## Aaram Yun


CONTACT INFORMATION

Rm. 501-3, Engr. Bldg. 3,
School of Electrical & Computer Engineering,
Ulsan National Institute of Science and Technology (UNIST), UNIST-gil 50, Ulsan 689-798, Korea.

*Mobile:* +82 (0) 10-2845-8625
*E-mail:* aaramyun@unist.ac.kr


RESEARCH INTERESTS

My research area is cryptography, that is, design and analysis of provably secure cryptographic services. Currently, I am especially interested in

- Homomorphic cryptography: unlike conventional cryptography, homomorphic cryptography allows secure processing of cryptographically protected data, like encrypted ciphertexts or authenticated data, by third parties. I am especially interested in homomorphic authentication and verifiable computation.
- Post-quantum cryptography: due to Shor's algorithm, most of currently existing public-key cryptography will be broken, once a practical quantum computer is built. Post-quantum cryptography is to design cryptosystems secure even against quantum computers. I am interested in both the foundational computational problems and the proof methodology for post-quantum cryptography.
- Computational/mathematical foundations of cryptography: hardness of fundamental computational problems based on lattices, elliptic curves, or factorization. Also I am interested in computational complexity theory and algorithms.
- Computer security/applied cryptography: applying cryptographic techniques to build secure computer systems.

POSITIONS

**UNIST**, Ulsan, Korea — Sep. 2016 to present
Associate Professor in School of Electrical & Computer Engineering.

**UNIST**, Ulsan, Korea — Nov. 2010 to Aug. 2016
Assistant Professor in School of Electrical & Computer Engineering.

**University of Minnesota**, Twin Cities, U.S.A. — Sep. 2007 to Aug. 2010
Postdoctoral researcher in Department of Computer Science and Engineering.

**National Security Research Institute (NSRI)**, Daejeon, Korea. — Sep. 2003 to Jul. 2007
Senior researcher.

**Samsung SDS**, Seoul, Korea. — Jul. 2001 to Aug. 2003
Researcher at Information Technology Research Group.

EDUCATION

**Yale University**, New Haven, Connecticut, U.S.A. — Sep. 1995 to June 2001

Ph.D. in Mathematics, June 2001

- Research advisor: Professor Gregory Margulis

**KAIST**, Daejeon, Republic of Korea. — Mar. 1991 to Feb. 1995

B.S. in Mathematics, Feb. 1995

INTERNATIONAL JOURNAL PUBLICATIONS

[1] Aaram Yun, "Discrete Subgroups of the Special Linear Groups with Thin Limit Sets", Transactions of the American Mathematical Society, vol. 369(1), pp. 365–407, 2017.

[2] Jung Hee Cheon, Jinsu Kim, Moon Sung Lee, Aaram Yun, "CRT-based Fully Homomorphic Encryption over the Integers", *Information Sciences*, vol. 310, pp. 149–162, 2015.

[3] Shoichi Hirose, Je Hong Park, Aaram Yun, "A Simple Variant of the Merkle-Damgård Scheme with Permutation", *Journal of Cryptology*, vol. 25(2), pp. 271–309, 2012.

[4] Aaram Yun, Je Hong Park, Jooyoung Lee, "On Lai-Massey and Quasi-Feistel Ciphers", *Designs, Codes, and Cryptography*, vol. 58(1), pp. 45–72, 2011.

[5] Aaram Yun, Jung Hee Cheon, Yongdae Kim, "On Homomorphic Signatures for Network Coding", *IEEE Transactions on Computers*, vol. 59, no. 9, pp. 1295–1296, 2010.

DOMESTIC JOURNAL PUBLICATIONS

[6] Chihong Joo, Aaram Yun, "A Strongly Unforgeable Homomorphic MAC over Integers", Journal of the Korea Institute of Information Security and Cryptology (JKIISC), vol. 24, no. 3, pp. 461–475, 2014.

CONFERENCE PUBLICATIONS

[7] Fang Song, Aaram Yun, "Quantum Security of NMAC and Related Constructions", Proceedings of CRYPTO 2017, Lecture Notes in Computer Science, vol. 10402, pp. 283–309, Springer, 2017.

[8] Aaram Yun, "Generic Hardness of the Multiple Discrete Logarithm Problem", Proceedings of EUROCRYPT 2015, Lecture Notes in Computer Science, vol. 9057, pp. 817–836, Springer, 2015.

[9] Chihong Joo, Aaram Yun, "Homomorphic Authenticated Encryption Secure Against Chosen-Ciphertext Attack", Proceedings of ASIACRYPT 2014, Lecture Notes in Computer Science, vol. 8874, pp. 173-192, Springer, 2014.

[10] Jung Hee Cheon, Jean-Sébastien Coron, Jinsu Kim, Moon Sung Lee, Tancrède Lepoint, Mehdi Tibouchi, Aaram Yun, "Batch Fully Homomorphic Encryption Over the Integers", Proceedings of EUROCRYPT 2013, Lecture Notes in Computer Science, vol. 7881, pp. 315–335, Springer, 2013.

