Yongsoo Song

Yongsoo.Song@microsoft.com https://yongsoosong.github.io/
Building 99, One Microsoft Way, Redmond, WA 98052 +1 (858) 249-9390

POSITIONS

Microsoft Research, Redmond, WA, United States

- Senior Researcher, Cryptography Group — Jan 2019 – Present

University of California, San Diego, CA, United States

- Postdoctoral Researcher, Department of Computer Science and Engineering — Jan 2018 – Dec 2018

EDUCATION

Seoul National University, Seoul, Republic of Korea

- M.S. and Ph.D. in Mathematical Sciences — Sep 2012 – Feb 2018
  - Thesis: Homomorphic Encryption for Approximate Arithmetic
  - Advisor: Prof. Jung Hee Cheon
- B.S. in Mathematical Sciences — Mar 2005 – Aug 2012

OVERVIEW

I am a Senior Researcher in the Cryptography and Privacy Research Group at MSR, interested in a broad range of topics in data security and privacy. My research focuses on cryptographic primitives for secure computation and their applications.

- Design and implementation of high-performance Homomorphic Encryption (HE) schemes
- Improving usability and flexibility of modern cryptographic technology
- Applications in machine learning

PUBLICATIONS

CONFERENCES

[C11] H. Chen, W. Dai, M. Kim, and **Y. Song**, "Efficient Multi-Key Homomorphic Encryption with Packed Ciphertexts with Application to Oblivious Neural Network Inference," *The 26th ACM Conference on Computer and Communications Security (CCS 2019)*.

[C10] H. Chen, I. Chillotti and **Y. Song**, "Multi-Key Homomorphic Encryption from TFHE," *the 25th Annual International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT 2019)*.

[C09] H. Chen, I. Chillotti and **Y. Song**, "Improved Bootstrapping for Approximate Homomorphic Encryption," *The 38th Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT 2019)*.

[C08] D. Kim and **Y. Song**, "Approximate Homomorphic Encryption over the Conjugate-invariant Ring," *The 21st Annual International Conference on Information Security and Cryptology (ICISC 2018)*.

[C07] X. Jiang, M. Kim, K. Lauter and **Y. Song**, "Secure Outsourced Matrix Computation and Application to Neural Networks," *The 25th ACM Conference on Computer and Communications Security (CCS 2018)*.

[C06] J. H. Cheon, K. Han, A. Kim, M. Kim and **Y. Song**, "A Full RNS Variant of Approximate Homomorphic Encryption," *The 25th Conference on Selected Areas in Cryptography (SAC 2018)*.

[C05] J. H. Cheon, D. Kim, J. Lee, and **Y. Song**, "Lizard: Cut off the Tail! Practical Post-Quantum Public-Key Encryption from LWE and LWR," *The 11th Conference on Security and Cryptography for Networks (SCN 2018)*.

[C04] J. H. Cheon, K. Han, A. Kim, M. Kim, and **Y. Song**, "Bootstrapping for Approximate Homomorphic Encryption," *The 37th Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT 2018)*.

[C03] J. H. Cheon, A. Kim, M. Kim, and **Y. Song**, "Homomorphic Encryption for Arithmetic of Approximate Numbers," *The 23rd International Conference on the Theory and Applications of Cryptology and Information Security (ASIACRYPT 2017)*.

[C02] 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," *The 6th IFAC Workshop on Distributed Estimation and Control in Networked Systems (NECSYS 2016)*.

[C01] J. H. Cheon, T. Kim, and **Y. Song**, "A Group Action on $\mathbb{Z}_p^\times$ and the Generalized DLP with Auxiliary Inputs," *The 20th International Conference on Selected Areas in Cryptography (SAC 2013)*.

JOURNALS

[J07] M. Kim, **Y. Song**, B. Li, and D. Micciancio, "Semi-parallel logistic regression for GWAS on encrypted data," *BMC Med. Genomics*, 2019.

[J06] J. H. Cheon, D. Kim, Y. Kim and **Y. Song**, "Ensemble Method for Privacy-Preserving Logistic Regression based on Homomorphic Encryption," *IEEE Access 10.1109/ACCESS.2018.2866697*, 2018.

[J05] A. Kim, **Y. Song**, M. Kim, K. Lee, J. H. Cheon, "Logistic Regression Model Training based on the Approximate Homomorphic Encryption," *BMC Med. Genomics*, 2018.

[J04] 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*, 2018.

