Title: Toward a Quantum-Safe Future

Speakers: Michele Mosca

Series: Colloquium

Date: April 08, 2020 - 2:00 PM

URL: http://pirsa.org/20040005

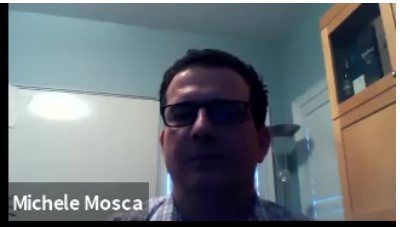
Abstract: There has been tremendous progress in the many layers needed to realize large-scale quantum computing, from the hardware layers to the high level software. There has also been vastly increased exploration into the potentially useful applications of quantum computers, which will drive the desire to build quantum computers and make them available to users. I will describe some of my research in quantum algorithmics and quantum compiling.

The knowledge and tools developed for these positive applications give us insight into the cost of implementing quantum cryptanalysis of today's cryptographic algorithms, which is a key factor in estimating when quantum computers will be cryptographically relevant (the "collapse time"). In addition to my own estimates, I will summarize the estimates of 22 other thought leaders in quantum computing.

What quantum cryptanalysis means to an organization or a sector depends not only on the collapse time, but also on the time to migrate to quantum-safe algorithms as well as the shelf-life of information assets being protected. In recent years, we have gained increasing insight into the challenges of a wide-scale migration of existing systems. We must also be proactive as we deploy new systems. Open-source platforms, like OpenQuantumSafe and OpenQKDNetwork, are valuable resources in helping meet many of these challenges.

While awareness of the challenges and the path forward has increased immensely, there is still a long road ahead as we work together with additional stakeholders not only to prepare our digital economy to be resilient to quantum attacks, but also to make us more resilient to other threats that emerge.

Toward a Quantum-Safe Future



Perimeter Institute Colloquium

8 April 2020

Michele Mosca

PERIMETER PI INSTITUTE FOR THEORETICAL PHYSICS

GRI GLOBAL RISK INSTITUTE

softwareQ

Quantum-Safe CANADA

CYBER SECURITY AND PRIVACY INSTITUTE UNIVERSITY OF WATERLOO

UNIVERSITY OF WATERLOO | IQC Institute for Quantum Computing

QUANTUM INDUSTRY CANADA

evolution

Security and readiness are too often an afterthought

https://www.wsj.com/articles/michael-hayden-says-u-s-is-easy-prey-for-hackers-1434924058

June 21, 2015 11:19 p.m. ET

THE WALL STREET JOURNAL.

Michael Hayden Says U.S. Is Easy Prey for Hackers

Former CIA and NSA chief says 'shame on us' for not protecting critical information better

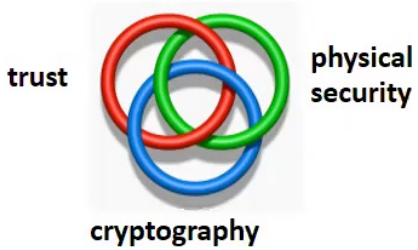
GEN. HAYDEN:
Then, all of us just fell in love with the ease and convenience and scale, so we decided to take things we used to keep if not in a safe, at least in our desk drawer, and put it up here, where it's by definition more vulnerable.
...
the next sound you hear will not be a digital bugle signaling the arrival of the digital cavalry to come save the day. The government ain't coming. You're not quite on your own, but you are more on your own up here [in cyberspace] than you in your lifetime have ever experienced being on your own down here.

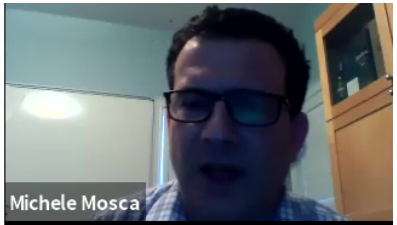
Cryptography is a foundational pillar of cybersecurity

- Cryptography allows us to achieve information security while using untrusted communication systems.

- *e.g.* Do you update your software and anti-virus daily? Why do you trust the source?

N.B. Cryptography is susceptible to "record now, decrypt later".

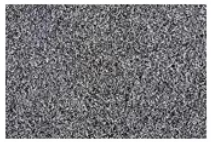




Message M
to be encrypted

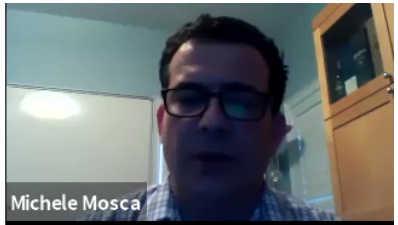
Shared key k

CipherText(k,M) =



Shared key k

Decrypted
Message M



- Symmetric encryption
- Key Establishment
- Authentication

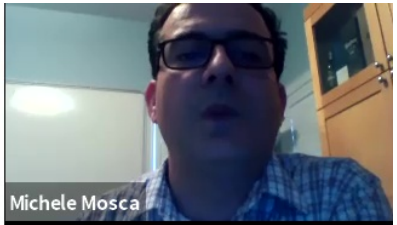
Message M to be encrypted

Shared key k

CipherText(k,M) =

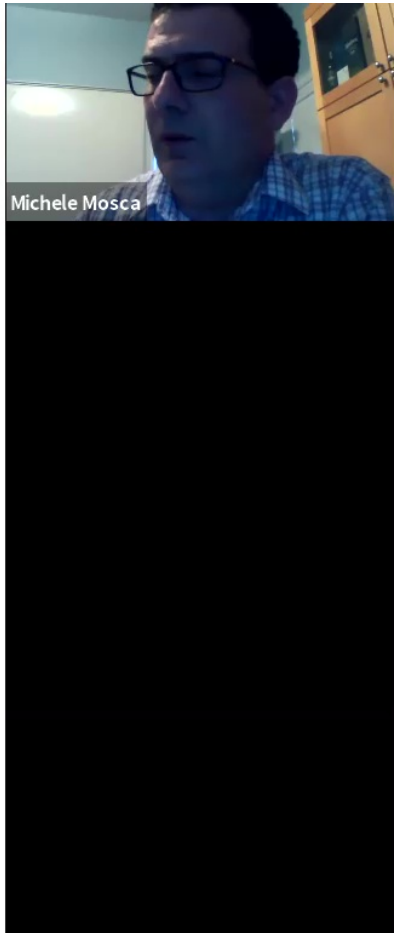
Shared key k

Decrypted Message M



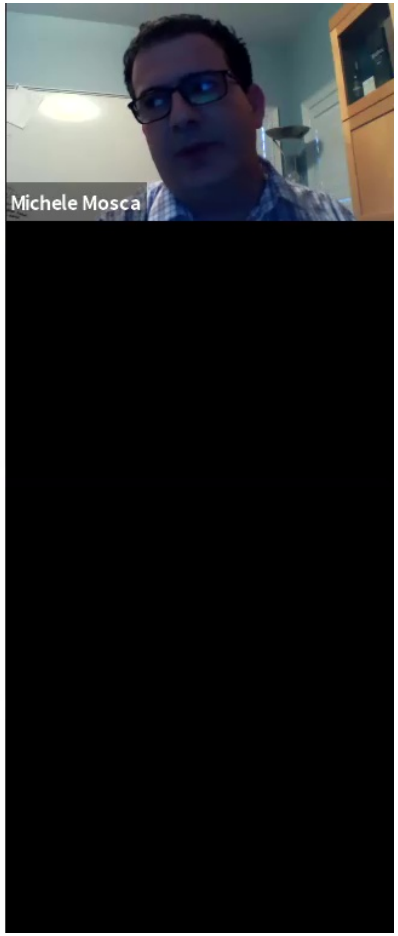
So many different vulnerabilities

- Fundamentally vulnerable cryptography
- Cryptography implementation errors
- User errors
- Platform implementation errors
- Platform design errors
- Admin errors
- Corrupt users
- Corrupt admin



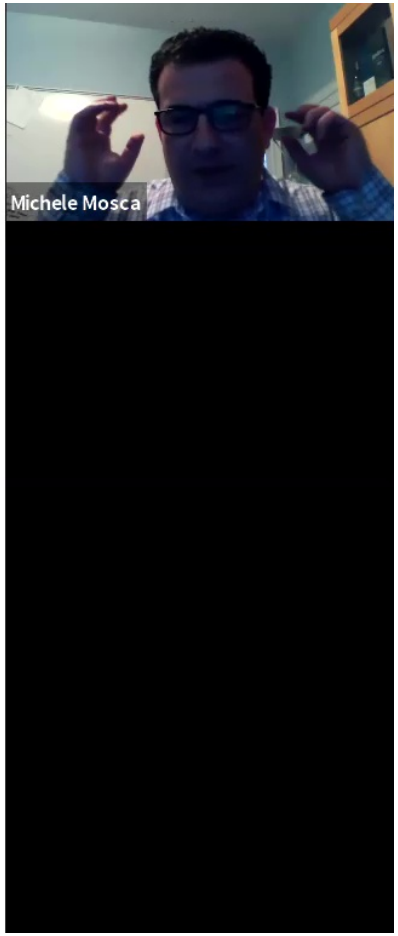
Vulnerabilities, ranked, from bad to worse?

- User errors
- Corrupt users
- Admin errors
- Corrupt admin
- Platform implementation errors
- Platform design errors
- Crypto implementation errors



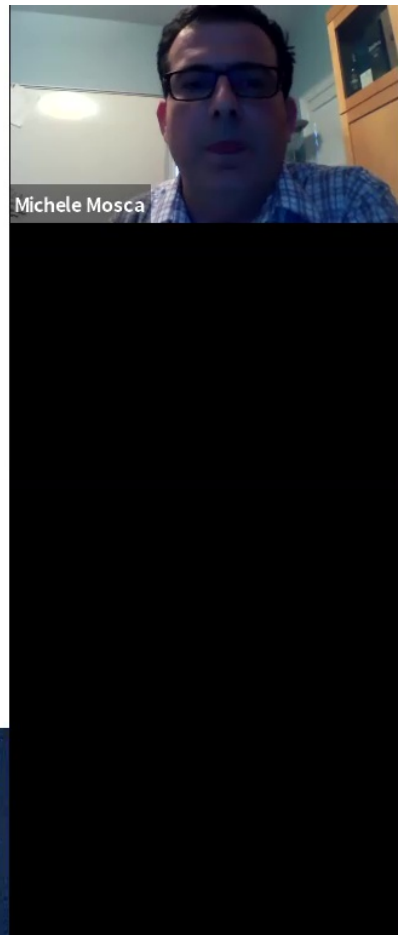
Vulnerabilities, ranked, from bad to worse?

- User errors
- Corrupt users
- Admin errors
- Corrupt admin
- Platform implementation errors
- Platform design errors
- Crypto implementation errors
- **Fundamentally vulnerable cryptography**



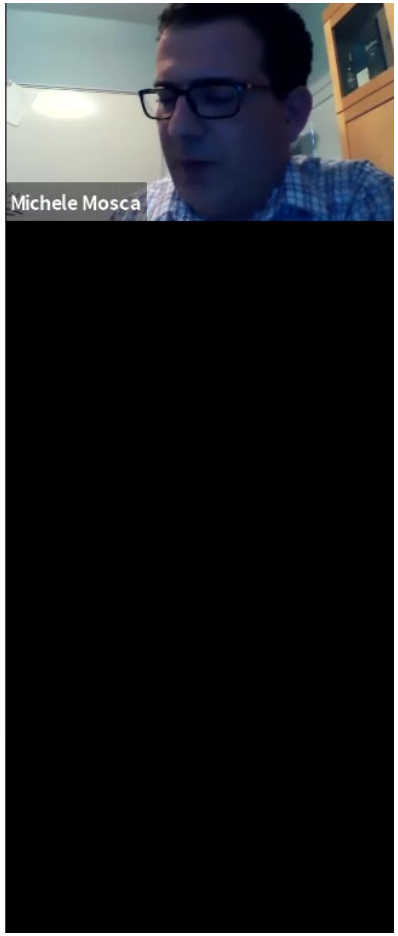
Vulnerabilities, ranked, from bad to worse?

- User errors
- Corrupt users
- Admin errors
- Corrupt admin
- Platform implementation errors
- Platform design errors
- Crypto implementation errors
- **Fundamentally vulnerable cryptography**



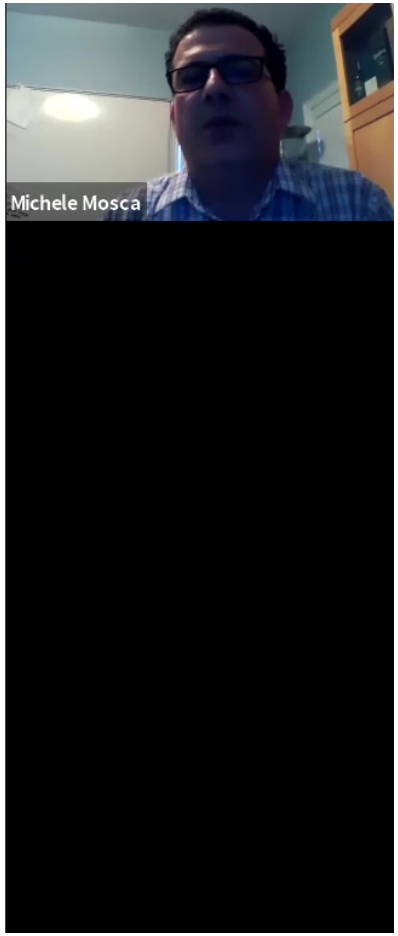
Unpredictable new vulnerabilities

"As is the norm, an unexpected problem occurred today."

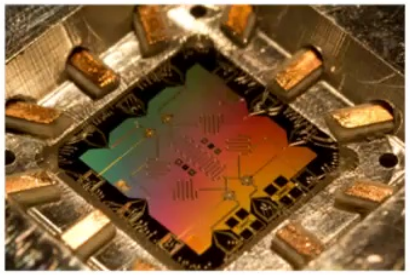


Do we have a strong cyber immune system?

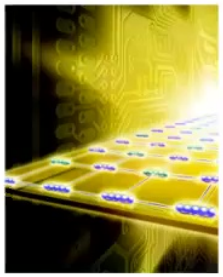
As an example, let’s consider one emerging threat.



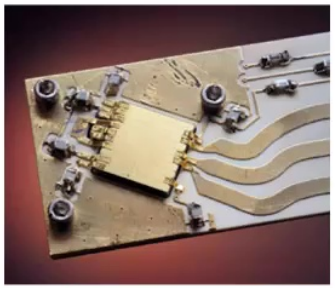
A new paradigm for computation: quantum computation



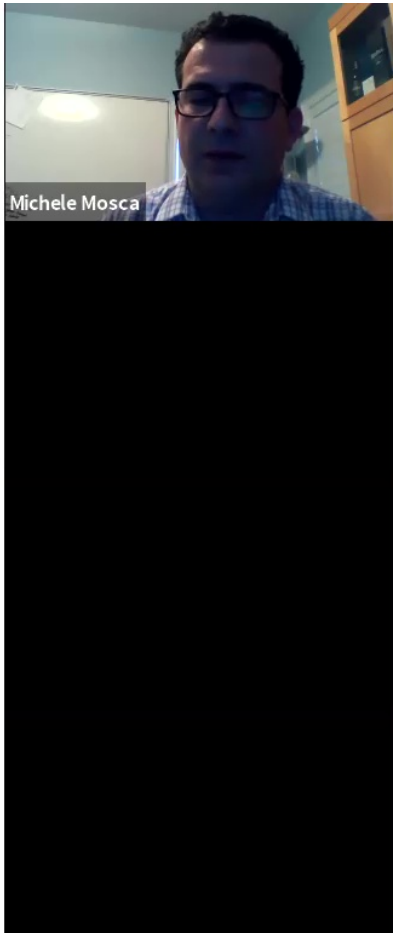
E. Lucero, D. Mariantoni, and M. Mariantoni



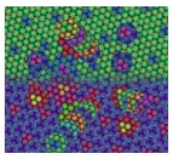
© Harald Ritsch



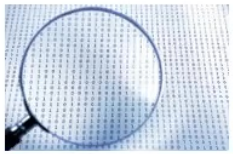
Y. Colombe/NIST



Strong desire to implement quantum technology



Designing new materials, drugs, etc.

