BYEONGKYU HAN

Ph.D. Student in Computer Science, University of Illinois at Chicago

bhan26 at uic dot edu

personal website | LinkedIn | GitHub

Research Interests

My research focuses on applied cryptography for verifiable computation and privacy-preserving systems. I am particularly interested in designing zero-knowledge proof systems, including zk-SNARKs, and reducing their proof generation and verification costs for practical deployment. I aim to extend this work to privacy-preserving and verifiable AI, protecting sensitive information while verifying the correct execution of AI computations.

Education

University of Illinois at Chicago, Chicago, USA Sep 2026 - Present
Ph.D. in Computer Science (Advisor: Alexander R. Block)

Kookmin University, Seoul, South Korea Mar 2024 – Feb 2026
M.S. in Electronics Engineering (Advisor: Jihye Kim, Hyunok Oh)

Kookmin University, Seoul, South Korea Mar 2019 – Feb 2024
B.B.A in AI, Big Data, and Management; Minor in Computer Science

Experience

University of Illinois at Chicago Sep 2026 - Present
Graduate Research Assistant

Kookmin University & Hanyang University Sep 2023 - Feb 2024
Joint Research Intern — IT Security and Privacy & Security and Privacy Labs

Manuscripts

[1] Aegis: Near-Real-Time Dynamic Proof of Liabilities for Off-Chain Ledgers
Gweonho Jeong, Jaewoong Lee, Minhae Kim, **Byeongkyu Han**, Jihye Kim, Hyunok Oh
[*Paper*], [*Code*], [*Slides*]

Publications

[1] LAMP: Linear Verification of Matrix Multiplication via Proximity Testing
Kyeongtae Lee, **Byeongkyu Han**, Jihye Kim, Hyunok Oh
S&P 2027
[*Paper*], [*Code*]

Projects

A Privacy-Preserving STO system with Near-Real-Time PoL Mar 2024 – Oct 2024

- Proposed a STO system providing privacy preserving, near-real-time PoL, and high-throughput trading.
- Extended **Aegis** to STO and designed the system to comply with Korean regulatory requirements.
- Achieved proof generation of 0.5s for 128 trades; reached 2,000 TPS through system optimizations.
- This system evolved into *zkPoRL* by *zkrypto*
- Slides: [PDF]

Activity

Ethereum Core Contribution Program (Mentor) Jun 2025 - Aug 2025
ZK Education Team (ZKET), Ethereum Foundation

- Mentored participants in research and development of privacy and scaling technologies.
- Conducted sessions reviewing foundational papers on Groth16, KZG, PLONK and FRI.
- Facilitated special sessions on Circle STARK, FHE, and Privacy-Preserving AI.
- Provided hands-on sessions in building zk-SNARK circuits using Noir, Cairo, and Halo2.

Ethereum Core Contribution Program (Participant) Jun 2024 - Aug 2024
Privacy and Scaling Explorations (PSE), Ethereum Foundation

- Participated in an 8-week study with the PSE team at the Ethereum Foundation.
- Studied and analyzed foundational papers on Groth16, PLONK, and FRI.
- Implemented a privacy-preserving, verifiable voting system ensuring vote and tally integrity.

Honors and Awards

Special Prize, National Cryptography Paper Competition 2025
Korea Cryptography Forum, Korea Institute of Information Security & Cryptology, South Korea

- Category: Application and Utilization of Cryptographic Technologies.
- Related Manuscripts: [1]

University Scholarships 2024 – 2025

- Professor-Nominated Merit Scholarship ($9,500 total for 4 semesters)

Teaching Assistant

Embedded Systems for Next Generation Communications Fall 2025
Data Structures Fall 2025
Introduction to Programming Fall 2025
Object-Oriented Programming Spring 2024
Programming Language Spring 2024