SCIENTIFIC REPORTS
natureresearch

OPEN

Subcarrier wave continuous variable quantum key distribution with discrete modulation: mathematical model and finite-key analysis

E. Samsonov[1,2]✉, R. Goncharov[1], A. Gaidash[1,2], A. Kozubov[1,2], V. Egorov[1,2] & A. Gleim[1]

In this paper we report a continuous-variable quantum key distribution protocol using multimode coherent states generated on subcarrier frequencies of the optical spectrum. We propose a coherent detection scheme where power from a carrier wave is used as a local oscillator. We compose a mathematical model of the proposed scheme and perform its security analysis in the finite-size regime using fully quantum asymptotic equipartition property technique. We calculate a lower bound on the secret key rate for the system under the assumption that the quantum channel noise is negligible compared to detector dark counts, and an eavesdropper is restricted to collective attacks. Our calculation shows that the current realistic system implementation would allow distributing secret keys over channels with losses up to 9 dB.

Quantum key distribution (QKD) is a method of sharing symmetric cryptographic keys between two parties that is based on encoding information in the states of quantum objects and subsequent distillation of the key through a classic communication channel. The first quantum cryptography protocols exploited the quantum system with degrees of freedoms[1–3]. A numerous amount of different techniques for security proofs for discrete variable QKD systems has already been presented[4–13]. Experimental implementations of this family of QKD protocols rely on single-photon detectors for quantum state measurements.

In turn, continuous-variable QKD (CV-QKD), which was proposed later, relies on methods of coherent detection, homodyne or heterodyne, for gaining information about the quantum states. In other words, single-photon detection is replaced by conventional optical communication methods. However, security proofs for CV-QKD protocols currently remain less advanced[14,15].

There are two types of CV protocols that differ by signal modulation method: Gaussian[16,17], where the complex amplitudes of coherent states are selected randomly from a normal distribution, and discrete modulation (DM)[18–22] with weak coherent phase-coded states. Other CV-QKD protocols are based on two-mode squeezed vacuum states transmission and measurement via homodyne or heterodyne detection[23]. Security proofs for Gaussian CV-QKD protocols remain the most developed: they were presented against general attacks in the finite key regime using several different approaches[24]. Security analysis for CV-QKD protocol with two-mode squeezed vacuum states was also performed[25,26]. Discrete-variable CV-QKD protocols possess several important advantages; among those are relative implementation simplicity and a possibility to minimize the number of parameters that need to be monitored. Nevertheless, security proofs for discrete-modulation CV-QKD systems require special consideration. In the asymptotic limit, its security has been proven against collective attacks[27]. Recently it was shown that security proof for CV-QKD with discrete modulation against general attacks is possible[27].

Here we propose an implementation of CV-QKD protocol based on subcarrier wave (SCW) technique[28–36]. A defining property of subcarrier wave DV-QKD is the method for quantum state encoding. In it, a strong monochromatic wave emitted by a laser is modulated in an electro-optical phase modulator to produce weak sidebands, whose phase with respect to the strong (carrier) wave encodes quantum information (for more details, see[30]). Like in any other DV-QKD systems, in SCW QKD the weak radiation component is detected by a single photon

[1]ITMO University, Kronverkskiy, 49, Saint Petersburg, 197101, Russia. [2]Quanttelecom LLC., Saint Petersburg, 199178, 6 Line 59, Russia. ✉e-mail: eosamsonov@itmo.ru

counter, and the measured observable has a discrete spectrum. In SCW CV-QKD protocol described in this work, Alice prepares coherent multimode states, which can be defined as quadratures of the bosonic field, while Bob performs coherent detection to establish correlations with Alice.

We propose a new coherent detection scheme for SCW QKD system, the main advantage of which is using the carrier wave (an essential part of SCW methodology) as a local oscillator. In practice, it solves the well-known problem of transmitting the local oscillator through the quantum channel (or its generation on receiver's side). This is a novel approach that has not been discussed in previous works dedicated to studying multimode CV QKD[37–39].

From telecommunication point of view, SCW approach possesses several additional advantages. Firstly, it is intrinsically robust against external conditions affecting the fiber and is ready to function in conventional telecom infrastructure. Secondly, it demonstrates unmatched spectral efficiency in the quantum channel, allowing for distributing several keys on separate closely-packed sidebands around a single optical carrier[29]. Thirdly, recent experiments[40] have shown that preservation of SCW quantum signal parameters in respect to the carrier allows transmitting phase-encoded quantum signals through the air providing invariance to telescope rotation that remains an important obstacle in traditional polarization-based free-space quantum communication, making the same QKD kit suitable for fiber and free-space QKD networks. Security proof of SCW QKD protocol with discrete variables against collective beam-splitting attack was proposed in[36], and more recently general finite-key security proof was presented in[41].

