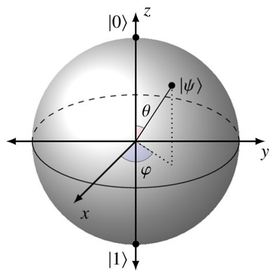
Cryptanalysis of isogeny-based post-quantum cryptography

James Clements

james.clements@bristol.ac.uk Lead Supervisor: Dr. Chloe Martindale

Quantum Computers

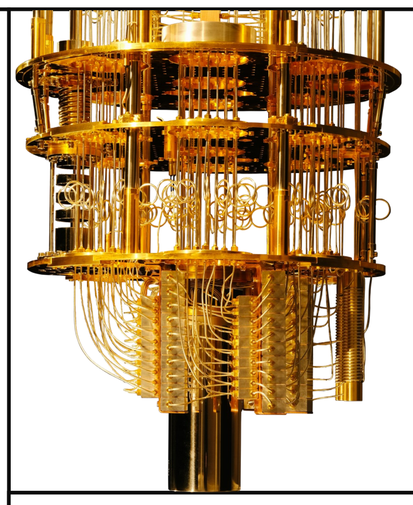
Quantum computers are a new kind of computer which perform computation using "**qubits**" instead of classical bits, 0 or 1.



They threaten cryptography in use today:

1. **Shor's Algorithm** efficiently solves the **integer factorization** and **discrete logarithm** problems breaking public-key cryptography. E.g. breaking TLS for internet communications.

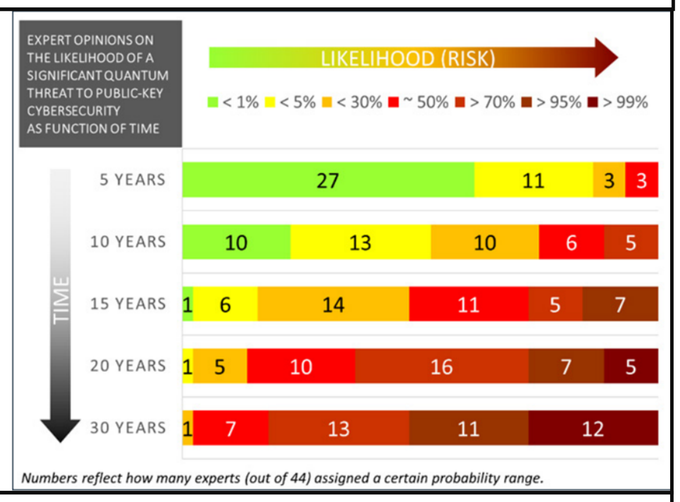
2. **Grover's Algorithm** speeds up breaking symmetric crypto, particularity relevant for small keys.



Quantum Threat Timeline

First **9-qubit** quantum computers emerged in 2016, **76-qubit** machines emerged recently. Quantum computing is already available through cloud services, and commercial products.

Maybe around **15 years** until it threatens crypto?



What can we replace classical public key cryptography with?

Symmetric Crypto (+ larger keys)	Quantum Cryptography	Post-Quantum Public-Key Replacements
Already exists, well understood, Not always feasible, may require network changes / more trust	Simpler adversarial model, fast ? Still experimental, very expensive, impossible with small devices ?	drop-in replacements, works everywhere Slower encryption, **security less understood**

National Institute of Standards and Technology (NIST) PQC 'Competition' 2016 - Present

Aims to establish new global standards in post-quantum public key crypto. Specifically **Key Encapsulation Mechanisms** and **Signature Schemes**. Considering candidates in turn, analysing their security, performance, and additional properties (e.g. forward secrecy, misuse resistance, and hardware support).

	Finalists	Alternates
KEMs/Encryption	Kyber NTRU SABER Classic McEliece	Bike FrodoKEM HQC NTRUprime SIKE
Signatures	Dilithium Falcon Rainbow	GeMSS Picnic SPHINCS+

Current Status: 7 finalists and 8 alternate candidates selected. The 3rd round of the competition is ongoing.
However, options for signature schemes are limited, and submissions for new schemes will reopen soon.

