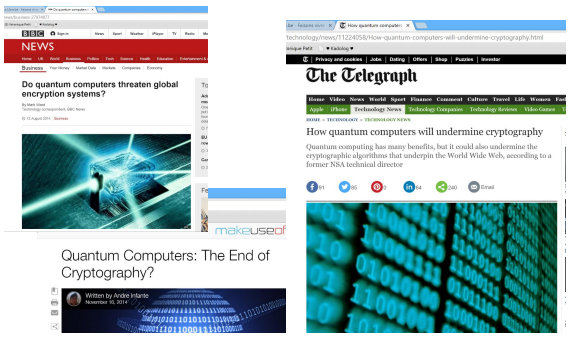
Advanced Cryptography

Quantum Algorithms

Christophe Petit

University of Oxford

The threat of quantum computers



The threat of quantum computers

- Quantum computers solve discrete logarithms & factoring
- Hence they break SSH, TLS , . . .
- Not known : security of lattice problems, polynomial systems solving, word problem, etc
- Not known : hardness of NP-hard problems
- Not known : can (large) quantum computers be built ?

Quantum key exchange

- Use quantum physics properties to realize key distribution with the ability to detect potential eavesdropping

Outline

Quantum computation model

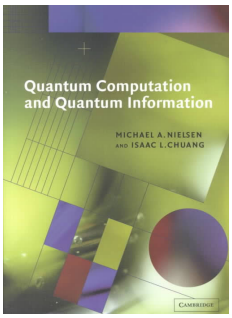
Simon's algorithm

Grover's search algorithm

Factorization and discrete logarithms

Quantum Key Exchange

Main reference



Credits

- Pictures are from original papers from Grover, Simon and Schor, Wikipedia or Google image

Outline

Quantum computation model

Simon's algorithm

Grover's search algorithm

Factorization and discrete logarithms

Quantum Key Exchange

qbits

- A classical bit can have value/*state* at either 0 or 1
- A quantum bit, or q-bit, is a *superposition* of these states

$$b = \alpha \cdot |0\rangle + \beta \cdot |1\rangle$$

where $\alpha, \beta \in \mathbb{C}$ are coefficients such that $|\alpha|^2 + |\beta|^2 = 1$

- A q-bit is in a *pure state* if all coefficients but one are 0
- Generalization to n qbits is $x = \sum_{i \in \{0,\dots,2^n-1\}} \alpha_i \cdot |i\rangle$ where i is written in binary and $\sum |\alpha_i|^2 = 1$
- Other notation : $x = (\alpha_0, \alpha_1, \dots, \alpha_{2^n-1})$
- Coefficients sometimes written up to a scaling factor

Measurements

- A *measurement* is an operator on superposition states, returning pure states
- Measurements are performed with respect to a particular basis, for example the *computational basis* $\{|i\rangle\}$
- If $x = \sum_{i \in \{0,\dots,2^n-1\}} \alpha_i \cdot |i\rangle$ then the probability to measure $|i\rangle$ in the computational basis is $|\alpha_i|^2$
- Measuring a qbit x is a non reversible operation, which actually modifies its value to the measured state
- We also say that the qbit *collapses* to a pure state

Reversible computation

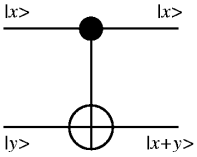
- Quantum computers only perform *reversible* operations
  - Any reversible function on n bits corresponds to a permutation on $\{0, \dots, 2^n - 1\}$
  - Any reversible function on n qbits corresponds to a unitary matrix U of dimension 2^n sending $\alpha = (\alpha_0, \dots, \alpha_{2^n-1})$ to β such that $\beta' = U\alpha'$
- Any classical function can be made reversible with the help of *ancilla bits* :
  - Replace $x \to f(x)$ by $(x, 0) \to (x, f(x))$

Remarks

- For a classical bit, information $\sim$ bit value
- A qbit is always a superposition of all possible values
- Information within *coefficients*, as in fact for classical bits if you write $b = \alpha_0|0\rangle + \alpha_1|1\rangle$ with $\alpha_i \in \{0, 1\}$
- Superpositions of states looks like parallel computing
- Still, cannot use that as such for brute force key search as only pure states are returned
- Quantum algorithms build a superposition of states such that *coefficients* associated to correct outputs are much bigger than others

