5

Quantum Encrypted Data Transfers in GRID

M. Dima[1], M. Dulea[1], A. Dima[2], M. Stoica[3] and M. Udrea[3]
[1]*Inst. for Nuclear Physics & Engineering*
[2]*Lairside Laser Center*
[3]*Inst. for Laser & Plasma Physics*
[1,3]*Romania*
[2]*UK*

1. Introduction

GRID computing includes applications, some of which are intelligence sensitive (genetics, space, industrial intellectual property, etc) and need to remain confidential. Current security is mostly based based on public (asymmetric) key algorithms (Salomaa, 1996) – hash function algorithms easy to calculate in direct, but estimated as impossible in reverse. The base assumption to this assertion is the difficulty of factorising prime numbers. This received however a serious blow in 1994 (Shor, 1994), when it was shown that (a hypothetical future) quantum computer could rapidly factorise prime numbers via a polynomial algorithm. As such messages could be intercepted and stored today awaiting for the availability of quantum processors, when they could conceivably be deciphered. Evidently, data with short "life-span" (2-5 years) is perfectly safe today, however censi, geological data, etc have long-term implications and need to be adequately protected.
The other main security contender currently in use is the symmetric-key AES encryption (Daemen and Rijmen, 1996-2001 and 2006), that comes in 3 versions of key length 128, 192 and 256 bit (with 10, 12, and 14 rounds, respectively). For AES-128 there is no known attack faster than the 2^{128} complexity of exhaustive search. However, AES-192 and AES-256 were recently shown (Biryukov and Khovratovich, 2009) to be breakable by attacks of 2^{176} and 2^{119} complexities. While these are much faster than the exhaustive search, they are non-practical, and do not to pose a real threat (at the rate the world produces today data, ca. $0.2 \cdot 10^{21}$ bytes/year ($2^{61} \times 256$-bit ciphertexts) it would take $2^{58} \cong 10^{17}$ years data's worth to recover just one AES key). The US National Security Agency (Hathaway, 2003) stated that "The design and strength of all key lengths of the AES algorithm (i.e., 128, 192 and 256) are sufficient to protect classified information up to the *secret* level." From this assessment and the simple estimates above, it is apparent that given adequate key distribution protection AES cannot be broken – at least not in the next 10^{17} years (for 1 key).
The secret key carrier on the other hand needs to be a stable long-term committed technology, that would not come under question any time soon (including from futuristic quantum processor attacks).

1.1 Key distribution

In cryptology it was shown (Vernam, 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 such a (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: attempts to measure in any way quantum states collapses the state into one of its projections. The quantum state cannot be regenerated to its initial state, therefore it is impossible to be cloned and a copy thereof to be kept. The distribution of public quantum keys is thus similar to the Vernam cipher (symmetrical - with secret key). In particular, in Europe this has attracted attention as a means of immunisation against Echelon interception (Willan, 2004).

2. Quantum encryption

To transmit keys in quantum format the information can be coded in the various degrees of freedom of the quantum system used – in this case laser light. Laser light offers a number of qualifying degrees of freedom: transverse position/momentum, linear/circular polarisation as well as 2-photon entangled states.

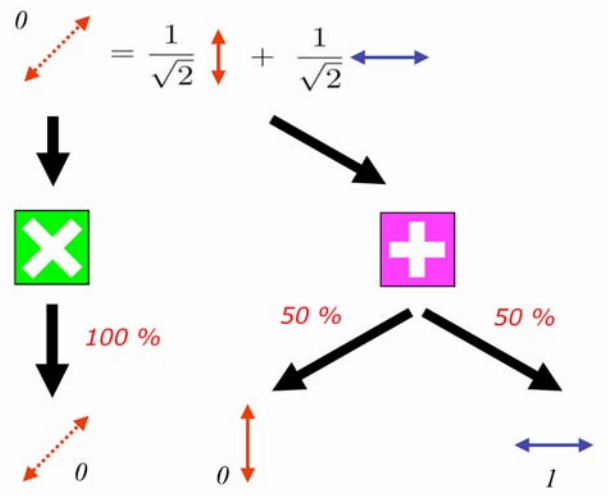

Fig. 1. Measurement of a circular R state in it's eigen basis (giving always the correct result) and in that of its conjugate, linear, basis (giving 50% of the time one state and 50% the other).

Whatever degrees of freedom are used, the central idea is to utilise sets of 2 conjugated degress of freedom. This is because if the receiver does not know in which base the bit was emitted and measures it in the wrong base, the laws of quantum mechanics guarantee an ambiguous outcome, thus conceiling the information. Consider in this respect figure 1 that shows the measurement of circular states in linear polarisation of laser light: $|R\rangle = 1/\sqrt{2}\ |\updownarrow\rangle + 1/\sqrt{2}\ |\leftrightarrow\rangle$ and $|L\rangle = 1/\sqrt{2}\ |\updownarrow\rangle - 1/\sqrt{2}\ |\leftrightarrow\rangle$. Measurement of $|R\rangle$ in the '×' basis gives

everytime the correct answer R since it is its own basis, in which it was produced. Measurement however in the the '+' basis (according to the norms-squared of its decomposition) yields 50% of time the answer ↕ and 50% of time ↔, as the figure shows. For other conjugate quantities, say transverse-coordinate and transverse-momentum, the decomposition gives an infinite series of the conjugate quantity's states: $\sqrt{2\pi}|x\rangle = \int \exp(-ikx)|k\rangle\, dk$. The norms-squared of the decomposition are now all (infinitesimal) equal. This aspect is conjugate-variable dependent. In all cases the fundamental idea of quantum encryption is that without the correct information on the base of the bit sent, its measurement in the base of its conjugate degree of freedom yields an ambiguous result, hence concealing the information sent. Therefore, such a commodity allows the design of a public-key communication protocol that can be implemented maintaining the confidentiality of the key.

There is still one more mention: all said is valid for *single* quantum entities (here photons). If we transmit N photons, the foreseeable interceptor (Eve), can make a statistics for each bit sent. She will observe when she has the wrong basis of figure 1: having enough photons, she divides the bit and sends it through both bases. The one with non-ambiguous statistics is evidently the right one. Hence without faint-photon pulses quantum protocols are rendered decipherable.

2.1 Faint-photon pulses

In order to use quantum properties, ensembles of very few quantum objects are necessary, to avoid small numbers of entities to be intercepted and the signal to be detected.

For 2-3 photon pulses interference with the pulse causes the collapse of the quantum states destroying the pulse. The hypothetical eavesdropper, Eve, intercepting pulses sent by Alice to Bob, either destroys them (revealing her presence), or lets them go through. Theoretically even 2-3 photon pulses may allow interception by keeping 1 photon and passing through the other 1-2. Technically that is very demanding – so-called "beam-splitting" attack (Dusek, 1999), and also, as it will be explained below.

