Pre- and Post-Quantum Elliptic Curve Cryptography

Part B: Structured Project

Aditya Mittal

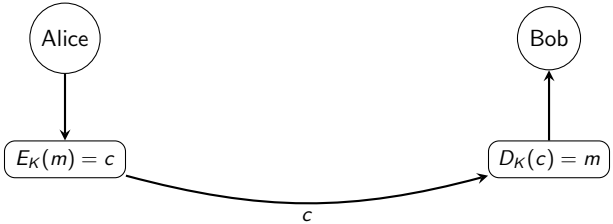
September 6, 2025

Overview

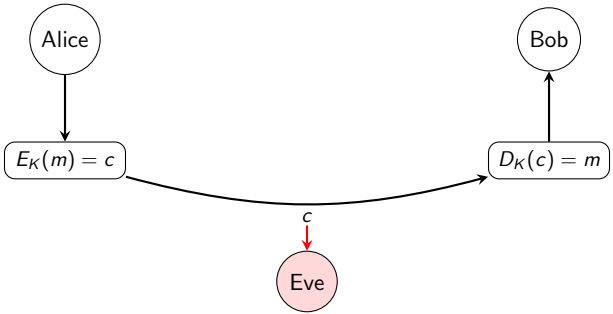
1. Cryptography Basics and The Discrete Logarithm Problem
2. Classic Elliptic Curve Cryptography
3. The Quantum Threat and Shor's Algorithm
4. A Post-Quantum Solution

