Bound entangled states with secret key and their classical counterpart

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

Entanglement is a fundamental resource for quantum information processing. In its pure form, it allows quantum teleportation [1] and sharing classical secrets [2]. 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 [3], yet sometimes still have a private classical key [4, 5]. We present a new and unexpected construction of bound entangled states with private key based on classical probability distributions. This construction gives a remarkable and long-sought classical analogue of bound entanglement [6–9]. 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 key from them.

I. 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 [10–12] or quantum state [2, 13]. 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, key distillation—the process of generating perfectly random, private and identical key from a given tripartite probability distribution $P_{ABE}$ shared among the three parties—and its quantum analogue, entanglement distillation, are problems of fundamental importance [11, 12, 14–18].

Depending on the shared resource and the task at hand, the parties might want to distill a private classical key (say, for use in a one-time pad) or entanglement in the form of Einstein-Podolsky-Rosen (EPR) pairs (say, for teleportation). Private key is weaker than entanglement: it can be obtained by measuring EPR pairs [2]. Thus, one can distill private key from a quantum state by first distilling EPR pairs. However, 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 [4]. Understanding bound entanglement is one of the deepest problems in quantum information theory and the key to unraveling several mysteries of entanglement [19–22].

Is there a classical analogue of bound entanglement? Previous studies have sought such a connection in the secret key agreement venue, looking for classical distributions from which no secret key could be distilled [6–9]. A particular classical distribution obtained by measuring a bound-entangled quantum state was considered in [6]. 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, whose existence demonstrates a clear distinction between secrecy and bound entanglement [4, 5].

| States | Quantum | Classical |
|--------|---------|----------|
| $|\psi\rangle_{ABE}$ | unambiguous quantum state | $P_{ABE}$ | unambiguous probability distribution |
| Entanglement distillation | $D(\rho_{AB})$ | EPR pairs by LOCC | $K_{PD}(P_{ABE})$ | secret key by public discussion |
| Secret key distillation | $K(\rho_{AB})$ | secret key by LOCC | $K(P_{ABE})$ | secret key by public discussion and noisy processing |

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) and its reduced state $\rho_{AB}$ is given by Eq. (5). The distillable entanglement from $\rho_{AB}$ shared between Alice and Bob is at least as large as the optimal key rate that can be distilled from the probability distribution $P_{ABE}$ using the standard protocols of public discussion, error correction and privacy amplification. The distillable key of the quantum state is an upper bound for the optimal key rate distillable from the classical distribution using the standard protocols together with noisy processing.

Below we provide a clean classical analogue of bound entanglement and private bound entanglement. It is based on an object that can be expressed as either a quantum state or a classical distribution. I.e., there is a one-to-one correspondence between a subset of tripartite pure quantum states $|\psi_{ABE}\rangle$ and tripartite classical probability distributions $P_{ABE}$. We call these states/distributions unambiguous (see Table I). We use this dual quantum/classical nature to establish several analogies between quantum and classical phenomena (see Table I). The impossibility of distilling entanglement...
from our quantum state using local operations and classical communication (LOCC) translates directly into the inability of classical parties to extract key from the associated distribution using the standard protocols of two-way public discussion, error correction, and privacy amplification. Similarly, the fact that quantum parties can still distill a secret key by LOCC has implications for the associated classical probability distributions. Indeed, key can be distilled from the classical distribution by augmenting the standard public discussion protocols with a noisy processing step. The fact that noisy processing is necessary in two-way distillation is new, and although no simple formula for $K(\rho_{AB})$ [3] exists, the deviation 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.

The partial transpose $^{1}$ (PT) of $\rho_{AB}$ is defined on the standard basis as

$$ (|a\rangle\langle a'|_A \otimes |b\rangle\langle b'|_B)^T := |a\rangle\langle a'|_A \otimes |b\rangle\langle b'|_B $$

and extended by linearity. If $\rho_{AB}$ is PT-invariant ($\rho_{AB} = \rho_{AB}^T$) then it has positive partial transpose and thus no distillable entanglement [3].

