Colin P. Williams (JPL)

NASA QUANTUM NETWORK

Collaborators:
Vadim Smelyanskiy (NASA Ames), Gabriel Durkin (NASA Ames), Bill Farr (JPL), Baris Erkmen (JPL), Paul Averill (JPL), Paul Toliver (Telcordia), Thomas Chapuran (Telcordia), Vikram Sharma (Quintessence Labs), Andrew Lance (Quintessence Labs)

Objective

- Create a prototype unconditionally secure NASA communications network, spanning terrestrial and Space links …
- …such that security is guaranteed *regardless* of an adversary's
  - Computing power
  - Mathematical genius
  - Cryptanalytic sophistication
- Use keys to protect both data in transit and data at rest

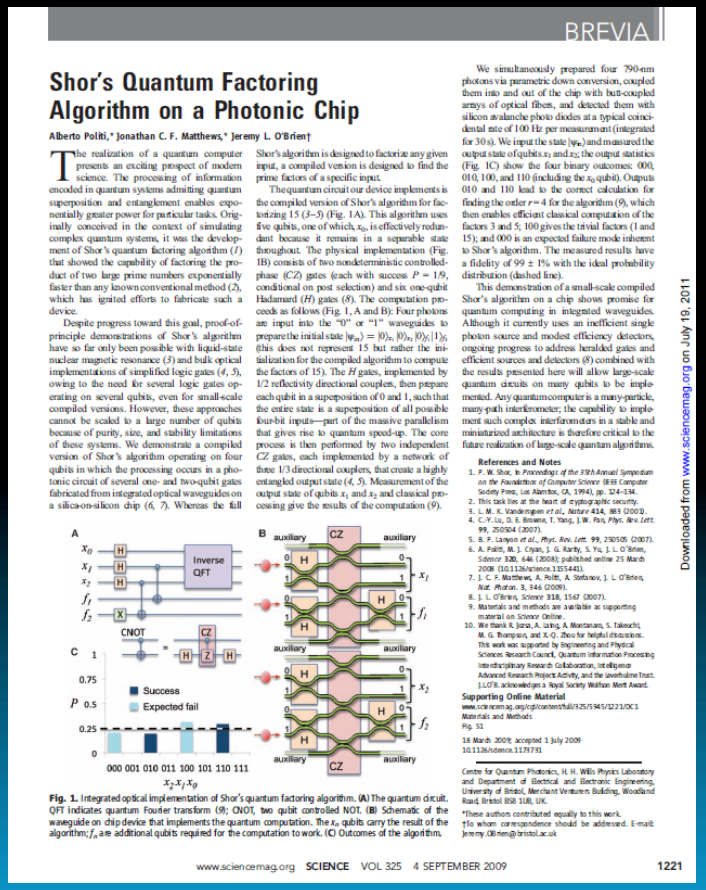
Impact if Successful

- Guarantees confidentiality in sharing of ITAR and export controlled data between centers & s/c
- Decreases vulnerability of Space assets such as satellites, telescopes, Space-stations, fuel-stores, interferometers, to "spoofed" commands
- Enhances safety of astronauts during missions
- No further upgrades will ever be necessary due to security concerns
  - Only optional upgrades for higher speeds if desired
- Extensible to microwave wavelengths[1]
- Proof of security established

[1] Preliminary work on extension to microwave wavelengths is reported in Christian Weedbrook, Stefano Pirandola, Seth Lloyd, and Timothy C. Ralph, "Quantum Cryptography Approaching the Classical Limit", Phys. Rev. Lett. 105, 110501 (2010)

Current NASA Network Security

- Current network security is based on standard firewalls & public-key infrastructure (PKI)
- Security of all public-key cryptosystems depends on the presumption that certain computations are intractable
  - Factoring integers breaks RSA
  - Computing discrete logarithms breaks elliptic curve
- But factoring & discrete logs are easy for quantum computers …
- Even conventional cloud computing poses a threat if a adversaries amass enough computing power



BREVIA

Shor's Quantum Factoring Algorithm on a Photonic Chip

Alberto Politi,* Jonathan C. F. Matthews,* Jeremy L. O'Brien†

The realization of a quantum computer presents an exciting prospect of modern science. The processing of information encoded in quantum systems admitting quantum superposition and entanglement enables exponentially greater power for particular tasks. Originally conceived in the context of simulating complex quantum systems, it was the development of Shor's quantum factoring algorithm (*1*) that showed the capability of factoring the product of two large prime numbers exponentially faster than any known conventional method (*2*), which has ignited efforts to fabricate such a device.

Despite progress toward this goal, proof-of-principle demonstrations of Shor's algorithm have so far only been possible with liquid-state nuclear magnetic resonance (*3*) and bulk optical implementations of simplified logic gates (*4*, *5*), owing to the need for several logic gates operating on several qubits, even for small-scale compiled versions. However, these approaches cannot be scaled to a large number of qubits because of purity, size, and stability limitations of these systems. We demonstrate a compiled version of Shor's algorithm operating on four qubits in which the processing occurs in a photonic circuit of several one- and two-qubit gates fabricated from integrated optical waveguides on a silica-on-silicon chip (*6*, *7*). Whereas the full Shor's algorithm is designed to factorize any given input, a compiled version is designed to find the prime factors of a specific input.

The quantum circuit our device implements is the compiled version of Shor's algorithm for factorizing 15 (*3*–*5*) (Fig. 1A). This algorithm uses five qubits, one of which, x_0, is effectively redundant because it remains in a separable state throughout. The physical implementation (Fig. 1B) consists of two nondeterministic controlled-phase (*CZ*) gates (each with success $P = 1/9$, conditional on post selection) and six one-qubit Hadamard (*H*) gates (*8*). The computation proceeds as follows (Fig. 1, A and B): Four photons are input into the "0" or "1" waveguides to prepare the initial state $|\psi_{in}\rangle = |0\rangle_{x_0}|0\rangle_{x_1}|0\rangle_{x_2}|1\rangle_{f_1}|1\rangle_{f_2}$ (this does not represent 15 but rather the initialization for the compiled algorithm to compute the factors of 15). The *H* gates, implemented by 1/2 reflectivity directional couplers, then prepare each qubit in a superposition of 0 and 1, such that the entire state is a superposition of all possible four-bit inputs—part of the massive parallelism that gives rise to quantum speed-up. The core process is then performed by two independent *CZ* gates, each implemented by a network of three 1/3 directional couplers, that create a highly entangled output state (*4*, *5*). Measurement of the output state of qubits x_1 and x_2 and classical processing give the results of the computation (*9*).

We simultaneously prepared four 790-nm photons via parametric down conversion, coupled them into and out of the chip with butt-coupled arrays of optical fibers, and detected them with silicon avalanche photo diodes at a typical coincidental rate of 100 Hz per measurement (integrated for 30 s). We input the state $|\psi_{in}\rangle$ and measured the output state of qubits x_1 and x_2; the output statistics (Fig. 1C) show the four binary outcomes: 000, 010, 100, and 110 (including the x_0 qubit). Outputs 010 and 110 lead to the correct calculation for finding the order $r = 4$ for the algorithm (*9*), which then enables efficient classical computation of the factors 3 and 5; 100 gives the trivial factors (1 and 15); and 000 is an expected failure mode inherent to Shor's algorithm. The measured results have a fidelity of 99 ± 1% with the ideal probability distribution (dashed line).

This demonstration of a small-scale compiled Shor's algorithm on a chip shows promise for quantum computing in integrated waveguides. Although it currently uses an inefficient single photon source and modest efficiency detectors, ongoing progress to address heralded gates and efficient sources and detectors (*8*) combined with the results presented here will allow large-scale quantum circuits on many qubits to be implemented. Any quantum computer is a many-particle, many-path interferometer; the capability to implement such complex interferometers in a stable and miniaturized architecture is therefore critical to the future realization of large-scale quantum algorithms.

References and Notes

1. P. W. Shor, in *Proceedings of the 35th Annual Symposium on the Foundations of Computer Science* (IEEE Computer Society Press, Los Alamitos, CA, 1994), pp. 124–134.
2. This task lies at the heart of cryptographic security.
3. L. M. K. Vandersypen *et al.*, *Nature* **414**, 883 (2001).
4. C.-Y. Lu, D. E. Browne, T. Yang, J.-W. Pan, *Phys. Rev. Lett.* **99**, 250504 (2007).
5. B. P. Lanyon *et al.*, *Phys. Rev. Lett.* **99**, 250505 (2007).
6. A. Politi, M. J. Cryan, J. G. Rarity, S. Yu, J. L. O'Brien, *Science* **320**, 646 (2008); published online 25 March 2008 (10.1126/science.1155441).
7. J. C. F. Matthews, A. Politi, A. Stefanov, J. L. O'Brien, *Nat. Photon.* **3**, 346 (2009).
8. J. L. O'Brien, *Science* **318**, 1567 (2007).
9. Materials and methods are available as supporting material on *Science* Online.
10. We thank R. Jozsa, A. Laing, A. Montanaro, S. Takeuchi, M. G. Thompson, and X.-Q. Zhou for helpful discussions. This work was supported by Engineering and Physical Sciences Research Council, Quantum Information Processing Interdisciplinary Research Collaboration, Intelligence Advanced Research Project Activity, and the Leverhulme Trust. J.L.O'B. acknowledges a Royal Society Wolfson Merit Award.

Supporting Online Material

www.sciencemag.org/cgi/content/full/325/5945/1221/DC1
Materials and Methods
Fig. S1

18 March 2009; accepted 1 July 2009
10.1126/science.1173731

Centre for Quantum Photonics, H. H. Wills Physics Laboratory and Department of Electrical and Electronic Engineering, University of Bristol, Merchant Venturers Building, Woodland Road, Bristol BS8 1UB, UK.

