

CONTACT INFORMATION Room 707, Natural Science Building, Hanyang University, 222 Wangsimni-ro, Seongdong-gu, Seoul, 04763, Republic of Korea

Homepage: [hyeonbumlee.github.io](https://github.com/hyeonbumlee)
 LinkedIn: www.linkedin.com/in/hyeonbum-lee
 ✉ E-mail: leehb3706@hanyang.ac.kr

RESEARCH BACKGROUND • **Cryptography:** Zero-Knowledge Proofs, SNARK, Proof System, Computation Theory

EDUCATION **Hanyang University**, Seoul Mar 2020 - Present

- Ph.D. Department of Mathematics
- Advisor: Prof. Jae Hong Seo.

Hanyang University, Seoul Mar 2014 - Feb 2018

- B.S. Department of Mathematics

RESEARCH PROJECTS **Zero-Knowledge Proofs & SNARK**

- **Logging and Zero-knowledge Proof based on Hierarchical Blockchain, Institute for Information and Communications Technology Promotion**
Supported by Institute of Information & Communications Technology Planning & Evaluation (IITP), Researcher, May 2022 - Apr 2023.
- **Research on the design technology of a cryptographic proof system suitable for Proof-Carrying Data**
Supported by National Security Research Institute (NSR), Researcher, Apr 2022 - Oct 2022.
- **A Study on Cryptographic Primitives for SNARK**
Supported by Institute of Information & Communications Technology Planning & Evaluation (IITP), Research Associate, Apr 2021 - Dec 2026.
- **Research on Incrementally Verifiable Computation Design Technique and Application Method**
Supported by National Security Research Institute (NSR), Researcher, Apr 2021 - Oct 2021.
- **Research on Post-Quantum Non-Interactive Zero-Knowledge Proofs**
Supported by National Research Foundation of Korea (NRF), Researcher, Mar 2020 - Feb 2025.
- **Research on Post-Quantum Zero-Knowledge Proofs Design Technique and Application Method**
Supported by National Security Research Institute (NSR), Researcher, Apr 2020 - Oct 2020.

Others

- **Secure Multi-party Approximate Computation**
Supported by Samsung Science & Technology Foundation, Researcher, Sep 2021 - Aug 2024.
- **A Study of Functional Encryption and Its Core Techniques**
Supported by Institute of Information & Communications Technology Planning & Evaluation (IITP) & National Research Foundation of Korea (NRF), Researcher, Mar 2020 - Jul 2021.

SELECTED PUBLICATIONS **Journal**

1. Chanyang Ju, **Hyeonbum Lee**, Heewon Chung, Jae Hong Seo, and Sungwook Kim, *Analysis of Zero-Knowledge Protocols for Verifiable Computation and Its Applications* Journal of The Korea Institute of Information Security & Cryptology VOL.31, NO.4, Aug. 2020
2. Chanyang Ju, **Hyeonbum Lee**, Heewon Chung, and Jae Hong Seo, *Efficient Sum-Check Protocol for Convolution* IEEE Access, VOL.9, pp.164047-164059, 2021, doi
3. Sungwook Kim, **Hyeonbum Lee**, Gwangwoon Lee, and Jae Hong Seo, *Sublinear Verifier Inner Product Argument under Discrete Logarithm Assumption* IEEE Transactions on Information Forensics and Security, VOL.18, pp.5332-5344, 2023, doi

4. Changhao Chenli, Wenyi Tang, **Hyeonbum Lee**, and Taeho Jung,
Fair2Trade: Digital Trading Platform Ensuring Exchange and Distribution Fairness
IEEE Transactions on Dependable and Secure Computing (Early Access), 2024, doi

