Title: Entanglement and Secret-Key Distillation from a Complementary Information Tradeoff

Date: Aug 13, 2008 04:00 PM

URL: http://pirsa.org/08080002

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. From the latter follows a new proof of the direct part of the quantum noisy channel coding theorem.

Quantum Info as Complementary Classical Info:
Secret Key and Entanglement Distillation via Processing Complementary Information

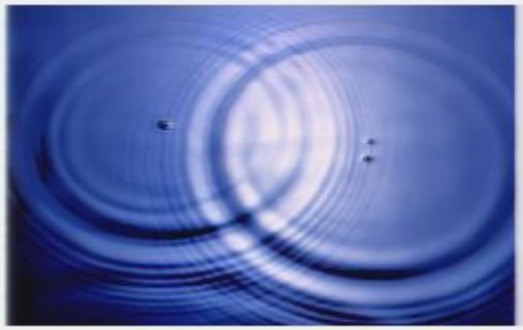
Joseph M. Renes and Jean-Christian Boileau

Theoretical Quantum Physics, Institut für Angewandte Physik
Technische Universität Darmstadt

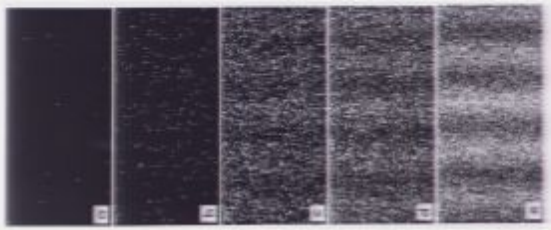
Center for Quantum Information and Quantum Control
University of Toronto

Perimeter Institute Quantum Discussion 2008 August 13

Complementarity is the essence of quantum mechanics...

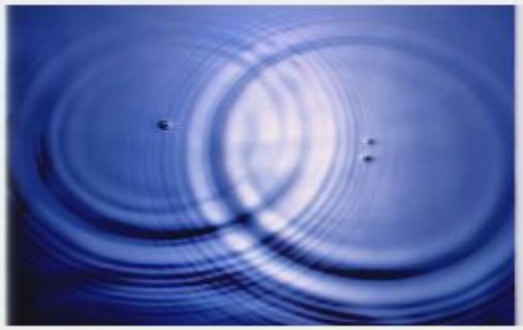


or

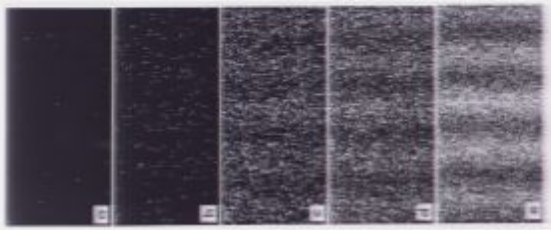


The double slit experiment "is impossible, absolutely impossible, to explain in any classical way, and has in it the heart of quantum mechanics. In reality, it contains the only mystery." -Feynman

Complementarity is the 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

But does it really *explain* anything?

YES! We can directly and concretely understand several tasks in quantum information theory in terms of complementarity.

Outline

1. Define what we mean by complementarity. Use an information-theoretic approach. (Surprise!)

2. Consider two common tasks in qinfo:
   Distillation of secret keys or entangled pairs.
   Recall known results and examine the logic behind them.

3. Construct protocols by using the complementarity approach.

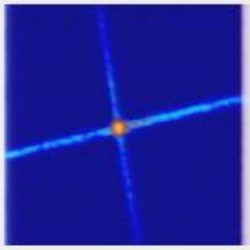
Information-Theoretic Complementarity

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.



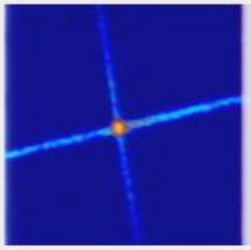
Quantum System (A)

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)

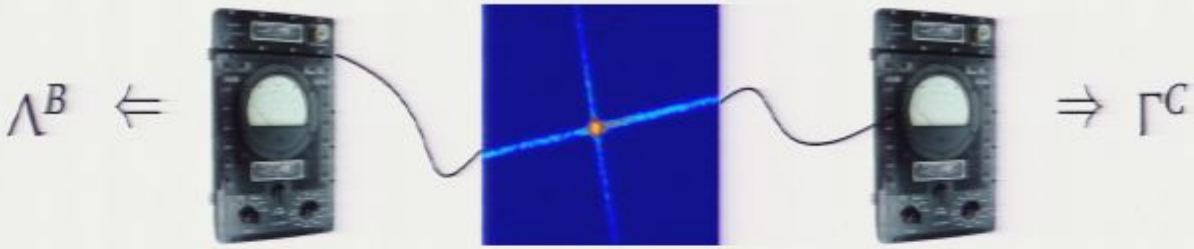
- For generalized Paulis X and Z, any state $|\Psi\rangle$ satisfies $H(X) + H(Z) \geq \log d$
- But how much info can we *simultaneously* extract?

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.



