Mengce Zheng

+86 15156053155
mengce.zheng@gmail.com

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

January 6, 2026
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**
Associate Professor & Major Leader in Cyberspace Security	2021.01 – Present
University of Science and Technology of China	**Hefei, China**
Postdoctoral Researcher in Cyberspace Security	2018.12 – 2020.12

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	2013.09 – 2018.11
B.E. "The LLL Algorithm and Its Applications in Cryptography" Advisor: Prof. Honggang Hu	2009.09 – 2013.07
The University of Tokyo	**Tokyo, Japan**
Visiting PH.D. "Security Analysis of RSA Using Lattice Reduction Algorithm" Advisor: Prof. Noboru Kunihiro	2016.10 – 2017.09

HONORS AND AWARDS

CSC Scholarship for Visiting Scholars	**2023**
EUR $1\,350 \times 12$	
Zhejiang Province University Leading Talent Training Project	**2022**
The Third Level – Young Talents	
Ningbo Leading Talent Training Project	**2021**
The Third Level	
CSC Scholarship for Joint Doctoral Students	**2016**
JPY $150\,000 \times 12$	
National Scholarship for Graduate Students	**2015**
CNY $20\,000$	

FUNDING ACQUISITION

Ningbo Youth Science and Technology Innovation Leading Talent	**2023.07 – 2025.06**	
Grant No. 2023QL007, "Research on Post-Quantum Cryptography and Security Protocols for Quantum Secure Communication Network"		1/1
Ningbo Natural Science Foundation	**2022.01 – 2023.12**	
Grant No. 2021J174, "Design and Analysis of Efficient Post-Quantum Cryptographic Algorithms Based on Mersenne Prime"		1/5
Zhejiang Natural Science Foundation	**2022.01 – 2024.12**	
Grant No. LGF22F020001, "Research and Applications of Secret Machine Learning Based on Multi-Party Fully Homomorphic Encryption"		2/6
The National Natural Science Foundation of China	**2021.01 – 2023.12**	
Grant No. 62002335, "Research on Cryptanalysis of RSA Type Algorithms Using Lattice-Based Method"		1/1
The National Natural Science Foundation of China	**2020.01 – 2023.12**	
Grant No. 61972370, "Derandomization Problem Under Cryptographic Function and Branching Program Calculation Model"		2/8

PUBLICATIONS

Journal Articles

- **Mengce Zheng**. New lattice-based partial key exposure attacks on common prime RSA. *Journal of Cryptographic Engineering* 15, 19 (2025).
- Fan Huang, Xiaolin Duan, Chengcong Hu, **Mengce Zheng**, Honggang Hu. MulLeak: Exploiting Multiply Instruction Leakage to Attack the Stack-optimized Kyber Implementation on Cortex-M4. *IACR Transactions on Cryptographic Hardware and Embedded Systems* 2025(2), 23–68 (2025).
- **Mengce Zheng**, Hao Kang. Lattice-based cryptanalysis of RSA-type cryptosystems: a bibliometric analysis. *Cybersecurity* 7: 74 (2024).
- **Mengce Zheng**. Revisiting RSA-polynomial problem and semiprime factorization. *Theoretical Computer Science* 1004: 114634 (2024).
- **Mengce Zheng**. Revisiting Small Private Key Attacks on Common Prime RSA. *IEEE Access* 12: 5203–5211 (2024).
- **Mengce Zheng**. Generalized implicit-key attacks on RSA. *Journal of Information Security and Applications* 77: 103562 (2023).
- **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).
- **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

- Michel Seck, Oumar Niang, Djiby Sow, Abderrahmane Nitaj, **Mengce Zheng**, Maher Boudabra. A New Generalized Attack on RSA-like Cryptosystems. In: *AFRICACRYPT* 2025.
- **Mengce Zheng**, Abderrahmane Nitaj. A Novel Partial Key Exposure Attack on Common Prime RSA. In: *AFRICACRYPT* 2025.
- **Mengce Zheng**, Yansong Feng, Abderrahmane Nitaj, Yanbin Pan. Improving RSA Cryptanalysis: Combining Continued Fractions and Coppersmith's Techniques. In: *ACISP* 2025.
- Hao Kang, **Mengce Zheng**. Generalized Cryptanalysis of Cubic Pell RSA. In: *Inscrypt* 2024.
- **Mengce Zheng**, Wei Yan. Improved Lattice-Based Attack on Mersenne Low Hamming Ratio Search Problem. In: *ACISP* 2024.
- **Mengce Zheng**. Partial Key Exposure Attack on Common Prime RSA. In: *Inscrypt* 2023.
- Yukun Cheng, **Mengce Zheng**, Fan Huang, Jiajia Zhang, Honggang Hu, Nenghai Yu. A Fast-Detection and Fault-Correction Algorithm against Persistent Fault Attack. In: *TrustCom* 2021.
- Zhimin Luo, **Mengce Zheng**, Ping Wang, Minhui Jin, Jiajia Zhang, Honggang Hu. Towards Strengthening Deep Learning-based Side Channel Attacks with Mixup. In: *TrustCom* 2021.
- **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.
- **Mengce Zheng**, Noboru Kunihiro, Honggang Hu. Improved Factoring Attacks on Multi-prime RSA with Small Prime Difference. In: *ACISP* 2017.

PRESENTATIONS

A Novel Partial Key Exposure Attack on Common Prime RSA   **Rabat, Morocco**
The 16th International Conference on the Theory and Applications of Security and Cryptography   2025.07

Improving RSA Cryptanalysis: Combining Continued Fractions and Coppersmith's Techniques   **Wollongong, Australia**
The 30th Australasian Conference on Information Security and Privacy   2025.07

Generalized Cryptanalysis of Cubic Pell RSA   **Kunming, China**
The 20th International Conference on Information Security and Cryptology   2024.12

Improved Lattice-Based Attack on Mersenne Low Hamming Ratio Search Problem   **Sydney, Australia**
The 29th Australasian Conference on Information Security and Privacy   2024.07

Implicit Related-Key Factorization Problem on the RSA Cryptosystem   **Fuzhou, China**
The 18th International Conference on Cryptology and Network Security   2019.10

Implicit-Key Attack on the RSA Cryptosystem   **Nanjing, China**
The 2nd International Conference on Science of Cyber Security   2019.08

Cryptanalysis of RSA Variants with Modified Euler Quotient   **Marrakesh, Morocco**
The 10th International Conference on the Theory and Applications of Security and Cryptography   2018.05

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

Auckland, New Zealand

The 22nd Australasian Conference on Information Security and Privacy

2017.07

Teaching

Advanced Cryptography	Fall 2024
Cryptography Theory and Technology & Advanced Cryptography	Spring 2024
Blockchain Theory and Technology & Information Security Design and Practice	Fall 2023
Advanced Cryptography	Spring 2023
Data Structures and Algorithms	Fall 2022
Cybersecurity Theory and Technology	Spring 2022
Data Structures and Algorithms	Fall 2021
Cybersecurity Theory and Technology	Spring 2021