*These authors contributed equally to this work.
†To whom correspondence should be addressed. E-mail: jeremy.OBrien@bristol.ac.uk

Recent NASA Incidents

- NASA networks are not sufficiently secure
- Recent incidents include:
  - 2009
    - "Cybercriminals infected NASA system that supports one of NASA's mission networks" U.S. OIG Audit Report (IG-11-017)
  - 2009
    - "22GB of export restricted data stolen from JPL" U.S. OIG Audit Report (IG-11-017)
  - 2011
    - "Inadequate Security Practices Expose Key NASA Network to Cyber Attack" U.S. OIG Audit Report (IG-11-017)
- Commercial satellite communications also vulnerable
  - 2002
    - "Commercial Satellite Security Should Be More Fully Addressed" U.S. GAO Report (GAO-02-781)

Recent Non-NASA Incidents

- "Night Dragon" (2009 onwards)
  - Systematic long term compromise of Western oil & gas companies
- "Aurora" (Jan 14, 2010)
  - Intruded Google + 2 dozen other companies
- "Shady Rat" (2006-2011)
  - Sustained global cyber-espionage attack on business and governments across 14 countries
- Believed orchestrated by a nation state

Operation "Shady Rat" Attacks

1. Source: "Global Energy Industry Hit in Night Dragon Attacks", http://blogs.mcafee.com/corporate/cto/global-energy-industry-hit-in-night-dragon-attacks
2. Operation Aurora, http://www.mcafee.com/us/threat-center/operation-aurora.aspx
3. Source: "Operation Shady Rat" http://blogs.mcafee.com/mcafee-labs/revealed-operation-shady-rat

Stated NASA Need …

- Need "unconditional information security"
  - Page 8 of NASA *Communication & Navigation Systems* Technology Roadmap

Table 1. *Example Challenge Progress Goals*

Challenge	Example Progress Goals		
	Near-term (thru 2016)	Midterm (2017-2022)	Far-term (2023-2028)
1 Remove Comm. as a Constraint		200 Mbps from 1 AU 30 Gbps from LEO	20 Gbps from 1 AU 3 Tbps from LEO
2 Remove Nav. as a Constraint	Increased reliance on next generation international GNSS (GPS, GLONAS, Galileo) receiver based navigation below GEO as well as a technology push for in-situ navigational observations, sensor data fusion, and autonomous PNT	Increased reliance on in-situ observations, data fusion, and autonomous PNT; supervised autonomy for missions beyond GEO	Fully autonomous PNT functions for all missions throughout the solar system; GPS-like navigation at Mars
3 Minimize Impact of Latency	Navigation/timekeeping to support -Semi-Autonomous pinpoint landing with 100-m accuracy: - Millimeter-level formation control	Navigation/timekeeping to support: -Autonomous pinpoint landing with 10-m ac-curacy - Micrometer-level formation control	Navigation/timekeeping to support: -Autonomous pinpoint landing with 1-m accuracy - Nanometer-level formation control
4 Minimize user burden		Reduction of 50% in transponder mass	Reduction of 75% in transponder mass
5 Integrity & Assurance	Interplanetary info security including international trust relation-ships with conditional security levels Validate unconditional information security techniques to low-Earth orbit (LEO)	Standard international trust relationships established and managed operationally Unconditional information security techniques employed with LEO and some deep-space missions	Global information trust relationships Internationally-standard unconditional information security with all space missions
6 Lower Lifecycle Cost	20% Reduction from current	40% Reduction from current	80% Reduction from current
7 Lack of Demo's	Optical comm. demo	Multi-function SDR demo	Deep space relay tech demo

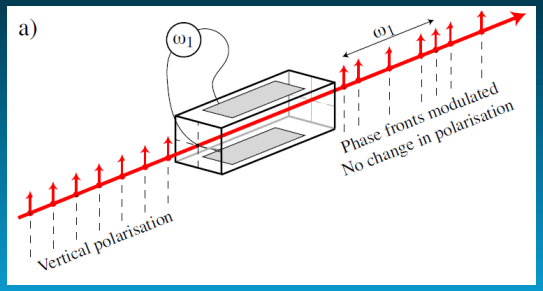
Source: Page TA05-8 in http://www.nasa.gov/pdf/501623main_TA05-CommNav-DRAFT-Nov2010-A.pdf

Solution: CV-QKD

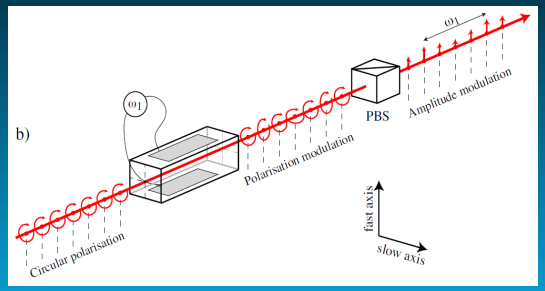
- Provides unconditionally secure communications based on Continuous Variable Quantum Key Distribution (CV-QKD)
  - **Key Generation**: Uses quantum non-determinism to generate truly random cryptographic keys
  - **Key Distribution**: Imprints them onto the amplitude and phase quadratures of a coherent laser beam. Security of the keys relies upon the impossibility of cloning unknown quantum states perfectly and limits on the knowledge one can have about non-commuting observables set by the Heisenberg Uncertainty Principle
  - **Key Distillation**: Performs error reconciliation & privacy amplification to distill out the secret key material
  - **Key Exploitation**: Uses the secret keys to implement an unconditionally secure classical cryptosystem such as a one time pad
- **Meets stated NASA requirement** for **"unconditional information security"** in new NASA Technology Roadmap
  - Supersedes prior DARPA & IARPA quantum networks by achieving higher data rates & greater compatibility with fiber and free-space laser optical comm.

What are "Amplitude" & "Phase" Quadratures?

- EM field is quantized by associating a quantum harmonic oscillator (QHO) with each mode of the radiation field
- QHO for a particular mode has a destruction operator "a" and a creation operator "$a^\dagger$"
  - "a" and "$a^\dagger$" not Hermitian and hence not observables
  - But certain operators built from them *are* observables:
    - $X^+ = a^\dagger + a$ = amplitude quadrature operator
    - $X^- = i\,(a^\dagger - a)$ = phase quadrature operator
    - X^+ and X^- are conjugate observables obeying the Heisenberg Uncertainty Principle
  - We imprint information on the phase and amplitude quadratures via phase and/or amplitude modulation



Imprinting information via phase modulation

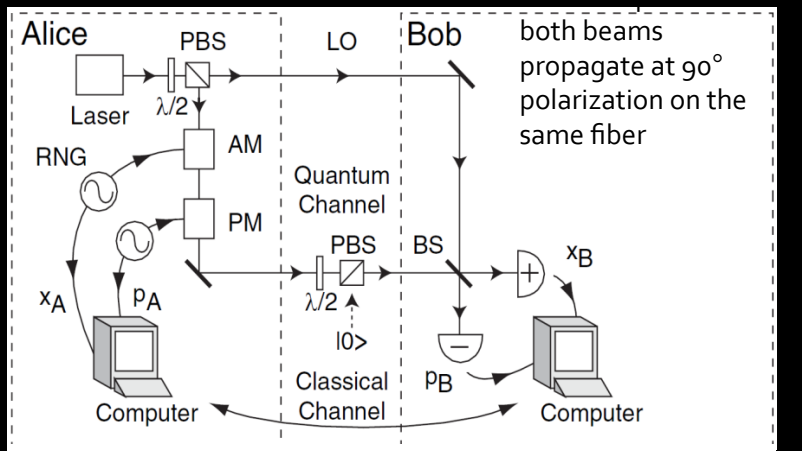


Imprinting information via amplitude modulation

CV-QKD Protocol (No-Switching)

Approach to CV-QKD based on the "no-switching" protocol[1]

1. Alice draws two random numbers, x_A and p_A, from two Gaussian distributions having mean zero and variance $V(x_A)$ and $V(p_A)$
2. Alice's prepares coherent state $|x_A + i\,p_A\rangle$ and sends it to Bob
3. Bob simultaneously measures both the amplitude (x_B) and phase (p_B) quadratures of the state on a 50:50 beam splitter. This creates correlated random data i.e., raw key material
4. Alice & Bob perform post-selection to ensure Eve's knowledge of Alice's key falls behind the information shared between Alice and Bob
5. Alice & Bob then perform error reconciliation & privacy amplification to distil out the key



PBS = polarizing beam splitter
RNG = random number generator
AM = amplitude modulator
PM = phase modulator
x_A = Alice's amplitude quadrature
p_A = Alice's phase quadrature
x_B = Bob's amplitude quadrature
p_B = Bob's phase quadrature
$|0\rangle$ = vacuum (channel noise added)
LO = local oscillator (for homodyne detection by Bob)

[1] C. Weedbrook, A. M. Lance, W. P. Bowen, T. Symul, T. C. Ralph, & P. K. Lam, "Quantum Cryptography without Switching," Phys. Rev. Lett. 93, 170504 (2004).

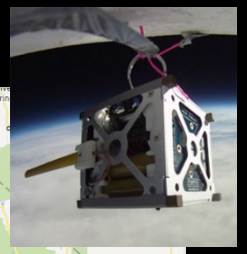
DV-QKD vs CV-QKD

- Most prior systems based on discrete variables (DV-QKD)
- We use quantum continuous variables (CV-QKD) & "no switching" protocol
  - Choice of quantum continuous variables allows use of COTS telecommunications components & "no-switching" CV-QKD is much faster than CV-QKD with basis switching

	DV-QKD	CV-QKD
Source	**Single photon source or strongly attenuated laser** • Difficult & resource intensive to produce single photons on demand • But use of attenuated laser opens security loophole (photon-number splitting attack) • Security can be improved using decoy state protocols	**Weakly modulated coherent laser** • Readily produced by COTS lasers • Use sideband frequencies > 50MHz have capacity to carry quantum information • Information encoded onto amplitude and phase quadratures using COTS amplitude and phase modulators • Modulators with bandwidths of 10-40GHz readily available
Detector	**Single photon detectors** • Key distribution rate limited by speed of single photon detectors • This depends on finite quantum detection efficiency, dark count rate, timing resolution (jitter), and recovery time (dead time)	**Homodyne detectors** • Amplitude and phase quadratures can be detected using COTS balanced homodyne detectors • Shot-noise to electronic dark noise clearance exceeding 10dB for bandwidth > 3GHz • Detector bandwidth could scale to 10GHz
Basis switching	**Needed** • Must constantly switch measurement basis • Cannot measure two orthogonal bases simultaneously	**Not needed (!)** • No need to switch measurement basis • Can encode information onto both the phase and amplitude quadratures • Can simultaneously measure both the phase and amplitude quadratures • Enables very high key exchange rates

