発表概要

束縛のタイミングを考慮した認証プロトコルについて

齋藤孝道[†] 萩谷昌己[††] 溝口文雄[†]

本発表では，公開鍵を用いた認証プロトコルの安全性について考える．特定の相手との内容を第三者に秘匿する通信をする際，確定した相手との秘密の通信のための鍵，つまり，セッション鍵の交換が行われる．それを実現するための公開鍵を用いた認証プロトコルがいくつか提案されているが，その中には悪意ある第三者にセッション鍵が漏洩するなどの問題を持つものもある．そこで，本発表ではセッション鍵の交換を含めた認証プロトコルはどのような要件を満たすべきかを考察し，安全な認証プロトコルに関する枠組みを定める．この中で特に，束縛のタイミングを考慮して，late binding という概念を導入する．また，本発表では，この late binding を用いたプロトコルの安全性を示し，この概念を考慮した認証プロトコルの例をいくつか示す．

Authentication Protocol Based on Timing of Binding

Takamichi Saito,[†] Masami Hagiya[††] and Fumio Mizoguchi[†]

In this presentation, we discuss authentication protocols using public-key cryptography. When initiator and responder communicate securely, they authenticate each other and exchange a session key. There are lots of authentication protocols for this purpose. However, some protocols may have critical flaw. Therefore, we provide requirements and framework for secure authentication protocol, and design some protocols derived from the framework. Moreover, we introduce the concept of late binding, which is based on timing of binding in a protocol. Finally, we propose some protocols based on the binding, and check the safty of the protocols by the requirements.

（平成 13 年 10 月 23 日発表）

† 東京理科大学
Science University of Tokyo
†† 東京大学
University of Tokyo