Wireless Personal Communications
https://doi.org/10.1007/s11277-023-10587-x

Design of Quantum Communication Protocols in Quantum Cryptography

Bilal A. Alhayani[1] · Omar A. AlKawak[2] · Hemant B. Mahajan[3] · Haci Ilhan[1] · Roa'a Mohammed Qasem[4]

Accepted: 30 June 2023

Abstract
Secure communication has developed into one of the most promising disciplines in the contemporary world. This is a highly essential subject for every business and body, and its advancements are increasing significantly. Quantum computing is becoming an increasingly popular kind of contemporary computing. This type of computing makes advantage of the fundamental characteristics of quantum mechanics to process information. Certain of the problems that were present in classical computing, such as the factoring discrete logarithm problem, have already been addressed by some writers in the field of quantum computing QC. Another significant challenge faced by conventional computing is one related to security, which may now be addressed thanks to quantum cryptography protocols. However, researchers have recently shown that even quantum encryption may be vulnerable to hacking. Implementing protocols for quantum cryptography still comes with a number of significant challenges, the most significant of which being quantum bit errors.

Keywords Quantum communication · Quantum cryptography · Physical sciences

1 Introduction

In this modern era, all computing systems, stored data, and communication devices regularly face cyber attacks all over the world. The hackers could steal and store the encrypted data containing important information about policies of government institutions and other organizations to decrypt them later using powerful machines for their benefits. The limitations of conventional computers in addressing various problems necessitate the requirement of better technologies.

✉ Bilal A. Alhayani
bilalalhayani1@gmail.com

[1] Department of Electronics and Communication, Yildiz Technical University, Istanbul, Turkey

[2] Department of Energy Engineering, College of Engineering, Al-Mussaib, University of Babylon, Hillah, Babil, Iraq

[3] Godwit Technologies, Pune, India

[4] Department of Electrical and Computer Engineering, Altinbas University, 34218 Istanbul, Turkey

Published online: 18 July 2023

The first problem with current computing technology is its limit on miniaturization. It cannot be controlled precisely below a specific size, which ultimately leads to a computational speed limit. It is called Moore's law [1]. At present, the latest Intel processor contains over a billion transistors squeezed into a small area, with each component separated by a distance of few nanometres. The extrapolation of this growth in time shows that soon, this technology would reach a separation of a few atom thicknesses. Then further scaling down will cause quantum tunnelling effect to occur, which results in gate leakage, causing a catastrophic loss of information. Thus, the emergence of this quantum phenomenon leads to an inescapable computational speed limit for the current technology. This problem necessitates an alternative technology that works successfully at quantum levels.

The second problem is with the security features of the current communication technology. Almost all secure communications such as bank transactions to the virtual private network (VPN) uses Rivest–Shamir–Adleman (RSA) protocol [2], the security of which relies on the unavailability of an efficient classical factorization algorithm. However, in 1994, Peter Shor announced his quantum algorithm for factoring large numbers [3] with an efficiencies unparalleled by any classical algorithm preceding it. It makes use of the quantum phase estimation technique to arrive at the desired output. In the future, a fully developed quantum computer with the capability of implementing Short's algorithm can factorize large numbers into their prime factors within polynomial time. This will certainly challenge the current encryption methods.

The next major problem with current computing technology is its in-efficiencies in simulating quantum mechanical systems. A classical computer would require an exponential amount of memory to simulate a quantum many-body system, which results in prolonged processing. Meanwhile, quantum computers can efficient simulate the same within polynomial time. In 1982, Richard Feynman [4] first predicted the capability of quantum computers in performing an efficient simulation of quantum systems over classical computers. Quantum simulation of chemical reactions and finding more efficient materials for deferent purposes could save time and money spent on the preparation and characterization of a few random materials done manually with great Effort.

Our conventional technology fails to address problems such as secure communication, faster computation, and efficient methods to process enormous data. Even though there exist several computing methods, the concept of computation using the properties of quantum mechanics seems to be a promising candidate in fulfilling the above requirements. In the last three decades, the field of quantum computation and quantum information has emerged as a very significant and rapidly developing area of research.

In 1985, David Deutsch proposed the first quantum algorithm [5] to showcase the quantum advantage over classical algorithms. In [6] published a quantum algorithm that finds a given item from an unsorted finite database faster than any classical algorithm. Grover's algorithm makes use of the amplitude amplification technique to achieve the desired output state. With the discovery of new quantum algorithms, this technology could theoretically solve tougher problems faster than any conventional computer. However, in practice, it is challenging to implement these quantum algorithms in the real noisy quantum computers available today. Apart from quantum algorithms, there are other interesting applications like quantum communication [7], quantum cryptography [8], quantum metrology [9] and quantum artificial intelligence [10]. With sufficient advancements, exploration of fundamental physics is possible through efficient simulation of the fundamental particles [11]; study the quantum nature of exotic objects like black holes and early universe [12]. All this progress could bring a paradigm shift in information towards a quantum age.

Most of this thesis is focused on developing new quantum communication and cryptographic protocols. In the subsequent sections, a brief introduction to the fundamental components of quantum computation like Qubits, quantum gates, and the quantum circuit model is given [13].

For the laws of quantum mechanics to be beneficial for computational purposes, the quantum mechanical computing system we develop should be able to prepare the initial states with high fidelity. Then we must be able to perform desired operations, manipulate and control those states perfectly. Finally, the desired output state must readout through measurement operation. However, the measurement outcome is inherently probabilistic in quantum mechanics. Hence this process must be repeated several times to get the output state.

Quantum bits or Qubits are the quantum version of bits in classical computation. This is the fundamental unit of information in quantum computation. The term 'Qubit' was coined by Benjamin Schumacher in 1995 [14]. Just like a classical bit can take 0 and 1, the Qubits, which is a two-level system (TLS), can exist in states j0i and j1i. The states fj0i; j1ig represented in Dirac's bracket notation, are the computational basis kits in the two-dimensional Hilbert space. Polarization states of photons, electron spin, nuclear spin, atoms trapped in optical lattices, Josephson junction etc. are used to realize Qubits experimentally.

