Reversible Secrecy in Classical and Quantum States

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*

We consider the problem of when two parties can, using local operations and public communication (LOPC), *reversibly* distill secret key from a tripartite probability distribution p_{XYZ} shared between themselves and an eavesdropper. This is compared to the analogous quantum problem of entanglement distillation under local operations and classical communication (LOCC). We first prove a strong necessary condition on the type of distributions that exhibit secret key reversibility. We identify a non-trivial class of distributions that satisfy this condition, and further show that two-way public communication is generally required to attain reversible secrecy. An indispensable tool used in our analysis is a conditional form of the Gács and Körner common information.

Our results are then translated into the quantum setting where we embed reversible distributions into quantum states and compare the related quantum distillation rates of both key and entanglement. It is found that the gap between the quantum rates and the classical key rate can be arbitrarily large in both directions. A wide class of binary distributions are presented that demonstrate classical key reversibility but fail to demonstrate entanglement reversibility when embedded into a quantum state. For such distributions, the classical key rate for certain reversible distributions is related to the concurrence entanglement measure of the embedded quantum state. When Eve's variable is a function of Alice and Bob's, the quantum and key rates are shown to coincide.

Inspired by the conceptual successes of entanglement theory, researchers have recently begun applying a resource-theoretic perspective toward the classical problem of *secret key agreement by public discussion* [1, 2]. Whereas the states in quantum information are density operators, the physical states in classical information theory are probability distributions. Analogous to entanglement, *secrecy* held against an unwanted eavesdropper can be regarded as a resource in the classical setting [3, 4].

While entanglement and secrecy have many formal similarities [3–11], this work focuses on the similarities that lie in the tasks of resource distillation and resource cost. Just as pure quantum states demonstrate reversible entanglement dilution and concentration by LOCC, we are interested in understanding when secrecy becomes a reversible resource by LOPC. The problem of secrecy reversibility asks the following: given a distribution p_{XYZ}, decide if $K_D(p_{XYZ}) = K_C(p_{XYZ})$, where $K_D(p_{XYZ})$ is the **secret key rate** [1, 2] and $K_C(p_{XYZ})$ is the **secret key cost** [12, 13].

To address the question of secrecy reversibility, a main tool we use is the *common information* between two random variables, J_{XY}, as introduced by Gács and Körner [14]. We generalize this to a conditional common function $J_{XY|Z}$ and use it to formulate and prove many of our results (See Section 2.2 in the supplemental material). We introduce the following classes of distributions that will play a crucial role in the study of reversible secrecy.
Definition: A distribution p_{XYZ} is said to be (also see Fig. 1 in the supplemental material):

- **Block independent** (BI) if $I(X:Y|J_{XY|Z}Z) = 0$ for any maximal conditional common function $J_{XY|Z}$.
- **Uniform block independent** (UBI) if it is block independent and if there exists some maximal conditional common function $J_{XY|Z}$ such that $H(J_{XY|Z}|X) = H(J_{XY|Z}|Y) = 0$.
- **Uniform block independent under public discussion** (UBI-PD) if it is block independent and if there exists some maximal conditional common function $J_{XY|Z}$ such that $H(J_{XY|Z}|XJ_{YZ}) = H(J_{XY|Z}|YJ_{XZ}) = 0$.

Example distributions are shown and discussed in Figure 1 (also see Figure 1 in the supplemental material).

Secrecy Reversibility:

We now use these definitions to state our main results.

Theorem 1. *A distribution p_{XYZ} has $K_C(p_{XYZ}) = K_D(p_{XYZ})$ iff there exists a channel $\overline{Z}|Z$ such that $p_{XY\overline{Z}}$ is BI and $I(X:Y|\overline{Z})$ is an achievable key rate.*

What sort of distributions satisfy the conditions of Theorem1?

Lemma 1. *If p_{XYZ} is UBI-PD, then $K_C(p_{XYZ}) = K_D(p_{XYZ}) = H(J_Z|Z)$.*

In the supplemental material we identify a more general class of reversible distributions that we denote by UBI-PD$\downarrow$. Compared to UBI-PD, distributions from UBI-PD$\downarrow$ have a much more complicated structure.

