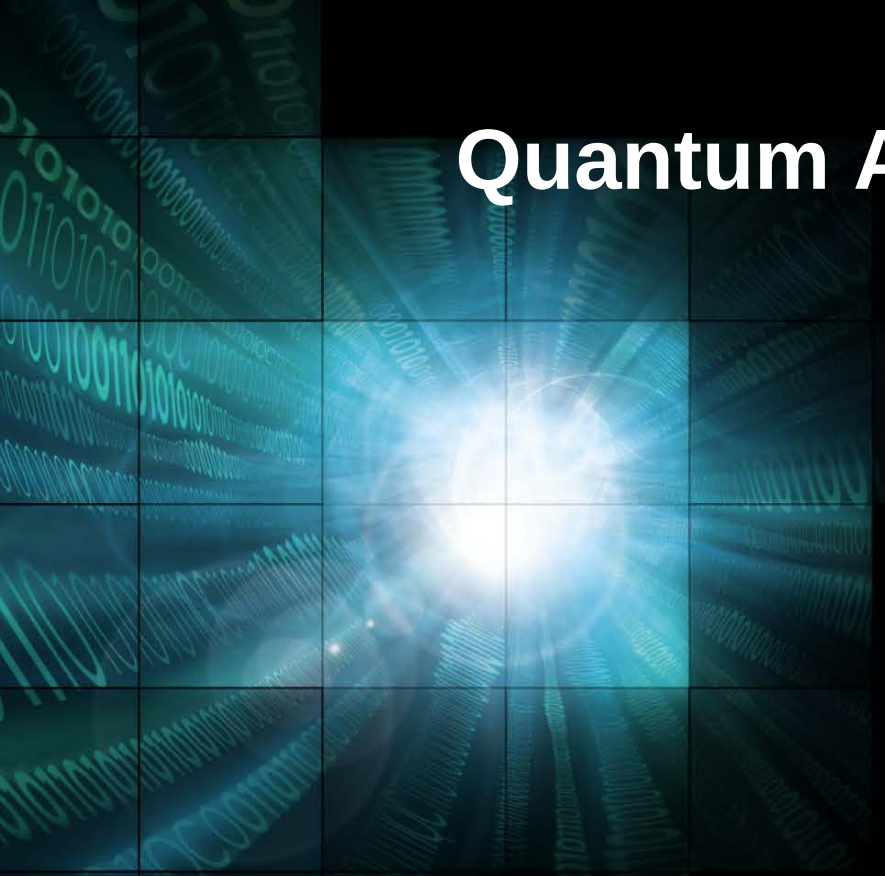


Quantum Algorithms Introduction

AIM Workshop on Quantum algorithms for analysis of public-key crypto

Michele Mosca

4 February 2019

PERIMETER INSTITUTE FOR THEORETICAL PHYSICS

evolutionQ

Quantum-Safe CANADA

UNIVERSITY OF WATERLOO | IQC Institute for Quantum Computing

softwareQ

CryptoWorks21



Cloud computing, Payment systems, Internet, IoT, etc…

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

Cryptography:RS[illegible]DH, EC[illegible]DSA,…, SHA, AES

So many different vulnerabilities

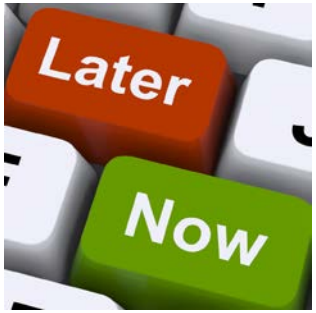
- Fundamentally vulnerable cryptography
- Cryptography implementation errors
- User errors
- Platform implementation errors
- Platform design errors
- Admin errors
- Corrupt users
- Corrupt admin

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

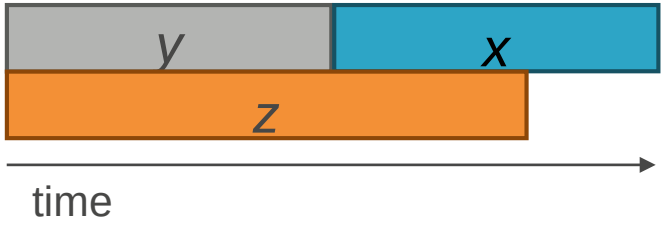
Do we need to worry *now*?

- Depends on*:
- How long do you need your cryptographic keys to be secure? – *security shelf-life* (*x* years)
- How much time will it take to re-tool the existing infrastructure with large-scale quantum-safe solution? (*y* years) – *migration time*
- How long will it take for a large-scale quantum computer to be built (or for any other relevant advance)? (*z* years) – *collapse time*
- "Theorem": If $x + y > z$, then worry.





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



Business bottom line

Fact: If x+y>z, then you will not be able to provide the required x years of security.

Fact: If y>z then cyber systems will collapse in z years with no quick fix.

Fact: Rushing “y” will be expensive, disruptive, and lead to vulnerable implementations.

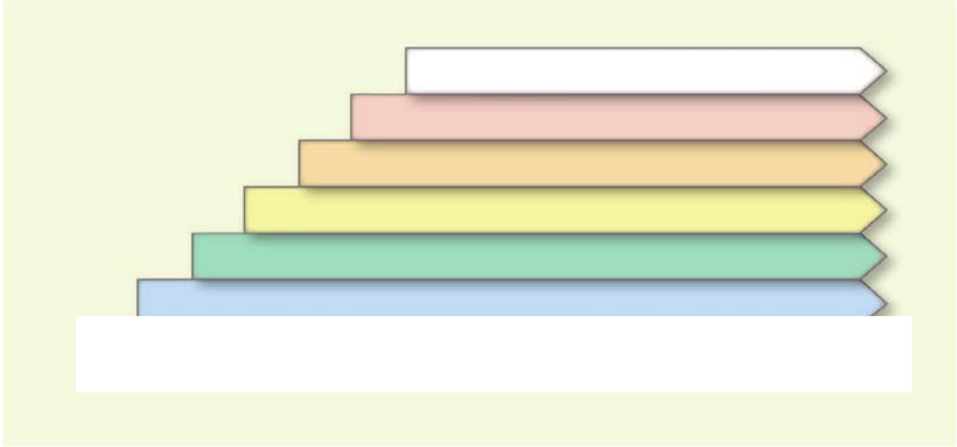
Prediction: In the next 6-12 months, more organizations will be differentiated by whether or not they have a well-articulated quantum risk management plan.

How close are we to having sufficient quantum resources?

REVIEW SCIENCE VOL 339 8 MARCH 2013

Superconducting Circuits for Quantum Information: An Outlook

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



What is ‘z’?

- **M. 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**”*.*
- **M. Mosca** ([NIST, April 2015], [ISACA**,** September 2015]): *“1/7 chance of breaking RSA-2048 by 2026, ½ chance by 2031”*
- **M. 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”*

http://nap.edu/QuantumComputing



Quantum Computing: Progress and Prospects

Report Release Webinar on 12/4 at 1pm EST

COMMITTEE ON TECHNICAL ASSESSMENT OF THE FEASIBILITY AND IMPLICATIONS OF QUANTUM COMPUTING

MARK A. HOROWITZ, NAE,[1] Stanford University, *Chair*
ALÁN ASPURU-GUZIK, University of Toronto
DAVID D. AWSCHALOM, NAS/NAE,[2] University of Chicago
BOB BLAKLEY, Citigroup
DAN BONEH, NAE, Stanford University
SUSAN N. COPPERSMITH, NAS, University of Wisconsin, Madison
JUNGSANG KIM, Duke University
JOHN M. MARTINIS, Google, Inc.
MARGARET MARTONOSI, Princeton University
MICHELE MOSCA, University of Waterloo
WILLIAM D. OLIVER, Massachusetts Institute of Technology
KRYSTA SVORE, Microsoft Research
UMESH V. VAZIRANI, NAS, University of California, Berkeley

Staff

EMILY GRUMBLING, Study Director, Computer Science and Telecommunications Board (CSTB)
SHENAE BRADLEY, Administrative Assistant, CSTB
JON EISENBERG, Senior Director, CSTB
KATIRIA ORTIZ, Associate Program Officer, CSTB
JANKI PATEL, Senior Program Assistant, CSTB

Key Finding 1: Given the current state of quantum computing and recent rates of progress, it is highly unexpected that a quantum computer that can compromise RSA 2048 or comparable discrete logarithm-based public key cryptosystems will be built within the next decade. (Chapter 7)

Key Finding 10: Even if a quantum computer that can decrypt current cryptographic ciphers is more than a decade off, the hazard of such a machine is high enough—and the time frame for transitioning to a new security protocol is sufficiently long and uncertain—that prioritization of the development, standardization, and deployment of post-quantum cryptography is critical for minimizing the chance of a potential security and privacy disaster. (Chapter 7)

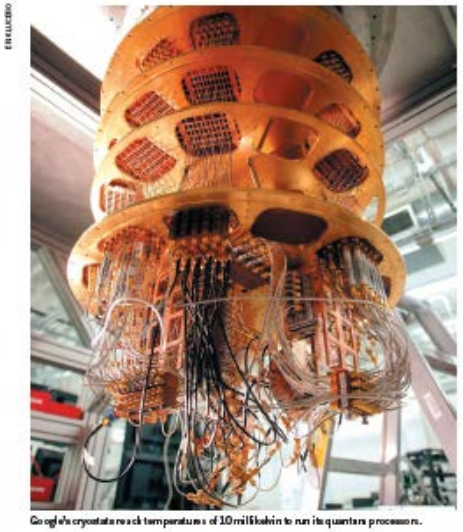
Non-fault-tolerant quantum devices

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."



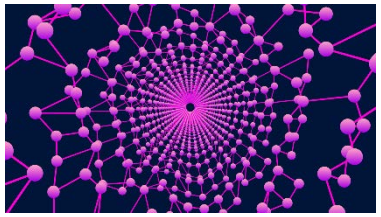
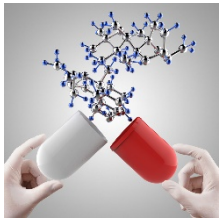
Google's cryostats reach temperatures of 10 millikelvin to run its quantum processors.

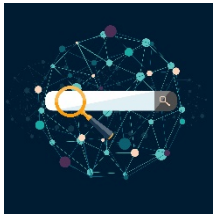
Commercialize early quantum technologies

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.

