

YoungBeom Kim 김영범

Ph.D. Student in Cryptography, Kookmin University

darania@kookmin.ac.kr · ko.ybkim@gmail.com · ybgraphy.com · github.com/whYBeKim · Google Scholar · ORCID

RESEARCH INTERESTS

Post-Quantum Cryptography, Software/Hardware Co-Design, Side-Channel Security

EDUCATION

2025.09 – 2026.02	Queen's University Belfast, UK Visiting Student · Host: Prof. Máire O'Neill
2023.03 – Present	Kookmin University, Republic of Korea Ph.D. Student, Cryptography · GPA 4.42 / 4.5 · Advisor: Prof. Seog Chung Seo
2021.03 – 2023.02	Kookmin University, Republic of Korea M.S., Cryptography · GPA 4.38 / 4.5 · Advisor: Prof. Seog Chung Seo <u>Top graduate of the Master's degree</u> Thesis: Efficient Implementation of Post-Quantum Cryptography Crystals-Kyber on 8-bit AVR Microcontroller
2019.03 – 2021.02	Kookmin University, Republic of Korea B.S., Cryptography · GPA 4.25 / 4.5 · Advisor: Prof. Seog Chung Seo <u>Top graduate of the College of Science and Technology</u>

PUBLICATIONS

[†] co-first author [‡] corresponding author

International Conference Papers

- [C14] A Crypto-Agile Mixed-Radix NTT Accelerator for Negacyclic and Trinomial Rings.
JaeSeok Lee, DongHyun Shin, **YoungBeom Kim**, Seog Chung Seo.
CHES 2027, 2027.
- [C13] CMALU: Compact Fault-Tolerant Modular Arithmetic Logic Unit for Post-Quantum Cryptography.
YoungBeom Kim, Malik Imran, Zain Ul Abideen, Ciara Rafferty, Ayesha Khalid, Máire O'Neill, Seog Chung Seo.
ICCAD 2026, 2026. [pdf] [code]
- [C12] Low-Stack HAETAE for Memory-Constrained Microcontrollers.
YoungBeom Kim, Christine van Vredendaal, Gustavo Banegas, Seog Chung Seo.
CHES 2026, 2026. [doi] [pdf] [code] [slides]
- [C11] Optimized Implementations of Keccak, Kyber, and Dilithium on the MSP430 Microcontroller.
DongHyun Shin, **YoungBeom Kim**[†], Ayesha Khalid, Máire O'Neill, Seog Chung Seo.
CHES 2026, 2026. [doi] [pdf] [code]
- [C10] Lightweight PQ KEM and Hybrid MQTT Protocol for 8-bit AVR Sensor Nodes.
Yifan Dong, **YoungBeom Kim**[†], Jieyu Zheng, Zhichuang Liang, Boyue Fang, Seog Chung Seo, Máire O'Neill, Yunlei Zhao.
CHES 2026, 2026. [doi] [pdf] [code] [slides]
- [C9] An Optimized Instantiation of Post-Quantum MQTT Protocol on 8-bit AVR Sensor Nodes.
YoungBeom Kim, Seog Chung Seo.
ASIA-CCS 2025, 2025. [doi] [pdf] [code] [slides]
- [C8] Multiplying Polynomials without Powerful Multiplication Instructions.
Vincent Hwang, **YoungBeom Kim**, Seog Chung Seo.
CHES 2025, 2025. [doi] [pdf] [code] [slides]
- [C7] Vectorized Implementation of Crystals-Kyber on NEON Extension.
YoungBeom Kim, Seog Chung Seo.
MobiSec 2023, 2023. [doi] [pdf]

