Hyung Tae Lee

Curriculum Vitae

Division of Computer Science and Engineering
College of Engineering
Jeonbuk National University
Jeonju 54896 Republic of Korea

hyungtaelee@jbnu.ac.kr
Office: +82-63-270-3384
Fax: +82-63-270-2394
http://www.hyungtaelee.com

Research Interests

Cryptography, Security, Computational Number Theory

Education

Seoul National University
PhD in Mathematics, Feb 2013
Supervisor: Jung Hee Cheon
Thesis: *Polynomial Factorization and Its Applications*

Seoul National University
Master of Science in Mathematics, Feb 2008
Supervisor: Jung Hee Cheon
Thesis: *Efficient Unlinakble BKS Scheme using Precomputation*

Seoul National University
Bachelor of Science in Mathematics, Feb 2006

Employment

Assistant Professor, Jeonbuk National University, Jeonju, Korea — Sep 2017 - Present

Research Fellow, Nanyang Technological University, Singapore — May 2014 - Aug 2017

Postdoctoral Researcher, Seoul National University, Seoul, Korea — Mar 2013 - Feb 2014

Summer Internship, NTT Secure Platform Laboratories, Tokyo, Japan — Jun 2011 - Aug 2011

Research Projects

- **A Study on Improvement of MPC-Based Digital Signatures** by Electronics and Telecommunications Research Institute (ETRI), PI, May 2021 – Oct 2021
- **A Study on Cryptographic Primitives for SNARK** by Institute of Information & Communications Technology Planning & Evaluation (IITP), Co-PI, Apr 2021 – Dec 2026
- **Cryptographic Schemes for Secure Computation and Their Applications** by National Research Foundation of Korea (NRF), PI, Mar 2021 – Feb 2026
- **A Study on MPC-Based Cryptographic Protocols** by Electronics and Telecommunications Research Institute (ETRI), PI, Jun 2020 – Nov 2020

- **Security Analysis of Code-Based Signature Schemes** by National Security Research Institute (NSR), PI, Apr 2019 – Oct 2019
- **Development of Fuzzy Extractor Based on Real Numbers** by Samsung Electronics, PI, Dec 2018 – Dec 2019
- **A Study of Cryptographic Techniques Based on Biometric Information** by Samsung Electronics, PI, May 2018 – Dec 2018
- **A Study on New Digital Signature Schemes from Coding Theory** by National Security Research Institute (NSR), PI, Apr 2018 – Oct 2018
- **Development of Cryptosystem and Its Applications in Post-Quantum Cryptography** by National Research Foundation of Korea (NRF), PI, Mar 2018 – Feb 2021

Scientific Papers

Journal Articles

[1] Benjamin Hong Meng Tan, **Hyung Tae Lee**†, Huaxiong Wang, Shuqin Ren, and Khin Mi Mi Aung, Efficient Private Comparison Queries over Encrypted Databases using Fully Homomorphic Encryption with Finite Fields, Accepted for publication in *IEEE Transactions on Dependable and Secure Computing*, Jan 2020. (†Corresponding author)

[2] Martianus Frederic Ezerman, **Hyung Tae Lee**†, San Ling, Khoa Nguyen, and Huaxiong Wang, Provably Secure Group Signature Schemes from Code-Based Assumptions, *IEEE Transactions on Information Theory*, Vol. 66, No. 9, pp. 5754–5773, Sep 2020. (†Corresponding author, A journal version of [17].)

[3] **Hyung Tae Lee**, San Ling, Jae Hong Seo, Huaxiong Wang, and Taek-Young Youn, Public Key Encryption with Equality Test in the Standard Model, *Information Sciences*, Vol. 516, pages 89–108, Apr 2020.

