PROCEEDINGS OF SPIE

Signal Processing, Sensor/Information Fusion, and Target Recognition XXVI

Ivan Kadar
Editor

10–12 April 2017
Anaheim, California, United States

Sponsored and Published by
SPIE

Volume 10200

Proceedings of SPIE 0277-786X, V. 10200

SPIE is an international society advancing an interdisciplinary approach to the science and application of light.

Signal Processing, Sensor/Information Fusion, and Target Recognition XXVI, edited by Ivan Kadar, Proc. of SPIE Vol. 10200, 1020001 · © 2017 SPIE · CCC code: 0277-786X/17/$18 · doi: 10.1117/12.2270668

The papers in this volume were part of the technical conference cited on the cover and title page. Papers were selected and subject to review by the editors and conference program committee. Some conference presentations may not be available for publication. Additional papers and presentation recordings may be available online in the SPIE Digital Library at SPIEDigitalLibrary.org.

The papers reflect the work and thoughts of the authors and are published herein as submitted. The publisher is not responsible for the validity of the information or for any outcomes resulting from reliance thereon.

Please use the following format to cite material from these proceedings:
Author(s), "Title of Paper," in *Signal Processing, Sensor/Information Fusion, and Target Recognition XXVI*, edited by Ivan Kadar, Proceedings of SPIE Vol. 10200 (SPIE, Bellingham, WA, 2017) Seven-digit Article CID Number.

ISSN: 0277-786X
ISSN: 1996-756X (electronic)

ISBN: 9781510609013
ISBN: 9781510609020 (electronic)

Published by
SPIE
P.O. Box 10, Bellingham, Washington 98227-0010 USA
Telephone +1 360 676 3290 (Pacific Time) · Fax +1 360 647 1445
SPIE.org

Printed in the United States of America.

Publication of record for individual papers is online in the SPIE Digital Library.

SPIEDigitalLibrary.org

Paper Numbering: *Proceedings of SPIE* follow an e-First publication model. A unique citation identifier (CID) number is assigned to each article at the time of publication. Utilization of CIDs allows articles to be fully citable as soon as they are published online, and connects the same identifier to all online and print versions of the publication. SPIE uses a seven-digit CID article numbering system structured as follows:

- The first five digits correspond to the SPIE volume number.
- The last two digits indicate publication order within the volume using a Base 36 numbering system employing both numerals and letters. These two-number sets start with 00, 01, 02, 03, 04, 05, 06, 07, 08, 09, 0A, 0B … 0Z, followed by 10-1Z, 20-2Z, etc. The CID Number appears on each page of the manuscript.

Contents

SESSION 1 MULTISENSOR FUSION, MULTITARGET TRACKING, AND RESOURCE MANAGEMENT I

SESSION 2 MULTISENSOR FUSION, MULTITARGET TRACKING, AND RESOURCE MANAGEMENT II

SESSION 3 INFORMATION FUSION METHODOLOGIES AND APPLICATIONS I

SESSION 4 INFORMATION FUSION METHODOLOGIES AND APPLICATIONS II

SESSION 5 INFORMATION FUSION METHODOLOGIES AND APPLICATIONS III

SESSION 7 SIGNAL AND IMAGE PROCESSING, AND INFORMATION FUSION APPLICATIONS I

SESSION 8 SIGNAL AND IMAGE PROCESSING, AND INFORMATION FUSION APPLICATIONS II

SESSION 9 SIGNAL AND IMAGE PROCESSING, AND INFORMATION FUSION APPLICATIONS III

POSTER SESSION

Authors

Numbers in the index correspond to the last two digits of the seven-digit citation identifier (CID) article numbering system used in Proceedings of SPIE. The first five digits reflect the volume number. Base 36 numbering is employed for the last two digits and indicates the order of articles within the volume. Numbers start with 00, 01, 02, 03, 04, 05, 06, 07, 08, 09, 0A, 0B...0Z, followed by 10-1Z, 20-2Z, etc.

Conference Committee

Symposium Chair

Donald A. Reago Jr., U.S. Army Night Vision & Electronic Sensors Directorate (United States)

Symposium Co-chair

Arthur A. Morrish Raytheon Space and Airborne Systems (United States)

Conference Chair

Ivan Kadar, Interlink Systems Sciences, Inc. (United States)

Conference Co-chairs

Bhashyam Balaji, Defence Research and Development Canada (Canada)
Erik P. Blasch, Air Force Research Laboratory (United States)
Lynne L. Grewe, California State University, East Bay (United States)
Thia Kirubarajan, McMaster University (Canada)
Ronald P. S. Mahler, Random Sets, LLC (United States)

Conference Program Committee

Mark G. Alford, Air Force Research Laboratory (United States)
William D. Blair, Georgia Tech Research Institute (United States)
Mark J. Carlotto, General Dynamics Advanced Information Systems (United States)
Alex L. Chan, U.S. Army Research Laboratory (United States)
Kuo-Chu Chang, George Mason University (United States)
Chee-Yee Chong, Independent Consultant (United States)
Marvin N. Cohen, Georgia Tech Research Institute (United States)
Frederick E. Daum, Raytheon Company (United States)
Jean Dezert, The French Aerospace Laboratory (France)
Mohammad Farooq, AA Scientific Consultants Inc. (Canada)
Laurie H. Fenstermacher, Air Force Research Laboratory (United States)
Charles W. Glover, Oak Ridge National Laboratory (United States)
I. R. Goodman, Consultant (United States)
Michael L. Hinman, Air Force Research Laboratory (United States)
Jon S. Jones, Air Force Research Laboratory (United States)
Georgiy M. Levchuk, Aptima, Inc. (United States)

Martin E. Liggins II, Consultant (United States)
James Llinas, University at Buffalo (United States)
Raj P. Malhotra, Air Force Research Laboratory (United States)
Alastair D. McAulay, Lehigh University (United States)
Raman K. Mehra, Scientific Systems Company, Inc. (United States)
Harley R. Myler, Lamar University (United States)
David Nicholson, BAE Systems (United Kingdom)
Les Novak, Scientific Systems Company, Inc. (United States)
John J. Salerno Jr., Harris Corporation (United States)
Robert W. Schutz, Consultant (United States)
Andrew G. Tescher, AGT Associates (United States)
Stelios C. A. Thomopoulos, National Center for Scientific Research Demokritos (Greece)
Wiley E. Thompson, New Mexico State University (United States)
Shanchieh Jay Yang, Rochester Institute of Technology (United States)

Session Chairs

1 Multisensor Fusion, Multitarget Tracking, and Resource Management I
Bhashyam Balaji, Defence Research and Development Canada (Canada)
Martin E. Liggins II, Consultant (United States)

2 Multisensor Fusion, Multitarget Tracking, and Resource Management II
Bhashyam Balaji, Defence Research and Development Canada (Canada)
Martin E. Liggins II, Consultant (United States)

3 Information Fusion Methodologies and Applications I
Ronald P. S. Mahler, Random Sets, LLC (United States)

4 Information Fusion Methodologies and Applications II
Michael L. Hinman, Air Force Research Laboratory (United States)
Martin E. Liggins II, Consultant (United States)

5 Information Fusion Methodologies and Applications III
Michael L. Hinman, Air Force Research Laboratory (United States)
Martin E. Liggins II, Consultant (United States)

6 Signal and Image Processing, and Information Fusion Applications I
Lynne L. Grewe, California State University, East Bay (United States)
Mark J. Carlotto, General Dynamics Mission Systems (United States)
Alex L. Chan, U.S. Army Research Laboratory (United States)

7 Signal and Image Processing, and Information Fusion Applications II
Mark J. Carlotto, General Dynamics Mission Systems (United States)
Lynne L. Grewe, California State University, East Bay (United States)
Alex L. Chan, U.S. Army Research Laboratory (United States)

8 Signal and Image Processing, and Information Fusion Applications III
Alex L. Chan, U.S. Army Research Laboratory (United States)
Lynne L. Grewe, California State University, East Bay (United States)
Mark J. Carlotto, General Dynamics Mission Systems (United States)

Introduction to the Invited Panel Discussion

"The Impact of Emerging Quantum Information Technologies (QIT) on Information Fusion, and Internet-of-Things"

Quantum physics and relativity are the basis of all known fundamental laws of the universe. Although the fundamentals of quantum physics have been well known since the 1920s, in the last few decades several novel consequences of the laws of quantum physics (particularly, in the areas of atomic, molecular and optical physics and quantum computer science and information theory) have been discovered. These developments have attracted the interest of major civilian and defense industries. In particular, the areas of sensing, quantum physics sets the bounds on the sensitivity of sensing - termed the Heisenberg limit - that is orders of magnitude below the sensitivity of current sensors. In the area of computing, it has been observed that a quantum computer allows some computations to be carried out that are unfeasible using current or future classical computing technology. In the area of communication, quantum physics enables provable secure communication and at much higher data rates than those allowed by classical Shannon limit. Many of these advances could have major near-term and long-term consequences in the areas of sensing, such as secure communication, cyber sensing, big data analytics, and machine learning, and hence sensor and information fusion.

This leads to the following questions:

- Which claims of the gains of quantum science are real and which are not?
- Which of these areas are practically achievable in the near-term, and which are long-term possibilities?
- What are the barriers to achieving the long-term possibilities?
- What are the connections between quantum technologies with algorithms and signal processing and system engineering relevant to information fusion?
- What can quantum communication play in the design of Cyber Physical Systems and Internet of Things, networking, security and encompassing information fusion?

The panel brought to the attention of the fusion community the importance of the application of QIT by highlighting issues, illustrating potential approaches, and addressing challenges. A number of invited experts discussed challenges of the QIT processing and research to address these challenges with information fusion. The panelists illustrated parts of the above mentioned areas over different applications and association with information fusion. The panel highlighted impending issues and challenges and used conceptual and real-world related examples associated with the applications of QIT.

Bhashyam Balaji
Ivan Kadar

Invited Panel Discussion

The Impact of Emerging Quantum Information Technologies (QIT) on Information Fusion, and Internet-of-Things

Organizers
Bhashyam Balaji, Defence R&D Canada
Ivan Kadar, Interlink Systems Sciences, Inc., USA.

Moderators
Erik Blasch, Air Force Research Lab, USA
Martin E. Liggins II, Consultant, USA

April 10, 2017
SPIE Conference Proceeding Vol. 10200
“Signal Processing, Sensor/Information Fusion and Target Recognition XXVI”
Anaheim, CA, 10-12 April 2017

Invited Panel Discussion

Panel Participants

Dr. Bhashyam Balaji, Defence R&D Canada
Prof. Amr Helmy, University of Toronto
Prof. Thomas Jennewein, Institute of Quantum Computing, Waterloo
Prof. Dirk Englund, MIT
Dr. Marco Lanzagorta, Naval Research Laboratory
Dr. Radhakrishnan Balu, Army Research Laboratory

Invited Panel Discussion

Topics

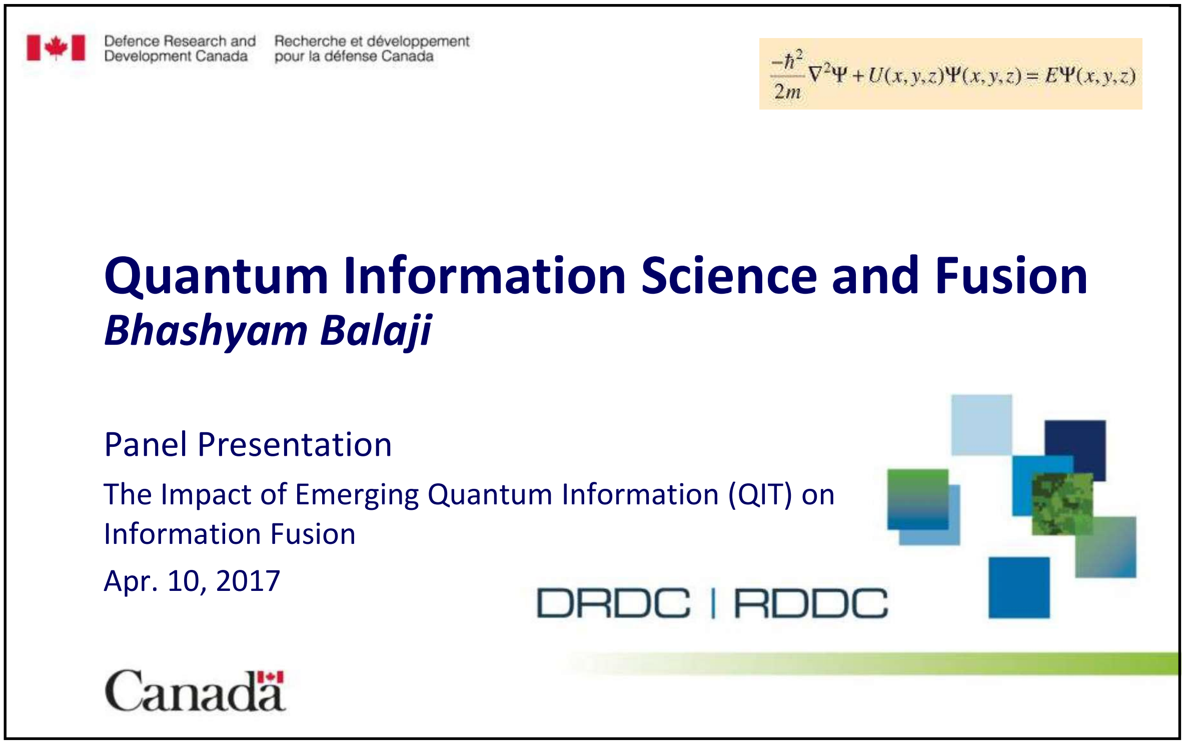
"Quantum Information Science and Fusion"
Bhashyam Balaji, Defence R&D Canada

"Radical Ideas in Quantum (Data Fusion) and (Quantum Data) Fusion"
Marco Lanzagorta, Naval Research Laboratory

"Towards Quantum Sensing with Optical Photons"
Thomas Jennewein, Institute of Quantum Computing, University of Waterloo

"Quantum Supremacy through Hybrid Photonic Technologies"
Amr Helmy, University of Toronto

"Quantum Secure Communications: Status and Outlook"
Dirk Englund, MIT



Defence Research and Development Canada
Recherche et développement pour la défense Canada

$$\frac{-\hbar^2}{2m}\nabla^2\Psi + U(x,y,z)\Psi(x,y,z) = E\Psi(x,y,z)$$

Quantum Information Science and Fusion

Bhashyam Balaji

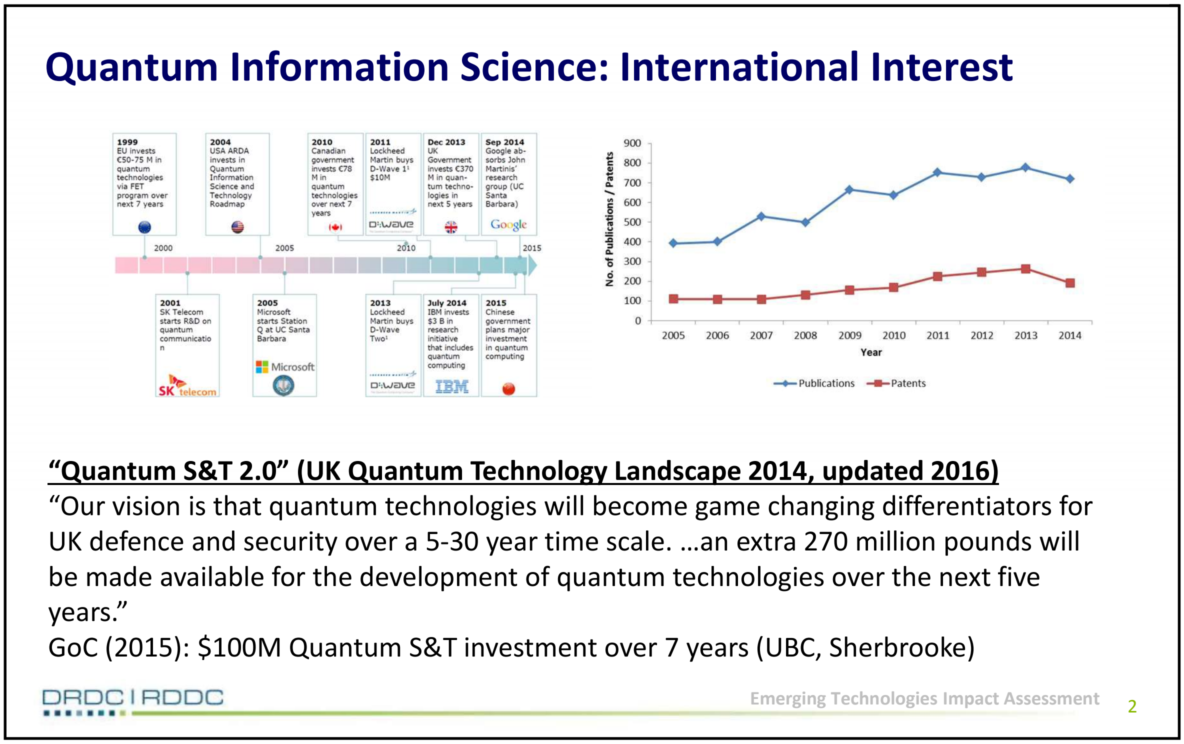
Panel Presentation

The Impact of Emerging Quantum Information (QIT) on Information Fusion

Apr. 10, 2017

DRDC | RDDC

Canada



Quantum Information Science: International Interest

1999 EU invests €50-75 M in quantum technologies via FET program over next 7 years

2001 SK Telecom starts R&D on quantum communicatio n

2004 USA ARDA invests in Quantum Information Science and Technology Roadmap

2005 Microsoft starts Station Q at UC Santa Barbara

2010 Canadian government invests €78 M in quantum technologies over next 7 years

2011 Lockheed Martin buys D-Wave 1¹ $10M

2013 Lockheed Martin buys D-Wave Two¹

Dec 2013 UK Government invests €370 M in quantum technologies in next 5 years

July 2014 IBM invests $3 B in research initiative that includes quantum computing

Sep 2014 Google absorbs John Martinis' research group (UC Santa Barbara)

2015 Chinese government plans major investment in quantum computing

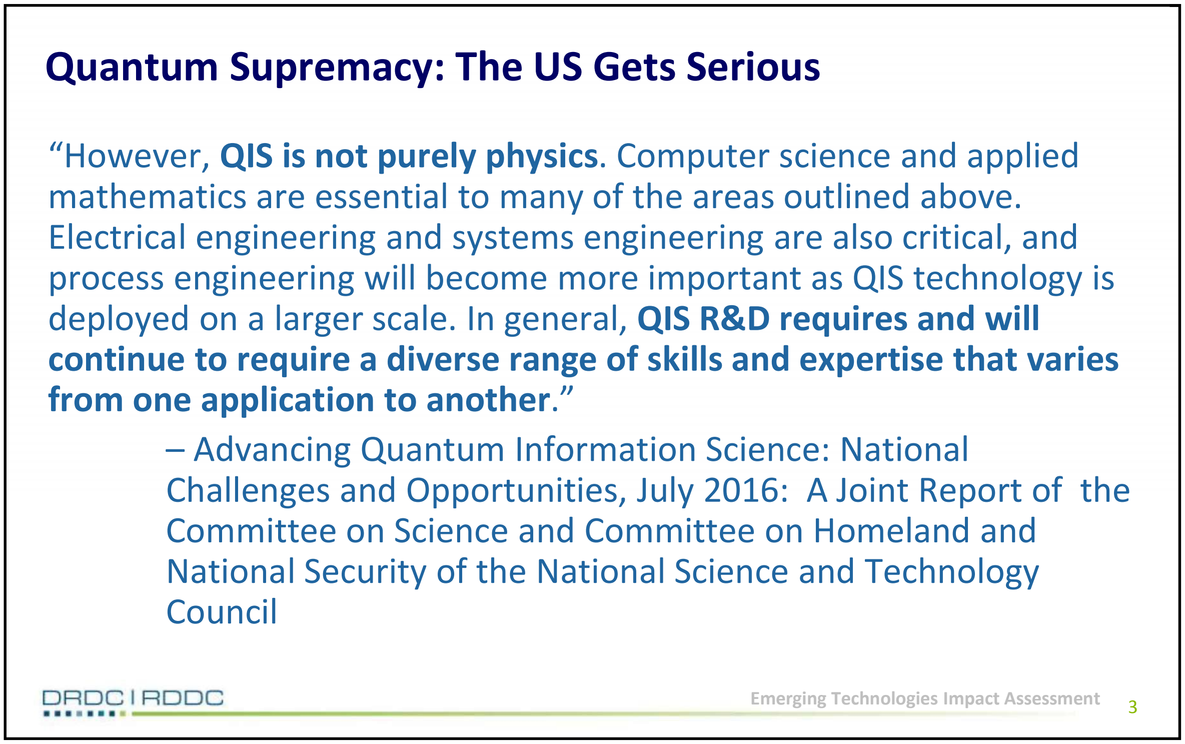
<u>"Quantum S&T 2.0" (UK Quantum Technology Landscape 2014, updated 2016)</u>

"Our vision is that quantum technologies will become game changing differentiators for UK defence and security over a 5-30 year time scale. …an extra 270 million pounds will be made available for the development of quantum technologies over the next five years."

GoC (2015): $100M Quantum S&T investment over 7 years (UBC, Sherbrooke)

DRDC | RDDC

Emerging Technologies Impact Assessment 2



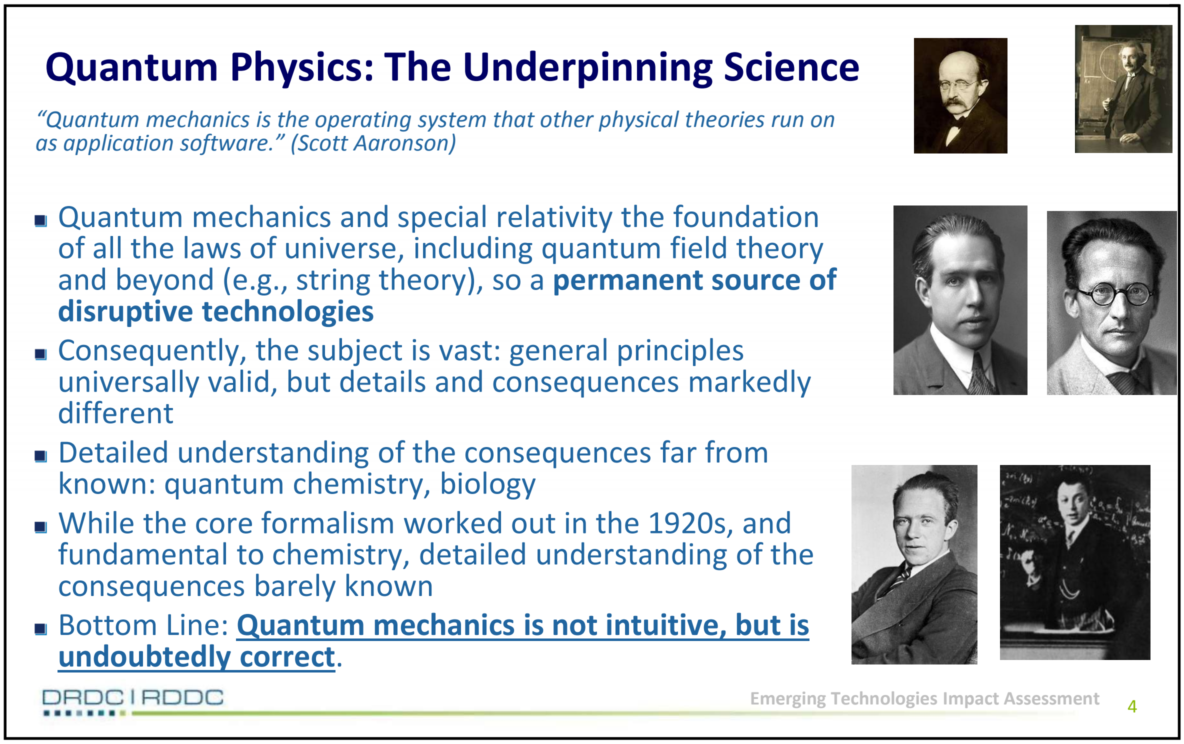
Quantum Supremacy: The US Gets Serious

"However, **QIS is not purely physics**. Computer science and applied mathematics are essential to many of the areas outlined above. Electrical engineering and systems engineering are also critical, and process engineering will become more important as QIS technology is deployed on a larger scale. In general, **QIS R&D requires and will continue to require a diverse range of skills and expertise that varies from one application to another**."

– Advancing Quantum Information Science: National Challenges and Opportunities, July 2016: A Joint Report of the Committee on Science and Committee on Homeland and National Security of the National Science and Technology Council

DRDC | RDDC

Emerging Technologies Impact Assessment 3



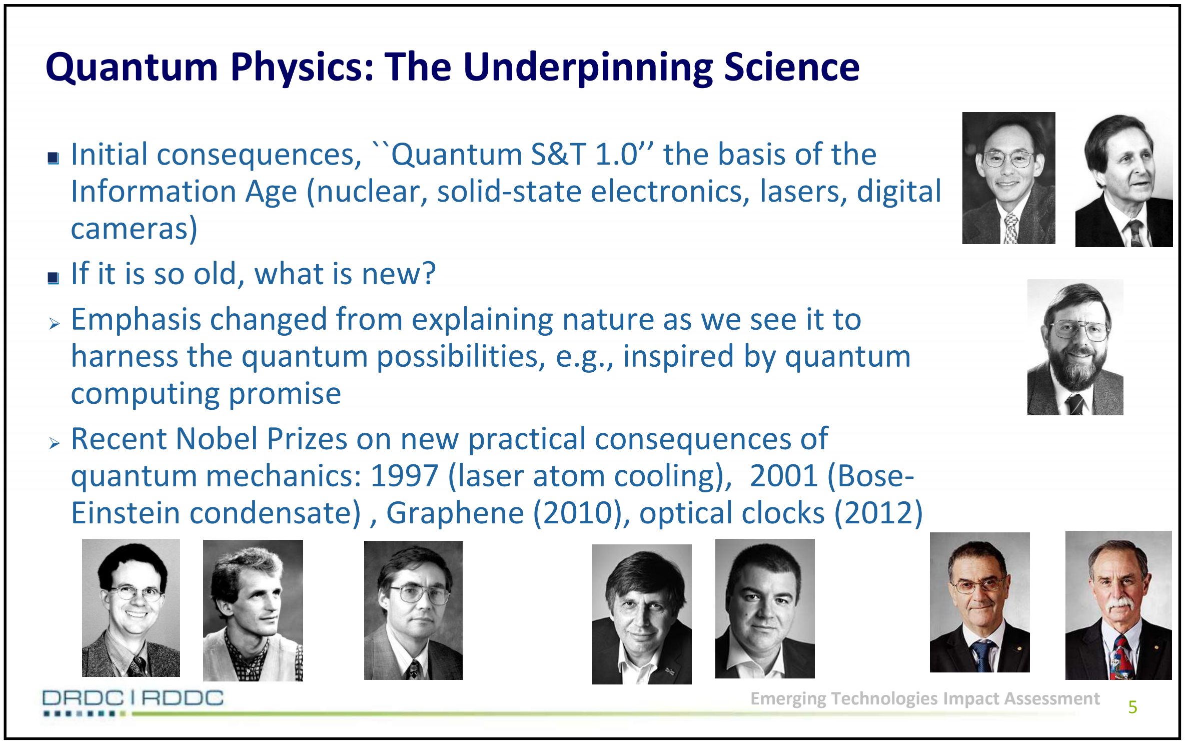
Quantum Physics: The Underpinning Science

"Quantum mechanics is the operating system that other physical theories run on as application software." (Scott Aaronson)

- Quantum mechanics and special relativity the foundation of all the laws of universe, including quantum field theory and beyond (e.g., string theory), so a **permanent source of disruptive technologies**
- Consequently, the subject is vast: general principles universally valid, but details and consequences markedly different
- Detailed understanding of the consequences far from known: quantum chemistry, biology
- While the core formalism worked out in the 1920s, and fundamental to chemistry, detailed understanding of the consequences barely known
- Bottom Line: **Quantum mechanics is not intuitive, but is undoubtedly correct**.

DRDC | RDDC

Emerging Technologies Impact Assessment 4

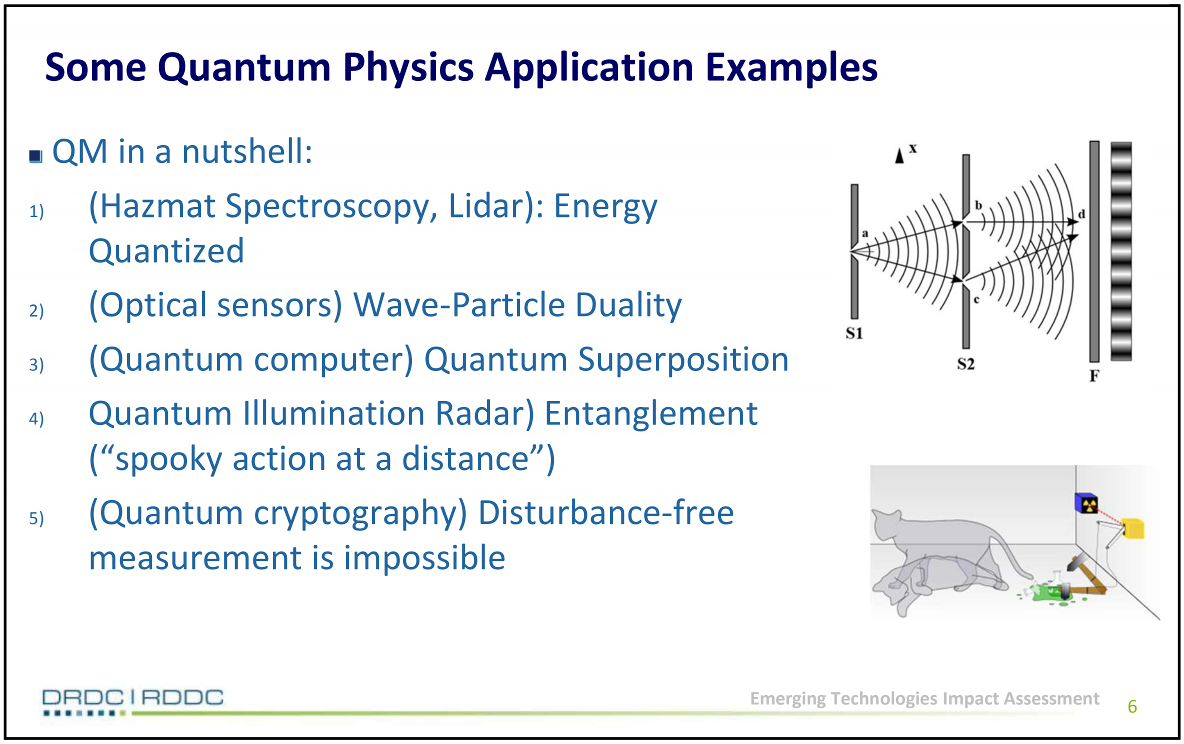


Quantum Physics: The Underpinning Science

- Initial consequences, ``Quantum S&T 1.0’’ the basis of the Information Age (nuclear, solid-state electronics, lasers, digital cameras)
- If it is so old, what is new?
  - Emphasis changed from explaining nature as we see it to harness the quantum possibilities, e.g., inspired by quantum computing promise
  - Recent Nobel Prizes on new practical consequences of quantum mechanics: 1997 (laser atom cooling), 2001 (Bose-Einstein condensate) , Graphene (2010), optical clocks (2012)

DRDC I RDDC

Emerging Technologies Impact Assessment 5



Some Quantum Physics Application Examples

- QM in a nutshell:

1) (Hazmat Spectroscopy, Lidar): Energy Quantized

2) (Optical sensors) Wave-Particle Duality

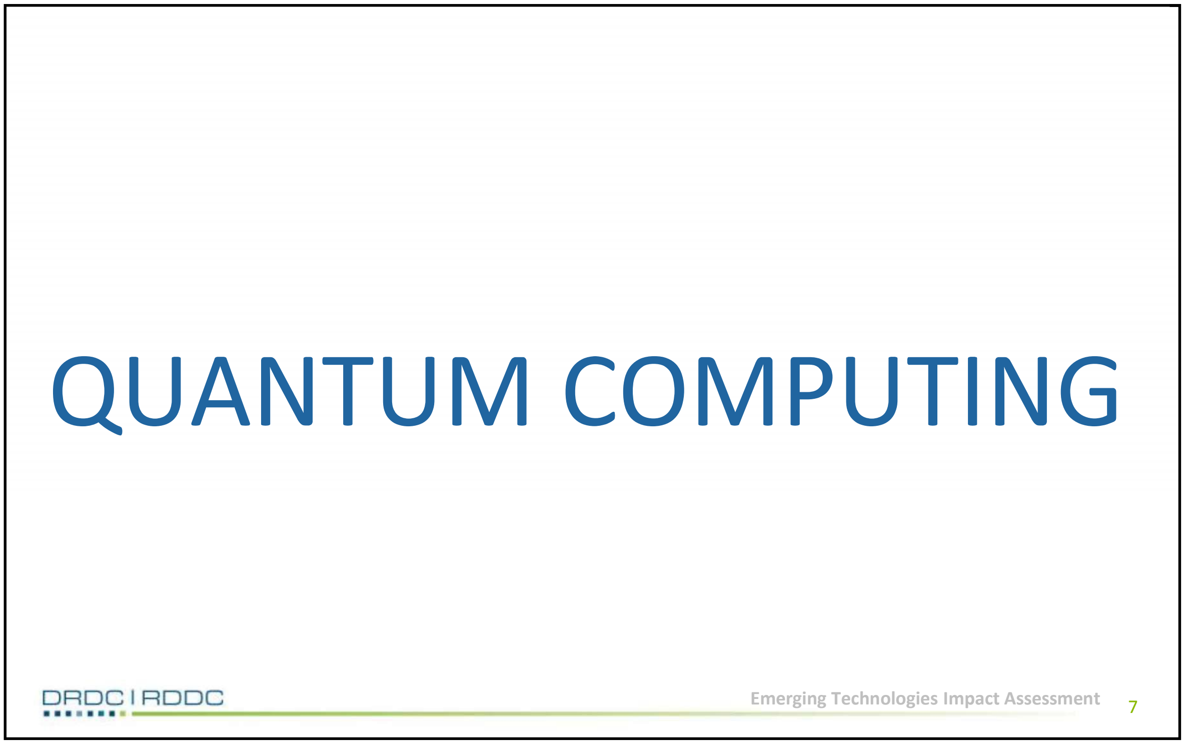
3) (Quantum computer) Quantum Superposition

4) Quantum Illumination Radar) Entanglement (“spooky action at a distance”)

5) (Quantum cryptography) Disturbance-free measurement is impossible

DRDC I RDDC

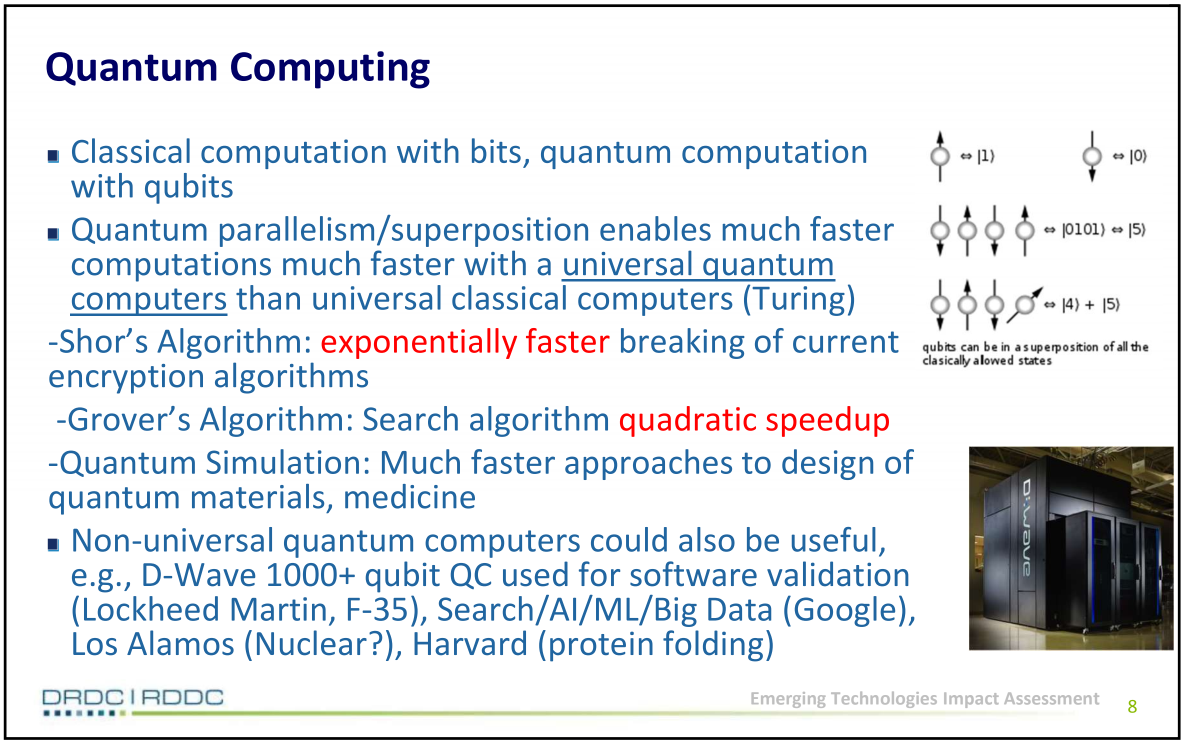
Emerging Technologies Impact Assessment 6



QUANTUM COMPUTING

DRDC | RDDC

Emerging Technologies Impact Assessment 7



Quantum Computing

- Classical computation with bits, quantum computation with qubits
- Quantum parallelism/superposition enables much faster computations much faster with a universal quantum computers than universal classical computers (Turing)

-Shor's Algorithm: exponentially faster breaking of current encryption algorithms

-Grover's Algorithm: Search algorithm quadratic speedup

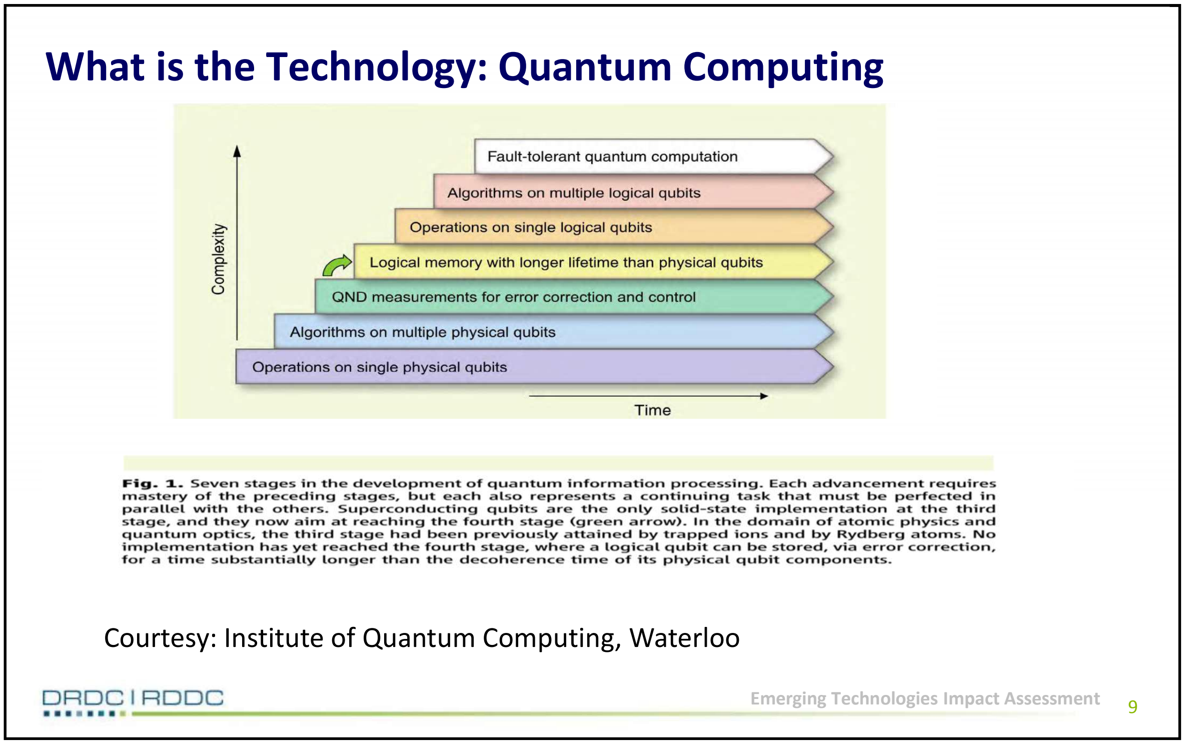
-Quantum Simulation: Much faster approaches to design of quantum materials, medicine

- Non-universal quantum computers could also be useful, e.g., D-Wave 1000+ qubit QC used for software validation (Lockheed Martin, F-35), Search/AI/ML/Big Data (Google), Los Alamos (Nuclear?), Harvard (protein folding)

qubits can be in a superposition of all the clasically allowed states

DRDC | RDDC

Emerging Technologies Impact Assessment 8

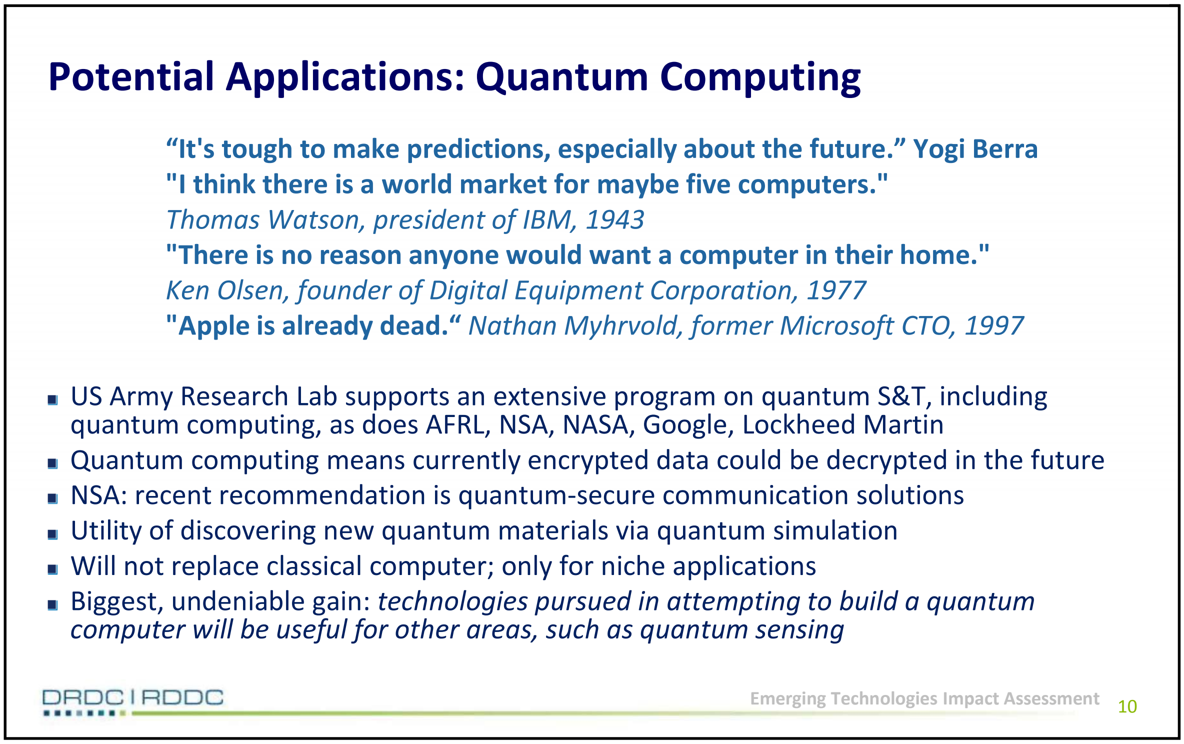


What is the Technology: Quantum Computing

Complexity
Time
Fault-tolerant quantum computation
Algorithms on multiple logical qubits
Operations on single logical qubits
Logical memory with longer lifetime than physical qubits
QND measurements for error correction and control
Algorithms on multiple physical qubits
Operations on single physical qubits

Fig. 1. Seven stages in the development of quantum information processing. Each advancement requires mastery of the preceding stages, but each also represents a continuing task that must be perfected in parallel with the others. Superconducting qubits are the only solid-state implementation at the third stage, and they now aim at reaching the fourth stage (green arrow). In the domain of atomic physics and quantum optics, the third stage had been previously attained by trapped ions and by Rydberg atoms. No implementation has yet reached the fourth stage, where a logical qubit can be stored, via error correction, for a time substantially longer than the decoherence time of its physical qubit components.

