Device-Independent Quantum Key Distribution Based on the Mermin-Peres Magic Square Game

Yi-Zheng Zhen,[1,2] Yingqiu Mao,[1,2] Yu-Zhe Zhang,[1,2] Feihu Xu,[1,2,3,*] and Barry C. Sanders[1,2,4,†]
[1]Hefei National Research Center for Physical Sciences at the Microscale and School of Physical Sciences, University of Science and Technology of China, Hefei 230026, China
[2]Shanghai Research Center for Quantum Science and CAS Center for Excellence in Quantum Information and Quantum Physics, University of Science and Technology of China, Shanghai 201315, China
[3]Hefei National Laboratory, University of Science and Technology of China, Hefei 230088, China
[4]Institute for Quantum Science and Technology, University of Calgary, Alberta T2N 1N4, Canada

(Received 2 February 2023; accepted 21 July 2023; published 25 August 2023; corrected 8 November 2023)

Device-independent quantum key distribution (DIQKD) is information-theoretically secure against adversaries who possess a scalable quantum computer and who have supplied malicious key-establishment systems; however, the DIQKD key rate is currently too low. Consequently, we devise a DIQKD scheme based on the quantum nonlocal Mermin-Peres magic square game: our scheme asymptotically delivers DIQKD against collective attacks, even with noise. Our scheme outperforms DIQKD using the Clauser-Horne-Shimony-Holt game with respect to the number of game rounds, albeit not number of entangled pairs, provided that both state visibility and detection efficiency are high enough.

DOI: 10.1103/PhysRevLett.131.080801

Device-independent quantum key distribution (DIQKD) enables distant parties to achieve quantum key distribution even with untrusted apparatuses [1–3]. DIQKD provides information-theoretic security [4–6] against certain side-channel attacks that compromise the security of conventional quantum key distribution implementations [7–9]. To achieve this security, DIQKD treats all devices that prepare, transmit, and measure information carriers as black boxes that could have been created by an adversary. A nonlocality test [10] is typically executed by two communicating parties to estimate an adversary's possible knowledge about the generated data. Based on the result of the test, the parties determine whether the data suffice to yield secure keys [4–6].

However, as a sacrifice for high-level security, DIQKD yields a low key rate, as confirmed by recent experimental demonstrations [11–13]. For the potential use of DIQKD in practice, a high key-rate DIQKD protocol is demanding. Here, we remedy this issue by employing the nonlocality test of a Mermin-Peres magic square game (MPG) [14,15] in DIQKD. The MPG is a special nonlocal game whose quantum strategies allow two players to win with unit probability [16,17], thereby exceeding the winning probability of other nonlocal games such as the Clauser-Horne-Shimony-Holt (CHSH) game [18]. These remarkable features enable the MPG to yield a distinct DIQKD protocol from conventional protocols [19–24].

Here, we propose a DIQKD protocol based on the MPG and prove security in the asymptotic case subject to collective attacks. Adopting the technique proposed in Ref. [25], we numerically determine thresholds for state visibility and detection efficiency required by the protocol to generate secure keys. We show that our MPG-based protocol generates a higher key rate, defined as the average number of secret bits generated in each instance of the protocol (namely, preparation, distribution, and measurement), compared to CHSH-based DIQKD protocols for certain parameter regimes. Precisely, we show that our MPG-based protocol demonstrates advantages if the state visibility exceeds 0.978 (with perfect detection) or if the detection efficiency exceeds 0.982 (with a perfect source). Our results show the potential advantage of using more complex entangled states in implementing DIQKD.

MPG-based DIQKD protocol.—Alice and Bob play the MPG [14–16], which is depicted and explained in Fig. 1. After the game, the referee decides whether Alice and Bob win or not according to the average winning probability

$$\omega = \sum_{x,y} \pi(x,y) P(a_y^x = b_x^y | x, y). \tag{1}$$

Here, $\pi(x,y)$ is the probability of distributing index pair (x,y), and $P(a_y^x = b_x^y|x,y)$ is the winning probability of Alice and Bob with respect to (x,y).