Scalable fault-tolerant quantum computer

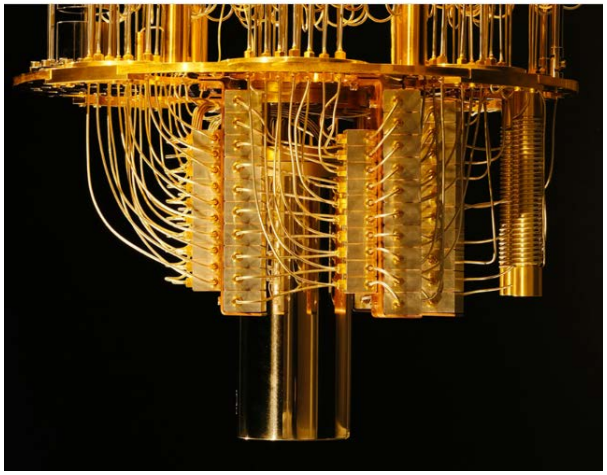
Known to solve many problems previously thought to be intractable



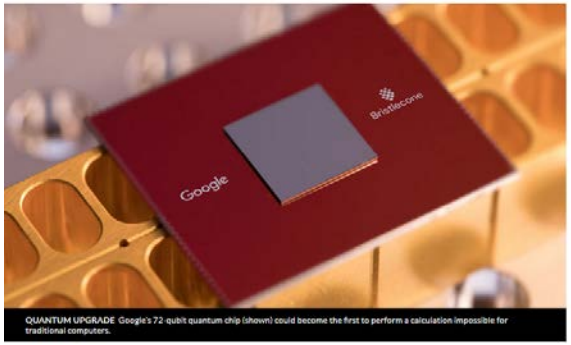

©2017 M. Mosca

IBM Q Network Learn Experiment



Google moves toward quantum supremacy with 72-qubit computer

IBM and Intel recently debuted similarly sized chips



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

Bloomberg

Technology

Microsoft Edges Closer to Quantum Computer Based on Elusive Particle

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

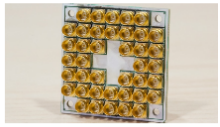
By Jeremy Kahn
March 28, 2018, 11:48 AM EDT *Corrected March 28, 2018, 2:09 PM EDT*

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

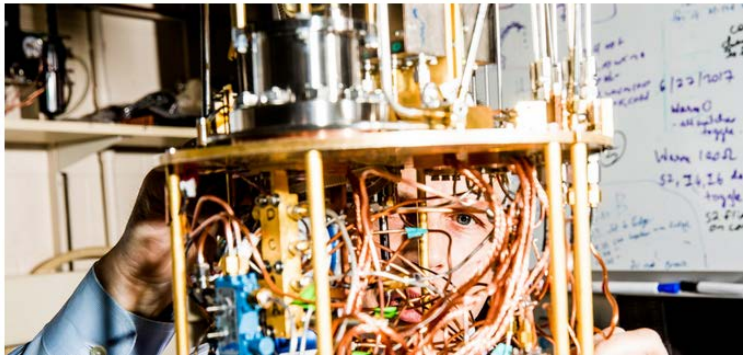
582 Shares



TECHNOLOGY

Yale Professors Race Google and IBM to the First Quantum Computer

By CADE METZ NOV. 13, 2017



POPULAR SCIENCE
WANT MORE?

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

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.



Lithium's Big

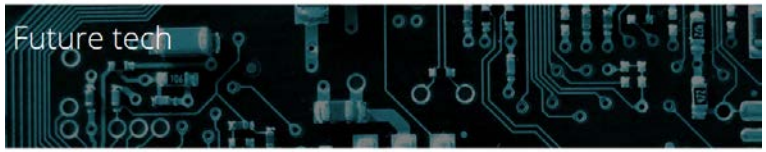
Alibaba puts 11-qubits quantum power on public cloud

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

China's Alibaba Hires Quantum Computer Scientist Mario Szegedy

PAN YUE
January 18, 2018 — 10:50 HKT

Follow Us:



Tencent Quantum Laboratory is under construction, the next three major laboratories will provide a wealth of AI scenarios

via:博客园 time:2017/12/29 20:31:04 readed:878

*SNG is putting a lot of effort into the layout of artificial intelligence. At present, SNG has excellen labs, audio and video labs, and quantum labs. *Tang Dao-sheng, senior executive vice president of Tencent Group and president of the Social Networking Group (SNG), said in his opening speech.



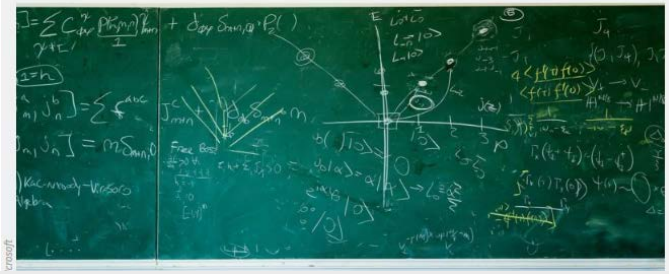
ars TECHNICA BIZ & IT TECH SCIENCE POLICY CARS GAMING & CULTURE

OH BOY! —

Microsoft's Q# quantum programming language out now in preview

It's pronounced "Q sharp."

PETER BRIGHT - 12/11/2017, 5:30 PM





Rigetti Rolls Out Latest Forest Quantum Developer Environment

By John Russell

February 27, 2018

Join the IBM Q Experience Community

The IBM Q Experience Community brings together researchers and quantum enthusiasts to share, connect and collaborate

Log in

What exactly are we trying to build?

Theorem:

The set

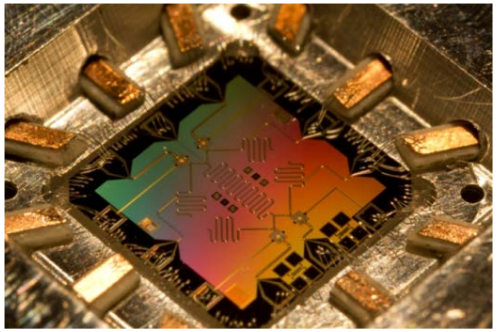
$$G = \{H, T, CNOT\}$$

is a universal set of gates.

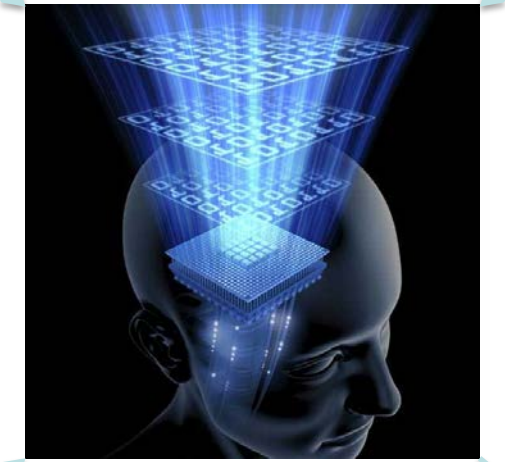
i.e. any *n*-qubit unitary operator *U* can be approximated with error ε, for any $\varepsilon > 0$, using a finite circuit with gates from *G*.

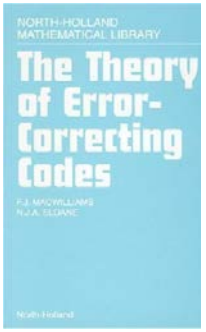
There are many other universal gate sets, though this “Clifford +T” gate set is studied extensively. There is an elegant theory of fault-tolerant quantum-error correction built around it.

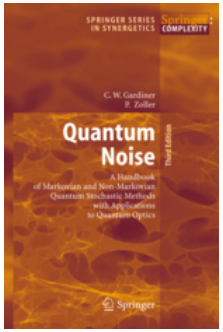
“Threshold theorem”



Architecture description







Error model

Threshold “ε”

If the error rates of the basic operations of the device are below ε,

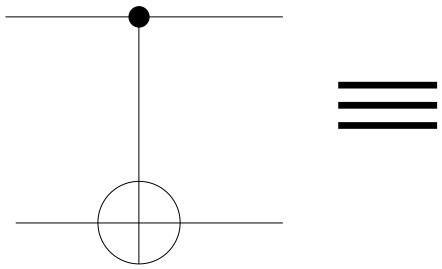
then we can efficiently scale quantum computations.

Physical qubits and gates versus logical qubits and gates

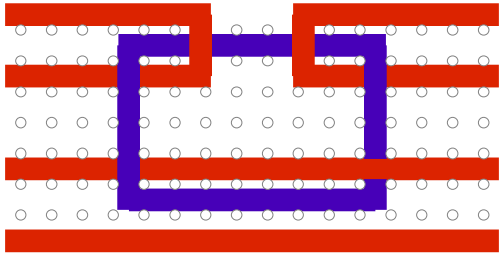
Logical layer

Physical layer

CNOT



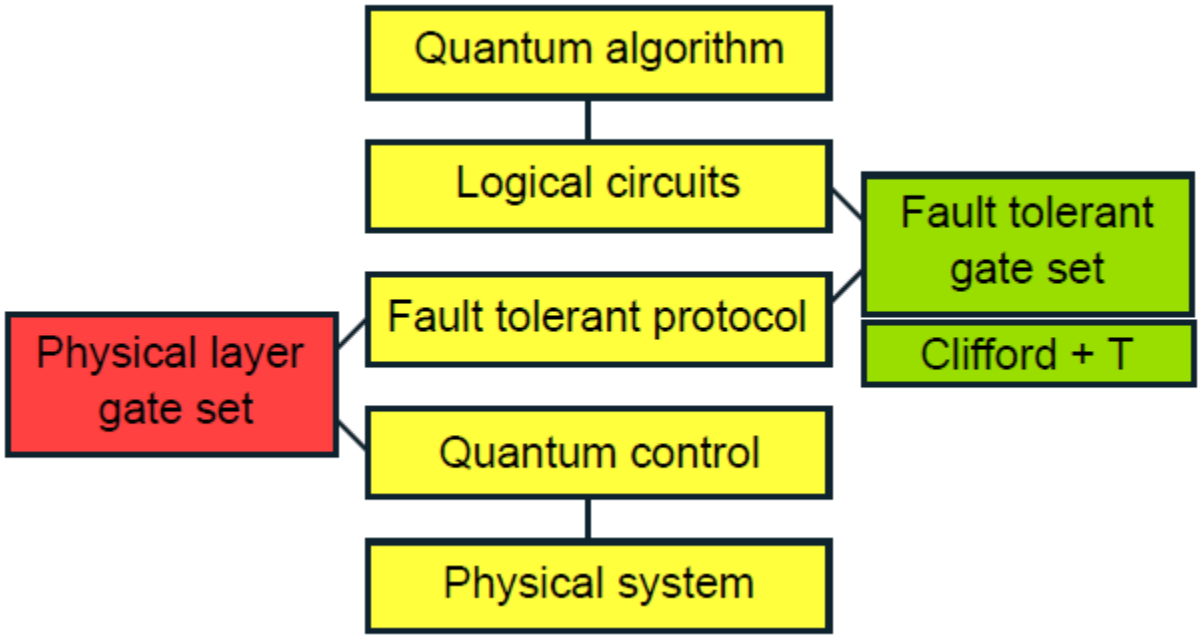
fault-tolerant CNOT



What resources are required to implement a specific quantum attack?

