Will Quantum Always Remain Basic Research or is it Ready to Power Great Products?

Optical Fiber Communication Conference

Rump Session

Chris Cole, Moderator

Adviser, II-VI Incorporated

8 March 2022

Han

Solo

OFC

II-VI

7:30 – 7:35

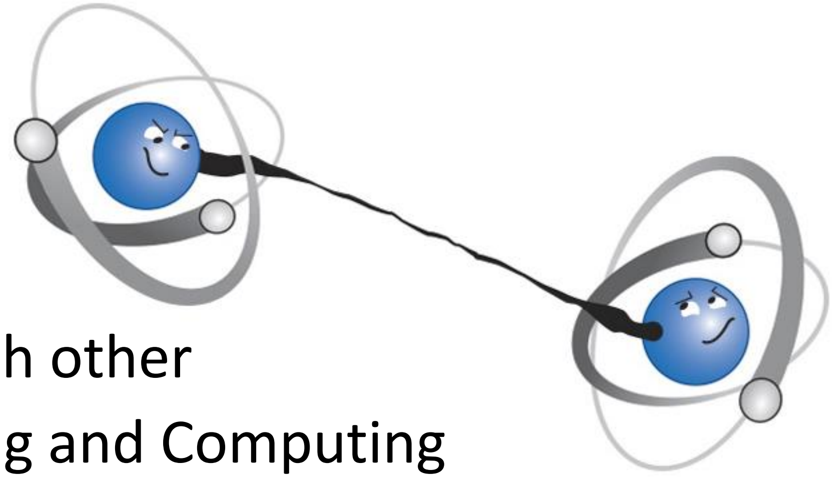
Quantum Topics in Rump Session Presentations

In the Presentations	Not in the Presentations
• Networking, for example: o Quantum Computing Platform (QCP) Networking o Quantum Information Processing (QIP) Networking • Cryptography, for example: o Quantum Key Distribution (QKD) o Quantum Error Correction (QEC) o Quantum Safe Cryptography (QSC)	• Sensing, for example: o Superconducting Quantum Interference (SQUID) Magnetometer o Optical Lattice Clock (OLC) o Challenging, but not controversial • Computing, for example: o Qubits o Quantum Processing Unit (QPU) o Controversial, but not a great OFC fit

- There is broad agreement about the science
- The debate is about feasibility, practicality, and timeliness of commercialization

Quantum Enthusiasts vs. Sceptics Teams Debate Format

- Moderator, Chris Cole, and Co-Moderator, Emina Soljanin, introduce the Session
- Followed by alternating Quantum Enthusiasts vs. Sceptics Team Member debates
- Each Provocateur gets 5 mins to present
- The audience then gets 5 mins to give:
  - tough and provocative questions
  - insightful comments
  - different perspectives
  - short, concise and to the point remarks
  - challenge the Moderators, Provocateurs and each other
  - any topic is fair game, including Quantum Sensing and Computing
- May Quantum Entanglement (the Force) be with you



Quantum Rump Session Schedule

PPT start	Q&A start	Name	Affiliation	Character	PPT start	Q&A start	Name	Affiliation	Character
Unentangles the Sides		Moderator			Balances the Force		Co-moderator		
7:35	n/a	Chris Cole	II-VI	Han Solo	7:40	7:45	Emina Soljanin	Rutgers University	Maz Kanata
Light Side Serves the Force		Quantum Enthusiasts Team Jedi Knight			Dark Side Opposes the Force		Quantum Sceptics Team Sith Lord		
7:50	7:55	Bruno Huttner	ID Quantique	Mace Windu	8:00	8:05	Peter Winzer	Nubis Comm.	Darth Sidious
8:10	8:15	Yong Zhao	Quantum CTek	Qui-Gon Jinn	8:20	8:25	Charles Clancy	MITRE	Darth Maul
8:30	8:35	Andrew Lord	British Telecom	Obi-Wan Kenobi	8:40	8:45	Glenn Wellbrock	Verizon	Darth Vader
8:50	8:55	Mekena Metcalf	Lawrence Berkeley Lab	Skywalker Ren	9:00	9:05	Takehisa Iwakoshi	Mie University	Kylo Ran
9:10	9:15	Inder Monga	ESnet	Yoda	9:20	9:25	Scott Hamilton	MIT Lincoln Laboratory	Count Dooku
9:30	9:35	Audience Poll			9:35	n/a	End		

QKD Entangled in Noisy (Down) Time

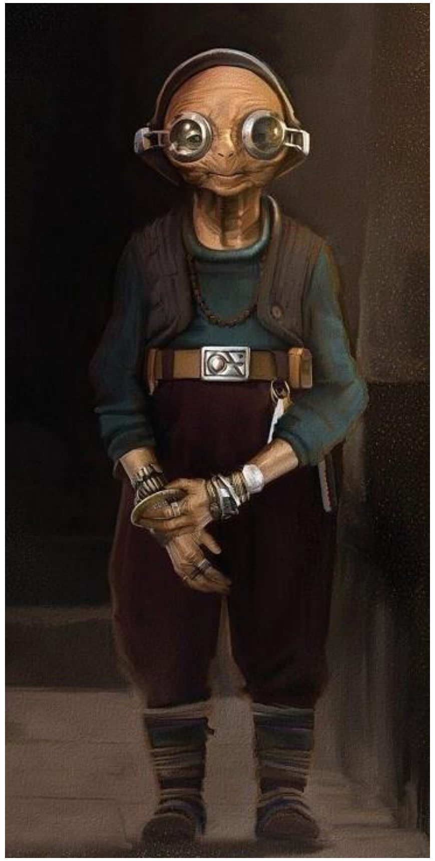
Emina Soljanin, Co-moderator

Professor, Electrical and Computer Engineering

Rutgers University

8 March 2022

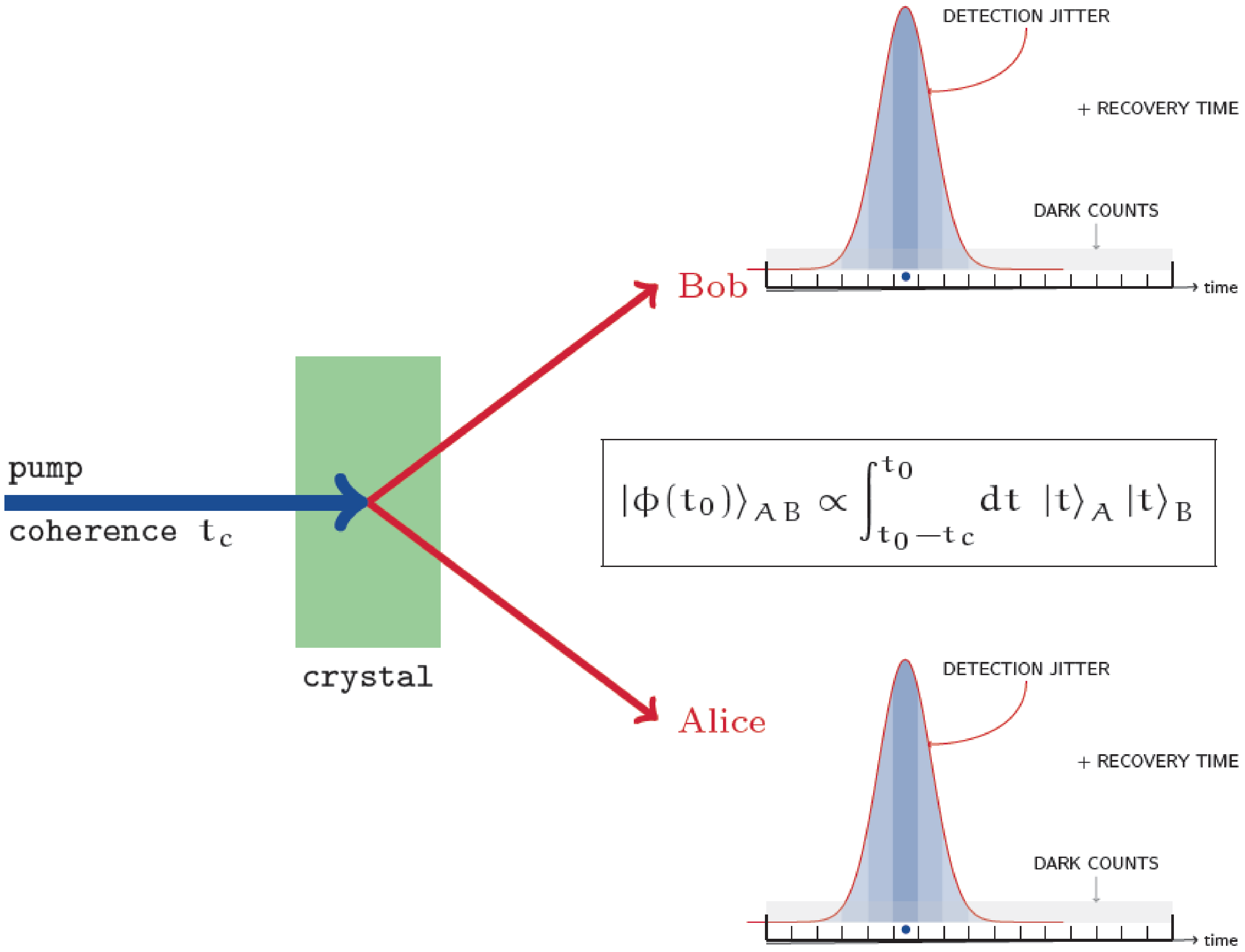
Maz
Kanata



“Maz has felt the Force ebb and flow, seeking an elusive balance between darkness and light.”

7:40 – 7:45

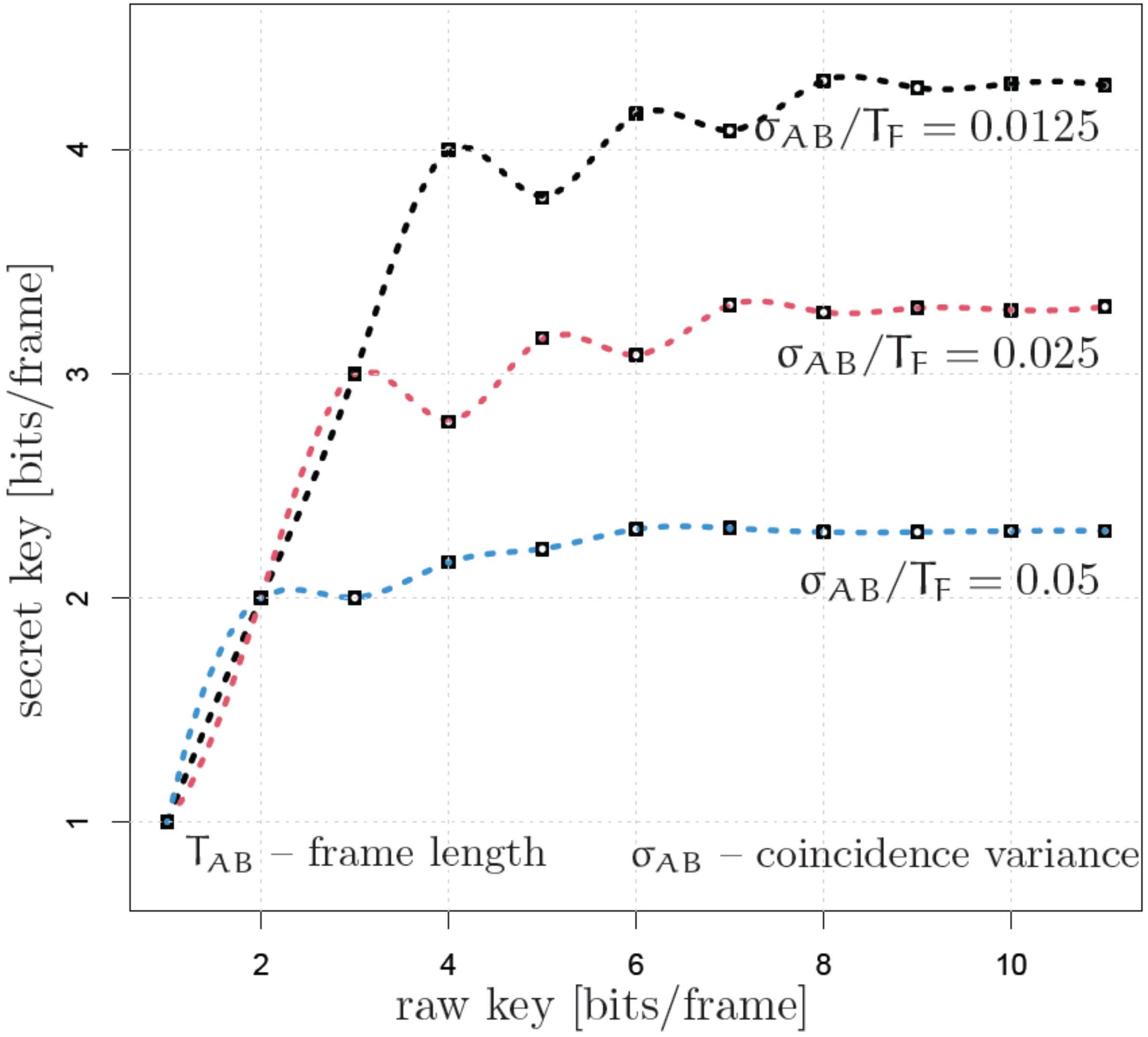
Time Carries Many Bits but Detectors Cannot Tell



$$|\phi(t_0)\rangle_{AB} \propto \int_{t_0-t_c}^{t_0} dt\ |t\rangle_A\, |t\rangle_B$$

