平成21年度 卒業論文

論文題目

現金と代替可能な電子マネーの研究

神奈川大学 工学部 電子情報フロンティア学科

学籍番号　200602823

工藤　護

指導担当者　木下宏揚　教授

目 次

第 1 章　序論　5

第 2 章　基礎知識　7

2.1 貨幣の説明 7
2.1.1 貨幣の種類 7
2.1.2 通貨発行制度 8
2.2 電子決済手段 9
2.3 暗号技術 12
2.3.1 共通鍵暗号方式 12
2.3.2 公開鍵暗号方式 12
2.3.3 ディジタル署名 13
2.3.4 ブラインド署名 15
2.4 離散対数問題 16
2.4.1 合同式 16
2.4.2 素数 17
2.4.3 離散対数問題 17
2.5 匿名通信路 18
2.6 離散対数問題を使用した電子マネー方式 18
2.6.1 支払い処理 18
2.6.2 登録プロトコル 19
2.6.3 支払いプロトコル 20
2.6.4 電子マネー発行 21
2.6.5 電子マネー廃棄 21

第 3 章　　提案　　22
3.1 分散データベースについて 22
3.1.1 データベースの分散 22
3.1.2 識別子の割り当て 23
3.2 プロトコル 24
3.2.1 前提条件 24
3.2.2 暗号化関数の定義 24
3.2.3 登録プロトコル 25
3.2.4 支払プロトコル 1 26
3.2.5 支払プロトコル 2 27
3.2.6 支払方法の比較 28

第 4 章　　結論　　29

謝辞　　30

参 考 文 献　　31

質疑応答　　33

図 目 次

2.1 アクセス型商品の仕組み 11
2.2 ストアドバリュー型商品の仕組み 11
2.3 共通鍵暗号方式 12
2.4 公開鍵暗号方式 13
2.5 ディジタル署名方式 14
2.6 支払処理 19
2.7 登録プロトコル 19
2.8 支払いプロトコル 20

3.1 分散データベースの階層構造 22
3.2 登録プロトコル 25
3.3 支払いの流れ 26
3.4 支払いの流れ 27

第1章

序論

近年，インターネットショッピングなどを始めとして電子的な決済が身近なものとなってきているが [1]，普及している電子マネーはそのほとんどがプリペイド型の電子マネーであり，価値を IC カードに記録しているため，偽造の問題や一度の決済でしか利用できないため現金との代替が不可能となっている．特に現在までに考案されている電子マネーは，既存の現金の機能，つまり，偽造対策，プライバシー保護，譲渡可能性という機能を模倣することを目標として構成されているため，本質的に既存の現金を超えるものとなっておらず，現金の補助的な決済手段となっている．また，印刷技術などの進歩より現金の偽造問題が深刻となっているため，現金は全国どこでも使える流通性があり，誰がどこで使用したかわからない匿名性，取引と同時に決済が完了する完了性，受け取った現金を別の用途にも使用できる汎用性などの特徴を持っているが，その反面，一万円札を持っていても価値を分割できない，集金との代替を目指す上で電子マネーもより強固な不正対策をすることが重要である．

集金・送金などの際に，コストがの高さや保管，紛失，盗難などにより取扱いが不便である．他にも貴重な紙資源を消費するなどの問題もある．

研究室では以前より電子マネーについての研究が行われており，通貨の発行量を調整するために中央銀行を電子マネーの発行機関にする方法や，支払時に支払者の電子マネーの金額が－の値になってしまう問題を，第三者機関を設置することで解決する方法，現金の特徴を継承しつつ電子マネーの利点

を持たせる方法などが考案されている.

本研究は，文献 [2][3] などを参考に，支払時に支払者の金額が－の値になってしまう問題を信頼のおける第三者機関を設置するという方式の第三者が取引に介入するという問題点を解決するため，当事者間のみで決済が完了するようにし，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で，マネーロンダリングや偽造などの問題とプライバシーの保護の両立を目指した電子マネーについて提案する.

また，中央銀行のデータベースを分散データベースにすることで，より効率的に情報を管理することをできるようにしている．特徴としては，データベースは取引金額，ユーザ個人の電子マネーが分からない，ユーザ個人の不注意による紛失，盗難がない．全額をデータベースが認証しているため金額の二重払いなどがない.

