sensors

MDPI

Article

Quantum Diffie–Hellman Extended to Dynamic Quantum Group Key Agreement for e-Healthcare Multi-Agent Systems in Smart Cities

Vankamamidi S. Naresh [1], Moustafa M. Nasralla [2], Sivaranjani Reddi [3] and Iván García-Magariño [4,5,*]

1 Department of Computer Science and Engineering, Sri Vasavi Engineering College, Tadepalligudeam 534101, India; vsnaresh111@gmail.com
2 Department of Communications and Networks Engineering, College of Engineering, Prince Sultan University, Riyadh 11586, Saudi Arabia; mnasralla@psu.edu.sa
3 Department of Computer Science and Engineering, Anil Neerukonda Institute of Technology & Science, Visakhapatnam 530003, India; rsivaranjani552008@gmail.com
4 Department of Software Engineering and Artificial Intelligence, Faculty of Computer Science, Complutense University of Madrid, 28040 Madrid, Spain
5 Instituto de Tecnología del Conocimiento, UCM, 28040 Madrid, Spain
* Correspondence: igarciam@ucm.es

Received: 5 June 2020; Accepted: 11 July 2020; Published: 15 July 2020

Abstract: Multi-Agent Systems can support e-Healthcare applications for improving quality of life of citizens. In this direction, we propose a healthcare system architecture named smart healthcare city. First, we divide a given city into various zones and then we propose a zonal level three-layered system architecture. Further, for effectiveness we introduce a Multi-Agent System (MAS) in this three-layered architecture. Protecting sensitive health information of citizens is a major security concern. Group key agreement (GKA) is the corner stone for securely sharing the healthcare data among the healthcare stakeholders of the city. For establishing GKA, many efficient cryptosystems are available in the classical field. However, they are yet dependent on the supposition that some computational problems are infeasible. In light of quantum mechanics, a new field emerges to share a secret key among two or more members. The unbreakable and highly secure features of key agreement based on fundamental laws of physics allow us to propose a Quantum GKA (QGKA) technique based on renowned Quantum Diffie–Hellman (QDH). In this, a node acts as a Group Controller (GC) and forms 2-party groups with remaining nodes, establishing a QDH-style shared key per each two-party. It then joins these keys into a single group key by means of a XOR-operation, acting as a usual group node. Furthermore, we extend the QGKA to Dynamic QGKA (DQGKA) by adding join and leave protocol. Our protocol performance was compared with existing QGKA protocols in terms of Qubit efficiency (QE), unitary operation (UO), unitary operation efficiency (UOE), key consistency check (KCC), security against participants attack (SAP) and satisfactory results were obtained. The security analysis of the proposed technique is based on unconditional security of QDH. Moreover, it is secured against internal and external attack. In this way, e-healthcare Multi-Agent System can be robust against future quantum-based attacks.

Keywords: quantum group key; quantum summation; quantum information; quantum teleportation; participant attacks; sensor; multi-agent system

1. Introduction

Nowadays the creation of a healthy society is the major concern, as the people living in this society are facing many problems—especially in healthcare. Over the years, advancement in the medical sciences has created effective diagnosis solutions to many life-threatening diseases. However, the rapid growth of technology, population and urban lifestyles have increased the demand to think about the smartness [1–3] of healthcare networks, in which the people will get the medical monitoring and treatment in a more quick and efficient manner.

In order to better provide healthcare services to the needy, healthcare stake holders such as citizens, medical practitioners, pharmaceutical companies, healthcare specialists, researchers and metropolitan managers are working together in an integrated Internet of Things (IoT)-environment in order to (i) offer emergency services with minimized healthcare access response time, (ii) offer remote treatment, (iii) collaborate with hospitals and doctors around the city and (iv) save time, money—and eventually lives.

E-healthcare technology in smart cities combines smart technologies, smart wearable devices and multi-agent sensors to support smart e-healthcare applications which can build a smart healthcare city. Nowadays, numerous initiatives have been taken to encourage the continuous monitoring of people's health condition through smart wearable devices like fitness bands and health monitoring apps in smart phones. These devices aim not only at monitoring health status continuously, but also at providing needed solutions at the right time. The smart wearable devices help to remotely assess individual health status or fitness regime without any professional help. To name a few applications, these devices can be used to help check blood and glucose level, body temperature, heartbeat, cardiovascular problems, vision quality and chronic ailments. Smart-city healthcare technology interacts with smart devices, collects data produced by these devices, and finally transfers these to doctors, researchers and the healthcare experts for better personalized diagnosis and solutions. In order to collect, analyze, process and suggest the best diagnoses, we need to integrate a system which is capable of performing different operation wisely and effectively.

MAS is a paradigm of great importance because a system capable of learning and changing its way of acting dynamically provides a great potential to face many problems the behavior of whose agents in the environment we do not know. This adds more levels of difficulty in tasks of consensus and coordination between agents, as they may be learning at all times and changing their behavior. A MAS is a distributed autonomous system consisting of multiple agents, who are autonomous in computing with good knowledge and solving capability. All these agents work collectively to provide effective healthcare to the citizens living in the city. Thus, a MAS approach can be considered as an effective approach to design and implement for the following reasons:

i. Provide an opportunity to divide the problem into subproblems solved by agents present in the MAS working as a team for defining and integrating information from different healthcare units to process the information efficiently;
ii. Propose best medical diagnostics to the patient based on the information collected from the patient;
iii. Provide coordination between different units and between the actors involved in the treatment process and tries to optimize the exchange of data between the units.

The advantages of MAS based e-healthcare systems include:

a. Efficiency: Increase efficiency in patient healthcare makes decrease in costs.
b. Increase in quality of care: e-health may improve the quality of patient healthcare by directing patient health information to the best quality diagnosis providers.
c. Encouragement of a new association between the patient and health proficient, towards a true partnership, where decisions are made in a shared manner.
d. Education of physicians through online sources (continuing medical education) and consumers (health education, tailored preventive information for consumers).

e. e-health permits patients to easily obtain health services online from global providers. These services can range from simple advice to more complex interventions or products such as pharmaceuticals.

As many numbers of zones are connected with each other through city healthcare management, it is highly impossible to provide efficient smart e-healthcare system with single software. In order to facilitate better smart healthcare system, the functionality should be divided into sub operations so that it can be autonomously monitored by a single software or hardware unit. Fortunately, MAS is an autonomous unit responsible for doing particular operations. Hence, the integration of MAS in smart city e-healthcare system will improve the efficiency. In recent days—taking the healthcare of citizens into the consideration—governments, along with public private partnerships are investing significantly in these projects. In year 2015, Dubai (UAE) established a unified national health database [4], which connect all hospitals and clinics for creating effective database concerning patient's medical history, ailments, surgeries and tests conducted. The aim is to save patients and help doctors perform diagnoses in an effective manner. In the South Pacific region, Australia initiated telemedicine and telehealth services [5], this improving both public and private hospitals.

As the data coming from the wearable devices communicate via wireless communication, the drawback for smart city healthcare is security and privacy issues. The main concern should be in terms of medical ID cards, which contains the personal details of the patient. In addition, hospitals must ensure security in encryption while issuing data collected for further processing for the benefit of the mankind. Hence, the security aspects of e-healthcare MASs are critical for providing security, privacy of healthcare data and safety of citizens in smart cities is the need of the hour. In this line of research, we propose a novel mechanism for securing the communication in distributed e-healthcare sensor systems with quantum principles, advancing the up-growing field of quantum-based security. In this way, e-healthcare MASs will be secure—even when quantum computing is able to be used to hack sensor systems.

2. Related Work

Different methodologies have been proposed earlier in for maintaining the privacy and security of the electronic health records (EHR) [6,7]. However, these methods need more security in order to distribute the health-related data. The e-healthcare systems are real time and have patient information which is in digital format. These are maintained by licensed persons. These data sets where formed by acquiring various data from different patients. In these EHRs, the authorized persons can be the patients or the doctors. The data present in the servers can be available in local or cloud, which stores and analyses the stored health data. The components which are present in the networks can be the inter connector between the patients and the medical staff for enhancing the broadcasting and distribution of data. However, there are many benefits to these systems: more threats are present in terms of security and privacy for the data used therein. These security threats are inherent to the system design. These threats can be classified into various categories such as data collection level [8–10], transmission level [11–14] and storage level [15,16], which are described more clearly in Section 3. Due to these threats in security and privacy of the EHR data, some users are not ready to use these applications. Hence, it is necessary to ensure that users should be ready to use the system without any hesitation. Therefore, it is important to propose a system for maintaining the security in the EHR data.

Quantum key distribution (QKD), started with a protocol BB84 by Bennett et al. [17] in 1984, addressed how to share an arbitrary key between 2 parties via single qubits using the quantum channel. The security of QKD uses arbitrary measurements of the qubits in one of two non-orthogonal bases, complementary and the fact that quantum mechanics rule out an eavesdropper from getting hold of information on the state of an unfamiliar qubit without upsetting it. In this way, any ensuing estimation of a complementary apparent on the same qubit becomes arbitrary. Moreover, entanglement and the superposition characteristics allow investigators to build up the quantum algorithm (QA) used to break the renowned RSA cryptosystem by quantum parallel computing. A QA can be a

powerful weapon to intimidate conventional cryptography. It allows investigators to build up quantum cryptography, which offer security using on physical laws rather than computational complexity, to shield in opposition to attacks from quantum computers. Moreover, further appealing applications conflicting the history are improved, such as quantum dense teleportation and coding. As far as this, three appealing branches of quantum cryptography are QKD [18–21], quantum secret sharing (QSS) [22–25] and quantum secure direct communication (QSDC) [26–29].

In 1991, Ekert developed an enterprise resource planning (ERP) based algorithms as a first QKD convention named E91 [30]. In the following year, an improvement was made by Bennett C; (H) and proposed an algorithm [31], which utilizes non symmetrical bases and two qubit states. Afterwards, in 2004, research was diverted onto key rate, key usage and storage space in bidirectional QKD. In 2004, Nguyen, proposed an algorithm [32] which permits two agents to swap over their secret message in one transmission, as a bidirectional QSDC (BQSDC) protocol or quantum dialog bidirectional. Gao et al. [33] in 2005, enhanced the protocol that adds a control head to assist the recipient to decrypt cipher message, which is exclusive of earlier knowledge about the message. Moreover, Jin et al. invented a multiparty QSDC (MQSDC) protocol [34], which permits agents to interchange their secret contributions, concurrently. Furthermore, Deng et al., [35]; Zhang et al., [36]; Chou et al. [37] and Hwang et al. [38] all invented competent multiparty QSS (MQSS) protocols during 2005 to 2012. Subsequently, Jia et al. [39]; Liao et al. [40]; Hsu et al. [41] and Liu et al. [42] as well introduced the proposal of dynamic MQSDC (DMQSDC) for the period of the period of 2012 to 2016.

