Trusted quantum remote sensing based on self-testing of entangled states

Xing-Xiang Peng, Wen-Hao Zhang, Peng Yin, Gong-Chu Li, Lei Chen, Geng Chen,* Chuan-Feng Li,† and Guang-Can Guo
Chinese Academy of Sciences Key Laboratory of Quantum Information, University of Science and Technology of China, Hefei 230026, China and Chinese Academy of Sciences Center For Excellence in Quantum Information and Quantum Physics, University of Science and Technology of China, Hefei, Anhui 230026, China

(Received 3 September 2021; accepted 7 March 2022; published 25 March 2022)

In a typical scenario of quantum remote sensing, a server at the remote site sends the sensing information to the local site, so that the client there can make a diagnosis about the sensed field. In practice, the reliability of the sensing information may be undermined by kinds of errors, e.g., the imperfections of measurement devices or the attacks from a malicious eavesdropper. An alternative way to circumvent this problem is to encode the sensing information into entangled states, of which the form can be inferred in a device-independent manner, namely, self-testing. In this paper, we propose a protocol to make secure sensing of a parameter at the remote side. Upon receiving the remote sensing data, the local client can figure out the parameter range by inspecting the joint probabilities. In stark contrast, a malicious eavesdropper who is allowed to access all the remote data cannot either acquire the information of the parameter or cheat the client by replacing returned data with fake ones. We apply this protocol to a magnetic sensing scenario, and we show that the client can reliably estimate the strength range of the magnetic field, which could be intimately related to various mineral resources. Consequently, the client should not overslip any mineral resources by identifying the upper bound of magnetic strength. We also show that our protocol is valid even if the entangled states are mildly noisy.

DOI: 10.1103/PhysRevA.105.032615

I. INTRODUCTION

Quantum information processing [1,2] provides quantum advantages over its classical counterparts. In general, these advantages benefit from the quantum states, especially quantum entangled states, which are the cornerstones to realize more efficient computations [3,4], more secure cryptography [5–8], and more precise sensing [9–14].

Quantum measurement performed on the quantum states constitutes another indispensable ingredient to achieve these advantages in practice; however, quantum measurement normally suffers from two insurmountable faults, i.e., the imperfections of the measurement devices and the uncertainty about the dimensions of the system. In order to dispose of these two faults, "device-independent"(DI) protocols have kindled intense research since they are free of assuming the given dimension of each subsystem and exact quantum description of measurement devices [15]. In this case, we only need to perform projective measurements (PMs) and analyze the statistical probabilities. By testing the nonlocality with the recorded probabilities, one can certify the quantum state (up to local isometry), which is the so-called self-testing and was first raised by Mayers and Yao [16]. Recently, lots of theoretical and experimental efforts have been devoted to the self-testing of various entangled states [15–21]. Besides ensuring security in communication, the quantum information community attempts to incorporate security into quantum sensing scenarios, utilizing various quantum states. Recently, a delegated remote sensing method with built-in security has been proposed [22] and then experimentally verified by an experiment [23].

When a quantum state is used for sensing a physical parameter, normally the quantum state is coupled to an external field and the parameter is encoded into the state. To figure out the parameter, one has to measure the quantum state to learn its form. In this sense, by adapting self-testing to quantum sensing, it is in principle feasible to transfer the DI characteristics of the PMs into the estimation of a certain parameter in the quantum state. The DI feature of self-testing confers the quantum sensing ability to resist certain attacks and offers a trusted conclusion about the estimated parameter.

In this paper, we apply the idea of self-testing to a remote sensing scenario as diagramed in Fig. 1. Alice and Bob share entangled photon pairs and encode a remote parameter into the quantum states, and then implement self-testing of the outcome state to figure out the range of the parameter. Due to the DI characteristics of self-testing, the estimation of the parameter is impervious to attacks on the remote side, which helps Alice to make adequate decisions. As an example, our protocol can be used for remote sensing of the magnetic field, which should be generated by certain underground mineral resources. In such a scenario, Alice diagnoses that there is no mineral resource at Bob's location if only she observes sufficiently high nonlocality by combining the local measurement results of both sides. Therefore, Alice should not overslip any mineral resources, even an eavesdropper attack on the remote side to steal and replace all the local results there. Moreover, our protocol is robust to the imperfections of the