We now restrict to unambiguous distributions $P_{ABE}$ that yield PT-invariant states $\rho_{AB}$ (see Appendix B), and maximize the distillable key $K(\rho_{AB})$. While there is in general no simple formula for $K(\rho_{AB})$, Devetak and Winter [23] gave a lower bound $^{2}$

$$ K(\rho_{AB}) \geq I(X; B) - I(X; E). $$

Here the right-hand side is evaluated on the state $\rho_{XBE}$ which results from $|\psi\rangle_{ABE}$ when Alice performs a measurement whose outcome is $X$. The resulting positive rate gives the private bound entanglement we sought. Table II summarizes our findings for various dimensions, and Fig. 2 shows the structure of our smallest example, a $3 \times 3$ state, in detail. Explicit parameters for all these examples can be found in Appendix A.

1 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.

2 Here $I(X; B) := S(X) + S(B) − S(XB)$ is the quantum mutual information between $X$ and $B$, defined in terms of the von Neumann entropy $S(\rho) := −\text{Tr}(\rho \log \rho)$. 

---

**II. CONSTRUCTION**

Our construction is based on tripartite probability distributions $P_{ABE}$ whose probabilities $p(a, b, c)$ have a special combinatorial structure (see Fig. 1):

$$ \forall a, b, c \quad |\{a : p(a, b, c) > 0\}| \leq 1, $$

$$ \forall a, b, c \quad |\{b : p(a, b, c) > 0\}| \leq 1, $$

$$ \forall a, b, c \quad |\{c : p(a, b, c) > 0\}| \leq 1, $$

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

$$ |\psi\rangle_{ABE} := \sum_{a, b, c} \sqrt{p(a, b, c)} |a\rangle_A |b\rangle_B |c\rangle_E $$

where the states $|a\rangle_A, |b\rangle_B, |c\rangle_E$ are orthonormal bases for systems $A, B, E$ respectively, and with a bipartite mixed state

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

on Alice and Bob whose purification is held by Eve. Such states have a special structure, since all eigenvectors of $\rho_{AB}$ have the same Schmidt basis.
TABLE II. A summary of private bound entangled states obtained using our construction. Here $d_A$ and $d_B$ are the dimensions of Alice and Bob, $d_E$ is the dimension of Eve. The third column is a numerical lower bound on the amount of distillable private key. The amount of private key in our $4 \times 4$ example exceeds 0.0213399 achieved by [5]. Our $4 \times 4$ example can be embedded in the $5 \times 6$ and $6 \times 5$ 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 |
|------------------|-------|---------------------|
| $3 \times 3$     | 4     | 0.00657852          |
| $4 \times 4$     | 6     | 0.0293914           |
| $4 \times 5$     | 8     | 0.0480494           |
| $5 \times 6$     | 10    | 0.0378462           |
| $6 \times 5$     | 10    | 0.0354342           |

III. IMPLICATIONS FOR CLASSICAL KEY AGREEMENT

There are a number of techniques for classical key agreement. The most fundamental is a combination of error correction and privacy amplification (EC+PA), which achieves a rate of the mutual information difference $I(A;B) - I(A;E)$ [11]. 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 [12]. Similarly, Maurer considered public discussion protocols where Alice and Bob exchange the information about their variables in a two-way fashion [16]. Public discussion includes as special cases post-selection and reverse reconciliation, but does not include noisy processing. Maurer showed that two-way public discussion can be strictly stronger than one-way. But it has been assumed that in the two-way setting noisy processing gives no benefit.

By considering the classical unambiguous probability distributions associated with 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 from these distributions using public discussion, a positive rate is achieved by noisy processing and one-way discussion.

Our methods use the following observation (see Appendix C): any classical key-distillation protocol on the distribution $P_{ABE}$ can be boosted to a key-distillation protocol with the same rate on state $\rho_{AB}$ defined in Eq. (5). Similarly, any classical key distillation protocol on $P_{ABE}$ using only public discussion can be boosted to a quantum protocol with the same rate but yielding pure entanglement. The examples we have given are bound entangled, so the distillable key by public discussion must be zero. Nevertheless, secure key can be extracted by LOCC. Because of the special form of our states, these protocols can be converted into classical protocols for distilling secure key from the associated unambiguous distribution using noisy local processing in addition to public communication. This analogy is summarized in Table I. We thus have found the desired classical analogues of bound entanglement and private bound entanglement.
IV. CONCLUSIONS

The standard construction of private bound entangled states involves two systems for each party [4, 5], a “key” system yielding private correlations upon measurement, and a “shield” system that weakens Eve’s correlation with the key. Our construction is fundamentally different. It promotes an unambiguous classical probability distribution to a quantum state without employing the key/shield distinction. 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 [5], and further examples in other dimensions.