Many quantum cryptographic algorithms [43–50] were proposed by diversified authors, which were widely used in many modern applications. Still, the progress of quantum key Agreement (QKA) is the significant subtopic in QKD. In QKD, one-member fix on the key and then distributes it to the other members, where as in QKA, more than one participant will be involved in key derivation. The QKA aiming to collect the pieces from all or selected participants to create a secret key.

The idea of multiparty QKA (MQKA) was first presented in 2012 when Shi et al. [51] proposed the foremost MCQAP dependent on Bell estimation and Bell states. After this, Liu et al. [52] brought up the drawbacks in this protocol, and afterward proposed one more MCQAP utilizing single particles. Since this point, many more MQKA protocols have been proposed. In 2013, Sun et al. [53] made the endeavor to improve the productivity of Liu et al.'s. MCQAP and propose a MCQAP in traveling mode. Unevenly, this protocol has additionally been shown to be unfair [54]. In 2014, an appropriated mode MCQAP is proposed with GHZ states by Xu et al. [55]. Around the same time, two traveling mode MQKA protocols were given cluster states and six-qubit states, separately by Sun et al. [56–58]. In the interim, however, these traveling type of MCQAP agreements proposed in these are out of line with collusion attack, i.e., a nontrivial subset of the group members can conspire to find the final shared key devoid of being noticed by others. In 2016, Huang et al. introduced a traveling mode MCQAP with single photons and unitary tasks [59]. Recently, Cao et al. also introduced a traveling mode MCQAP dependent on quantum search algorithms [60].

In turn—to attain the key generation setting and the generalization of two-party to MQKA—these MQKA protocols utilize the unicast communication method, swapping information one-for-one basis. Like this, the resource utilization will increase rapidly with the increase of members. In 2016, Zeng et al. [61] introduced a proficient MCQAP that relies on MQSDC utilizing 'broadcast' transmission, which implies that all agents can trade their mystery message, greatly improving effectiveness—yet additionally conserving time and quantum asset. In this work, we propose a MQKAP which can oppose both outer and inner attacks. In contrast, the proposed method utilizing the multicast transmission protocol is more viable than other current MQKAP. The proposed technique is based on the idea of generalization of two-party QKA to MDQKAP/ DQGKA. We expect the results of the proposed work will be useful for advanced research on fair MQKAPs. In this paper, we effectively use the proposed MDQKAP/DQGKA for secure communication in e-healthcare multi-agent system in smart cities.

Contributions

The main contributions of this work are indicated below:

- Propose a three-layered architecture for zonal healthcare systems;
- Propose a schematic arrangement of multi-agent system in zonal healthcare system which facilitates improvement in quality of healthcare;
- Propose a quantum group key agreement (QGKA) suitable for secure communication among multiple agents to achieve security in sharing the patient information;
- To prove the performance of proposed protocols is efficient in terms of Qubit efficiency (QE), unitary operation (UO), unitary operation efficiency (UOE), key consistency check (KCC), security against participants attack (SAP).

The remainder of this article is organized as follows. Section 3 presents the background of the protocol, two party QKA protocol with single photons. Section 4 presents the proposed methodology. Section 5 discusses the experimentation environment and the results. Section 6 presents the comparative analysis of the proposed work with other existing methods, considering fairness and security. The last section mentions a concise conclusion and future work.

3. Background Protocol for Quantum-Based Security in e-Healthcare Multi-Agent Systems

3.1. Notations

Here we specify all notations used in this paper. Table 1 indicates the list of abbreviations used in this article.

Table 1. List of acronyms of key concepts used in this article.

Notation	Description
QKD	Quantum key distribution
QKA	Quantum key agreement
MQKA	Multi-party QKA
QGKA	Quantum group key agreement protocol
DQGKA	dynamic quantum group key agreement protocol
MAS NJGK	Multi agent systems New join group key
NLGK	New leave group key
GC	Group controller
PGK	Previous group key
m	Number of bits exchanges between the nodes

3.2. Outline of Quantum Two-Party Key Generation

Key generation plays a vital role in all cryptosystems, which is used for encrypting as well as decryption of messages. To understand the basics of key agreement for background quantum concepts, one can refer a quantum Diffie–Hellman protocol. Although this work is focused on its particular application of e-healthcare MASs, this generation mechanism is general to most kind of systems.

In this direction, first we present the outline of the established two-party key agreement using quantum operations as depicted in Figure 1. At the end of the process, both A and B parties are left with a common shared key.

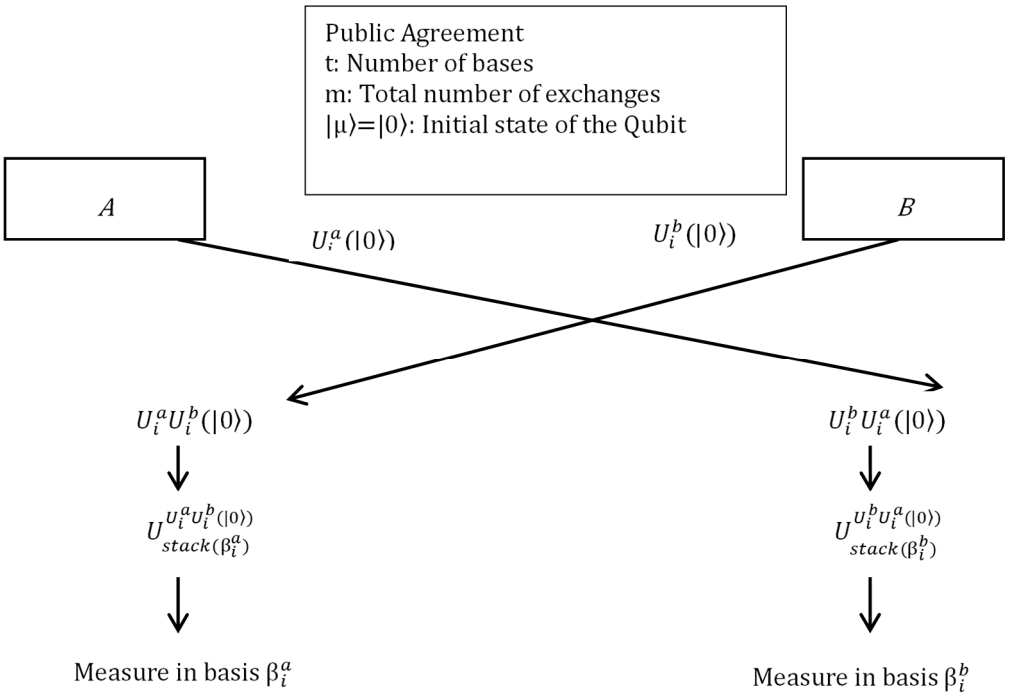

Figure 1. Outline of quantum two-party key-generation protocol.

3.3. Two-Party Quantum Key-Generation

Figure 2 shows the complete analysis of two-party quantum k bit ($\beta = \{\beta_1, \beta_2, \beta_3, \ldots, \beta_k, k > 1\}$) key agreement. Initially, both users involved in communication publicly decide k bases; also the m value (number of qubits used in key agreement). Each user individually selects m random bases $\beta_1^a, \beta_2^a, \ldots, \beta_m^a$, where $\beta_i^a \in \beta$ and $\beta_1^b, \beta_2^b, \ldots, \beta_m^b$, where $\beta_i^b \in \beta$, also, m random bits $a_1, a_2, a_3, \ldots, a_m$ and $b_1, b_2, b_3, \ldots, b_m$, then calculates U_i^a to $|0\rangle$, finally sends to other participants.

Phase 1: Initialization

1. A and B publicly agreed on "k" bases $\beta = \{\beta_1, \beta_2, \beta_3, \ldots\ldots, \beta_k, k > 1\}$
2. Let $l = m - d$ be +ve length of the key to be exchanged, where "m" is the quantity of qubits to be exchanged and "d" be the number of qubits discarded during the detection of Eves presence
3. Moreover, they agreed on early state pf qubit $|\mu\rangle = |0\rangle$ that will be manipulated and exchanged

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

Phase 2: Key agreement

Let $k'' = \{k_1, k_2, k_3, \ldots., k_m\}$ and $k^1 = \{k_1^1, k_2^1, \ldots, k_m^1\}$ be seq random bits obtained by A and B correspondingly and

i. A and B announces the bases to each other
ii. For each execute i where $\beta_i^a \neq \beta_i^b$ discard the values k_i and k_i^1 from k'' and k^1
iii. A and B choose k bits from the result set of bits, treated as the key, used in forthcoming communication.

Figure 2. Two-party quantum key agreement algorithm.

After receiving the keys from the other user, the key finalization process is initiated by discussing publicly about the used basis. The key bit is accepted in final key when the predicted key bit is matched with the bases used. Otherwise, it is discarded. This operation continues until all the m bits are processed. The bits satisfying the similarity check are be the final key used for encryption and decryption.

4. Proposed MAS Based e-Healthcare System Architecture

In this section, first we propose a zone level three-layered system architecture. Next, we present the MAS arrangement to facilitate effective processing in the zonal-level architecture. To address secure communication in the proposed architecture, we present a quantum-based group-key agreement. Finally, we integrate the above to establish MAS based e-healthcare system in a city named as smart healthcare city.

4.1. Zonal Level Healthcare System Architecture

In this subsection, we present a three-layered architecture of the zonal-level healthcare system as depicted in Figure 3. This is named as the infrastructure layer, middleware layer and the stakeholder layer.

