

# Complementarity and Privacy:

## From Private State Distillation to Quantum Channel Coding

Joseph M. Renes  and Jean-Christian Boileau 



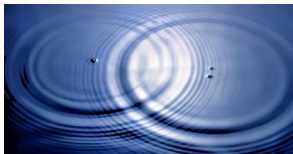
Theoretical Quantum Physics, Institut für Angewandte Physik  
Technische Universität Darmstadt



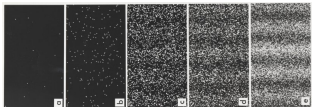
Center for Quantum Information and Quantum Control  
University of Toronto

CEQIP 5    Telč, Czech Republic    2008 June 5

## Complementarity: Essence of Quantum Mechanics



or



The double slit experiment "is impossible, absolutely impossible, to explain in any classical way, and has in it the heart of quantum mechanics. In reality, it contains the only mystery." -Feynman

## Privacy: Ubiquitous in Quantum Information Theory

- ☞ Quantum cryptography
- ☞ Entanglement! (monogamy)
- ☞ Informs nearly every aspect of QIT



Importance of both privacy and complementarity is no coincidence!

To convince you, this talk will. . .

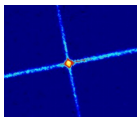
- 1 Recall an information-theoretic description of complementarity
- 2 Use this to describe private and entangled states in terms of complementary info
- 3 Construct distillation procedures for private states and entanglement

# Entropic Uncertainty Relation

Maassen & Uffink  
PRL 60 1103 (1988)

$$H(O^A) + H(\tilde{O}^A) \geq -\log \max_{jk} |\langle j|\tilde{k}\rangle|^2$$

$O^A, \tilde{O}^A$  operators on system  $A$ ; eigenvectors  $|j\rangle$  and  $|\tilde{k}\rangle$ ;  $H(\cdot)$  entropy.



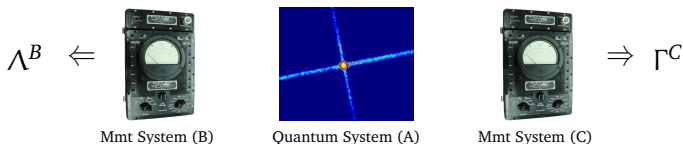
Quantum System (A)

- Consider generalized Paulis  $X$  and  $Z$ : State  $|\Psi\rangle$  satisfies  $H(X) + H(Z) \geq \log_2 d$
- But how much info can we *simultaneously* extract?

## Entropic Uncertainty Relation Maassen & Uffink PRL 60 1103 (1988)

$$H(O^A) + H(\tilde{O}^A) \geq -\log \max_{jk} |\langle j|\tilde{k}\rangle|^2$$

$O^A, \tilde{O}^A$  operators on system  $A$ ; eigenvectors  $|j\rangle$  and  $|\tilde{k}\rangle$ ;  $H(\cdot)$  entropy.



- Consider generalized Paulis  $X$  and  $Z$ : State  $|\Psi\rangle$  satisfies  $H(X) + H(Z) \geq \log_2 d$
- But how much info can we *simultaneously* extract? Include mmt systems!

## Information Exclusion Principle Hall PRL 74 3307 (1995)

$$H(O^A|\Lambda^B) + H(\tilde{O}^A|\Gamma^C) \geq -\log \max_{jk} |\langle j|\tilde{k}\rangle|^2$$

$\Lambda^B, \Gamma^C$  measurements on  $B, C$ ;  $H(\cdot|\cdot)$  conditional entropy

➡ tradeoff in simultaneously available, complementary classical information

## Complementarity leads directly to private/entangled states

### Entanglement

- ☞  $\psi^{AB}$  is maximally-entangled when  $H(Z^A|Z^B) = H(X^A|X^B) = 0$
- ☛ Simultaneous eigenstate of  $X^A X^B$  and  $Z^A Z^B$ .

### Private States

Horodecki<sup>3</sup>, Oppenheim  
PRL 94 160502 (2005)



Alice: Key+Shield



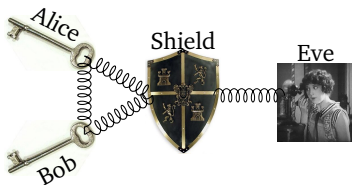
Eve



Bob: Key+Shield

- ☞ Key systems  $A$  &  $B$ , non-local *shield* system  $S$ , eavesdropper  $E$ .
- ☞  $Z^A$  generates the key, which is random:  $H(Z^A) = \log_2 d$ .
- ☞  $\exists \Lambda^B$  such that  $H(Z^A|\Lambda^B) = 0$
- ☞  $\exists \tilde{\Lambda}^{BS}$  such that  $H(X^A|\tilde{\Lambda}^{BS}) = 0$
- ☛ Key is correlated & random
- ☛  $H(Z^A|\Gamma^E) = \log_2 d$ , key is private

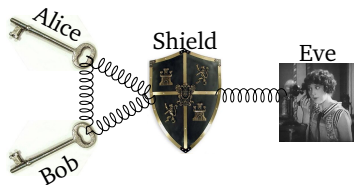
## Shield deflects key correlations from Eve



- Needn't concern ourselves with Eve's system; all statements pertain to the systems held by Alice and Bob.

