Communicating Secret Information Without Secret Messages

Naya Nagy, Marius Nagy and Selim G. Akl

School of Computing
Queen's University
Canada

SUM ERGO COMPUTO

Main Result

- We show that secret information can be shared by a sender and a receiver without it ever being encrypted in a secret message.
- Our protocol relies on the assumption that public information can be protected, an assumption present in all cryptographic protocols.
- It is equivalent to a one-time pad protocol.

Background

Conventional Cryptosystems

- Secret-key cryptosystems
  - Substitution (confusion) and permutation (diffusion)
  - One-time pad

Unconventional Cryptosystems

- Public-key cryptosystems
- Quantum cryptography (secret keys without prior encounter)
- Communicating secret information without secret messages

Background

Conventional Cryptosystems

- Secret-key cryptosystems

  Alice: $C = E_k(M)$ ⟶ Bob: $M = E_k^{-1}(C)$

  - Substitution (confusion) and permutation (diffusion)

    Alice: LOVE→TEAH→HATE⟶Bob: HATE→TEAH→LOVE

  - One-time pad

    Alice: $C = 1011 \oplus \mathbf{1101} = 0110$⟶Bob: $M = 0110 \oplus \mathbf{1101} = 1011$

Unconventional Cryptosystems

- Public-key cryptosystems
- Quantum cryptography (secret keys without prior encounter)
- Communicating secret information without secret messages

ONE TIME PAD

Key for message 1: 100111001011000111…..

Key for message 2: 011001100111000011…..

.

.

.

Key for message *n*: 101110000110101010…..

.

.

.

Background

Conventional Cryptosystems

- Secret-key cryptosystems
  - Substitution (confusion) and permutation (diffusion)
  - One-time pad

Unconventional Cryptosystems

- Public-key cryptosystems

  Alice: $C = B(M) \qquad \longrightarrow \qquad$ Bob: $M = B^{-1}(C)$

- Quantum cryptography (secret keys without prior encounter)
- Communicating secret information without secret messages

The basic RSA public key cryptosystem

1. Bob generates two large prime numbers p and q and computes $n = p \text{ x } q$
2. Bob generates e such that $\gcd(e, (p - 1)(q - 1)) = 1$
3. Bob generates d such that $ed = 1 \bmod (p - 1)(q - 1)$
4. Bob publishes (e,n) as his public key, while keeping p, q, and d secret.

When Alice wishes to send a message M secretly to Bob

1. Alice looks up Bob’s public key (e, n), computes $C = M^e \bmod n$ and sends C to Bob.
2. Upon receipt of C, Bob computes $M = C^d \bmod n$.

Note:

1. Digital Signature: Alice can use her secret key to “sign” her message.
2. The security of the RSA cryptosystem rests on the difficulty of factoring large numbers
3. However, other attacks on the basic RSA cryptosystem (besides factoring *n*) are possible, making it generally insecure.

Even more secure versions than the basic RSA can be compromised.

In particular, when quantum computing becomes a reality, it will be possible to factor large numbers very quickly and break the RSA cryptosystem.

This would signal the end of e-commerce which relies heavily on public-key cryptography.

Fortunately, quantum computing will also provide the solution in the form of quantum cryptography.

Background

Conventional Cryptosystems

- Secret-key cryptosystems
  - Substitution (confusion) and permutation (diffusion)
  - One-time pad

Unconventional Cryptosystems

- Public-key cryptosystems
- Quantum cryptography (secret keys without prior encounter)

  Alice: $q_1, q_2, \ldots, q_n \longleftarrow$ Qubit Provider $\longrightarrow$ Bob: $q'_1, q'_2, \ldots, q'_n$

