QKD DEVELOPMENT PROJECTS

Elisabeth Andriantsarazo, Tomáš Novák, Josef Vojtěch

CESNET – Optical networks department

16th Apr 2023

Overview

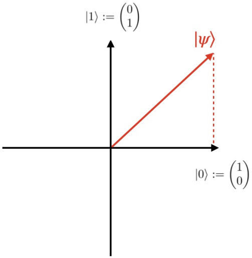
Notation

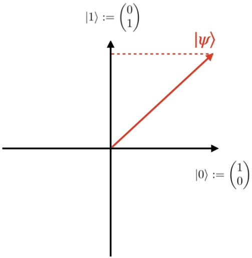
Classical information	Quantum information
bit	qubit
either 0 or 1	superposition
0 1	$\alpha\|0\rangle + \beta\|1\rangle$
measurement yields	measurement yields
0 for 0	0 with probab. $\|\|\alpha\|\|^2$
1 for 1	1 with probab. $\|\|\beta\|\|^2$

Tab.: *Comparison of classical and quantum information.*

Transition to classical bit

Extraction of 0 or 1 bit from qubit means measuring the qubit in the computational basis.





Measurement

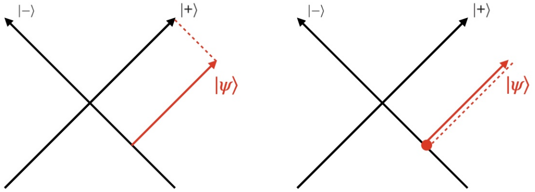


Fig.: *Alternative basis:* $|+\rangle = |\mathbf{0}\rangle + |\mathbf{1}\rangle$ *and* $|-\rangle = |\mathbf{0}\rangle - |\mathbf{1}\rangle$.

Creating a random outcome

We are able to distinguish only orthogonal states, such as $|\mathbf{0}\rangle, |\mathbf{1}\rangle$ or $|+\rangle, |-\rangle$.

BB84

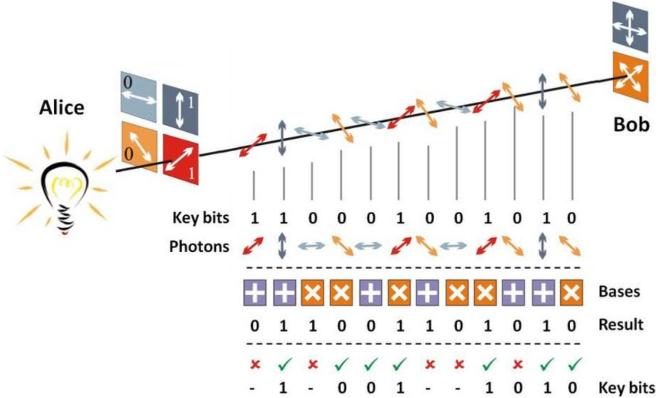


Fig.: *The BB84 prepare and measure QKD protocol. Alice sends to Bob single photons (or other two-level quantum systems), which Bob then measures and extracts information from them.*

How does the BB84 protocol work?

1. Alice encodes her string of bits: **0** as $|\mathbf{0}\rangle, |\mathbf{1}\rangle$ and **1** as $|+\rangle, |-\rangle$
2. Alice sends her string of states to Bob
3. Bob measures each **qubit** in the $|\mathbf{0}\rangle, |\mathbf{1}\rangle$ or in the $|+\rangle, |-\rangle$ basis at random
4. Alice anounces her string of bits
5. Bob discards any bits where a different basis was used for measurement
6. Alice selects a subset of bits to check on eavesdropping by Eve

BB84

1. Alice tells Bob which bits she selected
2. Alice and Bob compare the values
3. If:
   3.1 an acceptable number of bits agree, they continue with the protocol
   3.2 more than an acceptable number of bits disagree, they abort with the protocol
4. If (3.1) was the case, they perform privacy amplification on the remaining bits
5. Alice and Bob now share completely random and secure secret key

