Secret Handshakes based on Shortened Versions of DSS

Abstract

Balfanz et al. in 2003 introduced secret handshakes as mechanisms designed to prove group membership and share a secret key between two fellow group members. A secret handshake protocol allows two users to mutually verify another’s authenticity without revealing their own identity. In a secret handshake Verification if the verification succeeds the users may compute a common shared key for further communication. Thus secret handshakes can be appropriately turned into an authenticated key exchange protocol. The present paper proposes two secret handshakes scheme based on variations DSS-1 and DSS-2 of DSS signature. It is shown that proposed schemes are secure under the random oracle model along with comparison of computational complexity of proposed schemes with existing schemes.

References


**Index Terms**

Computer Science  Security

**Keywords**

Secret Handshakes, Credential, ElGamal, DSA, DSS-1, DSS-2, Computational Complexity.