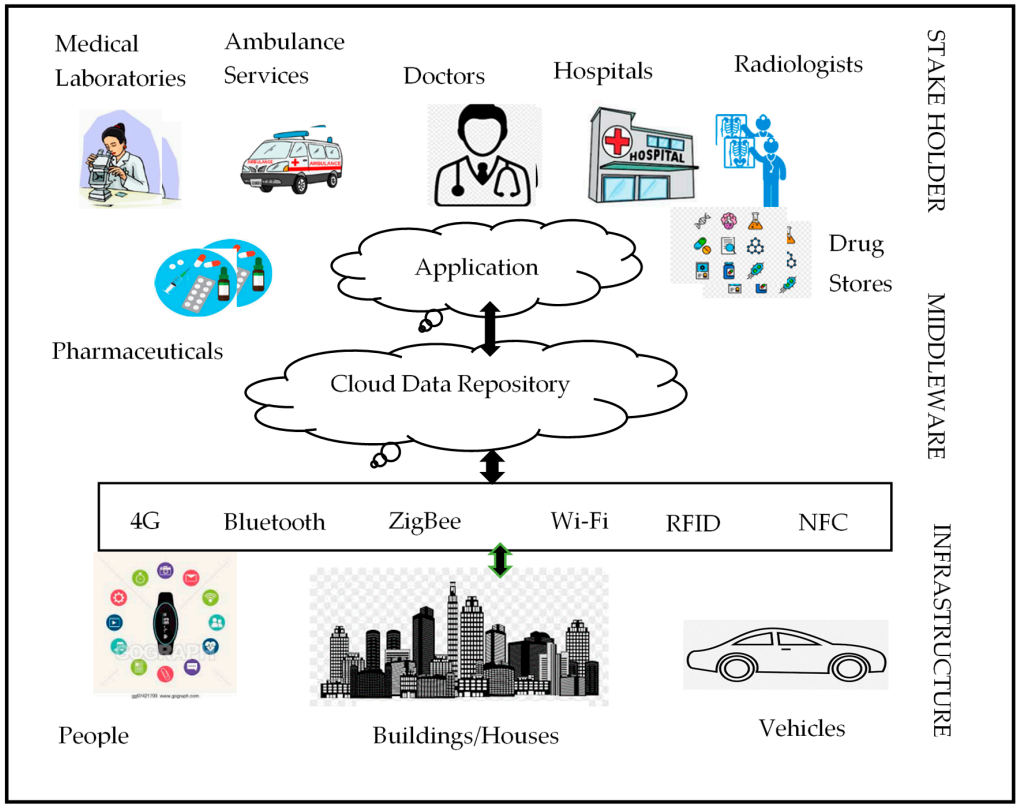

Figure 3. Zone level healthcare system architecture.

A. Infrastructure Layer: This layer is the patient–data–producer layer. It collects the health data from wearable devices, WBANs, houses/buildings and the sensors attached to the vehicles. All the collected data will be transferred to the middleware layer through communication protocols like 4 G, Bluetooth, Zigbee, etc.

B. Middleware Layer: This layer's responsibilities include data collection from the infrastructure layer, data processing, data storage on local data storage area and sharing of the information with the concerned stakeholder for further processing of the patient data. It is also responsible to transfer the data to the central healthcare management system.

C. Stakeholder Layer: This layer consists of the all the healthcare experts who can able to work on patient health records. The stakeholders in this layer includes doctors, laboratories, pharmaceuticals, ambulance services, medical stores, radiologists, etc. As the patient data are collected from the middle layer, it will be dispatched to relevant stake holder in order to provide qualitative diagnosis. It also responsible to share the patient health records with the research laboratories when the doctors failed to trace the disease for analysis, in the continuation, the drugs can be manufactured by the pharmaceutical's companies.

4.2. Smart Healthcare Architecture

In this subsection the smart city healthcare architecture is depicted in Figure 4, this arrangement is connecting the healthcare system. Traditionally, smart city is divided in zones for better administration and each zone has its own healthcare system. Keeping in view, fast and effective data processing and technical challenges, it is assumed that smarter city objective will be achieved in an incremental manner. We used the concept of zone level service; arrangement supports step-by-step movement towards a smart city. Each zone has its own autonomous healthcare system that comprises a local data collection center, communication infrastructure and local stake holder.

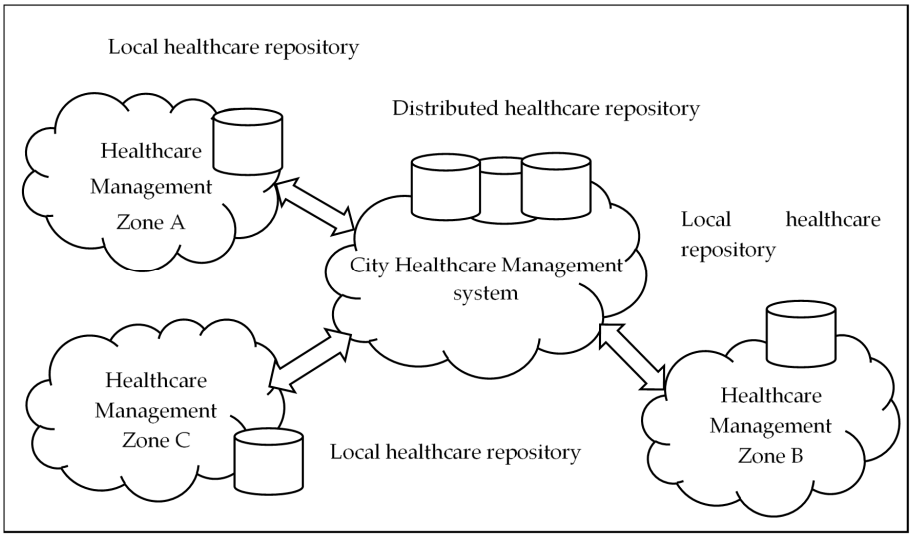

Figure 4. Smart city healthcare architecture.

In Figure 4 we can observe that, a city healthcare management system, is connecting the healthcare system of three zones termed as zone A, zone B and zone C. The responsibilities of the city healthcare management include, patient health information collection from different zones, storing of collected patient health information in master repository and sharing of health record of patient in one zone to stake holders in other zones to provide better diagnosis.

As many numbers of zones are connected with each other through city healthcare management, it is highly impossible for one software to provide efficient smart healthcare system. In order to facilitate better smart healthcare system, the functionality should be divided into sub operations and then autonomously monitored by a single software or hardware unit. Fortunately, MAS is an autonomous unit responsible for doing particular operation. Hence, adapting MAS in healthcare provides quality service to the patient effectively. Figure 5 shows the zone-wise MAS, consisting of the following agents:

1. Health data agent: These are nothing, but the primary patient health recording devices, continuously monitor the health parameters of the patient, forward the health information to the data-collection agent. In general, the health data agents can be wearable devices, WBAN networks, etc. In addition to monitoring of citizen health, it is also responsible to transfer the collected information to the nearby data-collection agent;

2. Data-collection agent: This is the unit placed at the region wise, it is responsible to collect the data from all the devices (citizen wearable devices, building/houses, vehicles, etc.), and then transfer it to the department agent;
3. Department agent: The department agent is the software placed in the zone head office, responsible to collect patient data from all the regions in connection with it, this agent usually presents in the middle layer. The responsibilities of the department include, data processing using any of the machine learning algorithms, and then place it onto the data storage unit;
4. Data persistence agent: The data persistence agent is responsible to extract a piece of required patient data present on the database storage unit and then forward it to data visualization unit as well as to the stake holder agent;
5. Stake holder's agent: The stakeholders' agent is usually present in top layer, is responsible to deliver the extracted patient information to the required stakeholders includes, booking an appoint to doctor, sending alert to ambulance, etc.

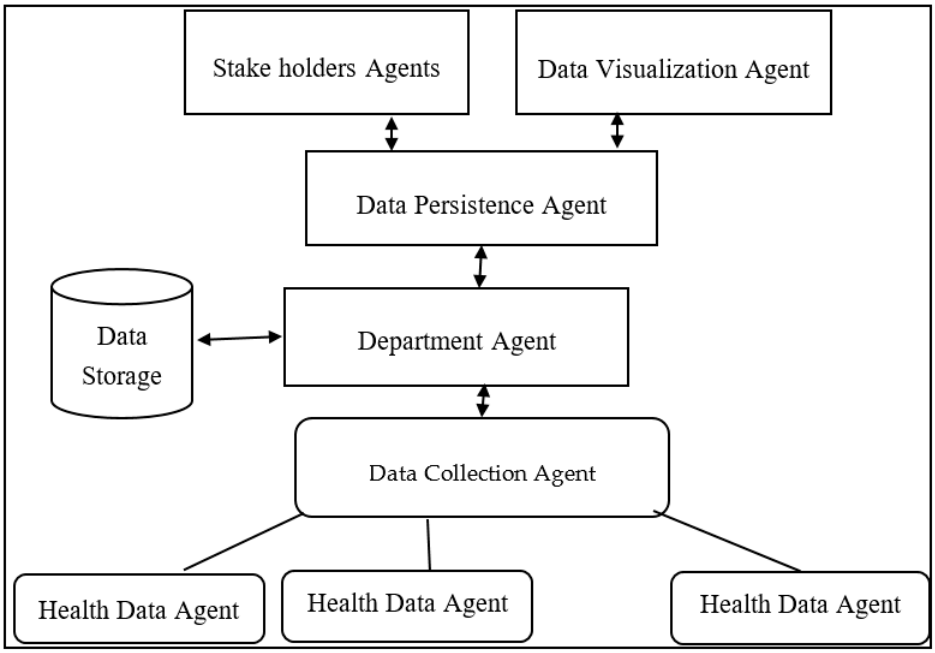

Figure 5. Multiagent architecture of smart city healthcare system in a zone.

Hence, smart city e-healthcare system is the arrangement, which integrated different zones through the MAS. As we already aware of that, communication between multiple agents raises security and privacy challenges. In order to provide, security to the patient information, which is passing through multiple agents at multiple levels need to be secured. In this paper, we are proposing a quantum group key agreement protocol to secure the patient health information. The key can be used in encryption and decryption algorithms to secure the information. The provision of security algorithm based on fundamental laws of physics, the scope of unhackability and easiness in usages made us to prefer quantum key cryptography in key agreement between the agents.

4.3. Quantum Group Key Agreement Protocol

Let $M_1, M_2, M_3, \ldots, M_n$ be the members of the group.

Public agreement: All the group members M_i, $1 \leq i \leq n$ agree on the set of t bases $\beta_1, \beta_2, \ldots, \beta_t$, for $t > 1$ to use and the quantity of qubits to exchange. The value of m is based on the required key length and discarded quantity of qubits during the detection of presence and errors.

Step 1: In this step the group controller forms two parties with remaining members and generates QDH two-party keys, respectively, as follows:

The GC $M_{1,}$ generates two party keys with $M_{i,}$ $2 \leq i \leq n$.

$$QDH_{M_1M_i}(t) \rightarrow k_{1,i,} 2 \leq i \leq n$$

In this step of proposed protocol in the process of generating two-party keys, entanglement allows legitimate parties to detect eavesdroppers by virtue of the fact that if the sender and recipient each have a photon the two of which are related by quantum mechanical entanglement -interception or measurement by an adversary will change the two photon system in a way that the legitimate parties can readily detect.

