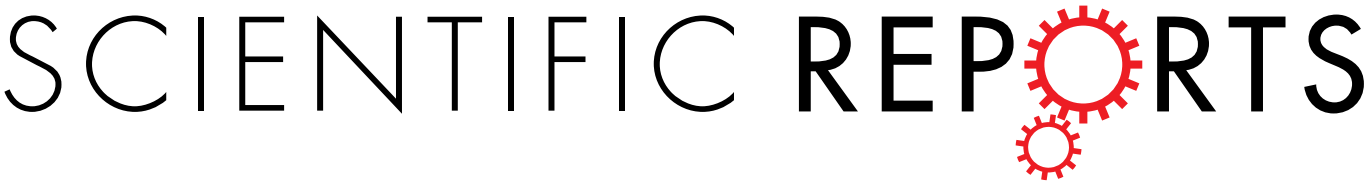

OPEN

Geometric discord: A resource for increments of quantum key generation through twirling

Received: 01 April 2015
Accepted: 24 June 2015
Published: 26 August 2015

Xiaohua Wu[1] & Tao Zhou[2]

In the present work, we consider a scenario where an arbitrary two-qubit pure state is applied for the quantum key generation (QKG). Using the twirling procedure to convert the pure state into a Werner state, the error rate of the key can be reduced by a factor of 2/3. This effect indicates that entanglement is not the sufficient resource of QKG protocol since it is not increased in the twirling procedure. Based on the fact that the geometric discord is increased in the twirling procedure, we argue that the geometric discord should be taken as a necessary resource for the QKG task. Besides the pure state, we also give other two types of mixtures where twirling may increase the discord and reduce the error rate of the generated key.

How to quantify and characterize the nature of correlations in a quantum state, has a crucial applicative importance in the field of quantum information processing[1] beyond the fundamental scientific interest. It is well known that a bipartite quantum state can contain both classical and quantum correlations. Quite recently, quantum discord was introduced as a more general measure of quantum correlation[2,3] beyond the quantum entanglement[4]. Since it was regarded as a resource for quantum cryptography[5], quantum computation[6], quantum state merging[7,8], and remote state preparation[9], quantum discord has attracted much attention in recent works[6–34].

Among all the known quantum tasks, quantum key distribution (QKD) is one of the most important cases that have been widely discussed in both the theoretic and experimental aspects[35]. In 1984, Bennet and Brassard[36] firstly proposed the QKD protocol. In 1991, Ekert proposed a QKD protocol independent on the BB84 paper[37], and it is also called the Einstein-Podolsky-Rosen (EPR) protocol since the maximally entangled states, or the EPR pairs, are used to complete the task[35].

In the present work, we develop a generalized EPR protocol where an arbitrary two-qubit state is applied for the quantum key generation (QKG). The error rate of the generated key can be taken as the figure of merit for this task. In the BB84 protocol, the key is sent from Alice to Bob[36], but in our work, the key is generated in a different scheme: The keys are undetermined until Alice or Bob performs a measurement on their parts, respectively.

A pure state can be converted into a Werner state in a twirling procedure, and it is interesting that simultaneously the error rate of the key can be reduced by a factor of 2/3 in our QKG scheme. It has already been known that twirling can never increase the entanglement, and therefore, the observed effect, where twirling effectively improves the performance of the pure state in QKG protocol, shows that entanglement is not the sufficient resource for this task. Instead, the geometric discord can be increased in the twirling procedure, and this indicates that the geometric discord may be taken as a necessary quantum resource in the QKG protocol. For the general two-qubit case, we obtain the relation between the error rate and the geometric discord. Based on this, the observed effect may be well explained by the fact that the geometric discord of the pure state can indeed be increased by twirling. Furthermore, we give other two types of mixed states, where twirling may increase the discord and reduce the error rate of the generated key at the same time.

[1]College of Physical Science and Technology, Sichuan University, Chengdu 610064, China. [2]School of Physical Science and Technology, Southwest Jiaotong University, Chengdu 610031, China. Correspondence and requests for materials should be addressed to X.W. (email: wxhscu@scu.edu.cn) or T.Z. (email: taozhou@swjtu.edu.cn)

The EPR protocol for QKD

To process on, we should first notice that an arbitrary two-qubit state ρ, which lies in the Hilbert space $\mathcal{H}^1 \otimes \mathcal{H}^2$ with each $\mathcal{H}^i (i = 1, 2)$ being a two-dimensional space, can always be expressed as

$$\rho = \frac{1}{4}\left(\mathbb{I} \otimes \mathbb{I} + x_3\sigma_3 \otimes \mathbb{I} + y_3\mathbb{I} \otimes \sigma_3 + \sum_{i,j=1}^{3} T_{ij}\sigma_i \otimes \sigma_j\right) \tag{1}$$

in a fixed basis carefully chosen, where $\sigma_1 = |\uparrow\rangle\langle\downarrow| + |\downarrow\rangle\langle\uparrow|$, $\sigma_2 = -i|\uparrow\rangle\langle\downarrow| + i|\downarrow\rangle\langle\uparrow|$, and $\sigma_3 = |\uparrow\rangle\langle\uparrow| - |\downarrow\rangle\langle\downarrow|$ are the Pauli operators, and $T_{ij} = \mathrm{Tr}\left[\rho(\sigma_i \otimes \sigma_j)\right]$, $x_3 = \mathrm{Tr}[\rho(\sigma_3 \otimes \mathbb{I})]$, $y_3 = \mathrm{Tr}[\rho(\mathbb{I} \otimes \sigma_3)]$. Assume that the states above consist of two spin-1/2 particles labeled by 1 and 2, and Alice measures particle 1 with a fixed observable $\sigma\boldsymbol{a} = \boldsymbol{\sigma}\cdot\boldsymbol{a}$ while Bob performs a measurement on the particle 2 with the observable $\sigma_{\boldsymbol{b}} = \boldsymbol{\sigma}\cdot\boldsymbol{b}$, where $\boldsymbol{a}$ and $\boldsymbol{b}$ are two unit vectors. Then, *a joint measurement for the observable* $\sigma_{\boldsymbol{a}} \otimes \sigma_{\boldsymbol{b}}$ *is called to be optimal if and only if* $Tr[\rho(\sigma_{\boldsymbol{a}} \otimes \sigma_{\boldsymbol{b}})] = max_{\boldsymbol{n}}\langle\sigma_{\boldsymbol{a}} \otimes \sigma_{\boldsymbol{n}}\rangle$. For simplicity, hereafter, we denote $\langle\boldsymbol{a} \otimes \boldsymbol{b}\rangle = \langle\sigma_{\boldsymbol{a}} \otimes \sigma_{\boldsymbol{b}}\rangle$. Now four probabilities $\omega_{\pm\pm}(\boldsymbol{a}, \boldsymbol{b})$ can be introduced, *i.e.*, $\omega_{++}(\boldsymbol{a}, \boldsymbol{b})$ is the corresponding probability in the case that the measurement results for both particles are positive, when the joint measurement $\sigma_{\boldsymbol{a}} \otimes \sigma_{\boldsymbol{b}}$ has been performed. Then, for an arbitrary two-bit state ρ, one should have

