ECDSA - Application and Implementation Failures

Markus Schmid
mschmid@umail.ucsb.edu

November 1, 2015

1 Abstract

Besides Integer-Factorization schemes and Discrete Logarithm schemes, Elliptic Curve Cryptography (ECC) is the newest member of public-key algorithms with practical relevance. It is based on the algebraic structure of elliptic curves over finite fields. Compared to RSA and Discrete Logarithm (DL) schemes, in many cases ECC has performance advantages with respect to fewer computations, and bandwidth advantages due to shorter signatures and keys. In addition, ECC provides the same level of security but with significantly shorter operands.[3] The Elliptic Curve Digital Signature Algorithm (ECDSA) is the elliptic analogue of the Digital Signature Algorithm (DSA). It uses the advantages of elliptic curves and was standardized in the US in 1999 by the American National Standards Institute (ANSI).[2]

After a short introduction of ECC and the comparison in terms of security of RSA and ECC, the main purpose of this paper is to present the ECDSA and its applications.[4, 1] Furthermore, implementation failures like in the case of the ECDSA based code authentication of the Playstation 3 in 2010 will be analyzed.

References

[1] Joppe W. Bos, Marcelo E. Kaihara, Thorsten Kleinjung, Arjen K. Lenstra, and Peter L. Montgomery. On the security of 1024-bit rsa and 160-bit elliptic curve cryptography. 2009.

[2] Don Johnson, Alfred Menezes, and Scott Vanstone. The elliptic curve digital signature algorithm (ecdsa). *International Journal of Information Security*, pages 36–63, 2001.

[3] Christof Paar and Jan Pelzl. *Understanding Cryptography.* A Textbook for Students and Practitioners. Springer-Verlag, Berlin Heidelberg, second edition, 2010.

[4] Serge Vaudenay. The security of dsa and ecdsa - public key cryptography - pkc 2003. *Lecture Notes in Computer Science*, pages 309–323, 2003.