Miran Kim

7000 Fannin St, Houston, TX, 77030, United States
Miran.Kim@uth.tmc.edu +1 (713) 500-3988

WORK EXPERIENCE

University of Texas, Health Science Center at Houston, United States
- Assistant Professor, School of Biomedical Informatics — May 2018 – Present

University of California, San Diego, CA, United States
- Postdoctoral Researcher, Division of Biomedical Informatics. — Mar 2017 – Apr 2018

Microsoft Research, United States
- Research Intern, Mentor: Dr. Kristin Lauter — Jan 2015 – Apr 2015

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

PUBLICATIONS

REFEREED JOURNAL PUBLICATIONS

[J09] **M. Kim**, J. Lee, L. Ohno-Machado, and X. Jiang: Secure and differentially private logistic regression for horizontally distributed Data. *To appear in IEEE Transactions on Information Forensics and Security*, 2019.

[J08] **M. Kim**, Y. Song, B. Li, and D. Micciancio: Semi-parallel logistic regression for GWAS on encrypted data. *To appear in BMC Medical Genomics*, 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 2019*;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 2018*;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 2018*;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 2017*;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 2016*; 32(2):211-218, 2016.

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

REFEREED CONFERENCE PUBLICATIONS

[C09] **M. Kim**: Homomorphic encryption for protecting genome privacy. In *Proceedings of IEEE EMBS International Conference on Biomedical and Health Informatics-BHI 2019.* 2019.

[C08] X. Jiang, **M. Kim**, K. Lauter, and Y. Song: Secure outsourced matrix computation and application to neural networks. In *Proceedings of the 25th ACM SIGSAC Conference on Computer and Communications Security–CCS 2018.* 2018.

[C07] J. H. Cheon, K. Han, A. Kim, **M. Kim** and Y. Song: A full RNS variant of approximate homomorphic encryption. In *Proceedings of the 24th International Conference on Selected Areas in Cryptography–SAC 2018.* 2018.

[C06] J. H. Cheon, A. Kim, **M. Kim**, and Y. Song: Bootstrapping for approximate homomorphic encryption. In *Proceedings of the 37th Annual International Conference on the Theory and Applications of Cryptographic Techniques–EUROCRYPT 2018*, 2018.

[C05] J. H. Cheon, A. Kim, **M. Kim**, and Y. Song: Homomorphic encryption for arithmetic of approximate numbers. In *Proceedings of the 23rd International Conference on the Theory and Applications of Cryptology and Information Security–ASIACRYPT 2017*, 2017.

[C04] 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 6th IFAC Workshop on Distributed Estimation and Control in Networked Systems–NECSYS 2016*, 2016.

[C03] 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*, 2015.

[C02] J.H. Cheon, **M. Kim**, and M. Kim: Search-and-compute on encrypted data. In *Proceedings of the Financial Cryptography and Data Security–FC 2015*, 2015.

[C01] J.H. Cheon, **M. Kim**, and K. Lauter: Homomorphic computation of edit distance. In *Proceedings of the Financial Cryptography and Data Security–FC 2015*, 2015.

TECHNICAL REPORTS

[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. *Draft Homomorphic Encryption Standard*, available at HomomorphicEncryption.org. 2017.

PATENTS

[P04] *Protection of Cyber-Physical Systems with Homomorphic Encryption*, 1020180092199, 2018.

[P03] *Method for Managing Data and Apparatuses therefor*, US Patent App. US20170004324A1, 2017.

[P02] *Method for Calculating Edit Distance Between DNA Genomic Sequence through Homomorphic Encryption*, 1020160017708, 2016.

[P01] *A Method for Managing Data and Apparatuses therefor*, 1020150094823, 2015.

CONSULTING AND INDUSTRY PROJECTS

- Cancer Phenotyping for personalized combinatorial drug therapy — May 2018 – present
  CPRIT (Cancer Prevention & Research Institute of Texas).
- Decentralized differentially-private methods for dynamic data release and analysis — Sep 2017 – present
  NIH/NIGMS (National Institute of Health, National Institute of General Medical Sciences) (R01GM118609).
- Encryption methods and software for privacy-preserving analysis of biomedical data — Mar 2017 – Apr 2018
  NIH (U01EB023685)
- Development of homomorphic encryption for data analysis — 2015 – 2016
  Samsung.
- Fusion-based next generation privacy/sw security technology — 2014 – 2015
  Samsung.
- A development of public key encryption for the hybrid scheme which combines public key — 2013 – 2014
  Samsung.

PENDING SUPPORT

- *PI* in an NIH R01 grant: "Development of Secure Genotype-Phenotype Association Models with Efficient Correction for Population Stratification" (9/1/2019-8/31/2023)
- *co-PI* in an NIH R43 grant: "Practical Applications for Securely Outsourced Genomic Data Analysis" (9/1/2019-8/31/2020)
- *co-I* in an NIH R21 grant: "Development of Computational Methods for Analysis and Protection of Incidental Genotype Information Leakage from Rna Sequencing Datasets" (9/1/2019-8/31/2021)
- *co-I* in an NIH R01 grant: "Mygenerank: A Digital Platform For Next-Generation Genetic Studies" (4/1/2019-3/31/2024)

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
  http://www.kwms.or.kr/index.php?mp=5_4.
- Nominated at Marquis's Who's Who in the World — 2018
  Marquis's Who's Who.
- 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.

PRESENTATIONS

- Homomorphic Encryption for Protecting Genome Privacy — May 2019
  IEEE EMBS International Conference on Biomedical and Health Informatics 2019, Chicago, IL, 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 Competition 2018, San Diego, CA, USA.
- Progress on Genomic Privacy and Security — Jul 2018
  Seoul National University Bundang Hospital - Big Data Center, Bundang, Republic of Korea.
- Secure Logistic Regression Model Training based on Homomorphic Encryption — Jun 2018
  The 2018 KWMS International Conference, Seoul, Republic of Korea.
- 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 Competition 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 — Mar 2015
  iDASH Genomic Data Privacy and Security Protection Competition 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.

MEDIA MENTIONS

- Awards for Young Korean Female Mathematics — Jul 2018
  Knowledge@yonhapnews,etnews,hankyung,seouldaily,insight,asiatimes,etoday,fomos
- 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 2019-06-15*]