- A billion physical qubits and a trillion physical gates?
- A million qubits and 100 million gates?
- Something else?
- Asymptotic complexity estimates give a very coarse-grained approximation.
- To attempt to estimate this question, we need a more fine-grained study of the full tool chain between algorithms and physical qubits.

Quantum compilers



Examples of technical advances in quantum compilation

- Use number theory methods to bypass Solovay-Kitaev algorithm and achieve optimal synthesis of one-qubit unitaries (over Clifford and T gates)
- Use matroid partitioning to reduce T-complexity and T-depth
- Use channel representation of unitaries to find optimal T-depth

The art of quantum algorithmics is to choreograph constructive interference on desirable outcomes and destructive interference on undesirable outcomes.

Some basic tools

The Hadamard basis change

$$|0\rangle \xrightarrow{\text{H}} \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$$

$$|1\rangle \xrightarrow{\text{H}} \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$$

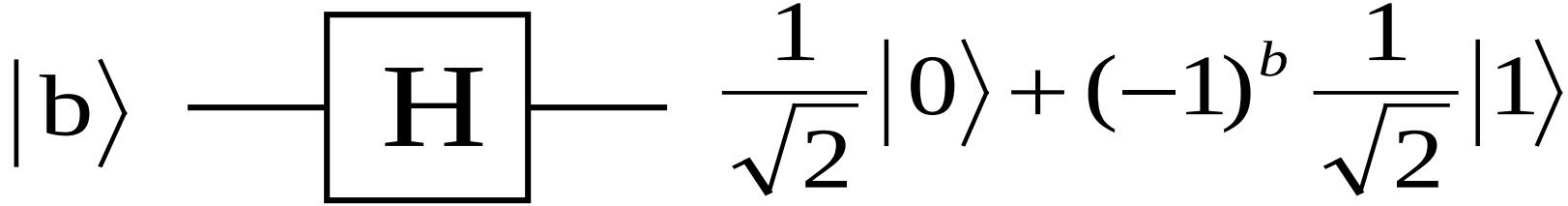
$$\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle \xrightarrow{\text{H}} |0\rangle$$

$$\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle \xrightarrow{\text{H}} |1\rangle$$

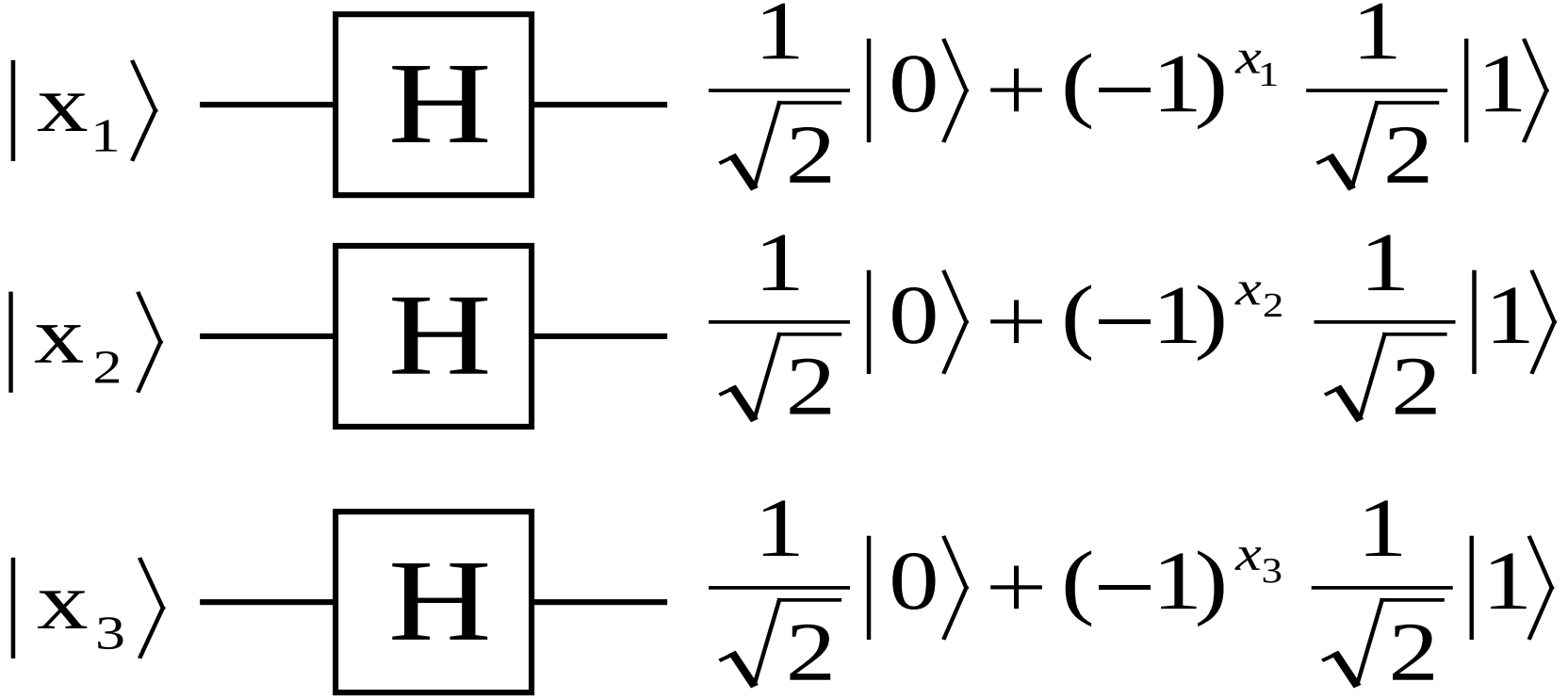
The Hadamard transformation: summary

$$|\mathrm{b}\rangle \xleftrightarrow{H} \frac{1}{\sqrt{2}}|0\rangle + (-1)^{b}\frac{1}{\sqrt{2}}|1\rangle$$

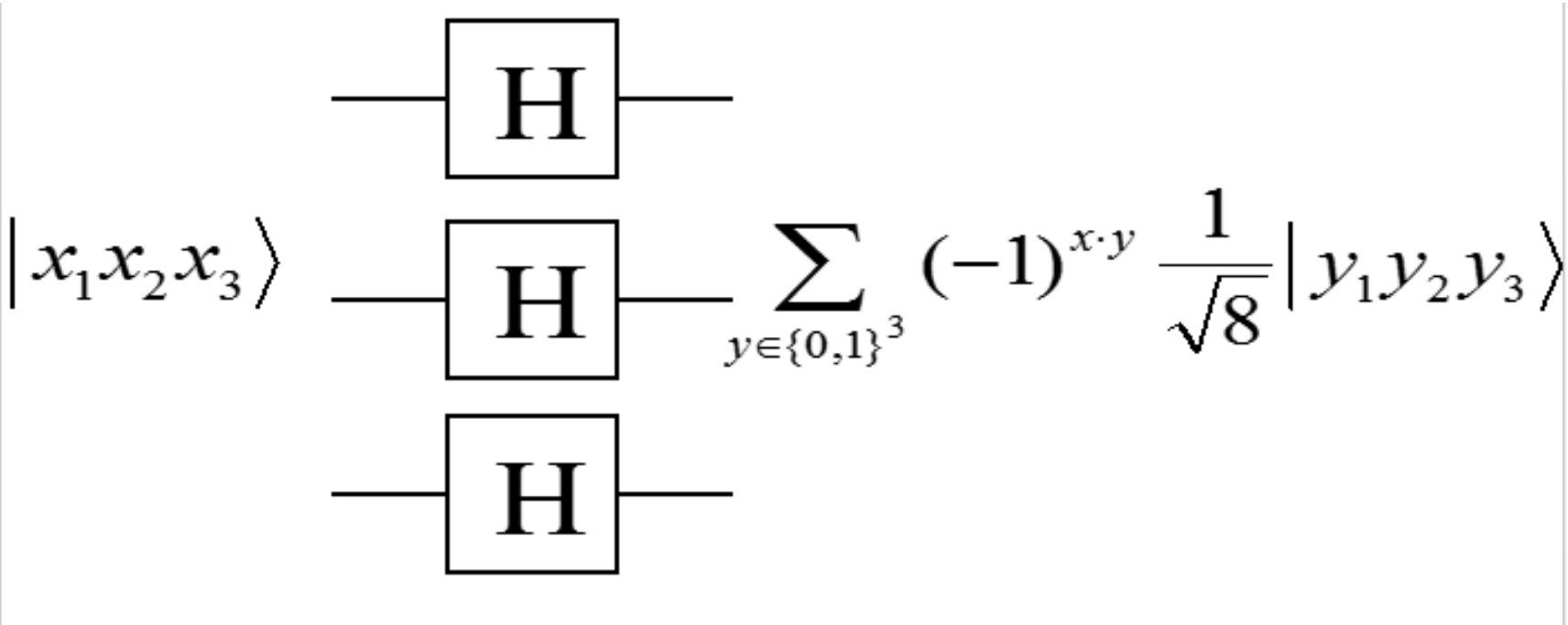
The Hadamard transformation: circuit notation



