Privacy-Preserving Multiparty Computation for Quantum-Resilient Healthcare Sensor Networks: A Systematic Review

Sultan Almuhammadi, Linah Alharbi, Mayada Chaabani
Information and Computer Science Department,
King Fahd University of Petroleum and Minerals, Dhahran, Saudi Arabia

The authors contributed equally to this work.
Email: (muhamadi, g202412160, g202321010)@kfupm.edu.sa

Abstract

Secure multiparty computation (MPC) enables multiple entities to collaboratively compute functions over private inputs without revealing the underlying data. In modern healthcare systems, distributed sensor and actuator networks—comprising wearable devices, implantable sensors, edge gateways, and clinical cloud platforms—require privacy-preserving collaborative analytics to support diagnosis, monitoring, and automated therapeutic decisions. At the same time, the rapid advancement of quantum computing threatens many classical cryptographic foundations underpinning secure medical data exchange and distributed computation.

This systematic literature review (SLR) investigates Post-Quantum and quantum secure multiparty computation protocols ([P]Q-MPC) and evaluates their suitability for deployment in sensor and actuator network environments, particularly in healthcare Internet of Things (IoMT) systems. Twenty primary studies published between 2022 and early 2025 were systematically identified and analyzed. The review categorizes protocols according to cryptographic assumptions, primitives, supported multiparty functionalities, architectural models, threat models, and availability of experimental validation.

The findings reveal a dominant reliance on quantum cryptographic techniques, with widespread use of quantum key distribution and quantum one-time pad encryption. Third-party-assisted architectures are prevalent, reflecting practical deployment models such as edge- or cloud-assisted healthcare networks. Most protocols focus on foundational functionalities—including private set intersection, summation, maximum/minimum computation, and logical operations—which align closely with typical healthcare sensor network requirements such as distributed aggregation, anomaly detection, and secure decision triggering. However, scalability analysis and real-world performance evaluation remain limited. This review identifies research gaps and outlines future directions for designing quantum-resilient MPC protocols suitable for large-scale healthcare sensor and actuator systems. The results provide researchers and practitioners with a structured foundation for integrating Post-Quantum and quantum-secure computation into next-generation medical IoT infrastructures.

Keywords: secure Multiparty Computation; Sensor and Actuator Networks; Healthcare IoT; PQ-MPC; Q-MPC

1 Introduction

Secure Multiparty Computation (MPC) has attracted significant attention as an effective solution for protecting data privacy and security [1]. MPC is a generic cryptographic functionality that involves two or more parties, each holding private inputs, who aim to jointly compute a function over their inputs while ensuring maximum privacy and correctness [2]. MPC has moved beyond theoretical research and has been successfully applied in real-world settings, including private data analysis and privacy-preserving computations across industries such as healthcare and finance [3].

Quantum computing harnesses the principles of superposition and entanglement, enabling quantum systems to perform certain computations more efficiently than classical computers. This computational advantage poses a serious threat to classical cryptographic systems, especially those based on public-key primitives, as demonstrated by Shor's algorithm, which can efficiently factor large integers and compute discrete logarithms [4]. Since many

MPC protocols rely on classical cryptographic assumptions, particularly for setup and key exchange, they are vulnerable to quantum attacks. In response, researchers have proposed Post-Quantum secure multiparty computation (PQ-MPC) protocols that rely on quantum-resistant cryptographic primitives such as lattice-based, code-based, and hash-based schemes [5]. In parallel, some protocols explore quantum secure multiparty computation (Q-MPC) that leverages quantum communication or computation to achieve security guarantees.

This systematic literature review (SLR) focuses on identifying and analyzing existing research on both PQ-MPC and Q-MPC protocols. Given the progressive advancements in quantum computing and Post-Quantum cryptography, as well as the essential role of MPC in privacy-preserving applications, it is crucial to assess current approaches, classify them according to cryptographic assumptions and threat models, and uncover gaps and challenges for future research. Based on our review of the literature, no previous SLR has comprehensively addressed the landscape of PQ-MPC and Q-MPC protocols.

The main objective of this SLR is to investigate and evaluate the current state of Post-Quantum and quantum MPC protocols. Our findings aim to assist researchers in designing, evaluating, and improving MPC protocols that are resistant to quantum adversaries, based on insights gathered from existing studies. The results will also guide practitioners in selecting appropriate PQ-MPC or Q-MPC protocols for their specific application contexts. The contributions of this SLR to the field are outlined below:

1. A collection of 20 studies on [P]Q-MPC, published from 2022 up to 2025, has been identified and can serve as a foundation for future research in this area.
2. Key contextual information about the [P]Q-MPC protocols examined in the selected studies is summarized, enabling researchers to more effectively select, design, implement, and evaluate secure multiparty computation protocols suited to their specific needs.
3. Research gaps are uncovered, and future research directions are proposed to strengthen the development of quantum-resilient MPC protocols.
4. Opportunities for future work that could assist both researchers and practitioners interested in this domain are identified.

The remainder of this paper is structured as follows: Section 2 gives a general background on secure multiparty computation in healthcare sensor and actuator networks and highlights the quantum threat on medical data. Section 3 provides an overview of existing systematic literature reviews and surveys. Section 4 details the methodology employed in conducting this SLR. The results of this work are presented and discussedsed in Section 5 and Section 6, respectively. Section 7 outlines the limitations of this SLR, and Section 8 concludes the study.

2 Background

Modern healthcare systems increasingly rely on interconnected sensor and actuator networks to enable continuous monitoring, intelligent decision-making, and automated therapeutic interventions [6]. These systems range from wearable health trackers and implantable medical devices to hospital-wide monitoring infrastructures and remote patient monitoring platforms. Collectively, they form a complex ecosystem commonly referred to as the Medical Internet of Things (IoMT) [7].

Healthcare sensor networks typically consist of distributed sensing devices that collect physiological, biochemical, or environmental data. Examples include electrocardiogram (ECG) sensors, glucose monitors, pulse oximeters, blood pressure monitors, temperature sensors, and motion tracking devices. These sensors generate continuous streams of highly sensitive patient data. In many scenarios, the collected data must be aggregated, analyzed, and acted upon in near real time [8].

Unlike traditional centralized healthcare data systems, modern IoMT deployments are inherently distributed. Data may be generated at a patient's home, transmitted to edge devices or gateways, processed locally or in the cloud, and shared among multiple stakeholders including physicians, hospitals, insurers, and research institutions. This distributed architecture introduces significant privacy and security challenges, particularly when multiple parties must collaboratively compute over private patient data without exposing raw information [9].

Secure Multiparty Computation (MPC) provides a natural cryptographic framework for enabling such collaborative analytics [10]. In healthcare sensor networks, MPC can allow different entities—such as hospitals, laboratories, and wearable device providers—to jointly compute diagnostic statistics, risk scores, or predictive models without revealing individual patient records. This property is especially critical in multi-institutional healthcare systems where regulatory compliance and patient confidentiality are paramount [11].

2.1 Wearables and Distributed Patient Data Aggregation

Wearable medical devices represent one of the fastest-growing components of healthcare sensor networks. These devices continuously monitor physiological signals and often operate in resource-constrained environments. Data generated by wearables is typically transmitted to smartphones, edge gateways, or hospital servers, where aggregation and analysis occur [12]. A common requirement in such systems is privacy-preserving aggregation. For example:

- Computing the average heart rate across a cohort of patients.
- Determining the maximum or minimum glucose level within a monitoring group.
- Detecting whether any patient's reading exceeds a critical threshold.
- Performing private set intersection (PSI) to identify overlapping patient records across institutions.

