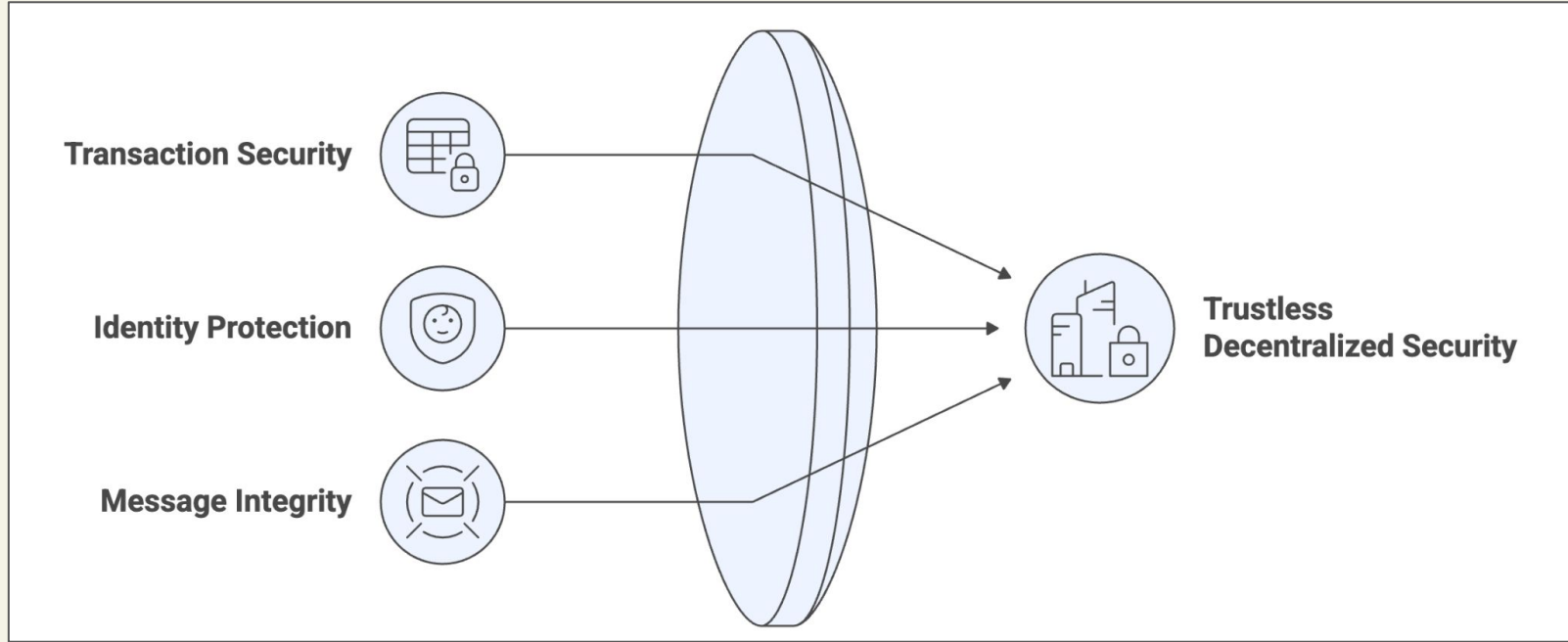
The background is dark blue with several light blue decorative shapes: a triangle in the top-left, a bracket on the right, and a bracket in the bottom-left. The title is displayed in a white, monospaced font within a dark blue rectangular area that has a window-like header with three colored dots (purple, blue, green) in the top-left corner.

Addressing Quantum Threats and Introduction to Post-Quantum Cryptography in the XRPL

