Coherent state quantum key distribution with multi letter phase-shift keying

Denis Sych\textsuperscript{1,2,3} and Gerd Leuchs\textsuperscript{1,2}

\textsuperscript{1} Max Planck Institut für die Physik des Lichts, Günther–Scharowsky–Strasse 1/Bau24, D-91058 Erlangen, Germany
\textsuperscript{2} Institut für Optik, Information und Photonik, Universität Erlangen–Nürnberg, Staudtstrasse 7/B2, 91058 Erlangen, Germany
E-mail: denis.sych@mpl.mpg.de

New Journal of Physics \textbf{12} (2010) 053019 (10pp)
Received 27 December 2009
Published 13 May 2010
Online at http://www.njp.org/
doi:10.1088/1367-2630/12/5/053019

Abstract. We present a protocol for quantum key distribution using discrete modulation of coherent states of light. Information is encoded in the variable phase of coherent states which can be chosen from a regular discrete set ranging from binary to continuous modulation, similar to phase-shift keying in classical communication. Information is decoded by simultaneous homodyne measurement of both quadratures and requires no active choice of basis. The protocol utilizes either direct or reverse reconciliation, both with and without postselection. We analyze the security of the protocol and show how to enhance it by the optimal choice of all variable parameters of the quantum signal.

Contents

1. Introduction \hspace{1cm} 2
2. Description of the protocol \hspace{1cm} 3
3. Security analysis \hspace{1cm} 3
3.1. Information between Alice and Bob \hspace{1cm} 4
3.2. Eve’s information \hspace{1cm} 5
3.3. Postselection \hspace{1cm} 7
4. Results \hspace{1cm} 8
5. Conclusions \hspace{1cm} 9
Acknowledgments \hspace{1cm} 10
References \hspace{1cm} 10

\textsuperscript{3} Author to whom any correspondence should be addressed.
1. Introduction

Quantum key distribution (QKD) is a procedure of information exchange between two parties, the sender Alice and the receiver Bob, which allows one to distribute absolutely secure data between them (Dušek et al. 2006, Gisin et al. 2002, Scarani et al. 2009). The distinctive part of QKD with respect to classical communication is the use of a quantum information channel, where the signal is protected from unauthorized duplication Bennett and Brassard 1984, Dieks 1982, Ekert 1991, Wooters and Zurek 1982). Mathematically, the information signal can be described by discrete variables (DV) or by continuous variables (CV) (Cerf et al. 2007), although physically the signal can be of various kinds: single photons (Bennett and Brassard 1984), weak coherent pulses (Bennett 1992), squeezed states (Hillery 2000, Ralph 1999) and other systems where a signal possesses essentially quantum properties.

A universal characteristic that can be compared for different QKD protocols (apart from their experimental realizations) is the secret key generation rate (shortly, key rate)—i.e. the average amount of secure information per elementary transmission (e.g. per light pulse). In order to transmit higher total amount of secure data, one can increase the pulse repetition rate or increase the key rate. The first way is limited mainly by experimental techniques, whereas the second one is defined by mathematical properties of the given QKD protocol.

In the case of DV QKD, it has been shown that extensions of the standard four-letter BB84 protocol (Bennett and Brassard 1984) to higher number of letters in the alphabet can improve performance in terms of higher critical error rate or longer communication lines (Bechmann-Pasquinucci and Gisin 1999, Bruß 1998, Sych et al. 2004, 2005).

In the case of CV QKD, the first protocols were based on Gaussian alphabets consisting of either coherent or squeezed states. The common weak point of these protocols is high sensitivity to losses in the quantum communication channel, which initially was believed to lead to the so-called ‘3 dB loss limit’: the key rate is equal to zero when channel losses are higher than 50%. After the invention of postselection (Silberhorn et al. 2002) and reverse reconciliation (Grosshans et al. 2003) this limit was overcome, and the key rate was substantially improved. The further enhancement can be done with help of two-way communication (Pirandola et al. 2008). Another interesting option for improving characteristics of QKD is to consider discrete alphabets (Heid and Lütkenhaus 2006, Namiki and Hirano 2003) instead of Gaussian ones. Protocols with Gaussian alphabets have an advantage of simpler security analysis, whereas the protocols based on discrete modulation are easier to realize in practice.