Traditional centralized approaches require raw data sharing, increasing the risk of data breaches and regulatory violations [13]. In contrast, MPC enables distributed patient data aggregation while preserving confidentiality. Each participating entity retains its local data, and only the final computation result is revealed. This approach reduces exposure of sensitive health information and aligns with data minimization principles in healthcare privacy frameworks [14]. Moreover, as healthcare analytics increasingly incorporate machine learning and predictive modeling, distributed computation becomes even more critical. Federated and collaborative analytics over medical sensor data can benefit from MPC frameworks that ensure both privacy and correctness in adversarial environments [15].

2.2 Actuator Coordination in Medical Systems

Healthcare networks do not consist solely of sensors; actuator systems play an equally critical role. Actuators perform physical actions in response to sensed data and computed decisions [16]. Examples include:

- Insulin pumps adjusting dosage based on glucose readings.
- Implantable cardiac devices delivering therapeutic pulses.
- Robotic surgical systems executing precision operations.
- Smart infusion pumps regulating medication delivery.
- Automated ventilators responding to respiratory measurements.

In many scenarios, actuator decisions depend on aggregated or jointly computed data. For instance, dosage adjustments may rely on trend analysis derived from multiple sensor inputs. In telemedicine or remote surgery settings, secure coordination between multiple devices and control systems is essential. If these computations are performed insecurely, adversaries may manipulate actuator behavior, potentially causing life-threatening consequences. Therefore, ensuring both confidentiality and integrity of distributed computations is fundamental [17].

Secure MPC protocols can provide cryptographic guarantees that actuator-triggering decisions are computed correctly without leaking underlying patient data. For example, threshold-based logical operations (e.g., secure AND/OR functions) can determine whether alarm conditions are met, while preserving privacy of individual sensor readings. Similarly, secure maximum/minimum computations can identify abnormal physiological values without exposing full datasets [18]. In edge-assisted architectures, a third-party server (e.g., hospital cloud or quantum-enabled cloud service) may assist in computation while patients' devices remain lightweight and partially classical [19].

2.3 The Quantum Threat to Long-Lived Medical Data

Healthcare data are among the most sensitive and long-lived forms of personal information. Medical records may remain relevant for decades, especially for chronic conditions, genetic data, and longitudinal studies. Unlike short-lived transactional data, healthcare information must retain confidentiality far into the future [17].

This longevity introduces a critical risk in the context of quantum computing. Many current cryptographic systems rely on classical public-key assumptions, such as factoring or discrete logarithms, which are vulnerable to quantum algorithms [20]. An adversary could collect encrypted medical data today and decrypt it in the future once sufficiently powerful quantum computers become available. This "harvest now, decrypt later" threat is particularly severe for healthcare records [21].

Healthcare sensor networks often rely on secure channels, key exchange protocols, and encryption schemes that may not be quantum-resistant. If these mechanisms fail under quantum attacks, both stored medical data and transmitted sensor readings become vulnerable. In addition to confidentiality risks, integrity threats also emerge. If authentication or signature schemes are compromised by quantum adversaries, attackers may impersonate legitimate devices, inject false sensor readings, or manipulate actuator commands [22].

Post-Quantum cryptographic primitives and quantum-secure communication techniques are therefore essential for safeguarding medical IoT systems against long-term threats. The systematic analysis of Post-Quantum MPC (PQ-MPC) and quantum MPC (Q-MPC) protocols becomes highly relevant in this context. By identifying which protocols rely on quantum-resistant assumptions and which leverage quantum communication mechanisms, it becomes possible to evaluate their suitability for deployment in healthcare sensor and actuator networks.

2.4 Implications for Quantum-Resilient Healthcare Networks

Integrating quantum-resilient MPC protocols into healthcare sensor networks can address several emerging challenges [23]:

1. Privacy-Preserving Data Sharing: Hospitals and research institutions can collaborate on patient analytics without exposing raw medical records.
2. Secure Edge Computing: Lightweight patient devices can delegate computation to more powerful servers without sacrificing confidentiality.
3. Robust Actuator Decision-Making: Therapeutic actions can be triggered through secure distributed logic.
4. Long-Term Confidentiality: Adoption of Post-Quantum primitives ensures protection against future cryptanalytic advances.
5. Scalable Multi-Party Coordination: Distributed healthcare ecosystems can securely compute across multiple stakeholders.

However, practical deployment requires careful consideration of scalability, hardware constraints, communication overhead, and adversarial models. Healthcare sensor networks demand not only theoretical security but also robust performance under real-world conditions, including noisy channels, intermittent connectivity, and heterogeneous device capabilities. Consequently, evaluating existing [P]Q-MPC protocols through the lens of healthcare IoT provides a meaningful application-oriented perspective. By mapping cryptographic assumptions, architectural models, and threat resilience to healthcare requirements, it becomes possible to assess which protocols are immediately deployable and which require further refinement.

3 Related Work

This section presents an overview of previous systematic literature reviews (SLRs) and surveys related to secure multiparty computation (MPC). Several studies have addressed MPC protocols since their early development. Du et al. [24] provided a comprehensive overview of MPC issues and their applications, highlighting privacy-preserving collaborative computations across multiple domains. However, their study was limited to protocols relying on classical cryptographic assumptions.

Feng et al. [25] conducted an SLR focused on concretely efficient MPC protocols, emphasizing communication and computational efficiency improvements in classical security models. Their review, however, did not consider threats posed by quantum adversaries.

Zhou et al. [1] surveyed MPC protocols in the context of machine learning applications, specifically addressing privacy-preserving training and inference. Their work proposed valuable MPC models for online inference, federated learning, and model sharing. Nevertheless, their review was limited to classical settings and did not consider Q-MPC.

In a similar direction, Gamiz et al. [26] provided a systematic review addressing the challenges of applying MPC in large-scale data and resource-constrained environments. They identified key obstacles to practical MPC deployment, including hardware limitations, computational costs, and scalability issues. However, their analysis did not extend to Q-MPC.

Morales et al. [27] conducted an SLR focusing on a specific MPC problem, namely Private Set Intersection (PSI) protocols. Their review examined PSI techniques under semi-honest security models. Although their work introduced important ideas regarding Post-Quantum security within the PSI domain, it addressed only a specific subset of Q-MPC rather than the broader protocol landscape.

In summary, previous systematic reviews have primarily addressed classical MPC protocols, either generally or within specific applications such as PSI. However, none have systematically reviewed the integration of quantum and Post-Quantum cryptographic primitives into MPC. Consequently, there remains a critical need for a comprehensive synthesis of research targeting quantum and Post-Quantum MPC.

This review seeks to address this gap by systematically collecting, analyzing, and categorizing the existing body of work on [P]Q-MPC protocols. The goal of this SLR is to provide researchers and practitioners with a structured and detailed reference of current approaches, as well as to identify major research challenges and future directions for the development of [P]Q-MPC protocols.

4 Methodology

We conducted the review based on the systematic methodology proposed by Kitchenham et al. [28] to review studies on both quantum and Post-Quantum MPC ([P]Q-MPC) Protocols. This section outlines research questions, search queries, selection criteria, quality assessment, data extraction, and synthesis.

4.1 Research Questions

This SLR aims to explore the current state of [P]Q-MPC protocols. Table 1 presents the research questions considered within this study.

Table 1: Targeted Research Questions

RQ	Research Question
RQ1	What cryptographic assumptions underpin existing [P]Q-MPC protocols (e.g., hardness of lattice problems, code-based problems, or quantum mechanical principles)?
RQ2	What types of cryptographic primitives are employed in practical [P]Q-MPC protocols?
RQ3	What multiparty functionalities have been implemented in [P]Q-MPC protocols (e.g., private set intersection, summation, multiplication)?
RQ4	What architectural models (distributed or third-party-assisted) are used in [P]Q-MPC protocols, and what quantum capabilities are assumed for the involved parties?
RQ5	What threat models are considered in the design and analysis of [P]Q-MPC protocols?
RQ6	What is the availability of experimental validation or implementation results for [P]Q-MPC protocols?