(a) Block Independent (BI):

$p_{XY|Z=0}$

Y ↓ \ X →	0	1	2
0	1/8	1/8	·
1	1/8	1/8	·
2	·	·	1/2

$p_{XY|Z=1}$

Y ↓ \ X →	0	1	2
0	1/6	1/6	·
1	1/6	1/6	·
2	·	·	1/3

$p_{XY|Z=2}$

Y ↓ \ X →	0	1	2
0	1/2	·	·
1	·	1/8	1/8
2	·	1/8	1/8

(b) Uniform Block Independent under Public Discussion (UBI-PD):

$p_{XY|Z=0}$

Y ↓ \ X →	0	1	2
0	1/8	1/8	·
1	1/8	1/8	·
2	·	·	1/2

$p_{XY|Z=1}$

Y ↓ \ X →	0	1	2
0	1/6	1/6	·
1	1/6	1/6	·
2	·	·	1/3

$p_{XY|Z=2}$

Y ↓ \ X →	3	4	5
0	1/2	·	·
1	·	1/8	1/8
2	·	1/8	1/8

FIG. 1. (a) A BI but not UBI-PD distribution. Given Z, Alice and Bob's distribution decomposes into independent blocks. (b) A UBI-PD distribution. Note that, once Alice publicly announces whether $X \in \{0,1,2\}$ or $X \in \{3,4,5\}$ (which is information already known to Eve), Alice and Bob know what block their event (X,Y) belongs to for each value of Z.

Communication Dependency in Reversible Distillation:

To understand the role of communication in secrecy reversibility, we consider optimal secret key distillation rates by one-way communication. Here, we use Ahlswede and Csiszar's classic single-letter formula for the one-way rate $\overrightarrow{K}_D(p_{XYZ})$ [2] to obtain the following technical tool.

Proposition 1. *Distribution p_{XYZ} satisfies $\overrightarrow{K}_D(p_{XYZ}) = I(X:Y|Z)$ iff there exists variables $KUXYZ$ with K and U ranging over sets of size no greater than $|\mathcal{X}|+1$ such that*

$$\begin{aligned} &(1)\quad KU - X - YZ, && (2)\quad X - KUZ - Y, \\ &(3)\quad U - Z - Y, && (4)\quad K - YU - Z. \end{aligned} \tag{1}$$

Using this proposition, the following observations are shown: (i) attaining reversible key distillation by one-way communication depends on the direction of the communication, and (ii) two-way communication may be necessary in order to achieve reversible distillation. While these facts may not be overly surprising at first sight, we note that for the analogous problem of entanglement distillation from quantum states, all known examples of reversibility have protocols that attain reversibility with one-way communication, regardless of the communication direction [15–17].

Classical Embeddings in Quantum States

Let p_{XYZ} be a fixed triparite probability distribution, and let $\{|x\rangle\}_{x=0}^{d_A-1}$, $\{|y\rangle\}_{y=1}^{d_B-1}$, and $\{|z\rangle\}_{z=0}^{d_E-1}$ be a fixed orthonormal basis for Alice, Bob, and Eve's system, respectively. A **qqq embedding** of the distribution p_{XYZ} is the tripartite pure state

$$|\Psi_{ABE}\rangle = \sum_{xyz} \sqrt{p(xyz)}|xyz\rangle.$$

and $\rho_{AB} = tr_E \Psi_{ABE}$ is Alice and Bob's corresponding reduced state.

For the quantum states associated with p_{XYZ}, there are three primary rates of interest: (1) $K_D(\Psi_{ABE})$: the LOPC rate of key distillation from $|\Psi_{ABE}\rangle$ (see Ref. [8] for a formal definition); (2) $E_D(\rho_{AB})$: the LOCC rate of entanglement distillation from ρ_{AB} [18]; (3) $E_C(\rho_{AB})$: the LOCC rate of entanglement cost for the creation of ρ_{AB} [19]. We compare these quantities to the key cost rate $K_C(p_{XYZ})$ and key distillation rate $K_D(p_{XYZ})$ when the underlying distribution p_{XYZ} has reversible secrecy.