Quantum circuits and CNOT gates

- Useful to focus on a small number of small/*local* gates, and build arbitrary circuits from there
- CNOT : controlled NOT gate

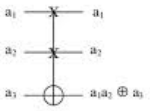


$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

Phase shifts and Toffoli gates

- Relative phase shift on a single qbit $\begin{pmatrix} e^{i\theta} & 0 \\ 0 & 1 \end{pmatrix}$
- Toffoli : doubly controlled NOT

T_3 = CC-NOT	⟨000⟩	...					⟨110⟩	⟨111⟩
⟨000⟩	1	0	0	0	0	0	0	0
⟨001⟩	0	1	0	0	0	0	0	0
⟨010⟩	0	0	1	0	0	0	0	0
⟨011⟩	0	0	0	1	0	0	0	0
⟨100⟩	0	0	0	0	1	0	0	0
⟨101⟩	0	0	0	0	0	1	0	0
⟨110⟩	0	0	0	0	0	0	0	1
⟨111⟩	0	0	0	0	0	0	1	0



- Toffoli gates are universal : can build any logical circuit

Hadamard gates

- Hadamard gate on one qbit

$$H_1 = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

- Parallel application on n qbits gives H_n such that

$$H_n = \frac{1}{\sqrt{2}} \begin{pmatrix} H_{n-1} & H_{n-1} \\ H_{n-1} & -H_{n-1} \end{pmatrix}$$

- (Remark : the matrix for parallel transformations is the tensor product of individual transformations)
- The n-bit pure state $|i\rangle$ is transformed into $\sum(-1)^{i.j}|j\rangle$ where $i \cdot j$ is the scalar product on the n-bit vectors i and j

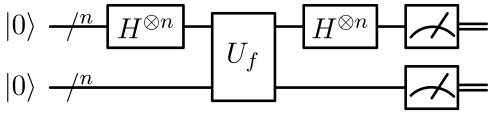
Outline

Simon's problem

- Given : oracle access to a function $f : \{0,1\}^n \to \{0,1\}^n$
- Promise : $\exists s \in \{0,1\}^n$ such that for all $y, z \in \{0,1\}^n$ we have $f(y) = f(z)$ if and only if $y = z \oplus s$ or $y = z$ (possibly $s = 0$ in which case f is bijective)
- We want to compute s
- Best classical algorithm needs $\Omega(2^{n/2})$: random trials until a collision is found

Simon's algorithm

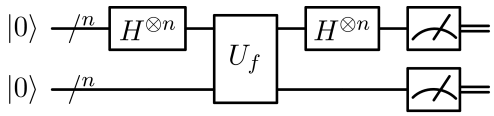
- Perform the following experiment



Here $U_f|x_1\rangle|x_2\rangle = |x_1 \oplus x_2\rangle|f(x_1)\rangle$

- Output $|y\rangle|f(x)\rangle$ implies that $y \cdot s = 0$ (see next slide)
- Repeating $O(n)$ times gives enough information to recover s with linear algebra over $\mathbb{F}_2$

Simon's algorithm



- After first Hadamard transform we have $\sum_x |x\rangle|0\rangle$
- After oracle we have $\sum_x |x\rangle|f(x)\rangle$
- After second Hadamard transform we have $\sum_{x,y}(-1)^{x\cdot y}|y\rangle|f(x)\rangle$
- Observe a particular couple $(y, f(x))$ with probability proportional to $\left|(-1)^{x\cdot y} + (-1)^{(x+s)\cdot y}\right|^2$

Remarks

- Can relax the promise somewhat : allow some collisions $f(y) = f(z)$ for $z \neq y, y \oplus s$
- See *Breaking Symmetric Cryptosystems using Quantum Period Finding* for some cool crypto applications

Outline

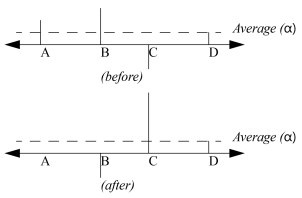
The search problem

- Given a function $C : \{1, \ldots, N\} \rightarrow \{0, 1\}$ such that $C(x) = 1$ for exactly one value x, compute this value
- Classically, given only black box access to C : $N/2$ random trials succeed with probability at least $1/2$

