Post-Quantum Cryptography (PQC) in China and the Development of PQC in Tongsuo

Yuchen Wang

Ant Group

October 9, 2025

Table of Contents

PQC in China

- Academic research
  - Novel PQC signatures and KEMs
  - Attacks, post-quantum protocols and security reductions
- NIST's PQC standardization process
  - Jintai Ding (Xi'an Jiaotong-Liverpool University) co-invented ML-KEM
  - Ding also co-invented Rainbow $\Rightarrow$ NIST PQC Project finalists, SNOVA and UOV $\Rightarrow$ NIST Call for Additional Signatures round 2
  - A team predominantly affiliated with IIE, CAS invented LAC $\Rightarrow$ NIST PQC Project round 2 (first author: Xianhui Lu)

PQC in China

- PQC competitions
  - The National Cryptographic Algorithm Design Competition, 2018
  - Next-generation Commercial Cryptographic Algorithms Program (NGCC), 2025
- PQC implementations and commercial products
  - Open source libraries: Tongsuo, OpenHiTLS and PQMagic
  - Chip, Hardware Cryptographic Module (HSM) and Key Management System (KMS)

PQC in China - Academic Research

PQC in China: Academic Research

- Recent work since 2018
- First or corresponding author with China affiliation
- Focus on new designs of KEMs and signatures, also with:
  - Attacks on NIST PQC proposals
  - Post-quantum protocols
  - Improvements of security reductions

PQC Research in China: KEMs (1)

- On lattice assumptions
  - LAC [Lu+18]: NIST PQC competition
  - AIGIS-Enc [Zha+20]: PKC 2020
  - BAT [Fou+22]: TCHES 2022
  - CTRU/CNTR [Lia+24]: Computer Standards & Interfaces 2024
  - NEV [ZFY23]: ASIACRYPT 2022
  - SCloud+ [Wan+24]: SSR 2024
- On other assumptions
  - SIAKE [Xu+19]: ASIACRYPT 2019
  - NH-ROLLO [Son+23]: ASIACRYPT 2023

PQC Research in China: KEMs (2)

- [Lu+18] *LAC: Practical Ring-LWE Based Public-Key Encryption with Byte-Level Modulus*
  - Based on the Ring-LWE (RLWE) assumption
- AIGIS-Enc [Zha+20] *Tweaking the Asymmetry of Asymmetric-Key Cryptography on Lattices: KEMs and Signatures of Smaller Sizes*
  - Based on the Asymmetric Module-LWE (AMLWE) assumption
  - 1.01x ~1.31x (resp., 1.14x ~1.36x) faster than Kyber in encapsulation (resp., decapsulation)

	NIST-I		NIST-III		NIST-V	
	|pk|	|ct|	|pk|	|ct|	|pk|	|ct|
LAC	544	704	1056	1352	1056	1464
AIGIS-Enc	672	672	896	992	1472	1536
kyber[1]	800	768	1184	1088	1568	1568

[1] We follow the parameter sets specified by NIST FIPS 203

PQC Research in China: KEMs (3)

- [Fou+22] *BAT: Small and Fast KEM over NTRU Lattices*
  - Based on NTRU and RLWR assumptions.
  - Fast encapsulation of ~11k cycles with AVX2
- [ZFY23] *NEV: Faster and Smaller NTRU Encryption using Vector Decoding*
  - Based on NTRU and RLWE assumptions
  - 1.42x ~1.74x faster than Kyber, 5.03x ~29.94x faster than NTRU-HRSS/HPS
- CTRU/CNTR [Lia+24] *Compact and Efficient KEMs over NTRU Lattices*
  - Based on NTRU and RLWE/RLWR assumptions
  - 1.2x~2.6x faster than Kyber, 1.6x ~23x faster than NTRU-HRSS

PQC Research in China: KEMs (4)

	NIST-I		NIST-III		NIST-V	
	|pk|	|ct|	|pk|	|ct|	|pk|	|ct|
BAT	521	473	-	-	1230	1006
NEV	615	615	-	-	1229	1229
CTRU	768	640	1152	960	1536	1408
CNTR	768	640	1152	960	1536	1280
kyber	800	768	1184	1088	1568	1568
NTRU-HRSS[2]	1138	1138	-	-	2401	2401
NTRU-HPS	930	930	1230	1230	1842	1842

