Shor and Grover Algorithm and Quantum Key Distribution

Hao Chung

National Taiwan University

r05921076@ntu.edu.tw

December 20, 2016

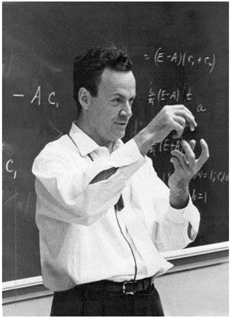
Overview

1. Introduction to Quantum Computing
2. Shor's Algorithm
3. Grover Search Algorithm
4. Quantum Key Distribution
5. Recent Progress on Quantum Computer

Outline

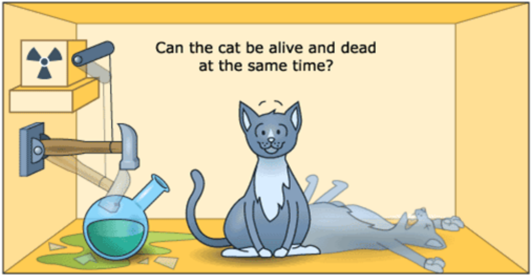
The beginning of quantum computing

- Simulating physics with computers
  - In 1982, Feynman proposed the idea of creating machines based on the laws of quantum mechanics instead of the laws of classical physics
- Why quantum can do better than classical?
  - Superposition
  - Entanglement



Superposition

- A quantum state can be in many possibilities “simultaneously” before measurement.
- Shrodingers cat

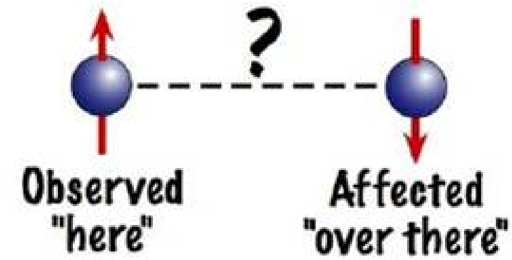


Superposition

- Classical state: probabilistic distribution is due to our ignorance.
- Quantum state: uncertainty is due to the essence or Nature.

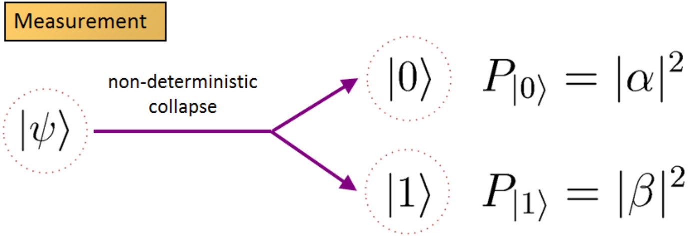
Entanglement

- Two physical objects have some correlation such that measuring one of them will affect the other.



Measurement

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$



$$|\psi\rangle = \alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle$$

$$\Rightarrow |\alpha|^2 + |\beta|^2 + |\gamma|^2 + |\delta|^2 = 1$$

Mathematical Structure

- Postulate 1: A quantum system is described a unit vector in the Hilbert space.
  - Hilbert space $\equiv$ an inner product space on $\mathbb{C}$
- Dirac notation: $\binom{1}{0} = |0\rangle, \binom{0}{1} = |1\rangle$
- Postulate 2: Quantum operation is described by a unitary operator U.
  - Unitary operator is an operator satisfies $UU^{\dagger} = I$, where † denotes the conjugate-transpose.

Universal Set

A set of unitary operators is called universal set if all the unitary operator can be made up of the members of the set.

Theorem (Universal Set)

$\{X, Z, H, T, CNOT\}$ forms an universal set.

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

$$T = \begin{pmatrix} 1 & 0 \\ 0 & e^{\frac{i\pi}{4}} \end{pmatrix}, CNOT = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

Quantum Parallel

A single quantum computer can compute multiple computations simultaneously by the effect of superposition.

- $$U_f(|x\rangle\,|0\rangle) = |x\rangle\,|f(x)\rangle$$
  $$|\psi\rangle = \sum_{x=0}^{2^n-1} |x\rangle\,|0\rangle$$
  $$U_f\,|\psi\rangle = \sum_{x=0}^{2^n-1} |x\rangle\,|f(x)\rangle$$

The problem is we only can find out one of the result from measurement.