When distilling classical key, the adage "quantum is more powerful than classical" holds true, but the question is whether "quantum Eve" becomes more powerful than "quantum Alice and Bob" when embedding $p_{XYZ} \to |\Psi_{ABE}\rangle$. For example, from the state $|\Psi_{ABE}\rangle$, all 3 parties could recover the encoded distribution p_{XYZ} as a "classical state" $\sum_{xyz} p(xyz)|xyz\rangle\langle xyz|$ simply by dephasing, in which case Alice and Bob could distill $K_D(p_{XYZ})$ asymptotically. However, as the adversary, dephasing may not be Eve's optimal strategy, and so we cannot simply conclude that $K_D(\Psi_{ABE}) \geq K_D(p_{XYZ})$. A gap $K_D(p_{XYZ}) > K_D(\Psi_{ABE})$ means that Alice and Bob gain more from the quantum embedding than Eve, while a gap $K_D(\Psi_{ABE}) > K_D(p_{XYZ})$ indicates that Eve gains more. We find, by building off our classical analysis, that both scenarios can occur, and no general bounds exist between $K_D(p_{XYZ})$ and $K_D(\Psi_{ABE})$.

The bulk of our work investigates when gaps do and do not exist between the various rates under a qqq embedding. While partial results have been previously obtained on this topic [8, 11], here we provide a number of new findings based on our analysis of secrecy reversibility. Our results are partially summarized in Table I. To draw comparisons between the classical and quantum rates, we also make use of the following well-known upper bounds on the quantum rates: (a) the relative entropy of entanglement $E_r(\rho_{AB})$ [20]; (b) the squashed entanglement $E_{sq}(\rho_{AB})$; [21]; (c) the

Type of Distribution	Relationship between Classical key rate, Quantum key rate, and Entanglement
General	Arbitrary gaps; i.e. there exists no $N_1 \geq 0$ or $N_2 \geq 0$ such that $-N_1 \leq \Big(K_D(p_{XYZ}) - K_D(\Psi_{ABE}) \vee E_D(\rho_{AB}) \Big) \leq N_2 \quad \forall p_{XYZ}.$ [Supp. Mat. Proposition 7 and Corollary 3]
Secrecy Reversible	$K_D(p_{XYZ}) \geq E_{sq}(\rho_{AB}).$ [Supp. Mat. Theorem 3]
Secrecy Reversible + UBI-PD	$K_D(p_{XYZ}) \geq E_F(\rho_{AB}).$ Two qubits: $K_C(p_{XYZ}) = K_D(p_{XYZ})$ but $E_C(\rho_{AB}) > E_D(\rho_{AB})$ unless ρ_{AB} is pure or separable. [Supp. Mat. Theorem 3 and Lemma 5]
Secrecy Reversible + Semi-unambiguous	$K_C(p_{XYZ}) = E_{sq}(\rho_{AB}) = K_D(\Psi_{ABE}) = K_D(p_{XYZ}).$ [Supp. Mat. Corollary 4]
Secrecy Reversible + UBI-PD + Semi-Unambiguous	$K_C(p_{XYZ}) = E_F(\rho_{AB}) = E_{sq}(\rho_{AB}) = E_r(\rho_{AB}) = K_D(\Psi_{ABE}) = K_D(p_{XYZ}).$ [Supp. Mat. Corollary 4]

TABLE I. A comparison of distillation rates and entanglement measures for various types of distributions p_{XYZ} and their embedding into quantum states $|\Psi_{ABE}\rangle$ and ρ_{AB}. Semi-unambiguous distributions were studied in Ref. [8] and can be given the entropic characterization of $H(Z|XY) = 0$. All relationships are proven in the supplemental material.

entanglement of formation $E_F(\rho_{AB})$ [22]. Recall that $K_D(\Psi_{ABE})$ and $E_D(\rho_{AB})$ are both upper bounded by the relative entropy of entangled $E_r(\rho_{AB})$, as well as the squashed entanglement $E_{sq}(\rho_{AB})$ [23–25].

For binary UBI-PD distributions, we are able to exactly compute the gap between $K_D(p_{XYZ})$ and $E_F(\rho_{AB})$.

Lemma 2. *If p_{XYZ} is a uniformly block independent distribution with $|\mathcal{X}| = |\mathcal{Y}| = 2$, then*

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

where $\mathsf{E}(x) := h(\frac{1}{2}[1-\sqrt{1-x^2}])$ and $h(x) := -x\log x - (1-x)\log(1-x)$. Note that $\mathsf{E}(x)$ is a convex function, so this theorem shows $K_D(p_{XYZ}) \geq E_F(\rho_{XY})$ for UBI distributions in two qubits. Also, observe that $E_F(\rho_{AB}) = 0$ iff $K_C(p_{XYZ}) = K_D(p_{XYZ}) = 0$.

