# Attacking the ECDLP with Quantum Computing

Sam Green and Can Kizilkale
sam.green@cs.ucsb.edu, cankizilkale@cs.ucsb.edu

December 7, 2015

# Table of contents

# August 2015 NSA announcement

"Currently, Suite B cryptographic algorithms are specified by the National Institute of Standards and Technology (NIST) and are used by NSA's Information Assurance Directorate in solutions approved for protecting classified and unclassified National Security Systems (NSS). Below, **we announce preliminary plans for transitioning to quantum resistant algorithms**." [0]

# Quantum computing in Fall 2015 news

Hype: "**A 'watershed announcement' from Google regarding quantum computers is expected to be made on 8 December**, according to a board member of the quantum computing firm D-Wave." [1]

"Intel to Invest $50 Million in Quantum Computers" [2]

"LANL Orders 1000+ Qubit D-Wave 2X [adiabatic] Quantum Computer" [3]

"...nearly 20 qubits have been juxtaposed in a single quantum register. However, **scaling this or any other type of qubit to much larger numbers while still contained in a single register will become increasingly difficult**, as the connections will become too numerous to be reliable." [4]

# Review of ECDLP

Let $E$ be an elliptic curve over $\mathbb{F}_p$ given by the Weierstrass equation

$$E : y^2 \equiv x^3 + ax + b \pmod{p}.$$

And let points $S$ and $T$ be in $E(\mathbb{F}_p)$. The ECDLP is to find $k$ (assuming it exists) such that

$$k \equiv \log_T S \pmod{p} \text{ or } S \equiv [k]T \pmod{p}.$$

# Classical ECDLP attacks

Exhaustive Search

$$O(n)$$

Pollard $\rho$

$$O(\sqrt{p}), \text{ where } p \text{ is the largest prime divisor of } n$$

Pohlig-Hellman

$$O(\sqrt{p}), \text{ where } p \text{ is the largest prime divisor of } n$$

Index-calculus (only sub-exponential attack)

$$L_p[\frac{1}{3}, 1.923]$$

Reference: [7]

# What is a qubit?

A classical bit only takes 1 or 0.

Qubit: 2 dimensional complex vector, so each qubit $\in \mathbb{C}^2$.

There are 2 base vectors $|0\rangle$, $|1\rangle$ which are orthogonal to each other:

$$
\begin{aligned}
|0\rangle &= (0,1)^\mathsf{T}, \\
|1\rangle &= (1,0)^\mathsf{T}.
\end{aligned}
$$

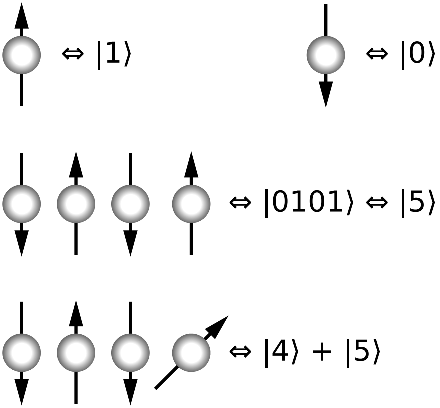
Each qubit is represented as a superposition of these. That is

$$|\phi\rangle = \alpha|0\rangle + \beta|1\rangle,$$

where

$$|\alpha|^2 + |\beta|^2 = 1.$$

# Visualizing superposition




qubits can be in a superposition of all the clasically allowed states

image credit: Wikipedia

# Bloch sphere

To represent a qubit in 3D space, we use a Bloch sphere

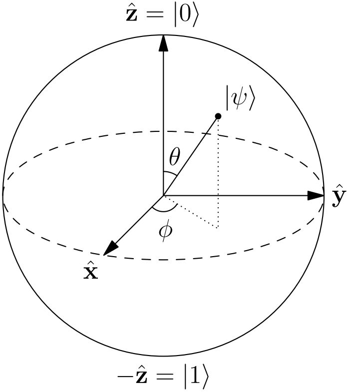



image credit: Wikipedia

$$|\psi\rangle = \cos(\tfrac{\theta}{2})|0\rangle + \sin(\tfrac{\theta}{2})e^{i\phi}|1\rangle$$

# Measurement

What are we measuring?
For a standard qubit: $\alpha|0\rangle + \beta|1\rangle = |\alpha|^2, |\beta|^2$.

