

# Private States in Quantum Key Distribution

Joseph M. Renes  and Jean-Christian Boileau <sup>IQC</sup>



Theoretical Quantum Physics, Institut für Angewandte Physik  
Technische Universität Darmstadt



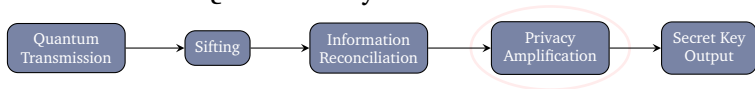
Institute for Quantum Computing, University of Waterloo

Tropical QKD

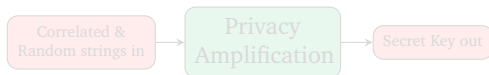
Waterloo

2007 June 13

## Quantum Key Distribution

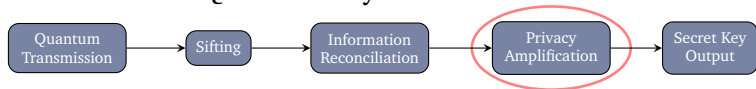


Private states arise in the quantum description of privacy amplification



- Generalization of QKD as virtual entanglement distillation (Lo-Chau, Shor-Preskill, ...) Contrast with other descriptions: LOPC (ccq states: Devetak & Winter, Renner & König), uncertainty principle (Koashi)
- Import known results from quantum communication theory (entanglement distillation, error-correcting codes, etc.)
- Different approach/picture useful for analyzing QKD security
  - Physical understanding of the mechanism of security
  - Understand helpfulness of adding noise, degenerate codes, etc.
  - Extend security proofs in new directions: finite key length (?)

## Quantum Key Distribution



Private states arise in the quantum description of privacy amplification

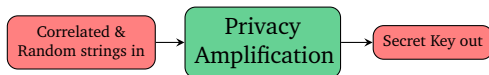


- Generalization of QKD as virtual entanglement distillation (Lo-Chau, Shor-Preskill, ...) Contrast with other descriptions: LOPC (ccq states: Devetak & Winter, Renner & König), uncertainty principle (Koashi)
- Import known results from quantum communication theory (entanglement distillation, error-correcting codes, etc.)
- Different approach/picture useful for analyzing QKD security
  - Physical understanding of the mechanism of security
  - Understand helpfulness of adding noise, degenerate codes, etc.
  - Extend security proofs in new directions: finite key length (?)

## Quantum Key Distribution



Private states arise in the quantum description of privacy amplification



- Generalization of QKD as virtual entanglement distillation (Lo-Chau, Shor-Preskill, ...) Contrast with other descriptions: LOPC (ccq states: Devetak & Winter, Renner & König), uncertainty principle (Koashi)
- Import known results from quantum communication theory (entanglement distillation, error-correcting codes, etc.)
- Different approach/picture useful for analyzing QKD security
  - Physical understanding of the mechanism of security
  - Understand helpfulness of adding noise, degenerate codes, etc.
  - Extend security proofs in new directions: finite key length (?)

## Quick Outline

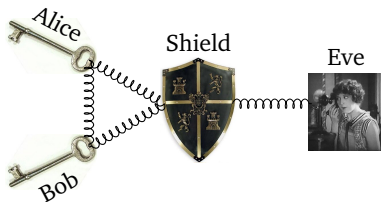
- 1 What are private states?  
How do they relate to secret keys?
- 2 How can private states be distilled from imperfect sources?  
How does this relate to privacy amplification?
- 3 What can we do with private states in QKD?

Private states are quantum purifications of secret keys.

