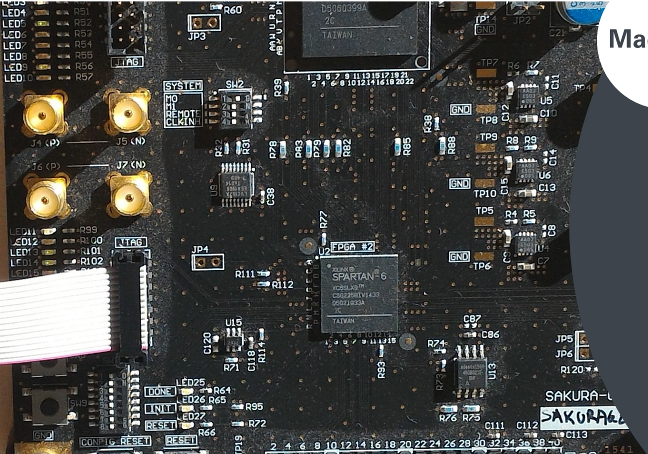
Universität Stuttgart



Maël Gay

Our Research Interests and Your Opportunities

Why this Presentation ?

- Lectures must cover (somewhat) well-established knowledge, but new research results often lack maturity to be included into regular teaching
- We want to show you what we are working on now, but the topics change over time (this material is from 2024)
- Useful especially if you are planning to focus in our area, write a thesis with us...
- Brief sketches rather than fully-fledged coverage, but providing references to further probe yourself

General Overview

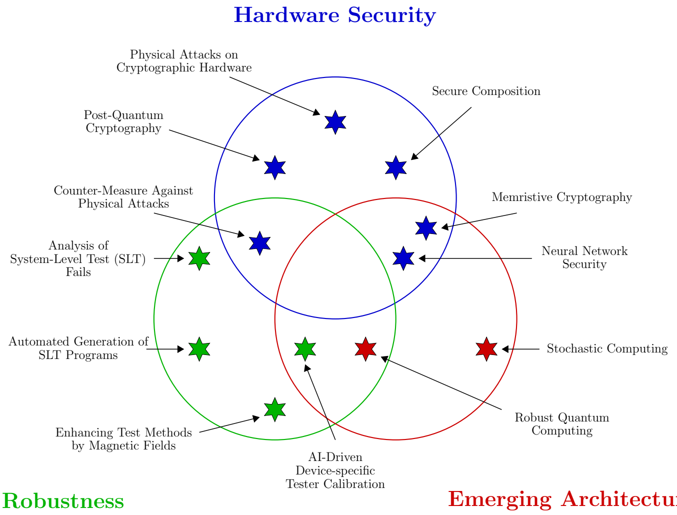
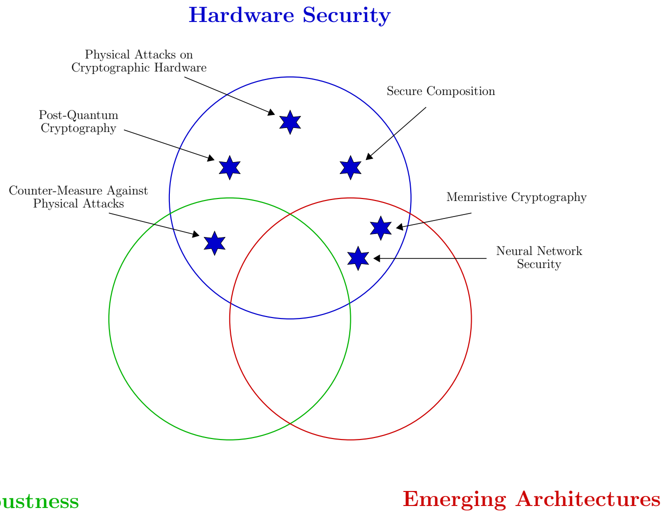


