Comput Syst Sci & Eng (2020) 6: 457–465

International Journal of
Computer Systems
Science & Engineering

Multiparty Quantum Key Agreement With Strong Fairness Property

Vankamamidi S. Naresh[1,*] **and Sivaranjani Reddi**[2]

[1] *Department of Computer Science and Engineering, Sri Vasavi Engineering College, Tadepalligudeam-534101, Andhra Pradesh, India*
[2] *Department of Computer Science and Engineering, Anil Neerukonda Institute of Technology & Science, Visakhapatnam 530003, Andhra Pradesh, India*

Multiparty Key Agreement (MKA) is the backbone for secure multiparty communication. Although numerous efficient MKA-cryptosystems are available in the classical field, their security relies on the assumption that some computational issues are infeasible. To overcome this dependency, a new area, quantum cryptography, evolves to support key agreement among two or more participants securely. In this paper, first, we present a two-part quantum key agreement with Strong Fairness Property (SFP) and extends it to a Multiparty Quantum Key Agreement (MQKA) protocol. In the first round of proposed MQKA, a participant will act as a group controller (GC) and establishes two-party groups with each of the residual participants and agreed on a quantum two-party-style shared key per each of the two-party. In the second round, the GC computes public keys for each of the respective parties by combining these two-party keys using XOR-operation, excluding that party's two-party key. Next, the GC sends separate public keys to the individual participants. After receiving the respective public-key, each of the respective participants computes the multiparty key by joining their public-key with their two-party key using XOR. Finally, GC computes the multiparty key, as the GC knows all the two-party keys, it combines them with XOR and acts as a usual group participant. The proposed protocol has compared with other renowned MQKA protocols in terms of four standards parameters, namely transmission number (TN), qubit measurement number (QM), qubit for channel checking (QCC), and the qubit efficiency (QE) and acceptable results achieved. The security of the proposed MQKA relies on the absolute security of a two-part quantum key agreement with Strong Fairness Property (SFP). Moreover, it is secure against both internal and external attacks.

Keywords: Quantum multiparty key; strong fairness property; quantum summation; key manipulation attacks; quantum information; quantum teleportation.

1. INTRODUCTION

With the fast development in present day correspondence, profoundly secure multiparty correspondence is turning into a significant research area in a choice of group ware applications, such as teleconferencing, real-time information services, telemedicine, distributive interactive simulations, and grid computing. An insightful research was carried out in this area through conventional cryptography by various researchers. However the security of conventional cryptography often relies on unproven computational assumptions. So in this paper we motivated towards "multiparty quantum key agreement with SFP" that promises unconditional security based on the fundamental laws of quantum mechanics.

Quantum key Agreement (QKA) begins with the BB84 [17] protocol in 1984 by Bennett et al. The BB84 protocol used to generates a two-party shared key using single qubits via a quantum channel. The QKA's security relies on one of the two non-orthogonal or complementary randomly measured qubits. Further, the quantum mechanics principles shield the QKA from eavesdropper who tries to interpret the information. Likewise, any guaranteed prediction of complementary evidence on the same qubit turns out to be random. Besides, the characteristic of superposition and entanglement permits researchers to establish the quantum algorithm (QA) breaking the prominent RSA using quantum parallel computing. Conventional cryptographic algorithms can be easily intimidated by a robust quantum algorithm. Further, it permits researches to establish quantum algorithms based on physical laws in opposition to traditional cryptographic computations to protect from attacks of quantum computers. The QKD [18–21], Quantum Secure Direct Communication (QSDC) [22–25], and Quantum Secret Sharing (QSS) [26–29] are exciting applications like quantum dense teleportation and coding.

*vsnaresh111@gmail.com.

Ekert proposed an ERP relied upon the scheme in 1991 as a first QKD named E91 [33]. In the subsequent years, C. H. Bennett made an extension and developed an algorithm [34] that uses two-qubit states and nonsymmetrical bases. Next, the research focus was on key usage, key rate, and space storage in two-way QKD in 2004. Subsequently, Nguyen [35] presented a scheme that allows two agents to exchange the message securely in one communication, named QSDC scheme or two-way quantum dialogue. In 2005 Gao et al. [36] extended the scheme to decrypt message safely without prior knowledge regarding the message. Further multiparty QSDC (MQSDC) scheme was invented by Jin et al. [37] that allows the concurrent exchange of messages securely. In the Contemporary period, Man and Xia designed a two-way controlled QSDC (CBQSDC) scheme based on the standard features of CQSDC and BQSDC.

Moreover, Zhang et al., [38], Deng et al., [39], Hwang et al., [40], and Chou et al. [41] have developed proficient Multiparty-QSS (MQSS) schemes in the duration of 2005 to 2012. Afterward, Jia et al., [42]; Hsu et al., [43]; Liao et al., [44]; and Liu et al. have launched a dynamic MQSDC (DMQSDC) schemes from 2012 to 2016. Various QKA schemes [7, 10, 11, 12, 13, 14, 15, 16] were developed by different authors, which are extensively utilizing in various contemporary applications. Even though the growth of MQKA is the noteworthy subtopic in QKD, in that, a participant picks a key and distributes it to the remaining parties, on the other hand, in QKA, more number of participants will contribute in deriving the QMPK. The MQKA intends to gather the shares from some or all participants to produce a QMPK.

The thought of MQKA was foremost developed in 2012 by Shi et al. [47], the prime MCQA scheme based on Bell states and Bell estimation. Next, Liu et al. [3] pointed out the shortcoming in this scheme and then presented another MCQA Pre lied on single particles. Afterward, many researchers developed MQKA schemes. In 2013, Sun et al. improved the performance of Liu et al. 's protocol and established an MCQAP. [30] in traveling mode. Further, this scheme has been proven to be unfair [31]. In 2014, Xu et al. [32] developed a suitable mode MCQA scheme based on GHZ states. At the same time, Sun et al. ([4], [5], [6])., developed two traveling modes MQKA schemes based on six-qubit states and cluster states separately. Meanwhile, these traveling mode MCQAPs ([4], [5], [6]) are insecure against collusion attack. In 2016, Huang et al. initiate another traveling mode MCQAP using unitary tasks and single photons [9]. Next, Cao et al. exhibited a traveling mode MCQAP based on quantum search algorithms [2].

