Problem 3

Hashing into Supersingular Curves

by Steven D. Galbraith

1 Introduction

There are many situations in discrete-log based cryptography when one wants to "hash" to the group. One famous example is the BLS signature scheme [BLS04], where $H(m)$ is a group element and the signature is $[s]H(m)$, where s is the private key of the signer. It is also a convenient fact that one can easily set up instances of the discrete logarithm problem such that no-one knows the solution. For example, one can choose a large prime p such that 2 is a primitive root modulo p, and ask for the discrete logarithm of 3 with respect to the base 2. This allows for *untrusted setup* for schemes like Pedersen commitments. For finite fields and elliptic curves it is well-understood how to generate arbitrary group elements and hence the problem of hashing to the group is easy. For ideal class groups there are some subtleties, but it is a solved problem [SBK25].

In isogeny-based cryptography it is natural to ask if these sorts of task can also be performed. In the context of isogenies, this usually means generating a supersingular curve E over a given field $\mathbb{F}_{p^2}$ in such a way that nothing is known about the endomorphism ring $\mathrm{End}(E)$, not even to the person who generated the curve. For example, this is needed to securely use the CGL hash [EHL+18], for a commitment scheme [Ste21], and for many other protocols.

2 History

The problem of generating a random supersingular curve was mentioned by Boneh and Love [LB20] where they called it *demonstrating a hard curve*.

There is no good solution known to the problem. Two papers explicitly discuss unsuccessful attempts to solve the problem [BBD+24; MMP25]. Mostly these are exploring mathematical ideas that might allow to produce a supersingular curve without leaking information, but none of the solutions is satisfactory. There is also a quantum algorithm proposed in [BBD+24], where the idea is to perform a random walk "in superposition" and then observe the quantum state so that it "collapses" to a single elliptic curve (also see [MDJ26]). One problem with that approach is that it is intrinsically non-deterministic and so can't be used as a hash function. There is also the risk that a malicious party would perform the observations a different way to learn information about the isogeny path.

To get around the lack of a solution to the problem, multi-party protocols have been developed that allow such a curve to be set up by a collection of

mutually untrusting players [BD21; BCC+23; MJ23]. This approach is suitable in some contexts, but is not always an acceptable solution to the problem.

3 Problem Statement

Problem 3: Hashing into Supersingular Curves

Given a prime p, output a deterministic algorithm H that takes a random seed m as input and computes in polynomial-time the j-invariant[1] of a supersingular curve E over $\mathbb{F}_{p^2}$. Any user who runs H must not learn any information about the endomorphism ring beyond the information available if they were just provided by the curve E. Similarly, any user who runs H must not learn any information to help compute an isogeny from E to any other previously fixed supersingular curve E_0 over $\mathbb{F}_{p^2}$.

It is important to understand that a solution to this problem is an algorithm, and the main property of the algorithm is that it is secure even when run by a malicious user. For example, it is easy to write an algorithm to sample a random supersingular curve that deletes the internal state when the algorithm terminates, and only outputs E. But a malicious user who deviates from the correct execution by remembering the internal state would be able to learn $\mathrm{End}(E)$. It is also important that the person who designed the algorithm should not have any advantage over other users. For example, an algorithm that contains a hard-coded list of supersingular curves would not be acceptable, since the implementer might know $\mathrm{End}(E)$ for all the curves.

This problem is of a different nature to other isogeny problems as it is about the existence of an algorithm, rather than about the complexity of solving a computational problem. So it is unclear if there is any way to relate it to any other standard computational problem in isogeny crypto. It is also unclear whether there is any way to prove it is hard to solve the problem.

In most applications we require the set of possible outputs of H to be exponentially large. Indeed, we would ideally want the output E to be uniformly distributed (in the sense that if the seeds m are sampled uniformly from a large enough set then the output distribution $H(m)$ is arbitrarily close to uniform on the set of supersingular j-invariants).

Note that one can efficiently recognise a supersingular curve E. The obstruction to solving this problem by random sampling is that the probability that a random $j \in \mathbb{F}_{p^2}$ is supersingular is roughly $12/p$, and hence one cannot reach a supersingular curve in polynomial time.

Some related problems are discussed in [GS25].

[1] Any other well-defined representative of isomorphism classes of supersingular curves could also be used instead of the j-invariant.

References

[BBD+24] Jeremy Booher, Ross Bowden, Javad Doliskani, Tako Boris Fouotsa, Steven D Galbraith, Sabrina Kunzweiler, Simon-Philipp Merz, Christophe Petit, Benjamin Smith, Katherine E Stange, et al. "Failing to hash into supersingular isogeny graphs". In: *The Computer Journal* 67.8 (2024), pp. 2702–2719 (cit. on p. 1).

