Bound Entangled States with a Private Key and their Classical Counterpart

Maris Ozols, Graeme Smith, and John A. Smolin
IBM TJ Watson Research Center, 1101 Kitchawan Road, Yorktown Heights, New York 10598, USA

(Received 6 June 2013; published 18 March 2014)

Entanglement is a fundamental resource for quantum information processing. In its pure form, it allows quantum teleportation and sharing classical secrets. Realistic quantum states are noisy and their usefulness is only partially understood. Bound-entangled states are central to this question—they have no distillable entanglement, yet sometimes still have a private classical key. We present a construction of bound-entangled states with a private key based on classical probability distributions. From this emerge states possessing a new classical analogue of bound entanglement, distinct from the long-sought bound information. We also find states of smaller dimensions and higher key rates than previously known. Our construction has implications for classical cryptography: we show that existing protocols are insufficient for extracting private key from our distributions due to their "bound-entangled" nature. We propose a simple extension of existing protocols that can extract a key from them.

DOI: 10.1103/PhysRevLett.112.110502 PACS numbers: 03.67.Dd, 03.67.Hk

Introduction.—A fundamental goal of cryptography is to establish secure communication between two parties, Alice and Bob, in the presence of an eavesdropper Eve. This can be achieved by allowing Alice and Bob to encrypt their communication using a key obtained from some initially shared resource—a joint probability distribution [1–3] or quantum state [4,5]. However, this resource may not be useful in its original form—the shared key may not be perfectly random, private, or identical for both parties. Thus, classical key distillation—the process of generating a perfectly random, private, and identical key from a given tripartite probability distribution P_{ABE} shared among the three parties—and the similar quantum task of entanglement distillation from a tripartite quantum state $|\psi\rangle_{ABE}$, are problems of fundamental importance [2,3,6–10].

Private key is weaker than entanglement—it can be obtained by measuring Einstein-Podolsky-Rosen (EPR) pairs [4]. Thus, one can distill private key from a quantum state by first distilling EPR pairs. This strategy is not optimal in general due to the existence of private bound entanglement—entangled states from which EPR pairs cannot be distilled, but nevertheless a private key can be obtained [11,12].

Private bound-entangled states demonstrate a striking distinction between two forms of correlation: private classical key and shared entanglement. The best rate at which Alice and Bob can generate private key from $|\psi\rangle_{ABE}$ when only Eve has access to the E part of the initial state and all public messages sent by Alice and Bob is called the *private key rate*, denoted by $K(\psi_{ABE})$. Now, in addition to the above, assume that Eve also has access to all ancillary trash systems that Alice and Bob have introduced during the protocol. I.e., all information produced during the protocol—other than the final key—becomes available to Eve once the protocol is over. In such a case, distilling a key becomes much harder. In the language of [11,12], the final "key" system cannot be protected by any "shield" systems kept by Alice and Bob. In fact, as the following simple observations imply, Alice and Bob have no choice but to resort to distilling a much stronger resource—entanglement. One can check that (i) if Alice and Bob can distill entanglement, they maintain privacy from Eve even if she has access to all ancillary trash systems produced during the protocol; (ii) conversely, the only way of obtaining a resource that guarantees privacy between Alice and Bob when all trash systems are available to Eve is to distill entanglement [13]. Thus, the best rate of producing a private key in the more restricted scenario when all ancillary trash systems are available to Eve, is the same as the entanglement distillation rate $D(\psi_{ABE})$—the best rate at which Alice and Bob can distill EPR pairs from $|\psi\rangle_{ABE}$ via local operations and classical communication (LOCC). Private bound-entangled states have $D(\psi_{ABE}) = 0$ and $K(\psi_{ABE}) > 0$.