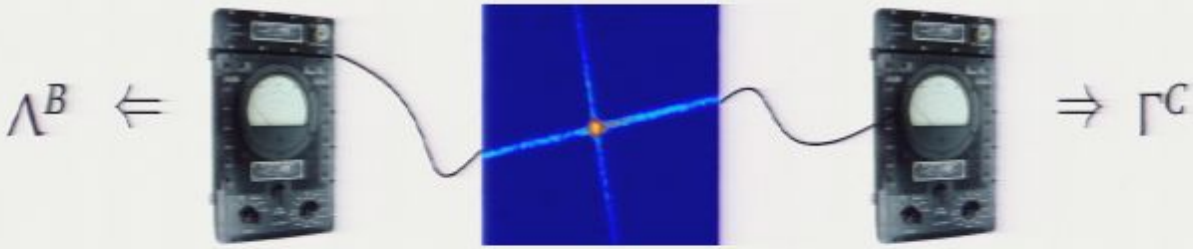
- For generalized Paulis X and Z, any state $|\Psi\rangle$ satisfies $H(X) + H(Z) \geq \log d$
- But how much info can we *simultaneously* extract? Include mmt systems!

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.



- For generalized Paulis X and Z, any state $|\Psi\rangle$ satisfies $H(X) + H(Z) \geq \log d$
- But how much info can we *simultaneously* extract? Include mmt systems!

Information Exclusion Principle

Hall
PRL 74 3307 (1995)

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

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

- tradeoff in simultaneously available, complementary classical information

Complementary Information Tradeoff

JMR & JCB
arxiv:0806.3984 [quant-ph]

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

- Replace classical mutual information with Holevo upper bound.
  $H(O^A|B)$ is quantum conditional entropy after Alice measures O^A
- Numerical support for conjecture up to dimension 12.
- Holds for generalized Paulis X^A and Z^A.
  proof from strong subadditivity — Christandl & Winter, IEEE TIT **51** 3159 (2005)

Complementary Information Tradeoff

JMR & JCB
arxiv:0806.3984 [quant-ph]

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

- Replace classical mutual information with Holevo upper bound.
  $H(O^A|B)$ is quantum conditional entropy after Alice measures O^A
- Numerical support for conjecture up to dimension 12.
- Holds for generalized Paulis X^A and Z^A.
  proof from strong subadditivity — Christandl & Winter, IEEE TIT **51** 3159 (2005)

Two standard QIP protocols:
Distillation of Secret Keys or Entangled Pairs

(And state merging, too.)

Complementary Information Tradeoff

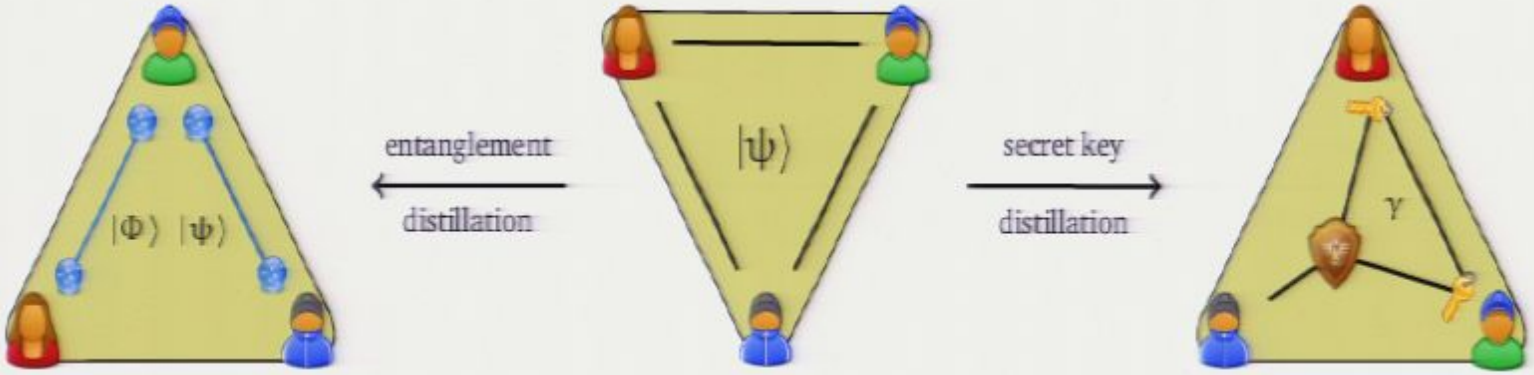
JMR & JCB
arxiv:0806.3984 [quant-ph]

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

- Replace classical mutual information with Holevo upper bound.
  $H(O^A|B)$ is quantum conditional entropy after Alice measures O^A
- Numerical support for conjecture up to dimension 12.
- Holds for generalized Paulis X^A and Z^A.
  proof from strong subadditivity — Christandl & Winter, IEEE TIT **51** 3159 (2005)

Two standard QIP protocols:
Distillation of Secret Keys or Entangled Pairs

(And state merging, too.)



