ETH zürich DINFK APPLIED CRYPTO GROUP

PQC or QKD?

Professor Kenny Paterson
Applied Cryptography Group
ETH Zurich

Symposium on Post-Quantum Cryptography
November 3, 2021

Cryptography Everywhere

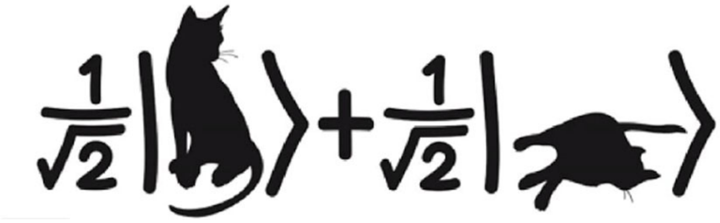
APPLIED CRYPTO GROUP

- e-commerce
- social media
- online personal banking
- debit/credit card payments
- interbank payments
- secure messaging (WhatsApp, Signal, Telegram)
- mobile telephony

- VPN/remote access
- video conferencing
- secure cloud data storage
- privacy-preserving contact tracing (GAEN, DP3T)
- Cryptocurrencies
- military and government communications systems

Quantum Computing

Basic tenet of quantum physics: superposition.

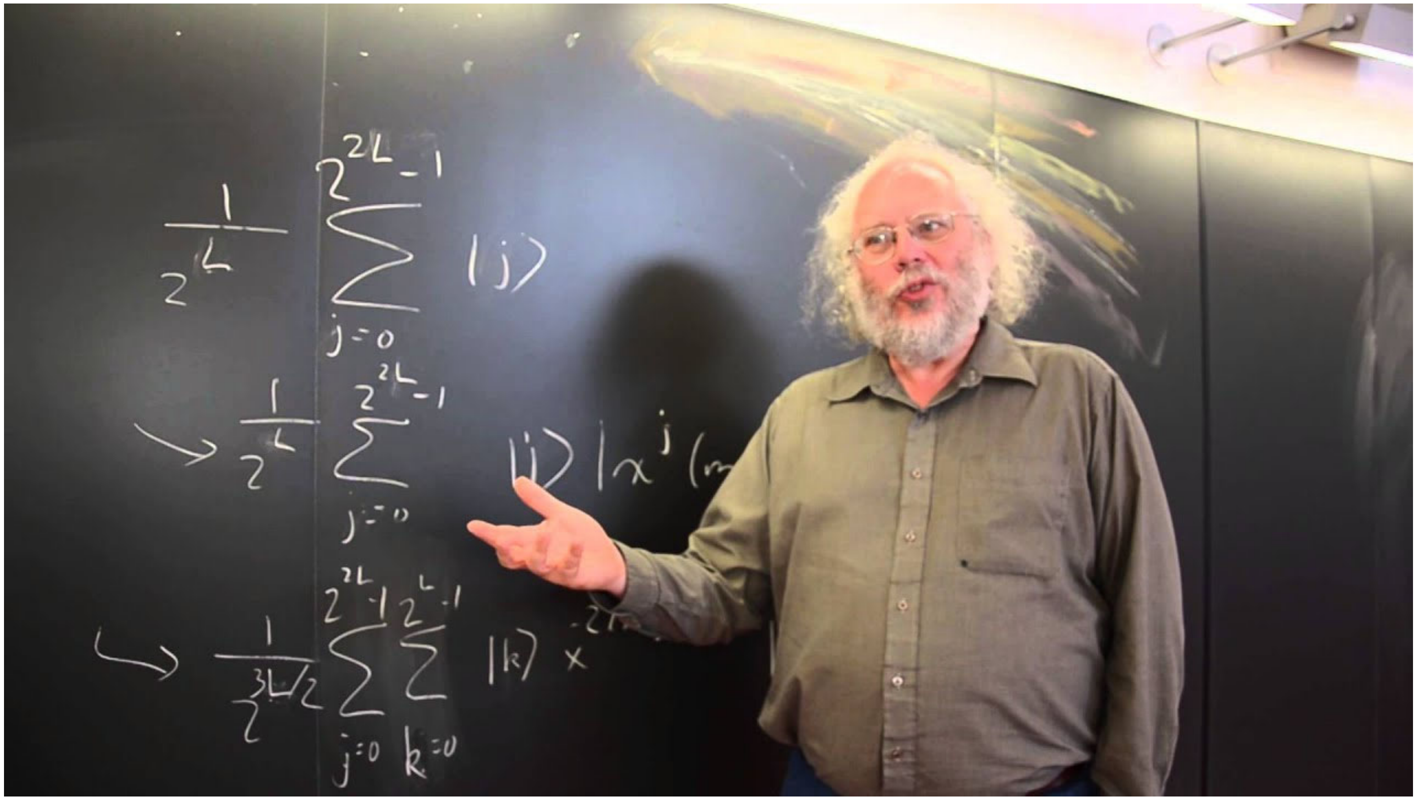

$\frac{1}{\sqrt{2}}|\ \rangle + \frac{1}{\sqrt{2}}|\ \rangle$

Qubit: basic unit of quantum computation, loosely a superposition of classical “0” and “1” bits.

Quantum gates: analogues of classical computing gates – AND, NOT, etc – acting on qubits.