4.2 Study Selection

A paper was included in the review if and only if it met all those inclusion criteria.

- **IC1**: a research paper that was peer-reviewed and published in a journal or a conference.
- **IC2**: proposes a new secure multiparty computation protocol designed to resist quantum attacks.
- **IC3**: provides security analysis and formal proofs.

Papers that met at least one of the following criteria was excluded from the review.

- **EC1**: work in progress, Master's thesis, Ph.D. dissertations, book chapters, or abstract.
- **EC2**: Written in non-English language.
- **EC3**: Review-based studies, such as systematic literature reviews (SLRs) or surveys.

4.3 Search Strategy Design

We retrieved relevant studies by searching five major digital libraries, including IEEE Xplore, ACM Digital Library, ScienceDirect, Wiley, and Scopus. The search was conducted in April 2025 and included studies published from 2022 up to April 2025. Additionally, we considered studies available as 'early access' in the selected digital libraries. To construct the search string, we identified common keywords derived from the research questions relevant to the focus of this systematic literature review. Since the review centers on Post-Quantum Secure Multiparty Computation, we focused on identifying synonyms for 'Post-Quantum', 'Secure Multiparty', and 'Protocol'. A pilot search was conducted across all selected digital libraries, leading to refinements of the final search string presented below.

- **Post-Quantum**: ("quantum" OR "Post-Quantum" OR "quantum-resistant" OR "quantum-safe") AND
- **Secure Multiparty**: ("multiparty computation" OR "secure multiparty computation" OR "MPC" OR "SMPC") AND
- **Protocols**: (protocol OR scheme OR implementation)

Applying the search string across the selected digital libraries yielded a total of 731 potential studies (Figure 1). It should be noted that the search string was adapted to meet the specific query requirements of each database, and filters were used when necessary. Approximately 6049 results were initially retrieved from ScienceDirect, and 1892 results from the Wiley online library, most of which were irrelevant. Consequently, we applied a filter to limit the results to computer science, reducing the final set to 183 studies in ScienceDirect and 66 studies in Wiley Online Library. We reduced the number of search terms in ScienceDirect by omitting the last AND branch due to its limitation of supporting only eight (AND/OR) operators. The search procedure used to identify relevant studies was conducted as follows:

1. The search string was applied to identify relevant studies from the selected libraries, yielding a total of **731** potential studies. Subsequently, **60** duplicate studies were removed.

2. The inclusion/exclusion criteria were initially applied to titles and abstracts, resulting in the exclusion of **649** studies. The inclusion/exclusion criteria (IC/EC) were then applied to the full texts, leading to **20** studies remaining.
3. Finally, a total of **20** primary studies (Appendix A) were selected after conducting the quality assessment. Papers that scored below the defined quality assessment threshold were excluded. Thus, the final dataset comprised **20** studies that successfully passed the third selection round and were used in the data extraction and synthesis.

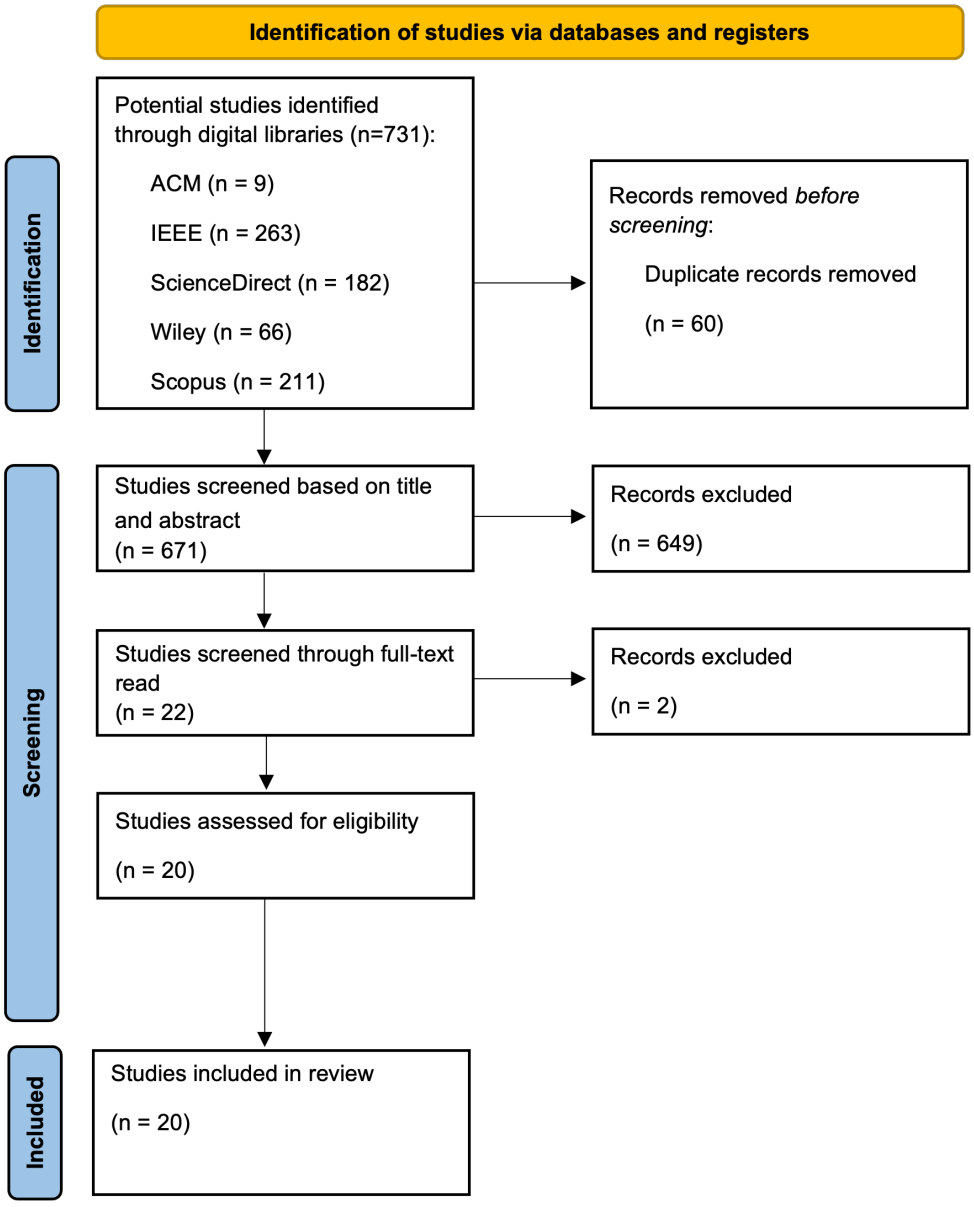

Figure 1: Search Process.

4.4 Quality Assessment

Assessing the quality of selected studies is a crucial step, as it aids in interpreting key research findings and evaluating the quality of extracted data. Quality evaluation varies significantly based on the type of the SLR, and there are no standardized definitions of primary quality metrics for studies [29]. In this review, we applied different quality assessment criteria, including clarity of research questions, methodology, proofs, experimental details, and limitations. The primary goal of our quality assessment was to support the selection of studies capable of adequately addressing the formulated research questions by ensuring high-quality extracted data. Table 2 presents the quality assessment checklist used in this SLR. the maximum achieved score was 5. Following

the approach of [30], we defined a threshold at 50%, meaning that any study scoring below 2.5 was excluded. Ultimately, no studies were excluded based on this assessment.