Another significant entity in any computation process is information processing or manipulation of data stored in registers. Just like logic gates in classical computation, quantum logic gates are used to manipulate data or quantum state stored in quantum registers. A quantum logic gate acts on Qubit to change its state. For n particle state, the quantum gate is represented by a 2^n unitary matrix [15]. This study is arranged as follows: in part 2, a description of the literature review; in Sect. 3, a description of the research technique; in Sect. 4, an analysis of the results and discussion; and in Sect. 5, a description of the final conclusion and future work.

2 Literature Review

Literature review in respect of Study of Design of Quantum Communication Protocols in Quantum Cryptography has been given.

In the first study, authors [16] demonstrated that it is feasible to carry out probabilistic teleportation of a generic three-particle GHZ state using three Bell pairs that are not maximally entangled. Earlier research demonstrates that the perfect teleportation of any arbitrary three-particle state is realisable via the use of a really entangled six-qubit state as well as through the use of three different sets of W-class states.

While [17] used a five-Qubit entanglement channel and five-particle joint measurement [18], utilised three sets of four-Qubit cluster states to accomplish the identical quantum job. It can be seen from the quantum cost of these plans that their efficiency is not on par with that of the other programmes.

In the paper [18], a four-qubit cluster state is used as an entanglement channel. The authors successfully lowered the quantum cost of the job by only requiring two Bell measurements to finish it. In our first technique, which is denoted by the letter PP1 in the table, we did the same thing by using four-particle joint measurements. However, our second technique (PP2) illustrates that by employing two Bell pairs and two Bell measurements, the QC for this work may be reduced by an additional two units, bringing the total number of QC units down to four.

In [19], a technique was developed that calls for a N + 1 W-class state to be used as an entanglement channel. However, the need of multipartite entanglement channels presents an experimental obstacle in the process of putting these methods into practise. After then, a large number of other plans were suggested in order to complete the same quantum job while using less entanglement resources.

In [20], a comprehensive assessment of the experimental obstacles that must be overcome in a variety of quantum systems in order to achieve full Bell detection is presented. The teleportation method used in this approach may either be probabilistic or deterministic, depending on how well the detection system works. As a result, in order to put the suggested plan into action, you will need a quantum system with a Bell detection efficiency of one hundred percent.

It was shown in [21] that both of them are technically distinct from one another. Even if the quantum cost of each of these strategies is the same, our strategy is experimentally more practical than others owing to the fact that our method is uncomplicated and uncomplicated, and because it provides for the possibility of a speedup as a result of a decrease in the circuit depth. Additionally, we discovered that the quantum cost of our method for all N-particle generalised Bell-type states is equal to 3N plus 1.

A modified measure of efficiency was presented in [22]. This metric takes into account the decoy Qubits that are employed for eavesdrop checking.

In [23] 'Alternative 3', there are differences between the two. We perform a two-stage eavesdrops checking. Anyone of the users (Alice or Bob) initiates the first eavesdrop checking by randomly selecting the Qubits and the receiver's performance of a unitary operation on his sequence before the encoding of the message gives the protocol enhanced security. Here, we also present the generalization of our protocol to N number of controllers using sets of GHZ-like states.

The ballots in this protocol, which are states that are entangled, move just once while the operation is being carried out in [24]. When the secure entanglement channels have been set up, the voters will be able to cast their ballots knowing that their votes are completely safe.

Using the BB84 protocol, the author of [25] proposes a terrestrial relay-assisted approach for a free-space quantum key distribution (QKD) system. In addition, the results of many experiments have shown that the relay-assisted proposal is superior than the direct point-to-point transmission scheme when used to long link ranges, which are characterised by especially degrading turbulence effects.

The author of [26] spoke about the security analysis of two different three-party quantum key distribution techniques (QKDPs). The dense-coding attack might easily penetrate these protocols because of their weakness. It was discovered that the eavesdropper Eve was able to get the session key by sending entangled Qubits to Alice in the form of a bogus signal and then doing combined measurements in a manner that followed Alice's encoding. The procedure of the assault was very much like that of a dense-coding conversation that took place between Eve and Alice. In addition to the information that was delivered, this assault did not cause any faults, which Alice and Bob did not find out about. At long last, the source of such ambiguity as well as a potential approach to the development of these protocols were explained in their paper.

The author of [27] discusses the risk assessment of two different three-party quantum key distribution techniques (QKDPs). The dense-coding attack might easily penetrate these protocols because of their weakness. It was discovered that the eavesdropper Eve was able to get the session key by sending entangled Qubits to Alice in the form of a bogus signal and then doing combined measurements in a manner that followed Alice's encoding. The procedure of the assault was very much like that of a dense-coding conversation that took place between Eve and Alice.

The author of [28] reported the cryptanalysis of a four party quantum key distribution technique that included a collective eavesdropping-check. This approach was used to prevent eavesdropping. Eavesdropping is possible in the QSS protocol since there are dishonest agents included in the protocol. This eavesdropping does not result in any errors being introduced into Alice's secret messages.

Both the implicit quantum key distribution protocol (3AQKDP) and the explicit quantum key distribution protocol are grouped together in the system that the author proposes in [29]. (3AQKDPMA). Establishing a secure connection between the two parties allows for the prevention of attacks such as eavesdropping, man-in-the-middle, and replay. Because of their strategy, the number of communication cycles has been cut down. This is because both types of cryptography have the capacity to detect the presence of hidden information.

The author of [30] discusses a quantum authenticated key distribution mechanism that may be used to carry out key allocation. In addition to this, it is created to guarantee that the communicators involved in the exchange have been verified both tacitly and explicitly. Participants in their protocol are reliant on a third party only for the authentication phase of the process.

Using four non-orthogonal two-particle entangled states, [31] presented a protocol for multi-party quantum secret sharing. This protocol would allow for the sharing of the secret. The new technique achieves theoretical efficiency for qubits that are far higher than 50%, getting close to 100%. The entangled states may be used to generate the private key, with the exception of the entangled states that are needed to check for the presence of an eavesdropper. The quantum assault on this form of protocol, which is known as an opaque cheat attack, is taken into consideration and contrasted with the quantum key distribution.

In the paper [32], the authors offer a novel method for communicating quantum secrets that only requires one non-entangled Qubit. A sender is able to safely broadcast a secret message to N receivers using this approach by consecutively transferring a qubit from one party to the next. These receivers are only able to decrypt the message by working together after randomly shuffling the polarisation of the qubit. Also discussed was the fact that the quantum secret sharing scheme was based on the one between a sender and two receivers, but that it could be generalised to work with any number of recipients. Since the system is able to use a very weak coherent pulse as a qubit, it is theoretically possible to implement it using the technology that is already available.