- A special source generates time-entangled photon pairs
- Entangled photons arrive to Alice & Bob simultaneously
- Alice & Bob detect photon arrivals by imperfect detectors
- The raw key is extracted from “coincidental” arrival times

High Raw Key Rate Does not Mean High Secret Key Rate



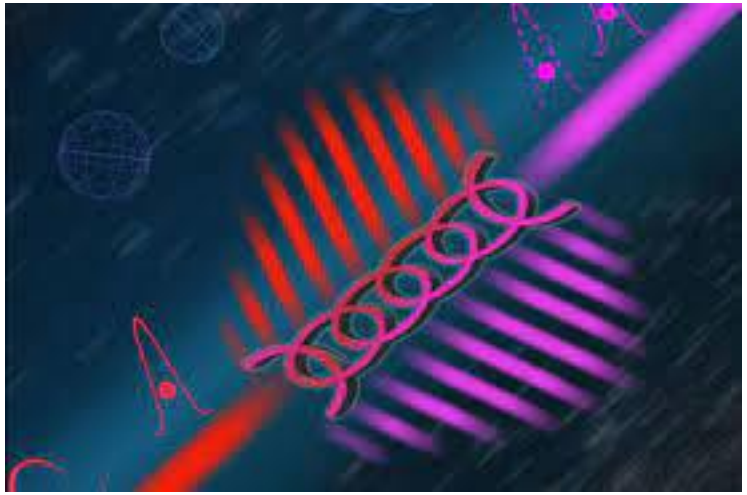
Raw-key is extracted by time binning

- the smaller the time bin
- the higher the raw key rate
- the more Alice & Bob disagree
- the more bits must be sent over the public channel for key reconciliation

<u>The secret key rate becomes saturated</u>

Can time-entanglement QKD live up to its promise?

vs.

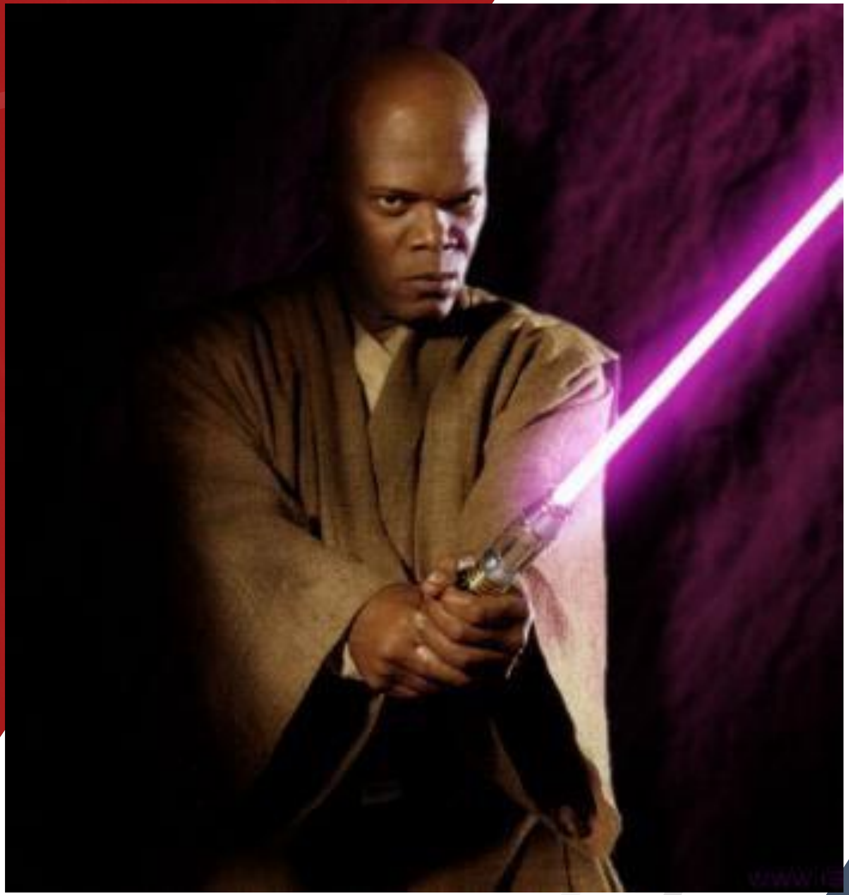


Mace Windu vs. Darth Sidious

Quantum is Already Powering Great Products

Bruno Huttner
Director of Quantum
Strategic Initiatives

ID Quantique



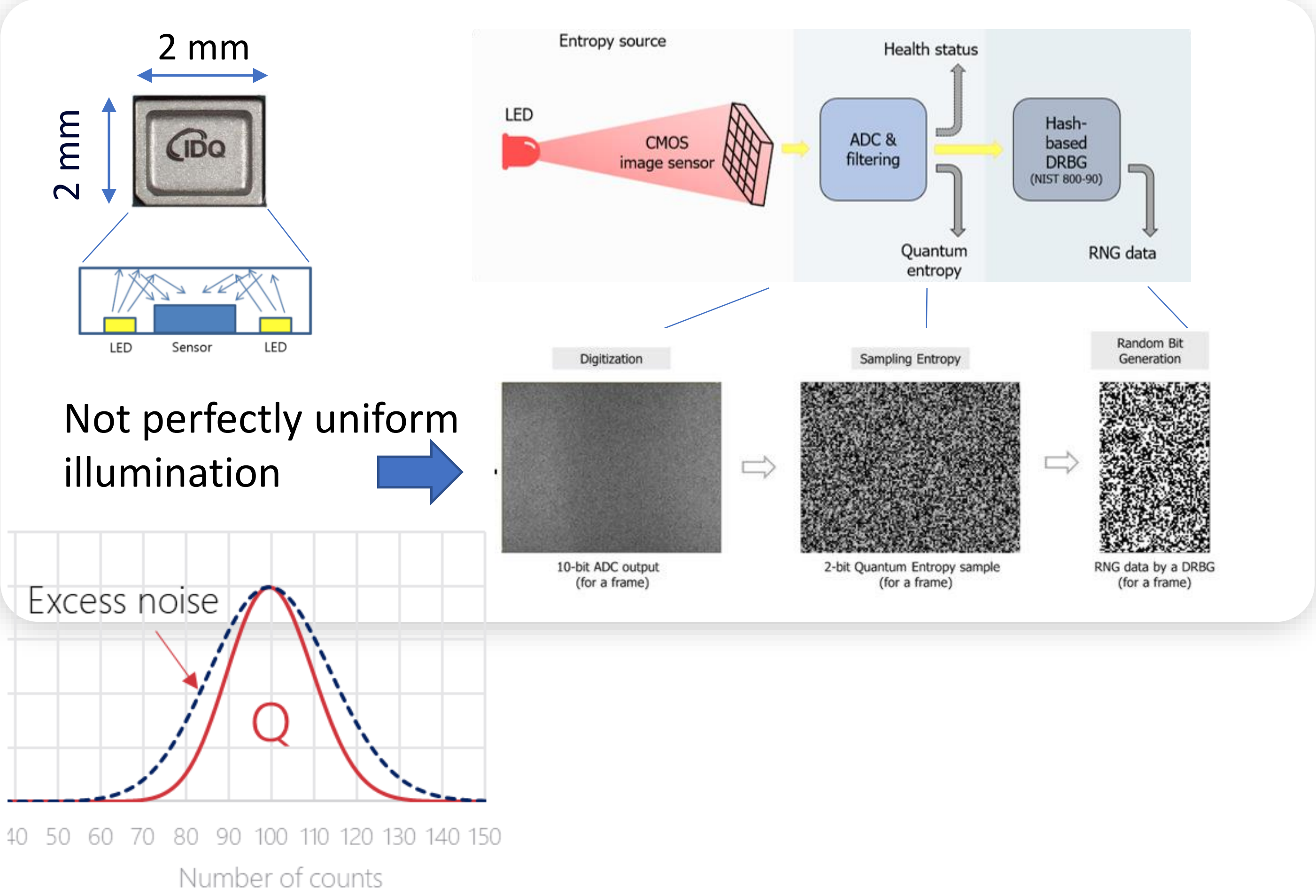
Mace Windu

March 2022

7:50 – 7:55

Quantum at Small Scale

Quantum-based Randomness for all Your Appliances

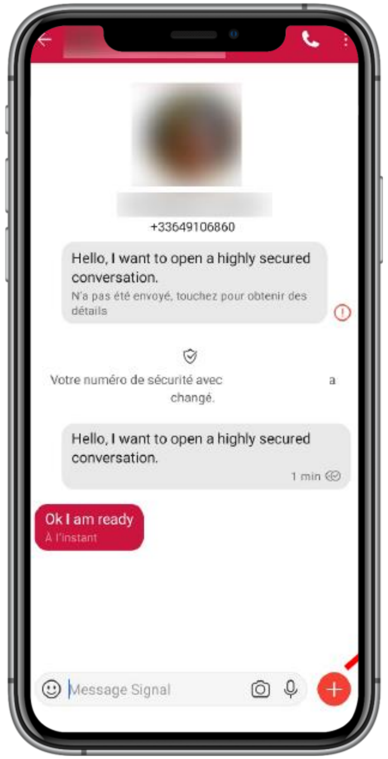


Not perfectly uniform illumination

Application Example:

Quantum-Safe Messaging with Quantum Random Number Generator (QRNG) and added PQC layer

CRYPTONEXT SECURITY



+33649106860

Hello, I want to open a highly secured conversation.

N'a pas été envoyé, touchez pour obtenir des détails

Votre numéro de sécurité avec a changé.

Hello, I want to open a highly secured conversation.