- [C6] Optimized Kyber Implementation on 16-bit MSP430 Microcontroller.
DongHyun Shin, **YoungBeom Kim**, Seog Chung Seo.
MobiSec 2023, 2023. [doi] [pdf]
- [C5] PQWAVE-MHT: Post-Quantum Secure WAVE Protocol Based on Merkle Hash Tree for Secure V2X Communication.
YoonSun Han, **YoungBeom Kim**, Seog Chung Seo.
MobiSec 2023, 2023. [doi] [pdf]
- [C4] Simulation of Vehicle-to-Vehicle Communication Based on Selected PQC-DSA.
YoungBeom Kim, Seog Chung Seo.
MobiSec 2022, 2022. [doi] [pdf]
- [C3] Parallel Implementation of PIPO Block Cipher on 32-bit RISC-V Processor.
YuJin Kwak, **YoungBeom Kim**, Seog Chung Seo.
WISA 2021, 2021. [doi] [pdf]
- [C2] Efficient Implementation of SHA-3 Hash Function on 8-bit AVR-Based Sensor Nodes.
YoungBeom Kim, Hojin Choi, Seog Chung Seo.
ICISC 2020, 2020. [doi] [pdf]
- [C1] An Efficient Implementation of AES on 8-bit AVR-Based Sensor Nodes.
YoungBeom Kim, Seog Chung Seo.
WISA 2020, 2020. [doi] [pdf]

International Journal Papers

- [J18] A Hardware/Software Co-Optimization of HQC Using Tightly-Coupled Accelerators on a 32-bit Ibex Core.
Seog Chung Seo, **YoungBeom Kim**[†].
IEEE Transactions on Circuits and Systems II, SCIE, Q1, IF 4.9, 2026. [doi] [pdf]
- [J17] Accelerating SMAUG-T using the number theoretic transform on modern high-end CPUs.
WooHyung Ko, **YoungBeom Kim**, Seog Chung Seo.
ETRI Journal, SCIE, Q3, IF 2.0, 2026. [doi] [pdf] [code]
- [J16] Accelerating ALTEQ with Hardware-Software Co-Design on FPGA.
Youngel Choi, Jaesok Kim, **YoungBeom Kim**, Seog Chung Seo.
IEEE Access, SCIE, Q2, IF 4.2, 2025. [doi] [pdf]
- [J15] Vectorized Implementation of Kyber and Dilithium on 32-bit Cortex-A Series.
YoungBeom Kim, Seog Chung Seo.
IEEE Access, SCIE, Q2, IF 3.6, 2024. [doi] [pdf]
- [J14] KpqBench: Performance and Implementation Security Analysis of KpqC Competition Round 1 Candidates.
Yongryel Choi, Mingi Kim, **YoungBeom Kim**, Jingyo Song, Jaehwan Jin, Heeseok Kim, Seog Chung Seo.
IEEE Access, SCIE, Q2, IF 3.6, 2024. [doi] [pdf]
- [J13] Optimized Implementation of SMAUG-T on Resource-Constrained 16-bit MSP430 MCU.
MinGi Kim, DongHyun Shin, WooHyung Ko, **YoungBeom Kim**, Seog Chung Seo.
ICT Express, SCIE, Q2, IF 4.2, 2024. [doi] [pdf]
- [J12] Optimizing Crystals-Dilithium Implementation in 16-bit MSP430 Environment Utilizing Hardware Multiplier.
DongHyun Shin, **YoungBeom Kim**, Seog Chung Seo.
ICT Express, SCIE, Q2, IF 4.2, 2024. [doi] [pdf]
- [J11] Signature Split Method for a PQC-DSA Compliant with V2V Communication Standards.
YoungBeom Kim, Seog Chung Seo.
Applied Sciences, SCIE, Q1, IF 2.5, 2023. [doi] [pdf]
- [J10] Accelerating Falcon on ARMv8.
YoungBeom Kim, Jingyo Song, Seog Chung Seo.
IEEE Access, SCIE, Q2, IF 3.9, 2022. [doi] [pdf]
- [J9] Crystals-Dilithium on ARMv8.
YoungBeom Kim, Jingyo Song, Seog Chung Seo.
Security and Communication Networks, SCIE, Q3, IF 1.968, 2022. [doi] [pdf]