Courtesy: Institute of Quantum Computing, Waterloo



Potential Applications: Quantum Computing

“It's tough to make predictions, especially about the future.” Yogi Berra
"I think there is a world market for maybe five computers."
Thomas Watson, president of IBM, 1943
"There is no reason anyone would want a computer in their home."
Ken Olsen, founder of Digital Equipment Corporation, 1977
"Apple is already dead.“ *Nathan Myhrvold, former Microsoft CTO, 1997*

- US Army Research Lab supports an extensive program on quantum S&T, including quantum computing, as does AFRL, NSA, NASA, Google, Lockheed Martin
- Quantum computing means currently encrypted data could be decrypted in the future
- NSA: recent recommendation is quantum-secure communication solutions
- Utility of discovering new quantum materials via quantum simulation
- Will not replace classical computer; only for niche applications
- Biggest, undeniable gain: *technologies pursued in attempting to build a quantum computer will be useful for other areas, such as quantum sensing*

S&T Trends/Future Directions: Quantum Computing

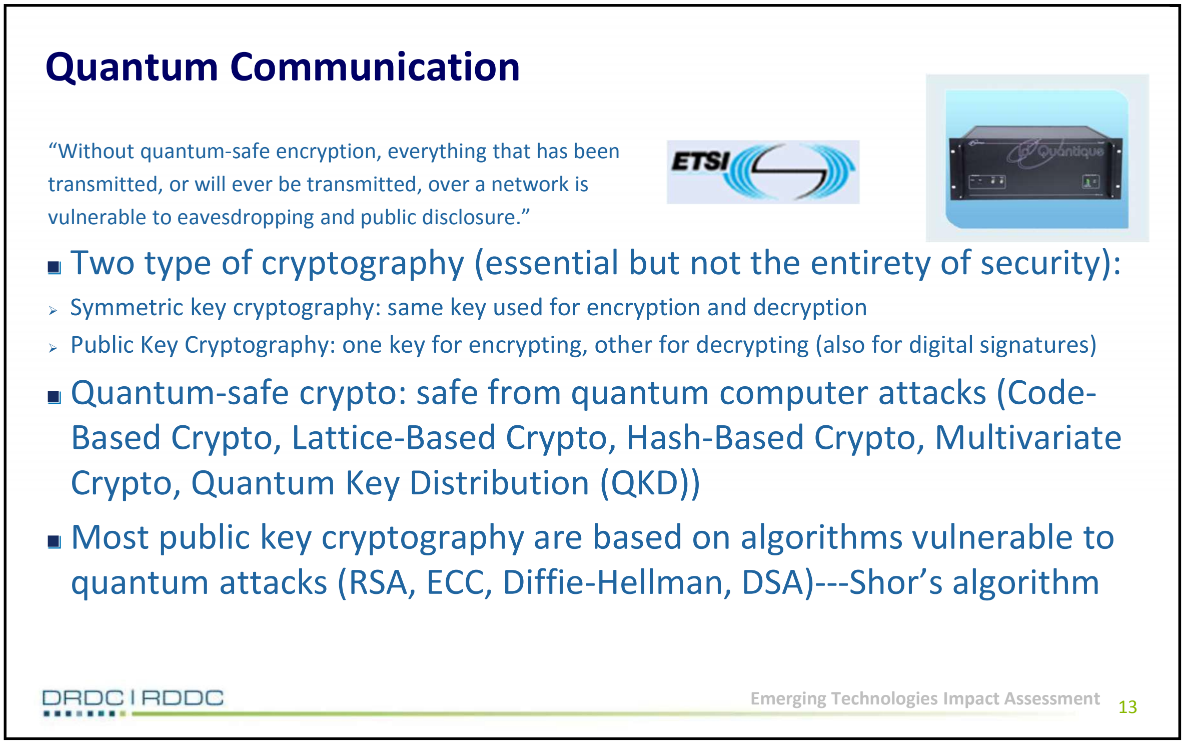
HOW'S YOUR QUANTUM COMPUTER PROTOTYPE COMING ALONG?
GREAT!
THE PROJECT EXISTS IN A SIMULTANEOUS STATE OF BEING BOTH TOTALLY SUCCESSFUL AND NOT EVEN STARTED.
CAN I OBSERVE IT?
THAT'S A TRICKY QUESTION.

- QC hardware and architecture
- The search for the disruptive hardware technology (analogous to transistors for classical computers) will continue
- It is unclear when a dramatic breakthrough will happen
- Larger class of important problems solved more efficiently: Machine Learning, Optimization
- Standards: qubits, correlation, coherence time
- Exploitation of non-universal QC to solve certain problems

DRDC | RDDC Emerging Technologies Impact Assessment 11

QUANTUM COMMUNICATION

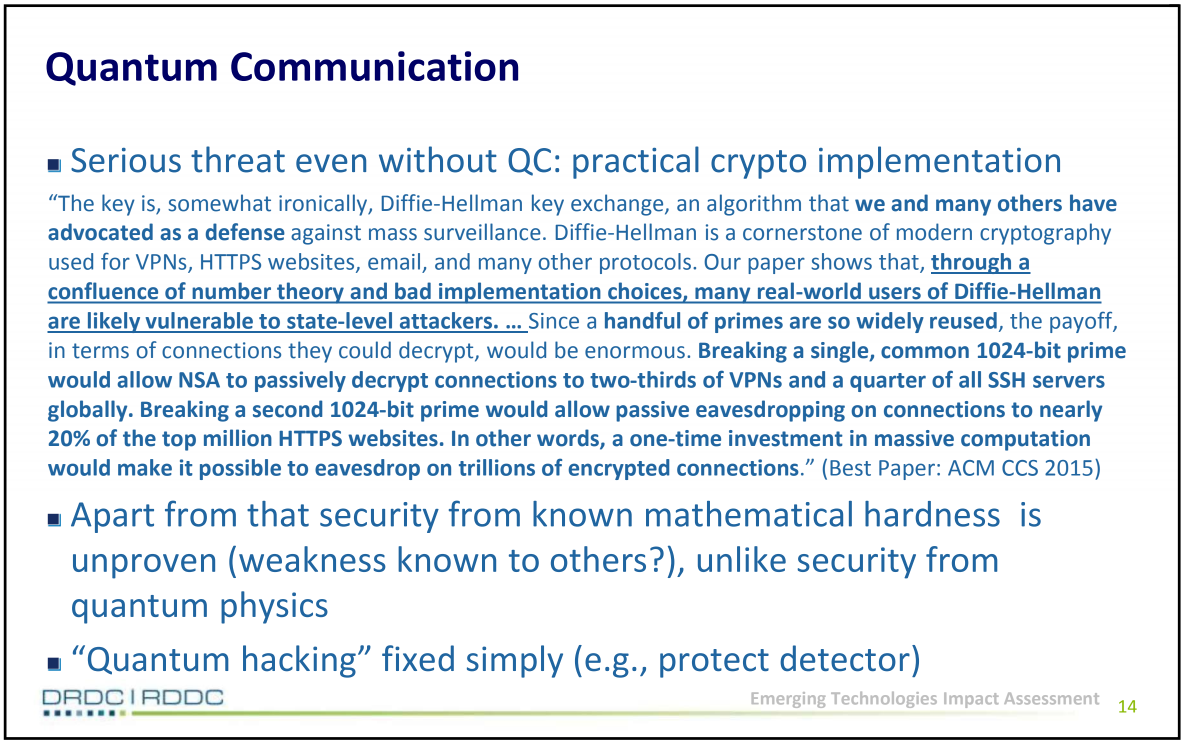
DRDC | RDDC Emerging Technologies Impact Assessment 12



Quantum Communication

"Without quantum-safe encryption, everything that has been transmitted, or will ever be transmitted, over a network is vulnerable to eavesdropping and public disclosure."

- Two type of cryptography (essential but not the entirety of security):
  - Symmetric key cryptography: same key used for encryption and decryption
  - Public Key Cryptography: one key for encrypting, other for decrypting (also for digital signatures)
- Quantum-safe crypto: safe from quantum computer attacks (Code-Based Crypto, Lattice-Based Crypto, Hash-Based Crypto, Multivariate Crypto, Quantum Key Distribution (QKD))
- Most public key cryptography are based on algorithms vulnerable to quantum attacks (RSA, ECC, Diffie-Hellman, DSA)---Shor's algorithm



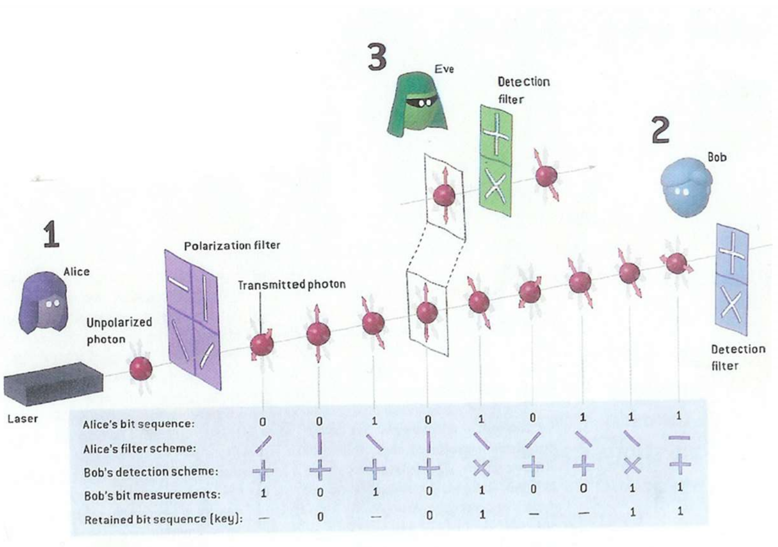
Quantum Communication

- Serious threat even without QC: practical crypto implementation

"The key is, somewhat ironically, Diffie-Hellman key exchange, an algorithm that **we and many others have advocated as a defense** against mass surveillance. Diffie-Hellman is a cornerstone of modern cryptography used for VPNs, HTTPS websites, email, and many other protocols. Our paper shows that, **through a confluence of number theory and bad implementation choices, many real-world users of Diffie-Hellman are likely vulnerable to state-level attackers. …** Since a **handful of primes are so widely reused**, the payoff, in terms of connections they could decrypt, would be enormous. **Breaking a single, common 1024-bit prime would allow NSA to passively decrypt connections to two-thirds of VPNs and a quarter of all SSH servers globally. Breaking a second 1024-bit prime would allow passive eavesdropping on connections to nearly 20% of the top million HTTPS websites. In other words, a one-time investment in massive computation would make it possible to eavesdrop on trillions of encrypted connections**." (Best Paper: ACM CCS 2015)

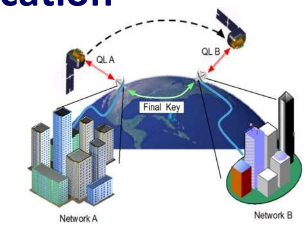
- Apart from that security from known mathematical hardness is unproven (weakness known to others?), unlike security from quantum physics
- "Quantum hacking" fixed simply (e.g., protect detector)

Quantum Key Distribution

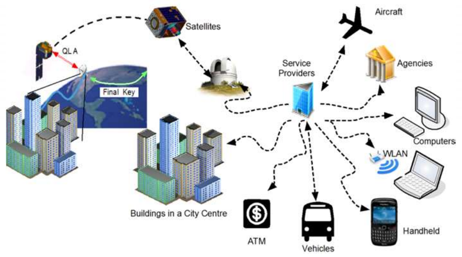


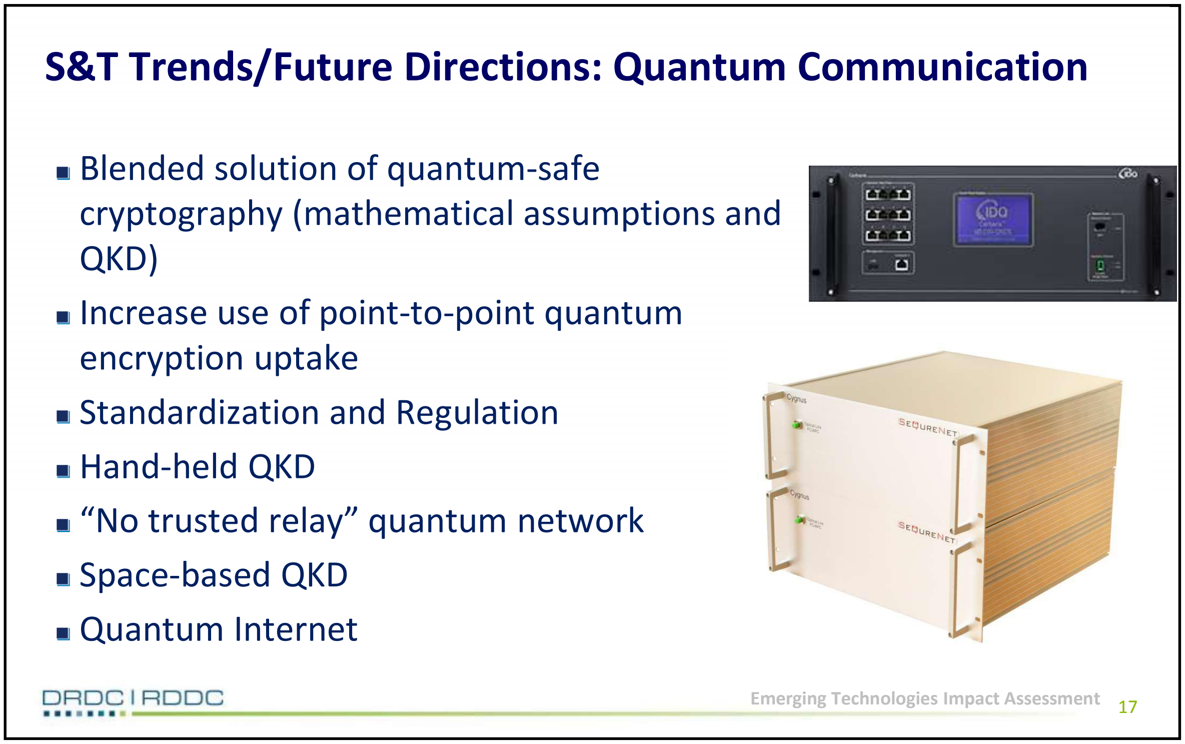
Alice's bit sequence:	0	0	1	0	1	0	1	1	1
Alice's filter scheme:	/	|	\	|	\	/	\	\	—
Bob's detection scheme:	+	+	+	+	×	+	+	×	+
Bob's bit measurements:	1	0	1	0	1	0	0	1	1
Retained bit sequence (key):	—	0	—	0	1	—	—	1	1

Potential Applications: Quantum Communication



- Quantum-safe communication based on QKD
- Provably secure communication within base
- Longer distance secure communication via fiber
- Space-based QKD : Satellite bridges the large gap between ground based quantum networks
- Secure cloud communication
- Air-to-ground communication/data link
- Quantum internet



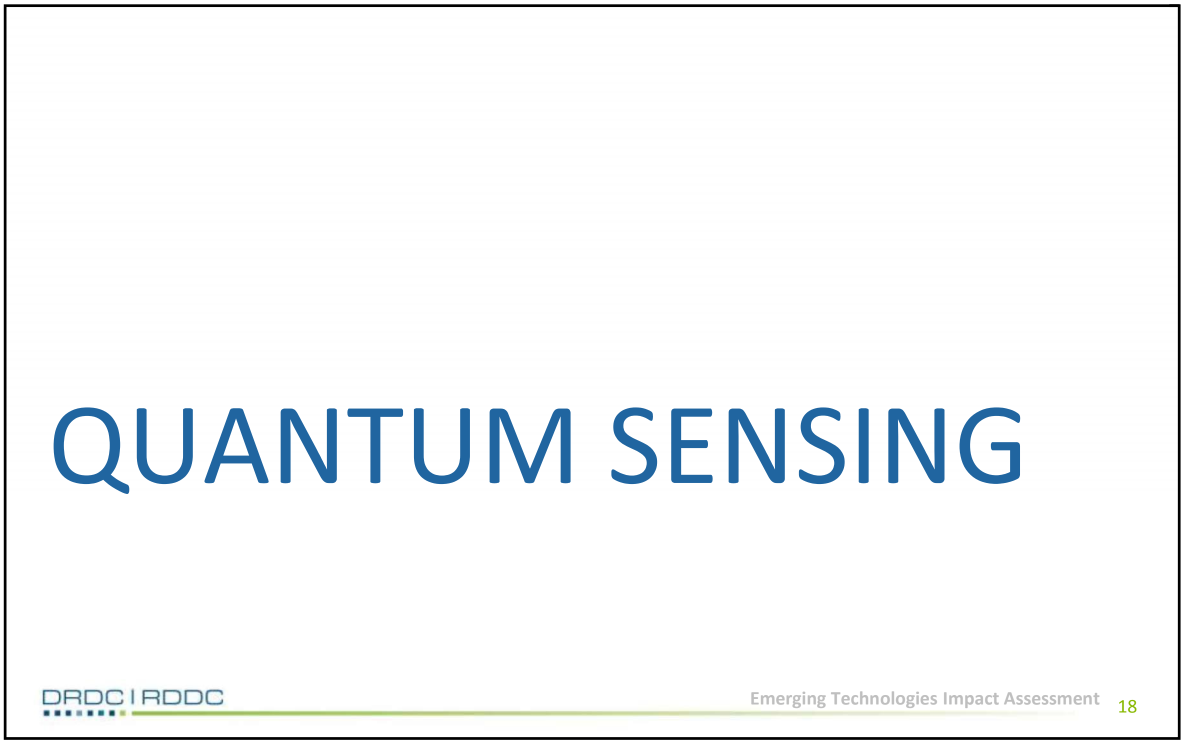


S&T Trends/Future Directions: Quantum Communication

- Blended solution of quantum-safe cryptography (mathematical assumptions and QKD)
- Increase use of point-to-point quantum encryption uptake
- Standardization and Regulation
- Hand-held QKD
- "No trusted relay" quantum network
- Space-based QKD
- Quantum Internet

DRDC I RDDC

Emerging Technologies Impact Assessment 17



QUANTUM SENSING

DRDC I RDDC

Emerging Technologies Impact Assessment 18

Active Quantum Sensing

- Classical Sensor performance limit(Standard Quantum Limit): $1/N^{1/2}$
- Ultimate (Quantum) sensor performance limit (**Heisenberg Limit**): 1/N
- Reason for quantum gain: Quantum Entanglement, Squeezed States,…
- Classification of Active Quantum Sensors

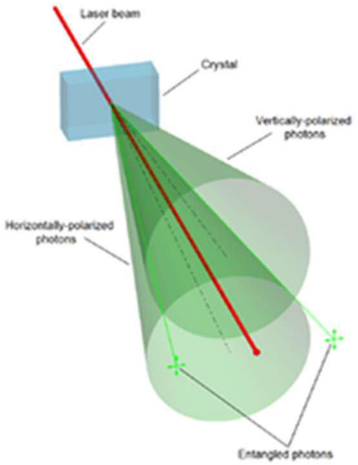
Type 0: Classical Transmitter and Receiver

Type 1: Classical Transmitter and Quantum Receiver

Type 2: Quantum Transmitter and Classical Receiver

Type 3: Quantum Transmitter and Quantum Receiver (Quantum Radar/Lidar)

- Position, Navigation and Timing Sensing: inertial navigation system (no GPS)
- Quantum Clocks: Microwave and Optical Clocks

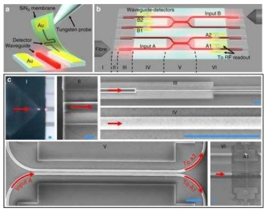


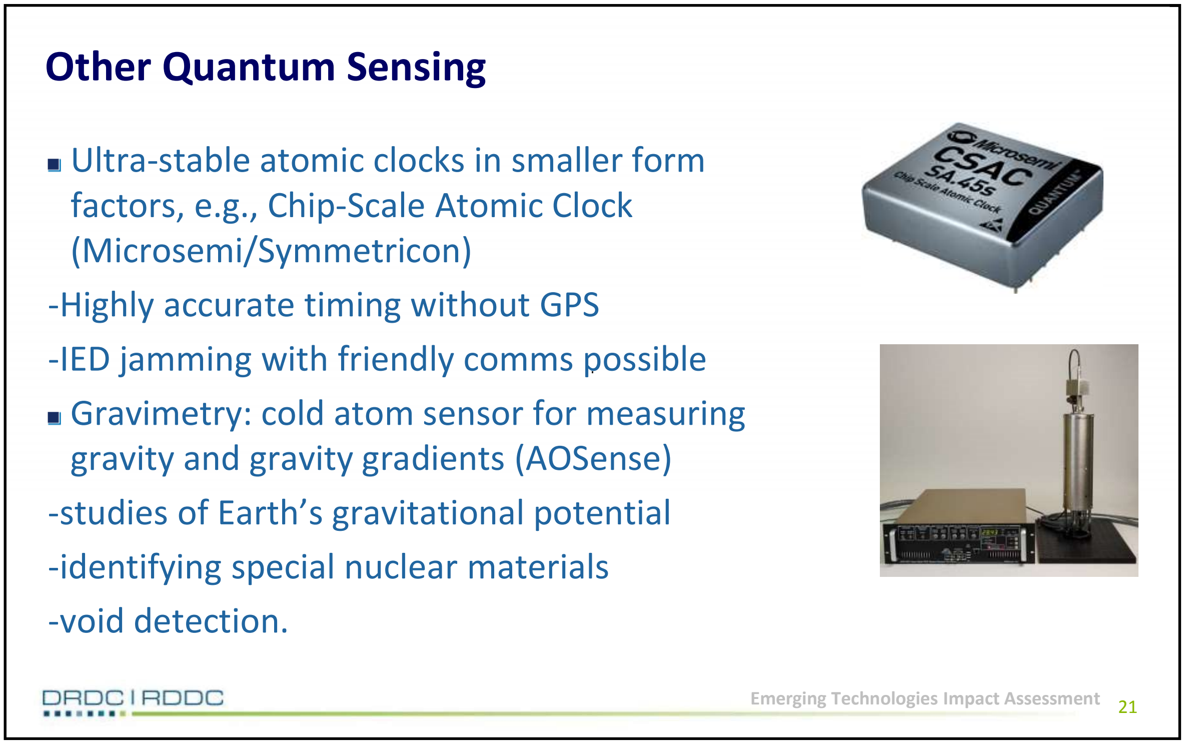
Some Quantum Sensing Technological Possibilities

- Massive gains in sensitivity possible even with **far-from-optimal quantum-enhanced sensing**, e.g., single photon imaging

“LIDAR signal-acquisition time must be long enough to **collect the 100 to 1000 photons per pixel (ppp)** … a framework that recovers accurate reflectivity and 3D images simultaneously using on the **order of 1 detected ppp averaged over the scene**.”

- Rethink active and passive optical imaging sensors (covert range finding, lidar, IR, multi-spectral and hyperspectral sensors) including standoff chemical detection
- Similar gains definitely possible in microwave regime as well: quantum-enhanced radar (microwave quantum optics) and quantum ESM---superconducting qubits, Rydberg atoms, etc used in QC





Other Quantum Sensing

- Ultra-stable atomic clocks in smaller form factors, e.g., Chip-Scale Atomic Clock (Microsemi/Symmetricon)

-Highly accurate timing without GPS

-IED jamming with friendly comms possible

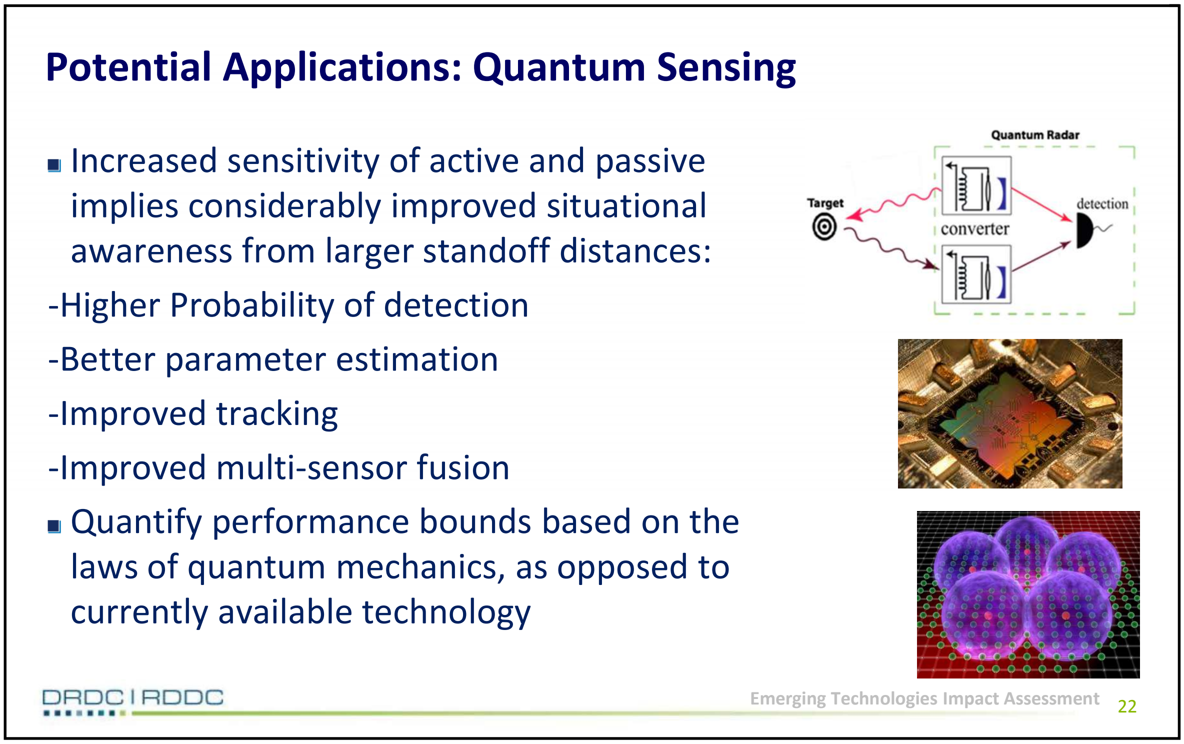
- Gravimetry: cold atom sensor for measuring gravity and gravity gradients (AOSense)

-studies of Earth's gravitational potential

-identifying special nuclear materials

-void detection.

DRDC I RDDC Emerging Technologies Impact Assessment 21



Potential Applications: Quantum Sensing

- Increased sensitivity of active and passive implies considerably improved situational awareness from larger standoff distances:

-Higher Probability of detection

-Better parameter estimation

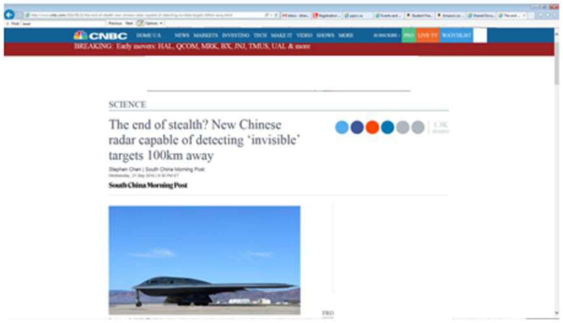
-Improved tracking

-Improved multi-sensor fusion

- Quantify performance bounds based on the laws of quantum mechanics, as opposed to currently available technology

DRDC I RDDC Emerging Technologies Impact Assessment 22

Quantum Radar in the News


CNBC HOME U.S. NEWS MARKETS INVESTING TECH MAKE IT VIDEO SHOWS MORE

BREAKING: Early movers: HAL, QCOM, MRK, BX, JNJ, TMUS, UAL & more

SCIENCE

The end of stealth? New Chinese radar capable of detecting 'invisible' targets 100km away

Stephen Chen | South China Morning Post

South China Morning Post

…**worked with quantum scientists** at the University of Science and Technology of China in Hefei, Anhui province, where many quantum technology breakthroughs have been achieved, including **the world's longest quantum key distribution network for secured communication and the development of the world's first quantum satellite**.

A top Chinese military technology company …announced it had **developed a new form of radar able to detect stealth planes 100km away**. …the new **radar system's entangled photons** had detected targets 100km away in a recent field test. …China's **first "single-photon quantum radar system" had "important military application values"** because it used entangled photons to **identify objects "invisible" to conventional radar systems**. "**The figure in declassified documents is usually a tuned-down version of the real performance**…potential for the **development of highly mobile and sensitive radar systems** able to survive the most challenging combat engagements. Quantum radar systems could be small and would be **able to evade enemy countermeasures such anti-radar missiles** because the ghostly quantum entanglement could not be traced, it said

Quantum Illumination Lidar: Lab Investigation

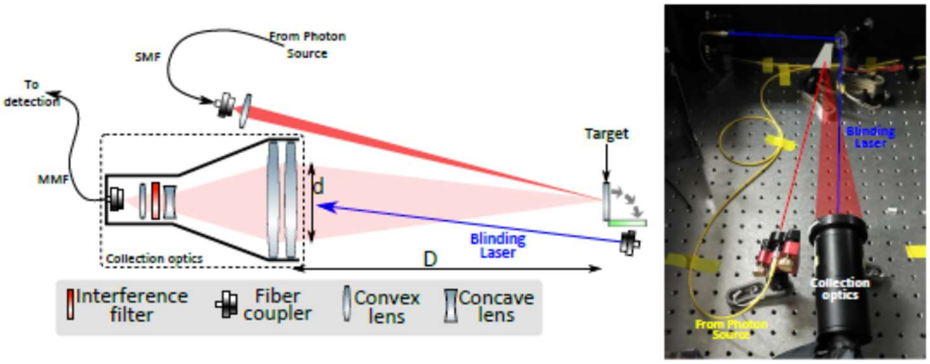
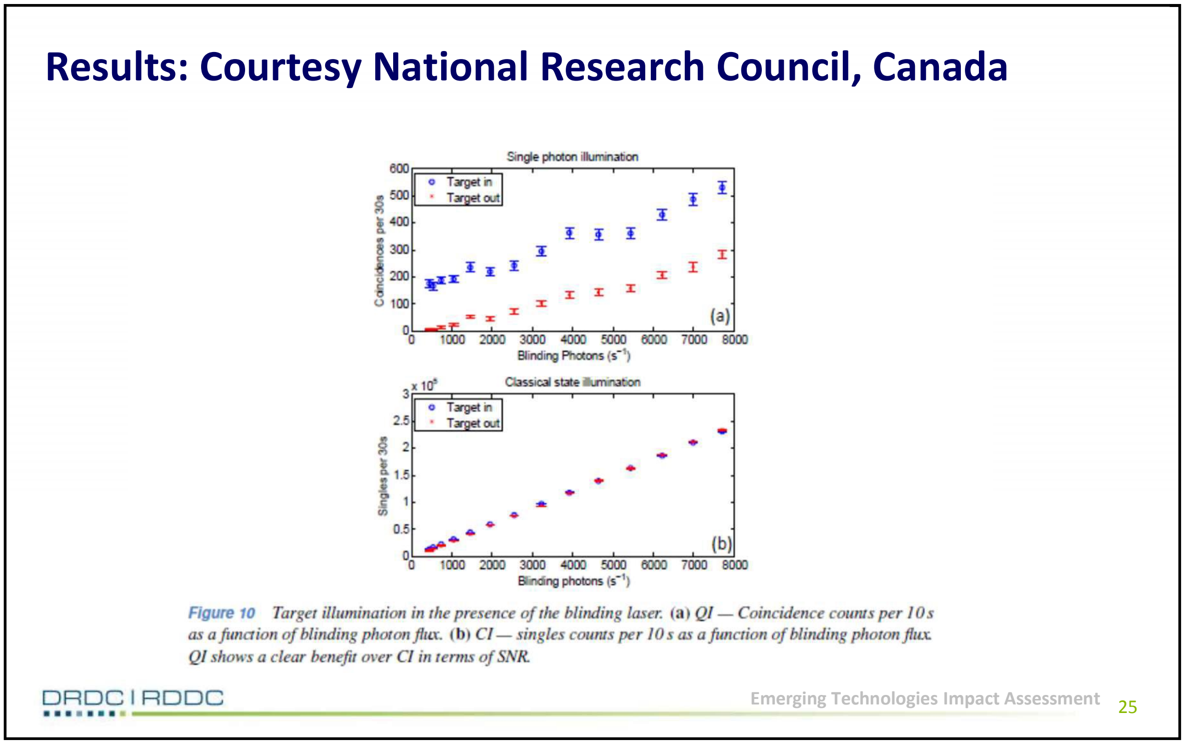


Figure 6 (a) *Schematic diagram of the illumination setup. The target is irradiated with photons from the source delivered via a single mode fiber (SMF) and scattered photons are imaged by the collection optics onto the tip of a multimode fiber (MMF). The MMF delivers photons to the APD for detection. The collection optics are a distance D form the target and the diameter of the mode that is collected is d. The ratio d/D will determine the fraction of the scattered photons that can be collected (see text). An auxiliary laser beam (the blinding laser) is used to provide a background.* (b) *Photograph of the apparatus.*

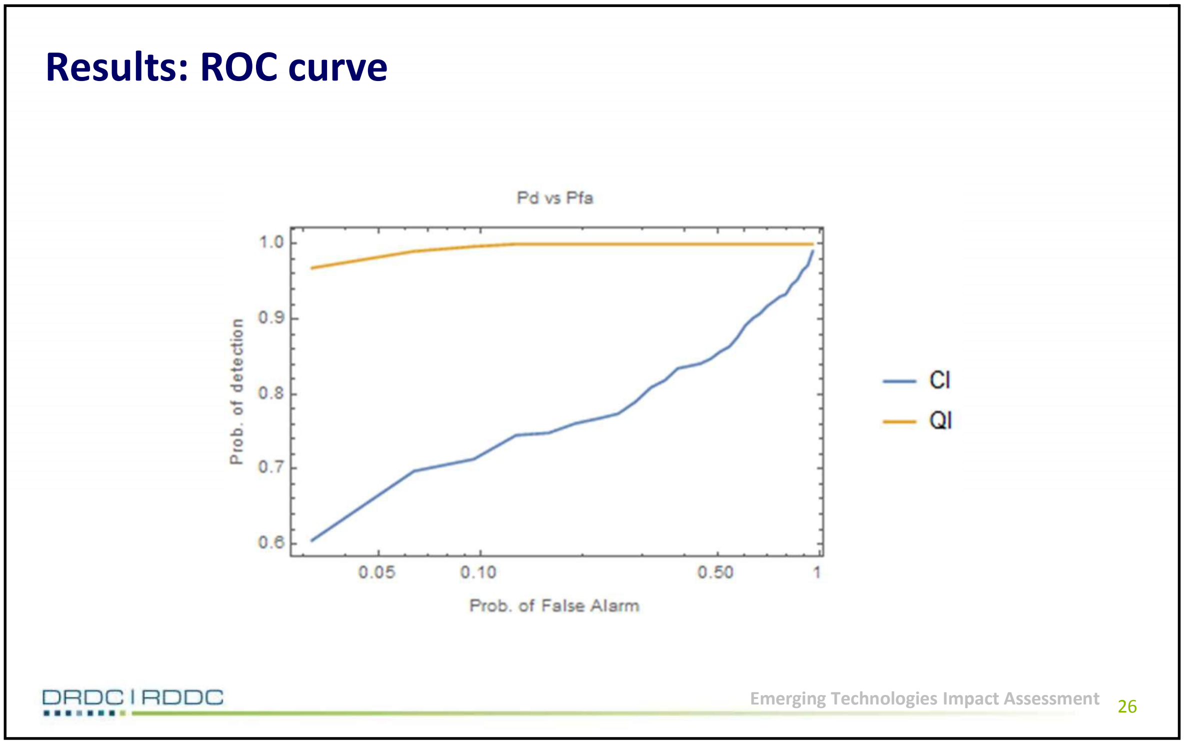


Results: Courtesy National Research Council, Canada

Figure 10 *Target illumination in the presence of the blinding laser.* **(a)** *QI — Coincidence counts per 10 s as a function of blinding photon flux.* **(b)** *CI — singles counts per 10 s as a function of blinding photon flux. QI shows a clear benefit over CI in terms of SNR.*

DRDC | RDDC

Emerging Technologies Impact Assessment 25

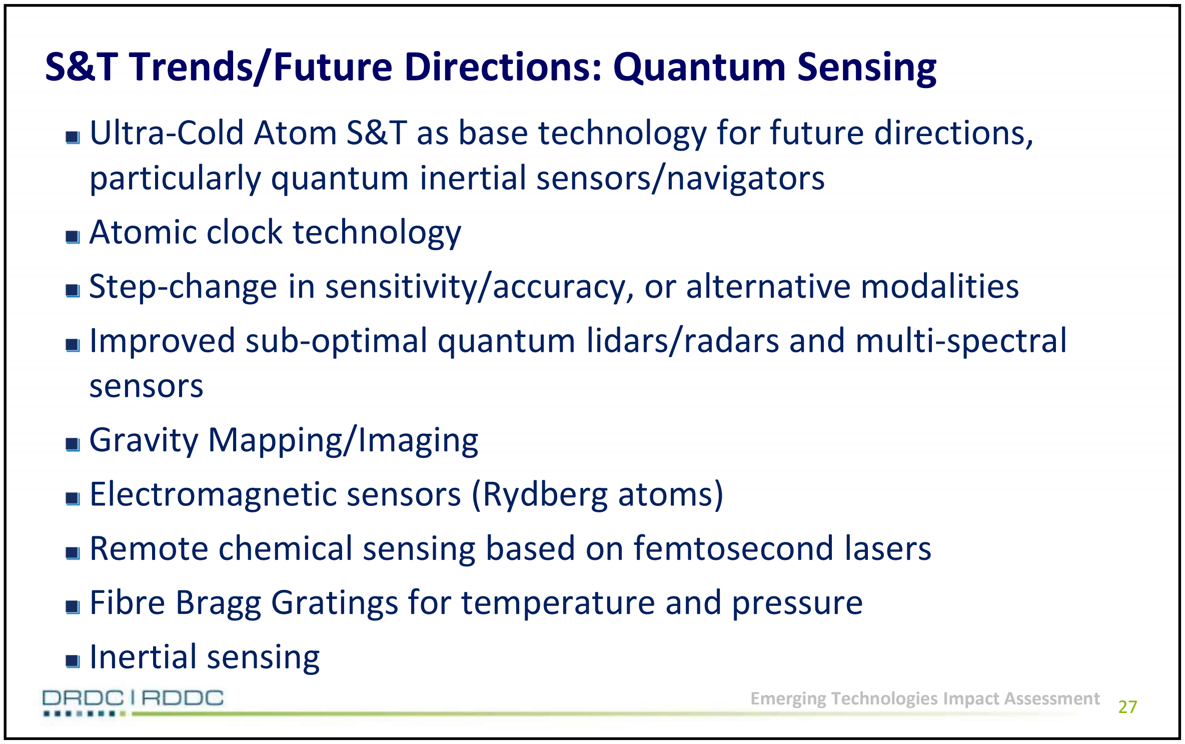


Results: ROC curve

DRDC | RDDC

Emerging Technologies Impact Assessment 26

xxx

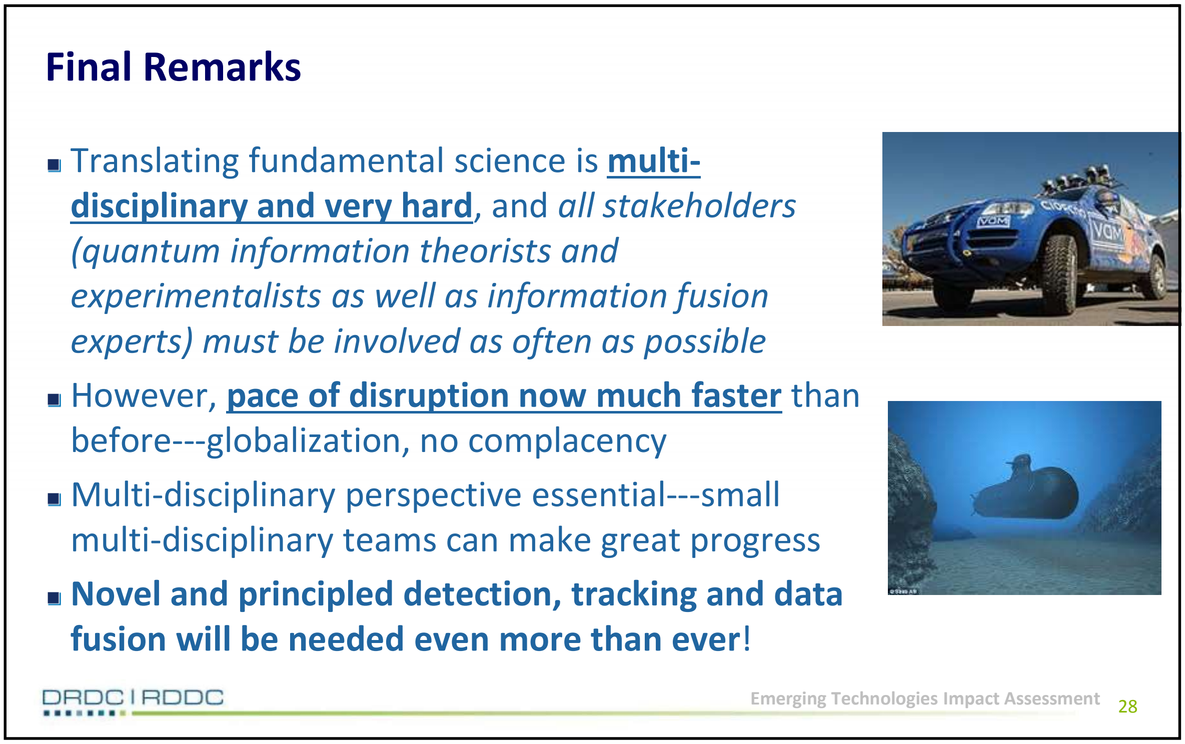


S&T Trends/Future Directions: Quantum Sensing

- Ultra-Cold Atom S&T as base technology for future directions, particularly quantum inertial sensors/navigators
- Atomic clock technology
- Step-change in sensitivity/accuracy, or alternative modalities
- Improved sub-optimal quantum lidars/radars and multi-spectral sensors
- Gravity Mapping/Imaging
- Electromagnetic sensors (Rydberg atoms)
- Remote chemical sensing based on femtosecond lasers
- Fibre Bragg Gratings for temperature and pressure
- Inertial sensing

DRDC | RDDC

Emerging Technologies Impact Assessment 27



Final Remarks

- Translating fundamental science is **multi-disciplinary and very hard**, and *all stakeholders (quantum information theorists and experimentalists as well as information fusion experts) must be involved as often as possible*
- However, **pace of disruption now much faster** than before---globalization, no complacency
- Multi-disciplinary perspective essential---small multi-disciplinary teams can make great progress
- **Novel and principled detection, tracking and data fusion will be needed even more than ever**!