*chengeng@ustc.edu.cn
†cfli@ustc.edu.cn

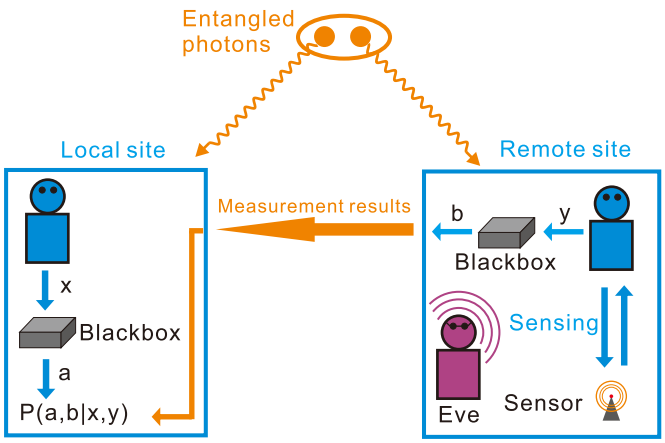

FIG. 1. Diagram for the trusted remote sensing protocol. Initially, Alice (local client) and Bob (remote server) share a pair of maximally entangled photons, which maximally violate certain Bell inequalities. Bob is assigned to make remote sensing with his photon, and his actions are limited to coupling the parameter with his photon, and implementing PMs with a black-box-like device, and then he sends these projection results to Alice via one-way classical communication. Alice also makes PMs with a black-box-like device, and then figures out the range of the sensed parameter via self-testing, by inspecting the violation achieved by joint probabilities $P(a, b|x, y)$ [(x, y) denotes the measurement settings on Alice's and Bob's sides, resulting in corresponding outcomes (a, b)]. A possible eavesdropper named Eve may invade the remote side and access all the projection results there. However, Eve cannot acquire any information of the parameter since the parameter is encoded as a nonlocal phase. Moreover, Eve cannot cheat Alice by replacing these results with fake ones, since Alice's decision is based on a sufficiently high violation, which cannot be faked with local operations.

shared entangled state, and the white noise merely reduces the probability to reach a conclusive diagnosis, while not the credibility of such a diagnosis.

We will first introduce self-testing in Sec. II A, describe our protocol in detail in Sec. II B, and finally show the simulated results in Sec. II C.

II. THEORY FRAMEWORK

A. Self-testing

In a self-testing scenario, Alice and Bob share some quantum states ρ. They want to certify that these quantum states are identical with a target state $|\varphi_{\text{tar}}\rangle$, while simply using a black-box-like measurement device. Their actions are limited to choosing measurement settings (x, y) and observing the corresponding outcomes (a, b), therefore the only available information for them is the conditional probabilities $P(a, b|x, y)$. In order to test the shared state, Alice and Bob have to rely on a Bell operator $\mathcal{B}$, the quantum bound of which can only be attained by the target state. Therefore, if $P(a, b|x, y)$ achieves the maximal violation of the Bell inequality, Alice and Bob can certify that their shared states are equal to $|\varphi_{\text{tar}}\rangle$ up to a local isometry [17,18].

Normally, $P(a, b|x, y)$ may not achieve the maximal violation and the difference between $|\varphi_{\text{tar}}\rangle$ and ρ is characterized by the extractability $\Xi(\rho \to |\varphi_{\text{tar}}\rangle)$, which is defined as the maximum fidelity taken over all possible quantum channels (completely positive trace-preserving maps) of appropriate input and output registers [24]. The robustness bound of self-testing $\mathcal{Q}_{\varphi_{\text{tar}},\mathcal{B}}(\beta)$ quantifies the lowest possible extractability when acquiring a nonmaximal violation β of $\mathcal{B}$. In other words, if the observed expected value of $\mathcal{B}$ is β, the shared state ρ satisfies [24]

$$\Xi(\rho \to |\varphi_{\text{tar}}\rangle) \geqslant \mathcal{Q}_{\varphi_{\text{tar}},\mathcal{B}}(\beta), \tag{1}$$

where $\mathcal{Q}_{\varphi_{\text{tar}},\mathcal{B}}(\beta)$ represents the lowest extractability from $|\varphi_{\text{tar}}\rangle$, when one observes a violation β of the inequality $\mathcal{B}$. In Refs. [25,26], a self-testing protocol has been proposed for all pure two-qubit states written as

$$|\varphi(\theta_{\text{tar}})\rangle = \cos(\theta_{\text{tar}})|HH\rangle + \sin(\theta_{\text{tar}})|VV\rangle. \tag{2}$$

It has proven that any state in the form of Eq. (2) maximally violates the tilted Clauser-Horne-Shimony-Holt (CHSH) Bell inequalities [27] written as

$$\begin{aligned}\mathcal{B}[\alpha(\theta_{\text{tar}})] = {} & \alpha(\theta_{\text{tar}})A_0 + A_0(B_0 + B_1) \\ & + A_1(B_0 - B_1) \leqslant 2 + \alpha(\theta_{\text{tar}}),\end{aligned} \tag{3}$$

where $0 \leqslant \alpha(\theta_{\text{tar}}) \leqslant 2$ and $0 \leqslant \theta_{\text{tar}} \leqslant \pi/4$. In this family of inequalities, A_x $(x \in \{0, 1\})$ represents the two binary-outcome measurements on Alice's side, and B_y $(y \in \{0, 1\})$ represents that on Bob's side. The quantum bound of $\mathcal{B}[\alpha(\theta_{\text{tar}})]$ is calculated as $\beta^{\mathcal{Q}} = \sqrt{8 + 2\alpha^2(\theta_{\text{tar}})}$ with $\alpha(\theta_{\text{tar}}) = 2/\sqrt{1 + 2\tan^2(2\theta_{\text{tar}})}$. The observables used to achieve the quantum bound are

$$\begin{aligned}& A_0 = \sigma_3, \quad A_1 = \sigma_1, \\ & B_0 = \cos(\mu)\sigma_3 + \sin(\mu)\sigma_1, \quad B_1 = \cos(\mu)\sigma_3 - \sin(\mu)\sigma_1,\end{aligned} \tag{4}$$

with $\tan(\mu) = \sin(2\theta_{\text{tar}})$, and σ_1, σ_2, and σ_3 are three Pauli matrices. It is easy to see that, if $\theta_{\text{tar}} = \pi/4$, Eq. (3) reduces to the standard CHSH Bell inequality [28,29].

