CASA
CYBER SECURITY IN THE AGE OF LARGE-SCALE ADVERSARIES

Automated Generation and Evaluation of Masked Hardware

M. Sc. Nicolai Müller
Implementation Security Group
Ruhr University Bochum

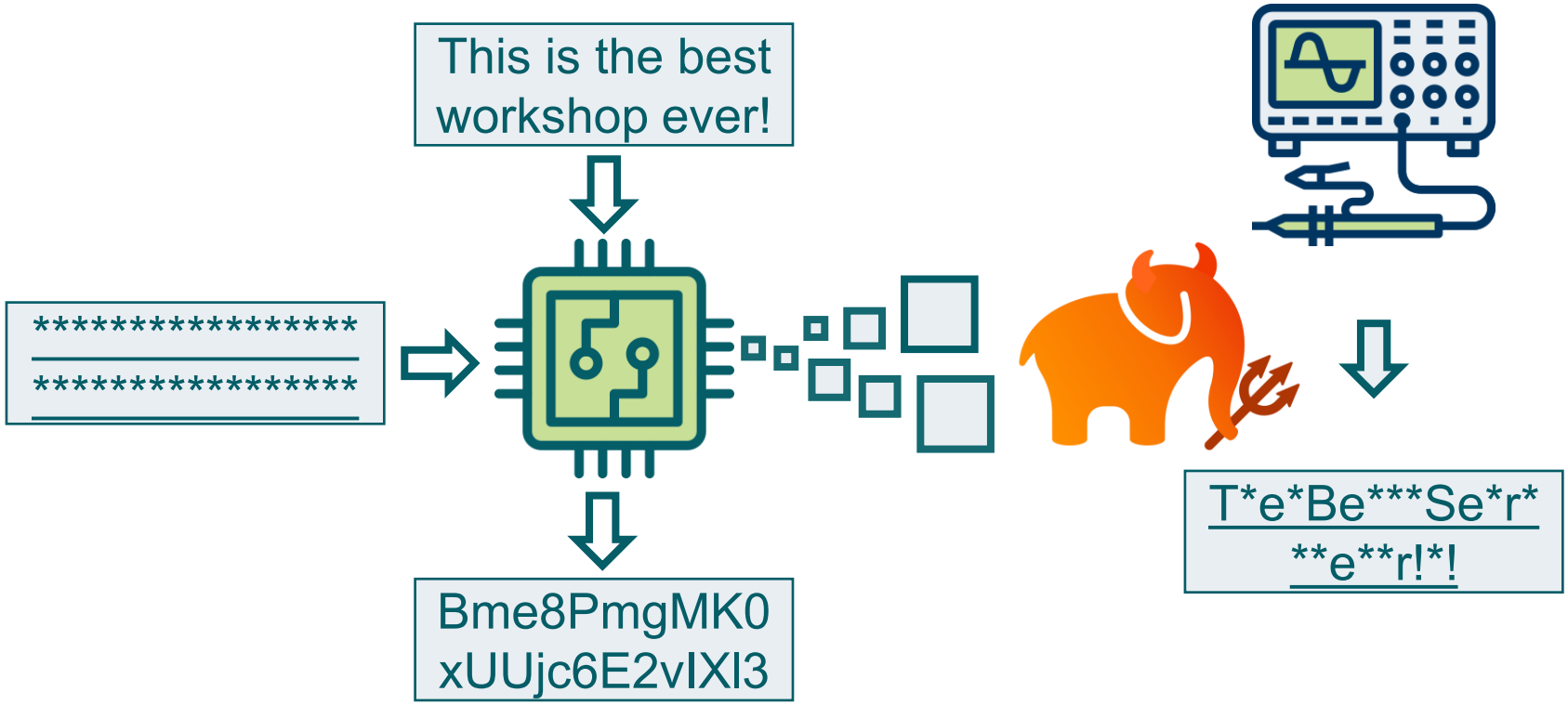
RUHR UNIVERSITÄT BOCHUM
RUB

Gefördert durch
DFG Deutsche Forschungsgemeinschaft

HGI HORST GÖRTZ INSTITUT

CASA
CYBER SECURITY IN THE AGE OF LARGE-SCALE ADVERSARIES

SIDE-CHANNEL ANALYSIS ATTACKS

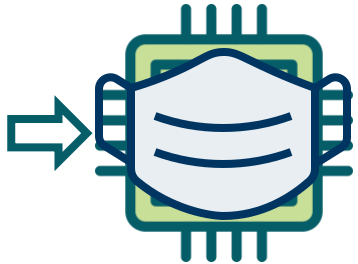


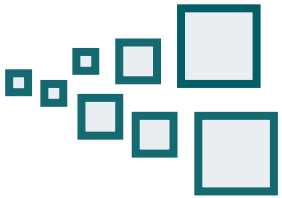
CASA
CYBER SECURITY IN THE AGE OF LARGE-SCALE ADVERSARIES

COUNTERMEASURES

$$x^0, \ldots, x^d$$
$$x = x^0 \oplus \cdots \oplus x^d$$