While our finding that noisy processing is necessary for two-way key distillation concerns a purely classical question, reaching this conclusion appears to require a detour through quantum mechanics—we know of no classical proof of this result. This suggests an exciting possibility of using quantum means to solve other questions in classical cryptography and information theory.

Bound entangled states are not just a curious mathematical construction—their existence has been verified experimentally in several physical systems [24–31]. The Smolin state was prepared using polarized photons [25, 26, 31] and later using trapped ions [27]. A pseudo-bound entangled state was created using nuclear magnetic resonance [28]. A continuous-variable bound entangled state of light was prepared by [29]. Finally, states with more distillable key than entanglement have been prepared [30, 31], however they are not bound.

So far no experiment has demonstrated a private bound entangled state. The simplest known such state is given by our construction (see Fig. 2). It can be prepared by randomly sampling four pure entangled two-qutrit states (three of them 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⟩_{AB} and |11⟩_{AB}, and permuting the standard basis vectors 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 [20]. 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 4-dimensional input, which is the smallest known example.

ACKNOWLEDGMENTS

We acknowledge Charles Bennett and Debbie Leung for commenting on an earlier version of this manuscript. This work was supported by DARPA QUEST program under contract number HR0011-09-C-0047.

[1] Charles H. Bennett, Gilles Brassard, Claude Crépeau, Richard Jozsa, Asher Peres, and William K. Wootters. Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. Phys. Rev. Lett., 70(13):1895–1899, Mar 1993. doi:10.1103/PhysRevLett.70.1895.

[2] Artur K. Ekert. Quantum cryptography based on bell’s theorem. Phys. Rev. Lett., 67(6):661–663, Aug 1991. doi:10.1103/PhysRevLett.67.661.

[3] Michał Horodecki, Paweł Horodecki, and Ryszard Horodecki. Mixed-state entanglement and distillation: Is there a “bound” entanglement in nature? Phys. Rev. Lett., 80(24):5239–5242, Jun 1998. arXiv:quant-ph/9801069, doi:10.1103/PhysRevLett.80.5239.

[4] Karol Horodecki, Michał Horodecki, Paweł Horodecki, and Jonathan Oppenheim. Secure key from bound entanglement. Phys. Rev. Lett., 94(16):160502, Apr 2005. arXiv:quant-ph/0309110, doi:10.1103/PhysRevLett.94.160502.

[5] Karol Horodecki, Łukasz Pankowski, Michał Horodecki, and Paweł Horodecki. Low-dimensional bound entanglement with one-way distillable cryptographic key. Information Theory, IEEE Transactions on, 54(6):2621–2625, 2008. arXiv:quant-ph/0506203, doi:10.1109/TIT.2008.921709.

[6] Nicolas Gisin, Renato Renner, and Stefan Wolf. Linking classical and quantum key agreement: Is there a classical analog to bound entanglement? Algorithmica, 34(4):389–412, 2002. arXiv:quant-ph/0005042, doi:10.1007/s00453-002-0972-7.

[7] Renato Renner and Stefan Wolf. New bounds in secret-key agreement: The gap between formation and secrecy extraction. In Advances in Cryptology – EUROCRYPT 2003, volume 2656 of Lecture Notes in Computer Science, pages 562–577. Springer, 2003. doi:10.1007/3-540-39200-9_35.

[8] Antonio Acín, J. Ignacio Cirac, and Lluis Masanes. Multiparticle bound information exists and can be activated. Phys. Rev. Lett., 92(10):107903, Mar 2004. arXiv:quant-ph/0311064, doi:10.1103/PhysRevLett.92.107903.

[9] Giuseppe Pretiico and Antonio Acín. Can bipartite classical information resources be activated? 2012. arXiv:1203.1445.

[10] Claude E. Shannon. Communication theory of secrecy systems. Bell System Technical Journal, 28(4):656–715, Oct 1949. URL: http://www3.alcatel-lucent.com/bstj/vol28-1949/articles/bstj28-4-656.pdf.

