Quantum Computing and Quantum Communications at LANL

Rolando D. Somma
Theory Division
Los Alamos National Laboratory
somma@lanl.gov
LA-UR-13-28120

WWRF31– Vancouver
October 22, 2013

Quantum Computing and Quantum Communications at LANL

Rolando D. Somma

Theory Division

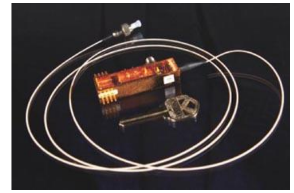
Los Alamos National Laboratory

somma@lanl.gov

LA-UR-13-28120

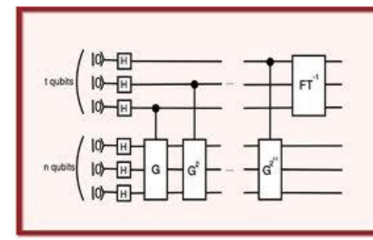
WWRF31– Vancouver

October 22, 2013



Richard Hughes

Quantum communications



Rolando Somma

Quantum computing

Cristian Batista Malcolm Boshier

Condensed matter and BECs

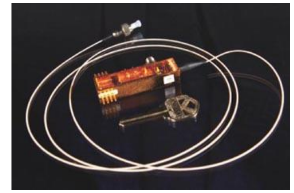
Wojciech Zurek

Decoherence & Foundations

Los Alamos
NATIONAL LABORATORY
EST. 1943

Quantum efforts and some people at LANL

LDRD

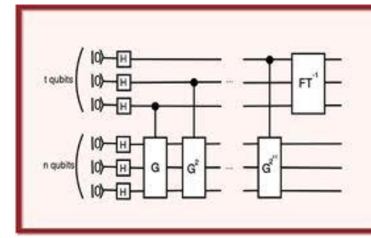



Richard Hughes

Quantum communications


Wojciech Zurek

Decoherence & Foundations

Rolando Somma

Quantum computing


Cristian Batista Malcolm Boshier

Condensed matter and BECs

Quantum efforts and people at LANL

Topics, Collaborations, and Funding

- **Quantum computing**
  - Quantum algorithms for optimization
  - Adiabatic quantum computation
  - Collaborations with Sandia National Laboratories – AQUARIUS Project
  - Funding: SNL, AFOSR, NSF
  - Rolando Somma (LANL), Andrew Landahl (SNL), Anand Ganti (SNL)

- **Quantum communications**
  - Quantum cryptography: network communications, long distance QKD, fast random number generation
  - Funding: LDRD, DARPA
  - Rolando Somma, Richard Hughes, Beth Nordholt, Ray Newell, Glen Peterson (LANL)

- **Condensed matter theory**
  - Quantum phase transitions
  - Exact solvability and efficient computational methods
  - Funding: LDRD
  - Rolando Somma, Cristian Batista (LANL)

Los Alamos NATIONAL LABORATORY EST. 1943

LDRD

Topics, Collaborations, and Funding

- **Quantum computing**
  - **Quantum algorithms for optimization**
  - Adiabatic quantum computation
  - Collaborations with Sandia National Laboratories – AQUARIUS Project
  - Funding: SNL, AFOSR, NSF
  - Rolando Somma (LANL), Andrew Landahl (SNL), Anand Ganti (SNL)

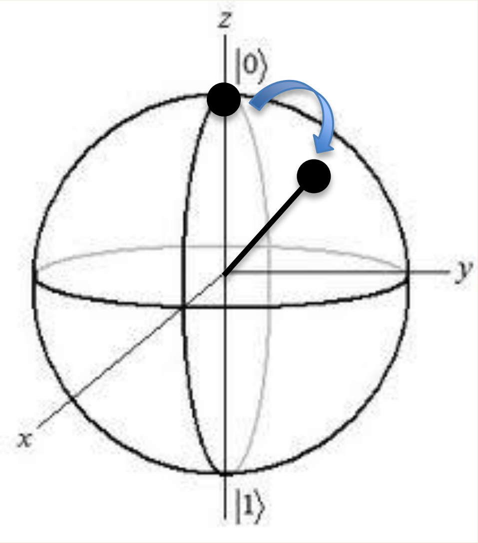
- **Quantum communications**
  - **Quantum cryptography: network communications**, long distance QKD, fast random number generation
  - Funding: LDRD, DARPA
  - Rolando Somma, Richard Hughes, Beth Nordholt, Ray Newell, Glen Peterson (LANL)

- **Condensed matter theory**
  - Quantum phase transitions
  - Exact solvability and efficient computational methods
  - Funding: LDRD
  - Rolando Somma, Cristian Batista (LANL)

Los Alamos NATIONAL LABORATORY EST. 1943

LDRD

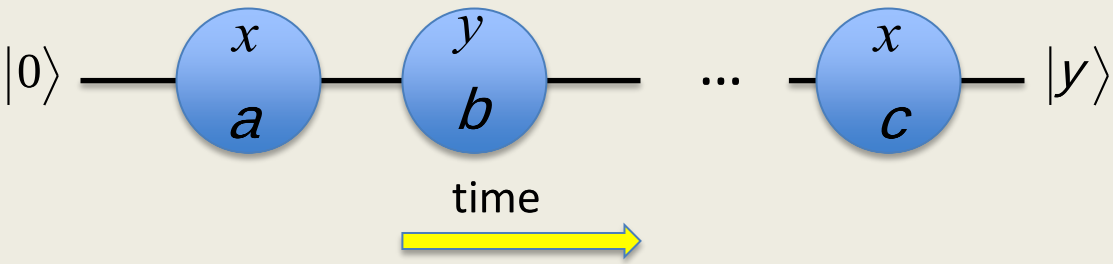
Quantum algorithms



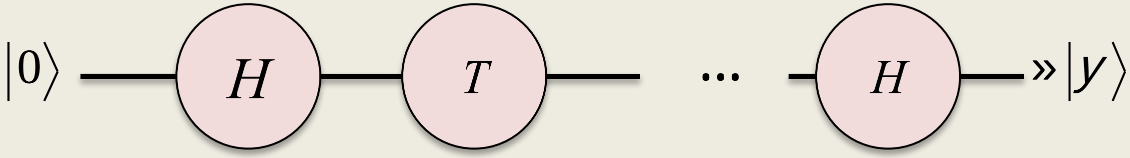
Instead of bits we have qubits: $|\psi\rangle = a|0\rangle + b|1\rangle$ with $|a|^2 + |b|^2 = 1$

One-qubit operations: Rotations/Reflections in Bloch sphere

One-qubit circuits:



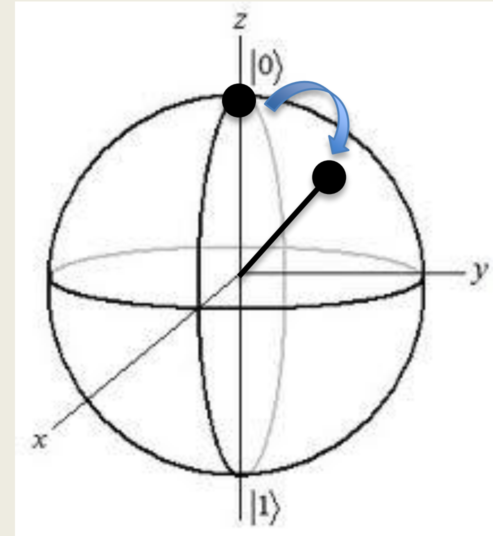
Universal set of one-qubit (unitary) operations: $H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$; $T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}$



Los Alamos NATIONAL LABORATORY EST. 1943

LDRD

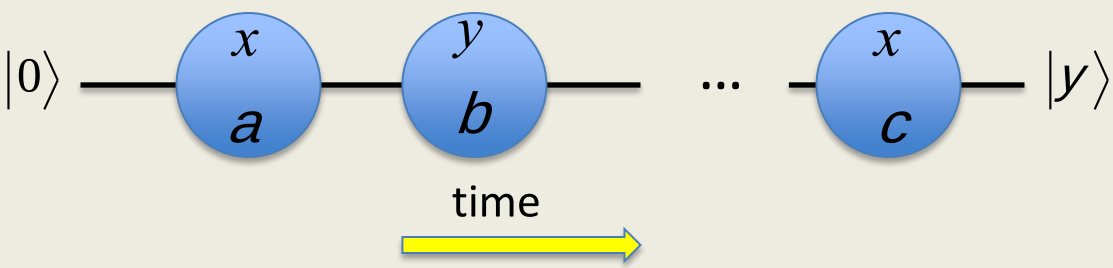
Quantum algorithms



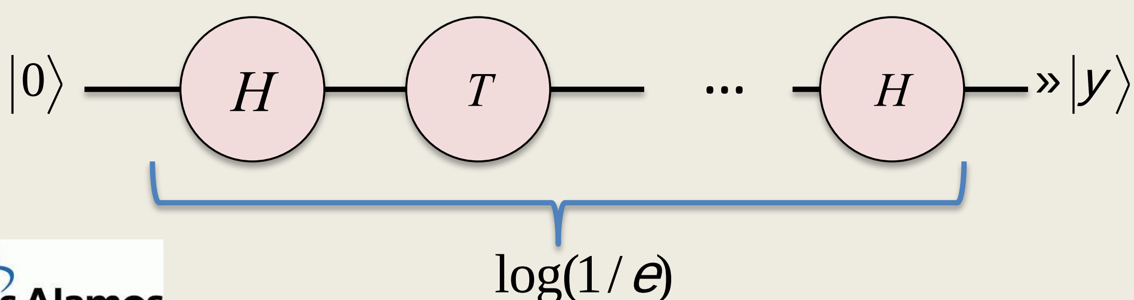
Instead of bits we have qubits: $|\psi\rangle = a|0\rangle + b|1\rangle$ with $|a|^2 + |b|^2 = 1$

One-qubit operations: Rotations/Reflections in Bloch sphere

One-qubit circuits:



Universal set of one-qubit (unitary) operations: $H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$; $T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}$

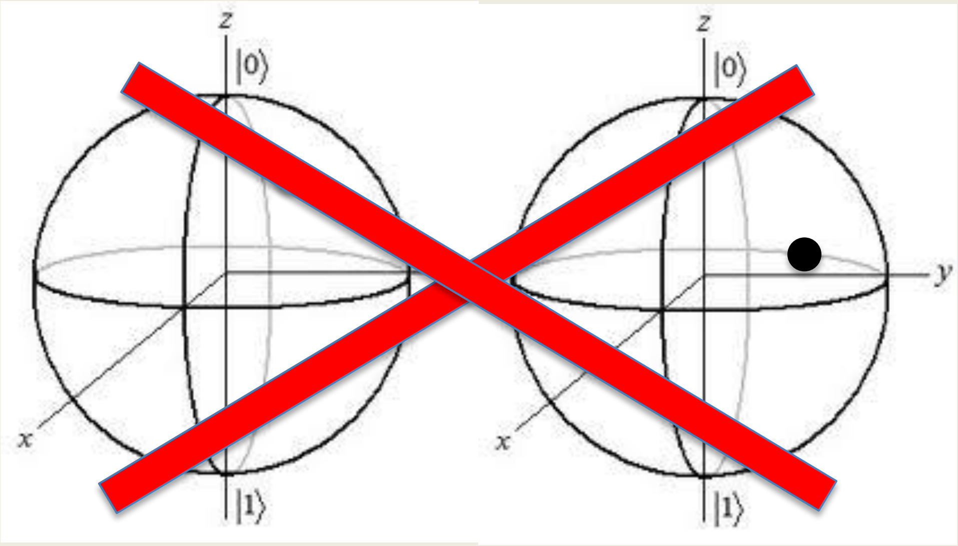


$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$; $|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$

Quantum algorithms

Two qubit states: $|\psi\rangle = a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle$ with $|a|^2 + |b|^2 + |c|^2 + |d|^2 = 1$

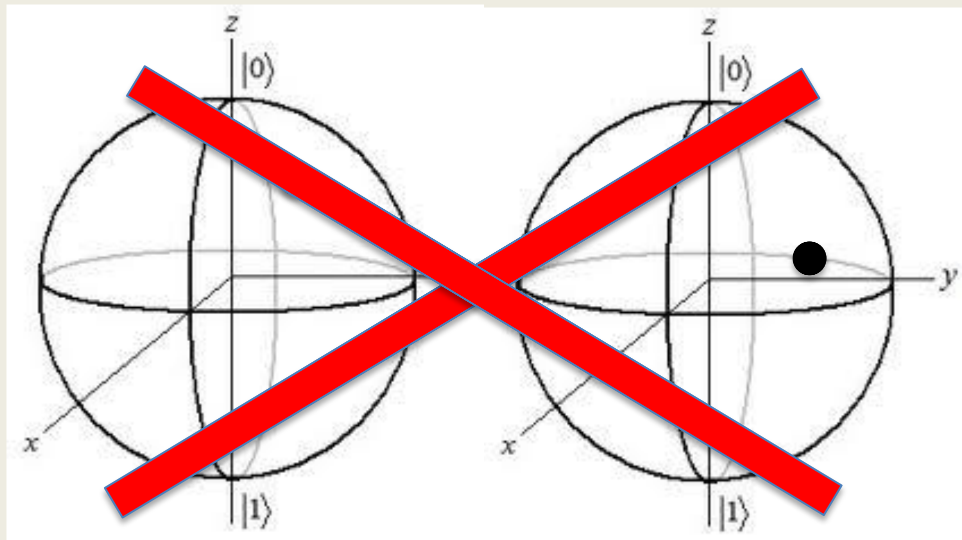
Two-qubit operations: Controlled operations or "entangling gates"



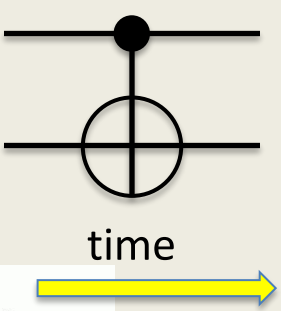
Quantum algorithms

Two qubit states: $|\psi\rangle = a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle$ with $|a|^2 + |b|^2 + |c|^2 + |d|^2 = 1$

Two-qubit operations: Controlled operations or "entangling gates"



Example: Controlled not



$$c - NOT = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

$$|00\rangle = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix};\ |01\rangle = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix};\ldots$$

Quantum algorithms

Many-qubit states:

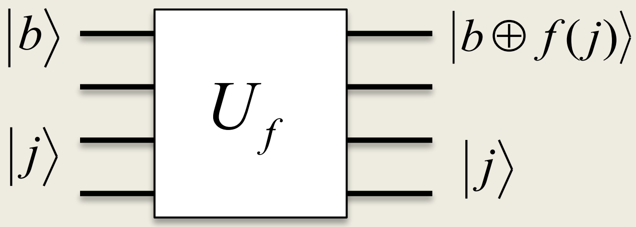
$$|\psi\rangle = \sum_{j=0}^{2^n-1} a_j |j\rangle \;\; ; \;\; \sum_{j=0}^{2^n-1} |a_j|^2 = 1$$

Quantum algorithms

Many-qubit states:

$$|\psi\rangle = \sum_{j=0}^{2^n-1} a_j |j\rangle \ ; \ \sum_{j=0}^{2^n-1} |a_j|^2 = 1$$

In the quantum oracle model, we also assume access to a black box. s.t.

