SECURE TRANSPORT OF UTC (CNM) THROUGH QUANTUM KEY DISTRIBUTION

Luis Adrián Lizama[1,2], Mauricio López Romero[1], Salvador Venegas Andraca[2], Eduardo De Carlos López[1]
[1]Centro Nacional de Metrología, El Marqués, Querétaro, México
[2]ITESM, Campus Estado de México, Atizapán de Zaragoza, Estado de México, México
{llizama, jlopez, edlopez}@cenam.mx, {svenegas, A00437591}@itesm.mx

Abstract: Oscillators are usually synchronized by means of a master reference oscillator in a local laboratory. In this paper we propose a secure synchronization method over a communication network. The protocol underlies in the context of Continuous Variable Quantum Key Distribution (CV-QKD), and is primarily used to distribute a cryptographic key by means of a measurement known in quantum optics as Quantum Non Demolition (QND), a technique to overcome the Heisenberg uncertainty. This kind of measurement is used here to enhance the CV-QKD properties in order to be applied to multiparty protocols that pursue a Group Key Agreement (GKA). Remarkably, when the group members hit the phase component of Alice´s key they can use it to synchronize an oscillator, allowing a scheme for the secure transport of UTC(CNM) trough quantum key distribution. The protocol named Full Quantum Key Distribution by Feedback Non Demolition (FQKD-FND) is Complete (C) in the sense that Alice and Bob contribute each other to construct a pair of mutual authentication keys, provided a full duplex quantum channel. We introduce a Mutual Reverse Reconciliation (MRR) method, so FQKD-FND preserves security properties of Direct Reconciliation (DR) and Reverse Reconciliation (RR) protocols, but it has an increased tolerance to noise of a lossy channel. FQKD-FND does not require a second quantum channel, neither the Local reference Oscillator (LO) to be sent. Due to the second transmitted key, the Feedback Non Demolition (FND) of the system can be used to monitor continuously the noise level of the channel, so an intruder can be exposed at every time.

1. INTRODUCTION

Quantum Key Distribution (QKD) is a technique that allows two parties, usually named Alice and Bob to share a common secret key to be used with cryptographic purposes [1,2]. The first QKD protocol was created by Bennet and Brassard in 1984, called BB84 [18]. In BB84, Alice prepares the elements of the key by means of eigenstates of two observables that don’t commute between them. BB84 uses polarization states of individual photons to send the key and Bob gets some elements of this key by passing the photons trough an appropriate filter. The protocol relies on the nonortogonality of the polarization bases used, because it implies the impossibility to distinguish deterministically between two nonorthogonal states. Because BB84 uses weak coherent pulses, the probability that an individual pulse contains more than one photon is different from zero. It constitutes a severe obstacle that limits the performance and distance of the secure transmission. So BB84 is hard to be compatible with the actual photonic networks.

Continuous variable quantum key distribution protocols work with modulated coherent pulses, which allow gigabit transmission speed and the use of available sources of light and detectors. The modulation of the continuous variable is Gaussian and can be done by coherent states or squeezed states. It has been showed that in both cases the secret information rate is the same and that do not depends on the level of squeezing of light [10]. Due to its greater facilities, the first continuous variable protocol GG02 uses coherent state modulation [3]. GG02 is a CV-QKD protocol that codifies the signal on amplitude quadratures of light. The uncertainty principle of Heisenberg prohibits measuring simultaneously both quadratures with complete precision. The optic signal operates at low intensities to ensure the overlap of quantum states. Among other disadvantages, implemented continuous variable protocols don’t offer quantum mutual authentication and is not possible to establish a jointed key, because the key goes from Alice to Bob. On the other hand, CV-QKD protocols are sensitive to the noise level in Reverse Reconciliation Protocols (RR) and to the losses of the channel in Direct Reconciliation Protocols (RR). Moreover the Local Oscillator (LO) is necessary to be sent trough another channel.

2. QUANTUM NON DEMOLITION (QND)

Quantum non demolition measurements constitute a technique to overcome the limitations imposed by the Heisenberg uncertainty. It allows that a measurement of a quantum state can be done repeatedly. The purpose of a QND device, usually named optical tap [4, 6], is to measure the same observable obtaining the same result. Therefore QND measurements imply repeatability. In a QND measurement, the noise fluctuations are directed to an observable, which is conjugated of one that contains the information.

QND measurements can be seen as a way to achieve noise free distribution of information codified on a modulated light beam. Several optical taps disposed in series over an optical line could extract information without degradation for users further down [5]. It is also possible to adjust the gain of the device in order to compensate the losses that occur on the line below. An amplifier optical tap can drive at the same time, losses and noise of the channel [6].