  Measure :1 0 0 1 1 0 1 1 1 1 0 Measure:1 1 1 0 1 0 0 0 1 0 0

  Secret key k: 1 1 0 1 0 Secret key k: 1 1 0 1 0

  $C = E_k(M) \qquad \longrightarrow \qquad M = E_k^{-1}(C)$

- Communicating secret information without secret messages

Alice	0	1	1	0	0	1	0	0	0	1	0	0	1	1	0
	×	+	×	+	+	+	×	×	+	+	×	+	×	×	×
	↗	↑	↖	→	→	↑	↗	↗	→	↑	↗	→	↖	↖	↗
Bob	+	+	×	+	×	×	+	×	×	+	+	+	×	+	×
	1	1	1	0	0	1	1	0	1	1	0	0	1	1	0
key		1	1	0				0		1		0	1		0

Background

Conventional Cryptosystems

- Secret-key cryptosystems
  - Substitution (confusion) and permutation (diffusion)
  - One-time pad

Unconventional Cryptosystems

- Public-key cryptosystems
- Quantum cryptography (secret keys without prior encounter)
- Communicating secret information without secret messages

Some intuition

Suppose you and a friend wish to communicate in secret.

In order to arrange for this to happen, you get together and choose a book that you both like and of which both of you have the exact same edition.

Let’s say you wish to send your friend this message:

STAY SAFE

You use the agreed upon book to create the secret message to send.

In the **book**, you find

an S on page 30, line 12, character 6,

a T on page 2, line 21, character 14,

an A on page 100, line 22, character 20,

a Y on page 62, line 17, character 26,

a space on page 26, line 18, character 8,

an S on page 3, line 2, character 13,

an A on page 205, line 1, character 1,

an F on page 25, line 18, character 18,

an E on page 5, line 21, character 18.

You send to your friend the sequence:

30,12,6,2,21,14,100,22,20,62,17,26…5,21,18

Using the book, your friend recreates the message **STAY SAFE**.

This is the well-known “book cipher” algorithm.

It can be improved by using a different book for each message.

The only trouble is that you need to meet your friend (in person or virtually) in order to set up the process (choosing the book or books) before starting to exchange messages.

The algorithm to follow is, in some sense, the “book cipher” approach to cryptography revisited, with a quantum twist that is theoretically unbreakable.

And you don’t need to meet your friend before starting the secret exchange.

Communicating secret information without secret messages

What is new?

1. There is no encryption key as such
   - Alice encodes her secret message using a public nondeterministic algorithm

2. There is no encryption as such
   - Alice encodes each bit of her secret message as a nondeterministically selected index in a binary array, and transmits it publicly.

Communicating secret information without secret messages

Furthermore:

1. Like public-key cryptography, there is no prior meeting,
   - but unlike public-key cryptography there is no secret key

2. Like one-time pads, each bit is used once,
   - but unlike one-time pads, there is no secret encounter.

What is a 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,

$$|0\rangle \text{ and } |1\rangle,$$

$|\alpha|^2$ is the probability to measure a 0, and

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

When are two qubits entangled?

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 is entangled if the states of the two qubits are dependent.

The entangled states we use are the four Bell states:

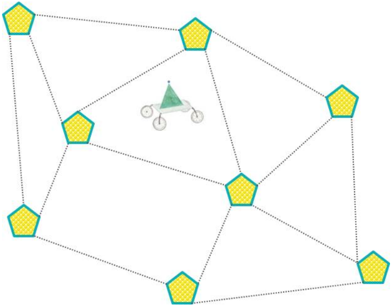
$\Phi^+ = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, $\Phi^- = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$,

$\Psi^+ = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$, $\Psi^- = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$.

These states also form a basis for measuring an ensemble of two qubits.

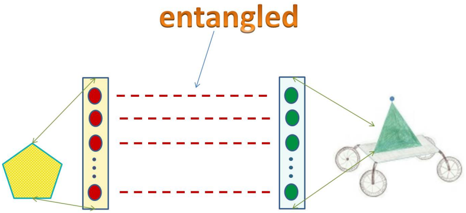
The setting

The setting consists of a set of users and a central authority (CA).



The setting

Each user can store ℓ qubits in an entanglement with ℓ qubits in the CA.



The CA:

1. Is trusted.
2. Knows the identity of every user.
3. Performs on demand an entanglement swapping acting on two arbitrary user memories. As a result the two users have an array of pairwise entangled qubits.

