Myungsun Kim

Curriculum Vitae

Department of Mathematics
Gachon University
Room 611, Gachon Hall
1342 Seongnam-daero, Sujeong-gu, Seongnam-si
Gyeonggy-do 13120, South Korea

msunkim@gachon.ac.kr
Office: +82.31.750.8852
Cell Phone: +82.10.4109.0156

Research Interest

Cryptographic Primitives

- Cryptographic gadgets for efficient MPC
- Dynamic Searchable Encryption
- Efficient ADSs for verifiable DB queires

Cryptographic Applications

- Privacy and Integrity in set operations
- Privacy-preserving data mining

Education

Seoul National University

- Ph.D. in Mathematics, August 2012.
  Advisor: Jung Hee Cheon
  Thesis title: Cryptographic shuffles and their applications.

KAIST

- Masters of Engineering in Computer Science, August 2002.
  Advisor: Kwangjo Kim
  Thesis title: Provably secure identification scheme based on the bilinear Diffie-Hellman problem.

Sogang University

- Bachelor of Engineering in Computer Science, August 1994.

Experiences

Associate professor

- Department of Mathematics, Gachon University (Since Mar. 2021)

Associate professor

- Department of Information Security, The University of Suwon (Sep. 2012 – Feb. 2021)

Senior research engineer

- DRM Lab, DM R&D Center, Samsung Electronics Mar. 2003 – Dec. 2007.

Junior programmer

- IT Support Group, Korea Exchange Bank, Sep. 1994 – Jun. 2000.

Research Projects

Basic science research program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education, Science and Technology (MEST).

- Subject: A study on the efficiency of verifiable query evaluation from authenticated data structures (since Jun. 2023 to 2025).

Basic science research program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education, Science and Technology (MEST).

- Subject: Cryptography for private database queries (since Jun. 2017 to 2022).

Development of broadcasting, communication service technologies through the Institute for Information and communications Technology Promotion (IITP) Grant funded by the Korean Government (MSIT).

- Subject: A Study on Cryptographic Primitive for SNARK (since Apr. 2021 to 2026).

Development of broadcasting, communication service technologies through the Institute for Information and communications Technology Promotion (IITP) Grant funded by the Korean Government (MSIT).

- Subject: Privacy-Preserving and Vulnerability Analysis for Smart Contract (since Apr. 2018 to 2020).

Basic science research program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education, Science and Technology (MEST).

- Subject: Private set operations on the cumulative data model (since May 2014).

Scientific Papers

- **In Preparations**
  - Multiparty Delegated Private Set Union with Efficient Updates on Outsourced Data, with Heewon Chung
  - WildBerry: Verifiable Wildcard Query Evaluation over Dynamic Databases, with Hyung Tae Lee
- **International Journal Articles**

[J1] Myungsun Kim and Injae Lee, Taming the round efficiency of cryptographic protocols for private web search schemes. Information Sciences 612: 1–21 (2023).

[J2] HeeWon Chung and Kyoohyung Han and Chanyang Ju and Myungsun Kim and Jae Hong Seo, Bulletproofs+: Shorter Proofs for a Privacy-Enhanced Distributed Ledger. IEEE Access 10: 42067–42082 (2022).

[J3] Myungsun Kim, Toward Round-Efficient Verifiable Re-Encryption Mix-Net. IEEE Access 10: 91397–91413 (2022).

[J4] Myungsun Kim and Sangrae Cho and Seongbong Choi and Young-Seob Cho and Soohyung Kim and Hyung Tae Lee, A Key Recovery Protocol for Multiparty Threshold ECDSA Schemes. IEEE Access 10: 133206–133218 (2022).

[J5] Heewon Chung, Myungsun Kim, Ahmad Al Badawi, Khin Mi Mi Aung, and Bharadwaj Veeravalli. Homomorphic comparison for point numbers with user-controllable precision and its applications. Symmetry 12(5): 788-810 (2020).

[J6] Myungsun Kim, Hyung Tae Lee, San Ling, Shu Qin Ren, Benjamin Tan, Huaxiong Wang. Search condition-hiding query evaluation on encrypted databases. IEEE Access 7: 161283-161295 (2019).

[J7] Myungsun Kim and Hyung Tae Lee. Experimenting With Non-Interactive Range Proofs Based on the Strong RSA Assumption. IEEE Access 7: 117505-117516 (2019).