- Initially Alice, Bob, and Eve share (many copies of) a pure state $|\psi\rangle$.
- In *entanglement distillation* Alice and Bob create entangled states $|\Phi\rangle$ using only one-way classical communication.
- Related is the *state merging* protocol in which Alice transfers her part of the purification of Eve's system to Bob. Both can be performed simultaneously.
- In *key distillation* Alice and Bob use one-way classical communication to create a shared private random classical string. In QM this is described by a *private state* γ, comprising the two (identical) key strings and a *shield* which deflects Eve's correlations from it.

- Key distillation rate Devetak & Winter ProcRoySocA **461** 207 (2005)

$$K_{\rightarrow}(\psi) \geq I(Z^A : B) - I(Z^A : E) = H(Z^A|E) - H(Z^A|B)$$

- Entanglement distillation rate

$$E_{\rightarrow}(\psi) \geq H(B) - H(AB) = -H(A|B).$$

- Communication cost $I(A:E)$ in either case.

- State merging at the same rates/costs Horodecki, Oppenheim, Winter Nature **436** 7051 (2005)
- Channel coding from entanglement distillation via teleportation

Decouple

Alice & Eve

- Sensible approach for key generation...
- Use Uhlmann's Theorem for entanglement generation: Schumacher & Westmoreland QIP 1 5 (2002).

$$\psi^A \simeq 1^A/d^A \quad \text{and} \quad \psi^{AE} \simeq \psi^A \otimes \psi^E$$

$$\Downarrow \quad \exists\, U^B \quad \text{s.t.}$$

$$U^B |\psi\rangle^{ABE} \simeq \sum_{jk} \sqrt{q_k/d^A}\, |j\rangle^A |j,k\rangle^B |k\rangle^E$$

  - d^A is the dimension of A
  - eigenvalues/vectors of ψ^A (ψ^E) are $1/d^A$, $|j\rangle^A$ (q_k,$|k\rangle^E$),
  - $|j,k\rangle^B$ are orthonormal.
- By coherently measuring B, ψ^{AB} can be (nearly) transformed into Φ^{AB}.

  But we only know U^B must exist.

Complementarity-based Approach

Decouple

Alice & Eve

- Sensible approach for key generation...
- Use Uhlmann's Theorem for entanglement generation: Schumacher & Westmoreland QIP 1 5 (2002).

$$\psi^A \simeq 1^A/d^A \quad \text{and} \quad \psi^{AE} \simeq \psi^A \otimes \psi^E$$

$$\Downarrow \quad \exists\, U^B \quad \text{s.t.}$$

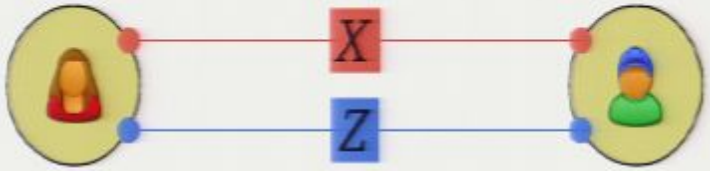
$$U^B |\psi\rangle^{ABE} \simeq \sum_{jk} \sqrt{q_k/d^A}\, |j\rangle^A |j,k\rangle^B |k\rangle^E$$

  - d^A is the dimension of A
  - eigenvalues/vectors of ψ^A (ψ^E) are $1/d^A$, $|j\rangle^A$ (q_k,$|k\rangle^E$),
  - $|j,k\rangle^B$ are orthonormal.
- By coherently measuring B, ψ^{AB} can be (nearly) transformed into Φ^{AB}.

  But we only know U^B must exist.

Complementarity-based Approach

Couple Alice and Bob classically, twice.



- Quantum correlations between Alice and Bob are equivalent to two complementary classical correlations, say X and Z correlations.
- Quantum error correction strategy. But can we achieve the known rates? Answer: YES!
- Gives an explicit construction of the decoder

Complementarity of private/entangled states

Entangled Pairs

- $H(Z^A|B) = H(X^A|B) = 0 \quad \Rightarrow \quad \psi^{AE} = \psi^A \otimes \psi^E$;
  now follow decoupling argument from before.
- ψ^{AB} has maximal entanglement when $H(Z^A|B) = H(X^A|B) = 0$

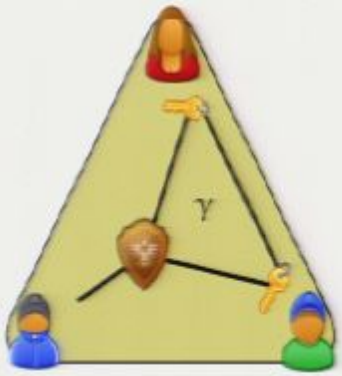
Complementarity of private/entangled states

Entangled Pairs

- $H(Z^A|B) = H(X^A|B) = 0 \quad \Rightarrow \quad \psi^{AE} = \psi^A \otimes \psi^E$;
  now follow decoupling argument from before.
- ψ^{AB} has maximal entanglement when $H(Z^A|B) = H(X^A|B) = 0$

Private States

Horodecki[3], Oppenheim
PRL 94 160502 (2005)



Z^A generates the key.

