Introduction to Quantum Algorithms

Gustavo Banegas
gustavo@cryptme.in
cryptme.in/talks
ECRYPT-NET meeting, Leuven, Belgium

Department of Mathematics and Computer Science
Technische Universiteit Eindhoven

Friday 23rd September, 2016

Content

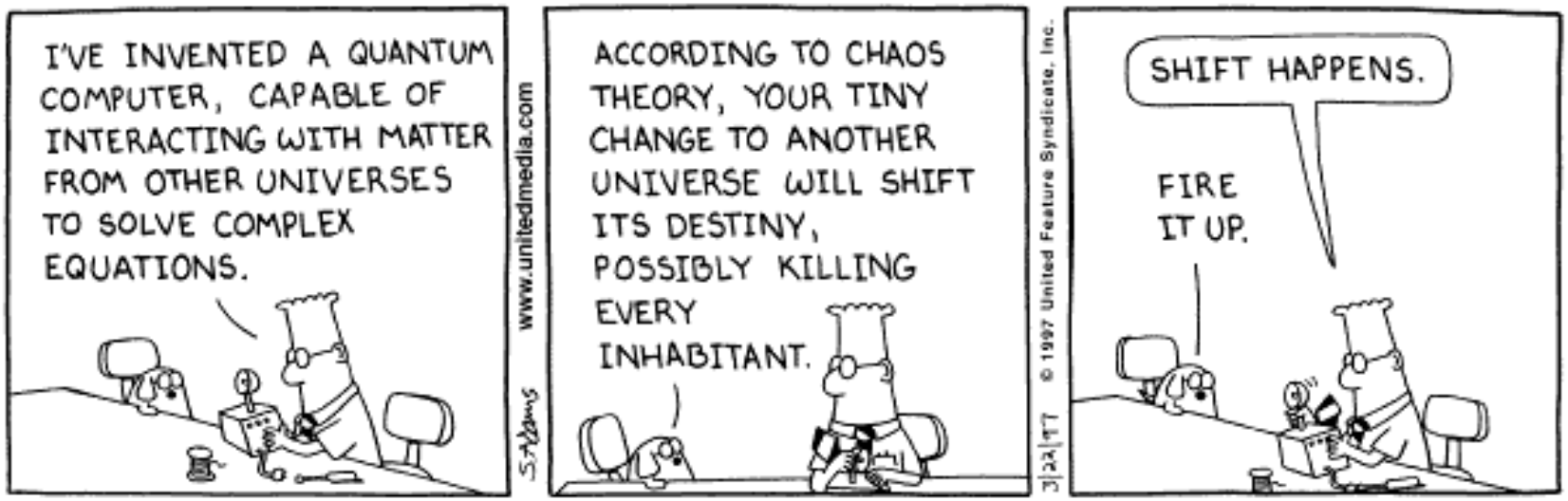
Introduction

Why study post-quantum?