We will show that a similar distinction exists also in the classical world. In the classical case, a private key must be distilled from a shared probability distribution P_{ABE} by public discussion between Alice and Bob. At each step of the protocol, either Alice or Bob generates a public message from her or his random variables, followed by a stochastic map that modifies the variables. In general, such maps might not be reversible and thus partially destroy the information (we call such maps *noisy processing*). We denote by $K(P_{ABE})$ the best private key rate obtainable by such protocols (i.e., protocols that involve public discussion and noisy processing). In an alternative scenario, Alice and Bob can only create new random variables but cannot modify or destroy the existing ones [14]. Furthermore, all variables (except the ones that contain the key) become available to Eve at the end of the protocol. We denote the

© 2014 American Physical Society

best key rate of such protocols by $K_{\mathrm{PD}}(P_{ABE})$, where PD stands for *public discussion* (the protocol involves only public discussion and no noisy processing). Because in the quantum setting it is distillable entanglement that is resistant to giving trash systems to Eve, its natural classical analogue is K_{PD}. The quantum quantity corresponding to the private key achieved by including noisy processing $K(P_{ABE})$ is simply the private key obtainable by LOCC, $K(\psi_{ABE})$. Table I summarizes the quantities of interest.

Previous studies pursuing a classical analogue of bound entanglement [15–18] looked for distributions with $K(P_{ABE}) = 0$. A particular distribution, obtained by measuring a bound-entangled quantum state, was considered in [15]. It was hoped that because the quantum state was bound, no key would be distillable from the classical distribution. This hope was tempered by the discovery of private bound-entangled states [11,12], whose existence demonstrates a clear distinction between secrecy and bound entanglement. Our work establishes a similar distinction classically by giving distributions with $K_{\mathrm{PD}}(P_{ABE}) = 0$ that cannot be created by public discussion, in direct analogy with quantum bound-entangled states. We specifically do not solve the long-standing question of whether or not there is bound information [15–18], which corresponds to $K(P_{ABE}) = 0$ according to our notation (see Table I) and which we would prefer to call "bound private key". It is interesting to note that in the tripartite case, an affirmative answer has been demonstrated classically [17].

Construction.—Our results are based on tripartite probability distributions P_{ABE} whose probabilities $p(a, b, e)$ have a special combinatorial structure [19] (see Fig. 1):

$$\forall b, e \quad |\{a : p(a, b, e) \neq 0\}| \leq 1, \tag{1}$$

$$\forall a, e \quad |\{b : p(a, b, e) \neq 0\}| \leq 1, \tag{2}$$

$$\forall a, b \quad |\{e : p(a, b, e) \neq 0\}| \leq 1, \tag{3}$$

where $|S|$ denotes the size of set S. We call such distributions *unambiguous*, since any two parties can uniquely determine the third party's variable. Such distributions have a convenient graphical representation (see Fig. 2), which together with P_{AB} determines the full distribution P_{ABE} (up to permutations on E).

We identify P_{ABE} with a tripartite pure state

$$\begin{aligned} |\psi\rangle_{ABE} &:= \sqrt{P_{ABE}} \\ &:= \sum_{a,b,e} \sqrt{p(a, b, e)}\, |a\rangle_A |b\rangle_B |e\rangle_E, \end{aligned} \tag{4}$$

where $|a\rangle_A$, $|b\rangle_B$, $|e\rangle_E$ are standard basis vectors for systems A, B, E and with a bipartite mixed state

$$\rho_{AB} := \mathrm{Tr}_E |\psi\rangle\langle\psi|_{ABE} \tag{5}$$

on Alice and Bob whose purification is held by Eve. Such states have a special structure, since all eigenvectors of ρ_{AB} have the same Schmidt basis.

The *partial transpose* (PT) [20] of ρ_{AB} is defined on the standard basis as

$$(|a\rangle\langle a'|_A \otimes |b\rangle\langle b'|_B)^{\Gamma} := |a\rangle\langle a'|_A \otimes |b'\rangle\langle b|_B \tag{6}$$

and extended by linearity. If ρ_{AB} is PT invariant ($\rho_{AB}^{\Gamma} = \rho_{AB}$) then it has positive partial transpose and thus no distillable entanglement [21] (unambiguous distributions P_{ABE} that yield PT-invariant states ρ_{AB} are characterized in Appendix B, Ref. [22]).

