Computer Security

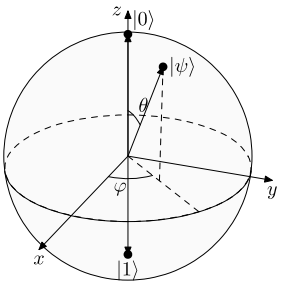
Quantum Cryptography - basics

Quantum Technology

- Quantum Computing
  - solving problems much, much faster than classical computers
- Quantum Communication/Cryptography
  - using Physics to generate secure keys and detect eavesdropping
- Quantum Sensing
  - using quantum states to measure physical quantities like gravity or magnetic fields with extreme precision

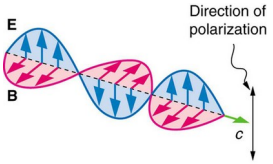
Quantum bit

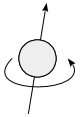
- classical bit:
  - binary state of system
  - smallest unit of information, valued: 0 or 1
  - analogy: normal light switch, can be "on" or "off"
- quantum bit, qubit
  - two-level mathematical state of physical system[1]
  - vector in a two-dimensional Hilbert space:
    - $|q\rangle = a\,|0\rangle + b\,|1\rangle$ [2]
  - value unknown; upon measurement: |0> or |1> (--> 0 or 1)
  - analogy: spinning coin
    - while spinning: ? ; when stopped: one definite result!
  - examples...



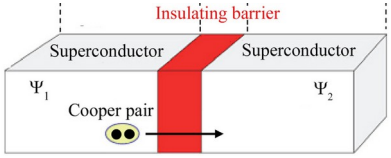
1 according to Quantum Mechanics!
2 *a* and *b* can be complex numbers

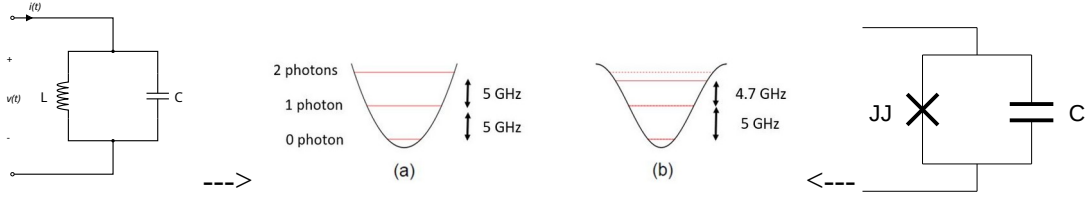
...Quantum bit...





- examples:
  - ex1: photon polarization (see ahead)
  - ex2: electron spin
  - ex3: superconducting circuits
    - two quantized current states
    - $|0\rangle$ and $|1\rangle$: the 2 first quantum states of nonlinear superconducting circuit
      - e.g., a Josephson junction[3]

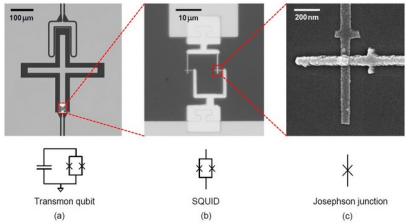




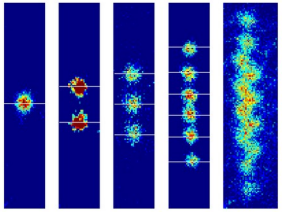
3 Josephson effect (1962): current may tunnel through an insulating barrier separating two super-conductors (voltage across remaining zero up to a (critical) current value.

...Quantum bit: superconducting circuits...

- control: microwave pulses conducted by wires
  - anharmonicity allows tuning the transitions: setting the qubit!
- good: fast transition speed (ns)
- bad: short coherence time (us)



- ex4: trapped ions
  - two atomic energy levels of an ion (Ca^+, Yb^+...)
  - ion is trapped in vacuum, hold in place by oscillating RF electric field, sufficiently cooled
  - control: laser pulses
  - good: extremely long coherence time (sec/min) ;
  - bad: slow transition speed (ms)
- ...



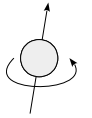
...Quantum bit...

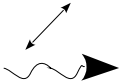
- multiple qubits
  - 1 bit : 2 states
  - 2 bits: 4 states
  - n bits: 2^n states
    - n qubits represent 2^n states at once (in superposition)
      - but we get **do not** get all answers at once
      - measuring, we get 1 state!