Step 2: The GC, M_1computes the partial key component " $\oplus_{i=2,i\neq j}^{n} k_{1,i}$" for each member M_i and encrypt them with the respective to members shared key and send them to the respective members as follows:

$$M_1 \overset{E_{k_{1,j}}[\oplus_{i=2,i\neq j}^{n} k_{1,i}]}{\longrightarrow} M_j,\ 2 \leq j \leq n$$

Step 3: After receiving the message from M_1 each group member M_j, decrypts the partial key component with respective key and XORed it with their own shared key to computes the group key as follows.

$$Group\ Key = QGDH_{M_1M_{2\ldots}M_n}(t) = \oplus_{i=2}^{n} k_{1,i}$$

Step 4: Finally, as the GC knows all the two-party keys, he can easily compute the group key by joining all the two-party keys with EX–OR as *Group Key* $\oplus_{i=2}^{n} k_{1,i}$.

4.4. Dynamic Quantum Group-Key Agreement Protocol

The GKA protocol, QGKA, is primarily suitable for static groups, in which the group members are fixed. However, in spite of the existing group members, there are the scenarios where, we need to add a new member (or) delete an existing group member from the initial group. To address this dynamic connectivity of nodes in group, join and leave protocols are added to QGKA technique is termed as DQGKA.

In this subsection we extend the quantum group key agreement protocol by proposing member join protocol and member leave protocol

4.4.1. Member Join Protocol

This protocol will uphold the secrecy of the earlier group key even after join of new members in the group.

i. Once per fresh member M_{n+1} need to add into group, it informs the GC and produce *QDH* key $k_{1,n+1}$ with GC by taking the advantage of *QDH*.

ii. The GC produces r_{n+1} a random quantum string and broadcasts $k_{1,n+1} \oplus r_{n+1}$ to group members M_i present before. Upon getting, new GK is calculated as

$$NJKA = PGK \oplus k_{1,n+1} \oplus r_{n+1} = \oplus_{i=2}^{n+1} k_{1,i} \oplus r_{n+1}$$

iii. The GC sends out $PGK \oplus r_{n+1}$ *to* M_{n+1}. Now M_{n+1} compute the fresh key as

$$NJKA = PGK \oplus r_{n+1} \oplus k_{1,n+1} = \oplus_{i=2}^{n+1} k_{1,i} \oplus r_{n+1}$$

4.4.2. Member Leave Protocol

This protocol secures the new group key derived by current group members from the members leaving the group along with the outsider.

This protocol will secure the new group key derived by current group members from the members leaving the group along with the outsider.

(i) Once M_j desires to leave from group, it informs the group controller.

(ii) The GC produces r_j a random quantum string and sends out $k_{1,j} \oplus r_j$ by enciphering with $k_{1,i}$ to the respective group member M_j, $i \neq j$, i.e., excluding members left from group. In other words, $M_1 \overset{E_{k_{1,i}}[k_{1,j} \oplus r_j]}{\longrightarrow} M_j$, for $1 \leq i \leq n$, $i \neq j$.

(iii) On getting, group member M_i decipher the received message with $k_{1,j}$ and calculate the fresh key as under:

$$NLKA = PGK \oplus k_{1,j} \oplus r_j = \oplus_{i=2, i \neq j}^{n} k_{1,i} \oplus r_j$$

(iv) In addition, M_L calculates new key as:

$$NLKA = PGK \oplus k_{1,j} \oplus r_j = \oplus_{i=2, i \neq j}^{n} k_{1,i} \oplus r_j$$

Table 2 shows the computation and communication cost of the DQGKA for different operations like group initialization, member join and member leave operations.

Table 2. DQGKA computation and communication cost.

Protocol	**Communication**				**Computation**
DQGKA	**Rounds**	**Messages**	**Unicast**	**Broadcast**	**XOR Operation**
Initialize	2	$m-1$	$m-1$	0	$2\,m$
Join	1	2	1	1	4
Leave	1	$m-2$	$m-2$	0	3

5. Security Analysis of the Proposed Quantum Based Approach for Securing MAS Based E-Healthcare System

In this section, first we discussed the performance and security of QDH protocol and then show that the proposed protocol DQGKA presented in Sections 4.3 and 4.4 all have the same inherent security features, such as key secrecy, forward secrecy, backward secrecy. Further we present protection from some of the important attacks such as internal eavesdropping, intercept and resend attack with fairness analysis.

5.1. The Performance and Security of QDH Protocol

Alice and Bob $m > 1$. Let s, $0 \leq s \leq m$, be the number of usable qubits obtained from these exchanges, i.e., the number of qubits for which Alice and Bob selected the same bases. Let σ be the fraction of s compared to detect Eve. Therefore, number of comparisons performed by Alice and Bob to detect Eve is $k = s \times \sigma$. The number of bits in the secret shared key is $l = s - k$. The number of usable qubits obtained in QDH (t) depends on two factors:

- the number of bases used, t;
- the number of exchanges performed, m.

Since Alice and Bob independently, randomly and uniformly probability that they will choose the same exact basis, for any given exchange, is $1/t$. Then the number of usable qubits obtained from m exchanges is $s = \frac{m}{t}$.

The efficiency of the protocol, ϱ, is then defined as the ratio of the number of usable qubits to the number of exchanges performed in the protocol. This result in, $\varrho = \frac{s-(\sigma \cdot s)}{m} = \frac{1-\sigma}{t}$.

The security of QDH (t) depends on Alice and Bob performing a sufficient number of exchanges so that Eve can be detected with high probability. The sum $1 - \sigma$ of the usable qubits result in bits that constitute the shared secret key.

The probability of detecting Eve for a given number of exchanges m and number of bases t is computed as follows:

In the QDH (t) protocol, k of the s usable qubits are used to detect Eve and the remaining $s - k$ qubits constitute the key whenever Eve is not detected. The probability of Eve not being detected in these k exchanges.

In general, in a protocol QDH (t), $t > 1$ available bases, the probability of Eve measuring at least one of the qubits with a basis other than that chosen by Alice and Bob $P(A) = \frac{t^2+1}{t^2}$. The probability of the measured qubits producing different values $P(B/A) = \frac{1}{2}$.

Note that $P(B/A)$ is computed assuming that all of the four-qubit pair value 00, 01, 10 and11 are equally likely. This is the case whenever the base angle chosen by Eve differs from that of Alice and Bob in a way that the qubit measured by Eve collapse to 0 and 1 with roughly equal probabilities.

Therefore, the probability of detecting Eve in QDH (t) is, $P_d = 1 - \left(\frac{t^2+1}{2t^2}\right)^k$.

- With the increase in number of bases, t, is increased; we see that probability of Eve going undetected tends to one-half (for each exchange) and the probability of detection in k comparisons becomes:

$$P_d = 1 - \left(\frac{1}{2}\right)^k \text{ as } t \to \infty.$$

- Our results showed that with the increase in number of comparisons k, probability of detecting Eve in QDH (t) increases.
- Eve can be detected with a probability $P_d = 0.5$, even when $k = 1$.

5.2. Security of Proposed Protocol DQGKA

Theorem 1. *The group key derived using quantum group key agreement protocol is indistinguishable in polynomial time from random numbers.*

Proof. Each of the two-party shared keys generated in the Step 1 of quantum group key agreement protocol is secure, because it uses a *QDH* protocol. That is, all the two-party shared keys exchanged in Step 1 are indistinguishable from random numbers in polynomial time.

The GC $M_{1,}$ generates two party keys with M_i, $2 \le i \le n$.

$$QDH_{M_{1,}M_i}(t) \to k_{1,i,} 2 \le i \le n$$

In this step of proposed protocol in the process of generating two-party keys, entanglement allows legitimate parties to detect eavesdroppers by virtue of the fact that if the sender and recipient each have a photon the two of which are related by quantum mechanical entanglement -interception or measurement by an adversary will change the two photon system in a way that the legitimate parties can readily detect. Hence, that man in the middle attack can be easily detected.

In Step 2 The GC, M_1 computes the partial key component " $\oplus^{n}_{i=2,i\neq j} k_{1,i}$" for each member M_i, respectively and send them to the respective members.

$$M_1 \overset{E_{k_{1,j}}[\oplus^n_{i=2,i\neq j} k_{1,i}]}{\longrightarrow} M_j,\ 2 \le j \le n$$

Note that these partial key component is also secured as it is obtained by XORed the secured shared keys generated in Step 1. Further, the GC sends these partial key components to the respective group members securely through established encrypted link between them. After receiving, the respective member decrypts their partial key component and computes the group key securely by XORing with own shared key as follows:

$$\text{group key} = QGDH_{M_1M_{2,\ldots}M_n}(t) = \oplus^n_{i=2} k_{1,i}$$

Since the group key $\oplus_{i=2}^{n} k_{1,i}$ is indistinguishable from random numbers in polynomial time, and thus secured. □

Theorem 2. *The join protocol of DQGKA satisfies the properties of backward security.*

Proof. This protocol will uphold the secrecy of the earlier group key even after join of new members in the group as follows:

(i) Once per fresh member M_{n+1} need to add into group, it informs the GC and produce QDH key $k_{1,n+1}$ with GC by taking the advantage of *QDH*.
(ii) The GC produces r_{n+1} a random quantum string and broadcasts $k_{1,n+1} \oplus r_{n+1}$ to group members Mi present before. Upon getting, new GK is calculated as $NJKA = PGK \oplus k_{1,n+1} \oplus r_{n+1} = \oplus_{i=2}^{n+1} k_{1,i} \oplus r_{n+1}$.
(iii) The GC sends out $PGK \oplus r_{n+1}$ to M_{n+1}. Now M_{n+1} compute the fresh key as $NJKA = PGK \oplus r_{n+1} \oplus k_{1,n+1} = \oplus_{i=2}^{n+1} k_{1,i} \oplus r_{n+1}$.

As in step 3 the GC sends out $PGK \oplus r_{n+1}$ to M_{n+1}. Since M_{n+1} does not know r_{n+1} it cannot find PGK and hence, backward secrecy is attained of join protocol *DQGKA*. □

Theorem 3. *The leave protocol of DQGKA satisfies the properties of the forward security.*

Proof. This protocol will secure the new group key derived by current group members from the members leaving the group along with the outsider.

