Unconditional security of entanglement-based continuous-variable quantum secret sharing

Ioannis Kogias,[1,*] Yu Xiang,[2] Qiongyi He,[2] and Gerardo Adesso[1,†]
[1]*School of Mathematical Sciences, The University of Nottingham, University Park, Nottingham NG7 2RD, United Kingdom*
[2]*State Key Laboratory of Mesoscopic Physics, School of Physics, Peking University, Collaborative Innovation Center of Quantum Matter, Beijing 100871, China*
(Received 8 April 2016; published 12 January 2017)

The need for secrecy and security is essential in communication. Secret sharing is a conventional protocol to distribute a secret message to a group of parties, who cannot access it individually but need to cooperate in order to decode it. While several variants of this protocol have been investigated, including realizations using quantum systems, the security of quantum secret sharing schemes still remains unproven almost two decades after their original conception. Here we establish an unconditional security proof for entanglement-based continuous-variable quantum secret sharing schemes, in the limit of asymptotic keys and for an arbitrary number of players. We tackle the problem by resorting to the recently developed one-sided device-independent approach to quantum key distribution. We demonstrate theoretically the feasibility of our scheme, which can be implemented by Gaussian states and homodyne measurements, with no need for ideal single-photon sources or quantum memories. Our results contribute to validating quantum secret sharing as a viable primitive for quantum technologies.

DOI: 10.1103/PhysRevA.95.012315

I. INTRODUCTION

Secret sharing [1,2] is a task where a *dealer* sends a secret S to n (possibly, dishonest) *players* so that the cooperation of a minimum of $k \leqslant n$ players is required to decode the secret. Protocols that accomplish this are called (k,n)-threshold schemes. The need for such a task appears naturally in many situations, from children's games and online chats, to banking, industry, and military security: the secret message cannot be entrusted to any individual, but coordinated action is required to decrypt it in order to prevent wrongdoings.

For the classical implementation of the simplest (2,2)-threshold scheme, Alice, the dealer, encodes her secret into a binary string S and adds to it a random string R of the same length, resulting in the coded cypher $C = S \oplus R$, where "$\oplus$" denotes addition modulo 2. She then sends R and C, respectively, to the players Bob and Charlie. While the individual parts R and C carry no information about the secret, only by collaboration the players can recover S adding their strings together: $R \oplus C = S$. General (k,n)-threshold classical schemes are a bit more involved. Such protocols, however, face the same problem as any other classical key distribution protocol: *eavesdropping*. An eavesdropper, Eve, or even a dishonest player, can intercept the transmission and copy the parts sent from the dealer to the players, thus accessing the secret.

An obvious way to proceed would be for Alice to first employ standard two-party quantum key distribution (QKD) protocols [3], to establish separate secure secret keys with Bob and Charlie, then implement the classical procedure to split the secret S into parts R and C, and use the obtained secret keys to securely transmit these parts to each player. The advantage of this protocol, which we call parallel QKD (pQKD), is that it exploits unconditional security offered by the well-studied two-party QKD against eavesdropping and, very importantly, that it can be unconditionally secure against any possible dishonest actions of the players. However, pQKD can be demanding in terms of resources, as for a general (k,n) scenario it requires the implementation of n distinct QKD protocols plus the classical procedure to split the secret [1], thus becoming less efficient with increasing n.

An alternative proposal to cope with these difficulties lies in so-called *quantum secret sharing* [4] (QSS)—alias quantum sharing of a classical secret, distinct from quantum *state* sharing [5,6], in which the secret is a quantum state rather than a classical message—which allows for implementing a (k,n)-threshold scheme supported by a *single* classical post-processing, regardless of the number of players n. Unfortunately, as we shall see below, there exists no provably secure QSS scheme at the moment that enjoys the unconditional security of pQKD against both eavesdropping and dishonesty.

Hillery, Bužek, and Berthiaume [4] (HBB, for short) proposed the first (2,2)- and (3,3)-threshold QSS schemes that use multipartite entanglement to split the classical secret, and protect it from eavesdropping and dishonest players in a single go. Various other entanglement-based (HBB-type) schemes have been proposed [7–14], some being more economic in the required multipartite entanglement [15,16], while others allowing for more general (k,n)-threshold schemes [17–21]. A different entanglement-based QSS scheme has also been proposed, where entangled states are directly used as secure carriers and splitters of information [22]. A few experimental demonstrations have been reported as well [6,16,23–25]. The security of all current schemes, however, is limited to either plain external eavesdropping unrealistically assuming honest players, or limited types of attacks by eavesdroppers and dishonest participants, yet sharing ideally pure maximally entangled states. Furthermore, all such schemes are vulnerable to participant attack and cheating [7,26,27], and no method is currently known to deal with such conspiracies in general, not even in the ideal case of pure shared states.