Conference

1. Sungwook Kim, **Hyeonbum Lee**, Jae Hong Seo, [alphabetical order]
Efficient Zero-Knowledge Arguments in Discrete Logarithm Setting: Sublogarithmic Proof or Sublinear Verifier
ASIACRYPT 2022, Taipei, Taiwan, December 5–9, 2022, Proceedings, doi
2. **Hyeonbum Lee**, and Jae Hong Seo,
TENET : Sublogarithmic Proof and Sublinear Verifier Inner Product Argument without a Trusted Setup
IWSEC 2023, Yokohama, Japan, Aug 29-31, 2023, Proceedings, doi
3. **Hyeonbum Lee**, Kyuhwan Lee, Wenyi Tang, Shankha Shubhra Mukherjee, Jae Hong Seo, and Taeho Jung
PrivHChain: Monitoring the Supply Chain of Controlled Substances with Privacy-Preserving Hierarchical Blockchain
Poster Acceptance, IEEE ICBC 2024, Dublin, Ireland, May 27-31, 2024

Workshop

1. **Hyeonbum Lee**, and Jae Hong Seo,
On the Security of Nova Recursive Proof System
6th ZKProof Workshop, Berlin, Germany, May 22-24, 2024, ePrint

EXPERIENCE

Work Experience

- **Visiting Scholar**
 - Host : Prof. Taeho Jung
Institute : University of Notre Dame, IN
Period : Sep 1, 2022 - Mar 1, 2023
- **Teaching Experience**
 - Spring 2023: PBL: Cryptography, Teaching Fellow (Part-time Lecturer)
 - Spring 2022: Calculus I, Teaching Assistant
 - Spring 2021: Calculus I, Teaching Assistant
 - Fall 2020: Modern Algebra II, Teaching Assistant
 - Spring 2020: Modern Algebra I, Teaching Assistant

TALKS & PRE-SENTATIONS

Presentations

- *On the Security of Nova Recursive Proof System*
6th ZKProof Workshop, Berlin, May 24, 2024
- *On the Security of Nova IVC*
2024 KMS Spring Meeting, Daejeon, Apr 19, 2024
- *TENET : Sublogarithmic Proof and Sublinear Verifier Inner Product Argument without a Trusted Setup*
IWSEC 2023, Yokohama, Aug 30, 2023
- *Efficient Zero-Knowledge Arguments in Discrete Logarithm Setting : Sublogarithmic Proof or Sublinear Verifier*
Asiacrypt 2022, Taipei, Dec 07, 2022
- *Efficient zero-knowledge arguments in discrete logarithm setting without pairing: Sublinear verifier*
2022 KMS Spring Meeting, Virtual, Apr 28, 2022
- *Transparent and efficient zero-knowledge arguments from discrete log with better complexity*
2021 KMS Spring Meeting, Virtual, Apr 30, 2021

HONORS &
AWARDS

Awards

- ***Excellence Prize***, Best Research Paper Award for graduate students
The Research Institute for Natural Sciences, Hanyang University Feb 2024
- ***Grand Prize***, National Cryptographic Technology Contest.
Korea Cryptography Forum Oct 2022
- ***Special Prize***, National Cryptographic Technology Contest.
Korea Cryptography Forum Oct 2021, Oct 2023
- ***SUMMA CUM LAUDE***, Graduate Honors.
Hanyang University Feb 2018
- ***Dean's list***
College of Natural Science, Hanyang University 2016 (Fall)

Scholarships & Stipends

- **Teaching Assistant Scholarship**
Hanyang University
\$6000/year Sep 2020 - Aug 2022
- **Master and Ph.D Program Scholarship**
Hanyang University
Full tuition for 3 years (\approx \$12000/year) Mar 2020 - Feb 2023
- **Hanyang Excellent Scientist Scholarship**
Hanyang University
Full tuition for 4 years (\approx \$8000/year) Mar 2014 - Feb 2018

SERVICES

External Reviewer

- ASIACRYPT2023; PKC2023; ICISC 2021; ASIACRYPT 2021; PQCrypto 2021; APKC 2021; ProvSec 2020;