In this work, we address the question how one can further increase the key rate of CV QKD with discrete modulation by varying the geometry of the quantum alphabet. Having in mind the idea of improving the properties of DV QKD by use of more symmetric alphabets with higher number of letters (Sych et al. 2005), we present a new CV QKD protocol which generalizes previous ones with discrete modulation (Heid and Lütkenhaus 2006, Lorenz et al. 2004, Namiki and Hirano 2003). Namely, the protocol employs an alphabet with \( N \) coherent states \(|\alpha_k\rangle = |a e^{i(2\pi/N)k}\rangle\) which have relative phases \((2\pi/N)k\) and a fixed amplitude \(a\). In classical communication, this type of encoding is known as phase-shift keying (PSK). We perform a security analysis of the proposed protocol for lossy but noiseless quantum channels, providing full optimization of all parameters of the protocol, and show how the number of letters affect the key rate.
2. Description of the protocol

An elementary information transmission in the multi-letter PSK protocol is as follows:

- The sender (Alice) chooses a random equiprobable number \( k = 1 \ldots N \) and sends the respective coherent state \( |\alpha_k\rangle = |\alpha e^{i(2\pi/N)k}\rangle \).
- The receiver (Bob) measures the state by splitting the signal at a 50/50 beam splitter and measuring two conjugate quadratures \( \hat{x} \) and \( \hat{p} \) at the output ports by homodyning each signal—such a scheme is called heterodyne measurement (Lorenz et al 2004, Weedbrook et al 2004), where the two conjugate measurements can be separated in time or space. The results of the measurements are \( \beta_x \) and \( \beta_p \), which we write as a pure coherent state \( |\beta\rangle = |\beta_x + i\beta_p\rangle \).
- Bob assigns a classical number \( l \) to the measured state \( |\beta\rangle \) by finding a state \( |\alpha_l\rangle \) which is the closest alphabet’s state to the state \( |\beta\rangle \): \( |\langle \alpha_l|\beta\rangle|^2 = \max_n |\langle \alpha_n|\beta\rangle|^2 \). Generally speaking, this classical value \( l \) decoded by Bob can be different from the initial value \( k \) sent by Alice because of intrinsic quantum uncertainty even in the absence of eavesdropping or any channel noise.

The elementary information transmission from Alice to Bob can be schematically shown as a ‘\( k \rightarrow l \)’ channel:

\[
\begin{align*}
  k & \quad \text{encoding} \quad |\alpha_k\rangle \quad \text{measurement} \quad |\beta\rangle \quad \text{decoding} \quad l.
\end{align*}
\]

As long as the considered quantum alphabet has a regular \( 2\pi/N \) phase-shift symmetry, and all states have an equal probability to be sent, all channel inputs and outputs (1) are equiprobable. We note that there is no active choice of measurement basis in our protocol, therefore there is no basis reconciliation needed. All transmissions contribute to the total secure key, and nothing is discarded unlike in previous protocols with discrete modulation and homodyne detection (Namiki and Hirano 2006).

After the measurement, Bob can (but not necessarily has to) use the postselection idea (Silberhorn et al 2002), when he decides whether to keep the transmission depending on the value \( \beta \). The elementary transmission (1), possibly followed by postselection, is repeated until Alice and Bob collect enough data to perform classical error correction and privacy amplification procedures (Gisin et al 2002). The resulting data are a secret key.

The amplitude \( a \) and the number of letters \( N \) can be flexibly adjusted for a given information channel. The exact optimization for a given channel transmittance will be discussed later. These parameters are supposed to be publicly known, particularly by the potential eavesdropper. We note that the number of states can be arbitrary large. In the limit of infinity \( N \rightarrow \infty \), we have a continuous phase modulation. Thus our protocol can be viewed as a smooth transition between discrete (Heid and Lütkenhaus 2006, Lorenz et al 2004, Namiki and Hirano 2003) and continuous (Grosshans and Grangier 2002, Silberhorn et al 2002, Weedbrook et al 2004) modulation of CV.