Throughout, we employ the unbiased MPG: $\pi(x,y) = 1/9$. When using classical strategies (see one example in Sec. IA of Supplemental Material [26]), Alice and Bob's average winning probability is at most $8/9$ [17,27]. As classical strategies are equivalent to local hidden variables, $\omega \leq 8/9$ is actually a Bell inequality; some quantum strategies violate this inequality [17,27]. Here, we denote a quantum strategy as $(\rho, \mathcal{M})$ and its

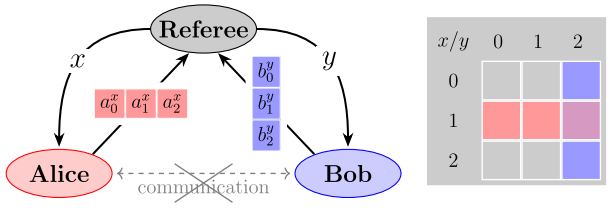

FIG. 1. The Mermin-Peres magic square game. Two players, Alice and Bob, fill a 3×3 magic square over many rounds for both of them to win. In each round, a referee generates two random "trits" $x, y \in \{0, 1, 2\}$ and sends row index x to Alice and column index y to Bob. Alice and Bob then reply to the referee with a row $[a_0^x, a_1^x, a_2^x]$ and a column $[b_0^y, b_1^y, b_2^y]^\mathsf{T}$, respectively, where all a_i^x, b_j^y for $i, j \in \{0, 1, 2\}$ are bits that satisfy $\oplus_i a_i^x = 0$ and $\oplus_j b_j^y = 1$. The winning condition is that Alice and Bob share the same value for the overlapped grid, i.e., $a_{i=y}^x = b_{j=x}^y$. During the game, Alice and Bob are forbidden to communicate with each other.

average winning probability as $\omega(\rho, \mathcal{M})$, where ρ is the distributed quantum state and $\mathcal{M}$ is the set of Alice's and Bob's quantum measurements used to generate the outputs. In particular, when the state is two pairs of maximally entangled qubits,

$$\Psi_2 = \Psi^+_{A_1B_1} \otimes \Psi^+_{A_2B_2}, \quad \Psi^+ := \frac{|00+11\rangle\langle 00+11|}{2}, \tag{2}$$

a measurement set $\mathcal{M}_{\text{opt}}$ (details in Sec. IB of Supplemental Material [26]) exists such that Alice and Bob will win the MPG: $\omega(\Psi_2, \mathcal{M}_{\text{opt}}) = 1$ with optimal quantum strategy $(\Psi_2, \mathcal{M}_{\text{opt}})$.

Crucially, the MPG certifies whether the outputs are correlated in every input pair. This feature allows us to design a DIQKD protocol, as introduced in Protocol 1. In this protocol, two communication parties, also termed Alice and Bob, initially generate data by playing the MPG. They announce their inputs and record the overlapped bits. To estimate parameters, Alice communicates with Bob which part of the bits serves as raw keys with the remaining part of the bits announced to play the MPG. If the average winning probability estimated from the announced data is less than an expected value ω_{exp}, they abort the protocol; otherwise, they perform data reconciliation on raw keys to obtain the final keys.

Security analysis.—To prove security for a DIQKD protocol, one needs to consider general adversary attacks and finite-data effect [4–6]. On the other hand, one can also temporarily consider weak security where adversary attacks are independent identically distributed (IID) collective and where the number of rounds N is infinite (asymptotic scenario), followed by extending the weak security to the general scenario [6,28,29]. Here, we analyze the weak security of Protocol 1.

Protocol 1. The MPG-based DIQKD protocol.

Input: N—number of rounds,
ω_{exp}—expected winning probability of the MPG

Output: $\boldsymbol{K}_\text{A}$—Alice's final key, $\boldsymbol{K}_\text{B}$—Bob's final key.

Data generation: In each round $n \in [N] = \{1, \ldots, N\}$, Alice and Bob independently pick $x_n, y_n \in \{0, 1, 2\}$, uniformly at random. They inject x_n and y_n to their devices and record the outputs $[a_0^{x_n}, a_1^{x_n}, a_2^{x_n} = a_0^{x_n} \oplus a_1^{x_n}]$ for Alice and $[b_0^{y_n}, b_1^{y_n}, b_2^{y_n} = b_0^{y_n} \oplus b_1^{y_n} \oplus 1]$ for Bob, respectively.

Announcement: Alice and Bob announce their inputs $\{x_n\}$ and $\{y_n\}$. They keep the bits $\{a_{y_n}^{x_n}\}$ and $\{b_{x_n}^{y_n}\}$, respectively.

Parameter estimation: Alice picks a random index subset $[K] \subsetneq [N]$ with a length γN and communicates $[K]$ with Bob. They use the bits with indexes in $[K]$ as raw keys $\boldsymbol{A}$ and $\boldsymbol{B}$, respectively, and announce the remaining bits, based on which they estimate the average winning probability ω of the MPG. If $\omega < \omega_{\text{exp}}$, they abort the protocol; otherwise, they proceed.