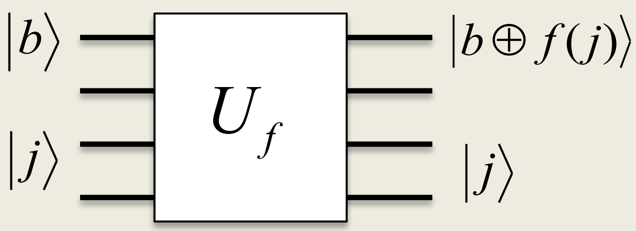


Quantum algorithms

Many-qubit states:

$$|\psi\rangle = \sum_{j=0}^{2^n-1} a_j |j\rangle \; ; \; \sum_{j=0}^{2^n-1} |a_j|^2 = 1$$

In the quantum oracle model, we also assume access to a black box. s.t.



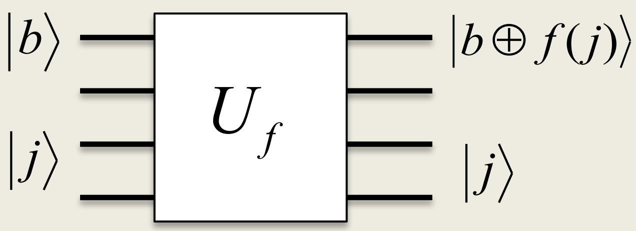
Theorem: H, T, and c-NOT are universal, i.e., they can implement any n-qubit unitary operation

Quantum algorithms

Many-qubit states:

$$|\psi\rangle = \sum_{j=0}^{2^n-1} a_j |j\rangle \;\; ; \;\; \sum_{j=0}^{2^n-1} |a_j|^2 = 1$$

In the quantum oracle model, we also assume access to a black box. s.t.



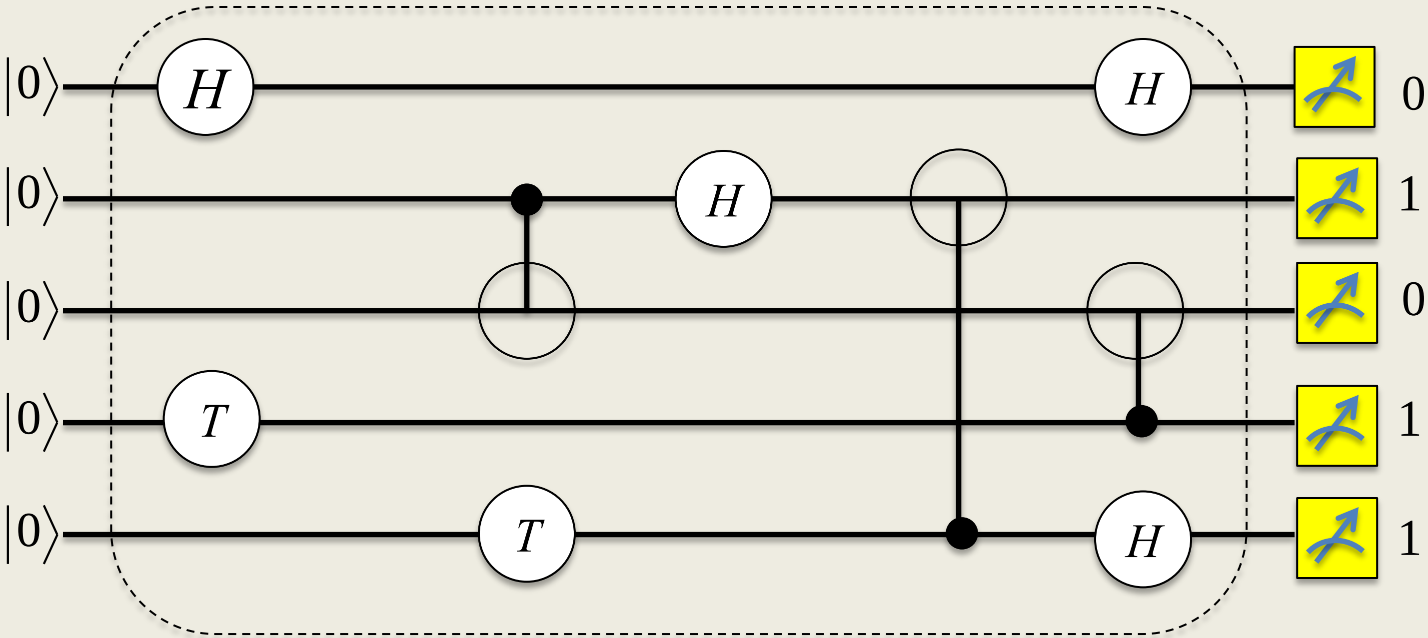
Theorem: H, T, and c-NOT are universal, i.e., they can implement any n-qubit unitary operation

Measurement: To obtain classical information, a quantum state has to be observed

Born's rule: $\Pr(j) = |a_j|^2 \longrightarrow$ "collapse of wave function"

$$|\psi\rangle \rightarrow |j\rangle$$

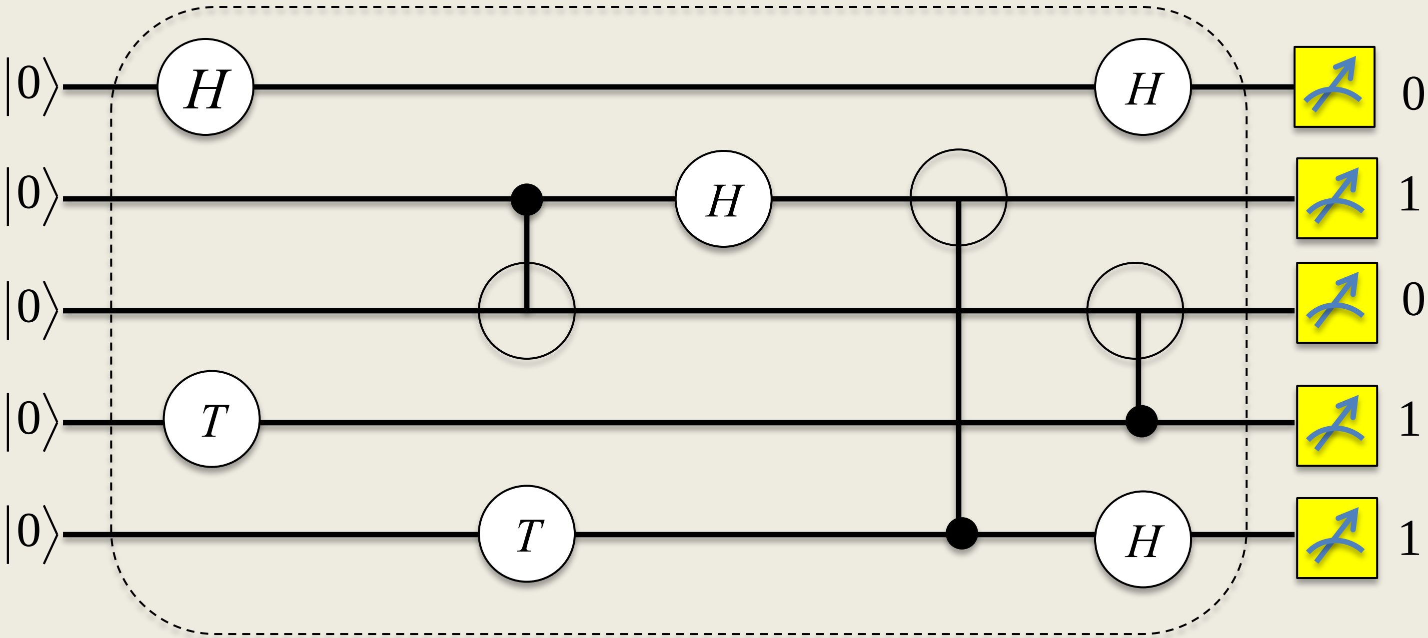
Quantum algorithms

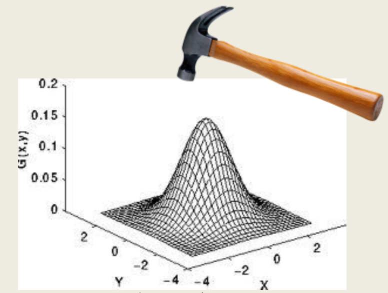


U: It encodes the problem

Circuit model

Quantum algorithms





$|y_f\rangle$

U: It encodes the problem

Initial state $|00...0\rangle$

Evolution $U = V_1 V_2 .... V_L$

Final state $|\psi_f\rangle = a_{00...0}|00...0\rangle + a_{10...0}|10...0\rangle + ... + a_{11...1}|11...1\rangle$

Measurement $|j\rangle$, $\Pr(\sigma) = |a_j|^2$

Circuit model

Quantum speedups: Deutsch-Jozsa

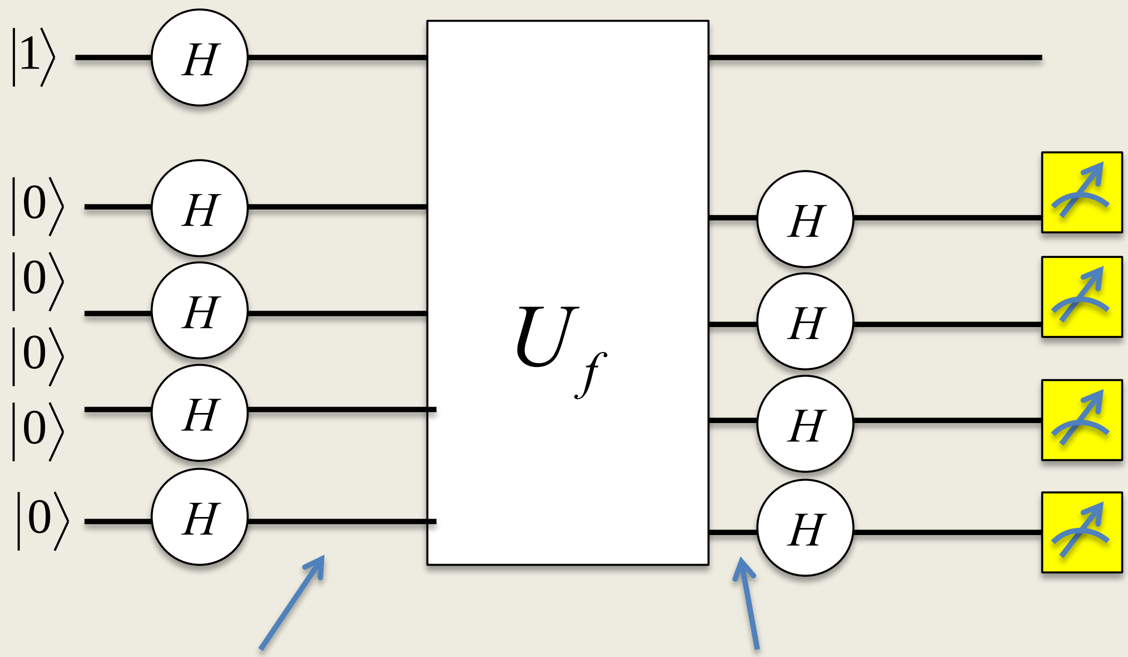
Given: an oracle for $f:\{0,1\}^n \rightarrow \{0,1\}$; such that f is constant or balanc

Goal: decide which case it is using the oracle and other f-independent gates

Quantum speedups: Deutsch-Jozsa

Given: an oracle for $f:\{0,1\}^n \rightarrow \{0,1\}$; such that f is constant or balanc

Goal: decide which case it is using the oracle and other f-independent gates

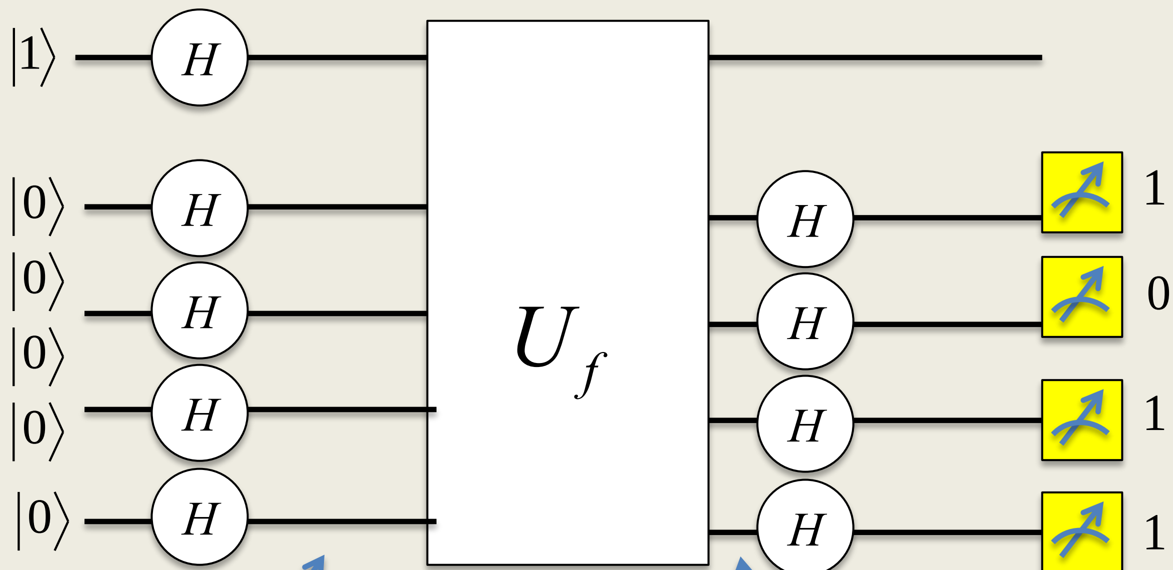


$$\left(\frac{1}{\sqrt{2^n}}\sum_{j=0}^{2^n-1}|j\rangle\right)\frac{|0\rangle-|1\rangle}{\sqrt{2}} \qquad \frac{1}{\sqrt{2^n}}\left(\sum_{j=0}^{2^n-1}|j\rangle\frac{|f(j)\rangle-|1\oplus f(j)\rangle}{\sqrt{2}}\right)$$

