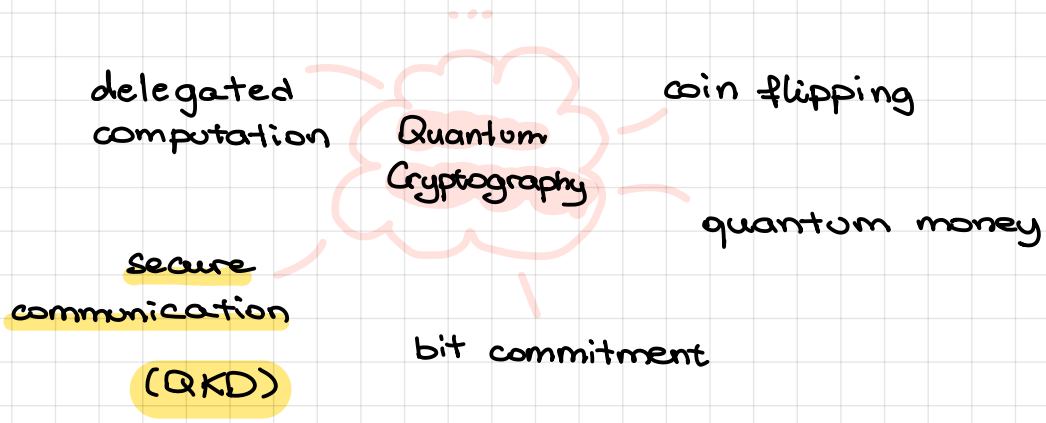
Carla Ferradini - cferradini@phys.ethz.ch

Quantum Cryptography

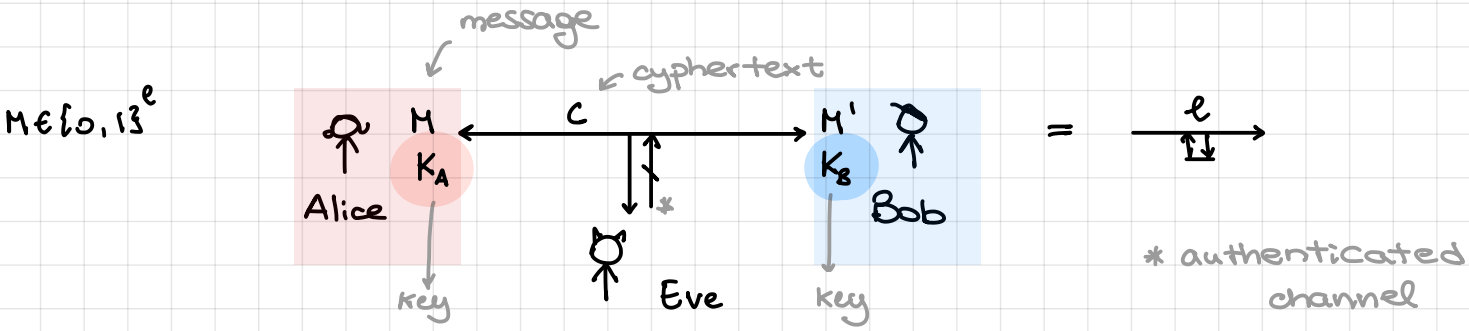
using quantum mechanics

any protocol that aims at hiding info from some third party

e.g.



Task: secure communication, i.e., Alice sends securely a ℓ-bit message to Bob



Concretely: we want to prove $M = M'$ (correctness)

$P(m|c) = P(m) = 2^{-\ell}$ (secrecy)

the OTP protocol:

Ingredients:

- classical authenticated channel
  Eve can listen but not modify it
- secret and identical keys of length ℓ (same length of M)
  i.e., $K_A = K_B = K \in \{0,1\}^\ell$ $P(K) = 2^{-\ell}$

Recipe:

1. Alice produces $C = M \oplus K$ and sends it to Bob
2. Bob receives C and computes $M' = C \oplus K$

Alice		Bob
M	01101001	C 11100100
⊕		⊕
K	10001101	K 10001101
C	11100100	M' 01101001

Public

proof:

Correctness:

$M' = C \oplus K = M \oplus K \oplus K = M$

Secrecy:

$P(M|C) = P(M) = 2^{-\ell}$

Issues: the key cannot be reused => it has to be at least as long as the message

Should we look for better classical protocols? NO

Shannon's thm: for all classical protocols this is the case.

proof: Secrecy is equivalent to $I(M:C)=0 \Leftrightarrow H(M|C) = H(M)$

Correctness is equivalent to $H(M|CK)=0$

$$I(M:K|C) = H(M|C) - H(M|CK) = H(M|C) = H(M) = \ell$$

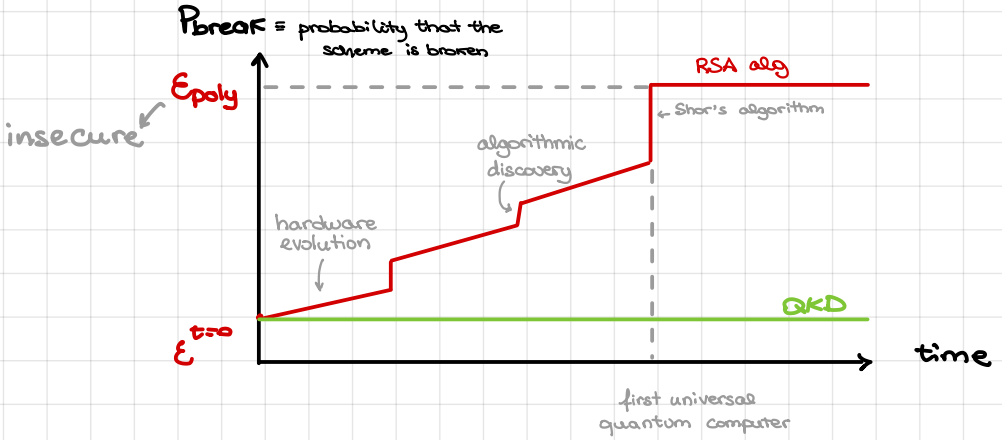
(the messages are unif. distributed)

$$H(K|C) - H(K|MC) \leq H(K|C) \leq H(K) = k$$

(k = length of the key; positivity of $H(x|y)$)

$$\Rightarrow \quad \ell \leq k$$

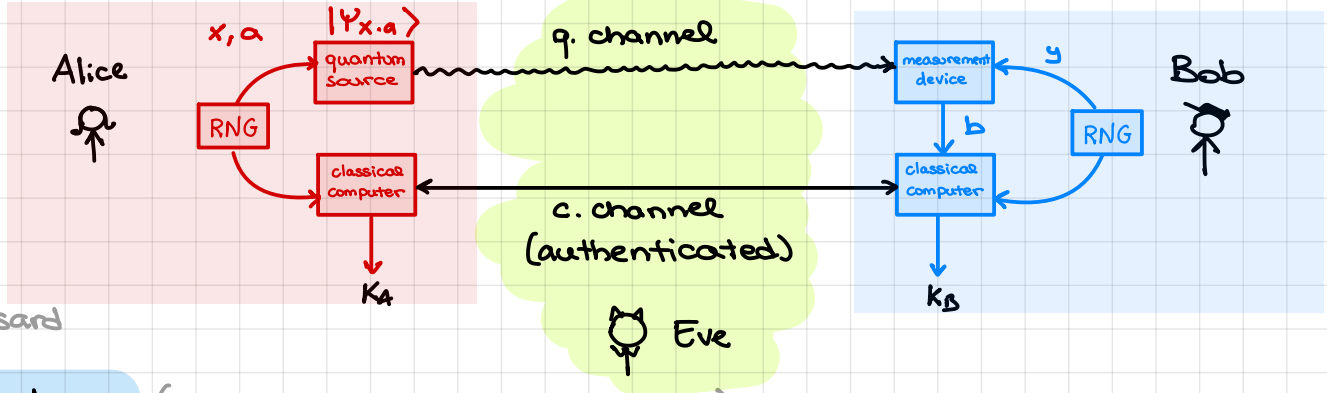
=> Classical crypto: add computational assumptions about the power of the adversary, eg., Eve cannot factorise large numbers (RSA algorithm)