Data reconciliation: Alice and Bob apply error correction and privacy amplification on the raw keys $\boldsymbol{A}$ and $\boldsymbol{B}$ to obtain final secure keys $\boldsymbol{K}_\text{A}$ and $\boldsymbol{K}_\text{B}$, respectively.

Suppose that an MPG-based DIQKD protocol with a predetermined ω_{exp} is successfully implemented. We analyze if and how much secure key can be established for the case of IID collective attacks in the asymptotic scenario. Because DIQKD assumes the correctness and completeness of quantum theory, data generated in the protocol can be described by quantum measurements on a quantum state. As all quantum devices are untrusted, the precise quantum state and quantum measurements are unknown. Nevertheless, the assumption of IID collective attacks allows one to suppose that [19], in each round, the adversary Eve produces a quantum state ψ_{ABE} [6,19] and distributes it to Alice and Bob.

Measurements in the protocol, without losing generality, can always be described by the sets of projector-valued measures $\{M^x_{a_0a_1}\}_x$ for Alice and $\{N^y_{b_0b_1}\}_y$ for Bob, respectively. Here, x and y denote the inputs (i.e., measurement settings) while a_0a_1 and b_0b_1 are bits representing Alice's and Bob's outputs,

$$[a_0^x, a_1^x, a_2^x = a_0^x \oplus a_1^x], \qquad [b_0^y, b_1^y, b_2^y = b_0^y \oplus b_1^y \oplus 1]^\mathsf{T}, \tag{3}$$

respectively. For

$$\rho := \text{tr}_\text{E}[\psi_{\text{ABE}}], \qquad \mathcal{M} := \{\{M^x_{a_0a_1}\}_x, \{N^y_{b_0b_1}\}_y\}, \tag{4}$$

$(\rho, \mathcal{M})$ is evidently a quantum strategy for the MPG. The only constraint on $(\rho, \mathcal{M})$ is that the protocol is not aborted; i.e., $\omega(\rho, \mathcal{M}) \geq \omega_{\text{exp}}$.

An essential feature of the protocol is that raw keys are generated by all (x, y) pairs of quantum measurements in

$\mathcal{M}$ on the state ψ_{ABE}. For each input pair (x, y), whatever the precise forms of $\{M^x_{a_0 b_1}\}$ and $\{N^y_{b_0 b_1}\}$ are, the quantum state after the measurement can always be expressed as a classical-classical-quantum state.

$$\tau_{xy} \coloneqq \sum_{a_y^x, b_x^y} |a_y^x\rangle\langle a_y^x|_{\mathrm{A}} \otimes |b_x^y\rangle\langle b_x^y|_{\mathrm{B}} \otimes \hat{\phi}_{\mathrm{E}}(a_y^x b_x^y), \quad (5)$$

where a_y^x, b_x^y are the raw keys (bits from the overlapping grid of Alice's row and Bob's column) and $\hat{\phi}_{\mathrm{E}}(a_y^x b_x^y)$ is the unnormalized quantum state characterizing Eve's knowledge of the raw keys.

An appropriate one-way data-reconciliation protocol always exists such that a certain amount of secure keys can be processed from the raw keys while eliminating Eve's information [30]. As a result, for each input pair of (x, y), at least a ratio $\min\{0, r(\tau_{xy})\}$ of the raw keys will remain as final keys, where

$$r(\tau_{xy}) \coloneqq H(\boldsymbol{A}|E)_{\tau_{xy}} - H(\boldsymbol{A}|\boldsymbol{B})_{\tau_{xy}}. \quad (6)$$

Here, $H(|)$ denotes the conditional von Neumann entropy, and the bold symbols $\boldsymbol{A}$ and $\boldsymbol{B}$ imply that Alice and Bob's states are in classical states, representing the raw keys $\boldsymbol{A}$ and $\boldsymbol{B}$, respectively.

Finally, the security of the protocol should take all possible ψ_{ABE} into account, which implies that the final keys correspond to the worst case of all quantum strategies $(\rho, \mathcal{M})$. We define the key rate of DIQKD as the ratio of the length of final keys and the number of *all* rounds. In the asymptotic limit $N \to \infty$, the key rate can be expressed as

$$R = \min\left\{0, \frac{\gamma}{9} \inf_{(\rho,\mathcal{M})} \sum_{xy} r(\tau_{xy})\right\}, \quad (7)$$

subject to

$$\omega(\rho, \mathcal{M}) \geq \omega_{\mathrm{exp}}. \quad (8)$$

Here, the coefficient $\gamma/9$ comes from the fact that each input pair (x, y) occurs with a probability $1/9$ while a ratio γ of the rounds is used as raw keys. The key rate defined here characterizes how many secure keys can be generated given the number of experimental rounds, which is different from the definition used in some literature where the test rounds are excluded [24].