The genetic algorithm and the quantum genetic algorithm were both discussed in [33]. Both algorithms have been put through their paces with 25 separate runs and 500 generations of iteration each. The global complexity of QGA may be described as of the order of O (N), where N is the population size. The level of complexity required for a GA is on the order of O. (N 2). Because of this, the complexity has been simplified into a linear form.

Quantum Inspired Cuckoo Search Algorithm was the name given to a novel inspired algorithm that was introduced in [34]. (QICSA). The Cuckoo Search method and the fundamentals of quantum computing serve as the foundation for this QICSA. This method is able to solve effectively the combinatorial optimization problems by using some of the concepts of quantum computing, such as the representation of qubits, measurement of qubits, superposition of states, and interference. The combination of quantum computing with biological computing has led to the development of an effective hybrid framework that provides a better balance between the exploratory and exploitative capacities of the search process. The efficacy of the suggested framework, as shown by the experimental results on the knapsack issue, as well as its capacity to provide solutions of a high quality.

In the paper [35], the authors propose two different optimization algorithms: the first, cuckoo optimization, is a heuristic method, and the second, the genetic algorithm, is a meta-heuristic method [36]. Their goal is to maximise both the level of optimization achieved and the speed with which calculations can be performed. The suggested approach and technique are still open to modifications and adjustments that will allow for an ever-increasing rate of acceleration [37]. The method that has been proposed can be used in a variety of industrial fields, agricultural fields, and other fields as long as they have an optimization problem; all that is required is to reconfigure the problem parameters, and then they will have a good opportunity to optimise the problem effectively.

3 Research Methodology

Quantum cryptography is a technique that involves the use of the laws of quantum mechanics to enable the parties involved to exchange random strings of qubits with one another. These qubits may be used as a key to encrypt and decode messages that are being sent between the parties.

The structure of the quantum cryptosystem, which makes use of two primary channels of communication and is shown in Fig. 1, is shown here. The first method is known as the quantum channel, and its purpose is to send and receive quantum bits in addition to producing the session key. The open channel is the second option, and it is the one that the sender and the receiver use to determine whether or not their quantum bits are being intercepted. Both the transmitter and the receiver use their session key to encrypt the plain text and decode the cypher text, which secures their communication between the two parties. The distribution of keys is the key to ensuring the integrity of a quantum cryptosystem's system. Once an eavesdropper acquires the quantum bits that are needed to assemble the session key, there is a change in the quantum state of the system. As a result, the eavesdropper is now able to be identified. As a result, the direction that quantum cryptology is heading in is towards a Quantum Secret Sharing (QSS) Protocol that is both practical and effective.

3.1 Quantum Key Distribution

Quantum key distribution, often known as QKD, is a protocol that uses the basic rules of quantum physics to ensure that all communications are kept private. It makes it possible for two authorised users, who are often referred to as Alice and Bob, to generate a shared secret random bit string that may be used as a key in cryptographic applications such as message encryption (for example, the one-time pad) and authentication. QKD guarantees unconditional security based on the basic rules of quantum physics, in contrast to the security that is provided by conventional encryption, which is only dependent on untested computational assumptions.

A quantum channel is required for QKD in order to communicate the polarisation bases, whereas a classical channel is required in order to exchange the secret key. Fortunately, in the realm of classical cryptography, there are safe authentication systems

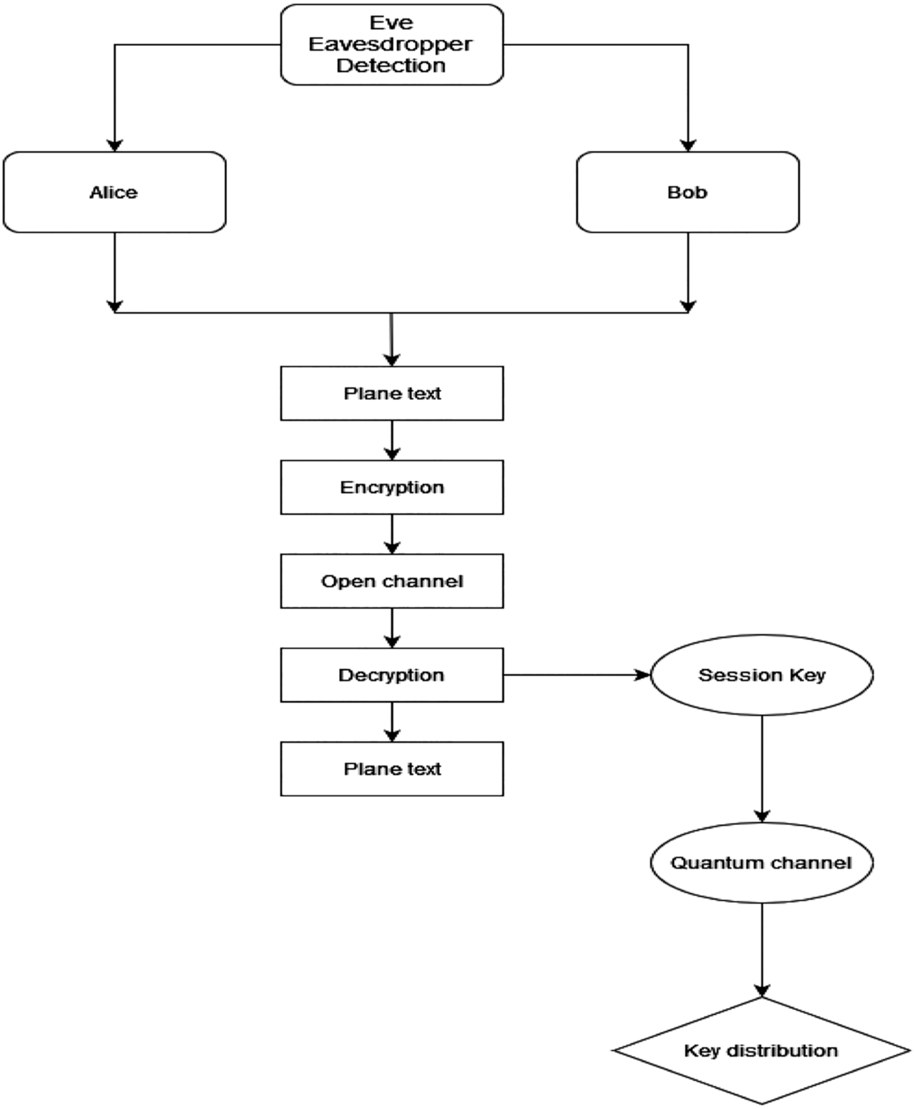

Fig. 1 Flowchart of quantum cryptosystem

like the Wigman-Carter authentication scheme that may be used. Additionally, the efficiency of these unconditionally protected authentication techniques should not be overlooked. Only O (log N) bits of the shared key are required in order to authenticate an N-bit communication. The objective of QKD is not key distribution but rather key growth due to the fact that just a minimal quantity of pre-shared secure bits is required for communication between Alice and Bob. As a result, QKD offers a fundamental answer to an issue that has hitherto been hard to solve.

