Brojogopal Sapui

Papstdorfer str. 37, 01277 Dresden, Germany | +49 178 763 2365 | brojogopal.sapui@gmail.com |
linkedin.com/in/brojogopal-sapui-66a2a1116

Just finished Ph.D. specializing in **embedded hardware security, building secure systems IPs, and crypto & ML accelerators**. Expertise in leakage and fault modeling of crypto accelerators, secure execution of AI kernels on FPGA/embedded platforms, side-channel and fault-injection validation, secure architecture design, information-flow tracking, and runtime protection of AI workloads. Strong skills on Python, embedded C/C++, SystemVerilog, cryptographic validation, and hands-on FPGA experience.

Technical Skills

Programming: C++, Embedded C, Python, Verilog/SystemVerilog, TCL
Security: Secure execution flows, model confidentiality, side-channel (SPA/DPA/CPA), fault injection, constant-time analysis, information-flow tracking, in hardware accelerators.
Cryptography: AES, RNG/TRNG evaluation, integrity/confidentiality primitives, hash/MAC flows, secure provisioning workflows
Platform Security: Firmware integrity validation, secure loading of AI kernels (FPGA/edge)
Hardware/ML: TFLite/ONNX deployment familiarity, edge-AI accelerator profiling, secure weight/model handling, robustness validation
EDA Tools: Cadence Virtuoso/GENUS/INNOVUS, Synopsys VCS/DC, Xilinx Vivado/Vitis
Verification: UVM, security verification, FPGA prototyping, firmware–RTL co-debug

Work Experience

Research Scientist — Secure Emerging AI Hardware Design Feb 2026 — Present
NaMLab gGmbH, Dresden, Germany Dresden

- Leading the design and tape-out of **rFET**-based hardware building blocks and test chips, exploring security-enabling mechanisms (e.g., bias-based obfuscation and side-channel resilience) for AI accelerators.
- Implementing and validating **logic-locking and masking circuits** using rFETs to protect intellectual property (IP) against reverse engineering, hardware trojans and side-channel attacks on AI accelerators.
- Collaborating on the design of a secure **Network-on-Chip (NoC)** for **Hardware Root of Trust** systems, integrating our internally developed **rFET-based transistor-level security primitives** to enable enhanced protection against reverse engineering, tampering, and side-channel attacks.
- Managing the full **physical design and secure layout flow** using **GlobalFoundries** process technologies, including sign-off and multi-project wafer (MPW) preparation.
- Developing cross-layer security strategies integrating emerging device characteristics with **RTL-level obfuscation**.

Research Assistant (PhD) — Hardware Security for Emerging AI Accelerators Feb 2022 — Present
Karlsruhe Institute of Technology (KIT), Germany Karlsruhe

- Built secure execution and validation flows for crypto (AES etc.) and AI (CNN, SNN etc.) accelerators in FPGA, including **secure loading, runtime monitoring, and isolation of ML models**.
- Designed automated **side-channel and fault-injection (SCA/FI)** frameworks using ChipWhisperer Pro + Tektronix MSO to evaluate ML kernels, integrity, and runtime leakage.
- Developed **trusted execution–style isolation** for accelerator pipelines using RTL-level information-flow tracking and restricted-domain execution.
- Modeled fault resilience and integrity of ReRAM/MRAM-based CiM units; validated secure execution behavior from SPICE to FPGA firmware.
- Implemented **constant-time and randomized scheduling** as countermeasures to microarchitectural leakage in ML models.
- Created secure loading flows for hypervector models (AI accelerators such as HDC) and evaluated protection of stored ML weights under adversarial access.

- **Skills:** Embedded C/C++, TFLite/ONNX runtime familiarity, firmware-flow control, secure model handling, Python/TCL, Vivado/Vitis, Synopsys VCS.

Embedded Software Developer — Automotive Security Feb 2021 — Jan 2022
Wipro Technologies R&D, India | General Motors Kolkata

- Developed secure ECU provisioning and registration workflows (C++), including **firmware integrity checks, secure onboarding**, and authenticated update flows.
- Conducted system-level testing with CANoe/CANalyzer; analyzed runtime behavior and security posture of in-vehicle firmware modules.
- Contributed to automotive-grade threat analysis and integration of crypto primitives for data integrity and secure message transport.
- **Skills:** C/C++, firmware security, TLS flows, AUTOSAR, CAN security, threat-modeling support, secure provisioning.

Lead Project Engineer — Quantum Randomness & Cryptography Jan 2019 — Jan 2021
Indian Statistical Institute (ISI) Kolkata, under supervsision of Prof. Goutam Paul Kolkata

- Evaluated **quantum TRNG entropy sources**, bias/leakage, and cryptographic quality using embedded setups and Python-based statistical analysis.
- Conducted background surveys on **PQC accelerators**, with focus on the role of hardware entropy sources for lattice-based and code-based PQC implementations.
- **Skills:** Cryptographic validation, confidentiality/integrity testing, embedded C, firmware-level robustness.

Research Fellow — Physical Unclonable Functions (PUFs) Security Jul 2016 — Dec 2018
Indian Institute of Technology Kharagpur , under supervision of Prof. Debdeep Mukhopadhyay Kharagpur

- Designed and evaluated **PUF architectures** resistant to ML cloning attacks; implemented FPGA/ASIC prototypes and lightweight countermeasures.
- Integrated PUF response processing with crypto modules for secure key-generation and authentication pipelines.
- **Skills:** Verilog/SystemVerilog, FPGA prototyping, reliability/security evaluation, ML-driven attack modeling.