MQKA schemes to accomplish the key production setting and the extension of two-party QKA to MQKA rely on the unicast for information exchange. In 2016, Zeng et al. developed a capable MCQAP based on MQSDC using broadcast transmission; with this, all agents can exchange their secret message, which leads to better efficiency.

To assess the following security aspects, MQKAs first, we present the following security definitions based on ISO/IEC DIS 11770-3 [50].

Security property: An external eavesdropper can't get any handy information on the established shared secret devoid of being tracked, and the protocol ought to guarantee the concerned members to share the same key.

Weak fairness property: Every member contributes her/ his share to influence the established shared secret.

Strong fairness property: Every member doesn't have an advantage of a single bit over the others to agree on the established shared secret, i.e., none of the participants can alter even one bit of the established shred secret.

After analyzing the security aspects of MQKs presented in the literature, it was evident that these key agreements don't satisfy the two essential security requirements: i) No member should be able to derive the final key, which is to be shared among participants. ii) Any changes in the key shared will be recognized by the other patrician(s).

We address the above security issues by incorporating the above security features. We first propose a two-party QKA with SFP. Next, it was extended to MQKAP, which can defend both inner and outer attacks. The proposed technique relies on the thought of extending two-party QKA with SFP to MQKAP.

The remainder of this work is structured as follows. Section two presents the background two-party QKA protocol with single photons in detail. Section three offers the MQKAP with SFP. Afterward, in section four, the security analysis of MQKAP with SFP is investigated. In section five, the results and discussion are presented. Finally, section six the comparative analysis with other existing methods. At last, we concluded the paper along with future work.

2. BACKGROUND

Secure key agreements occupy a critical role in cryptography, which can handle encrypting and decrypting communication. Before entering into QKA for the background of quantum concepts, one can refer to a quantum basic two-party protocol [17, 51].

2.1 Quantum Two-Party Diffie-Hellman Key Generation Algorithm

First as a background protocol for the proposed work first we present Overview of Quantum Two-Party DH-Key Generation Protocol in Figure 1.

2.2 Quantum Two-Party DH-key Generation Protocol

The Figure 2 shows comprehensive study of quantum two-party DH k-bit ($\beta = \{\beta_1, \beta_2, \beta_3, \ldots, \beta_k, k > 1\}$) key agreement.

Firstly, both participants engaged in communication openly agreed on k bases, also the m value (number of qubits used in key agreement). Both members individually choose m random bases $\beta_1^a, \beta_2^a, \beta_3^a, \ldots, \beta_m^a, \beta_i^a \epsilon \beta$ and $\beta_1^b, \beta_2^b, \ldots, \beta_m^b, \beta_i^b \in \beta$, also m random bits $a_1, a_2, a_3, \ldots, a_m$ and $b_1, b_2, b_3, \ldots, b_m$ then computes U_i^a to $|0\rangle$, at last, send, to other the member.

On reception keys from other members, the key agreement method will be started by announcing openly regarding the basis utilized, and the key bit will be accepted in the final shared key when the predicted key bit is matched with the bases used, otherwise discarded. This operation will be continued until

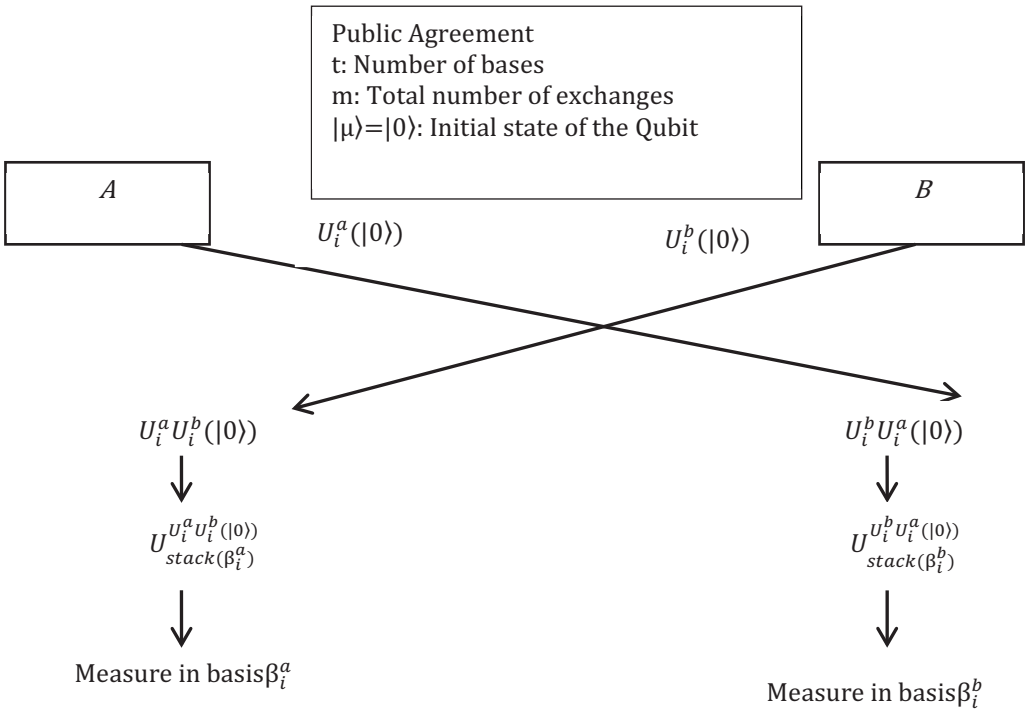


Figure 1 Overview of Quantum Two-Party DH-Key Generation Protocol.