[J8] Myungsun Kim, Hyung Tae Lee, San Ling, Benjamin Hong Meng Tan, Huaxiong Wang: Private Compound Wildcard Queries Using Fully Homomorphic Encryption. IEEE Transactions on Dependable and Secure Computing, 2019, 16(5): 743-756.

[J9] Heewon Chung, Myungsun Kim. Encoding of Rational Numbers and Their Homomorphic Computations for FHE-Based Applications. International Journal of Foundations of Computer Science, 2018, 29(6): 1023-1044.

[J10] Myungsun Kim, Hyung Tae Lee, San Ling, Huaxiong Wang. On the Efficiency of FHE-Based Private Queries. IEEE Transactions on Dependable and Secure Computing, 2018, 15(2): 357-363.

[J11] Myungsun Kim, Benjamin Z. Kim. An experimental study of encrypted polynomial arithmetics for private set operations. Journal of Communications and Networks 19(5): 431-441 (2017).

[J12] Jung Hee Cheon, Miran Kim, and Myungsun Kim. Optimized search-and-compute circuits and their applications to query evaluation on encrypted data. IEEE Transactions on Information Forensics and Security, 2015: PP(99) (Online first published and as the corresponding author).

[J13] Abedelaziz Mohaien, Denis Foo Kune, Eugene Vasserman, Myungsun Kim, and Yongdae Kim. Secure encounter-based mobile social networks: requirements, designs, and tradeoffs. IEEE Transactions on Dependable and Secure Computing, 2013: 10(6), 380-393 (as the co-author).

[J14] Myungsun Kim, Jihye Kim, and Jung Hee Cheon. Compress multiple ciphertexts using ElGmal schemes. Journal of KMS, 2013: 50(2), 361–377 (as the first author).

[J15] Myungsun Kim, Hyung Tae Lee, and Jung Hee Cheon. A generalization of Agrawal et al.'s protocol for N-party private set intersection. Journal of Internet Technology, 2012: 13(6), 909–918 (as the first author).

[J16] Sungwook Kim, Eun Young Kwon, Myungsun Kim, Jung Hee Cheon, Seong-ho Ju, Young-hoon Lim, and Moon-seok Choi. A secure smart-metering protocol over power-line communication. IEEE Transaction on Power Delivery, 2011: 26(4), 2370–2379 (as the co-author).

- **Refereed International Conference Publications**

[C1] Jung Hee Cheon, Miran Kim, and Myungsun Kim. Search-and-compute on encrypted data. Financial Cryptography Workshops 2015 (as the corresponding author).

[C2] Bolam Kang, Sung Cheol Goh, and Myungsun Kim. Private web search with constant round efficiency. ICISSP 2015 (as the corresponding author).

[C3] Myungsun Kim, Abedelaziz Mohaisen, Jung Hee Cheon, and Yongdae Kim . Private over-threshold aggregation protocols. ICISC 2012 (as the first author).

[C4] Myungsun Kim and Jihye Kim. Privacy-preserving web search. ICUFN 2012 (as the first author).

[C5] Myungsun Kim, Hyung Tae Lee, and Jung Hee Cheon. Mutual private set intersection with linear complexity. WISA 2011 (as the first author).

[C6] Myungsun Kim, Jung Hee Cheon, Seokbeom Hong, and Seungmoon No. Universally human verifiable electronic voting scheme. ICONI 2010 (as the first author).

[C7] Myungsun Kim and Kwangjo Kim. A new identification scheme based on the bilinear Diffie-Hellman problem. ACISP 2002 (as the first author).

[C8] Myungsun Kim, Jongseong Kim, and Kwangjo Kim. Anonymous fingerprinting as secure as the bilinear Diffie-Hellman assumption. ICICS 2002 (as the first author).

- **Domestic Journal Publications**

[D̃1] Myungsun Kim and Bolam Kang. A generalization of zero-knowledge proof of polynomial equality. Journal of KICS, 2015: 40(5), 833–840 (as the first and corresponding author).

[D̃2] Myungsun Kim and Jaesung Park. A secure frequency computation method over multisets. Journal of KICS, 2014: 39B(06), 370–378 (as the first author).

