International Journal of Software and Informatics, ISSN 1673-7288
http://www.ijsi.org, ijsi@iscas.ac.cn, +86-10-62661048
IJSI, 2025, 15(4): 397–399, doi: 10.21655/ijsi.1673-7288.00355

Preface

Preface to the Special Issue on Post-quantum Cryptography and Blockchain Applications

Jian Weng (翁健)[1], Liehuang Zhu (祝烈煌)[2], Yunlei Zhao (赵运磊)[3]

[1] (College of Cyber Security, Jinan University, Guangzhou 510632, China)
[2] (School of Cyberspace Science and Technology, Beijing Institute of Technology, Beijing 100081, China)
[3] (School of Computer Science and Engineering, Fudan University, Shanghai 201203, China)
Corresponding author: Yunlei Zhao, ylzhao@fudan.edu.cn

Citation Weng J, Zhu LH, Zhao YL. Preface to the special issue on post-quantum cryptography and blockchain applications, *International Journal of Software and Informatics*, 2025, 15(4): 397–399. http://www.ijsi.org/1673-7288/355.htm

In the context of deep integration of digital technologies into work and life, modern public-key cryptography forms a robust defense, safeguarding daily communication, financial transactions, and commercial security. However, the rapid development of quantum computing poses a disruptive threat to currently deployed public-key cryptosystems. Ensuring the long-term security of cyberspace and navigating the strategic migration of cryptographic technologies in the quantum era has consequently emerged as a significant global challenge for the generational transition of cryptography and a focal point of major-power strategic competition. Since 2019, blockchain technology has been elevated to a national strategy in China, incorporated as an important component of the "New Infrastructure" initiative and featured in the national "14th Five-Year Plan" and the "Long-Range Objectives for 2035". It has become an indispensable trust infrastructure for the nation's future digital economy. Post-quantum security is an essential requirement and a critical metric for the next generation of the blockchain infrastructure. In February 2025, China initiated a global solicitation for proposals for its next-generation post-quantum cryptography standards.

This special issue focuses on the mathematical foundations and security mechanisms of post-quantum cryptography, along with algorithm design and optimization, efficient and secure software/hardware implementations, and their applications in blockchain. Addressing the specific demands that post-quantum secure blockchain places on cryptography in terms of security guarantees, size, and throughput, it pays particular attention to consensus mechanisms and cryptographic techniques adapted for post-quantum secure blockchain systems.

An overview of five representative papers in this issue is as follows.

The paper "*Tighter Reductions of LWE Problems with Semi-uniform Seeds*" addresses the learning with errors (LWE) problem, a fundamental computationally hard problem underpinning lattice-based public-key cryptography. By refining techniques from the study of Hint-LWE problem hardness, it presents a dimension-preserving reduction from the standard LWE problem in Euclidean/ideal/module lattices to the corresponding semi-uniform LWE (SU-LWE) problem. The reduction techniques used are independent of the algebraic structure of the underlying hard problem and remain unaffected by the embedding form (coefficient or canonical embedding)

Received 2025-02-19; Accepted 2025-02-26; IJSI published online 2025-12-30

when applied to hardness analysis of Ring/Module LWE problems. The resulting reduction incurs only a small loss in the Gaussian error parameter, and the generalized reduction loss is independent of the number of samples. Furthermore, the hardness reduction for the corresponding problem on ideal lattices does not require non-standard assumptions like the decisional small polynomial ratio (DSPR) assumption or its variants. Since the IND-CPA security proof for basic public-key encryption schemes designed using the Lindner-Peikert framework with a compressed public key relies on instantiating a specific type of SU-LWE problem, the reduction results for the SU-LWE problem on module lattices presented in this paper could be applied to the theoretical security evaluation of efficient, practical lattice-based encryption/key encapsulation mechanisms (KEMs) such as Kyber (NIST Round 1 design), Aigis, and AKCN-MLWE. Asymptotically, using the reduction results from this paper, the IND-CPA security of the underlying encryption schemes used in the aforementioned constructions may be reduced, in a dimension-preserving manner, to appropriately parameterized standard LWE problems. Compared with known reduction results, this paper not only preserves the dimension of the lattice associated with the hard problem but also ensures a smaller loss (gap) between the Gaussian parameter of the corresponding standard LWE problem and the parameter used in the scheme, thereby providing tighter theoretical security support for the relevant schemes.