第2章

基礎知識

2.1 貨幣の説明

貨幣は古来より物々交換から始まった取引である [14][16]．最初は物々交換であったが持ち運びに不便であることや短い時間しか商品価値を保つことができないなどの利用から金を使った貨幣が生まれた．

貨幣は簡単に手に入ったり簡単に作れるものであったりしては都合が悪い．偽造されたりしてはならないため最近の通貨は高度な技術を使って貨幣に彫刻したり一つも大きさや重さ厚みに狂いがないようになっている．これらを考えると電子マネー [5][6] は通貨としての理想像にあっていると考えられる．

2.1.1 貨幣の種類

- **兌換紙幣**

  発行者の信用で同額の金貨や銀貨と交歓を約束した紙幣．中央銀行は発行した紙幣と同額の金や銀を常時保管する．

- **不換紙幣**

  日本銀行法が制定されることで発行できるようになった兌換義務のない紙幣．国の信用で流通するので信用貨幣ともいう．経済が急速に発展

すると金の生産量が追いつかなくなり金本位制を保持するのが難しくなるので管理通貨制度へ移行した.

2.1.2 通貨発行制度

- **金本位制**

  金そのものを貨幣として実際に流通させる方式である．実際には流通に足りる金貨が常備できない高額になりがちな金貨は持ち運びが不便などの理由により金貨を流通させることができない．そのため中央銀行が金地金との交換を保証された兌換紙幣とその補助貨幣を流通させることで貨幣価値を裏付ける方式.

- **管理通貨制度**

  通貨の総量・総額を政策目標（物価の安定経済の成長雇用の安定国際収支の安定など）に合わせて調整しようとする経済政策のこと．景気や物価調整のために柔軟な通貨調整ができるメリットがある.

2.2 電子決済手段

電子決済手段[15][17]は大きく分けると下の2つに分類される．

- **アクセス型商品**
  アクセス型商品はインターネットなど各種ネットワークや汎用のパソコンなどを用いて預金振替などの集中処理型の決済手段に対して遠隔地から支払い指示を行うことで電子的に決済を行う手段である．金銭的価値は利用者の手元ではなく常に銀行の預金口座など決済手段の提供主体に存在する．ストアドバリュー型と比較するとシステム障害や価値紛失時の復元，不正処理の発見・追跡の面で信頼性が高い．

- **ストアドバリュー型商品**
  ストアドバリュー型商品は現・預金と引き換えに発行された電子的な情報である金銭的価値を資金の保有者自身が管理するICカードやパソコン上のソフトウェアなどに蓄えておき財・サービスの購入時にこれを取引相手に引き渡すまたはこれを書き換えることによって電子的に決済を行う手段である．一般にストアドバリュー型商品が銀行預金の振り替えによる決済より低コストで利便性が高いと言われているのは預金口座残高を減額していったん電子的価値に交換した後は決済手段の提供主体が利用者別に残高や取引記録を管理しないことが主な利用である．これはその多くが少額の決済を主な対象としていることから処理の確実性を若干犠牲にすることで利便性を高めているためである．電子的価値の処理方法は転々流通性を持ち現・預金化しなくても他の主体との取引にそのまま使用できるものと必ず現・預金化しなければいけないものがある．

またアクセス型商品とストアドバリュー型商品は以下のように細かく分けることもできる.

- アクセス型商品
  - オンラインバンキング型電子的価値が存在する預金口座に対してネットワーク経由で振替指示を行うことにより決済を行う.
  - クレジットカード型クレジットカード情報を暗号により安全に小売店に送信しその後は物理的にカードを提示する場合と同様に預金口座間の資金移動で決済を行う.
  - 電子小切手型小切手情報をネットワーク経由で電子的に送信しその後は通常の小切手と同様預金口座間の資金移動により決済を行う.
- ストアドバリュー型
  - IC カード型電子的価値を IC カード上に保存し IC カードを物理的に提示して本価値を相手に引き渡すことにより決済を行う.
  - ネットワーク型（ソフトウェア型）電子的価値をパソコンのソフトウェア上に保存しこれをネットワーク経由で送信することにより決済を行う.

