Public discussion in Quantum Cryptography

Geir Ove Myhr

Institut für Theoretische Physik I
Universität Erlangen-Nürnberg
and
Institute for Quantum Computing
University of Waterloo

With:
Norbert Lütkenhaus, Waterloo and Joe Renes, Darmstadt

IQC Institute for Quantum Computing | Norges forskningsråd | Friedrich-Alexander-Universität Erlangen-Nürnberg

2006-08-16 / CQISC'06 Calgary

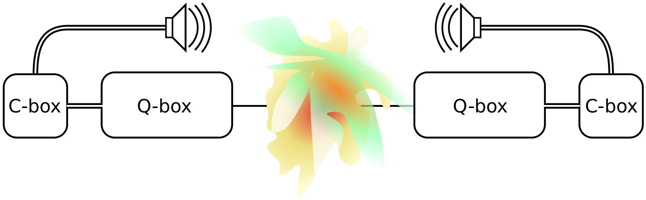
Outline

Outline

Two phases of quantum key distribution

1. *Quantum* apparatus to generate *classical* data
2. Post-processing of the data, including *public* communication

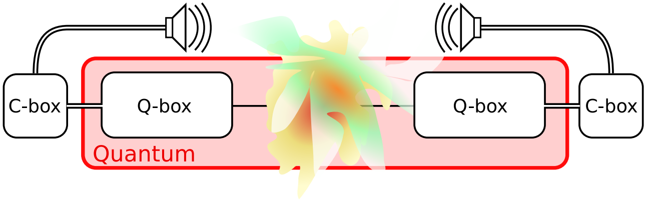
If the data is found to be good enough, this will lead to a secret key



Two phases of quantum key distribution

1. *Quantum* apparatus to generate *classical* data
2. Post-processing of the data, including *public* communication

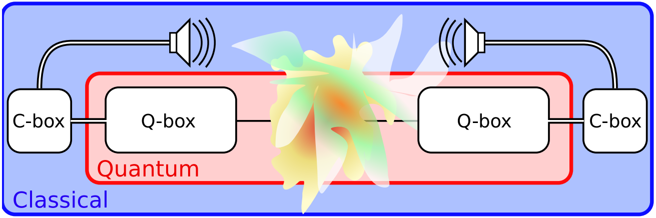
If the data is found to be good enough, this will lead to a secret key



Two phases of quantum key distribution

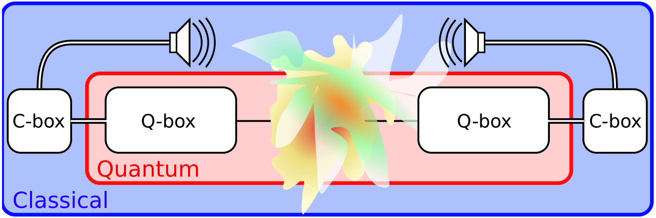
1. *Quantum* apparatus to generate *classical* data
2. Post-processing of the data, including *public* communication

If the data is found to be good enough, this will lead to a secret key



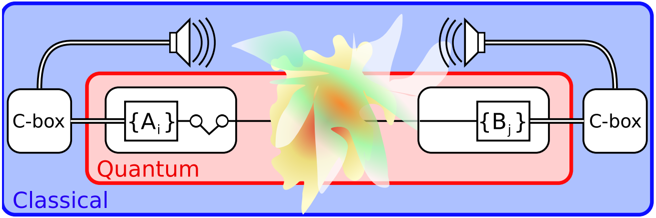
Replacement

- For the analysis, we can replace a box with another box that behaves the same way externally.
- Prepare & Measure $\leftrightarrow$ Entanglement based



Replacement

- For the analysis, we can replace a box with another box that behaves the same way externally.
- Prepare & Measure $\leftrightarrow$ Entanglement based



