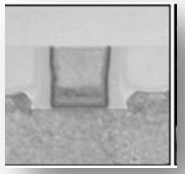
Quantum Information Processing

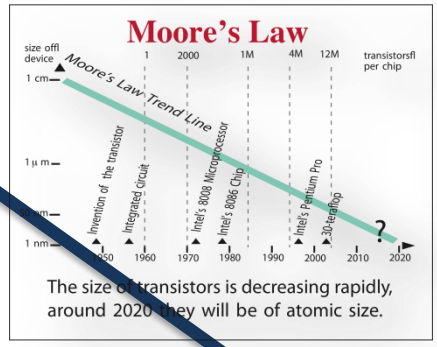
Raymond Laflamme
Executive Director
Institute for Quantum Computing
www.iqc.ca

Founding Member, Perimeter Institute
CSO, Universal Quantum Devices

MRI



Intel's 22 nm transistor



The size of transistors decreases by half every eighteen months

Laser

Quantum Mechanics

-Energy quantization, tunneling and wave/particle duality

Information Theory

The Superposition principle:
Quantum systems can be in more than one state at once

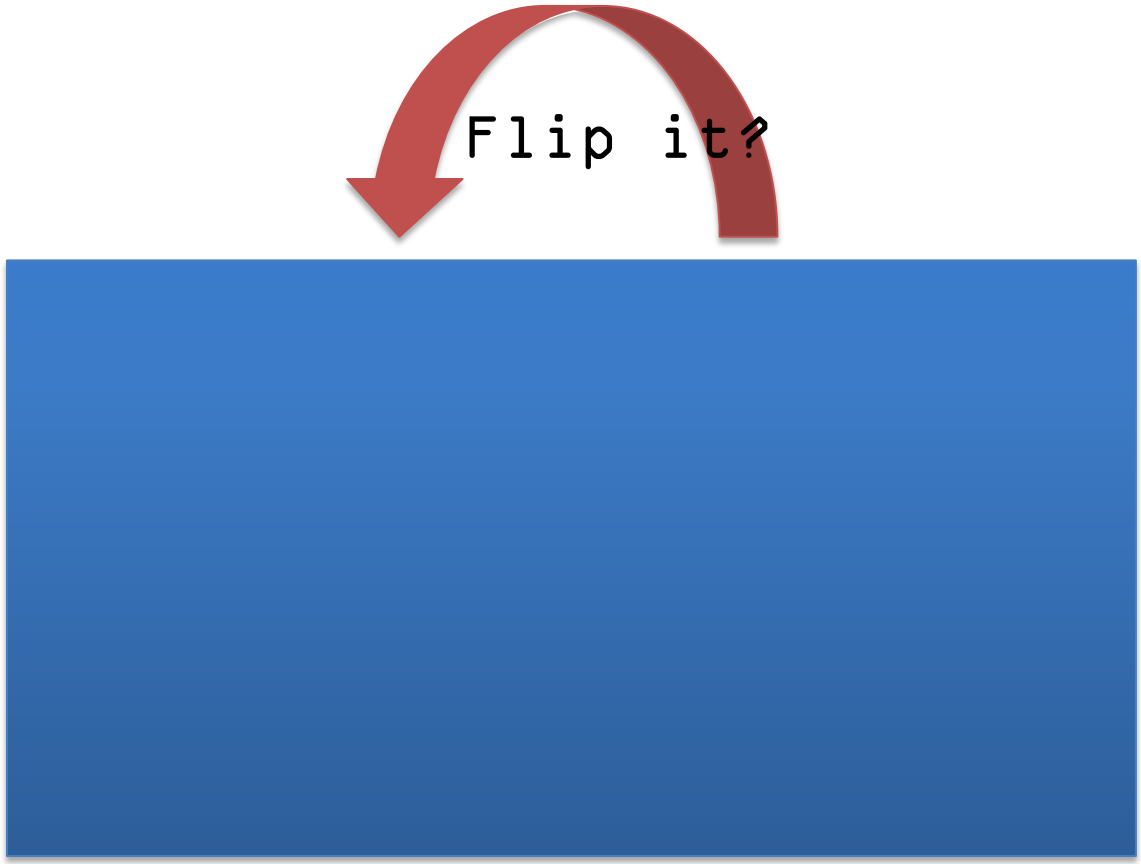
The Uncertainty principle:
Observing quantum systems cannot be done without perturbing them

A Quantum game

One where you can't lose!

