Quantum cryptanalysis: How to break some classical cryptosystems with quantum computers?

Miklos Santha

CNRS, IRIF, Université Paris Diderot, France

and

Centre for Quantum Technologies, NUS, Singapore

Plan of the talk

1. Crash course on quantum computing
2. Simon's problem
3. Factorisation
4. The Hidden Subgroup Problem (HSP)
5. Quantum safe cryptography

Classical bit: $b \in \{0,1\}$

Probabilistic bit

Probability distribution $d \in \mathbb{R}_+^{\{0,1\}}$ such that $\|d\|_1 = 1$.

$\Longrightarrow$ $d = (p, 1-p)$ with $p \in [0,1]$.

Quantum bit

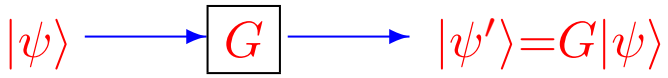
Superposition $|\psi\rangle \in \mathbb{C}^{\{0,1\}}$ such that $\||\psi\rangle\|_2 = 1$.

$\Longrightarrow$ $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ with $|\alpha|^2 + |\beta|^2 = 1$.

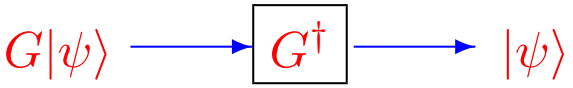
$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \; |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \; |\psi\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}.$$

Unitary transformation

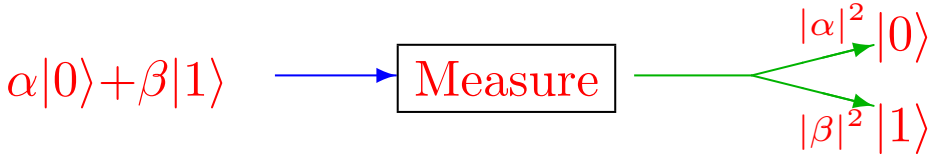
$|\psi\rangle \mapsto G|\psi\rangle$, with $G \in \mathbb{C}^{2\times 2}$ such that $G^\dagger G = Id$.



Unitary $\Longrightarrow$ Reversible:



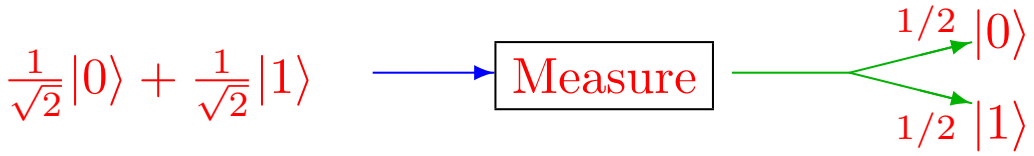
Measure: Reads and modifies.



$\Longrightarrow$ Superposition $\rightarrow$ Probability distribution.

Superposition: $|\psi\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$

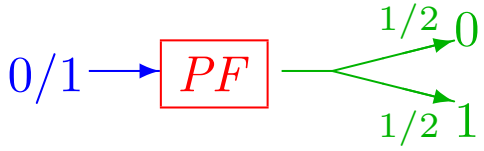
Measure



Unitary transformations

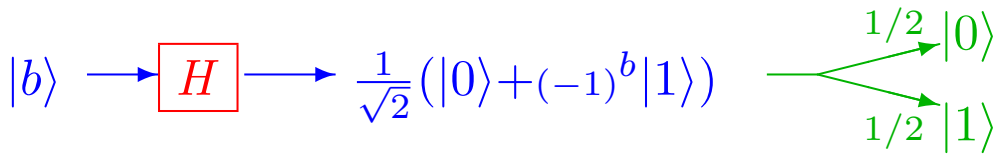
- NOT, $|0\rangle \leftrightarrow |1\rangle$: $G = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$.
- Hadamard: $H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$.

Probabilistic flip



Remark: $PF \circ PF = PF$.

