

Yongsoo Song

📍 9500 Gilman Drive #0404, La Jolla, CA 92093-0404, United States
✉ yongsoosong@ucsd.edu ☎ +1 (858) 249-9390

POSITIONS

University of California, San Diego, CA, United States

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

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

JOURNALS

- [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.

CONFERENCES

- [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,” <i>The 6th IFAC Workshop on Distributed Estimation and Control in Networked Systems (NECSYS 2016)</i> .																						
	[C01] J. H. Cheon, T. Kim, and Y. Song , “A Group Action on \mathbb{Z}_p^\times and the Generalized DLP with Auxiliary Inputs,” <i>The 20th International Conference on Selected Areas in Cryptography (SAC 2013)</i> .																						
MANUSCRIPTS	<p>[E05] Y. Song, J. Cyranka, D. Kim and S. Gao, “Convergence Analysis of Gradient Descent with Errors,” 2018.</p> <p>[E04] J. H. Cheon, D. Kim, J. Lee, J. Shin, and Y. Song, “Instant Privacy-Preserving Biometric Authentication for Hamming Distance Matcher,” 2018.</p> <p>[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,” <i>Draft Homomorphic Encryption Standard</i>, available at HomomorphicEncryption.org, 2017.</p> <p>[E02] J. H. Cheon and Y. Song, “Batch Fully Homomorphic Encryption over the Integers Revisited,” 2016.</p> <p>[E01] J. H. Cheon and Y. Song, “Secure Sketch for Set Distance on Noisy Data,” 2014.</p>																						
SOFTWARES	<p>[S02] J. H. Cheon, K. Han, A. Kim, M. Kim and Y. Song, “Bootstrapping of HEAAN,” https://github.com/kimandrik/HEAANBOOT, 2018.</p> <p>[S01] J. H. Cheon, A. Kim, M. Kim and Y. Song, “Implementation of HEAAN,” https://github.com/kimandrik/HEAAN, 2016.</p>																						
PATENTS	<p>[P04] J. H. Cheon and Y. Song, “Homomorphic Encryption Method of a Plurality of Messages Supporting Approximate Arithmetic of Complex Numbers,” 10-2016-0096184 (SNU-2016-0591), 2016.</p> <p>[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,” 10-2016-0075859 (SNU-2016-0413), 2016.</p> <p>[P02] J. H. Cheon and Y. Song, “Homomorphic Encryption Method by Which Ciphertext Size Is Reduced,” 10-2016-0051432 (SNU-2016-0319), 2016.</p> <p>[P01] J. H. Cheon, J.W. Kim, E. Kwon, K. Lee, H. Ryu and Y. Song, “Fingerprint Enrollment Method and Fingerprint Verification Method,” 10-2015-0067318 (SNU-2015-0692), 2015.</p>																						
HONORS & AWARDS	<table> <tr> <td>▪ First Prize, iDASH Genomic Data Privacy and Security Protection Competition 2018 http://www.humangenomeprivacy.org/2018/</td> <td>Oct 2018</td> </tr> <tr> <td>▪ First Prize, iDASH Genomic Data Privacy and Security Protection Competition 2017 http://www.humangenomeprivacy.org/2017/</td> <td>Oct 2017</td> </tr> <tr> <td>▪ Excellence Award, Crypto Contest Korea Cryptography Forum.</td> <td>Oct 2017</td> </tr> <tr> <td>▪ Second Prize, iDASH Genomic Data Privacy and Security Protection Competition 2016 http://www.humangenomeprivacy.org/2016/</td> <td>Nov 2016</td> </tr> <tr> <td>▪ Best Award, Crypto Contest Korea Cryptography Forum.</td> <td>Oct 2016</td> </tr> <tr> <td>▪ Excellence Award, Crypto Contest Korea Cryptography Forum.</td> <td>Oct 2014</td> </tr> <tr> <td>▪ Award for Excellence in Teaching Seoul National University.</td> <td>Aug 2014</td> </tr> <tr> <td>▪ Global PhD Fellowship (\$15,000) National Foundation Research of Korea.</td> <td>Sep 2012–Aug 2017</td> </tr> <tr> <td>▪ BK 21+ Scholarship Ministry of Education of Korea.</td> <td>Sep 2012–Aug 2017</td> </tr> <tr> <td>▪ Best Award, Undergraduate Mathematical Olympiad 2006 Korean Mathematical Society.</td> <td>Nov 2006</td> </tr> <tr> <td>▪ Excellence Award, Undergraduate Mathematical Olympiad 2005</td> <td>2005</td> </tr> </table>	▪ 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 (\$15,000) 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	2005
▪ 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 (\$15,000) 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	2005																						

Korean Mathematical Society.

- **Silver Medal**, the 45th International Mathematical Olympiad
Athens, Greece. Jun 2004

INVITED TALKS

- 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, Massachusetts, USA. Mar 2018
- Homomorphic Encryption for Approximate Arithmetic
Lattice and Cryptography Meeting, ENS de Lyon. 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

CONSULTING AND INDUSTRY PROJECTS

- Analysis of Multilinear Maps and Indistinguishability Obfuscation
DARPA. Jan 2017 – Dec 2017
- Development of Homomorphic Encryption for Data Analysis
Samsung. Jun 2015 – Sep 2017
- Fingerprint Data Protection and Authentication Algorithm
Samsung. Mar 2014 – Feb 2015

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 2018-10-26]