Table 2: Quality Assessment Checklist

QA	Quality Criteria	Score
Q1	Are the aims and research questions clearly defined?	(+1) Yes / (0) No
Q2	Is the methodology clearly described (e.g., protocol design, threat model, assumptions)?	(+1) Yes / (0) No
Q3	Are the security claims justified through proofs or formal analysis?	(+1) Yes / (0) No
Q4	Are any experiments or benchmarks conducted and well-documented?	(+1) Yes / (0) No
Q5	Are limitations or open issues discussed transparently?	(+1) Yes / (0) No

4.5 Data Extraction

We designed a data extraction form using Excel sheets to systematically gather the information necessary for addressing our research questions. The data extraction form consisted of seven sections: (1) cryptographic assumptions; (2) cryptographic primitives; (3) multiparty functionality; (4) architectural models; (5) threat models; (6) experiment; (7) number of parties; (third party). Table 3 presents a detailed description of the data fields included within each section. This form facilitated the extraction of relevant data from the finalized collection of primary studies.

Table 3: Data extraction form

Extracted Data	RQ
Cryptographic assumptions	RQ1
Cryptographic primitives	RQ2
Multiparty functionality	RQ3
Architectural models	RQ4
Threat models	RQ5
Experiment	RQ6
Number of parties	RQ4
Third party	RQ4, RQ5

5 Results

This section presents the synthesized findings for each of the research questions guiding this review. The analysis is based on 20 primary studies (PS1–PS20 listed in Table 10 in Appendix A), which were systematically selected and examined.

5.1 Overview of the Primary Studies

The selected primary studies span the period from 2022 to April 2025. As shown in Figure 2, research activity in [P]Q-MPC has remained relatively steady, with a total of 4 studies published in 2022, 6 in 2023, 6 in 2024, and 4 already in early 2025. This consistent output suggests sustained research interest in secure multiparty computation under quantum threats, with no signs of decline in momentum.

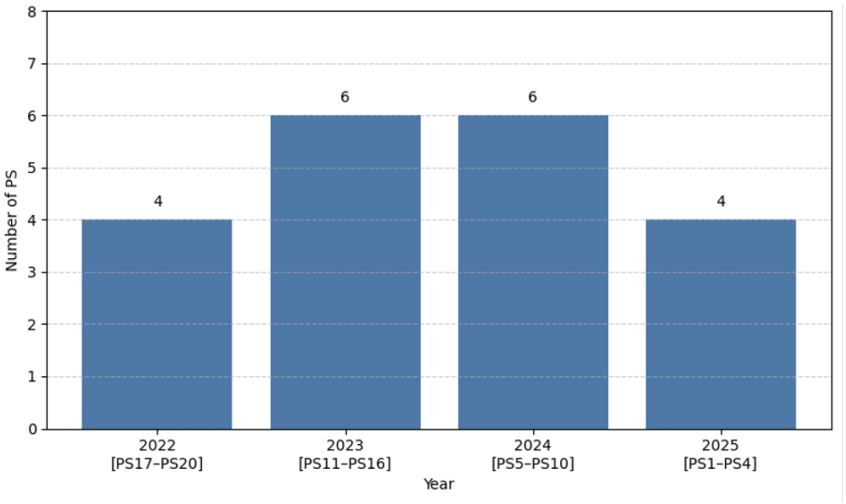

Figure 2: Distribution of primary studies over publication years

Figure 3 categorizes the studies based on the number of participating parties—distinguishing between two-party and general multiparty settings. While two-party protocols remain popular due to their simpler setup and lower communication overhead, a significant portion of the literature explores multiparty computation, demonstrating broader interest in collaborative privacy-preserving computations across multiple participants. Note that one study (PS5) proposed two different protocols, 2-party and multiparty, so it was counted in both categories.

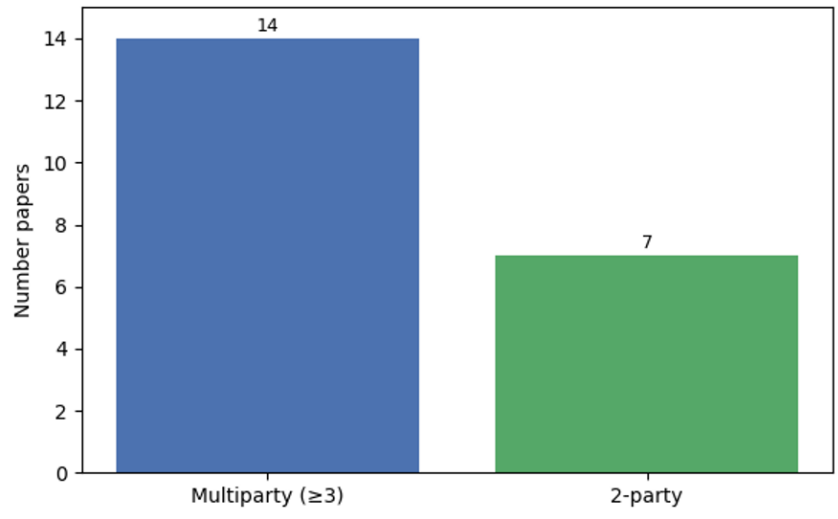

Figure 3: Distribution of studies by number of parties

5.2 RQ1: What cryptographic assumptions underpin existing [P]Q-MPC protocols?

Table 4 summarizes the cryptographic assumptions adopted in the reviewed studies. The majority (19 out of 20) rely on quantum or information-theoretic security, reflecting a strong emphasis on unconditional security guaranteed by the laws of quantum mechanics. Only one study (PS3) adopts Post-Quantum computational assumptions, specifically based on the Learning With Rounding (LWR) problem, a variant of the lattice-based hardness assumptions.

Table 4: Cryptographic Assumptions of Primary Studies

Assumption Type	**Primary Studies**	**# PSs**
Quantum / Information-Theoretic Security	PS1, PS2, PS4, PS5, PS6, PS7, PS8, PS9, PS10, PS11, PS12, PS13, PS14, PS15, PS16, PS17, PS18, PS19, PS20	19
Post-Quantum Computational Hardness	Lattice-based (LWR): PS3	1

5.3 RQ2: What types of cryptographic primitives are employed in practical [P]Q-MPC protocols?

The protocols implement a diverse set of cryptographic primitives, grouped into three major categories: key distribution, encryption, and encoding/obfuscation techniques. Table 5 details the types of primitives used and the corresponding studies. Quantum key distribution (QKD) is the most widely used method for key exchange. For encryption, the quantum one-time pad remains dominant due to its information-theoretic security. Various encoding methods, particularly those based on entanglement, are also prominent in encoding and obfuscating quantum data.

Table 5: Cryptographic Primitives Used in the Primary Studies

Category	**Primitive: Pimary Studies**	**# PSs**
Key Distribution	Generic quantum key distribution (QKD): (6) [PS1, PS5, PS7, PS8, PS14, PS16], Oblivious quantum key distribution: (1) [PS18], Mediated semi-quantum key distribution (SQKD): (1) [PS6], Phase-matching quantum conference key agreement: (1) [PS19], NA: (3) [PS3, PS4, PS20]	12
Encryption	Quantum One-Time Pad: (6) [PS1, PS2, PS14, PS16, PS19, PS20], Classical One-Time Pad: (3) [PS4, PS8, PS18] Quantum Rotation-based Encryption: (2) [PS5, PS7], Quantum Homomorphic Encryption: (1) [PS2], Classical Symmetric Encryption: (1) [PS3]	13
Encoding/Obfuscation	Entanglement-based: (5) [PS6, PS9, PS10, PS11, PS12], Phase encoding using a quantum oracle: (1) [PS13], Quantum Walk-based: (1) [PS15], Bloom Filter-based: (1) [PS8], Lattice-based OPRF from Ring-LPR problem: (1) [PS3]	9

Note: A study might appear in more than one category

5.4 RQ3: What multiparty functionalities have been implemented in [P]Q-MPC protocols?

Table 6 categorizes the multiparty functionalities implemented across the reviewed protocols. These functionalities span a wide range of operations, including set-based operations, arithmetic computations, logic-based functions, and domain-specific applications such as voting and auctions.

