Break ECDSA using quantum computer

jhhope1

September 7, 2022

Outline

Review of ECDSA

- The Elliptic Curve Digital Signature Algorithm (ECDSA) is a private key-public key signing algorithm that uses elliptic curve cryptography.
- In Bitcoin, the wallet owner can only sign a withdrawal transaction using the wallet's private key. Verifier uses the public key to verify that the owner sent the transactions.

Review of ECDSA

Elliptic curve

Elliptic curve $E(\mathbb{F}_p)$ is the set of solutions $(x, y) \in \mathbb{F}_p \times \mathbb{F}_p$ to the equation

$$y^2 \equiv x^3 + ax + b \mod p$$

with point at infinity $\mathcal{O}$ with prime p

We can define group operation over E

Review of ECDSA

For $P = (x_1, y_1), R = (x_2, y_2) \in E$

$$P + \mathcal{O} = \mathcal{O} + P = P$$

$$P + R = \begin{cases} \mathcal{O} & \text{if } (x_1, y_1) = (x_2, -y_2) \\ (x_3, y_3) & \text{otherwise} \end{cases}$$

where $x_3 = \lambda^2 - (x_1 + x_2)$, $y_3 = \lambda(x_1 - x_3) - y_1$

$$\lambda = \begin{cases} (y_2 - y_1)/(x_2 - x_1) & \text{if } P \neq R \\ (3x_1^2 + a)/(2y_2) & \text{if } P = R \end{cases}$$

Review of ECDSA

From now, we only consider the cyclic subgroup of E generated by the base point P

Cyclic subgroup of E

Cyclic subgroup of E generated by the base point $P \in E$

$$(P) = \{nP \in E : n \in Z\}$$

$Q = dP = P + P + \cdots + P$ can be easily calculated in $O(\log d)$ for a large integer $d = d_1 \cdots d_n$

$$Q = \sum_{d_k=1} 2^{n-k} P$$

Review of ECDSA

Discrete Logarithm Problem

For a given points $P, Q \in G$ the DLP is to find the discrete logarithm $d = \log_P Q \in \mathbb{Z}$ such that $dP = Q$.

Elliptic Curve DLP(ECDLP) is a computationally hard problem for a classical computer. ECDSA uses d as a private key and $Q = dP$ as a public key.

Review of ECDSA

ECDSA Parameters

a, b: constants of the curve $y^2 = x^3 + ax + b$

P: base point that generates a subgroup of large prime order q

q: order of P

d: private key

Q: public key dP

m: message

Review of ECDSA

Signature generation (d, m)

- z $= L_q$ leftmost bits of $\mathrm{HASH}(m)$ where L_q is the bit length of order q
- Select integer k randomly from $[1, q-1]$
- $(x_1, y_1) = kP$
- $r = x_1 \mod q$
- Signature $= \big(r, k^{-1}(z + rd)\big)$

Signature verification ($Q = dP$, m, r, s)

- $u1 = zs^{-1} \mod q$, $u1 = rs^{-1} \mod q$
- $(x_1, y_1) = u_1P + u_2Q$. If $(x_1, y_1) = \mathcal{O}$ then the signature invalid
- signature is valid if $r \equiv x_1 \pmod q$ invalid otherwise

ECDLP

Solving ECDLP breaks ECDSA!

ECDLP

For a base point P and public key $Q = dP$, consider a periodic function f.

$$\begin{aligned} f : \mathbb{Z} \times \mathbb{Z} &\to E \\ (x, y) &\mapsto xP + yQ \end{aligned}$$

f has two independent periods $(q, 0)$ and $(d, -1)$ in the plane $\mathbb{Z} \times \mathbb{Z}$.

$$f(x + q, y) = f(x, y) \text{ and } f(x + d, y - 1) = f(x, y)$$

Quantum computer can solve this problem efficiently

Quantum Computer

How can quantum computers solve the super hard problems of classical computers?