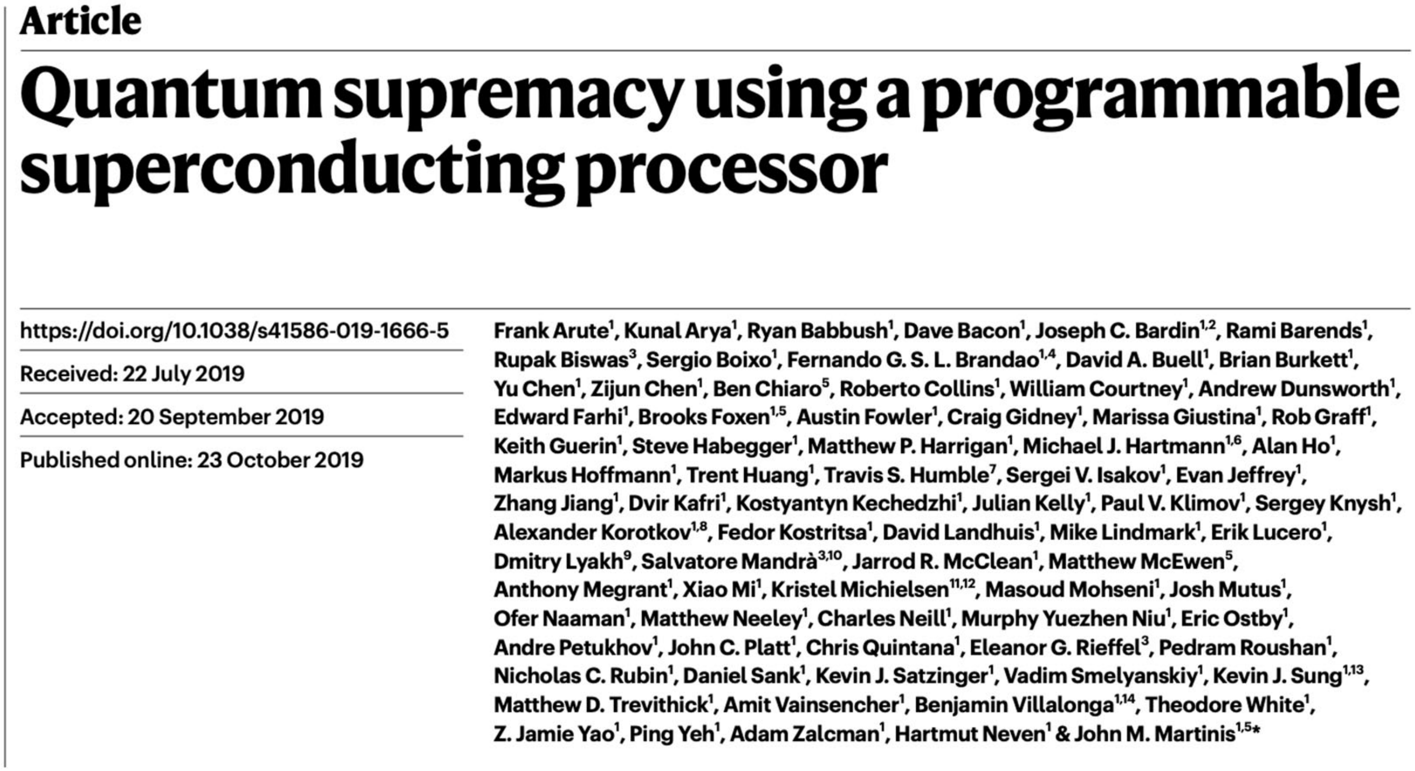
Quantum computing: execution of a sequence of quantum gates on ”all possible classical states in parallel”.

Shor’s Algorithm Breaks Classical **Public Key** Cryptography: RSA and ECC


$\frac{1}{2^L}\sum_{j=0}^{2^{2L}-1}|j\rangle$
$\rightarrow \frac{1}{2^L}\sum_{j=0}^{2^{2L}-1}|j\rangle|x^j$
$\hookrightarrow \frac{1}{2^{3L/2}}\sum_{j=0}^{2^{2L}-1}\sum_{k=0}^{2^L-1}|k\rangle\, x$

https://www.youtube.com/watch?v=hOlOY7NyMfs

Quantum Supremacy



Article

Quantum supremacy using a programmable superconducting processor

https://doi.org/10.1038/s41586-019-1666-5

Received: 22 July 2019

Accepted: 20 September 2019

Published online: 23 October 2019

Frank Arute[1], Kunal Arya[1], Ryan Babbush[1], Dave Bacon[1], Joseph C. Bardin[1,2], Rami Barends[1], Rupak Biswas[3], Sergio Boixo[1], Fernando G. S. L. Brandao[1,4], David A. Buell[1], Brian Burkett[1], Yu Chen[1], Zijun Chen[1], Ben Chiaro[5], Roberto Collins[1], William Courtney[1], Andrew Dunsworth[1], Edward Farhi[1], Brooks Foxen[1,5], Austin Fowler[1], Craig Gidney[1], Marissa Giustina[1], Rob Graff[1], Keith Guerin[1], Steve Habegger[1], Matthew P. Harrigan[1], Michael J. Hartmann[1,6], Alan Ho[1], Markus Hoffmann[1], Trent Huang[1], Travis S. Humble[7], Sergei V. Isakov[1], Evan Jeffrey[1], Zhang Jiang[1], Dvir Kafri[1], Kostyantyn Kechedzhi[1], Julian Kelly[1], Paul V. Klimov[1], Sergey Knysh[1], Alexander Korotkov[1,8], Fedor Kostritsa[1], David Landhuis[1], Mike Lindmark[1], Erik Lucero[1], Dmitry Lyakh[9], Salvatore Mandrà[3,10], Jarrod R. McClean[1], Matthew McEwen[5], Anthony Megrant[1], Xiao Mi[1], Kristel Michielsen[11,12], Masoud Mohseni[1], Josh Mutus[1], Ofer Naaman[1], Matthew Neeley[1], Charles Neill[1], Murphy Yuezhen Niu[1], Eric Ostby[1], Andre Petukhov[1], John C. Platt[1], Chris Quintana[1], Eleanor G. Rieffel[3], Pedram Roushan[1], Nicholas C. Rubin[1], Daniel Sank[1], Kevin J. Satzinger[1], Vadim Smelyanskiy[1], Kevin J. Sung[1,13], Matthew D. Trevithick[1], Amit Vainsencher[1], Benjamin Villalonga[1,14], Theodore White[1], Z. Jamie Yao[1], Ping Yeh[1], Adam Zalcman[1], Hartmut Neven[1] & John M. Martinis[1,5]*

