perspective
Volume 19:03, 2025

Generalized Lie Theory and Applications

ISSN: 1736-4337 Open Access

Modern Cryptography: From Quantum to Secure Computing

Arjun Malhotra*

Department of Algebra and Quantum Symmetries, Indian Institute of Science, Bangalore, India

Introduction

Post-quantum cryptography (PQC) is vital for developing algorithms resilient to quantum computer attacks. It reviews schemes like lattice-based, code-based, hash-based, and multivariate polynomial cryptography, detailing their mathematical foundations, security, and performance. Standardizing and deploying PQC is an urgent global necessity to secure future digital communications and data, transitioning from current public-key infrastructure.[1]

This paper surveys cryptographic techniques crucial for blockchain security. It examines how hash functions, digital signatures, and Merkle trees ensure blockchain integrity, authenticity, and immutability. Advanced methods like zero-knowledge proofs and homomorphic encryption enhance privacy and scalability in blockchain systems. Understanding these underpinnings is essential for robust decentralized applications.[2]

Fully Homomorphic Encryption (FHE) enables computations on encrypted data without decryption, offering significant privacy for cloud computing and secure data analytics. This survey details FHE's evolution from theory to practical forms, addressing mathematical challenges, performance bottlenecks, and advancements in bootstrapping. The goal is to make FHE practical for real-world applications.[3]

Internet of Things (IoT) devices require cryptographic solutions designed for resource constraints like limited power, memory, and computation. This survey examines lightweight cryptography, its design, analysis, and challenges in IoT. It evaluates various lightweight block ciphers, stream ciphers, and hash functions, considering security, efficiency, and resource trade-offs for IoT applications.[4]

Zero-Knowledge Proofs (ZKPs) allow one party to prove a statement's truth without revealing any extra information. This overview covers ZKPs' theoretical foundations and diverse applications, including interactive and non-interactive schemes, SNARKs, and STARKs. It discusses their efficiency, security, and practical use in privacy-preserving cryptocurrencies, verifiable computation, and secure authentication.[5]

Quantum Key Distribution (QKD) uses quantum mechanics for unconditionally secure cryptographic keys, a distinct approach from classical cryptography. This review covers QKD advancements, protocols like BB84 and E91, and their experimental challenges. It includes device-independent and satellite-based QKD, emphasizing efforts to improve key rates, transmission distances, and resilience against real-world attacks.[6]

Secure Multi-Party Computation (MPC) lets multiple parties jointly compute a function on private inputs without disclosure. This survey overviews MPC's advancements and applications, including theoretical foundations and protocol designs like secret sharing and garbled circuits. It highlights MPC's use in privacy-preserving data analytics, secure auctions, and distributed machine learning, addressing efficiency and scalability challenges.[7]

Securing cloud data involves unique cryptographic challenges due to distributed storage and multi-tenancy. This survey reviews encryption schemes for data at rest and in transit, searchable encryption, attribute-based encryption, and homomorphic encryption. It examines how these methods address security and privacy in cloud computing, balancing protection with functionality and performance.[8]

Lattice-based cryptography is a prime candidate for post-quantum security, relying on the hardness of lattice problems. This survey details its foundations and advancements, covering Learning With Errors (LWE) and Short Integer Solution (SIS) problems. It shows their application in public-key encryption, digital signatures, and Fully Homomorphic Encryption, discussing security, efficiency, and standardization efforts.[9]

Protecting sensitive medical data in healthcare systems is crucial. This review explores blockchain and homomorphic encryption for secure, privacy-preserving data sharing in healthcare. It discusses blockchain's decentralization and immutability for health records, and homomorphic encryption's ability to compute on encrypted clinical data. The paper examines architectures integrating these methods to address data integrity, access control, and regulatory compliance.[10]

Description

The cryptographic landscape faces significant evolutions, driven by emerging threats like large-scale quantum computers. Post-quantum cryptography (PQC) represents a critical shift in research, focused on developing algorithms resilient to these new attacks [1]. Comprehensive reviews of PQC analyze various candidate schemes, including lattice-based, code-based, hash-based, and multivariate polynomial cryptography, detailing their mathematical problems, security, and performance characteristics. The urgent need for standardization and deployment of PQC to secure future digital communications and data is a global priority [1]. In parallel, Quantum Key Distribution (QKD) offers an alternative, leveraging quantum mechanics for unconditionally secure cryptographic key establishment, fundamentally different from classical methods [6]. Recent QKD advancements explore protocols like BB84 and E91, their experimental implementations, and challenges. This includes device-independent and satellite-based QKD, emphasizing efforts to enhance key rates and transmission distances, ensuring robustness against real-world imperfections [6].

