PHYSICAL REVIEW A **72**, 050304(R) (2005)

Fault tolerant quantum key distribution protocol with collective random unitary noise

Xiang-Bin Wang*
Imai Quantum Computation and Information Project, ERATO, JST Daini Hongo White Building 201, 5-28-3, Hongo, Bunkyo, Tokyo 113-0033, Japan
(Received 18 May 2004; published 23 November 2005)

We propose an easy implementable prepare-and-measure protocol for robust quantum key distribution with photon polarization. The protocol is fault tolerant against collective random unitary channel noise. The protocol does not need any collective quantum measurement or quantum memory. A security proof and a specific linear optical realization using spontaneous parametric down conversion are given.

DOI: 10.1103/PhysRevA.72.050304 PACS number(s): 03.67.Dd, 03.67.Hk

INTRODUCTION

Quantum key distribution (QKD) [1,2] is one of the most important applications of the subject of quantum information. In constrast to classical cryptography, the security of QKD is guaranteed by elementary principles of quantum mechanics, and therefore the unconditional security can be achieved. For security, we have to distill out a shorter final key, since the eavesdropper (Eve) may pretend her disturbance is the noise from the physical channel. If the noise is too large, no final key can be obtained. To overcome this, one needs to design new fault tolerant protocols or new physical realizations for quantum key distribution. There are two approaches to this problem: one is to find a new protocol that raises the threshold of channel noise unconditionally, such as the protocol with two-way classical communications [3–5]; the other way is first to study the noise pattern and then find a way to remove or decrease the noise itself, such as the various methods to cancel the collective errors [6–8]. So far there are various realizations using either the phase coding [2,9] or the polarization information of single photons [10,11]. Those protocols using the phase coding require collective measurement at Bob's side. There are also proposals to remove the collective random unitary noise from the channel [6–8].

Here we raise a unique proposal to reduce the channel errors, or, equivalently, to raise the noise threshold. Our method does not require Bob to take any collective measurement. Our method is based on the widely accepted assumptions that the flipping errors of polarization (mainly) come from the random rotation by the fiber or the molecules in the air, with the degree of the rotation fluctuating randomly. Also, if several qubits are transmitted simultaneously and they are spatially close to each other, the random unitaries to each of them must be identical, i.e., the error of the physical channel is *collective*.

MAIN IDEA

Consider an arbitrary collective random unitary U which satisfies

$$U|0\rangle = \cos\theta|0\rangle + e^{i\phi}\sin\theta|1\rangle;$$

$$U|1\rangle = e^{i\Delta}(-e^{-i\phi}\sin\theta|0\rangle + \cos\theta|1\rangle). \quad (1)$$

Here $|0\rangle$, $|1\rangle$ represent horizontal and vertical polarization states, respectively. Note that the parameters Δ, ϕ, and θ fluctuate with time, therefore one has no way to make unitary compensation to a single qubit. However, the channel unitary error is a type of collective error to all qubits sent simultaneously, therefore it is possible to send qubits robustly because the collective errors on different qubits may cancel each other. With such type of collective unitary errors, we shall take the QKD in the subspace of the two-qubit state of

$$S = \{|01\rangle, |10\rangle\}. \quad (2)$$

In particular, we let Alice prepare and send Bob two-qubit states randomly chosen from $|01\rangle$, $|10\rangle$, $|\psi^{\pm}\rangle = 1/\sqrt{2}(|01\rangle \pm |10\rangle)$. Although state $|\psi^{-}\rangle$ remains unchanged under the collective unitary errors [12], the other three states do not remain unchanged. However, in our protocol, we shall let Bob first take a parity check to the two-qubit state to see whether it belongs to subspace S. If it does, he accepts it; if it does not, he discards it. The key point here is that, although the two-qubit states could be distorted by the collective random unitary, most often the distortion will drive the codes out of subspace S, therefore the distorted codes will be discarded by the protocol itself. The error rates to those *accepted* codes are normally small, provided that the channel noise is mainly from the collective unitary and the averaged value θ is not too large. For example, our protocol gives a good key rate if the averaged value $|\sin\theta|$ is $1/2$. (The dispersion, ϕ value can be arbitrarily large.) Explicitly, any collective rotation cannot exchange states $|\psi^{+}\rangle$ and $|\psi^{-}\rangle$; it can only drive $|\psi^{+}\rangle$ out of the subspace S. However, any state outside of S will be rejected, as required by our protocol. Therefore the rate of flipping between $|\psi^{+}\rangle$ and $\psi^{-}\rangle$ (phase-flip rate) is zero. A collective rotation U will also take the following effects:

$$U^{\otimes 2}|01\rangle = U|0\rangle \otimes U|1\rangle = \cos^2\theta|01\rangle - \sin\theta\cos\theta(e^{-i\phi}|00\rangle - e^{i\phi}|11\rangle) - \sin^2\theta|10\rangle. \quad (3)$$

*Electronic address: wang@qci.jst.go.jp

$$U^{\otimes 2}|10\rangle = U|1\rangle \otimes U|0\rangle = \cos^2\theta|10\rangle - \sin\theta\cos\theta(e^{-i\phi}|00\rangle - e^{i\phi}|11\rangle) - \sin^2\theta|01\rangle. \quad (4)$$

Since the states outside of the subspace S will be discarded, the net flipping between rate $|01\rangle$ and $|10\rangle$ (bit-flip rate) $r_b = \sin^4\theta/(\cos^4\theta + \sin^4\theta)$. Therefore, if the average rotating angle is small, the flipping rate r_b will be also small. [If we directly use the Bennett–Brassard 1984 (BB84) protocol, the bit-flip rate is $\sin^2\theta$, one magnitude of order larger than ours.] Moreover, in the ideal case that all flips come from the random rotation, since the phase-flip rate is zero, one can *always* distill some bits of final key provided that $r_b \neq 1/2$. The key rate is $1 + r_b \log_2 r_b + (1-r_b)\log_2(1-r_b)$. Note that if $r_b > 1/2$ one can simply reverse all bit values given by $|01\rangle$ and $|10\rangle$ and also distill some bits of final key. In practice, if θ does not change too fast, we can divide the data into many blocks. We inverse the bit values of those blocks with larger than $1/2$ error rate after the decoding. Note that we assume the phase-flip error to be always very small by our protocol.

Boileau *et al.* [8] has recently proposed a protocol with the collective random unitary error model. Our work differs from Ref. [8] in the following aspects: (1) The main idea is different. Reference [8] uses the fact that state $|\psi^-\rangle = 1/\sqrt{2}(|01\rangle - |10\rangle)$ is invariant under whatever rotations, therefore the linear combinations of a few $|\psi^-\rangle$ at different positions will work robustly. We use a subspace of a two-qubit state. Our states are not always invariant under random rotations, however, the randomly rotation can drive the original state out of the specific subspace and never or rarely switch any two states inside the subspace. After Bob discards all those transmitted codes outside subspace S, the phase-flip error will be totally removed and the bit-flip error will be significantly decreased. (2) The method is different. The protocol given by Boileau *et al.* requires three- or four-qubit entangled states, which could be technically difficult by currently existing technology. Our protocol only requires two-qubit states which can be produced effectively. (3) The result is different. Since our protocol is BB84-like [1], we do not have to worry about the channel loss in practice. Boileau's protocol is likely to be undermined by the channel loss, since it is B92-like [13,14]. In practice, the lossy rate for their protocol could be very high. Since they use at least three qubits to encode one, the joint survival rate is very low.

Protocol 1 and security proof. For clarity, we now give a protocol with collective measurements first and then reduce it to a practically feasible protocol without any collective measurements.