1 min

Ok I am ready

À l'instant

The first products for mass applications are already available

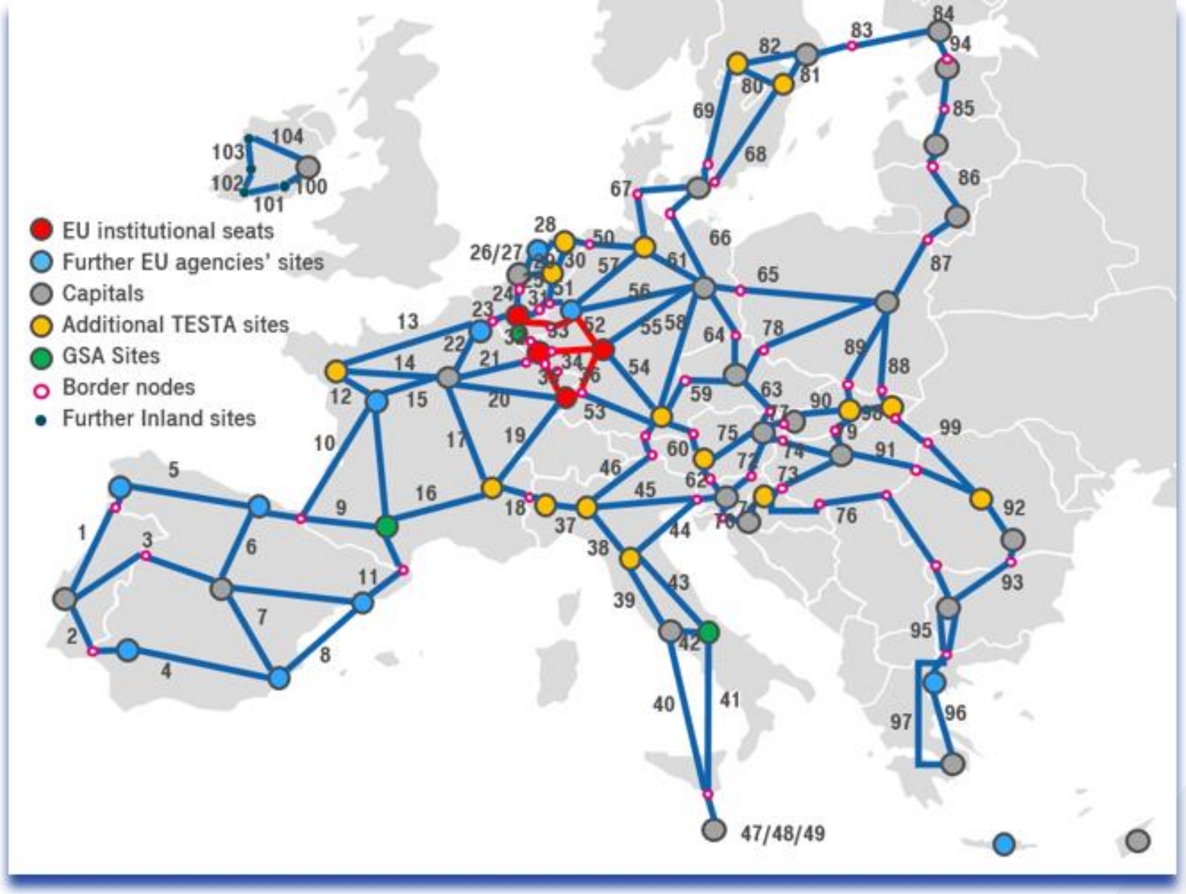
Quantum at Large Scale

EU Quantum Communication Infrastructure (QCI) Initiative

- Part of EU Cybersecurity Strategy
- Protects sensitive data and infrastructures
- Terrestrial and space components
- Integrates into existing infrastructure

QCI Timeline

- Preliminary phase (2020-2022):
  OpenQKD consortium and QKD Testbeds
- 1st phase (2022-2023): National Phases
- 2nd phase (2024 and beyond): Roll out
- Fully operational by 2027



Pan-European quantum keys will be available for all

Quantum to the Masses

The first products are already available…

and it is only the beginning!

Quantum Technologies: Fund-Raising Through Fear

Peter Winzer, Founder and CTO

8 March 2022

Darth Sidious

8:00 – 8:05

A Brief History of Technology Adoption

Technology	Research	Large-Scale Commercial	Lag [Years]
Transistor	1947	1953	6
Optical Fiber	1965	1976	11
Distributed Feedback Laser	1972	1987	15
Ethernet	1973	1983	10
Erbium-Doped Fiber Amplifier	1986	1990	4
Digital Coherent Detection	1991	2008	17
Fusion Reactors	1947	None	>75
Quantum Computing	1980	None	>41
Quantum Key Distribution	1984	None	>38

Apriori Network Systems

https://www.apriorinetwork.com/

Experimental demonstration of a 4,294,967,296-QAM-based Y-00 quantum stream cipher template carrying 160-Gb/s 16-QAM signals

Xi Chen,[1,*] Ken Tanizawa,[2] Peter Winzer,[3] Po Dong,[3] Junho Cho,[1] Fumio Futami,[2] Kentaro Kato,[2] Argishti Melikyan,[1] and K. W. Kim[1]

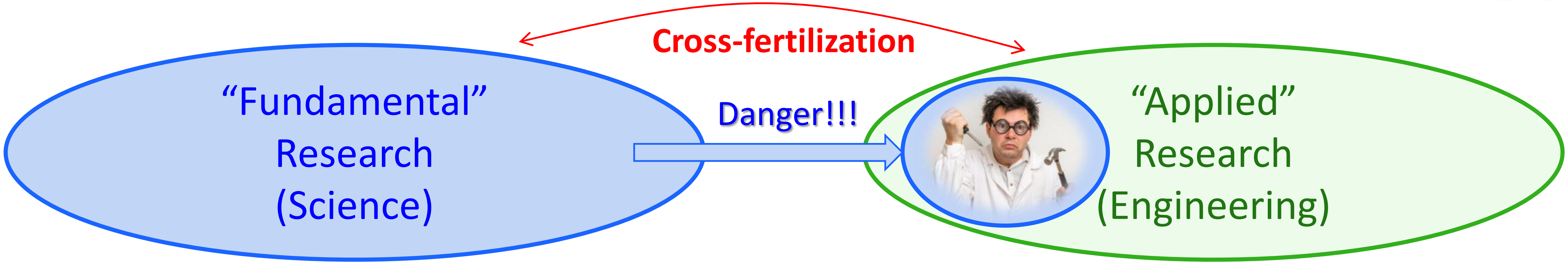
Fundamental research vs. real-world solutions for real-world needs

- Research fund-raising based on public fear-raising
- Example QKD: Security = Secure Key + Secure Encryption Algorithm

Existing solutions are sufficient
Alternative solutions exist

Not solved by QKD
(only known secure algorithm is the One-Time Pad)

Science vs. Engineering – And the Danger Zone



Cross-fertilization

"Fundamental" Research (Science)

Danger!!!

"Applied" Research (Engineering)

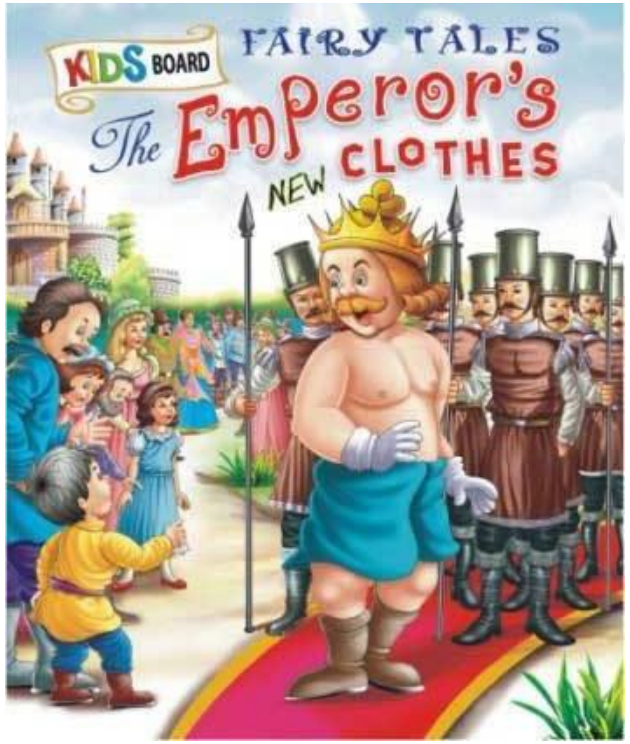
Ultimate goal:

Discovery:

understanding the world

Does *not* need any justification (particularly fear-raising!)

Society chooses to afford it



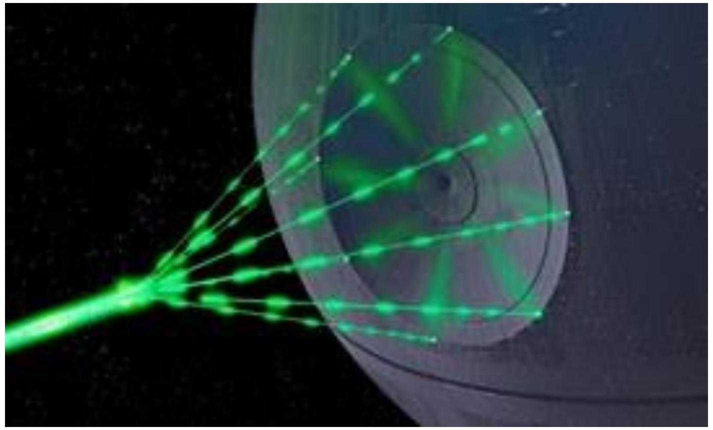
Ultimate goal:

Invention:

changing the world

Must have a practical justification

Paid for by technical innovations



nubis communications

Thank You !

Qui-Gon Jinn vs. Darth Maul

Quantum is Powering Great Products!

Dr. Yong Zhao
Vice Chairman of the Board
QuantumCTek Co., Ltd.

8 March 2022

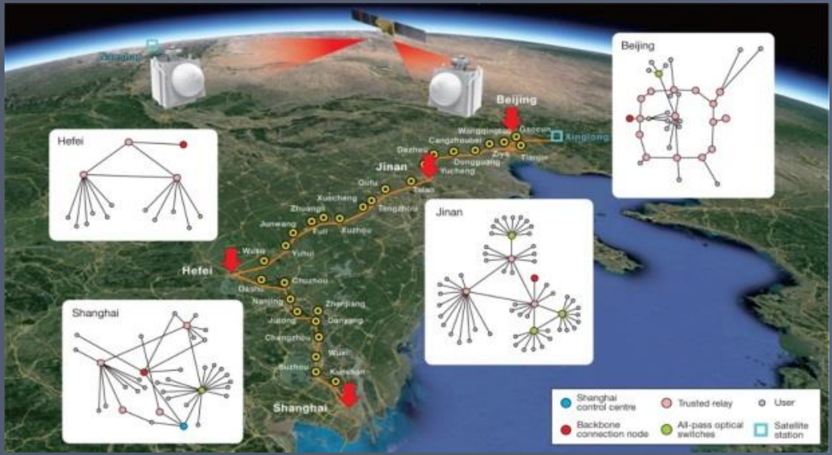
Qin-Gon Jinn

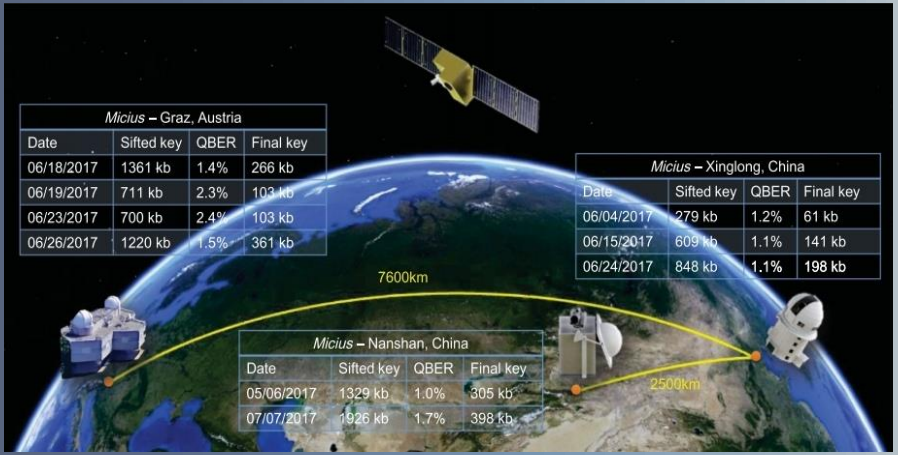
8:10 – 8:15

Great Products are Happening

国盾量子 QuantumCTek

Quantum Secured Infrastructure — Q-Crypto Networks



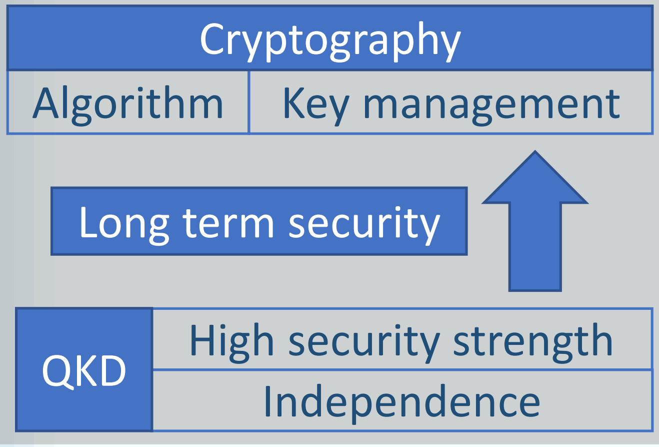


Micius – Graz, Austria			
Date	Sifted key	QBER	Final key
06/18/2017	1361 kb	1.4%	266 kb
06/19/2017	711 kb	2.3%	103 kb
06/23/2017	700 kb	2.4%	103 kb
06/26/2017	1220 kb	1.5%	361 kb