[D̃3] Myungsun Kim, Trends on cryptographic mix-net schemes and their future research directions. Journal of Security Engineering, 2014: 11(1), 49–64 (as the first author).

[D̃4] Myunsun Kim. Security analysis and enhancement of Tsai *et al.*'s smartcard based authentication scheme. Journal of KICS, 2013: 39B(01), 29–37 (as the first author).

[D̃5] Myungsun Kim. A brokered authentication scheme based on smartcard for multi-server authentication. Journal of KICS, 2013: 38B(03), 190–198 (as the first author).

- **Domestic Conference Publications**

[D1] Bolam Kang, Myungsun Kim, and Seung Chul Goh. Private over-threshold aggregate protocol from Bloom filter and commutative encryption. KICS-S 2015 (as the corresponding author).

[D2] Myungsun Kim, Sunghyu Han, Bongseon Kim, and Yunsang Kim. ID-based self-enforcing protection of digital content. CISC-S 2004 (as the first author).

[D3] Myungsun Kim, Jongseong Kim, Jungyeon Lee, and Kwangjo Kim. A securely transferable ebooks using public-key infrastructure, CISC-W 2001 (as the first author).

- **Technical Reports**

[R1] Myungsun Kim, Jinsu Kim, and Jung Hee Cheon, A public shuffle without private permutations. 2012:301

[R2] Myungsun Kim. A generalization of zero-knowledge proof of polynomial product equality. 2010.

Patents

[P1] Method and apparatus for efficiently encrypting/decrypting digital content according to broadcast encryption scheme, US9015077, with Bongseon Kim, Sunghyu Han, Youngsun Yoon, Sunnam Lee, and Jaeheung Lee, 2015.

[P2] Key management method using hierarchical node topology, and method of registering and deregistering user using the same, US8983071, with Sunghyu Han, Bongseon Kim, Youngsun Yoon, Sunnam Lee, and Jaeheung Lee, 2015.

[P3] Obfuscation method for process of encrypting/decrypting block cipher using boolean function expression and apparatus for the same, KR1012812750000, with Jung Hee Cheon, 2013.

[P4] Method and apparatus for managing digital content, US8474055, with Juhee Seo, Haksoo Ju, Jiyoung Moon, and Mihwa Park, 2013

[P5] System and method for building home domain using smart card which contains information of home network member device, US8347076, with Jaeheung Lee, Suhyun Nam, Yongjin Jang, and Yanglim Choi, 2013.

[P6] Method of controlling content access and method of obtaining content key using the same, US8341402, with Sunghyu Han, Youngsun Yoon, Sunnam Lee, Bongseon Kim, and Jaeheung Lee, 2012.

[P7] Method and devices for reproducing encrypted content and approving reproduction, US8321660, with Haksoo Ju and Jiyoung Moon, 2012.

[P8] Method of packaging broadcast contents, Lee Sunnam, US8301571, with Sunghyu Han, Youngsun Yoon, Jaeheung Lee, Bongseon Kim, and Moonyoung Choi, 2012.

[P9] Method for transmitting content in home network using user-binding, US8234493, with Sunghyu Han, Yongkuk You, Youngsun Yoon, Bongseon Kim, and Jaeheung Lee, 2012.

[P10] Key management method for home network and home network device and system using the same, US8170215, with Sunnam Lee, Suhyun Nam, Sangsu Choi, and Sunghyu Han, 2012.

[P11] Method and apparatus for managing digital content, US8161296, with Yoon Youngsun, Lee Sunnam, Kim Bongseon, Lee Jaeheung, and Han Sunghyu, 2012.

[P12] Method and apparatus for backing up and restoring domain information, US8156344, with Bongseon Kim, Sunghyu Han, Youngsun Yoon, Sunnam Lee, and Jaeheung Lee, 2012.

[P13] Method and apparatus for checking proximity between devices using hash chain, US8122487, with Jaeheung Lee, Sunghyu Han, Youngsun Yoon, Sunnam Lee, and Bongseon Kim, 2012.

[P14] Home network system and method therefor, US7979913, with Yongjin Jang, Suhyun Nam, and Jaeheung Lee, 2011.

[P15] Scrambling apparatus and method using conversion of motion vector information of video data, US7826615, with Suhyun Nam, Yongjin Jang, Sunnam Lee, Jaeheung Lee, and Sangsu Choi, 2010.