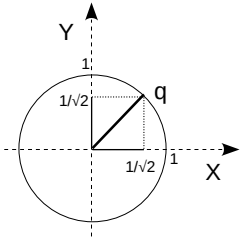
Physics' properties

- Superposition
- Interference
- Entanglement

Physics' properties





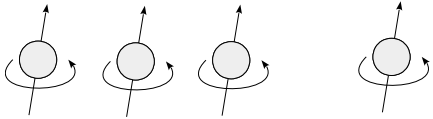


- Superposition
  - a qubit exists in multiple states simultaneously (both 0 and 1)
  - mathematical reasoning (think of polarized photons):
    - start with a qubit in a 45º state (doable):
      - wave-equation(qubit) = $1/\sqrt{2}\ |0\rangle + 1/\sqrt{2}\ |1\rangle$
    - if you measure it in 0º
      - you get $|0\rangle$ with a 50% chance (= $|1/\sqrt{2}|^2$) [4]
    - afterwards, it's wave-function will be $|0\rangle$ [5]

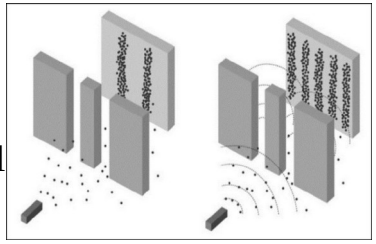
4 and a 50% chance of getting state $|1\rangle$, as the total probability must be 1: $|1/\sqrt{2}|^2 + |1/\sqrt{2}|^2$

5 what is called "collapsation" of the wave function

...Quantum bit: Physics' properties...



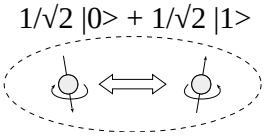
- Interference
  - qubits behave as waves, so they may interfere
    - constructively or destructively
  - mathematical reasoning:
    - start with a sequence of (unrelated) qubits;
    - when you send them (even one by one) through a double slit of sufficiently small dimensions, they will hit a screen in specific places determined by their "measurement" probabilities. As the launching proceeds, an interference pattern will appear.[6]



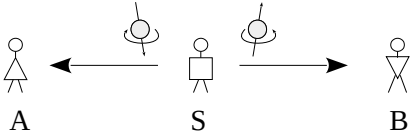
6 A similar (but no equal) interference effect could be seen by a single qubit moving through a single slit of adequate dimension; here instead of *interference*, the correct word is "*diffraction*".

...Quantum bit: Physics' properties...

- Entanglement
  - two or more qubits become "linked" in a single state
    - what happens to one **instantly** *influences* the other, regardless of distance[7]



  - mathematical reasoning (think of polarized photons):
    - start with 2 qubits in a "joint" superposition (e.g. positively correlated[8])
      - they aren't independent: they share a single mathematical description (wave-function)
    - confine one in "box"[9], take the other to a very far position[10]



    - measure one qubit, e.g. get |0> ; the *single* wave-function collapses instantly; afterwards, when measured, the far away qubit will guaranteed be |1>

7 what Einstein said as a "spooky action at a distance"
8 Many times, two entangled particles have variables that are anti-correlated, e.g. one photon's spin is 1/2 and the other's is -1/2.
9 if a photon, it could be put between two ideal parallel mirrors
10 if a photon, let it travel until far away

Quantum Cryptography

Motivation

- public-key crypto relies on *hard classical problems*
  - RSA:
    - $K^+ = (e, n)$; $K^- = (\boldsymbol{d}, n)$ ---> $\boldsymbol{d}$?
    - if p, q can be found such that $p \times q = n$ [11] : the Factoring Problem - hard for n huge!
      - $\phi(n) = (p\text{-}1) \times (q\text{-}1)$; $e \times d = 1 \pmod{\phi(n)}$ ---> $\boldsymbol{d}$!
  - Diffie-Hellman key exchange:
    - n, g, X $(= g^x \bmod n)$, Y $(= g^y \bmod n)$; $g^{xy} \bmod n = K_{AB}$ ---> $\boldsymbol{g^{xy}}$?
    - if x and y can be found such that $x = \log_g X \bmod n$, $y = \log_g Y \bmod n$: the Discrete Logarithm Problem - hard for X, Y huge!
      - x, y ---> $\boldsymbol{g^{xy}}$ **mod** $\boldsymbol{n}$!

11 p, q primes

...Quantum Cryptography: Motivation...

