発表概要

帰納的アプローチに基づく理想的電子現金方式のモデル化および証明支援系 Isabelle/HOL による安全性の証明

吉丸　始須雄[†1]　　高　橋　和　子[†1]

本研究では，帰納的アプローチに基づいて理想的電子現金方式をモデル化し，その安全性について，証明支援系 Isabelle/HOL を用いて証明を与える．理想的電子現金方式とは，「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 条件を満足する電子現金プロトコルである．この安全性は，「電子現金のコピー，偽造等による不正利用ができないこと」と定義されている．本研究の対象とするプロトコルは，電子現金のデータ構造として二分木を採用しており，支払いは金額に相当するノードを使うと定義される．また，同じ枝にあるノードを使用すると，額面以上の金額を使うという不正利用が生じるように設計されている．通常はユーザの購買に関するプライバシーを銀行を含む他者が把握することはできないが，不正利用が発覚した際に，使用されたノードの情報から不正利用者を割り出すことができる仕掛けになっており，これによって安全性を保証している．プロトコルのモデル化には，Paulson らの提案した帰納的アプローチを用いる．しかし，彼らの構築したモデルは金額を扱ったものではない．一方，このプロトコルにおける安全性を扱うには，二分木上のノードの位置情報と電子現金の金額の考慮が不可欠である．そのため，本研究ではこれらを量的なデータとしてモデルに与え，証明を試みる．

Modeling an Ideal Electronic Cash Scheme Based on an Inductive Approach and Proving Its Security by a Proof Assistant Isabelle/HOL

Shizuo Yoshimaru[†1] and Kazuko Takahashi[†1]

Modeling an Ideal Electronic Cash Scheme Based on an Inductive Approach and Proving Its Security by a Proof Assistant Isabelle/HOL. We make a model of an electronic cash (e-cash) scheme based on an inductive approach and prove its security using a proof assistant Isabelle/HOL. An ideal e-cash scheme is a protocol that satisfies the following properties: independence, security, untraceability, off-line operation, transferability and divisibility. Among these properties, we focus on security: "no overspending is allowed." Our target protocol adopts a binary tree as a data structure of an e-cash, and a payment is defined as spending a node corresponding to the amount. It is designed so that overspending appears if a user spends a pair of nodes in the same branch. Usually the other agents including a bank cannot know a private information on payment. However, once overspending appears, the malicious user can be identified from the information of the spent nodes, which guarantees security. We adopt an induction approach proposed by Paulson, et. al to model this protocol. However, amount of payment cannot be handled in their model. On the other hand, in order to handle security in our target protocol, we have to consider both the positional information of a node in a binary tree and an amount of the payment as a natural number. In this presentation, we give them as concrete data to the model, and try to prove that the security holds.

（平成 22 年 3 月 15 日発表）

†1 関西学院大学大学院理工学研究科
School of Science & Technology, Kwansei Gakuin University