A major difference of SCW approach from the previous CV-QKD protocols is using multimode coherent states generated on subcarrier frequencies. It therefore requires special consideration of security proof technique for the CV-QKD protocol. The most advanced security descriptions for typical CV-QKD protocols with Gaussian and discrete modulation assume that the quantum channel has losses and imposes Gaussian noise on the observed quadrature distributions. For CV-QKD this usually requires estimating a covariance matrix of the bipartite state shared by Alice and Bob[24]. In Gaussian modulation protocols the variances and covariances directly measured by Alice and Bob give a covariance matrix. In case of DM protocols it is harder to obtain, but in[27] a major step towards the full security proof of DM CV-QKD has been presented. The lower bound against collective attacks is calculated by solving a semidefinite program that computes the covariance matrix of the state shared by Alice and Bob in the entanglement-based version of the protocol. Our aim in this work is to demonstrate universality of CV-QKD protocol based on SCW technique. Hence we build a mathematical model of CV-QKD protocol based on SCW method and show the possibility of performing security proof analysis in case of multimode coherent states. Unconditional security proof is out of scope of this paper and will be a subject for a separate study. Here we perform finite-key security analysis using fully quantum asymptotic equipartition property technique[8] and calculate the lower bound on secret key rate under the assumption that detector dark counts remain a dominant contribution to the total noise level[20]. The key rates are obtained for direct reconciliation scheme with post-selection in case of collective attacks.

Results

Subcarrier wave CV-QKD setup. In SCW method the signal photons are not emitted directly by a laser source but are generated on subcarrier frequencies, or sidebands, in course of phase modulation of an intense optical carrier. Laser source emits coherent light with frequency ω. Alice modulates this beam in a traveling wave electro-optical phase modulator with the microwave field with frequency Ω and phase φ_A[42]. As a result, pairs of sidebands are formed at frequencies $\omega_k = \omega + k\Omega$, where integer k runs between the limits: $-S \leq k \leq S$. Modulation index at Alice side is chosen so that the total number of photons in the sidebands is less than unity (according to the QKD protocol). In the proposed SCW CV-QKD setup shown in Fig. 1 Alice sends weak coherent states along with the carrier through a quantum channel. Alice prepares her states using quadrature phase-shift modulation by choosing from a finite set of states $\varphi_A \in \{0, \pi/2, \pi, 3\pi/2\}$. Receiver (Bob) applies much higher modulation index than Alice on his modulator and randomly selects x or P measurement introducing phase shift $\varphi_B \in \{0, \pi/2\}$, respectively, in each transmission window T. Here we consider CV-QKD protocol with discrete modulation, so we formally leave Alice's block the same as in initial DV-QKD system[30], but completely change the detection scheme.

Figure 2 describes the operation of proposed coherent detection scheme in detail. We avoid mentioning the words "homodyne" and "heterodyne" purposely because this paper does not consider a classical scheme, but its analog, corresponding to the more general definition of "coherent detection". By definition, homodyne detection is characterized by interference of a weak signal with a powerful local oscillator on a 50/50 beam splitter. After interference, the number of photons at the detectors n_1 and n_2 depends on phase difference $\Delta = \phi_A - \phi_B$. Then, the difference in photo-electrons n_e can be determined by signal subtraction through the measuring of current. Coherent detection scheme employed in this work is similar to homodyne detection. Homodyning in SCW-CV is carried out directly in the phase modulator in the Bob module (instead o a 50/50 beam splitter) for each of the sidebands independently. After the second modulation interference is observed at frequencies $\omega_k = \omega + k\Omega$ if equal microwave field frequencies Ω are used by Alice and Bob. Resulting carrier and subcarriers wave power depends on phase difference between φ_A and φ_B. In case of constructive (Fig. 2a) or destructive (Fig. 2b) interference, subcarriers wave power becomes either more or less than the carrier wave power, respectively. A narrow spectral filter then separates the carrier from the sidebands. Finally the two output modes (carrier and all the sidebands) are detected by two different photodiodes, and their photo currents are subtracted. Thus, one can extract information encoded in the the phase of the oscillating signal. Similar to traditional homodyne detection in QKD, Bob measures only one quadrature component at a time.

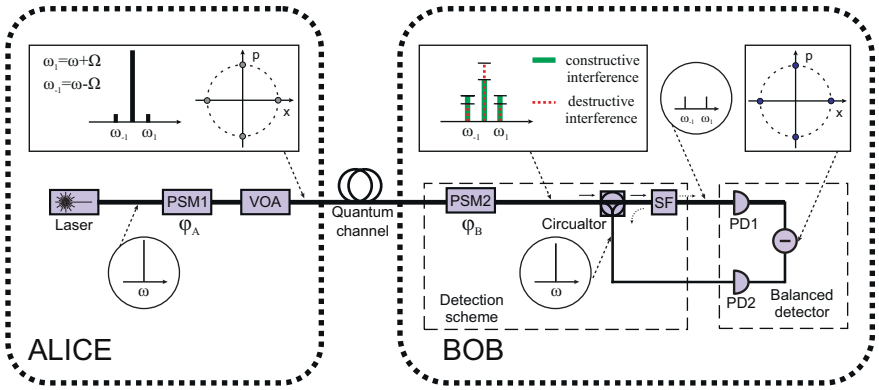

Figure 1. Principal scheme of SCW CV-QKD setup. PSM is an electro-optical phase modulator; VOA is a variable optical attenuator; SF is a spectral filter that cuts off the carrier; PD is a photodiode. Diagrams in circles show the absolute value of signal spectrum taking into account only the first-order subcarriers. Diagrams in squares illustrate the absolute value of signal spectrum and comparison of spectra for various phase shifts; different coherent states are shown on phase plane.

