Heewon Chung

Personal Data

Nationality:	Republic of Korea
Phone:	+82-10-8496-2841
email:	tyler.heewonchung@gmail.com

Education

Sep, 2013 - Aug, 2017	**Doctor of Philosophy** in *Mathematics*, Seoul National University Thesis: "Secure Computation via Homomorphic Encryption" Academic Advisor: Prof. Jung Hee Cheon
Sep, 2010 - Aug, 2013	**Master of Science** in *Mathematics*, Seoul National University Thesis: "Efficient Inversion Algorithms and Its Applications to ECDLP" Academic Advisor: Prof. Jung Hee Cheon
Mar, 2005 - Aug, 2010	**Bachelor of Science** in *Mathematics*, Korea Advanced Institute of Science and Technology (KAIST) Academic Advisor: Prof. Sang Geun Hahn

Careers

Jeonbuk National University

Mar, 2025 -	**Assistant Professor**, Department of Software Engineering

DESILO Inc.

Jan, 2022 - Feb, 2025	**Cryptography Researcher**, Research Team

Hanyang Univeristy

Apr, 2020 - Nov, 2021	**Postdoctoral Researcher**, Department of Mathematics Supervisior: Prof. Jae Hong Seo

MEDIUM

Jan. 2020 - Mar, 2020	**Researcher**, *M5 Team* in R&D Center
Aug, 2019 - Dec, 2019	**Researcher**, *Blockchain Cryptography Team* in R&D Center

Korea Telecom

Dec, 2018 - July, 2019	**Manager**, *Blockchain Biz Center in Future Platform Business Group*
Feb, 2018 - Nov, 2018	**Associate Research Engineer**, *Blockchain Center* in Institute of Convergence Technology

Seoul National Univeristy

Oct, 2017 - Feb, 2018	**Postdoctoral Researcher**, *Research Institute of Mathematics* Supervisor: Prof. Jung Hee Cheon

Agency for Science, Technology and Research, Singapore

Nov, 2016 - Apr, 2017	**Research Assistant**, *Data Center Technologies Division* in Data Storage Institute Supervisor: Dr. Khin Mi Mi Aung

Teaching

2020 Spring - **Instructor** at Seoul National Univeristy, Rep. of Korea

- Field Application of Blockchain
- Field Application Research of Blockchain

Research Interests

My research interests lie primarily in all aspects of cryptography, including but not limited to private set operations, foundations of blockchain, practical applications using fully homomorphic encryption and etc. I am also interested in solving scalability problems in the blockchain using zero-knowledge proofs, especially, SNARKs, incrementally verifiable computation, and vector commitment.

- SNARKs and Verifiable Computation
  - Incrementally Verifiable Computation & Proof-Carrying Data
  - Polynomial Commitment
  - Membership Proofs
  - One-out-of-Many Proofs
- Blockchain and Cryptocurrencies
  - Payment-Channel Network
  - Confidential Transaction
  - Multiparty ECDSA and Threshold Signature
- Practical Application using Homomorphic Encryption
  - Arithmetic on Real Numbers
  - Private Database Queries

Papers

- "Multiparty Delegated Private Set Union with Efficient Updates on Outsourced Data", *H. Chung, M. Kim, C. Yang*, IEEE Transactions on Dependable and Secure Computing, doi: 10.1109/TDSC.2024.3419576, 2024
- "Authentication of Multi-agent System with Verifiable Computation", *S. Lee, D. Kim, H. Chung, J. Kim, H. Shim*, IEEE Conference on Decision and Control 2024
- "Amortized Efficient zk-SNARKs from Linear-Only RLWE Encodings", *H. Chung, D. Kim, J. H. Kim, J. Kim*, Journal of Communications and Networks, 10.23919/JCN.2023.000012, 2023
- "Bulletproofs+: Shorter Proofs for Privacy-Enhanced Distributed Ledger", *H. Chung, K. Han, C. Ju, M. Kim, J. H. Seo*, IEEE Access 10: 42067-42082, 2022
- "Efficient Sum-Check Protocol for Convolution", *C. Ju, H. Lee, H. Chung, J. H. Seo, S. Kim*, IEEE Access 9: 164047-164059, 2021
- "연산을 검증하기 위한 영지식 증명 프로토콜의 기법 및 응용 사례 분석", 주찬양, 서재홍, 이현범, 정희원, Journal of The Korea Institute of Information Security and Cryptology, vol. 31, no. 4, pp. 675-686, 2021
- "Homomorphic Comparison for Point Numbers with User-Controllable Precision and its Applications", *K. Aung, A. Badawi, H. Chung, M. Kim, B. Veeravalli*, Symmetry 2020, 12(5), 788

- “Encoding of Rational Numbers and Their Homomorphic Computations for FHE-based Applications”, *H. Chung, M. Kim*, International Journal of Foundation Computer Science, 29(7): 1023-1044, 2018

- “An Improvement of Algorithm for ECDLP over Small Degree Extension Fields”, *J. H. Cheon, H. Chung, H.T. Lee*, 2014 Conference on Information Security and Cryptology, Pusan National University, Rep. of Korea

Draft

- Doubly Efficient Fuzzy Private Set Intersection for High-dimensional Data with Cosine Similarity (in peer-review), *H. Son, S. Paik, Y. Kim, S. Kim, H. Chung, and J.H. Seo*