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

- Pick a basis for the key ( $Z$  basis) and let  $P_{jk}^{AB} = |jk\rangle\langle jk|$
- Perfect secret key bit:  $\kappa^{ABE} = \left(\frac{1}{2} \sum_k |kk\rangle\langle kk|^{AB}\right) \otimes \rho^E$
- Include *shield*  $S$  and purify  $\kappa^{ABE}$  to private state  $|\gamma\rangle^{ABSE}$

Shield deflects AB correlations from E



Definition

$$|\gamma\rangle = \frac{1}{\sqrt{2}} \sum_k |kk\rangle^{AB} V_k^S |\xi\rangle_{SE} = U^{ABS} |\Phi\rangle^{AB} |\xi\rangle^{SE}$$

• Unitaries  $V_k^S$  and state  $|\xi\rangle^{SE}$  arbitrary

•  $|\Phi\rangle^{AB}$  maximally entangled

Twisting operator:  $U^{ABS} = \sum_{jk} P_{jk}^{AB} \otimes V_{jk}^S$

Shield owned by AB, but not part of key

— Entanglement with a twist —

Twisted state definition a little unnatural; our concern is secrecy!

An equivalent definition is the more intuitive one:

Secrecy definition:  $|\gamma\rangle^{ABSE}$  a private state iff

- ① AB systems are **correlated & random**:  $p_{jk} = \text{Tr}[\gamma^{ABSE} P_{jk}^{AB}] = \frac{1}{2} \delta_{jk}$ .
- ② Eve is **ignorant of the key**:  $\gamma_j^E = \gamma_k^E$  for all  $j, k$ .  $\gamma_k^E = 2\text{Tr}_{ABS}[\gamma^{ABSE} P_{kk}^{AB}]$ .

Alternate definition—Bob+Shield are entangled with Alice.

Suppose Alice measured her key system in the  $X$  basis,

leaving Bob+Shield with  $\sigma_x^{BS} = 2\text{Tr}_E[\langle \tilde{x} |^A \gamma^{ABSE} | \tilde{x} \rangle^A]$ .

Entanglement definition:  $|\gamma\rangle^{ABSE}$  a private state iff

- ① AB systems are **correlated & random**:  $p_{jk} = \text{Tr}[\gamma^{ABSE} P_{jk}^{AB}] = \frac{1}{2} \delta_{jk}$ .
- ② Bob+Shield **can predict  $X^A$** :  $\sigma_x^{BS} \sigma_{x'}^{BS} = 0$  for all  $x \neq x'$ .

## Intuitive private state distillation method: Assumptions

- Input raw key bit is random, but shared by Alice and Bob
- They are asymptotically many i.i.d. copies (collective attack)

Shared state is  $|\Psi\rangle^{ABSE} = \left( \frac{1}{\sqrt{2}} \sum_k |kk\rangle^{AB} |\varphi_k\rangle^{SE} \right)^{\otimes n}$



Alice



Shield+Eve



Bob

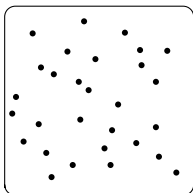
- Suppose Alice measures  $X^A$ , obtains  $\mathbf{x}$  (with uniform probability).  
BS state is

$$\rho_{\mathbf{x}}^{BS} = Z_B^{\mathbf{x}} \rho^{BS} Z_B^{\mathbf{x}}$$

where  $\rho^{BS} = \frac{1}{2} \sum_{\mathbf{k}, \mathbf{k}'} |\mathbf{k}\rangle \langle \mathbf{k}'|^B \otimes \text{Tr}_E[|\varphi_{\mathbf{k}}\rangle \langle \varphi_{\mathbf{k}'}|^{SE}]$

## Distillation Scheme: Alice narrows the possible $\rho_x^{BS}$

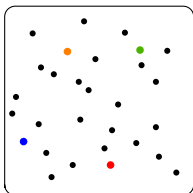
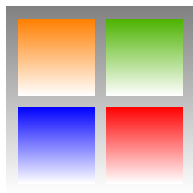
- Bob+Shield information =  $I(X:BS) = \chi(\{\frac{1}{2}, \rho_x^{BS}\})$  (Holevo info)
- Pick a random subset  $T$  of the possible  $\mathbf{x}$ s, size  $nI(X:BS)$ . With high probability, the  $\rho_x^{BS}$  for  $\mathbf{x} \in T$  are perfectly distinguishable

Alice  $\mathbf{x}$  strings $\rho_x^{BS}$  state support

- ☞ Alice picks a random subset containing the actual  $\mathbf{x}$  and tells Bob.
- ☞ Rate should therefore be  $I(X:BS)$ .