BB84

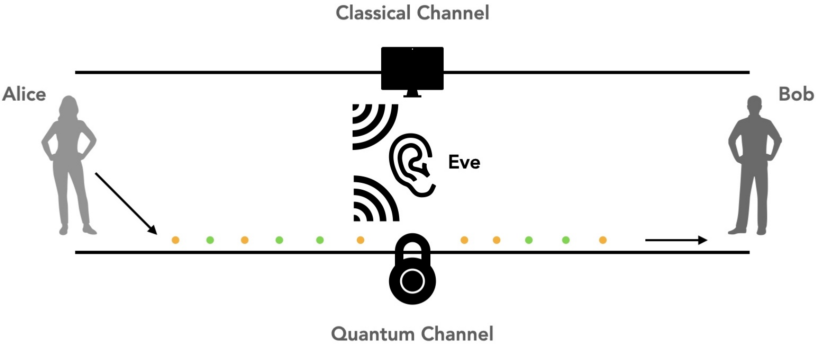


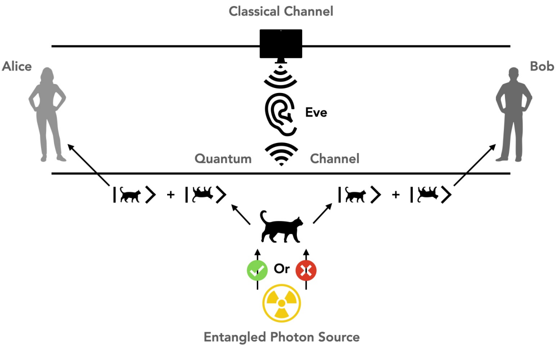
Fig.: *The BB84 prepare and measure QKD protocol. From [2].*

From single particles to entanglement

BBM92

BBM92 – proposed by Bennett, Brassard, and Mermin in 1992

- Entangled version of the BB84 protocol
- Two entangled photons used in communication sent by source – Charlie



Entanglement

Phenomenon of entanglement

- particles cannot be described individually
- state of one particle determines the state of others

Separable state:

$$|D\rangle_1 \otimes |H\rangle_2 = \frac{1}{\sqrt{2}}(|H\rangle_1 + |V\rangle_1) \otimes |H\rangle_2 = \frac{1}{\sqrt{2}}(|HH\rangle + |VH\rangle)$$

Inseparable entangled state:

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|HH\rangle + |VV\rangle)$$

If we know the state of one of the particles we know the state of the other

Entanglement

Bell basis of the entangled states

$$|\boldsymbol{\Phi}^{+}\rangle = \frac{\mathbf{1}}{\sqrt{\mathbf{2}}}(|\boldsymbol{HH}\rangle + |\boldsymbol{VV}\rangle) = \frac{\mathbf{1}}{\sqrt{\mathbf{2}}}(|\boldsymbol{DD}\rangle + |\boldsymbol{AA}\rangle) \quad (1)$$

$$|\boldsymbol{\Phi}^{-}\rangle = \frac{\mathbf{1}}{\sqrt{\mathbf{2}}}(|\boldsymbol{HH}\rangle - |\boldsymbol{VV}\rangle) = \frac{\mathbf{1}}{\sqrt{\mathbf{2}}}(|\boldsymbol{DA}\rangle + |\boldsymbol{AD}\rangle) \quad (2)$$

$$|\boldsymbol{\Psi}^{+}\rangle = \frac{\mathbf{1}}{\sqrt{\mathbf{2}}}(|\boldsymbol{HV}\rangle + |\boldsymbol{VH}\rangle) = \frac{\mathbf{1}}{\sqrt{\mathbf{2}}}(|\boldsymbol{DD}\rangle + |\boldsymbol{AA}\rangle) \quad (3)$$

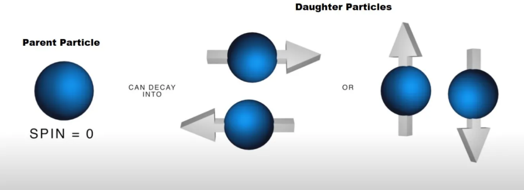
$$|\boldsymbol{\Psi}^{+}\rangle = \frac{\mathbf{1}}{\sqrt{\mathbf{2}}}(|\boldsymbol{HV}\rangle - |\boldsymbol{VH}\rangle) = \frac{\mathbf{1}}{\sqrt{\mathbf{2}}}(|\boldsymbol{AD}\rangle - |\boldsymbol{DA}\rangle) \quad (4)$$

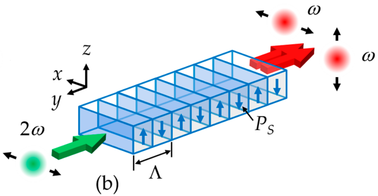
We see correlations or anti-correlation of given Bell state in different H/V or D/A basis