A Quantum game

A Quantum game

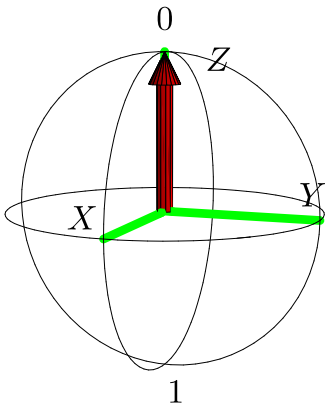


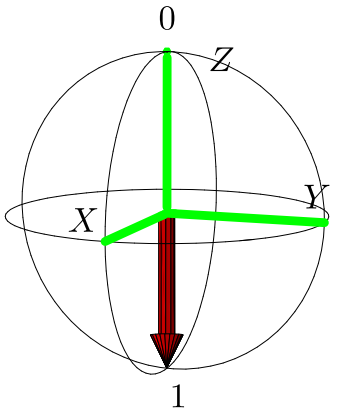
A Quantum game

A Quantum game

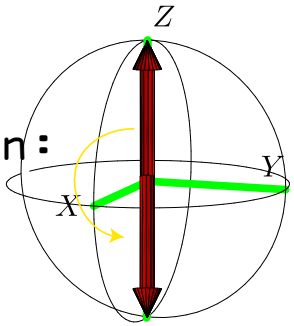
I have 50% chance of winning

A Quantum game



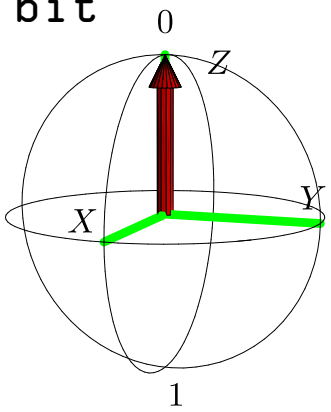


Flipping the coin:

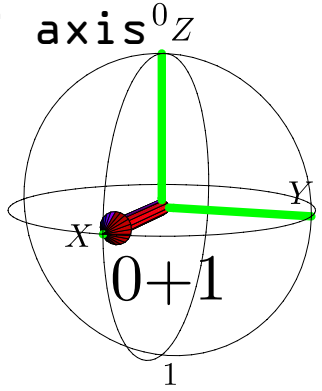


A Quantum game

Take a quantum bit

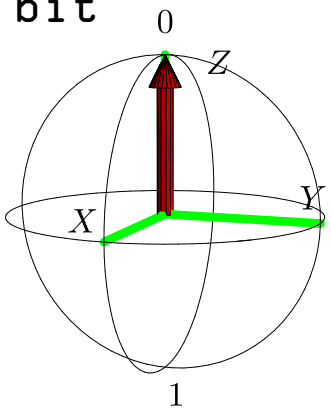


Rotate around the Y axis

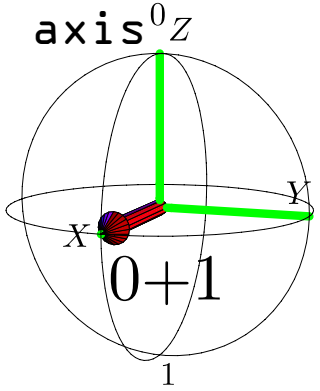


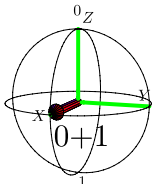
A Quantum game

Take a quantum bit

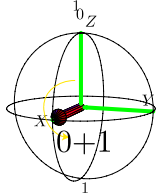


Rotate around the Y axis





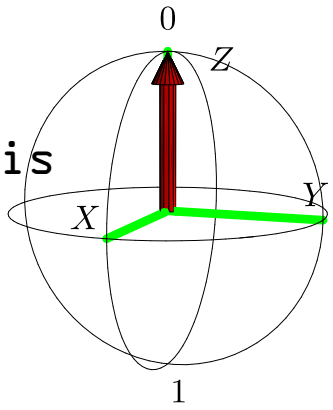
- No Flip the state is 0+1



- Flip the state is 1+0 =0+1

A Quantum game

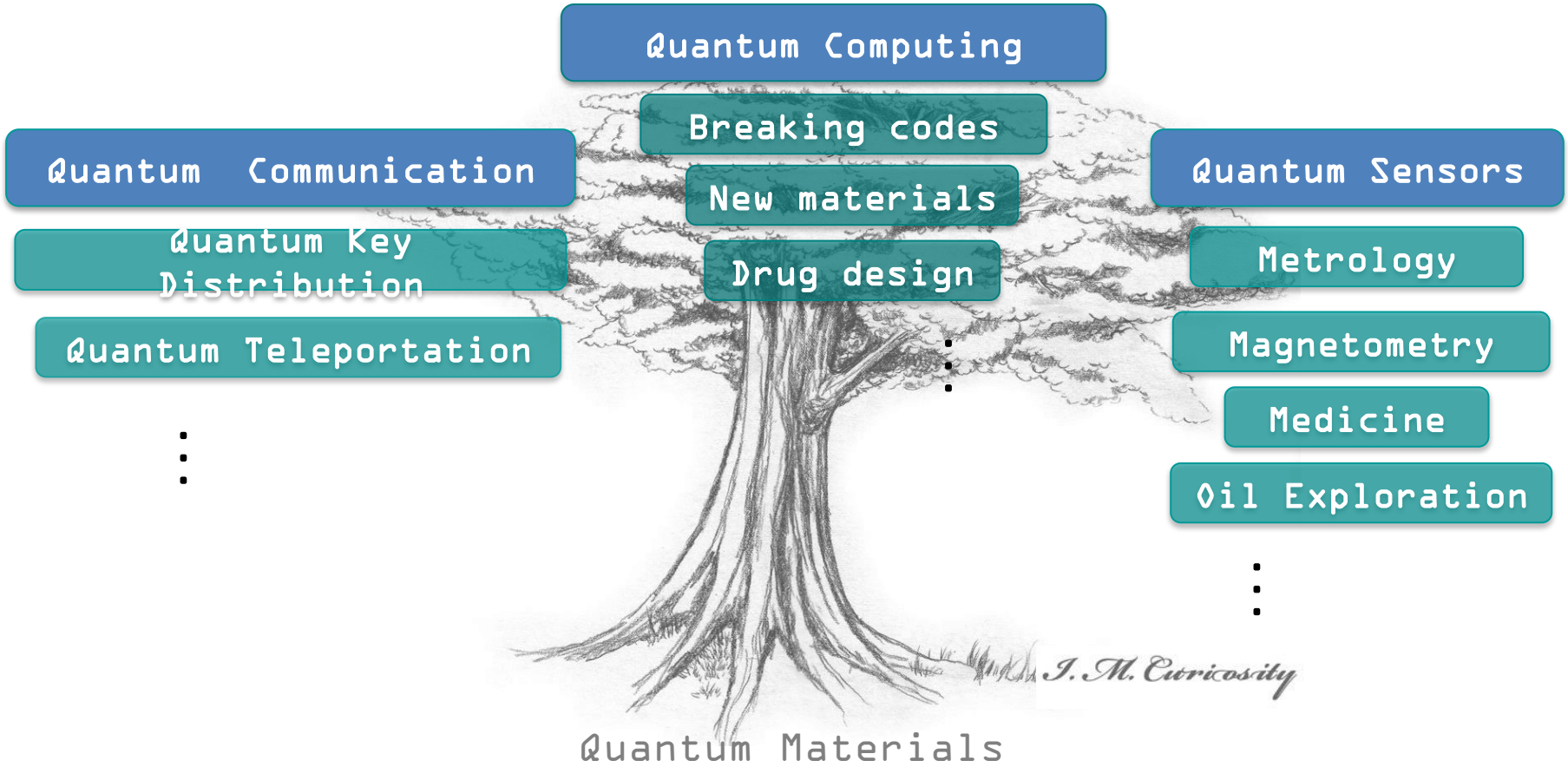
Rotate back around the Y axis



And know the answer

The Quantum Tree

Applications of quantum information science and technology



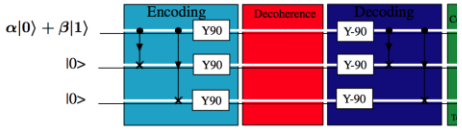
How can we build quantum computers?

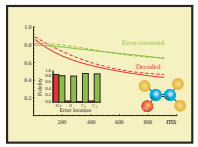
- A system that has quantum bits and has scalable architecture
- Controlling the qubits
  - Initializing them
  - Evolution (one and two qubit gates)
  - Measurement
  - All this with relatively small noise

Controlling quantum devices

Adapt our control methods for the laws of quantum mechanics

Development of Quantum Error Correction has been seen as a breakthrough and [illegible] experimental





(Error rate $\epsilon \rightarrow c\epsilon^2$)

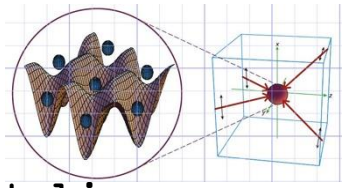
1998:
T2: H= 3s , C1=1.1s, C2=0.6s
DE: $0.85 - 1.10t + O(t^2)$
EC: $0.79 - 0.09t + O(t^2)$

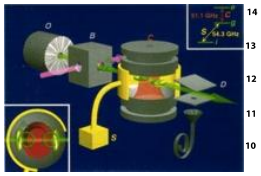
2011: (J. Zhang, et al R.L., PRA 84, 034303, 2011)
T2: H= 1.7s , C1=1.18s, C2=0.45s
DE: $0.99 - 0.436t + O(t^2))$
EC: $0.98 - 0.017t + O(t^2)$

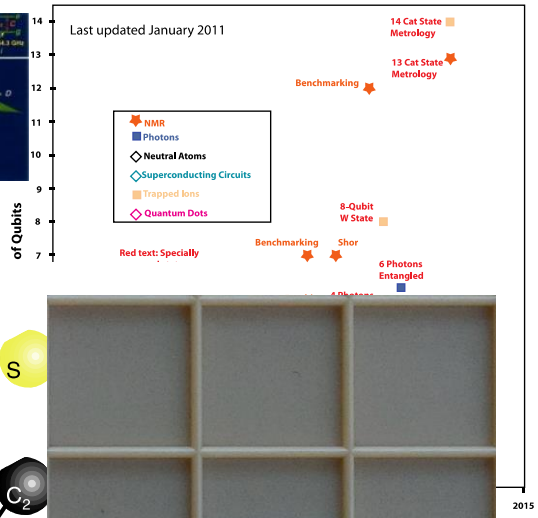
A cornerstone is the Accuracy Threshold Theorem which says that as long as the error rate is smaller than a threshold it is possible to manage errors from imperfection and imprecision of realistic devices.

