International Journal of Quantum Information
© World Scientific Publishing Company

PRACTICAL QUANTUM KEY DISTRIBUTION USING POLARIZATION ENTANGLED STATES

FABIO A. BOVINO, PIETRO VARISCO, ANNA MARTINOLI, PAOLO DE NICOLO,
SANDRA BRUZZO, ANNA MARIA COLLA, and GIUSEPPE CASTAGNOLI

Quantum Optics Lab, Elsag spa, Via G. Puccini 2
I-16154 Genova Italy
quantum@elsag.it

GIOVANNI DI GIUSEPPE

Department of Physics, University of Camerino
I-62032 Camerino (MC) Italy
gianni.digiuseppe@unicam.it

ALEXANDER V. SERGIENKO

Quantum Imaging Lab, Department of Electrical & Computer Engineering and Physics,
Boston University, 8 Saint Mary's St.
Boston MA 02215 USA
AlexSerg@bu.edu

Received (Day Month Year)
Revised (Day Month Year)

We present the architecture and recent experimental results for a Quantum Key Distribution system realized at Elsag spa Quantum Optics Laboratory with a key distribution rate suitable for practical industrial applications. The current system can reliably distribute secure cryptographic keys at a rate of 1,500 bit per second and higher at few hundred meters, with Quantum Bit Error Rate lower than 1%.

Keywords: Quantum Key Distribution; entangled-photon source; User Unit; synchronization; software architecture; Quantum Bit Error Rate; visibility.

1. Introduction

In a previous paper [2] we described a system, developed at Elsag spa, for quantum cryptographic key generation and distribution (QKD). The aim of our research was to demonstrate the feasibility of industrially relevant quantum cryptographic systems by producing a two-user prototype, with a key generation rate useful for real practical use, i.e. above 1 kbit/sec at increasing inter-user distances. Our prototype is based on the implementation of BB84 protocol [1] using polarization-entangled states transmitted over single-mode fibers at the wavelength of 830 nm.

In this paper we present the progress of the prototype and recent experimental results.

2. System Description and Operation

The prototype consists of a server (in charge of general communication management, production and distribution of sequences of entangled photons pairs) and few user units, each connected to the server through an optical fiber quantum channel, besides the traditional public communication channel (in the current setup, a LAN running Elsag's proprietary middleware MWP$^{\mathrm{TM}}$).

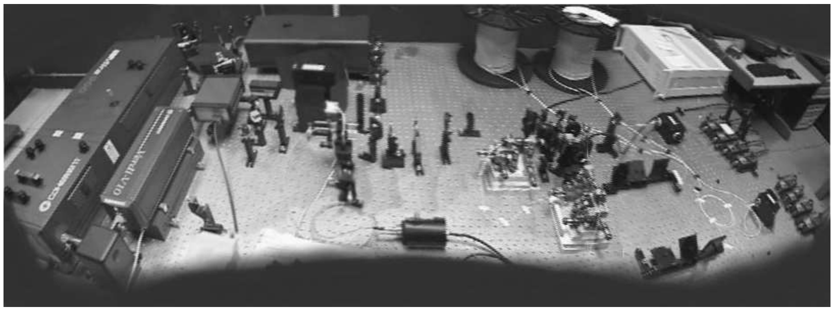

Fig. 1. A view of the experimental set-up.

In our experimental setup, a 3mm BBO crystal (Type II SPDC) is injected by a 415 nm pulse obtained by doubling a mode-locked laser (MiraVerdi system, 830 nm), operating in ultrafast regime (70–120fs) with a repetition rate of 76 Mhz. The temporal width of the pulses is controlled by changing the bandwidth of the mode-locked laser. By temporal engineering [2] we eliminated the decoherence effects due to the clock of the pump pulse and we obtained entangled states with high fidelity. In one arm of the interferometer a $\lambda/2$ wave plate rotates the polarization of 90° before the polarizing beam splitter (PBS). The paths are bent introducing a *"trombone"* to control the length of one arm of the interferometer, thus making it possible to erase the temporal distinguishability due to the crystal birefringence.

Entanglement engineering and high coupling efficiency [3] allowed us to achieve a high-rate production of high-fidelity entangled states even with low average power pump pulse (4–20mW), namely 565 entangled photon pairs/second per milliwatt of pumping power per mm of crystal.