Threshold and upper bound for key rate

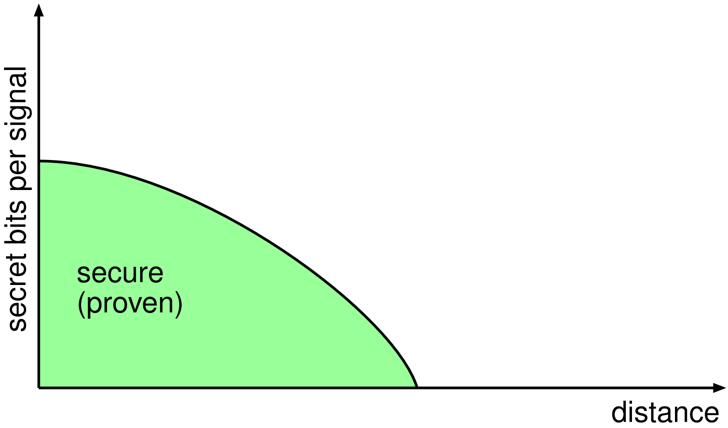
- General bound and threshold
  - If you cannot prove entanglement from your data, no secret key (Marcos Curty)
  - Specific attack: Eve splits the state into separable and entangled part
    $\Rightarrow$ Upper bound (Tobias Moroder)
- One way bound and threshold
  - If you cannot rule out a symmetric extension of the state, no secret key from one way communication
  - Eve can split into parts with and without symmetric extension
    $\Rightarrow$ One-way upper bound

Threshold and upper bound for key rate

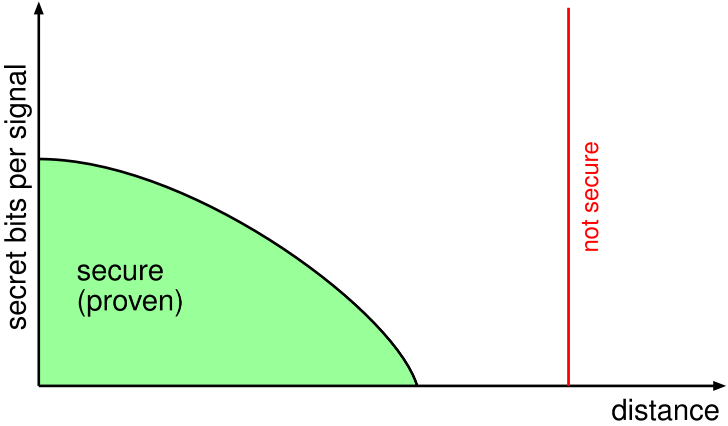
- General bound and threshold
  - If you cannot prove entanglement from your data, no secret key (Marcos Curty)
  - Specific attack: Eve splits the state into separable and entangled part
    $\Rightarrow$ Upper bound (Tobias Moroder)
- One way bound and threshold
  - If you cannot rule out a symmetric extension of the state, no secret key from one way communication
  - Eve can split into parts with and without symmetric extension
    $\Rightarrow$ One-way upper bound