Producing entanglement

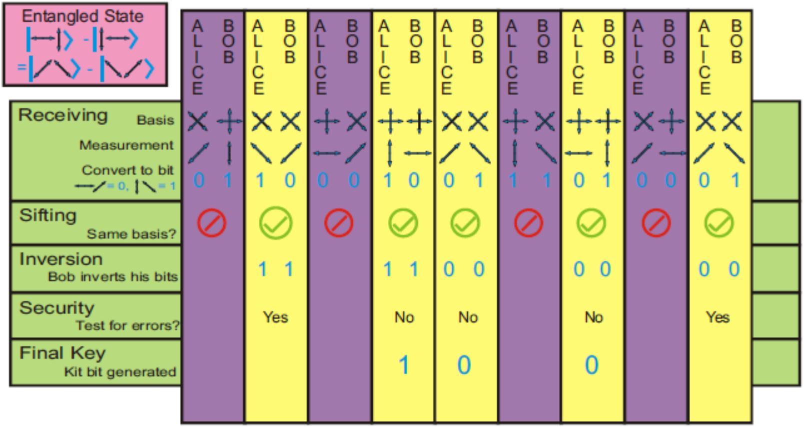
Means of production:

- decay of spin 0 particle into two spin 1/2 particles
- SPDC in non-linear crystals





BBM92


Entangled State
Receiving
Basis
Measurement
Convert to bit
= 0, = 1
Sifting
Same basis?
Inversion
Bob inverts his bits
Security
Test for errors?
Final Key
Kit bit generated
ALICE
BOB
0 1
1 0
0 0
1 0
0 1
1 1
0 1
0 0
0 1
1 1
1 1
0 0
0 0
0 0
Yes
No
No
No
Yes
1
0
0

BBM92

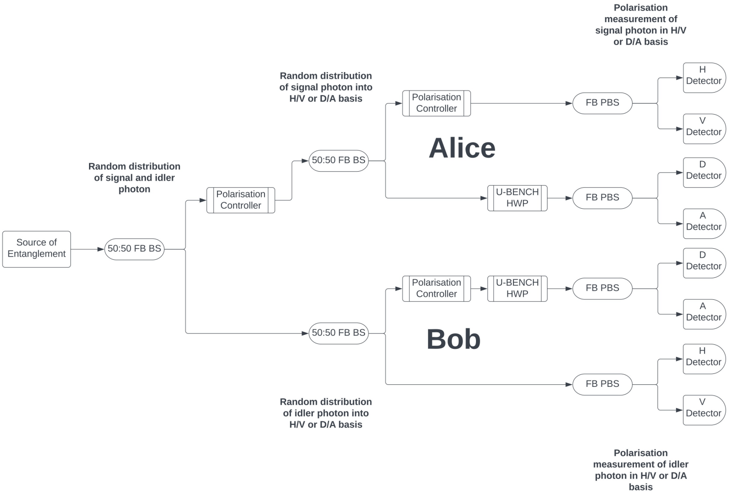
Steps necessary to operate functional QKD protocol

- Random choices of basis at Alice and Bob
- Sifting – classical channel communication to decide if the chosen basis were the same
- Error reconciliation – as the real-life conditions disturbs the entangled state, errors would be present even without Eva listening
- Privacy amplification – sacrificing a piece of the key to produce a matrix, that is multiplying blocks of key
- Quantum bit error rate (QBER) – to detect eavesdropper

The final key is about a third of the length of the received correct coincidence counts

