VLAD GHEORGHIU[1,2,3]

NON-ASYMPTOTIC QUANTUM RESOURCE ESTIMATION

QuAC 2019, 19 May 2019, Darmstadt, Germany

[1]Institute for Quantum Computing, [2]softwareQ Inc., [3]evolutionQ Inc.

vlad.gheorghiu@uwaterloo.ca vlad@softwareq.ca

QUANTUM COMPUTING - BOTH A BLESSING AND A CURSE

Powerful new quantum technologies are emerging, which promise tremendous benefits…

…but also pose serious threats to our communications, control and information security.

CURRENT PUBLIC-KEY (ASYMMETRIC CRYPTOGRAPHY) - BROKEN

- Key establishment scheme over a noisy channel. Result: pair of "public/secret key". Like "shouting in a room full of people and establishing a secret".
- Security based on hardness of factoring large numbers or solving the discrete log problem in large finite groups
- Completely broken by **Shor's algorithm** - instance of Abelian Hidden Subgroup Problem (HSP), f(x) = f(y) iff xH = yH (i.e. f is constant on cosets)
  - G = ? H = ? f(x) = a^x mod N f(x) = f(y) iff x = y + H
- No quick "patching" available
- Post-quantum schemes (Lattices/Multivariate/Code-based/Isogenies). Main disadvantages: key sizes/efficiency/less scientific scrutiny.

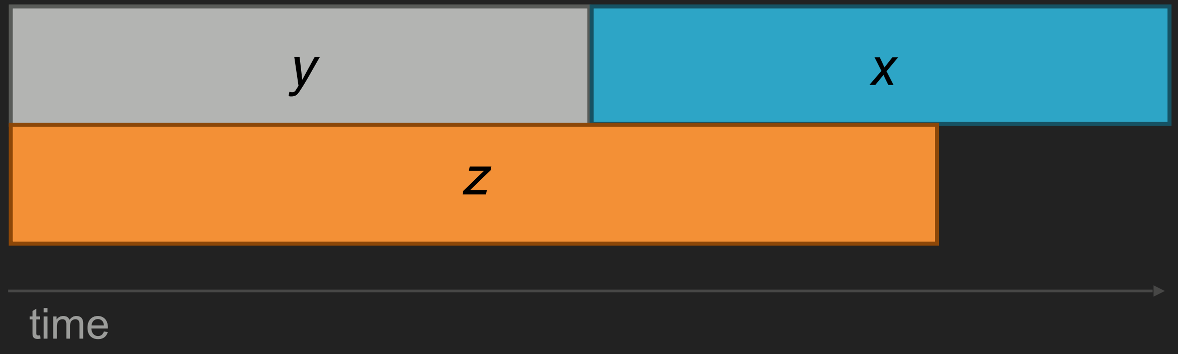
SYMMETRIC CRYPTOGRAPHY AND HASH FUNCTIONS – WEAKENED

- Hash functions: map arbitrary long inputs to fixed size outputs. Examples (of cryptographic hash functions): SHA-256, SHA3-256, SHA3-512, MD5 etc.
- Used extensively in digital signatures. Security of digital signatures is based on the hardness of finding collisions of pre-images.
- Cyphers: "scramble" the input according to a (secret) key. Examples: AES, DES, 3-DES. Used in combination with public key cryptography to encode communication over an insecure channel.
- Weakened by quantum computers (NOT BROKEN)

- Best generic attack on such systems is to apply Grover's quantum search algorithm and achieve (only) a quadratic improvement over exhaustive search in a black-box query model
- Does not parallelize well. Searching space of size N and K quantum computers running on parallel -> [N/K]^(1/2) and not [N^(1/2)] / K.
- Conservative defence: compensate for the potential square root loss in security by doubling the size of the security parameter (key size, output length of a hash function etc.)
- Suitable response for the cryptographer who wants to make worst case assumptions, however many of us want to know exactly the cost of such an attack

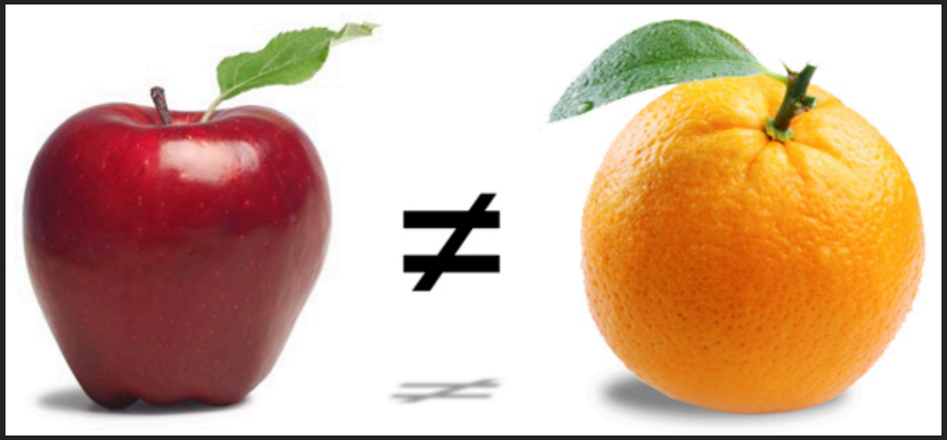
DO WE NEED TO WORRY NOW?

- Depends on:
  - X = Security shelf life
  - Y = Migration time
  - Z = Collapse time
- "Theorem" (Michele Mosca, eprint.iacr.org/2015/1075)
  - If X + Y > Z, then worry!

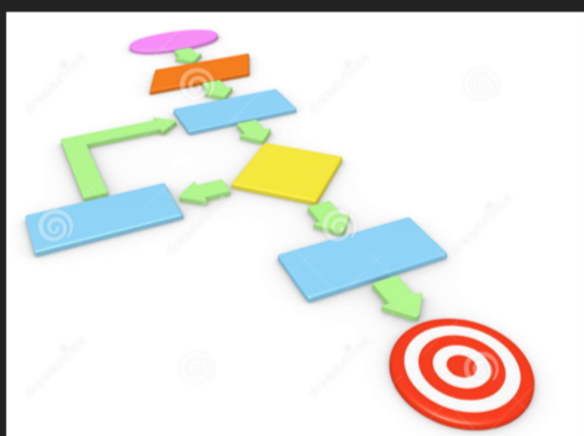


MAIN ISSUES/QUESTIONS IN NON-ASYMPTOTIC QRE

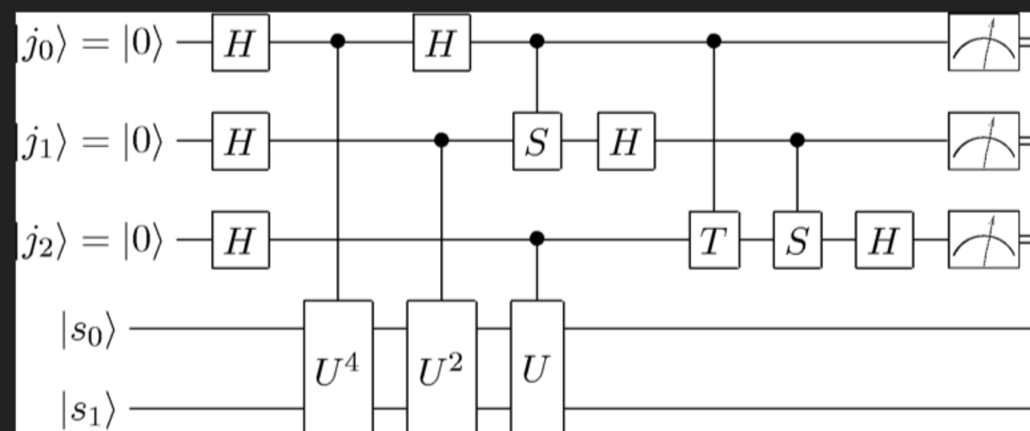
- Given a specific quantum algorithm, how "large" should a quantum computer be? Or, what are the constants in Os(…) and Omegas(…)?
- How "fast" is the computation being performed?
- How do we properly quantify the time/space volume?
- What is the basic "unit" of computation (i.e. the quantum version of FLOPs)?
- How do we compare (fairly) a quantum computer with a classical one?



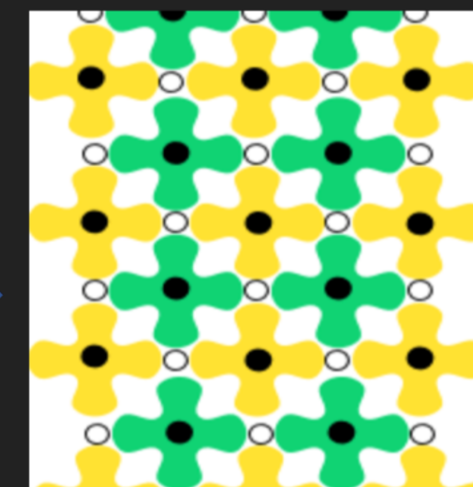
RUNNING A QUANTUM PROGRAM



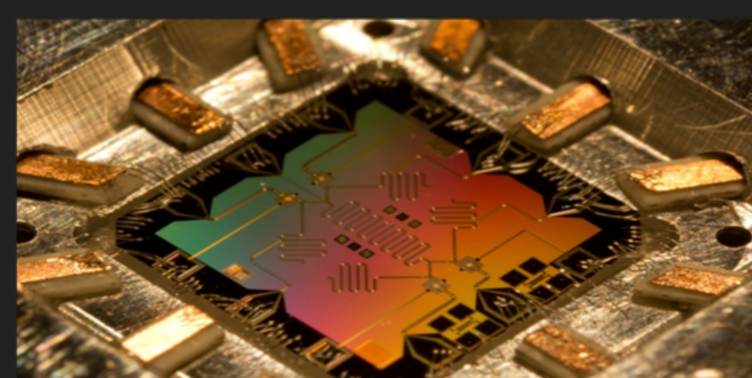
Algorithms (abstract layer)



Quantum circuits (logical layer)