- $\exists\, \Lambda^B$ such that $H(Z^A|\Lambda^B) = 0$
- Key is correlated
- $\exists\, \tilde{\Lambda}^{BS}$ such that $H(X^A|\tilde{\Lambda}^{BS}) = 0$
- $H(Z^A|\Gamma^E) = \log d$, key is private and random

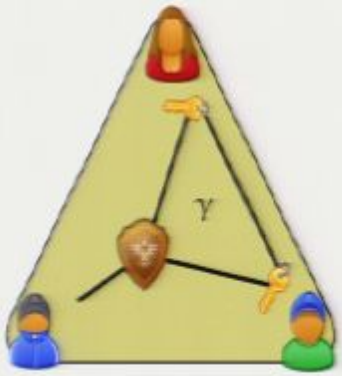
Complementarity of private/entangled states

Entangled Pairs

- $H(Z^A|B) = H(X^A|B) = 0 \quad \Rightarrow \quad \psi^{AE} = \psi^A \otimes \psi^E$;
  now follow decoupling argument from before.
- ψ^{AB} has maximal entanglement when $H(Z^A|B) = H(X^A|B) = 0$

Private States

Horodecki[3], Oppenheim
PRL 94 160502 (2005)

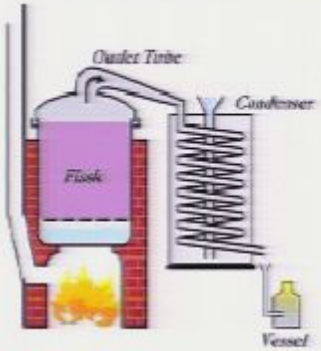


Z^A generates the key.

- $\exists\, \Lambda^B$ such that $H(Z^A|\Lambda^B) = 0$
- Key is correlated
- $\exists\, \tilde{\Lambda}^{BS}$ such that $H(X^A|\tilde{\Lambda}^{BS}) = 0$
- $H(Z^A|\Gamma^E) = \log d$, key is private and random

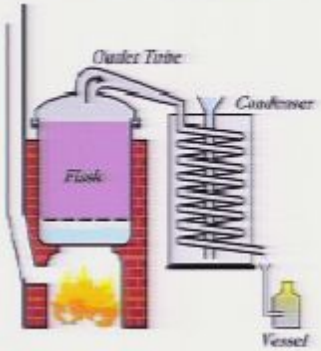
- Also works approximately

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).

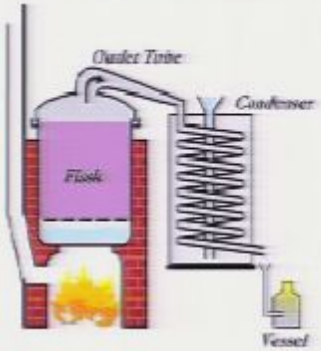
Private State/Entanglement Distillation...



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).

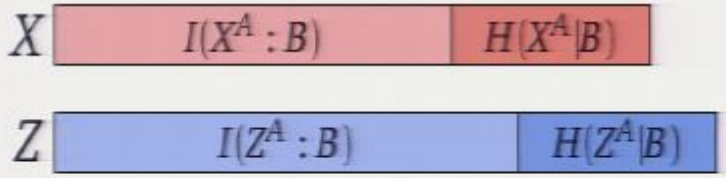
...by transmitting "missing" information

Private State/Entanglement Distillation...

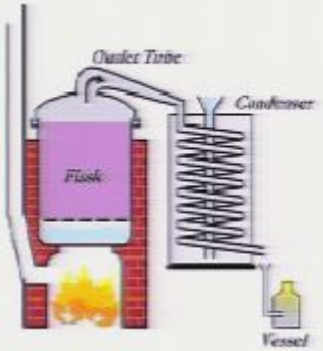


Given many copies of an arbitrary resource state, $\Psi^{AB[S]} = (\psi^{AB(S)})^{\otimes n}$, convert into (approximate) private/entangled states using local operations and (one-way) classical communication (with high probability).

...by transmitting "missing" information

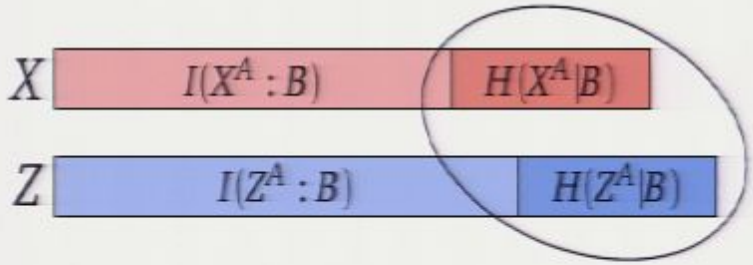


Private State/Entanglement Distillation...



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).