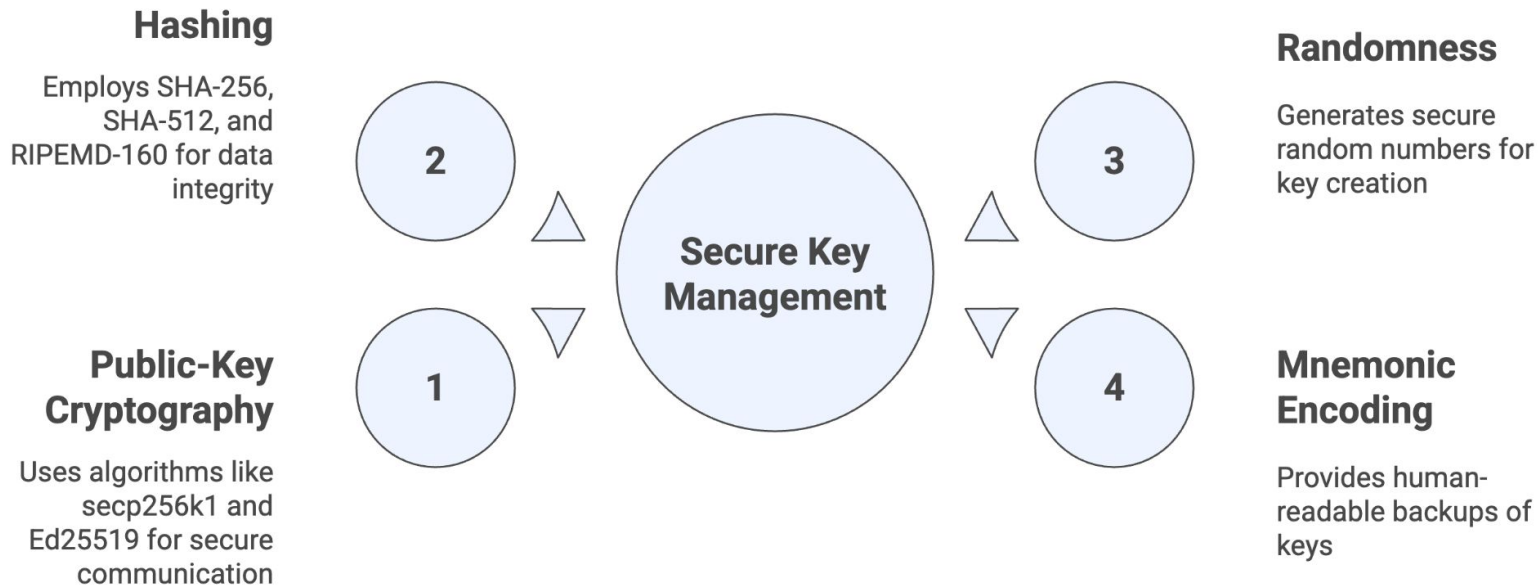
Atharva Lele
Staff
Trinity College Dublin

