

THE IMPORTANCE OF TIME AND FREQUENCY REFERENCE IN QUANTUM ASTRONOMY AND QUANTUM COMMUNICATIONS

**Tommaso Occhipinti^{1,2}, Paolo Zoccarato¹, Ivan Capraro², Pietro Bolli³,
Filippo Messina³, Giampiero Naletto², Paolo Villoresi², and Cesare Barbieri¹**

¹Department of Astronomy, University of Padova, Italy

²Department of Information Engineering, University of Padova, Italy

³INAF Astronomical Observatory Cagliari, Italy

E-mail: {tommaso.occhipinti, ivan.capraro, giampiero.naletto,
paolo.villoresi}@dei.unipd.it
{paolo.zoccarato, cesare.barbieri}@unipd.it
{pbolli, messina}@ca.astro.it

Abstract

Very accurate and stable time tagging capabilities are fundamental for Quantum Astronomy and Quantum Key Distribution. The main task of Quantum Astronomy is to find particular signatures of different astrophysical emission mechanisms or scattering processes by measuring the statistics of the arrival time of each incoming photon. This line of research will be particularly important with future extremely large telescopes. On the other hand, Quantum Key Distribution (QKD) assures a secure cryptographic key sharing between optical transmitters and receivers through the synchronous exchange of quantum states (e.g., single polarized photons).

Both technologies need to detect the arrival times each photon with very high temporal resolution in order to discriminate the signal photons from the background ones. In this article, we present the activities of our research group on Quantum Astronomy and Quantum Key Distribution, taking into account their very strict requirements.

For Quantum Astronomy, we have developed an instrument called AquEYE capable of time-tagging each incoming single photon using as detectors four Single Photon Avalanche Diodes (SPAD). In this experiment, we need to maintain an absolute time scale reference with a maximum error phase less than 1 ns for measurements lasting more than 30 minutes. For the development phase of our instrument, we used an available rubidium oscillator disciplined by a GPS receiver. This system will supply the reference clock and trigger signal to our acquisition electronics, which are based on a time-to-digital converter. In the paper, we will present the more advanced solution we have under evaluation.

As we are also working in the realization of a QKD prototype, we will present our study on time and frequency stability of the local oscillators of the electronics. For the moment, we are using two simple quartzes, but in the article we will show the results of several mathematical simulations. With them, we will analyze the performance tradeoffs in terms of the final

Report Documentation Page				Form Approved OMB No. 0704-0188	
Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.					
1. REPORT DATE NOV 2007		2. REPORT TYPE		3. DATES COVERED 00-00-2007 to 00-00-2007	
4. TITLE AND SUBTITLE The Importance of Time and Frequency Reference in Quantum Astronomy and Quantum Communications				5a. CONTRACT NUMBER	
				5b. GRANT NUMBER	
				5c. PROGRAM ELEMENT NUMBER	
6. AUTHOR(S)				5d. PROJECT NUMBER	
				5e. TASK NUMBER	
				5f. WORK UNIT NUMBER	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) University of Padova, Department of Astronomy, Italy,				8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)				10. SPONSOR/MONITOR'S ACRONYM(S)	
				11. SPONSOR/MONITOR'S REPORT NUMBER(S)	
12. DISTRIBUTION/AVAILABILITY STATEMENT Approved for public release; distribution unlimited					
13. SUPPLEMENTARY NOTES 39th Annual Precise Time and Time Interval (PTTI) Meeting, 26-29 Nov 2007, Long Beach, CA					
14. ABSTRACT see report					
15. SUBJECT TERMS					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT Same as Report (SAR)	18. NUMBER OF PAGES 18	19a. NAME OF RESPONSIBLE PERSON
a. REPORT unclassified	b. ABSTRACT unclassified	c. THIS PAGE unclassified			

cryptographic key rate, through different synchronization techniques and frequency reference sources.

INTRODUCTION

MOVING TO QUANTUM MECHANICS

This paper describes the work of a research group composed by Engineers, Astronomers, and Physicists of the University of Padua (Italy) and Astronomical Observatory of Cagliari (Italy). The group is involved in two main innovative research topics, Quantum Astronomy (QA) and Quantum Communications (QC). Although superficially unrelated, both applications share their founding principles on the rules of Quantum Mechanics and precise time measurement and distribution.

In the past decades, Quantum Mechanics exited the realm of theoretical physics, touching with its implications and practical applications many aspects of today Information Technology. In several cases, it was brought even to a revolution as the implications of the four postulates of Quantum Mechanics [1] dramatically changed our vision on technological applications. We refer, for example, to the secure transmission of cryptographic keys or to the impressive speedup of some particular calculations into information machines based on quantum bits (*qubits*) and quantum logic gates [2].

With the designation “quantum system,” we mean a physical system whose behavior is strongly dominated by the rules of quantum mechanics, in contrast with a “classical system” obeying classical laws. Photons are the perfect example of such quantum system. In a great variety of scientific investigations and technological applications, the properties of photons can be studied and applied, considering what the previously mentioned four postulates of quantum mechanics describe. In particular, single photons are the most commonly used carrier of information in Quantum Communications.

For these reasons, it is possible to understand why, for example, a quantum receiver for QKD (Quantum Key Distribution [3] and a detector for Quantum Astronomy [9,10] are very similar. Both devices share a detecting front-end, where the single photon arriving from a quantum transmitter or an astrophysical source is converted into a voltage pulse, and a time-tagging apparatus that assigns to this pulse a temporal reference.

In order to understand the importance of time referenceS in Quantum Astronomy and Quantum Communication, the next two paragraph summarizes the two topics underlying the fundamental ideas and key properties.

SINGLE PHOTONS FROM ASTRONOMICAL SOURCES

Now that almost all wavelength regions are accessible to astronomy from ground and space, the thrust is moving towards higher temporal resolution. Numerous discoveries were made with temporal resolutions of milliseconds and slower: optical and X-ray pulsars; planetary occultations; cataclysmic variable stars; pulsating white dwarfs; flickering high-luminosity stars; X-ray binaries; gamma-ray burst afterglows; and so on. A limit for such optical studies has been that conventional CCD-like detectors do not readily permit frame-rates faster than 1-10 ms, while photon-counting detectors either had low quantum efficiency or else photon-count rates limited to no more than some hundreds of KHz. Nanosecond time resolution and time-tagging capability would enable entirely new studies of phenomena such as: variability close to black holes; surface convection on white dwarfs; non-radial oscillation spectra in neutron stars; fine structure on neutron star surfaces; photon-gas bubbles in accretion flows; and possible

free-electron lasers in the magnetic fields around magnetars [10].

