

# Quantum Communication and Cryptography

Joseph M. Renes



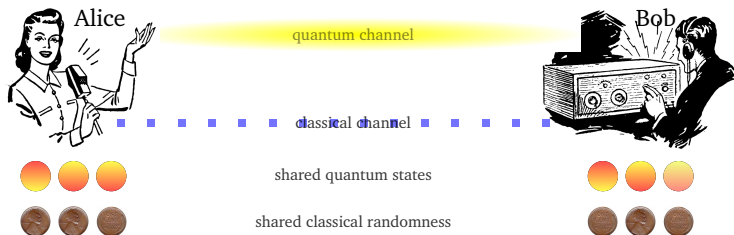
Theoretical Quantum Physics, Institut für Angewandte Physik  
Technische Universität Darmstadt



IQING 5

Innsbruck

2007 April 12



## Communication between distant parties

- Send messages
- Distributed computation
- Cryptographic use
- Create entanglement

## Major point: Interchangeability of resources

- noisy channel  $\rightarrow$  noiseless channel; noiseless + randomness  $\rightarrow$  noisy
- low-fidelity EPR pairs + classical communication  $\rightarrow$  maximal entanglement
- ...

## Overview recent work in quantum information theory. (in the strict sense)

- 1 Resource framework: how the myriad of protocols fit together.
  - Expressed as inequalities, for instance teleportation:  
 $[qq] + 2[c \rightarrow c] \leq [q \rightarrow q]$
  - Quantum family tree: Fully-Quantum Slepian-Wolf
- 2 Connection between Entanglement and Secret Keys
  - static/dynamic & quantum/classical:
    - entanglement generation & distillation
    - secret key generation & distillation
  - protocols have essentially the same proof
- 3 Erasure is Fundamental
  - Closer look at quantum capacity
  - Decoupling from the environment is enough
  - For coding, just pick a random subspace

## Unit Resources

Ideal cbit channel	$[c \rightarrow c]$		$[q \rightarrow q]$	Ideal qbit channel
Private cbit channel	$(c \rightarrow c)$			
Shared randomness	$[cc]$		$[qq]$	Shared entanglement

## Simple Protocols

$$\text{Teleportation} \quad [qq] + 2[c \rightarrow c] \geq [q \rightarrow q]$$

$$\text{Dense Coding} \quad [q \rightarrow q] + [qq] \geq 2[c \rightarrow c]$$

$$\text{Entanglement Distribution} \quad [q \rightarrow q] \geq [qq]$$

$$\text{Private Communication} \quad [qq] + [c \rightarrow c] \geq (c \rightarrow c)$$

$$[q \rightarrow q] \geq (c \rightarrow c)$$

I. Devetak, A. W. Harrow, and A. Winter, quant-ph/0512015

## General Resources

noisy channel  $\langle \mathcal{N}^{A \rightarrow B} \rangle$       shared state  $\langle \varphi^{AB} \rangle$

## Standard Protocols

Schumacher compression  $S(\rho^A)[q \rightarrow q] \geq \langle \text{id}^{A \rightarrow B} \rangle$

HSW theorem  $\langle \mathcal{N}^{T \rightarrow B} \rangle \geq I(X:B)[c \rightarrow c]$

Quantum capacity  $\langle \mathcal{N}^{T \rightarrow B} \rangle \geq I(A)B[q \rightarrow q]$

Entanglement distillation  $\langle \rho^{AB} \rangle + I(A:E)[c \rightarrow c] \geq I(A)B[qq]$

---

## General Resources

noisy channel  $\langle \mathcal{N}^{A \rightarrow B} \rangle$       shared state  $\langle \varphi^{AB} \rangle$

## Standard Protocols

Schumacher compression  $S(\rho^A)[q \rightarrow q] \geq \langle \text{id}^{A \rightarrow B} \rangle$

HSW theorem  $\langle \mathcal{N}^{T \rightarrow B} \rangle \geq I(X:B)[c \rightarrow c]$

Quantum capacity  $\langle \mathcal{N}^{T \rightarrow B} \rangle \geq I(A)B[q \rightarrow q]$