$$\omega_{++}(\boldsymbol{a}, \boldsymbol{b}) + \omega_{+-}(\boldsymbol{a}, \boldsymbol{b}) + \omega_{-+}(\boldsymbol{a}, \boldsymbol{b}) + \omega_{--}(\boldsymbol{a}, \boldsymbol{b}) = 1,$$

and the correlation function, $\langle\boldsymbol{a} \otimes \boldsymbol{b}\rangle$, can be expressed as

$$\langle\boldsymbol{a} \otimes \boldsymbol{b}\rangle = \omega_{++}(\boldsymbol{a}, \boldsymbol{b}) + \omega_{--}(\boldsymbol{a}, \boldsymbol{b}) - \omega_{+-}(\boldsymbol{a}, \boldsymbol{b}) - \omega_{-+}(\boldsymbol{a}, \boldsymbol{b}).$$

With the optimal measurement defined above, the maximally entangled states are the ones satisfying $\langle\boldsymbol{a} \otimes \boldsymbol{b}\rangle_{\max} = 1$ for an arbitrary vector $\boldsymbol{a}$.

Now, we come to the EPR protocol for QKD. It is well known that maximally entangled states can be applied to generate a randomly distributed key as in the following arguments[38]:

1. A large amount of EPR pairs shared by Alice and Bob are prepared, and Alice (Bob) randomly measures her (his) particle of a EPR pair with $\sigma_{\boldsymbol{a}}$ or $\sigma_{\boldsymbol{a}'}$ ($\sigma_{\boldsymbol{b}}$ or $\sigma_{\boldsymbol{b}'}$), where $\boldsymbol{a}' \perp \boldsymbol{a}$, $\boldsymbol{b}' \perp \boldsymbol{b}$;
2. After sufficient runs of measurements have been performed, Alice and Bob exchange the information about the observable used in each run over a public channel;
3. The experimental data from the measurements for the observables $\sigma_{\boldsymbol{a}} \otimes \sigma_{\boldsymbol{b}'}$ and $\sigma_{\boldsymbol{a}'} \otimes \sigma_{\boldsymbol{b}}$ are discarded. In other words, the remaining data come from the measurements performed by the observables $\sigma_{\boldsymbol{a}} \otimes \sigma_{\boldsymbol{b}}$ and $\sigma_{\boldsymbol{a}'} \otimes \sigma_{\boldsymbol{b}'}$;
4. Finally, by arranging their own remaining experiment data in time sequence, each observer can obtain a random key, a long string of symbols like "$+ + - + - \cdots +$".

Usually, the maximally entangled state may be chosen to be $|\Phi^+\rangle = (|\uparrow\uparrow\rangle + |\downarrow\downarrow\rangle)/\sqrt{2}$. In the present paper, we use the same symbol Φ^+ o denote the density operator of the pure state, $\Phi^+ = |\Phi^+\rangle\langle\Phi^+|$, if no confusion is caused. The QKD task realized in the EPR protocol above was proven to be equivalent to the BB84 scheme[38]. Furthermore, one may verify that the two-particle state $\overline{\rho}$,

$$\overline{\rho} = (\mathbb{I} \otimes \varepsilon)\Phi^+, \tag{2}$$

can be also applied to complete the QKD task. For instance, suppose that Alice randomly selects the measurement from $\sigma_{\boldsymbol{x}}$ or $\sigma_{\boldsymbol{y}}$ ($\boldsymbol{x} = (1, 0, 0)$ and $\boldsymbol{y} = (0, 1, 0)$), the EPR protocol realized with $\overline{\rho}$ is equivalent to the BB84 scheme where Alice prepares particles in a random sequence of the four states, $\frac{\sqrt{2}}{2}(|\uparrow\rangle \pm |\downarrow\rangle)$ and $\frac{\sqrt{2}}{2}(|\uparrow\rangle \pm i|\downarrow\rangle)$, and sends them to Bob via a noisy quantum channel ε.

The quantum key generation protocol

In the present work, we shall consider a more general scenario where the arbitrary two-qubit state in Eq. (1) is applied for the quantum key generation (QKG). Compared with the EPR protocol, the differences come from the following two aspects:

1. To get a random distributed key, it is necessary that the two eigenvectors of $\sigma_{\boldsymbol{a}}$ ($\sigma_{\boldsymbol{a}'}$) should appear with equal probability in each measurement, which means, for the state ρ in Eq. (1), it is required that $\boldsymbol{a}$ ($\boldsymbol{a}'$) should be chosen in the $x - y$ plane of the Bloch sphere. For simplicity, we choose that $\boldsymbol{a} = \boldsymbol{x}$ and $\boldsymbol{a}' = \boldsymbol{y}$.
2. The keys in Alice's site may be different from the ones in Bob's site, and the following two measurable quantities, $\delta^{\boldsymbol{x}}(\rho) = \omega_{+-}(\boldsymbol{x}, \boldsymbol{b}) + \omega_{-+}(\boldsymbol{x}, \boldsymbol{b})$, and $\delta^{\boldsymbol{y}}(\rho) = \omega_{+-}(\boldsymbol{y}, \boldsymbol{b}') + \omega_{-+}(\boldsymbol{y}, \boldsymbol{b}')$, can be used to characterize the discrepancy. The physical meaning of $\delta^{\boldsymbol{x}}$ and $\delta^{\boldsymbol{y}}$ are clear: They are the probabilities that Alice's measurement result is different from the one of Bob's when the joint measurement $\sigma_{\boldsymbol{x}} \otimes \sigma_{\boldsymbol{b}}$

and $\sigma_{\boldsymbol{y}}\otimes\sigma_{\boldsymbol{b}'}$ are performed, respectively.