Complementarity is directly responsible for quantum privacy!

## Shield deflects key correlations from Eve



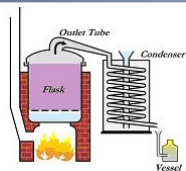
Needn't concern ourselves with Eve's system; all statements pertain to the systems held by Alice and Bob.

Complementarity is directly responsible for quantum privacy!

## Also works approximately, in the following sense:

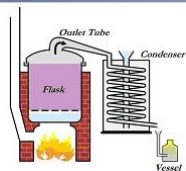
- If  $\exists \Lambda^B, \tilde{\Lambda}^B$  such that  $p_e^z \leq \epsilon_z, p_e^x \leq \epsilon_x$ , then  
 $\|\psi^{AB} - \Phi^{AB}\|_1 \leq 2(\sqrt{\epsilon_x} + \sqrt{\epsilon_z})$
- If  $\exists \Lambda^B, \tilde{\Lambda}^{BS}$  such that  $p_e^z \leq \epsilon_z, p_e^x \leq \epsilon_x$ , then  
 $\psi^{ABS}$  is an  $(\epsilon_z + \sqrt{\epsilon_x})$ -private state  
(actual key  $(\epsilon_z + \sqrt{\epsilon_x})$ -close to perfect key)

## Private State/Entanglement Distillation. . .



Given many copies of an arbitrary resource state,  $\Psi^{AB(S)} = (\psi^{AB(S)})^{\otimes n}$ , convert into (approximate) private/entangled states using local operations and (one-way) classical communication (with high probability).

## Private State/Entanglement Distillation. . .



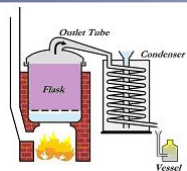
Given many copies of an arbitrary resource state,  $\Psi^{AB(S)} = (\psi^{AB(S)})^{\otimes n}$ , convert into (approximate) private/entangled states using local operations and (one-way) classical communication (with high probability).

. . . by transmitting “missing” information

X   $H(X)$

Z   $H(Z)$

## Private State/Entanglement Distillation. . .



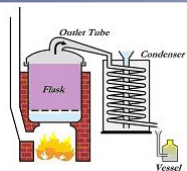
Given many copies of an arbitrary resource state,  $\Psi^{AB(S)} = (\psi^{AB(S)})^{\otimes n}$ , convert into (approximate) private/entangled states using local operations and (one-way) classical communication (with high probability).

. . . by transmitting “missing” information

$$X \quad \begin{array}{|c|c|} \hline I(X:\tilde{\Lambda}) & H(X|\tilde{\Lambda}) \\ \hline \end{array}$$

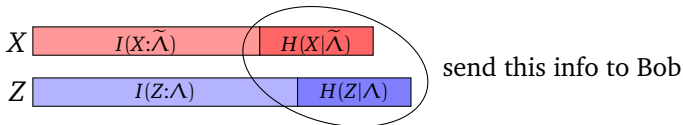
$$Z \quad \begin{array}{|c|c|} \hline I(Z:\Lambda) & H(Z|\Lambda) \\ \hline \end{array}$$

## Private State/Entanglement Distillation...

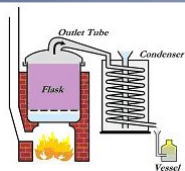


Given many copies of an arbitrary resource state,  $\Psi^{AB(S)} = (\psi^{AB(S)})^{\otimes n}$ , convert into (approximate) private/entangled states using local operations and (one-way) classical communication (with high probability).

... by transmitting “missing” information

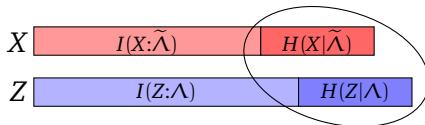


## Private State/Entanglement Distillation...



Given many copies of an arbitrary resource state,  $\Psi^{AB(S)} = (\psi^{AB(S)})^{\otimes n}$ , convert into (approximate) private/entangled states using local operations and (one-way) classical communication (with high probability).

... by transmitting “missing” information



send this info to Bob

Idea is same as (static) HSW theorem:

- ☞ Bob has measurement  $\Lambda^B$ , wants to learn  $Z^A$ , but  $\Psi_z^B$ 's not distinguishable
- ☞ Alice sends random function of  $Z^A$  (hash function) of appropriate size
- ➡ narrows possible  $z$ 's enough for  $\Lambda^B$  to distinguish corresponding  $\Psi_z^B$ 's

Details: [arXiv.0803.3096](https://arxiv.org/abs/0803.3096) [quant-ph]

## MEASUREMENTS

- HSW theorem generates  $\Lambda^B, \tilde{\Lambda}^{BS}$  from  $\Psi_z^B, \Psi_x^{BS}$  (pretty good measurement).
- Hash function size:  $nH(Z^A|B), nH(X^A|BS)$  (*quantum* conditional information).

