Introduction to Quantum Key Distribution

Matthias Christandl

Fakultät für Physik
Ludwig-Maximilians-Universität München

January 2010

Overview

- Introduction
- Quantum Key Distribution
- Security Proof

Introduction

- What is information?
  - A mathematical concept describing "knowledge". Basic unit is the bit 0 / 1.
  - A physical concept $0 \widehat{=}$ 

and $1 \widehat{=}$ 

Introduction

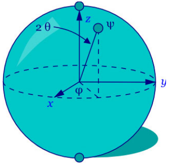
- What is information?
  - A mathematical concept describing "knowledge". Basic unit is the bit 0 / 1.
  - A physical concept $0 \hat{=}$ 

and $1 \hat{=}$ 

- The world is not made up of light switches, the world is made up of atoms and photons
- Atoms and photons are described by quantum mechanics
- The spin of an atom describes the information we have about it 

Introduction

- spin-$\frac{1}{2}$ system: points on the sphere

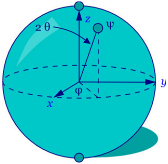


$$\begin{pmatrix} \cos\theta \\ e^{i\varphi}\sin\theta \end{pmatrix} = \cos\theta|$$  $$\rangle + e^{i\varphi}\sin\theta|$$  $$\rangle$$

- unit of information is the quantum bit or "qubit"

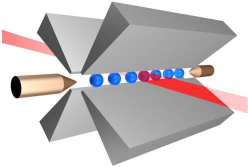
Introduction

- spin-$\frac{1}{2}$ system: points on the sphere

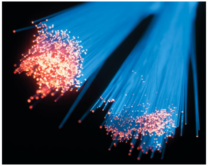


$$\begin{pmatrix} \cos\theta \\ e^{i\varphi}\sin\theta \end{pmatrix} = \cos\theta\,|$$  $$\rangle + e^{i\varphi}\sin\theta\,|$$  $$\rangle$$

- unit of information is the quantum bit or "qubit"
- we can manipulate and transmit qubits

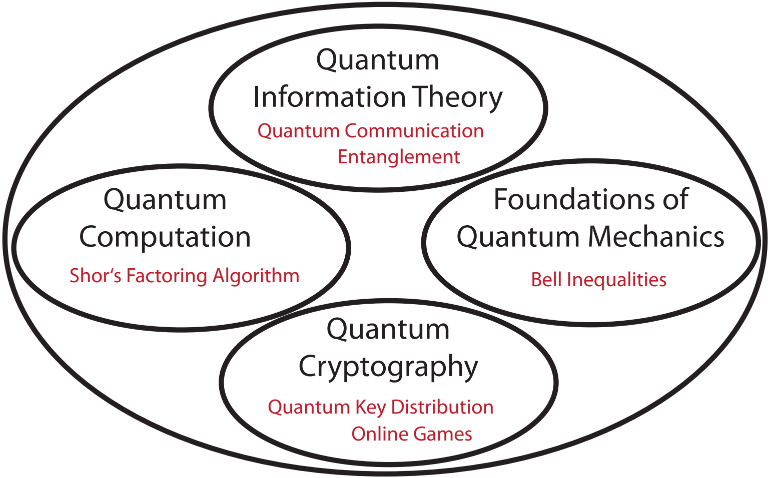


ion trap



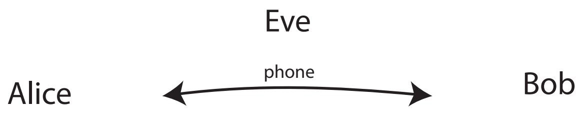
optical fibre

Quantum Information Science



Quantum Key Distribution

- Alice und Bob want to communicate in secrecy, but their phone is tapped.



Quantum Key Distribution

- Alice und Bob want to communicate in secrecy, but their phone is tapped.

Eve

Alice ⟷ phone ⟷ Bob

- If they share key (string of secret random numbers),

Alice   Eve   Bob

message
+key
----
cipher

→

cipher
- key
----
message

- cipher is random and message secure (Vernam, 1926)

Quantum Key Distribution

- Alice und Bob want to communicate in secrecy, but their phone is tapped.