The phase-shift information ($e^{i\phi}$) is lost.

By changing the basis with a unitary transformation, we capture phase shift information:

$$|+\rangle = \frac{|0\rangle}{\sqrt{2}} + \frac{|1\rangle}{\sqrt{2}},$$
$$|-\rangle = \frac{|0\rangle}{\sqrt{2}} - \frac{|1\rangle}{\sqrt{2}}.$$

$$\frac{|0\rangle}{\sqrt{2}} + \frac{e^{i\theta}|1\rangle}{\sqrt{2}} \rightarrow \frac{1 - e^{i\theta}}{\sqrt{2}}|+\rangle + \frac{1 + e^{i\theta}}{\sqrt{2}}|-\rangle$$

# Multiple bits in one register

Every sequence of bits will be mapped into an orthogonal state in a register.

For example, when we have two qubits, the state of the register will be a superposition of $|00\rangle, |01\rangle, |10\rangle,$ and $|11\rangle$.

Register $= \alpha_1|00\rangle + \alpha_2|01\rangle + \alpha_3|10\rangle + \alpha_4|11\rangle$

# Entanglement

Can the state of the register be written as the multiplication of multiple qubits? Yes, this is quantum entaglement.

No entanglement example:
$(a_1|0\rangle + b_1|1\rangle)(a_2|0\rangle + b_2|1\rangle) = a_1a_2|00\rangle + a_1b_2|01\rangle + b_1a_2|10\rangle + b_1b_2|11\rangle$.

We measure the first bit. If it is $|0\rangle$ or $|1\rangle$ then the second bit is always $a_2|0\rangle + b_2|1\rangle$.

Entanglement example: $\frac{1}{2}|00\rangle + \frac{\sqrt{3}}{2\sqrt{2}}|10\rangle + \frac{\sqrt{3}}{2\sqrt{2}}|11\rangle$.

We measure the first bit. If it is $|0\rangle$ then the second bit is always $|0\rangle$. If is is $|1\rangle$ the second bit is $\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$.

# Quantum gates

$$\text{NOT-gate} = \text{Pauli-X} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

Corresponse to the rotation of a point on the Bloch sphere by $\pi$ radians around the x-axis. Also

$$\text{Pauli-Y} = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \text{ and Pauli-Z } = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

# Hadamard gate

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

Deals with a singular bit. Allows transformation of both $|0\rangle$ and $|1\rangle$ into states with equal probabilities.

# Phase-shift gate

$$\Theta = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{pmatrix}$$

Maps $|0\rangle$ to $|0\rangle$
Maps $|1\rangle$ to $e^{i\theta}|1\rangle$

# Example: Deutsch's algorithm

Solves contrived problem:
Given $f : \{0,1\} \to \{0,1\}$, determine if $f(0) = f(1)$.

Need one more concept:
$U_f(|x\rangle|y\rangle) = |x\rangle|y \oplus f(x)\rangle$

$U_f$ is a device whose inputs and outputs can be known, but there is no information about its internal structure.

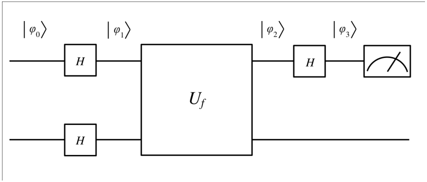



image credit: [5]

# Deutsch's algorithm

1. Take two qubits, in states $|0\rangle$ and $|1\rangle$. Then $|\phi_0\rangle = |0, 1\rangle$.

2. Apply Hadamard gate to both qubits to put them in a superposition of states. The state is now

$$|\phi_2\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \frac{|0\rangle - |1\rangle}{\sqrt{2}} = \frac{|0,0\rangle - |0,1\rangle + |1,0\rangle - |1,1\rangle}{2}.$$

