

Mengce Zheng

+86 15156053155

mengce.zheng@gmail.com

No. 8 Qianhu South Road, Ningbo, Zhejiang, China

April 25, 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

Major Leader in Cyberspace Security

Associate Professor in College of Information and Intelligence Engineering

Ningbo, China

2022 – Present

2021 – Present

University of Science and Technology of China

Postdoctoral Researcher in Cyberspace Security (Hosted by Prof. Nenghai Yu)

Hefei, China

2019 – 2020

EDUCATION

University of Science and Technology of China

PH.D. & M.S. “Lattice-Based Cryptanalyses of RSA and Its Variants” Advisor: Prof. Honggang Hu

B.E. “The LLL Algorithm and Its Applications in Cryptography” Advisor: Prof. Honggang Hu

Hefei, China

2013 – 2018

2009 – 2013

The University of Tokyo

Visiting PH.D. “Security Analysis of RSA Using Lattice Reduction Algorithm” Advisor: Prof. Noboru Kunihiro

Tokyo, Japan

2016 – 2017

HONORS AND AWARDS

Zhejiang Province University Leading Talent Training Program

The Third Level – Young Talents

2022

Ningbo Leading Talent Training Project

The Third Level

2021

CSC Scholarship for Joint Doctoral Students

JPY 150 000 × 12

2016 – 2017

National Scholarship for Graduate Students

CNY 20 000

2015

FUNDING ACQUISITION

The National Natural Science Foundation of China

Grant No. 62002335, “Research on Cryptanalysis of RSA Type Algorithms Using Lattice-Based Method”

2021 – 2023

1/1

The National Natural Science Foundation of China

Grant No. 61972370, “Derandomization Problem Under Cryptographic Function and Branching Program Calculation Model”

2020 – 2023

2/8

Zhejiang Province Public Welfare Technology Application Research

Grant No. LGF22F020001, “Research and Application of Encrypted Machine Learning Using Multi-Party Fully Homomorphic Encryption”

2022 – 2024

2/6

Ningbo Natural Science Foundation

Grant No. 2021J174, “Design and Analysis of Efficient Post-Quantum Cryptographic Algorithms Based on Mersenne Prime”

2022 – 2023

1/5

PUBLICATIONS

Journal Articles

- **Mengce Zheng**, Zhigang Chen, Yaohui Wu. Solving Generalized Bivariate Integer Equations and Its Application to Factoring With Known Bits. *IEEE Access* 11: 34674–34684 (2023).
- **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).

Mengce Zheng

+86 15156053155

mengce.zheng@gmail.com

No. 8 Qianhu South Road, Ningbo, Zhejiang, China

April 25, 2023

<https://mengcezheng.github.io>

- 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

The 18th International Conference on Cryptology And Network Security

Fuzhou, China

Oct. 2019

Implicit-Key Attack on the RSA Cryptosystem

The 2nd International Conference on Science of Cyber Security

Nanjing, China

Aug. 2019

Cryptanalysis of RSA Variants with Modified Euler Quotient

The 10th International Conference on the Theory and Applications of Security and Cryptography

Marrakesh, Morocco

May 2018

Improved Factoring Attacks on Multi-prime RSA with Small Prime Difference

The 22nd Australasian Conference on Information Security and Privacy

Auckland, New Zealand

Jul. 2017

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