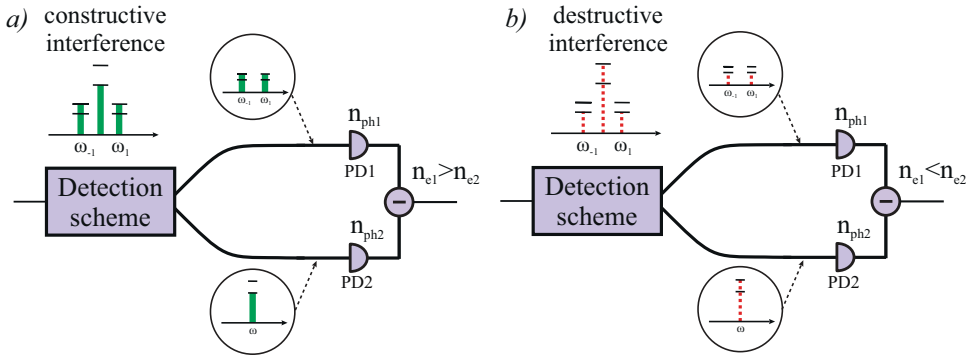

Figure 2. SCW coherent detection scheme operation. The charts show energy distribution between the carrier and the subcarriers in case of constructive (**a**) and destructive (**b**) interference. Subcarrier signal power becomes higher or lower than the carrier power, respectively. Horizontal dashes added for illustrative purposes.

Subcarrier wave CV-QKD protocol. The protocol consists of the following steps:

1. Alice prepares a multimode coherent state $|\psi_0(\varphi_A)\rangle = \otimes_{k=-S}^{s} |\alpha_k(\varphi_A)\rangle_k$ by choosing from a finite set of states (4 states is in our case). She assumes $|\psi_0(0)\rangle, |\psi_0(\pi/2)\rangle$ as "0" and $|\psi_0(\pi)\rangle, |\psi_0(3\pi/2)\rangle$ as "1".
2. Bob measures the received state in one of two bases: x or p applying a random $\varphi_B = 0, \varphi_B = \pi/2$ phase shift. The procedures described above are repeated required (large) number of times.
3. For each time instance, Alice and Bob reveal their selected bases, and mismatched bases are discarded. Bob forms his bit string by assigning 0 for negative v and 1 for the positive v values in measurement results. The threshold values are selected to maximize the secure key rate.
4. Alice and Bob apply error correction and privacy amplification procedures. In this paper, we consider only the case of direct reconciliation (DR), when Bob adjusts his data in accordance with the data of Alice. As a result, the secure secret key is distributed.

Quantum state preparation. The states prepared by Alice can be described in terms of representation basis of abelian cyclic point symmetry groups C_M respectively. The protocol which we propose here is based on four coherent states (number of bases $N = 2$). The initial state at Alice's side is $|\sqrt{\mu_0}\rangle_0 \otimes |vac\rangle_{SB}$, where $|vac\rangle_{SB}$ is the sidebands vacuum state and $|\sqrt{\mu_0}\rangle_0$ is the carrier wave coherent state with the average number of photons μ_0 emitted from a coherent monochromatic light source with frequency ω.

The state at the Alice's modulator output is a multimode coherent state

$$|\psi_0(\varphi_A)\rangle = \bigotimes_{k=-S}^{S} |\alpha_k(\varphi_A)\rangle_k, \tag{1}$$

with coherent amplitudes

$$\alpha_k(\varphi_A) = \sqrt{\mu_0}\, d^S_{0k}(\beta_A) e^{-i(\theta_1+\varphi_A)k}, \tag{2}$$

where θ_1 is a constant phase and $d^S_{nk}(\beta_A)$ is the Wigner d-function that appears in the quantum theory of angular momentum[43]. Argument of the d-function β_A is determined by the Alice's modulation index m_A, disregarding the modulator medium dispersion this dependence can be written as

$$\cos(\beta_A) = 1 - \frac{1}{2}\left(\frac{m_A}{S + 0.5}\right)^2. \tag{3}$$

The detailed description of electro-optic modulation process for quantum states can be found in[44].

Detection. The traveling wave phase modulator on the Bob's side has the same modulation frequency Ω as in the Alice's one, but a different phase φ_B and modulation index m_B. The resulting state is also a multimode coherent state

$$|\psi_B(\varphi_A, \varphi_B)\rangle = \bigotimes_{k=-S}^{S} |\alpha'_k(\varphi_A, \varphi_B)\rangle_k, \tag{4}$$

with coherent amplitudes

$$\alpha'_k(\varphi_A, \varphi_B) = \sqrt{\mu_0 \eta(L)}\, \exp(-i\theta_2 k) d^S_{0k}(\beta'), \tag{5}$$

where $\eta(L)$ is the transmission coefficient of the quantum channel. New argument of the d-function is

$$\cos\beta' = \cos\beta_A \cos\beta_B - \sin\beta_A \sin\beta_B \cdot \cos(\varphi_A - \varphi_B + \varphi_0), \tag{6}$$

where θ_2 and φ_0 are phases determined by phase modulator structure[44]. In order to achieve constructive interference, Bob should use φ_0 as an offset for his phase and apply microwave phase $\varphi = \varphi_0 + \varphi_B$ in his modulator. According to[36], the average number of photons arriving at the first arm of Bob's detector in the transmission window T is

$$n_1(\varphi_A, \varphi_B) = \mu_0 \eta(L) \eta_B (1 - (1 - \vartheta)|d^S_{00}(\beta')|^2), \tag{7}$$

where η_B is the losses in Bob's module and ϑ is carrier wave attenuation factor. Thus the average number of photons arriving at the second arm of Bob's detector is

$$n_2(\varphi_A, \varphi_B) = \mu_0 \eta(L) \eta_B (1 - \vartheta)|d^S_{00}(\beta')|^2, \tag{8}$$

After simple mathematical manipulations, we obtain

$$\beta' = \beta_A \sqrt{(\delta^2 + 2\delta \cos(\varphi_A - \varphi_B + \varphi_0) + 1)}, \tag{9}$$

where $\delta = \beta_B/\beta_A$.