1. A quantum computer is a device that performs calculations using qubits that correspond to bits in a classical computer.
2. A quantum state is a vector space with dimensions that increase exponentially with the number of qubits.
3. Quantum computers perform various operations on these quantum states, and use them to solve problems that classical computers cannot solve quickly.

Qubit

Qubit lives in 2-dimensional $\mathbb{C}$-vector (hilbert) space V with two orthonormal basis states $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ and $|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$.
Every state $|\psi\rangle$ is represented as a superposition(linear combination) of those basis.

$$|\psi\rangle = a\,|0\rangle + b\,|1\rangle = \begin{pmatrix} a \\ b \end{pmatrix}$$

where

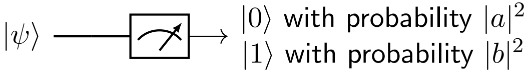
$$a, b \in \mathbb{C}$$
$$|a|^2 + |b|^2 = 1$$

Superposition and Measurement

When we measure the state

$$|\psi\rangle = a\,|0\rangle + b\,|1\rangle$$

the probability of outcome $|0\rangle$ is $|a|^2$ and the probability of outcome $|1\rangle$ is $|b|^2$. After the measurement state collapses to the corresponding outcome state.



1-Qubit quantum logic gate

From a Schrödinger equation's time evolution of a quantum state, quantum logic gates are unitary operators.

$$|\psi\rangle \ —\boxed{U}— \ |\phi\rangle = U|\psi\rangle$$

where

$$U^\dagger U = 1$$

Example. X gate

X gate flips quantum bit.

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \text{ or}$$

$$X(a|0\rangle + b|1\rangle) = b|0\rangle + a|1\rangle$$

1-Qubit quantum logic gate

Example. Y gate

Also flips quantum bit with different phase.

$$Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$$

Example. Phase shift gate

Shifts phase of $|1\rangle$ state by θ.

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

1-Qubit quantum logic gate

Example. Hadamard gate

Hadamard gate transforms the basis states into superposition states with probability 1/2 for each states.

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

or

$$H\left|x\right\rangle = \left|0\right\rangle + e^{\pi x i \left|1\right\rangle} \text{ where } x \in \{0, 1\}.$$

For example,

$$H\left|0\right\rangle = \frac{1}{\sqrt{2}}(\left|0\right\rangle + \left|1\right\rangle)$$

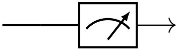
$$H\left|1\right\rangle = \frac{1}{\sqrt{2}}(\left|0\right\rangle - \left|1\right\rangle)$$

1-Qubit quantum logic gate

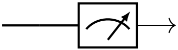
Question. Distinguish two states

Let $|\psi\rangle = \dfrac{|0\rangle + |1\rangle}{\sqrt{2}}$ and $|\phi\rangle = \dfrac{|0\rangle - |1\rangle}{\sqrt{2}}$

Distinguish two states.

$|\psi\rangle$ 

$|0\rangle$ with probability $1/2$
$|1\rangle$ with probability $1/2$

$|\phi\rangle$ 

$|0\rangle$ with probability $1/2$
$|1\rangle$ with probability $1/2$

We get the same probability distribution outcome if we measure two states directly.

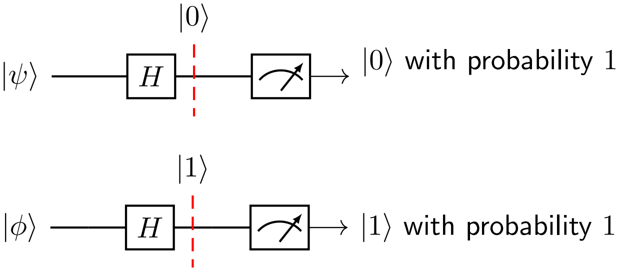
1-Qubit quantum logic gate

Question. Distinguish two states

Let $|\psi\rangle = \dfrac{|0\rangle + |1\rangle}{\sqrt{2}}$ and $|\phi\rangle = \dfrac{|0\rangle - |1\rangle}{\sqrt{2}}$

Distinguish two states.