NASA Quantum Network

- **Terrestrial CV-QKD Network**
  - Runs on DOE's ESnet dark fiber backbone
  - High key rates
  - Long haul fiber CV-QKD (~550km)
  - Shared classical / quantum traffic
  - Use of DWDM in quantum communications
  - CV quantum relays (near term)
  - CV quantum repeaters (long term)
  - CV optical routers
- **Free space CV-QKD Networks**
  - Intra-city links
  - Links to UAVs and aircraft
  - Links to satellites
  - Fiber to free-space optical interconnects
- **Theory component**
  - Proof of security specialized to real channel
  - Theory of protocols, turbulence, effect of losses



Dark fiber path from L.A. to Sunnyvale

A	818 West 7th Street, Los Angeles, CA, 90017
B	5245 Kazuko Court, Moorpark, CA 93021
C	1667 Walter St, Ventura, CA 93003
D	122 Helena Ave, Santa Barbara, CA 93101
E	331 N A St, Lompoc, CA 93436
F	775 Capitolio Way, San Luis Obispo, CA 9340
G	61921 Cattlemen Rd, San Ardo, CA 63450
H	500 Front St #A, Soledad, CA 93960
I	South Street, San Martin, CA 95046
J	1380 Kifer Rd, Sunnyvale, California 94086

Current Team

- **NASA (JPL & Ames)**
  - Quantum cryptographic protocols / security proofs / loopholes
  - Quantum optics / opto-electronics design / optics fabrication
  - Deep Space optical comm / pointing & tracking / Table Mountain
  - Knowledge of atmospheric channels
  - Local network integration
- **Telcordia**
  - Experienced in practical quantum networking (Washington, D.C.)
    Optical routers / network management
- **QuintessenceLabs**
  - Commercial quality CV-QKD components
  - Error reconciliation / privacy amplification software / packaging
  - Inventors of CV-QKD and no-switching protocol
- **ESnet**
  - Dark fiber & access sites from Los Angeles to Sunnyvale

NASA Experience: Optical Communications

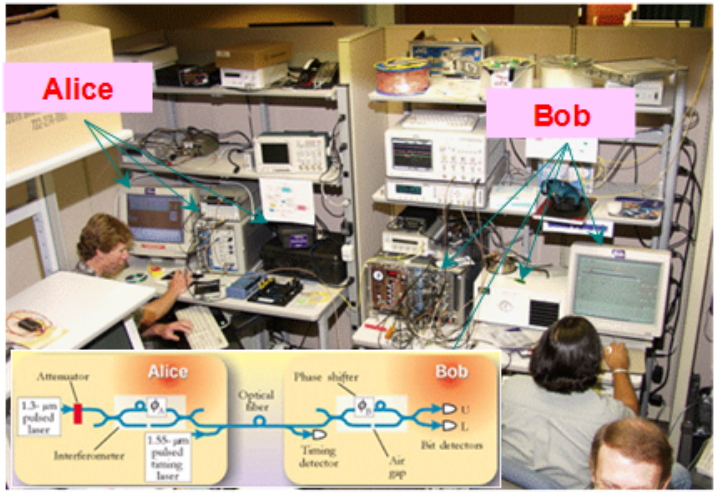
- NASA missions are generating progressively more data which must be transmitted back to Earth reliably, efficiently, and inexpensively
- Optical communications key to realizing the NASA goals of a virtual presence in space and development of an interplanetary network
- Payoffs:
  - 10 – 100x increase in data transmission rates
  - Reduction of the antenna area to 1% of current size
  - Reductions of weight, moment and power

Optical communications enables missions to communicate further into deep space because of its high bandwidth, low mass and low power consumption.

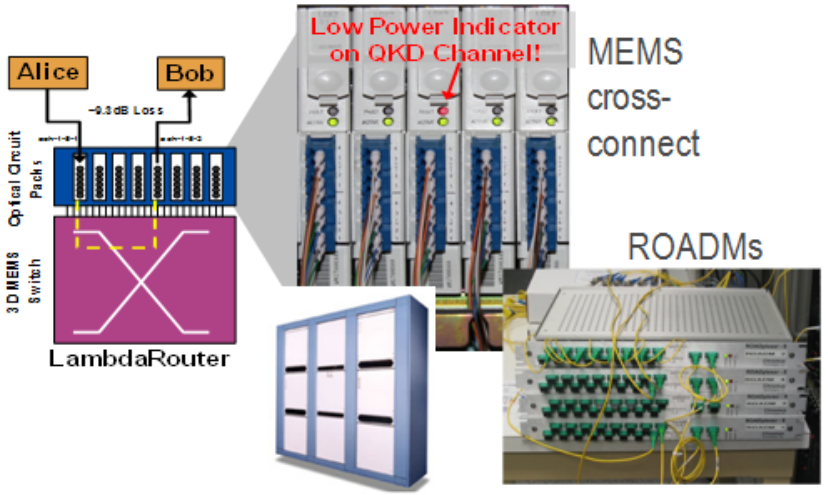
- Optical communications demos:
  - High-data rate laser pulse transmission
  - Space-based optical receiver
  - Space-based optical pointing
- JPL Optical Communications Group has the experience, capabilities, and facilities to support development of a deep-space optical comm demonstration experiments

Telcordia Experience: Quantum Networks

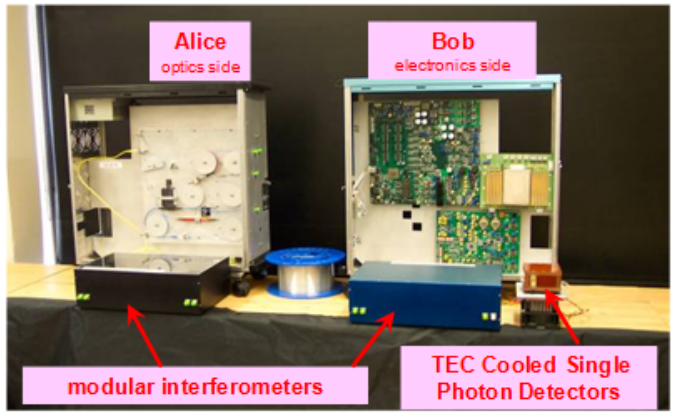
LANL 2nd generation fiber QKD system (F2)



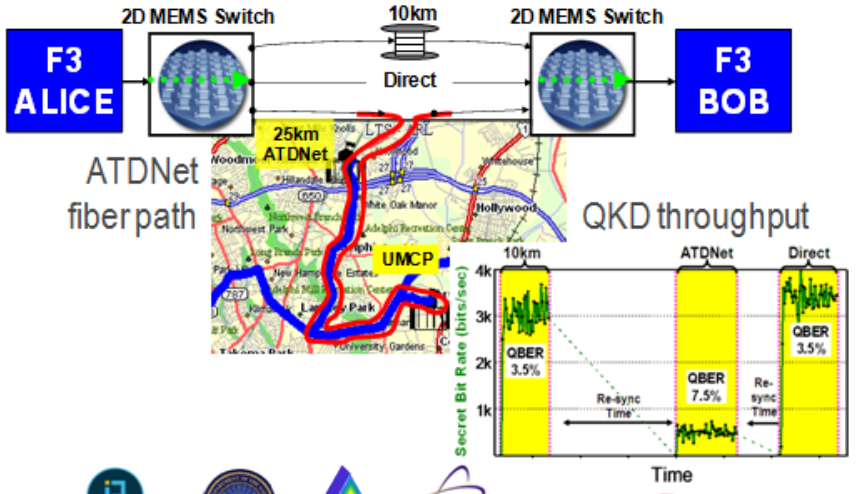
QKD Transmission through all-optical switches



LANL 3rd generation fiber QKD system (F3)



QKD Transmission through optical switches and ATDNet



Ref: R. J. Hughes and T.E. Chapuran, "Introduction to Quantum Cryptography", *Optical Fiber Communications (OFC) Short Course*, Los Angeles, CA, 2011

IARPA LTS Los Alamos NATIONAL LABORATORY Telcordia

Quintessence Experience: CV-QKD

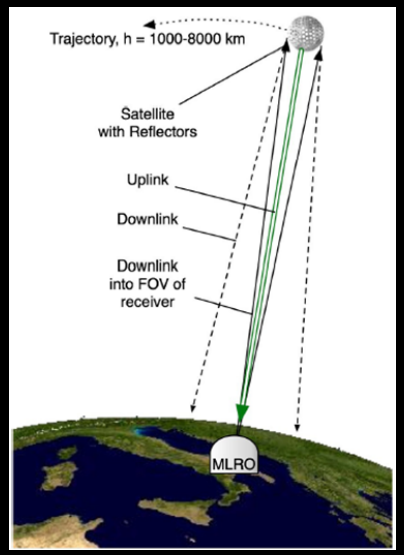
- Quintessence Labs Pty Ltd, is an Australian company based on R&D at Australian National University and is opening a U.S. subsidiary
- Offers products across 4 functional layers including link encryption based on CV-QKD and the one-time pad cipher
- Result is unconditionally secure communications with security guaranteed by the laws of quantum mechanics

Functional Layer	Performance/Feature Target
Cryptographic support	Link and network encryption appliances supporting legacy and one-time pad ciphers Gbit/s traffic throughput with low latency Embeddable key management client software libraries Third party device and application support
Key management	Secure generation, storage, distribution, and destruction of keys Encryption policy and control Monitoring and auditing OASIS KMIP interface Key material and meta data replication Separation of duty
Quantum key distribution	Continuous variable quantum key distribution Fibre optic and free space quantum channels Up to 100 km separation using SMF 28e optical fibre Secret key rate up to 10's Mbit/s
Entropy Source	Quantum entropy source Optical and electronic, hardware true RNG Very high speed – 10's Gbit/s

State-of-the-Art in Space-based QKD

- **European Union & European Space Agency have supported development of QKD in fiber networks and free space**
  - Feasibility of 300 km Quantum Key Distribution with Entangled States, New J. Phys. 11, 085002 (2009)
  - The SECOQC Quantum Key Distribution Network in Vienna, New J. of Physics 11, 075001 (2009).
  - Transmission of Entangled Photons over a High-Loss Free-Space Channel, www.2Physics.com (May 30, 2009).
  - A Fully Automated Entanglement-based Quantum Cryptography System for Telecom Fiber Networks, New J. of Physics 11, 045013 (2009).
  - Quantum Communications at ESA: Towards a Space Experiment on the ISS, Acta Astronautica 63, 165 – 178 (2008).
  - Experimental Verification of the Feasibility of a Quantum Channel between Space and Earth, New J.of Physics 10, 033038 (2008).
  - Space-QUEST. Experiments with Quantum Entanglement in Space, Proceedings of the 2008 Microgravity Sciences and Process Symposium, quant-ph/ 0806.0945v1 (2008).
  - Entanglement-based quantum communication over 144 km, Nature Physics 3, 481 - 486 (2007); Nature Highlight of the Year 2007

- **European Union / European Space Agency have much expertise**
- **If interested in partnering contact me**



Graphical representation of experiment performed between the Matera Laser Ranging Observatory in Italy to the Ajisai satellite, at some 1485 km above the Earth in March 2008. This experiment proved the feasibility of sending single photons between a satellite and Earth

Who Cares?

