PHYSIK

TECHNISCHE UNIVERSITÄT
KAISERSLAUTERN

Quantum cryptography

Dennis Breu

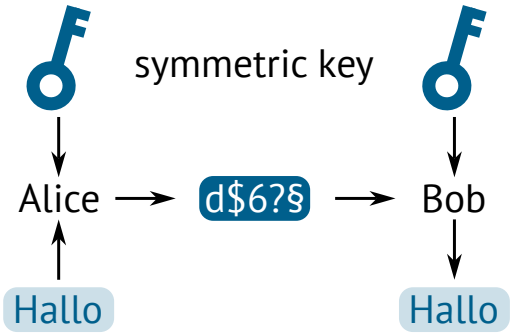
Hauptseminar II
Physics Department
TU Kaiserslautern

8. December 2022

Cryptography basics

Cryptography classes

Symmetric Cryptography

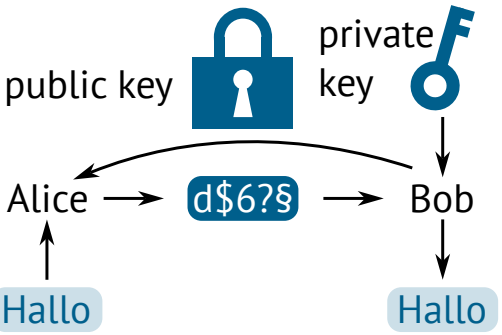


- Key encrypts and decrypts data

✗ Difficult key distribution

✓ Resistant against quantum algorithms

Asymmetric Cryptography



- Public key encrypts
- Private key decrypts

✓ Easy key distribution

✗ Vulnerable to quantum algorithms

One-time-pad encryption

First proposed by Gilbert Vernam of AT&T in 1926

Basic Idea:

1. Alice generate random key and shares it with Bob
2. Alice adds key to the message to encrypt it
3. Alice send Bob scrambled massage
4. Bob adds key to the message to decrypt it

Key can only be uses once
Provably secure because of randomness

01111	Message	Encryption
00100	Key	
01011	Scrambled message	

01011	Scrambled message	Decryption
00100	Key	
01111	Message	

RSA Encryption

Developed by Rivest, Shamir and Adleman in 1977

$$\mathrm{E} = \mathrm{D}^{\mathrm{e}} \mod \mathrm{n}$$
$$\mathrm{D} = \mathrm{E}^{\mathrm{d}} \mod \mathrm{n}$$

Where is the vulnerability?

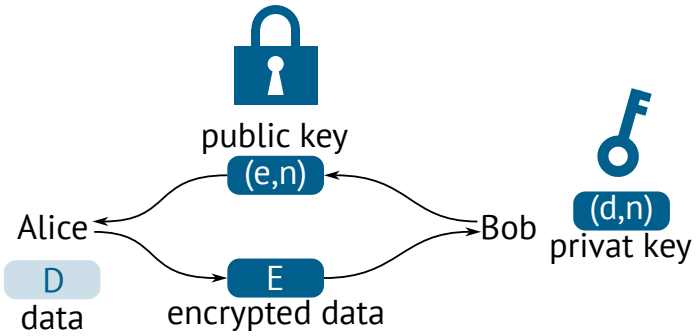
In the key generation!

1. Pick random large prime numbers q and p
2. $n = q \cdot p$

...

Prime factorization is an NP-Problem

$\Rightarrow$ **Shor's algorithm on quantum computer**



Modulus for RSA 2048

25550909340115004306969099256841041521403931134831367441037920936953172144238782143891862065143647520840758264764510439766942183382106261867198976994572443321931920272461817333800987851188720295545478631020462604164785318984177719580486894822464147344861380523296735111420755587700852810843787957559283406178035288932159314859944178663058185892610532765020716303660594447831618987107632648959313527071275211791343095891809469628598885664071873208718902829852701778758257945069092172910954646629609703304173354257793464081968956093052230868341072714111083745979088171270893581654318338992309744153206195632891473910363

Problems and Solutions

So symmetric Cryptography after all?

But how do we distribute keys?

