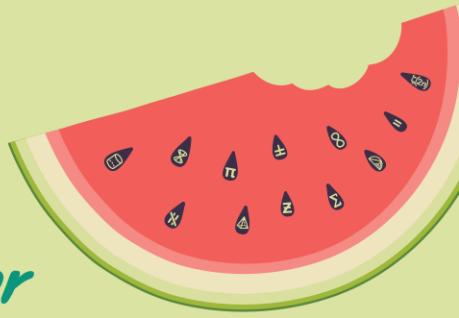
AMSI SUMMER RESEARCH SCHOLARSHIPS 2024–25

Get a taste for Research this Summer



Post-Quantum Cryptography

Shirley Wang

Supervised by Professor Nalini Joshi

The University of Sydney

Jane Street®

AMSI AUSTRALIAN MATHEMATICAL SCIENCES INSTITUTE

Abstract

Shor's algorithm threatens to break classical cryptographic protocols by factoring integers in polynomial time using the quantum Fourier transform (QFT). However, extending this to non-abelian groups is challenging due to the multidimensional nature of their irreducible representations. We propose a cryptographic protocol based on non-abelian groups, such as Okamoto curves, leveraging their structural complexity for enhanced security against quantum attacks. This approach underscores the potential of non-abelian group-based cryptosystems as candidates for post-quantum security.

Statement of Authorship The descriptions of RSA, Shor's algorithm, and Okamoto curves are based on the original papers. The idea for the cryptographic protocol and the analysis of the limitations of Shor's algorithm is our own work.

Acknowledgements I would like to thank my supervisor, Nalini, for her support throughout this project. Our weekly meetings were both productive and insightful, making one of my first forays into mathematical research really enjoyable. Her feedback, particularly on the conference presentation and the report, was invaluable in refining my work.

Contents

1 Introduction

Public-key cryptography relies on the computational hardness of integer factorisation and discrete logarithm problems, both of which are compromised by Shor's quantum algorithm. Shor's method employs the quantum Fourier transform (QFT) threatens to solve these problems in polynomial time. Recent progress in quantum hardware, such as Amazon and Microsoft's quantum chip prototypes, suggests that cryptographically relevant quantum computers may emerge sooner than previously anticipated. This risk is compounded by "harvest now, decrypt later" attacks, where adversaries collect encrypted data for future decryption. In response, the Australian Signals Directorate mandates transition to quantum-resistant cryptosystems by 2030 [7].

While Shor's algorithm efficiently solves the Hidden Subgroup Problem (HSP) for abelian groups via the QFT, non-abelian groups—which lack commutativity—resist such attacks. The HSP for non-abelian groups remains an open problem with current quantum techniques, making them candidates for post-quantum cryptography. We propose a protocol based on non-abelian platform groups, such as translation groups over Okamoto curves, in effort to demonstrate the potential of non-abelian groups for post-quantum cryptography.

However, challenges remain. Security arguments for cryptographic protocols often rely on heuristic assumptions rather than formal hardness proofs. Further, recursive group operations in our protocol introduce computational overhead, limiting practicality. Additionally, current post-quantum cryptographic efforts have prioritised lattice-based schemes, leaving non-abelian approaches understudied despite their potential to diversify post-quantum security.

2 Public Key Cryptography

Cryptography is the study of constructing and analysing protocols that ensure secure communication in the presence of adversarial behavior. Before the 1970s, cryptographic methods relied primarily on classical ciphers, which required a pre-shared secret key for encryption and decryption. These systems can be likened to a strongbox with a combination lock: both sender and receiver must securely agree on a key before exchanging messages. However, the necessity of a secure key distribution channel posed a fundamental challenge to scalability and security.

Public key cryptography shifted this paradigm by introducing asymmetric key pairs—one for encryption and another for decryption. While these keys are mathematically related, it must

be computationally hard to derive the decryption key from the encryption key. This asymmetry enables the encryption key to be publicly shared, allowing anyone to encrypt messages, while only the intended recipient, possessing the corresponding private key, can decrypt them.