Present situation in QKD

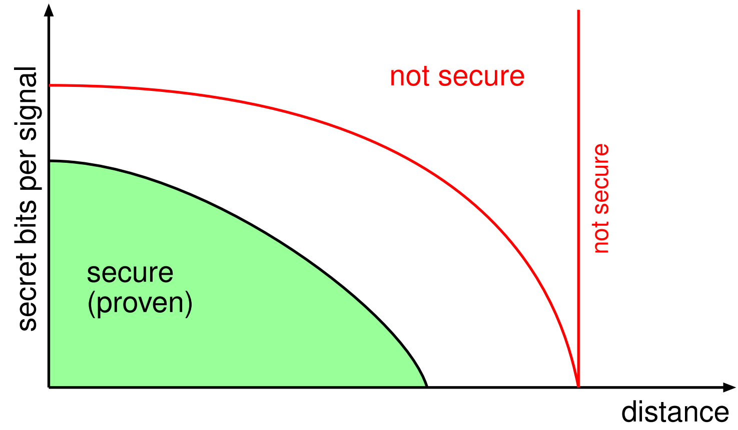
Present situation in QKD



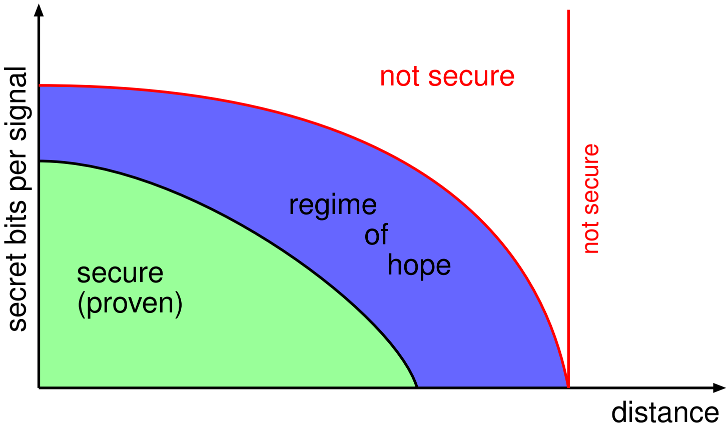
Present situation in QKD



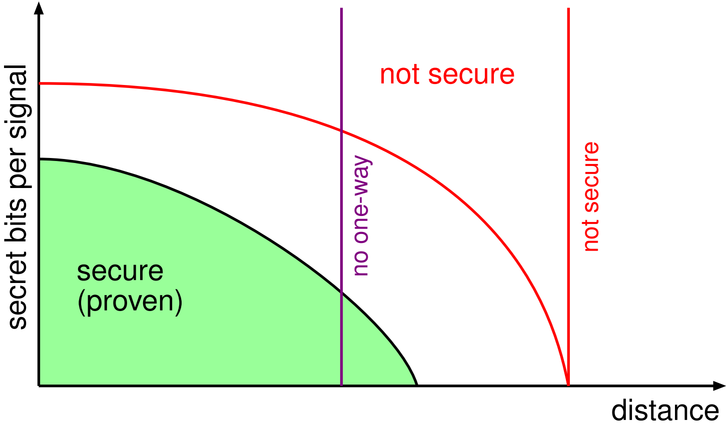
Present situation in QKD



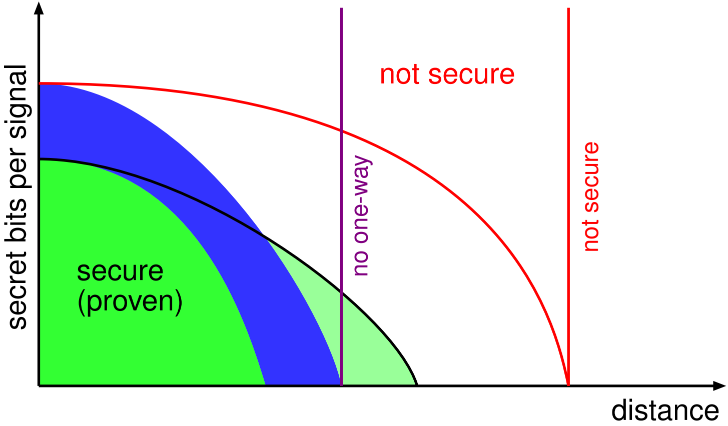
Present situation in QKD



Present situation in QKD



Present situation in QKD



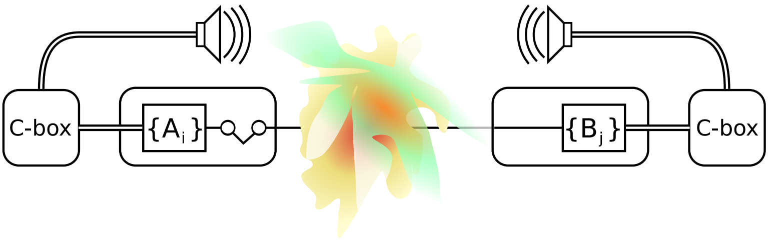
How to get rid of symmetric extensions?

- To get key from states above one-way threshold we have to get rid of the symmetric extension
- If there is a symmetric extension from Bob, he can get rid of it by talking to Alice
- Gottesman-Lo trick (B-step):

Outline

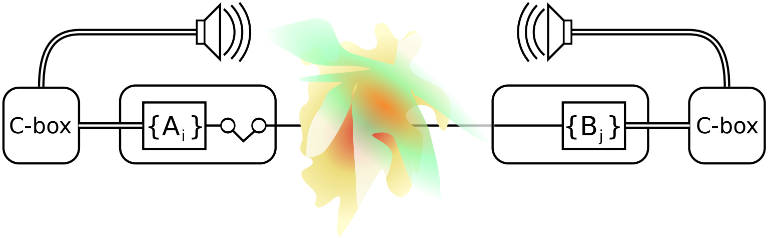
Another replacement

- What really happens: Measure a POVM, announce a function of the result
- Replacement: Do measurement in two steps
  1. An incomplete measurement to measure what is to be announced
     → check entanglement and symmetric extension
  2. Complete the measurement to get a partially secret bit



