

Mincheol Son

CRYPTOGRAPHY RESEARCHER

✉ encrypted.def@gmail.com | 🏠 encrypted.gg | 💻 encrypted-def | 🐦 @baaaaaarkingdog | 🎓 Mincheol Son

Publications

AIM: Symmetric Primitive for Shorter Signatures with Stronger Security

Copenhagen, Denmark

CCS 2023

Nov. 2023 (To appear)

- S Kim, J Ha, **M Son**, B Lee, D Moon, J Lee, S Lee, J Kwon, J Cho, H Yoon, J Lee
- The first and second authors contributed equally to this work

The AIMER Signature Scheme

NIST PQC ADDITIONAL DIGITAL SIGNATURE SCHEMES PROPOSAL

Jun. 2023

- J Cho, M Cho, J Ha, S Kim, J Kim, B Lee, J Lee, J Lee, D Moon, **M Son**, H Yoon
- Authors names are listed alphabetically

Rubato: Noisy Ciphers for Approximate Homomorphic Encryption

Trondheim, Norway

EUROCRYPT 2022

Jun. 2022

- J Ha, S Kim, BH Lee, J Lee, **M Son**
- Authors names are listed alphabetically

Two papers are under review in PKC 2024 and EUROCRYPT 2024

Work Experiences

Samsung Research

Seoul, South Korea

SECURITY RESEARCH INTERN

Jan. 2018 - Feb. 2018

- Analyzed vulnerabilities of embedded system in a black box setting

Honors & Awards

2019-2023 **Finalist**, DEFCON 27-31 CTF Finals

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

- Participated in other various competitions and the total prize money is 27M KRW(≈23500 USD)

Writing

Blog posts about blockchain & cryptography

Zellic

WRITER

Apr. 2023 - Present

- How Does Tornado Cash Work? (link)
- ZK-Friendly Hash Functions (link)
- Algebraic Attacks on ZK-Friendly Hash Functions (link)
- CSPRNGs: How to Properly Generate Random Numbers (link)

Blog posts about computer science (written in Korean)

Samsung Software Membership

WRITER

Jan. 2019 - Jun. 2022

- Zero Knowledge Proof using AES (link)
- TLS 1.3 Protocol (link)
- Intel Intrinsics(SIMD) Guide (link)
- Cryptographic characteristics of Large S-box and Algebraic attacks (link)
- Other 31 posts (link)

Education

Korea University

Seoul, South Korea

B.S. IN CYBER DEFENSE

Mar. 2016 - Feb. 2020

- GPA 4.19/4.5

KAIST (Korea Advanced Institute of Science and Technology)

MASTER IN CRYPTOGRAPHY

- GPA 4.03/4.3
- Thesis title - Study on digital signatures based on zero-knowledge proof for one-way function preimages

Daejeon, South Korea

Sep. 2020 - Aug. 2022

KAIST (Korea Advanced Institute of Science and Technology)

PHD IN CRYPTOGRAPHY

- Interested in Zero-Knowledge Proof, Multi-Party Computation, and Post-Quantum Cryptography

Daejeon, South Korea

Sep. 2022 - Present

Extracurricular Activities

Author 20↑ Challenges at ctfs, mostly cryptography

CTF ORGANIZER

- Attacking ZK-SNARK-like protocol ([link](#))
- Challenges inspired by disclosed vulnerability of MEGA Cloud Storage ([link](#))
- Other 20 challenges ([link](#))

Feb. 2022 - Present

Author a basic cryptography & algorithm lecture

LECTURER

- Author a basic algorithm lecture at blog and youtube (Written in Korean) ([link](#))
- Author a basic cryptographic lecture at dreamhack (Written in Korean) ([link](#))

Dec. 2018 - Present

Presidential Science Scholarship

RECIPIENT

- Granted 60M KRW(≈52000 USD)

Apr. 2016 - Feb. 2020

Codeforces

COMPETITOR

- Rating 2410 (Grandmaster, Top 0.7%) ([link](#))

Sep. 2016 - Oct. 2020