James Hyunmin Kim, Ph.D.

SoC Security Architect | Hardware Security Expert

United Arab Emirates | +971 56 917 4985 | hmkim.sec@gmail.com
LinkedIn | Google Scholar

PROFESSIONAL SUMMARY

Full-stack hardware security architect with **15+ years** of experience spanning the complete security system stack—from **full-custom analog circuits** and **semi-custom ASIC design** to **FPGA implementation** and **secure firmware development**. Proven track record at global semiconductor leaders including NXP, Synopsys, Secure-IC, Silicon Labs, and TII. Ph.D. from KU Leuven (imec-COSIC) with deep expertise in cryptographic implementations and side-channel countermeasures. **Led cross-functional teams (up to 7 engineers)** in security architecture, FPGA development, and security analysis. Delivered **CAVP-certified security IPs**, led **4 silicon tape-outs**, and published **10+ peer-reviewed papers** (41 citations) including Best Paper Award.

CORE COMPETENCIES

Secure SoC Architecture | ARM TrustZone / RISC-V PMP | Root of Trust / HSM | TEE (OP-TEE/NuttX) | Secure Boot & Key Mgmt | Trust Chain | Life-Cycle Management | Remote Attestation | Side-Channel Analysis | Threshold Implementation | Post-Quantum Cryptography | Crypto IP Design | Memory Encryption | PUF/TRNG | Security for AI Hardware | Hardware Fuzzing | FIPS 140-2/3 | Common Criteria (CC) | ISO 26262 / ASIL | Functional Safety | RTOS Security | RTL Design (UVM) | Formal Verification | ASIC/FPGA Development

PROFESSIONAL EXPERIENCE

Technology Innovation Institute (TII)

Abu Dhabi, UAE

Senior SoC Security Researcher and Architect — Dec 2023 - Present

SoC ARCHITECTURE | FPGA | TECHNICAL LEADERSHIP | RESEARCH

- **Led security/control subsystem architecture (team of 5)**: Defined ARM/RISC-V security subsystem, control subsystem, safety island, and power/clock/reset management for drone SoC platform
- **Led FPGA design for drone flight controller (team of 7)**: DShot 150/300/600/1200 ESC protocol implementation; ML-powered timing error correction with neural network for anomaly detection
- **Led comprehensive security analysis for Saluki product (team of 7)**: End-to-end security assessment using Keysight Inspector/Spider and ChipWhisperer; identified and mitigated critical vulnerabilities
- **Led remote attestation verifier development (team of 3)**: SMT-enhanced verifier with hardware-backed prover for secure device identity
- **Secure Boot Architecture**: Multi-stage boot chain with OpenTitan/Caliptra Root of Trust; formal verification using Z3 SMT solver and TLA+; PQC migration with CRYSTALS-Dilithium on Xilinx Zynq 7000
- **Key Management System**: Secure boot, secure update, key lifecycle on Microchip PolarFire FPGA and NXP i.MX93 with TEE (NuttX/OP-TEE), NIST SP 800-57 compliant

Silicon Laboratories International Pte. Ltd.

Singapore

Associate Staff Digital Design Engineer — Oct 2022 - Nov 2023

SoC DESIGN | IMPLEMENTATION & INTEGRATION | ASIC

- **Implementation:** eFUSE controller, OTP controller, Bus Level Security (BLS) enhancement, Memory controller - full RTL design to synthesis
- **Integration:** Security subsystem architecture with ARM TrustZone; PUFrt, SRAM PUF, crypto hardware accelerators, and 3rd party security IPs
- **Architected custom crypto engines** (symmetric/PKC) with comprehensive UVM verification framework
- Developed comprehensive **unit test environment** for security IP validation and regression testing

Secure-IC Pte Ltd / Secure-IC S.A.S
Singapore / France

Secure & Safe RISC-V Program Manager / Senior R&D Engineer Jun 2021 - Sep 2022

RISC-V | FreeRTOS/ZEPHYR | SAFETY-RESILIENT | ASIC

- **Represented company at RISC-V International** for security standards development
- **Designed dual-core lockstep** for automotive safety; defined ASIL B/C/D requirements for memory/ECC controllers
- **PMP implementation** and integration into Securyzr platform; Hypervisor and Secure OS adaptation into HSM
- First RTOS integration at Secure-IC: FreeRTOS/Zephyr porting to Securyzr HSM with secure firmware development
- Developed **Verification IP** using Vunit framework on open source platform
- **Supervised 2 Ph.D. candidates** at Telecom Paris on security/safety co-design

