DUHYEONG KIM

Curriculum Vitae

CONTACT INFORMATION

Affiliation	Intel Labs
Address	2111 NE 25th Ave, Hillsboro, OR 97124, USA
E-mail	`duhyeong.kim@intel.com`
Website	`https://du1204.github.io`

PROFESSIONAL EXPERIENCE

Research Scientist @ Intel Labs Apr 2021 ∼ Present
Security and Privacy Research *Hillsboro, OR, United States*

- *Technical lead* of FHE algorithm & workload team
- *Design* efficient cryptographic protocols with provable security
- *Implement* privacy solutions for real-world applications including ML and AI

EDUCATION

Seoul National University (SNU), Republic of Korea

Integrated M.S./Ph.D. in Mathematical Sciences Mar 2015 ∼ Feb 2021
Advisor: Prof. Jung Hee Cheon
Thesis: Machine Learning on Encrypted Data and Homomorphic Comparison [pdf]
Best PhD Dissertation Award from the College of Natural Sciences

B.S. in Mathematical Sciences Mar 2011 ∼ Feb 2015
Honers: *Summa Cum Laude*

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*

RESEARCH INTERESTS

- **Fully Homomorphic Encryption (FHE)**
  - Design, Optimization and Implementation
  - Privacy-preserving machine learning (PPML) / Private AI based on FHE
    - ✓ Logistic regression, clustering, neural network, similarity search, transformer, etc.
    - ✓ FHE-friendly polynomial approximation of non-polynomial functions
- **Zero-knowledge Proof (ZKP)**
  - Practical lattice-based ZKP with polynomial overhead
  - Hardness analysis on Learning with Errors (LWE) variants
- **Post-Quantum Cryptography**

- Practical public-key encryption, digital signature and identity-based encryption based on lattices
- Construction of practical lattice trapdoors

FUNDED RESEARCH PROJECTS

Fully Homomorphic Encryption and its Applications

3. "Data Protection in Virtual Environments (DPRIVE)". Supported by Defense Advanced Research Projects Agency (DARPA), 2021 ∼ 2024.
    - To develop and demonstrate a Fully Homomorphic Encryption (FHE) acceleration platform that delivers FHE computation within 10x of overhead with regard to unencrypted computation on best-known CPU-based computing platforms.
    - Technical lead of the FHE algorithm & workload team
        - SEAL-BGV and OpenFHE-CKKS w/ bootstrapping for small word-size architecture
        - Logistic regression, CNN inference, etc.
2. "Development and Library Implementation of Fully Homomorphic Machine Learning Algorithms supporting Neural Network Learning over Encrypted Data". Supported by the IITP Grant through the Korean Government, Apr 2020 ∼ Feb 2021.
1. "Development of homomorphic encryption for DNA analysis and biometry authentication". Supported by the IITP Grant through the Korean Government, Apr 2016 ∼ Dec 2018.

Post-Quantum Cryptography

2. "Development of lattice-based post-quantum public-key cryptographic schemes". Supported by the IITP Grant through the Korean Government, Apr 2017 ∼ Dec 2019.
1. "Development of light-weight public-key encryption based on new hard problems". Supported by the SRFC Grant through Samsung Electronics, Oct 2014 ∼ Sep 2017.

PUBLICATIONS

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

Conference

11. Gabrielle De Micheli, **Duhyeong Kim**, Daniele Micciancio and Adam Suhl. "Faster Amortized FHEW bootstrapping using Ring Automorphisms." IACR International Conference on Public-Key Cryptography (*PKC 2024*).
10. Rashmi Agrawal, Jung Ho Ahn, Flavio Bergamaschi, Ro Cammarota, Jung Hee Cheon, Fillipe D. M. de Souza, Huijing Gong, Minsik Kang, **Duhyeong Kim** et al. "High-precision RNS-CKKS on fixed but smaller word-size architectures: theory and application." Proceedings of the 11th Workshop on Encrypted Computing & Applied Homomorphic Cryptography (*WAHC 2023*).
9. **Duhyeong Kim**, Dongwon Lee, Jinyeong Seo and Yongsoo Song. "Proof of Plaintext Knowledge with Polynomial Overhead from Hint-RLWE." In Advances in Cryptology (*CRYPTO 2023*).
    ○ *Grand Award at Korea Cryptography Contest 2023 (1st place)*
8. Chris Wilkerson, Sachin Taneja, Raghavan Kumar, Sanu Mathew, Jeremy Casas, Jin Yang, Michael Steiner, Huijing Gong, Wen Wang, **Duhyeong Kim**, Ro Cammarota et al. "Intel® HERACLES: Homomorphic Encryption Revolutionary Accelerator with Correctness for Learning-oriented End-to-End Solutions." Presented at *GOMACTech 2023*.