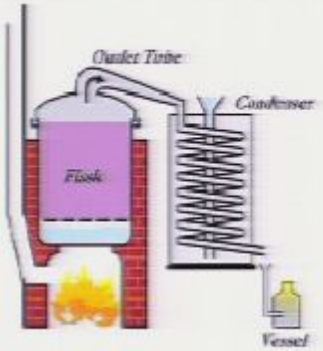
...by transmitting "missing" information



send this info to Bob.

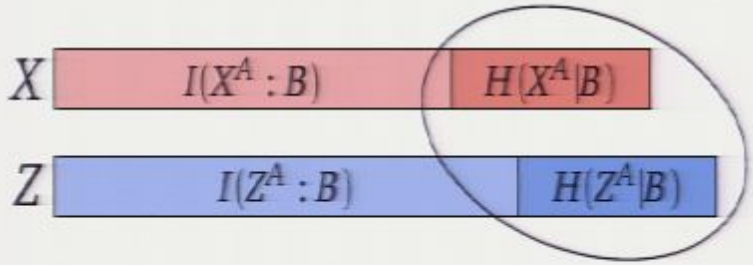
Here's how:

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.

Here's how:

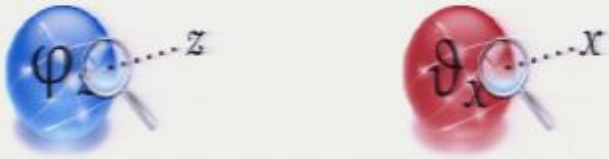
Here's how:

We start with $|\psi\rangle^{ABSE} = \sum_z \sqrt{p_z}\,|z\rangle^A\,|\varphi_z\rangle^{BSE} = \sum_x \sqrt{q_x}\,|\tilde{x}\rangle^A\,|\vartheta_x\rangle^{BSE}$

Here's how:

We start with $|\psi\rangle^{ABSE} = \sum_z \sqrt{p_z}\,|z\rangle^A\,|\varphi_z\rangle^{BSE} = \sum_x \sqrt{q_x}\,|\widetilde{x}\rangle^A\,|\vartheta_x\rangle^{BSE}$

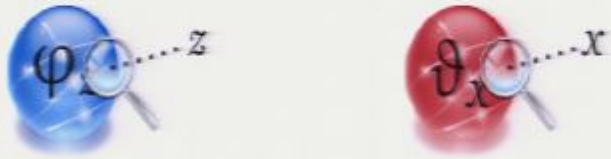
- Task is to extract z from φ_k^B and x from ϑ_x^{BS}.



Here's how:

We start with $|\psi\rangle^{ABSE} = \sum_z \sqrt{p_z}\,|z\rangle^A\,|\varphi_z\rangle^{BSE} = \sum_x \sqrt{q_x}\,|\widetilde{x}\rangle^A\,|\vartheta_x\rangle^{BSE}$

- Task is to extract z from φ_k^B and x from ϑ_x^{BS}.



- Alice sends hints to Bob, enabling the states to be distinguished. Then he can construct a private state or entangled pair.

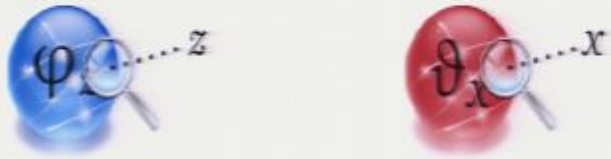
Possible zs

Support of φ_z^B

Here's how:

We start with $|\psi\rangle^{ABSE} = \sum_z \sqrt{p_z}\,|z\rangle^A\,|\varphi_z\rangle^{BSE} = \sum_x \sqrt{q_x}\,|\widetilde{x}\rangle^A\,|\vartheta_x\rangle^{BSE}$

- Task is to extract z from φ_k^B and x from ϑ_x^{BS}.



- Alice sends hints to Bob, enabling the states to be distinguished. Then he can construct a private state or entangled pair.

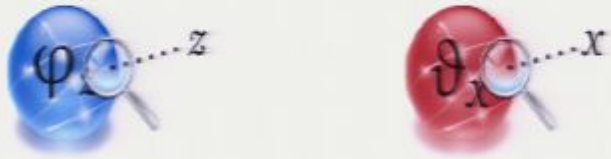
Possible zs

Support of φ_z^B

Here's how:

We start with $|\psi\rangle^{ABSE} = \sum_z \sqrt{p_z}\,|z\rangle^A\,|\varphi_z\rangle^{BSE} = \sum_x \sqrt{q_x}\,|\widetilde{x}\rangle^A\,|\vartheta_x\rangle^{BSE}$

- Task is to extract z from φ_k^B and x from ϑ_x^{BS}.



- Alice sends hints to Bob, enabling the states to be distinguished. Then he can construct a private state or entangled pair.

Possible zs

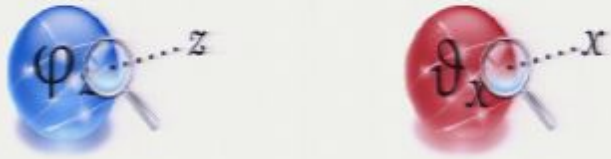
Support of φ_z^B

- The hints are generated by measuring stabilizers of a (suitably-chosen) CSS code; this ensures hint information exists simultaneously

Here's how:

We start with $|\psi\rangle^{ABSE} = \sum_z \sqrt{p_z}\,|z\rangle^A\,|\varphi_z\rangle^{BSE} = \sum_x \sqrt{q_x}\,|\widetilde{x}\rangle^A\,|\vartheta_x\rangle^{BSE}$

- Task is to extract z from φ_k^B and x from ϑ_x^{BS}.