[11] Aaron D. Wyner. The wire-tap channel. Bell System Technical Journal, 54(8):1355–1387, Oct 1975. URL: http://www3.alcatel-lucent.com/bstj/vol54-1975/
In this appendix we give a list of unambiguous probability distributions $P_{ABE}$ in various small dimensions obtained by our construction (see Table II for a summary). They are specified using the graphical representation explained in Fig. 2. In each case we provide the two-dimensional diagram on $AB$ together with the reduced distribution $P_{AB}$ (rows correspond to Alice and columns to Bob, and symbol $X$ indicates that Alice and Bob’s variables never have the corresponding value: see Eq. (B1) in Appendix B). In addition, we list the value of $K(P_{ABE})$ and the conditional distribution $Q_{X|A}$ that describes the noisy processing performed by Alice to obtain a random variable $X$ from $A$ (rows of $Q_{X|A}$ correspond to $X$ and columns correspond to Alice). In all cases we chose $X$ to be of dimension two, which was sufficient for obtaining a positive rate.

Appendix A: Examples
$$K(P_{ABE}) \geq 0.0057852$$

$$P_{AB} = \begin{pmatrix}
0.167184 & 0.171529 & 0.001243 \\
0.089041 & 0.091355 & 0.017492 \\
0.441714 & 0.017157 & 0.003285
\end{pmatrix}$$

$$Q_{X|A} = \begin{pmatrix}
1 & 0 & 0.670965 \\
0 & 1 & 0.329035
\end{pmatrix}$$

$$K(P_{ABE}) \geq 0.0293914$$

$$P_{AB} = \begin{pmatrix}
0.024798 & 0.033970 & 0.128999 & 0.009393 \\
0 & 0.087320 & 0.094498 & 0.035793 \\
0.128999 & 0.024798 & 0.103690 & 0.035793
\end{pmatrix}$$

$$Q_{X|A} = \begin{pmatrix}
1 & 0 & 1 & 0 \\
0 & 1 & 0 & 1
\end{pmatrix}$$

$$K(P_{ABE}) \geq 0.0480494$$

$$P_{AB} = \begin{pmatrix}
0.015228 & 0.033970 & 0.092123 & 0.004989 & 0.103690 \\
0.103690 & 0.033970 & 0.092123 & 0.004989 & 0.015228 \\
0.015228 & 0.004989 & 0.092123 & 0.033970 & 0.103690
\end{pmatrix}$$

$$Q_{X|A} = \begin{pmatrix}
1 & 1 & 0 & 0 \\
0 & 0 & 1 & 1
\end{pmatrix}$$

$$K(P_{ABE}) \geq 0.0378462$$

$$P_{AB} = \begin{pmatrix}
0.076349 & 0.004299 & 0.070542 & 0 & 0 & 0.014384 \\
0.014674 & 0.006016 & 0.098724 & 0.006016 & 0.014674 & 0.098724 \\
0.050896 & 0.020867 & 0.047025 & 0.020867 & 0.050896 & 0.047025 \\
0 & 0 & 0.014384 & 0.004299 & 0.076349 & 0.070542 \\
0 & 0.022142 & 0.074083 & 0.022142 & 0 & 0.074083
\end{pmatrix}$$

$$Q_{X|A} = \begin{pmatrix}
0 & 0 & 1 & 0 & 1 & 1 \\
1 & 1 & 0 & 1 & 0 & 1
\end{pmatrix}$$

$$K(P_{ABE}) \geq 0.0354342$$

$$P_{AB} = \begin{pmatrix}
0.026574 & 0.061138 & 0.065969 & 0 & 0 \\
0.003409 & 0.056660 & 0.061138 & 0 & 0.011779 \\
0.004843 & 0.080489 & 0.012023 & 0.026034 & 0.089945 \\
0 & 0.056660 & 0.061138 & 0.003409 & 0.011779 \\
0 & 0.061138 & 0.065969 & 0.026574 & 0 \\
0.026034 & 0.080489 & 0.012023 & 0.004843 & 0.089945
\end{pmatrix}$$

$$Q_{X|A} = \begin{pmatrix}
0 & 1 & 1 & 0 & 1 & 0 \\
1 & 0 & 0 & 1 & 0 & 1
\end{pmatrix}$$
Appendix B: PT-invariance