Besides such applications in high-speed astrophysics, the final aim is to reach timescales sufficiently short to reveal the quantum-optical statistics of photon arrival times. Higher-order coherences of light may, in principle, convey information about the physics of light emission (e.g., stimulated emission as in a laser) or propagation (e.g., whether photons reach us directly from the source, or have undergone scattering on their way). Such properties of light have been studied for quite some time in the laboratory, but have not yet been applied to astrophysics. Such higher-order coherence of light can be measured from the arrival-time statistics of individual photons. For astronomically realistic passbands (1 nm, say), the required time resolution is on the order of picoseconds, much shorter than current photometric resolutions. On the more manageable nanosecond scales, the quantum effects are diluted, but still measurable, as demonstrated years ago by the Hanbury Brown-Twiss intensity interferometer, the [so far] only astronomical instrument that measured the second-order coherence of light. Using concepts related to this spatial intensity interferometer, analogous interferometry in the time domain (“photon-correlation spectroscopy”), already used in laboratory experiments, could be extended to the astronomical field to reach the spectral resolutions $\approx 10^8$ required to resolve known optical laser emission around Eta Carinae and other peculiar emission objects. We shall, therefore, present in the following our considerations about the possibilities to measure and distribute to several telescopes this very accurate time.

COMMUNICATING WITH SINGLE POLARIZED PHOTONS

The elaboration of information done with the help of quantum systems is often called Quantum Computation, while the communication of this information between different Quantum Computers is called Quantum Communication (QC), which is very often realized with the transmission of single polarized photons [3]. A particular form of QC solves even two problems: sharing a symmetric cryptographic key between the transmitter and the receiver and detecting the intrusion of an eavesdropper inside the communication channel. This technique is then called Quantum Key Distribution (QKD) or, more generally, Quantum Cryptography.

Quantum key distribution was proposed first by C.Bennet and G. Brassard in 1984 [4]. Since then, several implementations have been developed both in fiber and free space environment [5,6]. Each QKD protocol involves usually two communication stages between Alice and Bob (transmitter and receiver respectively). During the first stage, the transmission of the qubits takes place over a quantum channel. At this stage, Alice and Bob share a string of raw data that needs to be processed in order to distill a secure key. This is done by a public discussion over a classical channel. To complete this discussion Alice and Bob have to: (i) get the raw data (depending on the physical implementation, this could be done in different ways), (ii) delete double clicks and empty slots caused respectively by noise and attenuation on the channel, (iii) decide whether to keep or delete the remaining bits according to the protocol’s base measurement (sifting), (iv) correct the sifted key, and, finally, (error correction) (v) run the privacy amplification to reduce the information that Eve (the Eavesdropper) may have gained.

In general, to maximize the signal photon collection in a QKD system, three different filtering procedures, spectral, spatial, and temporal, are desirable. With the first one, we keep only photons of Alice’s wavelength (this can be achieved with standard optical filters); the second procedure ensures that only photons coming from Alice’s direction are collected (optical fiber or fine pointing in free space); the third is **temporal filtering**, which we now discuss in some detail. Temporal filtering means that it is essential to know that the measurement made by Bob at a certain instant t_1 corresponds exactly to the qubit sent at the instant t_0 by Alice. The strength of the method relies on the fact that security resides in fundamental laws of quantum mechanics, i.e. the no-cloning theorem that states the impossibility of cloning a quantum state. Therefore, by manipulating and transmitting, as well as measuring quantum states, there is no way to eavesdrop information without being visible.

TIME AND FREQUENCY REQUIREMENTS

After the previous short description of Quantum Astronomy and Quantum Cryptography, we outline now the requirements of both subjects in terms of the typical quantities of time and frequency reference science, such as: error phase, stability, and accuracy. Beforehand, we underline that both QA and QKD have to detect single photons from a natural source or from a quantum transmitter. Therefore, the main common requirement is a good stability and accuracy of the sampling component in the acquisition system. QA and QKD, in fact, share the electronic front-end system, which is essentially formed by some single photon detector that converts the real arrival time of the photon into a digital pulse (e.g., a Single Photon Avalanche Photodiode, SPAD) and a very high speed sampling element [7,8]. The output of this sampler, the digital arrival time information (absolute or relative), is given to top level software capable of storing the data, in order to achieve the purposes of QA and QKD.

SINGLE TELESCOPE QUANTUM ASTRONOMY

Quantum Astronomy needs to determine the arrival time of photons with a precision of 100 ps or better (the future target may be 1 ps) continuously for the entire duration of the observations, which can last from few seconds up to several hours.

In order to put these considerations to practical observational tests, we have built an instrument named AquEYE (the Asiago Quantum Eye), a prototype “quantum” photometer for the Asiago 182cm telescope. AquEYE must provide the time tags of the photons coming from different astronomical sources with an error phase of about 100 ps over exposure times as long as 3 hours. This requirement needs to be transformed in terms of oscillator specifications. Given the simple relation between *frequency offset* f_0 and *phase error* Δt , $f_0 = \Delta t/T$, where T is the measurement time (that we assume is 3 hours), the frequency offset required to satisfy the constraints on the phase error is $f_0 = 10^{-10}/10800 = 9,26 \cdot 10^{-15}$ for the 100-ps requirements and $f_0 = 10^{-12}/10800 = 9,26 \cdot 10^{-17}$ for the 1-ps requirements.

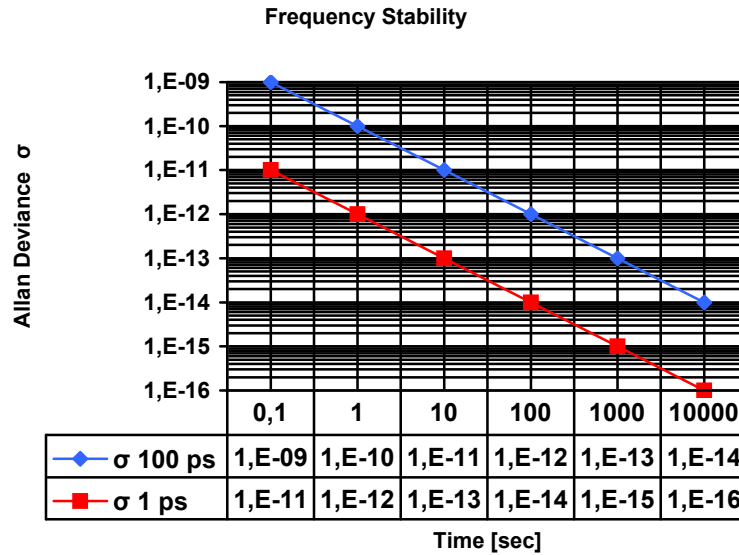


Figure 1. Oscillator frequency stability required for Quantum Astronomy. Acceptable values for 100 ps requirements lie below the blue line and for 1 ps lie below the red line.

Since there is no necessity for real-time processing, the requirements about frequency offset are not critical, because the frequency offset may be estimated and then removed in the data-processing phase. The minimum frequency stability required, i.e. the instantaneous deviation of the phase error from the phase offset, is depicted on Figure 1. The blue line is the upper limit for the requirements of 100 ps, while the red one is the one for the requirements of 1 ps.

