Miran Kim

50 UNIST-gil, Ulju-gun, Ulsan, South Korea
mirankim@unist.ac.kr +82 (052) 217-2256

EDUCATION

Seoul National University, Seoul, Republic of Korea

- Ph.D. in Mathematical Sciences — Mar 2012 – Feb 2017
  - Thesis: Arithmetics of Ciphertexts under Homomorphic Encryption
  - Advisor: Prof. Jung Hee Cheon
- M.S. in Mathematical Sciences — Mar 2010 – Feb 2012
  - Thesis: A New Young Wall Realization of the Kirillov-Reshetikhin Crystal $\mathbf{B}(\omega_2)$ for $U_q(D_3^{(2)})$
  - Advisor: Prof. Seok Jin Kang
- B.S. in Mathematical Education — Mar 2006 – Feb 2010

WORK EXPERIENCE

Ulsan National Institute of Science and Technology, Ulsan, South Korea — Aug 2020 – Present

- Assistant Professor, Department of Computer Science and Engineering
- Assistant Professor, Artificial Intelligence Graduate School

University of Texas, Health Science Center at Houston, TX, United States — May 2018 – Jul 2020

- Assistant Professor, School of Biomedical Informatics

University of California, San Diego, CA, United States — Mar 2017 – Apr 2018

- Postdoctoral Researcher, Division of Biomedical Informatics, School of Medicine
- Supervisor: Dr. Xiaoqian Jiang

Microsoft Research, WA, United States — Jan 2015 – Apr 2015

- Research Intern in the Cryptography and Privacy Research Group
- Mentor: Dr. Kristin Lauter

Seoul National University, Seoul, South Korea — Jan 2013 – Feb 2017

- Research assistant, Department of Mathematical Sciences

SELECTED PUBLICATIONS

REFEREED CONFERENCE PUBLICATIONS

[C09] H. Chen, **M. Kim**, I. Razenshteyn, D. Rotaru, Y. Song, and S. Wagh: Maliciously secure matrix multiplication with applications to private deep learning. To appear in *Proceedings of the International Conference on the Theory and Applications of Cryptology and Information Security–ASIACRYPT 2020*.

[C08] H. Chen, W. Dai, **M. Kim**, and Y. Song: Efficient multi-key homomorphic encryption with packed ciphertexts with application to oblivious neural network inference. In *Proceedings of the ACM SIGSAC Conference on Computer and Communications Security–CCS*, pp.395-412, 2019.

[C07] X. Jiang, **M. Kim**, K. Lauter, and Y. Song: Secure outsourced matrix computation and application to neural networks. In *Proceedings of the ACM SIGSAC Conference on Computer and Communications Security–CCS*, pp.1209-1222, 2018.

[C06] J. H. Cheon, K. Han, A. Kim, **M. Kim**, and Y. Song: A full RNS variant of approximate homomorphic encryption. In *Proceedings of the International Conference on Selected Areas in Cryptography–SAC*, LNCS, vol:11349, pp.347-368, 2018.

[C05] J. H. Cheon, K. Han, A. Kim, **M. Kim**, and Y. Song: Bootstrapping for approximate homomorphic encryption. In *Proceedings of the Annual International Conference on the Theory and Applications of Cryptographic Techniques–EUROCRYPT*, LNCS, vol:10820, pp.360-384, 2018.

[C04] J. H. Cheon, A. Kim, **M. Kim**, and Y. Song: Homomorphic encryption for arithmetic of approximate numbers. In *Proceedings of the International Conference on the Theory and Applications of Cryptology and Information Security–ASIACRYPT 2017*, LNCS, vol:10624, pp.409-437, 2017.

[C03] J. Kim, C. Lee, H. Shim, J. H. Cheon, A. Kim, **M. Kim**, and Y. Song: Encrypting controller using fully homomorphic encryption for security of cyber-physical systems. In *Proceedings of the IFAC Workshop on Distributed Estimation and Control in Networked Systems–NECSYS*, 49(22):175-180, 2016.

[C02] J.H. Cheon, **M. Kim**, and K. Lauter: Homomorphic computation of edit distance. In *Proceedings of the Financial Cryptography and Data Security–FC*, LNCS, vol:8976, pp.194-212, 2015.

[C01] J.H. Cheon, **M. Kim**, and M. Kim: Search-and-compute on encrypted data. In *Proceedings of the Financial Cryptography and Data Security–FC*, LNCS, vol:8976, pp.142-159, 2015.

REFEREED JOURNAL PUBLICATIONS

[J11] S. Karimi, X. Jiang, R. Dolin, **M. Kim**, and Aziz Boxwala: A secure system for genomics clinical decision support. To appear in *Journal of Biomedical Informatics*, 2020.