DRDC | RDDC

Emerging Technologies Impact Assessment 28

DRDC | RDDC

SCIENCE, TECHNOLOGY AND KNOWLEDGE FOR CANADA'S DEFENCE AND SECURITY

SCIENCE, TECHNOLOGIE ET SAVOIR POUR LA DÉFENSE ET LA SÉCURITÉ DU CANADA

29

References

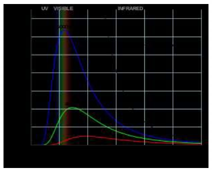
- *Quantum Sensing: A Scientometric Study, NRC Nov 2015*
- *UK Quantum Technology Landscape 2014*
- *Quantum Safe Cryptography and Security June 2015, European Telecommunication Standards Institute*
- *A Roadmap for quantum technologies in the UK, Oct 2015*
- *National Strategy for quantum technologies, UK, Oct 2015*

DRDC | RDDC

Emerging Technologies Impact Assessment 30

MISCELLANEOUS/BACKUP

What is the Underpinning Science

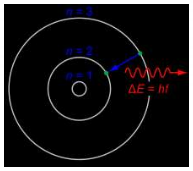


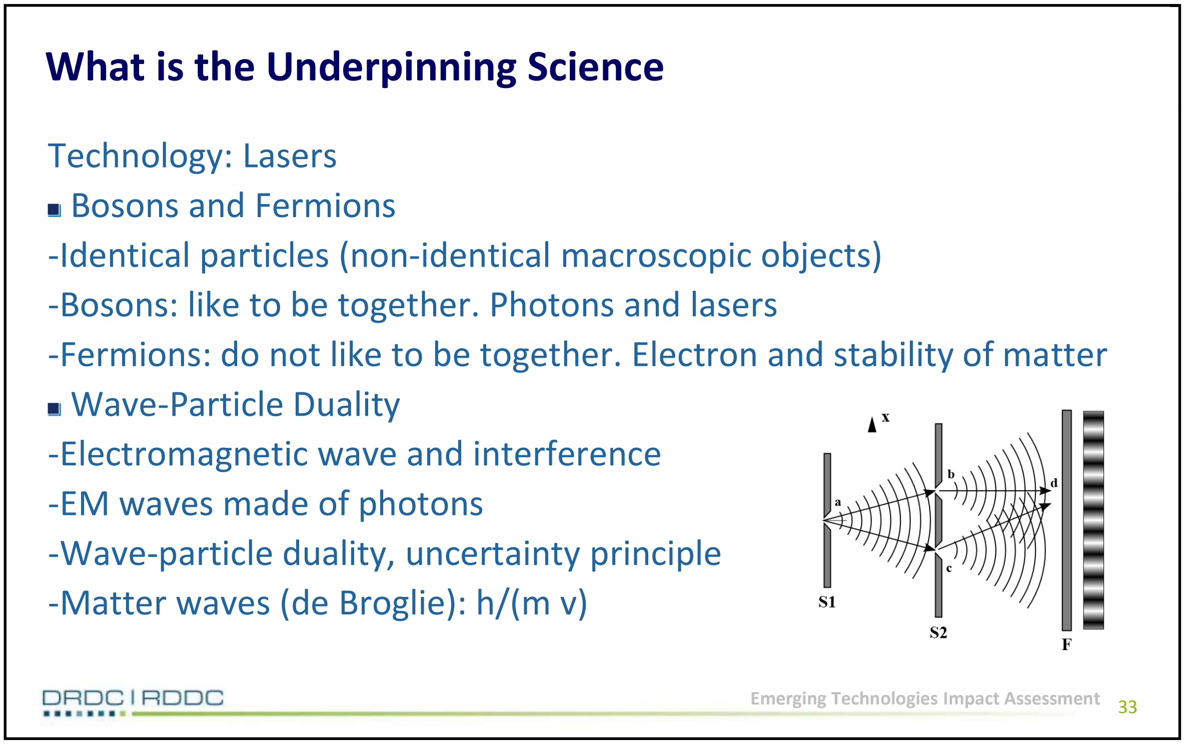
Example Technologies: time and frequency standards, microwave atomic clocks (Quantum 1.0) and optical atomic clocks (Quantum 2.0), spectroscopy, photonics, quantum optics

1) Energy Quantization

-Planck’s Law: radiation energy is “quantized”photon; E = h f

-Bohr Model of Atom: energy levels in atom





What is the Underpinning Science

Technology: Lasers

■ Bosons and Fermions

-Identical particles (non-identical macroscopic objects)

-Bosons: like to be together. Photons and lasers

-Fermions: do not like to be together. Electron and stability of matter

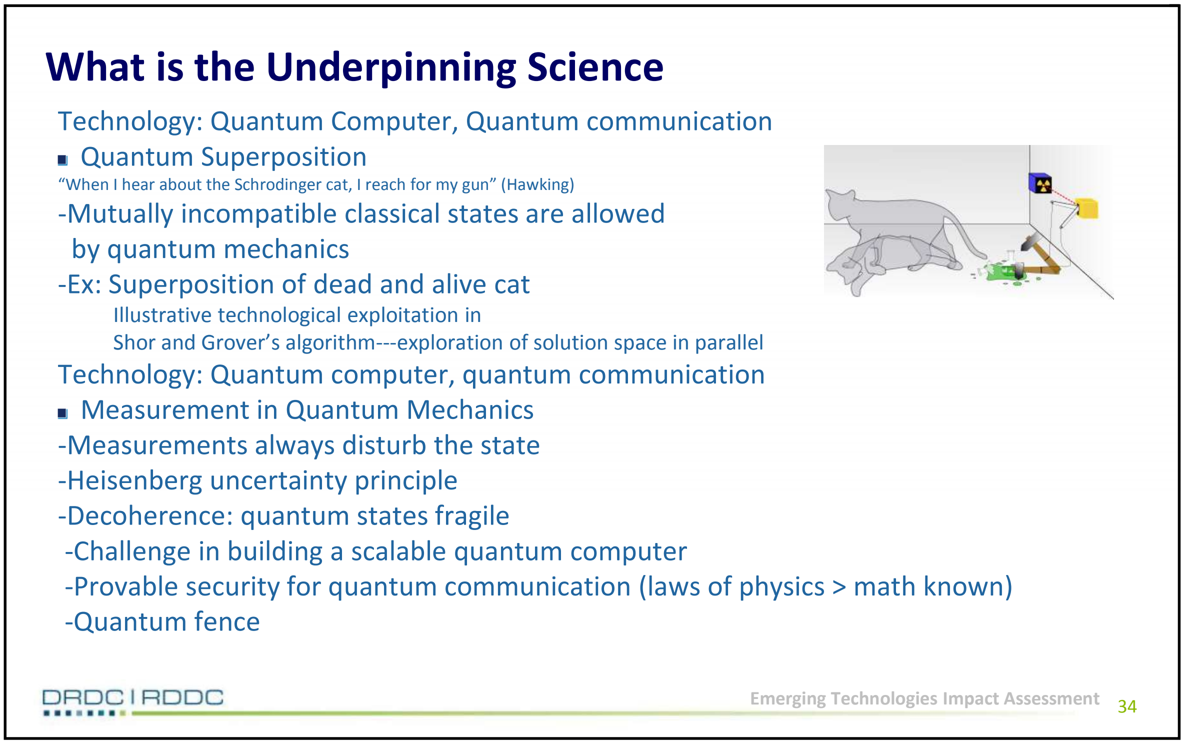
■ Wave-Particle Duality

-Electromagnetic wave and interference

-EM waves made of photons

-Wave-particle duality, uncertainty principle

-Matter waves (de Broglie): h/(m v)



What is the Underpinning Science

Technology: Quantum Computer, Quantum communication

■ Quantum Superposition

“When I hear about the Schrodinger cat, I reach for my gun” (Hawking)

-Mutually incompatible classical states are allowed by quantum mechanics

-Ex: Superposition of dead and alive cat

Illustrative technological exploitation in Shor and Grover’s algorithm---exploration of solution space in parallel

Technology: Quantum computer, quantum communication

■ Measurement in Quantum Mechanics

-Measurements always disturb the state

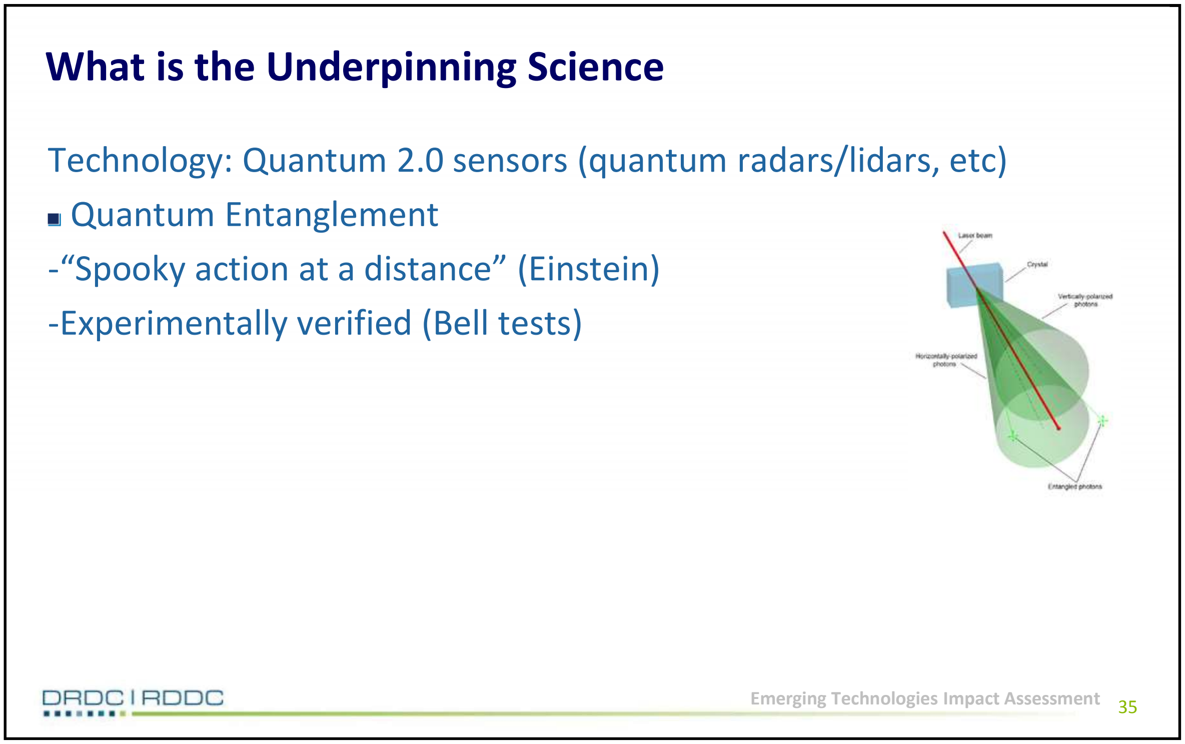
-Heisenberg uncertainty principle

-Decoherence: quantum states fragile

-Challenge in building a scalable quantum computer

-Provable security for quantum communication (laws of physics > math known)

-Quantum fence



What is the Underpinning Science

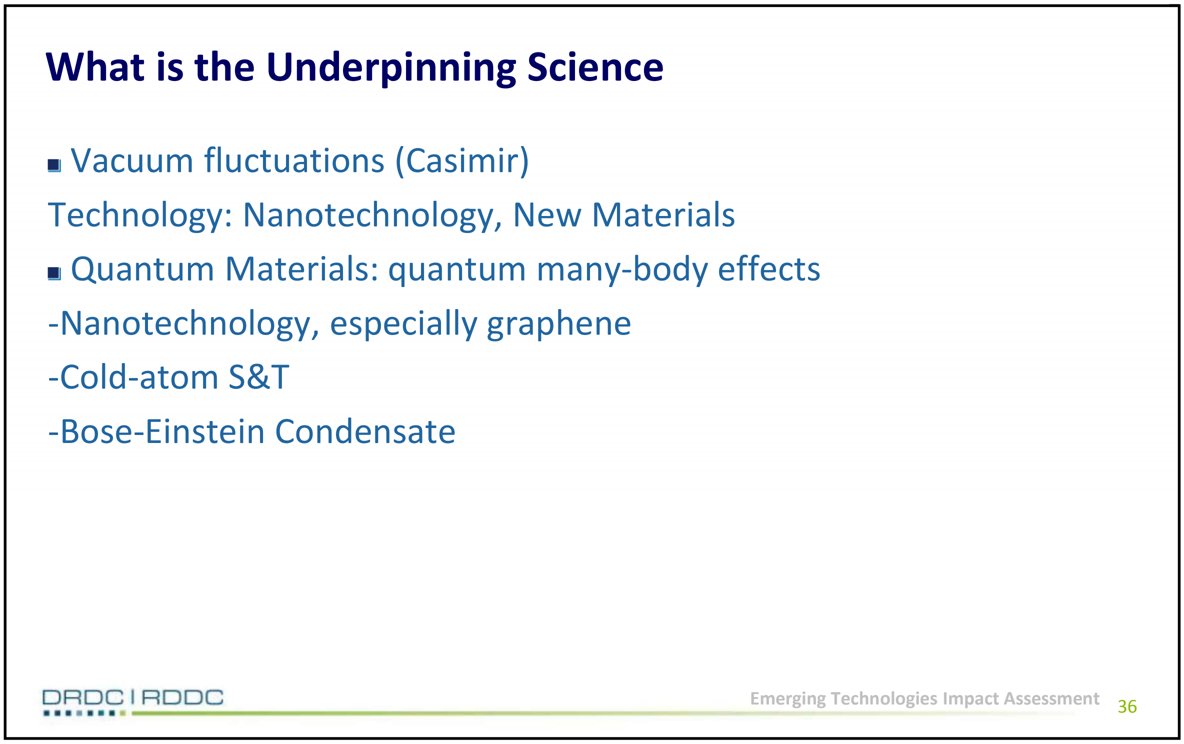
Technology: Quantum 2.0 sensors (quantum radars/lidars, etc)

- Quantum Entanglement

-“Spooky action at a distance” (Einstein)

-Experimentally verified (Bell tests)

Laser beam
Crystal
Vertically-polarized photons
Horizontally-polarized photons
Entangled photons



What is the Underpinning Science

- Vacuum fluctuations (Casimir)

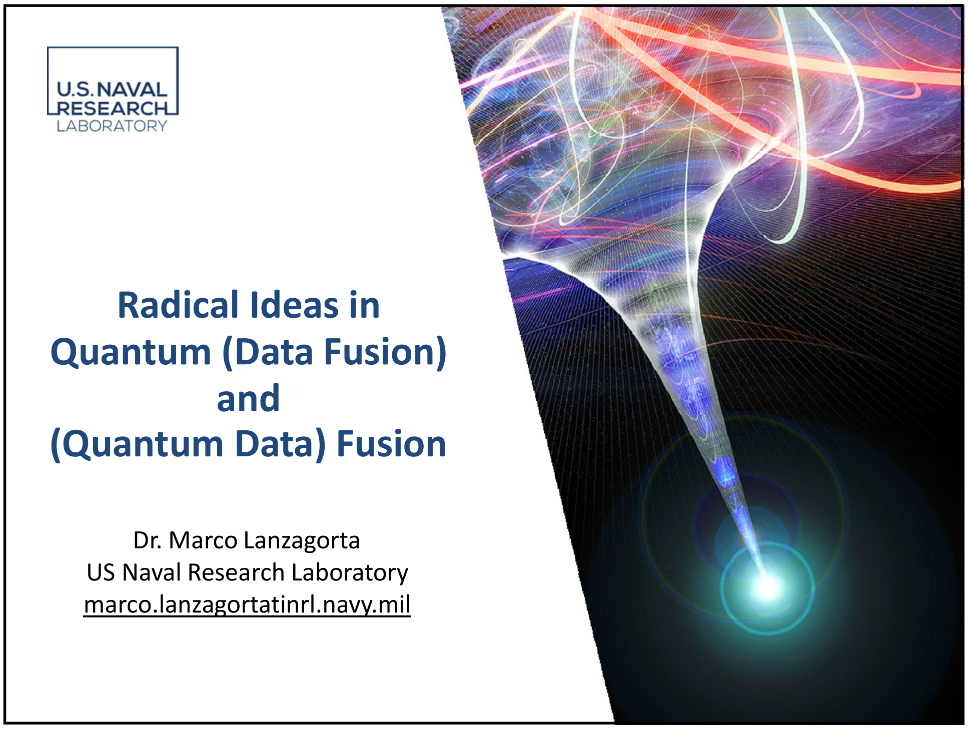
Technology: Nanotechnology, New Materials

- Quantum Materials: quantum many-body effects

-Nanotechnology, especially graphene

-Cold-atom S&T

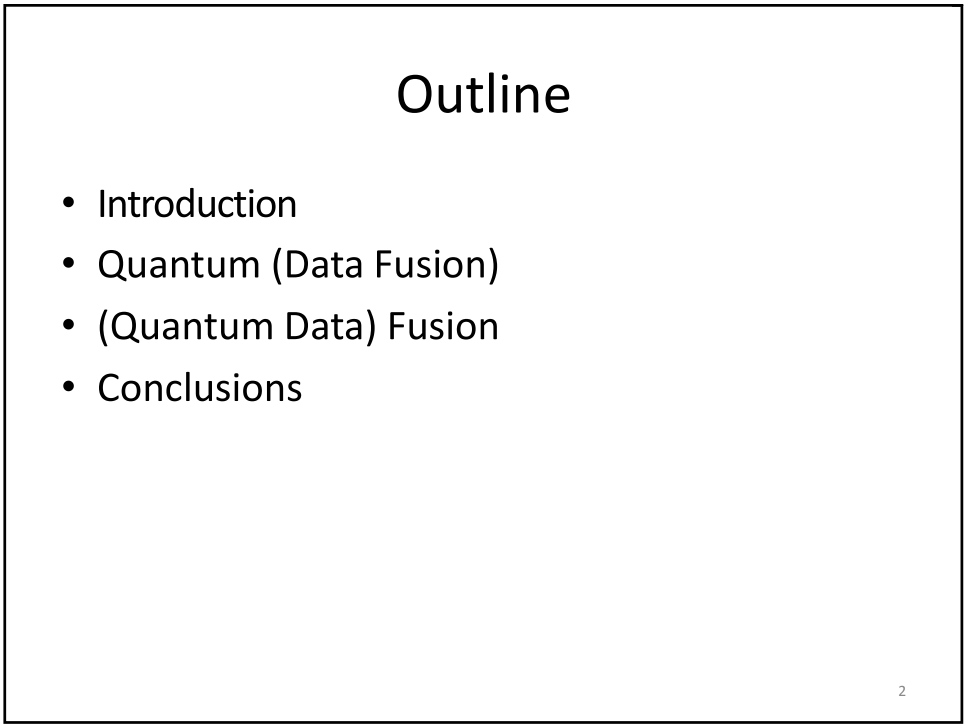
-Bose-Einstein Condensate



U.S. NAVAL RESEARCH LABORATORY

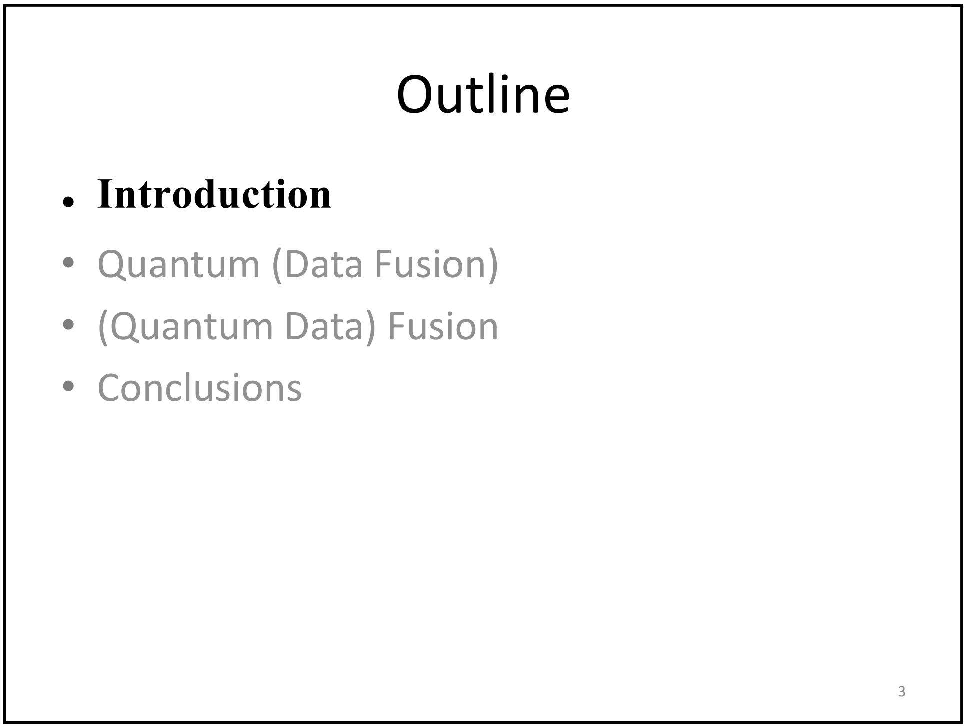
Radical Ideas in Quantum (Data Fusion) and (Quantum Data) Fusion

Dr. Marco Lanzagorta
US Naval Research Laboratory
marco.lanzagortatinrl.navy.mil



Outline

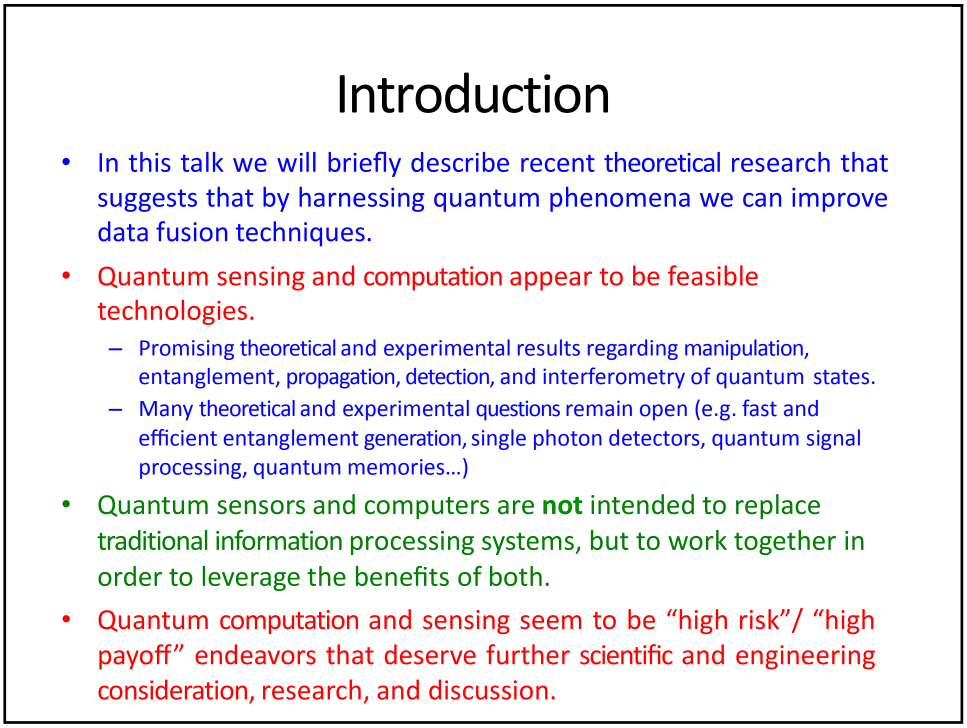
- Introduction
- Quantum (Data Fusion)
- (Quantum Data) Fusion
- Conclusions



Outline

- **Introduction**
- Quantum (Data Fusion)
- (Quantum Data) Fusion
- Conclusions

3

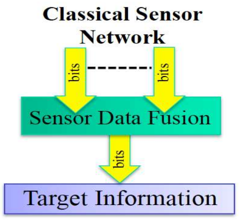


Introduction

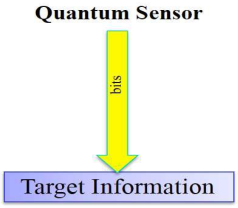
- In this talk we will briefly describe recent theoretical research that suggests that by harnessing quantum phenomena we can improve data fusion techniques.
- Quantum sensing and computation appear to be feasible technologies.
  - Promising theoretical and experimental results regarding manipulation, entanglement, propagation, detection, and interferometry of quantum states.
  - Many theoretical and experimental questions remain open (e.g. fast and efficient entanglement generation, single photon detectors, quantum signal processing, quantum memories…)
- Quantum sensors and computers are **not** intended to replace traditional information processing systems, but to work together in order to leverage the benefits of both.
- Quantum computation and sensing seem to be “high risk”/ “high payoff” endeavors that deserve further scientific and engineering consideration, research, and discussion.

State-of-the-Art

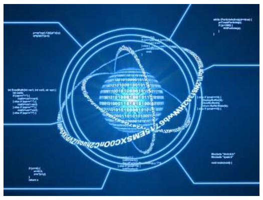
Data Fusion



Quantum Sensing



Quantum Computing



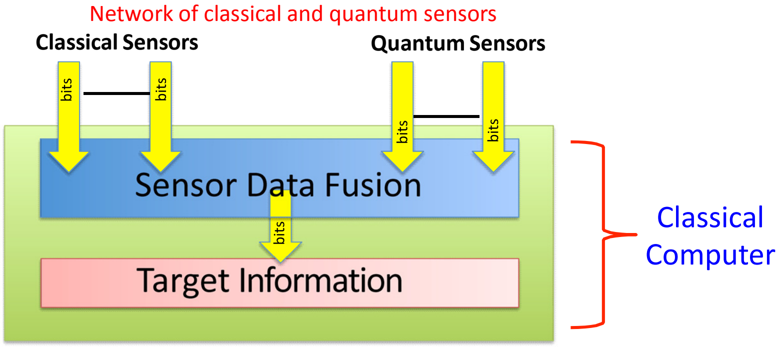
Active areas of research, but not much interaction between them

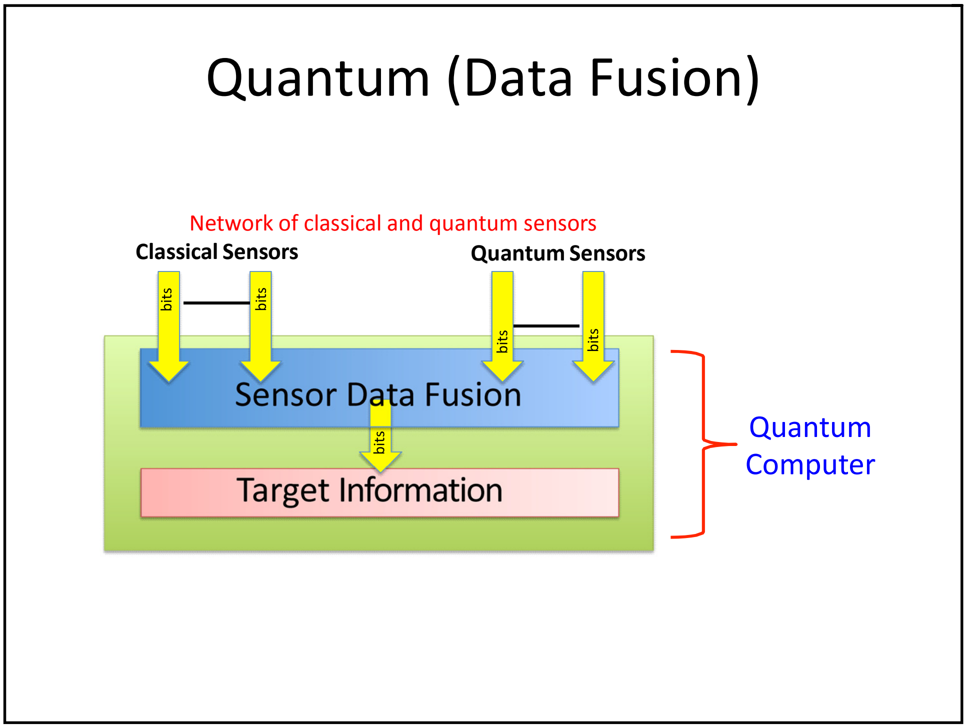
Sensor Data Fusion: how to combine the sensor data from each node in the network to provide the most accurate, complete, timely, and dependable target information available

Quantum Sensing: how to harness quantum phenomena to improve the performance of sensing devices

Quantum Computing: how to harness quantum phenomena to improve the performance of information processing systems

Classical Data Fusion





Quantum (Data Fusion)

Network of classical and quantum sensors

Classical Sensors

Quantum Sensors

bits

bits

bits

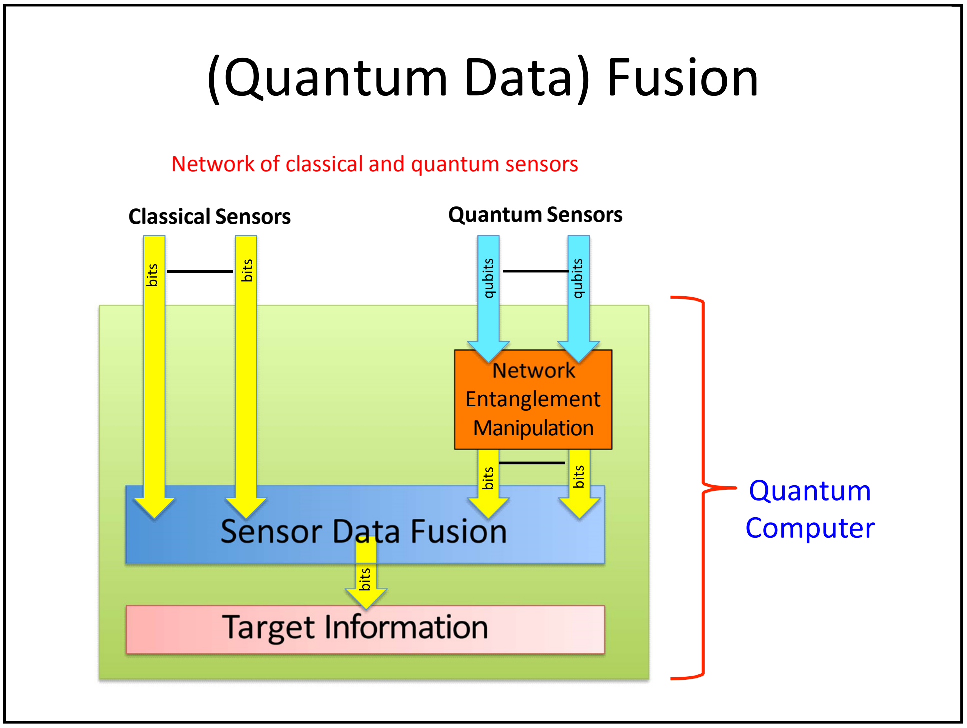
bits

Sensor Data Fusion

bits

Target Information

Quantum Computer



(Quantum Data) Fusion

Network of classical and quantum sensors

Classical Sensors

Quantum Sensors

bits

bits

qubits

qubits

Network Entanglement Manipulation

bits

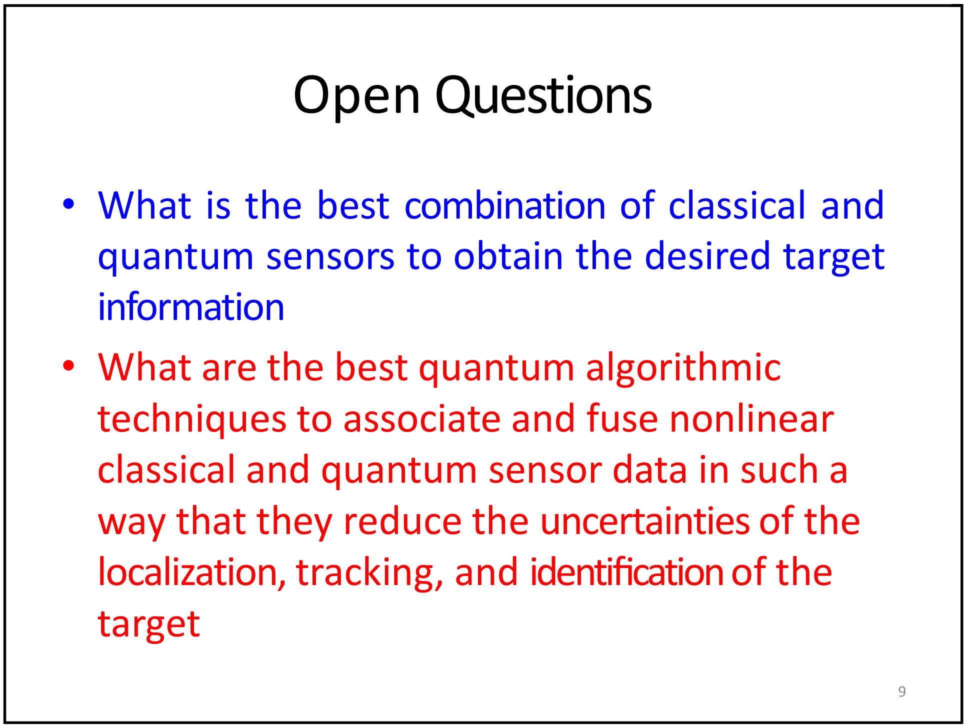
bits

Sensor Data Fusion

bits

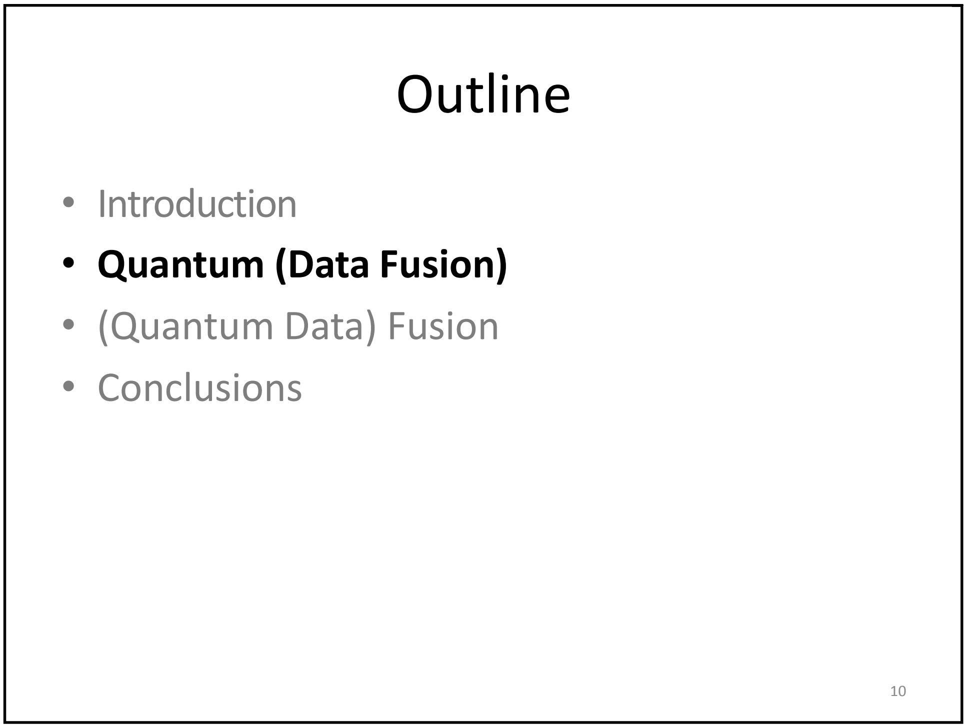
Target Information

Quantum Computer



Open Questions

- What is the best combination of classical and quantum sensors to obtain the desired target information
- What are the best quantum algorithmic techniques to associate and fuse nonlinear classical and quantum sensor data in such a way that they reduce the uncertainties of the localization, tracking, and identification of the target



Outline

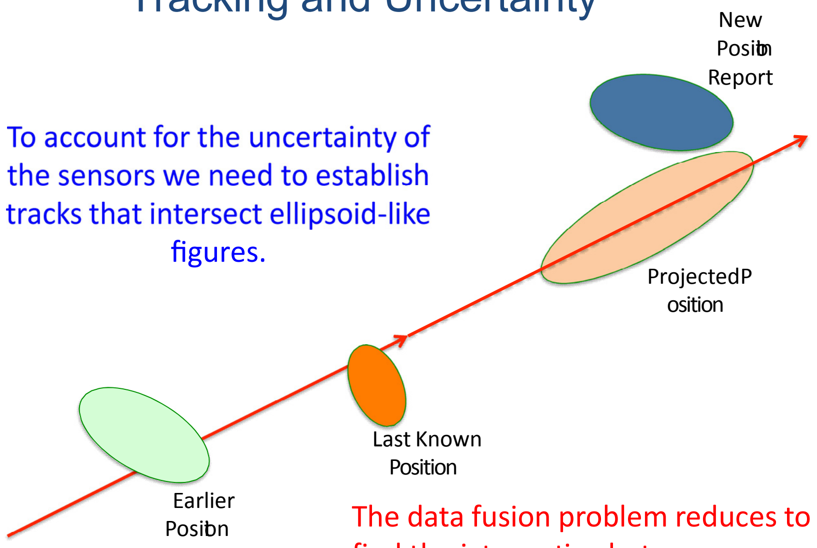
- Introduction
- **Quantum (Data Fusion)**
- (Quantum Data) Fusion
- Conclusions

Data Fusion and Target Tracking

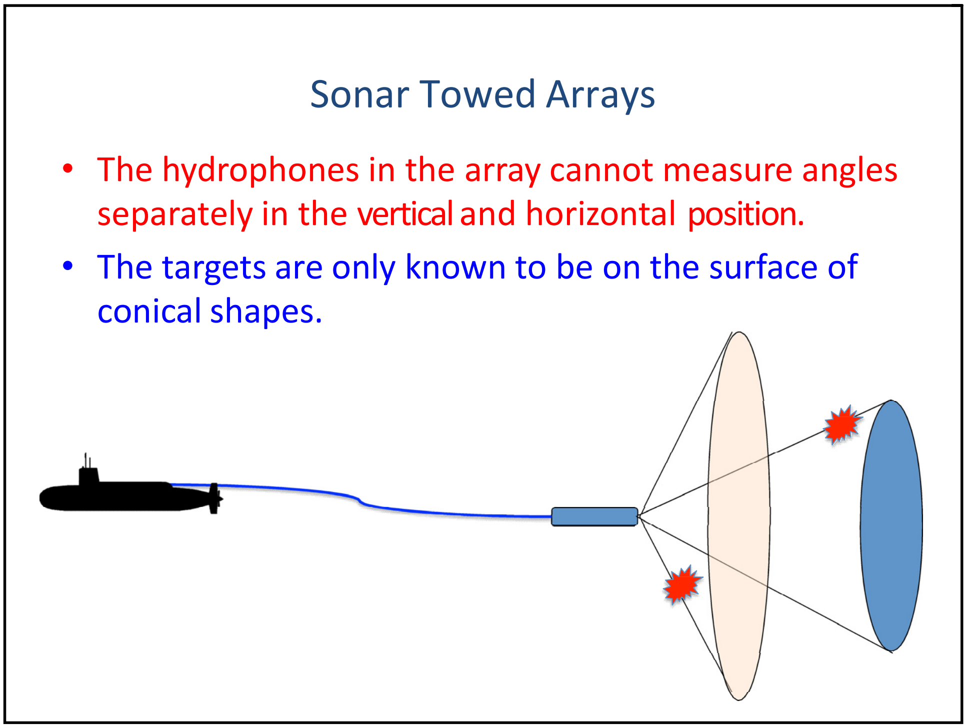
- Multi-sensor data fusion for target tracking is of critical importance to DoD.
  - Missile Defense Systems
  - Sonar Tracking for Undersea Warfare
  - Missile Guidance Systems
  - Command and Control
- The computational kernel of all these applications is basically the same: sophisticated searches in a multidimensional space.
- These are computationally intensive applications which are easily overwhelmed when the datasets grow into the hundreds of elements.

Tracking and Uncertainty

To account for the uncertainty of the sensors we need to establish tracks that intersect ellipsoid-like figures.

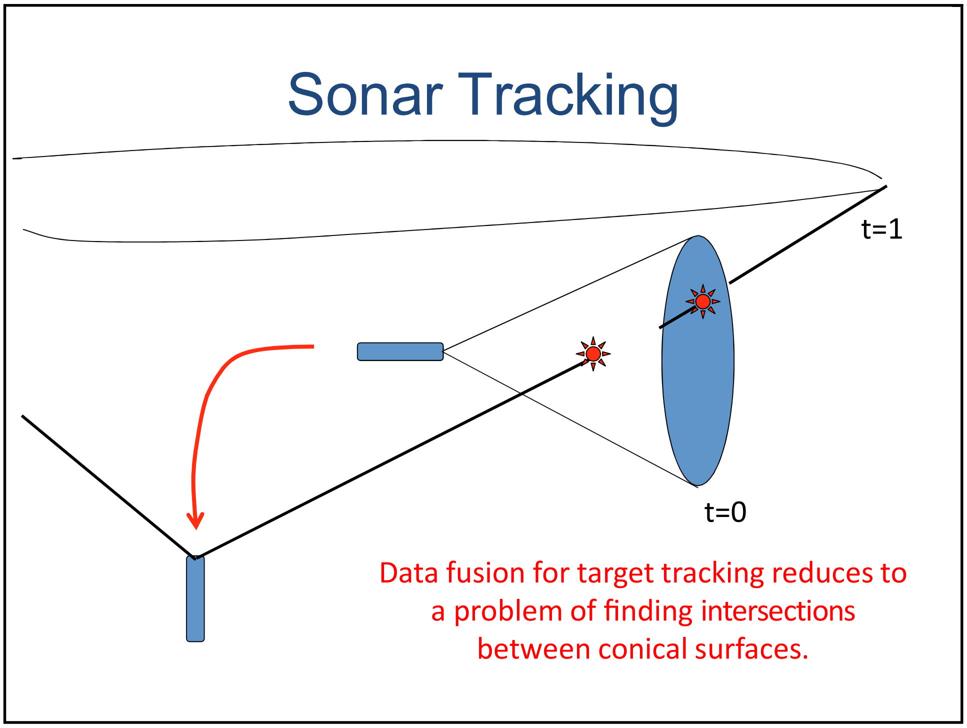


The data fusion problem reduces to find the intersection between ellipsoids and lines



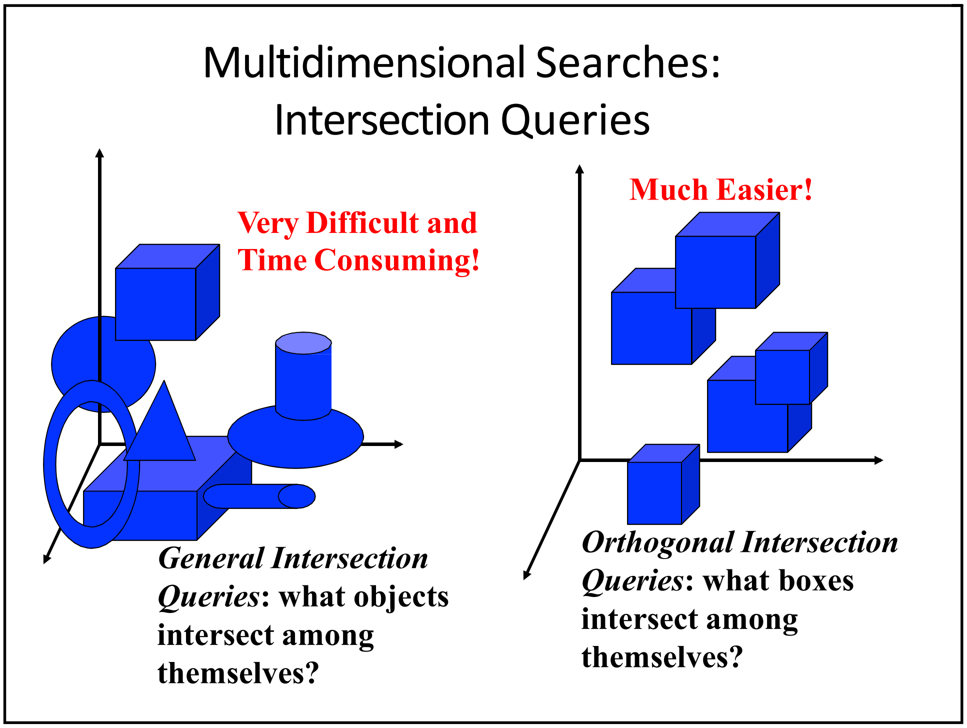
Sonar Towed Arrays

- The hydrophones in the array cannot measure angles separately in the vertical and horizontal position.
- The targets are only known to be on the surface of conical shapes.



