A Classical Analog to Entanglement Reversibility

Eric Chitambar [1],* Ben Fortescue [1],† and Min-Hsiu Hsieh [2]‡

[1] *Department of Physics and Astronomy, Southern Illinois University, Carbondale, Illinois 62901, USA*
[2] *Centre for Quantum Computation & Intelligent Systems, University of Technology Sydney, NSW 2007, AU*

In this paper we introduce the problem of secrecy reversibility. This asks when two honest parties can distill secret bits from some tripartite distribution p_{XYZ} and transform secret bits back into p_{XYZ} at equal rates using local operation and public communication (LOPC). This is the classical analog to the well-studied problem of reversibly concentrating and diluting entanglement in a quantum state. We identify the structure of distributions possessing reversible secrecy when one of the honest parties holds a binary distribution, and it is possible that all reversible distributions have this form. These distributions are more general than what is obtained by simply constructing a classical analog to the family of quantum states known to have reversible entanglement. An indispensable tool used in our analysis is a conditional form of the Gács-Körner common information.

I. Introduction:

In any QKD protocol, the classical post-processing of measurement data is an essential step in obtaining secret key. For two-party secrecy, the measurement data typically consists of a tripartite distribution p_{XYZ}: Alice (X) and Bob (Y) share correlations about which, undesirably, Eve (Z) has side information. The distribution is manipulated using local operations and public communication (LOPC), and the goal is to obtain secret bits $\Phi_{XY} \cdot q_Z$. Here, $\Phi_{XY}(i,j) = (1/2)\delta_{ij}$ is a perfectly correlated bit while q_Z is an arbitrary and uncorrelated distribution. Inspired by the conceptual successes of entanglement theory and the distillation of entangled bits (ebits) under local operations and classical communication (LOCC), researchers have recently begun applying a resource-theoretic perspective toward the notion of secrecy in classical information theory [1, 2]. The goal of this paper is to better understand the problem of secret key distillation for application in QKD by sharpening the resource-theoretic characterization of secrecy.

Quantum entanglement and classical secrecy share many striking similarities [1–9]. One important similarity lies in the tasks of resource distillation and resource cost. For a bipartite quantum state ρ_{AB}, its *distillable entanglement* $E_D(\rho_{AB})$ quantifies, roughly speaking, the amount of ebits that can be distilled from ρ_{AB} using LOCC [10] (in the many-copy sense), while its *entanglement cost* $E_C(\rho_{AB})$ quantifies the amount of ebits required to generate ρ_{AB} using LOCC [11]. For a distribution p_{XYZ}, its "secrecy content" can analogously be quantified in terms of its distillable key $K_D(p_{XYZ})$ [12, 13] and its key cost $K_C(p_{XYZ})$ [14]. Here, the distillation goal is to obtain secret bits Φ_{XY} from p_{XYZ}, while the formation goal is simulate p_{XYZ} using Φ_{XY} and public communication. Compared to entanglement theory, much less is known about the relationship between K_D and K_C, except for the expected hierarchy $K_C \geq K_D$ [14]. The *secrecy reversibility problem* asks what distributions satisfy $K_C(p_{XYZ}) = K_D(p_{XYZ})$.

II. Introducing a Zoo of Distributions:

Our results involve identifying certain tripartite distributions with important secrecy properties. A hierarchy of such distributions and their relationship to the reversibility problem are summarized in Fig. 1. We quickly summarize the definitions here.

For distribution p_{XY}, a **maximal common function** is a variable J_{XY} such that

$$H(J_{XY}) = \max_K \{H(K) : 0 = H(K|X) = H(K|Y)\}. \tag{1}$$

The value $H(J_{XY})$ has been identified by Gács and Körner as the *common information* between X and Y [15]. It can be shown that for every p_{XY}, the variable J_{XY} is unique up to a relabeling of its range. For a tripartite distribution p_{XYZ}, we will denote a maximal common function of the conditional distribution $p_{XY|Z=z}$ by $J_{XY|Z=z}$. Then, a *maximal conditional common function* $J_{XY|Z}$ is just a collection of maximal common functions $\{J_{XY|Z=z} : p(z) > 0\}$. We say that a distribution p_{XYZ} is **block independent** (BI) if $I(X : Y|J_{XY|Z}Z) = 0$; equivalently, if the distribution decomposes as

