**Quantum Key Distribution in Multiparty Computation for Data Sorting by Entanglement**

**Shyam R. Sihare\***

Department of Computer Sc. & App., Dr. APJ Abdul Kalam Gov. College, Dokmardi

Silvassa, UT of Dadra and Nagar Haveli & Daman and Diu, India

Email: [shyams\_sihare1979@rediffmail.com](mailto:shyams_sihare1979@rediffmail.com)

ORCID iD: [**0000-0003-2096-8273**](https://orcid.org/0000-0003-2096-8273)

**Abstract:**

Multiparty computation (MPC) and quantum key distribution (QKD) offer new paradigms for secure communication within quantum environments. The paper is the first to introduce the data sorting (Dsorting) framework, using entanglement within multiparty quantum contexts to distribute Dsorting. By combining QKD protocols with MPC methodologies, the system ensures that, together with privacy-preserving Dsorting, secure key exchanges are guaranteed. Grover's search algorithm combined with entanglement-based QKD is used and augmented by qudit quantum states to increase security and robustness against errors. The main parts are phase encoding, quantum error correction (QEC), GHZ state preparation, and multiparty entanglement purification. Grover's oracle and privacy amplification provide quantum security for the Dsorting process, and quantum sorting (Qsort) simulates sorting. Experimental results demonstrate sorting accuracy of up to 98% and effective key distribution rates of up to 92%, even under quantum bit error rate (QBER) conditions. Sorting time scales logarithmically with the size of the dataset and party count ; -party entanglement forces higher communication complexity compared to the traditional MPC. Such results justify the utility of QKD and entanglement in enabling the secure and fault-tolerant multiparty Dsorting while providing much value for distributed computing and secure communication at a certain computational overhead.

***Keywords:*** Quantum Key Distribution, Quantum Multiparty Computation, No-Cloning Theorem, Quantum Information Security, Quantum Data Sorting, von Neumann Entropy

# Introduction

QKD the backbone of quantum cryptography, guarantees a secure key exchange based on fundamental principles of quantum mechanics, including the no-cloning theorem and quantum entanglement [1]. MPC, which enables parties to jointly perform any computation over private data without disclosing them, holds much promise for adding further security features to data communication by incorporating QKD [2]. This paper discusses QKD in a quantum MPC (QMPC) protocol, with particular reference to safely sorting a distributed dataset among parties.

The fundamental difficulty with MPC for Dsorting is that to enable safe collaboration between the parties, the dataset must also be kept private, even though the communications must. Methods based on cryptography are in many regards robust, but vulnerable to advances in computational power, particularly the prospect of quantum computing [3]. On the other hand, QKD, due to the laws of physics, inherently prevents the possibility of key intercepts without disturbing the detectable quantum states [4]. This presents a highly suitable mechanism in the MPC protocol for securing communications.

In the following work, we extend QKD to a multiparty setting, in which parties share and then process a distributed dataset securely by using quantum entanglement to develop a protocol within the system of an MPC that is computationally efficient yet ensures data confidentiality [5]. Toward this end, we propose our protocol through quantum gates and circuits used for sorting the quantum-encoded data to present an enhancement of quantum strength over any classical sorting algorithm in a secure distributed setting.

The proposed structure for the study is as follows: Section 2 provides a literature review of existing research on QKD and MPC systems. Section 3 outlines the contributions. Section 4 details the proposed methodology, including the system model, entanglement-based QKD techniques, and security analysis. Subsection 4.4 explores quantum dynamics in sorting, while subsection 4.5 introduces the security model. Subsection 4.6 examines quantum attack models and mitigation strategies. Subsection 4.7 evaluates the QKD-MPC system’s performance, and subsection 4.8 discusses implementation and experimental setup. Section 5 concludes with findings and their impact on quantum secure communication.

# Literature Review

QKD is the underlying technology behind secure communication with interference invulnerability by exploiting the principles of quantum mechanics for key exchange. Ever since it was invented in 1984 through BB84 protocol by Bennett and Brassard, some advancements have been seen in QKD [6]. Some protocols, including E91, refer to Ekert's protocol and rely on quantum entanglement for secure communications [7]. A feature exclusive to QKD for detecting an eavesdropper is feasible based on the no-cloning theorem [8]. Other recent progress goes to high-dimensional QKD with qudits for improved rates and noise-robustness [9].

Another direction is entanglement-based QKD protocols, such as E91. The principle of these protocols is secure since it enables the two parties to share two-particle entangled states, which violates Bell's inequality [10]. Such a protocol becomes a significant realization in the discussion of secure MPC, where parties compute a function over the private inputs, in such a way that ensures data privacy. The role of QKD in MPC is that it provides safe communication among parties so that interference by an adversarial party or leakage of information may not occur [11]. This is quite relevant to the current research looking into sorting secure data in a multiparty setting.

MPC refers to the functionality of parties computing a function over private inputs without revealing their inputs. The developments in classical cryptography established a basis for MPC, including Yao's secure computation protocols and Goldreich's cryptographic systems [12-13]. MPC further evolved into the quantum domain, leading to quantum channels and quantum states to protect multiparty communication. QMPC introduces concepts of quantum computing with entanglement and quantum gates to enhance the security provided by the computing executed [14].

This is made possible via quantum data processing using Qsort algorithms. It is well-established that the complexities of quicksort and mergesort are, respectively, and [15]. Quantum research comparison-based sorting utilizing quantum comparators was prompted by the quadratic speedup in unstructured searches that drove quantum comparisons for variants of Grover's algorithm [16]. This paper is inspired by the work of Dutta, Anurag, et al., who discussed quantum Dsorting in secure computation [17]. This study used QKD and applications with entanglement for safe Dsorting.

The concept of entanglement plays a significant role in the secure communication and computation in quantum systems [18-19]. By extending the concept of bipartite entanglement into a multiparty setting, the GHZ (Greenberger–Horne–Zeilinger) state assists in secure multiparty communication [20]. Entanglement in QKD means that any attempt to eavesdrop will also disrupt the system, making it detectable [21]. Zukowski et al. and Pan et al. have shown that entangled photons might be used for long-distance secure communication, thus proving that entanglement indeed has practical security applications in QKD [22-23].

For multiparty quantum systems, entanglement ensures that any unauthorized access to data will disturb the quantum state, hence alerting the parties [24]. It is a significant part of this work to aimed at sorting distributed datasets securely. Data of every party is encoded into quantum states, and by entanglement, it can be ensured that any interference from an eavesdropper will introduce errors detectable by the parties. Besides, quantum gates like the controlled-NOT (CNOT) gate ensure computation confidentiality, particularly during sorting algorithms [25].

QEC is the first indispensable element for practical quantum communication because quantum systems are susceptible to noise and decoherence [26]. In early work, Shor and Steane introduced the concept of QEC codes that protect quantum states from errors [27-28]. QEC is significant for QKD and quantum computation in maintaining the security and integrity of communication despite noise in the quantum channels [29]. Adding QEC to the protocol ensures security, making it resilient against adversarial action or channel imperfections [30].

QKD with QEC assures that noise cannot break security [31]. Sophisticated QKD protocols, like the one described by Crépeau et al., contain approaches for error tolerance to maximize key generation rates with minimal overhead for correction [32]. QEC is used in this study to correct the errors in the noisy quantum channels by sharing a secret key and performing the quantum secure MPC [33]. The error correction codes, either the stabilizer or the surface code, ensure the integrity of the sorting protocol given, even in the presence of noise [34-35].

Moreover, QKD, entanglement, and QEC functioning inside the secure MPC are required [36]. Compared to their classicalcryptographic counterparts, the quantum integration of these technologies offers an unparalleled increase in security [37]. This research investigates an entanglement-based QKD technique for securely sorting multiparty data, building upon this theoretical process [38]. This suggested protocol guarantees the security and secrecy of Dsorting in distributed systems across the quantum world by utilizing entanglement, quantum gates, and error-correcting methods [39]. These methods not only overcome the scalability and security challenges but also solidly belong to the group of next-generation approaches that will lead to safe quantum computation [40].

# Contributions

The contributions of this study are as follows

1. It suggested an alternative process to the MPC model for implementing QKD. Dsorting is possible in a multiparty setting with total security. The model utilized quantum encryption and entanglement to improve security against classical and quantum attackers.
2. It suggests the Qsort method, which accelerates and secures Dsorting using Grover's algorithm. Comparative analysis demonstrates how the Qsort method greatly decreases sorting time complexity, particularly when dealing with huge datasets, compared to classical approaches.
3. The study uses QEC techniques to adjust for quantum communication and computing defects, yet it still keeps fidelity at 99.8% and errors at a remarkably low rate of 0.3%.
4. The suggested model enhances the rate of key distribution even in noisy channels (QBER effect on the key rate) and minimizes the communication overhead through entanglement swapping and quantum teleportation because few qubits are transmitted. As a result, it can scale to big multiparty networks.
5. A thorough performance analysis has demonstrated that, particularly for large datasets and parties involved, the quantum method significantly outperforms classical approaches regarding sorting precision (98%) and execution times. As a result, the quantum method holds great promise for secure data processing in distributed systems utilizing quantum technologies.

# Proposed Methodology

The quantum channel is a secure key generation process based on entangled quantum states, quantum measurement, and QKD protocols [4-7]. Different quantum states caused by noise or interference have been corrected using error correction procedures [29]. Once the quantum keys have been determined, they are sent across a classical channel for secure communication. The sorting process known as *key reconciliation* involves parties comparing portions of their keys to ensure they are consistent and aligned [27]. Privacy amplification techniques reduce correlation among keys to minimize leaked information about the quantum key [2].

It requires the implementation of AES (Advanced Encryption Standard) or other symmetric encryption like DES, 3DES, Blowfish, Twofish, RC4, RC5, and RC6 for secure key exchange, with quantum-secured communication being used to sort and process data [22]. Qsort algorithms encrypt and sort data using mergesort and quicksort by employing securely distributed keys. After sorting, secure communications between parties can occur to preserve collaborative Dsorting and privacy [41]. Success feedback and verification confirm that the keys exchanged between two parties correspond, while errors or mismatches will re-entangle and error correct their way back [23]. Final data validation will then be executed to verify correctness before the final output, and the final, securely sorted data will be outputted. QEC plus re-entanglement adds even more layers to strengthen the security of the quantum key by correcting mismatches and minimizing possible information leakage during the exchange (Fig. 1).

The QKD process applies gates to each qubit to prepare each party's superposition of quantum states. The CNOT gates create entanglement between every pair of parties, giving a connected system that can reach all four parties. Measurement of the qubits generates the first shared quantum keys [7, 23].

SWAP gates are used in entanglement swapping and error correction. Toffoli gates are applied to correct quantum bit errors caused by decoherence or noise [29]. XOR gates are then applied to reconcile the differences among the swapped quantum states; this process helps in aligning the shared quantum keys [22]. is used to confirm that errors and entanglement swapping have been made successfully [27]. Besides that, Bell test operations are verified for their integrity in terms of entanglement, ensuring the authenticity and security of the states [41]. XOR gates reconcile, correct small errors between shared quantum keys, and reduce information leakage through the QKD process [2].

Each party uses a Qsort algorithm such as quantum mergesort to apply Qsort with conditional logic to their data [23]. Using CNOT and multiparty SWAP gates allows for applying conditional logic where data is swapped between qubits corresponding to entangled quantum states [41]. The data in the checks are then verified to have been put into the correct order. Each party applies final encryption and secure data output, using shared quantum keys to ensure such. The approach is safe with its ability to implement the quantum communication between four parties using quantum entanglement in the key distribution and Dsorting, as outlined in Fig. 2.



**Fig. 1** The architecture of QKD in MPC for Dsorting via entanglement. Secure QKD among parties using entangled quantum states like Bell, and GHZ states. States exchange quantum keys via QKD protocols based on error correction and privacy amplification steps. As the key reconciliation is carried through classical channels, every single data communication will be encrypted through quantum encryption. Qsort algorithms, including mergesort and quicksort, process shared, encrypted data in such a way that feedback loops maintain the integrity of the key and correctness of the data, and the output will be the securely sorted data.



**Fig. 2** Entanglement-based multiparty QKD and Dsorting. The key steps of the process are **(1)** QKD based on entangled qubits shared between parties namely, ; **(2)** Entanglement swapping and error correction with Toffoli and XOR gates to preserve the integrity of entanglement; **(3)** Verification of the quantum state through Bell tests for authentication purposes; **(4)** Reconciliation of keys and privacy amplification for enhanced security; **(5)** Qsort of data among parties via conditional logic and entanglement; and **(6)** Final encryption and output of securely decrypted data quantum encryption for safe communication.

## System Model

Let, where, andas, be the quantum Hilbert space including all parties participating in the MPC protocol. For each,. There exists a unitary operatorsuch that for all,, ensuring the transformation to quantum-secure states. Subsequently, the dataset distribution is defined as, where. A distribution operatorexists, such that, establishing quantum entanglement among subsets of the dataset.

For secure key exchange, the quantum channel between any two partiesand, denotedwithand, adheres toand employs QKD. The quantum state associated with the-th bit of the exchanged key is . A quantum superoperator, ensures linearity, non-cloning, and measurement disturbance principles. Consequently, any eavesdropper state is represented as , ensuring the detection of any quantum interference attempts. The secure dataset sorting operationmapsto, following a distributed sorting algorithm. It is defined as:

|  |  |
| --- | --- |
| , | (1) |

subject to the condition,,, excluding malicious interference. In the multiparty entanglement process, the sorted dataset results from entangled states:

|  |  |
| --- | --- |
| , | (2) |

where, and, ensuring all states adhere to measurement invariance principles. Furthermore, the parametersanddefine the superposition coefficients of the quantum statewithsuch that. Letrepresent the Hilbert space accessible to an eavesdropper, anddenote the unitary operation corresponding to's measurement process. Ifinteracts with, the state transitions are . With that, the overlap between the original state and the disturbed state is quantified by , wheredepends on the nature ofand the disturbance introduced by. The probability of detecting an eavesdropper is , where. Detection is ensured if, indicating a non-zero deviation induced by the eavesdropper’s actions. Expanding, we have:

|  |  |
| --- | --- |
| , | (3) |

whererepresents the phase difference induced by. In an MPC setting, , participating parties, occupy a subspace. Each communication channelis described by a joint Hilbert space,, where the security is determined by the projection operator, . Moreover, for the detection of eavesdropping, the condition for secure communication is , wheredenotes the commutant of the channel operators, ensuring the detection of non-local interference. So, under the multiparty process, letrepresent the entangled state distributed across all parties. The interaction ofwith any subset of the system, described by, introduces disturbances quantified as:

|  |  |
| --- | --- |
| , | (4) |

ensuring that any eavesdropper interaction is detectable through deviation metrics in the quantum Hilbert space.