In this appendix we describe the PT-invariance condition of $\rho_{AB}$ in terms of the underlying unambiguous distribution $P_{ABE}$. Recall from Eqs. (1) to (3) in Sect. II that $P_{ABE}$ is unambiguous if any two parties can together recover the value of the third party’s variable. For example, if Alice has $a$ and Bob has $b$, then Eve’s value is

$$e(a, b) := \begin{cases} e & \text{if } p(a, b, e) \neq 0, \\ \mathbb{Y} & \text{otherwise,} \end{cases}$$  \hfill (B1)

where $\mathbb{Y}$ (guzz) is a special symbol that lies outside of Eve’s alphabet [32] and indicates that Alice and Bob never have the pair $(a, b)$. Notice that the reduced distribution on Alice and Bob is given by

$$p(a, b) := \sum_{e} p(a, b, e) = \begin{cases} 0 & \text{if } e(a, b) = \mathbb{Y}, \\ p(a, b, e(a, b)) & \text{otherwise.} \end{cases}$$  \hfill (B2)

Recall from Eq. (6) that a bipartite state $\rho_{AB}$ is PT-invariant if $\rho_{AB}^T = \rho_{AB}$, where the partial transposition is defined on the standard basis as

$$(|a\rangle\langle a'|_A \otimes |b\rangle\langle b'|_B)^T := |a\rangle\langle a'|_A \otimes |b\rangle\langle b'|_B$$  \hfill (B3)

and extended by linearity. The following lemma relates PT-invariance of $\rho_{AB}$ to two properties of the underlying unambiguous distribution $P_{ABE}$. The first property says that the diagram associated to $P_{ABE}$ can be obtained by superimposing several crosses (see Fig. 2), and the second property says that each $2 \times 2$ submatrix corresponding to a cross has rank one. For example, if $P_{ABE}$ has the diagram shown in Fig. 2, then the entries of $P_{AB}$ must satisfy

$$\det \begin{pmatrix} p_{00} & p_{01} \\ p_{10} & p_{11} \end{pmatrix} = \det \begin{pmatrix} p_{11} & p_{12} \\ p_{21} & p_{22} \end{pmatrix} = \det \begin{pmatrix} p_{00} & p_{02} \\ p_{20} & p_{22} \end{pmatrix} = 0.$$

**Lemma 1.** Let $P_{ABE}$ be an unambiguous probability distribution. Then the following condition on $P_{ABE}$ is equivalent to $\rho_{AB}$ being PT-invariant: if $e(a, b) = e(a', b') \neq \mathbb{Y}$ for some $a \neq a'$ and $b \neq b'$ then

1. $e(a, b') = e(a', b) \neq \mathbb{Y}$, and
2. $p(a, b)p(a', b') = p(a, b')p(a', b),$

where $e(a, b)$ and $p(a, b)$ are defined in Eqs. (B1) and (B2), respectively.

**Proof.** We expand $\rho_{AB}$ using Eqs. (5) and (4) and compute the partial transpose according to Eq. (B3):

$$\left(\rho_{AB}\right)^T = \left(\text{Tr}_E |\psi\rangle\langle\psi|_{ABE}\right)^T$$

$$= \sum_{e} \left( \sum_{a,a',b,b'} \sqrt{p(a, b, e)p(a', b', e)} |a\rangle\langle a'|_A \otimes |b\rangle\langle b'|_B \right)^T$$

$$= \sum_{e} \left( \sum_{a,a',b,b'} \sqrt{p(a, b', e)p(a', b, e)} |a\rangle\langle a'|_A \otimes |b\rangle\langle b'|_B \right),$$

where we relabeled $b$ and $b'$. This is equal to $\rho_{AB}$ if and only if

$$\forall a, a', b, b': \sum_{e} \sqrt{p(a, b, e)p(a', b', e)} = \sum_{e} \sqrt{p(a, b', e)p(a', b, e)}.$$

Since $P_{ABE}$ is unambiguous, each of the two sums contains at most one nonzero term. Moreover, both sides are nonzero exactly when the first condition holds, and equal exactly when the second condition holds.

**Appendix C: Classical-quantum correspondence**

The main reason for introducing unambiguous probability distributions is Theorem 5 that establishes a relationship between the rate $K_{PD}(P_{ABE})$ of private key that can be distilled from an unambiguous probability distribution $P_{ABE}$ by public discussion, and the distillable entanglement $D(\rho_{AB})$ of the quantum version $\rho_{AB}$ of that distribution. The proof of this theorem follows from several lemmas.
Lemma 2. Let $P_{ABE}$ be an unambiguous distribution, and suppose $P_{AM,BM,EM}$ can be generated from $P_{ABE}$ by public discussion where $M$ is the public message. Then the probability distribution $P_{AM,BM,EM}$ is also unambiguous.