Quantum key distribution

Useful feature of quantum states

- Objective randomness
  - $\Rightarrow$ Impossible to crack using algorithms
- Disturbed if measured unless the measurement is compatible
- No cloning theorem
  - $\Rightarrow$ Man in the middle attacks can be recognised
- Entanglement?

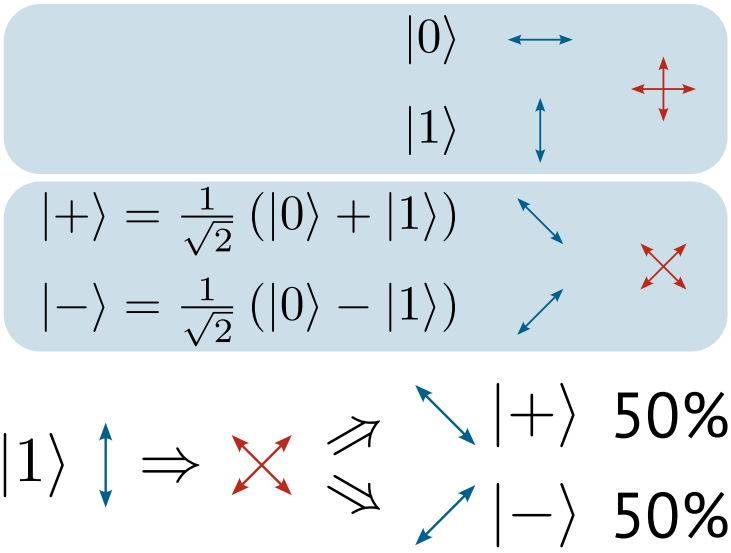
BB84

Developed in 1984 by Charless Bennett and Gilles Brassard

Basic Ideas:

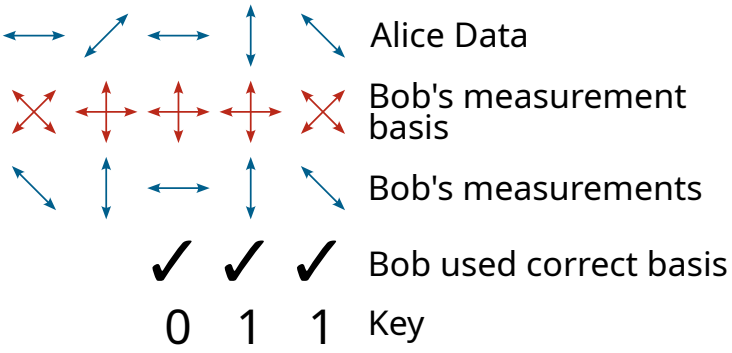
- Encode key via polarisation of single photons
- Basis of polarisation is chosen randomly
- Eavesdropper doesn't know the basis

$\Rightarrow$ If measured wrongly, the polarisation is changed



Example of a BB84 QKD

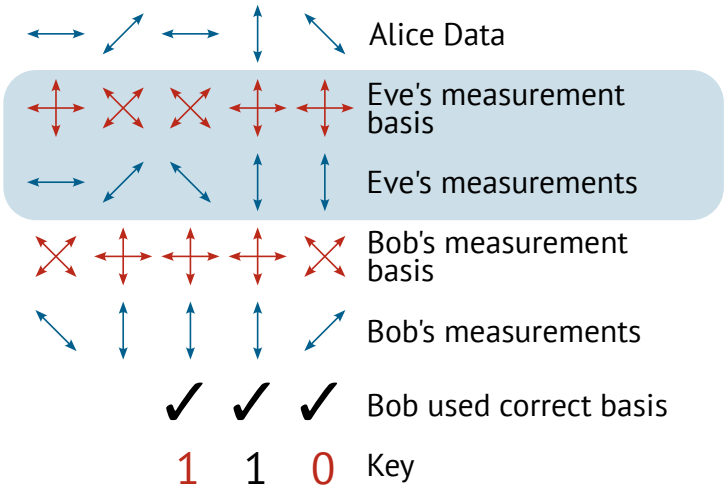
1. Alice sends a random key randomly encoded in the 0° or 45° basis
2. Bob randomly measures in the 0° or 45° basis
3. Alice and Bob publicly compare their measuring basis
4. Bits with the same basis are kept



