Dienstag, 21. Juni 2016 19:00

# Lecture 23/06/2016

## 16 Quantum communication

### 16.1. Quantum key distribution

#### 16.1.1 Cryptography

Alice wants to send secret message to Bob:

⇒ modern cryptography

publicly known algorithm for encoding ($\hat{E}$) and decoding ($\hat{D}$) + shared (secret) key ($k$)

$\hat{E}_k(M) = C \quad \rightarrow \quad \hat{D}_k(C) = M$

$M$ ... plaintext message

$C$ ... encrypted message

- Examples (see slides, Cesar & one time pad)

One time pad:

- Message and key have same length
- add key to message
- Claude-Shannon (1949): is absolutely secure, if key is fully random and only used once

⇒ Communication is secure if there is a secure way to exchange / generate a secret key

Solution:

- public-key-method: security not proven

- public-key-method: security not proven
- Quantum-key distribution

## 16.1.2 Quantum-key-distribution

**No-cloning theorem:**
it is impossible to perfectly copy an unknown quantum state

Proof: We assume there is an operation $\hat{U}$ which copies an arbitrary quantum state:

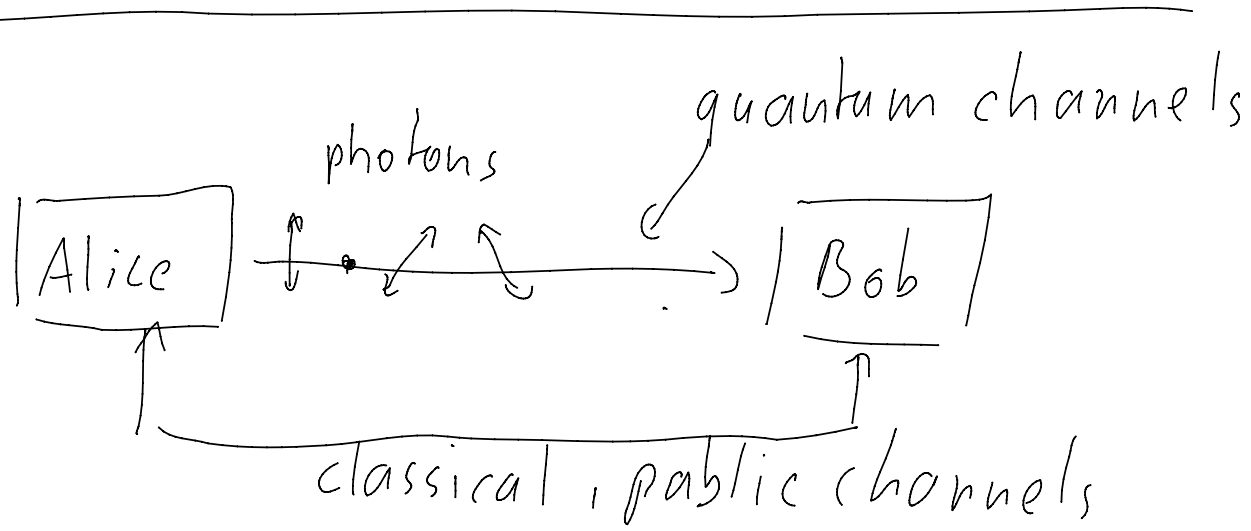
$$\hat{U}\,|\phi\rangle|0\rangle \longrightarrow |\phi\rangle|\phi\rangle$$
$$\hat{U}\,|4\rangle|0\rangle \longrightarrow |4\rangle|4\rangle$$

$$\Rightarrow \hat{U}\,[|\phi\rangle + |4\rangle]|0\rangle \longrightarrow |\phi\rangle|\phi\rangle + |4\rangle|4\rangle$$

($\hat{U}$ linear operator)