$$k^0, \ldots, k^d$$
$$k = k^0 \oplus \cdots \oplus k^d$$



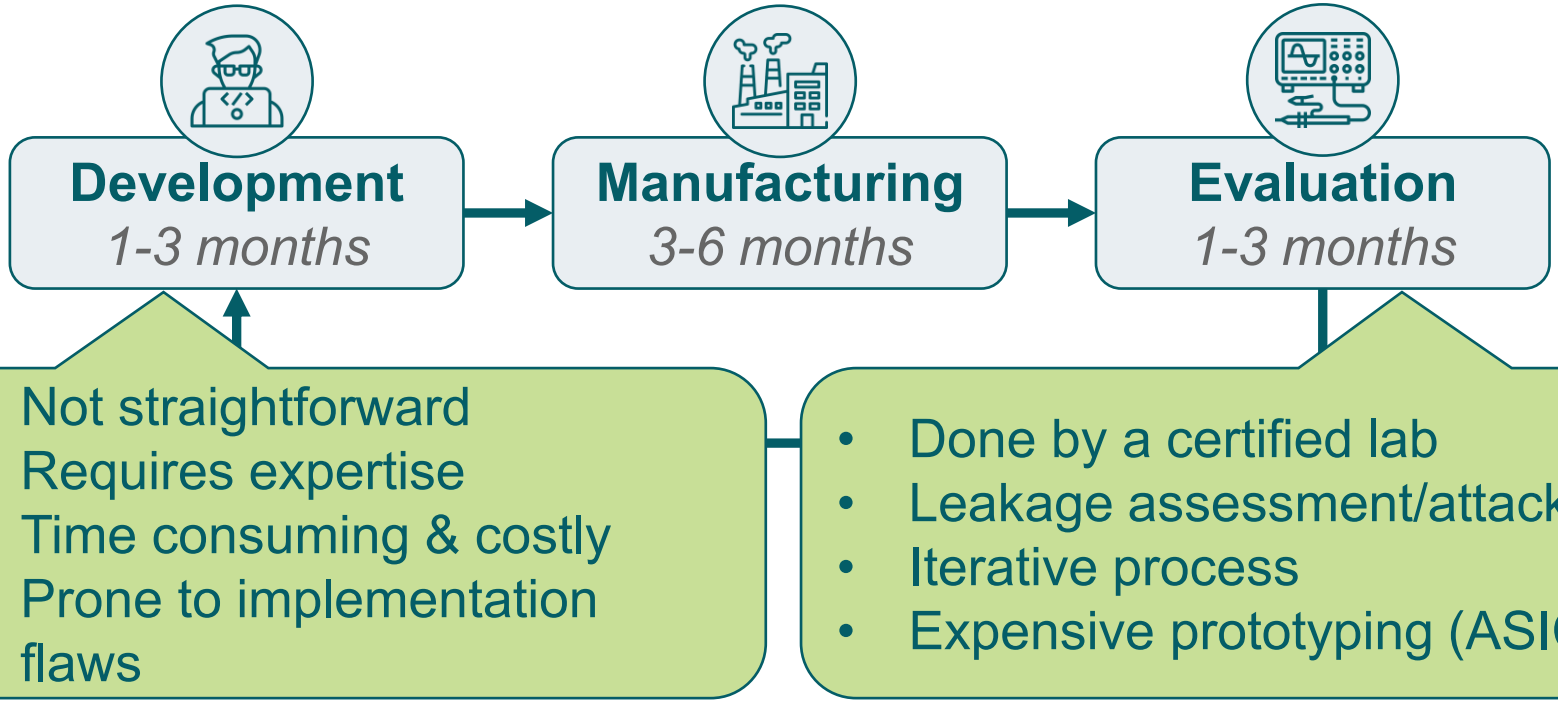


****
****

$$c^0, \ldots, c^d$$
$$c = c^0 \oplus \cdots \oplus c^d$$

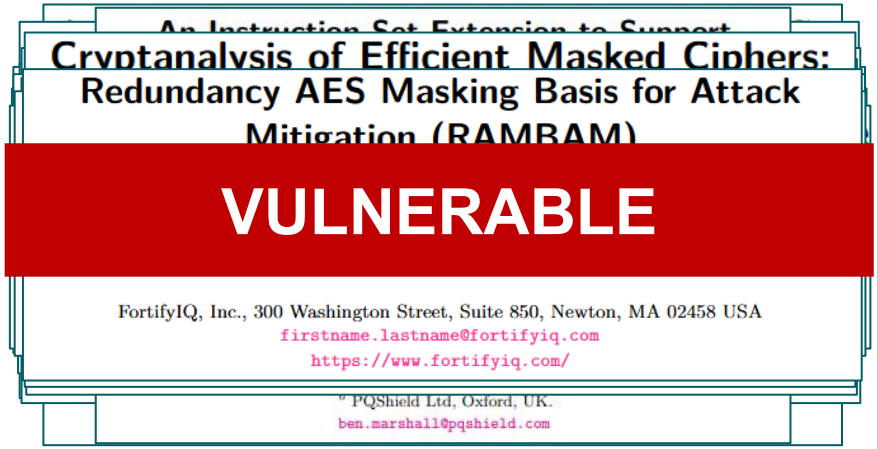
SECURITY-AWARE HARDWARE DESIGN FLOW

CASA
Cyber Security in the Age of Large-Scale Adversaries



CHALLENGES

MASKING SCHEME



An Instruction Set Extension to Support

Cryptanalysis of Efficient Masked Ciphers:

Redundancy AES Masking Basis for Attack Mitigation (RAMBAM)

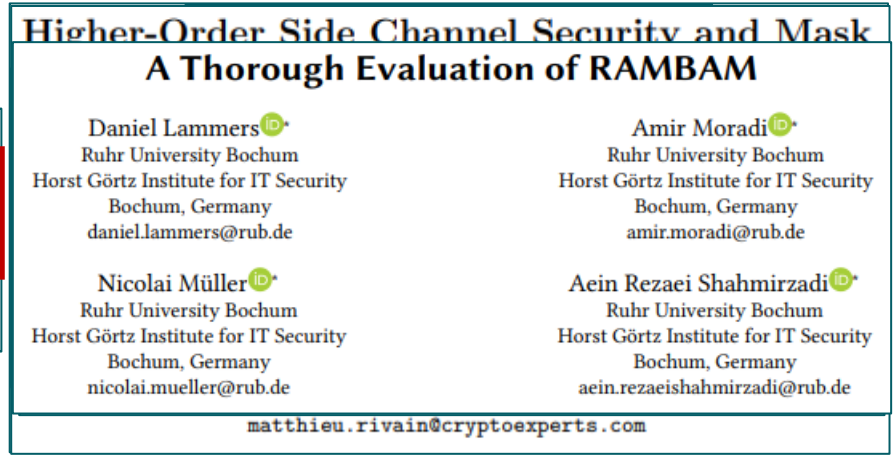
VULNERABLE

FortifyIQ, Inc., 300 Washington Street, Suite 850, Newton, MA 02458 USA
firstname.lastname@fortifyiq.com
https://www.fortifyiq.com/

PQShield Ltd, Oxford, UK.
ben.marshall@pqshield.com

CHES 2022

SECURITY ANALYSIS



Higher-Order Side Channel Security and Mask

A Thorough Evaluation of RAMBAM

Daniel Lammers
Ruhr University Bochum
Horst Görtz Institute for IT Security
Bochum, Germany
daniel.lammers@rub.de

Amir Moradi
Ruhr University Bochum
Horst Görtz Institute for IT Security
Bochum, Germany
amir.moradi@rub.de

Nicolai Müller
Ruhr University Bochum
Horst Görtz Institute for IT Security
Bochum, Germany
nicolai.mueller@rub.de

Aein Rezaei Shahmirzadi
Ruhr University Bochum
Horst Görtz Institute for IT Security
Bochum, Germany
aein.rezaeishahmirzadi@rub.de

