Myungsun Kim

Curriculum Vitae

Department of Information Security
College of Information & Technology
The University of Suwon
IT Bldg. Room 501
17 Wauan-gil, Bongdam-eup,
Hwaseong (445-743), Republic of Korea

msunkim@suwon.ac.kr
Office: +82.31.229.8353
Cell Phone: +82.10.4109.0156

Research Interest

Cryptographic Algorithms

- Design and Analysis focused on Fully Homomorphic Encryption.
- Speed-up and Implementation of FHE schemes.

Secure Multi-party Computation

- Design and Implementation, focused on Private Set Operations.

FHE-based applications

- Private Database Query Processing with Practical Efficiency.

Education

Seoul National University

- Ph.D. in Mathematics, August 2012.
  Advisor: Jung Hee Cheon
  Thesis title: Cryptographic shuffles and their applications.
  GPA: 88.1/100

ICU (Information & Communications University); unfortunately at 2009, merged into 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.
  GPA: 95.0/100

Sogang University

- Bachelor of Engineering in Computer Science, August 1994.
  GPA: 82.1/100

Experiences

Assistant professor

- Department of Information Security, Colledge of Information & Technology, The University of Suwon (Since September 2012)
  - Modern cryptography (Textbook: Understanding cryptography, by C. Parr *et al.*)

· Data structure (Textbook: Fundamentals of data structures in C, by E. Horowitz *et al.*)
· Introduction to algorithm (Textbook: Algorithms, by R. Sedgewick)
· Discrete mathematics (Textbook: Discrete mathematics and its application, by K. Rosen)
· Database security (Textbook: Database security & auditing, by H. Afyouni)

Senior research engineer

– DRM Lab, DM R&D Center, Samsung Electronics March 2003 – December 2007.
  · References: [P1-P2], [P4-P15]

Programming engineer

– IT Support Team, Korea Exchange Bank, September 1994 – June 2000.

Awards and Honors

Seoul Science fellowship

– Seoul National University, Korea, September 2008 – December 2009.

Best paper at CISC-S 2004.

Graduated with Honors (Magna Cum Laude) at KAIST.

Projects

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).
– References: [S1-S2], [S4-S5], [M1-M2], [J1]

Industry-University cooperative reseach through SK Telecom.

– Development of Fully Homomorphic Encryption and its Biometric-based Application, with Jung Hee Cheon, (since September 2014).
– References: [S3]

Industry-University cooperation specialization program supervised by the NIPA (National IT Industry Promotion Agency (NIPA) under the Ministry of Science, ICT and Future Planning.

– Subject: Information Security Technology Development for the establishment of a secure smart work environment, with Seung-Chul Goh (since July 2014).
– References: [C2], [$\tilde{\text{D}}$1], [D1]

Teaching and Advising

Advising

– HeeWon Chung, PhD Candidate in Department of Mathematical Sciences, Seoul National University (Since September 2014).

Teaching Assistant

- Calculus, Seoul National University, September 2008 – June 2010.
- Linear algebra, Seoul National University, September 2010 – June 2011.

Scientic Papers

- **In Revision**
  - Jung Hee Cheon, HeeWon Chung, and Myungsun Kim. Ghostshell: Secure Biometric Authentication using Integrity-based Homomorphic Evaluations.
- **In Submissions and/or Accepted**

[S1] Encoding of rational numbers for FHE-based applications, with HeeWon Chung.

[S2] Private web search with an expected constant round. [C2] has a serious error which is fixed in this full version.

[S3] Better Security for Queries on Encrypted Databases, with Hyung Tae Lee, San Ling, Shu Qin Ren, Benjamin Hong Meng Tan, and Huaxiong Wang.

[S4] On the Efficiency of FHE-based Private Queries, with Hyung Tae Lee, San Ling, and Huaxiong Wang. Appeared at IEEE Transactions on Dependable and Secure Computing.

[S5] An experimental study of encrypted polynomial arithmetics for private set operations, with Benjamin Z. Kim.

- **In Minor or Major Revisions**

[M1] Private over-threshold aggregation protocols over distributed databases, with Aziz Mohaisen, Jung Hee Cheon, and Yongdae Kim to IEEE Transactions on Knowledge and Data Engineering with Major revision.

- **International Journal Articles**

[J1] 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).

[J2] 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).

[J3] 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).

[J4] 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).

[J5] 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.

[C2] Bolam Kang, Sung Cheol Goh, and Myungsun Kim. Private web search with constant round efficiency. ICISSP 2015.

[C3] Myungsun Kim, Abedelaziz Mohaisen, Jung Hee Cheon, and Yongdae Kim . Private over-threshold aggregation protocols. ICISC 2012.

[C4] Myungsun Kim and Jihye Kim. Privacy-preserving web search. ICUFN 2012).

[C5] Myungsun Kim, Hyung Tae Lee, and Jung Hee Cheon. Mutual private set intersection with linear complexity. WISA 2011.

[C6] Myungsun Kim, Jung Hee Cheon, Seokbeom Hong, and Seungmoon No. Universally human verifiable electronic voting scheme. ICONI 2010.

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

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

- **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.

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

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

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

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

- **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.

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

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

- **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.