If $P(a, b|x, y)$ achieves the quantum bound of $\mathcal{B}[\alpha(\theta_{\text{tar}})]$, it can be certified that ρ can be determinately extracted to $|\varphi(\theta_{\text{tar}})\rangle$. If Alice and Bob observe a violation β below $\beta^{\mathcal{Q}}$, they can still conclude that ρ should be different from $|\varphi(\theta_{\text{tar}})\rangle$ with a specific distance, which is decided by the self-testing bound formalized in Refs. [19,21].

B. Protocol

By introducing self-testing into the remote sensing as diagramed in Fig. 1, Alice and Bob can make a trusted diagnosis since the initial maximally entangled state will not be changed if the sensed magnetic field is sufficiently weak, and thus the observed violation of the CHSH inequality can approach $\beta^{\mathcal{Q}}$. Observing a smaller violation could result from a stronger magnetic field or, failing to observe the maximal violation, in these cases, Alice makes the exploitation to ensure that no mineral is missed. The optical realization of our protocol is given in Fig. 2. Alice prepares a maximally entangled photon pair with a beta barium borate crystal, then she sends one photon to Bob. Alice and Bob can encode the strength of the magnetic field into the shared entangled states, and thus the maximally entangled Bell states

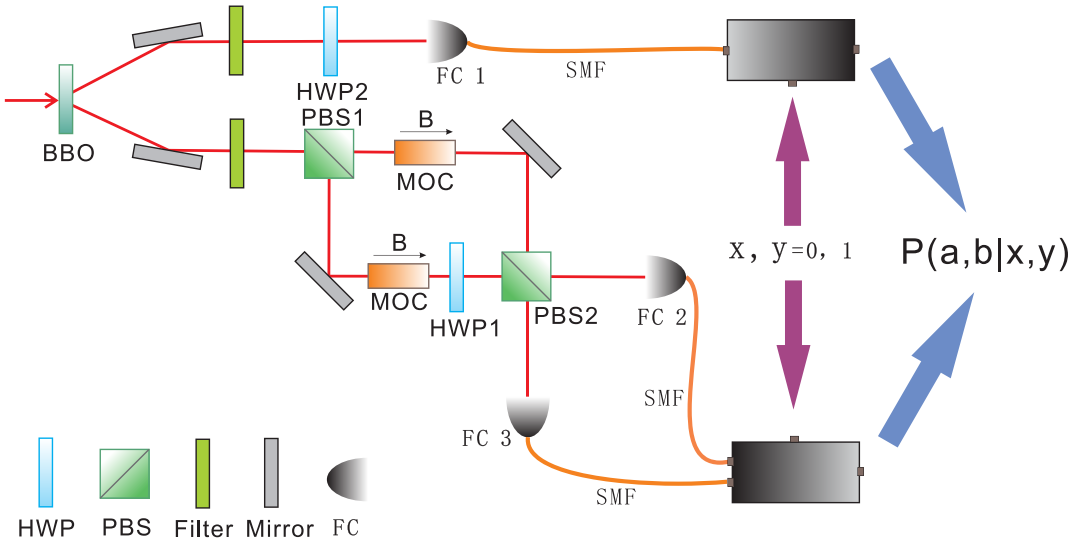

FIG. 2. Optical realization of the trusted remote sensing protocol. On Alice's side (local site), the maximally entangled photon pairs are generated by pumping a nonlinear crystal. One of the photons is sent to Bob (remote site) to sense the strength of the magnetic field, the direction of which can be predetermined. The existence of an abnormal magnetic field may cause the photon pairs to evolve into partially entangled states after Bob's photons pass the sensor containing a Mach-Zehnder interferometer (MZI), which consists of two polarized beam splitters (PBS), two magnetic-optical crystals (MOC), and a half-wave plate (HWP). PBS1 splits $|H\rangle$ and $|V\rangle$ polarized components into two arms of MZI. Being parallel with the abnormal magnetic field, MOC in the upper arm rotates $|H\rangle$ to $\cos(\theta)|H\rangle + \sin(\theta)|V\rangle$. On the lower arm, MOC rotates $|V\rangle$ to $\cos(\theta)|V\rangle - \sin(\theta)|H\rangle$, and then transforms to $\cos(\theta)|H\rangle - \sin(\theta)|V\rangle$ by following a HWP. On Alice's side, HWP2 is set as $\pi/4$. As a result, the photon pairs evolve to $\cos\theta|HH\rangle + \sin(\theta)|VV\rangle$ ($\cos\theta|HV\rangle - \sin(\theta)|VH\rangle$) when Bob's photons exit MZI and enter FC2 (FC3). Both Alice and Bob can perform PMs with their black-box-like devices. Finally, Alice needs to analyze statistical results to infer the form of the outcome states and estimate the strength of the magnetic field. FC, fiber collimator; SMF, single mode fiber; BBO, beta barium borate crystal.

$|\varphi(\pi/4)\rangle = \frac{1}{\sqrt{2}}(|HH\rangle + |VV\rangle)$ can be transformed to the partially entangled pure two-qubit state $|\varphi(\theta)\rangle = \cos(\theta)|HH\rangle + \sin(\theta)|VV\rangle$ or $\cos(\theta)|HV\rangle - \sin(\theta)|VH\rangle$ [$|H\rangle$ ($|V\rangle$) is the horizontal (vertical) polarized component of photons], which is admissible according to Nielsen's theorem [30]. The eventual states from Bob's two outcomes are different; however, they are equivalent states up to a local isometry. Finally, Alice needs to choose the one achieving higher violation based on measurement outcomes to make parameter estimation. Without loss of generality, suppose $\cos(\theta)|HH\rangle + \sin(\theta)|VV\rangle$ can achieve a higher violation in the following discussions.

