Technical Report 2013-605
Communicating Secret Information Without Secret Messages

Naya Nagy[1], Marius Nagy[1], and Selim G. Akl[2]

[1] College of Computer Engineering and Science
Prince Mohammad Bin Fahd University, Al Khobar, KSA
{nnagy,mnagy}@pmu.edu.sa
[2] School of Computing, Queen's University
Kingston, Ontario, Canada
akl@cs.queensu.ca

July 22, 2013

Abstract. This paper shows that information can be shared or passed from a sender to a receiver even if not encoded in a message. In the protocol designed in this paper, no parts of useful information ever travel via communication channels between the source and the destination. The setting is a wireless sensor networks in which nodes are endowed with coherent qubits that can be read and set within the node. Additionally, there exists a central authority that manages the identity of the nodes and can perform entanglement swapping. Our protocol relies on the assumption that public information can be protected, an assumption present in all cryptographic protocols.

Keywords: Quantum Key Distribution, Quantum Cryptography, Intruder Detection, Security, Wireless Sensor Networks

> "The marble not yet carved
> can hold the form of every thought
> the greatest artist has."
> *Michelangelo Buonarroti*

1 Introduction

From the advent of quantum cryptography, protocols have been developed to enhance a secret key [1, 3], then to distribute a secret key starting from public information only [6]. This secret key is used to encode and then transmit a secret message from a sender Alice to a receiver Bob. In all protocols to date, some form of the message *travels* from Alice to Bob. In traditional protocols, this message is sent via a classical channel. We show in this paper, 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. Our protocol also authenticates the two parties at every step of communication.

The protocol presented in this paper 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 [5].

2 Qubits and Measurement

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 a $|\beta|^2$ is the probability to measure a 1.

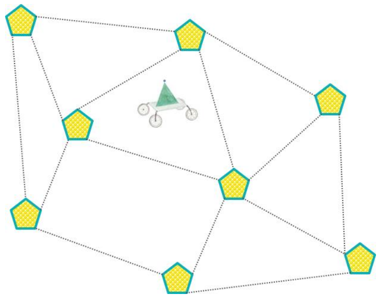


Fig. 1. The sensor network consists of random nodes, depicted as pentagons, and a central authority that is mobile in the field, depicted with wheels.

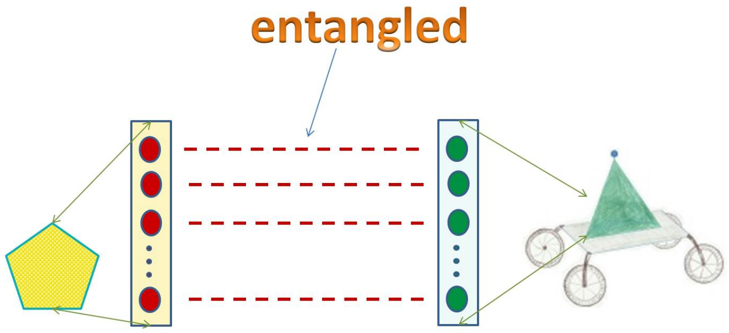


Fig. 2. l qubits of the sensors memory are pairwise entangled with l corresponding qubits in the central authority.

An ensemble of two qubits has the general form $q_A q_B = \alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle$, where $|\alpha|^2 + |\beta|^2 + |\gamma|^2 + |\delta|^2 = 1$. An ensemble of two qubits are entangled if the states of the two qubits are dependent. Entangled states that will be used in this paper are the four Bell states: $\Phi^+ = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, $\Phi^- = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$, $\Psi^+ = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$, and $\Psi^- = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$. The four Bell states also form a basis for measuring an ensemble of two qubits.

3 The Sensor Network

This section describes the particular setting of the sensor network as employed in this paper. The network has two types of components: sensor nodes and one central authority. The network has the usual topology of n sensors deployed randomly in the field. For simplicity, we assume all sensors to be structurally the same. That is, they have the same memory and equal computational capability. (In a practical setting, some sensors may have a priviledged status, being able to initiate a transmission, while others act as listeners.)