Why Cryptography Matters for Blockchain Systems

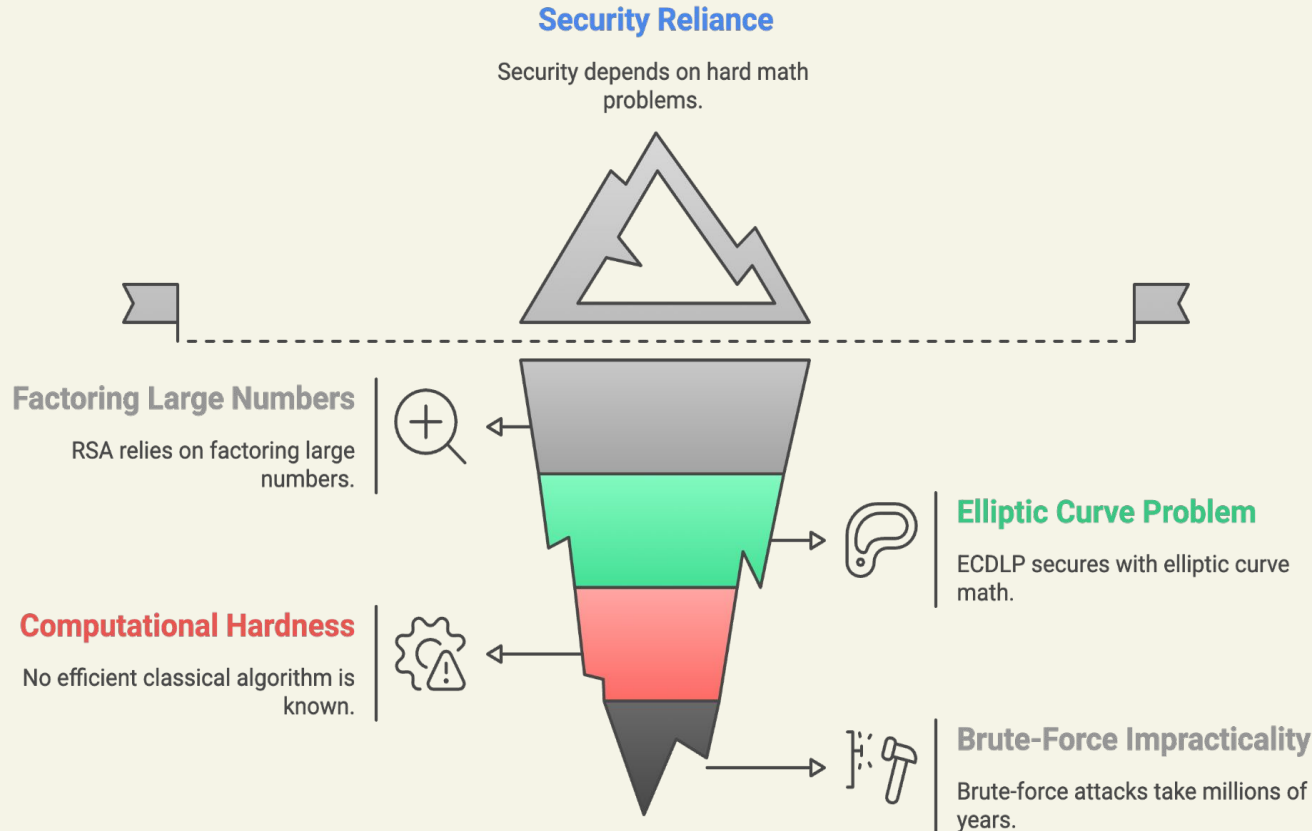


Classical Cryptography in XRPL

Components of Secure Key Management

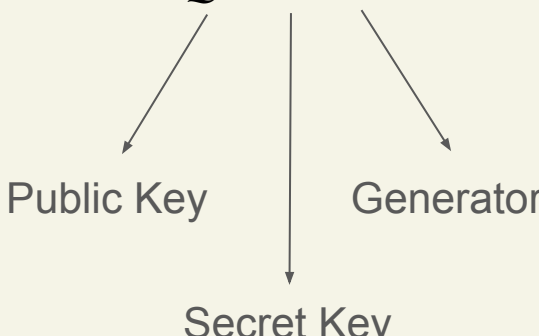


Why is it Secure? The “Hard Problem”



The Discrete Logarithm Problem (ECDLP) in secp256k1

- Secp256k1 is the elliptic curve used by XRPL for digital signatures.

- ECDLP : $Q = d \cdot G$


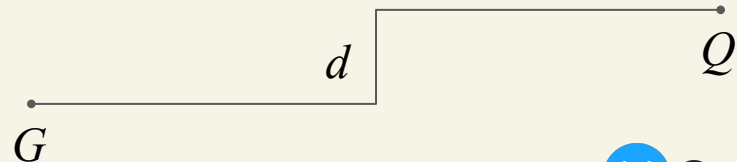
Public Key

Secret Key

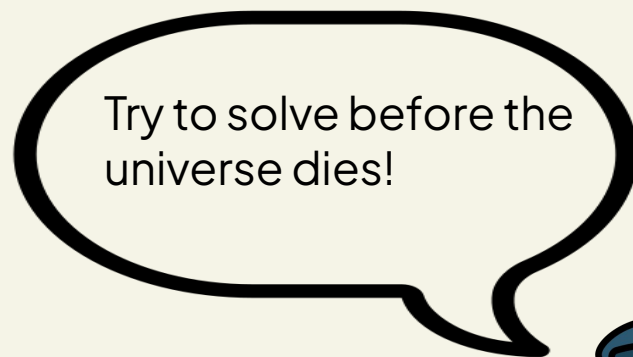
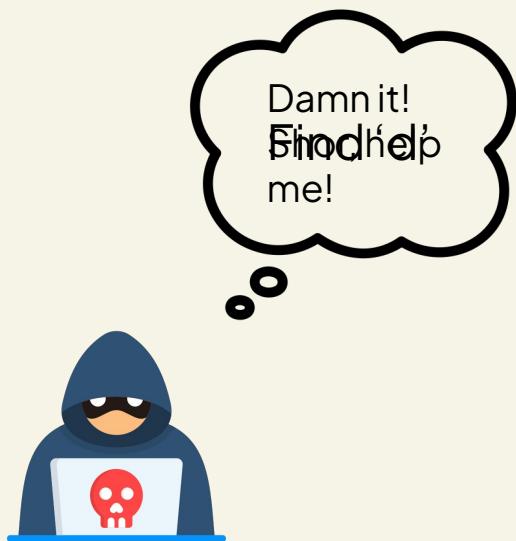
Generator