In our scheme, this state transformation is realized by coupling the polarization of Bob's photon with its momentum through the sensed magnetic field. Denoting the strength of the magnetic field, the Verdet constant, and the length of the magnetic-optical crystals as B, V, and l, the Hamiltonian $H = \hbar k\delta(t - t_0)\hat{A}\hat{P}$ couples the system and the meter with strength $k = VBl/p_0$. Here, the photon momentum is $p_0 = \hbar 2\pi/\lambda_0 = \hbar\omega_0/c$, where λ_0 (ω_0) denotes the central wavelength (frequency) of incident light. $\hat{A} = |R\rangle\langle R| - |L\rangle\langle L|$ is the system operator with $|R\rangle$ ($|L\rangle$) representing the right (left) circularly polarized component of light, and $\hat{P}$ is the momentum operator of light. After the sensing, the rotating angle θ_B in the outcome state $|\varphi(\theta_B)\rangle$ is calculated as

$$\theta_B = VBl. \tag{5}$$

Since the strength of the magnetic field at the Earth's surface is much lower than 1×10^{-2} T, θ_B is much smaller than π.

After collecting the photons passing the Mach-Zehnder interferometer, Alice and Bob should carry out steps as follows.

(1) Alice and Bob perform PMs on $|\varphi(\theta_B)\rangle$ according to the input (x, y) of their black-box-like measurement devices. Bob sends his measurement results, and Alice needs to make coincidence detection upon receiving Bob's signal, meanwhile classifying them into two groups based on the clicks from the two outcome ports on Bob's side. Then Alice calculates the conditional probabilities $P(a, b|x, y)$.

(2) Alice tests various (tilted) CHSH inequalities with the conditional probabilities $P(a, b|x, y)$. She analyzes these two groups of statistics and chooses the one achieving higher violation to implement self-testing. From the maximal violation of a certain $\mathcal{B}[\alpha(\theta_{\text{tar}})]$ and the corresponding robustness bound, Alice infers the lowest extractability $\mathcal{Q}_{\varphi_{\text{tar}},\mathcal{B}}(\beta)$ of $|\varphi(\theta_B)\rangle$ from $|\varphi(\theta_{\text{tar}})\rangle$.

(3) From $\mathcal{Q}_{\varphi_{\text{tar}},\mathcal{B}}(\beta)$, Alice can derive the possible forms of $|\varphi(\theta_B)\rangle$, and hence the value of θ_B. Utilizing Eq. (5), Alice estimates the range of B from the possible values of θ_B.

Although the eventual states from Bob's two ports are different, it will not affect the result of self-testing if Alice can distinguish the signal from FC2 or FC3, because two eventual states are equivalent up to a local isometry, and produce the same statistics $p(a, b|x, y)$ in the self-testing experiment. Consider a worst-case scenario in which Eve replaces all Bob's results in order to conceal the fact that there is a mineral resource at the sensed location. In this case, Eve has to produce data nearly achieving β^Q, which implies B is approximately zero. However, his faked data cannot violate

the CHSH inequality, which is guaranteed by the nonlocality of the shared states. According to the strategy adopted by Alice, she will make an exploration when she observes these local correlations, and she will not be cheated by Eve. A faked lower violation indeed leads to extra but useless efforts made by Alice. However, Eve will not acquire significant benefits in this way, since her target is to make Alice miss the mineral. From Alice's side, missing a mineral causes more serious harm than making extra efforts. From this point of view, a faked lower violation is not considered as a kind of valid cheating.

C. Results

Considering the imperfections in the sensing processing, we assume the outcome state is approximately a pure entangled state, while mixed with a small amount of white noise [31], and the density matrix is written as

$$\rho_\eta(\theta_B) = \eta\frac{\mathbb{I}_4}{4} + (1-\eta)|\varphi(\theta_B)\rangle\langle\varphi(\theta_B)|, \tag{6}$$

where $\mathbb{I}_4$ represents the 4×4 identity, and η is the weight of white noise in the mixed state. If and only if η is sufficiently small, $\rho_\eta(\theta_B)$ can still attain a Bell violation β approaching the quantum bound of $\mathcal{B}[\alpha(\theta_B)]$ [32].

For a perfectly pure outcome state which is supposed in the form of $|\varphi(\theta_B)\rangle$, which necessarily maximally violates $\mathcal{B}[\alpha(\theta_B)]$, the value of θ_B can be uniquely determined to give an exact estimation of B. However, when the white noises are taken into account, the outcome states cannot attain the quantum bound of any inequality. In this case, for the implementation of self-testing, one has to search for the maximal violation $\beta_{\max}$ of a given $\mathcal{B}[\alpha(\theta_B)]$.