- Secure Large Look-up Table Evaluation with Homomorphic Encryption (in peer-review), *H. Chung, H. Kim, Y. Kim, and Y. Lee*

- Computational Improvements to ADS-Based Verifiable Set Operations (in peer-review)

- Adaptive Successive Over-Relaxation Method for a Faster Iterative Approximation of Homomorphic Operations (in peer-review)

- Updatable Verifiable Computation without Proof Compositions

- “Ghostshell: Secure Biometric Authentication using Integrity-based Homomorphic Evaluations”, *J. H. Cheon, H. Chung, M. Kim, K. Lee*, Cryptology ePrint Archive, Report 2016/484

- “Encoding Rational Numbers for FHE-based Applications”, *H. Chung, M. Kim*, Cryptology ePrint Archive, Report 2016/344

Talks

Homomorphic Encryption

November 21, 2020	Invited Talk, Sungshin Women’s University, Rep. of Korea Title: “The Past 10 Years and The Next Chapter on Homomorphic Encryption”
April 25, 2015	2015 KMS Spring Annual Meeting, Pusan National University, Rep. of Korea Title: “Homomorphic Arithmetic on Real Numbers with Continued Fractions”

Bulletproofs+

December 19, 2020	ETHCon Korea 2020 Title: “Bulletproofs+: Shorter Proofs for Privacy-Enhanced Distributed Ledger”
July 3, 2020	2020 KMS Spring Annual Meeting Title: “Bulletproofs+: Shorter Proofs for Privacy-Enhanced Distributed Ledger”

Multiparty ECDSA

December 17, 2021	Invited Talk, Sungshin Women’s University Title: “How to Protect Your Assets Securely?”
May 13, 2020	Invited Talk, ETRI, Rep. of Korea Title: “Multiparty ECDSA with Application to Custody Service”
Oct. 25, 2019	2019 Fall Crypto Seminar, Hanyang University, Rep. of Korea Title: “Multiparty ECDSA with Application to Cryptocurrency Custody”

Confidential Transaction

December 02, 2021	Invited Talk, Enterprise Blockchain

	Title: “Skimming Confidential Transactions”
Sep. 4, 2019	Community of Practice, KISA Title: “A Road to Confidential Transaction”

Blockchain

April 07, 2022	Invited Talk, Gachon University Title: “Understanding Design of Blockchain”
Dec 5, 2019	Invited Talk, Jeonbuk National University, Rep. of Korea Title: “Beyond Bitcoin: Recent Key Results”
May 2, 2018	A Seminar on Industrial Mathematics Research Exchange, National Institute for Mathematical Sciences, Rep. of Korea Title: “Cryptography in the Blockchain”

Others

October 26, 2013	2013 KMS Fall Annual Meeting, University of Seoul, Rep. of Korea Title: “An Improvement of Algorithm for ECDLP over Small Degree Extension Fields”

Patents

KR 1020190024330	Method and System for Sharing Data, *S. Park, H. Chung, T. Hur*
KR 1020180173969	Survey Response Data Security Method and System, *H. Chung, S. Park*
KR 1020180075871	Apparatus and Method for Paying Insurance Claim based on Homomorphic Encryption and Blockchain, *H. Chung, T. Hur, S. Park*
KR 1020180003826	Electronic Device, Server and Controll Thereof, *J. Kim, J. Shin, J. H. Cheon, H. Chung, J. Jeong*
KR 1020150117454	Analytics Center and Its Control Method Thereof, and Service Providing Device and Control Method Thereof in co-operational Privacy Protection Communication Environment, *S. Jeong, K. Lee, S. Kim, J. H. Cheon, M. Kim, H. Chung*
KR 1020150117445	Storage Device and Control Method Thereof, *S. Jeong, K. Lee, S. Kim, J. H. Cheon, M. Kim, H. Chung*

Projects

Samsung Elec.	Privacy Preserving Pattern Matching	2016.09.01 - 2017.08.31
MISP[1]	DNA Analysis and Research for Practical Homomorphic Encryption for Secure Biometrics	2016.04.01 - 2016.12.31
SK Telecom	PoC for Homomorphic Encryption Usecase	2015.05.18 - 2015.12.31
SK Telecom	Applications for Homomorphic Encryptions	2014.09.01 - 2014.12.31
Samsung SDS	Thin-Client ID-based Encryption	2012.08.01 - 2012.12.31

[1] MISP is an abbreviation of Ministry of Science, ICT, and Future Planning.

Grants

October, 2020	2020 Korea Crypto Contest, Encouragement Award Title: “Bulletproofs+: Shroter Proofs for Privacy-Enhanced Distributed Ledger”
November 19, 2015	2015 Korea Crypto Contest, Encouragement Award Title: “On Encoding Real Numbers for Fully Homomorphic Encryption based on Applications”

Reference

From Academia	Prof. Jung Hee Cheon	Professor Department of Mathematical Sciences Seoul National University jhcheon@snu.ac.kr
	Prof. Jae Hong Seo	Associate Professor Department of Mathematics Hanyang University jaehongseo@hanyang.ac.kr
	Prof. Myungsun Kim	Assistant Professor Department of Mathematical Finance Gacheon University msunkim@gacheon.ac.kr
From Industry	Dr. Jinsu Kim	Senior Engineer Samsung Research Security Lab Samsung Electronics jinsu86.kim@samsung.com