where,

- Secret key (d) : random 256-bit integer.
- G is fixed base point.



Why is DLP hard for Classical Computers?



Quantum Computing

- Quantum algorithm is a step by step computational procedure performed on a quantum computer leveraging quantum phenomena like superposition, entanglement and interference.
- Can solve DLP in polynomial time.
- Uses quantum properties like Superposition (trying many possibilities at once) and the Quantum Fourier Transform to find hidden patterns (periods).

Shor's Algorithm

Once a quantum computer can run Shor's algorithm at a scale, anyone can recover the private key from a public key.

This breaks the fundamental security assumption of secp256k1 and all elliptic curve cryptography.

All digital signatures, wallet addresses, and transactions relying on secp256k1 become insecure.

Shor's Algorithm

Imagine you have a 100 x 100 giant grid of playing cards.

1) 10,000 cards

2) Look at 'all' cards at once.

3) Take a peek and suddenly we know that it is



4) Study the pattern on how all the 3♠ appear on the grid.

5) Take one final look and we know exactly which 3♠ is the secret one.

Shor's Algorithm : Working

- Curve secp256k1 : $y^2 = x^3 + 7$ over large finite field
- Base point : G
- Public key (Q)

$$Q = d \cdot G,$$

where, $d \rightarrow$ Secret Key , $G \rightarrow$ Generator

Problem : Find d ,

given Q and G .

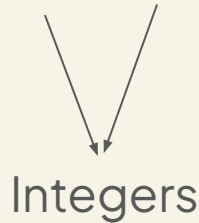
Shor's Algorithm : Working

Step 1 : Function for period finding

- Convert the Discrete Logarithm Problem into Period Finding Problem.

Attacker defines a function :

$$f(a, b) = a \cdot G + b \cdot Q \dots\dots\dots(Q = d \cdot G)$$



Shor's Algorithm : Working

Step 1) Function for Period Finding

$$f(a, b) = a \cdot G + b \cdot Q \dots\dots\dots(Q = d \cdot G)$$

$$f(a, b) = a \cdot G + b \cdot (d \cdot G)$$

$$f(a, b) = a \cdot G + b \cdot d \cdot G$$

$$f(a, b) = (a + bd) \cdot G$$

Shor's Algorithm : Working

Step 2) Quantum Superposition

Superposition : Quantum computer can create a superposition of all possible values of ' a ' and ' b '.

$$\sum_{a=0}^{n-1} \sum_{b=0}^{n-1} |a, b\rangle |f(a, b)\rangle$$

This means the quantum computer is, in a sense, "trying" all possible combinations of a and b at the same time.

Shor's Algorithm : Working

Step 3) Measurement : Collapsing to a subset

The quantum computer measures the second register (the point (a, b)), which collapses the state to all pairs (a, b) that map to the same point on the curve.

Measurements yield at a participant point ' R '. Then all the pairs (a, b) such that $f(a, b) = R$, remain in superposition.

$$f(a, b) = (a + bd)G \equiv R \implies a + bd \equiv k \pmod{n}$$

For some fixed k (depending on R), the remaining pairs satisfy a linear equation in a and b .

Shor's Algorithm : Working

Step 4) Quantum Fourier Transform

If (a_1, b_1) and (a_2, b_2) give the same point, then

$$a_1 + b_1d \equiv a_2 + b_2d \pmod{n}$$

$$(a_1 - a_2) + d(b_1 - b_2) \equiv 0 \pmod{n}$$

The QFT transforms the superposition into another superposition where the amplitudes are large for values that satisfy the hidden period (the secret d).

