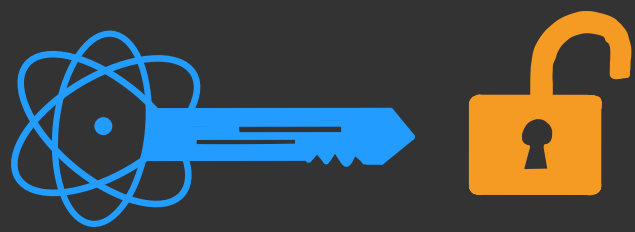
Quantum Cryptography



— Ramona Wolf —
— Quantum Information Theory (D-PHYS) —

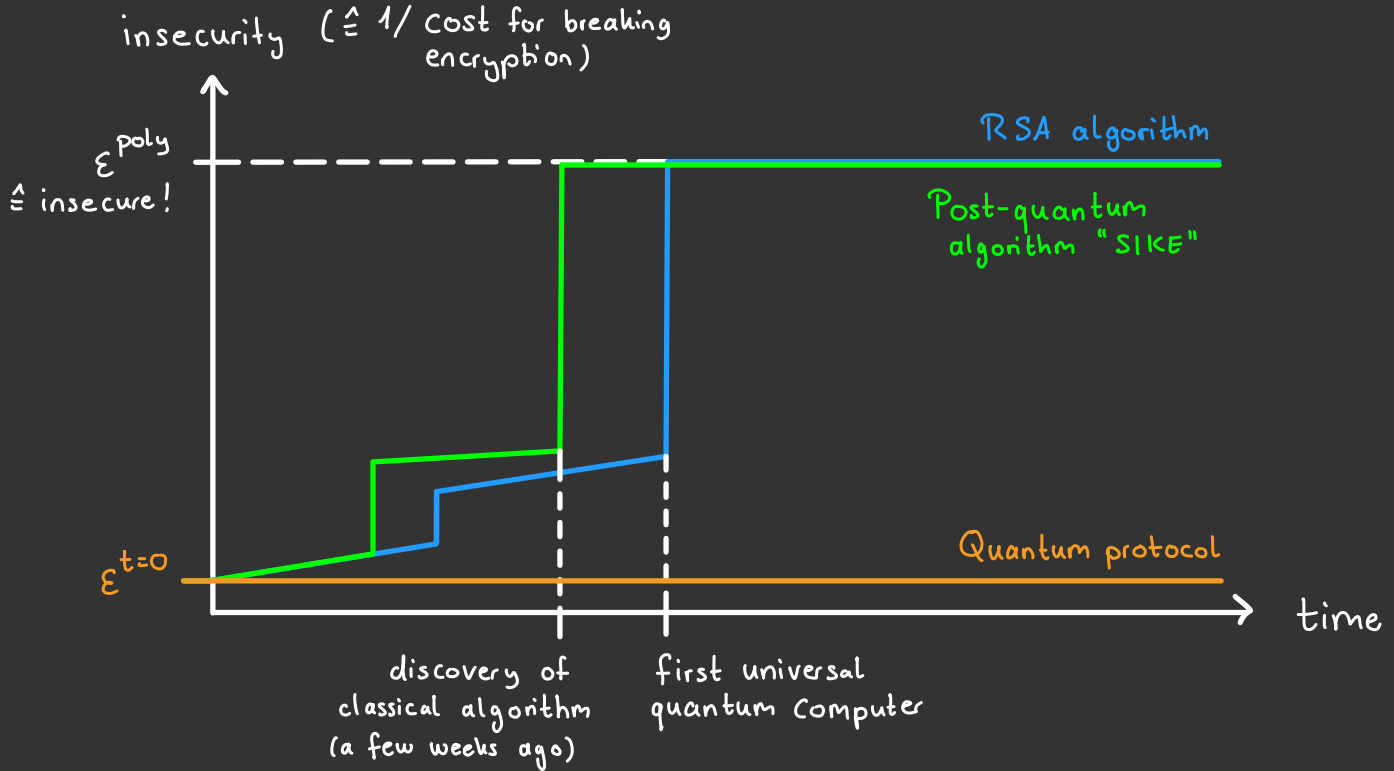
Why quantum cryptography?

