Mengce Zheng

+86 15156053155
mengce.zheng@gmail.com
No. 8 Qianhu South Road, Ningbo, Zhejiang, China
March 17, 2023
https://mengcezheng.github.io

Research Interest

Cryptography and Information Security: main focus on lattice-based cryptanalysis and post-quantum cryptosystems.

Employment

Zhejiang Wanli University — **Ningbo, China**
Major Leader in Cyberspace Security — 2022 – Present
Associate Professor in College of Information and Intelligence Engineering — 2021 – Present

University of Science and Technology of China — **Hefei, China**
Postdoctoral Researcher in Cyberspace Security (Hosted by Prof. Nenghai Yu) — 2019 – 2020

Education

University of Science and Technology of China — **Hefei, China**
PH.D. & M.S. “Lattice-Based Cryptanalyses of RSA and Its Variants” Advisor: Prof. Honggang Hu — 2013 – 2018
B.E. “The LLL Algorithm and Its Applications in Cryptography” Advisor: Prof. Honggang Hu — 2009 – 2013

The University of Tokyo — **Tokyo, Japan**
Visiting PH.D. “Security Analysis of RSA Using Lattice Reduction Algorithm” Advisor: Prof. Noboru Kunihiro — 2016 – 2017

Honors and Awards

Zhejiang Province University Leading Talent Training Program — **2022**
The Third Level – Young Talents

Ningbo Leading Talent Training Project — **2021**
The Third Level

CSC Scholarship for Joint Doctoral Students — **2016 – 2017**
JPY $150\,000 \times 12$

National Scholarship for Graduate Students — **2015**
CNY $20\,000$

Funding Acquisition

The National Natural Science Foundation of China — **2021 – 2023**
Grant No. 62002335, “Research on Cryptanalysis of RSA Type Algorithms Using Lattice-Based Method” — 1/1

The National Natural Science Foundation of China — **2020 – 2023**
Grant No. 61972370, “Derandomization Problem Under Cryptographic Function and Branching Program Calculation Model” — 2/8

Zhejiang Province Public Welfare Technology Application Research — **2022 – 2024**
Grant No. LGF22F020001, “Research and Application of Encrypted Machine Learning Using Multi-Party Fully Homomorphic Encryption” — 2/6

Ningbo Natural Science Foundation — **2022 – 2023**
Grant No. 2021J174, “Design and Analysis of Efficient Post-Quantum Cryptographic Algorithms Based on Mersenne Prime” — 1/5

Publications

Journal Articles

- **Mengce Zheng**. Revisiting the Polynomial-Time Equivalence of Computing the CRT-RSA Secret Key and Factoring. *Mathematics*, 10(13): 2238 (2022).
- **Mengce Zheng**, Noboru Kunihiro, Yuanzhi Yao. Cryptanalysis of the RSA variant based on cubic Pell equation. *Theoretical Computer Science* 889: 135–144 (2021).
- **Mengce Zheng**, Kaiping Xue, Shangbin Li, Nenghai Yu. A practical quantum designated verifier signature scheme for E-voting applications. *Quantum Information Processing* 20(7): 1–22 (2021).
- Zhigang Chen, Gang Hu, **Mengce Zheng**, Xinxia Song, Liqun Chen. Bibliometrics of Machine Learning Research Using Homomorphic Encryption. *Mathematics* 9: 2792 (2021).
- Qidong Jia, Kaiping Xue, Zhonghui Li, **Mengce Zheng**, David S. L. Wei, Nenghai Yu. An improved QKD protocol without public announcement basis using periodically derived basis.*Quantum Information Processing*, 20(2): 69 (2021).
- **Mengce Zheng**, Noboru Kunihiro, Honggang Hu. Lattice-based cryptanalysis of RSA with implicitly related keys. *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences* 103(8): 959–968 (2020).
- Jiajia Zhang, **Mengce Zheng**, Jiehui Nan, Honggang Hu, Nenghai Yu. A Novel Evaluation Metric for Deep Learning-Based Side Channel Analysis and Its Extended Application to Imbalanced Data. *IACR Transactions on Cryptographic Hardware and Embedded Systems* 2020(3): 73–96 (2020).

- **Mengce Zheng**, Honggang Hu, Zilong Wang. Generalized cryptanalysis of RSA with small public exponent. *SCIENCE CHINA Information Sciences* 59(3): 32108:1–32108:10 (2016).
- **Mengce Zheng**, Honggang Hu. Cryptanalysis of Prime Power RSA with two private exponents. *SCIENCE CHINA Information Sciences* 58(11): 1–8 (2015).