A typical setup uses a mono-mode laser, the intensity of which is attenuated at exit to the level of 2-3 photons/pulse. Since the laser line width is almost zero compared to the magnitude of its frequency, the light can be approximated as coherent. Today solid state lasers (in green for instance) have coherence lengths on the order of 100-200 m, and fiber-lasers in the range of km's. Coherence length is the distance over which the light wave has no phase-slips and retains the same frequency: $L = c/n\Delta f$, with c the speed of light, n the index of refraction in the respective medium and Δf the frequency width of the laser line. Evidently, for $\Delta f \to 0$, $L \to \infty$ and the laser is 100% mono-chromatic. The distribution of photon number of coherent states is given by a Poisson distribution:

$$p(n) = \frac{\mu^n e^{-\mu}}{n!}, \quad n = 0,1,2,...$$

where n is the number of photons and μ the average number of photons per pulse. For an attenuated pulse of $\mu = 0.1$, *90.48%* of pulses contain no photons, *9.05%* one photon, *0.45%* two photons, *0.02%* three photons, etc.

It can be seen that the price for security is that of over *90%* of pulses being empty.

Given the corpuscular nature of the signals we equate the probability for a detector of efficiency η to produce m photoelectrons in response to the $p(n)$ pulse:

$$p(m) = \sum_{n=m}^{\infty} \binom{n}{m} \eta^m (1-\eta)^{n-m} p(n)$$

The detector does not flag how many photons impacted it, rather it has a probability of producing an electrical output pulse (sum over all possible photo-electron numbers):

$$P = \sum_{m=1}^{\infty} p(m) = 1 - e^{-\eta\mu}$$

For N laser pulses there will be $PN = N_{detected}$ pulses, hence $\eta\mu = - ln(1-I_{detected}/I)$. To practically measure this quantity pulses are produced with a convenient (sub-MHz) frequency, attenuated, and measured as intensity vs. the source as the last equation shows. Knowing the detector efficiency η, the average number of photons/pulse μ is calculated. The systems have automated DAQ and data processing that controls this level. In the same procedure the attenuation (calibrated at the transmission's initiation protocol) over the optical fiber is calculated and monitored. Interception will be manifest as a rise in this figure, revealing Eve's presence.

2.2 Signal coding

The essence of quantum coding relies on chosing the correct measurement basis, a number of conjugate bases being available: transverse position/momentum, orthogonal polarisation bases, etc.

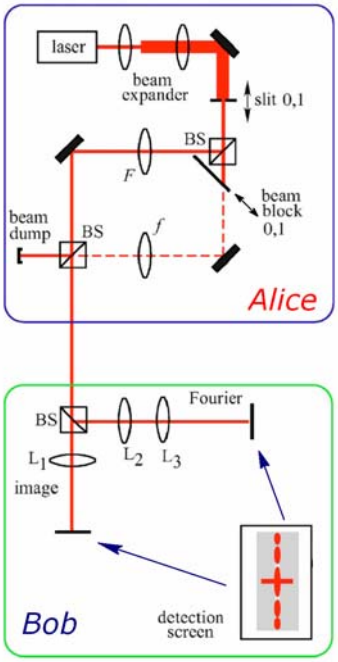

Fig. 2. Experimental setup of quantum key distribution scheme with photon transverse position and momentum.

Transverse position/momentum coding – this approach (Lemelle, 2006) encrypts the bits as two discrete positions of a simple slit aperture. In optics a transverse position measurement of a photon is associated with the near field or image plane, while a transverse momentum measurement is associated with the far-field or Fourier plane. Position and momentum measurements of an input field can be performed using simple optical imaging and Fourier systems along with a detector. An illustration of this scheme consists of two stages: preparation (Alice) and measurement (Bob). At Alice's a plane wave illuminates a small slit aperture placed in the input plane, which localises the photon in the transverse plane to within the spatial dimensions of the slit. Because the photon's position is now well defined, it can be considered in a definite transverse position state. In the second part Alice uses a random bit to decide which base (position or momentum) she will use:

- position basis (x): she will use her lens such as to image her slit plane onto Bob's input plane ($f_1^{-1} = d_1^{-1} + d_2^{-1}$), where f_1 is the focal length of the coding lens and $d_{1,2}$ the distances slit-to lens and lens to Bob's input plane,
- momentum basis (p): she will use her lens as a Fourier lens system ($f_1=d_1=d_2$) to create the Fourier transform of the slit at Bob's input plane, conducing Bob to chose a momentum eigen state.

In the measurement stage Bob also chooses one of the two measurement bases position or momentum randomply. Bob projects either:

- the (direct) image, by $f_2^{-1}=d_3^{-1}+d_4^{-1}$, where similarly to Alice f_2 is the decoding lens, and $d_{1,2}$ the distances input plane to lens and lens to detection screen, or
- the Fourier transform, by $f_2=d_3=d_4$ of his input plane onto his detection plane.

That is: Bob either transports, or Fourier transforms his input, in essence being the inverse of Alice's preparation system.

There are thus four possible (Alice, Bob) configurations: (xx), (xp), (px), and (pp), where "x" is the position basis and "p" the momentum basis.

Bob will have the correct result if his base choice matches Alice's base choice - i.e. only (xx) and (pp) will yield a correct transmission:

- for (xx) or (pp), Bob should detect a photon at the detector plane in a position corresponding to that of Alice's slit aperture. In the (xx) configuration, Alice and Bob implement two imaging systems, that is the image of the slit will be transported to the detection plane. In the (pp) configuration, two consecutive Fourier transforms are applied, returning a coordinate inversion. Thus, aside from this, Bob's detector plane will have the image of the slit position. In summary, when Alice and Bob use the same lens configurations, (xx) or (pp), their combined lens system produces the image of Alice's slit aperture. Consequently, Bob should detect the correct state that Alice has prepared;
- for the (xp) or (px) configurations, there is no correlation between Bob's detected position and Alice's slit position. In these arrangements Bob detects either the image of a Fourier transform or the Fourier transform of an image. The overall detection pattern will be that of a Fourier transform, providing no information on the position of Alice's slit, for the difference between "0" and "1" bits (a transverse position difference) shows up as a phase factor when Fourier transformed. Since detectors provide only amplitude information (phase being lost), precisely the crucial information is obscured, rendering the measurement lost.