Synopsys Canada ULC
Ottawa, Canada

Senior ASIC Digital Design Engineer, Security IP May 2019 - Apr 2021

SECURITY IP DESIGN | TRNG | ASIC

- **Led DWC TRNG/NIST TRNG development** achieving CAVP certification (Oct 2019), BSI AIS 31 compliant
- **Developed inline memory encryption (AES-XTS)** and PQC hardware modules; DRBG SCA countermeasure implementation
- SCA and FIA testing/countermeasures for AES-GCM/XTS and UPKA using NewAE tools; addressed vulnerabilities reported by Riscure
- **OSCCA compliance enhancement** for Chinese market certification requirements
- Delivered IPs compliant with FIPS 140-2/3, ISO 26262, OSCCA, ISO/SAE 21434

NXP Laboratories Ltd.
United Kingdom

Secure Hardware Engineer Mar 2018 - May 2019

CRYPTO IP | SIDE-CHANNEL COUNTERMEASURES | ASIC

- **Owned all block cipher IPs** including scalable ECDSA/ECC for 5 NIST prime curves; security analysis for crypto IPs
- **Secure hardware co-processor design** and integration of secure crypto sub-system
- Threshold implementations (TI) and SCA/FA countermeasures for CC-certified products
- Lightweight crypto IPs (PRESENT, Spongent, KATAN), TRNG/PUF solutions, and **cryptography library development**

Samsung Semiconductor
South Korea

Process Engineer, Lithography Division Dec 2005 - Jan 2009

SEMICONDUCTOR PROCESS | LITHOGRAPHY

- SEM/FIB lithography systems operation; semiconductor process expertise enabling hardware reverse engineering

EDUCATION

Ph.D., Electrical Engineering — KU Leuven, imec-COSIC, Belgium (2017)
Dissertation: "Side-channel security by design: Hardware level countermeasures"
Advisors: Prof. Bart Preneel, Prof. Ingrid Verbauwhede | 4 MPW tape-outs | Samsung smart card evaluation

Pre-doctoral Course — KU Leuven, Belgium (Aug 2011 - Sep 2012)
RSA/ECC with SCA countermeasures | **Best Paper Award at WISA 2012**

International Scholar — KU Leuven, Belgium (Aug 2010 - Aug 2011)
Three Phase Dynamic Current Mode Logic (TPDyCML) | 1 MPW tape-out (full-custom analog)

M.Sc., Information Security — Korea University, South Korea (2011)
GPA: 93.8% | SCA countermeasures, ASIC design, Korea Crypto Library (Klib)

PUBLICATIONS

[1] **H. Kim**, "Security-Quality Scorecard: A Comprehensive Framework for Quantitative Evaluation of Hardware-Enforced Boot Chain Security," *ISQED 2026*

[2] **H. Kim**, "On the Feasibility of Deploying Lattice-Based PQC in ARM TrustZone TEEs: A Systematic Vulnerability Assessment," *ICISC 2025*

[3] S. Miftah, A. Srivastava, **H. Kim**, S. Wei, K. Basu, "SymbFuzz: Symbolic Execution Guided Hardware Fuzzing," *MICRO 2025*

[4] **H. Kim** et al., "SMART DShot: Secure Machine-Learning-Based Adaptive Real-Time Timing Correction," *Applied Sciences 2025*

[5] A. Srivastava, S. Miftah, **H. Kim**, D. Pal, K. Basu, "PoSyn: A Graphical Approach Towards Side-Channel Aware Synthesis," *IEEE TVLSI 2025*

[6] S. Miftah, **H. Kim**, K. Basu, "InterConFuzz: A Fuzzing-based Comprehensive NoC Verification Framework," *DAC 2025*