Each User Unit (UU) is endowed of an integrated polarization measurement device and of four single photon avalanche detectors (PerkinElmer AQR14 SPAD). Polarization controllers are used for each UU. The SPAD's output is sent to a timestamp unit (Fast P7888 Time-of-Flight card) through a custom, in-house developed Coincidence Unit (CU), built around a programmable MAX7000 chip by Altera. The proprietary synchronization scheme [a] is based on a bright optical pulse sent by the Server to each UU. When the UU receives the bright pulse, there is a very

[a] Patent Application N. TO2004A00165, March 2004.

high probability to have all the detectors firing at the same time. However, a more conservative option was implemented in the CU, allowing to select a 3-fold rather than 4-fold coincidence. The CU output provides the start signal for the timestamp card, which begins to store in the timestamping list the arrival times, relative to the start, of the incoming stop pulses from the four SPAD's, together with the 2-bit address of the firing channel.

On the software side, the Server Unit consists essentially of a single process, the *QKD Server*, that manages the Initial Protocol for starting a key generation process between two Users in the network. Each User Unit is implemented with a client/server architecture (Figure 2). Friendly Graphical User Interfaces (GUI) are available to start and to monitor the whole key distillation process.

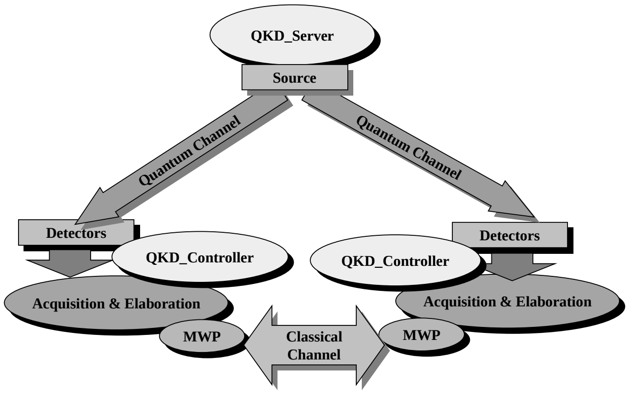

Fig. 2. Software Architecture.

The *QKD Controller* process, activated at the User Unit start-up in order to guarantee the network service, executes the Initial Protocol with the QKD Server of the Server Unit. The two QKD Client processes are *QKD Acquisition* and *QKD Elaboration*. The former executes sifting and QBER estimation on the data from the quantum channel (each data block corresponds to a data acquisition batch by the UU hardware, typically 100 msec); the latter executes error correction, privacy amplification and authentication [4]. The key generation session goes on until either the key produced has reached the size chosen by the operator, or a stop request is received.

A powerful feature of the software system is the possibility for administrator users to change some internal parameters on-line during key generation in order to improve the overall performance. Moreover, the system administrator can execute a-priori off-line performance tests on the quantum channel data in order to choose the most appropriate parameter values. Another key point of the system is the possibility of integration within different operative scenarios according to customer's requirements, with additional functionalities such as Key Distillation Monitoring and Quantum Channel Data characterization.

3. Experimental Results and Discussion

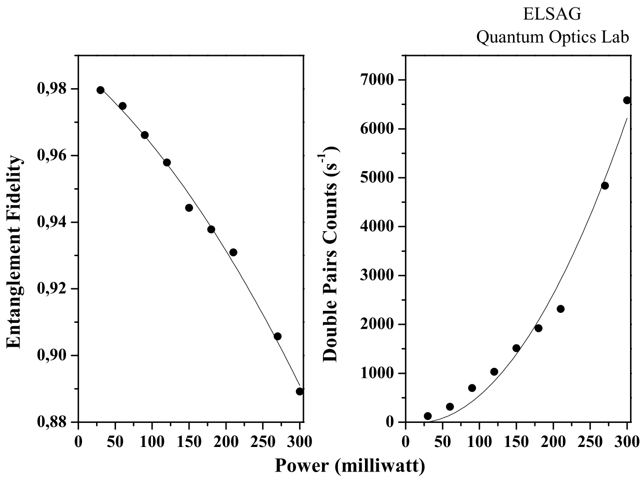

Fig. 3. Entanglement Visibility (left) and double pair counts (right) vs. pump power.