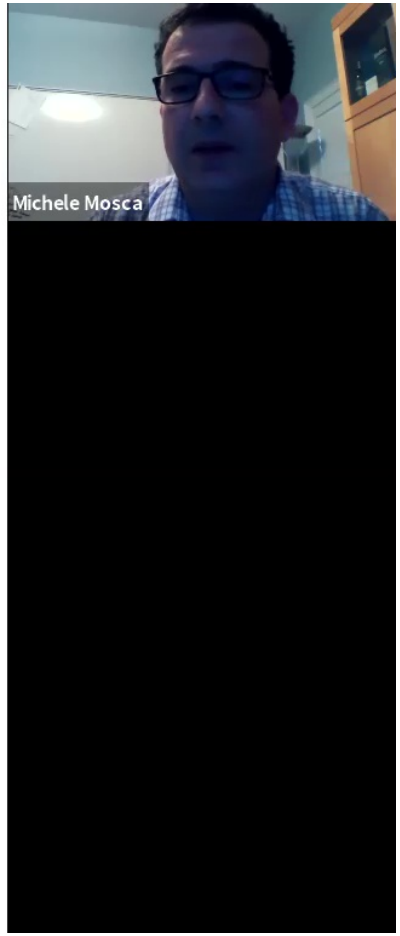


Optimizing

Sensing and measuring

Secure communication

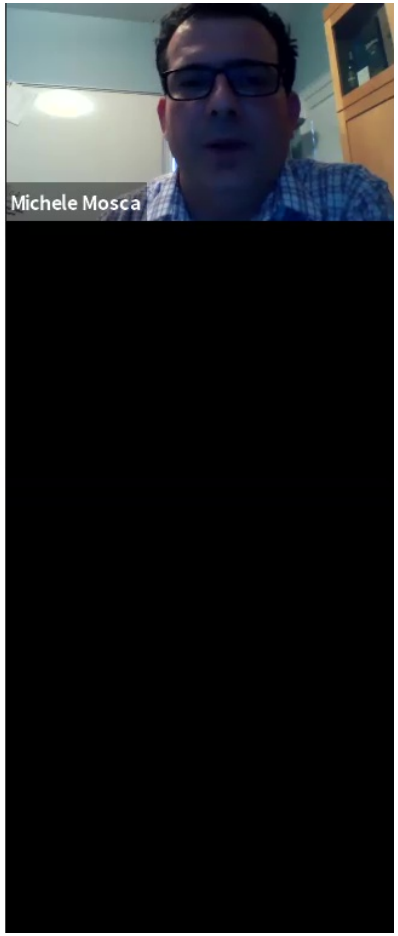
What else???



What sorts of practical applications?

Possibilities include:

- **Optimizing the design of new materials**
  - *For example, next generation materials could allow more efficient energy capture or transport or storage.*
- **Simulating chemical reactions at the quantum level**
  - *Potential applications include more efficient yields for chemical processes like the production of fertilizers.*
- **Optimization of designs or allocation or resources**
  - *For example, optimizing in the insertion of dampers in buildings to protect against earthquakes.*



COMPUTERS

IBM's new 53-qubit quantum computer is its biggest yet

The system will go online in October.

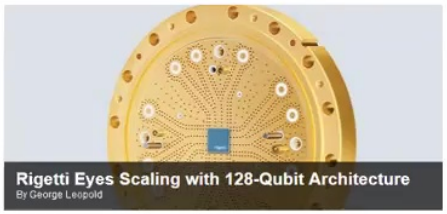
BY STEPHEN SHANKLAND | SEPTEMBER 18, 2019 5:00 AM PDT

A close-up view of the IBM Q quantum computer. The processor is in the silver-colored cylinder.

Stephen Shankland/CNET

Forbes

IBM Doubles Its Quantum Computing Power Again



Rigetti Eyes Scaling with 128-Qubit Architecture

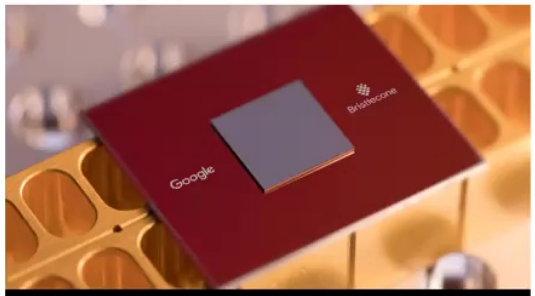
By George Leopold

August 10, 2018

Google moves toward quantum supremacy with 72-qubit computer

IBM and Intel recently debuted similarly sized chips

BY EMILY CONOVER | 1:17PM, MARCH 5, 2018



QUANTUM UPGRADE Google's 72-qubit quantum chip (shown) could become the first to perform a calculation impossible for traditional computers.

physicsworld

POLICY AND FUNDING | NEWS

Quantum Circuits bags $18m in first-round financing

20 Nov 2017 Hamish Johnston

Intel brings Quantum computing a step closer to reality

BY ROHITH BHASKAR OCT. 12, 2017, 2:57 P.M.

Intel is betting on its fabrication expertise to push quantum computing into the mainstream

2 shares

A lot of companies are pushing to make quantum computing real. Google, IBM, Microsoft among other prominent big names in the industry are already working on quantum machines that can work outside the confines of academia. Intel is betting on its

Bloomberg

Technology

Microsoft Edges Closer to Quantum Computer Based on Elusive Particle

Researchers make Majorana fermions, but now must try to control them

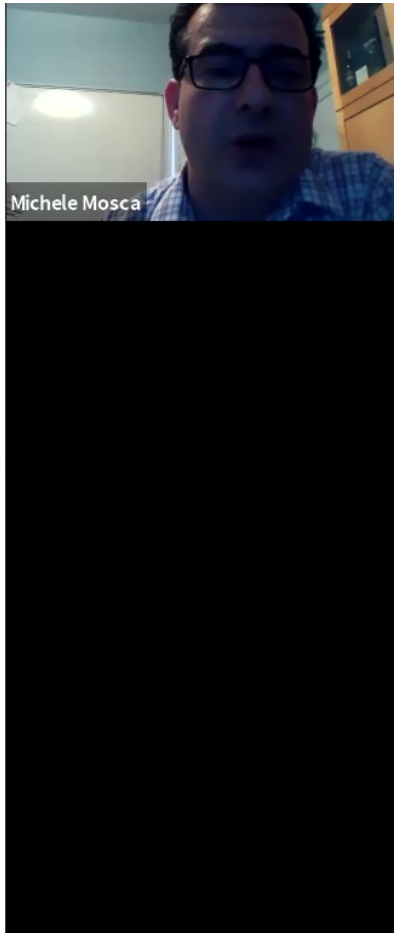
By Jeremy Kahn
March 28, 2018, 11:48 AM EDT *Corrected March 28, 2018, 2:09 PM EDT*

QUANTUM NEWS

Ion-based commercial quantum computer is a first

17 Dec 2018

physicsworld



POPULAR SCIENCE

WANT MORE?

Get Rogers Unison and stop paying for lines you don't use.

SCIENCE TECH DIY GOODS VIDEO ROLL THE DICE SUBSCRIBE

China is opening a new quantum research supercenter

The country wants to build a quantum computer with a million times the computing power presently in the world.

By Jeffrey Lin and P.W. Singer October 10, 2017

Lithium's Big

NATIONAL LABORATORY FOR QUANTUM INFORMATION SCIENCES

The $10 billion National Laboratory for Quantum Information Sciences in Hefei will be the center of China's attempt to take the global lead in quantum computing and sensing.

Alibaba puts 11-qubits quantum power on public cloud

Together with Chinese Academy of Sciences, Alibaba Cloud has unleashed superconducting quantum computing services on its public cloud, running on a processor with 11 quantum bits of power.

By Eileen Yu for By The Way | March 1, 2018 -- 14:11 GMT (06:11 PST) | Topic: Cloud

South China Morning Post EDITION: INTERNATIONAL

SCIENCE & RESEARCH

CHINA HK ASIA WORLD COMMENT BUSINESS TECH LIFE CULTURE SPORT WEEK IN ASIA POST MAG STYLE .TV

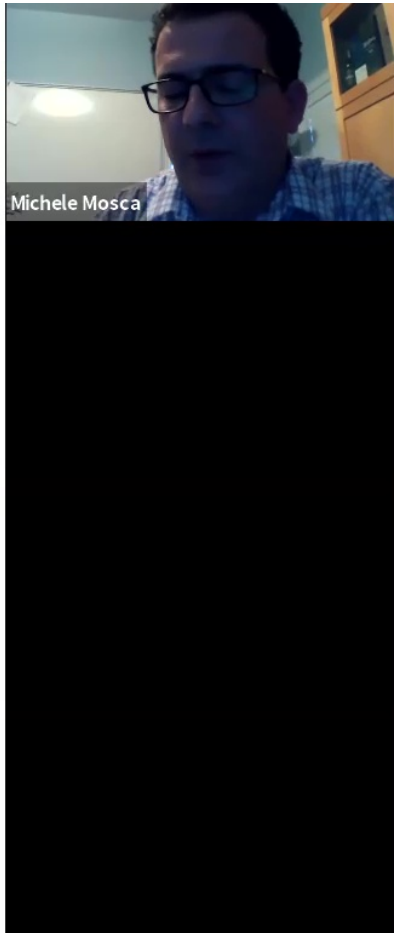
Tech / Science & Research

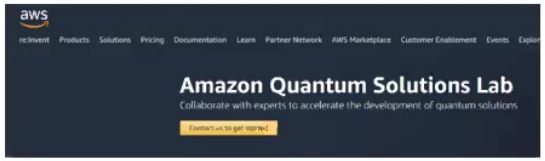
China's race for the mother of all supercomputers just got more crowded

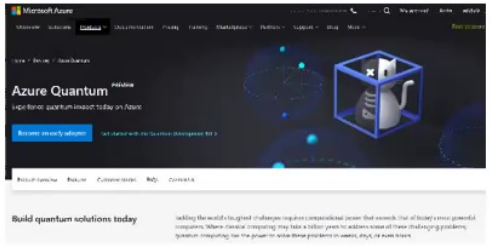
Baidu, Alibaba and Tencent jockey for position in the development of quantum computing, which delivers a faster and more efficient approach to processing information than today's fastest computers

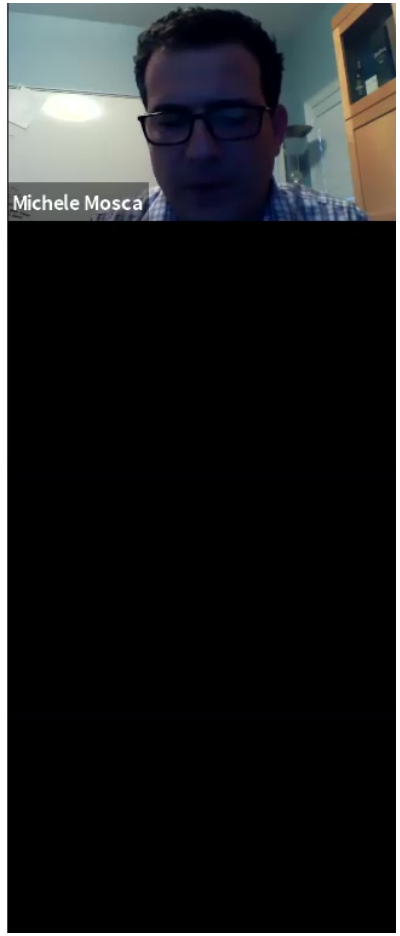
PUBLISHED : Monday, 12 March, 2018, 9:03am
UPDATED : Monday, 12 March, 2018, 9:02am

Baidu has entered the race to build quantum computers

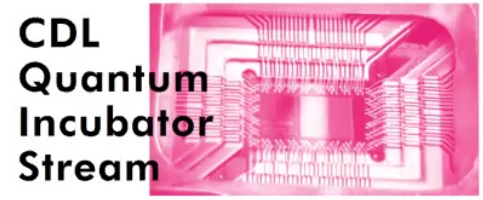


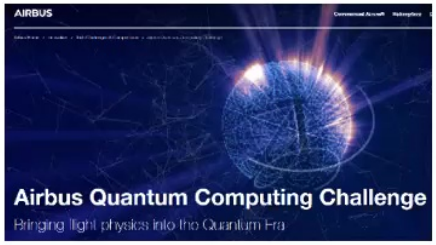






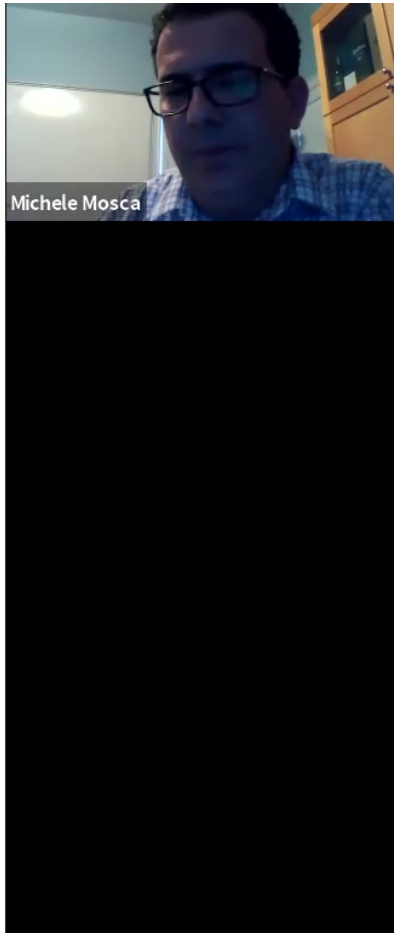
The Amazon Quantum Solutions Lab will help you get ready for quantum computing.





What can you do **now** with a quantum computer?

- Currently, not enough qubits for a realistic speed-up *(in circuit model)*. Proof-of-principle quantum programs.
- Main prize: understand NOW what it takes to use one and identify potential business cases, so your business will benefit ASAP once the tech is out there
- Priority: finding applications and optimizing algorithms
- Resource counts continue to decline as we improve algorithms/software; make sure you are prepared
- Plausible that in next 2-4 years (e.g. IARPA LogiQ) that a fault-tolerant qubit is demonstrated, followed by intense scaling effort
- Possible that some quantum advantage is attainable with sufficiently large NISQ devices or quantum annealers.

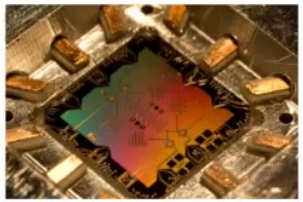


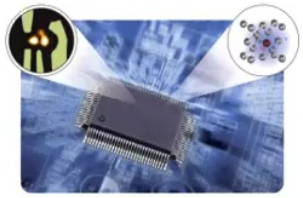
One serious problem for public-key cryptography

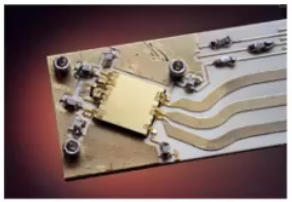
Algorithms for Quantum Computation: Discrete Logarithms and Factoring

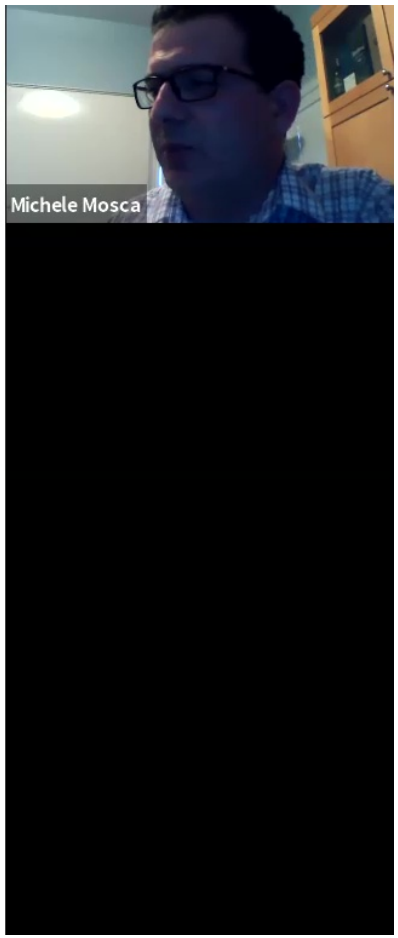
Peter W. Shor
AT&T Bell Labs
Room 2D-149
600 Mountain Ave.
Murray Hill, NJ 07974 USA

In Proceedings, 35th Annual Symposium on Foundations of Computer Science, Santa Fe, NM, November 20-22, 1994, IEEE Computer Society Press, pp. 124-134.


E. Lucero, D. Mariantoni, and M. Mariantoni


Christian Lagerek/Alamy

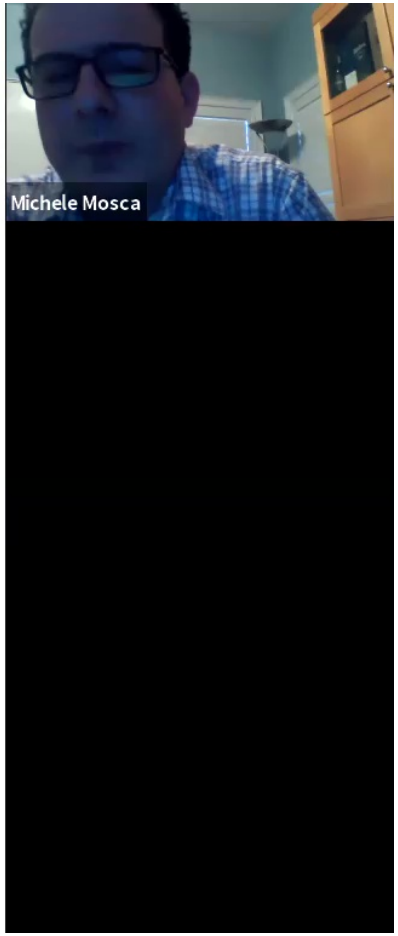

Y. Colombe/NIST



How secure will our current crypto algorithms be?

