# Isogeny-based cryptography

Quantum computers are coming.

They're going to break all of our current cryptosystems.

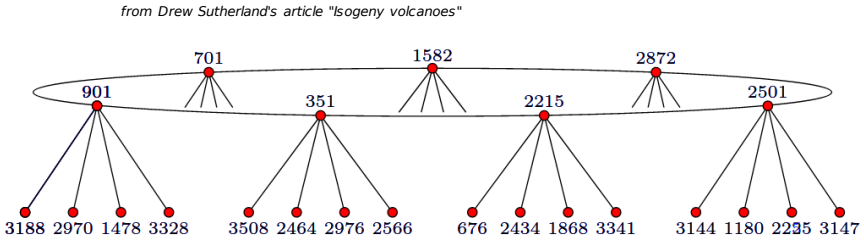
This will be a disaster.

So the crypto community is looking for **quantum-secure** systems; primitives which will be secure even against quantum computational attack.

One source of such cryptosystems comes from the realm of **isogenies of elliptic curves**.

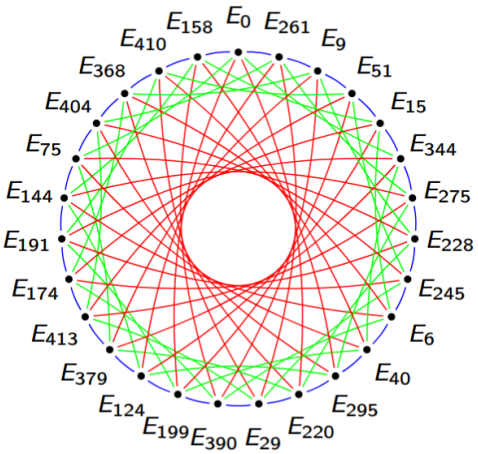
Isogenies are maps between elliptic curves. One can consider "elliptic curves up to isogeny". Considering these equivalence classes, one is led to consider **isogeny graphs**.

These look very different depending on whether the curves are **ordinary** or **supersingular**.




**Ordinary isogeny graph**

Isogeny volcano




**Supersingular isogeny graph**

Expander graph

Both have cryptographic applications, but expander graphs have **excellent mixing properties** which make them useful for secure hashes and random number generation.

Isogeny-based cryptography works by taking **random walks on supersingular isogeny graphs**. Because of the strong mixing properties, by doing this, you can end up anywhere on the graph. The random walk is the secret key; where you end up is the public key.

This then allows for a standard Diffie-Hellman key-exchange.

An attacker needs to compute an isogeny between the starting curve and the curve representing the public key in order to get the secret key.

This is considered hard even for a quantum computer.

But the quantum cryptanalysis of these algorithms is still very much an active area of research.