*john_k_423@yahoo.gr
†gerardo.adesso@nottingham.ac.uk

Zhang, Li, and Man [28] proposed the first (n,n)-threshold scheme that required no entanglement and was claimed to be unconditionally secure. Although it required perfect single-photon sources and quantum memories (rendering it impractical for current technology), it was later shown to be vulnerable to various participant attacks [29,30]. In the same category of entanglement-free QSS schemes, Schmid *et al.* proposed a protocol based on a single photon [31]; although originally claimed to be unconditionally secure, it was also shown to be vulnerable to participant attacks [32–35]. Alternative schemes can be devised to deal with particular attacks [29,30,32,33]; however, there currently exists no rigorous method against arbitrary participant attacks.

To sum up, almost two decades after the conception of QSS, no existing scheme (with or without entanglement) has been proven unconditionally secure against cheating of dishonest players. Hence any practical implementation of secure secret sharing needs to resort to conventional pQKD, while QSS schemes only served so far as a theoretical curiosity.

In this paper, we consider a continuous-variable version of an HBB-type scheme. We determine conditions on the extracted key rate for the secret to be unconditionally secure against both external eavesdropping and arbitrary cheating strategies of dishonest participants, in the limit of asymptotic keys, independently of the shared state, and for arbitrary (k,n)-threshold schemes. The central idea in our approach, to rigorously deal with arbitrary cheating strategies, is to treat the measurements announced by the players as an input or output of an uncharacterized measuring device (black box), analogously to how (possibly, hacked) measuring devices are treated in device-independent QKD [36]. In practice, this translates into making no assumption about the origin of the players' (possibly, faked) announced measurements, in contrast to previous QSS approaches that considered the players' actions as trusted, thus suffering from cheating strategies. The dealer, on the other hand, is regarded as a trusted party with trusted devices, which is a natural assumption for this task. At variance with device-independent QKD, where the *devices* are untrusted, for the QSS task we treat the *players* themselves as untrusted, independently of their devices. Therefore the framework established in this paper, which makes no assumptions about the players' measurements, allows us to prove security against general attacks of eavesdroppers and/or of dishonest players. This is achieved by making a sharp connection with, and extending all the tools of, the recently developed one-sided device-independent QKD (1sDI-QKD) [37], in particular for continuous-variable systems [38], which has been proven unconditionally secure in the limit of asymptotic keys. However, the approach introduced here is general and can be adapted to derive security proofs for discrete-variable QSS schemes as well as in the regime of finite keys [39].

The paper is organized as follows. In Sec. II we present our continuous-variable QSS protocol, focusing on the (2,2)-threshold case. In Sec. III we provide a proof of its unconditional security, adopting techniques from the 1sDI-QKD paradigm. In Sec. IV we present extensions to (k,n)-threshold schemes and analyze the experimental feasibility of our protocol. In Sec. V we summarize our work and discuss some future perspectives.

II. THE PROTOCOL

For illustration, we first focus on the (2,2)-threshold scheme. The trusted dealer Alice prepares a three-mode continuous-variable entangled state, keeps one mode, and sends the other modes to the untrusted players, Bob and Charlie, through individual unknown quantum channels. Alice is assumed to perform homodyne measurements of two canonically conjugate quadratures, $\hat{x}_A = (\hat{a} + \hat{a}^\dagger)/\sqrt{2}$ and $\hat{p}_A = (\hat{a} - \hat{a}^\dagger)/i\sqrt{2}$, on her mode, with corresponding outcomes X_A, P_A, satisfying $[\hat{x}_A, \hat{p}_A] = i$ (in natural units with $\hbar = 1$). Bob and Charlie, considered with uncharacterized devices, are entitled to two unspecified measurements each, labeled by $x_{B(C)}, p_{B(C)}$, with corresponding outcomes $X_{B(C)}, P_{B(C)}$. Nothing is assumed about the origin of these measurements.