The memory of the sensors 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. A sensor can transmit and receive binary messages to within a distance to its neighbors. Fig. 1 depicts the sensor network with sensors marked as pentagons.

The sensor network includes a *central authority*. The central authority (CA) is trusted. It is responsible for the following tasks:

1. The CA knows the identity of every sensor node by its plane coordinates (x, y). Therefore, the CA is able to identify a node.
2. The CA performs on demand an entanglement swapping acting on two arbitrary nodes. As a result the two sensors have an array of pairwise entangled qubit (see section 4).

The central authority is a mobile entity with the largest computational power.

4 Entanglement Swapping in the Sensor Network

Entanglement swapping is a variant of quantum teleportation [2], [7]. Suppose there exists an entangled qubit pair $q_1 q_1'$. The arbitrary, possibly unknown state of q_1' can be teleported to a geographically remote location using a second entangled pair $q_2' q_2$. As a result $q_1 q_2$ are entangled. Entanglement swapping has

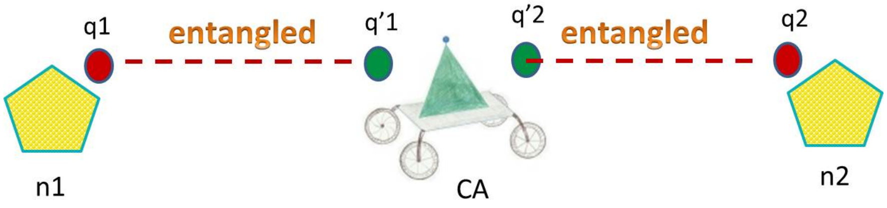


Fig. 3. Before entanglement swapping each sensor qubit is entangled with the central authority.

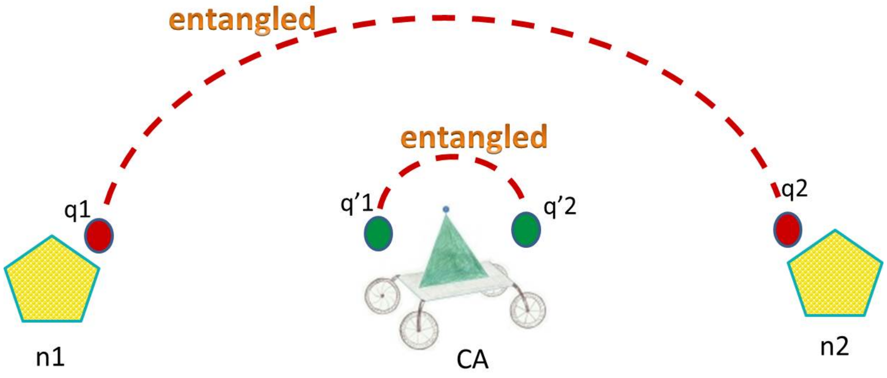


Fig. 4. After entanglement swapping the node qubits are entangled and their original pairs in the central authority are also entangled.

been demonstrated in practice [4]. This procedure is applied here to obtain an entanglement between two arbitrary sensor node. The central authority performs the quantum transformations necessary. Note that the central authority does not need to touch any node. Consider two sensor nodes n_1 and n_2 that want to share and entangled qubit pair. n_1 has qubits entangled with the central authority. Let one of these pairs be $q_1 q_1'$, where q_1 is physically located in the node n_1 and q_1' is located in the central authority, see Fig. 3. Similarly, $q_2' q_2$ is the pair shared by the central authority with the node n_2, where q_2' belongs to the central authority and q_2 belongs to the sensor node n_2. These four qubits form an ensemble

$$ensemble = q_1 q_1^{'} q_2^{'} q_2. \tag{1}$$

This order has been chosen so that the transformations applied by the central authority are easier to see. As 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

$$ensemble = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \otimes \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = \frac{1}{2}(|0000\rangle + |0011\rangle + |1100\rangle + |1111\rangle). \tag{2}$$

