Bull. Aust. Math. Soc. **101** (2020), 508–509
doi:10.1017/S0004972720000210

ISOGENIES OF ABELIAN VARIETIES IN CRYPTOGRAPHY

YAN BO TI

(Received 3 February 2020; first published online 16 March 2020)

2010 *Mathematics subject classification*: primary 11T71; secondary 11Y40, 94A60.

Keywords and phrases: post-quantum cryptography, number theory.

Isogenies of abelian varieties have been used in cryptography to create post-quantum cryptosystems. In particular, supersingular elliptic curve isogenies have been used to construct key exchange, encryption and signature protocols and hash functions. This thesis concerns itself with results relating to this cryptosystem and presents four main findings: two attacks, a reduction and a generalisation.

The two attacks on the cryptosystem are an adaptive attack and a fault attack. The adaptive attack targets instances of the cryptosystem using static keys and is able to recover the secret with close to optimal number of queries for most use cases. The fault attack targets the cryptosystem embedded in hardware and is able to recover the entire secret with one successful perturbation.

The reduction shows that breaking the cryptosystem is at most as difficult as computing endomorphism rings of supersingular elliptic curves. It relies on the equivalence of the category of supersingular elliptic curves under isogenies and the category of invertible modules under homomorphisms.

We also generalise the cryptosystem from isogenies between supersingular elliptic curves to isogenies between supersingular principally polarised abelian surfaces. In particular, we propose a genus-two version of the key exchange protocol called Genus Two SIDH (G2SIDH). We perform some analysis of the security of G2SIDH by studying the isogeny graph of principally polarised abelian surfaces. A by-product of this study is that a naive generalisation of the hash function to genus two is no longer collision resistant.

Parts of this research have been published in [1–3].

Thesis submitted to the University of Auckland in June 2019; degree approved 9 October 2019; supervisor Steven Galbraith.

References

[1] E. V. Flynn and Y. B. Ti, 'Genus two isogeny cryptography', in: *Post-Quantum Cryptography: Proceedings of the 10th International Conference, PQCrypto 2019, Chongqing, China, 2019 Revised Selected Papers*, Lecture Notes in Computer Science, 11505 (Springer, Cham, 2019), 286–306.

[2] S. D. Galbraith, C. Petit, B. Shani and Y. B. Ti, 'On the security of supersingular isogeny cryptosystems', in: *Advances in Cryptology—ASIACRYPT 2016: Proceedings of the 22nd International Conference on the Theory and Application of Cryptology and Information Security, Hanoi, Vietnam, Part I*, Lecture Notes in Computer Science, 10031 (Springer, Berlin, 2016), 63–91.

[3] Y. B. Ti, 'Fault attack on supersingular isogeny cryptosystems', in: *Post-Quantum Cryptography: Proceedings of the 8th International Workshop, PQCrypto 2017, Utrecht, The Netherlands, 2017*, Lecture Notes in Computer Science, 10346 (Springer, Cham, 2017), 107–122.

YAN BO TI, Department of Mathematics,
University of Auckland, Auckland 1010, New Zealand
e-mail: yanbo.ti@gmail.com

https://doi.org/10.1017/S0004972720000210 Published online by Cambridge University Press