Q-Deformed Quantum Cryptography

J. Hruby

Group of Cryptology, Union of Czech Mathematicians and Physicists, P.O.B.21 SK , 170 34 PRAHA 7, Czech Republic

Abstract. In this paper we present an application of the q-deformed quantum mechanics on quantum cryptography and possibility for a new eavesdropping strategy.

1 Introduction

Quantum cryptography (QC) [2, 12], a candidate for key transmission in such a way that nothing could intercept it, is based on the existence of quantum properties that are incompatible in the sense that measuring one property necessarily randomizes the value of the other. In recent literature [1, 5] the experimental demonstration of QC using polarized photons has been presented. The experimental demonstration of QC makes use either of two complementary properties in the sense of Heisenberg uncertainty principle like vertikal and diagonal polarizations or of the Einstein-Rosen-Podolsky correlations with two photon states and Bell's theorem. From the practical point of view and existence of local area networks using fibre optic communications the realisation of QC, using the optical fibre as quantum chanel, appears most realistic.The experimental demonstration of QC using polarized photons in optical fibre over more than 1 km was presented [8]. Generally QC could have one weakness: if foundations of quantum physics are deformed and the eavesdropper (E) works in the defined region where the quantum states approximately behave as classical. This paper presents the crucial role of the q-deformed quantum mechanics [4] and q-squeezed states [9, 11] for the eavesdropping strategies in QC. It is well known that for E it is possible to measure signal and resend an exact copy of it on a classical communication channel.The resulting quantum channel in QC is provably secure even against E with superior technology and unlimited computing power (even P = NP!) up to fundamental violation of accepted physical laws.Q-deformed quantum mechanics could be a weakness of the QC in this sense. In the case of quantum setting when the quantum mechanics is nondeformed E cannot measure principally all information from transmitted bits via quantum channel. However in the present quantum setting, it is shown in the work [1], that at least 25% of the pulses E fabricates will yield the wrong result if later successfully measured by a user B. This result is based on the definition of conjugate basis for polarized photons, from which conjugate coding [12] follows. The q-deformation of quantum mechanics, specially q-deformed version of the Bose commutation relation, can make better chance for E because in the certain region the optical states can behave approximately as the classical states [4]. For simplicity and

successful experimental demonstration [8, 10] we shall concentrate our efforts on the QC scheme using individual photons and this will be implemented in optical fibre as quantum channel. It will be done without lost of generality of theoretical conclusions for other than optical q-deformed quantum states.

2 Description of QC with single photon scheme

For demonstration of ordinary Heisenberg uncertainty relation in quantum optics and for its application on the quantum channel we shall assume an implementation of the polarimetric scheme using a fibre optic. At first we briefly describe the single photon scheme of QC key creation. The emitter A creates photons with one of the four polarizations (0^o, 45^o, 90^o, 135^o) chosen at random and transmits photons on a quantum channel to the reciever B. The reciever B chooses randomly to analyse either O^o - 90^o or 45^o - 135^o polarized photons. After the detection of a sufficient amount of photons, B sends on a public transmission link the orientations he has chosen to analyse. A then compares these data with his own polarizer orientations and publicly transmits to the B the events where both of them were using a compatible polarization.The other events are disregarded as well as no detection.The remaining events will be interpreted as 1 for O^o and 45^o and 0 for 90^o and 135^o. At that moment they can statistically verify the existence of E on the quantum channel comparing a short sample of their common data. E, who observed the data transmission,would have to choose randomly the orientation of his polarizer to detect the photon.In the case of nondeformation of quantum mechanics he has to send back the detected photons with his randomly chosen polarization orientation and it introduces 25% error which can be easily detected by the emitter and reciever after eliminating "technical wrong bits". The emitting light from the laser diod source of A can be described by the conventional boson anihilation operator a, creation operator a+ and the identity operator I, satisfying the commutation relation $[a, a+] == aa+ - a+a = I$ of the Heisenber-Weyl algebra [7]. The corresponding number operator is $N = aa+$ and has normalized eigenvectors $3 + n >$ for eigenvalues $n = 0, 1, 2....$ A coherent state $3+ >$ is defined as eigenvector of the anihilation operator a or as minimum uncertainty state