Then, depending on Bob's phase choice φ_B, the measured quadrature value is proportional to the difference between the photo currents of the two photodiodes. In the absence of noise the normalized quadrature value of the signal is obtained as

$$v_m = \frac{s(n_1(\varphi_A, \varphi_B) - n_2(\varphi_A, \varphi_B))}{2 \cdot \sqrt{n_{LO}}}, \tag{10}$$

where s is detector sensitivity, n_{LO} is mean number of photons on the carrier before the second phase modulation.

When bases coincide the power arriving at Bob's detectors will be greater either at its first or second arm, depending on the phase difference. The argument of d-function β_A (and, subsequently, modulation index) is determined by mean photon number which is selected to maximise secure key rate. Parameter δ, as a ratio of modulation indices, is optimized in order to achieve the same distinguishability of quadratures for different phases in a correctly chosen basis, so that $(n_1(0, 0) - n_2(0, 0)) = |n_1(\pi, 0) - n_2(\pi, 0)|$. Hence, Bob observes quadrature distributions that are symmetrically offset with respect to zero. The dependence of mean number of photons on the relative phase shift is illustrated in Fig. 3.

Quantum bit error rate. Succeeding the detection stage for pulses in correct bases we obtain two probability density distributions (Fig. 4) that contain information about binary signals. Our channel is characterised by excess noise variance Ξ and vacuum noise variance, which is constantly defined as $V = 1/4$[20,45]. So, the probability density to obtain quadrature value v is:

$$p = \sqrt{\frac{2}{\pi(1 + \Xi)}}\, e^{-2\frac{(v - v_m)^2}{1+\Xi}}, \tag{11}$$

The overlap between the distributions contributes to the bit errors. Bob can set the threshold value v_0 in order to reduce the number of errors, then Bob expects "0", if $v < -v_0$ and "1", if $v > v_0$, thereby increasing inconclusive

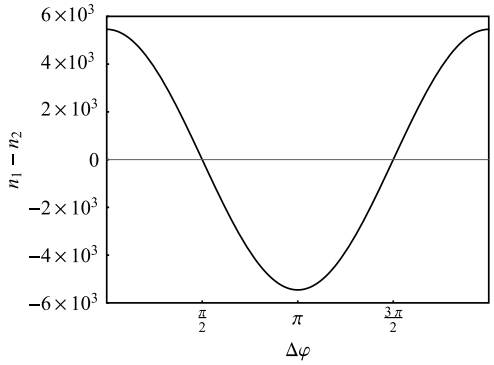

Figure 3. Dependence of the mean photon number difference on the relative phase shift represented by a cosine function. In this case the difference is maximal at points 0 and π and equals zero at points $\pi/2$ and $3\pi/2$.

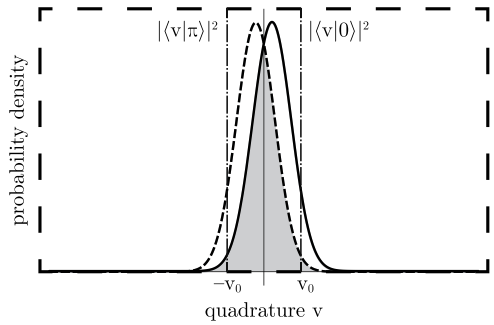

Figure 4. Quadrature distributions for correct basis with threshold values $\{-v_0, v_0\}$ with $\varphi_A = \varphi_B = \pi$.

result. Therefore for each choice of basis it has two input values, Alice's bits $x = \{0, 1\}$, and three output values: Bob's bits $y = \{0, 1\}$ and an inconclusive result or $y =$?. Considering the quantum channel as a binary symmetric channel (BSC), one may estimate detection probability density $(1 - g)$, where (g) is erasure, and the probability density that Bob assigns the wrong bit value (e), in other words, if $\varphi_A = \varphi_B = \pi$ we obtain:

$$1 - g = p(0|\varphi) + p(0|\pi + \varphi), \tag{12}$$

$$e = \frac{p(0|\pi + \varphi)}{p(0|\varphi) + p(0|\pi + \varphi)}. \tag{13}$$

After the post-selection stage, we can calculate bit error rate as $Q = E/P$, where the error probability E and post-selection rate P, respectively, are obtained as follows

$$E = \int_{-\infty}^{v_0} e(v)dv, \tag{14}$$

$$P = \int_{-v_0}^{v_0} (1 - g(v))dv. \tag{15}$$

Holevo bound. Let us consider a collective attack in the asymptotic limit on infinitely long keys for the case of our system and compute the corresponding asymptotic collective key rate using the Devetak-Winter approach[46]. We estimate an upper bound for Eve's knowledge about the data using Holevo bound[47] for weak coherent states. Finite-key analysis for our protocol is presented in the following section.

