Multidimensional reconciliation for continuous-variable quantum key distribution

Anthony Leverrier*, Romain Alléaume*, Joseph Boutros†, Gilles Zémor‡ and Philippe Grangier§
* TELECOM ParisTech
46, rue Barrault, 75634 Paris Cedex 13, France
Email: anthony.leverrier@enst.fr
†Texas $A\&M$ University at Qatar, Doha, Qatar
‡Institut de Mathématiques de Bordeaux, Université de Bordeaux 1,
Bordeaux, France
§Laboratoire Charles Fabry, Institut d'Optique, CNRS, Univ. Paris-Sud,
Campus Polytechnique, RD 128, 91127 Palaiseau Cedex, France

***Abstract*— We propose a method for extracting an errorless secret key in a continuous-variable quantum key distribution protocol, which is based on Gaussian modulation of coherent states and homodyne detection. The crucial feature is an eight-dimensional reconciliation method, relying on the algebraic properties of octonions. By using this coding scheme with an appropriate signal-to-noise ratio, the distance for secure continuous-variable quantum key distribution can be significantly extended.**

I. Introduction, context and previous work

Quantum key distribution (QKD) schemes [1] have led to the following scenario: Alice and Bob each are provided with correlated random variables, X and Y, respectively, and wish to extract a random secret key by discussion over a public channel, in presence of an eavesdropper, Eve, who is in possession of a third correlated variable Z. The key extraction strategy is classically split into two steps. In the first step, Alice and Bob, *reconcile* their data, i.e., Alice sends some extra public information to Bob, which, with the help of Y, enables Bob to recover X. In the second step, the *privacy amplification* phase [2], Alice randomly chooses, and publicly communicates to Bob, a compression function g, picked from a carefully prearranged set. The shared secret is then $g(X)$.

When X, Y and Z are classical variables, the size of the secret can in principle be arbitrarily close to $I(X;Y) - I(X;Z)$ [3]. In a more general setting, the variable of Eve should be considered to be a quantum state instead of a classical variable, and the size of the secret becomes $I(X;Y) - S(X;Z)$ where $S(X;Z)$ refers to the quantum mutual information [4] between X and the quantum state Z. This formula has also been proven to hold when X and Y refer to continuous variables [5], [6]. One might wonder why two different measures of information are needed to express the size of the secret. The reason for this comes from the different assumptions made on Alice's, Bob's and Eve's capabilities: while Eve is not supposed to be limited by any technological constraint (in particular, she has access to a quantum memory or even a quantum computer if she wants to), Alice and Bob live in our world and are restricted to use only classical equipment.

In this paper, we focus on continuous-variable protocols and more especially on the case when X and Y are *Gaussian* vectors. The real challenge here lies in the reconciliation phase, where Alice must communicate the minimum possible quantity of information to Bob that is sufficient for him to recover X

In the discrete setting, e.g. when X and Y are binary strings, it is folklore that the way to achieve reconciliation is for Alice to send to Bob the syndrome of X for a properly chosen linear code C [7]. By properly chosen one means a code achieving the capacity of the channel between Alice and Bob, i.e., whose dimension is close to but a little less than $I(X;Y)$. Bob is thus given a code C_X that X belongs to (namely the set of vectors with the same syndrome as X), and a noisy version Y of X that is just enough for him to recover X by decoding Y. Note that it is important to be able to measure the information given by C_X on the random variable X. To be more accurate, one should be able to estimate the value of $S(X;Z,C_X)$. A possibility is to make sure that the *a priori* distribution of X in the coset code C_X is uniform, meaning $P(X = x \mid C_X) = 1/2^k$ for every $x \in C_X$ and where $k = \dim C_X$. This is easily achieved by choosing the code C randomly and *independently* of X. In practice we will not choose a completely random code, but one for which we have a practical decoding algorithm and is close enough to the channel capacity. Fortunately, LDPC codes and turbo codes satisfy these requirements. Note that it is not strictly necessary for the code C_X to be the coset code of some linear code C, it is simply convenient.