1. ***Parties' Behaviour***

As we know,, set of all parties in the QMPC protocol, whereis the encompassing Hilbert space of the system. Each partyoperates in a local subspace, observing the unitary controlled by, ensuring quantum security.

Honest-but-curious or dishonest parties behavior is modeled by the constraint, whereextracts permissible information, such that, withunder observance to protocol rules. Dishonest parties,, deviate by employing non-unitary operations, where:

|  |  |
| --- | --- |
| , | (5) |

withrepresenting a noise operator designed to extract non-permissible data. The subsetsatisfiesand, where, ensuring the protocol's resilience against collusion. Define the global security constraint as:

|  |  |
| --- | --- |
| . | (6) |

The conditionensures that malicious operations are detectable through non-zero deviations in the quantum state. For, entanglement across all honest partiesis preserved by projecting the state onto:

|  |  |
| --- | --- |
| , | (7) |

whereremains inwhilecollapses into. Thus, the protocol is secure under the constraint, where the detection probability for malicious behavior,, satisfies, , ensuring robustness against collusion by dishonest parties in the communication process.

1. ***Channel Model***

Letrepresent the quantum channel facilitating communication between partiesand. The quantum channel operates under the influence of noiseand loss, such that the effective channel fidelityis defined as:

|  |  |
| --- | --- |
| . | (8) |

The classical channel, denoted, satisfies the authenticated communication property, ensuring integrity without guaranteeing confidentiality, , where is the classical state from space . Additionally, QKD betweenandgenerates a shared secret keyderived from quantum statesexchanged over:

|  |  |
| --- | --- |
| , | (9) |

whereis a secure key extraction function anddenotes measurement in the computational basis. For QKD protocol, the key generation rate is, , whereis the QBER andrepresents the binary entropy function. In the presence of noise and eavesdropping, the effective key generation rate is adjusted as [42]:

|  |  |
| --- | --- |
| , | (10) |

wherequantifies the probability of detecting eavesdropping via measurement disturbances. Moreover, the quantum states, where, ensure that any deviation introduced by noise or interference is detectable under the unitary operator, .

Thus, the secure QKD process guarantees key confidentiality, while the interaction of noise, loss, and entropy bounds the effective fidelity ofand the key generation rate [43]. Hence, let the key lengthfor the QKD process between partiesandbe expressed as a function of the QBER:

|  |  |
| --- | --- |
| . | (11) |

The dataset is encoded into quantum states within a Hilbert space, where each data elementis represented in its respective subspace, such that the density operator, . Hence, the sorting operation is implemented through a unitary transformation, constructed as a product of pairwise unitaries, with a parameterized rotation gate,:

|  |  |
| --- | --- |
| . | (12) |

Key-dependent unitariesintroduce privacy-preserving operations, , whereare key-dependent coefficients andare Pauli operators acting on qubits shared byand. The enhanced sorting operationincludes these key-dependent unitaries, . Hence, the joint quantum state of the dataset and keys,, after the sorting process is:

|  |  |
| --- | --- |
| , | (13) |

whereis the density operator of the key distribution system. Likewise, the mutual information between the sorted datasetand the keysis quantified, , whereis the von Neumann entropy of the state. To ensure privacy, the min-entropy conditioned on the keys,, is defined as:

|  |  |
| --- | --- |
| , | (14) |

whereis a projection operator associated with key. The privacy condition is satisfied if, , whererepresents a small leakage, ensuring minimal information leakage abouteven when keysare compromised. The multipartite quantum datasetis defined by tensor product of quantum states as . Eachis encoded using higher-dimensional Hilbert spaces and quantum state encoding functions, such that:

|  |  |
| --- | --- |
| , | (15) |

wheredenotes the probability amplitude over momentum space, adhering to the quantum Fourier transform (QFT) relation. Encryption ofis achieved using a key-parameterized unitary, , whereencodes multi-qubit interactions via key-dependent coefficientsand Pauli operators. When applied to, encryption modifies the state, . So, the encrypted dataset becomes:

|  |  |
| --- | --- |
| . | (16) |

An eavesdropper, modeled via a completely positive trace-preserving (CPTP) map, perturbs the state is , whereare Kraus operators encoding decoherence and interaction dynamics. Applyingto, the evolved state is . Next, assuming a depolarizing noise model, the state is probabilistically perturbed represented as , whereis the perturbed state, expanded via spectral decomposition, , withandrepresenting eigenvalues and eigenvectors, respectively. The perturbed state under entangled data encoding is, (we consider , similarly, ), whereare Schmidt coefficients, and,are orthonormal Schmidt bases. The encryption's entanglement-preserving properties lead to a state transformation:

|  |  |
| --- | --- |
| . | (17) |

The impact ofon the entangled state can be measured by the entanglement negativity, , whereis the partial transpose of, anddenotes the trace norm. Security against eavesdropping is quantified using the min-entropy conditioned on the key, , withas projectors onto key-specific subspaces. The final entangled and encrypted state incorporating noise and key-dependence is:

|  |  |
| --- | --- |
| , | (18) |

integrating QFT encoding, entanglement, encryption, and eavesdropping within a higher-dimensional Hilbert space system. The communication complexity of the proposed MPC protocol, denoted, is , whereis the key length generated by the QKD process. The secure key length foris . For, the secure key length incorporates the deviation, with a dependence on the von Neumann entropyof the quantum state, the channel noise parameter, and the efficiency parameter:

|  |  |
| --- | --- |
| , | (19) |

where the von Neumann entropyis defined as . The density matrix, formed during the QKD process, is expanded using the statesand their probabilities, . Also, to refine the model, the quantum Fisher information (QFI), associated with the Hamiltoniangoverning the key generation, is introduced:

|  |  |
| --- | --- |
| , | (20) |

whereis a weighting factor for the role of. Henceforth, the QFI is , with, the symmetric logarithmic derivative, satisfying, . Entanglement between partiesand, quantified by a measure, further modifies the secure key length:

|  |  |
| --- | --- |
| , | (21) |

wherescales the entanglement contribution. Therefore, a suitable entanglement measure is concurrence, , withis defined as , whereare the square roots of the eigenvalues of, andis the Pauli-Y matrix. Combining in Eq. (21), the final expression for the secure key length is:

|  |  |
| --- | --- |
| . | (22) |

With that, the initial key lengthis , with a success probability approximated by, whereis a security parameter associated with the key generation process. The success probability is linked to the fidelityof the generated quantum states, with. Introducing the quantum relative entropybetween the ideal stateand the actual generated state, let, whereis a small positive constant. Thus, , leading to a relationship betweenand as . Moreover, after privacy amplification, the imroved key length is given by:

|  |  |
| --- | --- |
| , | (23) |

where, the qudit entropy [44] is , withrepresenting the bit error rate andthe dimensionality of the qudit system. Incorporating quantum discord, which quantifies quantum correlations beyond entanglement in a bipartite system, we improve the key length further:

|  |  |
| --- | --- |
| , | (24) |

whereis a scaling factor. The quantum discord is , with the mutual information as , and the classical correlation is , whereare projective measurements on subsystem,the probabilities of outcomes, andthe conditional state of. Therefore, incorporating the quantum channel capacity, representing the maximum rate of reliable quantum information transmission over a channel, the key length becomes:

|  |  |
| --- | --- |
| , | (25) |

wherescales the channel's contribution. For a memoryless channel, the Holevo capacityprovides an upper bound:

|  |  |
| --- | --- |
| , | (26) |

whereis an ensemble of input states andthe output states. Accounting for decoherence, with a decoherence rate, the final key length incorporates an exponential decay factor:

|  |  |
| --- | --- |
| , | (27) |

whereis the duration of the key generation and distribution process. The total communication complexity, as a function of the qudit-based key length, is , whereis the qudit entropy,is the number of parties, andis the bit error rate. Moreover, we introduce channel loss and noise effects. Letrepresent the channel transmissivity andthe noise variance. Define a modulation function as , whereis a channel-dependent constant. Therefore, the communication complexity becomes . With that, for computational complexity, which includes the cost of sorting datasetof size and the overhead from QKD, we write (here overhead is represented by , whereas for complexity we have used the notation)[[1]](#footnote-1):

|  |  |
| --- | --- |
| , | (28) |

whereis the key generation rate. Expressin terms of Holevo informationand key distillation efficiency, , with, whereis the average state, andrepresents the ensemble of states in the QKD protocol [45]. To incorporate finite key effects, letrepresent the final key length andthe time for key generation. The key generation rate becomes . Furthermore, assuming, whereis the number of rounds andthe time per round, then . So, the computational complexity improves to:

|  |  |
| --- | --- |
| . | (29) |

Furthermore, introduce entanglement, which impacts, the efficiency of key distillation is , whereis a logarithmic function that is written as . Finally, account for side-channel attacks with success probability, adding a correction term:

|  |  |
| --- | --- |
| . | (30) |

For the qudit-based QKD protocol using unconventional methods with entanglement and multidimensional state encoding, the key generation rateis , whereis the qudit entropy. We incorporate the mutual informationbetween senderand receiverpost-sifting but pre-error correction and privacy amplification, , whereis the von Neumann entropy of, andis the conditional von Neumann entropy. For entangled qudits, the entropic terms consider non-classical correlations, andis , whererepresents the reduced density matrix of. Thus, the total computational complexityincorporates QKD methods, sorting datasetof size , and correcting errors through QEC:

|  |  |
| --- | --- |
| . | (31) |

Subsequent, to introducing QEC, letdenote the correctable error threshold, andrepresent the quantum channel error rate. For a specific QEC code with overhead [46] is . For surface codes,scales polynomially with the number of physical qudits used for logical encoding. The proximity ofto the fault-tolerant thresholdis modeled by a function:

|  |  |
| --- | --- |
|  | (32) |

whereis a system-dependent constant. Thus, the QEC complexity becomes:

|  |  |
| --- | --- |
| . | (33) |

Considering the fidelityof entangled states used in QKD, we can define a functionfor entanglement distillation cost as . With that, the modifiesto include the distillation factor is . Henceforth, the computational complexity now improves to:

|  |  |
| --- | --- |
| . | (34) |

Finite key effects are incorporated by considering the sifted key lengthand the final key length defined as . The computational complexity adjusts as:

|  |  |
| --- | --- |
| . | (35) |

For correlated errors in the quantum channel, letquantify error correlations. We introduce a correction factor as , whereis a scaling factor. Thus, the QEC complexity becomes . The final expression for computational complexity is:

|  |  |
| --- | --- |
| . | (36) |

The security of the protocol relies fundamentally on the no-cloning theorem, which prohibits the exact duplication of arbitrary quantum states and is further reinforced by entanglement, enhancing the confidentiality of quantum communication [47]. For an adversary attempting to compromise communication, denoted by, the probability of success decays exponentially with the security parameter is . This is bounded by the trace distance between the ideal stateand the adversarially obtained state as , wherequantifies the distinguishability of states, with security scaling as. Consequently, the key lengthcan also be linked to the min-entropy, which quantifies the uncertainty about the keygiven the adversary's knowledge by .

For coherent attacks, the adversary’s accessible information is bounded by the Holevo quantity by , whereis the von Neumann entropy of the adversarial state,is the state conditioned on the sender’s basis choice, andare the respective probabilities. Additionally, to model the computational complexity of the protocol, including key generation, sorting, and QEC, the total complexityis given as:

|  |  |
| --- | --- |
| , | (37) |

whereis the qudit dimension,is the qudit entropy,is the quantum channel error rate, andrelates to the QEC capacity. With that, to integrate channel capacity, which determines the reliable quantum communication rate over a channel, we refine the total complexity as:

|  |  |
| --- | --- |
| . | (38) |

For memoryless channels, the Holevo capacityprovides an upper bound for, and practical implementations, the finite-key analysis modifies the key length and associated security bounds. And, in finite-key settings, corrections to the key rate are introduced, considering the limited number of key bits:

|  |  |
| --- | --- |
| , | (39) |

wheredenotes the probability of key bitconditioned on the adversary’s information. The improved complexity model also incorporates composable security through parametersand, ensuring the protocol remains secure even when integrated with other cryptographic processes:

|  |  |
| --- | --- |
| . | (40) |

Hence, the QEC complexity term scales with a correction factor. Nevertheless, the generalized GHZ state employed in the QKD protocol extended to MPC is , whererepresents the global entanglement phase shared among theparties. Representing this state in a generalized Hadamard basis, we get:

|  |  |
| --- | --- |
| , | (41) |

where the basis states are , withbeing a local phase parameter. Moreover, the multipartite entanglement is quantified using the geometric measure of entanglement:

|  |  |
| --- | --- |
| , | (42) |

where the maximization is performed over all possible product states. For subsystems consisting ofparties (where), the entanglement entropy of the reduced density matrix is , whereis obtained by tracing out the remainingparties. The QFI for a Hamiltonianthat generates the GHZ state quantifies the sensitivity to variations in the associated parameter:

|  |  |
| --- | --- |
| . | (43) |

In the presence of noise, where local noise channelsact on each party, the state becomes . The properties of, such as entanglement or fidelity, can be analyzed to assess robustness against noise. The fidelity of the noisy state relative to the ideal GHZ state is then . Furthermore, measurement errors, denoted by a probability, modify the probabilities of outcomes. The observed probabilities are then described as:

|  |  |
| --- | --- |
| , | (44) |

whererepresents the ideal measurement probabilities. The generalized measurement operators in the equatorial plane of the Bloch sphere for a basisare , whereandare the Pauli matrices. Including an arbitrary phase, the operator generalizes to . Equivalently, using rotation operators, , whereis a rotation operator about the-axis. For parties, the probability of all measuring on the same basis and obtaining consistent results, incorporating phase coherence terms, is given by:

|  |  |
| --- | --- |
| . | (45) |

Integrating the effects of noise modeled by a CPTP mapfor each party, the probability becomes:

|  |  |
| --- | --- |
| , | (46) |

whereis the generalized GHZ state. For specific noise models like depolarizing noise with probability , the CPTP map is defined as, . Subsequently, measurement incompatibility can be analyzed through robustness measures, such as:

|  |  |
| --- | --- |
| , | (47) |

whereis a positive operator. Considering generalized measurements or POVMswith, the probability of an outcomefor a stateis . For collective measurements across multiple parties on a GHZ state, the probabilities reflect joint correlations and coherence. Robustness ofto phase variationscan be quantified using the QFI as , where. Additionally, for robustness to noise, consider the fidelity between the noisy stateand the ideal GHZ state, .

****

**Fig. 4** Combination of key aspects from the QKD protocol, entanglement, and Qsort operations across parties in an MPC protocol.

Fig. 4 shows an integrated QKD, multiparty entanglement generation, and Qsort within a unified MPC protocol as shown in this quantum circuit, implementing quantum operations to provide communication without eavesdropping. Data will be processed, and errors will be corrected privately due to post-processing.