(i) Once M_j desires to leave from group, it informs the group controller.
(ii) The GC produces r_j a random quantum string and sends out $k_{1,j} \oplus r_j$ by enciphering with $k_{1,i}$ to the respective group member M_i, $i \neq j$, (i.e.,) excluding members left from group. In other words, $M_1 \overset{E_{k_{1,i}}[k_{1,j} \oplus r_j]}{\longrightarrow} M_i$, for $1 \leq i \leq n$, $i \neq j$.
(iii) On getting, group member M_i decipher the received message with $k_{1,j}$ and calculate the fresh key as under:

$$NLKA = PGK \oplus k_{1,j} \oplus r_j = \oplus_{i=2, i \neq j}^{n} k_{1,i} \oplus r_j$$

(iv) In addition, M_L calculates new key as:

$$NLKA = PGK \oplus k_{1,j} \oplus r_j = \oplus_{i=2, i \neq j}^{n} k_{1,i} \oplus r_j$$

To exclude the shared key component $k_{1,j}$ of leaving member M_j from *PGK*, we use $PGK \oplus k_{1,j}$. To make the updated key secure from M_j, the GC includes another random r_j. Hence, we have the principal security prerequisite of member exiting holds with respect to previous members of the group and outsiders. □

5.3. Attacks on Proposed Protocol DQGKA

Protection from Internal Eavesdropping: In fact, inside members of the group have 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 provided the GC should be trustworthy. Hence, that the internal members of the group cannot influence the group key. Thus, the proposed protocol is protected from the eavesdropping attack of internal members.

Intercept and resend attack: As assault, Eavesdropper Eve (E) attempts to quantify the quantum states originating from A and afterward sends the changed states to B. As E, has no information about

basis of state chosen by A, he/she can just estimate which basis to measure in, similarly B does. In the event that E picks effectively, she/he can measure the right photon polarization state as it is sent by A and reacts in right state to B. If E picks wrongly, then state estimation is random, and the state conveyed to B is not as sent by A. Table 3 below shows an instance of this attack.

Table 3. Intercept and resend attack.

Quantum Key Transmission between User A, E and B										
User-A random bits	1	1	1	1	0	0	1	1	1	1
Random sending bases	X	X	+	+	+	X	X	+	X	X
Photons user-A sends	↘	↘	→	→	↑	↗	↘	→	↘	↘
E's measuring basis	X	X	+	X	+	X	+	+	+	X
Polarization Eve measures and communicate	↘	↘	→	↘	→	↗	↘	→	↘	↘
B's measuring basis	↘	↘	↘	→	→	↗	↘	→	↘	↘
Random received bases	X	X	X	+	+	X	+	X	+	X
PUBLIC DISCUSSION										
User-A says which bases were correct	√	√		√		√				√
OUTCOME										
Shared key between user-A and B	1	1		1		0				1

Basis used +0: ↑; +1: →; X0: ↗; X1: ↘ .

The likelihood E picks the wrong basis is 50% (supposing A picks arbitrarily), and if B measures this intercepted photon in the basis A gets an arbitrary result, i.e., a wrong outcome with likelihood of 50%. The likelihood of an intercepted photon creates an error in the key string is then 50% × 50% = 25%. If A and B openly contrast their key bits (thus leaving them as key bits, as they are no longer secret) the likelihood they discover variance and recognize the existence of E is $P_e = 1 - \left(\frac{3}{4}\right)^n$.

Hence, to notice an eavesdropper with probability $P_e = 0.999$. A and B require to compare n = 72 key bits. In the proposed protocol entanglement allows legitimate parties to detect eavesdroppers by virtue of the fact that if the sender and recipient each have a photon the two of which are related by quantum mechanical entanglement -interception or measurement by an adversary will change the two photon system in a way that the legitimate parties can readily detect.

Fairness Analysis: It is recognized fact that, in a group quantum cryptographic protocol, there is a possibility of attack from fraudulent members either external or internal. These members are having more scope to attack the protocol. Initially, he/she is able to change the legal photon sequence, next, bring in errors into the information. Further they may team up with some more unfair members in implementing the protocol. As the proposed protocol is using the concept of GC, the secured communication is happening between GC an individual participant in the group, even though all the participants can able to compute the shared key. For communication between two participants, it is proved that the proposed mechanism is secured against eavesdropping in previous section. Hence, proposed protocol is secured against participant attack.

6. Results and Discussion in the Context of Multi-Agent-Based e-Healthcare System in Smart Cities

In order to test the current approach, we have focused on common interactions in multi-agent system in smart cities, like in the context of doctor's appointment data set smart, this application belong to the context of smart cities, as the proposed approach is aimed at securing multi-agent system for e-healthcare in smart cities.

IBM developed a composer, suitable for quantum computing called as Qiskit, which can be used for real time experiments like quantum simulation, quantum algorithms development, testing of theoretical tasks, quantum cryptography and error correction. Qiskit comprises of four central

components: Terra (the code establishment, for forming quantum programs using circuits and pulses), Aqua (creating algorithms and applications), Ignis (removing noise and correcting errors) and Aer (quickening improvement by means of emulators, simulator and debuggers). In our experimentation, Aer, the 'air' component, pervades all Qiskit components. Hence, as to accelerate the improvement of quantum PCs better emulators, simulators and debuggers are required. Aer will assist us with understanding the cutoff points of traditional processors by showing to what degree they can copy quantum calculation. Moreover, we can use Aer to validate that present and near-future functions of quantum computers properly. This should be possible by extending the cutoff points of simulation and by recreating the impacts of practical noise on the calculation. Algorithms implementation has done using Aer elements in Qiskit. The generated quantum key is used to encrypt the dataset with the following information. In the experimentation, a doctor appointment dataset (110,356 doctor appoint records) is taken from the Kaggle [62] with 14 columns named as PatientID, AppointmentID, Gender, Scheduled Day, Appointment Day, Age, Neighborhood, Scholarship, Hypertension, Diabetes, Alcoholism, Handicap, SMS_received, No-show.

The proposed algorithm initially sets up a group with m users (healthcare agents or stake holders) among them the first user will act as the group controller (GC) aiming to share a common key among the group users. In the experimentation group is created for m = 5 users, user-1 becomes GC and other four are group members. Once the group users are identified, they decides the key length(n), in the experimentation the max key length used is 23 bits, generates possible numbers in range 0 to $2^{23} - 1$.After the finalization of the bit length, each user creates their own register with the bit length (n) in order to store n bits using the function quantum Register(). Each individual user will start sharing their contribution with GC, Table 4 shows the quantum key-sharing process between individual group member and the GC for a key length 10. Then, GC initiates a process to calculate the key to individual user from the received keys. For user-2 GC uses the keys received from other users except user-2, performs the XOR operation on these keys. Similarly, he follows the same procedure in computation of all other group users and communicates securely to the users, key calculation formula for user-i is given by $PK_{gci} = \oplus\left(K_j\right)$ for all $j \in \{1,n-1\}$ and $j \neq i$, where PK_{gci} is the partial key computed by GC for i-th member.

Table 4. Shared key calculated by all the other group users except GC.

Quantum Key Transmission between User-i and GC										
User-i random bits	1	1	1	1	0	0	1	1	1	1
Random sending bases	X	X	+	+	+	X	X	+	X	X
Photons user-i sends	↘	↘	→	→	↑	↗	↘	→	↘	↘
Random received bases	X	X	X	X	+	X	+	+	+	X
Bits GC has received	1	1	1	0	1	0	1	1	0	1
PUBLIC DISCUSSION										
GC reports the bases of received bits	X	X	X	X	+	X	+	+	+	X
Photons GC measured	↘	↘	↘	↗	→	↗	→	→	↑	↘
User-i says which bases were correct	√	√				√				√
OUTCOME										
Shared key between user-i and GC	1	1				0				1

Basis used: +0: ↑; +1: →; X0: ↗; X1: ↘ .

Table 5 shows the partial key component calculated by GC for these four users in the group. Afterwards, GC calculates the common group key by performing the XOR operation on all the keys of group users along with his key, it is calculated as PK_{gci}.

Table 5. Key component established by GC for the respective members.

User	Key Index	Individual Members-Two Party Keys Established with GC (K_i)	Two Party Keys after Length Adjustment	Partial Key Components Established by GC for the Respective Members
User-2	K_2	1101	1101	$K_3 \oplus K_4 \oplus K_5$
User-3	K_3	101	0101	$K_2 \oplus K_4 \oplus K_5$
User-4	K_4	0100	0100	$K_2 \oplus K_3 \oplus K_5$
User-5	K_5	1111	1111	$K_2 \oplus K_3 \oplus K_4$

Table 6 shows the final group key calculated by GC, all other group members. Group key is computed by XOR the received partial component from GC with his own key contribution, which is given by $Key_i = PKey_{GCi} \oplus K_i$, here Key_i established by each member will be the same, which we can use as a group key.

Table 6. Computation of final group key by all the users of e-healthcare.

User Number	Partial Key Component sent by GC ($PKey_{GCi}$)	Individual Two-Party Keys Established with GC (K_i)	Final GROUP KEY Key_i=$PKey_{GCi} \oplus K_i$
User-2	0101	1101	1000
User-3	1101	0101	1000
User-4	1100	0100	1000
User-5	0111	1111	1000

Algorithm development has done using the Qiskit built in functions, its description is shown in Table 7, each user in the group needs to create a register based the qubit length using QuantumRegister() function, then after a random number is generated using np.random.randin(),returns any number in the range 0 to 2^{n-1}, np.binary_repr() function is used to convert it into binary form in order to store on register.

Table 7. Qiskit functions.