- The Nature knows all the result but only tells us one!

Quantum Parallel

Example (Modular Exponential)

Let $f_{a,N}(x) = a^x \, mod \, N$, and U_f is an unitary operator corresponding to $f_{a,N}$.
Now we have $a = 7, N = 15$ and $|\psi\rangle = \frac{1}{2}(|0\rangle + |1\rangle + |2\rangle + |3\rangle)$.
Then,
$U_f(|\psi\rangle\,|0\rangle) = \frac{1}{2}(|0\rangle\,|1\rangle + |1\rangle\,|7\rangle + |2\rangle\,|4\rangle + |3\rangle\,|13\rangle)$.

The example shows that we somehow can compute $7^0, 7^1, 7^2, 7^3 \, (mod \, 15)$ simultaneously. The problem is "how we extract the answer?"

In the following slides, we will see that how different quantum algorithms deal with this problem.

Outline

Shor's Algorithm

Shor's algorithm has two parts:

- Classical part: reduce factoring to order-finding problem
- Quantum part: order-finding problem

Order-finding problem

For $a \in \mathbb{Z}_N^*$, the order of a in $\mathbb{Z}_N^*$ (or the order of a modulo N) is the smallest positive integer r such that

$$a^r \equiv 1\,(mod\; N).$$

The order-finding problem is given a positive integer $N \geq 2$ and an element $a \in Z_N^*$, try to find the order of a in Z_N^*.

Reduce Factoring to Order-finding Problem

If we have

$$a^r \equiv 1\,(mod\,N),$$

then

$$N \mid a^r - 1.$$

If r is even, we have

$$N \mid (a^{r/2} - 1)(a^{r/2} + 1).$$

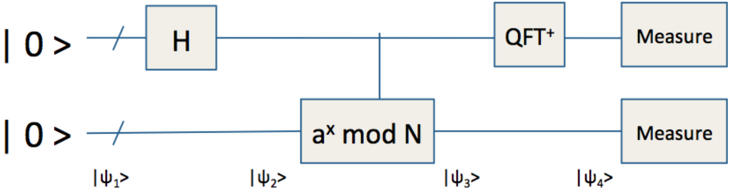
It cannot happen that $N \mid (a^{r/2} - 1)$, because this would mean that r was not the order of a. If $N \not| (a^{r/2} + 1)$, then $gcd(N, a^{r/2} + 1)$ is a non-trivial factor for N.

Theorem

If a is chosen randomly from Z_N^*, and r is the order of a, then

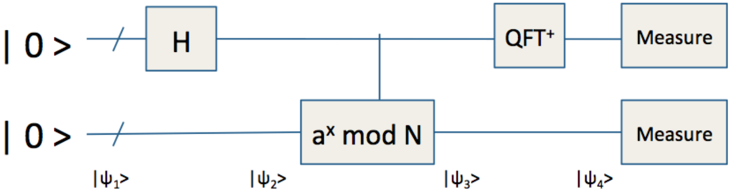
$$Pr[r \text{ is even} \wedge N \not| (a^{r/2} + 1)] \geq \frac{1}{2}.$$

Order-finding Problem



$|\psi_1\rangle = |0\rangle\,|0\rangle$
$|\psi_2\rangle = \sum_{x=0}^{2^n-1} |x\rangle\,|0\rangle$
$|\psi_3\rangle = \sum_{x=0}^{2^n-1} |x\rangle\,|a^x \text{mod N}\rangle$
$|\psi_4\rangle = \sum_{x=0}^{2^n-1} QFT^{\dagger}(|x\rangle)\,|a^x \text{mod N}\rangle$

- $QFT^{\dagger}(|x\rangle) = \sum_{t=0}^{N} e^{ixt/N}\,|t\rangle$



When measuring the second register and get some value "u", the first register will collapse to the pre-image of u, i.e. $\{i \,|\, f(i) = u\}$. Since modular exponential is a periodic function, where the period is the order of a.

We can find the period by Fourier transform.

Remark: the probability that the circuit output an even order of a is $\Omega(\frac{1}{\log \log N})$.