Micius – Xinglong, China			
Date	Sifted key	QBER	Final key
06/04/2017	279 kb	1.2%	61 kb
06/15/2017	609 kb	1.1%	141 kb
06/24/2017	848 kb	1.1%	198 kb

Micius – Nanshan, China			
Date	Sifted key	QBER	Final key
05/06/2017	1329 kb	1.0%	305 kb
07/07/2017	1926 kb	1.7%	398 kb

The first stage —— QKDN



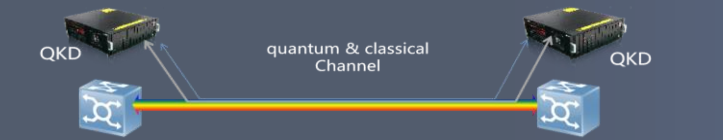
Cryptography

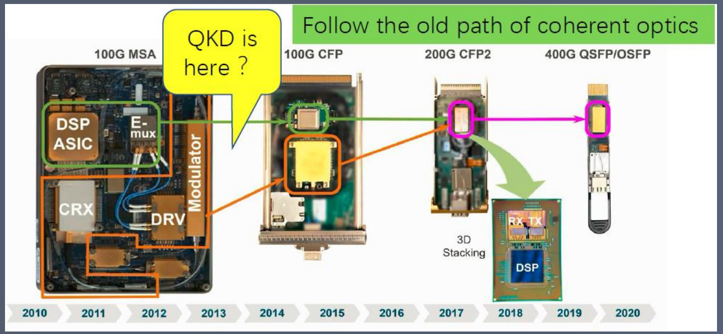
Algorithm | Key management

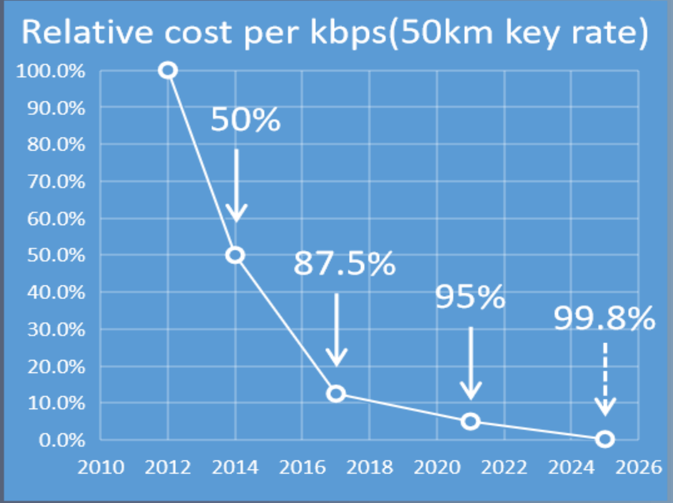
Long term security

QKD | High security strength | Independence

Integrated & Cost-effective







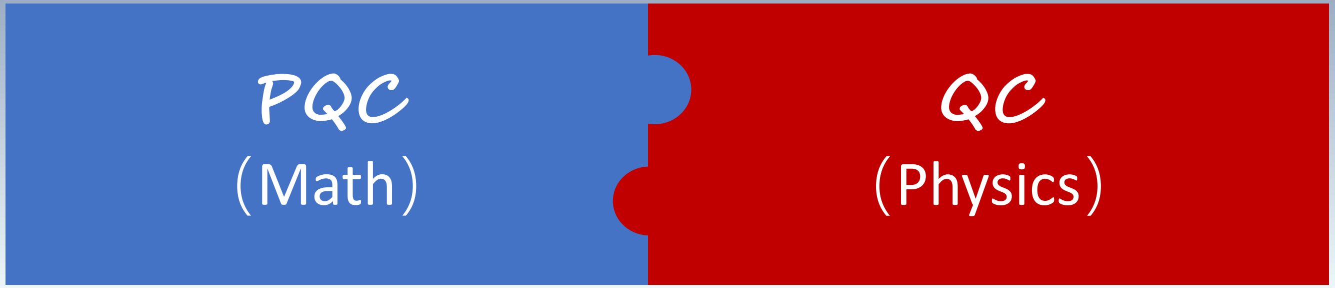
Standardized, Certified & Reliable

ITU ISO IEC ETSI

No Single Technology can Defeat All Security Threats

QKD security is theoretically clear **VS** PQC security is theatrically uncertain: security ≠ mathematical problem complexity

Both QKD and PQC need more testing and analysis, and both improve with the back and forth of attack and defense



PQC
(Math)

QC
(Physics)

May the Quantum Be With You

Security: E2E with PQC

T. Charles Clancy, Ph.D.

Fellow of the IEEE

SVP, MITRE Corporation

8 March 2022

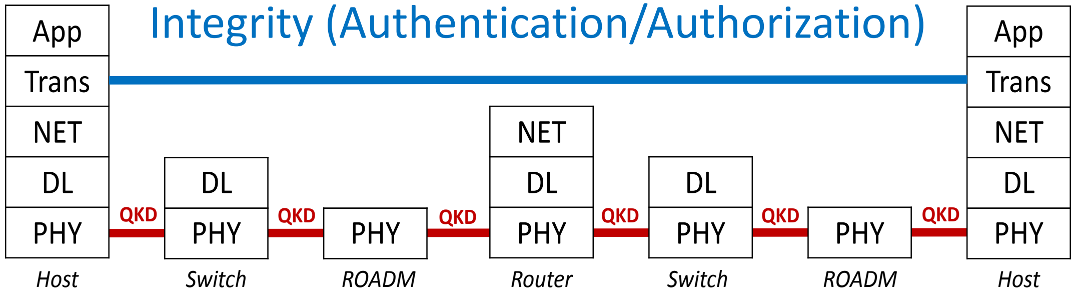
MITRE

Darth
Maul

8:20 – 8:25

Security Must be End to End

Transport Layer Security (TLS) + PQC - E2E - Confidentiality, Integrity (Authentication/Authorization)



Hop-by-Hop Only, Confidentiality Only

QKD:
- Forward Secrecy
- Unconditional Security
- Requires Independent Unconditionally Secure Authentication
- Vulnerable to MITM

TLS + PQC:
- Authentication and Key Agreement
- Forward Secrecy (for most ciphers)
- Security conditioned on P≠NP
- TLS itself has history of vulnerabilities

Survey of TLS vulnerabilities, July 2021, *Wikipedia*

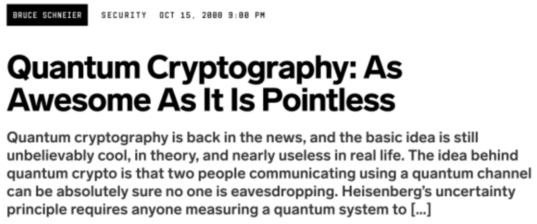
Attacks	Security			
	Insecure	**Depends**	**Secure**	**Other**
Renegotiation attack	0.1% support insecure renegotiation	<0.1% support both	99.2% support secure renegotiation	0.7% no support
RC4 attacks	0.4% support RC4 suites w/ modern browsers	6.5% support some RC4 suites	93.1% no support	N/A
TLS Compression (CRIME attack)	>0.0% vulnerable	N/A	N/A	N/A
Heartbleed	>0.0% vulnerable	N/A	N/A	N/A
ChangeCipherSpec injection attack	0.1% vulnerable and exploitable	0.2% vulnerable, not exploitable	98.5% not vulnerable	1.2% unknown
POODLE attack against TLS (against SSL 3.0 not included)	0.1% vulnerable and exploitable	0.1% vulnerable, not exploitable	99.8% not vulnerable	0.2% unknown
Protocol downgrade	6.6% Downgrade defence not supported	N/A	72.3% Downgrade defence support	21.0% unknown

Focus on PQC for Quantum Safe Cryptography

- QKD does not actually address the Internet threat model
- PQC does, and should be the focus for building quantum-safe security for the Internet
- Bruce Schneier, WIRED Security, Oct. 15, 2008:

Quantum Cryptography: As Awesome As It Is Pointless

… as awesome and pointless as a double-bladed light saber.



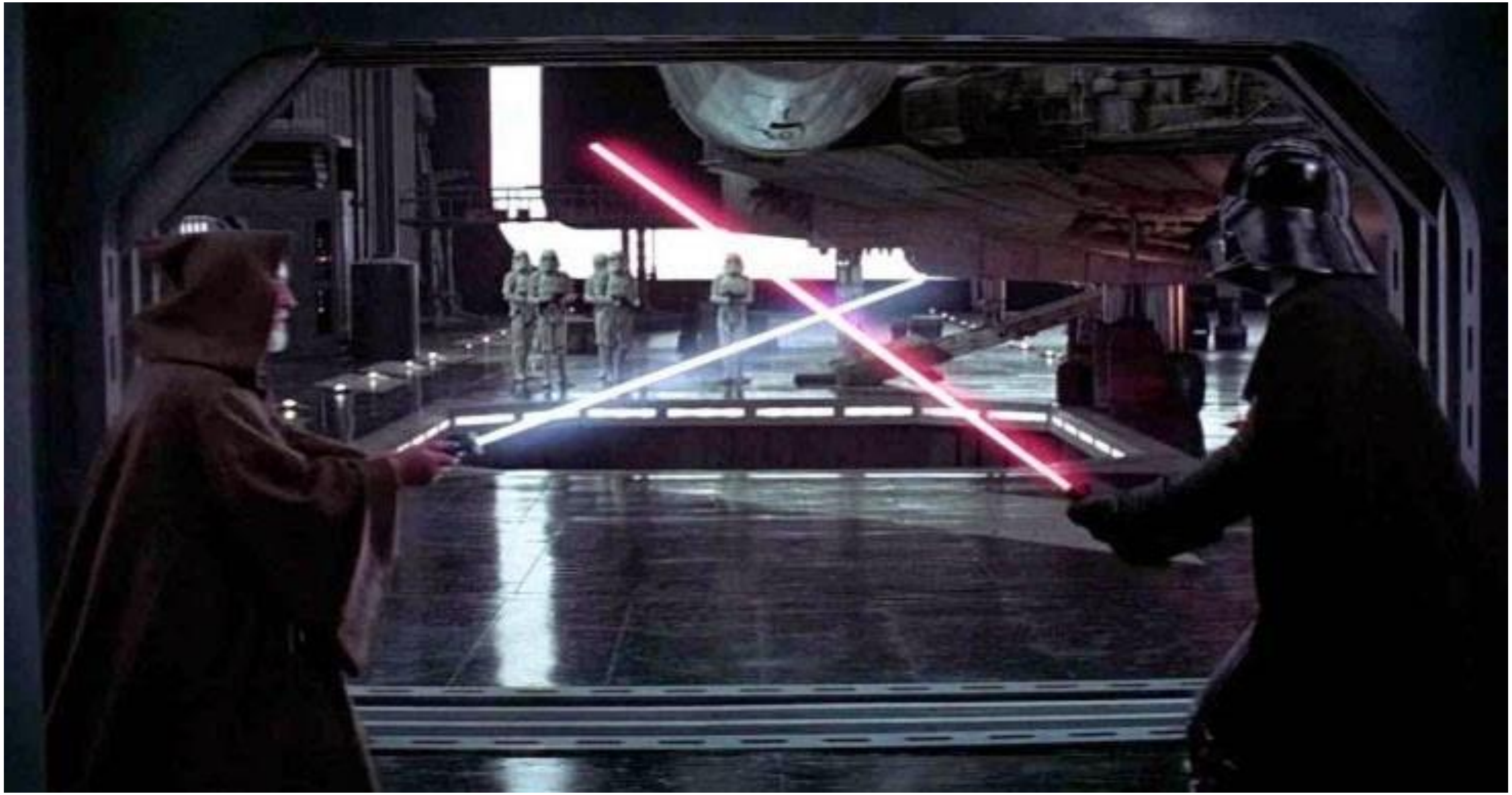
BRUCE SCHNEIER SECURITY OCT 15, 2008 9:00 PM

