Frontiers of Physics
https://doi.org/10.1007/s11467-020-1025-x
Front. Phys.
16(2), 21503 (2021)

RESEARCH ARTICLE

Generic security analysis framework for quantum secure direct communication

Zhang-Dong Ye[1], Dong Pan[1], Zhen Sun[3], Chun-Guang Du[1], Liu-Guo Yin[2,3,4,5,†], Gui-Lu Long[1,2,4,5,‡]

[1] *State Key Laboratory of Low-Dimensional Quantum Physics and Department of Physics, Tsinghua University, Beijing 100084, China*
[2] *Frontier Science Center for Quantum Information, Beijing 100084, China*
[3] *School of Information and Technology, Tsinghua University, Beijing 100084, China*
[4] *Beijing National Research Center for Information Science and Technology, Beijing 100084, China*
[5] *Beijing Academy of Quantum Information Sciences, Beijing 100193, China*
Corresponding authors. E-mail: [†] *yinlg@tsinghua.edu.cn,* [‡] *gllong@tsinghua.edu.cn*
Received September 1, 2020; accepted October 20, 2020

Quantum secure direct communication provides a direct means of conveying secret information via quantum states among legitimate users. The past two decades have witnessed its great strides both theoretically and experimentally. However, the security analysis of it still stays in its infant. Some practical problems in this field to be solved urgently, such as detector efficiency mismatch, side-channel effect and source imperfection, are propelling the birth of a more impeccable solution. In this paper, we establish a new framework of the security analysis driven by numerics where all the practical problems may be taken into account naturally. We apply this framework to several variations of the DL04 protocol considering real-world experimental conditions. Also, we propose two optimizing methods to process the numerical part of the framework so as to meet different requirements in practice. With these properties considered, we predict the robust framework would open up a broad avenue of the development in the field.

Keywords quantum secure direct communication (QSDC), practical security analysis, secrecy capacity optimization, detector efficiency mismatch, convex optimization

1 Introduction

Quantum secure direct communication (QSDC) was proposed by Long and Liu in 2000 [1, 2], which is a way of achieving secure communication by transmitting secret information directly over the quantum channel. Guaranteed by quantum-mechanical properties of the information carriers, say entangled photons [1, 3, 4] or single photons [5], two legitimate distant parties can detect eavesdropping on-site during the communication via random sampling of the quantum states. The past two decades have witnessed the blossom of QSDC both theoretically and experimentally. In addition to point-to-point protocols [1, 1, 3–5], multiuser communication schemes have also made great strides [6, 7]. Recently, the theoretical protocols of measurement-device-independent QSDC that eliminate the loopholes of the measurement devices have been proposed [8–12], while device-independent QSDC protocols that relax the security assumptions on the quantum devices are brewing up for example in Ref. [13]. Meanwhile, more interesting schemes contributed to the aim of QSDC have been established, such as quantum illumination [14], quantum data locking [15] and quantum low probability of intercept [16]. In the aspect of experiments, the first proof-of-principle implementation using a frequency coding strategy [17] demonstrates the feasibility of QSDC over a noisy quantum channel, which is afterwards followed by a demonstration experiment of entanglement-based QSDC protocol materialized by the quantum-memory-assisted (QMA) system [18]. In particular, the QMA system makes it promising to conduct super-long-distance communication [19] and to construct QSDC networks. The free-space communication scheme has been studied as well, shown in the literature [20]. Moreover, some typical applications of optical quantum information have been presented [21–24], which are promisingly potential to facilitate the implementation of QSDC.

Despite the great progress achieved, the security analysis of QSDC had been staying at the qualitative stage for a time before Qi *et al.* came up with the first quantitative analysis framework [25] illuminated by the two-way QKD analysis strategy in Refs. [26, 27]. On the top of Qi's framework, the work in Ref. [28] gives a further exposition

*arXiv: 2011.14546. This article can also be found at http://journal.hep.com.cn/fop/EN/10.1007/s11467-020-1025-x.

on the asymptotic secrecy capacity of QSDC under the collective attacks. However, some idealized assumptions have to be made in this framework to accommodate the strategy used in Ref. [27]. For example, bits "0" and "1" come up randomly in the encoded message and furthermore, the information source could be perfectly compressed. On the other hand, the calculation to find the eigenvalues of the Gram matrix involved is pretty mathematically technical especially when the composite system of the legitimate users and the adversary becomes complicated in the cases where practical conditions are considered or higher dimensional protocols are carried out.

In this work, we establish a new framework of the security analysis to completely address the above-stated problems getting in the way at present and bridge the gap between ideal protocols and practical implementations. In the framework, we are looking at the forward channel security rather than that of the backward one as the information reading totally depends on the states from the forward channel. If those states are kept secure, the security of the backward channel will be unquestioned naturally. In other words, if we reliably estimate the secrecy capacity of the forward channel, we are able to guarantee communication security by choosing the encoding strategy according to the secrecy capacity. Besides, inspired by the numerical security proof methods in QKD [29, 30], we resort to a numerical means of handling the analysis of the adversary's behavior instead of doing it manually. This could dramatically simplify the analysis process especially when we take into account the practical conditions, such as detector efficiency mismatch, side-channel effect, source imperfection and so on, in practical communications while some of the imperfections have been considered in QKD already such as in references [31, 32]. It should be emphasized that this framework can be generalized to finite-size effect scenarios by using statistical methods and loosening the constraints used in our case. We are confident that this work would greatly propel the development in the QSDC field.

The rest of the paper is arranged as follows. In Section 2, we formally define the prototype of QSDC protocols and describe the communication process in quantum-mechanical language. Then, on the top of the prototype, the security analysis framework is constructed in Section 3. Two optimization methods are proposed in Section 4 to meet various real-world needs and also the algorithm cores are both lined up in this part. Afterward, we apply our framework to several examples in Section 5. Then come the Conclusion and Appendix.