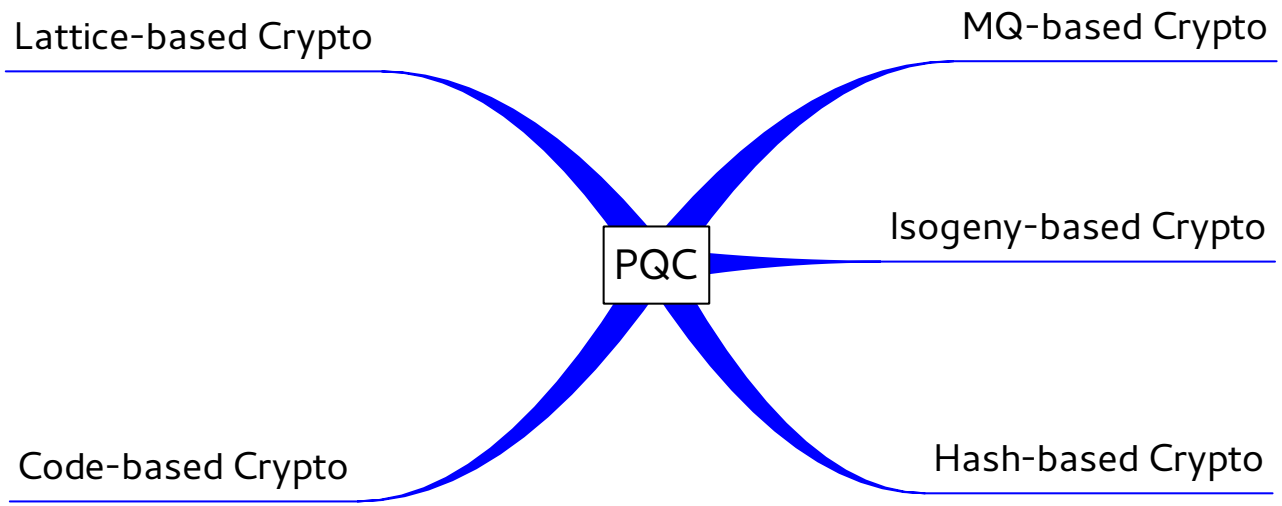
> *"Somebody announces that he's built a large quantum computer. RSA is dead. DSA is dead. Elliptic curves, hyperelliptic curves, class groups, whatever, dead, dead, dead." (Bernstein, 2005)*

Introduction

In other words...



Overview

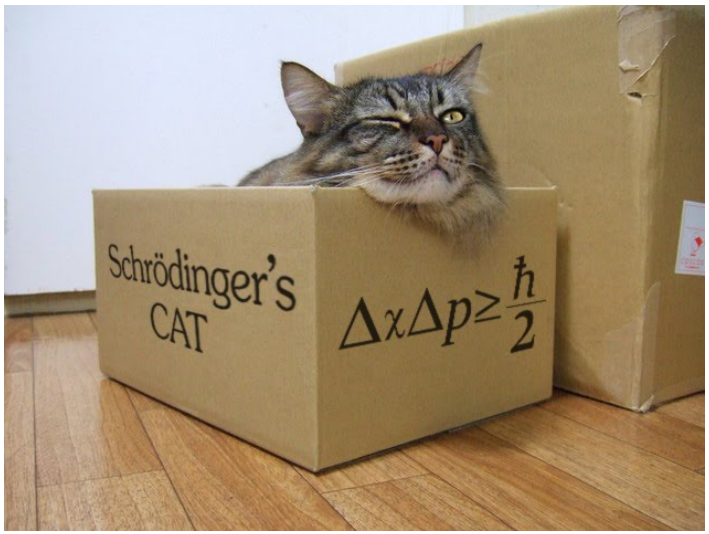

Lattice-based Crypto
MQ-based Crypto
PQC
Isogeny-based Crypto
Code-based Crypto
Hash-based Crypto

How?

Ok! How to attack with quantum algorithms?

