Abstract

The rapid progress in the internet requires multiple message communication over the wider area to improve the mobile network security. Due to the multiple message communication, the security is a most important concern in mobile network. The bilinear Certificate less Aggregate Signcryption Scheme guarantees the security under several attacks, and therefore provides security and non-repudiation. However, the multiple messages through a single operation are a difficult task to improve the network security. In addition, multilinear map based signcryption scheme provides the confidentiality and authenticity but it is complicated for handling when number of messages gets increased rapidly. In order to overcome the problem in multiple message communication, Exponentiated Multilinear Vectorized Certificateless Signcryption (EMV-CLSC) technique is introduced. The EMV-CLSC technique is used to verify the multiple messages through a single Signcryption process. An efficient certificate less signcryption technique performs the multiple message communication between senders and receiver to ensure the network security. In EMV-CLSC, the multilinear vectorized model is applied for handling the high volume of data and multiple data format while distributing the message...
Exponentiated Multiple Message Communication using Certificateless Signcryption for Mobile Network Security

...simultaneously. This helps to reduce the memory consumption while processing the multiple data. The proposed EMV-CLSC technique provably improves the security with public key verifiability and cipher text authenticity. Based on, the authorized users only access the network and the messages are protected. At last, the Broadcast message is secured using Digital Signature verification in uncsigncryption process. A certificate less signcryption process with multiple bits is used to highly secure the multiple messages using EMV-CLSC technique. This helps to protect the messages against the attacks and improve the mobile network security. An experimental result shows that the proposed EMV-CLSC technique improves the network security in terms of computational cost, memory consumption, communication overhead and secured message distributing rate compared to the state-of-the-art works.

References

Exponentiated Multiple Message Communication using Certificateless Signcryption for Mobile Network Security

Pages 50-56

12. Zhongyuan Qin, Xinshuai Zhang, Kerong Feng, Qunfang Zhang, and Jie Huang, “An Efficient Key Management Scheme Based on ECC and AVL Tree for Large Scale Wireless Sensor Networks”, Hindawi Publishing Corporation International Journal of Distributed Sensor Networks, Volume 2015, August 2015, Pages 1-7


Index Terms

Computer Science Security

Keywords

Mobile network security, Certificateless scheme, Signcryption, Multilinear vectorized model,
multiple message communication, signature verification.