Algorithm	Key Length	Security level (Conventional Computer)	Security level (Quantum Computer)
RSA-1024	1024 bits	80 bits	~0 bits
RSA-2048	2048 bits	112 bits	~0 bits
ECC-256	256 bits	128 bits	~0 bits
ECC-384	384 bits	192 bits	~0 bits
AES-128	128 bits	128 bits	~64 bits
AES-256	256 bits	256 bits	~128 bits

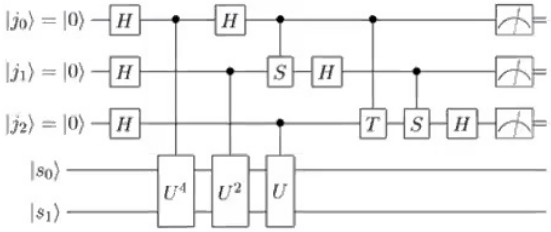
*For symmetric crypto, known attacks are “only” quadratic, so doubling key or hash lengths suffices (against known attacks).



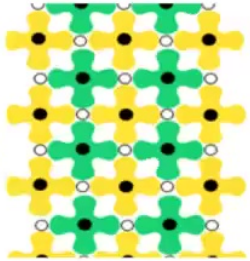
How large of a quantum computer is needed?

https://qsoft.iqc.uwaterloo.ca/

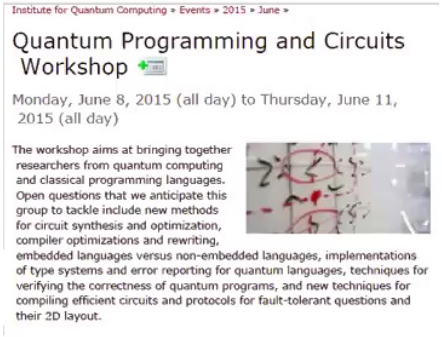
Algorithms (abstract layer)



Quantum circuits (logical layer)



Error correcting layer

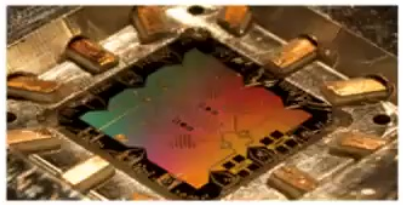


Institute for Quantum Computing » Events » 2015 » June »

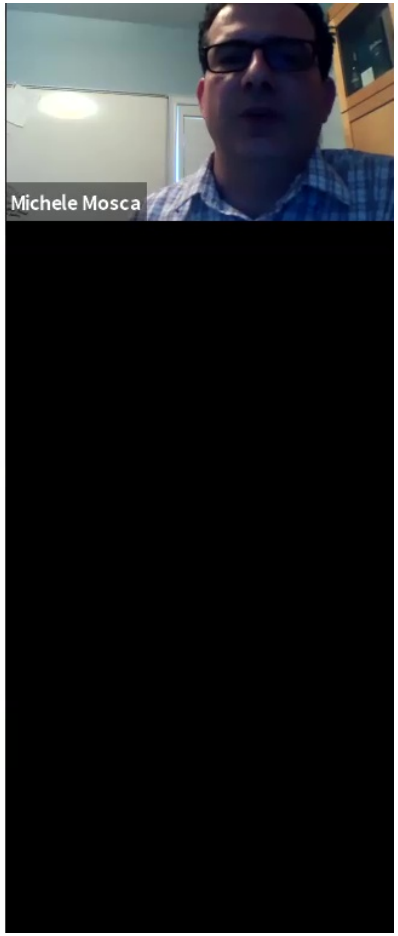
Quantum Programming and Circuits Workshop

Monday, June 8, 2015 (all day) to Thursday, June 11, 2015 (all day)

The workshop aims at bringing together researchers from quantum computing and classical programming languages. Open questions that we anticipate this group to tackle include new methods for circuit synthesis and optimization, compiler optimizations and rewriting, embedded languages versus non-embedded languages, implementations of type systems and error reporting for quantum languages, techniques for verifying the correctness of quantum programs, and new techniques for compiling efficient circuits and protocols for fault-tolerant questions and their 2D layout.

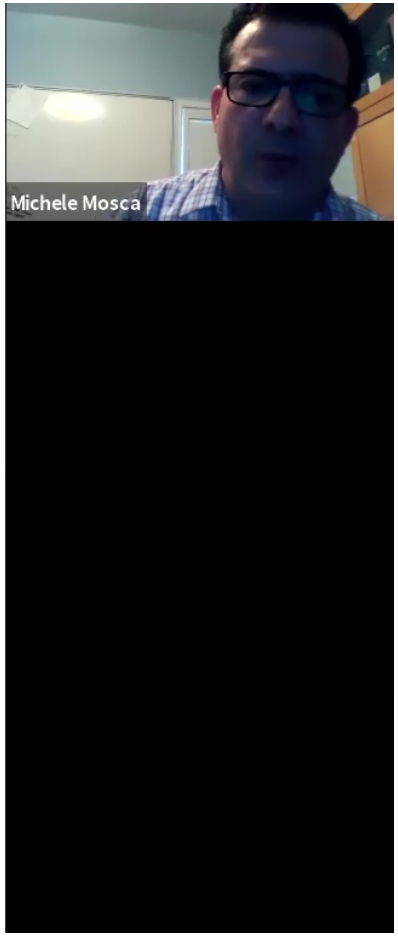


Hardware (physical layer)



Some useful circuit synthesis and optimization tools

- Brute force exhaustive synthesis of multi-qubit unitaries
- Parallel collision-finding algorithms applied to circuit synthesis
- Optimal T-depth synthesis of one-qubit unitaries
- Optimization of T-depth via matroid partitioning
- Optimizing phase polynomials via Reed-Muller decoding

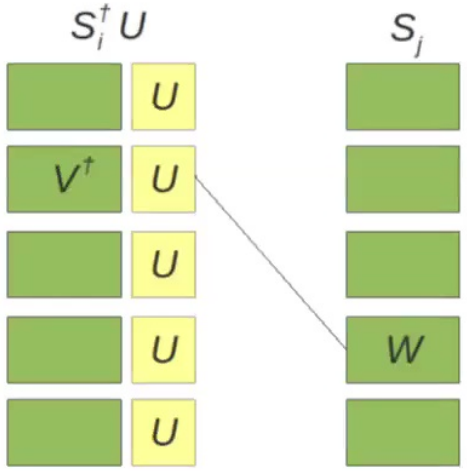


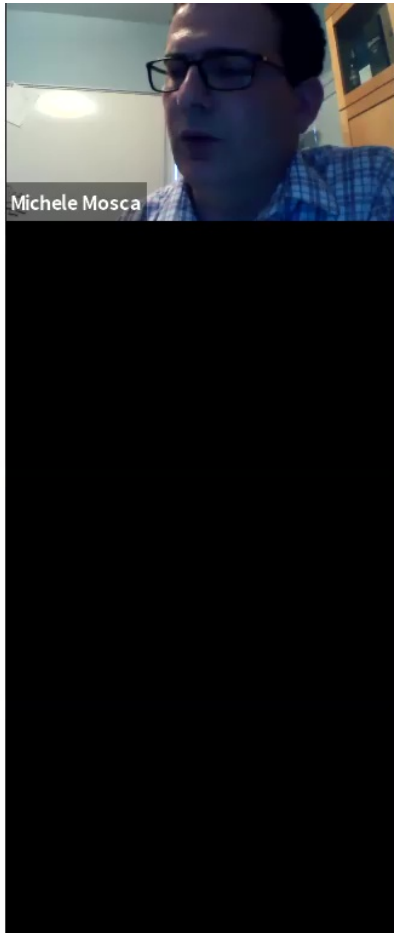
Synthesis tools

General multi-qubit MITM [AMMR13, TCAD]

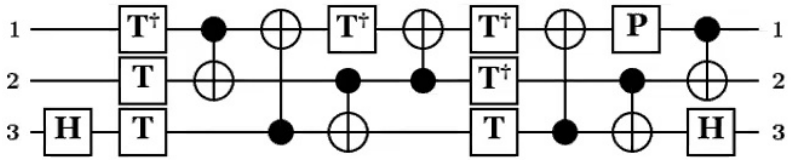
Applied parallel collision-finding method

[Di Matteo, M 16, QST]

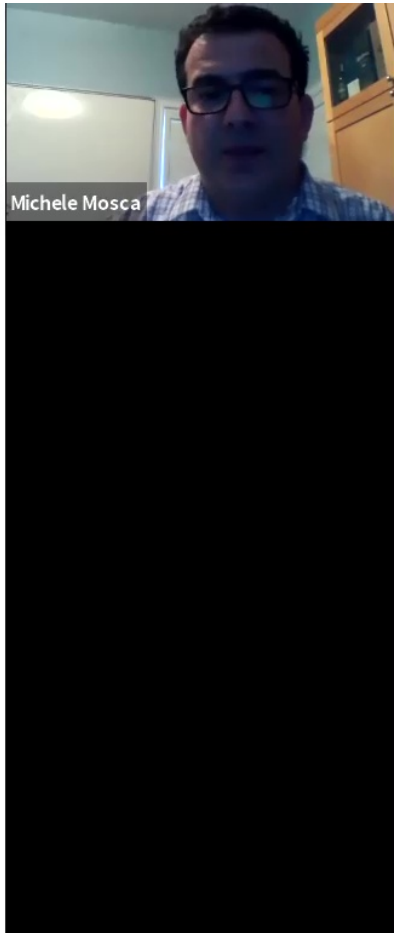




Efficient Toffoli circuits



- T-depth 3 Toffoli (40% improvement)



T-gate parallelization

- Selinger showed that the T-depth of the Toffoli could be reduced to 1 with the addition of enough ancilla qubits.

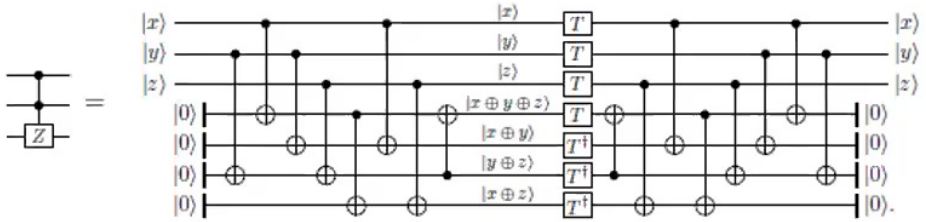
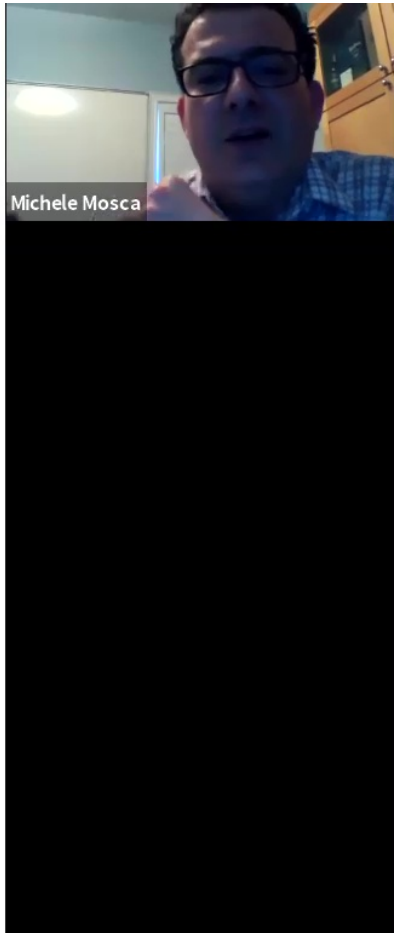


Figure 1: T-depth 1 representation of the Toffoli gate

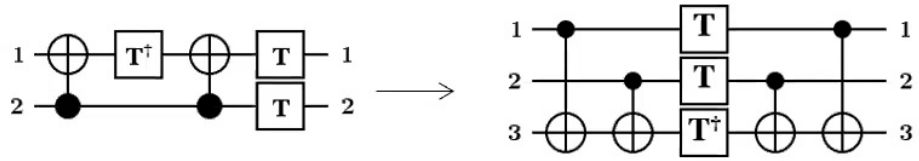
arXiv:1210.0974v2 [quant-ph] 3 Apr 2013



A framework for T-gate parallelization (AMM13)

arXiv:1303.2042v1 [quant-ph] 8 Mar 2013

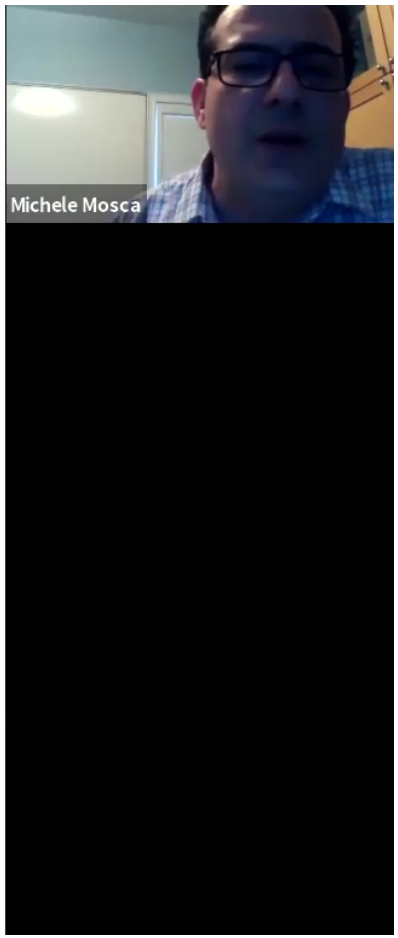
Our result: Can write {CNOT, T} circuits in T-depth 1 using unbounded ancillae



e.g. $U: |a,b\rangle \rightarrow e^{\frac{i\pi}{4}(-(a\oplus b)+a+b)}|a,b\rangle$

Idea: prepare qubits in states that are XORs of inputs then perform all T gates at once

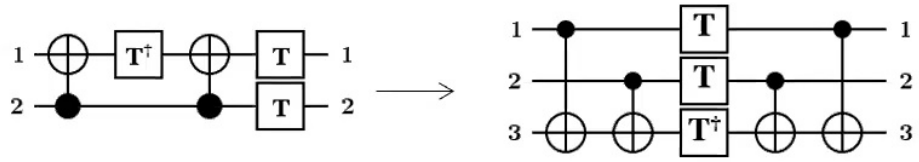
$$|ab0\rangle \rightarrow |a,b,a\oplus b\rangle \rightarrow e^{\frac{i\pi}{4}(-(a\oplus b)+a+b)}|a,b,a\oplus b\rangle \rightarrow e^{\frac{i\pi}{4}(-(a\oplus b)+a+b)}|a,b,0\rangle$$



A framework for T-gate parallelization (AMM13)

arXiv:1303.2042v1 [quant-ph] 8 Mar 2013

Our result: Can write {CNOT, T} circuits in T-depth 1 using unbounded ancillae

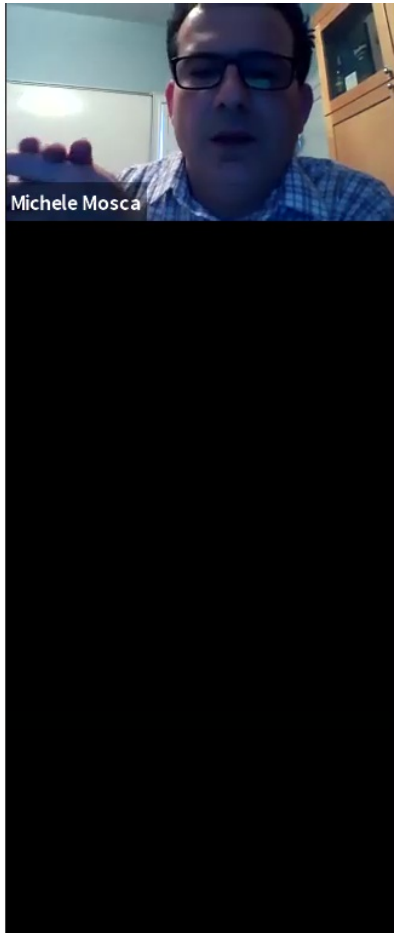


$$U\colon |a,b,c\ldots\rangle \to e^{\frac{i\pi}{4}\sum_{i=1}^{k} f_i(a,b,c,\ldots)}|g(a,b,c,\ldots\rangle$$

e.g. $U\colon |a,b\rangle \to e^{\frac{i\pi}{4}(-(a\oplus b)+a+b)}|a,b\rangle$

Idea: prepare qubits in states that are XORs of inputs then perform all T gates at once

$$|ab0\rangle \to |a,b,a\oplus b\rangle \to e^{\frac{i\pi}{4}(-(a\oplus b)+a+b)}|a,b,a\oplus b\rangle \to e^{\frac{i\pi}{4}(-(a\oplus b)+a+b)}|a,b,0\rangle$$



A framework for T-gate parallelization (AMM13)

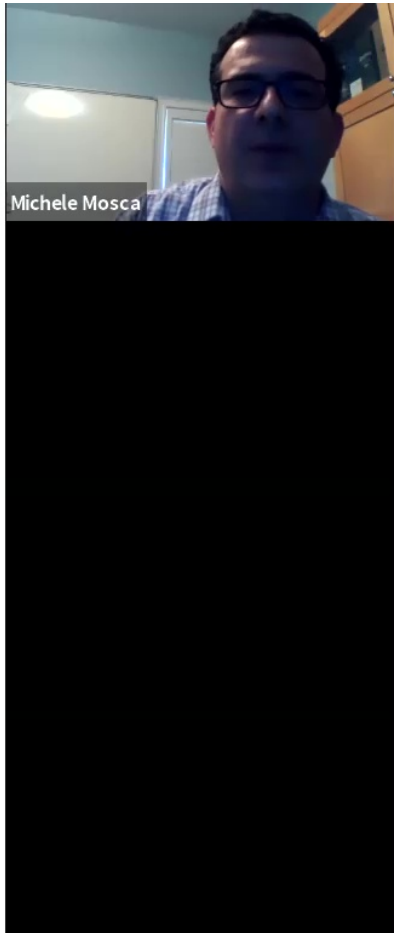
arXiv:1303.2042v1 [quant-ph] 8 Mar 2013

Also considered any given number of ancilla qubits.

e.g. if we have 80 terms in 6 variables and 2 ancilla qubits (so 8 qubits total), can we partition the variables into 10 parts, and have T-depth 8?