# Deutsch's algorithm

3. Apply $U_f$ to get

$$
\begin{aligned}
|\phi_2\rangle &= U_f\left(\frac{|0,0\rangle - |0,1\rangle + |1,0\rangle - |1,1\rangle}{2}\right) \\
&= \frac{|0,0 \oplus f(0)\rangle - |0,1 \oplus f(0)\rangle + |1,0 \oplus f(1)\rangle - |1,1 \oplus f(1)\rangle}{2} \\
&= \frac{|0,f(0)\rangle - |0,\overline{f(0)}\rangle + |1,f(1)\rangle - |1,\overline{f(1)}\rangle}{2} \\
&= \left[\frac{(-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle}{\sqrt{2}}\right]\left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right] \\
&= \begin{cases} (\pm)\frac{|0\rangle+|1\rangle}{\sqrt{2}}\frac{|0\rangle-|1\rangle}{\sqrt{2}} & \text{if } f \text{ is constant,} \\ (\pm)\frac{|0\rangle-|1\rangle}{\sqrt{2}}\frac{|0\rangle-|1\rangle}{\sqrt{2}} & \text{if } f \text{ is balanced.} \end{cases}
\end{aligned}
$$

# Deutsch's algorithm

4. Apply Hadamard gate

$$|\phi_3\rangle = \begin{cases} (\pm)|0\rangle\frac{|0\rangle-|1\rangle}{\sqrt{2}} & \text{if } f \text{ is constant,} \\ (\pm)|1\rangle\frac{|0\rangle-|1\rangle}{\sqrt{2}} & \text{if } f \text{ is balanced.} \end{cases}$$

5. Measure the state of the first qubit. Measured result gives the solution of the initial problem.

# Applying quantum to ECDLP

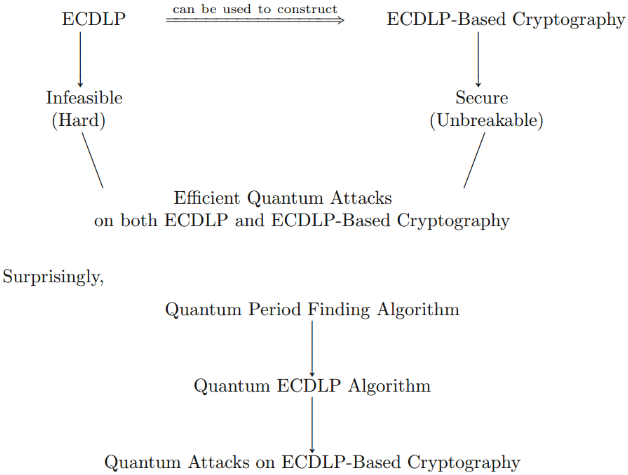



image credit: [6]

# Shor's algorithm introduction

Gven a natural number $N$, find its nontrivial factors.

The best classical factoring algorithm requires

$$O(e^{1,9(\log N)^{\frac{1}{3}}(\log\log N)^{\frac{2}{3}}}).$$

And Shor's factoring algorithm [8] is only

$$O(\log N^3).$$

# Shor's algorithm circuit

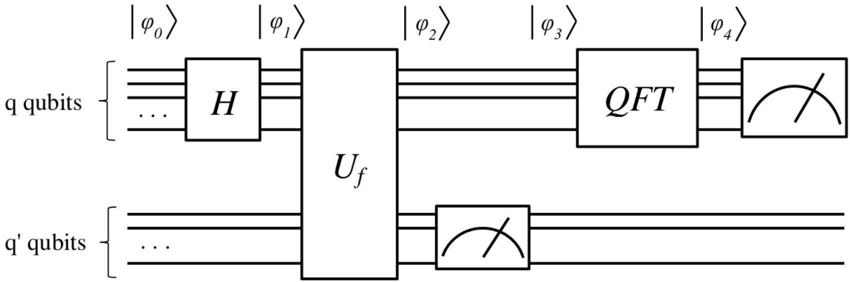



image credit: [5]

# Shor's algorithm [5]

1. Pick a random number $1 < a < N$ and compute the greatest common divisor $\gcd(a, N)$. This can be done efficiently with Euclid's algorithm[20]. If $\gcd(a, N) \neq 1$, congratulations, you are extremely lucky and don't even need a factoring algorithm; $\gcd(a, N)$ is a nontrivial factor of $N$.
If that is not the case, proceed to step 2.