Entanglement distillation  $\langle \rho^{AB} \rangle + I(A:E)[c \rightarrow c] \geq I(A)B[qq]$

---

Transmit  $\rho^A$  by first compressing it, then using a noiseless channel

## General Resources

noisy channel  $\langle \mathcal{N}^{A \rightarrow B} \rangle$       shared state  $\langle \varphi^{AB} \rangle$

## Standard Protocols

Schumacher compression  $S(\rho^A)[q \rightarrow q] \geq \langle \text{id}^{A \rightarrow B} \rangle$

HSW theorem  $\langle \mathcal{N}^{T \rightarrow B} \rangle \geq I(X:B)[c \rightarrow c]$

Quantum capacity  $\langle \mathcal{N}^{T \rightarrow B} \rangle \geq I(A:B)[q \rightarrow q]$

Entanglement distillation  $\langle \rho^{AB} \rangle + I(A:E)[c \rightarrow c] \geq I(A:B)[qq]$

- Transmit classical message over a quantum channel
- Start with the state  $\rho^{XT} = \sum_x p_x |x\rangle\langle x|^X \otimes \rho_x^T$
- Send  $T$  to obtain  $\sigma^{XB} = \mathcal{N}^{T \rightarrow B}(\rho^{XT})$
- $I(X:B)$  is the Holevo quantity  $\chi = S(\sum_x p_x \sigma_x^B) - \sum_x p_x S(\sigma_x^B)$ .

## General Resources

noisy channel  $\langle \mathcal{N}^{A \rightarrow B} \rangle$       shared state  $\langle \varphi^{AB} \rangle$

## Standard Protocols

Schumacher compression  $S(\rho^A)[q \rightarrow q] \geq \langle \text{id}^{A \rightarrow B} \rangle$

HSW theorem  $\langle \mathcal{N}^{T \rightarrow B} \rangle \geq I(X:B)[c \rightarrow c]$

Quantum capacity  $\langle \mathcal{N}^{T \rightarrow B} \rangle \geq I(A)B[q \rightarrow q]$

Entanglement distillation  $\langle \rho^{AB} \rangle + I(A:E)[c \rightarrow c] \geq I(A)B[qq]$

- 
- Encode quantum messages for transmission over a noisy channel
  - Input ensemble state  $\rho^T$  has purification  $|\psi\rangle\langle\psi|^{TA}$
  - Channel outputs  $\sigma^{AB} = \mathcal{N}^{T \rightarrow B}(\rho^{TA})$
  - $I(A)B = -H(A|B)$  is the coherent information.

## General Resources

noisy channel  $\langle \mathcal{N}^{A \rightarrow B} \rangle$       shared state  $\langle \varphi^{AB} \rangle$

## Standard Protocols

Schumacher compression  $S(\rho^A)[q \rightarrow q] \geq \langle \text{id}^{A \rightarrow B} \rangle$

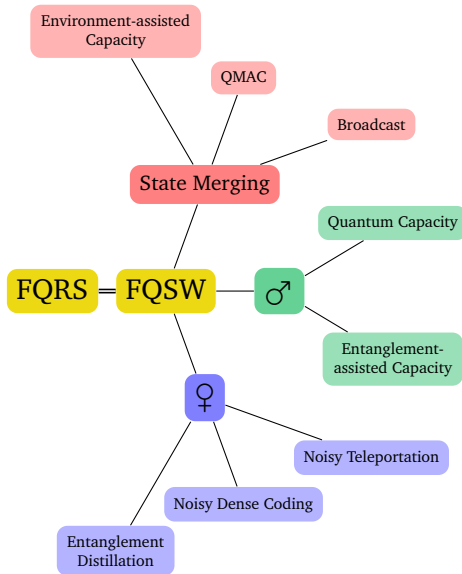
HSW theorem  $\langle \mathcal{N}^{T \rightarrow B} \rangle \geq I(X:B)[c \rightarrow c]$

Quantum capacity  $\langle \mathcal{N}^{T \rightarrow B} \rangle \geq I(A)B[q \rightarrow q]$