Sonar Tracking

Data fusion for target tracking reduces to a problem of finding intersections between conical surfaces.



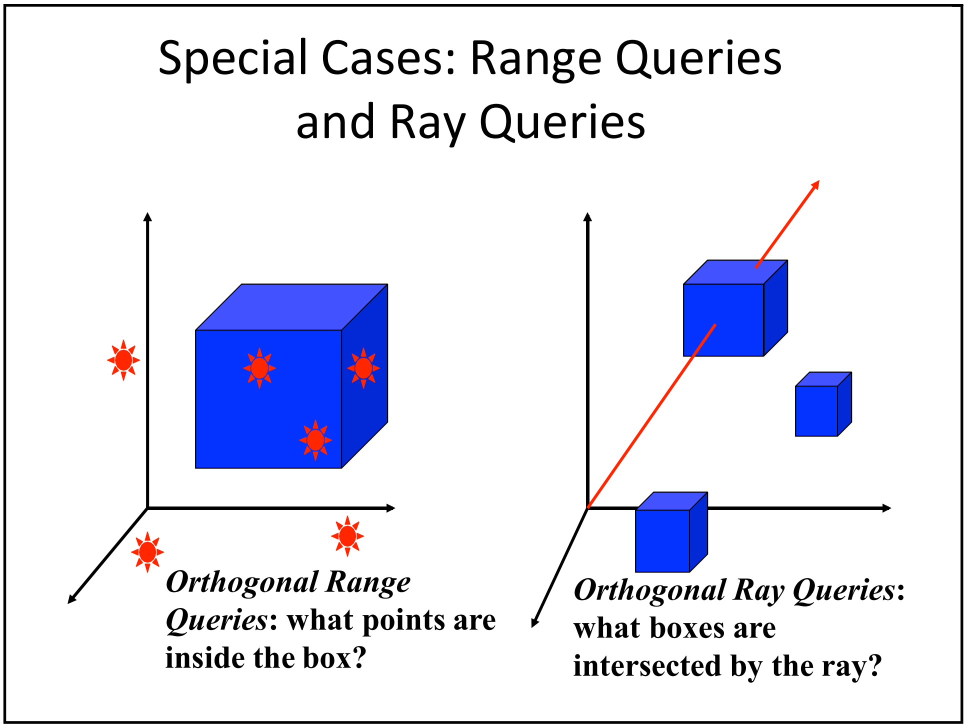
Multidimensional Searches: Intersection Queries

Very Difficult and Time Consuming!

***General Intersection Queries*: what objects intersect among themselves?**

Much Easier!

***Orthogonal Intersection Queries*: what boxes intersect among themselves?**



Special Cases: Range Queries and Ray Queries

***Orthogonal Range Queries*: what points are inside the box?**

***Orthogonal Ray Queries*: what boxes are intersected by the ray?**

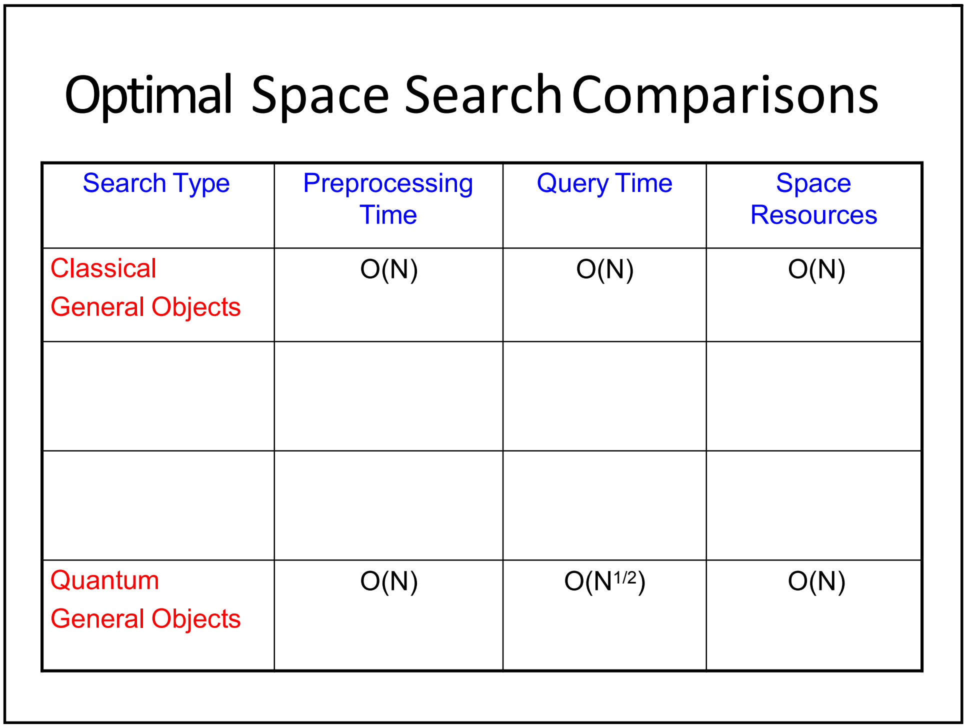
Grover's Algorithm

Quantum algorithm developed by Lov Grover to perform a search of an item from an unsorted and unstructured list of *N* records.

- Performs the search in $O(\sqrt{N})$
- Instead of the *O(N)* required by brute force methods in classical computing.
- This algorithm offers a perfect example of the advantages offered by the parallel manipulation of a quantum superposition.

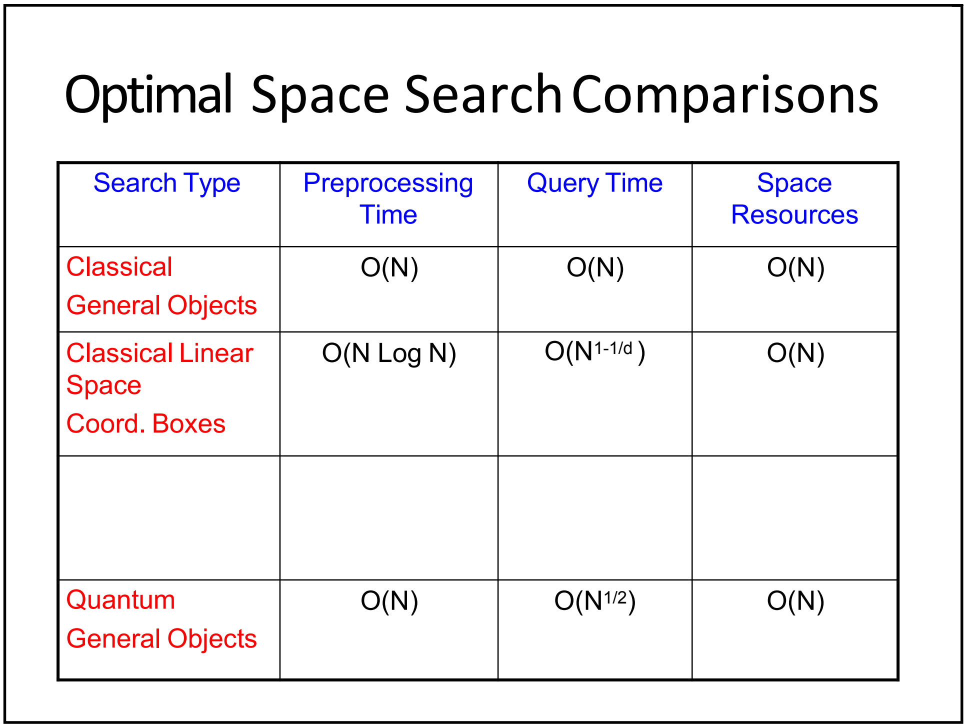
Unsorted & Unstructured Datasets

- If there is no way to sort and/or structure the dataset, then Grover's algorithm is unbeatable.
  - Find a needle in a haystack.
- However, most scientific, industrial, military and financial datasets are alphanumerical strings that can be sorted, structured and ordered.
- But, it may be relevant for multidimensional general intersection queries!



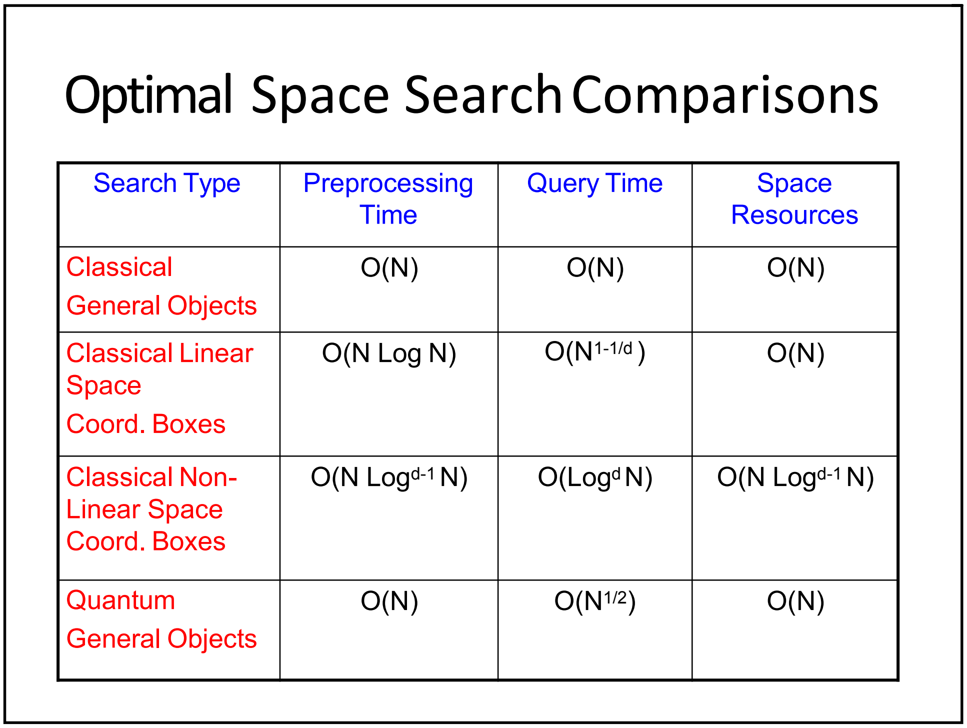
Optimal Space Search Comparisons

Search Type	Preprocessing Time	Query Time	Space Resources
Classical General Objects	O(N)	O(N)	O(N)
Quantum General Objects	O(N)	O($N^{1/2}$)	O(N)



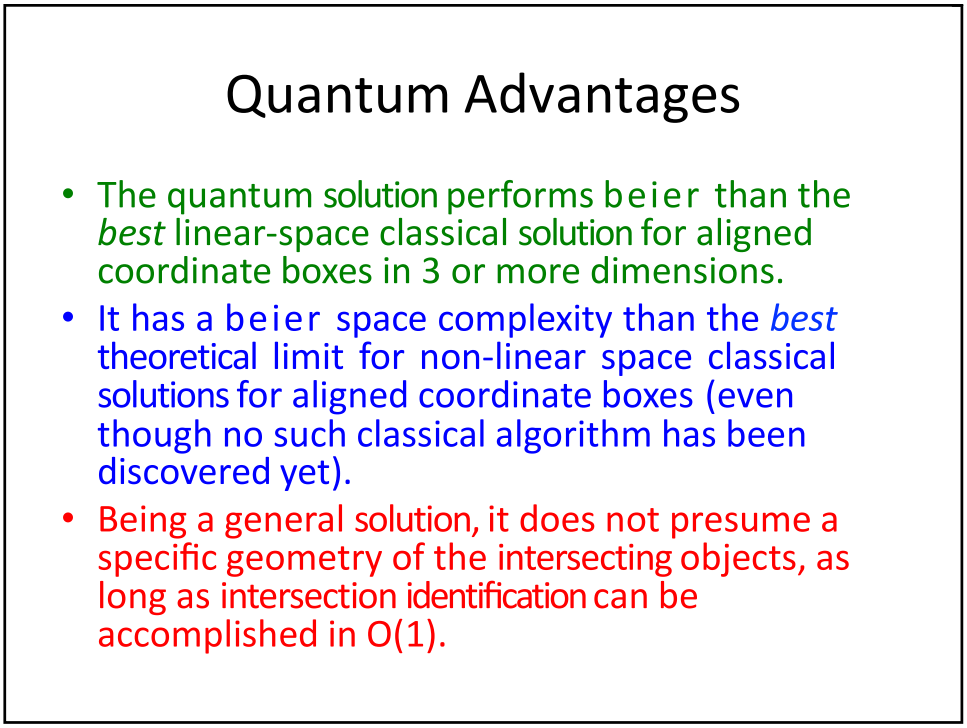
Optimal Space Search Comparisons

Search Type	Preprocessing Time	Query Time	Space Resources
Classical General Objects	O(N)	O(N)	O(N)
Classical Linear Space Coord. Boxes	O(N Log N)	O($N^{1-1/d}$)	O(N)
Quantum General Objects	O(N)	O($N^{1/2}$)	O(N)



Optimal Space Search Comparisons

Search Type	Preprocessing Time	Query Time	Space Resources
Classical General Objects	O(N)	O(N)	O(N)
Classical Linear Space Coord. Boxes	O(N Log N)	$O(N^{1-1/d})$	O(N)
Classical Non-Linear Space Coord. Boxes	$O(N\ \mathrm{Log}^{d-1} N)$	$O(\mathrm{Log}^{d} N)$	$O(N\ \mathrm{Log}^{d-1} N)$
Quantum General Objects	O(N)	$O(N^{1/2})$	O(N)



Quantum Advantages

- The quantum solution performs better than the *best* linear-space classical solution for aligned coordinate boxes in 3 or more dimensions.
- It has a better space complexity than the *best* theoretical limit for non-linear space classical solutions for aligned coordinate boxes (even though no such classical algorithm has been discovered yet).
- Being a general solution, it does not presume a specific geometry of the intersecting objects, as long as intersection identification can be accomplished in O(1).

Outline

- Introduction
- Quantum (Data Fusion)
- **(Quantum Data) Fusion**
- Conclusions

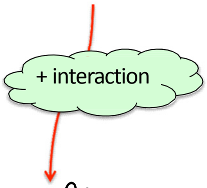
23

Qubit Sensors

Consider 1 qubit sensors, where the information of the physical interaction measured is encoded in the amplitudes:

$$i \;=\; ↲|0i + ,B|1 \qquad \overset{✓}{\begin{matrix} ↲ \\ ,B \end{matrix}}$$

Arbitrary initial state



We assume that the effect of the physical interaction is a rotation of the state of the qubit

$$^{0}i \;=\; \begin{matrix} \cos ⌧/2 & \sin ⌧/2 \\ -\ \sin ⌧/2 & \cos ⌧/2 \end{matrix} \;\overset{◆✓}{}\; \begin{matrix} ↲ \\ ,B \end{matrix}$$

Final state

The rotation angle encodes the effects of the physical interaction that is being measured: finding the angle will give information about the physical environment

Qubit Sensor Sensitivity

Qubit sensors: measurement probabilities change after interacting with the environment

Statistics over a large number of single qubit states gives information about the value of the rotation angle, which is related to the physical interaction:

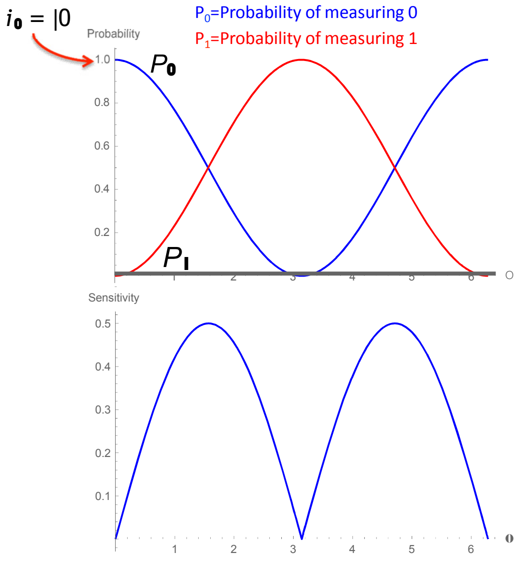
$$\theta \approx 2 \arccos \left(\sqrt{\frac{N_0}{N}} \right)$$

N= Total number of qubits

N_0= Number of measurements that give 0

We define the qubit sensor sensitivity as:

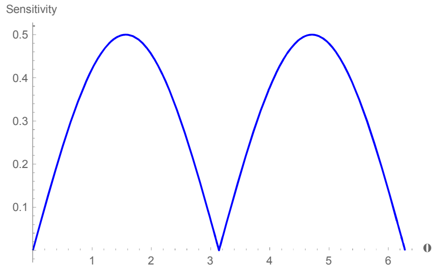
$$S = \frac{dP_i}{d\theta}$$



N-Qubit Sensor Network

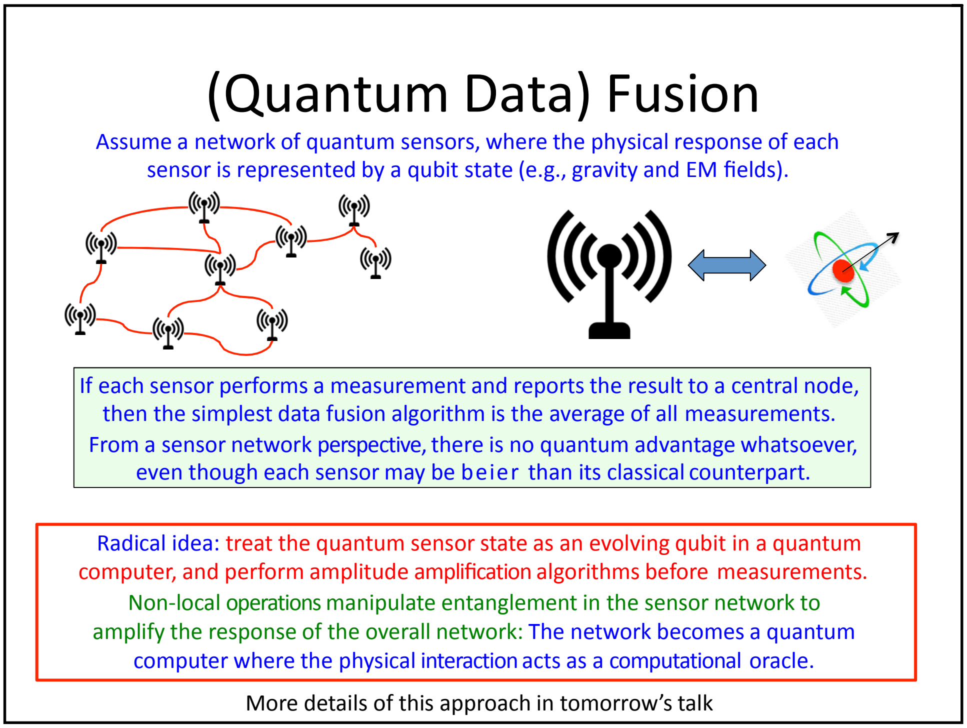
Lets assume N noiseless qubit sensors.

The precision to compute the rotation angle increases with N.



However, the sensitivity of a N-qubit system is the same as the sensitivity of a single qubit.

If we just process the bits produced by the sensors, then there is no sensitivity advantage whatsoever to having many quantum sensors measuring the same physical property



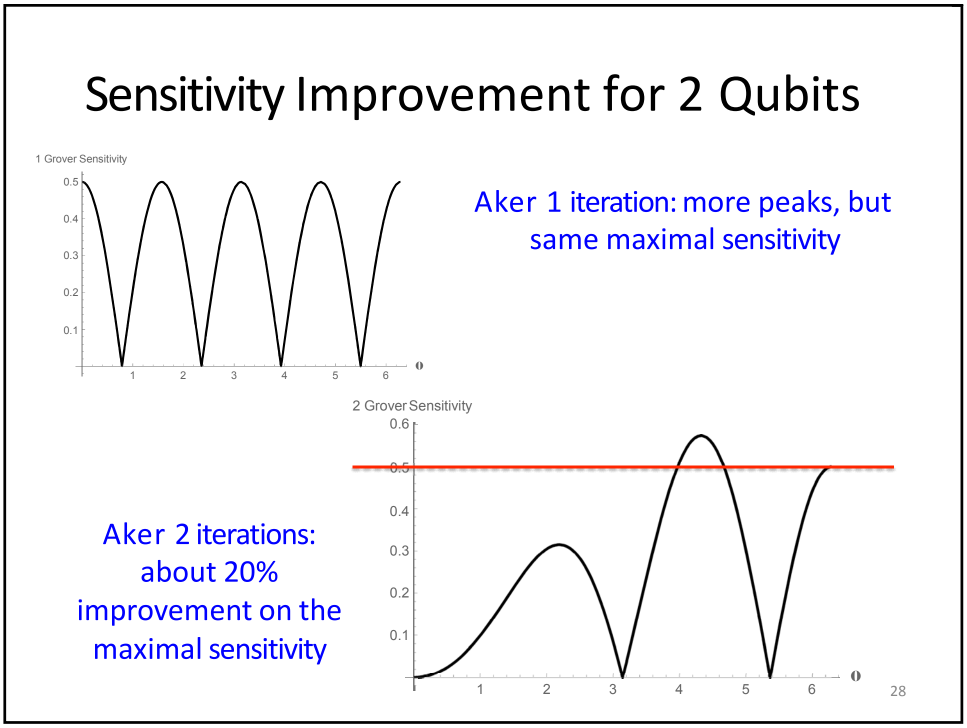
(Quantum Data) Fusion

Assume a network of quantum sensors, where the physical response of each sensor is represented by a qubit state (e.g., gravity and EM fields).

If each sensor performs a measurement and reports the result to a central node, then the simplest data fusion algorithm is the average of all measurements. From a sensor network perspective, there is no quantum advantage whatsoever, even though each sensor may be better than its classical counterpart.

Radical idea: treat the quantum sensor state as an evolving qubit in a quantum computer, and perform amplitude amplification algorithms before measurements. Non-local operations manipulate entanglement in the sensor network to amplify the response of the overall network: The network becomes a quantum computer where the physical interaction acts as a computational oracle.

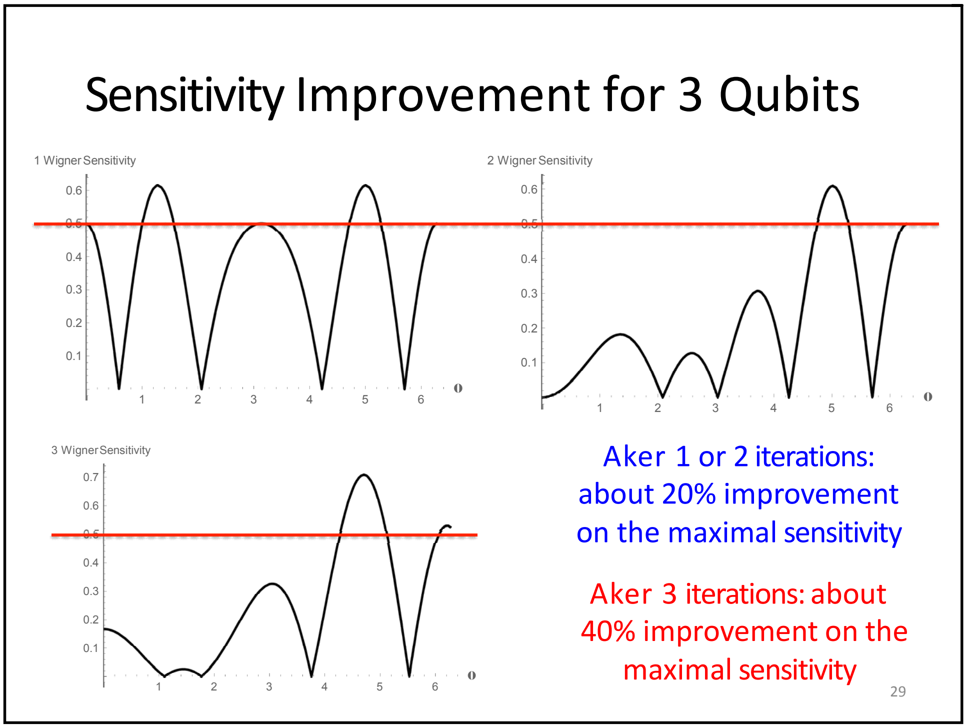
More details of this approach in tomorrow's talk



Sensitivity Improvement for 2 Qubits

After 1 iteration: more peaks, but same maximal sensitivity

After 2 iterations: about 20% improvement on the maximal sensitivity

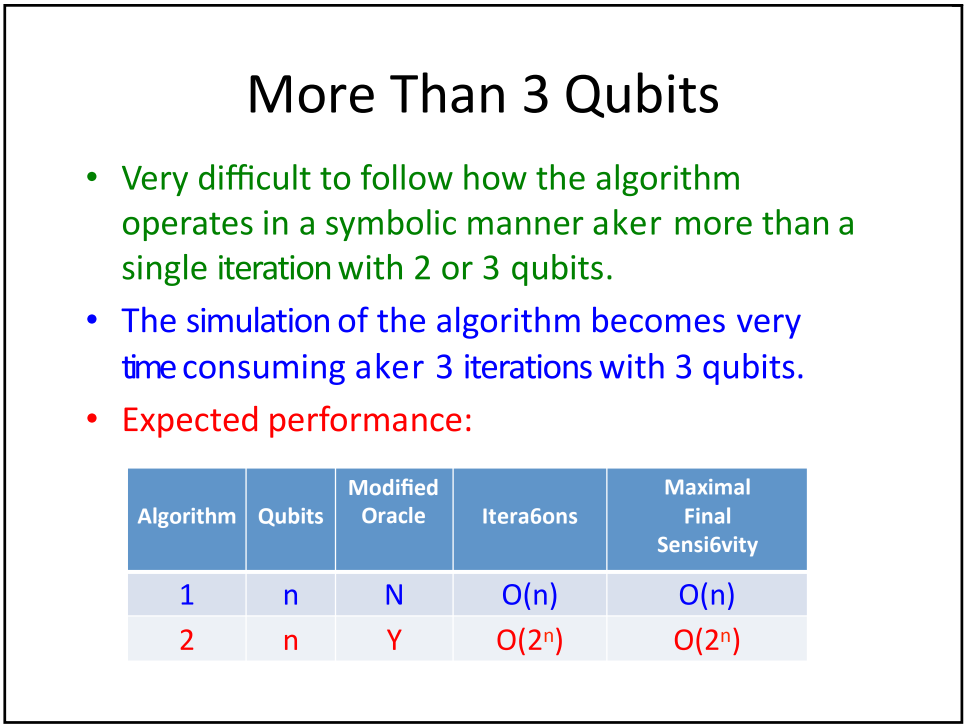


Sensitivity Improvement for 3 Qubits

Aker 1 or 2 iterations: about 20% improvement on the maximal sensitivity

Aker 3 iterations: about 40% improvement on the maximal sensitivity

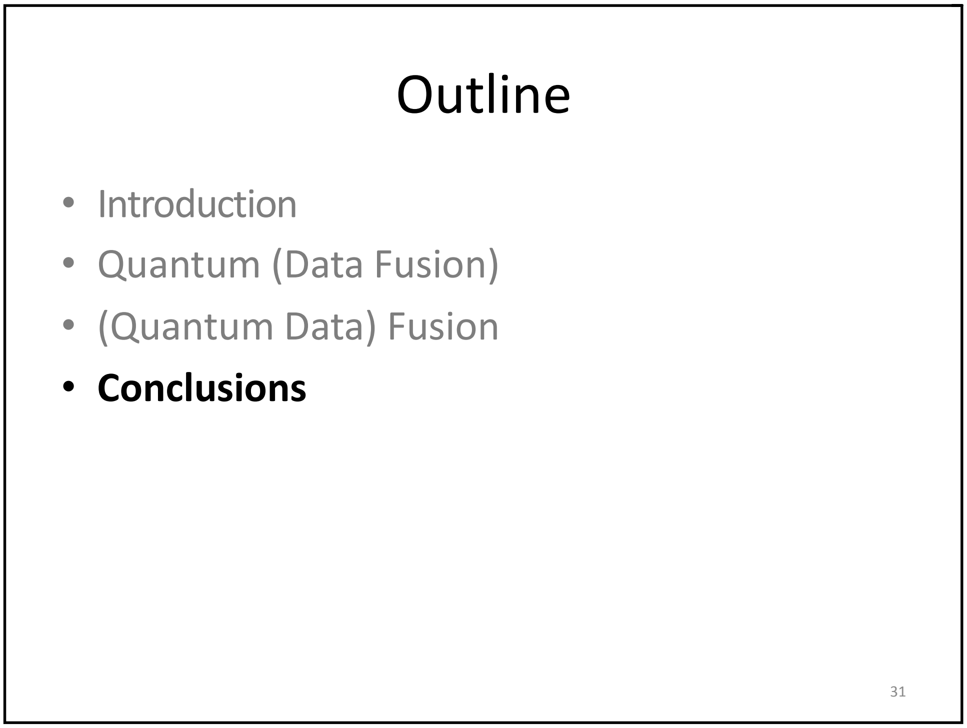
29



More Than 3 Qubits

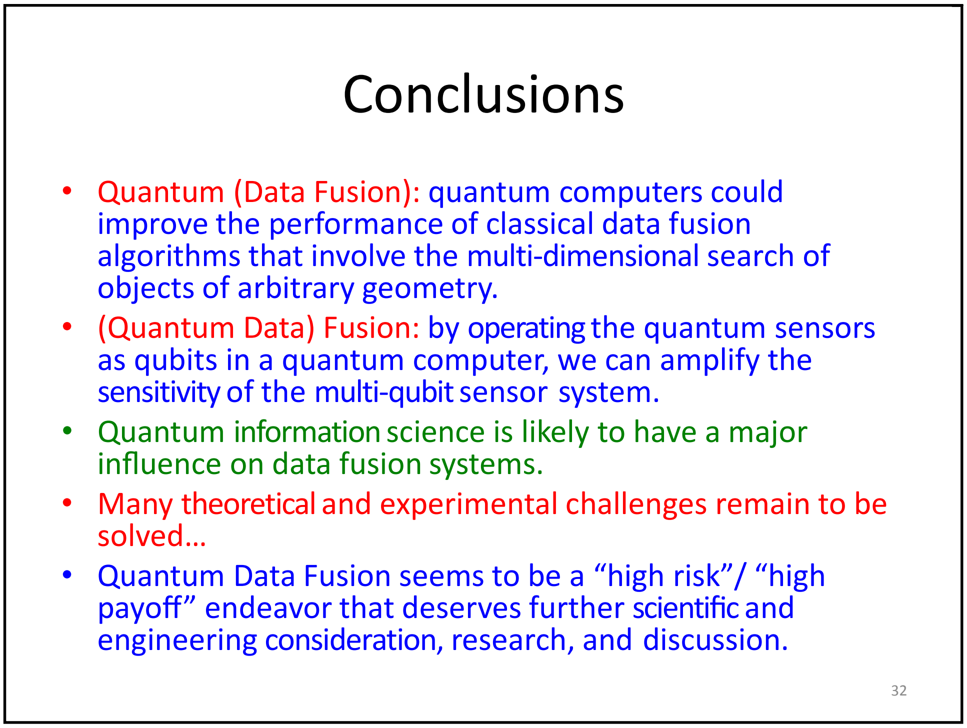
- Very difficult to follow how the algorithm operates in a symbolic manner aker more than a single iteration with 2 or 3 qubits.
- The simulation of the algorithm becomes very time consuming aker 3 iterations with 3 qubits.
- Expected performance:

Algorithm	Qubits	Modified Oracle	Itera6ons	Maximal Final Sensi6vity
1	n	N	O(n)	O(n)
2	n	Y	$O(2^n)$	$O(2^n)$



Outline

- Introduction
- Quantum (Data Fusion)
- (Quantum Data) Fusion
- **Conclusions**



Conclusions

- Quantum (Data Fusion): quantum computers could improve the performance of classical data fusion algorithms that involve the multi-dimensional search of objects of arbitrary geometry.
- (Quantum Data) Fusion: by operating the quantum sensors as qubits in a quantum computer, we can amplify the sensitivity of the multi-qubit sensor system.
- Quantum information science is likely to have a major influence on data fusion systems.
- Many theoretical and experimental challenges remain to be solved…
- Quantum Data Fusion seems to be a “high risk”/ “high payoff” endeavor that deserves further scientific and engineering consideration, research, and discussion.

Thank You

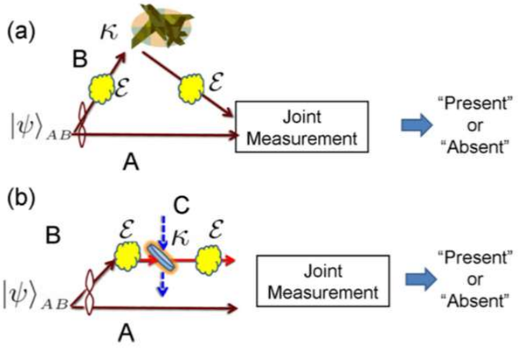
Towards Quantum Sensing with Optical Photons

Thoams Jennewein
Quantum Photonics Laboratory

University of Waterloo

Long term goals

- Quantum Enhanced Sensing
- Quantum Imaging
- Quantum LIDAR
- Quantum Secured Ranging



PHYSICAL REVIEW A **90**, 052308 (2014)

Quantum illumination in the presence of photon loss

ShengLi Zhang,[1,2] XuBo Zou,[1] JianHong Shi,[2] JianSheng Guo,[2] and GuangCan Guo[1]

[1] *Key Laboratory of Quantum Information, University of Science and Technology of China (CAS), Hefei 230026, China*

[2] *Zhengzhou Information Science and Technology Institute, Zhengzhou 450004, China*

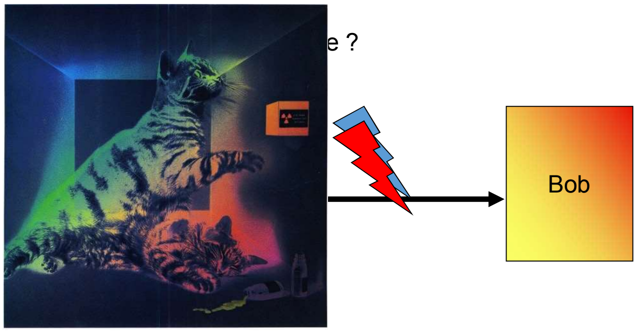
(Received 18 July 2014; revised manuscript received 11 September 2014; published 6 November 2014)

Quantum illumination can be used to detect the low-reflectivity target hidden in strong background noise.

Quantum Key Distribution

Close the loophole of key distribution:

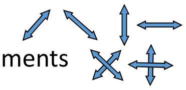
Only transmit single quanta of light per bit.



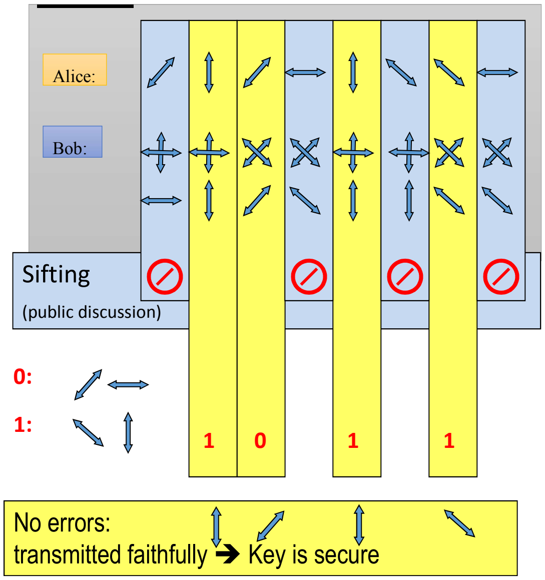
C. Bennett, G. Brassard, (1984). A. Ekert (1991)
Reviews: N. Gisin, et al., Rev. Mod. Phys (2002),
V. Scarani et al, Rev. Mod. Phys (2009)

Bennett Brassard Protocol – BB84

Quantum Protocol:
Create random key:
➔random signals
➔random measurements



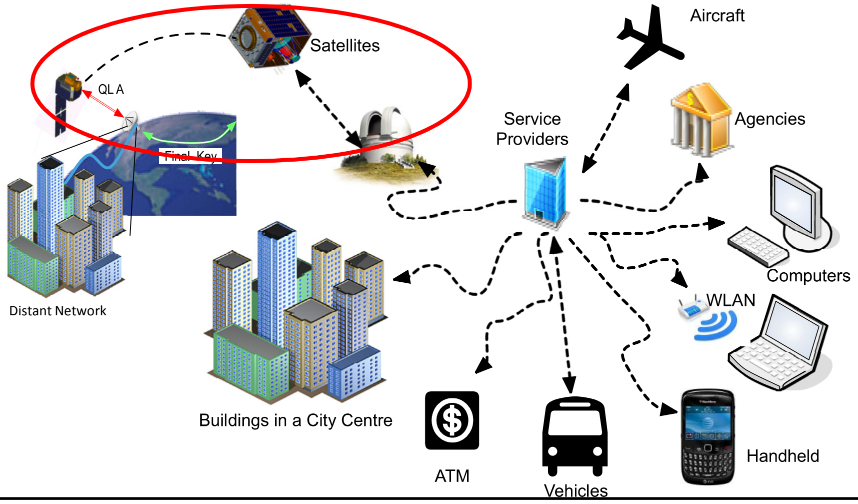
Classical Protocol:
Public discussion over faithful classical channel: distinguish **deterministic** from **random processes**



No errors:
transmitted faithfully ➔ Key is secure

Quantum Internet – the vision

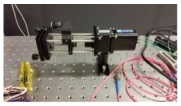
Qubit distribution,
Useful for secure communications, quantum computing, metrology



UNIVERSITY OF WATERLOO | IQC

Quantum Satellite Receiver Prototype

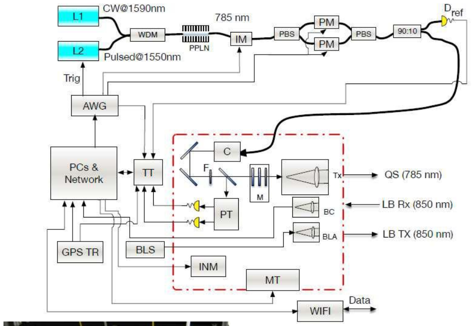
- Fine Pointing System
- Integrated Optical Assembly
- Control and Data Processing Unit
- Single Photon Detectors
- COTS Refractor Telescope
- COTS FLIR Pan-Tilt Motor



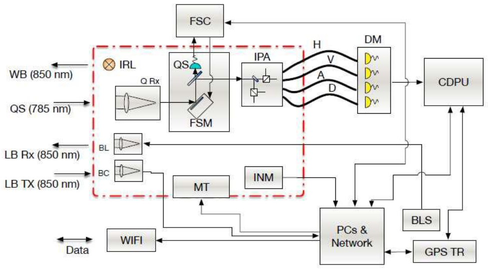
T. Jennewein, et al ADVANCES IN PHOTONICS OF QUANTUM COMPUTING, MEMORY, AND COMMUNICATION VII, volume 8997 of Proceedings of SPIE, 2014.
J-P Bourgoin, et al. A comprehensive design and performance analysis of low Earth orbit satellite quantum communication. NEW JOURNAL OF PHYSICS, 15, 2013.