Algorithm

Algorithm 1 Shor's Algorithm

Require: Input: an odd, composite integer N that is not a prime power
Ensure: Output: a non-trivial factor of N

```
repeat
    randomly choose a ∈ {2, ⋯ , N − 1}
    compute gcd(a, N) = d
    if d ≥ 2 then
        return d
    else
        run the circuit to find r
        compute d = gcd(a^{r/2} − 1, N)
        return d if d ≥ 2
    end if
until find the order successfully
```

Example

Example

Assume we want to factor 15. We choose $a = 7$. The first step is to prepare a superposition state

$$|\psi\rangle = \frac{1}{4}\sum_{x=0}^{15} |x\rangle\,|0\rangle\,.$$

Next, compute the modular exponential and yield

$$|\psi'\rangle = \tfrac{1}{4}(|0\rangle\,|1\rangle + |1\rangle\,|7\rangle + \ldots + |15\rangle\,|13\rangle)$$
$$= \tfrac{1}{4}\big((|0\rangle + |4\rangle + |8\rangle + |12\rangle)\,|1\rangle$$
$$+(|1\rangle + |5\rangle + |9\rangle + |13\rangle)\,|7\rangle$$
$$+(|2\rangle + |6\rangle + |10\rangle + |14\rangle)\,|4\rangle$$
$$+(|3\rangle + |7\rangle + |11\rangle + |15\rangle)\,|13\rangle\,\big)$$

Example

Example (con'd)

The quantum Fourier transform yields

$$\frac{1}{4}\big((|0\rangle + |4\rangle + |8\rangle + |12\rangle)\,|1\rangle$$
$$+(|0\rangle + i\,|4\rangle - |8\rangle - i\,|12\rangle)\,|7\rangle$$
$$+(|0\rangle - |4\rangle + |8\rangle - |12\rangle)\,|4\rangle$$
$$+(|0\rangle - i\,|4\rangle - |8\rangle + i\,|12\rangle)\,|13\rangle\,\big)$$

When measuring the first register, we can get the even order with probability $\Omega(\frac{1}{\log\log 15})$.

Time Complexity

Assume we want to factor a n-bit number N:

- Modular exponential: $\Theta(n^3)$
- QFT: $\Theta(n^2)$
- Succeed probability: $\Omega(\frac{1}{\log n})$

Thus, the total time complexity is $O(n^3 \log n)$.

Example

To factor a 2048-bit number, we need roughly $2048^3 \cdot \log 2048 \sim 10^{11}$ operations. If we assume each operation takes 1 microsecond on a quantum computer, it takes only one day to factor the number.

Outline

Motivation of Grover Search Algorithm

Envelope Problem: Suppose you have N envelopes. One of them has money inside but others are empty. How many trials do you need to do for finding money?

- Worst case: $N-1$ times.
- In average: $N/2$ times.
- Even you allow the probability of failure P_f (a constant), you still need to try $O(N)$ times.

Grover suggests an algorithm for such problem only takes $O(\sqrt{N})$ operations.

Grover Algorithm

One important design technique for quantum algorithm is preparing a superposed state that exploits quantum parallelism and try to maximize the amplitude of the right answer.

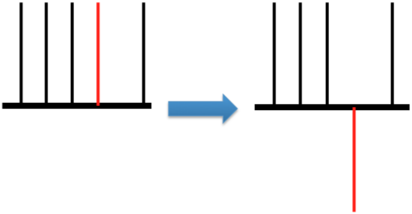
Grover algorithm is a beautiful example for demonstrating this technique. One Grover iteration consists of two steps:

1. Phase inversion
2. Inversion about mean

After many iterations, we can get the result with high probability.

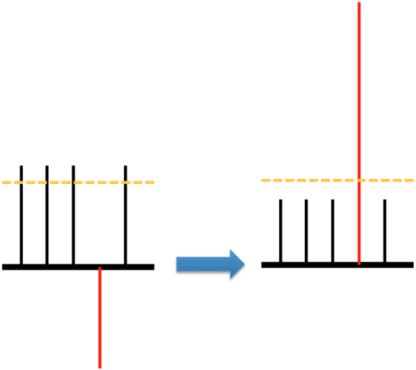
Phase inversion

- First, we prepare a superposed state $|\psi\rangle = \sum_{x=0}^{N} \frac{1}{\sqrt{N}} |x\rangle$
- Assume the red one is the right answer we want to obverse
- Second, we inverse the amplitude of the right answer, i.e. $\frac{1}{\sqrt{N}} |x\rangle \to -\frac{1}{\sqrt{N}} |x\rangle$



Inversion about mean

- Orange dotted line represents the average of all the amplitude
- Since the red one has negative amplitude, the average will slightly lower than most amplitude.
- If we inverse each amplitude about the mean, the amplitude of the right answer will grow about three times high.



