Journal of Computer Science

Original Research Paper

Carving Secret Messages out of Public Information

Naya Nagy, Marius Nagy and Selim G. Akl

Queen's University, Kingston, Ontario, Canada

Article history
Received: 20-10-2014
Revised: 19-01-2015
Accepted: 22-01-2015

Corresponding Author:
Naya Nagy
Queen's University, Kingston, Ontario, Canada
Email: naya.nagy@gmail.com

Abstract: This study shows that secret information can be shared or passed from a sender to a receiver even if not encoded in a secret message. In the protocol designed in this study, no parts of the original secret information ever travel via communication channels between the source and the destination, no encoding/decoding key is ever used. The two communicating partners, Alice and Bob, are endowed with coherent qubits that can be read and set and keep their quantum values over time. Additionally, there exists a central authority that is capable of identifying Alice and Bob to share with each half of entangled qubit pairs. The central authority also performs entanglement swapping. Our protocol relies on the assumption that public information can be protected, an assumption present in all cryptographic protocols. Also any classical communication channel need not be authenticated. As each piece of secret information has a distinct public encoding, the protocol is equivalent to a one-time pad protocol.

Keywords: Quantum Key Distribution, Quantum Cryptography, Intruder Detection, Security

Introduction

From the advent of quantum cryptography, protocols have been developed to improve the capabilities and performance of classical cryptography protocols. Quantum cryptography exploits the laws of quantum physics, working with qubits rather than bits. Qubits are endowed with quantum properties: A qubit's state can be a superposition of two binary states; a qubit in an unknown state cannot be cloned into a copy of itself; etc. Bennett and Brassard's (1984) started the field with a protocol that enhances a secret key. A small secret key already shared by Alice and Bob, the two communicating partners, can be securely enhanced to a secret key of arbitrary length. The protocol employed qubits measured in two orthogonal bases and is the first to be able to detect an intruder that only listens to the communication between Alice and Bob. Also the security level can be made arbitrarily large by increasing the number of qubits. Bennett (1992) shows a similar result using qubits measured in nonorthogonal bases. Ekert (1991) showed that key enhancement can be elegantly done with entangled qubits, where each qubit of a Bell entangled qubit pair is shared by Alice and Bob. The protocol also checks the state of entanglement of the shared qubits and thus again an intruder can be detected with a probability arbitrarily large. All protocols described until now need the two partners Alice and Bob to be authenticated by an existing classical protocol. Thus, for authentication purposes a small secret key need to be already shared by the communicating partners. Nagy and Akl (2007) show a quantum protocol in which secret information is obtained from public protected information only. Thus, this protocol does not need classical authentication of the partners, authentication is done through quantum means only. Therefore, this protocol is a genuine quantum key distribution protocol rather than a quantum key enhancement protocol. Another variant of quantum key distribution protocols are based on entanglement and entanglement swapping. A theoretical protocol developed for quantum sensor networks can be found (Nagy *et al*., 2010). Practical implementations with theoretical security proofs have been presented in (Braunstein and Pirandola, 2012; Lo *et al*., 2012). The protocol presented here will use entanglement swapping, but exhibits basic different features.

All protocols described in the previous paragraph aim to develop a secret key which is then used to encode and transmit a secret message from a sender Alice to a receiver Bob. Bob finally decodes the message. In all protocols to date, some form of the message travels from Alice to Bob. In traditional protocols, this message is encoded and sent via a classical channel. We show in this study, that using quantum means, a message need not travel at all. The message appears to both Alice and Bob, based on information they transmit to each other wholly unconnected to the content of the message. The

transmitted information is therefore fully public and need only be authenticated. Authentication is done from within the information that is shared. Every step of the communication is authenticated separately. Thus an intruder cannot masquerade at any point of the protocol. Note also that all information exchanged between Alice and Bob and pertaining to one message is fully independent from the information for a second message and therefore the protocol is equivalent to communicating with one-time pads (Denning, 1982). Note that there is no need for an encoding/decoding key, as the message never "travels".