Phase 1: Initialization:

1. *A* and *B* openly agreed on "*k*" bases $\beta=\{\beta_1,\beta_2,\beta_3,---,\beta_k\ ,\ k>1\}$
2. Let the length of the key to be exchanged be *"l"=m-d* where *"m"* be the amount of q bits to be swap over and *"d"* be the amount of *q* bits leftover during the revealing of Eve's presence
3. Besides, both parties agreed on early on state pf qubit $|\mu\rangle=|0\rangle$ that will be altered and exchanged

A	***B***
1. *A* randomly picks *"m"* bases $\beta_1^a,\beta_2^a,---,\beta_m^a,\ \beta_i^a \in \beta$ 2. A generates *m* arbitrary and uniform bit seq: $a_1,a_2,a_3,---,a_m$ 3. *A* encodes a_i in base β_i^a by applying U_i^a to $\|0\rangle$, where U_i^a=R(θ_{a_i}) and sends to Bob.	1. *A* randomly picks *"m"* bases $\beta_1^b,\beta_2^b,---,\beta_m^b,\beta_i^b \in \beta$ 2. A generates *m* arbitrary and uniform bit seq: $b_1,b_2,b_3,---,b_m$ 3. *A* encodes b_i in base β_i^b by applying U_i^b to $\|0\rangle$, where U_i^b=R(θ_{b_i}) and sends to Alice.

Phase 2: Key agreement

Let $k=\{k_1,k_2,k_3,---,k_m\}$ and $k^1=\{k_1^1,k_2^1,---,k_m^1\}$ be arbitrary seq of bits attained by *A* and *B* respectively and

i. *A* and *B* publicize the bases to each other

ii. For each *i* such that $B_i^a \neq B_i^b$ discard the values k_i and k_i^1 from *k* and k^1

iii. *A* and *B* picks *k* bits from resultant set of bits, treated as the key and will be used in forthcoming communication.

Figure 2 Complete Analysis of Quantum Two-Party DH.

processing all the "*m*" bits. The bits that satisfy the resemblance check will be the final shared key used for decryption and encryption.

3. THE PROPOSED PROTOCOLS

In this section, first, propose a two-party QKA with strong fairness property. Next, it was extended to MQKAP with strong fairness property, which can defend both inner and outer attacks.

3.1 Two-Party Quantum key agreement Protocol With SFP.

This protocol aims to achieve strong fairness, as presented in Figure 3. To achieve this, the two-party key agreement technique must satisfy the following requirements:

1. No participant should be able to derive the final key, which is to be shared between the two participant(s).
2. Any changes in the key shared will be recognized by the other patrician(s).

Based on the targeted requirements, the proposed protocol is divided into three phases as follows (shown in figure)

1. Particle Exchange: In this stage, the participants send or receive the sequence of particles. It is required that, every participant involved in the key agreement phase has to complete the transmission of particles to other participants.
2. Public Discussion Stage: This phase tries to make sure that the photons passed through this channel are Attack free from the outside eavesdropping attacks.
3. Key Negotiation Stage: All the participants help with one another to derive the final secret key. Note that, only the participants involved in the key agreement phase can be able to obtain the common shared key.

Based on the above three-phase model, initially, a two-party key agreement is designed, then extended to a multiparty key agreement. Suppose A and B are the two parties who would like to negotiate a shared secret key. Both the participants A and B agree on the following encoding rules: a binary value "0" is encoded as one of the two polarization states {vertical or horizontal} and a value "1" is encoded as {45-degrees or 135-degrees}, and vice versa.

Public Exchange:

Step 1: A and B separately chooses an N-bit private key named as K_A and K_B.

Step 2: A generates the sequence of particles S_A from K_A based on the pre-agreed rules, respectively. Then, she randomly reorders the S_A particles denoted as S'. Note that A only knows the original order of sequence. In addition to reordering, A prepares a sufficient number of decoy particles D_a and introduced into (S'_A) denoted as S'^*_A.

Similarly, B follows the same procedure in parallel and calculates S_B from K_B, then (S'_B) and finally S'^*_B

At the end of this phase, A transfers S'^*_A to B, B also transfers S'^*_B onto A in parallel.

Public Discussion Stage:

Step 3: A and B acknowledge each other through the secure channel immediately after receiving the sequences. Then, both of the participants start publishing the positions (Pos of $D_{A,B}$) and measurement bases (Bases of A, B) of the decoy particles. The receiver measures the decoy particles and returns them to the sender subsequently. Now, A and B check, whether the received measurement results are matched to the initial states they prepared. The protocol will be aborted when the error rate is higher than the threshold pre-defined. Otherwise, A and B can confirm that the channel is the eavesdropping attack free. Then, A extracts the S'_B form S'^*_B by discording the decoy particles (D_B). similarly, B does the same operations to extract S'_A from S'^*_A.

Key Agreement:

Step 4: A broadcasts her bases of measurement and ordering of the particles (Bases, $Order_A$) to B. similarly, B broadcasts his bases of measurements and ordering of the particles (Bases, $Order_B$)to A.

Step 5: A applies the reverse reorder operation on the S'_B to retrieve S_B. parallelly B applies the reverse reorder operation on the S'_A to retrieve S_A.

Step 6: A and B discard all events where they use different bases for a signal.

Step 7: A and B individually convert the polarization of all the remaining data (S''_A and S''_B) into the binary string termed as raw key denoted as (K''_A and K''_B). They can perform the length equalization to equate the length of the individual participant key contribution in order to perform the XOR operation to generate the $K = K''_A \bigoplus K''_B$.

3.2 Multiparty Quantum Key Agreement Protocol With Strong Fairness (MQKA)

This section describes the procedure to achieve the strong fairness in a multiparty group by extending the mechanism described in the two-party key agreement technique. Let us assume a group with n members named as $M_1, M_2, M_3, \ldots, M_n$. Based on the targeted requirements, all the participants in the group agree on the following encoding rules: a binary value "0" is encoded as one of the two polarization states {vertical or horizontal} and a value "1" is encoded as {45-degrees or 135-degrees}, and vice versa.