Two states can be distinguished by applying the Hadamard gate.



2-Qubit state

Each of the two qubits lives in a different(but isomorphic) vector space V_1, V_2.
As a simple thought, we can think the set of two qubit states and operators below.

- A set of 2-qubit states must contain at least $(|\psi_1\rangle, |\psi_2\rangle)$ for all states $|\psi_1\rangle \in V_1$, $|\psi_2\rangle \in V_2$. (We call this separable state)
- A set of 2-qubit gates contain at least operators (U_1, U_2) for all unitary operators $U_1 \in \mathbf{U}(V_1)$, $U_2 \in \mathbf{U}(V_2)$ such that

$$
\begin{aligned}
(U_1, U_2) : V_1 \times V_2 &\to V_1 \times V_2 \\
(|\psi_1\rangle, |\psi_2\rangle) &\mapsto (U_1 |\psi_1\rangle, U_2 |\psi_2\rangle)
\end{aligned}
$$

2-Qubit state

However, there are unsatisfactory and critical problems with this set of states.

- If $V_1 \times V_2$ is a whole space of 2-Qubit states, 2-qubit states no longer forms a vector space.(Or not a useful interpretation).
- If $\mathbf{U}(V_1) \times \mathbf{U}(V_2)$ is a whole space of 2-Qubit gates, 2-qubit gate is not linear(these operators are not even bilinear).
- This set contains no **entangled states**.

2-Qubit state

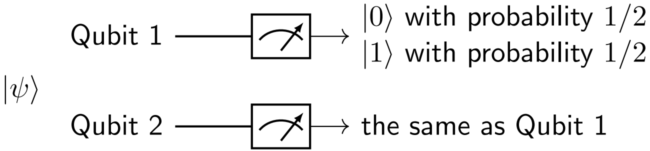
Surprisingly, there are **entangled states** in our nature.

Entangled state

An entangled state is a quantum state that cannot be factored in as a product of its local 1-qubit states.

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle|0\rangle + |1\rangle|1\rangle)$$

If we measure $|\psi\rangle$, we get entangled probability distribution.



2-Qubit state

So we can strongly guess that the space of 2-qubit states forms a vector space that takes operator (U_1, U_2) as a linear operator.

Tensor product

Let V_1 and V_2 be two vector spaces, with respective bases B_{V_1} and B_{V_2}. The tensor product $V_1 \otimes V_2$ is a vector space generated by $\{|j\rangle_1 \otimes |k\rangle_2 : |j\rangle_1 \in B_{V_1}, |k\rangle_2 \in B_{V_2}\}$

The tensor product of two vectors is defined below.

$$v \otimes w = \sum_{j,k} v_j w_k \, |j\rangle_1 \otimes |k\rangle_2$$

From now, we ignore subscript on the basis that represents the qubit number.

2-Qubit state

2-qubit space is $V \otimes V$.

$$|\psi\rangle = a_{00}|0\rangle \otimes |0\rangle + a_{01}|0\rangle \otimes |1\rangle + a_{10}|1\rangle \otimes |0\rangle + a_{11}|1\rangle \otimes |1\rangle$$
$$= \sum_{x_1, x_2=0}^{1} a_{x_1 x_2} |x_1\rangle \otimes |x_2\rangle$$

where $\sum_{x_1,x_2=0}^{1} |a_{x_1 x_2}|^2 = 1$

Conventions

We usually use binary form of non-negative integer x when expressing multiqubit basis.