The following formula rewrites the central authority’s two qubits (namely, q_1' and q_2') highlighting the Bell basis

$$\begin{aligned} ensemble = \frac{1}{2}(|0\rangle \otimes \frac{1}{\sqrt{2}}(|\Phi^+\rangle + |\Phi^-\rangle) \otimes |0\rangle + |0\rangle \otimes \frac{1}{\sqrt{2}}(|\Psi^+\rangle + |\Psi^-\rangle) \otimes |1\rangle + \\ |1\rangle \otimes \frac{1}{\sqrt{2}}(|\Psi^+\rangle - |\Psi^-\rangle) \otimes |0\rangle + |1\rangle \otimes \frac{1}{\sqrt{2}}(|\Phi^+\rangle - |\Phi^-\rangle) \otimes |1\rangle) \end{aligned}$$

$$
\begin{aligned}
&= \frac{1}{2\sqrt{2}}(|0\rangle \otimes |\Phi^+\rangle \otimes |0\rangle + |1\rangle \otimes |\Phi^+\rangle \otimes |1\rangle + \\
&|0\rangle \otimes |\Phi^-\rangle \otimes |0\rangle - |1\rangle \otimes |\Phi^-\rangle \otimes |1\rangle + \\
&|0\rangle \otimes |\Psi^+\rangle \otimes |1\rangle + |1\rangle \otimes |\Psi^+\rangle \otimes |0\rangle + \\
&|0\rangle \otimes |\Psi^-\rangle \otimes |1\rangle - |1\rangle \otimes |\Psi^-\rangle \otimes |0\rangle). \qquad (3)
\end{aligned}
$$

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 (see Fig. 4). The central authority will have to communicate the result of the measurement to one of the nodes. This node will be chosen to be the node initiating the entanglement swapping n_1 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

$$ensemble_{1,4} = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle). \qquad (4)$$

   $q_1 q_2$ are entangled by a Bell Φ^+ entanglement. n_1 knows the the measured value of its qubit q_1 will coincide with the measured value of the node's n_2 qubit q_2.
2. Φ^-. The remaining qubits have collapsed to

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

   $q_1 q_2$ are not quite Φ^+ entanglement, as the phase is rotated. Still, the values measured for the qubits coincide, and that is sufficient to have a consensus on the measured values of $q_1 q_2$.
3. Ψ^+. The remaining qubits have collapsed to

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

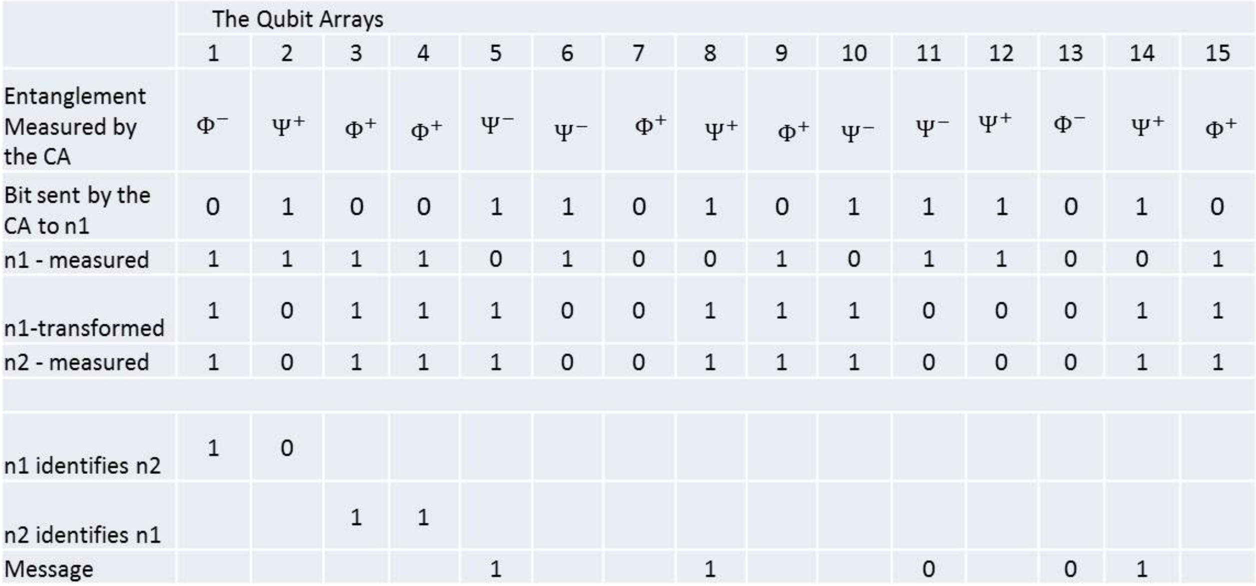
   The bit value of n_1 is reversed to the bit value of n_2. After measuring its qubit, n_1 has to take the complement of the resulting bit.
4. Ψ^-. The remaining qubits have collapsed to