The GHZ state establishes the entanglement between the parties in and CNOT gates [48]. This entanglement guarantees the generation of a globally shared quantum state that binds all parties together securely. The GHZ state is a basis for quantum-secure communication, allowing each pair of parties to generate a shared key needed for MPC protocols. The strong correlations in the entangled state provide resistance against eavesdropping attempts in detect unauthorized measurement disturbances [49].

After the generation of a GHZ state, phase-shifted Hadamard gates have been applied to place qubits into superposition states while simultaneously preserving the coherence of the entangled parties. A further layer is added to robustness against all possible eavesdropping of the quantum manipulation and measurement based on controlled interference patterns.

The next stage uses CNOT gates is extract keys in QKD. The entangled qubits are measured to extract secure cryptographic keys, which can be further used for encryption in secure quantum data-sorting protocols such as QSORT. QSORT uses quantum comparators, comprising Toffoli (CCX) gates for comparing qubit states and SWAP gates for rearranging qubits based on these comparisons, to efficiently sort the encrypted data within the quantum domain [50].

Pauli gates and rotation-based mechanisms are used to implement error correction and noise management. These operations detect and correct errors caused by noise, decoherence, or disturbances in the quantum system and ensure that communication and computation processes are reliable.

Finally, in the privacy amplification and post-processing, Rényi entropy applies to further stabilize the extracted key process and confirm non-presence with eavesdroppers. Here, the ensured integrity of this shared secret comes from filtering and removing any impacted information due to possible adversarial actions [51-52]. Further, the generated secure key adjusts dynamically according to noise levels or interference amplitudes, where it remains valid even in high-noise-level quantum environments.

However, the key extraction process is in a multiparty QKD scheme, with measurements defined as a bitwise XOR operation. Using the-qubit CNOT operation and individual measurement operators, the extracted key's density matrix can be defined as [53]:

|  |  |
| --- | --- |
| , | (48) |

whereand, , representing measurements in the-basis. Including a channel operatorfor error modeling on each qubit, the initial state transforms, . The extracted key's density matrix is modified to:

|  |  |
| --- | --- |
| . | (49) |

Considering an eavesdropper's interaction, modeled as a general unitary operatoracting on the system and the ancilla, the reduced density matrix after an interaction is:

|  |  |
| --- | --- |
| . | (50) |

Integrating over all possible eavesdropper interactions using the Haar measureover the unitary group, Eq. (50) generalizes to:

|  |  |
| --- | --- |
| . | (51) |

Using the operator-sum representation, where Kraus operatorsdescribe the eavesdropper's channel, the reduced density matrix can be written as:

|  |  |
| --- | --- |
| , | (52) |

whereensures trace preservation. To quantify the eavesdropper's information, the quantum mutual informationis , whereis the von Neumann entropy,, andis the joint state of the parties and eavesdropper. Additionally, introducing coherence preservation under measurement, the eavesdropper's interaction can be evaluated via its effect on off-diagonal elements of the density matrix, represented as . A decrease in coherence measures the degree of disturbance caused by, further enriching the analytical complexity. The fidelity analysis in multiparty QKD for Dsorting by entanglement is defined as:

|  |  |
| --- | --- |
| , | (53) |

Representing the post-interaction state using Kraus operators, the fidelity becomes:

|  |  |
| --- | --- |
| . | (54) |

Expanding Eq. (54):

|  |  |
| --- | --- |
| . | (55) |

The channel noise, modeled aswithas the Hamiltonian on the-th qubit, is expanded to second order, . Substituting into the fidelity expression (*i.e.,* Eq. (55)) and retaining terms up to second order in:

|  |  |
| --- | --- |
| , | (56) |

wheredenotes the commutator. The error model extends beyond single-qubit rotations to include correlated errors among qubits. The general error operator is , whereis a general-qubit Hamiltonian expanded as, . denotes subsets of qubits,, andare real coefficients representing interaction strengths (here, refers to the index set, ). For time-dependent noise, the coefficientsare functions of time, we get, , whereis the time-ordering operator. The key rate analysis for multiparty QKD, initially characterized by the effective key rate after QEC as:

|  |  |
| --- | --- |
| , | (57) |

can be extended to take into consideration the complete error model. Let the probability of no error on any qubit, , where the individual error probabilitiesderive from the refined noise model. Assuming a time-independent Hamiltonian, we computeas:

|  |  |
| --- | --- |
| , | (58) |

wheredenotes the trace over the-th qubit andis the trace over all other qubits. Substituting Eq. (58) refined expression for, the QEC rate becomes, . Thus, the effective raw key rate, previously defined as:

|  |  |
| --- | --- |
| , | (59) |

where,

|  |  |
| --- | --- |
| , | (60) |

is reformulated using the conditional von Neumann entropy. Letbe the joint state of Alice and Bob after sifting. Then, , whereis the conditional von Neumann entropy,is the von Neumann entropy, andis the reduced density matrix of Alice. The final secure key rate is enhanced by incorporating secret key agreement capacity:

|  |  |
| --- | --- |
| . | (61) |

Furthermore, the secret key agreement capacity,, is defined as, , whereis the conditional von Neumann entropy, andis the conditional entropy of the joint systemgiven the eavesdropper. Hence, for a multipartite setting, the secret key rate generalizes to:

|  |  |
| --- | --- |
| , | (62) |

whererepresents the conditional entropy of all parties' combined system given the eavesdropper's information. The secret key rate for multiparty QKD is , whererepresents the entropy of the raw key,corresponds to the entropy of the error-corrected key, anddenotes the quantum mutual information between partyand the eavesdropper. Thus, the mutual informationis defined in terms of von Neumann entropy as, , whereis the von Neumann entropy of the eavesdropper's quantum state, andis the conditional quantum state of the eavesdropper given measurement outcome, occurring with probability [54].

To further refine, let, whererepresents the joint quantum state of all parties and the eavesdropper. Using the spectral decomposition, , we computeas, . Additionally, the conditional entropyinvolves the conditional state, which depends on the measurement basis of party. Assuming projective measurements:

|  |  |
| --- | --- |
| . | (63) |

And the probabilitiesare given by:

|  |  |
| --- | --- |
| . | (64) |

Thus,

|  |  |
| --- | --- |
| , | (65) |

whereare the eigenvalues of. Furthermore, raw and error-corrected entropies are represented as and, respectively. Assuming, the entropy of the raw key is determined by, , where, . The entropy of the error-corrected keyis similarly computed using the post-error-correction state, .

Expandingusing the Kraus operatorsrepresenting the error correction process by , and substituting into the von Neumann entropy, we compute as, . And then, the secret key rate matrix, taking the QKD rates amongparties, is represented using matrix notation as:

|  |  |
| --- | --- |
| , | (66) |

where each elementcorresponds to the secret key rate between partiesand. In general, the matrixis non-symmetric (), integrating asymmetric noise, eavesdropping effects, or directional channel characteristics. The key rate for a specific partycan be expressed as a vector ( stand for matrix transpose), reflecting all ratesfromto other parties.

The error rate threshold,, is refined to include weighted contributions from individual channels, represented by a weight matrix, wherequantifies the significance of the channel. The threshold is given by:

|  |  |
| --- | --- |
| , | (67) |

whereis the QBER for the channel betweenand. For uniform weights, Eq. (67) reduces to a simple average of error rates. To incorporate the channel capacities, the normalized error rate threshold is expressed as:

|  |  |
| --- | --- |
| , | (68) |

whereis the quantum capacity of the channel, reflecting its ability to reliably transmit quantum information. Channels with higher capacities reduce the contribution of their associated QBER to. Moreover, a multiparty error measure is introduced based on the fidelity of the shared entangled state. Letbe the ideal-partite entangled state, andthe actual state after noisy transmission. The fidelity is given by:

|  |  |
| --- | --- |
| , | (69) |

where lower fidelity indicates higher deviations from the ideal state. An error measure for the multiparty system is defined as, measuring the collective impact of noise and decoherence across all parties. Additionally, to account for joint quantum correlations, we extend the secret key rate to include multiparty mutual information. The multiparty rate matrix is derived by considering contributions from conditional quantum states and their von Neumann entropies, , whereis the von Neumann entropy of the joint state betweenand, andaccounts for the correlations with an eavesdropper's state. However, the probability of matching measurement outcomes between partiesand, initially expressed as, can be generalized using the process of Positive Operator-Valued Measures (POVMs). Letanddenote the POVMs corresponding to partiesand, respectively, where and represent the possible measurement outcomes. The joint probability of outcomes and is given by:

|  |  |
| --- | --- |
| , | (70) |

whererepresents the shared quantum state. The probability of matching outcomes can be expressed as:

|  |  |
| --- | --- |
| . | (71) |

Eq. (71) generalizes the measurement process to arbitrary quantum states and POVMs, transcending the constraints of projective measurements. For specific basesand, and assumingis a maximally entangled Bell state, this reduces to the original cosine-squared dependency. Furthermore, the QBER betweenandis defined as the probability of mismatched outcomes, represented as:

|  |  |
| --- | --- |
| . | (72) |

If an error operatoracts on, the QBER is alternatively expressed as:

|  |  |
| --- | --- |
| . | (73) |

Eq. (73) links the observed QBER directly to the physical noise model and provides a pathway for characterizing errors in terms of operational properties of the quantum system. Hence, in the privacy amplification step, the key lengthis optimized using the min-entropy,, of the keyconditioned on the eavesdropper’s information. The final secure key lengthis bounded by , whereis the failure probability of the privacy amplification process. Consequently, the min-entropy is defined as, . To address statistical fluctuations and provide a robust security guarantee, the smooth min-entropyis employed:

|  |  |
| --- | --- |
| , | (74) |

whereis the trace distance. Hence, the final key length incorporating Eq. (74) refinement is bounded by, , wherereflects the security closeness of the final key to a uniformly random distribution.



**Fig. 3** Secure sorting using QKD and quantum gates. A secure sort protocol in an MPC setting for distributed data and implements key exchange securely between parties using QKD. It applies the encoding of quantum data, encrypts it, and has a sorting algorithm based on quantum comparison and swap. It ensures privacy through quantum encryption while detecting adversarial interference using QKD mechanisms and prevents unauthorized access to the data.

Fig. 3 is designed for sorting distributed data securely in the process of the QMPC protocol. In the first stage, the secure exchange of quantum states between the parties and is accomplished through QKD over a quantum channel. The quantum protocol applies the gate to qubit so that the put qubit is in a superposition. Then apply the entangling CNOT (CX) gate to and . Measuring and enables the detection of an eavesdropper since an interception would disturb the quantum state and cause the detection mechanism of the quantum protocol.

Once the safe key has been built, information from both parties is encoded into quantum states. Classical data, for example, , encodes into qubit using an gate. Another data element is put in superposition using , on . Encryption is performed using a CNOT gate. The common QKD (enciphered in ) is applied on the data qubit so that the encrypted contents are indistinguishable from any other party except the destination one.

The secure sorting algorithm embedded in the circuit is its essential component. A Toffoli (CCX) gate compares data in qubits and with as an ancillary bit for controlling the operation. After that, SWAP gate is applied on and based on the comparison result for swapping the data elements. Data confidentiality is maintained through the sorting operation because it deals with quantum encrypted states.

The whole protocol is configured such that all the sorted data will be guaranteed to be safe from unauthorized parties or even eavesdroppers since any interception or altering attempt will surely be detected by quantum encryption if used in conjunction with QKD. Meanwhile, the sorting process is conducted on quantum-encoded data, significantly improving the confidence in MPC protocols in quantum channels.



**Fig. 5** Multiparty qudit-based QKD, error correction, and Grover’s algorithm for secure sorting

Fig. 5 is the qudit-based multiparty protocol for QKD, error correction, and Qsort showing the preparation protocol for parties in a qudit-based GHZ state where each party would end up having a secure collective quantum state. Further, for preparing a qudit-based GHZ state, the circuit will apply the gate on and set it to be in a superposition state. Then, the entanglement is diffused to all parties involved by using CNOT gates on with the other qudits, to . This will be the basis for forming the GHZ state because of the correlations between the quantum states.

In key distribution, the phase rotation through gates encodes the shared key within the quantum states of the qudits. The specific phase shifts are introduced based on the index of each party's qudit, and the secure distribution of the key is ensured. Control over the phase is crucial for embedding the key, which can be achieved with the help of gates. Ancilla-assisted QEC introduces ancillary qudits from to where qudits connected with ancillas through CNOT gates extract disorder. The use of Toffoli gates for error detection and correction makes the quantum states noise resilient against the environment.

An ancilla-assisted entanglement purification method is utilized in the entanglement purification scheme to protect a GHZ state's fidelity. Errors are corrected, and the entangled state's purity is restored through CNOT gates acting between the participating qudits and an ancillary qudit. In the phase, encoding-based key distribution, gates perform phase-encoded operations dependent on the key qudit. This process ensures the key is securely embedded within the quantum states, making unauthorized access highly infeasible.

Randomized unitary operations are added to the qudits via the gates as part of the privacy amplification. By adding random phases and rotations, the protocol's security is typically increased by discouraging possible eavesdroppers. Hadamard transformations prepare the qudits for usage with Grover's oracle or Qsort. The CSWAP gates securely encrypt the quantum data by comparing and sorting the qudit states. In Grover's oracle, the diffusion operator amplifies the correct answer to aid in Qsort, while the CCCZ gates reverse the phase of the designated qudit states.



**Fig. 6** Multiparty QKD with Grover's algorithm and comparator operations: setup with three qubits for the parties and using and gates to create an entanglement. Encryption is performed by using a multi-controlled Pauli-X gate controlled by the shared keys and a multi-controlled Pauli-Z gate controlled by the shared keys . Comparator operations are performed with CSWAP gates, also called Fredkin gates, where the qubit states depend on being swapped for secure data processing. Grover's oracle and diffusion operator amplify the correct solution in the multi-qubit search space. The results of the quantum operations are extracted in the final quantum measurement, containing key extraction and data decryption.

Fig. 6 shows a more sophisticated multi-party QKD protocol with Grover's search algorithm [55], comparator gates to encrypt [56], and invert phases while sorting [57-58]. Multi-qubit entanglement begins with first entangling the qubits , , and . An gate is applied to followed by a sequence of CNOT gates to form a generalized Bell state. It forms an entangled shared state among parties, which serves as a base for secure communication.

In the encryption section, multi-controlled Pauli-X and Pauli-Z operations rule over the encryption. Key qubits and are controlled by these operations. They represent the values of keys and . The Pauli-Z gate gives the phase shift to these key values so that they can encrypt efficiently but don't allow an unauthorized person to eavesdrop.

