16 Quantum Key distribution

Classical Cryptography

- Caesar cipher:
  replace letter x by a letter n position further in the alphabet
  $x \to x + n \mod 26$

A	T	A	C	K	A	T	D	A	W	N	plain text
D	W	D	F	N	D	W	G	D	Z	Q	encrypted message

- Easily breakable
- Enhanced version with longer key (Vigenère cipher): $x_i \to x_i + n_i$
  but still unsafe when key $(n_1, n_2, n_3, \ldots)$ too short

One time pad

- Similar to Vigenère cipher with
  - length of key = length of message
  - key is chosen randomly (important)
  - Principle: $x_i \rightarrow \underbrace{x_i + n_i \bmod 26}_{\rightarrow \text{ also random number}}$

    random number

  - Binary version:

```
        100101101   message
  XOR   101111010   key
        ---------
        001010111   encrypted message
```

- Properties:
  - perfectly secure (Claude Shannon)
  - requires very long keys (same as text length)

→ Problem: how to distribute key

Possible attacking strategies

- Intercept-resend
  (Eve measures photons and sends similar photon to Bob)

Alice's random bit	0	1	1	0	1	0	0	1
Alice's random sending basis	+	+	×	+	×	×	×	+
Photon polarization Alice sends	↑	→	↘	↑	↘	↗	↗	→
Eve's random measuring basis	+	×	+	+	×	+	×	+
Polarization Eve measures and sends	↑	↗	→	↑	↘	→	↗	→
Bob's random measuring basis	+	×	×	×	+	×	+	+
Photon polarization Bob measures	↑	↗	↗	↘	→	↗	↑	→
PUBLIC DISCUSSION OF BASIS								
Shared secret key	0		0			0		1
Errors in key	✓		✗			✓		✓

→ Introduces error when Eve measures in different basis than Bob

→ Eve can be detected

Error correction

- In real live, there are always errors in the communication (even without Eve)

- Error correction:

P=0 P=1 P=1

```
Alice’s key: 10010  11010  11001
Bob’s   key: 10010  11110  11001
```

P=0 P=0 P=0

Exchange of parity bits between Alice and Bob

→ Alice+ Bob have same key,

→ Eve gains some information about the key

Privacy Amplification

- From the measured error rate
  → determine maximal knowledge of Eve

- To remove Eve's knowledge:
  Apply a random universal hash function F on the key

  $F: \{0,1\}^n \rightarrow \{0,1\}^m$ (n … key length, $m < n$)

  → Key length is reduced, but knowledge of Eve on the remaining key is reduced.

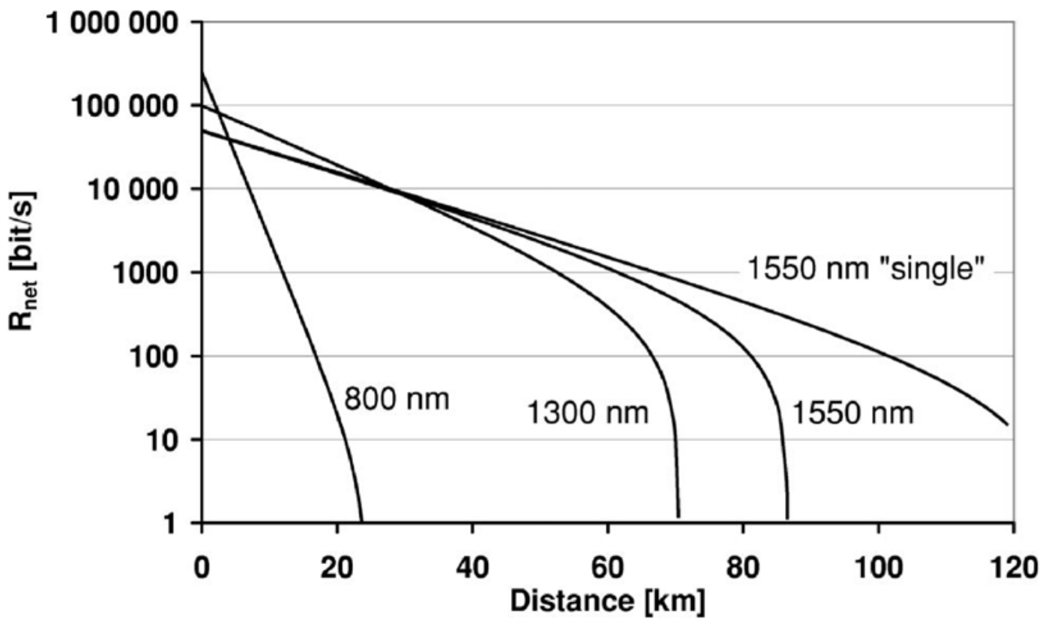
- higher error-rate
  → higher potential knowledge of Eve
  → larger reduction in the length of the remaining key