=> Quantum Key Distribution: use QM to produce a key and then use OTP

Lecture I - QKD protocols

Set up:



Bennett Brassard

BB84 protocol: (prepare-and-measure protocol)

for N rounds:

QUANTUM PHASE

1. Alice randomly chooses x, a and prepares the state $|\Psi_{x,a}\rangle$ where:

$$|\Psi_{00}\rangle = |0\rangle \qquad |\Psi_{01}\rangle = |1\rangle \qquad |\Psi_{10}\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}} \equiv |+\rangle \qquad |\Psi_{11}\rangle = \frac{|0\rangle-|1\rangle}{\sqrt{2}} \equiv |-\rangle$$

(x: basis choice; a: basis element choice)

$0 \Rightarrow \mathcal{B} = \{|0\rangle, |1\rangle\}$

$1 \Rightarrow \mathcal{B} = \{|+\rangle, |-\rangle\}$

then she sends it to Bob.

2. Bob randomly chooses y and measures the state in the corresponding basis:

$y=0$ $\{|0\rangle, |1\rangle\}$ $\qquad$ $y=1$ $\{|+\rangle, |-\rangle\}$

he stores the outcome b of the measurement

Alice's bit strings	$X = x_1 x_2 \dots x_N$	basis choice
	$A = a_1 a_2 \dots a_N$	key bits
Bob's bit strings	$Y = y_1 y_2 \dots y_N$	basis choice
	$B = b_1 b_2 \dots b_N$	key bits

CLASSICAL PHASE

3. Alice and Bob send their basis choices X, Y through the classical channel and discard the rounds where $x_i \neq y_i$

4. Alice and Bob randomly choose a subset of A and B to estimate errors in their respective strings

If the error rate is below a certain threshold they continue, else they abort

5. they perform classical post-processing to produce the final keys

(error correction; privacy amplification)

Example

measurements by Bob: $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = |+\rangle$ $x=1$ $a=0$

$y=0$ mmt in $\{|0\rangle, |1\rangle\}$ ↙ ↘ $y=1$ mmt in $\{|+\rangle, |-\rangle\}$

$P[|0\rangle] = P[|1\rangle] = \frac{1}{2}$ $P[|+\rangle] = 1$ $P[|-\rangle] = 0$

⇒ $b=0$ with 50% prob, $b=1$ with 50% prob ⇒ $b=0$ with 100% prob

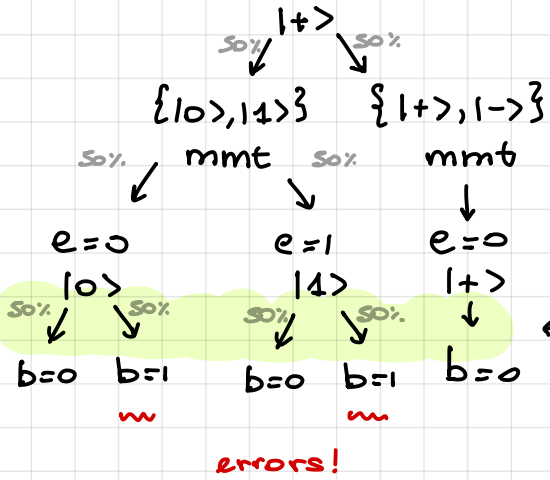
First assume that Eve doesn't act (correctness):

