NEC Develops World's Most Efficient Privacy Preserving Authentication Scheme

July 22 2005

NEC Corporation announced that it has developed the world's most efficient privacy preserving authentication scheme (or group signature scheme) in terms of signature length and computational complexity, social infrastructure vital to both the privacy protection of individuals and security within a networked society.

Group signature schemes have been long sought after as they are believed to fulfill security and privacy needs simultaneously, i.e. they enable authorization of a user, without identifying the user, thus allowing the user a certain amount of anonymity. It is believed that these schemes may be applied to many systems in the future in which user anonymity is required such as in anonymous credential systems, and video/book rental systems, among others.

The main characteristics of a privacy preserving authentication scheme are:

(1) Enables verification of individuals belonging to a limited group who have authorized access, without actually identifying the user by an ID or personal name etc, reducing the risk of information leaks and protecting the hoarding of surplus personal information.
(2) Identification of the authenticated individual is only allowed by special authorities (specified administrators). As a result, disorderly and unjust use of anonymity is prevented as these authorities can revoke anonymity.

NEC's authentication scheme realizes the world's shortest authentication data length through the development of a new, original algorithm. Moreover, it has been verified as highly secure while simultaneously carrying out efficient creation and verification of authentication data by the world's most efficient computational complexity realized by the adoption of cryptographic protocol technology. Early group signature schemes/authentication schemes required large computational cost and long signature lengths; however, NEC's technological breakthrough enables shorter signature lengths at minimum cost.

Anonymous authentication schemes may enable, for example, a credit card transaction system with reduced risk of personal information leaks. This is mainly because a usual credit card transaction can be carried out at a retail premises by verifying that a user has an official contract with a certain credit card company, without providing the information terminal in the retail premises with the card no. or personal information of the user, however, the credit card company itself (administrator) can identify the holder of the credit card making the payment.

Essentially, information is hidden from certain parties, who should not have access to the information. This kind of technology can also be applied to loan systems such as those in video shops or libraries to protect the privacy of the borrower.

NEC's newly developed group signature scheme enables the world's most efficient signature length and computational complexity, proving security, and bringing the technology one more step closer to business model application. NEC believes that this technology will act as basic technology for next-generation solutions. This new breakthrough has proven the basic functions of the algorithm, and the next step for NEC is to verify practicality.

This development will provide NEC with the opportunity to apply its research-level group signature technology to a real business model application here forth.

Citation: NEC Develops World's Most Efficient Privacy Preserving Authentication Scheme (2005, July 22) retrieved 19 April 2024 from https://phys.org/news/2005-07-nec-world-efficient-privacy-authentication.html

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.