

Quantum Cryptographic Key Distribution Protocols

Lelde Lace, Oksana Scegulnaja-Dubrovskaja, Ramuns Usovs, Agnese Zalcmāne

Institute of Mathematics and Computer Science,
University of Latvia, Raina bulv. 29, Riga, LV-1459, Latvia.

***Abstract** The application of the principles of quantum mechanics to cryptography has led to a respectable new dimension in confidential communication. As a result of these developments, it is now possible to construct cryptographic communication systems which detect unauthorized eavesdropping should it occur, and which give a incontestable guarantee of no eavesdropping should it not occur. Here several protocols for such communication systems are explored. We first examine quantum bit commitment protocols which are proven as not being unconditionally secure, then, we take a look at proposed protocols which are constructed to disprove the proofs claiming that unconditionally secure quantum bit commitment protocols are impossible.*

Keywords: Quantum Cryptography, Key distribution, Protocol

1. Introduction

Quantum cryptography, quantum computing and quantum teleportation are three examples of potential 21st century technologies [13, 8] made possible by recent advances in quantum device engineering and quantum information theory. Of the three, quantum cryptography seems closest to practical realisation [13]. One form of quantum cryptography uses secret keys exchanged in the form of streams of polarisation-encoded or phase-encoded single photons transmitted over public optical communication channels. The security of these keys rests upon fundamental laws of quantum physics, rather than on the computational difficulty of breaking public keys as in the well known RSA crypto-system which requires finding the prime factors of large integers. These laws ensure that any attempt to intercept the key and measure the unknown quantum state (for example the polarisation) of individual photons inevitably introduces noise into the QKD channel and so alerts the users to the presence of the eavesdropper and the potential loss of security [5].

Quantum keys are transmitted (traditionally by "Alice") in the form of streams of photons which carry quantum information in the form of quantum bits or "qubits". Unlike classical information bits the qubits carried by single photons cannot be labeled as either "1" or "0" with certainty. They are a statistical superposition of these two states and each photon will finally be counted (by "Bob") as either a one bit or a zero bit with a *probability* determined by how he configures his single-photon receiver. This is an example of the well known importance of the observer (Bob) in determining the outcomes of quantum measurements. It is this inherent quantum uncertainty which prevents an eavesdropper ("Eve") from intercepting, copying and retransmitting qubits without introducing gross errors - it is just not possible to determine the unknown quantum state of a single photon with certainty.

Following "authentication" (mutual identification of Alice and Bob), quantum key distribution can be divided into four basic operations [12].

The first of these is the generation of a raw binary key sequence and its transmission over a quantum channel.

The second operation involves the preliminary selection and indexing of this raw key sequence by Alice and Bob over a public channel in which they agree to discard bits which fails to satisfy criteria imposed by the protocol used in the exchange. This obviously needs to be done without revealing publicly the values of the individual bits in the raw sequence.

The third operation is the estimation of the bit error rate and the subsequent correction of errors, again over a public channel. This involves the comparison and discarding of incorrect bits.

The fourth operation is known as privacy amplification. It involves the deliberate sacrifice of bits as part of the error correction procedure and the shortening of the sequence to reduce the bit error rate until identical secret bit sequences are finally held by Alice and Bob. This constitutes the final key sequence. A fifth operation has been identified by Hughes et al [12] as the renewal of the authentication code using part of the final key.

In this paper several different quantum cryptography protocols are shown.

2. The BB84 quantum cryptographic protocol

The BB84 quantum coding scheme was the first proposed quantum encoding and was introduced by Charles H. Bennett and Gilles Brassard in 1984 [1]. Hence, the protocol is called BB84. It is the basic tool most of the quantum protocols are based upon.

The BB84 protocol utilizes any two incompatible orthogonal quantum alphabets in the Hilbert space H . For our description of BB84, we have selected the *circular polarization quantum alphabet* A_o and the *linear polarization quantum alphabet* A . This cryptographic scheme uses pulses of polarized light, with one photon per pulse.