Distance Limits

- Error correction and privacy amplification
  → Alice and Bob obtain identical key, Eve has only negligible knowledge
  → **But, key generation rate is reduced**
- As losses + errors increase with communication distance
  → Limit to the maximum distance of QKD

Generation rate of secure key vs. length of optical fiber:

Rev. Mod. Phys. **74**, 145 (2002)



Photon-number-splitting attack

- Real-life implementations of BB84 protocol use attenuated laser pulses (not single photons)
  - Typical values: pulse contain about 0.1 photon
  - Poisson statistics requires:

    → every 10th pulse contains 1 photons and every 100th pulse contains 2 photons

- Attack strategy:
  - Eve performs non-destructive photon number measurement
  - If pulse contains 2 photons, Eve removes one and measures it

→ Eve knows 10% of the photons without introducing errors

Man-in-the-middle attack

- QKD requires communication between Alice and Bob via public channel (key generation, error correction, …)

- If attacker has full control of public channel, he can simulate Bob to Alice and vice versa (“man in the middle”)

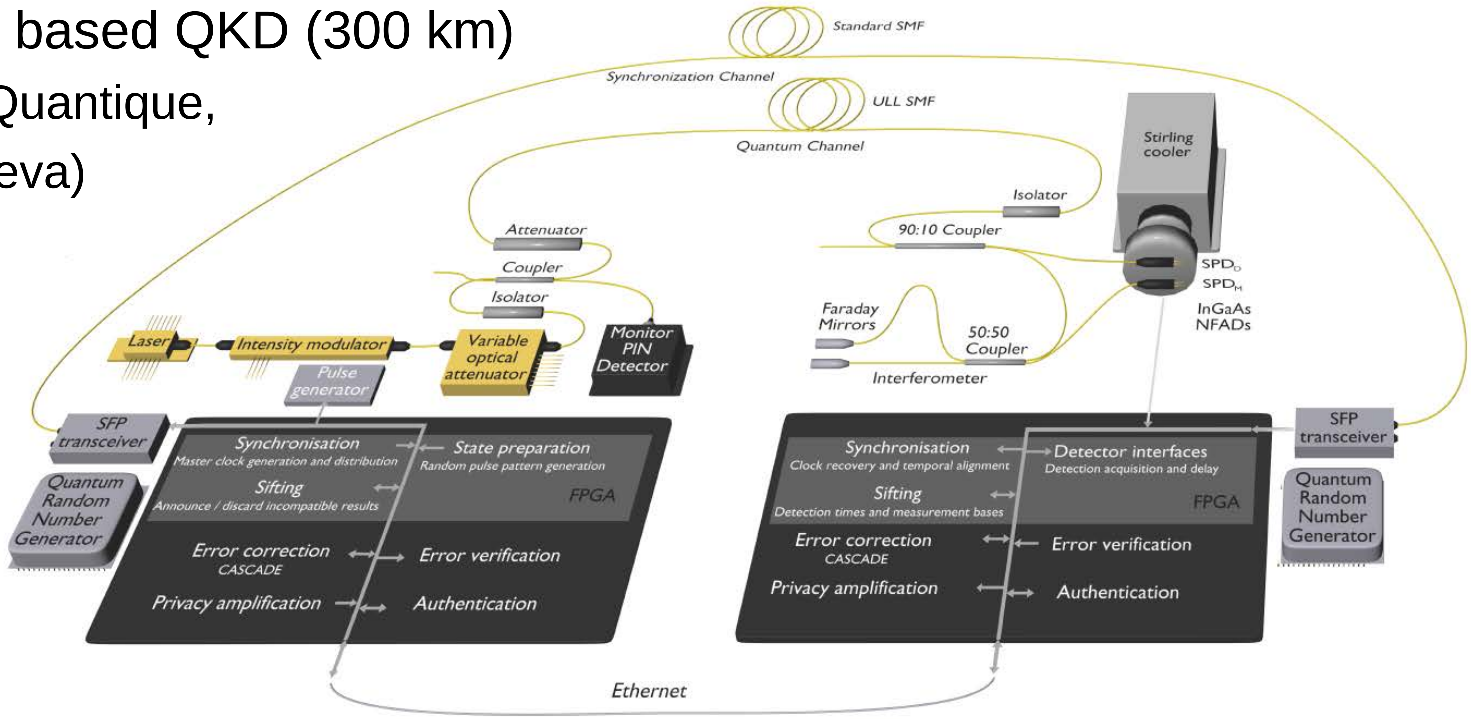
  → Can gain full information about the message

- Solution: Prior to communication, Alice and Bob need already an initial shared secret key

  → use classical (secure) authentication scheme to verify identity of the communication partner