Based on the condition that Alice (Bob) selects $\boldsymbol{x}$ and $\boldsymbol{y}$ ($\boldsymbol{b}$ and $\boldsymbol{b}'$) with equal probability, it is reasonable to define *the (average) error rate of the key*, to be

$$\delta(\rho) = \frac{1}{2}[\delta^{x}(\rho) + \delta^{y}(\rho)],$$

and it can be taken as the figure of merit to quantify the general EPR protocol designed above. With the two equalities, $\delta^{\boldsymbol{x}}(\rho) = (1 - \langle \boldsymbol{x}\otimes\boldsymbol{b}\rangle)/2$ and $\delta^{\boldsymbol{y}}(\rho) = (1 - \langle \boldsymbol{y}\otimes\boldsymbol{b}'\rangle)/2$, one can obtain

$$\delta(\rho) = \frac{1}{2} - \frac{1}{4}(\langle \boldsymbol{x}\otimes\boldsymbol{b}\rangle + \langle \boldsymbol{y}\otimes\boldsymbol{b}'\rangle), \tag{3}$$

which shows that the error rate is decided by the expectation values of the two observables $\sigma_{\boldsymbol{x}}\otimes\sigma_{\boldsymbol{b}}$ and $\sigma_{\boldsymbol{y}}\otimes\sigma_{\boldsymbol{b}'}$ introduced before.

Choosing certain local unitary transformations, a bipartite pure state can always be expressed as

$$|\Omega\rangle = \cos\left(\frac{\pi}{4} - \frac{\gamma}{2}\right)|\uparrow\uparrow\rangle + \sin\left(\frac{\pi}{4} - \frac{\gamma}{2}\right)|\downarrow\downarrow\rangle, \tag{4}$$

with γ a free parameter, $0\le\gamma\le\pi/2$. When $\gamma=\pi/2$, $|\Omega\rangle$ is a product state, $|\Omega\rangle = |\uparrow\uparrow\rangle$. Recently, we have shown that the two-qubit state in Eq. (1) can be expressed in an equivalent form[39]:

$$\rho = (\mathbb{I}\otimes\varepsilon)\Omega,$$

if the reduced density matrix, $\rho_1 = \mathrm{Tr}_{\mathcal{H}^2}[\rho]$, is a mixed state. With the relation above, one may easily find that our QKG protocol cannot be taken as a variation of the known QKD scheme. Under the condition that the quantum channel ε is noiseless, Alice and Bob could get a perfect key via the BB84 or the EPR protocol. However, under the same condition, the key generated by ρ always has a non-vanishing error rate, $\delta=\sin^2(\gamma/2)$, if $0<\gamma<\pi/2$.

Twirling and its effects

In 1989, Werner gave a one parameter family of twirling invariant states which do not violate the Bell inequality although these states are entangled[40]. Since then, twirling has been widely discussed in many quantum tasks, such as the entanglement distillation[41,42] and quantum process tomography[43–45]. Following the definition in Ref. [42], any two-qubit state ρ subjected to the $U\otimes U^{*}$ twirling, where U is an arbitrary two-dimensional unitary transformation, can produce a Werner state $\rho_W(F)$ as

$$\rho_W(F) = \mathcal{T}(\rho) \equiv \int_{U\in \mathrm{SU}(2)} U\otimes U^{*}\rho\,(U\otimes U^{*})^{\dagger}\mathrm{d}U \tag{5}$$

with $F = \langle\Phi^{+}|\rho|\Phi^{+}\rangle$. By introducing the four maximally entangled states, $|\Phi^{\pm}\rangle = (|\uparrow\uparrow\rangle \pm |\downarrow\downarrow\rangle)/\sqrt{2}$ and $|\Psi^{\pm}\rangle = (|\uparrow\downarrow\rangle \pm |\downarrow\uparrow\rangle)/\sqrt{2}$, a Werner state $\rho_W(F)$ in Eq. (5) is

$$\rho_W(F) = F\Phi^{+} + \frac{1-F}{3}(\Phi^{-} + \Psi^{+} + \Psi^{-}), \tag{6}$$

where F is a real number, and $0\le F\le 1$. For the two-qubit states, the Werner states are the unique ones which are invariant under the twirling procedure[40]. From the definition in Eq. (5), it is easy to verify that the pure state in Eq. (4) subjected to the twirling can produce a Werner state with $F=\cos^2(\gamma/2)$.

In the QKG task developed in the argument above, where an arbitrary two-qubit state is applied to generate a randomly distributed key, there exist some cases that twirling can be used to reduce the error rate of the key. As an important example, by performing twirling on the pure state, the error rate of the key will be effectively reduced,

$$\delta(\mathcal{T}(\Omega)) = \frac{2}{3}\delta(\Omega). \tag{7}$$

The derivation of this equation is in the following.

First, for the state in Eq. (1), by some algebra, one can obtain

$$\langle \boldsymbol{x}\otimes\boldsymbol{b}\rangle_{\max} = \sqrt{\sum_{j=1}^{3} T_{1j}^{2}},\ \ \langle \boldsymbol{y}\otimes\boldsymbol{b}'\rangle_{\max} = \sqrt{\sum_{j=1}^{3} T_{2j}^{2}}. \tag{8}$$

Then, for the pure state in Eq. (4), the density operator can be written as

$$\Omega(\gamma) = \frac{1}{4}[\mathbb{I}\otimes\mathbb{I} + \sin\gamma(\sigma_3\otimes\mathbb{I} + \mathbb{I}\otimes\sigma_3) + \cos\gamma(\sigma_1\otimes\sigma_1 - \sigma_2\otimes\sigma_2) + \sigma_3\otimes\sigma_3].$$

and therefore, with the optimal settings $\boldsymbol{b}=(1,\ 0,\ 0)$ and $\boldsymbol{b}'=(0,\ -1,\ 0)$, we can obtain $\langle \boldsymbol{x}\otimes\boldsymbol{b}\rangle_{\max} = \langle \boldsymbol{y}\otimes\boldsymbol{b}'\rangle_{\max} = \cos\gamma$. The minimum error rate $\delta(\Omega)=\sin^2(\gamma/2)$.