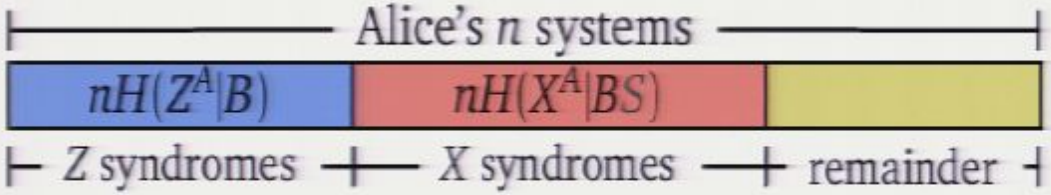
- Alice sends hints to Bob, enabling the states to be distinguished. Then he can construct a private state or entangled pair.

Possible zs

Support of φ_z^B

- The hints are generated by measuring stabilizers of a (suitably-chosen) CSS code; this ensures hint information exists simultaneously
- Finally, the (static) HSW theorem sets the size of the hints $\Rightarrow H(Z^A|B)$.

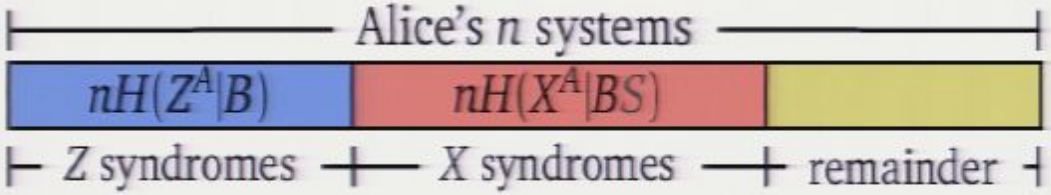
At what rates?



Naïve rate

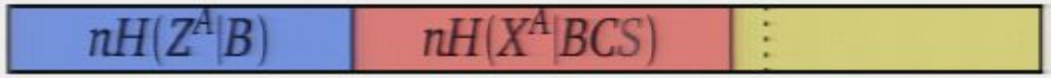
$1-H(Z^A|B)-H(X^A|BS)$

At what rates?



Naïve rate
$1-H(Z^A|B)-H(X^A|BS)$

- But it's a two-step process! After step one Bob has a Z^A basis copy of Alice's system in C.



Refined rate
$1-H(Z^A|B)-H(X^A|BCS)$

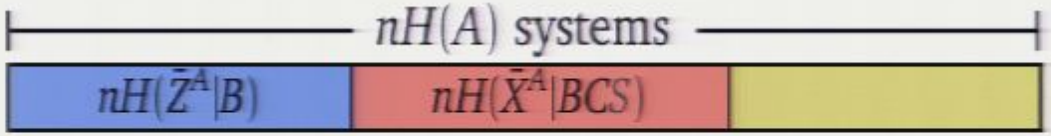
- Voilá! Can show refined rate equals $H(Z^A|E) - H(Z^A|B)$ for key distillation (with S) and $-H(A|B)$ for entanglement distillation (without S).
- However, too much communication is used in the process: $1 + H(E) - H(AE) > I(A:E)$.

State merging?

- The purification of Eve's state *is* merged in the protocol

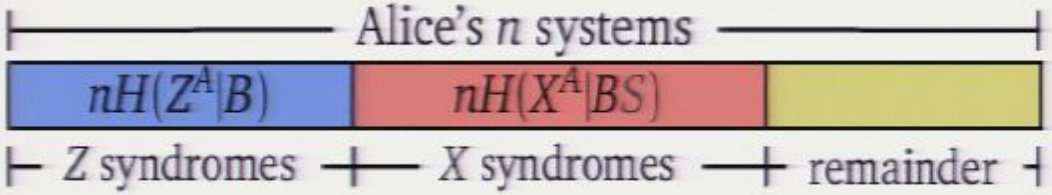
  Since Alice and Bob end up with $|\Phi\rangle$, the purification essentially has nowhere else to go

- Must fix communication rate. Trick is to first compress Alice's state to $H(A)$ qubits and then run the protocol.



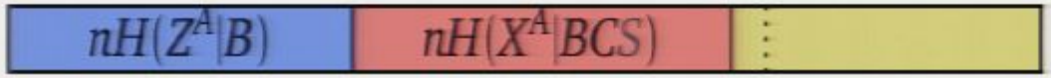
- Which screws up the X^A HSW measurement on the BS system...
- But via some magic it can be restored! Fortunately, the states ϑ_x^{BCS} are group covariant, which implies that the original mmt can be suitably modified for the compressed state.

At what rates?