- symmetric -key crypto, sometimes rely on brute-force classical difficulty
  - AES:
    - no shortcuts to secret keys; keys are too big to be attacked by brute-force
- hash functions crypto, sometimes rely on brute-force classical difficulty
  - SHA-2,3:
    - no shortcuts to "reversion" (collision!); hashes are too big to be attacked by brute-force

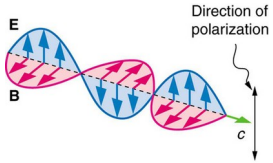
...Quantum Cryptography: Motivation...

- Quantum computing eases those types of problems
  - quantum hardware
  - "quantum" software
    - Shor algorithm : breaks RSA and Diffie-Hellman
    - Grover algorithn : breaks AES with "small" keys and SHA 2, 3 with "small" size
- So, for security, use:
  - Quantum cryptography (doesn’t rely on hard math but on Physics' laws)
  - Post-Quantum Cryptography (not vulnerable to Quantum Computing known algorithms)

Quantum Communication/Cryptography

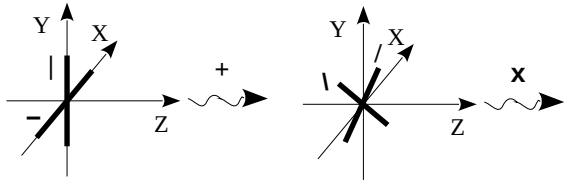
- Quantum Key Distribution:
  - using Physics to generate secure keys and detect eavesdropping
- 2 protocols as examples:
  - BB84 protocol (Bennet & Brassard, 1984)
    - measurement changes the state (experimenter interacts with system)
    - uncertainty / incompatibility (some properties cannot be known at the same time)
    - no cloning (an unknown quantum state cannot be copied)
  - E91 protocol (Ekert, 1991)
    - measurement changes the state (experimenter interacts with system)
    - uncertainty / incompatibility (some properties cannot be known at the same time)
    - entanglement (parts of a system are inter-related)

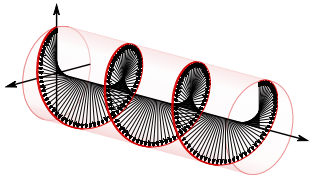
Intuition with polarization of light



Classical light

- electromagnetic field in motion
- polarization:
  - geometric orientation of electric (or magnet) field vibration of light
  - almost always perpendicular to direction of motion (transversal waves)[12]
  - can be linear or circular/elliptical
  - can be static (over space and time): e.g. laser light
  - can change over space and time (circular polarization)
  - can change randomly over space and time ("normal" light, such as sunlight)





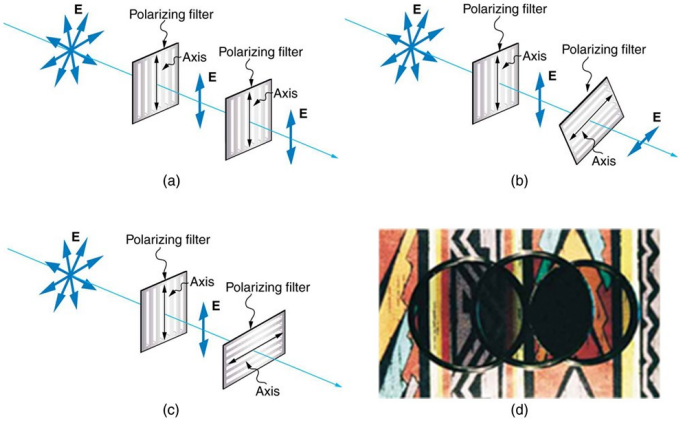
12 very specific exceptions can be found: evanescent waves in interface with materials, highly focused beams...

...Intuition with polarization of light: Classical light...

- polarization measurement coordinate basis possibilities
  - linear: + basis: vertical (|) , horizontal (—)
  - linear: x basis: diagonal (/) , anti-diagonal (\)
  - circular: o basis: Right , Left[13]
- filtering:
  - linear: selective absorption, intensity decreases (at least 50% for unpolarized light)
  - wave plate: phase retardation, intensity is preserved (~100% minus minor reflection)

13 are represented with complex (imaginary) numbers

- polarized sunglasses use linear horizontal filters
  - to block sunlight reflected from horizontal surfaces (water, road...)