It is generally accepted as necessary conditions of the QND measurements the following inequalities: $T_S + T_M > 1$ (where T_M and T_S are the transfer rate of signal to quantum noise from the input signal to the meter and the signal outputs, respectively) and $V_{S|M} < 1$ (the quantum state of the signal is evaluated trough the conditional variance $V_{S|M}$ that left in the system after the measurement). In the ideal case of QND perfect we have $T_{S+M} = 2$ and $V_{S|M} = 0$ [6].

Suppose now that Bob wants to use the QND relationships to send Alice the elements of his key. Bob could use phase rotators to obtain the needed configurations. To send the elements of his key (Q_{B1} ó P_{B1}), Bob could attach any element of Alice´s key, Q_A or P_A. The choice of Bob is random, so it is harder for Eve to previously know the option used by Bob. For the present analysis, we will consider the following relationships (see Fig. 1):

$$\begin{gathered} Q_{B2} = Q_{B1} + fQ_A \\ P_{B2} = P_{B1} \\ Q_O = Q_A \\ P_O = P_A - fP_{B1} \end{gathered} \tag{1}$$

$$\begin{gathered} Q_{B2} = Q_{B1} \\ P_{B2} = P_{B1} + fP_A \\ Q_O = Q_A - fQ_{B1} \\ P_O = P_A \end{gathered} \tag{2}$$

where $f = \sqrt{G} - \sqrt{G}^{-1}$, and G is the gain of the QND device and depends on the operation frequency. From Eq. (1): $Q_{B2} = Q_{B1} + fQ_A$, is known that we can measure Q_A trough the meter beam Q_{B2}. The successful of the measurement is reached when we have a large signal to noise rate fQ_A/Q_{B1}, that is to say if f is large, the rate is large, given that $Q_{B1}$is on the level of vacuum noise. In fact, the ideal QND is reached when f is arbitrarily large. Now consider quadrature $Q_{B1}$is also modulated and contains the information of Bob´s key. Then we have $Q_{B1} = Q_V + Q_{MB}$, where Q_{MB} is due to Bob's modulation and Q_V is the noise at the vacuum level as before. Because the elements of Eq. (1) are in the same quadrature, we have $Q_{B2} = Q_V + Q_{MB} + fQ_A$. Hence it holds that the signal to noise rate $fQ_A/(Q_V + Q_{MB})$ is still large, allowing Bob to obtain Q_A. The same case applies to the output equation $P_O = P_A - fP_{B1} = Q_V + Q_{MA} - fP_{B1}$, whereby Alice obtains Bob´s quadrature P_{B1}. Therefore, Alice obtains Bob´s modulations and Bob obtains Alice's modulations.

3. FQKD-FND PROTOCOL

Our protocol suggests that CV-QKD and quantum non demolition measurement QND can be used jointly to distribute a key between two or more parties. Trough QND we can achieve not disrupting a quadrature component of Alice's key element, which in principle, can be either quadrature. So it allows the cascade distribution of an Alice's key element over a group of users [12]. But also, taking advantage of the symmetry of the QND measurement Bob can send Alice a key (in QND are used two source beams, which allow us to introduce and intercalate Bob´s key).

Let us describe the protocol for two users and later for three users. Then we will make the analysis of the security of the protocol and we will discuss other variants taking as parameter the squeezing factor of the light beams. Below we describe the steps of the protocol of Full Quantum Key Distribution by Feedback Non Demolition (FQKD-FND), FQKD for short (the Fig. 2 shows the general scheme of FQKD):

1. Alice sends Bob the elements of a key codified in the quadrature QA and the elements of another key codified in the quadrature PA.
2. Bob prepare the elements of a key codified in the quadrature Q_{B1} and the elements of another key codified in the quadrature P_{B1}. Bob performs a non demolition measurement trough an arrangement device QND^1 that corresponds to Eq. (1) or QND^2 that corresponds to Eq. (2), making this randomly. The input beam to the device is QA | PA and the meter beam is local to Bob QB1 | PB1. According to Eqs. (1) y (2), if Bob uses QND^1 he must measure the quadrature Q and if he uses QND^2 he must measure P, so Bob recover Alice's key element.
3. Bob sends back to Alice the output quadratures Q_O | P_O of the device $QND^{1,2}$ trough a full duplex channel. Alice chooses randomly to measure one of the quadratures Q_O | P_O [13-16].
4. Alice announces to Bob trough the public channel, which quadrature she chose in each measurement. Bob does not need announce his chooses because due to Eq. (1) and (2) Alice uses her measurements to know Bob's selections. Thus, if Alice reads her own quadrature in the feedback beam, Alice and Bob will share an Alice's key element. If Alice reads a quadrature different to her own in the feedback beam, Alice uses the QND relationships to obtain Bob's quadrature component. In this case, Alice and Bob share a Bob´s key element and also an Alice´s key element, previously obtained by Bob, which is an element of Alice's another key element sent in the orthogonal quadrature (see Table I, for simplicity we have assumed that *f*=1 in Eqs. (1) and (2)).
5. Alice starts a reverse reconciliation with Bob. The key distillation process finish once the key is amplified.