Stakeholder	Motivation
DOD	• Need assured GPS, command, control, communications, reconnaissance, surveillance, mission video feed capabilities • DARPA, ONR, and USAF funded only discrete variable QKD previously
NASA	• Missions need to prevent unauthorized commanding of spacecraft • Must ensure security of ITAR and Export Controlled Data
Intelligence	• NRO needs to ensure downlinked imagery is confidential • CIA/NSA needs assured confidential communications
NOAA	• Needs to prevent unauthorized commanding of satellites
State Department	• Need to ensure diplomatic communiqués are kept confidential
Federal Reserve / Treasury / Banks	• Need to be able to talk discreetly to stabilize markets • Need to execute financial transactions confidentially
FAA	• Need to be able to rely on GPS and satellite communications
DOE / DHS / Utilities	• Critical infrastructure protection, e.g, power, water, gas
Healthcare	• Need to increase electronic patient record keeping and sharing yet ensure patient confidentiality
Commercial Space	• Share similar issues as NASA. Insurance companies underwriting commercial Space services must minimize risk of loss of services & s/c

Technical Challenges

- Extending the range of CV-QKD in fiber, e.g., by:
  - Modifying the optical states and/or protocol
  - Developing a true CV quantum repeater (initial work in [1])
- Extending the range of CV-QKD in free space, e.g., by:
  - Modifying the quantum states and/or protocol
  - Pushing CV-QKD to microwave wavelengths (initial work in [2])
- Demonstrating CV-QKD between moving platforms over atmospheric channels
- Proving the security of the CV-QKD protocol we shall develop
- Ensuring any given *implementation* of CV-QKD is secure *in practice* i.e., loophole free, not just secure in theory
  - Requires firewalled team of motivated quantum hackers
- Boosting the key distribution rate to Gbps

1. Nicolas Sangouard, Christoph Simon, Nicolas Gisin, Julien Laurat, Rosa Tualle-Brouri, and Phillipe Grangier, "Quantum Repeaters with Entangled Coherent States," J. Opt. Soc. Am. B, Vol. 27, No. 6, June (2010)
2. Christian Weedbrook, Stefano Pirandola, Seth Lloyd, and Timothy C. Ralph, "Quantum Cryptography Approaching the Classical Limit", Phys. Rev. Lett. 105, 110501 (2010)

Summary

- Previous QKD systems use discrete variables, i.e., single photon sources, single photon detectors, and must constantly switch bases and implement DV-QKD
- We use continuous variables (CV-QKD), bright coherent lasers, homodyne detection, and need not switch basis
- CV-QKD simplifies implementation and has the potential to scale to faster key rate and greater range
- CV-QKD offers potential to permanently secure NASA communications
- Also CV-QKD especially well suited to free-space optical communications
- We propose a fully integrated fiber and free-space CV-QKD system
- Our team consists of the inventors of CV-QKD, the no-switching protocol, quantum optics experts, & companies experienced in quantum networking
- Staged milestones allow measurable progress and build synergistically towards end-to-end system

NASA APPLICATIONS OF QUANTUM COMPUTING

Colin P. Williams
Jet Propulsion Laboratory
Colin.P.Williams@jpl.nasa.gov, 650-242-2051

Vadim Smelyanskiy
NASA Ames
Vadim.N.Smelyanskiy@nasa.gov, 650-604-2261

Why is NASA Interested in Quantum Computers?

- Harness quantum physical phenomena not available to conventional computers
  - E.g., superposition, interference, entanglement, non-locality, non-determinism, non-clonability
- Allows us to solve problems in new ways
  - E.g., can operate on all 2^n combinations of *n* bits simultaneously and extract a collective property of the result in the time it takes to do the same operation on just one of these n-bit strings classically
  - Most profound advance in computer science in 100 yrs

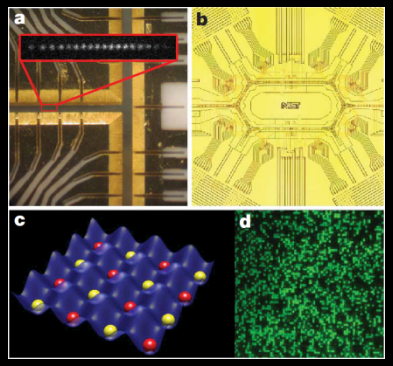
Alternative Models of Quantum Computing

Alternative Models

- Quantum Circuit Model
- Higher base quantum logic – qu*d*its
- One-way quantum computers
- Exchange-only quantum computers
- Quantum cellular automata
- Topological quantum computers
- Adiabatic quantum computers

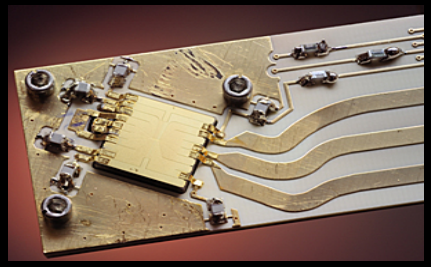
Progress in Quantum Hardware

Trapped ion & trapped neutral atom quantum processors



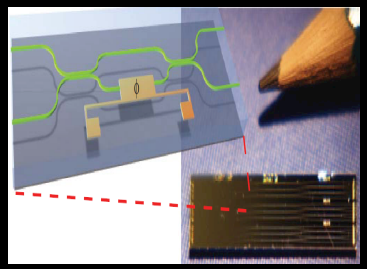
TODAY: Trapped atom qubits. a, Multi-level linear ion trap chip; the inset displays a linear crystal of several $^{171}Yb^{+}$ ions fluorescing when resonant laser light is applied (the ion–ion spacing is 4 mm). b, Surface ion trap chip with 200 zones distributed above the central hexagonal racetrack of width 2.5mm. c, Schematic of optical lattice of cold atoms formed by multi-dimensional optical standing wave potentials. d, Rb atoms from a Bose condensate confined in a 2D optical lattice, with atom–atom spacing of 0.64 mm.

New trapped ion quantum chip with microwave coupling



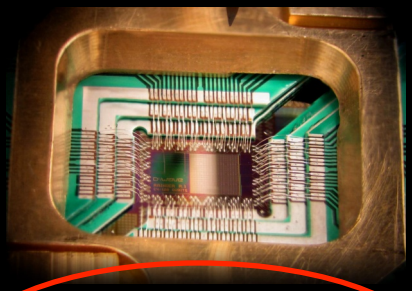
TODAY: A 2 qubit gold ion trap on aluminum nitride backing. Two ions hover above the middle of the square gold trap, which measures 7.4 millimeters on a side. The ions are manipulated and entangled using microwaves fed into wires on the trap from the three thick electrodes at the lower right[1].

Photonic quantum chip



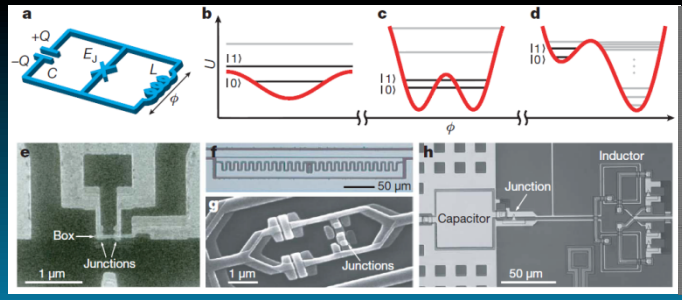
TODAY: A 10-qubit photonic chip containing 10 silica waveguide interferometers with thermo-optic controlled phase shifts for photonic quantum gates. Green lines show optical waveguides; yellow components are metallic contacts. Pencil tip shown for scale[2].

DWave special purpose adiabatic quantum computer

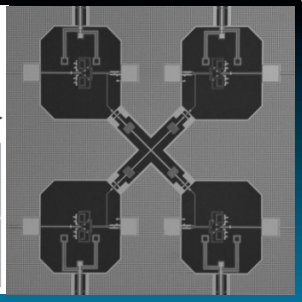


TODAY: DWave-1 Rainier 128-qubit superconducting quantum annealing machine.