Table 1. Circular Polarization Quantum Alphabet A_o

Symbol	Bit
$ \rangle$	1
$\langle $	0

Table 2. Linear Polarization Quantum Alphabet A

Symbol	Bit
\updownarrow	1
$ \rangle$	0

The polarizations determine the angle: $\theta_1 = 0, \theta_2 = \frac{\pi}{4}, \theta_3 = \frac{\pi}{2}, \theta_4 = \frac{3\pi}{4}$. The corresponding qubit is

$\sin \theta_i |0\rangle + \cos \theta_i |1\rangle$. To transfer between different bases, a matrix $A = \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix}$ can be used [10]. The

correspondence among qubits given in both bases is shown in the Table 3:

Table 3. The correspondence among qubits

Angle of polarisation	Linear basis	Circular basis
0	$ 1\rangle$	$\frac{1}{\sqrt{2}} (0\rangle + 1\rangle)$
$\frac{\pi}{4}$	$\frac{1}{\sqrt{2}} (0\rangle + 1\rangle)$	$ 0\rangle$
$\frac{\pi}{2}$	$ 0\rangle$	$\frac{1}{\sqrt{2}} (0\rangle - 1\rangle)$
$\frac{3\pi}{4}$	$\frac{1}{\sqrt{2}} (0\rangle - 1\rangle)$	$ 1\rangle$

In order to generate a random key, Alice must send either horizontal or vertical polarization with equal probability. Each state vector of one basis has equal-length projections onto all vectors of the other basis. That is, if a measurement on a system prepared in one basis is performed in the other basis, its outcome is entirely random and the system loses all the information of its previous state.

To keep Eve from successfully eavesdropping, Alice also uses randomly the alternative circular polarizations randomly choosing between left-handed and right-handed photons. Bennett and Brassard note that, if Alice were to

use only one specific orthogonal quantum alphabet for her communication to Bob, then Eve's eavesdropping could go undetected. For Eve could intercept Alice's transmission with 100% accuracy, and then imitate Alice by retransmitting her measurements to Bob. If, for example, Alice used only the orthogonal quantum alphabet A_0 , then Eve could measure each bit of Alice's transmission with a device based on some circular polarization measurement operator such as

$$|>\rangle\langle >| \text{ or } |<\rangle\langle <|$$

The above strategy used by Eve is called *opaque eavesdropping* [7].

To assure the detection of Eve's eavesdropping, Bennett and Brassard require Alice and Bob to communicate in two stages, the first stage over a one-way quantum communication channel from Alice to Bob, the second stage over a two-way public communication channel. Here we assume that the information on the public channel can be eavesdropped, but cannot be changed.

- 1) At the beginning, Alice and Bob, agree about the alphabets used (A_0 and A_1).
- 2) Now Alice, the sender, generates a sequence of random bits that she wants to transmit, and randomly and independently for each bit she chooses her encoding basis, linear or circular.
- 3) Bob, the receiver, randomly and independently of Alice, chooses his measurement bases for each qubit, either linear or circular. He write down the results of measurements, but keep them secret. Statistically, their bases coincide in 50% of cases, when Bob's measurements provide deterministic outcomes and perfectly agree with Alice's bits.
- 4) Bob notifies Alice what bases he used for each measurement.
- 5) Alice notifies Bob about those measurements for which her base and Bob base have coincided. The bits that correspond to the coincided basis are kept as the new key.

Eve is compelled to create errors in the transmission, because she cannot know the basis that corresponds to each transmitted bit. Alice and Bob detect eavesdropping by revealing a probabilistic chosen substring of the new key and notifying each other about the count of erroneous bits (discrepancy of bits). Should at least one comparison reveal an inconsistency, then Eve's eavesdropping has been detected. If Eve had tried to eavesdrop all the transmitted qubits, the discrepancy can reach 25%. Since the bits used to test for eavesdropping are communicated over the open public channel, they must always be discarded and only the remaining bits constitute the key. Although one cannot prevent eavesdropping, one can always detect, if someone has tried to eavesdrop how smart or gentle may be the attempt. If the legitimate users do not agree with the security of the transmission channel, they can always try to make key exchange again.