The frequency reference unit available at present in Asiago is composed by a rubidium oscillator and a GPS receiver. The local oscillator is a FS725 rubidium frequency standard produced by Stanford Research Systems and the GPS receiver is the Mini-T produced by Trimble. The placing of the AquEYE units (acquisition electronics, time & frequency, and control) inside the Asiago-Cima Ekar Observatory is show in Figure 2-a, while Figure 2-b shows the positions of the GPS antenna now under investigation. At present, position number 2 is the preferred one for reducing multipath and augmenting the number of visible satellites (we paid attention to the presence of the big metallic dome).

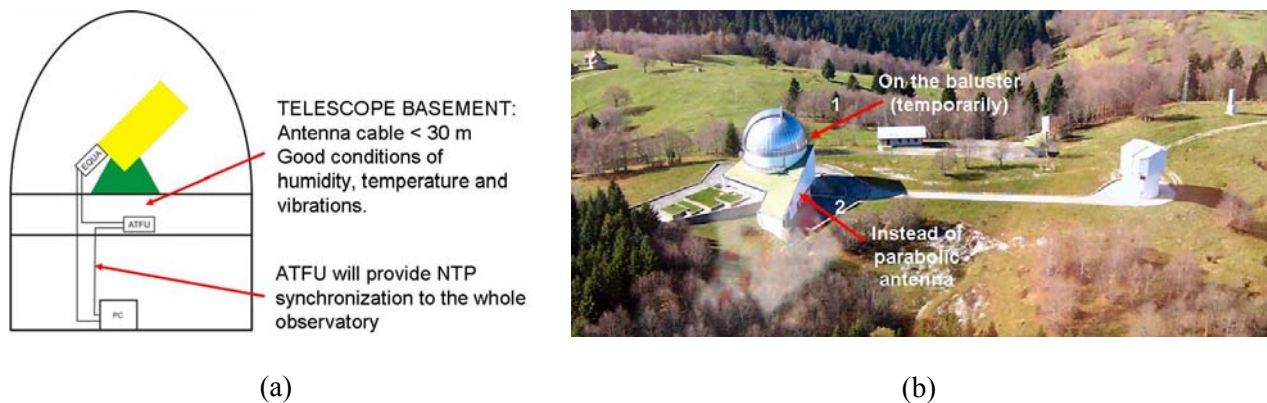


Figure 2. Disposition of AquEYE units at the Asiago AO of Cima Ekar (a) and positions of GPS antenna (b).

The Time & Frequency unit has been placed in the telescope basement because of worse environmental conditions in the dome, where humidity and temperature can exceed the specified values (the Observatory is at a 1340-m altitude).

LONG-DISTANCE OPTICAL INTENSITY INTERFEROMETRY

The second aim of AquEYE is to realize a modern version of the Hanbury Brown-Twiss intensity interferometry, with a baseline from Asiago to the Crni Vrh Astronomical Observatory of Ljubljana, at a distance of about 195 km.

In order to acquire good data for this particular form of Quantum Astronomy, it is important to achieve a very good relative synchronization between the two locations of acquisition. The better this synchronization, the easier the task of correlating the data will be.



Figure 3. Baseline between Asiago and Ljubljana AOs.

ACHIEVING TEMPORAL FILTERING FOR QUANTUM CRYPTOGRAPHY

The time and frequency requirements for communication (in particular, for Quantum Key Distribution) with quantum states encoded in single polarized photons are similar to the one for Quantum Astronomy, but they solve different necessities and tradeoffs typical of a communication system.

As previously said, the performances of QKD systems in the cryptographic key generation rate can be improved by using three filtering processes. Temporal filtering is crucially important for several reasons, in particular for noise reduction; rejecting the signals that arrive outside a well specified time windows will shield from unwanted detections. Moreover, it is important to exploit and benefit from the characteristics of the optical detectors used in the communication system. Single photon detectors, such as SPADs, after each detection have a dead time from 40 to 100 ns in which they can not detect any photon, and for this reason any unwanted detection has a double negative effect: it is unwanted as it decreases the final secure key rate, and it blinds the SPAD for the duration of the dead time, preventing the detection of a good photon.

Any QKD system, either in free space or based on optical fibers, can be run with or without the so-called *gated mode*. In the first case, the detectors run freely, getting everything they receive from the quantum channel. In the second case, the detector is switched on only when the arrival of one of the sent photon is expected (a substantial difference with the Quantum Astronomy operation). A picture illustrating the two situations can be found in Figure 4. Time synchronization is important for both methods: to assign a precise time tag or to open the gate of our receiver only at the right time. However, for Quantum Communications, the first method is exceedingly sensitive to noise for the previously mentioned reasons, and it is not considered feasible.

In conclusion, in QKD applications, it is extremely important to maintain a good relative time reference between the sender and the transmitter. We can synchronize Alice and Bob in many different ways, all of which can be enclosed in two distinct families: self-synchronization and external synchronization.

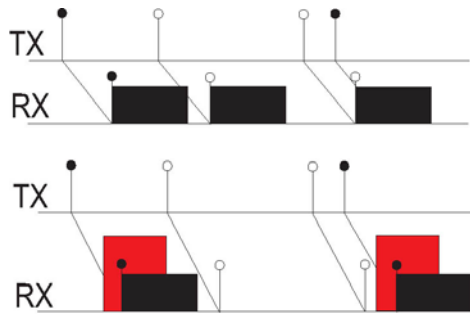


Figure 4. Transmitting/Receiving procedures, without and with the so-called “gated mode,” in which the detectors are open only when a transmitted photon is expected. (Red=Gates, Black= Dead time of the detectors).

• Self-synchronization:

Alice and Bob can extract the synchronization signal by the transmitted data as in many usual telecommunication schemes. Since in QKD we deal with single quantum state transmission and detection, that are probabilistic processes; an additional bright laser is needed to implement this kind of synchronization. The additional laser has to be carefully used, because it can blind the SPAD if used in the same time-slot as the single photon transmission [6,7].

• External synchronization:

In this case, both Alice and Bob have their own clock. As soon as the two clocks are relatively synchronized (same starting point), they can be used either for the photon tag in non-gated mode or for the gate signal reference in gated mode. The relative synchronization of the two clocks is normally done in advance by means of the use of Pseudo-Random Sequences and then adjusted during the communication phase [7]. Both methods have advantages and disadvantages and both have been developed in many experiments.

EXPERIMENTS AND PROTOTYPES

In this section, we describe two practical examples taken from our activities on Quantum Astronomy and Quantum Key Distribution. The already mentioned AquEYE instrument is a four-channel photometer that acquires the time tag of each incoming photon using four SPADs, a 35-ps-precision Time-to-Digital Converter (TDC), and a storing and control unit where all arrival times are stored for scientific analysis. Concerning QKD, we are developing a practical implementation of a B92 (Bennett 92) protocol communication system (called QuAKE) based on the free space propagation of the quantum states (single polarized photons). QuAKE is a network application, which starts from a physical layer where the creation and detection of the qubits is done, and implements also the data correction and final generation of the cryptographic keys.

