Hardware design for supersingular isogeny Diffie-Hellman key exchange

Lejla Batina, Pedro Maat Masolino, and Joost Renes

Digital Security Group, Radboud University, The Netherlands
{lejla, P.Massolino, j.renes@cs.ru.nl}

Abstract Recently, there is a lot of initiative for looking into suitable post-quantum cryptography (PQC) alternatives to classical public-key cryptography (PKC) algorithms such as RSA and Elliptic Curve Cryptography (ECC). Namely, when a powerful quantum computer would be built, these PKC algorithms are expected to be broken.
In this work we discuss hardware design challenges and trade-offs for supersingular isogeny Diffie-Hellman (SIDH) key-exchange. SIDH is an interesting primitive because it features substantially shorter public keys than other post-quantum key-exchange alternatives. At the moment, there exist several SIDH-based proposals for key-exchange and signatures and while the security of those is yet to be scrutinized, it is clear that efficient implementations in both software and hardware are challenging.
Similar to classical public-key cryptosystems, isogeny-based algorithms rely heavily on modular multiplication. The best known algorithm for modular multiplication in hardware is Montgomery multiplication. The main idea is to replace expensive divisions modulo a large integer by cheap divisions by a power of 2 that can be realized by simple bit shifts. Nevertheless, the special structure of primes used in isogeny-based cryptography i.e. primes of the form of $p = f \cdot 2^a 3^b - 1$ brings in new challenges in optimizing existing algorithms for finite field arithmetic.
Moreover, there is a need for hybrid solutions: key-exchange or signatures that are based on the combination of of classic and post-quantum schemes. Such schemes would only break if the classic and the post-quantum scheme were both broken and hence provide a higher level of assurance. With respect to this, ECC is a natural alley of SIDH using ECC arithmetic as an underlying layer for efficient implementations.
In this work we propose a flexible hardware architecture that supports both ECDH and SIDH. To this end, we use a bipartite modular multiplication method that is combining the Montgomery and classical modular multiplication algorithm. The hardware realization of the algorithm implies a substantial speed-up with some overhead in area. Finally, we also discuss side-channel resistance for our architecture and propose some "almost-free" countermeasure benefiting from the mathematical structure of SIDH.

Keywords: Post-quantum cryptography, isogenies, Diffie-Hellman key exchange, hardware implementations