Table of Contents

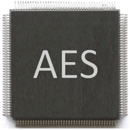
Hardware-Oriented Cryptography

1

Hardware-Oriented Cryptography



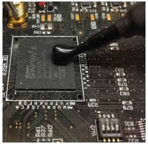
Cryptographic Primitives



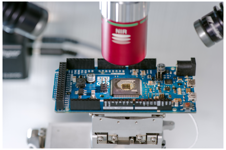
Cryptographic Primitives

```
// ---------------------------------------------------------------------------
// Control signals
// ---------------------------------------------------------------------------
  always @(posedge clock or negedge resetn) begin
    if ( resetn == 1'b0 ) begin
      busy <= 1'b0;
      start_flag <= 1'b0;
      key_val <= 1'b0;
      round_n <= 4'h0;
    end
    else begin
      // Busy flag
      if ( start == 1'b1 ) busy <= 1'b1;
      else if (( now_state == `KEY_EXP ) && ( round_n == n ) && ( start_flag != 1'b1 )) busy <= 1'b0;
      else if (( now_state == `ROUND_LOOP ) && ( round_n == n )) busy <= 1'b0;
      else busy <= busy;

      // Start flag
      if ( start == 1'b1 ) start_flag <= 1'b1;
      else if ( now_state == `ROUND_LOOP ) start_flag <= 1'b0;
      else start_flag <= start_flag;

      // Nr counter
      if ( next_state == `IDLE ) round_n <= 4'h0;
      else round_n <= round_n + 1'b1;

      // Key valid flag
      if (( now_state == `KEY_EXP ) && ( round_n == n )) key_val <= 1'b1;
      else key_val <= key_val;

     // Clock Selection
      if (( now_state == `ROUND_LOOP ) && ( round_n == f_round ) && ( fault_t == 1'b1 )) sel <= 1'b1;
      else sel <= 1'b0;
    end
  end
```

Hardware Design => Physical Restrictions



Vulnerabilities: Especially if Physical Access is Allowed



Side-channel attacks: DPA, DFA...

Hardware-Oriented Cryptography

Post-Quantum Cryptography

- As computing power increased, security was increased by **increasing key sizes**

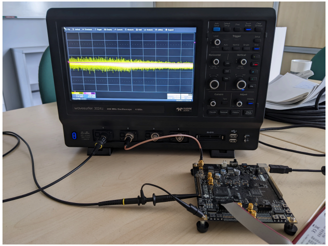
- **New threat**: quantum computers & algorithms (example: Shor's algorithm)
- **Need**: (hardware) cryptosystem which will withstand attacks in the future

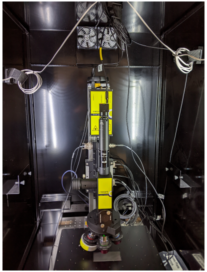
- **Solution**: Post-Quantum Cryptography (PQC)
- Still based on hard problems, but hard even if quantum computers are available

- **Example**: Kyber encryption scheme, based on Learning With Errors (LWE) problem over module lattices
- **Our interest**: Attacking & improving PQC algorithms hardware implementations

Physical Attacks on Cryptographic Hardware

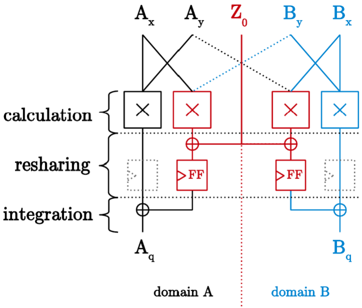
- **What are physical attacks ?**
- Attacks which make use of the physical properties to recover secret data
- **Our interest**:
  - Side-Channel Analysis (SCA): uses side-channels (e.g. power consumption)
  - Fault Injection Attacks (FIAs): use perturbations (e.g. induced by a laser)
  - AutoFault: automated framework for algebraic fault attacks
- **Examples**:

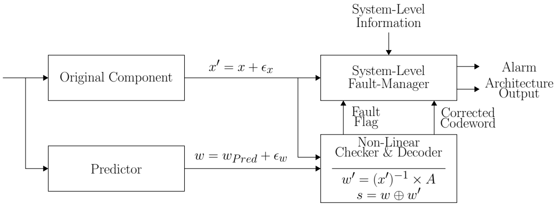




Counter-Measure Against Physical Attacks

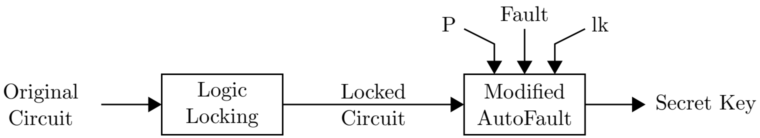
- If physical attacks are a threat, **how do we protect circuits** against them ?
- **Counter-measures of interest to us**:
  - Masking: introduce randomness to prevent side-channel leakages
  - Error-Correcting Codes (ECC): correct faults before they can be leveraged





Secure Composition

- **Overall idea**: multiple counter-measure can interfere with each other and create new vulnerabilities (e.g. increase side-channel leakage)
- **Secure composability**: make sure counter-measures can be merged without issues
- **Our work**:
  - Mitigation of increased SCA leakage induced by ECC
  - Locking Enabled Differential Analysis (LEDA): logic locking as an attack vector



Memristive Cryptography

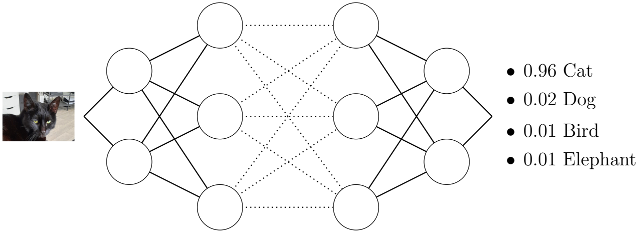
- Memristors are devices which have **two resistive states**, switchable by applying a certain voltage (or current), and they retain their values
- Used for in-memory computing, but **what about cryptographic applications ?**
- The correlation between power consumption and secret data is different: theoretically **more resilient to SCA**
- **In practice: still vulnerable to SCA**, but the attacks may need to be adapted

- **Our interests**:
  - Graph-based synthesis of memristive cryptosystem (Majority Inverter Graphs)
  - Power consumption simulation of memristor-based circuits
  - SCA on small memristive circuits based on Stochastic Approach
  - Masking counter-measure applied to memristive cryptography

Neural Network Security

- **Neural Networks** (and generally AI) have gained significant traction recently, but **what about their security** or secret data involved ?
- Attacks effective against cryptosystems have recently been applied to NNs
- **Weights & biases can be recovered**, as well as the overall structure of the NN

- **Our goals**:
  - Simulation of mixed-signals NNs
  - Physical attacks against NNs (e.g. power SCA)
  - Counter-measures applied to NNs