To further prove that the protocol can produce correct and secure keys, we need to show that the key rate R has positive values when implementing the protocol using certain quantum strategies. We first consider an ideal case, namely, implementing the protocol with the optimal quantum strategy $(\Psi_2, \mathcal{M}_{\mathrm{opt}})$ and setting $\omega_{\mathrm{exp}} = 1$. As the inputs are unbiased and randomly picked, the test rounds and the key rounds have the same correlations, both of which yield $\omega = 1$, so the protocol will not be aborted. Meanwhile, Alice and Bob's raw keys are uniformly distributed and perfectly correlated (see details in Sec. IB of Supplemental Material [26]). We have $H(\boldsymbol{A}|\boldsymbol{B})_{\tau_{xy}} = 0$ for any (x, y). Furthermore, $\omega = 1$ in the MPG can self-test two singlets [31]; i.e., the unknown quantum state must be locally isometric to two pairs of maximally entangled 2-qubit states. Such states cannot be correlated with a third party because of entanglement monogamy [32]. Combining with the fact that $\boldsymbol{A}$ is uniformly random for all τ_{xy}, we have $H(\boldsymbol{A}|E)_{\tau_{xy}} = 1$, indicating that the adversary has no information on $\boldsymbol{A}$. As a result, we obtain $R = \gamma$ for this ideal case, which shows that the protocol can indeed produce secure keys.

For nonideal cases when general quantum strategies are adopted or when noises are involved, we can bound R via the recently developed technique of quasirelative entropy [25]. Precisely, a lower bound for $H(\boldsymbol{A}|E)_{\tau_{xy}}$ in Eq. (6) can be derived as [25]

$$H(\boldsymbol{A}|E)_{\tau_{xy}} \geq c_m + \sum_{k=1}^{m-1} c_k \min\langle\psi|G_k(x, y)|\psi\rangle, \quad (9)$$

where $c_m = \sum_{k=1}^{m-1} c_k$ and $c_k = w_k/(t_k \ln 2)$, with $\{(t_k, w_k)|k = 1, \ldots, m\}$ a set of m nodes and weights of the Gauss-Radau quadrature, and $G_k(x, y)$ is defined as

$$G_k(x, y) \coloneqq \sum_{a_y \in \{0,1\}} \{\Pi^x_{a_y}[Z_{a_y} + Z^\dagger_{a_y} + (1 - t_k) Z^\dagger_{a_y} Z_{a_y}] + t_k Z_{a_y} Z^\dagger_{a_y}\}, \quad (10)$$

with Z_{a_y} an arbitrary operator and $\Pi^x_{a_y}$ the projector-valued measure corresponding to Alice's input x and output a_y^x. Combining with Eqs. (7) and (8), the minimization in Eq. (9) is taken over all possible pure states $|\psi\rangle = |\psi\rangle_{\mathrm{ABE}}$ and measurement strategies $\mathcal{M} = \{\{M^x_{a_0 a_1}\}_x, \{N^y_{b_0 b_1}\}_y\}$ subject to

$$\omega(\rho, \mathcal{M}) \geq \omega_{\mathrm{exp}}, \qquad \rho = \mathrm{tr}_{\mathrm{E}}[|\psi\rangle\langle\psi|_{\mathrm{ABE}}], \quad (11a)$$

$$\Pi^x_{a_y=0} = \begin{cases} M^x_{00} + M^x_{01} & \text{if } y = 0 \\ M^x_{00} + M^x_{10} & \text{if } y = 1 \\ M^x_{00} + M^x_{11} & \text{if } y = 2, \end{cases} \quad (11b)$$

$$\Pi^x_{a_y=1} = \mathbb{1} - \Pi^x_{a_y=0}, \quad (11c)$$

$$0 = [M^{x'}_{a_0 a_1}, N^{y'}_{b_0 b_1}], \quad (11d)$$

$$0 = [M^{x'}_{a_0 a_1}, Z_{a_y}] = [Z_{a_y}, N^{y'}_{b_0 b_1}], \quad (11e)$$

$$\forall\ a_{0,1,y}, b_{0,1} \in \{0, 1\}, \quad \forall\ x', y' \in \{0, 1, 2\}. \quad (11f)$$

This constrained minimization can be resolved via the Navascués-Pironio-Acín (NPA) hierarchy [33], which is numerically computable via solving a semidefinite program [34]. In Sec. II of Supplemental Material [26],

we numerically show that $H(\boldsymbol{A}|E)_{\tau_{xy}}$ has a positive lower bound if $\omega_{\text{exp}} > 0.9575$, which implies that the protocol can produce secure keys if, in the end, Eq. (7) has a positive value.