This concept can be visualised as a strongbox with two distinct locks: one for securing and another for unlocking. By making the locking mechanism (encryption key) public, anyone can securely store information, yet only the intended recipient, with the unlocking key, can retrieve it.

A popular implementation of public key cryptography is discussed next.

2.1 RSA Cryptosystem

Introduced by Rivest, Shamir, and Adleman in 1977 [6], the RSA cryptosystem is a cornerstone of modern cryptography, relying on the computational hardness of integer factorisation. Its security is based on the infeasbility of deriving private keys from public information within a reasonable timeframe using classical computing.

To illustrate the RSA protocol, consider Alice, Bob, and Eve. Bob wishes to send Alice a secure message over an insecure channel, while Eve, an eavesdropper, attempts to intercept and decipher it. The RSA algorithm enables Bob to communicate securely with Alice despite Eve's presence.

RSA Encryption and Decryption

Alice		**Bob**
$n \leftarrow pq$		
$\varphi(n) = (p-1)(q-1)$		$m \in [0, n)$
$e \in (1, \varphi(n)), \gcd(e, \varphi(n)) = 1$		
	$\xrightarrow{(n,e)}$	
		$\mathrm{C} \leftarrow m^e \mod n$
	$\xleftarrow{C}$	
$d \leftarrow e^{-1} \mod \varphi(n)$		
$m \leftarrow C^d \mod n$		

Key generation begins with Alice selecting two large primes, p and q, and computing their product n, which defines the arithmetic domain for encryption and decryption. She selects a

public encryption key e, and computes a private decryption key d as its multiplicative inverse modulo $\varphi(n)$. Alice is easily able to decrypt Bob's message by computing $C^d \mod n = m$ (by a lemma of Fermat's Little Theorem), recovering the original message.

For Eve to decrypt the message, she must compute d, which requires knowledge of $\varphi(n)$, and thus the prime factors p and q. Factoring n to find p and q is classically prohibitive for sufficiently large primes, ensuring the security of the cryptosystem. However, as we will discuss below, quantum algorithms offer polynomial time attack.

RSA remains widely deployed in securing digital communications, underpinning web encryption, secure remote access, digital signatures, and electronic payment authentication.

2.2 Hardness of Factorisation

The security of many public-key cryptosystems, including RSA, hinges on the computational intractability of factoring, or of solving the discrete logarithm problem (DLP): finding x such that

$$g^x = h \mod p$$

No polynomial-time algorithm is currently known for integer factorisation or DLP. The most efficient classical method for factoring large semiprimes—particularly those exceeding 110 decimal digits—is the General Number Field Sieve (GNFS). This algorithm has a subexponential time complexity:

$$O\left(\exp\left((64/9)^{1/3}(\log n)^{1/3}(\log\log n)^{2/3}\right)\right).$$

For sufficiently large n, the computational effort required to factorise it far exceeds practical time constraints, rendering RSA secure against classical attacks.

3 Quantum Computation

In 1994, Peter Shor introduced an algorithm that promises an exponential speedup over the best-known classical algorithms for integer factorisation and DLP, assuming the existence of a fault-tolerant quantum computer [8]. Shor's algorithm leverages the principles of quantum superposition and entanglement to efficiently solve the order-finding problem, to efficiently factor large semiprimes. This result could potentially undermine the security of public-key cryptosystems, such as RSA encryption, that rely on the intractability of factoring large semiprimes.

We first explain concepts of quantum computation that underpin Shor's algorithm.

3.1 Fundamentals of Quantum Computation

Definition 3.1.1 (Qubits). A qubit is a two-level quantum system represented as a unit vector in the Hilbert space $\mathbb{C}^2$. It is described by a linear combination (superposition) of the computational basis states $|0\rangle$ and $|1\rangle$:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle, \quad \text{where } \alpha, \beta \in \mathbb{C} \text{ and } |\alpha|^2 + |\beta|^2 = 1.$$

The computational basis states are given by:

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \quad |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}.$$

Since global phase factors of the form $e^{i\theta}$ do not affect measurement outcomes, the state space is effectively described by the complex projective space $\mathbb{C}P^1$, which can be visualised using the Bloch sphere. When dealing with multiple qubits, the state space extends from $\mathbb{C}^2$ to the tensor product space $\mathbb{C}^{2^n}$ for an n-qubit system.