Cryptography Basics and The Discrete Logarithm Problem

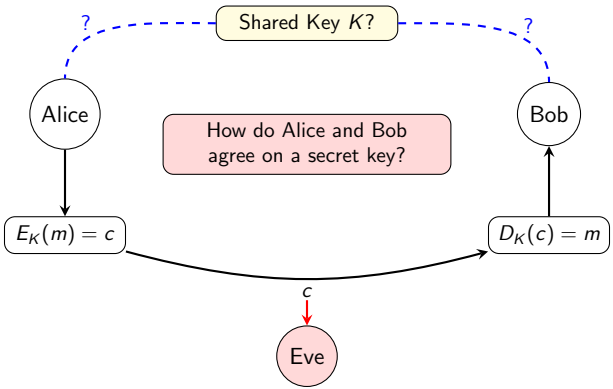
A Challenge with Secrecy



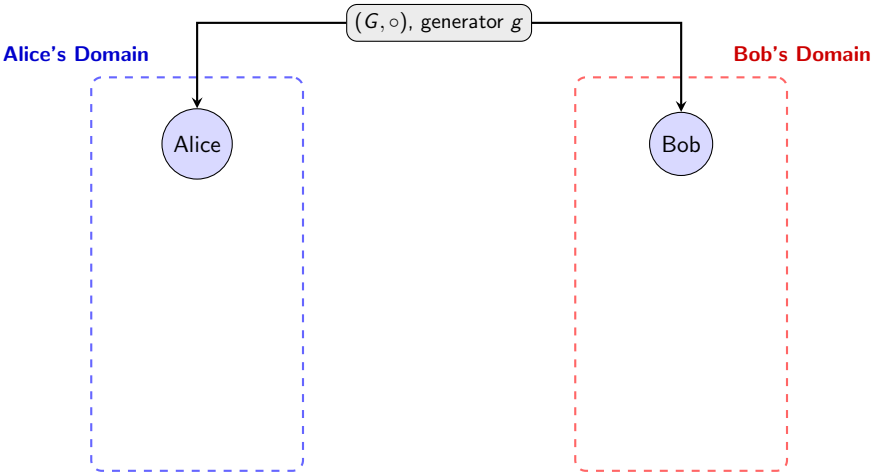
A Challenge with Secrecy



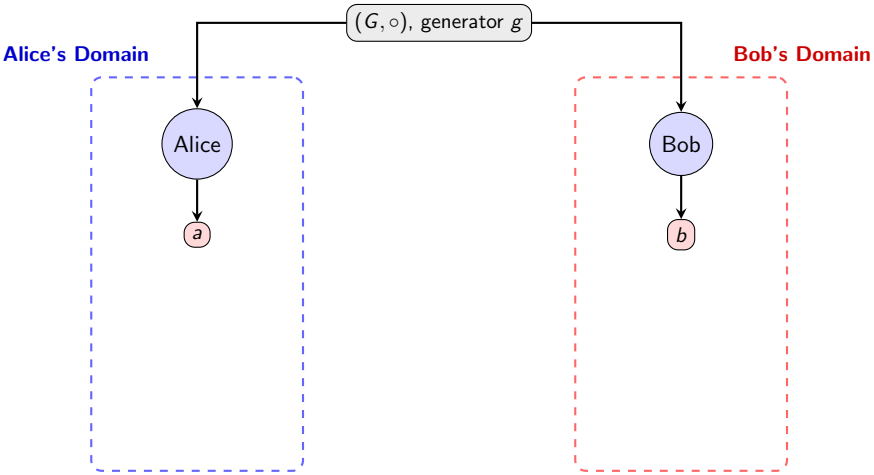
A Challenge with Secrecy



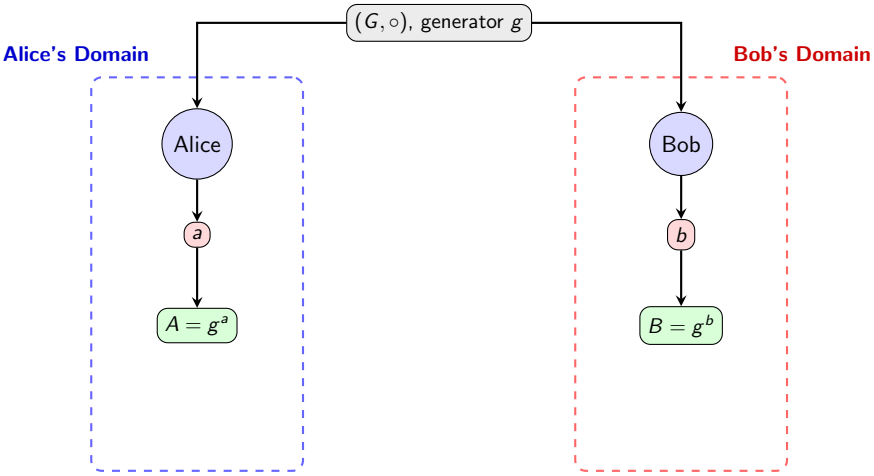
The Diffie-Hellman Key Exchange



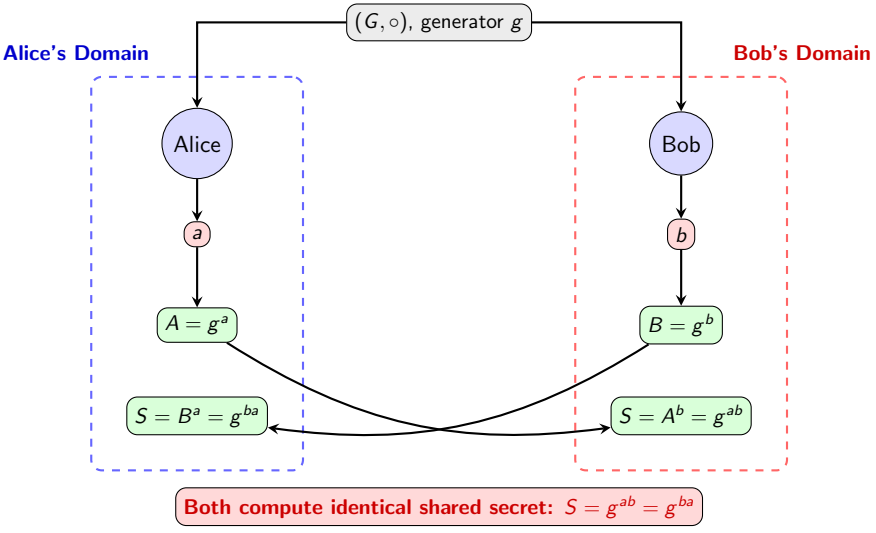
The Diffie-Hellman Key Exchange



The Diffie-Hellman Key Exchange



The Diffie-Hellman Key Exchange



The Discrete Logarithm Problem

- Attackers can still hear encoded information $A = g^a, B = g^b$ sent over the channel
- If they can somehow recover either a or b, they could then can recover $S = A^b = B^a$