In our protocol, Alice's goal is to establish a unique secret key, not with Bob's or Charlie's individual measurements (as in standard two-party QKD), but with a collective (nonlocal) degree of freedom for Bob and Charlie, say $\bar{X}$, that strongly correlates with one of Alice's quadratures, say X_A. The unique secret key can be accessed only when the players communicate their local measurements, i.e., collaborate. For example, if the three parties shared a maximally entangled state and their outcomes were perfectly correlated as $X_A \simeq -X_B + X_C$, one would choose $\bar{X} = -X_B + X_C$ as such collective degree of freedom.

Alice sends additional copies to Bob and Charlie, and each time all parties randomly choose and measure their parts, getting outcomes X_i, P_i, respectively, with $i = A,B,C$, until they have a sufficiently long list of correlated data. Afterwards, all parties announce their measurement choice for each copy and keep only the data originating from correlated measurements (depending on the shared state). A random subset of this data, chosen by the dealer, is then publicly revealed and used to estimate the size of the secret key (*parameter estimation* step [40]) that will provide secure QSS (see below). Finally, if the estimated key is nonzero, Alice proceeds to the conventional classical post-processing steps of *direct reconciliation* and *privacy amplification* [40] to create her final secret key, and sends the encrypted secret to Bob and Charlie. However, only when, and if, Bob and Charlie collaborate to form the joint variable $\bar{X}$, can they apply the post-processing instructions on $\bar{X}$ to acquire Alice's secret key. In what follows we will derive conditions on the key rate to generate secret bits, from the correlations of X_A and $\bar{X}$, that are unconditionally secure against eavesdropping and dishonest participants.

III. SECURITY PROOF

A. Security against eavesdropping

Let us first study security against eavesdropping, following the QKD work of Walk *et al.* [38]. Neglecting detector and reconciliation efficiencies, the direct reconciliation asymptotic secret key rate is known to be lower bounded by the Devetak-Winter formula [41],

$$K \geqslant I(X_A : \bar{X}) - \chi(X_A : E), \tag{1}$$

which finds many uses in quantum information and communication [36,38,40,42–50]. Here

$$I(X_A : \bar{X}) = H(X_A) - H(X_A|\bar{X}) \tag{2}$$

is the classical mutual information between Alice's variable X_A and the joint variable $\bar{X}$, with $H(X) = -\int dX p(X) \log p(X)$ being the Shannon entropy for a variable X with probability distribution $p(X)$, and

$$\chi(X_A : E) = S(E) - \int dX_A p(X_A)\, S\big(\rho_E^{X_A}\big) \tag{3}$$

being the Holevo bound [51], which represents the maximum possible knowledge an eavesdropper can get on the key. The term $S(E) = -\mathrm{Tr}(\rho_E \log \rho_E)$ is the von Neumann entropy of Eve's reduced state ρ_E, whereas $\rho_E^{X_A}$ denotes Eve's state conditioned on Alice's measurement of $\hat{x}_A$ with outcome X_A. All logarithms in this paper are taken in base 2. A positive value of the right-hand side of (1) implies security of the key against collective attacks of the eavesdropper, and by virtue of Ref. [47] also against general coherent attacks.

Defining the conditional von Neumann entropy

$$S(X_A|E) = H(X_A) + \int dX_A p(X_A)\, S\big(\rho_E^{X_A}\big) - S(E)\,, \tag{4}$$

and the conditional Shannon entropy

$$H(X_A|X_B) = \int dX_B p(X_B) H(X_A|x_B = X_B)\,, \tag{5}$$

with $H(X_A|x_B = X_B) = -\int dX_A p(X_A|X_B) \log p(X_A|X_B)$, one can recast the key rate (1) as a balance of conditional entropies,

$$K \geqslant S(X_A|E) - H(X_A|\bar{X}). \tag{6}$$

We can now use fundamental *entropic uncertainty relations* that provide a lower bound to Eve's uncertainty [45,52–56],

$$S(X_A|E) + S(P_A|BC) \geqslant \log 2\pi, \tag{7}$$

for the derivation of which Alice's canonical commutation relations have been assumed, while Eve is assumed to purify the state shared by Alice, Bob, and Charlie, i.e., $\rho_{ABC} = \mathrm{Tr}_E(|\Psi_{ABCE}\rangle\langle\Psi_{ABCE}|)$. Substituting the uncertainty relation (7) back into (6) and recalling that $S(P_A|BC) \leqslant S(P_A|\bar{P}) = H(P_A|\bar{P})$ (since measurements cannot decrease the entropy), where $\bar{P}$ is a joint variable for Bob and Charlie optimally correlated with Alice's momentum P_A, we get

$$K \geqslant \log 2\pi - H(X_A|\bar{X}) - H(P_A|\bar{P})\,, \tag{8}$$

i.e., a bound on the key rate (hence, on Eve's maximal knowledge on the key X_A) only involving conditional Shannon entropies, that can be estimated using the announced measurement outcomes during the parameter estimation stage.