3.2 Quantum Cryptographic Properties

3.2.1 Quantum Superposition

A probabilistic wave function, also known as the Schrodinger equation, is used to explain a quantum. This function indicates the probability of finding the quantum in a specific location, but it does not reveal the quantum's precise location. In the absence of an observer, a quantum may be in any one of its many conceivable states, but the phenomenon known as quantum superposition describes how it can exist in all of those states at the same time.

3.2.2 Heisenberg's Uncertainty Principle

The observation of quantum phenomena is further complicated by the fact that when measuring the location of a quantum, we are unable to determine the precise velocity of the quantum, and vice versa: when measuring the velocity of a photon, we are unable to determine the exact position of the photon (Strictly speaking, it is the momentum which is the property under consideration here.)

3.2.3 Quantum Entanglement

Quantum entanglement is a phenomena that is known as “spooky activity at a distance,” and it is a strange quantum trait that has importance to Quantum Key Distribution. As a result of the research conducted by Einstein, Podolsk, and Rosen on the phenomena, it is possible to generate pairs of quanta that exhibit behaviour consistent with that of a single entity. These pairings are referred to as EPR pairs. For instance, quanta have a feature that is referred to as "spin." One quantum may have spin up, while the other could have spin down, resulting in a total spin value of zero; nevertheless, until a measurement is done, it is not evident which of the two pairs of quanta is which. When just one member of the pair is measured, the result is that the wave function of the other member collapses into the opposite state. It would seem that it is aware instantly that its partner has been measured, which would appear to violate Einstein's discovery that nothing can move faster than light. The Einstein-Podolsk-Rosen (EPR) paradox is the name given to this conundrum, and it has never been satisfactorily answered. It has been hypothesised that this peculiar quantum behaviour may be employed in teleportation in the manner of Star Trek; however, the original item would be destroyed in the process, which is a rather regrettable side consequence.

3.3 Problem Identification

Some of the problems that have plagued conventional computing, such as factoring and the discrete logarithm problem, have been resolved in quantum computing thanks to the work of Peter Shor and Lov Grover. Another significant difficulty with classical computing is its lack of built-in security, which has been addressed by the development of quantum cryptography protocols. In spite of this, researchers have recently shown that even quantum encryption can be broken via a process called quantum hacking. Quantum bit errors are the most obvious issue that arises when attempting to implement quantum cryptography protocols; yet, there are still significant challenges connected with doing so. As a result, the emphasis of this body of work is on doing an analysis of the security of multiparty communication with regards to performance characteristics such as calculation time and error rate.

3.4 Methodology

Quantum Secret Sharing, often known as QSS, is an essential part of the field of quantum cryptography, which brings together quantum mechanics and traditional encryption. QSS is one of the most significant areas of quantum cryptography. In the course of this piece of study, efficient cryptographic approaches have been applied in order to provide a solution to a variety of assaults, including the heuristic attack and the intercept and resend attack.

- Quantum key distribution combined with heuristic assault.
- Elliptic Curve Cryptography with Heuristic Attack-Based Question and Answer Security System
- Heuristic attack based on hyper elliptic curve cryptography with QSS
- Hyperelliptic curve cryptography with intercept and resend attack based question and answer security system (QSS).

3.4.1 Quantum Secret Sharing with Heuristic Attack

By producing the pairings in the entangled state, this analysis makes it possible for the protocol to exchange quantum state information with the parties involved. Additionally, it allows the resilience of the protocol to be evaluated. The resilience of the system is determined by producing heuristic assaults using various heuristic algorithms, such as the genetic algorithm, cuckoo, and Tabu search algorithm. The implementation of quantum key distribution among four parties is shown here. The efficiency of this method of quantum secret sharing may be shown in terms of the overall time, the length of time required for encryption, the mistake rate, and the amount of time required for decryption. This was broken down into three stages: the QSS protocol, a heuristic attack, and an examination of the QSS protocol. These three processes are carried out in sequential order, after which the information on the quantum state is sent more efficiently.

3.4.2 Elliptic Curve Cryptography with Heuristic Attack Based QSS

Sharing of quantum state information among the parties involved in the quantum system via the Four party QSS protocol, which results in a lack of security in the process, In order to solve the security issue, a brand new elliptic curve cryptography-based QSS approach that requires the participation of four parties has been presented.

3.4.3 Hyper Elliptic Curve Cryptography with Heuristic Attack Based QSS

"Existing techniques of security, such as elliptic curve encryption, are implemented in each of the four QSS protocols. Cryptography based on elliptic curves is difficult to implement in real-time applications, and it is also challenging to determine whether or not an existing implementation is valid. ECC-based QSS has a lower mistake rate when compared to four-party QSS, but it does not provide the same level of security information. It has been suggested to use hyper elliptic curve encryption as a solution to this constraint. Evaluation of two-, three-, and four-party quantum secret sharing using hyper elliptic curve cryptography is performed based on total time, encryption time, error rate, and decryption time.”

3.5 Quantum Secret Sharing with Heuristic Attack

3.5.1 Attack Generation by Quantum Inspired Genetic Algorithm (QIGA)

Genetic algorithms, often known as GAs, are a kind of heuristic search algorithm that is adaptable and is based on the evolutionary concepts of natural selection and genetics. As such, they constitute an astute use of a method known as random search, which is applied in order to resolve optimization issues. GAs use previous knowledge to lead the search towards the part of the search space that has superior performance, despite the fact that they are randomised. This implies that GAs are not random, despite the fact that they are randomised.

