

CONTACT INFORMATION Room 736, Natural Science Building, Hanyang University, 222, Wangsimni-ro, Seongdong-gu, Seoul, 04763, Republic of Korea  
Tel: +82 10-7137-0381  
Homepage:  
Linkedin: <https://www.linkedin.com/in/hyeonbum-lee-a176b120a/>  
✉ E-mail: [leehb3706@hanyang.ac.kr](mailto:leehb3706@hanyang.ac.kr)

RESEARCH BACKGROUND  
EDUCATION • **Cryptography:** Zero-Knowledge Proofs, Verifiable Computing, Computational theory  
**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 & Verifiable Computing**  
• **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, *Efficient Sum-Check Protocol for Convolution*  
IEEE Access, vol. 9, pp. 164047-164059, 2021, doi:[10.1109/ACCESS.2021.3133442](https://doi.org/10.1109/ACCESS.2021.3133442).  
2. Chanyang Ju, **Hyeonbum Lee**, Heewon Chung, and Jae Hong Seo, *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

EXPERIENCE **Work Experience**  
• **Teaching Assistant**

- Spring 2021: Calculus I
- Fall 2020: Modern Algebra II
- Spring 2020: Modern Algebra I

#### Others

TECHNICAL SKILLS • *Technical Softwares:* MATLAB,  $\text{\LaTeX}$ .

TALKS & PRE-SENTATIONS      **Presentations**

- *Transparent and efficient zero-knowledge arguments from discrete log with better complexity*  
2021 KMS Spring Meeting, Virtual, 30 Apr. 2021

HONORS & AWARDS      **Awards**

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

**Scholarships**

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

SERVICES      **External Reviewer**

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