Robust Polarization-Based Quantum Key Distribution over a Collective-Noise Channel

J.-C. Boileau,[1] D. Gottesman,[2] R. Laflamme,[1,2] D. Poulin,[1,2] and R.W. Spekkens[2]

[1]*Institute for Quantum Computing, University of Waterloo, Waterloo, ON, N2L 3G1, Canada*
[2]*Perimeter Institute for Theoretical Physics, 35 King Street North, Waterloo, ON, N2J 2W9, Canada*

(Received 3 July 2003; published 8 January 2004)

We present two polarization-based protocols for quantum key distribution. The protocols encode key bits in noiseless subspaces or subsystems and so can function over a quantum channel subjected to an arbitrary degree of collective noise, as occurs, for instance, due to rotation of polarizations in an optical fiber. These protocols can be implemented using only entangled photon-pair sources, single-photon rotations, and single-photon detectors. Thus, our proposals offer practical and realistic alternatives to existing schemes for quantum key distribution over optical fibers without resorting to interferometry or two-way quantum communication, thereby circumventing, respectively, the need for high precision timing and the threat of Trojan horse attacks.

DOI: 10.1103/PhysRevLett.92.017901 PACS numbers: 03.67.Pp, 03.67.Dd, 42.65.Lm

Quantum key distribution (QKD), such as the BB84 protocol proposed by Bennett and Brassard in 1984, allows two parties (Alice and Bob) to generate an arbitrarily long random secret key, provided that they initially share a short secret key and that they have access to a quantum channel [1]. As opposed to classical key distribution, the secrecy of the generated key does not rely on computational assumptions but simply on the laws of physics: as long as quantum mechanics holds, the information available to an eavesdropper (Eve) can be made arbitrarily small.

Photons are obvious candidates for mediators of quantum information since they are fast, cheap, and interact weakly with the environment. Both free air and optical fiber based QKD have been realized experimentally; see [2,3] for reviews. Any experimental implementation of QKD naturally has to deal with the issue of noise in the quantum channel, which substantially complicates the security of QKD, as Eve may attempt to disguise her eavesdropping as noise from another source. Standard security proofs deal with channel noise, including photon loss, and show that Eve acquires essentially no information provided the noise rate is not too high. Higher noise rates mandate lower key generation rates, and once it becomes too large, secure key generation is impossible.

Building a viable quantum cryptographic system therefore depends on ensuring that the noise rate is low. The degree of freedom used to encode the information can be the polarization of the photon, its phase, or some combination of both. Purely phase-based schemes have been realized experimentally [4] but require complex interferometric setups, high precision timing, and stable low temperatures. Interferometry becomes even more challenging with multiphoton states because of the difficulty of keeping phase coherence between the photons. A scheme which escapes some of these limitations using a clever encoding of key bits was proposed recently [5].

Polarization-based schemes also come with a disadvantage as optical fibers rotate polarizations of transmitted photons, and the degree of rotation fluctuates over time. If left untreated, this would result in an unacceptably high error rate. A number of proposals have been made to handle this source of errors; we present a new solution which is in some ways superior. Singlet states $|\Psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$, where $\{|0\rangle, |1\rangle\}$ is any basis of the qubit Hilbert space, have the property that they are unchanged under equal rotations on both qubits; this is the defining property of a noiseless subspace. (If one's qubits are the polarization degrees of freedom of single photons, as we assume here, then $|0\rangle$ and $|1\rangle$ can be taken to denote, for instance, the vertical and horizontal polarization states.) We present two protocols that take advantage of this property to encode key bits in four- or three-photon states. These states should be experimentally realizable and form simple examples of a noiseless subspace or subsystem, respectively (also called a decoherence-free subspace and subsystem) [6–8].

Free-space QKD is largely immune to the problem of polarization rotation: the coupling between the photons and the molecules in the atmosphere can be absorbed in a dielectric constant to very good approximation. Unfortunately, the same cannot be said about optical fiber. Rather, the dielectric constant acquires a spatial and temporal dependence, yielding an overall time dependent unitary transformation of the polarization state of a single photon, $U(t)$, as the net effect of the fiber. This varies on the time scale of thermal and mechanical fluctuations of the fiber, the shortest of which we refer to as τ_{fluc}. If the time delay between the photons is small compared to τ_{fluc}, the effect of this noise on the state of N photons is well approximated by

$$\rho_N \rightarrow [U(t)]^{\otimes N} \rho_N [U(t)^\dagger]^{\otimes N}, \tag{1}$$

where t now denotes the time of transmission. This is known as the unitary collective noise model [6].