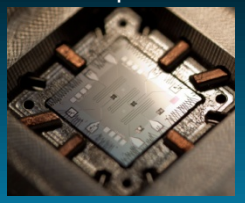
Conventional superconducting quantum chips



Charge-based qubit (Schoelkopf) | Flux-based qubit (Mooij) | Phase-based qubit (Martinis)



TODAY: 2-qubit super-conducting von Neumann architecture chip demonstrated

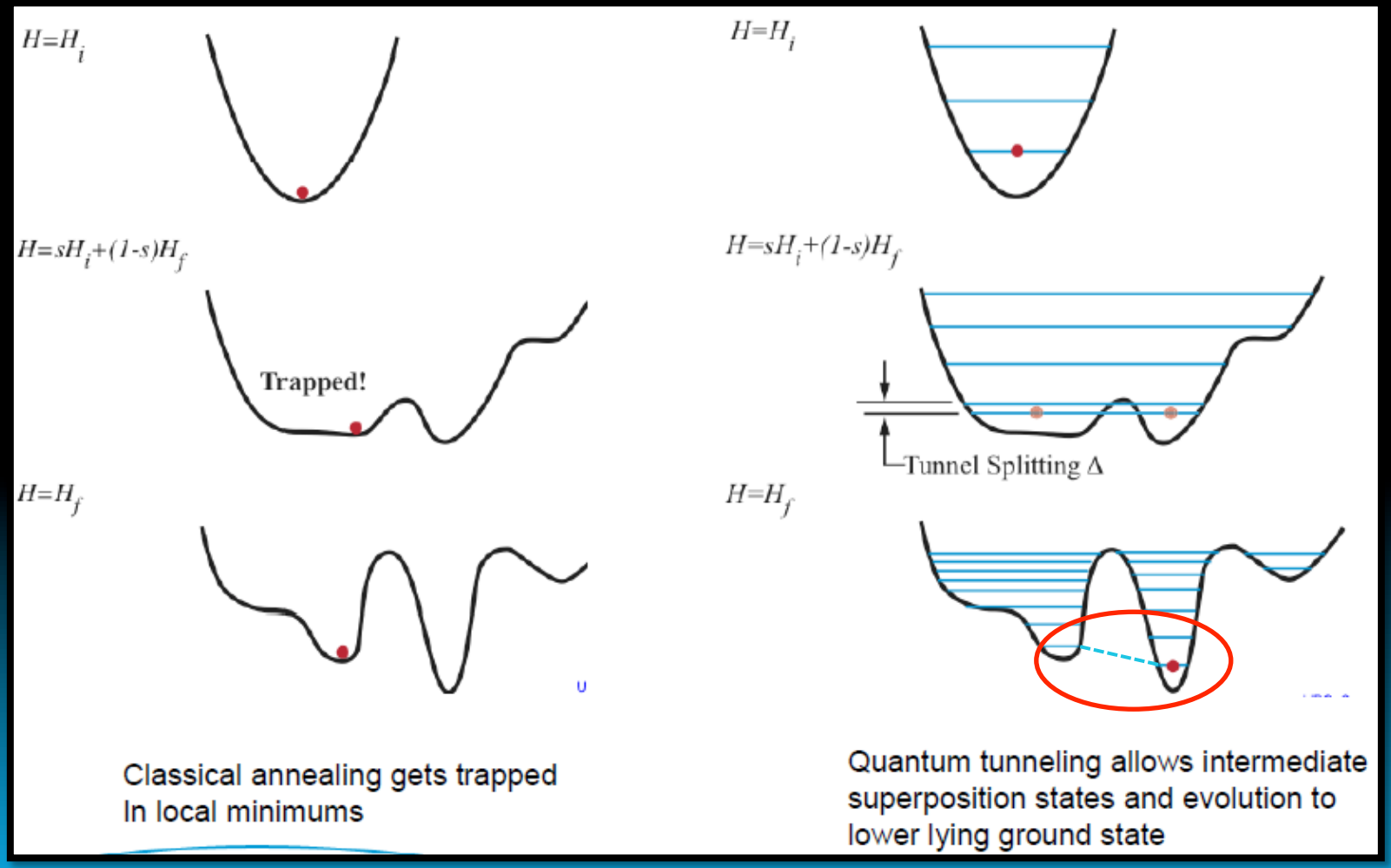


TODAY: 3-qubit entanglement has been demonstrated in superconducting qubits[3].

1. C. Ospelkaus, U. Warring, Y. Colombe, K.R. Brown, J.M. Amini, D. Leibfried and D.J. Wineland. "Microwave quantum logic gates for trapped ions.," *Nature*. August 11th (2011).
2. J. C. F. Matthews, A. Politi, A. Stefanov, & J. L. O'Brien, "Manipulation of Multiphoton Entanglement in Waveguide Quantum Circuits," Nature Photonics, 3, 346–350 (2009).
3. M. Neeley, Radoslaw, C. Bialczak, M. Lenander, E. Lucero, M. Mariantoni, A. D. O'Connell, D. Sank, H. Wang, M. Weides, J. Wenner, Y. Yin, T. Yamamoto, A. N. Cleland, J.M. Martinis, "Generation of Three-Qubit Entangled States using Superconducting Phase Qubits," Nature 467, 570-573 (2010).

Thermal vs Quantum Annealing

- Quantum system can explore solution landscape defined by objective function in superposition and tunnel to global minimum



Courtesy DWave Systems, Inc.

How Quantum Annealing via AQC Works

- Step 1: Re-cast the problem as combinatorial optimization
  - Map any NP-complete or NP-hard problem into an equivalent combinatorial optimization problem such that the optimal solution corresponds to the minimum of an energy function given by:

$$E(\vec{s}) = -\sum_{i=1}^{N} h_i s_i - \sum_{i<j} J_{ij} s_i s_j \text{ where } s_i = \pm 1 \text{ and } h_i, J_{ij} \in \mathbf{R}$$

- Step 2: Load optimization problem onto quantum processor
  - Hardware designed to find ground state of Ising Hamiltonian natively

$$H_P = -\sum_{i=1}^{N} h_i \hat{\sigma}_i^z - \sum_{i<j} J_{ij} \hat{\sigma}_i^z \hat{\sigma}_j^z$$

- Step 3: Initialize hardware to ground state of Hamiltonian H_I

$$H_I = -\sum_{i=1}^{N} \hat{\sigma}_i^x$$

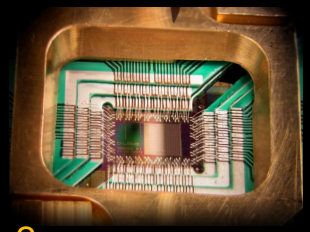
- Step 4: Slowly (adiabatically) interpolate from H_I to H_P

Instantaneous Hamiltonian ⟹ $H(t) = \frac{t}{T} H_P + \left(1 - \frac{t}{T}\right) H_I$

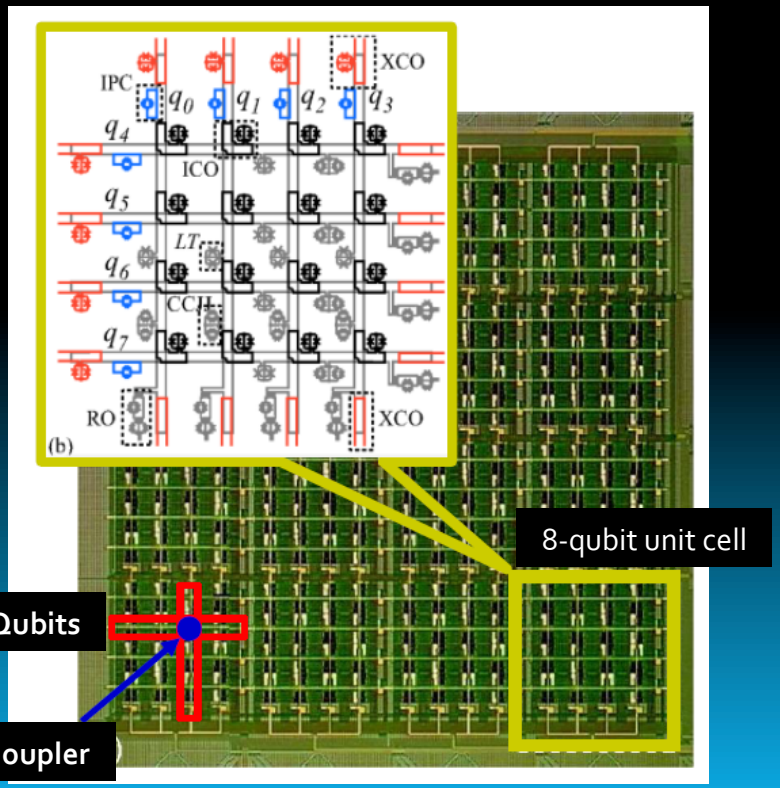
  - **Why it Works: Adiabatic Theorem of Quantum Mechanics** guarantees system stays in the ground state of the instantaneous Hamiltonians passed through and therefore ends in the ground state of H_P

Quantum Annealing Processor

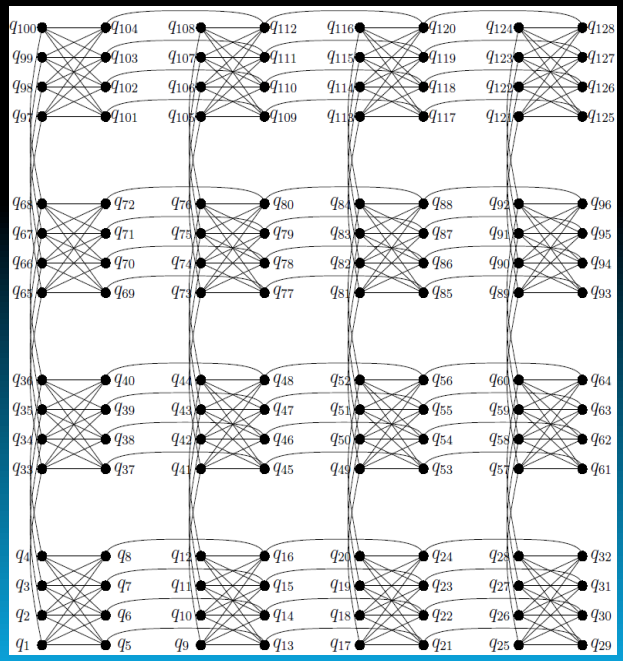
- Quantum annealing is an alternative quantum computing model that is progressing faster
- A working quantum annealing processor (DWave-1) based on 128 superconducting flux qubits exists today
  - 500-qubit version due by Q2 2012



The DWave-1 processor implements a fixed non-planar connection topology on 128 qubits. Different problems are encoded by changing the coupling strengths J_{ij} between qubits and the biases h_i of each qubit. **Harnesses quantum phenomena not available to conventional computers**, i.e., superposition, entanglement, tunneling, to find energy minima much faster than is possible using any conventional computer.