Grover's algorithm

- Initialize n-qbit register with uniform superposition $\sum_i |i\rangle$ using Hadamard transform (here we assume $N = 2^n$)
- Repeat the following unitary operations $O(\sqrt{N})$ times
  - Phase shift : if $C(S) = 1$ then phase shift by π, otherwise do nothing
  - Inversion about average : apply $D = -I + 2P$, where $P_{ij} = \frac{1}{N}$
- Measure the register
- Return the value measured

Inversion about average



- P such that $P_{ij} = \frac{1}{N}$ is averaging operator
- $Dv = Pv - (v - Pv)$
- $D = H_n R H_n$ where
  - $R_{ij} = 0$ if $i \neq j$,
  - $R_{ii} = -1$ if $i \neq 0$,
  - $R_{00} = 1$

Intuition

- Start from uniform superposition with coefficients $2^{-n/2}$
- All coefficients remain real values
- After first phase shift, all coefficients have norm $2^{-n/2}$, all coefficients but one are positive
- First inversion about average slightly decreases the positive coefficients, and roughly brings the negative coefficient to a positive value $3 \cdot 2^{-n/2}$
- The next phase shift turns this coefficient negative again
- The next inversion about average increases again its absolute value

Complexity

- Lemma : as long as the coefficient corresponding to x with $C(x) = 1$ is smaller than $\frac{1}{\sqrt{2}}$, each loop iteration increases this coefficient by at least $\frac{1}{2\sqrt{N}}$ and leaves the other coefficients positive
- Constant probability of success after $O(\sqrt{N})$ iterations

Remarks

- Does not use any structure of the function C (C can be accessed as a black box)
- Continuing the loop will decrease the success probability
- Can be adapted when there are several x with $C(x) = 1$
- See *Quantum Amplitude Amplification and Estimation* by Brassard-Hoyer-Mosca-Tapp for some generalizations
- Cryptographic consequences : double your key sizes

Outline

Discrete Fourier Transform

- Let $f : [1, \ldots, N] \to \mathbb{C}$ an L_2-bounded function
- Fourier transform of f is a function $\tilde{f} : [1, \ldots, N] \to \mathbb{C}$ with

$$\tilde{f}(y) = \sum_{x=1}^{N} f(x) e^{-2\pi i x y / N}$$

(up to some normalization factor)

- Well-known in engineering for sending periodic functions to a sum of Dirac's delta functions and vice-versa

Quantum Fourier Transform

- Linear transformation A_q sending a state $\sum_a f(a)|a\rangle$ to

$$\sum_{c=0}^{q-1} \tilde{f}(c)|c\rangle \;=\; \frac{1}{q^{1/2}} \sum_{a=0}^{q-1} \sum_{c=0}^{q-1} f(a) \exp(2\pi i a c/q)\ |c\rangle$$

- Equivalently, linear transformation sending any pure state $|a\rangle$ to

$$\frac{1}{q^{1/2}} \sum_{c=0}^{q-1} \exp(2\pi i a c/q)\ |c\rangle$$

- Construction easier when $q = 2^\ell$, but adapt otherwise

Local gates used

- Hadamard transform on gate j

$$R_j = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

- Special phase shifts $S_{j,k}$ with $k > j$

$$S_{j,k} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & e^{i\pi/2^{k-j}} \end{pmatrix}$$

Local gates used (2)

- Swap gates

$$W_{j,k} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

Fast Fourier Transform

- We have

$$\sum_x f(x)e^{-2\pi ixy/2^\ell} = \sum_{x'} f(2x')e^{-2\pi ix'y/2^{\ell-1}} + e^{-2\pi iy/2^\ell}\sum_{x'} f(2x'+1)e^{-2\pi ix'y/2^{\ell-1}}$$

- Recursive formula reduces DFT complexity from $O(q^2)$ to $O(q \log q)$

Quantum Fourier transform circuit

- Do QFT on the $\ell - 1$ most significant bits
- Phase shift by $e^{-2\pi iy/2^\ell}$ if the least significant bit is 1
- QFT on one bit is just Hadamard transform
- Writing $y = \sum y_k 2^k$ the phase shift is implemented with $\ell - 1$ elementary phase shifts by $e^{-2\pi i y_k 2^{k-\ell}}$
- Only $O(\ell^2)$ quantum gates needed