Quantum speedups: Deutsch-Jozsa

Given: an oracle for $f : \{0,1\}^n \rightarrow \{0,1\}$; such that f is constant or balanc

Goal: decide which case it is using the oracle and other f-independent gates



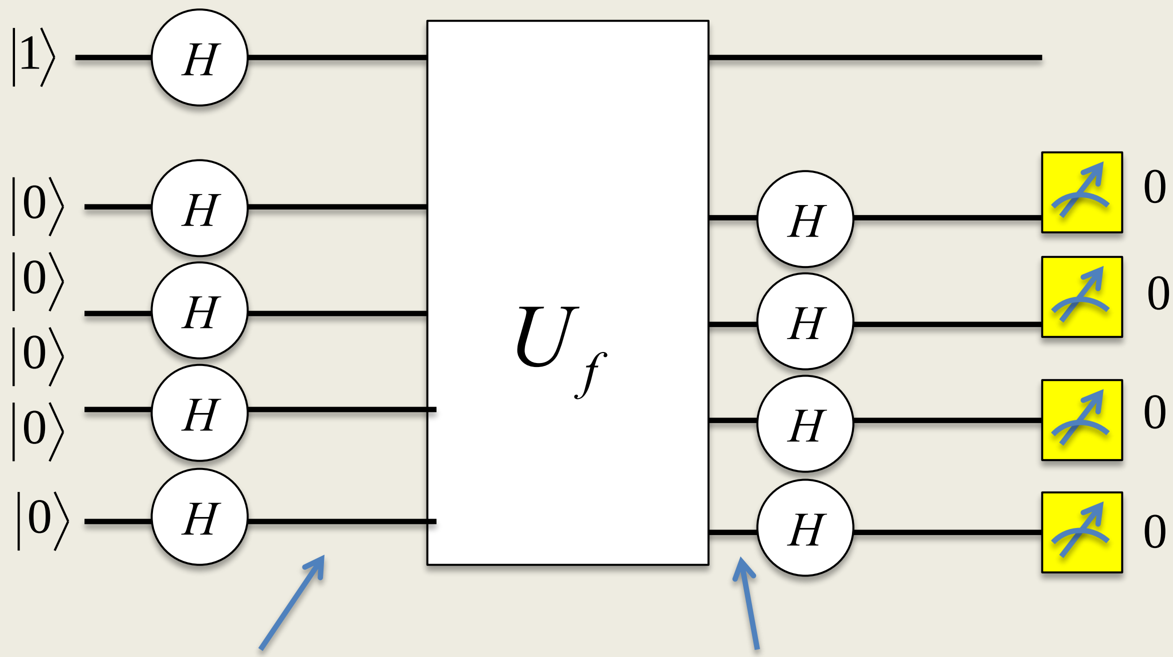
If it is balanced

$$\left(\frac{1}{\sqrt{2^n}}\sum_{j=0}^{2^n-1}|j\rangle\right)\frac{|0\rangle-|1\rangle}{\sqrt{2}} \qquad \frac{1}{\sqrt{2^n}}\left(\sum_{j=0}^{2^n-1}|j\rangle\frac{|f(j)\rangle-|1\oplus f(j)\rangle}{\sqrt{2}}\right)$$

Quantum speedups: Deutsch-Jozsa

Given: an oracle for $f:\{0,1\}^n \rightarrow \{0,1\}$; such that f is constant or balanc

Goal: decide which case it is using the oracle and other f-independent gates



If it is constant

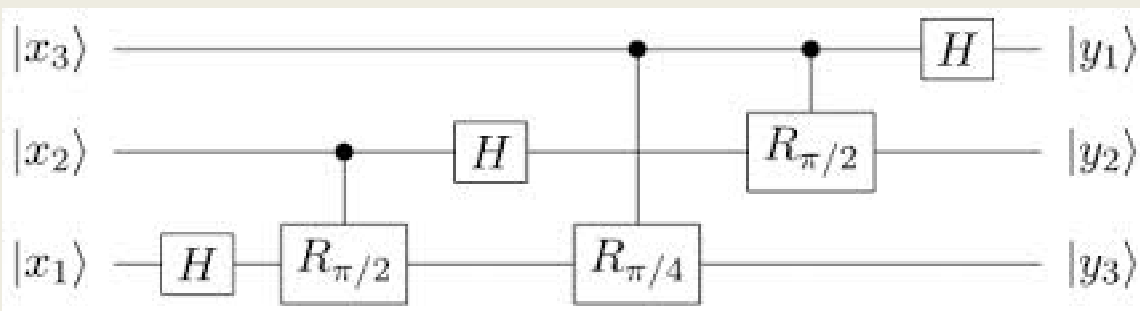
$$\left(\frac{1}{\sqrt{2^n}}\sum_{j=0}^{2^n-1}|j\rangle\right)\frac{|0\rangle-|1\rangle}{\sqrt{2}} \qquad \frac{1}{\sqrt{2^n}}\left(\sum_{j=0}^{2^n-1}|j\rangle\frac{|f(j)\rangle-|1\oplus f(j)\rangle}{\sqrt{2}}\right)$$

Quantum speedups: Fourier Transform

Basically, D-J is performing a Fourier transform. If the function is constant, then we transform the state to the “delta-function” 00…0. If it is balanced, the Fourier transform has no components at 00….0

Theorem: The (quantum) Fourier transform can be implemented with log(N) resources

$$|j\rangle \rightarrow \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} e^{i2\pi j*k/2^n} |k\rangle$$



Quantum computers are “good” at computing periods of functions (as long as we can encode this information in a quantum state efficiently)

Quantum speedups: Factoring and more

Shor's algorithm exploits a reduction from factoring to period finding. Then, the QFT can be used to compute the period. Time ~ n^3

Quantum computers can break encryption methods based on RSA

Quantum speedups: Factoring and more

Shor's algorithm exploits a reduction from factoring to period finding. Then, the QFT can be used to compute the period. Time ~ n^3

Quantum computers can break encryption methods based on RSA

The QFT can also be used to compute the eigenvalues of unitary operations. In particular, it can be used to estimate physical quantities at precisions that are classically impossible (Heisenberg limit)

Quantum speedups: Factoring and more

Shor's algorithm exploits a reduction from factoring to period finding. Then, the QFT can be used to compute the period. Time ~ n^3

→ Quantum computers can break encryption methods based on RSA

The QFT can also be used to compute the eigenvalues of unitary operations. In particular, it can be used to estimate physical quantities at precisions that are classically impossible (Heisenberg limit)

For similar reasons, quantum computers can be used to compute and simulate physical systems efficiently. This is hard classically; the main reason why quantum computers were proposed by Feynman in 1982

Quantum speedups in optimization: LANL results

Goal: Find configuration k that minimizes or maximizes $E[j]$ (cost function

Traveling salesman problem

$E[j]:=$ distance of route j

Quantum algorithms to solve optimization problems can be "naturally" developed by means of adiabatic state transformations

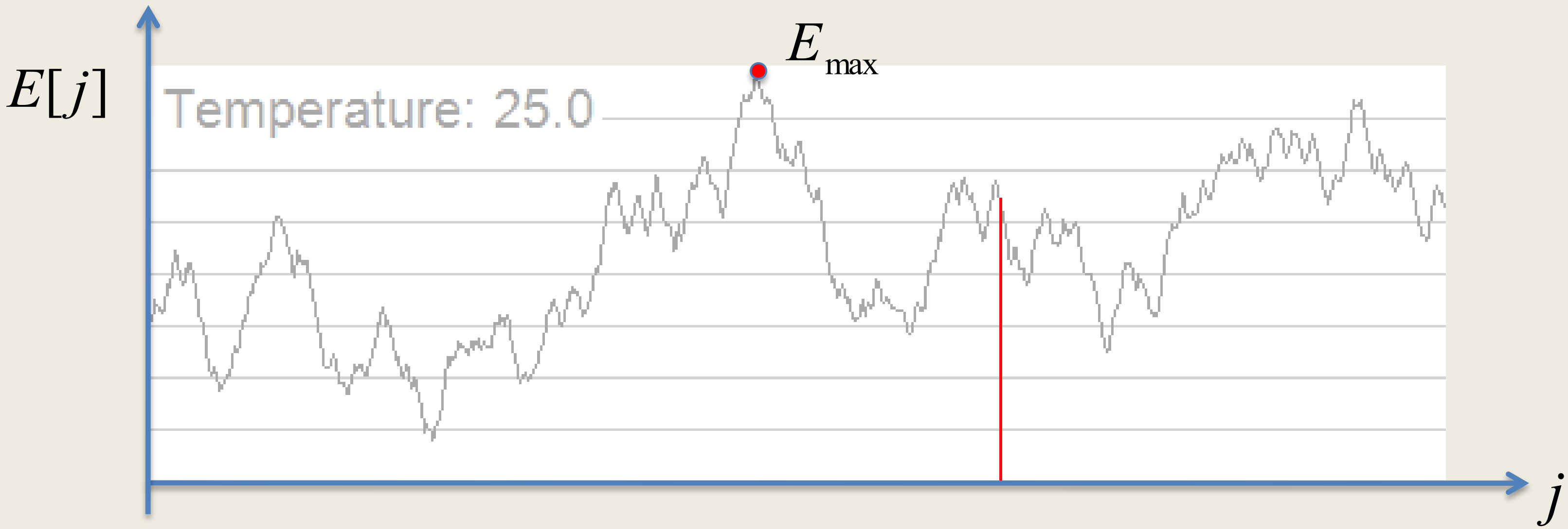
$$\left|\psi_f\right\rangle \approx \left|k\right\rangle$$

Los Alamos NATIONAL LABORATORY EST. 1943

LDRD

Quantum speedups in optimization: LANL results

Simulated Annealing: Speedup of classical Monte-Carlo algorithms

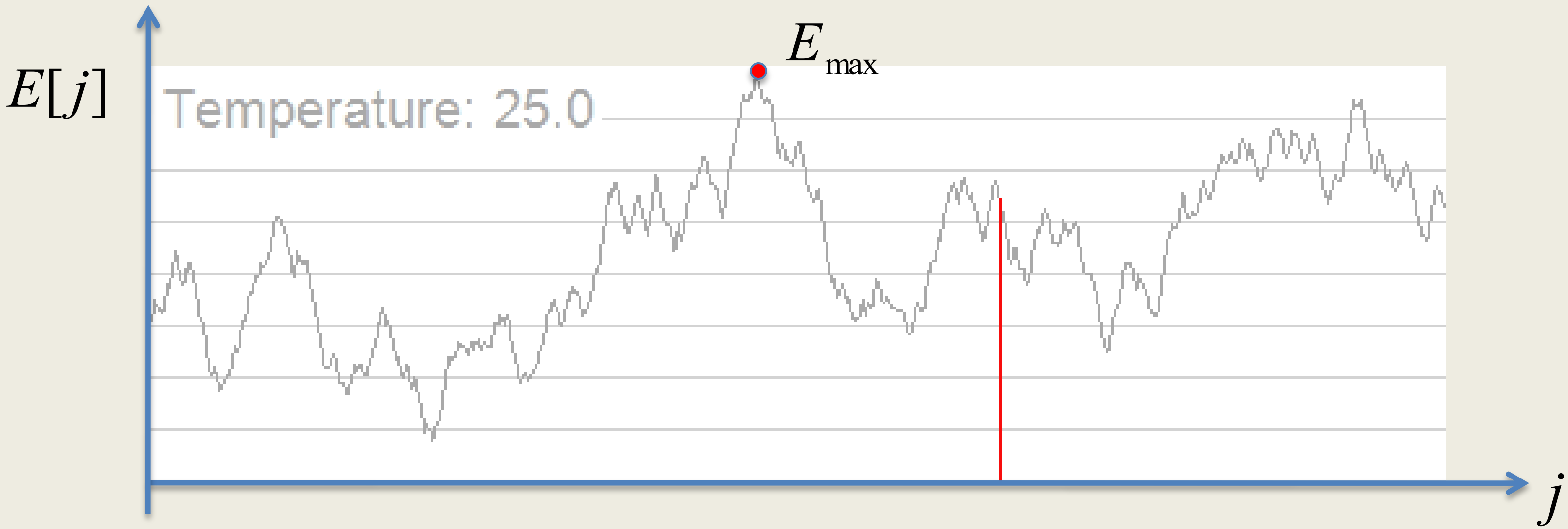


By lowering a “simulated” temperature, we can reach the maximum (or minimum) of E

The cost of simulated annealing is the number of Monte Carlo steps: $T_{\text{mix}} \propto \frac{1}{\Delta}$

Quantum speedups in optimization: LANL results

Simulated Annealing: Speedup of classical Monte-Carlo algorithms



By lowering a “simulated” temperature, we can reach the maximum (or minimum) of E

The cost of simulated annealing is the number of Monte Carlo steps: $T_{\text{mix}} \propto \frac{1}{\Delta}$

Spectral gap of stochastic matrix

Quantum speedups in optimization: LANL results

Speedup of classical Monte-Carlo algorithms

Markov Process

S

One-to-one correspondence

U

Quantum Circuit

The cost of the quantum method is determined by the # of gates:

$$T_{\text{quantum}} \propto \sqrt{T_{\text{mix}}}$$

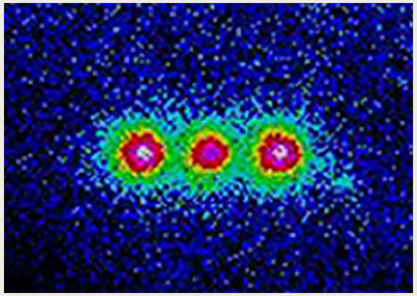
"Quantum simulations of classical annealing processes", RS, Boixo, Barnum, Knill, Phys. Rev. Lett. 101, 130504 (2008)

Los Alamos NATIONAL LABORATORY EST. 1943

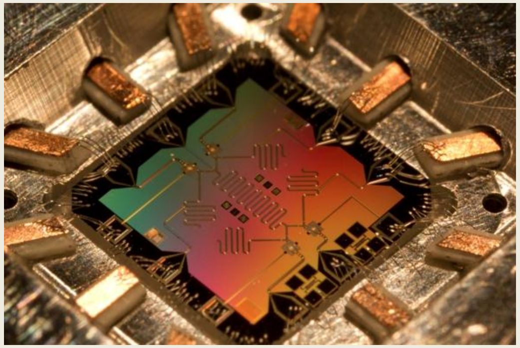
LDRD

Large quantum computers are far from being realized due to decoherence problems: preserving “superposition” states is an experimental challenge. On one side, quantum systems must be isolated. On the other, we should be able to control them.