$$a\ 3+ > = < a >\ 3+ > \tag{1}$$

where $< a >=< +3a3+ >$ is the expectation value for the operator a in the state $3+ >$. Let Q and P are canonical variables, which are defined as follows

$$a = 1/|2(Q + i\,P),\ a+ = 1/|2(Q - i\,P) \tag{2}$$

and $[Q, P] = i$. If we define $/P = P- < P >$ and $/Q = Q- < Q >$, the Heisenberg's uncertainty relation can be obtained as usual:

$$1/2 = 1/23 < [Q, P] > 3 = 1/23 < [/Q,\ /P] > 3\ <\ 3 < /Q, /P > 3\ <$$

$$< < /Q2 > 1/2\ < /P2 > 1/2 \tag{3}$$

In this sense the photons behave as quantum states. The essential quantum property, a manifestation of Heisenberg's uncertainty principle, is the existence of pairs of properties that are incompatible in the sense that measuring one property necessarily randomizes the value of the other (the measuring of Q randomizes the value of P). The same is valid for polarization in QC: the measuring a single photon's polarization in one basis (for example linear) randomizes its polarization in another basis (for example circular), and vice versa. Of course it would not be valid, if the photon behaves as classical state.This effect can appear in the q-deformed quantum mechanics.

3 The uncertainty relation in q-deformed quantum mechanics

More recently q-deformed coherent states of quantum Heisenberg-Weyl have attracted a lot of attention due to their possible applications in physics and mathematical physics [11, 4]. The existence of a family of quantum mechanics - each for different value of a parameter q - was shown. We shall applied this result in QC to obtain information about eavesdropping possibilities in this q-deformed QC. Let the annihilation operator a and the creation operator $a+$ which describe a photon satisfies the q-algebra commutation relation

$$a\,a+ - q\,a+a = I, \tag{4}$$

where q is a real parameter in the range $0 < q < 1$ and I is the identity operator. Let P and Q be Hermitian operators which are written in terms of a and $a+$ as

$$P = aa + a*a+, \quad Q = aa + a*a+, \tag{5}$$

where a , a are complex parameters. Then from the q-commutation relation (4) follows

$$[P,Q] = (aa* - a*a)[I + (q-1)a+a] = R \tag{6}$$

which becomes to the ordinary commutation relation when $q = 1$ and $D = aa* - a*a = -i$. If the determinant of the transformation (5) $D = 0$, Q and P are commuting variables but in this case the transformation (5) is not invertible; it is assumed D is not equal zero. The uncertainty relation follows immediately from (6),

$$1/43 < R > 32 \; << /Q2 >< /P2 > \tag{7}$$

what is well known form for uncertainty relations for operators $PQ - QP = -iR$ i.e. $[Q,P] = iR$. All expectation values can be computed using the coherent states.The uncertainties of Q and P as well as the matrix element of their commutator have the form:

$$< /Q2 >= 3a32\,[1 + (q-1)3\%32], \tag{8}$$

$$< /P2 >= 3a32\,[1 + (q-1)3\%32], \tag{9}$$

$$< PQ > - < QP >= (aa* - a*a)\,[1 + (q-1)3\%32], \tag{10}$$

where % = ¡a¿. These uncertainty relations (8)-(10) are valid for arbitrary operators fulfilling (7) and representing conjugate properties. In QC any pair of polarization states will be refered to as a basis if they correspond to a reliably measure property of a single photon, and two bases will be said to be conjugate [12] if quantum mechanics decrees that measuring one property completely randomizes the other.But in the case of q-deformed quantum mechanics it is not necessary to be valid, because from (8)-(10) follows:

1. the uncertainty of measurements of both bases is a function of parameter % and each of these uncertainties is a constant for q=1 i.e. the case of ordinary quantum mechanics
2. since $3\%32 < (1-q) - 1$ it is seen at the boundary of the region in which the coherent state with polarization is approached, both (7) and (8) tend to zero.It means that those coherent states that correspond to parameter % near the boundary of the defined region behave - approximately - as classical states and E can obtain the full information about them and A and B can obtain no information about eavesdropping on those states
3. those coherent states lying in the vicinity of the origin (% = 0) behave as the nondeformed states because their dispersion is - approximately - constant
4. for values of % near the boundary (10) tends to zero so that operators are almost commuting
5. from uncertainties (8)-(10) two limiting processes can be considered: a) 3%32 tending to $(1-q) - 1$ for a fixed value of q, b) q approaching 1. The most important result of q-deformed QC (q is not equal 1) is that classical and quantum effects coexist and it gives the theoretical possibility for eavesdropping.The classical behaviour occurs for the values of % such that $3\%32w(1-q)-1$ and the quantum for all other values of %. The value $q = 1$ corresponds to the commutation relation of ordinary quantum mechanics and when q tends to 1, 3%32 tends to the infinity in the boundary.

4 Conclusions for the cryptanalysis of QC

For the cryptanalysis of the QC it is necessary to construct a optical quantum cryptography device based on a single photon scheme and it is possible to use the phase of the photon or its polarization. A numerical simulation of a cryptography device is not sufficient for the cryptanalysis, as it does not reflect the physical reality on which QC device is based. Nevertheless the cryptanalysis of QC is an ideal opportunity for verifying the basis principles of quantum theory and their q-deformation,thanks to the colossal statistical sets of data which are exactly processed by the mathematical tests - used for the purpose of excluding E. At first must be done the theoretical-physical and technical analysis of the optical QC device and experimental data from the point of: i) stability of measurement, false pulses and disturbances on optical system ii)the evaluation of experimental errors by statistical methods. On the ground of these analysis of experimental data the extraction of that part of the experimental results, which can be interpreted

only in the sense of the conclusions of q-deformed quantum mechanics and the determination of the magnitude q, must be done. QC appears also as a new direction of the verification of superposition principle in quantum mechanics [6] and as a good experimental world for the quantum nondemolition measurements of the photon in quantum optics [3]. The cryptanalysis from the point of these new directions on optical QC device must be also done. Limits of security of QC and new information about central ideas of quantum theory can be obtained. In such a way optical QC device is the cheapest experimental device for the verification of validity of the laws of microworld.

References

1. C. H. Bennett, F. Bessette, G. Brassard, L. Salvai and J. Smolin. *Experimental Quantum Cryptography.* J. Cryptol. 5, pp. 3-28, 1992.
2. C.H. Bennett,G. Brassard and A. Ekert. Sci. Am. , October issue, pp.26-33,1992
3. C.M. Caves, *Quantum nondemolition measurements,* in Quantum optics, Exper. Gravit. and Measur. Theor. , Ed. P. Meystre and M.O.Scully, Plenum Press 1981,p.567.
4. S. Codriansky, *Localized states in deformed quantum mechanics.* Phys. Lett A 184, pp.381-384, 1994.
5. A.K. Eckert, J.G.Rarity, P.R.Tapster and G.M.Palma. Phys.Rev.Lett.,69 (1992) 1293.
6. D.M. Greenberger , M.A. Horne and A. Zelinger , *Multiparticle interferometry and the superposition principle,* Phys. Today, August, pp.22-29,1993.
7. J.R. Klauder and E.S.G. Sudarshan, FUNDAMENTALS OF QUANTUM OPTICS, W.A. Benjamin, INC. NEW YORK AMSTERDAM (1968).
8. A. Muller, J. Brequet and N. Gisin, *Experimental demonstration of quantum cryptography using polarized photons in optical fibre over more than 1 km.* Europhys, Lett. 23,6, pp. 383-388, 1993.
9. A.I. Solomon and J. Katriel. *On q-squeezed states.* J. Phys. A: Math. Gen. 23, pp. L1209-L1212, 1990.
10. P.D. Towsend, J.G. Rarity and P.R. Tapster, Electron. Lett., 29 (1993)634.
11. Fa-Bo Wang, Le-Man Kuang. *Even and odd q-coherent states and their optical statistics properties.* J. Phys. A: Math. Gen. 26, pp. 293-300, 1993.
12. S. Wiesner, *Conjugate coding.* manuscript written circa 1970, unpublished until it appeared in Sigact News, Vol. 15, no. 1, pp. 78-88, 1983.