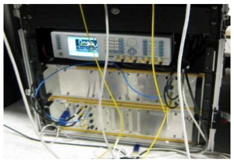
Airborne Quantum Key Distribution, September 2016

Transmitter: Smiths Falls



Receiver: Twin Otter Aircraft





Weak-coherent pulse source with
Randomized Polarization Modulated

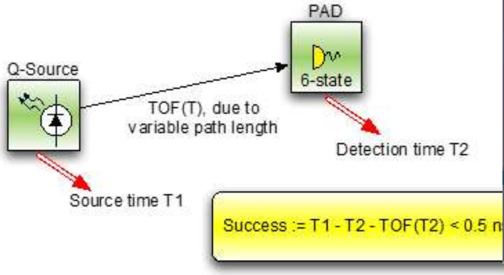
Airborne demonstration of a quantum key distribution receiver payload
Christopher J. Pugh, et al, arXiv:1612.06396 [quant-ph]

Flights

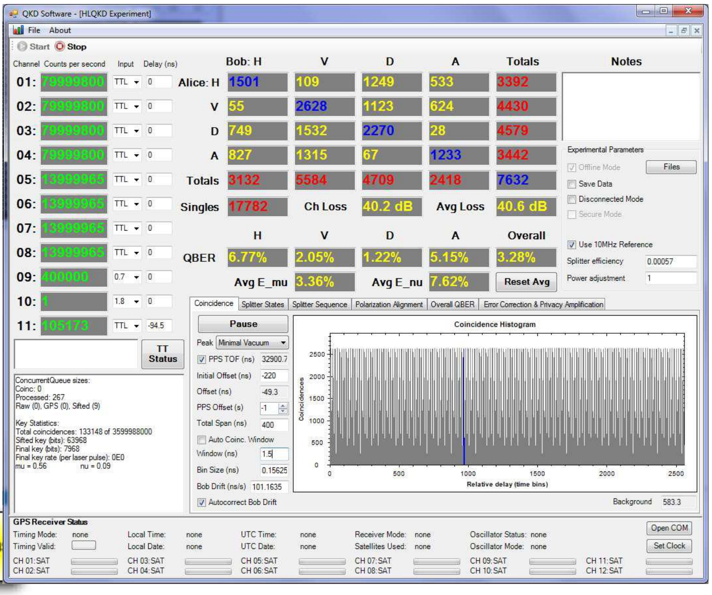
- Both Line and Arc passes
- 15 Passes, 7 successful
- Example Pass 7km Arc

Data analysis

- GPS locations for initial alignment
- Correction of clock drift
- QBER used to identify TOF
- Ranging



Success := T1 - T2 - TOF(T2) < 0.5 n


QKD Software - [HLQKD Experiment]

File About
Start Stop
TT Status
Pause
Reset Avg
Files
Open COM
Set Clock
Coincidence | Splitter States | Splitter Sequence | Polarization Alignment | Overall QBER | Error Correction & Privacy Amplification
Coincidence Histogram
Coincidences
2500
2000
1500
1000
500
0
0
500
1000
1500
2000
2500
Relative delay (time bins)

Channel	Counts per second	Input	Delay (ns)
01:	79999800	TTL	0
02:	79999800	TTL	0
03:	79999800	TTL	0
04:	79999800	TTL	0
05:	13999965	TTL	0
06:	13999965	TTL	0
07:	13999965	TTL	0
08:	13999965	TTL	0
09:	400000	0.7	0
10:	1	1.8	0
11:	105173	TTL	-94.5

	Bob: H	V	D	A	Totals
Alice: H	1501	109	1249	533	3392
V	55	2628	1123	624	4430
D	749	1532	2270	28	4579
A	827	1315	67	1233	3442
Totals	3132	5584	4709	2418	7632
Singles	17782	Ch Loss	40.2 dB	Avg Loss	40.6 dB

	H	V	D	A	Overall
QBER	6.77%	2.05%	1.22%	5.15%	3.28%
	Avg E_mu	3.36%	Avg E_nu	7.62%	

Notes

Experimental Parameters
☑ Offline Mode
☐ Save Data
☐ Disconnected Mode
☐ Secure Mode
☑ Use 10MHz Reference
Splitter efficiency 0.00057
Power adjustment 1

```
ConcurrentQueue sizes:
Coinc: 0
Processed: 267
Raw (0), GPS (0), Sifted (9)

Key Statistics:
Total coincidences: 133148 of 3599988000
Sifted key (bits): 63968
Final key (bits): 7968
Final key rate (per laser pulse): 0E0
mu = 0.56          nu = 0.09
```

Peak Minimal Vacuum
☑ PPS TOF (ns) 32900.7
Initial Offset (ns) -220
Offset (ns) -49.3
PPS Offset (s) -1
Total Span (ns) 400
☐ Auto Coinc. Window
Window (ns) 1.5
Bin Size (ns) 0.15625
Bob Drift (ns/s) 101.1635
☑ Autocorrect Bob Drift
Background 583.3

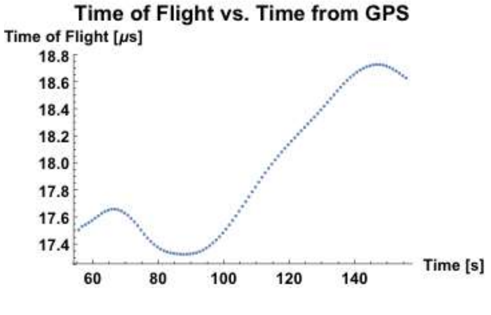
GPS Receiver Status

Timing Mode:	none	Local Time:	none	UTC Time:	none	Receiver Mode:	none	Oscillator Status:	none
Timing Valid:	☐	Local Date:	none	UTC Date:	none	Satellites Used:	none	Oscillator Mode:	none

CH 01: SAT
CH 02: SAT
CH 03: SAT
CH 04: SAT
CH 05: SAT
CH 06: SAT
CH 07: SAT
CH 08: SAT
CH 09: SAT
CH 10: SAT
CH 11: SAT
CH 12: SAT

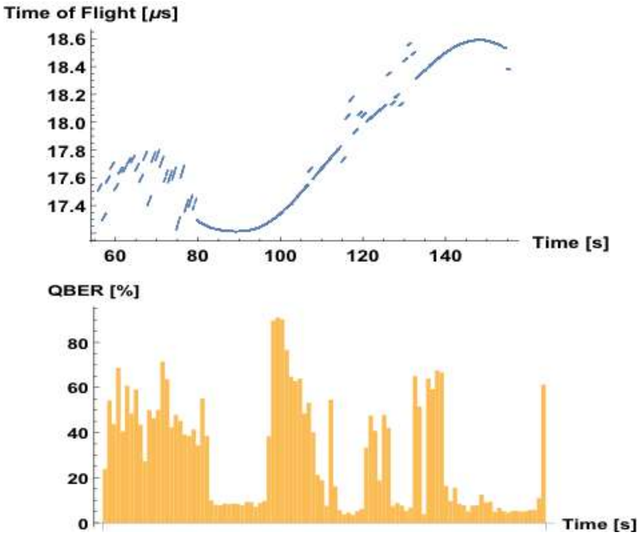
Ranging

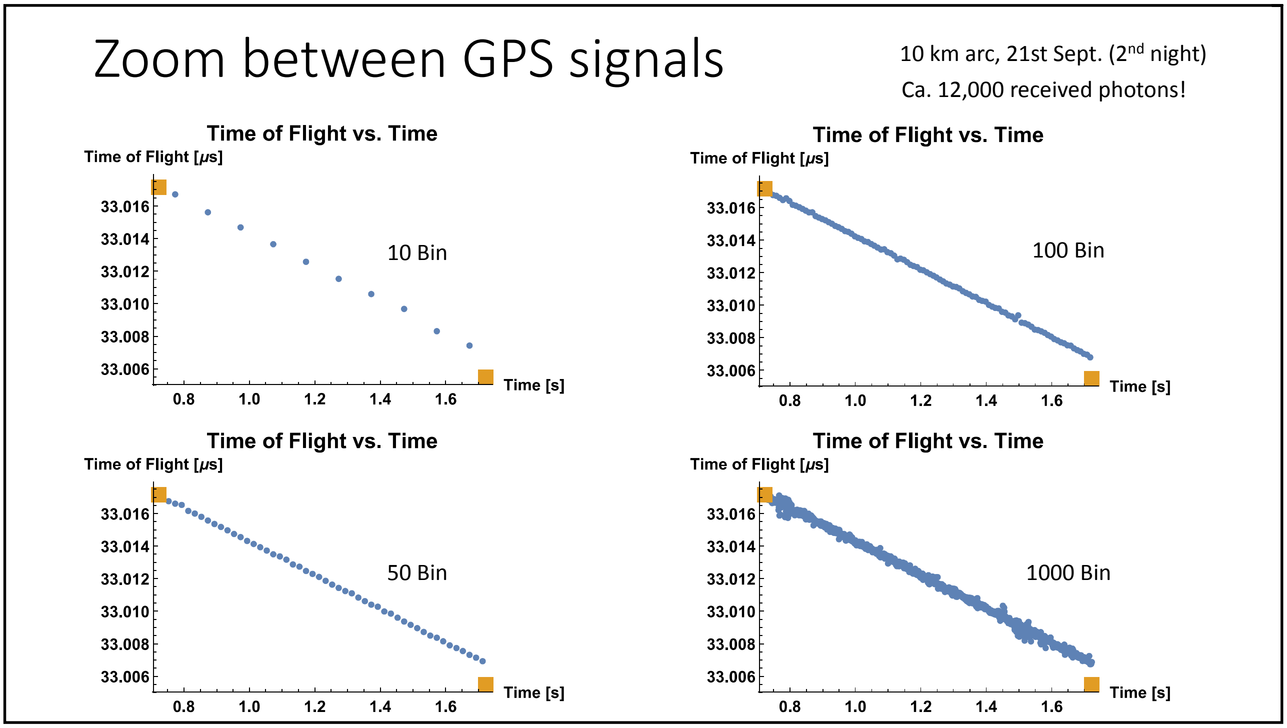
- Quantum Signal Analysis
- Intervals of 1/1000 s or even shorter



From 1 Hz GPS locations

5km arc, 20th September (1st night)

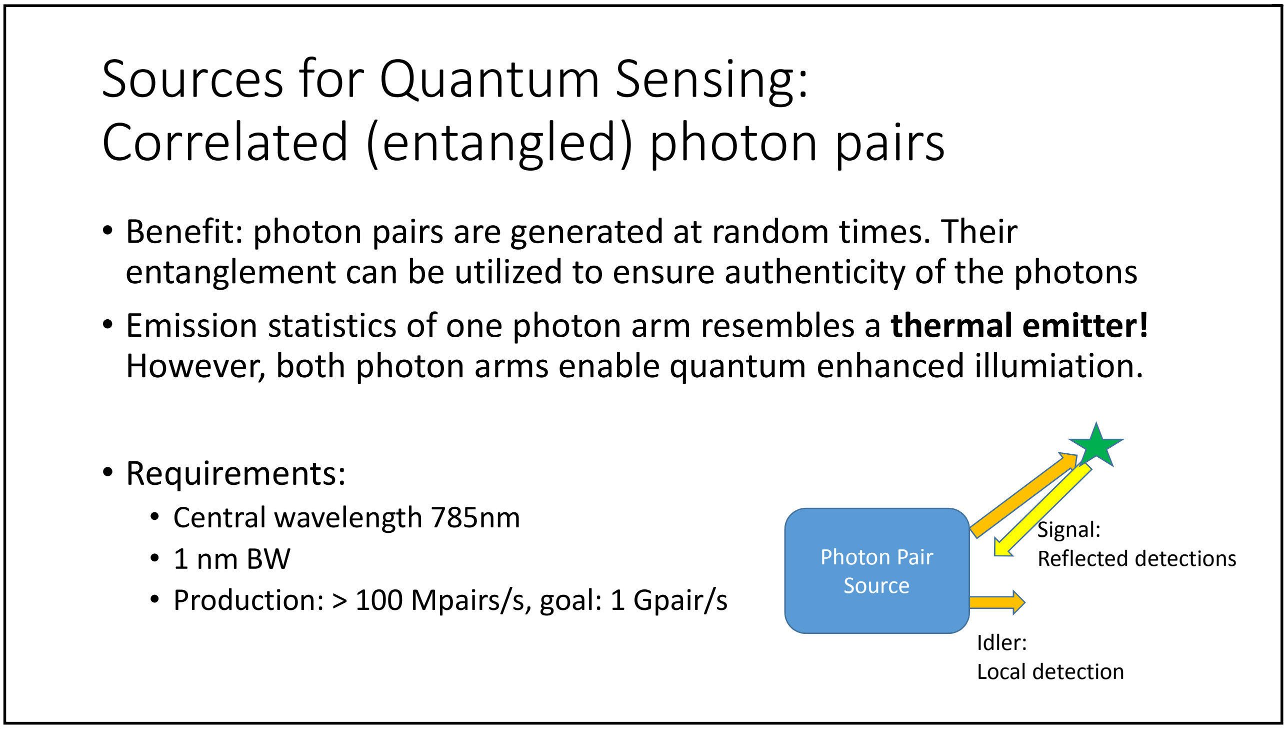




Zoom between GPS signals

10 km arc, 21st Sept. (2^{nd} night)

Ca. 12,000 received photons!



Sources for Quantum Sensing: Correlated (entangled) photon pairs

- Benefit: photon pairs are generated at random times. Their entanglement can be utilized to ensure authenticity of the photons
- Emission statistics of one photon arm resembles a **thermal emitter!** However, both photon arms enable quantum enhanced illumiation.
- Requirements:
  - Central wavelength 785nm
  - 1 nm BW
  - Production: > 100 Mpairs/s, goal: 1 Gpair/s

Photon Pair Source

Signal:
Reflected detections

Idler:
Local detection

Creating Photon Entanglement

- Parametric Conversion in |2 or |3
  - Optical crystal, fiber, atoms,…

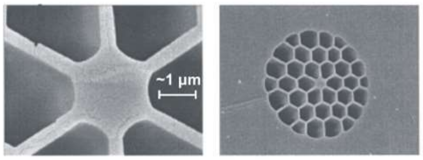


Fig. 1. Electron microscope image of the PCF used with core diameter d=2 µm, λ_0 = 715 nm

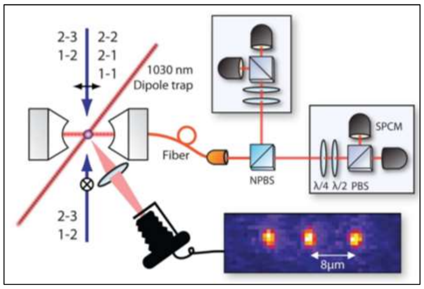
J. Rarity group, 2005

- Quantum Dots

A. Shields group, Nature, 439, 179 (2006)

- Atoms

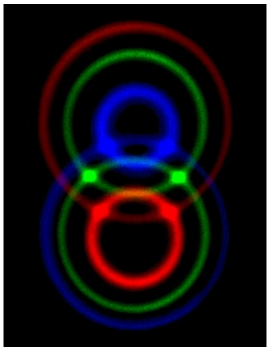
G. Rempe group, PRL 102, 030501 (2009)



13

Spontaneous Prametric Downconversion

- Best source presently: spontaneous parametric down conversion (SPDC)*



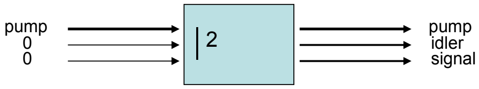
P. Kwiat et al. PRL 75, 4337, (1995):

Phasematching: $\omega_p = \omega_s + \omega_i \quad \vec{k_p} = \vec{k_s} + \vec{k_i},$

Hamiltonian: $\mathcal{H} = \varepsilon_0 \int_V d^3\mathbf{r}\, \chi^{(2)} E_p^{(+)} E_s^{(-)} E_i^{(-)} + \text{H.c.},$

SPDC state (1st order):

$$|\psi(\omega_i,\omega_s)\rangle = \int d\omega_i d\omega_s\, \delta(\omega_p - \omega_i - \omega_s)\text{sinc}\left(\frac{L\Delta\mathbf{k}}{2}\right) a_{i,H}^{\dagger}(\omega_i) a_{s,V}^{\dagger}(\omega_s)\, |0\rangle\, .$$



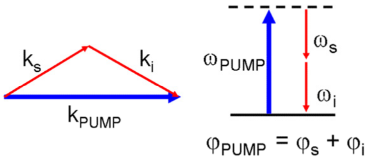
nonlinear optical medium:
BBO, PPKTP, PPLN ...

* A. White (insp. W. Churchill): SPDC is the worst source of photon pairs, except for all others.

Crystal materials and phase matching

- Proven optically nonlinear materials include:
  - BBO, PPKTP, PPLN, PPLT, PPLN:Mg
- Configuration (type I or type II):
  - Type I allows to access to the highest nonlinear tensor coefficient, but:
    - Need shorter poling periods wrt type II (order of 3 – 4 µm)
    - need two 90º crossed crystals or Sagnac cavity geometry to achieve polarisation entanglement
    - of-degeneracy scheme to reduce bandwidth (2 nm less over >10 nm at 770/845 nm for a 15 mm long PPKTP)
- Crystal sensitivity to effects:
  - Photorefractive effect
  - Gray-tracking
  - Multiphoton absorption

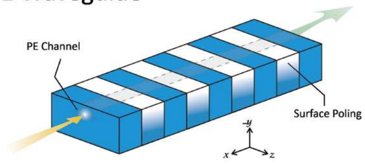
PPKTP (Raicol, Israel)



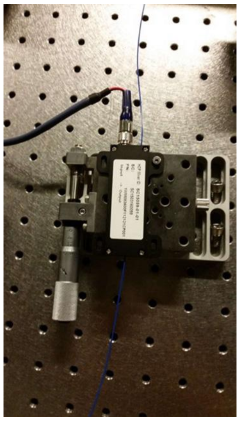
Recent Advances, towards SPDC with Giga-pairs/second emission rates

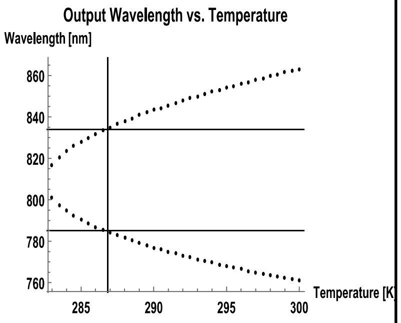
- Utilize Waveguides in PP-LN
- Fiber pigtailed
- Thermalized

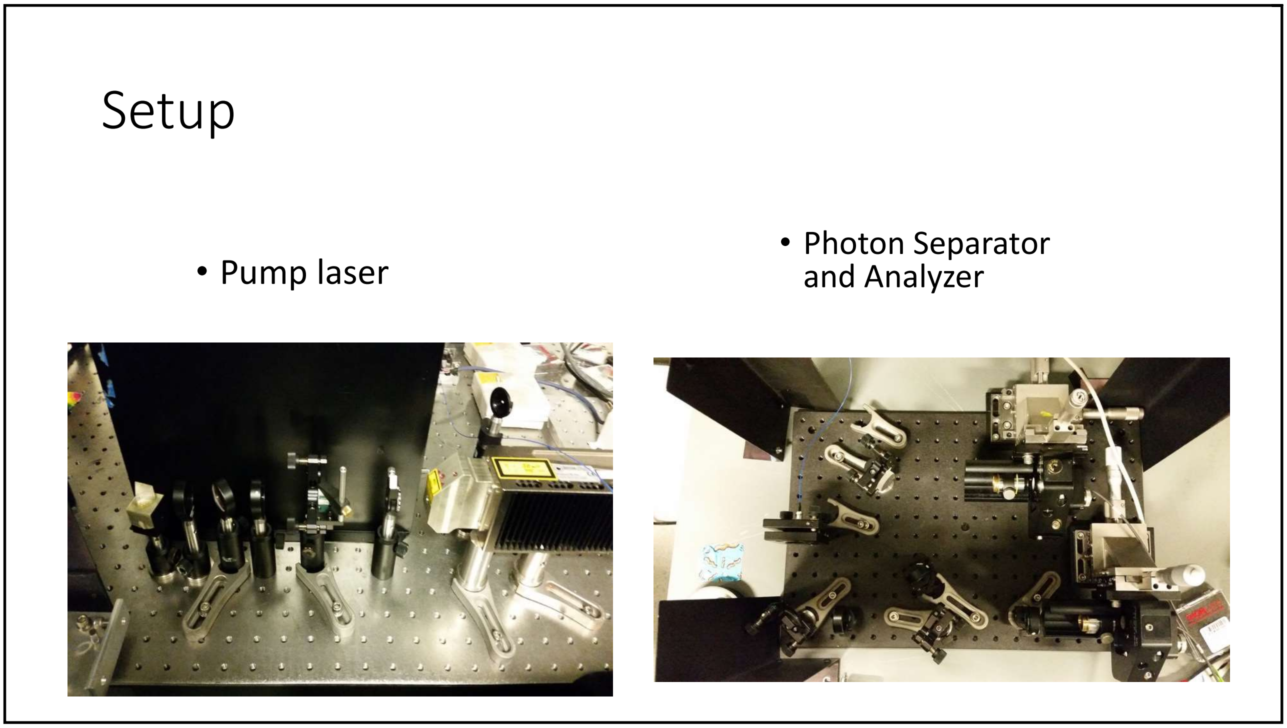
PE Waveguide



From HCPhotonics

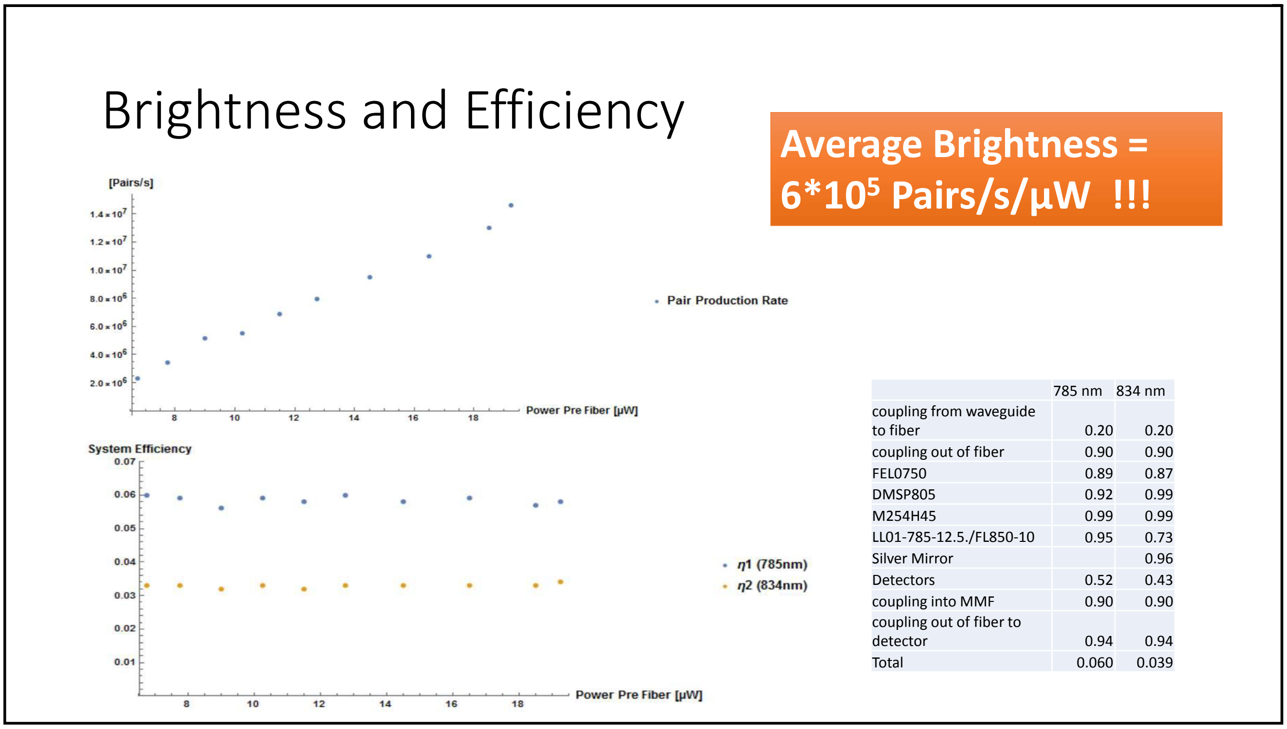






Setup

- Pump laser
- Photon Separator and Analyzer



Brightness and Efficiency

Average Brightness = $6*10^5$ Pairs/s/μW !!!

	785 nm	834 nm
coupling from waveguide to fiber	0.20	0.20
coupling out of fiber	0.90	0.90
FEL0750	0.89	0.87
DMSP805	0.92	0.99
M254H45	0.99	0.99
LL01-785-12.5./FL850-10	0.95	0.73
Silver Mirror		0.96
Detectors	0.52	0.43
coupling into MMF	0.90	0.90
coupling out of fiber to detector	0.94	0.94
Total	0.060	0.039

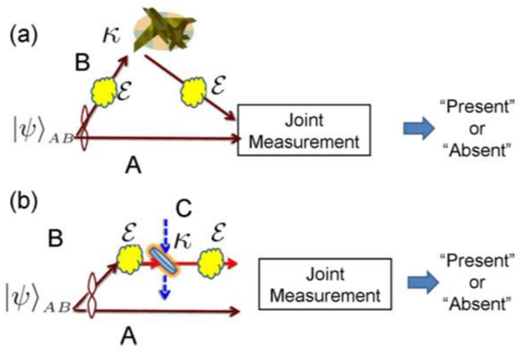
Conclusions:
Quantum Communication Receiver demonstrated on Aircraft, was used for ranging at the quantum level

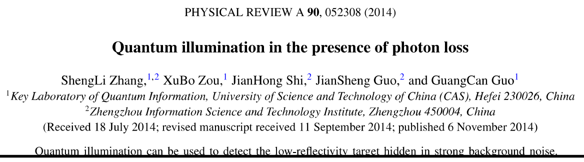
- Received photons: ca. 10 Kphotons/s, ca. 2.5 fW
- Can be reduced to about 1000 pts/second
- Quantum Source, emits 200 Mphotons/s, ca. 50 pW
- Novel Entangled pair sources reached the emission rates required for quantum sensing applications

Airborne demonstration of a quantum key distribution receiver payload
Christopher J. Pugh, et al, arXiv:1612.06396 [quant-ph]

Recent advanced on quantum photons bring the long term goals closer

- Quantum Enhanced Sensing
- Quantum Imaging
- Quantum LIDAR
- Quantum Secured Ranging

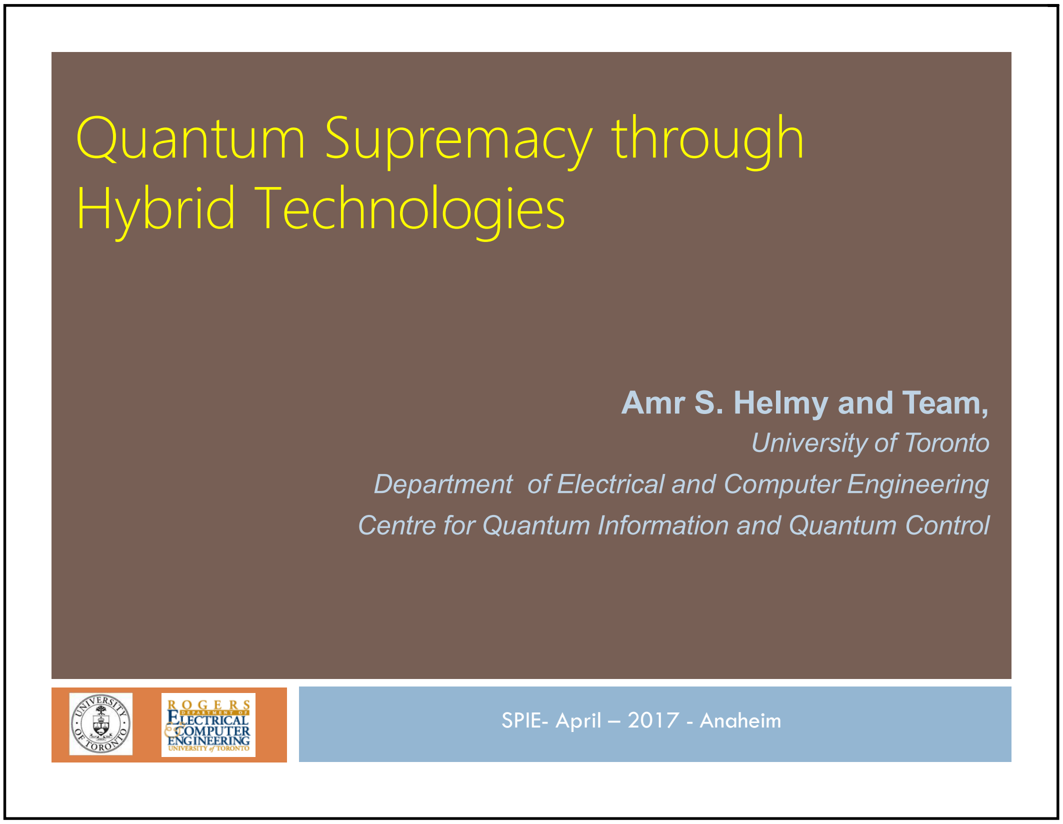



PHYSICAL REVIEW A **90**, 052308 (2014)

Quantum illumination in the presence of photon loss

ShengLi Zhang,[1,2] XuBo Zou,[1] JianHong Shi,[2] JianSheng Guo,[2] and GuangCan Guo[1]
[1] *Key Laboratory of Quantum Information, University of Science and Technology of China (CAS), Hefei 230026, China*
[2] *Zhengzhou Information Science and Technology Institute, Zhengzhou 450004, China*
(Received 18 July 2014; revised manuscript received 11 September 2014; published 6 November 2014)

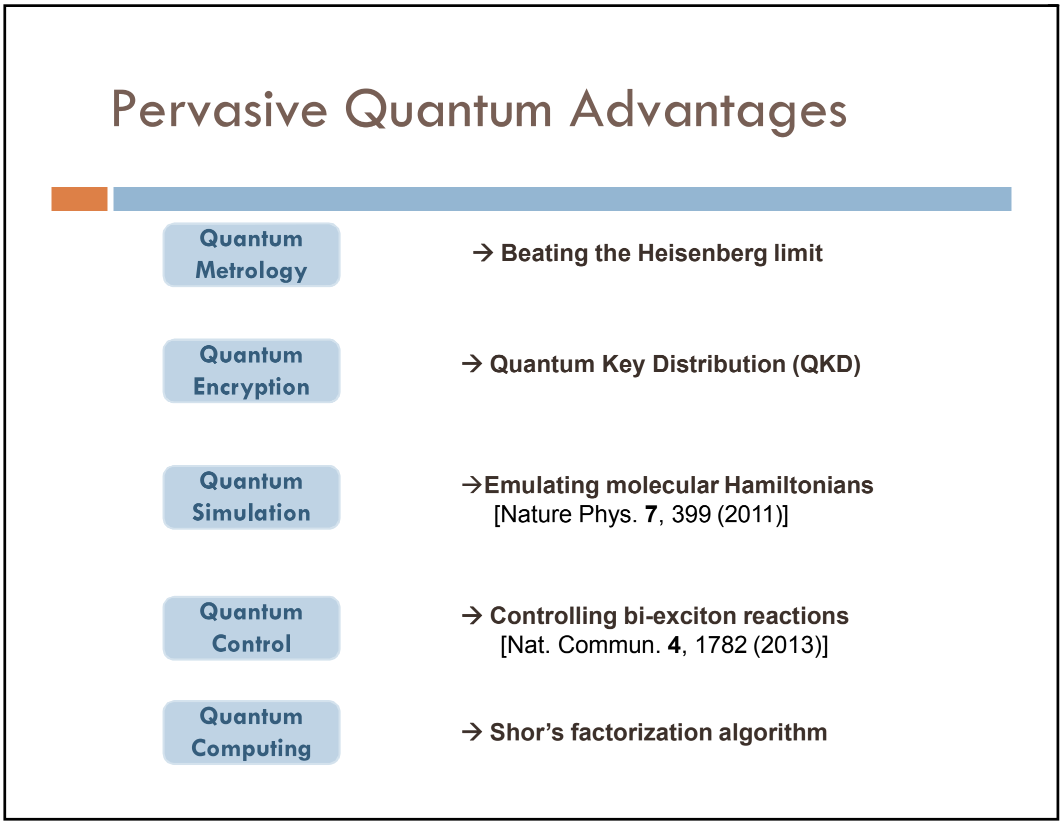
Quantum illumination can be used to detect the low-reflectivity target hidden in strong background noise.



Quantum Supremacy through Hybrid Technologies

Amr S. Helmy and Team,
University of Toronto
Department of Electrical and Computer Engineering
Centre for Quantum Information and Quantum Control

SPIE- April – 2017 - Anaheim



Pervasive Quantum Advantages

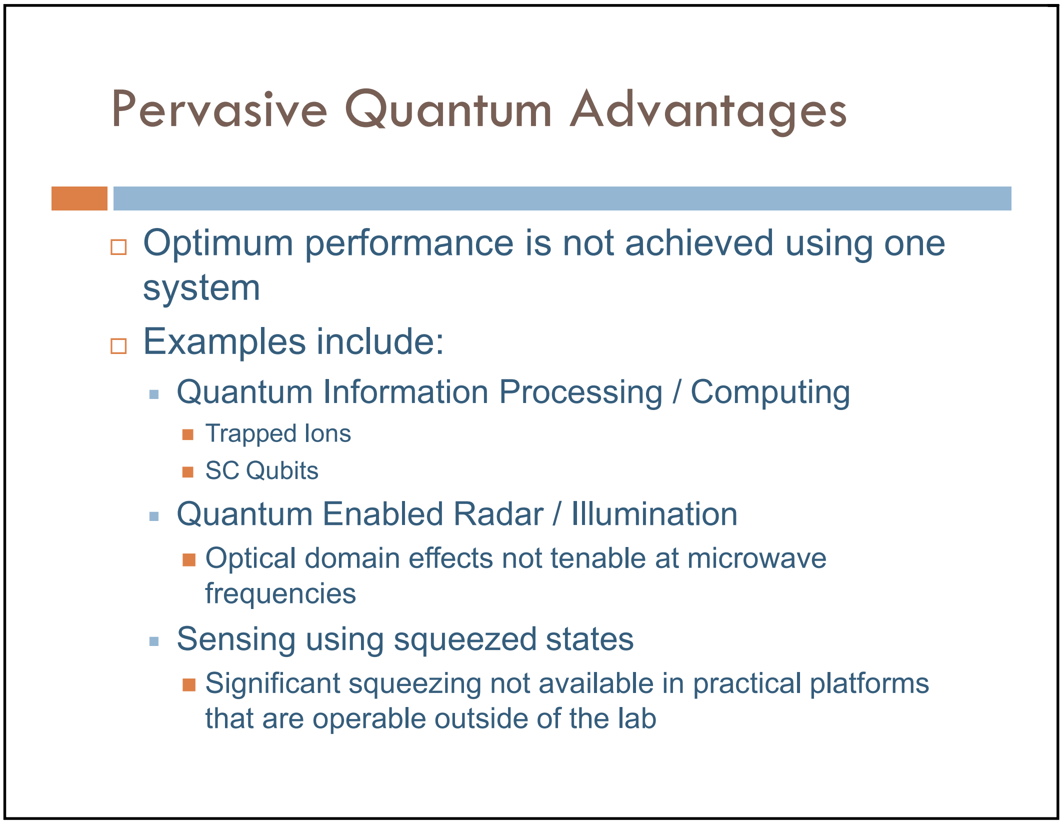
Quantum Metrology → **Beating the Heisenberg limit**

Quantum Encryption → **Quantum Key Distribution (QKD)**

Quantum Simulation →**Emulating molecular Hamiltonians**
[Nature Phys. **7**, 399 (2011)]

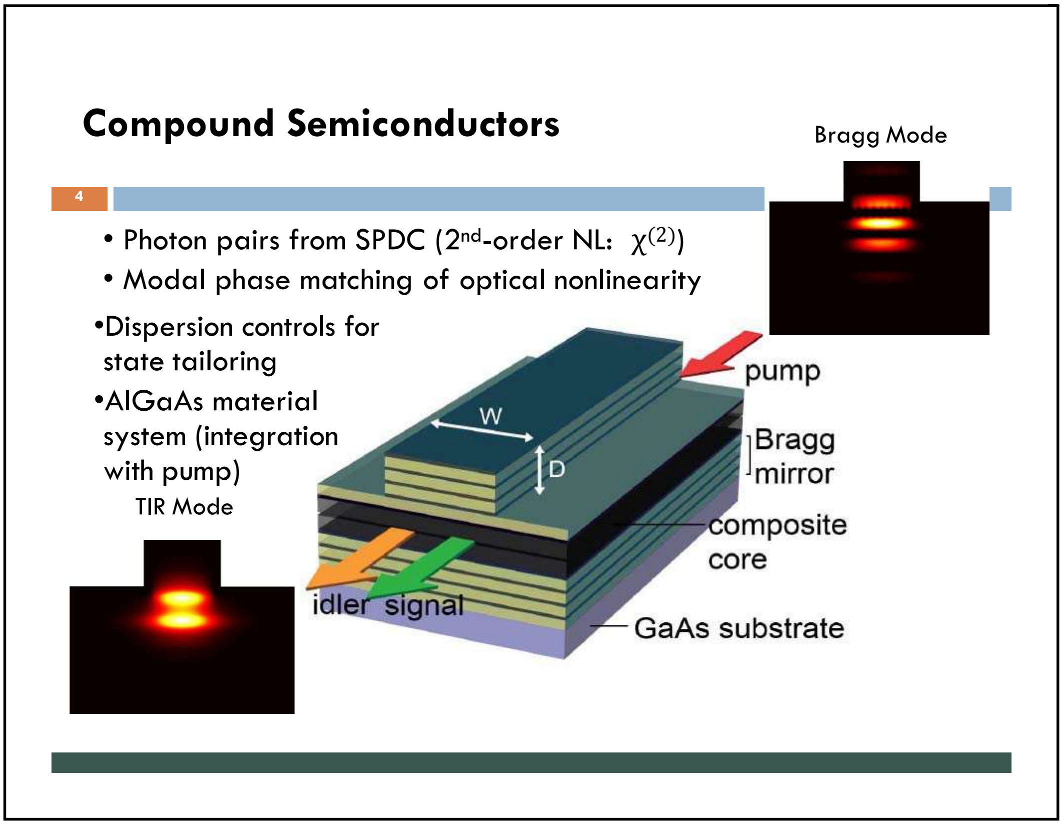
Quantum Control → **Controlling bi-exciton reactions**
[Nat. Commun. **4**, 1782 (2013)]

Quantum Computing → **Shor's factorization algorithm**



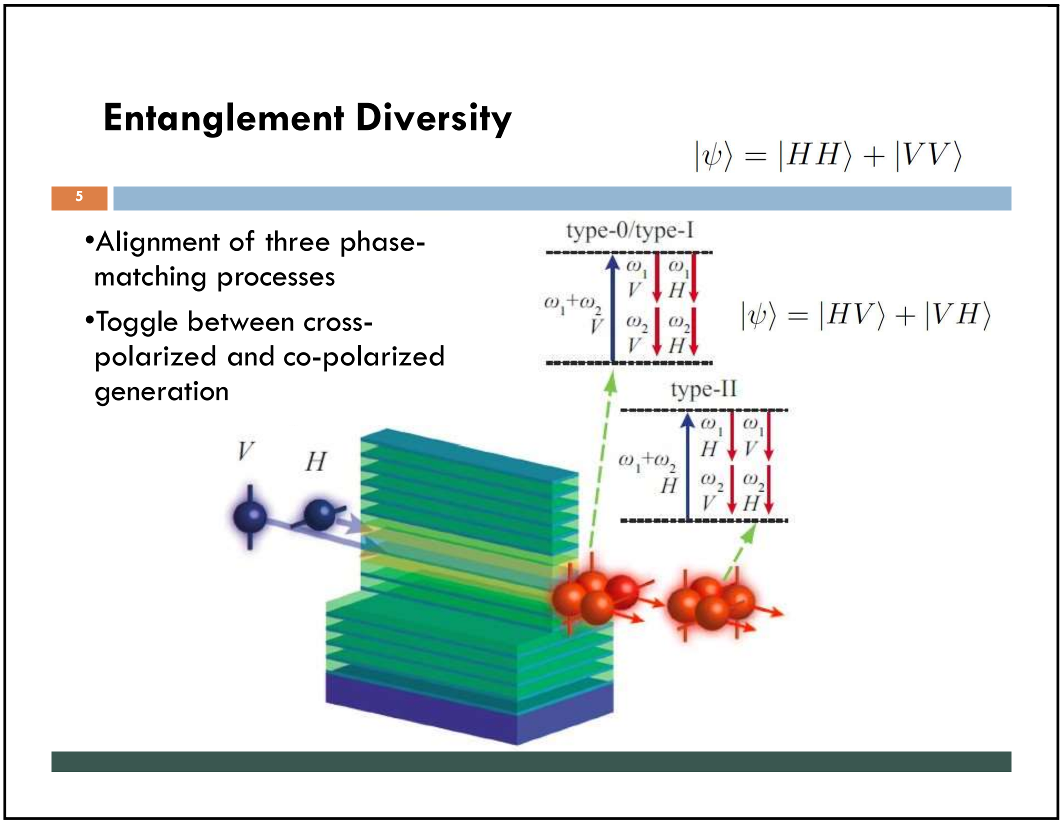
Pervasive Quantum Advantages

- Optimum performance is not achieved using one system
- Examples include:
  - Quantum Information Processing / Computing
    - Trapped Ions
    - SC Qubits
  - Quantum Enabled Radar / Illumination
    - Optical domain effects not tenable at microwave frequencies
  - Sensing using squeezed states
    - Significant squeezing not available in practical platforms that are operable outside of the lab



Compound Semiconductors

- Photon pairs from SPDC (2nd-order NL: $\chi^{(2)}$)
- Modal phase matching of optical nonlinearity
- Dispersion controls for state tailoring
- AlGaAs material system (integration with pump)



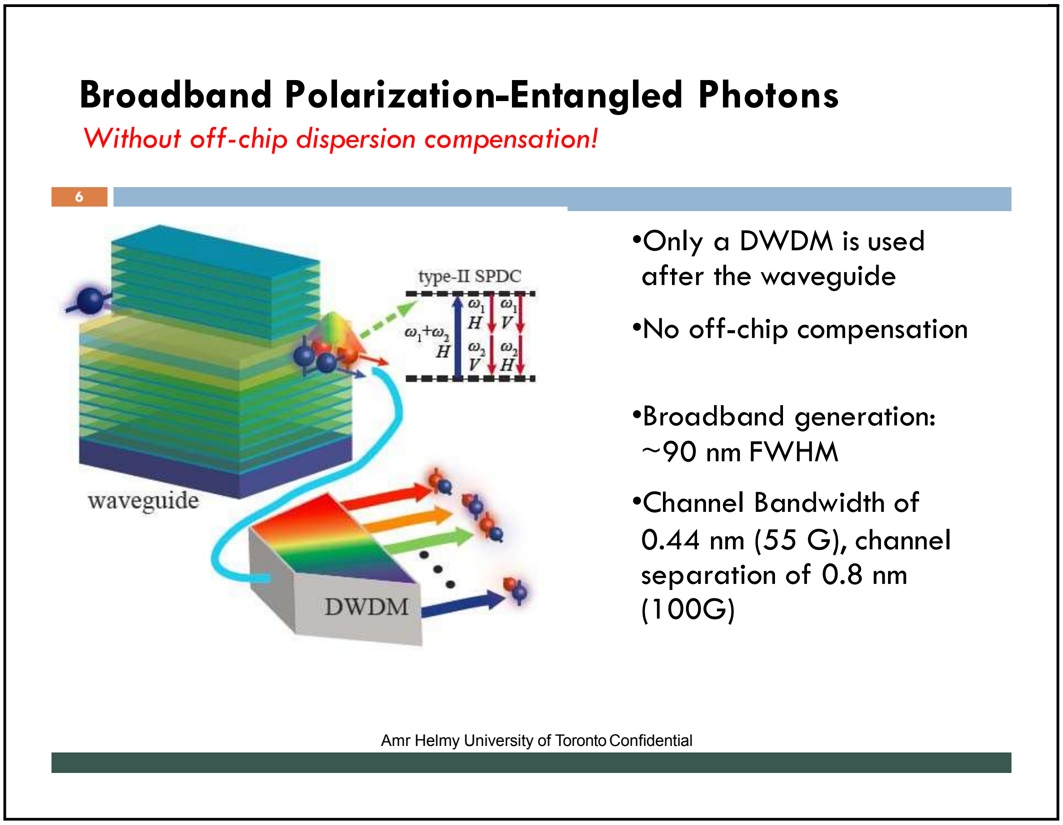
Entanglement Diversity

$|\psi\rangle = |HH\rangle + |VV\rangle$

5

- Alignment of three phase-matching processes
- Toggle between cross-polarized and co-polarized generation

$|\psi\rangle = |HV\rangle + |VH\rangle$



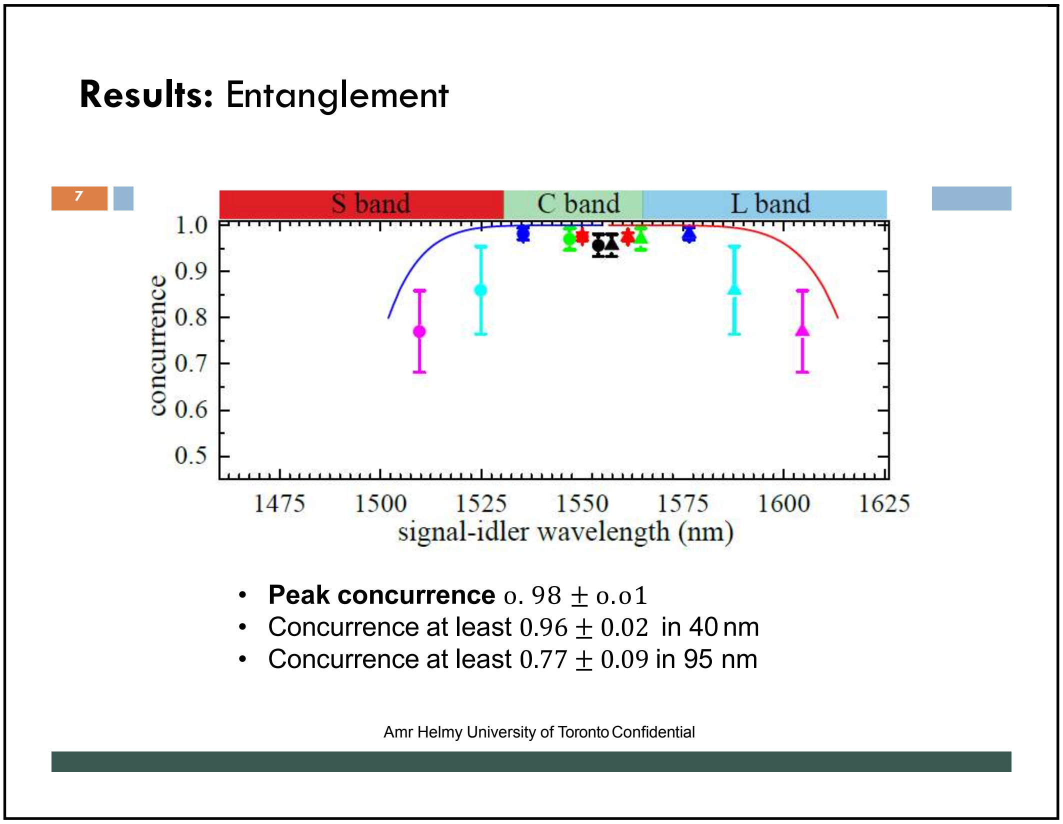
Broadband Polarization-Entangled Photons

Without off-chip dispersion compensation!