Goal: Secure communication

→ Messages cannot be overheard

→ Messages cannot be tampered with

Why quantum cryptography?



Unbreakable security

key	0 1 0 1 1	1 0 0 1 0	ciphertext
message	1 1 0 0 1	0 1 0 1 1	key
ciphertext	1 0 0 1 0	1 1 0 0 1	message

public channel

ciphertext is independent of the message!

Unbreakable security

Cryptographic key:

1. Uniformly random
2. Identical for Alice and Bob
3. Unknown to Eve

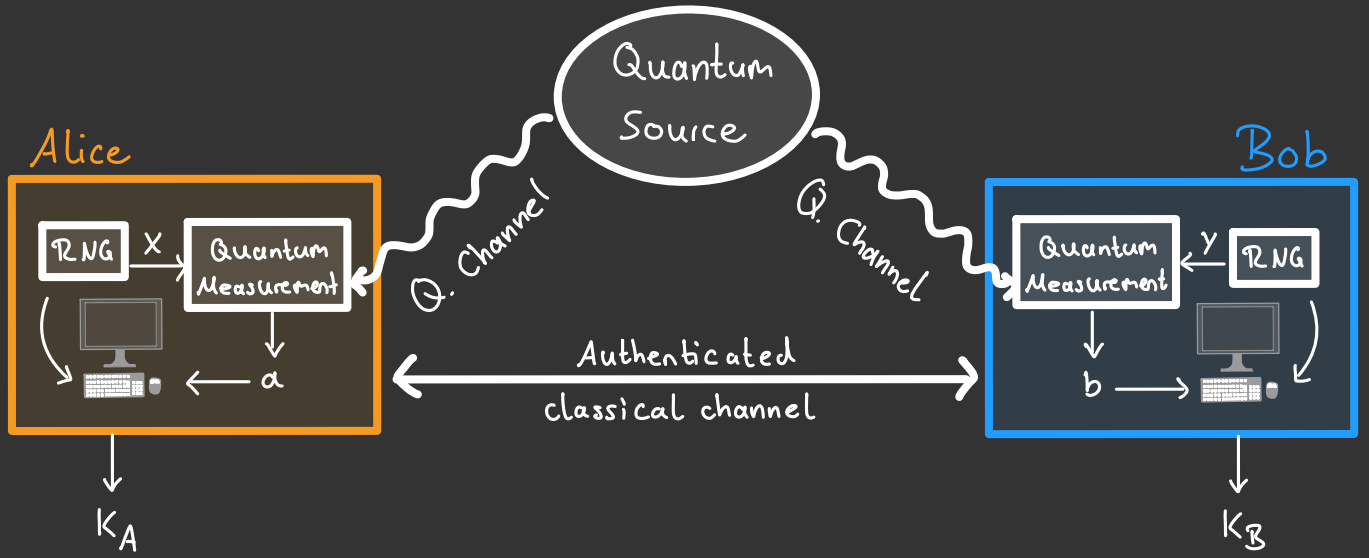
How can

quantum cryptography

achieve this?

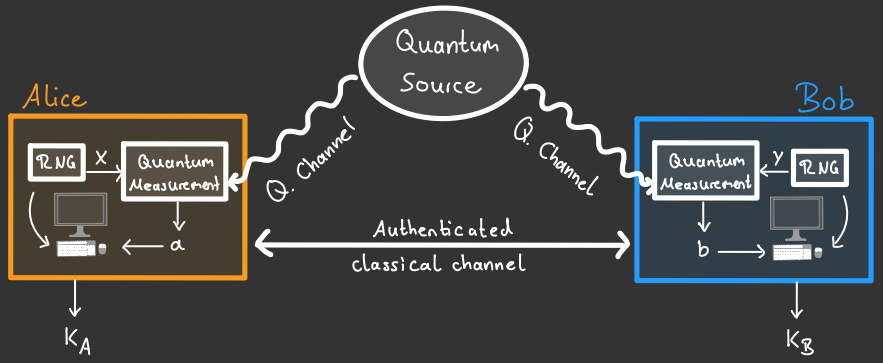
Quantum key distribution

Cryptographic key:
1. Uniformly random
2. Identical for Alice & Bob
3. Unknown to Eve



