発表概要

プロセス代数を用いたセキュリティ・プロトコル記述

櫻田英樹†

プロトコルとそのセキュリティを表現する方法について述べる．セキュリティ・プロトコルの安全性を検証する研究がさかんであるが，認証や鍵共有などの単純にプロトコルに比べて，電子商取引で用いられるような大きなセキュリティ・プロトコルの安全性はあまり研究されていない．その理由の1つとして，大きく複雑なプロトコルとそのセキュリティを柔軟に記述する方法がないためであると考えられる．本研究では，これらを記述する方法を提案する．

Describing Security Protocols in a Process Algebra

Hideki Sakurada†

We discuss on a method to express security protocols and their security properties. Although there are a lot of works on analysis of security protocols, there are few works on more large protocols such used in e-commerce than simple protocols such as key-distribution protocols. One of the reason is that there is few tools with which we can flexibly describe large protocols and their security. We propose a method to describe them with a process algebra.

（平成13年7月26日発表）

† NTTコミュニケーション科学基礎研究所
NTT Communication Science Laboratories