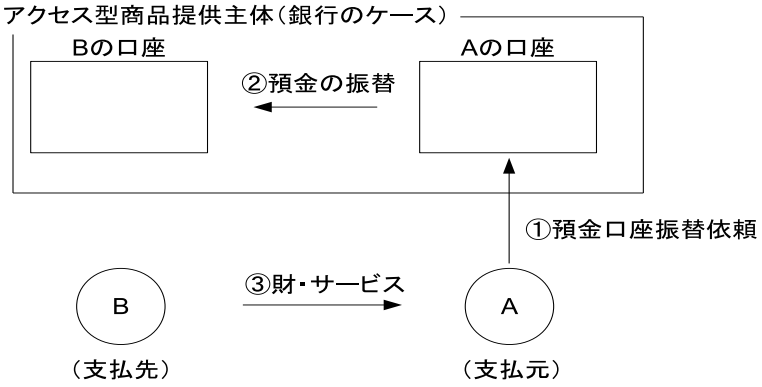

図 2.1 アクセス型商品の仕組み

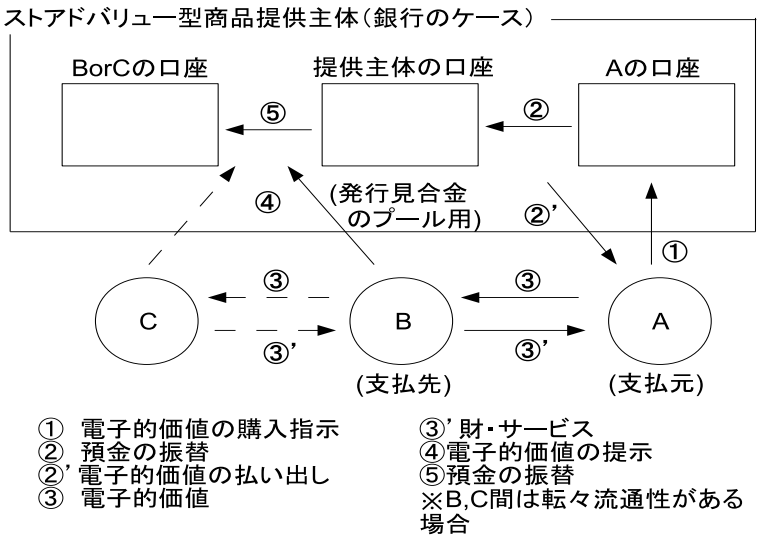

図 2.2 ストアドバリュー型商品の仕組み

2.3　暗号技術

2.3.1　共通鍵暗号方式

図 2.3 は共通鍵暗号方式を示す．メッセージの暗号化と複合化で同じ鍵を使う方式．メッセージに送り手と受け手は秘密に鍵を共有することになる．扱いが簡単であり処理速度が速い半面，相手毎に固有の鍵を作成しなければならない．あらかじめ安全な方法で相手に鍵を渡さなければならないことから限られた特定の相手とのやり取りに向いている．共通鍵暗号方式の代表的なものに DES 方式がある．

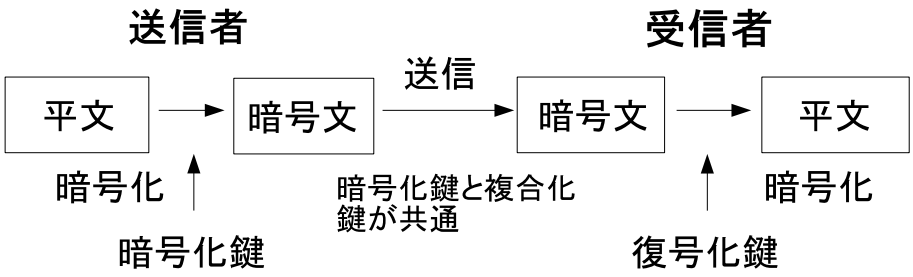

図 2.3　共通鍵暗号方式

2.3.2　公開鍵暗号方式

図 2.4 は公開鍵暗号方式 [7][9] を示す．メッセージを暗号化する鍵（公開鍵）と複合する鍵（複合鍵）の 2 つの鍵を使用する．2 つの鍵には数学的な関係があり 2 つの鍵のうちの一方の鍵で暗号化したデータを複合化できるのはもう一方の鍵を使用した場合に限られる．また公開鍵から秘密鍵を解くことが困難であることが数学的の証明されている．公開鍵暗号方式において秘密鍵は第三者に開示しなければ保証される．公開鍵暗号の代表的なものには RSA 暗号がある．