It depends: each part should be able to reconstruct the input bits.

- **Matroid partitioning**
  - poly-time algorithm for finding minimal partitions of matroids (a set with an independence relation)



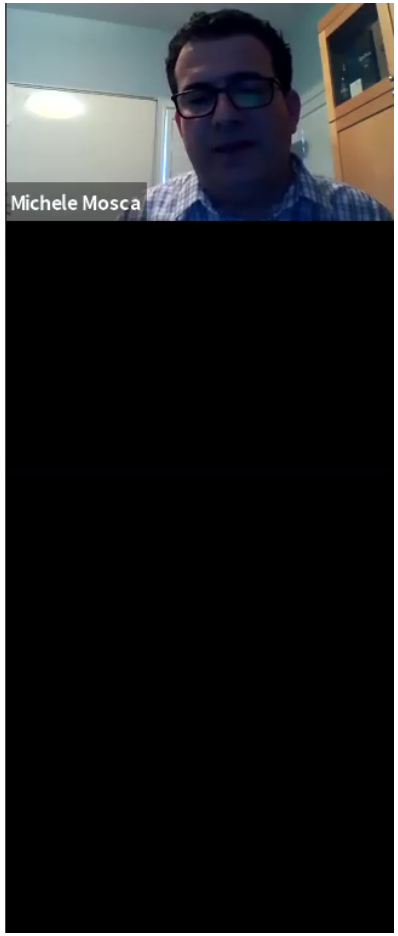
T-parallelization algorithm

- First write circuit over {CNOT, T, H}
- For each {CNOT, T} subcircuit:
  - Find $f_1, \ldots, f_k, g$ s.t.

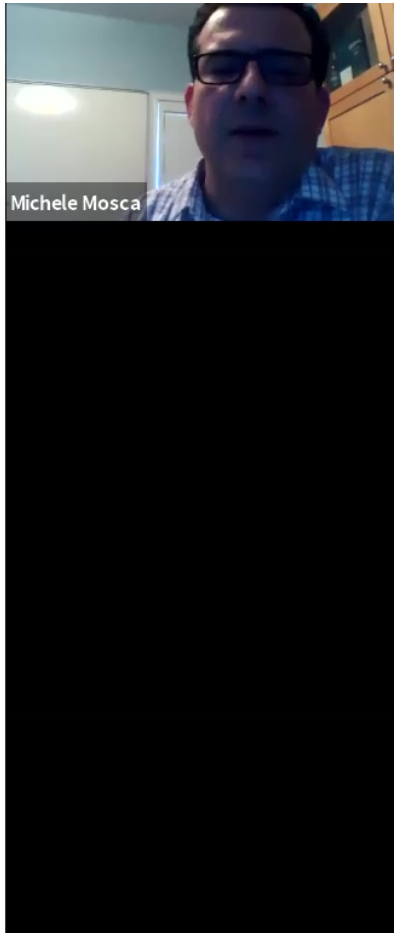
    $$U: |abc \ldots\rangle \rightarrow e^{\frac{i\pi}{4}\sum_{i=1}^{k} f_i(a,b,c,\ldots)} |g(a,b,c,\ldots\rangle$$
  - Find minimal partition P of $f_1, \ldots, f_k$
  - For each $p \in P$, synthesize T-depth 1 circuit for

    $$V: |abc \ldots\rangle \rightarrow e^{\frac{i\pi}{4}\sum_{f\in p} f(a,b,c,\ldots)} |abc \ldots\rangle$$

- Benchmark results (18 arithmetic circuits):
  - 32.1% avg *T*-count reduction
  - 53.5% avg *T*-depth reduction (no ancillas)
  - 82.4% avg *T*-depth reduction (as many ancillas as inputs)



One-qubit gate synthesis (thanks to Vadym Kliuchnikov for slides)



- Algorithm building block: **Quantum Fourier Transform**
  - Uses $R_Z(\phi) = \begin{pmatrix} e^{-i\phi/2} & 0 \\ 0 & e^{i\phi/2} \end{pmatrix}, \phi = \frac{\pi}{2^n}$
- Available gates in **Clifford+T** gate library:
  - Single qubit:
    - $T = \begin{pmatrix} 1 & 0 \\ 0 & \omega \end{pmatrix}, \omega = e^{i\pi/4} \qquad H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$
    - $P = \begin{pmatrix} 1 & 0 \\ 0 & \omega^2 \end{pmatrix}$, Pauli: X, Y, Z
  - Two qubit: $CNOT = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$

Known approaches to unitary approximation

[Before number-theoretic methods]

Name	Gates	Classical run-time	Number of ancillae	Resource state
[1] Solovay-Kitaev	$O\left(\log^{3.97}(1/\varepsilon)\right)$	$O\left(\log^{2.71}(1/\varepsilon)\right)$	0	no
[2] Brute force	$O(\log(1/\varepsilon))$	$2^{O(\log^c(1/\varepsilon))}$	0	no
[3] Phase kickback	$O(\log(1/\varepsilon))$	$O(\log(1/\varepsilon))$	$O(\log(1/\varepsilon))$	yes
[4] PAR	$O(1)$	$O(\log(1/\varepsilon))$	$O(1)$	yes
[5]States ladder	$O\left(\log^{>1.12}(1/\varepsilon)\right)$			yes

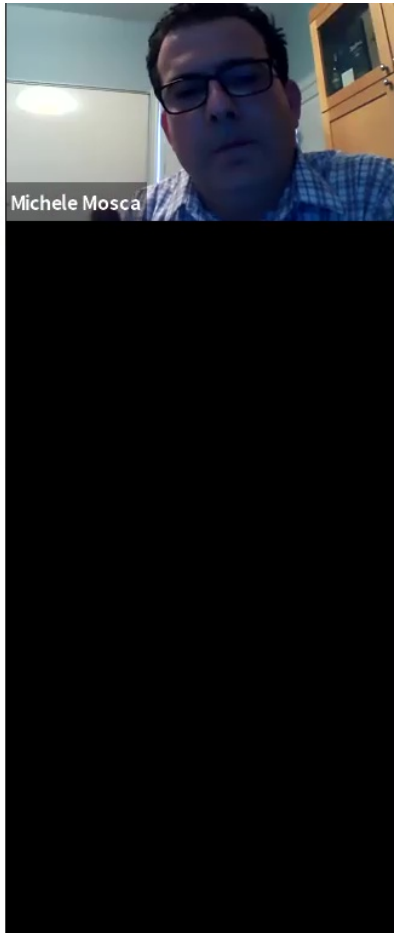
[1] C. M. Dawson and M. A. Nielsen, "The Solovay-Kitaev algorithm" [2005], [1995,1997][Any universal gate set]

[2] A. G. Fowler, "Constructing arbitrary Steane code single logical qubit fault-tolerant gates" [2004][Clifford+T]

[3] A. Y. Kitaev, A. H. Shen, and M. N. Vyalyi, Classical and Quantum Computation [1999][Clifford+T]

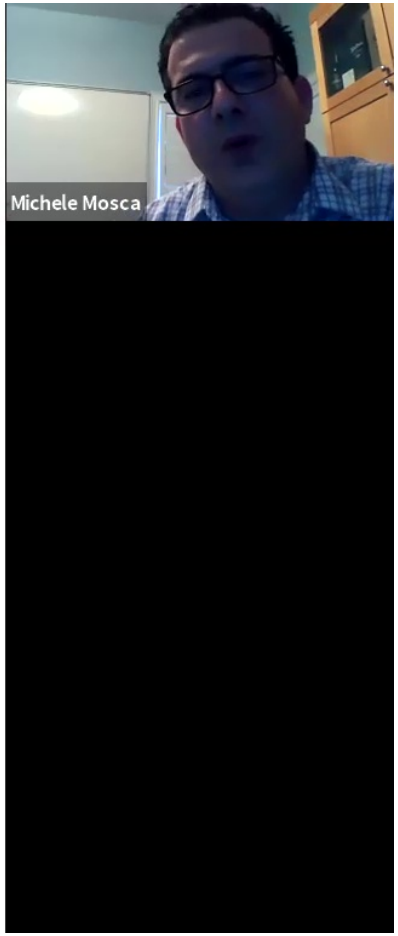
[4] N. C. Jones et al. "Simulating chemistry efficiently on fault-tolerant quantum computers" [2012][Clifford+T]

[5] G. Duclos-Cianci, K. M. Svore "A State Distillation Protocol to Implement Arbitrary Single-qubit Rotations" [2012][Clifford+T]

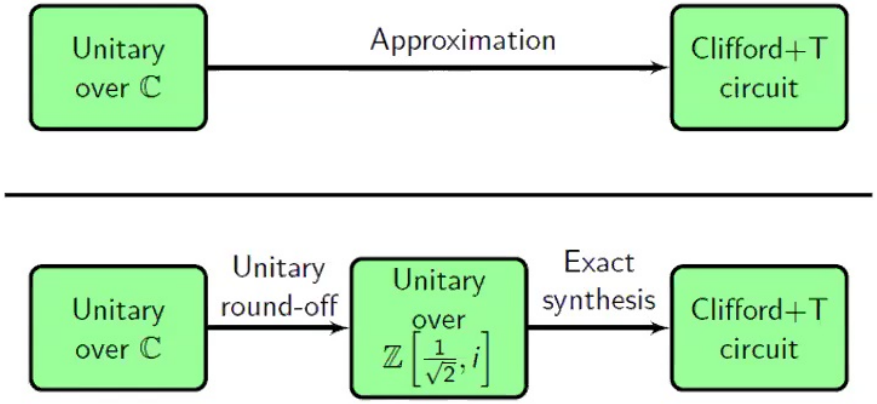


Non-constructive results

- Exists gate set saturating bound $O(\log(1/\varepsilon))$ for $SU(2)$:
  - A. Lubotzky, R. Phillips and P. Sarnak "Hecke operators and distributing points on the sphere I", [1986]
  - A. Lubotzky, R. Phillips and P. Sarnak "Hecke operators and distributing points on the sphere II", [1987]
- Exists gate set saturating bound$O(\log(1/\varepsilon))$ for $SU(d)$:
  - A. W. Harrow, B. Recht, I. L. Chuang "Efficient Discrete Approximations of Quantum Gates", [2001]
- Any universal gate set with algebraic entries saturates bound $O(\log(1/\varepsilon))$ in $SU(2)$
  - J. Bourgain, A. Gamburd, "On the spectral gap for finitely generated subgroups of SU(2)", [2008]
- Any universal gate set with algebraic entries saturates bound $O(\log(1/\varepsilon))$ in $SU(d)$
  - J. Bourgain, A. Gamburd, "A Spectral Gap Theorem in SU(d)" [2011]

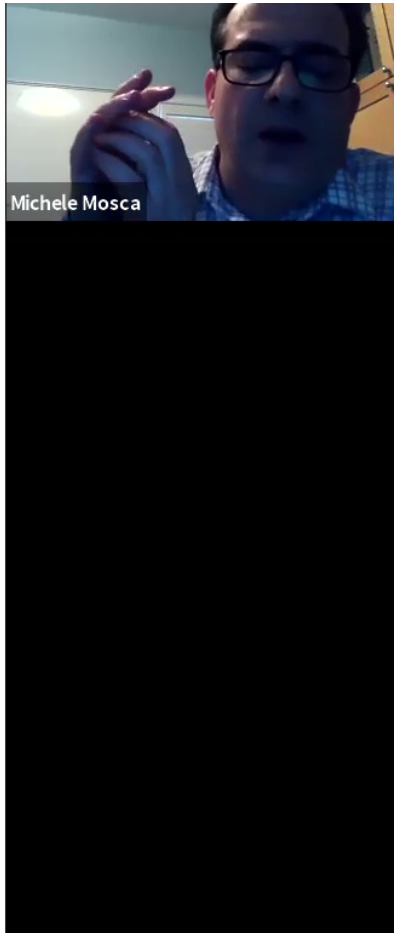


New approach to unitary approximation



$$\mathbb{Z}\left[\frac{1}{\sqrt{2}}, i\right] := \left\{ \frac{1}{\sqrt{2}^n} \left(a + b\omega + c\omega^2 + d\omega^3\right) \middle| a, b, c, d, n \in \mathbb{Z} \right\}, \omega = e^{i\pi/4}$$

[KMM13] V. Kliuchnikov, D. Maslov, and M. Mosca, "Fast and efficient exact synthesis of single qubit unitaries generated by Clifford and T gates", in Quantum Information and Computation. [arXiv:1206.5236]



Single qubit exact synthesis: main result

- Gate set $\mathscr{G}$: $H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$, $T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}$

  $P = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$, Pauli X, Y, Z

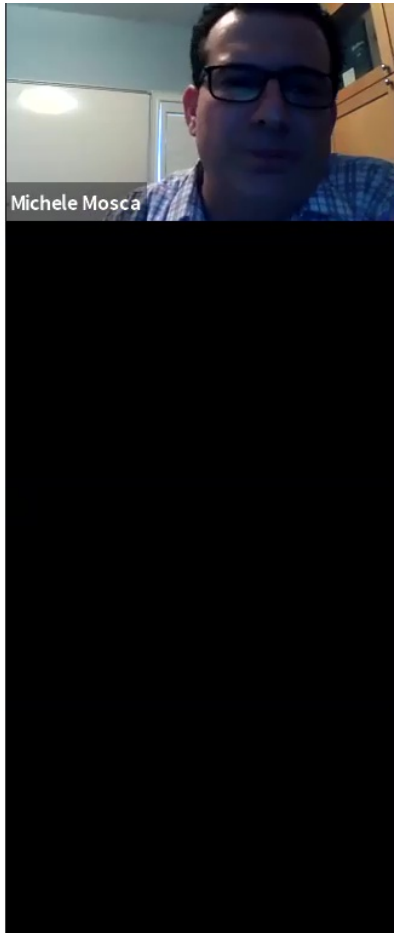
Theorem

Single qubit unitary U can be implemented exactly using $\mathscr{G}$ if and only if it has entries of the form:

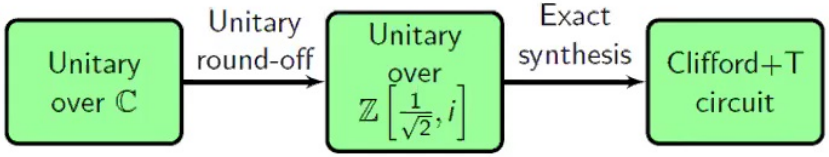
$$\frac{1}{\sqrt{2}^n}\left(a + b\omega + c\omega^2 + d\omega^3\right) a, b, c, d, n \in \mathbb{Z}$$

$$\omega = e^{i\pi/4}.$$

There exists an efficient algorithm that produces circuit that implements unitary with a minimal number of H and T gates.