Quantum Cryptography: As Awesome As It Is Pointless

Quantum cryptography is back in the news, and the basic idea is still unbelievably cool, in theory, and nearly useless in real life. The idea behind quantum crypto is that two people communicating using a quantum channel can be absolutely sure no one is eavesdropping. Heisenberg's uncertainty principle requires anyone measuring a quantum system to […]

MITRE

Obi-Wan Kenobi vs. Darth Vader



QKD is a Steppingstone to a Quantum Internet

Andrew Lord
Sr. Manager of Optical Research, BT
Visiting Professor, Essex University

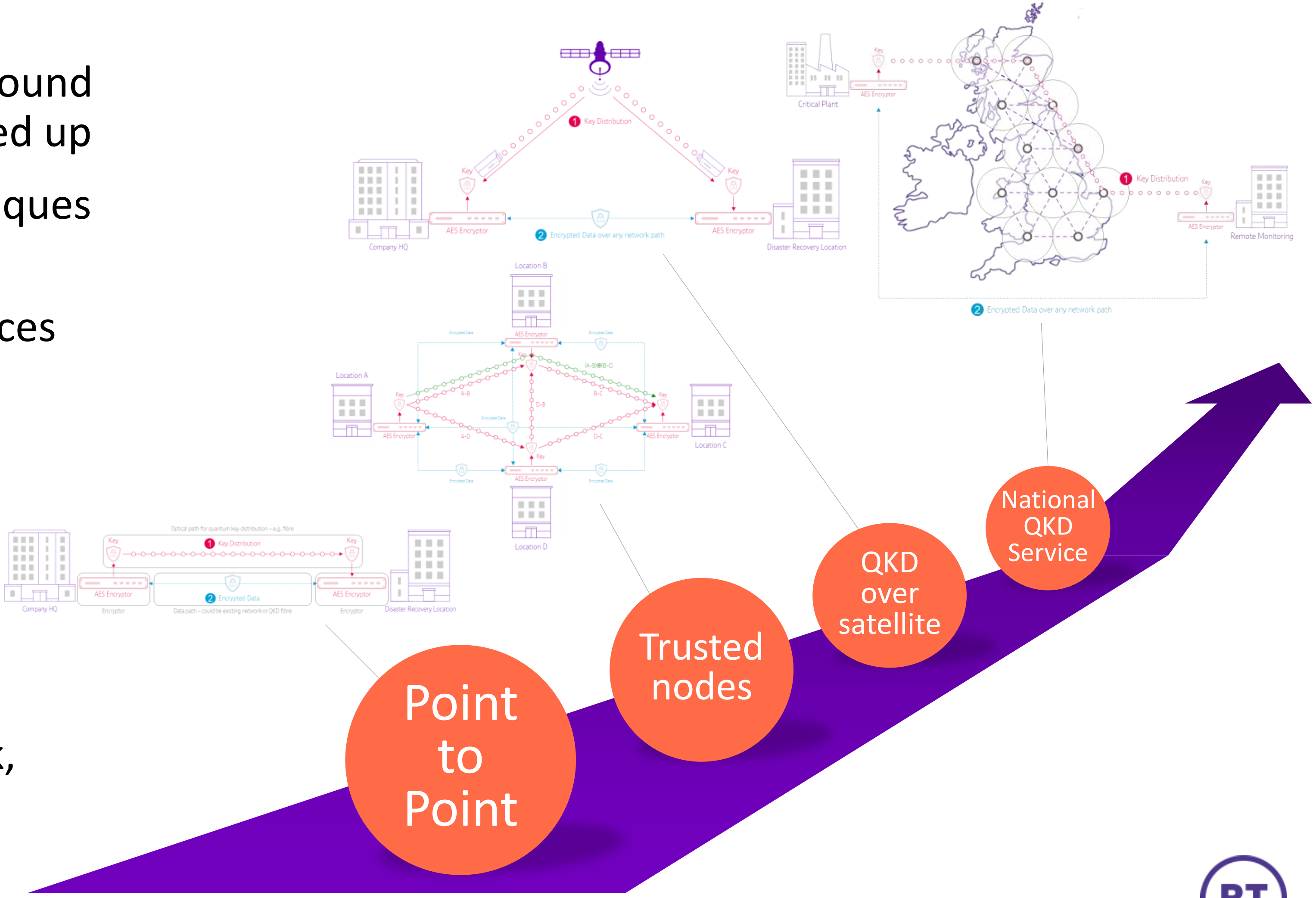
8 March 2022

Ben Obi-Wan Kenobi

8:30 – 8:35

QKD is Real, Secure and the First Step on the Quantum Trajectory

- BT launching a QKD network service around London in April 2022 – customers signed up
- Mathematical-based encryption techniques included (not an either-or)
- Quantum security enables selling services over lots of BT owned optical fibre.
- Mathematical crypto is not reliable:
  - RSA / DH already broken by Shor[1]
  - Lattice codes are under threat or already broken for all we know
  - Backdoors are built-in
- Trajectory towards a quantum network, interconnecting quantum and classical compute resources

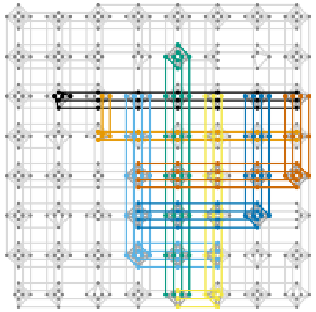


[1] Peter W. Shor, "Algorithms for quantum computation: discrete logarithms and factoring". Proceedings 35th Annual Symposium on Foundations of Computer Science, Nov. 1994.

The Quantum Force is With Us Now

QKD Supports the BT Ambition to be the National Purveyor of Trust

https://arxiv.org/pdf/2006.14057.pdf
Two quantum Ising algorithms for the Shortest Vector Problem: one for now and one for later
David Joseph,[1, 2] Adam Callison,[2] Cong Ling,[1] and Florian Mintert[2]
[1] Electrical and Electronic Engineering Department, Imperial College London
[2] Physics Department, Imperial College London
Phys. Rev. A 103, 032433, 26 March 2021



logical qubits embedded as qubit chains (of physical qubits) into the chimera topology

Q&A
8:35 – 8:40

Universal Adoption is Key to Scalable Networking

Darth Vader

Glenn Wellbrock
Director, Optical Transport
Network Architecture,
Design and Planning
Verizon

8 March 2022

verizon✓

8:40 – 8:45

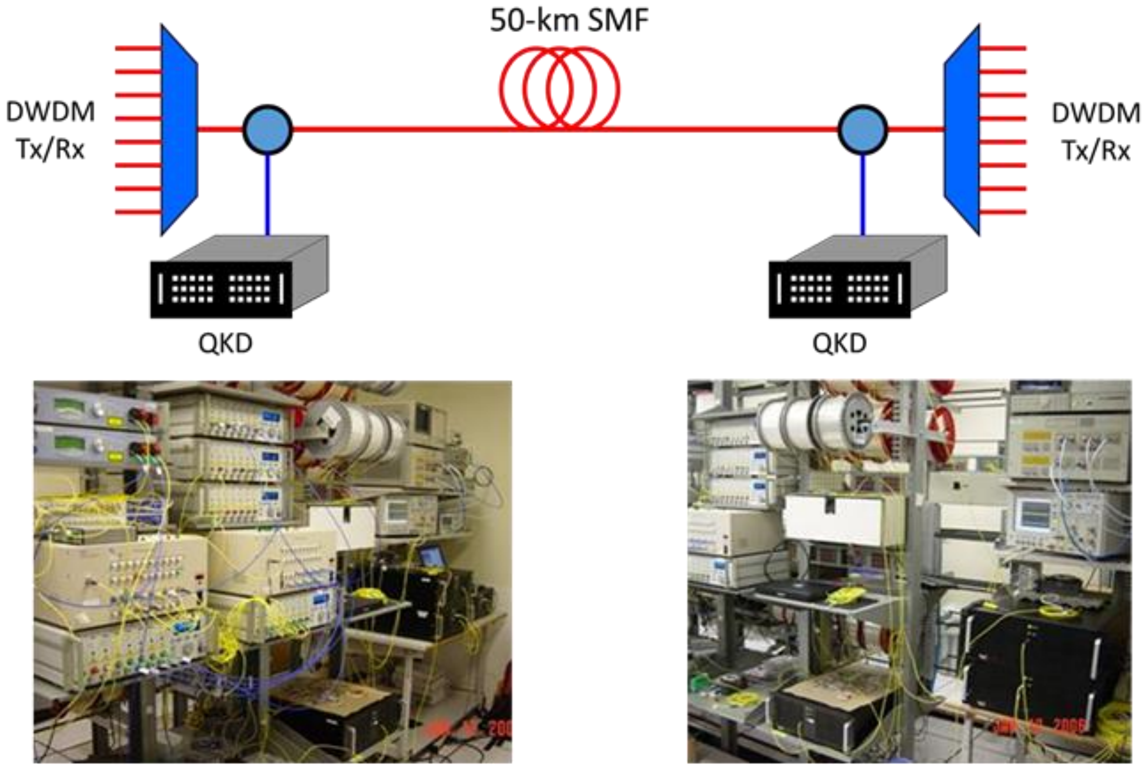
Practical = Great Products

- NISTIR 8309: Status Report on the Second Round of the NIST Post-Quantum Cryptography (PQC) Standardization Process
- Quantum-resistant cryptography (QRC)
- Standards based
- Resistant to classical and quantum computer code breaking (forward secrecy)
- Resistant to side-channel attacks
- Interoperable with existing communications protocols and networks
- Easily implemented with conventional electronics
- Drop-in replacement for exiting cryptography
- Universal, simple, flexible, free

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

Great Science ≠ Great Products

16-year-old Verizon QKD



Reference: TJ Xia and G. Wellbrock et al., OFC 2006, OTuJ7. (Ref-416)

Number sold to date by Verizon rhymes with Ziro (the Hutt)