Results.—Using the properties of unambiguous distributions and Eq. (4), which promotes any classical distribution to a quantum state, we establish a strong analogy between classical and quantum distillation problems in Table I. We show that a classical protocol with an unambiguous initial distribution can be "lifted" to a quantum protocol with an unambiguous initial state, without decreasing the associated distillation rate.

Theorem 1: Let P_{ABE} be an unambiguous probability distribution and $|\psi\rangle_{ABE}$ be the associated quantum state. The distillable entanglement of $|\psi\rangle_{ABE}$ is at least as big as the distillable key by public discussion of P_{ABE},

$$D(\psi_{ABE}) \geq K_{\mathrm{PD}}(P_{ABE}). \tag{7}$$

The distillable key of $|\psi\rangle_{ABE}$ is at least as big as the distillable key by public discussion and noisy processing of P_{ABE} [23],

$$K(\psi_{ABE}) \geq K(P_{ABE}). \tag{8}$$

TABLE I. Quantum-classical dictionary for states and distillation rates. A tripartite probability distribution P_{ABE} is unambiguous if it satisfies Eqs. (1)–(3). The associated quantum state $|\psi_{ABE}\rangle$ is given by Eq. (4).

	Quantum	Classical
States	$\|\psi\rangle_{ABE}$ unambiguous quantum state	P_{ABE} unambiguous probability distribution
Entanglement distillation (public trash)	$D(\psi_{ABE})$ EPR pairs by LOCC	$K_{\mathrm{PD}}(P_{ABE})$ private key by public discussion
Private key distillation (private trash)	$K(\psi_{ABE})$ private key by LOCC	$K(P_{ABE})$ private key by public discussion and noisy processing

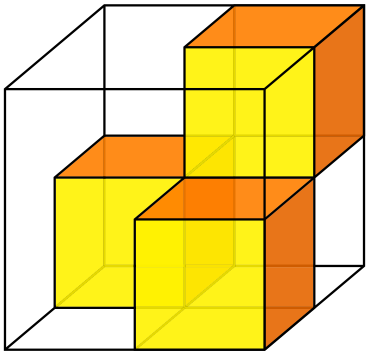

FIG. 1 (color online). A three-dimensional representation of an unambiguous probability distribution P_{ABE}. Each axis corresponds to one of the three parties and each cube represents a triple (a, b, e) such that $p(a, b, e) \neq 0$. Intuitively, Eqs. (1)–(3) say that the small cubes do not overlap if this block is compressed along any of the three axes.

Proof.—Let $\sqrt{Q_{ABE}}$ be the quantum state associated to distribution Q_{ABE} at some step of the classical protocol, and let $\sqrt{M}$ denote the entry-wise square root of the stochastic map M that is applied. Without loss of generality, M introduces a new random variable. Hence, if Q_{ABE} is unambiguous then so is $M \cdot Q_{ABE}$. By induction, the distribution remains unambiguous throughout the protocol. Furthermore, at every step $\sqrt{M} \cdot \sqrt{Q_{ABE}} = \sqrt{M \cdot Q_{ABE}}$, which allows lifting the classical protocol to a quantum one. The quantum protocol achieves the same rate due to properties of unambiguous states (see Appendix C for complete proof). ■

Recall that private bound-entangled states have $D(\psi_{ABE}) = 0$ and $K(\psi_{ABE}) > 0$, implying that entanglement and private key are distinct resources in the quantum world. We show that K_{PD} and K also correspond to distinct resources classically.