Distillation Scheme: Alice narrows the possible  $\rho_{\mathbf{x}}^{BS}$ 

- Bob+Shield information =  $I(X:BS) = \chi(\{\frac{1}{2}, \rho_{\mathbf{x}}^{BS}\})$  (Holevo info)
- Pick a random subset  $T$  of the possible  $\mathbf{x}$ s, size  $nI(X:BS)$ . With high probability, the  $\rho_{\mathbf{x}}^{BS}$  for  $\mathbf{x} \in T$  are perfectly distinguishable

Alice  $\mathbf{x}$  strings $\rho_{\mathbf{x}}^{BS}$  state support

- ☞ Alice picks a random subset containing the actual  $\mathbf{x}$  and tells Bob.
- ☞ Rate should therefore be  $I(X:BS)$ .

## Two pitfalls

- ① Alice & Bob mustn't disturb (all) the correlated  $Z$  values
- ② Must reduce to prepare & measure scheme, i.e. to *privacy amplification*

*Random linear hashing* solves both problems

- Alice chooses random strings  $\mathbf{u}_i$  and broadcasts  $h_i = \mathbf{u}_i \cdot \mathbf{x}$ .
- Secret key bits turn out to be  $s_j = \mathbf{v}_j \cdot \mathbf{k}$ ,  
for a linearly independent set  $\mathbf{v}_j$  such that  $\mathbf{v}_j \cdot \mathbf{u}_i = 0$  for all  $i, j$
- Secret key at rate  $I(X : BS) = 1 - I(A : E)$  (as in D & W, R & K, etc.)
- ☞ Scheme is reducible to privacy amplification!
- ☞ Linear structure makes it easy to construct untwisting operator  
Details: JMR & JCB, quant-ph/0702187

Integration into QKD proof: can we calculate  $I(X : BS)$ ? Do we know  $\Psi^{ABS}$ ?

### Tagged Signals: Multiphoton pulses

- Tagging breaks  $X$  correlation between Alice and Bob + Shield
- $I(X : BS)$  easy to compute: just throw out tagged signals

Local Randomization: Alice adds i.i.d. noise at rate  $q$ 

➡ noise register & control-NOT gate

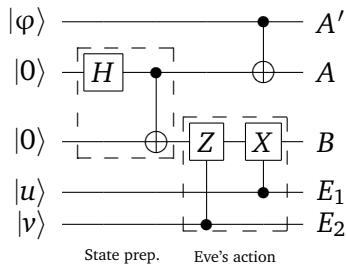
☞ Use  $|\varphi\rangle_{A'} = \sqrt{1-q}|0\rangle + \sqrt{q}|1\rangle$

☞ Apply  $\text{CNOT}_{A' \rightarrow A}$

➡ System  $A'$  is the shield.

Can compute  $I(X : BS)$

➡ **CNOT gives Bob info about  $X^A$**



☞ For *unknown* shields, see Horodecki<sup>3</sup>, Leung, and Oppenheim, quant-ph/0608195v2

## Summary

- ☞ Private States are the quantum description of secret keys
- ☞ Simple generalization of entanglement:  
Bob+Shield can predict  $Z^A$  and  $X^A$ .
- ☞ Easy to distill, at least using linear hashing:  
Rate  $I(X : BS)$  identical to that of other methods,  $1 - I(X : E)$ .

## Future Directions

- Explore connections to other proof methods
- Coherent attacks (especially when shield unknown)
- Extend to general 2-universal hashing
- Apply to practical issues, including finite key



Alexander von Humboldt



Stiftung/Foundation