Meanwhile, the Werner state in Eq. (6) has an equivalent form,

$$\rho_W(F) = \frac{1}{4}\left[\mathbb{I}\otimes\mathbb{I} + \frac{4F-1}{3}(\sigma_1\otimes\sigma_1 - \sigma_2\otimes\sigma_2 + \sigma_3\otimes\sigma_3)\right],$$

and with the same optimal settings as the pure state, we have $\langle \boldsymbol{x}\otimes\boldsymbol{b}\rangle_{\max} = (4F-1)/3$. By taking $F=\cos^2(\gamma/2)$, the minimum error rate of the pure state after twirling is $\delta(\mathcal{T}(\Omega)) = \frac{2}{3}\sin^2(\gamma/2)$, which exactly gives the result in Eq. (7).

Geometric discord as a resource for QKG

It has been mentioned before that the effect of twirling shown in Eq. (7) indicates that entanglement is not the sufficient resource to realize the QKG protocol, and hence some other quantum resource beyond entanglement should be responsible for this. In the present work, we argue that quantum geometric discord may be viewed as this kind of quantum resource. Our argument is based on the following two aspects.

(i) For the general two-qubit states, we have the following lemma.

Lemma 1. *The geometric discord for a general two-qubit state, $\mathcal{D}_g(\rho)$, is bounded by two optimal values $\delta^{\boldsymbol{x}}_{min}(\rho)$ and $\delta^{\boldsymbol{y}}_{min}(\rho)$ such that*

$$\mathcal{D}_{\mathrm{g}}(\rho) \le \left[\frac{1}{2} - \delta^{\boldsymbol{x}}_{\min}(\rho)\right]^2 + \left[\frac{1}{2} - \delta^{\boldsymbol{y}}_{\min}(\rho)\right]^2. \tag{9}$$

Proof: To verify this relation, we should recall the definition of the geometric discord as the first step. If Alice performs an arbitrary projective measurement $\{\Pi^a_i\}$ on ρ, the final state of the joint system is $\chi_\rho = \sum_i \Pi^a_i\otimes\mathbb{I}\rho\Pi^a_i\otimes\mathbb{I}$. Usually, χ_ρ is regarded as the classic-quantum (CQ) state. With the squared Hilbert-Schmidt norm, $||A||^2=\mathrm{Tr}(AA^\dagger)$, the geometric discord is defined as $\mathcal{D}_{\mathrm{g}}(\rho) = \min_{\Pi^a}\left\|\rho-\chi_\rho\right\|^2$[16]. Following the result in Ref. [17], this quantity can also be expressed as the difference of two purities,

$$\mathcal{D}_{\mathrm{g}}(\rho) = \|\rho\|^2 - \max_{\Pi^a}\left\|\chi_\rho\right\|^2. \tag{10}$$

Now, we introduce a special CQ-state $\widetilde{\chi}_\rho$,

$$\widetilde{\chi}_\rho = \frac{1}{4}\left(\mathbb{I}\otimes\mathbb{I} + x_3\sigma_3\otimes\mathbb{I} + y_3\mathbb{I}\otimes\sigma_3 + \sum_{j=1}^{3}T_{3j}\sigma_3\otimes\sigma_j\right), \tag{11}$$

and obviously, this is the final state after that the projective measurement ($\Pi_1 = |\uparrow\rangle\langle\uparrow|$, $\Pi_2 = |\downarrow\rangle\langle\downarrow|$) is performed by Alice. With the definition in Eq. (10), one has $\mathcal{D}_{\mathrm{g}}(\rho) \le \|\rho\|^2 - \left\|\widetilde{\chi}_\rho\right\|^2$. By jointing it with the Eqs. (3) and (8) and the relation

$$4\left(\|\rho\|^2 - \left\|\widetilde{\chi}_\rho\right\|^2\right) = \sum_{j=1}^{3}T^2_{1j} + \sum_{j=1}^{3}T^2_{2j},$$

the result in Eq. (9) is easily obtained.

Considering a subset of the two-qubit state where the two correlation functions $\langle \boldsymbol{x}\otimes\boldsymbol{b}\rangle$ and $\langle \boldsymbol{y}\otimes\boldsymbol{b}'\rangle$ have the same maximum value, say $\langle \boldsymbol{x}\otimes\boldsymbol{b}\rangle_{\max} = \langle \boldsymbol{y}\otimes\boldsymbol{b}'\rangle_{\max}$, we get a relation between the error rate and the geometric discord,

$$\delta_{\min}(\rho) \le \frac{1}{2}\left(1 - \sqrt{2\mathcal{D}_{\mathrm{g}}(\rho)}\right). \tag{12}$$

The equality is saturated if $\widetilde{\chi}_\rho$ is the closest CQ-state to ρ.

As an example, we focus on the so-called X-type state,

$$\rho_X = \begin{pmatrix} \rho_{11} & 0 & 0 & \rho_{14}e^{i\gamma_{14}} \\ 0 & \rho_{22} & \rho_{23}e^{i\gamma_{23}} & 0 \\ 0 & \rho_{23}e^{-i\gamma_{23}} & \rho_{33} & 0 \\ \rho_{14}e^{-i\gamma_{14}} & 0 & 0 & \rho_{44} \end{pmatrix}, \tag{13}$$

where $\rho_{ij}(i, j = 1, 2, 3, 4)$ and γ_{ij} are real positive numbers. The X-states constitute a subclass of the general two-qubit state in Eq. (1) with $T_{13} = T_{23} = T_{31} = T_{32} = 0$. Now, the special CQ-state, $\widetilde{\chi}_\rho$, should be

$$\widetilde{\chi}_\rho = \frac{1}{4}\left(\mathbb{I} \otimes \mathbb{I} + x_3\sigma_3 \otimes \mathbb{I} + y_3\mathbb{I} \otimes \sigma_3 + T_{33}\sigma_3 \otimes \sigma_3\right). \tag{14}$$

As one of the main results given by Bellomo *et al.*[17], $\widetilde{\chi}_\rho$ in Eq. (14) should be the closest CQ-state to the state ρ_X in Eq. (13) if $k_1 \leqslant k_3$, where

$$\begin{aligned} k_1 &= 4(\rho_{14}^2 + \rho_{23}^2), \\ k_3 &= 2[(\rho_{11} - \rho_{33})^2 + (\rho_{22} - \rho_{44})^2]. \end{aligned} \tag{15}$$

(ii) The effect in Eq. (7) may be well explained by the fact that twirling increases the geometric discord of a pure state. This result is supported by the following two lemmas.