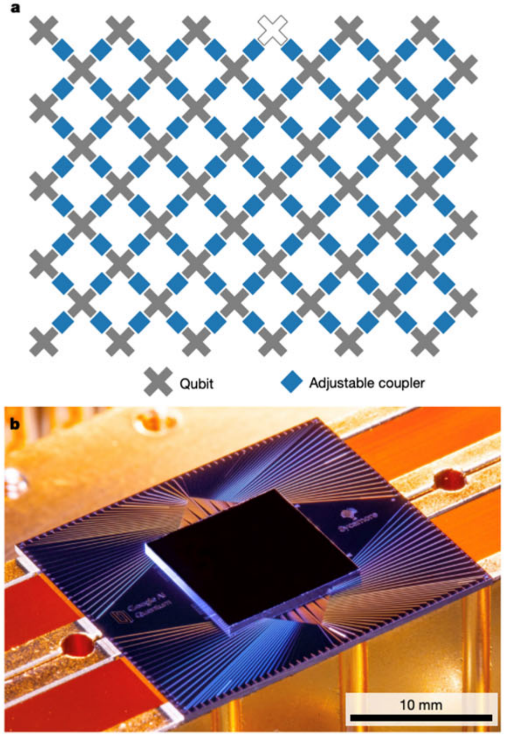
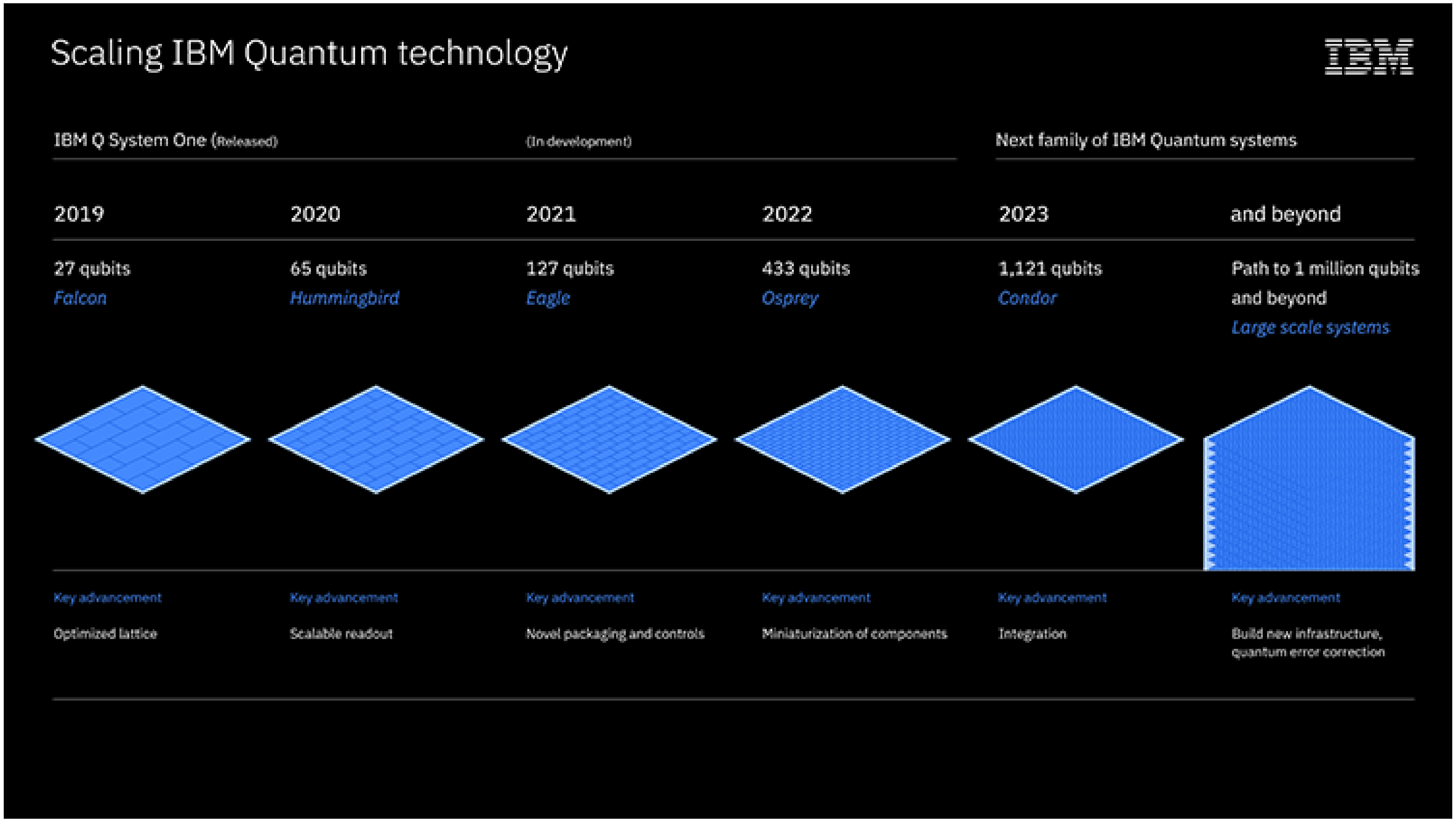


Fig. 1 | The Sycamore processor. a, Layout of processor, showing a rectangular array of 54 qubits (grey), each connected to its four nearest neighbours with couplers (blue). The inoperable qubit is outlined. **b**, Photograph of the Sycamore chip.

Quantum Computing’s Prospects According to IBM

APPLIED CRYPTO GROUP



Scaling IBM Quantum technology

IBM

IBM Q System One (Released) | (In development) | Next family of IBM Quantum systems

2019	2020	2021	2022	2023	and beyond
27 qubits *Falcon*	65 qubits *Hummingbird*	127 qubits *Eagle*	433 qubits *Osprey*	1,121 qubits *Condor*	Path to 1 million qubits and beyond *Large scale systems*
Key advancement	Key advancement	Key advancement	Key advancement	Key advancement	Key advancement
Optimized lattice	Scalable readout	Novel packaging and controls	Miniaturization of components	Integration	Build new infrastructure, quantum error correction

