Quantum SMPC: Rich in theory, limited in practice

A systematic review of quantum secure multi-party computation

Nicoleta Dobrică[1]
Supervisors: Dr. Zeki Erkin[1]**, Dr. Roland Kromes**[1]
[1]EEMCS, Delft University of Technology, The Netherlands

A Thesis Submitted to EEMCS Faculty Delft University of Technology,
In Partial Fulfilment of the Requirements
For the Bachelor of Computer Science and Engineering
June 22, 2025

Name of the student: Nicoleta Dobrică
Final project course: CSE3000 Research Project
Thesis committee: Dr. Zeki Erkin, Dr. Roland Kromes, Dr. Xucong Zhang

An electronic version of this thesis is available at http://repository.tudelft.nl/.

Abstract

Secure Multi-Party Computation (SMPC) is a widely-used cryptographic tool for privacy-preserving data analysis. The progress in the field of quantum computing has led to the development of Quantum SMPC (QSMPC), which promises information-theoretic security based on physics laws. There is a significant number of proposed protocols. However, as the number of theoretical protocols grows, their practical viability remains unclear. Our paper presents a systematic literature review of 37 recent QSMPC protocols to assess the state of the field, focusing on protocol functionality, quantum resource requirements, privacy-ensuring techniques, and feasibility on current technologies. Our analysis reveals a plethora of innovative theoretically-private protocols, constrained by significant practical issues. We found that protocols tend to rely on a core set of quantum resources, including entangled states (Bell, GHZ), Quantum Key Distribution, and decoy particles to ensure security. We also observe a frequent reliance on a semi-honest third party. Most importantly, we identify a noticeable gap in feasibility. 19 out of 37 of the papers surveyed provide no clear discussion on the practicality of the proposed protocols. The papers that do discuss this topic describe small-scale simulations, which may require algorithmic compromises and are tested in ideal conditions only. Our findings highlight a gap between theory and practice, suggesting that real-world application of the protocols is not yet possible, given the current state of quantum hardware.

1 Introduction

In our increasingly interconnected world, the ability to derive insights from distributed data is of high importance. From collaborative medical research [1] to financial fraud detection [2], multi-party computation represents a significant prerequisite. Secure Multi-Party Computation (SMPC) is a cryptographic technique which addresses this issue, allowing two or more parties in a distributed computing environment to jointly compute a function based on their private inputs [3]. The core principles and requirements characterizing SMPC are privacy, correctness, independence of inputs, guaranteed output delivery and fairness.

However, in recent years, the rapid development of quantum computing has raised several questions related to the security of existing protocols. Shor's algorithm for integer factorization is commonly mentioned on this topic [4]. Therefore, the motivation for adapting SMPC to quantum computing can be traced to two reasons. First of all, there is a need to design protocols resistant to attacks from quantum adversaries. Secondly, quantum computing offers the possibility of developing protocols whose privacy guarantees are rooted in laws of physics, instead of computational assumptions that may be broken. This would allow for information-theoretic security, such that the security of said protocols could not be broken.

The development of Quantum Secure Multi-Party Computation (QSMPC) has progressed significantly over the past years. Foundational work demonstrated how quantum states could be split and reconstructed using entanglement [5], leading to the first verifiable quantum secret sharing scheme [6]. This study led to the first generalized protocol for multi-party quantum computation [7], establishing a viable pathway for secure quantum collaboration. Since then, the field has expanded, with researchers proposing protocols with diverse goals, built using techniques and protocols like quantum homomorphic encryption (QHE) [8], quantum key distribution (QKD) [9], quantum one-time pad (QOTP) [10] or Shor's algorithm [11].

There is an increasing number of proposed QSMPC protocols that have yet to be systematically examined and compared. Given the current limitations of today's Noisy

Intermediate-Scale Quantum (NISQ) hardware, it is of particular interest to investigate how protocols have accounted for the practical implementation issues. Liu et al. [12] have undertaken a survey of Quantum Private Comparison protocols, classifying them based on the quantum principles they leverage. However, the study dates from more than ten years ago and is limited to comparison protocols. Another paper by Kumar et al. [13] compares specific QSMPC protocols based on metrics like communication overhead, computational resources and security guarantees. Nevertheless, they only focus on six protocols, without employing a systematic selection process. Consequently, a systematic literature review has not yet been attempted, to our knowledge, in particular one to also raise the issue of feasibility.

Our aim is to analyze how secure multi-party computation is being adapted to quantum computing, addressing the significant gap in literature. Conducting such a literature review provides insights for understanding how quantum paradigms impact privacy. We are able to assess the current state of development for QSMPC and identify the technical challenges that still remain, in the hopes of guiding future research toward practical solutions.

To accomplish this goal, our main contribution is as follows. We provide a structured overview of the quantum adaptations of classical secure multi-party computation techniques from the last five years. We classify these schemes based on the different functionalities they attempt to perform. We examine the quantum resources and techniques these protocols rely on, and investigate the mechanisms through which they achieve privacy. Finally, we evaluate the feasibility of the schemes under current technology. By feasibility, we refer to the possibility of running the proposed protocols in the present day, taking into account the number of participants and qubits they have been tested with. A lot of the proposed quantum protocols lean towards the theoretical, due to a lack of suitable technologies. However, part of them have been successfully simulated using IBM Qiskit, while for the others, it is worth seeing what are the main barriers hindering their implementation.

We organized the paper in seven sections. Following the introduction, Section 2 presents preliminary information on quantum concepts that will be mentioned throughout the paper. Section 3 describes the methodology that was used to conduct the survey. Section 4 provides the analysis of QSMPC protocols according to the papers surveyed. Section 5 focuses on the ethics behind the research. Section 6 serves as a discussion of the obtained results and limitations, while Section 7 concludes the report, including suggestions for future work.

2 Preliminaries

In this section, we introduce the notions that we will mention in the next sections of the paper. We include information on secret sharing and homomorphic encryption. We also introduce fundamental concepts, tools, commonly used operations, and important protocols or techniques for quantum computing.

2.1 Secret sharing and homomorphic encryption

In **Shamir's secret sharing** protocol, a secret is split into multiple shares, which are given to participants. To recover the secret, only a predetermined fraction of participants is required [14]. For this purpose, the third party computes a polynomial of degree $t-1$, where t represents the number of shares that are necessary to recover the secret. The reconstruction process relies on the Lagrange interpolation of the polynomial at the origin.

Homomorphic encryption is a cryptographic technique which allows computations to be done directly on the ciphertext. Upon decryption, the result would be the same as after performing the same computation on the unencrypted message [15].

2.2 Fundamental quantum concepts

A **qubit** is the basic unit of quantum information [16]. A qubit is a two-level system, while a qudit is a d-level system (also called d-level or d-dimensional states) [17]. The term q-qubit state can be used to refer to a system composed of q individual qubits. The **global phase** is a phase factor that applies to an entire quantum state and is not physically measurable [18]. The **Bloch Sphere** is often used as a visual representation of the state of one qubit, as can be seen in Figure 1.

