QUANTUM KEY DISTRIBUTION FROM A RANDOM SEED

Eduin H. SERNA
Quantum Technology Laboratory, ADAPTUN SAS,
Carrera 69A No. 44A-36 Torre 3 Int 502, Medellín, Colombia

It is designed a new quantum cryptography protocol that generates various secret and secure keys of the same size of the transmitted qubits, implying zero information losses between the interlocutors. Besides, generates key swapping between the two recipients of photons, without even sharing a past secret key. This protocol differs from BB84 just in the classic procedures, using a random seed and asymmetric cryptography.

PACS numbers: 03.67.Dd 03.67.Hk

I. INTRODUCTION

One of the most difficult practical problems when conducting secure communication is the key distribution. Shannon in 1949 [1], established that if the key, is random, has the same length of the message to code and is used one time only, then it is guaranteed statistical independence of the cryptogram with respect to the message. In fact, it is the only system demonstrated to be mathematically secure. However, the need to distribute and store securely the keys, generally long and just for one use, limits its implementation. This panorama remained the same until 1984, year in which Bennett and Brassard presented the first quantum key distribution protocol (QKD), called BB84 [2]. This protocol is that the interlocutors (Alice, Bob) transmit the key through a quantum channel. The quantum contribution to the security of the process is that an eavesdropper cannot extract information without revealing its presence to the interlocutors.

Essentially the QKD protocols BB84, B92 [3], E91 [4] and SARG04 [5] apply two processes: - Raw key exchange, obtained from the initial interpretation of the quantum states exchanged between Alice and Bob. - Public Reconciliation, where, Alice and Bob obtain the secret key from the published information. Thus, QKD is the only method physically secure to exchange secret keys [6].

In this article it is presented a new protocol that is identical to the BB84 for all the quantum manipulations, but differs from it by using Private Reconciliation from a Random Seed and Asymmetric Cryptography. Thus allowing the generation of larger secure keys.

This article is designed as follows: Sec II presents the formalism of the BB84 protocol, Sec III present the new protocol and its differences from the BB84 and Sec IV contains the conclusions.

II. BB84 PROTOCOL

A. Quantum Part

Alice and Bob exchange a set of encoded photons according to four states \(|0\rangle, |1\rangle, |+\rangle, |-\rangle\), which gather forming two basis with orthogonal states \(\mathcal{B}_0 = \{|0\rangle, |1\rangle\}\) and \(\mathcal{B}_1 = \{|+\rangle, |-\rangle\}\), where \(|\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)\). Coding the binary value 0 to the states \(|0\rangle\) and \(|+\rangle\), and the binary value 1 to the states \(|1\rangle\) and \(|-\rangle\). For simplicity it is denoted \(|\psi_{00}\rangle \equiv |0\rangle, |\psi_{01}\rangle \equiv |1\rangle, |\psi_{10}\rangle \equiv |+\rangle, |\psi_{11}\rangle \equiv |-\rangle\).

- **Raw Key Exchange**
  - Alice generates two random strings with the same length, \(N\), The strings will correspond to the keys Alice wants to share with Bob, one of binary basis \(s_1 s_2 \ldots s_N\) and the other of binary values \(i_1 i_2 \ldots i_N\). From the elements occupying the concrete position, \(k\), in both strings, Alice obtains the associated state \(|\psi_{s_k i_k}\rangle\) and sends it to Bob through a quantum channel.
  - Bob generates a random string of binary basis \(m_1 m_2 \ldots m_N\) that will correspond to the key it wants to share with Alice. Bob measures each received state \(|\psi_{s_k i_k}\rangle\) in the corresponding base \(\mathcal{B}_{m_k}\), obtaining a binary string \(a_1 a_2 \ldots a_N\).

B. Classic Part

Alice and Bob exchange a set of binary strings.

- **Public Reconciliation**
  - Bob sends to Alice the sequence of basis \(m_1 m_2 \ldots m_N\), through an public channel authenticated.
  - Alice compares the strings \(s_1 s_2 \ldots s_N\) and \(m_1 m_2 \ldots m_N\), sending to Bob the binary sequence \(l_1 l_2 \ldots l_N\) with \(l_k = s_k \oplus m_k\).
Alice and Bob share now a sequence of binary values \( i_k = a_k \) formed by \( l_k = 0 \).

An example of the BB84 is given in the Table 1. In perfect conditions Alice and Bob share and generate an identical random key.

### III. NEW PROTOCOL

#### A. Quantum Part

- **Random seed**
  - Alice or Bob publish a random binary string \( x_1 x_2 \ldots x_N \).

- **Missing Key Exchange**
  - Alice sums \( s_k \oplus x_k \), \( k = 1, 2, \ldots, N \). Obtaining a sequence of binary basis \( t_1 t_2 \ldots t_N \) and generates other random string of binary values \( j_1 j_2 \ldots j_N \) that will correspond to other key that it wants to exchange with Bob. From the elements occupying a concrete position, \( k \), of the preceding strings, Alice obtains the associated state \( |\psi_{x_j k}⟩ \) and sends it to Bob through a quantum channel.
  - Bob sums \( (1 \oplus m_k) \oplus x_k \), \( k = 1, 2, \ldots, N \). Obtaining the string of binary basis \( N_1 N_2 \ldots N_N \) and measures each received state \( |\psi_{x_j k}⟩ \) with the corresponding base \( B_{n_k} \) generating the string \( b_1 b_2 \ldots b_N \).