Definition 3.1.2 (Interference). Interference arises when probability amplitudes of quantum states combine either constructively or destructively, affecting the probability distribution of measurement outcomes. Quantum algorithms leverage interference to amplify the probability of correct solutions while suppressing incorrect ones.

Definition 3.1.3 (Entanglement). Two qubits are entangled if their joint state cannot be expressed as a tensor product of two independent single-qubit states. That is, given an n-qubit system $|\psi\rangle \in \mathbb{C}^{2^n}$, the system is separable if it can be written as

$$|\psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle \otimes \cdots \otimes |\psi_n\rangle.$$

Otherwise, the system exhibits entanglement.

Definition 3.1.4 (Quantum Measurement). In the computational basis $\{|0\rangle, |1\rangle\}$, a quantum measurement collapses the state probabilistically. Given a qubit state

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

the measurement outcomes obey the Born rule:

$$P(0) = |\alpha|^2, \quad P(1) = |\beta|^2.$$

3.2 Shor's Algorithm - Factoring as Period Finding

Shor's algorithm reduces the factoring problem to finding the period r of the query function $f(x) = a^x \mod N$, where a is a random integer coprime with N. The group structure of $\mathbb{Z}_N^*$ allows us to view the problem as finding the *hidden subgroup* of the additive group of integers modulo r. Specifically, the function $f(x) = a^x \mod N$ is constant on cosets of the subgroup generated by r, i.e., $f(x) = f(x + r)$, where f is an injective function on cosets.

3.2.1 Quantum Fourier Transform

The Quantum Fourier Transform (QFT) maps an n-qubit state $|x\rangle = |x_1 x_2 ... x_n\rangle$ in the computational basis to $|\tilde{x}\rangle$ in the Fourier basis through superposition and phase shifts [1]:

$$
\begin{aligned}
|\tilde{x}\rangle &= \mathrm{QFT}\,|x\rangle \\
&= \frac{1}{\sqrt{N}} \sum_{y=0}^{2^n-1} e^{\frac{2\pi i x y}{N}} |y\rangle \\
&\qquad\qquad \text{where } y = y_1 y_2 \dots y_n \text{ in binary} \\
&= \frac{1}{\sqrt{N}} \sum_{y_1=0}^{1} \sum_{y_2=0}^{1} \cdots \sum_{y_n=0}^{1} e^{\frac{2\pi i x}{N} \sum_{k=1}^{n} y_k 2^{n-k}} |y_k\rangle \\
&= \frac{1}{\sqrt{N}} \bigotimes_{k=1}^{n} \left[|0\rangle + e^{\frac{2\pi i x}{N} 2^{n-k}} |1\rangle \right] \\
&= \frac{1}{\sqrt{N}} \bigotimes_{k=1}^{n} \left[|0\rangle + e^{\frac{2\pi i x}{2^k}} |1\rangle \right] \\
&= \frac{1}{\sqrt{N}} \left(|0\rangle + e^{\frac{2\pi i x}{2}} |1\rangle \right) \otimes \left(|0\rangle + e^{\frac{2\pi i x}{4}} |1\rangle \right) \otimes \cdots \otimes \left(|0\rangle + e^{\frac{2\pi i x}{n}} |1\rangle \right)
\end{aligned}
$$

So, given an n-qubit register initialised in the computational basis

$$|x\rangle = \bigotimes_{k=1}^{n} |x_k\rangle.$$

the QFT transforms it into a tensor product of *Hadamard-like states*, each accumulating a phase dependent on higher-order bits:

$$|\tilde{x}\rangle = \frac{1}{\sqrt{N}} \bigotimes_{k=1}^{n} \left(|0\rangle + e^{\frac{2\pi i x}{2^k}} |1\rangle \right).$$

The QFT can be implemented as on quanutm hardware as a sequence of phase rotations by Hadamard and Controlled Phase Rotation gates.

