Quantum communication protocols based on entanglement swapping

Guillermo Morales-Luna
Computer Science Department, CINVESTAV-IPN, Mexico City, Mexico
E-mail: gmorales@cs.cinvestav.mx

Abstract. We recall several cryptographic protocols based on entanglement alone and also on entanglement swapping. We make an exposition in terms of the geometrical aspects of the involved Hilbert spaces, and we concentrate on the formal nature of the used transformations.

1. Introduction
Entanglement has been widely exploited in the design of protocols and procedures for communication, cryptography and computation within quantum contexts. Quantum codes guarantee that information has been transmitted without any alteration. Cryptographic protocols aid for key agreement for secure communication, namely unconditionally secure information exchange. Entanglement has been used to implement and to speed-up paradigmatic quantum algorithms [1, 2].

Entanglement swapping may entangle two quantum systems without direct interaction among them, and this fact is exploited within several quantum cryptography schemes.

Here, we recall several well known cryptographic protocols using entanglement, alone, and entanglement swapping: the Quantum Secure Direct Communication Protocol (see Table 3 below) communicates securely bit strings with an even length, the Quantum Bidirectional Communication Protocol (see Table 4 below) is a generalization of the above protocol in which the communicating parts exchange simultaneously messages of even bit length, the Quantum Multidirectional Communication Protocol (see Table 8 below) allows the message exchange among three parts using the maximally entangled GHZ states, at Table 9 we recall a three parties protocol in which two correspondents communicate securely just after the authorisation of a third party (who does not catch the message exchange), and finally, the Key Agreement Protocol Using Entanglement Swapping is sketched at Table 10 in order to illustrate the use of entanglement swapping in cryptographic protocols.

We emphasize the algebraic aspect of the Hilbert space nature of all the involved protocols. We establish a correspondence among unitary transforms, obtained as tensor products of Pauli maps, and permutations of basic vectors in the Hilbert spaces. These correspondence are summarized at Tables 2 and 6. Also, explicit expressions of the Bell basis, in terms of the Hadamard basis, are given.

For any two integer numbers $i, j \in \mathbb{Z}^+$, with $i \leq j$, let us write

$$[i, j] = \{i, i + 1, \ldots, j - 1, j\}.$$
2. Qubits and Pauli transforms

Let $\mathbb{H}_1 = \mathbb{C}^2$ be the two-dimensional complex Hilbert space. The unit sphere of $\mathbb{H}_1$ is the set of qubits. The canonical basis consists of the vectors $e_0 = [1 0]^T$ and $e_1 = [0 1]^T$. Usually, it is written $|0\rangle = e_0$ and $|1\rangle = e_1$. Let $h_0 = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and $h_1 = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ be the vectors forming the Hadamard basis at $\mathbb{H}_1$.

Let us consider the Pauli operators

$$
\sigma_0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \\
\sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}
$$

and let us number them as $[\sigma_0 \sigma_1 \sigma_2 \sigma_3] = [\sigma_0 \sigma_x \sigma_y \sigma_z]$. The action of these operators over the vectors at the canonical and the Hadamard basis is sketched at Table 1. At each entry is located the value of $\sigma_i$ at the vector labeling the corresponding column. We see that, up to a factor which is a unitary complex number, the canonical basis remains fixed by $\sigma_0$ and $\sigma_3$ and is switched by $\sigma_1$ and $\sigma_2$ while the Hadamard basis remains fixed by $\sigma_0$ and $\sigma_1$ and is switched by $\sigma_2$ and $\sigma_3$. Thus, the operator $\sigma_2$ is switching both basis.

