Abstract

This paper presents the simulation of privacy-related applications employing blind signature (BS) schemes. Two popular privacy-related applications: traditional BS based electronic voting system (EVS) and traditional offline electronic payment protocol (EPP) have been chosen here. A BS scheme is a cryptographic protocol that plays a vital role to conduct the electronic transactions of privacy-related applications securely but anonymously. It ensures the confidentiality of the private information of a user while she involves in an electronic transaction over the internet. Intuitively, existing BS schemes can be categorized as traceable and untraceable. RSA cryptosystem based two popular schemes from two categories: the scheme of Chaum [1] from traceable schemes and the scheme of Hwang et al. [2] from untraceable schemes have been chosen here for simulation. The upshot of the simulation model is the comparison of computation time requirement of blinding, singing, unblinding and verification operations involved in different steps of privacy-related applications evaluated by the chosen BS schemes.
An Exploitation of Blind Signature Schemes to Simulate Privacy-related Applications

- D. Chaum, &quot;Blind signatures system,&quot; Advances in Cryptology, CRYPTO'83, pp. 153-156, 1983.

Index Terms

Computer Science

Security

Keywords

Blind Signature Scheme Untraceability Electronic Voting System Electronic Payment Protocol