Abstract

Pervasive computing environments allow users to get services anytime and anywhere. Security has become a great challenge in pervasive computing environments because of its heterogeneity, openness, mobility and dynamicity. In this paper, we propose two heterogeneous deniable authentication protocols for pervasive computing environments using bilinear pairings. The first protocol allows a sender in a public key infrastructure (PKI) environment to send a message to a receiver in an identity-based cryptography (IBC) environment. The second protocol allows a sender in the IBC environment to send a message to a receiver in the PKI environment. Our protocols admits formal security proof in the random oracle model under the bilinear Diffie–Hellman assumption. In addition, our protocols support batch verification that can speed up the verification of authenticators. The characteristic makes our protocols useful in pervasive computing environments.