3. Security analysis

We investigate the security of our protocol assuming there is no excess noise in the quantum channel. In this case the best possible attack is the beam splitting attack (Heid and Lütkenhaus 2006). We allow Eve to have unlimited access to all the losses, as she could replace the real lossy information channel with an ideal lossless one.
The beam splitting transformation is $|\alpha_k\rangle_A \rightarrow |\beta_k\rangle_B \otimes |\epsilon_k\rangle_E$, where Alice’s initial state $|\alpha_k\rangle$ is split to Bob’s state $|\beta_k\rangle$ and Eve’s state $|\epsilon_k\rangle$:

$$|\beta_k\rangle = |\sqrt{\eta}\alpha_k\rangle, \quad |\epsilon_k\rangle = |\sqrt{1-\eta}\alpha_k\rangle$$

(2)

and $\eta$ is the channel transmittance.

In this beam splitting scenario, Eve does not introduce any excess noise on Bob’s side, whereas in any other better eavesdropping strategy Eve necessarily does. For example, if Eve would make an intercept-resend attack, then she adds at least one unit of shot noise. Afterwards, she can attenuate the signal, and the excess noise will be proportionally reduced. As a remark on the side, we see in this way, that the maximum tolerable excess noise cannot exceed that of the intercept-resend strategy, i.e. cannot be higher than channel transmittance $\eta$.

In real communication lines, such as optical fibers or free space, excess noise (typically, about 1% of shot noise (Elser et al 2009, Lorenz et al 2004, 2006)) is introduced mainly by imperfections of the experimental setup, and there is almost no measurable excess noise due to the channel itself. If the absence of channel excess noise is experimentally verified, then the eavesdropping strategy based on beam splitting is the best possible attack, at least for the values of the channel transmittance $\eta \gg 0.01$.

3.1. Information between Alice and Bob

The amount of classical mutual Shannon information $I_{AB}$ transmitted from Alice to Bob via the channel (1) is equal to the difference of $a$ priori (before measurement) and $a$ posteriori (after measurement) entropies (Shannon 1948). Before any measurement, all channel outcomes are equiprobable for Bob, so his $a$ priori entropy $H_{Bob}^{prior}$ is the unconditional ‘pure guess’ entropy equal to $\log_2 N$ bit per transmission.

The conditional probability density to measure the state $|\beta\rangle$ when a state $|\alpha_k\rangle$ has been sent is $p(\beta|k) \sim |\langle\beta|\beta\rangle|^2 \sim e^{-|\beta-\beta_k|^2}$. The total unconditional probability density to measure a state $|\beta\rangle$ is $p(\beta) = (1/N) \sum_{k=1}^N p(\beta|k)$. Its normalization $\int p(\beta) \, d\beta = 1$ also yields the normalization of $p(\beta|k) = (1/\pi) e^{-|\beta-\beta_k|^2}$.

After the measurement of $|\beta\rangle$, the probability $p_l(\beta)$ that the state $|\alpha_k\rangle$ was initially sent is

$$p_l(\beta) = \frac{p(\beta|l)}{N p(\beta)} = \frac{1}{\pi N p(\beta)} e^{-|\beta-\beta_l|^2}.$$

(3)

As we discussed above, the measured state $|\beta\rangle$ is decoded by Bob to a classical value $l$ such that the state $|\alpha_l\rangle$ is the closest alphabet’s state to the measured state $|\beta\rangle$. Corresponding regions in the phase space are shown by different shades of grey in figure 1. In the case when $l = k$ the value (3) is the probability of decoding the correct result, otherwise (3) is the error probability of decoding a wrong result $l \neq k$.

Bob’s $a$ posteriori entropy $H_{Bob}^{post}$ is the Shannon entropy of the total probability distribution $P(\beta) = \{p_1(\beta), p_2(\beta), \ldots, p_N(\beta)\}$ conditioned on the measured state $|\beta\rangle$:

$$H_{Bob}^{post}[P(\beta)] = - \sum_{k=1}^N p_k(\beta) \log_2 p_k(\beta).$$

(4)

Finally, the amount of classical information transmitted from Alice to Bob via the channel (1):

$$I_{AB} = \int p(\beta) I_{AB}(\beta) \, d\beta,$$

(5)

where $I_{AB}(\beta) = \log_2 N + \sum_{k=1}^N p_k(\beta) \log_2 p_k(\beta)$.