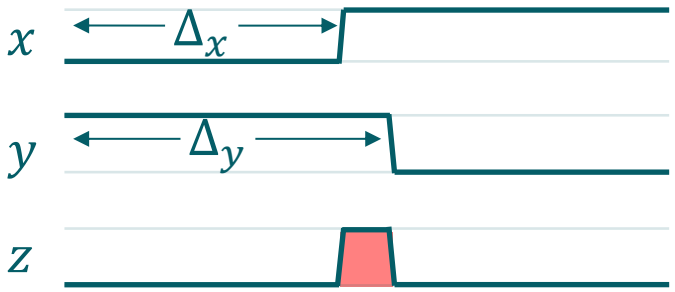
matthieu.rivain@cryptoexperts.com

CCS 2023

PROBLEMS

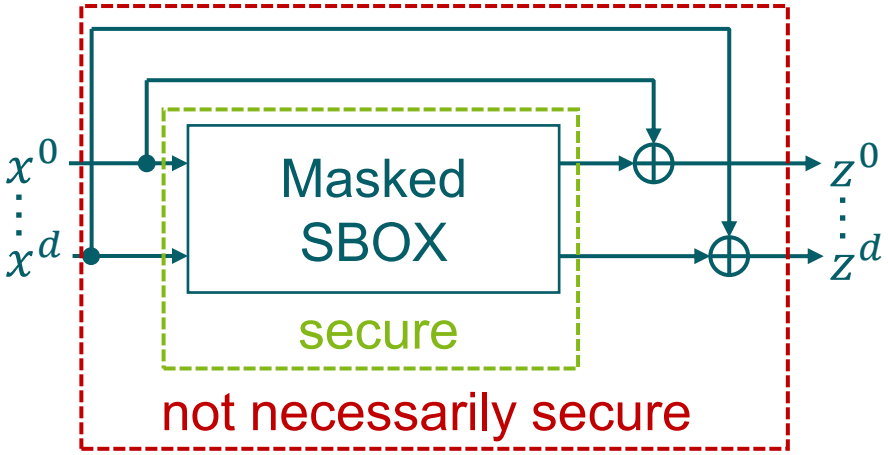
Physical Defaults

$$z = x \cdot y, \qquad x, y, z \in GF(2)$$



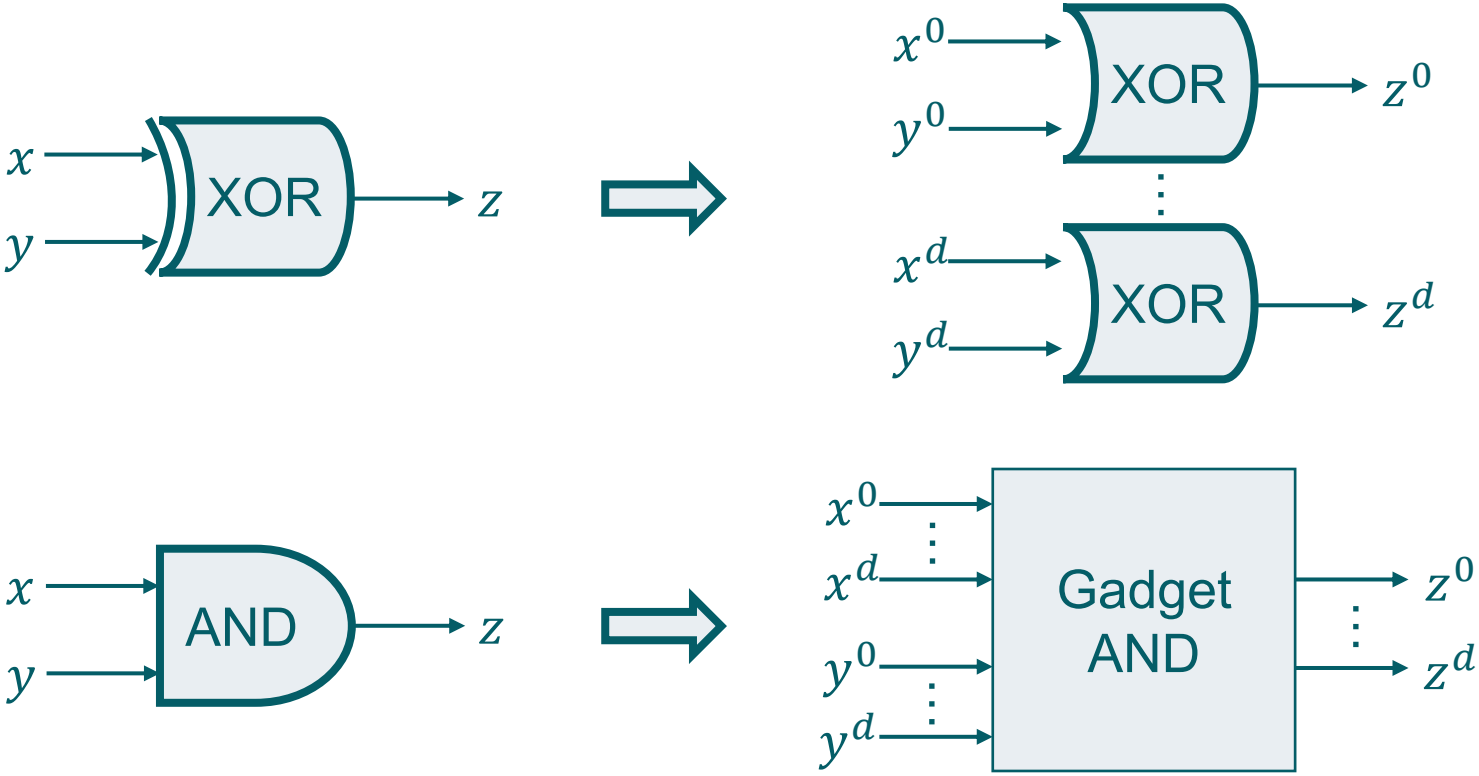
Requires proofs under robust adversary models!