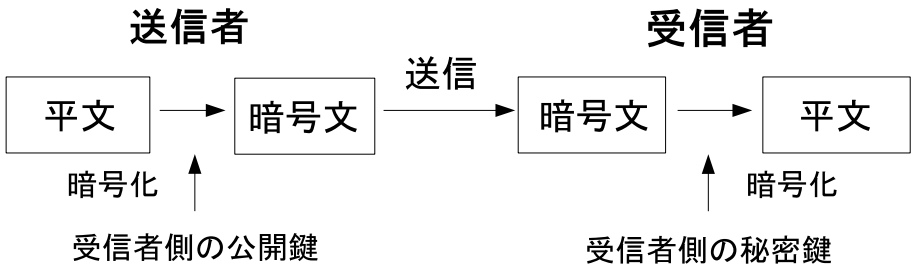

図 2.4 公開鍵暗号方式

2.3.3 ディジタル署名

図 2.5 にディジタル署名方式 [4] を示す．ディジタル署名は公開鍵暗号方式を応用している．発信者は平文を一方向ハッシュ関数で圧縮したものを秘密鍵で暗号化させて署名を作成し平文に添付して送付する．受信者は署名を公開鍵で複合し一方で送られた平文を同じハッシュ関数で圧縮して両者を比較し一致すれば確かに（秘密鍵を持っている）発信者本人が発行したものである．さらにデータの改竄もなかったということを同時に検証したメッセージダイジェストだけを暗号化・複合化するので高速の処理できる．なおディジタル署名はネットワーク上を平文が流れるためデータ内容に機密性を保証するものではない．また改竄を防止したり修復したりする機能も持っていない．

