Security of Distributed-Phase-Reference Quantum Key Distribution

MORODER, Tobias, et al.

Abstract
Distributed-phase-reference quantum key distribution stands out for its easy implementation with present day technology. For many years, a full security proof of these schemes in a realistic setting has been elusive. We solve this long-standing problem and present a generic method to prove the security of such protocols against general attacks. To illustrate our result, we provide lower bounds on the key generation rate of a variant of the coherent-one-way quantum key distribution protocol. In contrast to standard predictions, it appears to scale quadratically with the system transmittance.

Reference

DOI : 10.1103/PhysRevLett.109.260501
Security of Distributed-Phase-Reference Quantum Key Distribution

Tobias Moroder,1 Marcos Curty,2 Charles Ci Wen Lim,3 Le Phuc Thinh,4 Hugo Zbinden,3 and Nicolas Gisin3
1Naturwissenschaftlich-Technische Fakultät, Universität Siegen, Walter-Flex-Straße 3, D-57068 Siegen, Germany
2EI Telecomunicación, Department of Signal Theory and Communications, University of Vigo, E-36310 Vigo, Spain
3Group of Applied Physics, University of Geneva, CH-1211 Geneva, Switzerland
4Centre for Quantum Technologies, National University of Singapore, 3 Science Drive 2, Singapore 117543, Singapore

Distributed-phase-reference quantum key distribution stands out for its easy implementation with present day technology. For many years, a full security proof of these schemes in a realistic setting has been elusive. We solve this long-standing problem and present a generic method to prove the security of such protocols against general attacks. To illustrate our result, we provide lower bounds on the key generation rate of a variant of the coherent-one-way quantum key distribution protocol. In contrast to standard predictions, it appears to scale quadratically with the system transmittance.

DOI: 10.1103/PhysRevLett.109.260501

PACS numbers: 03.67.Dd, 03.67.Hk, 03.67.Mn

Introduction.—Quantum key distribution (QKD) is on the verge of becoming a standard tool for secure communications [1]. In its original proposal, QKD is based on the transmission of single photons. However, since true single photon sources are not available yet most experimental prototypes and all current commercial products of QKD use weak laser pulses. A main drawback of these systems is that some signals contain more than one photon prepared in the same quantum state. This fact severely limits the distances that can be achieved by these techniques due to the photon number splitting attack [2].

To enhance the performance of practical QKD systems, several approaches have been proposed. One solution is to send a strong reference pulse together with the quantum signals [3]. A second approach is based on the decoy state method, where the transmitter sends states with different intensities [4]. Both schemes provide a secret key generation rate that scales linearly with the system transmittance [3,4]. A third alternative is to use distributed-phase-reference (DPR) QKD protocols. They differ from standard QKD schemes in that the receiver now performs joint measurements on subsequent signals, often given in the form of coherence measurements [5,6]. This approach includes the differential-phase-shift [5] and the coherent-one-way (COW) [6] protocol. In the former, the sender prepares coherent states of equal intensity but modulates their phases; in the COW protocol all pulses share a common phase but their intensities vary. A complete security proof of DPR-QKD in a realistic setting has been missing for many years. So far, security has only been proven against restricted types of attacks [7–9] or assuming single photon sources [10].

In this letter, we present a generic method to prove security of practical DPR-QKD against general attacks. This solves a long-standing open question in the field of quantum communications [1]. We illustrate our result by providing nontrivial lower bounds for a variant of the COW protocol [11], which maintains all the practical advantages.

Our analysis suggests that practical DPR-QKD might not be as robust against imperfections as initially foreseen; i.e., its key rate appears to scale quadratically with the system transmittance.

Security discussion.—The challenge in DPR-QKD is to prove security against general, also termed coherent, attacks. Usually such attacks are known to be of no advantage to the eavesdropper (Eve) in comparison to collective attacks by virtue of the de Finetti theorem [12]. This theorem applies, for instance, when the underlying quantum state shared by the legitimate users (Alice and Bob) is permutationally invariant. In standard QKD this is typically ensured by performing simultaneous random permutations on the classical measurement results. DPR-QKD defines, however, a fixed ordering of the signals by its coherence measurements and, therefore, it is not possible to permute the classical outcomes without destroying vital information. However, such a predicament can be circumvented by grouping the entire signal stream into blocks. More specifically, consider Alice and Bob grouping their signals into subsequent blocks of size $m$ with $m$ being optimized for the expected behavior. When permuting these blocks one preserves the coherence information within them while the information between the blocks is destroyed. Still this is enough to apply the de Finetti argument on the level of blocks. As a result, the state shared by Alice and Bob after distributing a large number $mN$ of signals satisfies $\rho_{AB}^{mN} = \rho_{AB}^{\otimes N}$ and security against collective attacks on these signal blocks implies security against coherent attacks in the original setting.