https://www.ibm.com/blogs/research/2020/09/ibm-quantum-roadmap/
February 2021

Responding to the CryptApocalypse

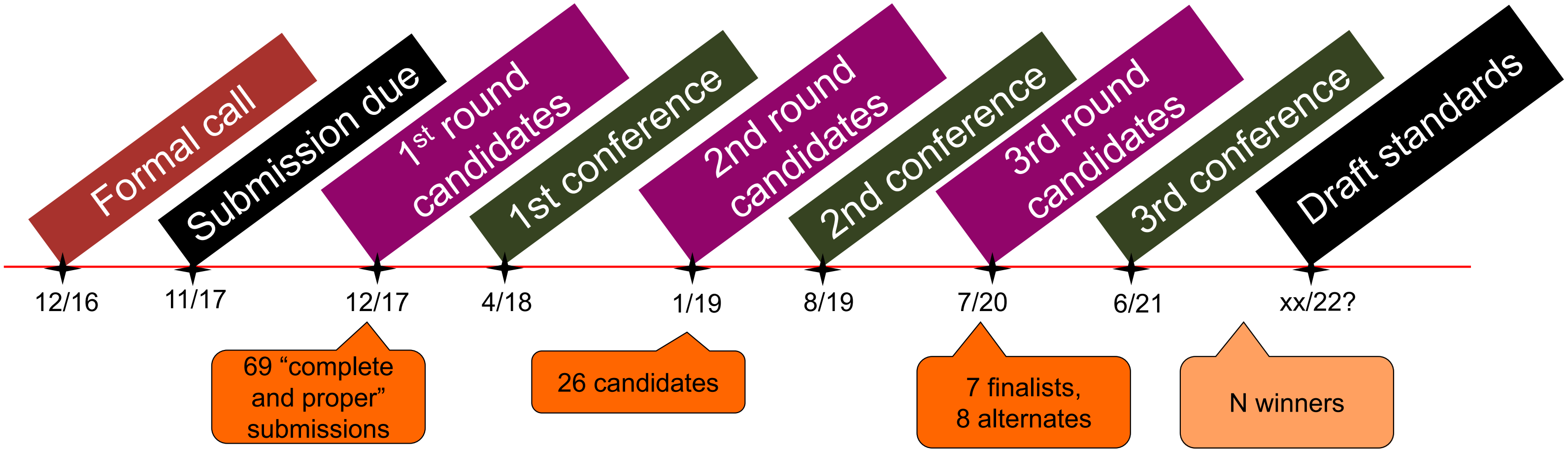
More usefully:

- Design new cryptosystems that we believe resist attack by quantum computers.
- **Post-quantum cryptography (PQC).**
- Aka quantum-resistant, quantum-immune or quantum-safe cryptography.

PQC and NIST

NIST competition, 2016 – 2023(ish) for standardising post-quantum public key algorithms.

- http://csrc.nist.gov/groups/ST/post-quantum-crypto/
- **Formal project start:** 2012.
- **Evaluation criteria**: security, cost, flexibility/simplicity/adoptability.
- **Process (5-7 years)**:



Formal call

12/16

Submission due

11/17

1st round candidates

12/17

69 “complete and proper” submissions

1st conference

4/18

2nd round candidates

1/19

26 candidates

2nd conference

8/19

3rd round candidates

7/20

7 finalists, 8 alternates

3rd conference

6/21

Draft standards

xx/22?

N winners

Challenges for Deploying PQC

The NIST process is proceeding in an orderly fashion and will produce a sensible and conservative portfolio of options in a reasonable timeframe.

But…

- PQC has a **different performance profile** to current PKC.
- PQC algorithms are likely to suffer from **implementation vulnerabilities**.
- Uncertainty over **patents**.
- Risk of **early lock-in** to potentially bad choices through premature experimentation/deployment/alternative standardisation.
- Significant **further standardisation** and **integration** work lies ahead.

But What About Quantum Cryptography?

- Quantum Key Distribution (QKD) promises **unconditional** security.
  - “Security based only on the correctness of the laws of quantum physics”.

- Often contrasted with security offered by currently deployed public key cryptography (PKC).
  - Currently deployed PKC is vulnerable to algorithmic advances in conventional algorithms for factoring, discrete logs, etc.
  - Currently deployed PKC is vulnerable to large-scale quantum computers.
  - Post-quantum PKC rests on relatively new hardness assumptions which could be invalidated by new quantum – or even classical – algorithms.

QKD

“Quantum cryptography offers the only protection against quantum computing, and all future networks will undoubtedly combine both through the air and fibre-optic technologies.”

Dr. Brian Lowans,

Quantum and Micro Photonics Team Leader,

QinetiQ.

QKD

“All cryptographic schemes used currently on the Internet would be broken…. ”

Prof. Giles Brassard,
Quantum Works launch meeting,
University of Waterloo,
27th September 2006.

QKD

According to *MIT Technology Review,* in 2003*,* QKD was one of:

> *"10 Emerging Technologies That Will Change the World."*

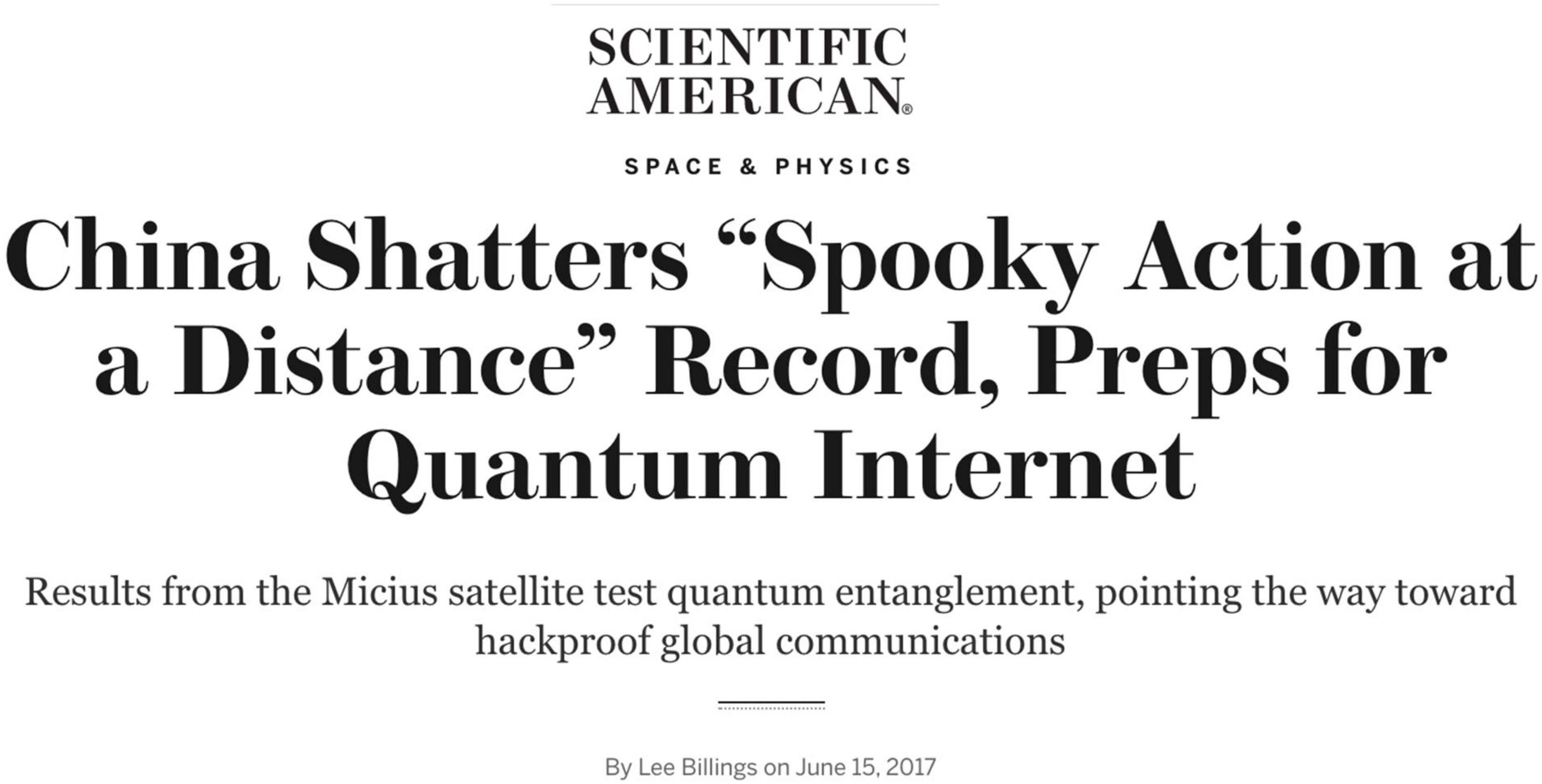
According to Dr. Burt Kaliski Jr., former chief scientist at RSA Security:

> *"If there are things that you want to keep protected for another 10 to 30 years, you need quantum cryptography."*

QKD

- These examples are taken from a presentation I gave **15 years ago** (at the Fields Institute, University of Toronto)!

- More recent examples of the promotion of QKD are easy to find...



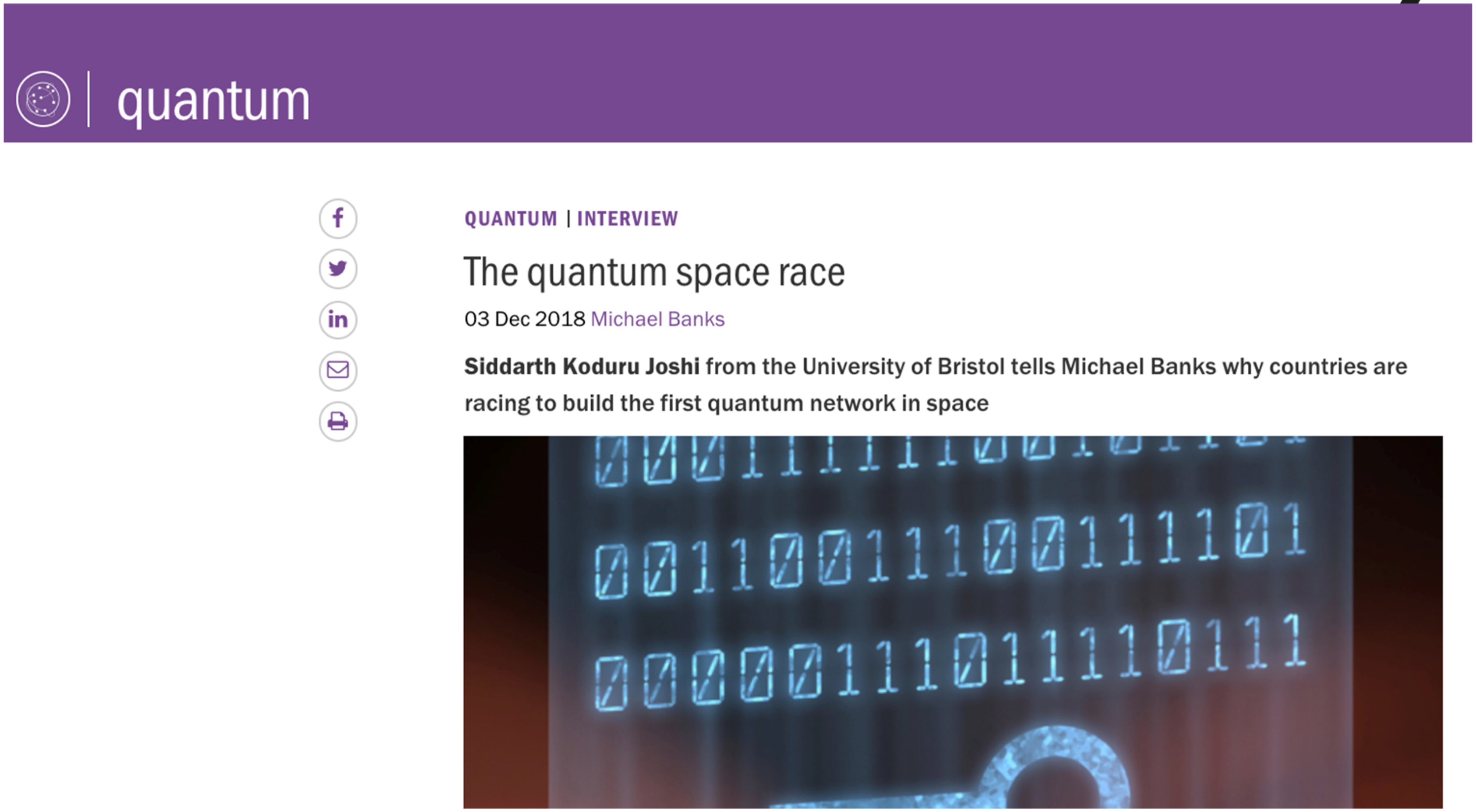
SCIENTIFIC AMERICAN®

SPACE & PHYSICS

China Shatters "Spooky Action at a Distance" Record, Preps for Quantum Internet

Results from the Micius satellite test quantum entanglement, pointing the way toward hackproof global communications