[2]For NTRU-HRSS/HPS, we follow the parameter sets specified by draft-fluhrer-cfrg-ntru-03

PQC Research in China: KEMs (5)

- [Wan+24] *Scloud+: An Efficient LWE-Based KEM Without Ring/Module Structure*
  - Based on unstructured LWE problem
  - 1.29x~1.36x faster than FrodoKEM [Bos+16] in encap+decap

	NIST-I		NIST-III		NIST-V	
	|pk|	|ct|	|pk|	|ct|	|pk|	|ct|
Scloud+	7200	5456	11136	10832	18744	16916
FrodoKEM	9616	9720	15632	15744	21520	21632
kyber	800	768	1184	1088	1568	1568
HQC	2249	4497	4522	9042	7245	14485

PQC Research in China: KEMs (6)

- SIAKE [Xu+19] *Strongly Secure Authenticated Key Exchange from Supersingular Isogenies*
  - One-Way CCA KEM based on SI-DDH assumption
  - 2/3-pass AKE protocols based on SI-DDH/One-Oracle SIDH
- NH-ROLLO [Son+23] *Blockwise Rank Decoding Problem and LRPC Codes: Cryptosystems with Smaller Sizes*
  - Rank-based crypto: (More-efficient) code-based crypto relies on rank metric rather than Hamming metric (e.g., HQC)
  - Generic coding technologies that improve the communication costs of rank-based KEMs in NIST PQC competition up to 50%.

PQC Research in China: Signatures (1)

- Lattice-based
  - AIGIS-Sig [Zha+20]: PKC 2020
  - Mitaka: EUROCRYPT 2022 [Esp+22a], CRYPTO 2022 [Esp+22b]
  - Robin, Eagle and Hufu [YJW23]: CRYPTO 2023
- Hash-based
  - SPHINCs-α [ZCY23]: CRYPTO 2023

PQC Research in China: Signatures (2)

- AIGIS-Sig [Zha+20] *Tweaking the Asymmetry of Asymmetric-Key Cryptography on Lattices: KEMs and Signatures of Smaller Sizes*
  - Sign is 1.01x ~1.46x faster than Dilithium
- [Esp+22a] *MITAKA: A Simpler, Parallelizable, Maskable Variant of Falcon*
  - Sign is 2.02x ~2.32x faster than Falcon
- [Esp+22b] *Shorter Hash-and-Sign Lattice-Based Signatures*
  - More compact Falcon and Mitaka with ellipsoidal Gaussian distribution and reduced modulus
  - At the cost a few bits of security

PQC Research in China: Signatures (3)

- Robin & Eagle [YJW23] *Compact Lattice Gadget and Its Applications to Hash-and-Sign Signatures*
  - A series of post-quantum signature schemes with lattice gadgets
  - Robin: the instantiation based on NTRU without NTRU trapdoor
  - Eagle: the instantiation based on RLWE
- Hufu: the proposal submitted to NIST competition for additional signatures
  - A LWE-based signature with the compact gadget technique

PQC Research in China: Signatures (4)

	NIST-I		NIST-III		NIST-V	
	|pk|	|sig|	|pk|	|sig|	|pk|	|sig|
AIGIS-Sig	1056	1852	1568	3046	-	-
Mitaka	896	713	-	-	1792	1405
Robin	1227	992	1990	1527	2399	1862
Eagle	-	-	1952	3052	-	-
Hufu	1059	2455	2177	3540	3573	4520
Falcon[3]	576	425	-	-	1152	805
Falcon[4]	896	410	-	-	1792	780
Mitaka[3]	576	475	-	-	1152	935
Mitaka[4]	896	460	-	-	1792	905
Dilitihum[5]	-	-	1952	3309	2952	4627
Falcon	896	666	-	-	1792	1280

[3]The variant of $q = 257$ by [Esp+22b]

[4]The variant of $\gamma = 8$ by [Esp+22b]

[5]For Dilitihum, we follow the parameter sets specified by NIST FIPS 204

PQC Research in China: Signatures (5)

- SPHINCS-α [ZCY23] *Revisiting the Constant-Sum Winternitz One-Time Signature with Applications to SPHINCS+ and XMSS*
  - Prove that the constant-sum WOTS$^+$ one-time signature is size-optimal among all tree-based OTS

