Abstract

The aim of an efficient deniable authentication protocol is to enable a receiver to identify the source of a given message but not to prove the identity of the sender. Lu and Cao [7, 10] confirmed that the previous protocols had a common weakness in which any third party can impersonate the intended receiver to verify the signature of the given message, and they proposed a new protocol based on bilinear pairing using single sender and sender group. They claimed that their protocol could provide complete security and properties of a deniable authentication protocol based on bilinear pairing using single sender and sender group, we will point out that the protocol in two papers is unable to prove the source of the given message to any third party, even if he/she fully cooperates with the third party.

References

- Y. Aumann, and M. Rabin, "Efficient deniable authentication of long
messages,” International Conference on Theoretical Computer Science in Honor of Professor Manuel Blum’s 60th Birthday, Hong Kong, China, Apr. 1998.

Index Terms

Computer Science  Security

Keywords

Deniable Authentication; Information Security; Cryptography; Bilinear Pairing; Mac; Digital Signature