6

- Only a DWDM is used after the waveguide
- No off-chip compensation
- Broadband generation: ~90 nm FWHM
- Channel Bandwidth of 0.44 nm (55 G), channel separation of 0.8 nm (100G)

Amr Helmy University of Toronto Confidential

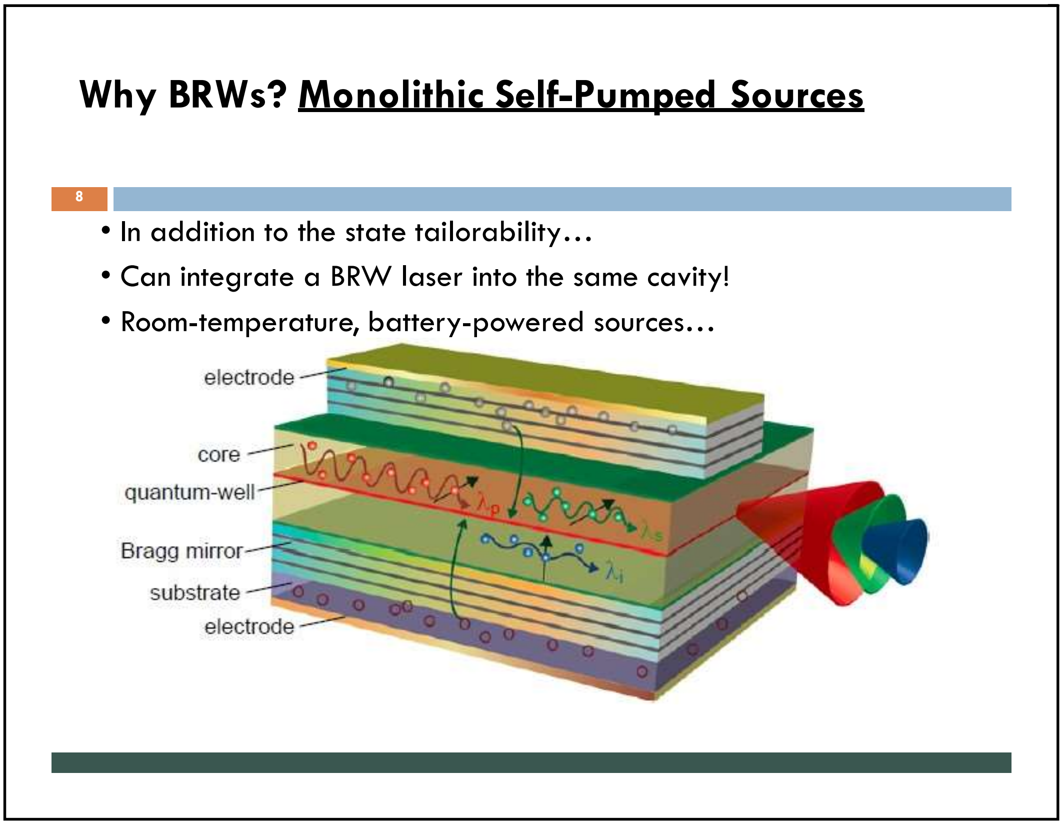


Results: Entanglement

7

- **Peak concurrence** 0.98 ± 0.01
- Concurrence at least 0.96 ± 0.02 in 40 nm
- Concurrence at least 0.77 ± 0.09 in 95 nm

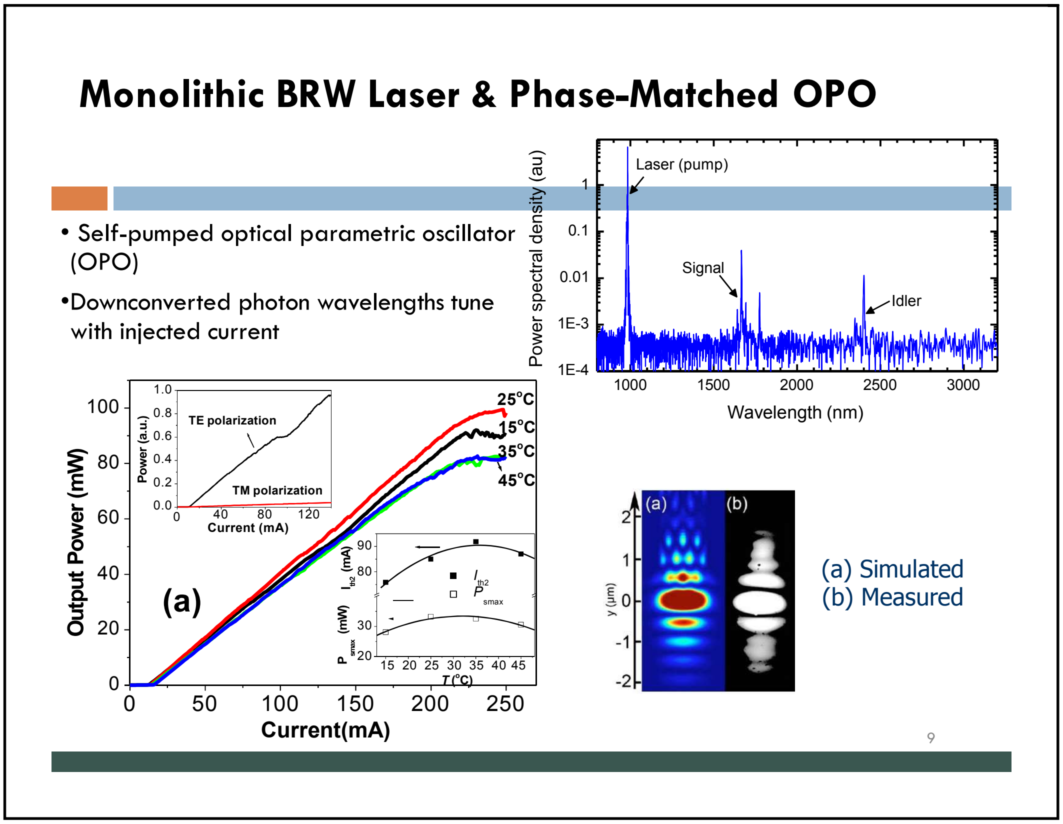
Amr Helmy University of Toronto Confidential



Why BRWs? Monolithic Self-Pumped Sources

8

- In addition to the state tailorability…
- Can integrate a BRW laser into the same cavity!
- Room-temperature, battery-powered sources…

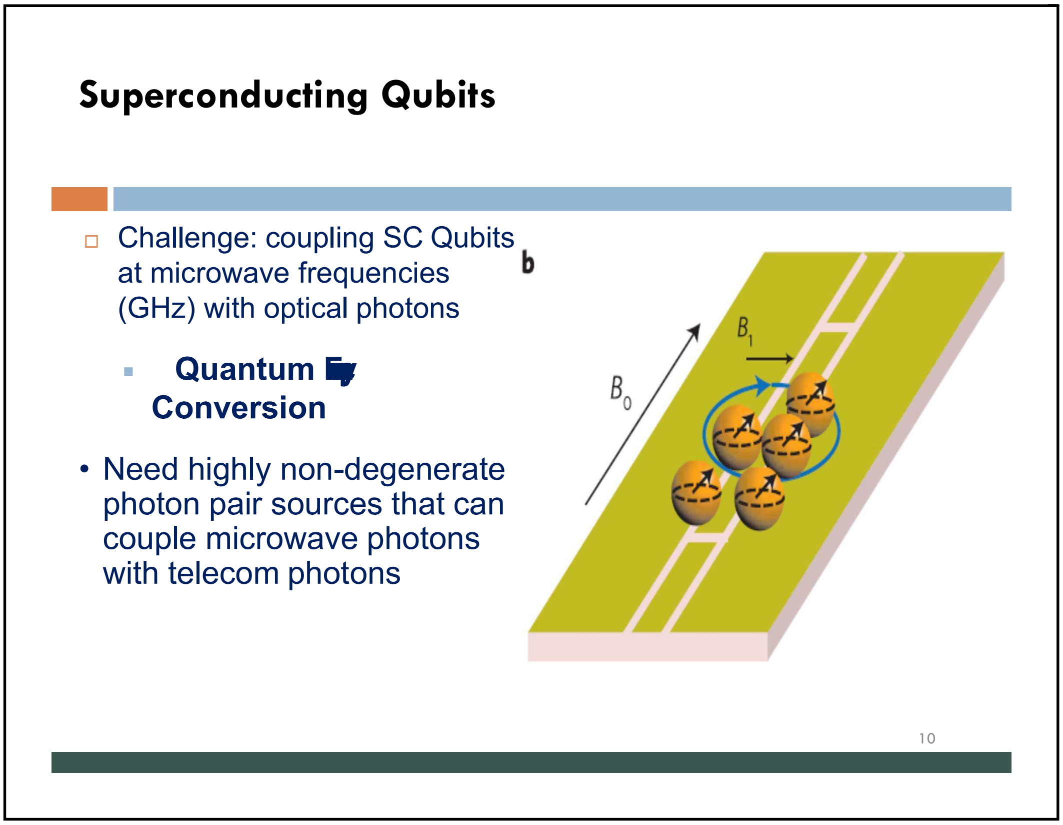


Monolithic BRW Laser & Phase-Matched OPO

- Self-pumped optical parametric oscillator (OPO)
- Downconverted photon wavelengths tune with injected current

(a) Simulated
(b) Measured

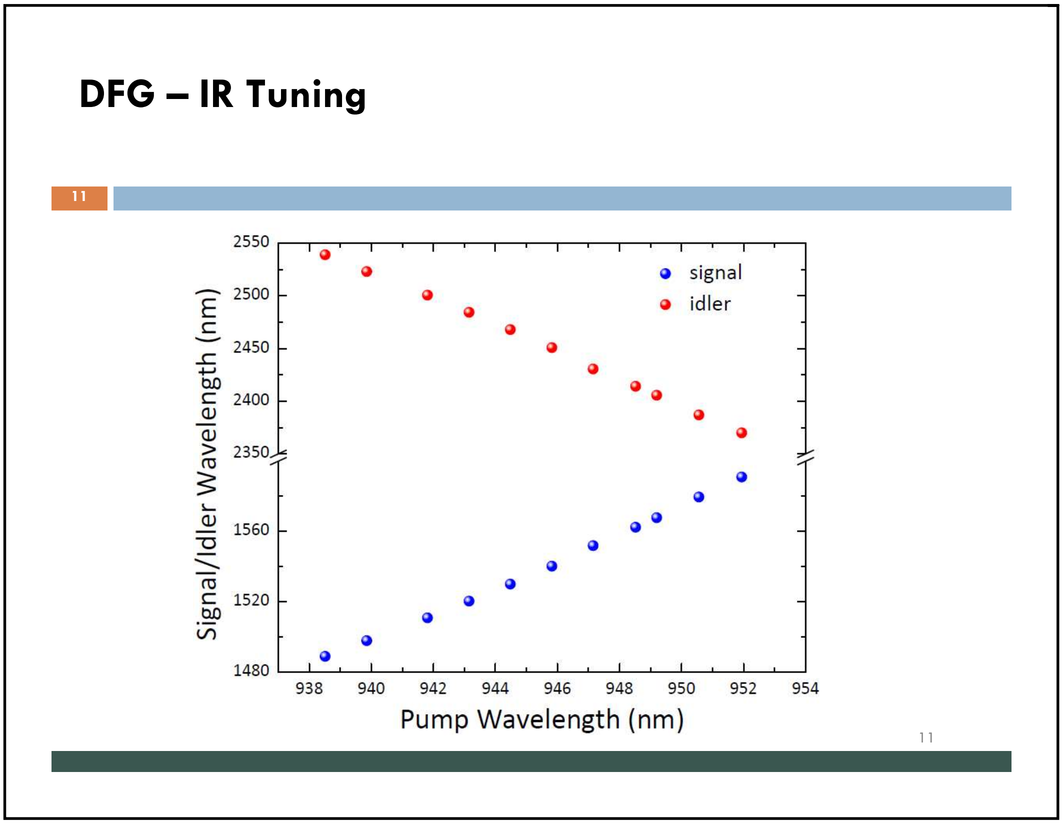
9



Superconducting Qubits

- Challenge: coupling SC Qubits at microwave frequencies (GHz) with optical photons
  - **Quantum ⮚ Conversion**
- Need highly non-degenerate photon pair sources that can couple microwave photons with telecom photons

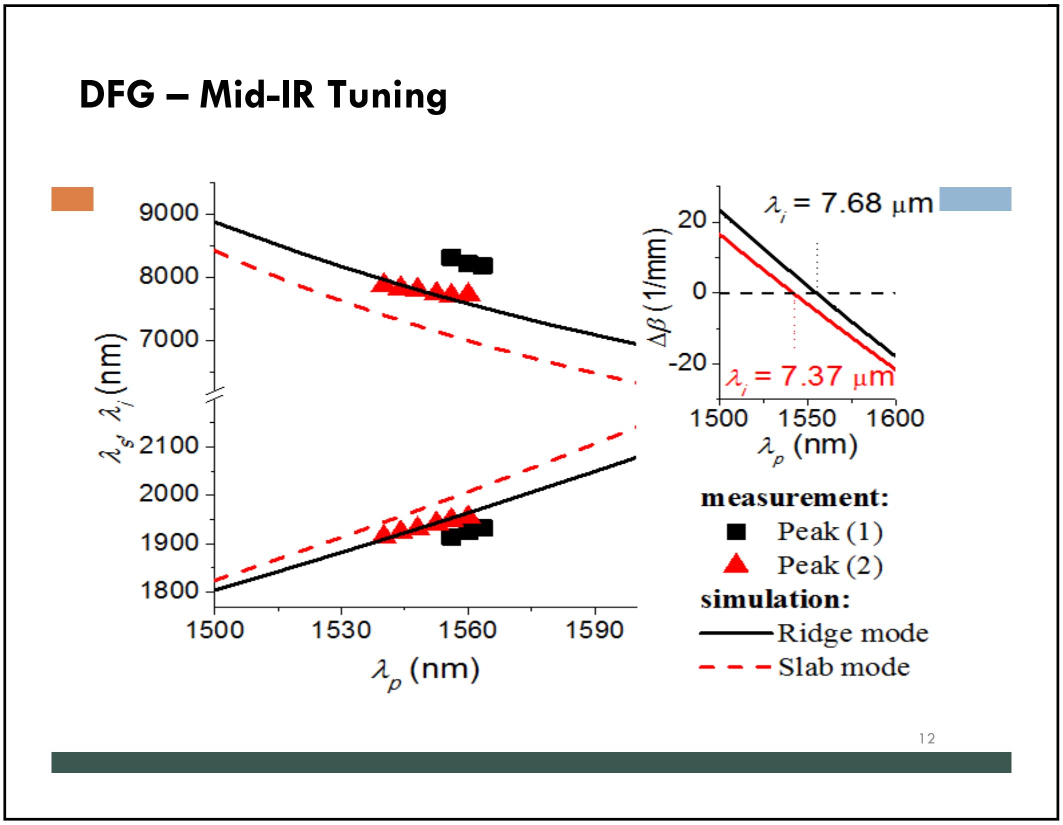
10



DFG – IR Tuning

11

11

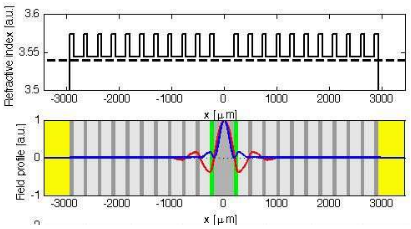


DFG – Mid-IR Tuning

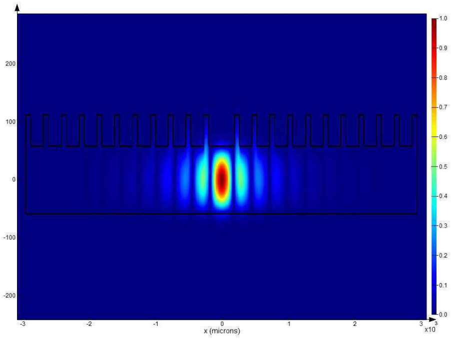
12

DFG – THz Phase Matching in BRWs

1D Equivalent Structure



2D Structure



- DFG of two telecom photons near 1550 nm, giving a photon at 1 THz
- BRWs can help bridge the gap between optical and microwave qubits

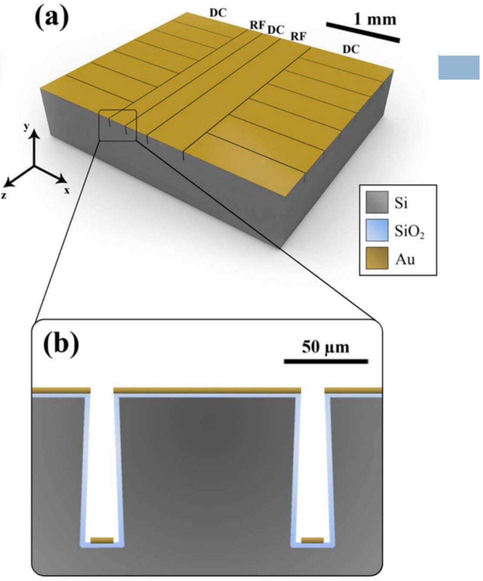
2D THz mode index	Phase matching mode index
3.53866	3.53962

AS Helmy Group Confidential

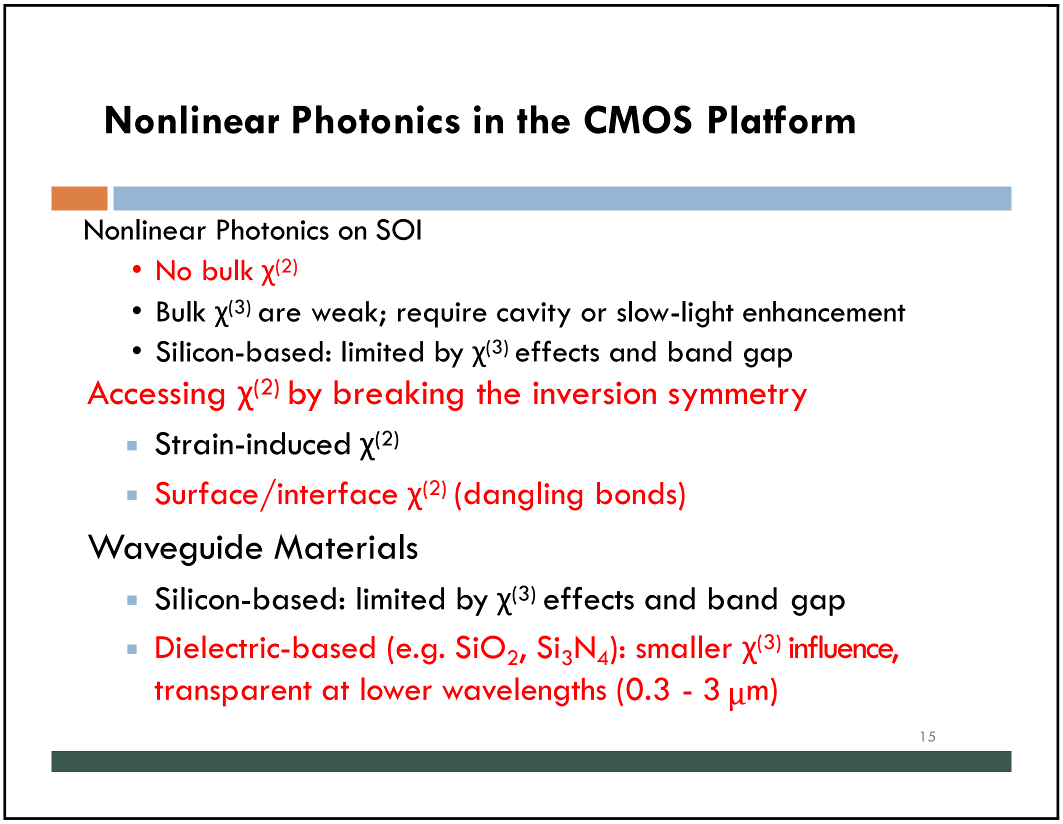
13

Critical Path: Integrated Traps

- □ Trapped ions are the pre-eminent building blocks for quantum information processing
- □ Traps have already been developed to help scale ion-based quantum computing
- □ The technologically important Si has been used to develop one of the most important atom traps: The Paul Trap



14



Nonlinear Photonics in the CMOS Platform

Nonlinear Photonics on SOI

- No bulk $\chi^{(2)}$
- Bulk $\chi^{(3)}$ are weak; require cavity or slow-light enhancement
- Silicon-based: limited by $\chi^{(3)}$ effects and band gap

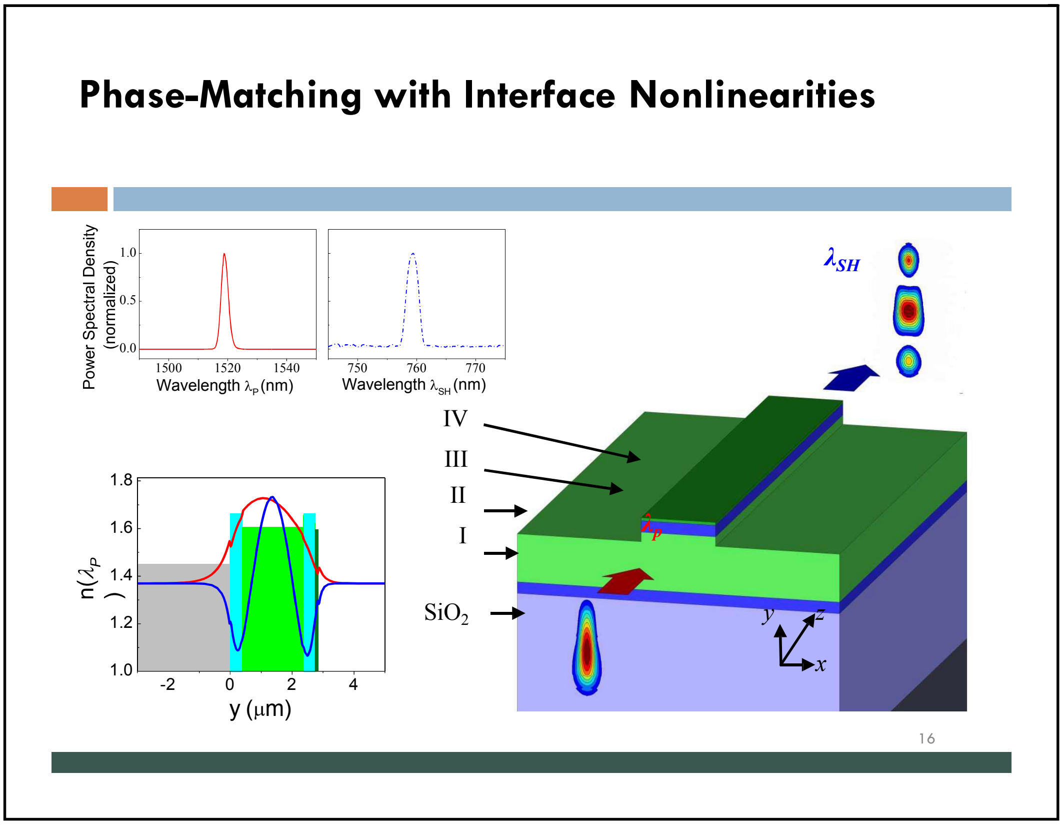
Accessing $\chi^{(2)}$ by breaking the inversion symmetry

- Strain-induced $\chi^{(2)}$
- Surface/interface $\chi^{(2)}$ (dangling bonds)

Waveguide Materials

- Silicon-based: limited by $\chi^{(3)}$ effects and band gap
- Dielectric-based (e.g. SiO_2, Si_3N_4): smaller $\chi^{(3)}$ influence, transparent at lower wavelengths (0.3 - 3 μm)

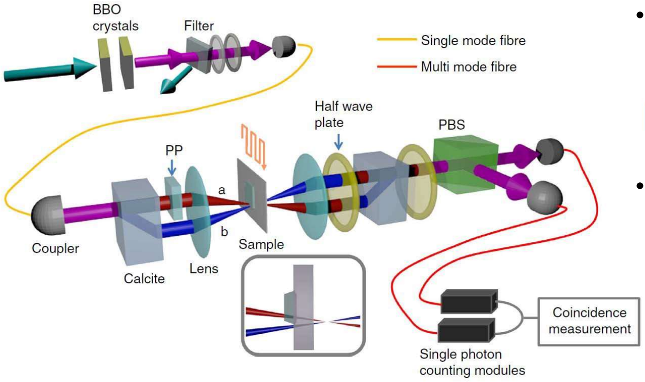
15



Phase-Matching with Interface Nonlinearities

16

Entanglement-Enhanced Microscopes



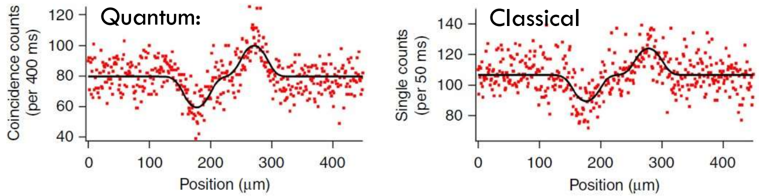
- Path-Entangled States provide spatial super-resolution

$$|\psi\rangle = |N0\rangle + |0N\rangle$$

- Maintaining max. path entanglement while allowing state tunability?

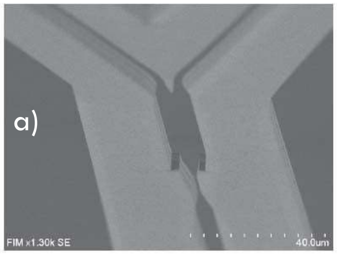
S/N is 1.35 ± 0.12 times better than classical

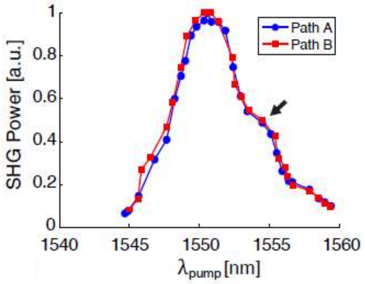
Ono *et al*., Nat. Comms. 4, 2426 (2013)

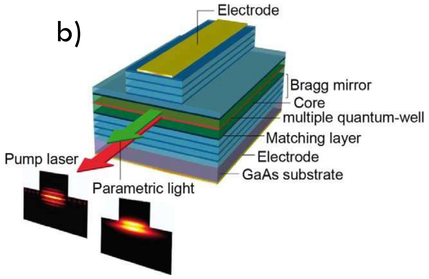


Path Entanglement <u>at the Source</u>

Compatible with the diverse dynamic tunability of BRWs.





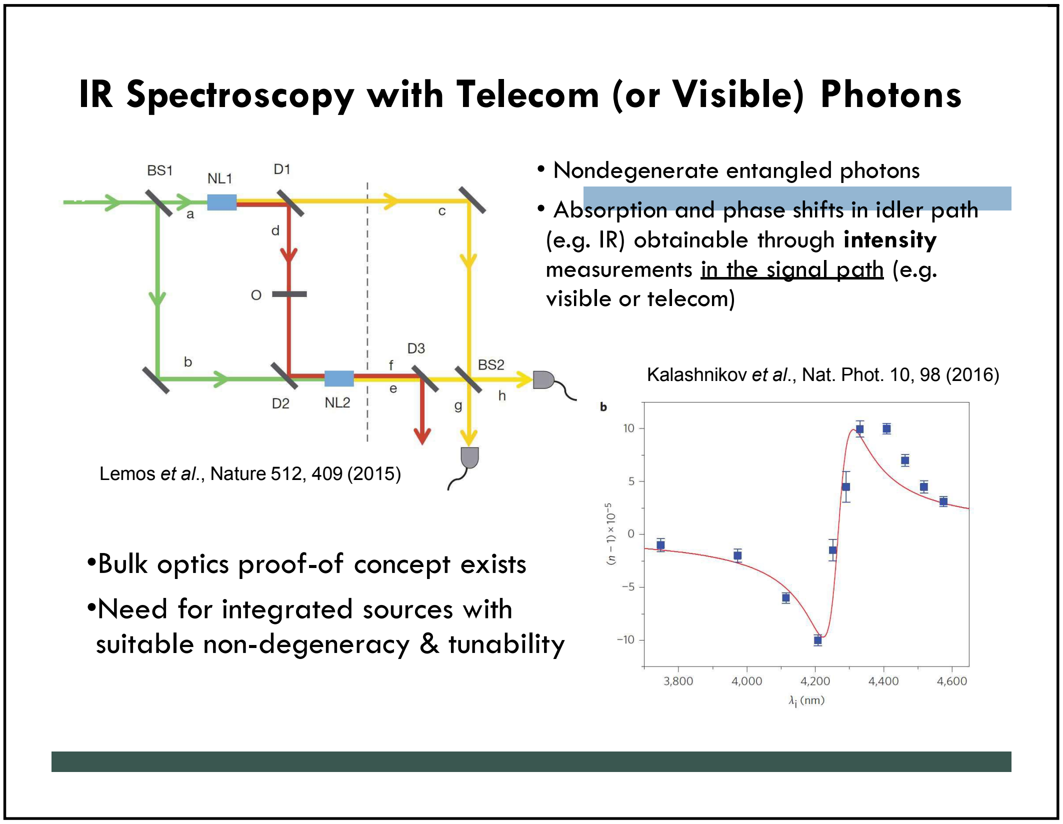


Need <u>indistinguishable</u> sources, ideally alignment-free.

a) Dual-path sources

b) Self-pumped sources

(use the two counter-propagating directions)



IR Spectroscopy with Telecom (or Visible) Photons

BS1
NL1
D1
a
d
c
O
b
D2
NL2
f
e
D3
BS2
g
h

Lemos *et al.*, Nature 512, 409 (2015)

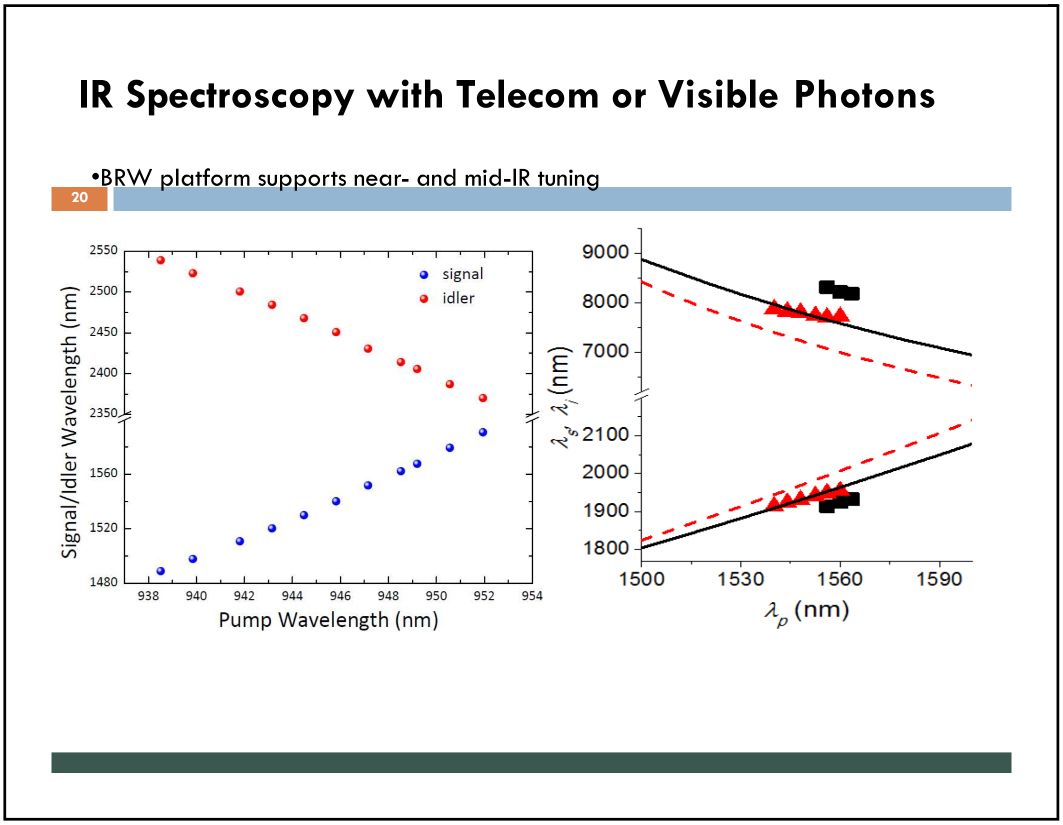
- Nondegenerate entangled photons
- Absorption and phase shifts in idler path (e.g. IR) obtainable through **intensity** measurements in the signal path (e.g. visible or telecom)

Kalashnikov *et al.*, Nat. Phot. 10, 98 (2016)

b
10
5
0
−5
−10
$(n-1)\times10^{-5}$
3,800
4,000
4,200
4,400
4,600
λ_i (nm)

•Bulk optics proof-of concept exists

•Need for integrated sources with suitable non-degeneracy & tunability

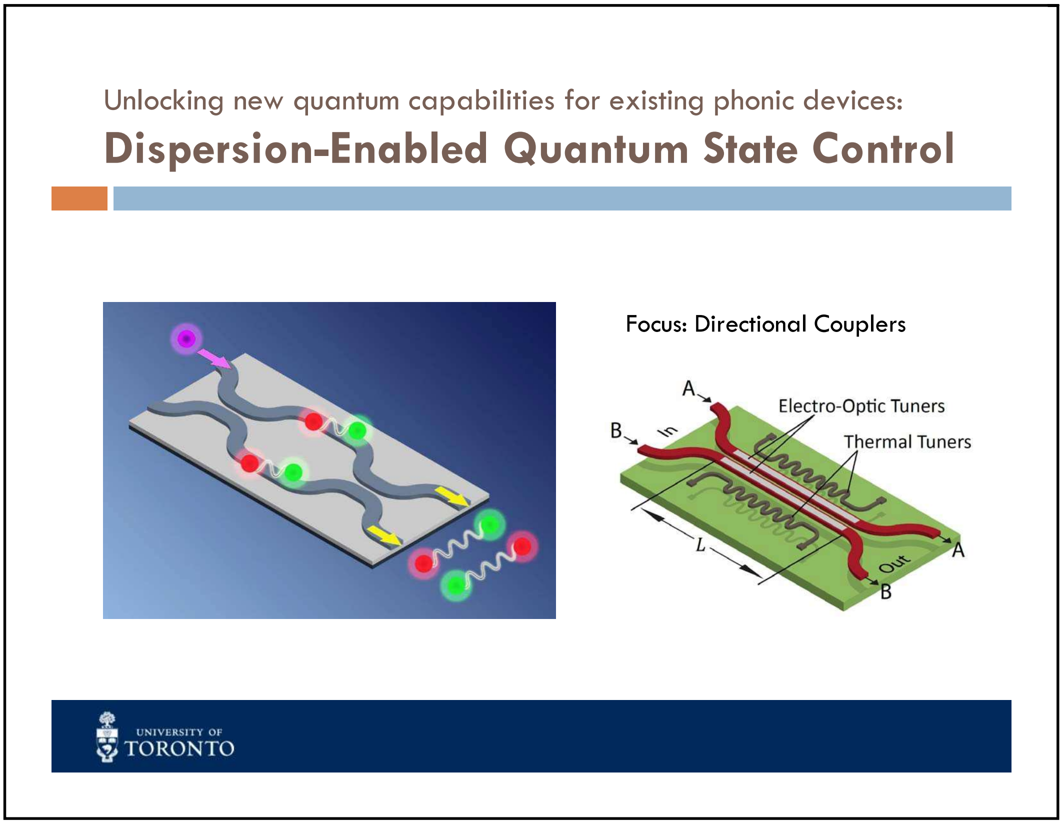


IR Spectroscopy with Telecom or Visible Photons

•BRW platform supports near- and mid-IR tuning

20

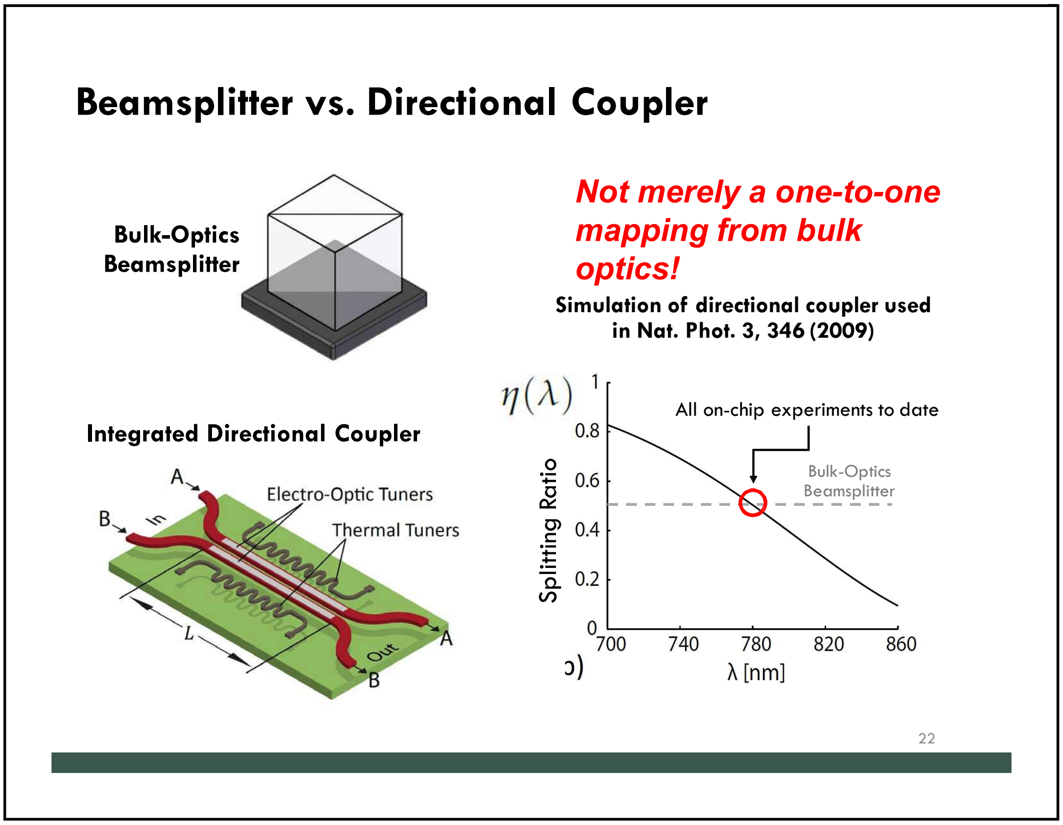
2550
2500
2450
2400
2350
1560
1520
1480
Signal/Idler Wavelength (nm)
signal
idler
938
940
942
944
946
948
950
952
954
Pump Wavelength (nm)
9000
8000
7000
2100
2000
1900
1800
λ_s, λ_i (nm)
1500
1530
1560
1590
λ_p (nm)



Unlocking new quantum capabilities for existing phonic devices:

Dispersion-Enabled Quantum State Control

Focus: Directional Couplers



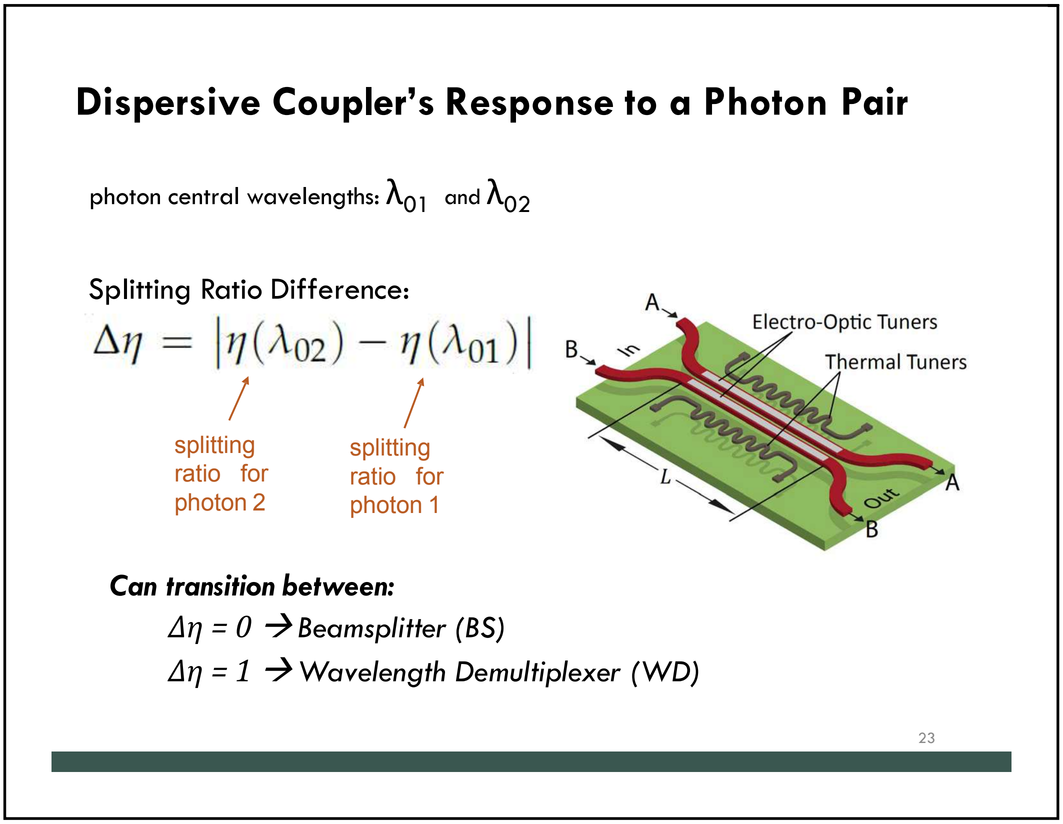
Beamsplitter vs. Directional Coupler

Bulk-Optics Beamsplitter

Integrated Directional Coupler

Not merely a one-to-one mapping from bulk optics!