Protocol 1. (1) *Preparation of the encoded BB84 states.* Alice creates a number of single-qubit states, each of them randomly chosen from $\{|0\rangle, |1\rangle, |\pm\rangle\}$. She puts down each one's preparation basis and bit value: state $|0\rangle$, $|+\rangle$ for bit value 0, the other two states are for 1. She also prepares ancillas which are all in state $|0\rangle$. She then encodes each individual qubit with an ancilla into a two-qubit code through the following controlled NOT (CNOT) operation: $|00\rangle \to |01\rangle$; $|10\rangle \to |10\rangle$; $|11\rangle \to |11\rangle$; $|01\rangle \to |00\rangle$. The second digit in each state is for the ancilla. Such encoding operation changes $(|0\rangle, |1\rangle)$ into $(|01\rangle, |10\rangle)$ and $|\pm\rangle$ into $|\psi^\pm\rangle$. (2) *State transmission.* Alice sends those two-qubit codes to Bob. (3) *Error rejection and decoding.* Bob takes the same CNOT operation as used by Alice in encoding. He then measures the second qubit in the Z basis: if it is $|1\rangle$, he discards both qubits and notifies Alice; if he obtains $|0\rangle$, he measures the first qubit in either the X or Z basis and records the basis as his "measurement basis" in the QKD protocol. The bit value of a code is determined by the measurement outcome of the first qubit after decoding, $|0\rangle$, $|+\rangle$ for bit value 0, $|1\rangle$, $|-\rangle$ correspond to 1. (4) *Basis announcement.* Through public discussion, they discard all those decoded qubits with different measurement bases in two sides. (5) *Error test.* They announce the values of all X bits and some of the Z bits. If too many values disagree, they abort the protocol, otherwise, they distill the remaining bits for the final key. (6) *Final key distillation.* Alice and Bob distill the final key by the classical CSS code [15].

The unconditional security here is equivalent to that of the BB84 protocol [1,12] with a lossy noisy channel: *Protocol 1* can be regarded as an encoded BB84 protocol with additional steps of encoding, error rejection, and decoding. If Eve can attack *Protocol 1* successfully with operation $\hat{A}$ during the stage of codes transmission, she can also attack the BB84 protocol successfully with

$$\hat{A}' = \hat{E} \to \hat{A} \to \hat{R} \to \hat{D} \quad (5)$$

during the qubit transmission and then pass the decoded qubit to Bob, where $\hat{E}$, $\hat{R}$, $\hat{D}$ are encoding, error rejection, and quantum decoding, respectively. (The operation of encoding, error rejection, or decoding does not requires any information about the unknown BB84 state itself.) Obviously, the BB84 protocol with attack $\hat{A}'$ is identical to *Protocol 1* with attack $\hat{A}$. To Alice and Bob, the BB84 protocol with Eve's attack $\hat{A}'$ is just a BB84 protocol with a lossy channel. (Eve must discard some codes in the error rejection step.) Therefore *Protocol 1* must be secure, since the BB84 protocol is unconditionally secure even with a lossy channel.

Protocol 2. Though we have demonstrated the unconditional security of *Protocol 1*, we do not directly use *Protocol 1* in practice since it requires the local CNOT operation in encoding and decoding. We now reduce it to another protocol without any collective operations. First, since there are only four candidates in the set of BB84 states, instead of encoding from BB84 states, Alice may directly produce four random states of $|01\rangle$, $|10\rangle$, $|\psi^+\rangle$, $|\psi^-\rangle$. Note that except for Alice herself, no one else can see whether the two-qubit codes in transmission are directly produced or if the encoding results from BB84 states. One may simply produce the states of those two-qubit codes by the spontaneous parametric down conversion [16,17]. Second, in the decoding and error rejection step, Bob can carry out the task by *postselection*. For all those codes originally in state $|01\rangle$ or $|10\rangle$, Bob can simply take local measurements in the Z basis to each qubit and then discard those outcomes of $|0\rangle \otimes |0\rangle$ or $|1\rangle \otimes |1\rangle$ and only accept the outcome $|0\rangle \otimes |1\rangle$, which is regarded as a bit value 0, and $|1\rangle \otimes |0\rangle$, which is regarded as bit value 1. The net flipping rate between $|01\rangle$ and $|10\rangle$ is re-