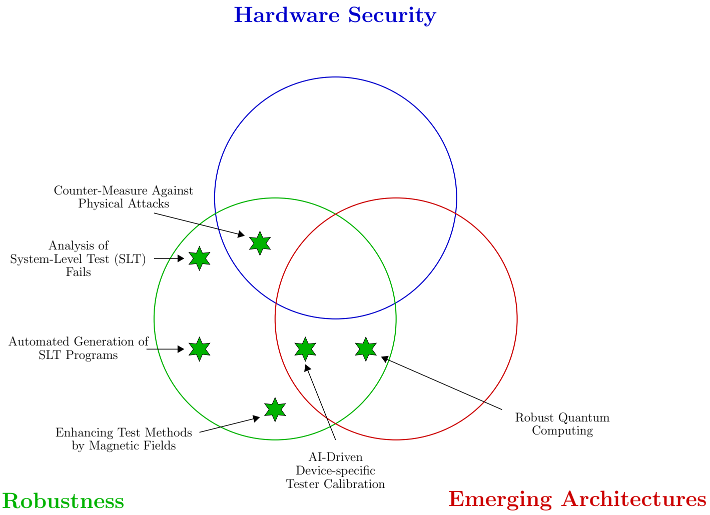
To Probe Further

- PQC scheme CRYSTALS-Kyber: https://pq-crystals.org/kyber/
- Correlation Power Analysis: https://doi.org/10.1007/978-3-540-28632-5_2
- Differential Fault Attack on AES: https://doi.org/10.1007/978-3-642-21040-2_15
- AutoFault: https://doi.org/10.1109/FDTC.2019.00012
- Domain-Oriented Masking: https://doi.org/10.1145/2996366.2996426
- ECC Architectures: https://doi.org/10.1007/s13389-020-00234-7
- LEDA: https://doi.org/10.1109/HOST55118.2023.10133696
- Memristor: https://doi.org/10.1109/IVSW.2019.8854394
- SCA on Memristor: https://doi.org/10.1109/ATS59501.2023.10317969
- Majority-Inverter Graph: https://doi.org/10.1145/2593069.2593158

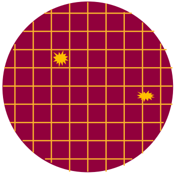
Robust Systems

2

Robust Systems



System-Level Test (SLT)



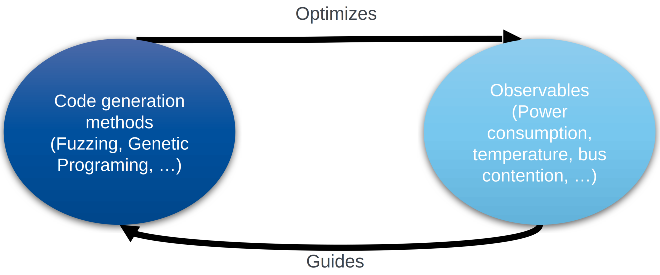
Manufactured circuit
with defects

Post-manufacturing test

System-level test
SLT-unique fails reported

- **Why are there SLT-unique fails**, and how to prevent them ?
  Complex defects ? Coverage holes ? System-level interactions ?
- **How to generate SLT programs** with desired characteristics ?
  E.g. software-based stress test from high-level architecture models
- How to incorporate **self-awareness** of SoC-under-test ?