The setup described above was implemented by (Lemelle, 2006), illustrating the technique. Although the experiment was performed using an intense laser source (vulnerable to

eavesdropping), it allowed the clear illustration of the probability distribution's at Bob's detection plane (in the faint-photon case). This intensity pattern is an illustration of Bohr's complementarity principle playing the crucial role in a faint-photon practical application. The same level of security as with polarization bases, can be achieved if using faint-photons.
The experimental setup shown in figure 2 is somewhat more elaborate than the simple 2-lens system above, but offers certain technical advantages.
Alice's setup used a red diode laser was used to illuminate a single thin slit aperture with width a=100 m. Before the slit the beam passed through a 2 beam expander consisting of a 25 and 50 mm lens in confocal arrangement. Alice toggles the slit between positions s_0 and s_1 using a simple translation stage. In principle, a piezoelectric or similar device driven by a random number generator could be used to toggle the slit position. After the slit there is a typical Mach-Zehnder interferometer with non-polarizing 50–50 beam splitters, with the imaging lens in one arm and the Fourier transform lens in the other. The interferometer allows Alice to switch between x and p encoding by simply choosing which of the arms to block. Alice can then toggle between the imaging arm and the Fourier arm using a simple movable beam block. Because one arm of the interferometer is always blocked, no interferometric stability is required. However, the interference can be exploited to initially ensure that the imaging and Fourier arms are properly aligned. Alice's imaging system is made up of a 250 mm focal length lens f , which creates the image of the slit on Bob's input plane at a distance 1000 mm from the slit in one exit arm of the interferometer. For her Fourier system a 500 mm focal length lens F creates the Fourier transform of the slit on Bob's input plane. The other exit arm is blocked by a beam dump.
Bob's detection system consisted of a 50-50 non-polarizing beam splitter that implemented the random choice between detection bases. In one output of the beam splitter was an imaging system and the other arm a Fourier system. In this proof of principle experiment a digital web-cam was used to photograph the detection screen (ca. 1mm resolution). Therefore the slit's image was magnified. For this reason, Bob's imaging system consisted of a 75.6 mm focal length lens L_1 placed so as to create a magnification factor of M_2=8. For the Fourier system, a 250 mm focal length lens L_2 was used to create the Fourier transform.
The different focal lengths in Alice and Bob's p configurations create a magnification factor of 1/2. To compensate for this magnification factor, an additional 50 mm focal length lens L3 was used to image the Fourier plane onto the detection screen with a magnification factor of about 16, giving an overall magnification factor of 8.
Figure 3 shows the results corresponding to Bob's transverse position measurements configuration. In figure 3a, Alice encoded bit value 0 using slit position s_0 and the x configuration. Consequently, Bob detected light in the left region on his position detection screen. In figure 3b Alice sendt bit value 1 using slit position s1 and the x configuration; likewise Bob detected light in the right position of his detection screen. These results show the correlation between the slit position and Bob's detection position when both parties implement x configurations. Figures 3c and 3d show results when Alice encodes slit positions s_0 and s_1 using momentum encoding. Here photons fall on both detector positions independent of the slit position, indicating no correlation between Alice's preparation and Bob's measurements.
Figure 4 shows digital photos of the results at Bob's momentum detector for the same sequence of measurements as in figure 3. In figures 4a and 4b Alice used x encoding to send slit positions s_0 and s_1, respectively. No correlation was seen at Bob's momentum detector. In figures 4c and 4d Alice used momentum encoding to send slit positions s_0 and s_1, and as

expected Bob detected photons in the correct positions (observe the "-" sign, inversion, associated with the double-Fourier transform).

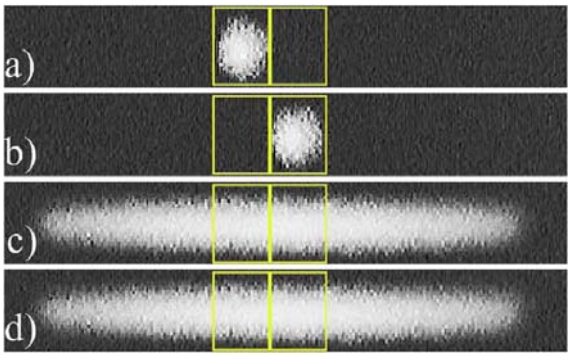

Fig. 3. Results for using position base: (a) bit 0 and (b) bit 1 for Alice encoding in position base, (c) bit 0 and (d) bit 1 for Alice encoding in momentum base.

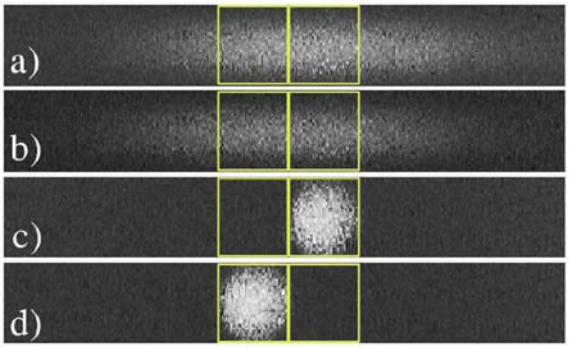

Fig. 4. Results for using momentum base: (a) bit 0 and (b) bit 1 for Alice encoding in position base, (c) bit 0 and (d) bit 1 for Alice encoding in momentum base.

The correlations shown in figures 3a, 3b, 4c and 4d show that Alice can send random bits to Bob, while the random results shown in figures 3c, 3d, 4a, and 4b demonstrate that an eavesdropper Eve will necessarily disturb the system when she guesses the wrong measurement basis. Furthermore, her disturbance will show up in Bob's measurement results. As discussed, for each photon sent, it is necessary for Eve to guess Alice's basis, x or p. After transmission, Eve will know if she guessed correctly or not by listening in on Alice and Bob's classical communication. If she guessed correctly, she will have detected the photon at the correct position and will know the bit that Alice sent. She will have reproduced Alice's original state and sent it to Bob. However, one-half of the time Eve guesses incorrectly, and every photon has an equal probability of being detected at either position, as shown in figures 3c, 3d, 4a and 4b. In this case, Eve has no information regarding the bit sent by Alice and is thus unable to reproduce her original state with certainty. If Alice and Bob calibrate their system correctly, Eve will cause a 25% error rate if she intercepts every photon.

Polarisation coding – this approach encrypts the bits in the bases shown in figure 1. Should Bob measure the pulse in the wrong base, he will obtain an ambiguous result. Similar to position-momentum encoding, faint photon pulses are crucial: should there be plenty of photons, the pulse can be divided into two, measured in both bases and retained the result only of the one not ambiguous (the wrong base would have a 50-50% statistic of "0" and "1" photons).

Phase coding – this approach encrypts the phase difference in a Mach-Zehnder interferometer as in the setup of (Hendrych, 2002). Alice and Bob each have a phase shifter in one of the arms of the interferometer (figure 5) and by applying suitable combinations of phase shifts, the interference can be tuned to be constructive/destructive (bits 1,0), or (quantum mechanically) random. The probability for a photon from the laser, entering the interferometer, and detected at detector D1 or D2 is: $(1 \pm \cos(\Delta\varphi)) / 2$ - for the case of zero attenuation and no environmental noise.

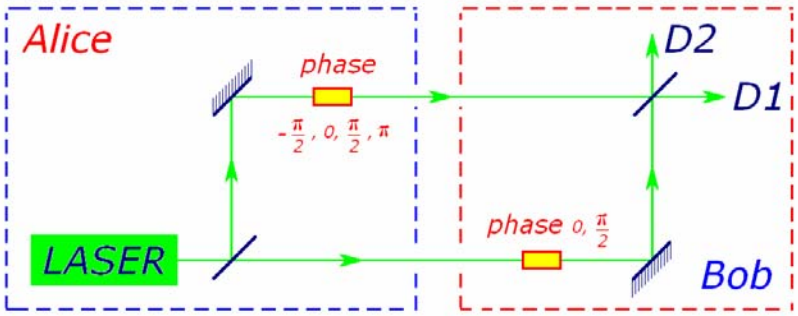

Fig. 5. Quantum encoding of phase difference in a Mach-Zehnder interferometer. For $\Delta\varphi = (0, \pi)$ Bob's base coincides with Alice's and his measurements are exact. For $\Delta\varphi = \pm\pi/2$ his base does not coincide with Alice's and the results of his measurements are stochastic (with the quantum predicted probabilities).