2-Qubit basis notation

$$|x_1\rangle \otimes |x_2\rangle = |x_1\rangle\,|x_2\rangle = |x_1 x_2\rangle = |x\rangle$$

Where $x = x_1 x_{2(2)} = 2^1 \cdot x_1 + 2^0 \cdot x_2$

Example. $|2\rangle$ state

$$|1\rangle \otimes |0\rangle = |1\rangle\,|0\rangle = |10\rangle = |2\rangle$$

2-Qubit state

Let's rewrite the formulas using conventions

$$
\begin{aligned}
|\psi\rangle &= a_{00}|00\rangle + a_{01}|01\rangle + a_{10}|10\rangle + a_{11}|11\rangle \\
&= \sum_{x=0}^{2^2-1} a_x |x\rangle
\end{aligned}
$$

where $\sum_{x=0}^{2^2-1} |a_x|^2 = 1$

2-Qubit state

Tensor product of two states

Tensor product of two states $|\psi\rangle = a|0\rangle + b|1\rangle$, $|\phi\rangle = c|0\rangle + d|1\rangle$ is

$$\begin{aligned}
&|\psi\rangle \otimes |\phi\rangle \\
&= (a|0\rangle + b|1\rangle) \otimes (c|0\rangle + d|1\rangle) \\
&= ac|00\rangle + ad|01\rangle + bc|10\rangle + bd|11\rangle \\
&= ac|0\rangle + ad|1\rangle + bc|2\rangle + bd|3\rangle
\end{aligned}$$

2-Qubit state

Measurement on 2-qubit

How does a 2-qubit state collapse if we measure the first qubit?

2-Qubit state

Measurement on 2-qubit

How does a 2-qubit state collapse if we measure the first qubit?

If we measure the first qubit of the state $|\xi\rangle = a\,|0\rangle\,|\psi\rangle + b\,|1\rangle\,|\phi\rangle$, it will collapse to $|0\rangle \otimes |\psi\rangle$ with probability $|a|^2$ or $|1\rangle \otimes |\phi\rangle$ with probability $|b|^2$.

2-Qubit state

Example 1.

$$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \text{ measure 1st qubit} \rightarrow |00\rangle : 1/2,\ |11\rangle : 1/2$$

The second qubit of the collapsed state **depends on** the first qubit.

Example 2.

$$(a\,|0\rangle + b\,|1\rangle)\,|\phi\rangle \text{ measure 1st qubit } \rightarrow |0\rangle\,|\phi\rangle : |a|^2,\ |1\rangle\,|\phi\rangle : |b|^2$$

The second qubit of the collapsed state is **independent** of the first qubit.

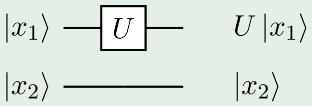
2-Qubit gates

Also, all unitary operators exists on 2-Qubit system.

Example. 1-qubit gate on 2-qubit system

It is of course possible to apply an arbitrary single gate U to the first qubit.

$$(U \otimes I) |x_1 x_2\rangle = U |x_1\rangle \otimes |x_2\rangle$$



2-Qubit gates

Example. CNOT gate

Controlled NOT gate flip second qubit if the first qubit is 1.

$$\mathrm{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

or equivalently,

$$\mathrm{CNOT}\,|x_1 x_2\rangle = |x_1\, x_1 \oplus x_2\rangle$$

where $x_k \in \{0, 1\}$ for all $k \in \{1, 2\}$

2-Qubit gates

Example. CPHASE gate

Controlled PHASE gate shifts phase of second qubit if the first qubit is 1.

$$\mathrm{CPHASE}_\theta = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & e^{i\theta} \end{pmatrix}$$

or equivalently,

$$\mathrm{CPHASE}_\theta \left|x_1 x_2\right\rangle = e^{i\theta x_1 x_2} \left|x_1 x_2\right\rangle$$

where $x_k \in \{0, 1\}$ for all $k \in \{1, 2\}$

n-Qubit states

In general, n-Qubit state lives in the tensor product space $V \otimes V \otimes \cdots \otimes V$ with dimension $N = 2^n$.
Thus, a quantum computer can operate over a high-dimensional $(N = 2^n)$ vector space with only a few (n) qubits.

$$\downarrow$$

Quantum Supremacy

Conventions

We usually use binary form of nonnegative integer x when expressing multiqubit basis.

n-Qubit basis notation

$$|x_1\rangle \otimes |x_2\rangle \otimes ... \otimes |x_n\rangle = |x_1\rangle |x_2\rangle ... |x_n\rangle = |x_1 x_2 ... x_n\rangle = |x\rangle$$

Where $x = x_1 x_2 ... x_{n(2)}$

Example. $|6\rangle$ state in 4-qubit system

$$|0\rangle \otimes |1\rangle \otimes |1\rangle \otimes |0\rangle = |0\rangle |1\rangle |1\rangle |0\rangle = |0110\rangle = |6\rangle$$

Conventions

Sometimes it is convenient to think of qubits as several groups. These groups are called quantum registers.

