THE QUANTGRID PROJECT (RO) – QUANTUM SECURITY IN GRID COMPUTING APPLICATIONS*

1M. DIMA, 1M. DULEA, 1E. PAUNA, 1M. PETRE, 1B. MITRICA,
2M. STOICA, 2M. UDREA, 3R. STERIAN, 3P. STERIAN

1 National Institute for Nuclear Physics and Engineering, P.O. Box MG-6, RO-077125
Bucharest-Măgurele, Romania, E-mail: modima@nipne.ro
2 National Institute for Plasma and Laser Physics, Str. Atomistilor, Nr. 409, P.O. Box MG-36,
RO-077125, Măgurele, Bucharest, Romania
3 University Polytechnica, Splaiul Independenței 313, Bucharest, R-060042, Romania

Received October 10, 2008

The QUANTGRID Project, financed through the National Center for Programme Management (CNMP-Romania), is the first attempt at using Quantum Crypted Communications (QCC) in large scale operations, such as GRID Computing, and conceivably in the years ahead in the banking sector and other security tight communications. In relation with the GRID activities of the Center for Computing & Communications (Nat.’l Inst. Nucl. Phys. – IFIN-HH), the Quantum Optics Lab. (Nat.’l Inst. Plasma and Lasers – INFLPR) and the Physics Dept. (University Polytechnica – UPB) the project will build a demonstrator infrastructure for this technology. The status of the project in its incipient phase is reported, featuring tests for communications in classical security mode: socket level communications under AES (Advanced Encryption Std.), both proprietary code in C++ technology. An outline of the planned undertaking of the project is communicated, highlighting its impact in quantum physics, coherent optics and information technology.

1. INTRODUCTION

GRID computing currently includes applications that are intelligence sensitive (genetics, space, industrial intellectual property, etc). Current security of said information is based on public (asymmetric) key algorithms – hash function algorithms that easily calculable directly, but impossible (un-proven) in reverse. The base assumption is that of the difficulty of factorising prime numbers, which received a serious blow in 1994 (Peter Shor), when it was shown that a quantum computer can factorise rapidly prime numbers via a polynomial algorithm. Such message, intercepted today and stored until quantum processors become available, can be deciphered. Evidently, data with 2–5 year “life span” are perfectly safe today, however censi, geological data, etc need to


be adequately protected. Quantum crypted communications eliminate the possibility that in the future (with the onset of quantum processors) these may be deciphered. In crypting theory it was shown (G. Vernam, AT&T – 1926) that the use of a hash function with a key of equal length (or greater) than the message can guarantee the safety of the communication. The problem of the (symmetrical) key protocol is however the exhaustion of the hash tables (the functions are implemented as tables using random numbers delivered by natural sources – for instance alpha decays). After exhausting the tables, the communication partners need to re-establish contact and exchange a new set of tables. This has come to be known as the Key Distribution Problem. Quantum Key Distribution (QKD) is secured by the very essence of the quantum nature: any quantum state measured in any way collapses into one of its projections. It cannot be re-generated to its initial state, thus being impossible to be cloned and a copy thereof be kept. Therefore the distribution of quantum public key is similar to the Vernam cipher (symmetrical – with secret key).

2. THE QUANTGRID PROJECT

Quantum Crypted Communications have not been tested previously in Romania, although such tests have been performed internationally, in the US, France, Germany, and by the major swiss banks in Geneva. The ongoing QUANTGRID project will apply this technology to GRID communications through optical fiber. This approach will allow to optimise the quantum security technology and experiment proprietary algorithms for the optimum data-volume/security for this new type of communications. Expertise obtained thereby will be disseminated nationally by attracting interested bodies in this type of communications: Parliament, Executive, bank system, national security agencies (SRI, STS, SPP, SIE). The field is of marked international attention currently (transition to a new generation of crypting), and much so in the European Union where immunisation against Echelon interception [1] is sought.

2.1. QUANTUM KEY DISTRIBUTION

Crypting theory relies on the use of a hash function that converts a plain text into a code. The hash function uses what is termed as a key to cipher the plain message. In 1926 G. Vernam (AT&T) has shown that by using a hash function with a key of equal length (or greater) to that of the message it can be mathematically guaranteed that the message is secure for communication. Claude Shannon has further shown in two reference papers of 1948 [2] and 1949 [3] how to best encode information by developing information entropy, and
that all theoretically unbreakable ciphers must have the same requirements as the one-time pad.

The problem of the (symmetrical) key protocol is however the exhaustion of the hash tables (the functions are implemented as tables using random numbers delivered by natural sources – for instance alpha decays). After exhausting the tables, the communication partners need to re-establish contact and exchange a new set of tables. This has come to be known as the Key Distribution Problem.

One form to circumvent this problem is by using Public Key Distribution, such as RSA \cite{4}). In 1994 however Peter Shor, showed that a quantum computer could factorise rapidly prime numbers via a polynomial algorithm.

Quantum Key Distribution (QKD) is secured by the very essence of the quantum nature: any quantum state measured in any way collapses into one of its projections and it cannot be cloned.

2.2. BB84 PROTOCOL

In 1984 Charles Bennett and Gilles Brassard \cite{5} proposed a protocol for quantum key distribution – today implementable on a variety of quantum states (of which polarisation states and entangled-photon states the most prominent).

For exemplification we will show the polarised-photon version of the protocol – Fig. 1 based on faint photon-pulses, containing 2–3 photons.

![BB84 Protocol](image)

Fig. 1 – Charles Bennett and Gilles Brassard quantum key distribution protocol of 1984 – shown here in its version using photon polarisation states.