There are several ways to deal with collective noise. The most obvious way is to continuously estimate the transformation $U(t)$ and systematically compensate for it.

However, this requires an interruption of the transmission and, if the fluctuations become too rapid, the communication channel becomes useless. A second possibility—a phase-polarization hybrid which has been used successfully to realize QKD over 67 km [9]—uses the Faraday orthoconjugation effect [10] to autocompensate the effect of $U(t)$. Roughly speaking, if the transformation on the photon during its transmission from Bob to Alice is described by $U(t)$, it can be $U(t)^{-1}$ when the photon is transmitted back from Alice to Bob, yielding no net transformation overall. The quantum information can be encoded by an extra phase transformation performed by Alice before returning the photon to Bob. Obviously, this technique works only if $U(t)$ is roughly constant throughout the transmission of the photon; this sets an upper limit of $c\tau_{\mathrm{fluc}}$ to the distance over which QKD can be implemented with this scheme. (However, with today's technology, photon loss is a much more serious limitation to the distance over which QKD can be achieved.)

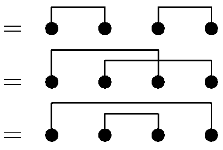
Although such two-way quantum communication can eliminate collective noise, it allows for new attacks not possible against BB84. Since Alice receives and emits signals, it is possible for Eve to probe her laboratory—a technique known as the Trojan horse attack. There are many ways in which she can do this. She could add a weak signal to the channel at a slightly different frequency and recover some information about Alice's phase transformation by subsequently filtering the output signal. Eve could also try to entangle an ancilla system with the signal before it enters Alice's laboratory and perform a joint measurement on the two after Alice has retransmitted the signal. She could also intercept the signal, send a different signal to Alice, and thereafter measure the output to estimate the applied phase transformation, etc. Technical solutions for some of these attacks have been proposed. However, Eve has an enormous variety of attacks available, and to prove true information-theoretic security, one must assume that Eve has arbitrary technological power; e.g., she can outperform the best frequency filtering available to Alice and Bob. Because of its inherent use of two-way quantum communication, the protocol is formally quite different from the standard BB84 protocol and proving its security may be quite difficult. (Note, however, that QKD must make use of two-way classical communication between Alice and Bob, and this presents no particular barrier to security proofs. Indeed, taking full advantage of two-way classical communication results in a protocol with substantially greater tolerance for noise [11].)

The schemes we propose here are purely polarization based and cope with collective noise without resorting to two-way quantum communication. In the first protocol, the quantum information is encoded in a noiseless subspace, while in the second protocol it is encoded on a noiseless subsystem. [Such encodings also obviate the need for Alice and Bob to share a reference frame (such as, for instance, a known relative alignment of their linear polarizers), as has been pointed out in the context of quantum communication in Ref. [12].] A noiseless subspace is invariant under the action of the collective noise operation (here $U^{\otimes N}$). Any state within it is therefore unaffected (modulo a global unphysical phase) by the noise. When such a subspace does not exist, it may still be possible to find a set of density operators which are invariant under the effect of noise. These density operators instead form a noiseless subsystem on which pure states can be encoded.

The protocols we present use singlet states as building blocks. Information is encoded in the pairing of the photons; the various ways of organizing three or more photons into pairs provide us with different states with which to encode information. The photons must be distinguishable if different pairings are to correspond to different physical states: they need to be labeled in some way. Physically, this means that the photons must differ with respect to some degree of freedom. Here the photons are assumed to differ in their time of arrival; they are spatially separated in the optical fiber. Furthermore, each bit is encoded on multiphoton states which must also be distinguished even in the presence of noise. Therefore, the multiplets of photons must be spatially separated by a distance greater than the separation between individual photons inside a multiplet. The fluctuation time τ_{fluc} needs to be large only with respect to the difference in the arrival times of the first and the last photon of a multiplet.