Quantum register

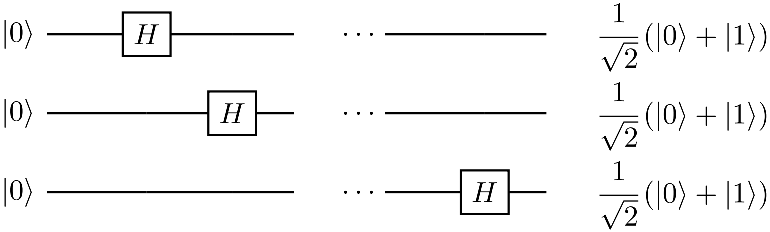
We call $|x\rangle$ and $|y\rangle$ quantum register.

$$\begin{aligned} &|x_1\rangle \otimes |x_2\rangle \otimes ... \otimes |x_l\rangle \otimes |y_1\rangle \otimes |y_2\rangle \otimes ... \otimes |y_m\rangle \\ &= |x_1x_2...x_l\rangle \otimes |y_1y_2...y_m\rangle = |x\rangle \otimes |y\rangle \\ &= |x\rangle |y\rangle = |x, y\rangle \end{aligned}$$

Where $x = x_1x_2...x_{l(2)}$, $y = y_1y_2...y_{m(2)}$

Quantum supremacy

We can generate the equal superposition of all basis.



$$
\begin{aligned}
&H \otimes H \otimes \cdots \otimes H \left|0\right\rangle \\
&= \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \cdots \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \\
&= \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle
\end{aligned}
$$

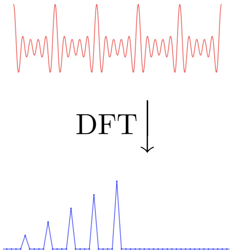
Quantum Fourier Transform

Discrete Fourier Transform

The discrete fourier transform of a sequence $\{A_x\}_{x=0}^{N-1}$ is defined by

$$\mathrm{DFT}(A)_y = \sum_{x=0}^{N-1} \frac{A_x e^{2\pi xyi}}{\sqrt{N}}$$

The DFT finds the period of a sequence.



Quantum Fourier Transform

Recall.

$\#$ of qubit $= n$
$\#$ of basis $= N = 2^n$
$y = y_1 y_2 ... y_{n(2)} = \sum_{k=1}^{n} y_k 2^{n-k}$
$|y\rangle = \bigotimes_{k=1}^{n} |y_k\rangle = y_1 \otimes y_2 \otimes ... \otimes y_n$

Quantum Fourier Transform

The QFT is the classical discrete Fourier transform applied to the coefficients of a quantum state.

$$\mathrm{QFT} : |x\rangle \mapsto \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} e^{\frac{2\pi x y i}{N}} |y\rangle$$

Quantum Fourier Transform

$$\mathrm{QFT}(|x\rangle) = \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} e^{\frac{2\pi x y i}{N}} |y\rangle$$

$$= \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} e^{2\pi i x \sum_{k=1}^{n} \frac{y_k}{2^k}} |y\rangle = \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} \prod_{k=1}^{n} e^{\frac{2\pi i x y_k}{2^k}} |y_1 y_2 \dots y_n\rangle$$

$$= \frac{1}{\sqrt{N}} (|0\rangle + e^{\frac{2\pi i x}{2^1}} |1\rangle) \otimes (|0\rangle + e^{\frac{2\pi i x}{2^2}} |1\rangle) \otimes \dots \otimes (|0\rangle + e^{\frac{2\pi i x}{2^n}} |1\rangle)$$

$\therefore \mathrm{QFT}(|x\rangle)$ is a separable state!