The next paragraph describes the timing systems of AquEYE and QuAKE, underlying the engineering choices on oscillators and external UTC references, and showing our results.

QUANTUM ASTRONOMY INSTRUMENTATION

A rubidium-based main clock (see Figure 6) has been chosen to provide to the whole AquEYE system a

frequency and time reference. This rubidium oscillator assures stable and reliable performance with an accuracy of $\pm 5 \cdot 10^{-11}$. Different outputs are provided by the instrument: 10 MHz and 5 MHz sinusoid waves and the PPS (Pulse Per Second) signal; moreover, it can be phase-locked to an external PPS signal (like, for example, the reference provided by GPS allowing the synchronization with the Coordinated Universal Time (UTC)).

Since the astrophysical experiment will be performed exploiting the interferometry technique, a common synchronization is required. Therefore, together with the rubidium oscillator, a GPS receiver has also been purchased to discipline the rubidium to the UTC scale. It is well known that, whereas the rubidium in free-running shows a stable but not very accurate behavior, with the GPS synchronization, it becomes more accurate but less stable; in this section, we will quantify this concept through several measurements.

In order to measure the rubidium's performance, in terms of stability and accuracy, we used the "Time & Frequency Laboratory" of the Astronomical Observatory of Cagliari, Italy (see Figure 6). This laboratory, equipped with advanced instrumentation, participates in the calculation of the international time scales by sending its clock data to the BIPM (Bureau International des Poids et Mesures).

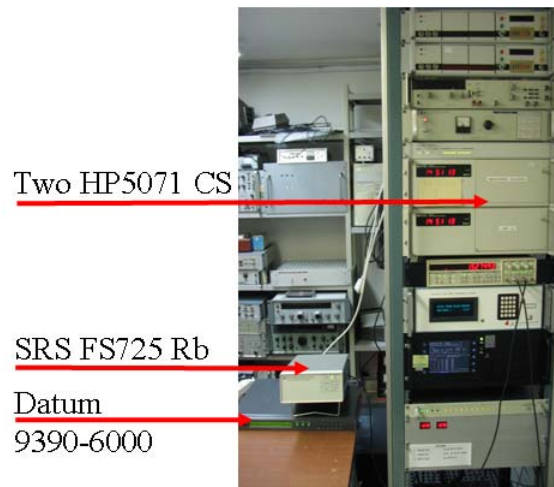


Figure 5. Time & Frequency Laboratory of the Astronomical Observatory of Cagliari.

It is worth noticing that in order to perform the calibration, the Device under Test (DUT), in our case the rubidium, must be compared to a standard that should outperform the DUT by a specified ratio in order for the calibration to be valid. This ratio is called the Test Uncertainty Ratio (TUR); if possible, a TUR of 10:1 is often a right choice. The Cagliari "Time & Frequency Laboratory" is equipped with two commercial cesium clocks (HP-5071A) that provide a practical realization of the second sufficiently accurate for our application. The time and frequency measurements required for the rubidium's characterization have been performed by the Time-Interval and Frequency Counter SR620 of Stanford Research Systems (hereafter abbreviated TIC). Briefly, the instrument's main performances are the single-shot timing resolution (25 ps) and its 1.3 GHz frequency range.

The first two setup measurements are sketched in Figure 7; on the left (Figure 7-a), one can see the characterization of the rubidium in the stand-alone configuration, whereas on the right (Figure 7-b), the atomic clock is disciplined by GPS. In both experiments, we adopted the cesium clock for the 10 MHz reference; moreover, the measurements were performed by comparing the time interval between two pps

signals: one provided by the rubidium and the other by the cesium. Data are recorded with a step of 2 seconds. Since the astrophysical experiment should be about 3 hours long, the data acquisition has been performed for the same interval time. Therefore, each file contains about 5000 samples.

The interval delay between the two pps signals are read by the TIC and then, via RS232, sent to a dedicated computer for the data acquisition. After that, offline, the commercial software Stable 32 has been used for data processing. During the postprocessing phase, we are able to convert data from phase to frequency domain, to remove outliers, to plot graphs, and to calculate basic and specialized statistics.

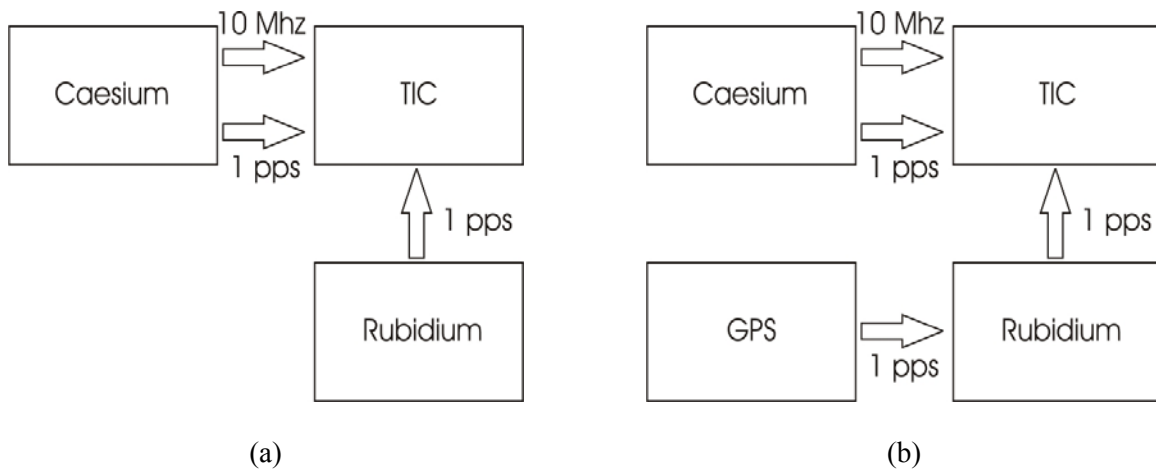


Figure 6. Two different measurement configurations.

Figure 8 shows the analysis of the configuration labelled (a). For phase data, we obtained a linear ramp with a slope of $2 \cdot 10^{-11}$, that also corresponds to the frequency offset (Figure 8-a). Therefore, the rubidium's behavior is a bit better than the accuracy declared in the data-sheet. On the other hand, after 3 hours, a total phase error of about 100 ns is seen. By removing such drift in the postprocessing phase, the curve of Figure 8-b is obtained. At this stage, the maximum error accumulated during 3 hours is reduced to about 3 ns.

We have evaluated also the Allan deviation, which describes the noise affecting data. In Figure 9, one can see this result, which agrees very well with those expected from the nominal data (see Table 1). The linear slope of the Allan deviation fits with the white frequency noise, which is the most common noise for a rubidium standard in the short term.

Table 1. Comparison of the Allan deviation between measured and declared values.