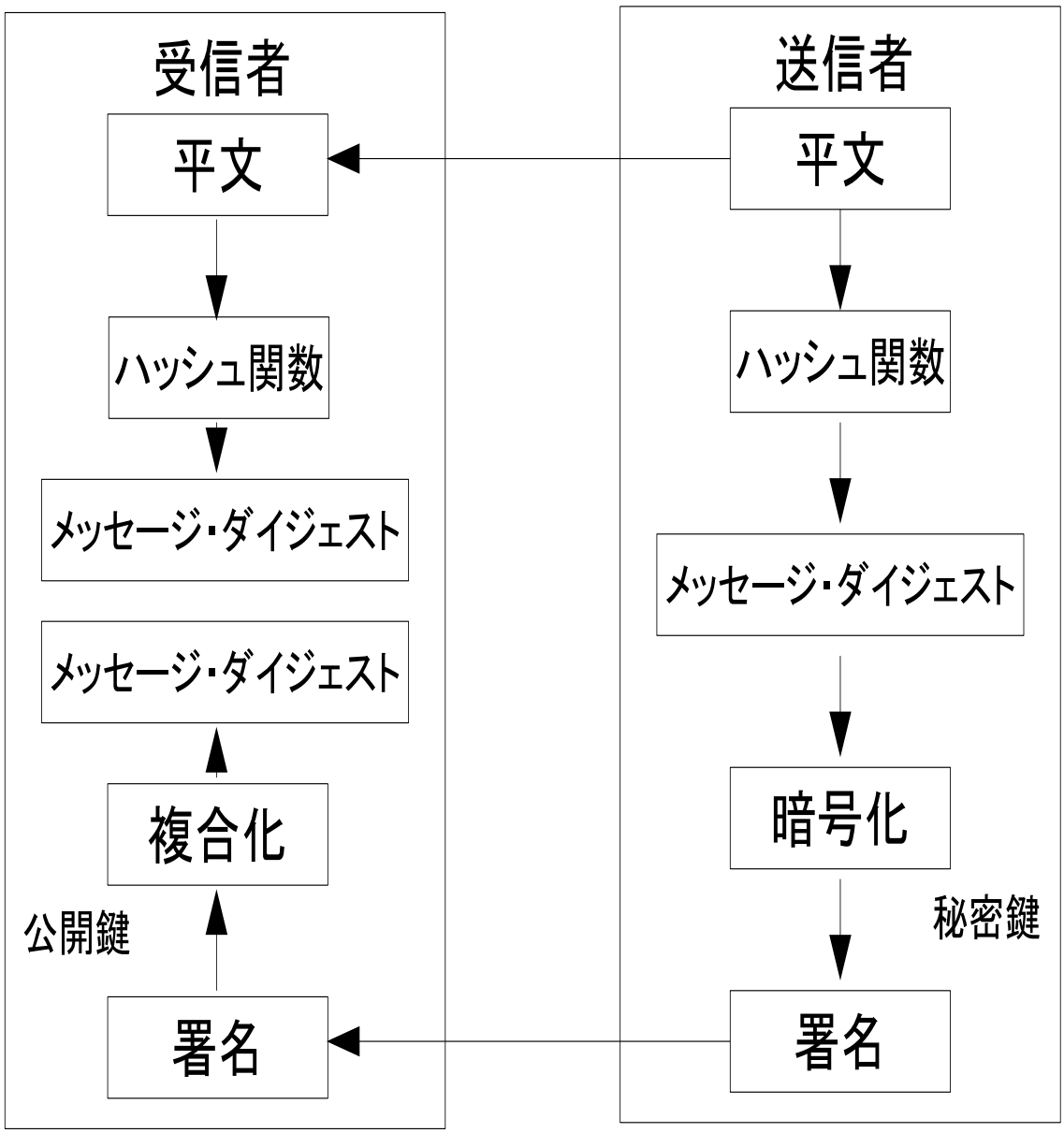

図 2.5　ディジタル署名方式

2.3.4 ブラインド署名

銀行が電子マネーにディジタル署名するとき電子マネーに含まれる貨幣番号を銀行に見えないようにする技術．ディジタル署名はRSA暗号によって暗号化が行われる．署名前の電子マネーをX署名後をMとすると次の式で表される．

$$(X^e)\ mod\ n = M$$

しかし銀行がXに直接署名を行いMを作成すると銀行側にXの内容がわかってしまいどの貨幣番号の電子マネーを誰に発行したかも分かってしまう．そこでXはユーザ側が決めてさらに乱数Rを使いZに変換する．このZに署名してもらうことでXを知られずに出来たQを再びRで返還するとMができる．

1. ユーザは貨幣番号Xと乱数Rを生成しZを求め銀行に電送．

$$Z = (XR^d)\ mod\ n$$

2. 銀行はZに署名を行いQを生成しユーザに電送する．

$$Q = (Z^e)\ mod\ n$$

3. ユーザは以下の手順でMを導き出す．まずR'を求める．

$$(RR')\ mod\ n = 1$$

またQは以下のように表されるので

$$\begin{aligned} Q &= (Z^e)\ mod\ n \\ &= (XR^d)^e\ mod\ n \\ &= (X^e\ R^{ed})\ mod\ n \\ &= (X^eR)\ mod\ n \end{aligned}$$

よって

$$\begin{aligned} (QR')\ mod\ n &= (X^eR)\ mod\ n\ R'\ mod\ n \\ &= (X^eR)\ mod\ n \\ &= (X^e)\ mod\ n \\ &= M \end{aligned}$$

2.4　離散対数問題

2.4.1　合同式

整数 a, b の差 $a - b$ が 0 または整数 N の倍数であるとき

$$a \equiv b\ (\ mod\ N)$$

と書き a, b とは N を法として合同であるといいこのような関係式を合同式と呼ぶ．a を N で割った余りが r のとき $a = qN + r$ と書けるので（ただし q は商）明らかに $a \equiv r\ (mod\ N)$ である．

$(mod\ N)$ の集合として $\{0, \cdots, N-1\}$ の整数の集合を Z_N で表す．

$$Z_N = \{0, \cdots, N-1\}$$

$a \equiv b\ mod\ N$ かつ $a \in Z_N$ のとき

$$a = (b\ (\ mod\ N))$$

と書く．b が整数のとき a は b を N で割った余りとなる．$\{1, \cdots, N-1\}$ のうち N との最大公約数が 1（つまり N と互いに素）である整数の集合を Z_N で表す．よって

$$Z_N = \{x | 1 \leqq x \leqq N-1, gcd(x, N) = 1\}$$

ここで gcd は（great common divisor）を表す．$-x\ (mod\ N)$ について $(N-1) - (-1) = N$ などで $N - 1 \equiv -1\ (mod\ N)$ である．一般に $1 \leqq x \leqq N-1$ に対し次式が成り立つ．

$$N - x \equiv -x\ mod\ N$$

2.4.2 素数

2以上の整数pが1とp自身以外に約数を持たないときpをいう．フェルマーの定理についてpが素数のとき$Z_p = \{1, 2, \cdots, p-1\}$である．
pが素数のとき任意の$a \in Z_P$に対し次式が成り立つ．

$$a^{p-1} \equiv 1 \ mod \ p$$

位数とはpが素数のとき$a \in Z_P$に対し$a^x \equiv 1 \ mod \ p$となる最小の正整数xをaの位数といい$ord_p(a)$で表す．フェルマーの定理により$0 \leqq ord_p(a) \leqq p-1$である．