Let $\mathbb{H}_2 = \mathbb{H}_1 \otimes \mathbb{H}_1$ be the Hilbert space containing the 2-quregisters. Any 2-quregister $\mathbf{x}$ has two components $\mathbf{x}_0$ and $\mathbf{x}_1$, each at the factor space $\mathbb{H}_1$, they are qubits. Let for $i, j \in [0, 1]$, $b_{ij} = \frac{1}{\sqrt{2}} ((|0i\rangle + (-1)^j |1j\rangle ))$, here the overline denotes complement modulus 2. Then $B = (b_{ij})_{i,j\in [0,1]}$ is the Bell basis of $\mathbb{H}_2$ and consists of four maximally entangled states. In terms of the Hadamard basis, the Bell vectors are expressed as follows:

$$
b_{00} = \frac{1}{\sqrt{2}} (h_0 \otimes h_0 + h_1 \otimes h_1) \\
b_{01} = \frac{1}{\sqrt{2}} (h_1 \otimes h_0 + h_0 \otimes h_1) \\
b_{10} = \frac{1}{\sqrt{2}} (h_0 \otimes h_0 - h_1 \otimes h_1) \\
b_{11} = \frac{1}{\sqrt{2}} (h_1 \otimes h_0 - h_0 \otimes h_1)
$$

Any sequence $C = (c_k)_{k \geq 0}$ whose terms are elements of $B$ determines two sequences of qubits $C_0 = (c_{k0})_{k \geq 0}$ and $C_1 = (c_{k1})_{k \geq 0}$.
Through the radix expression of an index in base 2, we may number the Bell basis as $B = (b_k)_{k \in \{0, 2^{3}-1\}}$. The tensor products $σ_{ij} = σ_i \otimes σ_j$ determine bijections $α_{ij} : B → B$, such that
\[
∀(i, j) \in [0, 3]^2 \forall k \in [0, 2^3 - 1] : \quad σ_{ij}(b_k) ∈ L(α_{ij}(k)).
\] (2)

Let $A_2 : σ_{ij} → α_{ij}$ be the map that associates to each tensor product $σ_{ij}$ the corresponding permutation that it defines at the Bell basis. The image of $A_2$ consists of just $4 = 2^2$ permutations $(β_ℓ)_{ℓ \in [0, 2^3-1]}$, and each permutation is defined by 4 tensor products $σ_{ij}$ as summarized at the Table 2: the first column displays the index $ℓ$, the second column the permutation $β_ℓ$, and the third column the list of tensor product maps $σ_{ij}$ producing $β_ℓ$ under the map $A_2$.

**Table 2. Correspondence on permutations of the Bell basis and tensor products of Pauli operators**

| ℓ | β_ℓ | $A_2^{-1}(β_ℓ)$ |
|---|-----|-----------------|
| 0 | 0 1 2 3 | {σ_{00}, σ_{01}, σ_{02}, σ_{03}} |
| 1 | 2 3 0 1 | {σ_{01}, σ_{00}, σ_{03}, σ_{02}} |
| 2 | 3 2 1 0 | {σ_{02}, σ_{03}, σ_{00}, σ_{01}} |
| 3 | 1 0 3 2 | {σ_{03}, σ_{02}, σ_{01}, σ_{00}} |

Table 2 can in turn be summarized as
\[
∀i ∈ [0, 3] : \quad A_2(σ_{iβ}(i)) = β_0, \quad A_2(σ_{iβ}(i)) = β_1,
\]
\[
A_2(σ_{iβ}(i)) = β_2, \quad A_2(σ_{iβ}(i)) = β_3.
\] (3)

By looking at relation (2), we see that if $i$ and $k$ remain fixed, then the index $j$ can be encoded by the value $α_{ij}(k)$. This property can be exploited for secure communication purposes.

In Table 3 a Quantum Secure Direct Communication Protocol [3] is sketched. The purpose of this protocol is to communicate securely a word in $[0, 3]$. Alice should communicate a message $[μ_κ]_{κ=0}^{m-1} ∈ [0, 3]^m$. Alice and Bob fix a Pauli transform $σ_i$, a Bell quregizer $b_k ∈ B$, an integer $n > m$ and an index set $J ∈ [0, n - 1]^{(m)}$. They share initially a constant sequence $C = (c_κ)^{n-1}_{κ=0}$ whose terms coincide with $b_k ∈ B$.