	NIST-I		NIST-III		NIST-V	
	128-f	128-s	192-f	192-s	256-f	256-s
SPHINCS+	17088	7856	35664	16224	49856	29792
SPHINCS-α	16720	6880	34896	14568	49312	27232

PQC Research in China: Attacks (1)

- [Din+21] *The Nested Subset Differential Attack: A Practical Direct Attack Against LUOV Which Forges a Signature Within 210 Minutes* (EUROCRYPT'21)
  - Forge a signature with public key, against LOUV (NIST PQC Project round 2)
- [WWW23] *Exploring Decryption Failures of BIKE: New Class of Weak Keys and Key Recovery Attacks* (CRYPTO'23)
  - Decrease the security level of BIKE (NIST PQC Project round 4) with new key recovery attacks
- [Zha+23] *Improved Power Analysis Attacks on Falcon* (EUROCRYPT'23)
  - Practical key-recovery side-channel attacks of Falcon's samplers

PQC Research in China: Attacks (2)

- [Lin+25] *Do Not Disturb a Sleeping Falcon: Floating-Point Error Sensitivity of the Falcon Sampler and Its Consequences* (EUROCRYPT'25)
  - Identify a vulnerability in Falcon's lattice discrete Gaussian sampler, which can be used to attack deterministic Falcon
- [Lia+25] *Achilles: A Formal Framework of Leaking Secrets from Signature Scheme via RowHammer* (USENIX Security'25)
  - RowHammer checking tools for signatures including ML-DSA

PQC Research in China: Protocols

- [Bai+24] *MPC-in-the-Head Framework without Repetition and its Applications to the Lattice-based Cryptography* (S&P'24)
  - Efficient non-interactive proof-of-possession of lattice key (e.g., for MLKEM-512, ~80 KB proof and <1s verification time).
- [ZJZ24] *CPA-secure KEMs are also sufficient for Post-Quantum TLS 1.3* (ASIACRYPT'24)
  - Improves the proofs of [HV22] (EUROCRYPT'22) with tighter bounds in the Quantum ROM (QROM).
- [LLH24a] *Efficient Asymmetric PAKE Compiler from KEM and AE* (ASIACRYPT'24)
- [LLH24b] *Universal Composable Password Authenticated Key Exchange for the Post-Quantum World* (EUROCRYPT'24)
  - Generic constructions UC-secure (asymmetric)-PAKE and instantiations with LWE and GA-DDH

PQC Research in China: Security Proofs of KEMs

- The line of research [Jia+18; JZM21; GSX23; JMZ23; Che+24; GLX24]
  - Improve the security proofs of FO transofrmation (IND-CPA PKE $\rightarrow$ IND-CCA KEM)
  - Tighter proofs with less security loss (e.g, $\mathcal{O}(q^2) \rightarrow \mathcal{O}(1)$)
  - Security proofs in the Quantum ROM rather than classical ROM
  - Can be used to optimize the choices of parameters
- [Zho+24] *SoK: Post-Quantum Key Encapsulation Mechanisms — Security Definitions, Constructions, and Applications* (SSR'24)
  - A detailed survey on this topic

PQC Standard in China: Current Standard (1)

- The hierarchy of cryptographic standards in China
- The GM/T (GuoMi for "National Cryptography") Series
  - Published by the State Cryptography Administration (SCA)
  - National industry standards for cryptographic algorithms
- The GB/T (GuoBiao for "National Standard") Series
  - Published by the Standardization Administration of China (SAC)
  - Mature and important GM/T standards can be "promoted" to GB/T standards
  - e.g., SM3 hash algorithm: GM/T 0004-2012 $\Rightarrow$ GB/T 32905-2016

PQC Standard in China: Current Standard (2)

- Asymmetric algorithms: the SM2 standard
  - ”ShangMi” stands for ”cryptographic algorithms for commercial usage”.
  - GM/T 0003-2012 or GB/T 32918-2016
  - Part 1: General notions for elliptic curve cryptography.
  - Part 2: Digital signature
  - Part 3: Key exchange protocol
  - Part 4: Public key encryption
  - Part 5: Parameter definition


