Titles and abstracts LID4:

Andrea Basso: New SIDH Countermeasures for More Efficient Key Exchanges

Abstract: The Supersingular Isogeny Diffie-Hellman (SIDH) protocol has been the most efficient isogeny-based encryption protocol, until a series of breakthroughs led to a polynomial-time key-recovery attack on SIDH. While some countermeasures have been proposed, the resulting schemes are significantly slower and larger than the original protocol.

In this talk, we discuss new countermeasure techniques that lead to significantly more efficient and compact protocols. We first introduce the concept of artificially oriented curves, which are curves with an associated pair of subgroups. We show that this information is sufficient to build parallel isogenies and thus obtain an SIDH-like key exchange, which also reveals significantly less information compared to previous constructions. We thus obtain two such protocols: binSIDH (or binary SIDH), which relies on fixed-degree isogenies, and terSIDH (or ternary SIDH), which instead is more efficient but requires variable degree isogenies. We also present a hybrid variant of binSIDH and terSIDH where one party computes SIDH-like isogenies, resulting in reduced computation times for one party at the cost of a moderate increase for the other party.

Lastly, we present our proof-of-concept implementation of the proposed protocols and discuss their results. Despite being implemented in a high-level language, these protocols show very competitive running times, which suggests they might be the most efficient isogeny-based encryption protocols.

Guido Lido: Isogeny graphs with level structure and their spectrum

A familiar object in isogeny based cryptography is the graph whose vertices are supersingular elliptic curves and whose edges are isogenies of fixed degree l. It is immediate to prove that from each vertex there are exactly l+1 outgoing edges, while it is less obvious that such a graph is connected and that it has the Ramanujan property, a property about the spectrum of the adjacency matrix that implies that random walks very soon visit all vertices with the same probability. In our talk we look at a generalization of these graphs, namely graphs whose vertices are pairs (E,T), where E is a supersingular elliptic curve and T is some information on the n-torsion of E (e.g. a basis, a point, a subgroup) for fixed n. It is easy to notice that the secret keys in SIDH are exactly walks in such a generalized isogeny graph, and the public keys are vertices. These graphs can be multipartite, implying that the Ramanujan property is not always satisfied. By studying modular curves over mixed characteristics we relate isogeny graphs to geometric and cohomological objects, which allows us to prove the appropriate modification of the Ramanujan property. The properties of these generalized isogeny graphs are useful for a statistical zero knowledge proof of knowledge of an isogeny, which is part of a work with Basso, Connolly, De Feo, Fouotsa, Morrison, Panny, Patranabis and Wesolowski to generate elliptic curves with unknown endomorphisms.

Mingjie Chen: SCALLOP-HD: group action from 2-dimensional isogenies

In this talk, we present a new group action called SCALLOP-HD, which builds on the recent SCALLOP group action introduced by De Feo, Fouotsa, Kutas, Leroux, Merz, Panny and Wesolowski in 2023. Utilizing the isogeny embedding technique from Kani's Lemma, SCALLOP-

HD surpasses SCALLOP in scalability and potentially in efficiency — a claim to be confirmed by implementation results. This is joint work with Antonin Leroux.

Jonas Meers: Solving the Hidden Number Problem for CSIDH and CSURF via Automated Coppersmith

We define and analyze the Commutative Isogeny Hidden Number Problem, which is the natural analogue of the Hidden Number Problem in the CSIDH and CSURF setting. In short, the task is as follows: Given two supersingular elliptic curves E_A , E_B and access to an oracle that outputs some of the most significant bits of the CDH of two curves, an adversary must compute the shared curve $E_{AB} = CDH(E_A, E_B)$. We show that we can recover E_{AB} in polynomial time by using Coppersmith's method as long as the oracle outputs $13/24 + \varepsilon \approx 54\%$ (CSIDH) and $31/41 + \varepsilon \approx 76\%$ (CSURF) of the most significant bits of the CDH, where $\varepsilon > 0$ is an arbitrarily small constant.