Error correcting layer

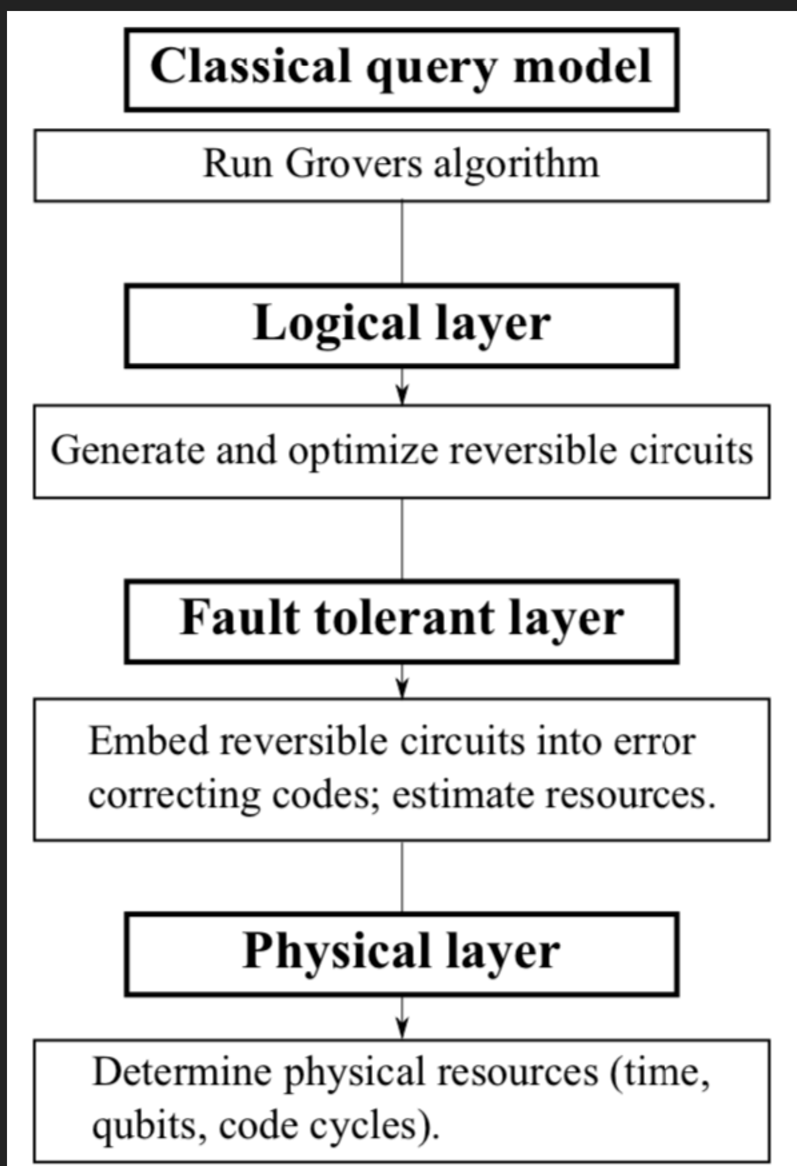


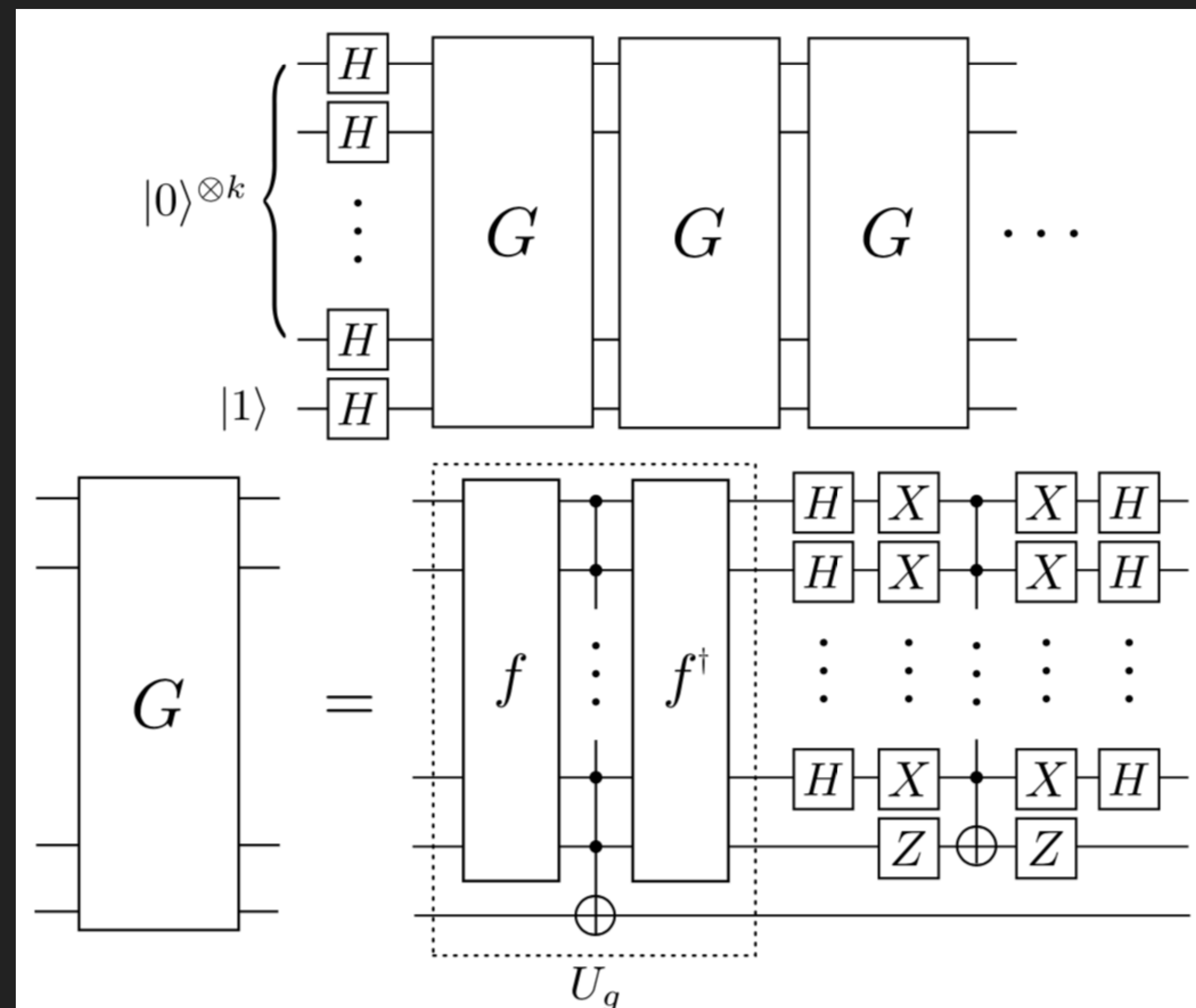
Hardware (physical layer)

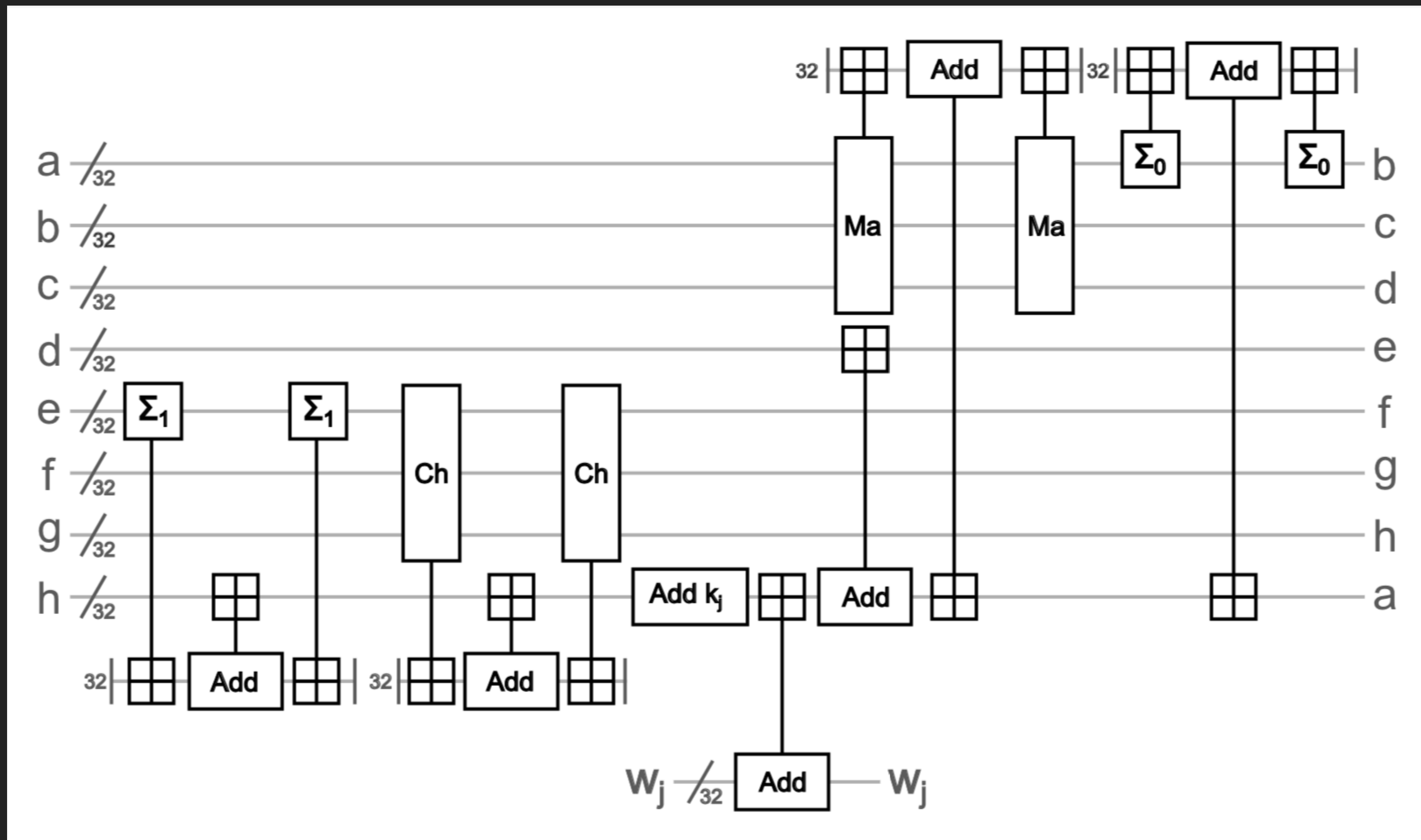
OVERHEAD

- Logical level: reversibility constraints
  - Compute - copy - un-compute (Bennett's trick)
  - Replace x -> f(x) by |x, y> -> |x, y + f(x)>, run on |x, 0>
    - |x>|0> -> |f(x)>|junk(x)>, copy and un-compute
    - |x>|0>|y> -> |f(x)>|junk(x)>|y> -> |f(x)>|junk(x)>|y+f(x)> -> |x>|0>|y+f(x)>
  - K {NOT, AND} -> 2K + n over Toffoli
- Physical layer: fault tolerant model (surface codes)
  - Encode 1 logical qubit into n physical qubits (~1000 overhead)
- Classical control (should not be ignored)
  - Syndrome detection, classical processing

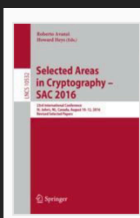
OPENING UP BLACK BOXES







SHA256 oracle



International Conference on Selected Areas in Cryptography

SAC 2016: Selected Areas in Cryptography – SAC 2016 pp 317-337 | Cite as

Estimating the Cost of Generic Quantum Pre-image Attacks on SHA-2 and SHA-3

Authors | Authors and affiliations

Matthew Amy, Olivia Di Matteo, Vlad Gheorghiu, Michele Mosca, Alex Parent, John Schanck

THE CLIFFORD GROUP

- The Pauli group is the unitary group generated by the Pauli operators X, Y, Z
- The Clifford group is the unitary group that maps Pauli operators to Pauli operators under conjugation, i.e.

$$C_n = \{U : UPU^\dagger = P\},$$

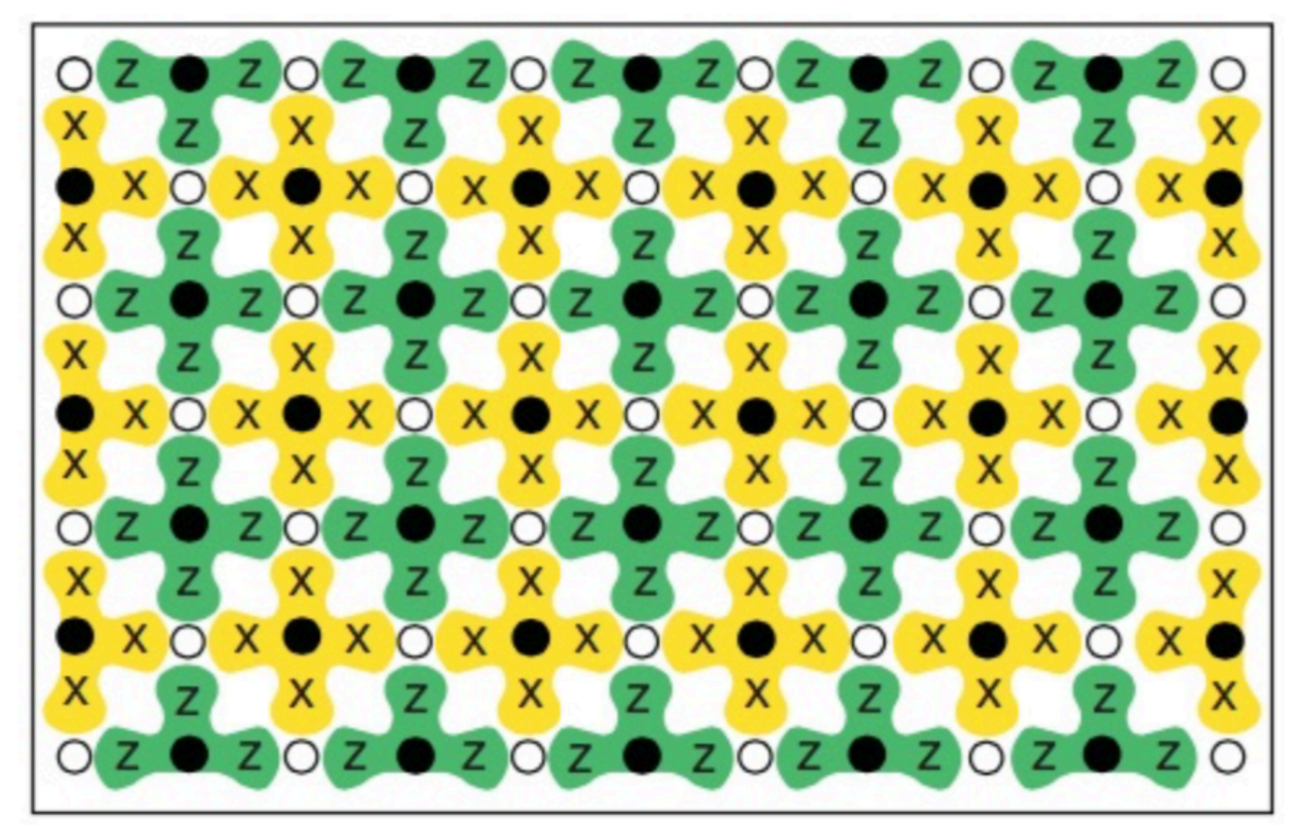
- Examples: X, Y, Z, H, CNOT
- The Clifford group on n qubits is generated by <H, S, CNOT>