New Journal of Physics 12 (2010) 053019 (http://www.njp.org/)
Figure 1. Reconciliation and postselection areas for the five-letter protocol. Different shades of grey correspond to the regions in the phase space where measurement results $|\beta\rangle$ are associated with a given letter. Letters are shown as black circles. Dashed lines show the borders of the postselection areas for a case when amplitude is $a = 1.4$, and transmittance varies from $0.95$ (the smallest area) to $0.4$ (the biggest area) with a step $0.05$.

3.2. Eve’s information

As we have mentioned above (1), the classical data decoded by Bob can differ from the initially encoded by Alice. Thus they have to perform certain error correction procedures (Dušek et al 2006, Gisin et al 2002, Scarani et al 2009). To calculate Eve’s potential information, we should take into account a particular type of classical communication between Alice and Bob during the error correction. We consider two cases of one-way classical communication: direct reconciliation and reverse reconciliation.

In the first strategy, Bob tries to guess the values encoded by Alice, with help of certain additional classical information (e.g. parity bits) which Alice should sent to Bob. Direction of classical information flow is the same as in the quantum part of the protocol, hence the name ‘direct reconciliation’. In the second strategy, Alice tries to guess the values decoded by Bob, and Bob should send additional information to Alice, so classical communication goes in the opposite direction with respect to the quantum part, hence the name ‘reverse reconciliation’.

After the error correction, Alice and Bob have the same raw of data on both sides. With respect to the uncorrected data, Alice and Bob have less bits, but each bit contains higher amount of information. The same applies to Eve: in both direct and reverse reconciliation, we assume Eve can have full access to the error correction information and she tries to correct her bits as well, either with information from Alice or from Bob. In order to have an information advantage over Eve, the information shared between Alice and Bob has to be higher than the information Eve can obtain about Alice’s states (in the case of direct reconciliation) or about Bob’s states (in the case of reverse reconciliation).

We also assume that after the beam splitting Eve can keep her individual signals $|\epsilon_k\rangle$ in a quantum memory as long as she wants, particularly till the end of the error correction step, and perform the best possible measurement after she obtains information from the classical
communication part of the protocol. In other words, Eve is not restricted to any practical way of information extraction from the states $|\psi_k\rangle$, but she is doing noiseless beam slitting to acquire her states. Under these assumptions, her potential knowledge is bounded by the Holevo information (Devetak and Winter 2005, Holevo 1973, Scarani et al 2009).

In the general case, the Holevo information $\chi$ sets the upper bound on the information which can be transmitted by a state randomly chosen from a set of $N$ states $\hat{\rho}_k$ with a respective probability $p_k$:

$$\chi = S \left( \sum_{k=1}^{N} p_k \hat{\rho}_k \right) - \sum_{k=1}^{N} p_k S(\hat{\rho}_k),$$

where $S(\hat{\rho})$ is the von Neumann entropy $S(\hat{\rho}) = -\text{Tr} \hat{\rho} \log_2 \hat{\rho}$.

3.2.1. Direct reconciliation. In the direct reconciliation case, Eve has a state (2) conditioned only on Alice’s sent state $|\alpha_k\rangle$. Eve’s conditional state is pure, thus her information is equal to the von Neumann entropy $I_{AE} = S(\hat{\rho}_E)$ of her unconditional state $\hat{\rho}_E = (1/N) \sum_{k=1}^{N} |\epsilon_k\rangle \langle \epsilon_k|$. To calculate $S(\hat{\rho}_E)$ we need to find the eigenvalues of $\hat{\rho}_E$. The rotational symmetry of the phase-shift alphabet allows us to write Eve’s conditional states in an orthogonal basis $\{ |m\rangle \}$ as (Chefles and Barnett 1998)

$$|\epsilon_k\rangle = \sum_{m=1}^{N} c_m e^{i(2\pi/N)km} |m\rangle. \quad (7)$$

In the basis $\{ |m\rangle \}$ Eve’s unconditional state takes the diagonal form

$$\hat{\rho}_E = \frac{1}{N} \sum_{k=1}^{N} |\epsilon_k\rangle \langle \epsilon_k| = \sum_{m=1}^{N} |c_m|^2 |m\rangle \langle m|, \quad (8)$$

so Eve’s information is equal to $I_{AE} = S(\hat{\rho}_E) = H[C]$, where $H[C]$ is the Shannon entropy (4) of the probability distribution $C = \{|c_1|^2, |c_2|^2, \ldots, |c_N|^2\}$.