原子元についてpを素数のとき$ord_p(g) = p-1$となるpをZ_pの原子元（あるいは生成元）という．2乗3乗を求めていったとき$(p-1)$乗して初めて1になる数が原子元である．
pを素数gをZ_pの原子元とする．このとき$i = 0,\cdots,p-2$に対し$a_i = g^i \ mod \ p$とおくと

$$\{a_0, a_1, a_2, \cdots a_{p-2}\} = \{1, 2, \cdots, p-1\}$$

が成り立つ．

2.4.3 離散対数問題

gがZ_pの原子元のとき任意の$a \in Z_p$に対し$a = g^x \ mod \ p$となるxが必ず存在するということが分かる．このようなxをaの離散対数という．ここでaの離散対数を求める問題を離散対数問題[13]という．すなわち離散対数問題とは素数p, Z_pの原子元g及び$a \in Z_p$が与えられたとき

$$a = g^x \ mod \ p$$

となる$x \in \{0, 1, \cdots, p-2\}$を求めよという問題である．

xから$a = g^x \ mod \ p$を計算することは簡単である．しかしpが大きいときaからxを求めることは困難である．実際離散対数問題を解く効率的なアルゴリズムは見つかっていない．

2.5　匿名通信路

匿名通信路 [11] の利用目的として悪意を持つ人に個人の情報が渡らないようにする自衛と掲示板や個人間商取引での行為と実世界の個人とを結びつけたくないという 2 点が挙げられる.

匿名性を実現するための方法として匿名通信路は信頼できる第三者機関を通じて通信する方法 MIX-net や DC-net を利用する方法などが知られている. 複数の送信者からのメッセージをセンターで混ぜ合わせることによってメッセージの匿名性を保証するものやノード間で無造作にコピーを繰り返しオリジナルを不明確にすることで匿名性を実現しているものがある.

2.6　離散対数問題を使用した電子マネー方式

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

$$D_x = g^{M_x} \ mod \ n$$

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.

2.6.1　支払い処理

取引前のデータベースの情報は

$$D_{A1} = g^{M_{A1}} \ mod \ n, D_{B1} = g^{M_{B1}} \ mod \ n$$

であり取引後は

$$D_{A2} = g^{M_{A2}} \ mod \ n, D_{B2} = g^{M_{B2}} \ mod \ n$$

となる. また, 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.

$$g^{M_A 1} g^{M_B 1} = g^{M_A 2} g^{M_B 2} \ mod \ n$$

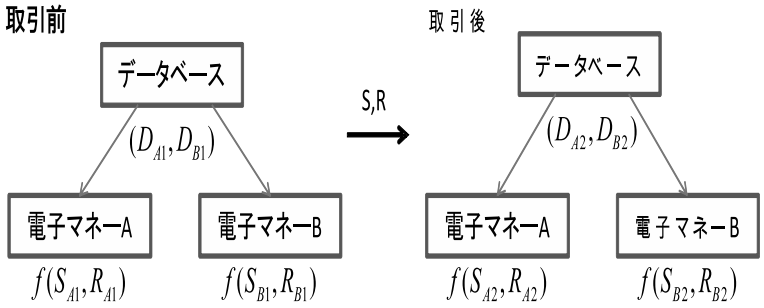

図 2.6 支払処理

2.6.2 登録プロトコル

以下の図2.7にUser登録及び，電子マネー発行の流れを示す.