Simulation of directional coupler used in Nat. Phot. 3, 346 (2009)



Dispersive Coupler's Response to a Photon Pair

photon central wavelengths: λ_{01} and λ_{02}

Splitting Ratio Difference:

$$\Delta\eta = \left|\eta(\lambda_{02}) - \eta(\lambda_{01})\right|$$

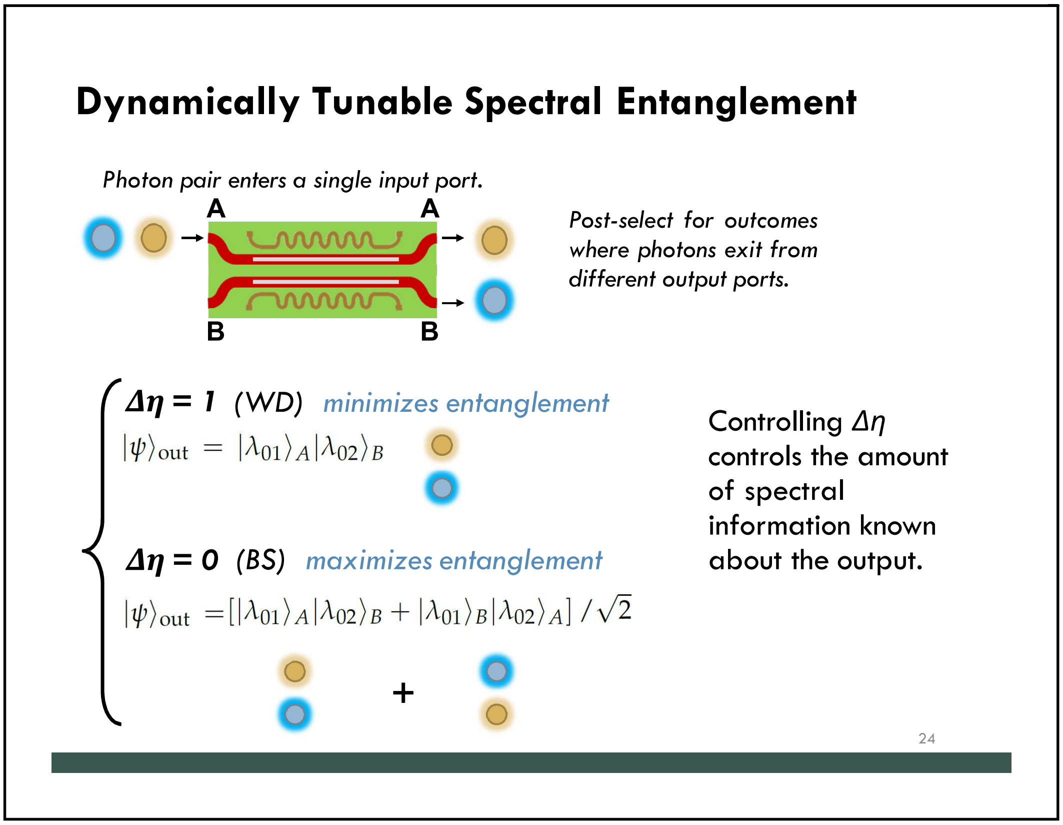
splitting ratio for photon 2

splitting ratio for photon 1

Can transition between:

$\Delta\eta = 0$ → Beamsplitter (BS)

$\Delta\eta = 1$ → Wavelength Demultiplexer (WD)



Dynamically Tunable Spectral Entanglement

Photon pair enters a single input port.

Post-select for outcomes where photons exit from different output ports.

Δη = 1 *(WD)* *minimizes entanglement*

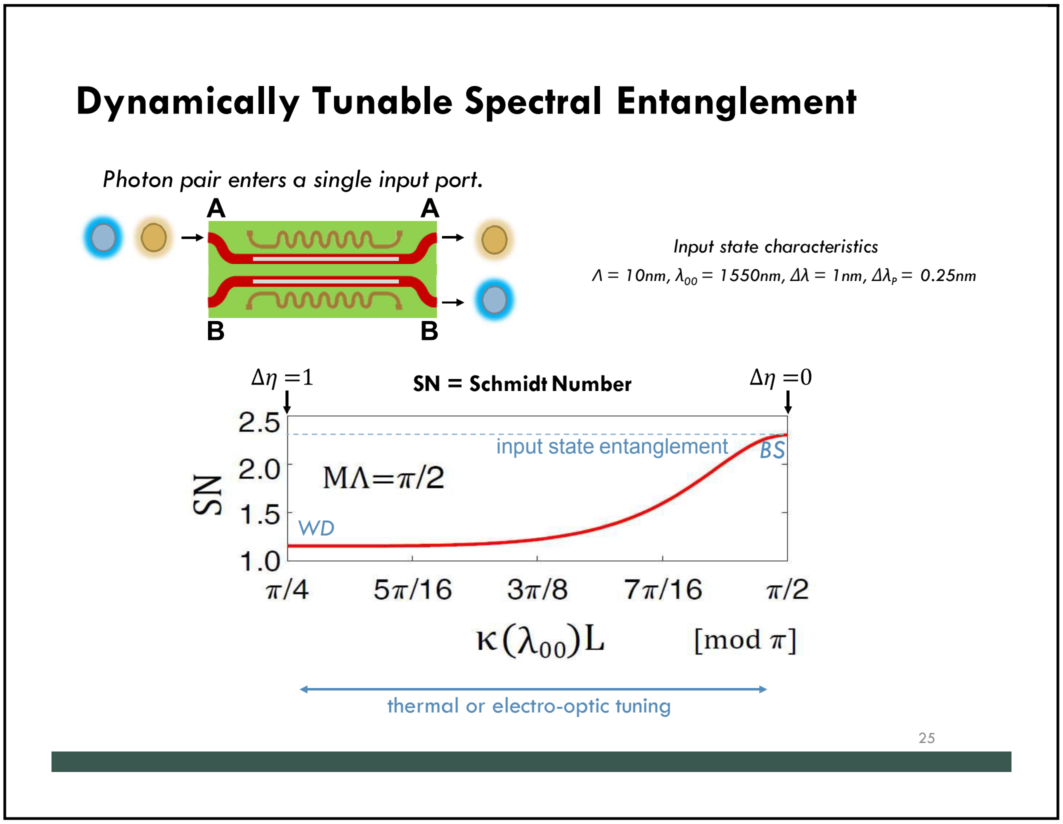
$$|\psi\rangle_{\text{out}} = |\lambda_{01}\rangle_A |\lambda_{02}\rangle_B$$

Δη = 0 *(BS)* *maximizes entanglement*

$$|\psi\rangle_{\text{out}} = [|\lambda_{01}\rangle_A |\lambda_{02}\rangle_B + |\lambda_{01}\rangle_B |\lambda_{02}\rangle_A] \,/\, \sqrt{2}$$

+

Controlling *Δη* controls the amount of spectral information known about the output.



Dynamically Tunable Spectral Entanglement

Photon pair enters a single input port.

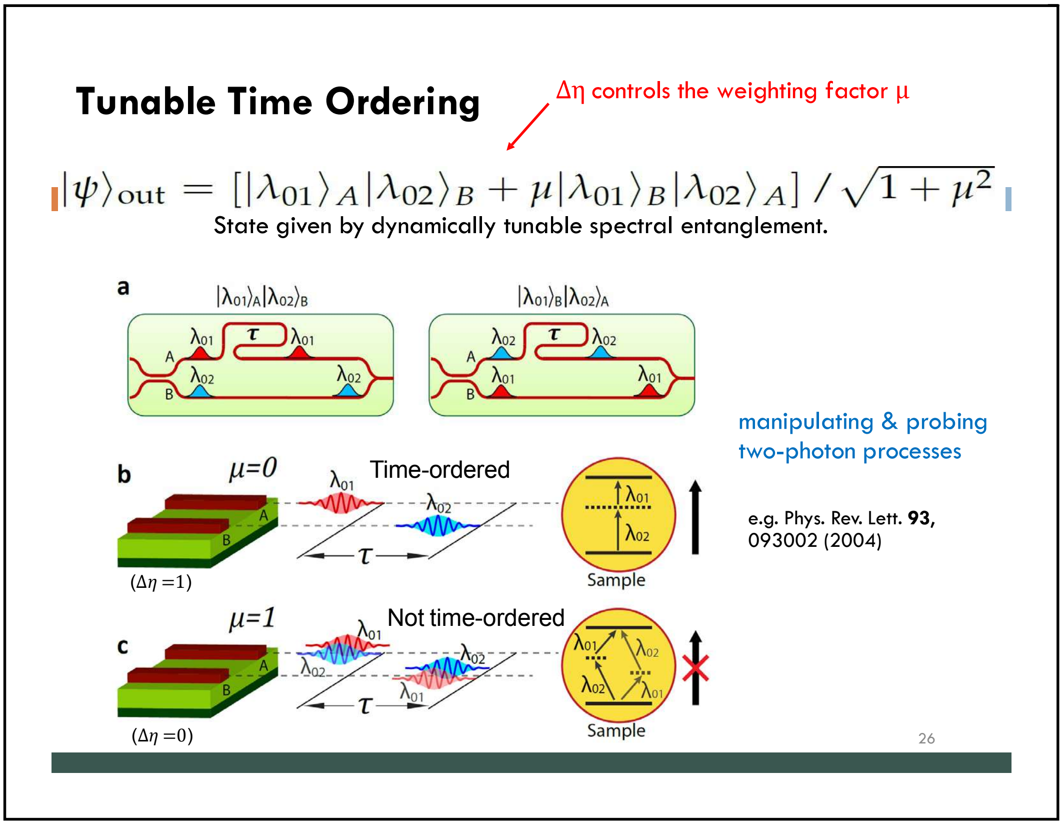
Input state characteristics

$\Lambda = 10nm,\ \lambda_{00} = 1550nm,\ \Delta\lambda = 1nm,\ \Delta\lambda_p = 0.25nm$

SN = Schmidt Number

thermal or electro-optic tuning

25



Tunable Time Ordering

Δη controls the weighting factor μ

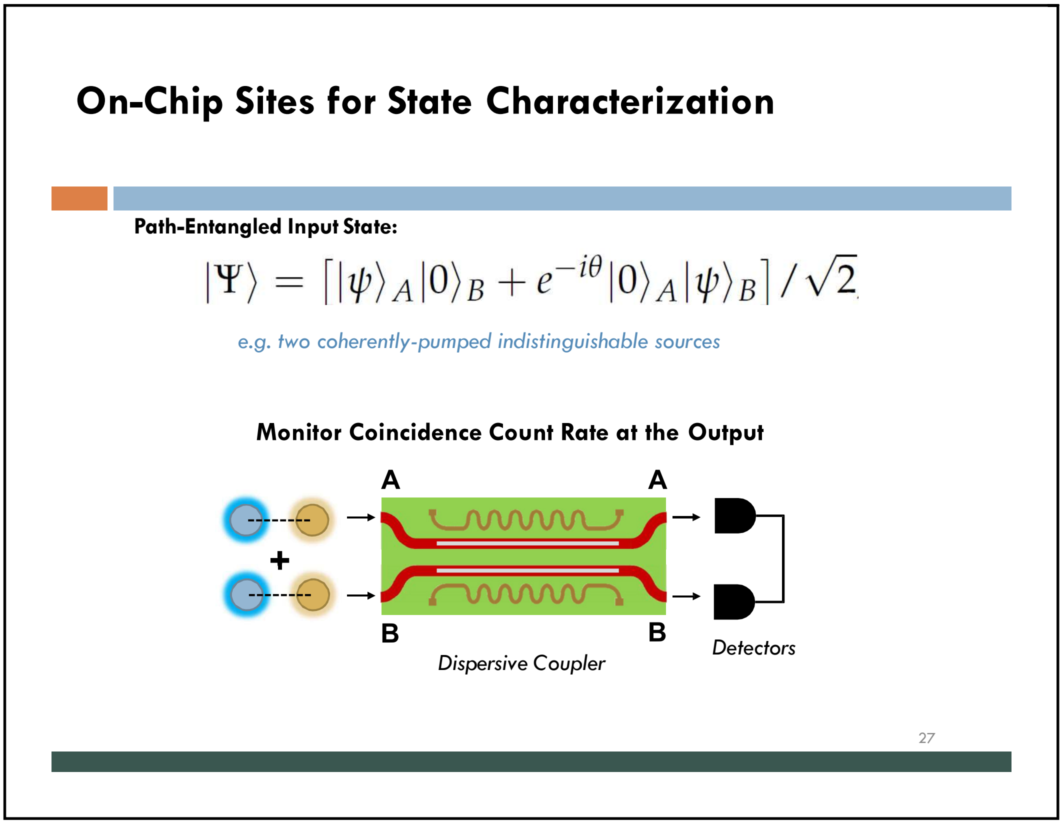
$$|\psi\rangle_{\text{out}} = [|\lambda_{01}\rangle_A |\lambda_{02}\rangle_B + \mu|\lambda_{01}\rangle_B |\lambda_{02}\rangle_A] \,/\, \sqrt{1+\mu^2}$$

State given by dynamically tunable spectral entanglement.

manipulating & probing two-photon processes

e.g. Phys. Rev. Lett. **93**, 093002 (2004)

26



On-Chip Sites for State Characterization

Path-Entangled Input State:

$$|\Psi\rangle = \left[|\psi\rangle_A|0\rangle_B + e^{-i\theta}|0\rangle_A|\psi\rangle_B\right]/\sqrt{2}$$

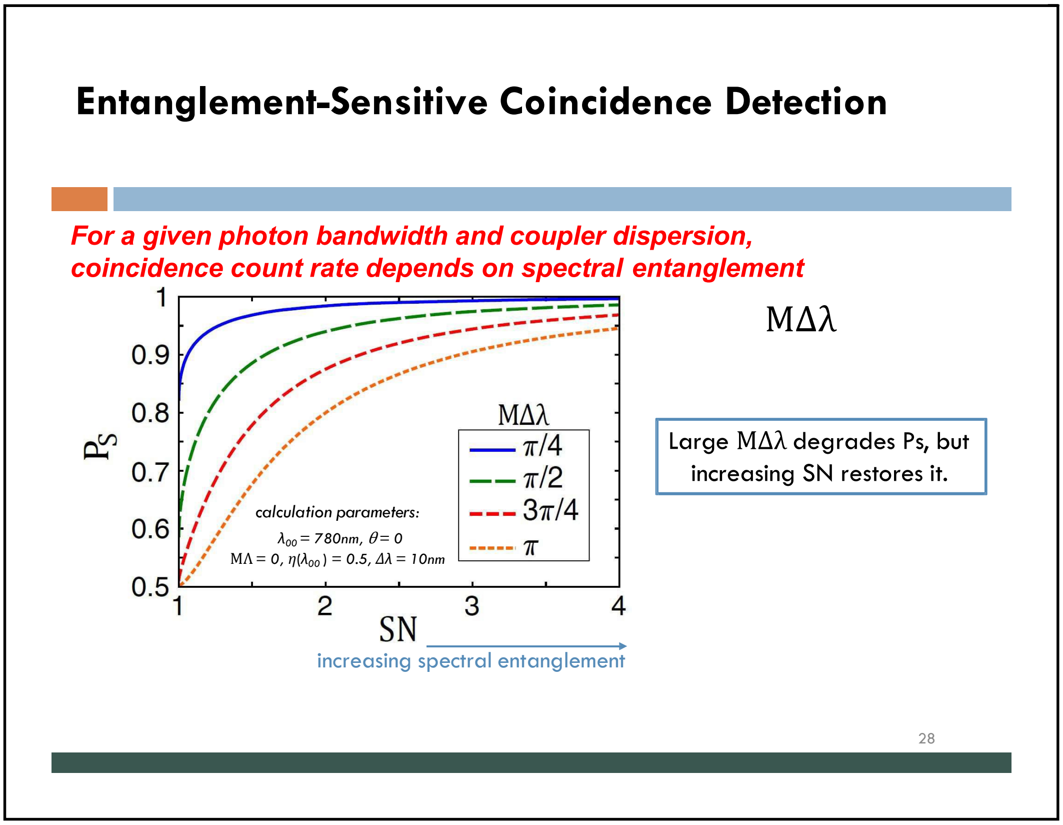
e.g. two coherently-pumped indistinguishable sources

Monitor Coincidence Count Rate at the Output

Dispersive Coupler

Detectors

27



Entanglement-Sensitive Coincidence Detection

For a given photon bandwidth and coupler dispersion, coincidence count rate depends on spectral entanglement

calculation parameters:

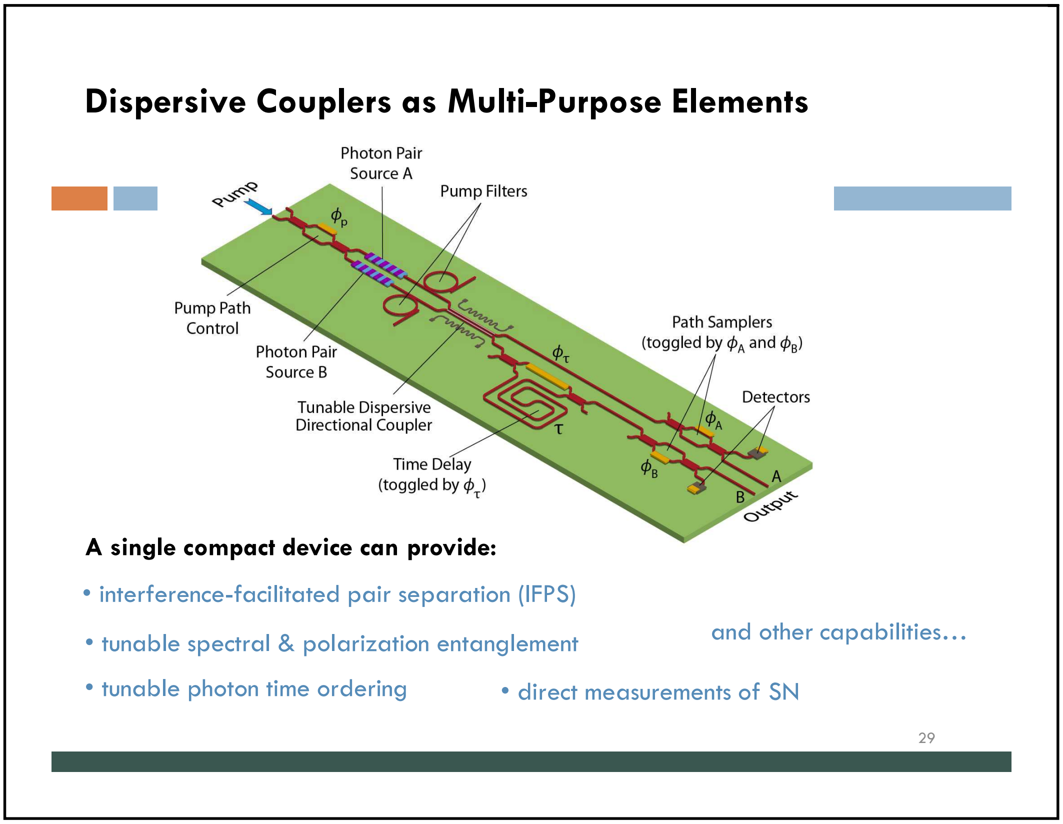
$\lambda_{00} = 780nm,\ \theta = 0$

$M\Lambda = 0,\ \eta(\lambda_{00}) = 0.5,\ \Delta\lambda = 10nm$

increasing spectral entanglement

Large MΔλ degrades Ps, but increasing SN restores it.

28



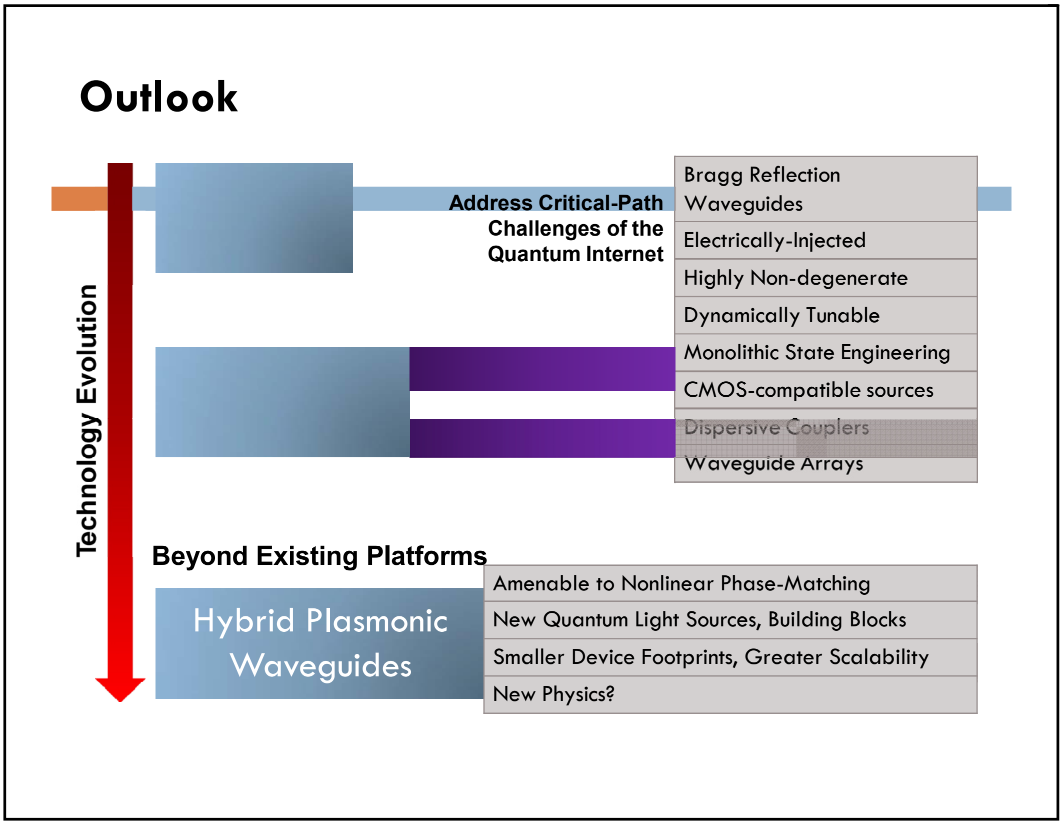
Dispersive Couplers as Multi-Purpose Elements

A single compact device can provide:

- interference-facilitated pair separation (IFPS)
- tunable spectral & polarization entanglement
- tunable photon time ordering
- direct measurements of SN

and other capabilities…

29



Outlook

Address Critical-Path Challenges of the Quantum Internet

Bragg Reflection Waveguides
Electrically-Injected
Highly Non-degenerate
Dynamically Tunable
Monolithic State Engineering
CMOS-compatible sources
Dispersive Couplers
Waveguide Arrays

Beyond Existing Platforms

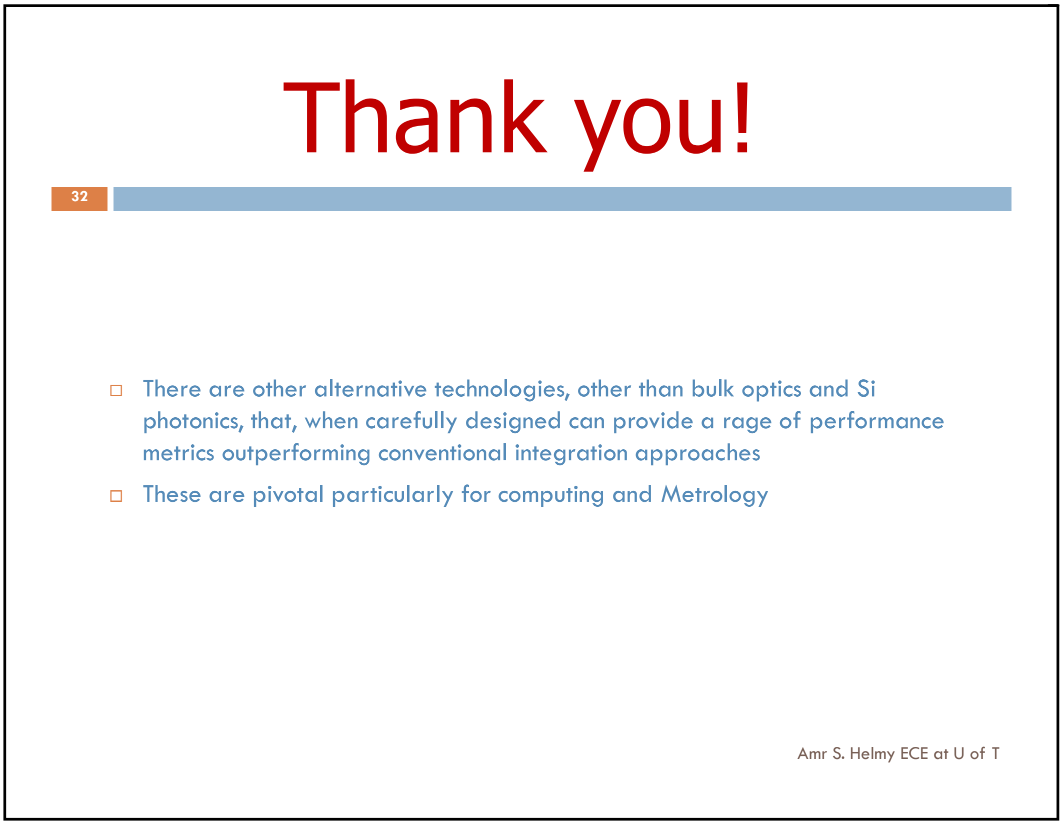
Hybrid Plasmonic Waveguides

Amenable to Nonlinear Phase-Matching
New Quantum Light Sources, Building Blocks
Smaller Device Footprints, Greater Scalability
New Physics?

Group Members and Collaborators

31

- □ Junbo Han, Bhavin Bijlani, Tong Cunzhu, Payam Abolghasem, Dongpeng Kang, Ankita Anriban, Nima Zareian, Greg Iu, Ryan Marchildon, Haoyu He, Arthur Pang,
- □ New Group Members: Han , Eric Chen, Daniel Giovannini, Aharon Brodutch, Zhizhong Yang
- □ G. Weihs and T Jennewein UW
- □ Sipe Group U of T

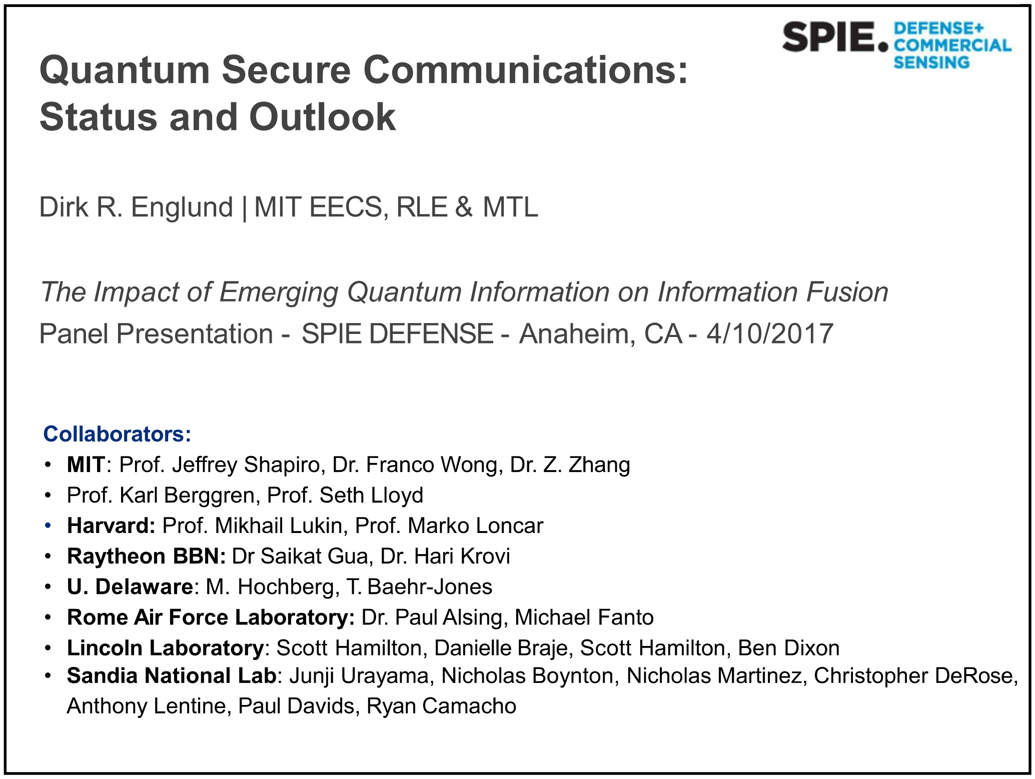


Thank you!

32

- □ There are other alternative technologies, other than bulk optics and Si photonics, that, when carefully designed can provide a rage of performance metrics outperforming conventional integration approaches
- □ These are pivotal particularly for computing and Metrology

Amr S. Helmy ECE at U of T



SPIE. DEFENSE+ COMMERCIAL SENSING

Quantum Secure Communications: Status and Outlook

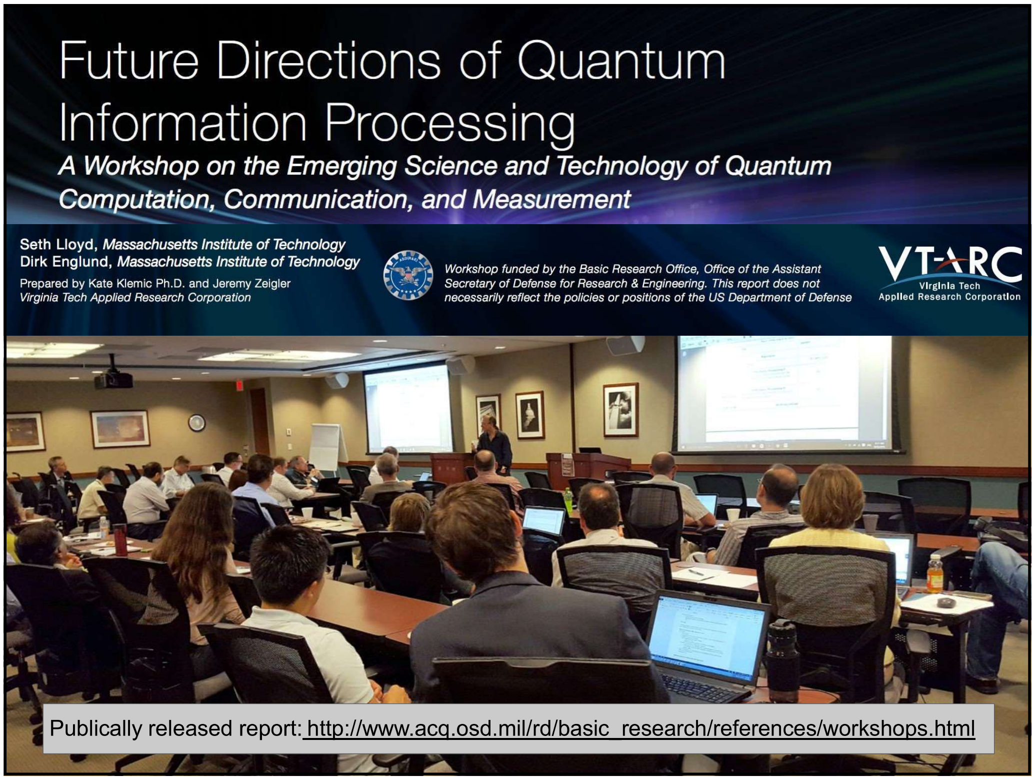
Dirk R. Englund | MIT EECS, RLE & MTL

The Impact of Emerging Quantum Information on Information Fusion

Panel Presentation - SPIE DEFENSE - Anaheim, CA - 4/10/2017

Collaborators:

- **MIT**: Prof. Jeffrey Shapiro, Dr. Franco Wong, Dr. Z. Zhang
- Prof. Karl Berggren, Prof. Seth Lloyd
- **Harvard:** Prof. Mikhail Lukin, Prof. Marko Loncar
- **Raytheon BBN:** Dr Saikat Gua, Dr. Hari Krovi
- **U. Delaware**: M. Hochberg, T. Baehr-Jones
- **Rome Air Force Laboratory:** Dr. Paul Alsing, Michael Fanto
- **Lincoln Laboratory**: Scott Hamilton, Danielle Braje, Scott Hamilton, Ben Dixon
- **Sandia National Lab**: Junji Urayama, Nicholas Boynton, Nicholas Martinez, Christopher DeRose, Anthony Lentine, Paul Davids, Ryan Camacho



Future Directions of Quantum Information Processing

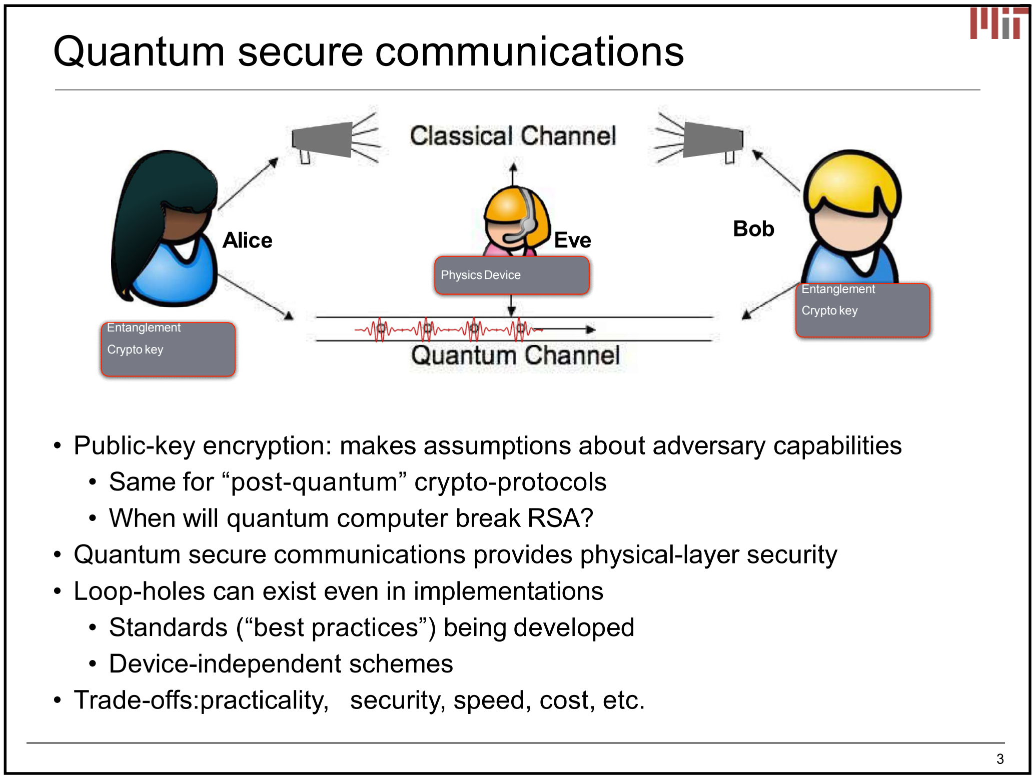
A Workshop on the Emerging Science and Technology of Quantum Computation, Communication, and Measurement

Seth Lloyd, *Massachusetts Institute of Technology*
Dirk Englund, *Massachusetts Institute of Technology*
Prepared by Kate Klemic Ph.D. and Jeremy Zeigler
Virginia Tech Applied Research Corporation

Workshop funded by the Basic Research Office, Office of the Assistant Secretary of Defense for Research & Engineering. This report does not necessarily reflect the policies or positions of the US Department of Defense

VT-ARC Virginia Tech Applied Research Corporation

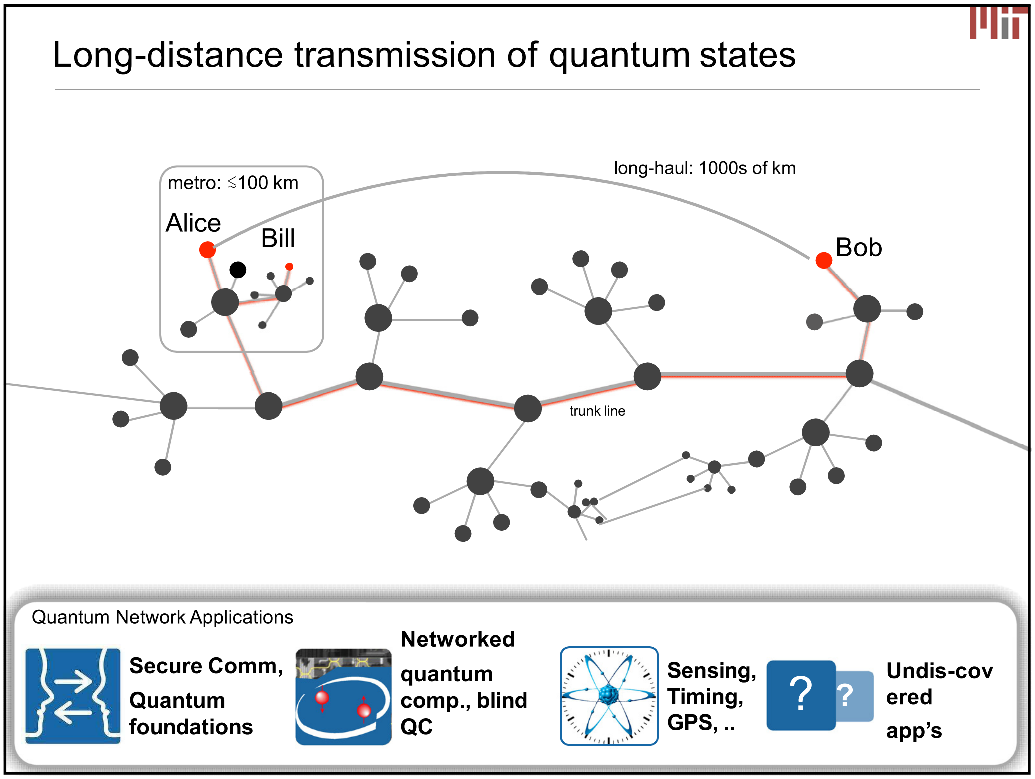
Publically released report: http://www.acq.osd.mil/rd/basic_research/references/workshops.html



Quantum secure communications

- Public-key encryption: makes assumptions about adversary capabilities
  - Same for “post-quantum” crypto-protocols
  - When will quantum computer break RSA?
- Quantum secure communications provides physical-layer security
- Loop-holes can exist even in implementations
  - Standards (“best practices”) being developed
  - Device-independent schemes
- Trade-offs:practicality,   security, speed, cost, etc.

3



Long-distance transmission of quantum states

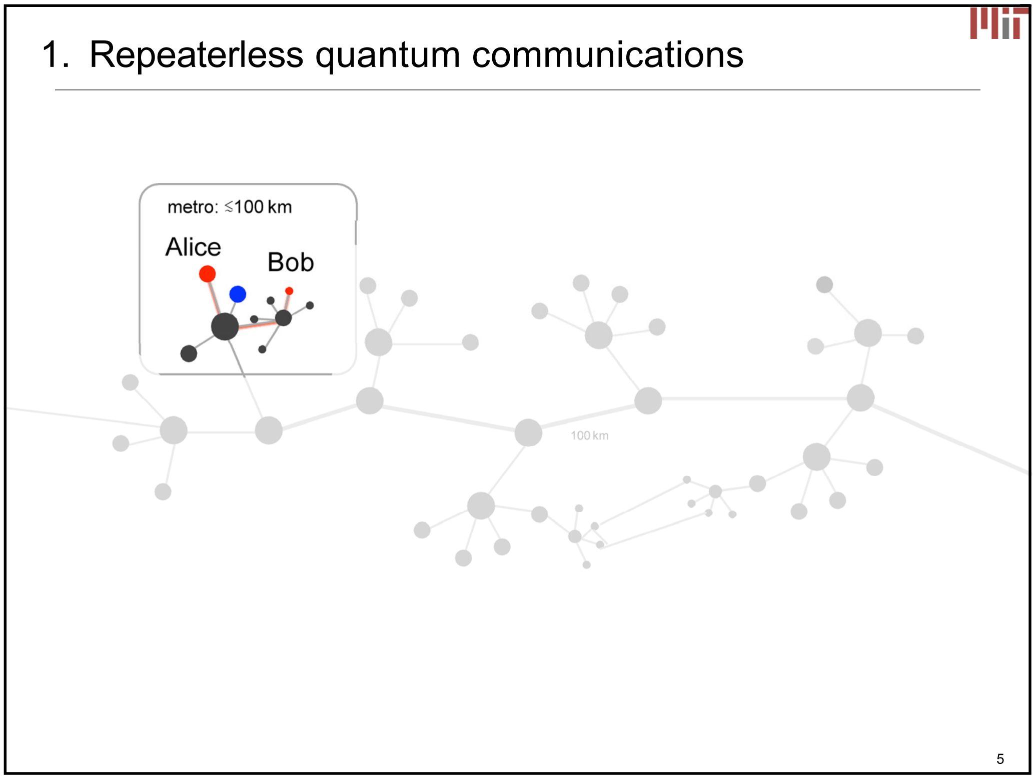
Quantum Network Applications

Secure Comm, Quantum foundations

Networked quantum comp., blind QC

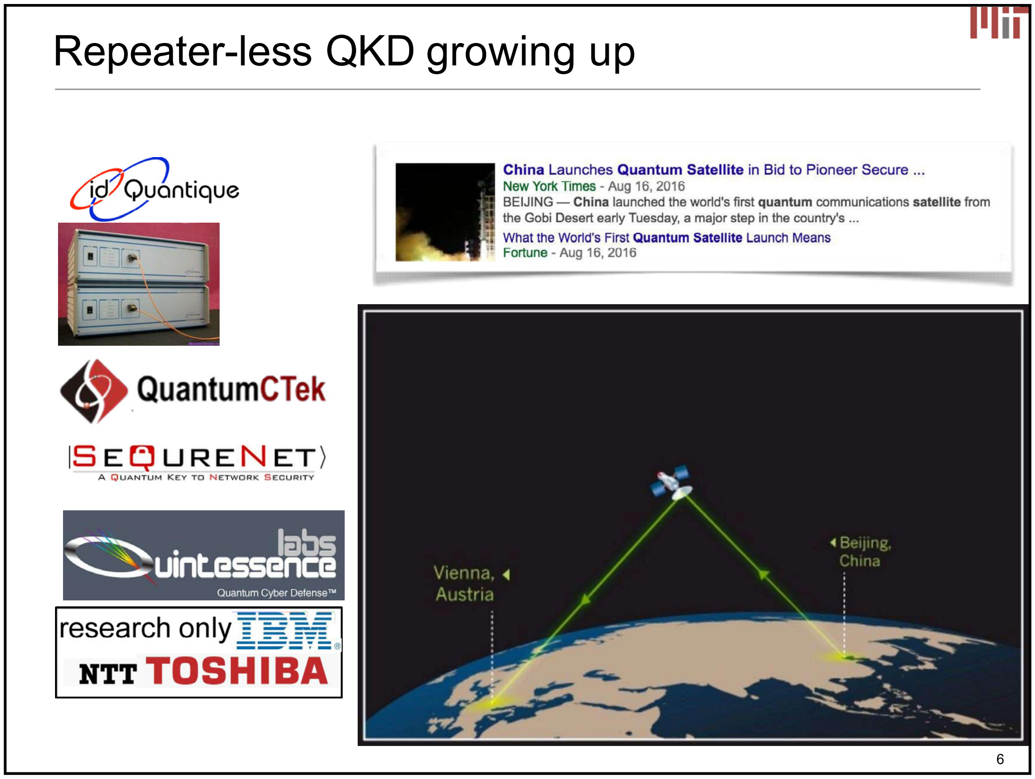
Sensing, Timing, GPS, ..