Using sequences of entangled quregisters it is also possible to build bidirectional communication protocols. In Table 4 a Quantum Bidirectional Communication Protocol is sketched [4]. The purpose of this protocol is to communicate securely two words in $[0, 3]^n$, one going from Alice to Bob and the other in the opposite direction. Alice and Bob should interchange messages in $[0, 1]^{2n}$, and they share initially a constant sequence $C = (c_κ)^{n-1}_{κ=0}$.

### 3. Entanglement swapping

Entanglement swapping is a phenomenon which allows to put two particles into entangled states although these particles have not been close at any time. Departing from two pairs of entangled particles, a particle is chosen from each pair, then the joint pair of selected particles is measured with respect to the Bell basis, resulting in an entangled state. As a consequence, the pair consisting of the two partner particles is also entangled. This last pair is the result of the entanglement swapping beginning from the original two pairs.

In two 2-quregisters there are involved 4 qubits, let us identify them with the four indexes in the integer interval $[0, 3]$. Let us write $|ε⟩_μ$, for $ε ∈ \{0, 1\}$, $μ ∈ [0, 3]$, to denote the state of
Table 3. Quantum Secure Direct Communication Protocol

| Alice | Bob |
|-------|-----|
| pads the message $[\mu]_{m=0}^{m-1}$ into a sequence $[j]_{\kappa=0}^{\kappa-1}$ by inserting the message into the positions at $J$ | sends $D_1$ through a quantum channel |
| codifies the message $[j]_{\kappa=0}^{\kappa-1}$ by calculating $D_1 = (\sigma_i(c_{\kappa}))_{\kappa=0}^{\kappa-1}$ | receives $D_1$ |
| calculates $D_0 = (\sigma_i(c_{\kappa}))_{\kappa=0}^{\kappa-1}$, which actually completes the calculation of $D = ([\sigma_i \otimes \sigma_j](c_{\kappa}))_{\kappa=0}^{\kappa-1}$ | calculates $E$ by measuring each term at $D$ with respect to the Bell basis |
| recovers the sequence $(\alpha_{ij}(k))_{\kappa=0}^{\kappa-1}$, consequently the padded sequence $[j]_{\kappa=0}^{\kappa-1}$ and the original message $[\mu]_{m=0}^{m-1}$ | since she knows $i_\kappa$, using (2), she recovers $j_\kappa$ |

Table 4. Quantum Bidirectional Communication Protocol

| Alice | Bob |
|-------|-----|
| by taking pairs of contiguous bits, she writes her message as a word $(i_\kappa)_{\kappa=0}^{\kappa=n-1} \in [0,3]^n$ | by taking pairs of contiguous bits, he writes his message as a word $(j_\kappa)_{\kappa=0}^{\kappa=n-1} \in [0,3]^n$ |
| codifies her message by calculating $D_0 = (\sigma_i(c_{\kappa}))_{\kappa=0}^{\kappa-1}$ | codifies his message by calculating $D_1 = (\sigma_j(c_{\kappa}))_{\kappa=0}^{\kappa-1}$ |
| sends $D_0$ through a quantum channel | receives $D_1$ |
| receives $D_1$ | sends $D_1$ through a quantum channel |
| for each $\kappa \in [0,n-1]$ she measures the entangled quregister $d_\kappa$ with respect to the Bell basis |
| since she knows $i_\kappa$, using (2), she recovers $j_\kappa$ |
| for each $\kappa \in [0,n-1]$ he measures the entangled quregister $d_\kappa$ with respect to the Bell basis |
| since he knows $j_\kappa$, using (2), he recovers $i_\kappa$ |

the $\mu$-th qubit. For any two different indexes $\mu, \nu \in [0,3]$, let the respective Bell basis of the Hilbert space $\mathbb{H}_2$ be

$$b_{ij}^{(\mu\nu)} = \frac{1}{\sqrt{2}} \left( |0i\rangle_{\mu\nu} + (-1)^j |1j\rangle_{\mu\nu} \right),$$

