

# Entanglement and Secret-Key Distillation from a Complementary Information Tradeoff

Joseph M. Renes (1) and Jean-Christian Boileau (2)

1: Institut für Angewandte Physik, Technische Universität Darmstadt, Hochschulstraße 4a,  
D-64289 Darmstadt, Germany. joe.renes@physik.tu-darmstadt.de

2: Center for Quantum Information and Quantum Control, University of Toronto, Canada

## Abstract

One of the quintessential features of quantum information is its exclusivity, the inability of strong quantum correlations to be shared by many physical systems. Likewise, complementarity has a similar status in quantum mechanics as the sine qua non of quantum phenomena. We show that this is no coincidence, and that the central role of exclusivity in quantum information theory stems from the phenomenon of complementarity. We adopt an information-theoretic approach to complementarity, which leads to a new and simple definition of private states and new proofs of the achievable asymptotic rates of both secret key and entanglement distillation.

## Complementary Information Tradeoff

We start by formulating a tradeoff on the amount of information which can be simultaneously known about two complementary observables. Consider a physical system  $A$  with  $\dim(A) = d^A < \infty$  and the generalized Pauli operators  $X^A$  and  $Z^A$ . Any auxiliary systems  $B$  and  $E$  can only be correlated with the observables on  $A$  to the extent that the tripartite quantum state fulfills the relation

$$S(X^A|B) + S(Z^A|E) \geq \log_2 d^A. \quad (1)$$

Here  $S$  is the von Neumann entropy and  $S(X^A|B)$  denotes the conditional entropy of the outcomes of the  $X^A$  measurement given system  $B$ . This tradeoff relation is similar to one developed for channels [1] and inherits its proof based on strong subadditivity [2]. We conjecture that it also holds for arbitrary observables after replacing the bound by  $c = -\log_2 \max_{x,z} |\langle \lambda_x | \xi_z \rangle|^2$ , where  $|\lambda_x\rangle$  and  $|\xi_z\rangle$  the eigenvectors of the two observables, thereby generalizing the entropic uncertainty relation [3].

The cryptographic implications of this tradeoff are immediate. Suppose systems  $A$  and  $B$  belong to Alice and Bob, who wish to create a secret key by each measuring the  $Z$  observable on their respective systems. If  $S(Z^A|Z^B) = 0$ , then the key is perfectly correlated. If  $S(X^A|B) = 0$ , then  $S(Z^A|E) = \log_2 d$ , meaning the key is also secret from the eavesdropper Eve. Moreover, it is easy to see that  $\psi^{AB}$  is maximally-entangled when  $\epsilon = 0$ .

## Secret Key & Entanglement Distillation

Maximal entanglement is not required to create a secret key, however; more generally any *private state* will do [4]. Private states contain additional “shield” systems  $S$  which do not pertain directly to the key but are not con-

trolled by the eavesdropper Eve. Including the shield in the second condition above yields our new characterization:  $\gamma^{ABS}$  is a private state iff (i)  $S(Z^A|Z^B) = 0$  and (ii)  $S(X^A|BS) = 0$ , a formulation which emphasizes that the key is secret as long as full information about the conjugate observable is stored *somewhere* the systems held by Alice and Bob.

This fact leads us directly to a means of private state distillation, or indeed entanglement distillation when there is no shield, one similar to a scheme employed by Koashi [5]. Given an arbitrary resource state  $\psi^{ABS}$ , Bob and Bob+Shield already have some information about  $Z^A$  and  $X^A$ , respectively, and Alice only needs to supply the rest [6]. In this way, the task of distillation reduces to extracting classical information from the corresponding conditional quantum states, with the help of classical side information from Alice. Using CSS codes ensures that the side information of both observables can be simultaneously realized, and the result is a one-shot private state distillation protocol potentially useful for analyzing the security of quantum key distribution protocols.

In the asymptotic case of many copies of  $\psi^{ABS}$  we apply a slightly-modified HSW theorem and find that when distilling either private states or entanglement, the achievable rate  $R \geq S(Z^A|E) - S(Z^A|B)$ . This agrees with the results of [7], but uses linear CSS codes instead of random codes, and the proof focuses on the systems held by Alice and Bob, rather than directly decoupling Eve via privacy amplification.

$R$  is also the coherent information of an entangled state transmitted through a noisy channel, and the bound implies the direct part of the quantum noisy channel coding theorem for CSS codes. Additionally, the HSW theorem gives an explicit construction of the decoder, solving an open question posed in [8].

## References

- [1] M. Christandl and A. Winter, IEEE Trans. Inf. Theory **31**, 5139 (2005).
- [2] JMR and JCB, arXiv:0806.3984 [quant-ph].
- [3] H. Maassen and J. B. M. Uffink, Phys. Rev. Lett. **60**, 1103 (1988).
- [4] {K., M., P.} Horodecki and J. Oppenheim, Phys. Rev. Lett. **94**, 160502 (2005).
- [5] M. Koashi, J. Phys.: Conf. Ser. **36**, 98 (2006) and arXiv:0704.3661 [quant-ph].
- [6] JMR and JCB, arXiv:0803.3096 [quant-ph].
- [7] I. Devetak and A. Winter, Proc. R. Soc. A **461**, 207 (2005).
- [8] P. Hayden, P. W. Shor, and A. Winter, Open Syst. Inf. Dyn. **15**, 71 (2008).