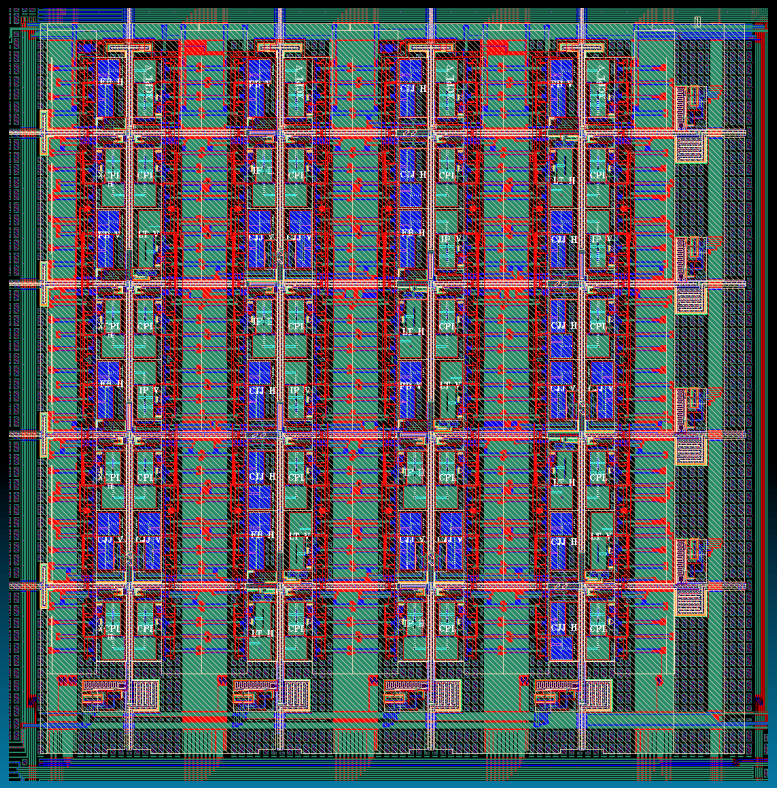


≡



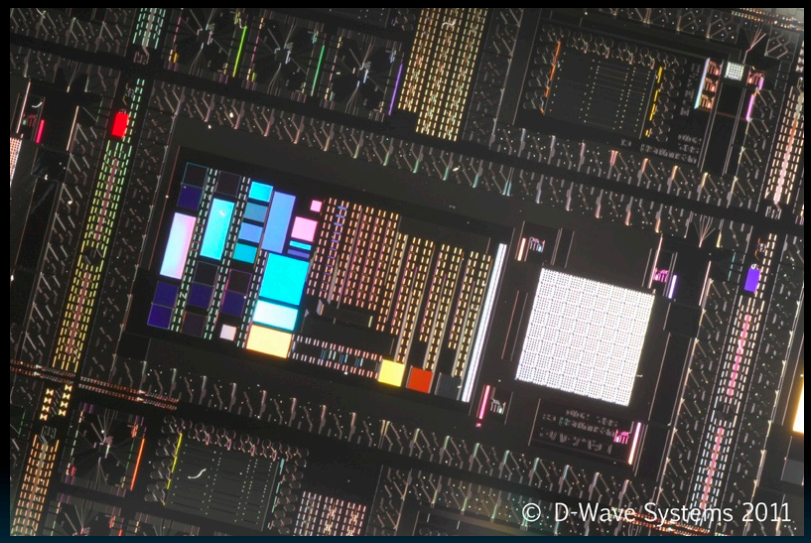
State-of-the-Art Adiabatic Quantum Computer Chips

Current Design



Rainier

Next Generation Design



Vesuvius (500 qubits)

- Higher density / more qubits per unit area
- More robust against process defects = higher yields
- Larger tunnel splitting = more robust quantum dynamics
- Less parametric variability
- Read no longer heats up the chip

Images courtesy of DWave Systems, Inc.

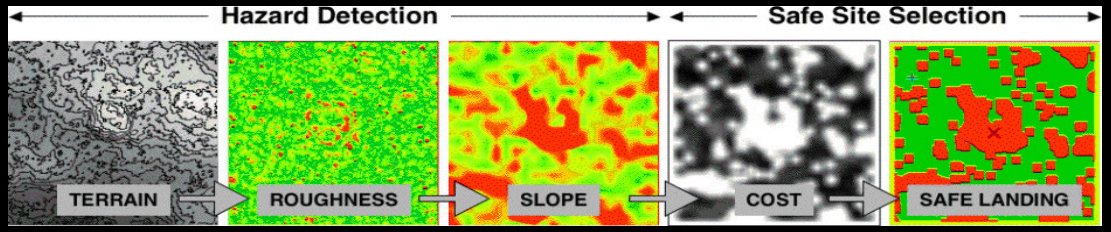
Comparison of Approaches

Characteristic	Conventional (Circuits)	Unconventional (Annealing)	Impact of Difference
Design philosophy	Bottom-up	Top-down	Had a functional processor from day 1
Design cycle	1-2 per year	8-10 per year	Rapid design-build-test cycle accelerates progress and focuses R&D efforts
Computational model	Quantum circuit model	Quantum annealing of programmable Ising model	Processor is specialized for solving hard optimization problems
Physical model	Local unitary operations	Global operations with always-on coupling between qubits	Quantum many body effects provides intrinsic robustness to low-frequency noise at cryogenic temperatures
Attitude towards noise	Noise is bad and must be eliminated	Noise is tolerated and a little can be beneficial	Presumption that all noise is bad is flawed
Do we see a Moore's law for qubits?	Rate of progress in terms of number of qubits is very slow & at best linear in time	Number of qubits doubling every 18 months: 512 qubits by 2012 (D-Wave)	**Perhaps fastest route to a quantum processor of significant capability**

Applications

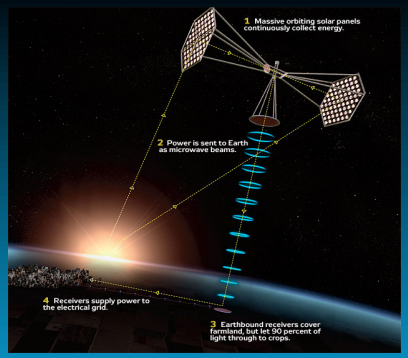
N.B. the quantum processor solves the quantum Ising model and all computational problems mappable to it *natively*, i.e., as a physical evolution. The quantum annealing time is extraordinarily fast in comparison to the speed conventional processors can solve these problems using our best classical algorithms

Relevance to Human Exploration Systems

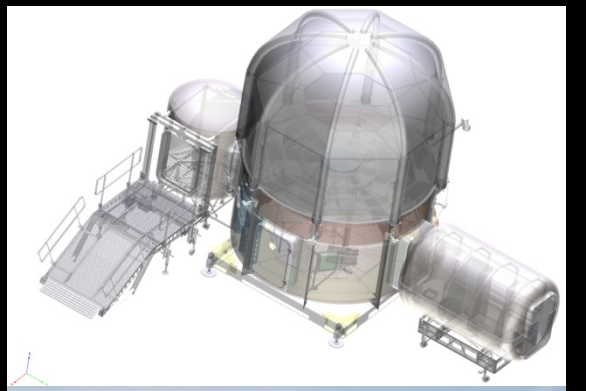


Machine learning of classifiers / image registration used in ALHAT (Autonomous landing & hazard avoidance technologies)

Logistics – optimal cargo loading to minimize storage volume while maximizing access



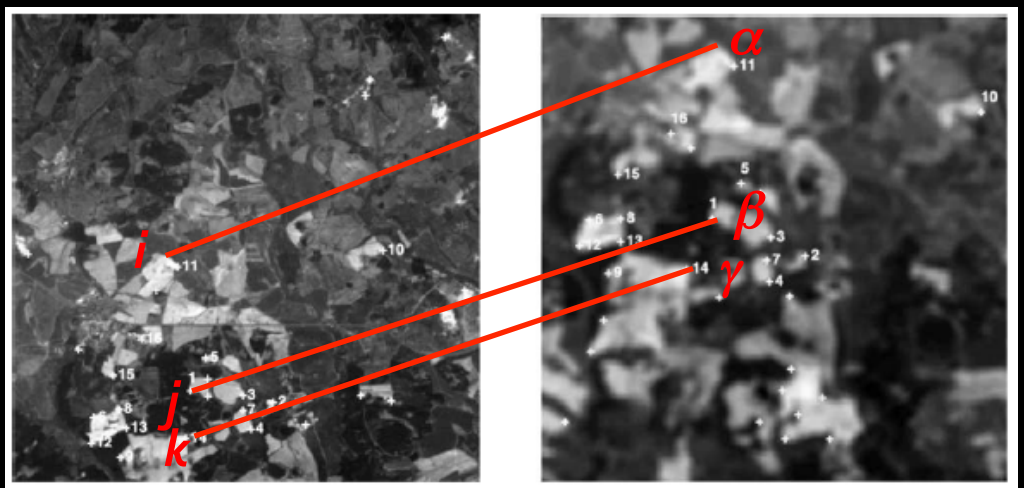
Planning & scheduling assembly of large structures in space or work activities in human-robotic exploration



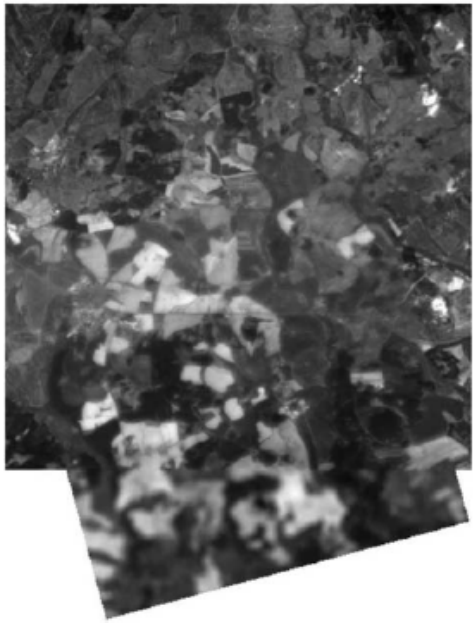
V&V and **optimal sensor placement** for human habitats, and surface / flight exploration vehicles

Example: Image Registration

- Goal: Co-register and mosaic two or more images of the same scene taken at different times, from different viewpoints, and/or in different wavebands
- Solve via quantum annealing