By Lee Billings on June 15, 2017



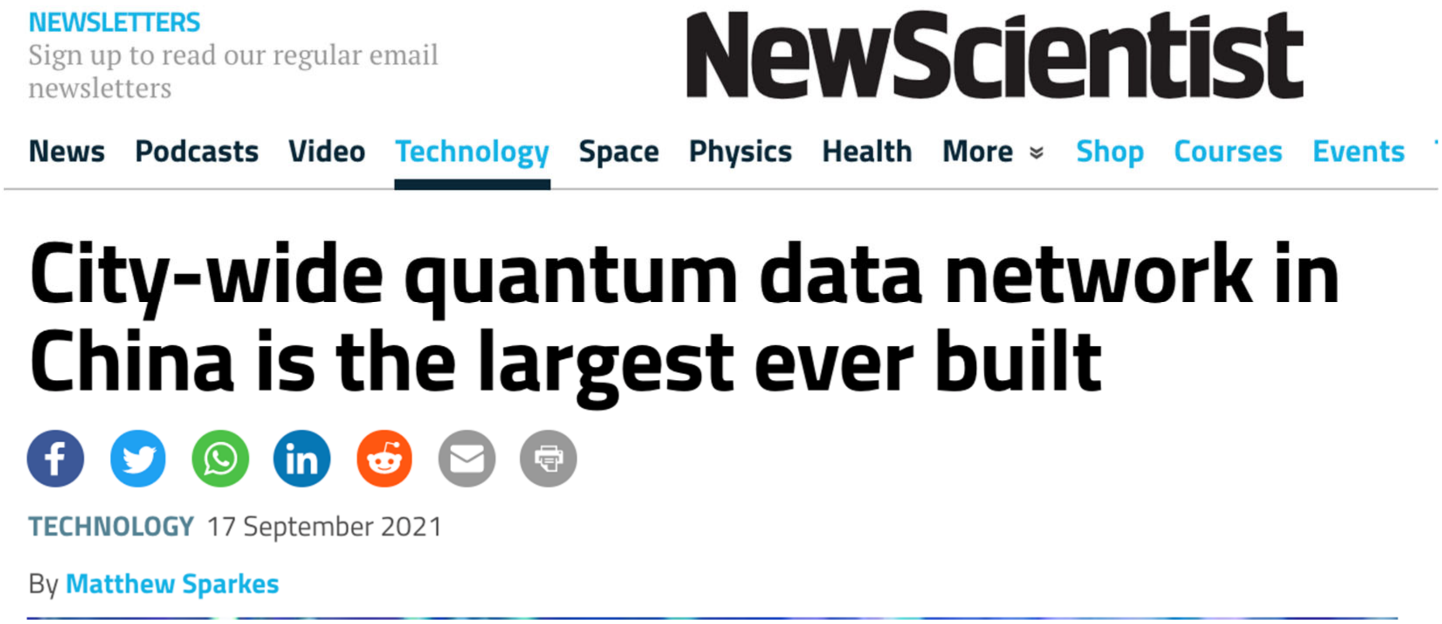
quantum

QUANTUM | INTERVIEW

The quantum space race

03 Dec 2018 Michael Banks

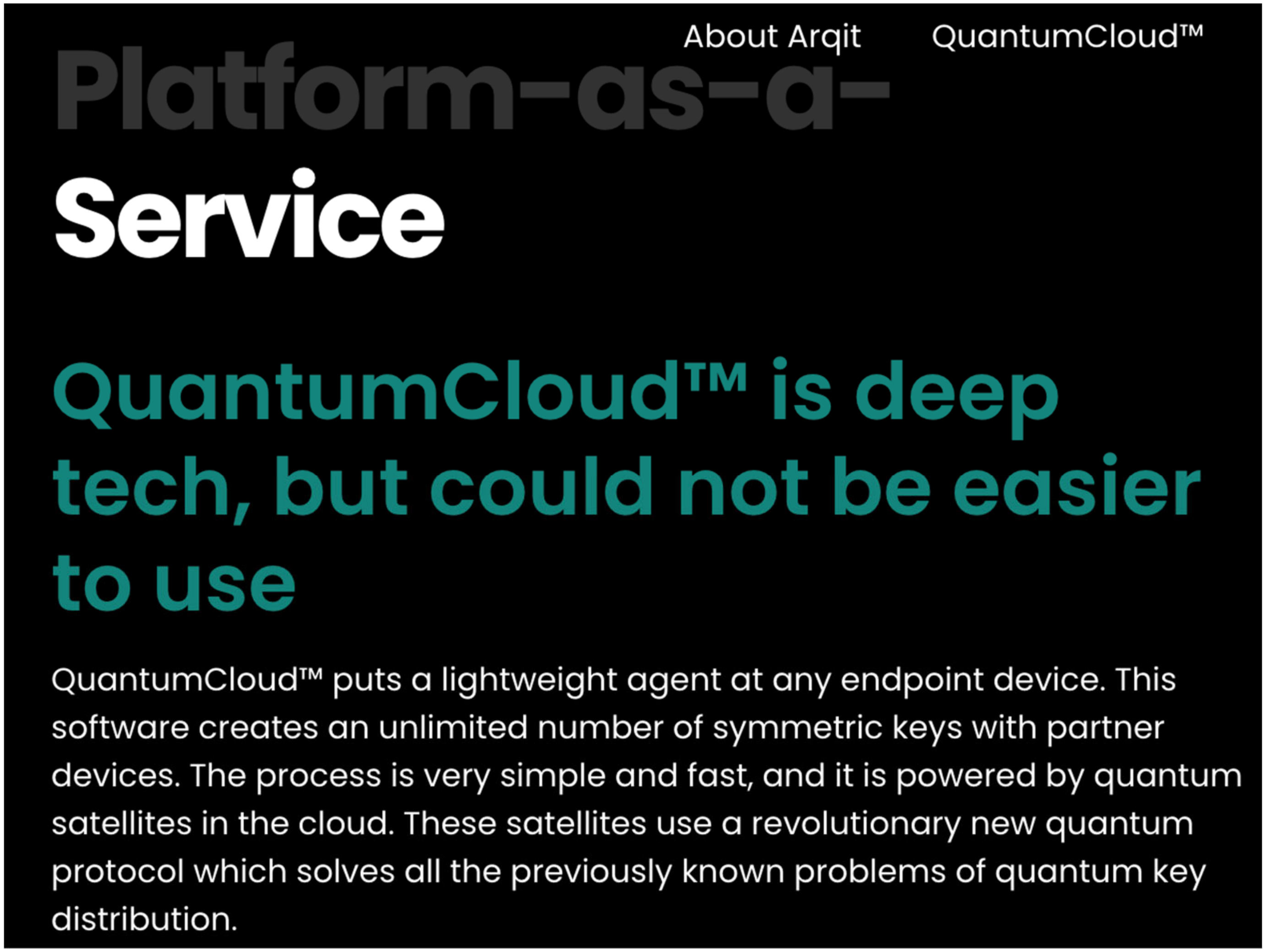
Siddarth Koduru Joshi from the University of Bristol tells Michael Banks why countries are racing to build the first quantum network in space