Set-based operations are the most common category, with protocols implementing private set intersection (PSI), PSI-cardinality, and oblivious set inclusion decision. Arithmetic functionalities include summation, product computation, and even matrix multiplication. Logic-based operations such as AND, OR, and XOR are also explored, alongside applications in geometric reasoning and secure decision-making.

Only one study (PS4) explores general-purpose secure function evaluation using quantum circuits, highlighting the potential for more expressive [P]Q-MPC frameworks in the future.

Table 6: Multiparty Functionalities Implemented in the Primary Studies

Category	**Multiparty Functionality: Primary Studies**	**#PSs**
Set-Operations	PSI: (4) [PS1, PS3, PS7, PS14], PSI-Cardinality: (3) [PS6, PS18, PS19], Oblivious Set Inclusion Decision: (1) [PS8],	8
Arithmetic	Max & Min: (2) [PS2, PS20], Summation: (2) [PS10, PS15], Product Computation: (1) [PS12], Matrix Multiplication: (1) [PS11]	6
Boolean/Logic	Logical AND: (2) [PS16, PS19], Binary Boolean Functions: (1) [PS9], Logical OR: (1) [PS20], Logical XOR: (1) [PS16]	5
Geometric	Circle Intersection: (1) [PS13]	1
Voting/Decision	Blind Millionaire Problem: (1) [PS5], One vote Veto: (1) [PS16], Sealed-Bid Auction: (1) [PS17]	3
General purpose	Function evaluation of classical input with quantum circuits: (1) [PS4]	1

Note: A study might appear in more than one functionality

5.5 RQ4: What architectural models are used in [P]Q-MPC protocols, and what quantum capabilities are assumed for the involved parties?

As shown in Table 7, the architectural models used in the reviewed protocols fall into two broad categories: distributed models and third-party-assisted models.

Distributed architectures are adopted in 7 studies, with 6 assuming quantum capabilities for the communicating parties and one (PS3) supporting classical parties but integrating Post-Quantum components to enhance security.

Third-party-assisted architectures are more prevalent, appearing in 13 studies. Among these, 4 protocols explicitly assume a fully quantum third party interacting with weak or classical clients. In 9 studies, the architectural model includes a third party but without clear assumptions about its quantum capabilities. These hybrid models reflect current practical constraints and highlight the unique role quantum clouds or mediators play in enabling functionality or trust management.

Table 7: Architectural Model and Quantum Capabilities of the Primary Studies

Architecture	Quantum Capabilities	Primary Studies	#PSs
Distributed	Quantum	[PS11, PS13, PS14, PS17, PS18, PS20]	6
	Classical	[PS3]	1
Third Party-based	Fully quantum TP and weak clients	[PS1, PS2, PS4, PS6]	4
	NA	[PS5, PS7, PS8, PS9, PS10, PS12, PS15, PS16, PS19]	9

5.6 RQ5: What threat models are considered in the design and analysis of [P]Q-MPC protocols?

Table 8 provides a breakdown of the threat models considered across the primary studies, grouped by internal, third-party, and external adversaries.

Internal adversaries are the most thoroughly analyzed. The semi-honest model is dominant, with 12 studies assuming participants follow the protocol but attempt to infer private inputs. Meanwhile, 7 studies assume malicious behavior, and only one study omits explicit assumptions. Regarding corruption thresholds, 5 protocols tolerate a single corrupted party, while others go further: 2 tolerate $n-2$ corruptions, and 4 tolerate up to $n-1$. In 9 cases, thresholds are not applicable or not specified.

Third-party adversaries are generally assumed to be semi-honest (8 studies) or non-collusive (8 studies). Only 4 protocols consider malicious TPs, and one study (PS4) allows for collusion. This is notable given the growing reliance on third parties in quantum-assisted settings.

External adversaries, particularly eavesdroppers, are addressed in 16 studies through detection mechanisms—a significant advancement enabled by quantum technology (e.g., via QKD). Only 4 studies do not include such countermeasures.

Table 8: Threat Models of the Primary Studies

Adverary Type	Assumptions		Primary Studies	#PSs
Internal	Honesty assumptions	Semi-honest	PS1, PS3, PS5, PS7, PS8, PS9, PS12, PS15, PS16, PS17, PS18, PS20	12
		Malicious	PS2, PS4, PS6, PS10, PS11, PS13, PS19	7
		Not provided	PS14	1
	Corruption threshold	Single party	PS6, PS8, PS9, PS14, PS17	5
		n parties	2 parties: (1) [PS20], N-2 parties: (2) [PS10, PS15], N-1 parties(4): [PS1*, PS4, PS5, PS7]	7
		NA	Not Applicable: (4) [PS3, PS11, PS13, PS18], Not Provided: (5) [PS2, PS9, PS12, PS16, PS19]	9
Third party	Honesty assumptions	Semi-honest	PS1, PS6, PS7, PS9, PS10, PS12, PS15, PS16	8
		Malicious	PS2, PS4, PS8, PS19	4
	Corruption	Non-collusive	PS1*, PS5, PS7, PS8, PS9, PS10, PS16, PS19	8
		Collusive	PS4	1
		Not provided	PS2, PS6, PS12, PS15	4
	Not Applicable		PS3, PS11, PS13, PS14, PS17, PS18, PS20	7
External	Eavesdropping-detection	Applied	PS1, PS2, PS4, PS5, PS6, PS7, PS8, PS9, PS10, PS11, PS13, PS15, PS16, PS18, PS19, PS20	16
		NA	PS3, PS12, PS14, PS17	4

* TP non-collusive with the initiator participant
N refers to the total number of parties while n is the number corrupted parties

5.7 (RQ6) What is the availability of experimental validation or implementation results for [P]Q-MPC protocols?

Table 9 summarizes the availability of experimental validation or implementation results in the primary studies. Out of 20 studies, 12 provided some form of experimental or implementation evidence, with the majority coming from quantum MPC proposals using IBM Quantum Simulator. In contrast, many theoretical studies or those focused on protocol design lacked empirical results.

Table 9: Availability of Experimental Results of Primary Studies

Experimental Results Availability	Study Category	Primary Studies	#PSs
Available	Quantum	PS5, PS6, PS7, PS8, PS9, PS11, PS16, PS17, PS18, PS19, PS20	11
	Post-Quantum	PS3	1
Not available	Quantum	PS1, PS2, PS4, PS10, PS12, PS13, PS14, PS15	8
	Post-Quantum	-	-

6 Discussion

The current landscape of [P]Q-MPC research reflects a field in active exploration, shaped by the constraints of quantum hardware, the urgency of Post-Quantum security, and the long-standing goals of secure multiparty computation. A dominant theme is the widespread adoption of quantum cryptographic primitives—even in the face of growing maturity and accessibility of Post-Quantum (PQ) cryptography. While lattice-based and code-based constructions (e.g., PS3) offer promising security foundations, they remain underutilized compared to quantum-native primitives.