It is crucial that information about the pairing resides only in the polarization state of the photon. For example, variations in the frequency of the photons can reveal pairing information: the frequencies of the two photons in each singlet must add up to the frequency of the pump, but the frequencies of photons in different singlets need not match. By measuring the photons' energy, Eve can learn about how they are paired without affecting their polarization. This energy signature can be eliminated by filtering the photons before they leave Alice's laboratory. Indeed, if the bandwidth of the filter is smaller than the bandwidth of the pump laser, almost no information about the pairing can be recovered by Eve. Frequency filtering also decreases decoherence due to polarization mode dispersion in the fiber [2]. Similarly, we must wash out the phase relation between photon pairs. That is, the information must be encoded only on the relative order of the photons, not in their absolute time of arrival. This can be achieved by choosing the time delay between the photons in each multiplet at random from a certain range.

We now present our two protocols: the first one encodes the quantum information on four-photon states, while the second only requires three-photon states. We do not prove their security here, but rather point only to their similarities with a protocol proposed by Bennett in 1992 (B92) [13] which is known to be secure [14]. We hope to provide a complete security proof in a later paper. The first protocol requires the definition of three normalized states of a photon quartet:



$$\begin{aligned}|\psi_1\rangle &= \qquad = \tfrac{1}{\sqrt{2}}(|a\rangle - |b\rangle)\\ |\psi_2\rangle &= \qquad = \tfrac{1}{\sqrt{2}}(|c\rangle - |b\rangle)\\ |\psi_3\rangle &= \qquad = \tfrac{1}{\sqrt{2}}(|a\rangle - |c\rangle).\end{aligned} \tag{2}$$

All these states correspond to pairs of single states: in $|\psi_1\rangle$, photons one and two form a singlet state and so do photons three and four. The two other states correspond to the two other ways of pairing four photons as illustrated by the diagrams. The states are invariant under uniform rotations, so, in any basis, these states can be decomposed into the superpositions noted above, where $|a\rangle = (|0101\rangle + |1010\rangle)/\sqrt{2}$, $|b\rangle = (|0110\rangle + |1001\rangle)/\sqrt{2}$, and $|c\rangle = (|0011\rangle + |1100\rangle)/\sqrt{2}$.

It is straightforward to verify that $|\langle\psi_i \mid \psi_j\rangle| = 1/2$ for $i \neq j$. It is therefore impossible to reliably distinguish any pair of these states, but it is possible to make a measurement that provides some information. Measuring the polarization of all four photons allows Bob to distinguish states $|a\rangle$, $|b\rangle$, and $|c\rangle$. Therefore, if Alice restricts her transmission to one of a pair of states, Bob can tell which of the two states she sent 50% of the time. For example, suppose Alice transmits one of the pair $\{\psi_1, \psi_2\}$. When Bob measures either "0101" or "1010," he can conclude that she sent $|\psi_1\rangle$. When he gets either "1100" or "0011," he concludes she sent $|\psi_2\rangle$. Given any other outcome, Bob cannot deduce with certainty which state she sent. We now present the protocol.

Protocol 1.—Included are the following steps:

(1) Alice chooses a random $(4 + \delta)n$ bit string X and a random $(4 + \delta)n$ trit string B.

(2) Alice encodes each bit $\{0, 1\}$ of X according to $\{\psi_1, \psi_2\}$ if the corresponding trit of B is 0; $\{\psi_2, \psi_3\}$ if B is 1; or $\{\psi_3, \psi_1\}$ if B is 2.

(3) Alice sends the $(4 + \delta)n$ quartets of photons to Bob.

(4) Bob receives the photons and announces this fact. For each of the $(4 + \delta)n$ photon quartets, he randomly chooses between the rectilinear or the diagonal polarization basis. He then measures each of the four photons of each quartet according to this choice of basis.

(5) Alice announces B. Given this information, and using the procedure described above, Bob can determine, for each quartet, whether or not his measurement was conclusive, and if conclusive, the value of the encoded bit.