Fig[14]: Left: The effect of rotating two polarizing filters, where the first polarizes the light. (a) All is passed by the second polarizing filter. (b) Only part of the light is passed. (c) No light is passed. (d) Photograph, where a polarizing filter is placed above two others, with axis perpendicular to the one on the right (dark area) and parallel to the one on the left (lighter area).
Right photo: https://eyemantra.org/eye-care/polarized-sunglasses/

14 https://pressbooks.online.ucf.edu/phy2054lt/chapter/polarization/ (credit: P.P. Urone)

Quantum light

- photons in quantum wave function
- photon polarization coordinate basis possibilities
  - linear: + basis: vertical (|) , horizontal (—)
  - linear: x basis: diagonal (/) , anti-diagonal (\)
  - circular: o basis: Right , Left[15]
- photon state representation as linear combination of values of each basis:
  - photon_state = a * | + b * - (+ basis)
  - photon_state = c * \ + d * / (x basis)
  - photon_state = e * L + f * R(o basis)

15 are represented with complex (imaginary) numbers

...Intuition with polarization of light: Quantum light...

- measuring in the "wrong" basis gives **random results**:
  - e.g. if Alice sends a vertical photon, | → (code basis: +)
  - and if Bob measures it in the × basis, he will get (exclusive or):
    - / (50% chance)
    - \ (50% chance)
- also, measuring (might) **change** the original state (if done with the **incorrect** basis)
  - e.g. Alice sent a vertical photon, Bob got a / state: the original state was lost!
  - So, “If you lack info, you can’t measure without leaving traces!” (eavesdropping detection!)

Where does "Quantum" appears?

- Quantum cryptography does not use strong classical light beams:
  - it uses singular photons (or very weak pulses approximating them)
  - the state of those photons are not ever known for sure, unless measured (and, so, changed)
- Classically:
  - a beam can be split, taking a small fraction and letting the rest continue (albeit weaker)
    - the small fraction can be measured and possibly goes unnoticed by the correct receiver
    - eavesdropping goes undetected
    - “randomness” usually comes from noise or lack of knowledge

...Where does "Quantum" appears?...

- Quantumly:
  - a photon is indivisible, cannot be split
    - either is measured (destroying its state) and forwarded altered or
    - passes untouched (and give no knowledge of its state)
  - unknown quantum states cannot be copied
    - so, one cannot copy a photon, measure one copy and forward the other
  - randomness and disturbance are fundamental
    - even with perfect knowledge, outcomes are probabilistic
    - measurement irreversibly changes the original state
  - unintuitive weirdness is common
    - with entangled photons, what happens to one photon irreversibly affects the others
      - no matter how far away they are!

BB84 Protocol

Goal

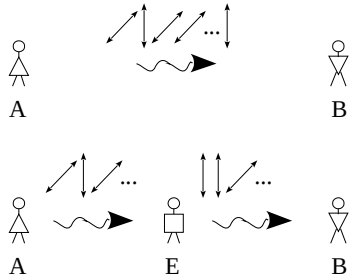
- two parties get to agree on a shared secret (key)

Conditions

- two communication paths are available:
  - one, open but quantum in essence
  - other, classic and public, with only integrity protection
  - both can be eavesdropped
- agreement is statistically achieved
  - if not, the protocol is repeated

Entities

- Alice (sender)
- Bob (receiver)
- possibly, Eve (attacker)



Operation

- Step 1: Encoding
  - Alice sends qbits to Bob using *random* basis (reference of coordinates):
    - + basis → (|, —)
    - × basis → (/ ,)
- Step 2: Measurement
  - Bob measures polarization of the arriving qbits with a *randomly* chosen basis for each

...BB84 Protocol...

- Step 3: Public discussion
  - Alice & Bob compare **basis only** for each measurement
    - they keep only the matching ones
  - they compare a **subset** of bits
    - if too many errors: **Eve detected** (or noise...)!
- Step 4: Key extraction
  - remaining (secret) bits = shared key

BB84 Demo[16]

Without eavesdropping:

		Photon:	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	**Obs:**
Quantum channel	Alice's filters		+	+	x	+	+	x	x	+	x	x	+	x	x	x	x	+	
		Alice sends:	–	–	/	|	–	/	\	|	/	\	|	/	/	|	\	–	
	Bob's filters		+	x	+	+	+	+	+	+	x	+	+	x	x	x	x	+	
		Bob's readings:	–	/	|	|	–	|	–		/	|		/		/	\	–	assume 10% failures
Public "integral" channel	Bob tells filters		+	x	+	+	+	+	+		x	+		x		x	x	+	
	Alice tells hits		.			.	.				.			.			.	.	7 photons "usable"! Probab: (1-0,1) * 0,5 * 16 = 7.2
	Bob tells 50% values		–				–							/			\		
	Alice compares to hers		–			.	–				.			/			\	.	
	secret shared string:					**1**					**1**							**0**	– : 0 ; | : 1 ;; \ : 0 ; / : 1