Proof. It suffices to consider only 1-round protocols, since the general case follows by induction. Without loss of generality, let the protocol consist of a message $m$ sent from $A$ to $B$ according to some conditional distribution $q(m|a)$. The probability distribution $P_{AM,BM,EM}$ is then given by $p((a,m),(b,m),(e,m)) = p(a,b,e)q(m|a)$. To check that $P_{AM,BM,EM}$ is unambiguous, we fix $(b,m)$ and $(e,m)$ (or equivalently $b,e,m$) and verify that

\[
\{(a,m) : p((a,m),(b,m),(e,m)) \neq 0\} = \{(a,m) : p(a,b,e)q(m|a) \neq 0\}
\]

\[
\leq |\{a : p(a,b,e) \neq 0\}|
\]

\[
\leq 1,
\]

which is the first condition in Eq. (1). Similarly, we find the second two conditions are satisfied.

Lemma 3. If $P_{AM,BM,EM}$ can be generated by public discussion from $P_{ABE}$, then the corresponding quantum state $\rho_{AM,BM}$ can be generated from $\rho_{AB}$ by LOCC.

Proof. We begin by proving the result for one-way protocols from Alice to Bob. Let Alice’s message $m$ be chosen according to conditional distribution $q(m|a)$. Then the probabilities of $P_{AM,BM,EM}$ are given in terms of $P_{ABE}$ by $p((a,m),(b,m),(e,m)) = p(a,b,e)q(m|a)$. In the quantum case, $\rho_{AM,BM}$ can be obtained from $\rho_{AB}$ by having Alice perform a POVM with Kraus operators

\[
A_m = \sum_a \sqrt{q(m|a)}|a\rangle\langle a|_A
\]

and keeping a copy of $m$ as well as sending it to both Bob and Eve. The multi-round result follows by repeatedly applying this observation.

Let us state some definitions that are necessary for the next lemma. The coherent information of a state $\rho_{AB} = \text{Tr}_E|\psi\rangle\langle\psi|_{ABE}$ is given by $I(A|B)_{\rho_{AB}} := S(B) - S(E)$. The advantage of a tripartite distribution $P_{ABE}$ is given by $A(P_{ABE}) := I(A;B) - I(A;E)$.

Lemma 4. Let $P_{ABE}$ be an unambiguous classical tripartite distribution. Then,

\[
I(A|B)_{\rho_{AB}} = A(P_{ABE}).
\]

Proof. The advantage of $P_{ABE}$ is given by

\[
A(P_{ABE}) = I(A;B) - I(A;E)
\]

\[
= H(B) - H(B|A) - H(E) + H(E|A).
\]

Since $P_{ABE}$ is unambiguous, from Eq. (1), we know that for fixed $a$, conditional distributions on $B$ and $E$ are identical up to relabeling of the outputs. Thus, for a fixed $a$ we have $H(B|A = a) = H(E|A = a)$, which implies $H(B|A) = H(E|A)$. This gives us

\[
A(P_{ABE}) = H(B) - H(E),
\]

where the RHS is evaluated on the classical variables $B$ and $E$ distributed according to $p(a,b,e)$.

Now, note that

\[
I(A|B)_{\rho_{AB}} = S(B) - S(E),
\]

with the entropies evaluated on $|\psi\rangle\langle\psi|_{ABE}$. From Eqs. (3) and (2) applied to $|\psi\rangle_{ABE}$, we find that

\[
\rho_E = \sum_{a,b,c} p(a,b,c)|e\rangle\langle e|,
\]

\[
\rho_B = \sum_{a,b,c} p(a,b,c)|b\rangle\langle b|,
\]

so that the von Neumann entropies on the right-hand side of Eq. (C9) are identical to the Shannon entropies in Eq. (C8), which proves the result.
Theorem 5. Let $P_{ABE}$ be an unambiguous probability distribution. Then, the distillable entanglement of $\rho_{AB}$ is at least as big as the distillable key by public discussion of $P_{ABE}$:

$$D(\rho_{AB}) \geq K_{PD}(P_{ABE}).$$

Proof. Suppose we can achieve a key rate $R$ by using public discussion to distill from $P_{ABE}$. Then, for every $\delta > 0$ there is an $n$ and a public discussion protocol with message history $M$ yielding distribution $P_{A^nB^nM^nE^nM^n}$ that gives an advantage $\frac{1}{2} A(P_{A^nM^nB^nM^nE^nM^n}) > R - \delta$. By Lemma 2 we know that $P_{A^nM^nB^nM^nE^nM^n}$ is unambiguous, so that Lemma 3 implies that the corresponding quantum state $\rho_{A^nM^nB^nM^n}$ can be generated from $n$ copies of $\rho_{AB}$ by LOCC. Furthermore, Lemma 4 implies that the coherent information of $\rho_{A^nM^nB^nM^n}$ is equal to $A(P_{A^nM^nB^nM^nE^nM^n})$. Since the coherent information is an achievable rate of entanglement distillation, we thus find that the distillable entanglement of $\rho_{AB}$ is at least and can be made arbitrarily close to $R$. \hfill \Box

The following lemma shows a relationship between the distillable key of an unambiguous probability distribution, and the key that can be distilled from its quantum version using a particular “classical” strategy.

Lemma 6. Let $P_{ABE}$ be an unambiguous probability distribution. Then,

$$K(\rho_{AB}) \geq K(P_{ABE}).$$

Proof. Alice and Bob make local copies of the variables they have and then proceed with the classical protocol. The local copies ensure that Eve is dephased in the standard basis. The security of the classical protocol implies that Eve is ignorant of the key also in the quantum case. \hfill \Box

Appendix D: Deferral of noisy processing

In this appendix we argue that classical randomized private key distillation protocols can without loss of generality be cast in a specific form. In Sect. III we described two types of protocols (see Fig. 3): ones that involve a noisy processing step, which can modify the local random variables by a stochastic map, and ones that do not. The following lemma shows that the two types of protocols described in Fig. 3 are the most general ones for the cases of not having noisy processing and having noisy processing, respectively.

Lemma 7. The following holds:

1. if noisy processing is not involved, there is no advantage for Alice and Bob to introduce extra local random variables other than those initially given to them (i.e., $A$ for Alice and $B$ for Bob);

2. if noisy processing is allowed throughout the protocol, it can always be deferred till the very last step.

Proof. For the first claim, note that each step of any classical randomized protocol can be described in terms of a conditional probability distribution: the probability of generating a particular value of any new random variable in terms of already existing variables. These can be used to generate a joint probability distribution of all variables—local variables and messages alike—throughout the protocol. Specifically, at the end of the protocol these give a distribution on $(A, A_1, \ldots, A_n, B, B_1, \ldots, B_n, M_1, \ldots, M_n)$, where $A_i$ and $B_i$ are the local random variables generated in the $i$th round of the protocol by Alice and Bob, respectively, $M_i$ is the $i$th message sent, and $n$ is the number of rounds. From this, we can compute a set of conditional distributions for messages $M_i$ conditioned solely on the previous messages and either $A$ or $B$ (depending on whether Alice or Bob generates $M_i$). Thus, in the last step Alice can first generate $(A, M_1, \ldots, M_n)$ and then use the conditional probability distributions for the $A_i$ given $(A, M_1, \ldots, M_n)$ to generate the remaining local random variables $(A_1, \ldots, A_n)$. Bob can generate his local random variables similarly. However, generating these extra variables at the last step of the protocol does not affect the final rate achieved by EC+PA. This follows by using the chain rule for the mutual information.

For the second claim, let’s assume that Alice and Bob use local noisy processing at every step of the protocol, and let $\tilde{A}_i$ and $\tilde{B}_i$ denote their local random variables at step $i$. For example, Alice produces $\tilde{A}_i$ and $M_i$ from $(\tilde{A}_{i-1}, M_1, \ldots, M_{i-1})$ by a stochastic map. However, imagine that instead of destroying her previous random variable $\tilde{A}_{i-1}$ every time, Alice makes a local copy of it and keeps it around. Such protocol has exactly the same form as described in the first scenario, except in the last step both parties have to destroy all their local variables except the last one. Now we can apply the same argument as before and defer the creation of the local variables till the last step. After that each party destroys all their local variables except the last one. This yields an equivalent randomized protocol, where noisy processing is applied only in the last step. \hfill \Box