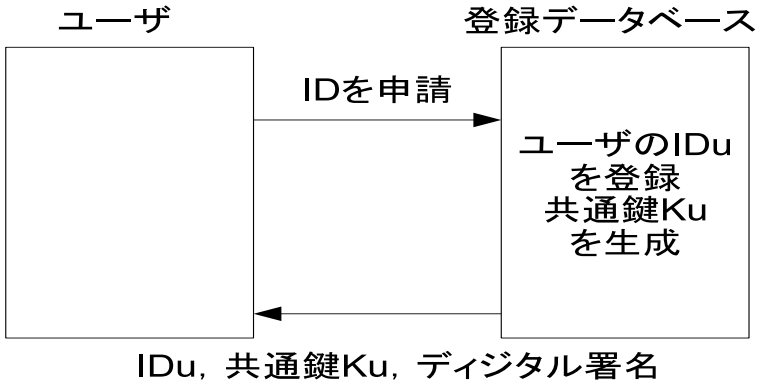

図 2.7 登録プロトコル

User登録から電子マネー発行までの手順は，まず，UserはDatabaseにIDを申請する．次にDatabaseは受信したIDをIDuとしてUser登録Databaseに登録し，登録したIDu，共通鍵Ku，ディジタル署名をUserに発行する．

2.6.3　支払いプロトコル

以下の図 2.8 に支払いの流れを示す.

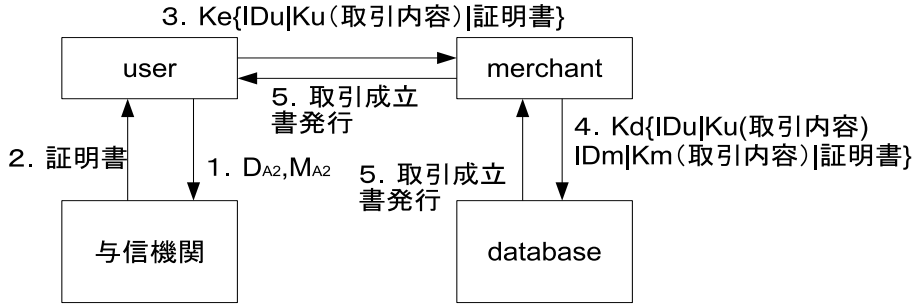

図 2.8　支払いプロトコル

- Ku, Km：登録した際の権利者の鍵
- $K'u, K'm$：データベース内の鍵
- $Kd, K'd$：データベース内の公開鍵，秘密鍵
- $Ke, K'e$：商店の公開鍵，秘密鍵

1. User は登録機関から受け取った電子マネーと取引額を与信機関の公開鍵で暗号化し，通信に用いる共通鍵と共に与信機関に送る.
2. 与信機関は送られてきた User の電子マネーを複合化し，User の支払い後の金額がプラスであること，Merchant がプラスであることに署名した証明書を通信に用いる共通鍵で User に送る.
3. User は与信機関から受け取った証明書と登録機関から受け取った電子マネー及び共通鍵 Ku で暗号化した取引内容と IDu を Merchant の公開鍵 Ke で暗号化して，Merchant に送る.
4. Merchant は受信した情報を秘密鍵 K'e により複合化し，結果と登録した鍵 Km で暗号化した取引内容と IDm を Database の公開鍵 Kd で暗号化し，Database へ送る.

5. Databaseでは受信した情報を秘密鍵K'dにより複合化し，Database内の鍵Ku，Kmで取引内容を複合化し決済を行う．Databaseは証明書よりUserの支払い後の金額がプラスであることを確認し，決済を完了する．その後，UserとMerchantに取引成立書を送る．

2.6.4 電子マネー発行

電子マネーを新しく発行する場合，日本銀行が空の電子マネーを作る．$D_x = g^{M_x} \ mod \ n$ の式の M_x に欲しい電子マネーの金額を入れる．D_x にはデータベースに登録する電子マネーの金額が入る．日本銀行以外の普通の銀行は日本銀行に現金と電子マネーを換えてもらう．日本銀行が電子マネーの流通量を把握し，調整を行うことでマネーサプライのコントロールが可能となる．

2.6.5 電子マネー廃棄

日本銀行が流通量を把握した上で電子マネーを発行し，現金と同様に電子マネーの流通を調整する．廃棄は，日本銀行のデータベースから電子マネーの情報を削除することで完了する．