Conference Proceedings

- Shukun An, Jianzhao Liu, Xiaolin Duan, **Mengce Zheng**, Honggang Hu. Strengthening Profiled Side Channel Attacks on AES via Multi-view Information Aggregation. *CIS* 2021.
- Yukun Cheng, **Mengce Zheng**, Fan Huang, Jiajia Zhang, Honggang Hu, Nenghai Yu. A Fast-Detection and Fault-Correction Algorithm against Persistent Fault Attack. *TrustCom* 2021.
- Zhimin Luo, **Mengce Zheng**, Ping Wang, Minhui Jin, Jiajia Zhang, Honggang Hu. Towards Strengthening Deep Learning-based Side Channel Attacks with Mixup. *TrustCom* 2021.
- Wenlong Cao, Fan Huang, **Mengce Zheng**, Honggang Hu. Attacking FPGA-based Dual Complementary AES Implementation Using HD and SD Models. In: *CIS* 2020.
- Minhui Jin, **Mengce Zheng**, Honggang Hu, Nenghai Yu. An Enhanced Convolutional Neural Network in Side-Channel Attacks and Visualization. In: *WCSE* 2020.
- Zhengguang Shi, Fan Huang, **Mengce Zheng**, Wenlong Cao, Ruizhe Gu, Honggang Hu, Nenghai Yu. Research on Online Leakage Assessment. In: *ICPCSEE* 2020.
- **Mengce Zheng**, Honggang Hu. Implicit Related-Key Factorization Problem on the RSA Cryptosystem. In: *CANS* 2019.
- **Mengce Zheng**, Honggang Hu. Implicit-Key Attack on the RSA Cryptosystem. In: *SciSec* 2019.
- Jiehui Nan, **Mengce Zheng**, Honggang Hu. Post-Quantum Pseudorandom Functions from Mersenne Primes. In: *FCS* 2019.
- Jiehui Nan, **Mengce Zheng**, Zilong Wang, Honggang Hu. A General Construction for Password-Based Authenticated Key Exchange from Witness PRFs. In: *FCS* 2019.
- Zilong Wang, Honggang Hu, **Mengce Zheng**, Jiehui Nan. Symmetric Lattice-Based PAKE from Approximate Smooth Projective Hash Function and Reconciliation Mechanism. In: *FCS* 2019.
- **Mengce Zheng**, Noboru Kunihiro, Honggang Hu. Cryptanalysis of RSA Variants with Modified Euler Quotient. In: *AFRICACRYPT* 2018.
- Xiaolong Yang, **Mengce Zheng**, Honggang Hu. Generic Generating Functions for the Counting Functions of Quadratic Functions with Prescribed Walsh Spectrum. In: *DSC* 2018
- **Mengce Zheng**, Noboru Kunihiro, Honggang Hu. Improved Factoring Attacks on Multi-prime RSA with Small Prime Difference. In: *ACISP* 2017.

Presentations

Implicit Related-Key Factorization Problem on the RSA Cryptosystem **Fuzhou, China**
The 18th International Conference on Cryptology And Network Security Oct. 2019

Implicit-Key Attack on the RSA Cryptosystem **Nanjing, China**
The 2nd International Conference on Science of Cyber Security Aug. 2019

Cryptanalysis of RSA Variants with Modified Euler Quotient **Marrakesh, Morocco**
The 10th International Conference on the Theory and Applications of Security and Cryptography May 2018

Improved Factoring Attacks on Multi-prime RSA with Small Prime Difference **Auckland, New Zealand**
The 22nd Australasian Conference on Information Security and Privacy Jul. 2017

Activities

CACR 2022 Annual Conference	Online, 2022
IACR CRYPTO/EUROCRYPT/ASIACRYPT/PKC/CHES	Online, 2022
CACR 2021 Annual Conference	Online, 2021
IACR CRYPTO/EUROCRYPT/ASIACRYPT/TCC	Online, 2021
The 23rd Quantum Information Processing Conference	Shenzhen, China, 2020
CACR 2019 Annual Conference	Xi’an, China, 2019
CACR Quantum Cryptography Conference	Wuhu, China, 2019
The 6th ETSI International Conference on Quantum Secure Cryptography	Beijing, China, 2018
The 2nd Fully Homomorphic Encryption and Its Application Frontier Forum	Guangzhou, China, 2018
Cryptography and Information Security Workshop	Okinawa, Japan, 2017
The 1st Asian Post-Quantum Cryptography Forum	Chengdu, China, 2016
CACR Cryptographic Algorithm Conference	Nanjing, China, 2015

CACR 2015 Annual Conference	Shanghai, China, 2015
CACR 2014 Annual Conference	Zhengzhou, China, 2014

Teaching

Advanced Cryptography & Blockchain Development and Application	Spring 2023
Data Structures and Algorithms	Fall 2022
Cybersecurity Theory and Technology	Spring 2022
Data Structures and Algorithms	Fall 2021
Cybersecurity Technology	Spring 2021