OPTOELECTRONICS AND ADVANCED MATERIALS – RAPID COMMUNICATIONS Vol. 4, No. 11, November 2010, p. 1840 - 1843

Classical and quantum communications in grid computing

M. DIMA*, M. DULEA, D. ARANGHEL, B. MITRICA, M. PETRE, M. STOICA[a], M. UDREA[a], R. STERIAN[b], P. STERIAN[b]
National Institute for Nuclear Physics and Engineering, P.O. Box MG-6, RO-077125 Bucharest-Magurele, Romania
[a]National Institute for Laser and Plasma Physics, P.O. Box MG-6, RO-077125 Bucharest-Magurele, Romania
[b]Polytechnical University, P.O. Box MG-6, RO-077125 Bucharest, Romania

The Quantum Crypted GRID Port developed under the D11-044 QUANTGRID project financed by the Romanian Center for Programme Management CNMP is presented: specifically the technology developed and the proprietary software used in the project. Quantum crypted communications eliminate the possibility of quantum-computer deciphering of messages (Shor's Lemma), while functioning with a public key exchange scheme – being secure by the very essence of quantum nature: any quantum state measured in any way collapses into one of its projections, thus it cannot be cloned and impossible to keep a copy thereof. The distribution of quantum public key is hence similar to the Vernam cipher (symmetrical – with secret key). The ongoing activities in this technology pertain to GRID communications through optical fiber and allow to optimise the quantum security technology and experiment proprietary algorithms for optimum data-volume/security for this new type of communications.

(Received May 5, 2010; accepted November 10, 2010)

Keywords: Quantum crypted optical communications, AES encryption, Sockets communications

1. Introduction

Communications' security today relies mostly on public (asymmetric) key algorithms: hash functions easily computed directly and asserted as impossible in reverse. Base assumption to this is the difficulty of factorising prime numbers, which received however a serious blow in 1994 (Peter Shor – quantum computer algorithm with a polynomial algorithm), rendering RSA, DSA, etc decipherable in the possible future. G. Vernam (AT&T, 1926) has shown the use of a hash function key (equal in length to the message) to guarantee communication safety. Symmetric key protocols however exhaust the hash tables and the communication partners need to re-establish contact to exchange a new set of tables: the Key Distribution Problem. Quantum Key Distribution (QKD) is secured by the very essence of the quantum nature: quantum states measured in any way collapse into one of the projections and cannot be re-generated, cloned, or copied, therefore they are by nature similar to the Vernam cipher. In Europe this has attracted attention as a means of immunisation against Echelon interception [1].

The technology here presented is based on polarised photon states of 2-3 photons. The key is encoded in the phase difference between two pulses traveling from Bob to Alice and back. Bob emits a (1550 nm) laser pulse that is split in two pulses by the (Ist, 50/50) beam splitter: one traveling through the long arm (phase modulating) long arm of an unbalanced interferometer and the other through the short (90^o rotating) short arm. All Bob fibers and optical elements are polarisation maintaining. The two pulses exit the Bob station through a polarisation beam splitter and travel to Alice, where they are reflected by a Faraday mirror, the second pulse phase modulated, both attenuated and sent back to Alice. Their return paths at Bob are complementary to the incoming ones (auto-compensated setup). In the long arm Bob applies a phase modulation on the first pulse (corresponding to the detection basis). The pulses recombine in the beam splitter and are detected here or after passing through the circulator.

2. "Quantgrid" equipment

A number of component providers [2] exist on the market, the setup here presented being based on Clavis2 components [3] from ID-Quantique, which offer the possibility of further configuration modification and future experimentation. The setup (Fig. 1) consists of the Bob station (receiver), the Alice station (sender), a 23.845 km (quantum channel) optical line between Alice and Bob for the secret key, 2 dedicated computers handling the Bob and Alice stations and a LAN Ethernet (classical channel) connection between the computers for the encrypted data. The components are described below:

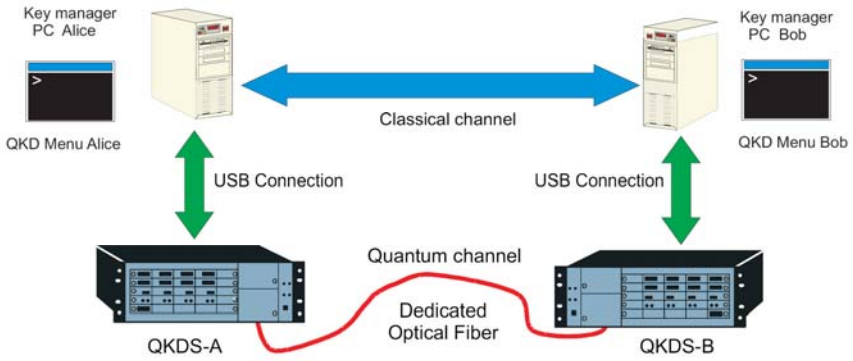

Fig. 1. Communication line setup with two dedicated computers (Bob – receiver and Alice – sender). The quantum channel (23.845 km) is a dedicated optical fiber line, while the classical channel is via LAN Ethernet.

