電子現金の分割利用可能性の形式化と帰納的証明

吉丸　始須雄、高橋　和子

本研究では、二分木構造を持つ電子現金について帰納的なモデルを与え、定理証明器 Isabelle/HOL を用いて仕様の検証を行った。

電子現金方式のうち、「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 条件を満足するものを「理想的電子現金方式」と呼ぶ。ここでは、理想的電子現金方式として提案されている一方式を形式化し、分割利用可能性についての検証を試みた。

分割利用可能性とは、一度発行された電子現金を、利用合計金額が額面の金額になるまで何度でも使うことができる、という性質である。本研究で扱う方式では、電子現金を二分木によって構成し、二分木上の操作を定義することにより、これを実現している。モデル化の際も同様に、二分木に基づくデータ構造や関数を帰納的に定義した。また、分割利用可能性については「ある電子現金から任意の金額を任意の回数支払った結果、残りの電子現金の金額はその差額に等しい」と解釈し、これを証明した。

なお、自然数と二分木という異なる帰納スキームを持つデータ間の対応関係を帰納法を使って証明するために、中間的なデータ構造として二進数を利用した。そのため、本論文では Isabelle/HOL での二進数の扱い方についても言及する。

Formalization of Divisibility of an Electronic Cash Scheme and Its Inductive Proof

SHIZUO YOSHIMARU and KAZUKO TAKAHASHI

We formalize an electronic cash scheme that uses a binary tree structure as an inductive model, and prove its divisibility using Isabelle/HOL.

An electronic cash sheme that satisfies the following six properties is called an ideal e-cash protocols: independence, security, untraceability, offline operation, transferability, and divisibility. Divisibility means that a user can spend an electronic cash in several separate transactions by dividing its value without over-spending. In the target sheme, a coin of some monetary value is encoded as a kind of binary tree, and a payment function is defined as an operation on it. In the formalization, we give an inductive definition to the data structure and functions based on the binary

tree.

The correctness of the divisibility is interpreted as follows: when an arbitrary amount is paid from an electronic cash several times, the amount remaining after payments is the difference between the original value and the payment value.

In the proof, we use a bit sequence as an intermediate data structure to successfully apply induction on the lemma on a natural number and a tree which have the different induction schemes. We also discuss the treatment of a bit sequence in Isabelle/HOL that is used in our approach.