UNIVERSAL SET OF GATES

- <C_n, T> is universal
- Every unitary U can be approximated as close as we want by a suitable product of gates from the Clifford + T set
- The Clifford group itself is not universal. In fact, if you restrict the computation only to Clifford gates (and Pauli measurements) you can simulate it efficiently on a classical computer (Gottesman-Knill theorem).
- The T gate is the problem-child of quantum computation. Hard to implement fault-tolerantly, requires additional resources.

SURFACE CODES

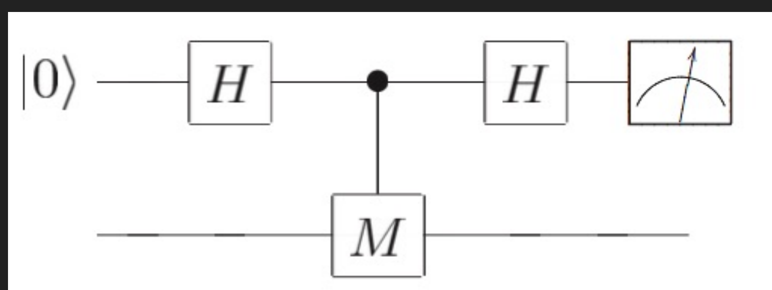
- The surface code consist of a lattice of 2 types of qubits: data qubits and measurement qubits. It is a particular instance of a topological code (A. Kitaev), namely the un-folded toric code.

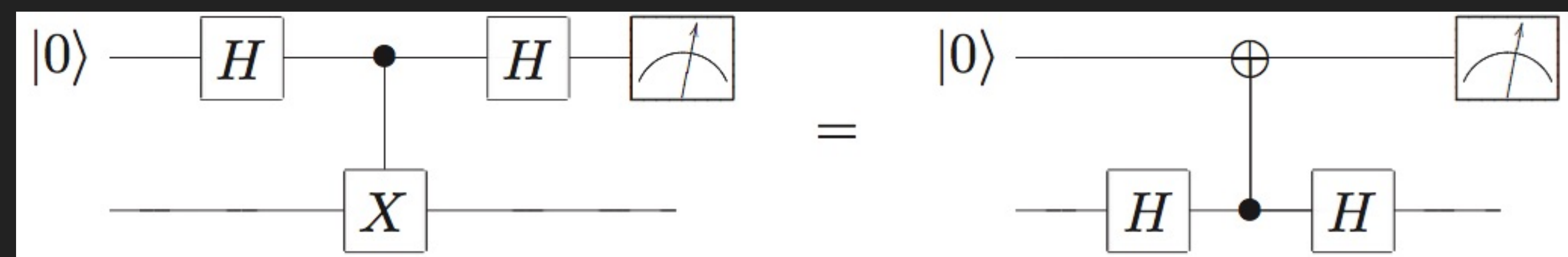


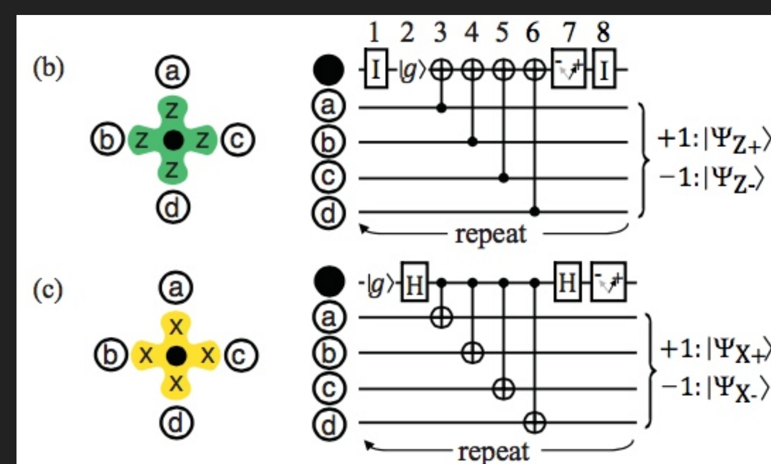
The surface code. Empty circles are data qubits (39), solid circles are measurement qubits (38), of two types: measure-X (yellow) and measure-Z (green). [PRA 86, 032324 (2012)].

SURFACE CODE CYCLES

- The X-type (yellow) and Z-type (green) stabilizers are measured at the same time







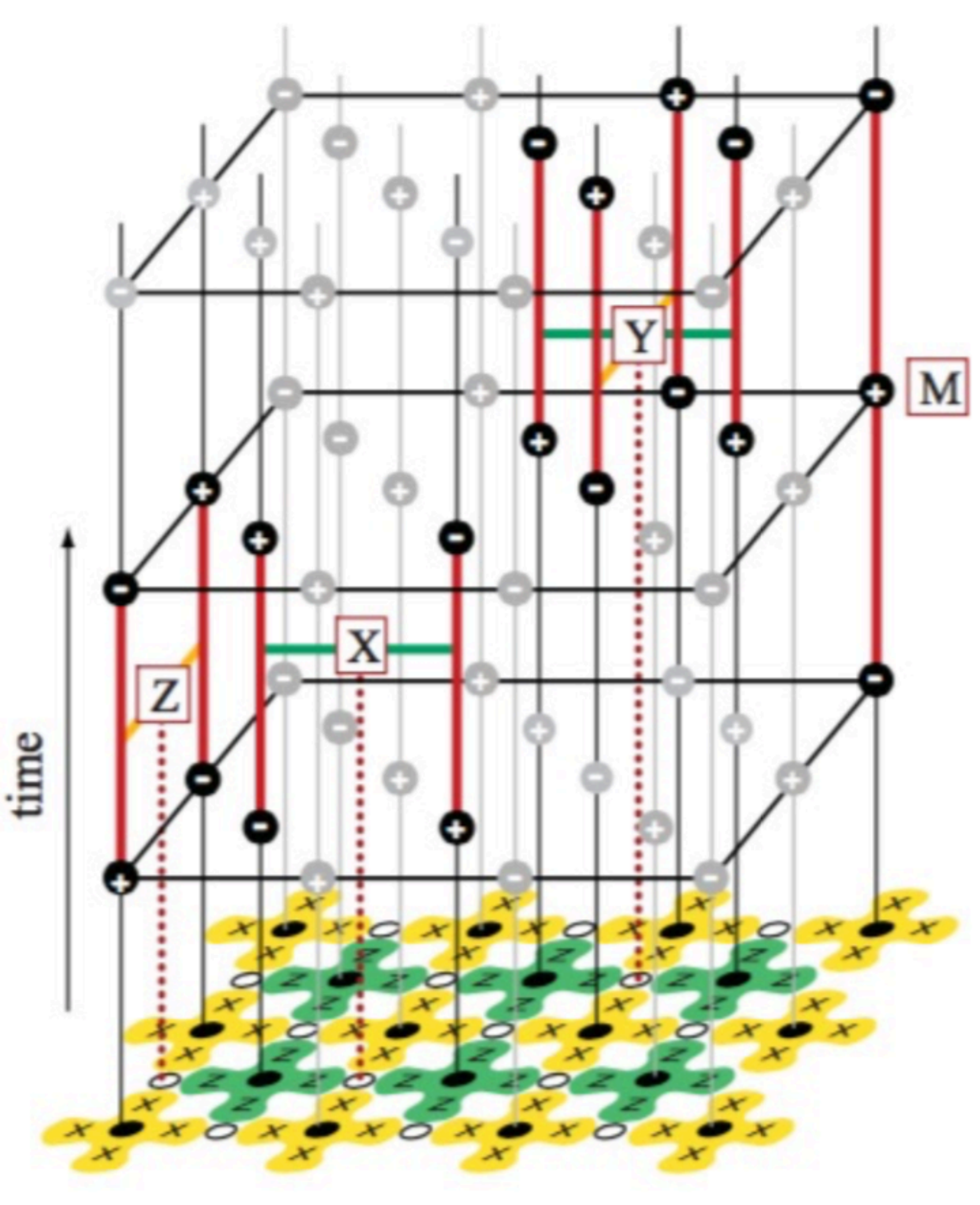
[PRA 86, 032324 (2012)]

- The measurement result is recorded (i.e. a string of 38 plus one and minus one).
- This procedure is called a surface code cycle. The cycle is repeated indefinitely (until the end of the computation).

DETECTING ERRORS

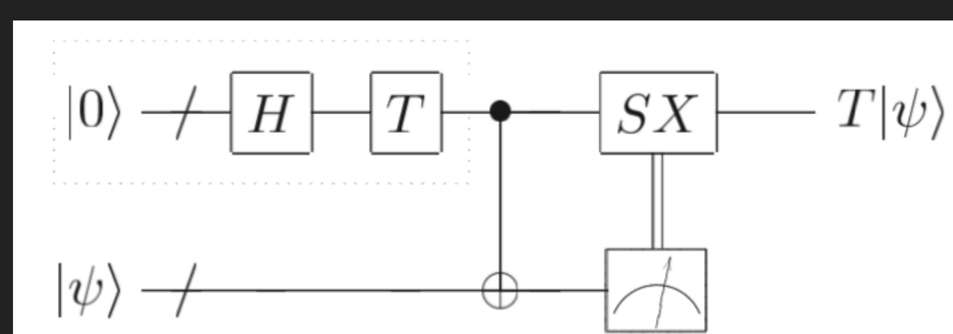
- What happens if there are no errors? The measurement results have to stay the same!
- What happens if there is an error on one of the data qubits or on the measurement qubit itself? The corresponding stabilizer measurement will differ from the previous cycle.
- The whole idea behind topological error correction is that the topology of the system "helps" in detecting and correcting the errors, provided that the error rate is reasonable (i.e., below the threshold)
- The error detection is a purely classical protocol: Edmonds' minimum-weight perfect-matching algorithm (1965).