Phase Inversion

Assume we have a classical boolean function $f(x)$ such that

$$f(x) = \begin{cases} 1, & \text{if } x \text{ is the answer we want} \\ 0, & \text{otherwise} \end{cases}$$

Let U_f be an unitary operator such that

$$U_f \left|x\right\rangle \left|q\right\rangle = \left|x\right\rangle \left|q \oplus f(x)\right\rangle,$$

which can be viewed as applying NOT gate on the desired state.

Magically, if we set $\left|q\right\rangle = \frac{\left|0\right\rangle - \left|1\right\rangle}{2}$, we would have

$$U_f \left|x\right\rangle \left|q\right\rangle = \left|x\right\rangle \frac{\left|1\right\rangle - \left|0\right\rangle}{2} = -\left|x\right\rangle \left|q\right\rangle,$$

which is the phase inversion we want.

Inversion about Mean

Q: If μ is the average, how can we inverse x about μ?
A: $(x-\mu)$ is the difference between them. $\mu-(x-\mu)=2\mu-x$ attains our goal.

Thus, in vector representation, inversion about mean can be done by

$$(2A-I)\left|x\right\rangle \text{,where } A=\begin{pmatrix} \frac{1}{2^n} & \frac{1}{2^n} & \cdots & \frac{1}{2^n} \\ \frac{1}{2^n} & \frac{1}{2^n} & \cdots & \frac{1}{2^n} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{1}{2^n} & \frac{1}{2^n} & \cdots & \frac{1}{2^n} \end{pmatrix}$$

Remark: It can be showed that $(2A-I)$ is an unitary operator:
Since $(2A-I)$ is a real symmetric matrix, $(2A-I)=(2A-I)^\dagger$.

$$(2A-I)(2A-I)=4A^2-4A+I=4A-4A+I=I$$

Example

Example (Grover iteration)

First, we prepare a superposed state and the red one is the amplitude we want to enhance.

$$|\psi_1\rangle = [\frac{1}{\sqrt{8}}, \frac{1}{\sqrt{8}}, \frac{1}{\sqrt{8}}, \frac{1}{\sqrt{8}}, \frac{1}{\sqrt{8}}, \frac{1}{\sqrt{8}}, \frac{1}{\sqrt{8}}, \frac{1}{\sqrt{8}}]$$

Then, we inverse the amplitude of the target.

$$|\psi_2\rangle = [\frac{1}{\sqrt{8}}, \frac{1}{\sqrt{8}}, \frac{1}{\sqrt{8}}, \frac{1}{\sqrt{8}}, \frac{1}{\sqrt{8}}, \frac{-1}{\sqrt{8}}, \frac{1}{\sqrt{8}}, \frac{1}{\sqrt{8}}]$$

The average of these numbers is $\frac{7\cdot\frac{1}{\sqrt{8}}-\frac{1}{\sqrt{8}}}{8} = \frac{3}{4\sqrt{8}}$. Calculating the inversion about hte mean, we have

$$|\psi_3\rangle = [\frac{1}{2\sqrt{8}}, \frac{1}{2\sqrt{8}}, \frac{1}{2\sqrt{8}}, \frac{1}{2\sqrt{8}}, \frac{1}{2\sqrt{8}}, \frac{5}{2\sqrt{8}}, \frac{1}{2\sqrt{8}}, \frac{1}{2\sqrt{8}}]$$

Example

Example (con'd)

If we do another Grover iteration, we get

$$|\psi_4\rangle = [\frac{-1}{4\sqrt{8}}, \frac{-1}{4\sqrt{8}}, \frac{-1}{4\sqrt{8}}, \frac{-1}{4\sqrt{8}}, \frac{-1}{4\sqrt{8}}, \frac{-1}{4\sqrt{8}}, \frac{11}{4\sqrt{8}}, \frac{-1}{4\sqrt{8}}, \frac{-1}{4\sqrt{8}}]$$

Note that $\frac{11}{4\sqrt{8}} = 0.97227$. The probability of getting right answer is

$$|\frac{11}{4\sqrt{8}}|^2 = 0.9453.$$

We can find the desired answer with probability 95% only using two iterations!

