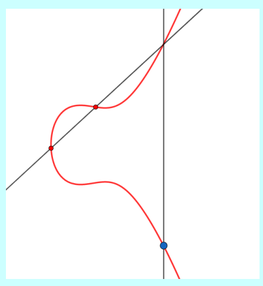
Too Much Information: How we cracked my favourite cryptosystem

PKI vs Quantum computers

The advent of quantum computers is marking a turning point in cryptography. Quantum computers will be able **to break most of the currently used public-key cryptosystems**.

Presently, one of the most utilised solutions in public-key cryptography is based on elliptic curves.

Unfortunately, this approach is **vulnerable to quantum computers.**



What is an Isogeny?

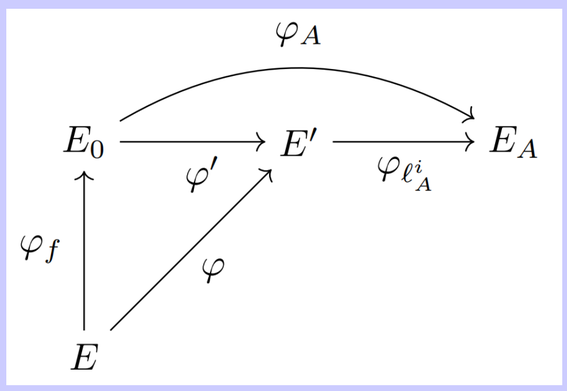
In the last 20 years, researchers have studied alternative methods to employ elliptic curves in a quantum scenario. Special maps, called isogenies, between elliptic curves, **substitute their arithmetic.**

Arguably, the most influential primitive in the field of isogeny-based cryptography is SIKE [1].

The attack

The security of SIKE relies on the supersingular isogeny with torsion(SSI-T) problem. We use the knowledge of the image of some torsion points under the secret isogeny to compute an isogeny between Abelian surfaces that **reveals the secret key** [2].

This attack does not even require quantum capabilities.



Implications

SIKE is the only isogeny-based cryptosystem in the fourth round of the **NIST PQC Standardization process**.

All the isogeny-based protocols that reveal the image of torsion points under the secret isogeny are vulnerable to this attack.

However, the security of isogeny-based protocols that do not rely on the same exact hardness assumption remains unchanged.

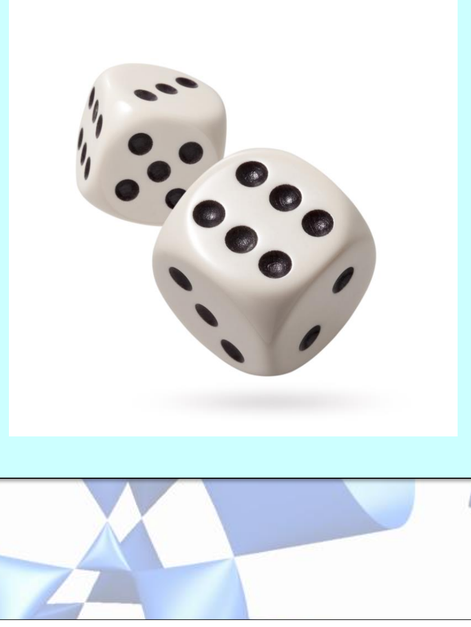
Lessons learnt

Using some sort of exoteric and almost-forgotten mathematics turned out to be the key ingredient of the attack. Generalising the mathematical concepts underlying existing cryptographic protocols could lead to new interesting **cryptoanalysis**.

Moving on

The ideas employed in the attack could be used constructively. The more complicated arithmetic of Abelian surfaces could be utilised to design other cryptographic primitives.

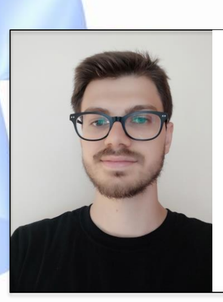
For instance, applications to **randomness beacons** in blockchains have already been considered.



Literature cited

[1] https://sike.org/

[2] LM, C. Martindale, “An attack on SIDH with arbitrary starting curve”



Luciano Maino

luciano.maino@bristol.ac.uk

Supervisors: Dr Chloe Martindale, Dr Matthew Bisatt