Problem 7

Strong Encryption Protocols

by Luca De Feo

1 Introduction

Construct public key encryption (nearly) as secure as SQIsign.

2 History

Isogeny-based key exchange and public key encryption (PKE) has been a bumpy journey. The Couveignes–Rostovtsev–Stolbunov [Cou06; RS06] key exchange started the whole field. Today, it is understood as one instantiation of a cryptographic group action, together with CSIDH [CLM+18], SCALLOP [FFK+23], PEGASIS [DEF+25], etc. It is a simple and elegant scheme whose security reduces to the group-action analogue of CDH, or even of discrete logarithm, thanks to a quantum reduction [GPSV18]. However, group-action-discrete-log is solved in quantum subexponential time by Kuperberg's algorithm, which is less than ideal.

SIDH [JD11] initiated the trend of isogeny-based key exchange based on "experimental" assumptions. It took 10 years for the experiment to terminate with a non-passing grade [CD23; MMP+23; Rob23]. Since then, several "fixes" to SIDH have emerged [FMP23; BF23; BMP23; BM25]. What they've got over group actions, is exponential quantum security, and thus (to varying degrees) small ciphertexts and public keys. However they are all based on some isogeny-with-torsion-information type of assumption [DFP24], unnervingly reminiscent of SIDH.

20+ years of research on isogeny-based crypto have singled out the Supersingular Isogeny Problem as the golden standard for a post-quantum assumption. The problem is now known to be equivalent to the *supersingular endomorphism ring problem (EndRing)* [Wes21], and the best quantum algorithms essentially amount to Grover search over the solution space [DG16; BJS14]. Despite this, **we only know how to build signatures whose security reduces to (nearly) EndRing** [BCC+23; ABD+25]. Ok, signatures and a handful of related primitives.

3 Problem Statement

Ideally, a solution to this problem would be a key exchange or PKE/KEM whose security reduces to EndRing, no strings attached. However this is probably

asking too much: the security of PKEs is defined via a deciding game, thus a reduction to a decisional problem is to be expected, but the obvious decisional version of EndRing is easy to decide.

The Random Oracle Model (ROM) can often be leveraged to reduce a distinguishing problem to a search problem, e.g., in the well known reduction of Hashed El Gamal's IND-CPA to CDH. We're ready to accept a proof in the ROM, as we are to accept one in an even more powerful model such as the Algebraic Isogeny Model [ABD+25]. Quantum reductions are of course allowed.

Problem 7: Strong Encryption Protocols

Define a Key Exchange or Public Key Encryption / Key Encapsulation Method and prove its passive / IND-CPA security reduces to the supersingular endomorphism ring problem (EndRing) via quantum polynomial reductions.

You are permitted use of:

- *The Generalized/Extended Riemann Hypothesis;*
- *Any standard symmetric assumptions on block/stream ciphers and hash functions;*
- *The Random Oracle Model;*
- *The Algebraic Isogeny Model.*

Efficiency of the scheme and tightness of the reduction are not criteria taken into account for this problem.

And if none of this is sufficient, we also accept as a solution a proof of impossibility of achieving key exchange or PKE / KEM based on EndRing in a *sufficiently credible* model. Because an abstract computation model must inevitably be formulated for this, and because opinions may vary on what "sufficiently credible" means, adjudging such a solution is left to the discretion of the proposers.

If we feel particularly inspired, we may even accept solutions that invoke extra assumptions, as long as they are widely accepted as "insignificant" in the face of EndRing. An example of such assumptions may be the "EndRing with hints" used to prove security of SQIsign [ABD+25]. Again, given the subjectivity of this criterion, we reserve full discretion in interpreting it.

Ultimately, the spirit of the problem is: **create PKE as secure as SQIsign**. As long as SQIsign is secure, that is... So don't be shy and submit your solution, if you feel it matches the description.

References

[ABD+25] Marius A. Aardal, Andrea Basso, Luca De Feo, Sikhar Patranabis, and Benjamin Wesolowski. "A Complete Security Proof of SQIsign". In: *Advances in Cryptology - CRYPTO 2025 - 45th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 17-21, 2025, Proceedings, Part VI*. Ed. by Yael Tauman Kalai and Seny F. Kamara. Vol. 16005. Lecture Notes in Computer Science. Springer, 2025, pp. 190–222. ISBN: 978-3-032-01886-1. DOI: 10.1007/978-3-032-01887-8_7 (cit. on pp. 1, 2).

[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. 1).