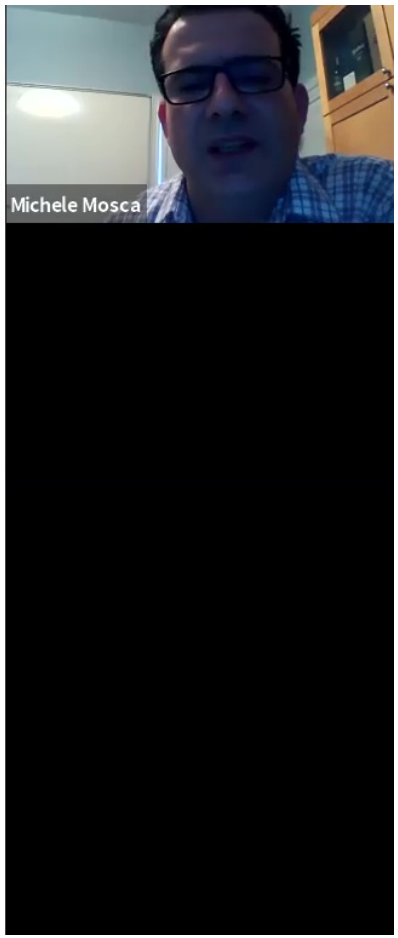
Rigorous efficient single qubit exact synthesis
(with two ancilla qubits)



Goal Approximate $\Lambda\left(e^{i\phi}\right) : \alpha|0\rangle + \beta|1\rangle \rightarrow \alpha|0\rangle + e^{i\phi}\beta|1\rangle$

Solution Approximately implement
$\alpha|000\rangle + \beta|100\rangle \rightarrow \alpha|000\rangle + e^{i\phi}\beta|100\rangle$

- Find a unitary U that approximately prepares $e^{i\phi}|00\rangle$ starting from $|00\rangle$
- Execute U controlled on the first qubit



Rounding off state $e^{i\phi}|00\rangle$

$$(\sin(\phi)+i\cos(\phi),0,0,0)$$
$$\Downarrow$$
$$|v\rangle=\tfrac{1}{2^n}\left(\lfloor 2^n\sin(\phi)\rfloor+i\lfloor 2^n\cos(\phi)\rfloor,a+ib,c+id,0\right)$$

Solving constraint $\||v\rangle\|=1$

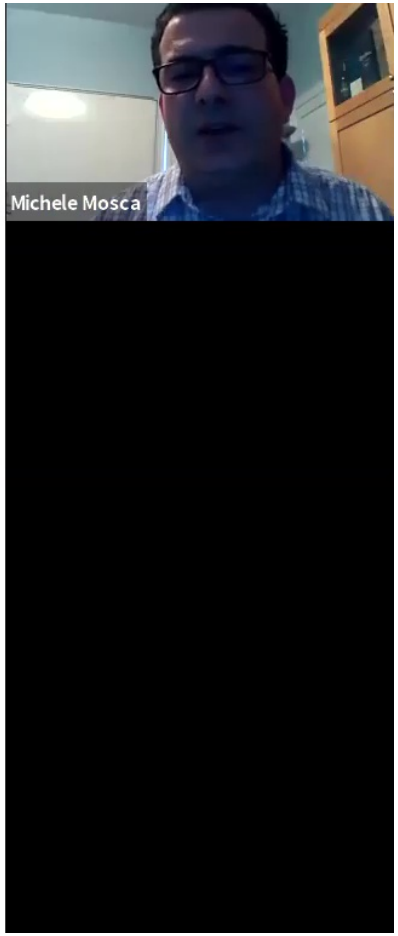
$$*: a^2+b^2+c^2+d^2=4^n-\lfloor 2^n\sin(\phi)\rfloor^2-\lfloor 2^n\cos(\phi)\rfloor^2=M$$

Complexity of finding a solution to $*$

$$O(\log^2(M)\log\log(M))$$

[$*$] M. O. Rabin and J. O. Shallit, "Randomized algorithms in number theory," Communications on Pure and Applied Mathematics, vol. 39, no. S1, pp. S239–S256, 1986.

[KMM13b] V. Kliuchnikov, D. Maslov, and M. Mosca, "Asymptotically optimal approximation of single qubit unitaries by Clifford and T circuits using a constant number of ancillary qubits", Physical Review Letters, **110**, 190502 (2013). [arXiv:1212.0822]



Post-Quantum Cryptography
Volume 9606 of the series Lecture Notes in Computer Science pp 29-43

Date: 04 February 2016

Applying Grover's Algorithm to AES: Quantum Resource Estimates

Markus Grassl, Brandon Langenberg, Martin Roetteler ✉ , Rainer Steinwandt

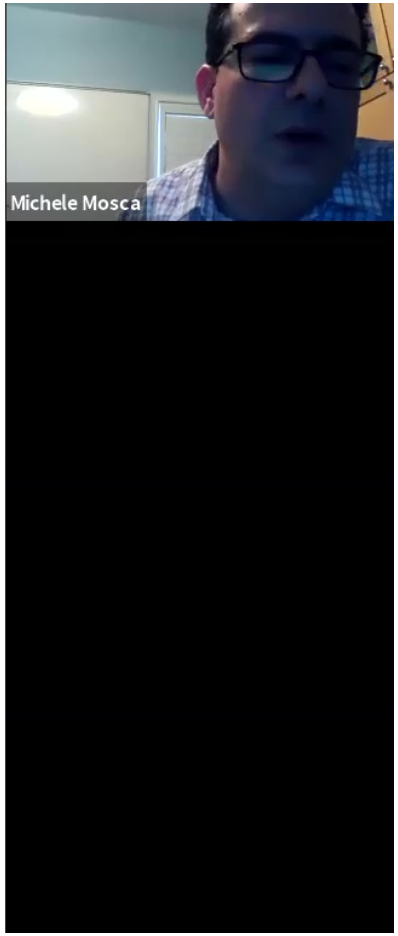
Our AES analysis, e.g. 192-bit AES:
5.9×10^6 qubits,
2^{121} surface code cycles,
$2^{137.5}$ total cost

Estimating the cost of generic quantum pre-image attacks on SHA-2 and SHA-3

Matthew Amy[1,4], Olivia Di Matteo[2,4], Vlad Gheorghiu[3,4], Michele Mosca[3,4,5,6], Alex Parent[2,4], and John Schanck[3,4]

		SHA-256	SHA3-256
Grover	T-count	1.27×10^{44}	2.71×10^{44}
	T-depth	3.76×10^{43}	2.31×10^{41}
	Logical qubits	2402	3200
	Surface code distance	43	44
	Physical qubits	1.39×10^7	1.94×10^7
Distilleries	Logical qubits per distillery	3600	3600
	Number of distilleries	1	294
	Surface code distances	$\{33, 13, 7\}$	$\{33, 13, 7\}$
	Physical qubits	5.54×10^5	1.63×10^8
Total	Logical qubits	$2^{12.6}$	2^{20}
	Surface code cycles	$2^{153.8}$	$2^{146.5}$
	Total cost	$2^{166.4}$	$2^{166.5}$

Table 3. Fault-tolerant resource counts for Grover search of SHA-256 and SHA3-256.



Bottom line for RSA-2048

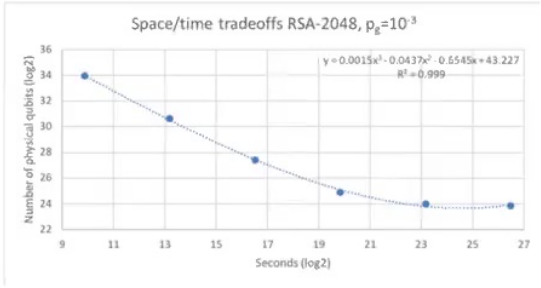


Fig. 4. RSA-2048 space/time tradeoffs with physical error rate per gate $p_g = 10^{-3}$. The scale is logarithmic (base 2). Approximately $y(16.3987) \approx 1.72 \times 10^8$ physical qubits are required to break the scheme in one day (24 hours). The number of T gates in the circuit is 2.41×10^{12}, the corresponding number of logical qubits is 4098, and the total number of surface code cycles is 4.69×10^{14}. The classical security parameter is approximately 112 bits.


arXiv.org > quant-ph > arXiv:1902.02332

Quantum Physics

Benchmarking the quantum cryptanalysis of symmetric, public-key and hash-based cryptographic schemes

Vlad Cheorghiu, Michele Mosca

(Submitted on 6 Feb 2019 (v1), last revised 7 Feb 2019 (this version, v2))

RSA-2048 – GIDNEY & EKERÅ UPDATES


arXiv.org > quant-ph > arXiv:1905.09749

Quantum Physics

How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits

Craig Gidney, Martin Ekerå

(Submitted on 23 May 2019)

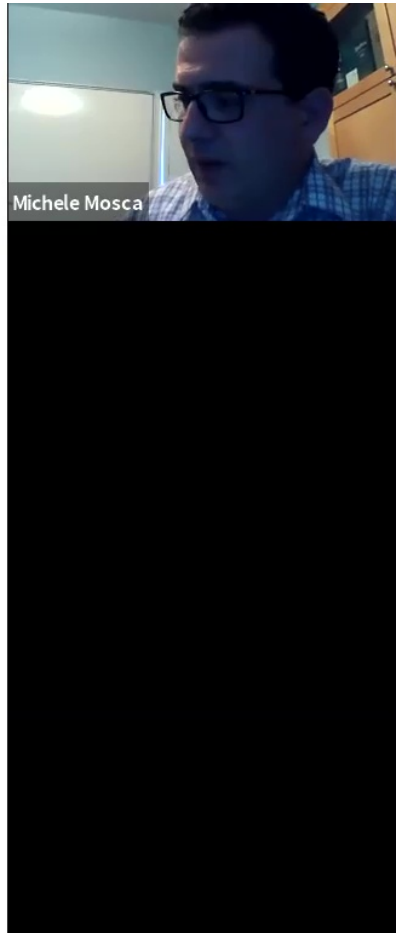
We significantly reduce the cost of factoring integers and computing discrete logarithms over finite fields on a quantum computer by combining techniques from Griffiths–Niu 1996, Zalka 2006, Fowler 2012, Ekerå–Håstad 2017, Ekerå 2017, Ekerå 2018, Gidney–Fowler 2019, Gidney 2019. We estimate the approximate cost of our construction using plausible physical assumptions for large-scale superconducting qubit platforms: a planar grid of qubits with nearest-neighbor connectivity, a characteristic physical gate error rate of 10^{-3}, a surface code cycle time of 1 microsecond, and a reaction time of 10 micro-seconds. We account for factors that are normally ignored such as noise, the need to make repeated attempts, and the spacetime layout of the computation. When factoring 2048 bit RSA integers, our construction's spacetime volume is a hundredfold less than comparable estimates from earlier works (Fowler et al. 2012, Gheorghiu et al. 2019). In the abstract circuit

no. of physical qubits reduced by ~10^2

Resource requirements keep going down.

	Physical assumptions				Approach		Estimated costs		
Historical cost estimate at $n = 2048$	Physical gate error rate	Cycle time (microseconds)	Reaction time (microseconds)	Physical connectivity	Distillation strategy	Execution strategy	Physical qubits (millions)	Expected runtime (days)	Expected volume (megaqubitdays)
Fowler et al. 2012 [17]	0.1%	1	0.1	planar	1200 T	single threaded	1400	1.1	1100
O'Gorman et al. 2017 [18]	0.1%	10	1	arbitrary	block CCZ	single threaded	220	3.7	850
Gheorghiu et al. 2019 [19]	0.1%	0.2	0.1	planar	1100 T	single threaded	170	1	170
(ours) 2019 (1 factory)	0.1%	1	10	planar	1 CCZ	serial distillation	16	6	90
(ours) 2019 (1 thread)	0.1%	1	10	planar	14 CCZ	single threaded	19	0.30	6.6
(ours) 2019 (parallel)	**0.1%**	**1**	**10**	**planar**	**28 CCZ**	**double threaded**	**20**	**0.31**	**5.9**

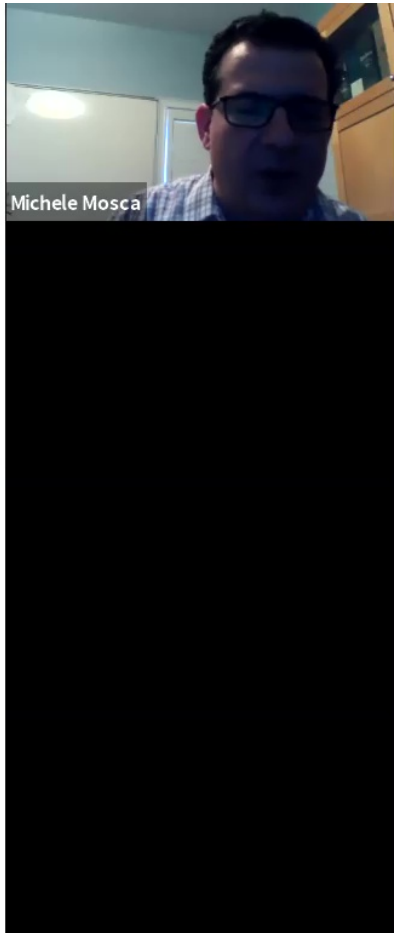
TABLE II. Historical estimates of the expected costs of factoring $n = 2048$ bit RSA integers, and the assumptions they used. Our spacetime volumes can be directly compared to the volume from Fowler et al. (we achieve a 165x improvement), because Fowler et al's estimate is dominated by distillation and changing the reaction time doesn't affect this volume. It is unclear how to compare O'Gorman et al.'s volume to ours, because of the difference in connectivity. Multiplying the volume from Gheorghiu et al. by 5, to account for the difference in cycle time, allows comparison to our volume (we achieve a 140x improvement). See Appendix B for details on each entry in this table.



Cloud computing, payment systems, internet, IoT, eHealth, etc…

Secure web browsing, Auto-updates, VPN, Secure email, Blockchain, etc…

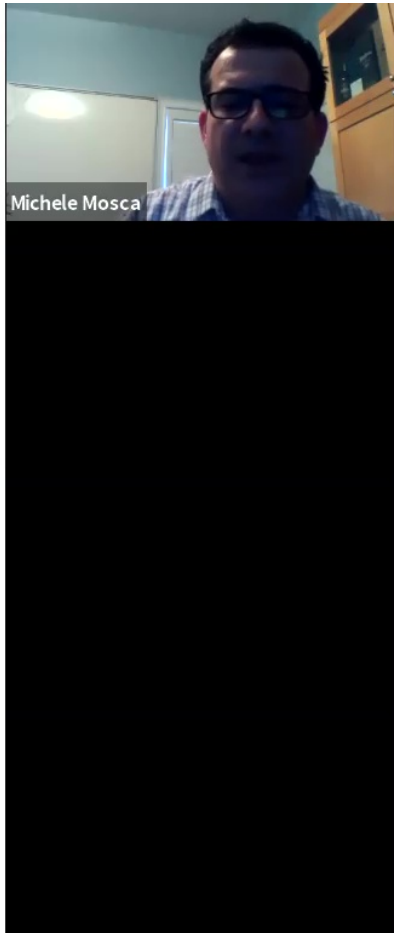
Cryptography:RSA, DSA, DH, ECDH, ECDSA,…, SHA, AES



Cloud computing, payment systems, internet, IoT, eHealth, etc…

Secure web browsing, Auto-updates, VPN, Secure email, Blockchain, etc…

Cryptography:RS… DH, ECD… DSA,…, SHA, AES



Non-fault-tolerant quantum devices

i.e. *quantum annealers, quantum simulators, NISQ*

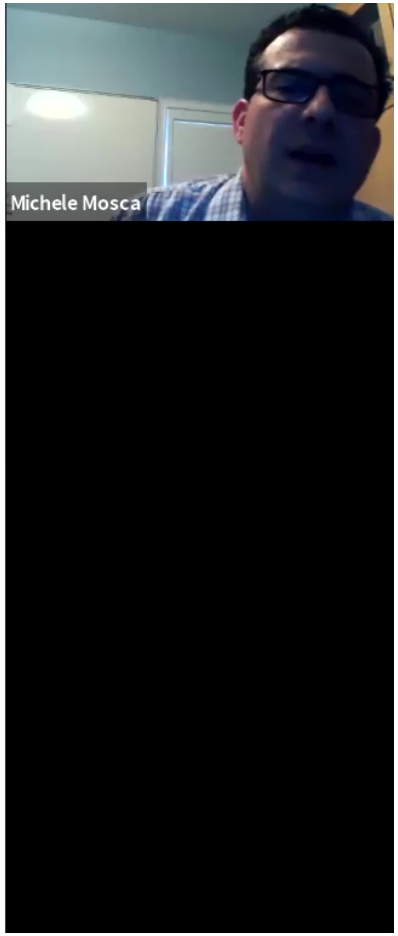
Not a known threat to cryptography

- Can they capture *some* of the power of quantum computation?
- Can they simulate themselves or similar systems faster/cheaper than conventional computers?
- Can they solve *useful* problems better than conventional devices?
- Can the same platforms be leveraged for fault-tolerant quantum computing?