$$p(x,y,z) = \sum_{J_{XY|Z=z}=j} p(x|z,j)p(y|z,j)p(j,z), \tag{2}$$

where $p(x|z,j)p(x|z,j') = 0$ and $p(y|z,j)p(y|z,j') = 0$ for $j \neq j'$. A BI distribution is called **secret block independent** (SBI) if Eve is uncorrelated from Alice and Bob (i.e. $p(j,z) = p(z)$). Next, a distribution is said to be **uniform block independent** (UBI) if it is block independent, and there exist local coarse-graining maps $K_X(X)$ and $K_Y(Y)$ such that $Pr[J_{XY|Z} = K_X = K_Y] = 1$ for some maximal common function $J_{XY|Z}$. In other words, Alice and Bob can determine the value for $J_{XY|Z}$ simply by consulting their local variable. With many copies of a UBI distribution, secret key can be distilled via privacy amplification at an optimal rate $H(J_{XY|Z}|Z) = I(X:Y|Z)$ [12, 16]. We say p_{XYZ} is **uniform block independent under public discussion** (UBI-PD) if it is BI and there is a public communication protocol generating messages M such that $p_{(MX)(MY)(ZM)}$ is UBI and $I(M:J_{XY|Z}|Z) = 0$. Finally, a distribution belongs to the class UBI-PD$\downarrow$ if there exists a channel $\overline{Z}|Z$ such that $p_{XY|\overline{Z}}$ is UBI with the required public communication M also satisfying $I(Z:J_{XY|\overline{Z}}|M\overline{Z}) = 0$. For a distribution belonging to UBI-PD$\downarrow$, it can be shown that $K_D(p_{XYZ}) = I(X:Y \downarrow Z)$.

III. Results:

Here we summarize our results. Proofs can be found in [17].

Lemma 1. *For the distribution p_{XYZ}, $K_C(p_{XYZ}) \geq I(X:Y \downarrow Z)$. Equality is obtained iff $p_{XY\overline{Z}}$ is BI, where $\overline{Z}|Z$ is the minimizer in $I(X:Y \downarrow Z)$. When equality holds, $K_C(p_{XYZ}) = I(X:Y \downarrow Z) = H(J_{XY|\overline{Z}}|\overline{Z})$.*

Due to their structure, every UBI-PD$\downarrow$ distribution demonstrates $K_D(p_{XYZ}) = I(X:Y \downarrow Z)$. Furthermore, since these distributions admit a channel $\overline{Z}|Z$ with $p_{XY\overline{Z}}$ being BI, Lemma 1 gives that $K_D(p_{XYZ}) = K_C(p_{XYZ})$ for every UBI-PD$\downarrow$ distribution. We have thus identified a family of distributions possessing reversible secrecy, and we conjecture that this family completely characterizes secrecy reversibility in the classical setting. The conjecture obviously holds true for any distribution with $0 = K_C(p_{XYZ}) = K_D(p_{XYZ})$ since $K_C(p_{XYZ}) = 0$ implies $I(X:Y \downarrow Z) = 0$ by Lemma 1, and any distribution satisfying the latter condition is UBI-PB$\downarrow$ by definition. The conjecture can also be shown as true for distributions satisfying $\min\{|\mathcal{X}|, |\mathcal{Y}|\} = 2$.

Conjecture 1. *$K_C(p_{XYZ}) = K_D(p_{XYZ})$ iff p_{XYZ} is UBI-PD$\downarrow$.*

Theorem 1. *If $\min\{|\mathcal{X}|, |\mathcal{Y}|\} = 2$, then $K_C(p_{XYZ}) = K_D(p_{XYZ})$ iff p_{XYZ} is UBI-PD$\downarrow$.*

Comparing Reversible Secrecy and Reversible Entanglement:

An arbitrary distribution $p(x,y,z)$ can be embedded into a tripartite quantum state via the following prescription:

$$|\Psi\rangle_{ABE} = \sum_{x,y,z} \sqrt{p(x,y,z)}|xyz\rangle. \tag{3}$$

We first consider embedding reversible distributions into quantum states as in Eq. (3). In particular, we focus on distributions with $|\mathcal{X}| = |\mathcal{Y}| = 2$ so that the corresponding $\rho_{AB} := \mathrm{Tr}_E\,|\Psi\rangle\langle\Psi|_{ABE}$ is a two-qubit state. We can make a comparison between the secret key of the underlying distribution and the entanglement of the embedded quantum state using an analytic formula for the entanglement of formation E_F[18].