Let us assume that the 2-quregister consisting of the qubits 0 and 1 is entangled as well as the pair of qubits 2 and 3. Then a basis of the space $\mathbb{H}_4$ is

$$B_{(01)(23)} = \left( z_{i_0 j_0 i_1 j_1} = b_{i_0 j_0}^{(01)} \otimes b_{i_1 j_1}^{(23)} \right)_{i_0 j_0 i_1 j_1 \in [0,1]}. \tag{4}$$
Each 2-quregister

By swapping the middle qubits, the following 4-quregisters result:

∀

where

and this relation is symmetric:



Each 2-quregister \( \mathbf{z}_{ij0i1j1} \) given by relation (5) can be expressed in terms of the 2-quregisters \( \mathbf{y}_{ij0i1j1} \) given by relation (7), namely:

\[
\mathbf{z}_{ij0i1j1} = \frac{1}{2} \left( \mathbf{y}_{ij0i1j1} + (-1)^{j_0} \mathbf{y}_{ij0i1j1} + (-1)^{j_1} \mathbf{y}_{ij0i1j1} + (-1)^{j_0+j_1} \mathbf{y}_{ij0i1j1} \right),
\]

and this relation is symmetric:

\[
\mathbf{y}_{ij0i1j1} = \frac{1}{2} \left( \mathbf{z}_{ij0i1j1} + (-1)^{j_1} \mathbf{z}_{ij0i1j1} + (-1)^{j_0} \mathbf{z}_{ij0i1j1} + (-1)^{j_0+j_1} \mathbf{z}_{ij0i1j1} \right),
\]

In this way, the entanglement of the 4-registers \( \mathbf{z} \) is reflected by the entanglement of the 4-registers \( \mathbf{y} \), in other words, the entanglement of the pairs (0, 1) and (2, 3) is swapped into the entanglement of the pairs (0, 2) and (1, 3), and conversely.

### 4. Three-entanglement

Let us consider multi-party bidirectional protocols. In particular, we will illustrate these procedures with three communicating parties. A proper protocol considers maximally entangled 3-quregisters, members of \( \mathbb{H}_3 = \mathbb{H}_1 \otimes \mathbb{H}_2 \). Any 3-quregister \( \mathbf{x} \) has three components \( \mathbf{x}_0, \mathbf{x}_1 \) and \( \mathbf{x}_2 \), each at the factor space \( \mathbb{H}_1 \), they are qubits. For \( \varepsilon_1, \varepsilon_2, \varepsilon_3 \in [0, 1] \) let

\[
\mathbf{b}_{\varepsilon_1\varepsilon_2\varepsilon_3} = \frac{1}{\sqrt{2}} \left( |0\varepsilon_1\varepsilon_2\rangle + (-1)^{\varepsilon_3} |1\varepsilon_1\varepsilon_2\rangle \right).
\]

These vectors form a basis, \( \mathcal{B}_3 \), analogous to the Bell basis in \( \mathbb{H}_3 \), but they are called Greenberger-Horne-Zeilinger (GHZ) states. In terms of the Hadamard vectors, the GHZ states are expressed as shown at the Table 5.
Let Table 6. As seen at the beginning of section 2, the operator \(Correspondence on permutations of the Bell basis and tensor products of Pauli\) in an analogous way as in (2):

Through the radix expression of an index in base 2, we may number the Bell basis as \(B_3 = (b_\ell)_{\ell \in \{0,2^3-1\}}\). The tensor products \(\sigma_{ijk} = \sigma_i \otimes \sigma_j \otimes \sigma_k\) determine bijections \(\alpha_{ijk} : B_3 \to B_3\) in an analogous way as in (2):

\[
\forall (i, j, k) \in [0, 3]^3 \forall \ell \in [0, 2^3 - 1] : \quad \sigma_{ijk}(b_\ell) \in \mathcal{L}(b_{\alpha_{ijk}(\ell)}). \tag{10}
\]