Naïve rate
$1-H(Z^A|B)-H(X^A|BS)$

- But it's a two-step process! After step one Bob has a Z^A basis copy of Alice's system in C.



Refined rate
$1-H(Z^A|B)-H(X^A|BCS)$

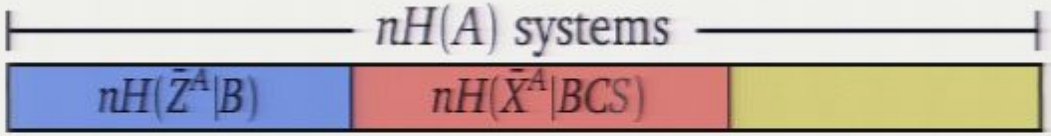
- Voilá! Can show refined rate equals $H(Z^A|E) - H(Z^A|B)$ for key distillation (with S) and $-H(A|B)$ for entanglement distillation (without S).
- However, too much communication is used in the process: $1 + H(E) - H(AE) > I(A:E)$.

State merging?

- The purification of Eve's state *is* merged in the protocol

  Since Alice and Bob end up with $|\Phi\rangle$, the purification essentially has nowhere else to go

- Must fix communication rate. Trick is to first compress Alice's state to $H(A)$ qubits and then run the protocol.



- Which screws up the X^A HSW measurement on the BS system...
- But via some magic it can be restored! Fortunately, the states ϑ_x^{BCS} are group covariant, which implies that the original mmt can be suitably modified for the compressed state.

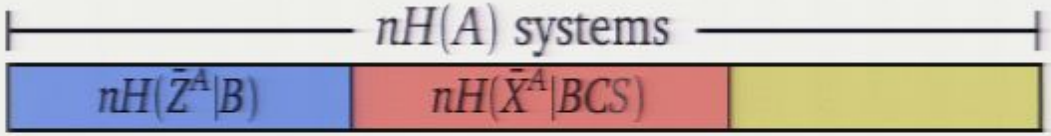
Fundamental results of quantum information theory rest on the phenomenon of complementarity

State merging?

- The purification of Eve's state *is* merged in the protocol

  Since Alice and Bob end up with $|\Phi\rangle$, the purification essentially has nowhere else to go

- Must fix communication rate. Trick is to first compress Alice's state to $H(A)$ qubits and then run the protocol.

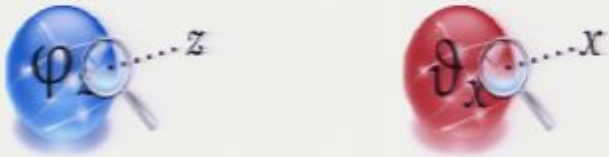


- Which screws up the X^A HSW measurement on the BS system...
- But via some magic it can be restored! Fortunately, the states ϑ_x^{BCS} are group covariant, which implies that the original mmt can be suitably modified for the compressed state.

Here's how:

We start with $|\psi\rangle^{ABSE} = \sum_z \sqrt{p_z}\,|z\rangle^A\,|\varphi_z\rangle^{BSE} = \sum_x \sqrt{q_x}\,|\widetilde{x}\rangle^A\,|\vartheta_x\rangle^{BSE}$

- Task is to extract z from φ_k^B and x from ϑ_x^{BS}.

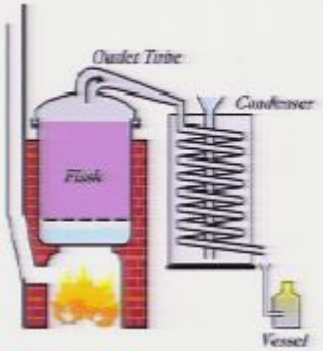


- Alice sends hints to Bob, enabling the states to be distinguished. Then he can construct a private state or entangled pair.

Possible zs

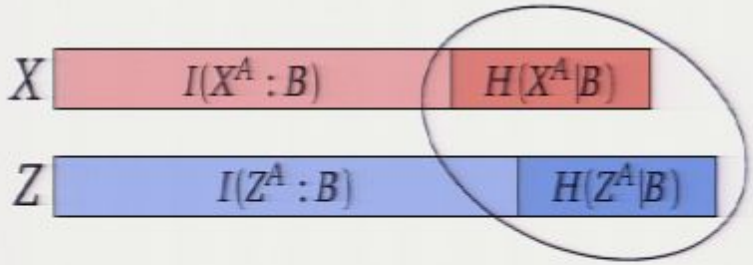
Support of φ_z^B

Private State/Entanglement Distillation...



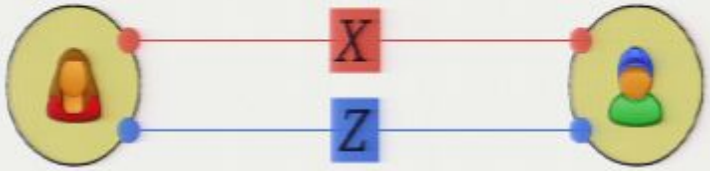
Given many copies of an arbitrary resource state, $\Psi^{AB[S]} = (\psi^{AB(S)})^{\otimes n}$, convert into (approximate) private/entangled states using local operations and (one-way) classical communication (with high probability).