Lemma 2. *For a pure state or a Werner state of a bipartite system, the minimal error rate of the key is*

$$\delta_{\min} = \frac{1}{2}\left(1 - \sqrt{2\mathcal{D}_g(\rho)}\right).$$

Proof. It is easy to see that both the Werner state in Eq. (6) and the pure state in Eq. (4) belong to the so-called X-type states. For the pure state, the quantities in Eq. (15) are $k_1 = \cos^2\gamma$, $k_3 = (1 + \sin^2\gamma)$, and $\langle \mathbf{x} \otimes \mathbf{b}\rangle_{\max} = \langle \mathbf{y} \otimes \mathbf{b}'\rangle_{\max} = \cos\gamma$, while for the Werner state, $k_1 = k_3 = (4F - 1)^2/9$, and $\langle \mathbf{x} \otimes \mathbf{b}\rangle_{\max} = \langle \mathbf{y} \otimes \mathbf{b}'\rangle_{\max} = (4F - 1)/3$. It is obvious that Eq. (12) is saturated for both the pure state and the Werner state, which completes the proof.

Lemma 3. *For a pure state in* Eq. (4) *and the Werner state produced by this state subjected to* $U \otimes U^*$ *twirling, the entanglement is the same, while the geometric discord is increased.*

Proof. It is well known that twirling is an irreversible operation, and therefore never increases the entanglement of the state[41]. To verify that the entanglement of a pure state is unchanged after a twirling procedure, recall that the entanglement of formation (EoF) is a well-defined measure of the entanglement for a two-qubit state ρ[46]

$$E[\rho] = H_2\left(\frac{1 + \sqrt{1 - \mathcal{C}^2(\rho)}}{2}\right),$$

where $H_2(x) = -x\log_2 x - (1 - x)\log_2(1 - x)$ is the binary entropy and $\mathcal{C}(\rho)$ is the concurrence of the state ρ. Direct calculation shows that, for the pure state in Eq. (4) and the Werner state in Eq. (6), $\mathcal{C}(\Omega(\gamma)) = \mathcal{C}\left(\rho_W\left(\cos^2\frac{\gamma}{2}\right)\right) = \cos\gamma$. Therefore, $E[\Omega] = E[\mathcal{T}(\Omega)]$, which means the entanglement is the same.

On the other hand, with Bellomo's result[17], the geometric discord for X-state ρ_X is $\mathcal{D}_g(\rho_X) = 2(\rho_{14}^2 + \rho_{23}^2)$ for the case $k_1 \leqslant k_3$. By some simple algebra, one can obtain

$$\mathcal{D}_g(\rho_W) = \frac{1}{2}\left(\frac{2\cos\gamma + 1}{3}\right)^2, \quad \mathcal{D}_g(\Omega) = \frac{1}{2}\cos^2\gamma. \tag{16}$$

It is clear that the twirling operation on the pure state has increased the geometric discord

$$\mathcal{D}_g(\rho_W) \geqslant \mathcal{D}_g(\Omega). \tag{17}$$

Non-locality decreased by twirling

In Bell's celebrited work[47], it is known that non-locality is a quantum phenomenon which can not be explained by a local-Hidden-variables (LHV) theorem. Usually, one may introduce a Bell operator $\hat{B}$ and calculate its expectation $\langle\hat{B}\rangle$ with the LHV theory. With a carefully chosen $\hat{B}$, one may find a bound C_0,

or equvalently, the Bell inequality $\langle\hat{B}\rangle^{\mathrm{LHV}} \leq C_0$ should hold in the LHV theorem. For an example, for the two-qubit states, one may choose $\hat{B}$ as

$$\hat{B} = \sigma_{\boldsymbol{a}} \otimes \frac{\sigma_{\boldsymbol{b}} + \sigma_{\boldsymbol{b}'}}{2} + \sigma_{\boldsymbol{a}'} \otimes \frac{\sigma_{\boldsymbol{b}} - \sigma_{\boldsymbol{b}'}}{2} \tag{18}$$

where $\boldsymbol{a}$, $\boldsymbol{a}'$, $\boldsymbol{b}$, and $\boldsymbol{b}'$ are free unit vectors in the Bloch sphere, and one may get $\langle\hat{B}\rangle^{\mathrm{LHV}} \leq 1$, the famous Clauser-Horne-Shimony-Holt (CHSH) inequality[48].

It has been shown in Werner's work[40] that the non-locality is an independent quantum correlation besides the entanglement, and then one may conject that in the QKG task the non-locality and the entanglement can be taken as the sufficient resources. To check this conjecture, we need a strict way to calculate the non-locality for a given two-qubit state, and in this paper, the non-locality of a given state ρ is quantified by its ability to violate the CHSH inequality,

$$\Delta(\rho) = \max_{\boldsymbol{a},\boldsymbol{a}',\boldsymbol{b},\boldsymbol{b}'} \mathrm{Tr}[\rho\hat{B}]. \tag{19}$$

Lemma 4. *The non-locality is decreased by twirling,* $\Delta(\mathcal{T}(\rho)) \leq \Delta(\rho)$.

Proof: The twirling procedure in Eq. (5) can be also realized with a set of selected unitary transformations $U \in \{U_i\}_{i=1}^{M}$ [41],

$$\mathcal{T}(\rho) = \frac{1}{M}\sum_{i=1}^{M}(U_i \otimes U_i^*)\,\rho\,(U_i \otimes U_i^*)^{\dagger}. \tag{20}$$

Denote the optimal Bell operator for $\Delta(\mathcal{T}(\rho))$ by $\hat{B}_{\mathrm{opt}}$, and then

$$\Delta(\mathcal{T}(\rho)) = \mathrm{Tr}\left[\mathcal{T}(\rho)\hat{B}_{\mathrm{opt}}\right]. \tag{21}$$

Introduce $\hat{B}_i = (U_i \otimes U_i^*)^{\dagger}\hat{B}_{\mathrm{opt}}(U_i \otimes U_i^*)$, and one can obtain $\Delta(\mathcal{T}(\rho)) = \frac{1}{M}\sum_{i=1}^{M}\mathrm{Tr}[\rho\hat{B}_i]$ from Eqs. (20) and (21). With the fact that $\mathrm{Tr}[\rho\hat{B}_i] \leqslant \max_{\boldsymbol{a},\boldsymbol{a}',\boldsymbol{b},\boldsymbol{b}'}\mathrm{Tr}[\rho\hat{B}]$ and the definition in Eq. (19), we shall arrive at the desired result.

