Quantum secret sharing with polarization-entangled photon pairs

Brian P. Williams,[1,*] Joseph M. Lukens,[1] Nicholas A. Peters,[1,2] Bing Qi,[1,3] and Warren P. Grice[1,†]

[1]*Quantum Information Science Group, Computational Sciences and Engineering Division, Oak Ridge National Laboratory, Oak Ridge, Tennessee 37831, USA*

[2]*Bredesen Center for Interdisciplinary Research and Graduate Education, The University of Tennessee, Knoxville, Tennessee 37996, USA*

[3]*Department of Physics and Astronomy, The University of Tennessee, Knoxville, Tennessee 37996, USA*

(Received 4 February 2019; published 11 June 2019)

We describe and experimentally demonstrate a more practical three-party quantum secret sharing (QSS) protocol using polarization-entangled photon pairs. The source itself serves as an active participant and can switch between the required photon states by modulating the pump beam only, thereby making the protocol less susceptible to loss and amenable to fast switching. We derive a security proof based on quantum key distribution, demonstrating our QSS protocol to be secure against both eavesdropping and dishonest participants. Compared to three-photon protocols, the practical efficiency is dramatically improved as there is no need to generate, transmit, or detect a third photon.

DOI: 10.1103/PhysRevA.99.062311

I. INTRODUCTION

Most quantum security protocols, such as quantum key distribution (QKD) [1–4], are designed for two parties, yet many practical security situations involve multiple parties. An example is secret sharing, in which a secret distributed to members of a group can be reconstructed only when a sufficient number of the group members combine their respective portions [5,6]. In *quantum* secret sharing (QSS), the partial secrets are distributed to N participants via quantum states in such a way that any subset of them containing at least k parties (with $k \leqslant N$) can combine their information to determine the information possessed by the dealer. As initially envisioned [7–9], QSS relies on distributing an $(N+1)$-partite Greenberger-Horne-Zeilinger (GHZ) state [10] to $N+1$ users who perform measurements; any one party can function as the dealer, or secret holder, and the remaining N players can determine the dealer's result only if they collaborate, making this a QSS technique for disseminating shared *classical* information. Other protocols have focused on QSS of *quantum* information [11,12], and a variety of alternative multipartite entangled resources have been considered in both discrete- [13–18] and continuous-variable [19–23] encodings. Yet large quantum states are extremely challenging to realize in the laboratory, and more practical QSS versions have emerged, based on simpler quantum resources such as entangled photon pairs [24–27] or single photons [28–31].

In this paper, we introduce a modified entangled-photon QSS protocol optimized for polarization qubits. In contrast to the original proposal for Bell pairs [24], preparing input states in our case is possible by modulation of the pump beam only, so that fast and lossy phase modulators can be incorporated *before* quantum state generation, thereby preserving entanglement downstream. We experimentally observe the quantum correlations required for our protocol, obtaining, on average, three-party correlations at $(89.3 \pm 0.5)\%$ with respect to their ideal values. Bolstered by a security proof built on QKD, our QSS protocol is practical and well suited to current technology.

II. BACKGROUND

At a high level, QSS relies on correlations present in the preparation and measurement of some quantum system. For one-to-N-party QSS of classical information, each user (including the dealer) possesses two bits of data: one bit is *public*, which is shared freely among all parties; the other is *private*, revealed only to a subset of players working together to determine the private bit of the dealer (the secret). While both classical and quantum secret sharing can be considered for subsets of size k ($k \leqslant N$) in so-called (k, N) threshold schemes, here we focus on QSS for the particular case $k = N$; that is, only all N players sharing their private bits can determine the private bit of the remaining $(N+1)$th party.