Skywalker Rey vs. Kylo Ren

Building Blocks for a Quantum Internet

Mekena Metcalf
Applied Math and Computational Research Division, Berkeley Lab

8 March 2022

Skywalker Rey

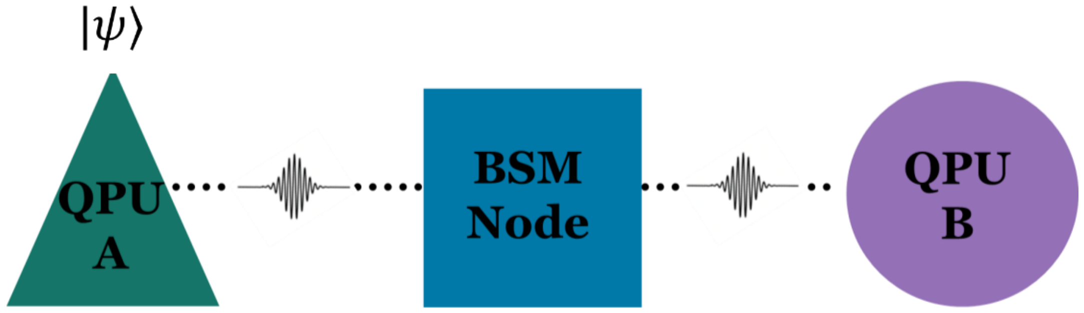
BERKELEY LAB

BERKELEY LAB
LAWRENCE BERKELEY NATIONAL LABORATORY

U.S. DEPARTMENT OF ENERGY

8:50 – 8:55

Bob and Alice Meet the Bell State



$|\psi\rangle$

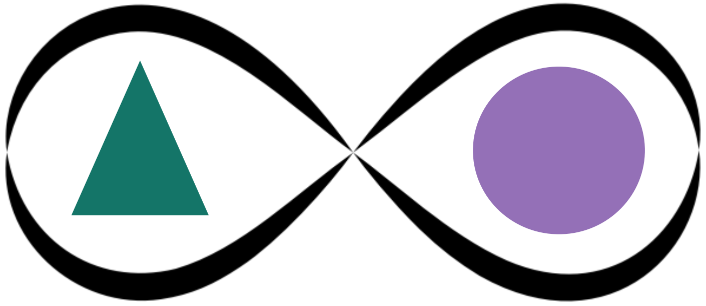
QPU A

BSM Node

QPU B

Quantum Revolution 2.0

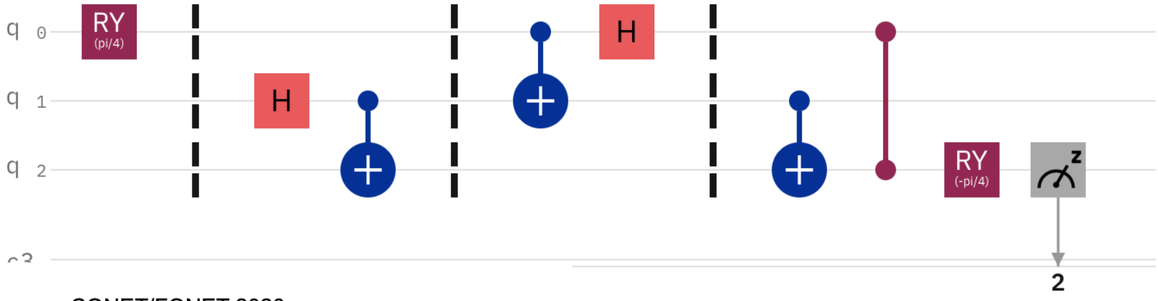
Put properties of quantum mechanics like *measurement, entanglement and superposition* to commercial use



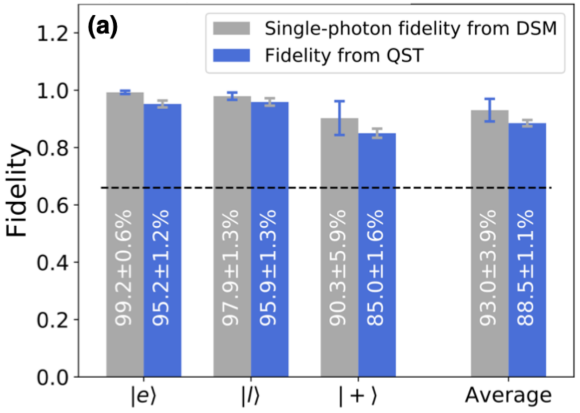
A Bell State is a maximally entangled state

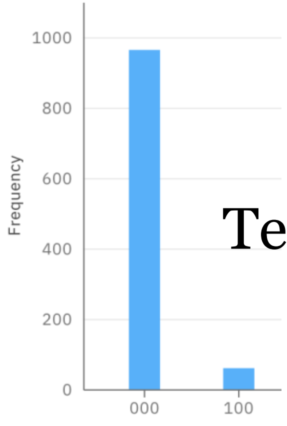
$$|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

Teleportation on IBM Montreal



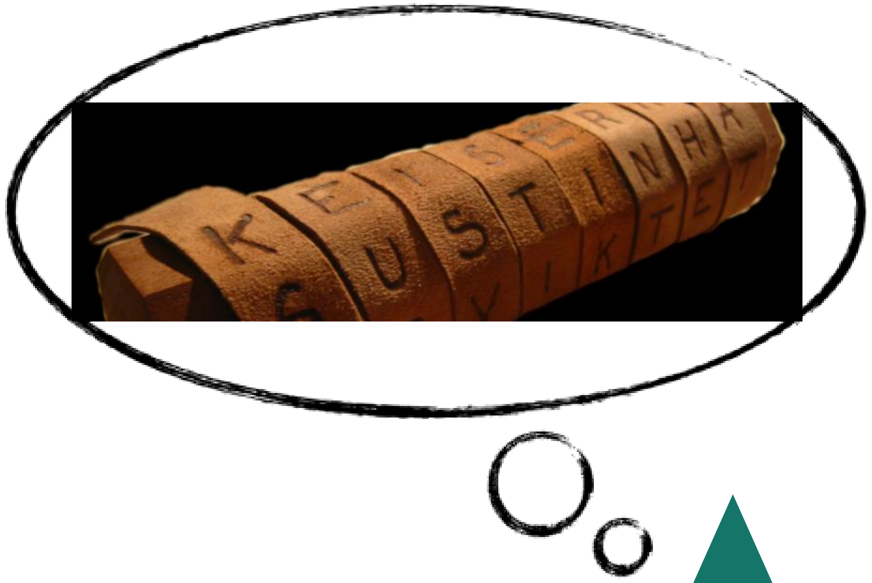
CQNET/FQNET 2020

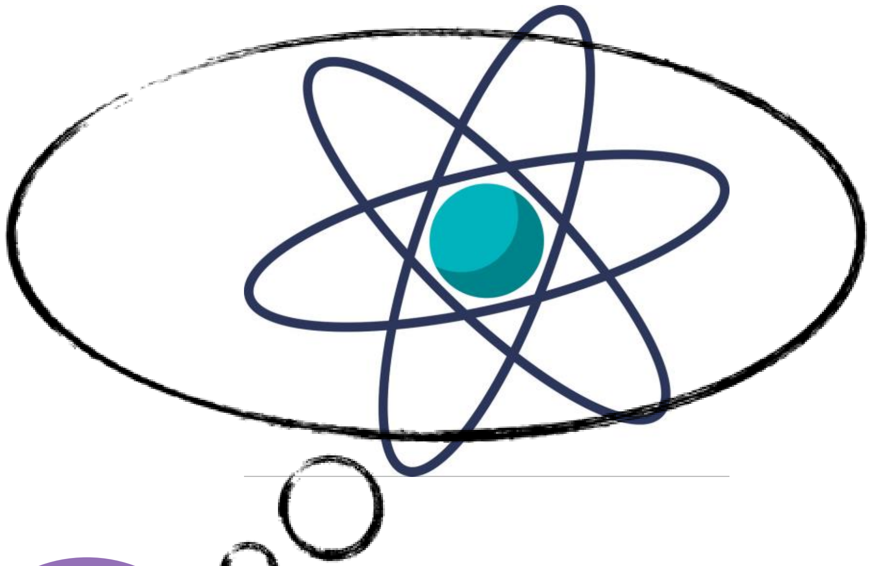


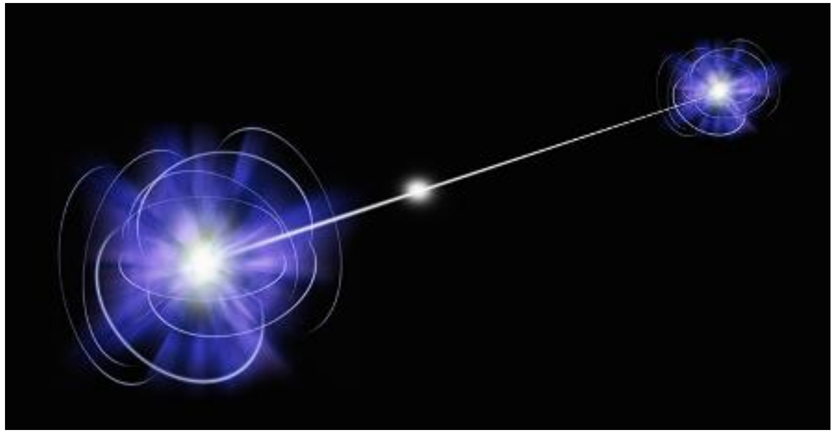


94% Accuracy/ Teleportation Fidelity

Stay in the Past or Join the Future?







Q&A
8:55 – 9:00

Quantum Networks and QKD Are Not Ready for Business

Kylo Ren (Ben Solo)

Takehisa Iwakoshi
Mie University
Dept. of Information Engineering
8 March 2022
iwakoshi@cs.info.mie-u.ac.jp

9:00 – 9:05

QKD Security is Not Proven

Experimental

- Impossible to prove the security of QKD systems because there are no attackers to launch collective/coherent attacks.
- Impossible to list all unknown device-imperfections and side-channels.

Theoretical

- Many researchers believe Shor and Preskill proved the equivalence of Prepare-and-Measure QKDs and Quantum-Error-Correction QKDs in 2000.
- Counter examples show the former can never supply IID keys for One-Time Pad, in Shannon sense, unlike the latter.

Cryptography Expert Consensus

- NSA/USA, ENISA/EU, NCSC/UK, ANSSI/France do not recommend QKD.
- For the whole system to be Information-Theoretic Secure (ITS), QKD requires ITS authentication procedures, which QKD cannot do standalone.
- QKD requires hardware patches and upgrades, unlike software cryptography.
- QKD is vulnerable to Denial-of-Service attacks because the signals are fragile.

QKD is not Practical

- QKD will remain in everlasting R&D phase with no products realized
- QKD researchers should investigate better approaches, for example: Y00 Quantum Cryptography using bright quantum states
- Detailed references and appendix: https://www.researchgate.net/publication/357791716

Fall into the Dark Side of the Quantum Force

Q&A
9:05 – 9:10

Yoda vs. Count Dooku

Quantum Communication (*teleportation*) Enables Scalable Quantum Computing

Inder Monga,
Executive Director,
Energy Sciences Network
Lead Principal Investigator,
Quantum Application
Network Testbed (quant-net)