(6) Alice and Bob discard all bits where Bob's measurement was inconclusive. With high probability, there are at least $2n$ bits left, which they keep. Otherwise, they abort the protocol.

(7) Alice selects a random subset of n bits and tells Bob which bits were selected.

(8) Alice and Bob announce and compare the value of the n selected bits to estimate Eve's interference; if more than an acceptable number of errors are found, they abort the protocol.

(9) Alice and Bob perform information reconciliation and privacy amplification on the remaining n bits.

In step (4) the choice of basis does not affect the measurement outcome of Bob: this is, in fact, the main property of the encoding. Nevertheless, it is crucial that Eve does not know in which basis the measurement is performed. If she knew, she could measure in the same basis as Bob and would know everything Bob knew. Since she does not know, she will frequently measure in a different basis than Bob and therefore introduce errors that will reveal her presence.

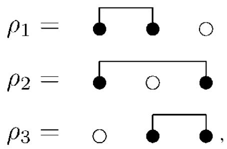
As the protocol is written, in step (6) Alice and Bob discard any bits for which Bob's measurement is inconclusive. Nevertheless, an inconclusive result could still be useful. Indeed, any measurement result whose weight differs from two, e.g., "1011," indicates that Eve has tampered with the communication. This provides Alice and Bob with some extra data to estimate Eve's interference: only allowed code words should be observed by Bob.

If steps (4) and (5) are inverted, which could only provide Eve with more information, we get a protocol quite similar to B92. Alice encodes the bit in two preselected nonorthogonal states which she sends down the quantum channel. Bob then performs a von Neumann measurement chosen at random from a certain set: this is also required in B92. Nevertheless, there are certain differences in the nature of these measurements which must be studied carefully to arrive at a complete security proof. We are currently working on these issues. The B92 protocol is not secure if the transmission rate is below 1/2. Eve can replace the noisy channel by a perfect channel and measure Alice's output in such a way that she achieves a conclusive discrimination with probability 1/2, in which case she knows the state and can send it to Bob. In the case of an inconclusive result, she does not send anything. From Alice and Bob's point of view, this would be indistinguishable from the natural noise. By delaying the announcement of B, our proposal escapes this limitation.

The simplicity of the measurement—single photon polarization—is a clear advantage of this protocol. (The possibility of discriminating between states that are invariant under collective noise, without having recourse to collective measurements, has also been noted in Ref. [15].) Furthermore, proof of principle for photon-based noiseless subspace has been realized [16] and the specific states required by our protocols have already been produced by several groups [17,18]. Two singlet states can be produced in a short time interval via parametric down-conversion by sending a femtosecond pump laser pulse back and forth across a crystal (using a mirror). Since the photons are emitted in different directions, the EPR pairs can be clearly distinguished. The achieved production rate are relative low (a few hertz), but this technique is still in its infancy. Optical delays and switches can be used to create any of the three states of Eq. (2).

At first glance, it appears there are two copies of the information in this encoding. For instance, if Alice announces that the bit is encoded as $\{\psi_1, \psi_2\}$, the value of the first two measurement outcomes is enough to sometimes deduce the value of the encoded bit: it is necessarily 1 if the outcomes are the same. The same holds for the measurement outcomes on the last two photons. Nevertheless, this redundancy is intrinsic to our quantum encoding scheme and does not provide Eve with any extra information. The second protocol we present exploits this redundancy to reduce the size of the encoding.

Protocol 2.—This is a slight modification of Protocol 1. In step (3), instead of sending the entire state to Bob, Alice randomly discards one photon from each quartet and sends the remaining three. In step (5), Alice should also announce which photon she has discarded. Therefore, the three pure states of Eq. (2) are replaced by the three mixed states



(3)

where the "○" denotes the maximally mixed state. These states are obviously invariant under collective noise. Furthermore, any pair can be distinguished with a finite probability, just as with the states in Protocol 1. This follows from the fact that they constitute nonorthogonal mixed states with nonidentical supports and the fact that one can achieve probabilistic error-free discrimination of such mixed states [19]. For example, suppose that Alice has announced that the bit is encoded as $\{\rho_1, \rho_2\}$. Clearly, any measurement outcome of Bob's where photon 1 and photon 2 come out parallel rules out the state ρ_1. Here, the two outcomes "000" and "111" never occur in the absence of eavesdropping; they indicate that Eve has tampered with the communication.