The original GHZ-based protocol [7] enjoys a satisfying symmetry for all parties, with public bits being measurement *bases* and private bits measurement *results*. Yet GHZ states are notoriously difficult to generate, so that experimental QSS demonstrations rely on intrinsically rare events, such as two-pair creation in spontaneous parametric down-conversion (SPDC) [9]. Fortunately, one-to-N QSS does not actually require $(N+1)$-partite entanglement, since each party need not measure a quantum system—only modify it. For example, a single-photon protocol in which intermediate parties rotate the state via one of four unitaries produces the same correlations as measurements of a GHZ state [28]. Likewise, a source of entangled photon pairs switching between four states permits QSS in which the source is an active participant [24]. While demonstrated experimentally for time-bin-entangled photons

[*] williamsbp@ornl.gov

[†] Present address: Qubitekk, LLC, Vista, California 92081, USA.

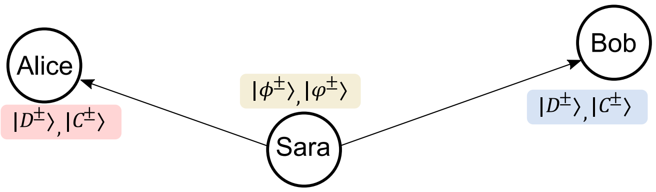
Alice
$|D^{\pm}\rangle, |C^{\pm}\rangle$
$|\phi^{\pm}\rangle, |\varphi^{\pm}\rangle$
Sara
Bob
$|D^{\pm}\rangle, |C^{\pm}\rangle$

FIG. 1. Three-party quantum secret sharing protocol. Sara chooses one of four entangled states; Alice and Bob randomly select to measure in either the diagonal or circular bases, recording their measurement results.

[25], to our knowledge no implementation of two-photon QSS with polarization qubits has been realized.

TABLE I. Combinations of public bits leading to correlated events, along with ideal values for the private bit correlation (second column), those measured experimentally (third column), and quantum bit-error rate (QBER) for pairwise combinations (fourth column).

Public bits (S, A, B)	$\langle\varepsilon\rangle$ (Ideal)	$\langle\varepsilon\rangle$ (Experiment)	Pairwise QBER (%)
(ϕ, D, D)	$+1$	$+0.89 \pm 0.01$	5.6 ± 0.7
(ϕ, C, C)	-1	-0.88 ± 0.01	6.1 ± 0.7
(φ, D, C)	$+1$	$+0.901 \pm 0.009$	4.9 ± 0.6
(φ, C, D)	$+1$	$+0.90 \pm 0.01$	5.1 ± 0.7

III. PROTOCOL

Figure 1 outlines our proposed protocol. We consider the three-party correlations between source Sara and receivers Alice and Bob. Central to enabling a practical polarization-entangled version of QSS is Sara's choice of states. We select the two ϕ Bell states as one basis, and "plus/minus i" states as the other:

$$\begin{aligned} |\phi^{\pm}\rangle &= \frac{1}{\sqrt{2}}(|HH\rangle \pm |VV\rangle), \\ |\varphi^{\pm}\rangle &= \frac{1}{\sqrt{2}}(|HH\rangle \pm i\,|VV\rangle), \end{aligned} \tag{1}$$

where $|mn\rangle \equiv |m\rangle_{\text{Alice}} \otimes |n\rangle_{\text{Bob}}$ and $|H\rangle$ ($|V\rangle$) denotes the horizontal (vertical) polarization eigenstate. Any measurement that would unambiguously identify the first two states would not be able to discern the second pair, and vice versa, due to the fact that $|\langle\phi^{\pm}|\varphi^{\pm}\rangle|^2 = |\langle\phi^{\pm}|\varphi^{\mp}\rangle|^2 = \frac{1}{2}$. In this way, we can define Sara's public bit S as the basis choice $S \in \{\phi, \varphi\}$ and her private bit s as the state within that basis, $s \in \{+, -\}$.

Importantly, these states are more convenient for experimental implementation than those considered in previous proposals for two-photon QSS, where linear combinations of Bell states form the second basis [24,27]. Use of a single source in that case for preparation of all four states requires polarization rotation of one of the two photons *after* generation. On the other hand, all the states in Eq. (1) share the same correlations in H and V, differing only in relative phase between the $|HH\rangle$ and $|VV\rangle$ contributions. Switching between all states can be effected by modifying the phase between the H and V components of the pump beam before generation. Since loss experienced by the pump has no impact on state generation (aside from needing more pump power), one can employ high-speed and potentially lossy phase modulators without degrading the performance of QSS.