Entanglement distillation  $\langle \rho^{AB} \rangle + I(A:E)[c \rightarrow c] \geq I(A)B[qq]$

---

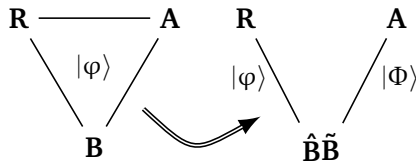
- Distill maximal entanglement from  $\varphi^{AB}$
- use only local operations and classical communication
- $E$  comes from purifying  $\varphi^{AB}$  to  $|\psi\rangle\langle\psi|^{ABE}$



## 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

$$r = I(A)B = H(B) - H(AB)$$

I. Devetak and A. Winter, PRL 93 080501 (2004).

### Entanglement Generation

Use  $n$  copies of the channel  $\mathcal{N}$  to generate  $nr$  bits of shared entanglement,  $(\Phi^{AB})^{\otimes nr}$

### Secret Key Generation

Use  $n$  copies of the channel  $\mathcal{N}$  to generate  $nr$  bits of shared secret key,  $(\kappa^{ABE})^{\otimes nr}$

### Entanglement Distillation

Convert  $(\rho^{AB})^{\otimes n}$  into  $nr$  ebits  $\Phi^{\otimes nr}$  using 1-LOCC

### Secret Key Distillation

Convert  $(\bar{\rho}^{AB})^{\otimes n}$  into  $nr$  secret key bits  $\kappa^{\otimes nr}$  using 1-LOPC

Rows: Static vs. Dynamic

Columns: Classical vs. Quantum

$$r = I(A)B = H(B) - H(AB)$$

I. Devetak and A. Winter, PRL 93 080501 (2004).

### Entanglement Generation

Use  $n$  copies of the channel  $\mathcal{N}$  to generate  $nr$  bits of shared entanglement,  $(\Phi^{AB})^{\otimes nr}$

### Secret Key Generation

Use  $n$  copies of the channel  $\mathcal{N}$  to generate  $nr$  bits of shared secret key,  $(\kappa^{ABE})^{\otimes nr}$

### Entanglement Distillation

Convert  $(\rho^{AB})^{\otimes n}$  into  $nr$  ebits  $\Phi^{\otimes nr}$  using 1-LOCC

### Secret Key Distillation

Convert  $(\bar{\rho}^{AB})^{\otimes n}$  into  $nr$  secret key bits  $\kappa^{\otimes nr}$  using 1-LOPC



Specify  $\mathcal{E}$ ncoding for Alice and  $\mathcal{D}$ ecoding for Bob.  
Same as quantum channel capacity

$$r = I(A)B = H(B) - H(AB)$$

I. Devetak and A. Winter, PRL 93 080501 (2004).

### Entanglement Generation

Use  $n$  copies of the channel  $\mathcal{N}$  to generate  $nr$  bits of shared entanglement,  $(\Phi^{AB})^{\otimes nr}$

### Secret Key Generation

Use  $n$  copies of the channel  $\mathcal{N}$  to generate  $nr$  bits of shared secret key,  $(\kappa^{ABE})^{\otimes nr}$

### Entanglement Distillation

Convert  $(\rho^{AB})^{\otimes n}$  into  $nr$  ebits  $\Phi^{\otimes nr}$  using 1-LOCC

### Secret Key Distillation

Convert  $(\bar{\rho}^{AB})^{\otimes n}$  into  $nr$  secret key bits  $\kappa^{\otimes nr}$  using 1-LOPC



Specify  $\mathcal{E}$ ncoding for Alice and  $\mathcal{M}$ easurement for Bob.

$$\kappa^{ABE} = \frac{1}{2} \sum_k |kk\rangle\langle kk|^{AB} \otimes \rho^E$$

$$r = I(A)B = H(B) - H(AB)$$

I. Devetak and A. Winter, PRL 93 080501 (2004).

### Entanglement Generation

Use  $n$  copies of the channel  $\mathcal{N}$  to generate  $nr$  bits of shared entanglement,  $(\Phi^{AB})^{\otimes nr}$