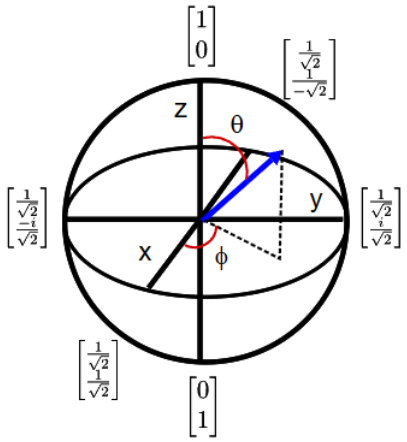

Figure 1: Bloch Sphere. Source: From [19].

The **No-Cloning Theorem** is a fundamental principle that claims it is impossible to create an identical copy of an arbitrary unknown quantum state [20].

Entanglement is a quantum phenomenon in which the quantum states of two or more particles cannot be described independently of each other, even though the individual particles may be separated [16]. **Superposition** is the principle that a quantum system can exist in multiple states at the same time. That state is a combination of all possible states. A system is in a **mixed state** if it is unclear what state it was prepared in [21]. The entangled states mentioned in this paper are:

- **Bell states**: A set of four specific, maximally entangled two-qubit states [22].

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \quad (1) \qquad |\Phi^-\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) \quad (2)$$

$$|\Psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) \quad (3) \qquad |\Psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) \quad (4)$$

- **Greenberger-Horne-Zeilinger (GHZ) states**: A type of entangled state involving three or more qubits [23].
- **Cat States**: A generalization of Bell states from two qudits to n qudits [24].

Quantum Walk (QW) States are quantum states that evolve according to the rules of a quantum walk, a quantum analogue of a classical random walk [25].

Measurement is the act of observing a quantum system, which collapses its superposition into a single, definite state. This leads to the **Measurement-Disturbance** property, which claims that measuring a quantum system generally disturbs it, altering its state [26]. Bell measurements refer to determining which Bell state the system is in [27].

2.3 Quantum gates and operations

Unitary Operations/Transformations are represented by unitary matrices, which are norm-preserving and maintain the same probabilities of the quantum states [28].

We consider two types of gates. We placed the mathematical representations of Hadamard and Pauli gates and rotation and shift operators below each of their definitions.

2.3.1 Single-Qubit Gates

- **Hadamard Gate (H)**: Creates a superposition through the transformation of the $|0\rangle$ state to the equal superposition of the $|0\rangle$ and $|1\rangle$ states [29].

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \tag{5}$$

- **Pauli Gates (X, Z, Y)**: A set of fundamental gates corresponding to bit-flips (X), phase-flips (Z), and both (Y) [29]. The Y gate is equivalent to applying both the X and Z gates and a global phase.

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \tag{6} \qquad Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \tag{7} \qquad Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \tag{8}$$

- **Rotation Operations**: A general class of gates that rotate a qubit's state on the Bloch sphere [29].

$$R_{\hat{n}}(\theta) = e^{-i\theta\,\hat{n}\cdot\vec{\sigma}/2} \tag{9}$$

- **Identity Operation**: A gate corresponding to the identity matrix, often used for placeholder or alignment purposes [30].

- **Shift Operations**: Operations that shift the basis states of a qudit [31].

$$QS_k = \sum_{j=0}^{d-1} |j+k\rangle\langle j| \tag{10}$$

2.3.2 Multi-Qubit Gates

- **Controlled-NOT (CNOT) Gate**: A two-qubit gate that flips the target qubit if the control qubit is in a specific state [32].

- **SWAP Gate**: A two-qubit gate that swaps the states of the two qubits [32].

- **Toffoli Gate**: Sometimes referred to as Controlled CNOT, it is a three qubit gate that flips the target qubit if both control qubits are in a specific state [32].

Quantum Fourier Transform (QFT): The quantum analogue of the discrete Fourier transform [33]. The QFT transforms between two bases, from the computational basis to the Fourier basis. It is mathematically defined as:

$$\mathrm{QFT}|x\rangle = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{2\pi i x k/N} |k\rangle \tag{11}$$

2.4 Quantum protocols and techniques

Quantum Key Distribution (QKD): A protocol that uses quantum mechanics to establish a secure shared key between two parties [34].

Shor's Algorithm: A quantum algorithm which efficiently solves the problems of integer factorization, discrete logarithm and period-finding [4]. However, the number of qubits it requires for it to be applicable to large numbers cannot be supported by current technology.

Quantum One-Time Pad: A quantum encryption scheme analogous to the classical one-time pad, providing information-theoretic security [10]. It hides the state of a qubit by applying consecutive X or Z operations based on a generated key.

Decoy States/Particles: A security technique where decoy states are inserted into a stream of quantum signals to detect eavesdropping [35]. The sender tells the receiver the locations of the particles and the measurement bases, then the receiver measures the particles accordingly and verifies the results with the sender. Depending on the protocol, there is a considerable chance an attacker would detect a decoy particle, which will introduce errors in the message they intercept and might be detected by the sender.

2.5 Quantum software development kit

Due to limited access to the necessary resources, researchers frequently employ quantum software development kits (SDK) to test out the implementation of their theoretical proposed protocols. One of the most popular quantum SDKs is the open-source IBM Qiskit [36]. It allows the execution of quantum circuits and access to quantum processing units (QPU). As of the writing of this paper, a QPU can use up to 156 qubits [37].

3 Methodology

Systematic reviews offer the key advantages of providing overviews of existing research, while minimizing individual biases. This approach enables the clear tracing of the research process and supports reproducibility. We considered two options for the methodology, PRISMA [38] and snowballing [39]. PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) represents a set of guidelines for researchers to follow when conducting systematic reviews, while snowballing involves starting from a reduced set of papers and expanding the search with other studies they reference or are cited by. As PRISMA encourages the use of structured documentation, to visualize the identification, screening, and selection of relevant literature, and does not rely on a well-chosen starting point, we decided it would be more suitable for a systematic, reproducible literature review. In the next subsections, we explain how we constructed the search query and provide details on the paper selection process.

3.1 Search query

SMPC is a vast field, with various subcategories. We had to reduce them, for the survey to be feasible within the given time frame. Therefore, we composed the search query in two steps. We used an initial, more general query to identify the most common subcategories of SMPC. Then, we adapted it to include the most common results, which brought us to the final version. The precise search queries can be found in Appendix A.1.

It is worth noting that a significant number of papers reference quantum-safe protocols or post-quantum cryptography, which fall outside the scope of this survey. However, because these terms appear in both relevant and irrelevant papers to our survey, we could not exclude them through query filtering without risking the omission of valid results. As a result, we had to manually exclude papers by reviewing their titles and abstracts.

3.2 Selection process

The academic databases that we used to identify relevant literature are Scopus, Web of Science and IEEE Xplore. We used the same query for each and the results were filtered to have the publication date between 2020 and 2025. Scopus also allowed for the option of filtering results based on language, so English-only results were displayed. Figure 2 shows the full selection process. The exact selection criteria used to filter out papers can be found in Appendix A.2. In the end, 37 papers were considered for the literature review.