Eve

Alice $\xleftrightarrow{\text{phone}}$ Bob

- If they share key (string of secret random numbers),

Alice  Eve Bob

```
  010 101 101
 +101 110 001
 ------------
  111 011 100   ──────────►   111 011 100
                             +101 110 001
                             ------------
                              010 101 101
```

- cipher is random and message secure (Vernam, 1926)

Quantum Key Distribution

- key is as long as the message

  Shannon (1949): this is optimal ☹

  secret communication $\hat{=}$ key distribution

Quantum Key Distribution

- key is as long as the message

  Shannon (1949): this is optimal ☹

  secret communication $\hat{=}$ key distribution
- possible key distribution schemes:

Quantum Key Distribution

- key is as long as the message

  Shannon (1949): this is optimal ☹

  secret communication $\hat{=}$ key distribution
- possible key distribution schemes:
  - Alice and Bob meet $\Rightarrow$ impractical

Quantum Key Distribution

- key is as long as the message

  Shannon (1949): this is optimal ☹

  secret communication $\hat{=}$ key distribution
- possible key distribution schemes:
  - Alice and Bob meet $\Rightarrow$ impractical
  - Weaker level of security
    - assumptions on speed of Eve's computer (public key cryptography)
    - assumptions on size of Eve's harddrive (bounded storage model)

Quantum Key Distribution

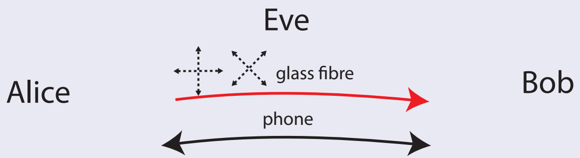
- key is as long as the message

  Shannon (1949): this is optimal ☹

  secret communication $\hat{=}$ key distribution
- possible key distribution schemes:
  - Alice and Bob meet $\Rightarrow$ impractical
  - Weaker level of security
    - assumptions on speed of Eve's computer (public key cryptography)
    - assumptions on size of Eve's harddrive (bounded storage model)
  - Use quantum mechanical effects (Bennett & Brassard 1984, Ekert 1991)

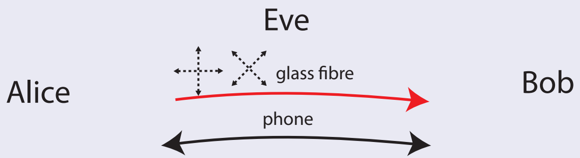
Quantum Key Distribution

prepare & measure (Wiesner 1970's, Bennett & Brassard 1984)



Quantum Key Distribution

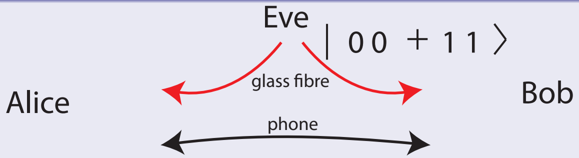
prepare & measure (Wiesner 1970's, Bennett & Brassard 1984)



Security guaranteed by uncertainty principle

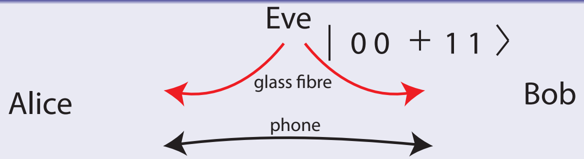
- Alice sends eigenstates of σ_z or σ_x.
- Bob measures observable σ_z or σ_x.
- They tell each other the observable, but not the result.
- They should obtain the same result when they used the same observable $\Rightarrow$ key
- If Eve measures in the wrong observable, they have an error with probability $\frac{1}{2}$, since $[\sigma_z, \sigma_x] \neq 0$.

entanglement-based (Ekert 1991)



Quantum Key Distribution

entanglement-based (Ekert 1991)



Security guaranteed by monogamy of entanglement

- Alice and Bob check (Bell inequality):
  $|\psi\rangle_{ABE} \stackrel{?}{=} \frac{1}{\sqrt{2}}(|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B)|\phi\rangle_E.$
  - If YES: Eve does not know their measurement results. Results are random $\Rightarrow$ key
  - If NO: they abort the protocol.

Quantum Key Distribution

- Entangled state of two qubits $\frac{1}{\sqrt{2}}(|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B)$

Quantum Key Distribution

- Entangled state of two qubits $\frac{1}{\sqrt{2}}(|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B)$
- New basis

$$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \quad |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

- easy calculation

$$\frac{1}{\sqrt{2}}(|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B) = \frac{1}{\sqrt{2}}(|+\rangle_A|+\rangle_B + |-\rangle_A|-\rangle_B)$$

Quantum Key Distribution

- Entangled state of two qubits $\frac{1}{\sqrt{2}}(|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B)$
- New basis

$$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \quad |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