Noise tolerance.—Consider the case where the optimal quantum strategy $(\Psi_2, \mathcal{M}_{\text{opt}})$ is supposed to be used to implement the MPG-based protocol. Here, we characterize the performance of the protocol under two types of noise. For the first type, we consider the imprecise preparation of Ψ_2 such that each qubit may be mixed with some white noise. The distributed state becomes $\rho_\nu \otimes \rho_\nu$ before the detection, where $\rho_\nu = \nu\Psi^+ + (1-\nu)\mathbb{1}/2$ and ν is the state visibility. For the second type, we consider the noise led by nonclick events in measurements. Such nonclick events are caused by the loss of the state in transmission or the inefficiency of the detector, and cannot be sifted out from the data (otherwise, it may open detection loopholes [10–13]). Instead, Alice and Bob must assign an output to the nonclick events. We consider the following procedure: in each round, unless Alice (or Bob) successfully measured her (or his) state, Alice (or Bob) will output values according to a deterministic strategy of the MPG (Table I in Sec. IA of Supplemental Material [26]). The detection efficiency on each side is assumed identical and denoted as η.

We consider two cases where only the white noise is involved and where only the detection inefficiency is involved. For each value of ν or η, we select ω_{exp} such that the produced data can pass the parameter estimation in the protocol. The results are shown in Fig. 2. In the figure, the red solid line is the key-rate lower bound of the MPG-based protocol, which is obtained by solving the semidefinite programming problem combining Eqs. (6)–(11). For the calculation, we set the NPA hierarchy as 2 and the number of nodes in the Gauss-Radau quadrature as 16. From the figure, we observe that the key rate decreases when the state visibility or detection efficiency becomes smaller. It shows that the MPG-based protocol can produce a positive key rate if the state visibility $\nu > 0.959$ or if the detection efficiency $\eta > 0.969$.

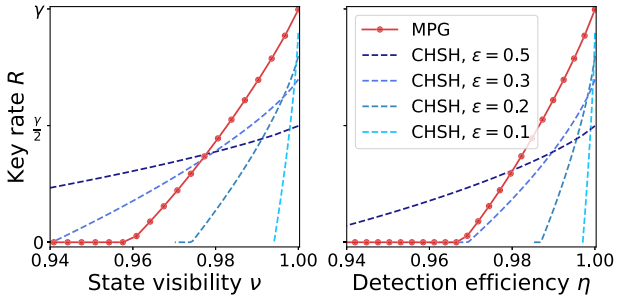

FIG. 2. Noise tolerance of the MPG-based protocol (red solid line) against the state visibility ν (left) and the detection efficiency η (right). Results of the CHSH-based protocols are plotted as blue dashed lines for comparison. ε represents the probability of Alice picking $x = 1$ in CHSH-based protocols.

Overcoming the key rate of CHSH-based protocols.—A prominent feature of the MPG-based protocol is that outputs of every input pair can be used to generate secure keys. As a result, all the outputs except that used in the estimation are collected as raw keys. This feature may enable the MPG-based protocol to yield a higher key rate than conventional DIQKD protocols. Particularly, if the optimal quantum strategy of the MPG can be faithfully implemented, the key rate $R_{\text{opt}} = \gamma$. It is actually the maximal key rate that any DIQKD protocol can achieve. As we will show, the MPG-based protocol outperforms a variety of CHSH-based protocols for certain regions of noise parameters.

In a standard CHSH-based protocol [19,20], Alice and Bob usually have inputs $x \in \{0,1\}$ and $y \in \{0,1,2\}$, respectively. To generate the data, Alice picks x uniformly at random while Bob picks $y \in \{0,1,2\}$ according to probabilities $(1-\gamma)/2, (1-\gamma)/2, \gamma$, respectively, and they input x and y into their local device and record the outputs $a, b \in \{0,1\}$. After obtaining all the data, they announce the inputs and select the outputs corresponding to the input pair $(x,y) \in \{0,1\}^2$ to play the CHSH game. If the average winning probability is above a certain threshold, they select the outputs corresponding to the input pair $(x,y) = (0,2)$ as the raw keys, followed by the data-reconciliation procedure to obtain the final keys. One can immediately see that the key rate cannot exceed $\gamma/2$, which is half of the optimal key rate of the MPG-based protocol.