garded as bit-flip rate. The nontrivial point is the phase-flip rate, i.e., the net flipping rate between states $|\psi^{\pm}\rangle$. Note that all these codes only take the role of indicating the phase-flip rate, we do not have to know explicitly which one is flipped and which one is not flipped. Instead, we only need to know the average flipping rate between $|\psi^{\pm}\rangle$. To obtain such information, we actually do not have to really carry out the error rejection and decoding steps to each of these codes. What we need to do is simply answer what the flipping rate *would* be if Bob really *took* the error rejection step and decoding step to each code of $|\psi^{\pm}\rangle$. One straightforward way is to let Bob take a Bell measurement to each code which was in state $|\psi^{\pm}\rangle$ originally. (*We shall call them* ψ^{+} or ψ^{-} *codes hereafter.*) For example, consider ψ^{+} codes, after transmission, if the distribution over four Bell states $|\psi^{+}\rangle, |\psi^{-}\rangle, |\phi^{+}\rangle, |\phi^{-}\rangle$ are $p_{\psi^{-}}, p_{\psi^{+}}, p_{\phi^{+}}, p_{\phi^{-}}$, respectively; after the Bell measurements, we conclude that the channel flipping rate of $|\psi^{+}\rangle \rightarrow |\psi^{-}\rangle$ is $p_{\psi^{-}}/(p_{\psi^{+}}+p_{\psi^{-}})$. This rate is equivalent to the flipping rate of $|+\rangle \rightarrow |-\rangle$ in the BB84 protocol. Note that the rate of $p_{\phi^{\pm}}$ has been excluded here since their corresponding states are outside of the subspace S and should be discarded by our protocol.

Bell measurement is not the unique way to see the distribution over four Bell states for a set of states. We can also simply divide the set into three subsets and take collective measurements ZZ to subset 1, XX to subset 2, and YY to subset 3. We can then *deduce* the distribution over the four Bell states. Here ZZ, XX, YY are parity measurements to a two-qubit code in Z, X, Y basis, respectively. (Y: measurement basis of $\{|y\pm\rangle = 1/\sqrt{2}(|0\rangle \pm i|1\rangle)\}$.) Note that classical statistics works perfectly here because all these collective measurements commute [18,19]. These collective measurements can be simply replaced by local measurements to each qubit since once we have obtained the results of local measurements of $Z\otimes Z, X\otimes X, Y\otimes Y$ we also know the parity information. (In this paper, $Z\otimes Z$ represents a local measurement to each qubit in the Z basis; ZZ represents a collective measurement for the parity in the Z basis.)

Before going into the reduced protocol, we show the explicit relationship between the phase-flip rate and the local measurement results. Note that Bob has randomly divided all the received two-qubit codes into three subsets and he will take local measurement $Z\otimes Z, X\otimes X, Y\otimes Y$ to each of the qubits of each codes in subset 1,2,3, respectively. Consider all ψ^{-} codes first. Denote $\epsilon_z, \epsilon_x, \epsilon_y$ for the rate of wrong outcome for ψ^{-} codes in subset 1,2,3, respectively, i.e., the rate of codes whose two qubits have the same bit values in basis Z, X, Y, respectively. Given values $\epsilon_{z,x,y}$ we immediately have

$$p_{\phi^{+}} + p_{\phi^{-}} = \epsilon_z, \tag{6}$$

$$p_{\psi^{+}} + p_{\phi^{+}} = \epsilon_x, \tag{7}$$

$$p_{\psi^{+}} + p_{\phi^{-}} = \epsilon_y. \tag{8}$$

Our aim is only to see the flipping rate from $|\psi^{-}\rangle$ to $|\psi^{+}\rangle$; other types of errors are discarded since they have gone out of the given subspace S. The net flipping rate from $|\psi^{-}\rangle$ to $|\psi^{+}\rangle$ is

$$t_{\psi^{-}\rightarrow\psi^{+}} = \frac{p_{\psi^{+}}}{p_{\psi^{-}} + p_{\psi^{+}}} = \frac{\epsilon_x + \epsilon_y - \epsilon_z}{2(1-\epsilon_z)}. \tag{9}$$

In a similar way we can also have the formula for the value of $t_{\psi^{+}\rightarrow\psi^{-}}$, the flipping rate from $|\psi^{+}\rangle$ to $|\psi^{-}\rangle$,

$$t_{\psi^{+}\rightarrow\psi^{-}} = \frac{\epsilon'_x + \epsilon'_y - \epsilon'_z}{2(1-\epsilon'_z)}. \tag{10}$$

Here $\epsilon'_{x,y,z}$ are the rate of wrong outcome in local measurement basis $X\otimes X, Y\otimes Y, Z\otimes Z$, respectively, to all codes originally in $|\psi^{+}\rangle$. The total phase-flip error is

$$t_p = \frac{t_{\psi^{-}\rightarrow\psi^{+}} + t_{\psi^{+}\rightarrow\psi^{-}}}{2}. \tag{11}$$