Function Name	Description
Quantum Register (n, name='qr')	Used to store one qubit bit
Classical Register (n, name='cr')	For storing the output of the measurement
Quantum Circuit (qr, cr, name='Alice')	Collections of quantum gates interconnected by quantum wires
np.random.randint (0, high=2n)	Generate a random number between 0 to 2n
np.binary_repr (alice_key, n)	Returns the binary equivalent of the given number n as a string
BasicAer.get_backend ('qasm_simulator')	Simulates the circuit in the backend
execute (bob, backend = backend, shots = 1).result()	Executes the circuit created using qsam simulator in the backend

Overall, the experimentation was started using a group with 2 users, extended to 5 and 10 users and checked the functionality of the proposed algorithm. Figure 6 shows the key-sharing time between individual users and the GC by varying variable key lengths. The graph shows the key-sharing time for 5-, 10- and 20-bit lengths. Key-sharing time is the time used in quantum key transmission between user i and the GC. As the detailed process explains in Table 4, this was always constant irrespective of group users. However, the time increased linearly with respect to the increase in bit length, because, as the key length increased the time needed to guess the basis, as the public discussion in order to know the bases used by the user and final shred key derivation time also increased. Figure 7 shows the GC qubit generation time in the key-sharing process. This is the time the GC required to guess the bases upon receiving of the key from the user. The time in this process increased with an increase in

group users. From Table 4, it can be observed that before finalization of the key between two users, there was a communication in public for sharing the basis. Figure 8 represents the time had spent in public conversation in order to finalize the key. Afterwards, GC finalized the key to individual user by performing the XOR operation on other n − 1 users. This computation time is presented in Figure 9. From the graph we can observe that with an increase in number of group members and the key length, computation time also increased. Figure 10 shows the secure communication time complexity between the data-collection agent and the department agent after collecting the doctor appointment dataset from the infrastructure layer. First, he derived the key with department agent using two-party quantum key agreement. Then, he encrypted the collected data using the key by doing the repeated XOR between the aggregated dataset and key. Next, the ciphered dataset was transferred onto department agent. The department agent collected the cipher dataset and then extracted the doctors appoint dataset using the key agreed with data-collection agent. Finally, the deciphered appointment dataset was stored onto the database. In the overall process, four phases were mainly involved: key agreement time complexity, encryption time complexity, decryption time complexity and overall computation time complexity. From the graph we can observe that more time was required for the key agreement phase than the encryption/decryption phase. Multicast and broadcast secure healthcare data sharing can be done using QDGKA—along with the encryption and decryption procedures specified in this paper.

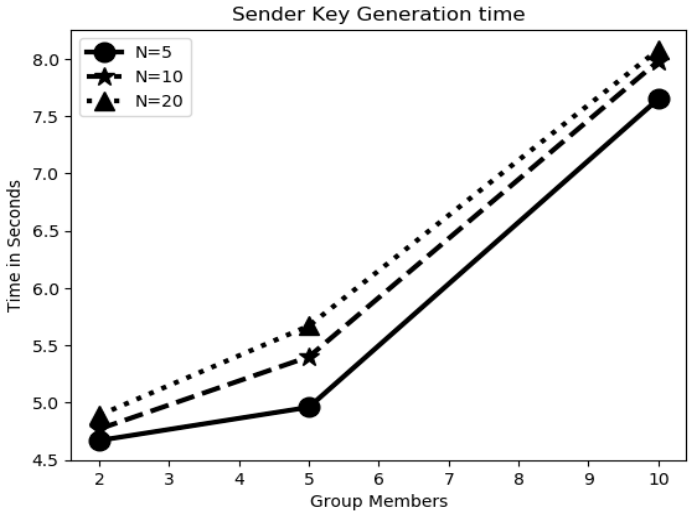

Figure 6. Key-generation time among multi-agents/stake holders.

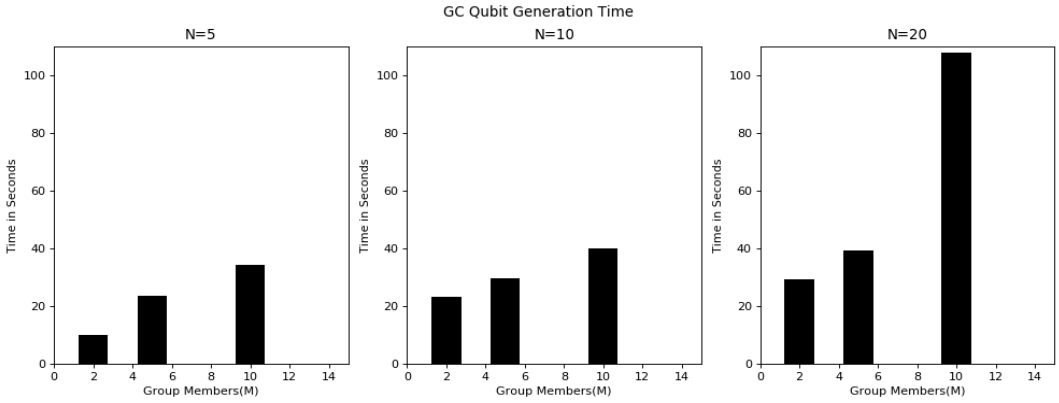

Figure 7. Time for qubit generation by GC.

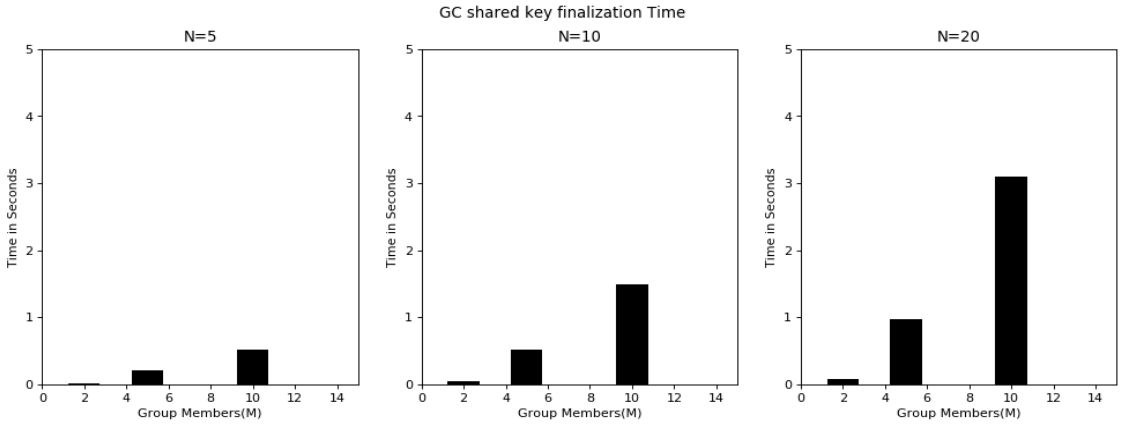

Figure 8. Time for shared key finalization with individual user through public discussion.

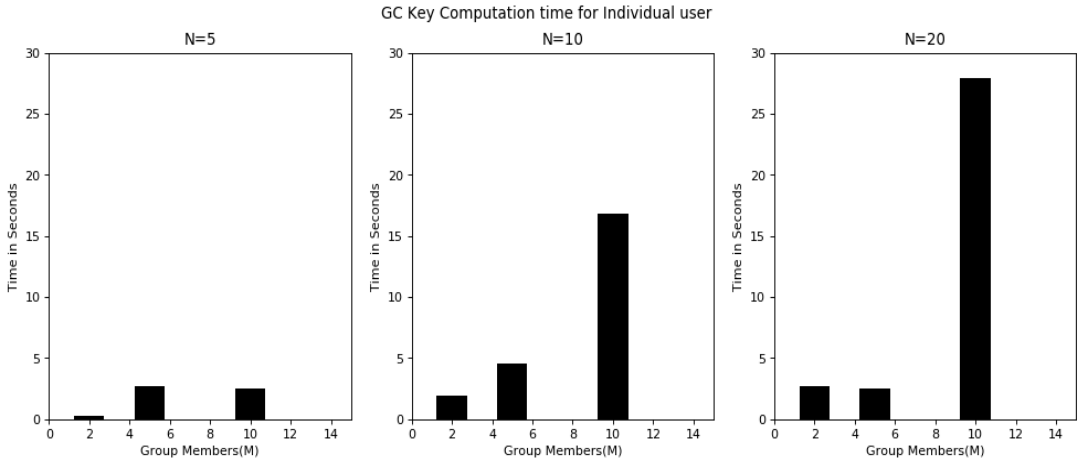

Figure 9. User partial key generation time by the GC.

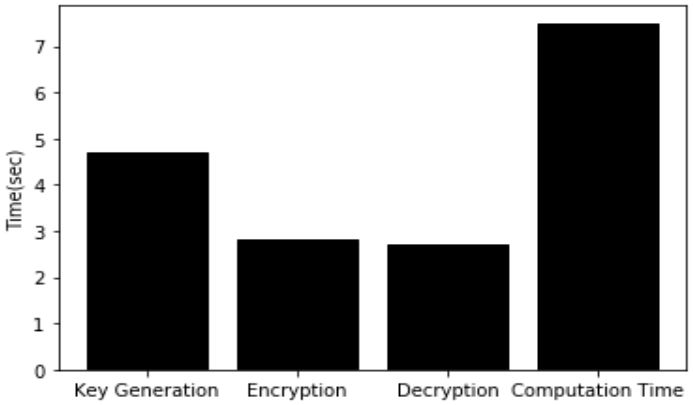

Figure 10. Time complexity of various operations for secure data processing in e-healthcare multi-agent system.

7. Comparative Analysis of Protocols for Securing Multi-Agent-Based e-Healthcare System

The effectiveness of the proposed technique was compared with seven on hand MQKA protocols, namely LGMHW, HSXLFJY, WSH, SYW, SZWYZL and CM. A comparative analysis of MQKA protocols is presented below, and the precise comparative results are shown in Table 8. The features considered for performance comparison includes:

Table 8. Comparative analysis of multiparty QKA (MQKA) protocols.

MQKA Protocol	QE	UO	UOE	SAP	KCC	Entanglement Required
LGMHW [52]	$\frac{1}{N(N-1)}$	no	0	secure	no	no
HSXLFJY [59]	$\frac{1}{2N^2}$	yes	$\frac{1}{N^2}$	secure	no	no
WSH [63]	$\frac{1}{2N(N-1)}$	yes	$\frac{1}{N(N-1)}$	secure	no	no
SYW [58]	$\frac{2}{N(N+4)}$	yes	$\frac{2}{N(N-1)}$	insecure	no	yes
SZWYZL [57]	$\frac{1}{N(2N+3)}$	yes	$\frac{2}{N(2N-1)}$	insecure	no	yes
CM [60]	$\frac{1}{N(N+1)}$	yes	$\frac{2}{N(N+1)}$	secure	no	yes
HUA [64]	$\frac{1}{2N}$	yes	$\frac{1}{2N^2}$	secure	yes	no
Proposed	$\frac{1}{2N}$	yes	$\frac{1}{2N^2}$	secure	yes	yes

N = number of participants.

Qubit efficiency (QE): The qubit effectiveness is characterized as the proportion of the length of the final shared key (nc) foundation in the protocol to the total of the quantity of qubits utilized (q) and number of old style bits exchanged (b) for disentangling the message by barring the traditional correspondence utilized for checking the eavesdropping, Hence, $QE = nc/(q + b)$. Concretely, to build up a L-bit final shared key in perfect state, every one of the included members ought to set up a sequence of $L + kL$ photons, where k is detection rate. In the just one eavesdropping detection, every member will utilize kL photons in his/her groupings for checking spying. Since there are N members associated with the protocol proposed, the total quantity of the photons, which will be utilized in setting up a L-bit final shared key, is $N(L + kL)$. Consequently, the qubit effectiveness of our protocol is, $QE = \frac{L}{N(L+kL)}$.