[BCC+23] Andrea Basso, Giulio Codogni, Deirdre Connolly, Luca De Feo, Tako Boris Fouotsa, Guido Maria Lido, Travis Morrison, Lorenz Panny, Sikhar Patranabis, and Benjamin Wesolowski. "Supersingular Curves You Can Trust". In: *Advances in Cryptology - EUROCRYPT 2023*. Ed. by Carmit Hazay and Martijn Stam. Vol. 14005. Lecture Notes in Computer Science. Springer, 2023, pp. 405–437. DOI: 10.1007/978-3-031-30617-4_14 (cit. on p. 2).

[BD21] Jeffrey Burdges and Luca De Feo. "Delay Encryption". In: *Advances in Cryptology - EUROCRYPT 2021 - 40th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Zagreb, Croatia, October 17-21, 2021, Proceedings, Part I*. Ed. by Anne Canteaut and François-Xavier Standaert. Vol. 12696. Lecture Notes in Computer Science. Springer, 2021, pp. 302–326. ISBN: 978-3-030-77869-9. DOI: 10.1007/978-3-030-77870-5_11 (cit. on p. 2).

[BLS04] Dan Boneh, Ben Lynn, and Hovav Shacham. "Short Signatures from the Weil Pairing". In: *J. Cryptol.* 17.4 (2004), pp. 297–319. DOI: 10.1007/S00145-004-0314-9 (cit. on p. 1).

[EHL+18] Kirsten Eisenträger, Sean Hallgren, Kristin Lauter, Travis Morrison, and Christophe Petit. "Supersingular Isogeny Graphs and Endomorphism Rings: Reductions and Solutions". In: *Advances in Cryptology – EUROCRYPT 2018*. Ed. by Jesper Buus Nielsen and Vincent Rijmen. Cham: Springer International Publishing, 2018, pp. 329–368. ISBN: 978-3-319-78372-7 (cit. on p. 1).

[GS25] Elif Ozbay Gurler and Patrick Struck. "How (not) to Build Identity-Based Encryption from Isogenies". In: *Selected Areas in Cryptography - SAC 2025 - 32nd International Conference, Toronto, ON, Canada, August 13-15, 2025, Revised Selected Papers*. Ed. by Christina Boura, Atefeh Mashatan, and Ali Miri. Vol. 16207. Lecture Notes in Computer Science. Springer, 2025, pp. 589–615. ISBN: 978-3-032-10535-6. DOI: 10.1007/978-3-032-10536-3_22 (cit. on p. 2).

[LB20] Jonathan Love and Dan Boneh. "Supersingular curves with small noninteger endomorphisms". In: *Proceedings of ANTS, Open Book Series* 4.1 (2020), pp. 7–22 (cit. on p. 1).

[MDJ26] Maher Mamah, Jake Doliskani, and David Jao. *Spectral Theory of Isogeny Graphs and Quantum Sampling of Secure Supersingular Elliptic Curves*. Cryptology ePrint Archive, Paper 2026/171. 2026. URL: https://eprint.iacr.org/2026/171 (cit. on p. 1).

[MJ23] Youcef Mokrani and David Jao. "Generating supersingular elliptic curves over F p with unknown endomorphism ring". In: *International Conference on Cryptology in India*. Springer. 2023, pp. 159–174 (cit. on p. 2).

[MMP25] Marzio Mula, Nadir Murru, and Federico Pintore. "On random sampling of supersingular elliptic curves". In: *Annali di Matematica Pura ed Applicata (1923-)* 204.3 (2025), pp. 1293–1335 (cit. on p. 1).

[SBK25] István András Seres, Péter Burcsi, and Péter Kutas. "How (Not) to Hash into Class Groups of Imaginary Quadratic Fields?" In: *Topics in Cryptology - CT-RSA 2025 - Cryptographers' Track at the RSA Conference 2025, San Francisco, CA, USA, April 28-May 1, 2025, Proceedings*. Ed. by Arpita Patra. Vol. 15598. Lecture Notes in Computer Science. Springer, 2025, pp. 303–326. ISBN: 978-3-031-88660-7. DOI: 10.1007/978-3-031-88661-4_13 (cit. on p. 1).

[Ste21] Bruno Sterner. "Commitment Schemes from Supersingular Elliptic Curve Isogeny Graphs". In: *IACR Cryptol. ePrint Arch.* 2021 (2021), p. 1031. URL: https://eprint.iacr.org/2021/1031 (cit. on p. 1).