Based on this, we shall show that the conjecture above does not hold. The reason is quite clear: In the twirling process, both the non-locality and the entanglement is non-increased, and therefore they can not be viewed as the resource of effect in Eq. (7).

Other cases where twirling reduces the error rate

In the BB84 scheme, Alice prepares particles in a random sequence of the four states, $\frac{1}{\sqrt{2}}(|\uparrow\rangle \pm |\downarrow\rangle)$ and $\frac{1}{\sqrt{2}}(|\uparrow\rangle \pm i|\downarrow\rangle)$, and sends them to Bob. Suppose Eve, an eavesdropper, use a quantum cloning machine (QCM) to clone these states. The optimal QCM of Eve is described by a unitary transformation U for the jointed system of Bob and Eve[49],

$$\begin{aligned} &\mathrm{U}|\uparrow\rangle_B|\uparrow\rangle_E \rightarrow |\uparrow\rangle_B|\uparrow\rangle_E, \\ &\mathrm{U}|\downarrow\rangle_B|\uparrow\rangle_E \rightarrow \sin\alpha|\uparrow\rangle_B|\downarrow\rangle_E + \cos\alpha|\downarrow\rangle_B|\uparrow\rangle_E, \end{aligned} \tag{22}$$

where the free parameter α is constrained by $0 \leq \alpha \leq \pi/2$. The effect of the optimal QCM on Bob's state can be represented by an amplitude damping channel $\varepsilon_{\mathrm{AD}}$ with the Kraus operators[50],

$$E_0 = \begin{pmatrix} 1 & 0 \\ 0 & \cos\alpha \end{pmatrix}, E_1 = \begin{pmatrix} 0 & \sin\alpha \\ 0 & 0 \end{pmatrix}. \tag{23}$$

Correspondingly, the scenario discussed above is equivalent to our QKG scheme where a state $\overline{\rho}$,

$$\overline{\rho} = (\mathbb{I} \otimes \varepsilon_{\mathrm{AD}})\Phi^{+}, \tag{24}$$

has been applied to generate the randomly distributed keys. For convenience, we rewrite $\overline{\rho}$ with an explicit form,

$$\overline{\rho} = \frac{1}{2}\begin{pmatrix} 1 & 0 & 0 & \cos\alpha \\ 0 & 0 & 0 & 0 \\ 0 & 0 & \sin^2\alpha & 0 \\ \cos\alpha & 0 & 0 & \cos^2\alpha \end{pmatrix}, \tag{25}$$

and, obviously, it belongs to the X-type state defined Eq. (13). With Eq. (15), we get $k_1 = \cos^2\alpha$ and $k_3 = \cos^4\alpha$. For the present case, $k_1 \geq k_3$, the geometric discord should be

$$\mathcal{D}_g(\overline{\rho}) = (\overline{\rho}_{14} - \overline{\rho}_{23})^2 + \frac{1}{2}\Big[(\overline{\rho}_{11} - \overline{\rho}_{33})^2 + (\overline{\rho}_{22} - \overline{\rho}_{44})^2\Big], \tag{26}$$

a result given by Bellomo *et al.*[17]. By jointing it with Eq. (24), we shall get $\mathcal{D}_g(\overline{\rho}) = \frac{1}{4}(\cos^2\alpha + \cos^4\alpha)$.

Meanwhile, with the equivalent form of $\overline{\rho}$,

$$\overline{\rho} = \frac{1}{4}[\mathbb{I}\otimes\mathbb{I} + \sin^2\alpha\mathbb{I}\otimes\sigma_3 + \cos^2\alpha\sigma_3\otimes\sigma_3 + \cos\alpha(\sigma_1\otimes\sigma_1 - \sigma_2\otimes\sigma_2)],$$

we can obtain $\langle \boldsymbol{x}\otimes\boldsymbol{b}\rangle_{\max} = \langle \boldsymbol{y}\otimes\boldsymbol{b}'\rangle_{\max} = \cos\alpha$ with the optimal settings $\boldsymbol{b} = (1, 0, 0)$ and $\boldsymbol{b}' = (0, -1, 0)$. By putting it back into Eq. (3), the minimum error rate of $\overline{\rho}$ is known to be $\delta(\overline{\rho}) = \sin^2\frac{\alpha}{2}$.

When $\overline{\rho}$ is subjected to twirling, it produce a Werner state, $\mathcal{T}(\overline{\rho}) = \rho_W(F)$, with $F = \cos^2\frac{\alpha}{2}$. With a simple derivation, one may get $\mathcal{D}_g(\mathcal{T}(\overline{\rho})) = \frac{1}{2}\left(\frac{2\cos\alpha+1}{3}\right)^2$ and $\delta(\mathcal{T}(\overline{\rho})) = \frac{2}{3}\sin^2(\alpha/2)$. One can see that, after the state $\overline{\rho}$ is subjected to twirling, the error rate will be reduced by a factor of 2/3 while its geometric discord is also increased,

$$\delta(\mathcal{T}(\overline{\rho})) = \frac{2}{3}\delta(\overline{\rho}),\ \mathcal{D}_g(\mathcal{T}(\overline{\rho})) \geq \mathcal{D}_g(\overline{\rho}). \tag{27}$$