Integration time [Second]	From data-sheet	Measured
1	$< 2 \times 10^{-11}$	2×10^{-11} at 2 second
10	$< 1 \times 10^{-11}$	8×10^{-12}
100	$< 2 \times 10^{-12}$	1×10^{-12}

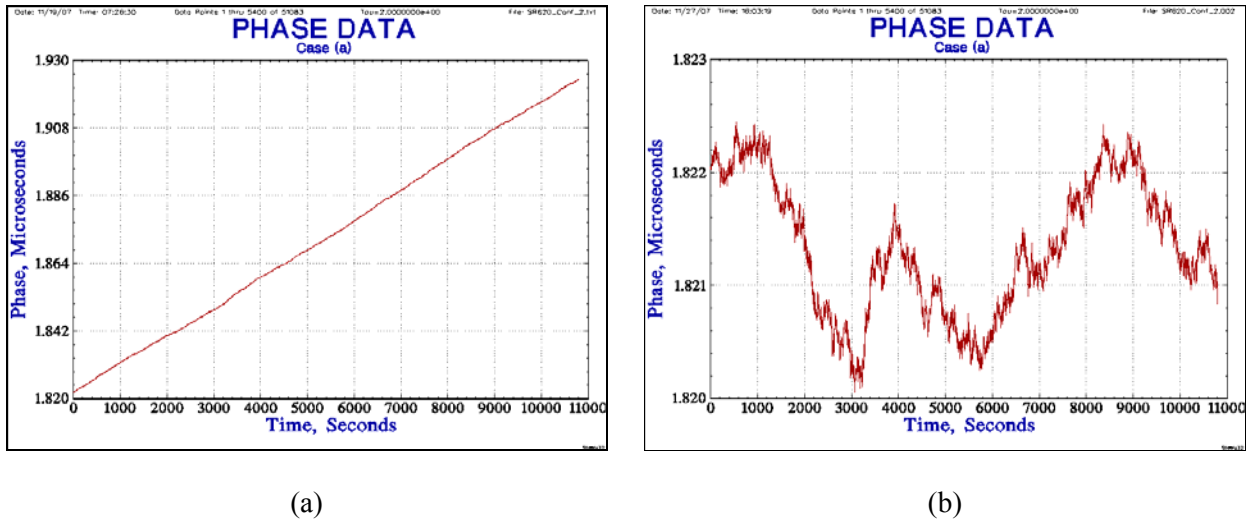


Figure 7. Three hours of phase data for the rubidium in free-running (a) and the residual stochastic error phase after removing offset and drift frequency (b).

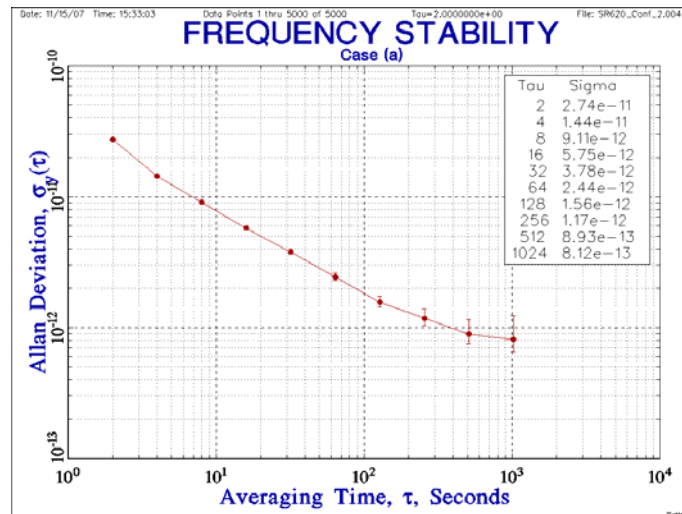


Figure 8. Allan deviation for the rubidium in free-running.

As a second step, we performed the same analysis for the configuration (b) of Figure 7. This configuration, although reducing the frequency offset, has the drawback of introducing stochastic noise, because the GPS periodically corrects the rubidium oscillation to keep it aligned as much as possible to the UTC scale.

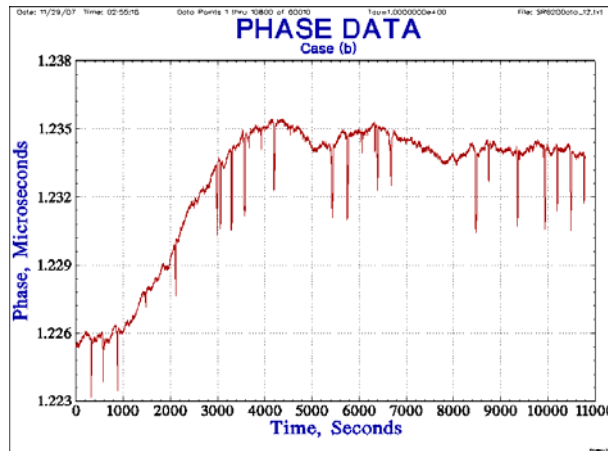


Figure 9. Three hours of phase data for the rubidium disciplined by a GPS pps.

The benefit of this configuration (see Figure 10) is that the maximum phase offset is limited, even for a very long period. For example, in this case, the total phase error is about 13 ns. On the other hand, the drawback is due to higher noise of GPS with respect to the rubidium. We are investigating the peaks visible in Figure 10 that could be the effects of the phase-locking circuitry of our rubidium accepting the disciplining pps in input. From these experiments, we believe it possible to maintain, with the available instruments, the phase error within 3 ns for the entire duration of the experiment (typically less than 4 hours).

On the other hand, another procedure can be adopted. It would consist of estimating, with the aid of GPS, the rubidium offset and drift, and correcting them in postprocessing, instead of disciplining the rubidium with the GPS directly. This configuration is useful also because the final setup of our experiment could not use the TIC instrument. Instead of it, we will take advantage of the precision of our scientific acquisition electronics based on a Time-to-Digital Converter (TDC, 25-ps resolution). The configuration for this purpose is shown in Figure 11, with the connection indicated by the red arrow.

The practical realization of this procedure may be affected by the fact that the reference frequency of the acquisition electronics is given by the rubidium oscillator itself. In any case, this problem should affect only the stability of pps measurements, making the pps differences noisier, but the offset estimation should be sufficiently accurate.

In order to verify the feasibility of the above solution, a case test has been realized in the Cagliari Laboratory. The 10 MHz from the rubidium oscillator has been used as reference frequency to the TIC that in this case stands for the TDC, and we have acquired the phase differences between the pps in input from the rubidium and the GPS, as shown in Figure 12, which we call the Operational Configuration.

The results of TIC measurements are shown in Figure 13. As expected, the data are very noisy; on the other hand, the estimated frequency offset is $1.2232 \cdot 10^{-11}$, with a phase error of about 110 ns. This value is of the same order of the frequency offset determined with the frequency reference given by the cesium oscillator, namely $2 \cdot 10^{-11}$.