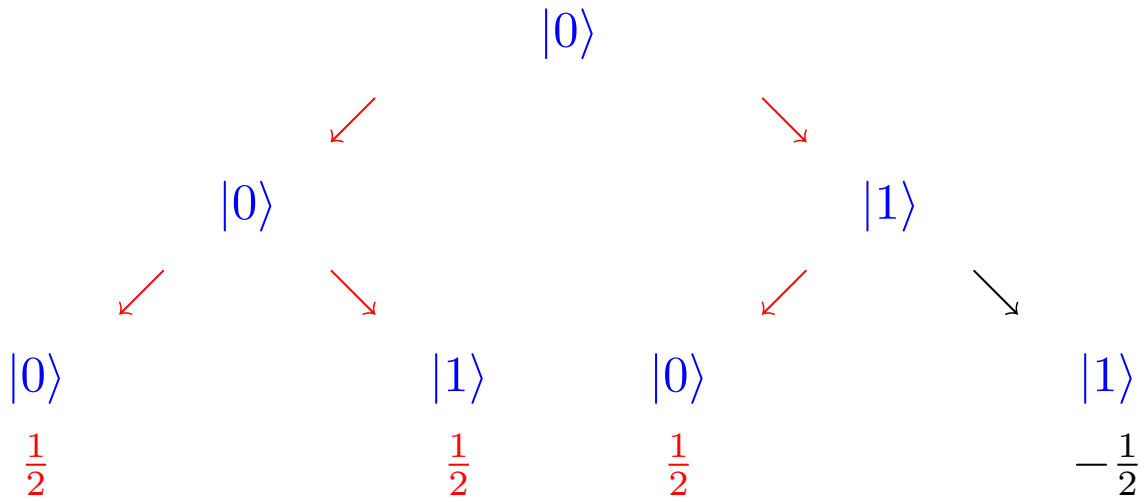
Quantum flip



Conclusion : $PF = \text{Measure} \circ H$.

Question : $H \circ H =$?

$\rightarrow: +\frac{1}{\sqrt{2}}, \quad \rightarrow : -\frac{1}{\sqrt{2}}.$



$H \circ H|b\rangle = |b\rangle \quad \Longrightarrow \quad H \circ H = Id.$

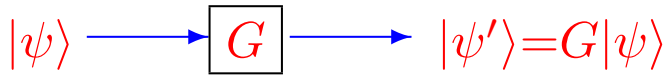
Conclusion : Measures change the computation

Definition: n-qubit $\leftrightarrow$ tensor product of n qubits.

$|\psi\rangle \in \mathbb{C}^{\{0,1\}^n}$ such that $\||\psi\rangle\|_2 = 1$.

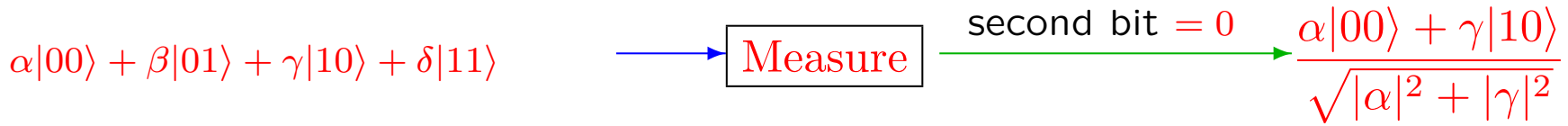
$\Longrightarrow |\psi\rangle = \sum_{x\in\{0,1\}^n} \alpha_x|x\rangle$ with $\sum_x |\alpha_x|^2 = 1$.

Unitary transformation: $|\psi\rangle \mapsto G|\psi\rangle$, with $G \in \mathrm{U}(2^n)$.

