

# Andrey Kim

동탄기흥로 393-15, 1503동, 2601호, 화성시, 경기도, 대한민국, 18479

✉ kimandr.kz@gmail.com

🌐 kimandrik

🔗 kimandrik

☎ +82 10 6695 1989

## EDUCATION

---

### Seoul National University

Seoul, South Korea

*PhD in Mathematics: 3.65/4.00*

*Sep. 2014 - Aug. 2019*

**Thesis:** Multivariate Homomorphic Encryption for Approximate Matrix Arithmetics

### Moscow State University

Moscow, Russia

*Specialist (eq. MA) in Mathematics: 4.88/5.00*

*Sep. 2006 - Jun. 2011*

**Thesis:** On testing statistical hypotheses for a Brownian motion with changing drift term

## EXPERIENCE

---

### Samsung Advanced Institute of Technology

Suwon, Republic of Korea

*Staff Researcher*

*Oct. 2020 - now*

- Researching on HE schemes.

### New Jersey Institute of Technology

Newark, NJ, USA

*Research Scientist*

*Jan. 2020 - Aug. 2020*

- contribute to PALISADE library.

### Cryptolab

Seoul, Republic of Korea

*Cryptographic Engineer*

*Mar. 2019 - Aug. 2019*

- develop HEAAN library.

### Deutsche Bank

Moscow, Russia

*Java Quant Developer*

*Apr. 2013 - Jul. 2014*

- develop mathematical and statistical methods for trading.

## HONORS AND AWARDS

---
























- 2017 Best Solution, iDASH Genomic Data Privacy and Security Protection Competition 2017
- 2017 Excellence Award, Crypto Contest, Korea Cryptography Forum 2017
- 2016 Best Award, Crypto Contest, Korea Cryptography Forum 2016
- 2004-2006, 45-47th International Mathematical Olympiad (Gold Medal, Silver Medal, Bronze Medal)
- 2004-2006 21-23rd Balkan Mathematical Olympiad (Silver Medal, Gold Medal, Gold Medal)

## ADDITIONAL

---

- Programming: Java, C++, R, Matlab, Python
- Passed CFA Level 1
- Coursera: Deep Learning Specialization, Python for Everybody, Machine Learning with TensorFlow on Google Cloud Platform
- Languages: Russian/Native, English/Fluent, Korean/Beginner
- Work Permission: South Korea (F5 visa)
- ORCID: 0000-0002-0974-6787