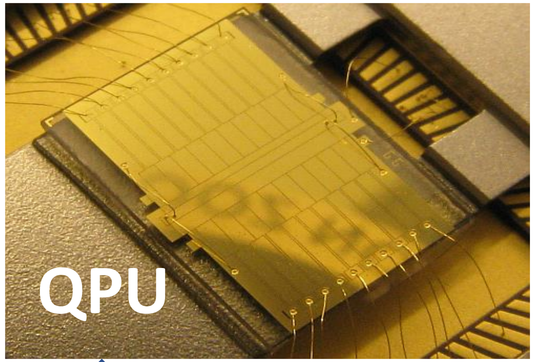
8 March 2020

Yoda

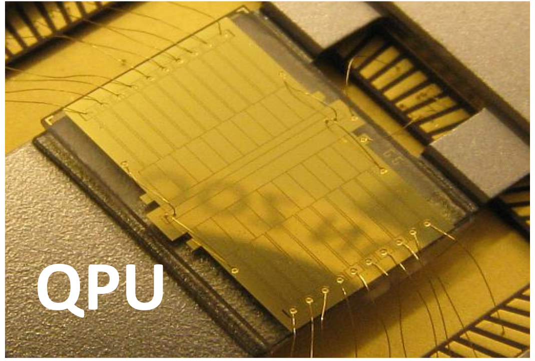
ESnet

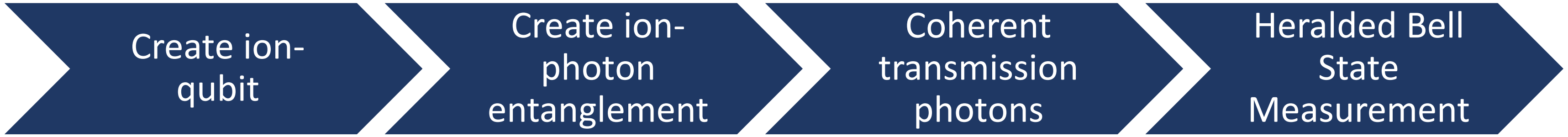
9:10 – 9:15

Quantum Teleportation transports quantum state



No-cloning Theorem determines architecture



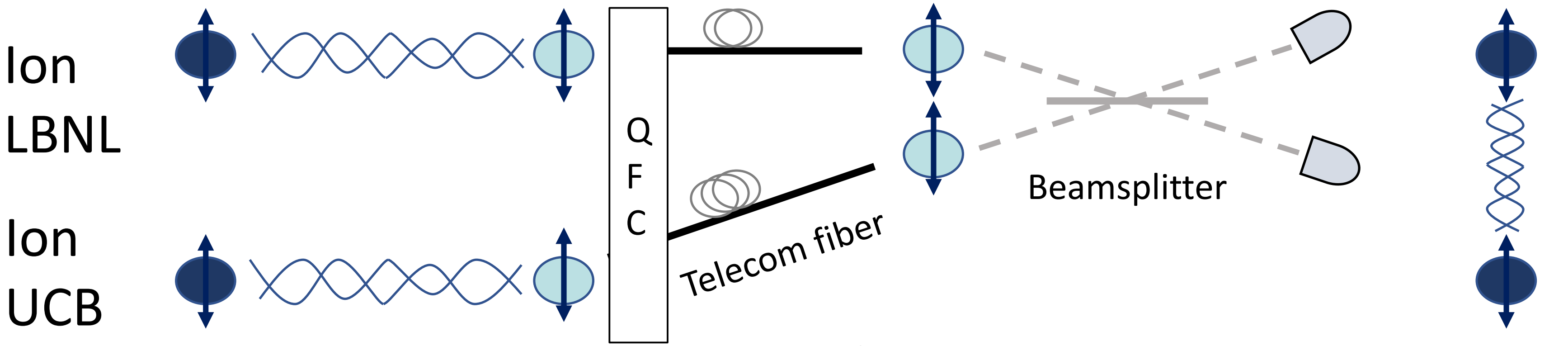


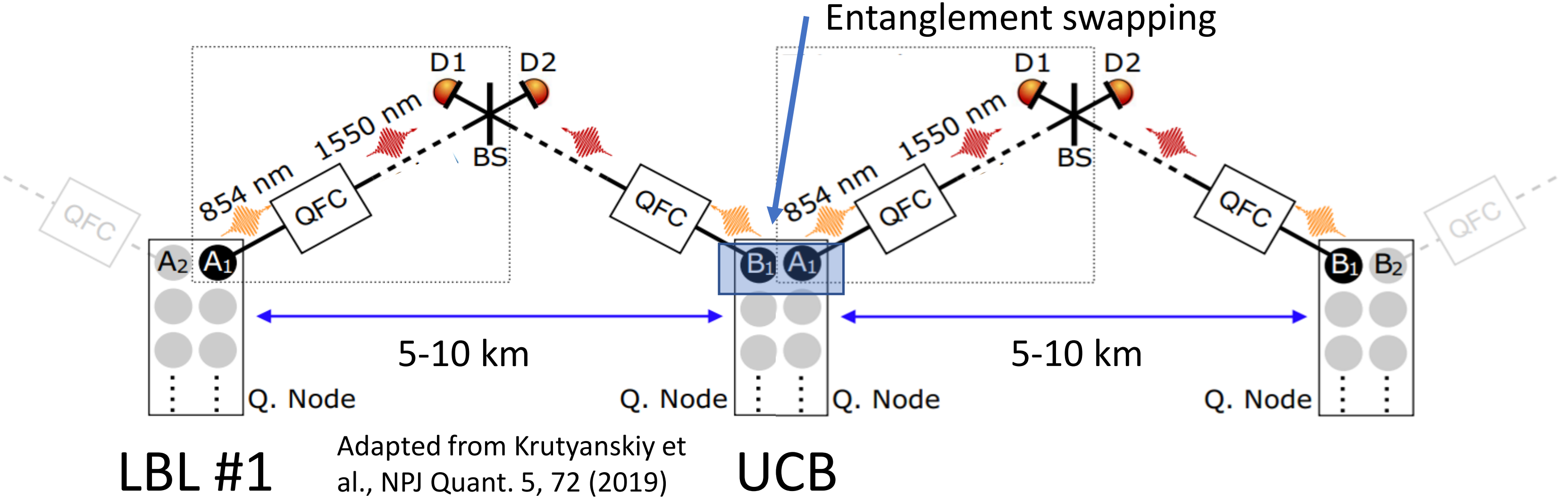
Create ion-qubit

Create ion-photon entanglement

Coherent transmission photons

Heralded Bell State Measurement





Adapted from Krutyanskiy et al., NPJ Quant. 5, 72 (2019)

Are we there yet?

Quantum Networking based on teleportation commercialization requires a new ecosystem of materials, processes, devices, components, sub-systems, systems and protocols.

Teleportation with ions: Riebe et al. Nature 429, 734 (2004), Barrett et al., Nature 429, 737 (2004)

ESnet

Quantum (Teleportation) Still Requires Basic Technology Development

Scott Hamilton
Leader, Optical Communications Technology Group
MIT Lincoln Laboratory

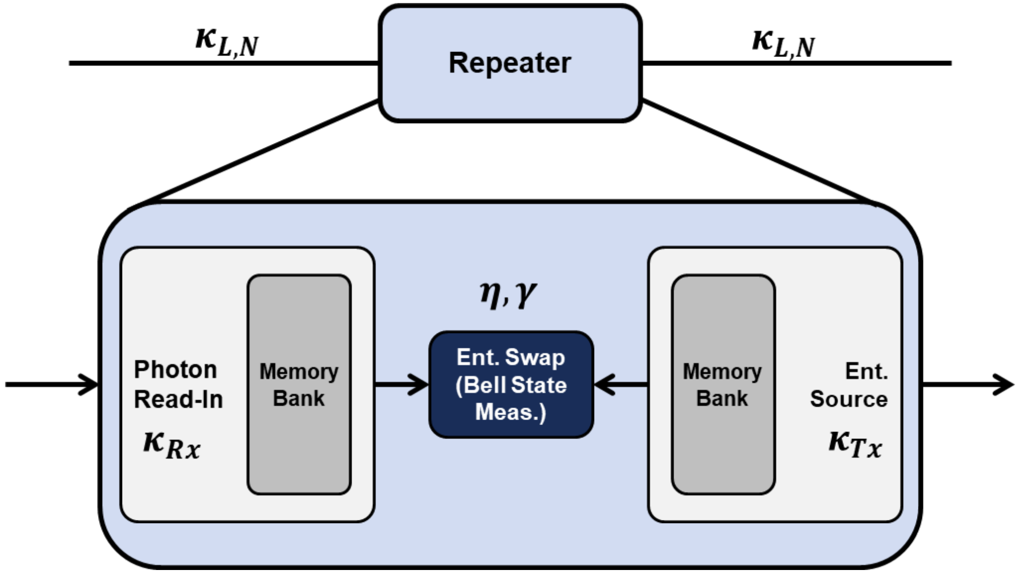
8 March 2022

1951–2021
LINCOLN LABORATORY
MASSACHUSETTS INSTITUTE OF TECHNOLOGY

Count Dooku

9:20 – 9:25

Should Industry Develop Distributed Quantum Networks?



$\kappa_{L,N}$ Repeater $\kappa_{L,N}$

Photon Read-In κ_{Rx}

Memory Bank

η, γ

Ent. Swap (Bell State Meas.)

Memory Bank

Ent. Source κ_{Tx}

- Each entanglement swap has usage efficiency $\boldsymbol{\eta}$
  - Limited memory, Bell State resolution
  - Total Rate: $\kappa_{L,N}\kappa_{Rx}\kappa_{Tx}\eta^N$
- Each BSM has fidelity efficiency $\boldsymbol{\gamma}$
  - Memory decoherence, heralding noise
  - Total Fidelity: $\sim\gamma^N$

Repeater Technology Options are Limited

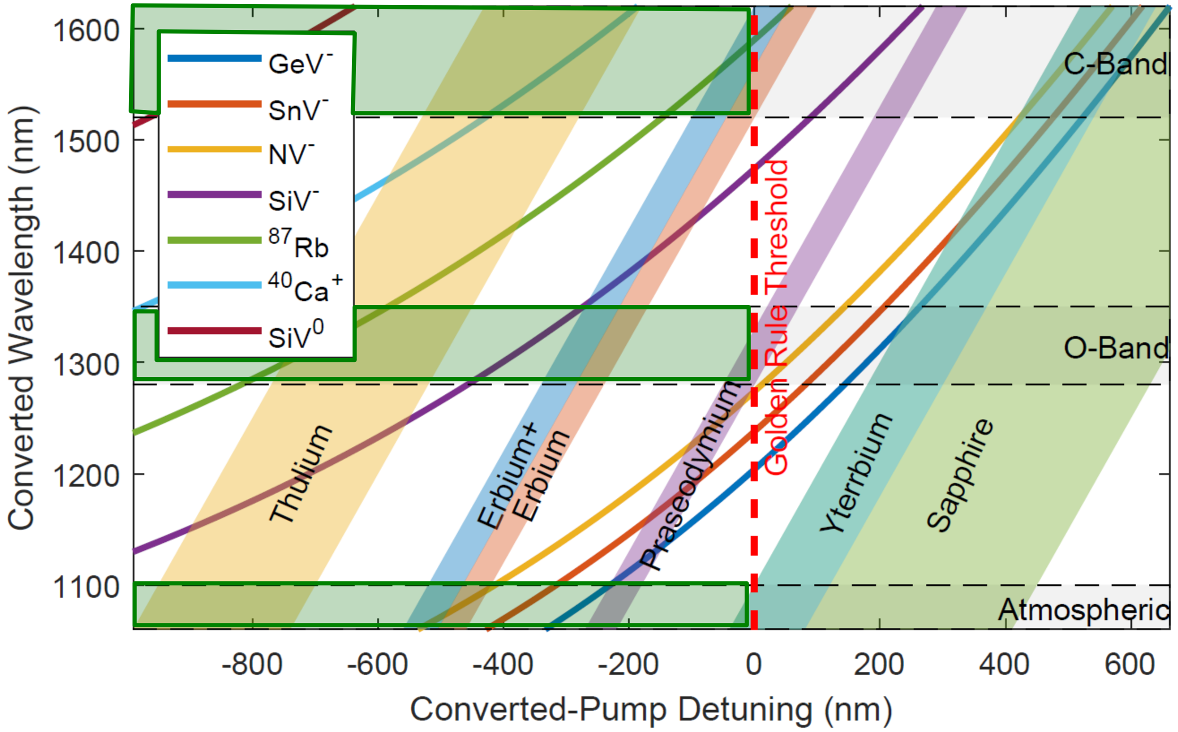
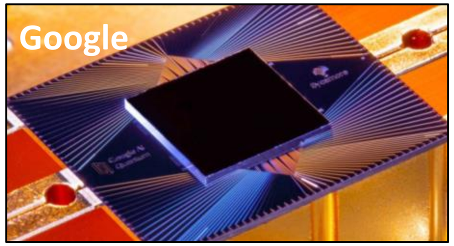