As a typical BB84 protocol implementation, Alice randomly sets one of the four phase shifts $-\pi/2$, 0, $\pi/2$, π and Bob also randomly chooses his measurement basis by setting his phase shift 0, or $\pi/2$. When $\Delta\varphi = 0, \pi$, the measurement being performed in the same base, yields bits 1, 0 (constructive, or destructive interference). However, when Bob's base is orthogonal to Alice's base, the outcome can be ambiguous.

Since Alice and Bob are spatially separated, this implementation of would suffer from substantial problems due to environment perturbations, thermal drifts, etc. For the interference not to be washed out, the difference of the optical lengths of the interferometer's arms must stay constant to within a fraction of the wavelength of the used light. Different temperature fluctuations in the two optical fibers result in different changes in their refractive indices and smear out the interference.

To avoid this problem both paths of the interferometer can be launched into the same optical fiber, figure 6.

Such an interferometer comprises of two identical unbalanced interferometers, with path length difference much greater than the coherence length of the laser. Thus altough no interference occurrs in the small interferometers, globally the total system preserves the correct interference. Fiber couplers perform random 50:50 splitting, so photons can go on

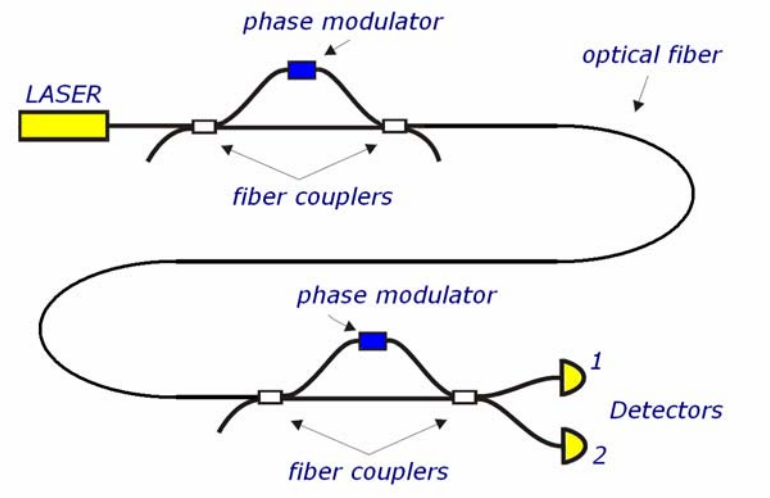

Fig. 6. Environmental perturbations can be eliminated using a time-multiplexing interferometer. In this setup Alice's and Bob's interferometers are identical unbalanced interferometers, whose with path length differences on the order of tens of cm.

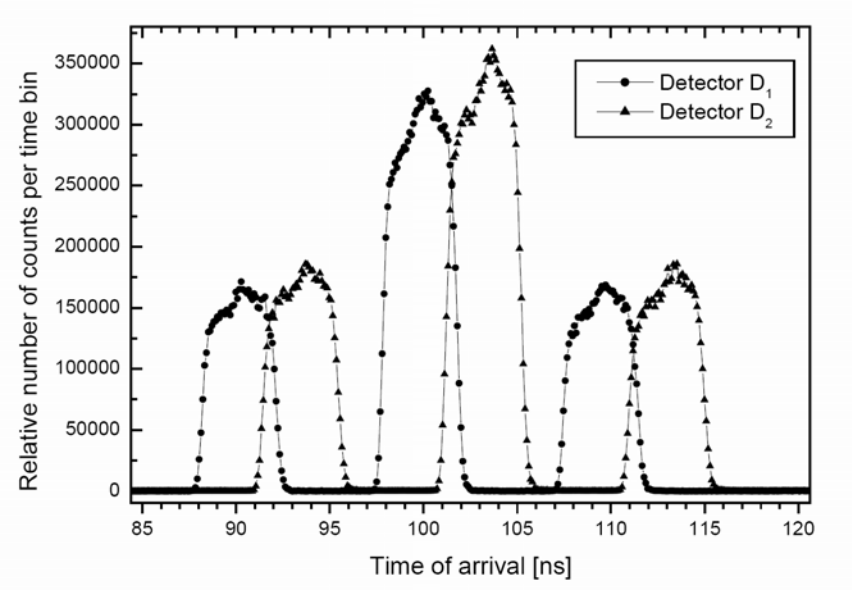

Fig. 7. Time of arrival for pulse in a 15-m time-multiplexing interferometer (circles detector D1, triangles D2). Photons arrive in 3 time windows separated by 10 ns (corresponding to the arm length difference of 2m): the leftmost peak photons taking short-short paths, the rightmost peak photons taking long-long paths. Interference occurs only in the middle (long-short, short-long) time window.

any of the four possible combinations from Alice to Bob: Alice's short path and Bob's short path 25 %, Alice's long path and Bob's short path 25 %, Alice's short path and Bob's long path 25 % and Alice's long path and Bob's long path 25 %. Typicall the length difference between the short and long arms of either interferometer is tens of cm's. Photons arrive at Bob's detectors in three time windows (separated by typically 10 ns – figure 6). There is no interference in the first and third time (short-short and long-long paths), however long-short and short-long paths are indistinguishable – and interfere. This method in effect is an interferometer analogous to that of figure 4, however, at the expense of losing half the photons (on the short-short- and long-long paths) it is possible to eliminate environmental fluctuations by being assured of having both paths of the interferometer equally affected by the latter. What still needs to be stabilised are the small unbalanced interferometers, where the short an long paths are spatially separated. To achieve this, the small unbalanced interferometers can be placed for instance in Styrofoam boxes (Hendrych, 2002).
As an overview on the effects contributing to the widths of the peaks: part is due to the width of laser pulses (4 ns), 0.5 ns to detector jitter and 0.3 ns to processing electronics jitter.
Entanglement coding – in this approach the photons are created by shining the laser through a non-linear crystal, producing entangled pairs of photons via spontaneous parametric downconversion. Figure 8 shows that in either polarisation base, the same (maximal) entanglement is present. As Alice (or even a third party – can be Eve !) prepares an entangled pair, she holds her part of the pair, a photon, and sends to Bob his part, the pair photon. When either Bob or Alice detects one's own photon, quantum laws guarantee that the other's photon is in the entanglement correspondent state.

