Attacking the ECDLP with Quantum Computing

Sam Green and Can Kazilkale
sam.green@cs.ucsb.edu, cankizilkale@cs.ucsb.edu

November 1, 2015

Abstract

Quantum computers have been a topic of interest for cryptographers since the formulation of Shor's factoring algorithm in 1994 [3]. A modified version of Shor's algorithm for attacking the elliptic curve discrete logarithm problem (ECDLP) was created in 2003 [2]. The (theoretical) quantum ECDLP attack appears to have withstood the academic test of time [1, 4, 5].

In this presentation we will review the ECDLP and give the algorithmic complexity of the best known classical computing attack against the ECDLP. Next, we will give a brief introduction to quantum computing and related mathematical notation, after which we will cover a quantum ECDLP attack algorithm and will give an example. Finally, we will compare the complexity of the classical attack to the quantum attack we have covered.

References

[1] D. Cheung, D. Maslov, J. Mathew, and D. Pradhan. On the design and optimization of a quantum polynomial-time attack on elliptic curve cryptography. *Proceedings of the 3rd Workshop on Theory of Quantum Computation, Communication, and Cryptography*, Tokyo, Japan, February 2008.

[2] J. Proos and C. Zalka. Shor's discrete logarithm quantum algorithm for elliptic curves. *Quantum Information and Computation*, Vol. 3, No. 4, pp 317-344, July 2003.

[3] P. Shor. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. *Proceedings of the 35th Annual Symposium on Foundations of Computer Science*, Santa Fe, NM, November 1994.

[4] S. Yan. Quantum Attacks on ECDLP-Based Cryptosystems, in *Quantum Attacks on Public-Key Cryptosystems.* Springer, pp 137-188, March 2013.

[5] A. Childs, W. van Dam. Quantum algorithms for algebraic problems. Reviews of Modern Physics, Vol. 82, No. 1, pp 1-52, January 2010.