Another example of the two-qubit state, where the error rate of the key can be effectively decreased by twirling, is

$$\overline{\rho} = (\mathbb{I}\otimes\varepsilon_{\mathrm{PD}})\Phi^+ \tag{28}$$

where $\varepsilon_{\mathrm{PD}}$ denotes a phase damping channel[1]. The Kraus operators of $\varepsilon_{\mathrm{PD}}$ are $E_0 = \cos(\beta/2)\mathbb{I}$ and $E_1 = \sin(\beta/2)\sigma_3$ ($0 \leq \beta \leq \pi/2$). It can be taken as a model for the situation where a maximally entangled state Φ^+ is subjected to partial decoherence[2]. With the explicit form

$$\overline{\rho} = \frac{1}{2}\begin{pmatrix} 1 & 0 & 0 & \cos\beta \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ \cos\beta & 0 & 0 & 1 \end{pmatrix}, \tag{29}$$

one may check that it belongs to the X-type states with $k_1 \leq k_3$. After the twirling has been performed, it produce a Werner state with $F = \cos^2(\beta/2)$. With a simple calculation, we get the results: $\mathcal{D}_g(\overline{\rho}) = \frac{1}{2}\cos^2\beta$, $\delta(\overline{\rho}) = \sin^2(\beta/2)$, $\mathcal{D}_g(\mathcal{T}(\overline{\rho})) = \frac{1}{2}\left(\frac{2\cos\beta+1}{3}\right)^2$ and $\delta(\mathcal{T}(\overline{\rho})) = \frac{2}{3}\sin^2(\beta/2)$. Obviously, the the relations in Eq. (27) also hold.

In the work of Horodeckis'[42], it has been proven that the twirling of state $\overline{\rho} = (\mathbb{I}\otimes\varepsilon)\Phi^+$, is equivalent to the twirling of the channel ε,

$$\mathcal{T}(\overline{\rho}) = (\mathbb{I}\otimes\mathcal{T}(\varepsilon))\Phi^+ \tag{30}$$

where $\mathcal{T}(\varepsilon)$ is a depolarizing channel by performing twirling on the initial channel ε. Since the scheme for the twirling of the quantum channel has been developed in recent years[43–45], one may realize the QKG tasks with $\overline{\rho}$ (given in Eq. (24) or Eq. (28)) and $\mathcal{T}(\overline{\rho})$, respectively, and the effect of twirling estimated in Eq. (27), $\delta(\mathcal{T}(\overline{\rho})) = \frac{2}{3}\delta(\overline{\rho})$, can be observed in experiments.

Conclusions and Summaries

In the present work, with the developed QKG scheme, we have demonstrated that twirling can efficiently reduce the error rate of the key generated by some given two-qubit states and argued that the quantum geometric discord may be taken as a necessary resource for the QKG protocol.

From the definition in Eq. (5), we see that twirling is a series of bi-local operations, and it can increase the geometric discord of pure states. It should be noticed that this property of twirling has not been revealed in previous works. Specifically, it has been shown that geometric measure of quantumness of multipartite systems with arbitrary dimension cannot increase under any local quantum channel, if the initial state is pure[51]. However, as it is shown in Eq. (17), the geometric discord is increased when the pure state is subjected to twirling.

Besides the pure states, we also find another two types of mixed states where the twirling can increase the geometric discord and decrease the error rate at the same time. Actually, under which conditions the twirling may increase the geometric discord of the general states is still an open question. Even for the arbitrary two-qubit state, the conditions for applying the twirling procedure to increase the geometric discord and reduce the error rate of the generated key are still unknown. We expect that our results could lead to further theoretical or experimental consequences.