Step 1: Let M_1 become the Group Controller (GC) and then from the two-party with the remaining group members and generate the common two-party key agreement(TKA)

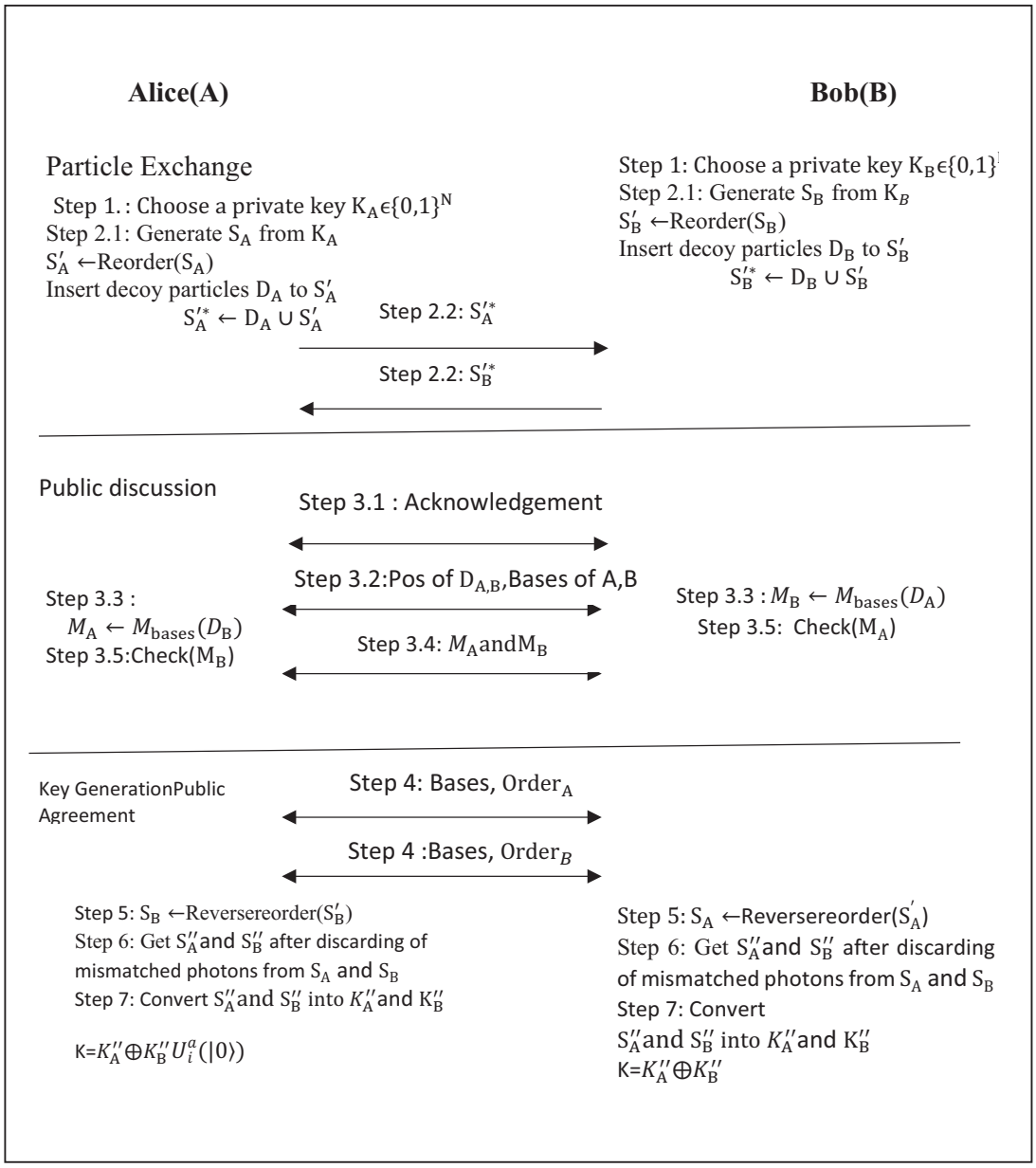


Figure 3 Two-Party Quantum Key Agreement Protocol with SFP.

between GC and the i^{th} group member $M_i, 2 \leq i \leq n$, which was discussed in section 3.1, is termed as follows:

$$TKA_{M_1,M_i} \rightarrow k_{1,i}, \quad \text{for } 2 \leq i \leq n$$

Step 2: After completion of TKA between GC and the i^{th} group member M_i, $2 \leq i \leq n$, GC will take the responsibility to derive the Partial Group Key (PGK) for each group member M_i, $2 \leq i \leq n$ termed as PGK_i, is calculated simply by applying XOR operation on the two-party keys by excluding the i^{th} member two-party key. The partial group key derived by the GC is

$$PGK_{i,} = \oplus_{j=2,i\neq j}^{n} k_{1,j}, \text{ for } 2 \leq i \leq n$$

Then send it securely to the corresponding M_i, $2 \leq i \leq n$ through the encrypted link established between GC and each of the members accordingly.

$$M_1 \xrightarrow{E_{k_{1,j}}\left[\oplus_{i=2,i\neq j}^{n} k_{1,i}\right]} M_j, \text{ for } 2 \leq j \leq n$$

Step 3: After receiving the message from M_i each group member $2 \leq i \leq n$, computes the final multiparty group key MGK_i as follows.

$$MGK_i = PGK_i \oplus k_{1,i} = \oplus_{i=2}^{n} k_{1,i}, \text{ for } 2 \leq i \leq n$$

Step 4: Finally, the GC also computes the final Multiparty Group Key (MGK_i) by computing XOR of the $k_{i,1}$ for $2 \leq i \leq n$.

4. SECURITY AND FAIRNESS ANALYSES

Here, we show that the proposed MQKA is secure against both the outsider eavesdropping attack and insider attack. Besides, we discuss how the proposed scheme satisfies the requirements of the strong fairness property.

4.1 Security of two-Party QKA Against Outsider Attack

In this part, we use several well-known attacks (Intercept, resend, and correlation-elicitation Attack) as examples to show that the proposed Two-Party QKA is secure against the outsider eavesdropping attack. Moreover, we prove that the proposed protocol is free from information leakage.