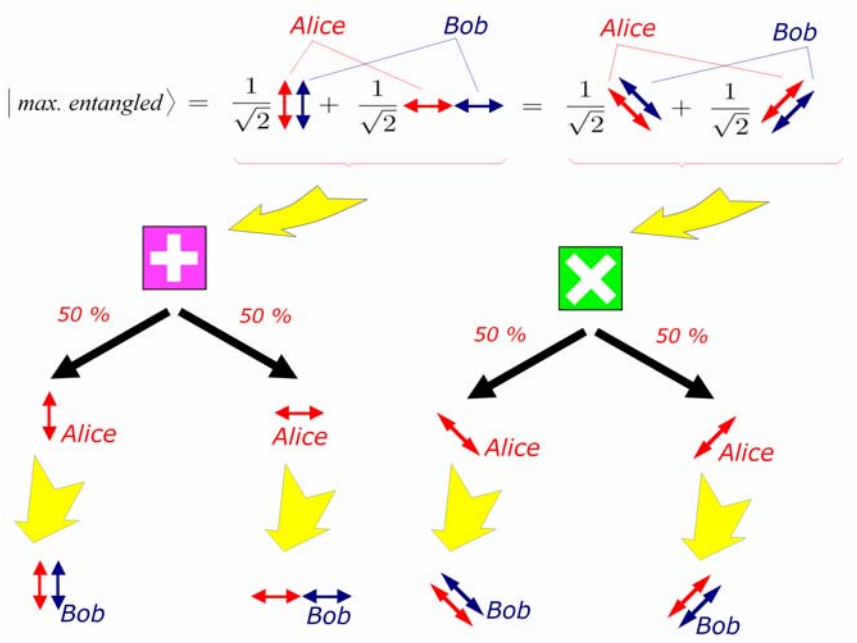

Fig. 8. Collapse of the entangled state by Alice's detection of her photon guarantees that Bob has his photon in the same state of polarisation *and* in the same base.

Any attempt at eavesdropping by Eve destroys the correlated pair in a way that Alice and Bob can detect. Eve cannot gain any information by capturing photons because *the actual information does not exist until Bob or Alice make their measurements*. The act of measuring creates the actual bit (0, or 1) that is to be sent. This is because either of the photons is in a *non*-eigen state for *both* bases (indeed an outstanding feature even for single-particle quantum mechanics !) and the collapse of its wavefunction determines what bit value the measuremtent will be. A remarkable consequence is that the bit's creation basis is decided upon measurement, and that namely by either Alice or Bob. Should the other use the wrong basis, an ambiguous result will ensue.
Should Eve conceive substituting herself for the source of entangled photons and produce 3 entanglement correlated photons, with the extra one held for herself without disturbing Alice or Bob, this will be noticed in the wavelength of the photons. At the single-photon level this translates in a different detection efficiency and non-optimal (path and thermal drift) compensations all equipments have. At the statistical level the wavelength can be measured and the generated keys discarded.

2.3 The BB84 protocol

Figure 9 illustrates how Alice transmits to Bob a raw key, how this is sifted and how this is further used to detect communication channel noise/ interference and produce the final key – (Bennett and Brassard, 1984).

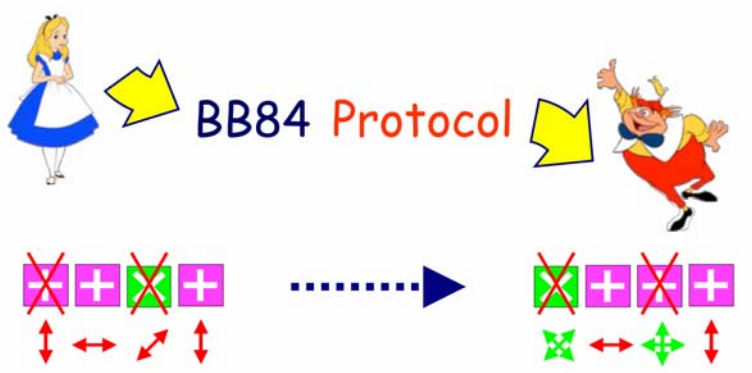

Fig. 9. Schematic of the BB84 protocol: the role of conjugate quantum bases (+, ×) and outcome both when using the correct and when using the wrong base are shown.

Firstly Alice selects the base for each bit, then decides on the 0,1 value of the bit. She does not tell Bob about the choices, not yet. She then sends the set to Bob, who chooses randomly a base in which to measure the qubits (quantum bits). In figure 8 the fist base is wrong and the result unreliable. The second one is correct and the recorded result faithful to the set sent by Alice ... etc. After the set is received Alice and Bob publicly exchange the information about the bases (and not about the bits). They discard those where Bob was wrong. For the hypothetical intercepter Eve this information is too late. To be in any way relevant she should have intercepted at least 2 photons and have measured one in one base and one in the other. However 2 photons out of a 2-3 photon pulse is too much (moreover, intercepting 1 photon for 1 measurement is likely insuficient).

In case of the **position/momentum** method the BB84 protocol would ensue as follows:

- Before any key bits are transmitted, Alice and Bob align their detectors so that Bob can establish detection positions that correspond to Alice's slit positions. They perform this alignment procedure using (xx) and (pp) configurations.
- Alice generates random bits a1 and a2. She aligns her slit aperture to position s(a1) and prepares either an x eigenstate a2=0 or a p eigenstate a2=1 to Bob's input plane.
- Bob generates a random bit b2, which determines the basis x or p in which he will measure. He detects the photon and records the result as bit b1. If no photon is detected, the run is automatically discarded.
- Alice and Bob repeat steps 2 and 3 until a sufficient number of photons have been transmitted and detected.
- Bob reveals his detection bases x or p for all his measurements using a classical communication channel. They agree to discard all results in which they prepared/measured in conjugate bases.
- Alice and Bob use a subset of the remaining results to check the quality of their correlations and estimate the error rate, which can be used to determine an upper bound on the amount of information possibly available to Eve. If the error rate is too large, Alice and Bob regard transmitted key compromised, they discard it and do not use it in crypting data. They repeat the run.
- If the error rate is acceptable, Alice and Bob use error correction to minimize errors and privacy amplification to minimize Eve's information.

In the of **entangled-photons**, the BB84 protocol takes the following form:

- Alice encodes each random bit value using one of two non-orthogonal polarizations: for example, horizontal (H) or +45º (D) can encode "0", while vertical (V) or −45◦ (E) can encode "1"
- Bob randomly measures each photon's polarization in either of the two conjugate bases (H/V or D/E) and records the results.
- Then, by conventional public communications Alice and Bob reveal their basis choice (but not the bit value) for each detected event, and sift out the (perfectly correlated) set for which they used the same bases, and discard the uncorrelated, wrong-basis events (approximately half of the detected bits in an ideal system). If Eve intercepts every photon, measures its polarization, and sends an appropriately polarized photon on to Bob, she will induce an error rate of 25–50%. The lower limit is obtained only if Eve makes her measurements in the same bases used by Alice and Bob (or in a basis that lies in the same plane on the Poincare sphere: for example, if Alice and Bob use the (H/V) and (D/E) linear polarization bases, then eavesdropping in any linear polarization basis will yield an error rate of 25%. In contrast, eavesdropping in the left/right (L/R) circular polarization basis will induce an error rate of 50% (Naik, 2000).