Shor's Algorithm : Working

Step 5) Measurement and Extraction of the Period (d)

- Measures the state.
- Collapsing it to a value that gives an equation:

$$a + bd \equiv 0 \pmod{n}$$

- This is a linear equation involving a secret ' d '.
- Repeat to get enough equations to solve for ' d ' with classical math.
- Classic math involves the use of Euclidean algorithm to solve equations and recover ' d '.

Shor's Algorithm

1. Convert DLP to PFP.
2. Quantum Superposition.
3. Measurement : Collapsing to a subset
4. Quantum Fourier Transform
5. Measurement : Extraction of the Period (d).

Card Analogy

1. Giant grid (100 x100)
2. Looking at 'all' cards at once.
3. Take a peek to know what card it is.
4. Analyse the pattern of the card.
5. Final look to know *which* is the exact card.

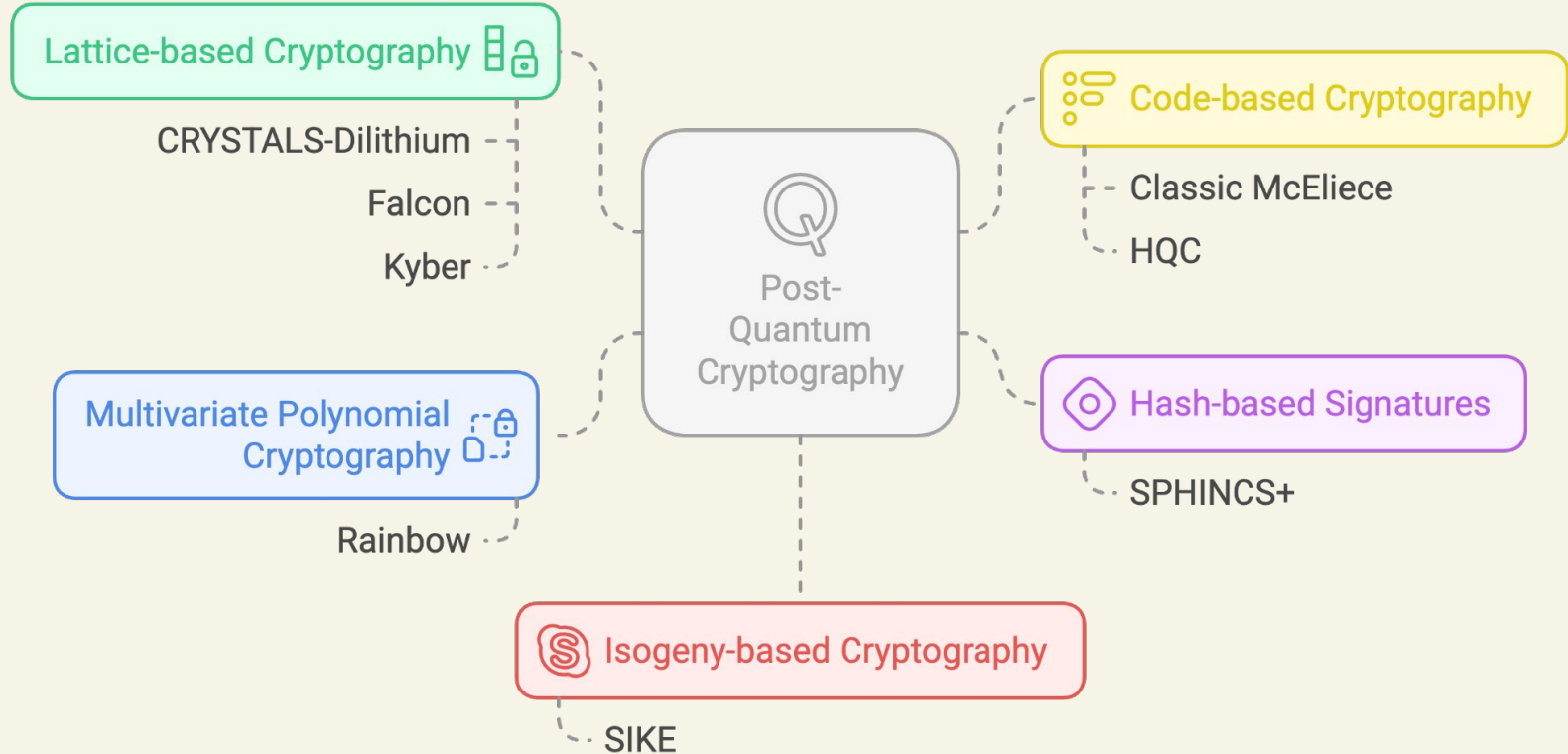
The Need for Post Quantum Cryptography