To make the bound even more accessible, we proceed to express it only in terms of second moments, instead of dealing with conditional probability distributions. For this aim, we recall that the Shannon entropy of an arbitrary probability distribution is maximized by a Gaussian distribution of the same variance. In other words, $H(X_A|\bar{X}) \leqslant H_G(X_A|\bar{X}) = \log\sqrt{2\pi e V_{X_A|\bar{X}}}$, where

$$V_{X_A|\bar{X}} = \int d\bar{X} p(\bar{X}) \big(\langle X_A^2\rangle_{\bar{X}} - \langle X_A\rangle_{\bar{X}}^2\big) \tag{9}$$

is the minimum inference variance of Alice's position outcome when the joint outcome $\bar{X}$ is known; and similarly for $H(P_A|P)$. The final key rate is then bounded as follows:

$$K \geqslant -\log\big(e\sqrt{V_{X_A|\bar{X}} V_{P_A|\bar{P}}}\big). \tag{10}$$

We see that a nonzero key rate (secure against eavesdropping) can be achieved when $E_{A|BC} \equiv V_{X_A|\bar{X}} V_{P_A|\bar{P}} < e^{-2}$.

B. Security against dishonesty

We derived conditions such that Alice's key is secure from eavesdropping and the players can safely obtain the key whenever they decide to collaborate. However, one needs to consider also the potential cheating strategies of the players themselves.

Suppose now that Bob is a dishonest player. His goal would be to guess Alice's key (hence, access the secret) using solely his own local measurements x_B, p_B, entirely bypassing the required collaboration with Charlie. A most general cheating strategy for Bob would be: first, to secretly intercept Charlie's mode during its transmission using general coherent attacks to increase his knowledge on Alice's key; and second, to lie about his measurements. A positive key rate in (10) does not guarantee security against such general participant attacks and cheating.

Here we derive additional conditions on the key rate so that Bob cannot cheat or access the secret by himself. Our central observation is to reconsider the Devetak-Winter formula (1) and now treat Bob as an eavesdropper, together with Eve. This means that in the Holevo bound $\chi(X_A : E)$ defined in (3), that expresses the knowledge of party E on the key X_A, we will include Bob himself. This leads to a modified Devetak-Winter formula,

$$K \geqslant I(X_A : \bar{X}) - \chi(X_A : EB), \tag{11}$$

where EB refers now to the unknown joint quantum state of Eve and Bob. A positive key rate in (11) would imply security of Alice's key against joint general attacks by Bob and Eve on Charlie's system. Also, Bob and Eve's maximum knowledge of the key, $\chi(X_A : EB)$, can be upper-bounded as seen below using Alice and Charlie's measurements, independently of Bob's (possibly, faked) announced measurements, therefore providing security against Bob's cheating. The uncertainty relation that we will use to bound Bob and Eve's knowledge will be a slightly modified version of (7),

$$S(X_A|EB) + S(P_A|C) \geqslant \log 2\pi. \tag{12}$$

Following similar steps as previously described, we thus end up with the following bound on the key rate:

$$K \geqslant -\log\big(e\sqrt{V_{X_A|\bar{X}} V_{P_A|P_C}}\big). \tag{13}$$

Notice that the key rate bound in (13) is smaller than the one in (10) that did not take dishonesty into account, due to $V_{P_A|\bar{P}} \leqslant V_{P_A|P_C}$, which is expected since the eavesdroppers'

knowledge on the key is increased by including Bob together with Eve.

To intuitively understand why this condition prohibits any cheating from Bob, we recall first that the key is generated solely by the $X_A, \bar{X}$ outcomes. By examination of the uncertainty relation (12), taking into account that $\log\sqrt{2\pi e V_{P_A|P_C}} \geqslant S(P_A|C)$, we see that the better Charlie can estimate Alice's momentum [i.e., the smaller $S(P_A|C)$] the larger Bob and Eve's ignorance should be on the key elements X_A. The previous condition (10), not accounting for participant dishonesty, only demanded that $S(P_A|BC)$ is small enough, which can be true even if $S(P_A|C)$ is arbitrarily large, thus allowing Bob to reach good knowledge of the key [i.e., small $S(X_A|EB)$], through (12).

