

Suhyeon Lee

Seoul, Republic of Korea • orion-alpha_at_korea.ac.kr • <https://suhyeonlee.com>

PROFESSIONAL SUMMARY

Blockchain security researcher with a focus on incentive design and game-theoretic analysis of blockchain protocols. My work spans security and economic vulnerabilities in Layer 2 systems and PoW/PoS blockchains, with results presented at venues including AFT, ICBC, and WTSC. Currently a Visiting Research Fellow at Hashed Open Research, with prior experience as a Security Researcher at Tokamak Network, a Singapore-based Ethereum Layer 2 company. I have taught a graduate-level blockchain course at Korea University. Prior to academia, I served seven years as an officer in the Republic of Korea Army at the Agency for Defense Development and the ROK Cyber Operations Command.

EDUCATION

Sep. 2017 – Feb. 2023 **Ph.D. in Cybersecurity**

Department of Information Security, School of Cybersecurity, Korea University

Supervisor: Prof. Seungjoo Kim

Thesis: Revisiting Conventional Wisdom in PoW and PoS-based Blockchains

Mar. 2012 – Feb. 2016 **B.Eng. in Cyber Defense**

Department of Cyber Defense, Korea University

Supervisor: Prof. Jong In Lim

PROFESSIONAL EXPERIENCE

Nov. 2025 – **Visiting Research Fellow**

Hashed Open Research

- Contributing to project-based research and reports on blockchain and cryptocurrency

June. 2023 – Mar. 2026 **Security Researcher**

Tokamak Network

- Security research focusing on Layer 2 blockchain systems

Sep. 2024 – Aug. 2025 **Adjunct Professor**

School of Cyber Security, Korea University

- Teaching a regular lecture SCS606 "Blockchain and Cryptocurrency"

Jul. 2019 – May. 2023 **Research Officer / Army Captain**

ROK Cyber Operations Command

- Participated in Korea-US joint military exercises and inter-agency cooperation.

- Led multiple cyber defense R&D projects including system design, cryptography, and AI technologies.

Jul. 2016 – Jul. 2019 **Researcher / Army Lieutenant**

2nd R&D Institute, Agency for Defense Development (ADD)

- Participated in R&D for collecting and processing Cyber Threat Intelligence (CTI).

- Participated in R&D for development of secure Real Time Operation System (RTOS) for weapon systems with high security verification (EAL \geq 4).

PROFESSIONAL SERVICE

Program Committee

WTSC 2026 – 10th Workshop on Trusted Smart Contracts (in association with Financial Cryptography 2026)

ICBC 2026 – IEEE International Conference on Blockchain and Cryptocurrency

ICDCS 2026 – 46th IEEE International Conference on Distributed Computing Systems

External Reviewer

Industry Presentations

ETHCC 2026, ETHCC 2025, ETHSofia 2024, ETHTokyo 2024, ETHVenice 2024

WORKING PAPERS (Preprint)

S. Lee et al., "Commit-Reveal²: A Deployable Randomness Beacon with a Robust Accountability Framework for Smart Contracts," *IEEE Transactions on Dependable and Secure Computing (TDSC)*, under revision.

S. Lee, and Y. Park, "Looking for Attention: Attention Test Design for Validator Monitoring in Optimistic Rollups," *arXiv:2505.24393*, June 2025.

S. Lee, and H. Kim, "Inside Qubic's Selfish Mining Attack in Monero: Evidence, Tactics, and Limits," *arXiv:2512.01437*, December 2024.

PUBLICATIONS – INTERNATIONAL CONFERENCES

S. Lee, D. Nguyen, and D. Lee, "(Im)possibility of Incentive Design for Challenge-based Blockchain Protocols," *In Proceedings of the 10th Workshop on Trusted Smart Contracts (WTSC 2026)*, in association with *Financial Cryptography 2026*, pp. TBD, St. Kitts, Saint Kitts and Nevis, March 6, 2026.

S. Lee, "180 Days After EIP-4844: Will Blob Sharing Solve Dilemma for Small Rollups?," *In Proceedings of the DICG Workshop*, in association with the *45th IEEE International Conference on Distributed Computing Systems (ICDCS 2025)*, pp. TBD, Glasgow, UK, July 20–23, 2025.

S. Lee, and E. Gee, "Commit-Reveal²: Randomized Reveal Order Mitigates Last-Revealer Attacks in Commit-Reveal," *In Proceedings of the IEEE International Conference on Blockchain and Cryptocurrency (ICBC 2025)*, pp. TBD, Pisa, Italy, June 2-6, 2025.

S. Lee, "Hollow Victory: Analysis on Challenger's Incentive in Optimistic Rollup Dispute Game," *In Proceedings of the 9th Workshop on Trusted Smart Contracts (WTSC 2025)*, in association with *Financial Cryptography 2025*, pp. TBD, Miyakojima, Japan, April 18, 2025.

H. Yang, **S. Lee**, and S. Kim, "A Tip for IOTA Privacy: IOTA Light Node Deanonymization via Tip Selection," *In Proceedings of the International Conference on IEEE Blockchain Conference (ICBC 2024)*, Dublin, Ireland, May 2024.

S. Lee, and S. Kim, "Do You Really Need to Disguise Normal Servers as Honeypots?," *In Proceedings of the 40th International Conference on IEEE Military Communications Conference (MILCOM 2022)*, pp. 166-172, Rockville, MD, US, November 2022.