The BB84 quantum transmission is a standard cryptographic and quantum primitive that can be used in different kind of protocols. Quantum key distribution using BB84 quantum transmission enjoys good cryptographic properties making it more secure but more difficult to implement than the B92 quantum transmission described below.

3. The B92 quantum cryptographic protocol

As with the BB84 quantum protocol, the B92 protocol [4] can be described in terms of any quantum system represented by a two dimensional Hilbert space. For our description, we choose the two dimensional Hilbert space H representing the polarization states of a single photon. B92 can be implemented in terms of any non-orthogonal basis. We choose as our non-orthogonal basis the kets

$$| \rangle \text{ and } | \bar{\rangle}$$

where $| \rangle$ and $| \bar{\rangle}$ denote respectively the kets representing the polarization state of a photon linearly polarized at an angle θ and an angle $-\theta$ with respect to the vertical, where $0 < \theta < \pi/4$.

Unlike BB84 which requires two orthogonal quantum alphabets, B92 requires only a single non-orthogonal quantum alphabet. We choose the nonorthogonal quantum alphabet A :

Table 4. Linear Polarization Quantum Alphabet A

Symbol	Bit
$ \rangle$	1
$ \bar{\rangle}$	0

As in BB84, Alice and Bob communicate in two stages, the first over a one-way quantum channel, the second over a two-way public channel.

Alice uses the quantum alphabet A to send her random binary sequence to Bob. Since $| \rangle$ and $| \rangle$ are not orthogonal, there is no one experiment that will unambiguously distinguish between these two polarization states.

Bob can use one of many possible measurement strategies. Bennett [4] suggests the measurements be based on the two incompatible experiments corresponding to the projection operators

$$P = 1 - | \rangle \langle | \text{ and } P^- = 1 - | \rangle \langle |$$

In this case, Bob either correctly detects Alice's transmitted bit, or an ambiguous result, i.e., an *erasure*, denoted by "?". Assuming that Alice transmits 0's and 1's at random with equal probability and that, for each incoming bit, Bob at random with equal probability chooses to base his experiment on either of the incompatible operators P or P^- , then the probability of Bob's correctly receiving Alice's transmission is

$$\frac{1 - \langle | \rangle \rangle^2}{2}$$

and the probability of receiving an erasure is

$$\frac{1 - \langle | \rangle \rangle^2}{2}, \text{ where } \langle | \rangle \rangle = \cos(2 \theta)$$

and where $0 < \theta < \pi/4$. Thus, Bob receives more than 50% erasures.

On the other hand, Ekert et al [7] suggest a more efficient measurement process for Bob. They suggest that Bob base his experiments on the *positive operator valued measure (POVM)* [2] consisting of the operators

$$A = \frac{P}{1 - \langle | \rangle \rangle}, A^- = \frac{P^-}{1 - \langle | \rangle \rangle}, \text{ and } A_? = 1 - A - A^-$$

With this more efficient detection method, the probability of an inconclusive result is now

$$\langle | \rangle \rangle = \cos(2 \theta), \quad 0 < \theta < \pi/4.$$

Stage 2 for the B92 protocol is the same as that for the BB84 protocol except for phase 1. In phase 1 of stage 2, Bob publicly informs Alice as to which time slots he received non-erasures. The bits in these time slots become Alice's and Bob's raw keys. Eve's presence is detected by an unusual error rate in Bob's raw key. It is also possible to detect Eve's presence by an unusual erasure rate for Bob. However, Ekert et al [7] do point out that Eve can choose eavesdropping strategies which have no effect on the erasure rate, and hence, can only be detected by unusual error rates in Bob's raw key.

4. Entanglement-based quantum key distribution

Another class of QKD protocols is based on quantum entanglement. The security of the original proposal was ensured by checking the violation of Bell's inequalities [3]. The simplified version of the protocol works in a very similar way as BB84.

Entanglement, Bell's inequalities

Two or more quantum systems are entangled if their global state cannot be expressed as a direct product or a statistical mixture of direct products of any quantum states of individual systems. Entanglement leads to many interesting effects unknown in classical physics.