4.1.1 Intercept and Resend Attack

Let Eve (E) be an eavesdropper, an outsider, who is having the excellent quantum ability and be determined to get hold of the two-party secret key between Alice (A) and Bob (B). The E has to obtain private keys of A and B by Intercepting the quantum bit sequence sent by A to B in Step 2 and measures the sequences to get the private keys KA, KB.

Next, E transmits the fake sequence of quantum bits that have identical values as E's measurement outcome against the expectation of passing the eavesdropping check of the Public Discussion Stage. But E doesn't have an idea regarding the positions of the decoy bits and the agreed measurement bases. Every decoy bit is in one of the four states of polarization $\{|1\rangle, |0\rangle, |+\rangle, |-\rangle\}$, so that the probability that a member can obtain the right measurement outcome is $\frac{3}{4}$ even if E, by chance, measures it (in the X-basis or Z-basis). Hence, E will pass the eavesdropping check in the public discussion stage with a considerable probability in Step 3. Moreover, if there are "l" decoy particles suffering from $E's$ Attack, the likelihood that E can pass the eavesdropping check has become $\left(\frac{3}{4}\right)^l$ Hence E will be detected with a probability $\left(\frac{3}{4}\right)^l \to 1$ as $l \to \infty$.

4.1.2 Correlation-Elicitation Attack

In Correlation-Elicitation (CE) attack, the eavesdropper E may try to Intercept S'^*_A and S'^*_B as the controlled photons and subsequently prepares some auxiliary photons as the target photons, to obtain the useful information of A and B's private key. For example, E entangles her auxiliary photons with S'^*_A performing the controlled-NOT (CNOT) operation on every two photons, i.e., use one photon of S'^*_A to be the control bit and use a qubit in the state of $|0\rangle$, to be the target bit. If the control bit is in Z-basis, we cannot detect this Attack. Because in this case, the control bit can't be changed by the CNOT operation. And if the control bit is in Xbasis, we have the probability $\frac{1}{2}$ to detect the eavesdropping. Because in this case, the control bit has been entangled with the target bit. There is the probability $\frac{1}{2}$ before and the likelihood of $\frac{1}{2}$ to get the same measurement result of the control bit as to get a different measurement result. Overall, for one decoy photon, the detection rate is $\frac{1}{4}$. Hence E will be detected with a probability $\left(\frac{3}{4}\right)^l \to 1 \quad as \quad l \to \infty$.

4.1.3 Information Leakage Analysis

The safety of the shared key is crucial for the members, and a kind of passive Attack called information leakage that enables E to dig out the shared secret from the measurement results. Now, we show that the proposed QKA scheme can avoid the information leakage setback. In the QKA protocol, if E desires to eavesdrop in whichever helpful information, she/he ought to capture the S'^*_A and S'^*_B in Step 2. Similar to the study of Intercept and Resend Attack, for one bit, the probability for E to attain the accurate measurement outcome is $\frac{3}{4}$. Consequently, the measurement outcome of one qubit holds $1 - \sum P_i \log_2 P_i = 1 - \frac{3}{4}\log_2\frac{3}{4} - \frac{1}{4}\log_2\frac{1}{4} \approx 0.1887$ bit of information. So that given the measurement outcomes, E is able to get hold of around 18.87% of A and $B's$ private key. However, the analysis of Intercept and Resend Attack shows that this Attack can be detected in Step 3. Furthermore, in step 7, privacy intensification can guarantee no information leakage in the proposed protocol. For example, if we assume the privacy intensification remains 80% of the raw key K' to be the final shared secret key K, i.e., the condensed part is 20%, which greater than 18.87%. Consequently, the proposed QKA protocol is free from information leakage.

Hence the two-party QKA is secured from External Eavesdropping.

4.2 Security MQKA Protocol

4.2.1 Security MQKA Protocol From External Eavesdropping

Each of the two-party shared key generated using Two-Party Quantum Key agreement Protocol with SFP of section 3.1 in the step 1 of MQKA is secured from External Eavesdropping, as discussed in subsection 4.1. The partial group keys computed by the GC in step two of MQKA is also secured as it is obtained by XORed the secured shared keys generated in step 1. Further, the GC sends these partial group keys to respective group members securely through the established encrypted link between them. After receiving respective members decrypting their partial key component and computes the group key securely by XORing with their shared key in MQKA. Since the group key $\bigoplus_i^n = 2_{1,i}^k$ is indistinguishable from random numbers in polynomial time, and thus secured.

4.2.2 Security MQKA Protocol From Internal Eavesdropping

In fact, inside members of the group have a greater capacity to attack than the outsiders. The untrustworthy nature of inner members, who could get the advantage from replacing the sequence of messages with the fascinated sequence, in turn, to stay away from these, commence an internal attack in opposition to the group through his acquired the assets. As the proposed quantum group key agreement is contributory in nature and provided, the GC is trustworthy, the internal members of the group can't influence the group key. Thus, the proposed protocol is protected from the eavesdropping attack of internal members.

4.3 Strong Fairness

The design of the proposed two-party QKA in Section 3.1 presents how to accomplish the SFP in a two-party QKA. With the proposed method, members can't obtain any helpful information (other participants' private keys) to get the final

Table 1 Comparative Analysis

MQKA protocol	TN	QMN	QCC	QE	No of message states
[3]	$2n(n-1)$	$2n(n-1)$	$60n(n-1)$	$\frac{1}{n(n-1)}$	$N\ n(n-1)$
[9]	$2n^2$	$2n$	$60n^2$	$\frac{1}{2n^2}$	nN
[49]	$2n(n-1)$	$2n(n-1)$	$60n(n-1)$	$\frac{1}{2n^2-2n}$	$Nn(n-1)$
[50]	$4(n-1)$	$2n$	$120(n-1)$	$\frac{1}{3(n)}$	0
proposed	$2(n-1)$	$2(n-1)$	$60(n-1)$	$\frac{1}{3(n-1)}$	0

Where N is the key length, n is no of participants in the group

shared secret key till the public discussion phase is completed. Therefore, as per the proposed solution, if a malicious member tries to abort the protocol to influence the final group key intentionally, then with a greater probability, he/she would be detected by the other participant, so SFP is achieved in two-party QKA. Hence strong fairness is preserved in MQKA as it is based on two-party QKA.