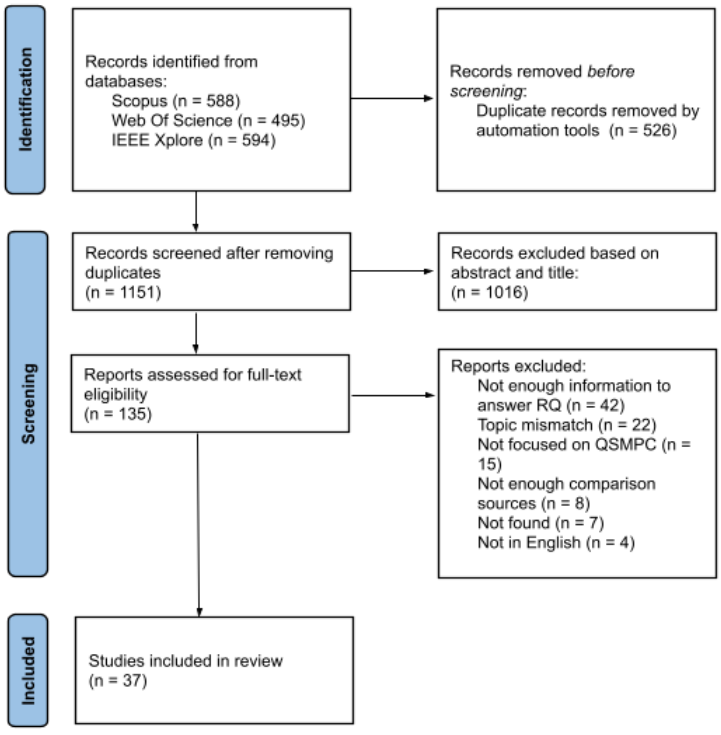

Figure 2: PRISMA flowchart diagram. Source: Adapted from [40].

4 Analysis of QSMPC protocols

In this section, we provide a summary of the findings of the 37 selected papers on QSMPC. The proposed protocols vary across the functionalities they accomplish. For a clearer overview, we constructed Table 1, including information on the quantum resources, use of third parties, privacy-ensuring techniques, and feasibility for each paper. Papers account for both internal and external attacks when discussing privacy. A common assumption in all but one paper is the existence of a secure noiseless and lossless quantum channel. The table is structured by publication year of the included papers, to identify trends within each year. In the rest of this section, we elaborate on these insights, grouping discussion of papers based on their protocol functionality. The main categories that we identified are multiplication and summation, auction and voting, set operations, comparison operations and others (the last subsection includes protocols that we could not include in any of the previously mentioned groups and are too few in number to have their own category).

Table 1: Table of papers included in the literature review. Feasibility NA means the problem of feasibility was not tackled within the paper, while small-scale feasible means the protocol was simulated using IBM Qiskit or a similar platform with a reduced number of qubits and participants.

Paper	**Techniques and resources**	**Third party**	**What ensures privacy**	**Feasibility**
		2020		
[41]	Secret sharing, entangled states, QFT, Pauli gates	No	Entanglement	Small-scale feasible, switch QFT to H
[42]	QKD, Bell states, rotations	Yes	Decoy particles, private permutations	NA
		2021		
[43]	Secret sharing, t-particle entangled states, QFT, Pauli gates	No	Entanglement	NA
[44]	Secret sharing, q-qubit states, QFT, CNOT	No	No information about the global state	NA
[31]	d-dimensional Bell states, shift operation	No	Measurement basis, decoy particles, random number sequences, no-cloning theorem	NA
[24]	d-level Bell states, cat states	Yes	Decoy particles, secrecy of keys	NA
[45]	d-level Bell states	Yes	Decoy particles, no access to shared state	NA
[18]	Secret sharing, entangled states, H and CNOT gates, QFT operations	No	Information hidden in global phase	Small-scale feasible
[33]	QFT operations, particle sequences	Yes	Decoy particles, entanglement	Not feasible
[9]	QKD, GHZ states, H gates	Yes	Decoy particles, measurement basis, secrecy of keys	NA
[46]	n-qubit entangled states, CNOT gates	No	Encoding method, no-cloning theorem	NA
		2022		
[47]	Secure multi-party disjunction protocol, Bell states, Pauli gates	No	Mixed states	Small-scale feasible
		2023		
[48]	Secret sharing, d-dimensional GHZ states	Yes	Decoy particles, hash functions, secrecy of keys	NA
[49]	QKD, unitary operations, H gates, single photon states	Yes	Measurement basis, decoy particles	NA
[25]	QW states, H gates, shift operations	Yes	Secret number of step evolutions	NA

[50]	Multi-party authenticated summation scheme, single photon states	No	Measurement disturbance	Small-scale feasible
[30]	QHE, Toffoli gate, QOTP algorithm, single photon states	Yes	Decoy particles, mixed states	Small-scale feasible
[35]	Unitary operations, X and CNOT gates, single photon states	Yes	Decoy particles, particle shuffling	NA
[10]	Swap operations, quantum One Time Pad, Pauli gates, photon sequences	No	Mixed states	NA
[11]	Shor's algorithm, CNOT gates, inverse QFT, q-qubit particles	No	Entanglement	NA
[51]	d-level 2-particle entangled states, shift operations	Yes	Decoy particles, measurement disturbance	NA
[52]	QSMC AND protocol, QKD, entangled states, rotation operations	Yes	Measurement basis, secrecy of keys	Small-scale feasible, Bell measurement replaced by single particle measurement
[53]	d-qubit particles, QFT, rotation operations	No	Phase-information not obtainable under entanglement	Small-scale feasible, custom modular multiplication gate
			2024	
[15]	Homomorphic encryption, unitary transformations, q-qubit states	No	Measurement basis, homomorphic encryption	NA
[54]	d-dimensional Bell states, Pauli gates	Yes	Decoy particles	NA
[23]	GHZ states, Z and X gates	Yes	Decoy particles	NA
[55]	Quantum encryption, rotation operations, single photon states, QKD	Yes	Decoy particles, no-cloning theorem	Small-scale feasible
[56]	QKD, Bell states, rotation operations	Yes	Decoy particles, unidentified rotations	Small-scale feasible, replaced Bell measurement by single-particle measurement
[57]	Quantum sequences, Quantum Fourier adder	Yes	Decoy particles, mixed states	Small-scale feasible
[58]	Shift operations, d-dimensional quantum states, X, Z and H gates	Yes	Decoy particles, random encryption passwords	Small-scale feasible
[59]	QKD, unitary operations, H gates, photon sequences	Yes	Decoy particles	NA
[60]	GHZ states, phase rotations, Pauli-Z rotation, Bell states	Yes	No-cloning and measurement-disturbance properties	Small-scale feasible
[61]	Bell states, rotation operations	Yes	Measurement basis	Small-scale feasible
			2025	
[62]	Bell states, unitary operations, rotations, QKD	Yes	Decoy particles, secrecy of unitary operations	Small-scale feasible, Bell measurement replaced with CNOT and H gates
[63]	d-level single photon states, shift operations, unitary operations	Yes	Decoy particles, secrecy of unitary operations	Small-scale feasible, noise taken into account
[64]	Quantum walk states, Hadamard, X, CNOT, Toffoli gates, Quantum Random Number Generator	Yes	Decoy particles, particle shuffling, random numbers	Small-scale feasible
[65]	Quantum private permutation scheme, quantum millionaire subprotocol, Pauli gates, H, CNOT, SWAP gates, inverse QFT, entangled states	Yes	Random vectors, entanglement	Small-scale feasible

4.1 Multiplication and summation protocols

Multiplication and summation are foundational operations in SMPC, therefore the studies targeting them were also the most numerous. The surveyed protocols frequently use secret sharing and employ the computational powers of a third party (TP).