2 General QSDC protocol

2.1 The protocol

For simplicity of presentation, we will describe the entanglement based protocol while the prepare-and-measurement protocol can be viewed as an equivalent by the source replacement scheme [33].

Step 1: The entanglement source (hypothetically held by Bob) allocates two qubits respectively to Alice and Bob. Repeat this for N ($N \to \infty$) times.

Step 2: When Alice and Bob receive the qubits, Bob measures the qubit with his positive-operator valued measurements (POVMS) $\{F_j^B\}$ while Alice with probability $c \ll 1$, measures by the POVMs $\{F_i^A\}$. At the meantime, they exchange the measurement outcome information via a classical channel and negotiate with each other to do a security estimation to make sure the quantum channel security capacity $\mathcal{C}_s$ is no less than 0. Otherwise, they abolish the communication and go back to step 1.

Step 3: Alice encodes the rest $(1-c)N$ qubits with a certain set of unitary operators $\{U_k^A\}$ and resends those photons encoded to Bob and Bob decodes the message by using the measurement basis that he used in step 2 (if step 4 is needed, some check qubits are marked among the message qubits). So far a batch of secure communication has been completed. They go on to step 1 for the next round, or for the sake of robustness, they could additionally carry out step 4 even though no useful information would be leaked to the adversary.

Step 4: Before decoding the message, Bob will do a second round check by measuring these in-advance inserted checking qubits from step 3 to guarantee the integrity of the information.

2.2 Quantum-mechanical description of the prototype

The entanglement source produces a two-qubit state ρ_{AB}. Once the bipartite state (to be exact, the system of Alice) is exposed to the forward public quantum channel $\mathcal{E}_f$, it evolves into

$$\rho'_{ABC} = \mathcal{E}_f(\rho_{AB}), \tag{1}$$

which should be a pure state where the adversary Charlie holds the purifying system C since we suppose Charlie is powerful enough within the scope of quantum mechanics. After the encoding step, the whole system becomes

$$\rho''_{ABCE} = \mathcal{E}_E(\rho'_{ABC}) \tag{2}$$

with $\mathcal{E}_E(\cdot)$ an encoding map used to encode the message into the state and E as a register storing the encoding information. Here we are not going to specify the form of $\mathcal{E}_E(\cdot)$ as we will give the security proof without knowing the specific formula of $\mathcal{E}_E(\cdot)$. As long as Alice has the states encoded, she resends them back to Bob who is going to do a word-reading map denoted by $\mathcal{E}_W(\cdot)$ where W is the register system keeping the reading-out information. Thus comes the final compound state

$$\rho'''_{ABCEW} = \mathcal{E}_W\left(\mathcal{E}_b(\rho''_{ABCE})\right) \tag{3}$$

with $\mathcal{E}_b(\cdot)$ as the backward channel. Similarly, the specific form of $\mathcal{E}_W$ is not important in the later analysis. The whole process description is illustrated as in Fig. 1.

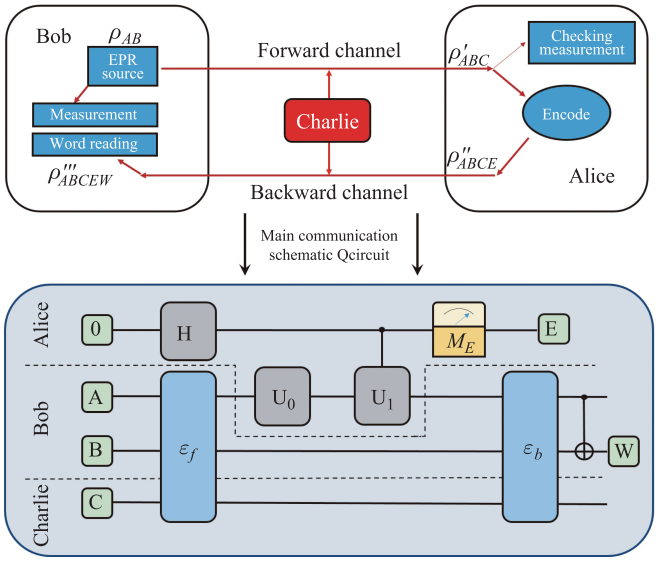

Fig. 1 Schematic of quantum secure direct communication and the main communication quantum circuit. The lower part is used as an illustration of the main communication process. H is a Hardmard gate; U_0 and U_1 are the encoding unitary gates; M_E is the post-selection measurement selected by Alice to encode classical information; 0 denotes state $|0\rangle$ while A, B, C, E, W denote the corresponding registers: A, the qubit that Bob transmits to Alice; B, the qubit Bob possesses at his laboratory; C, the adversary's system (needless to be a qubit system); E, the register storing encoding information of Alice; W, the register storing Bob's decoding information. Here the entanglement state $\rho_{AB} = (|00\rangle + |11\rangle)/\sqrt{2}$.

3 Security proof framework

According to information theory [34], secret communication can be guaranteed if the main channel capacity $\mathcal{C}_m$ of the legitimate bipartite users is bigger than that of the eavesdropping channel, $\mathcal{C}_c$, that is to say, the users can obtain a positive secrecy capacity

$$\begin{aligned}\mathcal{C}_s &= \mathcal{C}_m - \mathcal{C}_c \\ &= I(E^A : W^B) - I(E^A : C) \\ &= H(E^A|C) - H(E^A|W^B),\end{aligned} \tag{4}$$

where $I(X|Y) = S(\rho_X) + S(\rho_Y) - S(\rho_{XY})$ represents mutual entropy and $H(X|Y) = S(\rho_{XY}) - S(\rho_Y)$ represents the conditional von Neumann entropy with $S(\rho)$ as the von Neumann entropy. The superscripts in the equations denote the possessors of the registers.

