Dongwoo Kang

Homepage | redr1102@korea.ac.kr

Summary

I am a Ph.D. student at Korea University working in cryptography, with a primary focus on the security evaluation of symmetric-key primitives under realistic implementation-level threats.

Research Interests

My research interests lie broadly in the design, analysis, and secure implementation of cryptographic systems. I am particularly interested in understanding how cryptographic primitives behave under realistic adversarial models and how theoretical security notions translate into practical security guarantees.

More generally, I aim to study cryptographic mechanisms that provide strong security assurances in real-world environments. My long-term research goal is to contribute to the development of robust and trustworthy cryptographic infrastructures across diverse application domains.

Education

2025 - present Ph.D. Student (Integrated M.S./Ph.D. Program) in Cybersecurity at **Korea University**
2021 - 2025 B.S. in Mathematics at **Korea University** (GPA: 3.71/4.5)

Publications

Kang, Dongwoo, Inhun Lee, et al. (2025). "Side-Channel Attack on Tweakable Block Cipher SCARF for Cache Address Randomization". In: *Proceedings of the 2025 Winter Conference of the Korea Institute of Information Security & Cryptology (KIISC)*. in Korean.

Kang, Dongwoo et al. (2025). "Full-round Linear Attacks for Block Cipher DNA-PRESENT". In: *Proceedings of the 2025 Summer Conference of the Korea Institute of Information Security & Cryptology (KIISC)*. in Korean.

Kang, Dongwoo, Hanbeom Shin, DongHyeon Kim, et al. (2026). Manuscript under review.

Awards

Encouragement Award 2025 Cryptographic Analysis Contest, Korea Institute of Information Security & Cryptology (KIISC)

Skills

Programming	C, Python.
Tools	Chipwhisperer.
AI-assisted Research	Experience integrating large language models into research workflows for literature review, code prototyping, and scholarly writing support.