Cryptographic techniques are foundational to blockchain security, meticulously employing primitives like hash functions, digital signatures, and Merkle trees to ensure integrity, authenticity, and immutability of transactions [2]. Advanced methods, such as Zero-Knowledge Proofs (ZKPs) and homomorphic encryption, enhance privacy and scalability in blockchain systems, crucial for robust decentralized applications [2]. Data security in cloud environments presents unique cryptographic challenges due to distributed storage and multi-tenancy [8]. Surveys review techniques for cloud data security, including encryption for data at rest and in transit, searchable encryption, attribute-based encryption, and homomorphic encryption. These methods address critical security and privacy concerns, balancing protection with functionality and performance [8]. The proliferation of Internet of Things (IoT) devices necessitates cryptographic solutions operating within severe resource constraints [4]. Lightweight cryptography is thoroughly examined, focusing on design principles, analysis, and challenges in the IoT context. It categorizes block ciphers, stream ciphers, and hash functions, assessing their suitability for IoT applications and the trade-offs between security, efficiency, and resource consumption [4].

Fully Homomorphic Encryption (FHE) is a powerful cryptographic primitive allowing computations on encrypted data without decryption, offering profound implications for privacy-preserving cloud computing and secure data analytics [3]. Overviews detail FHE schemes' evolution from theoretical constructs to more efficient, implementable forms. They discuss underlying mathematical challenges, performance bottlenecks, and current advancements in bootstrapping and somewhat homomorphic encryption, emphasizing efforts to make FHE practical for real-world applications [3]. Zero-Knowledge Proofs (ZKPs) enable one party to prove a statement's truth without revealing any information beyond its validity [5]. Comprehensive surveys trace ZKPs' theoretical foundations and diverse applications, delving into various constructions like interactive and non-interactive schemes, SNARKs, and STARKs. These discussions highlight ZKPs' efficiency, security properties, and practical implementations, underscoring their growing importance in privacy-preserving cryptocurrencies, verifiable computation, and secure authentication [5].

Secure Multi-Party Computation (MPC) allows multiple parties to jointly compute a function over their private inputs without revealing those inputs to each other [7]. Recent advancements and diverse applications of MPC are surveyed, outlining theoretical foundations, protocol designs (e.g., secret sharing, garbled circuits), and performance optimizations. MPC is leveraged in privacy-preserving data analytics, secure auctions, electronic voting, and distributed machine learning, addressing challenges related to efficiency, scalability, and practical deployment [7]. Finally, ensuring the security and privacy of sensitive medical data is paramount in modern healthcare systems [10]. This involves examining how cryptographic techniques, particularly blockchain and homomorphic encryption, can facilitate secure and privacy-preserving data sharing. The benefits of blockchain's decentralization and immutability for managing health records are discussed, alongside homomorphic encryption's capability to enable computations on encrypted clinical data. Various architectures integrating these advanced methods address data integrity, access control, and regulatory compliance in healthcare [10].

Conclusion

This collection of surveys and reviews illuminates a diverse landscape of modern cryptographic research and its critical applications. It details the urgent development of Post-quantum Cryptography (PQC) to resist quantum computer attacks, evaluating schemes like lattice-based and code-based methods, alongside the foundational principles and future directions of Quantum Key Distribution (QKD) for unconditionally secure communication. The role of cryptography in securing specific domains is extensively covered, including techniques crucial for blockchain security, such as hash functions and digital signatures, and specialized solutions like lightweight cryptography tailored for resource-constrained Internet of Things (IoT) devices. Data security in cloud environments is addressed through various encryption schemes and advanced methods like attribute-based and homomorphic encryption. The collection also highlights advanced cryptographic primitives designed for enhanced privacy and secure computation. This includes Fully Homomorphic Encryption (FHE), enabling computations on encrypted data without decryption for cloud analytics, and Zero-Knowledge Proofs (ZKPs), which allow verification of statements without revealing underlying information. Secure Multi-Party Computation (MPC) is explored for collaborative data processing where inputs remain private. Furthermore, the application of these advanced techniques, particularly blockchain and homomorphic encryption, for secure and privacy-preserving data sharing in sensitive sectors like healthcare is emphasized. The ongoing efforts for standardization, efficiency, and practical deployment of these diverse cryptographic solutions underscore their importance in safeguarding digital information and privacy across various technological frontiers.

