DongWon Lee

[+82 10 –7751-3203] [dongwonlee95@gmail.com]
[Github: github.com/Lee-DongWon]

EDUCATION

- B.S in Mathematics and Software (Double Major), Sungkyunkwan University, South Korea [2014.2 ~ 2021.2]
  - **GPA:** 4.39 / 4.5
  - **Honors:** Samsung Science Talent Scholarship.
- Ph.D in Computer Sciences, Seoul National University, South Korea [2021.9 ~ Present]

Overview

I am a Ph.D. student in the Department of Computer Science and Engineering at Seoul National University. My advisor is Yongsoo Song and my research interests are in cryptography, privacy and security. Before studying in Seoul National University, I studied and obtained Bachelor's degree in Sungkyunkwan University, from 2014. During the course, my major was mathematics and computer science. I worked as an undergraduate research student with Hyoungshick Kim, from 2019 to 2020. I also did an internship in CSIRO Data 61, from September to December 2019. In these days, I'm especially interested in homomorphic encryption, zero-knowledge proof and multi-party computation.

- Improve the performance of Homomorphic Encryption (HE) schemes.
- Design a modern cryptographic technology with high usability and flexibility of and use it to enhance the efficiency.
- Applying cryptographic primitives to various applications such as machine learning.

PAPERS

<Conferences>

- Accelerating HE Operations from Key Decomposition Technique
  - Miran Kim, Dongwon Lee, Jinyeong Seo, Yongsoo Song
  - CRYPTO 2023 (https://eprint.iacr.org/2023/413.pdf)
- Toward Practical Lattice-based Proof of Knowledge from Hint-MLWE
  - Duhyeong Kim, Dongwon Lee, Jinyeong Seo, Yongsoo Song
  - CRYPTO 2023 (https://eprint.iacr.org/2023/623.pdf)
- Asymptotically Faster Multi-Key Homomorphic Encryption from Homomorphic Gadget Decomposition
  - Taechan Kim, Hyesun Kwak, Dongwon Lee, Jinyeong Seo, Yongsoo Song
  - CCS 2023 (https://eprint.iacr.org/2022/347.pdf)
- A General Framework of Homomorphic Encryption for Multiple Parties with Non-Interactive Key-Aggregation
  - Dongwon Lee, Hyesun Kwak, Yongsoo Song, Sameer Wagh
  - ACNS 2024 (https://eprint.iacr.org/2021/1412.pdf)
- BlindFilter: Privacy-Preserving Spam Email Detection Using Homomorphic Encryption
  - Dongwon Lee, Myeonghwan Ahn, Hyesun Kwak, Jin B. Hong, Hyoungshick Kim
  - SRDS 2023 (https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=10419317)
- Functional Bootstrapping for FV-style cryptosystems
  - Dongwon Lee, Seonhong Min, Yongsoo Song
  - Submitted (https://eprint.iacr.org/2024/181.pdf)

<Journals>

- PP-GSM: Privacy-Preserving Graphical Security Model for Security Assessment as a Service
  - Dongwon Lee, Yongwoo Oh, Jin B. Hong, Hyoungshick Kim
  - FGCS 2022 (https://doi.org/10.1016/j.future.2022.12.041)

- Share to Gain: Collaborative Learning with Dynamic Membership via Multi-Key Homomorphic Encryption
  - David Ha Eun Kang, Duhyeong Kim, Yongsoo Song, Dongwon Lee, Hyesun Kwak, Brian Anthony
  - Submitted (https://assets.researchsquare.com/files/rs-3552389/v1_covered_6cdaf277-d43d-4d21-855a-409cc3ed8d1f.pdf?c=1700109058)

PRESENTATIONS

- Asymptotically Faster Multi-Key Homomorphic Encryption from Homomorphic Gadget Decomposition
  - 2022 Global KMS (Korean Math. Soc.) International Conference.
  - 2023 ACM SIGSAC Conference on Computer and Communications Security (ACM CCS)

- A Unified Framework of Homomorphic Encryption for Multiple Parties with Non-Interactive Setup
  - 2024 International Conference on Applied Cryptography and Network Security (ACNS)

AWARDS & WORK EXPERIENCE

<Awards>

- Samsung Humantech Paper Award
  - Silver Prize in Computer Science & Engineering: “Accelerating HE Operations from Key Decomposition Technique” [2023]

- National Cryptography Contest
  - Best Award (3,000$): “Asymptotically Faster Multi-Key Homomorphic Encryption from Homomorphic Gadget Decomposition” [2022]
  - Special Prize (1,000$): “A Unified Framework of Homomorphic Encryption for Multiple Parties with Non-Interactive Setup” [2021]

- National College Student Mathematics Contest
  - Silver Prize. (Top 15% or 10% by region.) [2015]
  - Bronze Prize. (Top 25% or 20% by region.) [2017]

<Work Experience>

- Work as an undergraduate student in laboratory of professor Hyoungshik Kim, Sungkyunkwan University. [2019.1 ~ 2020.12]
  - Research about privacy-preserving (Naïve Bayesian) spam filtering model using homomorphic encryption.

- Internship program in CSIRO Data 61, Australia [2019.9 ~ 2019.12]
  - Research about privacy-preserving graphical security model using homomorphic encryption.
  - Research on randomness of password in several applications.

- Internship program in CryptoLab, Seoul National University. [2020.1 ~ 2020.2]
  - Study about details of homomorphic encryption scheme, especially CKKS scheme (HEaaN).
  - Implement web service using Django and other frameworks.

SKILLS & INTERESTS

Programming: C++(Intermediate), Python (Intermediate), GO(Intermediate), Java(Basic).

Language skill: Korean(native), English (Fluent)

Interests: Climbing, soccer, playing ‘Baduk (Go game)’.