The Discrete Logarithm Problem

Given a group $G = \langle g \rangle$, an element $h = g^x$, can we recover $\log_g h = x$ efficiently?

- If the answer is yes, Alice and Bob are in trouble

Examples

Solving DLP in $(\mathbb{Z}_n, +)$ is easy: we want to solve $xg \equiv h \bmod n$. So we want to find $x = g^{-1}h \bmod n$, and we can find $g^{-1} \bmod n$ in $O((\log n)^2)$ with the Euclidean algorithm if $\gcd(g, n) = 1$. Else there is not a solution.

Remark

Factoring is another thought-to-be-hard problem: it is easy to multiply $pq = N$, but factoring N into p, q is hard.

Classic Elliptic Curve Cryptography

Definition: Elliptic Curve (Weierstrass Form)

Let $\mathbb{K}$ be a field, and $a, b, c \in \mathbb{K}$. An *elliptic curve over* $\mathbb{K}$, denoted $E/\mathbb{K}$, is an equation of one of the following forms based on $\mathrm{Char}(\mathbb{K})$:

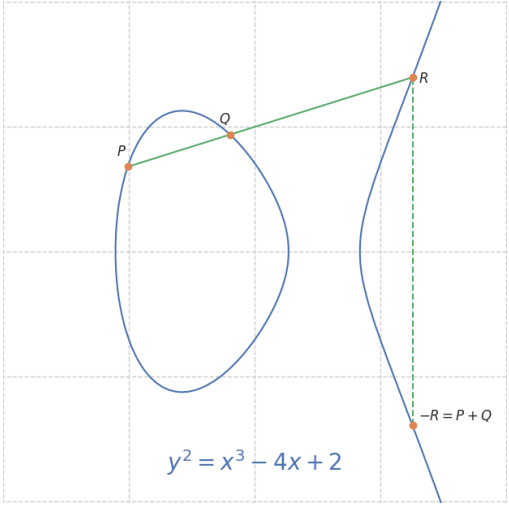
$$\begin{cases} \mathrm{Char}(\mathbb{K}) = 2: & y^2 + cy = x^3 + ax + b \\ \mathrm{Char}(\mathbb{K}) = 3: & y^2 = x^3 + ax^2 + bx + c \\ \mathrm{Char}(\mathbb{K}) > 3: & y^2 = x^3 + ax + b \end{cases}$$

Let $E(\mathbb{K}) = \{(x, y) \in \mathbb{K}^2 : (x, y) \text{ satisfy } E\} \cup \{\infty\}$ where we include an element ∞ called the "point at infinity".

- For convenience, we assume $\mathrm{Char}(\mathbb{K}) > 3$, but all methods are easily adapted.

Group Law for Elliptic Curves

- There is a nice geometric way to define a group over $E(\mathbb{K})$.



Group Law for Elliptic Curves

The Group $(E(\mathbb{K}), \oplus)$

Let $P = (x_P, y_P)$, $Q = (x_Q, y_Q)$.