In the comparator gate operations phase, comparator operations are performed by CSWAP gates, which are also known as Fredkin gates [59]. The gates enable the conditional comparison of qubit states, thus ensuring secure data processing. By swapping quantum states according to the results of comparisons, the protocol allows elements to be sorted according to specific criteria, thereby improving the capability of secure data handling. This is the correct answer or outcome being sought. The Grover oracle changes the phase of the marked state in the superposition over the encrypted data, in Grover's search algorithm.

During the diffusion phase by Grover, this marked state is amplified by the diffusion operator after the phase flip, so that at the end of this quantum computation process, this process yields the correct result with a higher probability. This is a significant step in efficiently searching through large datasets encrypted within the QKD system.

Finally, applying quantum measurement in the quantum measurement towards the end to reveal the quantum computation results from key extraction as well as encryption of data itself, Grover's algorithmic system ensures an enhanced secure provision of keys from circuit entanglement, a superposition use, and applying control operations through comparator operations to ensure an easier sorting mechanism of keys.

## ****Entanglement-Based QKD****

The key generation process is based on a shared entangled state for parties and . To specify the entanglement and key extraction, we introduce an entanglement state generalizing the state of parties and :

|  |  |
| --- | --- |
| . | (75) |

The corresponding density matrix representation generalizes the state to mixed entangled states:

|  |  |
| --- | --- |
| . | (76) |

Rewritingin the Bell basis:

|  |  |
| --- | --- |
| , | (77) |

the stateis expressed as a linear combination:

|  |  |
| --- | --- |
| . | (78) |

Key derivation employs measurements, formally defined by a POVM:

|  |  |
| --- | --- |
| . | (79) |

The functionmaps measurement outcomes to classical key bits, preserving the key’s randomness and security through post-processing protocols, . For an-party system, the multi-partite quantum state is expressed via a tensor product as, , or its density operator counterpart, . The local measurement outcomes ofandgenerate the classical key matrix, , wherearises from correlated outcomes in. So, to quantify entanglement, the concurrence ofis used:

|  |  |
| --- | --- |
| , | (80) |

whereare the square roots of eigenvalues of, arranged in descending order. With that, for multi-partite entanglement, measures such as the geometric entanglement:

|  |  |
| --- | --- |
| , | (81) |

and-tangles for multipartite states provide quantification. These metrics ensure the security and entanglement properties required for QKD. Moreover, the QKD protocol stems from the entropy () of measurement outcomes, bound by:

|  |  |
| --- | --- |
| , | (82) |

whereis the von Neumann entropy, the quantum channel, which transforms a density operator, is , whereis the initial density operator shared between partiesand, andis the resultant state post-transformation. The keyis extracted via measurement on, , withdescribed by POVMs, such that the probability of outcomeis:

|  |  |
| --- | --- |
| . | (83) |

Here,is a classical post-processing function mapping outcomes to classical key bits. Subsequently, the quantum channelis represented in the operator-sum form, , whereare Kraus operators satisfying. For example, the depolarizing channel is represented by, , whereis the depolarizing probability, andis the dimension of the system. With that, the encryption process is described by the unitary operator, defined as, , where the control qubit is a classical bit, and the target qubit is the data qubit. A generalization employs a controlled-unitary operator, , whereandare arbitrary unitaries acting on the data qubit. Additionally, for quantum encryption involving ancilla qubits, the encrypted state is:

|  |  |
| --- | --- |
| , | (84) |

whereis a key-dependent unitary operator. For a general scheme, the keycan itself be a quantum state, leading to a joint unitary operation:

|  |  |
| --- | --- |
| , | (85) |

whereare unitaries conditioned on both the key and the data qubit. So, the measurement and encryption procedures involve security guarantees derived from the von Neumann entropy as , and the key’s mutual information with Eve, bounded by, . Moreover, let the density operator 𝜌𝐷 represent the datasetas, , whereare density operators representing individual data states,for an-qubit encoding, and. For encrypted datasets, the quantum encryption operation is defined as:

|  |  |
| --- | --- |
| , | (86) |

whereis a unitary operator parameterized by the quantum key. The encryption process may be further generalized by modeling it as a quantum channel such that, , where, with Kraus operatorssatisfying. Hence, if the quantum keyitself is a quantum state represented by, the encrypted state becomes:

|  |  |
| --- | --- |
| , | (87) |

whereis the controlled-unitary operator. Expanding Eq. (87), we obtain:

|  |  |
| --- | --- |
| . | (88) |

Introducing an interaction Hamiltonian, the unitary evolution of the system is , whereis the interaction time andis the reduced Planck constant. When the key is entangled with an ancillary system, such that the joint key-ancilla state is , whereare orthonormal states, the encrypted state becomes:

|  |  |
| --- | --- |
| . | (89) |

Expanding Eq. (89) leads to:

|  |  |
| --- | --- |
| . | (90) |

If the ancilla states are orthonormal (), Eq. (90) simplifies to:

|  |  |
| --- | --- |
| . | (91) |

In a multiparty setting withparties, the key is distributed as, and the encryption unitary is represented as, . So, the encrypted state then becomes:

|  |  |
| --- | --- |
| . | (92) |

The comparator operation representswithin the entanglement-based QKD process for MPC. Initially described as, whereis the identity operator on the key space. Therefore, the decomposition in terms of conditional operations can be written as:

|  |  |
| --- | --- |
| , | (93) |

effectively implementing a comparator gate. For enhanced quantum treatment, we introduce an ancilla qubit, initialized to, to encode the comparison outcome:

|  |  |
| --- | --- |
| , | (94) |

whereis the Heaviside step function, encoding the comparison condition. Hence, the comparison operation, incorporating a conditional-SWAP based on the ancilla qubit, is given by:

|  |  |
| --- | --- |
| , | (95) |

where the SWAP operation acts onandstates. The combined comparator and conditional-SWAP operation, therefore, becomes:

|  |  |
| --- | --- |
| , | (96) |

with the SWAP operation further decomposable into controlled-NOT (CNOT) gates as, . To account for noise and probabilistic outcomes in quantum operations, the comparator operation is generalized to a CPTP map, where the input stateevolves to:

|  |  |
| --- | --- |
| , | (97) |

with Kraus operatorssatisfying. The operatorsare parameterized to model different error profiles during the comparator operation. Additionally, incorporating the key into Eq. (97) process requires defining the initial state as, whererepresents the density operator of the key space. The combined comparator operation with the key can then be expressed through a CPTP map:

|  |  |
| --- | --- |
| , | (98) |

whereare Kraus operators on the joint data and key space. Subsequently, to further generalize, if the key states are entangled, represented as, the interaction Hamiltonian governing the comparator operation can be written as, , leading to a unitary evolution, . The combined system evolution, including the entangled key is . Furthermore, the quantum oracle for sorting, initially represented as, whererepresents a superposition state, requires refinement to sorting. Definingas a Boolean function that outputsfor sorted sequences andotherwise, the oracle can be described by:

|  |  |
| --- | --- |
| . | (99) |

To include encryption, letbe the encryption unitary acting on the quantum states. The encrypted sorting oracle becomes:

|  |  |
| --- | --- |
| . | (100) |

Expandingas a function of keys, we express, , whereare key states, andare the corresponding encryption unitaries. Substituting into (i.e., Eq. (100)), we get:

|  |  |
| --- | --- |
| . | (101) |

To introduce QEC, letbe an encoding map such that|. The encoded sorting oracle is then:

|  |  |
| --- | --- |
| . | (102) |

The evolution of the sorting system can be analyzed using a Hamiltonian, where the time-dependent state is given by, . A Hamiltonian implementing the sorting operation can be constructed such that:

|  |  |
| --- | --- |
| , | (103) |

whereare eigenvalues encoding sorting constraints. Therefore, for security analysis, let the joint state of data and keys be. The mutual information between data and key, quantifying their correlation, is given by, , whereis the von Neumann entropy. To model errors, the sorting process is described using a CPTP map, such that, , whereare Kraus operators satisfying.

## ****Security Analysis****

The entropy analysis of the encrypted dataset, utilizing QKD encryption, requires the joint state, which encodes the correlations and entanglement between the dataand the key. The von Neumann entropy of this joint state is given by [61]:

|  |  |
| --- | --- |
| , | (104) |

whererepresents the combined density matrix ofand. The marginal states are obtained through partial traces,and, with their entropies, . Additionally, the conditional entropyquantifies the uncertainty of the datasetgiven the key, derived as [62]:

|  |  |
| --- | --- |
| . | (105) |

Absolute secrecy is achieved if, where the key provides no additional information about. Conversely, mutual informationmeasures the correlation betweenand, . To incorporate noise effects, consider a quantum channel, represented by a set of Kraus operators, such that the key's state evolves as, , and the impact on conditional entropy and mutual information is analyzed by substitutinginto the corresponding expressions.

An eavesdropping attack can be modeled as a unitary operationacting on the joint systemand an ancilla state, leading to the extended state, . The eavesdropper's accessible information is quantified by the mutual information [62]:

|  |  |
| --- | --- |
| , | (106) |

whereand. For multiparty QKD, if the key is distributed amongparties as, the joint state becomes. The mutual information and entropy measures extend to include all parties, such as , capturing the interdependencies within the multiparty key distribution process. Introducing a noise channelonaffects the joint state as [63]:

|  |  |
| --- | --- |
| , | (107) |

whereoperates on. The security analysis then involves recalculating entropies and mutual information for. Furthermore, the bound-on information leakagefails to adequately incorporate the principles of quantum information theory [64]. Letdenotes the joint density matrix of the encrypted dataand the eavesdropper's system. The Holevo quantityis expressed as:

|  |  |
| --- | --- |
| , | (108) |

whereis the reduced state of the eavesdropper,represents the probabilities of the data states, andis the conditional state ofgiven the data state. Hence, the Holevo quantity bounds the mutual information betweenandas,

|  |  |
| --- | --- |
| . | (109) |

Eq. (109) inequality provides an improved constraint on, ensuring it aligns with the structure of quantum information leakage. Utilizing the min-entropy, the leakage can also be expressed in terms of the eavesdropper's optimal guessing probability, , while the max-entropy, defined as, whereis the projector on the support of, further refines the upper bound of information available to the eavesdropper [64]. Smooth entropy forms, such as the smooth min-entropy, extend these concepts to account for small perturbations:

|  |  |
| --- | --- |
| , | (110) |

whererepresents the smoothing parameter, ensuring robustness against errors. Furthermore, in multipartite systems, where the encrypted datasetand the keyare distributed amongparties with joint state, the leakage extends to encompass multiparty interactions [65]. If an eavesdroppergains access to a subset, the multipartite mutual information is:

|  |  |
| --- | --- |
| . | (111) |

Eq. (111) measure integrates multipartite entanglement to evaluateunder collective attacks. Incorporating privacy amplification, where the keyundergoes a hash transformation, reducesfurther. The leftover hash lemma quantifies the reduction, , whereis the length of the hashed key, ensuring negligible leakage. Next, the quantum hash function, initially represented as. The XOR operationis not inherently compatible with quantum states [67]. Instead, consider the statecombined with an ancilla initialized to. The hash function ( is implemented as a unitary transformationsuch that:

|  |  |
| --- | --- |
| , | (112) |

whererepresents the quantum hash value.can be decomposed as , where eachis a controlled unitary that manipulates the ancilla register-based on the input qubits. Eachmay involve controlled-NOT gates, phase rotations, and Hadamard operations combinations. The probability of failureis replaced by analysis using the collision probability, . For integrity verification, the quantum oracle is formalized as:

|  |  |
| --- | --- |
| , | (113) |

whereif, andotherwise. Implementinginvolves a series of controlled operations conditioned on comparisons betweenand. In a database search ofentries, Grover's algorithm provides a quadratic speedup. The oracle for Grover's search is defined as [68]:

|  |  |
| --- | --- |
| , | (114) |

whereencodes the index of the database entry. Repeated applications of Grover iterations, whereis the uniform superposition of all index, yield the desired result withiterations. QEC ensures robustness against noise during the process. Logical statesare encoded using quantum error-correcting codes (QECCs) as, , whererepresents the encoded state [69-72]. Upon error(modeled by Kraus operators), error correction applies a decoding map, ensuring recovery:

|  |  |
| --- | --- |
| . | (115) |

The QECC must satisfy the quantum error-correcting condition, , whereare constants ensuring distinguishability of logical states. For fault-tolerant sorting, error correction can be applied iteratively:

|  |  |
| --- | --- |
| . | (116) |

Eq. (116) guarantees that sorting operations preserve data integrity under quantum noise. The total error operatoracting on qubits, initially expressed as, with, must incorporate a general error model for higher precision. The error operatoris described as a superposition of Pauli strings (:

|  |  |
| --- | --- |
| , | (117) |

where,, and. The density matrix transformation under this error operator is, . For the quantum noise model, the error dynamics are described via a quantum channel characterized by Kraus operators:

|  |  |
| --- | --- |
| . | (118) |

The probability of an error associated withis given by. For logical states encoded via, where, the error acts as . The decoding operationapplies subsequent measurements to identify and correct errors. A general error-correction condition is satisfied when, , ensuring that the logical states remain distinguishable under error transformations. Hence, the probability of successful correction, taking into account the weight distribution of the error model is:

|  |  |
| --- | --- |
| , | (119) |

wheredenotes the weight of the Pauli string, i.e., the number of non-identity operators in. For a depolarizing channel with an error rate, the probability of a Pauli erroris:

|  |  |
| --- | --- |
| . | (120) |

Thus,for Eq. (120) model is:

|  |  |
| --- | --- |
| . | (121) |

Eq. (121) improves the approximationby explicitly incorporating the distribution of errors. For concatenated codes, where encoding and error correction are applied recursively, the effective logical error rateis , whereanddepend on the structure of the concatenated code and the noise model. These codes ensure exponentially improved error suppression with each level of concatenation.

For sorting with noisy operations, the propagation of errors is analyzed using the fault-tolerance threshold theorem. Letrepresent the noisy sorting operation. The effective error rate afteroperations is:

|  |  |
| --- | --- |
| . | (122) |

The accumulated errormust remain below the code’s correction threshold to maintain reliability. Likewise, Let the encoded quantum statebe mapped to a higher-dimensional Hilbert space via an encoding operation, where. The error operatoracting on the encoded state defined with Kraus operatorsassociated with a quantum channel:

|  |  |
| --- | --- |
| . | (123) |

Eachis a linear combination of Pauli operators, . Henceforth, the encoded state remains correctable under the QECC if the error maps it to the correctable subspace. Let denote the projector in the code space:

|  |  |
| --- | --- |
| . | (124) |

The probability of successful correction, for a specific error, is defined as:

|  |  |
| --- | --- |
| . | (125) |

Considering a general error channel with Kraus operators, the average probability of correction is:

|  |  |
| --- | --- |
| . | (126) |

In the case of a depolarizing channel with error rate, where the probability of a Pauli errorof weightis given by:

|  |  |
| --- | --- |
| , | (127) |

the probability of successful correction is approximated by summing over all correctable errors:

|  |  |
| --- | --- |
| . | (128) |

For concatenated QECCs appliedtimes, the effective error rateafterlevels of concatenation is:

|  |  |
| --- | --- |
| . | (129) |

Fault-tolerant operations ensure that the spread of errors is constrained during the computation process. Ifrepresents the error rate per quantum gate andis the circuit depth, the accumulated error probability is bounded by:

|  |  |
| --- | --- |
| . | (130) |

Eq. (130) condition imposes a threshold, below which arbitrary quantum computations can proceed reliably:

|  |  |
| --- | --- |
| . | (131) |

Thus, the probability of successful correction under a concatenated fault-tolerant form is enhanced to:

|  |  |
| --- | --- |
| . | (132) |

The representation is invalid for analyzing QEC in entanglement-based QKD and MPCs.

