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`
Birth	4th December, 1993

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)

Gyeonggi Science High School, Republic of Korea

High School Diploma — Mar 2009 ∼ Feb 2011

RESEARCH INTERESTS

- **Homomorphic Encryption (HE)**
  - Construction of New HE Schemes
  - Algorithms for Homomorphic Non-Arithmetic Operations
  - Privacy-Preserving Machine Learning
- **Lattice-based Cryptography**
  - Post-Quantum Public-Key Encryption
  - Construction of Lattice Trapdoor
  - Reduction/Analysis on Lattice-based Hard Problems

WORK EXPERIENCES

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

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

PUBLICATIONS

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

Conference

5. Jung Hee Cheon, Kyoohyung Han and **Duhyeong Kim**. "Faster bootstrapping of FHE over the integers." In International Conference on Information Security and Cryptology (ICISC), pp. 242-259. Springer, Cham, 2019.

4. Jung Hee Cheon, Dongwoo Kim, **Duhyeong Kim**, Hun Hee Lee and Keewoo Lee. "Numerical Methods for Comparison on Homomorphically Encrypted Numbers." In International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT), pp. 415-445. Springer, Cham, 2019.

    - *Invited to Journal of Cryptology (Top 3 of 71 accepted papers among 307 submissions)*
    - *Excellence Award at 5^{th} Samsung DS Industry-Academy Cooperation Project Paper Award*

3. Jung Hee Cheon, **Duhyeong Kim**, and Jai Hyun Park. "Towards a practical cluster analysis over encrypted data." In International Conference on Selected Areas in Cryptography (SAC), pp. 227-249. Springer, Cham, 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." BMC Medical Genomics 13, 77 (2020).

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

5. *Miran Kim, *Arif Harmanci, Jean-Philippe Bossuat, Sergiu Carpov, Jung Hee Cheon, Ilaria Chillotti, Wonhee Cho, David Froelicher, Nicolas Gama, Mariya Georgieva, Seungwan Hong, Jean-Pierre Hubaux, **Duhyeong Kim**, Kristin Lauter, Yiping Ma, Lucila Ohno-Machado, Heidi Sofia, Yongha Son, Yongsoo Song, Juan Troncoso-Pastoriza and Xiaoqian Jiang. "Ultra-Fast Homomorphic Encryption Models enable Secure Outsourcing of Genotype Imputation. Available at `https://www.biorxiv.org/content/10.1101/2020.07.02.183459v1`.

4. Jung Hee Cheon, **Duhyeong Kim**, Taechan Kim and Yongha Son. "A New Trapdoor over Module-NTRU Lattice and its Application to ID-based Encryption". Available at `https://eprint.iacr.org/2019/1468.pdf`.

3. Jung Hee Cheon, Dongwoo Kim and **Duhyeong Kim**. "Efficient Homomorphic Comparison Methods with Optimal Complexity". Available at `https://eprint.iacr.org/2019/1234.pdf`.
   - *Gold Award at 26th Samsung Humantech Paper Award (1st place in Computer Science & Engineering)*
2. *Yongsoo Song, Jacek Cyranka, **Duhyeong Kim** and Sicun Gao. "Convergence and Oscillation of Low-Precision Stochastic Gradient Descent".
1. Jung Hee Cheon, Dongwoo Kim, **Duhyeong Kim**, Joohee Lee and Yongsoo Song. "Instant Privacy-Preserving Biometric Authentication for Hamming Distance Matcher". Available at `https://eprint.iacr.org/2018/1214.pdf`.