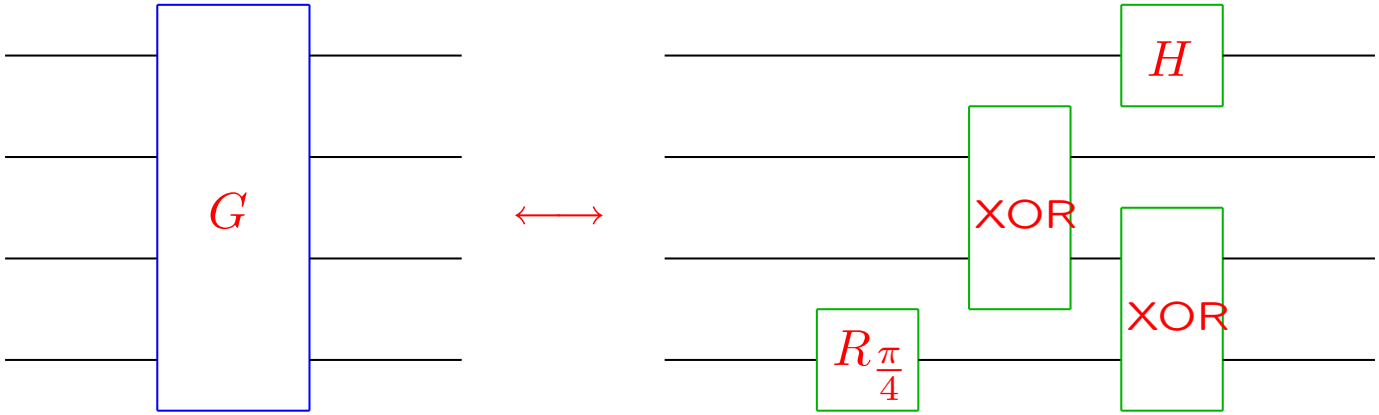


Measure

Partial measure



Quantum circuit: ($G \in U(16)$)



Theorem [DiV95,BMPRV99]:

Every transformation on n-qubit decomposes into transformations on 1-qubit and 2-qubit.

$\Longrightarrow$ Universal family.

Simon's problem

Computing a function by oracle

Let $f : \{0,1\}^n \to \{0,1\}^m$ be a function

Classical computing

$$\begin{array}{rccc} C_f : & \{0,1\}^n & \to & \{0,1\}^m \\ & x & \mapsto & f(x) \end{array}$$

Reversible computing

$$\begin{array}{rccc} R_f : & \{0,1\}^{n+m} & \to & \{0,1\}^{n+m} \\ & (x,y) & \mapsto & (x, y \oplus f(x)) \end{array}$$

Quantum computing

$$\begin{array}{rccc} U_f : & \mathbb{C}^{\{0,1\}^{n+m}} & \to & \mathbb{C}^{\{0,1\}^{n+m}} \\ & |x\rangle|y\rangle & \mapsto & |x\rangle|y \oplus f(x)\rangle \\ & |x\rangle|0\rangle & \mapsto & |x\rangle|f(x)\rangle \end{array}$$

Simon's problem (SIMON)

SIMON

Input (given by an oracle): A function $f : \{0,1\}^n \to \{0,1\}^n$
Promise:

$$\exists s \neq 0^n, \quad f(x) = f(y) \iff (x = y \quad \text{or} \quad x = y \oplus s)$$

Output: s.

Remark: f is a periodical function and we are looking for its period

Complexity: Number of evaluations of f and the computation time.

Deterministic: $2^{n-1} + 1$ evaluations.

Probabilistic: $\Omega(2^{n/2})$ evaluations.

Theorem[Simon'94]: The problem SIMON can be solved by a quantum algorithm with $O(n)$ evaluations and in time $O(n^3)$.

Hadamard (Fourier) Transform on n-qubit

Recall:

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

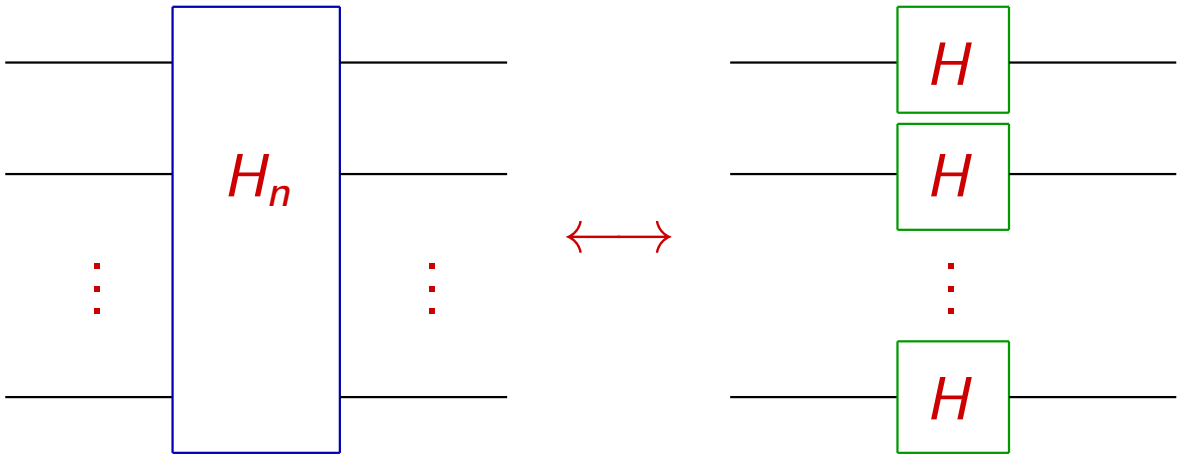
Definition:

$$H_n|x\rangle = \frac{1}{2^{n/2}} \sum_y (-1)^{x \cdot y} |y\rangle$$

where $x \cdot y = \sum_i x_i y_i \mod 2$

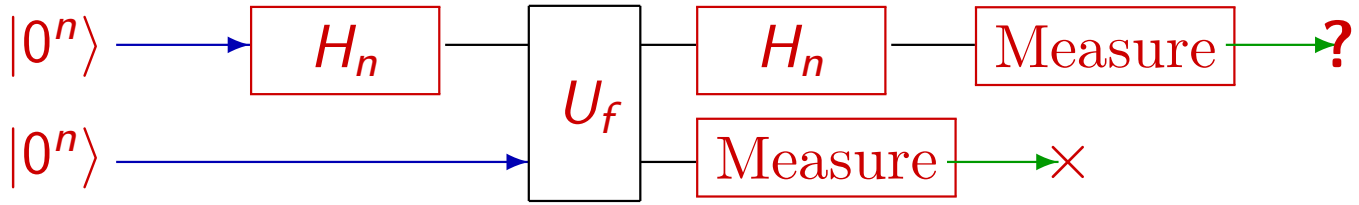
Example: $\langle 101011|H_6|110111\rangle = -1/8$

Quantum circuit for H_n:



Simon's algorithm

Circuit



Analysis

- Initialisation : $|0^n\rangle|0^n\rangle$
- H_n on the 1st register: $\frac{1}{2^{n/2}} \sum_{x\in\{0,1\}^n} |x\rangle\ |0^n\rangle$
- Evaluation of f : $\frac{1}{2^{n/2}} \sum_x |x\rangle\ |f(x)\rangle$
- Measure of the 2nd register: $\frac{1}{\sqrt{2}} \left(|a\rangle + |a\oplus s\rangle\right) |f(a)\rangle$
- H_n on the 1st register: $\frac{1}{2^{n/2}\sqrt{2}} \sum_y \left((-1)^{a\cdot y} + (-1)^{(a\oplus s)\cdot y}\right) |y\rangle$

$$= \frac{1}{2^{n/2}\sqrt{2}} \sum_y (-1)^{a\cdot y} \left(1 + (-1)^{s\cdot y}\right) |y\rangle$$

- Measure of the 1st register: uniform y such that $s\cdot y = 0$

Conclusion : In $O(n)$ iterations we obtain a system of linear equations of rank $n-1$ $\Longrightarrow$ the 2 solutions are $\{0^n, s\}$.

Factorisation

Classical reductions

Factorisation

Input: a composite number N

Output: a non-trivial divisor of N.

Square Root

Input: N

Output: y such that $y^2 = 1 \mod N$ and $y \neq \pm 1 \mod N$.

Fact 1: Factorisation $\leq$ Square Root.

Proof: $N|(y+1)(y-1) \implies$
$\gcd(N, y \pm 1)$ is a non-trivial divisor of N

Order

Input: $N, a \in \mathbb{Z}_N^*$

Output: the period r of the function $x \to a^x \mod N$.

Fact 2: Square Root $\leq_R$ Order.

Proof: Let $x \in \mathbb{Z}_N^*$ random, $x^r = 1 \mod N$. Then
$\Pr[r \text{ is even and } x^{r/2} \neq \pm 1 \mod N] \geq 1/2$.

Example: $N = 24, x = 5, r = 2$. Then $\gcd(5 \pm 1, 24)$ divides 24

Computing the order (with help)

The function $x \to a^x \mod N$ is periodical over $\mathbb{Z}$.

To compute the period, we will approximate the infinite group $\mathbb{Z}$ by a "big" cyclic group $\mathbb{Z}_q$ (taking $q \approx N^2$).

I will suppose that $r = \text{order}(a) \mod N$ divides q.