Error detection, [PRA 86, 032324 (2012)]



A (Q)BIT OF MAGIC

- Clifford gates can be implemented “directly” in the surface code via measurement patterns (turning stabilizers on/off, braiding, lattice surgery)
- In contrast, the T gate (T := |0⟩⟨0| + exp(pi*i/4)|1⟩⟨1|) can not be implemented in the surface code
- We need it to achieve universal quantum computation.
  We use a “trick”: we produce it with the help of a resource, called… a magic state.
- Magic state $$|A_L\rangle := \frac{|0\rangle + \mathrm{e}^{\pi \mathrm{i}/4}|1\rangle}{\sqrt{2}}$$
- “Code injection”



...AND DISTILLERIES (NOT OF ALCOHOLIC KIND)

- In general, it is hard to come up with a perfect magic state (as hard as implementing the T gate itself).
- However, starting with a "bad" magic state, we can purify it via magic state distillation using concatenated codes
- The error rate thus decreases exponentially! In general, magic states are produced offline, in so called magic state factories, and are injected in the circuit when needed.
- ~90% of a circuit physical footprint (no. of qubits) consists of distilleries. Reducing the T-count is of paramount importance.

Magic State Distillation: Not as Costly as You Think

Daniel Litinski

May 17 2019 quant-ph arXiv:1905.06903v1

Despite significant overhead reductions since its first proposal, magic state distillation is often considered to be a very costly procedure that dominates the resource cost of fault-tolerant quantum computers. The goal of this work is to demonstrate that this is not true. By writing distillation circuits in a form that separates qubits that are capable of error detection from those that are not, most logical qubits used for distillation can be encoded at a very low code distance. This significantly reduces the space-time cost of distillation, as well as the number of qubits. In extreme cases, it can cost less to distill a magic state than to perform a logical Clifford gate on full-distance logical qubits.

COST METRIC FOR FAULT-TOLERANT QUANTUM COMPUTATION

- *Without significant future effort, the classical processing will almost certainly limit the speed of any quantum computer, particularly one with intrinsically fast quantum gates.* [A. Fowler et al, "Towards practical classical processing for the surface code: Timing analysis", Phys. Rev. A 86, 042313 (2012)]
- Assumptions:
  - The resources required for any large quantum computation are well approximated by the resources required for that computation on a surface code based quantum computer
  - The classical error correction routine for the surface code on an $L \times L$ grid of logical qubits requires an $L \times L$ mesh of classical processors (ASICs (application-specific integrated circuit))
  - Each ASIC performs a constant number of operations per surface code cycle
  - The temporal cost of one surface code cycle is equal to the temporal cost of one oracle function invocation

COST METRIC FOR FAULT-TOLERANT QUANTUM COMPUTATION

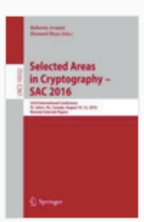
- The cost of a quantum computation involving L logical qubits for a duration of σ surface code cycles is equal to the cost of classically evaluating an oracle function $L \cdot \sigma$ times.
- Equivalently we say that one logical qubit cycle is equivalent to one oracle function invocation.
- p1_out = 1/T_c for distilleries -> series of code distances
- p2_out = 1/C_c for the Grover circuit -> circuit code distance

SHA-256, SHA3-256

		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	$2^{166.4}$	$2^{166.5}$

	$T/T^\dagger$	$P/P^\dagger$	Z	H	CNOT	T-Depth	Depth
Round	5278	0	0	1508	6800	2262	8262
Round (Opt.)	3020	931	96	1192	63501	1100	12980
Stretch	1329	0	0	372	2064	558	2331
Stretch (Opt.)	744	279	0	372	3021	372	2907
SHA-256	401584	0	0	114368	534272	171552	528768
SHA-256 (Opt.)	228992	72976	6144	94144	4209072	70400	830720

Table 1. T-par optimization results for a single round of SHA-256, one iteration of the stretch algorithm and full SHA-256. Note that 64 iterations of the round function and 48 iterations of the stretch function are needed. The stretch function does not contribute to overall depth since it can be performed in parallel with the rounds function. No X gates are used so an X column is not included. The circuit uses 2402 total logical qubits.



International Conference on Selected Areas in Cryptography
SAC 2016: Selected Areas in Cryptography – SAC 2016 pp 317-337 | Cite as

Estimating the Cost of Generic Quantum Pre-image Attacks on SHA-2 and SHA-3

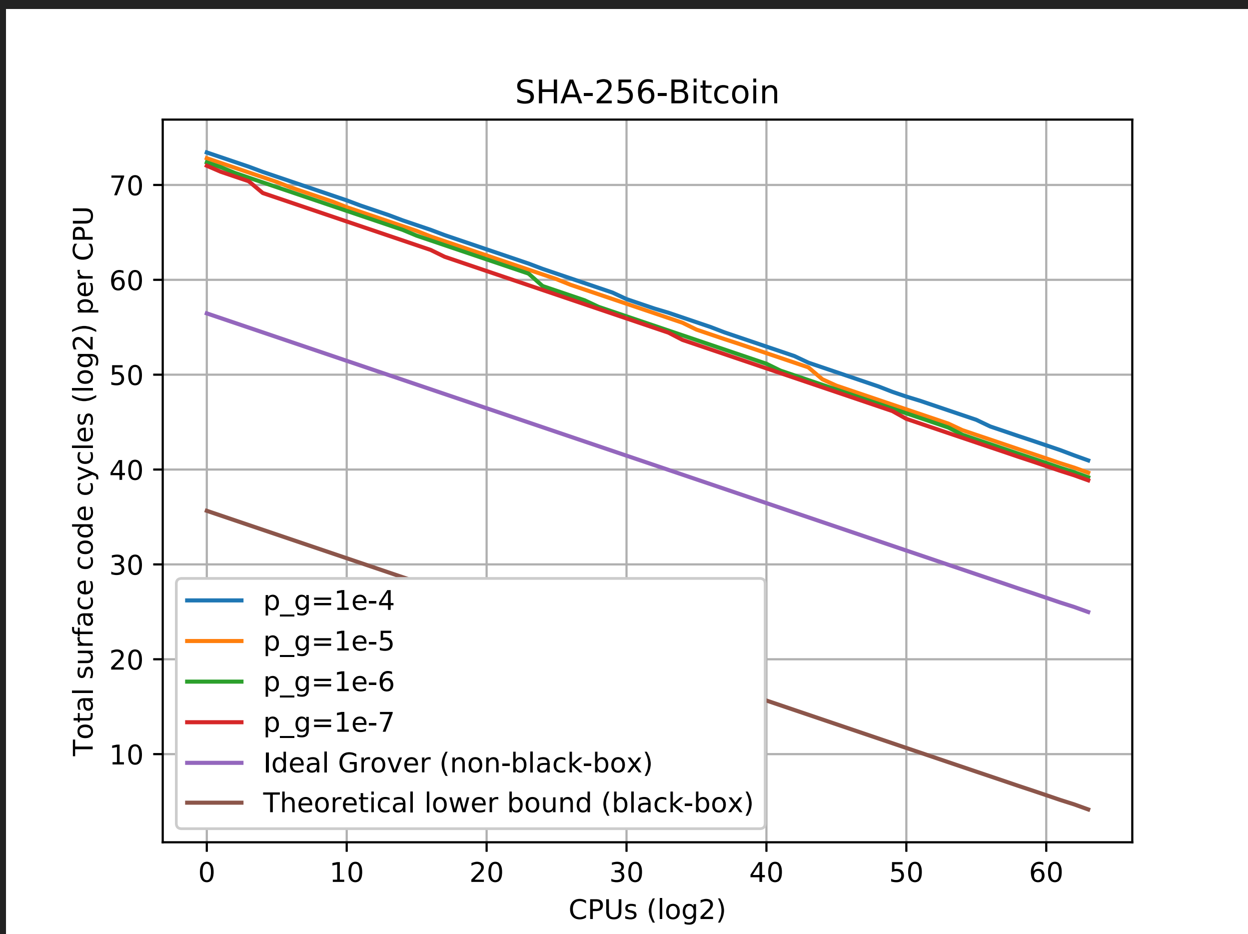
Authors Authors and affiliations

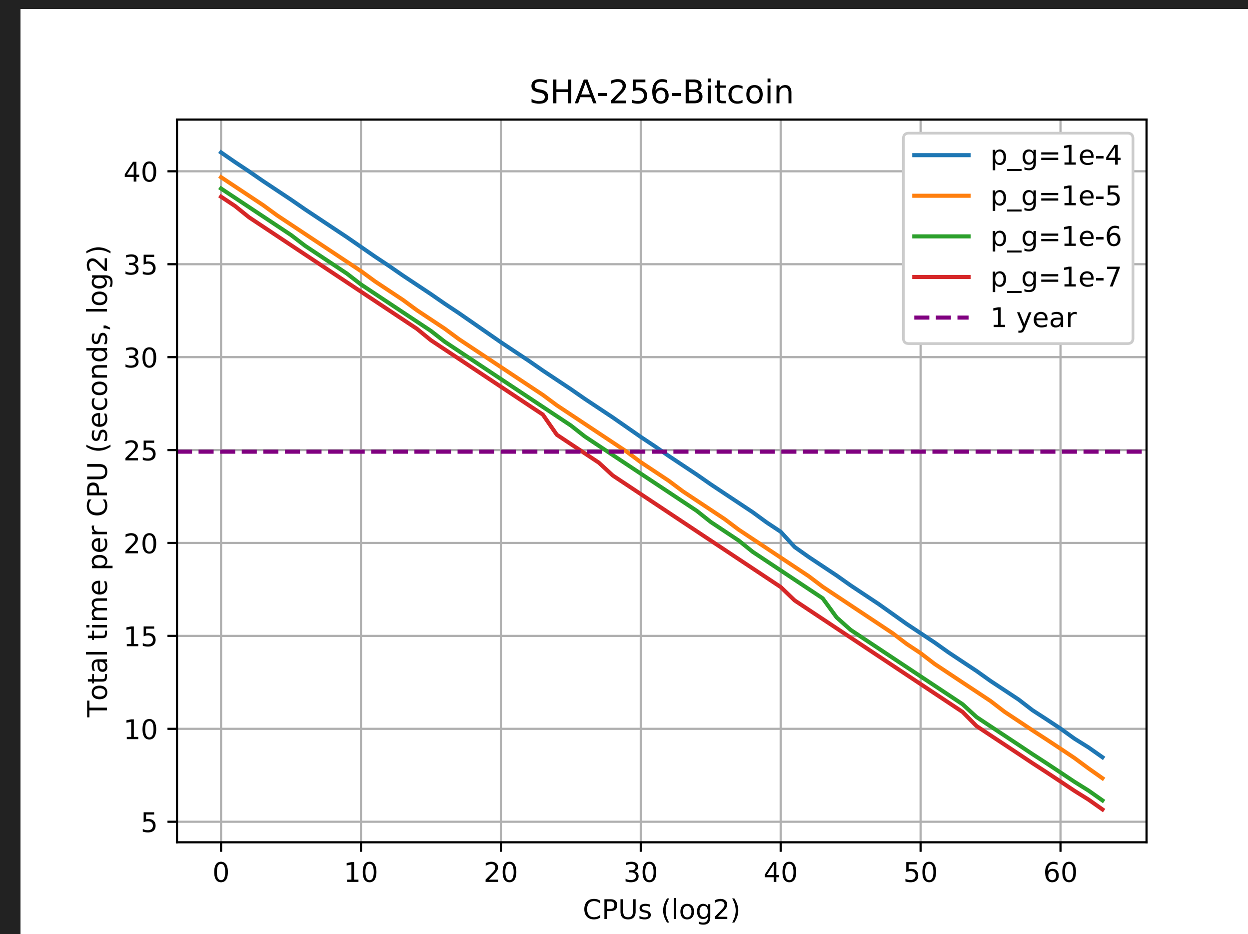
Matthew Amy, Olivia Di Matteo, Vlad Gheorghiu, Michele Mosca, Alex Parent, John Schanck

Conference paper
First Online: 20 October 2017

Part of the Lecture Notes in Computer Science book series (LNCS, volume 10532)