It can be seen now how Eve's presence is revealed to Alice and Bob. After obtaining the sifted key, they can sacrifice a small part of the bits to test the noise/error-rate of the communication channel: Alice decides which bits and Bob sends publicly their values. Alice then reports back the BER (bit error rate). If this is above 11% (Lütkenhaus, (1999), should Eve be the reason for this high value, it may be assumed that she has had a starting-to-be-viable chance at gaining information on the transmission. Figure 10 (falling curve) shows the set's discarded fraction as a function of sifted key error rate during information reconciliation (Brassard Salvail, 1993), a protocol to eliminate errors in the set used. Privacy

amplification is a method for reducing (and effectively eliminating) Eve's partial information on the transmission. This can be done with a hash function, randomly chosen from a given set of functions, with entry a binary string of length equal to the key and output a shorter string reducing the probability of Eve having knowledge of the new key to a minimal value (calculated as a ratio of the shrinkage factor). Secure transmission is guaranteed for error rate under 11 %.

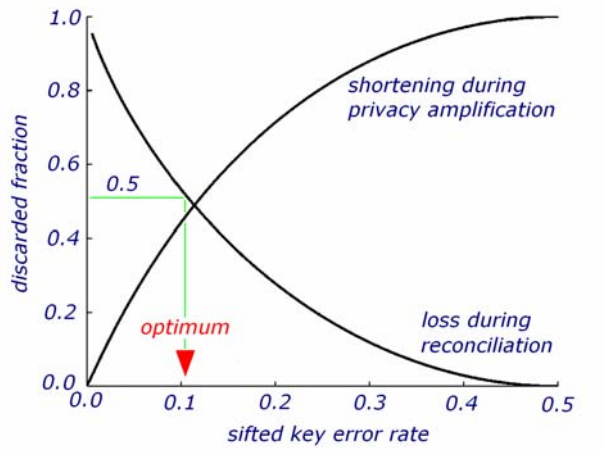

Fig. 10. Losses for Information Reconciliation and Privacy Amplification as a function of sifted key error rate. Secure transmission is guaranteed for error rate < 11%.

3. QUANTGRID – Encryption for GRID Applications

It is evident that this encryption technology is attractive to a number of other technologies relying on encrypted communications, such as bank communications, government communications and of course GRID-computing file transfers.

In this respect a test programme was started in the Institute for Nuclear Physics and Engineering (Particle Physics and IT Department) in collaboration with the Institute for Lasers and Plasma Physics and the Polytechnical University (all Bucharest-Romania). The applications under way in the department concern processing data from CERN's LHC experiments, thus large data fluxes are involved. It is known that quantum encryption equipment produces key rates on the order of a few kbps. These need to be amplified in order to be used for the large amounts of data involved. This can be achieved for instance by taking sections from the last transmitted data segment and AES-encrypting them, then using this volume of key as the actual one to do the encryption.

In the following will be described our quantum encryption stand and the software we produced to use in the actual data transmissions of this project (QUANTGRID, 2010).

3.2 Quantum encryption unit

A number of component providers (Equipment, 2010) exist on the market, the setup here presented being based on Clavis2 components (ID-Quantique, 2009) from ID-Quantique, which offer the possibility of further configuration modification and future experimentation.

The setup in figure 11 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:

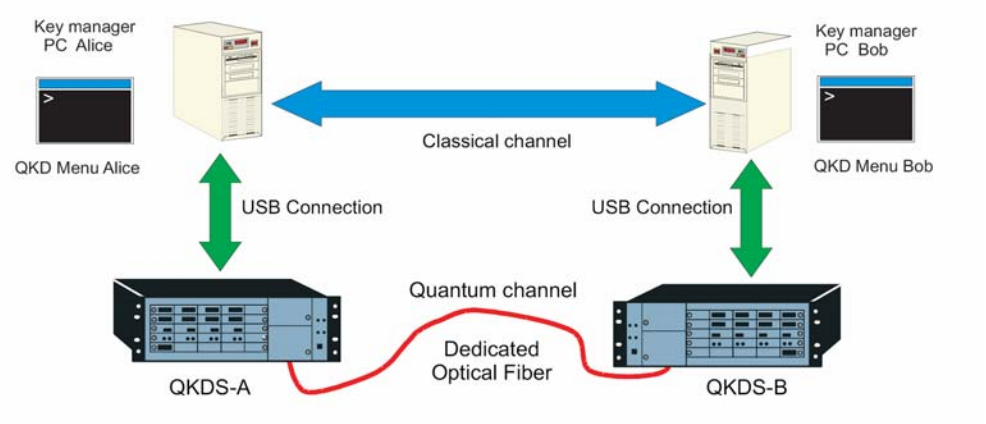

Fig. 11. Communication line setup with two dedicated computers (Bob – receiver and Alice – sender). The quantum channel (23.845 km) is a dedicated optical fiber line, while the classical channel is via LAN Ethernet.

Bob station (receiver) – for an auto-compensated setup, the information Alice sends is physically produced by Bob in the form of intense laser pulses that are sent to Alice, reflected back (phase modulated) and detected by Bob as the 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 of -17 dBm @ 500ps, pulse duration of 300-2500 ps, pulse power measured with a photodiode
- 2 Photon-Counting Detectors: bias voltage controlled, 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° 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 detector 1/2 counts, then sent to the controlling PC via USB/microcontroller.

Fig. 12. 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.

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).

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).

The actual processes that take place on the equipment are numerous, both units, Alice and Bob, being highly automated. The mode of operation of the hardware is in cycles. During each cycle, a complete frame is produced. A cycle contains the following steps (figure 13):

- **Laser pulse train** – the electronics sends a train of laser pulses (period 200 ns) and produces the laser start signal. The number of pulses is limited by the long delay line enclosed in Alice.
- **Alice sync** – synchronization of Alice's clock to the incoming laser pulse train frequency, producing a clock synchronization signal.
- **Alice phase modulation** – phase modulation (PM) gate is then applied on the second component of each pulse. Phase modulation amplitude is chosen randomly from the four states for each pulse. Phase modulation is applied after a fixed Alice coarse delay versus clock synchronization signal, corresponding to the laser pulse train time of flight through the delay line.
- **Bob phase modulation** – phase modulation gate is applied on the first component of each pulse. Phase modulation amplitude is chosen randomly from two states for each pulse. Phase modulation is applied after a fixed Bob PM coarse delay, corresponding to a roundtrip of the laser pulse train time of flight through the transmission line and Alice. The Bob detector-1 Coarse Delay is used as reference point to compute the Bob PM Coarse Delay.
- **Bob detection** – detector-1 and detector-2 (D1 and D2) gates are applied on the single photon detectors to activate them when encoded weak pulses return. These gates are applied after a variable delay – combination of a coarse delay and a fine delay for each detector – versus laser start signal. These variable delays (for D1 and D2) are determined from the line measurement process, so that the detectors are activated when the laser pulses hit them. These delays are independent for each detector.