Bob station (receiver) – for an auto-compensated setup, the information Alice sends is physically produced by Bob: intense laser pulses, which are sent to Alice, reflected back (phase modulated) and detected by Bob as receiver. After the laser the pulses are split and enter an unbalanced interferometer: one half through the long arm and the other through the short one, after which they are further recombined at an exit phase beam-splitter. On the return way from Alice the pulses take complementary paths and the long arm applies the phase modulation corresponding to Bob's decision for a measurement basis. They then interfere and are detected with the single-photon detectors (avalanche photodiodes in Geiger mode). Polarization maintaining fibers are used throughout.

Components:

- Laser Diode: pulse energy = -17 dBm @ 500ps, pulse duration = 300-2500 ps, power = measured with photodiode
- 2 Photon-Counting Detectors: bias voltage controlled (2), dead-time on/off and duration (FPGA controlled)
- Phase modulator: with phase voltage control (0, π)
- Optical Components: circulator, coupler, polarization splitter.

Electronics:

- mainboard – used for handling of high level functions. On-board microcontroller providing USB interface, running temperature regulation, and dedicated PortC and I2C for communication with other electronic components (FPGA and ADC/DAC I2C compatibles, temperature sensor, etc). The FPGA controls 4 different pulsers, DAQ, formatting and storage. An on-board acquisition channel monitors component operations.
- laser, phase modulator and detector boards – dedicated to optoelectronic interfacing, mainly for specific driving functions in accordance to the optoelectronics they drive (gating and/or temperature regulation).

The electronics performs five main tasks:

1. *Status monitoring and hardware parameter storage* – monitoring of power supplies, APD cooler current/temperature, etc, mainly by the microcontroller.
2. *Laser diode control* – duration and timing of pulses through an FPGA driven pulser mode (mainboard implemented). Temperature regulation and laser power measurement are performed using the internal photodiode of the laser.
3. *Phase modulator control* – duration and amplitude setting of phase modulation pulses through an FPGA driven pulser mode (mainboard implemented). Two different states are possible: zero/adjustable amplitude state (state 0/1).
4. *Photon-counting detectors control* – independent setting of bias voltage for each detector. A current source embedded on the detector board (mainboard microcontroller steered), regulates the detector temperature to -50^{o} C and allows control of the duration and timing of the gates applied on the APD, by sensing avalanches and converting them on FPGA captured detections.
5. *Transfer of bit values for key exchange* – retrieval of random bits generated by the mainboard embedded random generator. The 2 bits values are sent sequentially to the phase modulator board, for storage in embedded memory together the detector1/2 counts, then sent to the controlling PC via USB/microcontroller.

Alice station (sender) – although not directly, physically, producing the pulses, it encodes them by modulating the phase of the second pulse half. The pulses from Bob are split at input by a 10/90 coupler, with the bright part (90%) directed to a classical detector which provides the timing for gating and scrutinizes the incoming signal for intensity variations from potential eavesdroppers (Trojan Horse attack: intense signal injection for phase modulator probing, i.e. - for the sent information). The weak part (10%) is directed into the "quantum emitter": variable optical attenuator (set to guarantee "faint photon" level of the pulses sent to Bob), long delay line (12 or 24

km, preventing spurious detections caused from Rayleigh backscattering), phase modulator (acting on the second half of each pulse) and Faraday mirror (ensuring passive compensation of polarisation mode dispersion effects in the optical link on a round-trip).

Fig. 2. Communication line setup used in the QUANTGRID D11-044 project (Inst. For Laser and Plasma Phys. – Bucharest), with its two dedicated computers (Bob – receiver and Alice – sender). The quantum channel (23.845 km) optical fiber spool is on top of the Bob station. The classical channel linking the computers is local LAN Ethernet.

Components:

- Variable optical attenuator (dual channel): attenuation 1.5 - 50 dB, channel 1 (at quantum emitter input), channel 2 (in front of the classical detector)
- Classical Detector: bias voltage 30 - 60V, 2 discriminators (detection of Bob's pulses and monitoring of incoming – Trojan Horse attack guard)
- Phase modulator: phase voltage with 4 values (0, $\pi/2$, π, $3\pi/2$)
- Optical components: delay line, coupler, Faraday mirror.

Electronics:

- mainboard – handling high level functions, it includes a microcontroller providing the USB interface, running a dedicated 8 bit interface to the FPGA and an I2C bus for communications with other electronic components (DAC, ADC, temperature sensor, etc). An FPGA controlling four different pulsers, data acquisition, formatting and storage before sending them to the PC is used. The peripheral boards enclose components with mainly specific driving functions according to the optoelectronic they have to drive (gating and/or temperature regulation), and an acquisition channel which is used to monitor component operations.
- detector and phase modulator boards – dedicated to optoelectronic interfacing, with components having mainly specific driving functions according to the optoelectronics they drive (gating and/or temperature regulation), and an acquisition channel which is used to monitor component operations.