Measuring Efficiency (ME): As the proposed protocol only requires detection of one eavesdropping, the amount of estimations essential in this protocol is relatively low. In particular, to set up an L-bit final shared key, in theory, each member is required to execute $(L + kL)$ measurements. To be specific, $N(L + kL)$ measurements are required in this whole process of the protocol. Consequently, the ME (the ratio of the length of final shared key to the quantity of the executed measurements) of the protocol is $ME = \frac{L}{N(L+kL)} = \frac{1}{N(1+k)}$.

Unitary operation efficiency (UOE): In view of the fact that the protocol's security is mostly based on the unitary operations executed on the transmitted photons. Here, we compute the UOE as the ratio of the length of final shared key to the quantity of the executed unitary operations of the protocol. Concretely, to set up an L bit final shred key, every member is required to execute $N(L + kL)$ unitary operations in theory. Specifically, $N^2(L + kL)$ unitary operations are required in total. Thus, UOE of our protocol is $UOE = \frac{L}{N^2(L+kL)} = \frac{1}{N^2(1+k)}$.

In addition, in the current MQKAP, after the members affirm that there exists no eavesdropping in the executing method of the protocol—every member straightforwardly utilizes the estimations after the effects of the rest of the quantum data transporters conclude a given binary string as his/her final key.

LGMHW protocol [52]: This protocol is in opposition to against participant attack and does not require entanglement; efficient with QE value $\frac{1}{N(N-1)}$ and UOE is zero.

HSXLFJY protocol [59]: This protocol is secured in opposition to participant attack and does not require entanglement; efficient with QE value $\frac{1}{2N^2}$ and UOE is $\frac{1}{N^2}$.

WSH protocol [63]: This protocol is secured in opposition to participant attack and does not require entanglement; efficient with QE value $\frac{1}{2N(N-1)}$ and UOE is $\frac{1}{N(N-1)}$.

SYW protocol [58]: This protocol is not secured in opposition to participant attack and requires entanglement; efficient with QE value $\frac{2}{N(N+4)}$ and UOE is $\frac{2}{N(N-1)}$.

SZWYZL protocol [57]: This protocol is not secured in opposition to participant attack and requires entanglement; efficient with QE value $\frac{1}{N(2N+3)}$ and UOE is $\frac{2}{N(2N-1)}$.

CM protocol [60]: This protocol is secured in opposition to participant attack and requires entanglement; efficient with QE value $\frac{2}{N(N+1)}$ and UOE is $\frac{2}{N(N+1)}$.

HUA protocol [64]: This protocol is secured in opposition to participant attack and does not require entanglement; efficient with QE value $\frac{1}{2N}$ and UOE is $\frac{1}{2N^2}$.

Proposed protocol: This protocol is secured in opposition to participant attack and requires entanglement; efficient with QE value $\frac{1}{2N}$ and UOE is $\frac{1}{2N^2}$.

8. Conclusions and Future Work

This study has proposed a QDGKA protocol using QDH technique for securing e-healthcare MASs in the context of smart cities against quantum-based attacks. The security provided by the protocol is capable to resist the eavesdropping attacking from internal as well as external participants. We showed that our protocol is secure against participant attack and requires entanglement; efficient with QE value $\frac{1}{2N}$ and UOE is $\frac{1}{2N^2}$. The security of the proposed solution is based on the unconditional security of the QDH. The results in the context of group key agreement among the users in the smart city show the potentiality of the proposed QDGKA in comparison with existing alternatives. Further, the computation complexity of the proposed work is evaluated on doctor's appointment dataset and obtained satisfactory results in executing a multi-agent-based e-healthcare system in a smart city.

As a part of future work, we may further establish formal security model for this dynamic quantum group key agreement, thus council authorities trust these systems to be actually deployed in e-healthcare MASs of smart cities. We also plan to integrate the proposed approach to improve our system for improving mobility and quality of life of visually impaired people [65] for improving the security of this system.

Author Contributions: All the authors designed the idea of applying quantum computing for securing e-healthcare multi-agent system from future computing-based attacks. V.S.N. conceived the overall idea for contributing significantly towards identifying solution to collaborative communication applications by proposing quantum group key agreement. M.M.N. detected how IoT devices communicate through networks. S.R. played a crucial role in implementing proposed quantum group key agreement. I.G.-M. designed the integration of quantum-based security in multi-agent-based coordination. All authors have read and agreed to the published version of the manuscript.

Funding: This work is supported by the research project "Utilization of IoT and sensors in smart cities for improving quality of life of impaired people" with reference 52-2020.

Acknowledgments: V.S.N. would like to thank his great father V. Bala Surya Narayana, family members and Management of Sri Vasavi Engineering College, Tadepalligudem who encouraged and supported me to do this work. Further we all are very much thankful to reviewers and Journal Authorities. Moreover, we acknowledge Prince Sultan University (PSU) and the Renewable Energy Lab for their valuable support and provision of research facilities that were essential for the completion of this work. We also acknowledge "CITIES: Ciudades inteligentes totalmente integrales, eficientes y sotenibles" (ref. 518RT0558) funded by CYTED ("Programa Iberoamericano de ciencia y tecnología para el desarrollo") and "Diseño colaborativo para la promoción del bienestar en ciudades inteligentes inclusivas" (TIN2017-88327-R) funded by the Spanish council of Science, Innovation and Universities from the Spanish Government.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. García-Magariño, I.; Lacuesta, R.; Lloret, J. Agent-Based Simulation of Smart Beds with Internet-of-Things for Exploring Big Data Analytics. *IEEE Access* **2017**, *6*, 366–379. [CrossRef]
2. Gonzalez-Landero, F.; Garcia-Magariño, I.; Amariglio, R.; Lacuesta, R. Smart Cupboard for Assessing Memory in Home Environment. *Sensors* **2019**, *19*, 2552. [CrossRef]
3. Garcia-Magarino, I.; Gonzalez-Landero, F.; Amariglio, R.; Mauri, J.L. Collaboration of Smart IoT Devices Exemplified with Smart Cupboards. *IEEE Access* **2019**, *7*, 9881–9892. [CrossRef]

4. Rayes, I.K.; Hassali, M.A.; Abduelkarem, A.R. Perception of Community Pharmacists Toward Their Current Professional Role in the Healthcare System of Dubai, United Arab Emirates. *Saudi Pharm. J.* **2014**, *23*, 235–240. [CrossRef] [PubMed]
5. Moffatt, J.; Eley, D. The Reported Benefits of Telehealth for Rural Australians. *Aust. Heal. Rev.* **2010**, *34*, 276–281. [CrossRef]
6. Fernández-Alemán, J.L.; Señor, I.C.; Lozoya, P.; Ángel, O.; Toval, A. Security and Privacy in Electronic Health Records: A Systematic Literature Review. *J. Biomed. Informatics* **2013**, *46*, 541–562. [CrossRef] [PubMed]
7. Abd-Elhafiez, W.M.; Reyad, O.; Mofaddel, M.A.; Fathy, M. Image Encryption Algorithm Methodology Based on Multi-Mapping Image Pixel. In *Advances in Intelligent Systems and Computing*; Springer Science and Business Media LLC: Berlin/Heidelberg, Germany, 2019; pp. 645–655.
8. Khan, F. Automated Segmentation of Lung Parenchyma Using Colour Based Fuzzy C-Means Clustering. *J. Electr. Eng. Technol.* **2019**, *14*, 2163–2169. [CrossRef]
9. Manirabona, A.; Fourati, L.C.; Boudjit, S. Investigation on Healthcare Monitoring Systems. *Int. J. E-Health Med. Commun.* **2017**, *8*, 1–18. [CrossRef]
10. Han, S.; Zhao, S.; Li, Q.; Ju, C.H.; Zhou, W. PPM-HDA: Privacy-Preserving and Multifunctional Health Data Aggregation with Fault Tolerance. *IEEE Trans. Inf. Forensics Secur.* **2015**, *11*, 1940–1955. [CrossRef]
11. Tang, J.; Liu, A.; Zhao, M.; Wang, T. An Aggregate Signature Based Trust Routing for Data Gathering in Sensor Networks. *Secur. Commun. Netw.* **2018**, *2018*, 1–30. [CrossRef]
12. Sun, W.; Cai, Z.; Liu, F.; Fang, S.; Wang, G. A Survey of Data Mining Technology on Electronic Medical Records. In Proceedings of the 2017 IEEE 19th International Conference on e-Health Networking, Applications and Services (Healthcom), Dalian, China, 12–15 October 2017; Institute of Electrical and Electronics Engineers: Piscataway, NJ, USA, 2017; pp. 1–6.
13. Chandrasekhar, S.; Ibrahim, A.; Singhal, M. A Novel Access Control Protocol Using Proxy Signatures for Cloud-Based Health Information Exchange. *Comput. Secur.* **2017**, *67*, 73–88. [CrossRef]
14. Bonab, T.H.; Masdari, M. Security attacks in wireless body area networks: Challenges and issues. *Acad. R. Sci. Outre-Mer Bull. Seances* **2015**, *4*, 100–107.
15. Azeez, N.A.; Oluwatosin, A. CyberProtector: Identifying Compromised URLs in Electronic Mails with Bayesian Classification. In Proceedings of the International Conference Computational Science and Computational Intelligence (CSCI), Las Vegas, NV, USA, 15–17 December 2016.
16. MuthamilSelvan, T.; Balamurugan, B. Comparative Performance AnalysisofVariousClassifiersfor Cloud E-HealthUsers. *Int. J. E-Health Med. Commun.* **2019**, *10*, 86–101. [CrossRef]
17. Bennett, C.H.; Brassard, G. Quantum cryptography: Public key distribution and coin tossing. In Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India, 9–12 December 1984; pp. 175–179.
18. Liu, L.; Guo, F.-Z.; Qin, S.-J.; Wen, Q.-Y. Round-Robin Differential-Phase-Shift Quantum Key Distribution with a Passive Decoy State Method. *Sci. Rep.* **2017**, *7*, 42261. [CrossRef] [PubMed]
19. Shih, H.-C.; Lee, K.-C.; Hwang, T. New Efficient Three-Party Quantum Key Distribution Protocols. *IEEE J. Sel. Top. Quantum Electron.* **2009**, *15*, 1602–1606. [CrossRef]
20. Liu, B.; Gao, F.; Wen, Q.-Y. Single-Photon Multiparty Quantum Cryptographic Protocols with Collective Detection. *IEEE J. Quantum Electron.* **2011**, *47*, 1383–1390.
21. Lin, S.; Guo, G.D. Quantum key distribution: Defeating collective noise without reducing efficiency. *Quantum. Inf. Comput.* **2014**, *14*, 845–856.
22. 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. *Sci. Rep.* **2017**, *7*, 2485. [CrossRef]
23. Yang, Y.-H.; Gao, F.; Wu, X.; Qin, S.-J.; Zuo, H.-J.; Wen, Q.-Y. Quantum Secret Sharing via Local Operations and Classical Communication. *Sci. Rep.* **2015**, *5*, 16967. [CrossRef]
24. Yang, Y.-G.; Teng, Y.-W.; Chai, H.-P.; Wen, Q.-Y. Fault-Tolerant Quantum Secret Sharing Against Collective Noise. *Phys. Scr.* **2011**, *83*, 25003. [CrossRef]
25. Song, X.; Liu, Y.-B.; Deng, H.-Y.; Xiao, Y.-G. (t, N) Threshold D-Level Quantum Secret Sharing. *Sci. Rep.* **2017**, *7*, 6366. [CrossRef] [PubMed]
26. Hu, J.-Y.; Yu, B.; Jing, M.-Y.; Xiao, L.-T.; Jia, S.-T.; Qin, G.-Q.; Long, G. Experimental Quantum Secure Direct Communication with Single Photons. *Light. Sci. Appl.* **2016**, *5*, e16144. [CrossRef] [PubMed]