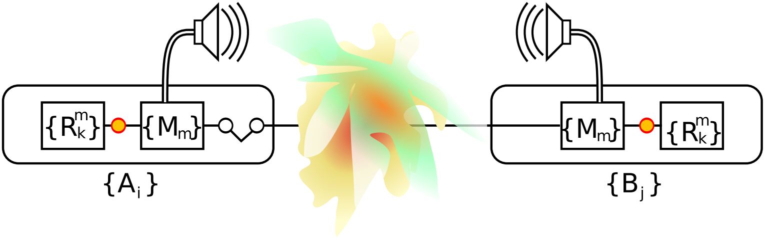
Another replacement

- What really happens: Measure a POVM, announce a function of the result
- Replacement: Do measurement in two steps
  1. An incomplete measurement to measure what is to be announced
     $\rightarrow$ check entanglement and symmetric extension
  2. Complete the measurement to get a partially secret bit



Another replacement

- What really happens: Measure a POVM, announce a function of the result
- Replacement: Do measurement in two steps
  1. An incomplete measurement to measure what is to be announced
     → check entanglement and symmetric extension
  2. Complete the measurement to get a partially secret bit



Outline

QKD, thresholds and upper bounds

Announcement measurements

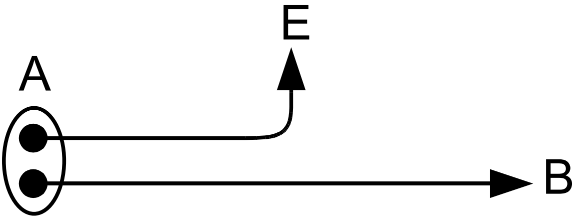
Examples

Wrapping up...

BB84 apparatus – different siftings

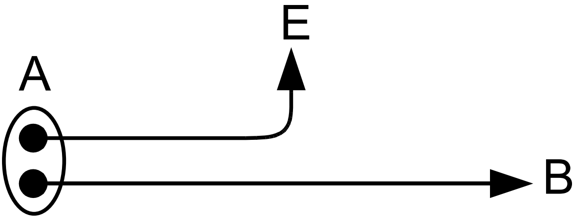
- Real POVM elements: $\{|0\rangle\langle 0|, \quad |+\rangle\langle +|, \quad |1\rangle\langle 1|, \quad |-\rangle\langle -|\}$
- BB84-announcement:
  $\{|0\rangle\langle 0| + |1\rangle\langle 1|, \quad |+\rangle\langle +| + |-\rangle\langle -|\} = \{I, I\}$
- SARG-announcement:
  - Alice: $\{|0\rangle\langle 0| + |+\rangle\langle +|, \quad |+\rangle\langle +| + |1\rangle\langle 1|, \quad \ldots\}$
  - Bob (corresponding to Alice's first outcome):
    $\{|1\rangle\langle 1| + |-\rangle\langle -|, \quad |0\rangle\langle 0| + |+\rangle\langle +|\}$

BB84/SARG with two photons



- BB84-announcement:
  $\rho^{\text{out}} = U\sqrt{F}\rho^{\text{in}}\sqrt{F}U^{\dagger} = \frac{1}{2}(|00\rangle\langle 00| + |11\rangle\langle 11|)$
- SARG-announcement:
  $\rho^{\text{out}} = U\sqrt{F}\rho^{\text{in}}\sqrt{F}U^{\dagger} = 0.85|\Phi^{+}\rangle\langle\Phi^{+}| + 0.15|\Phi^{-}\rangle\langle\Phi^{-}|$

BB84/SARG with two photons



- BB84-announcement:
  $\rho^{\text{out}} = U\sqrt{F}\rho^{\text{in}}\sqrt{F}U^\dagger = \frac{1}{2}(|00\rangle\langle 00| + |11\rangle\langle 11|)$
- SARG-announcement:
  $\rho^{\text{out}} = U\sqrt{F}\rho^{\text{in}}\sqrt{F}U^\dagger = 0.85|\Phi^+\rangle\langle\Phi^+| + 0.15|\Phi^-\rangle\langle\Phi^-|$

Chau scheme

Postprocessing scheme with highest known threshold

- Procedure:
  - Take two bits
  - Announce their parity
  - Keep one bit if equal parity for A and B
- Result:
  - Low enough noise: Destroys symmetric extension
  - Higher noise: Keeps symmetric extension, but does not destroy (all) entanglement

Outline

Further complications

- What if we don't know the complete effective state?
- Can find entanglement witnesses to still verify entanglement
- Can restrict those witnesses to those that will witness entanglement *after* a particular announcement

Summary

- By a replacement we can analyze the effective quantum states after announcement
- A useful announcement is one that gets rid of symmetric extension
- We haven't found any new ones yet...