One approach relies on classical secret sharing schemes enhanced by quantum mechanics. Sutradhar et al. propose two such protocols: one for multiplication using Lagrange interpolation [43] and another that uses polynomial encoding and the QFT [44]. These protocols ensure privacy by distributing shares such that individuals or small colluding groups cannot reconstruct the secrets. Their security against intercept attacks is robust, as the transmitted quantum states initially contain no secret information. Another protocol extends this concept to summation [41]. While theoretically sound, its implementation on IBM Qiskit for 15 players required substituting the resource-intensive QFT with a simpler Hadamard gate, due to current technology limitations.

Other protocols employ a semi-honest third party to coordinate the computation. For instance, Li et al. [48] have participants prepare d-dimensional GHZ states, with a TP performing the summation. Security is increased by decoy particles to detect eavesdropping and hash functions to prevent forgery, providing protection against the collusion of up to $n-2$ parties, where n is the total number of participants. Similarly, Wang et al. [24] use a TP to distribute cat states and Bell states, where participants encode data via local measurements, while privacy is again guaranteed through decoy particles. A dynamic protocol is introduced by Luo et al. [15], which combines quantum states with homomorphic encryption and allows the simultaneous computation of both multiplication and summation. This hybrid approach allows a semi-honest TP to verify results and enables parties to be added or removed from the computation. More details about the techniques used for privacy and quantum resources within these protocols are in Table 1.

Another category of protocols relies on passing a quantum state sequentially between participants. In the protocol by Wu et al. [49], each participant successively encodes their data onto a single photon state, with decoy particles and secret measurement basis being used for security reasons. Joseph et al. [25] propose a similar sequential method using quantum walk states. As participants do not know the number of quantum step evolutions done by TP, they cannot retrieve the state of the system, nor use measurement, as the superposition state would collapse, so privacy is also guaranteed.

However, discussion on the feasibility of all but one protocols mentioned in this subsection is limited, as can be seen in Table 1. Most authors comment on the feasibility of different steps of their protocols, but no actual information on a simulation is given.

4.2 Auction and voting protocols

Quantum protocols for auctions and voting aim to ensure privacy and verifiability, even sometimes removing the need for a fully trusted central authority. One scheme by Shi et al. [47] implements a sealed-bid auction without any auctioneer by using a custom secure multi-party disjunction protocol. Bidders collaboratively identify the winning price interval, with privacy of non-winning bids being preserved through the transmission of a mixed state, revealing no information. The feasibility of this approach was demonstrated through a simulation on IBM Qiskit. Another auction protocol uses secret sharing and QFT to jointly compute bid summations [18], ensuring privacy by hiding information in the global phase, which cannot be obtained through an attacker's direct measurement. The individual secret sharing and summation protocols are tested independently using IBM Qiskit.

In the realm of voting, protocols showcase a similar trade-off between distributed trust and third-party assistance. The protocol by Zheng et al. [23] utilizes a TP to prepare a shared GHZ state on which votes are encoded, with decoy particles helping to maintain privacy, but no actual simulation mentioned. In contrast, the anonymous veto voting protocol by

Yu et al. [50] leverages a measurement-device-independent (MDI) framework combined with blockchain for record-keeping. Its privacy comes from the fact that measuring the auxiliary particle of the attacker also changes the detection particle and they cannot learn anything about the votes. The protocol was simulated successfully on IBM Qiskit.

4.3 Set operations protocols

Protocols for private set intersection (PSI), union (PSU), and cardinality have been suggested. Quite commonly, a semi-honest third party prepares, distributes, or analyzes quantum states, as seen in Table 1. For instance, the PSI protocols by Chen et al. [35] and Hou et al. [62] have a TP distribute particles from Bell states, which participants then encode with their set information. Similarly, the PSI cardinality protocol by Liu et al. [30] uses quantum homomorphic encryption, where a TP uses a Toffoli gate to determine equality. It was successfully simulated for two participating parties.

Other approaches employ a sequential model. In the PSI protocol by Huang et al. [55], single-photon sequences are passed in a circle among participants for encoding before returning to the TP for decryption. This minimizes direct communication but centralizes the final computation. The protocol was successfully simulated using 6 participants.

A few protocols rely on different mechanisms. Mohanty et al. [10] propose a PSI protocol where the initiator decrypts the final state after a series of controlled swaps, relying on quantum one-time pad encryption of mixed states for security. Similarly, the protocol for PSI in paper [33] also has the third party prepare particle sequences, which the participants perform QFT operations on according to their individual strings. The PSU protocol by Liu et al. [11] takes the approach of encoding sets into integers and using Shor's period-finding algorithm to compute the least common multiple, thereby revealing the union. However, the feasibility of protocols requiring complex operations like multiple QFTs [33] remains infeasible for current quantum hardware.

4.4 Comparison operations protocols

Comparison operations protocols target relationships between data, such as equality, extremum and greatness. The millionaires' problem is addressed by several protocols, often using a TP to generate quantum states. The schemes by Zhang et al. [51] and Hou et al. [63] both involve a TP preparing d-level states, on which participants encode their secrets using shift operations. Privacy is protected using decoy particles [51] or by encoding secrets on arbitrary particles to thwart collusion attacks. Another protocol for the socialist millionaire problem is proposed by Hou et al. [56], using shared keys and quantum sequences prepared by a third party, who ultimately performs a Bell measurement to determine the equality result. Its privacy is preserved by the fact that TP is not able to identify the rotations performed by participants. The protocol in [63] was simulated on IBM Qiskit using 5 qubits, while the simulation in [56] replaced the Bell-state measurement with single-particle measurements.

Beyond this specific problem, researchers have explored diverse quantum resources for private comparison. Wang et al. [64] use Quantum Walks (QW), while Huang et al. [9] utilize GHZ states and QKD. This last protocol was also successfully simulated using 5 qubits.

Other comparison tasks have also been tackled. Joseph et al. [57] describe a tree-based anonymous ranking protocol. In a multi-round process, a TP uses quantum sequences to represent data ranges, building a binary search tree that allows participants to determine

their rank privately. Protocols for finding the minimum or maximum value have also been proposed [52, 58], using techniques like a custom QSMC-AND protocol or sequential shift operations. All three protocols were successfully simulated, although in the case of [52], a replacement of the Bell measurement with single particle measurement was necessary.