- easy calculation

$$\frac{1}{\sqrt{2}}(|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B) = \frac{1}{\sqrt{2}}(|+\rangle_A|+\rangle_B + |-\rangle_A|-\rangle_B)$$

- If Alice and Bob measure observable $\sigma_z \Rightarrow$ same result
- If Alice and Bob measure observable $\sigma_x \Rightarrow$ same result

Quantum Key Distribution

- Entangled state of two qubits $\frac{1}{\sqrt{2}}(|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B)$
- New basis

$$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \quad |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

- easy calculation

$$\frac{1}{\sqrt{2}}(|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B) = \frac{1}{\sqrt{2}}(|+\rangle_A|+\rangle_B + |-\rangle_A|-\rangle_B)$$

- If Alice and Bob measure observable $\sigma_z \Rightarrow$ same result
- If Alice and Bob measure observable $\sigma_x \Rightarrow$ same result
- Converse is true, too:
  - same measurement result $\Rightarrow$ they have state $\frac{1}{\sqrt{2}}(|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B)$
  - Alice and Bob can test whether or not they have the state $\frac{1}{\sqrt{2}}(|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B)$!

Quantum Key Distribution

- Assume that Alice and Bob have the state $|\phi\rangle_{AB} = \frac{1}{\sqrt{2}}(|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B)$ and measure in the same basis.
- Can someone else guess the result?

Quantum Key Distribution

- Assume that Alice and Bob have the state
  $|\phi\rangle_{AB} = \frac{1}{\sqrt{2}}(|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B)$
  and measure in the same basis.
- Can someone else guess the result?
- No! The measurement result is secure!
  - Total state of Alice, Bob and Eve

    $$|\psi\rangle_{ABE} = |\phi\rangle_{AB} \otimes |\phi\rangle_E,$$

  - because Alice and Bob have a pure state
  - Eve is not at all correlated with Alice and Bob!
  - Monogamy of entanglement
  - Try: $|\psi\rangle_{ABE} = \frac{1}{\sqrt{2}}(|0\rangle_A|0\rangle_B|0\rangle_E + |1\rangle_A|1\rangle_B|1\rangle_E)$
    $\rho_{AB} = \frac{1}{2}(|0\rangle_A|0\rangle_B\langle 0|_A\langle 0|_B + |1\rangle_A|1\rangle_B\langle 1|_A\langle 1|_B)$
    different from
    $|\phi\rangle\langle\phi|_{AB} = \frac{1}{2}(|0\rangle_A|0\rangle_B\langle 0|_A\langle 0|_B +$
    $|1\rangle_A|1\rangle_B\langle 0|_A\langle 0|_B + |0\rangle_A|0\rangle_B\langle 1|_A\langle 1|_B + |1\rangle_A|1\rangle_B\langle 1|_A\langle 1|_B)$

The Quantum Key Distribution Protocol

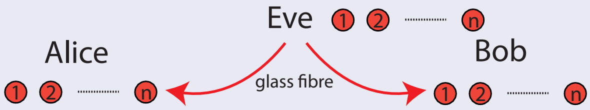
Distribution

The Quantum Key Distribution Protocol

Distribution

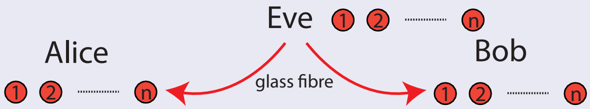
The Quantum Key Distribution Protocol

Distribution

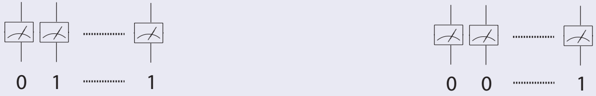


The Quantum Key Distribution Protocol

Distribution

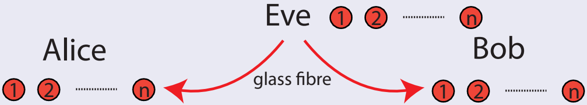


Measurement with σ_x or σ_z

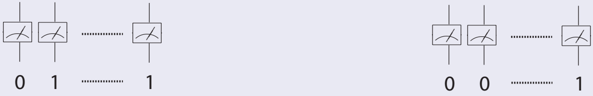


The Quantum Key Distribution Protocol

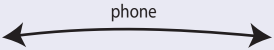
Distribution



Measurement with σ_x or σ_z

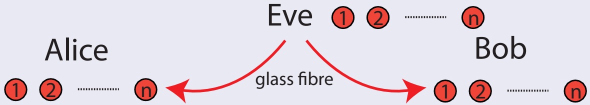


Error-free? $|\phi\rangle_{AB} \stackrel{?}{=} \frac{1}{\sqrt{2}}(|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B)$