7. Jung Hee Cheon, Dongwoo Kim, **Duhyeong Kim**, Joohee Lee and Yongsoo Song. ”Lattice-Based Secure Biometric Authentication for Hamming Distance.” Australasian Conference on Information Security and Privacy (*ACISP 2021*).

6. Jung Hee Cheon, Dongwoo Kim and **Duhyeong Kim**. “Efficient Homomorphic Comparison Methods with Optimal Complexity”. In International Conference on the Theory and Application of Cryptology and Information Security (*ASIACRYPT 2020*).
   - ○ *Gold Award at 26th Samsung Humantech Paper Award (1st place in Computer Science & Engineering)*

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 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 2019*).
   - ○ *Runner-up: Invited to Journal of Cryptology (Top 3 of 71 accepted papers among 307 submissions)*
   - ○ *Excellence Award at 5th 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 2019*).

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

Journal

8. *David Ha Eun Kang, **Duhyeong Kim**, Yongsoo Song, Dongwon Lee, Hyesun Kwak, and Brian W. Anthony. “Harnessing the potential of shared data in a secure, inclusive, and resilient manner via multi-key homomorphic encryption.” *Scientific Reports* (2024).

7. Jung Hee Cheon, Dongwoo Kim, **Duhyeong Kim** and Keewoo Lee. “On the Scaled Inverse of $(x_i - x_j)$ modulo Cyclotomic Polynomial of the form $\Phi_{p^s}(x)$ or $\Phi_{p^s q^t}(x)$”. *Journal of the Korean Mathematical Society* (2022).

6. *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.” *Cell Systems* (2021).

5. *Ha Eun David Kang, **Duhyeong Kim**, Sangwoon Kim, David Donghyun Kim, Jung Hee Cheon and Brian W. Anthony. “Homomorphic Encryption as a *secure PHM outsourcing solution for small and medium manufacturing enterprise.” *Journal of Manufacturing Systems* (2021).

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* (2016): 72-80.

MANUSCRIPTS

10. ***Duhyeong Kim**, *Yujin Nam, *Wen Wang, Huijing Gong, Ro Cammarota, Mariano Tepper, Ishwar Bhati, Theodore L. Willke and Tajana S. Rosing. "GraSS: Graph-based Similarity Search on Encrypted Query." Under submission.
9. *Meron Zerihun Demissie, Alexander Viand, **Duhyeong Kim**, Ro Cammarota and Todd Austin. "Automating Data-Oblivious Transformations for FHE." Under submission.
8. Jean-Philippe Bossuat, Ro Cammarota, Jung Hee Cheon, Ilaria Chillotti, Benjamin R. Curtis, Wei Dai, Huijing Gong, Erin Hales, **Duhyeong Kim** et al. "Security Guidelines for Implementing Homomorphic Encryption." Available at `https://eprint.iacr.org/2024/463.pdf`.
7. *Sejun Kim, *Wen Wang, ***Duhyeong Kim**, Adish Vartak, Michael Steiner, and Ro Cammarota. "Towards a Polynomial Instruction Based Compiler for Fully Homomorphic Encryption Accelerators." Available at `https://eprint.iacr.org/2024/707.pdf`.
6. Leo de Castro, **Duhyeong Kim**, Miran Kim, Keewoo Lee, Seonhong Min, Yongsoo Song. "More Efficient OLE and MPC Preprocessing or: Linear HE Circuit Privacy Almost For Free." Under the submission.
5. Jung Hee Cheon, Hyeongmin Choe, Saebyul Jung, **Duhyeong Kim**, Dah Hoon Lee, and Jai Hyun Park. "Arithmetic PCA for Encrypted Data." Available at `https://eprint.iacr.org/2023/1544.pdf`.
4. Jung Hee Cheon, Wonhee Cho and **Duhyeong Kim**. "Note on IND-CPA+ Security of CKKS."
3. Jung Hee Cheon, Seungwan Hong and **Duhyeong Kim**. "Remark on the Security of CKKS Scheme in Practice." Available at `https://eprint.iacr.org/2020/1581.pdf`.
2. 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`.
1. *Yongsoo Song, Jacek Cyranka, **Duhyeong Kim** and Sicun Gao. "Convergence and Oscillation of Low-Precision Stochastic Gradient Descent."

WORKING PAPERS

1. ***Duhyeong Kim** and Anupam Golder. "Modified Bit-wise FHE for Hardware Accelerators based on Polynomial-ISA."