It has been proven in Ref. [27] that for any set of PMs performed on the state $|\varphi(\theta_B)\rangle$ the following inequality holds for a given $\mathcal{B}[\alpha(\theta_{\text{tar}})]$:

$$\begin{aligned}&\text{Tr}(\mathcal{B}[\alpha(\theta_{\text{tar}})]|\varphi(\theta_B)\rangle\langle\varphi(\theta_B)|)\\ &\leqslant \alpha(\theta_{\text{tar}})\cos(2\theta_B) + 2\sqrt{1+\sin^2(2\theta_B)}.\end{aligned} \tag{7}$$

In the sense that the white noise does not contribute to the violation of $\mathcal{B}[\alpha(\theta_{\text{tar}})]$, the total violation achieved by $\rho_\eta(\theta_B)$ can be calculated as

$$\begin{aligned}\beta = \text{Tr}\{\mathcal{B}[\alpha(\theta_{\text{tar}})]\rho_\eta(\theta_B)\} \leqslant (1-\eta)[\alpha(\theta_{\text{tar}})\cos(2\theta_B)\\ + 2\sqrt{1+\sin^2(2\theta_B)}],\end{aligned} \tag{8}$$

which can be saturated when the observables are selected to be those in Eq. (4), and the corresponding violation is denoted as $\beta_{\max}$.

In our protocol, β is maximized for a certain outcome state $\rho_\eta(\theta_B)$, by setting $l = 10$ cm and $V = 148.5$ rad/T m. Two paradigmatic values of B are selected as $B = 0.0616$ and 0.0012 T, and θ_B can be calculated from Eq. (5). By certifying $\beta_{\max}$ of a certain $\mathcal{B}[\alpha(\theta_{\text{tar}})]$, one can obtain $\mathcal{Q}_{\varphi_{\text{tar}},\mathcal{B}}(\beta_{\max})$ for a noisy $\rho_\eta(\theta_B)$. As shown in Fig. 3, by drawing a point on the robustness bound with the horizontal coordinate value equal to $\beta_{\max}$, $\mathcal{Q}_{\varphi_{\text{tar}},\mathcal{B}}(\beta_{\max})$ is identified as the vertical coordinate value of this point.

A nonunity $\mathcal{Q}_{\varphi_{\text{tar}},\mathcal{B}}(\beta_{\max})$ implies that $\rho_\eta(\theta_B)$ should be within a limited distance with $|\varphi(\theta_{\text{tar}})\rangle$, which restricts the value of θ_B in a certain range. The outcome states can be self-tested into either $|\varphi(\pi/4)\rangle$ with standard CHSH inequality $\mathcal{B}[\alpha(\pi/4)]$ or $|\varphi(\theta_B)\rangle$ with the tilted CHSH inequality $\mathcal{B}[\alpha(\theta_B)]$. As a result, θ_B can be jointly restricted by combining these two self-testing channels. For the two paradigmatic values of B, the estimated results for two different levels of white noise are investigated and given in Table I. As shown in Table I, the actual value of B in the first column is exactly within the estimated range by self-testing, which is given in the last column. We can set criterion for the existence of a mineral resource, and then Alice can adopt such a strategy that if the upper bound of the estimated range is below the criterion she diagnoses that there is no mineral there and abandons this location; otherwise, she will make an exploration there. In other words, the estimation of B is always larger than the real value. As a result, no matter what value of the criterion is preestablished, when Alice asserts that B is below the criteria, the actual value must be further lower than the criteria; otherwise, when the estimation surpasses the criteria, the actual value may still be lower than the criteria. This overestimation leads to extra efforts while not being cheated, since they never mistake a larger B as a lower one. In practice, the criterion can be determined from substantial experiences with nearly unity confidence; that is, the existence probability of mineral resources is nearly zero if the actual B is below the criterion. Without loss of generality, we can suppose the criterion are $B \geqslant 0.05$ T. When the actual value of B is 0.0616 T, as shown in the top four rows in Table I, the estimated upper bound is always larger than 0.05 T for the two levels of the white noise and the two self-testing channels. Consequently, Alice's decision is to make an exploration there and she will successfully discover the mineral resource. For a small value of B equal to 0.0012 T and a low noise level with $\eta = 0.001$, the estimated upper bound is 0.0392 and 0.0298 T for the two self-testing channels, respectively. In this case, Alice will abandon the exploration to avoid unnecessary efforts. When the noise level increases to $\eta = 0.005$, the estimation range exceeds 0.05 T for both self-testing channels, and Alice will make an unavailing exploration.

Apparently, a more noisy outcome state necessarily degrades the violation of the Bell inequality used for self-testing. Thereby, the tolerant degree of the noise is decided by the tightness of the self-testing bound, in the sense that a tighter bound will promise a higher $\mathcal{Q}_{\varphi_{\text{ref}},\mathcal{B}}(\beta_{\max})$, which leads to a tighter upper bound of B and a lower probability of unavailing explorations.