Quantum key distribution

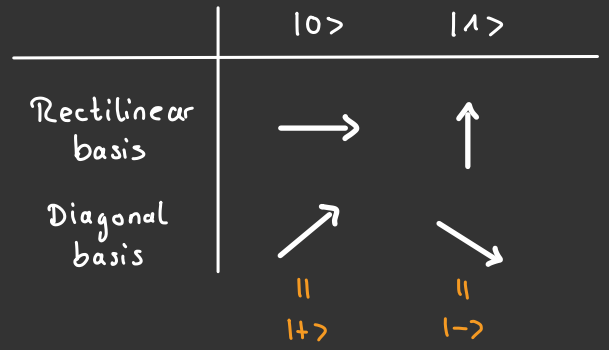
Cryptographic key:
1. Uniformly random
2. Identical for Alice & Bob
3. Unknown to Eve



Qubits: $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$

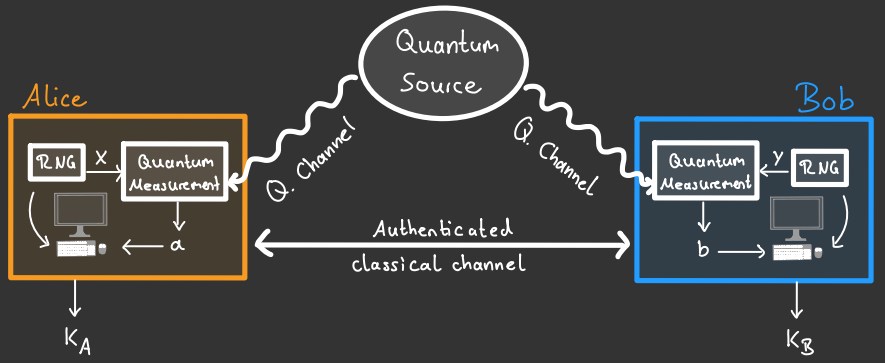
e.g. using polarized photons:

$|\psi\rangle = \tilde{\alpha}|+\rangle + \tilde{\beta}|-\rangle$



Quantum key distribution

Cryptographic key:
1. Uniformly random
2. Identical for Alice & Bob
3. Unknown to Eve



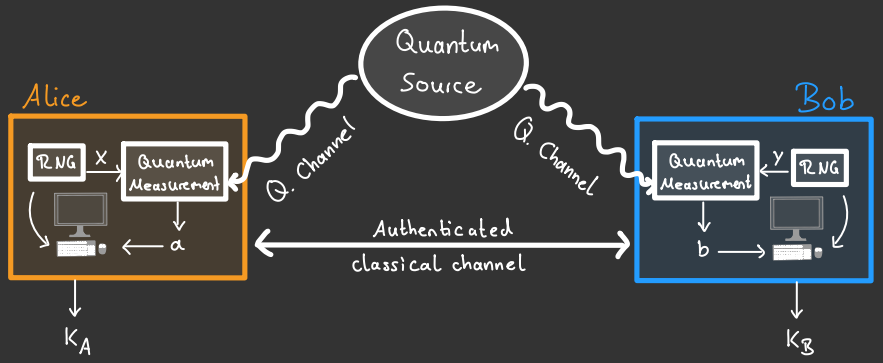
Randomness: Alice receives a qubit: $|\psi\rangle_A = \frac{|0\rangle + |1\rangle}{\sqrt{2}} = \frac{\rightarrow + \uparrow}{\sqrt{2}}$