The Hadamard transformation on several bits



The Hadamard transformation: global view



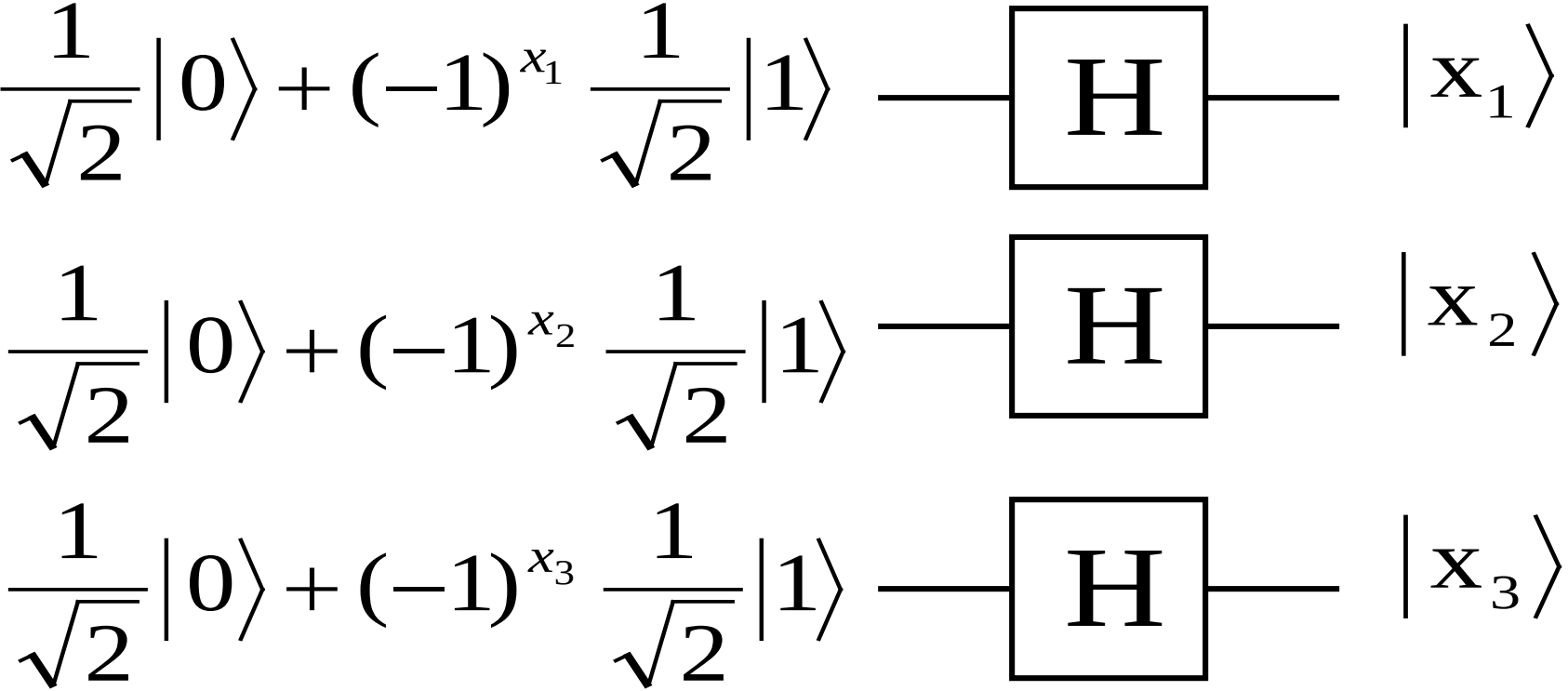
The Hadamard transformation: global view

$$\left|x_1 x_2 x_3\right\rangle \xrightarrow{H \otimes H \otimes H} \sum_{y \in \{0,1\}^3} (-1)^{x \cdot y} \frac{1}{\sqrt{8}} \left|y_1 y_2 y_3\right\rangle$$

The Hadamard transformation: global view

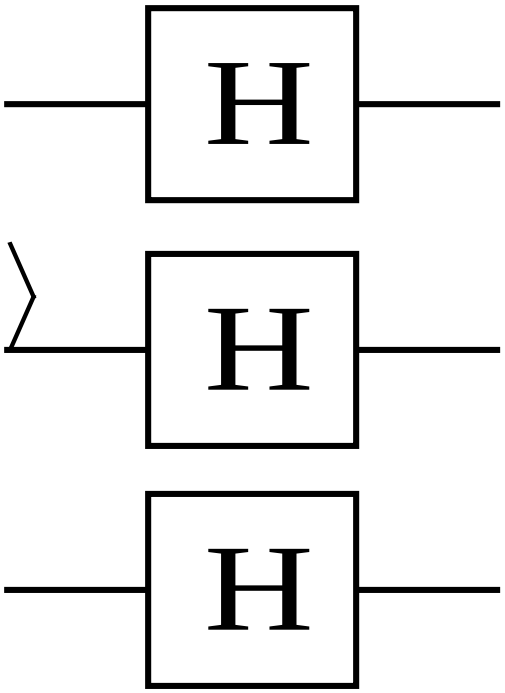
$$H \otimes H \otimes H \left| x_1 x_2 x_3 \right\rangle = \sum_{y \in \{0,1\}^3} (-1)^{x \cdot y} \frac{1}{\sqrt{8}} \left| y_1 y_2 y_3 \right\rangle$$

The Hadamard transformation on several bits



The Hadamard transformation: global view

$$\sum_{y\in\{0,1\}^3} (-1)^{x\cdot y} \frac{1}{\sqrt{2}} \left| y_1 y_2 y_3 \right\rangle$$



$$\left| x_1 x_2 x_3 \right\rangle$$

The Hadamard transformation: global view

$$\sum_{y\in\{0,1\}^3} (-1)^{x\cdot y} \frac{1}{\sqrt{2}} \left| y_1 y_2 y_3 \right\rangle \xrightarrow{H\otimes H\otimes H} \left| x_1 x_2 x_3 \right\rangle$$

Looking at NOT and CNOT in Hadamard bases

Consider applying a NOT gate to the following states

$$|0\rangle + |1\rangle \xrightarrow{\text{NOT}} |0\rangle + |1\rangle$$

$$|0\rangle - |1\rangle \xrightarrow{\text{NOT}} -(|0\rangle - |1\rangle)$$

e.g.

Now consider applying a controlled-NOT gate to the following states

$$|0\rangle(|0\rangle+|1\rangle)\xrightarrow{\text{CNOT}}|0\rangle(|0\rangle+|1\rangle)$$

$$|1\rangle(|0\rangle+|1\rangle)\xrightarrow{\text{CNOT}}|1\rangle(|0\rangle+|1\rangle)$$

$$|0\rangle(|0\rangle-|1\rangle)\xrightarrow{\text{CNOT}}|0\rangle(|0\rangle-|1\rangle)$$

$$|1\rangle(|0\rangle-|1\rangle)\xrightarrow{\text{CNOT}}-|1\rangle(|0\rangle-|1\rangle)$$

Computing functions into the phase

Suppose we know how to compute a function

$$f : \{0,1\} \rightarrow \{0,1\}$$

$$|x\rangle|c\rangle \xrightarrow{U_f} |x\rangle|c \oplus f(x)\rangle$$

$$|x\rangle\left(|0\rangle - |1\rangle\right) \xrightarrow{U_f} (-1)^{f(x)}|x\rangle\left(|0\rangle - |1\rangle\right)$$

Generalization (Kitaev): Eigenvalue “kick-back”

Suppose we know how to compute an operator

$$U|\psi\rangle = e^{i\phi}|\psi\rangle$$

Then the “controlled-U” gives us

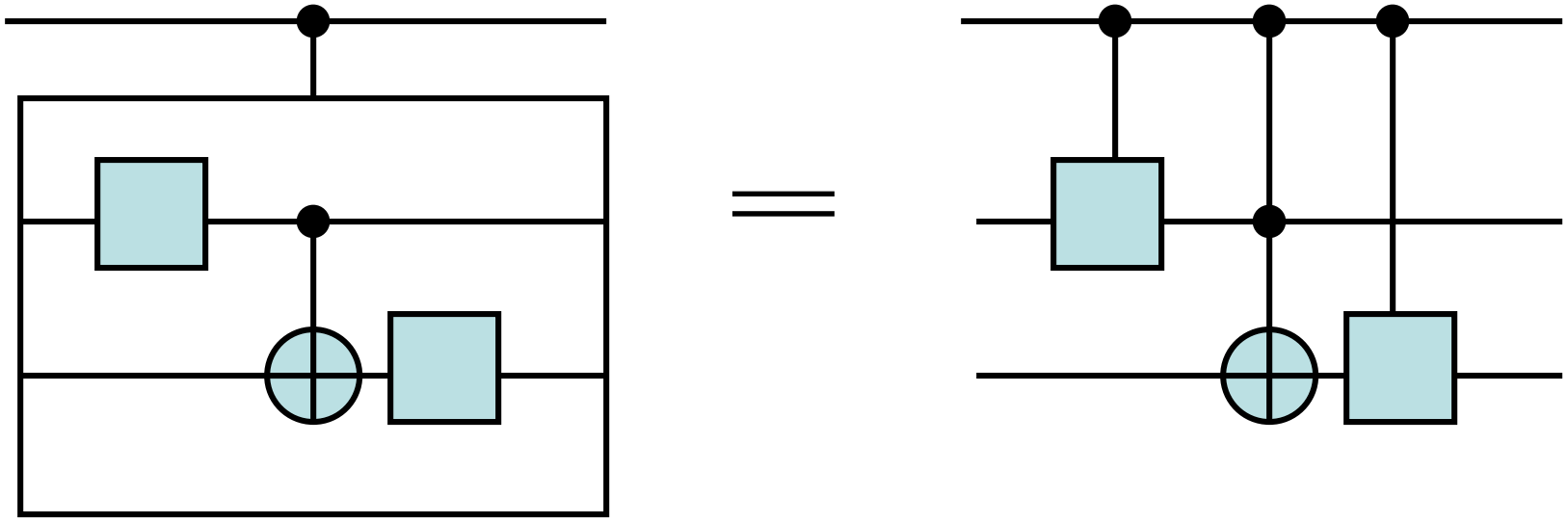
$$c-U|0\rangle|\psi\rangle = |0\rangle|\psi\rangle$$

$$c-U|1\rangle|\psi\rangle = e^{i\phi}|1\rangle|\psi\rangle$$

$$c-U\left(|0\rangle+|1\rangle\right)|\psi\rangle = \left(|0\rangle+e^{i\phi}|1\rangle\right)|\psi\rangle$$

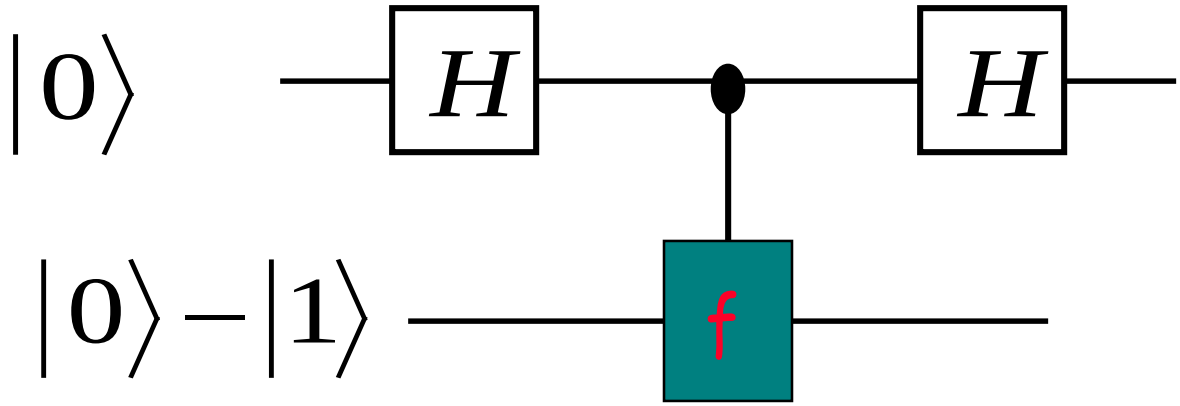
How do we implement c-U?

