14.1 Quantum Cryptography

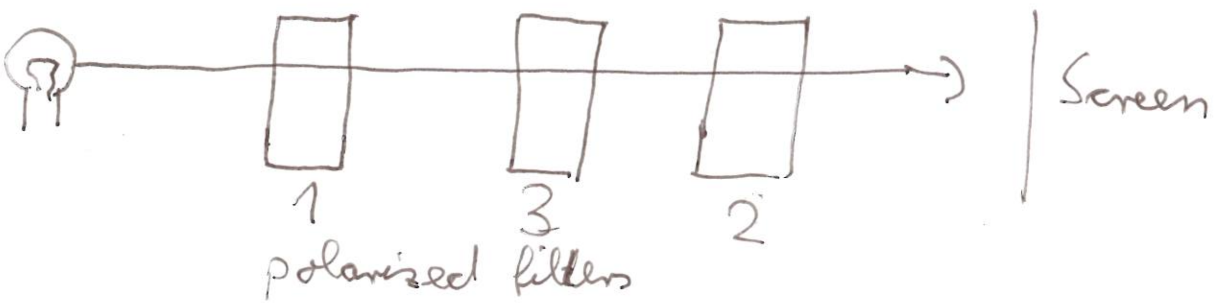
Quantum cryptography is strongly related to quantum computers. There exists an efficient alg. for factoring large numbers (Shor, 1994, s. Tr & Wash. 2nd ed. 460 ff), ready to use once a powerful quantum computer exists. This would endanger many of the presently used cryptographic protocols and alg.

In parallel, quantum cryptography was developed to ensure physically secure transmission, particularly secure against quantum computing facilities. Quantum cryptography is based on quantum effects, not easily accessible for non-physicists.

Quantum mechanics is a difficult subject with concepts where everyday experiences are not applicable.

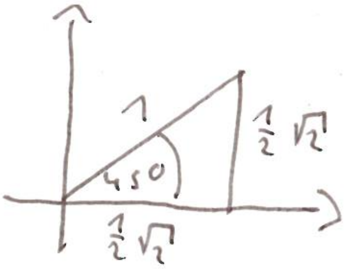
We need particles like electrons or photons that we are able to observe. Photons make up light which is easily observable. They serve best for explaining the basic principles of quantum cryptography.

14.1.1 A quantum experiment



Filter 1 : Vertically polarized
Filter 2 : Horizontally polarized
Filter 3 : Diagonally polarized

Polarization of photons
is described by a
complex unit vector



(a,b) of length $|a|^2+|b|^2=1$

Choose a basis $|\uparrow\rangle$, $|\rightarrow\rangle$ (notation from physics)

Measurement postulate of quantum mechanics

Given a device for measuring polarization with $|\uparrow\rangle$, $|\rightarrow\rangle$
A photon with polarization $a|\uparrow\rangle + b|\rightarrow\rangle$ is measured with probability $|a|^2$ as $|\uparrow\rangle$ and with prob. $|b|^2$ as $|\rightarrow\rangle$
Measuring will change the state to the result of the measurement

Model for the experiment

Photon with random polarization
Filter with $|\uparrow\rangle$ $|\rightarrow\rangle$

- measured as $|\uparrow\rangle$ with prob $1/2$, has polarization $|\uparrow\rangle$, pass through
- measured as $|\rightarrow\rangle$ with prob $1/2$, has polarization $|\rightarrow\rangle$, reflected
- Filter 2 (without Filter 3) with basis $|\rightarrow\rangle$, $|\uparrow\rangle$ lets no photon pass
- Filter 3 in between 1 and 2 with basis $|\nearrow\rangle$, $|\nwarrow\rangle$
- Photons will pass Filter 1 with prob $1/2$
- These pass filter 3 with prob $1/2$
- These pass filter 2 with prob $1/2$

Intensity: $1/8$ of the original

14.2 Quantum Key Exchange

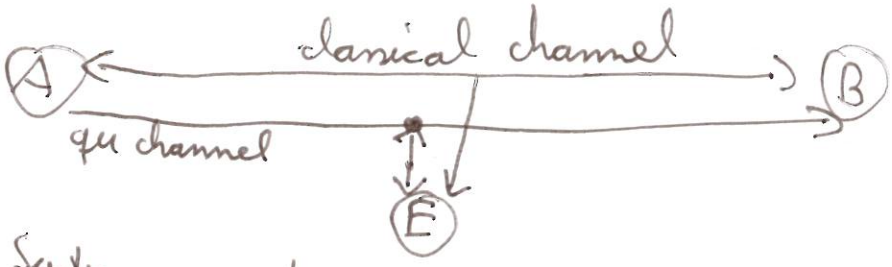
Choose an orthonormal basis $|0\rangle$ $|1\rangle$ of a 2-dim. complex vector space. Each unit vector is called a quantum bit (qubit), written as

$a|0\rangle + b|1\rangle$ s.t. $|a|^2 + |b|^2 = 1$

The probability of observing a qubit in state $|0\rangle$ is $|a|^2$

A and B want to exchange a sequence of bits. They use a classical channel and a quantum channel (one which transmits photons without altering the polarization).

Eve has access to both channels.



System parameters

Alice and Bob use two bases

$B_1 = \{ |\uparrow\rangle, |\rightarrow\rangle \}$ (rectlinear, +)

$B_2 = \{ |\nearrow\rangle, |\nwarrow\rangle \}$ (diagonal, ×)

Encryption

Alice selects randomly B_1 or B_2

If she chooses B_1 (+) she encodes

0 as $|\uparrow\rangle$ (vertically polarized photon)

1 as $|\rightarrow\rangle$ (horizontally polarized photon)

If she chooses B_2 (×) she encodes

0 as $|\nearrow\rangle$ (diag, NE pol. photon)

1 as $|\nwarrow\rangle$ (diag, NW pol. photon)

Decryption:

1. Bob measures the polarization of received photons randomly with B_1 or B_2, keeps the result secret.
2. B tells A over the classical channel which bases he has chosen.
3. A tells B which bases are correct

A and B will agree on approx. half the amount of bits A has sent. These bits are used as key for the one-time pad, AES.

Example

Alice

Bits	0	1	1	1	0	0	1	0	...
random bases	+	X	+	+	X	X	+	X	...
qubit (photon)	$\lvert\uparrow\rangle$	$\lvert\nwarrow\rangle$	$\lvert\rightarrow\rangle$	$\lvert\rightarrow\rangle$	$\lvert\nearrow\rangle$	$\lvert\nearrow\rangle$	$\lvert\rightarrow\rangle$	$\lvert\nearrow\rangle$	...

Bob

Random bases	X	X	X	+	X	+	+	X	...
Bits		c		c	c		c	c	...
Correct		1		1	0		1	0	...

Security is based on physical phenomena. If Eve observes the channel i.e., photons from A, she will change the state, hence, introducing add. errors.

Actual implementations work over a distance of 100 km using conventional fiber optic cables (Sep '15)

Though, Lucamarini et al. 2018: „rate-distance limit may be overcome"

Suggestion for 550 km by "Twin-Field quantum key distribution scheme."