The protocol presented in this study is a technical paraphrase of the idea that information depends on the understanding of the communicating partners, that is to say it appears in the mind of beholder (Jackendoff, 1985).

The setting chosen for our protocol is the standard two party Alice-and-Bob setting. Alice and Bob can communicate directly only via a public unauthenticated classical channel. Note that this channel does not need authentication, the usual requirement in key distribution protocols. It is the information content that travels over the classical channel that is authenticated. Additionally, both Alice and Bob have a quantum connection to a central authority. The central authority and Alice (or Bob) share entangled qubit pairs and the central authority can identify Alice and Bob.

The Protocol's Setting

The basic building block of our protocol is the qubit. A qubit in superposition is defined by $q = \alpha|0\rangle + \beta|1\rangle$, where $|\alpha|^2 + |\beta|^2 = 1$. When measured in the computational basis, $|0\rangle$ and $|1\rangle$, $|\alpha|^2$ is the probability to measure a 0 and $|\beta|^2$ is the probability to measure a 1.

An ensemble of two qubits has the general form $q_1q_2 = \alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle$, where $|\alpha|^2 + |\beta|^2 + |\gamma|^2 + |\delta|^2 = 1$. An ensemble of two qubits is entangled if the states of the two qubits are dependent. The entangled states used in this study are the four Bell states: $\phi^+ = \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right), \phi^- = \frac{1}{\sqrt{2}}\left(|00\rangle - |11\rangle\right)$, $\psi^+ = \frac{1}{\sqrt{2}}\left(|01\rangle + |10\rangle\right), and\ \psi^- = \frac{1}{\sqrt{2}}\left(|01\rangle - |10\rangle\right)$. The four Bell states also form a basis for measuring an ensemble of two qubits.

The setting (Fig. 1) of the protocol consists of the following players: Alice and Bob are the two partners that want to communicate in secret and the Central Authority (CA) that is trusted manages entangled qubits.

For simplicity, we assume that Alice and Bob are structurally the same. That is, they have the same memory and equal computational capability. The memory of both Alice and Bob consists of *l* qubits. Qubits can be written and read. When written, the qubit can be set to an arbitrary superposition $q = \alpha|0\rangle + \beta|1\rangle$ with $|\alpha|^2 + |\beta|^2 = 1$. When read, the qubit collapses to a classical 0 with probability $|\alpha|^2$ or 1 with probability $|\beta|^2$, depending on the superposition. Alice and Bob can transmit and receive classical binary messages.

The system includes the trusted central authority. The *l* qubits of each Alice and Bob are pairwise entangled with *l* corresponding qubits of the central authority, Fig. 2. The central authority is responsible for the following tasks:

- The CA knows the identity of Alice and Bob, that is to say the CA knows with whom the qubits are entangled. This can be set up well before the intended communication and may stay as long as the physical entanglement of the *l* qubits holds
- The CA performs on demand an entanglement swapping acting on both Alice and Bob. As a result Alice and Bob have an array of pairwise entangled qubits (see section 3)

The most important feature of the CA is that all tasks performed are independent of the content of the message. The central authority is an entity with larger computational power, storing more qubits and being able to perform entanglement swapping.

Entanglement Swapping

Entanglement swapping is the main action performed by the central authority. Technically, entanglement swapping is a variant of quantum teleportation (Bennett *et al*., 1993; Vaidman, 1994). Suppose there exists an entangled qubit pair $q_1q'_1$. The arbitrary, possibly unknown state of q'_1 can be teleported to a geographically remote location using a second entangled pair q'_2q_2. As a result q_1q_2 are entangled. Entanglement swapping has been demonstrated in practice (Halder *et al*., 2007). This procedure is applied here to obtain an entanglement between Alice and Bob. The central authority performs the quantum transformations necessary. Note that the central authority does not need to have any physical contact or connection to Alice or Bob. As mentioned in section 2 Alice and Bob have each *l* qubits entangled with the central authority. Let one of the pairs Alice shares with the central authority be $q_1q'_1$, where q_1 is physically located with Alice and q'_1 is located in the central authority, Fig. 3. Similarly, q'_2q_2 is the pair shared by the central authority with Bob, where q'_2 belongs to the central authority and q_2 belongs to Bob. These four qubits form an ensemble Equation 1:

$$ensemble = q_1 q'_1 q'_2 q_2 \quad (1)$$

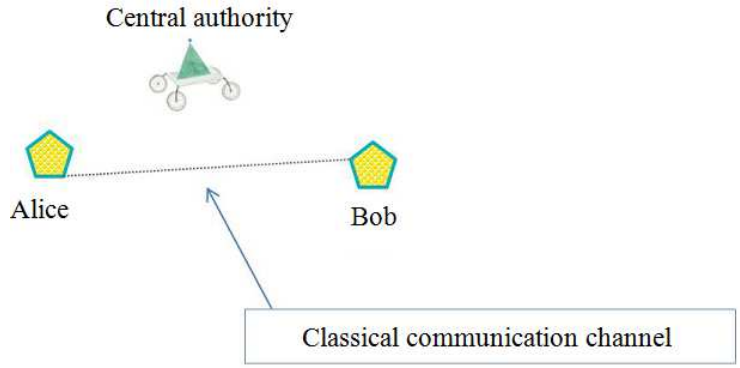

Fig. 1. Alice and Bob can communicate via an unauthenticated classical channel. The central authority is trusted and providesentangled qubitspairs

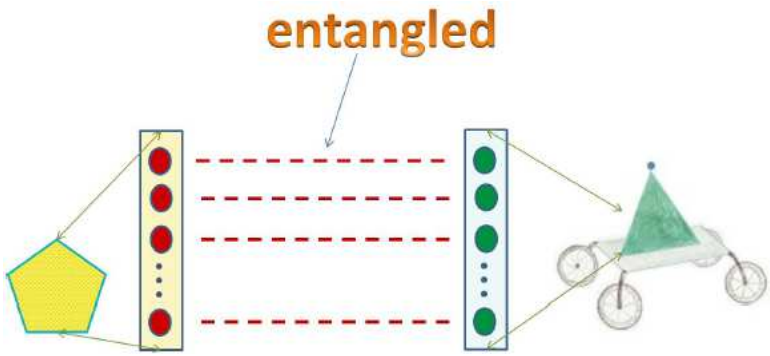

Fig. 2. *l* qubits of Alice's memory are pairwise entangled with *l* corresponding qubits in the central authority

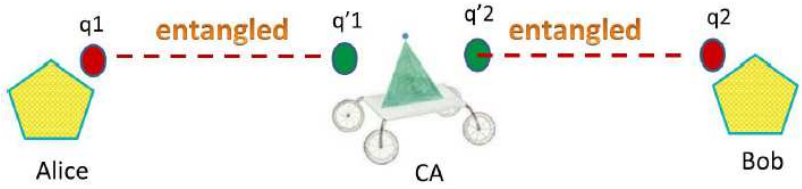

Fig. 3. Before entanglement swapping each sensor qubit is entangled with the central authority

This order has been chosen so that the transformations applied by the central authority are easier to see. Assuming both qubit pairs (q_1,q'_1) and (q_2,q'_2) are entangled in the ϕ^+ Bell state, the ensemble can be rewritten as Equation 2:

$$\begin{aligned} ensemble &= \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right) \otimes \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right) \\ &= \frac{1}{2}\left(|0000\rangle + |0011\rangle + |1100\rangle + |1111\rangle\right) \end{aligned} \tag{2}$$