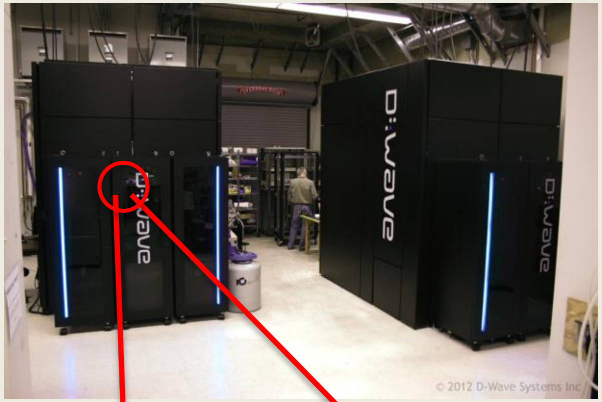
Ion traps (Wineland’s group)
10’s of qubits
10’s of gates

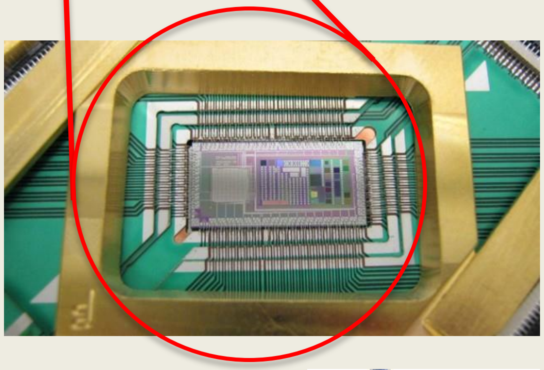


Martini’s (UCSB)
Superconducting qubits
1 logic qubit?



Dwave: 100’s qubits
Special purpose
Quantum? Speedups?



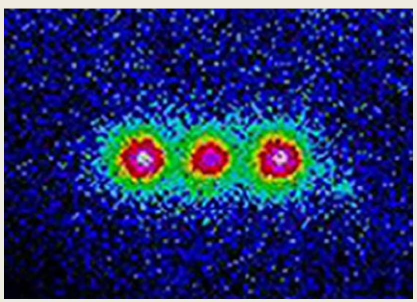


Los Alamos
NATIONAL LABORATORY
EST.1943

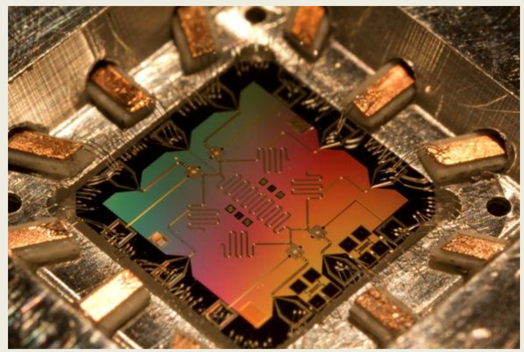
LDRD

Large quantum computers are far from being realized due to decoherence problems: preserving "superposition" states is an experimental challenge. On one side, quantum systems must be isolated. On the other, we should be able to control them.

Ion traps (Wineland's group)
10's of qubits
10's of gates



Martini's (UCSB)
Superconducting qubits
1 logic qubit?



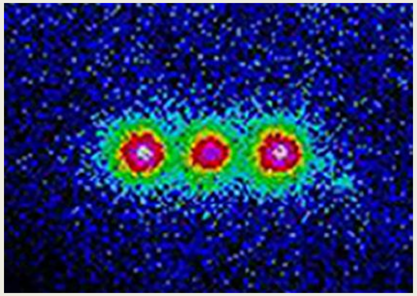
Dwave: 100's qubits
Special purpose
Quantum? Speedups?

Los Alamos
NATIONAL LABORATORY
EST. 1943

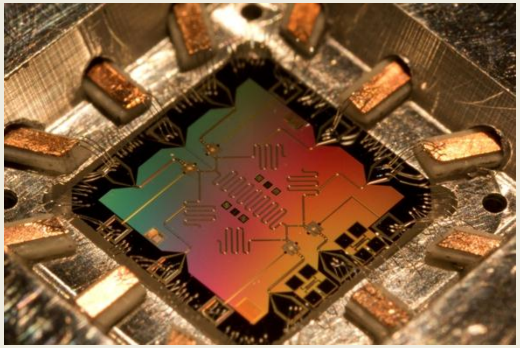
LDRD

Large quantum computers are far from being realized due to decoherence problems: preserving "superposition" states is an experimental challenge. On one side, quantum systems must be isolated. On the other, we should be able to control them.

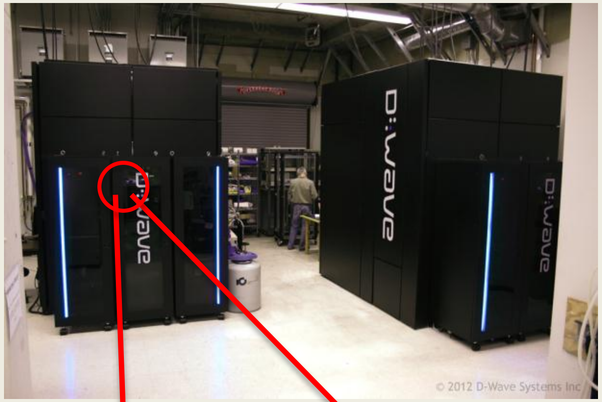
Ion traps (Wineland's group)
10's of qubits
10's of gates

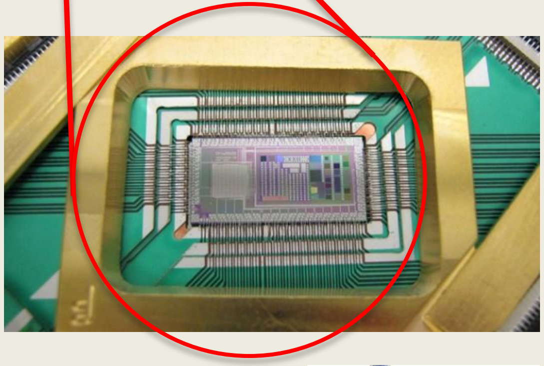


Martini's (UCSB)
Superconducting qubits
1 logic qubit?



Dwave: 100's qubits
Special purpose
Quantum? Speedups?





What makes quantum computers powerful?

Los Alamos NATIONAL LABORATORY EST. 1943

LDRD

Prospects of quantum information in the near future:

Immediate or near-future applications of quantum information includes secure communications. Our LANL quantum crypto team is devising ways of implementing secure network and long distance communications.

Quantum communications: Avoiding cyber attacks

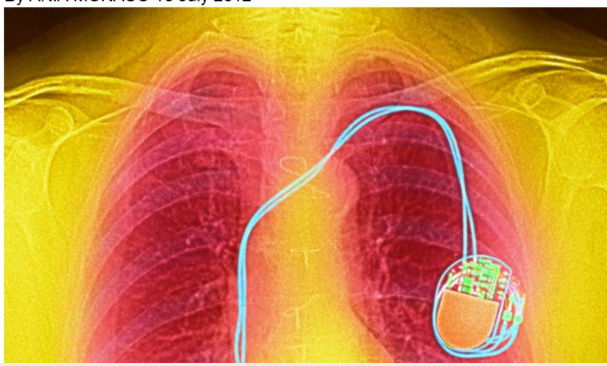
Hardly a day passes by without a new cyber threat:

Home (/) / Tech Focus (/technology-focus) / Tech topic (/technology-focus/technology-topic)

Keeping Hackers Out of Implanted Medical Devices

Researchers find way to prevent attacks on wireless medical equipment

By ANIA MONACO 16 July 2012



Computers and smartphones aren't the only electronics that can be hacked. Alarmingly, during the past few years several researchers have found that wireless and wearable medical devices, like pacemakers (http://theinstitute.ieee.org/technology-focus/technology-topic/hacking-hearts101), insulin-delivery systems

Dropbox Spam Attack Blamed on Another Website's Breach

Published: Wednesday, 1 Aug 2012 | 3:57 PM ET   Text Size

By: Cadie Thompson
Technology Editor, CNBC.com

Source: Dropbox.com

The cloud storage service Dropbox is blaming a recent spam attack on a stolen password from a breach on another website.

About two weeks ago **Dropbox users began reporting spam messages** sent to the email addresses they were using for their Dropbox account. After investigating the matter, the cloud storage company discovered that usernames and passwords stolen from another site has also been used to access some accounts.

The security of classical cryptography relies on the hardness of solving a particular problem. The most common example is RSA, which is intrinsically tied to FACTORING.

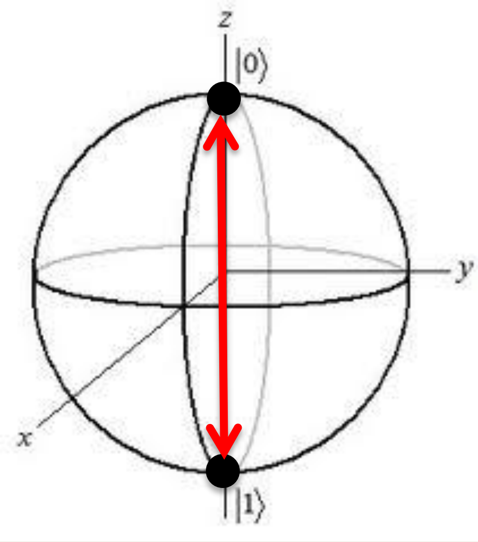
Future proof?

Key distribution: A cryptographic primitive

The goal is to share a random, secret key between two parties. If KD is possible, many other cryptographic tasks can be securely implemented. These include sending messages using the one-time pad, secret sharing, etc.

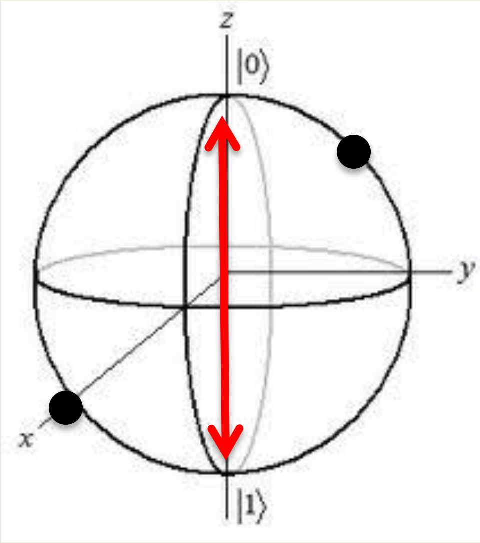
The shared key is fully random. This implies that encoded sent information is no different than pure noise (one-time pad)

Why Quantum Information?



A measurement in the computational basis reveals 0 or 1, depending on the qubit state

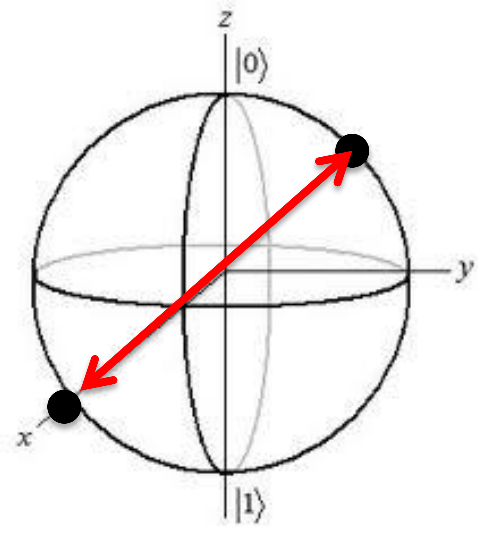
Why Quantum Information?



A measurement in the computational basis reveals 0 or 1 with probability 1/2

$$|y\rangle = \frac{|0\rangle \pm |1\rangle}{\sqrt{2}}$$

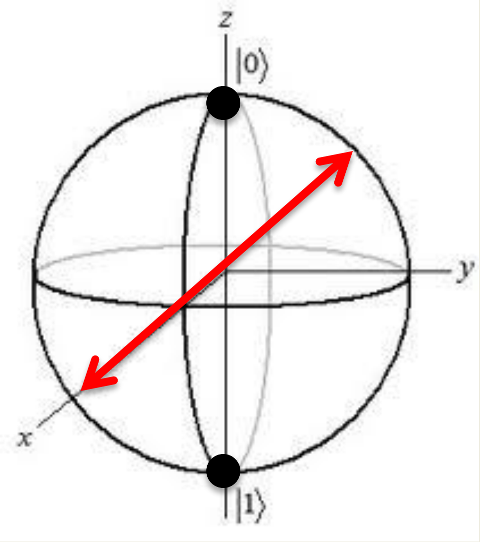
Why Quantum Information?



A measurement in the "diagonal" basis reveals 0 or 1 depending on the state

$$|y\rangle = \frac{|0\rangle \pm |1\rangle}{\sqrt{2}}$$

Why Quantum Information?



A measurement in the “diagonal” basis reveals 0 or 1 with probability 1/2

Why Quantum Information?

Unless the state is known, the outcome of a measurement may be non-deterministic

In addition, quantum states cannot be copied (no-cloning)

$$\left.\begin{array}{l} |0\rangle \to |00\rangle \\ |1\rangle \to |11\rangle \end{array}\right\} \Rightarrow \frac{|0\rangle + |1\rangle}{\sqrt{2}} \to \frac{|00\rangle + |11\rangle}{\sqrt{2}} \neq \frac{|0\rangle + |1\rangle}{\sqrt{2}} \frac{|0\rangle + |1\rangle}{\sqrt{2}}$$

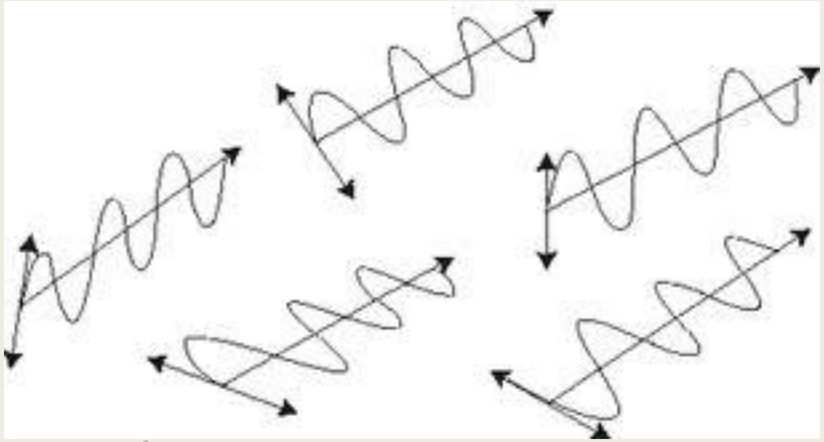
Maximum uncertainty state

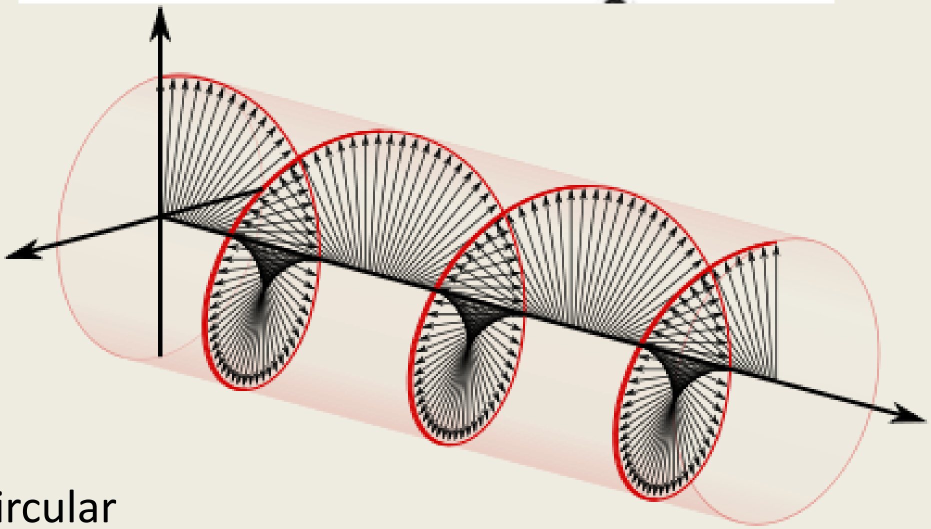
Any interaction with an eavesdropper will be detected by the parties in the communication: For example, if the eavesdropper makes a measurement, it will "collapse" and disturb the state, and the disturbance can be quantified.

