定理証明器による電子現金プロトコルのモデル化と検証

安田　武史、高橋　和子

本発表では、定理証明器 Isabelle/HOL を用いて、電子現金プロトコルを帰納的にモデル化しその仕様を検証する方法を示す。

電子現金方式に要求される仕様は一般に、「完全情報化」、「安全性」、「プライバシー」、「オフライン性」、「譲渡可能性」、「分割利用可能性」の 6 つであり、このすべての仕様を満たす電子現金方式が提案されている。我々は、この方式の 1 つを帰納的手法を用いてモデル化し、「安全性」、「分割利用可能性」の仕様が満たされていることを検証した。

対象とする方式では、電子現金は Binary Tree Approach により実現されており、分割利用するための操作がこの二分木上で定義されている。また、ビットコミットメントを使うことで二重使用を防止している。これらの仕組みを取り込んだデータ構造や関数を帰納的に定義した。プロトコルのモデル化は、Paulson の帰納的アプローチに基づき、送受信イベントをレースとしてリストに格納する形ですべて帰納的に記述した。

検証においては、モデル化に対応した仕様の解釈を行った。「安全性」は「誰かが二重使用を行った場合、必ず発覚する」と解釈し、「分割利用可能性」は「ある金額から任意の金額を使用した場合、残りの金額も正当な電子現金である」と解釈し、それぞれ検証した。

この結果、定理証明器を電子現金プロトコルの検証に使える可能性を示すことができた。

Verification of Electronic Cash Protocol Using a Theorem Prover

Takeshi YASUDA and Kazuko TAKAHASHI

We show inductive modeling of an electronic cash protocol and verification that its requirements are satisfied using a theoreom prover Isabelle/HOL. It is said that an electronic cash should satisfy the following six requirements. Independence, security, privacy, off-line, transferability, and divisibility. An electronic cash scheme that satisfies all of them has been proposed.

We formalize the protocol on this scheme. The scheme is implemented using a binary tree on which the operation for divisable use is defined. Moreover, double-spending is detected by the bit-commitment. We define the data structure and recursive functions that reflect these mechanism. In modeling a protocol, we use Paulson's inductive approach, in which each event of sending/receiving is stored as a trace.

We verified the security and divisability of the six requirements. As for security, we verify the assertion that if double-spending of an electronic cash occurs, then it can be detected. As for divisability, we verify the assertion that if we use some portion of a well-defined electronic cash, then the reminder is also a well-defined one.

As a result, we showed the possibility that thereom provers can be applied to verification on electronic cash protocols.