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

   Now n_1's qubit compared to n_2's qubit has both the bit value reversed and the phase is rotated. After measuring its qubit, n_1 has to take the complement of the resulting bit.

The central authority has to communicate with n_1 by a public channel so that the node 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, the node n_1 measures its qubit directly and for a 1 the node has to measure its qubit and then complement the resulting binary value in order to obtain the value measured by the node n_2.

After the communication step, the nodes n_1 and n_2 will be able to have a consensus on the value of a bit without having ever met.



	The Qubit Arrays														
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Entanglement Measured by the CA	Φ^-	Ψ^+	Φ^+	Φ^+	Ψ^-	Ψ^-	Φ^+	Ψ^+	Φ^+	Ψ^-	Ψ^-	Ψ^+	Φ^-	Ψ^+	Φ^+
Bit sent by the CA to n1	0	1	0	0	1	1	0	1	0	1	1	1	0	1	0
n1 - measured	1	1	1	1	0	1	0	0	1	0	1	1	0	0	1
n1-transformed	1	0	1	1	1	0	0	1	1	1	0	0	0	1	1
n2 - measured	1	0	1	1	1	0	0	1	1	1	0	0	0	1	1
n1 identifies n2	1	0													
n2 identifies n1			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 n_1 and n_2.

5 The Protocol

We will present the protocol via an example. Suppose the node n_1 wants to send a message to the location (x, y) in the field. n_1 is the initiator of the transmission. For example, the message to be send is 11001, of length $l_m = 5$.

Phase I: Entanglement Swapping.

Sharing the marble not yet carved.

In this phase, the initiator node n_1 makes a connection with the destination node n_2 that needs to receive the message.

Step 1: When the central authority is available, n_1 contacts the central authority and requests an entanglement connection with a node available in the proximity of the desired location (x, y).

Step 2: The destination node n_2, positioned closely to (x, y), is chosen by the central authority based on the mapping node/position that the central authority has.

Step 3: The central authority looks up two arrays of qubits entangled with n_1 and n_2 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 n_1 be $a'_1 = q1'_1\, q1'_2 \dots q1'_{3\times l_m}$. Thus, n_1 has a corresponding array $a_1 = q1_1\, q1_2 \dots q1_{3\times l_m}$. The array belonging to the central authority and entangled with n_2 is $a'_2 = q2'_1\, q2'_2 \dots q2'_{3\times l_m}$, and n_2 has the corresponding array $a_2 = q2_1\, q2_2 \dots q2_{3\times l_m}$.

Step 4: 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. Fig. 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 the node n_1, shown in the row entitled “n1 - measured”, and the collapse of the qubits $q2_i$, held by the node n_2, shown in the row entitled “n2 - measured”.

