Abstract

There is an increased activity in research and development conducted to improve current payment systems in parallel with the progress of Internet. Signcryption combines the functionalities of encryption and digital signing in a single logical step. It is a cryptographic primitive that provides confidentiality, integrity, authentication and non-repudiation. Identity-based cryptography serves as an efficient alternative to the traditional certificate-based cryptosystems. This paper introduces an efficient electronic payment system based on signcryption without bilinear pairings. This e-cash system is more efficient than other schemes employing bilinear pairings and involves less computational cost. In the proposed protocol, the token is issued and authenticated by the bank to prevent double spending problem. The customer delegates his signing capability to the merchant. The bank verifies the identities of both the original signer (customer) and the proxy signer (merchant) and ensures the originality of the transaction. Unlike the existing e-payment systems, the problem of double spending of e-cash does not arise because each transaction is made uniquely identifiable. Hence, no separate protocol is needed to check double-spending. The performance and the security analysis of the proposed e-cash system are discussed revealing its strength from the
viewpoint of security and efficiency with regard to computations required.

References


Index Terms

Computer Science Security

Keywords

E-cash payment system Signcryption Bilinear Pairings E-Commerce Security