Similar to QKD's key rate analysis, to make sure the security of a QSDC protocol we have to consider the worst-case scenario when calculating the secrecy capacity, which means we think of

$$\mathcal{C}_s = \min[H(E^A|C) - H(E^A|W^B)]_{\rho'''_{ABCEW}}. \tag{5}$$

Note that the second term of the right hand side of Eq. (5) is determined by Alice and Bob's error correction sacrifice. So to be more tight, it can be drawn out of the minimization, leaving

$$\mathcal{C}_s = \min[H(E^A|C)]_{\rho'''_{ABCE}} - H(E^A|W^B)_{\rho'''_{ABCEW}} \tag{6}$$

$$\geq \min[H(K^B|C) - H(K^B|K^A)]_{\rho'_{ABC}} - H(E^A|W^B)_{\rho'''_{ABCEW}} \tag{7}$$

$$= \min[H(K^B|C)]_{\rho'_{ABC}} - \gamma h(Q_f) - \gamma h(Q_b), \tag{8}$$

where K denotes an imaginary qubit-bit transforming map result for example in polarization system, $|H\rangle, |D\rangle \to 0$ and $|V\rangle, |A\rangle \to 1$ with $|H\rangle, |D\rangle, |V\rangle, |A\rangle$ respectively standing for horizontal, diagonal, vertical, anti-diagonal polarizations. γ is error correction rate. Without a further declaration, we will take γ to be 1 as the error correction process is conducted at Shannon limitation for the following numerics. Eq. (7) is derived from the fact that Charlie would not know more useful information from the state ρ''_{ABCE} than that from the forward channel eavesdropping since the encoding information depends totally on the original state of the qubits sent by Bob. The equal sign of Eq. (7) holds when Charlie reads out all the information from the qubits which he has controlled after forward channel taping. For the purpose of convenience, we define two terms to characterize the secrecy capacity (see Appendix A for classified elaboration). *Secure capacity* $\mathcal{C}_s^s = \min[H(K^B|C)]_{\rho'_{ABC}} - H(K^B|K^A)_{\rho'_{ABC}}$. Under this capacity, the adversary knows nothing about the information sent. *Reliable capacity* $\mathcal{C}_s^r$ stands for the secrecy capacity where backward channel error rate Q_b and forward channel error rate Q_f are both considered. For convenience, we take $Q_f = Q_b = Q$ to compute the reliable capacity since without extra influence caused by the adversaries, Q_b would be no bigger than Q_f. In fact, considering the two-round compensation effect for the optical system [35], Q_b should be always less than Q_f. Therefore, since Q_f and Q_b are both from observations, the ultimate goal of calculating the secrecy capacity is to optimize the first term of Eq. (8),

$$g = \min H(K^B|C) \tag{9}$$

with the other terms obtained from specific communication implementation. The qubit–bit map can also be visioned as an isometry $\mathcal{V}_K = \sum_l \kappa_l^B \otimes |l\rangle$ with respect to ρ'_{AB}, κ_l^B being a projector subjected to $\sum_l \kappa_l^B = I_B$. Using that ρ'_{ABC} is pure, we technically remove the dependence of Charlie's system in the optimization by the method mentioned in Refs. [29, 36, 37], achieving

$$g(\rho'_{AB}) = \min_{\rho'_{AB}} S(\rho'_{AB} || \sum_l \kappa_l^B \rho'_{AB} \kappa_l^B), \tag{10}$$

$$\text{s.t. } \mathrm{tr}(\rho'_{AB} \cdot F_i^A \otimes F_j^B) = Pr_{ij}, \tag{11}$$

$$\mathrm{tr}(\rho'_{AB}) = 1, \tag{12}$$

$$\rho'_{AB} \succ 0, \tag{13}$$

with Pr_{ij} as the joint probability from observation of *step 2* of the protocol, where $S(\varrho||\varsigma) = \mathrm{tr}(\varrho\log\varrho - \varsigma\log\varsigma)$ represents the relative entropy whose convexity over variable ρ'_{AB} is guaranteed as is shown in Ref. [38]. In other words, $\mathcal{C}_s$ must have a global minimum over the feasible domain of a constrained density operator. Now the secrecy capacity is only relying on the composite system ρ'_{AB} which can be easily constrained by the forward channel checking measurement. Notice that sometimes an imaginary post-selection is needed in general, that is, this ρ'_{AB} will be subjected to a post-selection map $\mathcal{G}$. This map won't impact the form of Eq. (10), and more detailed discussion on this map could be found in Ref. [29].

4 Optimization proposals

In this section, we are going to present two useful optimization methods to handle Eq. (10) in order to obtain the secrecy capacity. Beforehand, we define a feasible domain set $\mathcal{D} = \{\rho \succ 0 : \mathrm{tr}(\rho F_i^A \otimes F_j^B) = Pr_{ij},\ \mathrm{tr}(\rho) = 1\}$ constrained by Eqs. (11)–(13). Then, the optimization methods go as what follows.

4.1 Special projected gradient descent

First, we present a special projected gradient descent method (SPGD) [39, 40], in which, a "momentum" χ_s at s-th iteration is involved to memorize the last sub-optimizing point. This method helps to avoid a dramatic descend and departing too much from the feasible domain $\mathcal{D}$ compared with the traditional gradient descent method. With $\mathcal{P}_{\mathcal{D}}(\cdot)$ as the map projecting any point in the density operator space into the feasible domain $\mathcal{D}$, the iteration core of the algorithm can be described as

$$\chi_{s+1} = \mu\chi_s - \zeta \cdot \nabla g(\rho_s), \tag{14}$$
$$\rho_{s+1} = \mathcal{P}_{\mathcal{D}}(\rho_s + \chi_{s+1}), \tag{15}$$

where μ controls the depth of the memorization of the last point and χ is the step size which can be decided according to the practical iteration numbers or set to be a constant. $\nabla g(\rho_s)$ is the gradient of $g(\rho)$ in Eq. (10) when $\rho = \rho_s$ and ρ_s is the s-th iteration (sub-optimization) point. Empirically, this method works more properly than merely-projected gradient descent in our case considering the restriction to the feasible domain is kind of strong.