		Basis	$\{\|0\rangle,\|1\rangle\}$				$\{\|+\rangle,\|-\rangle\}$				
1. Alice's choices	X	0	1	1	0	0	1	0	0	1	0
Basis element →	A	0	1	1	1	0	0	1	0	0	1
state prepared		$\|0\rangle$	$\|-\rangle$	$\|-\rangle$	$\|1\rangle$	$\|0\rangle$	$\|+\rangle$	$\|1\rangle$	$\|0\rangle$	$\|+\rangle$	$\|1\rangle$
2. Bob's choices	y	0	0	1	0	1	1	0	1	1	0
Bob's outcomes	B	0	0	1	1	0	0	1	1	0	1
3. Check if $x_i=y_i$:		✓	✗	✓	✓	✗	✓	✓	✗	✓	✓
⋮											

keys match!

Now Eve can intercept the q. state and act on it: What can Eve do?

- copying: not allowed in QM
- measuring: she doesn't know Alice's basis choice
- entangle her state: Bob expects a pure state ⇒ errors



		↙ Basis	↙ {|0⟩,|1⟩}					↙ {|+⟩,|−⟩}			
1. Alice's choices	X	0	1	1	0	0	1	0	0	1	0
Basis element →	A	0	1	1	1	0	0	1	0	0	1
state prepared		|0⟩	|−⟩	|−⟩	|1⟩	|0⟩	|+⟩	|1⟩	|0⟩	|+⟩	|1⟩
2. Bob's choices	Y	0	0	1	0	1	1	0	1	1	0
Bob's outcomes	B	0	0	0	1	0	0	0	0	0	0
3. Check if $x_i=y_i$:		✓	✗	✓	✓	✗	✓	✓	✗	✓	✓
4. Shared rounds	A	0		0			0				
		11		~~1~~	??		11	??		??	??
	B	0		1			0				

Observed error rate: 1/3 for $N \gg 1$ they are close
Actual error rate: 3/7

If they choose to continue...

5. Final strings

x	x	x	1	x	x	1	x	0	1		
			1			0		0	0		

→ classical post processing to produce the final keys!

End of the first hour

Recall: the key is secure if it's 1) uniformly distributed
2) identical for Alice and Bob
3) unknown to Eve

How do we guarantee this? Security proofs

Lecture II - Security of QKD

We can mathematically prove that a QKD protocol is secure!

Set of assumptions: QM is correct ⋮ —Security proof→ Security criterion $\frac{1}{2}\|\rho^r - \rho^i\| \leq \varepsilon$

1) What does it mean that a protocol is secure?

2) What are the assumptions that enter the proof?
↳ about nature, our protocol, ...

3) How can we show that 1) is satisfied if 2) is?

1) Security criterion

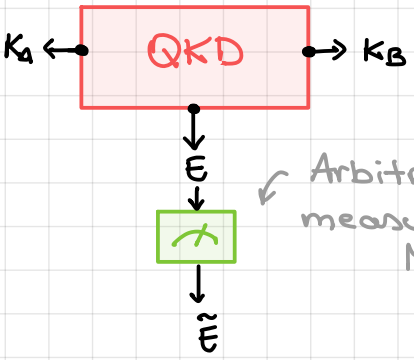
Properties of a secure key:

1) uniform $\forall\, k \in \{0,1\}^\ell \quad P_K(k) = 2^{-\ell}$

2) identical for Alice and Bob $K_A = K_B$

3) unknown to Eve $P_{KE} = P_K \times P_E$ for classical E
$\rho_{KE} = \rho_K \otimes \rho_E$ for quantum E

Is it all?