Education

Ph.D. in Hardware Security, Karlsruhe Institute of Technology (KIT), Germany, *Jan 2026*. Grade - Magna cum laude
M.Tech. in VLSI Design, NIT Meghalaya, India, 2016. Grade- (CGPA) 8.33/10.
B.Tech. in Electronics & Communication, MAKAUT, India, 2012.

Selected Publications

- “When Faults Don’t Vanish: Persistent Fault Analysis on MRAM-AES,” DATE’26.
- “HyFault: Voltage-Level Fault Injection Attacks on FPGA-based Edge-AI Accelerators,” ASP-DAC’26.
- “DL-Assisted Side-Channel Analysis on HDC Accelerators,” ICCAD’25.
- Other publications in TCAD’25, ASP-DAC’25, DATE’23, JETCAS’21, etc.

Supervision

- Master Thesis — SAT-based formal verification and robustness validation of AI accelerators.
- HiWi Thesis — Remote side-channel analysis using on-chip delay sensors (FINN framework).

Languages

English (Fluent), Bengali (Native), German (Basic A1).

Publications

1. **Brojogopal Sapui**, Priyanjana Pal, Mehdi B. Tahoori, "**When Faults Don't Vanish: Persistent Fault Injection and Key Recovery on MRAM-Backed AES**," *Design, Automation & Test in Europe Conference (DATE)*, 2026, Verona, Italy, Apr. 2026.
2. **Brojogopal Sapui**, and Mehdi B. Tahoori, "**HyFault: Voltage-Level Fault Injection Attacks on FPGA-based Hyperdimensional Computing Accelerators**," *Asia and South Pacific Design Automation Conference (ASP-DAC)*, 2026, Hongkong, Jan. 2026.
3. **Brojogopal Sapui**, and Mehdi B. Tahoori, "**Leaks beyond Bits: Deep Learning-Assisted Side-Channel Attacks on Hyperdimensional Computing Accelerators**," *IEEE/ACM International Conference on Computer-Aided Design (ICCAD)*, Munich, Germany, Oct. 2025, pp 1-9.
4. **Brojogopal Sapui**, Mahboobe Sadeghipourrudsari, and Mehdi B. Tahoori, "**Collide & Conquer: Side-channel Attack on Hyper-dimensional Computing (HDC) Accelerators**," *Asian Test Symposium / ITC-Asia*, 2025, Tokyo, Japan, Dec. 2025.
5. **Brojogopal Sapui**, and Mehdi B. Tahoori, "**Power Side-Channel Analysis and Mitigation for Neural Network Accelerators based on Memristive Crossbars**," *Asia and South Pacific Design Automation Conference (ASP-DAC)*, Incheon, South Korea, Jan. 2024, pp. 612–617.
6. **Brojogopal Sapui**, Jonas Krautter, Mahta Mayahinia, Atousa Jafari, Dennis Gnad, Sergej Meschkov, and Mehdi B. Tahoori, "**Power Side-Channel Attacks and Countermeasures on Computation-in-Memory Architectures and Technologies**," *IEEE European Test Symposium (ETS)*, Venice, Italy, May 2023, pp. 1–6.
7. **Brojogopal Sapui**, Sergej Meschkov, and Mehdi B. Tahoori, "**Side-Channel Attack with Fault Analysis on Memristor-based Computation-in-Memory**," *IEEE International Symposium on On-Line Testing and Robust System Design (IOLTS)*, Rennes, France, Jul. 2024, pp. 1–7.
8. **Brojogopal Sapui**, and Mehdi B. Tahoori, "**Side-Channel Collision Attacks on Hyperdimensional Computing Based on Emerging Resistive Memories**," *Asia and South Pacific Design Automation Conference (ASP-DAC)*, Tokyo, Japan, Jan. 2025.
9. **Brojogopal Sapui**, Priyanjana Pal, and Mehdi B. Tahoori, "**Side-Channel Vulnerability Analysis of Flexible Neuromorphic Circuits**," *IEEE/ACM International Conference on Computer-Aided Design (ICCAD)*, Munich, Germany, Oct. 2025.
10. Priyanjana Pal, **Brojogopal Sapui**, Dennis D. Weller, and Mehdi B. Tahoori, "**Efficient Analog Error Correction for Printed Unary-Encoded Computing**," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems (TCAD)*, Early Access, 2025.
11. Haibin Zhao, **Brojogopal Sapui**, Michael Hefenbrock, Zhidong Yang, Michael Beigl, and Mehdi B. Tahoori, "**Highly-Bespoke Robust Printed Neuromorphic Circuits**," *Design, Automation & Test in Europe Conference (DATE)*, Antwerp, Belgium, Apr. 2023, pp. 1–6.
12. Nimesh Shah, Durba Chatterjee, **Brojogopal Sapui**, Debdeep Mukhopadhyay, and Arindam Basu, "**Introducing Recurrence in Strong PUFs for Enhanced Machine Learning Attack Resistance**," *IEEE Journal on Emerging and Selected Topics in Circuits and Systems (JETCAS)*, vol. 11, no. 2, pp. 319–332, 2021,
13. F. Lalchhandama, **Brojo Gopal Sapui**, and Kamalika Datta, "**An Improved Approach for the Synthesis of Boolean Functions Using Memristor-Based IMPLY and INVERSE-IMPLY Gates**," *IEEE Computer Society Annual Symposium on VLSI (ISVLSI)*, Pittsburgh, PA, USA, Jul. 2016, pp. 319–324.