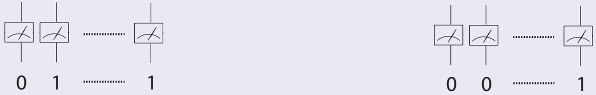


The Quantum Key Distribution Protocol

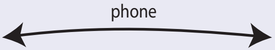
Distribution



Measurement with σ_x or σ_z



Error-free? $|\phi\rangle_{AB} \stackrel{?}{=} \frac{1}{\sqrt{2}}(|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B)$



If YES: key. If NO: no key

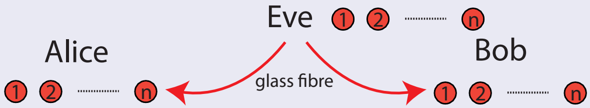
Quantum Key Distribution

- entanglement $\Rightarrow$ key
- key $\Rightarrow$ perfectly secure communication
- not possible with classical physics
- future (quantum) technology!

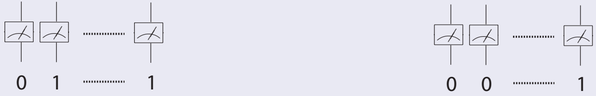
Security Proof

The Quantum Key Distribution Protocol

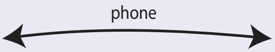
Distribution



Measurement with σ_x or σ_z



Error-free? $|\phi\rangle_{AB} \stackrel{?}{=} \frac{1}{\sqrt{2}}(|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B)$



If YES: key. If NO: no key

Security Proof

- Honest Eve would distribute

$$|\Psi\rangle^n_{ABC} = |\psi\rangle^{\otimes n}_{ABE} \qquad \text{bits are independent}$$

$$|\psi\rangle_{ABE} = |\phi\rangle_{AB} \otimes |\phi\rangle_E \qquad \text{Eve knows nothing}$$

$$|\phi\rangle_{AB} = \frac{1}{\sqrt{2}}(|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B) \qquad \text{bits are random}$$

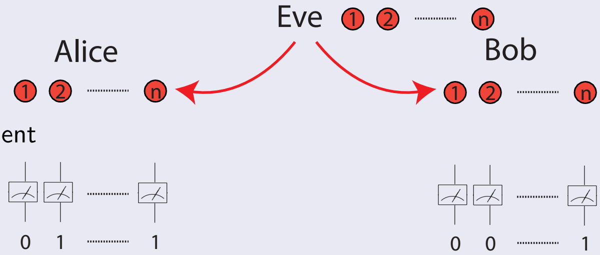
- Alice and Bob need to test whether Eve is honest or not.

Security Proof

- If Eve sends states of the form $|\Psi\rangle^n_{ABC} = |\psi\rangle^{\otimes n}_{ABE}$
- Alice and Bob test (on a subset): Are the pairs are of the form $|\phi\rangle_{AB} = \frac{1}{\sqrt{2}}(|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B)$
  i.e. is the data error-free ?
- If YES, standard statistical analysis implies
  - (almost) all remaining triples are of the form $|\phi\rangle_{AB} \otimes |\phi\rangle_E$
    $\Rightarrow$ resulting bits are (almost) identical and random
    $\Rightarrow$ Eve has (almost) no information about bits
  - Alice and Bob perform error correction
  - Alice and Bob delete a few random bits $\Rightarrow$
    Eve has no information about remaining bits
    (privacy amplification)
    $\Rightarrow$ key
- If NO, abort the protocol

The Protocol

Distribution $|\Psi\rangle^n_{ABC} = |\psi\rangle^{\otimes n}_{ABE}$



Measurement

Error Estimation ↔ compare subset

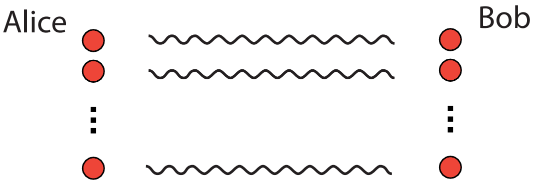
$$|\phi\rangle_{AB} \stackrel{?}{=} \frac{1}{\sqrt{2}}(|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B)$$

NO: Abort protocol

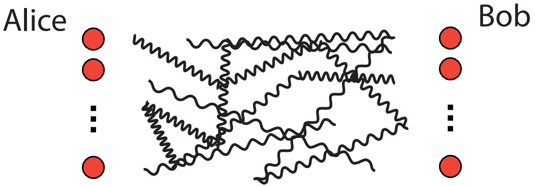
YES: 1 0 ⋯ 1 ↔ error correction & privacy amplification ↔ 1 0 ⋯ 1

Security Proof

- Proof works as long as $|\Psi\rangle_{ABC}^{n} = |\psi\rangle_{ABE}^{\otimes n}$.