Suppose that the state shared by all parties after transmitting a $m$ block signal is $\rho_{\text{AB}}^{mB}$. Let us first consider the effect of public announcements by Alice and Bob. This announcement, labeled as $\nu$, tells them when to discard all measurement results from the block due to an inconclusive event, or which parts of the acquired data become the sifted raw key in case of a conclusive event. On the level of quantum states this is described by suitable maps $\Lambda_\nu^A \otimes \Lambda_\nu^B$. 

\[ \Lambda_\nu^A \otimes \Lambda_\nu^B \]
Given an announcement $v$ that happens with probability $p(v)$, the three parties share the state $\sigma_{ABE,v}^m$ determined by

$$\Lambda_+^A \otimes \Lambda_+^B (\rho_{ABE}^m(v)) = \rho_{ABE}^m(v),$$

with $\Lambda_A^A$, $\Lambda_B^B$ being respective conditional output spaces.

For each announcement $v$, one can use the one-way classical post-processing key rate formula [13]. If system $\bar{A}$ denotes a qubit and Alice’s raw key is obtained by projecting this system onto $|0\rangle_{\bar{A}}$, $|1\rangle_{\bar{A}}$, then a lower bound on the secret key rate is given by $1-h_2(e_{\bar{A}})-h_2(\delta_{\bar{A}})$. Here $h_2$ represents the binary entropy, $e_\bar{A}$ is the symmetrized bit error between the key measurements of Alice and Bob, and $\delta_{\bar{A}}$ denotes the corresponding error, typically called phase error, when Alice performs a dichotomic measurement in a mutually unbiased basis and Bob in his other setting. This last parameter is used to upper bound Eve’s knowledge on the sifted key generated by Alice. Note that $\delta_{\bar{A}}$ does not need to be measured directly, it only needs to be estimated.

To consider that the output system $\bar{A}$ is a qubit implies that Alice can, at best, distill one secret bit per block. Nevertheless, this restriction should not have a significant impact on the key rate in a long distance regime since Bob observes, if any, most often only one single conclusive event per $m$ arriving signals due to the high losses in the channel (given that $m$ is not too big).

Instead of estimating separate phase errors $\delta_{\bar{A}}$, it is often easier to combine all conclusive announcements $v \in V_c$ into an averaged version. Let $G = \sum_{v \in V_c} p(v) \leq 1$ denote the total sifted key gain. Then, we have that the secret key rate per block $R_m$ is bounded by [14]

$$R_m \geq \inf_{\rho_{AB}^m} \sum_{v \in V_c} p(v)[1 - h_2(e_v) - h_2(\delta_v)] \quad (1)$$

$$\geq \inf_{\rho_{AB}^m} G[1 - h_2(\bar{e}_c) - h_2(\bar{\delta}/G)]$$

$$\geq G[1 - h_2(\bar{e}_c) - h_2(\bar{\delta}^{\text{max}}/G)]. \quad (2)$$

Here one uses concavity of $h_2$ to lower bound $R_m$ by the averaged (conditional) error rates $\bar{e}_c = \sum_{v \in V_c} p(v)e_{\bar{A}}/G$ and $\bar{\delta} = \sum_{v \in V_c} p(v)\delta_v$. The last step takes into account that $\bar{e}_c$ and $G$ are observed quantities and that the optimization is attained at the largest phase error $\bar{\delta}^{\text{max}}$ compatible with the obtained data since $h_2$ increases in $[0, \frac{1}{2}]$.