Here we use direct reconciliation scheme[48]. In this case Alice sends error correction information to Bob and the secret key is determined by Alice's data. Eve can rotate all states stored in her quantum memory after reconciliation and before her measurement. Holevo bound can be found considering unconditioned channel density operator. The Eve's quantum state, conditioned on Alice's data, is

$$|\psi_E(\varphi_A)\rangle = |\psi_0(\varphi_A)\rangle. \tag{16}$$

Eve needs to discriminate between the states in one basis

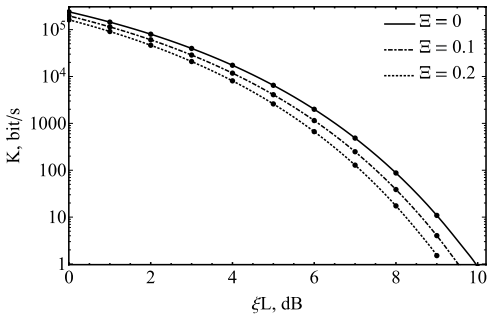

Figure 5. Secure key rate K dependence on channel loss in SCW CV-QKD system with discrete modulation including several cases of asymptotic key: with excess noise $\Xi = 0$, $\Xi = 0.1$ and $\Xi = 0.2$.

$$\rho = \frac{1}{2}|\psi_E(0)\rangle\langle\psi_E(0)| + \frac{1}{2}|\psi_E(\pi)\rangle\langle\psi_E(\pi)|. \tag{17}$$

The Holevo bound is given by

$$\chi_{DR} = S(\rho) - \sum_j p_j S(\rho_j), \tag{18}$$

where $S(\rho)$ is the von Neumann entropy, index j enumerates the possible states in the quantum channel, ρ_j is the ancilla state under condition that jth state was attacked, p_j is the weight of the jth state. The von Neumann entropy of a density operator is the Shannon entropy of its eigenvalues. The eigenvalues of the channel density operator ρ are

$$\lambda_{1,2} = \frac{1}{2}(1 \pm |\langle\psi(0)|\psi(\pi)\rangle|). \tag{19}$$

The overlapping of our states can be described as

$$\langle\psi(0)|\psi(\pi)\rangle = \exp[-\mu_0(1 - d_{00}^S(2\beta_A))]. \tag{20}$$

We therefore obtain the Holevo bound using binary Shannon entropy function $h(x)$:

$$\chi_{DR} = h\left(\frac{1}{2}(1 - \exp[-\mu_0(1 - d_{00}^S(2\beta_A))]\right). \tag{21}$$

Now we are able to estimate the secure key generation rate K:

$$K = \int_{\nu_0}^{\infty} \frac{(1-g)}{NT}[1 - h(e) - \chi]d\nu. \tag{22}$$

The secret key rates as functions of channel loss are shown in Fig. 5. The parameters of the system are $T = 100$ ns, $\eta_B = 10^{-0.64}$, $\vartheta = 10^{-6}$, $\varphi_0 = 5°$. We consider the ideal case and the case of the excess noise variance $\Xi = 0.1$. The parameters μ, μ_0 and ν_0 are optimized so as to maximize the secret key rate. The value ν_0 was optimized for losses at various distances. Equation (22) describes only the asymptotic case of infinitely long key sequences. In order to evaluate real keys it makes sense to carry out another estimation taking into account finite-key effects.

Secure key generation rate with finite-key effects. To estimate appropriate bound on secure key rate we consider the notation of Rényi entropies since they describe the worst case and not the average one[9,49]. We bound ε-smooth min-entropy[41,49,50] as follows:

$$H_{min}^{\varepsilon_s}(\mathbf{A}|\mathbf{E}) \geq n\left(H(\mathbf{A}|\mathbf{E}) - \frac{\delta(\varepsilon_S)}{\sqrt{n}}\right), \tag{23}$$

where

$$\delta(\varepsilon_s) = 4\log(2 + \sqrt{2})\sqrt{\log\left(\frac{2}{\varepsilon_s^2}\right)}, \tag{24}$$

here and $H(\mathbf{A}|\mathbf{E})$ is conditional von Neumann entropy and it denotes the entropy of Alice's bit conditioned on Eve's side-information in a single round, Eve's side information is $\mathbf{E}$. Conditional von Neumann entropy in case of direct reconciliation can be bounded as $H(\mathbf{A}|\mathbf{E}) \geq 1 - \chi_{DR}$. On the error correction step both parties should check and remover the errors in their bit strings. Here we assume that Alice and Bob use low-density parity-check

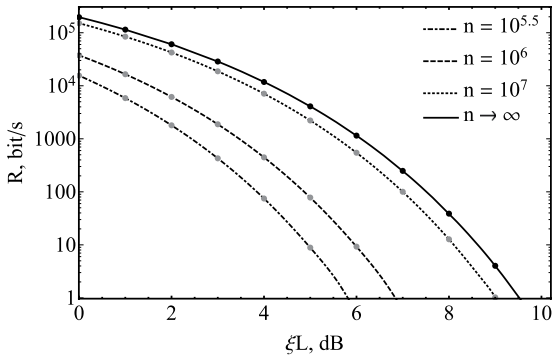

Figure 6. Secure key rate R dependence on channel loss in SCW CV-QKD system with discrete modulation for different number of detected quantum bits n.