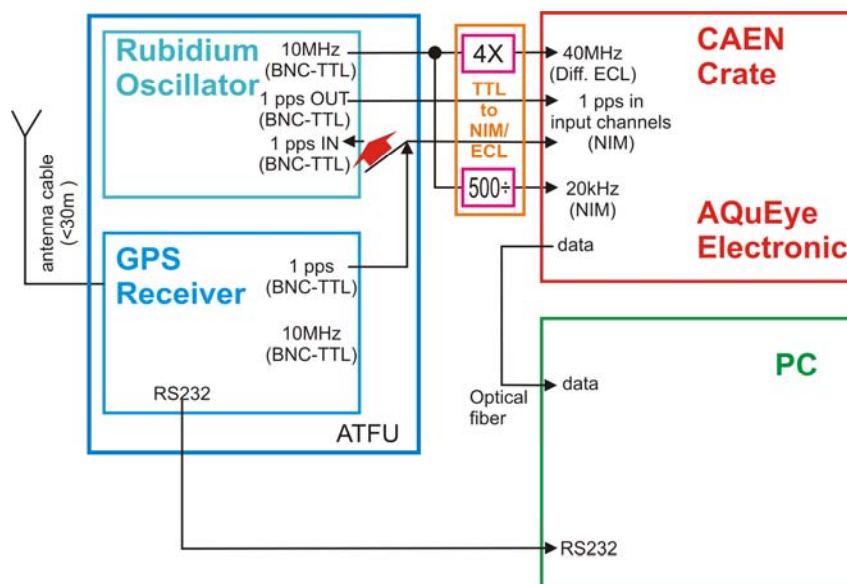


Figure 10. Connection of Acquisition Electronics, Time & Frequency, and Control units.

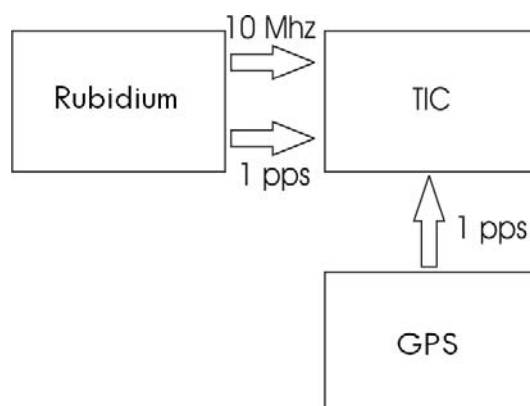


Figure 11. Operational Configuration.

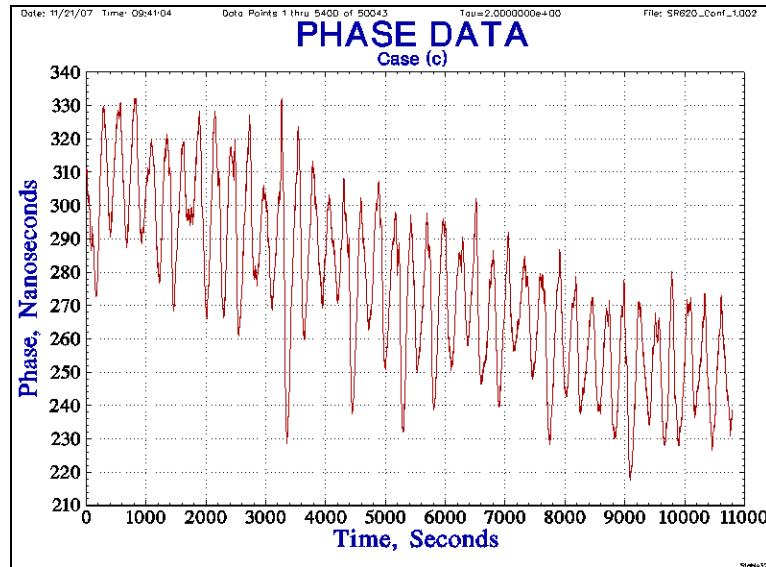


Figure 12. Phase data for the operational configuration.

QUANTUM KEY DISTRIBUTION EXAMPLES

Self-Synchronization Example

The self-synchronization is the technique we have chosen for QuAKE [7,11]. It is composed by two entities, namely ALICE and BOB linked by a quantum channel and by a public classical channel. The channel for quantum transmission is a free-space channel. Some peculiar features of QuAKE are the presence of a fully functional Adaptive Optics (AO) system for the correction of atmospheric-induced beam wandering, the use of generic TCP/IP networks as channel for public discussion, and the use of an FPGA (Field Programmable Gate Arrays) as electronics for control and synchronization. In the system, there is also high-level software, written in Java, for error correction, privacy amplification [4,11], and interfacing with top-level applications like cryptographic and networks security programs.

We implemented the self-synchronization procedure using a third laser, called the synchronization laser, in addition to the two quantum-signal lasers that are required for a B92 protocol. The lasers share a common optical path in order to transmit information about the timing of the system.

The third laser, pulsed at 1.25 MHz, is used to synchronize the transmitter and the receiver and to open the gates at the right moment. We organized the classical communication in frame and slots: a slot corresponds to a pulse of the transmitting laser, whereas a frame is a collection of 512 slots. Each communication consists of 512 frames. The number of slots and frames are communicated using a pulse duration modulation (PDM) of the synchronization laser changing its duty cycle. The clock reference is instead transmitted using on-off modulation (OOK) of the same laser during the transmission.

At the receiver, we use an FPGA (a Xilinx ML403 board equipped with a Virtex 4 FX chip) in order to acquire and store the data. The system takes the 1.25 MHz signal coming from the APD (Avalanche Photodiode) that converts the synchronization signal from the optical domain into an electric signal and a 100 MHz clock coming from a local oscillator inside the ML403 Board. With the help of a DCM (Digital

Clock Manager), we multiply by 3 the input 100 MHz clock and then we sample the signal coming from the APD. Doing so, we create a copy of the synchronization clock and other faster clocks that can be used for the generation of the Gate signals.

At every creation of a cryptographic key, the system starts decoding the frame code; then a sequence of synchronization signals and single photons are sent alternatively. Due to the fact that the transmitter and the receiver are synchronized, the FPGA can easily generate the signal GATE and open the detectors just when needed (see the next figure).

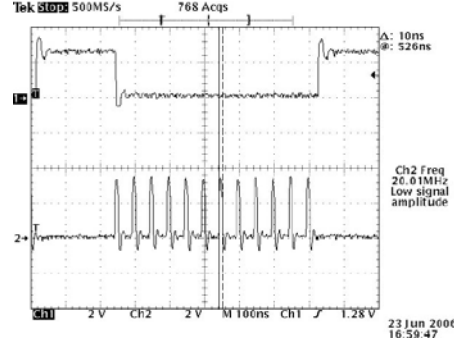


Figure 13. The first signal in this oscilloscope is the synchronizing clock (1.25 MHz); the second is the gate functions for the detectors (SPADs).