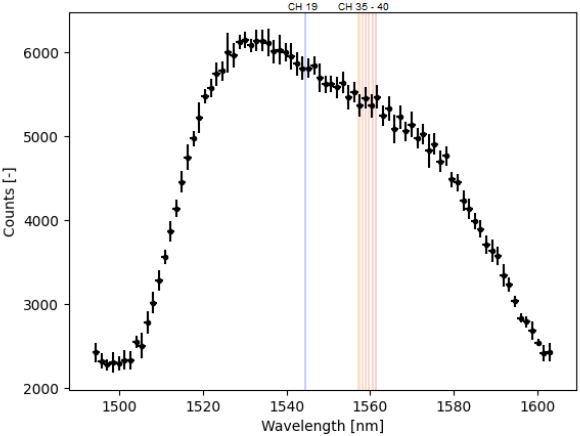
Implementation of BBM92

Almost all-fibered laboratory implementation



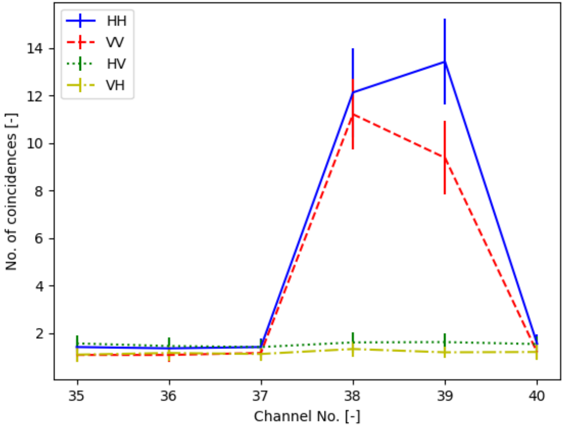
Implementation of BBM92

The measured spectrum of the source by a tunable filter. DWDM channels shown



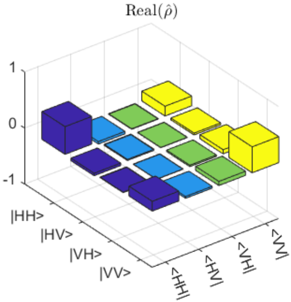
Implementation of BBM92

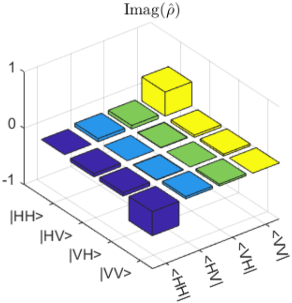
Visibility over the channels of DWDM



Implementation of BBM92

Density matrix – reconstruction of state
$|\Phi\rangle = \frac{1}{\sqrt{2}}(|HH\rangle + e^{-i\varphi}|VV\rangle)$





Implementation of BBM92

Problems

- Polarization changes due to fibered implementation – polarisation controllers
- Chromatic dispersion – use of DWDM
- Polarization mode dispersion – aligning PM fibers

Results

- Average rate of coincidences detected was $\mathbf{(275 \pm 4)}$ counts/s
- Average QBER was $\mathbf{(4.8 \pm 0.7)}$ %
- About $\mathbf{30}$ % of the bits contributed to the final key rate of $\mathbf{(86 \pm 1)}$ bits/s

cesnet

Running QKD projects

Network Security in Post-Quantum Era – NeSPoQ (BUT, TUO, CESNET)

- 2021-2025, provider: Ministry of interior CZ
- Practical application of QKD PQCfor links with **100Gbps** + traffic
- **PQC** (post-quantum cryptography) into FPGA hardware
- Application sponsor: National Cybersecurity Burro - NÚKIB

Running QKD projects

CZ-QCI ISI, CESNET, CTU, MU, UPOL, TUO, BTU
DIGITAL-2021-QCI-01-DEPLOY-NATIONAL

- Connecting Prague-Brno-Ostrava
- Project starting date: 1st Match 2023
- Project end date: 31 August 2026

Running QKD projects

7.6 Mrd € Digital Europe

1.6 Mrd € Cybersecurity

170 M€ Quantum Comm.

3 calls

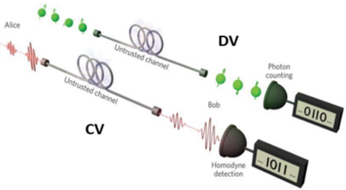
Call 3: DIGITAL-2021-QCI-01-EUROQCI-QKD
2M€, Planning group for future QCI deployment

Call 2: DIGITAL-2021-QCI-01-DEPLOY-NATIONAL
108M€, 5M€ per member state to establish first QKD test-beds

Call 1: DIGITAL-2021-QCI-01-INDUSTRIAL

„Create a European Industrial Ecosystem for Secure QCI technologies and systems“

- 44M€ Total (5-15M€ per project/consortium)
- FR: 50% (75% SME)
- secure (>EAL4), standardized (ETSI, etc.), industrialized QKD-system at TRL 8-9
- integration in existing telecom networks
- Deadline Mar 29, 2022
- Grant Agreement approx. Sep 2022



References

- Nielsen, M.A. and Chuang, I. (2002)
  "Free-Space Quantum Key Distribution."
- Carrasco-Casado, A., Fernández, V. and Denisenko, N., (2016)
  "Free-space quantum key distribution."
  Optical Wireless Communications: An Emerging Technology 589 – 607.
- Picture from Hashdork.com (2023)
  "Quantum Entanglement Explained."
  [online] https://hashdork.com/quantum-computing-entanglement-explained/

References

Ilhwan, K., Donghwa, L. and Kwang, J. L. (2021)
"Study of Type II SPDC in Lithium Niobate for High Spectral Purity Photon Pair Generation."

Picture from Wikipedia.com (2023)
"BBM92 protocol"
[online]
https://en.wikipedia.org/wiki/BBM92_protocol