Yongsoo Song

y.song@snu.ac.kr https://yongsoosong.github.io/ Google Scholar
1 Gwanak-ro, Gwanak-gu, Seoul, South Korea (+82) 10-6653-7771

OVERVIEW

I am an Associate Professor in the Department of Computer Science and Engineering at Seoul National University.

My research specializes in Privacy-Enhancing Cryptography (PEC) for secure computation. This includes fully homomorphic encryption, multi-party computation, and zero-knowledge proofs, approached from both theoretical and applied perspectives.

EDUCATION

Seoul National University, Seoul, South Korea

- M.S. and Ph.D. in Mathematical Sciences — Sep 2012 – Feb 2018
  - Thesis: Homomorphic Encryption for Approximate Arithmetic
  - Advisor: Jung Hee Cheon
- B.S. in Mathematical Sciences — Mar 2005 – Aug 2012
  - Fulfilled two years of mandatory military duty in South Korea — Jan 2008 – Dec 2009

WORK EXPERIENCES

Seoul National University, Seoul, South Korea

- Associate Professor — Mar 2025 – Present
- Assistant Professor — Mar 2021 – Feb 2025

Microsoft Research Redmond, WA, United States

- Senior Researcher, Cryptography and Privacy Research Group — Jan 2019 – Feb 2021
- Manager: Kristin Lauter

UC San Diego, CA, United States

- Postdoctoral Researcher, Department of Computer Science and Engineering — Jan 2018 – Dec 2018
- Supervisor: Sicun (Sean) Gao

UC San Diego, CA, United States

- Visiting scholar, Division of Biomedical Informatics — Jun 2017 – Sep 2017
- Supervisor: Xiaoqian Jiang

ENS de Lyon, Lyon, France

- Internship, Computer Science Department — Jul 2015 – Aug 2015
- Supervisor: Damien Stehlé

PUBLICATIONS

CONFERENCES

[C25] "TopGear 2.0: Accelerated Authenticated Matrix Triple Generation with Scalable Prime Fields via Optimized HE Packing"
Hyunho Cha, Intak Hwang, Seonhong Min, Jinyeong Seo, Y. Song
IEEE S&P 2025

[C24] "Enhanced CKKS Bootstrapping with Generalized Polynomial Composites Approximation"
Seonhong Min, Joon-Woo Lee, Y. Song
ACM ASIACCS 2025

[C23] "Simpler and Faster BFV Bootstrapping for Arbitrary Plaintext Modulus from CKKS"
Jaehyung Kim, Jinyeong Seo, Y. Song
ACM CCS 2024

[C22] "Concretely Efficient Lattice-based Polynomial Commitment from Standard Assumptions"
Intak Hwang, Jinyeong Seo, Y. Song
Crypto 2024

[C21] "Towards Practical Multi-key TFHE: Parallelizable, Key-compatible, Quasi-linear Complexity"
Hyesun Kwak, Seonhong Min, Y. Song
PKC 2024

[C20] "A General Framework of Homomorphic Encryption for Multiple Parties with Non-interactive Key-Aggregation"
Hyesun Kwak, Dongwon Lee, Y. Song, Sameer Wagh
ACNS 2024

[C19] "Optimizing HE operations via Level-aware Key-switching Framework"
Intak Hwang, Jinyeong Seo, Y. Song
WAHC 2023

[C18] "Asymptotically Faster Multi-key Homomorphic Encryption from Homomorphic Gadget Decomposition"
Taechan Kim, Hyesun Kwak, Dongwon Lee, Jinyeong Seo, Y. Song
ACM CCS 2023

[C17] "Toward Practical Lattice-based Proof of Knowledge from Hint-MLWE"
Duhyeong Kim, Dongwon Lee, Jinyeong Seo, Y. Song
Crypto 2023

[C16] "Accelerating HE Operations from Key Decomposition Technique"
Miran Kim, Dongwon Lee, Jinyeong Seo, Y. Song
Crypto 2023

[C15] "Faster TFHE Bootstrapping with Block Binary Keys"
Changmin Lee, Seonhong Min, Jinyeong Seo, Y. Song
AsiaCCS 2023

[C14] "Efficient Homomorphic Conversion Between (Ring) LWE Ciphertexts"
Hao Chen, Wei Dai, Miran Kim, Y. Song
ACNS 2021

[C13] "Lattice-Based Secure Biometric Authentication for Hamming Distance"
Jung Hee Cheon, Dongwoo Kim, Duhyeong Kim, Joohee Lee, Junbum Shin, Y. Song
ACISP 2021

[C12] "Maliciously Secure Matrix Multiplication with Applications to Private Deep Learning"
Hao Chen, Miran Kim, Ilya Razenshteyn, Dragos Rotaru, Y. Song, Sameer Wagh
ASIACRYPT 2020