The coefficients $|c_m|^2$ are derived from a system of $N$ linear equations enumerated by an index $k = 1, \ldots, N$:

$$\sum_{m=1}^{N} e^{i(2\pi/N)km} |c_m|^2 = \langle \epsilon_N | \epsilon_k \rangle. \quad (9)$$

It has a formal analytical solution

$$|c_m|^2 = \frac{1}{N} \sum_{n=1}^{N} e^{-i(2\pi/N)m-n-a^2(1-a)(1-e^{i2\pi/N})}, \quad (10)$$

where the coefficients $c_m$ depend on the signal amplitude $a$ and the channel transmittance $\eta$.

3.2.2. Reverse reconciliation. In the case of reverse reconciliation Eve has a state (2) conditioned on Bob’s measured state $|\beta\rangle$. After classical communication Eve can possibly find out the average amount of information (5) between Alice and Bob in each transmission, so we assume this value is publicly open. To simplify the security analysis, we also assume that Bob
announces the amplitude of the measured state, so Eve knows the measured state $|\beta\rangle$ up to a cyclic phase shift $2\pi/N$. We denote these possible states as $|\beta^{(l)}\rangle$. On her side, Eve has to distinguish between the states $\hat{\rho}^{(l)}_E = \sum_k p_k(\beta^{(l)})|\epsilon_k\rangle\langle\epsilon_k|.

After averaging, Eve’s state is $(1/N)\sum\hat{\rho}^{(l)}_E = \hat{\rho}_E$, so the left entropy term in (6) is the same as we calculated before for the case of direct reconciliation. Due to the $2\pi/N$ phase-shift symmetry of the alphabet, the averaging in the right entropy term in (6) is just equal to the entropy of any of the states $\hat{\rho}^{(l)}_E$, let it be the first one $\hat{\rho}^{(1)}_E$.

Again, we can rewrite Eve’s states $|\epsilon_k\rangle$ in the orthogonal basis (7). Unfortunately, the state $\hat{\rho}^{(1)}_E$ in this basis takes a non-diagonal form $\hat{\rho}^{(1)}_E = \sum_{k,m,n} (p_k(\beta^{(1)})c_m\epsilon_n^*e^{i(2\pi/N)k(m-n)}|m\rangle\langle n|).$ We analytically calculate eigenvalues of this state for a given $N$, but the result is too large to be presented here. Finally, Eve’s information is $I_{BE}(\beta) = S[\hat{\rho}_E] - S[\hat{\rho}^{(1)}_E]$.

3.3. Postselection

The key rate $G$, i.e. the amount of secret information per transmission (1), is equal to the difference between Bob’s and Eve’s information (Devetak and Winter 2005, Renner 2007):

$$G = \int p(\beta)G(\beta) \, d\beta, \quad G(\beta) = I_{AB} - I_{AE, BE}, \quad (11)$$

where $I_{AE}$ and $I_{BE}$ refer to direct and reverse reconciliation, respectively.

In the case of direct reconciliation, Eve has to guess what was sent by Alice. If the channel transmittance is lower than 50%, Eve can potentially have a better signal than Bob, thus Eve’s information can be higher than Bob’s information and no secure communication is possible. To overcome this ‘3 dB limit’ we use the postselection idea (Silberhorn et al 2002), so that Bob has an information advantage over Eve ($I_{AB} > I_{AE}$), i.e. we select only that part of transmissions which give us positive terms $G(\beta)$.

The postselection procedure in the direct reconciliation scenario can be qualitatively described as follows: Eve’s information $I_{AE}$ does not depend on Bob’s measured state $\beta$, so the key rate can be increased if Bob accepts only those transmissions where $\beta$ is such that he has higher information than Eve ($I_{AB}(\beta) > I_{AE}$). Instead of integration over the whole phase space (11) we have integration over the postselected area (PSA):

$$G_{PS} = \int_{PSA} p(\beta) (I_{AB}(\beta) - I_{AE}) \, d\beta. \quad (12)$$

To find this PSA we numerically solve an equation $I_{AB}(\beta) > I_{AE}$. As an example in figure 1 we show the borders of the PSA for five letter protocol as the dashed lines. Different dashed lines correspond to different values of transmittance $\eta = 0.4, 0.45, 0.5, \ldots, 0.95$, and the amplitude is fixed $a = 1.4$. The PSA is the phase space except the central region bounded by a dashed line. If the measured state $|\beta\rangle$ lies inside the region the transmission should be omitted, otherwise it is accepted. The higher the transmittance, the smaller the omitted region, the bigger the PSA and the higher the key rate (12).