Jana Sotáková: Computing traces of endomorphisms

Take a supersingular elliptic curve E with unknown endomorphism ring. Now suppose that by some magic you obtain several endomorphisms on E, say, given to you as cycles in some isogeny graph. To be able to identify the quaternionic order they generate and break all your favorite cryptography, you still need to compute the trace pairing on End(E). In joint work with Travis Morrison, Lorenz Panny, and MIchael Wills, we improve on this computational task using a generalization of the SEA algorithm together with several tricks to speed up the process.

Pierrick Dartois: SQISignHD: signing with higher dimensional isogenies.

The SQISign isogeny-based post-quantum digital signature scheme introduced by De Feo, Kohel, Leroux, Petit and Wesolowski outputs very compact signatures at the expense of a high signature time. In this presentation, we recall how SQISign works and introduce a new scheme based on SQISign and the polynomial time torsion point attacks against SIDH due to Castryck, Decru, Maino, Martindale and Robert. We use these ideas to sign with dimension one isogenies and verify with higher dimensional isogenies. This scheme scheme has better security properties and signatures even more compact than in the original SQISign scheme. We provide an implementation of the signature way faster than SQISign. For the verification phase, we propose a proof of concept implementation of dimension four isogeny computation, demonstrating the potential of our scheme for cryptographic applications.

Tako Boris Fouotsa: A look at SQISignHD.

Laurane Marco: Towards Isogeny Based Encryption from the MSIDH and the SIDH attacks.

At Eurocrypt 2023, three papers (Castryck-Decru, Maino-Martindale-Panny-Pope-Wesolowski, Robert) described polynomial attacks on SIDH/SIKE. These attacks solve the supersingular isogeny problem with smooth torsion point information, assuming the order of the torsion points is at least the square root of the degree of the secret isogeny. At the same conference, some relatively costly countermeasures were suggested by Fouotsa, Moriya and Petit, among which M-SIDH. In M-SIDH, the torsion point information is masked using a secret scalar, which is hard to recover for some well chosen parameters. In the same paper, an attack that exploits small endomorphisms on the starting curve in M-SIDH was presented. Hence obliging the scheme to

use a curve with unknown endomorphism ring, or a curves with provably no small endomorphism.
In this work, we show how to transform this small endomorphism attack on M-SIDH into a trapdoor one way function, which we name setaHD We then use our trapdoor one way function to derive a public key encryption scheme. More importantly, we show how to derive an Identity Based Encryption scheme from our trapdoor one way function.
This is the very first isogeny based Identity Based Encryption scheme. We discuss the security of our schemes and provide parameter estimates.
The decryption algorithm in both our public key encryption scheme and our Identity Based Encryption scheme computes higher dimension (dimension 8 in general, and dimension 4 at the cost of using larger parameters) isogenies of prime degree up to thousands. There are polynomial time formulas to compute these isogenies but they are not yet practical. Hence our constructions are theoretical to date, but a proof of concept implementation may be possible in the near future since the computation of higher dimension isogenies is an active research area.

Jonathan Komada Eriksen AprèsSQI: A pretty rad extension to signing in SQIsign

We improve verification in the SQIsign signature scheme. By using higher extension fields in the signing procedure, we are able to significantly extend the amount of $2^\bullet$-torsion available, which provides a large speed-up in verification, at the cost of a modest slow down during signing. Moreover, the increase in $2^\bullet$-torsion allows several other speed-ups on the level of curve arithmetic. The synergy between these high-level and low-level improvements allow a verification speed-up up to a factor of (TBD, currently, more than 3 times) for NIST Level I in terms of Fp-operations compared to the verification currently used in the reference implementation of SQIsign.

Bruno Sterner: Twin-smooth integers in isogeny-based cryptography

Some recent isogeny-based cryptosystems are instantiated using cryptographic-sized primes p such that p^2-1 is either smooth or has a large smooth cofactor. This includes the signature scheme SQISign that was recently submitted to NIST's alternative signatures proposal. Finding such primes that minimise the smoothness bound of p^2-1 is the most challenging part of this problem. This is because there is a theoretical limit as to how small the smoothness bound of p^2-1 can be. In this talk, I aim to present current and upcoming ideas that address this problem and its related problem of finding twin-smooth integers as well as discuss some subtleties when applying these ideas to cryptosystems.