To make a full comparison between the MPG-based protocol and protocols based on the CHSH game, we consider a variety of protocols based on biased CHSH games [35]. Suppose that in the CHSH-based protocol, Alice picks $x = 0,\ 1$ according to probabilities $1-\varepsilon,\ \varepsilon$, respectively, while Bob's probabilities of picking y remain the same. Then, the optimal key rate of the protocol becomes $\gamma(1-\varepsilon)/2$, which is higher than that of the standard CHSH-based protocol and is approaching γ when $\varepsilon \to 0$. We provide the details of the biased CHSH game and its induced DIQKD protocols in Sec. IIIA of Supplemental Material [26].

We compare the performance of MPG-based protocol and CHSH-based protocols with different input probabilities. We suppose that the optimal quantum strategy for the biased CHSH game is used to implement the CHSH-based protocol [35,36]. It turns out that when introducing the white noise, it is equivalent to treating the distributed state as ρ_ν. When a nonclick event occurs, Alice (or Bob) will output 0 for any input x (or y) such that a deterministic classical strategy is equivalently selected.

The results are shown again in Fig. 2, where the key-rate lower bounds of the CHSH-based protocols with different ε's are plotted with blue dashed lines. These key-rate lower bounds are obtained in a similar fashion to calculating the

key-rate lower bound for the MPG-based protocol, as presented in Sec. IIIB of Supplemental Material [26]. We observe that all key rates decrease when state visibility or detection efficiency decreases. As expected, decreasing ε can increase the optimal key rate of CHSH-based protocols. Nevertheless, these protocols cannot exceed the key rate of the MPG-based protocol in regions of $\nu > 0.978$ and $\eta > 0.982$, showing the advantage of the MPG-based protocol in these regions.

Discussion.—We have shown that our MPG-based protocol generates more secret keys per instance of protocol than CHSH-based protocols, in regions where the state visibility and detection efficiency are high. This comparison is made on the basis that the costly resource is the number of nonlocal games executed in the experiment [23,24]. Indeed, the secrecy of the keys in DIQKD is guaranteed by winning nonlocal games. Therefore, our result implies that a more complex nonlocal game may lead to a higher amount of secure keys per game round.

Nevertheless, the number of nonlocal games does not necessarily equal to the number of entangled states generated by the source, which is usually the considered resource in practice. In the case where the source generates a certain number of 2-qubit entangled states, the CHSH-based protocol is preferred. This is because the CHSH-based protocol can run twice as many rounds as that of a MPG-based protocol, and more keys could be produced. Also, the CHSH-based protocol is more robust against diminished state visibility and detection efficiency.

As for the realization of Protocol 1, the resource state Ψ_2 can be produced using two identical preparation of entangled singlets, or using the hyperentanglement technique to reduce the experimental overheads [37–39]. An obvious downside of the protocol is its high requirements for state visibility and detection efficiency. The selection of platforms is important to fulfill the desired requirements. For instance, the platform with remote matter-qubit entanglement can provide a higher detection efficiency. Meanwhile, theoretical improvements, including the use xof on-maximally entangled states [21,22], noisy-preprocessing procedures [40], and postselection techniques [41], can be considered to reduce the requirements of the protocol on the experimental imperfections.

In addition, regarding the higher key rate of the MPG-based protocol over CHSH-based protocols, one may wonder if there are improvements on the CHSH-based protocol such that the key rate γ can be achieved. For instance, in the standard CHSH-based protocol, one can add a key-generation agreement after the state distribution but before the measurements. Such step allows Alice and Bob to do either key generation or CHSH test [i.e., the original rounds corresponding to $(x, y) = (1, 2)$ do not exist], which theoretically enables the key rate to be as high as γ. However, the security of the modified protocol requires an additional assumption that no unwanted information is leaked during the key-generation agreement step [42]. We remark that the MPG-based protocol can achieve a key rate as high as γ without relying on the above additional assumption.

Conclusions.—We have proposed the DIQKD protocol based on the MPG and have provided the security analysis of the protocol against the collective attacks in the asymptotic scenario. We have numerically characterized the regions of two noise parameters, namely, state visibility and detection efficiency, when the MPG-based protocol can produce secure keys. We have further shown that, in certain regions, the MPG-based protocol has a higher key rate over a variety of protocols based on CHSH games. Our result shows the advantage of a sophisticated nonlocal game in DIQKD protocols and the potential usage of high-dimensional entanglement in device-independent quantum information tasks.

