

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
Website	https://du1204.github.io
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: <i>Summa Cum Laude</i> (Major GPA: 4.13/4.3)	

Gyeonggi Science High School, Republic of Korea

High School Diploma	Mar 2009 ~ Feb 2011
---------------------	---------------------

RESEARCH INTERESTS

- **Homomorphic Encryption**

- Algorithms for Homomorphic Non-Arithmetic Operations
- Privacy-Preserving Machine Learning

- **Lattice-based Cryptography**

- Post-quantum Public-Key Encryption
- Lattice Trapdoor Construction
- Reduction/Analysis on Lattice-based Hard Problems

VISITING RESEARCH

UTHealth	Aug 2018
Hosted by Prof. Xiaoqian Jiang	<i>Houston, TX, United States</i>

ENS de Lyon	Dec 2017 ~ Jan 2018
Hosted by Prof. Damien Stehlé	<i>Lyon, France</i>

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.
 - Award: *Invited to Journal of Cryptology (Top 3 of 71 accepted papers among 306 submissions)*

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. Jung Hee Cheon, Dongwoo Kim and **Duhyeong Kim**. “Efficient Homomorphic Comparison Methods with Optimal Complexity”.
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>.

TALKS

Efficient Homomorphic Comparison Methods with Optimal Complexity East Asian Core Doctoral Forum on Mathematics 2020	Jan 2020 (planned) <i>Tokyo, Japan</i>
Numerical Methods for Comparison on Homomorphically Encrypted Numbers ASIACRYPT 2019	Dec 2019 (planned) <i>Kobe, Japan</i>
Approximate Homomorphic Encryption over the Conjugate-Invariant Ring ICISC 2018	Nov 2018 <i>Seoul, Republic of Korea</i>
Lizard: A practical post-quantum public-key encryption from LWE and LWR SCN 2018	Sep 2018 <i>Amalfi, Italy</i>
Hash-and-Sign Signature over General NTRU lattices Winter Crypto Camp	Jan 2018 <i>Konjiam Resort, Republic of Korea</i>
The practical post-quantum public-key encryption from LWE and LWR 2017 KMS Annual Meeting	Oct 2017 <i>Dankook University, Republic of Korea</i>

PATENTS

2. Jung Hee Cheon, **Duhyeong Kim**, Yongsoo Song and Kyoohyung Han. *WO2019117694*, filed December 17, 2018
1. Joohee Lee, Jung Hee Cheon, **Duhyeong Kim** and Aaram Yun. *KR1020170183661*, filed December 29, 2017

SERVICES

Reviewer / External Reviewer

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

TEACHING EXPERIENCE

Introduction to Cryptography	Mar 2017 ~ Jun 2017
Differential and Integral Calculus	Mar 2015 ~ Dec 2017
Linear Algebra	Mar 2015 ~ Dec 2017

AWARDS

One of the Winners of iDASH 2019 Track 2: HE-based Genotype Imputation	Oct 2019 <i>National Institutes of Health (NIH)</i>
Global Empowerment Program for top 10% of Global PhD Fellowship Research Grant: \$5,000	May 2018 <i>National Foundation Research of Korea</i>
Global PhD Fellowship Research Grant: Tuition+\$20,000/year for 5 years	Mar 2016 ~ Present <i>National Foundation Research of Korea</i>
Awards for Excellence in Teaching For teaching Differential and Integral Calculus	Mar 2016 <i>Seoul National University</i>
The Presidential Science Scholarship Academic Grant: Tuition+\$5,000/year for 4 years	Mar 2011 ~ Feb 2015 <i>Korea Student Aid Foundation</i>
Gold Medal at Korean Mathematical Olympiad Top 40	Nov 2009 <i>Korean Mathematical Society</i>

LANGUAGES AND SKILLS

Languages	Korean (native), English (fluent)
Skills	C/C++, Python, L ^A T _E X