ICS 35.040
L 80
备案号：36826—2012

GM

中华人民共和国密码行业标准

GM/T 0003.1—2012

SM2 椭圆曲线公钥密码算法
第 1 部分：总则

Public key cryptographic algorithm SM2 based on elliptic curves—
Part 1: General

2012-03-21 发布　　2012-03-21 实施

国家密码管理局　发布

PQC Standard in China: Current Standard (3)

- Details of SM2 standard
- SM2 signature
  - Different from ECDSA $\Rightarrow$ has been incorporated into ISO/IEC 14888-3
  - SM2 signature is resistant to key substitution attacks (where DSA/ECDSA cannot)
  - [Zha+15] *Security of the SM2 Signature Scheme Against Generalized Key Substitution Attacks* (SSR'15)
- SM2 key exchange
  - SM2 key exchange is a MQV-style protocol
- SM2 parameter
  - Part 5 also specifies a new curve (a.k.a., "SM2Curve")

PQC Standard in China: Post-Quantum Competition (1)

- The National Cryptographic Algorithm Design Competition 2018
  - Public key track: PKE/KEM, key exchange and signature
  - Encourage post-quantum designs
- First Prize:
  - AIGIS-sig, LAC.PKE and AIGIS-enc
- Second Prize:
  - LAC.KEX, SIAKE, Scloud and AKCN
  - AKCN [JZ17] *Optimal Key Consensus in Presence of Noise*

PQC Standard in China: Post-Quantum Competition (2)

- Announcement on Launching the Next-generation Commercial Cryptographic Algorithms Program (NGCC) by Feb, 2025
  - Global-wide competition hold by Institute of Commercial Cryptography Standards (ICS)
  - For public key algorithms, hash algorithms and block ciphers, require post-quantum security

Home > Notice

Announcement on Launching the Next-generation Commercial Cryptographic Algorithms Program (NGCC)

2025-02-05

Font size: Big Middle Small

In response to the threat of quantum computing and to promote the standardization of the next-generation commercial cryptographic algorithms, the Institute of Commercial Cryptography Standards (ICCS) is launching a global program to call for proposals for next-generation public-key cryptographic algorithms (NGCC-PK), cryptographic hash algorithms (NGCC-CH) and block cipher algorithms (NGCC-BC), according to the arrangement of Chinese Cryptography Standardization Technical Committee. The candidate algorithms will be evaluated in terms of security, performance and other features, and the finalists will be considered for standardization. ICCS looks forward to global algorithm submissions and comments, and encourages international cooperations in algorithm design.

Further notifications of the program will be released on www.nccc.org.cn

Institute of Commercial Cryptography Standards, China

February 5, 2025

PQC in China: Open Source Libraries

- Tongsuo (https://github.com/Tongsuo-Project/Tongsuo)
  - China local fork of OpenSSL
  - Currently supported post-quantum features: SM2DH-MLKEM768 hybrid key exchange for TLS 1.3 and ML-DSA
- OpenHiTLS (https://github.com/openHiTLS/openHiTLS)
  - Supported post-quantum algorithms: ML-DSA, ML-KEM, SLH-DSA and SCloud+
  - Support the hybrid key exchange methods described in draft-kwiatkowski-tls-ecdhe-mlkem-03.
- PQMagic (https://github.com/pqcrypto-cn/PQMagic)
  - High-performance post-quantum cryptographic implementations
  - ML-DSA, ML-KEM, SLH-DSA, AIGIS and SPHINCS-α

PQC in China: Chip, HSM and KMS (1)

- Many China companies are developing servers, HSMs and chips for post-quantum algorithms
- Mainly support NIST standards and post-quantum RNG
- Post-quantum crypto chips
  - C*Core (GuoXin) Technology Co.,Ltd's CCUPHPQ01.
  - TuringQ (Tuling Liangzi)'s TQ03-QRNGC-64
  - Anhui ASKY Quantum (Wentian Liangzi) Technology's chip-level post-quantum crypto card

PQC in China: Chip, HSM and KMS (2)

- HSMs, gateways, and key/certificate management systems
  - sansec (SanWei Xinan)'s post-quantum crypto hardware cryptographic module (HSM), SDK and key/certificate management systems.
  - CETC (China Electroics Technology Group Corporation) has published "LiangKai" post-quantum cryptographic product series.
  - Aliyun's GVSM post-quantum cryptogrphic server (beta): supports ML-KEM, ML-DSA, SLH-DSA, LMS and XMSS.

