WONHEE CHO

27-441, 1, Gwanak-ro, Gwanak-gu, Seoul, Republic of Korea ◇ +82-2-880-6272
wony0404@snu.ac.kr ◇ linkedin.com/in/WonheeCho

EDUCATION

Seoul National University, Republic of Korea

Integrated Ph.D in Mathematical Sciences Mar 2017 - Present
Advisor: Prof. Jung Hee Cheon
Focus: Cryptography (Homomorphic Encryption, Statistical Cryptanalysis)

B.S. in Mathematical Sciences and Economics
Honers: Summa Cum Laude (GPA: 4.07/4.3) Mar 2011 - Feb 2017

Gyeonggi Science High School, Republic of Korea Mar 2009 - Feb 2011

RESEARCH INTERESTS

- **Homorphic Encryption (HE)**
  - Efficient bootstrapping algorithm for HE
  - Threshold structure for HE
  - Privacy-preserving machine learning (PPML) based on HE
  - Max algorithm for HE
- **Cryptanalysis of Cryptographic Primitives**
  - Statistical analysis
    - Indistinguishability obfuscation (iO)
    - Function encryption (FE)
    - Pseudo random function (PRF)
  - Algebraic analysis
    - Approximate greatest common divisor problem (AGCD)

RESEARCH PROJECTS

Homomorphic Encryption and its Applications

3. "Data Protection in Virtual Environments (DPRIVE)". Supported by DARPA Nov 2022 - Dec 2023

2. "Development and Library Implementation of Fully Homomorphic Machine Learning Algorithms supporting Neural Network Learning over Encrypted Data". Supported by the IITP Grant through the Korean Government Apr 2020 - Dec 2023

1. "Development of homomorphic encryption for DNA analysis and biometry authentication". Supported by the IITP Grant through the Korean Government Apr 2016 - Dec 2018

Functional Encryption and its Analysis

1. "The mathematical structure of functional encryption and its analysis". Supported by the IITP Grant through the Korean Government Nov 2016 - Jul 2021

PUBLICATIONS

Authors are listed in alphabetical order by last name, unless an asterisk (*) is indicated.

CONFERENCES

[C06] Jung Hee Cheon, Wonhee Cho, Jaehyung Kim, Damien Stehlé, "Homomorphic Multiple Precision Multiplication for CKKS and Reduced Modulus Consumption," ACM Conference on Computer and Communications Security (CCS), 2023

[C05] Youngjin Bae, Jung Hee Cheon, Wonhee Cho, Jaehyung Kim, Taekyung Kim, "META-BTS: Bootstrapping Precision Beyond the Limit," ACM Conference on Computer and Communications Security (CCS), 2022

- Best award, National Cryptography Contest 2022

[C04] Jung Hee Cheon, Wonhee Cho, Jeong Han Kim, Jiseung Kim, "Adventures in crypto dark matter: attacks, fixes for weak pseudorandom functions," IACR International Conference on Public-Key Cryptography (PKC), 2021

[C03] *Sunwoong Kim, Keewoo Lee, Wonhee Cho, Yujin Nam, Jung Hee Cheon, Rob A Rutenbar, "Hardware architecture of a number theoretic transform for a bootstrappable RNS-based homomorphic encryption scheme," 2020 IEEE 28th Annual International Symposium on Field-Programmable Custom Computing Machines (FCCM), 2020

[C02] *Sunwoong Kim, Keewoo Lee, Wonhee Cho, Jung Hee Cheon, Rob A Rutenbar, "FPGA-based accelerators of fully pipelined modular multipliers for homomorphic encryption," 2019 International Conference on ReConFigurable Computing and FPGAs (ReConFig), 2019

[C01] Jung Hee Cheon, Wonhee Cho, Minki Hhan, Jiseung Kim, Changmin Lee, "Statistical Zeroizing Attack: Cryptanalysis of Candidates of BP Obfuscation over GGH15 Multilinear Map," Annual International Cryptology Conference (CRYPTO), 2019

JOURNALS

[J06] *Seungwan Hong, Jai Hyun Park, Wonhee Cho, Hyeongmin Choe, Jung Hee Cheon, "Secure tumor classification by shallow neural network using homomorphic encryption," BMC genomics, 2022

- First Winner of Track 1, iDASH Genomic Data Privacy and Security Protection Competition 2020

[J05] Jung Hee Cheon, Wonhee Cho, Jeong Han Kim, Jiseung Kim, "Adventures in crypto dark matter: attacks, fixes and analysis for weak pseudorandom functions," Designs, Codes and Cryptography, 2022

[J04] *Miran Kim, Arif Ozgun Harmanci, Jean-Philippe Bossuat, Sergiu Carpov, Jung Hee Cheon, Ilaria Chillotti, Wonhee Cho, David Froelicher, Nicolas Gama, Mariya Georgieva, Seungwan Hong, Jean-Pierre Hubaux, Duhyeong Kim, Kristin Lauter, Yiping Ma, Lucila Ohno-Machado, Heidi Sofia, Yongha Son, Yongsoo Song, Juan Troncoso-Pastoriza, Xiaoqian Jiang, "Ultrafast homomorphic encryption models enable secure outsourcing of genotype imputation," Cell systems, 2021

- Second Winner of Track 2, iDASH Genomic Data Privacy and Security Protection Competition 2019

[J03] Wonhee Cho, Jiseung Kim, Changmin Lee, "Extension of simultaneous Diophantine approximation algorithm for partial approximate common divisor variants," IET Information Security, 2021

[J02] Wonhee Cho, Jiseung Kim, Changmin Lee, "(In) security of concrete instantiation of Lin17's functional encryption scheme from noisy multilinear maps," Designs, Codes and Cryptography, 2021

[J01] Jung Hee Cheon, Wonhee Cho, Minki Hhan, Jiseung Kim, Changmin Lee, "Algorithms for crt-variant of approximate greatest common divisor problem," Journal of Mathematical Cryptology, 2020

- 1^{st} award, National Cryptography Contest 2017

MANUSCRIPTS

[M04] Jung Hee Cheon, Wonhee Cho and Jiseung Kim, "Improved Universal Thresholdizer from Iterative Shamir Secret Sharing."