[J03] J. H. Cheon, K. Han, S. Hong, H. J. Kim, J. Kim, S. Kim, H. Seo, H. Shim, and **Y. Song**, "Toward a Secure Drone System: Flying with Real-time Homomorphic Authenticated Encryption," *IEEE Access DOI 10.1109/ACCESS.2018.2819189*, 2018.

[J02] 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.

[J01] M. Kim, **Y. Song**, and J. H. Cheon, "Secure Searching of Biomarkers Using Hybrid Homomorphic Encryption Scheme," *BMC Med. Genomics. 2017;10:42*, 2017.

BOOK AND BOOK CHAPTERS

[B01] J. H. Cheon, T. Kim, and **Y. Song**, "The Discrete Logarithm Problem with Auxiliary Inputs," In *Algebraic Curves and Finite Fields. Cryptography and Other Applications*, Berlin, Boston: De Gruyter, 2014.

MANUSCRIPTS

[E08] H. Chen, W. Dai, M. Kim and **Y. Song**, "Efficient Homomorphic Conversion Between (Ring) LWE Ciphertexts," 2019 (submitted to PKC 2020).

[E07] H. Chen, M. Kim, I. Razenshteyn, D. Rotaru, **Y. Song** and S. Wagh, "Maliciously Secure Matrix Multiplication with Applications to Private Deep Learning," 2019 (submitted to EUROCRYPT 2020).

[E06] H. Chen, L. Chua, K. Lauter and **Y. Song**, "On the concrete approximation factor of BKZ2.0 on uSVP lattices," 2019 (submitted to EUROCRYPT 2020).

[E05] **Y. Song**, J. Cyranka, D. Kim and S. Gao, "Convergence and Oscillation of Low-Precision Stochastic Gradient Descent," 2019.

[E04] J. H. Cheon, D. Kim, J. Lee, J. Shin, and **Y. Song**, "Instant Privacy-Preserving Biometric Authentication for Hamming Distance Matcher," 2018.

[E03] D. Archer, L. Chen, J. H. Cheon, R. Gilad-Bachrach, R. A. Hallman, Z. Huang, X. Jiang, R. Kumaresan, B. A. Malin, H. Sofia, and **Y. Song**, "Applications of Homomorphic Encryption," *Draft Homomorphic Encryption Standard*, available at HomomorphicEncryption.org (white paper), 2017.

[E02] J. H. Cheon and **Y. Song**, "Batch Fully Homomorphic Encryption over the Integers Revisited," 2016.

[E01] J. H. Cheon and **Y. Song**, "Secure Sketch for Set Distance on Noisy Data," 2014.

PROJECTS / SOFTWARES

[S04] "Microsoft SEAL: The Microsoft Simple Encrypted Arithmetic Library," https://www.microsoft.com/en-us/research/project/microsoft-seal/, 2019.

[S03] "Full RNS Variant of HEAAN," https://github.com/HanKyoohyung/FullRNS-HEAAN, 2018.

[S02] "Bootstrapping of HEAAN," https://github.com/kimandrik/HEAANBOOT, 2018.

[S01] "Implementation of HEAAN," https://github.com/kimandrik/HEAAN, 2016.

PATENTS

[P08] J. H. Cheon, **Y. Song** and K. Han, "Method for Authenticating Evaluation Results of Homomorphic-Encrypted Data," KR20190005540A, 2019.

[P07] J. H. Cheon and **Y. Song**, "Method for Authenticating Biometric Information Which Protects Biometric Information," KR101838008B1 and WO2018199713A1, 2017.

[P06] H. Sim, J. H. Cheon, **Y. Song**, M. Kim, J. Kim, C. Lee, "Method for Processing Dynamic Data by Fully Homomorphic Encryption," KR101919940B1 and WO2018147497A1, 2017.

[P05] J. H. Cheon, **Y. Song** and K. Han, "Terminal device for performing homomorphic encryption, server device for calculating encrypted messages, and methods thereof," KR101965628B1, 2016.

[P04] J. H. Cheon and **Y. Song**, "Homomorphic Encryption Method of a Plurality of Messages Supporting Approximate Arithmetic of Complex Numbers," KR101861089B1, 2016.

[P03] J. H. Cheon and **Y. Song**, "Homomorphic Encryption Method Supporting Floating-Point Arithmetic and Floating-Point Arithmetic Method for Encrypted Message Generated by the Same," KR101971215B1, 2019.