## HASH FUNCTIONS

- Need to compute  $X$  and  $Z$  hash functions  $\Rightarrow$  use CSS code!
- Hash functions are linear
- Enables reduction from private state distillation to secret key distillation:  
 $X$  hash function becomes privacy amplification

## RATES

- Private States:  $P_{\rightarrow}(\psi^{ABS}) \geq 1 - H(Z^A|B) - H(X^A|Z^ABS)$  (two-step process)
- $P_{\rightarrow}(\psi^{ABS}) = K_{\rightarrow}(\psi^{ABS}) \geq I(Z^A:B) - I(Z^A:E)$ ,  
the “quantum” Csiszar-Körner bound on secret key distillation
- Entanglement:  $E_{\rightarrow}(\psi^{AB}) \geq I_c(A)B = S(B) - S(AB)$ , the hashing bound.

## Quantum Channel Capacity

Hashing inequality  $E_{\rightarrow}(\psi^{AB}) \geq I_c(A)B$  implies the lower bound on the quantum channel capacity,  $I_c(\rho, \mathcal{N})$ .

- Combine entanglement distillation with teleportation
- Directly generate code subspace using the CSS hash functions

## Differences from other approaches

- ☞ Usual approach is to purify the Alice-Bob system in order to get at Eve's system
- ☞ Next, *decouple* Eve's system somehow, perhaps using privacy amplification.
- ☞ Then appeal to Uhlmann's theorem to construct the desired decoder: If Alice-Eve system is in a product state, the purification gives the decoding unitary transforming the state into an entangled/private state.

Here we do not consider try to decouple Eve's system; instead focus on complementary information held by Alice and Bob. Decoder is directly constructed by the HSW theorem, not indirectly from the purifying unitaries.

Fundamental results of quantum information theory rest on the phenomenon of complementarity

### Outlook & Open Questions:

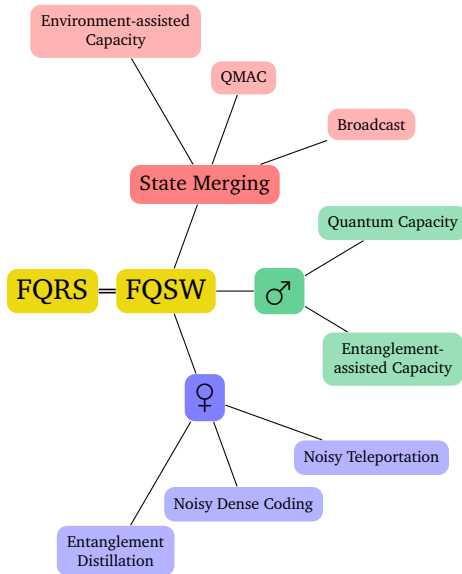
- Private states useful in practical QKD security proofs
- “Quantize” the information exclusion principle to get a stronger bound
- Can we make the protocol coherent and get the FQSW protocol (the mother of all protocols)?



## Complementary Information Tradeoff (conjectured)

$$S(O^A|B) + S(\tilde{O}^A|C) \geq -\log \max_{jk} |\langle j|\tilde{k}\rangle|^2$$

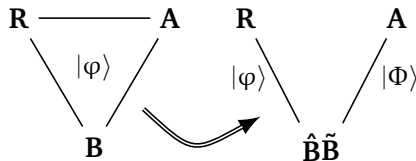
- “quantized” information exclusion principle
  - replace classical mutual info with quantum mutual info (Holevo quantity)
- stronger than classical version (locking); implies uncertainty relation
- tightest tradeoff for conjugate observables:  $-\log \max_{jk} |\langle j|\tilde{k}\rangle|^2 = \log \dim(A)$
- related to: quantum channel uncertainty relation Christandl & Winter  
IEEE TIT 51 3159 (2005).
  - “dynamic” version of “static” CIT
  - holds for conjugate observables
  - proof from strong subadditivity; can apply proof to CIT
- numerical evidence for non-conjugate observables ( $d \approx 20$ )
- can saturate the bound for conjugate observables with nonextremal states



## Fully-Quantum Slepian-Wolf

Given: state  $|\varphi\rangle^{ABR}$  and noiseless quantum communication

Goal: distill EPR pairs and transfer  $\varphi^A$  completely to Bob



$$\langle W^{S \rightarrow AB} : \varphi^S \rangle + \frac{1}{2} I(A:R)[q \rightarrow q] \geq$$

$$\frac{1}{2} I(A:B)[qq] + \langle \text{id}^{S \rightarrow \hat{B}} : \varphi^S \rangle.$$

A. Abeyesinghe, I. Devetak, P. Hayden, and A. Winter, quant-ph/0606225