- [J8] Optimized Implementation of PIPO Block Cipher on 32-bit ARM and RISC-V Processors.
YoungBeom Kim, Seog Chung Seo.
IEEE Access, SCIE, Q2, IF 3.9, 2022. [doi] [pdf]
- [J7] Chaining Optimization Methodology: A New SHA-3 Implementation on Low-End Microcontrollers.
YoungBeom Kim, Taek-Young Youn, Seog Chung Seo.
Sustainability, SSCI, Q2, IF 3.889, 2021. [doi] [pdf]
- [J6] Efficient Implementation of AES and CTR_DRBG on 8-bit AVR-Based Sensor Nodes.
YoungBeom Kim, Seog Chung Seo.
IEEE Access, SCIE, Q2, IF 3.476, 2021. [doi] [pdf]
- [J5] High-Speed Fault Attack Resistant Implementation of PIPO Block Cipher on ARM Cortex-A.
 Jingyo Song, **YoungBeom Kim**, Seog Chung Seo.
IEEE Access, SCIE, Q2, IF 3.476, 2021. [doi] [pdf]
- [J4] High-Speed Implementation of PRESENT on AVR Microcontroller.
 Hyeokdong Kwon, **YoungBeom Kim**, Seog Chung Seo, Hwajeong Seo.
Mathematics, SCIE, Q1, IF 2.592, 2021. [doi] [pdf]
- [J3] Efficient Implementation of ARX-Based Block Ciphers on 8-bit AVR Microcontrollers.
YoungBeom Kim, Hyeokdong Kwon, SangWoo An, Hwajeong Seo, Seog Chung Seo.
Mathematics, SCIE, Q1, IF 2.258, 2020. [doi] [pdf]
- [J2] Parallel Implementations of ARX-Based Block Ciphers on Graphic Processing Units.
 SangWoo An, **YoungBeom Kim**, Hyeokdong Kwon, Hwajeong Seo, Seog Chung Seo.
Mathematics, SCIE, Q1, IF 2.258, 2020. [doi] [pdf]
- [J1] Designing a CHAM Block Cipher on Low-End Microcontrollers for Internet of Things.
 Hyeokdong Kwon, SangWoo An, **YoungBeom Kim**, Hyunji Kim, Seung Ju Choi, Kyoungbae Jang, Jaehoon Park, Yunjun Kim, Seog Chung Seo, Hwajeong Seo.
Electronics, SCIE, Q3, IF 2.397, 2020. [doi] [pdf]

HONORS & AWARDS

2024	First Prize (NIS Director's Award) , National Cryptography Contest <i>PQ-MSP: Faster Keccak, Kyber, and Dilithium on MSP430 Microcontroller for Quantum-Secure IoT Communication</i>
2024	Honorable Mention , National Cryptography Contest <i>Optimization Methods of NTT-Unfriendly Ring Based PQC Algorithms on 16-bit MSP430 MCU</i>
2023	First Prize (NIS Director's Award) , National Cryptography Contest <i>Performance and Implementation Security Analysis of KpqC Competition Round 1 Candidate</i>
2023	First Prize (NIS Director's Award) , National Cryptography Contest <i>Optimized Crystals-Kyber on 8-bit AVR-based Sensor Nodes</i>
2021	Second Prize (KISA President's Award) , National Cryptography Contest <i>PQ-BSM: Optimized PQC-DSA Software for Securing BSM Messages on V2X Environment</i>
2020	First Prize (NIS Director's Award) , National Cryptography Contest <i>ARX-based Korean Block Ciphers with CTR Mode and CTR DRBG on Embedded Processors and GPU</i>
2020	Special Prize (KIISC President's Award) , National Cryptography Contest <i>Efficient Implementations of AES and CTR_DRBG on 8-bit AVR-based Sensor Nodes</i>
2020	Special Prize (KIISC President's Award) , National Cryptography Contest <i>Efficient Implementations of SHA-3 Hash Function for Various Platforms</i>

ACADEMIC SERVICE

2027	CASCADE · Program Committee (PC)
2027	CHES · Artifact Evaluation Committee (AEC)
2025, 2026	CHES · External Artifact Reviewer

SKILLS

Programming	C, Assembly (ARMv7/v8 incl. NEON, AVR, MSP430, RISC-V), Python
Embedded & HW	Bare-metal optimization on 8-/16-/32-bit MCUs · FPGA HW/SW co-design (Xilinx Vivado/Vitis) · tightly-coupled accelerator design
Cryptography	PQC implementation (ML-KEM/ Kyber, ML-DSA/ Dilithium, Falcon, HQC, HAETAΕ, SMAUG-T) · symmetric primitives (AES, SHA-3, ARX ciphers) · constant-time and fault-resistant coding · KCMVP/CMVP

LANGUAGES

Korean (native) · English (intermediate)