Discussion and Conclusion

In this work we have studied the problem of secrecy reversibility and related it to the entanglement structure of embedded qqq states. From the work of Renner and Wolf [12], it was previously known that having reversible secrecy requires a key rate equal to the intrinsic information. Our work adds the strong structural constraint that Eve's optimal channel must leave the distribution block independent. Our findings also nicely complement the work of Horodecki *et al.* who showed that key cost of p_{XYZ} will equal the intrinsic information whenever p_{XYZ} can be built from a mixture of private distributions, each with a key cost given by the mutual information. Our Theorem 1 shows that block independent distributions are precisely this class of distributions requiring $\sum_z p(z)I(X:Y|Z=z)$ secret bits to generate.

We were able to identify a class of non-trivial distributions that demonstrate secrecy reversibility, which we have called UBI-PD$\downarrow$. We further offered an example showing that attaining reversible secrecy can require two-way communication. This is perhaps an unexpected finding considering that all known reversible entanglement distillation protocols are one-way.

We have examined the properties of quantum states obtained through a qqq embedding of reversible distributions. It was shown that no general relationship exists between the classical key rate, the quantum key rate, and the entanglement distillation rate. In fact, we have succeeded in showing arbitrarily large gaps between the quantum and classical rates. Using the structure of two-qubit entangled states, we were able to prove that unless the state is pure or separable, all two-qubit UBI embeddings lack entanglement reversibility, despite the fact that they are generated by reversible classical distributions.

Just as entanglement can be understood as a physical resource useful for performing certain tasks, classical secrecy can be given a similar resource-theoretic interpretation. We hope this paper helps advance the understanding of secrecy as a fungible resource and its relationship to entanglement.

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

[1] U. Maurer, Information Theory, IEEE Transactions on **39**, 733 (1993).
[2] R. Ahlswede and I. Csiszár, Information Theory, IEEE Transactions on **39**, 1121 (1993).
[3] D. Collins and S. Popescu, Phys. Rev. A **65**, 032321 (2002).
[4] K. Horodecki, M. Horodecki, P. Horodecki, and J. Oppenheim, Foundations of Physics **35**, 2027 (2005).
[5] N. Gisin, R. Renner, and S. Wolf, Algorithmica **34**, 389 (2002).
[6] A. Acín, L. Masanes, and N. Gisin, Phys. Rev. Lett. **91**, 167901 (2003).
[7] A. Acín and N. Gisin, Phys. Rev. Lett. **94**, 020501 (2005).
[8] 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.
[9] J. Oppenheim, R. W. Spekkens, and A. Winter, "A classical analogue of negative information," (2008), accepted into Phys. Rev. Lett., arXiv:quant-ph/0511247v2.
[10] J. Bae, T. Cubitt, and A. Acín, Phys. Rev. A **79**, 032304 (2009).
[11] M. Ozols, G. Smith, and J. A. Smolin, Phys. Rev. Lett. **112**, 110502 (2014).
[12] 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.
[13] A. Winter, in *Information Theory, 2005. ISIT 2005. Proceedings. International Symposium on* (2005) pp. 2270–2274.
[14] P. Gács and J. Körner, Problems of Control and Information Theory **2**, 149 (1973).
[15] C. H. Bennett, H. Bernstein, S. Popescu, and B. Schumacher, Phys. Rev. A **53**, 2046 (1996), quant-ph/9511030.
[16] P. Horodecki, R. Horodecki, and M. Horodecki, Acta Physica Slovaca **48**, 141 (1998).
[17] K. G. H. Vollbrecht, R. F. Werner, and M. M. Wolf, Phys. Rev. A **69**, 062304 (2004).
[18] E. M. Rains, Phys. Rev. A **60**, 173 (1999).
[19] P. M. Hayden, M. Horodecki, and B. M. Terhal, J. Phys. A: Math. Gen. **34**, 6891 (2001).
[20] V. Vedral and M. B. Plenio, Phys. Rev. A **57**, 1619 (1998).
[21] M. Christandl and A. Winter, Journal of Mathematical Physics **45**, 829 (2004).
[22] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, Phys. Rev. A **54**, 3824 (1996).
[23] K. Horodecki, M. Horodecki, P. Horodecki, and J. Oppenheim, Phys. Rev. Lett. **94**, 160502 (2005).
[24] K. Horodecki, M. Horodecki, P. Horodecki, and J. Oppenheim, Information Theory, IEEE Transactions on **55**, 1898 (2009).
[25] M. Christandl, "The structure of bipartite quantum states: Insights from group theory and cryptography," (2006), phD Thesis.