[J10] JL Raisaro, F. Marino, J. Troncoso-Pastoriza, R. Beau-Lejdstrom, R. Bellazz, E. V. Bernstam, M. Bucalo, Yong Chen, A. Gottlieb, A. Harmanci, **M. Kim**, Y. Kim, J. Klann, C. Klersy, B. A. Malin, M. Méan, F. Prasser, L. Scudeller, A. Torkamani, J. Vaucher, M. Puppala, S. T.C. Wong, M. Frenkel-Morgenstern, H. Xu, B. M. Musa, A. G. Habib, A. Wilcox, H. M. Salihu, H. Sofia, X. Jiang, JP Hubaux: SCOR: A secure international informatics infrastructure to investigate COVID-19. *Journal of the American Medical Informatics Association*; ocaa172, 2020.

[J09] **M. Kim**, Y. Song, B. Li, and D. Micciancio: Semi-parallel logistic regression for GWAS on encrypted data. *BMC Medical Genomics*; 13(99), 2020.

[J08] **M. Kim**, J. Lee, L. Ohno-Machado, and X. Jiang: Secure and differentially private logistic regression for horizontally distributed data. *IEEE Transactions on Information Forensics and Security*; 15(1):695-710, 2019.

[J07] Y. Jiang, J. Hamer, C. Wang, X. Jiang, **M. Kim**, Y. Song, Y. Xia, N. Mohammed, M. N. Sadat, and S. Wang: SecureLR: Secure Logistic Regression model via a hybrid cryptographic protocol: *IEEE/ACM Transactions on Computational Biology and Bioinformatics*;16(1):113-123, 2019.

[J06] A. Kim, Y. Song, **M. Kim**, K. Lee, and J. H. Cheon: Logistic regression model training based on the approximate homomorphic encryption. *BMC Medical Genomics*;11:S4, 2018.

[J05] **M. Kim**, Y. Song, S. Wang, Y. Xia, and X. Jiang: Secure logistic regression based on homomorphic encryption: design and evaluation. *JMIR Med Inform*;6(2):e19, 2018.

[J04] **M. Kim**, Y. Song, and J. H. Cheon: Secure searching of biomarkers using hybrid homomorphic encryption scheme. *BMC Medical Genomics*;10:42, 2017.

[J03] J.H. Cheon, **M. Kim**, and M. Kim: Optimized search-and-compute circuits and their application to query evaluation on encrypted data. *IEEE Transactions on Information Forensics and Security*; 11(1):188-199, 2016.

[J02] S. Wang, Y. Zhang, W. Dai, K. Lauter, **M. Kim**, Y. Tang, H. Xiong, and X. Jiang: HEALER: Homomorphic computation of ExAct Logistic rEgRession for secure rare disease variants analysis in GWAS. *Bioinformatics*; 32(2):211-218, 2016.

[J01] **M. Kim** and K. Lauter: Private genome analysis through homomorphic encryption. *BMC Medical Informatics and Decision Making*; 15(Suppl 5):S3, 2015.

TECHNICAL REPORTS

[T02] J.H. Cheon, A. Costache, R.C. Moreno, W. Dai, N. Gama, M. Georgieva, S. Halevi, **M. Kim**, S. Kim, K. Laine, Y. Polyakov, Y. Song: Introduction to Homomorphic Encryption. To be available at HomomorphicEncryption.org. 2020.

[T01] M. Brenner, W. Dai, S. Halevi, K. Han, A. Jalali, **M. Kim**, K. Laine, A. Malozemoff, P. Paillier, Y. Polyakov, K. Rohloff, E. Savaş, and B. Sunar: A standard API FOR RLWE-based homomorphic encryption. Available at HomomorphicEncryption.org. 2017.

ABSTRACTS

[A02] **M. Kim**: Homomorphic encryption for protecting genome privacy. In *Proceedings of IEEE EMBS International Conference on Biomedical and Health Informatics-BHI 2019.* 2019.

[A01] Y. Zhang, W. Dai, S. Wang, **M. Kim**, K. Lauter, J. Sakuma, H. Xiong, and X. Jiang: SECRET: Secure Edit distance Computation over homomoRphic EncrypTed data. In *Proceedings of the 5th Annual Translational Bioinformatics Conference–TBC*, 2015.

PATENTS

[P06] Apparatus for approximately processing encrypted messages and methods thereof, US Patent App. US 20200036511A1, Jan 2020.

[P05] Apparatus for processing approximate encrypted messages and methods thereof, KR-102040120-B1, application date: Nov 2019.

[P04] Method and system for communicating homomorphically encrypted data, US Patent App. US10198592B2, publication date: Feb 2019.