Tongsuo's Implementation of PQC

Tongsuo's Implementation of PQC

Tongsuo's Implementation of PQC: Current status

- Post-quantum features in current Tongsuo master
- Hybrid key exchange SM2DH-MLKEM768 for TLS 1.3
  - Combines ECDHE with SM2Curve and MLKEM768
  - Adopts the MLKEM reference implementation from the design team (pq-crystals)
- ML-DSA and hybrid signature with SM2 and MLDSA-65
  - The hybrid design follows the specification of draft-ietf-lamps-pq-composite-sigs-07
  - Adopts the MLDSA reference implementaion (also, from pq-crystals)

Tongsuo's Implementation of PQC

Tongsuo's Implementation of PQC: Roadmap (1)

- Goal 1: support more post-quantum features
  - NIST's standard algorithms: ML-DSA, ML-KEM and SLH-DSA
  - Experimentally support non-standardized Algorithms
- Goal 2: explore pathways for integrating PQC into China's standards
  - Hybrid with GM/T cryptographic altorithm standards
  - e.g., GB/T 32907-2016: the SM4 block cipher
  - The applications of post-quantum/hybrid primitives in China's standards of protocols
  - e.g., GB/T 38636-2020: Transport Layer Cryptography Protocol (TLCP), which is a TLS-1.2 style protocol

Tongsuo's Implementation of PQC: Roadmap (2)

- Goal 3: optimize performance for post-quantum algorithms
  - With specific hardware features (e.g., AVX, ARM64, RISC-V,$\cdots$)
- Goal 4: support more post-quantum features
  - Distributed key management
  - Side-channel resistant implementation
  - Acclerate high-impact PQC research
- We are expecting more suggestions and PRs!

The End

https://github.com/Tongsuo-Project/Tongsuo

tianwu.wyc@antgroup.com

References I

[Bai+24] Weihao Bai et al. “MPC-in-the-Head Framework without Repetition and its Applications to the Lattice-based Cryptography”. In: *IEEE Symposium on Security and Privacy, SP 2024, San Francisco, CA, USA, May 19-23, 2024*. IEEE, 2024, pp. 578–596.

[Bos+16] Joppe W. Bos et al. “Frodo: Take off the Ring! Practical, Quantum-Secure Key Exchange from LWE”. In: *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, Vienna, Austria, October 24-28, 2016*. Ed. by Edgar R. Weippl et al. ACM, 2016, pp. 1006–1018.

[Che+24] Jinrong Chen et al. “Tighter Proofs for PKE-to-KEM Transformation in the Quantum Random Oracle Model”. In: *Advances in Cryptology - ASIACRYPT 2024 - 30th International Conference on the Theory and Application of Cryptology and Information Security, Kolkata, India, December 9-13, 2024, Proceedings, Part IV*. Ed. by Kai-Min Chung and Yu Sasaki. Vol. 15487. Lecture Notes in Computer Science. Springer, 2024, pp. 101–133.

References II

[Din+21] Jintai Ding et al. “The Nested Subset Differential Attack - A Practical Direct Attack Against LUOV Which Forges a Signature Within 210 Minutes”. In: *Advances in Cryptology - EUROCRYPT 2021 - 40th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Zagreb, Croatia, October 17-21, 2021, Proceedings, Part I*. Ed. by Anne Canteaut and François-Xavier Standaert. Vol. 12696. Lecture Notes in Computer Science. Springer, 2021, pp. 329–347.

[Esp+22a] Thomas Espitau et al. “Mitaka: A Simpler, Parallelizable, Maskable Variant of Falcon”. In: *Advances in Cryptology - EUROCRYPT 2022 - 41st Annual International Conference on the Theory and Applications of Cryptographic Techniques, Trondheim, Norway, May 30 - June 3, 2022, Proceedings, Part III*. Ed. by Orr Dunkelman and Stefan Dziembowski. Vol. 13277. Lecture Notes in Computer Science. Springer, 2022, pp. 222–253.

References III

[Esp+22b] Thomas Espitau et al. “Shorter Hash-and-Sign Lattice-Based Signatures”. In: *Advances in Cryptology - CRYPTO 2022 - 42nd Annual International Cryptology Conference, CRYPTO 2022, Santa Barbara, CA, USA, August 15-18, 2022, Proceedings, Part II*. Ed. by Yevgeniy Dodis and Thomas Shrimpton. Vol. 13508. Lecture Notes in Computer Science. Springer, 2022, pp. 245–275.