For the purpose of finding a solution to a problem, GAs act as a simulation of the survival of the fittest among people over the course of many generations. Each generation is made up of a population of character strings that function in a manner very similar to that of chromosomes. Every person in the room stands in for a point in the search area as well as a potential answer. After then, an evolutionary process is forced onto the population’s members in order to bring about change. The heuristic attack that will be used to analyse the QSS protocol will be produced via the exploitation of GA. The following is a description of each step involved in the process of using a QSS protocol analyzer with a GA attack:

Algorithm 1:

- *Step 1* In the first step of the process, you will generate random solutions of chromosomes in the form of a matrix that is as close to the solutions found for Bob, Charlie, and David as possible.
- *Step 2* Determine the effectiveness of the fitness function by using the formula that is shown in Equation.
- *Step 3* In the third and final step, genetic operations such as crossover and mutation are carried out in order to develop new potential solutions. In this section, the single point crossover and mutation processes will be carried out.
- *Step 4* The procedure is repeated as many times as necessary until the maximum number of possible iterations is achieved.

After that, we determine the minimal error rate that was indicated in the equation.

$$\xi =_{M_e}^{argE_{rmin}:<\lambda} \tag{1}$$

“If ξ is the observation random variable, M_e ◌ृ is the parameter used for the minimization of error, which is used as an argument here. $argE_{rmin}$ And λ is the minimum error rate and threshold rate value respectively.”

3.5.2 Attack Generation by Quantum Inspired Tabu Search Algorithm (QITSA)

“Tabu search, sometimes known as TS, is an iterative process developed for the purpose of finding optimal solutions to optimization issues. It is used to the resolution of a broad variety of challenging optimization issues, including job shop scheduling, graph colouring (which is related), the Traveling Salesman Problem (TSP), and the capacitated arc routing problem.”

The Tabu search method begins by producing an initial solution to be used as input. This solution is then passed on to the Adaptive Memory Procedure, also known as AMP.

During each each iteration, tours are chosen from the AMP in a biassed way to design a new solution. This process is known as iteration. In an effort to avoid reaching the minimum value, non-Tabu viable alternatives are produced. Intensification and diversification are two memory-based methods that comprise an essential part of the TS core concept. When using the Intensification approach, areas close to appealing solutions are explored in depth. This technique normally works by beginning a new search from a solution that has already been determined to provide satisfactory results. The following paragraphs detail the steps involved in doing QSS assessments using a TS-based heuristic attack:

Algorithm 2

Step 1 Initial solution is generated as heuristic attacker and tours are added to the Adaptive Memory Procedure in Step 1. (AMP).

Step 2 Assess the fitness function using the Bell state measurement to determine the error rate.

Step 3 In order to design new solutions, iterations will choose tours from the AMP in a biassed way and use those tours as their starting point.

Step 4 For the newly created solutions, repeat step 2, as described above.

Step 5 The newly produced solution will be included to the Tabu list if the error rate assessed in Step 4 is lower than the error rate evaluated in Step 2. If this is not the case, the proposed remedy will be abandoned.

Step 6 The iteration process is continued at this point to determine the minimal error rate based on Eq. 2.

$$E_{rmin} = \frac{\sum_{m=0}^{M}(M_a - M_e)}{M} \tag{2}$$

3.5.3 Attack Generation by Quantum Inspired Cuckoo Search Algorithm (QICSA)

“In the strategy game known as cuckoo search (CS), each egg in a nest stands for a different solution, and a cuckoo egg stands for an additional solution. The goal is to employ the new and possibly superior solutions (cuckoos) to replace a solution that is not doing very well in the nests. In its most basic form, each nest contains a single egg. The technique may be modified to work with scenarios that are more complex, such as those in which each nest contains many eggs that each represent a different set of answers. The following is a description of the technique for doing QSS analysis using CSA as the heuristic attack:”

Algorithm 3

- *Step 1* Consider the objective function to have a threshold error rate of () as the first step.
- *Step 2* The second step is to construct the first population as a solution that is developed as an attacker using heuristics.
- *Step 3* Carry out an assessment of the error rate using the Bell state measurement.
- *Step 4* Perform Levy flights to create fresh solutions and assess the fitness function as the fourth step in the process.
- *Step 5* The iteration process will continue till.
- *Step 6*Find the error rate probability factor, denoted by the notation [0, 1].

"Evaluation allows for the identification of the best solutions with the lowest possible error rate. Eavesdropper Eve does not exist if the evaluated error rate does not exceed the threshold function, which is denoted by the symbol and can be found in Eq. 3. If this is not the case, the communication has been compromised."

$$\mathrm{E_r} = \mathrm{M_a} - \mathrm{M_e}, \tag{3}$$

$\mathrm{M_a}$-Matrix generated by Alice; $\mathrm{M_{e-}}$Matrix generated by eavesdropper.

4 Results and Discussion

To determine how secure the information exchange is, this four-party QSS protocol generates various heuristic attacks with the names QIGA, QITSA, and QICSA. The calculation of the average error rate, the calculation of the error rate deviation, the calculation of the average computational time, and the calculation of the time deviation are all done and tabulated below in this part.

It is clear from looking at Tables 1 and 2 which approach achieves better results while using less computing time and carrying out a greater number of repetitions. Also, the transmission must be determined to have a minimum error rate that is lower than the threshold value in order for it to be considered secure. If this is not the case, the information may have been compromised by an eavesdropper. During this investigation, heuristic attacks are formulated in order to do cryptanalysis. This might be accomplished by the use of the Matrix creation of the heuristic assaults. Changing the matrix size under 10 separate tests allows for an evaluation of the suggested system's performance, after which the findings are compared to the QIGA, QITSA, and QICSA. The results for each of the conditions are

Table 1 Average error rate and average computation time

Iterations	Average error rate			Average consumption time (sec)		
	QIGA	QICSA	QITSA	QIGA	QICSA	QITSA
10	0.5375	0.4	0.35	0.018162	0.012237	0.014621
20	0.4	0.35	0.275	0.019874	0.014943	0.010203
30	0.3875	0.325	0.3	0.021312	0.011617	0.013204
40	0.375	0.3	0.325	0.022683	0.010491	0.014435
50	0.375	0.3	0.3	0.023986	0.01065	0.010167

Table 2 Error rate deviation and computation time deviation

Iterations	Error rate deviation			Computation time deviation(sec)		
	QIGA	QICSA	QITSA	QIGA	QICSA	QITSA
10	0.158607	0.229129	0.122474	0.004236	0.00342	0.006892
20	0.122474	0.122474	0.075	0.001454	0.009629	0.000887
30	0.117925	0.114564	0.1	0.002176	0.003505	0.008579
40	0.136931	0.1	0.114564	0.003372	0.000816	0.011351
50	0.125	0.1	0.1	0.004663	0.000629	0.001296

shown in the table below, and the technique for holding onto the least error value is presented for additional investigation.

