Supplementary information for "High-rate quantum key distribution using Gaussian-modulated coherent states"

Frédéric Grosshans*, Gilles Van Assche†, Jérôme Wenger*, Rosa Brouri*,
Nicolas J. Cerf† & Philippe Grangier*

* *Laboratoire Charles Fabry de l'Institut d'Optique, CNRS UMR 8501, 91403 Orsay, France*

† *Ecole Polytechnique, CP 165, Université Libre de Bruxelles, 1050 Bruxelles, Belgium*

Experimental set-up.

The source consists of a CW laser diode (SDL 5412) at 780nm associated with an acousto-optic modulator, used to chop pulses with a duration 120ns (full width at half-maximum), at a repetition rate 800kHz. To reduce the excess noise, a grating-extended external cavity is used, and the beam is spatially filtered using a single mode fiber. Light pulses are then split onto a beam-splitter, one beam being the local oscillator (LO), the other Alice's signal beam. The data is organised in bursts of 60,000 pulses, separated by time periods used to lock the phase of the LO, and sequences of pulses to synchronize the parties. In the present experiment, there is a burst every 1.6 seconds, corresponding to a duty cycle of about 5%, which is obviously under-optimised but should be easy to improve in further experiments.

The coherent state distribution is generated by modulating both the amplitude and phase of the light pulses with the appropriate probability law. In the present experiment, the amplitude of each pulse is arbitrarily modulated at the nominal 800 kHz rate by an integrated electro-optic LiNbO3 Mach-Zehnder interferometer. In contrast, due to the unavailability of a fast phase modulator at 780 nm, the phase is not randomly modulated but scanned continuously from 0 to 2π using a piezoelectric transducer (PZT). For such a deterministic phase variation, the security of the protocol is not warranted, and thus no genuine secret key could be distributed strictly speaking. However, the experiment provides realistic data, having exactly the awaited structure provided that random phase permutation on Bob's data are performed.

Due to an imbalance between the paths of the interferometer which modulates the amplitude of the signal beam, the extinction is not strictly zero. In the present experiment that is only aimed at a proof of principle, we substract the offset field from the data received by Bob. In a real cryptographic transmission, the offset field should be compensated by Alice, either by adding a zeroing field, or by using a better modulator.

All voltages for the electro-optic modulator or the PZT are generated by an acquisition board (National Instruments PCI6111E) connected to a computer. Although all discussions assume the modulation to be continuous, digitised voltages are used in practice. With our experimental parameters, a resolution of 8 bits is enough to hide the amplitude or phase steps under the shot noise. Since the modulation voltage is produced using a 16 bits converter, and the data is digitised over 12 bits, we may fairly assume the modulation and measurement to be continuous.

The homodyne detection was checked to be shot-noise limited for LO power up to 5 10^8 photons/pulse. In the present experiment, we used 1.3 10^8 photons/pulse for LO power, while each signal pulse contains up to 250 photons. Depending on the run, the overall detection efficiency is either 0.81 or 0.84, due to optical transmission (0.92), mode-matching visibility (0.96 or 0.99) and photodiode quantum efficiency (0.92).

The experiment is thus carried out in such a way that all useful parameters can be measured experimentally. Reconciliation and privacy amplification protocols can thus be performed in realistic – though not fully secret – conditions. The limitations of the present set-up are essentially due to the lack of appropriate fast amplitude and phase modulators at 780 nm. This should be easily solved by operating at telecom wavelengths (1540-1580 nm) where such equipment is readily available. Let us point out also that it is not convenient to transmit separately the signal and LO, so a better solution would be to use a frequency sideband technique similar to Mérolla *et al.* [S1]. Then all light pulses are transmitted together along the same fiber, and a separate radio-frequency is sent from Alice to Bob in order to reconstruct the optical phase information.