- Identity: $P \oplus \infty = \infty \oplus P = P$
- Inverses: $-P = (x_P, -y_P)$. If $P = \infty$, then $-P = \infty$.
- Addition: If $P \neq Q$, define

$$P \oplus Q = \left(\left(\frac{y_Q - y_P}{x_Q - x_P} \right)^2 - x_P - x_Q, -\left(\frac{y_Q - y_P}{x_Q - x_P}(x_R - x_P) + y_P \right) \right)$$

If $P = Q$, let

$$P \oplus P = \left(\left(\frac{3x_P^2 + a}{2y_P} \right)^2 - 2x_P, -\left(\frac{3x_P^2 + a}{2y_P}(x_R - x_P) + y_P \right) \right)$$

The Quantum Threat and Shor's Algorithm

The Quantum Threat and Q-Day

- Elliptic curves promise an efficient speedup of certain cryptographic schemes
- However, we have assumed a very simple model of computation
- That is not what the future necessarily holds

Shor's Algorithm

There is an algorithm* that solves DLP and factoring in $O((\log n)^3)$.

The Quantum Threat and Q-Day

- Elliptic curves promise an efficient speedup of certain cryptographic schemes
- However, we have assumed a very simple model of computation
- That is not what the future necessarily holds

Shor's Algorithm

There is an algorithm* that solves DLP and factoring in $O((\log n)^3)$.

*However, it is a *quantum algorithm*

Introduction to Quantum Computing

- Classical bits: are either 0 or 1
- Quantum bits (a.k.a. *qubits*): infinitely many *in-between* states of 0 and 1
- Formally, qubits are vectors $|v\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$ for $\alpha, \beta \in \mathbb{C}$
- Upon *measuring* $|v\rangle$, we get $|0\rangle$ with probability $|\alpha|^2$ and $|1\rangle$ with probability $|\beta|^2$
- When $\alpha, \beta \neq 0$, say $|v\rangle$ is in *superposition*

Remark

This is the key to *almost all* of quantum mechanics! Working in this modified probability space implies most quantum results theoretically.

- Unitary maps act as logic gates; fundamental operations.

Quantum Parallelism

- So what?
- Let $f : \{0,1\} \to \{0,1\}$ be the function $f(x) = 1 - x$
- Consider unitary $U_f : |x\rangle \to |f(x)\rangle$
- Look at the following:

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

- With *one* use of U_f i.e. one use of f, we got *two* values of f!
- Extends: one use of U_f can give $\sum |n\rangle\, |f(n)\rangle$

Example Problem

Order-Finding Problem

Given $\gcd(a, N) = 1$, can we find minimal r such that $a^r = 1 \bmod N$?

- **Classically**: no fast solution
- **Quantum**: yes with parallelism $\sum |t\rangle |a^t \bmod N\rangle$

Remark

Shor's algorithm is a reduction of factoring to order-finding. Similarly, it reduces DLP to a similar period-finding problem.

A Post-Quantum Solution

Isogeny-Based Cryptography

- One major direction being explored is with *isogeny-graphs*
- The suggested problem: find a path in a graph *without* already being given the edges
- Nodes = Elliptic groups up to isomorphism
- Edges = Homomorphisms

A Bit More on Isogenies

- Fancy word for (rational) homomorphism $\phi : E_1(\overline{\mathbb{K}}) \to E_2(\overline{\mathbb{K}})$
- Elliptic curves as groups endow lots of structure onto isogenies

Proposition

All isogenies are surjective.

Theorem

For every finite subgroup $G \leq E(\overline{\mathbb{K}})$, there exists a unique elliptic curve E/G and isogeny $\phi : E \to E/G$ with $\ker \phi = G$.