SHA-256 BITCOIN





arXiv.org > quant-ph > arXiv:1902.02332

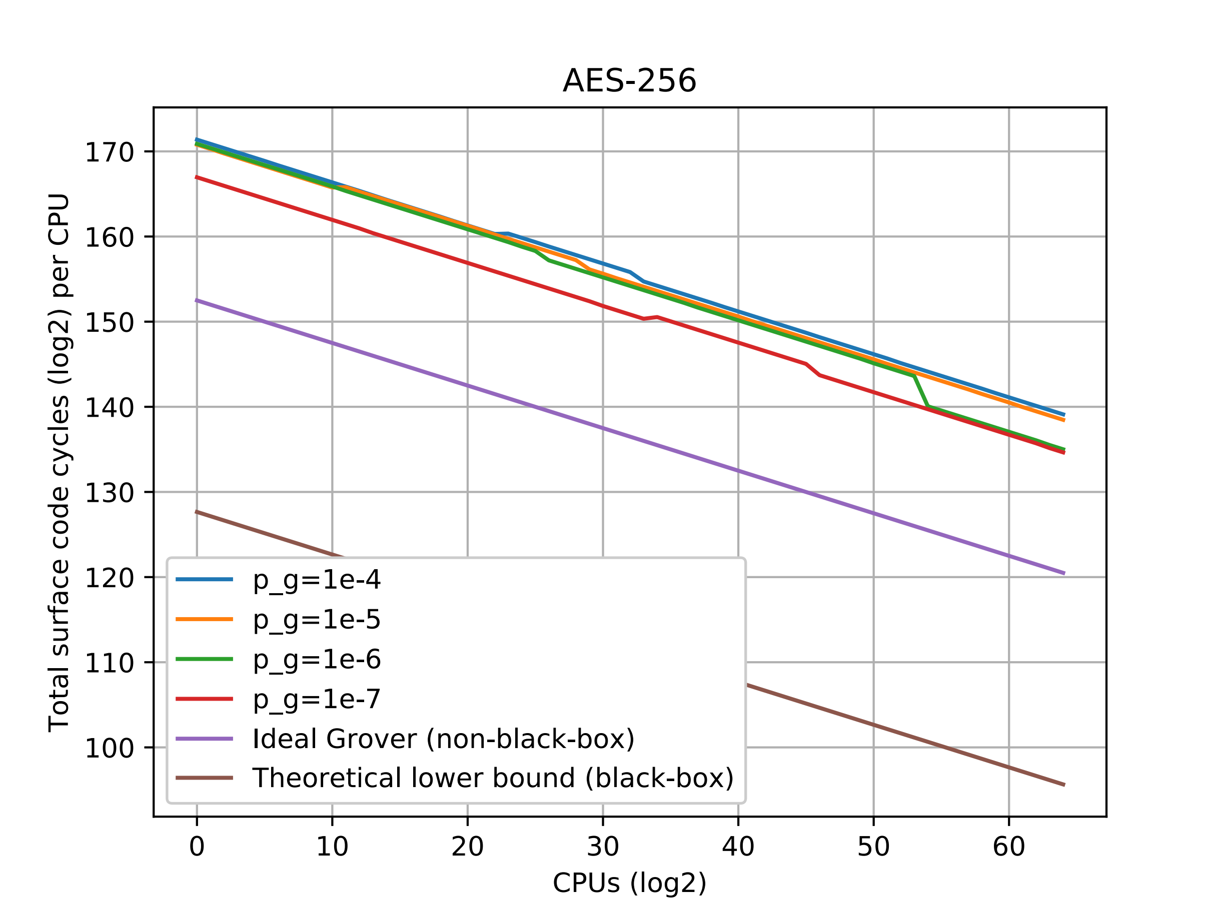
Quantum Physics

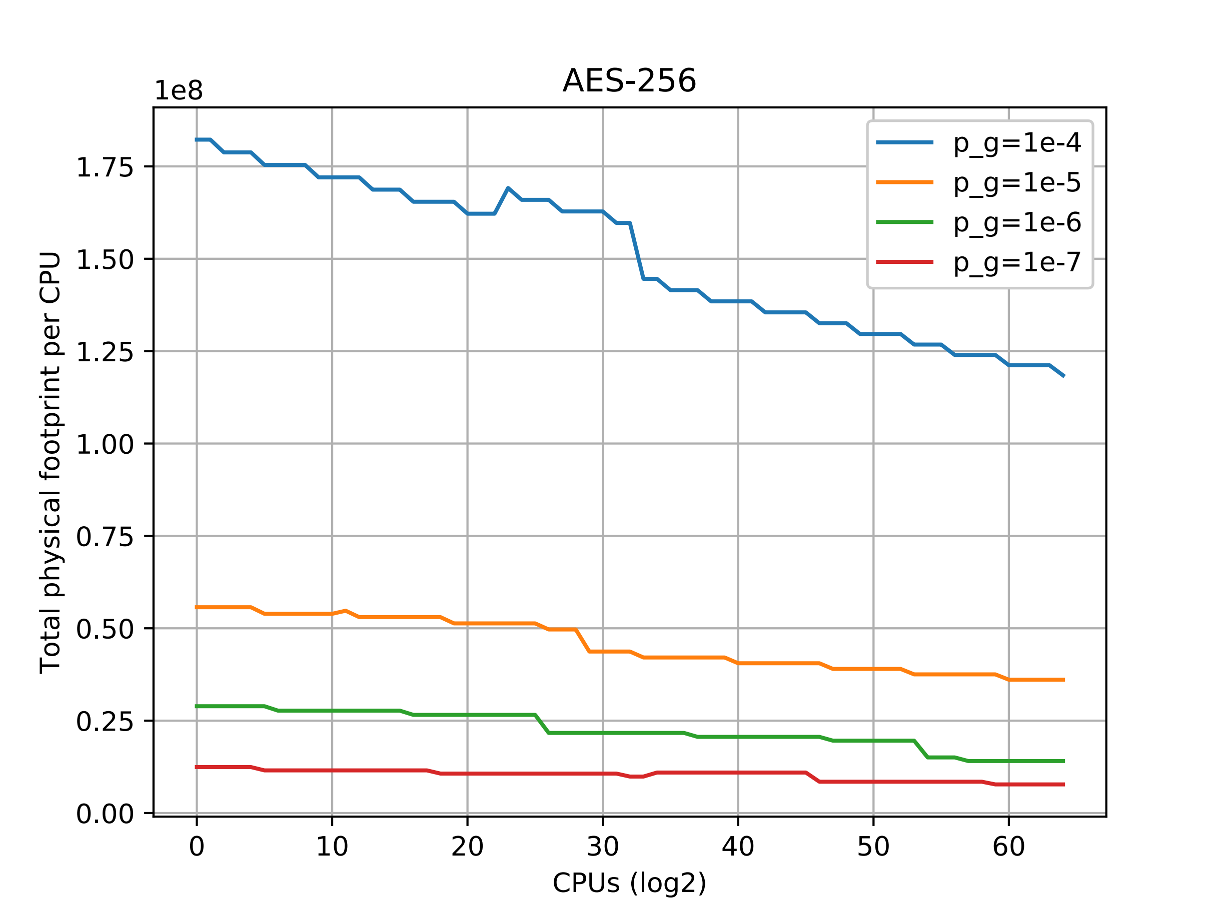
Benchmarking the quantum cryptanalysis of symmetric, public-key and hash-based cryptographic schemes

Vlad Gheorghiu, Michele Mosca

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

AES-256






arXiv.org > quant-ph > arXiv:1902.02332

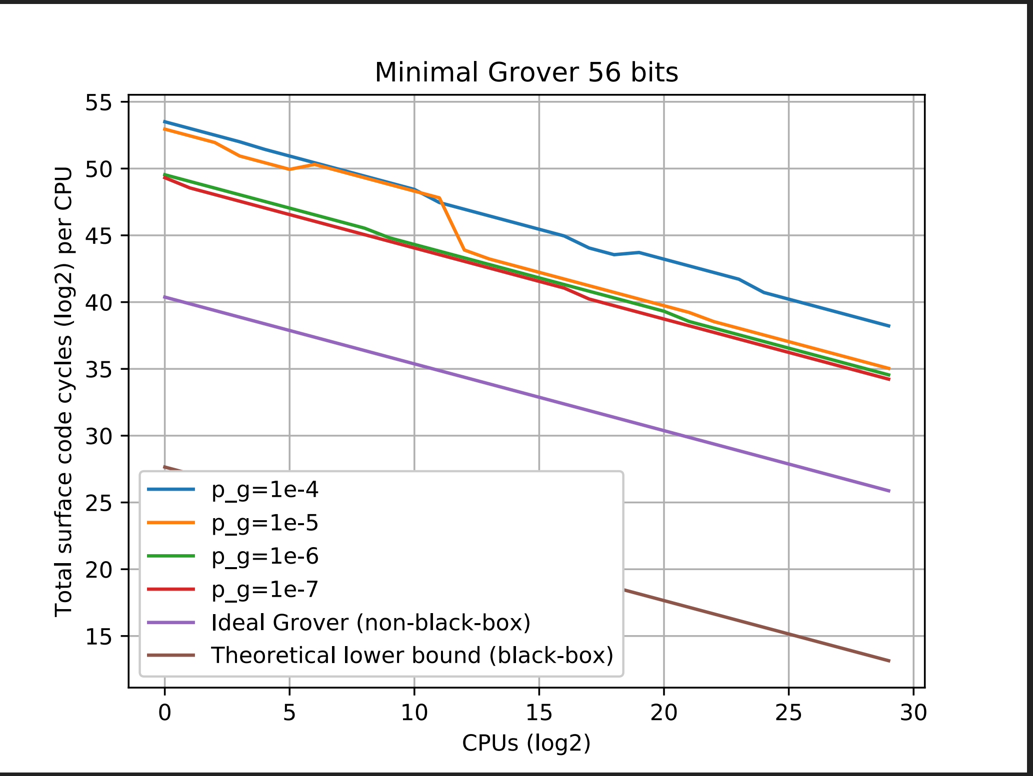
Quantum Physics

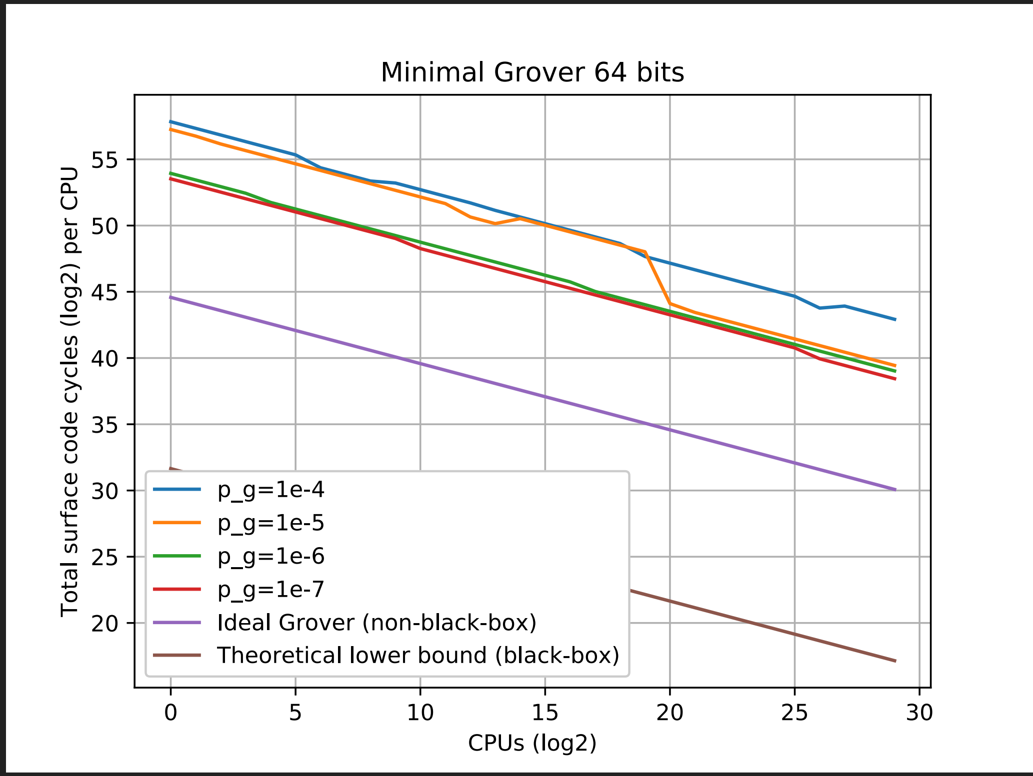
Benchmarking the quantum cryptanalysis of symmetric, public-key and hash-based cryptographic schemes