We gratefully acknowledge valuable discussions with Nai-Le Liu, Kai Chen, Li Li, and Valerio Scarani. This work was supported by National Natural Science Foundation of China (Grants No. 62031024, No. 12005091, No. 12104444), National Key Research and Development Program of China (Grants No. 2020YFA0309700), Shanghai Academic/Technology Research Leader (Grants No.21XD1403800), and Shanghai Science and Technology Development Funds (Grants No. 22JC1402900). Y. M. acknowledges support from the China Postdoctoral Science Foundation (Grant No. 2021M693093). F. X. acknowledges the support from the Tencent Foundation.

*feihuxu@ustc.edu.cn
†bsanders@ustc.edu.cn

[1] A. K. Ekert, Quantum Cryptography Based on Bell's Theorem, Phys. Rev. Lett. **67**, 661 (1991).
[2] D. Mayers and A. Yao, Quantum cryptography with imperfect apparatus, in *Proceedings of the 39th Annual Symposium on Foundations of Computer Science* (IEEE, Palo Alto, 1998), pp. 503–509.
[3] J. Barrett, L. Hardy, and A. Kent, No Signaling and Quantum Key Distribution, Phys. Rev. Lett. **95**, 010503 (2005).
[4] U. Vazirani and T. Vidick, Fully Device-Independent Quantum Key Distribution, Phys. Rev. Lett. **113**, 140501 (2014).
[5] C. A. Miller and Y. Shi, Robust protocols for securely expanding randomness and distributing keys using untrusted quantum devices, J. Assoc. Comput. Mach. **63**, 33:1 (2016).
[6] R. Arnon-Friedman, F. Dupuis, O. Fawzi, R. Renner, and T. Vidick, Practical device-independent quantum cryptography via entropy accumulation, Nat. Commun. **9**, 459 (2018).
[7] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Quantum cryptography, Rev. Mod. Phys. **74**, 145 (2002).
[8] F. Xu, X. Ma, Q. Zhang, H.-K. Lo, and J.-W. Pan, Secure quantum key distribution with realistic devices, Rev. Mod. Phys. **92**, 025002 (2020).

