Mincheol **Son**

encrypted.def@gmail.com | encrypted.gg | encrypted-def | @baaaaaarkingdog | Mincheol Son

Publications

Shorter VOLE-in-the-Head-based Signatures from Vector Semi-Commitment *Preprint*
S Kim, B Lee, and M Son *Jun 2025*

Polocolo: A ZK-Friendly Hash Function Based on S-boxes Using Power Residues *Eurocrypt 2025*
J Ha, S Hwang, J Lee, S Park, and M Son *May 2025*

Relaxed Vector Commitment for Shorter Signatures *Eurocrypt 2025*
S Kim, B Lee, and M Son *May 2025*

FRAST: TFHE-friendly Cipher Based on Random S-boxes *ToSC 2024*
M Cho, W Chung, J Ha, J Lee, E Oh, and M Son *Sep 2024*

AIM: Symmetric Primitive for Shorter Signatures with Stronger Security* *CCS 2023*
S Kim†, J Ha†, M Son, B Lee, D Moon, J Lee, S Lee, J Kwon, J Cho, H Yoon, and J Lee *Nov 2023*

Mitigation on the AIM Cryptanalysis* *preprint*
S Kim, J Ha, M Son, and B Lee *Sep 2023*

The AIMer Signature Scheme *NIST PQC Additional Digital Signature Proposal*
J Cho, M Cho, J Ha, S Kim, J Kim, B Lee, J Lee, J Lee, D Moon, M Son, and H Yoon *Jun 2023*

Rubato: Noisy Ciphers for Approximate Homomorphic Encryption *Eurocrypt 2022*
J Ha, S Kim, B Lee, J Lee, and M Son *Jun 2022*

Study on digital signatures based on zero-knowledge proof for one-way function preimages *Master's thesis*
M Son *Jun 2022*

Author are listed alphabetically unless marked with an asterisk (*).

Authors listed with a dagger (†) contributed equally.

Talks

Polocolo: A ZK-Friendly Hash Function Based on S-boxes Using Power Residues

- Eurocrypt 2025, Madrid, Spain *May 2025*
- KSIAM 2025, Seoul, South Korea *May 2025*

Education

KAIST (Korea Advanced Institute of Science and Technology) *Daejeon, South Korea*
PhD in Cryptography *Sep 2022 - Aug 2026 (Expected)*

- Interested in Zero-knowledge Proof, and Post-Quantum Cryptography
- Advised by Prof. Jooyoung Lee

KAIST (Korea Advanced Institute of Science and Technology) *Daejeon, South Korea*
Master in Cryptography *Sep 2020 - Aug 2022*

- GPA 4.03/4.3
- Advised by Prof. Jooyoung Lee

Korea University *Seoul, South Korea*
B.S. in Cyber Defense *Mar 2016 - Feb 2020*

- GPA 4.19/4.5

Work Experiences

Samsung Research *Seoul, South Korea*
Security Research Intern *Jan 2018 - Feb 2018*

- Analyzed vulnerabilities within a black-box setting for embedded software developed in C#
- Identified logical and cryptographic flaws and reported them to software vendors

Extracurricular Activities

CTF

Challenge author *Feb 2022 - Present*

- Authored 20+ challenges in 6 CTFs, many are about cryptography (link)
- Addressed recent cryptographic topics in the challenges, such as ZKP, PQC, and recent vulnerabilities

Dreamhack (Hosted by Theori)

Lecturer *Aug 2020 - Nov 2020*

- Co-authored cryptography lectures (in Korean) in Dreamhack, a security community hosted by an offensive security company Theori
- Aims to cover both theoretical and practical aspects of cryptography (link)

Algorithm blog and Youtube

Lecturer and Creator *Dec. 2018 - Present*

- Curated algorithm lectures (in Korean) for personal algorithm blog and Youtube channel
- Covered 37 algorithm topics including arrays, linked lists, bfs, sorting, dynamic programming, graphs, and union-find
- The lectures are publicly viewable, not-for-profit, and has garnered 90,000+ views (link1) (link2)

Codeforces

Competitive Programmer *Sep 2016 - Oct 2020*

- Participated in 76 contests on Codeforces, a worldwide competitive programming platform
- Achieved rating 2410 (Top 0.7%) (Profile)

Honors & Awards

2024	**Grand Prize**, National Crypto Contest	*Seoul, South Korea*
2019-2023	**Finalist**, DEFCON 27-31 CTF Finals (CTF team CyKor, Super Guesser)	*Las Vegas, USA*
2022	**18th Place**, Quora Programming Challenge	*Online*
2018	**5th Place**, ACM-ICPC Hanoi Regional	*Hanoi, Vietnam*
2018	**6th Place**, ACM-ICPC Seoul Regional	*Seoul, South Korea*
2018	**1st Place**, Samsung Electronics Connect6 SW Algorithm Competition	*Seoul, South Korea*

Scholarship

Presidential Science Scholarship

Recipient *Apr 2016 - Feb 2020*

- Granted for selected 150 STEM students in nation each year
- Covered admission fee and full amount of school support fees

Writing

Blockchain & cryptography *Zellic*

- Introducing Polocolo: A ZK-Friendly Hash Function for PLONK with Lookup (Part 1)
- How Does Tornado Cash Work?
- ZK-Friendly Hash Functions
- Algebraic Attacks on ZK-Friendly Hash Functions
- CSPRNGs: How to Properly Generate Random Numbers

Computer science (in Korean) *Samsung Software Membership*

- Zero Knowledge Proof using AES
- TLS 1.3 Protocol
- Intel Intrinsics (SIMD) Guide
- Other posts