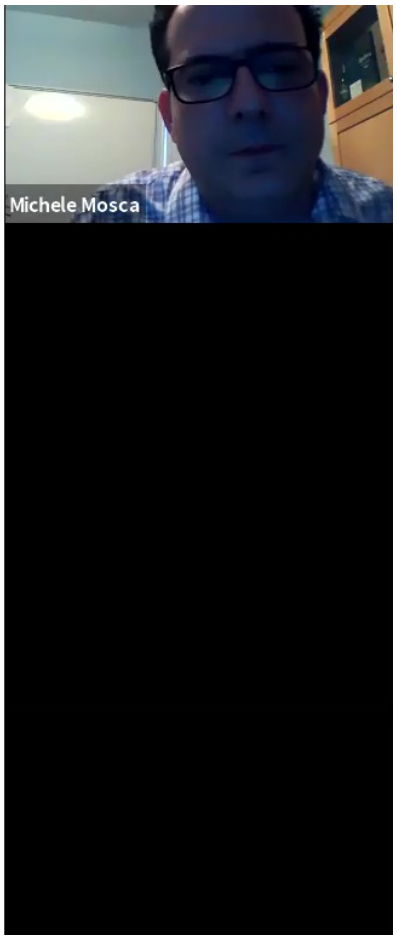
"Similarly, although there is no proof today that imperfect quantum machines can compute fast enough to solve practical problems, that may change."

Commercialize early quantum technologies

Masoud Mohseni, Peter Read, Hartmut Neven and colleagues at Google's Quantum AI Laboratory set out investment opportunities on the road to the ultimate quantum machines.



On some alternative quantum factoring approaches…



Factoring semi-primes with (quantum) SAT-solvers

Michele Mosca*[1] and Sebastian R. Verschoor†[2]

and question the practical effectiveness of this approach for factoring large numbers. We find no evidence that this is a viable path toward factoring large numbers, even for scalable fault-tolerant quantum computers, as well as for various quantum annealing or other special purpose quantum hardware.

https://arxiv.org/pdf/1902.01448.pdf

On speeding up factoring with quantum SAT solvers

Michele Mosca[1], João Marcos Vensi Basso*[2], and Sebastian R. Verschoor[3]

We present a SAT circuit that can be given to quantum SAT solvers such as annealers in order to perform this step of factoring. If quantum SAT solvers achieve any speedup over classical brute-force search, then our factoring algorithm is faster than the classical NFS.

https://arxiv.org/pdf/1910.09592.pdf

A low-resource quantum factoring algorithm

Daniel J. Bernstein[1,2], Jean-François Biasse[3], and Michele Mosca[4,5,6]

heuristics, is $L^{p+o(1)}$ where $p > 1.9$. The new time complexity is asymptotically worse than Shor's algorithm, but the qubit requirements are asymptotically better, so it may be possible to physically implement it sooner.

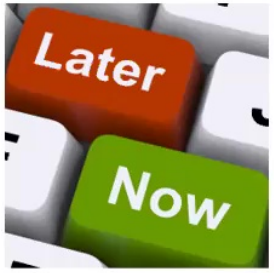
https://eprint.iacr.org/2017/352

Do we need to worry *now*?

Depends on*:

- *security shelf-life* (*x* years)
- *migration time (y years)*
- *collapse time (z years)*

"Theorem": If $x + y > z$, then worry.

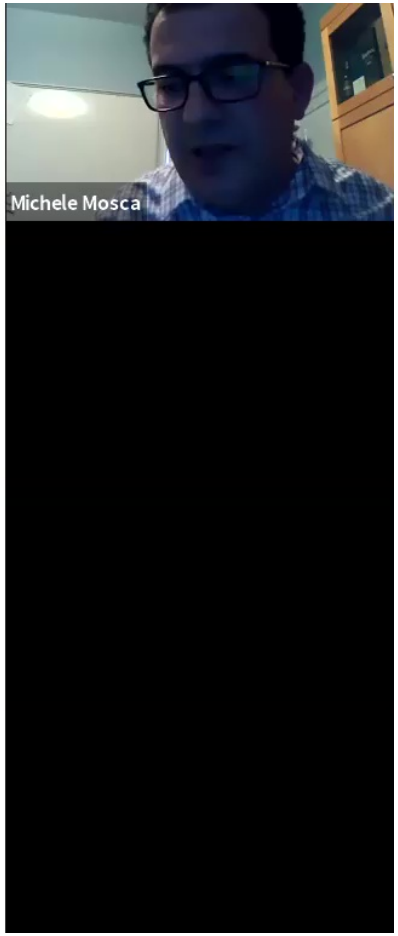



ZDNet

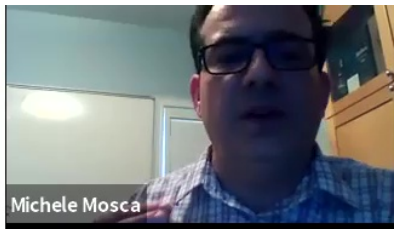
IBM warns of instant breaking of encryption by quantum computers: 'Move your data today'

Welcome to the future transparency of today as quantum computers reveal all currently encrypted secrets -- a viable scenario within just a few years.

*M. Mosca: e-Proceedings of 1st ETSI Quantum-Safe Cryptography Workshop, 2013. Also http://eprint.iacr.org/2015/1075



A very recent milestone



"Quantum supremacy"

nature

Article | Published: 23 October 2019

Quantum supremacy using a programmable superconducting processor

Frank Arute, Kunal Arya, [...] John M. Martinis

Nature **574**, 505–510 (2019) | Download Citation

2139 Altmetric | Metrics »

Google claims it has achieved 'quantum supremacy' – but IBM disagrees

Task that would take most powerful supercomputer 10,000 years 'completed by quantum machine in minutes'

Critical Future Milestone:
Scalable fault-tolerant logical qubits

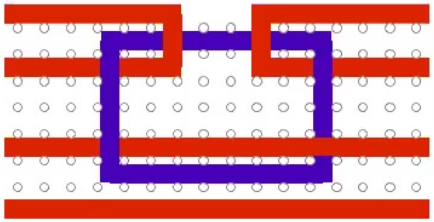
Logical layer

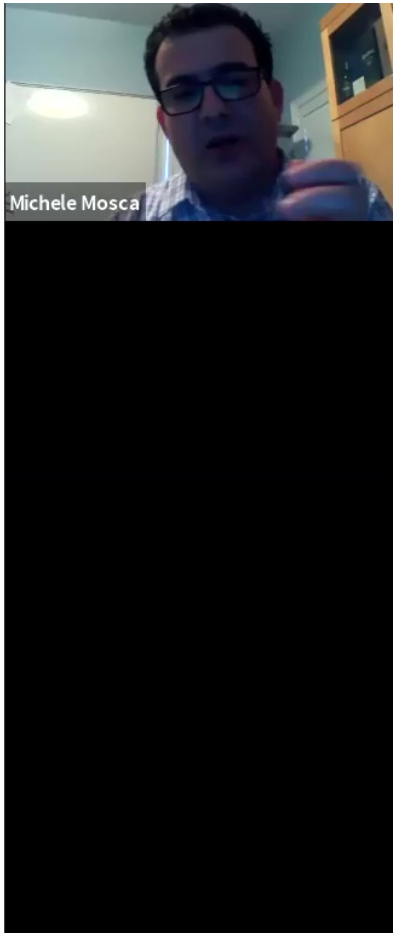
Physical layer

CNOT

=

fault-tolerant CNOT





Estimating ‘z’?

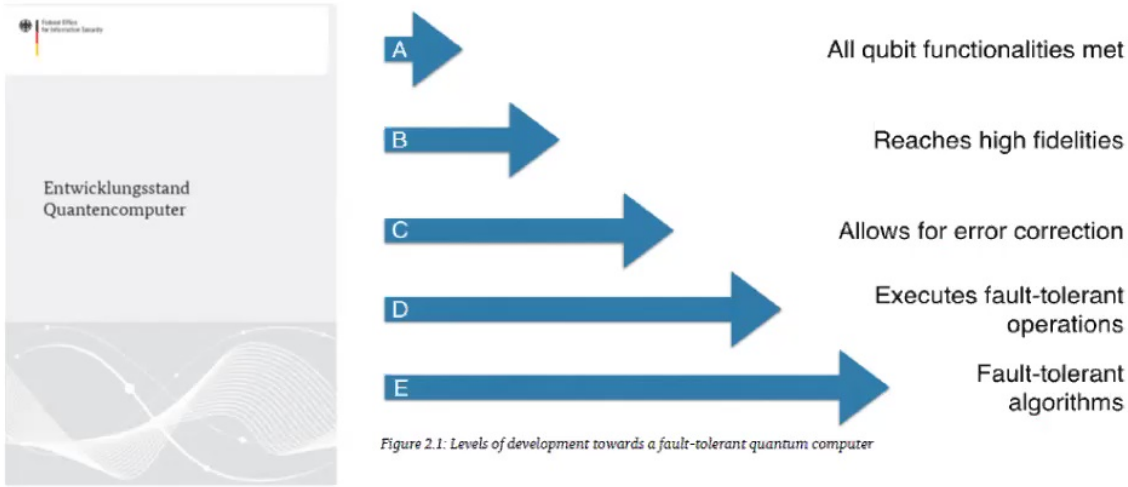
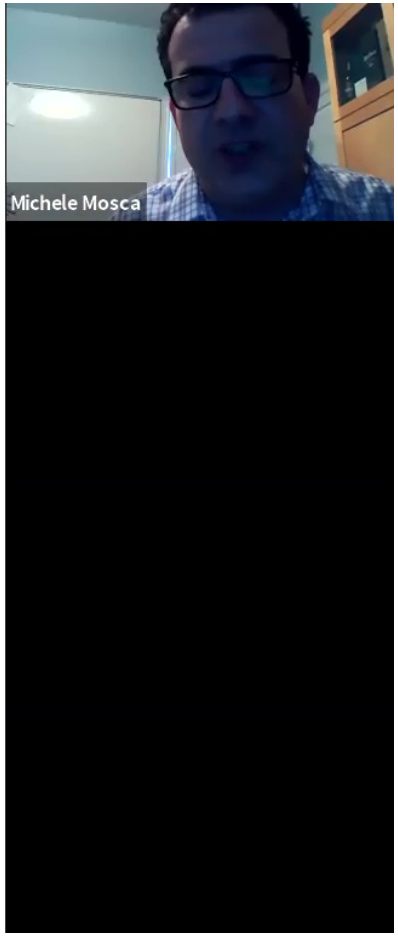


Figure 2.1: Levels of development towards a fault-tolerant quantum computer

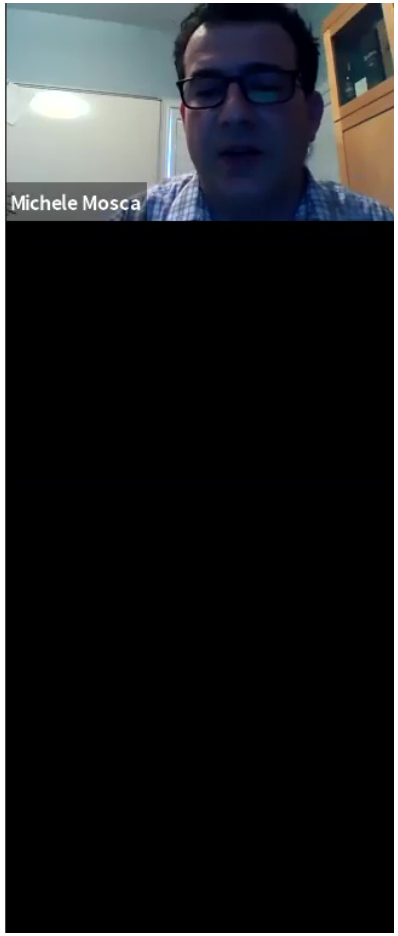
https://www.bsi.bund.de/DE/Publikationen/Studien/Quantencomputer/quantencomputer.html
(first draft in 2018; updated version 1.1 in 2019)



What is ‘z’?

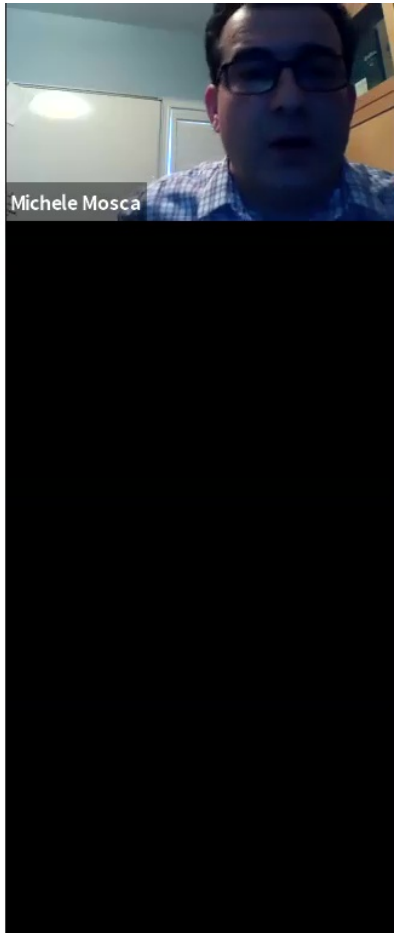
- **Michele Mosca** [Oxford, 1996]: *“20 qubits in 20 years”*
- **Microsoft Research** [October 2015]: *”Recent improvements in control of quantum systems make it seem feasible to finally build a quantum computer* **within a decade**”.
- **Michele Mosca** ([NIST, April 2015], [ISACA, September 2015]): *“1/7 chance of breaking RSA-2048 by 2026, ½ chance by 2031”*
- **Michele Mosca** [London, September 2017]*: “1/6 chance within 10 years”*
- **Simon Benjamin** [London, September 2017]: *Speculates that if someone is willing to “go Manhattan project” then “maybe 6-12 years”*
- **Michele Mosca** [Seattle, November 2019]: ***1/5 chance within 10 years***

See also: https://globalriskinstitute.org/publications/quantum-threat-timeline/

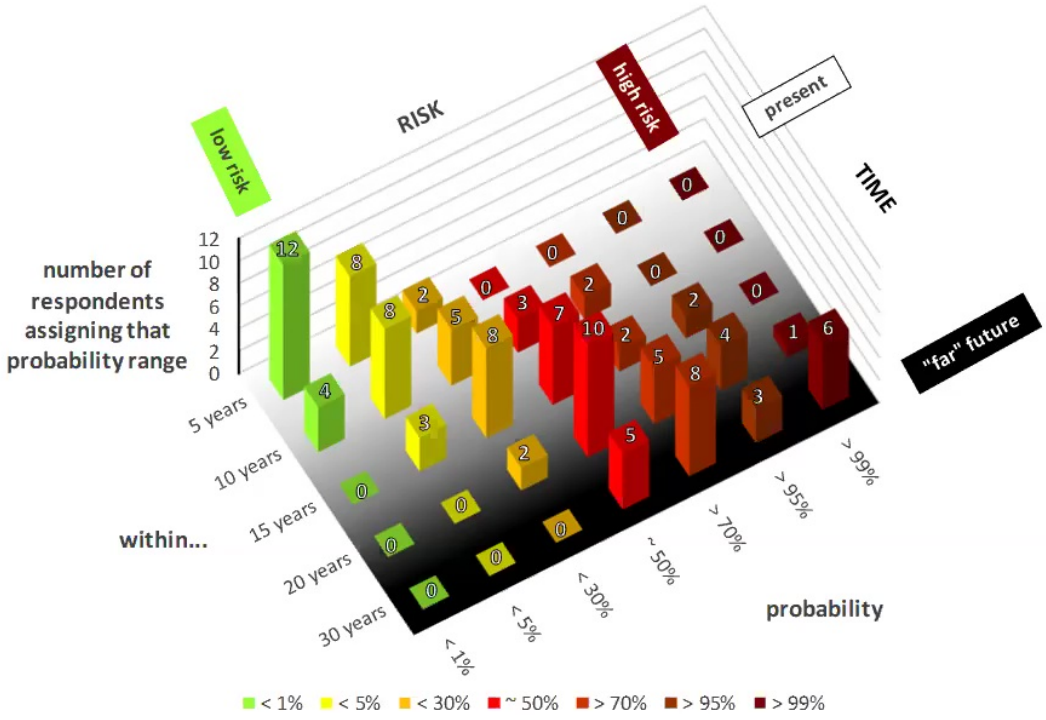


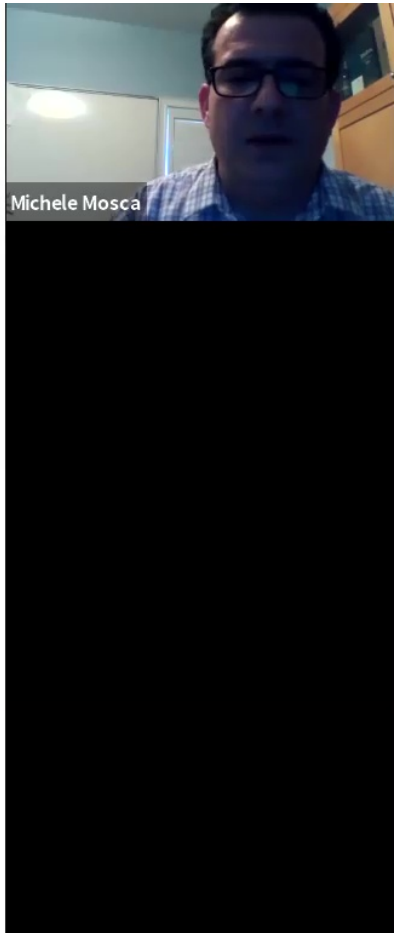
Name	Institution
Scott Aaronson	University of Texas at Austin
Dorit Aharonov	The Hebrew University of Jerusalem
Dave Bacon	Google
Simon Benjamin	University of Oxford
Alexandre Blais	Université de Sherbrooke
Ignacio Cirac	Max Planck Institute of Quantum Optics
Bill Coish	McGill University
David DiVincenzo	Forschungszentrum Jülich
Runyao Duan	Institute for Quantum Computing, Baidu Research
Martin Ekerå	KTH Royal Institute of Technology and Swedish NCSA
Artur Ekert	University of Oxford and National University of Singapore