The *Hadamard gate* (H) is a unitary and Hermitian operator that act on single qubits ot create a superposition of the computational basis states.

It can be represented by the matrix:

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

Applying H to the computational basis states results in:

$$H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \quad H|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle),$$

or in general:

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

A *Controlled Phase Rotation gate (CROT)* applies a phase shift $e^{i\theta}$ to a target qubit conditioned on the state of the control qubit. For the QFT, the phase is typically $\theta = \frac{2\pi}{2^k}$, where k corresponds to the qubit index:

$$CROT_k\,|x_j\rangle = e^{\frac{2\pi i}{2^k} x_j}\,|x_j\rangle]$$

Note that the Hadamard gate is just a special case of the Controlled Phase Rotation gate, with $k = 1$.

The matrix representation is:

$$CROT_k = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\frac{2\pi}{2^k}} \end{pmatrix}$$

Quantum Fourier Transform - Implementation

We initialise the quantum register with n qubits, $|x\rangle = |x, x_2, \ldots, x_n\rangle$, and apply the gates in sequence on qubit 1:

(1) $\left[|0\rangle + e^{\frac{2\pi i}{2}x_1}|1\rangle\right] \otimes |x_2, \ldots, x_n\rangle$

(2) $\left[|0\rangle + e^{\frac{2\pi i}{2^2}x_2} e^{\frac{2\pi i}{2^1}x_1}|1\rangle\right] \otimes |x_2 x_3 \ldots x_n\rangle$

...

(n) $\left[|0\rangle + e^{\frac{2\pi i}{2^n}x_n} \ldots e^{\frac{2\pi i}{2^1}x_1}|1\rangle\right] \otimes |x_2, x_3, \ldots, x_n\rangle$
$= \left[|0\rangle + e^{2\pi i \frac{x}{2^n}}|1\rangle\right] \otimes |x_2 x_3 \ldots x_n\rangle$

Iterate for each qubit i up to n, applying H to qubit i, and $CROT$ to each subsequent qubit.

Finally, swap qubits symmetrically from both ends of the register.

The final quantum state $|\tilde{x}\rangle$ is now in the Fourier basis.

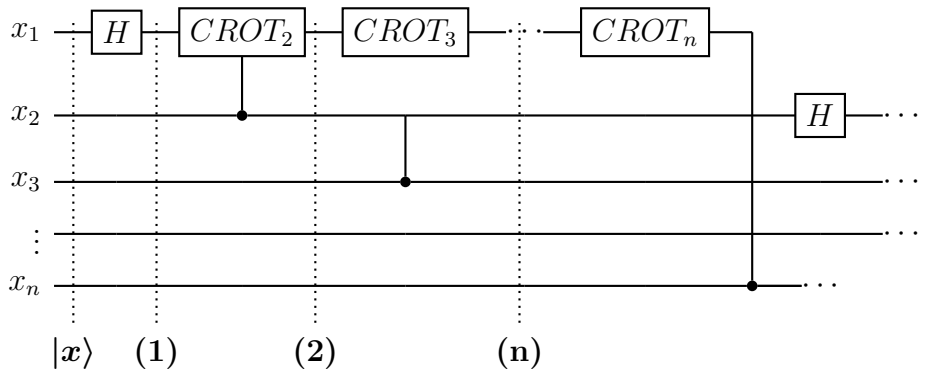


Figure 1: Quantum circuit that implements the QFT. Note that since both H and $CROT$ are unitary operators, the QFT is also unitary.

3.2.2 Representation Theory and the QFT

Group Representations Let G be a finite group and $\mathrm{GL}(d, \mathbb{C})$ the group of invertible $d \times d$ complex matrices under multiplication. A *representation* of G is a homomorphism:

$$\varphi : G \to \mathrm{GL}(d, \mathbb{C}), \quad \text{satisfying} \quad \varphi(g_1 g_2) = \varphi(g_1)\varphi(g_2) \quad \forall g_1, g_2 \in G.$$

A representation φ is said to be *irreducible* if there is no proper nontrivial subspace of the vector space that remains invariant under all matrices in the image of φ. In other words, if V is the vector space on which φ acts, the only subspaces that are preserved under all transformations $\varphi(g)$ for $g \in G$ are the trivial subspace $\{0\}$ and V itself. Irreducible representations (irreps) serve as the fundamental building blocks of more complex representations, much like prime numbers are the building blocks of integers.