The following formula rewrites the central authority's two qubits (namely, q'_1 and q'_2) highlighting the Bell basis, Equation 3:

$$\begin{aligned} ensemble &= \frac{1}{\sqrt{2}}\left(|0\rangle\right) \otimes \frac{1}{\sqrt{2}}\left(|\phi^+\rangle + |\phi^-\rangle\right) \otimes |0\rangle \\ &+ |0\rangle \otimes \frac{1}{\sqrt{2}}\left(|\psi^+\rangle + |\psi^-\rangle\right) \oplus |1\rangle + \\ &\left|1\rangle \otimes \frac{1}{\sqrt{2}}\left(|\psi^+\rangle - |\psi^-\rangle\right) \otimes |0\rangle + |1\rangle \otimes \frac{1}{\sqrt{2}}\left(|\phi^+\rangle - |\phi^-\rangle\right) \otimes |1\rangle\right) \\ &= \frac{1}{2\sqrt{2}}\left(|0\rangle \oplus |\phi^+\rangle \otimes |0\rangle + |1\rangle \oplus |\phi^+\rangle \otimes |1\rangle + \right. \\ &|0\rangle \otimes |\phi^-\rangle \otimes |0\rangle - |1\rangle \otimes |\phi^-\rangle \otimes |1\rangle + \\ &|0\rangle \otimes |\psi^+\rangle \otimes |1\rangle + |1\rangle \otimes |\psi^+\rangle \otimes |0\rangle + \\ &\left.|0\rangle \otimes |\psi^-\rangle \otimes |1\rangle - |1\rangle \otimes |\psi^-\rangle \otimes |0\rangle\right) \end{aligned} \tag{3}$$

The central authority now measures the qubits physically located at the station, q'_1 and q'_2, in the Bell basis (ϕ^+,ϕ^-, ψ^+,ψ^-).

It is interesting to see what happens to the state of the other two qubits after this measurement (Fig. 4). The central authority will have to communicate the result of the measurement to the initiating communication partner, Alice, with whom the central authority is in direct communication. The following is the list of possible measurement results by the central authority. If the central authority has measured:

1. ϕ^+. The remaining qubits have collapsed to Equation 4:

$$ensemble_{1,4} = \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right) \quad (4)$$

q_1q_2 are entangled by a Bell ϕ^+ entanglement. Alice knows the measured value of its qubit q_1 will coincide with the measured value of Bob's qubit q_2.

2.ϕ^-. The remaining qubits have collapsed to Equation 5:

$$ensemble_{1,4} = \frac{1}{\sqrt{2}}\left(|00\rangle - |11\rangle\right) \quad (5)$$

q_1q_2 are not quite ϕ^+ entangled, as the phase is rotated. Still, the values measured for the qubits coincide and that issufficient to have a consensus on the measured values of q_1q_2.

3. ψ^+. The remaining qubits have collapsed to Equation 6:

$$ensemble_{1,4} = \frac{1}{\sqrt{2}}\left(|01\rangle + |10\rangle\right) \quad (6)$$

The bit value of Alice is reversed with respect to the bit value of Bob. After measuring its qubit, Alice has to take the complement of the resulting bit.

4. ψ^-. The remaining qubits have collapsed to Equation 7:

$$ensemble_{1,4} = \frac{1}{\sqrt{2}}\left(|01\rangle - |10\rangle\right) \quad (7)$$

Again, the bit value of Alice is reversed with respect to the bit value of Bob. The phase rotation does not influence the measurement. After measuring its qubit, Alice has to take the complement of the resulting bit so that it coincides with Bob's bit.

The central authority has to communicate with Alice by a public channel so that she knows the value measured by the central authority: ϕ^+, ϕ^-, ψ^+, or ψ^-. The central authority has to send only one bit of information to discriminate between the measured values. The central authority sends a binary 0 for ϕ^+ or ϕ^- and a 1 for ψ^+ or ψ^-. For a 0, Alice measures its qubit directly and for a 1 she has to measure its qubit and then complement the resulting binary value in order to obtain the value measured by Bob.

After the communication step, Alice and Bob will be able to have a consensus on the value of a bit without having ever met.