City-wide quantum data network in China is the largest ever built

TECHNOLOGY 17 September 2021

By Matthew Sparkes



Platform-as-a-Service

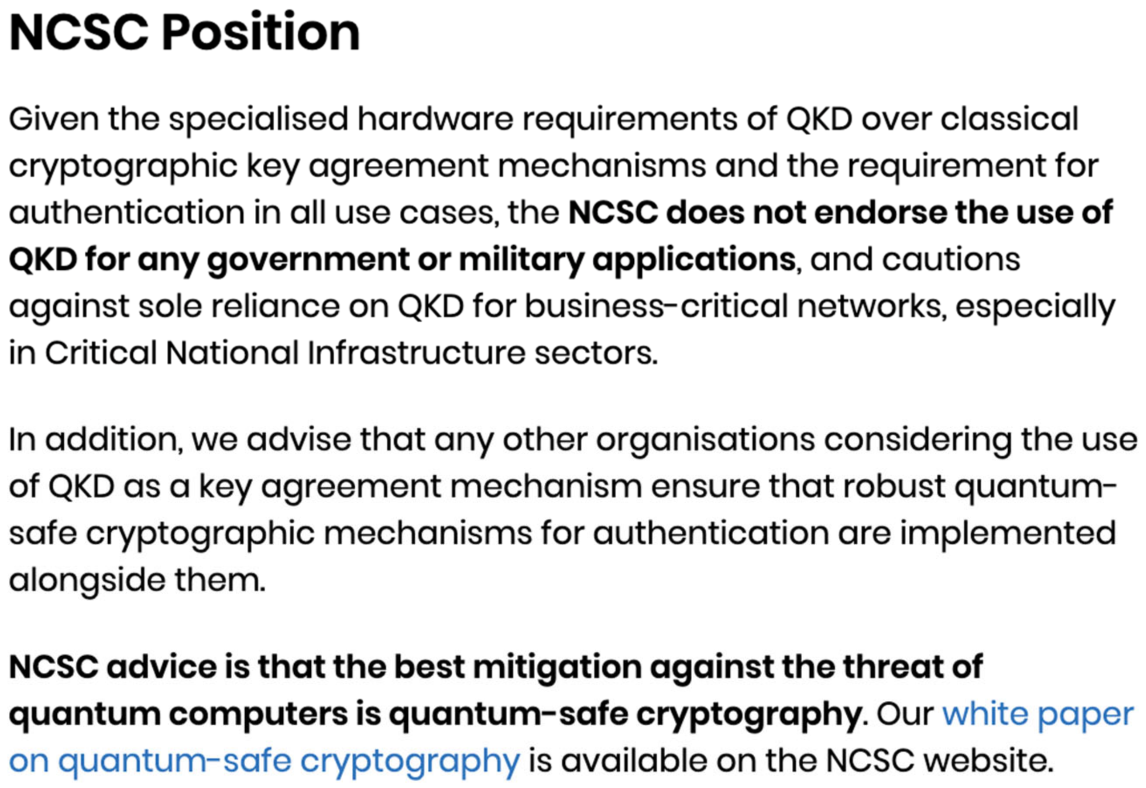
QuantumCloud™ is deep tech, but could not be easier to use

QuantumCloud™ puts a lightweight agent at any endpoint device. This software creates an unlimited number of symmetric keys with partner devices. The process is very simple and fast, and it is powered by quantum satellites in the cloud. These satellites use a revolutionary new quantum protocol which solves all the previously known problems of quantum key distribution.

Challenges to QKD Adoption

1. QKD does not solve the same problem as public key cryptography does: QKD permits communications only with pre-agreed partners.
2. QKD systems have limits on rate and range: no unconditional security in practice, no end-to-end security.
3. Security in theory does not equal security in practice.
4. QKD systems do not offer significant security benefit over what we can already achieve with low-cost (or even free) classical techniques.

QKD or PQC? The NCSC/GCHQ View



NCSC Position

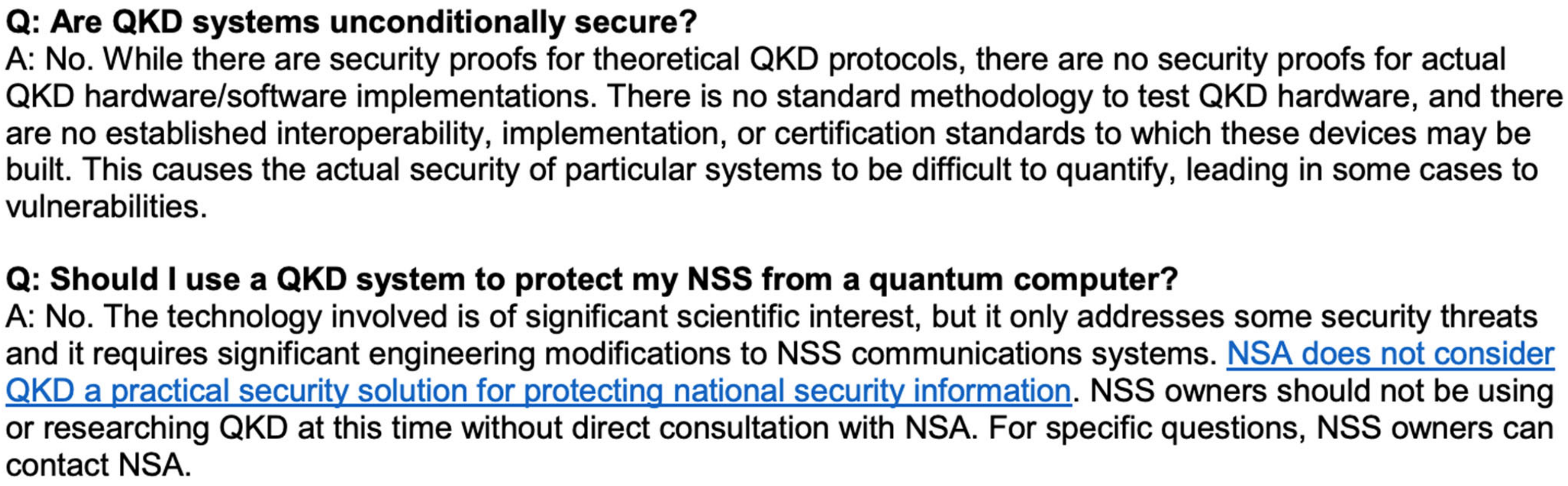
Given the specialised hardware requirements of QKD over classical cryptographic key agreement mechanisms and the requirement for authentication in all use cases, the **NCSC does not endorse the use of QKD for any government or military applications**, and cautions against sole reliance on QKD for business-critical networks, especially in Critical National Infrastructure sectors.