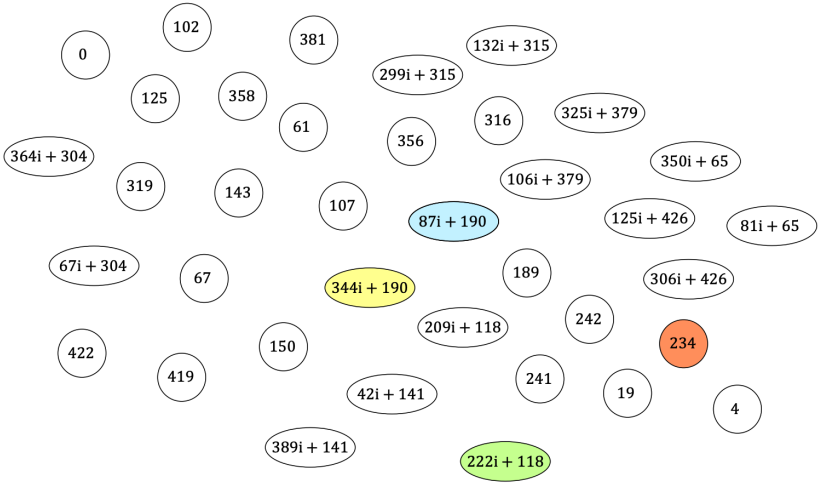
Examples

- The multiplication-by-n map $[n](P) = nP$ is an endomorphism.
- (Frobenius map) If $\mathrm{Char}(\mathbb{K}) = p$, then $\Phi_p(x, y) = (x^p, y^p)$ is an isogeny between $E : y^2 = x^3 + ax + b$ and $E^{(p)} : y^2 = x^3 + a^p x + b^p$.

Supersingular Isogeny Diffie-Hellman (SIDH)

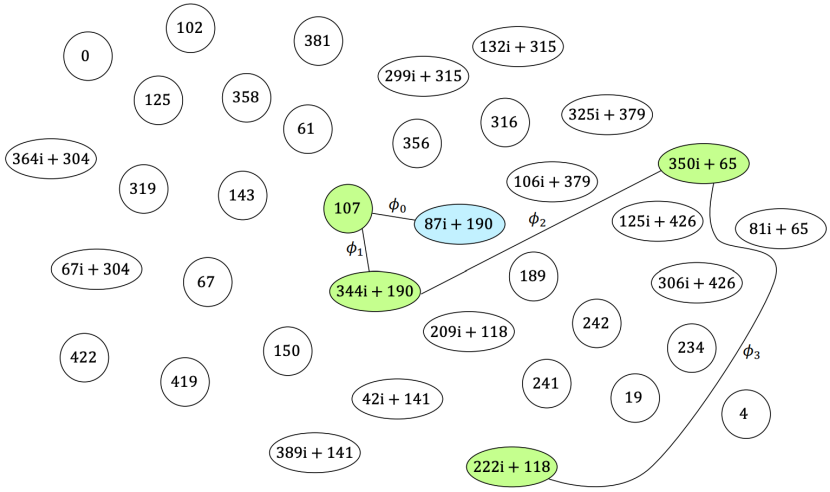
- As the name suggests, this is a generalization of classical Diffie-Hellman using highly connected isogeny graph
- Consider all isomorphism classes of over field of characteristic p
- Idea: Alice and Bob take random walks over the graph with different degree isogenies, and arrive at a common elliptic curve.

An Example

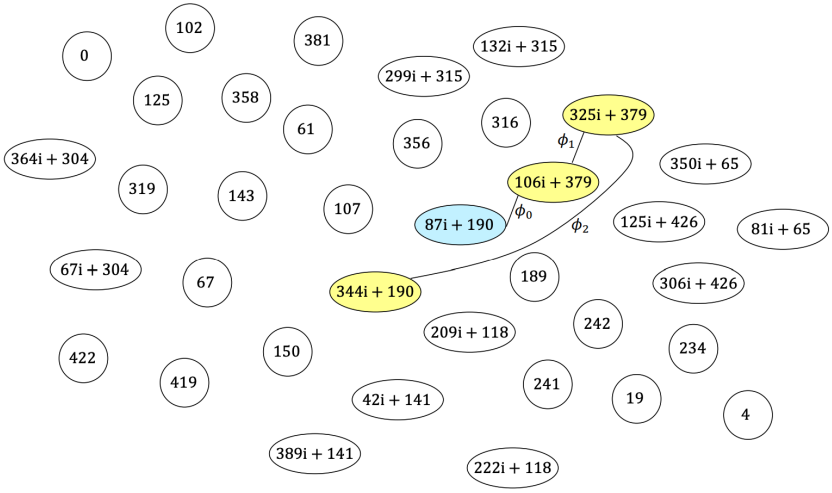


Costello, C. (2019). Supersingular isogeny key exchange for beginners. Cryptology ePrint Archive, Report 2019/1321, Figures 1,7,8,9,10. https://eprint.iacr.org/2019/1321.pdf