Characters and Abelian Groups For abelian G, all irreps are one-dimensional. These are called *characters*, defined as homomorphisms $\chi : G \to \mathbb{C}^\times$ satisfying:

$$\chi(e) = 1, \quad \chi(g)^{|G|} = 1 \quad \forall g \in G \quad \text{(hence } \chi(g) \text{ are roots of unity)}.$$

The set $\widehat{G}$ (the *Pontryagin dual*) of all characters forms a group under pointwise multiplication:

$$(\chi \cdot \psi)(g) = \chi(g)\psi(g), \quad \text{with } \widehat{G} \cong G.$$

where φ and χ are characters of G.

QFT of Group Elements For cyclic $G = \mathbb{Z}_N$, the QFT simply maps the computational basis to the character basis:

$$\mathrm{QFT}_N : |k\rangle \mapsto \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} \chi_k(x)|x\rangle, \quad \text{where } \chi_k(x) = e^{2\pi i k x/N}.$$

The QFT here can be understood as a projection into a space of these frequencies.

Orthogonality of Characters The characters χ_k also form an orthogonal set, which we show by computing the inner product:

$$\langle \chi_k, \chi_{k'} \rangle = \frac{1}{N} \sum_{g \in G} \chi_k(g)\overline{\chi_{k'}(g)}.$$

$$= \frac{1}{N} \sum_{g \in G} \omega_N^{k \cdot g} \cdot \omega_N^{-k' \cdot g} = \frac{1}{N} \sum_{g \in G} \omega_N^{(k-k') \cdot g}.$$

- If $k = k'$, then the exponent $(k - k') \cdot g = 0$ for all $g \in G$. In this case, the sum becomes:

$$\langle \chi_k, \chi_k \rangle = \frac{1}{N} \sum_{g \in G} 1 = \frac{1}{N} \cdot N = 1.$$

- If $k \neq k'$, then the exponent $(k - k') \cdot g$ is nonzero for at least some $g \in G$. This sum is a geometric series with N terms, where each term is a power of $\omega_N^{(k-k')\cdot g}$. Since ω_N is a primitive N-th root of unity, the sum of all the N-th roots of unity equals zero:

So the inner product is:

$$\langle \chi_k, \chi_{k'} \rangle = \begin{cases} 1 & \text{if } k = k', \\ 0 & \text{if } k \neq k'. \end{cases}$$

This confirms that the set of characters $\{\chi_k\}$ for $k = 0, 1, 2, \ldots, N-1$ forms an *orthogonal set.*

Application to Shor's Algorithm In the hidden subgroup problem (HSP) for $G = \mathbb{Z}_N$, let $H \leq G$. The QFT isolates $H^\perp \subset \widehat{G}$, defined as:

$$H^\perp = \{\chi_k \in \widehat{G} \mid \chi_k(h) = 1 \ \forall h \in H\}.$$

Post-QFT measurement yields random $\chi_k \in H^\perp$, providing constraints:

$$\sum_{h \in H} \chi_k(h) = \begin{cases} |H| & \text{if } \chi_k \in H^\perp, \\ 0 & \text{otherwise.} \end{cases}$$

The outcome of the measurement is a group element g whose corresponding character χ_g lies in the orthogonal complement $H^\perp$ of H. This orthogonality condition means that the measurement gives a random g constrained by the condition $\chi_g(h) = 1$ for all $h \in H$, and this constraint allows for the unique determination of H.

By collecting multiple such measurements (i.e., measuring g in a way that constrains χ_g to lie in $H^\perp$), we gather enough information to uniquely determine the structure of the subgroup H. This is because each g provides a constraint (since $\chi_g(h) = 1$ for all $h \in H$), and after a few such measurements, these constraints can uniquely specify the subgroup H.