What is entanglement swapping?

Entanglement swapping is a variant of quantum teleportation.

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 been demonstrated in practice.

This procedure is applied here to obtain an entanglement between two arbitrary users.

The central authority performs the quantum transformations necessary.

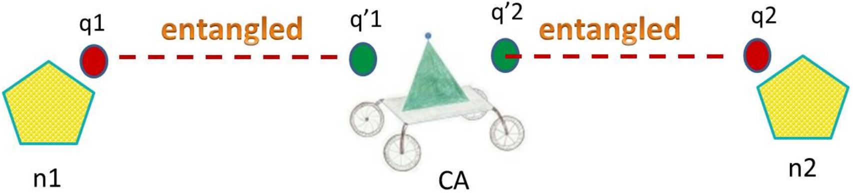
Note that the central authority does not need to touch the qubits of any user.

What is entanglement swapping?

Consider two users n_1 and n_2 that want to share and entangled qubit pair.

n_1 has qubits entangled with the CA and so does n_2.

Let one of these pairs be $q_1 q_1'$, where q_1 is physically located at user n_1 and q_1' is located in the CA.



Similarly, $q_2' q_2$ is the pair shared by the CA with user n_2, where q_2' belongs to the CA and q_2 belongs to user n_2.

What is entanglement swapping?

These four qubits form an ensemble

$$\mathit{ensemble} = q_1 q_1^{'} q_2^{'} q_2.$$

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

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

What is entanglement swapping?

Rewriting the CA's two qubits q'_1 and q'_2 in the Bell basis:

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

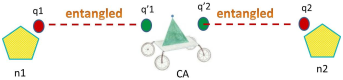
$$\begin{aligned}
= \tfrac{1}{2\sqrt{2}}(&|0\rangle \otimes |\Phi^+\rangle \otimes |0\rangle + |1\rangle \otimes |\Phi^+\rangle \otimes |1\rangle + \\
&|0\rangle \otimes |\Phi^-\rangle \otimes |0\rangle - |1\rangle \otimes |\Phi^-\rangle \otimes |1\rangle + \\
&|0\rangle \otimes |\Psi^+\rangle \otimes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

What is entanglement swapping?

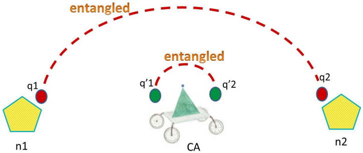
The CA now measures the qubits physically located at the station, q'_1 and q'_2, in the Bell basis $(\Phi^+, \Phi^-, \Psi^+, \Psi^-)$.

It is interesting to see what happens to the state of the other two qubits after this measurement.

BEFORE

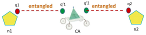


AFTER

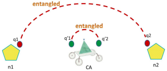


What is entanglement swapping?

BEFORE



AFTER



The CA will have to communicate the result of the measurement to one of the two users.

This user will be chosen to be the one initiating the entanglement swapping, namely, user n_1 with whom the central authority is in direct communication.

The following is the list of possible measurement results by the central authority.

What is entanglement swapping?

If the CA has measured:

- Φ^+. The remaining qubits have collapsed to

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

  $q_1 q_2$ are entangled by a Bell Φ^+ entanglement. n_1 knows the measured value of its qubit q_1 will coincide with the measured value of n_2's qubit q_2.

- Φ^-. The remaining qubits have collapsed to

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

  $q_1 q_2$ are not quite in a 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 $q_1 q_2$.

What is entanglement swapping?

If the CA has measured:

- Ψ^+. The remaining qubits have collapsed to

$$\mathit{ensemble}_{1,4} = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle). \tag{3}$$

  The bit value of n_1 is reversed with respect to the bit value of n_2. After measuring its qubit, n_1 has to take the complement of the resulting bit.

- Ψ^-. The remaining qubits have collapsed to

$$\mathit{ensemble}_{1,4} = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle). \tag{4}$$

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

What is entanglement swapping?

The CA has to communicate with n_1 by a public channel so that the user knows the value measured by the CA: Φ^+, Φ^-, Ψ^+, or Ψ^-.

