Comment

Signature with message recovery

Chris J. Mitchell and Chan Yeob Yeun

Information Security Group

Royal Holloway, University of London

Egham, Surrey TW20 0EX, UK

Email : {c.mitchell,c.yeun}@rhbnc.ac.uk

Abstract

The purpose of this Comment is to point out that the discrete logarithm based signature with message recovery scheme proposed by Chen in [1] is actually not a signature scheme. It would more accurately be described as an authenticated encryption scheme.

Comments

Chen's scheme [1] is based on the discrete logarithms problem and is claimed to combine the same efficiency as Horster-Michels-Petersen and Lee-Chang [2, 3], with a simpler specification. In addition to a level of message authentication, Chen's scheme also provides message encryption, although this is only apparent from the detailed specification

of the scheme. However, the scheme is not a signature scheme in the normal sense of the term, contrary to the claim in [1].

In a signature with message recovery scheme, see for example [4], the Trusted Third Party (TTP) can always verify the signatures which are sent by the receiver B without B having to divulge any long term secret information to the TTP. However, in the authenticated encryption schemes described in [2, 3], only the sender A and the receiver B can verify a protected message sent from A to B. This is because B can only verify such a message with the aid of his private decryption key. It is for this reason that the authors of both [2] and [3] have been careful to call their schemes authenticated encryption schemes rather than combined signature/encryption schemes, although nowhere is this point made explicit in [2] or [3].

In order to verify a signature generated using the scheme proposed by Chen, the receiver B needs to use his private key. It is straightforward to verify that a third party cannot verify the 'signature' (r, s) unless B is prepared to divulge his private key. This holds even if B is prepared to supply the recovered plaintext message m and both A's and B's public keys, in addition to the received signature.

This is an unacceptable property for a true signature scheme, where one would normally expect signature verification to be possible without compromise of any private keys. Thus it would be more appropriate to refer to the scheme as an authenticated encryption scheme, analogously to the terminology used in [2, 3]. Finally note that similar remarks have been made in [5] regarding schemes recently proposed by Zheng.

References

[1] K. Chen. "Signature with message recovery". *Electronics Letters*, 34(20):1934, 1998.

[2] P. Horster, M. Michels, and H. Petersen. "Authenticated encryption schemes with low communication costs". *Electronics Letters*, 30(15):1212–1213, 1994.

[3] W. Lee and C. Chang. "Authenticated encryption scheme without using a one-way function". *Electronics Letters*, 31(19):1656–1657, 1995.

[4] K. Nyberg and R.A. Rueppel. "Message recovery for signature schemes based on the discrete logarithm problem". In *Advances in Cryptology – Proceedings of EUROCRYPT '94*, pages 175–190. Springer-Verlag, 1995.

[5] H. Petersen and M. Michels. "Crytanalysis and improvement of signcryption schemes". *IEE Proceedings on Computers and Digital Techniques*, 145:149–151, 1998.