Eavesdropping detection in the BB84 protocol

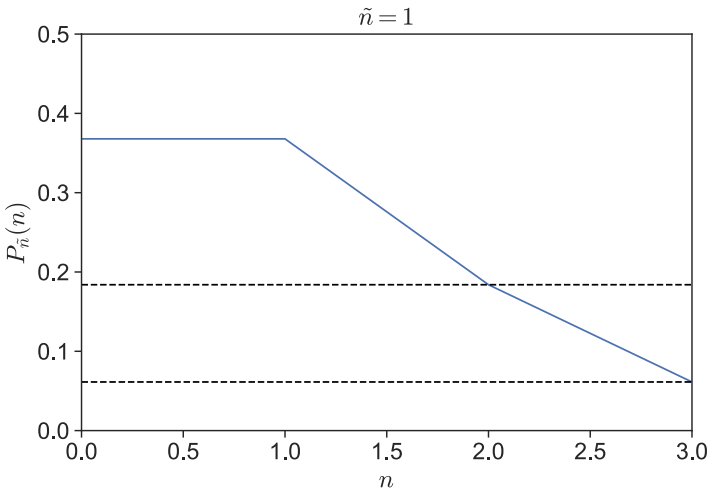
How do we detect eavesdropping?

By comparing part of the key!



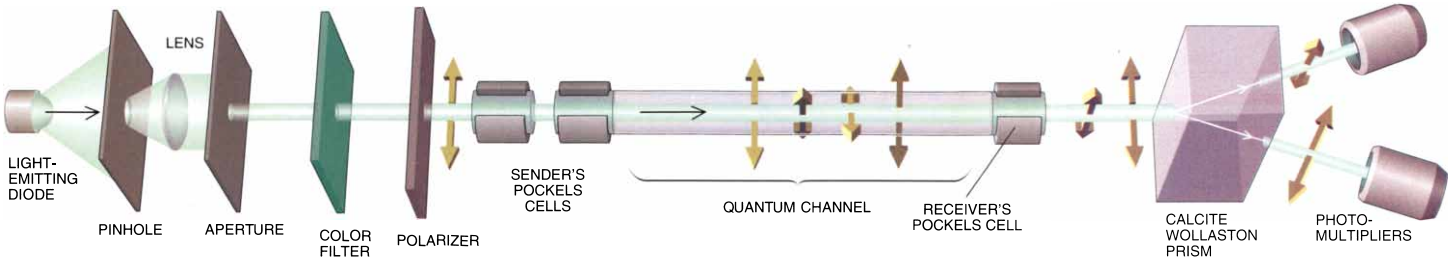
Problems in the real world

- Coherent light sources
  - ⇒ Hard to send single photons
  - ⇒ Beam splitting attacks and measuring of both axis
- Dark counts
- Bit flips
- Losses
  - ⇒ False detection of eavesdropper
- High trough put is needed
  - ⇒ Key distillation / privacy amplification



Experiments

IBM prototype



Bennett, Brassard et. al. Scientific American , Vol. 267, No. 4 (OCTOBER 1992), pp. 50-57

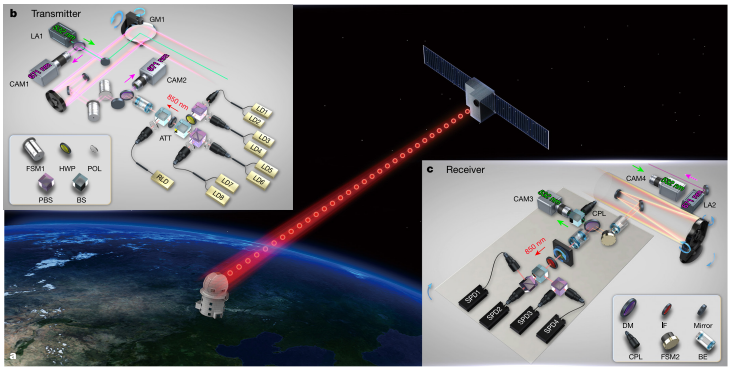
Distance only 34cm $\Rightarrow$ Losses increase exponential