4.2 Conditional gradient descent

Also, we can apply the conditional gradient descent method (CGD) [41] to the optimization in Eq. (10) as this method is talented for dealing with the optimization with constraints set in advance. The main idea of the method is to transform an optimization problem into a series of linear optimizations until it finds a proper optimum. Based on this thought, the method works efficiently at the beginning interactions but converges slowly afterwords. The core part of the algorithm reads

$$\rho_{s+1} = \zeta\omega_s + (1-\zeta)\rho_s, \tag{16}$$
$$\omega_{s+1} = \arg\max_{\sigma\in\mathcal{D}} \mathrm{tr}(\nabla g(\rho_s)\cdot\sigma), \tag{17}$$

where ζ also denotes the step size which can be decided by another minimization in each iteration to make sure an optimal step decrease, or simply determined by the iteration number as the former method does. As a rough approximation has been made in each sub-optimization, finding the ultimate optimum will come across a precision problem. Usually, the global optimum stands outside the feasible domain leaving the constrained optimum lying on the boundary of the constraints. This might also pose a numerical challenge for the "approximation" optimization because the behaviour of it is kind of subtle around the boundary.

5 Applications to specific examples

With all the framework defined and optimization methods proposed, we then apply our security analysis approach to several protocols where some are hard (or even impossible) to achieve an analytical security proof, such as those with all detector efficiencies included.

5.1 DL04 protocol and DL04-6-state protocol

First, as an appetite try-on, we utilize the new framework to calculate the secrecy capacity of the famous QSDC protocol DL04 [5] based on entanglement source. According to the source replacement scheme, both entanglement-based and prepare-and-measure protocols can be equal-

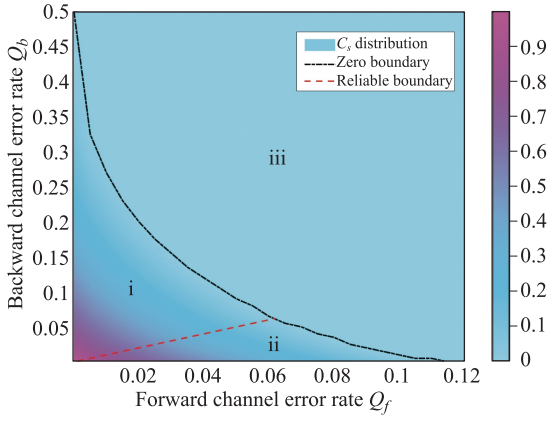

Fig. 2 Secrecy capacity distribution of DL04 protocol vs. forward channel error rate Q_f and backward channel error rate Q_b. The black dash line is the boundary of the secure and insecure scenarios. "iii" denotes the insecure one while "i"+"ii" represents the opposite. The red dash line represents the boundary where $Q_f = Q_b$ that partitions the part of secure scenario.

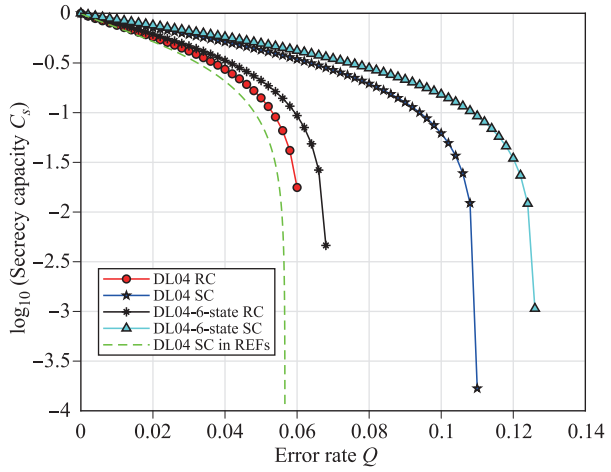

Fig. 3 Secrecy capacity subjected to logarithm based on 10 vs. error rate Q. All the capacities stand for DL04 protocols classical or improved. The green dash line denotes the result from Refs. [25, 28] while the others are derived from the new numerical framework. The abbreviation "RC" represents reliable capacity while "SC" represents secure capacity. Every symbol here denotes a numerical result. Note that when Q_f and Q_b are used together, we take them both as Q, i.e., $Q_f = Q_b$ to facilitate the plotting and demonstration.

ized. The result of the secrecy capacity vs. forward and backward channel error rates, Q_f and Q_b, is shown in Fig. 2 where three partitions denoted by i, ii, and iii are divided by two boundaries, respectively zero capacity boundary and reliable capacity boundary. The black curve seems a bit defective because of numerical precision. This can be refined by tightening the precision parameters and increasing the dot density. In Fig. 3, we compare the secrecy capacities derived from the new method and the previous method in Refs. [25, 28]. Our new method beats the previous one for both secure capacity and reliable capacity. We also make some variation on the classical DL04 protocol via introducing σ_y basis checking measurement when carrying out the security checking phase. That is, in the modified protocol, DL04-6-state protocol, more information can be obtained from the check phase used to bound the adversary's knowledge of the state shared by Alice and Bob. As demonstrated in the figure, this modification improves capacity for it shrinks the searching space of the problem Eq. (10).

5.2 Imperfection of detectors

In practical communication, the optical detectors are far from perfect as the real-world efficiencies of the detectors are not 1. Meanwhile, each of the detectors used in the experiment may not match one another, i.e., they possess different efficiencies. If every detector matches, one can simply attribute the common loss rate of the detector to the channel loss, which would decrease the capacity proportionally. However, the mismatch of the detectors can not be handled by this trivial attribution since the adversary may take advantage of the loophole caused by the spatial-mode detector-efficiency mismatch [42, 43]. So it poses a problem to be considered in the implementation of QSDC. Under our framework, this problem can be easily addressed by incorporating each of the efficiencies into the checking measurement operators. Note that the mismatch of Bob's decoding detectors does not ruin the security.