4.5 Hamming Distance, Vector Dominance, Two-Party Functions

Beyond standard arithmetic and comparison, QSMPC protocols have been designed for other computational tasks. Protocols have also been proposed specifically for computing two-party functions.

Secure Hamming distance computation, with direct applications in fields like bioinformatics, is addressed by two surveyed protocols. The protocol by Ma et al. [42] is specifically designed for comparing DNA sequences by converting them to binary strings and using Bell states and QKD. Peng et al. [59] propose a more general protocol where participants apply operations on photon sequences prepared by a TP. None of them was fully simulated.

A protocol for secure vector dominance, which determines if one vector's elements are greater than another's, is proposed by Liu et al. [65]. It combines a quantum private permutation scheme with a millionaire subprotocol, disguising inputs with random vectors to ensure privacy. Entanglement of particles guarantees that any attempt to measure the particles illegitimately will collapse the state, making such an attack ineffective. The simulation of the protocol had a high success rate and was executed for 2 parties.

Finally, there are protocols that aim for more generalized secure two-party computation. Liu et al. [53] present a method for scalar product computation using d-qubit states and QFT. As it is impossible to obtain phase information under entanglement, attacks fail. An integer comparison protocol for two parties is suggested by Shi et al. [46]. One party will encode their integer into two randomized quantum databases, then apply quantum phase transformations to entangled qubit states sent by the other party. This allows them to encode their secret and return the entangled states, such that the other can extract phase information and determine who has the larger input. A protocol by Rahmani et al. [60] computes general Boolean functions by encoding inputs into GHZ states, with security guaranteed by quantum principles like the no-cloning theorem and the measurement-disturbance property. Protocols [60] and [53] were successfully simulated, with [60] only being attempted on a 2-bit OR function.

5 Responsible Research

In this paper, we follow the TU Delft Code of Conduct [66]. We adhere to the Integrity Statement while conducting and reporting our research. More specifically, we are in agreement with the sentiment of research being verifiable and TU Delft members being "open and transparent about (...) the activities they perform". In this section, we explain the steps we took to ensure this claim and also expand upon the use of LLMs during the process of writing the paper.

5.1 Integrity and transparency of the research

An important objective of our paper was to ensure that the research process was transparent, reproducible and replicable. To that end, we have explicitly documented all sources of literature used in the survey, including the databases queried, the exact search terms

applied, and the criteria used for inclusion and exclusion of papers. Details on these topics can be found in Section 3. This decision allows other researchers to independently reproduce the search process and verify or extend the results. The sources that we used come from reputable databases and publications. We used Zotero [67], available for free for TU Delft students, to organize and annotate the literature, further supporting traceability and reproducibility. All sources we used within the paper are properly cited as references and all results are reported accurately and completely.

We recognize the risk of bias to be present when conducting scientific research. In our case, bias could come from the paper identification activity and result reporting. To mitigate this issue, our selection process was guided by clearly stated inclusion criteria, as stated in Appendix A.2. We also reported any manual filtering we had done transparently, to avoid introducing unintentional bias. In Section 6, we additionally discuss the limitations present in the papers that were selected and acknowledge possible biases in result reporting that come as a consequence of having a single perspective over the data.

We used no data from human subjects, and we processed no sensitive information.

We anticipate no new risks to arise beyond the paper, as it was only a literature review of pre-existing work. The findings might be used to better document quantum SMPC protocols, but malicious parties should not be able to gain any new information. Although we do point out in Section 6 that protocol reliance on semi-honest third parties can constitute a security risk in the real-world, none of the papers surveyed imply any real-life application of the protocols in the near-future. Therefore, this issue does not require ethical considerations at the moment.

5.2 Use of LLMs

For our paper, LLMs were used to improve the quality of the writing only. The process was to first write a section using own words, then prompting an LLM to "improve the writing of the section". This would suggest different phrasings or more formal expressions with the same meaning. None of the output from the LLM was used verbatim in the paper, everything was evaluated and further rephrased by us before being included. We also used for obtaining the appropriate Latex commands to create tables and figures of a desired structure. The exact queries we used can be found in Appendix A.3.

6 Discussion

Our systematic review of 37 papers in QSMPC from the last 5 years shows the field to be rich in theoretical innovation, but marked by a significant gap between theory and practice. In this section, we discuss the findings of our survey, exploring the array of proposed protocols, their reliance on quantum resources and privacy mechanisms, and their readiness for real-world implementation. We also go over the limitations of the review in this section.

6.1 Protocol diversity and common quantum resources

Our survey confirms that researchers are applying QSMPC to a wide category of computational problems. The protocols span from foundational arithmetic operations like multiplication and summation to more complex tasks, such as auctions or voting, and even with more specific goals, like Hamming distance computations. This range demonstrates that QSMPC has the potential be applied to multiple privacy-dependent domains.

Despite this diversity in functionality, we identified a clear group of common quantum techniques and resources. Regardless of the protocol's ultimate goal, it frequently relies on a few core concepts and procedures:

- **Entangled States**: Multi-particle entangled states, particularly d-dimensional Bell and GHZ states, are used to create secure correlations between participants. As one of the most common quantum concepts, it is expected that it is fundamental to protocols in every category, from summation ([48]) to comparison ([60]).
- **Single Photon States**: As opposed to entangled states, protocols perform operations on single photon states due to their ease of implementation and measurement ([49, 50, 30]).
- **Quantum Fourier Transform**: QFT is frequently proposed across protocols involving arithmetic, such as summation ([44]) and set union ([11]), due to its ability to efficiently manipulate quantum states.
- **Quantum Key Distribution**: As one of the more developed quantum cryptographic primitives, QKD was abundantly used across papers to share keys ([49, 56, 9]).

We did not include Pauli gates in the above list, as they are common operators in the majority of quantum protocols, regardless whether they are designed for SMPC or not [29]. Additionally, all but one paper assume the existence of a noiseless, lossless, secure quantum channel, which is not suitable for realistic operating conditions.

The choice of these resources and techniques is directly linked to the feasibility challenges that we discuss later. The high resource cost of preparing and maintaining multi-qubit entangled states and the gate depth required for operations like QFT and inverse QFT ([65]) represent some of the primary obstacles to implementation.

6.2 Privacy Guarantees

The privacy guarantees of the surveyed protocols predominantly stem from two sources: quantum principles and honesty assumptions. The most common technique to guard against external eavesdropping is the use of decoy particles, as seen in several papers ([48, 49, 23, 55]). An attacker is then detected through the measurement-disturbance principle. Other guarantees rely on the no-cloning theorem ([31, 46]) or the fact that if information is hidden in a global state or phase, it is inaccessible to attacking parties ([18, 53]).

A common trend is the reliance on a semi-honest third party. 25 out of 37 protocols depend on a semi-honest TP to perform important tasks like preparing and distributing initial states, coordinating participants, or performing the final measurements. This represents a strong trust assumption and may become a vulnerability in a real-world scenario. 12 out of 37 papers do suggest schemes that do not employ third parties, such as [47], but they represent a minority. Our survey shows that research into quantum protocols that can function under malicious third parties is still lacking.