Hypothesis about the detector's noise : "realistic" vs "paranoid" assumptions

After the quantum exchange, Alice and Bob reveal a subset of their values taken randomly to evaluate the transmission G and the total added noise variance. This variance has four contributions: the shot noise N_0, the channel noise $\chi_{line} N_0$, the electronics noise of Bob's detector ($N_{el} = 0.33\ N_0$), and the noise due to imperfect homodyne detection efficiency ($N_{hom} = 0.27\ N_0$). The two detection noises N_{el} and N_{hom} originate from Bob's detection system, so one may reasonably assume that they do not contribute to Eve's knowledge. This "realistic" assumption has been followed in the article. In that case, the noise from Bob's detection system also affects Eve's information so, in eq (4b), we take $(V_{B|E})_{min} = N_0 / \{G_{line} (\chi_{line} + V^{-1}) \} + N_{el} + N_{hom}$, where G_{line} stands for the line transmission.

In contrast, in a "paranoid" approach, one should assume that the noises N_{el} and N_{hom} are also controlled by Eve, that gives her a supplementary advantage. In that case,

$(V_{B|E})_{min}$ will be given by $N_0 / \{G (\chi + V^{-1})\}$, where G now includes both the line and detection efficiencies and χ includes both the line and detection noises. In all cases, the value of I_{BA} is given by eq. (4a), where χ is the total equivalent noise including both transmission and detection.

Presently we were able to extract practically a key with up to 3.1dB losses under the "realistic" approach with a reverse reconciliation protocol. Considering now the "paranoid" assumption and reverse reconciliation, the ideal secret key rate is 420 kb/s for a lossless line, and 200 kb/s for G_{line}= 0.79 (1.0dB). However, secret bits could be delivered only in the lossless case, at a practical rate of 195 kb/s. It is clear that an increase in the reconciliation efficiency would immediately translate into a larger achievable range. Let us point out that we always assume in both the “realistic” or the “paranoid” approach that Eve has an ideal software, quantum memories, perfectly entangled beams, etc. If any of these hypothesis is relaxed, the practical secure range may be extended over the “threshold” presently set by the limited reconciliation efficiency. However, it is not the purpose of the present paper to discuss such “constrained attacks”.

Implementation of secret key distillation.

Secret key distillation was performed by a computer program written in standard C++ that implements the steps described in the paper. Although Alice's and Bob's data are both processed on the same computer, it is done in the same way as if the parties were distant and were using a network connection as classical channel. The particular platform used is a regular PC running Linux.

As bursts of data are input to the program, a part of the Gaussian key elements are sacrificed and used to estimate the characteristics of the quantum channel. This includes the variances and the correlation coefficient between both sides, which would be exchanged between Alice and Bob over the public authenticated classical channel in a real-life setup.

Depending on the value of the estimated I_{AB}, the two parties agree on appropriate binary functions (slices [S2,S3]) that will transform their Gaussian values into bits. These bits are then reconciliated, as described in the paper, with sliced error correction[S2,S3] and an implementation[S4] of Cascade[S5] as a sub-routine. In our implementation, 5 binary functions are used per Gaussian key elements, out of which 2 or 3 (depending on I_{AB}) are fully disclosed, while the remaining 3 or 2 are reconciliated using Cascade.

Next, the data are moved to the privacy amplification routine. Excluding the bits that are fully disclosed and from which no secret key can be extracted, the reconciliated bits are processed by use of a transformation randomly taken in a universal class of hash functions[S6,S7], which in our case is the class of truncated linear functions in a finite field. First, we consider the reconciliated bits as coefficients of a binary polynomial in a representation of the Galois field $GF(2^{110503})$, hereby called the reconciliated polynomial. Then Alice and Bob publicly and randomly choose a random element of the same field and multiply the reconciliated polynomial with this chosen element. Finally, they extract from the resulting polynomial the desired number of least significant bits. In our implementation, the representation of the field is $GF(2)[x]/(p)$, where $p = x^{110503}+x^{519}+1$ is an irreducible polynomial over $GF(2)$, see ref.[S8]. The fact that this operation can be implemented efficiently[S9] motivated our choice. The size of the field allows us to process up to 110503 bits at once, or equivalently blocks of about 55200 Gaussian key elements when Cascade operates on 2 bits per Gaussian key element or of 36800 elements with 3 bits per element. To produce a longer key, the Gaussian key elements must thus be grouped into blocks.