Without this (irrealistic) hypothesis a classical correction (via continuous fractions) is necessary

ORDER (with help)

Input: $N, a \in \mathbb{Z}_N^*, q$ such that $r = \text{order}(a) \mod N$ divides q
Output: r

Consequence: The function

$$\begin{array}{rccc} f: & \mathbb{Z}_q & \to & \mathbb{Z}_N \\ & x & \mapsto & a^x \mod N \end{array}$$

is periodical.

Quantum Fourier Transform $\mod q$

Let ω_q be a q-th primitive root of the unity

Definition: The Quantum Fourier Transform $\mod q$ is the function

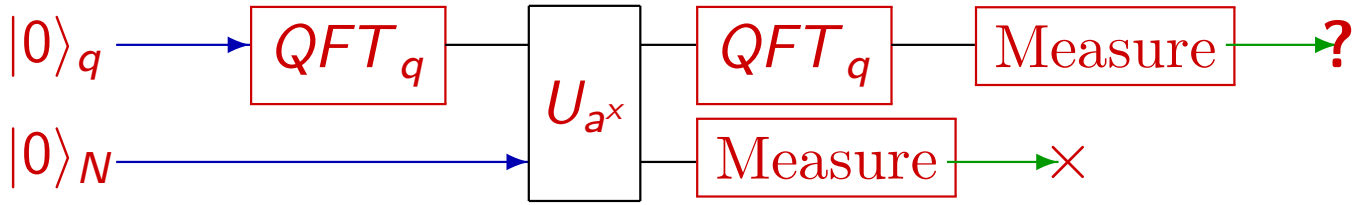
$$\begin{array}{rccc} QFT_q: & \mathbb{C}^q & \to & \mathbb{C}^q \\ & |x\rangle & \mapsto & \frac{1}{\sqrt{q}} \sum_{y \in \mathbb{Z}_q} \omega_q^{xy} |y\rangle \end{array}$$

Example: $\langle 1|QFT_4|3\rangle = -i/2$

Theorem: QFT_q can be computed approximately by a quantum algorithm in time $O((\log q)^2)$.

Shor's algorithm for ORDER (with help)

Circuit



Analysis

- Initialisation : $|0\rangle_q|0\rangle_N$
- QFT_q on 1st register: $\frac{1}{\sqrt{q}} \sum_{x=0}^{q-1} |x\rangle_q \, |0\rangle_N$
- Evaluation of a^x : $\frac{1}{\sqrt{q}} \sum_{x=0}^{q-1} |x\rangle_q \, |a^x\rangle_N$
- Measure of 2nd register: $\frac{1}{\sqrt{\frac{q}{r}}} \sum_{j=0}^{\frac{q}{r}-1} |jr+k\rangle_q \, |a^k\rangle_N$
- QFT_q on 1st register: $\frac{1}{\sqrt{q}} \sum_{c=0}^{q-1} \sqrt{\frac{r}{q}} \sum_{j=0}^{\frac{q}{r}-1} \omega_q^{(jr+k)c} |c\rangle_q$

$$= \sum_{c=0}^{q-1} \left(\frac{\sqrt{r}}{q} \, \omega_q^{kc} \sum_{j=0}^{\frac{q}{r}-1} (\omega_q^{rc})^j \right) |c\rangle_q$$

$$= \sum_{c=0}^{q-1} \alpha_c \, |c\rangle_q$$

Shor's algorithm for ORDER (with help)

Evaluation of the amplitudes $\alpha_c = \frac{\sqrt{r}}{q}\ \omega_q^{kc}\ \sum_{j=0}^{\frac{q}{r}-1} (\omega_{\frac{q}{r}}^{c})^j$:

$$\alpha_c = \begin{cases} 0 & \text{if } \frac{q}{r} \text{ doesn't divide } c \\ \frac{1}{\sqrt{r}}\ \omega_q^{kc} & \text{if } \frac{q}{r} | c \end{cases}$$

Evaluation of the probabilities: One measures $t\frac{q}{r}$, for $t = 0, \ldots, r-1$, with probability $|\frac{1}{\sqrt{r}}\ \omega_q^{kc}|^2 = \frac{1}{r}$.