[4] Myungsun Kim, **Hyung Tae Lee**†, San Ling, Shu Qin Ren, Benjamin Hong Meng Tan, and Huaxiong Wang, Search Condition-Hiding Query Evaluation on Encrypted Databases, *IEEE Access*, Vol. 7, No. 1, pages 161283–161295, Dec 2019. (†Corresponding author)

[5] Myungsun Kim and **Hyung Tae Lee**†, Experimenting with Non-Interactive Range Proofs Based on the Strong RSA Assumption. *IEEE Access*, Vol. 7, No. 1, pages 117505–117516, Dec 2019. (†Corresponding author)

[6] **Hyung Tae Lee**, San Ling, Jae Hong Seo, and Huaxiong Wang, Public Key Encryption with Equality Test from Generic Assumptions in the Random Oracle Model. *Information Sciences*, Vol. 500, pages 15–33, Oct 2019.

[7] Myungsun Kim, **Hyung Tae Lee**†, San Ling, Benjamin Hong Meng Tan, and Huaxiong Wang, Private Compound Wildcard Queries using Fully Homomorphic Encryption. *IEEE Transactions on Dependable and Secure Computing*, Vol. 16, No. 5, pages 743–756, Sep 2019. (†Corresponding author)

[8] Khin Mi Mi Aung, **Hyung Tae Lee**, Benjamin Hong Meng Tan, and Huaxiong Wang, Fully Homomorphic Encryption over the Integers for Non-Binary Plaintexts. *Theoretical Computer Science*, Vol. 771, pages 49–70, Jun 2019.

[9] Kai Zhang, Jie Chen, **Hyung Tae Lee**†, Haifeng Qian, and Huaxiong Wang, Efficient Public Key Encryption with Equality Test in the Standard Model. *Theoretical Computer Science*, Vol. 755, pages 65–80, Jan 2019. (†Corresponding author)

[10] Myungsun Kim, **Hyung Tae Lee**†, San Ling, and Huaxiong Wang, On the Efficiency of FHE-Based Private Queries. *IEEE Transactions on Dependable and Secure Computing*, Vol. 15, No. 2, pages 357–363, Mar 2018. (†Corresponding author)

[11] **Hyung Tae Lee**, San Ling, Jae Hong Seo, and Huaxiong Wang, Semi-Generic Construction of Public Key Encryption and Identity-Based Encryption with Equality Test. *Information Sciences*, Vol. 373, pages 419–440, Dec 2016.

[12] **Hyung Tae Lee**, San Ling, Jae Hong Seo, and Huaxiong Wang, CCA2 Attack and Modification of Huang et al.'s Public Key Encryption with Authorized Equality Test. *The Computer Journal*, Vol. 59, No. 11, pages 1689–1694, Nov 2016.

[13] **Hyung Tae Lee**, San Ling, and Huaxiong Wang, Analysis of Gong et al.'s CCA2-Secure Homomorphic Encryption. *Theoretical Computer Science*, Vol. 640, pages 104–114, Aug 2016.

[14] Myungsun Kim, **Hyung Tae Lee**, and Jung Hee Cheon. A Generalization of Agrawal et al.'s Protocol for n-Party Private Set Intersection, *Journal of Internet Technology*, Vol. 13, No. 6, pages 909–918, Nov 2012.

Refereed International Conference/Workshop Publications

[15] Sunpill Kim, Yunseong Jeong, Jinsu Kim, Jungkon Kim, **Hyung Tae Lee**, and Jae Hong Seo, IronMask: Modular Architecture for Protecting Deep Face Template, To appear in *CVPR 2021*, Mar 2021.

[16] **Hyung Tae Lee**, Huaxiong Wang, and Kai Zhang, Security Analysis and Modification of Identity-Based Encryption with Equality Test from ACISP 2017, In *Proceedings of ACISP 2018*, pages 780–786, 2018.

[17] Martianus Frederic Ezerman, **Hyung Tae Lee**, San Ling, Khoa Nguyen, and Huaxiong Wang, A Provably Secure Group Signature Scheme from Code-Based Assumptions, In *Proceedings of ASIACRYPT 2015 Part I*, pages 260–285, 2015.

[18] Jung Hee Cheon, **Hyung Tae Lee**, and Jae Hong Seo, A New Additive Homomorphic Encryption based on the co-ACD Problem, In *Proceedings of ACM CCS 2014*, pages 287–298, 2014.

[19] **Hyung Tae Lee** and Jae Hong Seo, Security Analysis of Multilinear Maps over the Integers, In *Proceedings of CRYPTO 2014 Part I*, pages 224–240, 2014.