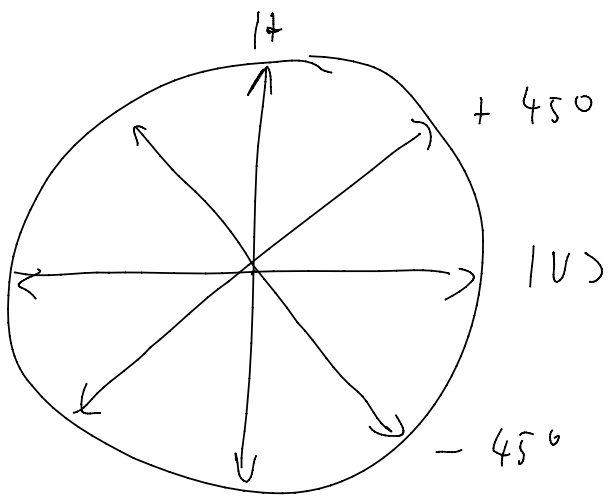
$$\neq (|\phi\rangle + |4\rangle)(|\phi\rangle + |4\rangle) \quad \lightning$$

**BB84-Protocoll (Benett-Brusard)**




- Alice and Bob want to create a secret key
  ⇒ Alice sends Bob a sequenz of photons that are randomly prepared in one of the 4 pol. states $|H\rangle$, $|V\rangle$, $|+45°\rangle$, $|-45°\rangle$

14




- For each photon Bob chooses randomly the measurement basis $|H\rangle/|V\rangle$ or $\pm 45°$
- After the measurements: (not the result!)
  - Bob tells Alice in which bases he measured each photon via public channel (newspaper, telephone, internet...).
  - Alice tells Bob, in which cases they coincide with the basis in which Alice's photon was prepared

  ⇒ For these cases Bob's polarization measurement results are identical to the state Alice prepared

  ⇒ they share a common "string" of photon-polarizations

  ⇒ assign bit value "0" to $|H\rangle, |+45\rangle$ and "1" to $|V\rangle, |-45\rangle$

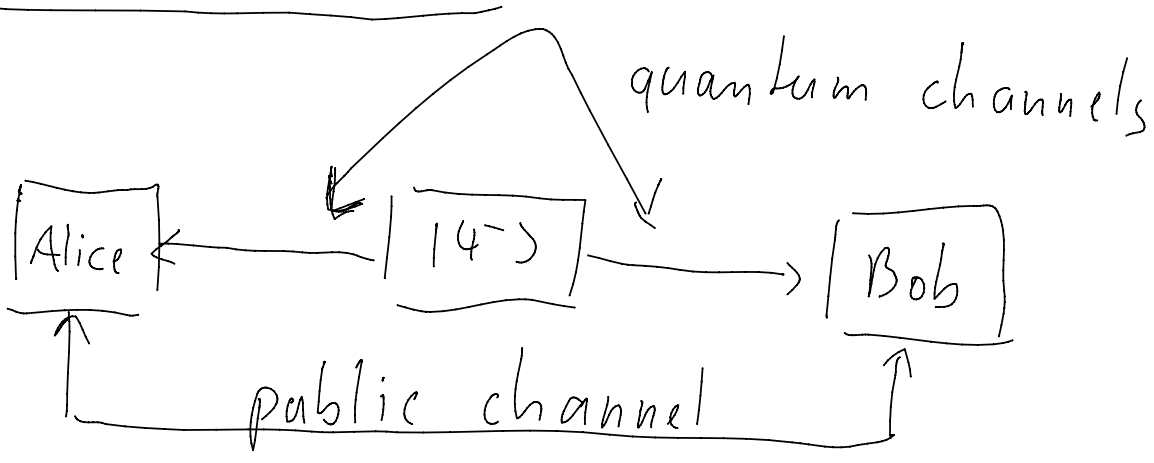
  ⇒ secret key

Checking for Eavesdropper (Eve)

Eve has to intercept the photons (e.g.

- Eve has to intercept the photons from Alice, measure them and then send them to Bob
  => introduces errors, i.e. Bob's results are not identical to the state prepared by Alice
- to check for Eve, Alice and Bob compare a subset of the key (publicly) for errors
  - error rate too high => Eve tried to intercept communication
  => key is rejected

## Ekert - Protocol




- photon pair source, prepares e.g. $|4^-\rangle$ Bell-state. and sends one photon to Alice and one to Bob
- Alice measures in H/V, +22,5° and 45°-basis
  Bob in -22,5°, H/V, +22,5° basis
  => key generation similar to BB84
- to check for Eve, Alice + Bob take a subset

- Check for Eve, Alice + Bob take a subset of photons and check if their measurement results Bell's inequality

Error correction, Privacy amplification
(see slides)