Alice and Bob measure in either the diagonal (D) or circular (C) bases, with eigenstates

$$|D^{\pm}\rangle = \frac{1}{\sqrt{2}}(|H\rangle \pm |V\rangle), \qquad |C^{\pm}\rangle = \frac{1}{\sqrt{2}}(|H\rangle \pm i\,|V\rangle). \tag{2}$$

We can define Alice's public bit $A \in \{D, C\}$ (basis choice) and private bit $a \in \{+, -\}$ (result), and similarly for Bob: public bit $B \in \{D, C\}$ and private bit $b \in \{+, -\}$. There are four combinations of public bits (S, A, B) that produce a secret, identified by expressing Eq. (1) in terms of $|D^{\pm}\rangle$ and $|C^{\pm}\rangle$:

$$\begin{aligned} |\phi^{\pm}\rangle &= \frac{1}{\sqrt{2}}(|D^{+}D^{\pm}\rangle + |D^{-}D^{\mp}\rangle) \\ &= \frac{1}{\sqrt{2}}(|C^{+}C^{\mp}\rangle + |C^{-}C^{\pm}\rangle), \\ |\varphi^{\pm}\rangle &= \frac{1}{\sqrt{2}}(|D^{+}C^{\pm}\rangle + |D^{-}C^{\mp}\rangle) \\ &= \frac{1}{\sqrt{2}}(|C^{+}D^{\pm}\rangle + |C^{-}D^{\mp}\rangle). \end{aligned} \tag{3}$$

In other words, the correlations required for QSS appear when Alice and Bob choose the same basis for the ϕ states, and different bases for the φ states. If Sara selects from $s \in \{+, -\}$ with equal probability, the private bits (s, a, b) in each of the above lines assume all possibilities with equal probability individually and pairwise, yet collectively they are perfectly correlated. We can express the quantum correlation via the total parity (product of the signs), $\varepsilon = sab$, which adopts the value $+1$ (-1) for an even (odd) number of negative private bits, and has a definite value in each of the rows in Eq. (3).

Table I provides a summary of the public bit combinations leading to quantum correlations; for the other four public bit selections, the outcomes $\varepsilon = \pm 1$ are equally probable, and QSS is not possible. (As in other QSS protocols, this 50% failure rate can be circumvented by selecting basis combinations asymmetrically [8]).

We now describe how our QSS protocol proceeds and outline its general security against both external eavesdroppers and dishonest participants.

Quantum stage.

(1) Sara randomly selects public bits $S \in \{\phi, \varphi\}$ and private bits $s \in \{+, -\}$, prepares the state $|S^{s}\rangle$, and sends the photons to Alice and Bob.

(2) Alice and Bob randomly and independently choose to measure their photons in either the D or C basis.

(3) When both Alice and Bob detect photons, the three participants keep their data as raw key.

(4) They repeat steps (1)–(3) to generate more raw key.

After the quantum stage, one party is chosen as the dealer (either Sara, Alice, or Bob) while the other two serve as players.

Classical postprocessing stage.

(1) The dealer assumes player 1 is dishonest and player 2 is honest (there is no point to QSS if *both* players are dishonest).

(2) The dealer randomly selects a subset of raw key and requests that player 1 announce both the public and private bits.

(3) The dealer and player 2 estimate a lower bound secure key rate R_1 for two-party QKD, under the assumption that player 1 collaborates with eavesdroppers (see details below).

(4) They repeat steps (1)–(3) reversing the roles of the two players, giving the lower bound secure key rate R_2.

(5) The dealer determines the secure key rate R of the QSS protocol as the minimum of R_1 and R_2.

(6) The dealer requests the players to announce their public bits for the remaining data [32]. Using Table I and all the public bits from the three parties, the dealer announces the transmissions leading to correlated data. All parties keep the corresponding private bits as the sifted key.

