Dongwoo Kang

Homepage | redr1102@korea.ac.kr

Summary

I am a Ph.D. student at Korea University working in cryptograhpy, with a primary focus on the mathematical and implementation-level cryptanalysis on Arithmetization-Oriented Primitives for Zero-Knowledge Proofs (ZKP).

Research Interests

My research interests originally focused on the analysis of block ciphers, particularly in understanding their mathematical structures and resistance against implementation attacks such as side-channel and fault attacks. Building upon this background, my interests have gradually expanded toward arithmetization-oriented cryptographic primitives for ZKPs, where both mathematical properties and implementation aspects play critical roles.

I am particularly interested in analyzing these primitives from both mathematical and implementation perspectives, emphasizing the need to integrate considerations of implementation attacks into the primitive design process. While countermeasures such as masking and hiding are effective techniques against side-channel leakage, my long-term research goal is to design cryptographic primitives whose underlying structures are inherently resilient to implementation attacks.

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)
	B.E. in Smart Security at **Korea University** (Double Major)	
	Micro Degree in Cryptographic Technology at **Korea University**	

International Publications

Dongwoo Kang Hanbeom Shin, DongHyeon Kim et al. (2026). "SDDT: An Operation Skip Attack Framework for Bitslice Ciphers—Validated on PIPO". In: *Selected Areas in Cryptography*. To appear.

Dongwoo Kang, Jaesik Kang and Seungwoon Lee (2024). *Defense Mechanism Using Purifier and Detector Against Adversarial Patch Attacks for Unmanned Combat Systems*. Poster presented at WISA 2024.

Domestic Publications

Dongwoo Kang, HeeSeok Kim and Seokhie Hong (2026). "Epoch-based Re-keying for Full Disk Encryption to Avoid Cumulative Side-channel Leakage". In: *Proceedings of the 2026 Summer Conference of the Korea Institute of Information Security & Cryptology (KIISC)*. in Korean.

Dongwoo Kang Inhun Lee, HeeSeok Kim and Seokhie Hong (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.

Dongwoo Kang, Hanbeom Shin and Seokhie Hong (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.

* Earlier publications may appear under the name Dongu Kang or Dong-u Kang.

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.