Complexity

All the gate can be constructed in $O(1)$ basic gate. Operate $O(\sqrt{N})$ can attend the maximum probability to get the right answer. Thus, the total time complexity is $O(\sqrt{N})$.

Note that $f(x)$ could be "any" boolean function that can be implemented in quantum circuit. Thus, if you have plaintext-ciphertext pair, Grover algorithm could leads to quadratic speed up.

Example (AES-128)

Assume we want to break AES-128.
If we have a plaintext-ciphertext pair (m, c), then we can have a function $f(x)$ such that output 1 when $c = Enc_x(m)$. About 2^{64} Grover iterations could find the correct key with high probability.

Outline

Quantum Key Distribution

- In 1984, Charles Bennett and Gilles Brassard proposed a practical quantum key distribution (QKD) protocol, a.k.a. BB84.
- QKD is not based on the mathematical problem but on the properties of quantum mechanics.

Structure of QKD

Let Alice and Bob be the two persons that they want to have a same shared secret key.

They have two channels:

- **Authenticated public channel:** A classical digital channel which the identities of two parties are authenticated, but all the information is public. That is, the adversary knows all the information on this channel.
- **Insecure quantum channel:** An optic fiber which could be eavesdropped or tempered by adversary.

Some Facts of Quantum Key Distribution

- There are two bases that Alice and Bob use in BB84: $\oplus$ and $\otimes$.

Basis	Binary 1	Binary 0
$\oplus$	$\lvert\updownarrow\rangle$ $\theta = 0^\circ$	$\lvert\leftrightarrow\rangle$ $\theta = 90^\circ$
$\otimes$	$\lvert\nearrow\rangle$ $\theta = 45^\circ$	$\lvert\nwarrow\rangle$ $\theta = 135^\circ$

- When Alice uses $\oplus$ basis, she can send either $\lvert\updownarrow\rangle$ or $\lvert\leftrightarrow\rangle$. When using $\otimes$ basis, she can send either $\lvert\nearrow\rangle$ or $\lvert\nwarrow\rangle$.

Some Facts of Quantum Key Distribution

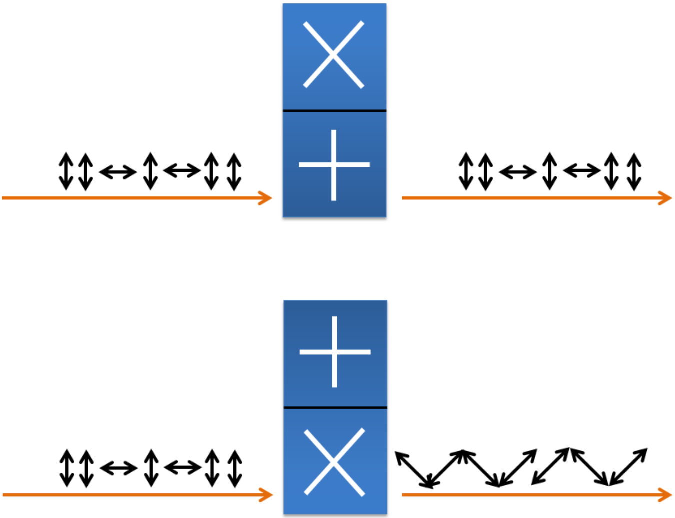
- If a $|\uparrow\rangle$ is measured under $\oplus$ basis, the result will be $|\uparrow\rangle$ with probability 100%. The same goes for $|\rightarrow\rangle$ under $\oplus$ and $|\nearrow\rangle$ or $|\nwarrow\rangle$ under $\otimes$.
- If a $|\nearrow\rangle$ is measured under $\oplus$ basis, the result will be $|\uparrow\rangle$ with probability 50% or $|\rightarrow\rangle$ with probability 50%. (Because a single photon could not split, it can only be one of the possibility.)

Mathematical representation

This can be considered as changing the basis,

where $\oplus$ uses $\left\{ \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right\}$ and $\otimes$ uses $\left\{ \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix}, \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{-1}{\sqrt{2}} \end{pmatrix} \right\}$.