**Phase error estimation.**—The main difficulty of computing Eq. (2) is to upper bound the average phase error $\bar{\delta}$. This parameter can be expressed as an expectation value on the original bipartite state $\rho_{ABE}^m = \text{tr}_E(\rho_{ABE}^m)$, using adjoint maps

$$\bar{\delta} = \sum_{v \in V_c} p(v)\text{tr}(\sigma_{ABE}^m F_{\delta_v}) = \sum_{v \in V_c} \text{tr}[\Lambda_v^A \otimes \Lambda_v^B (\rho_{AB}^m) F_{\delta_v}]$$

$$= \text{tr}[\rho_{AB}^m \sum_{v \in V_c} \Lambda_v^A \otimes \Lambda_v^B (F_{\delta_v})] = \text{tr}(\rho_{AB}^m F_{\delta}). \quad (3)$$

Here $F_{\delta}$ denote the corresponding phase error operators on the state $\sigma_{ABE,v}^m$. Partial knowledge of Alice and Bob about the state $\rho_{AB}^m$ can be parsed as known expectation values $k_i = \text{tr}(\rho_{AB}^m K_i)$ for certain operators $K_i$. This means that the search for the maximum phase error $\bar{\delta}^{\text{max}}$ can be cast into a semidefinite program [15],

$$\text{max} \quad \text{tr}(\rho_{AB}^m F_{\delta})$$

$$\text{s.t.} \quad \rho_{AB}^m \geq 0, \quad \text{tr}(\rho_{AB}^m K_i) = k_i \quad \forall i. \quad (4)$$

Such special convex optimization problems can be solved efficiently using standard tools to obtain the exact optimum, even for large dimensions.

**Available information and its description.**—Let us be more precise about which expectation values $k_i$ are known in a prepare and measure scheme, where Alice sends potentially mixed states $\rho_i^A$ with a *priori* probability $p(i)$. This state preparation can be formulated in an entanglement-based version as follows [16]: Alice first creates a source state $|\Psi^m\rangle_{AB} = \sum_i \sqrt{p(i)} |i\rangle_A |\rho_i^A\rangle_{B,E}$, where $|\rho_i^A\rangle_{B,E}$ denote purifications of the signal states $\rho_i^A$ to an inaccessible shield system $A_s$. Afterwards, she measures her bit system $A_b$ in the standard basis, thereby, producing the correct signal states at site $B$ which are sent to Bob. Eve transforms the overall source state to the final tripartite state $\rho_{ABE}^m$ with $A = A_b A_s$. On the receiving side, Bob performs a measurement modeled by $B_k$. As a result, both Alice and Bob observe the expectation values of $i |i\rangle_A \otimes 1_B \otimes B_k$. Moreover, since Eve is restricted to interact only with Bob’s system, the reduced density matrix $\rho_{AB}^m = \text{tr}_{BE}(\rho_{ABE}^m)$ is fixed and given by the source state. This information can be added by including expectation values of $T_k \otimes 1_B$, where $T_k$ denotes a tomographic complete operator set on $A$. Both sets of observables constitute the previously denoted operators $K_i$.

The signal states and performed measurements in practical DWR-QKD are described by operators on an infinite dimensional Fock space of several modes. In order to apply the de Finetti theorem [12] and to numerically obtain an upper bound using Eq. (4), it is necessary to formulate this problem in a manageable, finite-dimensional form. Clearly, system $A_b$ is finite. For Bob’s measurements, one can employ the squash model argument [17]. Here the real measurement is notionally decomposed into a two-step procedure by first applying a map that transforms any incoming signal to a finite-dimensional output state on which a specified target measurement $B_k$ is performed. Since this map can be even given to Eve, its output state only lowers the key generation capabilities of Alice and Bob, and one readily works in finite dimensions. For our simulations we assume that Bob has inefficient photon number resolving detectors with state independent dark counts. Furthermore, we restrict our analysis to the single photon events within a block. In this case the map outputs either a single photon, measured with the perfect detection scheme, or an auxiliary state that triggers all inconclusive events, see Ref. [18] for details.

For the shield system $A_s$ one uses only partial information of the reduced state, a technique known as tagging [19]. In the

---

*PRL 109, 260501 (2012) PHYSICAL REVIEW LETTERS week ending 28 DECEMBER 2012*
case of phase randomized signal blocks, an example that we consider later, a purification stores the total number of photons of the block in the shield system $|n⟩_A$. Using tomography on the subspace spanned by all states with $n = 1, \ldots, n_{\text{cut}}$, together with an ancilla $|N⟩_A$, for all other cases, the shield system can effectively be described in finite dimensions.

