

# 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** Apr 2021 ~ Present  
Security and Privacy Research, Intel Labs *OR, United States*

## 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  
Honors: *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

---

- **Homomorphic Encryption (HE)**
  - Construction of new HE schemes and algorithms
  - Privacy-preserving machine learning (PPML) based on HE
    - ✓ Transformation of ML algorithms into HE-friendly forms
    - ✓ Complexity-optimal polynomial approximation method
- **Lattice-based Cryptography**
  - Practical post-quantum cryptosystems
  - Construction of practical lattice trapdoors
  - Reduction and analysis on lattice-based hard problems

## RESEARCH PROJECTS

---

### Homomorphic Encryption and its Applications

3. “Data Protection in Virtual Environments (DPRIVE)”. Supported by Defense Advanced Research Projects Agency (DARPA), 2021 ~ present.
  - 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.
  - Main Contributor of algorithm and software development on FHE bootstrapping and applications.
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.” To Appear at PKC 2024.
10. Rashmi Agrawal, Jung Ho Ahn, Flavio Bergamaschi, Rosario 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), pp. 549580. Springer, Cham. 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), pp. 653-672. Springer, Cham, 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), pp. 221-256. Springer, Cham, 2020.

- *Gold Award at 26<sup>th</sup> Samsung Humantech Paper Award (1<sup>st</sup> 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), 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.
  - *Runner-up: Invited to Journal of Cryptology (Top 3 of 71 accepted papers among 307 submissions)*
  - *Excellence Award at 5<sup>th</sup> 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

- 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* 168 (2016): 72-80.

## MANUSCRIPTS

---

- 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”.

## TALKS

---

### **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

### **Proof of Plaintext Knowledge with Polynomial Overhead**

Crypto Winter Camp 2023 in Konjiam Reseort, Republic of Korea

Jan 2023

### **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

---

<b>Korea Cryptography Contest</b> Grand Award (\$10,000); 1st place	Oct 2023 <i>Korea Institute of Information Security and Cryptology</i>
<b>PhD Dissertation Award</b> Best Award in Mathematical Sciences	Feb 2021 <i>College of Natural Sciences, Seoul National University</i>
<b>5<sup>th</sup> Samsung DS Industry-Academy Cooperation Project Paper Award</b> Excellence Award (\$2,500)	Jul 2020 <i>Samsung Electronics</i>
<b>26<sup>th</sup> Samsung Humantech Paper Award</b> Gold Award (\$10,000); 1st place in CSE	Feb 2020 <i>Samsung Electronics</i>
<b>Runner-up: Asiacrypt 2019</b> Invited to Journal of Cryptology	Dec 2019 <i>International Association for Cryptologic Research</i>
<b>Korea Cryptography Contest</b> Excellence Award (\$1,500)	Nov 2019 <i>Korea Institute of Information Security and Cryptology</i>
<b>iDASH 2019</b> One of the Winners of Track 2	Oct 2019 <i>National Institutes of Health (NIH)</i>
<b>Global Empowerment Program</b> For top 10% of Global PhD Fellowship; Grant: \$5,000	May 2018 <i>National Research Foundation of Korea</i>
<b>Global PhD Fellowship</b> Research Grant: Tuition+\$20,000/year for 5 years	Mar 2016 ~ Present <i>National Research Foundation of Korea</i>
<b>Awards for Excellence in Teaching</b> For teaching Differential and Integral Calculus	Mar 2016 <i>Seoul National University</i>
<b>The Presidential Science Scholarship</b> Academic Grant: Tuition+\$5,000/year for 4 years	Mar 2011 ~ Feb 2015 <i>Korea Student Aid Foundation</i>
<b>University Students Contest of Mathematics</b> Silver Prize (Top 40)	Nov 2012 <i>Korean Mathematical Society</i>

## 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 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)

---

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

## LANGUAGES AND SKILLS

---

<b>Languages</b>	Korean (native), English (fluent)
<b>Skills</b>	C/C++, Python, L <sup>A</sup> T <sub>E</sub> X

## REFERENCES

---

Rosario Cammarota	Principal Engineer at Intel Labs	<a href="mailto:rosario.cammarota@intel.com">rosario.cammarota@intel.com</a>
Jung Hee Cheon	Professor at SNU & CEO at CryptoLab	<a href="mailto:jhcheon@snu.ac.kr">jhcheon@snu.ac.kr</a>
Damien Stehlé	Chief Scientist at CryptoLab	<a href="mailto:damien.stehle@gmail.com">damien.stehle@gmail.com</a>
Xiaoqian Jiang	Associate Professor at UTHHealth	<a href="mailto:Xiaoqian.Jiang@uth.tmc.edu">Xiaoqian.Jiang@uth.tmc.edu</a>
Yongsoo Song	Assistant Professor at SNU	<a href="mailto:y.song@snu.ac.kr">y.song@snu.ac.kr</a>
Miran Kim	Assistant Professor at Hanyang Univ.	<a href="mailto:miran@hanyang.ac.kr">miran@hanyang.ac.kr</a>