(7) The dealer generates the final QSS key from the sifted key using one-way classical postprocessing as developed in QKD. Collaboratively, the two players can recover the QSS key using their private bits and error correction information from the dealer. Alone, each of them gains only an exponentially small amount of information about the QSS key.

IV. SECURITY

The security analysis of QSS is typically more involved than that of QKD. A security proof of QSS against eavesdroppers in the channels and dishonest players has only appeared recently [22], which introduced the key idea to treat measurements announced by the players as input or output from an uncharacterized device, while the dealer is assumed trusted. This allows them to apply the tools developed in one-sided device-independent QKD [33] in the security analysis of QSS. Here, we extend the above idea by applying the security proof of standard QKD with trusted devices, which can yield a better key rate in practice. This is based on the observation that at least one of the players in QSS is honest (although the dealer does not know who). By evaluating the potential secure key rate of QKD with each individual player (assuming all the other players are dishonest) and using the smallest one as the QSS key rate, security against collaborating attacks between the eavesdropper and any $N-1$ players can be guaranteed.

Here we briefly outline how to evaluate the secure key rate given that at most one of the two players is dishonest. There are two different cases.

Case 1: Dishonest player controls two-photon source. Sara is the dishonest player; let us assume the dealer is Alice. After the quantum stage, Alice randomly selects a subset of raw data and requests that Sara announce which entanglement states she prepared in those events. Given the information announced by Sara, the QKD process between Alice and Bob becomes conventional entanglement-based QKD with an untrusted entanglement source between two honest users. Its unconditional security has been well established [34,35].

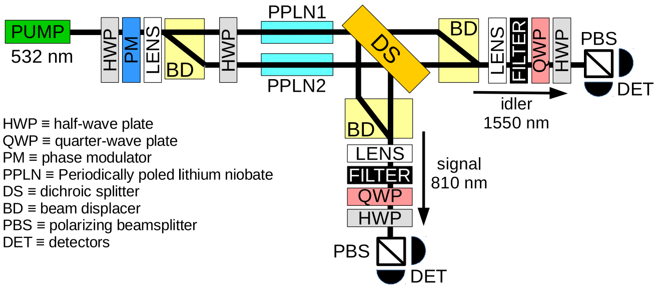

FIG. 2. Experimental setup. See text for details.

Case 2: Dishonest player controls one set of detectors. Let us deem Alice the dishonest player. To prove security, we introduce a *virtual* three-photon GHZ-state-based QKD protocol equivalent to the actual two-photon protocol. Specifically, we assume Sara prepares the state $|\Psi\rangle = \frac{1}{\sqrt{2}}(|HHH\rangle + |VVV\rangle)$ so that, by Eqs. (1)–(3),

$$\begin{aligned}|\Psi\rangle &= \frac{1}{\sqrt{2}}(|D^+\rangle\,|\phi^+\rangle + |D^-\rangle\,|\phi^-\rangle)\\ &= \frac{1}{\sqrt{2}}(|C^-\rangle\,|\varphi^+\rangle + |C^+\rangle\,|\varphi^-\rangle).\end{aligned} \tag{4}$$

If Sara measures one photon in the D (C) basis, depending on her measurement result, the other two photons will be projected onto $|\phi^+\rangle$ or $|\phi^-\rangle$ ($|\varphi^+\rangle$ or $|\varphi^-\rangle$), which are the states she prepares in the actual protocol. This implies the equivalence between this virtual protocol using GHZ states and the actual protocol. Since the measurements of different participants commute with each other, we can switch the order without changing the statistics of the measurement results. We can imagine that both Sara and Bob will keep their photons until Alice announces her measurement basis and results. In this picture, if Alice follows the protocol, she will project the other two photons onto one of the four entangled states in Eq. (1). With the information announced by Alice, Sara and Bob will know which entanglement state has been prepared. The QKD process between Sara and Bob again becomes conventional entanglement-based QKD.