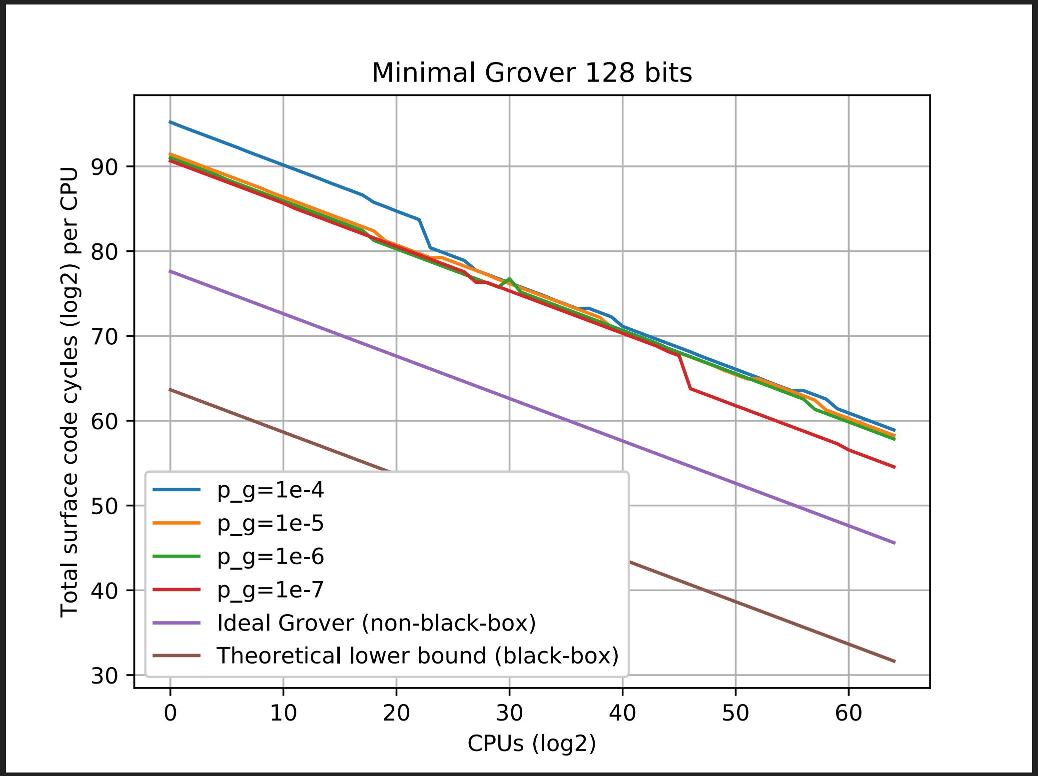
Vlad Gheorghiu, Michele Mosca

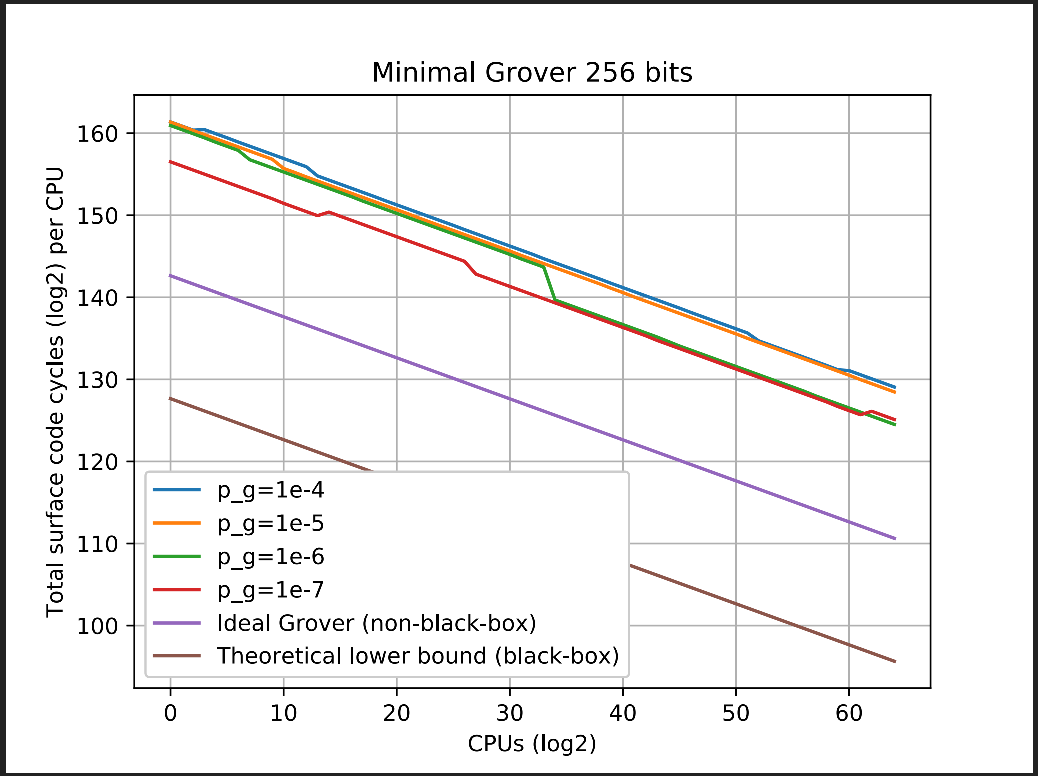
(Submitted on 6 Feb 2019 (v1), last revised 7 Feb 2019 (this version, v2))

INTRINSIC COST OF GROVER









RSA-2048

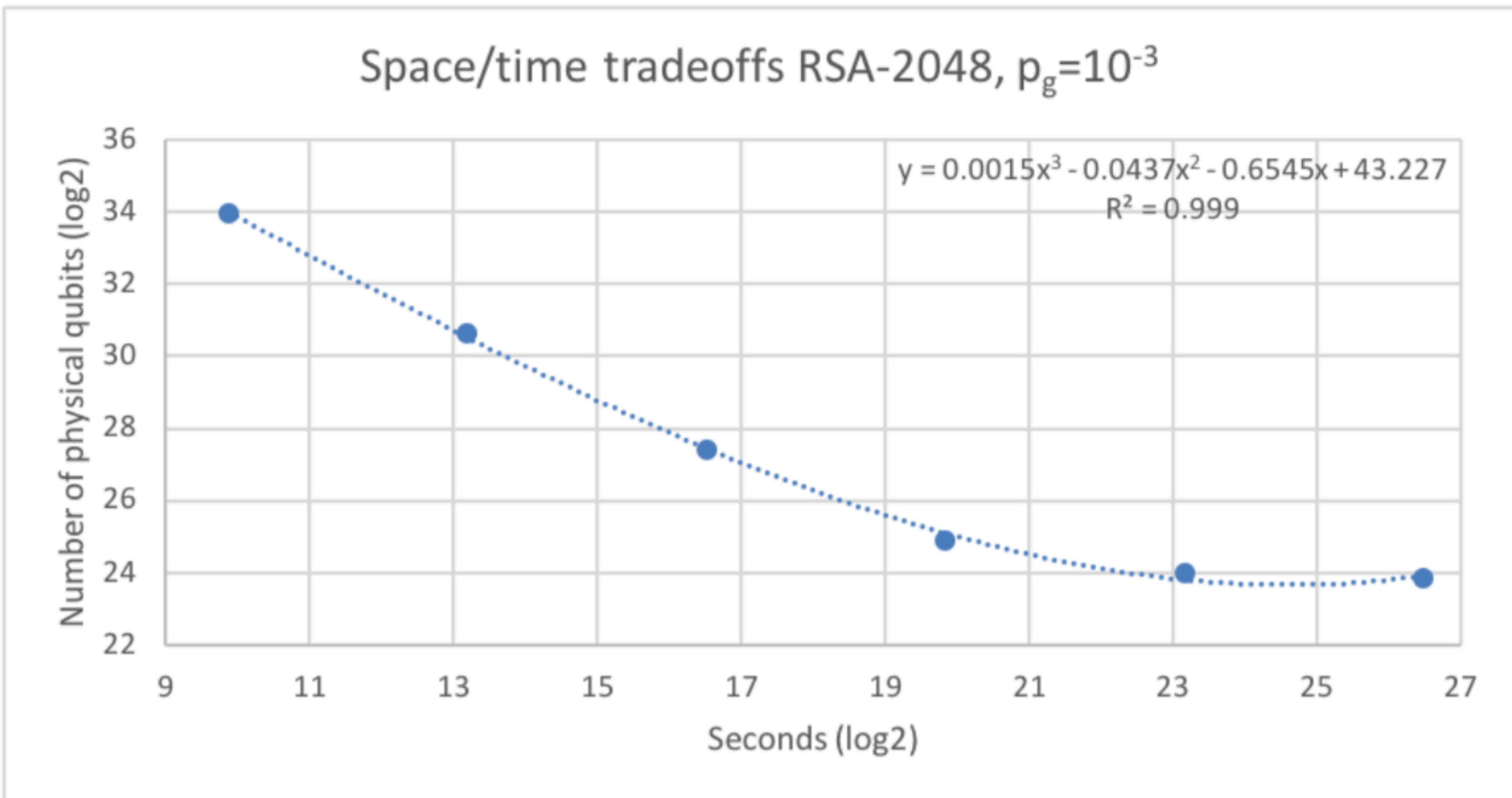


Fig. 4. RSA-2048 space/time tradeoffs with physical error rate per gate $p_g = 10^{-3}$. The scale is logarithmic (base 2). Approximately $y(16.3987) \approx 1.72 \times 10^8$ physical qubits are required to break the scheme in one day (24 hours). The number of T gates in the circuit is 2.41×10^{12}, 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

