Jinwei Zheng

jinwei.zheng@telecom-paris.fr · 91120, Palaiseau, France

Academic Interests

- ***Post-Quantum Cryptography***,
  Widely interested in fundamental hardness of lattice problem, lattice-based constructions, lattice analysis.

- ***Quantum Cryptography***,
  Widely interested in Quantum protocal construction and Quantum analysis;

- Always open to exploring new research directions.

Education

Télécom Paris, Institut Polytechnique de Paris, Palaiseau, France — Jan. 2024 – Present

- ***Degree***: Ph. D Expected
- ***Supervisors***: Prof. Duong Hieu Phan and Weiqiang Wen
- ***Major***: Cryptography

Chinese Academy of Science (CAS), Beijing, China — Sep. 2020 – Jun. 2023

- ***Institute***: Academy of Mathematics and System Science (AMSS)
- ***Degree***: Master of Sciences
- ***Supervisor***: Prof. Yanbin Pan
- ***Major***:
  Cryptography, Applied Mathematics, supervised by Yanbin Pan — Sep. 2021 – Jun. 2023
  Number Theory, Pure Mathematics, supervised by Yongquan Hu — Sep. 2020 – Sep. 2021
- ***Thesis***: Construction and Analysis on Schemes based on NTRU. (in Chinese)

Soochow University, Soochow, China — Sep. 2016 – Jun. 2020

- ***School***: School of Mathematical Sciences
- ***Degree***: Bachelor of Sciences
- ***Major***: Pure Mathematics
- ***Thesis***: Construction of Semi-Stable p-adic Representations. (in Chinese)

Publications and Preprints

- ***Entropic Hardness of Ring Learning with Errors, Revisited***,
  with Weiqiang Wen,
  under submission.
  - We refine the original reduction for the standard hardness of RLWE with entropic secrets, as compared with the approach of [Brakerski, Döttling, TCC 2020]. Our new reduction establishes standard hardness under improved parameters, allowing both smaller error and smaller modulus.
  - Our new proof method provides a new way to construct CCA-secure public-key encryption schemes based on RLWE, and potentially broadens the applicability of the sometimes-lossiness technique for RLWE.

- ***Module Learning With Errors and Structured Extrapolated Dihedral Cosets***,
  with Weiqiang Wen,
  accepted by Crypto 2026. [pdf]

- Inspired by the equivalence between LWE and EDCP in [Brakerski, Kirshanova, Stehlé and Wen, PKC 2018], we show that the MLWE problem is as hard as a variant of EDCP, which we refer to as the structured EDCP (stEDCP). This extension from EDCP to stEDCP relies crucially on the algebraic structure of the ring underlying MLWE: the extrapolation depends not only on the noise rate, but also on the ring's degree.
- We also present a reduction from stEDCP to EDCP. Therefore, to analyze the quantum hardness of MLWE, it may be advantageous to study stEDCP, which might be easier than EDCP.

- ***Zero-Knowledge Proofs of Quantumness***,
  with Duong Hieu Phan, Weiqiang Wen and Xingyu Yan,
  published on IACR Communications in Cryptology 1(4). [pdf]
  - This work introduces zero-knowledge proofs of quantumness (ZKPoQ), which prevent a malicious classical verifier from exploiting the quantum prover beyond verifying its quantum capability. It also shows that representative existing PoQ schemes, including factoring-based and NTCF-based constructions, can be upgraded to satisfy this stronger security notion.

- ***Adaptive Hardcore Bit and Quantum Key Leasing over Classical Channel from LWE with Polynomial Modulus***,
  with Duong Hieu Phan, Weiqiang Wen and Xingyu Yan,
  published on Asiacrypt 2024.[pdf]
  - This work constructs a noisy trapdoor claw-free functions (NTCF) family with the adaptive hardcore bit property from LWE with polynomial modulus. This removes the superpolynomial-modulus requirement in the previous approach of [Brakerski, Christiano, Mahadev, Vazirani, Vidick, FOCS 2018], which has been widely used in quantum protocol constructions. Directly, this implies a proof of quantumness protocol solely based on LWE with polynomial modulus.
  - Building on this improved NTCF family, this work improves the previous PKE-SKL construction over classical channels [Chardouvelis, Goyal, Jain, Liu, Eurocrypt 2025] by replacing the reliance on superpolynomial-modulus LWE with polynomial-modulus LWE. This yields a more efficient and better-parameterized construction while preserving the same classical-communication setting.

- ***Compact Encryption based on Module-NTRU problems***,
  with Shi Bai, Hansraj Jangir, Hao Lin, Tran Ngo, Weiqiang Wen,
  published on PQCrypto 2024. [pdf]
  - This work constructs compact lattice-based encryption schemes from the Module-NTRU problem and its vectorial variant, leveraging the module structure to obtain more flexible parameter choices. The resulting schemes achieve competitive ciphertext sizes for NIST security Levels 1, 3, and 5, namely about 614, 921, and 1228 bytes, respectively, with small decryption failure and without requiring specialized plaintext encoding or decoding.

- ***Polynomial-Time Key-Recovery Attacks against NTRUReEncrypt from ASIACCS'15***,
  with Zhen Liu and Yanbin Pan,
  published on J. Syst. Sci. Complex. 37(3): 1308-1325 (2024). [pdf]
  - This work gives polynomial-time key-recovery attacks against the NTRU-based proxy re-encryption scheme NTRUReEncrypt, showing that the delegator and delegatee can efficiently recover each other's private keys from ciphertext and re-encrypted ciphertext pairs. It also proposes a modified re-encryption procedure to resist these attacks.

PRESENTATIONS

- ***Module Learning With Errors and Structured Extrapolated Dihedral Coset***
  - August 2026 (coming soon): Crypto (conference) - Santa Barbara, United States;
  - June 2026: Télécom Crypto Day(seminar) - Palaiseau, France;

- May 2026: Journée Scientifique SecureCompute (workshop) - Paris, France.

- ***Adaptive Hardcore Bit and Quantum Key leasing over Classical Channel from LWE with Polynomial Modulus***[slides]
  - June 2025: PEPR Seminar - Paris, France;
  - April 2025: Journée C2 (workshop) - Pornichet, France;
  - January 2025: HCERES Seminar (Poster Presentation) - Palaiseau, France;
  - December 2024: Asiacrypt2024 (conference) - Calcutta, India.

SERVICE

- **External Reviewer:**
  STOC 2026 · TQC 2026 · CIC 2026 · Crypto 2026 · DCC 2026
  JoC 2025
  TCC 2024 · Crypto 2024 · ACISP 2024

TEACHING

- **Autumn Term 2025/26**
  TA: Quantique: architecture, programmation et cryptographie (Prof. Sébastien Canard)

HONORS AND AWARDS

- Merit Student, **AMSS, CAS** Jun. 2022
- Outstanding Graduate, **Soochow University** Jun. 2020
- Special Innovation and Entrepreneurship Scholarship, **Soochow University** Aug. 2019
- First prize, **National College Students Mathematics Competition** Oct. 2017
- Second Prize, **National Undergraduate Mathematical Contest in Modeling (China)** Nov. 2017