16 built with help from http://fredhenle.net/bb84/demo.php

With eavesdropping 1:

		Photon:	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	Obs:
Quantum channel	Alice's filters		x	+	+	+	x	x	x	x	+	x	+	x	x	+	+	x	
		Alice sends:	/	–	–	–	\	/	\	\	|	\	|	/	\	|	–	/	
	Eve's filters		+	+	+	x	+	+	+	x	x	x	+	x	x	+	x	+	
		Eve's readings:	|	–	–	\	–	|	–	\	/	\	|	/	\	|	\	|	
	Bob's filters		+	+	+	+	x	x	+	x	+	x	+	x	+	x	x	+	
		Bob's readings:	|		–	–		/	–	\	–	\		/		\	\	|	assume 10% failures
Public "integral" channel	Bob tells filters		+		+	+		x	+	x	+	x		x		x	x	+	
	Alice tells hits				.	.		.		.	.	.		.					7 photons "usable"!
	Bob tells 50% values				–	.		.		\	.	\		/					Probab: (1-0,1) * 0,5 * 16 = 7.2
	Alice compares to hers				–	.		.		\	.	\		/					
	secret shared string:					**0**		**1**			**1**								Eve was UNdetected!

With eavesdropping 2:

		Photon:	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	Obs:
Quantum channel	Alice's filters		x	+	x	x	x	+	+	x	+	x	x	x	x	x	+	+	
		Alice sends:	/	–	/	\	/	|	–	\	|	/	\	\	/	/	|	–	
	Eve's filters		+	+	x	x	x	+	x	+	x	x	x	+	+	+	+	+	
		Eve's readings:	|	–	/	\	/	|	/	–	\	/	\	|	|	–	|	–	
	Bob's filters		x	+	x	+	+	x	+	x	x	+	x	+	+	x	+	+	
		Bob's readings:	/	–	/	–	–	\	|	/	\	–	\	|	|	\	|	–	assume 0% failures
Public "integral" channel	Bob tells filters		x	+	x	+	+	x	+	x	x	+	x	+	+	x	+	+	
	Alice tells hits		.	.	.				.	.			.			.	.	.	9 photons "usable"!
	Bob tells 50% values		/	–	.				.	.			.			/	.	–	Probab: (1-0) * 0,5 * 16 = 8
	Alice compares to hers		/	–	.				.	.			.			\	.	–	
	secret shared string:																		Eve was detected (by chance!)! Measurements are discarded.

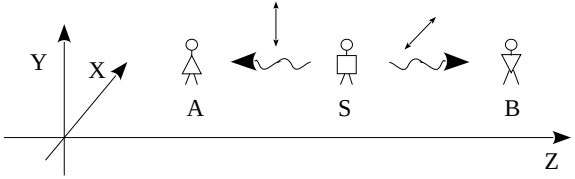
E91 Protocol

Goal

- two parties get to agree on a shared secret (key)
- a third party (could be untrusted) is needed for operation

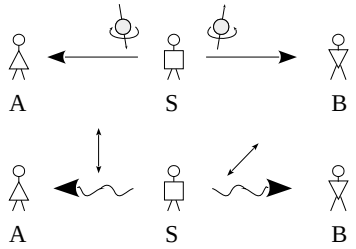
Conditions

- two communication paths are available:
  - one, open but quantum in essence
  - other, classic and public, with only integrity protection
  - both can be eavesdropped
- agreement is statistically achieved
  - if not, the protocol is repeated



Entities

- Alice (receiver)
- Bob (receiver)
- Source (can be untrusted!)



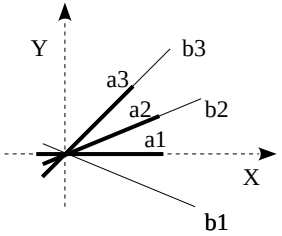
Operation

- Step 1: Entanglement
  - central source generates pairs of **entangled** particles [17]
  - sends one of the pair to Alice, the other to Bob

17 meaning, particles with correlated properties (spin, polarization...); let us suppose photons, but could be electrons, for example

...E91 Protocol...