As explained in the paper, the number of bits that are destroyed by privacy amplification depends on the amount of information that could be inferred by a potential eavesdropper. An easvesdropper Eve has two sources of knowledge. First, she may have attacked the quantum channel and second, she knows the error positions of the reconciliated bits from listening to the execution of Cascade. Let K be the final key, E the ancilla Eve uses for quantum eavesdropping, and Delta the error positions revealed during reconciliation. We thus need to evaluate I(K;E,Delta) = I(K;E) + I(K;Delta|E). The first term on the rhs is upper bounded by I_{BE} (in RR) or I_{AE} (in DR), while the second term is evaluated numerically for an entangling cloner attack.

This numerical evaluation of I(K;Delta|E) comes down to integrating I(K;Delta|E=e) for all possible outcomes e of E, weighted by the probability density function p(e) of E. In the case of the entangling cloner attack, E refers both to the knowledge of Eve's half of the EPR state she injects and to her eavesdropping of the state being sent to Bob, and so E denotes a bivariate Gaussian variable whose covariance matrix can be calculated from the channel characteristics (i.e., attenuation and added noise amplitude). For a given outcome e of E, Eve can infer A and B, Alice's and Bob's key elements as a bivariate Gaussian variable. Since K and Delta are discrete functions of only A and B, the probability distribution of K(A,B) and Delta(A,B) conditionally on E=e can be calculated, hence giving I(K;Delta|E=e).

Finally, a part of the generated key is used to encrypt[S10] the execution of the reconciliation for the next block. The remaining bits, namely the net secret key, can be then used for instance to encrypt the classical communications between Alice and Bob using a one-time pad.

References

S1. Mérolla, J.-M., Mazurenko, Y., Goedgebuer, J.-P. and Rhodes, W. T. Single Photon Interference in Sidebands of Phase-Modulated Light for Quantum Cryptography, *Phys. Rev. Lett.* 82, 1656-1659 (1999).

S2. Van Assche, G., Cardinal, J. & Cerf, N. J. Reconciliation of a quantum-distributed Gaussian key. *E-print arXiv:cs.CR/*0107030 (2001).

S3. Cerf, N. J., Iblisdir, S. & Van Assche, G. Cloning and cryptography with quantum continuous variables. *Eur. Phys. J. D* 18, 211-218 (2002).

S4. Nguyen, K. *Extension des Protocoles de Réconciliation en Cryptographie Quantique,* Master Thesis, (Université Libre de Bruxelles, Bruxelles, 2002).

S5. Brassard, G. & Salvail, L. Secret-key reconciliation by public discussion. *Advances in Cryptology - Eurocrypt'93, Lecture Notes in Computer Science,* 411-423 (Springer-Verlag, New York, 1993).

S6. Bennett, C. H., Brassard, G., Crépeau, C. & Maurer, U. M. Generalized privacy amplification. *IEEE Trans. on Inform. Theory* 41, 1915-1935 (1995).

S7. Carter, J. L. & Wegman, M. N. Universal Classes of Hash Functions. *J. of Comp. and Syst. Sci.* 18, 143-154 (1979).

S8. Brent, R. P. Larvala, S. & Zimmermann, P. A fast algorithm for testing irreductibility of trinomials mod 2. *Tech. Rep., Oxford University Computing Laboratory*, 1-16 (2000).

S9. Schönhage, A. Schnelle Multiplikation von Polynomen über Körpern der Charakteristik 2. *Acta Informatica* 7, 395-398 (1977).

S10. Lo, H.-K., Method for decoupling error correction from privacy amplification. *Eprint arXiv: quant-ph/* 0201030 (2002)

Correspondence and requests for materials should be addressed to Philippe Grangier (philippe.grangier@iota.u-psud.fr).