References

1. Nielsen, M. A. & Chuang, I. L. *Quantum Computation and Quantum information*, (Cambridge University Press, Cambridge, England, 2000).
2. Ollivier, H. & Zurek, W. H. Quantum Discord: A Measure of the Quantumness of Correlations. *Phys. Rev. Lett.* **88,** 017901 (2001).
3. Henderson, L. & Vedral, V. Classical, quantum and total correlations. *J. Phys. A* **34,** 6899 (2001).
4. Horodecki, R., Horodecki, P., Horodecki, M. & Horodecki, K. Quantum entanglement. *Rev. Mod. Phys.* **81,** 865 (2009).
5. Pirandola, S. Quantum discord as a resource for quantum cryptography. *Sci. Rep.* **4,** 6956 (2014).
6. Datta, A., Shaji, A. & Caves, C. M. Quantum Discord and the Power of One Qubit. *Phys. Rev. Lett.* **100,** 050502 (2008).
7. Madhok, V. & Datta, A. Interpreting quantum discord through quantum state merging. *Phys. Rev. A* **83,** 032323 (2011).
8. Cavalcanti, D. *et al.* Operational interpretations of quantum discord. *Phys. Rev. A* **83,** 032324 (2011).
9. Dakic, B. *et al.* Quantum discord as resource for remote state preparation. *Nature Phys.* **8,** 666 (2012).
10. Luo, S. Quantum discord for two-qubit systems. *Phys. Rev. A* **77,** 042303 (2008).
11. Luo, S. & Fu, S. Geometric measure of quantum discord. *Phys. Rev. A* **82,** 034302 (2010).
12. Huang, Y. Quantum discord for two-qubit X states: Analytical formula with very small worst-case error. *Phys. Rev. A* **88,** 014302 (2013).
13. Ali, M., Rau, A. R. P. & Alber, G. Quantum discord for two-qubit X states. *Phys. Rev. A* **81,** 042105 (2010).
14. Ali, M., Rau, A. R. P. & Alber, G. Erratum: Quantum discord for two-qubit X states [Phys. Rev. A 81, 042105 (2010)], *Phys. Rev. A* **82,** 069902 (2010).
15. Modi, K., Paterek, T., Son, W., Vedral, V. & Willimson, M. Unified View of Quantum and Classical Correlations. *Phys. Rev. Lett.* **104,** 080501 (2010).
16. Dakic, B., Vedral, V. & Brukner, C. Necessary and Sufficient Condition for Nonzero Quantum Discord. *Phys. Rev. Lett.* **105,** 190502 (2010).
17. Bellomo, B. *et al.* Unified view of correlations using the square-norm distance. *Phys. Rev. A* **85,** 032104 (2012).
18. Galve, F., Plastina, F., Paris, M. G. A. & Zambrini, R. Discording Power of Quantum Evolutions, *Phys. Rev. Lett.* **110,** 010501 (2014).
19. Lang, M. D. & Caves, C. M. Quantum Discord and the Geometry of Bell-Diagonal States. *Phys. Rev. Lett.* **105,** 150501 (2010).
20. Streltsov, A., Kampermann, H. & Bruß, D. Linking Quantum Discord to Entanglement in a Measurement. *Phys. Rev. Lett.* **106,** 160401 (2011).
21. Piani, M. *et al.* All Nonclassical Correlations Can Be Activated into Distillable Entanglement, *Phys. Rev. Lett.* **106,** 220403 (2011).
22. Zurek, W. H. Quantum discord and Maxwell's demons. *Phys. Rev. A* **67,** 012320 (2003).
23. Girolami, D. & Adesso, G. Quantum discord for general two-qubit states: Analytical progress. *Phys. Rev. A* **83,** 052108 (2011).
24. Cen, L.-X., Li, X.-Q., Shao, J. & Yan, Y. Quantifying quantum discord and entanglement of formation via unified purifications. *Phys. Rev. A* **83,** 054101 (2011).
25. Zhou, T., Cui, J. & Long, G. L. Measure of nonclassical correlation in coherence-vector representation. *Phys. Rev. A* **84,** 062105 (2011).
26. You, B. & Cen, L.-X. Necessary and sufficient conditions for the freezing phenomena of quantum discord under phase damping. *Phys. Rev. A* **86,** 012102 (2012).
27. Rahimi-Keshari, S., Caves, C. M. & Ralph, T. C. Measurement-based method for verifying quantum discord. *Phys. Rev. A* **87,** 012119 (2013).
28. Xu, J.-S. *et al.* Experimental Recovery of Quantum Correlations in Absence of System-Environment Back-Action. *Nat. Commun.* **4,** 2851 (2013).
29. Aaronson, B., Lo Franco, R. & Adesso, G. Comparative investigation of the freezing phenomena for quantum correlations under nondissipative decoherence. *Phys. Rev. A* **88,** 012120 (2013).
30. Bellomo, B., Lo Franco, R. & Compagno, G. Dynamics of geometric and entropic quantifiers of correlations in open quantum systems. *Phys. Rev. A* **86,** 012312 (2012).
31. Pirandola, S. *et al.* Optimality of Gaussian Discord. *Phys. Rev. Lett.* **113,** 140405 (2014).
32. Li, H., Li, Y.-S., Wang, S. H. & Long, G. L. Characterizing Quantum Correlations in Arbitrary Dimensional Bipartite Systems Using Hurwitz's Theory. *Commun. Theor. Phys.* **61,** 273 (2014).
33. Doustimotlagh, N., Wang, S., You, C. & Long, G. L. Enhancement of quantum correlations between two particles under decoherence in finite-temperature environment. *EPL* **106,** 60003 (2014).
34. Zhang, P., You, B. & Cen, L.-X. Stabilized quantum coherence and remote state preparation in structured environments, Chinese Sci. *Bull.* **59,** 3841 (2014).
35. Gisin, N., Ribordy, G., Tittel, W. & Zbinden, H. Quantum cryptography. *Rev. Mod. Phys.* **74,** 145 (2002).
36. Bennett, C. H. & Brassard, G. in proceedings of IEEE international Conference on Computers, System, and Signal Processing, pages 175-179, IEEE, New York, 1984, Bangalore, India, December 1984.
37. Ekert, A. K. Quantum cryptography based on Bell's theorem. *Phys. Rev. Lett.* **67,** 661 (1991).
38. Bennett, C. H., Brassad, G. & Mermin, N. D. Quantum Cryptography without Bell's theorem. *Phys. Rev. Lett.* **68,** 557 (1992).
39. Wu, X. H. & Zhou, T. *Quantum discord for the general two-qubit cas*e. arXiv:1504.00129, to be published in Quantum Inf. Process.
40. Werner, R. F. Quantum states with Einstein-Podolsky-Rosen correlations admitting a hidden-variable model. *Phys. Rev. A* **40,** 4277 (1989).
41. Bennett, C. H., DiVincenzo, D. P., Smolin, J. A. & Wootters, W. K. Mixed-state entanglement and quantum error correction. *Phys. Rev. A* **54,** 3824 (1996).
42. Horodecki, M., Horodecki, P. & Horodecki, R. General teleportation channel, singlet fraction, and quasidistillation. *Phys. Rev. A* **60,** 1888 (1999).
43. Dankert, C., Cleve, R., Emerson, J. & Livine, E. Exact and approximate unitary 2-designs and their application to fidelity estimation. *Phys. Rev. A.* **80,** 012304 (2009).
44. Bendersky, A., Pastawski, F. & Paz, J. P. Selective and Efficient Estimation of Parameters for Quantum Process Tomography. *Phys. Rev. Lett.* **100,** 190403 (2008).
45. Schmiegelow, C. T., Bendersky, A., Larotonda, M. A. & Paz, J. P. Selective and Efficient Quantum Process Tomography without Ancilla, *Phys. Rev. Lett.* **107,** 100502 (2011).
46. Wootters, W. K. Entanglement of Formation of an Arbitrary State of Two Qubits. *Phys. Rev. Lett.* **80,** 2245 (1998).
47. Bell, J. S. On the problem of hidden variables in quantum mechanics. *Rev. Mod. Phys.* **38,** 447 (1964).
48. Clauser, J. F., Horne, M. A., Shimony, A. & Holt, R. A. Proposed experiment to test local hidden variable theories. *Phys. Rev. Lett.* **23,** 880 (1969).
49. Niu, C. S. & Griffith, R. B. Two-qubit copying machine for economical quantum eavesdropping. *Phys. Rev. A* **60,** 2764 (1999).
50. Wu, F. & Wu, X. H. Designing the optimal quantum cloning machine for qubit case. *Quantum Inf. Process.* **11,** 1 (2012).
51. Streltsov, A., Kampermann, H. & Bruß, D. Behavior of Quantum Correlations under Local Noise. *Phys. Rev. Lett.* **107,** 170502 (2011).

Acknowledgements
The authors are very grateful to Prof. L.-X. Cen for helpful discussions. This work was partially supported by the National Natural Science Foundation of China under the Grant No. 11405136, and the Fundamental Research Funds for the Central Universities of China A0920502051411-56.

Author Contributions
X.W. completed the calculation. X.W. and T.Z. wrote the manuscript text together. All authors reviewed the manuscript.

Additional Information
Competing financial interests: The authors declare no competing financial interests.

How to cite this article: Wu, X. and Zhou, T. Geometric discord: A resource for increments of quantum key generation through twirling. *Sci. Rep.* **5**, 13365; doi: 10.1038/srep13365 (2015).