The peripheral boards perform the following tasks:

1. *Status monitoring and hardware parameter storage* – monitoring of power supplies, temperature and storage for availability to the controlling computer.
2. *Variable optical attenuator control* – by the two variable optical attenuators. The stepper motor attenuator is controlled through an I2C bus.
3. *Classical detector control* – used to set bias voltage and threshold levels of the two discriminators connected to detector output. Synchronization output signal of the discriminators is fed back into the high-level electronics.
4. *Phase modulation* – voltage setting for the four phase values (one for each state) via DAC and multiplexer. Precise timing of the actuation comes from the delay of the timing signal from the classical detector.
5. *Transfer of bit values for key exchang* – retrieval of random bits generated by the embedded random generator on the mainboard. The 2 bit values are sent sequentially to the phase modulator, there stored on embedded data memory and sent to the controlling PC (through the microcontroller and USB bus).

3. Crypting protocol and proprietary software

The key exchange procedure is shown in Fig. 3 (the BB84 protocol [5], described in detail elsewhere). Given the secure key-exchange we can now proceed with the communications' technology and afferent crypting protocols. We developed two proprietary C++ technology packages: **SXV4** (for sockets communications) and **AXV4** (for AES crypting conforming to FIPS-197), the performance of both being shown in Fig. 4.

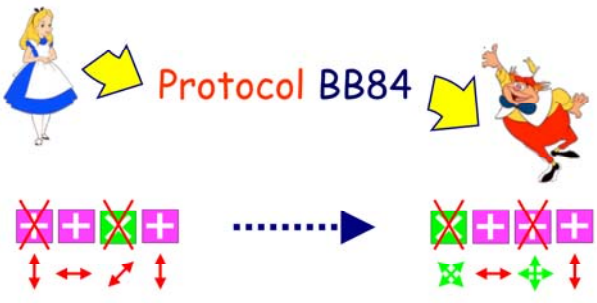

Fig. 3. Implementation of the BB84 protocol with polarised faint photon pulses.

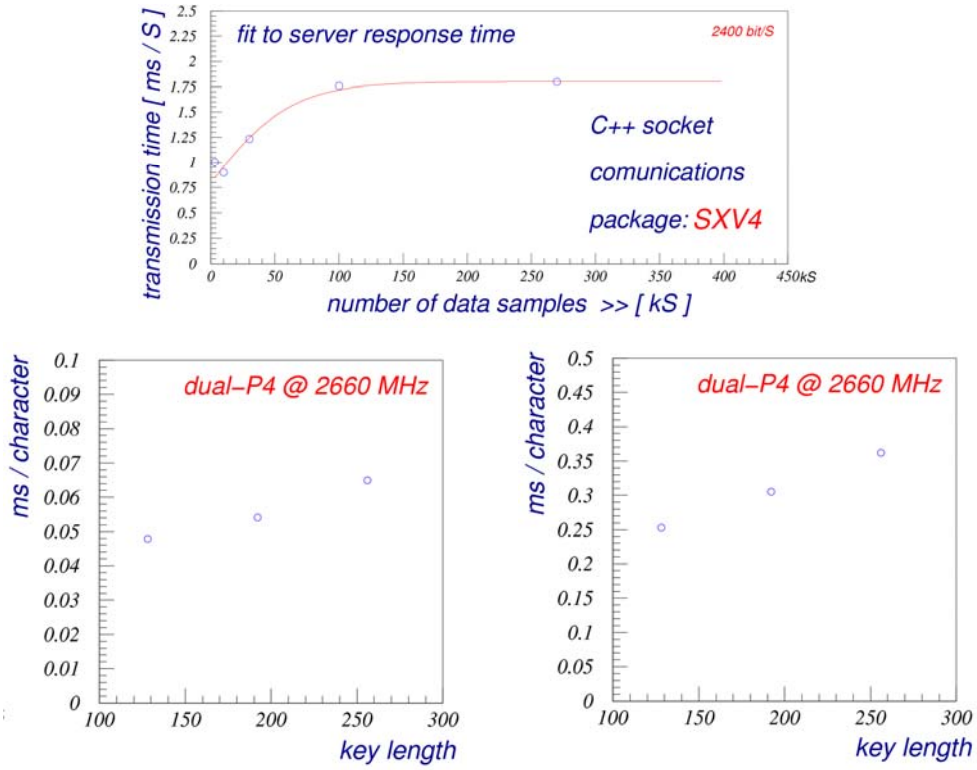

Fig. 4. Top figure: server response times under SXV4, bottom figures: crypting (left) and de-crypting (right) times under AXV4 vs. cypher's key length.

Acknowledgements

The work and technology presented were financed under the D11-044 "QUANTGRID" project by the Romanian Center for Project Management CNMP.

References

[1] Network World 17.05.2004, P. Willan – EU seeks QKD response to Echelon.

[2] ID-Quantique (Geneva), MagiQ (Boston), QuintessenceLabs (Canberra).

[3] ID-3100 Clavis^2 Components Documentation v1.1, Feb. 2009, © ID-Quantique.

[4] Hopping-sockets in AES crypting, D11-044 QUANTGRID Activity Report'09.

[5] C. H. Bennett, G. Brassard, Proc. IEEE Intn.'l Conf. Computers, Systems, and Signal Processing, Bangalore, 175 (1984).

*Corresponding author: modima@nipne.ro