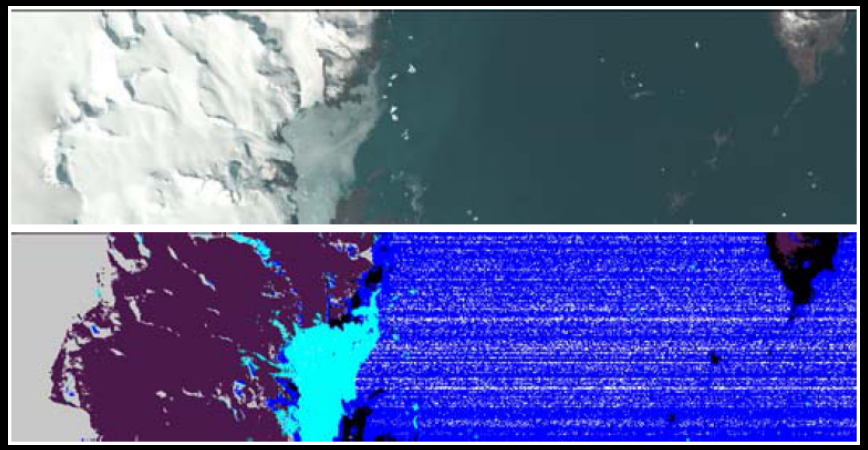


$$x^{opt} = \arg\min_{x} \left(- \underbrace{\sum_{i,\alpha=1}^{N} x_{i,\alpha} d_{feat}(i,\alpha)}_{\text{Feature Similarity}} - \underbrace{\sum_{i,\alpha;j,\beta=1}^{N} x_{i,\alpha} x_{j,\beta} d_{geom}(i,\alpha;j,\beta)}_{\text{Geometric Consistency}} \right)$$



Example: Machine Learning

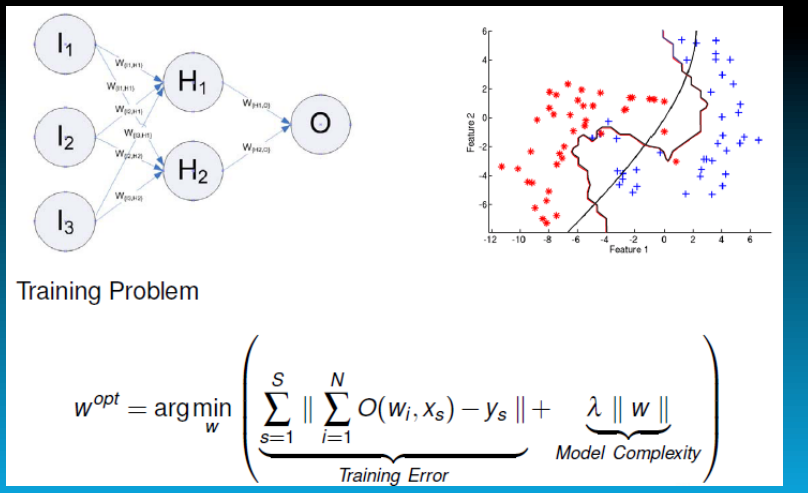
- Learning a classifier to automatically label satellite images as water v land v ice v snow v cloud v unknown



Top is false color image
Bottom is classifier output:

- **blue** = water
- **black** = land
- **cyan** = ice
- **purple** = snow
- **gray** = cloud
- **white** = unknown

- Solve via quantum annealing …
  - A classifier is constructed as a linear superposition of a set of weak classifiers
  - The weights in the superposition are optimized in a learning process that strives to minimize the training error as well as the number of weak classifiers used
  - No efficient solution to this problem is known



Example: Optimal Sensor Placement

- Goal: find the minimum number of sensors & their locations which provide the same level of discriminability as the case in which all observables are measured
- Solved by mapping to 0-1 integer programming, which can be solved by quantum annealing
  - Let $S(x_i)$ = a sensor for reading variable x_i
  - Let $M = H^T$ = transpose of the hypothetical signature matrix
  - Let $\widetilde{M} = \begin{pmatrix} M \\ \{R_{ij}\} \end{pmatrix}$ where $R_{ij} = |R_i - R_j|$ where $R_i = i$-th row of H

Device Schematic

Component M_1 r_1: $x = a \times b$,
Component M_2 r_2: $y = b \times c$,
Component M_3 r_3: $z = c \times d$,
Component M_4 r_4: $t = d \times e$,
Component A_1 r_5: $f = x + y$,
Component A_2 r_6: $g = y + z$,
Component A_3 r_7: $h = z + t$.

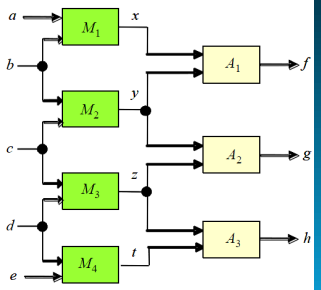


Figure. 1. An adder-multiplier circuit

Analytic Redundancy Relations

$$f - ab - bc = 0, \quad g - bc - de = 0, \quad h - cd - de = 0, \quad (2)$$
$$f - g - ab + cd = 0, \quad g - h - bc + de = 0.$$

If we consider only single component failures and represent each fault with its corresponding component, then the signature matrix is as follows:

ARR	M_1	M_2	M_3	M_4	A_1	A_2	A_3
$f-ab-bc=0$	1	1	0	0	1	0	0
$g-bc-de=0$	0	1	1	0	0	1	0
$h-cd-de=0$	0	0	1	1	0	0	1
$f-g-ab+cd=0$	1	0	1	0	1	1	0
$g-h-bc+de=0$	0	1	0	1	0	1	1

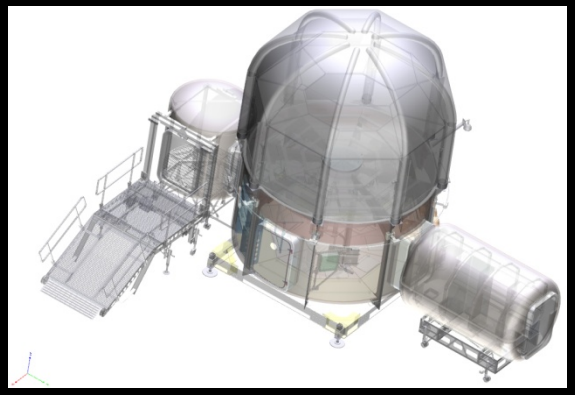
Signature Matrix H

Table 1. The Hypothetical Signature Matrix (HSM) of the system of Figure 1

No.	ARR	M_1	M_2	M_3	M_4	A_1	A_2	A_3
1	$x-ab=0$	1	0	0	0	0	0	0
2	$y-bc=0$	0	1	0	0	0	0	0
3	$z-cd=0$	0	0	1	0	0	0	0
4	$t-de=0$	0	0	0	1	0	0	0
5	$f-x-y=0$	0	0	0	0	1	0	0
6	$g-y-z=0$	0	0	0	0	0	1	0
7	$h-z-t=0$	0	0	0	0	0	0	1
8	$f-g-x+z=0$	0	0	0	0	1	1	0
9	$g-h-y+t=0$	0	0	0	0	0	1	1
10	$f-ab-bc=0$	1	1	0	0	1	0	0
11	$g-bc-cd=0$	0	1	1	0	0	1	0
12	$h-cd-de=0$	0	0	1	1	0	0	1
13	$f-g-ab+cd=0$	1	0	1	0	1	1	0
14	$g-h-bc+de=0$	0	1	0	1	0	1	1
15	$f-ab-y=0$	1	0	0	0	1	0	0
16	$g-bc-z=0$	0	1	0	0	0	1	0
17	$h-cd-t=0$	0	0	1	0	0	0	1
18	$f-x-bc=0$	0	1	0	0	1	0	0
19	$g-y-cd=0$	0	0	1	0	0	1	0
20	$h-z-de=0$	0	0	0	1	0	0	1
21	$f-g-ab+z=0$	1	0	0	0	1	1	0
22	$g-h-bc+t=0$	0	1	0	0	0	1	1
23	$f-g-x+cd=0$	0	0	1	0	1	1	0
24	$g-h-y+de=0$	0	0	0	1	0	1	1

$$\text{minimize} \quad \left| \bigcup_{i=1}^{m} S(x_i) \right|,$$
$$\text{subject to} \quad \widetilde{M}\boldsymbol{x} \geq \mathbf{1}, \quad x_j = 0 \text{ or } 1$$