Candidates can be grouped into 5 different categories:

Code-Based Encryption	Lattice-Based Encryption and Signatures	Multivariate Signatures	Hash-Based Signatures	Isogeny-Based Encryption and Signatures
Short ciphertexts, Large public keys	Fastest encryption, Huge keys, slow signatures	Short signatures, Large public keys, slow	Well-studied security, small public keys, Large signatures, slow	Smallest keys, drop-in replacements, Slow encryption, **security less understood**

Isogeny–Based Cryptography

NIST: "We are most interested in a general-purpose digital signature scheme which is not based on structured lattices"
- This is something isogeny-based cryptography could offer.

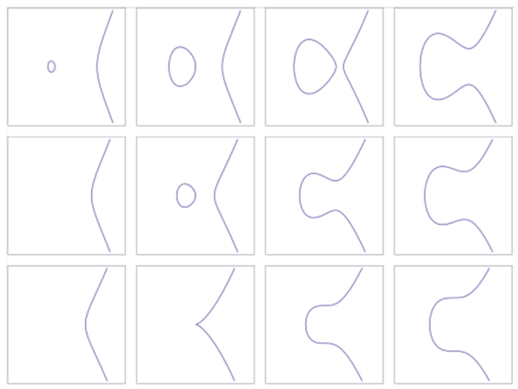
An *elliptic curve* is a curve in 2 dimensional space of the form $y^2 = x^3 + ax + b$, upon which a group law can be defined algebraically. They've been used in cryptography for decades, however traditional elliptic curve cryptography is not secure against a quantum adversary.

An *isogeny* is a rational map between elliptic curves. Isogeny-based cryptography utilizes these isogenies to provide post-quantum secure cryptographic primitives. It is a much newer area, having rapidly developed within the last 5-10 years.

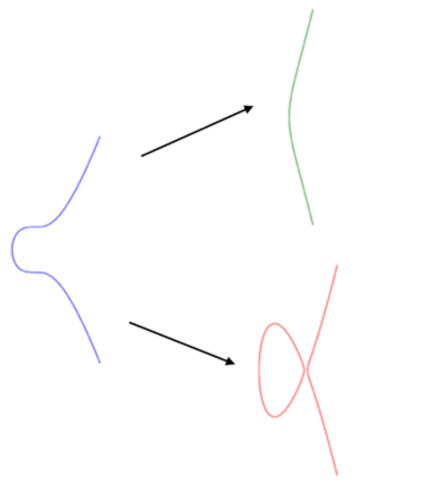
All cryptosystems are based on underlying problems which are believed to be hard to solve. This 'hardness' assumption, guarantees it is infeasible for an adversary to break it in a reasonable amount of time. For isogeny-based cryptography, these problems are based on finding isogenies.

For example, *the isogeny problem*, is given two elliptic curves, linked by an isogeny, find the isogeny between them. The assumed hardness of this problem makes the isogeny-based key-exchange CSIDH (pronounced "sea-side") post-quantum secure.

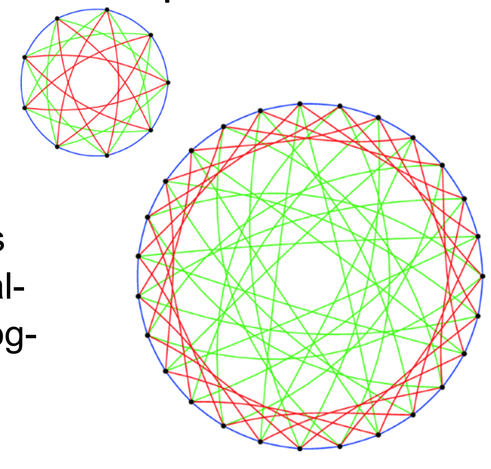
Elliptic Curves



Isogenies - Maps between elliptic curves



Supersingular Isogeny Graphs - used in CSIDH



Cryptanalysis of Isogeny-Based Cryptography

NIST: "Confidence in the hardness of the (underlying) problems would continue to benefit from more study"

Since the hardness of these cryptographic problems is assumed. It might not be true. However, it should be tested, by attempting to solve the problem efficiently, i.e. trying to break the cryptographic scheme. This is called *cryptanalysis*.

As a new area, the hardness of isogeny-based problems is less well-understood, and hence they are less trusted for real-world applications. To become a new standard, this needs to change, and further cryptanalysis of these schemes is required. This is my research project; mathematically studying the security of isogeny-based schemes such as CSIDH, SIKE/SIDH, SQISign, and more.