In the Gaussian setting, one could in principle achieve channel capacity by choosing for C_X a random spherical code, i.e., a set of vectors of cardinality a little less than $2^{I(X;Y)}$, lying on the n-dimensional sphere centered on the origin and of radius $\|X\|$. However we face two practical challenges, namely decoding C_X and making sure that the *a priori* distribution of X in C_X is uniform. Another possibility consists in first quantizing X then using only a finite number l of bits to describe the code containing the quantized version of X [8]. One can show that Eve cannot gain more than l

978-1-4244-2571-6/08/$25.00 ©2008 IEEE

bits of information about X, even in a quantum context [9]. Whereas this method is particularly well suited for high signal-to-noise ratios (SNR), it is not so efficient for low SNR, which is problematic since it is the situation one encounters when performing quantum key distribution (QKD) over reasonable distances (a few tens of kilometers). In fact, we are here particularly interested in the case where the SNR is low, meaning that $I(X;Y) \leq n$ where n is the dimension of X and Y.

In real-world continuous-variable quantum key distribution schemes, two practical suggestions have been put forward and implemented. The first scheme, *slice reconciliation* [8], [10], consists in quantizing X and performs poorly at low SNR, mainly because it breaks the Gaussian symmetry of the problem. In the second scheme [11], [12], Alice reveals the absolute value $|x_i|$ of each component of $X = (x_1 \cdots x_n)$. The information is then coded in the sign of each x_i. This simple scheme suffers some limitations for a Gaussian modulation of X since the Gaussian distribution is centered around 0 and most of the data will consequently have a small absolute value, meaning that their sign will be difficult to discriminate. To overcome this problem, it has been proposed to use post-selection [12], [13] to get rid of the low-amplitude data and only keep the more meaningful large-amplitude data. Unfortunately, this approach has a major drawback in terms of security since the status of the post-selected data is still unclear and might allow Eve to implement some powerful attacks.

Here we are interested in generalizing the second scheme in a way that does not require post-selection anymore. This can be done by defining the code C_X in two steps. First, one defines on the sphere of radius $\|X\|$ an isomorphic image Q_X of the n-dimensional Hamming cube $\mathbb{F}_2^n$. Given Q_X, the channel between Alice and Bob becomes a binary input additive white Gaussian noise (AWGN) channel. Then we are almost back to the discrete case and the problem becomes simply that of defining an efficiently decodable code $C_X \subset Q_X$ that comes close to the new channel (sub)capacity: in practice an LDPC code is used. Note that if the SNR is low enough, this subcapacity is almost equal to the capacity of the channel, which would be attained for a Gaussian modulation. In this setting, the new challenge is to find the best way of defining the cube Q_X. We have three requirements:

- Giving Q_X should not leak more information on X than is necessary, this again means that the *a priori* distribution of X in Q_X should be uniform.
- The resulting channel capacity between Alice and Bob should be as large as possible.
- Defining Q_X should be realisable in practice: actual values of n range from 10^5 to 10^6. The reason for this is twofold: one needs long codes to reasonably approach the Shannon limit of the channel, and the use of long blocks is also necessary in order to reduce the uncertainty on $I(X;Y) - S(X;Z)$ due to the estimation of the channel parameters.

In the present work we shall study a definition of Q_X which performs better than previous protocols at low SNR without requiring any post-selection. The rest of the paper is organised as follows: Section II gives restrictions on the dimension n of the space for which efficient descriptions of cubes Q_X can be done. Section III is concerned by the description of such cubes and presents a realistic reconciliation protocol for continuous-variable Quantum Key Distribution, whose performance is analyzed in Section IV.

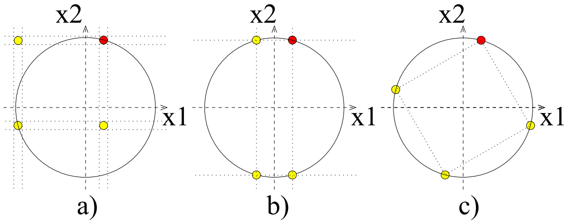

Fig. 1. Consider two successive states X_1, X_2 sent by Alice: the states really sent correspond to $X_1 > 0, X_2 > 0$. Figures a), b) and c) show the cube Q_X described by Alice for three different reconciliation protocols. a) corresponds to slice reconciliation [8], [10]: the four states are well separated but the Gaussian symmetry is broken, b) corresponds to the case where the information is encoded on the sign of the Gaussian value [12]: the symmetry of the problem is preserved but some states are very close and thus difficult to discriminate, c) corresponds to the approach presented in this paper where the states are well separated and the symmetry is preserved.