We can also account for Charlie's dishonesty in an exactly analogous manner (just replace $B \leftrightarrow C$ above), leading us to

$$K \geqslant -\log\left(e\sqrt{V_{X_A|\bar{X}} V_{P_A|P_B}}\right). \tag{14}$$

Putting everything together, the final bound on the asymptotic key rate to provide unconditional security against general attacks of an eavesdropper, and against arbitrary (individual) cheating methods of both Bob and Charlie, which include the announcement of faked measurements and general attacks of Bob on Charlie's system and of Charlie on Bob's system, is

$$\begin{aligned} K &\geqslant I(X_A:\bar{X}) - \max\{\chi(X_A:EB), \chi(X_A:EC)\} \\ &\geqslant -\log\left(e\sqrt{V_{X_A|\bar{X}}\max\{V_{P_A|P_C}, V_{P_A|P_B}\}}\right), \end{aligned} \tag{15}$$

which is the minimum of the bounds (13) and (14). A positive key rate (15) remarkably provides security against all kinds of attacks that existing QSS protocols suffered from (e.g., fake announced measurements [7], Trojan horse attacks [29], etc.), for the sole reason that the players Bob and Charlie are not assumed to be performing trusted quantum operations but are treated as black boxes, in contrast to all previous schemes.

IV. DISCUSSION AND EXTENSIONS

In Fig. 1 we demonstrate the feasibility of the protocol in a concrete realization, where the key rate (15) is plotted against the squeezing degree of a noisy tripartite entangled Gaussian cluster state. Notice that the same key rate can also be achieved by an equivalent protocol that solely requires bipartite entanglement (that would represent the so-called prepare-and-measure counterpart to the presented protocol, borrowing a QKD terminology), thus further reducing the technological requirements for the state preparation. More generally, given the recent progress in the generation of large-scale continuous-variable entangled states [59–65], we expect our secure protocol to be recognized as a competitive candidate for practical QSS, as an alternative to conventional pQKD.

Finally, we show how to generalize the secret key rate bound (15) to any (k,n)-threshold QSS scheme. To start with, let us denote the n players as $B_1, B_2, \ldots, B_n$. A (k,n)-threshold scheme has two requirements: first, no collaboration of any $k-1$ players should be able to access the secret. We incorporate this requirement into Eq. (15) by considering all possible combinations of $k-1$ out of n players, the total number of which equals the binomial coefficient $\binom{n}{k-1}$, as potential collaborative eavesdroppers, and choosing the maximum Holevo information over all collaborations to attain the maximum possible knowledge on the key by any of these groups. Second, any collaboration of k players, known as the *access structure*, should be able to decode the message. Let us attribute a joint variable $\bar{X}_i$ to each k-player collaboration correlated to Alice's X_A, with $i = 1, \ldots, \binom{n}{k}$. This amounts to Alice sending as much error-correction information as needed, such that even the k-player collaboration least correlated to Alice, i.e., with the smallest $I(X_A:\bar{X}_i)$, can access her key. Taking the above into account, the key rate of the protocol will be,

$$\begin{aligned} K \geqslant \min&\left\{I(X_A:\bar{X}_1), \ldots, I\left(X_A:\bar{X}_{\binom{n}{k}}\right)\right\} \\ &- \max\left\{\chi(X_A:ES_1), \ldots, \chi\left(X_A:ES_{\binom{n}{k-1}}\right)\right\}, \end{aligned} \tag{16}$$

where S_i denotes a particular sequence of $k-1$ players, e.g., $S_1 = B_1 \cdots B_{k-1}$. A positive value of the right-hand side of Eq. (16) guarantees unconditional security of our QSS protocol against eavesdropping and arbitrary collaborative cheating strategies of any group of $k-1$ potentially dishonest players. This analysis readily extends to arbitrary access structures, where a subset of privileged players can access the key.