TALKS

Complexity-Optimal Homomorphic Comparison
East Asian Core Doctoral Forum on Mathematics 2020 in Tokyo, Japan — Jan 2020
Winter Crypto Camp 2020 in Konjiam Resort, Republic of Korea — Jan 2020
Crypto Lab in Seoul, Republic of Korea — Dec 2019

Numerical Methods for Homomorphic Comparison
Asiacrypt 2019 in Kobe, Japan — Dec 2019

A New Trapdoor over Module-NTRU Lattices and its Applications
Winter Crypto Camp 2019 in Konjiam Resort, Republic of Korea — Jan 2019

Approximate HE over the Conjugate-Invariant Ring (a.k.a. **Real-HEAAN**)
ICISC 2018 in Seoul, Republic of Korea — Nov 2018

Lizard: A New Practical Post-Quantum PKE from LWE and LWR
SCN 2018 in Amalfi, Italy — Sep 2018
2017 KMS Annual Meeting in Dankook University, Republic of Korea — Oct 2017

PATENTS

5. Jung Hee Cheon, **Duhyeong Kim** and Yongha Son. ID-based Encryption over Generalized NTRU Trapdoor Lattice. *KR1020190155732*, filed November 28, 2019.
4. Jung Hee Cheon, **Duhyeong Kim** and Dongwoo Kim. Apparatus for Processing Non-Polynomial Operation on Encrypted Messages and Methods Thereof. *KR1020190128403*, filed October 16, 2019.
3. Jung Hee Cheon, **Duhyeong Kim**, Yongsoo Song and Kyoohyung Han. Terminal Device Performing Homomorphic Encryption, Server Device Processing Ciphertext and Methods Thereof. *US16478596*, filed December 7, 2018.
2. Jung Hee Cheon, **Duhyeong Kim** and Yongsoo Song. Method for Homomorphic Encryption of Plain Text in Real Numbers. *KR1020180129749*, filed October 29, 2018, and issued October 29, 2019.
1. Joohee Lee, Jung Hee Cheon, **Duhyeong Kim** and Aaram Yun. Method for Key Generation, Encryption, and Decryption for Public Key Encryption Scheme Based on Module-Wavy and Module-LWR. *KR1020170183661*, filed December 29, 2017, and issued September 25, 2019.

AWARDS

5th Samsung DS Industry-Academy Cooperation Project Paper Award — Jul 2020
Excellence Award ($2,500) — *Samsung Electronics*

26th Samsung Humantech Paper Award — Feb 2020
Gold Award ($10,000); 1st place in CSE — *Samsung Electronics*

Runner-up: Asiacrypt 2019 Dec 2019
Invited to Journal of Cryptology *International Association for Cryptologic Research*

Korea Cryptography Contest Nov 2019
Excellence Award ($1,500) *Korea Institute of Information Security and Cryptology*

iDASH 2019 Oct 2019
One of the Winners of Track 2 *National Institutes of Health (NIH)*

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

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

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

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

University Students Contest of Mathematics Nov 2012
Silver Prize (Top 40) *Korean Mathematical Society*

Korean Mathematical Olympiad Nov 2009
Gold Prize (Top 40) *Korean Mathematical Society*

SERVICES

Reviewer / External Reviewer

- Designs, Codes and Cryptography (DCC), Journal of Cryptology (JoC), IEEE Transactions on Computers (TC), Journal of Biomedical and Health Informatics (JBHI)
- CRYPTO 2017; ASIACRYPT 2019; PKC 2020, 2019; CT-RSA 2019; ANTS 2020; FC 2017; PQCrypto 2020, 2019, 2018

TEACHING EXPERIENCE

Introduction to Cryptography Mar 2017 $\sim$ Jun 2017

Differential and Integral Calculus Mar 2015 $\sim$ Dec 2017

Linear Algebra Mar 2015 $\sim$ Dec 2017

GITHUB REPOSITORIES

`https://github.com/idashSNU/Imputation/tree/master/ModHEaaN` Light Version of HEAAN

`https://github.com/idashSNU/Imputation` HE-based Genotype Imputation

`https://github.com/LizardOpenSource/Lizard_c` Reference Implementation of Lizard

`https://github.com/du1204/EnsembleLR` HE-based Ensemble Logistic Regression

`https://github.com/du1204/iDASH2018` HE-based Semi-Parallel GWAS

LANGUAGES AND SKILLS

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

REFERENCES

Jung Hee Cheon	Professor at Seoul National University	jhcheon@snu.ac.kr
Damien Stehlé	Professor at ENS de Lyon	damien.stehle@ens-lyon.fr
Xiaoqian Jiang	Associate Professor at UTHealth	Xiaoqian.Jiang@uth.tmc.edu