Undis-cov ered app’s



1. Repeaterless quantum communications

5

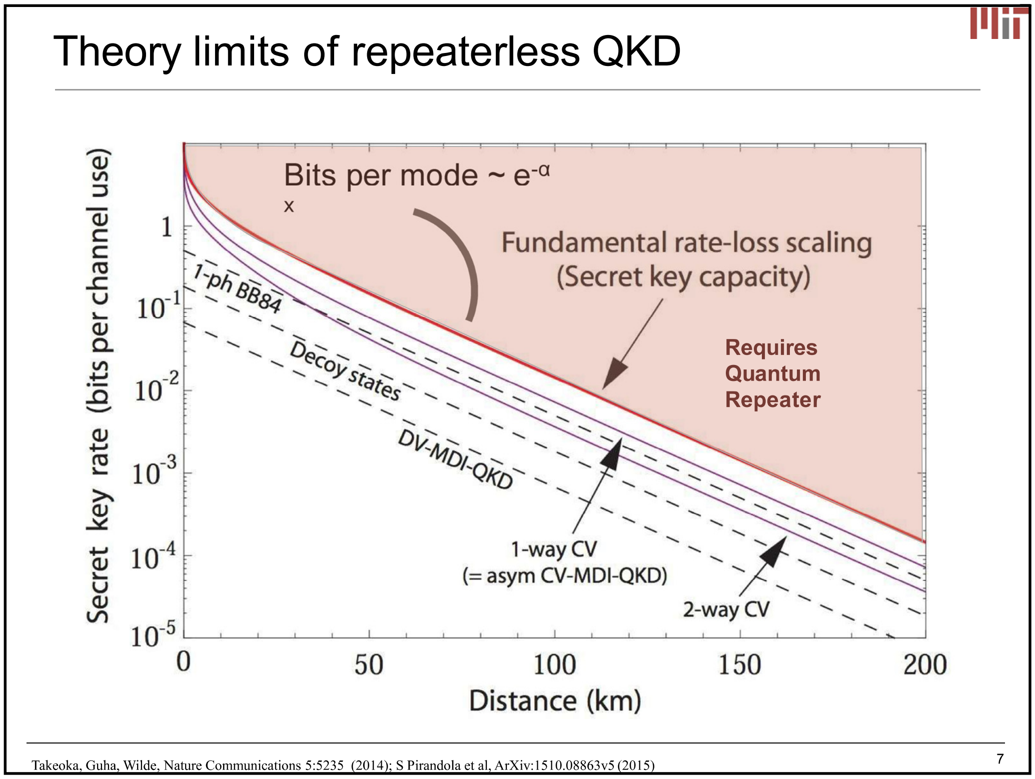


Repeater-less QKD growing up

research only IBM
NTT TOSHIBA

China Launches **Quantum Satellite** in Bid to Pioneer Secure ...
New York Times - Aug 16, 2016
BEIJING — **China** launched the world's first **quantum** communications **satellite** from the Gobi Desert early Tuesday, a major step in the country's ...
What the World's First **Quantum Satellite** Launch Means
Fortune - Aug 16, 2016

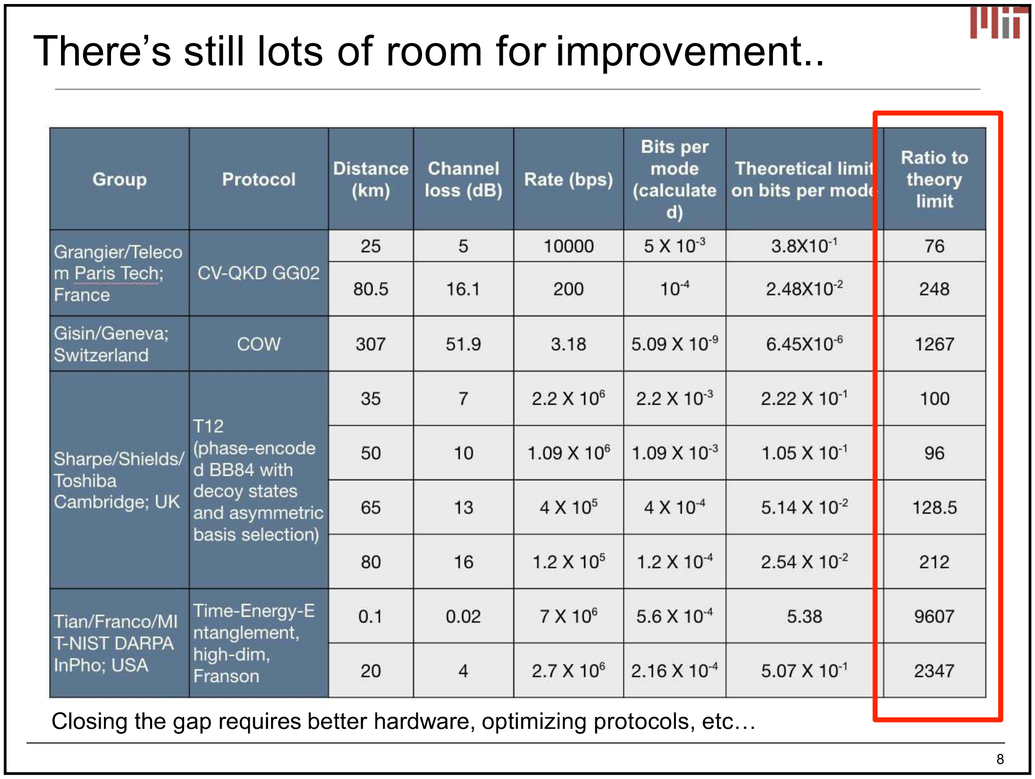
6



Theory limits of repeaterless QKD

Takeoka, Guha, Wilde, Nature Communications 5:5235 (2014); S Pirandola et al, ArXiv:1510.08863v5 (2015)

7

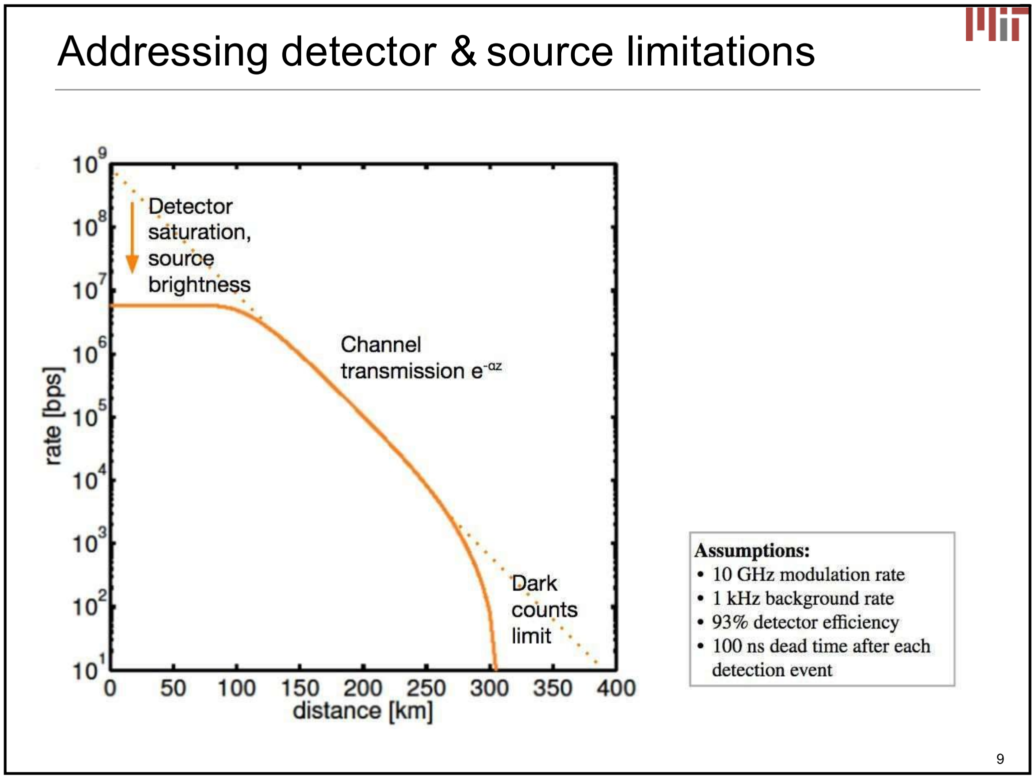


There's still lots of room for improvement..

Group	Protocol	Distance (km)	Channel loss (dB)	Rate (bps)	Bits per mode (calculated)	Theoretical limit on bits per mode	Ratio to theory limit
Grangier/Telecom Paris Tech; France	CV-QKD GG02	25	5	10000	5 X 10^{-3}	3.8X10^{-1}	76
		80.5	16.1	200	10^{-4}	2.48X10^{-2}	248
Gisin/Geneva; Switzerland	COW	307	51.9	3.18	5.09 X 10^{-9}	6.45X10^{-6}	1267
Sharpe/Shields/ Toshiba Cambridge; UK	T12 (phase-encoded BB84 with decoy states and asymmetric basis selection)	35	7	2.2 X 10^{6}	2.2 X 10^{-3}	2.22 X 10^{-1}	100
		50	10	1.09 X 10^{6}	1.09 X 10^{-3}	1.05 X 10^{-1}	96
		65	13	4 X 10^{5}	4 X 10^{-4}	5.14 X 10^{-2}	128.5
		80	16	1.2 X 10^{5}	1.2 X 10^{-4}	2.54 X 10^{-2}	212
Tian/Franco/MIT-NIST DARPA InPho; USA	Time-Energy-Entanglement, high-dim, Franson	0.1	0.02	7 X 10^{6}	5.6 X 10^{-4}	5.38	9607
		20	4	2.7 X 10^{6}	2.16 X 10^{-4}	5.07 X 10^{-1}	2347

Closing the gap requires better hardware, optimizing protocols, etc…

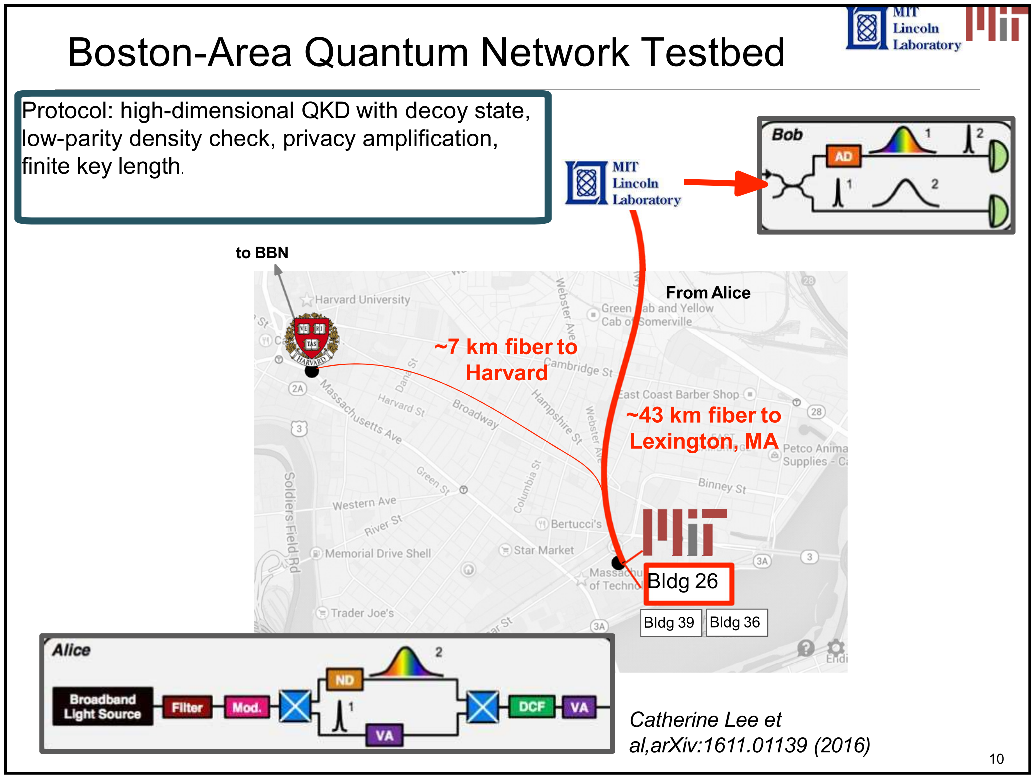
8



Addressing detector & source limitations

Assumptions:
- 10 GHz modulation rate
- 1 kHz background rate
- 93% detector efficiency
- 100 ns dead time after each detection event

9

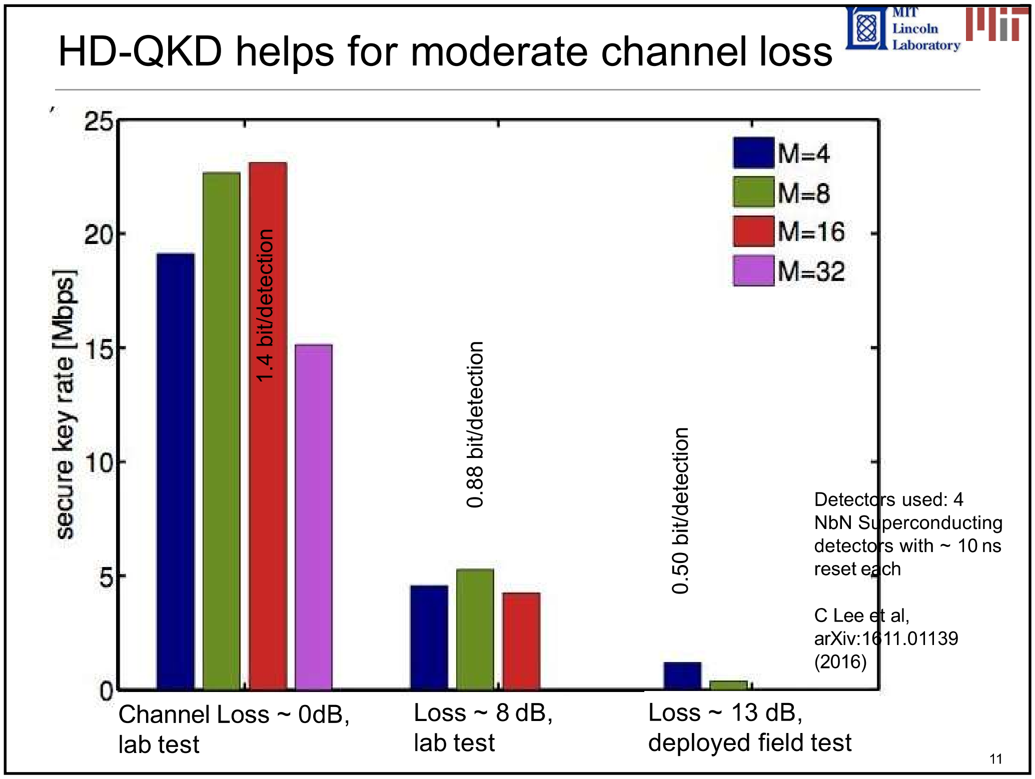


Boston-Area Quantum Network Testbed

Protocol: high-dimensional QKD with decoy state, low-parity density check, privacy amplification, finite key length.

Catherine Lee et al,arXiv:1611.01139 (2016)

10

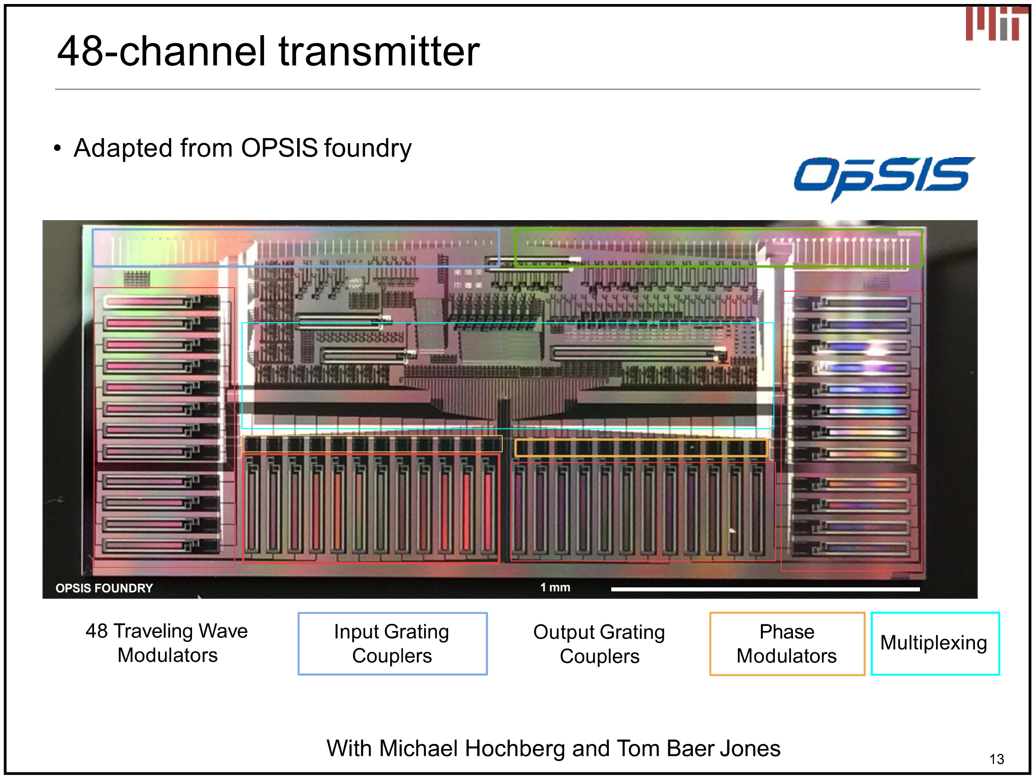


HD-QKD helps for moderate channel loss

Detectors used: 4 NbN Superconducting detectors with ~ 10 ns reset each

C Lee et al, arXiv:1611.01139 (2016)

11



48-channel transmitter

- Adapted from OPSIS foundry

48 Traveling Wave Modulators

Input Grating Couplers

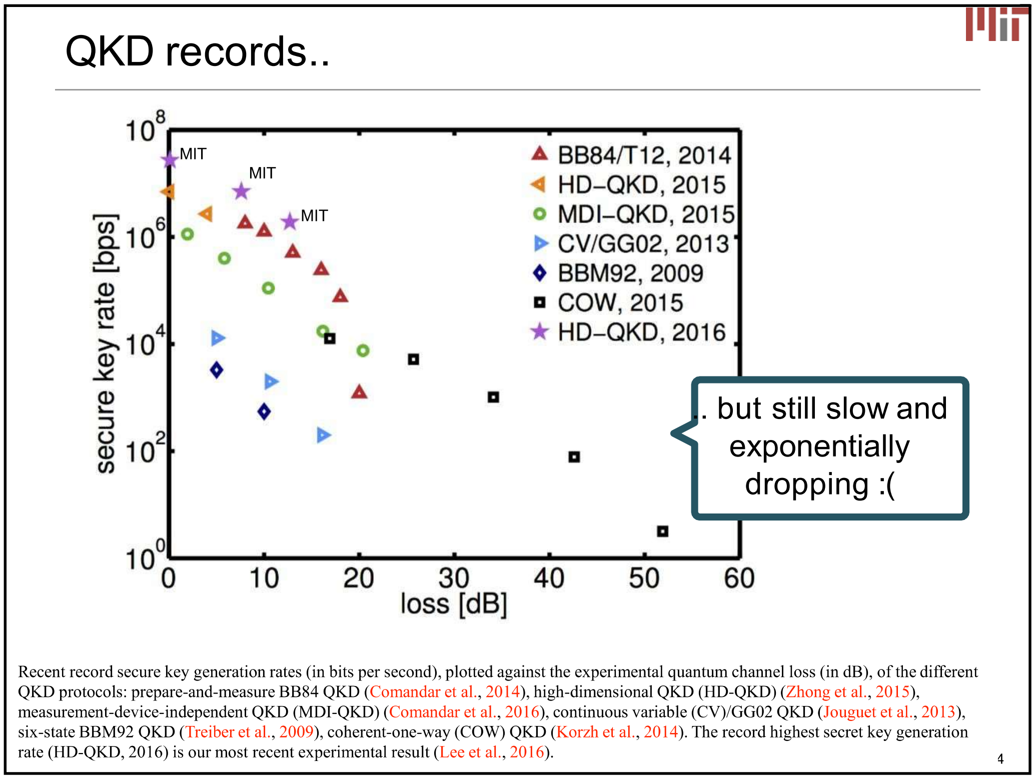
Output Grating Couplers

Phase Modulators

Multiplexing

With Michael Hochberg and Tom Baer Jones

13

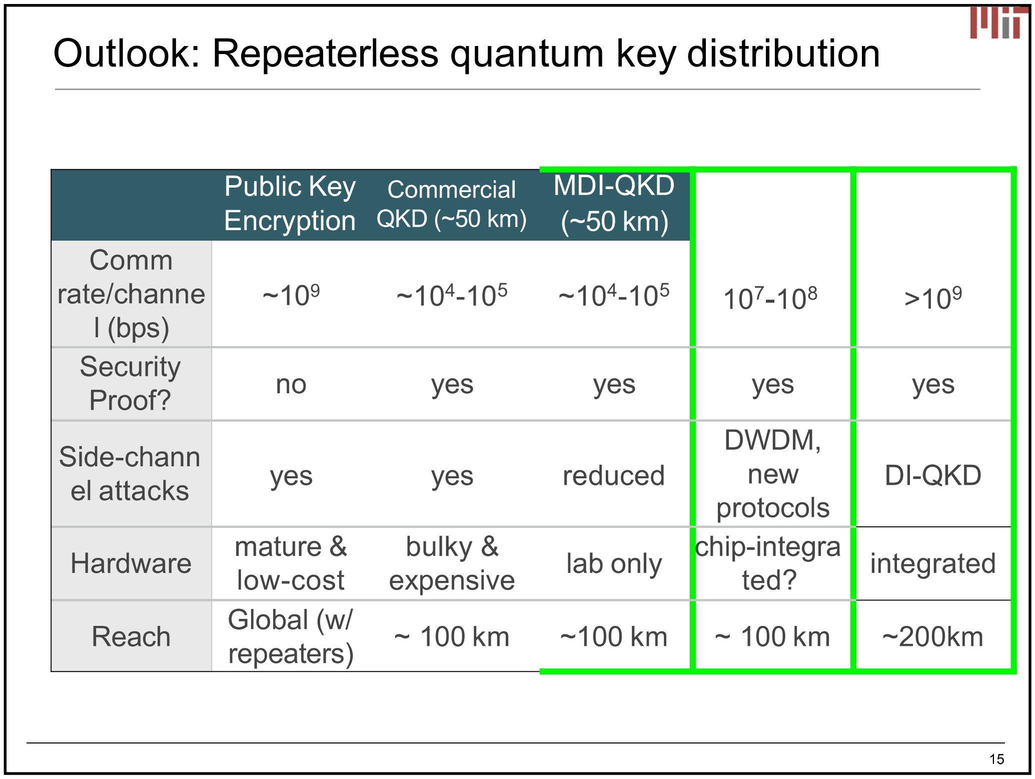


QKD records..

.. but still slow and exponentially dropping :(

Recent record secure key generation rates (in bits per second), plotted against the experimental quantum channel loss (in dB), of the different QKD protocols: prepare-and-measure BB84 QKD (Comandar et al., 2014), high-dimensional QKD (HD-QKD) (Zhong et al., 2015), measurement-device-independent QKD (MDI-QKD) (Comandar et al., 2016), continuous variable (CV)/GG02 QKD (Jouguet et al., 2013), six-state BBM92 QKD (Treiber et al., 2009), coherent-one-way (COW) QKD (Korzh et al., 2014). The record highest secret key generation rate (HD-QKD, 2016) is our most recent experimental result (Lee et al., 2016).

4



Outlook: Repeaterless quantum key distribution

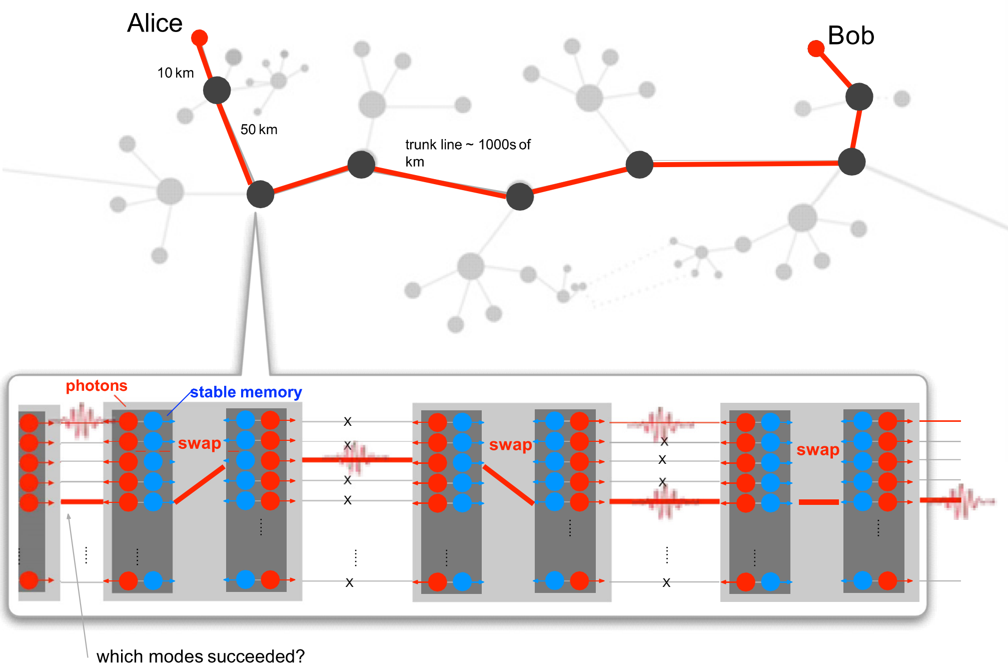
	Public Key Encryption	Commercial QKD (~50 km)	MDI-QKD (~50 km)		
Comm rate/channel (bps)	~10^9	~10^4-10^5	~10^4-10^5	10^7-10^8	>10^9
Security Proof?	no	yes	yes	yes	yes
Side-channel attacks	yes	yes	reduced	DWDM, new protocols	DI-QKD
Hardware	mature & low-cost	bulky & expensive	lab only	chip-integrated?	integrated
Reach	Global (w/ repeaters)	~ 100 km	~100 km	~ 100 km	~200km

15

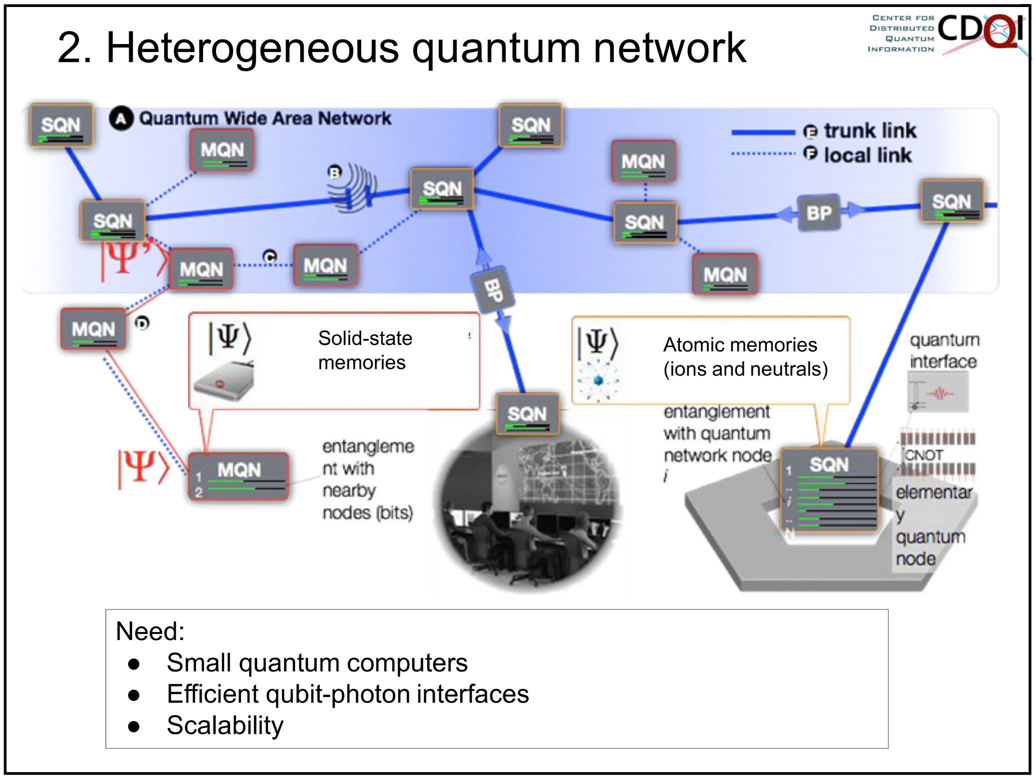
QKD questions

- QKD can improve classical crypto networks (e.g., seeding P-RNG)
- What speed to we actually require over what distance?
  - What impact would 10 kbit/second have ..
    - Over 300 km, 1000 km, ..?
    - How often to re-key, etc?
    - Now that quantum computers are becoming real, need for closer discussions between classical and quantum crypto
- What rates will “post-quantum” crypto protocols achieve (beyond RSA, etc)?
- What level of security do *we actually need?*
  - DI-QKD, covert communications, etc

2. Quantum repeater networks



H. Briegel et al, PRL 81 (1998)

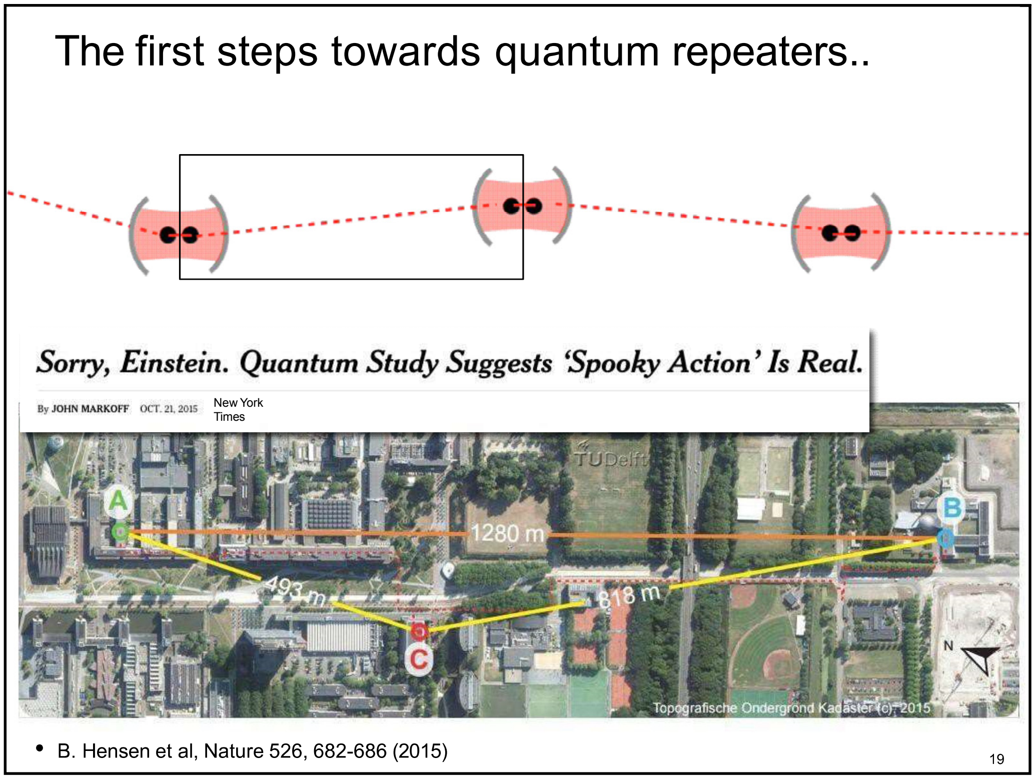


2. Heterogeneous quantum network

Center for Distributed Quantum Information
CDQI
A Quantum Wide Area Network
B
C
D
E trunk link
F local link
SQN
MQN
BP
|Ψ'⟩
|Ψ⟩
Solid-state memories
Atomic memories (ions and neutrals)
entanglement with nearby nodes (bits)
entanglement with quantum network node i
quantum interface
CNOT
elementary quantum node
1
2
i
N

Need:

- Small quantum computers
- Efficient qubit-photon interfaces
- Scalability

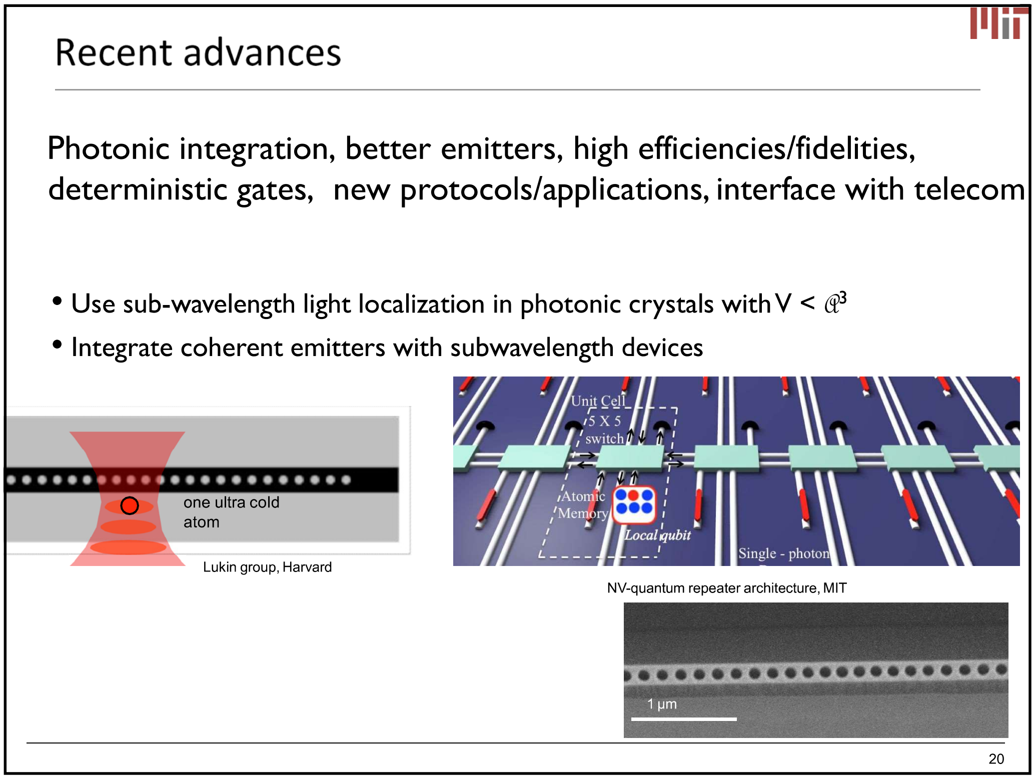


The first steps towards quantum repeaters..

Sorry, Einstein. Quantum Study Suggests 'Spooky Action' Is Real.

By JOHN MARKOFF OCT. 21, 2015 New York Times

- B. Hensen et al, Nature 526, 682-686 (2015)



Recent advances

Photonic integration, better emitters, high efficiencies/fidelities, deterministic gates, new protocols/applications, interface with telecom

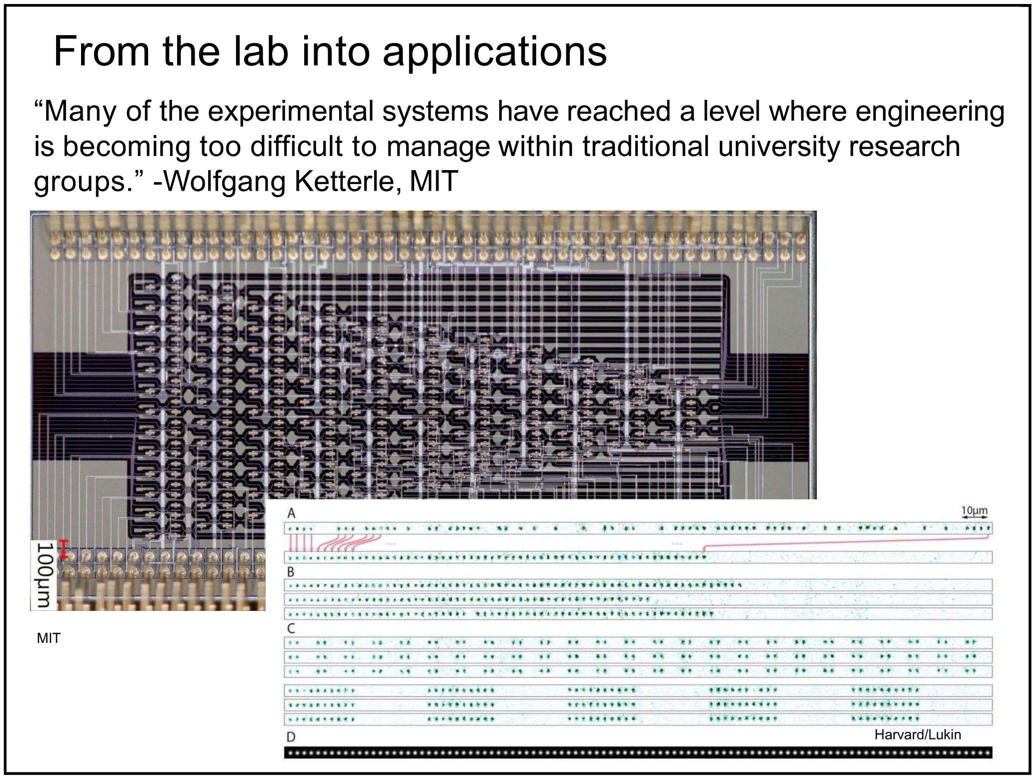
- Use sub-wavelength light localization in photonic crystals with V < @^{3}
- Integrate coherent emitters with subwavelength devices

one ultra cold atom
Unit Cell
5 X 5
switch
Atomic
Memory
Local qubit
Single - photon
1 µm

Lukin group, Harvard

NV-quantum repeater architecture, MIT

20



From the lab into applications

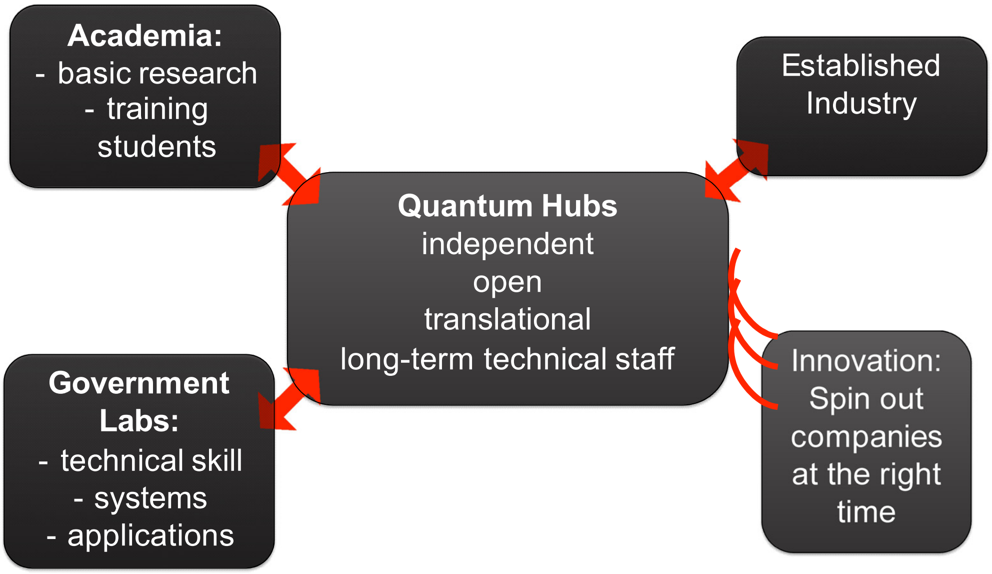
“Many of the experimental systems have reached a level where engineering is becoming too difficult to manage within traditional university research groups.” -Wolfgang Ketterle, MIT

100µm
A
10µm
B
C
D

MIT

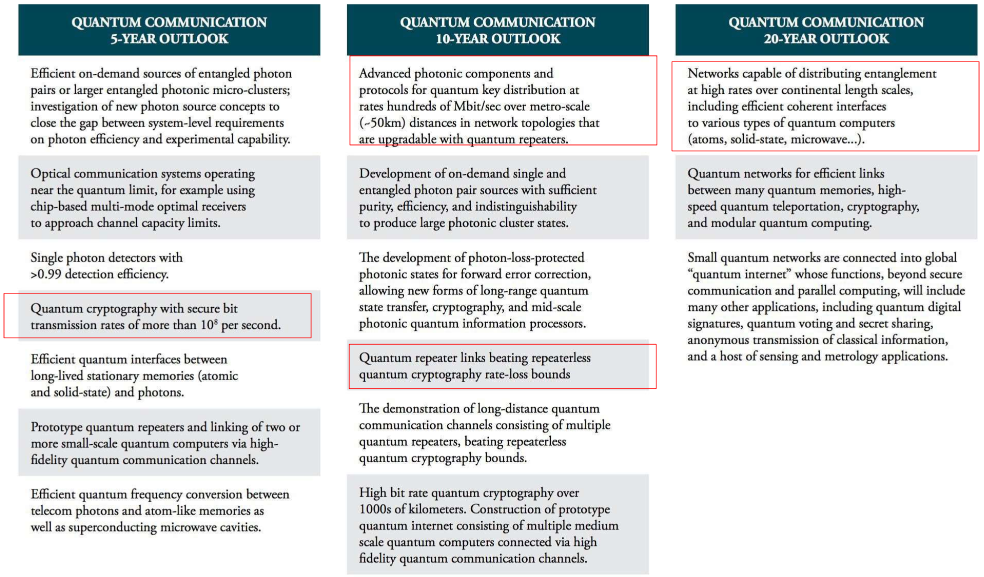
Harvard/Lukin

Building a Quantum Ecosystem



22

Quantum Communication - Outlook



QUANTUM COMMUNICATION 5-YEAR OUTLOOK

Efficient on-demand sources of entangled photon pairs or larger entangled photonic micro-clusters; investigation of new photon source concepts to close the gap between system-level requirements on photon efficiency and experimental capability.

Optical communication systems operating near the quantum limit, for example using chip-based multi-mode optimal receivers to approach channel capacity limits.

Single photon detectors with >0.99 detection efficiency.

Quantum cryptography with secure bit transmission rates of more than 10^8 per second.

Efficient quantum interfaces between long-lived stationary memories (atomic and solid-state) and photons.

Prototype quantum repeaters and linking of two or more small-scale quantum computers via high-fidelity quantum communication channels.

Efficient quantum frequency conversion between telecom photons and atom-like memories as well as superconducting microwave cavities.

QUANTUM COMMUNICATION 10-YEAR OUTLOOK

Advanced photonic components and protocols for quantum key distribution at rates hundreds of Mbit/sec over metro-scale (~50km) distances in network topologies that are upgradable with quantum repeaters.

Development of on-demand single and entangled photon pair sources with sufficient purity, efficiency, and indistinguishability to produce large photonic cluster states.

The development of photon-loss-protected photonic states for forward error correction, allowing new forms of long-range quantum state transfer, cryptography, and mid-scale photonic quantum information processors.

Quantum repeater links beating repeaterless quantum cryptography rate-loss bounds

The demonstration of long-distance quantum communication channels consisting of multiple quantum repeaters, beating repeaterless quantum cryptography bounds.

High bit rate quantum cryptography over 1000s of kilometers. Construction of prototype quantum internet consisting of multiple medium scale quantum computers connected via high fidelity quantum communication channels.

QUANTUM COMMUNICATION 20-YEAR OUTLOOK

Networks capable of distributing entanglement at high rates over continental length scales, including efficient coherent interfaces to various types of quantum computers (atoms, solid-state, microwave...).

Quantum networks for efficient links between many quantum memories, high-speed quantum teleportation, cryptography, and modular quantum computing.

Small quantum networks are connected into global "quantum internet" whose functions, beyond secure communication and parallel computing, will include many other applications, including quantum digital signatures, quantum voting and secret sharing, anonymous transmission of classical information, and a host of sensing and metrology applications.

Publically released report: http://www.acq.osd.mil/rd/basic_research/references/workshops.html