STM JOURNALS

International Journal of
Computer Science Languages

Volume 2, Issue 1, 2024
January–June
DOI (Journal): 10.37591/IJCSL

https://journals.stmjournals.com/ijcsl

Review IJCSL

An Investigative Study of Quantum-safe Secure Multi-party Computation

Aiswarya Dwarampudi[1], Yamuna Mundru[2], Manas Kumar Yogi[1,*]

Abstract

This article represents the comprehensive investigation in the emerging field of quantum-safe secure multi-party computation (QSSMPC) and presents novel perspectives to address the impending threat posed by quantum computers to classical cryptographic systems. As the era of quantum computing approaches, traditional encryption methods become vulnerable to quantum algorithms, necessitating the development of quantum-resistant cryptographic protocols. In this context, the paper introduces innovative approaches to secure multi-party computation in a quantum-safe framework. It discusses the theoretical foundations of quantum-safe cryptography and its integration into multi-party computation protocols. The paper also explores practical implementations and potential applications of QSSMPC in real-world scenarios, emphasizing the importance of transitioning towards quantum-resistant cryptographic techniques to ensure the long-term security of sensitive data. The provided viewpoints seek to actively engage in the ongoing discussion surrounding quantum-safe cryptographic systems, providing valuable perspectives that guide the creation of resilient and secure computing frameworks in the post-quantum era.

Keywords: Quantum, secure multi-party computation (SMPC), security, privacy, encryption, private key

INTRODUCTION

Secure multi-party computation (SMPC) is a cryptographic method facilitating the collaborative computation of a function involving private inputs from multiple parties while maintaining the confidentiality of those inputs. The primary objective of SMPC is to support joint computations without disclosing sensitive information [1]. This is accomplished by employing cryptographic protocols designed to safeguard the privacy and integrity of the inputs provided by the participating parties. In SMPC, each party holds a private input, and they wish to compute a function collectively without disclosing their individual data. The protocol guarantees that at the end of the computation, each party learns only the output of the function and nothing more. This is particularly valuable in scenarios where trust is limited, and parties are unwilling or unable to share their raw data due to privacy concerns [2].

***Author for Correspondence**
Manas Kumar Yogi
E-mail: manas.yogi@gmail.com

[1]Assistant Professor, Department of Computer Science & Engineering, Pragati Engineering College, Kakinada, Andhra Pradesh, India
[2]Assistant Professor, Department of Computer Science & Engineering–Artificial Intelligence & Machine Learning (CSE–AI & ML), Pragati Engineering College, Kakinada, Andhra Pradesh, India

Received Date: February 19, 2024
Accepted Date: April 30, 2024
Published Date: May 09, 2024

Citation: Aiswarya Dwarampudi, Yamuna Mundru, Manas Kumar Yogi. An Investigative Study of Quantum-safe Secure Multi-party Computation. International Journal of Computer Science Languages. 2024; 2(1): 39–44p.

Effectiveness in Network Security

Privacy Preservation

SMPC is highly effective in maintaining the privacy of sensitive information in network security scenarios. For example, in a collaborative intrusion detection system, multiple entities may want to collectively analyze network traffic patterns to detect anomalies without exposing individual network data.

Secure Data Aggregation

In network monitoring and data aggregation, SMPC allows entities to securely aggregate information without revealing the raw data. This is

crucial for obtaining a global view of network health or security status while preserving the confidentiality of specific data points.

Decentralized Key Management

SMPC can be applied to decentralized key management in secure communication networks. Multiple parties can collaboratively compute cryptographic operations without sharing their private keys, enhancing the security of communication protocols.

Distributed Threat Intelligence

In the context of threat intelligence sharing, organizations can use SMPC to collaboratively analyze and correlate threat data without exposing the specifics of their own security incidents. This facilitates a collective defense against cyber threats while safeguarding sensitive information.