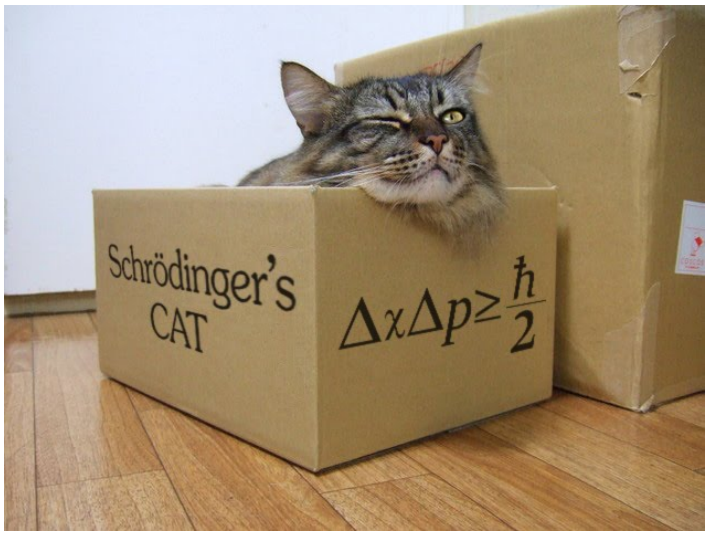
Qubits

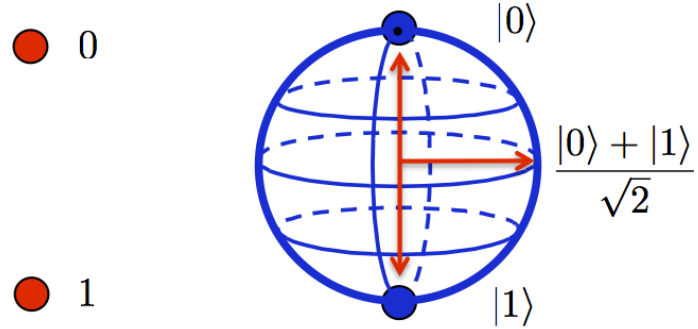
Superposition



Qubits

Superposition





Classical Bit **Qubit**

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \quad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

$$\alpha\,|0\rangle + \beta\,|1\rangle \;\;,\; |\alpha|^2 + |\beta|^2 = 1$$

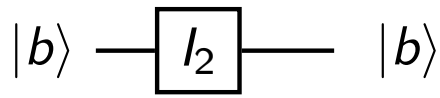
Measuring Qubits

Measuring the state collapses the superposition

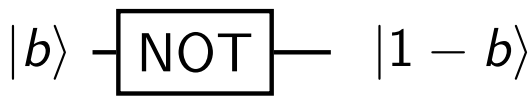
Classical & Quantum Gates

Classical Gates

- Identity:

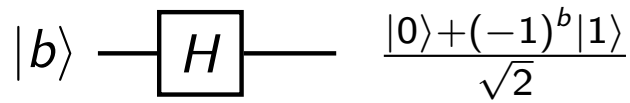


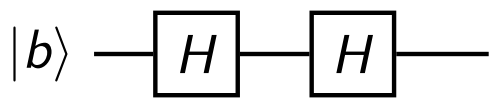
- Negation:



Hadamard Gate

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





n-qubit system

Definition

$$|\psi\rangle \in \mathbb{C}^2 \text{ such that } || \, |\psi\rangle \, || = 1$$

$$|\psi\rangle = \sum_{x \in \{0,1\}^n} \alpha_x \, |x\rangle$$

where

$$\sum_{x \in \{0,1\}^n} |\alpha_x|^2 = 1$$

Example - 2-qubit system

- 4 basis states
  $|0\rangle \otimes |0\rangle$, $|0\rangle \otimes |1\rangle$, $|1\rangle \otimes |0\rangle$, $|1\rangle \otimes |1\rangle$
- It is common to use $|1\rangle \, |0\rangle$ or $|10\rangle$

Deutsch-Jozsa Problem

Deutsch-Jozsa Problem

- Input: $f : \{0,1\}^n \to \{0,1\}$ either constant or balanced
- Output: 0 iff f is constant
- Constraint: f is a **black-box**

Query Complexity

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

Deutsch-Jozsa Problem

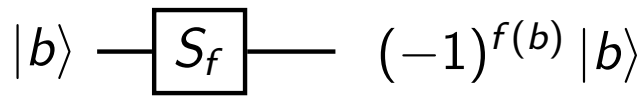
- Input: $f : \{0,1\}^n \to \{0,1\}$ either constant or balanced
- Output: 0 iff f is constant
- Constraint: f is a **black-box**