V. EXPERIMENT

In order to explore these correlations experimentally, we utilize the polarization-entangled photon source in Fig. 2. Based on a similar design for 1550-nm entangled photons [36], this source relies on type-zero SPDC in two parallel, orthogonally rotated, periodically poled lithium niobate (PPLN) crystals. With a combination of beam displacers preceding and following the two crystals, we are able to generate a superposition of HH and VV photon pair amplitudes in a single spatial mode. This design is stable and has been shown to offer bright, high-fidelity entanglement [36], with a modified version applied in one of the seminal loophole-free Bell inequality tests [37]. The main difference here is the creation of nondegenerate photons; we pump with a frequency-doubled Nd:YAG laser at 532 nm and produce photons at 810 nm (Alice) and 1550 nm (Bob), using a dichroic splitter to separate them. By modulating the phase between the two

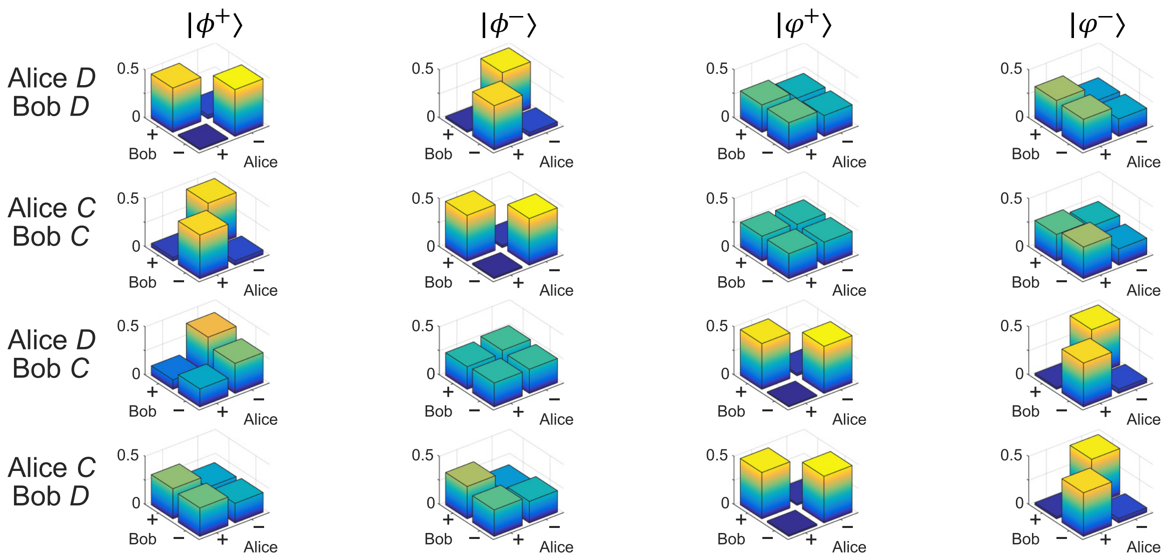

FIG. 3. Experimentally measured outcome probabilities for Alice and Bob, conditioned on input state and measurement bases.

pump polarizations prior to the first beam displacer, we ideally produce the state $|\Psi\rangle \propto |HH\rangle + e^{i\alpha}|VV\rangle$, with the phase α tunable from 0 to 2π, producing Sara's QSS states [Eq. (1)].

To characterize each of these states, we utilize polarization analyzers in both of the photon arms. To reduce noise on the InGaAs avalanche photodiodes (APDs) used for the 1550-nm photon, we trigger them with detections on the free-running Si APDs for the 810-nm photon using a field-programmable gate array. As an example, the fidelity for preparation of the state $|\phi^+\rangle$ we measure at $\langle\phi^+|\rho|\phi^+\rangle = 0.949 \pm 0.001$ (without subtraction of accidentals), where we use Bayesian tomography to reconstruct the full two-photon density matrix ρ [38,39].