Description of the protocol.—To illustrate our results we analyze the security of a variant of the COW protocol [11]. The basic setup is shown in Fig. 1. Alice uses a laser, followed by an intensity modulator (IM), to prepare a sequence of coherent states $|0⟩|α⟩$ and $|α⟩|0⟩$. On the receiving side, Bob employs an active optical switch to distribute each pair of incoming pulses into the data or the monitoring line. The data line measures the arrival time of the pulses in detector $D_d$ and creates the raw key. Whenever Bob sees a "click" in this detector in time instance $i$, he decides at random whether to publicly announce a detection event in time instances $i$ and $i+2$ or $i$ and $i-2$. The first case is associated with a bit value 0; the second case corresponds to a bit value 1. If the state sent by Alice in these time instances is $|0⟩|α⟩$ ($|α⟩|0⟩$), then she assigns to it a bit value 0 (1) and tells Bob to keep his result. Otherwise, the result is discarded. The monitoring line checks coherence between subsequent even and odd pulses by interfering them on a 50:50 beam splitter and measuring the outputs in detectors $D_+$ and $D_-$. As in the original COW [6] these coherence measurements check for eavesdropping, though now "decoy signals" no longer need to be included actively, providing a certain practical advantage of this modified version.

In the security analysis we assume that Alice and Bob do not use coherence information between consecutive blocks and that the sifted key is created only from signals within the same block that is guaranteed by a slight change in Bob’s public announcement. One can reorder the $2m$ possible detection time slots of a given block to form a closed chain with the first and last time instances connected. Now, if Bob observes a "click" in the first time slot, he announces a detection event in time instances one and three or one and $2m-1$ with equal probability and similarly for the other cases.

Simulation.—For simulation purposes, we consider that Bob’s detectors are identical with a dark count rate of $10^{-7}$. The channel model includes an intrinsic error rate of 1% in the data line together with an additional misalignment in the monitoring line that reduces the visibility to 99% [18]. We study two different scenarios: (a) the case where all different $m$-signals blocks share the same phase, and (b) the scenario where each block is phase randomized. The resulting lower bounds on the secret key rate per pulse, i.e., $R_m/(2m)$, are illustrated in Fig. 2. For comparison, this figure also includes a lower bound on the secret key rate for

![Figure 1](https://example.com/figure1.png)

**FIG. 1.** Schematic description of a COW protocol [11] with an active measurement choice. Bob reads the raw key in detector $D_d$. Moreover, he uses an optical switch to send some pairs of consecutive pulses to a monitoring line that examines the coherence between even and odd pulses. The lower left corner shows an example of the public announcement.

![Figure 2](https://example.com/figure2.png)

**FIG. 2 (color online).** Lower bound on the secret key rate given by Eq. (2) per pulse on a logarithmic scale (base 10) vs the total system loss in dB for the COW protocol illustrated in Fig. 1 using signal blocks carrying $m$ bits of information (i.e., $2m$ optical pulses) in the security proof. The upper figure corresponds to the case where all blocks of signals share a common phase, while in the lower figure each block is phase randomized. For comparison, we include a lower bound on the secret key rate for a coherent-state version of the BB84 protocol [20] with and without phase randomization [19,21]. We consider three main errors: an intrinsic error rate of 1% in the data line, an additional misalignment in the monitoring line reducing the visibility to 99%, and a dark count rate of $10^{-7}$ for each detector. Moreover, in the lower figure we assume $n_{\text{cut}} = 2$. 

PRL 109, 260501 (2012)
a coherent-state version of the Bennett-Brassard (BB84) protocol [20] with and without phase randomization [19,21]. For a given total system loss, i.e., including the losses in the channel and in Bob’s detection apparatus, we optimize the lower bound over the respective signal strength $\alpha$ of Alice’s source, which is of order 0.1. As expected, we find that case (b) performs better than that where all blocks share a common phase, since the signal states are less distinguishable for an eavesdropper without a global phase. We obtain that the tolerable system loss for the COW protocol is, respectively, $= 19$ dB (a), and $= 22$ dB (b). The bit error and visibility at these cutoff points are, respectively, $= 3\%$ and $= 96\%$ (a), and $= 5\%$ and $= 93\%$ (b). Let us emphasize that the lower bound with $m = 2$ even holds for threshold detectors [18].