[Fou+22] Pierre-Alain Fouque et al. “BAT: Small and Fast KEM over NTRU Lattices”. In: *IACR Trans. Cryptogr. Hardw. Embed. Syst.* 2022.2 (2022), pp. 240–265. DOI: 10.46586/TCHES.V2022.I2.240-265. URL: https://doi.org/10.46586/tches.v2022.i2.240-265.

References IV

[GLX24] Jiangxia Ge, Heming Liao, and Rui Xue. “Measure-Rewind-Extract: Tighter Proofs of One-Way to Hiding and CCA Security in the Quantum Random Oracle Model”. In: *Advances in Cryptology - ASIACRYPT 2024 - 30th International Conference on the Theory and Application of Cryptology and Information Security, Kolkata, India, December 9-13, 2024, Proceedings, Part IV*. Ed. by Kai-Min Chung and Yu Sasaki. Vol. 15487. Lecture Notes in Computer Science. Springer, 2024, pp. 3–34.

[GSX23] Jiangxia Ge, Tianshu Shan, and Rui Xue. “Tighter QCCA-Secure Key Encapsulation Mechanism with Explicit Rejection in the Quantum Random Oracle Model”. In: *Advances in Cryptology - CRYPTO 2023 - 43rd Annual International Cryptology Conference, CRYPTO 2023, Santa Barbara, CA, USA, August 20-24, 2023, Proceedings, Part V*. Ed. by Helena Handschuh and Anna Lysyanskaya. Vol. 14085. Lecture Notes in Computer Science. Springer, 2023, pp. 292–324.

References V

[HV22] Loïs Huguenin-Dumittan and Serge Vaudenay. “On IND-qCCA Security in the ROM and Its Applications - CPA Security Is Sufficient for TLS 1.3”. In: *Advances in Cryptology - EUROCRYPT 2022 - 41st Annual International Conference on the Theory and Applications of Cryptographic Techniques, Trondheim, Norway, May 30 - June 3, 2022, Proceedings, Part III*. Ed. by Orr Dunkelman and Stefan Dziembowski. Vol. 13277. Lecture Notes in Computer Science. Springer, 2022, pp. 613–642.

[Jia+18] Haodong Jiang et al. “IND-CCA-Secure Key Encapsulation Mechanism in the Quantum Random Oracle Model, Revisited”. In: *Advances in Cryptology - CRYPTO 2018 - 38th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 19-23, 2018, Proceedings, Part III*. Ed. by Hovav Shacham and Alexandra Boldyreva. Vol. 10993. Lecture Notes in Computer Science. Springer, 2018, pp. 96–125.

References VI

[JMZ23] Haodong Jiang, Zhi Ma, and Zhenfeng Zhang. “Post-quantum Security of Key Encapsulation Mechanism Against CCA Attacks with a Single Decapsulation Query”. In: *Advances in Cryptology - ASIACRYPT 2023 - 29th International Conference on the Theory and Application of Cryptology and Information Security, Guangzhou, China, December 4-8, 2023, Proceedings, Part IV*. Ed. by Jian Guo and Ron Steinfeld. Vol. 14441. Lecture Notes in Computer Science. Springer, 2023, pp. 434–468.

[JZ17] Zhengzhong Jin and Yunlei Zhao. “Optimal Key Consensus in Presence of Noise”. In: *IACR Cryptol. ePrint Arch.* (2017), p. 1058. URL: http://eprint.iacr.org/2017/1058.

References VII

[JZM21] Haodong Jiang, Zhenfeng Zhang, and Zhi Ma. “On the Non-tightness of Measurement-Based Reductions for Key Encapsulation Mechanism in the Quantum Random Oracle Model”. In: *Advances in Cryptology - ASIACRYPT 2021 - 27th International Conference on the Theory and Application of Cryptology and Information Security, Singapore, December 6-10, 2021, Proceedings, Part I*. Ed. by Mehdi Tibouchi and Huaxiong Wang. Vol. 13090. Lecture Notes in Computer Science. Springer, 2021, pp. 487–517.