The quadrature values of Alice and Bob vary inside a previous agreed modulation variance. We have considered that, i.e. a positive quadrature leads a binary 1.

In FQKD we assume that despite the channel´s noise, Alice can discriminate between her modulation and the joint modulation performed by Alice and Bob trough the QND device. This means that when Alice receives a modulation that equals her own, this cannot be originated by the joint noisy modulation, and when Alice receives a modulation different from her own, by which Alice infers a joint modulation, this cannot be generated by her own noisy modulation, thus Alice knows she share a key element with Bob. Just remain considering that when Alice receives a modulation different from her own, it comes from a joint modulation or from a noisy joint modulation.

So, Bob's reconciliation process just has to manage the errors that come from the noise of the joint modulation. As Alice subtracts her key element of the joint modulation, it allows that the reconciliation process handle the total noise (from Alice and the channel) that is introduced to Bob's modulation. To correct transmission errors, Alice must remove her own received elements of the information flux of the reconciliation process, because they do not contain Bob's information. On her own, Alice does not require to modify the reverse error correction process. We call Mutual Reconciliation Process (MRR).this method where Alice and Bob correct in reverse their key element errors

4 MULTIPARTY FQKD

Some advantages of FQKD protocol are the following:

1. Mutual authentication, because it uses two keys: one from Alice to Bob, and other from Bob to Alice.
2. Increased tolerance to noise, because it has the properties of RR and DR reconciliation protocols [7,8,9].
3. It is not necessary to send the Local Oscillator (LO) signal. Alice and Bob could execute an initial routine to adjust his own LOs, through a confirmation of an initial authentication key.
4. At each measurement, Alice can sense the noise level of the channel. Thanks to Bob´s feedback, it is possible to detect the noise fluctuations of the channel that could lead to detect Eve.
5. FQKD can be generalized to a multiparty protocol, where participants try to establish a group key [5].

Let's take the case of three users, which appears executed in the Table II. Here, it will be necessary that in addition to Alice, Charles must publish his selections trough the public channel. For his location on the optical line, Bob is the appropriate to tell the others which category the group is. In this example, we distinguish three categories for a multipartite distillation key:

Category I. Key between Alice and Bob and key between Alice and Charles.

Alice reads $Q_A – Q_{B1}$ or $P_A – P_{B1}$ or $Q_A – Q_{C1}$ or $P_A – P_{C1}$: These are elements to reconcile a key between pairs, Alice and Bob and Alice and Charles, respectively.

Category II. Key between Bob and Charles.

1. Charles reads $Q_A – Q_{B1}$ or $P_A – P_{B1}$, Alice and Bob key elements. For Alice's measure there are two possibilities:

a) Alice reads $P_A – P_{C1}$: Alice can calculate P_{C1}. Alice joints all the elements PC1 of this category and composes a common secret key with Charles. Due to Bob´s announcements and encrypting a message with this key, Alice send to Charles the Q_A elements, by which Charles calculate the $–Q_{B1}$ elements. Now Bob and Charles can obtain a secret common key.

b) Alice reads $Q_A – Q_{B1}$: Alice and Charles have the same measurement ($Q_A – Q_{B1}$), so they can compose a common secret key. Due to Bob´s announcements Alice send to Charles the Q_A elements and Charles proceed to calculate the $–Q_{B1}$ elements, trough Bob and Charles can compose a secret common key.

2. Charles reads Q_A or P_A.

Bob and Charles have the same measurement (Q_A or P_A), so they can compose a common secret key, which is known by Alice.

Category III. Key between Alice, Bob and Charles.