(LDPC) codes[51]. Bob randomly chooses a k bits and sends them to Alice, then Alice estimates the quantum channel parameters. It should be noted that LDPC codes succeed only if the actual error rate value Q_{real} is less than a reference value parameterized in the code. Thus, Alice needs to consider an additional error rate fraction ΔQ. It can be estimated in order to maximize the probability of successful error correction in one round while keeping the secret key rate as high as possible. Then Alice computes the syndrome of LDPC code that corrects up to $n(Q_{est}+\Delta Q)$ error bits. We denote the length of the syndrome as

$$code_{EC} \approx nf_{EC}h(Q_{est} + \Delta Q), \tag{25}$$

where f_{EC} is error correction efficiency. Using the syndrome, Bob corrects the bits forming some new bit string $\mathbf{B}'$ and applies a two-universal hash function with output length $check_{EC}$. Bob then sends the hash to Alice in order to check whether their strings match. If the hashes are different, Alice enlarges ΔQ or aborts the protocol. Otherwise Alice obtains the bit string $\mathbf{A}'$. The remaining smooth-entropy is

$$H_{min}^{\varepsilon_s}(\mathbf{A}'|\mathbf{E}) \geq n\left(H(\mathbf{A}|\mathbf{E}) - \frac{\delta(\varepsilon_S)}{\sqrt{n}}\right) - k - code_{EC} - check_{EC}, \tag{26}$$

where sample size k is estimated by maximizing the key rate[41]. At privacy amplification step Alice and Bob hash their bit strings to a key of length l[41,52]

$$l = n\left(H(\mathbf{A}|\mathbf{E}) - \frac{\delta(\varepsilon_S)}{\sqrt{n}}\right) - k - code_{EC} - check_{EC} - loss_{PA}, \tag{27}$$

At the error correction step, we have to estimate "correctness error" ε_{EC}. From the properties of 2-universal hashing ε_{EC} is

$$\varepsilon_{EC} = 2^{-check_{EC}}, \tag{28}$$

The trace distance d between the protocol output and an ideal output is bounded by $d \leq \varepsilon_s + \varepsilon_{PA}$. We therefore obtain that the protocol is ε_{QKD}-secure and correct protocol, with $\varepsilon_{QKD} = \varepsilon_{EC} + \varepsilon_s + \varepsilon_{PA}$. Finally, the dependence of average secret key rates on losses in the quantum channel for different values of n is

$$R = \int_v^\infty \frac{1-g}{NT} \cdot \left(1 - \chi - 4\frac{1}{\sqrt{n}}\log(2+\sqrt{2})\sqrt{\log\left(\frac{2}{\varepsilon_s^2}\right)} - \frac{1}{n}\left(k + code_{EC} + \log\frac{1}{\varepsilon_{EC}} + \log\frac{1}{\varepsilon_{PA}} - 2\right)\right)dv. \tag{29}$$

It should be noted that in the asymptotic case $n \to \infty$, the Eqs. (22) and (29) converge to the same expression. The secret key rates for different values of n are presented in Fig. 6 as a function of channel loss. The parameters μ, μ_0, k and v_0. are optimized so as to maximize the secret key rate. The value v_0 is also optimized for losses at various distances. The considered security parameters are as follows: $\varepsilon_s = \varepsilon_{PA} = 10^{-10}$, $\varepsilon_{EC} = 2^{-256}$.

Discussion

In this paper we proposed the implementation of CV-QKD protocol using SCW method, built a mathematical model of the proposed scheme and demonstrated the security proof technique. We calculated the secure key rate for discrete modulation CV-QKD protocol with post-selection in the asymptotic and finite-size regime. We calculated the lower bound on the secret key rate for the CV-QKD system under the assumption that the quantum channel noise is negligible compared to detector noise and Eve is restricted to collective attacks. Our calculation

shows that the system allows to provide a secret key for channel losses up to 9 dB in a realistic system implementation. It is important to note that our scheme also allows to implement CV-QKD with Gaussian modulation and the presented security analysis can be adopted there. Subsequent works will focus on a full security proof, as well as the experimental implementation of the proposed protocol.