Today 144km are possible

Satellite-to-ground QKD

Chinese Micius Satellite

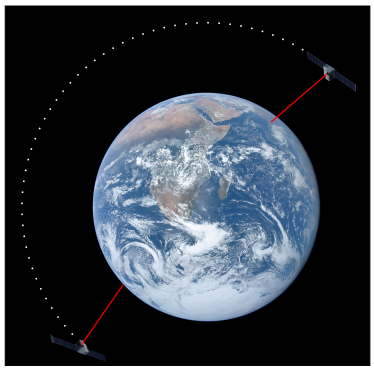
- launched 16 August 2016
- uses decoy-state BB84 QKD transmitter
- since September 2016 QKD to Xinglong on a regular basis



Liao, SK., Cai, WQ., Liu, WY. et al. Nature 549, 43–47 (2017)

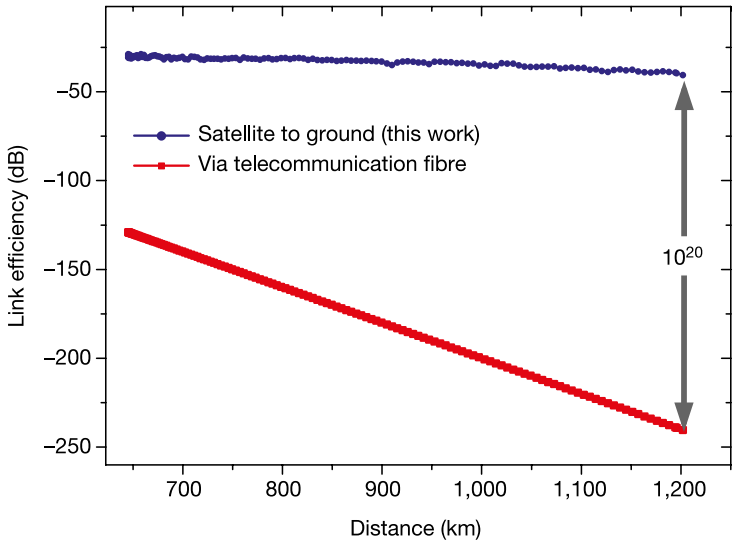
Advantages of Satellites

- Effectiv thickness of atmosphere only 10km
- Connect two arbitrary ground stations
- Hard to temper with . . . **but not impossible**



https://de.wikipedia.org/wiki/Erde (modified)

Last accessed:02.12.22 17:50



Liao, SK., Cai, WQ., Liu, WY. et al. Nature 549, 43–47 (2017)