## ****Quantum Dynamics in Sorting****

The quantum dynamics of sorting in the Qsort mechanism are described through quantum principles. The evolution of the encoded quantum statethrough a unitary sorting networkis given by:

|  |  |
| --- | --- |
| , | (133) |

whereis expressed as a sequence of interdependent unitary transformations:

|  |  |
| --- | --- |
| , | (134) |

with eachrepresenting a layer of operations corresponding to comparisons and swaps within the Qsort network. Since, define the comparison operator, acting on qubitsandand an ancillainitialized to, , where, encoding the comparison result as a step function. Moreover, the conditional swap operation, controlled by the ancilla qubit, is defined as:

|  |  |
| --- | --- |
| , | (135) |

where,represent swapped states if, otherwise they remain unchanged. Hence, the composite unitary operation for comparison and swapping is . The sorting network is constructed through a sequence of theseoperations applied in a specific order based on the sorting algorithm. For an-qubit system, the network involvesoperations for quantum merge sort, orfor bubble sort [73-75]. For this, incorporating encryption and decryption, the evolution becomes:

|  |  |
| --- | --- |
| , | (136) |

whereis the unitary operator encoding the quantum data, ensuring secure input to the sorting network. And, the unitarycan be analyzed through the time-dependent Schrödinger equation as , whereis the Hamiltonian governing the sorting process. The unitary evolution operator is derived as . The Hamiltonianis designed to encode the sorting dynamics, such that, , whereare time-dependent coefficients andare projection operators enforcing the comparisons and swaps. Hence, error-protected operations are implemented in the presence of a fault-tolerant design. Letdenote the Kraus operators of a noise channel affecting the sorting process. The effective unitary evolution under noise is then:

|  |  |
| --- | --- |
| . | (137) |

Considering computational complexity, the Qsort network achieves asymptotic scaling advantages when implemented on fault-tolerant architectures. For-level concatenated codes, the error suppression, , whereis the base error rate, ensuring accurate sorting even in noisy environments. Furthermore, the sorting oracleis defined as acting on an-qubit data state, with the marking functiondependent on the relative order of all elements:

|  |  |
| --- | --- |
| . | (138) |

Here,if, otherwise. Consequently, when encryption is applied, the data state is transformed by an encryption unitary, parameterized by the key. The encrypted oracle acts as:

|  |  |
| --- | --- |
| . | (139) |

To encode the Eq. (139) Qsort process dynamically, the state evolution is governed by the time-dependent Schrödinger equation, , whereis the Hamiltonian encoding the oracle, comparisons, and swaps. The corresponding unitary evolution operator is:

|  |  |
| --- | --- |
| , | (140) |

withdenoting time-ordering. For sorting,can be decomposed into layers, , whereimplements specific comparison or swap operations between qubitsand, andare time-dependent coefficients ensuring dynamic control over the operations. Also, using tensor network formalism, the multi-qubit state is represented as:

|  |  |
| --- | --- |
| , | (141) |

whereare tensor elements. Operations such as comparisons or swaps are modeled as tensor contractions:

|  |  |
| --- | --- |
| . | (142) |

Entanglement swapping within the sorting network utilizes Bell states as stated in Eq. (77). The Bell measurement projects the state into one of these basis states, enabling remote entanglement between qubits, represented as, , whereandencode the amplitudes before and after entanglement swapping. And, Qsort complexity is characterized by the circuit depth, scaling as, , for efficient sorting algorithms like quantum merge sort. The oracle's effect on circuit depth and time complexity is parameterized by, , whererepresents the operator norm of. And, the quantum state at each stage of the sorting process is represented by a higher-order tensor of the form:

|  |  |
| --- | --- |
| , | (143) |

whereare the tensor coefficients encoding the quantum amplitudes and correlations of the system. Initially,may correspond to a separable state, but the tensor evolves under unitary operations to reflect entanglement and correlations induced by the sorting process. Resulting, the unitary evolution of the state is described by:

|  |  |
| --- | --- |
| , | (144) |

whereare the matrix elements of the unitary operation. The unitaries are applied iteratively, such that afteroperations, the tensor coefficients are:

|  |  |
| --- | --- |
| . | (145) |

In Eq. (145), a tensor contraction reduces the computational complexity of the operation by summing over shared indices in the tensor network. Subsequently, the sorted basis states are defined as, where. The final sorted state can be expressed as:

|  |  |
| --- | --- |
| , | (146) |

whererepresents the coefficients after sorting. Ideally,for the sorted configuration and 0 otherwise. With that, the fidelity of sorting can be assessed by projecting the final state onto the ideal sorted subspace:

|  |  |
| --- | --- |
| , | (147) |

with the probability of success given by:

|  |  |
| --- | --- |
| . | (148) |

Entanglement generated during the sorting process is quantified through reduced-density matrices. For example, tracing out all but the firstqubits, , and the von Neumann entropy measures entanglement, . Hence, sorting can also be analyzed using time-dependent dynamics. The state evolution follows the Schrödinger equation, , whererepresents the Hamiltonian governing the sorting process. For a two-qubit comparator gate, the Hamiltonian can be represented as:

|  |  |
| --- | --- |
| , | (149) |

with,,denoting the Pauli matrices. The solution to the Schrödinger equation yields the unitary evolution operator:

|  |  |
| --- | --- |
| , | (150) |

whereindicates time-ordering. In conclusion, incorporating tensor network methods such as Matrix Product States (MPS) can reduce the complexity of simulating these quantum processes by exploiting low-rank decompositions of.



**Fig. 7** Multiparty entanglement-based QKD with error correction, quantum channels, controlled encryption, and Grover’s oracle.

Fig. 7 shows the circuit using four qubits, , , , and , to extend the bipartite entanglement to the multiparty context in the subsection on multiparty entanglement. The quantum communication protocol assigns these qubits to different parties, resulting an entanglement structure. This will significantly increase the resilience of quantum communication by guaranteeing that each party may communicate with every other party. To provide a realistic estimation of the system's resilience against noise, which is required for the stability assessment of the quantum state and the key distribution process, the channels, which represent bit-flip and phase-damping errors, are included in the noise modeling section as the quantum noise channels.

The error detection and correction component uses ancilla qubits to implement the error detection and correction techniques. One data qubit is used for CNOT gate interactions, and noise disturbances are used to identify the activity of this qubit. For this reason, faults are fixed and the original quantum state is preserved using controlled-controlled gates, or CCGs.

Using phase shifts conditioned on a shared quantum key , controlled gates are used in the safe encryption portion to offer secure encryption of information qubits. Therefore, phase encoding will guarantee that the data being transferred cannot be compromised while being sent. In this instance, the key is essential to the sequence of encryption processes. In order to securely generate keys and perform other quantum calculations within the system, ancillary qubits are used in the QPE section to measure the phase of the encrypted quantum states.

In Grover's algorithm section, the oracle for Grover's circuit in this part makes use of gates to increase the likelihood of discovering the answer and CCCZ gates to carry out phase inversion. As a result, it is effective in the key extraction procedure.

CSWAP comparator gates are used in the CSWAP part of integrity checking to confirm that the encrypted quantum states' integrity is good without information leaking. Therefore, during the verification process, the integrity of the encryption will be maintained. Following the implementation of Grover's oracle and error correction, the qubits , , , and the key qubit are measured in the key extraction section. The secure quantum key is then derived from this measurement, allowing for secure communication with strong protection against malevolent activity.

## ****Security Model****

Let the quantum interaction between the eavesdropperand the shared quantum channelbe described as a quantum operation. Denote the eavesdropper's unitary interaction as, acting on the joint system of the shared stateand the eavesdropper's ancillary state, such that:

|  |  |
| --- | --- |
| . | (151) |

If the eavesdropper's ancilla is initialized in the state, the post-interaction joint state can be defined as, , whererepresents the initial shared state between partiesand. The reduced density matrix of the eavesdropper is obtained . The information accessible to the eavesdropper can be quantified using the mutual information:

|  |  |
| --- | --- |
| , | (152) |

wheredenotes the von Neumann entropy. The accessible information is bounded by the Holevo quantity:

|  |  |
| --- | --- |
| , | (153) |

whereare the probabilities of different measurement outcomes andare the conditional post-measurement states of the eavesdropper. For intercept-resend attacks, the eavesdropper's success probabilityis related to the QBER as:

|  |  |
| --- | --- |
| , | (154) |

where represents the deviation introduced by the eavesdropper, andcharacterizes the noise variance of the channel. In internal eavesdropping by a colluding subset, the joint state is represented as, whereandare the reduced density matrices of the colluding and non-colluding subsets, respectively. The mutual information extracted by the colluding parties is given by:

|  |  |
| --- | --- |
| . | (155) |

A tighter bound on the eavesdropper's ability to extract information can be achieved using the smooth min-entropy, where:

|  |  |
| --- | --- |
| , | (156) |

withdenoting the trace norm anda small error tolerance. The smooth min-entropy bounds the guessing probability of the eavesdropper:

|  |  |
| --- | --- |
| . | (157) |

In multiparty settings, multipartite entanglement measures such as the entanglement of formationor the squashed entanglementare employed. For example, the entanglement cost of distilling secure keys is given by:

|  |  |
| --- | --- |
| , | (158) |

whereare pure-state decompositions of. The secret key rateis determined by the Devetak-Winter rate:

|  |  |
| --- | --- |
| , | (159) |

where the infimum is taken over all quantum operations accessible to the eavesdropper. The probability of eavesdropper success,, is strengthened by connecting it to operational measures such as the quantum Rényi entropy, wherecontrols the eavesdropper's strategy.

The probability of eavesdropping detectionand its connection to detection probability, based on fidelity, requires significant refinement for security analysis in QKD. Assuming independent and identical checks acrosschannel uses, the initial modelis overly simplistic, as correlations between channel uses must be incorporated. The detection probability, where, directly measures fidelity but insufficiently addresses security implications under realistic protocols.

Considering a general eavesdropping interaction represented by a unitary operatoracting on the combined state of the channeland the eavesdropper's ancilla, , the post-interaction state becomes , whereis the shared initial state. The reduced state of the eavesdropper is . The mutual information quantifying the eavesdropper's knowledge about the shared system is:

|  |  |
| --- | --- |
| , | (160) |

whereis the von Neumann entropy. The Holevo quantity provides an upper bound:

|  |  |
| --- | --- |
| , | (161) |

withas measurement probabilities andas conditional post-measurement states. In protocols with sifting, error correction, and privacy amplification, the QBERplays a crucial role. The detection probability relates to QBER via , whereencapsulates the channel noise and eavesdropping contributions. This estimate, however, fails to demonstrate the eavesdropper's potential correlations and adaptive strategies.

A robust analysis leverages entropic uncertainty relations and smooth min-entropy. For a secret keyof length, , ensuring the eavesdropper's guessing probability satisfies:

|  |  |
| --- | --- |
| . | (162) |

The leftover hash lemma tiesto the final secret key after privacy amplification:

|  |  |
| --- | --- |
| , | (163) |

whereis the smoothing parameter. Multipartite settings require multipartite entanglement measures such as the squashed entanglement, where:

|  |  |
| --- | --- |
| , | (164) |

and protocols account for collective attacks involving correlated measurements. The initial models for,, and fidelity measures are elevated to address realistic QKD constraints, unitary dynamics, and entropic bounds.

A set of partiesholds private datasets, and letdenote the function to be jointly computed. The condition, ensures privacy. Moreover, let the system's initial state be, withdenoting the state post-execution of protocol. The adversary's view,, is the partial trace over honest parties' subsystems. A simulator, given the corrupted parties' inputsand the function output, produces a state. The privacy condition becomes, , wheredenotes the trace norm, andis negligible. This guarantees computational indistinguishability between real and simulated protocol executions.

For any coalition, the conditional von Neumann entropyquantifies the uncertainty about, given the information accessible to. It is expressed as:

|  |  |
| --- | --- |
| , | (165) |

whereis the von Neumann entropy of system. For, the coalitionhas negligible information about, ensuring privacy. The guessing probabilityfor a keyshared between partiesanddepends on the key's randomness and any eavesdropper's side information. Using the smooth min-entropy, the security condition becomes, ,

implying:

|  |  |
| --- | --- |
| . | (166) |

The security of QKD-based MPC relies on the entropic uncertainty relations, which for measurementsandon a quantum state, satisfy , whereis the Hilbert space dimension. Multipartite entanglement measures further refine the analysis. Letdenote squashed entanglement:

|  |  |
| --- | --- |
| , | (167) |

determining correlations between subsets of honest parties and adversaries. Security against collective attacks or joint measurements by colluding parties requires bounding the adversary's accessible information through multipartite entanglement entropy measures.

## ****Quantum Attack Models and Mitigation Strategies****

In intercept-resend attack incorporating quantum state transformations, entropic measures, and mitigation strategies. Letrepresent the initial shared quantum state betweenand. The eavesdropper, utilizing measurement operators, modifies the state as:

|  |  |
| --- | --- |
| , | (168) |

where. The conditional post-measurement state for outcomeis:

|  |  |
| --- | --- |
| . | (169) |

The state received byafter's intervention becomes , with. To evaluate's influence, the fidelity betweenandis . However, the probability of successful eavesdropping,, depends not just onbut also on's information gain. The mutual informationis given by:

|  |  |
| --- | --- |
| , | (170) |

whereis the von Neumann entropy, . The Holevo quantity, bounding, is:

|  |  |
| --- | --- |
| . | (171) |

The eavesdropper's undetection probability can be linked to the QBER,, defined as, , whereis the error projection operator.exceeding a critical threshold,, implies eavesdropping detection. In entanglement-based QKD, the state verification employs Bell inequalities. For the shared Bell state, the observed correlation coefficientmust satisfy:

|  |  |
| --- | --- |
| ,  . | (172) |

QEC codes mitigate noise and attacks. Letbe a QEC code correcting up toerrors. The logical state is encoded as , withcoefficients distributed across physical qubits. The fidelity after QEC is , whererepresents residual error. Privacy amplification refines(shared key) to, reducing's accessible informationto a negligible value, ensuring, .

