現金と代替可能な電子マネーの研究

木下研究室　　工藤　護 (200602823)

1　はじめに

インターネットなどを利用した電子的な決済が増える中、現在普及している電子マネーはプリペイド型電子マネーであり、一度の決済にしか利用できないために現金との代替が不可能である。また、印刷技術の進歩などにより、現金の偽造の問題などが深刻となっているので、より強固な不正対策が必要である。本稿では既存の電子マネーのように現金の補助的な決済手段としてではなく、転々流通性を持ち、マネーサプライのコントロールが可能な現金と代替ができる電子マネーについて考察する。

2　提案方式について

2.1　基本構造

基本構造として以前より研究室で研究されている離散対数論を使用した、中央銀行発行の電子マネーを用いる。また、データベースを分散データベース化し、階層構造を為すことでトラフィックと処理の集中を避ける。

2.2　離散対数問題を使用した電子マネー

電子マネーの構造は S_x を 64bit の金額、R_x を 448bit の乱数とすると、

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

となり、データベースに蓄積される電子マネー x の認証子 D_x は原子元を g とすると、

$$D_x = g^{M_x} modn$$

となる。また、本システムにおける通信はすべて匿名通信路を用いる。離散対数問題を使用する利点は、データベースが電子マネーの合計金額を管理しているので二重支払いなどの問題が起こらず、D_x から M_x を求めることが難しく、データベースに対してユーザーの匿名性を保つことができる。

2.3　支払処理

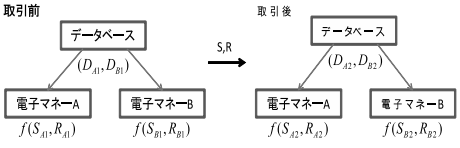

図 1: 支払処理

取引前のデータベースの情報は、

$$D_{A1} = g^{M_{A1}} modn, D_{B1} = g^{M_{B1}} modn$$

であり、取引後は、

$$D_{A2} = g^{M_{A2}} modn, D_{B2} = g^{M_{B2}} modn$$

となる。

取引前後のデータベース上で下記の式より A,B の電子マネーの合計が一致していることを検査する。

$$g^{M_A 1} g^{M_B 1} = g^{M_A 2} g^{M_B 2} modn$$

現段階では支払時に支払い側の手持ち金額が－になってしまう状況への対応を、受領者側にユーザーの設定した乱数を公開して確認してもらう、金額ビットを制限し乱数に対する bit の対応を全パターン、データベースに登録するなど比較検討する。

3　分散データベースについて

3.1　データベースの分散

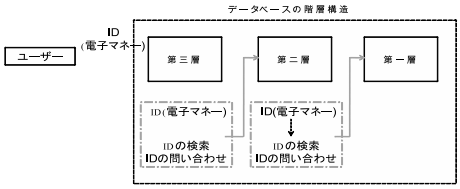

図 2: 分散データベースの階層構造

中央銀行のデータベースはトラフィックと処理の集中を避けるために図のように分散化し、階層構造をなす。支払の受領者が最寄りのデータベースにアクセスし、データベースは支払者と受領者の電子マネーを識別子を手掛かりに検索していき、両者の電子マネーが存在するデータベース間でトランザクションが行われる。

3.2　識別子の割り当て

識別子はどのデータベースに存在するか容易に見つけることが出来るように割り当てる必要がある。

例－XX＄AA.BB.CC.centralbank.YY.ZZ

AA～ZZ の部分はデータベースを保持するサーバの完全修飾ドメイン名（FQDN）を示し、XX は電子マネーのシリアル番号、AA,BB,CC はデータベースの階層構造を示す。また、＄はシリアル番号と FQDN の区切り文字を示している。このように識別子を割り当てることで検索を行う際の手掛かりとなり、データベース内での検索がより効率的になると考えられる。

4　まとめ

離散対数論を使用することで匿名性の確保は出来るが、資金洗浄などの不正への対処も視野に入れ安全性との両立を目指していきたいと思う。