Computing r: If $\gcd(t, r) = 1$, then

$$\gcd(t\tfrac{q}{r}, q) = \gcd(t\tfrac{q}{r}, r\tfrac{q}{r}) = \gcd(t, r)\tfrac{q}{r} = \tfrac{q}{r}$$

Chance of measuring $t\frac{q}{r}$ with $\gcd(t, r) = 1$:

$$\Pr[\ \gcd(t, r) = 1] = \frac{\phi(r)}{r} = \omega(\log\log r) = \omega(\log\log N)$$

Conclusion: One repeats this quantum process $O(\log\log N)$-times to succeed with constant probability close to 1.

Hidden Subgroup Problem (HSP)

Hidden Subgroup Problem (HSP)

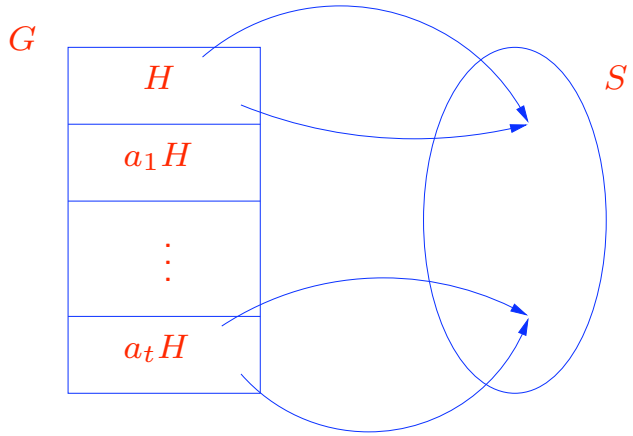
HSP$(G;\mathcal{H})$ where G finite group, $\mathcal{H}$ family of subgroups of G

Input(possibly by oracle): a function $f : G \to S$

Promise: f hides a subgroup $H \in \mathcal{H}$:

$$f(x) = E(xH),$$

where E is injective on the left cosets of H.



Sortie: Generators for H H.

Complexity: Number oracle requests and time

Quantum solutions for HSP

The success of HSP:

Theorem[Shor'94]: HSP is solvable in abelian groups in quantum polynomial time in $\log(|G|)$.

Corollary Factorisation (HSP in $\mathbb{Z}_q$) and the discrete logarithm (HSP in $\mathbb{Z}_{p-1} \times \mathbb{Z}_{p-1}$) are computable in quantum polynomial time.

Extension to $\mathbb{R}$ and $\mathbb{R}^m$

Extension to certain non-abelian groups

Extension hidden algebraic sets of higher degree

Characters of an abelian group

Let G be an abelian group.

Definition: A character $\chi : G \to \mathbb{C}^*$ is a group homomorphism.

Remark: $\chi(x)$ is a $|G|^{\text{th}}$ root of the unity.

$\widehat{G} = \{\text{characters of } G\}$.

Theorem: G and $\widehat{G}$ are isomorphic. $\widehat{G} = \{\chi_y : y \in G\}$.

Examples: $G = \mathbb{Z}_q$: $\chi_y(x) = \omega_q^{x \cdot y}$.

$G = G_1 \times G_2$: $\chi_y(x) = \chi_{y_1}(x_1)\chi_{y_2}(x_2)$.

Definition: Let $H \leq G$. Its orthogonal subgroup is

$$H^\perp = \{y \in G : \forall h \in H, \chi_y(h) = 1\}.$$

Theorem: Soit $H \leq G$. There exists a deterministic algorithm that computes H from $H^\perp$ in time $O(\log^3 |G|)$.

Quantum Fourier Transform in an abelian group

Let G be an abelian group.
We consider $\mathbb{C}^G$, the Hilbert space generated by G.

Bases:

- Dirac: $\{|x\rangle : x \in G\}$.
- Characters: $\{|\chi_y\rangle : y \in G\}$,
  where $|\chi_y\rangle = \sum_x \chi_y(x)|x\rangle$.

Definition: $QFT_G : |y\rangle \mapsto \frac{1}{\sqrt{G}}|\chi_y\rangle$.