[P03] Method for Processing Dynamic Data by Homomorphic Encryption, KR-101919940-B1, publication date: Nov 2018.

[P02] Method for Calculating Edit Distance Between DNA Genomic Sequence through Homomorphic Encryption, KR-101817087-B1, publication date: Jan 2018.

[P01] A Method for Managing Data and Apparatuses therefor, KR-20170004456-A, publication date: Jan 2017.

PROJECTS

- *PI* in a Seed grant by UNIST (1.200109): "Secure genomic analysis on encrypted data" (10/1/2020-present)
- *Co-I* in an Institute of Information & communications Technology Planning & Evaluation (IITP) by the Korea government (MSIT) (2020-0-01336): "Articifial intelligence graduate school support" (9/1/2020-present)
- Microsoft Research Award - 2019 Dr. Kim's Research Collaboration ($55,000)
- *Co-PI* in NIH R41 grant (R41HG010978): "Secure Outsourced computation of genomic data" ($344,948, 9/9/2019-8/31/2020, PI: Karimi)
- *Co-I* in Cancer Prevention Research Institute of Texas (CPRIT) Rising Stars Award (CPRIT RR180012): "Cancer Phenotyping for personalized combinatorial drug therapy" ($939,405, 5/1/2018-4/30/2023, PI: Jiang)
- *Co-I* in an NIH R01 grant (R01GM124111): "Privacy-preserving methods and tools for handling missing data in distributed health data networks" ($475,135, 09/08/2017-06/30/2021, PI: Qi)
- *Co-I* in an NIH U01 grant (U01EB023685): "Encryption methods and software for privacy-preserving analysis of biomedical data" (10/01/16 - 04/30/18, PI: Tang)
- *Co-I* in Samsung grant: "Development of homomorphic encryption for data analysis" (2015 - 2016, PI: Cheon)
- *Co-I* in Samsung grant: "Fusion-based next generation privacy/sw security technology" (2014 - 2015, PI: Cheon)
- *Co-I* in Samsung grant: "A development of public key encryption for the hybrid scheme which combines public key" (2013 - 2014, PI: Cheon)

PROFESSIONAL SERVICE

- Organizer of the iDASH Privacy Workshop 2019-Present
- Program committee for Genome Privacy and Security (GenoPri) 2019-Present
- Program committee for Mathcrypt 2019
- Member for the Global Alliance for Genomics and Health (GA4GH) Data Security 2019

HONORS & AWARDS

- First Prize, iDASH Genomic Data Privacy and Security Protection Competition 2018 Oct 2018
  Organized by NIH, http://www.humangenomeprivacy.org/2018/
- Awards for Young Korean Female Mathematicians Jun 2018
  Organized by Korean Women in Mathematics Sciences, http://www.kwms.or.kr/index.php?mp=5_4.
- First Prize, iDASH Genomic Data Privacy and Security Protection Competition 2017 Oct 2017
  Organized by NIH, http://www.humangenomeprivacy.org/2017/
- Excellence Award, Crypto Contest Oct 2017
  Korea Cryptography Forum.
- Second Prize, iDASH Genomic Data Privacy and Security Protection Competition 2016 Nov 2016
  Organized by NIH, http://www.humangenomeprivacy.org/2016/
- Grand Prize Crypto Contest Oct 2016
  Korea Cryptography Forum.
- Special Prize Crypto Contest Nov 2015
  Korea Cryptography Forum.
- First Prize, iDASH Genomic Data Privacy and Security Protection Competition 2015 Mar 2015

Organized by NIH, http://www.humangenomeprivacy.org/2015/

- BK 21+ Scholarship 2013 – 2015
  Ministry of Education of Korea.
- Outstanding Teaching Assistant Awards Feb 2011
  Seoul National University.
- BK 21 Scholarship 2010 – 2012
  Ministry of Education of Korea.
- Korea Student Aid Foundation – National Science and Engineering Scholarship 2006 – 2009