Light polarization

In quantum communications, single qubit states correspond to single-photon states that are prepared choosing a particular polarization. For example, the computational basis can correspond to HV polarization. The diagonal basis is the DA polarization or circular.

planar

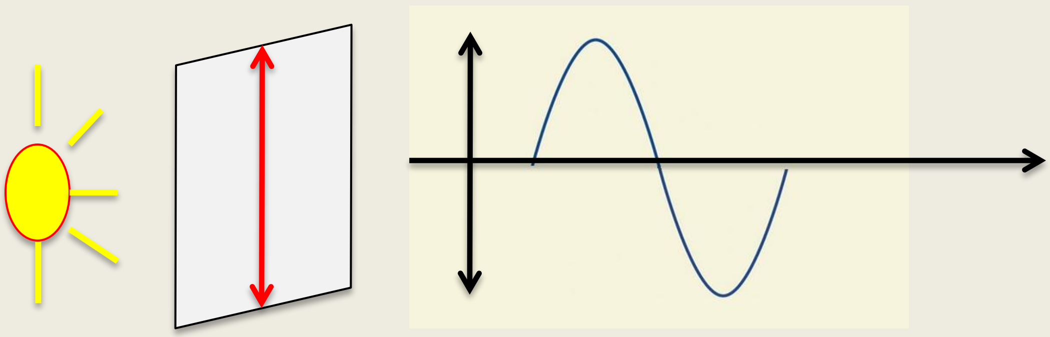




circular

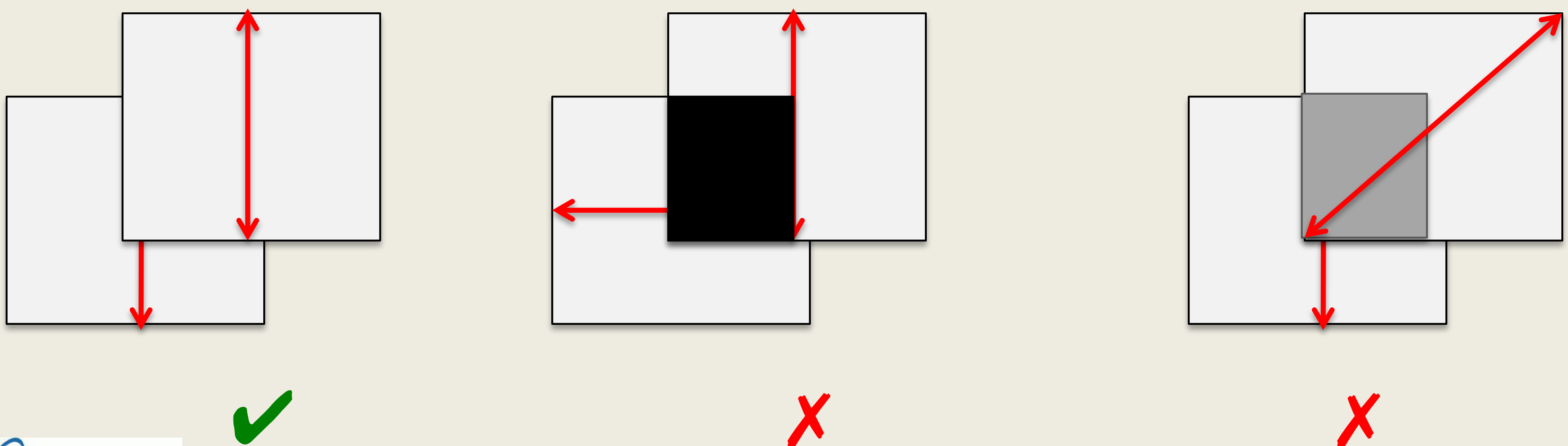
Light polarization

A polarizer determines the polarization

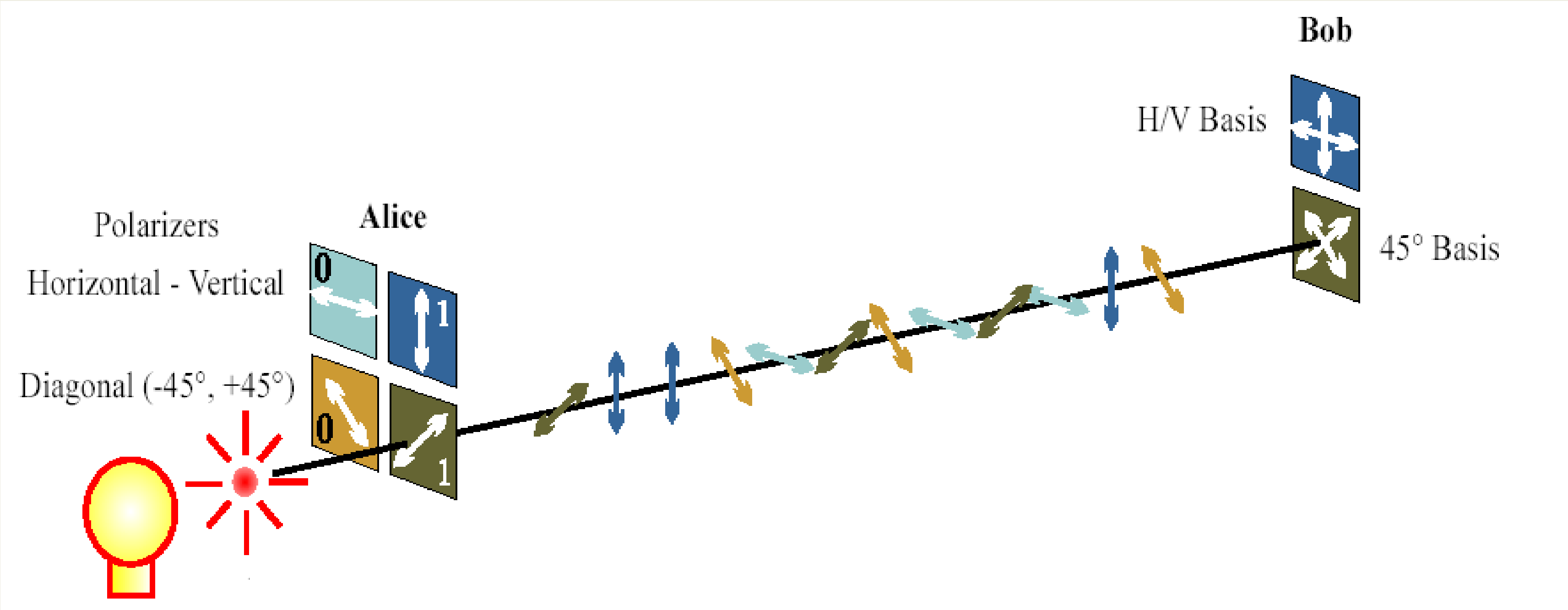


Light source

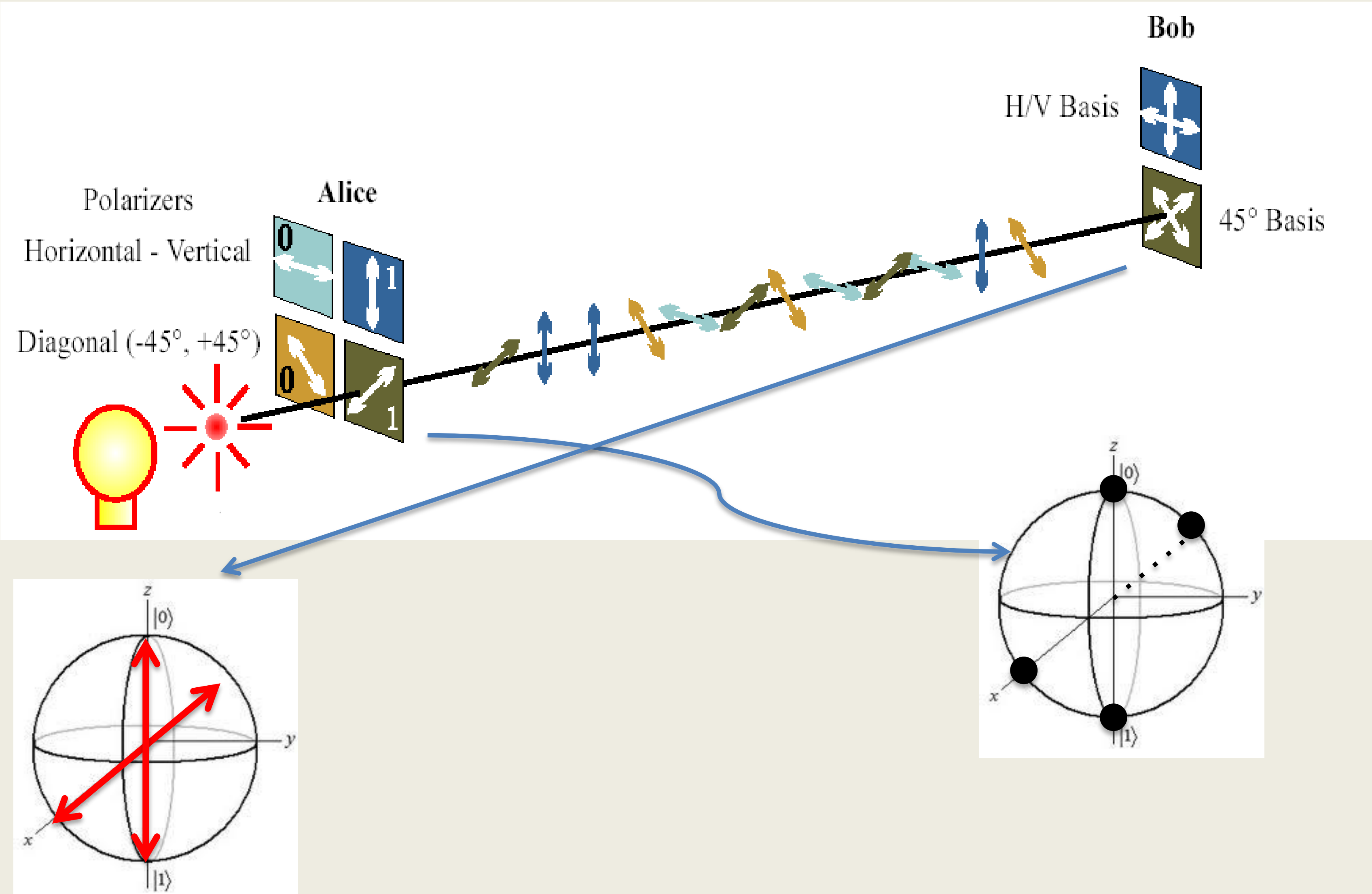
Measurements by an eavesdropper (different polarization axes)



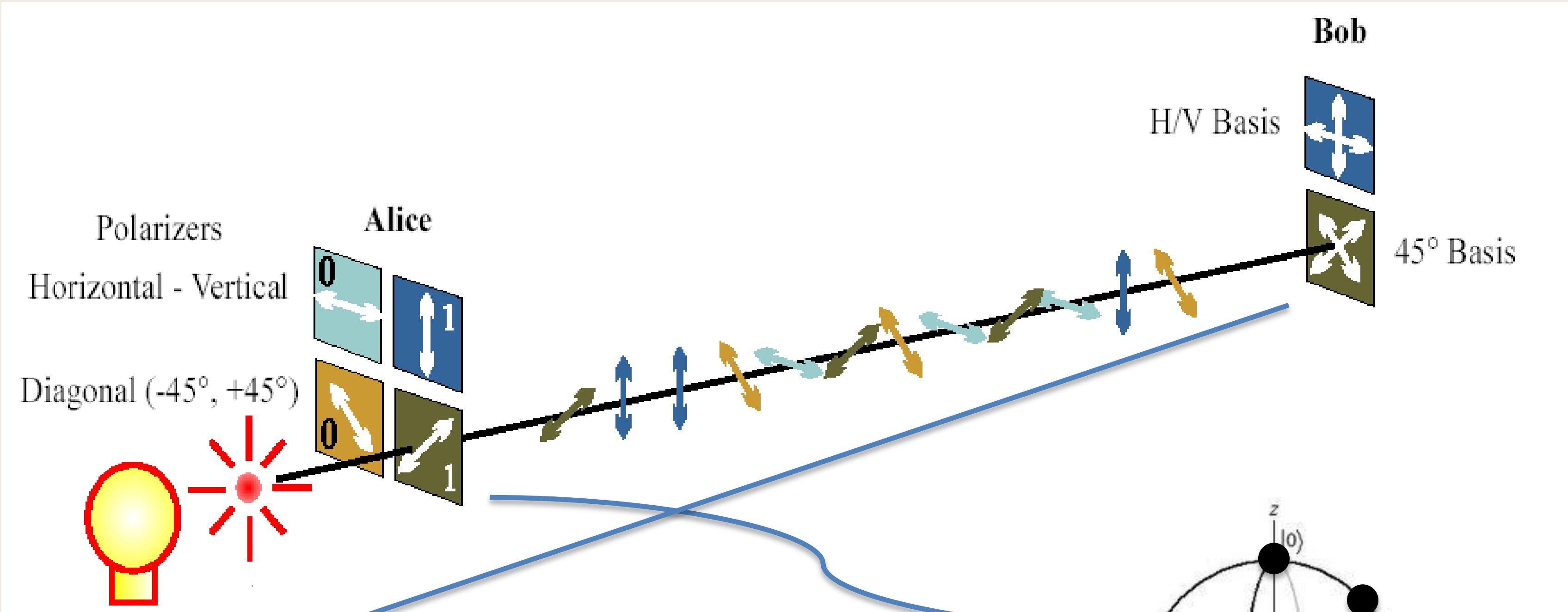
Quantum communications: Quantum key distribution and BB84