Let us denote $A(n_1)$ and $B(n_2)$ random variables, getting discrete values ± 1 , corresponding to measurement results on two separated but somehow correlated particles, where the settings of respective measurement devices are represented by unit vectors n_1 and n_2 (note that A depends only on n_1 and B only on n_2 – this rejects the locality condition). The randomness of A and B is supposed to be caused only by some random parameters that may be common for both the particles and those we do not know (the premise of reality).

Assuming two spin-half particles are in the entangled state, the quantum prediction for correlation function reads:

$$C(n_1, n_2) = \langle |(n_1 \cdot \hat{1})(n_2 \cdot \hat{2})| \rangle,$$

where \hat{n}_1, \hat{n}_2 are vectors of Pauli matrices. If we choose the settings of the measurement apparatuses in such a way that \hat{n}_2 with \hat{n}_1 , \hat{n}_1 with \hat{n}_3 and \hat{n}_1 with \hat{n}_2 include angle $\pi/4$, while \hat{n}_1 with \hat{n}_3 include angle $3\pi/4$, we find that $|C(\hat{n}_1, \hat{n}_2) + C(\hat{n}_1, \hat{n}_3) + C(\hat{n}_2, \hat{n}_3) - C(\hat{n}_1, \hat{n}_2)| = 2\sqrt{2} > 2$.

Original Ekert's protocol and its simplified form

According to Ekert's protocol [3], Alice and Bob each obtain one particle from a pair of spin-1/2 particles in the entangled state. (In fact, it does not matter whether they share two entangled spin-1/2 particles or, e.g., two photons with entangled polarizations.) Alice and Bob perform measurements on their respective particles in three bases defined by three orientations of their measurement devices (e.g., Stern-Gerlach apparatuses). For simplicity let us suppose that they use only directions lying in the plane perpendicular to the trajectory of the particles. Alice's bases make angles with respect to the vertical $\theta_2 = \pi/4$, $\theta_3 = \pi/2$ and $\theta_1 = \pi/4$, and Bob's bases are $\theta_2 = \pi/2$, $\theta_3 = 3\pi/4$. For these values Bell's inequality states $|C(\hat{n}_1, \hat{n}_2) + C(\hat{n}_1, \hat{n}_3) + C(\hat{n}_2, \hat{n}_3) - C(\hat{n}_1, \hat{n}_2)| = 2\sqrt{2} > 2$. There are nine possible combinations. After the quantum full transmission, during which Alice and Bob randomly and independently set their measurement bases, the settings are publicly announced. When identical bases were used, the outcomes of their measurements are correlated and become the cryptographic key. The probability that Alice and Bob use the same basis is 2/9. An eavesdropper attempting to correlate his probe with the other two particles would disturb the purity of the singlet state, which would result in a smaller violation of the inequality or no violation at all.

A year later Bennett et al. [6] proposed a simpler entanglement-based protocol without invoking directly Bell's theorem. Here, both Alice and Bob choose only from two bases corresponding to two perpendicular orientations of their spin-measurement devices in a way very similar to BB84 protocol. In fact, the only difference from BB84 is that Alice does not send particles in a chosen spin (or polarization) state but she measures her particle from the entangled pair in one of two conjugated bases. She must select bases randomly and independently from Bob. The rest is the same as in BB84: After the transmission Alice and Bob compare their bases and keeps only those results when they used the same bases.

5. QBC protocols

Quantum bit commitment is a scheme in quantum cryptography that was developed to be unconditionally secure. There have been works that show that it is impossible [9] to have an unconditionally secure QBC scheme, nevertheless some holes in those impossibility proofs have been discovered [2] and such protocols will be presented.

The statement, underlying logic, and security of protocol QBCp3m can be simply presented as follows.