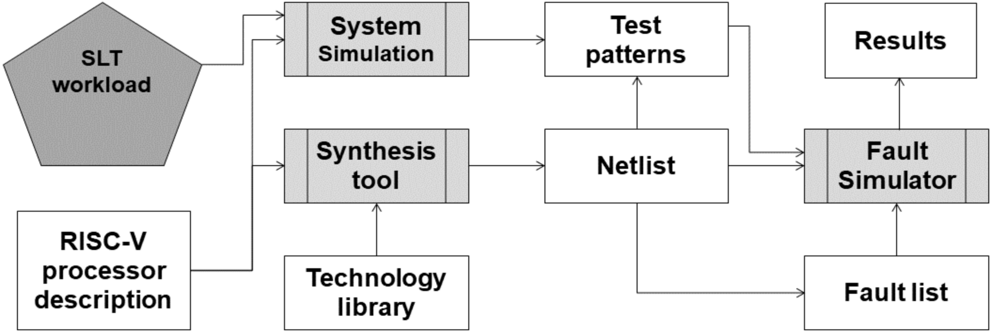
Test Program Generator for SLT



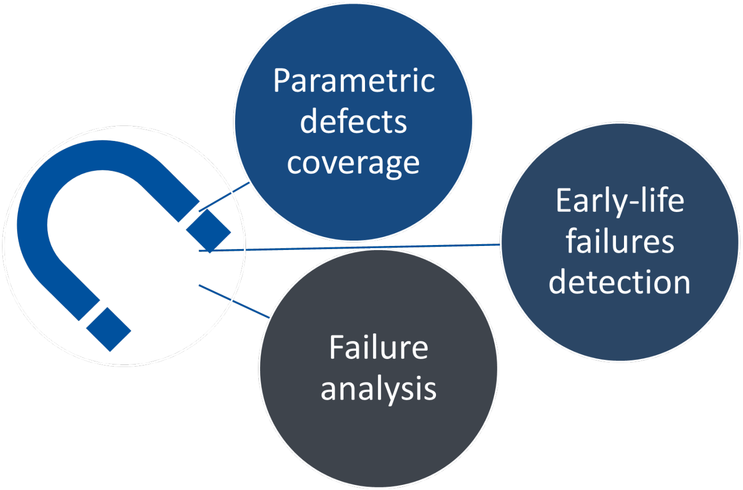
Metrics to determine quality of method and generated test suite (Test Length, Fault Coverage [using custom fault models], ...)

- **Vision**: SLT program generator that incorporates concepts from circuit testing and from software engineering

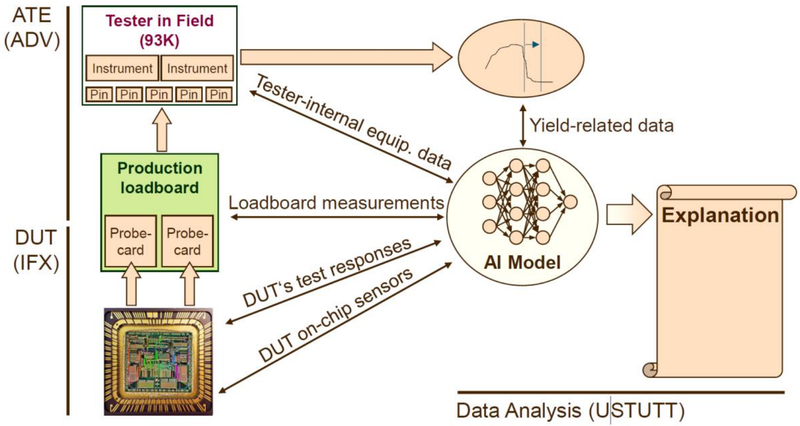
Systematic Analysis of SLT Fails



Enhancing Test Methods by Magnetic Fields



AI-Driven Device-specific Tester Calibration



- Artificial Intelligence driven Device Tester Calibration (AI-DeTeC):
  Improve semiconductor yield using AI-based methodologies

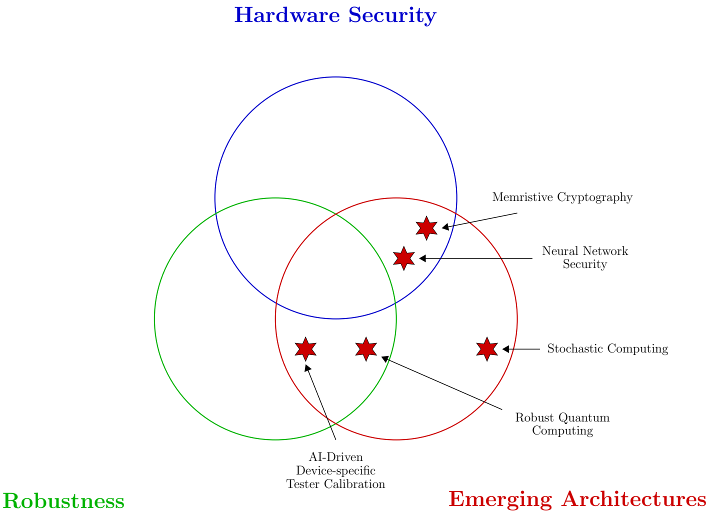
To Probe Further

- SLT: https://doi.org/10.1109/VLSI-DAT.2018.8373238
- Mysteries of SLT: https://doi.org/10.1109/ATS49688.2020.9301557
- Greybox SLT Generation: https://doi.org/10.1109/ETS56758.2023.10173985
- LLMs SLT Generation: https://doi.org/10.1109/ETS61313.2024.10567741
- Genetic Programming (SLT): https://doi.org/10.1109/ETS61313.2024.10567817
- Scan Test vs. SLT: https://doi.org/10.1109/VTS60656.2024.10538586
- WaSSaBi: https://doi.org/10.1109/TCSI.2024.3357975