The paper "*SM3-OTS*: *Compact Post Quantum One-time Signature Scheme Based on Chinese Cryptographic Algorithm SM3*" focuses on the important direction of hash-based post-quantum signatures. This paper designs a new compact one-time signature scheme, SM3-OTS, based on the Chinese national cryptographic hash algorithm SM3. It addresses the issue of large signature size in the WOTS+ scheme used within the SPHINCS+ signature framework. By utilizing the binary and hexadecimal information of the message digest value as indices for the node positions of the first 32 and the last 16 hash chains respectively, the scheme shortens the key length and signature length compared with traditional hash-based one-time signature schemes. This results in a reduction of approximately 29% compared with WOTS+ within SPHINCS+, improving signing efficiency and storage adaptability.

The paper "*Hardware Optimization of Lattice-based Digital Signature Algorithm Based on FPGA*" proposes a novel pure hardware implementation scheme. The core contributions include fine-grained segmented timing control logic, a high-throughput two-dimensional polynomial operation array, and an optimized parallel dual-core sampling module design. The authors of this paper introduce a unified circuit architecture that supports the signing process across different security levels, offering advantages in both high performance and high resource reuse rate. The design is implemented and tested on the Xilinx Artix-7 FPGA platform and compared with existing works. The results show that compared with the most recent literature, the proposed design achieves speedups of 7.4, 8.3, and 5.6 folds for signature generation across the three security levels, respectively.

The paper "*Quantum-resistant and Efficient Blockchain Authentication Storage Scheme*" proposes an efficient quantum-resistant authenticated storage (EQAS) scheme for blockchains, aiming to address the security threats posed by quantum computing to existing blockchain authenticated storage techniques. EQAS introduces stateless hash-based signatures and employs a dynamic forest chain (DFORC) and a super-tree structure to decouple data storage from authentication, thereby improving efficiency and effectively ensuring the integrity and security of the authentication process. Compared with conventional blockchain authenticated storage schemes, EQAS optimizes the state update mechanism while effectively avoiding the I/O bottleneck issue inherent in Merkle Patricia Trie structures. Experimental results demonstrate that the EQAS scheme outperforms existing authenticated storage schemes in both authentication efficiency and security.

The paper "*Post-quantum Blockchain System Based on Multi-parent Chain Auxiliary Proof-of-work Consensus Mechanism*" proposes a post-quantum blockchain system characterized by diversified computing power and the application of autonomously controllable post-quantum signatures. For the foundational signature algorithm of the security mechanism of the blockchain, the system adopts Dilithium-prime, a post-quantum digital signature based on prime-order number fields. Compared with the international standard Dilithium algorithm, Dilithium-prime has a simpler underlying algebraic structure, potentially offering more robust long-term security, while maintaining comparable computational efficiency. A multi-ancestor-chain-assisted proof-of-work consensus mechanism is employed, which reuses computational power to diversify the sources of hashing power enhancing security and improving computational power utilization. To address significant disparities in computational power among multiple ancestor chains, the authors design and apply a dynamic and flexible difficulty adjustment algorithm, effectively coping with fluctuations in hashing power and ensuring the stable operation of the multi-ancestor-chain blockchain system.

Jian Weng, Ph.D., professor and doctoral supervisor at Jinan University, a member of the CCF, and a member of the Cyberspace Security Discipline Review Group under the Academic Degrees Committee of the State Council. He serves as the director of the National and Local Joint Engineering Research Center for Cybersecurity Detection and Protection Technology and is a recipient of the National Science Fund for Distinguished Young Scholars. He has received one National Technology Invention Award (Second Class) and two provincial/ministerial level first prizes. His main research fields include cryptography and information security.

Liehuang Zhu, Ph.D., professor and doctoral supervisor at Beijing Institute of Technology, a member of the CCF Council, director of the Blockchain Committee of the China Society of Chinese Computer Schools, director of the Intelligent Information Network Committee of the Chinese Association for Artificial Intelligence, and a member of the Teaching Guidance Committee for Cyberspace Security under the Ministry of Education. He is selected into the national high-level talent program for leading talents. He has presided over more than 40 national-level projects, including the National Key R&D Program of China and key projects of the National Natural Science Foundation of China. His main research fields include data security and privacy protection, blockchain security and regulation, and artificial intelligence security.

Yunlei Zhao, Ph.D., professor and doctoral supervisor at Fudan University, and a senior member of the CCF. He has presided over national-level talent fund projects, key R&D projects, and projects from the National Natural Science Foundation of China. He has published over 100 papers and has been granted or disclosed over 30 Chinese invention patents. He has received two provincial/ministerial level awards. His main research fields include cryptographic theory and applications, and the design and engineering implementation of post-quantum cryptographic algorithms.