Quantum Fourier Transform

$$\mathrm{QFT}(|x\rangle) = \frac{1}{\sqrt{N}} \otimes_{k=1}^{n} \left(|0\rangle + e^{2\pi i x/2^k} |1\rangle \right)$$

Let's transform the 1st qubit first.

Remark

$$H|x_k\rangle = \frac{|0\rangle + e^{i\pi x_k} |1\rangle}{\sqrt{2}}$$

1. $|x_1\rangle \rightarrow \frac{|0\rangle + e^{\frac{2\pi i x_1}{2}} |1\rangle}{\sqrt{2}}$ by directly applying Hadamard gate.

Quantum Fourier Transfrom

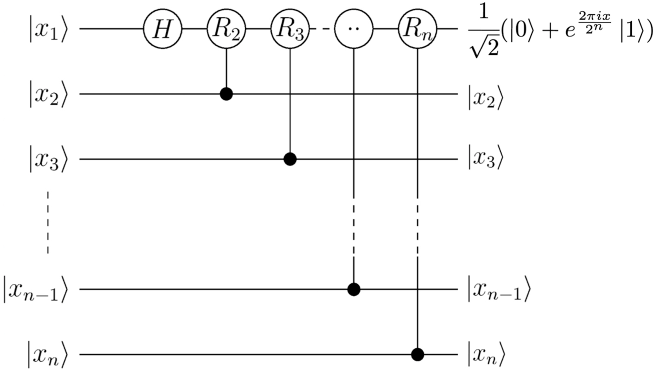
Remark

$$\mathrm{CPHASE}_\theta|x_k x_l\rangle = e^{i\theta x_k x_l}\,|x_k x_l\rangle$$

2. Shift phase of $|1\rangle$ by sequentially applying $R_k = \mathrm{CPHASE}_{\frac{2\pi i}{2^k}}$ gate controlled by the kth qubit for $k \in [2, n]$.

$$\begin{aligned}\frac{|0\rangle + e^{\frac{2\pi i x_1}{2}}\,|1\rangle}{\sqrt{2}} \rightarrow &\frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\, e^{2\pi i x/2^n}\right) \\ &= \frac{1}{\sqrt{2}}\left(|0\rangle + \prod_{k=1}^{n} e^{2\pi i x_k/2^k}\,|1\rangle\right)\end{aligned}$$

Figure: Transformation of first qubit



Quantum Fourier Transform

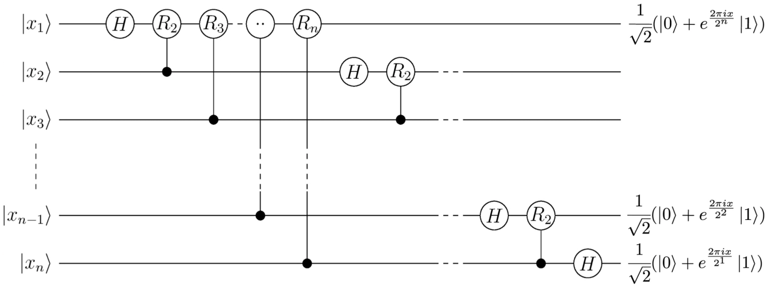
From the equation below,

$$e^{\frac{2\pi xi}{2^k}} = e^{\sum_{l=1}^{n} 2\pi i x_l/2^{n-k-l}} = e^{\sum_{l=n-k+1}^{n} 2\pi i x_l/2^{n-k-l}}$$

we only need the information of $x_{l\in[n-l+1,n]}$ when transforming the kth qubit.
QFT can be implemented by sequentially applying a gate sequence similar to the one above.