Protocol 1 is now replaced by the following practically feasible protocol without any collective measurement:

Protocol 2. (1) *Preparation of the encoded BB84 states.* Alice creates a number of two-qubit states and each of them are randomly chosen from $\{|01\rangle, |10\rangle, |\psi^{\pm}\rangle\}$. For each two-qubit code, she puts down "Z basis" if it is in state $|01\rangle$ or $|10\rangle$ or "X basis" ($\{|\pm\rangle\}$) if it is in one of the states $\{1/\sqrt{2}(|01\rangle \pm |10\rangle)\}$. For those code states of $|01\rangle$ or $\{1/\sqrt{2}(|01\rangle + |10\rangle)\}$, she denotes a bit value 0; for those code states of $|10\rangle$ or $\{1/\sqrt{2}(|01\rangle - |10\rangle)\}$, she denotes a bit value 1. (2) *Transmission.* Alice sends all the two-qubit codes to Bob. (3) *Measurement.* To each code, Bob measures the two qubits in a basis randomly chosen from $\{Z\otimes Z, X\otimes X, Y\otimes Y\}$. For example, if he happens to choose basis $Z\otimes Z$ for a certain code, he measures each qubit of that code in Z basis. (4) *Rejection of wrong results.* Alice announces her "preparation basis" for each code. Bob announces his measurement basis to each code. For those codes originally prepared in $|01\rangle$ or $|10\rangle$, they discard the results if Bob has used a basis other than $Z\otimes Z$. They also discard all codes outside the subspace S. (5) *Error test.* To all the survived results, they announce bit values of codes originally in $|\psi^{+}\rangle$ or $|\psi^{-}\rangle$. From the announced results they can calculate the phase-flip rate by formula (11). They can also estimate the bit-flip rate by annoucing some results of those survived codes which are originally in $|01\rangle$ or $|10\rangle$. (6) *Final key distillation.* Alice and Bob distill the final key by using the classical CSS code [15].

Physical realization of protocol 2. There are two parts in the realization. One is the source for the required four different two-qubit states at Alice's side. The other is the measurement device at Bob's side. Both of them can be realized with simple linear optical devices. The requested source states can be generated by SPDC process [16,17] as shown in Fig. 1. The measurement with random basis at Bob's side can be done by a polarizing beam splitter (PBS) and a rotator driven electrically, as shown in Fig. 2.

Another protocol for robust QKD with swinging objects. In some cases, especially in free space, the dispersion can be small while the random rotation angle θ can be large. We consider the extreme case that ϕ in unitary U is 0, or otherwise can be compensated to almost 0, but θ is random and can be arbitrarily large. The swinging angle of an airplane can be very large in certain cases. We can exactly use the

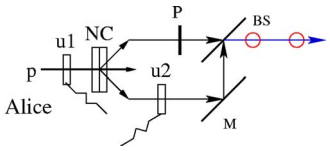

FIG. 1. (Color online) The source of a two-qubit state. P: $\pi/2$ rotator, BS: beam splitter, M: mirror, NC: nonlinear crystal, p: pump light in horizontal polarization, u1: unitary rotator, u2: phase shifter. u1 takes the value of 0, $\pi/2$, $\pi/4$ to produce state $|01\rangle$, $|10\rangle$, $|\psi^+\rangle$, respectively. u2 can be either I or σ_z.

collective unitary model, with all elements in U being real if there is no dispersion. Then we have a better method. It is well known that both states $|\phi^+\rangle$ and $|\psi^-\rangle$ are invariant under whatever real rotation. Any linear superposed state of these two are also invariant. Therefore we use the following for states $\{|\bar{0}\rangle=|\phi^+\rangle, |\bar{1}\rangle=|\psi^-\rangle;\ |+'\rangle=1/\sqrt{2}(|\bar{0}\rangle+|\bar{1}\rangle)=1/\sqrt{2}(|0\rangle|+\rangle+|1\rangle|-\rangle);\ |-'\rangle=1/\sqrt{2}(|0\rangle|-\rangle+|1\rangle|+\rangle)\}$. Bob need not take any collective measurement to determine the bit value. If he chooses the "Z" basis, he measures each of the two qubits in the Z basis, 00 or 11 for bit value 0 while 01 or 10 for bit value 1. If he chooses the "X" basis, he measures the first qubit in the Z basis and the second in the X basis, $|0\rangle|+\rangle$ or $|1\rangle|-\rangle$ for bit value 0 and $|0\rangle|-\rangle$ or $|1\rangle|+\rangle$ for bit value 1. There is no error rejection step here because there is expected to be no error after decoding, given the real rotation channel. Even for the QKDs with fixed object there is still a little bit of an advantage: they do not need take any bases alignment with each other. Each of them only needs to make sure their local measurement bases are BB84-like, i.e., the inner product of two bases are $1/\sqrt{2}$.