Considering above, we apply our framework to the analysis of detector efficiency mismatch cases. In order to obtain a set of experimental data, we simulate the measurement results under depolarizing channel $\mathcal{E}^d$, that is,

$$\mathcal{E}^d(\rho_{AB}) = \frac{\epsilon}{d_B(d_A-1)} \begin{pmatrix} I_A^{\not\in 0} & \\ & 0 \end{pmatrix} \otimes I_B + (1-\epsilon)\rho_{AB}, \quad (18)$$

where ϵ is the depolarizing parameter. d_A and d_B are the dimensions of respectively Alice's and Bob's systems. In the simulation, we vision Bob's detectors as ideal ones as it should be in the prepare and measurement scenario while Alice's are imperfect. "$\not\in 0$" denotes the space except the non-detection subspace (or called vacuum space). It should be emphasized that this framework can be used under arbitrary quantum channels including but not limited to the depolarizing one. For comparison, we set the bigger detector efficiency varying in $(1, 0.75, 0.5)$ and tune the mismatch rate η semi-continuously to observe the reliable capacity at each circumstance. From Fig. 4, the detector efficiency mismatch will certainly ruin the secrecy capacity of QSDC. Especially, we calculate a family of lines of $\eta_{big} = 0.5$ for these detector settings are close to practical ADP detectors, so the result may be used as a reference to real cases. Judging from the figure, we find that the SPGD method goes deeper than CGD does. The

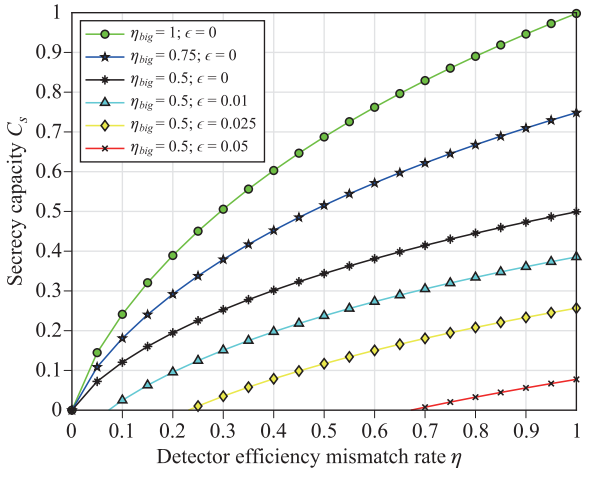

Fig. 4 Secrecy capacity C_s vs. detector efficiency mismatch rate η. The bigger detector efficiency denoted by η_{big} while the smaller one is $\eta \cdot \eta_{big}$. The depolarizing channel parameter ϵ varies in $(0, 0.01, 0.025, 0.05)$ and η_{big} varies in $(1, 0.75, 0.5)$. Note that the secrecy capacities here are referred to as reliable capacities. Every symbol denotes a numerical result.

red line shows CGD reaches a favourable sub-minimum in a very short time but it is hard for CGD to achieve a high precision result. That is to say, both of the two methods possess their advantages. To take advantage of each method, we combine them as a complementary one (COMB) demonstrated as the blue dotted line. This combination cuts down the ruining time to achieve an appropriate minimum up to the precision of 10^{-10}.

5.3 Comparison of the optimization methods

As in Section 4, we have brought forward two optimization methods, SPGD and CGD. In this part, we compare the speeds and optimizing depths of the two methods under DL04 protocol framework to illustrate their properties when solving the problem Eq. (10). In Fig. 5, the relations between optimizing depth and the time used to reach this depth are plotted. The optimizing depth is characterized by the gap between current sub-optimization value of the function $g(\rho)$ and the finial optimum which is fixed in advance according to SPGD's limit depth. Judging from the figure, we find that the SPGD method goes deeper and deeper in every iteration and eventually reaches the final "deepest" minimum illustrated as the green dots. The red dotted line shows CGD reaches a favourable sub-minimum in a very short time but it is hard for CGD to achieve a high precision result and after the first very efficient iteration, it oscillates back and forth around the first depth. Then it goes even worse after a few iterations. In conclusion, both of the two methods possess their advantages. To take advantage of each method, we combine them together as a complementary one (COMB) whose performance is demonstrated as the blue dotted line. This combination cuts down the ruining time to achieve an appropriate minimum up to the precision of 10^{-10} and considerably save half of the time of SPGD. Note that in the literature [30], the authors propose a dual problem of the optimization to make sure the tightness of the results derived from numerics. That is a good choice to guarantee the numerical results but it truly perplexes the problem itself. And sometimes when the requirement of the precision is pretty high, this dual optimization fails as shown in Fig. 2 and Fig. 5 in Ref. [44]. We propose these three methods as choices to make sure the optimization goes deep enough so that we could reliably keep the first significant digits of the numerical results.

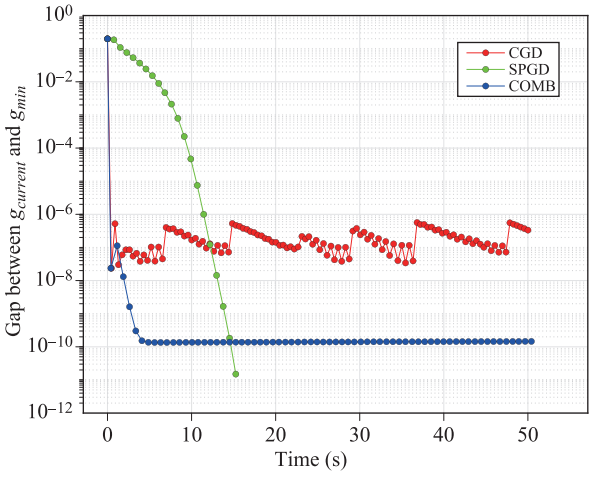

Fig. 5 The gap between current objective function value $g_{current}$ and the final minimum g_{min}. The dots on each line denote the iteration points. The green dotted line gives the optimization trend of special projected gradient descent (SPGD) method while the red line shows that of the conditional gradient descent (CGD) method. The blue line demonstrates the trend of the method stemming from the combination of CGD and SPGD. The comparison data are acquired under DL04 protocol background.