Replace every gate G in the circuit for U with a c-G.
For example,

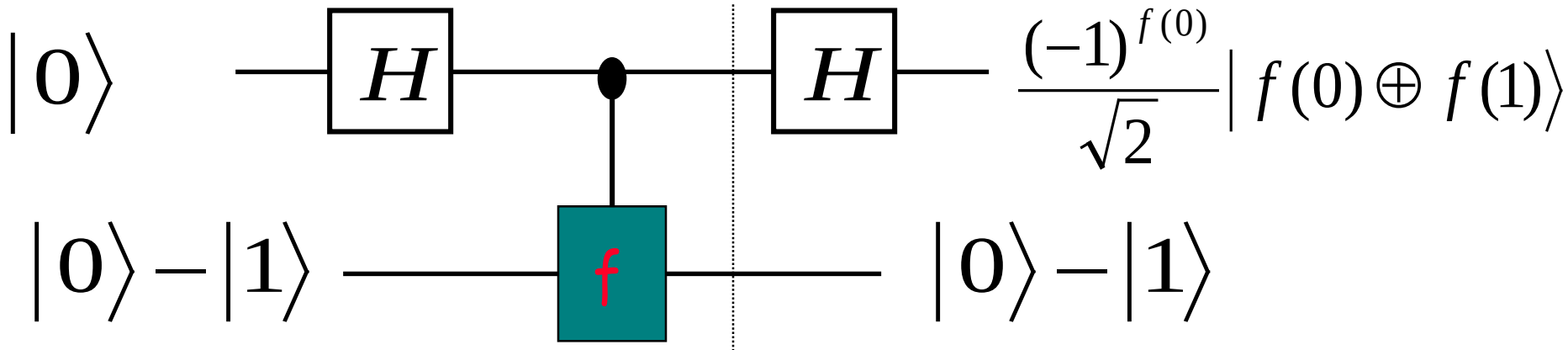


Deutsch's problem

Compute $f(0) \oplus f(1)$ using U_f only once



Deutsch algorithm



$$\frac{1}{\sqrt{2}}\left((-1)^{f(0)}|0\rangle+(-1)^{f(1)}|1\rangle\right)\left(|0\rangle-|1\rangle\right)$$

$$=\frac{(-1)^{f(0)}}{\sqrt{2}}\left(|0\rangle+(-1)^{f(0)\oplus f(1)}|1\rangle\right)\left(|0\rangle-|1\rangle\right)$$

Garbage-free implementations of f(x)

- Does the Deutsch algorithm work if when we implement

$$|x\rangle|0\rangle \longrightarrow |x\rangle|f(x)\rangle$$

we actually leave “junk” information in ancilla qubits?

$$|x\rangle|0\rangle|0\rangle \longrightarrow |x\rangle|f(x)\rangle|junk(x)\rangle$$

No!! We need a “clean” implementation of f(x).

Making reversible circuits

(see Fig. 1.6 in KLM text)

- One problem is that there will be junk left in the extra bits
- Bennett showed how to “uncompute” the junk

$$|x\rangle|0\rangle|0\rangle|0\rangle$$

$$\xrightarrow{compute\ f(x)} |x\rangle|f(x)\rangle|junk(x)\rangle|0\rangle$$

$$\xrightarrow{copy\ f(x)} |x\rangle|f(x)\rangle|junk(x)\rangle|f(x)\rangle$$

$$\xrightarrow{uncompute\ f(x)} |x\rangle|0\rangle|0\rangle|f(x)\rangle$$

Making reversible circuits

- An irreversible circuit with space S and depth (or “time”) T can thus be simulated by a reversible circuit with space in O(S+T) and time O(T)
- Bennett also showed how to implement a reversible version with time $O(T^{1+\varepsilon})$ and space O(S log(T)) or time O(T) and space $O(ST^{\varepsilon})$.

Bernstein-Vazirani problem

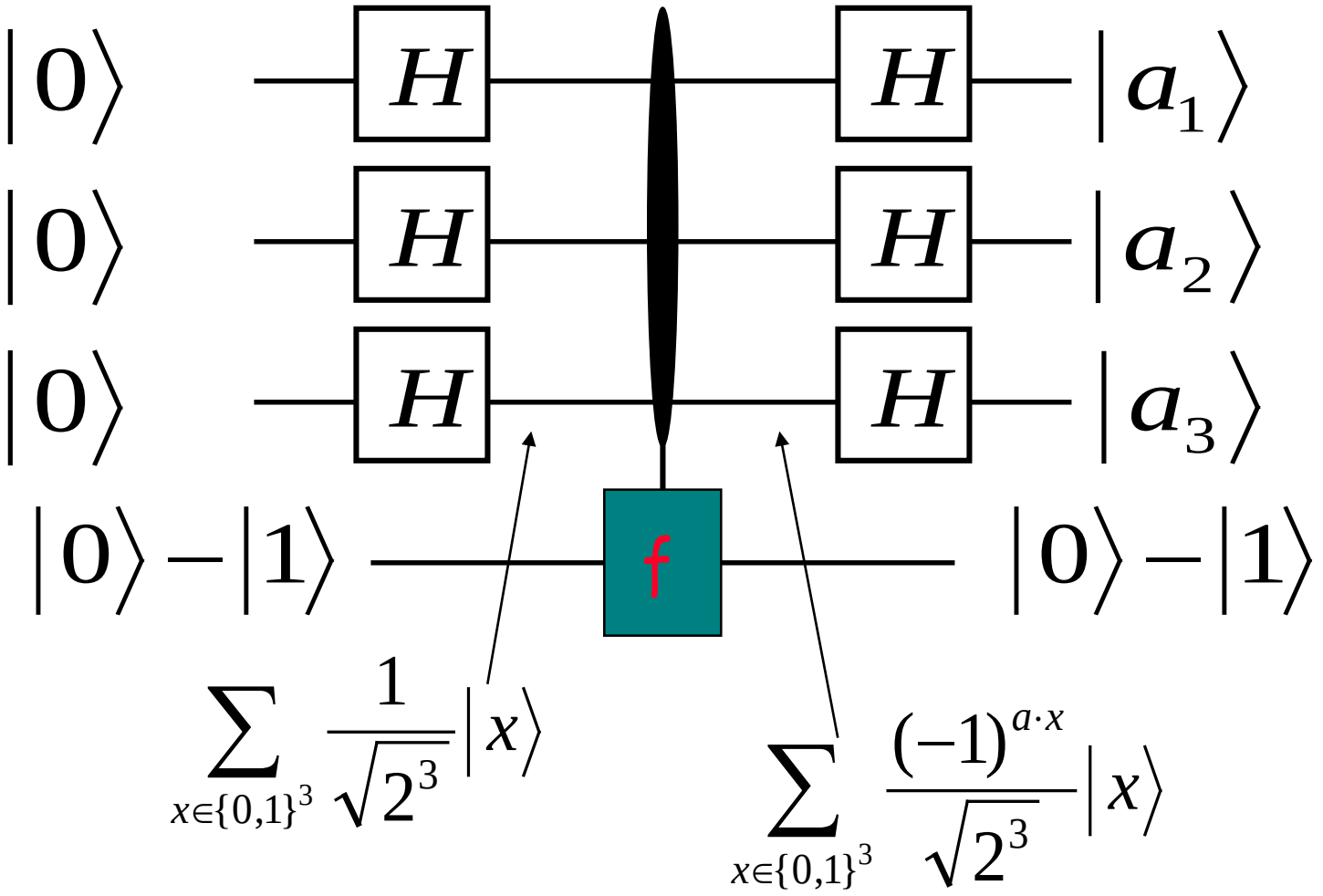
Suppose $f : \{0,1\}^n \to \{0,1\}$ is of the form $f(x) = a \cdot x$