We have essentially worked in two directions: (a) obtaining an efficient entangled photon source with low average pump power for possible miniaturization; and (b) maintaining polarization entanglement along the fibers for an extended distance aiming at networks of practical use.

(a) Our experimental results show a quadratic dependence of visibility on the average power of the UV pump laser. The reduction of entanglement visibility in short fibers is practically only due to double pairs emission. Since the lower limit for single emission events coincides with the level of multi-particle events in the same measurement (Fig. 3), there is a straightforward method to discriminate the latter, as they cause the simultaneous click of two (or more) detectors on the same User Unit: we can simply discard these events from the time stamping list, which is used for subsequent key distillation.

(b) We have successfully demonstrated the preservation of polarization entanglement along the fibers with increasing inter-user distances. Fig. 4 shows the interference patterns for inter-user distances of 475 m and 2,000 m respectively. These patterns can be seen as the “quantum” analogue of *“eye diagrams”* in classical communications. The birefringence of the fibers degrades entanglement visibility introducing Polarization Mode Dispersion (PMD). High fidelity (visibility >97%)

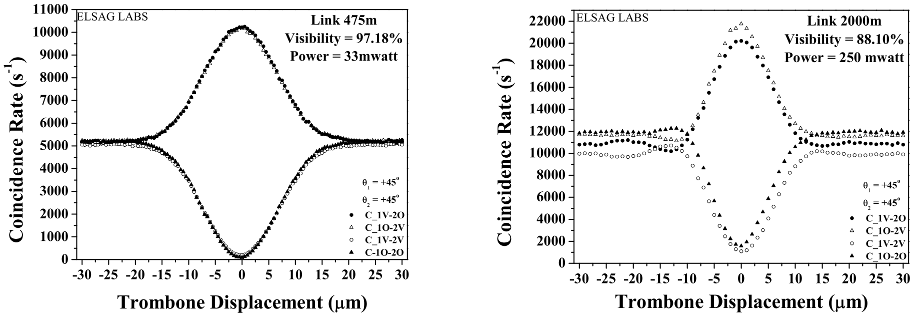

Fig. 4. Experimental results with an inter-user distance of 475 m. (left) and 2,000 m. (right).

was however recovered by simply using a group velocity compensator. For 2,000 m link we obtained a visibility >88%.

Concerning the whole system, key generation tests were performed adopting a rather low-end configuration: private 100 Mb LAN, User Units running on 1,6 GHz Pentium 3 machines, Server on 450 MHz Pentium 3. For users separated by 450 meters (coincidence rate 7%, QBER ∼ 1%) the system features sustained performances of more than ***1,500*** **bits/sec** of secure key. Several randomness tests run on the obtained keys were totally successful. The enhancement with respect to previously reported results [2] is essentially due to optimized re-design of the software libraries, along with accurate error rate estimation.

The above results are crucial for practical implementation of quantum key distribution protocols by entangled states. By temporal engineering and high coupling efficiency we obtained highly entangled states in femtosecond regime using a long crystal and very low average pump power. This can be a good starting point for future source miniaturization. We also proved that decoherence can be controlled up to distances relevant to some industrial applications (hundreds of meters). However, in order to implement a practical QKD system working at LAN dimension, it is necessary to increase entanglement visibility at long distance beyond the current results. We are currently investigating frequency engineering of the source in order to produce a narrow bandwidth emission. Another research direction concerns the adoption of new types of fibers currently under development.

Finally, the optimized software, developed at industrial standards, grants practical use of the system, enhanced throughput of the whole key generation process and robustness.

Acknowledgements

This work was developed within a Project funded by the Italian Ministry of Education, University and Research (MIUR), Grant N. 67679/ L.488/92.

References

1. C.H. Bennett and G. Brassard, in *Proc. Int. Conf. On Computer, Systems & Signal Processing*, Bangalore, India (1984), pp. 175-179.
2. F. A. Bovino *et al.*, in *Proc. SPIE's Aerosense 2003*, n. 5105-02, Orlando, USA (2003).
3. F. A. Bovino *et al.*, *Optics Communications* **227**, pp. 343-348 (2003).
4. A. M. D'Angelo, R. Dell'Eva, H. Inamori, A. Martinoli, *Journal of Modern Optics* **48**(13), pp. 1943–1956 (2001).