6 Conclusion

We have established a new security analysis framework oriented for quantum secure direct communication. First of all, the prototype of a generic QSDC protocol is redefined, and following this prototype we present the framework quantum-mechanically. Furthermore, we investigate the security of different variations of DL04 protocol via the new framework driven by numerical optimizations. Meanwhile, pursuing preciser and faster optimization, we have proposed two methods SPGD and CGD and studied their properties. As a result of the comparison, one could choose these methods according to practical requirements. Above all, we remark that this framework can be used to analyse almost any practical QSDC protocols as it simplifies the investigation of the adversary's actions and can take into account the implementation conditions such as real-world detector efficiencies and the imperfection of the communication source. With the constructive advantages of the framework, it can be extended to the finite-size secrecy capacity analysis as well. All in all, this framework may open up a broad avenue for the development of QSDC among the research community.

Acknowledgements We would like to thank Jiawei Wu for his generous providing of the comparison data in Fig. 3 and thank Jie Lin for the help of the numerical techniques. This work was supported by the National Key Research and Development Program of China under Grant No. 2017YFA0303700, the Key Research and Development Program of Guangdong province under Grant No. 2018B030325002, the National Natural Science Foundation of China under Grant No. 11974205, and Beijing Advanced Innovation Center for Future Chip (ICFC).

Appendix A Definitions and abbreviations

Secrecy capacity labeled by $\mathcal{C}_s$: the difference of the main channel capacity and the tap channel capacity.

Secret capacity (SC) labeled by $\mathcal{C}_s^s$: The secrecy capacity when backward channel is not considered. As described in the main text, the secrecy of QSDC can be totally guaranteed by forward channel checking, i.e., if $\mathcal{C}_s^s > 0$, the communication is secure.

Reliable capacity (RC) labeled by $\mathcal{C}_c^r$: The secrecy capacity when both forward and backward channels are considered. In addition to guaranteeing the secrecy of QSDC, if $\mathcal{C}_s^r > 0$, the integrity of the information conveyed during the communication is guaranteed.

Appendix B The derivation of the main optimization problem

In this section, we are going to derive the main optimization problem in Eq. (10) from Eq. (9),

$$g = \min H(K^B|C) = \min[S(\rho'^{*}_{CK^B}) - S(\rho'_C)]. \tag{19}$$

Using that ρ'_{ABC} is pure and $\mathcal{V}_K = \sum_l \kappa_l^B \otimes |l\rangle$ is an isometry, we obtain

$$\begin{aligned}
g &= \min\{S[\mathrm{tr}_{CK^B}(\rho'^{*}_{ABCK^B})] - S(\rho'_{AB})\} && (20)\\
&= \min\{S[\mathrm{tr}_{CK^B}(\sum_l \kappa_l^B \otimes |l\rangle\, \rho'_{ABC} \sum_{l'} \kappa_{l'}^B \otimes \langle l'|)]\\
&\quad - S(\rho'_{AB})\} && (21)\\
&= \min\{S[\mathrm{tr}_C(\sum_l \kappa_l^B \rho'_{ABC} \kappa_l^B)] - S(\rho'_{AB})\} && (22)\\
&= \min\{S(\sum_l \kappa_l^B \rho'_{AB} \kappa_l^B) - S(\rho'_{AB})\} && (23)\\
&= \min\{-\sum_l \mathrm{tr}[\kappa_l^B \rho'_{AB} \kappa_l^B \log(\sum_{l'} \kappa_{l'}^B \rho'_{AB} \kappa_{l'}^B)]\\
&\quad - S(\rho'_{AB})\} && (24)\\
&= \min\{-\mathrm{tr}[\rho'_{AB} \log(\sum_l \kappa_l^B \rho'_{AB} \kappa_l^B)] - S(\rho'_{AB})\} && (25)\\
&= \min S(\rho'_{AB} || \sum_l \kappa_l^B \rho'_{AB} \kappa_l^B). && (26)
\end{aligned}$$

Appendix C Entanglement based DL04 protocol with detector efficiency mismatch

We establish the model for entanglement based DL04 protocol with detector efficiency mismatch in this part. The POVMs Alice's measurement can be expressed as

$$\begin{aligned}
F_1^A &= p_z \eta_{big} |0\rangle\langle 0| \oplus (0)^{\in 0}, && (27)\\
F_2^A &= p_z \eta_{big} \eta |1\rangle\langle 1| \oplus (0)^{\in 0}, && (28)\\
F_3^A &= (1-p_z) \eta_{big} |+\rangle\langle +| \oplus (0)^{\in 0}, && (29)\\
F_4^A &= (1-p_z) \eta_{big} \eta |-\rangle\langle -| \oplus (0)^{\in 0}, && (30)\\
F_5^A &= I - \sum_{j=1}^{4} F_j^A, && (31)
\end{aligned}$$

where $|0\rangle, |1\rangle$ are the basis vectors of the Pauli operator σ_z, $|+\rangle, |-\rangle$ are the basis vectors of σ_x and $(0)^{\in 0}$ is a 1-by-1 "matrix" in non-click subspace. Similarly, the POVMs for Bob's measurement are

$$\begin{aligned}
F_1^B &= p_z |0\rangle\langle 0|, && (32)\\
F_2^B &= p_z |1\rangle\langle 1|, && (33)\\
F_3^B &= (1-p_z) |+\rangle\langle +|, && (34)\\
F_4^B &= (1-p_z) |-\rangle\langle -|, && (35)
\end{aligned}$$