Steven Galbraith: Some remarks on CSIDH and CSI-FiSh

The talk will discuss joint work with Hart Montgomery and Yi-Fu Lai on improving the quantum reduction from the group action DLP (vectorization) to the group action CDH (parallelization) in the case of CSIDH. The talk will also mention a lattice paradox in the CSIDH lattice, and why it does not help the asymptotic complexity of CSI-FiSh.

Damien Robert: Arithmetic of Kummer lines

We give formulas for the arithmetic of the biextension associated to the divisor $2(0_E)$ on different models of Kummer lines. Exponentiation in this biextension then gives efficient pairings algorithms.

Robi Pedersen: A new toolbox for CSIDH

The group action description of CSIDH allows a lot of versatility in the construction of cryptographic protocols, mainly due to the commutative composability of ideals in the group. Although this gives us more flexibility than the generic isogeny or the SIDH setting, many complex applications still seem out of reach.
In this work, we explore new approaches to compose ideals. We view the acting group as additive and explore the possibility of realizing multiplication, exponentiation and polynomial evaluation in this group. We realize these functionalities both in an ad-hoc way and using MPC techniques.
We then explore zero-knowledge proofs for these new arithmetic operations. While some of these proofs rely on a trusted setup, we also discuss how it can be removed in the MPC-in-the-head setting using cut-and-choose techniques.
We conclude our work by discussing applications of our new toolbox, including some failed attempts.

Marzio Mula: Hessian graphs

The determinant of the Hessian matrix of an elliptic curve E with nonzero j-invariant yields another elliptic curve Hess(E). Working up to isomorphism, we consider the map that sends a j-invariant in a finite field Fq to the j-invariant of the corresponding Hessian curve. This map defines a discrete dynamical system, i.e. a functional graph which we call Hessian graph, whose structure is remarkably regular. In light of applications to the problem of hashing in the supersingular Fp-isogeny graph, we attempt to characterize the connected components of the Hessian graph over Fp in which supersingular j-invariants are found. Joint work with F. Pintore and D. Taufer.

Yi-Fu Lai: Isogeny-based Blind Signatures and a New ROS Attack
In this talk, we construct the first provably-secure isogeny-based (partially) blind signature scheme using isogeny group actions. While at a high level the scheme resembles the Schnorr blind signature, our work does not directly follow from that construction, since isogenies do not offer as rich an algebraic structure.
Specifically, our protocol does not fit into the linear identification protocol abstraction introduced by Hauck, Kiltz, and Loss (EUROCYRPT'19), which was used to generically construct Schnorr-like blind signatures based on modules such as classical groups and lattices.
In more detail, our blind signature exploits the quadratic twist of an elliptic curve in an essential way to endow isogenies with a strictly richer structure than abstract group actions (but still more restrictive than modules). The basic scheme has public key size 128 B and signature size 8 KB under the CSIDH-512 parameter sets—these are the smallest among all provably secure post-quantum secure blind signatures.
Relying on a new ring variant of the group action inverse problem (GAIP), we can halve the signature size to 4 KB while increasing the public key size to 512 B. We provide preliminary cryptanalysis of and show that for certain parameter settings, it is essentially as secure as the standard . Finally, we show a novel way to turn our blind signature into a partially blind signature, where we deviate from prior methods since they require hashing into the set of public

keys while hiding the corresponding secret key—constructing such a hash function in the isogeny setting remains an open problem.

The security proofs in the paper show the log-concurrent security of the one more unforgeability for our schemes. It was believed that the non-linear structure of elliptic curves can make the scheme polylog-concurrently secure, which is essential to the polynomial-time ROS attack. We show a new variant of the ROS attack, running in polynomial time, that can break the polylog-concurrent security of the CSI-Otter and a few lattice-based blind signature schemes.