"It can be seen from Figure 2 that the error rate for QIGA and QICSA in 10th iteration is greater than that of QITSA by 3.6% and 10.6% respectively. In 20-thioteration, the error rate deviation for QIGA and QICSA is 4.7% greater than it is for QITSA. When compared to QITSA, QIGA and QICSA have an error rate deviation that is 1.7% and 1.4% greater respectively in the 30th iteration. However, QICSA has a smaller error rate variation than QIGA (3.6%) and QICSA (1.4%), in the case of 40thiteration. while, in the instance of the 50th iteration, QICSA and QITSA both have the same number for their error rate, and QICSA has a greater deviation of 2.5% than both QIGA and QITSA. As a result of this, one may draw the conclusion that if more iterations are performed using QICSA, then it will have a higher performance than QIGA and QITSA."

"It can be seen from Fig. 3 that the average error rate value of QIGA is higher than the value obtained by QICSA and QITSA in the 10th iteration. And the deviation difference between QIGA and QICSA is 13.7% in the 10th iteration, but it drops down to 0.5% in the 20th iteration and stays the same for further iterations to the same extent of the same value. Therefore, QIGA will have a terrible performance. The difference in deviation between QICSA and QITSA in the 20th iteration is 7.5%. This is due to the fact that QICSA has

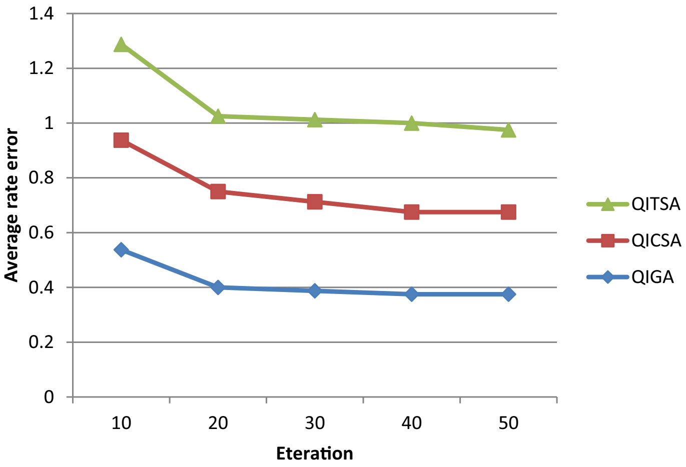

Fig. 2 Number of iterations versus average error rate

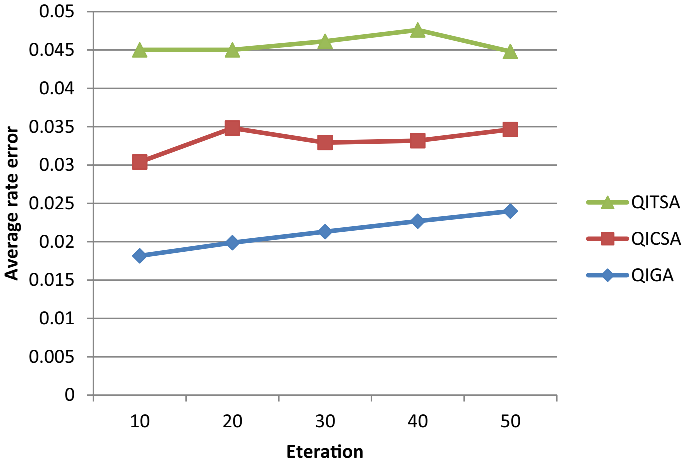

Fig. 3 Number of iterations versus error rate deviation

a larger error rate value. However, after looking at the results of the 30th run, the deviation difference was just 1.4%. And by the 40th iteration, QITSA has achieved a 1.4% improvement above QICSA. After fifty iterations, QITSA has deviated to the same level as QICSA, and both models have improved their performance. However, for subsequent iterations, there is a possibility that QITSA would vary further, while QICSA is stable to some amount, and as a result, QICSA performs more effectively."

"It can be shown in Fig. 4 that the QICSA algorithm performs better than both the QIGA and the QITSA algorithms. The places that are enclosed in the illustration above give the impression that they have not been chopped. In addition, the investigation leads one to the conclusion that raising the total number of iterations applied to QICSA would result in improved performance."

