Yongha Son

yongha.son@sungshin.ac.kr
yongyonghaa@gmail.com

Research Interest

- Secure Computation and Its Applications
- Post-Quantum Cryptography, especially Lattice-based Cryptanalysis

Career

2024.03 – Present	**Sungshin Women's University**, Republic of Korea Assistant Professor, Department of Convergence Security Engineering
2020.05 – 2024.02	**Samsung SDS**, Republic of Korea Senior Researcher, Security Algorithm Lab

Educations

2014.03 – 2020.02	**Seoul National University**, Republic of Korea PhD (Unified course) in Mathematical Science. *Advisor*: Prof. Jung Hee Cheon *Thesis*: A Study on ID-based Homomorphic Encryption with Noisy Key
2010.02 – 2014.02	**Seoul National University**, Republic of Korea BSc in Mathematics Education.

Publications

Alphabetical order by last name, unless an asterisk (*) is indicated.

Conference Papers

[C7] Private Set Operations from Circuit-Based PSI
- Jiseung Kim, Hyung Tae Lee and **Y. Son**
- ACM SAC 2026

[C6] Private Computation on Common Fuzzy Records
- Kyoohyung Han, Seongkwang Kim, and **Y. Son**
- Privacy Enhancing Technologies Symposium (PETS) 2025

[C5] Revisiting OKVS-based OPRF and PSI: Cryptanalysis and Better Construction
- Kyoohyung Han, Seongkwang Kim, Byeonghak Lee, and **Y. Son**
- ASIACRYPT 2024

[C4] PSI with computation or Circuit-PSI for Unbalanced Sets from Homomorphic Encryption
- ***Y. Son**, and Jinhyeok Jeong

- ACM AsiaCCS 2023

[C3] Improved Circuit-PSI via Equality Preserving Compression

- Kyoohyung Han, Dukjae Moon, and **Y. Son**
- Selected Areas in Cryptography (SAC) 2022

[C2] Revisiting the Hybrid attack on sparse and ternary secret LWET

- ***Y. Son**, and Jung Hee Cheon
- WAHC@CCS 2019

[C1] A Practical Post-Quantum Public-Key Cryptosystem Based on spLWE

- Jung Hee Cheon, Kyoohyung Han, Jinsu Kim, Chanmin Lee, and **Y. Son**
- ICISC 2016

Journal Papers

[J8] A Private-Identifier System from Scalable Private Set Union

- Sangmin Lee, Jiseung Kim, and **Y. Son**
- IET Information Security, Vol. 2026.

[J7] A Hybrid of Lattice-reduction and Meet-LWE via Near-Collision on Babai's Plane

- Minki Hhan, Jiseung Kim, Changmin Lee, and **Y. Son**
- Design, Codes and Cryptography, Vol. 94

[J6] Practical FHE Parameters Against Lattice Attacks

- Jung Hee Cheon, **Y. Son**, Donggeon Yhee
- Journal of the Korean Mathematical Society, Vol. 59

[J5] Privacy-preserving Breast Cancer Recurrence Prediction based on Homomorphic Encryption and Secure Two-Party Computation

- ***Y. Son**, Kyoohyung Han, Yong Seok Lee, Jonghan Yu, Young-Hyuck Im and Soo-Yong Shin
- PLoS One, Vol. 16

[J4] 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, **Y. Son**, Yongsoo Song, Juan Troncoso-Pastoriza, and Xiaoqian Jiang
- Cell Systems, Vol. 12

[J3] Privacy-preserving Approximate GWAS computation based on Homomorphic Encryption

- Duhyeong Kim, ***Y. Son**, Dongwoo Kim, Andrey Kim, Seungwan Hong, and Jung Hee Cheon
- BMC Medical Genomics, Vol. 13

[J2] A Hybrid of Dual and Meet-in-the-Middle Attack on Sparse and Ternary Secret LWE

- Jung Hee Cheon, Minki Hhan, Seungwan Hong, and **Y. Son**
- IEEE Access, Vol. 7

[J1] Faster Linear Transformations in HElib, Revisited

- Jung Hee Cheon, Hyeongmin Choe, Donghwan Lee, and **Y. Son**
- IEEE Access, Vol. 7

Awards

2022.11	Third Place, iDASH Secure Genome Analysis Competition 2022 Track IV: Secure Record Linkage
2022.10	**Gold Medal**, Samsung Best Paper Award 2022 HE-based Circuit-PSI for Unbalanced Inputs
2021.11	Second Place, iDASH Secure Genome Analysis Competition 2021 Track II: Homomorphic Encryption-based Secure Viral Strain Classification
2020.11	**First Place**, iDASH Secure Genome Analysis Competition 2020 Track I: Secure Multi-label Tumor Classification using Homomorphic Encryption
2019.10	Second Place, iDASH Secure Genome Analysis Competition 2019 Track II: Secure Genotype Imputation using Homomorphic Encryption
2018.11	Excellence Award, Korea Cryptography Forum A Hybrid of Dual and Meet-in-the-Middle Attack on Sparse and Ternary Secret LWE
2016.11	Excellence Award, Korea Cryptography Forum A Practical Post-Quantum Public-Key Cryptosystem Based on spLWE