### Secret Key Generation

Use  $n$  copies of the channel  $\mathcal{N}$  to generate  $nr$  bits of shared secret key,  $(\kappa^{ABE})^{\otimes nr}$

### Entanglement Distillation

Convert  $(\rho^{AB})^{\otimes n}$  into  $nr$  ebits  $\Phi^{\otimes nr}$  using 1-LOCC

### Secret Key Distillation

Convert  $(\bar{\rho}^{AB})^{\otimes n}$  into  $nr$  secret key bits  $\kappa^{\otimes nr}$  using 1-LOPC

- $\rho^{AB}$  is purified to  $|\psi\rangle^{ABE} = \sum_x \sqrt{p_x} |x\rangle^A \otimes |\psi_k\rangle^{BE}$
- regard  $|\psi_k\rangle^{BE}$  as  $\mathcal{N} \circ \mathcal{E}(|\varphi_k\rangle^T)$
- rate bound is known as the Hashing inequality

$$r = I(A)B = H(B) - H(AB)$$

I. Devetak and A. Winter, PRL 93 080501 (2004).

### Entanglement Generation

Use  $n$  copies of the channel  $\mathcal{N}$  to generate  $nr$  bits of shared entanglement,  $(\Phi^{AB})^{\otimes nr}$

### Secret Key Generation

Use  $n$  copies of the channel  $\mathcal{N}$  to generate  $nr$  bits of shared secret key,  $(\kappa^{ABE})^{\otimes nr}$

### Entanglement Distillation

Convert  $(\rho^{AB})^{\otimes n}$  into  $nr$  ebits  $\Phi^{\otimes nr}$  using 1-LOCC

### Secret Key Distillation

Convert  $(\bar{\rho}^{AB})^{\otimes n}$  into  $nr$  secret key bits  $\kappa^{\otimes nr}$  using 1-LOPC

- Starting point is  $\bar{\rho}^{AB} = \sum_k p_k |k\rangle\langle k|^A \otimes \psi_k^B$ , the decohered version.
- Use only one-way local operations and public communication

$$r = I(A)B = H(B) - H(AB)$$

I. Devetak and A. Winter, PRL 93 080501 (2004).

### Entanglement Generation

Use  $n$  copies of the channel  $\mathcal{N}$  to generate  $nr$  bits of shared entanglement,  $(\Phi^{AB})^{\otimes nr}$

### Secret Key Generation

Use  $n$  copies of the channel  $\mathcal{N}$  to generate  $nr$  bits of shared secret key,  $(\kappa^{ABE})^{\otimes nr}$

### Entanglement Distillation

Convert  $(\rho^{AB})^{\otimes n}$  into  $nr$  ebits  $\Phi^{\otimes nr}$  using 1-LOCC

### Secret Key Distillation

Convert  $(\bar{\rho}^{AB})^{\otimes n}$  into  $nr$  secret key bits  $\kappa^{\otimes nr}$  using 1-LOPC

In the asymptotic case we use the power of typical sequences and sets.

Consider coin with  $\Pr_{\text{heads}} = p$ :

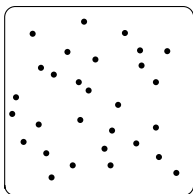
- After  $n \rightarrow \infty$  tosses, only the set of sequences for which  $\#_{\text{heads}} \approx np$  has nonnegligible probability
- Moreover, sequences occur with essentially equal probability
- Roughly  $2^{nH_2(p)}$  such sequences, for binary entropy  $H_2$

Apply the same to density matrices by working in the eigenbasis:

- $\rho$  has eigenvalues  $\{p, 1-p\}$
- ⇒  $\rho^{\otimes n}$  has support on subspace of dimension  $2^{nH_2(p)} = 2^{nS(\rho)}$
- ⇒  $\rho^{\otimes n}$  is essentially a projector onto this subspace

Start with  $n$  copies of  $\psi^{ABE} = \sum_k p_k |k\rangle\langle k|^A \otimes \psi_k^{BE}$

First correct errors: Bob doesn't know  $k$  exactly.  $\Rightarrow$  HSW Theorem!