Emerging Technologies

3

Emerging Technologies

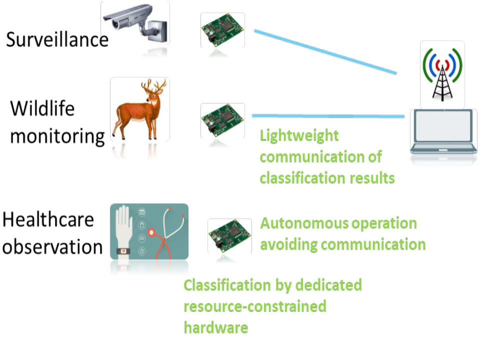


Emerging Technologies - Our Foci

- **Stochastic Computing**:
  - Stochastic computing (SC) for multimodal tasks (e.g. image classification)
  - Robustness of stochastic circuits under errors
  - Stochastic computing-based near sensor systems
- **Quantum Computing**:
  - Transpilation of quantum circuits: map a circuit to a quantum architecture with known noise levels
  - Investigate and improve robustness of quantum circuits

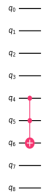
Stochastic Computing-based Near Sensor Systems

- **Need**: Neural networks in resource-constrained hardware
- **Advantage** of SC: low area/power (but potential accuracy loss)
- **Application example**: SC-based signal processing circuits (e.g. digital filters)

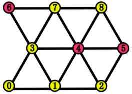


Near-Sensor System

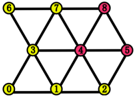
Quantum Circuits on Rydberg Qubit Lattices