Collaborative Security Analytics

SMPC enables organizations to perform joint security analytics, such as analyzing patterns of attacks or identifying vulnerabilities, without disclosing the details of individual security events. This cooperative strategy elevates the overall security stance of the network.

MOTIVATION OF THE STUDY

The progress in quantum computing technology represents a notable risk to the security of traditional cryptographic protocols. Traditional cryptographic systems, including those used in SMPC, may become vulnerable to quantum attacks. SMPC, a fundamental tool for privacy-preserving collaborative computations, is widely employed in scenarios ranging from healthcare to financial transactions. The imminent arrival of quantum computers necessitates immediate investigation into quantum-resistant versions of SMPC to guarantee the ongoing confidentiality and integrity of sensitive data.

Quantum Threat to Classical Cryptography [3, 4]

Quantum computers possess the capability to effectively address problems that are currently challenging for classical computers, such as factoring large numbers and computing discrete logarithms. For instance, Shor's algorithm poses a threat to the security of commonly employed public-key cryptographic systems like RSA (Rivest-Shamir-Adleman) and ECC (elliptic curve cryptography). As SMPC heavily relies on cryptographic primitives, the vulnerabilities introduced by quantum computing pose a critical challenge to the security guarantees of collaborative computations.

Criticality of SMPC in Sensitive Domains

SMPC is applied in critical sectors like healthcare, finance, and governmental operations, where maintaining paramount privacy and data confidentiality is essential. For instance, in healthcare, multiple parties may need to collaboratively analyze patient data for medical research without revealing individual patient records. The compromise of SMPC protocols due to quantum attacks could lead to severe privacy breaches and compromise the integrity of collaborative computations in these critical sectors.

Emergence of Quantum-safe Cryptography

Recognizing the looming threat of quantum computing, the cryptographic community has been actively developing quantum-safe or post-quantum cryptographic algorithms. However, the integration of these quantum-safe primitives into SMPC protocols requires careful consideration, as the nature of SMPC introduces additional complexities compared to traditional cryptographic applications.

Objective of the Study

The primary objective of this work is to design and evaluate quantum-safe SMPC protocols that resist quantum attacks while preserving the efficiency and functionality required for practical deployment. By addressing the quantum threat to SMPC, this study aims to contribute to the development of cryptographic solutions that ensure the long-term security of collaborative computations in the post-quantum era.

Significance of the Study

The findings of this work will have broad implications for the security and privacy of collaborative computations in quantum-vulnerable environments. As quantum computing technology matures, the insights gained from this study will guide the development of quantum-safe SMPC protocols, securing sensitive data against the evolving landscape of quantum threats.

NOVEL PERSPECTIVES

Designing a high-level model for quantum-safe SMPC involves integrating quantum-resistant cryptographic primitives into the traditional SMPC framework. The following is a conceptual high-level model for quantum-safe SMPC [5–7]:

- *Quantum-safe cryptographic primitives*
  - *Quantum-safe encryption:* Replace classical encryption schemes vulnerable to quantum attacks with quantum-resistant encryption algorithms. Examples include lattice-based or code-based encryption.
  - Implement quantum-safe authentication by employing digital signature schemes that are resistant to quantum attacks, ensuring the messages exchanged between parties maintain integrity and authenticity.
- *Quantum-safe key exchange:* Develop a key exchange protocol that is secure against quantum adversaries. This involves establishing a shared secret key between parties without exposing it to quantum attacks. Post-quantum key exchange mechanisms such as NTRU Encrypt or New Hope may be considered.
- *Hybrid cryptographic protocols:* Integrate quantum-resistant cryptographic primitives into the existing SMPC protocols. This could entail adopting a hybrid strategy that integrates classical and quantum-safe cryptographic operations, aiming to establish security measures against both classical and quantum threats.
- *Quantum-safe garbled circuits:* Adapt garbled circuit protocols, a common approach in SMPC, to use quantum-resistant cryptographic primitives. This guarantees the security of computations conducted on encrypted data, even when confronted with quantum adversaries.
- *Quantum-safe oblivious transfer:* Implement oblivious transfer protocols resistant to quantum attacks. Oblivious transfer is a crucial primitive in SMPC for secure information transfer, and ensuring its quantum resistance is essential for the overall security of the protocol.
- *Quantum-safe zero-knowledge proofs:* Incorporate quantum-safe zero-knowledge proofs to enhance the privacy and security guarantees of the SMPC protocol. Zero-knowledge proofs are essential in enabling parties to validate the accuracy of their statements without divulging sensitive information.
- *Security parameters and post-quantum transition:* Define security parameters for the quantum-safe SMPC model, considering both classical and quantum adversaries. Additionally, mechanisms for a smooth transition to post-quantum algorithms should be incorporated as quantum-resistant primitives are standardized.
- *Quantum-safe random number generation:* Ensure that random number generation within the protocol remains secure against quantum attacks. Quantum-safe pseudo-random number generators may be used to maintain unpredictability in cryptographic operations.
- *Quantum-safe error correction:* Implement error correction mechanisms that are resilient to quantum errors, as quantum-safe SMPC may involve quantum communication channels that are susceptible to quantum noise and errors.
- *Performance optimization:* Optimize the performance of the quantum-safe SMPC protocol to make it practical for real-world applications. Considerations include computational efficiency, communication overhead, and scalability.

CURRENT TRENDS

SMPC involves a range of protocols and methods crafted to enable multiple parties to collaboratively compute a function using their private inputs while ensuring the confidentiality of those inputs. In the

following text, we present some notable variants and related concepts within the broader realm of SMPC which are currently trending across all applications of cyber security [8–10]:

- *Threshold cryptography:* In threshold cryptography, a secret is divided among multiple parties, and only a threshold number of parties are required to collaborate to perform cryptographic operations. This is a specific form of SMPC where participants collectively contribute to key generation and cryptographic computations.
- *Homomorphic encryption:* Homomorphic encryption enables the execution of computations on encrypted data without the need for decryption. This is particularly relevant to SMPC, as it enables parties to collaboratively compute functions on sensitive data while maintaining privacy. Fully homomorphic encryption (FHE) supports arbitrary computations on encrypted data.
- *Zero-knowledge proofs:* Zero-knowledge proofs enable a party to demonstrate the truth of a statement to another party without disclosing any information about the statement itself. In SMPC, zero-knowledge proofs can be employed to validate the correctness of computations without disclosing the private inputs.
- *Differential privacy:* Differential privacy focuses on adding noise to the output of computations to protect individual privacy. In the context of SMPC, incorporating differential privacy ensures that the presence or absence of a single party's input does not significantly impact the output of the computation.
- *Function secret sharing:* Function secret sharing extends traditional secret sharing to allow parties to jointly compute a function of their shared secrets without reconstructing the individual secrets. This is a specialized variant of SMPC tailored for certain types of computations.
- *Secure function evaluation:* Secure function evaluation (SFE) is a specific class of SMPC where the primary goal is to securely evaluate a function on private inputs. It encompasses various cryptographic protocols and techniques for achieving this securely.
- *Secure multi-party protocols for machine learning:*
  - Tailored SMPC protocols are designed specifically for privacy-preserving machine learning.
  - These protocols enable the joint participation of multiple parties in training or evaluating machine learning models without the necessity of sharing their raw data.
- *Blockchain-based secure multi-party computation:* SMPC protocols integrated into blockchain networks enable decentralized and trustless collaborative computations. Blockchain-based SMPC is employed in scenarios where transparency and verifiability are crucial.
- *Secure two-party computation:* Two-party computation (2PC) is a subset of SMPC focusing on scenarios where only two parties are involved. It is a fundamental building block in multi-party computations, especially when considering scenarios with a client and a server.
- *Oblivious random access machine:* While not strictly a variant of SMPC, oblivious random access machine (ORAM) is often used in conjunction with SMPC to protect against side-channel attacks and enhance the privacy of data access patterns.