[BF23] Andrea Basso and Tako Boris Fouotsa. "New SIDH Countermeasures for a More Efficient Key Exchange". In: *Advances in Cryptology - ASIACRYPT 2023 - 29th International Conference on the Theory and Application of Cryptology and Information Security, Guangzhou, China, December 4-8, 2023, Proceedings, Part VIII*. Ed. by Jian Guo and Ron Steinfeld. Vol. 14445. Lecture Notes in Computer Science. Springer, 2023, pp. 208–233. ISBN: 978-981-99-8741-2. DOI: 10.1007/978-981-99-8742-9_7 (cit. on p. 1).

[BJS14] Jean-François Biasse, David Jao, and Anirudh Sankar. "A Quantum Algorithm for Computing Isogenies between Supersingular Elliptic Curves". In: *Progress in Cryptology - INDOCRYPT 2014 - 15th International Conference on Cryptology in India, New Delhi, India, December 14-17, 2014, Proceedings*. Ed. by Willi Meier and Debdeep Mukhopadhyay. Vol. 8885. Lecture Notes in Computer Science. Springer, 2014, pp. 428–442. ISBN: 978-3-319-13038-5. DOI: 10.1007/978-3-319-13039-2_25 (cit. on p. 1).

[BM25] Andrea Basso and Luciano Maino. "POKÉ: A Compact and Efficient PKE from Higher-Dimensional Isogenies". In: *Advances in Cryptology - EUROCRYPT 2025 - 44th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Madrid, Spain, May 4-8, 2025, Proceedings, Part II*. Ed. by Serge Fehr and Pierre-Alain Fouque. Vol. 15602. Lecture Notes in Computer Science. Springer, 2025, pp. 94–123. ISBN: 978-3-031-91123-1. DOI: 10.1007/978-3-031-91124-8_4 (cit. on p. 1).

[BMP23] Andrea Basso, Luciano Maino, and Giacomo Pope. "FESTA: Fast Encryption from Supersingular Torsion Attacks". In: *Advances in*

Cryptology – ASIACRYPT 2023. Ed. by Jian Guo and Ron Steinfeld. Vol. 14444. Lecture Notes in Computer Science. Springer, 2023, pp. 98–126. DOI: 10.1007/978-981-99-8739-9_4 (cit. on p. 1).

[CD23] Wouter Castryck and Thomas Decru. "An Efficient Key Recovery Attack on SIDH". In: *Advances in Cryptology - EUROCRYPT 2023 - 42nd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Lyon, France, April 23-27, 2023, Proceedings, Part V*. Ed. by Carmit Hazay and Martijn Stam. Vol. 14008. Lecture Notes in Computer Science. Springer, 2023, pp. 423–447. ISBN: 978-3-031-30588-7. DOI: 10.1007/978-3-031-30589-4_15 (cit. on p. 1).

[CLM+18] Wouter Castryck, Tanja Lange, Chloe Martindale, Lorenz Panny, and Joost Renes. "CSIDH: An Efficient Post-Quantum Commutative Group Action". In: *Advances in Cryptology - ASIACRYPT 2018 - 24th International Conference on the Theory and Application of Cryptology and Information Security, Brisbane, QLD, Australia, December 2-6, 2018, Proceedings, Part III*. Ed. by Thomas Peyrin and Steven D. Galbraith. Vol. 11274. Lecture Notes in Computer Science. Springer, 2018, pp. 395–427. ISBN: 978-3-030-03331-6. DOI: 10.1007/978-3-030-03332-3_15 (cit. on p. 1).

[Cou06] Jean Marc Couveignes. "Hard Homogeneous Spaces". In: *IACR Cryptol. ePrint Arch.* (2006), p. 291. URL: http://eprint.iacr.org/2006/291 (cit. on p. 1).

[DEF+25] Pierrick Dartois, Jonathan Komada Eriksen, Tako Boris Fouotsa, Arthur Herlédan Le Merdy, Riccardo Invernizzi, Damien Robert, Ryan Rueger, Frederik Vercauteren, and Benjamin Wesolowski. "PEGASIS: Practical Effective Class Group Action using 4-Dimensional Isogenies". In: *Advances in Cryptology - CRYPTO 2025 - 45th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 17-21, 2025, Proceedings, Part I*. Ed. by Yael Tauman Kalai and Seny F. Kamara. Vol. 16000. Lecture Notes in Computer Science. Springer, 2025, pp. 67–99. ISBN: 978-3-032-01854-0. DOI: 10.1007/978-3-032-01855-7_3 (cit. on p. 1).

[DFP24] Luca De Feo, Tako Boris Fouotsa, and Lorenz Panny. "Isogeny Problems with Level Structure". In: *Advances in Cryptology - EUROCRYPT 2024 - 43rd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Zurich, Switzerland, May 26-30, 2024, Proceedings, Part VI*. Ed. by Marc Joye and Gregor Leander. Vol. 14656. Lecture Notes in Computer Science. Springer, 2024, pp. 181–204. ISBN: 978-3-031-58750-4. DOI: 10.1007/978-3-031-58754-2_7 (cit. on p. 1).