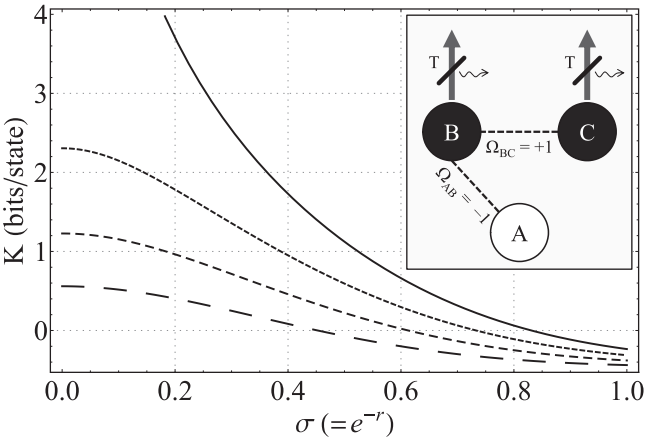

FIG. 1. The QSS secure key rate K, Eq. (15), is plotted against the squeezing r of a three-mode noisy Gaussian cluster state, obtained from a pure state [20] $\hat{U}_{AB}\hat{U}_{BC}|r\rangle_A|r\rangle_B|r\rangle_C$, with $\hat{U}_{ij} = \exp(\Omega_{ij}\hat{x}_i\hat{x}_j)$, after Bob and Charlie's modes undergo individual pure-loss channels (i.e., quantum-limited attenuating channels), each modeled by a beam splitter with transmissivity T and zero excess noise (see inset). From top to bottom, the curves correspond to $T = 1, 0.95, 0.9, 0.85$. All parties are assumed to be performing homodyne measurements of $\hat{x}_i, \hat{p}_i$, with $i = A, B, C$. The current experimentally accessible squeezing is limited to $r \lesssim 1.15$ (10 dB), or $\sigma \gtrsim 0.32$ [57,58], in which regime a nonzero K is still guaranteed for sufficiently large T, demonstrating the feasibility of our scheme.

V. CONCLUSIONS

We presented a feasible entanglement-based continuous-variable QSS scheme, and derived sufficient conditions for the protocol's secret key rate to provide unconditional security of the dealer's classical secret against general attacks of an eavesdropper and arbitrary cheating strategies, conspiracies, and attacks of the (possibly, dishonest) players, for all (k,n)-threshold schemes, and in the limit of asymptotic keys.

In our approach, we crucially identified the most physically relevant framework for QSS to be the 1sDI setting, treating the dealer as a trusted party with characterized devices and the players' devices as black boxes. The natural separation of roles between dealer and players renders QSS a well-suited task for the 1sDI setting, even more than two-party QKD itself [66]. At the same time, this observation enables us to adopt and generalize conventional 1sDI-QKD techniques to establish security of entanglement-based QSS, as demonstrated in this paper. Incidentally, while the resource behind 1sDI-QKD is known to be (bipartite) *steering* [67], a quantum correlation stronger than plain entanglement [68] and weaker than Bell nonlocality [69], one could suspect a similar connection in the present multiuser scenario. In a companion paper [70], we show in fact that *multipartite* steering [60,71] empowers secure QSS, providing an operational interpretation for a genuine multipartite continuous-variable steering measure.

Our work opens many avenues for further exploration. The presented security proof rests on general principles and can be extended from asymptotic to finite keys [39], suitable for concrete applications, and also to discrete-variable systems, used in the original QSS definition [4]; this will be the subject of future work. Moreover, although we provided sufficient security conditions for all (k,n)-threshold schemes, the identification of optimal families of states maximizing the key rate for each scheme was left open and will be addressed elsewhere.

Finally, our results pave the way for an unconditionally secure experimental demonstration of QSS, enabling its use in next-generation quantum communication networks.

ACKNOWLEDGMENTS

I.K. and G.A. acknowledge funding from the European Research Council under Grant No. 637352 (ERC StG GQCOP). Q.H. acknowledges the support of the National Natural Science Foundation of China under Grants No. 11274025 and No. 61475006. We thank A. Winter, N. Walk, E. Woodhead, and, particularly, A. Leverrier, for fruitful discussions. I.K. thanks R. Hawkins for proofreading the manuscript.