Let Alice send Bob a qubit in state $|\psi\rangle$ known only to herself, $|\psi\rangle = C|H_2^B\rangle$ in a fixed great circle C of the qubit Bloch sphere. Depending on $b = 0$ or 1 , Bob leaves it alone or rotates it to its orthogonal state $|\psi^\perp\rangle$, then sends it back to Alice among a number $n-1$ of random decoy qubit states. Independently of b , Alice can make the same qubit measurement of the basis $|\psi\rangle, |\psi^\perp\rangle$ on every of the n qubits before Bob opens. The protocol is still concealing with $\bar{P}_C^B \approx \frac{1}{2}$ as $n \rightarrow \infty$, because she does not know which qubit is the one she sent. It is clear that Alice cannot determine b any better by sending $|\psi\rangle = C|H_2^B\rangle$ or by entangling $|\psi\rangle$. Because Bob cannot gain any information on Alice's measurement basis via entanglement, his optimal cheating probability \bar{P}_C^A is given by an appropriate one-to-two clone fidelity p_A , which is independent of n and not arbitrarily close to 1. As he has to open 0 and 1 on two different qubits given Alice already measures, the optimality of p_A would be contradicted if he can do any better. Thus far, the quantitative claim of the impossibility proof, (IP) of $\bar{P}_C^B \approx \frac{1}{2} \Rightarrow \bar{P}_C^A \approx 1 \Rightarrow \frac{1}{n} \Rightarrow \bar{P}_C^A \approx 1 \Rightarrow \frac{1}{n}$ or (IP) $\lim_n \bar{P}_C^B \approx \frac{1}{2} \Rightarrow \lim_n \bar{P}_C^A \approx 1$ of, has been invalidated by the above protocol QBCp3m. More significantly, it shows that the impossibility proof formulation misses a whole class of protocols in which Alice can make the verifying measurement independently of b before Bob opens.

It is straightforward to extend QBCp3m to unconditionally secure protocols, such as QBC3m1 and QBC3m2, by having Alice send Bob a sequence of m independent $|\psi_i\rangle$'s with p_A^m set to any arbitrarily small value ϵ . Bob sends back each of the m uniformly modulated qubits in different restricted ways among n qubits. Alice makes the corresponding measurements before Bob opens. The resulting protocols are concealing with n sufficiently large for

any fixed m , which is determined by Bob's optimal cheating probability $\bar{P}_c^A = p_A^m$, and are thus fully unconditionally secure in the sense of $\lim_n \bar{P}_c^B = \frac{1}{2}$ and $\lim_n \bar{P}_c^A = 0$.

Protocol QBCp3m

- 1) Alice sends Bob a state $| \rangle$ known only to herself, randomly picked from a fixed known great circle C on the Bloch sphere of the qubit H_2^B
- 2) Bob modulates $| \rangle$ by $U_0 = I$ or $U_1 = R(\cdot, \mathcal{C})$, rotation of $| \rangle$ to its orthogonal state on C , for $b = 0$ or $b = 1$. He then picks $n - 1$ qubits with states independently and randomly chosen among all possible ones, and places the modulated qubit H_2^B randomly among them. He sends the n resulting qubits to Alice, each named by its position in the qubit sequence from 1 to n .
- 3) Alice measures $| \rangle, R, C | \rangle$ on each qubit. Bob opens by revealing the position of H_2^B and the bit value. Alice verifies by checking her measurement result on H_2^B .

Protocol QBCp3u

- 1) Alice sends Bob a state $| \rangle$ known only to herself, randomly picked from the four BB84 states on a fixed great circle C of the qubit H_2^B .
- 2) Bob modulates $| \rangle$ by $U_0 = I$ or $U_1 = R(\cdot, \mathcal{C})$ for $b = 0$ or 1 . He then picks $n - 1$ qubits with states independently and randomly from two orthogonal states known to Alice, places the modulated qubit H_2^B randomly among them, and sends the n qubits to Alice in a named order.
- 3) Bob opens by revealing the state of all the qubits and identifying H_2^B . Alice verifies by checking the corresponding projections.

Protocol QBC3m1

- 1) Alice sends Bob a product state $| \rangle | \rangle^1 \dots | \rangle^j \dots | \rangle^m, j = 1, \dots, m$, each $| \rangle^j$ named by its position and independently and randomly chosen from a BB84 state set S in C .
- 2) Bob modulates each and all $| \rangle^j$ by $U_0 = I$ or $U_1 = R(\cdot, \mathcal{C})$, then independently and randomly place the exact sequence among $N - 1$ qumodes, each a product of m qubits randomly distributed on S . He sends the N qumodes to Alice in a named order.
- 3) Alice measures the $m | \rangle^j, R, C | \rangle^j$ on each of the N qumodes. Bob opens by announcing which qumode is the modulated $| \rangle$ and the bit value. Alice verifies by checking her measurement result.