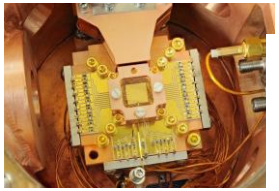
List of devices

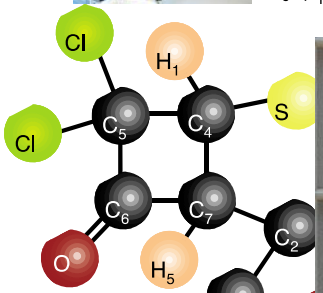
- Atom Traps
- Cavity QED
- Electron Floating on Helium
- Electron trapped by surface acoustic waves
- Ion Traps
- Electron & Nuclear Magnetic Reso
- NV centers in diamond
- Quantum Dots
  - Quantum Optics
  - Spintronics
    - Superconducting Josephson Junctions

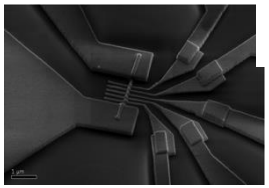




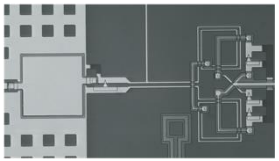




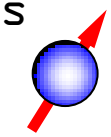
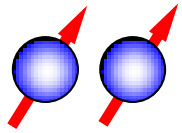
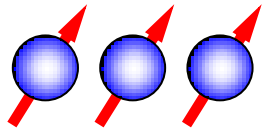
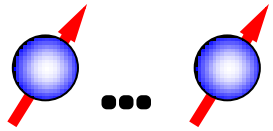




		Date
		2011
		2009
		2010
		2011
		2009
Single Trapped Ion	$4.8(2) \times 10^{-3}$	2008
Solid State NMR	$5(2) \times 10^{-3}$	2011
Superconducting Transmon	$7(5) \times 10^{-3}$	2010



Quantum Computers

# of Quantum bits (Qubits)		Quantum states	# of classical bits
1		0, 1	$2^1=2$
2		00, 01, 10, 11	$2^2=4$
3		000, 001, …111	$2^3=8$
⋮			
50		00000000000 0…	$2^{50}=1P$

The power of the superposition principle

What can we do with quantum computers?

- Simulation of quantum physics
  - Physics, Chemistry, Material Science
- Computer science
  - Searching
  - Solving mathematical equation,
    e.g. Pell's equation $x^2 - dy^2 = 1$,
    where d is a square-free integer
  - Quantum Random Walk and quickly traverse networks
    - Factoring, elliptic curves, elliptic curves is
      - …

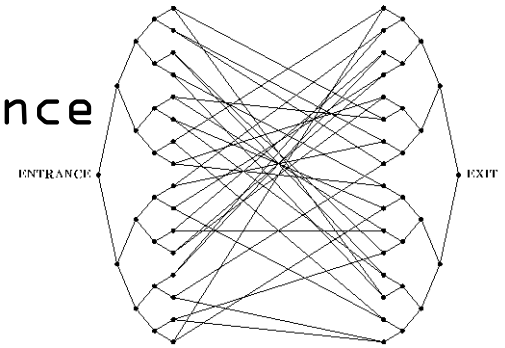


FIG. 15: The modified graph of Fig. 11. A big random cycle has been inserted between the two binary trees. This makes the classical task of penetrating the graph from root to root exponentially hard [27].

Quantum communication

Taking advantage of QM to communicate

- Quantum teleportation: how to transfer information from one location to another without going through the intervening space
- Quantum secret sharing
- Quantum digital signature
- But the best known is quantum key distribution

Alice

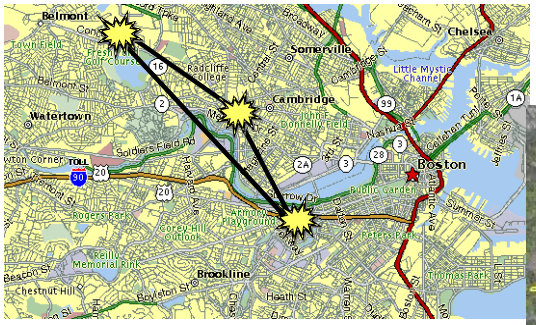
message 10101110
key 01110011
---
encrypted message 11011101