6.3 Feasibility Issues

One of the most noteworthy findings of our survey is the gap between the abundance of theoretically secure protocols and their demonstrated practical feasibility. This remains one of the most significant bottlenecks on the topic of protocol implementation.

From the papers surveyed, 19 out of 37 studies did not provide concrete information on feasibility. They would generally only make unquantifiable comments on how certain resource choices made their protocols more feasible or practical ([41, 35, 49, 42]). The remaining papers did provide details of simulations and practical implementations, predominantly accomplished through IBM Qiskit or similar software. However, their feasibility remains at a small scale, in ideal conditions. The following compromises generally had to be made due to current technological limitations:

- Algorithmic Simplification: Resource-intensive operations are frequently replaced with simpler alternatives. One example is substituting the QFT with a Hadamard gate ([41]).
- Measurement Simplification: More complex measurements, such as a Bell-state measurement, are often replaced with a series of easier to perform single-particle measurements ([56, 52]), which limits the scope of the tests.
- Scale Reduction: Simulations are typically run with a minimal number of participants (e.g., only 5 parties in [47]) and a few qubits for ([63]), which may not capture the scaling challenges or error propagation in larger, more realistic scenarios.
- Idealized Conditions: The majority of simulations are performed under the assumption of a noiseless environment, with almost perfect success rates. One protocol [63] does explicitly take noise into account, but is the only exception among the selected papers.

These compromises show that current QSMPC protocols, while theoretically sound, are still far away from being implemented within the constraints of today's NISQ hardware. As a consequence, the claim of 'feasibility' in current literature often refers to simplified proofs-of-concept rather than scalable, error-resistant implementations. Figure 3 shows the feasibility trends over the years from the selected papers. Presumably due to newer developments in the field of quantum computing, an increase in protocol feasibility analysis is noticeable within the more recent years. However, until the gap between theory and practice is addressed, the real-world applicability of these protocols will remain an open question.

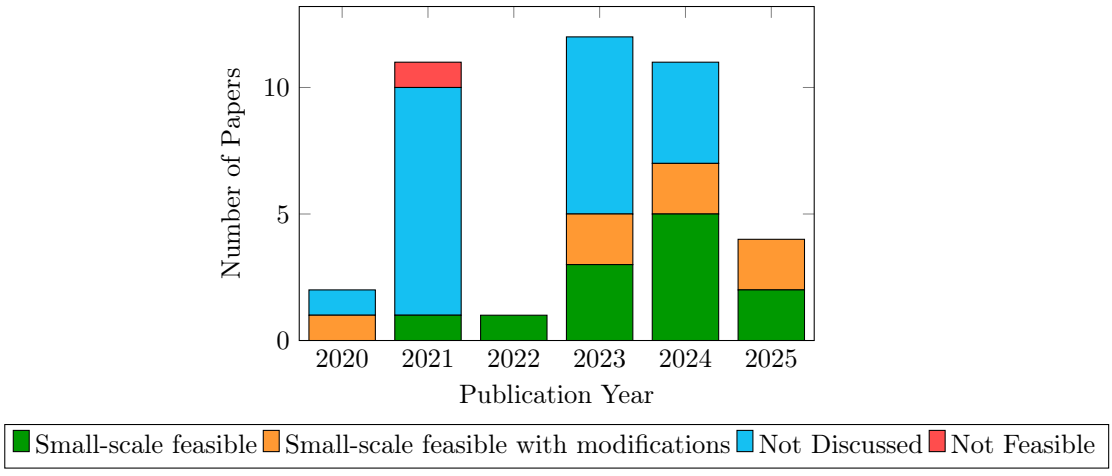

Figure 3: Trend of Protocol Feasibility by Publication Year.

6.4 Limitations

The literature review is limited by the range of selected papers and the duration of the research project. This is very clear when considering the number of papers that had to be discarded during the selection process (98). Only three academic databases were considered, so it is reasonable to assume that expanding the search field would have resulted in more papers to be taken into consideration and might have influenced our analysis. It is also important to keep in mind that the range of secure multi-party computation protocols is extensive, which made it impossible for us to include all possibilities in the search query and resulting paper. On the same note, if papers used different terminology to refer to QSMPC than we included in our query, it is likely we would have excluded them from our selection.

Another factor that contributed to the limited scope of the presented information is the lack of data on the feasibility of the protocols. Additionally, while a discussion on the efficiency of qubits within the protocols could have been made, we were limited by the details provided in each paper on this topic. Another limitation to note is related to the quantum resources of each paper included in the survey. In a few cases, only the most important techniques were mentioned in the protocol descriptions ([47]), without delving deeper into all required gates. This might cause our lists of resources in Table 1 to be incomplete.

It should also be taken into account that the entire literature review was performed by a single person, which means there exists the risk of oversights or misinterpretations in the QSMPC analysis, despite our best efforts. Lastly, the need for brevity in this paper required that information be condensed, limiting the depth to which protocols could be analyzed.

7 Conclusions and Future Work

In this paper, we aimed to analyze Quantum Secure Multi-Party Computation by examining protocols developed over the past five years. Our results have fulfilled our goal, identifying the field to be rich in theoretical proposals, but still lacking in practical implementations.

Firstly, regarding the types of schemes proposed, we identified a diverse range of protocols for functionalities from basic arithmetic (summation, multiplication, comparisons) to more specialized applications, including auctions, voting and set operations. Secondly, concerning the quantum resource requirements, we found that the proposed protocols consistently rely on a few components. The most commonly used are multi-particle entangled states and single photon states. More complex protocols frequently require resource-intensive operations, like the Quantum Fourier Transform. Thirdly, in terms of privacy guarantees, protocols achieve security for both internal and external attacks through two primary mechanisms: quantum principles, especially through the use of decoy particles to detect eavesdropping, and semi-honest third parties, which coordinate the protocols and perform computations or measurements. Finally, our research into feasibility shows that very few of the proposed schemes are practical on current technology. We identified a noticeable feasibility gap, with over half of the protocols lacking any implementation analysis, and others undertaking simulations in small-scale, ideal conditions. The missing necessary hardware, that would support more qubits and operations, represents the main obstacle hindering implementation. The extent of the effect of quantum noise on the protocols is also a significant unknown factor.

These findings indicate several possible directions for future research. We propose looking into protocols designed explicitly for the limitations of current quantum hardware, which account for noise in their practical simulations and employ quantum error correction. Another suggestion is to examine protocols that do not rely on semi-honest third parties for

proper functionality. Qubit efficiency calculations per protocol is another topic worth further investigation. Lastly, a literature review with a larger time frame might also provide more insights into the field.

References

[1] K. Sahinbas and F. O. Catak, "Secure multi-party computation-based privacy-preserving data analysis in healthcare IoT systems," in *Interpretable Cognitive Internet of Things for Healthcare*, pp. 57–72, Springer, 2023.

[2] D. Byrd and A. Polychroniadou, "Differentially private secure multi-party computation for federated learning in financial applications," in *ICAIF '20: The First ACM International Conference on AI in Finance, New York, NY, USA, October 15-16, 2020* (T. Balch, ed.), pp. 16:1–16:9, ACM, 2020.