for some $a \in \{0,1\}^n$

Given $|x\rangle|c\rangle \xrightarrow{U_f} |x\rangle|c \oplus f(x)\rangle$

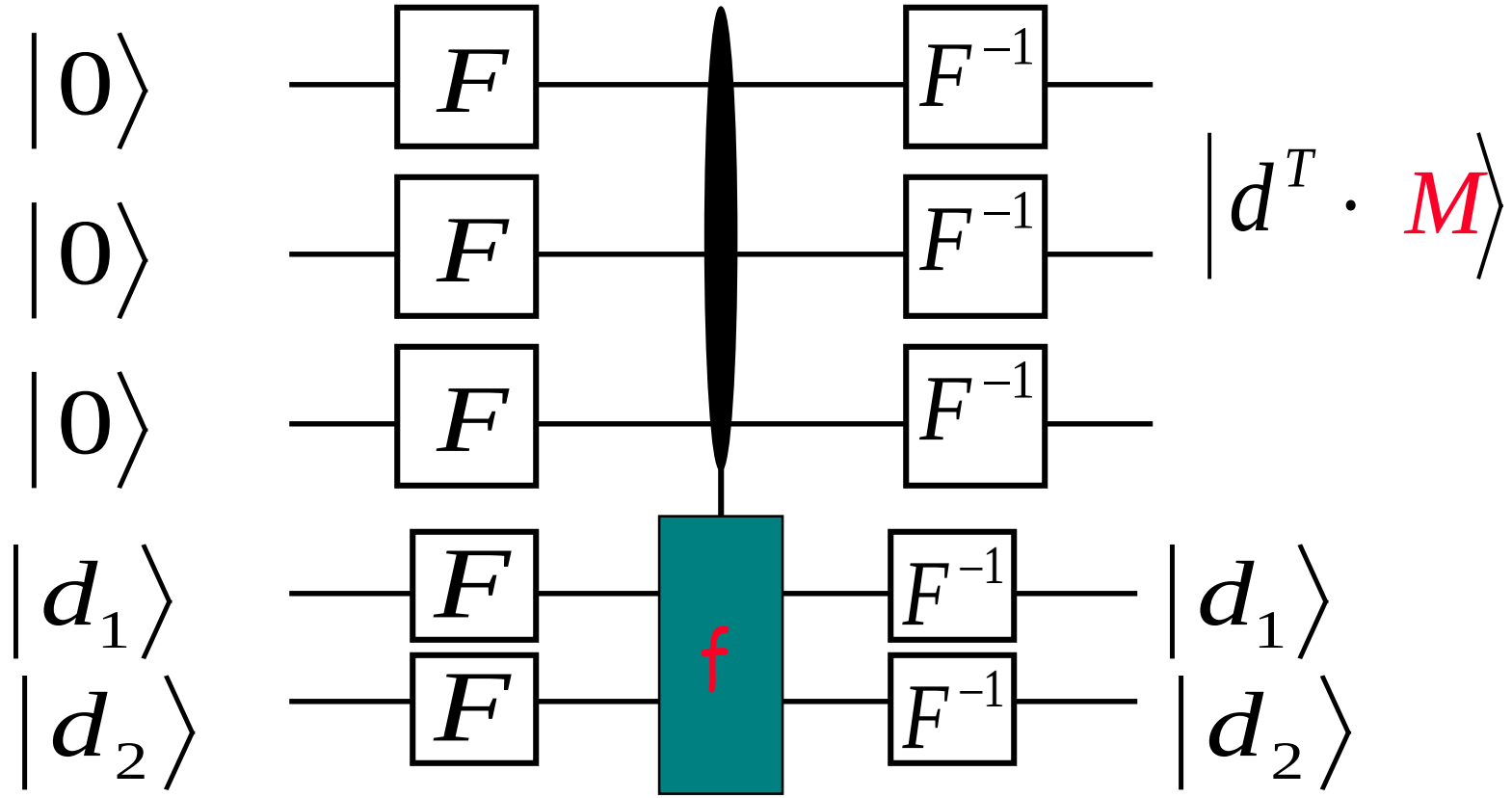
determine $a = a_1 a_2 \cdots a_n$

Bernstein-Vazirani problem



Generally

$$f : Z_p^n \rightarrow Z_p^m \qquad x \longrightarrow Mx$$



Another property of Hadamard transformation

Consider $S \leq Z_2^{\,n}$

$$S^{\perp} = \left\{ t : t \in Z_2^{\,n}, s \cdot t = 0 \ \forall s \in S \right\}$$

Let $$\left| y + S \right\rangle = \sum_{s \in S} \frac{1}{\sqrt{\left| S \right|}} \left| y + s \right\rangle$$

Then $$H^{\otimes n} \left| y + S \right\rangle = \sum_{t \in S^{\perp}} \frac{(-1)^{y \cdot t}}{\sqrt{\left| S^{\perp} \right|}} \left| t \right\rangle$$

Simon's problem

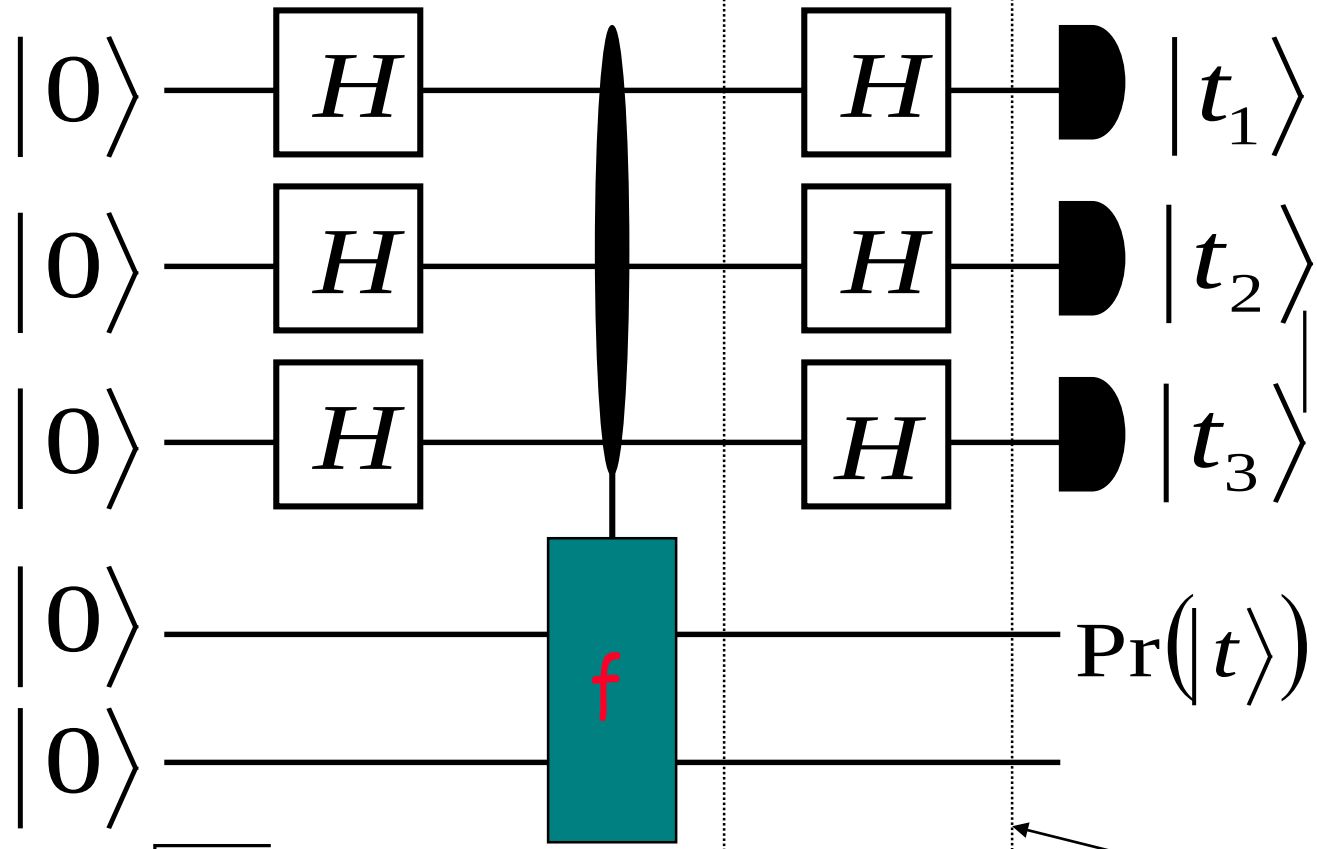
Suppose that $f : \{0,1\}^n \to X$ has the property that

$f(x) = f(y)$ iff $x + S = y + S$

For some "hidden subgroup" $S \leq Z_2{}^n$

Given $|x\rangle|0\rangle \xrightarrow{U_f} |x\rangle|f(x)\rangle$ find S

Simon's algorithm



$$\sum_{y+S \in Z_2^3/S} \sqrt{\frac{|S|}{|2^n|}} |y+S\rangle |f(y)\rangle$$

$$\frac{1}{|S^{\perp}|} \sum_{y+S \in Z_2^3/S} \left(\sum_{t \in S^{\perp}} (-1)^{y \cdot t} |t\rangle \right) |f(y)\rangle$$

Applications of Simon's algorithm??

Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer*

Peter W. Shor†

n 1996

computer. Indeed, while Bernstein and Vaziarni's problem appears contrived, Simon's problem looks quite natural. Simon's algorithm inspired the work presented in this paper.

Quantum Distinguisher Between the 3-Round Feistel Cipher and the Random Permutation

Hidenori Kuwakado
Graduate School of Engineering
Kobe University
1-1 Rokkodai-cho Nada-ku Kobe 657-8501, Japan

Masakatu Morii
Graduate School of Engineering
Kobe University
1-1 Rokkodai-cho Nada-ku Kobe 657-8501, Japan

$$
\begin{aligned}
\mathrm{FP}(x) &= \mathrm{FP}(a \parallel c) \\
&= c \oplus P_2(a \oplus P_1(c)) \\
&\quad \parallel (a \oplus P_1(c)) \oplus P_3(c \oplus P_2(a \oplus P_1(c))) \\
&= s \parallel t.
\end{aligned}
$$

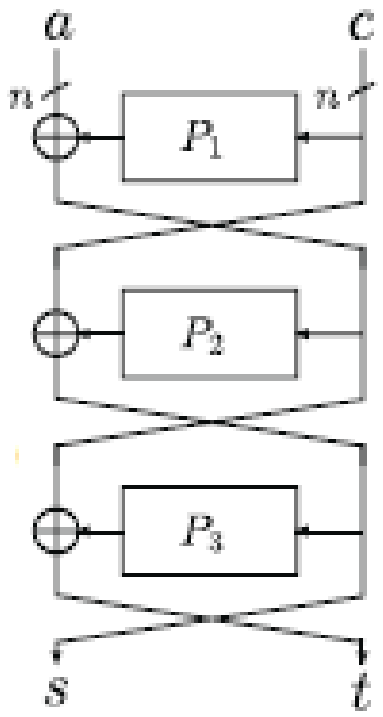


Fig. 1. The 3-round Feistel cipher with internal permutations, $\mathrm{FP}(a \parallel c) = s \parallel t$.

Let V be either the 3-round Feistel cipher with internal permutations (FP) or a random permutation (RP) on $\{0,1\}^{2n}$. Determine whether V is the FP or the RP by making queries to V. Notice that the query to the inverse mapping V^{-1} is not allowed.