She measures it in the rectilinear basis (= $\{|0\rangle, |1\rangle\}$)

Output: $Pr[0] = 50\%$, $Pr[1] = 50\%$ } uniformly random

Quantum key distribution

Cryptographic key:
1. Uniformly random
2. Identical for Alice & Bob
3. Unknown to Eve



Identical: Source sends entangled states $|\Phi\rangle_{AB} = \frac{|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B}{\sqrt{2}}$

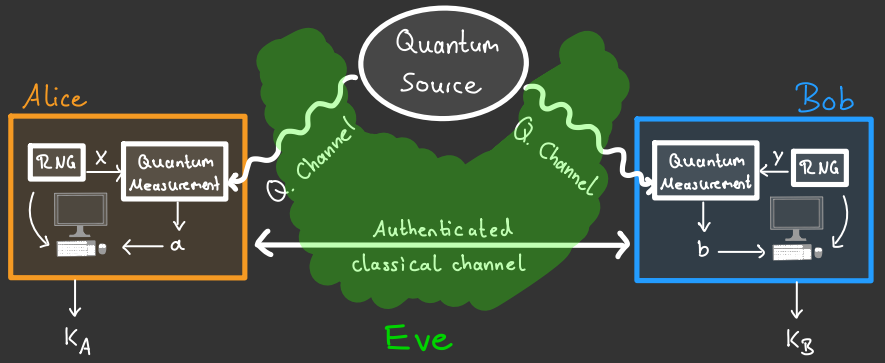
Alice and Bob both measure in the rectilinear basis:

$Pr[0,0] = Pr[1,1] = 50\%$
$Pr[0,1] = Pr[1,0] = 0\%$

=> Identical bit strings

Quantum key distribution

Cryptographic key:
1. Uniformly random
2. Identical for Alice & Bob
3. Unknown to Eve



Private: How can Eve get information?

1. Copy the quantum states => forbidden by the no-cloning theorem
2. Entangle her system with the quantum states
   => forbidden by monogamy of entanglement
3. Measure the quantum states => introduces errors
   attack can be detected!

Quantum key distribution

Cryptographic key:
1. Uniformly random
2. Identical for Alice & Bob
3. Unknown to Eve

The protocol:

I. Quantum phase

1. The source distributes quantum states
2. Alice and Bob measure these states

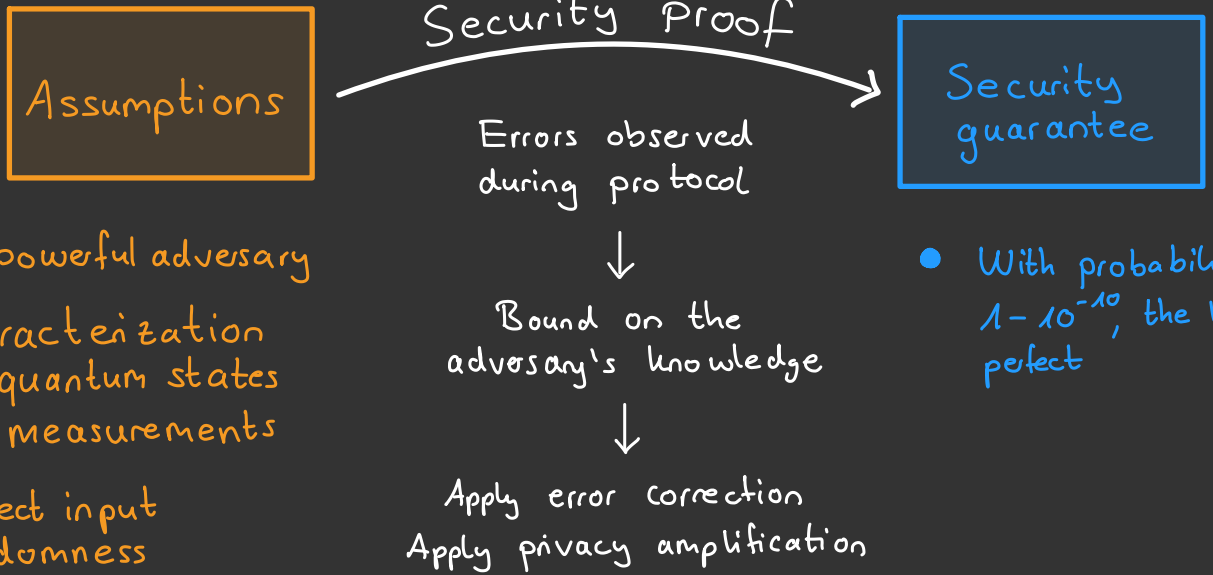
} Eve introduces errors here

3. Output: raw keys R_A, R_B → Imperfect cryptographic key

II. Classical post-processing

1. Alice and Bob estimate the errors in their raw keys:
   How close are R_A, R_B to a perfect key? → Quantum Mechanics allows us to quantify this!
2. They perform an error-correction protocol → identical bit strings
3. They do privacy amplification → random, private keys

Proving security



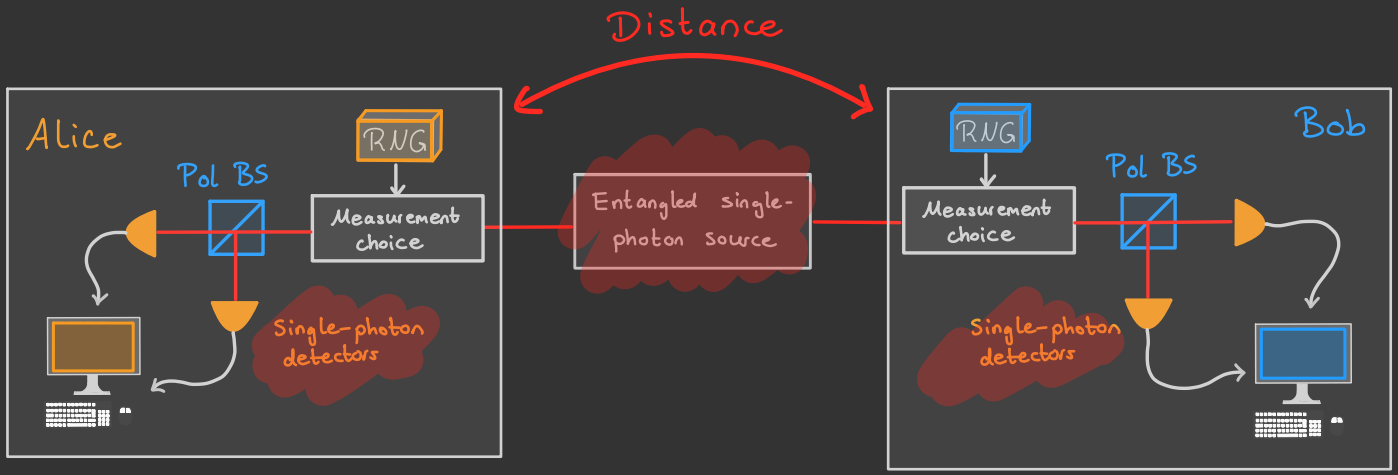
Challenges

Theory:

- Improve methods to calculate bounds on Eve's knowledge (analytical & numerical)
  → Get more key from the same data
- Use as few assumptions as possible
  → Security proof only holds if the assumptions are fulfilled
- Allow for imperfect input randomness
  → Realistic scenario

Challenges

Implementation:



- Perfect single-photon sources & detectors do not exist
- Achievable distances: Very limited due to photon losses
  → Quantum repeater

Takeaway messages

Quantum cryptography can provide unbreakable encryption

BUT some challenges have to be overcome:

- Improved security analysis
- Quantum repeaters
- Reasonable assumptions