encrypted message 11011101
key 01110011
---
message 10101110

Bob

The power of the uncertainty relation

QKD local network around the world

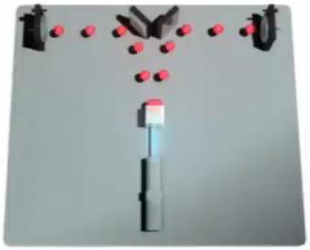


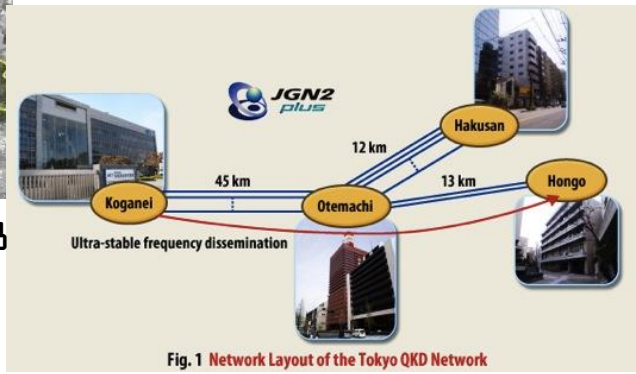
BBN Network 2004

www.bbn.com

European network 2008

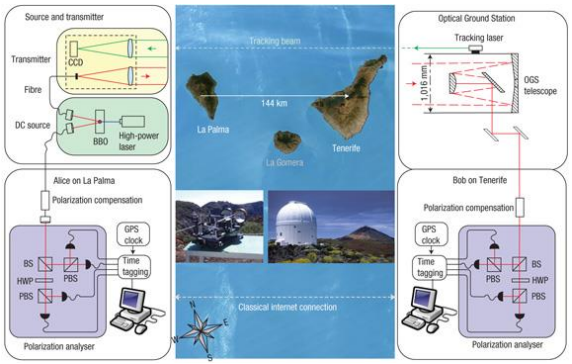
www.secoqc.net





Japanese network 2010

www.uqcc2010.org



Canarie Island experiment

http://www.nature.com/nature/journal/v489/n7415/full/nature11472.ht

QKD at IQC

COM DEV

INO

Canadian Space Agency | Agence Spatiale Canadienne

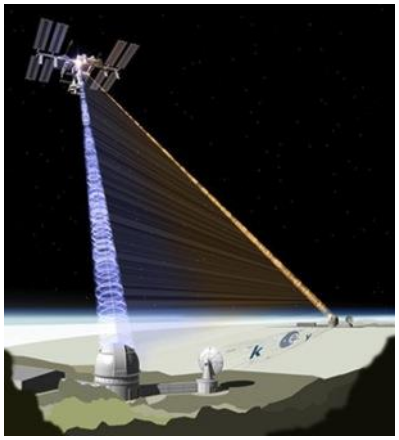
FedDev Ontario

COMMUNITECH

UNIVERSITY OF WATERLOO | IQC Institute for Quantum Computing

Satellite QKD

- Several Nations and Agencies have conducted studies on the feasibility of quantum communications with satellites
  - **USA:** design study and proof-of-concept experiments, patents
  - **ESA:** feasibility, design and proof-of-concept experiments, some HW development underway (Space-QUEST, ISS), demonstration of quantum ground station
  - **Canada:** feasibility study, design and proof-of-concept
  - **Japan:** collaboration in Space-QUEST & limited quantum-demonstrator within an optical communications payload already under way
  - **China:** feasibility and development of HW for QKD satellite under way (collaboration with Vienna group)
  - **UK:** feasibility study and conceptual design