Modern sensor networks—especially in healthcare—operate in distributed and data-sensitive environments. Wearable devices, implantable sensors, hospital monitoring systems, and remote patient platforms continuously generate private data that must often be processed collaboratively across multiple stakeholders. The multiparty functionalities identified in this review—such as private set intersection, summation, maximum/minimum computation, and logical operations—directly correspond to typical healthcare sensing tasks. For example:

- Summation protocols align with privacy-preserving aggregation of physiological signals across patient groups.
- Maximum/minimum computation supports anomaly detection in distributed monitoring systems.
- Logical AND/OR operations enable secure alarm triggering conditions.
- Private set intersection (PSI) facilitates cross-institutional patient record matching without revealing full datasets.

These mappings demonstrate that the majority of reviewed [P]Q-MPC protocols already implement foundational operations required in sensor network analytics. However, most studies focus on theoretical correctness and security proofs, with limited evaluation under realistic IoT constraints such as bandwidth limitations, latency requirements, or device heterogeneity.

A notable finding of this review is the dominance of third-party-assisted architectures. Such models closely resemble practical healthcare IoT deployments, where lightweight sensing devices delegate computational tasks to edge servers or cloud platforms. In healthcare systems, edge gateways aggregate data from multiple sensors before forwarding it to hospital infrastructure. Similarly, many Q-MPC protocols assume a semi-trusted quantum server assisting classical or weak clients. This structural similarity suggests that quantum-assisted MPC could be integrated into edge-assisted sensor networks with minimal architectural disruption. However, reliance on third parties introduces trust and collusion considerations. In medical environments, a cloud provider or hospital server may be honest-but-curious rather than fully trusted. Therefore, the threat models examined in the reviewed protocols—particularly semi-honest and malicious third-party assumptions—become directly relevant to real-world deployment in sensor and actuator systems.

In healthcare settings, actuators include insulin pumps, infusion systems, cardiac devices, ventilators, and robotic surgical platforms. Decisions controlling these actuators often depend on aggregated or jointly computed sensor data. The reviewed protocols supporting logical functions, ranking, and secure decision-making provide a cryptographic foundation for actuator-triggering logic. Importantly, integrity guarantees are as critical as confidentiality. Manipulation of distributed computations could result in incorrect actuator behavior. The adversary models explored in the surveyed studies highlight the need for robust defenses in safety-critical systems. Thus, [P]Q-MPC protocols should be evaluated not only for privacy preservation but also for correctness guarantees under adversarial conditions typical of cyber-physical system

Healthcare data are long-lived and highly sensitive. The potential for "harvest now, decrypt later" attacks poses a significant risk to stored medical sensor data and transmitted records. Classical cryptographic mechanisms currently deployed in IoMT systems may become vulnerable under large-scale quantum computing. The limited number of protocols relying on Post-Quantum computational hardness assumptions indicates a research imbalance. While quantum-native MPC protocols dominate the literature, practical deployment in sensor networks may favor Post-Quantum classical solutions due to hardware feasibility and cost considerations. From a healthcare infrastructure perspective, hybrid approaches combining Post-Quantum cryptography with classical MPC may provide a more immediately deployable path toward quantum resilience.

our results show that the diversity of cryptographic tools employed across quantum MPC protocols reveals an experimental phase, with techniques ranging from standard QKD schemes (e.g., PS1, PS5, PS7, PS8) to more specialized or hybrid approaches such as oblivious QKD (PS18) and semi-quantum key distribution (PS6). Similarly, encryption methods span from the widely used quantum one-time pad to more niche solutions like rotation-based encryption (PS5, PS7) and quantum homomorphic encryption (PS2). The variety continues with encoding strategies, which include entanglement-based obfuscation (e.g., PS9–PS12), quantum walks (PS15), and even classical elements like Bloom filters (PS8).

A practical design shift is evident in the preference for third-party-assisted architectures, found in over half of the surveyed protocols (e.g., PS1, PS2, PS4, PS6). These models often delegate quantum operations to a central server while allowing clients to remain classical or semi-quantum, making implementation more feasible given the current limitations of quantum hardware. However, this trend introduces new considerations regarding trust and adversarial capabilities, particularly where assumptions about non-collusion or semi-honest behavior are involved (e.g., PS5, PS9).

In terms of supported functionality, most protocols focus on foundational tasks such as set intersection (PS7, PS14) and basic arithmetic operations (PS10, PS15). This reflects a cautious and incremental development strategy aligned with the limited scale and reliability of near-term quantum devices. More expressive functionalities, such as general circuit evaluation or secure function computation with composability guarantees, remain rare and largely theoretical (PS4). Experimental validation has improved over time but still remains inadequate for most protocols. Among the 20 studies, 12 reported some form of implementation or simulation (e.g., PS5, PS8, PS11, PS17). However, these implementations typically target small-scale settings and omit analysis of scalability, error tolerance, and execution overhead.

Looking forward, several research directions could help advance the field. There is a clear need to design and benchmark MPC protocols using Post-Quantum assumptions such as lattice or code-based hardness. Further, a deeper analysis of third-party models is essential to understand how their inclusion affects privacy guarantees and trust assumptions. Enhancing robustness against actively malicious adversaries, as tackled in a few works (e.g., PS4, PS19), is also crucial for deployment in adversarial environments. Finally, experimental validation should extend beyond proof-of-concept implementations to include metrics such as scalability, noise resilience, and real-world performance. In summary, while [P]Q-MPC protocols have made significant conceptual advances, they remain in a formative stage. Bridging the gap between theoretical soundness and practical viability will be key to unlocking their full potential in secure and scalable quantum-era applications.

7 Limitations

Several limitations may affect the comprehensiveness and accuracy of this SLR. Below, we outline these limitations and the mitigation strategies adopted to minimize their impact.

- **Terminological Inconsistency in the [P]Q-MPC Field** The terminology used to describe quantum or Post-Quantum MPC protocols is not yet standardized. For example, some studies may describe their work under broader terms such as "secure quantum computation" or "delegated quantum computation" without explicitly using MPC-related keywords. To address this, we designed a comprehensive and inclusive search string covering known variations of relevant terms and conducted manual inspections of potentially ambiguous studies to determine their relevance.
- **Study Selection Bias** The process of selecting primary studies involves subjective judgments, especially in interpreting inclusion and exclusion criteria. To reduce potential bias, a structured multi-stage selection process was applied. Initially, studies were screened based on titles and abstracts, followed by full-text reviews. This process was carried out independently by two researchers, and disagreements were resolved through discussion to ensure consistency and fairness in study inclusion.
- **Interpretation and Categorization Subjectivity** The extraction and categorization of data—such as adversary models, cryptographic primitives, or functional capabilities—require interpretation of the authors' intentions, which may not always be explicit. To mitigate this, all extracted data were cross-validated, and ambiguous cases were discussed to reach consensus. Nevertheless, some degree of subjectivity in interpretation is unavoidable.

8 Conclusion

This systematic literature review examined the current state of Post-Quantum and quantum secure multiparty computation ([P]Q-MPC) protocols and analyzed their relevance to distributed computing in the quantum era. By systematically reviewing twenty primary studies published between 2022 and early 2025, this work categorized existing protocols according to their cryptographic assumptions, primitives, supported functionalities, architectural models, adversary models, and experimental validation status.

Beyond providing a structured synthesis of recent advances, this review contextualized [P]Q-MPC within the domain of sensor and actuator networks, with particular emphasis on healthcare Internet of Things (IoMT) systems. The findings demonstrate that many existing protocols already implement core functionalities required in distributed healthcare environments, including private set intersection, aggregation, extremum detection, and logical decision-making. These operations align closely with practical requirements such as privacy-preserving patient data aggregation, anomaly detection in remote monitoring systems, and secure triggering of medical actuators.

The architectural trends identified in the literature—especially the prevalence of third-party-assisted models—mirror real-world edge- and cloud-assisted sensor network deployments. However, reliance on semi-honest assumptions and limited analysis of collusion risks highlights the need for stronger adversarial modeling in safety-critical environments. In healthcare actuator systems, where computed decisions may directly influence therapeutic interventions, robustness against malicious behavior is essential.