II. Efficient orthogonal transformations of $\mathbb{R}^n$

The idea that we shall pursue here is best described in dimension $n = 2$. Figure 1 presents an example of the description of Q_X for different reconciliation protocols. One can easily see that the best way to describe Q_X is to respect the Gaussian symmetry (which translates into a spherical symmetry) while maximizing the distances between the different code words of C_X. The natural solution is to take for Q_X a cube of width $2\|X\|/\sqrt{n}$ inscribed in the sphere $\mathcal{S}^{n-1}(\text{O}, \|X\|)$ and containing X.

The norm of X follows a χ^2 distribution with n degrees of freedom which becomes a Dirac distribution for $n \gg 1$. Hence, Alice can reveal the value of $\|X\|$ to Bob without any significant loss of information, or equivalently use the normalized variable $X/\|X\|$ instead of X. Therefore, given $X \in \mathcal{S}^{n-1}$, one needs to define a cube Q_X centered on 0 and containing X such that the *a priori* distribution of X given Q_X is uniform. The easiest way to describe such a cube is simply to describe the orthogonal transformation transporting the canonical cube (whose vertices have coordinates $\pm 1/\sqrt{n}$) on the considered cube. In dimension 2, this method works well since Alice just needs to give Bob an angle in order to define the square containing X. We are interested in generalizing this method to higher dimensions.

The protocol would then be the following: Alice chooses randomly one of the vertices U of the canonical cube of $\mathbb{R}^n$ and gives to Bob the orthogonal transformation $M(X,U)$ mapping X on U. This transformation defines the cube Q_X. If

Alice has chosen U among an appropriate binary code C, then Bob can recover U from the knowledge of Y and $M(X,U)$. There are many such mappings M, but one needs a mapping easy to describe and to compute. An example is the reflection across the mediator hyperplane of X and U. Unfortunately, such an orthogonal transformation leaks some information about X and U because the distribution of X given $M(X,U)$ is not uniform for $n > 2$ due to the phenomenon of the concentration of the measure for spheres in dimensions $n > 2$, and therefore cannot be used by Alice in a QKD protocol.

A solution that does not give unnecessary information about X is to randomly choose an orthogonal transformation with uniform probability in the ensemble of orthogonal transformations mapping X to U. However, randomly generating such a transformation is not doable in practice for $n \gg 1$. For instance, generating a random orthogonal transformation on $\mathbb{R}^n$ requires one to draw an $n \times n$ Gaussian random matrix and to calculate its QR decomposition, i.e., its decomposition into an orthogonal and a triangular matrix which is an operation of complexity $O(n^3)$.

A practical solution involves the following. First, Alice and Bob agree publicly on a code C, then for each word $X \in \mathcal{S}^{n-1}$ sent by Alice and for each code word $U \in C \subset \mathcal{S}^{n-1}$ chosen by Alice, there should exist an continuous application M of the variables X and U such that $M(X,U) \in \mathrm{O}_n$ and $M(X,U)X = U$. Therefore if Alice gives $M(X,U)$ to Bob, she describes a cube Q_X containing X inscribed on the n-dimensional sphere and the code C_X is defined as the image of C by M^{-1}. The following theorem shows that the existence of such an application M restricts the possible values of n to be 1, 2, 4 or 8.

Let us first recall a result from Adams [14], which quantifies the number of independent vector fields on the unit sphere of $\mathbb{R}^n$:

Theorem 1: For $n = a \cdot 2^b$ with a odd and $b = c + 4d$, one defines $\rho_n = 2^c + 8d$. Then the maximal number of linearly independent vector fields on $\mathcal{S}^{n-1}$ is $\rho_n - 1$.

In particular, the only spheres for which there exist $(n-1)$ independent vector fields are the unit spheres of $\mathbb{R}$, $\mathbb{R}^2$, $\mathbb{R}^4$ and $\mathbb{R}^8$, which can, respectively, be seen as the units of the real numbers, the complex numbers, the quaternions and the octonions.