To test all QSS correlations, we prepare Sara's four states and measure the coincidences in every D and C basis combination for Alice and Bob. After backing out loss and detector efficiency [39], we obtain the 16 normalized probability distributions in Fig. 3. Each column denotes a particular state, while each row shows a specific Alice and Bob basis combination. As expected, strong correlations result for the cases in Table I, while near-uniform probabilities are obtained for the remaining public bit combinations. We can quantify the correlation in each case using an Alice and Bob parity measure, $\varepsilon_s = ab$, the subscript s signifying that this is conditioned on a specific state from Sara. Its expectation value is given by $\langle\varepsilon_s\rangle = P_{++} + P_{--} - P_{+-} - P_{-+}$, with the probabilities taken from the relevant plot in Fig. 3.

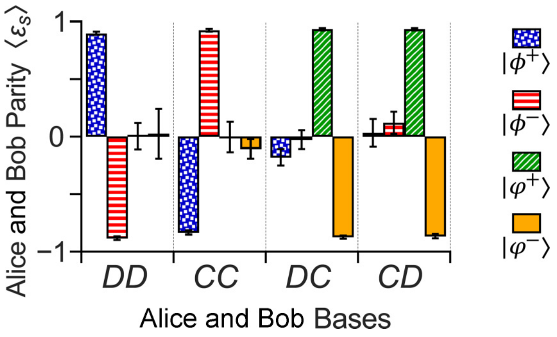

FIG. 4. Experimentally measured correlations, as expressed by expectation of the parity of Alice's and Bob's results.

We calculate all 16 of these correlation measures and display them in Fig. 4. (Error bars are plus or minus one standard deviation, computed from the Bayesian posterior distribution underlying the probabilities in Fig. 3.) For the basis combinations DD and CC, we find strong correlations with the $|\phi^\pm\rangle$ states, while for DC and CD the correlations are strong for $|\varphi^\pm\rangle$. We can combine pairs of these results to compute the expectation of the three-party correlation parameter $\langle\varepsilon\rangle = \frac{1}{2}(\langle\varepsilon_{s=+}\rangle - \langle\varepsilon_{s=-}\rangle)$, where we have assumed that each of Sara's options $s \in \{+,-\}$ are chosen with equal probability. This yields the numbers in the third column of Table I, whose absolute values average to 0.893 ± 0.005 compared to the ideal of unity. The corresponding pairwise QBER values (as needed for security analysis) follow in the fourth column. In our example, with completely honest players, the QBER is identical for each pair of users and equal to $\frac{1}{2}(1 - |\langle\varepsilon\rangle|)$. All values fall well below the 11% threshold of entanglement-based QKD using one-way communication [34,35], indicating the capacity for a positive secure QSS rate in our setup.

VI. DISCUSSION

While we have focused on pure QSS here, our physical setup is also compatible with QKD between any two of the three parties. With no modifications to the quantum stage of the protocol (state preparation and measurement), QKD between two participants can be realized by requiring the remaining party to reveal both public and private bits. This amounts to implementing steps (1)–(3) of the classical post-processing stage, but now for all raw key values, not just a random subset. Such an approach to QKD is especially flexible in that the communicating parties can be decided after all raw data have been collected. Additionally, by adding intermediate participants between the source and receivers (as in single-qubit QSS [28]), the protocol here can be extended to more than three users as well. Already considered as an extension of single-photon QSS [40], the use of entangled photons should benefit from the same advantages of entangled-photon QKD in the traditional point-to-point setting—namely, no need for decoy states and increased tolerance to loss [4]. However, adding users between the source and detectors will require Trojan-horse countermeasures. Whereas the "one-way" configuration of our basic three-user QSS protocol is naturally immune to Trojan-horse attacks [41], the many-user case is susceptible to an eavesdropper sending in and extracting probe light to read the phase shifts applied by intermediate parties. This is a known QSS vulnerability [40] that applies in extending our approach. Thus security measures beyond the proof introduced here would be essential for additional parties.