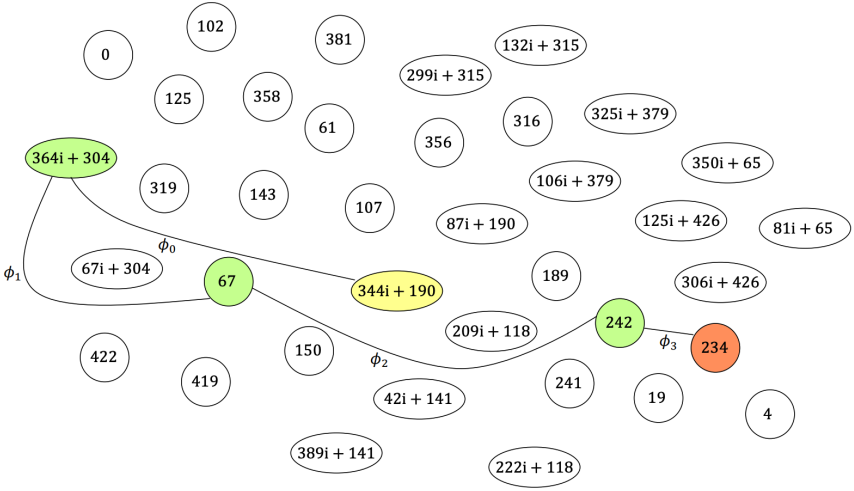
Alice's Public Key



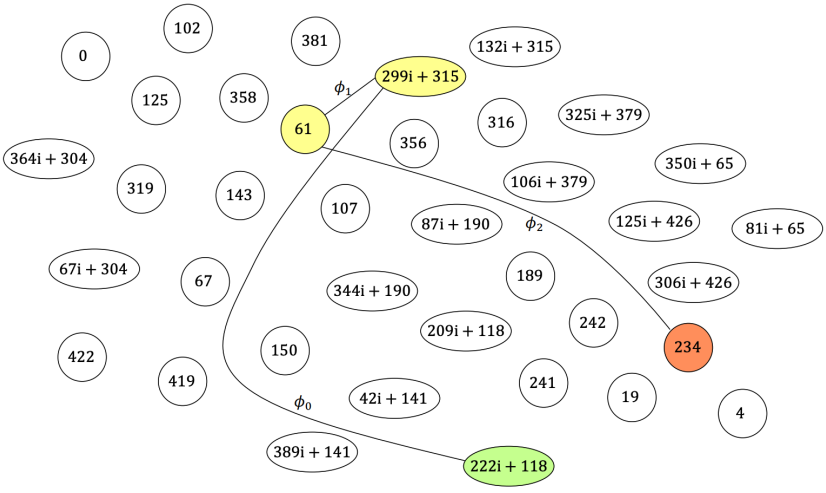
Bob's Public Key



Alice's Shared Computation



Bob's Shared Computation



Set Up

- **Public:**
  - Primes $p, p_a^{e_a}, p_b^{e_b}$
  - Initial curve $E/\mathbb{F}_{p^2}$
  - Torsion subgroups $E[p_a^{e_a}] = \langle P_a, Q_a \rangle$ and $E[p_b^{e_b}] = \langle P_b, Q_b \rangle$
- **Alice:**
  - **Secret:** $A = P_a + [m_a]Q_a$, $\alpha : E \to E/\langle A \rangle$
  - **Exchange:** $\{E/\langle A \rangle, \alpha(P_b), \alpha(Q_b)\}$
- **Bob:**
  - **Secret:** $B = P_b + [m_b]Q_b$, $\beta : E \to E/\langle B \rangle$
  - **Exchange:** $\{E/\langle B \rangle, \beta(P_a), \beta(Q_a)\}$
- **Shared Secret:** Curve $(E/\langle A \rangle)/\langle \alpha(B) \rangle \cong E/\langle A, B \rangle \cong (E/\langle B \rangle)/\langle \beta(A) \rangle$

More on SIDH

Isogeny Computation Problem

Given two elliptic curves E, E' over a finite field that are isogenous of degree d, find an isogeny $\phi : E \to E'$ with $\deg(\phi) = d$.