Theorem 2: If there exists a continuous application:

$$\begin{array}{rcl} M : \mathcal{S}^{n-1} \times \mathcal{S}^{n-1} & \longrightarrow & \mathrm{O}_n \\ (X,U) & \longmapsto & M(X,U) \end{array}$$

such that $M(X,U)X = U$ for all $X, U \in \mathcal{S}^{n-1}$, then $n = 1, 2, 4$ or 8.

Proof: The idea of the proof is to use the existence of such a continuous function M to exhibit a family of $(n-1)$ independent vector fields on S^{n-1}.

Let $(e_1, e_2, \ldots, e_n)$ be the canonical orthonormal basis of $\mathbb{R}^n$. For $1 \leq i \leq n$, let $u_i(x) = M(e_n, x)e_i$. One has: $u_n(x) = x$ and

$$(u_i(x)|u_j(x)) = e_i^T M(e_n,x)^T M(e_n,x) e_j = \delta_{i,j}$$

since $M(e_n, x) \in \mathrm{O}_n$. Then, for $x \in \mathcal{S}^{n-1}$, $u_1(x), u_2(x), \ldots, u_{n-1}(x)$ are $(n-1)$ independent vector fields on $\mathcal{S}^{n-1}$ and finally $n = 1, 2, 4$ or 8. □

III. Rotations on $\mathcal{S}^1$, $\mathcal{S}^3$ and $\mathcal{S}^7$

Now that we have proved that such an application M can only exist in $\mathbb{R}$, $\mathbb{R}^2$, $\mathbb{R}^4$ and $\mathbb{R}^8$, we will exhibit such applications that can be described and computed efficiently and prove that they do not leak unnecessary information to Eve. Note that the trivial case of $\mathbb{R}$ for which the unit sphere is $\{-1, 1\}$ corresponds to the method where one encodes a bit in the sign of the Gaussian variable [12].

A. Existence

Let us start with the easiest case: $\mathbb{R}^2$. The existence of such an application M verifying $M(X,U)X = U$ for the unit circle is obvious: it is simply the rotation centered on 0 of angle $\mathrm{Arg}(U) - \mathrm{Arg}(X)$ where $\mathrm{Arg}(X)$ denotes the angle between X and the x-axis. An alternative way to see M is $M(X,U) = U \cdot X^{-1}$ where X and U are identified with complex numbers of modulus 1. The same is true for dimensions 4 and 8 where $\mathcal{S}^3$ and $\mathcal{S}^7$ can, respectively, be identified with the units of the quaternions and the octonions, and for which a valid division exists.

B. Computation of $M(x, y)$

For $n = 2, 4$ and 8, there exists a (non-unique) family of n orthogonal matrices $\mathcal{A}_n = (A_1, \ldots, A_n)$ of $\mathbb{R}^{n \times n}$ such that $A_1 = \mathbb{1}_n$, and for $i, j > 1$, $\{A_i, A_j\} = -2\delta_{i,j}\mathbb{1}_n$ where $\{A, B\}$ is the anti-commutator of A and B. An example of these families is explicitly given in Section V. The following Lemma shows how to use such a family to construct a continuous function M with the properties described above.

Lemma 1: $M(X,U) = \sum_{i=1\ldots n} \alpha_i(X,U) A_i$ with $\alpha_i(X,U) = (A_i X|U)$ is a continuous map from $\mathcal{S}^{n-1} \times \mathcal{S}^{n-1}$ to O_n such that $M(X,U)X = U$.

Proof: First, because of the anti-commutation property, one can easily check that the family $(A_1X, A_2X, \ldots, A_nX)$ is an orthonormal basis of $\mathbb{R}^n$ for any $X \in \mathcal{S}^{n-1}$. Then, for any $X, U \in \mathcal{S}^{n-1}$, $(\alpha_1(X,U), \ldots, \alpha_n(X,U))$ are the coordinates of U in the basis $(A_1X, A_2X, \ldots, A_nX)$. This proves that $M(X,U)X = U$. Finally, the orthogonality of $M(X,U)$ follows from some simple linear algebra. □

Therefore $\alpha = (\alpha_1, \ldots, \alpha_n)$ is sufficient to describe $M(X,U)$ and the computation of α_i can be done efficiently since the matrices A_i are permutation matrices with a change of sign for some coordinates. In the QKD protocol, Alice chooses randomly U in a finite code and gives the value of $\alpha(X,U)$ to Bob, who is then able to compute $M(X,U)Y$ which is a noisy version of U. One should note that the final noise is just a “rotated” version of the noise Bob has on X: in particular, both noises are Gaussian with the same variance. This is true because the Gaussian distribution of the noise is invariant under orthogonal transformations.