Received: 27 January 2020; Accepted: 29 May 2020;
Published online: 22 June 2020

References

1. Bennett, C. H. & Brassard, G. Quantum cryptography: Public key distribution and coin tossing. *Theoretical Computer Science* **560**, 7–11, https://doi.org/10.1016/j.tcs.2014.05.025 (2014).
2. Bennett, C. H. Quantum cryptography using any two nonorthogonal states. *Physical Review Letters* **68**, 3121–3124, https://doi.org/10.1103/PhysRevLett.68.3121 (1992).
3. Bennet, C. H., Bessette, F., Brassard, G., Salvail, L. & Smolin, J. Experimental quantum cryptography. *Journal of Cryptology* **5**, 3–28 (1992).
4. Tamaki, K., Koashi, M. & Imoto, N. Unconditionally Secure Key Distribution Based on Two Nonorthogonal States. *Physical Review Letters* **90**, 4, https://doi.org/10.1103/PhysRevLett.90.167904 (2003).
5. Christandl, M., Renner, R. & Ekert, A. A generic security proof for quantum key distribution, arXiv:quant-ph/0402131 (2004).
6. Renner, R., Gisin, N. & Kraus, B. Information-theoretic security proof for quantum-key-distribution protocols. *Physical Review A* **72**, 012332, https://doi.org/10.1103/PhysRevA.72.012332 (2005).
7. Christandl, M., König, R. & Renner, R. Postselection technique for quantum channels with applications to quantum cryptography. *Physical Review Letters* **102**, 020504 (2009).
8. Tomamichel, M., Colbeck, R. & Renner, R. A fully quantum asymptotic equipartition property. *IEEE Transactions on Information Theory* **55**, 5840–5847, https://doi.org/10.1109/TIT.2009.2032797 (2009).
9. Renner, R. Security of Quantum Key Distribution. *International Journal of Quantum Information* **06**, 1–127, https://doi.org/10.1142/S0219749908003256 (2008).
10. Kraus, B., Gisin, N. & Renner, R. Lower and upper bounds on the secret-key rate for quantum key distribution protocols using one-way classical communication. *Physical Review Letters* **95**, 080501, https://doi.org/10.1103/PhysRevLett.95.080501 (2005).
11. Lo, H.-K. & Chau, H. F. Unconditional security of quantum key distribution over arbitrarily long distances. *Science* **283**, 2050–2056, https://doi.org/10.1126/science.283.5410.2050 (1999).
12. Shor, P. W. & Preskill, J. Simple proof of security of the bb84 quantum key distribution protocol. *Physical Review Letters* **85**, 441, https://doi.org/10.1103/PhysRevLett.85.441 (2000).
13. Lo, H.-K., Ma, X. & Chen, K. Decoy state quantum key distribution. *Physical Review Letters* **94**, 230504, https://doi.org/10.1103/PhysRevLett.94.230504 (2005).
14. Pirandola, S. *et al*. Advances in quantum cryptography, arXiv:1906.01645 (2019).
15. Scarani, V. *et al*. The security of practical quantum key distribution. *Reviews of Modern Physics* **81**, 1301–1350, https://doi.org/10.1103/RevModPhys.81.1301 (2009).
16. Grosshans, F. & Grangier, P. Continuous Variable Quantum Cryptography Using Coherent States. *Physical Review Letters* **88**, 4, https://doi.org/10.1103/PhysRevLett.88.057902 (2002).
17. Grosshans, F. *et al*. Quantum key distribution using gaussian-modulated coherent states. *Nature* **421**, 238–241, https://doi.org/10.1038/nature01289 (2003).
18. Hirano, T., Yamanaka, H., Ashikaga, M., Konishi, T. & Namiki, R. Quantum cryptography using pulsed homodyne detection. *Physical Review A - Atomic, Molecular, and Optical Physics* **68**, 7, https://doi.org/10.1103/PhysRevA.68.042331 (2003).
19. Leverrier, A. & Grangier, P. Continuous-variable quantum-key-distribution protocols with a non-Gaussian modulation. *Physical Review A - Atomic, Molecular, and Optical Physics* **83**, https://doi.org/10.1103/PhysRevA.83.042312 (2011).
20. Heid, M. & Lütkenhaus, N. Efficiency of coherent-state quantum cryptography in the presence of loss: Influence of realistic error correction. *Physical Review A - Atomic, Molecular, and Optical Physics* **73**, 1–7, https://doi.org/10.1103/PhysRevA.73.052316 (2006).
21. Brádler, K. & Weedbrook, C. Security proof of continuous-variable quantum key distribution using three coherent states. *Physical Review A* **97**, https://doi.org/10.1103/PhysRevA.97.022310 (2018).
22. Papanastasiou, P., Lupo, C., Weedbrook, C. & Pirandola, S. Quantum key distribution with phase-encoded coherent states: Asymptotic security analysis in thermal-loss channels. *Physical Review A* **98**, 1–8, https://doi.org/10.1103/PhysRevA.98.012340 (2018).
23. Cerf, N. J., Lévy, M. & Van Assche, G. Quantum distribution of Gaussian keys using squeezed states. *Physical Review A. Atomic, Molecular, and Optical Physics* **63**, 523111–523115, https://doi.org/10.1103/PhysRevA.63.052311 (2001).
24. Diamanti, E. & Leverrier, A. Distributing secret keys with quantum continuous variables: Principle, security and implementations. *Entropy* **17**, 6072–6092, https://doi.org/10.3390/e17096072 (2015).
25. Guang-Qiang, H., Si-Wei, Z., Hong-Bin, G. & Gui-Hua, Z. Security of quantum key distribution using two-mode squeezed states against optimal beam splitter attack. *Chinese Physics B* **17**, 1263–1268, https://doi.org/10.1088/1674-1056/17/4/019 (2008).
26. Madsen, L. S., Usenko, V. C., Lassen, M., Filip, R. & Andersen, U. L. Continuous variable quantum key distribution with modulated entangled states. *Nature Communications* **3**, 1083–1086, https://doi.org/10.1038/ncomms2097 (2012).
27. Ghorai, S., Grangier, P., Diamanti, E. & Leverrier, A. Asymptotic Security of Continuous-Variable Quantum Key Distribution with a Discrete Modulation. *Physical Review X* **9**, 021059, https://doi.org/10.1103/PhysRevX.9.021059 (2019).
28. Mérolla, J.-M., Mazurenko, Y., Goedgebuer, J.-P., Porte, H. & Rhodes, W. T. Phase-modulation transmission system for quantum cryptography. *Optics Letters* **24**, 104, https://doi.org/10.1364/ol.24.000104 (1999).
29. Mora, J. *et al*. Experimental demonstration of subcarrier multiplexed quantum key distribution system. *Optics Letters* **37**, 2031, https://doi.org/10.1364/ol.37.002031 (2012).
30. Gleim, A. V. *et al*. Secure polarization-independent subcarrier quantum key distribution in optical fiber channel using BB84 protocol with a strong reference. *Optics Express* **24**, 2619, https://doi.org/10.1364/oe.24.002619 (2016).
31. Gleim, A. *et al*. Sideband quantum communication at 1 mbit/s on a metropolitan area network. *Journal of Optical Technology* **84**, 362–367, https://doi.org/10.1364/JOT.84.000362 (2017).
32. Glejm, A. *et al*. Quantum key distribution in an optical fiber at distances of up to 200 km and a bit rate of 180 bit/s. *Bulletin of the Russian Academy of Sciences: Physics* **78**, 171–175, https://doi.org/10.3103/S1062873814030095 (2014).
33. Melnik, K. *et al*. Using a heterodyne detection scheme in a subcarrier wave quantum communication system. *Bulletin of the Russian Academy of Sciences: Physics* **82**, 1038–1041, https://doi.org/10.3103/S1062873818080294 (2018).
34. Gaidash, A., Kozubov, A. & Miroshnichenko, G. Methods of decreasing the unambiguous state discrimination probability for subcarrier wave quantum key distribution systems. *JOSA B* **36**, B16–B19, https://doi.org/10.1364/JOSAB.36.000B16 (2019).
35. Gaidash, A., Kozubov, A. & Miroshnichenko, G. Countermeasures for advanced unambiguous state discrimination attack on quantum key distribution protocol based on weak coherent states. *Physica Scripta* **94**, 125102, https://doi.org/10.1088/1402-4896/ab3277 (2019).

