# Yongdong Yeo

🌐 https://yongdongyeo.github.io | ✉ yongdong@snu.ac.kr | 📱 +82 10-4114-9921

## Summary

I am a Ph.D. student advised by **Prof. Jung Hee Cheon** at the Department of Mathematical Science, Seoul National University. My research area includes various topics of **Homomorphic Encryption**, including its applications and related protocols.

## Education

| | | |
|---|---|---|
| 2022 - present | Research Area: Homomorphic Encryption and Cryptography | |
| 2019 - present | Ph.D. student at **Department of Mathematical Science**,<br>**Seoul National University** | (GPA: 3.57/4.3) |
| 2014 - 2019 | B.S. at **Department of Mathematics, Konkuk University** | |

## Publications

### Conference & Journal

[1] Keewoo Lee and Yongdong Yeo. *SophOMR: Improved Oblivious Message Retrieval from SIMD-Aware Homomorphic Compression*. Cryptology ePrint Archive, Paper 2024/1814. To appear in USENIX Security. 2026. URL: https://eprint.iacr.org/2024/1814.

[2] Jung Hee Cheon, Minsik Kang, Taeseong Kim, Junyoung Jung, and Yongdong Yeo. "Batch Inference on Deep Convolutional Neural Networks With Fully Homomorphic Encryption Using Channel-By-Channel Convolutions". In: *IEEE Transactions on Dependable and Secure Computing* 22.2 (2025), pp. 1674–1685. DOI: 10.1109/TDSC.2024.3448406.

[3] Jihwan Kim, Jung Hee Cheon, and Yongdong Yeo. "OverModRaise: Reducing Modulus Consumption of CKKS Bootstrapping". In: *IACR Communications in Cryptology* 2.3 (Oct. 6, 2025). ISSN: 3006-5496. DOI: 10.62056/a3n5qjp10.

### Preprints

[1] Jung Hee Cheon, Hyeongmin Choe, Seunghong Kim, and Yongdong Yeo. *Multi-Party Homomorphic Encryption with Dynamicity and Ciphertext Reusability*. Cryptology ePrint Archive, Paper 2025/581. 2025. URL: https://eprint.iacr.org/2025/581.

[2] Jung Hee Cheon, Keewoo Lee, Jai Hyun Park, and Yongdong Yeo. *SIMD-Aware Homomorphic Compression and Application to Private Database Query*. 2024. arXiv: 2408.17063 [cs.CR]. URL: https://arxiv.org/abs/2408.17063.

## Honors & Awards

### (Korea) National Cryptography Contest

| | | |
|---|---|---|
| 2025, | Encouragement Award, $1500 | SophOMR: Improved Oblivious Message Retrieval from SIMD-Aware Homomorphic Compression |
| 2024, | Encouragement Award, $1500 | Reusable Dynamic Multi-Party Homomorphic Encryption |
| 2024, | Special Award, $500 | OverModRaise: Reducing Modulus Consumption of CKKS Bootstrapping |
| 2023, | Special Award, $500 | Private Database Queries with SIMD-Aware Homomorphic Compression |
| 2023, | Special Award, $500 | Batch Inference on Deep Convolutional Neural Networks with Fully Homomorphic Encryption Using Channel-By-Channel Convolutions |

## Invited Talks & Presentations

| | | |
|---|---|---|
| 2025 spring, | KMS Spring Meeting: | SophOMR: Improved oblivious message retrieval from SIMD-aware homomorphic compression |
| 2024 fall, | KMS Annual Meeting: | Reusable Dynamic Multi-Party Homomorphic Encryption |
| 2024 Aug., | MPC & SNARK Workshop: | SophOMR: Improved oblivious message retrieval from SIMD-aware homomorphic compression |
| 2023 Dec., | Dept. of Math at Konkuk University | Homomorphic Encryption and Its Application to Machine Learning |
| 2023 fall, | KMS Annual Meeting: | Private database query with SIMD-aware homomorphic compression |

## Teaching

To be Updated.

## Languages

| | |
|---|---|
| Korean | Native language. Fluent. |
| English | 2nd language. Proficient. |
| Japanese | 3rd language. Conversational. |
| Programming language: | C++, Go, Python, MatLab. Experience with AI-assisted tools. |

Last updated: February 4, 2026