Alice  $k$  strings



Bob state support

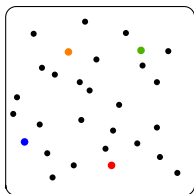
Bob cannot reliably distinguish the  $\psi_k^B$ . Can distinguish elements of a random subset!

- The  $\psi_k^B$  are essentially projectors of dimension  $\approx 2^{nH(B|K)}$
- Average state  $\psi^B$  lives on a space of size  $\approx 2^{nH(B)}$
- $\Rightarrow$  Intuitively we can pack in  $2^{nI(K:B)}$  disjoint  $\psi_k^B$

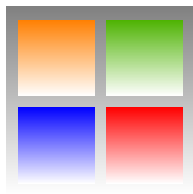
Hence, Alice projects onto a random subset of this size, and tells Bob which one.

Start with  $n$  copies of  $\psi^{ABE} = \sum_k p_k |k\rangle\langle k|^A \otimes \psi_k^{BE}$

First correct errors: Bob doesn't know  $k$  exactly.  $\Rightarrow$  HSW Theorem!



Alice  $k$  strings



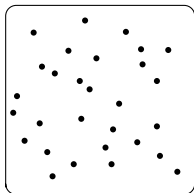
Bob state support

Bob cannot reliably distinguish the  $\psi_k^B$ . Can distinguish elements of a random subset!

- The  $\psi_k^B$  are essentially projectors of dimension  $\approx 2^{nH(B|K)}$
- Average state  $\psi^B$  lives on a space of size  $\approx 2^{nH(B)}$
- Intuitively we can pack in  $2^{nI(K:B)}$  disjoint  $\psi_k^B$

Hence, Alice projects onto a random subset of this size, and tells Bob which one.

Now perform privacy amplification to remove Eve's information.



Alice  $k$  strings



Eve state support

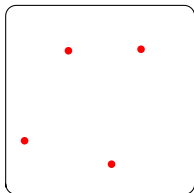
$\psi_k^E$  partially distinguishable; Eve can learn some information about the string  $k$ .

- Average state  $\psi^E$  is supported on a subspace of size  $\approx 2^{nH(E)}$
- Each  $\psi_k^E$  is a projector of dimension  $\approx 2^{nH(E|K)}$

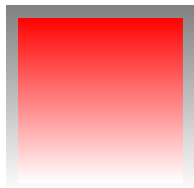
⇒ Intuitively, only  $\approx 2^{nI(K:E)}$  states are needed to cover the support of the average

Hence, if we label every state in the “cover” with the same secret key letter, Eve will have no information about it.

Now perform privacy amplification to remove Eve's information.



Alice  $k$  strings



Eve state support

$\psi_k^E$  partially distinguishable; Eve can learn some information about the string  $k$ .

- Average state  $\psi^E$  is supported on a subspace of size  $\approx 2^{nH(E)}$
- Each  $\psi_k^E$  is a projector of dimension  $\approx 2^{nH(E|K)}$

⇒ Intuitively, only  $\approx 2^{nI(K:E)}$  states are needed to cover the support of the average

Hence, if we label every state in the “cover” with the same secret key letter, Eve will have no information about it.

☞ How do we know these sorts of HSW and PA codes really exist?

Invoke the usual trick due to Shannon: **Show that random coding works with high probability!** The codewords  $k_{m,s}$  are such that:

- Bob can distinguish the  $\psi_{m,s}^B$
- Coarse-graining over  $s$  leaves Eve with indistinguishable  $\psi_m^E$
- Rate is  $r = I(A \setminus B) = I(K : B) - I(K : E)$
- Moreover, Alice only has to communicate  $nH(K|B)$  bits to Bob.

☞ For secret key *generation*, just feed a code into to the channel.