Principal property: Let $H \leq G$, $x \in G$. Then

$$TFQ_G|x + H\rangle = |H^\perp(x)\rangle, \quad \text{where}$$

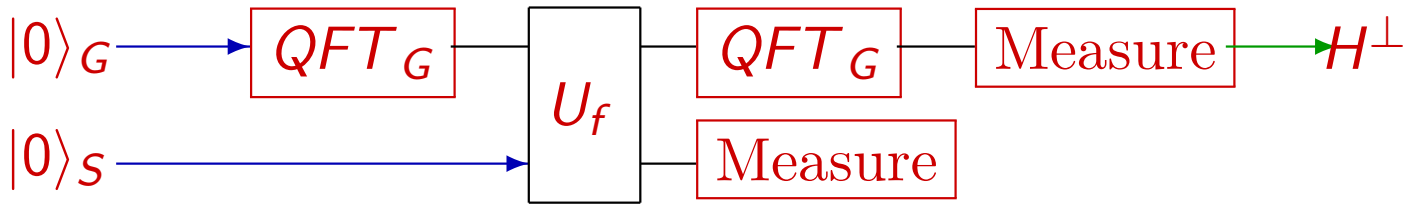
$|x + H\rangle = \frac{1}{\sqrt{|H|}} \sum_{h \in H} |x + h\rangle$ and
$|H^\perp(x)\rangle = \frac{1}{\sqrt{|H^\perp|}} \sum_{y \in H^\perp} \chi_y(x)|y\rangle$.

Theorem: The approximate QFT_G can be computed in quantum polynomial time.

Standard solution for HSP in a finite abelian group G

Repeated quantum Fourier sampling of f that hides H:

Circuit : **Fourier sampling^f(G)**



Analysis

- QFT_G on 1st register: $\sum_{x\in G} |x\rangle\ |0\rangle$
- Query f : $\sum_{x\in G} |x\rangle\ |f(x)\rangle$
- Measure of 2nd register: $|a+H\rangle\ |f(a)\rangle$
- QFT_G on 1st register: $|H^\perp(a)\rangle$
- Measure of 1st register: uniform y in $H^\perp$.

Simon and Order revisited

Simon:

$G = \{0,1\}^n$, $H = \{0^n, s\}$ for $0^n \neq s \in \{0,1\}^n$

$f(x) = f(y)$ if and only if $x = y$ where $x \oplus y = s$

Characters:

$$\chi_y : \begin{array}{ccc} \{0,1\}^n & \to & \mathbb{C} \\ x & \mapsto & (-1)^{x \cdot y} \end{array} \quad \text{for } y \in \{0,1\}^n$$

where $x \cdot y = \sum_{i=1}^{n} x_i y_i \mod 2$

$H^\perp = \{y : s \cdot y = 0\}$

Order (with help):

$G = \mathbb{Z}_q$, $H = \{0, r, 2r, \ldots\}$

The hiding function for H:

$$f : \begin{array}{ccc} \mathbb{Z}_q & \to & \mathbb{Z}_N \\ x & \mapsto & a^x \bmod N \end{array}$$

Characters:

$$\chi_c : \begin{array}{ccc} \mathbb{Z}_q & \to & \mathbb{C} \\ x & \to & \omega_q^{cx} \end{array} \quad \text{for } k \in \mathbb{Z}_q$$

$\chi_c(r) = 1$ if and only if q/r divides c, $H^\perp = \{c : q/r \text{ divides } c\}$

Quantum safe cryptography

Cryptosystems in danger

Theorem[Shor'94]: The HSP is solvable in finite abelian groups in quantum polynomial time.

Corollary: Factorisation, discrete logarithm, discrete logarithm in elliptic curves are solvable in quantum polynomial time.

A quantum computer would break the following systems:

- RSA
- Diffie-Hellman key exchange (DH)
- El Gamal encryption
- Digital Signature Algorithm (DSA)
- ECDH, ECDSA, ECIES
- pairing based cryptography
- etc.

RSA and factorization

Number theoretical fact: Let $n = pq$ where p and q are primes.
Euler's totient function: $\phi(n) = (p-1)(q-1)$. Then for every m,

$$m^{\phi(n)} = n \mod n$$

Key generation:
Public key: $n = pq$ and e such that $\gcd(e, \phi(n)) = 1$
Private key: d such that $ed = 1 \mod \phi(n)$.

Encryption: Let the message be $0 < m < n$

$$c = m^e \mod n$$

Decryption:

$$c^d = m^{ed} = m \mod n$$

Factorizing $n \iff$ Computing $\phi(n) \implies$ Breaking RSA
But this is not necessary, maybe there are other methods!