External Synchronization Example

In external synchronization, we let the transmitter and the receiver to run freely, but we establish a shared time reference by the use of external clocks. In order to test how the precision and stabilities of the time reference influences a QKD system, we developed a faint-pulse free-space channel QKD Matlab simulator, but the same general results are valid for optical fiber and also different quantum state transmission technologies (i.e. Entangled Photons protocols [6]).

The Matlab simulation starts from a sequence of pulses of duration T_{on} ; the number of photons per pulse has been implemented like a Poissonian random variable with mean μ . The transmission rate of the quantum states is simulated at a frequency F given by Alice's clock taking into account the attenuation of the channel and losses at both transmitter and receiver due to misalignment. At the receiver, Bob's clock is the time base for the generation of the gating pulses for the detectors. (The time duration of these pulses is T_{gate} .) These can be moved with respect to the signal pulses' (as shown in the next figure) arrival times by adjusting a programmable parameter.

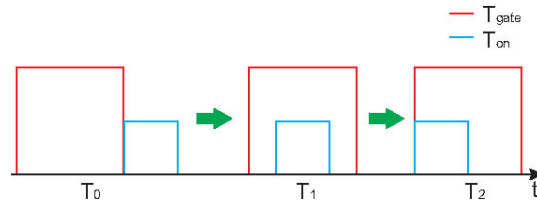


Figure 14. The transmitted single photons can be in any position inside the T_{on} rectangles. The gating functions, represented by red rectangles, can be placed in all the configurations above.

After the bits are shared between Alice and Bob, all the steps of the QKD protocol can run. For the purposes of this work, only the sifting procedure are taken into consideration, since error correction and privacy amplification will introduce only a scaling factor into the final key length (this is not true if there is noise in the system). In our simulation, we have also kept the ratio between T_{on} and T_{gate} constant. The aim of the investigation is the characterization of the system performances when the gate position is determined by a non-ideal clock (as this clock directly generates the gating functions' starting time and duration) for different T_{on} and T_{gate} , assuming a common start between the two clocks. This assumption is due to the fact that, with a postprocessing analysis of a pseudo-random sequence previously shared, it is always possible to get a useful precise common start. The clocks we have investigated are reported in Table 3.

Table 2. Oscillator parameters adopted for generating the simulated phase error.

Oscillator Type	Allan Deviation					Frequency
	1sec	10sec	100sec	10 ³ sec	10 ⁴ sec	offset
TCXO	$1 \cdot 10^{-9}$	$0.5 \cdot 10^{-9}$	$0.5 \cdot 10^{-8}$	$1 \cdot 10^{-7}$	$1 \cdot 10^{-6}$	$5 \cdot 10^{-7}$
OCXO	$1 \cdot 10^{-10}$	$3.16 \cdot 10^{-11}$	$1 \cdot 10^{-10}$	n.a.	n.a.	$5 \cdot 10^{-9}$
Rb	$2 \cdot 10^{-11}$	$1 \cdot 10^{-11}$	$2 \cdot 10^{-12}$	n.a.	n.a.	$5 \cdot 10^{-11}$
GPSDO TCXO	$1 \cdot 10^{-9}$	$3 \cdot 10^{-10}$	$3 \cdot 10^{-10}$	$2 \cdot 10^{-10}$	$1 \cdot 10^{-12}$	$1 \cdot 10^{-12}$
GPSDO OCXO	$2 \cdot 10^{-11}$	$2 \cdot 10^{-11}$	$3 \cdot 10^{-12}$	$2 \cdot 10^{-12}$	n.a.	$5 \cdot 10^{-14}$
GPSDO Rb	$1 \cdot 10^{-11}$	$2 \cdot 10^{-12}$	$4 \cdot 10^{-13}$	$2 \cdot 10^{-13}$	n.a.	$5 \cdot 10^{-14}$

The values of Allan deviation and frequency offset are simulated starting from commercial apparatus. The simulations are represented in the next three figures. On the x-axis, the value 0 means that the rise front of the signal pulse T_{on} coincides with the rise front of the Gate T_{gate} . It is possible to see the ideal case when we expect the convolution shape function between the pulse and the gate function and the non-ideal cases with different oscillators. We can see from the figures that, as T_{gate} increases, the difference between different oscillators becomes less evident. Considering a real QKD setup, we would like to open the gate just before the arrival of our photon; this means that we are in the flat part of these curves.

With a $T_{\text{gate}} = 5$ ns, all the clocks but the TCXO behave like the ideal case, given the half-convolution shape. With a $T_{\text{gate}} = 1$ ns, the GPS-disciplined TCXO starts to behave differently from the ideal case, but still works good in the flat part of the curve. The GPSDO-TCXO is no more valid for $T_{\text{gate}} = 100$ ps, demonstrating that, for very precise gating, a better clock like a OCXO or a GPSDO-OCXO is needed. This demonstrates the importance of the choice of the clocks and the impact it can have on the performances of the system.

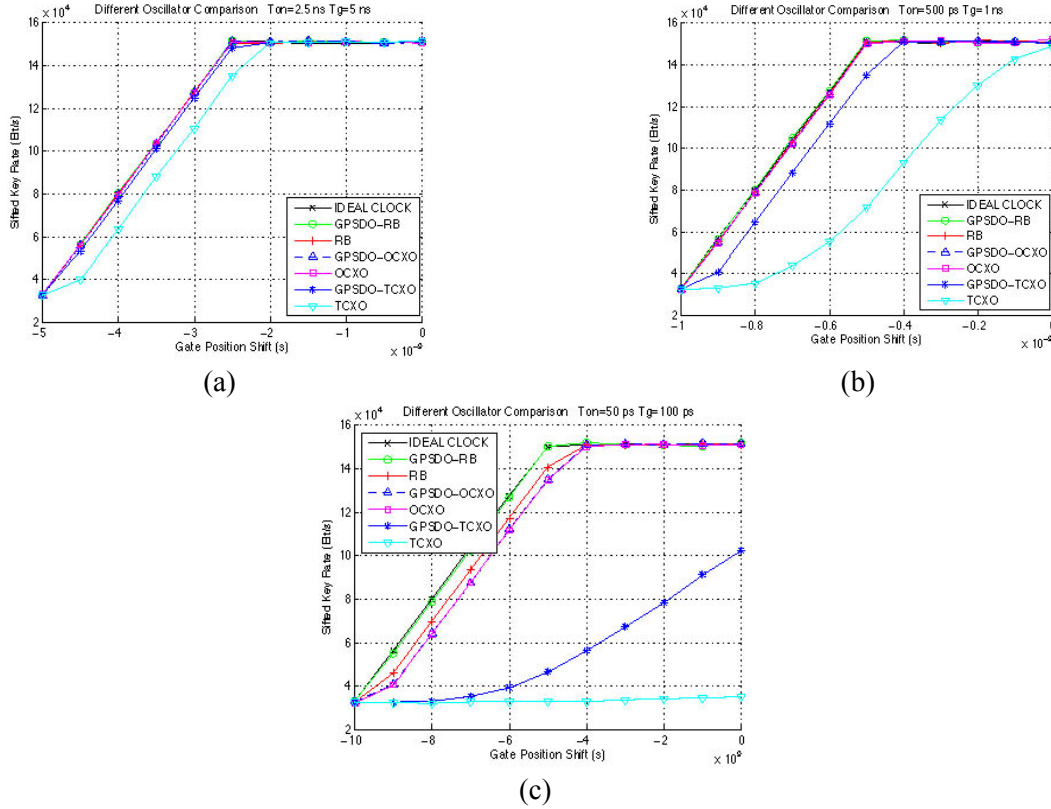


Figure 15. Length of generated shifted keys for a gate time of 5 ns (a), 100 ns (b), and 100 ps (c) for the several kinds of simulated oscillators.