The Protocol

We will present the protocol via an example. Suppose Alice wants to send a message to Bob. For definiteness, let the message to be transmitted be 11001, of length l_m = 5. For each bit of the message, Alice and Bob have to sacrifice a number of qubits larger than one. These qubits are initially entangled to the base station and are a part of Alice's and Bob's quantum memory. They cannot be reused for further protocols. The extra qubits are needed for two purposes:

- Authentication of Alice and Bob
- Ensure that enough classical 0s and classical 1s are generated during the protocol to hold the entirety of the message. As the 0s and 1s are generated randomly, there is a small chance that only one type of bits (for example only 0s) are generated and therefore the 1s in the message cannot be shared

To satisfy the above purposes, more qubits than the length of the message will be used up for the protocol. How many more qubits should be used depends on the level of security/certainty we want the protocol to have. Authentication is more certain when done on more qubits. In our toy example, we are sacrificing a number of $3\times l_m$ = 15 qubits. This number was chosen just to illustrate the working of the protocol and can vary largely.

The protocol described below has three phases: An entanglement swapping, a handshake with identification and thecreation of the message.

Phase I: Entanglement Swapping

In this phase, the initiator Alice makes a connection with Bob that needs to receive the message.

Step 1

When the central authority is available, Alice contacts the central authority and requests an entanglement connection with Bob. Recall that the CA knows the identity of both Alice and Bob.

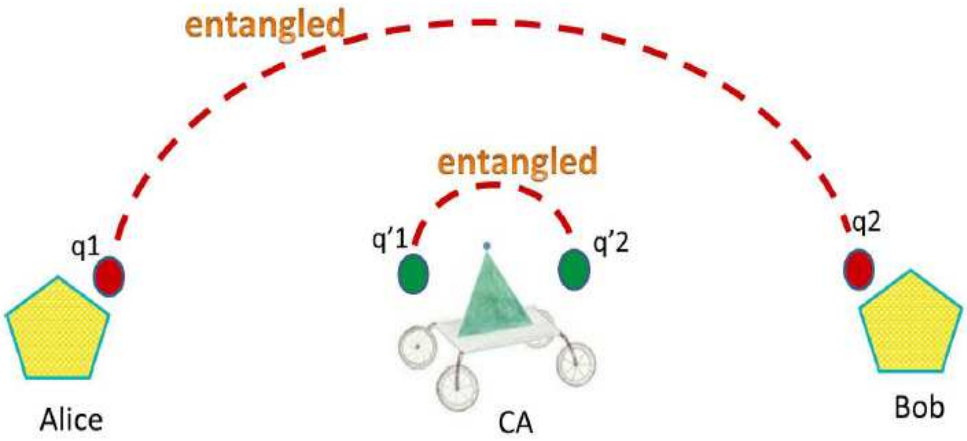

Fig. 4. After entanglement swapping the node qubits are entangled and their original pairs in the central authority are also entangled

Step 2

The central authority looks up two arrays of qubits entangled with Alice and Bob respectively. The length of the array should be well longer than the length of the message, for example $3\times l_m = 15$. Let the array entangled with Alice be $a'_1 = q1'_1\ q1'_2...q1'_{3\times lm}$. Thus, Alice has a corresponding array $a_1 = q1_1\ q1_2...\ q1_{3\times lm}$. The array belonging to the central authority and entangled with Bob is $a'_2 = q2'_1\ q2'_2...q2'_{3\times lm}$ and Bob has the corresponding array $a_2 = q2_1\ q2_2...q2_{3\times lm}$.

Step 3

The central authority performs a pairwise entanglement swapping on all ensembles $q1_i\ q1'_i\ q2'_i\ q2_i$, with $1 \leq i \leq 3\times l_m$. As a result all pairs of the form $q1_i\ q2_i$ are entangled in one of the Bell states. Figure 5 shows a possible collapse to Bell states for the chosen arrays of length 15. The row entitled "Entanglement Measured by the CA" shows the values measured by the CA for each $q1'_i\ q2'_i$, $1\leq i\leq 3\times l_m$. This measurement causes the collapse of the qubits $q1_i$, held by Alice, shown in the row entitled "Alice-measured" and the collapse of the qubits $q2_i$, held by Bob in the row entitled "Bob-measured".

Step 4

The central authority confirms to Alice that the entanglement swapping has been performed and transmits an array of bits that identify the type of entanglement. In our case, the CA transmits the array 0100111010111010, Fig. 5, the row entitled "Bit sent by the CA to Alice". Based on this bit, Alice transforms the measured qubit to fit the qubit of Bob. This transformation is shown in the row "Alice-transformed".