[11] Abedelaziz Mohaisen, Aaram Yun, Yongdae Kim, "Measuring the Mixing Time of Social Graphs", Proceedings of the 10th ACM SIGCOMM Conference on Internet Measurement (IMC'10), Melbourne, Australia, 2010.

[12] Aaram Yun, Chunhui Shi, Yongdae Kim, "On Protecting Integrity and Confidentiality of Cryptographic File System for Outsourced Storage", Proceedings of CCSW 2009: The ACM Cloud Computing Security Workshop, pp. 67–76, Springer, 2009.

[13] Vishal Saraswat, Aaram Yun, "Anonymous Signatures Revisited", Proceedings of ProvSec 2009, Lecture Notes in Computer Science, vol. 5848, pp. 140–153, Springer, 2009.

[14] Shoichi Hirose, Je Hong Park, Aaram Yun, "A Simple Variant of the Merkle-Damgård Scheme with Permutation", Proceedings of ASIACRYPT 2007, Lecture Notes in Computer Science, vol. 4833, pp. 113–129, Springer, 2007.

[15] Hongbo Yu, Xiaoyun Wang, Aaram Yun, Sangwoo Park, "Cryptanalysis of the Full HAVAL with 4 and 5 Passes", Proceedings of FSE 2006, Lecture Notes in Computer Science, vol. 4047, pp. 89–110, Springer, 2006.

[16] Hong-Su Cho, Sangwoo Park, Soo Hak Sung, Aaram Yun, "Collision Search Attack for 53-Step HAS-160", Proceedings of ICISC 2006, Lecture Notes in Computer Science, vol. 4296, pp. 286–295, Springer, 2006.

[17] Aaram Yun, Soo Hak Sung, Sangwoo Park, Donghoon Chang, Seokhie Hong, Hong-Su Cho, "Finding Collision on 45-Step HAS-160", Proceedings of ICISC 2005, Lecture Notes in Computer Science, vol. 3935, pp. 146–155, Springer, 2005.

[18] Aaram Yun, Jaeheon Kim, Dong Hoon Lee, "Cryptanalysis of a Divisor Class Group Based Public-Key Cryptosystem", Proceedings of ANTS 2004, Lecture Notes in Computer Science, vol. 3076, pp. 442–450, Springer, 2004.

## INVITED TALKS AND SEMINARS

- "Trends in Quantum Computation and Post-quantum Cryptography", Workshop for the Role of Cryptography in the Future Cyber Security, Apr. 8, 2016.
- "Generic Hardness of the Multiple Discrete Logarithm Problem", Dept. of Math., Yonsei University, Sep. 10, 2015.
- "Intro. to Cryptography", NIMS Summer School on Cryptography, June 22, 2015.
- "Provable Security and Mathematical Assumptions / Generic Group Model", Mathematical Cryptology Workshop, Ewha Womans University, Feb. 5, 2015.
- "Intro. to Cryptography", NIMS Summer School on Cryptography, June 24, 2014.
- "On Homomorphic Authenticated Encryption", 2014 KMS Spring Meeting, Apr. 26, 2014.
- "Homomorphic Authenticated Encryption", Dept. of Math., Ulsan National University, Jan. 23, 2014.
- "Understanding Cryptography", Dept. of Math., Ulsan National University, Dec. 12, 2013.
- "Homomorphic Cryptography", Dept. of Comp. Sci., POSTECH, Nov. 21, 2013.
- "Indifferentiability and Merkle-Damgård Construction", The Asian Mathematical Conference 2013 (AMC 2013), Jul. 4, 2013.
- "The Young Person's Guide to the Cryptography", NIMS Summer School on Cryptography, June 26, 2013.
- "Homomorphic Authentication of Data", Electronics and Telecommunications Research Institute (ETRI), Apr. 10, 2013.
- "Intro. to Cryptography via Homomorphic Encryption", Dept. of Math., Ulsan National University, Oct. 18, 2012.
- "Homomorphic Signatures", National Institute for Mathematical Sciences (NIMS), July 4, 2012.
- "Secure Network Coding", NIMS-SNU Collaborative Research Bridge, Nov. 6, 2009.
- "Anonymity of Encryption and Signature Schemes", NIMS-SNU Collaborative Research Bridge, Oct. 29, 2009.
- "Cryptanalysis of the Hash Function HAVAL", KIAS, Jul. 14, 2006.
- "Collision Attack for the Hash Function HAVAL", KAIST, May 4, 2006.

## Professional Activities

**Program Committees**

- ACISP 2017
- ASIACRYPT 2016
- ICISC 2016
- ACISP 2016 (Australasian Conference on Information Security and Privacy)
- ICISC 2015 (International Conference on Information Security and Cryptology), Program co-chair
- ICISC 2014
- ICISC 2013

**Conference organizing**

- Algorithmic Number Theory Symposium (ANTS-XI), Member of the Local Organizing Committee for ANTS-XI, 2014.

