

Jeongeun PARK

PERSONAL DATA

ADDRESS: A271 ElektroA Gløshaugen, Trondheim, Norway
EMAIL: jungeun7430@gmail.com or jeongeun.park@ntnu.no
PROFILE LINK: [Google Scholar](#), ORCID: 0000-0002-0557-3540

BIOGRAPHY

APR 2024 - PRESENT Associate professor, NTNU, Norway
APR 2021 - MAR 2024 Postdoctoral researcher in COSIC, KU Leuven, Belgium
MAR 2015-FEB 2021 Combined master-doctoral course in Mathematics with a specialization in Cryptography, Ewha Womans University, SEOUL, Republic Of Korea
Advisor: Prof. Hyang-Sook Lee
MAR 2010-FEB 2015 Bachelor of Science in MATHEMATICS
Ewha Womans University, SEOUL, Republic Of Korea

RESEARCH INTERESTS

Lattice based cryptography, Homomorphic encryption, Privacy preserving protocols.

RESEARCH EXPERIENCES

OCT 2018-MAR 2019 Internship Program at NTT Secure Platform Laboratories
TOKYO, Japan
Advisor: Mehdi Tibouchi

PUBLICATIONS

1. *FINALLY: A Multi-Key FHE Scheme Based on NTRU and LWE*, IACR Communications in Cryptology, Volume 1, Issue 3, 2024
 - joint work with Barry Van Leeuwen and Oliver Zajonc
2. *Faster Private Decision Tree Evaluation for Batched Input from Homomorphic Encryption*, SCN 2024
 - joint work with Kelong Cong, Jiayi Kang, and Georgio Nicolas
3. *NTRU-based FHE for Larger Key and Message Space*, ACISP 2024
 - joint work with Robin Jadoul, Axel Mertens, and Hilder V. L. Pereira
4. *Panacea: Non-interactive and Stateless Oblivious RAM*, Euro S&P 2024
 - joint work with Kelong Cong, Debajyoti Das, Georgio Nicolas.
5. *Revisiting Oblivious Top-k Selection with Applications to Secure k-NN Classification*, SAC 2024.
 - joint work with Kelong Cong, Robin Geelen, and Jiayi Kang
6. *Towards Practical Transciphering for FHE with Setup Independent of the Plaintext Space*, IACR Communications in Cryptology, Volume 1, Issue 1 (2024).
 - joint work with Pierrick Méaux and Hilder V. L. Pereira

7. *Efficient TFHE Bootstrapping in the Multiparty Setting*, IEEE Access, Vol. 11, pp. 118625 - 118638, 2023
 - joint work with Sergi Rovira
8. *Practical Randomized Lattice Gadget Decomposition With Application to FHE*, ESORICS 2023
 - joint work with Sohyun Jeon, Hyang-Sook Lee
9. *FINAL: Faster FHE instantiated with NTRU and LWE*, ASIACRYPT 2022
 - joint work with Charlotte Bonte, Ilia Iliashenko, Hilder V. L. Pereira, and Nigel P. Smart
10. *On Pairwise Gaussian bases and LLL algorithm for three dimensional lattices*, Journal of Korean Mathematical Society, Vol. 59, pp. 1047-1065 (2022), Nov 2022
 - joint work with Kitae Kim, Hyang-Sook Lee, Seongan Lim, and Ikkwon Yie
11. *SortingHat: Efficient Private Decision Tree Evaluation via Homomorphic Encryption and Transciphering*, ACM CCS 2022
 - joint work with Kelong Cong, Debajyoti Das, and Hilder V. L. Pereira
12. *Homomorphic Encryption for Multiple Users with Less Communications*, IEEE Access Vol. 9, pp. 135915-135926 (2021), Oct 2021
 - A single-authored paper
13. *Efficient Lattice Gadget Decomposition Algorithm with Bounded Uniform Distribution*, IEEE Access, Vol. 9, pp. 17429 - 17437 (2021)
 - joint work with Sohyun Jeon and Hyang-Sook Lee
14. *SHECS-PIR: Somewhat Homomorphic Encryption-based Compact and Scalable Private Information Retrieval*, ESORICS 2020
 - joint work with Mehdi Tibouchi
15. *Towards Round-Optimal Secure Multiparty Computations: Multikey FHE without a CRS*, International Journal of Foundations of Computer Science, Vol. 31, No. 02, pp. 157 - 174 (2020)
 - joint work with Eunkyung Kim and Hyang-Sook Lee
16. *On the Security of Multikey Homomorphic Encryption*, IMACC 2019
 - joint work with Hyang-Sook Lee
17. *Towards Round-Optimal Secure Multiparty Computations: Multikey FHE without a CRS*, ACISP 2018
 - joint work with Eunkyung Kim and Hyang-Sook Lee