NSA recommendations for a quantum safe cryptography

The "guidance" of National Security Agency (NSA) in August 2015:

"Our ultimate goal is to provide cost effective security against a potential quantum computer.

We are working with partners across the USG, vendors, and standards bodies to ensure there is a clear plan for getting a new Suite of algorithms that are developed in an open and transparent manner that will form the foundation of our next Suite of cryptographic algorithms.

Until this new suite is developed and products are available implementing the quantum resistant suite, we will rely on current algorithms. For those partners and vendors that have not yet made the transition to Suite B algorithms, we recommend not making a significant expenditure to do so at this point but instead to prepare for the upcoming quantum resistant algorithm transition".

NIST quantum safe project

http://csrc.nist.gov/groups/ST/post-quantum-crypto/

15 Décembre 2016: "The National Institute of Standards and Technology (NIST) is now accepting submissions for quantum-resistant public-key cryptographic algorithms. The deadline for submission is November 30, 2017.

In recent years, there has been a substantial amount of research on quantum computers. If large-scale quantum computers are ever built, they will be able to break many of the public-key cryptosystems currently in use.

The question of when a large-scale quantum computer will be built is a complicated one. While in the past it was less clear that large quantum computers are a physical possibility, many scientists now believe it to be merely a significant engineering challenge.

It has taken almost two decades to deploy our modern public key cryptography infrastructure. We must begin now to prepare our information security systems to resist quantum computing".

Methods for quantum safe cryptography

- Error correcting code based (McElice 1978)
- Hash based (Merkle 1979)
- Lattice based (Ajtai 1996)
- Multivariate polynomial based (Patarin 1996)
- Supersingular elliptic curve isogeny based (Rostovtsev and Stolbunov 2006)
- Symmetric key based (AES)

Candidate proposals for NIST

	Signatures			KEM/Encryption			Overall	
		NIST	F.		NIST	F.	NIST	F.
Lattice-based	CRYSTALS-DILITHIUM DRS FALCON pqNTRUSign qTESLA	4	5	Compact LWE CRYSTALS-KYBER Ding Key Exchange EMBLEM and R.EMBLEM FrodoKEM Giophantus HILA5 KINDI LAC Lepton LIMA Lizard LOTUS NewHope NTRUEncrypt NTRU-HRSS-KEM NTRU Prime Odd Manhattan OKCN/AKCN/CNKE Round2 SABER Three Bears Titanium	24	23	28	28
Code-based	pqsigRM RaCoSS RankSign	5	3	BIG QUAKE BIKE Classic McEliece DAGS Edon-K HQC LAKE LEDAkem LEDApkc LOCKER McNie NTS-KEM Ouroboros-R QC-MDPC KEM Ramstake RLCE-KEM RQC	19	17	24	20
Multi-variate	DualModeMS GeMSS Gui HiMQ-3 MQDSS LUOV Rainbow	7	7	CFPKM DME SRTPI	6	3	13	10
Hash-based	Gravity-SPHINCS SPHINCS+	4	2				4	2
Others	Picnic Post-quantum RSA-Signature WalnutDSA	3	3	Guess Again HK17 Mersenne-756839 Post-quantum RSA-Encryption RVB SIKE	8	6	11	9
Total		23	20		57	49	80	69

The story of the SOLILOQUY cryptosystem

SOLILOQUY: A cautionary tale[Campbell, Groves, Shepherd '14]

A publication of the Communications-Electronics Security Group in the Government Communications Headquarters

Developed in 2007, abandoned in 2014 due to quantum attacks

"We would like to state clearly that, following our work on the quantum algorithm, we have stopped the development of SOLILOQUY as a potential quantum-resistant primitive and we do not recommend its use for real-world deployement.

As of late 2014, when novel types of quantum-resistant cryptography are being developed for real world deployment, we caution that much care and patience will be required to ensure that each design receives a thorough security assessment.

It would seem that quantum algorithms for resolving Abelian Hidden Subgroup Problems have broader applicability to cryptography than 'traditionally' documented".

Plan of the talk was

1. Crash course on quantum computing
2. Simon's problem
3. Factorisation
4. The Hidden Subgroup Problem (HSP)
5. Quantum safe cryptography

Thank you!