Changmin Lee

Curriculum Vitae

School of Computational Sciences
Korea institute for advanced study (KIAS)
85 hoegiro, Dongdaemun-gu Korea
Email: changminlee@kias.re.kr, changminlee.kr@gmail.com
Phone: +82-10-2749-2395

Research Interest

Computational Number Theory, Algebraic Number Theory, Lattice Theory, Applied Mathematics-Cryptography

Education

2012–2017	Ph.D. in Mathematical Science, Seoul National University, Korea. **Advisor.** Prof. Jung Hee Cheon
2007–2012	BSc in Mathematical Science, Seoul National University, Korea.

Career

2020.10.–Now	KIAS Fellow, KIAS, Korea
2020.05.–2020.09	Visiting researcher, IMDARC, Korea
2020.01.–2020.05	Research visitor, The Simons Institute for the Theory of Computing, Berkeley, USA
2018.10.–2020.09	Labex Milyon Postdoctoral researcher, ENS de Lyon, France
2017.09–2018.09	Postdoctoral researcher, The Research Institute of Basic Sciences, Seoul National University, Korea.
2017.02–2017.08	Assistant researcher, The Research Institute of Basic Sciences, Seoul National University, Korea.
2015.09–2017.02	Researcher, The Research Institute of Basic Sciences, Seoul National University, Korea.

Papers

In Publication

2021	Wonhee Cho, Jiseung Kim, and Changmin Lee, "Extension of SDA algorithm for PACD variants", IET Information Security
2021	Wonhee Cho, Jiseung Kim, and Changmin Lee, "(In)security of concrete instantiation of Lin17's Functional Encryption Scheme from Noisy Multilinear Maps", Designs, Codes and Cryptography
2020	Jung Hee Cheon, Wonhee Cho, Minki Hhan, Minsik Kang, Jiseung Kim and Changmin Lee, "Algorithms for CRT-variant of Approximate Greatest Common Divisor Problem", Nutmic'19 and Journal of Mathematical Cryptology.
2019	Changmin Lee, Alice Pellet-Mary, Damien Stehlé, and Alexandre Wallet, "An LLL Algorithm for Module Lattices", Asiacrypt 2019.
2019	Jung Hee Cheon, Wonhee Cho, Minki Hhan, Jiseung Kim, and Changmin Lee, "Statistical Zeroizing Attack: Cryptanalysis of Candidates of BP Obfuscation over GGH15 Multilinear Map", Crypto 2019.
2019	Jung Hee Cheon, Kyoohyung Han, Changmin Lee, Hansol Ryu, and Damien Stehlé, "Cryptanalysis on the CLT13 Multilinear Map ", Journal of Cryptology
2018	Jung Hee Cheon, Minki Hhan, Jiseung Kim, and Changmin Lee, "Cryptanalysis on the HHSS Obfuscation Arising from Absence of Safeguards", IEEE Access.
2018	Jung Hee Cheon, Minki Hhan, Jiseung Kim, and Changmin Lee, "Cryptanalyses of Branching Program Obfuscations over GGH13 Multilinear Map from the NTRU Problem", Crypto 2018
2018	Jung Hee Cheon, Changmin Lee, and Hansol Ryu, "Cryptographic Multilinear Maps and their Cryptanalysis", IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, Vol.E101
2017	Taechan Kim and Changmin Lee, "Lattice Reductions over Euclidean Rings with Applications to Cryptanalysis", IMACC 2017
2016	Jung Hee Cheon, Pierre-Alain Fouque, Changmin Lee, Brice Minaud, and Hansol Ryu, "Cryptanalysis of the New CLT Multilinear Map over the Integers", Eurocrypt 2016
2016	Jung Hee Cheon, Jinhyuck Jeong, and Changmin Lee, "An Algorithm for NTRU Problems and Cryptanalysis of the GGH Multilinear Map without a Low-Level encoding of zero", ANTS-XII
2016	Jung Hee Cheon, Kyoo Hyung Han, Jinsu Kim, Changmin Lee, and Yongha Son, "A Practical Post-Quantum Public-Key Cryptosystem Based on spLWE", ICISC 2016
2015	Jung Hee Cheon, Kyoohyung Han, Changmin Lee, Hansol Ryu, and Damien Stehlé, "Cryptanalysis of the Mulilinear Map over the integers", Eurocrypt 2015