- Quantum computers threaten the security of today's digital signatures and encryption.
- Shor's algorithm can break RSA, secp256k1, and Ed25519—core algorithms used in XRPL and most blockchains.
- Blockchains, transactions, accounts, funds, etc; everything would be compromised!
- To withstand these attacks, we need strong encryption and signature algorithms like Post Quantum Cryptographic Algorithms.

What is Post-Quantum Cryptography?

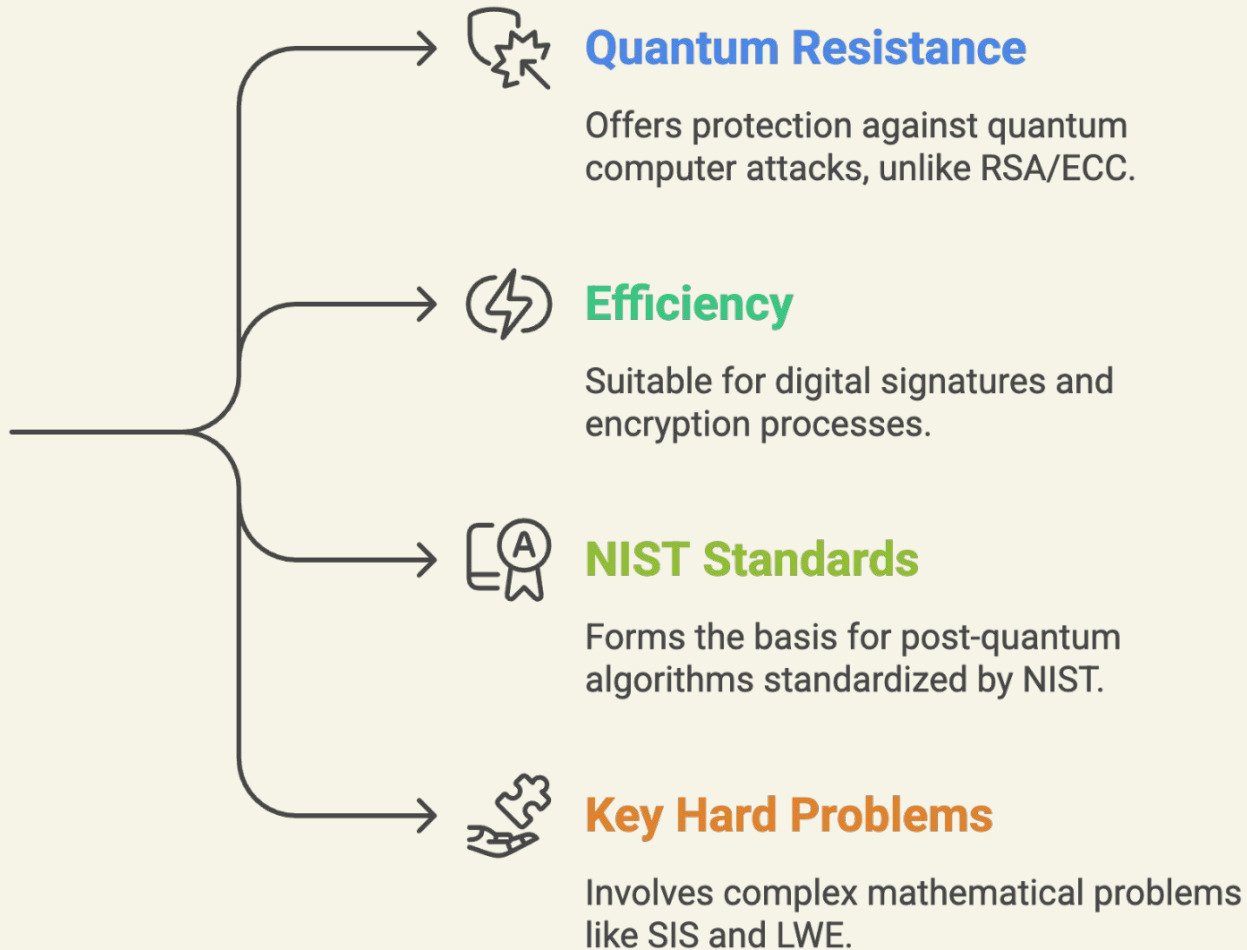
- Post-Quantum Cryptography (PQC) refers to cryptographic techniques designed for classical computers to be secure against attacks performed using both classical and quantum computers.
- Unlike RSA and ECC, which are broken by quantum algorithms like Shor's, PQC is built on mathematical problems that are believed to be hard even for quantum computers.