PREPRINTS

COMMUNITY INVOLVEMENT

1. PC member of [PETs 2025](#), [Euro S&P 2025](#)
2. PC member of [ISC 2024](#)
3. PC member of [WAHC 2023](#)
4. PC chair of [CFAIL 2023](#)
5. PC member of [FHE.org conference 2023](#)

6. a reviewer for [Mathematical Reviews](#)
7. Reviewed papers of Journal of Cryptology, Asiacrypt, ACNS, SCN in 2022
8. Reviewed papers of Asiacrypt, Eurocrypt, ESORICS in 2021

HONORS AND AWARDS

2017	Special Award, Crypto Contest, Korea Cryptography Forum
2015-2018	Research Assistant in the Project from the National Research Foundation of Korea (NRF) funded by the Ministry of Science ICT and Future Planning,
2015-2016, 2018, 2020	Brain Korea 21 Plus (BK21 Plus) Scholarship
2018-2021. FEB	Research Assistant in the Project from the National Research Foundation of Korea (NRF) funded by the Korea Government(MSIT).

INVITED TALKS/LECTURES

2022 NOV	Invited talk about FHE based on NTRU: challenges and solutions in Chung-Ang University, Korea
2022 DEC	Invited talk about Homomorphic encryption and its applications to a privacy preserving machine learning algorithm in Chung-Ang University, Korea
2022 DEC	Invited talk about Homomorphic encryption and its applications to a privacy preserving machine learning algorithm in Ewha Womans University, Korea
2023 MAR	Invited lecture on Applications of FHE in The 3rd ISC Winter School on Cryptography.
2023 JUNE	Invited talk about Pancea: Non-interactive and Stateless Oblivious RAM, Inria Rennes.
2023 JUNE	Invited talk about FHE and its applications, Joint workshop by Nokia Bell Labs + DistriNet + COSIC.
2023 JULY	Invited talk, EWHA-KMS International Workshop on Cryptography.

PRESENTATIONS

- 1 (Poster) Necessary and sufficient condition for shortest vectors in lattices of low dimension
-2017 Joint Mathematics Meetings (JMM), in Atlanta, Georgia, January 4-7.
- 2 A necessary and sufficient condition for shortest vectors in lattices of dimension 2, 3
-2017 Korean Mathematical Society (KMS) Spring Meeting, Gwangju, Republic of Korea, April 27-29.
- 3 A three round multiparty computation using MFHE without CRS
-2018 Korean Mathematical Society (KMS) Spring Meeting, Seoul, Republic of Korea, April 21-23.
- 4 Towards Round-Optimal Secure Multiparty Computations: Multikey FHE without a CRS
-2018 ACISP, Wollongong, NSW, Australia, July 11-13.
- 5 Multi key fully homomorphic encryption without CRS and its application.
- 2019 Tokyo University, TAKAGI and TAKENAKA Group, Tokyo, Japan, November 22.
- 6 SHECS-PIR: Somewhat Homomorphic Encryption-based Compact and Scalable Private Information Retrieval
- 2019 NTT secure platform laboratories, Tokyo, Japan, March 14.
- 7 SHECS-PIR: Somewhat Homomorphic Encryption-based Compact and Scalable Private Information Retrieval
- 2019 Korean Mathematical Society (KMS), Chuncheon, Republic of Korea, April 19-20.
- 8 Round optimal MPC from multikey fully homomorphic encryption schemes
-2019 Korean Women in Mathematical Society (KWMS), Seoul, Republic of Korea, August 22-23.

- 9 On the Security of Multikey Homomorphic Encryption
- 2019 IMACC, Oxford, UK, December 16-18
- 10 On the Security of Multikey Homomorphic Encryption
- 2020 Korean Mathematical Society (KMS) Spring Meeting, Virtual Meeting, Republic of Korea, July 3.
- 11 SHECS-PIR: Somewhat Homomorphic Encryption-based Compact and Scalable Private Information Retrieval
- 2020 ESORICS, Virtual Meeting, September 14-16.
- 12 SHECS-PIR: Somewhat Homomorphic Encryption-based Compact and Scalable Private Information Retrieval
- 2020 Ewha Womans University-Japan Women's University-Ochanomizu University Joint Symposium, Virtual Meeting, December 11.
- 13 Homomorphic Encryption for Multiple Users with Less Communications - 2021 EU-Korea Conference on Science and Technology (EKC), Hybrid Meeting, October 24.
- 14 (poster) Efficient privacy preserving tools based on homomorphic encryption, - 2022 FHE.org workshop, Trondheim, Norway, May 29.
- 15 SortingHat: Efficient Private Decision Tree Evaluation via Homomorphic Encryption and Transciphering, ACM CCS 2022, Los Angeles, USA, Nov 9.
- 16 (poster) Efficient TFHE Bootstrapping in the Multiparty Setting, - 2023 FHE.org workshop, Tokyo, Japan, March 26.
- 17 (poster) Panacea: Non-interactive and Stateless Oblivious RAM,
- 2023 FHE.org workshop, Tokyo, Japan, March 26.