☞ Entanglement case: make states & operations coherent

- Start with  $|\Psi\rangle^{ABE} = \sum_k \sqrt{p_k} |k\rangle^A \otimes |\psi_k\rangle^{BE}$  in the static case
- coherently project onto one of the random HSW subsets
- ...
- convert static to dynamic as before

## Can instead construct PA codes based on the uncertainty principle!

- 1 From  $\rho^{AA'BB'}$ , measure  $Z^A$  and  $Z^B$  to create a key
  - Key is private iff Bob +  $A'$  can predict  $X^A$  mmt (think entanglement)
  - Defines the set of *private states* Horodecki<sup>3</sup> and Oppenheim, PRL 94, 160502 (2005)
  - UP: Bob's knowledge of  $X^A$  constrains Eve's knowledge of  $Z^A$ .
- 2 If  $\rho_x^{BB'}$  gives only partial information...
  - Use HSW theorem again!
  - Alice picks a random subset, erasing info Bob doesn't have
- 3 Watch out!
  - $X^A$  measurement is hypothetical, isn't actually performed
  - Figure out what key would have been...
  - If actual key distillation and  $X^A$  measurement commute, ok
  - Noisy preprocessing examined in: J. M. Renes and G. Smith, PRL 98, 020502 (2007).
  - General shield (but using only linear functions) considered in:

J. M. Renes and J.-C. Boileau, quant-ph/0702187.

## From FQSW:

“In contrast to most proofs in information theory, instead of showing how to establish perfect correlation of some kind between the sender and the receiver, our proof proceeds by showing that the protocol *destroys* all correlation between the sender and a reference system. **Since destruction is a relatively indiscriminate goal, the resulting proof is correspondingly simple.**”

**Quantum capacity strategy:** P. Hayden, M. Horodecki, J. Yard, and A. Winter, quant-ph/0702005

- View problem as sending entanglement with high fidelity
- Pick a random subspace at the encoder
- Decoupling from the environment ensures a decoder

## Decoupling implies (good) decoding

**Given** a channel  $\mathcal{N}^{T \rightarrow R}$ , purify it to a unitary  $V_{\mathcal{N}}^{T \rightarrow RE}$  by using an additional system  $E$ . Now put half a maximally entangled state  $|\Phi\rangle^{AT}$  through the channel, producing  $|\psi\rangle^{ARE} = V_{\mathcal{N}}^{T \rightarrow RE} |\Phi\rangle^{AT}$ .

**Then** there exists a decoding map  $\mathcal{D}^{R \rightarrow B}$  such that

$$F\left(|\Phi\rangle^{AB}, \mathbb{1}^A \otimes \mathcal{D} \circ \mathcal{N}(\Phi^{AT})\right) \geq 1 - \|\psi^{AE} - \mathbb{1}^A/d_A \otimes \psi^E\|_1$$

Use a random subspace of the appropriate size.

- Suppose  $|\psi\rangle^{AE}$  comes out of the channel such that  $\psi^A$  is maximally-mixed. (Put in an entangled state...)
- Now project onto a subspace  $\hat{A}$  using  $\Pi^{A \rightarrow \hat{A}}$ , obtaining  $\psi_{\Pi}^{\hat{A}E}$ .
- By first applying a unitary we can use  $\Pi$  to project onto any subspace we like:  $\psi_U^{\hat{A}E} \propto (\Pi U \otimes \mathbb{1}^E) \psi^{AE} (U^\dagger \Pi \otimes \mathbb{1}^E)$
- Averaging over all choices of  $\Pi$  yields

$$\int_{\mathcal{U}(A)} dU \left\| \psi_U^{\hat{A}E} - \mathbb{1}^{\hat{A}}/d_{\hat{A}} \otimes \psi_U^E \right\|_1 \leq \sqrt{|\hat{A}| |E| \text{Tr}[(\psi^{AE})^2]}$$

- ➡ RHS small  $\Rightarrow$  channel output decoupled  $\Rightarrow$  decoding operation
- ➡ Encoding operation is  $U^\dagger \Pi$ , since original input maximally-entangled.
- ➡ For the case of *block inputs* to a *memoryless* channel, we can evaluate the rhs by using typical sequences and subspaces...