5. RESULTS AND DISCUSSION

In this section, the performance efficiency of the proposed technique is analyzed and compared with the efficiency with three current MQKA techniques, namely LGHW protocol [3], HSX protocol [9], WSH protocols [49] and Kun-Fei Yu [50] protocols. We have used four standards parameters for comparison, namely transmission number (TN), qubit measurement number (QM), qubit for channel checking (QCC), and the qubit efficiency (QE).

1. TN: Every qubit is counted up as the number of transmissions from every member, except for qubits for channel checking. Here, the transmission number is nothing but the number of qubits communicated from all the participants in the group.

2. QMN: This discusses the number of qubits measurement. In general, different quantum states are utilized in QKA, like qubit, GHZ states, Bell states, four and six-qubit states. The QKA schemes can finish the agreement procedure after the measurement. The cost is increased with an increase in the number of qubit s. Suppose that the similar length key is approved in every MQKA protocol, and the count of qubit measurement will be one. As it has to run Bell state measurements in every transmission, it takes a large number of qubits. They must set up several single qubits. The proposed procedure necessitates a smaller amount of qubits as the proposed scheme measures qubits merely in the last transmission.

3. QCC: The number of qubits required for checking the channel should be conferred with the sequence transmission. These sequences are embedded into the qubits for channel checking. For example, a sequence is composed of 300 qubits, and there are approximately 30 qubits for channel checking in a sequence. so, the probability of an eavesdropper being identified is around $1-\left(\frac{3}{4}\right)^{30} \approx 0.99$. Hene, without the loss of fairness, each protocol aggression $270n$ bit key, where n is the number of participants in the group.

4. QE: The qubit efficiency (QE) is defined as the ratio of the length of the final group key(c) shared to the sum of the qubits required for encoding and eavesdropping(q) and the number of bits needed for the decoding(b). Therefore, $QE = \frac{c}{q+b}$.

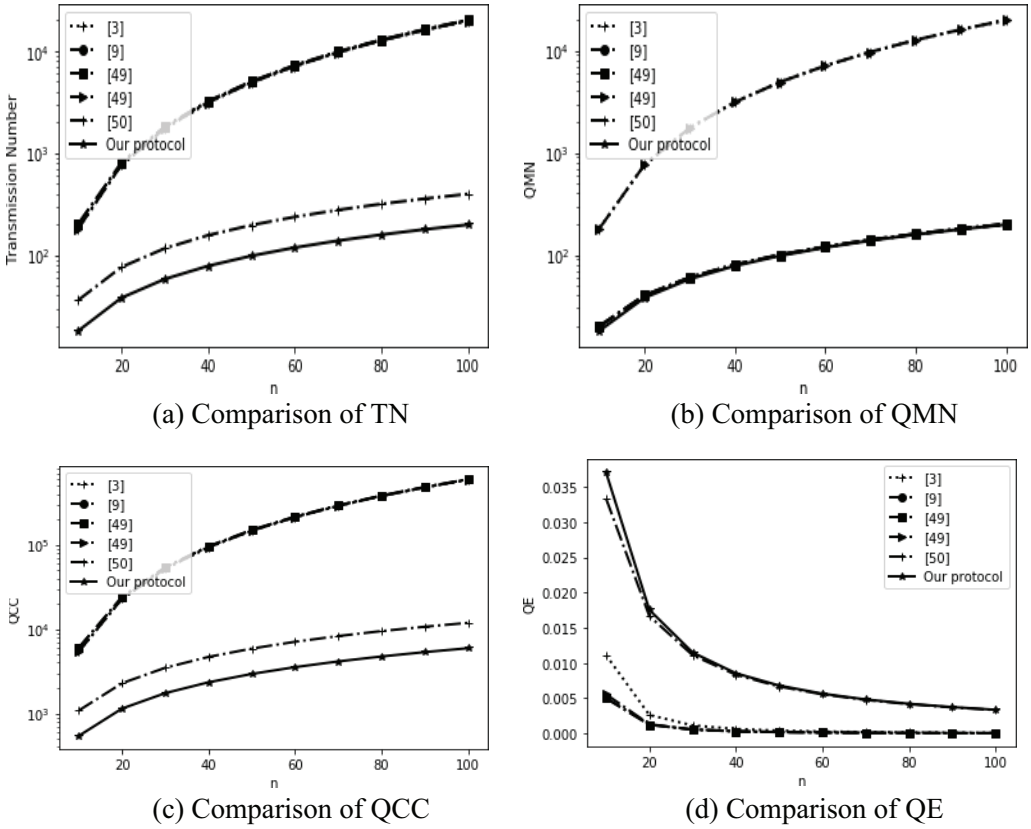
In the proposed two-party QKA protocol, to share N bit key, N single bit photons were used, and D decoy qubits are required in every key agreement process, and two rounds of transfer are involved. Totally $2(N+D)$ qubits should be necessary. The member A transfers $(N+D)$ bits to the member B to decode the partial shared key. Then the $QE = \frac{N}{2(N+D)+2N}$. Similarly, for multiparty QKA protocol, to share n bit group key N single photons along with D decoy qubits are required in every transaction, and as there are n members, needs $n-1$ rounds of transmission are involved. In total, $(n-1)(N+D)$ qubits should be required. So, the $QE = \frac{N}{(n-1)(N+D)+(n-1)N} = \frac{1}{3(n-1)}$, when $N = D$. Table 1 shows the comparative analysis of the proposed technique with other existing methods. From Table 1, we can observe that the proposed technique performance is more than other techniques. Figure 4 [(a)–(d)] shows the detailed graphical comparative analysis of the proposed protocol with other existing protocols.