Quantum Fourier Transform

Figure: QFT with the reversed bit order



Shor's Algorithm - DLP

Recall. Periodic function f on a plane

Let P be a generator of a group $G = (P)$ of prime order q and $Q = dP$ be a element of G. Then $f : \mathbb{Z}_q \times \mathbb{Z}_q \to G$ is a periodic function where

$$f(x, y) = xP + yQ$$

With period $(d, -1)$

Suppose that we can generate the following state $|\psi\rangle$ with three register.

$$|\psi\rangle = \frac{1}{q} \sum_{x,y=0}^{q-1} |x, y, xP + yQ\rangle$$

Shor's Algorithm - DLP

$$|\psi\rangle = \frac{1}{q}\sum_{x,y=0}^{q-1} |x, y, xP + yQ\rangle = \sum_{z'} c_{z'} |\phi_{z'}\rangle |z'P\rangle$$

Measure the last register $\rightarrow$ Obtain a random element $zP \in G$.
First two registers collapse in a superposition of all x, y with

$$xP + yQ = (x + dy)P = zP$$

Thus for each y there is exactly one solution of $x = z - dy \mod q$. So the state of the first two register is

$$\frac{1}{\sqrt{q}}\sum_{y=0}^{q-1} |z - dy \mod q, y\rangle$$

Shor's Algorithm - DLP

$$\frac{1}{\sqrt{q}} \sum_{y=0}^{q-1} |z - dy \mod q, y\rangle$$

Apply QFT(with order q) of the two registers.

$$\frac{1}{q^{3/2}} \sum_{x',y'=0}^{q-1} \sum_{y=0}^{q-1} e^{\frac{2\pi i((z-dy)x'+yy')}{q}} |x', y'\rangle$$

Coefficient of $|x', y'\rangle$ only survives if $y' = dx' \mod q$

$$\sum_{y=0}^{q-1} e^{\frac{2\pi i((z-dy)x'+yy')}{q}} = \begin{cases} qe^{\frac{2\pi i z x'}{q}} & \text{if } y' = dx' \mod q \\ 0 & \text{otherwise} \end{cases}$$

Shor's Algorithm - DLP

Finally, if we measure the two remaining registers, we obtain x', y' with $y' = dx'$.

$$\log_P Q = d = y' x'^{-1}$$

Now, we exploitted the private key d!
Using a Fourier transform of order $2^n \simeq q$ instead of q gives a good probability of gettting the right values in $\mathbb{Z}_q^2$ by rounding.

Elliptic Curve Discrete Logarithm Problem

If we can generate state ψ we can also solve ECDLP.

$$|\psi\rangle = \frac{1}{N} \sum_{x,y=0}^{N} |x, y, xP + yQ\rangle$$

Elliptic Curve Discrete Logarithm Problem

It is known that the following **modular arithmetics** of quantum numbers are efficiently (in polynomial time) implemented on a quantum computer.

Addition (`mod_add`)	$\|x, y\rangle \mapsto \|x, y, x + y \mod p\rangle$
Doubling (`mod_dbl`)	$\|x, y\rangle \mapsto \|x, y, 2x \mod p\rangle$
Multiplication (`mod_mul`)	$\|x, y\rangle \mapsto \|x, y, xy \mod p\rangle$
Inverse (`mod_inv`)	$\|x\rangle \mapsto \|1/x \mod p\rangle$

Elliptic Curve Discrete Logarithm Problem

Addition on elliptic curve can be implemented with operations mentioned above.

Group shift

Elliptic curve group operation for a fixed element $A \in E$ can be implemented in "general" case using modular operations.

$$U_A : |S\rangle \to |S + A\rangle$$

where $S = (x_S, y_S), A = (x_E, y_E) \in E, S,\ A \neq \mathcal{O},\ S + A \neq \mathcal{O},\ S \neq \pm A$
Controlled group operation controlled by a kth qubit is also possible.

$$\text{Controlled } U_A \, |x_k, S\rangle = |x_k, S + x_k A\rangle$$

Elliptic Curve Discrete Logarithm Problem

$2^k P$ and $2^k Q$ are easily calculated by a classical computer. Then, we can generate $|\psi\rangle = \sum_{x,y=0}^{N} |x, y, xP + yQ\rangle$ as follows.