Types of Post Quantum Cryptography





Why choose lattice-based cryptography?



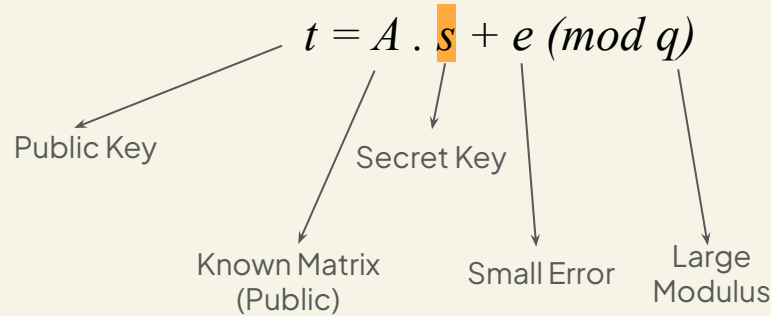
CRYSTALS-Dilithium (Background)

- PQC Standardised Candidate by NIST (National Institute of Standards and Technology).
- Fiat-Shamir with Aborts technique (uses Gaussian Sampling)
- Uniform Sampling (Easier to implement and more secure)
- Builds on the Bai and Galbraith scheme, which also uses uniform sampling, by introducing a new technique that reduces the public key size by more than half.
- The scheme is grounded in the hardness of the Module-LWE and Module-SIS problems, which generalize Ring-LWE.



CRYSTALS-Dilithium : Working

Problem Creation (LWE) : Given A & t , find s



If $e = 0$, system of linear equations (easily solvable).

If $e \neq 0$, system of equations where each equation is slightly “off”.

CRYSTALS-Dilithium : Working

Attack using Shor's algorithm :

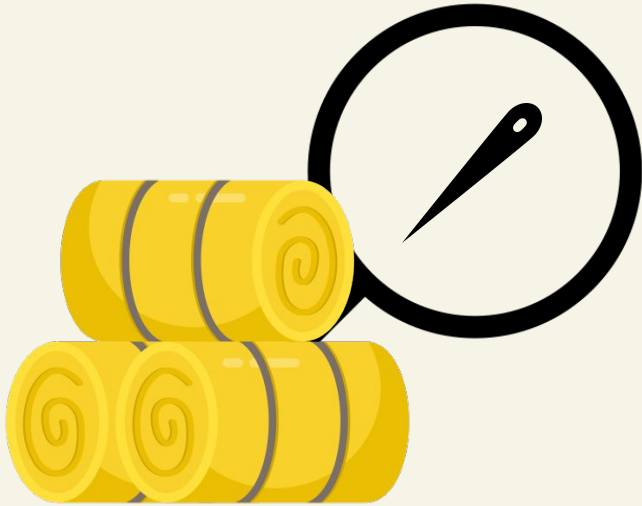
- Depends on the period-finding problem.
- Possible for factoring and discrete logs.
- LWE and SIS do not have this structure.
- Noise ' e ' destroys periodicity or algebraic structure which Shor's algorithm could exploit.