[3] Y. Lindell, "Secure multiparty computation," *Communications of the ACM*, vol. 64, no. 1, pp. 86–96, 2021.

[4] P. W. Shor, "Algorithms for quantum computation: Discrete logarithms and factoring," in *35th Annual Symposium on Foundations of Computer Science, Santa Fe, New Mexico, USA, 20-22 November 1994*, pp. 124–134, IEEE Computer Society, 1994.

[5] M. Hillery, V. Bužek, and A. Berthiaume, "Quantum secret sharing," *Physical Review A*, vol. 59, no. 3, p. 1829, 1999.

[6] R. Cleve, D. Gottesman, and H.-K. Lo, "How to share a quantum secret," *Physical review letters*, vol. 83, no. 3, p. 648, 1999.

[7] C. Crépeau, D. Gottesman, and A. D. Smith, "Secure multi-party quantum computation," in *Proceedings on 34th Annual ACM Symposium on Theory of Computing, May 19-21, 2002, Montréal, Québec, Canada* (J. H. Reif, ed.), pp. 643–652, ACM, 2002.

[8] 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. 16263–16274, 2025.

[9] X. Huang, S. Zhang, and W. Cheng, "Quantum private comparison based on ghz-type states," in *2021 IEEE AFRICON, Arusha, Tanzania, United Republic of, September 13-15, 2021*, pp. 1–4, IEEE, 2021.

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

[11] W. Liu, Q. Yang, and Z. Li, "Quantum multi-party private set union protocol based on least common multiple and Shor's algorithm," *International Journal of Quantum Information*, vol. 21, no. 7, p. 2340006, 2023.

[12] W. Liu, C. Liu, H. Wang, and T. Jia, "Quantum private comparison: a review," *IETE Technical Review*, vol. 30, no. 5, pp. 439–445, 2013.

[13] A. Kumar, N. Sekhar Dey, B. Chennakeshwar, and C. Anuvamshitha, "Quantum-Enhanced Secure Multi-party Computation for Cyber Security Applications," in *International Conference on Intelligent Computing and Big Data Analytics*, pp. 127–145, Springer, 2024.

[14] A. Shamir, "How to Share a Secret," *Communications of the ACM*, vol. 22, no. 11, pp. 612–613, 1979.

[15] M. Luo, F. Li, L. Liu, and S. Zhu, "Verifiable quantum protocol for dynamic secure multiparty summation based on homomorphic encryption," *Journal of Physics A: Mathematical and Theoretical*, vol. 57, no. 11, p. 115302, 2024.

[16] Microsoft | Azure, "What is a qubit?." `https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-is-a-qubit`, 2025. (accessed: 21.06.2025).

[17] Y. Wang, Z. Hu, B. C. Sanders, and S. Kais, "Qudits and high-dimensional quantum computing," *Frontiers in Physics*, vol. 8, p. 589504, 2020.

[18] R.-H. Shi, "Quantum Sealed-Bid Auction without a Trusted Third Party," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 68, no. 10, pp. 4221–4231, 2021.

[19] Microsoft | Quantum, "Single-qubit gates." `https://quantum.scene7.com/is/content/quantum/bloch2`, 2025. (accessed: 19.06.2025).

[20] Microsoft | Quantum, "Quantum teleportation." `https://quantum.microsoft.com/en-us/insights/education/concepts/quantum-teleportation`, 2025. (accessed: 21.06.2025).

[21] Microsoft | Tech Community, "Quantum Computing Primer: Pure and Mixed States." `https://techcommunity.microsoft.com/blog/educatordeveloperblog/quantum-computing-primer-pure-and-mixed-states/380514`, 2018. (accessed: 22.06.2025).

[22] Microsoft | Learn, "Entanglement and correlations." `https://learn.microsoft.com/en-us/azure/quantum/concepts-entanglement`, 2025. (accessed: 21.06.2025).

[23] Y. Zheng and B. Liu, "A secure multi-quantum voting protocol based on GHZ state," in *2024 International Conference on Generative Artificial Intelligence and Information Security, GAIIS 2024, Kuala Lumpur, Malaysia, May 10-12, 2024*, pp. 243–248, ACM, 2024.

[24] Y. Wang, P. Hu, and Q. Xu, "Quantum secure multi-party summation based on entanglement swapping," *Quantum Information Processing*, vol. 20, no. 10, p. 319, 2021.

[25] 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)*, pp. 1–5, IEEE, 2023.

[26] M. H. Mohammady, T. Miyadera, and L. Loveridge, "Measurement disturbance and conservation laws in quantum mechanics," *Quantum*, vol. 7, p. 1033, 2023.

[27] A. Wei, G. Cobucci, and A. Tavakoli, "Nonprojective bell-state measurements," *Physical Review A*, vol. 110, no. 4, p. 042206, 2024.

[28] Microsoft | Learn, "Vectors and matrices in quantum computing." `https://learn.microsoft.com/en-us/azure/quantum/concepts-vectors-and-matrices`, 2025. (accessed: 21.06.2025).

[29] Microsoft | Quantum, "Single-qubit gates." `https://quantum.microsoft.com/en-us/insights/education/concepts/single-qubit-gates`, 2025. (accessed: 21.06.2025).

[30] W. Liu, Y. Li, Z. Wang, and Y. Li, "A New Quantum Private Protocol for Set Intersection Cardinality Based on a Quantum Homomorphic Encryption Scheme for Toffoli Gate," *Entropy*, vol. 25, no. 3, p. 516, 2023.

[31] W. Wu and X. Ma, "Multi-party quantum summation without a third party based on d-dimensional bell states," *Quantum Information Processing*, vol. 20, no. 6, p. 200, 2021.

[32] Microsoft | Quantum, "Multi-qubit gates." `https://quantum.microsoft.com/en-us/insights/education/concepts/multi-qubit-gates`, 2025. (accessed: 21.06.2025).

[33] W. Liu and H.-W. Yin, "A Novel Quantum Protocol for Private Set Intersection," *International Journal of Theoretical Physics*, vol. 60, no. 6, pp. 2074–2083, 2021.

[34] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, "The security of practical quantum key distribution," *Reviews of modern physics*, vol. 81, no. 3, pp. 1301–1350, 2009.

[35] Y. Chen, H. Situ, Q. Huang, and C. Zhang, "A novel quantum private set intersection scheme with a semi-honest third party," *Quantum Information Processing*, vol. 22, no. 12, p. 429, 2023.

[36] IBM, "Introduction to Qiskit." `https://docs.quantum.ibm.com/guides`, 2025. (accessed: 19.06.2025).

[37] IBM, "Quantum processing units." `https://quantum.ibm.com/services/resources?tab=systems&limit=50&view=table`, 2025. (accessed: 19.06.2025).

[38] M. J. Page, J. E. McKenzie, P. M. Bossuyt, I. Boutron, T. C. Hoffmann, C. D. Mulrow, L. Shamseer, J. M. Tetzlaff, E. A. Akl, S. E. Brennan, *et al.*, "The PRISMA 2020 statement: an updated guideline for reporting systematic reviews," *British Medical Journal*, vol. 372, no. 71, 2021.

