DUHYEONG KIM

Curriculum Vitae

CONTACT INFORMATION

Affiliation	Department of Mathematical Sciences, Seoul National University
Address	1, Gwanak-ro, Gwanak-gu, Seoul, Republic of Korea, 08826
Office Number	+82-2-880-6272
E-mail	doodoo1204@snu.ac.kr

EDUCATION

Seoul National University, Republic of Korea

Integrated M.S./Ph.D. in Mathematical Sciences — Mar 2015 ∼ Present
Advisor: Prof. Jung Hee Cheon

B.S. in Mathematical Sciences — Mar 2011 ∼ Feb 2015
Honers: *Summa Cum Laude* (Major GPA: 4.13/4.3)

RESEARCH INTERESTS

- Homomorphic Encryption
  - Algorithms for Homomorphic Non-Arithmetic Operations
  - Privacy-Preserving Machine Learning
- Lattice-based Cryptography
  - Post-Quantum Cryptography
  - Reduction/Analysis on Lattice-based Hard Problems

VISITING RESEARCH

UTHealth — Aug 2018
Hosted by Prof. Xiaoqian Jiang — *Houston, TX, United States*

ENS de Lyon — Dec 2017 ∼ Jan 2018
Hosted by Prof. Damien Stehlé — *Lyon, France*

CONFERENCE PRESENTATIONS

Approximate Homomorphic Encryption over the Conjugate-Invariant Ring — Nov 2018
ICISC 2018 — *Seoul, Republic of Korea*

Lizard: A practical post-quantum public-key encryption from LWE and LWR — Sep 2018
SCN 2018 — *Amalfi, Italy*

PUBLICATIONS

Authors are listed in alphabetical order by last name, unless an asterisk (*) is indicated.

Conference

4. Jung Hee Cheon, Dongwoo Kim, **Duhyeong Kim**, Hun Hee Lee and Keewoo Lee. “Numerical Methods for Comparison on Homomorphically Encrypted Numbers.” To appear in ASIACRYPT 2019.

3. Jung Hee Cheon, **Duhyeong Kim** and Jai Hyun Park. “Towards a Practical Clustering Analysis over Encrypted Data.” To appear in Selected Areas in Cryptography (SAC) 2019.

2. **Duhyeong Kim**, and Yongsoo Song. “Approximate Homomorphic Encryption over the Conjugate-Invariant Ring.” In International Conference on Information Security and Cryptology (ICISC), pp. 85-102. Springer, Cham, 2018.

1. Jung Hee Cheon, **Duhyeong Kim**, Joohee Lee, and Yongsoo Song. “Lizard: Cut off the tail! A practical post-quantum public-key encryption from LWE and LWR.” In International Conference on Security and Cryptography for Networks (SCN), pp. 160-177. Springer, Cham, 2018.

Journal

4. ***Duhyeong Kim**, Yongha Son, Dongwoo Kim, Andrey Kim, Seungwan Hong and Jung Hee Cheon. “Privacy-preserving Approximate GWAS computation based on Homomorphic Encryption.” To Appear in BMC Medical Genomics.

3. *Joohee Lee, **Duhyeong Kim**, Hyungkyu Lee, Younho Lee, and Jung Hee Cheon. “RLizard: Post-Quantum Key Encapsulation Mechanism for IoT Devices.” IEEE Access 7 (2019): 2080-2091.

2. Jung Hee Cheon, **Duhyeong Kim**, Yongdai Kim, and Yongsoo Song. “Ensemble method for privacy-preserving logistic regression based on homomorphic encryption.” IEEE Access 6 (2018): 46938-46948.

1. Jung Hee Cheon, and **Duhyeong Kim**. “Probability that the k-gcd of products of positive integers is B-friable.” Journal of Number Theory 168 (2016): 72-80.

MANUSCRIPTS

3. *Yongsoo Song, Jacek Cyranka, **Duhyeong Kim** and Sicun Gao. “Convergence and Oscillation of Low-Precision Stochastic Gradient Descent”

2. Jung Hee Cheon, Dongwoo Kim, **Duhyeong Kim**, Joohee Lee and Yongsoo Song. “Instant Privacy-Preserving Biometric Authentication for Hamming Distance Matcher”.

1. Jung Hee Cheon, Kyoohyung Han and **Duhyeong Kim**. “Faster bootstrapping of FHE over the integers.” Available at `https://eprint.iacr.org/2017/079.pdf`.

SERVICES

Reviewer / External Reviewer

- ASIACRYPT 2019; PKC 2019; CT-RSA 2019; PQCrypto 2019, 2018; CRYPTO 2017; FC 2017
- Journal of Cryptology (JoC), IEEE Transactions on Computers (TC)

TEACHING EXPERIENCE

Introduction to Cryptography Mar 2017 ∼ Jun 2017

Differential and Integral Calculus Mar 2015 ∼ Dec 2017

Linear Algebra Mar 2015 ∼ Dec 2017

AWARDS

Global Empowerment Program for top 10% of Global PhD Fellowship May 2018
Research Grant: $5,000 *National Foundation Research of Korea*

Global PhD Fellowship Mar 2016 ∼ Present
Research Grant: Tuition+$20,000/year for 5 years *National Foundation Research of Korea*

Awards for Excellence in Teaching Mar 2016
For teaching Differential and Integral Calculus *Seoul National University*

The Presidential Science Scholarship Mar 2011 ∼ Feb 2015
Academic Grant: Tuition+$5,000/year for 4 years *Korea Student Aid Foundation*

Gold Medal at Korean Mathematical Olympiad Nov 2009
Top 40 of the National Mathematical Olympiad *Korean Mathematical Society*

LANGUAGES AND SKILLS

Languages	Korean (native), English (fluent)
Skills	C/C++, Python, LaTeX

Last updated on September 7, 2019