電子商取引の高セキュリティ化に関する研究

田村 裕子
北陸先端科学技術大学院大学

平成 16 年 3 月 30 日

Abstract

In the spread of electronic commerce such as an electoronic auction, an electronic mall through Internet, the most important benefit of electoronic commerce is that anyone can join anywhere at anytime. However, a user might been implicated in the crime, or information about a user gives might be disclosed or disseminated by the transaction with a malicious users or organization. Therefore, we propose schemes to prevent such problems as follows:

Signature with a Guarantee The most important benefit of electronic commerce is that anyone can join from anywhere at anytime. As a result, subjects with whom we make a contract have been more scattered geographically over a wide and rapidly spreaded. However, we have no way to verify the transaction with persons or organizations which are unfamiliar to us. Therefore, we need *a signature scheme with a guarantee* by other trustworty persons or organizations to transact with unfamiliar persons or organizations smoothly, through Internet. In this paper, we propose a new concept of a signature scheme with a guarantee, and propose a formal model and a basic scheme for it.

Anonymous Credential System As information gets increasingly accessible, it has been important that individuals control their information to protect their privacy, even if organizations which a user transacts team up. Anonymous credential systems allow users to work effectively and anonymously with multiple organizations by using different *pseudonyms*. Such systems are called anonymous when transactions carried out by the same user cannot be correlated. In the systems, an organization knows users by only pseudonym in which each pseudonym cannot be linked to others. An organization issues a *credential* on a pseudonym, and the corresponding user demonstrates the possession of this credential to another organization without revealing anything but the possession.

In the previous schemes, however, proving the possession of a credential gives a verifier the information about which organization a user transacts with, unfortunately. As a result, this compromises the privacy of users. The best an anonymous credential system should be able to choose the level of privacy according to its security policies. In this paper, we propose an anonymity-enhanced pseudonym system by showing a credential issued by a group. Furthermore, showing of multiple credentials needs much computational and communication cost. In this paper, we propose an efficient credential system which allows users to show multiple credentials

Proxy-bidding The most common auction style is the open-bid English auction. Bidders are required to be watching the current prices, and it usually takes a long time to close the auction. The proxy-bidding system is a method whereby a bidder asks proxy to go to the auction and bid on himself. Such a system makes bidding on auctions more convenient and less time consuming for bidders, is becoming popular in Internet. In this paper, we propose an efficient and safety proxy-bidding.