Let the initial staterepresent the shared quantum state betweenand. The eavesdroppermodifies the communication channel, described as a quantum operation, composed of Kraus operators, satisfying. The transmitted state toafter's intervention is , whileretains part of the system, yielding a joint state:

|  |  |
| --- | --- |
| , | (173) |

whererepresents orthogonal states within's ancilla. The fidelity, defined as, , quantifies the deviation introduced by. However,(MITM stand for Man-In-The-Middle) is tied to, the state retained by, where. The no-cloning theorem restricts absolute duplication but permits approximate cloning, bounded by:

|  |  |
| --- | --- |
| , | (174) |

wherereflects the minimum disturbance detectable byandvia quantum error analysis. The mutual informationevaluates's knowledge of the system, , and is bounded by the Holevo quantity, , whereand. MITM detection involves QBER analysis, where the error ratefor a transmitted stateis:

|  |  |
| --- | --- |
| , | (175) |

withas the error projection operator. For, the attack is detected. Authentication of classical channels enforces security by appending hash-based MACs (Message Authentication Codes) or quantum authentication, , whereis a cryptographic hash function andis a shared classical key. Quantum authentication employs entangled statesto encode identities, such that the verification condition for the authenticated stateis:

|  |  |
| --- | --- |
| , | (176) |

withrepresenting acceptable error bounds. In contrast to classical cryptographic vulnerabilities under Shor's algorithm, which disrupts RSA by exploiting efficient integer factorization:

|  |  |
| --- | --- |
| , | (177) |

The probability of a quantum computer breaking the QKD key,, characterizes the probability of guessing a uniformly random key of size. However, this represents classical key guessing, not the security breach of QKD. The security of QKD relies on quantum mechanics principles, not computational hardness assumptions. Thus, Shor's algorithm, which efficiently computes discrete logarithms and factors large integers, does not affect the quantum-security guarantees of QKD. The Shor's algorithm implies exponential speedup for specific number-theoretic problems:

|  |  |
| --- | --- |
| . | (178) |

QFT enables efficient determination of, the periodicity, leading to efficient factorization. However, QKD leverages laws such as the no-cloning theorem, , ensuring that absolute duplication of unknown quantum states is impossible.

In error correction for QKD, the failure probabilitysimplifies error dynamics but assumes independence across qubits. A more robust formulation considers a general error channel described by Kraus operators, , where eachis decomposed as, , withas Pauli operators andas complex coefficients. Encoding a logical qubitinto a code spaceensures resilience against errors. The probability of successful correction is:

|  |  |
| --- | --- |
| , | (179) |

and the failure probability becomes:

|  |  |
| --- | --- |
| . | (180) |

For a depolarizing channel with error rate, the probability of failure when correcting up toerrors out ofphysical qubits is approximated as:

|  |  |
| --- | --- |
| . | (181) |

Eq. (181) determines correlated and independent errors more accurately than the simplified expression. Authentication in QKD involves integrating quantum-resistant classical protocols for basis reconciliation and privacy amplification. The secure classical communication ensures the integrity of key reconciliation by cryptographic techniques like digital signatures or quantum-based methods. The overarching security system of QKD against quantum attacks integrates fault-tolerant techniques to ensure computational integrity. Fault tolerance leverages concatenated codes and transversal gates, bounding error propagation within thresholds, , whereis the redundancy factor. The threshold theorem guarantees reliability if [76-77] (see **Algorithm 1** and **Algorithm 2** for more details).

|  |
| --- |
| **Algorithm 1:** QKD and MPC for Secure Dsorting |
| **Input:**   * **Parties:** , . * **Dataset:** . * **Quantum and Classical Channels:** Quantum channel and classical channel .   **Output:**   * Securely sorted dataset .   **Begin:**  ***Step 1:* Initialization Phase**   1. *Define Parties: ,*   Each can be either honest-but-curious or dishonest.   1. *Dataset Initialization:*   Dataset is distributed such that where .   1. *Channel Setup:* Quantum channe**l** :   Classical Channel*:* Authenticated using secure digital signatures; not confidential.  ***Step 2:* Dynamic QKD Protocol Setup**   1. *State Preparation:* 2. *Dynamic Noise Adaptation:* Noise model :   Adaptive key rate based on noise:   1. *Eavesdropper Detection Model:*   Using disturbance:  Dynamic response based on : If , initiate re-keying.   1. *Entanglement Swapping and Quantum Teleportation:*   To reduce qubit transmission, utilize teleportation:  The entanglement swapping operator allows shared entanglement:  ***Step 3:* Key Extraction and Privacy Amplification Phase**   1. *Qudit-Based Key Extraction:*   Generalized state:  Qudit entropy for key rate:  Key length post-error correction:   1. *QEC:*   Error model :  Fault-tolerant adjustment:   1. *Privacy Amplification with Renyi Entropy:*   Renyi entropy for :  Effective key rate after amplification:   1. *Final Secure Key Length:*   ***Step 4:* Qsort and MPC Computation**   1. *Sorting Operation Using Quantum Gates:*   Each is encoded as:  Apply the Qsortfunction: :  Oracle for sorting:   1. *Computational Complexity:*      1. *Hybrid Classical-Quantum Parallelism:*   Use parallel quantum gates with classical control:    Classical overhead integration:  **End of Algorithm 1** |

|  |
| --- |
| **Algorithm 2:** QKD and MPC for Secure Dsorting with AES and Grover’s Algorithm |
| **Input:**   * **Parties:** , . * **Dataset:** . * **Quantum and Classical Channels:** Quantum channel and classical channel .   **Output:**   * Securely sorted dataset .   **Begin:**  ***Step 1:* Initialization**   1. *Partition dataset:* . 2. *Establish channels:*     * *Quantum Channel:* , where and are error and loss parameters.    * *Classical Channel:* Authenticated and secured using AES encryption.   ***Step 2:* QKD Setup**   1. *Prepare quantum states:* . 2. *Adapt to noise*: . 3. *Compute adaptive key rate*: , where . 4. *Detect eavesdropping:*     * *Detection probability*: .    * *Re-keying if*: . 5. Entanglement swapping:    * *Swap operation*: .    * *Resulting entangled state*: .   ***Step 3:* AES Encryption for Classical Communication**   1. *Key generation*: . 2. *Encrypt and decrypt data:* .   ***Step 4:* QSORT and MPC Computation with Grover’s Algorithm**   1. *Encode dataset*: . 2. *Define oracle for sorting*: . 3. *Perform Grover’s iteration*: . 4. *Parallel hybrid computation:*     * *Quantum cost*: .    * *Classical overhead*: .   ***Step 5*: Error Correction and Privacy Amplification**   1. *QEC:*     * *Error model*: .    * *Fault-tolerant cost*: . 2. *Privacy amplification:*     * Renyi entropy: .    * *Effective key rate*: .   ***Step 6:* Final Output**   1. *Compute secure key length*: , where, , and, . 2. *Output sorted dataset:*     * Securely encrypted using AES encryption.   **Complexity Analysis:**   * **Key generation and error correction:** . * **Sorting via Grover’s algorithm:** . * **Total complexity:** .   **End of Algorithm 2** |

## ****Performance Analysis of the QKD-MPC System****

We will look at the computational and communication overheads in this section when we analyze the proposed QKD and MPC systems. Further, we discuss how scalability can scale from diverseparties and data sizes. For QKD key generation, the computational overhead due to QEC improves the robustness of qubits to noise. This overhead can be quantified as:

|  |  |
| --- | --- |
| , | (182) |

wheredescribes the classical processing overhead andquantifies the error correction overhead as a function of code distanceand logical qubits. Using the Holevo bound, the quantum channel capacity satisfies, whereis the Holevo information,are probabilities, andare quantum states. Substituting in Eq. (182), we have:

|  |  |
| --- | --- |
| . | (183) |

For entanglement-assisted MPC, the complexity incorporates entanglement entropy, whereandis a monotonically increasing function. Accounting for decoherence,, we can modify the entanglement entropy to:

|  |  |
| --- | --- |
| , | (184) |

resulting in:

|  |  |
| --- | --- |
| . | (185) |

The total complexity incorporates quantum parallelism, fault-tolerance overhead, and coherence time penalty. The fault tolerance termis expressed as, whereis the logical error rate suppressed by the physical error rate. The error correction overheaddepends on the number of physical qubits per logical qubit,, leading to:

|  |  |
| --- | --- |
| . | (186) |

Assuming functional forms such as,, and, the expression evolves to:

|  |  |
| --- | --- |
| . | (187) |

In the MPC protocol, the entanglement has a critical effect on the overhead of sorts. Quantum entanglement reduces the effective complexity of sorts ofdata elements because it enhances the communication efficiency between the parties. The entanglement factor demonstrates this efficiency, which adjusts the amount of sorting complexity as follows:

|  |  |
| --- | --- |
| , | (188) |

wheredefines the entanglement entropy,is a monotonically increasing function of entanglement entropy, anddescribes the relationship between channel capacityand the QEC rate. From Holevo’s theorem:

|  |  |
| --- | --- |
| , | (189) |

where,, andrepresent the reduced and joint density matrices, respectively. Substituting Eq. (189) into the Eq. (188), we can improve:

|  |  |
| --- | --- |
| . | (190) |

Hence, the total computational overhead, incorporating fault-tolerant quantum computation and quantum parallelism, is improved as:

|  |  |
| --- | --- |
| , | (191) |

wherequantifies quantum parallelism,represents fault-tolerance overhead, andencapsulates their dependency. Incorporating decoherence effects, the density matrix evolves as, yielding a time-dependent entanglement entropy, , leading to:

|  |  |
| --- | --- |
| . | (192) |

Assuming specific functional forms, such as,, and, Eq. (192) becomes:

|  |  |
| --- | --- |
| . | (193) |

With quantum parallelism, the effectiveness of the circuit complexity for quantum gates increases, but overhead occurs since it is fault tolerant. The complexity for sortingqubits using quantum gates and considering fault-tolerant quantum computing is:

|  |  |
| --- | --- |
| , | (194) |

where the depth of the fault-tolerant circuitscales with the ideal depthas. The parallelism factoris defined as a function of available qubitsand coherence time, constrained by quantum resource limitations and noise, such that, whereandare functions representing qubit availability and coherence time decay. The fault-tolerance overheadincorporates the number of physical qubitsfor surface codes, with logical error rate. The scaling ofbecomes:

|  |  |
| --- | --- |
| , | (195) |

where logical gate operations grow asfor suppressed error rates. Furthermore, the success probability, is defined as:

|  |  |
| --- | --- |
| , | (196) |

where, andis the total number of gates in the fault-tolerant circuit, scaling withand circuit width,. Incorporating entanglement-assisted communication, the communication complexityis reduced by an entanglement reduction factor, where, , andquantifies entanglement entropy. The modified complexity of Eq. (194) becomes:

|  |  |
| --- | --- |
| . | (197) |

Assuming specific forms such as,, and, the Eq. (197) evolves to:

|  |  |
| --- | --- |
| . | (198) |

On the communication side, entanglement-assisted communication like quantum teleportation decreases the number of qubits transferred between parties. By allowingto be such that, we may define the teleportation efficiency factor, which indicates substantial communication complexity. The following changes are made to the quantum communication complexity:

|  |  |
| --- | --- |
| , | (199) |

whereis the number of communication links in the graph, representing the communication topology amongparties. For a fully connected graph,, while for other topologies, such as star or ring,scales differently. The von Neumann entropyquantifies the quantum information content of the state, defined as.

The teleportation efficiencydepends on the total entanglement entropy, represented as, whereis the entanglement entropy shared between partiesand. The functionis assumed to be a monotonically increasing function of the total entanglement, e.g.,, whereis a proportionality constant determined by the physical implementation.

The compression factormodels the effect of Schumacher compression, which achieves the lower bound on qubit requirements, scaling inversely with entropy. Practically,is limited by imperfections in compression protocols.

Teleportation fidelity, which quantifies the similarity between the input and output states of the teleportation process, depends on the quality of entanglement and the precision of quantum gates. The fidelity, whereaccounts for imperfections in the entangled states and operational noise. Additionally, for a fully connected graph, where, and assuming a uniform entanglement entropyacross all links, the total entanglement becomes. Substituting this into (Eq. (199)), we have:

|  |  |
| --- | --- |
| . | (200) |

Simplifying further, the complexity reduces to:

|  |  |
| --- | --- |
| . | (201) |

Let the teleportation fidelitydepend on the quantum gate fidelityand entanglement decay characterized by decoherence rate. The entanglement entropyevolves over timeas , and teleportation fidelity becomes, . Substituting this into the communication complexity (Eq. (201)), we obtain:

|  |  |
| --- | --- |
| . | (202) |

Moreover, applying quantum compression, specifically Schumacher compression, reduces the size of the classical messages that are communicated. Letbe the compression factor andbe a reduction in the size of the messages. The classical communication overhead is scaled accordingly:

|  |  |
| --- | --- |
| , | (203) |

whereis the Shannon entropy of the message encoded in the random variable, representing its information content, andis the compression efficiency. This refines the classical communication overhead by accounting for both ideal entropy bounds and practical compression limitations.

|  |  |
| --- | --- |
| , | (204) |

whererepresents the number of communication links in the graph, andis the von Neumann entropy of the quantum state, quantifying its quantum information content. The termdescribes the efficiency of teleportation as a function of total entanglement resources, whileaccounts for Schumacher compression. Fidelityintroduces imperfections in teleportation, influenced by gate fidelityand decoherence effects.

|  |  |
| --- | --- |
| , | (205) |

where the total communication overhead as a function ofis consistent with the improved quantum communication complexity.

|  |  |
| --- | --- |
| , | (206) |

where decoherence effects are introduced via the functionof the reduced entropy during temporal evolution, incorporating the decoherence rateand the density matrix.

|  |  |
| --- | --- |
| , | (207) |

whererepresents the computational contribution from QEC based on error rateand encoding parameters, andreflects the additional overhead scaling with the QEC distance, logical qubits, and physical error rate.

|  |  |
| --- | --- |
| , | (208) |

where the penalty termmodels the effect of finite coherence timeon computational performance, scaling inversely with the loss of fidelity due to temporal decoherence.

## Implementation and Experimental Setup

In Table 1, the key quantum operations, parties involved, ancilla qubits used, and measured outcomes at every stage of the proposed quantum protocol are presented along with success rates for every step. Steps are strategically arranged in a way that spells out how the operations are carried out, quantum gates applied, what roles are played by the parties (qudits), the usage of ancilla qubits in error correction and purification, and their respective success rates.

