Short proposal for EU Class-Group-Cost-Action

March 19, 2020

1 Project aim

The European community of isogeny-based cryptographers is growing fast, and those with sufficient resources have already been arranging short workshops to meet and exchange ideas. For example, the isogeny days at KU Leuven, the mini-symposium at the SIAM-AG conference,[1] the recent workshop in Birmingham,[2] or the upcoming summer school in Bristol.[3] However, by necessity, these relatively informal events are only open to researchers with access to travel money from their university or personal grants.

With the rapidly growing interest in isogeny-based problems, we want to encourage (especially early career) researchers from all over Europe to meet regularly to exchange ideas, with the aim of working on the major open problems in the area. That is, we want to make the existing informal network into a more formal network, increasing both the frequency of the meetings and the accessibility.

There are interesting open problems in isogeny-based cryptography involving both advanced mathematics (especially number theory) and advanced quantum information theory. Therefore, another major aim of this project is to bring people from number theoretic and quantum information theoretic backgrounds together with cryptographers to learn about and work on major open problems with the benefit of different perspectives.

2 Project plan

- At least once a year, in rotating locations, we will have a large workshop with all consortium partners and international experts from outside the consortium. This workshop will have both educational (lectures/school) and research (collaboration) components.
- Throughout each year, we will organise several smaller workshops run by a few different groups of partners throughout each year. These will also

[1] https://mathsites.unibe.ch/siamag19/

[2] https://iahmed88.wixsite.com/website

[3] https://isogenyschool2020.co.uk

be open to international interest from outside the consortium, and be either educational or collaboration focussed depending on the needs of the partners organising that workshop.

- We will support travel for continued collaboration between partners of the project.
- There is currently no comprehensive resource (such as a textbook) for learning the required background for this topic. We will put together a textbook containing the necessary background. We will also collate videos, blog posts, and other useful learning material from our schools and workshops on an open source online platform to aid newcomers to the topic.
- If appropriate, we will publish proceedings resulting from the research workshops.

3 Project background

Steady progress towards scalable quantum computers is threatening the foundation of asymmetric cryptography. There has been considerable effort in the last few years to develop new methods in cryptography that are resistant to advances in quantum computing, a field that has become known as *post-quantum cryptography.* These efforts include a standardization effort being run by NIST [9] to find new cryptography standards for industry and government that are quantum resistant.

The newest major area within post-quantum cryptography is *isogeny-based cryptography*, representing just one of n entries in the NIST competition, SIKE [5]. This protocol is a key encapsulation protocol based on SIDH [6] introduced by David Jao and Luca De Feo in 2011. It boasts the smallest private and public key sizes of all the entries in the NIST competition by a significant margin. Although it is the only isogeny-based entry in the NIST competition, there are now competing isogeny-based schemes [3, 2, 1] that have been introduced since 2016. As the topic is young it is likely that more competing schemes are still to come; indeed we hope that this project will start collaborations on new isogeny-based schemes, for example with higher functionality than the current proposals. The mathematical world of isogenies is extremely rich, and there are certainly more options to be explored, especially in a collaboration between number theorists and cryptographers.

As NIST pushes for standardization, there is still a lot of work to be done on cryptanalysis, even on the oldest isogeny-based scheme SIDH/SIKE. For example, Petit's attacks from 2017 [10] have been very recently improved [7] and could feasibly still be further improved with a new idea in the next years. The quantum cryptanalysis on the recent scheme CSIDH is far from understood for any concrete parameters [8], and a very recent paper [4] gave new ideas for classical cryptanalysis. It is vital that the community is confident that the cryptanalysis of these proposals and any future proposals is thorough before any kind of standard is proposed. Another vital topic to address before standardization is secure and efficient implementation, which is also still in the phase of continuous improvement. Isogeny-based systems, while boasting small key sizes, are relatively slow even compared to their competitors in the post-quantum world, so efficient implementation is necessary for these schemes to be of any practical use.

4 Partner countries

We welcome more partners, and currently include the following in our planned consortium:

- Belgium
  - KU Leuven: Wouter Castryck and Frederik Vercauteren
- Croatia
  - University of Zagreb: Filip Najman
- Czech Republic
  - Masaryk University: Vashek Matyas
- France
  - INRIA Paris: Ben Smith
- Hungary
  - Eötvös Loránd University: Sandor Kiss, Gergely Zábrádi
- Switzerland
  - IBM Research Zurich: Luca De Feo
- The Netherlands
  - Eindhoven University of Technology: Tanja Lange, Lorenz Panny
- Turkey
  - Yasar University: Huseyin Hisil
- United Kingdom
  - Birmingham University: Christophe Petit
  - Bristol University: Chloe Martindale

References

[1] Ward Beullens, Thorsten Kleinjung, and Frederik Vercauteren. CSI-FiSh: Efficient isogeny based signatures through class group computations. In *ASIACRYPT 2019*, 2019.

[2] Wouter Castryck and Thomas Decru. CSIDH on the surface. Cryptology ePrint Archive Report 2019/1404, 2019.

[3] Wouter Castryck, Tanja Lange, Chloe Martindale, Lorenz Panny, and Joost Renes. CSIDH: An efficient post-quantum commutative group action. In *ASIACRYPT 2018*, 2018.

[4] Wouter Castryck, Jana Sotáková, and Frederik Vercauteren. Breaking the decisional Diffie-Hellman problem for class group actions using genus theory. Cryptology ePrint Archive Report 2020/151, 2020.

[5] David Jao, Reza Azarderakhsh, Matthew Campagna, Craig Costello, Luca De Feo, Basil Hess, Amir Jalali, Brian Koziel, Brian LaMacchia, Patrick Longa, Michael Naehrig, Joost Renes, Vladimir Soukharev, and David Urbanik. Supersingular isogeny key encapsulation. 2019.

[6] David Jao and Luca de Feo. Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies. In *PQCrypto 2011*, 2011.

[7] Péter Kutas, Chloe Martindale, Lorenz Panny, Christophe Petit, and Kate Stange. Weak instances of SIDH under improved torsion point attacks, 2020. (upcoming).

[8] Chloe Martindale. *Overview of Attacks on Elliptic Curve Isogenies Based Systems*, 2020. Talk: `https://simons.berkeley.edu/talks/overview-attacks-elliptic-curve-isogenies-based-systems-0`.

[9] National Institute of Standards and Technology. Post-quantum cryptography standardization, December 2016. `https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Post-Quantum-Cryptography-Standardization`.

[10] Christophe Petit. Faster algorithms for isogeny problems using torsion point images. In *ASIACRYPT 2017*, 2017.