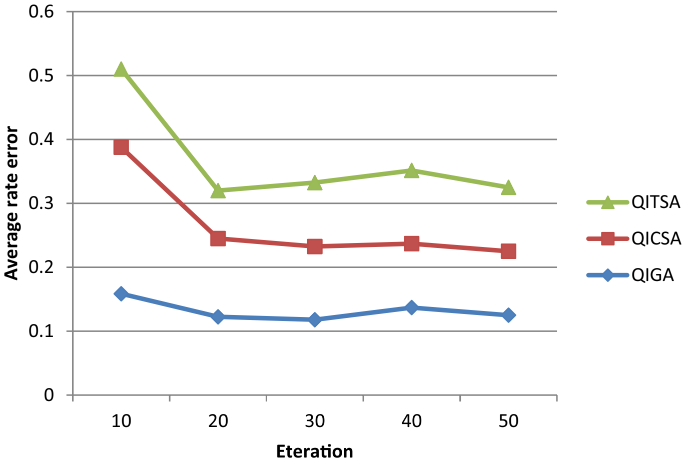

Fig. 4 Number of iterations versus average computation time

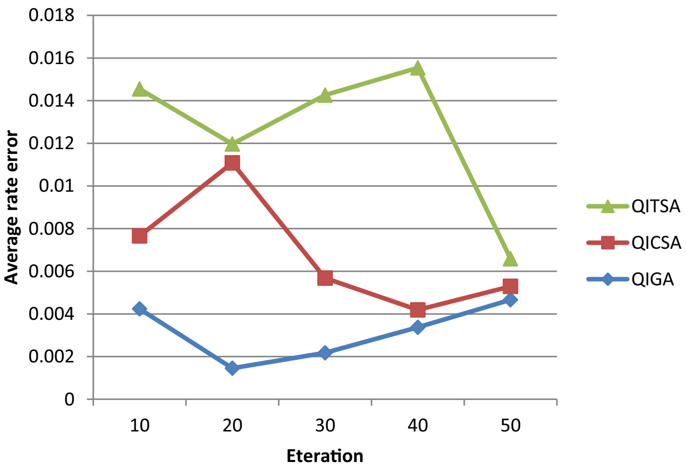

Fig. 5 Number of iterations versus computation time deviation

"It can be seen from Fig. 5 that the performance of QICSA is superior to that of QIGA and QITSA. According to the findings of the study, QICSA performs much better than the other two algorithms when subjected to a variety of iterations. According to the findings of the experiment, QICSA requires additional iterations in order to properly evaluate the robustness of the technique. As a result, when compared to traditional algorithms, the performance of evolutionary algorithms influenced by quantum mechanics is superior. This is possible due to quantum superposition, quantum entanglement, and quantum gates."

5 Conclusion and Future Work

"This study focuses on quantum inspired algorithms such as QIGA, QICSA, and QITSA and compares their performance to that of classical algorithms such as GA, CSA, and TSA. The findings of this study are presented in this publication. The genetic, cuckoo, and Tabu search algorithms, as well as the quantum inspired genetic algorithm, are used to construct heuristic assaults. The performances are measured in terms of the amount of time it takes to compute and the error rate. Based on the comparison, the quantum-inspired heuristic search algorithms perform better in terms of both error rate and computing time. This is due to the quantum principles, such as Heisenberg's uncertainty principle and the no-cloning theorem, which are used by these algorithms." For future Authentication Constraints like Quantum Digital Signature may be introduced in the proposed protocols and study can be conducted on their consistency. The proposed QSS protocol could be extended also to fuzzy neural approach.

Acknowledgements Not applicable.

Author Contributions The authors contributed significantly to the research and this paper, and the first author is the main contributor.

Funding This work received no specific funding.

Data Availability Not applicable.

Declarations

Conflict of interest The authors declare that they have no conflicts of interest to report regarding the present study.

Informed Consent Not applicable.

References

1. Dunjko, V., & Briegel, H. J. (2018). Machine learning & artificial intelligence in the quantum domain: A review of recent progress. *Reports on Progress in Physics, 81*(7), 074001.
2. Argüelles, C. A., & Jones, B. J. P. (2019). Neutrino oscillations in a quantum processor. *Physical Review Research, 1*, 033176.
3. Wehner, S., Elkouss, D., & Hanson, R. (2018). Quantum internet: A vision for the road ahead. *Science, 362*(6412), 9288.
4. Ren, J. G., Ping, X., Yong, H. L., Zhang, L., Liao, S. K., Yin, J., Liu, W. Y., Cai, W. Q., Yang, M., Li, L., Yang, K. X., Han, X., Yao, Y. Q., Li, J., Hai-Yan, W., Wan, S., Liu, L., Liu, D. Q., Kuang, Y. W., Pan, J. W. (2017). Ground-to-satellite quantum teleportation. *Nature, 549*(7670), 70–73. https://doi.org/10.1038/nature23675
5. Nandi, K., & Mazumdar, C. (2014). Quantum teleportation of a two qubit state using GHZ-like state. *International Journal of Theoretical Physics, 53*(4), 1322–1324.
6. Bennett, C. H., & Brassard, G. (2014). Quantum cryptography: Public key distribution and coin tossing. *Theoretical Computer Science, 560*, 7–11.
7. Hassanpour, S., & Houshmand, M. (2015). Efficient controlled quantum secure direct communication based on GHZ-like states. *Quantum Information Processing, 14*(2), 739–753.
8. Wang, J., Li, L., Peng, H., & Yang, Y. (2017). Quantum-secret-sharing scheme based on local distinguishability of orthogonal multiqudit entangled states. *Physical Review A*. https://doi.org/10.1103/PhysRevA.95.022320
9. Matsumoto, R. (2017). Unitary reconstruction of secret for stabilizer-based quantum secret sharing. *Quantum Information Processing, 16*(8), 202.
10. Lu, H., Zhang, Z., Chen, L. K., Li, Z. D., Liu, C., Li, L., Liu, N. L., Ma, X., Chen, Y. A., & Pan, J. W. (2016). Secret sharing of a quantum state. *Physical Review Letters, 117*(3), 030501.
11. Gravier, S., Javelle, J., Mhalla, M., & Perdrix, S. (2015). On weak odd domination and graph-based quantum secret sharing. *Theoretical Computer Science, 598*, 129–137. https://doi.org/10.1016/j.tcs.2015.05.038
12. Diep, D. N., Giang, D. H., & Phu, P. H. (2018). Application of quantum gauss-jordan elimination code to quantum secret sharing code. *International Journal of Theoretical Physics, 57*(3), 841–847.
13. Abulkasim, H., Hamad, S., & Elhadad, A. (2018). Reply to Comment on 'Authenticated quantum secret sharing with quantum dialogue based on Bell states.' *Physica Scripta, 93*(2), 027001.
14. Gao, G., Wang, Y., Wang, D., & Ye, L. (2018). Comment on 'Authenticated quantum secret sharing with quantum dialogue based on Bell states. *Physica Scripta, 93*(2), 027002.
15. Liu, Z.-M., & Zhou, L. (2014). Quantum teleportation of a three-qubit state using a five-qubit cluster state. *International Journal of Theoretical Physics, 53*(12), 4079–4082.
16. Liao, C.-H., Yang, C.-W., & Hwang, T. (2014). Dynamic quantum secret sharing protocol based on GHZ state. *Quantum Information Processing, 13*(8), 1907–1916.
17. Zhang, J.-L., Zhang, J.-Z., & Xie, S.-C. (2018). A Choreographed Distributed Electronic Voting Scheme. *International Journal of Theoretical Physics, 57*(9), 2676–2686.
18. Sharma, R. D., & De, A. (2016). Quantum voting using single qubits. *Indian Journal of Science and Technology, 9*(42), 032329.
19. Ghose, S., Kumar, A., & Hamel, A. M. (2014). Multiparty quantum communication using multiqubit entanglement and teleportation. *Physics Research International, 2014*, 1–8. https://doi.org/10.1155/2014/948750
20. Tian, J.-H., Zhang, J.-Z., & Li, Y.-P. (2016). A voting protocol based on the controlled quantum operation teleportation. *International Journal of Theoretical Physics, 55*(5), 2303–2310.
21. Thapliyal, K., Sharma, R. D., & Pathak, A. (2016). Protocols for quantum binary voting. *International Journal of Quantum Information, 15*(01), 1750007.