The BB84 protocol has the following steps: **Base choice** – both Alice and Bob choose random base choices for sending/receiving the photons. Both achieve this by phase-modulation and interference – in a Mach-Zender interferometer. **Bit generation** – in the base chosen Alice generates the bit she requires to send (1, or 0 – two polarisation orthogonal states). These she sends to
Bob. Bit analysis – Bob takes the photon-pulses and passes them through the Mach-Zender interferometer with the modulation chosen at (1). He notes down the results of the analysis: in case he has the correct basis these measurements represent real-bits, else 50% chance of having the real-bit. Base exchange – Bob and Alice communicate the bases they chose (NB – post-transmission!) and hash out those where they were in disagreement. Interception measurement – Alice asks Bob for a (sacrifice) subset of the bits received, which Bob transmits freely. The level of interference from Eve is determined by the BER (bit error rate) of this (sacrifice) subset. Sifted key – Bob is now in the possession of the “sifted” key, which is further transformed. PA, privacy amplification – due to a certain BER in the sifted key the correct key is regenerated via some redundancy built in the transmission. Such codes are termed privacy amplification algorithms, for instance in internet communications uuencode / decode are used. For quantum key distributions a number of such error correcting algorithms have been developed, most prominent being CSS [6], enhanced or not with low-density parity-check (LDPC) methods.

2.3. GRID SETUP

We are using the existing GRID infrastructure within IFIN-HH. The crypted data stream will be connected to one of the Storage Elements from a remote port-station hosting the quantum key distribution equipment. The other end of the equipment will be in INFLPR – who will also be providing the equipment – at a distance of 25 km of conventional SMF optical fiber.

2.3.1. Advanced Encryption Standard Security

The quantum key distribution modem needs to connect either next-by (via USB, protocol modes classes 02h or 0Ah), or locally (via a secured dedicated line).

We designed a local-link architecture enabling us to use hopping-sockets in relation with AES crypting. For this two elements were created: SXV4 – proprietary C++ class that handles socket level communications, and gives us a handle close to the hardware level of interacting with the communication ports, and AXV4 – proprietary C++ class implementing the FIPS-197 [7] AES standard, such that we hold control of the procedure. We intend to use hopping-sockets in combination with AES crypting as absolute security level locally.

We have tested the SVX4 C++ package on two servers of the same cluster – which would be very similar to the configuration QKD-modem-to-GRID port, by sending various data samples, of different lengths. Typical transmit-times are presented in Fig. 2 – function of the number of samples in the same transmit-job. We fitted the server response to saturating functions in order to have an estimate
of transmission times for repeated transmissions. The complete map of tests is shown in Fig. 3.

![Server response times to our proprietary SXV4 socket communications package, for 2400 bit/sample and 8000 bit/sample tests. Multiple samples are transmitted for each point on the plots. It can be seen that the OS-scheduler allots high priority to tasks loading the net-card with large data batches, in order to expedite the job, and lessens the priority of jobs using the net-card with many small data batches.]

AXV4 is our proprietary C++ implementation of the FIPS-197/2001 AES block cipher. Tests of AXV4 were performed by de/decrypting files of various volume of characters in each key length version (128, 192, 256) implying (10, 12, 14) rounds. For 128 bit key size the results for crypting are in Fig. 4 and for decrypting in Fig. 6. The “saturation” times are plotted in Figs. 5 and 7 vs. key-size.

3. QKD PROSPECTS

We expect to do some extensive testing of this technology, in particular we are interested in seeing how it performs under a determined attack.

In this respect we intend to realisation an interceptor node between IFIN-HH and INFLPR where we will inject intense laser pulses that will reach
Fig. 3 – Server response times to our proprietary SXV4 socket communications package, for 8, 24, 80, 240, 800, 2400, 8000, 24000 bit/sample tests vs. number of transmitted samples.

Fig. 4 – Performance of AXV4 in crypting a file function of file size. A saturation on the order of 60 μs/character can be seen from file sizes 2000 characters and up.
Fig. 5 – Performance of AXV4 in crypting a file function of the key length used (blue = 128 bit, red = 192, green = 256). The saturation time μs/character for each key length is on the right. A linear dependence with key size is observed.

Fig. 6 – Performance of AXV4 in decrypting a file function of file size. A saturation on the order of 270 μs/character can be seen from file sizes 2000 characters and up.

Fig. 7 – Performance of AXV4 in decrypting a file function of the key length used (blue = 128 bit, red = 192, green = 256). The saturation time μs/character for each key length is on the right. A linear dependence with key size is observed.
the Alice node, pass through the Mach-Zender interferometer and return with information on it’s phase modulation status (double-pass attacks). The Polytechnical institute will create the numerical methods for code interception = mostly code-analysis (statistical methods).

We will also record BER rates vs. interference laser power, pulse repetition rate, etc – as we are interested in the capacity of the technology to also withstand jamming.

Contributions of the project circumscribe themselves to a number of firsts: nationally – first quantum crypted communication line in Romania and first romanian proprietary privacy amplification algorithms, also first romanian experience at operating QKD technology; internationally – first implementation of quantum secured communications in a GRID environment.

Acknowledgements. This work is financed under the PNCDI-2 grant D11-044 / 2007 by the Romanian Center for Programme Management.

REFERENCES

7. Federal Information Processing Standards Publication 197 November 26, 2001 – ADVANCED ENCRYPTION STANDARD (AES), issued by the National Institute of Standards and Technology (NIST) after approval by the Secretary of Commerce pursuant to Section 5131 of the Information Technology Management Reform Act of 1996 (Public Law 104-106) and the Computer Security Act of 1987 (Public Law 100-235).