Quantum Fourier transform circuit (2)

- Compute from right to left

$$R_0 S_{0,1} S_{0,2} \ldots S_{0,\ell-1} \cdot R_1 S_{1,2} S_{1,3} \ldots S_{1,\ell-1} \cdot R_2 S_{2,3} S_{2,4} \ldots S_{2,\ell-1} \cdot \ldots \cdot R_{\ell-2} S_{\ell-2,\ell-1} \cdot R_{\ell-1}$$

- This gives the transformation

$$|a\rangle \rightarrow \frac{1}{2^{\ell/2}} \sum_{c=0}^{q-1} \exp(2\pi iac/q)\ |b\rangle$$

where b is the bit-reversal of c

- Use swap gates to get the QFT

Correctness (sketch)

- Overall amplitude change is OK
- Phase change from $|a\rangle$ to $|b\rangle$ is

$$\sum_{0 \le j < \ell} \pi a_j b_j + \sum_{0 \le j < k < \ell} \frac{\pi}{2^{k-j}} a_j b_k$$

and this is equal to $2\pi ac/2^\ell$ modulo 2π

Period finding

- Given $f : \mathbb{Z} \to \mathbb{Z}$ a periodic function, compute the period (smallest T such that $f(t) = f(t+T)$ for all t)
- Intuition : periods are easier to see in frequency domain
  - Apply Fourier transform to f
  - If $f(t) = e^{2\pi i \omega t}$ then its transform is just a Dirac at ω, so a measurement on it will return the frequency ω, from which we deduce $T = \omega^{-1}$
  - When f is more complicated, the Fourier transform may have several peaks but the main peaks can all be related to the period

From factoring to period finding

- General idea to factor n : find non trivial square root of 1
  - Take random x
  - Find smallest r such that $x^r = 1 \bmod n$
  - If r is even compute $\gcd(x^{r/2} \pm 1, n)$
- Gives a non trivial factor of n unless
  - r is odd $\Rightarrow$ x was a quadratic residue
  - r is even but $x^{r/2} = \pm 1 \bmod n$
- Note : for $n = pq$ period divides $\varphi(n) = (p-1)(q-1)$ (if p, q strong primes, solve a single quadratic equation !)

Computing the order of x

- Let q such that $n^2 < q = 2^\ell < 2n^2$
- Use two registers
- Put first register in uniform superposition $\sum_{a=0}^{q-1} |a\rangle|0\rangle$
- Compute $x^a \bmod n$ in second register

$$\sum_{a=0}^{q-1} |a\rangle|x^a \bmod n\rangle$$

- Apply Fourier transform on first register

$$\sum_{a=0}^{q-1} \sum_{c=0}^{q-1} \exp(2\pi i ac/q)|c\rangle|x^a \bmod n\rangle$$

- Observe the state

Computing the order of x

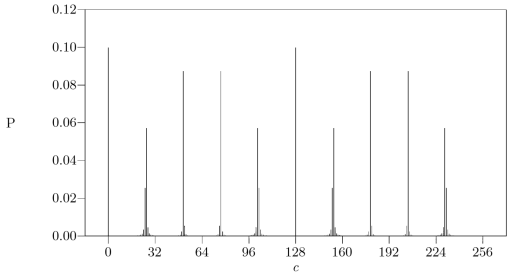
- Let T be the period of $f : a \to f(a) = x^a \bmod n$
- Probability to observe $|c, x^A \bmod n\rangle$ proportional to

$$\left| \sum_{\substack{a \,:\, x^a = x^A \bmod n \\ 0 \le a < q}} e^{2\pi i \left(\frac{ac}{q}\right)} \right|^2 = \left| \sum_{\substack{a = A + kT \\ 0 \le k \le q/T}} e^{2\pi i \left(\frac{ac}{q}\right)} \right|^2 = \left| \sum_{0 \le k \le q/T} e^{2\pi i k \left(\frac{Tc}{q}\right)} \right|^2$$

- If Tc/q close to an integer, then all elements in the sum have roughly the same phase (constructive interference), otherwise they will average to a small value

Computing the order of x

Probability of observing values of c between 0 and 255, given $q = 256$ and $T = 10$



