Dongwoo Kim – Curriculum Vitae

Affiliation	College of AI Convergence, Dongguk University
Email	(work) Dongwoo.Kim@dgu.ac.kr (personal) dwkim606@gmail.com
Website	`https://dwkim606.github.io`

Employment

- Present **College of AI Convergence, Dongguk University**, Seoul, South Korea
Mar 2023 Assistant Professor

-Feb 2023 **Western Digital Research**, Milpitas, CA, United States
Dec 2020 Principal Engineer - Security and Cryptography

- Dec 2020 **IMDARC, Seoul National University**, Seoul, South Korea
Mar 2020 Postdoctoral Researcher

Education

- Feb 2020 **Ph.D** in Mathematical Sciences at **Seoul National University**, Seoul, South Korea
Mar 2013 * Advisor: Prof. Jung Hee Cheon
* Thesis : Verifiable Computing for Approximate Arithmetic

- Feb 2013 **B.S.** in Mathematical Sciences (minor in Physics) - **Seoul National University**, Seoul, South Korea
Mar 2009 * Cum Laude

Research Interests

Improving several **cryptographic primitives** including:

- **Fully Homomorphic Encryption**
- Verifiable Computing, **zk-SNARK**, Zero-Knowledge Proof
- **Secure Multiparty Computation**
- Lattice-based (Post-Quantum) Cryptography

towards **Privacy-Preserving Machine Learning**, Secure Dynamic Control Systems, and other applications. More broadly, I am interested in developing theoretical results of cryptography, computer science, and mathematics into solutions for real-world problems.

Awards & Grants [Exchange rate: 1 USD $\approx 1,000$ KRW]

May 2023 - A Study on Credential Verification Technique Using Distributed Zero-Knowledge Proof
(60,000 USD) Commissioned research from ETRI

Nov 2020 Excellence Award at Korea Cryptography Contest
(2,000 USD) by Korea Institute of Information Security & Cryptology

Feb 2020 **Gold Award** (**1st place** in Computer Science & Engineering) at **Samsung Humantech Paper Award**
(10,000 USD) by Saumsung

Nov 2019 Excellence Award at Korea Cryptography Contest

(1,500 USD) by Korea Institute of Information Security & Cryptology

Nov 2017 Encouragement Award at Korea Cryptography Contest
(1,000 USD) by Korea Institute of Information Security & Cryptology

- Feb 2016 Basic Science Scholarship
Mar 2015 (5,000 USD) by Seoul National University

Publications

Authors are listed in *alphabetical order* following the conventions in the field of cryptography and mathematics.
Other papers without that convention are marked by an asterisk(*).

14. **Amortized Efficient zk-SNARK from linear-Only RLWE Encodings**
(*) Heewon Chung, *Dongwoo Kim* (Co-1st), Jeong Han Kim, and Jiseung Kim
Journal of Communications and Networks, (2023), `https://doi.org/10.23919/JCN.2023.000012`

13. **Optimized Privacy-Preserving CNN Inference With Fully Homomorphic Encryption**
(*) *Dongwoo Kim* (✉), & Cyril Guyot
IEEE Transactions on Information Forensics and Security, **18**, pp. 2175-2187 (2023), `https://doi.org/10.1109/TIFS.2023.3263631`

12. **Interactive Proof for Rounding Arithmetic**
Shuo Chen, Jung Hee Cheon, *Dongwoo Kim* (✉), & Daejun Park
IEEE ACCESS, **10**, pp. 122706-122725 (2022), `https://doi.org/10.1109/ACCESS.2022.3223136`

11. **Comparison of encrypted control approaches and tutorial on dynamic systems using Learning With Errors-based homomorphic encryption**
(*) Junsoo Kim, *Dongwoo Kim* (✉), Yongsoo Song, Hyungbo Shim, Henrik Sandberg, & Karl H. Johansson
Annual Reviews in Control, **54**, pp. 200-218 (2022), `https://doi.org/10.1016/j.arcontrol.2022.10.002`

10. **On the Scaled Inverse of $(x^i - x^j)$ modulo Cyclotomic Polynomial of the form $\Phi_{p^s}(x)$ or $\Phi_{p^s q^s}(x)$**
Jung Hee Cheon, Dongwoo Kim, Duhyeong Kim, & Keewoo Lee
J. Korean Math. Soc. **59** (3), pp. 621-634 (2022), `https://doi.org/10.4134/JKMS.j210446`

9. **Efficient verifiable computation over quotient polynomial rings**
(*) Jai Hyun Park, Jung Hee Cheon, & *Dongwoo Kim* (✉)
Int. J. Inf. Secur. **21**, pp. 953–971 (2022), `https://doi.org/10.1007/s10207-022-00590-x`

8. **MHz2k: MPC from HE over $\mathbb{Z}_{2^k}$ with New Packing, Simpler Reshare, and Better ZKP**
Jung Hee Cheon, *Dongwoo Kim* (✉), & Keewoo Lee
(CRYPTO 2021), [link]

7. **Lattice-based Secure Biometric Authentication for Hamming Distance**
Jung Hee Cheon, *Dongwoo Kim* (✉), Duhyeong Kim, Joohee Lee, Junbum Shin, & Yongsoo Song
The 26th Australasian Conference on Information Security and Privacy **(ACISP 2021)**, [link]