These variants and related concepts demonstrate the versatility and adaptability of SMPC in addressing different privacy and security requirements across various application domain as shown in Table 1 [11, 12].

FUTURE DIRECTIONS

The field of quantum-safe SMPC is dynamic and continually evolving. While it is challenging to predict specific future directions, here are five potential areas of development [13]:

- *Integration with quantum-safe blockchains:* Future research may explore the integration of quantum-safe SMPC with quantum-resistant blockchain technologies. This could enhance the security and privacy of decentralized applications, smart contracts, and consensus mechanisms in the presence of quantum adversaries.
- *Efficiency improvements and practical deployments:* As quantum-safe cryptographic primitives are further developed and standardized, future directions may focus on optimizing the efficiency of quantum-safe SMPC protocols. This includes reducing computational overhead, communication costs, and making the protocols more practical for deployment in various real-world scenarios.

Table 1. Taxonomy of quantum-safe secure multi-party computation (SMPC) approaches

Trends in quantum-safe SMPC	Applications	Benefits	Limitations
1. Post-quantum cryptography	Secure communications in the post-quantum era.	Resistance against quantum attacks.	Limited standardization of post-quantum cryptographic algorithms.
2. Lattice-based cryptography	Secure key exchange and encryption in SMPC.	Strong security guarantees against quantum adversaries.	Computationally intensive, impacting efficiency.
3. Code-based cryptography	Robust error correction in quantum-resistant protocols.	Resilience to quantum algorithms like Shor's.	Key sizes can be larger than some other post-quantum alternatives.
4. Hash-based cryptography	Digital signatures and secure hash functions.	Simplicity and resilience against quantum attacks.	Limited use cases due to one-time signature nature.
5. Multivariate polynomial cryptography	Digital signatures and public-key encryption.	Potential for shorter key sizes and efficient operations.	Security relies on the difficulty of solving systems of multivariate polynomial equations.
6. Hash-based digital signatures	Signing and authentication in secure communication.	Simplicity and resistance to quantum attacks.	Key sizes may be larger compared to some alternatives.
7. Quantum-safe key exchange	Establishing shared secret keys securely.	Ensures confidentiality against quantum adversaries.	May introduce additional computational overhead.
8. Integration with blockchain	Secure decentralized computations in blockchain networks.	Enhanced privacy and security for smart contracts.	Potential scalability challenges in blockchain networks.
9. Privacy-preserving machine learning	Collaborative data analysis without revealing raw data.	Maintains confidentiality in multi-party machine learning.	Computationally intensive for complex machine learning tasks.
10. Quantum-safe zero-knowledge proofs	Privacy-preserving authentication and computations.	Enhanced privacy guarantees in SMPC.	Computational complexity may affect protocol efficiency.

- *Advanced quantum-safe protocols for specific applications:* Research may lead to the development of specialized quantum-safe SMPC protocols tailored for specific applications, such as healthcare, finance, and internet of things (IoT) security. Customized protocols could provide optimized solutions that balance security requirements with the unique challenges of different domains.
- *Hybrid models integrating classical and quantum-safe components:* Future directions might involve the exploration of hybrid models that seamlessly integrate classical and quantum-safe components within SMPC protocols. This approach could leverage the strengths of both classical and quantum-resistant cryptographic techniques, providing a robust defense against both classical and quantum attacks.
- *Standardization and industry adoption:* With the ongoing efforts in standardizing post-quantum cryptographic algorithms, future directions may involve the incorporation of these standardized quantum-safe primitives into SMPC. As these standards become widely accepted, the industry adoption of quantum-safe SMPC could increase, leading to more secure collaborative computations.