[P02] J. H. Cheon and **Y. Song**, "Homomorphic Encryption Method by Which Ciphertext Size Is Reduced," KR101829267B1, 2018.

[P01] J. H. Cheon, J.W. Kim, E. Kwon, K. Lee, H. Ryu and **Y. Song**, "Fingerprint Enrollment Method and Fingerprint Verification Method," KR20160133991A, 2016.

HONORS & AWARDS

- **First Prize**, iDASH Genomic Data Privacy and Security Protection Competition 2018 — Oct 2018
  http://www.humangenomeprivacy.org/2018/
- **First Prize**, iDASH Genomic Data Privacy and Security Protection Competition 2017 — Oct 2017
  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
  http://www.humangenomeprivacy.org/2016/
- **Best Award**, Crypto Contest — Oct 2016
  Korea Cryptography Forum.
- Excellence Award, Crypto Contest — Oct 2014
  Korea Cryptography Forum.
- Award for Excellence in Teaching — Aug 2014
  Seoul National University.
- **Global PhD Fellowship** ($150,000) — Sep 2012–Aug 2017
  National Foundation Research of Korea.
- BK 21+ Scholarship — Sep 2012–Aug 2017
  Ministry of Education of Korea.
- **Best Award**, Undergraduate Mathematical Olympiad 2006 — Nov 2006
  Korean Mathematical Society.
- Excellence Award, Undergraduate Mathematical Olympiad 2005 — 2005
  Korean Mathematical Society.
- **Silver Medal**, the 45th International Mathematical Olympiad — Jun 2004
  Athens, Greece.

INVITED TALKS

- Construction and Bootstrapping of Approximate Homomorphic Encryption — Nov 2018
  22nd Workshop on Elliptic Curve Cryptography (ECC 2018), Osaka, Japan.
- Homomorphic Matrix Computation and Application to Neural Networks — Jun 2018
  Microsoft Research, Redmond, USA.
- Approximate Homomorphic Encryption: Construction and Application — Mar 2018
  The Second Homomorphic Encryption Standardization Workshop, Cambridge, USA.
- Homomorphic Encryption for Approximate Arithmetic — Dec 2017
  Lattice and Cryptography Meeting, ENS de Lyon, France.
- Homomorphic Encryption for Arithmetic of Approximate Numbers — Jun 2017
  Microsoft Research, Redmond, USA.
- Post-Quantum Public-Key Encryption from LWR — Mar 2017
  Korea Internet and Security Agency, Korea.

CONFERENCE PRESENTATIONS

- Multi Key Homomorphic Encryption from TFHE — Dec 2019
  ASIACRYPT 2019, Kobe, Japan.
- Multi Key Homomorphic Encryption with Packed Ciphertexts — Nov 2019
  CCS 2019, London, UK.
- A Full RNS Variant of Approximate Homomorphic Encryption — Aug 2018
  SAC 2018, University of Calgary, Canada.
- Bootstrapping for Approximate Homomorphic Encryption — May 2018
  EUROCRYPT 2018, Tel Aviv, Israel.
- Homomorphic Encryption for Arithmetic of Approximate Numbers — Dec 2017
  ASIACRYPT 2017, Hong Kong.
- Privacy-Preserving Logistic Regression based on the HEAAN Library — Oct 2017
  iDASH Privacy & Security Workshop 2017, Florida, USA.
- Secure Searching of Biomarkers Using Hybrid GSW Encryption Scheme — Nov 2016
  iDASH Privacy & Security Workshop 2016, Chicago, USA.
- Secure Sketch for Set Distance on Noisy Data — Oct 2014
  2014 KMS Annual Meeting, Yonsei University, Korea.
- A Group Action on $\mathbb{Z}_p^\times$ and the Generalized DLP with Auxiliary Inputs — Aug 2013
  SAC 2013, Simon Fraser University, Canada.

OTHER ACTIVITIES

- Co-chair of Mathcrypt'19
- Program committees of PKC'20, iDASH'19, ICCD'19, iDASH'18

OTHER WORK EXPERIENCE

- Visiting Scholar (Prof. Xiaoqian Jiang) — Jun 2017 – Sep 2017
  Division of Biomedical Informatics, University of California, San Diego, USA.
- Intern (Prof. Damien Stehlé) — Jul 2015 – Aug 2015
  Computer Science Department, ENS de Lyon, France.

LANGUAGES

- Korean: Native language.
- English: Fluent.

[*Last update on 2019-11-21*]