Where N is the key length, n is no of participants in the group

6. CONCLUSION AND FUTURE WORK

In this paper first, we proposed a two-part quantum key agreement with Strong Fairness Property (SFP) and extended it to a Multiparty Quantum Key Agreement (MQKA) protocol. We proved that the proposed MQKA is capable of resisting the eavesdropping attacking from external participants as well as internal. We showed that the proposed protocol is secured against well-known attacks such as Intercept, resend, and correlation-elicitation Attack. The security of the proposed solution is based on the absolute security of the two-party QKA with SFP. From the results section, the performance of the proposed technique is optimal when compared to other approaches in terms of four standards parameters, namely transmission number (TN), qubit measurement number (QM), qubit for channel checking(QCC), and the qubit efficiency (QE).

As part of future work, one can add dynamic cases such as updating the quantum group key when a new member joins/leaves the group. Further, one may establish a formal security model for this dynamic quantum group key agreement.



(a) Comparison of TN (b) Comparison of QMN

(c) Comparison of QCC (d) Comparison of QE

Figure 4 comparative analysis of proposed with other techniques.

DECLARATIONS

Acknowledgments

I would like to dedicate this work to my sweetest Father, V. Bala Surya Narayana. Further, I would like to thank my family members and Management of Sri Vasavi Engineering College, Tadepalligudem, who supported and encouraged me in the successful completion of this work. Finally, I am very much grateful to the reviewers and Journal Authorities for their valuable comments in improving the paper.

Authors' contributions

The first author conceived the overall idea for the article and contributed significantly towards identifying solutions to collaborative communication applications by proposing quantum group key agreement. The second author played a vital role in executing the proposed MQKA. Both the authors worked on results and comparative analysis and approved the final manuscript.

Funding

Presently not in receipt of any funding for this research work.

Data availability statement for the data used in this manuscript

Data will be provided based on an appeal to the corresponding author.

Competing interests

The authors declare that they have no competing interests.

REFERENCES

1. Huang, W., Su, Q., Liu, B., He, Y. H., Fan, F., & Xu, B. J. (2017). "Efficient multiparty quantum key agreement with collective detection" Sci. Rep. vol. 7 no. 1 2017. 15264. doi:10.1038/s41598-017-15227-6.
2. Cao, H., & Ma, W. (2017). Multiparty Quantum Key Agreement Based on Quantum Search Algorithm. Scientific reports, 7, 45046. doi:10.1038/srep45046
3. Liu, B., Gao, F. et al. Multiparty quantum key agreement with single particles. Quantum Inf Process 12, 3411–3420 (2013).
4. Sun, Z., Zhang, C., Wang, B., Li, Q. & Long, D. Improvements on multiparty quantum key agreement with single particles. Quantum Inf. Process. 12, 3411–3420 (2013).
5. Sun, Z., Zhang, C., Wang, B., Li, Q. & Long, D "Multiparty quantum key agreement by an entangled six-qubit state" Int. J. Theor. Phys. vol. 55 no. 3 pp. 1920–1929 (2016).
6. Sun, Z., Yu, J. & Wang, P. Efficient multiparty quantum key agreement by cluster states. Quantum Inf Process 15, 373–384 (2016).
7. Liu, W.J., Chen, Z.Y., Ji, S., Wang, H.B., Zhang, J.: Multiparty semi-quantum key agreement with delegating quantum computation. Int. J. Theor. Phys. 56, 3164 (2017).
8. Wang, P., Sun, Z. & Sun, X. "Multiparty quantum key agreement protocol secure against collusion attacks". Quantum Inf. Process. 16, 170 (2017).
9. Huang, W., Su, Q., Liu, B., He, Y. H., Fan, F., & Xu, B. J "Improved multiparty quantum key agreement in travelling mode." SCIENCE CHINA Physics, Mechanics & Astronomy 59, 120311 (2016)
10. Cai, B.B., Guo, G.D., Lin, S., Zuo, HJ, Yu, CH: " Multipartite quantum key agreement over collective noise channels." IEEE Photon. J. vol. 10 no. 1 Feb. 2018.