**Journal reviewer**

- ACM Transactions on Information and System Security (TISSEC)
- ACM Transactions on Sensor Networks (TOSN)
- ETRI Journal
- IEEE Transactions on Computers (TC)
- Journal of Communications and Networks (JCN)
- Journal of the Korea Institute of Information Security and Cryptology (JKIISC)
- Journal of the Korean Mathematical Society (JKMS)

## Teaching

| | |
|---|---|
| • CSE331 Intro. to Algorithms | Spring, 2011 |
| • MTH103 Applied Linear Algebra | Spring, 2011 |
| • CSE232 Discrete Mathematics | Fall, 2011 |
| • ECE518 Modern Cryptography | Fall, 2011 |
| • CSE331 Intro. to Algorithms | Spring, 2012 |
| • MTH201 Differential Equations | Spring, 2012 |
| • CSE232 Discrete Mathematics | Fall, 2012 |
| • ECE515 Algorithm Design | Fall, 2012 |
| • ECE717 Computational Complexity | Spring, 2013 |
| • CSE232 Discrete Mathematics | Fall, 2013 |
| • CSE331 Intro. to Algorithms | Fall, 2013 |
| • CSE232 Discrete Mathematics | Spring, 2014 |
| • ECE518 Modern Cryptography | Spring, 2014 |
| • CSE332 Theory of Computation | Fall, 2014 |
| • CSE232 Discrete Mathematics | Spring, 2015 |
| • CSE332 Theory of Computation | Fall, 2015 |
| • CSE232 Discrete Mathematics | Spring, 2016 |
| • ECE613 Special Topics in Comp. Engr. IV (Quantum Computation) | Spring, 2016 |
| • CSE332 Theory of Computation | Fall, 2016 |
| • CSE232 Discrete Mathematics | Spring, 2017 |
| • CSE530 Algorithms and Complexity | Spring, 2016 |
| • CSE332 Theory of Computation | Fall, 2017 |
| • ECE717 Computational Complexity | Fall, 2017 |

## Funding

- Institute for Information & communications Technology Promotion (IITP), Apr. 2017–Dec. 2019. “Development of lattice-based post-quantum public-key cryptographic schemes”. Amount: 1,200,000,000 KRW. Principal Investigator.
- Institute for Information & communications Technology Promotion (IITP), Nov. 2016–Jul. 2021. “The mathematical structure of functional encryption and its analysis”. Amount: 1,353,750,000 KRW. Co-investigator.
- Samsung Research Funding Center for Future Technology (ID160105475), Jun. 2016–May 2019. “Provable security in post-quantum cryptography”. Amount: 400,000,000 KRW. Principal Investigator.

- Cryptography Research Society, Feb. 2016–Nov. 2016. “Research on quantum algorithms and security analysis of modern cryptography”. Amount: 45,000,000 KRW. Principal Investigator.
- National Security Research Institute (NSRI) Collaborative Research Project, Apr. 2016–Oct. 2015. “Research on security proof and security analysis techniques for designing symmetric-key primitives”. Amount: 80,000,000 KRW. Co-investigator.
- National Research Foundation (NRF) General Research Program (No. 2011-0025127), Sep. 2011–Aug. 2016. “Research on homomorphic public-key cryptosystems”. Amount: 174,625,000 KRW. Principal Investigator.
- National Security Research Institute (NSRI) Collaborative Research Project, Apr. 2015–Nov. 2015. “Research on cryptographic security proof techniques for IoT information protection”. Amount: 90,000,000 KRW. Co-investigator.
- National Security Research Institute (NSRI) Collaborative Research Project, Mar. 2014–Oct. 2014. “Research on fundamental cryptographic technology for building ICT information protection infrastructure”. Amount: 90,000,000 KRW. Co-investigator.
- National Security Research Institute (NSRI) Collaborative Research Project, Jul. 2013–Nov. 2013. “Research on fundamental technologies for ICT information security”. Amount: 50,000,000 KRW. Co-investigator.

GRADUATE STUDENTS

- Chihong Joo, Mar. 2011–Aug. 2016
- Hyunmin Choi, Mar. 2014–present
- Jeongsu Kim, Mar. 2017–present

PROFESSIONAL MEMBERSHIPS

- International Association for Cryptologic Research (IACR), Member, 2005–present
- Korean Mathematical Society (KMS), Member, 2013–present
- Korea Institute of Information Security and Cryptology, Member, 2014–present

HONORS AND AWARDS

- Participated as a member of the Korean national team in the 31st International Mathematical Olympiad (IMO), July 1990.
- Silver medal in the 2nd National Mathematics and Science Competition, Oct. 1990.
- 1st prize in the 2nd Seoul Mathematics and Science Competition, Aug. 1990.
- Minister of Education Award in the 2nd National Personal Computer Competition, Apr. 1985.