[20] Jung Hee Cheon, Hyunsook Hong, and **Hyung Tae Lee**, Invertible Polynomial Representation for Private Set Operations, In *Proceedings of ICISC 2013*, pages 277–292, 2014.

[21] **Hyung Tae Lee**, HongTae Kim, Yoo-Jin Baek, and Jung Hee Cheon, Correcting Errors in Private Keys Obtained from Cold Boot Attacks, In *Proceedings of ICISC 2011*, pages 74–89, 2012.

[22] Myungsun Kim, **Hyung Tae Lee**, and Jung Hee Cheon, Mutual Private Set Intersection with Linear Complexity, In *Proceedings of WISA 2011*, pages 219–231, 2012.

Technical Reports

[23] **Hyung Tae Lee**, Jung Hee Cheon, and Jin Hong, Accelerating ID-based Encryption based on Trapdoor DL using Pre-computation, 2011. Available at http://eprint.iacr.org/2011/187.

Patents

Overseas Registrations

[1] HyoJin Yoon, Jung Hee Cheon, Seon Young Lee, **Hyung Tae Lee**, and Jung Hoon Sohn, Method and System for ID-based Encryption and Decryption, US 9,379,891, Jun 2016.

[2] Jung Hee Cheon, **Hyung Tae Lee**, and Jin Hong, Method and Apparatus for Solving Discrete Logarithm Problem using Pre-computation Table, US 9,077,536, Jul 2015.

Domestic Registrations

[3] Jung Hee Cheon, Taechan Kim, and **Hyung Tae Lee**, Computation Method of Encrypted Data using Homomorphic Encryption and Pairing-based Encryption and Server using the Same, KR 10-16-18941, Apr 2016.

[4] HyoJin Yoon, Jung Hee Cheon, Seon Young Lee, **Hyung Tae Lee**, and Jung Hoon Sohn, Method and System for ID-based Encryption and Decryption, KR 10-14-93212, Feb 2015.

[5] Jung Hee Cheon and **Hyung Tae Lee**, ID-based Additive Homomorphic Encryption Method, KR 10-13-27980, Nov 2013.

[6] **Hyung Tae Lee**, Jung Hee Cheon, and Jin Hong, Method of Solving a Discrete Logarithm Problem using Pre-computation Table and Apparatus Thereof, KR 10-11-66129, Jul 2012.

Professional Activities

Program Committee Member

- ASIACRYPT 2021-2020, 2016
- APKC 2021-2018
- ICISC 2021-2020, 2018-2014
- IWSEC 2017-2015
- ProvSec 2020-2018

Journal Reviewer

- Applied Sciences 2020
- Designs, Codes, and Cryptography 2020 ($\times 2$)
- Frontiers of Computer Science 2019

- Frontiers of Information Technology & Electronic Engineering 2016
- IEEE Access 2021 (×2)
- IEEE Transactions on Dependable and Secure Computing 2021, 2016
- IEEE Transactions on Information Theory 2019
- IEEE Transactions on Knowledge and Data Engineering 2020, 2017
- IEEE Transactions on Services Computing 2018
- IET Information Security 2021, 2019, 2018, 2017
- Information Sciences 2017
- International Journal of Computer Mathematics 2021
- KSII Transactions on Internet and Information System 2019
- Journal of Communications and Networks 2020
- Journal of Internet Technology 2017
- Security and Communication Networks 2020, 2019
- Theoretical Computer Science 2020 (×2), 2016
- The Journal of Korea Information and Communications Society (J-KICS) 2013

Talks (Selected & Invited, Conferences & Workshops)

- **Backward Secure Dynamic Searchable Symmetric Encryption with Efficient Updates**

  [1] Workshop on Modern Trends in Cryptography, Nanyang Technological University, Singapore, 14 Jun 2019

- **Introduction to Cryptographic Techniques using Biometric Information**

  [2] Mathematics Colloquium, Hanyang University, Seoul, Korea, 02 Nov 2018

- **Security Analysis and Modification of Identity-Based Encryption with Equality Test from ACISP 2017**