[1] A. Shamir, Commun. ACM **22**, 612 (1979).
[2] G. R. Blakley, in *afips* (IEEE, New York, 1899), p. 313.
[3] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).
[4] M. Hillery, V. Bužek, and A. Berthiaume, Phys. Rev. A **59**, 1829 (1999).
[5] R. Cleve, D. Gottesman, and H.-K. Lo, Phys. Rev. Lett. **83**, 648 (1999).
[6] A. M. Lance, T. Symul, W. P. Bowen, B. C. Sanders, and P. K. Lam, Phys. Rev. Lett. **92**, 177903 (2004).
[7] A. Karlsson, M. Koashi, and N. Imoto, Phys. Rev. A **59**, 162 (1999).
[8] L. Xiao, G. L. Long, F.-G. Deng, and J.-W. Pan, Phys. Rev. A **69**, 052307 (2004).
[9] Z.-j. Zhang and Z.-x. Man, Phys. Rev. A **72**, 022303 (2005).
[10] K. Chen and H.-K. Lo, Quant. Inf. Comput. **7**, 689 (2007).
[11] Y. Wu, J. Zhou, X. Gong, Y. Guo, Z.-M. Zhang, and G. He, Phys. Rev. A **93**, 022325 (2016).
[12] D. Gottesman, Phys. Rev. A **61**, 042311 (2000).
[13] Y. Fu, H.-L. Yin, T.-Y. Chen, and Z.-B. Chen, Phys. Rev. Lett. **114**, 090501 (2015).
[14] A. Marin and D. Markham, Phys. Rev. A **88**, 042332 (2013).
[15] F.-G. Deng, G. L. Long, and H.-Y. Zhou, Phys. Lett. A **340**, 43 (2005).
[16] W. Tittel, H. Zbinden, and N. Gisin, Phys. Rev. A **63**, 042301 (2001).
[17] A. M. Lance, T. Symul, W. P. Bowen, T. Tyc, B. C. Sanders, and P. K. Lam, New J. Phys. **5**, 4 (2003).
[18] D. Markham and B. C. Sanders, Phys. Rev. A **78**, 042309 (2008).
[19] A. Keet, B. Fortescue, D. Markham, and B. C. Sanders, Phys. Rev. A **82**, 062315 (2010).
[20] H.-K. Lau and C. Weedbrook, Phys. Rev. A **88**, 042313 (2013).
[21] Y. Wu, R. Cai, G. He, and J. Zhang, Quant. Inf. Process. **13**, 1085 (2014).
[22] S. Bagherinezhad and V. Karimipour, Phys. Rev. A **67**, 044302 (2003).
[23] 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).
[24] S. Gaertner, C. Kurtsiefer, M. Bourennane, and H. Weinfurter, Phys. Rev. Lett. **98**, 020503 (2007).
[25] 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).
[26] S.-J. Qin, F. Gao, Q.-Y. Wen, and F.-C. Zhu, Phys. Rev. A **76**, 062324 (2007).
[27] F.-G. Deng, X.-H. Li, and H.-Y. Zhou, arXiv:0705.0279.
[28] Z.-j. Zhang, Y. Li, and Z.-x. Man, Phys. Rev. A **71**, 044301 (2005).
[29] F.-G. Deng, X.-H. Li, H.-Y. Zhou, and Z.-j. Zhang, Phys. Rev. A **72**, 044302 (2005).
[30] S.-J. Qin, F. Gao, Q.-Y. Wen, and F.-C. Zhu, Phys. Lett. A **357**, 101 (2006).
[31] C. Schmid, P. Trojek, M. Bourennane, C. Kurtsiefer, M. Żukowski, and H. Weinfurter, Phys. Rev. Lett. **95**, 230505 (2005).
[32] G. P. He, Phys. Rev. Lett. **98**, 028901 (2007).
[33] G. P. He and Z. Wang, Quant. Inf. Comput. **10**, 28 (2010).
[34] V. Karimipour and M. Asoudeh, Phys. Rev. A **92**, 030301 (2015).
[35] A. Tavakoli, I. Herbauts, M. Żukowski, and M. Bourennane, Phys. Rev. A **92**, 030302(R) (2015).
[36] A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani, Phys. Rev. Lett. **98**, 230501 (2007).
[37] M. Tomamichel and R. Renner, Phys. Rev. Lett. **106**, 110506 (2011).
[38] N. Walk, S. Hosseini, J. Geng, O. Thearle, J. Y. Haw, S. Armstrong, S. M. Assad, J. Janousek, T. C. Ralph, T. Symul, H. M. Wiseman, and P. K. Lam, Optica **3**, 634 (2016).
[39] F. Furrer, T. Franz, M. Berta, A. Leverrier, V. B. Scholz, M. Tomamichel, and R. F. Werner, Phys. Rev. Lett. **109**, 100502 (2012).
[40] R. Renner, Int. J. Quant. Inf. **06**, 1 (2008).