[Lia+24] Zhichuang Liang et al. “Compact and efficient KEMs over NTRU lattices”. In: *Comput. Stand. Interfaces* 89 (2024), p. 103828. DOI: 10.1016/J.CSI.2023.103828. URL: https://doi.org/10.1016/j.csi.2023.103828.

[Lia+25] Junkai Liang et al. “Achilles: A Formal Framework of Leaking Secrets from Signature Schemes via Rowhammer”. In: *34thth USENIX Security Symposium, USENIX Security 2025, August 12-14, 2025*. USENIX Association, 2025.

References VIII

[Lin+25] Xiuhan Lin et al. “Do Not Disturb a Sleeping Falcon - Floating-Point Error Sensitivity of the Falcon Sampler and Its Consequences”. In: *Advances in Cryptology - EUROCRYPT 2025 - 44th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Madrid, Spain, May 4-8, 2025, Proceedings, Part II*. Ed. by Serge Fehr and Pierre-Alain Fouque. Vol. 15602. Lecture Notes in Computer Science. Springer, 2025, pp. 213–244.

[LLH24a] You Lyu, Shengli Liu, and Shuai Han. “Efficient Asymmetric PAKE Compiler from KEM and AE”. In: *Advances in Cryptology - ASIACRYPT 2024 - 30th International Conference on the Theory and Application of Cryptology and Information Security, Kolkata, India, December 9-13, 2024, Proceedings, Part V*. Ed. by Kai-Min Chung and Yu Sasaki. Vol. 15488. Lecture Notes in Computer Science. Springer, 2024, pp. 34–65.

References IX

[LLH24b] You Lyu, Shengli Liu, and Shuai Han. “Universal Composable Password Authenticated Key Exchange for the Post-Quantum World”. In: *Advances in Cryptology - EUROCRYPT 2024 - 43rd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Zurich, Switzerland, May 26-30, 2024, Proceedings, Part VI*. Ed. by Marc Joye and Gregor Leander. Vol. 14656. Lecture Notes in Computer Science. Springer, 2024, pp. 120–150. DOI: 10.1007/978-3-031-58754-2_5. URL: https://doi.org/10.1007/978-3-031-58754-2%5C_5.

[Lu+18] Xianhui Lu et al. “LAC: Practical Ring-LWE Based Public-Key Encryption with Byte-Level Modulus”. In: *IACR Cryptol. ePrint Arch.* (2018), p. 1009. URL: https://eprint.iacr.org/2018/1009.

References X

[Son+23] Yongcheng Song et al. “Blockwise Rank Decoding Problem and LRPC Codes: Cryptosystems with Smaller Sizes”. In: *Advances in Cryptology - ASIACRYPT 2023 - 29th International Conference on the Theory and Application of Cryptology and Information Security, Guangzhou, China, December 4-8, 2023, Proceedings, Part VII*. Ed. by Jian Guo and Ron Steinfeld. Vol. 14444. Lecture Notes in Computer Science. Springer, 2023, pp. 284–316.

[Wan+24] Anyu Wang et al. “Scloud$^+$: An Efficient LWE-Based KEM Without Ring/Module Structure”. In: *Security Standardisation Research - 9th International Conference, SSR 2024, Kunming, China, December 16, 2024, Proceedings*. Ed. by Xianhui Lu and Chris J. Mitchell. Vol. 15559. Lecture Notes in Computer Science. Springer, 2024, pp. 147–174.

References XI

[WWW23] Tianrui Wang, Anyu Wang, and Xiaoyun Wang. “Exploring Decryption Failures of BIKE: New Class of Weak Keys and Key Recovery Attacks”. In: *Advances in Cryptology - CRYPTO 2023 - 43rd Annual International Cryptology Conference, CRYPTO 2023, Santa Barbara, CA, USA, August 20-24, 2023, Proceedings, Part III*. Ed. by Helena Handschuh and Anna Lysyanskaya. Vol. 14083. Lecture Notes in Computer Science. Springer, 2023, pp. 70–100.

[Xu+19] Xiu Xu et al. “Strongly Secure Authenticated Key Exchange from Supersingular Isogenies”. In: *Advances in Cryptology - ASIACRYPT 2019 - 25th International Conference on the Theory and Application of Cryptology and Information Security, Kobe, Japan, December 8-12, 2019, Proceedings, Part I*. Ed. by Steven D. Galbraith and Shiho Moriai. Vol. 11921. Lecture Notes in Computer Science. Springer, 2019, pp. 278–308.