Theorem 2. *For reversible p_{XYZ} with $|\mathcal{X}| = |\mathcal{Y}| = 2$ and $K_D(p_{XYZ}) > 0$:*

$$K_D(p_{XYZ}) = \sum_{z\in\mathcal{Z}} p(z)\mathsf{E}\left(2\sqrt{p(0|z)p(1|z)}\right), \qquad E_F(\rho_{AB}) = \mathsf{E}\left(2\sum_{z\in\mathcal{Z}} p(z)\sqrt{p(0|z)p(1|z)}\right),$$

where $\mathsf{E}(x) := h(\frac{1}{2}[1-\sqrt{1-x^2}])$ is strictly convex in x for $h(x) := -x\log x - (1-x)\log(1-x)$. The equality $K_D(p_{XYZ}) = E_F(\rho_{AB})$ holds iff $H(X|Z=z)$ is constant for all $z \in \mathcal{Z}$.

It is natural to wonder whether a quantum state with an embedded reversible distribution will likewise possess reversible entanglement. However, one can already see in two qubits that this will not be true in general. Every two-qubit embedded ρ_{AB} with $K_D(p_{XYZ}) > 0$ will take the form $\rho_{AB} = \sum_z \sum_{j,j'=0}^{1} p(z)\sqrt{p(j|z)p(j'|z)}|jj\rangle\langle j'j'|$. This is a so-called maximally-correlated state for which entanglement reversibility is known to be lacking whenever ρ_{AB} is not pure [19, 20]. In fact, $E_F(\rho_{AB})$ is additive for the states of Theorem 2 [21]. Thus,

Corollary 1. *When $|\mathcal{X}| = |\mathcal{Y}| = 2$, any distribution with nonzero reversible secrecy will have nonzero reversible entanglement when embedded in a quantum state iff the embedded state is pure.*

Bipartite pure states are well-known to possess reversible entanglement under LOCC. Among the "zoo" of distributions introduced in this paper, we argue that SBI distributions are the closest classical analog to quantum pure states. An SBI distribution has the form

$$p(x,y,z) = \sum_j p(x|j)p(y|j)p(j)q(z), \tag{4}$$

where $p(x|j)p(x|j') = p(y|j)p(y|j') = 0$ if $j \neq j'$. The reason for this association is that a quantum embedding of any SBI distribution *à la* Eq. (3) recovers a pure state for Alice and Bob with Schmidt basis vectors $|\alpha_j\rangle = \sum_x \sqrt{p(x|j)}|x\rangle$ and $|\beta_j\rangle = \sum_y \sqrt{p(y|j)}|y\rangle$. Operational analogs between SBI distributions and bipartite pure states can also be demonstrated [1]. Beyond pure states, the only known quantum mixed states demonstrating entanglement reversibility are the so-called locally-flagged states [19, 20, 22, 23]. These are ensembles of pure states that can be perfectly discriminated using LOCC such that no entanglement is lost in the discrimination process. What is the classical analog of LOCC-flagged mixed states? Given the identification of an SBI distribution as a classical pure state, we identify LOPC-flagged classical states any distribution of the form

$$p(x,y,z) = \sum_{M=m} p(x,y|m)p(z|m)p(m) \tag{5}$$

where M is generated by a public communication protocol with $I(X:Y|J_{XY|M},M) = 0$ and $H(M|Z) = 0$. Analogous to LOCC-flagged states, an LOPC-flagged state is an ensemble of SBI distributions that can be perfectly distinguished using LOPC such that no secrecy from Eve is lost in the discrimination process. All LOPC-flagged distributions demonstrate secrecy reversibility, however there are many reversible distributions that are not LOPC-flagged.

CONCLUSIONS

We have presented a class of distributions UBI-PD↓ that are conjectured to fully characterize reversible secrecy. Despite the complexity of these distributions, validity of this conjecture would mean that reversibility of some distribution could be decided by a single-copy analysis. Turning back to the analogous problem of entanglement reversibility in quantum states, one might then likewise hope for a solution on the single-copy level. Only LOCC-flagged mixed states are known to possess entanglement reversibility, and these can indeed be identified by having a particular single-copy structure. We have proposed a classical analog to LOCC-flagged states that likewise possess reversible secrecy, but these do not constitute the full set of reversible states. Therefore, if only LOCC-flagged quantum states possess entanglement reversibility, then the analogous statement for secrecy in classical states would not be true. On the other hand, if entanglement and secrecy are truly on equal footing in terms of reversibility characters, then our findings might suggest the existence of reversible entanglement beyond LOCC-flagged states.