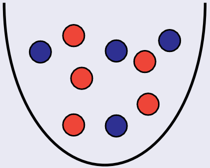


- But why should Eve prepare such a state? Why not the following?



De Finetti Theorem (Diaconis and Freedman, 1980)

Drawing balls from an urn with or without replacement results in almost the same probability distribution.



If k are drawn out of n, then

$$||P^k - \sum_i p_i Q_i^{\times k}||_1 \leq const \frac{k}{n}.$$

Security Proof

Quantum generalisations have been obtained by Størmer, Hudson & Moody, and Werner et al.. ($n = \infty$)

Quantum De Finetti Theorem

Ch., König, Mitchison, Renner, Comm. Math. Phys. 273, 473498 (2007)

Let ρ^n be a permutation-invariant state $\pi\rho\pi^{-1} = \rho$, then

$$||\rho^k - \sum_i p_i \sigma_i^{\otimes k}||_1 \leq const \frac{k}{n}$$

- $const = 4d^2$
- d dependence is necessary
- classically, k^2/n bound exists

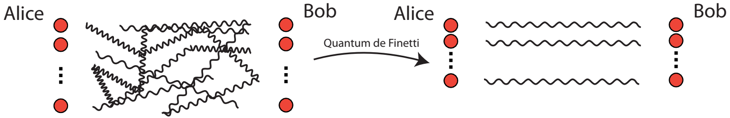
Proof sketch

- reduce problem to the Bosonic case $\pi\rho = \rho$, for all $\pi \in S_n$
- ρ lives on $\mathrm{Sym}^n(\mathbb{C}^d) \subset \mathrm{Sym}^k(\mathbb{C}^d) \otimes \mathrm{Sym}^{n-k}(\mathbb{C}^d)$
- measurement with $SU(d)$ coherent states $|\phi\rangle^{\otimes n} = |\phi\rangle^{\otimes k} \otimes |\phi\rangle^{\otimes n-k}$
- post-measurement on k particles: $\rho^k_{post} = \int \mu(\phi)|\phi\rangle\langle\phi|^{\otimes k}$
- gentle measurement $\rho^k \approx \rho^k_{post}$ (error k/n).

generalises to arbitrary irreducible representations of $SU(d)$.

Security Proof

- Alice and Bob select a random sample of pairs (after pairs have been distributed!)



$\Rightarrow$ can use proof from before (tensor product)
$\Rightarrow$ proof of the security of Quantum Key Distribution!

Security Proof

- Closer look: deviation from perfect key (due to quantum de Finetti theorem)
$$\epsilon \approx k/n$$
- n: number of pairs that Eve distributed
- k: number of bits of key

Security Proof

- Closer look: deviation from perfect key (due to quantum de Finetti theorem)

$$\epsilon \approx k/n$$

- n: number of pairs that Eve distributed
- k: number of bits of key
- key rate $r \approx k/n \approx \epsilon \approx 0 \Rightarrow$ not good enough
- need replacement for de Finetti theorem
- Renner's exp. de Finetti theorem, involved, non-optimal

Security Proof

Post-selection Technique

Ch., König, Renner, Phys. Rev. Lett. 102, 020504 (2009)

- Idea: Compare actual protocol with an ideal protocol (which produces perfect key)
- Theorem about permutation-covariant maps, rather than permutation-invariant states.

Post-selection Technique

Ch., König, Renner, Phys. Rev. Lett. 102, 020504 (2009)

- Idea: Compare actual protocol with an ideal protocol (which produces perfect key)
- Theorem about permutation-covariant maps, rather than permutation-invariant states.

- In QKD:
  - $r \approx k/n \approx 1 - \delta$ and $\epsilon \approx \exp(-\delta^2 n)$
  - optimal parameters
  - relevant in current experiments (since $n \approx 10^5$)
  - Eve's best attack $|\Psi^n_{ABE}\rangle = |\psi_{ABE}\rangle^{\otimes n}$
  - conceptual and technical simplification of security proofs
- Other applications: Quantum Reverse Shannon Theorem

Berta, Ch. and Renner, arXiv:0912.3805