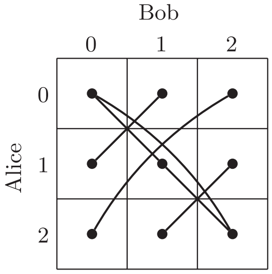

FIG. 2. A graphical representation of an unambiguous distribution P_{ABE} with $d_A = d_B = 3$ and $d_E = 4$. For each nonzero entry of $p(a, b, e)$ we put a dot at coordinates (a, b), and connect dots corresponding to the same symbol for Eve. Note that each cell contains at most one dot due to Eq. (3), and the resulting graph is a union of disjoint cliques (complete graphs) where each clique represents a different symbol for Eve. The above example has four connected components, hence, $d_E = 4$. Furthermore, no two vertices from a clique share the same column or row due to Eqs. (1) and (2). For PT invariance (see Appendix B), the diagram in addition must also be a union of crosses, i.e., pairs of edges $(a, b) - (a', b')$ and $(a, b') - (a', b)$ for some $a \neq a'$ and $b \neq b'$. The above diagram consists of three crosses: two small and one large.

Theorem 2: Unambiguous probability distributions P_{ABE} with $K_{PD}(P_{ABE}) = 0$ and $K(P_{ABE}) > 0$ exist.

Proof.—To guarantee $K_{\mathrm{PD}}(P_{ABE}) = 0$, we choose an unambiguous P_{ABE} corresponding to a PT-invariant ρ_{AB}. Then $D(\rho_{AB}) = 0$ and K_{PD} vanishes by Theorem 1. We obtain a positive value of $K(P_{ABE})$ by cleverly choosing the diagram of P_{ABE} (see Fig. 2) and numerically optimizing the right-hand side of

$$K(P_{ABE}) \geq I(X; B) - I(X; E), \qquad (9)$$

where $I(X; B)$ denotes the mutual information [24] between classical random variables X and B, and X is obtained by noisy processing of A. Table II summarizes our findings for various small dimensions, and Fig. 2 shows the structure of our smallest example, a 3 × 3 state. More details and explicit examples are provided in Appendix E. ■

Since our construction guarantees $D(\psi_{ABE}) = 0$, we can lift any P_{ABE} from Theorem 2 to a private bound-entangled state $|\psi\rangle_{ABE}$ by applying Theorem 1.

Corollary 3. Any P_{ABE} from Theorem 2 yields a private bound-entangled state $|\psi\rangle_{ABE}$ via Eq. (4).

This gives a new construction of private bound-entangled states (the only known construction before our work was [11,12]). In fact, due to the lifting established by Theorem 1, it is natural to consider the distribution P_{ABE} in Theorem 2 as a classical analogue of private bound entanglement. This provides a satisfactory resolution to the problem of finding a classical analogue of bound entanglement [15–18].

Implications for classical key agreement.—The basic technique for classical key agreement is a combination of error correction and privacy amplification (EC + PA), which achieves a rate of the mutual information difference

TABLE II. Summary of private bound-entangled states obtained using our construction. Here d_A, d_B, and d_E are the dimensions of Alice, Bob, and Eve. The third column is a numerical lower bound on the amount of distillable private key. The amount of private key in our 4 × 4 example exceeds 0.0213399 achieved by [12]. Our 4 × 5 example can be embedded in the 5 × 6 and 6 × 5 examples, but we report only states that are not trivially reducible to examples in smaller dimensions. This is why the last two examples have smaller key rates despite having larger dimensions.

$d_A \times d_B$	d_E	Bits of private key
3 × 3	4	0.0057852
4 × 4	6	0.0293914
4 × 5	8	0.0480494
5 × 6	10	0.0378462
6 × 5	10	0.0354342

$I(A;B) - I(A;E)$ [2]. Essentially all other protocols use EC + PA as a final step. For example, preceding EC + PA by a noisy processing step in which the distribution of A is modified gives the optimal key rate for distillation with one-way discussion from Alice to Bob [3]. Similarly, Maurer considered public discussion protocols where Alice and Bob exchange the information about their variables in a two-way fashion [8]. Public discussion includes as special cases postselection and reverse reconciliation, but does not include noisy processing. Maurer showed that two-way public discussion can be strictly stronger than one-way. He also suggested that in the two-way setting noisy processing might give no benefit [8]. Evidence suggesting the opposite later was given in [25].

By considering the classical unambiguous probability distributions that yield private bound-entangled states, we find that in general public discussion alone is insufficient for optimal key extraction even in the two-way setting. Stronger still, while no key can be distilled using only public discussion, a positive rate is achieved by noisy processing and one-way discussion.