11. W.-T. He J. Wang T.-T. Zhang F. Alzahrani A. Hobiny A. Alsaedi T. Hayat F.-G. Deng "High-efficiency three-party quantum key agreement protocol with quantum dense coding and bell states" Int. J. Theor. Phys. pp. 1–13 Jun. 2019.
12. Zhiwei Sun et. al., "Efficient Multiparty Quantum Key Agreement With a Single d-Level Quantum System Secure Against Collusive Attack", 12 Aug., 2019, Digital Object Identifier 10.1109/ ACCESS.2019.2931612.
13. Yin, X.R., Ma, W.P., Liu, W.Y.: Three-party quantum key agreement with two-photon entanglement. Int. J. Theor. Phys. 52, 3915–3921 (2013)
14. Yin, X.R., Ma, W.P., Shen, D.S., Wang, L.L. Wang "Three-party quantum key agreement with bell states" Acta Phys. Sinica vol. 62 no. 17 2013.
15. Shukla, C., Alam, N. & Pathak, A. "Protocols of quantum key agreement solely using Bell states and Bell measurement". Quantum Inf. Process. vol. 13 no. 11 pp. 2391–2405 (2014).
16. Zhu, Z.-C., Hu, A.-Q. & Fu, A.-M. "Improving the security of protocols of quantum key agreement solely using Bell states and Bell measurement." Quantum Information Processing 14, 4245–4254 (2015).
17. Bennett, C. H. and G. Brassard, Quantum cryptography: Public key distribution and coin tossing, Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India, December 1984, pp. 175–179.
18. Guo, F. Z., Liu, L., Qin, S. J. & Wen, Q. Y. Round-robin differential-phase-shift quantum key distribution with a passive decoy state method. Scientific Reports 7, 42261 (2017).
19. Shih, H. C., Lee, K. C. & Hwang, T. New efficient three-party quantum key distribution protocols. IEEE Journal of Selected Topics in Quantum Electronics 15, 1602–1606 (2009).
20. Liu, B., Gao, F. & Wen, Q. Y. Single-photon multiparty quantum cryptographic protocols with collective detection. IEEE J Quant. Electron. 47, 1383–1390 (2011).
21. Lin, S. & Guo, G. D. Quantum key distribution: defeating collective noise without reducing efficiency. Quantum. Inf. Comput. 14, 845–856 (2014).
22. Hu, J. Y. et al. Experimental quantum secure direct communication with single photons. Light-Science & Applications 5, 16144 (2015).
23. Huang, W., Wen, Q. Y., Jia, H. Y., Qin, S. J. & Gao, F. Fault tolerant quantum secure direct communication with quantum encryption against collective noise. Chin. Phys. B 21, 100308 (2012).
24. Yan, F. L. & Zhang, X. Q. A scheme for secure direct communication using EPR pairs and teleportation. European Physical Journal B 41, 75–78 (2004).
25. Lin, S., Wen, Q. Y. & Zhu, F. C. Quantum secure direct communication with χ-type entangled states. Phys. Rev. A 78, 064304 (2008).
26. Wang, T. Y., Liu, Y. Z., Wei, C. Y., Cai, X. Q. & Ma, J. F. Security of a kind of quantum secret sharing with entangled states. Scientific Reports 7, 2485 (2017).
27. Yang, Y. H. et al. Quantum secret sharing via local operations and classical communication. Scientific Reports 5, 16967 (2015).
28. Yang, Y. G., Teng, Y. W., Chai, H. P. & Wen, Q. Y. Fault-tolerant quantum secret sharing against collective noise. Phys. Scr. 83, 025003 (2011).
29. Song, X. L., Liu, Y. B., Deng, H. Y. & Xiao, Y. G. (t, n) Threshold d-Level Quantum Secret Sharing. Scientific Reports 7, 6366 (2017).
30. Sun, Z. W., Zhang, C., Wang, B. H., Li, Q. & Long, D. Y. Improvements on "multiparty quantum key agreement with single particles". Quantum Inf. Process. 12, 3411–3420 (2013).
31. Huang, W., Wen, Q. Y., Liu, B., Su, Q. & Gao, F. Cryptanalysis of a multiparty quantum key agreement protocol with single particles. Quantum Inf. Process. 13, 1651–1657 (2014).
32. Xu, G. B., Wen, Q. Y., Gao, F. & Qin, S. J. Novel multiparty quantum key agreement protocol with GHZ states. Quantum Inf. Process. 13, 2587 (2014).
33. Ekert, A. K. "Quantum cryptography based on Bellâs theorem," Physical Review Letters, vol. 67, no. 6, pp. 661–663, 1991.
34. Bennett C.H., "Quantum cryptography using any two non-orthogonal states," Physical Review Letters, vol. 68, no. 21, pp. 3121–3124, 1992.
35. Nguyen, B. A. Quantum dialogue. Phys. Lett. A 328, 6–10 (2004).
36. Gao, F., Qin, S.-J., Wen, Q.-Y. & Zhu, F.-C. An effective attack on the quantum key distribution protocol based on quantum encryption. Information Security and Cryptology, Lecture Notes in Computer Science 3822, 302–312 (2005).
37. Jin, X.-R. *et al*. Three-party quantum secure direct communication based on GHZ states. *Physics Letters A* **354**, 67–70 (2006).
38. Zhang, W. *et al*. quantum secure direct communication with quantum memory.
Physical Review Letters **118**, 220501 (2017).
39. Deng, F.-G., Zhou, P., Li, X.-H. & Zhou, C.-Y. Efficient multiparty quantum secret sharing with Greenberger-Horne-Zeilinger states. *Chinese Physics Letters* **23**, 1084–1087 (2006).
40. Hwang, T., Hwang, C.-C. & Li, C.-M. Multiparty quantum secret sharing based on GHZ states. *Physica Scripta* **83**, 045004 (2011).
41. Chou, Y.-H., Chen, S.-M., Lin, Y.-T., Chen, C.-Y. & Chao, H.-C. Using GHZ-state for multiparty quantum secret sharing without code table. *The Computer Journal* **56**, 1167–1175 (2012).
42. Jia, H.-Y., Wen, Q.-Y., Gao, F., Qin, S.-J. & Guo, F.-Z. Dynamic quantum secret sharing. *Physics Letters A* **376**, 1035–1041 (2012).
43. Hsu, J.-L., Chong, S.-K., Hwang, T. & Tsai, C.-W. Dynamic quantum secret sharing. *Quantum Information Processing* **12**, 331–344 (2013).
44. Liao, C.-H., Yang, C.-W. & Hwang, T. Dynamic quantum secret sharing protocol based on GHZ state. *Quantum Information Processing* **13**, 1907–1916 (2014).
45. Liu, H. *et al*. Multi-group dynamic quantum secret sharing with single photons. *Physics Letters A* **380**, 2349–2353 (2016).
46. Zeng, G.-J., Chen, K.-H., Chang, Z.-H., Yang, Y.-S. & Chou, Y.-H. Multiparty quantum key agreement based on quantum secret direct communication with GHZ states. *arXiv preprint arXiv:1602.00832* (2016).
47. Shi, R.-H. & Zhong, H. Multiparty quantum key agreement with Bell states and Bell measurements. Quantum Information Processing 12, 921–932 (2013).
48. ISO/IECDIS11770-3, *Information technology-Security techniques-Key Management-Part 3: Mechanisms Using Asymmetric Techniques.* International Organization for Standardization, 2013.
49. Wang, P., Sun, Z. & Sun, X. "Multiparty quantum key agreement protocol secure against collusion attacks". Quantum Inf. Process. 16, 170 (2017).
50. Yu, K.F., Yang, C.W., Hwang, T., Li, CM, Gu, J.: Design of quantum key agreement protocols with strong fairness property. arXiv:quant-ph/1510.02353v2 (2017).
51. Subramaniam, P., and Parakh,A., (2016) "A quantum Diffie–Hellman protocol," Int. J. Secur. Netw., vol. 11, no. 4, pp. 213–223, Jan. 2016.