Search or Article

(Help | Advanced sea

Quantum Physics

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

Vlad Gheorghiu, Michele Mosca

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

ECC NIST P-224

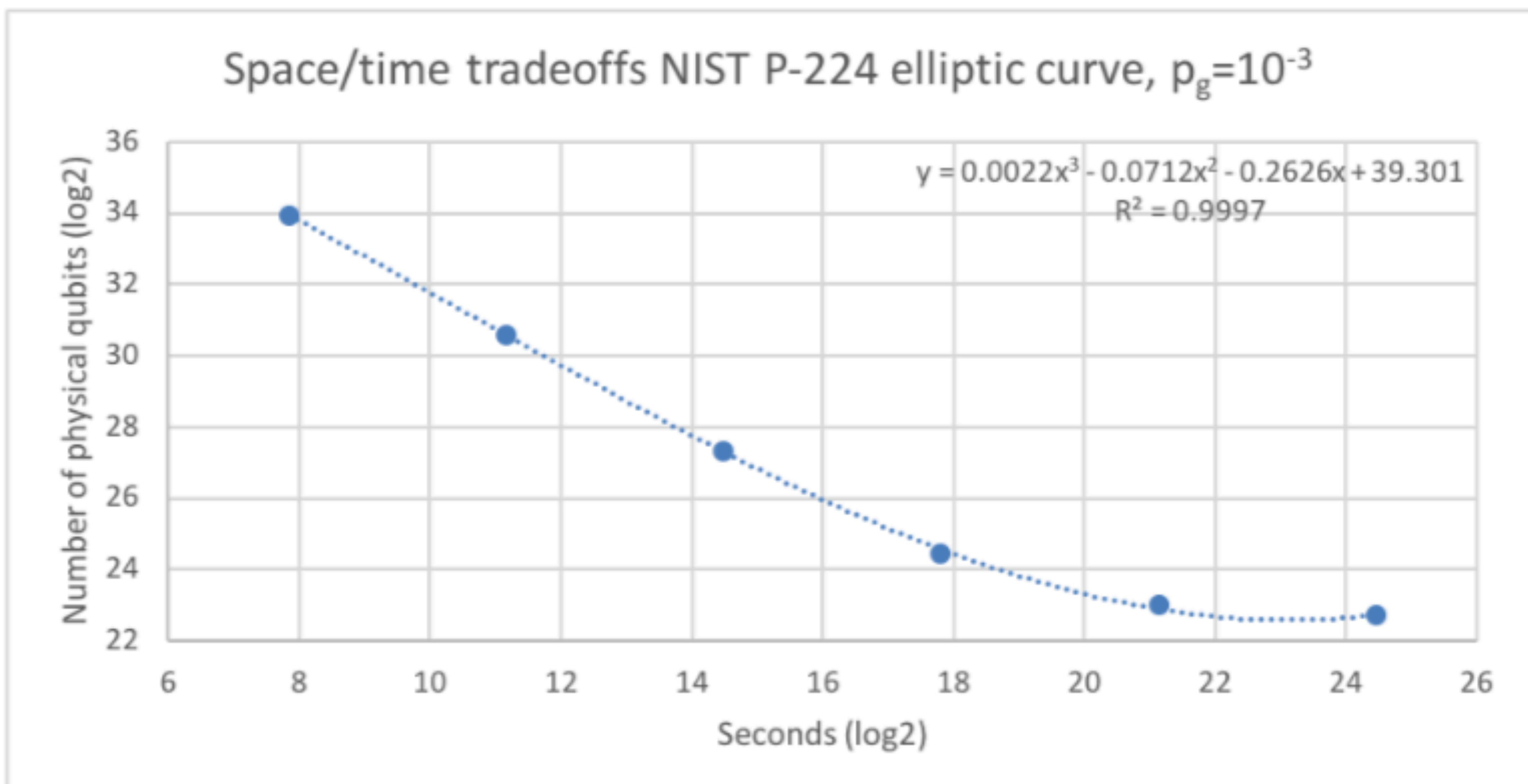


FIG. 59. NIST P-224 elliptic curve space/time tradeoffs with physical error rate per gate $p_g = 10^{-3}$. The scale is logarithmic (base 2). Approximately $y(16.3987) \approx 4.91 \times 10^7$ physical qubits are required to break the scheme in one day (24 hours). The number of T gates in the circuit is 5.90×10^{11}, the corresponding number of logical qubits is 2042, and the total number of surface code cycles is 1.15×10^{14}. The classical security parameter is 112 bits.

arXiv.org > quant-ph > arXiv:1902.02332

Search or Article

(Help | Advanced sea

Quantum Physics

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

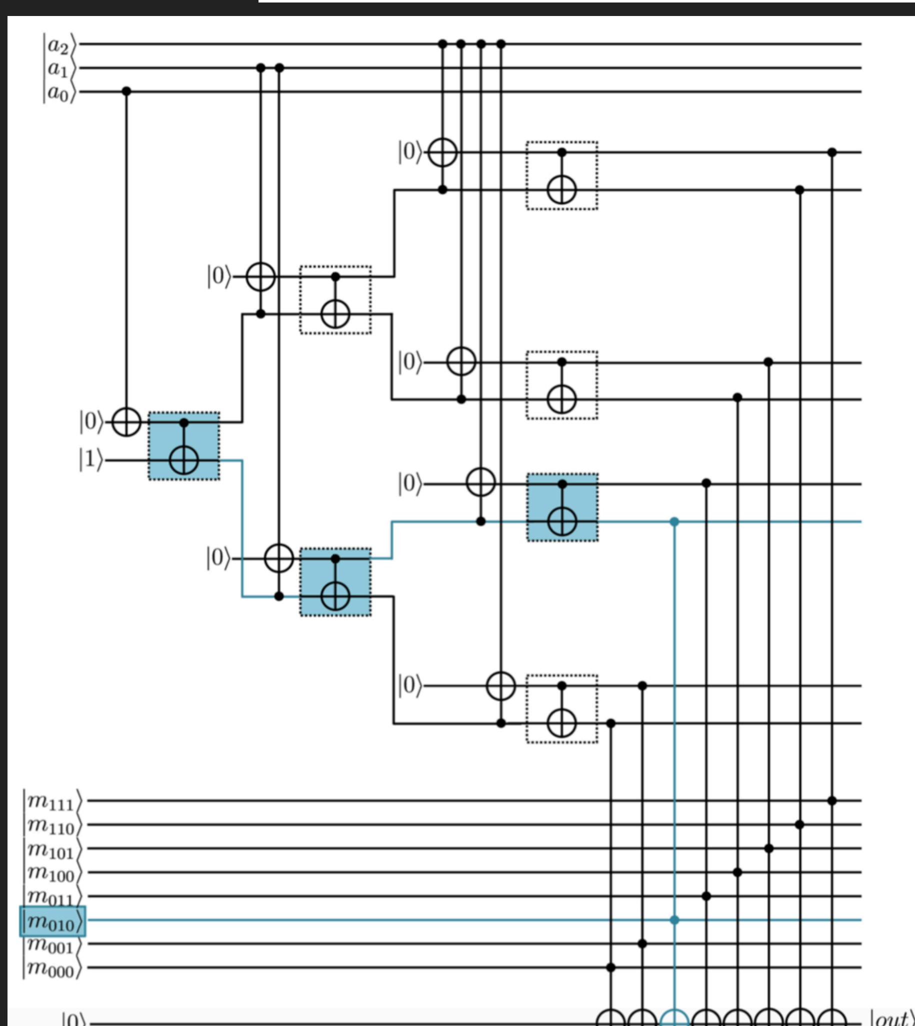
Vlad Gheorghiu, Michele Mosca

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

QRAM

Circuit	n	q	Total time (s)	Physical qubits
Bucket brigade parallel	15	-	$3.48 \cdot 10^{-4}$	$7.25 \cdot 10^{7}$
Large width small depth	15	14	$6.24 \cdot 10^{-4}$	$1.47 \cdot 10^{8}$
Small width large depth	15	14	7.86	$1.06 \cdot 10^{4}$
Bucket brigade parallel	36	-	$2.13 \cdot 10^{-3}$	$3.76 \cdot 10^{14}$
Large width small depth	36	35	$4.35 \cdot 10^{-3}$	$1.77 \cdot 10^{15}$
Small width large depth	36	35	$7.55 \cdot 10^{7}$	$7.03 \cdot 10^{4}$

TABLE II. Time and physical qubits required for fault-tolerant qRAM queries. The sizes $n = 15$ and $n = 36$ are analogous to 4KB and 8GB memory sizes respectively.



$$\sum_j \alpha_j |j\rangle|0\rangle \xrightarrow{qRAM} \sum_j \alpha_j |j\rangle|b_j\rangle$$

arXiv.org > quant-ph > arXiv:1902.01329

Search...

Help | Adv

Quantum Physics

Fault tolerant resource estimation of quantum random-access memories

Olivia Di Matteo, Vlad Gheorghiu, Michele Mosca

(Submitted on 4 Feb 2019)

Quantum random-access look-up of a string of classical bits is a necessary ingredient in several important quantum algorithms. In some cases, the cost of such quantum random-access memory (qRAM) is the limiting factor in the implementation of the algorithm. In this paper we study the cost of fault-tolerantly implementing a qRAM. We construct generic families of circuits which function as a qRAM, and analyze their resource costs when embedded in a surface code.

WHERE ARE WE TODAY? NISQ ERA

arXiv.org > quant-ph > arXiv:1801.00862

Search or Articl

(Help | Advanced se

Quantum Physics

Quantum Computing in the NISQ era and beyond

John Preskill

(Submitted on 2 Jan 2018 (v1), last revised 31 Jul 2018 (this version, v3))

Noisy Intermediate-Scale Quantum (NISQ) technology will be available in the near future. Quantum computers with 50-100 qubits may be able to perform tasks which surpass the capabilities of today's classical digital computers, but noise in quantum gates will limit the size of quantum circuits that can be executed reliably. NISQ devices will be useful tools for exploring many-body quantum physics, and may have other useful applications, but the 100-qubit quantum computer will not change the world right away --- we should regard it as a significant step toward the more powerful quantum technologies of the future. Quantum technologists should continue to strive for more accurate quantum gates and, eventually, fully fault-tolerant quantum computing.

Comments:	20 pages. Based on a Keynote Address at Quantum Computing for Business, 5 December 2017. (v3) Formatted for publication in Quantum, minor revisions
Subjects:	**Quantum Physics (quant-ph)**; Strongly Correlated Electrons (cond-mat.str-el)
Journal reference:	Quantum 2, 79 (2018)
DOI:	10.22331/q-2018-08-06-79
Cite as:	**arXiv:1801.00862 [quant-ph]** (or **arXiv:1801.00862v3 [quant-ph]** for this version)