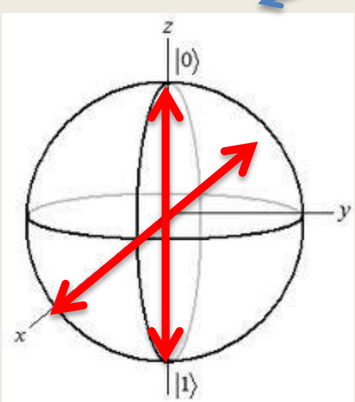


Quantum communications: Quantum key distribution and BB84



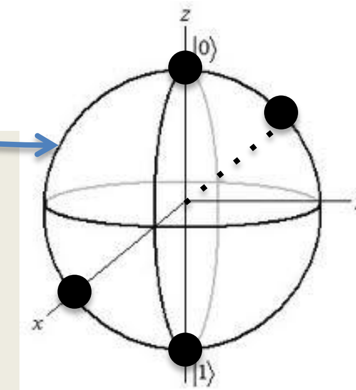
Quantum communications: Quantum key distribution and BB84





Preparation Alice / Bob Measure		+	+	×	×
		0	1	0	1
+	0	1	0	1/2	1/2
+	1	0	1	1/2	1/2
×	0	1/2	1/2	1	0
×	1	1/2	1/2	0	1

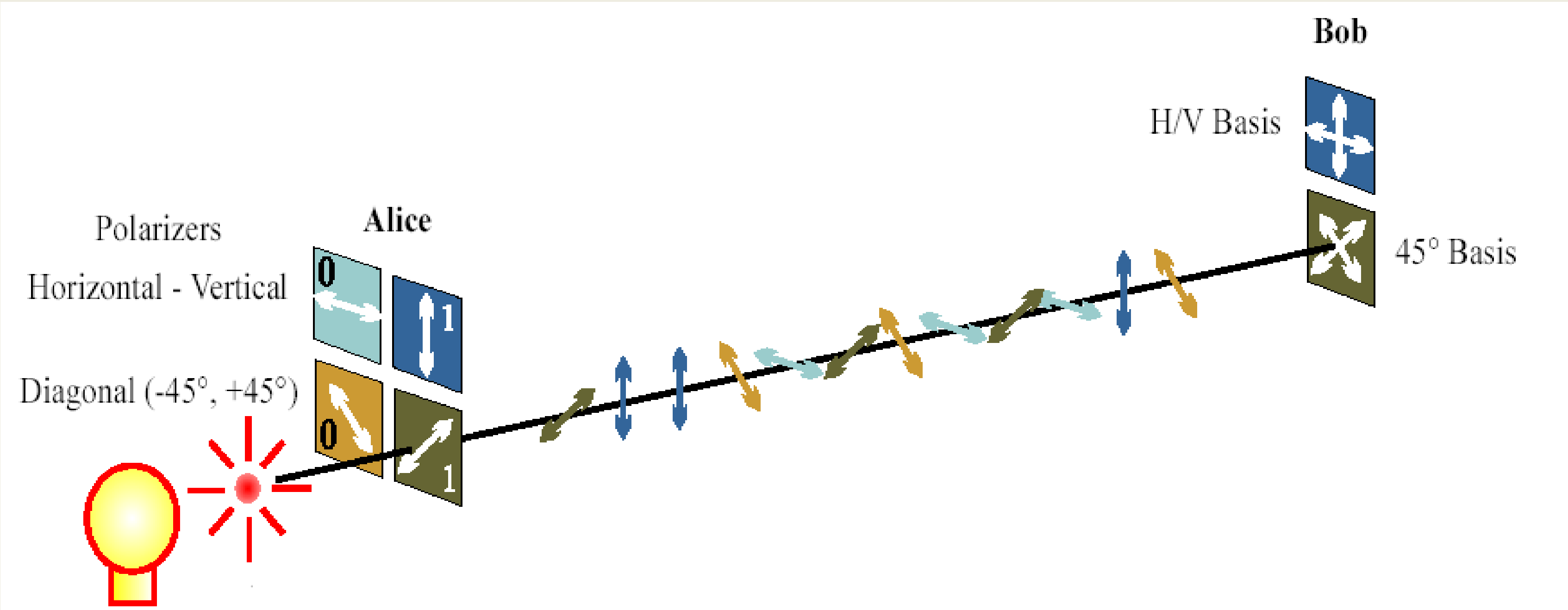
Measurement probabilities



Los Alamos
NATIONAL LABORATORY
EST. 1943

LDRD

Quantum communications: Quantum key distribution and BB84

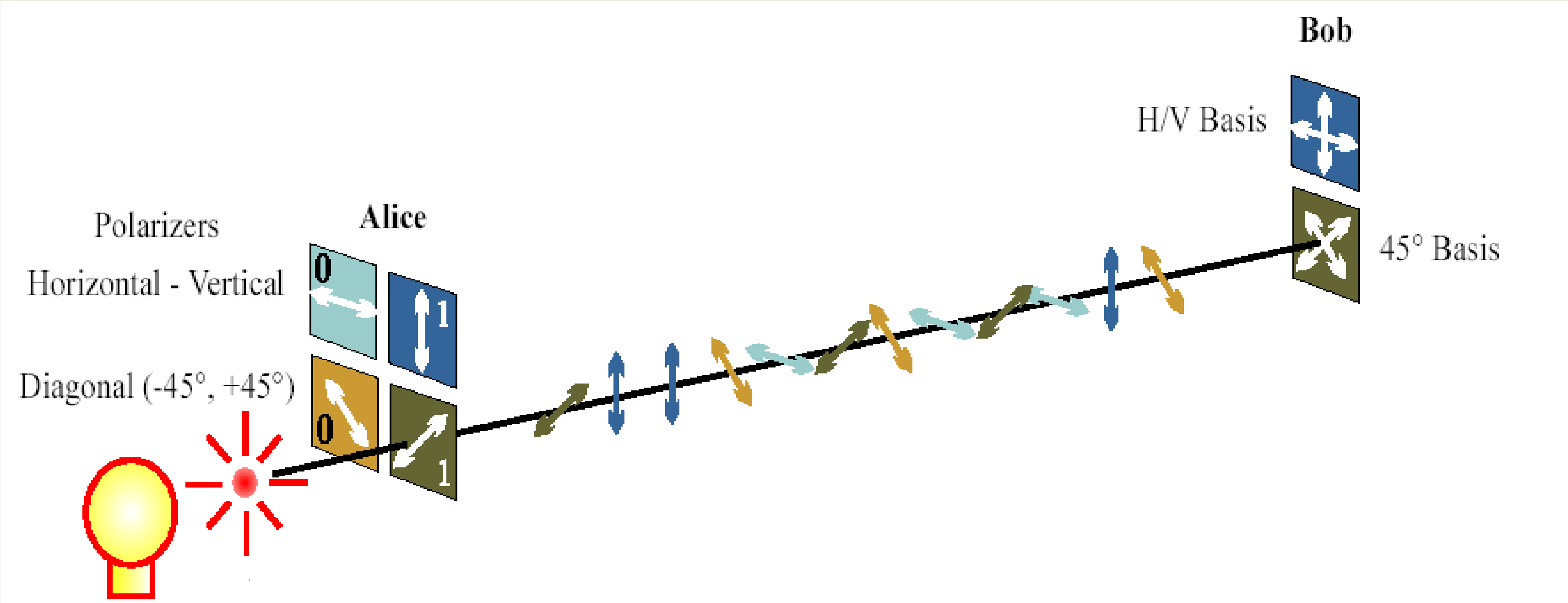


Bob Measure \ Preparation Alice		+	+	×	×
		0	1	0	1
+	0	1	0	1/2	1/2
+	1	0	1	1/2	1/2
×	0	1/2	1/2	1	0
×	1	1/2	1/2	0	1

I- Sifting:

Alice and Bob announce their preparation/measurement bases in a public channel. They only keep those bits in which the bases coincide.

Quantum communications: Quantum key distribution and BB84

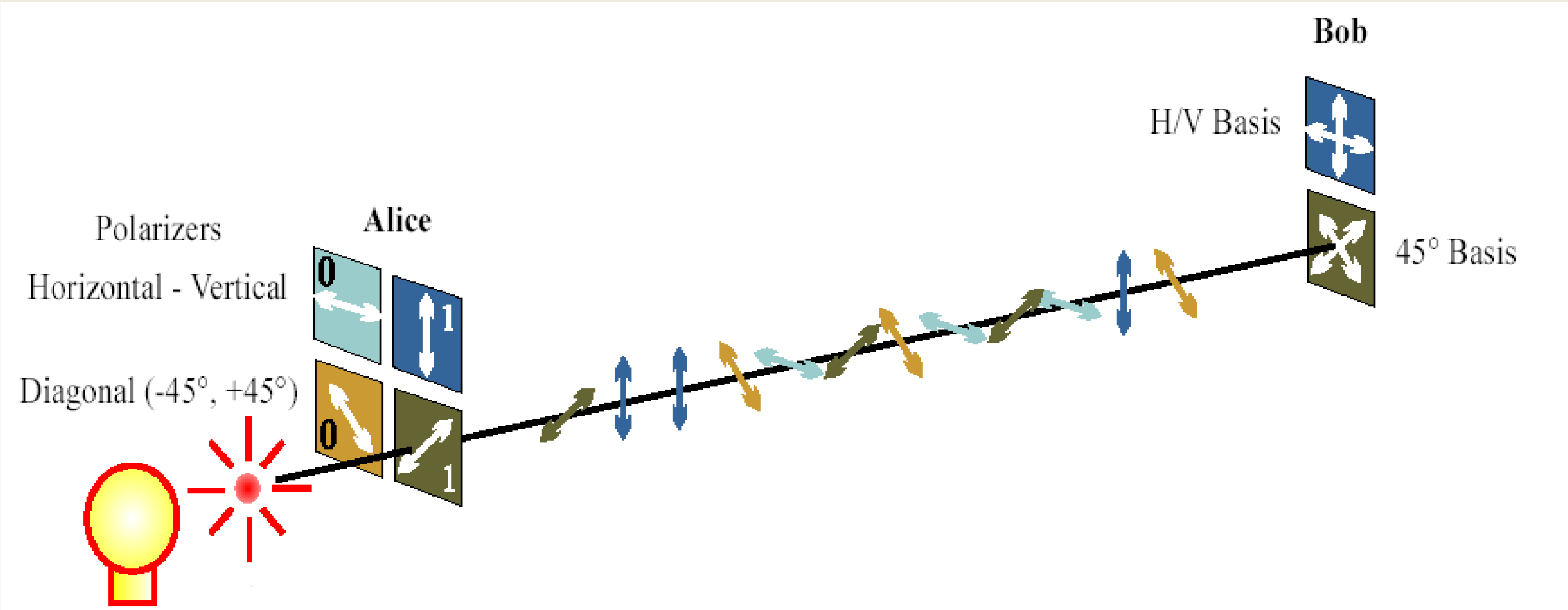


Preparation Alice / Bob Measure		+	+	×	×
		0	1	0	1
+	0	1	0	1/2	1/2
+	1	0	1	1/2	1/2
×	0	1/2	1/2	1	0
×	1	1/2	1/2	0	1

II- Error estimation:
Alice and Bob select a few random sifted bits and compare their values. In the presence of an eavesdropper, some bits will be different.

$$p_{\text{error}} < p_{\text{threshold}}$$

Quantum communications: Quantum key distribution and BB84



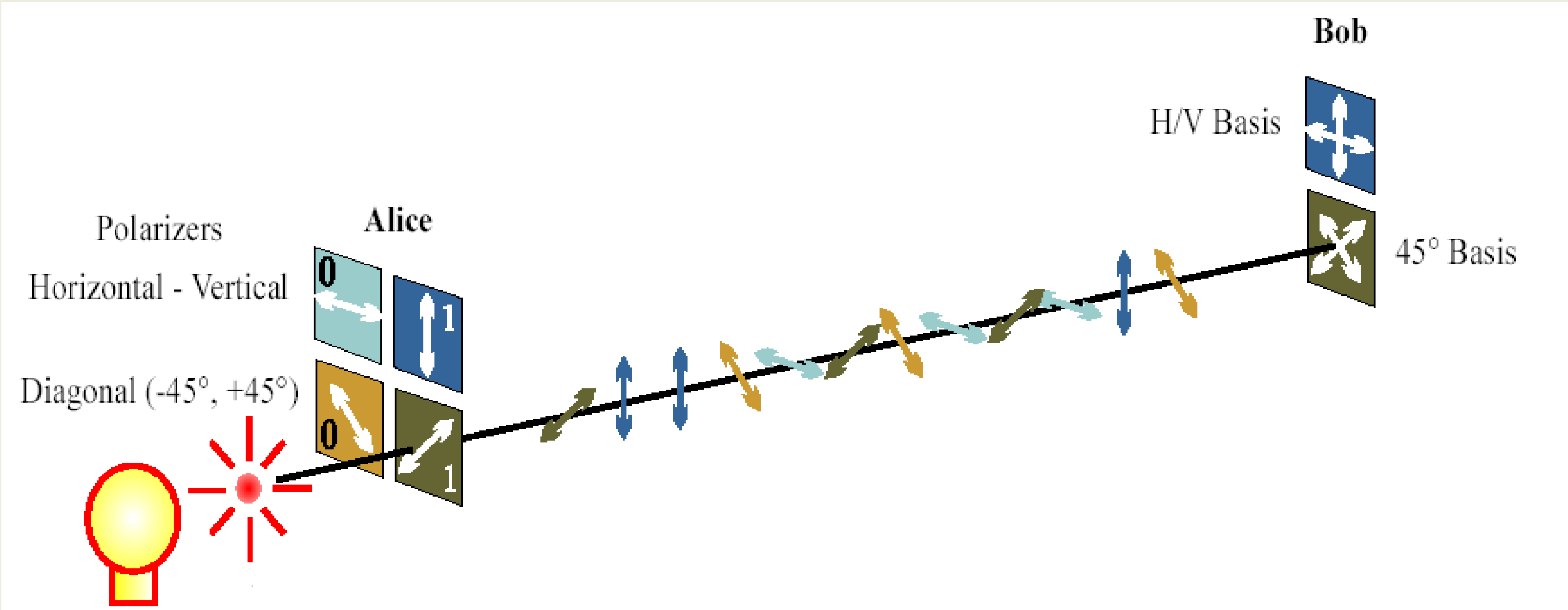
Preparation Alice / Bob Measure		+	+	×	×
		0	1	0	1
+	0	1	0	1/2	1/2
+	1	0	1	1/2	1/2
×	0	1/2	1/2	1	0
×	1	1/2	1/2	0	1

III- Information reconciliation: Alice and Bob perform error correction on the sifted bits with small information leakage.