...by transmitting "missing" information



send this info to Bob.

Couple Alice and Bob classically, twice.



- Quantum correlations between Alice and Bob are equivalent to two complementary classical correlations, say X and Z correlations.
- Quantum error correction strategy. But can we achieve the known rates? Answer: YES!
- Gives an explicit construction of the decoder

Complementarity-based Approach

- Key distillation rate Devetak & Winter ProcRoySocA **461** 207 (2005)

$$K_{\rightarrow}(\psi) \geq I(Z^A : B) - I(Z^A : E) = H(Z^A|E) - H(Z^A|B)$$

- Entanglement distillation rate

$$E_{\rightarrow}(\psi) \geq H(B) - H(AB) = -H(A|B).$$

- Communication cost $I(A:E)$ in either case.

- State merging at the same rates/costs Horodecki, Oppenheim, Winter Nature **436** 7051 (2005)
- Channel coding from entanglement distillation via teleportation

Complementary Information Tradeoff

JMR & JCB
arxiv:0806.3984 [quant-ph]

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

- Replace classical mutual information with Holevo upper bound.

  $H(O^A|B)$ is quantum conditional entropy after Alice measures O^A

- Numerical support for conjecture up to dimension 12.
- Holds for generalized Paulis X^A and Z^A.

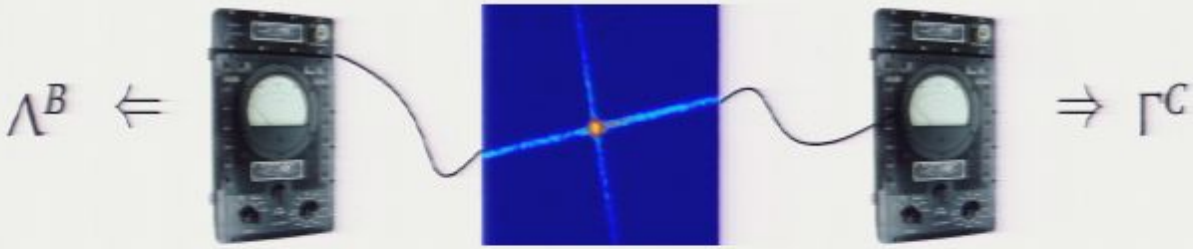
  proof from strong subadditivity — Christandl & Winter, IEEE TIT **51** 3159 (2005)

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.



- For generalized Paulis X and Z, any state $|\Psi\rangle$ satisfies $H(X) + H(Z) \geq \log d$
- But how much info can we *simultaneously* extract? Include mmt systems!

Information Exclusion Principle

Hall
PRL 74 3307 (1995)

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

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

- tradeoff in simultaneously available, complementary classical information

Complementary Information Tradeoff

JMR & JCB
arxiv:0806.3984 [quant-ph]

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

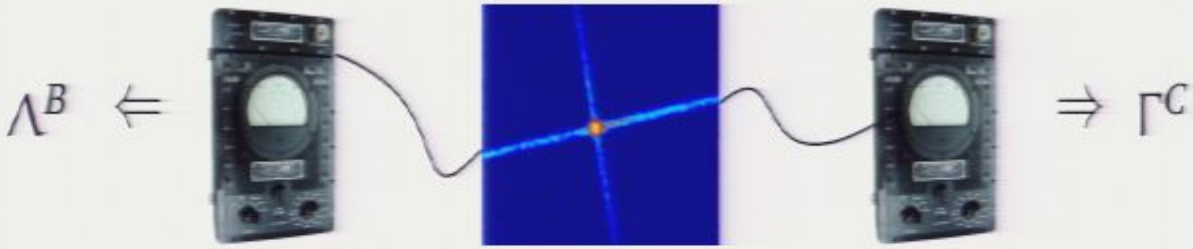
- Replace classical mutual information with Holevo upper bound.
  $H(O^A|B)$ is quantum conditional entropy after Alice measures O^A
- Numerical support for conjecture up to dimension 12.
- Holds for generalized Paulis X^A and Z^A.
  proof from strong subadditivity — Christandl & Winter, IEEE TIT **51** 3159 (2005)

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.



- For generalized Paulis X and Z, any state $|\Psi\rangle$ satisfies $H(X) + H(Z) \geq \log d$
- But how much info can we *simultaneously* extract? Include mmt systems!

Information Exclusion Principle

Hall
PRL 74 3307 (1995)

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

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

- tradeoff in simultaneously available, complementary classical information

Complementary Information Tradeoff

JMR & JCB
arxiv:0806.3984 [quant-ph]

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

- Replace classical mutual information with Holevo upper bound.
  $H(O^A|B)$ is quantum conditional entropy after Alice measures O^A
- Numerical support for conjecture up to dimension 12.
- Holds for generalized Paulis X^A and Z^A.
  proof from strong subadditivity — Christandl & Winter, IEEE TIT **51** 3159 (2005)