Treger and Patarin [6] have shown that any classical algorithm requires $\Theta(2^{\frac{n}{2}})$ queries to determine it. Namely, FP is secure against any chosen plaintext attack that makes queries less than $\Theta(2^{\frac{n}{2}})$.

[6] J. Treger and J. Patarin, "Generic attacks on Feistel networks with internal permutations," Progress in Cryptology – AFRICACRYPT 2009, Lecture Notes in Computer Science, vol. 5580, pp. 41–59, 2009.

Let V be either the 3-round Feistel cipher with internal permutations (FP) or a random permutation (RP) on $\{0,1\}^{2n}$. Let U_V be a unitary operator for computing V, which is defined by

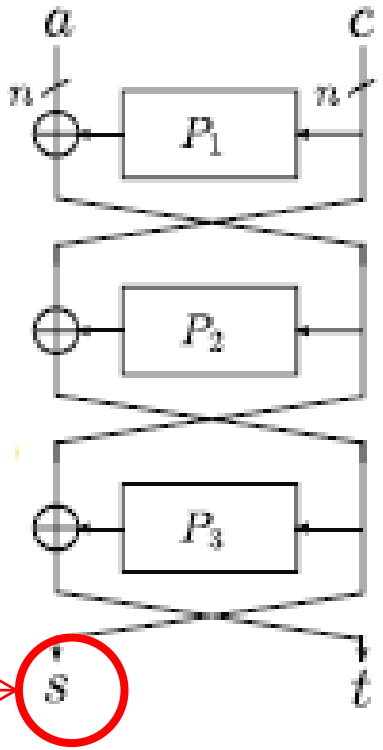
$$\mathrm{U}_V|x\rangle|y\rangle = |x\rangle|y \oplus V(x)\rangle,$$

where $x, y \in \{0,1\}^{2n}$. Determine whether V is the FP or the RP by making queries to U_V. The unitary operator for the inverse mapping V^{-1} is not given.

We previously showed that there was an exponential quantum algorithm for solving the problem with $O\left(2^{\frac{n}{4}}\right)$ queries [3].

[3] H. Kuwakado and M. Morii, "Quantum analysis of 2,3-round Feistel schemes," Proceedings of the 9th Asian Conference on Quantum Information Science, pp. 39–40, 2009.

$$
\begin{aligned}
\mathrm{FP}(x) &= \mathrm{FP}(a \parallel c) \\
&= c \oplus P_2(a \oplus P_1(c)) \\
&\quad \parallel (a \oplus P_1(c)) \oplus P_3(c \oplus P_2(a \oplus P_1(c))) \\
&= s \parallel t.
\end{aligned}
$$



Denote **W(x)=W(a||c)=s**

Fig. 1. The 3-round Feistel cipher with internal permutations, $\mathrm{FP}(a \parallel c) = s \parallel t$.

$$W(a\|c) = c \oplus P_2\left(a \oplus P_1(c)\right)$$

Let $\alpha, \beta \in \{0,1\}^n, \alpha \neq \beta, \quad b \in \{0,1\}$

Let $$f(b\|a) = \begin{Bmatrix} W(a\|\alpha) \oplus \beta & if\ \ b = 0 \\ W(a\|\beta) \oplus \alpha & if\ \ b = 1 \end{Bmatrix}$$

Then $f(b\|a) = f(b'\|a')$ *iff* $(b'\|a') \oplus (b\|a) = (1\|z)$

where $z = P_1(\alpha) \oplus P_1(\beta)$

So $$f\left(b\|a\right)=\ f\left(b'\|a'\right)\ \ iff\ \ \left(b'\|a'\right)\oplus\left(b\|a\right)=\left(1\|z\right)$$

where $$z=P_1\left(\alpha\right)\oplus P_1\left(\beta\right)$$

(N.B. the “only if” part is critical)

In other words, if W is based on the 3-round Feistel cipher, the derived function f will have the above property.

Simon’s algorithm will randomly sample vectors orthogonal to (1||z).

In other words, if W is based on the 3-round Feistel cipher, the derived function f will have the above property, and Simon's algorithm will randomly sample vectors orthogonal to (1||z).

However, if W is based on a random permutation, no such pattern is likely to emerge.

Thus, a quantum algorithm can efficiently distinguish a 3-round Feistel cipher with internal permutations from a random permutation.

Breaking Symmetric Cryptosystems using Quantum Period Finding

Marc Kaplan[1,2], Gaëtan Leurent[3] Anthony Leverrier[3], and María Naya-Plasencia[3]

[1] LTCI, Télécom ParisTech, 23 avenue dItalie, 75214 Paris CEDEX 13, France
[2] School of Informatics, University of Edinburgh,
10 Crichton Street, Edinburgh EH8 9AB, UK
[3] Inria Paris, France

arXiv:1602.05973v2 [quant-ph] 29 Mar 2016

We obtain attacks with very strong implications. First, we show that the most widely used modes of operation for authentication and authenticated encryption (*e.g.* CBC-MAC, PMAC, GMAC, GCM, and OCB) are completely broken in this security model. Our attacks are also applicable to many CAESAR candidates: CLOC, AEZ, COPA, OTR, POET, OMD, and Minalpher. This is quite surprising compared to the situation with encryption modes: Anand *et al.* show that standard modes are secure when using a quantum-secure PRF.
Second, we show that slide attacks can also be sped up using Simon's algorithm. This is the first exponential speed up of a classical symmetric cryptanalysis technique in the quantum model.

Generalization of Simon's problem, order-finding and DLP: "Hidden subgroup problem"

- A unifying framework was developed for these problems

$$f : G \to X$$

$$f(x) = f(y) \quad \text{iff} \quad x + S = y + S$$

for some $S \leq G$

- If G is Abelian, finitely generated, and represented in a reasonable way, we can efficiently find S.

Order finding (basis of quantum factoring):

$G = Z$ X any group

$f(x) = a^x$

$K = rZ$

(applies more generally to finding the period of any periodic function f)

Discrete Log of $b = a^k$ to base a :

$$G = Z_r \times Z_r \qquad X \quad \text{any group}$$

$$f(x, y) = a^{\,x}\, b^{\,y}$$

$$K = \langle (k, -1) \rangle$$

Hidden Linear Forms (Boneh+Lipton)

Self-shift equivalences (Grigoriev):

$$G = GF(q)^n \qquad X = GF(q)[X_1, X_2, ..., X_n]$$

$$f(a_1, a_2, ..., a_n) = P(X_1 - a_1, ..., X_n - a_n)$$

$$K = \{(a_1, ..., a_n) : P(X_1 - a_1, ..., X_n - a_n) = P(X_1, ..., X_n)\}$$

Abelian Stabilizer Problem (Kitaev)

Decomposing Abelian groups

- Any finite Abelian group G is the direct sum of finite cyclic groups

$$\langle g_1 \rangle \oplus \langle g_2 \rangle \oplus \quad \cdot \oplus \langle g_n \rangle$$

But finding generators $g_1, g_2, \quad , g_n$ satisfying $G = \langle g_1 \rangle \oplus \langle g_2 \rangle \oplus \quad \cdot \oplus \langle g_n \rangle$ is not always easy, e.g. for $e.g. \quad G = Z_N^*$ it's as hard as factoring N

- Given any polynomial sized set of generators, we can use the Abelian HSP algorithm to find new generators that decompose G into a direct sum of finite cyclic groups. http://arxiv.org/abs/cs/0101004

- Leads directly to an algorithm for computing the class group and class number of a quadratic number field [Watrous ‘00] (computing the class group of a more general number field is a much more difficult task).
- Decomposition of Abelian groups was also applied by
    - •Friedl, Ivanyos and Santha [FIS05] to test if a finite set with a binary operation is an Abelian group,
    - •Kedlaya [Ked06] to compute the zeta function of a genus *g* curve over a finite field F*q* in time polynomial in *g* and *q*, and
    - •Childs, Jao and Soukharev [CJS10] in order to construct elliptic curve isogenies in subexponential time.

What about non-Abelian HSP?

- Consider the symmetric group $G = S_n$
- S_n is the set of permutations of n elements
- Let G be an n-vertex graph
- Let $X_G = \{\pi(G) \mid \pi \in S_n\}$

Define $f_G : S_n \to X_G \qquad f_G(\pi) = \pi(G)$

hen

$$f_G(\pi_1) = f_G(\pi_2) \Leftrightarrow \pi_1 K = \pi_2 K$$

where

$$K = AUT(G) = \{\pi \mid \pi(G) = G\}$$

- So the hidden subgroup of f_G is the automorphism group of G

Dihedral Hidden Subgroup Problem

$$f : D_n \to X$$

$$f(b, x) = f(b', x') \Leftrightarrow (b - b', x - x') \in \{(0,0), (1, s)\}$$

- A quantum computer can easily compute states of the form ("coset states") for random x:

$$|0, x\rangle + |1, x + s \bmod n\rangle$$

- This can be easily converted to a state of the form (for random known k):

$$|0\rangle + e^{2\pi i k s / n}|1\rangle$$

Dihedral Hidden Subgroup Problem

- It is easy to find S given

$$|0\rangle + e^{2\pi i s/n}|1\rangle$$

$$|0\rangle + e^{2\pi i 2s/n}|1\rangle$$

$$|0\rangle + e^{2\pi i 4s/n}|1\rangle$$

$$|0\rangle + {}^{2\pi i 8s/n}|1\rangle$$

- Kuperberg's **sieving** method constructs these states from

$$e^{O\left(\sqrt{n}\right)}$$

samples of

$$|0\rangle + e^{2\pi i k s/n}|1\rangle$$

with random k.

Dihedral Hidden Subgroup Problem

- It is easy to find s given

$$|0\rangle + e^{2\pi i s/n}|1\rangle$$

$$|0\rangle + e^{2\pi i 2s/n}|1\rangle$$

$$|0\rangle + e^{2\pi i 4s/n}|1\rangle$$

$$|0\rangle + {}^{2\pi i 8s/n}|1\rangle$$

- Solving **average-case subset sum** suffices (Regev)

Applications of Dihedral Hidden Subgroup Algorithm

- Regev:

THEOREM 1.1. *If there exists a solution to the dihedral coset problem with failure parameter* f *then there exists a quantum algorithm that solves the* $\Theta(n^{\frac{1}{2}+2\mathsf{f}})$*-unique-SVP.*

Applications of Dihedral Hidden Subgroup Algorithm

- Consider this approach to Diffie-Hellman-like key exchange:
- Group G acting on a set X $g \in G,\ g^n = 1,\ x \in X,\ a, b \in Z_{>0}$
- Alice sends Bob $g^a(x)$
- Bob send Alice $g^b(x)$
- They both compute the key $g^{a+b}(x) = g^{b+a}(x)$
- (Childs-Ivanyos) Can use sieving to find a,b in time $e^{O\left(\sqrt{n}\right)}$
- Childs-Ivanyos also find efficient algorithms for discrete logs in semi-groups

Non-Abelian HSP

- Tools include non-Abelian QFT, “pretty good” measurements, “sieving”, and non-trivial reductions to Abelian HSP in some cases.