[C11] "Efficient Multi-Key Homomorphic Encryption with Packed Ciphertexts with Application to Oblivious Neural Network Inference"
Hao Chen, Wei Dai, Miran Kim, Y. Song
ACM CCS 2019

[C10] "Multi-Key Homomorphic Encryption from TFHE"
Hao Chen, Ilaria Chillotti, Y. Song
ASIACRYPT 2019

[C9] "Improved Bootstrapping for Approximate Homomorphic Encryption"
Hao Chen, Ilaria Chillotti, Y. Song
EUROCRYPT 2019

[C8] "Approximate Homomorphic Encryption over the Conjugate-invariant Ring"
Duhyeong Kim, Y. Song
ICISC 2018

[C7] "Secure Outsourced Matrix Computation and Application to Neural Networks"
Xiaoqian Jiang, Miran Kim, Kristin Lauter, Y. Song
ACM CCS 2018

[C6] "A Full RNS Variant of Approximate Homomorphic Encryption"
Jung Hee Cheon, Kyoohyung Han, Andrey Kim, Miran Kim, Y. Song
SAC 2018

[C5] "Lizard: Cut off the Tail! Practical Post-Quantum Public-Key Encryption from LWE and LWR"
Jung Hee Cheon, Duhyeong Kim, Joohee Lee, Y. Song
SCN 2018

[C4] "Bootstrapping for Approximate Homomorphic Encryption"
Jung Hee Cheon, Kyoohyung Han, Andrey Kim, Miran Kim, Y. Song
EUROCRYPT 2018

[C3] "Homomorphic Encryption for Arithmetic of Approximate Numbers"
Jung Hee Cheon, Andrey Kim, Miran Kim, Y. Song
ASIACRYPT 2017

[C2] "Encrypting Controller using Fully Homomorphic Encryption for Security of Cyber-Physical Systems"
Junsoo Kim, Chanhwa Lee, Hyungbo Shim, Jung Hee Cheon, Andrey Kim, Miran Kim, Y. Song
NECSYS 2016

[C1] "A Group Action on $\mathbb{Z}_p^\times$ and the Generalized DLP with Auxiliary Inputs"
Jung Hee Cheon, T. Kim, Y. Song
SAC 2013

JOURNALS

[J13] "Harnessing the Potential of Shared Data in a Secure, Inclusive, and Resilient Manner via Multi-key Homomorphic Encryption"
David Ha Eun Kang, Duhyeong Kim, Y. Song, Dongwon Lee, Hyesun Kwak, Brian W. Anthony
Scientific Reports 2024

[J12] "On the Concrete Security of LWE With Small Secret"
Lynn Chua, Hao Chen, Y. Song, Kristin Lauter

La Matematica 2024

[J11] "Comparison of Encrypted Control Approaches and Tutorial on Dynamic Systems Using Learning with Errors-based Homomorphic Encryption"
Junsoo Kim, Dongwoo Kim, Y. Song, Hyungbo Shim, Henrik Sandberg, Karl H Johansson
Annual Reviews in Control 2022

[J10] "Ultra-Fast Homomorphic Encryption Models enable Secure Outsourcing of Genotype Imputation"
Miran Kim, Arif Harmanci, Jean-Philippe Bossuat, Sergiu Carpov, Jung Hee Cheon, Ilaria Chillotti, Wonhee Cho, David Froelicher, Nicolas Gama, Mariya Georgieva, Seungwan Hong, Jean-Pierre Hubaux, Duhyeong Kim, Kristin Lauter, Yiping Ma, Lucila Ohno-Machado, Heidi Sofia, Yongha Son, Y. Song, Juan Troncoso-Pastoriza, Xiaoqian Jiang
Cell Systems 2021

[J9] "Computing Blindfolded on Data Homomorphically Encrypted under Multiple Keys: A Survey"
Asma Aloufi, Peizhao Hu, Y. Song, Kristin Lauter
ACM Computing Surveys 2021

[J8] "Privacy-Oriented Technique for COVID-19 Contact Tracing (PROTECT) Using Homomorphic Encryption: Design and Development Study"
Yongdae An, Seungmyung Lee, Seungwoo Jung, Howard Park, Y. Song, Taehoon Ko
Journal of Medical Internet Research 2021

[J7] "Semi-parallel Logistic Regression for GWAS on Encrypted Data"
Miran Kim, Y. Song, Baiyu Li, Daniele Micciancio
BMC Medical Genomics 2020

[J6] "Ensemble Method for Privacy-Preserving Logistic Regression based on Homomorphic Encryption"
Jung Hee Cheon, Duhyeong Kim, Yongdai Kim, Y. Song
IEEE Access 2018

[J5] "Logistic Regression Model Training based on the Approximate Homomorphic Encryption"
Andrey Kim, Y. Song, Miran Kim, Keewoo Lee, Jung Hee Cheon
BMC Medical Genomics 2018