Name	Institution
Daniel Gottesman	Perimeter Institute for Theoretical Physics and Quantum Benchmark Inc
Jungsang Kim	Duke University
Ashley Montanaro	University of Bristol
Andrea Morello	UNSW Sydney
Yasunobu Nakamura	The University of Tokyo
Tracy Northup	University of Innsbruck
Peter Shor	Massachusetts Institute of Technology
Stephanie Simmons	Simon Fraser University
Krysta Svore	Microsoft
Frank Wilhelm-Mauch	Saarland University
Shengyu Zhang	Tencent

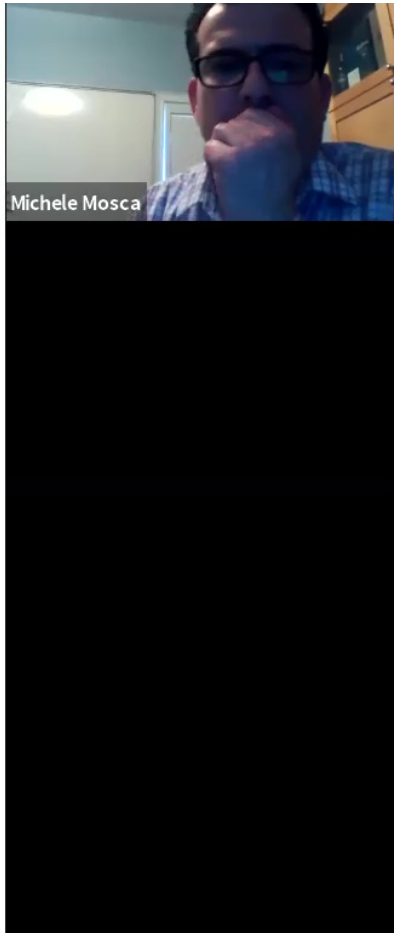


See also: https://globalriskinstitute.org/publications/quantum-threat-timeline/


Likelihood of a digital quantum computer able to break RSA-2048 in 24 hours as function of time
RISK
low risk
high risk
TIME
present
"far" future
number of respondents assigning that probability range
12
10
8
6
4
2
0
within...
5 years
10 years
15 years
20 years
30 years
probability
< 1%
< 5%
< 30%
~ 50%
> 70%
> 95%
> 99%


Michele Mosca

Quantum-safe cryptographic tool-chest



Quantum-safe cryptographic tool-chest

conventional quantum-safe cryptography

a.k.a. Post-Quantum Cryptography or Quantum Resistant Algorithms

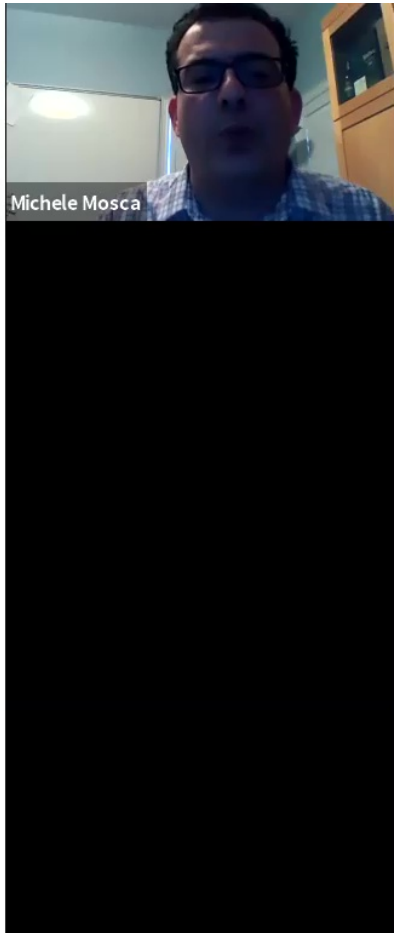
+

quantum cryptography

Courtesy of Qiang Zhang, USTC

http://www.idquantique.com/photon-counting/clavis3-qkd-platform/

Both sets of cryptographic tools can work very well together in quantum-safe cryptographic ecosystem



Terminology

“Quantum-safe”

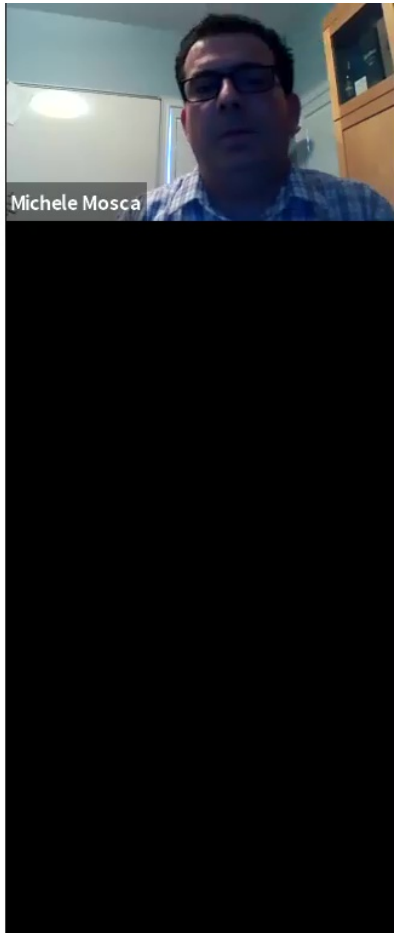
=

“designed to be safe in the era with large-scale quantum computers”

=

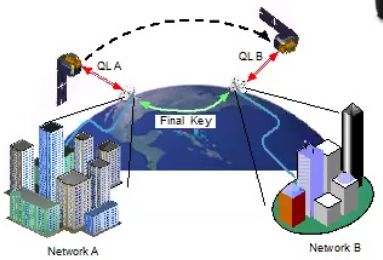
conventional “post-quantum”/ “quantum-resistant” cryptography

+ quantum cryptography

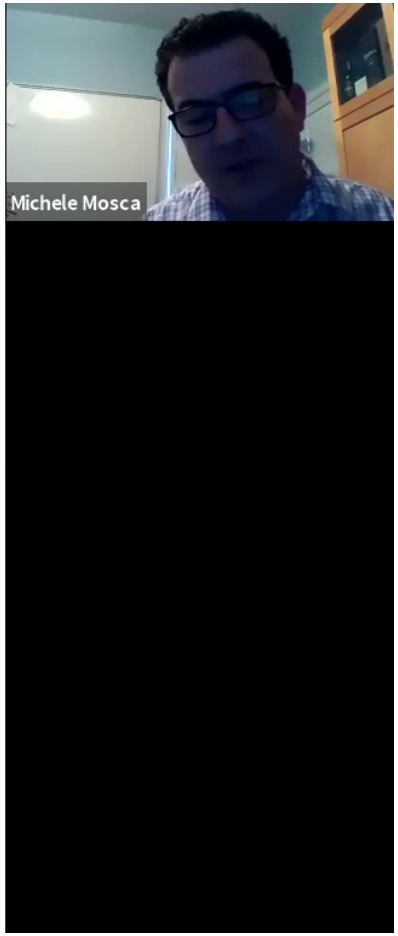


The ultimate key-establishment tool

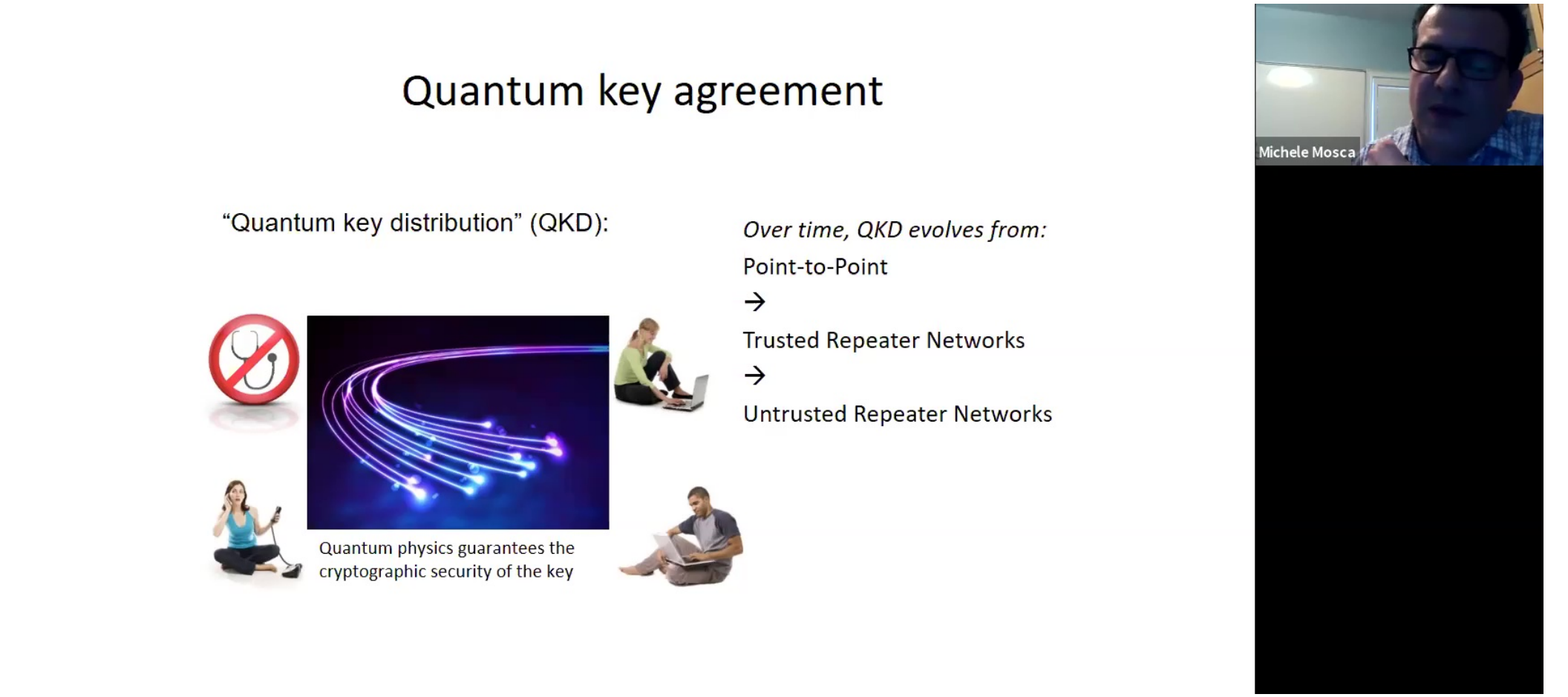
Quantum physics guarantees the security of the cryptographic key



- A quantum satellite in LEO can interconnect ground networks located anywhere on Earth.
- Together with ground-based repeaters, we will eventually have a "quantum internet".



Quantum key agreement



"Quantum key distribution" (QKD):

Quantum physics guarantees the cryptographic security of the key

Over time, QKD evolves from:

Point-to-Point

→

Trusted Repeater Networks

→

Untrusted Repeater Networks

Go “where the puck is going, not where it has been”

MACLEAN'S

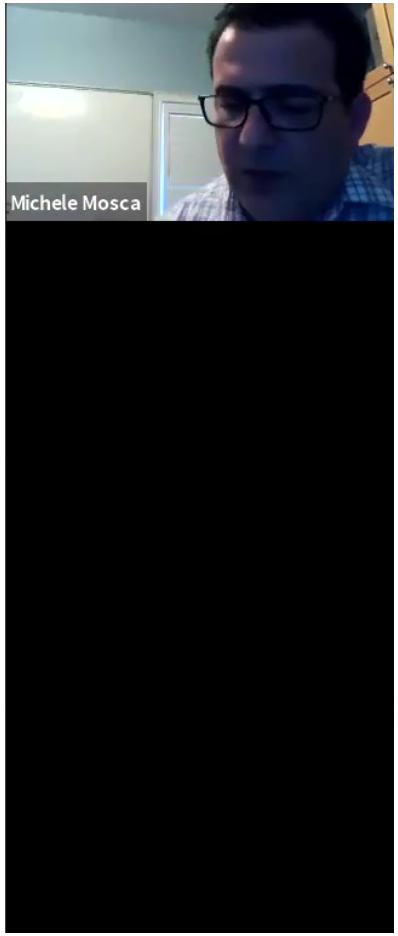
AUTHORS EDUCATION HUB THE ARCHIVE NEWSLETTERS CONTACT US

BUSINESS

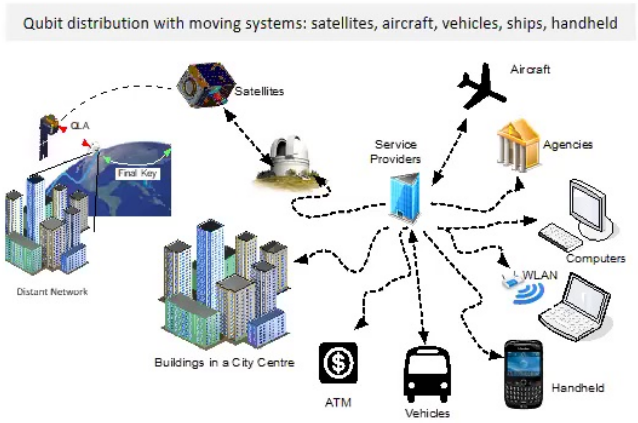
Why businesspeople won’t stop using that Gretzky quote

Everyone wants to be like Gretzky and skate to where the puck is going. Good luck with that.

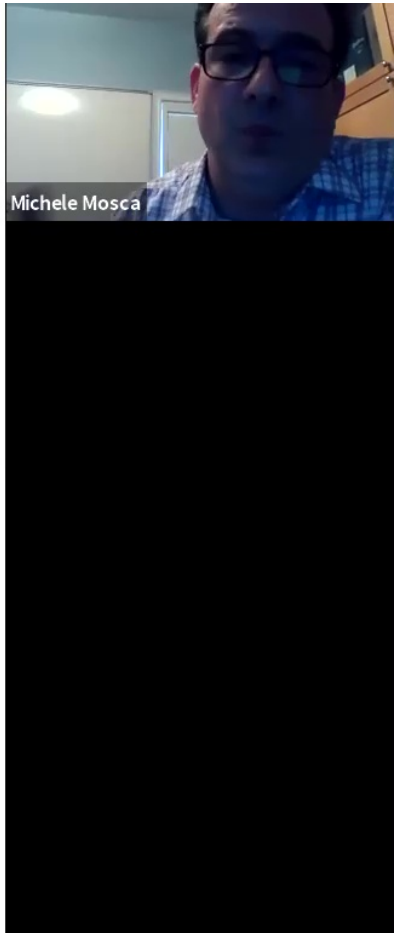
by Jason Kirby Sep 24, 2014



Quantum Internet – the Long Term Vision

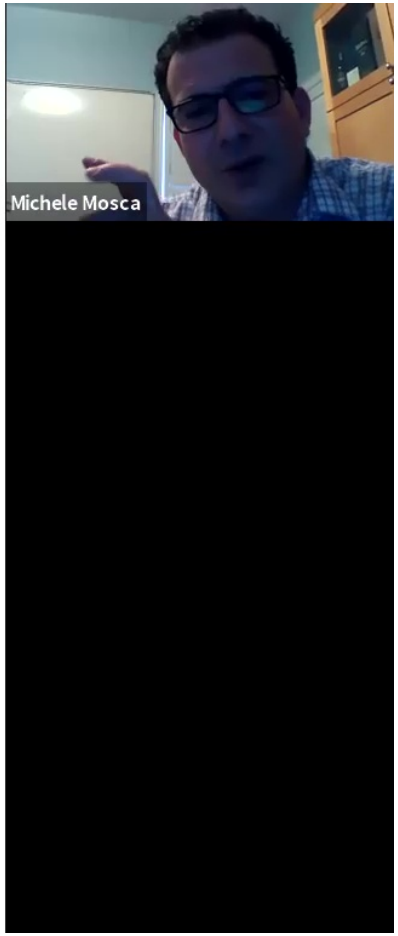


(Thanks to Thomas Jennewein)



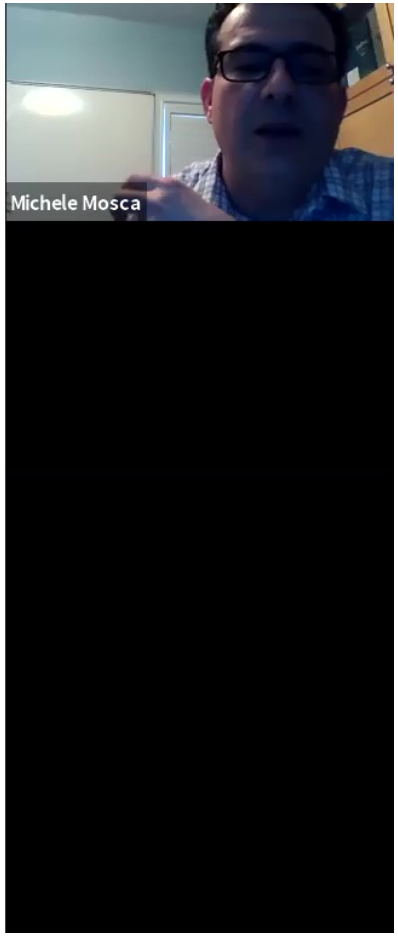
A historical fluke/opportunity

- Our current crypto infrastructure is not nearly as good as it could be.
- In practice it is nearly impossible to replace something "good enough" with something better.