Alice reads $P_A – P_{B1}– P_{C1}$ or $Q_A – Q_{B1}– Q_{C1}$, which contains Bob and Charles key elements. Alice knows that Bob and Charles have Q_A (or P_A). Bob and Charles know that Alice has $–P_{B1} – P_{C1}$ (ó $–Q_{B1} – Q_{C1}$). Bob knows P_{B1} (or $–Q_{B1}$) but unknowns $–P_{C1}$ (or $–Q_{C1}$). Charles knows $–P_{C1}$ (or $–Q_{C1}$) but unknowns $–P_{B1}$ (or $–P_{C1}$). In this category, Bob and Charles have the same Alice's quadrature Q_A (or P_A), by which they can compose a common secret key. With this key Alice, Bob and Charles can communicate confidentially. Now Bob and Charles can interchange their quadratures, so Bob send to Charles $–P_{B1}$ (or $–Q_{B1}$) and Charles send to Bob $–P_{C1}$ (or $–Q_{C1}$), then both calculate $–P_{B1}– P_{C1}$ and used it to authenticate Alice, since she has the component $–P_{B1}– P_{C1}$.

As we state at the beginning when Bob and Charles have the same Alice's phase quadrature, i.e. fourth column of Table II it can be exploited to synchronize an assigned oscillator.

4. CONCLUSIONS

It was described the FQKD protocol, which uses a reconciliation method called Mutual Reverse Reconciliation. MRR has the security properties of RR and DR protocols. FQKD can be generalized to a multiparty protocol. FQKD can be viewed as a secure synchronization method over a communication network given that the group members hit the phase component of Alice´s key, so they can use it to synchronize their local oscillator. Some experimental results show the feasibility of FQKD because there have been achieved values for the conditional variance ($V_{S|M}$) that goes from 0.70 to 0.85 and for cascade QND from 0.66 to 0.8 [5]. Moreover, values obtained for the information transfer (T_{S+M}) goes from 1.16 to 1.25 and 1.3 for cascade QND. In the case of squeezed meter beam T_{S+M} reaches 1.81 [11]. Although our protocol has not been implemented yet, we currently work in an implementation scheme using polarization beams over Cesium cells. Nevertheless we conceived the synchronization method to be applied to the phase quadratures of laser beams, which will require amplitude and phase modulators.

5. REFERENCES

[1] G. Assche. Quantum Cryptography and Secret-Key Distillation. Cambridge University Press. 2006

[2] Sergienko A. V. Quantum Communications and Cryptography. CRC Press. Taylor and Francis Group. 2006

[3] F. Grosshans et al. Quantum key distribution using gaussian-modulated coherent states. Letters to Nature. 421, 238-241, 2003.

[4] Grangier, Ph., Levenson, J. A. &Poizat, J.-Ph. Quantum non-demolition measurements in optics. Nature 396, 537-542, 1998.

[5] A. Levenson, K. Bencheikh. Repeated quantum non-demolition measurements, Applied Physics B 64, 193-201, 1997.

[6] S.F. Pereira, et. al. Backaction evading measurements for quantum nondemolition detection and quantum optical tapping. Phys. Review letters. Vol. 72, Number 2, January 1994.

[7] F. Grosshans and N.J. Cerf, Phys. Rev. Lett. 92, 047905 (2004).

[8] Nicolas Cerf, Philippe Grangier. Quantum cloning and key distribution with continuous variables. http://citeseerx.ist.psu.edu

[9] Frédéric Grosshans, Nicolas J. Cerf. Virtual entanglement and reconciliation protocols for quantum cryptography with continuous variables. Quantum Information and Computation, Vol. 0, No. 0, 2003.

[10] Frédéric Grosshans, Philippe Grangier. Continuous Variable Quantum Cryptography

Using Coherent States. Phys. Rev. Lett. Volume 88, Number 5, 2002.

[11] Ulrik L Andersen et. al. Quantum nondemolition measurement with a nonclassical meter input and an electro-optic enhancement. Quantum Semiclass. Opt. 4 S229, 2002.

[12] Monroy R., Steel G., Faulty Group Protocols. http://homepages.inf.ed.ac.uk/gsteel/group-protocol-corpus. Version 1.0, February 2007.

[13] Roland Karl Staubli and Peter Gysel. Crosstalk Penalties Due to Coherent Rayleigh Noise in Bidirectional Optical Communication Systems. Journal of Lightwave Technology, Vol. 9, No. 3. 1991.

[14] Jean-Pierre Goedgebuer, Andre Hamel, and Henri Porte. Full Bidirectional Fiber Transmission Using Coherence-Modulated Lightwaves. IEEE Journal of Quantum Electronics, Vol. 28. No. 12, 1992.

[15] Y. Kawamoto, T. Hirano, et. al. “Plug and Play” Systems for Quantum Cryptography with Continuous Variables. Quantum Electronics Conference, 2005.

[16] Y. Kawamoto, et.al. Controlling excess noise using acousto-optic modulator for quantum cryptography with continuous variables. Lasers and Electro-Optics, 2007 and the International Quantum Electronics Conference.