Query Complexity

- Deterministic: $2^{n-1} + 1$
- Quantum: 1

Deutsch-Jozsa Algorithm

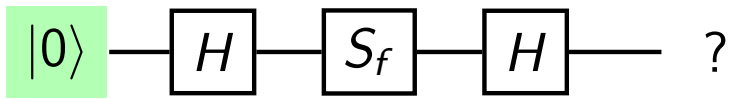
Implementation of S_f



Quantum Circuit

Deutsch-Jozsa Algorithm

Analysis $n = 1$



- Initialization: $|0\rangle$

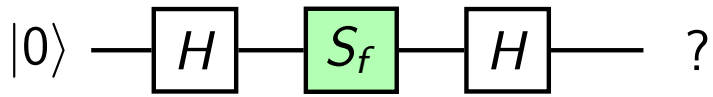
Deutsch-Jozsa Algorithm

Analysis $n = 1$

- Initialization: $|0\rangle$
- Parallelization: $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$

Deutsch-Jozsa Algorithm

Analysis $n = 1$



- Initialization: $|0\rangle$
- Parallelization: $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$
- Query: $\frac{1}{\sqrt{2}}((-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle)$

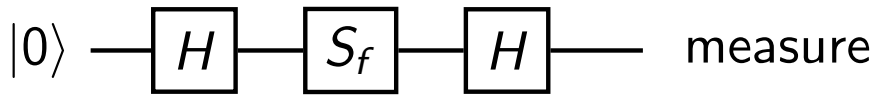
Deutsch-Jozsa Algorithm

Analysis $n = 1$

- Initialization: $|0\rangle$
- Parallelization: $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$
- Query: $\frac{1}{\sqrt{2}}((-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle)$
- Interferences: $\frac{1}{2}((-1)^{f(0)}(|0\rangle + |1\rangle) + (-1)^{f(1)}(|0\rangle - |1\rangle)$

Deutsch-Jozsa Algorithm

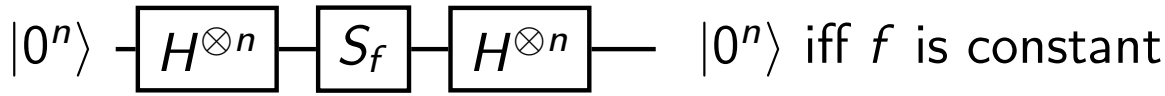
Analysis $n = 1$



- Initialization: $|0\rangle$
- Parallelization: $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$
- Query: $\frac{1}{\sqrt{2}}((-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle)$
- Interferences: $\frac{1}{2}((-1)^{f(0)}(|0\rangle + |1\rangle) + (-1)^{f(1)}(|0\rangle - |1\rangle)$
- Final State: $\frac{1}{2}(((-1)^{f(0)} + (-1)^{f(1)})|0\rangle + ((-1)^{f(0)} - (-1)^{f(1)})|1\rangle)$

Deutsch-Jozsa Algorithm

Generalizing...



- Initialization: $|00\ldots0\rangle = |0^n\rangle$
- Parallelization: $\frac{1}{2^{n/2}} \sum_{x\in\{0,1\}^n} |x\rangle$
- Query: $\frac{1}{2^{n/2}} \sum_{x\in\{0,1\}^n} (-1)^{f(x)} |x\rangle$
- Interferences: $\frac{1}{2^n} \sum_{x,y\in\{0,1\}^n} (-1)^{f(x)+x\cdot y} |y\rangle$
- Amplitude of $|0^n\rangle$: $\frac{1}{2^n} \sum_{x\in\{0,1\}^n} (-1)^{f(x)}$

Quantum Fourier Transform

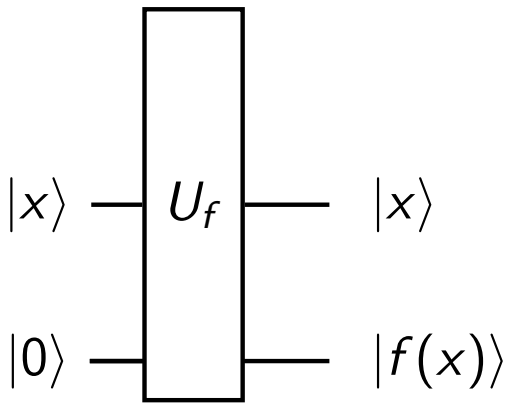
$$QFT_n |x\rangle = \frac{1}{2^{n/2}} \sum_y (-1)^{x \cdot y} |y\rangle$$