Verification & Validation



Lunar habitats

Flight software & hardware

V&V

Surface exploration vehicles

Space exploration vehicles

Massive air traffic flow optimization with separation assurance

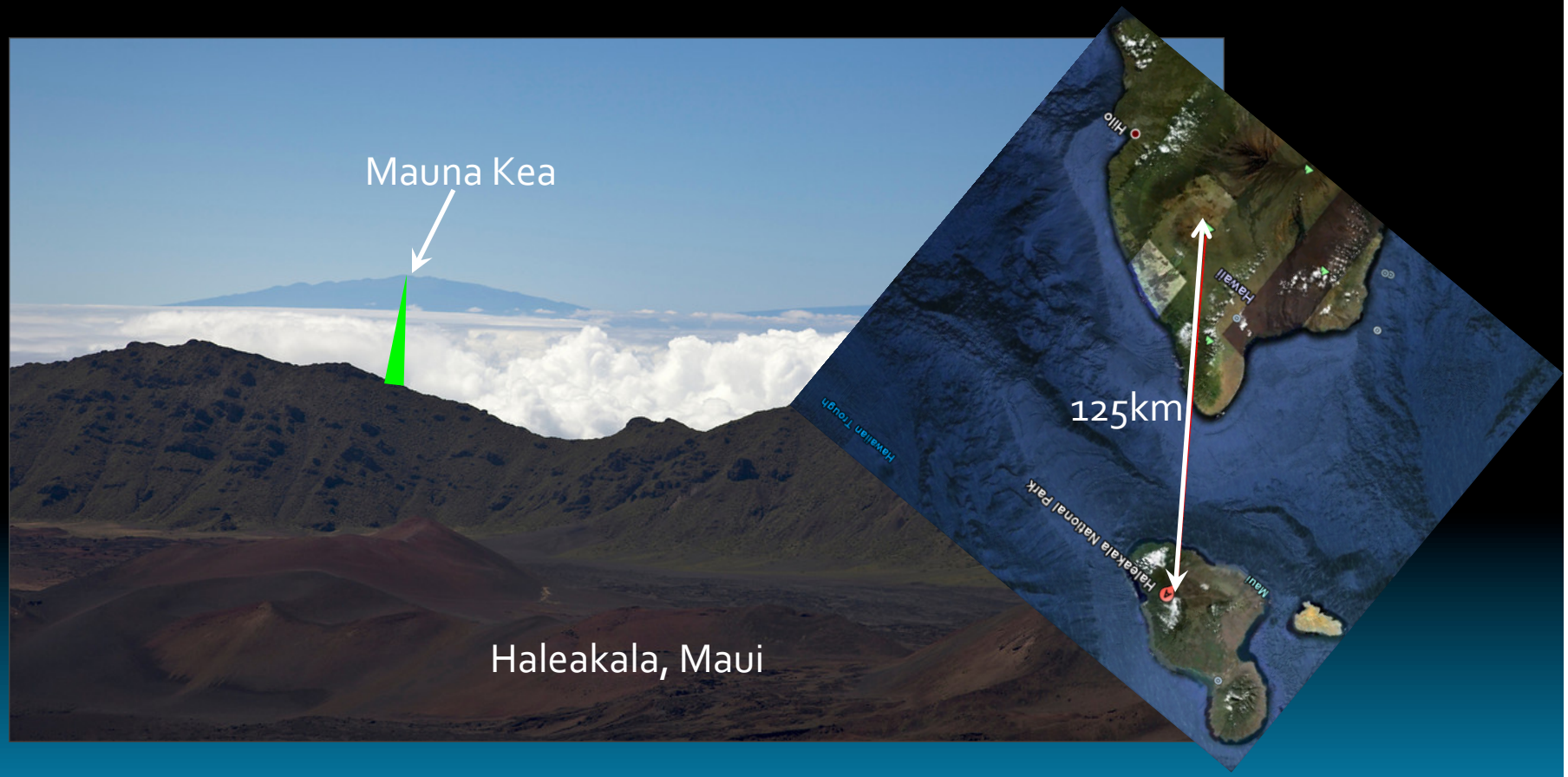
Risks & Payoffs

- **Risks**
  - Not all NASA-problems may be mappable to the current architecture
  - Use of chains of multiple qubits to connect non-adjacent qubits in the chimera graph might not scale indefinitely
  - Decoherence properties of the chip under scaling are not yet fully understood
- **Payoffs**
  - Provides a rich and functional platform for experimentation with quantum computer algorithms, programming languages, and architectures
  - Solves certain mission-critical problems faster
  - Solves certain mission-critical problems better (global, or lower local, minima)
  - Deploys practical quantum computing decades earlier than most expect
  - Opportunity to leapfrog ahead in quantum computing & show leadership
  - Catalyzes collaborations with industry and academia on NASA problems

Conclusions

- NASA/DWave have long track record in developing adiabatic quantum computing
- Practical applications feasible
- Time is right to focus on applications
- New chip designs being tested constantly resulting is faster speed, lower noise
- Contact me for more info:
  - Email: Colin.P.Williams@jpl.nasa.gov
  - Tel: 650-242-2051

Thank you!


Mauna Kea
Haleakala, Maui
125km
Hilo
Hawaii
Haleakala National Park
Maui

Backup

Key Milestones in CV-QKD

- (1999) Idea of encoding information onto non-commuting quadratures of coherent light [1]
  - Tim Ralph – now advisor to Quintessence Labs
- (2000) Extended CV-QKD to use squeezed states [2]
- (2000) Variant of squeezed state protocol that used binary modulated squeezed light [3]
- (2000) CV-QKD with continuous EPR correlations [4]
- (2001) Proof CV-QKD with squeezed states is unconditionally secure [5]
- (2001) Improved squeeze state protocol that relied on sending and detecting Gaussian information [6]
- (2002) New CV-QKD protocol based on coherent states [7]
  - This protocol suffers from the 3 dB loss limit, i.e., protocol becomes insecure for a transmission loss greater than 50%
- (2002) Post-selection introduced to overcome the 3 dB loss limit [8]
  - In post-selection, Alice and Bob only select data points where they have an information advantage over Eve

Milestones in CV-QKD (cont'd)

- (2003) Reverse reconciliation introduced to overcome 3 dB loss limit [9]
  - In a reverse reconciliation protocol, Alice corrects her keys to have the same values as Bob's
- (2004) No switching protocol was introduced to eliminate the need to change basis during encoding [10]
  - Simplifies implementation and enables higher secret key rates
- (2009-2011) CV-QKD proved secure [11, 12, 13]

[1] T. C. Ralph, "Continuous variable quantum cryptography," Phys. Rev. A, 61(1):010303, (1999).
[2] T. C. Ralph, "Security of continuous-variable quantum cryptography," Phys. Rev. A, 62, 062306 (2000).
[3] M. Hillery, "Quantum cryptography with squeezed states," Phys. Rev. A, 61(2):022309, Jan (2000).
[4] M.D. Reid, "Quantum cryptography with a predetermined key, using continuous variable Einstein-Podolsky-Rosen correlations," Phys. Rev. A, 62:022309, (2000).
[5] D. Gottesman and J. Preskill, "Secure quantum key distribution using squeezed states," Phys. Rev. A, 63:022309, (2001).
[6] N.J. Cerf, M. Levy, & G. Van Assche, "Quantum distribution of Gaussian keys using squeezed states," Phys. Rev. A, 63:052311,(2001).
[7] F. Grosshans & P. Grangier, "Continuous variable quantum cryptography using coherent states," Phys. Rev. Lett., 88:057902, (2002).
[8] Ch. Silberhorn, T. C. Ralph, N. Lutkenhaus, and G. Leuchs, "Continuous variable quantum cryptography: Beating the 3 dB loss limit," Phys. Rev. Lett., 89(16):167901, Sep (2002).
[9] F. Grosshans, N. J. Cerf, J. Wenger, R. Tualle-Brouri, and P. Grangier, "Virtual entanglement and reconciliation protocols for quantum cryptography with continuous variables," Quantum Information and Computation, 3:535–552, (2003).
[10] C. Weedbrook, A. M. Lance, W. P. Bowen, T. Symul, T. C. Ralph, & P. K. Lam, "Quantum Cryptography without Switching," Phys. Rev. Lett. 93, 170504 (2004).
[11] R. Renner and J. I. Cirac, "de Finetti Representation Theorem for Infinite-Dimensional Quantum Systems and Applications to Quantum Cryptography," Phys. Rev. Lett. 102 110504 (2009).
[12] A. Leverrier and P. Grangier, "Unconditional Security Proof of Long-Distance Continuous-Variable Quantum Key Distribution with Discrete Modulation," Phys. Rev. Lett. 102, 180504 (2009).
[13] A. Leverrier and P. Grangier, "Erratum: Unconditional Security Proof of Long-Distance Continuous-Variable Quantum Key Distribution with Discrete Modulation [Phys. Rev. Lett. 102, 180504 (2009)]," Phys. Rev. Lett. 106, 259902(E) (2011).

CV-QKD in Free-Space Communications

- CV-QKD has several attractive features for optical communications in free space
  - Robust to background light
    - Homodyne detectors rely on a local oscillator laser co-propagating with signal laser. Only photons with same frequency and same spatial mode as the local oscillator are detected
  - Robust to timing jitter
    - Local oscillator provide automatic timing reference
  - Robust to spatial jitter
    - As local oscillator and signal laser co-propagate in same spatial mode they both jitter spatially identically
  - No need for a "guide" laser
    - Adaptive optics can correct wavefront distortions due to propagation through atmosphere without need for a separate guide laser

  Easily miniaturized opto-electronics

Free-Space 2-Way Optical Communications Records

- Space-to-Space[1]:
  - Record set by the infrared diode neodymium laser on board the MESSENGER spacecraft in May 2005
  - 2-way communication was established across **24 million km**

- Ground-to-Ground[2]:
  - **276km** (but bandwidth about 4kHz)
- Ground-to-Ground (DV-QKD demo)[3,4]
  - **144 km** between La Palma and Tenerife

1. Source: http://en.wikipedia.org/wiki/Free-space_optical_communication
2. Source: http://www.modulatedlight.org/optical_comms/optical_qso_173mile.html
3. Source: http://www.quantum.at/research/quantum-teleportation-communication-entanglement/entangled-photons-over-144-km.html
4. Source: http://www.quantum.at/research/quantum-teleportation-communication-entanglement/entangled-photons-over-144-km.html

CV-QKD is Preferred Option for Free-Space Communications

- CV-QKD has many advantages over DV-QKD for optical communications in free space
  - Robust to background light
    - Homodyne detectors rely on a local oscillator laser co-propagating with signal laser. Only photons with same frequency and same spatial mode as the local oscillator are detected
  - Robust to timing jitter
    - Local oscillator provide automatic timing reference
  - Robust to spatial jitter
    - As local oscillator and signal laser co-propagate in same spatial mode they both jitter spatially identically
  - No need for a "guide" laser
    - Adaptive optics can correct wavefront distortions due to propagation through atmosphere without need for a separate guide laser

  Easily miniaturized opto-electronics

US OIG Audit – the Issue

- NASA relies on a series of computer networks to carry out its various missions, including controlling spacecraft like the International Space Station and conducting science missions like the Hubble Telescope. Therefore, it is imperative that NASA protect its computer networks from cyber attacks that could disrupt operations or result in the loss of sensitive data. In this audit, we evaluated whether NASA protected information technology (IT) assets on its Agency-wide mission computer network from Internet-based cyber attacks. Specifically, we assessed whether NASA adequately protected these IT assets from Internet-based attacks by regularly assessing risks and identifying and mitigating vulnerabilities. We also reviewed internal controls as appropriate.

US OIG Audit – the Results

- We found that computer servers on NASA's Agency-wide mission network had high-risk vulnerabilities that were exploitable from the Internet. Specifically, six computer servers associated with IT assets that control spacecraft and contain critical data had vulnerabilities that would allow a remote attacker to take control of or render them unavailable. Moreover, once inside the Agency-wide mission network, the attacker could use the compromised computers to exploit other weaknesses we identified, a situation that could severely degrade or cripple NASA's operations. We also found network servers that revealed encryption keys, encrypted passwords, and user account information to potential attackers. These data are sensitive and provide attackers additional ways to gain unauthorized access to NASA networks. These deficiencies occurred because NASA had not fully assessed and mitigated risks to its Agency-wide mission network and was slow to assign responsibility for IT security oversight to ensure the network was adequately protected.