Computing the order of x

- Quantum algorithm more likely to return $|c\rangle|x^a \bmod n\rangle$ when Tc/q close to an integer
- Let $Tc = dq + \epsilon$ with $|\epsilon| \leq T/2$
- Lemma : any such c occurs with probability $\geq 1/(3T^2)$
- We have

$$\left|\frac{c}{q} - \frac{d}{T}\right| \leq \frac{1}{2q}$$

- Since $q > n^2 > T^2$ the fraction d/T must be a continued fraction approximation of c/q
- Use Euclide algorithm to compute T

Discrete logarithms

- Given p, g, h we want to find r such that $g^r = h \bmod p$
- Now use 3 registers and $p < q < 2p$
- Put first two registers in uniform state then compute

$$\frac{1}{p-1}\sum_{a=0}^{p-2}\sum_{b=0}^{p-2}|a, b, g^a h^{-b} \bmod p\rangle$$

- Apply Fourier transform on first two registers

$$\frac{1}{(p-1)q}\sum_{a,b=0}^{p-2}\sum_{c,d=0}^{q-1}\exp\left(\frac{2\pi i}{q}(ac+bd)\right)|a, b, g^a h^{-b} \bmod p\rangle$$

Discrete logarithms

- Observe state $|c, d, y\rangle$ with probability

$$\left|\frac{1}{(p-1)q}\sum_{(a,b)\ |a-rb=k \bmod (p-1)}\exp\left(\frac{2\pi i}{q}(ac+bd)\right)\right|^2$$

- Analysis : split the exponential in two parts ; distinguish good and bad events ; show that good ones occur with constant probability, and that they allow to recover r

Remarks

- Period-finding can be adapted to any Abelian group
- In practice one must deal with errors
- Coppersmith : approximate FFT enough

Outline

Key Distribution

- Alice and Bob want to agree on a sequence of secret random bits, in the presence of an eavesdropper Eve
- They also want to detect eavesdropping if it occurs

Physical Set-up

- Polarized photons in 4 directions $\uparrow$, $\rightarrow$, $\nearrow$, $\searrow$ (with angles 0, 90, 45, 135)
- Alice sends polarized photons over a quantum channel
- Bob makes polarization measurements on these photons
- Alice and Bob also communicate over a classical channel
- Eve potentially makes measurements on the quantum channel and listens to the classical channel

Information Encoding and Measurement

- Bits are encoded as photon polarization, using either one of two orthogonal bases
  - $\uparrow = 0$, $\rightarrow = 1$
  - $\nearrow = 0$, $\searrow = 1$
- Alice chooses either basis randomly, chooses a random bit, encodes this bit as above and sends the photon to Bob
- Bob chooses either basis randomly, then measures the polarization with respect to this basis

By quantum physics laws...

- If Bob chooses the same basis as Alice, then he recovers the correct bit with probability one
- If Bob chooses the other basis, then the measurement will produce either vector basis with probability $1/2$
- If Eve makes a measurement in the same basis as Alice, she recovers the correct bit without modifying the photon
- If Eve makes a measurement in the other basis, she gets either vector basis with probability $1/2$, resulting in a change of basis for the photon sent to Bob

Protocol completion

- Alice and Bob use the classical channel to communicate each other which basis they used for each photon
- Photons measured with respect to the wrong basis are discarded
- A subset of n remaining bits are compared over the classical channel to detect eavesdropping, with error detection probability $1 - (3/4)^n$

Eavesdropping detection analysis

- No eavesdropping : all bits will match
- When Alice and Eve use the same basis, Bob's measurement is unchanged
- When Alice and Eve use different bases, Bob's measurement wrong with probability $1/2$
- Eve has a probability $1/2$ of using Alice's basis

In "practice"

- Large scale proof-of-concept experiments
- Commercial devices (but still limited use)
- Practical issues/ attacks :
  - Random measurement errors (not adversarial)
  - Man-in-the-middle attacks (need for authentication)
  - Two photons sent instead of one
  - Information on Alice/Bob basis choice

References

- Protocol described is Bennett-Brassard 1984
- Ekert 1991 uses entangled photons

Conclusion

- Quantum computers will kill currently deployed protocols based on discrete logarithm and factorization problems
- Also need to double all key sizes
- Quantum key exchange still needs classical authentication
- Some research challenges
  - Build a quantum computer
  - New crypto protocols based on alternative problems
  - Are those new problems hard for quantum/ classical computers ?