[J4] "SecureLR: Secure Logistic Regression Model via a Hybrid Cryptographic Protocol"
Yichen Jiang, Jenny Hamer, Chenghong Wang, Xiaoqian Jiang, Miran Kim, Y. Song, Yuhou Xia, Noman Mohammed, Md Nazmus Sadat, Shuang Wang
IEEE/ACM Transactions on Computational Biology and Bioinformatics 2018

[J3] "Toward a Secure Drone System: Flying with Real-time Homomorphic Authenticated Encryption"
Jung Hee Cheon, Kyoohyung Han, Seong-min Hong, Hyoun Jin Kim, Junsoo Kim, Suseong Kim, Hosung Seo, Hyungbo Shim, Y. Song
IEEE Access 2018

[J2] "Secure Logistic Regression Based on Homomorphic Encryption: Design and Evaluation"
Miran Kim, Y. Song, Shuang Wang, Yuhou Xia, Xiaoqian Jiang
JMIR Medical Informatics 2018

[J1] "Secure Searching of Biomarkers Using Hybrid Homomorphic Encryption Scheme"
Miran Kim, Y. Song, Jung Hee Cheon
BMC Medical Genomics 2017

OTHERS

[E2] "Introduction to Homomorphic Encryption and Schemes"
Jung Hee Cheon, Anamaria Costache, Radames Cruz Moreno, Wei Dai, Nicolas Gama, Mariya Georgieva,

Shai Halevi, Miran Kim, Sunwoong Kim, Kim Laine, Yuriy Polyakov, Y. Song
Protecting Privacy through Homomorphic Encryption, Springer, 2022

[E1] "The Discrete Logarithm Problem with Auxiliary Inputs"
Jung Hee Cheon, Taechan Kim, Y. Song
Algebraic Curves and Finite Fields: Cryptography and Other Applications, De Gruyter, 2014

PREPRINTS

[P8] "Provably Secure Approximate Computation Protocols from CKKS"
Intak Hwang, Yisol Hwang, Miran Kim, Dongwon Lee, Y. Song
Cryptology ePrint Archive, Paper 2025/395

[P7] "On the Security and Privacy of CKKS-based Homomorphic Evaluation Protocols"
Intak Hwang, Seonhong Min, Jinyeong Seo, Y. Song
Cryptology ePrint Archive, Paper 2025/382

[P6] "Practical Circuit Privacy/Sanitization for TFHE"
Intak Hwang, Seonhong Min, Y. Song
Cryptology ePrint Archive, Paper 2025/216

[P5] "Ciphertext-Simulatable HE from BFV with Randomized Evaluation"
Intak Hwang, Seonhong Min, Y. Song
Cryptology ePrint Archive, Paper 2025/203

[P4] "Carousel: Fully Homomorphic Encryption from Slot Blind Rotation Technique"
Seonhong Min, Y. Song
Cryptology ePrint Archive, Paper 2024/2032

[P3] "Practical Zero-Knowledge PIOP for Public Key and Ciphertext Generation in (Multi-Group) Homomorphic Encryption"
Intak Hwang, Hyeonbum Lee, Jinyeong Seo, Y. Song
Cryptology ePrint Archive, Paper 2024/1879

[P2] "More Efficient Lattice-based OLE from Circuit-private Linear HE with Polynomial Overhead"
Leo de Castro, Duhyeong Kim, Miran Kim, Keewoo Lee, Seonhong Min, Y. Song
Cryptology ePrint Archive, Paper 2024/1534

[P1] "Functional Bootstrapping for Packed Ciphertexts via Homomorphic LUT Evaluation"
Dongwon Lee, Seonhong Min, Y. Song
Cryptology ePrint Archive, Paper 2024/181

HONORS & AWARDS

Silver Prize, Samsung Humantech Paper Award 2023

Dissertation Award, Korean Mathematical Society 2020

First Prize, iDASH Genomic Data Privacy and Security Protection Competition 2018

First Prize, iDASH Genomic Data Privacy and Security Protection Competition 2017

Best Award, Crypto Contest, Korea Cryptography Forum 2016

Global PhD Fellowship, National Foundation Research of Korea 2012 – 2017
- Tuition and stipend for Ph.D. study ($30K/year, for 5 years)

Best Award, Undergraduate Mathematical Olympiad, Korean Mathematical Society 2006

Silver Medal, the 45th International Mathematical Olympiad (IMO 2004) 2004

PROFESSIONAL ACTIVITIES

Chair: Mathcrypt 2019

Program Committee: Asiacrypt 2025, CANS 2025, PKC 2025, ACNS 2025, USENIX Security 2024, PKC 2024, FHE.org 2024, ACM CCS 2023, PQCrypto 2023, FHE.org 2023, PQCrypto 2022, PKC 2022, PQCrypto 2021, PKC 2020, iDASH 2019, ICCD 2019, iDASH 2018

Member of **ISO/IEC JTC 1/SC 27/WG 2** – Cryptography and security mechanisms

---

Last updated on March 14, 2025