The CA has to send only one bit of information to discriminate between the measured values:

- a 0 for Φ^+ or Φ^-
- a 1 for Ψ^+ or Ψ^-.

For a 0, user n_1 measures its qubit directly.

For a 1, user n_1 has to measure its qubit and then complement the resulting binary value in order to obtain the value measured by user n_2.

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

The protocol: An example

Suppose user n_1 wants to send a message to user n_2.

For example, the message to be sent is 11001, of length $\ell_m = 5$.

Phase I: Entanglement Swapping.

Step 1: n_1 requests from CA an entanglement connection with n_2.

Step 2: CA looks up two arrays of qubits entangled with n_1 and n_2, respectively.

The length of each of these two arrays should be longer than the length of the message, for example $3 \times \ell_m = 15$.

The protocol: An example

Let the CA array entangled with n_1 be

$$a'_1 = q1'_1\, q1'_2 \dots q1'_{3\times\ell_m}.$$

Thus, n_1 has a corresponding array

$$a_1 = q1_1\, q1_2 \dots q1_{3\times l_m}.$$

The CA array entangled with n_2 is

$$a'_2 = q2'_1\, q2'_2 \dots q2'_{3\times\ell_m}.$$

Thus, n_2 has the corresponding array

$$a_2 = q2_1\, q2_2 \dots q2_{3\times\ell_m}.$$

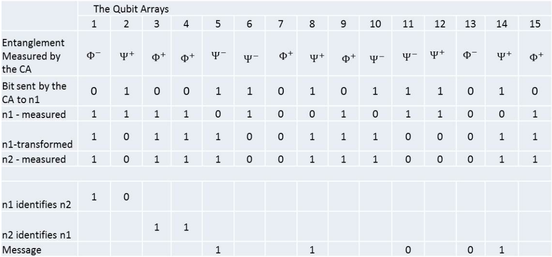
The protocol An example

Step 3: CA performs a pairwise entanglement swapping on all ensembles

$$q1_i\, q1'_i\, q2'_i\, q2_i,$$

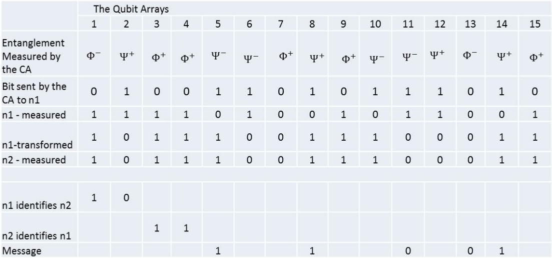
with $1 \leq i \leq 3 \times \ell_m$.

As a result all pairs $q1_i\, q2_i$ are entangled in one of the Bell states.



	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	

The protocol An example



	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	

The row entitled "Entanglement Measured by the CA" shows the values measured by the CA for each

$$q1'_i\, q2'_i,\ 1 \leq i \leq 3 \times \ell_m.$$

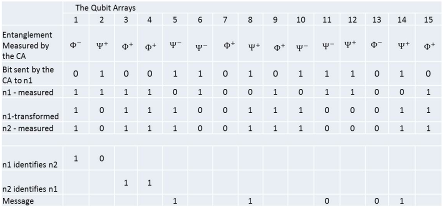
This measurement causes the collapse of the qubits $q1_i$, held by n_1, shown in the row entitled "n1 - measured",

and the collapse of the qubits $q2_i$, held by n_2, shown in the row entitled "n2 - measured".

The protocol: An example

Step 4: CA confirms to 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.



	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	

Based on these bits, n_1 transforms each measured qubit to fit the corresponding qubit of n_2.

This transformation is shown in the row “n1 - transformed”.

The protocol: An example

Phase II: Handshake.
Step 1: User n_1 identifies user n_2.

n_1 reads the first $k = 2$ qubits of the $3 \times \ell_m = 15$ qubits of its array a_1.