ACKNOWLEDGMENTS

Our work is supported by: the Harrison Project (GNSS Supervisory Authority), PRIN2006 (Italian Ministry of the University and Research), and Fondazione CARIPARO-University of Padova.

CONCLUSIONS

In this work, we have described our activities on Quantum Astronomy and Quantum Key Distribution. Starting from a brief introduction to them, the article presented the requirements for their time and frequency references. Even if QA and QKD are quite different, they share common techniques and devices in the detection units. Getting the arrival time of single photons is a difficult operation and it needs a very accurate and stable time and frequency reference. The time information is important for comparing the measurements in different places and to accurately correlate the acquired data, while the stability of the frequency generator assures the precision of the time tagging. As the QA timing requirements are very stringent, it is important to outline that in the future this scientific investigation will need an oscillator of the hydrogen maser class. This clock or even a more stable solution will assure good results, as the precision of the measurement will reach the picosecond level and the experiment itself will last many hours. Accepting observation for hundreds of minutes with a less stringent precision will allow use of a rubidium clock and a GPS timing receiver. Concerning Quantum Key Distribution, where the accuracy of the reference oscillator is a critical value because of the real-time operational mode, we

analysed only one particular way of implementing the protocol (B92 in free-space channel). In this case, a GPSDO-TCXO or an OCXO can be a good compromise in terms of performances and costs, assuring an acceptable final cryptographic key rate.

REFERENCES

- [1] P. A. M. Dirac, 1958, **The Principles of Quantum Mechanics, IV** (Oxford University Press, Oxford).
- [2] M. A. Nielsen and I. L. Chuang, 2000, **Quantum Computation and Quantum Information** (Cambridge University Press, Cambridge).
- [3] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, 2002, “*Quantum Cryptography*,” **Reviews of Modern Physics**, **74**, 145–196.
- [4] C. H. Bennett and G. Brassard, 1984, “*Quantum Cryptography: Public Key Distribution and Coin Tossing*,” in Proceedings of the International Conference on Computer, Systems, & Signal Processing, 1984, Bangalore, India, pp. 175-179.
- [5] J. C. Bienfang, A. J. Gross, A. Mink, B. J. Hershman, A. Nakassis, X. Tang, R. Lu, D. H. Su, C. W. Clark, and C. J. Williams, 2004, “*Quantum key distribution with 1.25 Gbps clock synchronization*,” **Optics Express**, **12**, 2011-2016.
- [6] C. Kurtsiefer, P. Zarda, M. Halder, P.M. Gorman, P.R. Tapster, J.G. Rarity, and H. Weinfurter, “*Long Distance Free Space Quantum Cryptography*,” **Proceedings of the SPIE**, **4917**, 25-31.
- [7] I. Capraro, T. Occhipinti, P. Zoccarato, C. Bonato, F. Tamburini, C. Barbieri, and P. Villoresi, 2007, “*The utilization of the GALILEO timing signals for Quantum Communications*,” in Proceedings of the 1st Colloquium Scientific and Fundamental Aspects of the Galileo Programme, 1-4 October 2007, Toulouse, France, in press.
- [8] P. Zoccarato, T. Occhipinti, C. Facchinetti, P. Bolli, F. Messina, I. Capraro, F. Tamburini, A. Dalla Torre, R. Zanello, A. Cadez, and C. Barbieri, 2007, “*The utilization of the GALILEO timing signals for advanced astronomical applications*,” in Proceedings of the 1st Colloquium Scientific and Fundamental Aspects of the Galileo Programme, 1-4 October 2007, Toulouse, France, in press.
- [9] C. Barbieri, D. Dravins, T. Occhipinti, F. Tamburini, G. Naletto, V. Da Deppo, S. Fornasier, M. D'Onofrio, R.A.E. Fosbury, R. Nilsson, and H. Uthas, 2007, “*Astronomical applications of quantum optics for extremely large telescopes*,” **Journal of Modern Optics**, **54**, 191-197.
- [10] C. Barbieri, V. Da Deppo, M. D'Onofrio, D. Dravins, S. Fornasier, R.A.E. Fosbury, G. Naletto, R. Nilsson, T. Occhipinti, F. Tamburini, H. Uthas, and L. Zampieri, 2006, “*QuantEYE, the Quantum Optics Instrument for OWL*,” in Proceedings of **The Scientific Requirements for Extremely Large Telescopes**, IAU Symposium 232, 14-18 November 2005, Cape Town, South Africa (Cambridge University Press, Cambridge), pp. 506-507.
- [11] I. Capraro and T. Occhipinti, 2008, “*Implementation of a Real Time High Level Protocol Software for Quantum Key Distribution*,” in Proceedings of the 2007 IEEE International Conference on Signal Processing and Communications, 24-27 November 2007, Dubai, UAE, in press.

- [12] C. Zucca and P. Tavella, February 2005, “*The clock model and its relationship with the Allan and related variances,*” **IEEE Transactions on Ultrasonics, Ferroelectrics, and Frequency Control**, UFFC-52, 289-296.
- [13] M. A. Lombardi, L. M. Nelson, A. N. Novick, and V. S. Zhang, 2001, “*Time and Frequency Measurements Using the Global Positioning System,*” **Cal Lab International Journal of Metrology**, July-September 2001, pp. 26-33.
- [14] C. Audoin and B. Guinot, 2001, **The Measurement of Time: Time, Frequency and the Atomic Clock** (Cambridge University Press, Cambridge), ISBN: 0-521-0039-70, 346 pp.
- [15] B. W. Parkinson and J. J. Spilker (eds.), 1996, **Global Positioning System: Theory and Applications, Vols. I-II, Progress in Astronautics and Aeronautics, 163** (American Institute of Aeronautics and Astronautics, Reston, Virginia).
- [16] R. Mannucci and F. Cordara, 2007, **Misurare il tempo e la frequenza** (Editrice Il Rostro, Segrate, Italy).