Los Alamos NATIONAL LABORATORY EST. 1943

LDRD

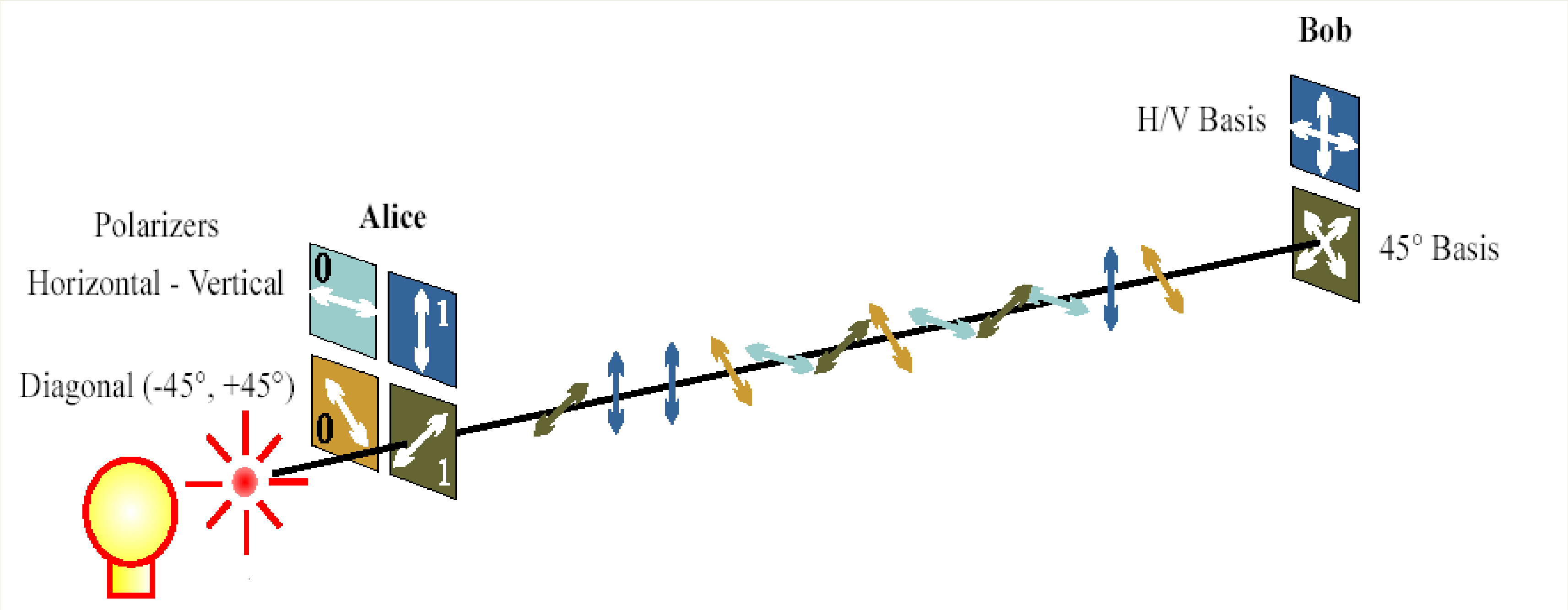
Quantum communications: Quantum key distribution and BB84



Preparation Alice / Bob Measure		+	+	×	×
		0	1	0	1
+	0	1	0	1/2	1/2
+	1	0	1	1/2	1/2
×	0	1/2	1/2	1	0
×	1	1/2	1/2	0	1

IV- Privacy amplification:
Due to IR, the eavesdropper has partial information. Privacy amplification reduces such information by Hashing the corrected bits (entropy extractor).

Quantum communications: Quantum key distribution and BB84



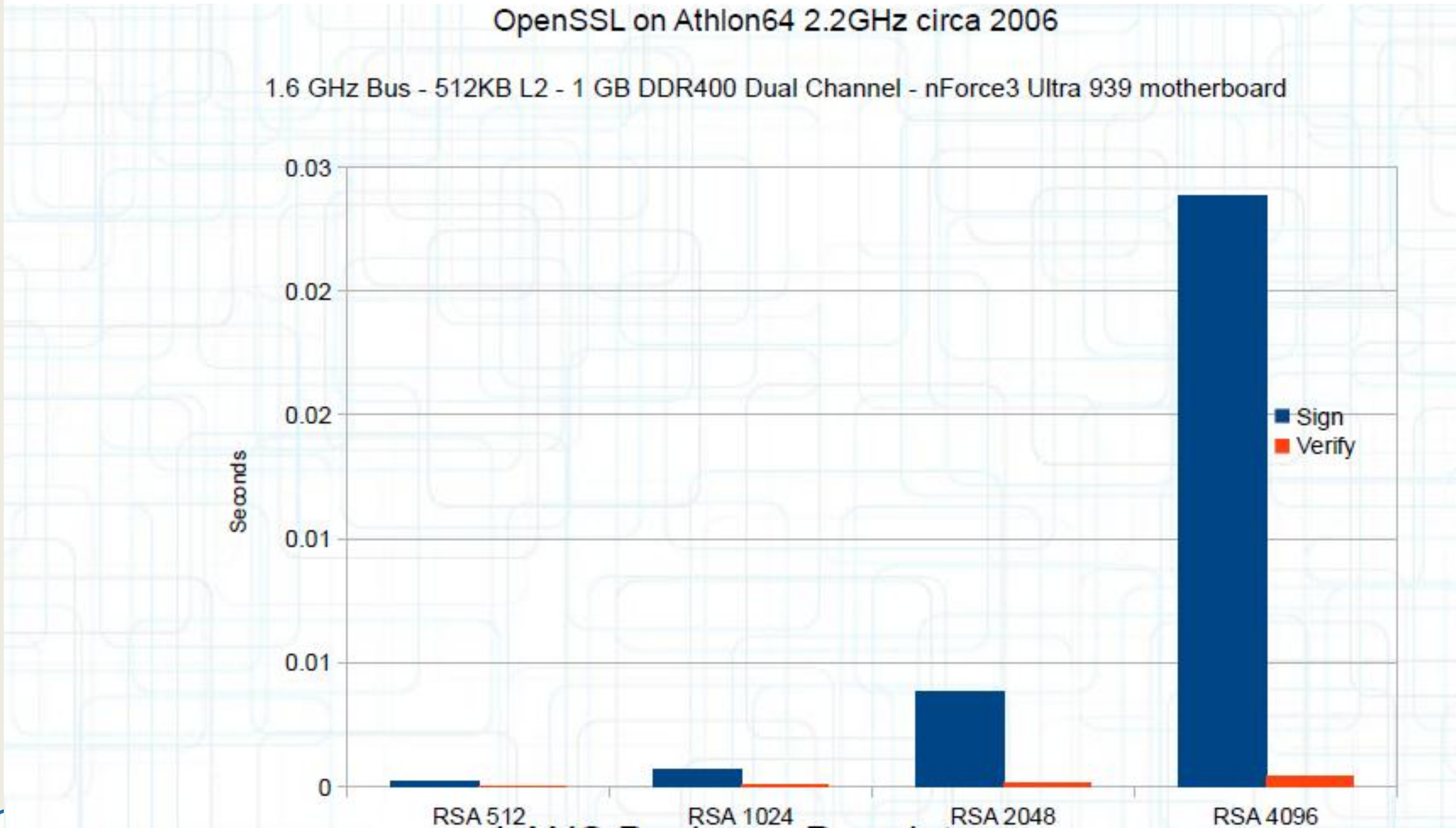
Final state:

$$\rho_{final} \approx \left[\frac{1}{|K|} \sum_{k \in keys} |k\rangle\langle k|_A \otimes |k\rangle\langle k|_B \right] \otimes \rho_{Eve}$$

The need for lightweight cryptography

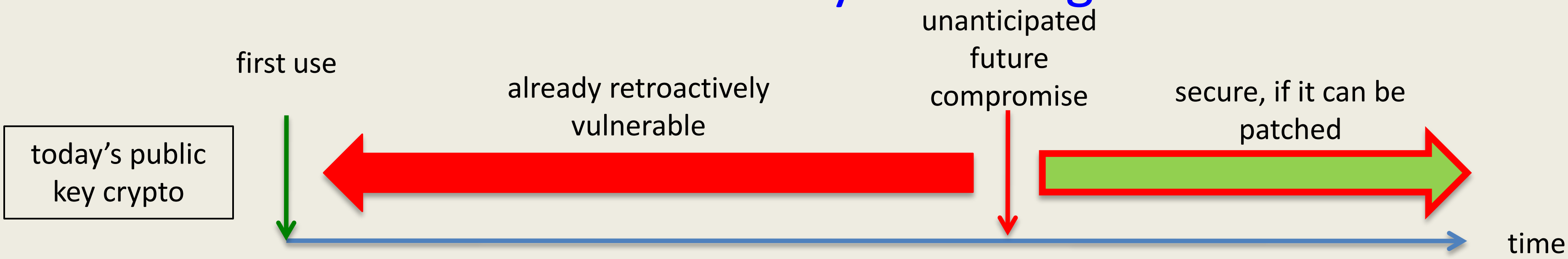
Today's public key cryptography:

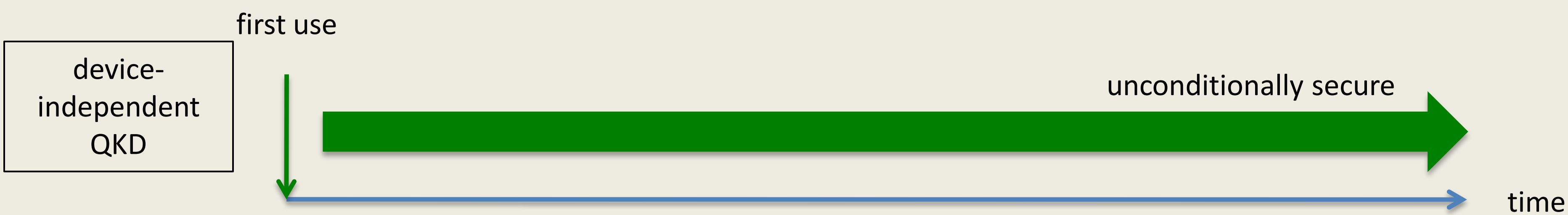
- retroactively vulnerable today to future, post-quantum-computer era
- **computationally too demanding for many emerging applications**



example: the "latency tax" of public key signatures

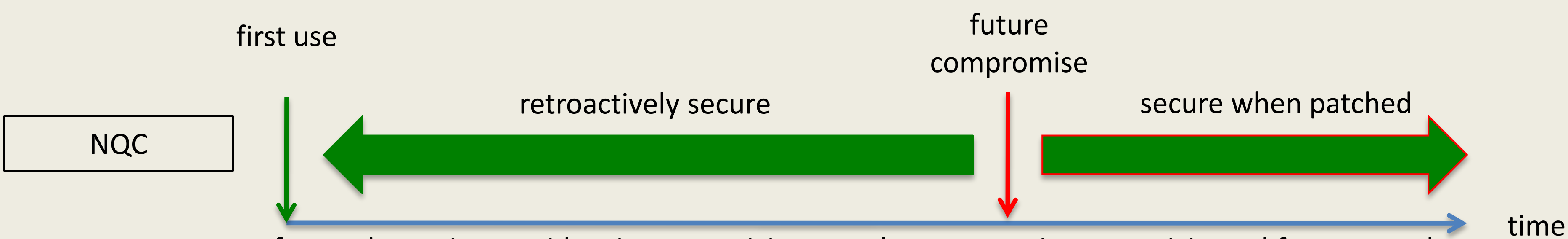
Forward security advantages





DIQKD has yet to be demonstrated, would only be feasible in a physics lab, and would only provide key distribution

- fascinating fundamental research, but unlikely to find practical applications



forward security provides time to anticipate and protect against unanticipated future attacks by patching, defense-in-depth, and operational doctrine (situational awareness)

PHYSICS 16 SEPTEMBER 2011 VOL 333 SCIENCE

Refining Quantum Cryptography

Richard Hughes and Jane Nordholt

PERSPECTIVES

Los Alamos NATIONAL LABORATORY EST. 1943

LDRD

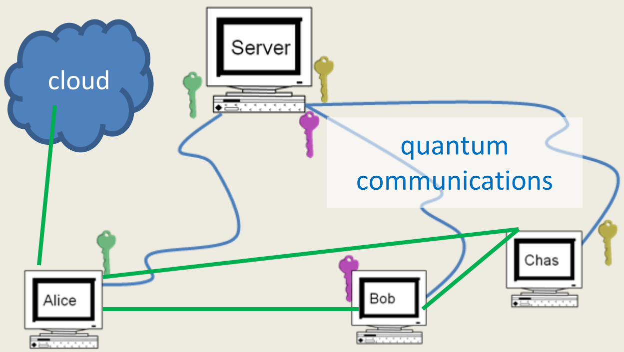
Quantum communications: Beyond QKD

- Most experimental efforts have demonstrated two party QKD…
  - Demonstration of multiparty QKD?
  - Network communications?
  - Implementation of other protocols?

At LANL, the network-centric quantum communications project (NQC) aims at the implementation of other protocols, including secure-identification, multiparty QKD, and secret sharing in multiparty networks.