Step 5: The central authority confirms to the node n_1 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 010011010111010, see Fig. 5, the row entitled “Bit sent by the CA to n1”. Based on this bit, n_1 transforms the measured qubit to fit the qubit of n_2. This transformation is shown in the row “n1 - transformed”.

Phase II: Handshake.

Step 1: **Node n_1 identifies node n_2.** The node n_1 reads the first $k = 2$ qubits of the $3 \times l_m = 15$ qubits of its array a_1. All readings in this phase are performed in the computational basis ($|0\rangle$ and $|1\rangle$). Note that $k << 3 \times l_m$, k should be considerable smaller than $3 \times l_m$. These k bits are the identifier of the message and are broadcast publicly over the network to identify the destination node n_2. In our example, the first bits broadcast over the network are 10, see Fig. 5. In practice, k has to be sufficiently large to discriminate among all the nodes in the network.

Step 2: Each node in the sensor network now reads the first k qubits of its workable memory. A node considers itself addressed if the qubits read from its memory coincide with the id of the message. In our case, node n_2 reads the proper sequence of qubits 10.

Step 3: **Node n_2 identifies node n_1.** Node n_2 reads the next $k = 2$ qubits in its memory and broadcasts them back, again publicly over the network. These qubits serve n_2 to identify n_1. In our case the qubits sent back are 11.

Step 4: When the node n_1 receives the broadcast message from node n_2, the handshake is complete.

Phase III: Creating the message.
Carving the marble.

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

Step 1: The node n_1 has the message to be sent 11001. For every bit in the message, n_1 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: n_1 broadcasts the array of indices that represent the message bits. In our example: 5, 8, 11, 13, 14.

Step 3: n_2 receives the order of the qubits and reads the message accordingly.

6 Conclusions

The protocol described in this paper transmits a secret message from a source node to a destination node in a wireless sensor network. The sensors 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 over the network. The only information over the network pertains to the order of the qubits in the message and identification information. As such, information transmitted over the network is public, but needs to be protected. As identification is easy, see Phase II steps 1 and 2, actually any broadcast that the source and destination nodes send over the network 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 the nodes may contain an identification of the node, excluding the possibility of masquerading.

The only trusted authority is the central authority, that knows the position (x, y) of all nodes. Note that, the central authority is trusted to perform the desired entanglement swapping only. 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 source node.

Thus, the protocol protects the content of the message from attacks of listening to the network, masquerading as a node, or listening to the communications of the central authority and the network. All information transmitted is public. The success of the protocol relies on quantum entanglement and teleportation.

References

1. C. H. Bennett and G. Brassard. Quantum cryptography: Public key distribution and coin tossing. In *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, pages 175–179, IEEE, New York, 1984. Bangalore, India, December 1984.
2. C.H. Bennett, G. Brassard, C. Crepeau, R. Jozsa, A. Peres, and W.K. Wootters. Teleporting an unknown quantum state via dual classical Einstein-Podolsky-Rosen channels. *Physical Review Letters*, 70:1895–1899, 1993.
3. Charles H. Bennett. Quantum cryptography using any two nonorthogonal states. *Physical Review Letters*, 68(21):3121–3124, May 1992.
4. M. Halder, A. Beveratos, N. Gisin, V. Scarani, C. Simon, and H. Zbinden. Entangling independent photons by time measurement. *Nature Physics*, 3:659–692, 2007.
5. Ray Jackendoff. Information is in the mind of the beholder. *Linguistics and Philosophy*, 8(1):23–33, 1985.
6. Naya Nagy and Selim G. Akl. Authenticated quantum key distribution without classical communication. *Parallel Processing Letters*, 17(2):323–335, September 2007.
7. L. Vaidman. Teleportation of quantum states. *Phys. Rev. A*, 49(2):1473–1476, Feb 1994.