Steps towards commercial QKD

- Increase distance of operation and develop approaches for networks

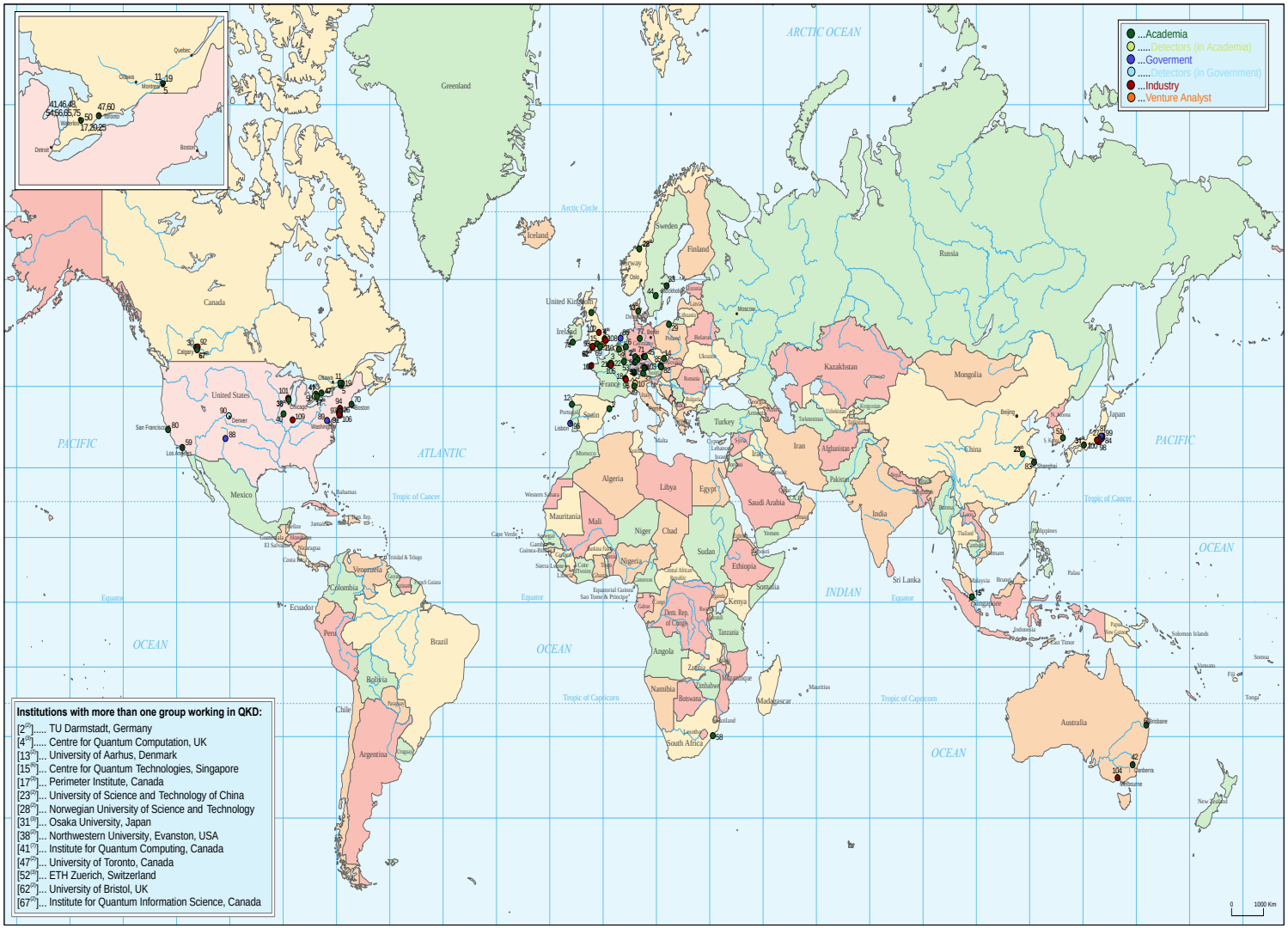
- Certification

ETSI 2013 Celebrating 25 years

- Establish Standards

IQC
Institute for Quantum Computing

Quantum Cryptography Groups Worldwide



Institutions with more than one group working in QKD:

[2[2]]..... TU Darmstadt, Germany
[4[2]]..... Centre for Quantum Computation, UK
[13[2]]... University of Aarhus, Denmark
[15[6]]... Centre for Quantum Technologies, Singapore
[17[3]]... Perimeter Institute, Canada
[23[2]]... University of Science and Technology of China
[28[2]]... Norwegian University of Science and Technology
[31[2]]... Osaka University, Japan
[38[2]]... Northwestern University, Evanston, USA
[41[7]]... Institute for Quantum Computing, Canada
[47[2]]... University of Toronto, Canada
[52[2]]... ETH Zuerich, Switzerland
[62[2]]... University of Bristol, UK
[67[2]]... Institute for Quantum Information Science, Canada

1..... A. Acin, Spain
2[2]..... G. Alber, Germany
3..... R. Alléaume, France
4[3]..... J. Barrett, UK
5..... G. Brassard, Canada
6..... D. Bruss, Germany
7..... G. Buller, Scotland
8..... N. Cerf, Belgium
9 [4[2]]..... M. Christandl, UK
10..... S. Cova, Italy
11..... C. Crepeau, Canada
12..... M. Curty, Spain
13[2]..... I. Damgard, Denmark
14..... M. Dusek, Czech Republic
15[6]..... A. Ekert, UK/Singapore
16 [15[6]]. B. Englert, Singapore
17[3]..... Ch. Fuchs, Canada
18..... N. Gisin, Switzerland
19..... N. Godbout, Canada
20 [17[3]]. D. Gottesman, Canada
21..... P. Grangier, France
22..... F. Grosshans, France
23[2]..... Guan-Can Guo, China
24 [23[2]]. Zheng-Fu Han, Chin
25 [17[3]]. L. Hardy, Canada
26..... M. Hillery, USA
27..... O. Hirota, Japan
28[2]..... D. Hjelme, Norway
29..... M. Horodecki, Poland
30..... St. Hosier, Canada
31[3]..... N. Imoto, Japan
32 [31[2]]. K. Inoue, Japan
33..... A. Karlsson, Sweden
34 [15[6]]. D. Kaszlikowski, Singapore
35 [4[3]]... A. Kent, UK
36 [31[2]]. M. Koashi, Japan
37..... B. Kraus, Austria
38[2]..... P. Kumar, USA
39 [15[6]]. C. Kurtsiefer, Singapore
40..... P. Kwiat, USA