CONCLUSION

Quantum-safe SMPC represents a critical frontier in the quest for cryptographic resilience against the imminent threat posed by quantum computing. As quantum technologies advance, traditional cryptographic systems face vulnerabilities that necessitate innovative solutions. The development of quantum-resistant cryptographic primitives, such as lattice-based and code-based cryptography, opens new avenues for securing collaborative computations in sensitive domains. The future of quantum-safe SMPC lies in the seamless integration of these advanced cryptographic techniques into practical, efficient, and scalable protocols. Efforts should focus on refining the performance of quantum-safe SMPC, ensuring its applicability across diverse industries, and fostering collaboration between quantum-safe cryptography and SMPC communities. Additionally, the standardization of post-quantum

cryptographic algorithms plays a pivotal role in enhancing the robustness of quantum-safe SMPC. As quantum-safe SMPC progresses, it holds the promise of preserving data confidentiality and integrity in the face of quantum threats, offering a paradigm shift in secure collaborative computations across healthcare, finance, blockchain, and beyond. The continued exploration of these frontiers will be pivotal in fortifying our digital ecosystems against the transformative capabilities of quantum computing.

REFERENCES

1. Fernandez-Carames TM, Fraga-Lamas P. Towards post-quantum blockchain: a review on blockchain cryptography resistant to quantum computing attacks. IEEE Access. 2020; 8: 21091–21116.
2. Kapourniotis T, Kashefi E, Leichtle D, Music L, Ollivier H. Asymmetric quantum secure multi-party computation with weak clients against dishonest majority. arXiv preprint arXiv:2303.08865. March 15, 2023. Available at https://eprint.iacr.org/2023/379
3. Innocenzi A. Theoretical Analysis and Experimental Implementation of Quantum Oblivious Transfer. Magisterale Thesis. Milan, Italy: Politecnico Milano; 2021/2022. Available at https://www.politesi.polimi.it/handle/10589/210720
4. Chen FL, Zhang H, Chen SG, Cheng WT. Novel two-party quantum private comparison via quantum walks on circle. Quantum Inform Process. 2021; 20 (5): 178.
5. Kumar A, Garhwal S. State-of-the-art survey of quantum cryptography. Arch Comput Methods Eng. 2021; 28: 3831–3868.
6. Jiang Y, Zhou Y, Feng T. A blockchain-based secure multi-party computation scheme with multi-key fully homomorphic proxy re-encryption. Information. 2022; 13 (10): 481.
7. Srivastava T, Bhushan B, Bhatt S, Haque AB. Integration of quantum computing and blockchain technology: a cryptographic perspective. In: Kumar R, Sharma R, Pattnaik PK, editors. Multimedia Technologies in the Internet of Things Environment, Volume 3. Singapore: Springer; 2022. pp. 197–228.
8. Prasad A, Sani A, Ong SY, Guntaguli N, Rampally S. Digital Client Identity and Management Using Blockchain. [Online]. November 2, 2023. Technical Disclosure Commons. Available at https://www.tdcommons.org/dpubs_series/6381/
9. Cao Z, Huang C, Li Y. A study on the improvement of computation, communication and security in garbled circuits. In 2021 6th International Conference on Intelligent Computing and Signal Processing (ICSP), Xi'an, China, April 9–11, 2021. pp. 609–617.
10. Kou TY, Che BC, Dou Z, Chen XB, Lai YP, Li J. Efficient quantum private comparison protocol utilizing single photons and rotational encryption. Chin Phys B. 2022; 31 (6): 060307.
11. Zhang K, Ma C, Sun Z, Zhang X, Zhou B, Wang Y. Privacy-preserving decision protocols based on quantum oblivious key distribution. Computers Mater Continua. 2020; 64 (3): 1915–1928.
12. Zhang Y, Gai K, Qiu M, Ding K. Understanding privacy-preserving techniques in digital cryptocurrencies. In: Qiu M, editor. Algorithms and Architectures for Parallel Processing: 20th International Conference, ICA3PP 2020, New York City, NY, USA, October 2–4, 2020, Proceedings, Part III Cham, Switzerland, Springer International; 2020. pp. 3–18.
13. Wallden P, Kashefi E. Cyber security in the quantum era. Commun ACM. 2019; 62 (4): 120–129.