S. Lee, D. Lee, and S. Kim, "Block Double-Submission Attack: Block Withholding Can Be Self-Destructive," *In Proceedings of the 4th International Conference on ACM Advances in Financial Technologies (AFT '22)*, Cambridge, MA, US, September 2022.

S. Lee and S. Kim, "Proof-of-Stake at Stake: Predatory, Destructive Attack on PoS Cryptocurrencies," *In Proceedings of ACM MobiCom 2020 Workshops – the 3rd International Workshop on Cryptocurrencies and Blockchains for Distributed Systems (CryBlock '20)*, pp. 7-11, Virtual Conference, September 2020.

S. Lee and S. Kim, "Blockchain for Cyber Defense: Will It Be as Good as You Think?" *the 28th DEF CON Hacking Conference (DEFCON 28) – the 2nd Blockchain Village*, Virtual Conference, August 2020.

S. Lee and S. Kim, "Countering Block Withholding Attack Efficiently," *In Proceedings of IEEE INFOCOM 2019 Workshops – the 2nd International Workshop on Cryptocurrencies and Blockchains for Distributed Systems (CryBlock '19)*, pp. 330-335, Paris, France, May 2019.

PUBLICATIONS – INTERNATIONAL JOURNALS

S. Lee, E. Jee, J. Lee, "Implementation of Cost-Effective Verification for Pietrzak's Verifiable Delay Function in Ethereum Smart Contracts," *Blockchain: Research and Applications (I/F 5.6)*, In Press, June 2025.

S. Lee and S. Kim, "Shorting Attack: Predatory, Destructive Short Selling on Proof-of-Stake Cryptocurrencies," *Concurrency and Computation: Practice and Experience (I/F 2)*, vol. 35, Issue 16, e6585, July 2023.

S. Lee and S. Kim, "Rethinking Selfish Mining under Pooled Mining," *ICT Express (I/F 4.754)*, vol. 9, Issue 3, pp. 356-361, June 2023.

S. Lee, H. K. Kim, and K. Kim, "Ransomware Protection using the Moving Target Defense Perspective," *Computers & Electrical Engineering (I/F 4.152)*, vol. 78, pp. 288-299, September 2019.

PATENTS

- S. Kim and **S. Lee**, "Method for generating to tag for tracking document," submitted, May 2022.
- H. Kim, K. Kim, and **S. Lee**, "Ransomware damage prevention method through extension randomization, recording medium and apparatus for performing the method," no. 10-2316404, October 2021.
- S. Kim and **S. Lee**, "A block withholding attack detection device and its operation method," no. 10-2122824, June 2020.
- S. Kim and **S. Lee**, "Mining pool management server capable of suppressing selfish mining strategies of competitive mining pools and method of operation," no. 10-2154354, September 2019.
- D. Lee, B. Ko, C. Lim, D. Kim, H. Ryu, **S. Lee**, and J. Park, "Device and method for extracting web page information through inference and learning of html tag information," no. 10-2018-0137256, December 2018.

INVITED TALKS

- Suhyeon Lee, "Research and Experience in Cyber Defense," Capstone Project in the Department of Cyber Defense, Korea University, Seoul, April 2023.
- Suhyeon Lee, "Threat Modeling for Cybersecurity of Industrial Products," 78ResearchLab, Gangnam-gu, Seoul, October 2022.
- Suhyeon Lee, "Shorting Attack on Proof-of-Stake Cryptocurrencies," Monthly Crypto Seminar in Ripple, Virtual, July 2022.
- Suhyeon Lee, "Blockchain Technology for Military Cyber Security," The 28th Network Security Conference Korea (NetSec-KR), COEX, Seoul, Korea, April 2022.
- Suhyeon Lee, "K-Cyber Security Challenge Winner's Talk," Conference Center of the Federation of Korean Industries, Seoul, December 2019.

LANGUAGE & ADDITIONAL SKILLS

- Language: Korean (native), English (proficient)
- Programming: C, Python (familiar)
- Certification: Certified Information Systems Security Professional (CISSP), Certification for English Mediated Instruction (Awarded by the Center for Teaching and Learning of Korea University)

AWARDS & HONORS

- Dec. 2019 **1st Prize in Korea Security Data Challenge (AI Section)**
Granted by Korea Internet & Security Agency (KISA)
- 2012 – 2016 **Full-tuition Military Scholarship**
Granted by Ministry of National Defense, Republic of Korea
- 2012 – 2016 **Merit-based Scholarship**
Granted by Korea University, Republic of Korea
- 2017 – 2019 **General Scholarships**
Granted by Korea University, Republic of Korea

REFERENCES

Professor. Seungjoo Kim (PhD Supervisor)

- School of Cybersecurity, Korea University, Republic of Korea
- President of Office of Digital Information, Korea University
- Member of Republic of Korea Presidential Defense Innovation Committee

Professor. Huy Kang Kim

- School of Cybersecurity, Korea University, Republic of Korea
- Director of Hacking and Countermeasure Research Lab (<https://ocslab.hksecurity.net>)

Senior Researcher. Donghwan Lee

- Agency for Defense Development, Republic of Korea

Chair-Professor. Jongin Lim

- School of Cybersecurity, Korea University, Republic of Korea
- Advisor of Kim & Chang Law Firm, Republic of Korea
- Former Special Advisor to the President for National Security