- Step 2: Measurement
  - Alice and Bob use a set of settings (or basis) for the property's measurement [18]
    - their basis have a specific relation (different angles/bases):
      - Alice's basis: (a1, a2, a3) = (0º, 22.5º, 45º)
      - Bob's basis: (b1, b2, b3) = (-22.5º, 22.5º, 45º)
  - Alice and Bob perform the measurements with a random choice of bases (angles)



18 let us suppose polarization, for photons; would be spin for electrons

Statistical significance

- each of their measurements has an outcome (0 or 1) that is not known for sure
- but their results are correlated according to Quantum Mechanics:
  - correlation E for photons in "singlet state", if measured in bases *a* an *b*:
    - $E(a, b) = -\cos(2*(angle_a - angle_b))$
    - for the Basis used by Alice and Bob, see nearby table (FIG)

Quantum Correlation Table

		Bob		
		b1	**b2**	**b3**
		-22,5	**22,5**	**45**
Alice **a1**	**0**	-0,71	-0,71	0
a2	**22,5**	0	-1	-0,71
a3	**45**	0,71	-0,71	-1

...E91 Protocol...

- Step 3: Public discussion
  - Alice and Bob compare settings (one of the three bases) they used (**not results!**) for each measurement
  - both split data into two groups
    - security test data: cases that will be used for testing correlations (of their settings)
      - correspond to the yellowish correlation values in the Quantum Correlation Table
    - key generation data: cases that will produce the matching, secret bits[19]
      - correspond to the green correlation values in the Quantum Correlation Table

19 really, as their results should be anti-correlated, they should get opposite bits

...E91 Protocol...

- Step 4: Private calculation
  - with Security test data, both Alice and Bob:
    - compute the *E* correlations between their results (real values measured)
    - check if they violate a Bell inequality[20] such as CHSH[21], meaning correlations are stronger than classical physics allows
      - $S = E(a1, b1) + E(a1, b2) + E(a3, b1) - E(a3, b2)$
      - $|S| \leq 2$ for classical particles
        - Violation: genuine quantum entanglement - secure bits can be obtained
        - No violation: possible eavesdropping (or noise) - abort the whole experiment and try again

20 A Bell-type inequality is a variation of the general "theorem" of Bell (1964) that appeared as an inequality. The inequality is built on two core assumptions that define a "classical" world: Locality - an action taken at one location cannot instantly affect an event at a distant location. (Einstein's "no information can travel faster than light") ; Realism - objects have definite properties (like spin or color) even when they aren't being measured. These are often called "hidden variables". If experimental results with particles show that Bell's inequality is not satisfied, Bell's "theorem" is proof that those particles behave as predicted by Quantum Physics and have none whatsoever "hidden variables" as suggested by Einstein and other renowned physicists in the 1930s.

21 CHSH test, meaning "Clauser, Horne, Shimony, Holt" test (1969), is a variation of the original Bell's inequality, that is easier to be put to experimental test. It specifies a statistical calculation of a type of correlation that produces different results depending on the quantum or classical properties of the variables. If the variables behave as predicted in classical (albeit Einsteinian) Physics, the test will produce results under or equal to 2; if the variables behave as predicted in Quantum Mechanics, the test produces results that go as far as $2\sqrt{2}$.

...E91 Protocol...

- Step 5: Key extraction (if no eavesdropping or no noise)
  - keep only results from compatible settings (one of them flips the bits!)
  - these form the shared secret key
- Step 6: Post-processing
  - strictly not part of the E91 protocol, but important in practice
  - Error correction:[22] fix possible mismatches due to measurement imperfection
    - e.g. by publicly exchanging some limited information, such as parity of groups of bits
      - as a down side, some information is leaked
  - Privacy amplification: remove effect of any leaked information
    - e.g. by using as shared key a hash of the original key