References XII

[YJW23] Yang Yu, Huiwen Jia, and Xiaoyun Wang. “Compact Lattice Gadget and Its Applications to Hash-and-Sign Signatures”. In: *Advances in Cryptology - CRYPTO 2023 - 43rd Annual International Cryptology Conference, CRYPTO 2023, Santa Barbara, CA, USA, August 20-24, 2023, Proceedings, Part V*. Ed. by Helena Handschuh and Anna Lysyanskaya. Vol. 14085. Lecture Notes in Computer Science. Springer, 2023, pp. 390–420.

[ZCY23] Kaiyi Zhang, Hongrui Cui, and Yu Yu. “Revisiting the Constant-Sum Winternitz One-Time Signature with Applications to SPHINCS$^+$ and XMSS”. In: *Advances in Cryptology - CRYPTO 2023 - 43rd Annual International Cryptology Conference, CRYPTO 2023, Santa Barbara, CA, USA, August 20-24, 2023, Proceedings, Part V*. Ed. by Helena Handschuh and Anna Lysyanskaya. Vol. 14085. Lecture Notes in Computer Science. Springer, 2023, pp. 455–483.

References XIII

[ZFY23] Jiang Zhang, Dengguo Feng, and Di Yan. “NEV: Faster and Smaller NTRU Encryption Using Vector Decoding”. In: *Advances in Cryptology - ASIACRYPT 2023 - 29th International Conference on the Theory and Application of Cryptology and Information Security, Guangzhou, China, December 4-8, 2023, Proceedings, Part VII*. Ed. by Jian Guo and Ron Steinfeld. Vol. 14444. Lecture Notes in Computer Science. Springer, 2023, pp. 157–189.

[Zha+15] Zhenfeng Zhang et al. “Security of the SM2 Signature Scheme Against Generalized Key Substitution Attacks”. In: *Security Standardisation Research - Second International Conference, SSR 2015, Tokyo, Japan, December 15-16, 2015, Proceedings*. Ed. by Liqun Chen and Shin’ichiro Matsuo. Vol. 9497. Lecture Notes in Computer Science. Springer, 2015, pp. 140–153.

References XIV

[Zha+20] Jiang Zhang et al. “Tweaking the Asymmetry of Asymmetric-Key Cryptography on Lattices: KEMs and Signatures of Smaller Sizes”. In: *Public-Key Cryptography - PKC 2020 - 23rd IACR International Conference on Practice and Theory of Public-Key Cryptography, Edinburgh, UK, May 4-7, 2020, Proceedings, Part II*. Ed. by Aggelos Kiayias et al. Vol. 12111. Lecture Notes in Computer Science. Springer, 2020, pp. 37–65.

[Zha+23] Shiduo Zhang et al. “Improved Power Analysis Attacks on Falcon”. In: *Advances in Cryptology - EUROCRYPT 2023 - 42nd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Lyon, France, April 23-27, 2023, Proceedings, Part IV*. Ed. by Carmit Hazay and Martijn Stam. Vol. 14007. Lecture Notes in Computer Science. Springer, 2023, pp. 565–595.

References XV

[Zho+24] Biming Zhou et al. “SoK: Post-Quantum Key Encapsulation Mechanisms - Security Definitions, Constructions, and Applications”. In: *Security Standardisation Research - 9th International Conference, SSR 2024, Kunming, China, December 16, 2024, Proceedings*. Ed. by Xianhui Lu and Chris J. Mitchell. Vol. 15559. Lecture Notes in Computer Science. Springer, 2024, pp. 120–146.

[ZJZ24] Biming Zhou, Haodong Jiang, and Yunlei Zhao. “CPA-Secure KEMs are also Sufficient for Post-quantum TLS 1.3”. In: *Advances in Cryptology - ASIACRYPT 2024 - 30th International Conference on the Theory and Application of Cryptology and Information Security, Kolkata, India, December 9-13, 2024, Proceedings, Part III*. Ed. by Kai-Min Chung and Yu Sasaki. Vol. 15486. Lecture Notes in Computer Science. Springer, 2024, pp. 433–464.