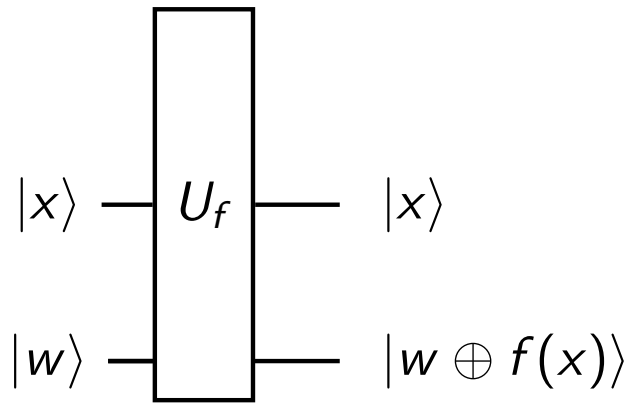
where

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

Simon's Problem

- Input: $f : \{0,1\}^n \to \{0,1\}^n$ such that
  $\exists s \in \{0,1\}^n : \forall x \neq y, f(x) = f(y) \iff y = x \oplus s$
- Output: s
- Constraint: f is a **black-box**

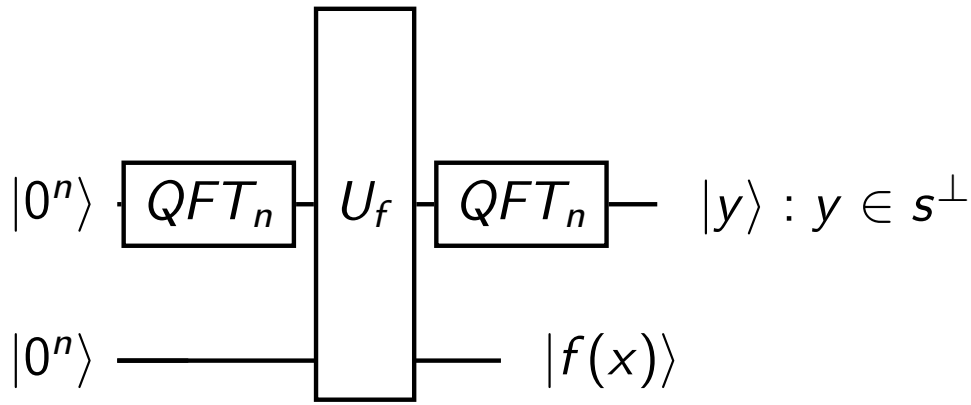




Complexity

- Classical: $O(\sqrt{2^n})$ queries by "Birthday paradox"
- Quantum: $O(n)$ queries and circuit size $O(n^3)$

Simon's Algorithm



- Initialization: $|0^n\rangle\,|0^n\rangle$
- Parallelization: $\frac{1}{2^{n/2}} \sum_x |x\rangle\,|0^n\rangle$
- Query f: $\frac{1}{2^{n/2}} \sum_x |x\rangle\,|f(x)\rangle$
- Filter: $\frac{1}{\sqrt{2}}(|x\rangle + |x \oplus s\rangle)\,|f(x)\rangle$
- Interferences: $\frac{1}{2^{(n+1)/2}} \sum_y ((-1)^{x\cdot y} + (-1)^{(x\oplus s)\cdot y})\,|y\rangle\,|f(x)\rangle$