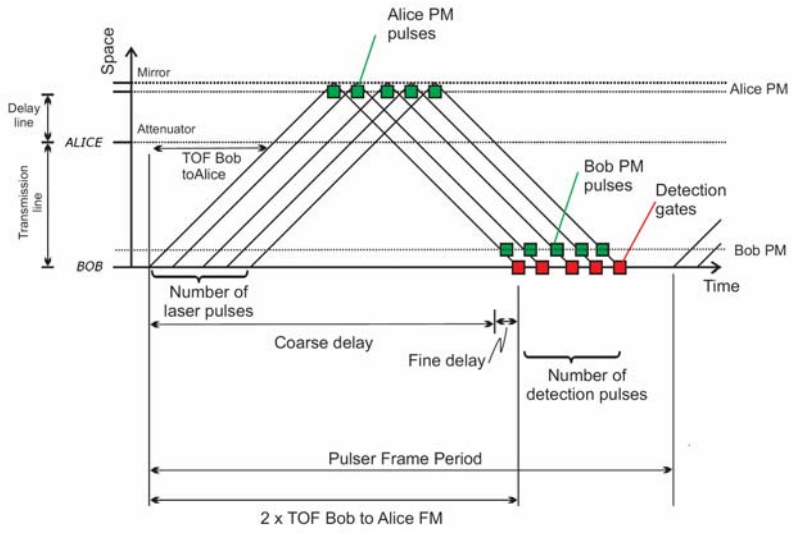

Fig. 13. Time sketch of the processes: Laser pulse train, Alice sync, Alice phase modulation, Bob phase modulation, Bob detection, Next frame, Raw key distillation

- **Next frame** – waiting for the end of the frame period. Next frame cannot be sent if the current frame is not received by Bob entirely.
- **Raw key distillation** – the entire procedure is repeated a number of times until the stop condition applies. Once this state has been reached, the pulser is reset. All measurements (Detection, Alice and Bob Phases) are stored and constitute the raw key. The data is then sent to the controlling computer for distillation and further processing.

3.3 Encryption and communications software

We designed 2 C++ packages enabling us to handle socket communications and AES encryption (SXV4 and AXV4, 2008). In particular we are working on applying the two packages in a hopping-sockets configuration in which we constantly change the connection port (based on a number transmitted in the encryption key) as to avoid software surveillance in the target computer:

- **SXV4** – proprietary C++ class for the handle of socket level communications. This gives us a handle close to the hardware level, of interacting with the communication ports
- **AXV4** – proprietary C++ class implementing the FIPS-197 AES standard. This allows us to take control of the procedure and intervene in taking information from intermediate stages in the en/decryption.

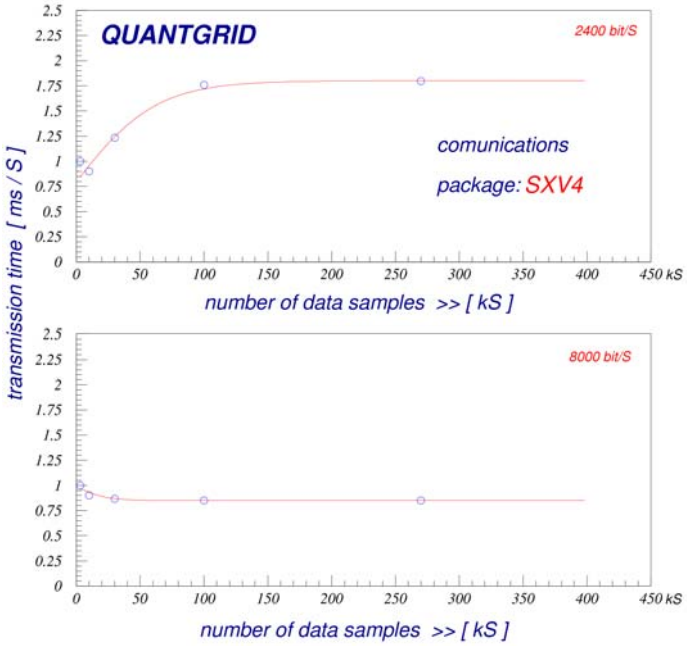

Fig. 14. Server response times package, for 2400 bit/sample and 8000 bit/sample tests. Multiple samples are transmitted for each point on the plots. It can be seen that an optimisation allots high priority to tasks loading the net-card with large data batches, in order to expedite the job, and lessens the priority for small batches of data on the net-card, whether they occur seldomly or frequently.

SXV4 tests – we have tested the C++ package on two servers on the same cluster – which is very similar to the configuration quant-modem-to-GRID port, by sending various data samples, of different lengths. Typical transmit-times are presented in figure 14 - 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. A complete map of tests was performed, in the range of 8, 24, 80, 240, 800, 2400, 8000, 24000 bit/sample.
For large samples (over 8000 bit/sample) the transmission time changes from a slowly rising one to a flat (or faintly decreasing) one, on the order of 1 ms/S. This has to do with the optimisation of large data fluxes (in a single connection) on ports.
AXV4 tests – we have tested the C++ package as AES is known to be somewhat slow on decryption. Indeed, in our implementation of the FIPS-197 standard we found it to be 5 times slower in decryption over encryption. Also, importantly, whereas for small versus large file sizes the time/character varies within 30% for decryption, for encryption this ratio is roughly a factor of 8 (figures 15 – encryption, and 16 – decryption).

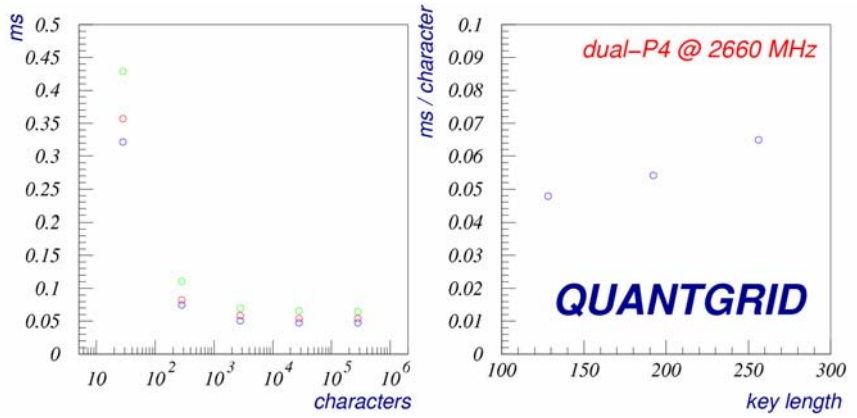

Fig. 15. Performance of AXV4 in encrypting a file function of file size (saturation on the order of 60 μs/character, for file above 2000 characters) – left. Performance function of the key length used (blue = 128 bit, red = 192, green = 256) – right. A linear dependence with key size is observed.

This is important in timing both sender and receiver processes such that they have the proper time in performing the necessary packing/unpacking, switching ports, etc.
Another interesting factor we looked for in the tests was the relative advantage time wise versus the key length used – on a dual-P4 2.66 Pentium machine:

- **128 bit key** – for this key length the average encryption time per character ranges exponentially decreasing from 0.32 ms/character (at 10 characters/file) down to 0.05 ms/character (at 300000 characters/file). For decryption the same numbers are 0.32 ms/character and 0.25 ms/character (a ratio of 1.28 vs. 6.4 for encryption).
- **192 bit key** – for this key length the average encryption time per character ranges exponentially decreasing from 0.36 ms/character (at 10 characters/file) down to 0.06 ms/character (at 300000 characters/file). For decryption the same numbers are 0.39 ms/character and 0.31 ms/character (a ratio of 1.26 vs. 6.0 for encryption).