Input Circuit
One 3-Qubit Gate



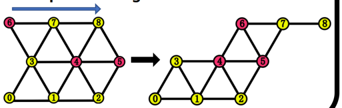
Rydberg Lattice Qubit Connectivity

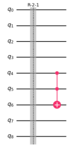


3-Qubit Gate Feasible on Qubit Triangles

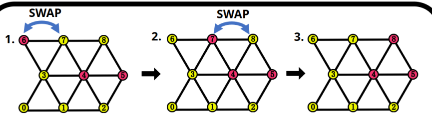
Rydberg Shift Solution

Shift Top Row to Right

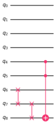




Output Circuit w/ Row Shift



Standard SWAP Solution



Output Circuit w/ SWAPs

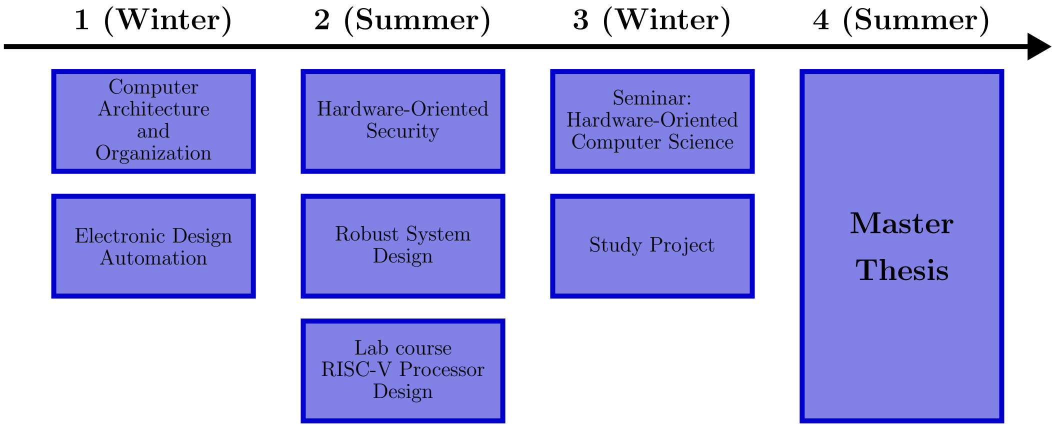
To Probe Further

- The Basic of SC: https://doi.org/10.1109/TCAD.2017.2778107
- SC under Errors: https://doi.org/10.1145/2990503
- SC Robustness: https://doi.org/10.1109/DSN-W58399.2023.00053
- SC NNs: https://doi.org/10.1109/ICRC.2019.8914706
- SC Digital Filter: https://doi.org/10.1109/DDECS60919.2024.10508903
- QC Transpilation: https://arxiv.org/pdf/2002.09783
- QC Robustness: https://doi.org/10.1038/ncomms5213
- QAOA Performance: https://doi.org/10.1007/s11128-022-03766-5

Connection to our Teaching Program

4

Our Offers with an Example Schedule



Teaching Offer Details & Information

- The previous slide is a **generic plan** and is **not guaranteed** for each semester (we may have to change our offering)
- We may also offer new courses or different seminars
- CAO and EDA are more general-interest lectures
- **HOS and RSD** are closer to our **own research foci**
- **RISC-V Processor Design** is a lab course, which **requires CAO**
- Other courses have no prerequisites
- We offer a single **seminar on both emerging architectures and hardware security**
- If you have to choose between a project and a seminar, we recommend the seminar
- We advise taking some of our courses before asking for a project

Theses & Other Projects

- We **do not have** a fixed list of **pre-defined topics**
  - **We want to define your dream topic**, as a thesis should be interesting to you
  - We cannot supervise a topic unrelated to our research foci
  - **Fill our questionnaire** on the HOCOS website and **send it with your transcript of records**
- We **encourage you to talk to group members** if a topic interests you
  - Do not hesitate to ask about our research, even early during your degree
  - We expect some **pre-existing knowledge** on the topics, for instance: HOS for security topics and Prof. Leymann's/Prof. Barz's lecture for quantum ones
  - Doing **a seminar with us is an advantage** (your thesis topic can, but does not have to extend your seminar topic)
- **Theses can lead to published papers**, a great opportunity for future careers
  - Example: SCA Analysis of IPM-RED
    `https://doi.org/10.1109/IOLTS60994.2024.10616073`

Contacts

- **Main contact** for theses: **Maël Gay** - mael.gay@informatik.uni-stuttgart.de
  Please send the filled questionnaire and transcript of records to me
- **Hardware Security**:
  - Maël Gay: PQC, SCA & FIA, counter-measures, NN security
  - Devanshi Upadhyaya: secure composition, NN security
  - Tarick Welling: PQC, SCA
  - Li-Wei Chen: memristive cryptography (attacks & counter-measures)
  - Felix Bayhurst: memristive cryptography (graph-based synthesis)
- **Robustness**:
  - Nourhan Elhamawy: systematic analysis of SLT fails
  - Denis Schwachhofer: test program generation for SLT
  - Anand Venkatachalam: AI-driven tester calibration
  - Karthik Pandaram: EM-based test methods
- **Emerging Technologies**:
  - Roshwin Sengupta: stochastic computing
  - Biswash Ghimire: quantum circuits

Recent Theses

- Implementation and Leakage Assessment of Inner Product Masking with Robust Error Detection
- NN-Based Side Channel Attack on Crystals-Kyber
- Machine Learning-based Side-Channel Attack on a Hardware Implementation of CRYSTALS-Kyber
- A Comparison of TVLA and HC in Side-Channel Leakage Detection
- Stochastic Computing based RNN Implementation on FPGA
- FPGA Implementation of Stochastic Morlet Wavelet Transform

Maël Gay
Institut für Technische Informatik (ITI), Universität Stuttgart

eMail	mael.gay@informatik.uni-stuttgart.de
Telefon	+49 711 685 88290
Fax	+49 711 685 88288