Protocol QBC3m2

- 1) Alice sends Bob a sequence of m qubits, each $| \rangle^j$ named by its position and independently and randomly chosen from a great circle C .
- 2) Bob modulates each and all $| \rangle^j$ by $U_0 = I$ and $U_1 = R(\cdot, \mathcal{C})$, then places each $U_b | \rangle^j$ independently and randomly among the j th of m succeeding N -sequences of qubits, the states of all the other qubits independently and randomly chosen. He sends the $n = mN$ succeeding qubits with their position names to Alice.
- 3) Alice measures $| \rangle^j, R, C | \rangle^j$ on the N qubits of the j th sequence for all j . Bob opens by revealing the positions of $U_b | \rangle^j$ and the bit value. Alice verifies by checking her measurement results on these qubits.

6. Conclusions

This paper presents a survey of most known quantum cryptographic protocols. Further research will include protocols evaluating and comparison, using such criteria as error possibility, quantum and classical memory bounds, noise sensitivity.

References

- [1] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing", Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India, December 1984, pp 175 - 179.
- [2] P. P. Busch, J. Lahati, P. Mittelstaedt, "The Quantum Theory of Measurement," Springer-Verlag, Berlin, LNP Vol. m2.
- [3] A. K. Ekert, "Quantum cryptography based on Bell's theorem", Physical Review Letters, Vol. 67, No. 6, 5 August 1991, pp 661 - 663.
- [4] C. H. Bennett, "Quantum cryptography using any two nonorthogonal states", Physical Review Letters, Vol. 68, No. 21, 25 May 1992, pp 3121 - 3124.
- [5] C. H. Bennett, F. Brassard, G. Brassard, L. Salvail, and J. Smolin, "Experimental Quantum Cryptography" Journal of Cryptology, 5/1, 1992, pp 3-28.
- [6] C. H. Bennett, G. Brassard, and N. D. Mermin, "Quantum cryptography without Bell's theorem", Physical Review Letters, Vol. 68, No. 5, 3 February 1992, pp 557 - 559.
- [7] A. K. Ekert, B. Huttner, G. Massimo Palma, and A. Peres, "Eavesdropping on quantum-cryptographical systems", Physical Review A, Vol. 50, No 2, August 1994, pp 1047-1056.
- [8] P. J. Edwards, "Quantum communication and computation in the 21st century: the second century after Marconi", IEEE Society Monitor, Vol 20. No. 4, 1995, pp 15-18.
- [9] H.-K Lo and H. F. Chau, "Is Quantum Bit Commitment Really Possible?", Physical Review Letters, Vol. 78, No. 17, 28 April 1997, pp 3410 - 3413.
- [10] M. Golovkins, "Ieskats kvan tu kriptogr ifij" Course paper, University of Latvia, 1998
- [11] Samuel J. Lomonaco "A Quick Glance at Quantum Cryptography", Cryptologia, Vol. XXIII, No. 1, 1999, pp 1 - 41
- [12] R. J. Hughes, W. T. Buttler, P. G. Kwiat, S. K. Lamoreaux, G. L. Morgan, J. E. Nordholt, C. G. Peterson, "Practical quantum cryptography for secure free-space communications", May 4 1999 (quant-ph/9905009).
- [13] A. Zeilinger, W. Tittel, G. Ribordy, N. Gisin, D. Deutsch, A. Ekert, D. Vincenzo and B. Terhal, "Quantum Information", Physics World, March 1998, pp. 33-57.
- [14] P. J. Edwards, "Quantum Cryptographic Key Distribution: 21st Century Technology", IEEE Society Monitor, Vol. 25, 2000, pp 25-28.
- [15] H. P. Yuen, "How Unconditionally Secure Quantum Bit Commitment is Possible", 2001 (quant-ph/0109055).