Example NQC use cases

Enterprise networks: c.f. Kerberos



also: access networks (e.g. FiOS)

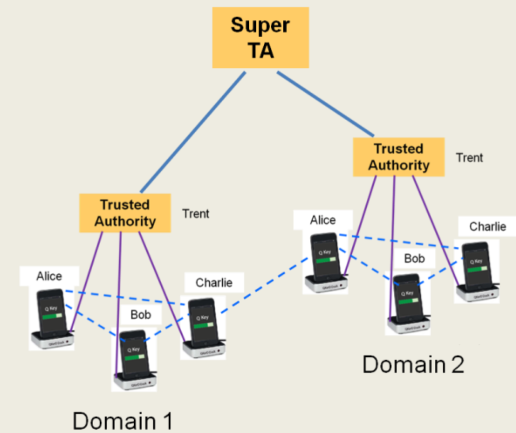
Alice and Bob establish a secure channel

Alice and Bob add Charlie to their secure conference

Alice requires Bob and Charlie to co-operate to access her secure database

Alice, Bob, Charlie require secure access to cloud

Scalable NQC ecosystem



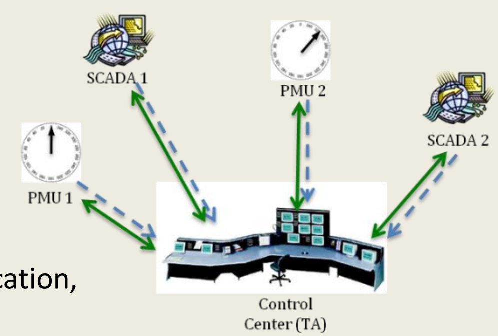
Securing handheld devices

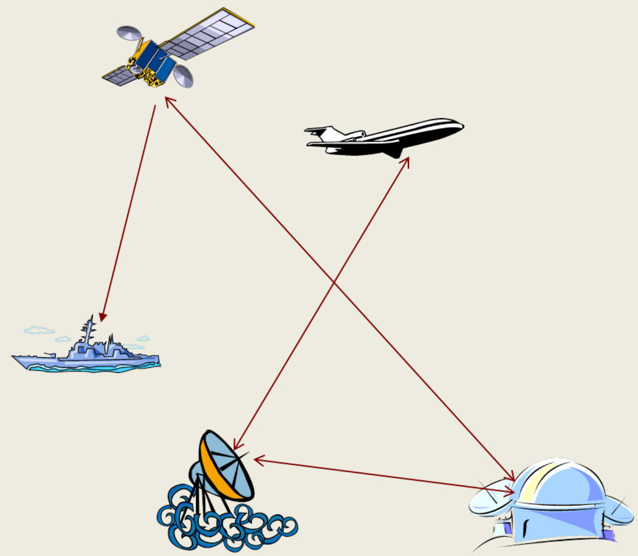
Establish mobile ad hoc networks:

- White House, battlefield, health care

Access control, identification, 2-factor authentication, single sign-on

Securing SCADA, SmartGrid



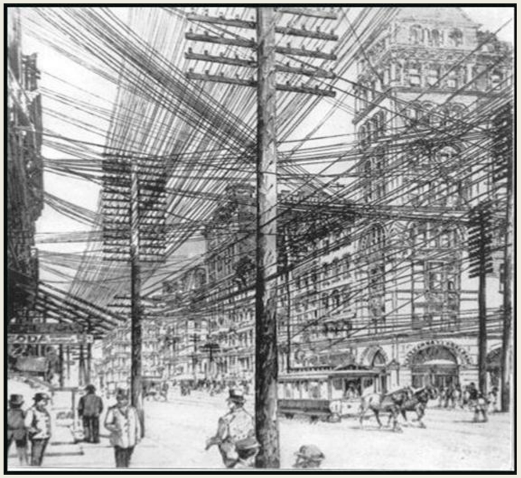


Establish global secure communications: ground, sea, air, space

Los Alamos NATIONAL LABORATORY EST. 1943

LDRD

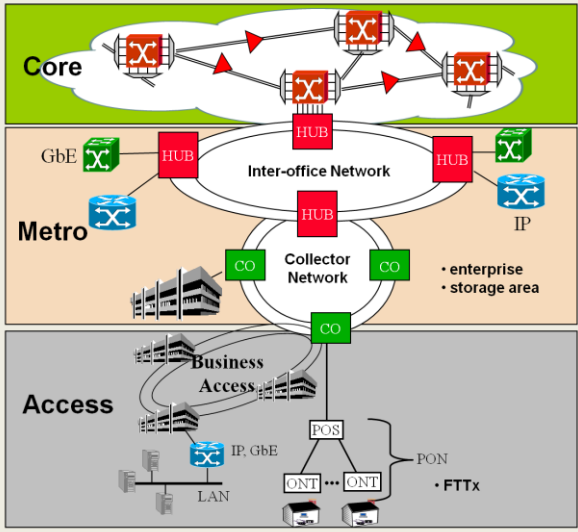
NQC Trends: LANL's idea



Broadway, 1890 *Book of Old New York*. Henry Collins Brown. 1913

networks are scalable

- from ~ N^2 point-to-point links …
- … to efficient interconnection of N end-users
- "Metcalfe's Law": value scales ~ N^2



Convergence:

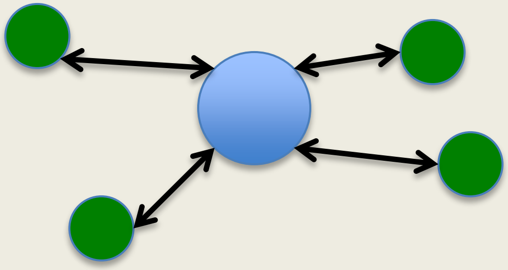
- everything on the (same) network … data, voice, control systems, satellites, …

Transparency:

- end-to-end optically transparent paths … more bandwidth, lower costs, reduced energy consumption

Consumerization:

- handheld devices, "the cloud", …

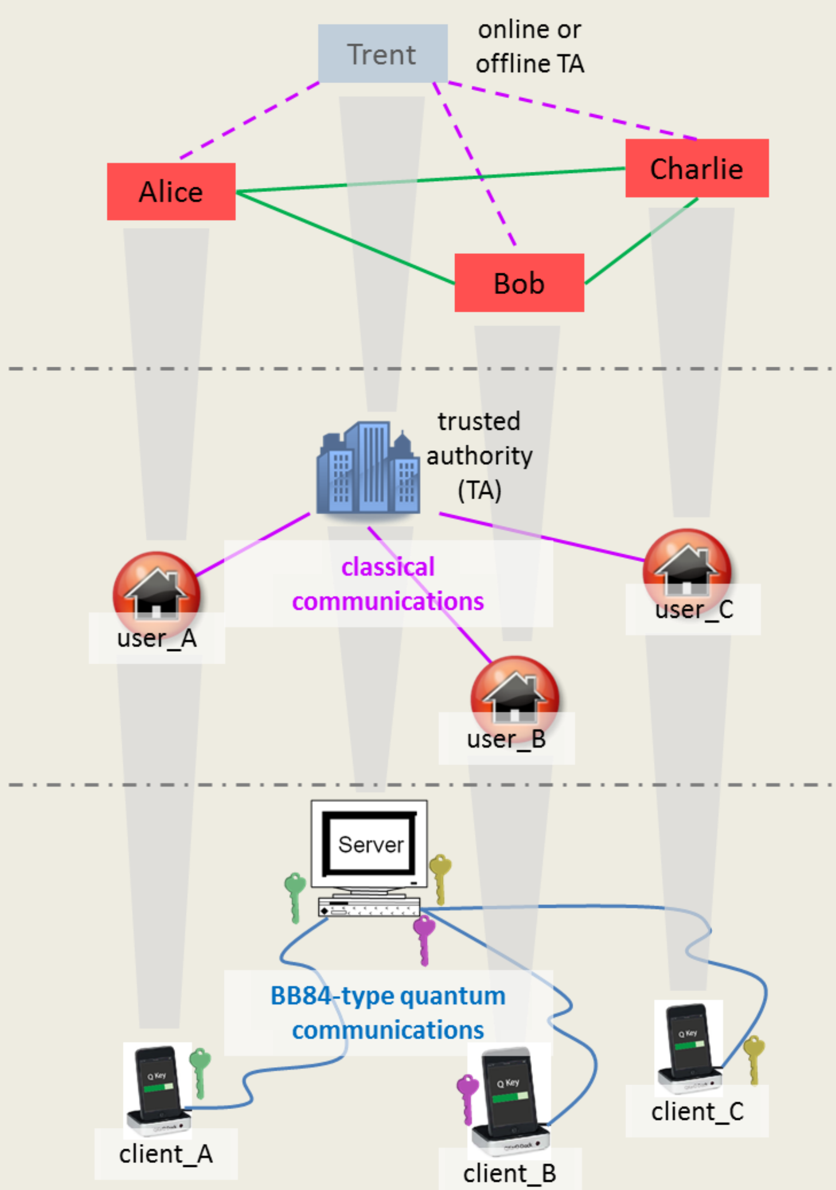


New cyber attack opportunities: challenges for cryptography

Los Alamos NATIONAL LABORATORY EST. 1943

LDRD

NQC invention: architecture



application layer:

- confidentiality
- authenticity
- integrity
- non-repudiation
- between users who may have no direct QC

quantum key management (QKM) layer:

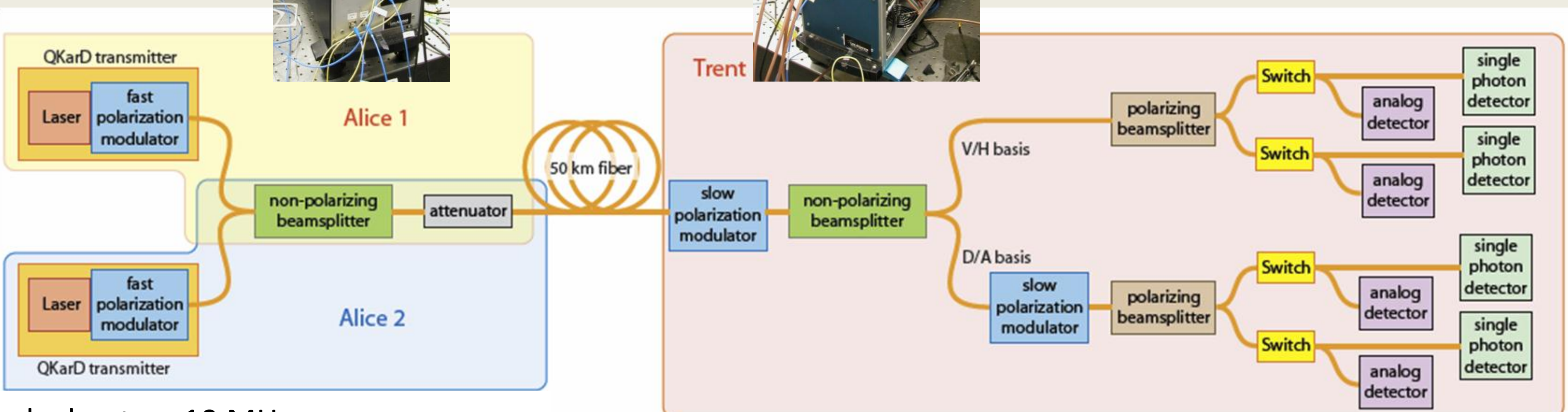
- classical protocols built from quantum primitives
  - key establishment
  - signatures
  - certificates

quantum protocol layer:

- quantum identification (QID)
- quantum key distribution (QKD)
- quantum secret splitting (QSS)

NQC testbed constructed using repurposed QC hardware

- 3-client / 1-server configuration
  - + hardware for up to 3 additional clients



clock rate = 10 MHz
wavelength = 1,550nm
mean photon no., μ = 0.2
•+ decoy protocol: μ = 0.7, 0.1, 0

50-km fiber spool
- redefine first portion of fiber to be within Alice's enclave for shorter ranges

InGaAs APDs

~kbps @ 50km
ber ~0.05
~1000 sessions, 1 sec each

Los Alamos NATIONAL LABORATORY EST. 1943

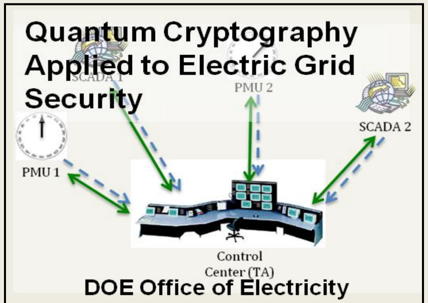
Quantum Communications: Some future directions

- Implementation of other primitives using photons
- Long distance QKD?
- Higher key bit rate?
- Fast random number generation

Los Alamos NATIONAL LABORATORY EST. 1943

LDRD

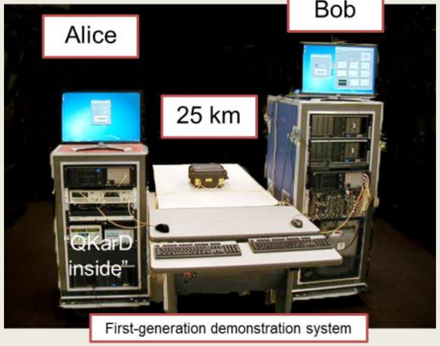
Follow on projects



DOE Office of Electricity Delivery and Energy Reliability

PI: J. E. Nordholt, P-21
LANL PM: K. Jonietz

Deliverable



Demonstrated in DOE testbed at UIUC, Dec 11, 2012

World's Fastest Quantum Random Number Generator

P.I.: J. E. Nordholt, P-21
LANL PM: G. A. Erickson

Funded: $450K (phase 1)

QUINESS

ultra-long distance QC in optical fiber: 10x state-of-the-art

P.I.: R. Newell, P-21

QRNG development

P.I.: J. E. Nordholt, P-21

"Internet and cloud security anchored in innovative RNG", K. McCabe (PI)

NQC: Publications & more

Refining quantum cryptography, Richard Hughes and Jane Nordholt, invited "Perspectives", Science 333, 1584 (2011)

Secure multi-party communication with quantum key distribution managed by trusted authority, R. J. Hughes, J. E. Nordholt, and C. G. Peterson. World Intellectual Property Organization, WO/2012/044855 *(2012)*

40Mbit/sec free-space optical communication link with real-time quantum encryption, R. T. Newell, J. E. Nordholt, C. G. Peterson, R. J. Hughes, LA-UR-11-06775 (2011).

Quantum Hacking, R. J. Hughes and J. E. Nordholt, Journal of Intelligence Community Research and Development, 18 August, 2011.

Optical Security for Transparent Networks: Data Obscuration and Quantum Cryptography, Richard Hughes and Jane Nordholt, to appear in "The Next Wave – The National Security Agency's Review of Emerging Technologies".

Secure Communications to, from and in space, R. J. Hughes and J. E. Nordholt, LA-UR-12-26206, in "Quantum Communication, Sensing and Measurement in space" (2012), Keck Institute for Space Studies workshop report, http://www.kiss.caltech.edu/study/quantum/index.html.

Security of decoy-state protocols for general photon number splitting attacks, Rolando D. Somma and Richard Hughes, Phys. Rev. A87, 062330 (2013).

Network centric quantum communications with applications to critical infrastructure protection, Richard Hughes, Jane Nordholt, Kevin McCabe, Raymond Newell, Charles Peterson, and Rolando Somma, arXiv:1305.0305 (2013).

Quantum Computing and Quantum Communications at LANL

Rolando D. Somma
Theory Division
Los Alamos National Laboratory
Please, email me at somma@lanl.gov for additional questions

THANK YOU!!

Los Alamos NATIONAL LABORATORY EST. 1943

LDRD