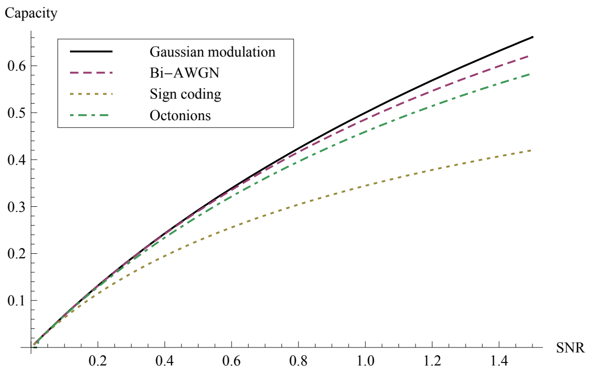

Fig. 2. Capacity of the Gaussian channel and subcapacities for the different binary channels mentionned in the text: Bi-AWGN channel (corresponding to a rotation in $\mathbb{R}^n$ for $n \gg 1$), "sign coding" [12] and the mulidimensional reconciliation based on the properties of the octonions

C. No leakage of information

In order to prove that $\alpha = M(X,U)$ does not give any information about $U \in C$ (where C is the code on which Alice and Bob agreed beforehand), one needs to show that the *a priori* distribution of U given α is uniform. This is true because X and U have uniform distributions on $\mathcal{S}^{n-1}$ and on C, respectively, and because the function:

$$\begin{array}{rcl} f_U : \mathbb{R}^n & \longrightarrow & \mathbb{R}^n \\ x & \longmapsto & f_U(x) = \alpha \text{ with } \alpha_i = (U|A_i x) \end{array}$$

has a constant Jacobian equal to 1 for each $U \in C$. To see this, one should note that the rows of the Jacobian matrix of f_U are the $A_i^T U$ which form an orthonormal basis of $\mathbb{R}^n$.

D. Resulting channel capacity between Alice and Bob

The channel between Alice and Bob is characterized by its signal-to-noise ratio. The capacity is achieved for a Gaussian modulation and is given by:

$$C = 1/2 \log_2(1 + \text{SNR}).$$

The reconciliation schemes presented above consist in the definition of a binary channel Q_X which results in a subcapacity for the channel. Figure 2 shows the subcapacities of the different cubes Q_X. First, if Q_X is a real n-dimensional cube (with width $2/\sqrt{n}$), then the channel defined by the reconciliation is the so-called Bi-AWGN channel. It is the best binary channel one can hope for and corresponds to a rotation in $\mathbb{R}^n$ for $n \gg 1$. The subcapacities of the "sign coding" scheme [12] and of the rotations in $\mathbb{R}^8$ are also displayed, showing the improvement brought by the method presented in this paper for a signal-to-noise ratio around 1.

IV. Application to continuous-variable QKD

Now that we have explained how efficient reconciliation of correlated Gaussian variables can be achieved with rotations in $\mathbb{R}^8$, let us look at the implications for continuous-variable QKD.

At the end of the quantum part of the continuous-variable QKD protocol [15], Alice and Bob share correlated random values and their correlation depends on the variance of the modulation of the coherent states and on the properties of the quantum channel. The channel can safely be assumed to be Gaussian since it corresponds to the case of the optimal attack for Eve [5], [6]. This means that it can be entirely characterized by its transmission and added noise and Bob's variable can be written as:

$$Y = TX + \xi$$

where T is the channel transmission and ξ is a centered Gaussian random variable. The channel transmission and the variance of ξ are accessible to Alice and Bob through an estimation step prior to the reconciliation. Once these parameters are known, one can calculate the signal-to-noise ratio of the transmission, which is the ratio between the variance of the signal (the variance of the Gaussian modulation of coherent states in our case) and the variance of the noise. The SNR quantifies the mutual information between Alice and Bob when a Gaussian modulation is sent over a Gaussian channel:

$$I(X;Y) = 1/2 \log_2(1 + \text{SNR}).$$

A typical figure of merit to evaluate the efficiency of the reconciliation protocol is the parameter β defined as the ratio between the dimension of the code used by Alice and Bob, and the mutual information between their data. In other words, β expresses the ratio between the information really extracted through the reconciliation and the information available.