2. Using a quantum computer, find the order of $a$ in the quotient group $(\mathbb{Z}/N\mathbb{Z})^\times$, i.e. the least natural number $r$ such that $a^r \equiv 1 \pmod N$. (Equivalently, find the period of the function $f(x) = a^x \pmod N$.)

3. If $2 \nmid r$ or $a^{\frac{r}{2}} \equiv -1 \pmod N$, go back to step 1.
Otherwise, $N|(a^r - 1) = (a^{\frac{r}{2}} + 1)(a^{\frac{r}{2}} - 1)$. Considering that $a^{\frac{r}{2}} \not\equiv -1 (\bmod N)$, and that $r$ is the order of $a$ in $(\mathbb{Z}/N\mathbb{Z})^\times$, it follows that $\gcd(a^{\frac{r}{2}} \pm 1, N)$ are nontrivial factors of $N$. (The existence of $a^{\frac{r}{2}}$ such that $a^{\frac{r}{2}} \not\equiv \pm 1 \pmod N$ is guaranteed by the Chinese remainder theorem[21]: Since $N$ is composite, odd, and not a prime power, there exist $p$ and $q$ such that $p, q > 2$, $\gcd(p, q) = 1$ and $N = pq$. From the Chinese remainder theorem it follows that there exists $x$ such that $x \equiv 1 \pmod p$ and $x \equiv -1 \pmod q$. It can be easily checked that $x^2 \equiv 1 \pmod N$ and $x \not\equiv \pm 1 \pmod N$.)

# Quantum algorithm comparisons [6]

Eicher-Opoku

$$O(n \log n + n\sqrt{p})$$

Proos-Zalka

$$O(\sqrt{n})$$

Kaye-Zalka

$$O(\sqrt{n})$$

# Algorithm comparisons [6]

| Quantum IFP | | | Quantum ECDLP | | | Classical |
|---|---|---|---|---|---|---|
| $\lambda$ | Qubits $2\lambda$ | Time $4\lambda^3$ | $\lambda$ | Qubits $7\lambda$ | Time $360\lambda^3$ | Time |
| 512 | 1024 | $0.54 \cdot 10^9$ | 110 | 700 | $0.5 \cdot 10^9$ | $c$ |
| 1024 | 2048 | $4.3 \cdot 10^9$ | 163 | 1000 | $1.6 \cdot 10^9$ | $c \cdot 10^8$ |
| 2048 | 4096 | $34 \cdot 10^9$ | 224 | 1300 | $4.0 \cdot 10^9$ | $c \cdot 10^{17}$ |
| 3072 | 6144 | $120 \cdot 10^9$ | 256 | 1500 | $6.0 \cdot 10^9$ | $c \cdot 10^{22}$ |
| 15360 | 30720 | $1.5 \cdot 10^{13}$ | 512 | 2800 | $50 \cdot 10^9$ | $c \cdot 10^{60}$ |

# Questions?

# References

[0] https://www.nsa.gov/ia/programs/suiteb_cryptography/
[1] http://www.ibtimes.co.uk/google-plans-watershed-quantum-computing-announcement-december-1528915
[2] http://www.wsj.com/articles/intel-to-invest-50-million-in-quantum-computers-1441307006
[3] http://www.hpcwire.com/off-the-wire/lanl-orders-1000-qubit-d-wave-2x-quantum-computer/
[4] http://jqi.umd.edu/news/how-do-you-build-large-scale-quantum-computer
[5] M. Kranjcevic, F. Kirsek, and P. Kunstek. Quantum Computing. White paper.
[6] S. Yan. *Quantum Attacks on Public-Key Crypto Systems*. Springer, 2013.
[7] D. Hankerson, A. Menezes, S. Vanstone. *Guide to Elliptic Curve Cryptography*. Springer, 2003.
[8] Peter Williston Shor (1959.-), American mathematician.