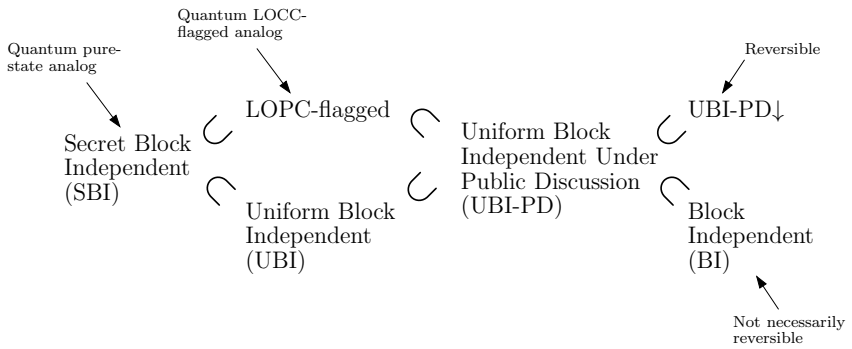

FIG. 1. A hierarchy of distribution classes and their relation to classes of reversible quantum states.

* echitamb@siu.edu
† bfortescue@siu.edu
‡ Min-Hsiu.Hsieh@uts.edu.au

[1] D. Collins and S. Popescu, Phys. Rev. A **65**, 032321 (2002).
[2] K. Horodecki, M. Horodecki, P. Horodecki, and J. Oppenheim, Foundations of Physics **35**, 2027 (2005).
[3] N. Gisin, R. Renner, and S. Wolf, Algorithmica **34**, 389 (2002).
[4] A. Acín, L. Masanes, and N. Gisin, Phys. Rev. Lett. **91**, 167901 (2003).
[5] A. Acín and N. Gisin, Phys. Rev. Lett. **94**, 020501 (2005).
[6] 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. Vadhan (Springer Berlin Heidelberg, 2007) pp. 456–478.
[7] J. Oppenheim, R. W. Spekkens, and A. Winter, "A classical analogue of negative information," (2008), accepted into Phys. Rev. Lett., arXiv:quant-ph/0511247v2.
[8] J. Bae, T. Cubitt, and A. Acín, Phys. Rev. A **79**, 032304 (2009).
[9] M. Ozols, G. Smith, and J. A. Smolin, Phys. Rev. Lett. **112**, 110502 (2014).
[10] E. M. Rains, Phys. Rev. A **60**, 173 (1999).
[11] P. M. Hayden, M. Horodecki, and B. M. Terhal, J. Phys. A: Math. Gen. **34**, 6891 (2001).
[12] R. Ahlswede and I. Csiszár, Information Theory, IEEE Transactions on **39**, 1121 (1993).
[13] U. Maurer, Information Theory, IEEE Transactions on **39**, 733 (1993).
[14] R. Renner and S. Wolf, in *Advances in Cryptology EUROCRYPT 2003*, Lecture Notes in Computer Science, Vol. 2656 (Springer Berlin Heidelberg, 2003) pp. 562–577.
[15] P. Gács and J. Körner, Problems of Control and Information Theory **2**, 149 (1973).
[16] C. Bennett, G. Brassard, C. Crepeau, and U. Maurer, Information Theory, IEEE Transactions on **41**, 1915 (1995).
[17] E. Chitambar, B. Fortescue, and M.-H. Hsieh, "A classical analog to entanglement reversibility," (2014), arXiv:1502.04433.
[18] W. K. Wootters, Phys. Rev. Lett. **80**, 2245 (1998).
[19] M. F. Cornelio, M. C. de Oliveira, and F. F. Fanchini, Phys. Rev. Lett. **107**, 020502 (2011).
[20] K. G. H. Vollbrecht, R. F. Werner, and M. M. Wolf, Phys. Rev. A **69**, 062304 (2004).
[21] G. Vidal, W. Dür, and J. I. Cirac, Phys. Rev. Lett. **89**, 027901 (2002).
[22] P. Horodecki, R. Horodecki, and M. Horodecki, Acta Physica Slovaca **48**, 141 (1998).
[23] R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki, Rev. Mod. Phys. **81**, 865 (2009).