Brojogopal Sapui

Schloßpl. 19, 76131 Karlsruhe, Germany | +49 178 763 2365 | brojogopal.sapui@gmail.com |
linkedin.com/in/brojogopal-sapui-66a2a1116

Completed Ph.D. (defense 16th Jan, 2026) in **embedded hardware security, secure systems, and crypto & ML accelerator protection**. 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 embedded C/C++, SystemVerilog, cryptographic validation, and hands-on FPGA experience.

Technical Skills

Programming: C++, Embedded C, Rust, Python, Verilog/SystemVerilog, TCL
Security: Threat modeling, secure execution flows, model confidentiality, side-channel (SPA/DPA/CPA), fault injection, constant-time analysis, information-flow tracking.
Threat Modeling Frameworks: STRIDE-style analysis; familiarity with **MITRE ATLAS™** ML threat taxonomy.
Adversarial ML: Adversarial examples (FGSM/PGD/C&W), robustness evaluation, attacker models (white/gray/black-box), attack pipelines using **ART (Adversarial Robustness Toolbox)** and **Foolbox**.
Cryptography: AES, RSA, 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, formal methods, security verification, FPGA prototyping, firmware–RTL co-debug

Work Experience

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

- Leading the design and tape-out of secure hardware architectures utilizing **Reconfigurable Field-Effect Transistors (RFETs)** for advanced security primitives.
- Implementing and validating **logic-locking circuits** to protect intellectual property (IP) against reverse engineering and hardware trojans.
- Managing the full **physical design and 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 — Embedded Hardware Security for Emerging AI Accelerators Feb 2022 — Jan 2026
Karlsruhe Institute of Technology (KIT), Germany Karlsruhe

- Built secure execution and validation flows for crypto (AES, SHA 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 **adversarial robustness evaluation** for embedded/accelerated inference, generating and benchmarking attacks (FGSM/PGD/C&W) using **ART** and **Foolbox** to validate threat models and mitigations.
- 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.
- 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, **ART/Foolbox**, Python/TCL, Vivado/Vitis, Synopsys VCS.

Embedded Software Developer — Automotive Security Feb 2020 — 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 2020
Indian Statistical Institute (ISI), Kolkata 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.

Researcher — Physical Unclonable Functions (PUFs) Jul 2016 — Dec 2018
Indian Institute of Technology Kharagpur Kharagpur

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

Education

Ph.D. in Embedded Hardware Security, Karlsruhe Institute of Technology (KIT), Germany, *expected Jan 2026*.
M.Tech. in VLSI Design, NIT Meghalaya, India, 2016. 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 HDC 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).