Conclusions.—We have concentrated on the analogy between quantum entanglement distillation and classical key distillation using only public discussion, and abandoned for now the search for bound information, which remains an important open question. This led us to observe the dual nature of unambiguous distributions and quantum states, which in turn suggested a proof that noisy processing is necessary for two-way key distillation. While this finding concerns a purely classical question, reaching this conclusion appears to require a detour through quantum mechanics—we know of no classical proof. This suggests an exciting possibility of using quantum means to solve other questions in classical cryptography and information theory.

Along the way we found a new construction of private bound-entangled states. The standard construction involves two systems for each party: a key system yielding private correlations upon measurement, and a shield system that weakens Eve's correlation with the key [11,12]. Our construction does not employ the key or shield distinction. Instead, we first construct a classical unambiguous probability distribution and promote it to a private bound-entangled quantum state. This gives an example in 3 × 3 dimensions, which is too small to accommodate key and shield subsystems. We also find an example in 4 × 4 with more key than that of [12], and further examples in other dimensions. Of course, though our constructions do not have a clear key or shield separation, a protocol that distills key from many copies of our states produces trash that cannot be safely handed over to Eve (the state is bound entangled after all). This trash can then be identified as the shield of the purified key.

Bound-entangled states are not just a curious mathematical construction—their existence has been verified experimentally [26–34]. The Smolin state was prepared using polarized photons [27,28,33,34] and trapped ions [29]. A pseudo-bound-entangled state was created using nuclear magnetic resonance [30]. A continuous-variable bound-entangled state of light was prepared by [31]. Finally, states with more distillable key than entanglement have been prepared [32,33]; however, they are not bound.

So far no experiment has demonstrated a private bound-entangled state. The simplest known example is given by our construction (Fig. 2). It can be prepared by randomly sampling four pure entangled two-qutrit states (three have Schmidt rank 2 and one has Schmidt rank 3). Furthermore, their amplitudes are real, so each individual state can be prepared by performing rotations around a single axis in the two-dimensional subspace spanned by $|00\rangle_{AB}$ and $|11\rangle_{AB}$, and permuting the standard basis vectors $|0\rangle$, $|1\rangle$, $|2\rangle$ of each qutrit.

Our work may facilitate an experimental demonstration of superactivation—a phenomenon wherein pairs of quantum channels, neither of which can transmit quantum information on its own, nevertheless have positive capacity when used together [35]. Channels with zero quantum capacity but positive private classical capacity are central to the phenomenon, and these can easily be constructed from our private bound-entangled states. Indeed, our 3 × 3 state gives rise to a zero-capacity channel acting on a single qutrit that can be superactivated by a 50% erasure channel with four-dimensional input, the smallest known example.

We acknowledge Charles Bennett and Debbie Leung for commenting on an earlier version of this manuscript. We also thank the anonymous referees for bringing Ref. [36] to our attention and for other useful suggestions. This work was supported by DARPA QUEST program under Contract No. HR0011-09-C-0047.

[1] C. E. Shannon, Bell Syst. Tech. J. **28**, 656 (1949).

[2] A. D. Wyner, Bell Syst. Tech. J. **54**, 1355 (1975).

[3] I. Csiszár and J. Körner, IEEE Trans. Inf. Theory **24**, 339 (1978).

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

[5] H.-K. Lo and H. F. Chau, Science **283**, 2050 (1999).

[6] C. H. Bennett, G. Brassard, and J.-M. Robert, SIAM J. Comput. **17**, 210 (1988).

[7] R. F. Ahlswede and I. Csiszár, IEEE Trans. Inf. Theory **39**, 1121 (1993).

[8] U. M. Maurer, IEEE Trans. Inf. Theory **39**, 733 (1993).

[9] C. H. Bennett, G. Brassard, C. Crépeau, and U. M. Maurer, IEEE Trans. Inf. Theory **41**, 1915 (1995).

[10] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, Phys. Rev. A, **54**, 3824 (1996).