Let \(A_3 : \sigma_{ijk} \mapsto \alpha_{ijk}\) be the map that associates to each tensor product \(\sigma_{ijk}\) the corresponding permutation at the Bell basis. The image of \(A_3\) consists of just \(8 = 2^3\) permutations \((\beta_\mu)_{\mu \in \{0,2^3-1\}}\), and each permutation is defined by 8 tensor products \(\sigma_{ijk}\) as summarized in Table 6. As seen at the beginning of section 2, the operator \(\sigma_2\) switches the canonical and the

### Table 5. The GHZ states in terms of the Hadamard basis of qubits.

| \(b_{\ell00}\) | \(b_{\ell01}\) | \(b_{\ell010}\) | \(b_{\ell011}\) | \(b_{\ell10}\) | \(b_{\ell101}\) | \(b_{\ell110}\) | \(b_{\ell111}\) |
|-----------------|-----------------|-----------------|-----------------|-----------------|-----------------|-----------------|-----------------|
| \(\frac{1}{2} (h_0 \otimes (h_0 \otimes h_0 + h_1 \otimes h_1) + h_1 \otimes (h_0 \otimes h_1 + h_1 \otimes h_0))\) | \(\frac{1}{2} (h_0 \otimes (h_0 \otimes h_0 + h_1 \otimes h_1) + h_0 \otimes (h_0 \otimes h_1 + h_1 \otimes h_0))\) | \(\frac{1}{2} (h_0 \otimes (h_0 \otimes h_0 - h_1 \otimes h_1) + h_1 \otimes (-h_0 \otimes h_1 + h_1 \otimes h_0))\) | \(\frac{1}{2} (h_0 \otimes (h_0 \otimes h_0 - h_1 \otimes h_1) + h_0 \otimes (h_0 \otimes h_1 + h_1 \otimes h_0))\) | \(\frac{1}{2} (h_0 \otimes (h_0 \otimes h_0 - h_1 \otimes h_1) + h_1 \otimes (-h_0 \otimes h_1 - h_1 \otimes h_0))\) | \(\frac{1}{2} (h_0 \otimes (h_0 \otimes h_0 - h_1 \otimes h_1) + h_0 \otimes (h_0 \otimes h_1 - h_1 \otimes h_0))\) | \(\frac{1}{2} (h_0 \otimes (h_0 \otimes h_0 + h_1 \otimes h_1) + h_1 \otimes (-h_0 \otimes h_1 - h_1 \otimes h_0))\) | \(\frac{1}{2} (h_0 \otimes (h_0 \otimes h_0 + h_1 \otimes h_1) + h_0 \otimes (-h_0 \otimes h_1 - h_1 \otimes h_0))\) |

