw. Embed. Syst., 2021(4):447–473, Aug. 2021.

[RBSG21] Jan Richter-Brockmann, Pascal Sasdrich, and Tim Güneysu. *Revisiting Fault Adversary Models - Hardware Faults in Theory and Practice.* Trans. On Computers, 2022

[RFSG22] Jan Richter-Brockmann, Jakob Feldtkeller, Pascal Sasdrich, and Tim G¨uneysu. VERICA - Verifi cation of Combined Attacks: Automated formal verification of security against simultaneous information leakage and tampering. IACR Trans. Cryptogr. Hardw. Embed. Syst. , 2022(4), 2022.

[SMG16] Tobias Schneider, Amir Moradi, and Tim Güneysu. *ParTI - Towards Combined Hardware Countermeasures Against Side-Channel and Fault-Injection Attacks.* In CRYPTO 2016, volume 9815 of Lecture Notes in Computer Science, pages 302–332. Springer, 2016.