[11] K. Horodecki, M. Horodecki, P. Horodecki, and J. Oppenheim, Phys. Rev. Lett., **94**, 160502 (2005).

[12] K. Horodecki, Ł. Pankowski, M. Horodecki, and P. Horodecki, IEEE Trans. Inf. Theory **54**, 2621 (2008).

[13] Trash systems include all purifying systems too, hence, a shared classical key is not private from Eve in this setting.

[14] This does not impose any restrictions by itself. The crucial difference is that all auxiliary variables must be surrendered to Eve at the end of the protocol.

[15] N. Gisin, R. Renner, and S. Wolf, Algorithmica **34**, 389 (2002).

[16] R. Renner and S. Wolf, *Advances in Cryptology—EUROCRYPT 2003*, Vol. 2656, Lecture Notes in Computer Science (Springer, New York, 2003), p. 562.

[17] A. Acín, J. I. Cirac, and L. Masanes, Phys. Rev. Lett. **92**, 107903(2004).

[18] G. Prettico and A. Acín, arXiv:1203.1445.

[19] Distributions with similar properties have been considered before: tripartite distributions that satisfy only Eq. (3) appeared in [36]; bipartite distributions with similar properties (called bi-disjoint distributions) appeared in [37].

[20] Normally one has to specify the system on which the partial transpose is performed. However, all our density matrices are real (and thus symmetric), so the partial transpose on Alice's side is equivalent to partial transpose on Bob's side.

[21] M. Horodecki, P. Horodecki, and R. Horodecki, Phys. Rev. Lett. **80**, 5239 (1998).

[22] All the Appendixes are available in the Supplemental Material [23]. The Appendixes also contain a detailed description of our state construction and additional examples.

[23] This was first observed in [36] (see Supplemental Material at http://link.aps.org/supplemental/10.1103/PhysRevLett.112.110502 for our proof).

[24] The mutual information between classical random variables X and B is defined as $I(X;B) := H(X) + H(B) - H(XB)$, where H is the entropy function given by $H(A) := -\sum_a p(a) \log\, p(a)$.

[25] A. Acín, N. Gisin, and L. Masanes, Phys. Rev. Lett. **97**, 120405 (2006).

[26] R. Horodecki, Europhysics News **41**, 21 (2010).

[27] E. Amselem and M. Bourennane, Nat. Phys. **5**, 748 (2009).

[28] J. Lavoie, R. Kaltenbaek, M. Piani, and K. J. Resch, Phys. Rev. Lett. **105**, 130501 (2010).

[29] J. T. Barreiro, P. Schindler, O. Gühne, T. Monz, M. Chwalla, C. F. Roos, M. Hennrich, and R. Blatt, Nat. Phys. **6**, 943 (2010).

[30] H. Kampermann, D. Bruß, X. Peng, and D. Suter, Phys. Rev. A **81**, 040304 (2010).

[31] J. DiGuglielmo, A. Samblowski, B. Hage, C. Pineda, J. Eisert, and R. Schnabel, Phys. Rev. Lett. **107**, 240503 (2011).

[32] K. Dobek, M. Karpiński, R. Demkowicz-Dobrzański, K. Banaszek, and P. Horodecki, Phys. Rev. Lett. **106**, 030501 (2011).

[33] K. Dobek, M. Karpiński, R. Demkowicz-Dobrzański, K. Banaszek, and P. Horodecki, Laser Phys. **23**, 025204 (2013).

[34] E. Amselem, M. Sadiq, and M. Bourennane, Sci. Rep. **3**, 1966 (2013).

[35] G. Smith and J. Yard, Science **321**, 1812 (2008).

[36] M. Christandl, A. Ekert, M. Horodecki, P. Horodecki, J. Oppenheim, and R. Renner, In *Theory of Cryptography*, Lecture Notes in Computer Science Vol. 4392, edited by S. P. Vadhan (Springer, New York, 2007), p. 456.

[37] J. Oppenheim, R. W. Spekkens, and A. Winter, arXiv:quant-ph/0511247.