All readings in this phase are performed in the computational basis

$$(|0\rangle \text{ and } |1\rangle).$$

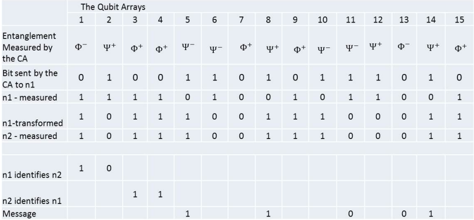
Note that $k << 3 \times \ell_m$.

In practice, k has to be sufficiently large to discriminate among all the users in the network.

The protocol: An example

These k bits are the identifier of the message and are broadcast publicly over the network to identify the destination user n_2.

In our example, the first bits broadcast over the network are 10.



	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	

Step 2:

Each user now reads the first k qubits of its workable memory.

A user considers itself addressed if the qubits read from its memory coincide with the id of the message. In our case, user n_2 reads the proper sequence of qubits 10.

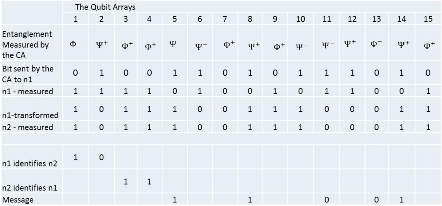
The protocol: An example

Step 3: User n_2 identifies user n_1.

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.



	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	

Step 4:

When n_1 receives the broadcast message from n_2, the handshake is complete.

The protocol: An example

Phase III: Creating the message.
This phase is equivalent to carving a message into an array of random bits.

Step 1:

User 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.

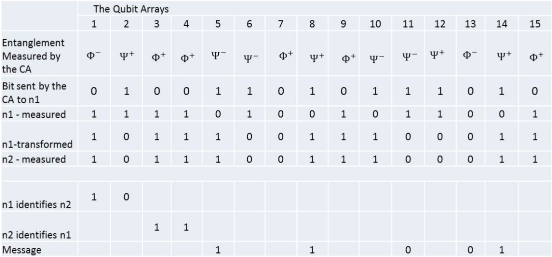
In our example, the message has to be carved into the array starting from index $2 \times k + 1 = 5$ until index $3 \times \ell_m = 15$.

The protocol: An example

The following indices may be chosen: 5, 8, 11, 13, 14.

Or: 15, 10, 12, 13, 8.

Note that the bits at those indices yield the correct message to be sent 11001.



	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	

The protocol: An example

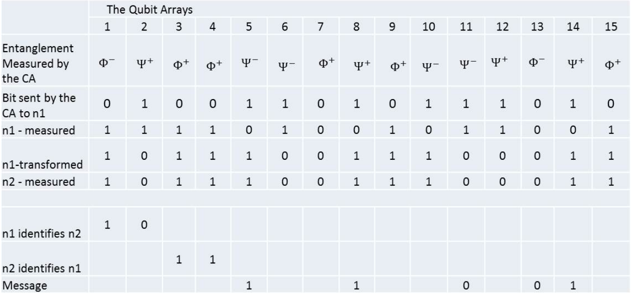
Step 2:

n_1 broadcasts the array of indices that represent the message bits:

5, 8, 11, 13, 14.

Step 3:

n_2 receives the order of the qubits and reads the message accordingly.



	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	

Conclusion

The protocol transmits a secret message from a source to a destination in a communication network.

Users of the network are endowed with quantum memories, memories of qubits that keep their quantum state of superposition or entanglement until read or written.

Phase II steps 1 and 2, and in fact any broadcast that the source and destination send over the network, can be authenticated.

Conclusion

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 users may contain an identification of the user, excluding the possibility of masquerading.

The only trusted authority is the CA, that knows the identities of all users. Note that:

- The CA is trusted to perform the desired entanglement swapping only.
- Even the CA cannot have any access to the content of the secret message.
- The CA needs to have a public authenticated classical channel with the source user.

Conclusion

Thus, the protocol protects the content of the message from attacks of

- listening to the network,
- masquerading as a user, or
- listening to the communications of the CA and the network.

All information transmitted is public.

The success of the protocol relies on quantum entanglement and teleportation.