### Table 6. Correspondence on permutations of the Bell basis and tensor products of Pauli operators

| \(\mu\) | \(\beta_\mu\) | \(A_3^{-1}(\beta_\mu)\) |
|--------|----------------|---------------------|
| 0      | 0 1 2 3 4 5 6 7 | \{\sigma_{000}, \sigma_{033}, \sigma_{111}, \sigma_{122}, \sigma_{212}, \sigma_{221}, \sigma_{303}, \sigma_{330}\} |
| 1      | 2 3 0 1 6 7 4 5 | \{\sigma_{003}, \sigma_{030}, \sigma_{112}, \sigma_{121}, \sigma_{211}, \sigma_{222}, \sigma_{300}, \sigma_{333}\} |
| 2      | 3 2 1 0 7 6 5 4 | \{\sigma_{001}, \sigma_{032}, \sigma_{110}, \sigma_{123}, \sigma_{213}, \sigma_{220}, \sigma_{302}, \sigma_{331}\} |
| 3      | 1 0 3 2 5 4 7 6 | \{\sigma_{002}, \sigma_{031}, \sigma_{113}, \sigma_{120}, \sigma_{210}, \sigma_{223}, \sigma_{301}, \sigma_{332}\} |
| 4      | 1 4 5 6 7 0 1 2 3 | \{\sigma_{010}, \sigma_{023}, \sigma_{101}, \sigma_{132}, \sigma_{202}, \sigma_{231}, \sigma_{313}, \sigma_{320}\} |
| 5      | 6 7 4 5 2 3 0 1 | \{\sigma_{013}, \sigma_{020}, \sigma_{102}, \sigma_{131}, \sigma_{201}, \sigma_{232}, \sigma_{310}, \sigma_{323}\} |
| 6      | 7 6 5 4 3 2 1 0 | \{\sigma_{011}, \sigma_{022}, \sigma_{100}, \sigma_{133}, \sigma_{203}, \sigma_{230}, \sigma_{312}, \sigma_{321}\} |
| 7      | 5 4 7 6 1 0 3 2 | \{\sigma_{012}, \sigma_{021}, \sigma_{103}, \sigma_{130}, \sigma_{200}, \sigma_{233}, \sigma_{311}, \sigma_{322}\} |

Hadamard basis. Let us consider just operators of the form \(\sigma_{ijk}\) where \(i \in \{0, 3\}, j, k \in \{0, 2\}\). Then, the restriction of Table 6 to operators at the set \(S = \{\sigma_{ijk}\} i \in \{0, 3\}, j, k \in \{0, 2\}\) is shown at Table 7.

In Table 8 a Quantum Multidirectional Communication Protocol is sketched [4, 5]. The purpose of this protocol is to communicate securely four classical bits, two emitted by Alice,
Table 7. Correspondence on permutations of the Bell basis and tensor products of Pauli operators at the set $S$, in alphabetical order according to the first element at $S \cap A_3^{-1}(\beta_\mu)$. Observe that if one index $i, j, k$ is known, the other two can be deduced form this index and the $3$-quregistert $\sigma_{ijk}(b_\ell)$.

| $\mu$ | $S \cap A_3^{-1}(\beta_\mu)$ |
|-------|-----------------------------|
| 0     | $\{\sigma_{000}, \sigma_{122}\}$ |
| 3     | $\{\sigma_{002}, \sigma_{120}\}$ |
| 5     | $\{\sigma_{020}, \sigma_{102}\}$ |
| 6     | $\{\sigma_{022}, \sigma_{100}\}$ |
| 7     | $\{\sigma_{200}, \sigma_{322}\}$ |
| 4     | $\{\sigma_{020}, \sigma_{320}\}$ |
| 2     | $\{\sigma_{220}, \sigma_{302}\}$ |
| 1     | $\{\sigma_{222}, \sigma_{300}\}$ |

one by Bob and another by Claire. By repeating the protocol the parties may exchange longer bit-strings. Alice, Bob and Claire should interchange four classical bits, two emitted by Alice, one by Bob and another by Claire. The parties share two GHZ states, $c_0 = c_1 = b_\ell \in \mathbb{H}_3$ with respective components $c_{00}, c_{10}, c_{20}$ and $c_{01}, c_{11}, c_{21}$. The components $c_{0k}, c_{1k}, c_{2k}$ are in possession of Alice, Bob and Claire respectively, $k \in [0, 1]$. The quregister $c_0$ is a record of the initial state $b_\ell$, while the quregister $c_1$ is to be transformed during the protocol.