Phase II: Handshake

Step 1

Alice Identifies Bob

Alice reads thefirst $k = 2$ qubits of the $3\times l_m = 15$ qubits of her arraya_1. All readings in this phase are performed in the computational basis $\left(|0\rangle and |1\rangle\right)$. Note that $k << 3\times l_m$, k should be considerably smaller than $3\times l_m$. These k bits are the identifier of the message and are sent publicly to Bob over the unauthenticated classical channel to identify Bob. In our example, the first bits sent are 10, Fig. 5. In practice, k has to be sufficiently large to discriminate the communicating partner.

Step 2

Bob considers himself "addressed" if the qubits read from its memory coincide with the id of the message. In our case, Bob reads the proper sequence of qubits 10.

Step 3

Bob Identifies Alice

Bob reads the next $k = 2$ qubits in its memory and sends them back to Alice, again publicly over the classical channel. These qubits serve Bob to identify Alice. In our case the qubits sent back are 11.

Step 4

When Alice receives the message from Bob, the handshake is complete.

Phase III: Creating the Message

This phase is equivalent to carving a message into an array of random bits.

	The Qubit Arrays														
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Entanglement Measured by the CA															
Bit sent by the CA to n1	0	1	0	0	1	1	0	1	0	1	1	1	0	1	0
Alice - measured	1	1	1	1	0	1	0	0	1	0	1	1	0	0	1
Alice-transformed	1	0	1	1	1	0	0	1	1	1	0	0	0	1	1
Bob - measured	1	0	1	1	1	0	0	1	1	1	0	0	0	1	1
Alice identifies Bob	1	0													
Bob identifies Alice			1	1											
Message					1			1			0		0	1	

Fig. 5. This is an example of the protocol applied on a small message 11001. An array of 15 qubit pairs are shared between Alice and Bob

Step 1

Alice wants to send the message 11001. For every bit in the message, Alice searches for a bit of the same value in the rest of the qubits of the entangled array. In our example, the message has to be carved into the array starting from index $2\times k + 1 = 5$ until index $3\times l_m = 15$. The following indices may be chosen: 5, 8, 11, 13, 14. Or another good choice is 15, 10, 12, 13, 8. In any case reading the bits for those indices yields the correct message.

Step 2

Alice sends to Bob the array of indices that represent the message bits. In our example: 5, 8,11, 13, 14. Note that the message can be carved as long as there are enough 0s and 1s in the array of measured qubits. The number of qubits used in the protocol has to give a comfortable probability that enough bits of both kinds will be generated: We chose $3\times l_m$ for definiteness only.

Step 3

Bob receives the order of the qubits and reads the message accordingly.

Note that in Phase III in our example Alice and Bob do not authenticate each other. If authentication is desired, then Phase II and III have to be merged into one more complex step. In such a case, with each message over the classical channel, the sender has to send identification information. This is done by sacrificing additional bits from the shared array.

Because identification can be done for each message sent over the classical channel, an intruder cannot masquerade. Also listening to the messages transmitted over the classical channel reveals nothing of the content of the message to be transmitted secretly from Alice to Bob. Therefore, the protocol is secure from eavesdropping. In fact nothing in the environment reveals the content of the secret message: An honest CA has no knowledge of the qubits measured by Alice and Bob and Alice and Bob do not reveal over any channel any values of the measured qubits used for carving the message. If the CA is not fully trusted, a verification step can be introduced. A dishonest CA may produce an entanglement of three qubits and then keep the third component of the entanglement. To prevent the CA from knowing the message Alice and Bob can sacrifice some additional qubits to check whether the possess a two qubit entanglement.

Conclusion

The protocol described in this study transmits a secret message from a source Alice to a destination Bob. Alice and Bob are endowed with quantum memories, memories of qubits that keep their quantum state of superposition or entanglement until read or written.