Proposal: i) $P_r[K_A \neq K_B] = 0$ for 2)

ii) $\sup_M \frac{1}{2}\left| P_{\tilde{E}K} - P_U \times P_{\tilde{E}} \right| = 0$ for 1+3)

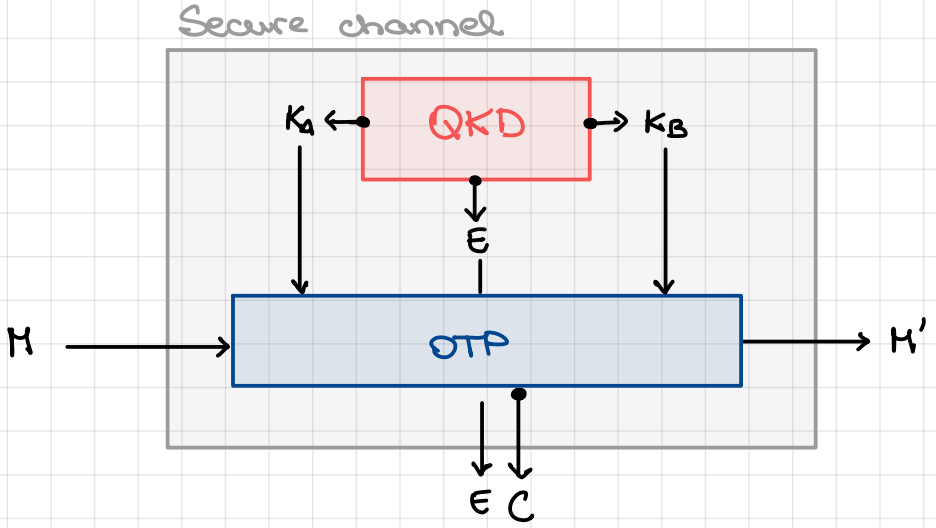
Is a key fulfilling i) and ii) secure? NO

↳ Why? Measuring is irreversible. Eve could preserve her q. system and measure it at a later time when she has more information

We can construct a scenario where i) and ii) are satisfied, but Eve learns the key with certainty [See arxiv 0409078]

the QKD protocol doesn't exist isolated e.g. QKD + OTP ⇒ secure channel

⇒ the security criterion should be composable, i.e.,



security statement I

+

security statement II

=

security statement of a secure channel

Composable definition of security: [see arxiv: 2102.00021]

↳ idea: construct a distinguishing game between a world with ρ^{real} and one with ρ^{ideal} and shows that, if ← is satisfied, the two worlds are not distinguishable

$$\frac{1}{2} \left\| \rho^{real}_{K_A K_B E} - \rho^{ideal}_{K_A K_B E} \right\|_1 = 0 \quad (\leq \varepsilon)$$

trace distance

where

$$\rho^{ideal}_{K_A K_B E} = 2^{-\ell} \sum_{\kappa \in \{0,1\}^\ell} |\kappa\rangle\langle\kappa|_{K_A} \otimes |\kappa\rangle\langle\kappa|_{K_B} \otimes \rho_E$$

identical for A and B 2)

unknown to Eve 3)

Uniform 1)

Soon on arxiv: axiomatic derivation of the security criterion [arxiv: ?? with M. Sandfuchs, R. Wolf, R. Renner]

2) Assumptions

the security proof is meaningful <u>only</u> if the assumptions are satisfied

Examples:

- Alice and Bob have access to an authenticated cl. channel
  can be achieved with a short key ⇝ "password"
- the Labs are isolated
  only authorised information gets out
- trust in the devices: they work according to their mathematical description, the RNGs actually produce random numbers, ...
- Quantum theory is correct ⇝ only QIT formalism is needed
  no Schrödinger equation, ...

  Quantum Gravity? Can gravitational effects give more power to Eve?
- Quantum theory is complete: no theory has more predictive power than QM

  follows from correctness + existence of randomness
  [arxiv:1005.5173]

  Counterexample: "Kish Cipher" based on thermodynamics which is <u>not</u> a complete theory!

3) Security proofs: current research ⇝ there is no recipe ☺

Other research topics in QKD:

* Device independent QKD
* On the classical post processing
* Experimental realizations
* ...

Thanks to Ramona Wolf for sharing her notes with me.