現金に替わる電子マネーの実装

木下研究室　　大城　翔太 (200702894)

1　はじめに

近年，日本では JR 東日本が発行する Suica，ビットワレットが発行する Edy など，発行会社ごとに多種多様な電子マネーが普及している．

それに伴い，利用するシーンも生活の中で増えているが，電子マネー間の相互利用はほとんど出来ない為，電車の運賃は鉄道会社の発行する交通系電子マネー，買い物はクレジットカード会社の発行する電子マネーで決済するなど，利用するシーンごとに電子マネーを使い分けているのが現状であり，現金の替わりになるまでは至っていない．

本研究では，安全性とプライバシーを確保した現金と代替可能な電子マネーを実装する為のシステムを提案する．

2　提案手法

2.1　基本構造

電子マネーの基本構造として、離散対数論を使用した電子マネーを用いる．離散対数問題を使用する事により，計算結果から元の数値を導き出す事が困難となる．

2.2　電子マネーの構造

S_x を金額,R_x を 448bit の乱数とすると

$$M_x = f(S_x, R_x) = 2^{448} S_x + R_x \tag{1}$$

データベースに蓄積する電子マネー x の認証子 D_x は, 原始根を g とすると,

$$D_x = g^{M_x} modn \tag{2}$$

となり, 離散対数問題を使用している事により, D_x から M_x を求める事が困難である．

2.3　決済処理の方法

データベースの情報は，ユーザーの電子マネーを A，受領者の電子マネーを B とすると次のようになる．

・取引前

$$D_{A1} = g^{M_{[A1]}} modn \tag{3}$$

$$D_{B1} = g^{M_{[B1]}} modn \tag{4}$$

・取引後

$$D_{A2} = g^{M_{[A2]}} modn \tag{5}$$

$$D_{B2} = g^{M_{[B2]}} modn \tag{6}$$

3　システムについて

3.1　本研究で取り扱う範囲

本研究ではユーザーと受領者の間の金銭のやりとりに重点をおいて研究を行う．
ユーザーが買い物をした時, 受領者とユーザーの取引前と取引後の金額を比べ, 取引が正しく行われたかを確かめるプログラムを作成する．

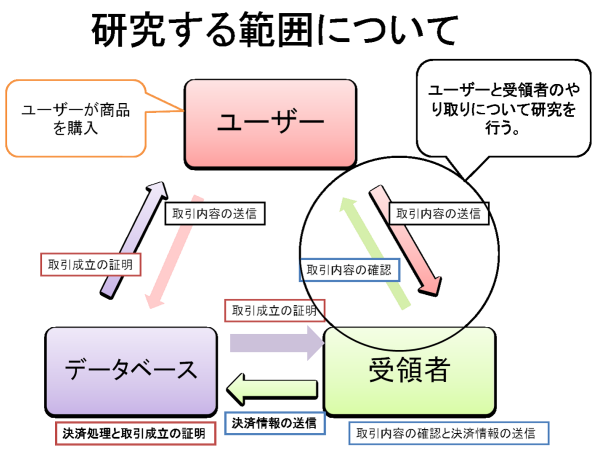

図 1: 取引の流れ

3.2　システムの提案方法

システムの提案には Java による実装方法を提案する．離散対数問題の計算においては, 非常に大きな桁の数を扱わなければならない為，大整数を扱うプログラムを用いて計算する．

4　まとめ

ユーザーと受領者による取引内容を暗号化して安全性を高め, 取引前と取引後を比較する事で金銭のやりとりが正しく行われたか確認するプログラムを Java により実現する事ができた．