PRESENTATIONS

- Homomorphic encryption and its application to Private AI Sep 2020
  UNIST AIGS Workshop, Ulsan, Republic of Korea.
- The iDASH Competition: Progress of homomorphic encryption for genomic privacy Apr 2020
  Simons Workshop: From theory to practice, The Simons Institute for the Theory of Computing, Berkeley, CA, USA.
- Practical applications of homomorphic encryption Dec 2019
  Guest seminar, Department of Mathematics, Hanyang University, Seoul, Republic of Korea.
- Practical applications of homomorphic encryption Dec 2019
  Samsung Advanced Institute of Technology Seminar, Seoul, Republic of Korea.
- Practical applications of homomorphic encryption Dec 2019
  International Conference on Information Security and Cryptology (ICISC) 2019, Seoul, Republic of Korea.
- Efficient multi-key homomorphic encryption and application to neural network inference Oct 2019
  Genome Privacy and Security (GenoPri) 2019, Boston, USA.
- Introduction to homomorphic encryption May 2019
  Guest seminar, Department of Electrical and Computer Engineering, Rice University, Houston, TX, USA.
- Homomorphic encryption for protecting genome privacy May 2019
  IEEE EMBS International Conference on Biomedical and Health Informatics 2019, Chicago, IL, USA.
- Practical applications of homomorphic encryption Jan 2019
  The workshop of The rising of biomedical informatics: hammers and nails,
  University of Texas, Health Science Center at Houston, Houston, TX, USA.
- Secure outsourced matrix computation and application to neural networks Oct 2018
  ACM SIGSAC Conference on Computer and Communications Security 2018, Toronto, ON, Canada.
- Semi-parallel logistic regression based on RNS-CKKS Oct 2018
  iDASH Genomic Data Privacy and Security Protection Workshop 2018, San Diego, CA, USA.
- Homomorphic encryption for protecting genomic privacy Oct 2018
  Guest seminar, University of Texas, Health Science Center at Houston, Houston, TX, USA.
- Progress on genome privacy and security Jul 2018
  Seoul National University Bundang Hospital - Big Data Center Seminar, Bundang, Republic of Korea.
- Secure logistic regression model training based on homomorphic encryption Jun 2018
  The 2018 KWMS International Conference, Seoul, Republic of Korea.
- Secure logistic regression based on homomorphic encryption Nov 2017
  Guest seminar, Department of Computer Science, UCSD, San Diego, CA, USA
- Homomorphic encryption for arithmetic of approximate Numbers Oct 2017
  iDASH Genomic Data Privacy and Security Protection Competition 2017, Orlando, FL, USA.
- Secure Searching of biomarkers using hybrid GSW encryption scheme Jan 2017
  Women in Mathematics Workshop, Seoul, Republic of Korea.
- Homomorphic encryption and its applications Dec 2016
  Korea Internet Security Agency, Seoul, Republic of Korea.
- Secure searching of biomarkers using Hybrid GSW Encryption Scheme Nov 2016
  iDASH Genomic Data Privacy and Security Protection Workshop 2016, Chicago, IL, USA.
- Guide to applications of homomorphic encryption Feb 2016
  Microsoft Research Seminar, Redmond, WA, USA.
- Private genome analysis through Homomorphic Encryption Apr 2015
  Mathematics of Lattices and Cybersecurity, Providence, RI, USA.
- Private genome analysis through homomorphic encryption Apr 2015
  Microsoft Research Seminar, San Diego, CA, USA.

- Private genome analysis through homomorphic encryption — Mar 2015
  iDASH Genomic Data Privacy and Security Protection Workshop 2015, San Diego, CA, USA.
- Homomorphic computation of Edit distance — Jan 2015
  WAHC'15 : 3rd Financial Cryptography Workshop on Applied Homomorphic Cryptography, San Juan, PR, USA.
- Search-and-compute on encrypted data — Jan 2015
  WAHC'15 : 3rd Financial Cryptography Workshop on Applied Homomorphic Cryptography, San Juan, PR, USA.
- Search-and-compute on encrypted data — Apr 2014
  The 2014 Global KMS International Conference, Gangneung, Republic of Korea.

TEACHING

- Discrete mathematics — Fall 2020

MEDIA MENTIONS

- Awards for Young Korean Female Mathematics — Jul 2018
  Knowledge@yonhapnews,etnews,hankyung,seouldaily,insight,asiatimes,etoday,fomos
- Vanderbilt-, IBM-, Microsoft-Led Teams Named Winners of Recent iDASH Genomic Privacy Competition Dec 2016
  Knowledge@GenomeWeb.
- The 10th Crypto Contest — Nov 2016
  http://www.etnews.com/20161123000272.
- Extreme cryptography paves way to personalized medicine — Mar 2015
  Knowledge@NatureNews.
- Cryptographer's Challenge: Keeping Genetic Secrets While Advancing Genetic Research — Mar 2015
  Knowledge@Microsoft Research.
- Hot Global Mathematicians of Cryptography — Mar 2015
  Knowledge@Donga.
- New Community Challenge Seeks to Evaluate Methods of Computing on Encrypted Genomic Data — Nov 2014
  Knowledge@GenomeWeb.

LANGUAGES

- Korean: Native language
- English: Fluent

SKILLS

- Basic: Matlab, R, Sage
- Intermediate: Python
- Advanced: C/C++

[*Last update on 2020-10-22*]