[39] C. Wohlin, "Guidelines for snowballing in systematic literature studies and a replication in software engineering," in *Proceedings of the 18th international conference on evaluation and assessment in software engineering*, pp. 38:1–38:10, ACM, 2014.

[40] PRISMA, "PRISMA flow diagram." `https://www.prisma-statement.org/prisma-2020-flow-diagram`, 2020. (accessed: 22.06.2025).

[41] K. Sutradhar and H. Om, "A Generalized Quantum Protocol for Secure Multiparty Summation," *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 67-II, pp. 2978–2982, Dec. 2020.

[42] M. Ma, Z. Liu, and Y. Xu, "Quantum protocol for privacy preserving Hamming distance problem of DNA sequences," *International Journal of Theoretical Physics*, vol. 59, pp. 2101–2111, July 2020.

[43] K. Sutradhar and H. Om, "A cost-effective quantum protocol for secure multi-party multiplication," *Quantum Information Processing*, vol. 20, no. 11, pp. 1–10, 2021.

[44] K. Sutradhar and H. Om, "Secret Sharing Based Multiparty Quantum Computation for Multiplication," *International Journal of Theoretical Physics*, vol. 60, no. 9, pp. 3417–3425, 2021.

[45] C. Zhang, Y. Long, and Q. Li, "Quantum summation using d-level entanglement swapping," *Quantum Information Processing*, vol. 20, no. 4, p. 137, 2021.

[46] R.-H. Shi, B. Liu, and M. Zhang, "Secure two-party integer comparison protocol without any third party," *Quantum Information Processing*, vol. 20, no. 12, p. 402, 2021.

[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] F. Li, H. Hu, S. Zhu, and P. Li, "A Verifiable (k,n)-Threshold Quantum Secure Multiparty Summation Protocol," *International Journal of Theoretical Physics*, vol. 62, no. 2, p. 17, 2023.

[49] W.-Q. Wu and M.-Z. Xie, "Quantum Secure Multi-Party Summation Using Single Photons," *Entropy*, vol. 25, no. 4, p. 590, 2023.

[50] H. Yu, R.-h. Shi, and W. Ke, "MDI quantum protocol for anonymous countable veto voting," *Physica Scripta*, vol. 98, no. 9, p. 095102, 2023.

[51] Y. Zhang, L. Zhang, K. Zhang, W. Wang, and K. Hou, "A new quantum-inspired solution to blind millionaires' problem," *Quantum Information Processing*, vol. 22, no. 1, p. 80, 2023.

[52] H.-X. Kong, H.-Y. Jia, X. Wu, and G.-Q. Li, "Robust Quantum Secure Multiparty Computation Protocols for Minimum Value Calculation in Collective Noises and Their Simulation," *International Journal of Theoretical Physics*, vol. 62, no. 8, p. 172, 2023.

[53] 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.

[54] F. Li, M. Luo, S. Zhu, and B. Pang, "General quantum secure multiparty computation protocol for simultaneous summation and multiplication," *Physica Scripta*, vol. 99, no. 1, p. 015107, 2024.

[55] 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.

[56] M. Hou, S.-Y. Sun, and W. Zhang, "Quantum private comparison for the socialist millionaire problem," *Frontiers in Physics*, vol. 12, p. 1408446, 2024.

[57] J. Joseph and S. T. Ali, "Tree-based quantum anonymous ranking protocol," *Quantum Information Processing*, vol. 23, no. 7, p. 263, 2024.

[58] Y. Lu and G. Ding, "A novel quantum security multi-party extremum protocol in a d-dimensional quantum system," *Physica Scripta*, vol. 99, no. 9, p. 095111, 2024.

[59] Z.-W. Peng, R.-H. Shi, R. Ding, and F.-F. Zhang, "A novel quantum protocol for secure hamming distance computation," *Quantum Information Processing*, vol. 23, no. 5, p. 165, 2024.

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

[61] Z. Rahmani, A. N. Pinto, and L. S. Barbosa, "Private computation of boolean functions using single qubits," in *Parallel Processing and Applied Mathematics - 15th International Conference, PPAM 2024, Ostrava, Czech Republic, September 8-11, 2024, Revised Selected Papers, Part II* (R. Wyrzykowski, J. J. Dongarra, E. Deelman, and K. Karczewski, eds.), vol. 15580 of *Lecture Notes in Computer Science*, pp. 301–312, Springer, 2024.

[62] M. Hou, Y. Wu, and S. Zhang, "Quantum Private Set Intersection Scheme Based on Bell States," *Axioms*, vol. 14, p. 120, Feb. 2025.

[63] K. Hou, H. Sun, Y. Yao, Y. Zhang, and K. Zhang, "A quantum solution to blind millionaire problem with only single-particle states," *EPJ Quantum Technology*, vol. 12, no. 1, pp. 1–17, 2025.

[64] J. -T. Wang and T. -Y. Ye, "A Novel Two-round Two-party Quantum Private Comparison Protocol Based on Quantum Walks," *IEEE Transactions on Computers*, no. 1, pp. 1–10, 2025.

[65] W. Liu, B. Su, and F. Sun, "Efficient Quantum Secure Vector Dominance and Its Applications in Computational Geometry," *IEEE Transactions on Computers*, vol. 74, no. 6, pp. 2129–2143, 2025.

[66] S. Roeser and S. Copeland, "TU Delft Code of Conduct," 2020.

[67] T. E. Vanhecke, "Zotero," *Journal of the Medical Library Association*, vol. 96, no. 3, p. 275, 2008.

A Appendix

A.1 Search queries

The initial query we used is:

"quantum AND ("multi party computation" OR "multi-party computation" OR "multiparty computation" OR "two party computation" OR "private set intersection" OR "threshold cryptography")"

The final query we used is:

"quantum AND ((("multi party" OR "multi-party" OR multiparty OR "two party") AND (computation OR summation)) OR "private set intersection" OR "millionaire problem" OR "millionaires' problem" OR "anonymous voting" OR "secure computational geometry" OR "matrix multiplication")"

A.2 Inclusion and Exclusion Criteria

We defined inclusion and exclusion criteria, to narrow down the selection of papers and guarantee the reproducibility of the review process.
Papers must meet the following inclusion criteria:

- The paper is written in English.
- The paper's primary focus is on quantum secure multi-party computation, with protocols or models that incorporate quantum technologies.
- The paper was published between 2020 and 2025.
- The paper includes technical descriptions or implementation details, rather than only high-level commentary.

Papers are excluded based on these criteria:

- The paper is not from peer-reviewed sources.
- The paper only mentions classical secure multi-party computation procedures.
- The paper discusses only post-quantum or quantum-safe secure multi-party computation and does not mention actual quantum operations or protocols.
- The paper focuses on quantum primitives without applying them to secure multi-party computation.
- The paper cannot be accessed via TU Delft.

A.3 LLM queries

- "Improve the writing in this section."
- "Give the structure for a table with 5 columns that allows for subtitles within the table in Latex."
- "Give the structure for a bar graph in Latex with legend that allows for different categories within the same bar."