[9] C. Portmann and R. Renner, Security in quantum cryptography, Rev. Mod. Phys. **94**, 025008 (2022).
[10] N. Brunner, D. Cavalcanti, S. Pironio, V. Scarani, and S. Wehner, Bell nonlocality, Rev. Mod. Phys. **86**, 419 (2014).
[11] D. P. Nadlinger, P. Drmota, B. C. Nichol, G. Araneda, D. Main, R. Srinivas, D. M. Lucas, C. J. Ballance, K. Ivanov, E. Y.-Z. Tan, P. Sekatski, R. L. Urbanke, R. Renner, N. Sangouard, and J.-D. Bancal, Experimental quantum key distribution certified by Bell's theorem, Nature (London) **607**, 682 (2022).
[12] W. Zhang, T. van Leent, K. Redeker, R. Garthoff, R. Schwonnek, F. Fertig, S. Eppelt, W. Rosenfeld, V. Scarani, C. C.-W. Lim, and H. Weinfurter, A device-independent quantum key distribution system for distant users, Nature (London) **607**, 687 (2022).
[13] W.-Z. Liu, Y.-Z. Zhang, Y.-Z. Zhen, M.-H. Li, Y. Liu, J. Fan, F. Xu, Q. Zhang, and J.-W. Pan, Toward a Photonic Demonstration of Device-Independent Quantum Key Distribution, Phys. Rev. Lett. **129**, 050502 (2022).
[14] N. D. Mermin, Simple Unified form for the Major No-Hidden-Variables Theorems, Phys. Rev. Lett. **65**, 3373 (1990).
[15] A. Peres, Incompatible results of quantum measurements, Phys. Lett. A **151**, 107 (1990).
[16] G. Brassard, A. Broadbent, and A. Tapp, Quantum pseudo-telepathy, Found. Phys. **35**, 1877 (2005).
[17] N. Gisin, A. A. Méthot, and V. Scarani, Pseudo-telepathy: Input cardinality and Bell-type inequalities, Int. J. Quantum. Inform. **05**, 525 (2007).
[18] 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).
[19] S. Pironio, A. Acín, N. Brunner, N. Gisin, S. Massar, and V. Scarani, Device-independent quantum key distribution secure against collective attacks, New J. Phys. **11**, 045021 (2009).
[20] A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani, Device-Independent Security of Quantum Cryptography Against Collective Attacks, Phys. Rev. Lett. **98**, 230501 (2007).
[21] E. Woodhead, A. Acín, and S. Pironio, Device-independent quantum key distribution with asymmetric CHSH inequalities, Quantum **5**, 443 (2021).
[22] P. Sekatski, J.-D. Bancal, X. Valcarce, E. Y.-Z. Tan, R. Renner, and N. Sangouard, Device-independent quantum key distribution from generalized CHSH inequalities, Quantum **5**, 444 (2021).
[23] J. R. Gonzales-Ureta, A. Predojević, and A. Cabello, Device-independent quantum key distribution based on Bell inequalities with more than two inputs and two outputs, Phys. Rev. A **103**, 052436 (2021).
[24] I. W. Primaatmaja, K. T. Goh, E. Y.-Z. Tan, J. T.-F. Khoo, S. Ghorai, and C. C.-W. Lim, Security of device-independent quantum key distribution protocols: A review, Quantum **7**, 932 (2023).
[25] P. Brown, H. Fawzi, and O. Fawzi, Device-independent lower bounds on the conditional von Neumann entropy, arXiv:2106.13692.
[26] See Supplemental Material at http://link.aps.org/supplemental/10.1103/PhysRevLett.131.080801 for the classical and quantum strategies for the MPG, the security of MPG-based protocol beyond the ideal case, and the CHSH-based DIQKD protocols.
[27] A. Cabello, "All versus Nothing" Inseparability for Two Observers, Phys. Rev. Lett. **87**, 010403 (2001).
[28] R. Arnon-Friedman, R. Renner, and T. Vidick, Simple and tight device-independent security proofs, SIAM J. Comput. **48**, 181 (2019).
[29] E. Y.-Z. Tan, P. Sekatski, J.-D. Bancal, R. Schwonnek, R. Renner, N. Sangouard, and C. C.-W. Lim, Improved DIQKD protocols with finite-size analysis, Quantum **6**, 880 (2022).
[30] I. Devetak and A. Winter, Distillation of secret key and entanglement from quantum states, Proc. R. Soc. A **461**, 207 (2005).
[31] X. Wu, J.-D. Bancal, M. McKague, and V. Scarani, Device-independent parallel self-testing of two singlets, Phys. Rev. A **93**, 062121 (2016).
[32] B. M. Terhal, Is entanglement monogamous?, IBM J. Res. Dev. **48**, 71 (2004).
[33] M. Navascués, S. Pironio, and A. Acín, Bounding the Set of Quantum Correlations, Phys. Rev. Lett. **98**, 010401 (2007).
[34] The PYTHON code for obtaining the key-rate bound can be found in https://github.com/YizhengZhen/Code_DIQKD_MPG.
[35] T. Lawson, N. Linden, and S. Popescu, Biased nonlocal quantum games, arXiv:1011.6245.
[36] A. Acín, S. Massar, and S. Pironio, Randomness versus Nonlocality and Entanglement, Phys. Rev. Lett. **108**, 100402 (2012).
[37] J.-M. Xu, Y.-Z. Zhen, Y.-X. Yang, Z.-M. Cheng, Z.-C. Ren, K. Chen, X.-L. Wang, and H.-T. Wang, Experimental Demonstration of Quantum Pseudotelepathy, Phys. Rev. Lett. **129**, 050402 (2022).
[38] T. Yang, Q. Zhang, J. Zhang, J. Yin, Z. Zhao, M. Żukowski, Z.-B. Chen, and J.-W. Pan, All-versus-Nothing Violation of Local Realism by Two-Photon, Four-Dimensional Entanglement, Phys. Rev. Lett. **95**, 240406 (2005).
[39] L. Aolita, R. Gallego, A. Acín, A. Chiuri, G. Vallone, P. Mataloni, and A. Cabello, Fully nonlocal quantum correlations, Phys. Rev. A **85**, 032107 (2012).
[40] M. Ho, P. Sekatski, E. Y.-Z. Tan, R. Renner, J.-D. Bancal, and N. Sangouard, Noisy Preprocessing Facilitates a Photonic Realization of Device-Independent Quantum Key Distribution, Phys. Rev. Lett. **124**, 230502 (2020).
[41] F. Xu, Y.-Z. Zhang, Q. Zhang, and J.-W. Pan, Device-Independent Quantum Key Distribution with Random Postselection, Phys. Rev. Lett. **128**, 110506 (2022).
[42] Otherwise, the untrusted devices may communicate with the adversary in the agreement step of each round.

Correction: Detection efficiency values in the penultimate sentence in the third paragraph and the last sentences of the 16th and 21st paragraphs were erroneous and have been set right. The expected winning probability value in the last sentence of the 14th paragraph was erroneous and has been set right. The right-hand panel of the originally published Fig. 2 contained errors and has been replaced. The original Supplemental Material contained similar errors and has been replaced.