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

PUBLICATIONS

CONFERENCES

[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

[E06] H. Chen, W. Dai, M. Kim, and **Y. Song**, "Multi-key Homomorphic Encryption with Packed Ciphertexts," 2019 (submitted to CCS'19).

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

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

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

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

LANGUAGES	▪ Korean: Native language.
	▪ English: Fluent.

SKILLS	LaTeX, C/C++, Python

[*Last update on 2019-09-09*]