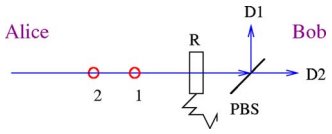

FIG. 2. (Color online) Measurement device at Bob's side. The rotator R offers a random rotation to both qubits in the same code. Each time, rotation is randomly chosen from unity $(|0\rangle,|1\rangle)\rightarrow(|+\rangle,|-\rangle)$, $(|0\rangle,|1\rangle)\rightarrow(|y+\rangle,|y-\rangle)$. The event of two clicks (at different times) on one detector ($D1$ or $D2$) shows that the two qubits of the code have the same bit value; two clicks on different detectors show that the two qubits have different bit values.

CONCLUSION

We have given a robust QKD protocol in polarization space given the fact that the collective random unitaries are dominant channel errors. Our protocol can obviously be extended to the six-state-like protocol [20] if we add one more candidate state of $1/\sqrt{2}(|0\rangle\pm i|1\rangle)$ in the source.

Note added. Recently, an interesting different protocol [21] for robust QKD also appeared.

ACKNOWLEDGMENTS

I thank Professor H. Imai for support, and J. W. Pan, B. S. Shi, and A. Tomita for discussions.

[1] C. H. Bennett and G. Brassard, in *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India, 1984* (IEEE, New York, 1984), pp. 175–179; C. H. Bennett and G. Brassard, IBM Tech. Discl. Bull. **28**, 3153 (1985).
[2] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).
[3] D. Gottesman and H.-K. Lo, IEEE Trans. Inf. Theory **49**, 457 (2003).
[4] H. F. Chau, Phys. Rev. A **66**, 060302(R) (2002).
[5] X. B. Wang, Phys. Rev. Lett. **92**, 077902 (2004).
[6] G. M. Palma, K. A. Suominen, and A. K. Ekert, Proc. R. Soc. London, Ser. A **452**, 567 (1996).
[7] Z. D. Walton *et al.*, Phys. Rev. Lett. **91**, 087901 (2003).
[8] J. C. Boileau, D. Gottesman, R. Laflamme, D. Poulin, and R. W. Spekkens, Phys. Rev. Lett. **92**, 017901 (2004).
[9] D. Stucki *et al.*, New J. Phys. **4**, 41 (2002).
[10] W. T. Buttler *et al.*, Phys. Rev. Lett. **81**, 3283 (1998).
[11] M. Aspelmeyer *et al.*, Science **301**, 621 (2003); M. Aspelmeyer *et al.*, IEEE J. Sel. Top. Quantum Electron. **9**, 1541 (2003); G. J. Rarity *et al.*, New J. Phys. **4**, 82 (2002).
[12] P. G. Kwiat *et al.*, Science **290**, 498 (2000).
[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] P. W. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000).
[16] P. G. Kwiat *et al.*, Phys. Rev. A **60**, R773 (1999).
[17] P. G. Kwiat, K. Mattle, H. Weinfurter, A. Zeilinger, A. V. Sergienko, and Y. Shih, Phys. Rev. Lett. **75**, 4337 (1995).
[18] H. K. Lo and H. F. Chau, Science **283**, 2050 (1999).
[19] D. Gottesman and J. Preskill, Phys. Rev. A **63**, 022309 (2001).
[20] D. Bruss, Phys. Rev. Lett. **81**, 3018 (1998).
[21] J.-C. Boileau, R. Laflamme, M. Laforest, and C. R. Myers, Phys. Rev. Lett. **93**, 220501 (2004).