- Like DLP and DH, solving ICP solves SIDH
- Thought to be hard in general for quantum computers

More on SIDH

Isogeny Computation Problem

Given two elliptic curves E, E' over a finite field that are isogenous of degree d, find an isogeny $\phi : E \to E'$ with $\deg(\phi) = d$.

- Like DLP and DH, solving ICP solves SIDH
- Thought to be hard in general for quantum computers

- Unfortunately, this does not really matter for SIDH
- SIDH was broken with a *classical attack* in July 2022 exploiting the auxiliary points $\{\alpha(P_b), \alpha(Q_b)\}$ in the exchange.

Conclusion

- Elliptic curves bridge the abstract nature of geometry with computationally nice algebra

Conclusion

- Elliptic curves bridge the abstract nature of geometry with computationally nice algebra
- Shor's algorithm and Q-Day hold some weight, but we still have some time

Conclusion

- Elliptic curves bridge the abstract nature of geometry with computationally nice algebra
- Shor's algorithm and Q-Day hold some weight, but we still have some time
- Good considering we still have some techniques to iron out

Shor's Algorithm

We want to factor integer N.

1. Pick random a, and compute $\gcd(a, N) = d$.
2. If $d > 1$, done!
3. If $d = 1$, then $a \in \mathbb{Z}_N^\times$ i.e. $\exists r$ minimal such that $a^r = 1 \bmod N$.
4. If r is even, then $N \mid a^r - 1 = (a^{r/2} - 1)(a^{r/2} + 1)$.
5. $N \nmid a^{r/2} - 1$ by choice of r. So if $\gcd(N, a^{r/2} - 1) > 1$, done!
6. If $\gcd(N, a^{r/2} - 1) = 1$, then $\gcd(N, a^{r/2} + 1) = N$, so try again.

Generalized Shor's Algorithm

1. Initialize two registers $|0\rangle\,|0\rangle$.
2. Uniform superposition with QFT:

$$|0\rangle\,|0\rangle \mapsto \frac{1}{\sqrt{|G|}} \sum_{g\in G} |g\rangle\,|0\rangle$$

3. Apply f to the second register with U_f:

$$\frac{1}{\sqrt{|G|}} \sum_{g\in G} |g\rangle\,|0\rangle \mapsto \frac{1}{\sqrt{|G|}} \sum_{g\in G} |g\rangle\,|f(g)\rangle = \frac{1}{\sqrt{|G|}} \sum_{g\in G} |g\rangle \left(\sqrt{\frac{|H|}{|G|}} \sum_{\ell\in H^\perp} \overline{\chi_\ell(g)}\,|\hat{f}(\ell)\rangle \right)$$

4. Apply QFT^{-1} to first register:

$$\sqrt{\frac{|H|}{|G|}} \sum_{\ell\in H^\perp} \left(\frac{1}{\sqrt{|G|}} \sum_{g\in G} \overline{\chi_\ell(g)}\,|g\rangle \right) |\hat{f}(\ell)\rangle \xrightarrow{\mathtt{QFT}^{-1}} \sqrt{\frac{|H|}{|G|}} \sum_{\ell\in H^\perp} |\ell\rangle\,|\hat{f}(\ell)\rangle$$

5. Measure the first register to obtain a random $\ell \in H^\perp$, which gives information on H.
6. Repeat steps 1–6 until H can be determined via the linear relations of $H^\perp$.