QFT on non-abelian groups When extended to non-abelian groups, the straightforward application of QFT fails. While in an abelian group, every irrep was one-dimensional, allowing the group to be expressed as a well-defined set of characters, where each element is bijectively mapped to a complex number corresponding to its character value, in the case of non-abelian groups, the irreps are higher-dimensional matrices. There is no simple dual group

structure that can act as a frequency space, and may require *qudit* entanglement. Qudits, which generalise qubits to higher-dimensional quantum systems, may better accommodate the higher-dimensional matrices that arise from non-abelian irreps.

Variants of the QFT have been found for certain non-abelian groups, including normal subgroups, solvable groups, and specific semidirect product p-groups with constant nilpotency class. Notably, Kuperberg's algorithm (2003) provides a solution to the Hidden Subgroup Problem (HSP) in the dihedral group with a time complexity of $2^{O(\sqrt{\log |G|})}$. However, for groups like the general linear group $\mathrm{GL}_n(q)$, where q is a finite field size, and many other non-abelian structures, efficient QFTs and solutions to the general non-abelian HSP remains a challenging open problem.

As such, post-quantum cryptographic key exchange protocols should be considered as alternatives to traditional approaches based on abelian groups. The inherent difficulty in efficiently solving the Hidden Subgroup Problem (HSP) in non-abelian settings suggests that these groups could provide a robust foundation for secure cryptographic primitives resistant to quantum attacks.

4 Cryptographic Implementation

4.1 Sketch of Protocol

We outline an preliminary idea of a cryptographic key exchange protocol based on operations in a non-abelian platform group and a nonlinear recurrence relation. The protocol ensures secure communication by leveraging the complexity of non-abelian group operations.

To begin with, both Alice and Bob agree on a non-abelian group G, such as symmetry groups on Okamoto curves, or $G = SL(2, \mathbb{F}_p)$, for instance. The constant group elements $C_1, C_2 \in G$ are publicly shared, along with a parity-dependent recurrence:

$$G_{k+1} = G_k \cdot G_{k-1} + C_1 \quad (\text{even } k), \quad G_k^{-1} \cdot G_{k-1}^{-1} + C_2 \quad (\text{odd } k).$$

Seed elements G_0 and G_1 are also shared.

Now, Alice and Bob each choose a large secret integer, n and m respectively. Alice then computes the sequence G_{n-1}, G_n by iterating the recurrence from initial values. She then sends G_{n-1}, G_n and the parity of n to Bob.

Similarly, Bob computes and sends G_{m-1}, G_m and the parity of m to Alice.

Now, they can each compute a shared key G_{n+m} by iterating the recurrence to the respective steps using the information exchanged.

The non-abelian structure ensures that solving the recurrence and extracting private keys from public information is exponentially hard. However, a platform group should be chosen such that Alice and Bob can compute their shared secret efficiently. Further, initial parameters must be carefully chosen so as to not create unintended symmetries that may simplify the problem. As with other cryptographic protocols, security claims often rely on heuristic assumptions rather than formal reductions to well-established hard problems, leaving protocols vulnerable to unforeseen attacks.

4.2 Okamoto Curves as a Platform Group

While the most widely used public-key algorithm remains the RSA algorithm, as computing power grows, increasingly large numbers are required to maintain its security, with its current recommendation being at least 2048 bits. Factorisation on elliptic curves provides another realisation of public key exchange, often preferred to the standard RSA algorithm because storage requirements are smaller for the same level of security.

Such curves are examples of algebraic curves, i.e., curves in two dimensionial complex space, which are defined by the vanishing of a polynomial.

The canonical form of an *elliptic curve* in $\mathbb{C}^2$ is given by $h = 0$, where given g_2, g_3,

$$h(u, v) = v^2 - u^3 - g_2\, u - g_3.$$

The addition theorem (or the group law) on such a curve is a mapping that takes two points A, B on it to another point denoted $A + B$ on the same curve. Geometrically, addition is given by taking the line through A and B, finding a third point of intersection of the line with the curve (which exists because it is a cubic curve) and taking its reflection in the horizontal axis, as shown in Figure 2.