Our simulations reveal that a main limiting factor in DPR-QKD seems to be the dark count rate of Bob’s detectors. For given experimental parameters, there is an optimal finite block size that allows a maximum tolerable total system loss. If one increases the block size further this does not translate into an improved lower bound or distance. This is due to the fact that, in the high loss regime, large-sized blocks suffer from a higher dark count probability per block than smaller-sized blocks, and this reduces the achievable secret key rate. A similar effect was observed in the security analysis for the differential-phase-shift protocol with true single photon sources [10]. For a dark count rate per pulse of $10^{-7}$, the optimal block size in the COW scheme turns out to be $m = 3$, i.e., 6 optical pulses. Also, this figure shows that a coherent-state version of the BB84 protocol without decoy states can deliver higher key rates per signal than the analyzed COW protocol assuming the same channel. The reason for this might be threefold: (1) the small optimal block size in the COW scheme; (2) considering blocks, it can be shown that certain multiphoton pulses are completely insecure; and, (3) most importantly, while in the BB84 the phase error is measured directly, in the COW protocol it has to be estimated.

Possible improvements.—To further improve the lower bounds shown in Fig. 2 there are several alternatives. Since a main limitation seems to come from dark counts, one may consider security in the fully calibrated device scenario where these errors are not attributed to Eve. As a quantitative bound on the performance of this scenario we investigated the case of a zero dark count rate, in which all bounds shown in Fig. 2 shift by about 3 dB, though the difference between the COW and the BB84 protocol remains. Additionally, one can evaluate different announcements in a similar spirit like the Scarani-Acín-Ribordy-Gisin protocol [22]. We considered different declarations, but unfortunately none of them enhanced the resulting rate [18]. Another possibility is to include, for instance, an extra monitoring line on Bob’s side to additionally check the coherence between subsequent pulses. The state distribution part of this protocol is then very similar to the original COW scheme [6] with an additional decoy signal composed by two vacuum pulses [9]. This hardware change improves the maximum tolerable system loss by about 1 dB.

Another hardware change might be to include additional phase differences in the signal stream, such that the signals states get closer to the one used in a BB84 protocol. Finally, one may ask whether different security techniques might provide better lower bounds. For instance, one could consider more valid detection events per block. This needs, however, much larger block sizes such that one obtains a reasonable fraction of two or more click events in the long distance limit. Another alternative would be to bound the rate by the individual phase errors, i.e., directly using Eq. (1). This could give a benefit if, for example, bits at the boundary are much closer to not infer by Eve than bit values originating from events well inside the block. Clearly, another option would be to abandon the block idea. However, even in this case Eve could always attack the signals block-wise. Though a coherence measurement across blocks would then reveal the eavesdropper, any coherence measurement within would still be fine. Hence, considering only an average visibility, this effect will become less and less important. All these alternatives definitely deserve further investigations, but we do not expect a dramatic improvement.

Conclusion.—We have presented a generic method to prove security of practical DPR-QKD against general attacks. With the explicit example of a variant of the COW protocol, we have shown that the performance of these schemes seems to be less robust against practical imperfections than originally expected.

We would like to thank H.-K. Lo, N. Lütkenhaus, V. Scarani, L. Sheridan, and N. Walenta for stimulating discussions about topic and technicalities, and L.M. Eriksson for comments on the presentation of the paper. T.M., M.C., and L.P.T. especially thank the Group of Applied Physics, University of Geneva, for hospitality and support during their stay at this institution, where parts of this research have been conducted. This work has been supported by the EU (Marie Curie CIG 293993/ENFOQI), the BMBF (Chist-Era Project QUASAR), the National Research Foundation and the Ministry of Education, Singapore, the National Centre of Competence in Research QSIT, the Swiss NanoTera project QCRIPT and the FP7 Marie-Curie IAAP QCERT project.

Note added.—A similar proof technique has recently been developed for a phase-randomized block version of the differential-phase-shift protocol [23], providing a likewise key rate behavior for realistic channel models.