Lacks of Composability



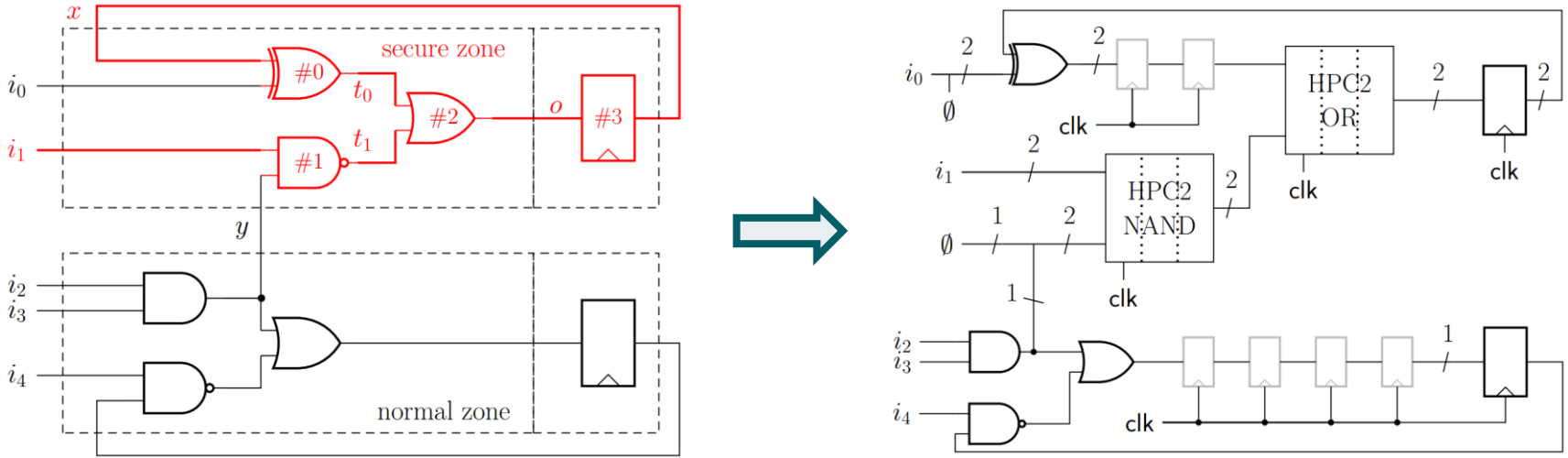
Requires dedicated proofs of composability!

