Abstract

This paper introduces a new authentication protocol using the tripartite signcryption scheme without bilinear pairings that provides confidentiality and authentication between three entities. Mobile communication seems very attractive to users as well as operators and service providers. However, despite of its numerous advantages, mobile communication has been facing many security problems. In this paper, it is demonstrated how the proposed tripartite signcryption scheme can be used to provide authentication and to guarantee secure communication. The use of the proposed tripartite signcryption scheme helps reduce the signaling overhead compared to the scheme in [1].

References

An Improved Authentication Protocol for Mobile Communication based on Tripartite Signcryption


Index Terms

Computer Science

Security

Keywords

Tripartite Signcryption Mobile Communication Mobile Security
An Improved Authentication Protocol for Mobile Communication based on Tripartite Signcryption