22 See ahead section on the need for error-correction in Quantum Cryptography or Computation.

E91 Toy Demo

E91: toy example

	Photon:	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	Obs:
Quantum channel	Source sends Alice	-1	1	-1	1	-1	1	-1	1	1	1	1	1	-1	1	-1	-1	-1 <--> 0
	Source sends Bob	1	-1	1	-1	1	-1	1	-1	-1	-1	-1	-1	1	-1	1	1	
	Alice's filters	a1 (0°)	a2 (22.5°)	a3 (45°)	a1 (0°)	a2 (22.5°)	a1 (0°)	a3 (45°)	a3 (45°)	a1 (0°)	a2 (22.5°)	a1 (0°)	a1 (0°)	a2 (22.5°)	a1 (0°)	a3 (45°)	a2 (22.5°)	
	Alice's measures:	-1	1	-1	1	-1	1	-1	1	-1	1	1	-1	-1	1	-1	-1	
	Bob's filters	b1 (-22.5°)	b2 (22.5°)	b3 (45°)	b3 (45°)	b2 (22.5°)	b1 (-22.5°)	b2 (22.5°)	b1 (-22.5°)	b1 (-22.5°)	b2 (22.5°)	b2 (22.5°)	b2 (22.5°)	b2 (22.5°)	b1 (-22.5°)	b3 (45°)	b1 (-22.5°)	
	Bob's measures:	1	-1	1	1	1	-1	-1	1	1	-1	-1	-1	1	-1	1	-1	
Public "integral" channel	group: ≠ orient	Test			Test		Test	Test	Test	Test		Test	Test		Test		Test	10
	group: = orient		Key	Key		Key					Key			Key		Key		6
Private calculations	E_{a1b1} = E (a1,b1)	(-1*1) /4					(1*(-1)) /4			(-1*1) /4					(1*(-1)) /4			E -1
	E_{a1b2} = E (a1,b2)											(1*(-1)) /2	(-1*(-1)) /2					0
	E_{a3b1} = E (a3,b1)								(1*1) /1									1
	E_{a3b2} = E (a3,b2)							(-1*(-1)) /1										1
	S = $E_{a1b1}+E_{a1b2}+E_{a3b1}-E_{a3b2}$																	**-1**
	secret shared string:		1	0		0					1			0		0		

Fig. E91: toy demonstration of calculations. Difficult to get reasonable results with small samples (here, 16 photon pairs). The final result (|S| = 1) is not usable, as it reveals eavesdropping or too imperfect measures (e.g. due to noise).

E91 vs BB84

- security of both is based on Quantum Physics' (statistical) principles:
  - measurement
    - disturbs the system
    - introduces errors
  - so, Eve must measure to read
    - Eve is detected!
- in E91, security is also based on a most weird principle: entanglement!
  - if Eve interferes:
    - entanglement is disturbed
    - Bell inequality is no longer violated
    - Eve is detected!

Quantum Key Distribution limitations

- requires special channels (fiber, satellites)
- distance (e.g. optical fiber: ~100–300 km, without special techniques)
- hardware complexity

Quantum key distribution (QKD) networks:

- Trusted node networks
  - keys pass through intermediate nodes, e.g. Alice -> Node1 -> Node2 -> Bob
  - each node must be trusted
- Quantum repeater networks
  - use *entanglement* to extend distance
  - no need to trust intermediate nodes
  - Still mostly experimental
  - with satellites: global-scale Quantum key distribution!

Quantum Computation

Need for error-correction!

- qubits are delicate physical states that interact easily with everything around[23]
- qubits loose their quantum properties (superposition and entanglement) by a minimal of such interaction - this phenomenon is "decoherence"
- qubits cannot be copied if they are in a unknown state ("No-cloning theorem")[24]
- operational and propagation errors are common, as quantum logic gates and transmission channels are not perfect
- error accumulate very, very rapidly, as they are small[25] but continuous
- ---> So, quantum error correction is a **must** but has to be done **indirectly** (by spreading the information from one "logic qubit" across several entangled "physical qubits")

23 quite different from "normal", classical bits!
24 traditional redundancy (e, g, Triple Modular Redundancy, keeping three copies of a bit and electing the correct value as the majority of the copies) cannot be used!
25 a qubit can easily undergo a small phase shift, not just a "flip" from 0 to 1

Bibliography

- 1984, C.H. Bennett, G. Brassard, "Quantum cryptography: public key distribution and coin tossing"
  - https://arxiv.org/abs/2003.06557
- 1991, A.K. Ekert, "Quantum Cryptography Based on Bell's Theorem", *Physical Review Letters*, 67(6), 661–663
  - **https://journals.aps.org/prl/abstract/10.1103/PhysRevLett.67.661**
- 2014, J. Martinez-Mateo et al., "Demystifying the Information Reconciliation Protocol Cascade"
  - https://arxiv.org/abs/1407.3257