Duhyeong **Kim**

SOFTWARE ENGINEER, MACHINE LEARNING · CRYPTOGRAPHY, SECURITY AND PRIVACY

12355 NE District Way, Bellevue, WA 98005

☎ (+1) 650-787-7595 | ✉ duhyeongkim@meta.com | ⌂ https://du1204.github.io/ | du1204 | duhyeongkim

"Great things begin where uncommon paths cross."

Experience

Meta Platforms, Inc. — *Bellevue, WA*

SOFTWARE ENGINEER, MACHINE LEARNING — *Jul 2025 - Present*

- Develop Empirical DP techniques within a privacy-preserving machine learning (PPML) framework for feature-level privacy quantification.
- Integrate state-of-the-art ML models (e.g., LLMs, Sequential Learning) to optimize performance under privacy constraints in Ads ranking.

Intel Labs — *Hillsboro, OR*

RESEARCH SCIENTIST/ENGINEER — *Apr 2021 - Jul 2025*

- Security and Privacy Research (SPR)
- HERACLES: Fully homomophic encryption (FHE) HW accelerator
  - *Technical lead* of the FHE algorithm and workload team.
  - *Designed* efficient cryptographic protocols with provable security.
  - *Implemented* privacy solutions for real-world applications, including ML/AI based on FHE.
  - Participated in the DPRIVE program funded by DARPA.
- Knowledge transfer of cryptographic algorithms and security to the teams of SW/HW engineers
- Technical Mentor of the Intel-academia cooperative research program (Crypto Frontier Center)
- Co-led the international standardization process of FHE algorithms.

UTHealth Houston — *Houston, TX*

VISITING RESEARCHER (HOSTED BY PROF. XIAOQIAN JIANG) — *Aug 2018*

- Developed efficient FHE algorithms for principal component analysis (PCA).

ENS de Lyon — *Lyon, France*

VISITING RESEARCHER (HOSTED BY PROF. DAMIEN STEHLÉ) — *Dec 2017 - Jan 2018*

- Analyzed the theoretical hardness of several algebraic variants of LWE, including binary RLWE.

Education

Seoul National University — *Seoul, Republic of Korea*

INTEGRATED M.S./PH.D. IN CRYPTOGRAPHY — *Mar 2015 - Feb 2021*

- Advisor: Prof. Jung Hee Cheon
- Thesis: Machine Learning on Encrypted Data and Homomorphic Comparison [pdf]
- Honers: *Best PhD Dissertation Award from the College of Natural Sciences*

Seoul National University — *Seoul, Republic of Korea*

B.S. IN MATHEMATICAL SCIENCES — *Mar 2011 - Feb 2015*

- Honers: *Summa Cum Laude* (Major GPA: 4.13/4.3)

Honors & Awards

2023	**Grand Award (1st Place)**, Korea Cryptography Contest	*Republic of Korea*
2023	**Best Award in Mathematical Sciences**, PhD Dissertation Award in College of Natural Science, SNU	*Republic of Korea*
2020	**Excellence Award**, Samsung DS Industry-Academy Cooperation Project Paper Award	*Republic of Korea*
2020	**Gold Award (1st Place in CSE)**, 26th Samsung Humantech Paper Award	*Republic of Korea*
2019	**Runner-up (Invited to Journal of Cryptology)**, Asiacrypt 2019 Paper Award	*Kobe, Japan*
2019	**Excellence Award**, Korea Cryptography Contest	*Republic of Korea*
2019	**Runner-up**, IDASH Secure Genome Analysis Competition	*Bloomington, IN*
2018	**Global Empowerment Program ($5,000)**, Top 10% of Global PhD Fellowship	*Republic of Korea*
2016	**Global PhD Fellowship**, Research Grant from National Research Foundation of Korea	*Republic of Korea*
2016	**Awards for Excellence in Teaching**, Differential and Integral Calculus in SNU	*Republic of Korea*
2012	**Silver Prize**, University Students Contest of Mathematics	*Republic of Korea*
2011	**Presidential Science Scholarship**, Academic Grant from Korea Student Aid Foundation	*Republic of Korea*
2009	**Gold Prize**, Korean Mathematical Olympiad	*Republic of Korea*

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. “Toward Practical Lattice-based Proof of Knowledge from Hint-MLWE.” 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

9. 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.” IACR Communications in Cryptology (2024).
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.

Preprints

9. ***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.
8. *Meron Zerihun Demissie, Alexander Viand, **Duhyeong Kim**, Ro Cammarota and Todd Austin. "Automating Data-Oblivious Transformations for FHE." Under submission.
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."

Presentation

Exploring Private AI Solutions Through FHE

- Joint Mathematics Meetings (JMM 2025) in Seattle, WA — Jan 2025

Secure Graph-based Similarity Search based on FHE

- SPR IL Talk at Intel Labs, Online — Oct 2024
- Keynote Talk at 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 Crypto Frontier Center Workshop in Hillsboro, OR — Oct 2023

Practical Proof of Knowledge Protocols based on Hint-MLWE

- Crypto 2023 in Santa Barbara, CA — Aug. 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 through Composite Polynomials

- 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

- 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

Services

2023 - Present **Co-Editor**, ISO/IEC 28033-3 Fully Homomorphic Encryption (Part 3) *International*

2015 - Present **Paper Review**, Designs, Codes and Cryptography (DCC); Journal of Cryptology (JoC); IEEE Transactions on Computers (TC); Journal of Biomedical and Health Informatics (JBHI); CRYPTO 2017; ASIACRYPT 2025, 2019; TCC 2025; PKC 2022, 2021, 2020, 2019; CT-RSA 2019; AsiaCCS 2023; ANTS 2020; FC 2017; PQCrypto 2020, 2019, 2018; ACISP 2021; WAHC 2019 *International*

Skills

Programming	C, C++, Python, Sage, LaTeX
Languages	Korean (native), English (fluent)

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`