36. Miroshnichenko, G. P., Kozubov, A. V., Gaidash, A. A., Gleim, A. V. & Horoshko, D. B. Security of subcarrier wave quantum key distribution against the collective beam-splitting attack. *Optics Express* **26**, 11292–11308, https://doi.org/10.1364/OE.26.011292 (2018).
37. Fang, J., Huang, P. & Zeng, G. Multichannel parallel continuous-variable quantum key distribution with gaussian modulation. *Physical Review A* **89**, 022315, https://doi.org/10.1103/PhysRevA.89.022315 (2014).
38. Gyongyosi, L. & Imre, S. Subcarrier domain of multicarrier continuous-variable quantum key distribution. *Journal of Statistical Physics* 1–24, https://doi.org/10.1007/s10955-019-02404-2 (2014).
39. Wang, Y., Mao, Y., Huang, W., Huang, D. & Guo, Y. Optical frequency comb-based multichannel parallel continuous-variable quantum key distribution. *Optics express* **27**, 25314–25329, https://doi.org/10.1364/OE.27.025314 (2019).
40. Kynev, S. M. *et al*. Free-space subcarrier wave quantum communication. *Journal of Physics: Conference Series* **917**, 052003, https://doi.org/10.1088/1742-6596/917/5/052003 (2017).
41. Kozubov, A., Gaidash, A. & Miroshnichenko, G. Finite-key security for quantum key distribution systems utilizing weak coherent states, arXiv:1903.04371 (2019).
42. Yariv, A. & Yeh, P. *Optical waves in crystals* 5 (Wiley, New York, 1984).
43. Varshalovich, D. A., Moskalev, A. N. & Khersonsky, V. *Quantum Theory of Angular Momentum*. (World Scientific, Singapore, 1988).
44. Miroshnichenko, G. P., Kiselev, A. D., Trifanov, A. I. & Gleim, A. V. Algebraic approach to electro-optic modulation of light: exactly solvable multimode quantum model. *Journal of the Optical Society of America B* **34**, 1177, https://doi.org/10.1364/JOSAB.34.001177 (2017).
45. Symul, T. *et al*. Experimental demonstration of post-selection-based continuous-variable quantum key distribution in the presence of Gaussian noise. *Physical Review A - Atomic, Molecular, and Optical Physics* **76**, 1–4, https://doi.org/10.1103/PhysRevA.76.030303 (2007).
46. Devetak, I. & Winter, A. Distillation of secret key and entanglement from quantum states. *Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences* **461**, 207–235, https://doi.org/10.1098/rspa.2004.1372 (2005).
47. Holevo, A. Bounds for the quantity of information transmitted by a quantum communication channel. *Problemy Peredachi Informatsii* **9**, 3–11 (1973).
48. Hirano, T. *et al*. Implementation of continuous-variable quantum key distribution with discrete modulation. *Quantum Science and Technology* **2**, https://doi.org/10.1088/2058-9565/aa7230 (2017).
49. Rényi, A. On Measures of Entropy and Information. In *Proceedings of the Fourth Berkeley Symposium on Mathematical Statistics and Probability, Volume 1: Contributions to the Theory of Statistics*, vol. 1, 547–561 (University of California Press, Berkeley, Calif., 1961).
50. Tomamichel, M. A framework for non-asymptotic quantum information theory, arXiv:1203.2142 (2012).
51. Gallager, R. Low-density parity-check codes. *IEEE Transactions on Information Theory* **8**, 21–28, https://doi.org/10.1109/TIT.1962.1057683 (1962).
52. Arnon-Friedman, R., Renner, R. & Vidick, T. Simple and tight device-independent security proofs. *SIAM Journal on Computing* **48**, 181–225, https://doi.org/10.1137/18m1174726 (2019).

Acknowledgements

This work was funded by Government of Russian Federation (grant MK-777.2020.8).

Author contributions

E. Samsonov and R. Goncharov wrote the main manuscript text; A. Gaidash and A. Kozubov reviewed math calculations; V. Egorov reviewed the manuscript. A. Gleim proposed the main scheme (Fig. 1).

Competing interests

The authors declare no competing interests.

Additional information

Correspondence and requests for materials should be addressed to E.S.

Reprints and permissions information is available at www.nature.com/reprints.

Publisher's note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.