Abstract

The present e-payment schemes permit anonymity property to protect customer privacy. However, the majority of these schemes have not offered a non-denial property. For example, several difficulties subsist in the schemes such as repudiation, loss, abuse, theft, and overspend-tracing. This article suggests an e-payment scheme wherein a temporary anonymous public key is embedded in a partial blind signature protocol to give a non-denial protection challenging the above mentioned attacks. This paper also shows that the combination of both a partial blind digital signature scheme and anonymous digital signature scheme will build a new e-payment scheme that will be stronger and safer than before.

References

An Efficient E-Payment Scheme


Index Terms

Computer Science  Security

Keywords

E-payment Scheme  E-coin Issue  Partial Blind Signature  Transport Layer Security