[7] S. Miftah, A. Srivastava, **H. Kim**, K. Basu, "Assert-O: Context-based Assertion Optimization using LLMs," *GLSVLSI 2024*

[8] **H. Kim**, S. Hong, B. Preneel, I. Verbauwhede, "STBC: Side-channel attack tolerant balanced circuit," *ISVLSI 2017*

[9] **H. Kim**, S. Hong, B. Preneel, I. Verbauwhede, "Binary Decision Diagram to design balanced secure logic styles," *IOLTS 2016*

[10] **H. Kim**, D. Han, S. Hong, "Mutual Information Analysis for Three-Phase Dynamic Current Mode Logic," *ETRI Journal 2015*

[11] **H. Kim**, V. Rozic, I. Verbauwhede, "Three Phase Dynamic Current Mode Logic," *WISA 2012* **(Best Paper Award)**

Additional: 5 domestic papers, 15 Korea patents (registered)

KEY PROJECTS

ML-DShot Engine	FPGA implementation of DShot 150/300/600/1200 ESC protocol with ML-powered timing correction using Kalman Filter, Fuzzy Logic, and Neural Network (2024-2025)
Key Management System	Secure boot/update/key lifecycle on Microchip PolarFire FPGA and NXP i.MX93 with TEE (NuttX/OP-TEE) (2024-2025)
AI Security Portfolio	Confidential Inference (TPM 2.0, AES-GCM), INT4/FP8 Quantization, FPGA Micro NPU (8×8 Systolic) (2024-2025)
Hardware Fuzzing	SymbFuzz (MICRO 2025), InterConFuzz: NoC verification (DAC 2025), PoSyn: SCA-aware synthesis (TVLSI)
Remote Attestation	Hardware-backed prover and SMT-enhanced verifier for secure device identity (2025)
Secure Boot Architecture	Multi-stage boot chain with OpenTitan/Caliptra RoT; formal verification (Z3 SMT, TLA+); PQC with CRYSTALS-Dilithium on Zynq 7000 (2023-Present)
TRNG (CAVP Certified)	FIPS 140-2/3, BSI AIS 31 compliant - certification Oct 2019 (Synopsys)
4 MPW Silicon Tape-outs	RSA-1024, ECC-193b, PRESENT, AES - all first-pass silicon (2012-2016)
STBC Secure Logic	Side-channel attack Tolerant Balanced Circuit using BDD-based synthesis (Ph.D. - ISVLSI 2017, IOLTS 2016)
TPDyCML (Full-Custom)	Three Phase Dynamic Current Mode Logic - full-custom analog SCA countermeasure (Ph.D. - WISA 2012 Best Paper)
Samsung Smart Card	Security evaluation and SCA vulnerability assessment for commercial smart card products (Ph.D. 2013-2014)

TECHNICAL SKILLS

Hardware	VHDL, Verilog, SystemVerilog, UVM | ASIC/FPGA | RTL-to-GDSII (4x MPW) | Full-custom analog
Programming	C/C++, Python, Perl, Tcl/Tk, GNU Make/CMake, MATLAB/SageMath
EDA Tools	Synopsys (VCS, DC, PT, SpyGlass, Verdi), Cadence (Xcelium, Genus, Virtuoso), Siemens (QuestaSim)
Security	ChipWhisperer (NewAE), Secure-IC Analyzr/Catalyzr
Platforms	ARM TrustZone, RISC-V PMP, OpenTitan, NuttX, OP-TEE, FreeRTOS, Zephyr
Cryptography	AES/SM4, RSA, ECC/ECDSA, PQC (ML-KEM, ML-DSA), TRNG/PUF, Threshold Implementation
Standards	FIPS 140-2/3, ISO 26262, ISO/SAE 21434, BSI AIS 31, OSCCA, Common Criteria

KEY ACHIEVEMENTS

CAVP Certification — TRNG, Oct 2019 (Synopsys)

4 MPW Tape-outs — First-pass silicon (2012-2016)

Best Paper Award — WISA 2012

RISC-V International Rep. — Company representative (2021-2022)

ML-DShot Engine — Neural network timing correction

15 Korea Patents — PUF, secure logic, crypto HW