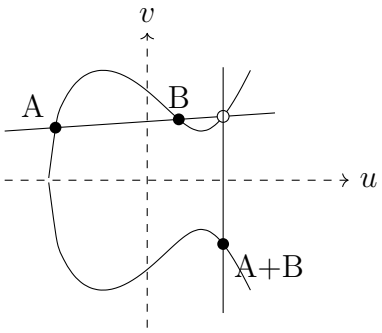


Figure 2: An example of a Weierstrass curve and addition theorem on it in $\mathbb{R}^2$, with the horizontal axis assumed to be given by u and the vertical given by v. The addition theorem takes two points labelled A and B to a third point, which is labelled $A + B$.

Okamoto curves are elliptic curves that exhibit non-commutative properties when combined with certain automorphism groups can be leveraged in post-quantum cryptographic protocols [3] [4].

Consider the fourth Painlevé equation:

$$P_{IV}: \quad q'' = \frac{1}{2q}(q')^2 + \frac{3}{2}q^3 + 2tq^2 + \left(a_2 - a_0 + \frac{t^2}{2}\right)q - \frac{a_1^2}{2q}$$

with $a_0 + a_1 + a_2 = 1$. Its Hamiltonian is:

$$H_{\mathrm{IV}}(q,p) = -a_1 p - a_2 q + pq(p - q - t).$$

Note that $H_{\mathrm{IV}} = k$ is an elliptic curve with distinctive symmetries. To consider symmetry group operations on such curves, we first convert into a system of ODEs given by

$$\begin{cases} f_0' &= f_0(f_1 - f_2) + \alpha_0, \\ f_1' &= f_1(f_2 - f_0) + \alpha_1, \\ f_2' &= f_2(f_0 - f_1) + \alpha_2, \end{cases} \tag{4.1}$$

where f_j are functions of t, $f_j' = \frac{df_j}{dt}$, and α_j are constants for $j = 0, 1, 2$.

From this system, we can see that the sum of the derivatives satisfies the relation

$$f_0' + f_1' + f_2' = \alpha_0 + \alpha_1 + \alpha_2.$$

We let

$$\alpha_0 + \alpha_1 + \alpha_2 = \kappa,$$

where κ is a constant. Hence, the sum of the functions is given by

$$f_0 + f_1 + f_2 = \kappa t + c,$$

where c is an arbitrary constant.

Transformations on parameters of the fourth Painlevé equation P_{IV} can be understood geometrically. Consider a two-dimensional plane, tiled by triangles, as shown in Figure 3.

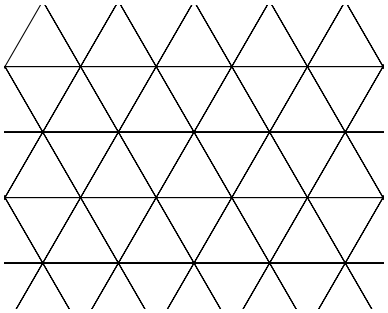


Figure 3: A triangular tiling of the plane.

We assign a coordinate $(\alpha_0, \alpha_1, \alpha_2)$ to each point in the plane as follows. First, identify one triangle Δ as a fundamental triangle. Second, let each edge of Δ be given by $\alpha_j = 0$, as shown in Figure 4. We assume that parallel lines in the triangular lattice differ by integer values, as shown in Figure 5.

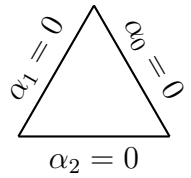


Figure 4: A fundamental triangle Δ in the tiling.

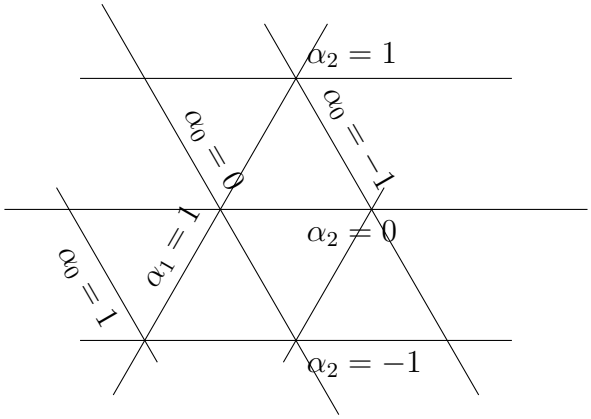


Figure 5: Integer values of α_j define edges of triangles in the tiling.