To find the key rate $G_{PS}$ as a function of transmittance $\eta$, we optimize the amplitude $a$ such as to maximize the key rate $G_{PS}(\eta) = \max_a G_{PS}(\eta, a)$.

In the case of reverse reconciliation, Eve has to guess Bob’s measurement result, thus her information cannot be higher than Bob’s information: $I_{AB} \geq I_{BE}$. Therefore, $G(\beta)$ is always nonnegative, and the postselection procedure does not have to be applied.

New Journal of Physics 12 (2010) 053019 (http://www.njp.org/)
4. Results

The calculated secret key rate $G_{\text{PS}}(\eta)$ and the optimal amplitude $a_0(\eta)$ for several alphabets are shown in figure 2. We can see, that for the channel transmittance $\eta < 0.9$ all the curves of the key rate are almost the same when the number of letters is more than 4.

In the case of reverse reconciliation, we have an interesting result: the higher the number of letters, the higher the key rate. We do not have an analytical expression for the $\infty$-letter alphabet, but its approximation by a high number of letter confirms that this is the best choice for all values of $\eta$. The key rate is higher than for the two-letter alphabet of almost an order of magnitude.

Discontinuity of the curve $a_0(\eta)$ for the five-letter alphabet is not a mistake. Due to the fact that the function $G(a)$ at a fixed value $\eta$ can have two slightly different global maxima, the exact optimization for variable $\eta$ may cause a ‘jump’ from one maximum to another.
Table 1. Values of transmittance $\eta$, where a curve $G_{PS}(N, \eta)$ intersects with a curve $G_{PS}(N + 1, \eta)$.

| $N$ | 2   | 3   | 4   | 5   | 6   | 7   | 8   |
|-----|-----|-----|-----|-----|-----|-----|-----|
| $\eta$ | 0.493 | 0.705 | 0.797 | 0.797 | 0.753 | 0.725 | 0.696 |

In the case of direct reconciliation, we can see that lines $G(\eta)$ for various numbers of letters are intersecting in different points, which are presented in Table 1. This means that for different values of transmittance $\eta$ there are different optimal numbers of letters. The higher the transmittance, the higher the optimal number of states.

Again, we do not have an analytical expression for the curve $G(N = \infty, \eta)$, but we found that left side of the curves quickly saturates (there is no essential difference between $G(N = 5, \eta)$ and $G(N = 64, \eta)$ for $\eta < 0.9$). So we can conjecture that the optimal alphabets can consist of 2, 3, 4 or $\infty$ letters. A curve $G(N = \infty, \eta)$ intersects with $G(N = 4, \eta)$ at the value $\eta \simeq 0.795$, so the most significant advantage of the multi-letter protocol over the two-letter protocol one can get in the case of high transmittance. The intuitive explanation is as follows:

In the case of high losses, Eve has a stronger signal than Bob. Thus the amplitude of the signal $a_0$ must be small, and Bob relies basically on the postselection. In postselection, it is harder for Bob to distinguish between many letters than between two. Thus with an increasing number of letters his information essentially decreases. In this case the alphabet with two letters outperforms the multi-letter alphabet.

In the opposite case of low losses Eve has a weaker signal, and Alice can increase the amplitude of the signal and number of letters. With higher amplitude of the signal Bob can better distinguish between many letters and increase his information. In the limit $\eta \to 1$ Alice can use signals with high amplitude and Bob can get almost $\log_2 N$ bit per transmission. Therefore, the more letters in the alphabet are, the higher Bob’s information is. In principle, one can use an arbitrary high number of letters, and in the limit $N \to \infty$ (continuous phase modulation) Bob’s information seems to be infinite. However, there are limiting factors from both experimental and theoretical viewpoints. Firstly, one can see in figure 2 the curves $G(\eta)$ and $a_0(\eta)$ start to essentially increase from the values $\eta > 0.99$. In any real experimental setup there are imperfections (inaccuracy, losses, etc), so the case $\eta > 0.99$ can hardly be achieved. Secondly, any real signal has certain energy limit, which sets maximum amplitude. Also taking into account excess noise in the channel might somewhat change the situation.