Finally, one of the primary practical advantages of our polarization-entangled QSS protocol is the reliance on pump polarization modulation to select Sara's quantum state, rather than modulation *after* photon-pair generation. When placed before the down-conversion crystal as done here, any introduced modulator loss can be compensated simply by turning up the pump power after the modulator but before the down-conversion crystal, preserving the ideal pair emission probability. On the other hand, were a fast polarization modulator placed in either the signal or idler path after generation to set the state, any loss would reduce the rate of transmitted entangled pairs and hence the QSS rate as well. In this case, turning up the pump power to compensate would introduce additional noise from increased multipair emission, so that the secure key rate would not be maintained. As an example, typical commercial fiber-pigtailed modulators impart ~3 dB loss, corresponding to either a twofold reduction in coincidences, or equivalently a fourfold increase in multipair probability for the same coincidence rate, when comparing postgeneration modulation against the pump modulation of our scheme.

In conclusion, we have introduced a pragmatic approach for QSS with polarization-entangled photons, with security based on that of QKD. Relying on pump phase modulation to prepare the necessary entangled states, our method tolerates high-speed and lossy phase modulators without degrading the performance of QSS. Our experimental implementation reveals the correlations necessary for three-party secret sharing, and extending to additional parties should be possible with minor modifications. Our approach could extend two-photon entanglement-based QKD to multiple users by promoting the entanglement source to a user and adopting a QSS protocol. This practical use of quantum resources should benefit commercial cryptography development and may inspire further improvements to QKD and QSS implementations.

ACKNOWLEDGMENTS

This work was performed at Oak Ridge National Laboratory, managed by UT-Battelle for the U.S. Department of Energy under Contract No. DEAC05-00OR22725. Funding was provided by the U.S. Department of Energy under the Cybersecurity for Energy Delivery Systems (CEDS) program.

[1] C. H. Bennett and G. Brassard, in *Proceedings of the International Conference on Computers, Systems & Signal Processing, Bangalore, India, 1984* (IEEE, Piscataway, NJ, 1984), pp. 175–179.

[2] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).

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

[4] H.-K. Lo, M. Curty, and K. Tamaki, Nat. Photon. **8**, 595 (2014).

[5] G. R. Blakley, in *Proceedings of the National Computer Conference* (AFIPS Press, 1979), Vol. 48, pp. 313–317.

[6] A. Shamir, Commun. ACM **22**, 612 (1979).

[7] M. Hillery, V. Bužek, and A. Berthiaume, Phys. Rev. A **59**, 1829 (1999).

[8] L. Xiao, G. L. Long, F.-G. Deng, and J.-W. Pan, Phys. Rev. A **69**, 052307 (2004).

[9] Y.-A. Chen, A.-N. Zhang, Z. Zhao, X.-Q. Zhou, C.-Y. Lu, C.-Z. Peng, T. Yang, and J.-W. Pan, Phys. Rev. Lett. **95**, 200502 (2005).

[10] D. M. Greenberger, M. A. Horne, and A. Zeilinger, in *Bell's Theorem, Quantum Theory and Conceptions of the Universe* (Springer, Berlin, 1989), pp. 69–72.

[11] R. Cleve, D. Gottesman, and H.-K. Lo, Phys. Rev. Lett. **83**, 648 (1999).

[12] D. Gottesman, Phys. Rev. A **61**, 042311 (2000).

[13] F.-G. Deng, X.-H. Li, C.-Y. Li, P. Zhou, and H.-Y. Zhou, Phys. Rev. A **72**, 044301 (2005).

[14] S. Gaertner, C. Kurtsiefer, M. Bourennane, and H. Weinfurter, Phys. Rev. Lett. **98**, 020503 (2007).

[15] D. Markham and B. C. Sanders, Phys. Rev. A **78**, 042309 (2008).

[16] A. Keet, B. Fortescue, D. Markham, and B. C. Sanders, Phys. Rev. A **82**, 062315 (2010).

[17] B. A. Bell, D. Markham, D. A. Herrera-Martí, A. Marin, W. J. Wadsworth, J. G. Rarity, and M. S. Tame, Nat. Commun. **5**, 5480 (2014).

[18] H. Lu, Z. Zhang, L.-K. Chen, Z.-D. Li, C. Liu, L. Li, N.-L. Liu, X. Ma, Y.-A. Chen, and J.-W. Pan, Phys. Rev. Lett. **117**, 030501 (2016).

[19] T. Tyc and B. C. Sanders, Phys. Rev. A **65**, 042310 (2002).

