Chapter 0

Foreword and postscript

SIKE and SIDH are insecure and should not be used. On August 5, 2022, Castryck and Decru posted a preprint [5] outlining an efficient classical key recovery algorithm against SIDH along with code implementing the algorithm and demonstrating its practicality. This work relies on the particular choice of starting curve value of $A = 6$ used in SIKE, but follow-up work by Maino and Martindale [38] and Robert [45] has shown that any modification of SIDH along the lines of varying the starting curve is also insecure. Moriya [40] and Fouotsa [18] have independently proposed different approaches to modifying SIDH to avoid the Castryck and Decru family of attacks, but both of these proposals severely degrade the performance and key size of SIDH by at least an order of magnitude. The general consensus at this time is that there is no known variant of SIDH which both retains roughly the same performance characteristics as what was originally proposed while also remaining secure.

The SIKE team considered the possibility of withdrawing from the NIST standardization process in light of these new results, but decided that the public would be better served by taking the opportunity to submit a 4th round proposal with this postscript included (and no other changes), so that the final version of the SIKE proposal accurately reflects the current status of the cryptosystem. Not everyone who browses the NIST PQCrypto candidates stays up to date with the discussion forum, and over time the record of what happened to SIKE may fade in long-term memory, so there is value in having NIST itself preserve this information, in the place where it is most likely to be seen by unwitting potential users. We recognize that we are lucky in this respect and that not every team overseeing a broken submission has had the opportunity to close out their submission in this manner.

Although there are no other active isogeny-based candidates participating in the NIST standardization process, we hope that research and development into isogeny-based cryptosystems will continue and that the post-quantum research community will continue to support and participate in such work. We stress that some isogeny-based cryptosystems, such as CGL [7], CSIDH [6], and SQIsign [14], are **not** based on SIDH, and are unaffected by the Castryck and Decru family of attacks. Although these cryptosystems are not currently active candidates in the NIST standardization process, our hope is that the research community will continue to study and develop these and other isogeny-based schemes with an eye towards eventual standardization.

The SIKE team wishes to thank all of the researchers and participants in the NIST standardization process who contributed to implementing, studying, benchmarking, and cryptanalyzing our submission. Such efforts are the means by which progress in science is achieved.