Although progress has been made in experimental validation, most implementations remain small-scale and proof-of-concept in nature. Critical aspects relevant to sensor and actuator networks—such as scalability, latency, communication overhead, energy efficiency, and long-term operational resilience—require further investigation. In addition, the imbalance between quantum-native protocols and Post-Quantum computational approaches suggests an opportunity for developing lightweight, deployable solutions suitable for resource-constrained medical devices. As quantum computing continues to evolve, the long-term confidentiality of healthcare data becomes a strategic concern. Integrating quantum-resilient MPC mechanisms into sensor and actuator infrastructures offers a promising pathway toward secure distributed analytics and automated decision systems capable of withstanding future cryptographic threats.

Overall, this review establishes a foundation for bridging advanced cryptographic research and practical deployment in next-generation sensor and actuator networks. Future work should prioritize scalable implementations,

rigorous threat modeling under realistic IoT conditions, and hybrid architectures that combine Post-Quantum security with existing healthcare infrastructures. Such efforts will be essential for enabling privacy-preserving, trustworthy, and quantum-resilient medical cyber-physical systems.

Acknowledgment

The author would like to thank King Fahd University of Petroleum and Minerals, Dhahran, Saudi Arabia, for supporting this research.

References

[1] I. Zhou, F. Tofigh, M. Piccardi, M. Abolhasan, D. Franklin, and J. Lipman, "Secure multi-party computation for machine learning: A survey," *IEEE Access*, 2024.

[2] H. K. Alper and A. Küpçü, "Optimally efficient multi-party fair exchange and fair secure multi-party computation," *ACM Transactions on Privacy and Security*, vol. 25, no. 1, pp. 1–34, 2021.

[3] C. Zhao, S. Zhao, M. Zhao, Z. Chen, C.-Z. Gao, H. Li, and Y.-a. Tan, "Secure multi-party computation: theory, practice and applications," *Information Sciences*, vol. 476, pp. 357–372, 2019.

[4] C. K. Gitonga, "The impact of quantum computing on cryptographic systems: Urgency of quantum-resistant algorithms and practical applications in cryptography," *European Journal of Information Technologies and Computer Science*, vol. 5, no. 1, pp. 1–10, 2025.

[5] A. Agarwal, J. Bartusek, V. Goyal, D. Khurana, and G. Malavolta, "Post-quantum multi-party computation," 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 40*. Springer, 2021, pp. 435–464.

[6] A. Ashwini, V. Kavitha, and S. Balasubramaniam, "Interconnected healthcare 5.0 ecosystems: Enhancing patient care using sensor networks," *Networked Sensing Systems*, pp. 225–246, 2025.

[7] N. Akhtar, S. Rahman, H. Sadia, and Y. Perwej, "A holistic analysis of medical internet of things (miot)," *Journal of Information and Computational Science*, vol. 11, no. 4, pp. 209–222, 2021.

[8] X. Chen, C. Hu, T. Xiang, P. Hu, J. Zhang, and X. Li, "Secure and efficient data collection and transmission scheme for healthcare services in wireless medical sensor network," *IEEE Transactions on Dependable and Secure Computing*, 2026.

[9] D. Kadam, A. P. Budaragade, U. Salunkhe, U. P. Gurav, and A. Patil, "Internet of medical things: Architecture, trends, challenges, and the evolution towards iomt 5.0," *Computer Networks and Communications*, pp. 148–163, 2025.

[10] P. Tamilselvi, V. Lathika, S. Jayachitra, S. Arunkumar, M. Balasubramani, and V. Kalaichelvi, "Secure multi-party computation for collaborative data analysis in network security," in *2024 international conference on intelligent and innovative technologies in computing, electrical and electronics (IITCEE)*. IEEE, 2024, pp. 1–5.

[11] A. M. Tawfik, A. Al-Ahwal, A. S. T. Eldien, and H. H. Zayed, "Pricollabanalysis: privacy-preserving healthcare collaborative analysis on blockchain using homomorphic encryption and secure multiparty computation," *Cluster Computing*, vol. 28, no. 3, p. 191, 2025.

[12] L.-Y. Ma and N. Soin, "Recent progress in printed physical sensing electronics for wearable health-monitoring devices: A review," *IEEE Sensors Journal*, vol. 22, no. 5, pp. 3844–3859, 2022.

[13] S. D. Pasham, "Privacy-preserving data sharing in big data analytics: A distributed computing approach," *The Metascience*, vol. 1, no. 1, pp. 149–184, 2023.

[14] B. Oluwafemi, "Privacy-preserving computation (homomorphic encryption, mpc)," *Journal of Contemporary Educational Research*, vol. 7, pp. 111–122, 2025.

[15] V. S. Naresh, A. Venkata Raju, and O. Srinivasa Rao, "Secure multiparty computation for privacy-preserving machine learning in healthcare: A comprehensive survey," *Wiley Interdisciplinary Reviews: Computational Statistics*, vol. 17, no. 3, p. e70046, 2025.

[16] N. Primeau, R. Falcon, R. Abielmona, and E. M. Petriu, "A review of computational intelligence techniques in wireless sensor and actuator networks," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 4, pp. 2822–2854, 2018.

[17] M. M. Madine, K. Salah, R. Jayaraman, I. Yaqoob, Y. Al-Hammadi, S. Ellahham, and P. Calyam, "Fully decentralized multi-party consent management for secure sharing of patient health records," *Ieee Access*, vol. 8, pp. 225 777–225 791, 2020.

[18] R. Borges, B. Ferreira, C. M. Antunes, M. Maximiano, R. Gomes, V. Távora, M. Dias, R. C. Bezerra, and P. Domingues, "Using secure multi-party computation to create clinical trial cohorts," *Journal of Cybersecurity and Privacy*, vol. 6, no. 1, p. 2, 2025.

[19] X. Xie, G. Cheng, H. Liu, L. Luo, B. Ren, and D. Guo, "Coedge: A collaborative architecture for efficient task offloading among multiple edge service providers," *IEEE Internet of Things Journal*, 2025.

[20] F. Boudot, P. Gaudry, A. Guillevic, N. Heninger, E. Thomé, and P. Zimmermann, "The state of the art in integer factoring and breaking public-key cryptography," *IEEE Security & Privacy*, vol. 20, no. 2, pp. 80–86, 2022.

[21] M. Adil, A. Ali, T. T. Tin, A. Farouk, S. Al-Kuwari, H. Song, Z. Jin *et al.*, "Quantum computing and the future of healthcare internet of things security: Challenges and opportunities," *IEEE Internet of Things Journal*, 2025.

[22] X. Lv, S. Rani, S. Manimurugan, A. Slowik, and Y. Feng, "Quantum-inspired sensitive data measurement and secure transmission in 5g-enabled healthcare systems," *Tsinghua Science and Technology*, vol. 30, no. 1, pp. 456–478, 2024.

[23] M. SaberiKamarposhti, K.-W. Ng, F.-F. Chua, J. Abdullah, M. Yadollahi, M. Moradi, and S. Ahmadpour, "Post-quantum healthcare: A roadmap for cybersecurity resilience in medical data," *Heliyon*, vol. 10, no. 10, 2024.

[24] W. Du and M. J. Atallah, "Secure multi-party computation problems and their applications: a review and open problems," in *Proceedings of the 2001 workshop on New security paradigms*, 2001, pp. 13–22.

[25] D. Feng and K. Yang, "Concretely efficient secure multi-party computation protocols: survey and more," *Security and Safety*, vol. 1, p. 2021001, 2022.