27. 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* **2012**, *21*, 100308. [CrossRef]
28. Yan, F.L.; Zhang, X.Q. A Scheme for Secure Direct Communication Using EPR Pairs and Teleportation. *Eur. Phys. J. B* **2004**, *41*, 75–78. [CrossRef]
29. Lin, S.; Wen, Q.-Y.; Gao, F.; Zhu, F.-C. Quantum Secure Direct Communication with χ-Type Entangled States. *Phys. Rev. A* **2008**, *78*, 064304. [CrossRef]
30. Ekert, A.K. Quantum cryptography based on Bellâs theorem. *Phys. Rev. Lett.* **1991**, *67*, 661–663. [CrossRef]
31. Bennett, C.H. Quantum cryptography using any two non-orthogonal states. *Phys. Rev. Lett.* **1992**, *68*, 3121–3124. [CrossRef]
32. Nguyen, B.A. Quantum Dialogue. *Phys. Lett. A* **2004**, *328*, 6–10. [CrossRef]
33. Gao, F.; Qin, S.-J.; Wen, Q.-Y.; Zhu, F.-C. An Effective Attack on the Quantum Key Distribution Protocol Based on Quantum Encryption. *Comput. Vis.* **2005**, *3822*, 302–312.
34. Jin, X.R.; Ji, X.; Zhang, Y.-Q.; Zhang, S.; Hong, S.-K.; Yeon, K.-H.; Um, C.-I. Three-Party Quantum Secure Direct Communication Based on GHZ States. *Phys. Lett. A* **2006**, *354*, 67–70. [CrossRef]
35. Deng, F.-G.; Zhou, P.; Li, X.-H.; Zhou, C.-Y. Efficient multiparty quantum secret sharing with Greenberger-Horne-Zeilinger states. *Chin. Phys. Lett.* **2006**, *23*, 1084–1087.
36. Zhang, W.; Ding, D.; Sheng, Y.; Zhou, L.; Shi, B.-S.; Guo, G.-C. Quantum Secure Direct Communication with Quantum Memory. *Phys. Rev. Lett.* **2017**, *118*, 220501. [CrossRef] [PubMed]
37. 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. *Comput. J.* **2012**, *56*, 1167–1175. [CrossRef]
38. Hwang, T.; Hwang, C.-C.; Li, C.-M. Multiparty Quantum Secret Sharing Based on GHZ States. *Phys. Scr.* **2011**, *83*, 45004. [CrossRef]
39. Jia, H.-Y.; Wen, Q.-Y.; Gao, F.; Qin, S.-J.; Guo, F.-Z. Dynamic Quantum Secret Sharing. *Phys. Lett. A* **2012**, *376*, 1035–1041. [CrossRef]
40. Liao, C.-H.; Yang, C.-W.; Hwang, T. Dynamic Quantum Secret Sharing Protocol Based on GHZ State. *Quantum Inf. Process.* **2014**, *13*, 1907–1916. [CrossRef]
41. Hsu, J.-L.; Chong, S.-K.; Hwang, T.; Tsai, C.-W. Dynamic quantum secret sharing. *Quantum Inf. Process.* **2013**, *12*, 331–344. [CrossRef]
42. Liu, H.; Ma, H.; Wei, K.; Yang, X.; Qu, W.; Dou, T.; Chen, Y.; Li, R.; Zhu, W. Multi-Group Dynamic Quantum Secret Sharing with Single Photons. *Phys. Lett. A* **2016**, *380*, 2349–2353. [CrossRef]
43. Liu, W.-J.; Chen, Z.-Y.; Ji, S.; Wang, H.-B.; Zhang, J. Multi-Party Semi-Quantum Key Agreement with Delegating Quantum Computation. *Int. J. Theor. Phys.* **2017**, *56*, 3164–3174. [CrossRef]
44. Cai, B.; Guo, G.; Lin, S.; Zuo, H.; Yu, C. Multipartite Quantum Key Agreement Over Collective Noise Channels. *IEEE Photon J.* **2018**, *10*, 1–11. [CrossRef]
45. He, W.T.; Wang, J.; Zhang, T.T.; Alzahrani, F.; Hobiny, A.; Alsaedi, A.; Hayat, T.; Deng, F.G. High-efficiency three-party quantum key agreement protocol with quantum dense coding and bell states. *Int. J. Theor. Phys.* **2019**, *58*, 2834–2846. [CrossRef]
46. Sun, Z.; Wu, C.; Zheng, S.; Zhang, C. Efficient Multiparty Quantum Key Agreement with a Single d -Level Quantum System Secure Against Collusive Attack. *IEEE Access* **2019**, *7*, 102377–102385. [CrossRef]
47. Yin, X.-R.; Ma, W.-P.; Liu, W.-Y. Three-Party Quantum Key Agreement with Two-Photon Entanglement. *Int. J. Theor. Phys.* **2013**, *52*, 3915–3921. [CrossRef]
48. Yin, X.R.; Ma, W.P.; Shen, D.S.; Wang, L. Three-party quantum key agreement with bell states. *Acta Phys. Sinica* **2013**, *62*, 17.
49. Shukla, C.; Alam, N.; Pathak, A. Protocols of Quantum Key Agreement Solely Using Bell States and Bell Measurement. *Quantum Inf. Process.* **2014**, *13*, 2391–2405. [CrossRef]
50. 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 Inf. Process.* **2015**, *14*, 4245–4254. [CrossRef]
51. Shi, R.-H.; Zhong, H. Multi-Party Quantum Key Agreement with Bell States and Bell Measurements. *Quantum Inf. Process.* **2012**, *12*, 921–932. [CrossRef]
52. Liu, B.; Gao, F.; Huang, W.; Wen, Q. Multiparty quantum key agreement with single particles. *Quantum Inf. Process.* **2013**, *12*, 1797–1805. [CrossRef]
53. Sun, Z.; Zhang, C.; Wang, B.; Li, Q.; Long, D. Improvements on "multiparty Quantum Key Agreement with Single particles". *Quantum Inf. Process.* **2013**, *12*, 3411–3420. [CrossRef]

54. Huang, W.; Wen, Q.-Y.; Liu, B.; Su, Q.; Gao, F. Cryptanalysis of a Multi-Party Quantum Key Agreement Protocol with Single Particles. *Quantum Inf. Process.* **2014**, *13*, 1651–1657. [CrossRef]
55. Xu, G.-B.; Wen, Q.-Y.; Gao, F.; Qin, S.-J. Novel Multiparty Quantum Key Agreement Protocol with GHZ States. *Quantum Inf. Process.* **2014**, *13*, 2587–2594. [CrossRef]
56. Sun, Z.; Huang, J.; Wang, P. Efficient multiparty quantum key agreement protocol based on commutative encryption. *Quantum Inf. Process* **2016**, *15*, 2101–2111. [CrossRef]
57. Sun, Z.; Zhang, C.; Wang, P.; Yu, J.; Zhang, Y.; Long, D. Multi-Party Quantum Key Agreement by an Entangled Six-Qubit State. *Int. J. Theor. Phys.* **2015**, *55*, 1920–1929. [CrossRef]
58. Sun, Z.; Yu, J.; Wang, P. Efficient Multi-Party Quantum Key Agreement by Cluster States. *Quantum Inf. Process.* **2015**, *15*, 373–384. [CrossRef]
59. Huang, W.; Liu, B.; Fan, F.; Su, Q.; Jia, H.; Yang, Y.; Xu, B. Improved Multiparty Quantum Key Agreement in Travelling Mode. *Sci. China Ser. G Phys. Mech. Astron.* **2016**, *59*, 120311. [CrossRef]
60. Cao, H.; Ma, W. Multiparty Quantum Key Agreement Based on Quantum Search Algorithm. *Sci. Rep.* **2017**, *7*, 45046. [CrossRef] [PubMed]
61. 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* **2016**, arXiv:1602.00832.
62. Medical Appointment No Shows. Available online: https://www.kaggle.com/joniarroba/noshowappointments (accessed on 21 August 2017).
63. Wang, P.; Sun, Z.; Sun, X. Multi-Party Quantum Key Agreement Protocol Secure Against Collusion Attacks. *Quantum Inf. Process.* **2017**, *16*, 170. [CrossRef]
64. Huang, W.; Su, Q.; Liu, B.; He, Y.-H.; Fan, F.; Xu, B.-J. Efficient Multiparty Quantum Key Agreement with Collective Detection. *Sci. Rep.* **2017**, *7*, 15264. [CrossRef] [PubMed]
65. Sobnath, D.; Rehman, I.U.; Nasralla, M.M. Smart Cities to Improve Mobility and Quality of Life of the Visually Impaired. In *Trends in Cloud-based IoT*; Springer Science and Business Media LLC: Berlin/Heidelberg, Germany, 2019; pp. 3–28.