as his detectors are viewed as ideal ones in order to completely model the original DL04 protocol which utilizes single photons in the scheme. p_z denotes the σ_z-basis-choosing factor. For simplicity of processing, p_z should be very close to 1 or 0 alternatively. Otherwise, a normalization factor has to be introduced in order not to underestimate the secrecy capacity as after the forward channel in the protocol, we assume an imaginary qubit–bit map to evaluate the information amount. As a mater of fact, there is no basis choosing phase during the formal communication period except the checking phase. Specifically in our nurmerics, we set $p_z = 0.999$. The simulated date used in Section 5.2 is produced as

$$Pr_{ij} = \mathrm{tr}(\mathcal{E}^d(\rho_{AB}) F_i^A \otimes F_j^B). \tag{36}$$

$\mathcal{E}^d(\cdot)$ is defined as in Eq. (18). The post-selection map $\mathcal{G}$ can be described by two Kraus operators $\{\mathcal{K}_1, \mathcal{K}_2\}$. We further choose

$$\mathcal{K}_1 = (|0\rangle_K \otimes \sqrt{F_1^A} + |1\rangle_K \otimes \sqrt{F_2^A}) \otimes \sqrt{F_1^B + F_2^B}, \tag{37}$$

$$\mathcal{K}_2 = (|0\rangle_K \otimes \sqrt{F_3^A} + |1\rangle_K \otimes \sqrt{F_4^A}) \otimes \sqrt{F_3^B + F_4^B}, \tag{38}$$

so that the projector operators in Eq. (10) read

$$\begin{aligned}
\kappa_0 &= |0\rangle_K \langle 0| \otimes I_{AB}, && (39)\\
\kappa_1 &= |1\rangle_K \langle 1| \otimes I_{AB}. && (40)
\end{aligned}$$

Note that κ_l here is no longer in terms of the original systems, A and B. With all the setting listed above, Fig. 4 in Section 5.2 should be achieved through the numerics.

References

1. G.-L. Long and X.-S. Liu, Theoretically efficient high-capacity quantum-key-distribution scheme, *Phys. Rev. A* 65(3), 032302 (2002)
2. G. L. Long, F. G. Deng, C. Wang, X. H. Li, K. Wen, and W. Y. Wang, Quantum secure direct communication and deterministic secure quantum communication, *Front. Phys. China* 2(3), 251 (2007)

