Supersingular Isogeny Key Exchange

Paul Galloway
pgalloway@cs.ucsb.edu

November 1st, 2015

Abstract

It is estimated that production-ready quantum computers will become a reality within the next 15 to 20 years.[1] If such devices are realized in the near future then many of the currently established public key encryption algorithms (specifically RSA, Diffie-Hellman, Elliptic Curve Diffie-Hellman, and Elliptic Curve DSA) will become insecure and will need to be replaced. It is prudent for us to begin considering such a scenario and to look into possible replacements.

In this paper we review the post-quantum Key exchange scheme known as Supersingular Isogeny Key Exhange (SIDH). This type of key exchange provides “forward secrecy” and any attack by a quantum system still takes exponential time.[2] Additionally, like the established Elliptic Curve Diffie-Hellman system, SIDH provides similar key sizes and computationally efficient implementations when compared to established schemes.

Along the way we will mention some necessary mathematical constructs that will supplement our basic understanding of Elliptic Curves. Supersingular elliptic curves and isogenies between such curves will be explored. We will show how such constructs allows us to thwart analysis by a quantum system.[3] Finally, we will mention why such a key exchange scheme is superior to other post-quantum systems such as the McEliece system or NTRU.

References

[1] http://www.ibmsystemsmag.com/mainframe/trends/IBM-Research/quantum_computing/
[2] http://cacr.uwaterloo.ca/techreports/2011/cacr2011-32.pdf
[3] http://ecc2011.loria.fr/slides/jao.pdf