Simon's Algorithm

- Initialization: $|0^n\rangle\,|0^n\rangle$
- Parallelization: $\frac{1}{2^{n/2}}\sum_x |x\rangle\,|0^n\rangle$
- Query f: $\frac{1}{2^{n/2}}\sum_x |x\rangle\,|f(x)\rangle$
- Filter: $\frac{1}{\sqrt{2}}(|x\rangle + |x\oplus s\rangle)\,|f(x)\rangle$
- Interferences: $\frac{1}{2^{(n+1)/2}}\sum_y((-1)^{x\cdot y} + (-1)^{(x\oplus s)\cdot y})\,|y\rangle\,|f(x)\rangle$

  $\frac{1}{2^{(n+1)/2}}\sum_y(-1)^{x\cdot y}(1 + (-1)^{s\cdot y})\,|y\rangle\,|f(x)\rangle$

  $\frac{1}{2^{(n-1)/2}}\sum_{y:s\cdot x=0}(-1)^{x\cdot y}\,|y\rangle\,|f(x)\rangle$

Simon's Algorithm

Finding s

- After $n+k$ interactions: $y^{(1)}, y^{(2)}, \ldots, y^{(n+k)} \in s^{\perp}$
- If $s = 0^n$ the y's have full rank (n) with prob. $\geq 1 - \frac{1}{2^k}$
- If $s \neq 0^n$ the y's have full rank $(n-1)$ with prob. $\geq 1 - \frac{1}{2^{k+1}}$
- Linear system where t denotes the unknown vector:

$$\begin{cases} y^{(1)} \cdot t = 0 \;=\; y_1^{(1)} \cdot t_1 + y_2^{(1)} \cdot t_2 + \ldots + y_n^{(1)} \cdot t_n \\ y^{(2)} \cdot t = 0 \;=\; y_1^{(2)} \cdot t_1 + y_2^{(2)} \cdot t_2 + \ldots + y_n^{(2)} \cdot t_n \\ \qquad\qquad \vdots \\ y^{(n+k)} \cdot t = 0 = y_1^{(n+k)} \cdot t_1 + y_2^{(n+k)} \cdot t_2 + \ldots + y_n^{(n+k)} \cdot t_n \end{cases}$$

System Solutions: 0's and s

Quantum World - overview

Quantum Basics

- Qubits
- Quantum Circuit Model
- Quantum Algorithms

Quantum Algorithms:

- Deutsch-Jozsa Algorithm
- Simon's Algorithm (Quantum period finding)
- Shor's Algorithm
- Grover's algorithm
- Quantum Walks

Quantum cryptanalysis research retreat (September 2016)
www.cryptme.in/slides

Next Steps

Projects

- Attack code-based cryptography (work with Aaron Lye from Bremen)
- Pre-image search with Grover's algorithm paralyzed (work with Daniel J. Bernstein)
- Estimation of gates and complexity of attack ECC (work with Tanja Lange)
- Quantum algorithms simulation in classical computers (work with Tung Chou from Eindhoven)
- Internship at Riscure with classical attacks on ECC

Basic Bibliography


Post-quantum cryptography. (Daniel J. Bernstein and Tanja Lange + Contributors). Retrieved September 20, 2016, from https://pqcrypto.org/


PQCRYPTO EU project. (n.d.). Retrieved January 25, 2016, from https://pqcrypto.eu.org/


Hayashi, M., Ishizaka, S., Kawachi, A., Kimura, G., & Ogawa, T. (2015). Invitation to Quantum Information Science. *In Introduction to Quantum Information Science* (pp. 1-12). Springer Berlin Heidelberg.


Bernstein, D. J., Buchmann, J., & Dahmen, E. (Eds.). (2009). *Post-quantum cryptography*. Springer Science & Business Media.


De Wolf, Ronald. Quantum Computing: Lecture Notes, 2013.


Grassl, Markus, et al. *Applying Grover's algorithm to AES: quantum resource estimates.* International Workshop on Post-Quantum Cryptography. Springer International Publishing, 2016.

Questions

Thank You!!

¿Questions?