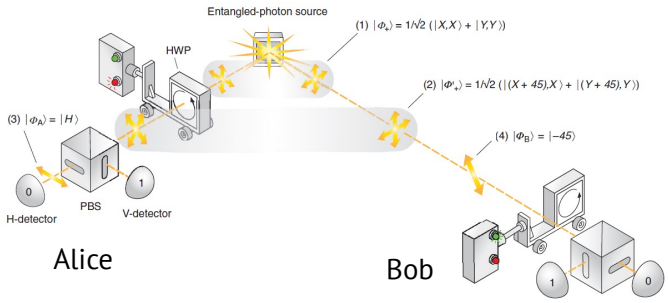
Quantum-entanglement-based QKD

Quantum-entanglement-based Protocol

Proposed by Artur Ekert in 1991

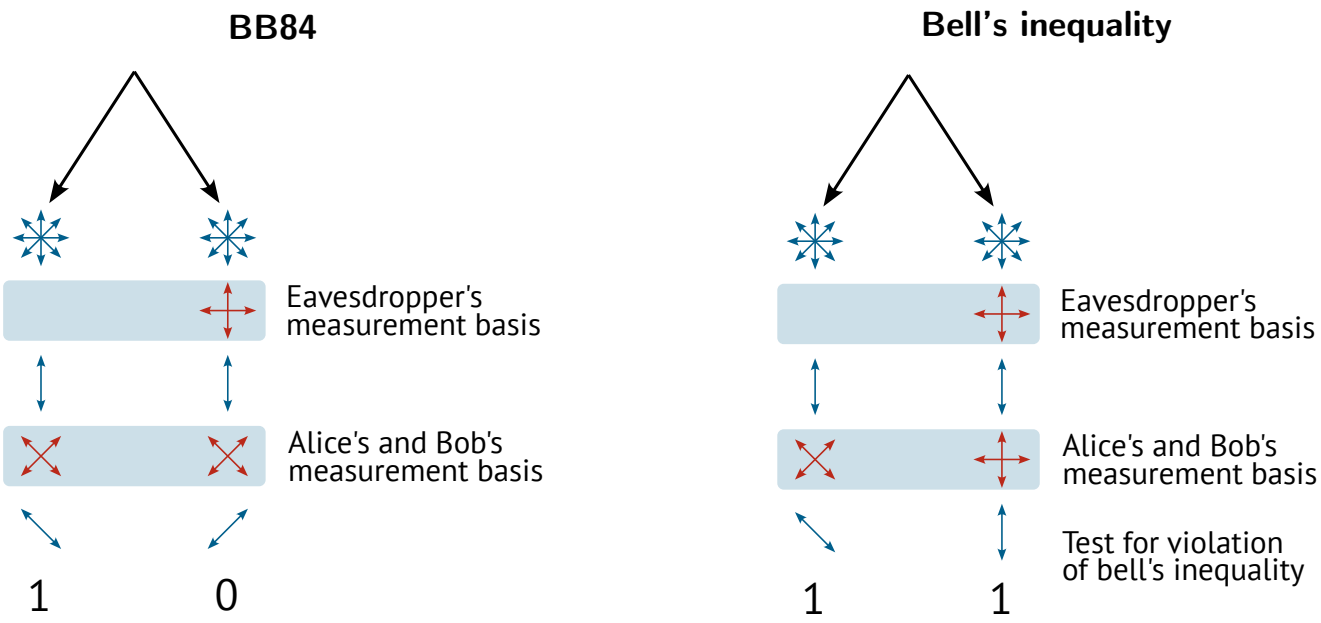
1. Create entangled photon pairs
2. Alice and Bob randomly choose measuring basis
3. Alice and Bob publicly compare their measuring basis
4. Bits with the same basis are kept

The key distributer, doesn't know the key!