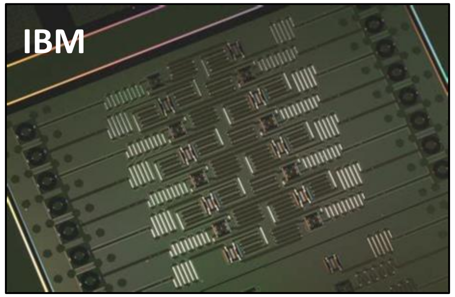
Figure courtesy of E. Bersin, MIT 2022

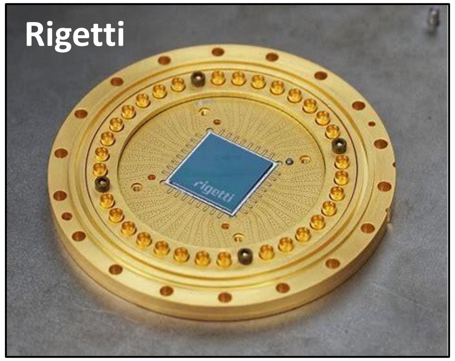
For distributed applications, we need to figure out how to build a repeater before Industry jumps into Quantum Network development

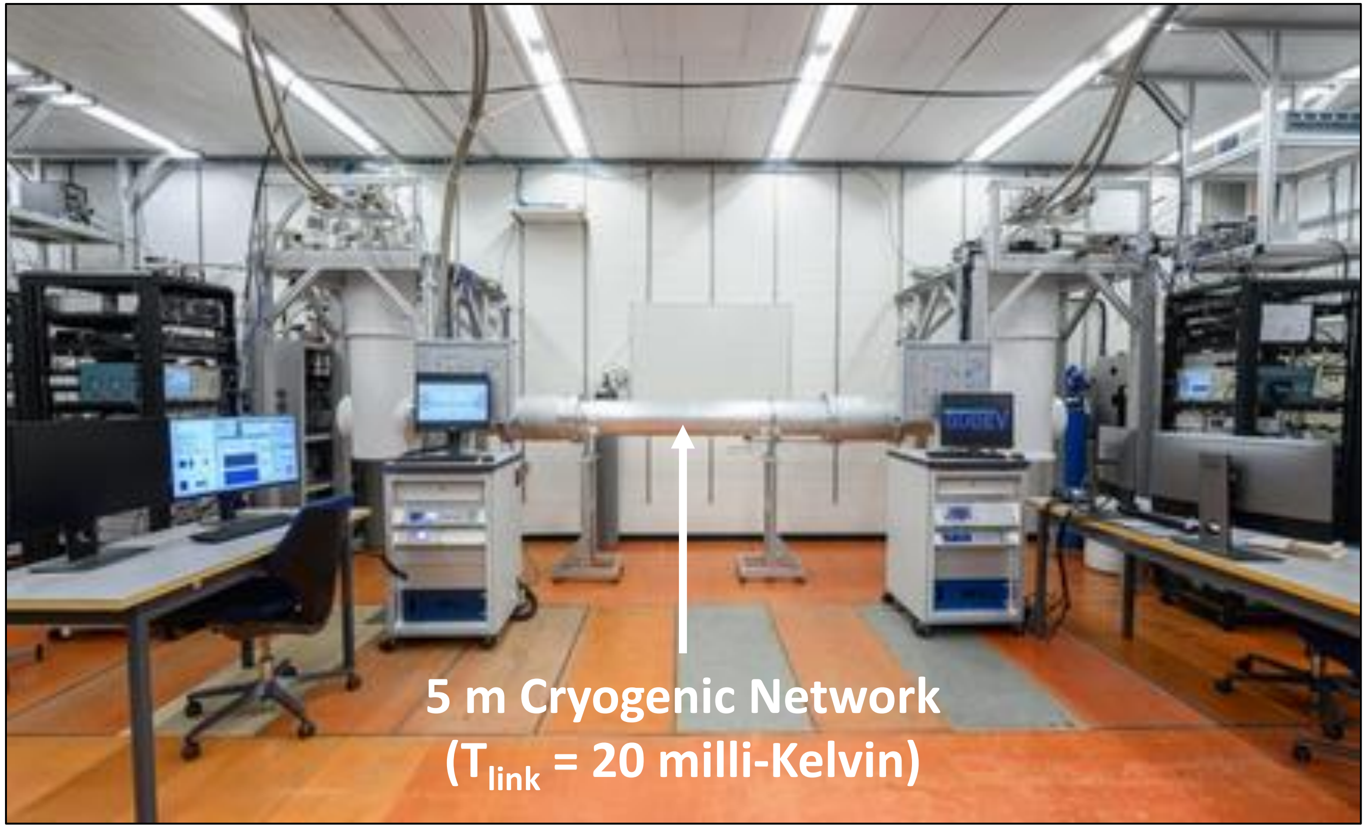
Fundamental use-case about Quantum is unanswered

Is this what Industry’s First Quantum Networks Will Look Like?







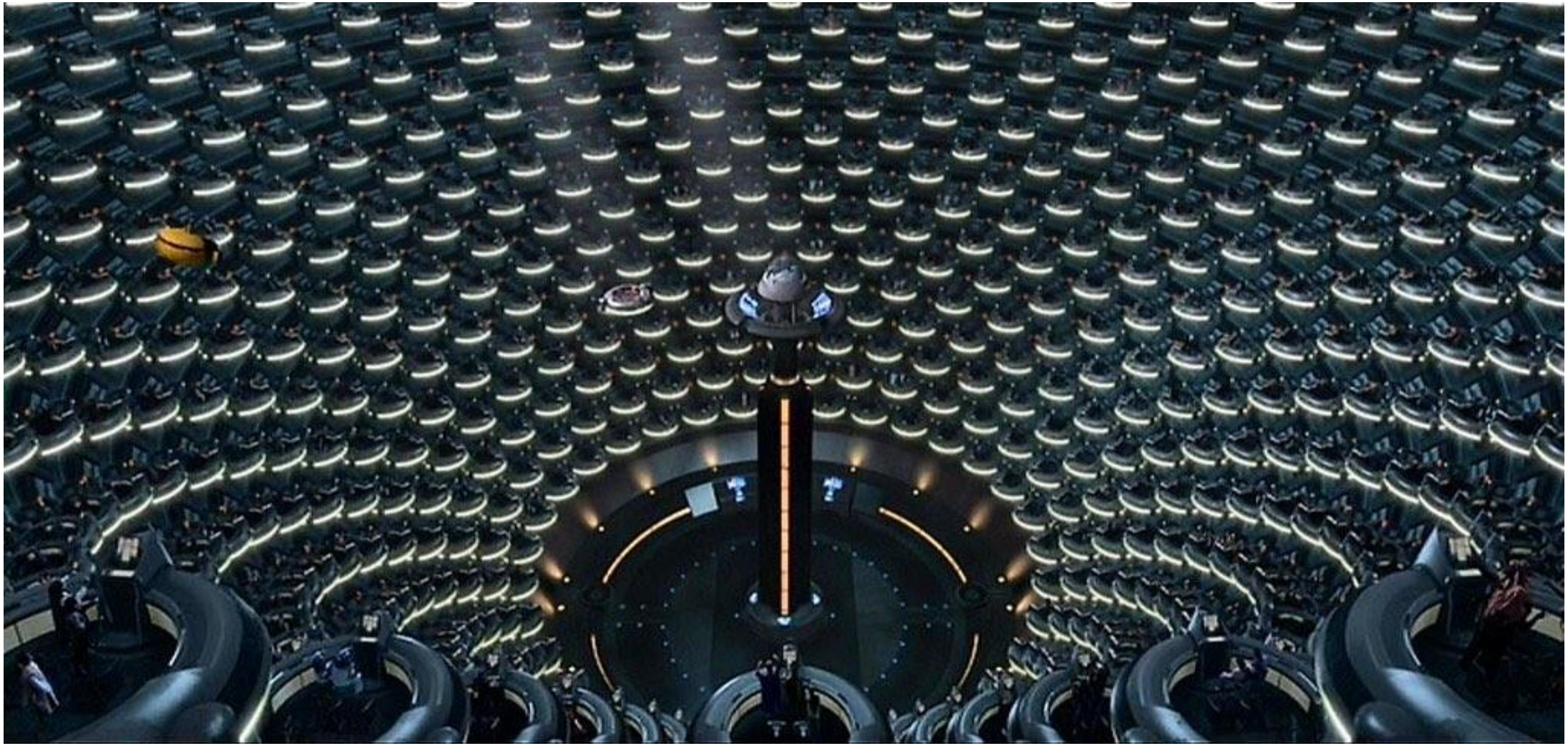


S. Storz, APS March Meeting 2020

LINCOLN LABORATORY
MASSACHUSETTS INSTITUTE OF TECHNOLOGY

Q&A
9:25 – 9:30

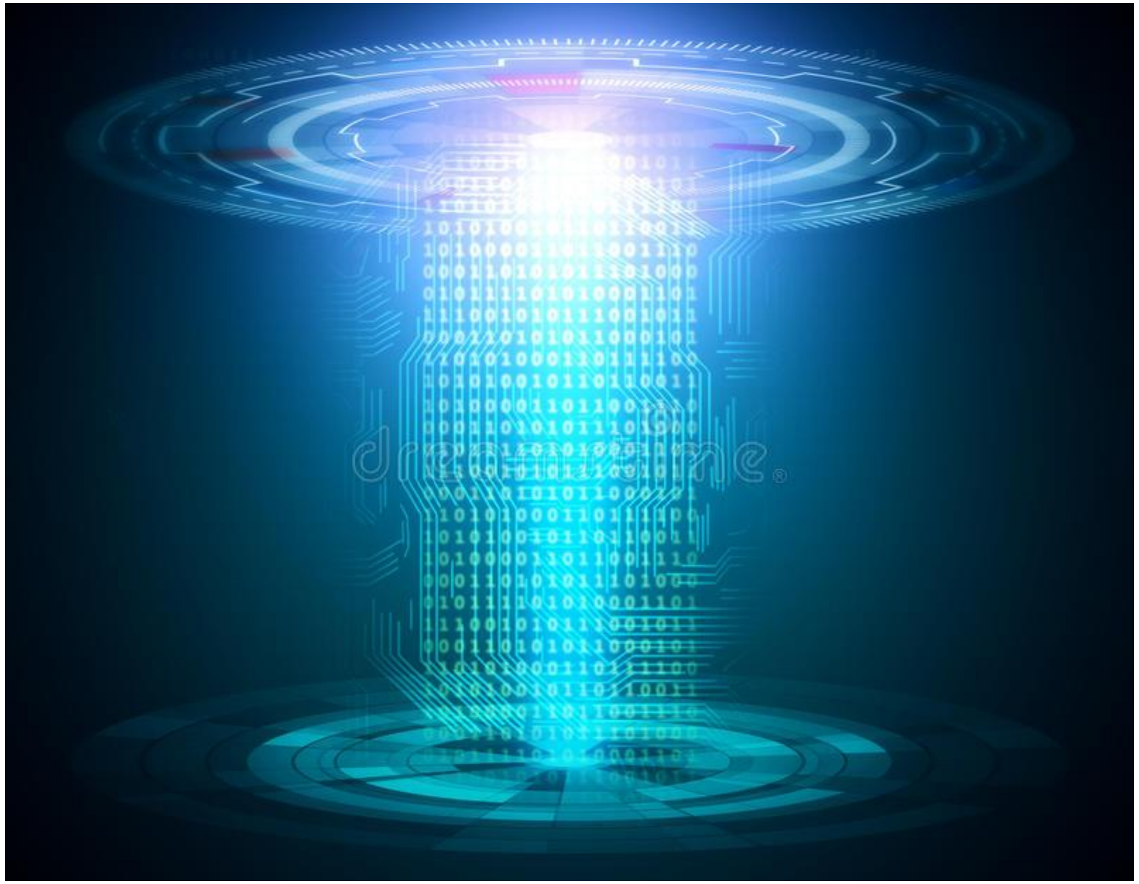
Move for a Vote of (No) Confidence in Quantum Products



Audience Poll

No.	Question	Vote #	Vote %
1	Will Quantum Networking & Cryptography Always Remain Basic Research?		
	Yes	16	28
	No	41	72
2	Is Quantum Networking & Cryptography Ready to Power Great Products?		
	Yes	28	42
	No	38	58
3	Which character would you rather assume?		
	Jedi Knight	43	66
	Sith Lord	22	34

OFC Rump Session on Quantum Networking & Cryptography



Scotty, Quantum Teleport us up!