[20] A. M. Lance, T. Symul, W. P. Bowen, T. Tyc, B. C. Sanders, and P. K. Lam, New J. Phys. **5**, 4 (2003).

[21] A. M. Lance, T. Symul, W. P. Bowen, B. C. Sanders, and P. K. Lam, Phys. Rev. Lett. **92**, 177903 (2004).

[22] I. Kogias, Y. Xiang, Q. He, and G. Adesso, Phys. Rev. A **95**, 012315 (2017).

[23] Y. Zhou, J. Yu, Z. Yan, X. Jia, J. Zhang, C. Xie, and K. Peng, Phys. Rev. Lett. **121**, 150502 (2018).

[24] A. Karlsson, M. Koashi, and N. Imoto, Phys. Rev. A **59**, 162 (1999).

[25] W. Tittel, H. Zbinden, and N. Gisin, Phys. Rev. A **63**, 042301 (2001).

[26] K. Chen and H.-K. Lo, Quantum Inf. Comput. **7**, 689 (2007).

[27] W. P. Grice, J. M. Lukens, N. A. Peters, and B. P. Williams, in *Conference on Lasers and Electro-Optics* (Optical Society of America, Bellingham, WA, 2018), p. FTu4A.5.

[28] C. Schmid, P. Trojek, M. Bourennane, C. Kurtsiefer, M. Żukowski, and H. Weinfurter, Phys. Rev. Lett. **95**, 230505 (2005).

[29] J. Bogdanski, N. Rafiei, and M. Bourennane, Phys. Rev. A **78**, 062307 (2008).

[30] L.-F. Han, Y.-M. Liu, J. Liu, and Z.-J. Zhang, Opt. Commun. **281**, 2690 (2008).

[31] M. Hai-Qiang, W. Ke-Jin, and Y. Jian-Hui, Opt. Lett. **38**, 4494 (2013).

[32] We remark that the order in which the two players announce their public bits in step (6) does not matter. This can be seen from Table I: whether an event will be kept or not is determined by three public bits. As long as the dealer is the last one to reveal his or her public bit, the dishonest player cannot change the probability of a particular event being selected or not.

[33] M. Tomamichel and R. Renner, Phys. Rev. Lett. **106**, 110506 (2011).

[34] M. Koashi and J. Preskill, Phys. Rev. Lett. **90**, 057902 (2003).

[35] X. Ma, C.-H. F. Fung, and H.-K. Lo, Phys. Rev. A **76**, 012307 (2007).

[36] P. G. Evans, R. S. Bennink, W. P. Grice, T. S. Humble, and J. Schaake, Phys. Rev. Lett. **105**, 253601 (2010).

[37] L. K. Shalm, E. Meyer-Scott, B. G. Christensen, P. Bierhorst, M. A. Wayne, M. J. Stevens, T. Gerrits, S. Glancy, D. R. Hamel, M. S. Allman, K. J. Coakley, S. D. Dyer, C. Hodge, A. E. Lita, V. B. Verma, C. Lambrocco, E. Tortorici, A. L. Migdall, Y. Zhang, D. R. Kumor, W. H. Farr, F. Marsili, M. D. Shaw, J. A. Stern, C. Abellán, W. Amaya, V. Pruneri, T. Jennewein, M. W. Mitchell, P. G. Kwiat, J. C. Bienfang, R. P. Mirin, E. Knill, and S. W. Nam, Phys. Rev. Lett. **115**, 250402 (2015).

[38] R. Blume-Kohout, New J. Phys. **12**, 043034 (2010).

[39] B. P. Williams and P. Lougovski, New J. Phys. **19**, 043003 (2017).

[40] W. P. Grice, P. G. Evans, B. Lawrie, M. Legre, P. Lougovski, W. Ray, B. P. Williams, B. Qi, and A. M. Smith, Opt. Express **23**, 7300 (2015).

[41] N. Gisin, S. Fasel, B. Kraus, H. Zbinden, and G. Ribordy, Phys. Rev. A **73**, 022320 (2006).