[DG16] Christina Delfs and Steven D. Galbraith. “Computing isogenies between supersingular elliptic curves over $\mathbb{F}_p$”. In: *Des. Codes Cryptogr.* 78.2 (2016), pp. 425–440. DOI: 10.1007/S10623-014-0010-1 (cit. on p. 1).

[FFK+23] Luca De Feo, Tako Boris Fouotsa, Péter Kutas, Antonin Leroux, Simon-Philipp Merz, Lorenz Panny, and Benjamin Wesolowski. “SCALLOP: Scaling the CSI-FiSh”. In: *Public-Key Cryptography - PKC 2023 - 26th IACR International Conference on Practice and Theory of Public-Key Cryptography, Atlanta, GA, USA, May 7-10, 2023, Proceedings, Part I*. Ed. by Alexandra Boldyreva and Vladimir Kolesnikov. Vol. 13940. Lecture Notes in Computer Science. Springer, 2023, pp. 345–375. ISBN: 978-3-031-31367-7. DOI: 10.1007/978-3-031-31368-4_13 (cit. on p. 1).

[FMP23] Tako Boris Fouotsa, Tomoki Moriya, and Christophe Petit. “M-SIDH and MD-SIDH: Countering SIDH Attacks by Masking Information”. In: *Advances in Cryptology - EUROCRYPT 2023 - 42nd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Lyon, France, April 23-27, 2023, Proceedings, Part V*. Ed. by Carmit Hazay and Martijn Stam. Vol. 14008. Lecture Notes in Computer Science. Springer, 2023, pp. 282–309. ISBN: 978-3-031-30588-7. DOI: 10.1007/978-3-031-30589-4_10 (cit. on p. 1).

[GPSV18] Steven D. Galbraith, Lorenz Panny, Benjamin Smith, and Frederik Vercauteren. “Quantum Equivalence of the DLP and CDHP for Group Actions”. In: *IACR Cryptol. ePrint Arch.* (2018), p. 1199. URL: https://eprint.iacr.org/2018/1199 (cit. on p. 1).

[HS23] Carmit Hazay and Martijn Stam, eds. *Advances in Cryptology - EUROCRYPT 2023 - 42nd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Lyon, France, April 23-27, 2023, Proceedings, Part V*. Vol. 14008. Lecture Notes in Computer Science. Springer, 2023. ISBN: 978-3-031-30588-7. DOI: 10.1007/978-3-031-30589-4.

[JD11] David Jao and Luca De Feo. “Towards Quantum-Resistant Cryptosystems from Supersingular Elliptic Curve Isogenies”. In: *Post-Quantum Cryptography - 4th International Workshop, PQCrypto 2011, Taipei, Taiwan, November 29 - December 2, 2011. Proceedings*. Ed. by Bo-Yin Yang. Vol. 7071. Lecture Notes in Computer Science. Springer, 2011, pp. 19–34. ISBN: 978-3-642-25404-8. DOI: 10.1007/978-3-642-25405-5_2 (cit. on p. 1).

[MMP+23] Luciano Maino, Chloe Martindale, Lorenz Panny, Giacomo Pope, and Benjamin Wesolowski. “A Direct Key Recovery Attack on SIDH”. In: *Advances in Cryptology – EUROCRYPT 2023. Part V*. Ed. by Carmit Hazay and Martijn Stam. Vol. 14008. Lecture

Notes in Computer Science. Springer, 2023, pp. 448–471. DOI: 10.1007/978-3-031-30589-4_16 (cit. on p. 1).

[Rob23] Damien Robert. "Breaking SIDH in Polynomial Time". In: *Advances in Cryptology - EUROCRYPT 2023 - 42nd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Lyon, France, April 23-27, 2023, Proceedings, Part V*. Ed. by Carmit Hazay and Martijn Stam. Vol. 14008. Lecture Notes in Computer Science. Springer, 2023, pp. 472–503. ISBN: 978-3-031-30588-7. DOI: 10.1007/978-3-031-30589-4_17 (cit. on p. 1).

[RS06] Alexander Rostovtsev and Anton Stolbunov. "Public-Key Cryptosystem Based on Isogenies". In: *IACR Cryptol. ePrint Arch.* (2006), p. 145. URL: http://eprint.iacr.org/2006/145 (cit. on p. 1).

[Wes21] Benjamin Wesolowski. "The supersingular isogeny path and endomorphism ring problems are equivalent". In: *62nd IEEE Annual Symposium on Foundations of Computer Science, FOCS 2021, Denver, CO, USA, February 7-10, 2022*. IEEE, 2021, pp. 1100–1111. ISBN: 978-1-6654-2055-6. DOI: 10.1109/FOCS52979.2021.00109 (cit. on p. 1).