5. Conclusions

To summarize, we have presented a new CV QKD protocol with coherent states. The protocol employs multi-letter PSK and heterodyne measurement. Security analysis of the proposed protocol is performed for the case of lossy but noiseless quantum channels. We have shown that for each given channel transmittance, one can find a certain optimal number of letters (2, 3, 4 or $\infty$), optimal amplitude of the signal (typically, 1–4 photons per pulse), and optimal postselection threshold, which increase the secret key rate about one order of magnitude comparing to the protocol with binary modulation.

New Journal of Physics 12 (2010) 053019 (http://www.njp.org/)
Acknowledgments

The authors thank Norbert Lütkenhaus for helpful discussions, and Dominique Elser and Christoffer Wittmann for valuable comments on the manuscript. DS acknowledges the Alexander von Humboldt Foundation for a fellowship.

References

Bechmann-Pasquinucci H and Gisin N 1999 Phys. Rev. A 59 4238–48
Bennett C H 1992 Phys. Rev. Lett. 68 3121–4
Bennett C H and Brassard G 1984 Proc. IEEE Int. Conf. on Computers, Systems ad Signal Processing (New York: IEEE) p 175
Brüll D 1998 Phys. Rev. Lett. 81 3018–21
Cerf N J, Leuchs G and Polzik E 2007 Quantum Information with Continuous Variables of Atoms and Light (London: Imperial College Press)
Chefles A and Barnett S M 1998 Phys. Lett. A 250 223–9
Devetak I and Winter A 2005 Proc. R. Soc. A 461 207
Dieks D 1982 Phys. Lett. A 92 271
Dušek M, Lütkenhaus N and Hendrych M 2006 Prog. Opt. 49 381–454
Ekert A K 1991 Phys. Rev. Lett. 67 661–3
Elser D, Bartley T, Heim B, Wittmann C, Sych D and Leuchs G 2009 New J. Phys. 11 045014
Gisin N, Ribordy G, Tittel W and Zbinden H 2002 Rev. Mod. Phys. 74 145
Grosshans F, Assche G V, Wenger J, Brouni R, Cerf N J and Grangier P 2003 Nature 421 238
Grosshans F and Grangier P 2002 Phys. Rev. Lett. 88 057902
Heid M and Lütkenhaus N 2006 Phys. Rev. A 73 052316
Hillery M 2000 Phys. Rev. A 61 022309
Holevo A 1973 Probl. Inf. Trans. 9 177
Lorenz S, Korolkova N and Leuchs G 2004 Appl. Phys. B 79 273
Lorenz S, Rigas J, Heid M, Andersen U L, Lütkenhaus N and Leuchs G 2006 Phys. Rev. A 74 042326
Namiki R and Hirano T 2003 Phys. Rev. A 67 022308
Namiki R and Hirano T 2006 Phys. Rev. A 74 032302
Pirandola S, Mancini S, Lloyd S and Braunstein S L 2008 Nat. Phys. 4 726–30
Ralph T C 1999 Phys. Rev. A 61 010303
Renner R 2007 Nat. Phys. 3 645–9
Scarani V, Bechmann-Pasquinucci H, Cerf N J, Dušek M, Lütkenhaus N and Peev M 2009 Rev. Mod. Phys. 81 1301
Shannon C 1948 Bell Syst. Tech. J. 27 379
Silberhorn C, Ralph T C, Lütkenhaus N and Leuchs G 2002 Phys. Rev. Lett. 89 167901
Sych D V, Grishanin B A and Zadkov V N 2004 Phys. Rev. A 70 052331
Sych D V, Grishanin B A and Zadkov V N 2005 Quant. Electron. 35 80
Weedbrook C, Lance A M, Bowen W P, Symul T, Ralph T C and Lam P K 2004 Phys. Rev. Lett. 93 170504
Wooters W K and Zurek W H 1982 Nature 299 802

New Journal of Physics 12 (2010) 053019 (http://www.njp.org/)