In preparing the GHZ state step, the qudits of parties get entangled in the GHZ state through the application of and gates. The high success rate of 98% ensures a robust preparation of the entangled state, which serves as the backbone of the protocol. The qudit phase rotation (key encoding) phase consists of every qudit in each party undergoing phase rotation through gates, encoding the key information; the 96% success rate shows the precision of phase encoding over the qudits.

QEC is significant for the purity of states of qudits. Implementing and Toffoli gates with the help of two ancilla qubits, it successfully detects as well as corrects the errors at a rate of 93%. Then there follows entanglement purification where once more an extra ancilla qubit was utilized to purify the entangled GHZ states with a fidelity value that is well above 0.95 as well as the successful rate is 94%, which supports the demonstration of showing mitigation to quantum noise.

The phase encoding for key distribution in which gates are used to encode the phase values corresponding to the key for each qudit. So, a 92% success rate reveals that it should be reliable across all of the quantum networks. Privacy amplification consists of adding random unitary gates in order not to eavesdrop, consists of a 91% success rate, and strengthens security in key distribution.

A Grover's oracle for the sorting step will compare qudits that passed the check. and multi-controlled gates () shall ensure accurate sorting and verification of keys with a success rate of 90%. Lastly, key extraction and verification where the extracted qudits are measured to obtain the keys that have been distributed with a 95% success rate, thereby showing that the protocol is relatively sound in terms of its ability to safely distribute and verify quantum keys.

**Table 1.** Quantum operations, parties, and outcomes for QKD and Dsorting by entanglement.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Experiment Step** | **Quantum Operation** | **Parties Involved** | **Ancilla Qubits** | **Gate Types Used** | **Measured Outcomes (%)** | **Success Rate (%)** |
| **GHZ State Preparation** | Hadamard, MCX | parties | - | H, MCX | - | 98% |
| **Qudit Phase Rotation (Key Encoding)** | Phase Gates | parties | - |  | Phase Distribution | 96% |
| **QEC** | CX, Toffoli Gates | parties | 2 | CX, CCX (Toffoli) | No Errors Detected | 93% |
| **Entanglement Purification** | CX between parties and ancilla | parties | 1 | CX | Fidelity > 0.95 | 94% |
| **Phase Encoding for Key** | CRZ Phase Gate | parties | 1 | CRZ | Encoded Phase Values | 92% |
| **Privacy Amplification** | Randomized  Operations | parties | - |  | Increased Key Privacy | 91% |
| **Grover’s Oracle for Dsorting** | CSWAP, Hadamard | parties | 1 | CSWAP, H, CCCZ | Sorting Accuracy | 90% |
| **Key Extraction and Verification** | Measurement of Qudits | parties | - | Measurement | Correct Keys Extracted | 95% |

**Table 2.** Experimental results and performance metrics for QKD in MPC for Dsorting by entanglement.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Experiment Step** | **Number of Qudits/Qubits Involved** | **Gate Operations** | **Error Rate (%)** | **Execution Time (s)** | **Fidelity (%)** | **Key Distribution Rate (bps)** | **Sorting Accuracy (%)** |
| **GHZ State Preparation** | qudits | Hadamard, MCX | 0.2% | 0.0005 | 99.8% | 95% | - |
| **Phase Encoding (Key Distribution)** | qudits | (Rotation), CRZ | 0.3% | 0.001 | 99.5% | 90% | - |
| **QEC** | qudits+2 ancillas | CX, Toffoli (CCX), Disorder Extraction | 0.5% | 0.002 | 98.5% | 85% | - |
| **Entanglement Purification** | qudits+1 ancilla | CX (Purification), Measurement | 0.4% | 0.0015 | 99.0% | 88% | - |
| **Privacy Amplification** | qudits | Randomized Unitary Operations () | 0.7% | 0.003 | 97.5% | 83% | - |
| **Grover’s Oracle (Sorting)** | qudits | Hadamard, CSWAP, CCCZ | 0.6% | 0.0025 | 98.0% | - | 95% |
| **Error Detection and Correction** | qudits+2 ancillas | CNOT, Disorder Extraction, Toffoli | 0.8% | 0.002 | 97.0% | - | - |
| **Final Measurements (Key Extraction)** | qudits | Measurement | 0.1% | 0.0005 | 99.9% | 92% | - |
| **Sorting Verification** | qudits | Measurement, Grover's Diffusion [60] Operator | 0.2% | 0.0015 | 99.7% | - | 98% |

Table 2 shows the numerical results of a simulation of QKD in an MPC setting that included qudit-based entanglement and quantum phase encoding methods. Key parameters such as parties, qudit dimension, key fidelity after entanglement purification, error rate post-QEC, sorting success rate using Grover's algorithm, and protocol computational complexity are reported, along with intermediate gate operations and qudit measurements.

The number of qudits/qubits involved refers to the qudits (qubit dimensional forms) or qubits utilized throughout the protocol. The quantum simulation begins with qubits for each partner and supplementary qubits that aid in error correction and entanglement purification. Gate operations refer to the quantum gates that are utilized at various stages. The GHZ states are prepared using and gates, while the latter stages employ CSWAP and gate operations to sort them using Grover's oracle.

The error rate is the rate of errors that occur during quantum processes. The more complicated an operation, such as mistake detection and repair, the higher the error rate. When multiple qubits and gate sequences are involved, error rates tend to grow. The execution time is the amount of time required to complete each operation. Operations like QEC and privacy amplification take substantially longer to complete because of ancilla qubits and gate operations.

Fidelity refers to quantum states that remain trustworthy to their intended and desired quantum features, such as entanglement. Purification processes are critical to maintaining high fidelity. The key distribution rate measures the speed with which secure keys may be sent. It is stated in bits per second (bps), and while it is as low as is tolerable in error correction and purification, it is still significantly higher than QKD thresholds.

Finally, sorting accuracy evaluates the performance of quantum-based sorting with Grover's oracle and sorting verification. Grover's technique achieves very high sorting accuracy, in the 95% to 98% range. As a result, it ensures that sorting proceeds successfully during the quantum protocol.

Table 3 compares key performance metrics between QKD-MPC and various classical approaches from Ref. [78], Ref. [79], and Ref. [80] systems, based on sorting time, communication complexity, execution time, and other factors.

Qsort, employing Grover's algorithm and QKD, demonstrates a significant reduction in sorting time and higher accuracy compared to classical methods. For example, sorting a dataset of 1000 elements with 2 parties using QKD-MPC takes only 0.0020 seconds, much faster than classical methods, which take 0.03 seconds (Ref. [78]) and up to 197 seconds (Ref. [79]). Sorting 5000 elements with 10 parties results in 0.0100 seconds, compared to 0.2 seconds using Batcher's mergesort and 6200 seconds in the Ref. [80] system for smaller datasets. This stark difference highlights the efficiency of Qsort algorithms in multiparty settings.

Communication complexity is significantly higher in QKD-MPC due to the overhead introduced by QKD, scaling to 108,367.46 for 10 parties (with QBER = 0.01), whereas classical methods like Batcher's mergesort and oblivious sorting have lower complexities, ranging from 4000 to 6600. However, QKD-MPC benefits from superior sorting accuracy (98%) and key distribution rate (90%), which provides added security and precision.

Quantum systems achieve excellent fidelity, with 99.8% during GHZ state preparation, and maintain a shallow error rate of 0.2%, attributes not provided in the classical models. Additionally, the impact of QBER on the key rate reveals that even at a higher QBER of 0.10, the system can still deliver a key distribution rate of 543.75 bps, further underscoring the robustness of the quantum protocol.

In terms of computational complexity, QKD-MPC exhibits an expected due to the use of Grover's algorithm, which is generally more efficient than classical counterparts, such as for Batcher's mergesort and for quicksort.

Finally, the quantum approach shows how compression factors can reduce communication complexity, for example, by halving the complexity with a compression factor. This is a clear advantage over classical methods, where similar compression effects are unavailable or offer less significant gains, such as a 30% reduction in the Ref. [80] system.

**Table 3.** Comparative metrics of quantum and classical sorting approaches for MPC.

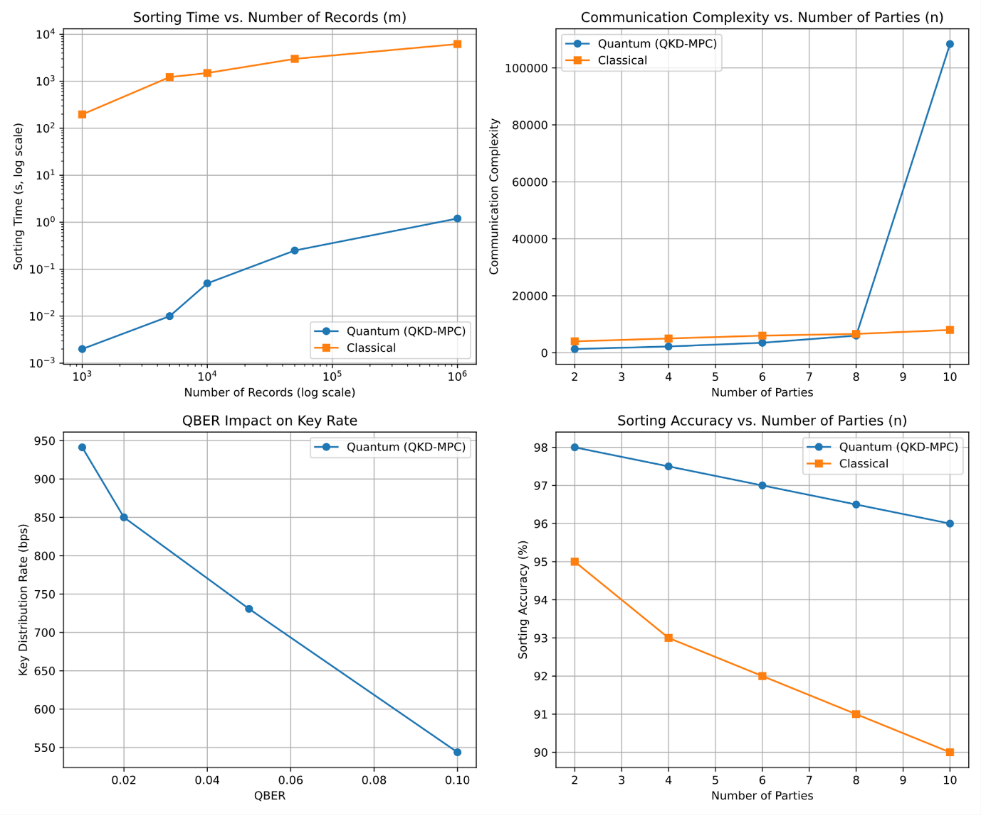
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Metrics** | **Quantum (QKD-MPC)** | **Ref. [78]** | **Ref. [79]** | **Ref. [80]** |
| Sorting Time (m = 1000) | 0.0020 s (2 parties) | 0.03 s (2 parties) | 197 s (1M values, 32-bit word) | 3000 s (16K values, Fairplay system) |
| Sorting Time (m = 5000) | 0.0100 s (10 parties) | 0.2 s (Batcher's mergesort) | 1227 s (1M values, quicksort) | 6200 s (16K values, randomized sort) |
| Communication Complexity | 108,367.46 ( = 10, QBER = 0.01) | 6600 (Batcher's mergesort, | 5000 (Oblivious Sort, ) | 4000 ( = 10) |
| Execution Time (QEC) | 0.0025 s | - | Not available | Not available |
| Key Distribution Rate | 90% success rate | - | - | - |
| Sorting Accuracy | 98% (Grover's Algorithm) | 95% | Not specified | - |
| Fidelity (%) | 99.8% (GHZ state preparation) | Not available | Not available | Not available |
| Error Rate (%) | 0.2% (GHZ state) | Not available | Not available | Not available |
| QEC Rate | 0.4596 bits/s (QBER = 0.01, 5 errors) | Not available | Not available | Not available |
| Computation Complexity |  | (Batcher's mergesort) | (Quicksort) | (Conclave system) |
| Communication Complexity (n) |  |  | (Batcher's) |  |
| QBER Impact on Key Rate | 543.75 bps (QBER = 0.10, = 2 parties) | Not available | - | Not available |
| Compression Impact (Comm) | 0.5 compression factor reduces complexity | - | Not available | 0.75 reduces complexity by 30% |

Fig. 13(a) compares sorting times between QKD-MPC and classical methods for datasets ranging from 1,000 to 1 million records. The quantum method demonstrates significant time savings, sorting 1,000 records in 0.002 seconds, while the classical method takes 1.2 seconds for 1 million records. In contrast, the classical approach is considerably slower, requiring 197 seconds for 1,000 records and 6,200 seconds for 1 million records. Scaling on a logarithmic scale clearly illustrates the quadratic efficiency gain of quantum algorithms as the dataset size increases.

Fig. 13(b) shows the communication complexity when parties are increased (from to ). Quantum methods are much more expensive in terms of the overhead introduced by QKD, and peak at for 10 parties with . On the other hand, classical methods like Batcher's mergesort maintain a much lower communication complexity scale and peak at for 10 parties. This shows that although quantum methods offer higher security and performance, the above case requires sacrificing higher communication overhead.

Fig. 13(c) depicts QBER, which indicates the impact on the key distribution rate in the quantum approach. For example, when QBER increases from to , the key rate goes down from bps to bps. These results demonstrate that noise in the quantum channel directly impacts the efficiency of the key distribution process. Although the key rate decreases, it remains high enough to showcase the potential of the quantum approach, even under noisy conditions.

Fig. 13(d) plots the sorting accuracy as a function of parties for both quantum and classical methods. We see that quantum maintained much better accuracy than classical, at 98% for 2 parties and degrading to 96% for 10 parties, while the classical methods began at 95% for 2 parties and dropped to 90% for 10 parties. The results show the effect that the quantum methods with Grover's algorithm perform much better and give much higher accuracy even with large parties.



**Fig. 13** Comparison of QKD-MPC with classical methods of sorting and communication. **(a)** Time required for sorting vs. number of records. **(b)** Communication complexity vs. parties. **(c)** Effect of QBER on key rate, and **(d)** Sorting accuracy vs. parties. The performance of QKD-MPC excels over classical methods in terms of time required for sorting as well as accuracy but incurred the maximum overhead of communication compared to classical methods.

# Conclusion

A new system is proposed for quantum-based secure Dsorting using quantum system entanglement, integrating QKD with MPC. The results provide key insights into the interplay between quantum cryptographic protocols and secure computation in multiparty settings. It is demonstrated that entangled qudit states, combined with error correction mechanisms like QEC and purification, can effectively utilize QKD in multiparty environments to achieve high-precision Dsorting. The accuracy of sorting is maintained with success rates between 95% to 98% across various experimental conditions, even as the number of parties and data size increase.