Generalizations of Abelian HSP

- Finding Hidden Shifts and Translations
- Can generalize to finding hidden “non-linear” structures. E.g. hidden radius problem, shifted subset problem, hidden polynomial problem
- Estimating “Gauss sums”
- Etc.

Generalizations of Abelian HSP

- Can view HSP has a hidden sub-lattice problem for $Z \otimes Z \otimes \quad \otimes Z = Z^n$.

  One way to generalize the problem, is to find a hidden sub-lattice of $R \otimes R \otimes \quad \cdot \otimes R = R^n$.

  Need to define appropriate ways for specifying/approximating inputs and outputs.

  Applications include solving Pell's equation, Principal Ideal Problem, and finding the unit group of a number field.

QUANTUM SEARCHING



Searching problem

Consider

$$f : \{0,1\}^n \rightarrow \{0,1\}$$

Given

$$U_f : |x\rangle|0\rangle \quad \cdot |x\rangle|f(x)\rangle$$

Find an x satisfying $f(x) = 1$

Application

Consider a 3-SAT formula

$$\Phi = C_1 \wedge C_2 \wedge \cdots \wedge C_M$$

$$C_j = (y_{j,1} \vee y_{j,2} \vee y_{j,2})$$

$$y_{j,k} \in \{x_1, x_2, \quad , x_n, \overline{x}_1, \overline{x}_2, \quad , \overline{x}_n\}$$

For a given assignment $\mathrm{x} = \mathrm{x}_1 \mathrm{x}_2 \quad \mathrm{x}_n$

$$f_\Phi(\mathrm{x}) = \begin{cases} 1 & \text{if } \mathbf{x} \text{ satisfies } \Phi \\ 0 & \text{otherwise} \end{cases}$$

Running times

Suppose there are t solutions to $f(x)=1$

Can find a solution to $f(x)=1$ using $O\left(\sqrt{\frac{2^n}{t}}\right)$ applications of U_f and $\tilde{O}\left(\sqrt{\frac{2^n}{t}}\right)$ other operations (without knowing t).

Parallelizing Brute-Force Search

Given M parallel quantum processors, finding an n-bit key requires time (measured in terms of function evaluations):

http://arxiv.org/abs/quant-ph/9711070

$$\Theta\left(\sqrt{\frac{2^n}{M}}\right)$$

e.g. Depth of parallel quantum attacks on AES-128 (in terms of function evaluations):

	Classical running time (1 processor)	**Classical running time (2^{40} processors)**	**Quantum running time (1 processor)**	**Quantum running time (2^{40} processors)**
AES-128	2^{128}	2^{88}	2^{64}	2^{44}

Des. Codes Cryptogr. (2015) 77:375–400
DOI 10.1007/s10623-015-0067-5

Finding shortest lattice vectors faster using quantum search

Thijs Laarhoven[1] · **Michele Mosca**[2,3,4] · **Joop van de Pol**[5]

Received: 15 October 2014 / Revised: 12 March 2015 / Accepted: 16 March 2015 /
Published online: 14 April 2015
© The Author(s) 2015. This article is published with open access at Springerlink.com

Abstract By applying a quantum search algorithm to various heuristic and provable sieve algorithms from the literature, we obtain improved asymptotic quantum results for solving the shortest vector problem on lattices. With quantum computers we can provably find a shortest vector in time $2^{1.799n+o(n)}$, improving upon the classical time complexities of $2^{2.465n+o(n)}$ of Pujol and Stehlé and the $2^{2n+o(n)}$ of Micciancio and Voulgaris, while heuristically we expect to find a shortest vector in time $2^{0.268n+o(n)}$, improving upon the classical time complexity of $2^{0.298n+o(n)}$ of Laarhoven and De Weger. These quantum complexities will be an important guide for the selection of parameters for post-quantum cryptosystems based on the hardness of the shortest vector problem.

Can be applied to speed up parts of complex classical algorithms, e.g. finding short vectors in a lattice.

On Quantum RAM

Some quantum algorithms require poly(n) computational qubits and $\exp(n^c)$ "quantumly accessible" classical bits.

What is the cost of $\exp(n^c)$ "quantumly accessible" classical bits compared to $\exp(n^c)$ computational qubits?

For superpolynomially many queries, it's not clear if there is much advantage. http://arxiv.org/abs/1502.03450

What is a qRAM?

- Quantum Random Access Memory; quantum equivalent of classical RAMs.
- A device with an array of memory cells, an input index register and an output register
- Queries memory addresses in superposition

- Value stored is either **classical** or quantum; we will focus on classical data here.

Applications of qRAM

- Grover's searching of unordered databases
- Collision finding and element-distinctness
- Dihedral hidden subgroup problems
- Linear equation solver (uses qRAM to prepare/input certain vectors)
- Generic cryptanalytic attacks
- Etc.

Generalization: Amplitude Amplification

Consider any algorithm A that successfully guesses a solution to

$f(x)=1$ with probability p

Quantum Amplitude Amplification finds a solution to $f(x)=1$

using $O\left(\frac{1}{\sqrt{p}}\right)$ (quantum) applications of A and of U_f

Analysis

Let S = cost of implementing A - “sampling” cost

Let C = cost of implementing U_f - “checking” cost

Let p = probability that a sample is a solution.

A classical search would have expected cost $\frac{1}{p}(S+C)$

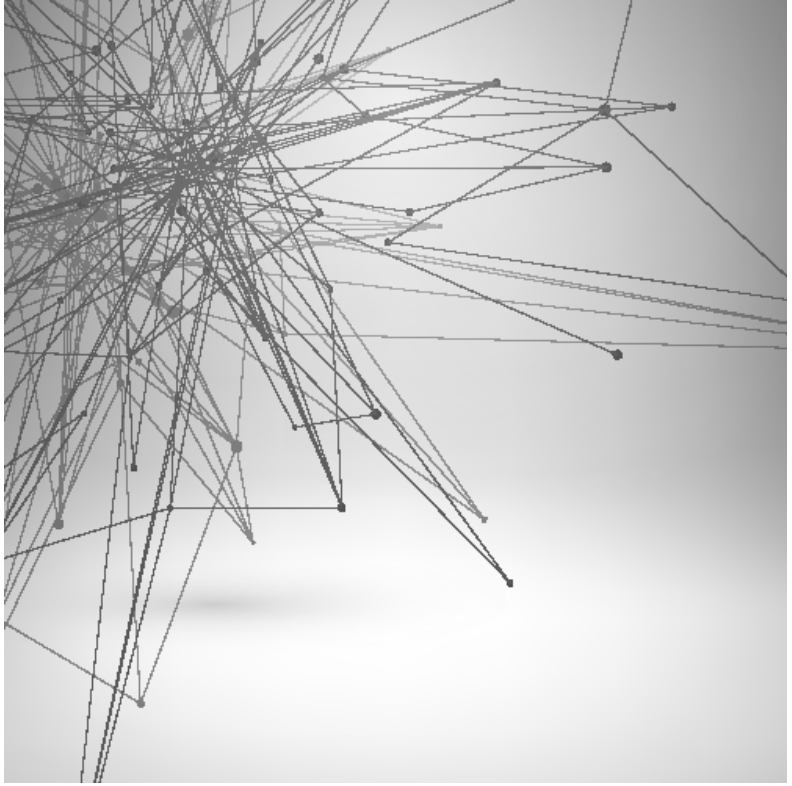
A quantum search would have expected cost $\frac{1}{\sqrt{p}}(S+C)$

Element Distinctness

- Consider $f : \{0,1\}^n \rightarrow X$
- Find $x \neq y$ such that $f(x) = f(y)$
- Classically (in the worst case) this takes $O(N)$ evaluations of f

Element Distinctness

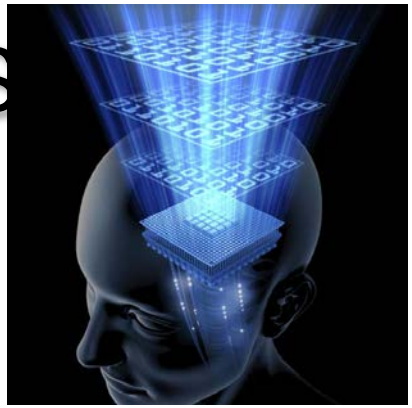
- Let A sample $\sqrt{N}$ random elements $f\left(x_j\right)$
- Thus $p \approx \frac{1}{\sqrt{N}}$
- Checking if any of the samples are not distinct over the range of f can be done in time $\tilde{O}\left(\sqrt{N}\right)$
- Thus $\frac{1}{\sqrt{p}}\left(S+C\right) \in \tilde{O}\left(N^{3/4}\right)$



Walk-based Quantum Searching

(will be covered later this week by another speaker)

Other algorithms and algorithic paradigms



Hamiltonian simulation

Under appropriate conditions we can efficiently approximate some properties of $e^{iHt}\left|\phi\right\rangle$

One application, in combination with eigenvalue estimation and other tools, is to determine some properties of the solution to ("well-conditioned") **sparse linear equations** (by Harrow, Hassidim and Lloyd (HHL), 2008).

Useful for cryptanalysis??

Quantum Algorithm for Optimization and Polynomial System Solving over Finite Field and Application to Cryptanalysis*

Yu-Ao Chen[1,2], Xiao-Shan Gao[1,2], Chun-Ming Yuan[1,2]
[1]KLMM, Academy of Mathematics and Systems Science
Chinese Academy of Sciences, Beijing 100190, China
[2]University of Chinese Academy of Sciences, Beijing 100049, China
Email: xgao@mmrc.iss.ac.cn

And more…

- Adiabatic algorithms
- Topological algorithms
- Span programs
- Etc.

http://quantumalgorithmzoo.org/ *(maintained by S. Jordan)*