6. **Flexible and Efficient Verifiable Computation on Encrypted Data**
Alexandre Bois, Ignacio Cascudo, Dario Fiore, & Dongwoo Kim
The 24th IACR International Conference on Public-Key Cryptography **(PKC 2021)**, [link]

5. **Efficient Homomorphic Comparison Methods with Optimal Complexity**
Jung Hee Cheon, Dongwoo Kim, & Duhyeong Kim
(ASIACRYPT 2020), [link]

4. **Privacy-preserving approximate GWAS computation based on Homomorphic Encryption**
(*) Duhyeong Kim, Yongha Son, *Dongwoo Kim* , Andrey Kim, Seungwan Hong, & Jung Hee Cheon
BMC Med Genomics **13**, 77 (2020), `https://doi.org/10.1186/s12920-020-0722-1`

3. **Authenticated Computation of Control Signal from Dynamic Controllers**
Jung Hee Cheon, Dongwoo Kim, Junsoo Kim, Seungbeom Lee, & Hyungbo Shim
The 59th IEEE Conference on Decision and Control **(CDC 2020)**, [link]

2. **Numerical Methods for Comparison on Homomorphically Encrypted Numbers**
   Jung Hee Cheon, Dongwoo Kim, Duhyeong Kim, Hun-Hee Lee, & Keewoo Lee
   (ASIACRYPT 2019), [link]

   ⋆ *Invited to Journal of Cryptology* (**Top 3** among 71 accepted papers (307 submissions total))

1. **Reusable Fuzzy Extractor with Practical Storage Size**
   Jung Hee Cheon, Jinhyuck Jeong, Dongwoo Kim, & Jongchan Lee
   The 23rd Australasian Conference on Information Security and Privacy **(ACISP 2018)**, [link]

Patents

6. **Tweaked Interpolation for Multiparty Computation**
   (KOR 10-2257779 *granted*)

5. **Plant Apparatus, Remote Controlling Apparatus and Method Thereof**
   (KOR 10-2404762 *granted*)

4. **Verifiable Computing for Approximate Computation**
   (KOR 10-2382952 *granted*, US 17/422278)

3. **Apparatus for Processing Non-polynomial Operation on Encrypted Messages and Methods Thereof**
   (KOR 10-2297536 *granted*, US 17/311567)

2. **User Device and Electronic Device for Sharing Data based on Block Chain and Homomorphic Encryption Technology and Methods Thereof**
   (KOR 10-2018-0040584, US 16/375,325 *granted*)

1. **Device for Processing Biological Data and Methods Thereof**
   (KOR 10-1938736 *granted*)

Talks

May 2021 Flexible and Efficient Verifiable Computation on Encrypted Data
IACR International Conference on Public-Key Cryptography (PKC2021), Online

Dec 2020 Authenticated Computation of Control Signal from Dynamic Controllers
59th IEEE Conference on Decision and Control, Online

Nov 2020 Verifiable Computation on Encrypted Data – with more Flexibility
Invited Talk at Crypto Seminar, Hanyang University, South Korea

Jan 2020 Verifiable Computing for Approximate Arithmetic
Invited Talk at Crypto Seminar, Ewha Womans University, South Korea

Nov 2019 Verifiable Computing
Invited Talk at Techtonic 2019, Samsung SDS, South Korea

Oct 2019 Interactive Proof for Rounding Arithmetic
2019 Korea Mathematical Society (KMS) Annual Meeting, South Korea

Oct 2019 Comparison on Homomorphically Encrypted Numbers: Towards Complexity-optimal Polynomial Approximation
Husik Symposium, Dep. of Mathematical Sciences, Seoul National University, South Korea

Aug 2019 Verifiable Computing and zk-SNARKs
Invited Talk at Bloom Technology, South Korea

Mar 2019 Reusable Fuzzy Extractor with Practical Storage Size
2018 Korea Mathematical Society (KMS) Annual Meeting, South Korea

Service

Teaching

2023-1	Discrete Mathematics Computational Thinking Quantum Computing

Conference/Journal Review

2022	ICML (recognized as **top 10%** reviewer), ASIACRYPT
2021	ACM TOPS (formerly known as TISSEC), IEEE TCNS
2020	IEEE CDC, ANTS, ASIACRYPT, PKC
2019	Designs, Codes and Cryptography
2019-2017 (sub-review)	CRYPTO, ASIACRYPT, NDSS, CT-RSA, PKC, PQC

Teaching Assistant

2019-1 2018-1,2	Mathematics for the Life Sciences
2019-1	Statistical Linear Algebra
- Feb 2018 Sep 2014	Basic Calculus (TA of Tutoring Program)
2013-1,2	Linear Algebra
2014-1 2013-1,2	Calculus I, II

Languages, Skills, and Others

Languages	Korean (native), English (fluent)
Skills	C/C++, Python (SageMath, TensorFlow), Go
Visiting (Sep-Dec 2017)	**ENS de Lyon**, Lyon, France. Hosted by **Damien Stehlé**