The Aspects of ECDSA

Sharon Levy
sharonlevy@umail.ucsb.edu

November 1, 2015

Abstract

Digital signatures are used world wide to verify the authenticity of messages and confirm that they have not been altered in transmission [2]. The Digital Signature Algorithm (DSA) is a Digital Signature Standard for the Federal Information Processing Standard and uses public key cryptography [1]. The Elliptic Curve Digital Signature Algorithm (ECDSA) is a version of DSA using elliptic curves.

In this paper, I will introduce ECDSA and discuss its key generation, signing, and verifying procedures. Then, I will compare this algorithm to the RSA digital signature algorithm and discuss its various advantages and drawbacks. Finally, I will discuss the security of ECDSA and attacks that can break it.

References

1. Johnson, Don and Menezes, Alfred. "The Elliptic Curve Digital Signature Algorithm (ECDSA)", 1999, http://cacr.uwaterloo.ca/techreports/1999/corr99-34.pdf
2. Arrendondo, Brandon and Jansma, Nicholas. "Performance Comparison of Elliptic Curve and RSA Digital Signatures", 2004, http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.129.7139&rep=rep1&type=pdf