3. F. G. Deng, G. L. Long, and X. S. Liu, Two-step quantum direct communication protocol using the Einstein–Podolsky–Rosen pair block, *Phys. Rev. A* 68(5), 042317 (2003)
4. C. Wang, F. G. Deng, Y. S. Li, X. S. Liu, and G. L. Long, Quantum secure direct communication with highdimension quantum superdense coding, *Phys. Rev. A* 71(4), 044305 (2005)
5. F. G. Deng and G. L. Long, Secure direct communication with a quantum one-time pad, *Phys. Rev. A* 69(5), 052319 (2004)
6. F. G. Deng, X. H. Li, C. Y. Li, P. Zhou, and H. Y. Zhou, Quantum secure direct communication network with Einstein–Podolsky–Rosen pairs, *Phys. Lett. A* 359(5), 359 (2006)
7. F. G. Deng, X. H. Li, C. Y. Li, P. Zhou, and H. Y. Zhou, Economical quantum secure direct communication network with single photons, *Chin. Phys.* 16(12), 3553 (2007)
8. Z. R. Zhou, Y. B. Sheng, P. H. Niu, L. G. Yin, G. L. Long, and L. Hanzo, Measurement-device-independent quantum secure direct communication, *Sci. China Phys. Mech. Astron.* 63(3), 230362 (2020)
9. P. H. Niu, Z. R. Zhou, Z. S. Lin, Y. B. Sheng, L. G. Yin, and G. L. Long, Measurement-device-independent quantum communication without encryption, *Sci. Bull.* 63(20), 1345 (2018)
10. Z. Gao, T. Li, and Z. Li, Long-distance measurement-device-independent quantum secure direct communication, *EPL* 125(4), 40004 (2019)
11. Z. K. Zou, L. Zhou, W. Zhong, and Y. B. Sheng, Measurement-device-independent quantum secure direct communication of multiple degrees of freedom of a single photons, *EPL* 131(4), 40005 (2020)
12. X. D. Wu, L. Zhou, W. Zhong, and Y. B. Sheng, High-capacity measurement-device-independent quantum secure direct communication, *Quantum Inform. Process.* 19(4), 354 (2020)
13. L. Zhou, Y. B. Sheng, and G. L. Long, Device-independent quantum secure direct communication against collective attacks, *Sci. Bull.* 65(1), 12 (2020)
14. J. H. Shapiro, Z. Zhang, and F. N. Wong, Secure communication via quantum illumination, *Quantum Inform. Process.* 13(1), 2171 (2014)
15. D. J. Lum, J. C. Howell, M. S. Allman, T. Gerrits, V. B. Verma, S. W. Nam, C. Lupo, and S. Lloyd, Quantum enigma machine: Experimentally demonstrating quantum data locking, *Phys. Rev. A* 94(2), 022315 (2016)
16. J. H. Shapiro, D. M. Boroson, P. B. Dixon, M. E. Grein, and S. A. Hamilton, Quantum low probability of intercept, *J. Opt. Soc. Am. B* 36(3), B41 (2019)
17. J. Y. Hu, B. Yu, M. Y. Jing, L. T. Xiao, S. T. Jia, G. Q. Qin, and G. L. Long, Experimental quantum secure direct communication with single photons, *Light Sci. Appl.* 5(9), e16144 (2016)
18. W. Zhang, D. S. Ding, Y. B. Sheng, L. Zhou, B. S. Shi, and G. C. Guo, Quantum secure direct communication with quantum memory, *Phys. Rev. Lett.* 118(22), 220501 (2017)
19. F. Zhu, W. Zhang, Y. Sheng, and Y. Huang, Experimental long-distance quantum secure direct communication, *Sci. Bull.* 62(22), 1519 (2017)
20. D. Pan, Z. Lin, J. Wu, H. Zhang, Z. Sun, D. Ruan, L. Yin, and G. Long, Experimental free-space quantum secure direct communication and its security analysis, *Photon. Res.* 8(9), 1522 (2020)
21. S. Pirandola, S. L. Braunstein, S. Lloyd, and S. Mancini, Confidential direct communications: A quantum approach using continuous variables, *IEEE J. Sel. Top. Quantum Electron.* 15(6), 1570 (2009)
22. C. Liu, K. Pang, Z. Zhao, P. Liao, R. Zhang, H. Song, Y. Cao, J. Du, L. Li, H. Song, Y. Ren, G. Xie, Y. Zhao, J. Zhao, S. M. H. Rafsanjani, A. N. Willner, J. H. Shapiro, R. W. Boyd, M. Tur, and A. E. Willner, Single-end adaptive optics compensation for emulated turbulence in a bidirectional 10-Mbit/s per channel free-space quantum communication link using orbital-angular-momentum encoding, *Research* 2019, 8326701 (2019)
23. N. Killoran, T. R. Bromley, J. M. Arrazola, M. Schuld, N. Quesada, and S. Lloyd, Continuous-variable quantum neural networks, *Phys. Rev. Research* 1(3), 033063 (2019)
24. C. Q. Hu, J. Gao, L. F. Qiao, R. J. Ren, Z. Cao, Z. Q. Yan, Z. Q. Jiao, H. Tang, Z. H. Ma, and X. M. Jin, Experimental test of tracking the king problem, *Research* 2019, 3474305 (2019)
25. R. Qi, Z. Sun, Z. Lin, P. Niu, W. Hao, L. Song, Q. Huang, J. Gao, L. Yin, and G. L. Long, Implementation and security analysis of practical quantum secure direct communication, *Light Sci. Appl.* 8(1), 22 (2019)
26. H. Lu, C. H. F. Fung, X. Ma, and Q. Y. Cai, Unconditional security proof of a deterministic quantum key distribution with a two-way quantum channel, *Phys. Rev. A* 84(4), 042344 (2011)
27. C. I. Henao and R. M. Serra, Practical security analysis of two-way quantum-key-distribution protocols based on nonorthogonal states, *Phys. Rev. A* 92(5), 052317 (2015)
28. J. Wu, Z. Lin, L. Yin, and G. L. Long, Security of quantum secure direct communication based on Wyner's wiretap channel theory, *Quantum Engineering* 1(4), e26 (2019)
29. P. J. Coles, E. M. Metodiev, and N. Lütkenhaus, Numerical approach for unstructured quantum key distribution, *Nat. Commun.* 7(1), 11712 (2016)
30. A. Winick, N. Lütkenhaus, and P. J. Coles, Reliable numerical key rates for quantum key distribution, *Quantum* 2, 77 (2018)
31. L. M. Liang, S. H. Sun, M. S. Jiang, and C. Y. Li, Security analysis on some experimental quantum key distribution systems with imperfect optical and electrical devices, *Front. Phys.* 9(5), 613 (2014)
32. Z. Cao, Z. Zhang, H. K. Lo, and X. Ma, Discrete-phaserandomized coherent state source and its application in quantum key distribution, *New J. Phys.* 17(5), 053014 (2015)
33. C. H. Bennett, G. Brassard, and N. D. Mermin, Quantum cryptography without Bell's theorem, *Phys. Rev. Lett.* 68(5), 557 (1992)

34. A. D. Wyner, The wire-tap channel, *Bell Sys. Tech. J.* 54(8), 1355 (1975)

35. G. Ribordy, J. Gautier, N. Gisin, O. Guinnard, and H. Zbinden, Automated "plug & play" quantum key distribution, *Electron. Lett.* 34(22), 2116 (1998)

36. P. J. Coles, L. Yu, V. Gheorghiu, and R. B. Griffiths, Information-theoretic treatment of tripartite systems and quantum channels, *Phys. Rev. A* 83(6), 062338 (2011)

37. P. J. Coles, Unification of different views of decoherence and discord, *Phys. Rev. A* 85(4), 042103 (2012)

38. S. Watanabe, R. Matsumoto, and T. Uyematsu, Tomography increases key rates of quantum-key-distribution protocols, *Phys. Rev. A* 78(4), 042316 (2008)

39. E. Bolduc, G. C. Knee, E. M. Gauger, and J. Leach, Projected gradient descent algorithms for quantum state tomography, *npj Quantum Inf.* 3(1), 1 (2017)

40. I. Sutskever, J. Martens, G. Dahl, and G. Hinton, On the importance of initialization and momentum in deep learning, in: International conference on machine learning, 2013, p. 1139

41. M. Jaggi, Revisiting Frank-Wolfe: Projection-free sparse convex optimization, in: Proceedings of the 30th international conference on machine learning, CONF, 2013, p. 427

42. L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, Hacking commercial quantum cryptography systems by tailored bright illumination, *Nat. Photonics* 4(10), 686 (2010)

43. S. Sajeed, P. Chaiwongkhot, J. P. Bourgoin, T. Jennewein, N. Lütkenhaus, and V. Makarov, Security loophole in free-space quantum key distribution due to spatial-mode detector-efficiency mismatch, *Phys. Rev. A* 91(6), 062301 (2015)

44. J. Lin, T. Upadhyaya, and N. Lütkenhaus, Asymptotic security analysis of discrete-modulated continuous variable quantum key distribution, *Phys. Rev. X* 9(4), 041064 (2019)