Won Geun Shin

+82-10-5020-5061 | shinryan9@korea.ac.kr | persShins

South Korea

Education

- **Korea University** *March 2024 - On Going*
  Ph.D Student South Korea
  - GPA: 4.3/4.5

- **Korea University** *March 2018 - Feb 2024*
  Bachelor's degree South Korea
  - GPA: 4.0/4.5

Publications

D=Domestic, I=International, C=Conference, J=Journal

[I.C.1] **Won Geun Shin**, JeongHwan Lee, Sangyun Jung, HeeSeok Kim. (2026). **ARMOR: First Order Masking of Activation and ArgMax Gadgets for Side Channel Resistant Neural Networks**. In *IACR Transactions on Cryptographic Hardware and Embedded Systems 2026.2 (2026)*, Accepted.

[I.C.2] MinAh Chae, **Won Geun Shin**, SangYun Jung, JiHun Yeom, DongHo Jeon, HeeSeok Kim. (2024). **The Threat of Password Guessing Attacks Exploiting Linguistic Characteristics: A Case Study on the Korean Domains**. In *2024 Silicon Valley Cybersecurity Conference (SVCC)*, IEEE.

[D.J.1] JeongHwan Lee, Sang-Yun Jung, **Won Geun Shin**, Sujin Park, HeeSeok Kim. (2023). **Trends in Side-Channel Countermeasures for LWE-like KEM and Digital Signature Schemes**. In *Review of KIISC* 33.3: 85-96.

[D.C.1] **Won Geun Shin**, Seunghyeon Jeon, HeeSeok Kim. (2025). **Optimizing Side-Channel Leakage Assessment with Accumulated Distributed Algorithms**. In *CISC-W'25*.

[D.C.2] **Won Geun Shin**, Sang-Yun Jung, HeeSeok Kim. (2023). **Side-Channel Countermeasure for Binary Neural Network Protection**. In *CISC-S'23*.

Honors and Awards

- **KIISC President's Award** 2025
  CISC 2025
- **Best Poster Awards** 2024
  IEEE SVCC 2024
- **Signal Processing Research Institute President's Award** 2023
  9th Crypto Contest
- **777 Command Commander Award** 2022
  8th Crypto Contest
- **KISA President's Award** 2023
  CISC 2023
- **ETRI President's Award** 2022
  Second Place in 5th Side-Channel Analysis Competition

Patent

1. HeeSeok Kim, Won Geun Shin, SangYun Jung (2024). **Side Channel Countermeasure for Activation Function of Binarized Neural Network** . Korean Patent No. 10-2024-0202916.

Talks

1. **Side-Channel Countermeasures and Security Evaluation**. In *Side Channel Analysis Tutorial (Workshop on Side Channel Analysis)* 2025 July 1.

PROJECTS

- **A Study of Emerging Security Attack Techniques and Their Implementation on Commercial Chips** — Oct 2025 - On Going
  - Side-Channel Attacks, Deep Learning
- **A Study on Physical Channel-based Hardware Vulnerability Validation of IoT Devices in a Black Box Environment** — May 2024 – Ongoing
  - Fault Attacks, IoT Devices
- **Development of chip integrity and system security verification technology to ensure the safety of the HW supply chain** — June 2024 - On Going
  - Side-Channel Attacks
- **Fault Injection Analysis of KpqC-Selected PQC Implementations** — Apr 2025 - Oct 2025
  - Fault Attacks, PQC
- **Empirical Study of Non-Invasive Countermeasures for Public-Key Cryptography on Commercial Platforms** — Apr 2025 - Oct 2025
  - Side-Channel Attacks
- **A Study on Security Vulnerabilities of Modern Processors Applicable to High-Risk Loss Environments** — May 2024 - Oct 2024
  - Side-Channel Attacks
- **Development of Physical Channel Vulnerability-based Attacks for Reliable On-Device Deep Learning Accelerator Design** — Jan 2022 – Dec 2024
  - Side-Channel Countermeasure, Side-Channel Attacks
- **Development of High-Performance Deep Learning-Based Side-Channel Analysis and Automation Techniques** — Mar 2022 – Feb 2023
  - Side-Channel Attacks, Deep Learning
- **A Study on Recent Trends in Fault Generation Mechanisms for Fault Injection Attacks** — Apr 2022 – Oct 2022
  - Fault Attacks