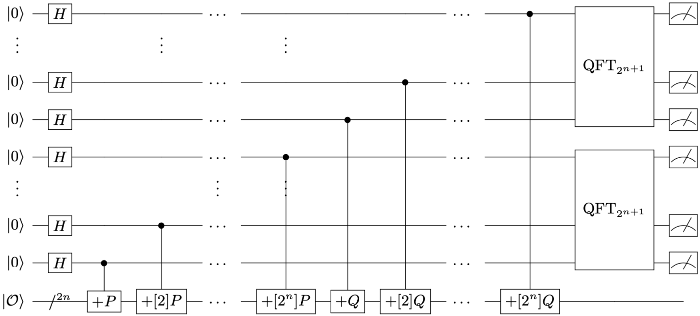
- Apply hadamard gates to the first and second registers.
- Apply $U_{2^{n-k}P}$ to the third register using the kth qubit of the first register as the control qubit.
- Do the same with the qubits in the second register as the control qubit.

Elliptic Curve Discrete Logarithm Problem

A point of infinity($|\mathcal{O}\rangle$) is not the general case mentioned above, so it cannot perform valid group operations.
We use the trick of setting the third register to kP for a random $k \in [0, q]$.
Then only $O(1/q)$ of states in one group shift is invalid.
$2n$ group shifts do not significantly affect the overall fidelity.
Also, initialize register does not affect the QFT.
$\therefore$ **Quantum computers can break ECDLP.**

Elliptic Curve Discrete Logarithm Problem

Figure: Quantum circuit of ECDLP solver



Elliptic Curve Discrete Logarithm Problem

Figure: Quantum resources to break ECDSA vs RSA

ECDLP in $E(\mathbb{F}_p)$ simulation results					Factoring of RSA modulus N interpolation from [21]		
$\lceil \log_2(p) \rceil$ bits	#Qubits	#Toffoli gates	Toffoli depth	Sim time sec	$\lceil \log_2(N) \rceil$ bits	#Qubits	#Toffoli gates
110	1014	$9.44 \cdot 10^9$	$8.66 \cdot 10^9$	273	512	1026	$6.41 \cdot 10^{10}$
160	1466	$2.97 \cdot 10^{10}$	$2.73 \cdot 10^{10}$	711	1024	2050	$5.81 \cdot 10^{11}$
192	1754	$5.30 \cdot 10^{10}$	$4.86 \cdot 10^{10}$	1 149	–	–	–
224	2042	$8.43 \cdot 10^{10}$	$7.73 \cdot 10^{10}$	1 881	2048	4098	$5.20 \cdot 10^{12}$
256	2330	$1.26 \cdot 10^{11}$	$1.16 \cdot 10^{11}$	3 848	3072	6146	$1.86 \cdot 10^{13}$
384	3484	$4.52 \cdot 10^{11}$	$4.15 \cdot 10^{11}$	17 003	7680	15362	$3.30 \cdot 10^{14}$
521	4719	$1.14 \cdot 10^{12}$	$1.05 \cdot 10^{12}$	42 888	15360	30722	$2.87 \cdot 10^{15}$

Impact on blockchains

- ECDSA is used to encrypt transactions on most blockchains (BTC, ETH, ...), and it could be broken if high-fidelity quantum computers are developed.
- However, since POW itself uses a hash function, and a sufficiently complex hash function is known to be quantum-safe, the consensus of the chain used is safe.

Post-Quantum Cryptography

The following encryption algorithms are known to be quantum-safe so far.

- Hash based
- Lattice-based cryptography
- Multivariate cryptography
- Code-based cryptography

References

- Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer.
- Shor's discrete logarithm quantum algorithm for elliptic curves
- Quantum Networks for Elementary Arithmetic Operations
- Quantum Resource Estimates for Computing Elliptic Curve Discrete Logarithms