[41] I. Devetak and A. Winter, Proc. R. Soc. London, Ser. A **461**, 207 (2005).
[42] B. Kraus, N. Gisin, and R. Renner, Phys. Rev. Lett. **95**, 080501 (2005).
[43] K. Horodecki, D. Leung, H.-K. Lo, and J. Oppenheim, Phys. Rev. Lett. **96**, 070501 (2006).
[44] M. Navascués, F. Grosshans, and A. Acín, Phys. Rev. Lett. **97**, 190502 (2006).
[45] M. Berta, M. Christandl, R. Colbeck, J. M. Renes, and R. Renner, Nat. Phys. **6**, 659 (2010).
[46] V. Scarani and R. Renner, Phys. Rev. Lett. **100**, 200501 (2008).
[47] R. Renner and J. I. Cirac, Phys. Rev. Lett. **102**, 110504 (2009).
[48] S. L. Braunstein and S. Pirandola, Phys. Rev. Lett. **108**, 130502 (2012).
[49] M. F. Cornelio, M. C. de Oliveira, and F. F. Fanchini, Phys. Rev. Lett. **107**, 020502 (2011).
[50] A. Streltsov, S. Lee, and G. Adesso, Phys. Rev. Lett. **115**, 030505 (2015).
[51] A. S. Holevo, Probl. Peredachi Inf. **9**, 3 (1973).
[52] J. M. Renes and J.-C. Boileau, Phys. Rev. Lett. **103**, 020402 (2009).
[53] F. Furrer, M. Berta, M. Tomamichel, V. B. Scholz, and M. Christandl, J. Math. Phys. **55**, 122205 (2014).
[54] R. L. Frank and E. H. Lieb, Commun. Math. Phys. **323**, 487 (2013).
[55] P. J. Coles, M. Berta, M. Tomamichel, and S. Wehner, arXiv:1511.04857.
[56] A. Ferenczi, Security proof methods for quantum key distribution protocols, Ph.D. thesis, University of Waterloo, 2013.
[57] T. Eberle, S. Steinlechner, J. Bauchrowitz, V. Händchen, H. Vahlbruch, M. Mehmet, H. Müller-Ebhardt, and R. Schnabel, Phys. Rev. Lett. **104**, 251102 (2010).
[58] T. Eberle, V. Händchen, and R. Schnabel, Opt. Express **21**, 11546 (2013).
[59] X. Su, Y. Zhao, S. Hao, X. Jia, C. Xie, and K. Peng, Opt. Lett. **37**, 5178 (2012).
[60] S. Armstrong, M. Wang, R. Y. Teh, Q. Gong, Q. He, J. Janousek, H.-A. Bachor, M. D. Reid, and P. K. Lam, Nat. Phys. **11**, 167 (2015).
[61] J. Roslund, R. M. Araujo, S. Jiang, C. Fabre, and N. Treps, Nat. Photonics **8**, 109 (2014).
[62] S. Gerke, J. Sperling, W. Vogel, Y. Cai, J. Roslund, N. Treps, and C. Fabre, Phys. Rev. Lett. **114**, 050501 (2015).
[63] M. Chen, N. C. Menicucci, and O. Pfister, Phys. Rev. Lett. **112**, 120505 (2014).
[64] S. Yokoyama, R. Ukai, S. C. Armstrong, C. Sornphiphatphong, T. Kaji, S. Suzuki, J. ichi Yoshikawa, H. Yonezawa, N. C. Menicucci, and A. Furusawa, Nat. Photonics **7**, 982 (2013).
[65] J. Yoshikawa, S. Yokoyama, T. Kaji, C. Sornphiphatphong, Y. Shiozawa, K. Makino, and A. Furusawa, APL Photon. **1**, 060801 (2016).
[66] C. Branciard, E. G. Cavalcanti, S. P. Walborn, V. Scarani, and H. M. Wiseman, Phys. Rev. A **85**, 010301 (2012).
[67] H. M. Wiseman, S. J. Jones, and A. C. Doherty, Phys. Rev. Lett. **98**, 140402 (2007).
[68] R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki, Rev. Mod. Phys. **81**, 865 (2009).
[69] N. Brunner, D. Cavalcanti, S. Pironio, V. Scarani, and S. Wehner, Rev. Mod. Phys. **86**, 419 (2014).
[70] Y. Xiang, I. Kogias, G. Adesso, and Q. He, Phys. Rev. A **95**, 010101 (2017).
[71] Q. Y. He and M. D. Reid, Phys. Rev. Lett. **111**, 250403 (2013).