UNIVERSITY OF CAMBRIDGE

Centre for Quantum Computation

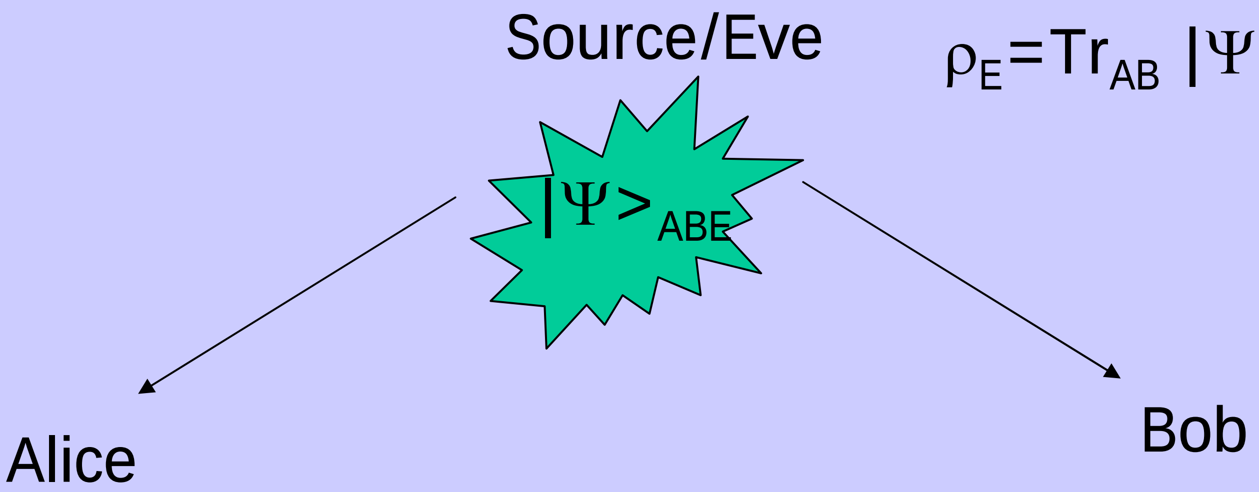
# A generic security proof for quantum key distribution

**Matthias Christandl**

**joint work with**

**Artur Ekert and Renato Renner**

# The Setting




$\rho_E = Tr_{AB} \, |\Psi\rangle\langle\Psi|$

$\rho = Tr_E \, |\Psi\rangle\langle\Psi|$

- Entanglement-based quantum key distribution (Ekert 1991)
- Alice and Bob perform (perfect) measurements:
  - on individual quantum states
  - independently of each other
- Alice and Bob perform one-way classical post-processing over authenticated channel
- Eve keeps the purification of quantum state (most general situation)

# Two Remarks

- Some prepare- and measure protocols can be analysed in this scenario. (E.g. BB84)
- We want to find a lower bound on the secret key rate in this scenario.

# Security of QKD

- Different ways of proving security (positive secret key rate)
- Mayers 1996 proved security of BB84
- Quantum privacy amplification (Deutsch *et al.* 1996) allows for extraction of singlets that yield secure key (need for QC ☹)
- Most security proofs build on the idea of entanglement distillation (e.g. Lo and Chao, Shor and Preskill, Gottesman and Lo, Tamaki, Koashi and Imoto)

# This Work

A new type of security proof

- that does not rely on entanglement distillation
- in contrast depends on the size of Eve’s memory

- that is applicable to a wide class of protocols

# The Protocol

Alice | $\rho \in \mathcal{B}((H_A \otimes H_B)^{\otimes N})$ | Bob

$H_A^{\otimes N}$ | | $H_B^{\otimes N}$

Tomography $\rightarrow \sigma \in \mathcal{B}(H_A \otimes H_B)$ ⟷ Tomography $\rightarrow \sigma \in \mathcal{B}(H_A \otimes H_B)$

POVM $\rightarrow X^{N'}$

POVM $\rightarrow Y^{N'}$

→ Information Reconciliation →

$X'^{N'}$

$K = F(X^{N'})$ → Privacy Amplification → $K' = F(X'^{N'})$

# Analysis

- Note: Eve has a state $\rho_E = Tr_{AB} |\Psi><\Psi|$
- Idea: 1) Bound the size of Eve's memory

  2) Apply the result on quantum memory (9 am)

  (König, Maurer and Renner, 2003)
- In the case of $\rho = \rho'^{\otimes N}$
- Eve holds a purification $\rho_E$ of $\rho$

  $\rightarrow S(\rho_E) = S(\rho) = N\,S(\rho') \approx N\,S(\sigma)$

  $\rightarrow$ Eve can encode her information into $\approx N\,S(\sigma)$ qubits
- Information sent in IR equals $\approx N\,H(X|Y)$
- Extractable key length $s \approx N\,(\max_{POVM} I(X;Y) - S(\sigma))$

# Comments, Applications …

- Proof for $\rho^{\otimes N} \in \mathcal{S}((H_A \otimes H_B)^{\otimes N})$

- General situation is work in progress…

- Generic proof for quantum key distribution
- Not based on entanglement distillation
- Applies to some protocols that are not tomographically complete
- Applies to prepare and measure protocols, e.g. BB84, 6-state, and entanglement-based protocols