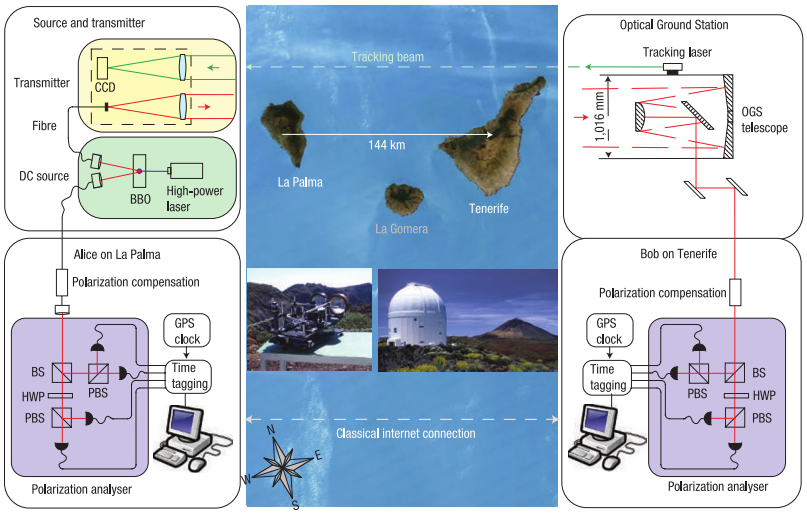


Widera, Quantum Optics Lecture 23, July 2022

Eavesdropper detection in Entanglement based Protocol

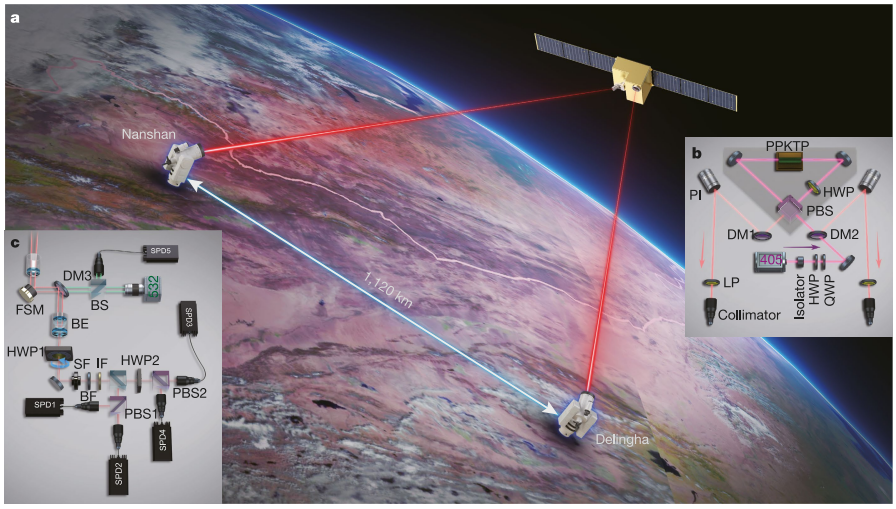


Entanglement-based quantum communication over 144km



Ursin, R., Tiefenbacher, F., Schmitt-Manderbach, T. et al. Nature Phys 3, 481–486 (2007)

Entanglement-based secure quantum cryptography over 1.120 kilometres

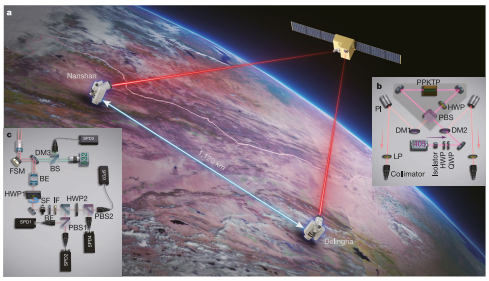


Yin, J., Li, YH., Liao, SK. et al. Nature 582, 501–505 (2020)

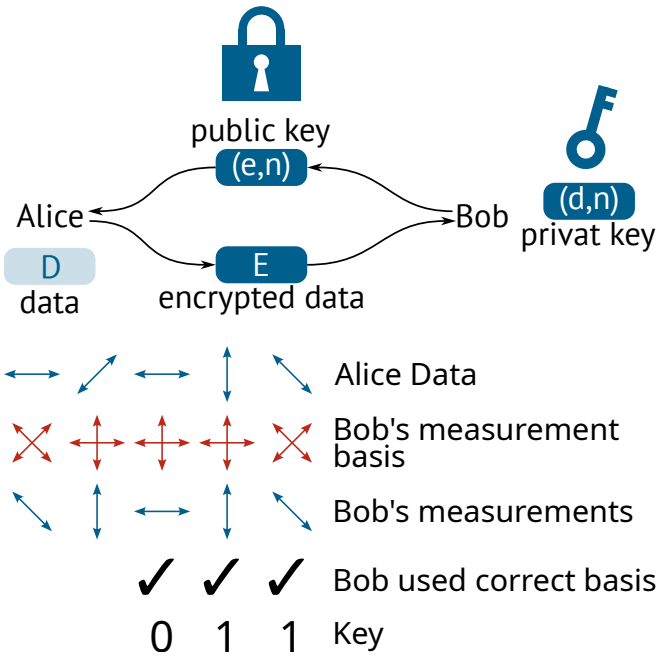
Summary

Summary

- Todays asymmetric cryptography algorithm can be cracked by quantum algorithms
- Quantum cryptography is just QKD
- QKD (BB84) doesn't need entanglement
- By using entanglement a key distributor doesn't know the key



Yin, J., Li, YH., Liao, SK. et al. Nature 582, 501–505 (2020)



Thank you for your attention!