In our protocol, the remote field B changes the initial state to an outcome state. The stronger the field is, the more distinctly the state changes. The inferred outcome state can be estimated by self-testing, and then we can figure out the possible range of B. The tighter the robustness bound is, the closer the upper bound to the real value of B. The robustness bound for CHSH is intensively studied and optimized, and thus states slightly differing from the maximally entangled states can be well self-tested. The robustness bound for tilted CHSH is relatively less robust; however, if the initial state is distinctly changed, self-testing with the tilted CHSH inequality may provide better estimation since the outcome state

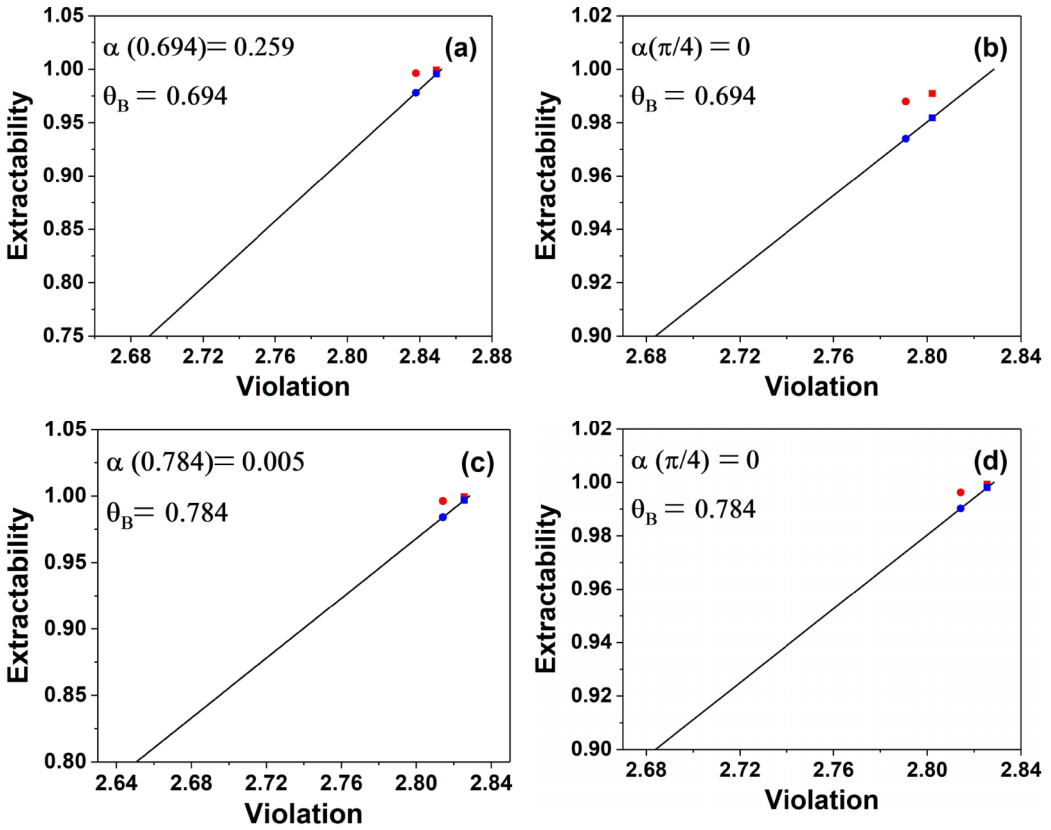

FIG. 3. Extractabilities against $\beta_{\max}$ when using different Bell inequalities. Two values of sensed B are investigated, yielding two different values of θ_B. The outcome state $\rho_\eta(\theta_B)$ is self-tested with two inequalities, namely, $\mathcal{B}[\alpha(\theta_{\text{tar}})]$ with $\theta_{\text{tar}} = \pi/4$ and θ_B, of which the target states are $|\varphi(\pi/4)\rangle$ and $|\varphi(\theta_B)\rangle$, respectively. The four subgraphs give the extractabilities for different θ_B and α, as labeled at the top left of each. The solid line in each subgraph is the robustness bound for corresponding $\mathcal{B}[\alpha(\theta_{\text{tar}})]$. Two different levels of noise, with η=0.005 and 0.001, are studied and the results are labeled by the circle and square dots in each subgraph. The red dots represent the real fidelity between the noisy state and the target states, while the blue dots on the robustness bound represent the lowest extractabilities from $\rho_\eta(\theta_B)$ to the target state.

approaches the maximum violation of these tilted inequalities. In Table I, the field is weak and the outcome state is only slightly different from the initial Bell state. As a result, the standard CHSH inequality offers a better estimation of the parameter; that is, the upper bound of the estimated range is closer to the real value of B.

In our protocol, Alice and Bob make coincidence detection of the photon pairs, and eventually they can figure out the parameter (strength of the field) through the statistical correlations of their results.

III. DISCUSSION

Previous works on self-testing are normally devoted to the DI characterization of entangled states, so they are implemented as preparing states and making PMs, eventually

TABLE I. The estimated range of B from the self-testing results of the outcome states. The outcome state $\rho_\eta(\theta_B)$ is jointly decided by θ_B and η, and can be self-tested to either $|\varphi(\theta_B)\rangle$ or $|\varphi(\pi/4)\rangle$. The fidelity between $\rho_\eta(\theta_B)$ and the target state is calculated and shown in the fifth column. The maximal violation $\beta_{\max}$ of $\mathcal{B}[\alpha(\theta_{\text{tar}})]$ achieved by $\rho_\eta(\theta_B)$ is given in the sixth column, and the lowest extractability $\mathcal{Q}_{\varphi_{\text{ref}},\mathcal{B}}(\beta_{\max})$ can thus be obtained from the robustness bound shown in Fig. 3. Since $\mathcal{Q}_{\varphi_{\text{ref}},\mathcal{B}}(\beta_{\max})$ is associated with the largest difference between θ_B and θ_{tar}, the range of θ_B can be identified together with that of B, as shown in the last column.