41[7]..... R. LaFlamme, Canada
42..... P.-K. Lam, Australia
43 [15[6]]. A. Lamas-Limares, Singapore
44..... J.-A. Larsson, Sweden
45..... G. Leuchs, Germany
46 [41[7]]. D. Leung, Canada
47[2]..... Hoi-Kwong Lo, Canada
48 [41[7]]. N. Luetkenhaus, Canada
49..... Ch. Macchiavello, Italy
50..... H. Majedi, Canada
51..... V. Makarov, South Korea
52[2]..... U. Maurer, Switzerland
53..... J.-M. Merolla, France
54 [41[7]]. M. Mosca, Canada
55..... J. Mueller-Quade, Germany
56 [41[7]]. A. Nayak, Canada
57..... J.-W. Pan, Germany/China
58..... F. Petruccione, South Africa
59..... J. Preskill, USA
60 [47[2]]. Li Qian, Canada
61..... T. Ralph, Australia
62[2]..... J. Rarity, UK
63 [2[2]]... J. Renes, Germany
64 [4[2]]... R. Renner, Switzerland
65 [41[7]]. K. Resch, Canada
66 [13[2]]. L. Salvail, Denmark
67[2]..... B. Sanders, Canada
68 [15[6]]. V. Scarani, Singapore
69..... R. Schack, UK
70..... A. Sergienko, USA
71..... C. Silberhorn, Germany
72 [28[2]]. J. Skaar, Norway
73 [67[2]]. W. Tittel, Canada
74..... P. D. Townsend, Eire
75 [41[7]]. G. Weihs, Canada
76..... H. Weinfurter, Germany
77..... R. Werner, Germany
78 [62[2]]. A. Winter, UK
79 [4[2]]... St. Wolf, Switzerland
80..... Y. Yamamoto, USA
81 [38[2]]. H. Yuen, USA
82..... A. Zeilinger, Austria
83..... H. Zeng, China
84..... AIST, A. Yoshizawa, Japan
85..... ARC, Ch. Monyk, Austria
86..... CWI, Ch. Schaffner, Netherl.
87..... ERATO-SORST, H. Imai, Japan
88..... LANL, R. J. Hughes, USA
89..... NIST, J. Bienfang, USA
90..... NIST, S.-W. Nam, USA
91..... AT&T, M. Brodsky, USA
92..... General Dynamics, Canada
93..... HP, B. Munro, UK
94..... IBM, CH. Bennett, USA
95..... ID-Quantique, Switzerland
96..... IT, P. Mateus, Portugal
97..... Magiq Technologies, USA
98..... Mitsubishi Electric, Japan
99..... NEC, A. Tomita, Japan
100..... NTT, H. Takesue, Japan
101..... Nucrypt, P. Kumar, USA
102..... Qinetiq, B. Lowans, UK
103..... Qutools, Germany
104..... Senetas, Australia
105..... SmartQuantum, France
106..... Telecordia, P. Toliver, USA
107..... Thales, France
108..... Toshiba, A. Shields, UK
109..... MITRE, G. Gilbert, USA
110..... Quantum Inf. Partners, UK