Some Facts of Quantum Key Distribution



Some Facts of Quantum Key Distribution

The properties of quantum mechanics:

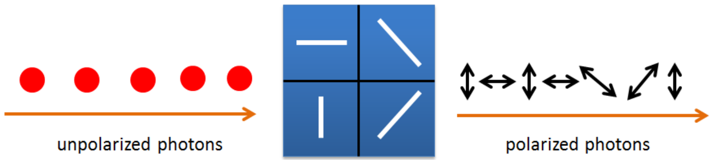
- No-cloning theorem: the quantum data could not be copied.
- Measurement: one could not measure a quantum state without changing the state.

Thus,

- The eavesdropper must resend a new photon after measuring the old one.
- The eavesdropper must “guess” the basis.

Step 1: Sending Polarized Photons

- Alice sends polarized photons. Each photon polarizes at one of the four possibilities randomly.
- Alice doesnt tell anyone including Bob what basis that she chooses.



Step 2: Measuring and Recording

- Bob measures the photons using a random choice of two bases and records the results.
- In average, half of the photons will be measured by wrong basis.

Step 3: Checking the Basis

- Bob tells Alice which basis he applied for each photons in public channel.
- Alice tells Bob which photons are measured correctly. Those photons are called "sifted photons" and other photons are aborted.

Step 4: Error Analysis

- Bob transmits some of the “sifted photons” to Alice.
- Alice does the error analysis:
  - If the channel is reliable, all the measured results should be the same.
  - If the channel is eavesdropped, there are 25% measured results are inconsistent.
    - The eavesdropper has 50% possibility to guess the wrong basis. For each wrong basis, Bob has 50% possibility to measure the wrong result.
- The sifted photons that are not used for error analysis are the shared secret key.

Summary

A's data	1	0	0	1	1	1	0	0	1	0	0	1
A's basis	$\oplus$	$\otimes$	$\oplus$	$\otimes$	$\otimes$	$\oplus$	$\oplus$	$\otimes$	$\oplus$	$\otimes$	$\otimes$	$\oplus$
θ ($^\circ$)	0	135	90	45	45	0	90	135	0	135	135	0
B's basis	$\otimes$	$\otimes$	$\oplus$	$\oplus$	$\otimes$	$\oplus$	$\otimes$	$\oplus$	$\oplus$	$\otimes$	$\oplus$	$\otimes$
B's result	1	0	0	0	1	1	0	1	1	0	1	1
Same basis ?	n	y	y	n	y	y	n	n	y	y	n	n
Sifted bits		0	0		1	1			1	0		
Data check ?		y	n		y	n			y	n		
Private key			0			1				0		

Information Reconciliation and Privacy Amplification

Information Reconciliation is a form of error correction carried out between Alice and Bob's keys, in order to ensure both keys are identical.

- Alice sends the syndrome of her key to Bob via public channel. This step will leak some information to Eve.
- Bob can correct his key by this syndrome and get a same key as Alice's with high probability.

Privacy amplification is a method for reducing (and effectively eliminating) Eve's partial information about Alice and Bob's key.

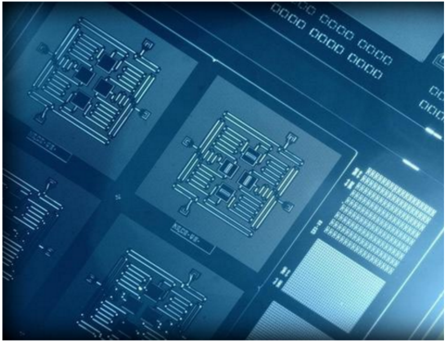
- Assume Alice and Bob share a weak secret X.
- Alice chooses a random seed Y and sends it to Bob via public channel.
- Alice and Bob can have a strong secret X' from seeded randomness extractor.

Outline

5-qubit vs 2000-qubit?

By Agam Shah | Follow

U.S. Correspondent, IDG News Service | May 4, 2016 4:42 AM PT



IBM's 5-qubit processor is accessible to the public via the cloud. Credit: IBM

SEP 27, 2016

D–Wave Systems Previews 2000–Qubit Quantum System

Comparison between Different Implementation