- Excellence award, National Cryptography Contest 2023

[M03] Jung Hee Cheon, Wonhee Cho and Minsik Kang, "A Distinguishing Attack and a Correlation Attack on a Reduced Variant of SNOW 3G."

[M02] Jung Hee Cheon, Wonhee Cho and Duhyeong Kim, "Note on IND-CPA+ Security of CKKS."

[M01] Jung Hee Cheon, Wonhee Cho, Seungwan Hong,and Chaewon Kim, "Efficient Homomorphic Max algorithm for Multivariables,"

- Participation award, National Cryptography Contest 2021

PATENTS

[P03] Jung Hee Cheon and Wonhee Cho, "Threshold Fully Homomorphic Encryption,"

- KOR 10-2023-0027008

[P02] Jung Hee Cheon, Wonhee Cho and Tae Kyung Kim, "Electronic Device and Controlling Method for Increasing An Operation Speed of Homomorphic Encrypted Data,"

- KOR 10-2023-0009570

[P01] Jung Hee Cheon, Wonhee Cho, Jinhyuck Jeong and Donggeon Yhee, "Apparatus for Performing Threshold Design on Secret Key and Method Thereof,"

- KOR 10-2160294 granted, KOR 10-2393942 granted, US 11201735 granted, PCT/KR2020/001687

AWARDS & HONORS

- National Cryptography Contest — Oct 2023
  Excellence Award ($1,500) — Korea Institute of Information Security and Cryptology
- National Cryptography Contest — Oct 2022
  Best Award ($3,000) — Korea Institute of Information Security and Cryptology
- National Cryptography Contest — Oct 2021
  Participation Award ($1,000) — Korea Institute of Information Security and Cryptology
- iDASH Genomic Data Privacy and Security Protection Competition (iDASH 2020) — Dec 2020
  First Winner of Track 1 — National institures of Health (NIH)
- National Cryptography Contest — Oct 2020
  Participation Award ($1,000) — Korea Institute of Information Security and Cryptology
- Scholarship for the next generation in basic fields — Mar 2020 - Feb 2021
  $24,000/year for 1 years — Seoul National University
- iDASH Genomic Data Privacy and Security Protection Competition (iDASH 2019) — Oct 2019
  Second Winner of Track 2 — National institures of Health (NIH)
- National Cryptography Contest — Oct 2017
  1^{st} Award ($10,000) — Korea Institute of Information Security and Cryptology

- BK 21+ Scholarship Mar 2017 - Aug 2017, Sep 2019 - Feb 2020, Mar 2021 - Present
  $7,500/year for M.S. and $12,000/year for Ph.D. Ministry of Education of Korea
- The Excellent national scholarship for science Mar 2011 - Feb 2017
  Academic Grant: Full-tuition for 4years Korea Student Aid Foundation
- Korean Mathematical Olympiad Nov 2009
  Silver Prize Korean Mathematical Society

TALKS

- **Improved Universal Thresholdizer from Iterative Shamir Secret Sharing.**
  2023 Korean Mathematical Society International Conference, Seoul, Republic of Korea Apr 2023
- **META-BTS: Bootstrapping Precision Beyond the Limit**
  CCS 2022 in Los Angeles, US Nov 2022
  2022 Korean Mathematical Society International Conference, Seoul, Republic of Korea Oct 2022
- **Adventures in crypto dark matter: attacks, fixes for weak pseudorandom functions**
  PKC 2021, Virtual May 2021
  2020 Korean Mathematical Society Spring Meeting, Virtual Jul 2020
- **Secure Genotype Imputation using HEaaN**
  iDASH Privacy & Security Workshop 2019, Indiana, US Oct 2019

EXPERIENCE

- General Assistant at the Graduate School of Mathematical Sciences Sep 2017 - Aug 2019
  Assistance for the entire assignment of assistants and operation of liberal mathematics to the Department of Mathematical Sciences Seoul National University
- Research Internship Apr 2016 - Feb 2017
  Conducted researches under the supervision of Prof. Jung Hee Cheon Seoul National University
- Teaching Assistant
  Calculus for Life Science Mar 2021 - Aug 2021
  Information Society and Mathematics Sep 2020 - Feb 2021
  Introduction to Cryptography Mar 2020 - Aug 2020
  Differential and Integral Calculus Mar 2017 - Feb 2020
- Military (Republic of Korea Army) Feb 2014 - Nov 2015

SERVICES

- Reviewer (Conferences)
  Asiacrypt 2019, 2021, 2022, 2023; Eurocrypt 2023, 2024; PKC 2019, 2021, 2024; CT-RSA 2019, 2020; PQCrypto 2020, 2021; WHAC 2021; ANTS 2020; FHE.org 2022
- Reviewr (Journals)
  Information Sciences

LANGUAGES AND SKILLS

Languages Korean (native), English (fluent)
Skills C/C++, Python, LaTeX