Joohee Lee

Curriculum Vitae

Positions

2022.3 – Present **Assistant Professor in Department of Convergence Security Engineering**, *Sungshin Women's University*, Seoul, Republic of Korea.

2019.8 – 2022.2 **Senior Engineer in Security Algorithm Lab**, *Samsung SDS*, Seoul, Republic of Korea.

Education

2013.3 – 2019.8 **PhD in Department of Mathematical Sciences**, *Seoul National University*, Seoul, Republic of Korea.
- *Thesis:* "Public-Key Encryption and Functional Encryption from LWR"
- *Advisor:* Jung Hee Cheon

2008.3 – 2013.2 **BSc in Department of Mathematics Education**, *Korea University*, Seoul, Republic of Korea.

Experiences

2023.6 Submitted a proposal "AIMer" to the NIST Post-Quantum Cryptography Standardization Project (Call for Additional Digital Signature Schemes).

2017.11 Submitted a proposal "Lizard" to NIST Post-Quantum Cryptography Standardization Project (Round 1 candidate).

2017.1 – 2017.4 Visiting Scholar in the University of California, Irvine (UCI).
- *Hosted by:* Prof. Stanislaw Jarecki

2016.7 – 2016.8 Visiting Scholar in the University of California, Irvine (UCI).
- *Hosted by:* Prof. Stanislaw Jarecki

2015.9 – 2016.2 Intern (Crypto Expert Training) in National Security Research Institute, Republic of Korea.

2015.7 – 2015.8 Intern in Electronics and Telecommunications Research Institute, Republic of Korea.

2015.3 – 2019.8 Teaching Assistant in Calculus at Seoul National University, Republic of Korea.

010-7177-6360 • *jooheelee@sungshin.ac.kr*

Publications

Authors are listed in alphabetical order by last name unless it is indicated with diamond (◇). Corresponding authors are indicated with stars (*).

◇ Joohee Lee, Jihoon Kwon, Ji Sun Shin*: Efficient Continuous Key Agreement with Reduced Bandwidth from a Decomposable KEM. *in IEEE Access, 2023*.

◇ Seongkwang Kim, Jincheol Ha, Mincheol Son, Byeonghak Lee, Dukjae Moon, Joohee Lee, Sangyub Lee, Jihoon Kwon, Jihoon Cho, Hyojin Yoon, and Jooyoung Lee*: AIM: Symmetric Primitive for Shorter Signatures with Stronger Security. *To appear in ACM CCS 2023*.

◇ Saerom Park, Junyoung Byun, and Joohee Lee*: Privacy-Preserving Fair Learning of Support Vector Machine with Homomorphic Encryption. *in The Web4Good Special Track at The ACM Web Conference 2022 (WWW 2022)*.

◇ Jaeseung Han, Taeho Lee, Jihoon Kwon, Joohee Lee, Il-Ju Kim, Jihoon Cho, Dong-Guk Han, and Bo-Yeon Sim*: Single-Trace Attack on NIST Round 3 Candidate Dilithium Using Machine Learning-Based Profiling. *in IEEE Access, 2021*

- Jihoon Cho, Jincheol Ha, Seongkwang Kim*, Joohee Lee, Jooyoung Lee*, Dukjae Moon, and Hyojin Yoon: Transciphering Framework for Approximate Homomorphic Encryption. *in the 27th Annual International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT 2021)*.

- Jung Hee Cheon, Dongwoo Kim*, Duhyeong Kim, Joohee Lee*, Junbum Shin, and Yongsoo Song: Lattice-based Secure Biometric Authentication for Hamming Distance. *in the 26th Australasian Conference on Information Security and Privacy (ACISP 2021)*.

◇ Bo-Yeon Sim, Jihoon Kwon, Joohee Lee, Il-Ju Kim, Taeho Lee, Jaeseung Han, Hyojin Yoon, Jihoon Cho, and Dong-Guk Han*: Single-Trace Attacks on Message Encoding in Lattice-Based KEMs. *in IEEE Access, 2020*.

◇ Saerom Park, Junyoung Byun, Joohee Lee, Jung Hee Cheon, and Jaewook Lee*: HE-friendly algorithm for privacy-preserving SVM training. *in IEEE Access, 2020*.

- Jung Hee Cheon, Haejin Cho, Jaewook Jung, Joohee Lee*, and Keewoo Lee: Efficient Identity-Based Encryption from LWR. *in Annual International Conference on Information Security and Cryptology (ICISC) 2019*.

◇ Joohee Lee, Duhyeong Kim, Hyungkyu Lee, Younho Lee*, and Jung Hee Cheon*: RLizard: Post-quantum Key Encapsulation Mechanism for IoT devices. *in IEEE Access, 2018*.

◇ Saerom Park*, Jaewook Lee*, Jung Hee Cheon, Joohee Lee, Jaeyun Kim, and Junyoung Byun: Security-preserving Support Vector Machine with Fully Homomorphic Encryption. *in SafeAI@AAAI 2019*.

- Jung Hee Cheon, Duhyeong Kim, Joohee Lee*, and Yongsoo Song: Lizard: Cut Off the Tail! A Practical Post-quantum Public-Key Encryption from LWE and LWR. *in Conference on Security and Cryptography for Networks (SCN) 2018*.