[26] I. Gamiz, C. Regueiro, O. Lage, E. Jacob, and J. Astorga, "Challenges and future research directions in secure multi-party computation for resource-constrained devices and large-scale computations," *International Journal of Information Security*, vol. 24, no. 1, pp. 1–29, 2025.

[27] D. Morales, I. Agudo, and J. Lopez, "Private set intersection: A systematic literature review," *Computer Science Review*, vol. 49, p. 100567, 2023.

[28] B. Kitchenham, L. Madeyski, and D. Budgen, "Segress: Software engineering guidelines for reporting secondary studies," *IEEE Transactions on Software Engineering*, vol. 49, no. 3, pp. 1273–1298, 2022.

[29] B. Kitchenham, O. P. Brereton, D. Budgen, M. Turner, J. Bailey, and S. Linkman, "Systematic literature reviews in software engineering–a systematic literature review," *Information and software technology*, vol. 51, no. 1, pp. 7–15, 2009.

[30] J. Wen, S. Li, Z. Lin, Y. Hu, and C. Huang, "Systematic literature review of machine learning based software development effort estimation models," *Information and software technology*, vol. 54, no. 1, pp. 41–59, 2012.

[31] T. Mohanty, V. Srivastava, S. K. Debnath, and P. Stănică, "Quantum secure protocols for multiparty computations," *Journal of Information Security and Applications*, vol. 90, p. 104033, 2025.

[32] S. Li, X.-Q. Cai, and T.-Y. Wang, "Secure multiparty computation for maximum and minimum values based on quantum homomorphic encryption," *Optics Express*, vol. 33, no. 7, pp. 16 263–16 274, 2025.

[33] Z. Shan, L. Zhang, Q. Wu, Q. Lai, and F. Guo, "Fast post-quantum private set intersection from oblivious pseudorandom function for mobile social networks," *Journal of Systems Architecture*, p. 103346, 2025.

[34] T. Kapourniotis, E. Kashefi, D. Leichtle, L. Music, and H. Ollivier, "Asymmetric secure multi-party quantum computation with weak clients against dishonest majority," *Quantum Science and Technology*, 2025.

[35] X. Huang, W. Zhang, and S. Zhang, "Practical quantum protocols for blind millionaires' problem based on rotation encryption and swap test," *Physica A: Statistical Mechanics and its Applications*, vol. 637, p. 129614, 2024.

[36] Y.-P. Chi, Y. Zhang, K.-J. Zhang, G. Xu, and X.-B. Chen, "A new protocol for semi-quantum private set of intersection and union mixed cardinality for any tripartite based on bell states," *Advanced Quantum Technologies*, vol. 7, no. 9, p. 2400137, 2024.

[37] X. Huang, W. Zhang, and S. Zhang, "Quantum multi-party private set intersection using single photons," *Physica A: Statistical Mechanics and its Applications*, vol. 649, p. 129974, 2024.

[38] R.-H. Shi and X.-Q. Fang, "Quantum scheme for privacy-preserving range max/min query in edge-based internet of things," *IEEE Transactions on Network and Service Management*, 2024.

[39] Z. Rahmani, A. H. M. N. Pinto, and L. M. D. C. S. Barbosa, "Secure two-party computation via measurement-based quantum computing," *Quantum Information Processing*, vol. 23, no. 6, p. 221, 2024.

[40] Y. Zhang, Y. Yao, H. Sun, K. Zhang, and T. Song, "A new hybrid protocol that simultaneously achieves quantum multiparty summation and ranking," *Advanced Quantum Technologies*, vol. 7, no. 6, p. 2400078, 2024.

[41] W.-J. Liu and Z.-X. Li, "Secure and efficient two-party quantum scalar product protocol with application to privacy-preserving matrix multiplication," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 70, no. 11, pp. 4456–4469, 2023.

[42] R. B. Christensen and P. Popovski, "Private product computation using quantum entanglement," *IEEE Transactions on Quantum Engineering*, vol. 4, pp. 1–9, 2023.

[43] Z.-X. Li, Q. Yang, B. Feng, and W.-J. Liu, "Quantum privacy-preserving two-party circle intersection protocol based on phase-encoded query," *International Journal of Theoretical Physics*, vol. 62, no. 7, p. 138, 2023.

[44] T. Mohanty and S. K. Debnath, "An information-theoretically secure quantum multiparty private set intersection," *Journal of Information Security and Applications*, vol. 78, p. 103623, 2023.

[45] J. Joseph and S. T. Ali, "Quantum secure multiparty summation based on quantum walks," in *2023 International Conference on Quantum Technologies, Communications, Computing, Hardware and Embedded Systems Security (iQ-CCHESS)*. IEEE, 2023, pp. 1–5.

[46] R.-h. Shi and X.-q. Fang, "Edge-assisted quantum protocol for secure multiparty logical and its applications," *Iscience*, vol. 26, no. 7, 2023.

[47] R.-H. Shi and Y.-F. Li, "A feasible quantum sealed-bid auction scheme without an auctioneer," *IEEE Transactions on Quantum Engineering*, vol. 3, pp. 1–12, 2022.

[48] ——, "Quantum private set intersection cardinality protocol with application to privacy-preserving condition query," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 69, no. 6, pp. 2399–2411, 2022.

[49] ——, "Quantum protocol for secure multiparty logical and with application to multiparty private set intersection cardinality," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 69, no. 12, pp. 5206–5218, 2022.

[50] R.-h. Shi and Y.-f. Li, "Privacy-preserving quantum protocol for finding the maximum value," *EPJ Quantum Technology*, vol. 9, no. 1, pp. 1–14, 2022.

A Primary Studies

Table 10 presents all primary studies included in this systematic literature review after quality assessment.

Table 10: Primary studies considered in this SLR

Study ID	Title	Ref
PS1	Quantum secure protocols for multiparty computations	[31]
PS2	Secure multiparty computation for maximum and minimum values based on quantum homomorphic encryption	[32]
PS3	Fast Post-Quantum privateset intersection from oblivious pseudorandom function for mobile social networks	[33]
PS4	Asymmetric secure multi-party quantum computation with weak clients against dishonest majority	[34]
PS5	Practical quantum protocols for blind millionaires' problem based on rotation encryption and swap test	[35]
PS6	A New Protocol for Semi-quantum Private Set of Intersection and Union Mixed Cardinality for Any Tripartite Based on Bell States	[36]
PS7	Quantum multi-party private set intersection using single photons	[37]
PS8	Quantum Scheme for Privacy-Preserving Range MAX/MIN Query in Edge-Based Internet of Things	[38]
PS9	Secure two-party computation via measurement-based quantum computing	[39]
PS10	A New Hybrid Protocol that Simultaneously Achieves Quantum Multiparty Summation and Ranking	[40]
PS11	Secure and Efficient Two-Party Quantum Scalar Product Protocol With Application to Privacy-Preserving Matrix Multiplication	[41]
PS12	Private Product Computation Using Quantum Entanglement	[42]
PS13	Quantum Privacy-preserving Two-party Circle Intersection Protocol Based on Phase-encoded Query	[43]
PS14	An information-theoretically secure quantum multiparty private set intersection	[44]
PS15	Qantum Secure Multiparty Summation Based on Quantum Walks	[45]
PS16	Edge-assisted quantum protocol for secure multiparty logical AND its applications	[46]
PS17	A Feasible Quantum Sealed-Bid Auction Scheme Without an Auctioneer	[47]
PS18	Quantum Private Set Intersection Cardinality Protocol with Application to Privacy-Preserving Condition Query	[48]
PS19	Quantum Protocol for Secure Multiparty Logical AND With Application to Multiparty Private Set Intersection Cardinality	[49]
PS20	Privacy-preserving quantum protocol for finding the maximum value	[50]