www.sciencemag.org SCIENCE VOL 339 8 MARCH 2013

Superconducting Circuits for Quantum Information: An Outlook

M. H. Devoret[1,2] and R. J. Schoelkopf[1*]

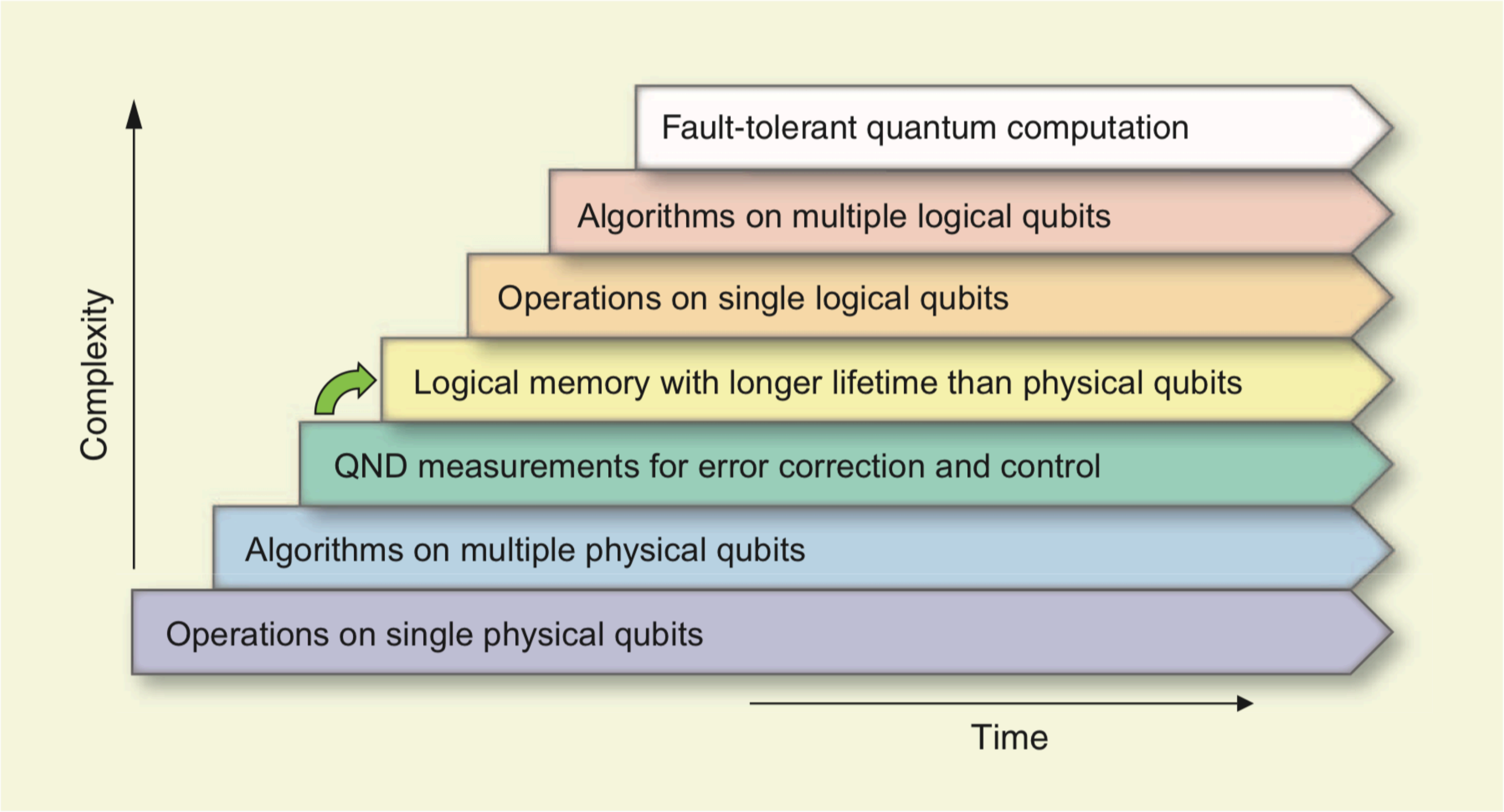
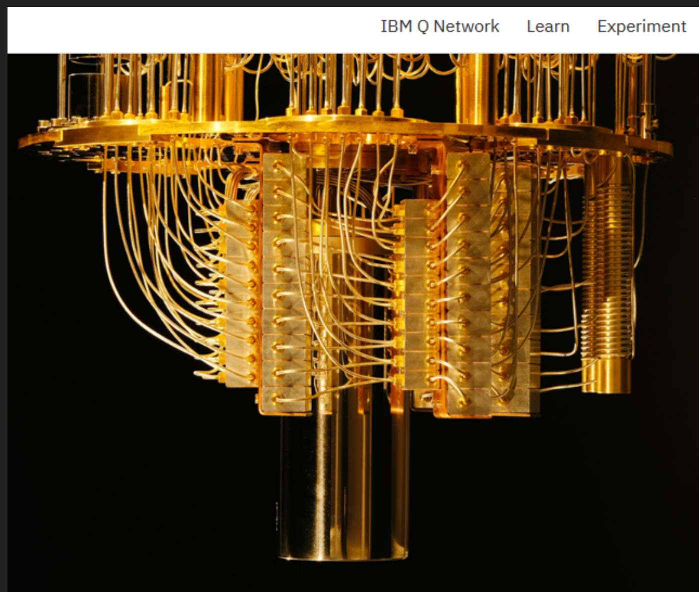
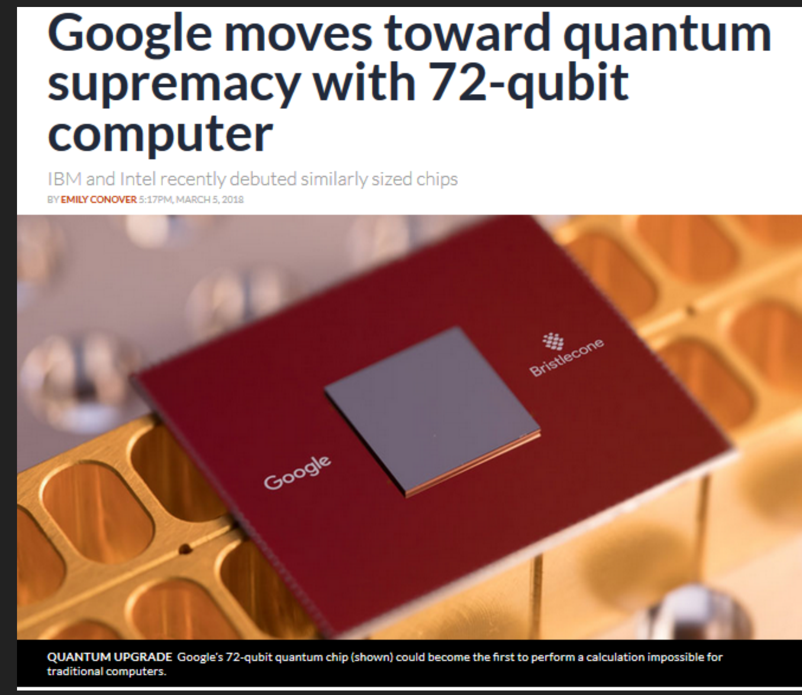
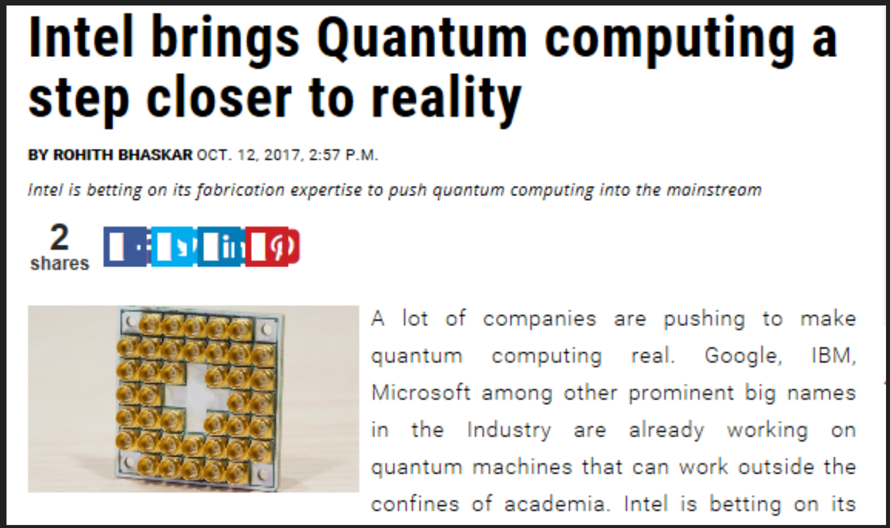


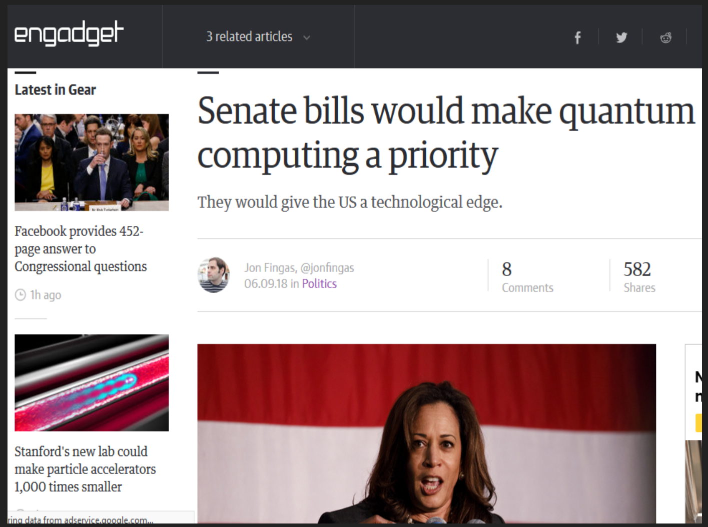
Fig. 1. Seven stages in the development of quantum information processing. Each advancement requires mastery of the preceding stages, but each also represents a continuing task that must be perfected in parallel with the others. Superconducting qubits are the only solid-state implementation at the third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

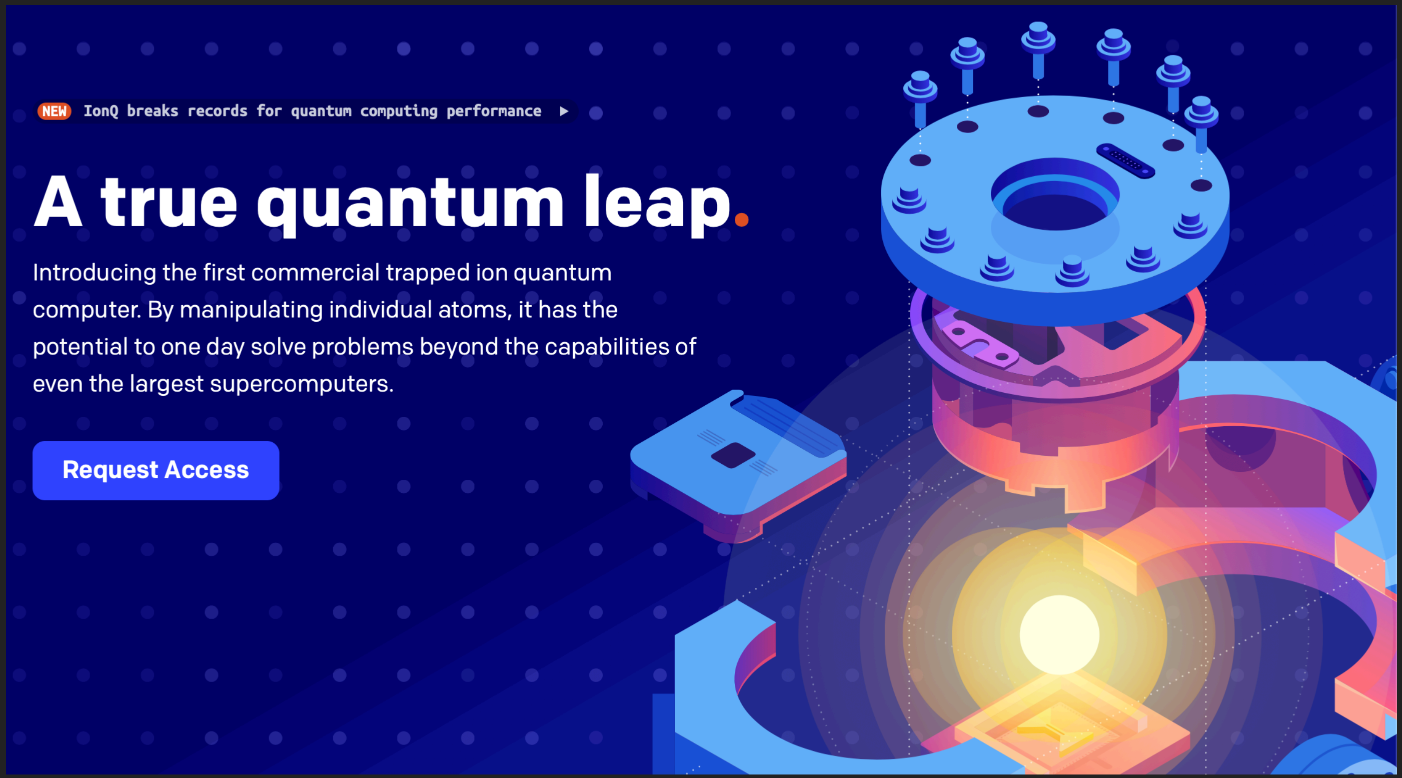

IBM Q Network
Learn
Experiment


Google moves toward quantum supremacy with 72-qubit computer
IBM and Intel recently debuted similarly sized chips
BY EMILY CONOVER 5:17PM, MARCH 5, 2018
Bristlecone
Google
QUANTUM UPGRADE Google's 72-qubit quantum chip (shown) could become the first to perform a calculation impossible for traditional computers.


Search
Bloomberg
Sign In
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


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


engadget
3 related articles
Latest in Gear
Facebook provides 452-page answer to Congressional questions
1h ago
Stanford's new lab could make particle accelerators 1,000 times smaller
Senate bills would make quantum computing a priority
They would give the US a technological edge.
Jon Fingas, @jonfingas
06.09.18 in Politics
8
Comments
582
Shares


NEW IonQ breaks records for quantum computing performance
A true quantum leap.
Introducing the first commercial trapped ion quantum computer. By manipulating individual atoms, it has the potential to one day solve problems beyond the capabilities of even the largest supercomputers.
Request Access


Rigetti Eyes Scaling with 128-Qubit Architecture
By George Leopold
August 10, 2018

POPULAR SCIENCE
WANT MORE?

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

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'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

THANK YOU

Vlad Gheorghiu

Post-doctoral fellow
Institute for Quantum Computing, University of Waterloo

Co-Founder and CEO, softwareQ Inc.
www.softwareq.ca

Quantum Risk Researcher, evolutionQ Inc.
www.evolutionq.com

vlad.gheorghiu@uwaterloo.ca vlad@softwareq.ca