Hyung Tae Lee

Curriculum Vitae

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

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

Research Interest

Cryptography, Computational Number Theory, Secure Protocol

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, Chonbuk 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 Grants

- **Seoul Science Fellowship**, by the Seoul Metropolitan Government, Sep 2008 - Feb 2010

Awards and Honors

- **Paper Award**, in the 6th Cryptology Paper Contest, hosted by Korea Government (National Intelligence Service), Nov 2012
- **Best Teaching Award**, by Faculty of Liberal Education, Seoul National University, Feb 2009

Scientific Papers

Journal Articles

[1] Myungsun Kim, **Hyung Tae Lee**†, San Ling, and Huaxiong Wang, On the Efficiency of FHE-Based Private Queries. Accepted for publication in *IEEE Transactions on Dependable and Secure Computing*, May 2016. (†Corresponding author)

[2] **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.

[3] **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.

[4] **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.

[5] 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

[6] 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.

[7] 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.

[8] **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.

[9] 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.

[10] **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.

[11] 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

[12] **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.

Domestic Applications

[7] Jung Hee Cheon, Jae Hong Seo, and **Hyung Tae Lee**, Additive Homomorphic Encryption and Decryption Method based on the co-ACD Problem and Apparatus using the Same, KR 10-2014-0098808, Aug 2014.

Professional Activities

Program Committee Member

- ASIACRYPT 2016
- ICISC 2017, 2016, 2015, 2014
- IWSEC 2017, 2016, 2015

Journal Reviewer

- Frontiers of Information Technology & Electronic Engineering 2016
- IEEE Transactions on Dependable and Secure Computing 2016
- IET Information Security 2017
- Information Sciences 2017
- Theoretical Computer Science 2016
- The Journal of Korea Information and Communications Society (J-KICS) 2013

External Reviewer

- EUROCRYPT, CRYPTO, ASIACRYPT, PKC, CT-RSA, FC and many other conferences/workshops

Talks (Invited, Conferences & Workshops)

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

  [1] 2017 KMS Annual Meeting, Dankook University, Cheonan, Korea, 28 Oct 2017

- **Introduction to Homomorphic Encryption**

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

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

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

- **Code-Based Cryptography**

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

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

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

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

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

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

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

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

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

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

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

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

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

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

- **Polynomial Factorization and Its Applications**

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

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

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

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

  [18] 2011 KMS Fall Meeting, Kyungpook National University, Daegu, Korea, 21 Oct 2011

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

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

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

- **Efficient Unlinkable BKS Scheme using Precomputation**

  [21] 2008 KMS Spring Meeting, Keimyung University, Daegu, Korea, 26 Apr 2008

Teaching

Lecture, Chonbuk National University, Jeonju, Korea

- Advanced Information Security (Graduate), Fall 2017
- Information Security (Undergraduate), Fall 2017

Lecture, Seoul National University, Seoul, Korea

- Calculus 2, Fall 2013

Teaching Assistant (Selected), Seoul National University, Seoul, Korea

- Calculus 1, 2, Spring 2007- Fall 2010
- Linear Algebra, Fall 2007, Spring 2011
- Number Theory, Spring 2011

Implementation Skills

Programming Languages

- C/C++: Fluent

Number Theory Library and Packages

- NTL: Fluent
- HElib, SAGE: Proficient