Patent

2018.12.18	"Polynomial Functional Encryption Method with Linear ciphertext size", Jung Hee Cheon, Changmin Lee, Yongha Son, Seunghwan Hong, Granted Patent, Republic of Korea, Registration Number: 1019320320000

In Submission

2021	Jiseung Kim and Changmin Lee, " Simple and Efficient Algorithm for Solving Ideal Factorization", Submitted to Mathematics of Computation
2021	Jiseung Kim and Changmin Lee, " A Polynomial Time Algorithm for Breaking NTRU Encryption with Multiple Keys ", Submitted to Designs, Codes and Cryptography
2021	Jiseung Kim, Changmin Lee, and Jeeun Lee, " Asymptotically Faster Algorithm for ACD: Breaking the DGHV homomorhpic encryption", Submitted to Eurocrypt 2022
2021	Jiseung Kim and Changmin Lee, " Cryptanalysis of the FRS obfuscation based on the CLT13 Multilinear Map", Submitted to Designs, Codes and Cryptography
2021	Jiseung Kim and Changmin Lee, " Finding Small Roots for Bivariate Polynomials Modulo an Ideal of the Ring of Integers", Submitted to Advances in Mathematics of Communications

Research activities

Talks

2021.06	"An LLL algorithm for Module lattices", Ewha-KMS International Workshop on Cryptography: Theory and Applications in Cryptography
2020.06	"Cryptanalysis based on Coppersmtih algorithm", The summer schools of Fourteenth Algorithmic Number Theory Symposium, University of Auckland, New Zealand
2020.05	"A new multivariate based algorithm for the PACD problem", Invited Talk in National Security Research Institute, Korea
2019.08	"Noise Analysis", Invited Talk in Samsung SDS Corporation, Korea
2019.08	"An LLL algorithm for Module lattices", Invited Talk in National Security Research Institute, Korea
2019.07	"Cryptanalysis of Candidates of BP obfucation over CLT13 Multilinear Map", ICIAM 2019 CJK-joint mini-symposium, held in Valencia University, Spain
2019.06	"Algorithms for CRT-variant of Approximate Greatest Common Divisor Problem", Nutmic 2019, held in Sorbonne University, France
2018.05	"Cryptanalysis of CRT-ACD problem", KSIAM 2018 Spring Conference, Korea
2017.12	"Cryptanalysis of the NTRU", Invited Talk in National Security Research Institute, Korea
2017.11	"Cryptnalaysis of GGH Multilinear Maps", AIM workshop - Constructing cryptographic multilinear maps, Palo Alto, U.S.A
2016.09	"An Algorithm for NTRU Problems", ANTS-XII, held in University of Kaiserslautern, Germany
2015.10	"Improved lattice algorithms for finding a shorter and closer lattice point ", 2015 KMS Fall Meeting, held in Yonsei university, Korea
2015.05	"Cryptanalysis of the Mulilinear Map over the integers", Invited Talk in Ewha woman university crypt lab, Korea
2015.04	"Cryptanalysis of the Mulilinear Map over the integers", Eurocrypt 2015, held in Sofia Hotel Balkan, Bulgaria
2015.02	"Cryptanalysis of the Mulilinear Map over the integers", Mathematical Cryptology Workshop, held in Yangyang Solbeach Hotel, Korea