  [3] ACISP 2018, Wollongong, Australia, 13 Jul 2018

- **Private Compound Wildcard Queries using Fully Homomorphic Encryption**

  [4] 2017 KMS Annual Meeting, Dankook University, Cheonan, Korea, 28 Oct 2017

- **Introduction to (Fully) Homomorphic Encryption**

  [5] Nanyang Technological University, 07 Aug 2019

  [6] Cyber Security Cluster, Institute for Infocomm Research (I^2R), A*STAR, Singapore, 15 Mar 2017

- **Private Database Queries using Fully Homomorphic Encryption**

  [7] International Workshop on Computational Mathematics, Ewha Womans University, Seoul, Korea, 16 Dec 2017

[8] International Conference for the 70th Anniversary of Korean Mathematical Society, Seoul National University, Seoul, Korea, 22 Oct 2016

- **Code-Based Cryptography**

  [9] Future Cryptographic Technology Symposium, Seoul National University, Seoul, Korea, 14 Jan 2016

- **A Provably Secure Group Signature Scheme from Code-Based Assumptions**

  [10] Sogang University, Seoul, Korea, 18 Oct 2016

  [11] National Security Research Institute (NSR), Daejeon, Korea, 21 Mar 2016

  [12] Ewha Woman's University, Seoul, Korea, 15 Jan 2016

  [13] National Institute for Mathematical Sciences (NIMS), Daejeon, Korea, 18 Dec 2015

  [14] Seoul National University, Seoul, Korea, 14 Dec 2015

- **A New Additive Homomorphic Encryption based on the co-ACD Problem**

  [15] ACM CCS 2014, Arizona, USA, 04 Nov 2014

  [16] National Institute for Mathematical Sciences (NIMS), 28 Aug 2014

  [17] NTU-SNU Joint Workshop on Mathematics and Applications, Nanyang Technological University, Singapore, 03 Oct 2013

  [18] The Asian Mathematical Conference (AMC) 2013, BEXCO, Busan, Korea, 02 Jul 2013

- **Invertible Polynomial Representation for Private Set Operations**

  [19] ICISC 2013, Seoul, Korea, 29 Nov 2013

- **Polynomial Factorization and Its Applications**

  [20] The 9th RIMS-KYOTO UNIVERSITY and SNU Joint Symposium on Mathematics, Seoul National University, Seoul, Korea, 18 Feb 2013

  [21] The 29th SNU Algebraic Camp, Yangyang, Korea, 31 Jan 2013

- **Correcting Errors in Private Keys Obtained from Cold Boot Attacks**

  [22] ICISC 2011, Seoul, Korea, 30 Nov 2011

  [23] 2011 KMS Fall Meeting, Kyungpook National University, Daegu, Korea, 21 Oct 2011

- **Discrete Logarithm with Pre-computation and Applications to Trapdoor DL Groups**

  [24] Korea Military Academy, Seoul, Korea, 06 Oct 2010

  [25] First Joint Meeting of KMS and AMS, Ewha Womans University, Seoul, Korea, 19 Dec 2009

- **Efficient Unlinkable BKS Scheme using Precomputation**

  [26] 2008 KMS Spring Meeting, Keimyung University, Daegu, Korea, 26 Apr 2008

Teaching

Lecture, Jeonbuk National University, Jeonju, Korea

- Advanced Information Security (Graduate), Spring 2020-2019, Fall 2017
- Advanced Computational Mathematics (Graduate), Spring 2021
- Advanced Computer Engineering 2 (Graduate), Fall 2018
- Basic of Computer Programming (Undergraduate), Spring 2018
- Cryptographic Algorithms (Graduate), Spring 2018
- Cryptographic Protocols (Graduate), Fall 2018
- Digital Forensics (Graduate), Spring 2020
- Discrete Mathematics (Undergraduate), Spring 2021-2018
- Information Security (Undergraduate), Fall 2020-2017
- Linear Algebra (Undergraduate), Fall 2020-2018

Lecture, Seoul National University, Seoul, Korea

- Calculus 2, Fall 2013

Implementation Skills

Programming Languages

- C/C++: Fluent

Number Theory Library and Packages

- NTL: Fluent
- HElib, SAGE: Proficient