Third, given a point P_0 in Δ, we define its coordinates $(\alpha_0, \alpha_1, \alpha_2)$ to be given by the orthogonal distance from P_0 to each respective edge.

The symmetry group of P_{IV} can then be understood as transformations that map the fundamental triangle to other triangles in the tiling. Reflections s_j across the line $a_j = 0$ form an *affine Weyl/Coxeter group* $W = \langle s_0, s_1, s_2 \rangle$, while $\tilde{W} = \langle s_0, s_1, s_2, \pi \rangle$ forms an *extended affine Weyl/Coxeter group* where π is the permutation operator, $\pi(\alpha_0, \alpha_1, \alpha_2) = (\alpha_1, \alpha_2, \alpha_0)$.

The three translations on the triangular lattice are defined by

$$T_1 = \pi\, s_2\, s_1,$$
$$T_2 = s_1 \pi s_2,$$
$$T_3 = s_2 s_1 \pi.$$

We can define a translation operation T acting on H on the $A_2^{(1)}$ lattice with axes a_0, a_1, a_2 given recursively by:

$$\begin{cases} \overline{q} & = p - q - t - \frac{a_2}{p} \\ \overline{p} & = \overline{q} - p + t + \frac{a_1 - 1}{\overline{q}} \\ \overline{a}_0 & = a_0 \\ \overline{a}_1 & = a_1 - 1 \\ \overline{a}_2 & = a_2 + 1. \end{cases}$$

This can form the basis of the cryptographic protocol outlined.

5 Conclusion

We have explored the vulnerabilities of current cryptographic systems to quantum computing, particularly through Shor's algorithm, which threatens abelian group-based protocols like RSA and Diffie-Hellman. We proposed non-abelian groups as a promising alternative for post-quantum security. The complexity of non-abelian groups, such as translation groups over Okamoto curves, braid groups, and matrix groups like $\mathrm{SL}(2, \mathbb{F}_p)$ offers resistance to quantum attacks due to the difficulty of solving the hidden subgroup problem. While these protocols are theoretically compelling, challenges related to computational efficiency and security assumptions remain.

References

[1] M. A. Nielsen, I. L. Chuang, Quantum computation and quantum information, Cambridge university press, 2010.

[2] M. Noumi, *Painlevé Equations through Symmetry*, Translations of Mathematical Monographs, **223** American Mathematical Society, 2004.

[3] K. Okamoto, Polynomial Hamiltonians associated with Painlevé equations. I, *Proc. Japan Acad. Ser. A Math. Sci.* **56**(6) 264–268 (1980).

[4] K. Okamoto, Studies on the Painlevé Equations. IV. third Painlevé equation PIII, *Funkcial. Ekvac.* **30** (2-3) 305–332 (1987).

[5] K. Okamoto, Studies on the Painlevé Equations. II. fifth Painlevé Equation PV, *Japan. J. Math. (N.S.)*, **13**(1) 47–76 (1987).

[6] Rivest, R.L. and Shamir, A. and Adleman, L., A method for obtaining digital signatures and public-key cryptosystems, *Communications of the ACM*, **21**(2) (1978) 120–126.

[7] Australian Cyber Security Centre, Cyber Security Guidelines: Cryptography, in *Australian Cyber Security Centre*, 2023, `https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/ism/cyber-security-guidelines/guidelines-cryptography`.

[8] Peter W. Shor, Algorithms for quantum computation: discrete logarithms and factoring, in *Proceedings 35th Annual Symposium on Foundations of Computer Science*, 35th Annual Symposium on Foundations of Computer Science, Santa Fe, NM, USA, 1994, 124–134, `10.1109/SFCS.1994.365700`.