Program Committee

PKC 2022	The 25th edition of the International Conference on Practice and Theory of Public-Key Cryptography, March 7-11, 2022, Yokohama, Japan
ICISC 2021	The 24th International Conference on Information Security and Cryptology, December 1-3, 2021, Seoul, Korea
MathCrypt 2021	The international Workshop on Mathematical Cryptology, August 15, 2021, Santa Barbara, USA
PKC 2021	The 24th edition of the International Conference on Practice and Theory of Public-Key Cryptography, May 9-13, 2021, Edinburgh, Scotland, UK
WAHC 2020	The 8th Workshop on Encrypted Computing & Applied Homomorphic Cryptography, December 15, 2020, Virtual Corona Edition
ICISC 2020	The 23rd International Conference on Information Security and Cryptology, December 2-4, 2020, Seoul, Korea
WAHC 2019	The 7th Workshop on Encrypted Computing & Applied Homomorphic Cryptography, November 11, 2019, London, UK
MathCrypt 2019	The second international Workshop on Mathematical Cryptology, August 18, 2019, Santa Barbara, USA
APKC 2018	The 5th ACM ASIA Public-Key Cryptography Workshop, June 4, 2018, Incheon, Korea

Awards

2018.04	**Excellent Dissertation Award**, "Mathematical Analysis of Cryptographic Multilinear Maps", granted by Korean Mathematical Society
2017.11	**Grand Prize**, "Cryptanalysis of CRT-ACD problem", granted in 2017 National Cryptography Contest
2017.11	**Excellence Prize**, "Analysis of a Candidate iO with GGH13 Multilinear Map", granted in 2017 National Cryptography Contest
2017.11	Special Prize, "Cryptanalysis of a Candidate iO FRS17", granted in 2017 National Cryptography Contest
2016.11	Encouragement Prize, "A Practical Post-Quantum Public-Key Cryptosystem Based on spLWE.", granted in 2016 National Cryptography Contest
2015.11	Encouragement Prize, "A new attack algorithm to LWE problem with small dimensions.", granted in 2016 National Cryptography Contest
2015.11	**Excellence Prize**, "A New Multilinear Map over the ring of integer.", granted in 2015 National Cryptography Contest
2015.04	**Best Paper Award**, "Cryptanalysis of the Mulilinear Map over the integers", granted in Eurocrypt 2015
2014.11	**Grand Prize**, "A simple attack methods against CLT scheme", granted in 2014 National Cryptography Contest

Projects

2019.09 – 2020.03	"The better algorithm for ideal lattice problems" supported by National Research Foundation of Korea (NRF), as a principal investigator
2018.10 – 2020.09	"Labex Milyon postdoctoral researcher" supported by French National Agency for Research (ANR), as part of the program "Investments for the Future"
2016.11 – 2018.09	"Analysis of Multilinear Maps and Indistinguishability Obfuscation" supported by Defense Advanced Research Projects Agency (DARPA) as a research worker
2016.11 – 2018.09	"The mathematical structure of functional encryption and its analysis" supported by Institute for Information & communications Technology Promotion (IITP) as a research worker
2014.11 – 2017.10	"Lattice-based hard problems and their cryptographic applications" supported by National Research Foundation of Korea (NRF) as a research worker
2014.10 – 2017.09	"Development of a novel lightweight public key cryptosystem based on new hardness problems" supported by Samsung Electronics as a research worker
2013.09 – 2015.08	"Development of homomorphic encryption supporting arithmetics on ciphertexts of size less than 1kB and its applications" supported by the IT R&D program of MSIP/KEIT as a research worker
2012.03 – 2015.02	"A Study on Cryptographic Hard Problems" supported by National Research Foundation of Korea (NRF) as a research worker
2012.12 – 2013.10	Supported by Samsung Electronics as a research worker*
2009.11 – 2009.12	"Future Internet-based cryptographic technology research" supported by Korea Basic Science Institute (KBSI) as a research worker

* The informations of project supported by Samsung Electronics are kept secret for security reasons.