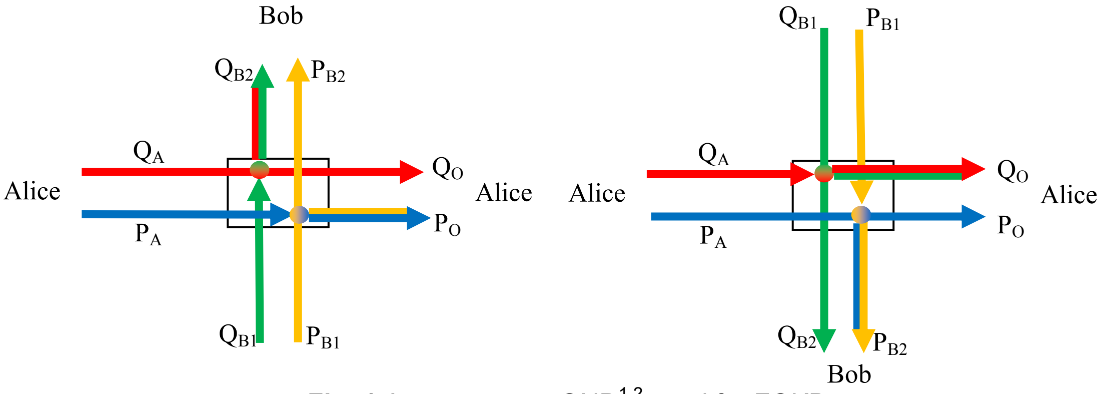

Fig. 1 Arrangements QND^{1,2} used for FQKD

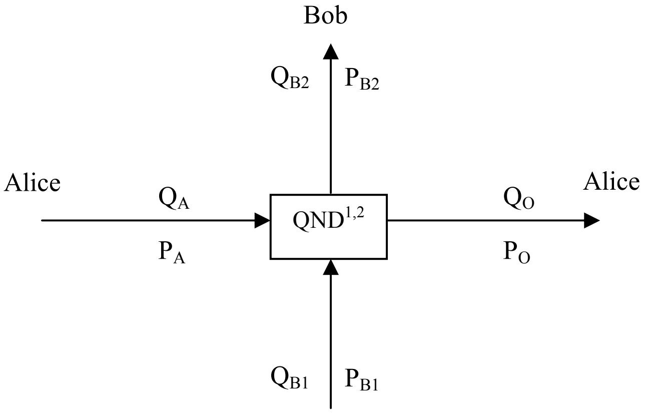

Fig. 3 General scheme of FQKD

Table I. An execution of FQKD protocol

Alice (preparation)		$Q_A \mid P_A$	$Q_A \mid P_A$	$Q_A \mid P_A$	$Q_A \mid P_A$	$Q_A \mid P_A$
Bob	QND[1,2]	${P_A}^2$	${Q_A}^1$	${Q_A}^1$	${P_A}^2$	${Q_A}^1$
	Back	$Q_A - Q_{B1} \mid P_A$	$Q_A \mid P_A - P_{B1}$	$Q_A \mid P_A - P_{B1}$	$Q_A - Q_{B1} \mid P_A$	$Q_A \mid P_A - P_{B1}$
Alice (measurement)		$Q_A - Q_{B1}$	Q_A	$P_A - P_{B1}$	P_A	$P_A - P_{B1}$

Table II. An execution of FQKD multiparty protocol (three participants)

Alice (preparación)		$Q_A \mid P_A$	$Q_A \mid P_A$	$Q_A \mid P_A$	$Q_A \mid P_A$	$Q_A \mid P_A$
Bob	QND	P_A	Q_A	Q_A	P_A	Q_A
	Feedback	$Q_A - Q_{B1} \mid P_A$	$Q_A \mid P_A - P_{B1}$	$Q_A \mid P_A - P_{B1}$	$Q_A - Q_{B1} \mid P_A$	$Q_A \mid P_A - P_{B1}$
Charles	QND	$Q_A - Q_{B1}$	Q_A	$P_A - P_{B1}$	P_A	$P_A - P_{B1}$
	Feedback	$Q_A - Q_{B1} \mid P_A - P_{C1}$	$Q_A \mid P_A - P_{B1} - P_{C1}$	$Q_A - Q_{C1} \mid P_A - P_{B1}$	$Q_A - Q_{B1} - Q_{C1} \mid P_A$	$Q_A - Q_{C1} \mid P_A$
Alice (medición)		$Q_A - Q_{B1}$	$P_A - P_{B1} - P_{C1}$	$P_A - P_{B1}$	P_A	$Q_A - Q_{C1}$