B (T)	θ_B(rad)	η	θ_{tar}(rad)	Fidelity	$\beta_{\max}$	$\mathcal{Q}_{\varphi_{\text{ref}},\mathcal{B}}(\beta_{\max})$	Estimated B (T)
0.0616	0.694	0.001	0.694	99.93%	2.8493	99.56%	0.0169–0.1063
0.0616	0.694	0.001	$\pi/4$	99.09%	2.8021	98.18%	−0.0911–0.0911
0.0616	0.694	0.005	0.694	99.63%	2.8379	97.80%	−0.0387–0.1619
0.0616	0.694	0.005	$\pi/4$	98.79%	2.7909	97.40%	−0.1090–0.1090
0.0012	0.784	0.001	0.784	99.93%	2.8256	99.35%	−0.0368–0.0392
0.0012	0.784	0.001	$\pi/4$	99.92%	2.8256	99.80%	−0.0298–0.0298
0.0012	0.784	0.005	0.784	99.63%	2.8143	98.41%	−0.0840–0.0863
0.0012	0.784	0.005	$\pi/4$	99.62%	2.8143	99.02%	−0.0667–0.0667

acquiring the fidelity of the tested state to the target state. In the current protocol, additional remote sensing is introduced and hence the initial probe state may evolve to a different one, and then by self-testing the outcome state we try to figure out the coupling parameter rather than the fidelity. Therefore, we aim to sense a parameter encoded during the dynamic of states, while self-testing aims to know the form of an invariable tested state. Moreover, due to the remote sensing scenario we consider, Alice and Bob can only make one-way classical communication and transmit the projection results from Bob to Alice unidirectionally.

Different from the secure communication problem, which can be well solved by quantum key distribution, our protocol resists the attacks on the remote side. In our protocol, the attacker named Eve can monitor all the results of Bob's projection, or even invade Bob's storage to replace Bob's data in order to cheat Alice. Consequently, Bob cannot adopt the method to directly measure the parameter and send the value encoded with the key, since Eve can know the value and replace it with a fake one. Alternatively, our protocol recurs to nonlocality of the shared probe states, because Eve cannot fake the nonlocality with local operations. For the same reason, we do not require authentication in our protocol, since Bob's knowledge is limited to the projection results while not the value of the parameter. In this case, even Eve is allowed to replace all the projection results that Bob sends to Alice, or Alice can only receive faked data from Eve; Eve still cannot mimic the maximal nonlocality.

In this paper, we show that the DI features in quantum information processing not only offer advantages in the measurement of quantum systems, but also can be applied to the estimation of physical quantities in a remote sensing scenario. Our protocol is partially DI; that is, the initial preparation and encoding process must be trusted, while the projective measurements are implemented in a DI way. When the studied quantity can be exactly encoded into the outcome quantum states from sensors, its value can be restricted within a special range by self-testing the outcome states into a certain target state. By implementing our trusted remote sensing, the upper bound of the quantity can be reliably determined, which is not affected by the errors in performing PMs, or even impervious to any possible disturbance from a malicious eavesdropper. When the quantity is the strength of a magnetic field created by some mineral resources, a reliable estimation about the maximal strength guarantees that no real mineral can be overslipped. We also study the robustness of our protocol to state imperfections, and the simulated results indicate that more imperfections merely lead to a looser upper bound of the estimation, while not reducing the credibility of the diagnosis about the absence of mineral resources.

ACKNOWLEDGMENTS

This work was supported by the National Key Research and Development Program of China (Grant No. 2017YFA0304100), National Natural Science Foundation of China (Grants No. 12122410, No. 11874344, No. 61835004, No. 61327901, No. 11774335, No. 91536219, and No. 11821404), the Fundamental Research Funds for the Central Universities (Grants No. WK2030000038 and No. WK2470000034).

[1] A. W. Harrow, A. Hassidim, and S. Lloyd, Quantum Algorithm for Linear Systems of Equations, Phys. Rev. Lett. **103**, 150502 (2009).

[2] L. M. K. Vandersypen, M. Steffen, G. Breyta, C. S. Yannoni, M. H. Sherwood, and I. L. Chuang, Experimental realization of Shor's quantum factoring algorithm using nuclear magnetic resonance, Nature (London) **414**, 883 (2001).

[3] P. W. Shor, Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer, SIAM J. Comput. **26**, 1484 (1997).

[4] L. K. Grover, Quantum Mechanics Helps in Searching for a Needle in a Haystack, Phys. Rev. Lett. **79**, 325 (1997).

[5] S. Wang, D.-Y. He, Z.-Q. Yin, F.-Y. Lu, C.-H. Cui, W. Chen, Z. Zhou, G.-C. Guo, and Z.-F. Han, Beating the Fundamental Rate-Distance Limit in a Proof-Of-Principle Quantum Key Distribution System, Phys. Rev. X **9**, 021046 (2019).

[6] C. H. Bennett and G. Brassard, Quantum cryptography: Public key distribution and coin tossing, in *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India* (IEEE, New York, 1984), p. 175.

[7] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, Experimental quantum cryptography, J. Cryptol. **5**, 3 (1992).

[8] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Quantum cryptography, Rev. Mod. Phys. **74**, 145 (2002).

[9] V. Giovannetti, S. Lloyd, and L. Maccone, Quantum enhanced measurements: Beating the standard quantum limit, Science **306**, 1330 (2004).