## PUBLICATIONS

- Andrey Kim, Yongwoo Lee, Maxim Deryabin, Jieun Eom, Rakyong Choi. *LFHE: Fully Homomorphic Encryption with Bootstrapping Key Size Less than a Megabyte*. 
- Ahmad Al Badawi, Jack Bates, Flavio Bergamaschi, David Bruce Cousins, Saroja Erabelli, Nicholas Genise, Shai Halevi, Hamish Hunt, Andrey Kim, Yongwoo Lee, Zeyu Liu, Daniele Micciancio, Ian Quah, Yuriy Polyakov, Saraswathy R.V., Kurt Rohloff, Jonathan Saylor, Dmitriy Suponitsky, Matthew Triplett, Vinod Vaikuntanathan, Vincent Zucca. *OpenFHE: Open-Source Fully Homomorphic Encryption Library*. In: WAHC'22  
- Yongwoo Lee, Daniele Micciancio, Andrey Kim, Rakyong Choi, Maxim Deryabin, Jieun Eom, Donghoon Yoo. *Efficient FHEW Bootstrapping with Small Evaluation Keys, and Applications to Threshold Homomorphic Encryption*. In: Advances in Cryptology – EUROCRYPT 2023 
- Andrey Kim, Maxim Deryabin, Jieun Eom, Rakyong Choi, Yongwoo Lee, Whan Ghang, Donghoon Yoo. *General Bootstrapping Approach for RLWE-based Homomorphic Encryption*. In: IEEE Transactions on Computers 
- Jaehee Jang, Andrey Kim, Byunggook Na, Younho Lee, Donggeon Yhee, Byoungnan Lee, Jung Hee Cheon, Sungroh Yoon. *Privacy-Preserving Deep Sequential Model with Matrix Homomorphic Encryption*. In: Asia CCS 2022. 
- Andrey Kim, Yuriy Polyakov, Vincent Zucca. *Revisiting Homomorphic Encryption Schemes for Finite Fields*. In: Advances in Cryptology - ASIACRYPT 2021.  
- Andrey Kim, Antonis Papadimitriou, Yuriy Polyakov. *Approximate Homomorphic Encryption with Reduced Approximation*. In: Topics in Cryptology - CT-RSA 2022.  
- Duhyeong Kim, Yongha Son, Dongwoo Kim, Andrey Kim, Seungwan Hong, Jung Hee Cheon. *Privacy-preserving Approximate GWAS computation based on Homomorphic Encryption*. BMC Med Genomics 13, 77 (2020).  
- Jung Hee Cheon, Andrey Kim, Donggeon Yhee *Multi-dimensional Packing for HEAAN for Approximate Matrix Arithmetics*.  
- Jung Hee Cheon, Kyoohyung Han, Andrey Kim, Miran Kim, Yongsoo Song. *A Full RNS Variant of Approximate Homomorphic Encryption*. In: Cid C., Jacobson Jr. M. (eds) Selected Areas in Cryptography – SAC 2018. SAC 2018. Lecture Notes in Computer Science, vol 11349. Springer, Cham.  
- Andrey Kim, Miran Kim, Yongsoo Song, Keewoo Lee, Jung Hee Cheon. *Logistic regression model training based on the approximate homomorphic encryption*. BMC Med Genomics 11, 83 (2018).  
- Junsoo Kim, Chanhwa Lee, Hyungbo Shim, Jung Hee Cheon, Andrey Kim, Miran Kim, and Yongsoo Song, *Encrypting Controller using Fully Homomorphic Encryption for Security of Cyber- Physical Systems*. 6th IFAC Workshop on Distributed Estimation and Control in Networked Systems, IFAC-PapersOnLine, 2016, 49.22: 175-180. 
- Jung Hee Cheon, Kyoohyung Han, Andrey Kim, Miran Kim, Yongsoo Song. *Bootstrapping for Approximate Homomorphic Encryption*. In: Nielsen J., Rijmen V. (eds) Advances in Cryptology – EUROCRYPT 2018. EUROCRYPT 2018. Lecture Notes in Computer Science, vol 10820. Springer, Cham.  
- Jung Hee Cheon, Andrey Kim, Miran Kim, Yongsoo Song. *Homomorphic Encryption for Arithmetic of Approximate Numbers*. In: Takagi T., Peyrin T. (eds) Advances in Cryptology – ASIACRYPT 2017. ASIACRYPT 2017. Lecture Notes in Computer Science, vol 10624. Springer, Cham.  

## PATENTS

---

- Jung Hee Cheon, Yongsoo Song, Andrey Kim, Miran Kim, Kyoohyung Han. *Apparatus for approximately processing encrypted messages and methods thereof*  
<https://patents.google.com/patent/US11115182B2>
- Jung Hee Cheon, Andrey Kim, Donggeon Yhee. *Operating device and method using multivariate packing*  
<https://patents.google.com/patent/US20220029783A1>
- Eom Jieun, Andrey Kim, Deriabin Maksim, Choi Rakyong, Whan Ghang, Dong-hoon Yoo, Yongwoo Lee. *Method and apparatus for modulus refresh in homomorphic encryption*  
<https://patents.google.com/patent/US20220376890A1/en>
- Eom Jieun, Maksim Deriabin, Andrey Kim, Yongwoo Lee, Choi Rakyong, Whan Ghang, Donghoon Yoo. *Encryption key generating method, apparatus, ciphertext operation method and apparatus using the generated encryption key*  
<https://patents.google.com/patent/US20220385461A1/en>
- Yongwoo Lee, Andrey Kim, Maksim Deriabin, Eom Jieun, Donghoon Yoo, Choi Rakyong. *Homomorphic encryption apparatus and method*  
<https://patents.google.com/patent/US20230171085A1/en>
- Yongwoo Lee, Andrey Kim, Choi Rakyong, Maksim Deriabin, Eom Jieun, Donghoon Yoo. *Apparatus and method with homomorphic encryption using automorphism*  
<https://patents.google.com/patent/US20230246807A1/en>