These states do not form noiseless subspaces, because any particular pure state in the decomposition of the density matrices ρ_1, ρ_2, or ρ_3 does not remain invariant under collective noise. Instead, it is transformed into another state in the decomposition of the same density matrix. For instance, $|\Psi^-\rangle \otimes |0\rangle$, in the decomposition of ρ_1, becomes under collective bit-flip $|\Psi^-\rangle \otimes |1\rangle$. The individual states are not noiseless, as is the space spanned by them; they therefore form a noiseless subsystem, and the density matrices are invariant under collective noise.

This second protocol shares many similarities with Protocol 1. It is our hope that essentially the same proof will be able to show that both protocols are secure. In practice, Alice does not have to create two photon pairs and discard one photon; she could simply create one pair and one additional photon in the maximally mixed state. This should greatly increase the transmission rate since pair creation schemes have relatively low efficiency. Furthermore, Protocol 2, based on trios of photons instead of quartets, should suffer less from photon loss and hence be realizable over greater distances.

On a speculative note, perhaps the two protocols could be hybridized into a more robust protocol. Alice could always encode her information on photon quartets. Bob could then divide the photon multiplets into two sets depending on how many photons from the quartet actually made it to the destination: set 1 when all four photons made it and set 2 when only three photons were detected. The outputs from set 1 could then be used to complete Protocol 1, while those of the second set would be used as in Protocol 2. However, this suggestion provides Eve with a wide variety of attacks unavailable in our two protocols, and its security must therefore be studied independently.

We thank Gilles Brassard for helpful comments on our protocols. J.-C. B., R. L., D. P., and R.W. S. receive financial support from Canada's NSERC. This work was partially funded by MITACS and ARDA.

[1] C. H. Bennett and G. Brassard, *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing* (IEEE, New York, 1984), p. 175.
[2] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).
[3] R. J. Hughes, J. E. Nordholt, D. Derkacs, and C. G. Peterson, New J. Phys. **4**, 43 (2002).
[4] P. Townsend, J. G. Rarity, and P. R. Tapster, Electron. Lett. **29**, 634 (1993).
[5] Z. D. Walton, A. F. Abouraddy, A.V. Sergienko, B. E. A. Saleh, and M. C. Teich, quant-ph/0304075.
[6] P. Zanardi and M. Rasetti, Phys. Rev. Lett. **79**, 3306 (1997).
[7] E. Knill, R. Laflamme, and L. Viola, Phys. Rev. Lett. **84**, 2525 (2000).
[8] J. Kempe, D. Bacon, D. A. Lidar, and K. B. Whaley, Phys. Rev. A **63**, 042307 (2001).
[9] D. Stucki, N. Gisin, O. Guinnard, G. Ribordy, and H. Zbinden, New J. Phys. **4**, 41 (2002).
[10] M. Martinelli, Opt. Commun. **72**, 341 (1989).
[11] D. Gottesman and H.-K. Lo, IEEE Trans. Inf. Theory **49**, 457 (2003).
[12] S. D. Bartlett, T. Rudolph, and R.W. Spekkens, Phys. Rev. Lett. **91**, 027901 (2003).
[13] C. H. Bennett, Phys. Rev. Lett. **68**, 3121 (1992).
[14] K. Tamaki, M. Koashi, and N. Imoto, Phys. Rev. Lett. **90**, 167904 (2003).
[15] A. Cabello, quant-ph/0303076.
[16] P. G. Kwiat, A. J. Berglund, J. B. Altepeter, and A. G. White, Science **290**, 498 (2000).
[17] J.-W. Pan, M. Daniell, S. Gasparoni, G. Weihs, and A. Zeilinger, Phys. Rev. Lett. **86**, 4435 (2001).
[18] Z. Zhao, T. Yang, Y.-A. Chen, A.-N. Zhang, M. Żukowski, and J-W. Pan, quant-ph/0302137.
[19] T. Rudolph, R.W. Spekkens, and P. S. Turner, Phys. Rev. A **68**, 010301(R) (2003).