The Elliptic Curve Diffie-Hellman (ECDH)

Joanna Lang and Rakel Haakegaard

November 2015

1 Abstract

The Elliptic Curve Diffie-Hellman (ECDH), a variant of the Diffie Hellman, allows two parties that have no prior knowledge of each other to establish a shared secret key over an insecure channel.[3] The Diffie-Hellman works over any group as long as the DLP in the given group is a difficult problem.[2] It is one of the first public key protocols, and it is used to secure a variety of Internet services. However, newly research from October 2015 suggests that the security of Diffie-Hellman key exchange is less secure than widely believed, and maybe not strong enough to prevent very well-funded attacks.

We will first discuss the usage and the security of the ECDH specificly, and then look into the newly published article from October 2015 [1] to see if the discoveries that have been made also apply to the ECDH.

2 References

1. Adrian, Bhargavan, Durumeric et. al. *How Diffie-Hellman Fails in Practice* (2015)
   Available from: https://weakdh.org/imperfect-forward-secrecy-ccs15.pdf (01-Nov-2015)

2. Koç, Çetin Kaya *Elliptic Curve Cryptography Fundamentals.*
   Available from http://cs.ucsb.edu/ koc/ecc/docx/09ecc.pdf (21-Oct-2015)

3. *Diffie–Hellman key exchange* (2015)
   Available from: https://en.wikipedia.org/wiki/Diffie(01-Nov-2015)