Elliptic Curve Digital Signature Algorithm and its Applications in Bitcoin

Arnt Gunnar Malvik
Bendik Witzoee

November 2015

1 Abstract

Elliptic Curve Cryptography is an approach to cryptography based on the usage of elliptic curves over finite fields. This approach allows for smaller key sizes when compared to other schemes in cryptography such as the RSA, while keeping the same level of security. The Elliptic Curve Digital Signature Algorithm (ECDSA) is the most widely used standardized elliptic curve-based signature scheme [2], with applications in diverse fields. One modern application of the ECDSA is found in the Bitcoin protocol, which has seen a surge in popularity as an open source, digital currency. The total value of existing Bitcoins is estimated at over 4.5 billion USD by November, 2015 [3], creating the need for a secure means of transaction and handling.

In this paper we will present the ECDSA, covering signature generation and verification. We will then discuss the consequences the choice of elliptic curves has on the performance and security of the ECDSA. As a real world application, we will discuss the Bitcoin protocol and its elliptic curve Secp256k1 [1]. Specifically, we will be looking at the Bitcoin's choice of a Koblitz curve instead of an elliptic curve over a prime field. The implications this choice has on ECDSA will then be discussed.

References

[1] BitcoinWiki. *Secp256k1*. URL: `https://en.bitcoin.it/wiki/Secp256k1`.

[2] Scott Vanstone Darrel Hankerson Alfred Menezes. "Guide to Elliptic Curve Cryptography". In: Springer, 2004. Chap. 4.4.1.

[3] Bitcoin Watch. *Economy*. URL: `http://www.bitcoinwatch.com/`.