TALKS

Exploring Private AI Solutions Through FHE
Joint Mathematics Meetings (JMM 2025) in Seattle, WA — Jan 2025 (planned)

Secure Graph-based Similarity Search based on FHE
SPR IL Talk at Intel Labs, Online — Oct 2024
Keynote Talk at Intel Crypto Frontier Center Workshop in Hillsboro, OR — Oct 2024

High-precision CKKS on small word-size architecture
Tech Talk at FHE.org, Online — Jan 2024
Keynote Talk at Intel Crypto Frontier Center Workshop in Hillsboro, OR — Oct 2023

Practical Proof of Knowledge Protocols based on Hint-MLWE

Crypto 2024 in Santa Barbara, CA August 2023
Crypto Winter Camp 2023 in Konjiam Resort, Republic of Korea Jan 2023

Faster Amortized FHEW Bootstrapping

Tech Talk at FHE.org, Online Feb 2023

High-quality FHE workloads with a focus on Logistic Regression in BGV

ESL Talk at Intel Labs, Online July 2022

Approximate FHE CKKS: A to Z

Tech Talk at NIST Crypto Reading Club, Online July 2022
PTR Talk at Intel Labs, Online May 2021

RLWE-based FHE: Capability, Algorithmic Complexity, and Security

ESL Talk at Intel Labs, Online Aug 2021

Complexity-Optimal Homomorphic Comparison

ASIACRYPT 2020 in Daejeon, Republic of Korea and Online Dec 2020
East Asian Core Doctoral Forum on Mathematics 2020 in Tokyo, Japan Jan 2020
Crypto Winter 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

Crypto Winter 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

9. Joohee Lee, Jung Hee Cheon, **Duhyeong Kim** and Aaram Yun. Method for generating public key and secret key based on module-wavy and module-lwr and method of encryption and decryption using the keys. *US11658819B2*, published May 23, 2023.

8. Jung Hee Cheon, **Duhyeong Kim** and Yongha Son. Methods of generating encryption key and digital signature based on lattices. *US11522718B2*, published December 6, 2022.

7. Jung Hee Cheon, **Duhyeong Kim** and Yongha Son. Identity-based encryption method based on lattices. *US20220021535A1*, published January 20, 2022.

6. Jung Hee Cheon, **Duhyeong Kim** and Yongha Son. ID-based Encryption over Generalized NTRU Trapdoor Lattice. *KR1020190155732*, filed November 28, 2019.

5. Jung Hee Cheon, **Duhyeong Kim** and Yongha Son. Method for Generating Encryption Key Based on Lattices and Signature Method Using thereof. *KR1020190155709*, 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, and issued August 27, 2021.

3. Jung Hee Cheon, **Duhyeong Kim**, Yongsoo Song and Kyoohyung Han. Terminal Device Performing Homomorphic Encryption, Server Device Processing Ciphertext and Methods Thereof. *US11101976B2*, published August 24, 2021.

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

Korea Cryptography Contest Oct 2023
Grand Award ($10,000); 1st place *Korea Institute of Information Security and Cryptology*

PhD Dissertation Award Feb 2021
Best Award in Mathematical Sciences *College of Natural Sciences, Seoul National University*

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

Global PhD Fellowship Mar 2016 ∼ 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 ∼ 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

Editor / Co-Editor

- ISO/IEC 28033-3 Fully homomorphic encryption (Part 3: Mechanisms for arithmetic on approximate numbers)

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 2022, 2021, 2020, 2019; CT-RSA 2019; AsiaCCS 2023; ANTS 2020; FC 2017; PQCrypto 2020, 2019, 2018; ACISP 2021; WAHC 2019

TEACHING EXPERIENCES

Computational Number Theory	Sep 2020 ∼ Dec 2020
Introduction to Cryptography	Mar 2017 ∼ Jun 2017
Differential and Integral Calculus	Mar 2015 ∼ Dec 2017
Linear Algebra	Mar 2015 ∼ Dec 2017

GITHUB REPOSITORIES (PUBLIC)

`https://github.com/idashSNU/Imputation/tree/master/ModHEaaN`	Light Version of HEAAN
`https://github.com/idashSNU/Imputation`	HE-based Genotype Imputation (iDASH'19)
`https://github.com/du1204/iDASH2018`	HE-based Semi-Parallel GWAS (iDASH'18)
`https://github.com/du1204/EnsembleLR`	HE-based Ensemble Logistic Regression
`https://github.com/LizardOpenSource/Lizard_c`	PoC Implementation of Lizard

LANGUAGES AND SKILLS

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

REFERENCES

Ro Cammarota	Sr. Principal Engineer at Intel Labs	`rosario.cammarota@intel.com`
Jung Hee Cheon	Professor at SNU & CEO at CryptoLab	`jhcheon@snu.ac.kr`
Damien Stehlé	Chief Scientist at CryptoLab	`damien.stehle@gmail.com`
Xiaoqian Jiang	Associate Professor at UTHealth	`Xiaoqian.Jiang@uth.tmc.edu`
Daniele Micciancio	Professor at UCSD	`daniele@cs.ucsd.edu`
Yongsoo Song	Assistant Professor at SNU	`y.song@snu.ac.kr`
Miran Kim	Assistant Professor at Hanyang Univ.	`miran@hanyang.ac.kr`

Last updated on November 18, 2024