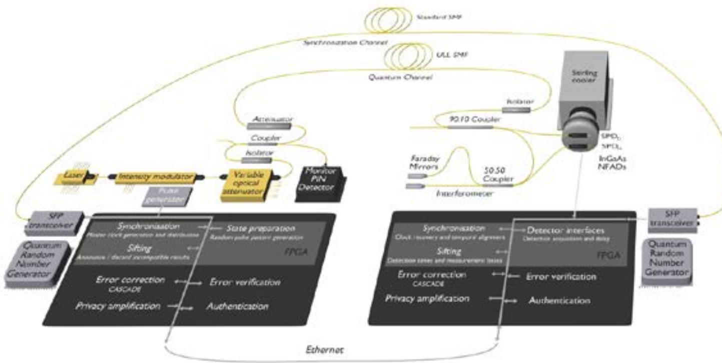
Experimental demonstrations

- Fiber based QKD (300 km)
  (ID-Quantique,
  Geneva)



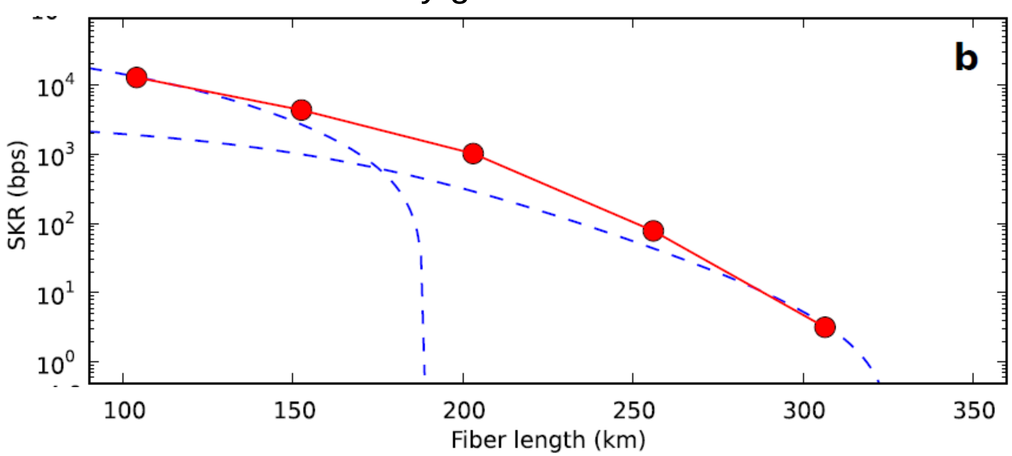
Experimental demonstrations

- Fiber based QKD (300km)
  (ID-Quantique,
  Geneva)



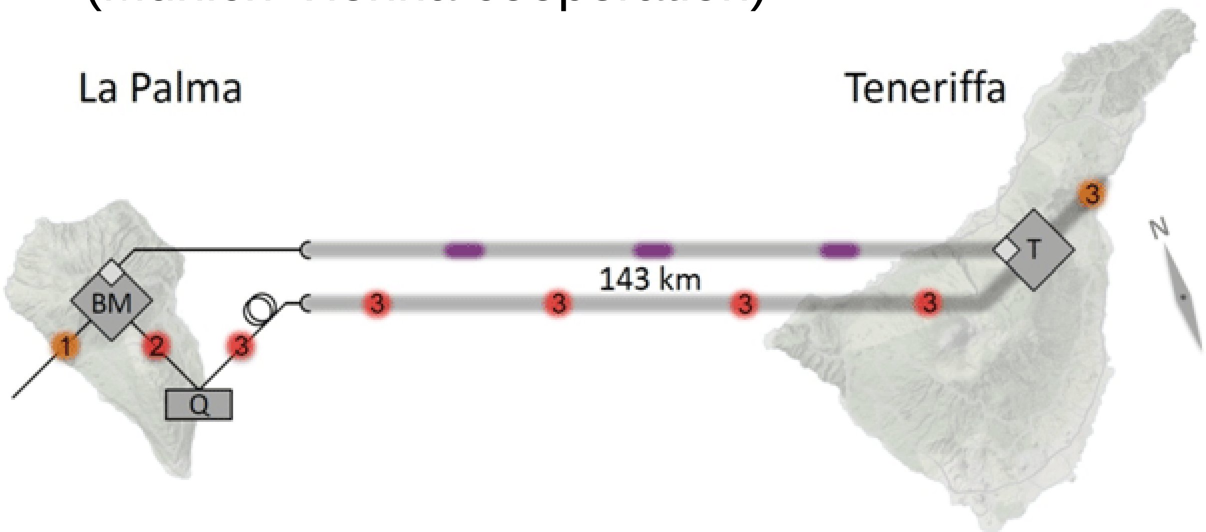
- Commercial company for fiber intregrated QKD systems and accesoires

Key generation rate



Experimental demonstrations

- Free-space QKD
  (Munich-Vienna cooperation)



- Implementation of BB84 + Ekert Protocol
- Experimental key rates: ~10 bits/s

- Distance similar to distance to orbit satellites

→ first step to satellite based QKD

Physical Review Letters **98**, 010504 (2007)
Nature Physics **3**, 481 (2007)

Outlook

- How to overcome distance limits ?
  - In classical communication → optical amplifier (repeater)
  - Not possible in quantum communication (no-cloning theorem)

⇨ quantum repeater