Note that the efficiency of reconciliation only depends on the correlation between Alice's and Bob's data, that is on the SNR. Thus, for a given transmission and excess noise, the secret key rate is a function of the SNR, which can be optimized by changing the variance of the modulation of the coherent states.

It is not easy to know exactly how the efficiency of reconciliation depends on the SNR. However, each reconciliation technique performs better for a certain range of SNR: slice reconciliation is usually used for a SNR around 3 [16] while rotations in $\mathbb{R}^8$ are optimal for a low SNR, typically around 0.5.

Figure 3 shows the performance of rotations in $\mathbb{R}^8$ compared to slice reconciliation for the experimental parameters of the QKD system developed at Institut d'Optique. Both approaches achieve comparable reconciliation efficiencies (around 90%) but for different SNR. One can observe two distinct regimes: for low loss, i.e., short distance, slice reconciliation is better but only rotations in $\mathbb{R}^8$ allow QKD over longer distances (over 50 km with the current experimental parameters).

Concerning the complexity of the reconciliation, one should be aware that almost all the computing time is devoted to decoding the efficient binary codes, either LDPC codes or turbocodes. Compared to this decoding, the rotation in $\mathbb{R}^8$ takes a negligible amount of time. Thus, the complexity of the reconciliation presented here is comparable to the one of slice reconciliation.

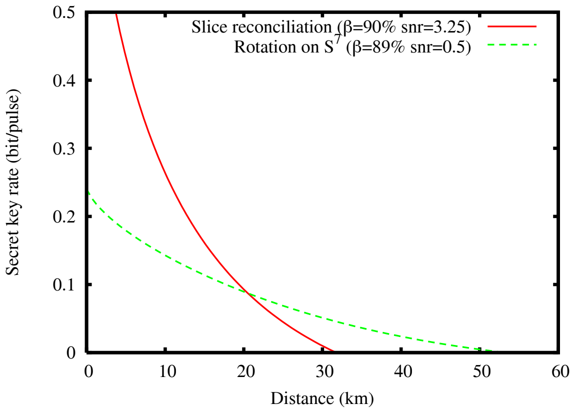

Fig. 3. Performance of slice reconciliation vs rotation in $\mathbb{R}^8$ with experimental parameters [16]. The reconciliation based on rotations in $\mathbb{R}^8$ uses a LDPC code of rate 0.26 [17]

V. Examples of families $\mathcal{A}_2$, $\mathcal{A}_4$ and $\mathcal{A}_8$

A. Notations

Let us introduce the following four 2 × 2 matrices: $K_0 = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right), K1 = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right), K_2 = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right), K3 = \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$, and the tensor product $K_{i_1,..,i_l} = K_{i_1} \otimes .. \otimes K_{i_l}$.

B. Examples

$$\mathcal{A}_2 = \{K_0, K_2\}$$
$$\mathcal{A}_4 = \{K_{00}, K_{32}, K_{20}, K_{12}\}$$
$$\mathcal{A}_8 = \{K_{000}, K_{332}, K_{320}, K_{312}, K_{200}, K_{102}, K_{123}, K_{121}\}$$

VI. Conclusion

We presented a new protocol for the reconciliation of correlated Gaussian variables. Currently, the main bottleneck of continuous-variable QKD lies in the impossibility for Alice and Bob to extract efficiently all the information available, this difficulty resulting in both a limited range and a limited rate for the key distribution. The method described in this article is particularly well suited for low signal-to-noise ratios, which is the situation encountered when one wants to perform QKD over long distances. By taking into account the current experimental parameters of the QKD link developed at the Institut d'Optique [16], one shows that this new reconciliation allows QKD over more than 50 km when previous schemes were limited to 30 km. Moreover, contrary to other protocols that have been proposed to increase the range of continuous-variable QKD, this protocol does not require any post-selection. Hence, the security proofs based on the optimality of Gaussian attacks [5], [6] remain valid, meaning that the protocol is secure against general collective attacks.