COMPOSABLE GADGETS



AUTOMATED GENERATION OF MASKED HARDWARE

CASA
CYBER SECURITY IN THE AGE OF LARGE-SCALE ADVERSARIES



Source: Knichel, D., Moradi, A., Müller, N., & Sasdrich, P. (2021). Automated Generation of Masked Hardware. *IACR Transactions on Cryptographic Hardware and Embedded Systems*, *2022*(1), 589-629. https://doi.org/10.46586/tches.v2022.i1.589-629

OPTIMIZED SECURITY-AWARE HARDWARE DESIGN FLOW

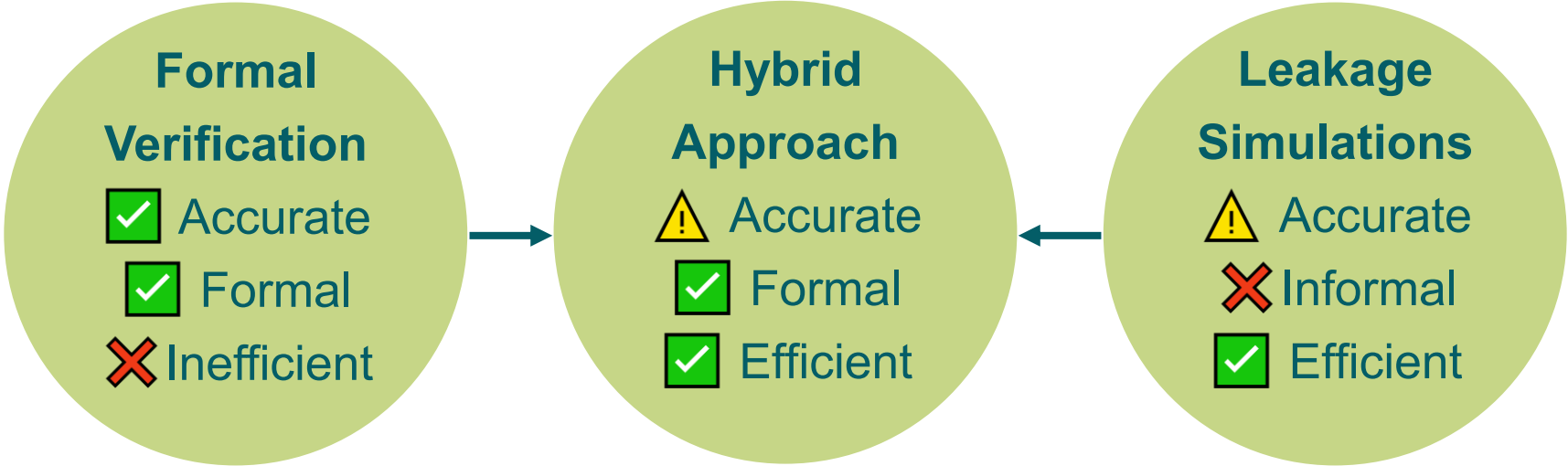
CASA
Cyber Security in the Age of Large-Scale Adversaries

- Done by AGEMA
- Provably secure results
- No knowledge required

- Gadget composability proven
- Manual or automated proofs
- No dedicated verification

Inefficient compared to manual masked circuits!

LEAKAGE EVALUATION



Source: Müller, N., & Moradi, A. (2022). PROLEAD: A Probing-Based Hardware Leakage Detection Tool. *IACR Transactions on Cryptographic Hardware and Embedded Systems*, *2022*(4), 311-348. https://doi.org/10.46586/tches.v2022.i4.311-348

CONCLUSIONS

Take Home Messages:

- Masking gives provable security but is difficult to implement
- Gadgets offer a systematic way to generate masked designs
- The overhead of gadgets is high compared to hand-made masking
- Manually masked designs should be evaluated with tools

Additional Resources:

https://www.informatik.tu-darmstadt.de/impsec/publications_impsec/index.en.jsp

CASA
CYBER SECURITY IN THE AGE OF LARGE-SCALE ADVERSARIES

Thanks! Any Questions?

Or maybe later:
nicolai.mueller@rub.de

RUHR-UNIVERSITÄT BOCHUM
Horst-Görtz-Institut für IT-Sicherheit
Exzellenzcluster CASA
MC 0.75 | Universitätsstr. 150 | 44780 Bochum | Germany
www.casa.rub.de | www.hgi.rub.de

Gefördert durch
DFG Deutsche Forschungsgemeinschaft

RUHR UNIVERSITÄT BOCHUM
RUB

HG HORST GÖRTZ INSTITUT