Dongjae Lee

Assistant Professor

Email: dongjae.lee@kangwon.ac.kr

Updated: 2025.01.08.

RESEARCH INTEREST

· Symmetric Cryptology & Quantum Cryptanalysis

EDUCATION

· **Korea University**, Seoul, Republic of Korea — Sep.2017 - Aug.2023
Ph.D. in Cybersecurity
Supervisor: Prof. Soekhie Hong (shhong@korea.ac.kr)
Ph.D. Thesis: **Practical Ciphertext-Only Attack on GMR Satellite Communication System**

· **Korea University**, Seoul, Republic of Korea — Mar.2012 - Feb.2016
B.Eng. in Cyber Defense
Supervisor: Prof. Soekhie Hong (shhong@korea.ac.kr)

· **Korea Science Academy (KSA) of KAIST**, Busan, Republic of Korea — Mar.2009 - Feb.2012
Math & Science specialized high school

WORK EXPERIENCE

· **Kangwon National University** — Sep.2024 – Present
Assistant Professor at Department of Convergence Security

· **Institute of Cyber Security & Privacy (ICSP)** at Korea University, Republic of Korea — Sep.2023 – Aug.2024
Postdoctoral Researcher
- Research on symmetric cryptology and quantum cryptanalysis

· **Defense Security Agency (DSA)**, Republic of Korea — Aug.2019 - May.2023
Special Cryptanalysis Officer / Army Captain
- Cryptanalysis and Signal Analysis

· **Agency for Defense Development (ADD)**, Seoul, Republic of Korea — Jul.2016 - Jul.2019
Researcher / Army Lieutenant
- Research on Forensics and Cyber Threat Intelligence (CTI)

PUBLICATIONS

International Journal & Conference Papers

· **Redefining Security in Shadow Cipher for IoT Nodes: New Full-Round Practical Distinguisher and the Infeasibility of Key-Recovery Attacks**
Sunyeop Kim, Myoungsu Shin, Seonkyu Kim, Hanbeom Shin, Insung Kim, Donggeun Kwon, **Dongjae Lee**, Seonggyeom Kim, Deukjo Hong, Jaechul Sung, and Seokhie Hong
IEEE Internet of Things Journal (2024), DOI: 10.1109/JIOT.2024.3491138

· **Improved Quantum Rebound Attacks on Double Block Length Hashing with Round-Reduced AES-256 and ARIA-256**
Dongjae Lee and Seokhie Hong
IACR Transactions on Symmetric Cryptology (2024), DOI: 10.46586/tosc.v2024.i3.238-265

· **Accurate False-Positive Probability of Multiset-based Demirci-Selçuk Meet-in-the-middle Attacks**
Dongjae Lee, Deukjo Hong, Jaechul Sung, and Seokhie Hong
IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences (2024), DOI: 10.1587/transfun.2023EAP1145

· **A Practical Ciphertext-Only Attack on GMR-2 System**
Dongjae Lee, Jaewoo Kim, Deukjo Hong, Jaechul Sung, and Seokhie Hong
IEEE Access (2023), DOI: 10.1109/ACCESS.2023.3271994

· **Improved Ciphertext-Only Attack on GMR-1**
Dongjae Lee, Deukjo Hong, Jaechul Sung, Seonggyeom Kim, and Seokhie Hong
IEEE Access (2021), DOI: 10.1109/ACCESS.2021.3139614

Domestic Journal & Conference Papers

· **Byte-wise equal property of the ARADI cipher**
Sunyeop Kim, Seonkyu Kim, Myoungsu Shin, Insung Kim, Hanbeom Shin, Donggeun Kwon, Byoungjin Seok, **Dongjae Lee**, Deukjo Hong, Jaechul Sung, and Seokhie Hong
KIISC Conference on Information Security and Cryptography Winter (2024)

· **New Square Attack with Partial Sums and FFT Technique on 6-round AES**
Hanbeom Shin, Seonkyu Kim, Myoungsu Shin, Insung Kim, Sunyeop Kim, Donggeun Kwon, Byoungjin Seok, **Dongjae Lee**, Deukjo Hong, Jaechul Sung, and Seokhie Hong
KIISC Conference on Information Security and Cryptography Winter (2024)

· **New Linear Distinguisher for Reduced-Round LEA**
Myoungsu Shin, Seonkyu Kim, Hanbeom Shin, Insung Kim, Sunyeop Kim, Donggeun Kwon, Byoungjin Seok, **Dongjae Lee**, Deukjo Hong, Jaechul Sung, and Seokhie Hong
KIISC Conference on Information Security and Cryptography Winter (2024)

· **Complexity Analysis of Key Committing Attacks on AES-based AEAD Scheme**
Seonkyu Kim, Myoungsu Shin, Hanbeom Shin, Insung Kim, Sunyeop Kim, Donggeun Kwon, Byoungjin Seok, **Dongjae Lee**, Deukjo Hong, Jaechul Sung, and Seokhie Hong
KIISC Conference on Information Security and Cryptography Winter (2024)

· **Differential and Differential Meet-In-The-Middle Attack on PIPO**
Insung Kim, Hanbum Shin, Sunyeop Kim, Seonkyu Kim, Myoungsu Shin, Donggeun Kwon, **Dongjae Lee**, Seonggyeom Kim, Deukjo Hong, Jaechul Sung, and Seokhie Hong
KIISC Conference on Information Security and Cryptography Summer (2023)

· **Real-time Cyber Threat Intelligent Analysis and Prediction Technique**
Changwan Lim, Youngsup Shin, **Dongjae Lee**, Sungyoung Cho, Insung Han, and Haengrok Oh
KIISE Transactions on Computing Practices (2019), DOI: https://doi.org/10.5626/KTCP.2019.25.11.565

· **A study of real-time cyber threat intelligent analysis and prediction technique**
Changwan Lim, Youngsup Shin, **Dongjae Lee**, Sungyoung Cho, Insung Han, and Haengrok Oh
Proceedings of the Korean Information Science Society Conference (2018)

RESEARCH EXPERIENCE

· Development of an efficient isogeny-based public key cryptography on various computational environment, National Research Foundation of Korea (NRF)
Jun.2023. – Aug.2024.

· Study on Quantum Security Evaluation of Cryptography based on Computational Quantum Complexity, Institute for Information & communication Technology Planning & evaluation (IITP)
Jun.2023. – Aug.2024.

· eMRAM based highly reliable and lower power authentication hardware design, Institute for Information & communication Technology Planning & evaluation (IITP)
Jun.2023. – Aug.2024.

· Confidential Research, Defense Security Agency (DSA), Republic of Korea
Apr.2013. – Nov.2013.

OTHER EXPERIENCE

· Completed KITRI Next-generation security leader training program (Best of Best) (2012)

AWARDS & HONORS

· Full Tuition Scholarship (Korea University), 2012 – 2016
Ministry of National Defense, Republic of Korea