In addition, we advise that any other organisations considering the use of QKD as a key agreement mechanism ensure that robust quantum-safe cryptographic mechanisms for authentication are implemented alongside them.

NCSC advice is that the best mitigation against the threat of quantum computers is quantum-safe cryptography. Our white paper on quantum-safe cryptography is available on the NCSC website.

https://www.ncsc.gov.uk/whitepaper/quantum-security-technologies
March 2020

QKD or PQC? The NSA View



Q: Are QKD systems unconditionally secure?
A: No. While there are security proofs for theoretical QKD protocols, there are no security proofs for actual QKD hardware/software implementations. There is no standard methodology to test QKD hardware, and there are no established interoperability, implementation, or certification standards to which these devices may be built. This causes the actual security of particular systems to be difficult to quantify, leading in some cases to vulnerabilities.

Q: Should I use a QKD system to protect my NSS from a quantum computer?
A: No. The technology involved is of significant scientific interest, but it only addresses some security threats and it requires significant engineering modifications to NSS communications systems. NSA does not consider QKD a practical security solution for protecting national security information. NSS owners should not be using or researching QKD at this time without direct consultation with NSA. For specific questions, NSS owners can contact NSA.

https://media.defense.gov/2021/Aug/04/2002821837/-1/-1/1/Quantum_FAQs_20210804.PDF
August 2021

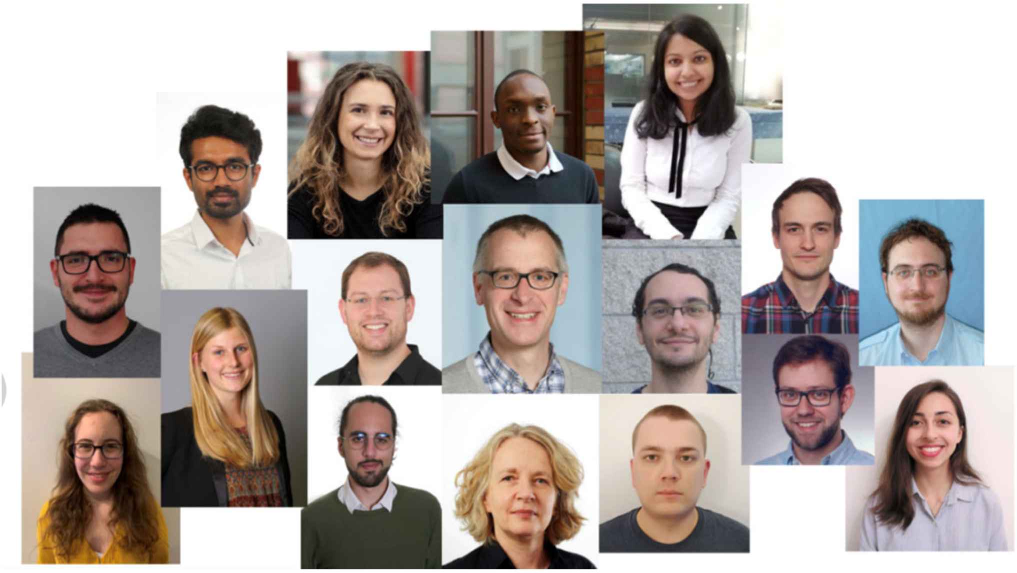
ETH zürich

Contact:

Professor Kenny Paterson
Applied Cryptography Group

Department of Computer Science
Universitätstrasse 6
8092 Zurich, Switzerland

https://appliedcrypto.ethz.ch/
kenny.paterson@inf.ethz.ch
@kennyog



APPLIED CRYPTO GROUP

1. QKD Does Not Solve the Same Problem as PKC

- QKD needs a logically separate authentic channel for agreeing on what measurements were made.
- That requires a pre-agreed key or the use of conventional digital signatures.
- If you want the promised unconditional security, only the first option works.
- Then QKD takes a pre-agreed key and uses it to create more shared keys.
- **Unconditionally secure QKD is actually unconditionally secure key expansion.**
- By contrast, PKC can be used to set-up shared keys **between any two parties** without needing pre-agreed keys, relying instead on authentication of public keys.

2. QKD Has Limits on Rate and Range

- Impressive gains in secure bit rate and range of QKD have been made.
- Mbit/s of secure key now achievable over, say, 50km.
- But for **unconditional security**, we need to consume 1 bit of key for every bit of data we wish to securely communicate.
- And modern networks run at Gbit/s rates.
- Can sacrifice unconditional security, but then no clear advantage over what we can do with classical shared-key systems.

2. QKD Has Limits on Rate and Range

- Going above 200km in commercial fibre optic cable seems hard because of dispersion losses.
- Cannot amplify QKD signals (quantum no-cloning theorem).
- So current and planned quantum networks rely on “trusted repeaters”.
- Consequently, they cannot provide end-to-end security for communications.
- But e2e security is “table stakes” in secure communications!
- May be addressed one day using quantum repeaters/entanglement-based systems.

3. Security in Theory ≠ Security in Practice.

- Security proofs for QKD apply for idealised systems and parameters.
- Unclear that those proofs extend to QKD as used in practice.
- And QKD has to run on real hardware and is vulnerable to implementation weaknesses – just like classical cryptography.
- cf. Bennett-Brassard’84: audio side channel in the experimental prototype.
- Can be portrayed as part of QKD’s evolution towards practical deployment.
- But we were promised unconditional security!

4. QKD Does Not Offer Significant Advantages Over Carefully Designed Classical Approaches

- Unconditionally secure QKD needs pre-agreed symmetric keys.
- But if you allow the use of a pre-agreed symmetric key, we can achieve all the security we need using only classical techniques.
- This won't be unconditionally secure, but neither is QKD in practice (because of limits on key rates).
- We can do all this without using any special hardware, with no range limitation, with e2e security, and at network line-speed.
- It's all tried and tested technology, available for free in network appliances, web browsers, operating systems today.
- **Technical difference**: consequences of master key compromise is different in hybrid QKD system and conventional system.