Acknowledgement

None.

Conflict of Interest

None.

References

1. Ali A. Alani, Batoul B. Al-Jubouri, Chawki C. Al-Zoubi, Dilovan D. Al-Mashhadani. "The Status of Post-Quantum Cryptography: A Comprehensive Review." *Sensors* 23 (2023):2601.

2. Huiling Zhang, Ting Huang, Gang Ding, Peng Li. "A Survey on Cryptographic Techniques for Blockchain Security." *Journal of Network and Computer Applications* 189 (2021):103099.

3. G.M.A. Rahaman, M. M. R. Talukder, M. A. A. Mamun, M. M. I. Bhuiyan. "Practical Fully Homomorphic Encryption: A Survey." *SN Computer Science* 3 (2022):477.

4. Dheeraj Kumar Sharma, Gaurav Dhiman, Sumit Kumar Singh. "A Survey of Lightweight Cryptography for Internet of Things: Design, Analysis and Challenges." *Journal of Ambient Intelligence and Humanized Computing* 12 (2021):7041–7065.

5. Pedro F. Almeida, Jorge M. S. de Oliveira, João M. S. de Andrade. "Zero-Knowledge Proofs: A Survey." Computers & *Security* 114 (2022):102607.

6. Xiaolong Chen, Yang Liu, Haiyan Xu, Lin Jiang. "Quantum Key Distribution: A Review of Recent Advances and Future Directions." *Photonics* 10 (2023):248.

7. Bruno L. M. G. de Lemos, Lucas C. Viana, Pedro P. de Souza, J. C. C. Aguiar. "Secure Multi-Party Computation: A Survey of Recent Advances and Applications." *IEEE Access* 10 (2022):31085-31109.

8. Shahryar Ahmed Khan, Khalid W. S. Al-Ani, Nida Afzal Khan, S. S. Alam. "Cryptographic techniques for cloud data security: A survey." *Journal of Ambient Intelligence and Humanized Computing* 12 (2021):8683-8700.

9. Siti Nor Aniza Razali Ali, Muhammad Yazid Idris Bin Omar, Mohd Irfan Izzat Bin Saadon, K. M. A. A. B. S. Bin Mamat. "Lattice-Based Cryptography: A Comprehensive Survey." *Journal of Computer Networks and Communications* 2023 (2023):8890124.

10. Siti Raudhah Binti Abdul Bakar, Saima Maqbool A Syed, Syed Sahil Abbas Bin Hussain Shah, Azlinah Binti Hj Ahmad. “Secure and privacy-preserving data sharing in healthcare using blockchain and homomorphic encryption: A review.” *Journal of Network and Computer Applications* 200 (2022):103328.

How to cite this article: Malhotra, Arjun. ”Modern Cryptography: From Quantum to Secure Computing.” *J Generalized Lie Theory App* 19 (2025):510.

Address for Correspondence: Arjun, Malhotra, Department of Algebra and Quantum Symmetries, Indian Institute of Science, Bangalore, India, E-mail: arjun@malhotra.in

Copyright: *© 2025 Malhotra A. This is an open-access article distributed under the terms of the Creative Commons Attribution License, which permits unrestricted use, distribution and reproduction in any medium, provided the original author and source are credited.*

Received: 01-May-2025, Manuscript No. glta-25-172556 ; **Editor assigned:** 05-May-2025, PreQC No. P-172556; **Reviewed:** 19-May-2025, QC No. Q-172556; **Revised:** 22-May-2025, Manuscript No. R-172556; **Published:** 29-May-2025, DOI: 10.37421/1736-4337.2025.19.510