- Jung Yeon Hwang, Stanislaw Jarecki, Taekyoung Kwon, Joohee Lee*, Ji Sun Shin, and Jiayu Xu: Round-Reduced Modular Construction of Asymmetric Password-Authenticated Key Exchange, *in Conference on Security and Cryptography for Networks (SCN) 2018*.

- Jung Hee Cheon, Jinhyuck Jeong, Joohee Lee, and Keewoo Lee*: Privacy-Preserving Computations of Predictive Medical Models with Minimax Approximation and Non-Adjacent Form, *in Financial Cryptography (FC) Workshops 2017*.
- Jung Hee Cheon, Hyunsook Hong, Joohee Lee*, and Jooyoung Lee: An Efficient Affine Equivalence Algorithm for Multiple S-Boxes and a Structured Affine Layer, *in Selected Areas in Cryptography (SAC) 2016*.

Patents

- Joohee Lee, Eunkyung Kim and Kyu Young Choi. "METHOD AND APPARATUS FOR MANAGING LWE INSTANCE"
  - Applied in United States, October 25, 2022 (17973013)
  - Applied in Republic of Korea, October 27, 2021 (KR1020210144640)
- Jihoon Kwon, Joohee Lee, Jihoon Cho, Jaeseung Han, Taeho Lee and Dong-Guk Han. "Apparatus and Method for Ciphertext Comparison Capable of Preventing Side Channel Attack"
  - Applied in Republic of Korea, October 28, 2021 (KR1020210145850)
- Joohee Lee, Dukjae Moon, Hyojin Yoon, Jihoon Cho, Seongkwang Kim, Jincheol Ha and Jooyoung Lee. "Method and Apparatus for Generating Key Stream"
  - Applied in Republic of Korea, April 23, 2021 (KR1020210052987)
- Jihoon Kwon, Joohee Lee, Hyojin Yoon, Jihoon Cho, Dong-Guk Han, Bo-Yeon Sim, Il-Ju Kim, Taeho Lee and Jaeseung Han. "Apparatus and Method for Preventing Side Channel Attack for NTRU LPRime Algorithm"
  - Applied in United States, October 27, 2020 (17081810)
- Joohee Lee, Dukjae Moon, Hyojin Yoon, Jihoon Cho, Eunkyung Kim, Seongkwang Kim, Jooyoung Lee, Jincheol Ha and Wonseok Choi. "Apparatus and Method for Encryption, Apparatus and Method for Converting Ciphertext";
  - Applied in United States, October 27, 2020 (17081862)
  - Applied in Republic of Korea, October 21, 2020 (KR1020200137067)
- Jinhyuck Jeong, Joohee Lee, Eunkyung Kim, Kyuyoung Choi, Dukjae Moon and Hyojin Yoon. "Apparatus and Method for Set Intersection Operation";
  - Applied in Europe, October 30, 2020 (20204811.2)
  - Applied in United States, October 26, 2020 (17079982)
  - Applied in Republic of Korea, December 24, 2019 (KR1020190174543)
- Joohee Lee, Jung Hee Cheon, Duhyeong Kim and Aaram Yun. "Method for Key Generation, Encryption and Decryption for Public Key Encryption Scheme Based on Module-Wavy and Module-LWR";
  - Applied in United States, June 18, 2020 (16904806)
  - Issued in Republic of Korea, September 25, 2019 (KR1020275080000)
  - Applied in Republic of Korea, December 29, 2017 (KR1020170183661)
- Jung Hee Cheon and Joohee Lee. "Calculating Apparatus for Encrypting Message by Public Key and Method Thereof";
  - Issued in Republic of Korea October 1, 2018 (KR1019056890000)
  - Applied in Republic of Korea November 18, 2016 (KR1020160154160)

Talks

2021 ACISP 2021, Virtual event, "Lattice-based Secure Biometric Authentication for Hamming Distance."

2019 ICISC 2019 in Seoul, Republic of Korea, "Efficient Identity-Based Encryption from LWR."

2018 SCN 2018 in Amalfi, Italy, "Round-Reduced Modular Construction of Asymmetric Password-Authenticated Key Exchange."

2018 NIST's First PQC Standardization Conference (2018) in Florida, United States, "Lizard."

2016 SAC 2016 in St. Johns, Canada, "An Efficient Affine Equivalence Algorithm for Multiple S-Boxes and a Structured Affine Layer."

2016 KMS 2016 Annual Meeting in Suwon, Republic of Korea, "A Survey of Asymmetric Password-based Authenticated Key Exchange."

Awards

2021 The Encouragement Awards, Crypto Contest, Korea Cryptography Forum, Republic of Korea; "Transciphering Framework for Approximate Homomorphic Encryption."

2017 The Encouragement Awards, Crypto Contest, Korea Cryptography Forum, Republic of Korea;

- "Lizard: Cut Off the Tail! A Practical Post-quantum Public-Key Encryption from LWE and LWR",
- "Privacy-Preserving K-means Clustering with Multiple Data Owners."

2016 The Excellence Award, Crypto Contest, Korea Cryptography Forum, Republic of Korea; "Privacy-Preserving Computations of Predictive Medical Models with Minimax Approximation and Non-Adjacent Form."

2015 The Excellence Award for Teaching Assistant, Seoul National University, Republic of Korea.