# Rainbow Cryptography

Name: Jalay Shah

Rainbow cryptography is a type of post-quantum cryptography based on multivariate public key cryptosystems. It belongs to the broader category of multivariate quadratic (MQ) schemes, which rely on solving systems of quadratic equations—a problem that is considered hard for both classical and quantum computers.

## Key Highlights

The multivariate polynomial approach: The multivariate polynomial approach in cryptography alludes to cryptographic plans that are based on the trouble of tackling frameworks of multivariate quadratic conditions over limited areas. This issue, known as the MQ issue, is computationally difficult, making it a promising establishment for post-quantum cryptography.

Signature Scheme: Rainbow cryptography is basically utilized as a digital signature calculation, guaranteeing genuineness and astuteness in communication.

## Benefits over Traditional Cryptography:

Quantum resistance: Quantum resistance in Rainbow cryptography alludes to its capacity to resist assaults from quantum computers, which posture a noteworthy risk to conventional cryptographic strategies like RSA and ECC. The essential advantage of quantum resistance in Rainbow cryptography is its security in a future where quantum computers are effective sufficient to break existing cryptographic frameworks. Quantum calculations, such as Shor's calculation, can proficiently figure huge numbers and solve discrete logarithms, which would break RSA and ECC encryption. Rainbow cryptography, based on the multivariate quadratic (MQ) issue, isn't vulnerable to these attacks, guaranteeing long-term security. As quantum computing progresses, classical cryptographic frameworks will get to be out of date. Rainbow quantum resistance gives a defend against this, making it a solid alternative for securing delicate information and communications within the post-quantum period.

Efficient Key Sizes: Compared to other post-quantum calculations, Rainbow regularly has littler key sizes and speedier signature era, which can be more proficient in a few applications.