

CONTACT INFORMATION	Room 707, Natural Science Building, Hanyang University, 222 Wangsimni-ro, Seongdong-gu, Seoul, 04763, Republic of Korea	Homepage: <a href="https://github.com/hyeonbumlee">hyeonbumlee.github.io</a> Linkedin: <a href="https://www.linkedin.com/in/hyeonbum-lee">www.linkedin.com/in/hyeonbum-lee</a> ✉ E-mail: <a href="mailto:leehb3706@hanyang.ac.kr">leehb3706@hanyang.ac.kr</a>
RESEARCH BACKGROUND	<ul style="list-style-type: none"> <li>• <b>Cryptography:</b> Zero-Knowledge Proofs, SNARK, Verifiable Computing, Secure Multi-Party Computation, Computation Theory</li> </ul>	
EDUCATION	<b>Hanyang University</b> , Seoul <ul style="list-style-type: none"> <li>• Ph.D. <a href="#">Department of Mathematics</a></li> <li>• Advisor: Prof. <a href="#">Jae Hong Seo</a>.</li> </ul>	Mar 2020 - Present
	<b>Hanyang University</b> , Seoul. <ul style="list-style-type: none"> <li>• B.S. Department of Mathematics</li> </ul>	Mar 2014 - Feb 2018
RESEARCH PROJECTS	<b>Zero-Knowledge Proofs &amp; SNARK</b> <ul style="list-style-type: none"> <li>• <b>Logging and Zero-knowledge Proof based on Hierarchical Blockchain, Institute for Information and Communications Technology Promotion</b> Supported by Institute of Information &amp; Communications Technology Planning &amp; Evaluation (IITP), Researcher, May 2022 - Apr 2023.</li> <li>• <b>Research on the design technology of a cryptographic proof system suitable for Proof-Carrying Data</b> Supported by National Security Research Institute (NSR), Researcher, Apr 2022 - Oct 2022.</li> <li>• <b>A Study on Cryptographic Primitives for SNARK</b> Supported by Institute of Information &amp; Communications Technology Planning &amp; Evaluation (IITP), Research Associate, Apr 2021 - Dec 2026.</li> <li>• <b>Research on Incrementally Verifiable Computation Design Technique and Application Method</b> Supported by National Security Research Institute (NSR), Researcher, Apr 2021 - Oct 2021.</li> <li>• <b>Research on Post-Quantum Non-Interactive Zero-Knowledge Proofs</b> Supported by National Research Foundation of Korea (NRF), Researcher, Mar 2020 - Feb 2025.</li> <li>• <b>Research on Post-Quantum Zero-Knowledge Proofs Design Technique and Application Method</b> Supported by National Security Research Institute (NSR), Researcher, Apr 2020 - Oct 2020.</li> </ul>	
	<b>Others</b> <ul style="list-style-type: none"> <li>• <b>Secure Multi-party Approximate Computation</b> Supported by Samsung Science &amp; Technology Foundation, Researcher, Sep 2021 - Aug 2024.</li> <li>• <b>A Study of Functional Encryption and Its Core Techniques</b> Supported by Institute of Information &amp; Communications Technology Planning &amp; Evaluation (IITP) &amp; National Research Foundation of Korea (NRF), Researcher, Mar 2020 - Jul 2021.</li> </ul>	
SELECTED PUBLICATIONS	<b>Journal</b> <ol style="list-style-type: none"> <li>1. Chanyang Ju, <b>Hyeonbum Lee</b>, Heewon Chung, Jae Hong Seo, and Sungwook Kim, <i>Analysis of Zero-Knowledge Protocols for Verifiable Computation and Its Applications</i> Journal of The Korea Institute of Information Security &amp; Cryptology VOL.31, NO.4, Aug. 2020</li> <li>2. Chanyang Ju, <b>Hyeonbum Lee</b>, Heewon Chung, and Jae Hong Seo, <i>Efficient Sum-Check Protocol for Convolution</i> IEEE Access, VOL.9, pp.164047-164059, 2021, doi</li> <li>3. Sungwook Kim, <b>Hyeonbum Lee</b>, Gwangwoon Lee, and Jae Hong Seo, <i>Sublinear Verifier Inner Product Argument under Discrete Logarithm Assumption</i> IEEE Transactions on Information Forensics and Security, VOL.18, pp.5332-5344, 2023, doi</li> </ol>	

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**, 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](#)

## 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 & PRESENTATIONS

### Presentations

- *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

- **Grand Prize**, National Cryptographic Technology Contest. Oct 2022  
Korea Cryptography Forum
- **Special Prize**, National Cryptographic Technology Contest. Oct 2021, Oct 2023  
Korea Cryptography Forum
- **SUMMA CUM LAUDE**, Graduate Honors. Feb 2018  
Hanyang University
- **Dean's list** 2016 (Fall)  
College of Natural Science, Hanyang University

### External Reviewer

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

## Scholarships & Stipends

- **Cryptography Research Fund for Students:**  
Asiacrypt 2022 registration and accommodation  
International Association for Cryptologic Research  
≈ \$800  
Dec 2022
- **Teaching Assistant Scholarship**  
Hanyang University  
\$6000/year  
Sep 2020 - Aug 2022
- **Master and Ph.D Program Scholarship**  
Hanyang University  
Full tuition for 3 years (≈ \$12000/year)  
Mar 2020 - Feb 2023
- **Hanyang Excellent Scientist Scholarship**  
Hanyang University  
Full tuition for 4 years (≈ \$8000/year)  
Mar 2014 - Feb 2018

SERVICES

## Others

TECHNICAL

SKILLS