[10] V. Giovannetti, S. Lloyd, and L. Maccone, Advances in quantum metrology, Nat. Photon. **5**, 222 (2011).

[11] M. W. Mitchell, J. S. Lundeen, and A. M. Steinberg, Super-resolving phase measurements with a multiphoton entangled state, Nature (London) **429**, 161 (2004).

[12] Y. Matsuzaki, S. C. Benjamin, and J. Fitzsimons, Magnetic field sensing beyond the standard quantum limit under the effect of decoherence, Phys. Rev. A **84**, 012103 (2011).

[13] G. Chen, N. Aharon, Y.-N. Sun, Z.-H. Zhang, W.-H. Zhang, D.-Y. He, J.-S. Tang, X.-Y. Xu, Y. Kedem, C.-F. Li, and G.-C. Guo, Heisenberg-scaling measurement of the single-photon Kerr non-linearity using mixed states, Nat. Commun. **9**, 93 (2018).

[14] G. Chen, L. Zhang, W.-H. Zhang, X.-X. Peng, L. Xu, Z.-D. Liu, X.-Y. Xu, J.-S. Tang, Y.-N. Sun, D.-Y. He, J.-S. Xu, Z.-Q. Zhou, C.-F. Li, and G.-C. Guo, Achieving Heisenberg-Scaling Precision with Projective Measurement on Single Photons, Phys. Rev. Lett. **121**, 060506 (2018).

[15] M. Zwerger, W. Dür, J. D. Bancal, and P. Sekatski, Device-Independent Detection of Genuine Multipartite Entanglement for All Pure States, Phys. Rev. Lett. **122**, 060502 (2019).

[16] D. Mayers and A. Yao, Self testing quantum apparatus, Quantum Inf. Comput. **4**, 273 (2004).

[17] I. Šupić and J. Bowles, Self-testing of quantum systems: A review, Quantum **5**, 424 (2021)

[18] G. Chen, W.-H. Zhang, P. Yin, C.-F. Li, and G.-C. Guo, Device-independent characterization of entanglement based on bell nonlocality, Fundam. Res. **1**, 1 (2021).

[19] W.-H. Zhang, G. Chen, P. Yin, X.-X. Peng, X.-M. Hu, Z.-B. Hou, Z.-Y. Zhou, S. Yu, X.-J. Ye, Z.-Q. Zhou, X.-Y. Xu, J.-S. Tang, J.-S. Xu, Y.-J. Han, B.-H. Liu, C.-F. Li, and G.-C. Guo, Experimental demonstration of robust self-testing for bipartite entangled states, npj Quantum Inf. **5**, 4 (2019).

[20] W.-H. Zhang, G. Chen, X.-X. Peng, X.-J. Ye, P. Yin, X.-Y. Xu, J.-S. Xu, C.-F. Li, and G.-C. Guo, Experimental Realization of Robust Self-Testing of Bell State Measurements, Phys. Rev. Lett. **122**, 090402 (2019).

[21] W.-H. Zhang, G. Chen, X.-X. Peng, X.-J. Ye, P. Yin, Y. Xiao, Z.-B. Hou, Z.-D. Cheng, Y.-C. Wu, J.-S. Xu, C.-F. Li, and G.-C. Guo, Experimentally Robust Self-Testing for Bipartite and Tripartite Entangled States, Phys. Rev. Lett. **121**, 240402 (2018).

[22] Y. Takeuchi, Y. Matsuzaki, K. Miyanishi, T. Sugiyama, and W. J. Munro, Quantum remote sensing with asymmetric information gain, Phys. Rev. A **99**, 022325 (2019).

[23] P. Yin *et al.*, Experimental Demonstration of Secure Quantum Remote Sensing, Phys. Rev. Appl. **14**, 014065 (2020).

[24] J. Kaniewski, Analytic and Nearly Optimal Self-Testing Bounds for the Clauser-Horne-Shimony-Holt and Mermin Inequalities, Phys. Rev. Lett. **117**, 070402 (2016).

[25] T. H. Yang and M. Navascués, Robust self-testing of unknown quantum systems into any entangled two-qubit states, Phys. Rev. A **87**, 050102(R) (2013).

[26] C. Bamps and S. Pironio, Sum-of-squares decompositions for a family of Clauser-Horne-Shimony-Holt-like inequalities and their application to self-testing, Phys. Rev. A **91**, 052111 (2015).

[27] A. Acín, S. Massar, and S. Pironio, Randomness Versus Nonlocality and Entanglement, Phys. Rev. Lett. **108**, 100402 (2012).

[28] J. S. Bell, On the Einstein-Podolsky-Rosen paradox, Phys. Phys. Fiz. **1**, 195 (1964).

[29] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, Proposed Experiment to Test Local Hidden-Variable Theories, Phys. Rev. Lett. **23**, 880 (1969).

[30] M. A. Nielsen, Conditions for a Class of Entanglement Transformations, Phys. Rev. Lett. **83**, 436 (1999).

[31] F. Nosrati, A. Castellini, G. Compagno, and R. Lo Franco, Robust entanglement preparation against noise by controlling spatial indistinguishability, npj Quantum Inf. **6**, 39 (2020).

[32] M. L. Almeida, S. Pironio, J. Barrett, G. Tóth, and A. Acín, Noise Robustness of the Nonlocality of Entangled Quantum States, Phys. Rev. Lett. **99**, 040403 (2007).