Table 8. Quantum Multidirectional Communication Protocol

| (i) | The two bits of Alice determine an index $i_A \in [0, 3]$. She applies $\sigma_{i_A}$ to her qubit $c_{01}$. |
| (ii) | Bob applies either $\sigma_0$ or $\sigma_2$ to his qubit $c_{11}$ according to the value of his bit. |
| (iii) | Claire applies either $\sigma_0$ or $\sigma_2$ to her qubit $c_{21}$ according to the value of her bit. |
| (iv) | They take a measure of the transformed quregister with respect to the Bell basis. |
| (v) | Using table 7, since each participant knows his/her own message, they recover the transmitted bits. |

Another bidirectional protocol [6] consists of three participants: Alice and Bob are the correspondents and Claire is the controller. The correspondents are able to communicate only after the authorization of the controller, but their correspondence should be kept in secret against the controller. The protocol is sketched at Table 9. Alice and Bob should interchange messages at $[0, 3]^m$ after the authorization granted by Claire. The parties share a constant sequence $(c_{\nu})_{\nu=0}^{n-1}$ whose entries coincide with a GHZ initial state $b_\ell$. The component sequence $(c_{0\nu})_{\nu=0}^{n-1}$, let us say for ease of explanation, is owned by Claire, the component sequence $(c_{1\nu})_{\nu=0}^{n-1}$ by Alice and the component sequence $(c_{2\nu})_{\nu=0}^{n-1}$ by Bob.

A Key Agreement Protocol Using Entanglement Swapping is obtained [7] as follows. Let $B_2^{(\mu\nu)}$ be the Bell basis considering two qubits $\mu, \nu \in [0, 3]$, $\mu \neq \nu$.

Let $c^{(01)}$, $c^{(23)}$ be two Bell 2-quregisters with respective components $c^{(0)}, c^{(1)}$ and $c^{(2)}, c^{(3)}$.

Alice may act on the pair $(c^{(01)}, c^{(23)}) = [c^{(0)}, c^{(1)}, c^{(2)}, c^{(3)}]$ either by $(A_0;) \mu$ doing nothing or by $(A_1)$ swapping the middle qubits, obtaining thus $[c^{(0)}, c^{(2)}, c^{(1)}, c^{(3)}]$.

Bob may act on the pair $(c^{(01)}, c^{(23)}) = [c^{(0)}, c^{(1)}, c^{(2)}, c^{(3)}]$ either by $(B_0)$ measuring $c^{(0)}, c^{(1)}$ with respect to the Bell basis $B_2^{(01)}$ and measuring $c^{(1)}, c^{(2)}$ with respect to the Bell
Table 9. Quantum Controlled Bidirectional Communication Protocol

(i) Alice and Bob agree a set \( J \subset [0, n - 1] \) of \( m \) positions among the index set \([0, m - 1]\).
(ii) Alice codifies her message \((a_\mu)_{\mu=0}^{m-1} \in [0, 3]^{m-1}\) by applying \( \sigma_{a_\mu} \) to her correspondent qubit \( c_{1\nu_\mu} \), with \( \nu_\mu \in J \), and she applies arbitrary Pauli operators at her qubits with indexes not in \( J \). Alice sends her codified sequence to Claire.
(iii) Bob codifies his message \((b_\mu)_{\mu=0}^{m-1} \in [0, 3]^{m-1}\) by applying \( \sigma_{b_\mu} \) to his correspondent qubit \( c_{2\nu_\mu} \), with \( \nu_\mu \in J \), and he applies arbitrary Pauli operators at his qubits with indexes not in \( J \). Bob sends his codified sequence to Claire.
(iv) Claire receives the component sequences \((c_{1\nu_\mu})_{\nu=0}^{n-1}\) and \((c_{2\nu_\mu})_{\nu=0}^{n-1}\), and she measures the whole sequence \((c_{\nu_\mu})_{\nu=0}^{n-1}\) with respect to the basis \( B_3 \). She sends her results to Alice and Bob as an authorization to proceed the transaction.
(v) Using the table 6, her knowledge of her own message and the index set \( J \), Alice recovers Bob’s message \((b_\mu)_{\mu=0}^{m-1} \in [0, 3]^{m-1}\).
(vi) Using the table 6, his knowledge of his own message and the index set \( J \), Bob recovers Alice’s message \((a_\mu)_{\mu=0}^{m-1} \in [0, 3]^{m-1}\).

basis \( B_2^{(23)} \) or \((B_1;1)\) by measuring \([c^{(0)},c^{(2)}]\) with respect to the Bell basis \( B_2^{(02)} \) and measuring \([c^{(1)},c^{(3)}]\) with respect to the Bell basis \( B_2^{(13)} \).