- **256 bit key** – for this key length the average encryption time per character ranges exponentially decreasing from 0.43 ms/character (at 10 characters/file) down to 0.07 ms/character (at 300000 characters/file). For decryption the same numbers are 0.41 ms/character and 0.37 ms/character (a ratio of 1.10 vs. 6.1 for encryption).

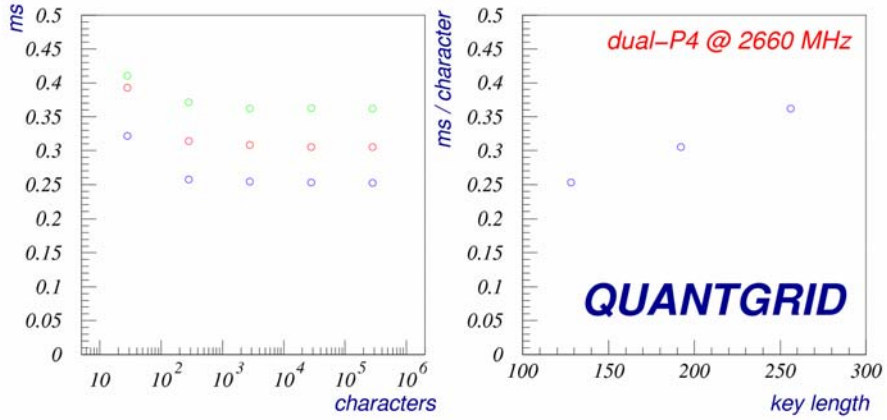

Fig. 16. Performance of AXV4 in decrypting a file function of file size (saturation on the order of 60 μs/character, for file above 2000 characters) – left. Performance function of the key length used (blue = 128 bit, red = 192, green = 256) – right. A linear dependence with key size is observed.

7. Conclusion

Quantum encryption is a very promising technology in securing data transfers – as shown, a number of quantum methods being available – each with its own advantages: simpler practical implementation, stability to thermal drift, immunity to eavesdropping, higher key generation rate. So far commercial components exist mostly in the form of polarisation and phase encoding.

Implementation in GRID-computing depends, at the moment at least, on boosting the key generation rate from a few kbps to at least a few 0.1 Mbps. This can be achieved for instance by using the quantum key to AES-encrypt sections of the transmitted data, and then use the resulting volume as key.

The project here presented, QUANTGRID, is a first attempt at using this technology in GRID data transfers. Auxiliary software was developed for embedding quantum keys in the transfers: a proprietary sockets package that allows to hop the communication port on the target machine avoiding surveillance software and an AES encryption package that allows to take control of the procedure and intervene in taking information from intermediate stages in the en/decryption. The project – funded under D11-044 (CNMP-Romania, for the quantum technology) and in part by PN-09370104 (ANCS-Romania, for the GRID technology) – is ongoing.

8. References

Salomaa, A. (1990). *Public-Key Cryptography,* Springer-Verlag, ISBN 3540613560, 9783540613565, Berlin, New York, London, Paris, Tokyo, 1996

Shor, P.W. (1994). Algorithms for quantum computation: discrete logarithms and factoring, *Proceedings of Foundations of Computer Science*, pp. 124 - 134, ISBN 0-8186-6580-7, Santa Fe, NM-US, November 1994 , IEEE Computer Society Press, Los Alamitos, CA-US

Daemen J. and Rijmen V. (2006). The Block Cipher Rijndael, in: *Lecture Notes in Computer Science,* 277-284, Springer-Verlag, ISBN 0302-9743, Berlin, Heidelberg; Federal Information Processing Standards Publication 197/Nov-2001 following Section 5131 of the Information Technology Management Reform Act (Public Law 104-106/1996) and Computer Security Act (Public Law 100-235/1987).

Biryukov A. and Khovratovich D. (2009). Related-Key Cryptanalysis of the Full AES-192 and AES-256, *Proceedings of Advances in Cryptology - ASIACRYPT 2009, 15th Intn.'l Conf. on the Theory and Application of Cryptology and Information Security*, pp. 1-18, ISBN 978-3-642-10365-0, Tokyo-Japan, December 2009, Matsui, Mitsuru (ed.), Springer-Verlag Berlin

Hathaway L. (2003). National Policy on the Use of the Advanced Encryption Standard (AES) to Protect National Security Systems and National Security Information.

Vernam G.S. (1926). Cipher Printing Telegraph Systems For Secret Wire and Radio Telegraphic Communications. *Journal of the IEEE,* Vol. 55, pp 109-115

Willan P. (2004). EU seeks quantum cryptography response to Echelon, in *Network World*, of 17.05.2004

Dusek M., Haderka O., Hendrych M. (1999). Generalized Beam-Splitting Attack in Quantum Cryptography with Dim Coherent States, *Opt. Comms*. 169, pp. 103-108

D.S. Lemelle, M.P. Almeida, P.H. Souto Ribeiro, S.P. Walborna (2006). A simple optical demonstration of quantum cryptography using transverse position and momentum variables, *Am. J. Phys.,* Vol. 74, pp 542-546

M. Hendrych (2002), *Experimental Quantum Cryptography*; also M. Dušck, O. Haderka, M. Hendrych, Practical Aspects of Quantum Cryptography, *Book Quantum Communication, Computing, and Measurement 2,* pp. 393-398, ISBN 978-0-306-46307-5, May 2007, Springer-Verlag US

Bennett C.H., Brassard G. (1984). Public Key Distribution and Coin Tossing, *Proceedings of IEEE International Conference on Computers Systems and Signal Processing*, pp. 175-179, Bangalore-India, 1984, IEEE, New York

D.S. Naik, C.G. Peterson, A.G. White, A.J. Berglund, P.G. Kwiat (2000). Entangled State Quantum Cryptography: Eavesdropping on the Ekert Protocol, *Phys. Rev. Lett..,* Vol. 84, pp 4733-4736

Lütkenhaus N. (1999). Estimates for practical quantum cryptography, *Phys. Rev.* . A59, pp. 3301-3319

Brassard G. and Salvail L. (1993). Secret key reconciliation by public discussion, *Proceedings of Advances in Cryptology: Eurocrypt'93*, pp. 410-423, ISBN 3-540-57600-2, Lofthus-Norway, May 1993, Lecture Notes in Computer Science 765, Springer-Verlag Berlin

QUANTGRID (2010) – project D11-044 "QUANTGRID" financed through the National Center for Programme Management (CNMP-Romania)

Equipment (2010) – ID-Quantique (Geneva), MagiQ (Boston), QuintessenceLabs (Canberra), SmartQuantum (Paris)

ID-Quantique (2009) – ID-3100 Clavis2 Components Documentation v1.1, Feb. 2009, © ID-Quantique

SXV4, AXV4 (2008) – QUANTGRID Activity Report 2008.