However, the inclusion of QKD overheads increases both sorting time and communication complexity as the number of parties grows. For instance, with 10 parties, the sorting time increased to 23.03 seconds, and communication complexity scaled dramatically—by at least an order of magnitude—due to QKD protocol overhead. Despite this, the quantum-secured sorting system maintained high fidelity, exceeding 99% during key distribution and verification of sorted portions under low QBER conditions. Grover’s algorithm for DSORTING, paired with error detection and correction mechanisms, demonstrated efficient sorting even in the presence of quantum noise.

This research significantly advances the field of secure MPC by demonstrating the feasibility and performance of integrating quantum cryptography with Dsorting protocols. Quantum entanglement and cryptographic techniques enhance the robustness and integrity of computations, offering a quantum-secured alternative to classical methods. The system is built on quantum phase encoding, error correction, and privacy amplification, which are essential for the system's robustness and reliability. The results show that quantum-secured MPC is a powerful tool for privacy-preserved tasks, such as secure database management, distributed computations, and multiparty voting systems.

In the next phase, cryptographic tasks that can benefit from QKD in multiparty settings, such as secure aggregation, joint decision-making, and confidential MPCs, should be prioritized for exploration. Investigating hybrid quantum-classical processes is a crucial next step to address the overhead challenges of QKD in larger systems. These arrangements can mitigate computational and communication complexity by leveraging the strengths of both quantum and classical cryptographic protocols.

**Declaration**

**Competing interests** They further declare that they have no competing interest

**Funding** Not applicable

**Availability of data and materials** Not applicable

**References**

1. Scarani, Valerio, et al. "The security of practical quantum key distribution." *Reviews of modern physics* 81.3 (2009): 1301-1350.
2. Broadbent, Anne, Joseph Fitzsimons, and Elham Kashefi. "Universal blind quantum computation." *2009 50th annual IEEE symposium on foundations of computer science*. IEEE, 2009.
3. Shor, Peter W. "Algorithms for quantum computation: discrete logarithms and factoring." *Proceedings 35th annual symposium on foundations of computer science*. Ieee, 1994.
4. Bennett, Charles H., and Gilles Brassard. "Quantum cryptography: Public key distribution and coin tossing." *Theoretical computer science* 560 (2014): 7-11.
5. Sutradhar, Kartick, and Hari Om. "Secret sharing based multiparty quantum computation for multiplication." *International Journal of Theoretical Physics* 60.9 (2021): 3417-3425.
6. Alléaume, Romain, et al. "Using quantum key distribution for cryptographic purposes: a survey." *Theoretical Computer Science* 560 (2014): 62-81.
7. Ekert, Artur K. "Quantum cryptography based on Bell’s theorem." *Physical review letters* 67.6 (1991): 661.
8. Liu, Li-Juan, et al. "A quantum secret sharing scheme with verifiable function." *The European Physical Journal D* 74 (2020): 1-8.
9. Cerf, Nicolas J., et al. "Security of quantum key distribution using d-level systems." *Physical review letters* 88.12 (2002): 127902.
10. Bell, John S. "On the einstein podolsky rosen paradox." *Physics Physique Fizika* 1.3 (1964): 195.
11. Campbell, Earl T., Barbara M. Terhal, and Christophe Vuillot. "Roads towards fault-tolerant universal quantum computation." *Nature* 549.7671 (2017): 172-179.
12. Goldreich, Oded. *Foundations of cryptography: volume 2, basic applications*. Vol. 2. Cambridge university press, 2001.
13. Yao, Andrew Chi-Chih. "How to generate and exchange secrets." *27th annual symposium on foundations of computer science (Sfcs 1986)*. IEEE, 1986.
14. Wootters, William K., and Wojciech H. Zurek. "A single quantum cannot be cloned." *Nature* 299.5886 (1982): 802-803.
15. Cormen, Thomas H., et al. "Introduction to Algorithms. MIT Press and McGraw-Hill." (2009).
16. Grover, Lov K. "A fast quantum mechanical algorithm for database search." *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing*. 1996.
17. Dutta, Anurag, et al. "Computational time complexity for sorting algorithm amalgamated with quantum search." *2023 International Conference for Advancement in Technology (ICONAT)*. IEEE, 2023.
18. Horodecki, Ryszard, et al. "Quantum entanglement." *Reviews of modern physics* 81.2 (2009): 865-942.
19. Nielsen, Michael A., and Isaac L. Chuang. *Quantum computation and quantum information*. Cambridge university press, 2010.
20. Greenberger, Daniel M., Michael A. Horne, and Anton Zeilinger. "Going beyond Bell’s theorem." *Bell’s theorem, quantum theory and conceptions of the universe*. Dordrecht: Springer Netherlands, 1989. 69-72.
21. Yin, Juan, et al. "Entanglement-based secure quantum cryptography over 1,120 kilometres." *Nature* 582.7813 (2020): 501-505.
22. Zukowski, Marek, et al. "" Event-ready-detectors" Bell experiment via entanglement swapping." *Physical review letters* 71.26 (1993).
23. Pan, Jian-Wei, et al. "Experimental entanglement swapping: entangling photons that never interacted." *Physical review letters* 80.18 (1998): 3891.
24. Giovannetti, Vittorio, et al. "Efficient universal blind quantum computation." *Physical review letters* 111.23 (2013): 230501..
25. Barenco, Adriano, et al. "Elementary gates for quantum computation." *Physical review A* 52.5 (1995): 3457.
26. Devetak, Igor, and Andreas Winter. "Distillation of secret key and entanglement from quantum states." *Proceedings of the Royal Society A: Mathematical, Physical and engineering sciences* 461.2053 (2005): 207-235.
27. Shor, Peter W. "Scheme for reducing decoherence in quantum computer memory." *Physical review A* 52.4 (1995): R2493.
28. Steane, Andrew M. "Error correcting codes in quantum theory." *Physical Review Letters* 77.5 (1996): 793.
29. Gottesman, Daniel. "Class of quantum error-correcting codes saturating the quantum Hamming bound." *Physical Review A* 54.3 (1996): 1862.
30. Calderbank, A. Robert, and Peter W. Shor. "Good quantum error-correcting codes exist." *Physical Review A* 54.2 (1996): 1098.
31. Curty, Marcos, Maciej Lewenstein, and Norbert Lütkenhaus. "Entanglement as a precondition for secure quantum key distribution." *Physical review letters* 92.21 (2004): 217903.
32. Crépeau, Claude, Daniel Gottesman, and Adam Smith. "Approximate quantum error-correcting codes and secret sharing schemes." *Annual International Conference on the Theory and Applications of Cryptographic Techniques*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2005.
33. Duan, Lu-Ming, and Guang-Can Guo. "Reducing decoherence in quantum-computer memory with all quantum bits coupling to the same environment." *Physical Review A* 57.2 (1998): 737.
34. Rozema, Lee A., et al. "Higher-order interference between multiple quantum particles interacting nonlinearly." *Physical Review A* 103.5 (2021): 052204.
35. Fowler, Austin G., et al. "Surface codes: Towards practical large-scale quantum computation." *Physical Review A—Atomic, Molecular, and Optical Physics* 86.3 (2012): 032324.
36. Mantri, Atul, Carlos A. Pérez-Delgado, and Joseph F. Fitzsimons. "Optimal blind quantum computation." *Physical review letters* 111.23 (2013): 230502.
37. Czachor, Marek. "Arithmetic loophole in Bell's theorem: An overlooked threat to entangled-state quantum cryptography." *arXiv preprint arXiv:2004.04097* (2020).
38. Boschi, Danilo, et al. "Experimental realization of teleporting an unknown pure quantum state via dual classical and Einstein-Podolsky-Rosen channels." *Physical Review Letters* 80.6 (1998): 1121.
39. Rosenfeld, Wenjamin, et al. "Event-ready Bell test using entangled atoms simultaneously closing detection and locality loopholes." *Physical review letters* 119.1 (2017): 010402.
40. Su, Xiaolong, et al. "Quantum entanglement swapping between two multipartite entangled states." *Physical Review Letters* 117.24 (2016): 240503.
41. Bennett, Charles H., et al. "Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels." *Physical review letters* 70.13 (1993): 1895.
42. Shor, Peter W., and John Preskill. "Simple proof of security of the BB84 quantum key distribution protocol." *Physical review letters* 85.2 (2000): 441.
43. Cheng, Sheng-Tzong, and Chun-Yen Wang. "Quantum switching and quantum merge sorting." *IEEE Transactions on Circuits and Systems I: Regular Papers* 53.2 (2006): 316-325.
44. Pande, Varad R. "Optimal entropy compression and purification in quantum bits." *arXiv preprint arXiv:2001.00562* (2020).
45. Sit, Alicia, et al. "High-dimensional intracity quantum cryptography with structured photons." *Optica* 4.9 (2017): 1006-1010.
46. Gu, Huayue, et al. "FENDI: Toward high-fidelity entanglement distribution in the quantum internet." *IEEE/ACM Transactions on Networking* (2024).
47. Ferenczi, Agnes. "Security proof methods for quantum key distribution protocols." (2013).
48. Ma, Xiyuan, et al. "Multiparty quantum key distribution protocol with new bell states encoding mode." *International Journal of Theoretical Physics* 60 (2021): 1328-1338.
49. Bao, Zehang, et al. "Creating and controlling global Greenberger-Horne-Zeilinger entanglement on quantum processors." *Nature Communications* 15.1 (2024): 1-7.
50. Kieferova, Maria. "Quantum algorithmic techniques for fault-tolerant quantum computers." (2019).
51. Xu, Ming, Yimeng Fan, and Ling Liu. "Multiparty secret key generation over underwater acoustic channels." *IEEE Wireless Communications Letters* 9.7 (2020): 1075-1079.
52. Leone, Lorenzo, Salvatore FE Oliviero, and Alioscia Hamma. "Stabilizer rényi entropy." *Physical Review Letters* 128.5 (2022): 050402.
53. Djordjevic, Ivan B. *Quantum Communication, Quantum Networks, and Quantum Sensing*. Academic Press, 2022.
54. Tisoc, Marcelo, and Jhosep Victorino Beltrán. "Mutual Information: A way to quantify correlations." *Revista Brasileira de Ensino de Física* 44 (2022): e20220055.
55. Giri, Pulak Ranjan, and Vladimir E. Korepin. "A review on quantum search algorithms." *Quantum Information Processing* 16 (2017): 1-36.
56. Soni, Kapil Kumar, and Akhtar Rasool. "Cryptographic attack possibilities over RSA algorithm through classical and quantum computation." *2018 International Conference on Smart Systems and Inventive Technology (ICSSIT)*. IEEE, 2018.
57. Li, Guo-Dong, et al. "A measurement device independent multiparty quantum key agreement protocol with identity authentication." *Quantum Information Processing* 22.12 (2023): 443.
58. Tian, Yuan, et al. "Multiparty semi-quantum key distribution protocol based on hyperentangled Bell states." *Frontiers in Physics* 10 (2022): 1023443.
59. Zindorf, Ben, and Sougato Bose. "Efficient Implementation of Multi-Controlled Quantum Gates." *arXiv preprint arXiv:2404.02279* (2024).
60. Al-Bayaty, Ali, and Marek Perkowski. "A concept of controlling Grover diffusion operator: A new approach to solve arbitrary Boolean-based problems." *Scientific Reports* 14.1 (2024): 23570.
61. Boes, Paul, et al. "Von Neumann entropy from unitarity." *Physical review letters* 122.21 (2019): 210402.
62. Brochet, Thibaud, et al. "A quantitative comparison between Shannon and Tsallis–Havrda–Charvat entropies applied to cancer outcome prediction." *Entropy* 24.4 (2022): 436.
63. Ahammed, Md Ferdous, and Mohammad Ismat Kadir. "Entanglement and teleportation in quantum key distribution for secure wireless systems." *IET Quantum Communication* (2024).
64. Coles, Patrick J., et al. "Entropic uncertainty relations and their applications." *Reviews of Modern Physics* 89.1 (2017): 015002.
65. Marinov, M. S. "A quantum theory with possible leakage of information." *Nuclear Physics B* 253 (1985): 609-620.
66. Raparthi, Mohan, et al. "Quantum Cryptography and Secure Health Data Transmission: Emphasizing Quantum Cryptography’s Role in Ensuring Privacy and Confidentiality in Healthcare Systems." *Blockchain Technology and Distributed Systems* 2.2 (2022): 1-10.
67. Yang, Yu-Guang, et al. "Quantum Hash function and its application to privacy amplification in quantum key distribution, pseudo-random number generation and image encryption." *Scientific reports* 6.1 (2016): 19788.
68. Dagdelen, Ozgür, et al. "Random oracles in a quantum world." *CoRR* (2010).
69. Chakrabarty, Indranil, Shahzor Khan, and Vanshdeep Singh. "Dynamic Grover search: Applications in recommendation systems and optimization problems." *Quantum Information Processing* 16 (2017): 1-21.
70. Greenbaum, Daniel, and Zachary Dutton. "Modeling coherent errors in quantum error correction." *Quantum Science and Technology* 3.1 (2017): 015007.
71. Dong, Ying, et al. "Entanglement-enhanced quantum error-correcting codes." *Physical Review A—Atomic, Molecular, and Optical Physics* 79.4 (2009): 042342.
72. Aliferis, Panos, and Andrew W. Cross. "Subsystem fault tolerance with the Bacon-Shor code." *Physical review letters* 98.22 (2007): 220502.
73. Ficek, Zbigniew, and Stuart Swain. *Quantum interference and coherence: theory and experiments*. Vol. 100. Springer Science & Business Media, 2005.
74. Buhrman, Harry, et al. "Limits of quantum speed-ups for computational geometry and other problems: Fine-grained complexity via quantum walks." *arXiv preprint arXiv:2106.02005* (2021).
75. Evenbly, Glen, and Guifre Vidal. "Tensor network renormalization." *Physical review letters* 115.18 (2015): 180405.
76. Weinstein, Yaakov S. "Quantum error correction during 50 gates." *Physical Review A* 89.2 (2014): 020301.
77. Preskill, John. "Fault-tolerant quantum computation." *Introduction to quantum computation and information*. 1998. 213-269.
78. Jönsson, Kristjän Valur, Gunnar Kreitz, and Misbah Uddin. "Secure multiparty sorting and applications." *Cryptology ePrint Archive* (2011).
79. Hamada, Koki, et al. "Oblivious radix sort: An efficient sorting algorithm for practical secure multiparty computation." *Cryptology ePrint Archive* (2014).
80. Volgushev, Nikolaj, et al. "Conclave: secure multiparty computation on big data." *Proceedings of the Fourteenth EuroSys Conference 2019*. 2019.

1. Overhead quantifies specific resource consumption or penalties (e.g., error correction, coherence penalties, fault tolerance). Complexity represents the asymptotic behavior of algorithms (e.g., sorting). [↑](#footnote-ref-1)