Acknowledgment

We thank Thierry Debuisschert, Eleni Diamanti, Simon Fossier, Frédéric Grosshans and Rosa Tualle-Brouri for helpful discussions. We also acknowledge the support from the European Union under the SECOQC project(IST-2002-506813) and the French Agence Nationale de la Recherche under the PROSPIQ project(No. ANR-06-NANO-041-05).

References

[1] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography", *Rev. Mod. Phys.*, vol. 74, pp. 145, 2002.

[2] C.H. Bennett, G. Brassard, C. Crepeau, and U.M. Maurer, "Generalized privacy amplification", *Information Theory, IEEE Transactions on*, vol. 41, no. 6, pp. 1915–1923, Nov 1995.

[3] J. Csiszar, I.; Korner, "Broadcast channels with confidential messages", *Information Theory, IEEE Transactions on*, vol. 24, no. 3, pp. 339–348, May 1978.

[4] Michael A. Nielsen and Issac L. Chuang, *Quantum Information and Quantum Computation*, Cambridge University Press, 2000.

[5] R. Garcia-Patron and N. J. Cerf, "Unconditional optimality of Gaussian attacks against continuous-variable quantum key distribution", *Phys. Rev. Lett.*, vol. 97, pp. 190503, 2006.

[6] M. Navascués, F. Grosshans, and A. Acín, "Optimality of Gaussian attacks in continuous-variable quantum cryptography", *Phys. Rev. Lett.*, vol. 97, pp. 190502, 2006.

[7] A. D. Wyner, "The wire-tap channel", *Bell System Technical Journal*, vol. 54, pp. 1355–1387, 1975.

[8] Gilles Van Assche, Jean Cardinal, and Nicolas J. Cerf, "Reconciliation of a Quantum-Distributed Gaussian Key", *IEEE Transactions on Information Theory*, vol. 50, no. 2, pp. 394–400, February 2004.

[9] R. Konig, U. Maurer, and R. Renner, "On the power of quantum memory", *Information Theory, IEEE Transactions on*, vol. 51, no. 7, pp. 2391–2401, 2005.

[10] Matthieu Bloch, Andrew Thangaraj, Steven W. McLaughlin, and Jean-Marc Merolla, "LDPC-based Gaussian Key Reconciliation", in *Proc. IEEE Information Theory Workshop*, Punta del Este, Uruguay, March 2006, arXiv:cs.IT/0509041.

[11] T. C. Ralph, "Continuous variable quantum cryptography", *Phys. Rev. A*, vol. 61, pp. 010303(R), 1999.

[12] C. Silberhorn, T.C. Ralph, N. Lütkenhaus, and G. Leuchs, "Continuous variable quantum cryptography: Beating the 3 db loss limit", *Phys. Rev. Lett.*, vol. 89, pp. 167901, 2002.

[13] Ryo Namiki and Takuya Hirano, "A practical limitation for continuous-variable quantum cryptography using coherent states", *Phys. Rev. Lett.*, vol. 92, pp. 117901, 2004.

[14] J.F. Adams, "Vector fields on spheres", *Annals of Math.*, vol. 75, pp. 603–632, 1962.

[15] F. Grosshans, G. Van Assche, J. Wenger, R. Brouri, N. J. Cerf, and P. Grangier, "Quantum key distribution using Gaussian-modulated coherent states", *Nature*, vol. 421, pp. 238, 2003.

[16] Jérome Lodewyck, Matthieu Bloch, Raúl García-Patrón, Simon Fossier, Evgueni Karpov, Eleni Diamanti, Thierry Debuisschert, Nicolas J. Cerf, Rosa Tualle-Brouri, Steven W. McLaughlin, and Philippe Grangier, "Quantum key distribution over 25km with an all-fiber continuous-variable system", *Phys. Rev. A*, vol. 76, pp. 042305, 2007.

[17] http://ltchwww.epfl.ch/research/ldpcopt, ".