#### B. Classic Part

Alice and Bob exchange a set of binary strings and apply in different binary arrangements the function \( f \) defined as follows:

\[
f(z, x, y) := \begin{cases} x, & z = 0 \\ y, & z = 1 \end{cases}
\]

- **Asymmetric Cryptography**
  - Alice sums \( i_k \oplus j_k \), \( k = 1, 2, \ldots, N \). Obtaining the binary string \( y_1 y_2 \ldots y_N \) that sends to Bob.
  - Bob encrypt \( m_k \) in \( u_k \) and \( v_k \) with
    \[
    u_k = n_k \oplus f(m_k, a_k, b_k \oplus y_k), \\
    v_k = n_k \oplus f(m_k, b_k, a_k \oplus y_k). 
    \]

#### III. NEW PROTOCOL

- **Random seed**
  - Alice or Bob publish a random binary string \( x_1 x_2 \ldots x_N \).

- **Missing Key Exchange**
  - Alice sums \( s_k \oplus x_k \), \( k = 1, 2, \ldots, N \). Obtaining a sequence of binary basis \( t_1 t_2 \ldots t_N \) and generates other random string of binary values \( j_1 j_2 \ldots j_N \) that will correspond to other key that it wants to exchange with Bob. From the elements occupying a concrete position, \( k \), of the preceding strings, Alice obtains the associated state \( |\psi_{x_j k}⟩ \) and sends it to Bob through a quantum channel.
  - Bob sums \( (1 \oplus m_k) \oplus x_k \), \( k = 1, 2, \ldots, N \). Obtaining the string of binary basis \( N_1 N_2 \ldots N_N \) and measures each received state \( |\psi_{x_j k}⟩ \) with the corresponding base \( B_{n_k} \) generating the string \( b_1 b_2 \ldots b_N \).

| \( k \) | \( i_k \oplus f(s_k, (1 \oplus i_k) \oplus u_k, j_k \oplus v_k) \) |
|---|---|
| 1 | 1010000000 |
| 2 | 1010000000 |
| 3 | 1010000000 |
| 4 | 1010000000 |
| 5 | 1010000000 |
| 6 | 1010000000 |
| 7 | 1010000000 |
| 8 | 1010000000 |
| 9 | 1010000000 |
| 10 | 1010000000 |
| 11 | 1010000000 |
| 12 | 1010000000 |

**TABLE I**: The Proposed Protocol from Alice (a) to Bob (b), \( N = 8 \). The steps 1a-3a and 1b-3b are equal to BB84. Where \( s \in \{0,1\} \), \( t = s \oplus x \), \( n = 1 \oplus s \oplus m \), \( y = i \oplus j \), \( u = n \oplus f(m, a, b \oplus y) \), \( v = n \oplus f(m, b, a \oplus y) \), \( key_m = t \oplus f(s, (1 \oplus i) \oplus u, j \oplus v) \), \( l = s \oplus m \), \( key_s = m \oplus l \), \( key_l = f(l, a, b \oplus y) \), \( y \), \( key_j \), \( f(l, a, b \oplus y) \).

- **Private Reconciliation**
  - Alice compares the strings \( s_1 s_2 \ldots s_N \) and \( m_1 m_2 \ldots m_N \), sending to Bob the binary sequence \( l_1 l_2 \ldots l_N \) with \( l_k = s_k \oplus m_k \).
  - Bob sums \( m_k \oplus l_k \), \( k = 1, 2, \ldots, N \). Obtaining the private string \( s_1 s_2 \ldots s_N \) of Alice and apply:
    \[
    f(l_k, a_k, b_k \oplus y_k) \equiv i_k \\
    f(l_k, a_k \oplus y_k, b_k) \equiv j_k, 
    \]

  \( k = 1, 2, \ldots, N \). Obtaining the private strings of Alice \( i_1 i_2 \ldots i_N \), \( y \), \( j_1 j_2 \ldots j_N \).
An example of this protocol is given in Table 1. In perfect conditions Alice and Bob share four secret and secure keys with length \( N \), \( m_1 m_2 \ldots m_N \), \( s_1 s_2 \ldots s_N \), \( i_1 i_2 \ldots i_N \), \( y j_1 j_2 \ldots j_N \).

C. Quantum Key Swapping

If Central is an emitting source of photons of BB84, B92 or E91, Alice and Bob are recipients of these photons. And following the steps of the previous protocol, both generate a common key without even sharing a past between them, due that Central compares the sequences \( m_{\text{Alice}} \) and \( m_{\text{Bob}} \) in the Private Reconciliation and informs in which they coincided. Besides, If Central used the same encoded states in Raw and Missing key Exchange for Alice and Bob, they share the private strings of Central.

IV. CONCLUSIONS

In summary, It has been demonstrated that using a random seed over a set of photons and asymmetric cryptography over the encoded bits, the QKD becomes a process of zero information losses, where the percentage of coincidence of the reconciliated key against the size of the raw key is 100% unlike the BB84 in which the expected is 50%. Besides, this protocol as the SARG04 is identical to the BB84 for all the quantum manipulations and differs only in the classic procedure. Thus, this protocol can be implemented in existing devices without modifications.

[1] C. E. Shannon, Bell System Technical Journal, vol. 28 pp.656-715. (1949).
[2] C.H. Bennett and G. Brassard, Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, 175 (1984).
[3] Ch.H. Bennett, Phys. Rev. Lett. 68, 3121 (1992).
[4] A. K. Ekert, Phys. Rev. Lett. 67, 661 (1991).
[5] V. Scarani, A. Acín, G. Ribordy, N. Gisin, Phys. Rev. Lett. 92, 057901 (2004).
[6] N. Gisin et al., Rev. Mod. Phys 74, 145 (2002).