In other words:

The problem is not about finding period or structure. It's about "guessing" through a high-dimensional, noisy space.

Example Analogy 1

ECDLP :



Shor's algorithm :



Example Analogy 1

LWE :



Shor's Algorithm :



Example Analogy 2

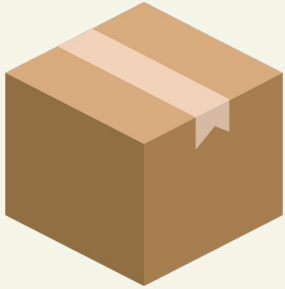


Sender

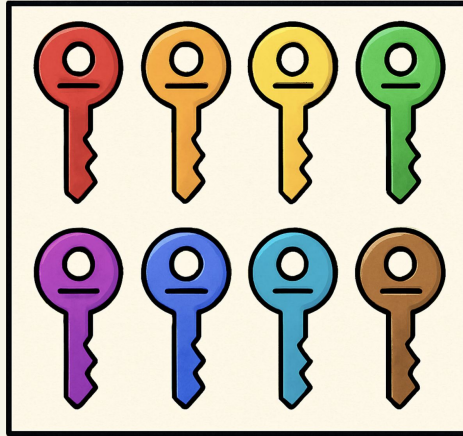


Receiver

Example Analogy 2



Secp256k1



ECDLP

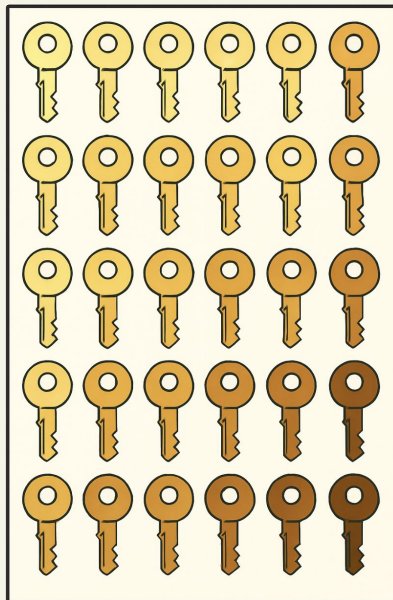


Shor

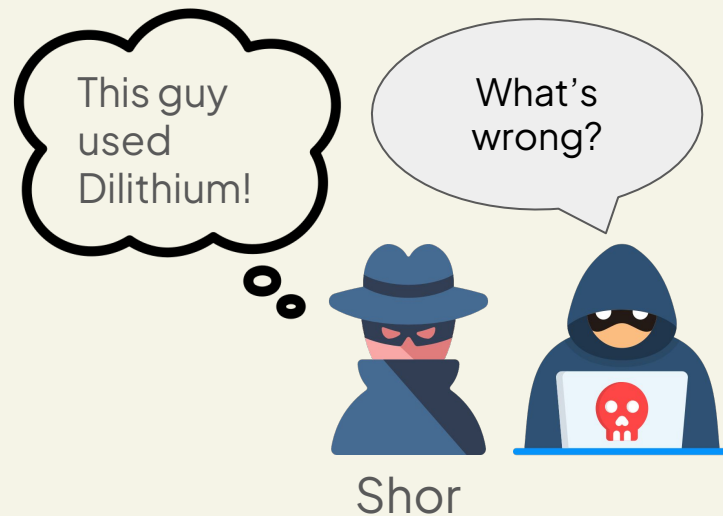
Example Analogy 2



CRYSTALS-
Dilithium



LWE, SIS, SVP



Integration of a PQC Algorithm into XRPL

- Study if your PQC Algorithm (Dilithium) is a good fit for XRPL.
- Analyse the cryptographic functions and check if Dilithium has similar functions. (if not, create to match existing functions).
- Introduce Dilithium as a new keytype.
- Modify the key size array to range from secp256k1 key size upto Dilithium key size.
- Modify the required cryptographic functions by adding Dilithium alongside existing key type arguments (secp256k1, ed25519–donna).
- Modify build commands for Dilithium (Cmakelists, conanfile) and test cases to include Dilithium alongside other key types.



Thank you! *