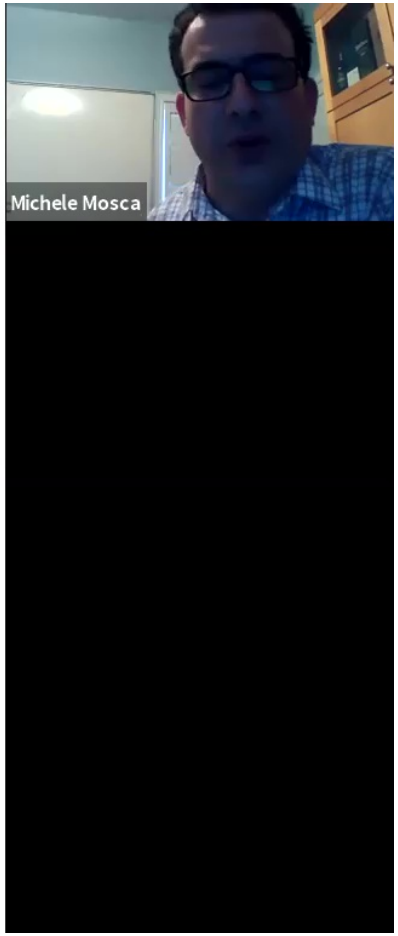


A historical fluke/opportunity

- Our current crypto infrastructure is not nearly as good as it could be.
- In practice it is nearly impossible to replace something "good enough" with something better.
- Given that we have no choice but to replace fundamental cryptography tools with something quantum-safe, the **"toolbox" must be opened.**



Other comments: hybrid hybrid hybrid ….



Hybrid QKD key agreement: combine QKD key with classical public-key derived key, so breaking derived key requires breaking *both* QKD implementation and public-key derived key.

It must be done carefully, but done right it means adding QKD only *increases* your security.

(e.g.

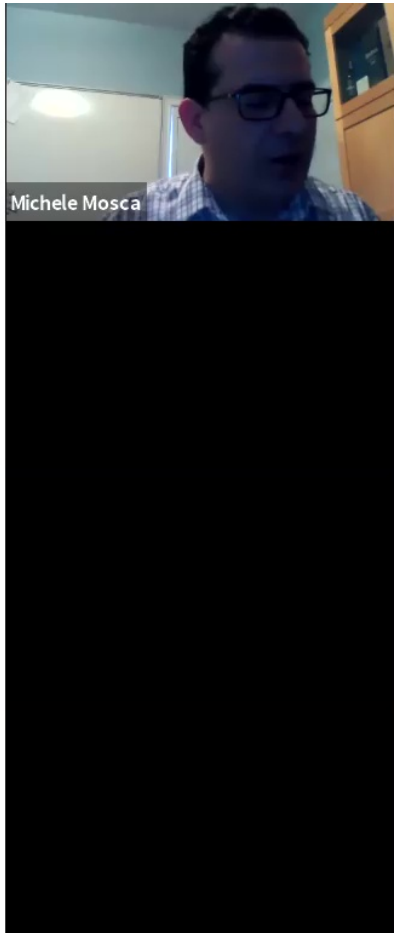
maybe QKD isn't resilient to certain parameters being leaked

maybe QKD equipment or software is open to some sort of side-channel or other compromise that the post-quantum implementation isn't

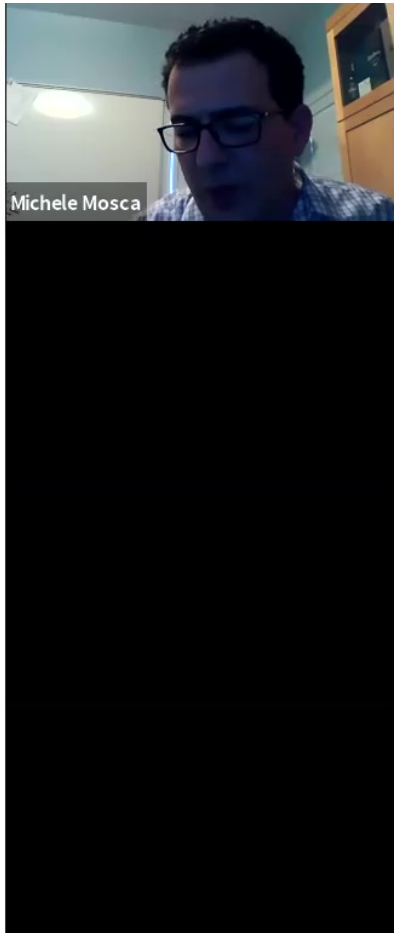
certification/validation issues (like FIPS 140-2))

How easy is it to evolve from one cryptographic algorithm to a quantum-secure one?

Are the standards and practices ready?



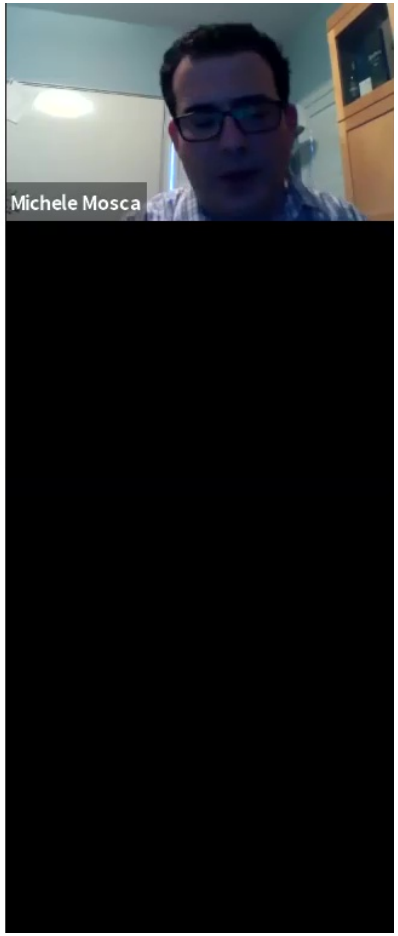
https://www.etsi.org/events/1607-etsi-iqc-quantum-safe-cryptography-workshop-2019



So what do we do about it now?

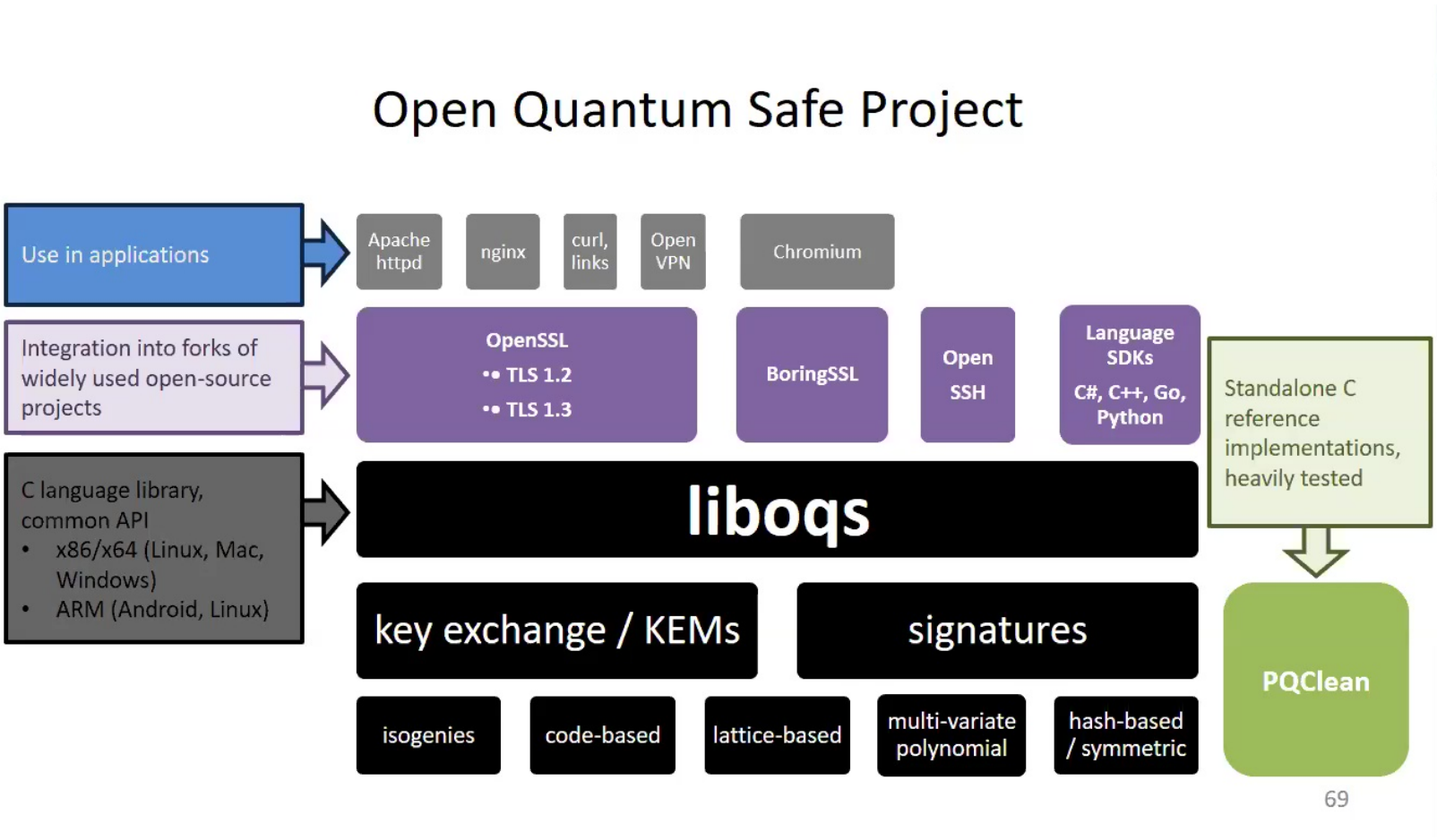
“Execution is 90% planning and 10% doing”

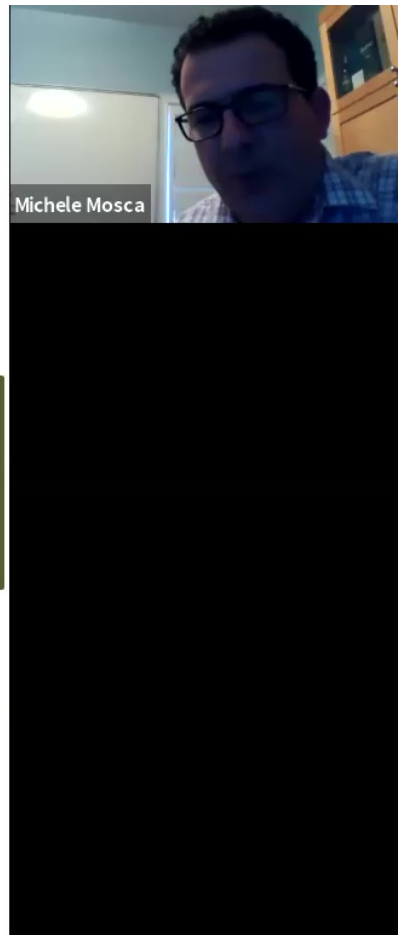
We don’t get to call a “time-out” if we’re not ready!



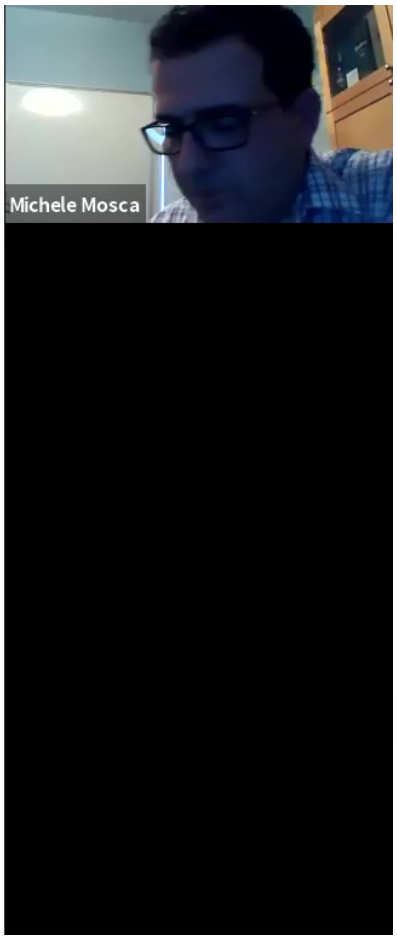
https://openquantumsafe.org/ • https://github.com/open-quantum-safe/

68


Open Quantum Safe Project
Use in applications
Apache httpd
nginx
curl, links
Open VPN
Chromium
Integration into forks of widely used open-source projects
OpenSSL
•• TLS 1.2
•• TLS 1.3
BoringSSL
Open SSH
Language SDKs
C#, C++, Go, Python
C language library, common API
• x86/x64 (Linux, Mac, Windows)
• ARM (Android, Linux)
liboqs
Standalone C reference implementations, heavily tested
key exchange / KEMs
signatures
PQClean
isogenies
code-based
lattice-based
multi-variate polynomial
hash-based / symmetric
69

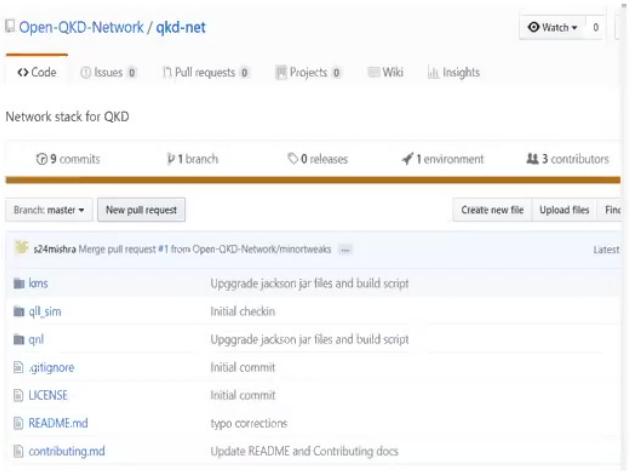

Michele Mosca

Open QKD Net : The Open Source Project



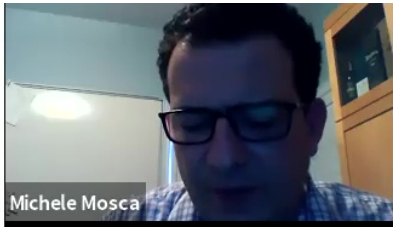
KMS/QNL/QLL-Sim Software

- Hosted at Github.com, managed by IQC team
- Source code license: MIT License
- QKD technology teams can use the system to issue keys to users with little effort
- Program language: Java
- Sample applications written in C



NRC·CNRC

Historic opportunity



Thank you!

Comments, questions and feedback are very welcome.

Michele Mosca
Associate Faculty, Perimeter Institute for Theoretical Physics
mmosca@perimeterinstitute.ca
Professor, Faculty of Mathematics
Co-Founder, Institute for Quantum Computing,
University of Waterloo www.iqc.ca/~mmosca
mmosca@uwaterloo.ca

CEO, evolutionQ Inc. @evolutionQinc
michele.mosca@evolutionq.com

Co-founder, softwareQ Inc. softwareq.ca