Quantum sensors

Neutron interferometry

Collaboration of IQC, NIST and Brockhouse Institute

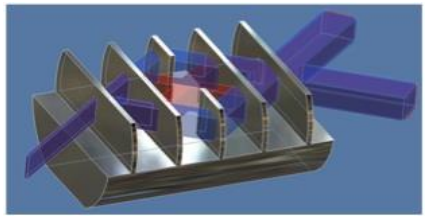
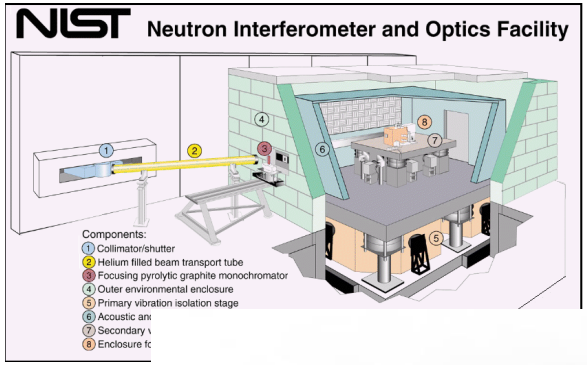
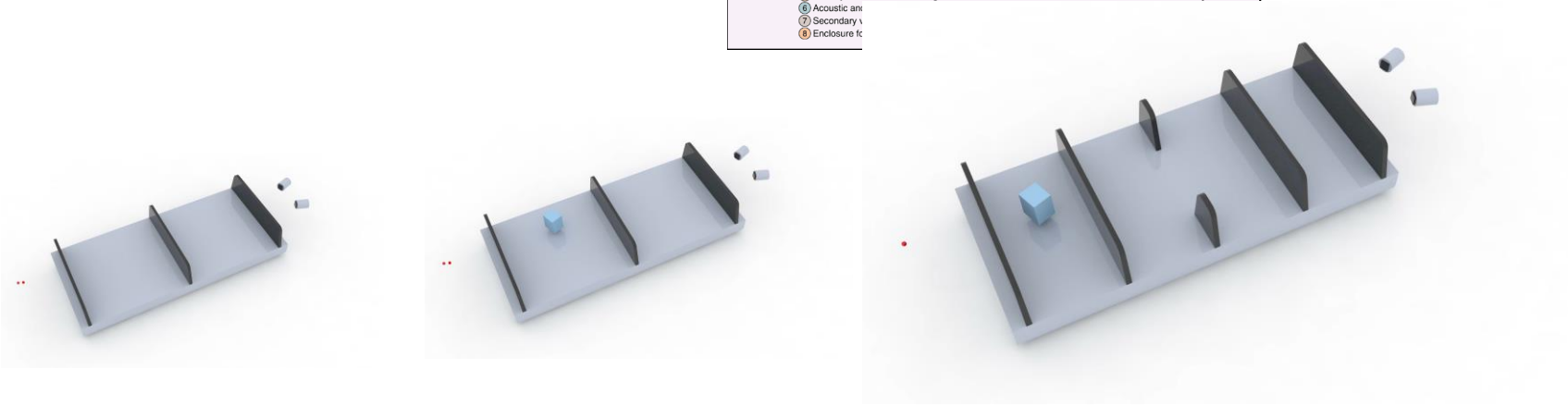
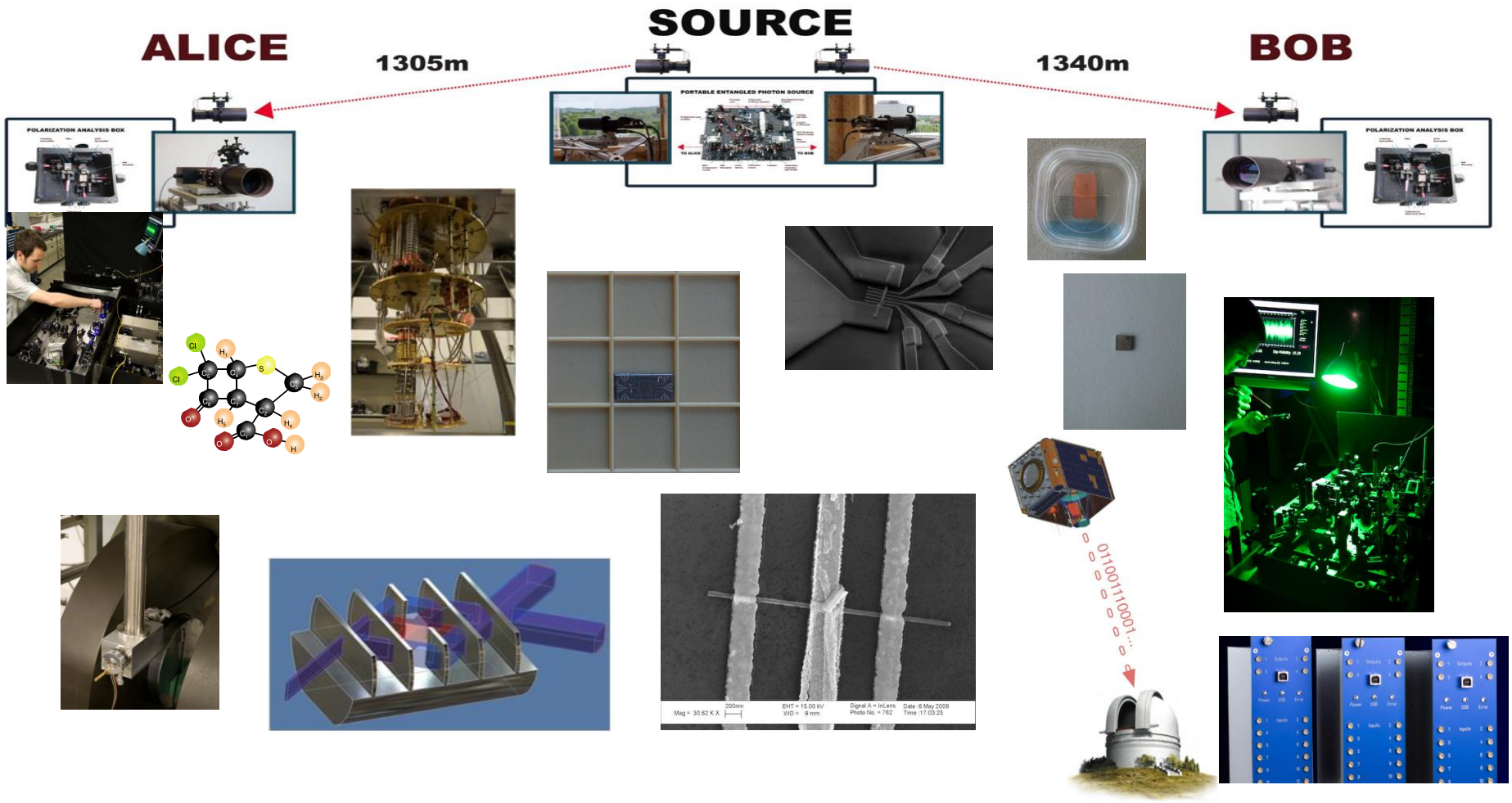


Figure from D. Pushin





Conclusion


ALICE
1305m
SOURCE
1340m
BOB
POLARIZATION ANALYSIS BOX
PORTABLE ENTANGLED PHOTON SOURCE
TO ALICE
TO BOB
POLARIZATION ANALYSIS BOX
011001110001...

Conclusion

IBM

TOSHIBA
Leading Innovation

Los Alamos
NATIONAL LABORATORY
EST. 1943

JOINT QUANTUM INSTITUTE

Institute for Quantum Information

MagiQ

OXFORD QUANTUM
A core for quantum science and technology

IQI

Sandia National Laboratories

hp

Quantum Valley
INVESTMENTS

UQDevices

Quantum Wave Fund
Riding the wave of quantum technology revolution

COM DEV

• • •

Thank you

Ontario

Industry Canada Industrie Canada

Canada

Quantum Teleportation

Bennet & al. PRl 1993

Nielsen, Knill & Laflamme, Nature, Nov 1998