The particularity of this protocol is that no information about the content of the message is ever transmitted in the environment. The only information that travels between Alice and Bob pertains to the order of the qubits in the message and authentication information. As such, information transmitted over the classical channels is public, but needs to be protected. As authentication is easy, see Phase II steps 1 and 2, actually any broadcast that the source and destination send to each other can be authenticated.

An eavesdropper meddling with the transmission within the network can gain absolutely no knowledge about the content of the message. Moreover, all communication between Alice and Bob may contain an identification of the node, excluding the possibility of

masquerading. Note that each identification is different than the previous one. In particular, if the two communicating partners apply the protocol several times in order to share several messages, any two different applications of the protocol share totally different information. If the eavesdropper listens to one execution of the protocol, she gains absolute no knowledge that may help her for a subsequent execution of the protocol. Thus, the scheme works equivalently to a one-time pad encoding scheme.

The only trusted authority is the central authority, that knows the identity of both Alice and Bob, as the CA has qubits entangled with each. Note that, the central authority is only trusted and entrusted to identify a communication request (from Alice) and to perform the desired entanglement swapping. Even the central authority cannot have any access to the content of the secret message. The central authority needs to have a public authenticated classical channel with the initiator of the communication, Alice. Thus, the protocol protects the content of the message from attacks of listening to any communication channel, masquerading as Alice or Bob, or listening to the communications of the central authority with Alice. All information transmitted is public. The success of the protocol relies on quantum entanglement and teleportation.

Acknowledgement

The authors appreciate the comments of the reviewers.

Funding Information

This research has received funding from Queen's University , Canada.

Author's Contributions

The three authors of the paper have contributed equally in all stages of the manuscript.

Ethics

This article is original and contains unpublished material. The corresponding author confirms that all of the other authors have read and approved the manuscript and no ethical issues are involved.

References

Bennett, C.H. and G. Brassard, 1984. Quantum cryptography: Public key distribution and coin tossing. Theoretical Comput. Sci., 560: 7-11. DOI: 10.1016/j.tcs.2014.05.025

Bennett, C.H., 1992. Quantum cryptography using any two nonorthogonal states. Phys. Rev. Lett., 68: 3121-3124. DOI: 10.1103/PhysRevLett.68.3121

Bennett, C.H., G. Brassard, C. Crepeau, R. Jozsa and A. Peres *et al*., 1993. Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. Phys. Rev. Lett., 70: 1895-1899. DOI: 10.1103/PhysRevLett.70.1895

Braunstein, S.L. and S. Pirandola, 2012. Side-channel-free quantum key distribution. Phys. Rev. Lett., 108: 5021-5024. DOI: 10.1103/PhysRevLett.108.130502

Denning, D.E.R., 1982. Cryptography and Data Security. 1st Edn., Addison-Wesley, Reading, Mass, University of Michigan, ISBN-10: 0201101505, pp: 400.

Ekert, A.K., 1991. Quantum cryptography based on Bell's theorem. Phys. Rev. Lett., 67: 661-663. DOI: 10.1103/PhysRevLett.67.661

Halder, M., A. Beveratos, N. Gisin, V. Scarani and C. Simon *et al*., 2007. Entangling independent photons by time measurement. Nature Phys., 3: 659-692. DOI: 10.1038/nphys700

Jackendoff, R., 1985. Information is in the mind of the beholder. Linguistics Philosophy, 8: 23-33. DOI: 10.1007/BF00653372

Lo, H.K., M. Curty and B. Qi, 2012. Measurement-device-independent quantum key distribution. Phys. Rev. Lett., 108: 5031-5034. DOI: 10.1103/PhysRevLett.108.130503

Nagy, N. and S.G. Akl, 2007. Authenticated quantum key distribution without classical communication. Parallel Process. Lett., 17: 323-335. DOI: 10.1142/S0129626407003058

Nagy, N., M. Nagy and S.G. Akl, 2010. Quantum security in wireless sensor networks. Natural Comput., 9: 819-830. DOI: 10.1007/s11047-010-9190-4

Vaidman, L., 1994. Teleportation of quantum states. Phys. Rev., 49: 1473-1476. DOI: 10.1103/PhysRevA.49.1473