22. Cao, H.-J., Ding, L.-Y., Jiang, X.-L., & Li, P.-F. (2018). A new proxy electronic voting scheme achieved by six-particle entangled states. *International Journal of Theoretical Physics, 57*(3), 674–681. https://doi.org/10.1007/s10773-017-3597-y
23. Zhang, J.-L., Xie, S.-C., & Zhang, J.-Z. (2017). An elaborate secure quantum voting scheme. *International Journal of Theoretical Physics, 56*(10), 3019–3028.
24. Xue, P., & Zhang, X. (2017). A simple quantum voting scheme with multi-Qubit entanglement. *Scientific Reports*. https://doi.org/10.1038/s41598-017-07976-1
25. Ballance, C. J., Harty, T. P., Linke, N. M., Sepiol, M. A., & Lucas, D. M. (2016). High-fidelity quantum logic gates using trapped-ion hyperfine Qubits. *Physical Review Letters*. https://doi.org/10.1103/PhysRevLett.117.060504
26. Zhu, G., Subaşı, Y., Whitfield, J. D., & Hafezi, M. (2018). Hardware-efficient fermionic simulation with a cavity–qed system. *Npj Quantum Information, 4*(1), 1–10.
27. Veldhorst, M., Eenink, H. G. J., Yang, C. H., & Dzurak, A. S. (2017). Silicon cmos architecture for a spin-based quantum computer. *Nature Communications*. https://doi.org/10.1038/s41467-017-01905-6
28. Kleißler, F., Lazariev, A., & Arroyo-Camejo, S. (2018). Universal, high-fidelity quantum gates based on superadiabatic, geometric phases on a solid-state spin-Qubit at room temperature. *Npj Quantum Information, 4*(1), 1–6.
29. Wendin, G. (2017). Quantum information processing with superconducting circuits: A review. *Reports on Progress in Physics, 80*(10), 106001.
30. Riedel, M. F., Binosi, D., Thew, R., & Calarco, T. (2017). The European quantum technologies flagship programme. *Quantum Science and Technology, 2*(3), 030501. https://doi.org/10.1088/2058-9565/aa6aca
31. Raymer, M. G., & Monroe, C. (2019). The US national quantum initiative. *Quantum Science and Technology, 4*(2), 020504.
32. Yin, J., Ren, J.G., Liao, S.K., Cao, Y., Cai, W.Q., Peng, C.Z. and Pan, J.W. (2019) Quantum science experiments with micius satellite. In *2019 Conference on Lasers and Electro-Optics (CLEO)*. pp 1–2, ISSN 2160-8989.
33. Roberson, T. M., & White, A. G. (2019). Charting the Australian quantum landscape. *Quantum Science and Technology, 4*(2), 020505.
34. Sussman, B., Corkum, P., Blais, A., Cory, D., & Damascelli, A. (2019). Quantum Canada. *Quantum Science and Technology, 4*(2), 020503.
35. Yamamoto, Y., Sasaki, M., & Takesue, H. (2019). Quantum information science and technology in Japan. *Quantum Science and Technology, 4*(2), 020502.
36. AlKawak, O. A., Ozturk, B. A., Jabbar, Z. S., & Mohammed, H. J. (2023). Quantum optics in visual sensors and adaptive optics by quantum vacillations of laser beams wave propagation apply in data mining. *Optik, 273*, 170396. https://doi.org/10.1016/j.ijleo.2022.170396
37. Alomari, E. S., Nuiaa, R. R., Alyasseri, Z. A. A., Mohammed, H. J., Sani, N. S., Esa, M. I., & Musawi, B. A. (2023). Malware detection using deep learning and correlation-based feature selection. *Symmetry, 15*(1), 123.

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Bilal A. Alhayani received the B.Sc. degree in Laser Engineering from university of Technology—Baghdad, Iraq in 1999–2004, and the M.Sc. degree in electronics and telecommunication engineering and electromagnetic from University of PuneIndia from 2011 to 2013 he was joined in Ph.D. researcher in 2014–2020 in Electronics and communication Department in Yildiz Technical UniversityIstanbul, Turkey. His general research interests lie in signal processing and communication theory and signal coding on wireless communication and image processing specific research area include cooperative communication techniques.

Omar A. AlKawak working as assistance prof in Department of Air Conditioning and Refrigeration Technical Engineering, Al-Mustaqbal University College, Hilla, Babil, Iraq. He is now a researcher in rImage processing Digital Signal Processing, and Information Security. Currently she is a lecturer in the University of Information Technology.

Hemant B. Mahajan awarded her B.Sc. degree in Electronic and Communication Engineering from Pune University, India, Research Analysis and Data Scientist, Godwit Technologies, Pune. His research interests are on Communication Engineering, Information technology, Digital Signal Processing, and Information Security. Currently she is a lecturer in the University of Information Technology and Communications/College of Business Informatics.

Haci Ilhan received the B.Sc. degree in Electronics and Communication Engineering from Yildiz Technical University, Istanbul, Turkey. The M.Sc. and the Ph.D. degree all in Electronics and Communication Engineering from Istanbul Technical University, Istanbul, Turkey. From 2001 to 2011 he was a research and teaching assistant in the communication department at Istanbul Technical University. Since 2011, he has been with the Department of Electronics and Communication, Yildiz Technical University, Istanbul Turkey, where he is an Associate Professor. His general research interests lie in communications theory and signal processing for communications with particular emphasis on wireless applications. Specific research areas include cooperative communication, MIMO communication techniques, space-time coding.

Roa'a Mohammed Qasem is a Ph.D. student at the Institute of Electrical and Computer Engineering (ECE), at the University of Altinbas in Turkey. She received her Bachelors in 2007 and her Masters in 2018. Her interests include machine learning, artificial intelligence, data mining, and IoT.