If the chosen actions are \((A_0,B_0)\) or \((A_1,B_1)\), the actions are said to be correlated, otherwise, they are anticorrelated.

Table 10. Key Agreement Protocol Using Entanglement Swapping

(i) Alice selects a sequence \( B = \{b_\alpha(k)\}_{k=0}^{2m-1} \) of entangled states at the Bell basis. Each pair of two such states \((b_\alpha(2k),b_\alpha(2k+1))\), \( k \in [0, m - 1] \), involves 4 qubits, say \([c^{(0k)},c^{(1k)},c^{(2k)},c^{(3k)}]\).
(ii) For each \( k \in [0, m - 1] \), Alice applies an operation \( A_0 \) or \( A_1 \) to the current pair \((b_\alpha(2k),b_\alpha(2k+1))\). She obtains the sequence \( C \) and she sends this sequence to Bob through a public quantum channel.
(iii) Bob receives the sequence \( C \) and for any block of 4 consecutive qubits, say \([d^{(0k)},d^{(1k)},d^{(2k)},d^{(3k)}]\), he selects randomly an operation \( B_0 \) or \( B_1 \) and he applies it to \([d^{(0k)},d^{(1k)},d^{(2k)},d^{(3k)}]\).
(iv) Alice and Bob exchange through a classic channel the lists of their corresponding selected operations.
(v) The common key is established by selecting the 4 blocks measurements corresponding to the correlated pairs of operations.
(vi) It is worth to remark that at the anticorrelated positions, both Alice and Bob may recover two common bits, corresponding to the initial state of Alice for the current 4-block.

In the protocol, the agreed common key is the juxtaposition of the measures obtained at the positions in which correlated operators do occur. When looking for a greater efficiency it is possible to recover also not 4, for 2 bits at any block corresponding to an anti correlated operator.
References
[1] Gisin N, Ribordy G, Tittel W and Zbinden H 2002 Rev. Mod. Phys. 74(1) 145–195 URL http://link.aps.org/doi/10.1103/RevModPhys.74.145
[2] Lanyon B P, Weinhold T J, Langford N K, Barbieri M, James D F V, Gilchrist A and White A G 2007 Phys. Rev. Lett. 99(25) 250505 URL http://link.aps.org/doi/10.1103/PhysRevLett.99.250505
[3] Deng F G, Long G L and Liu X S 2003 Phys. Rev. A 68(4) 042317 URL http://link.aps.org/doi/10.1103/PhysRevA.68.042317
[4] Gao Fei, Guo FenZhuo, Wen QiaoYan and Zhu FuChen 2008 Science China Physics, Mechanics & Astronomy 51 559 (pages 0) URL http://phys.scichina.com:8083/sciGe/EN/abstract/article_408422.shtml
[5] Song-Kong Chong and Tzonelih Hwang 2011 Optics Communications 284 515 – 518 ISSN 0030-4018 URL http://www.sciencedirect.com/science/article/pii/S0030401810008928
[6] Man Zhong-Xiao and Xia Yun-Jie 2006 Chinese Physics Letters 23 1680 URL http://stacks.iop.org/0256-307X/23/i=7/a=007
[7] Fei Gao, Fen-Zhuo Gao, Qiao-Yan Wen and Fu-Chen Zhu 2010 International Journal of Modern Physics B 24 4611–4618 (Preprint http://www.worldscientific.com/doi/pdf/10.1142/S021797921005661X) URL http://www.worldscientific.com/doi/abs/10.1142/S021797921005661X