第3章

提案

3.1 分散データベースについて

3.1.1 データベースの分散

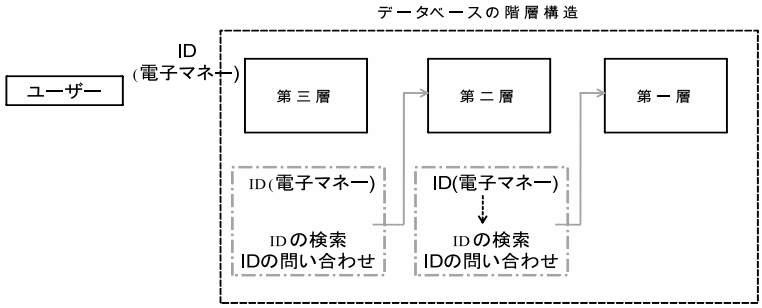

図 3.1 分散データベースの階層構造

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3.1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．

3.1.2 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，どのデータベースにIDが存在するかを見つける手掛かりとなり，データベース内でのID検索がより効率的になると考えられる．

3.2　プロトコル

本論文では，従来の方式でユーザの手持ち金額が支払後に－の値になってしまう問題を第三者機関を設置することで解決していたものを，第三者機関に頼らずに決済を完了させる支払い方式を二通り提案する．

3.2.1　前提条件

- 通信は全て匿名通信路を用いる
- Ku,Km：登録した際の権利者の鍵
- $K'u$,$K'm$：データベース内の鍵
- Ke：受領者の公開鍵
- $K'e$：受領者の秘密鍵
- Kd：データベース内の公開鍵
- $K'd$：データベース内の秘密鍵

3.2.2　暗号化関数の定義

- Ke, Kdは $\{\}$ を暗号化する関数
- Ku, Kmは（）を暗号化する関数
- $K'e, K'd$はKe, Kdを複合化する関数
- $K'u, K'm$はKu, Kmを複合化する関数

3.2.3 登録プロトコル

電子マネーの発行は全て日本銀行で行う．日本銀行以外の銀行は日本銀行に現金と電子マネーを換えてもらう．日本銀行発行にすることで，電子マネーの流通量などの調整ができ，マネーサプライのコントロールが可能となる．

ユーザ登録から電子マネーの発行までの手順として，ユーザはIDをデータベースに申請する．データベースは受信したIDuをユーザ登録データベースに登録し，ユーザにIDu，共通鍵Ku，デジタル署名を発行する．また，データベースは司法機関に共通鍵Kuを供託する．図3.2に登録プロトコル[10]を示す．

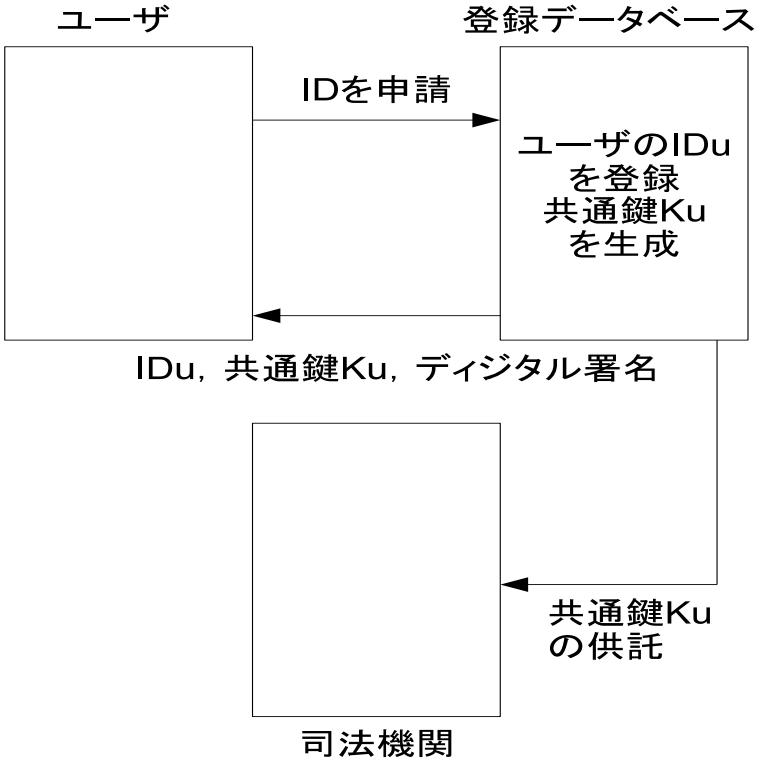

図 3.2 登録プロトコル

3.2.4　支払プロトコル 1

図 3.3 は支払いの流れ [8] を示す．取引内容とはユーザの支払金額を示す．

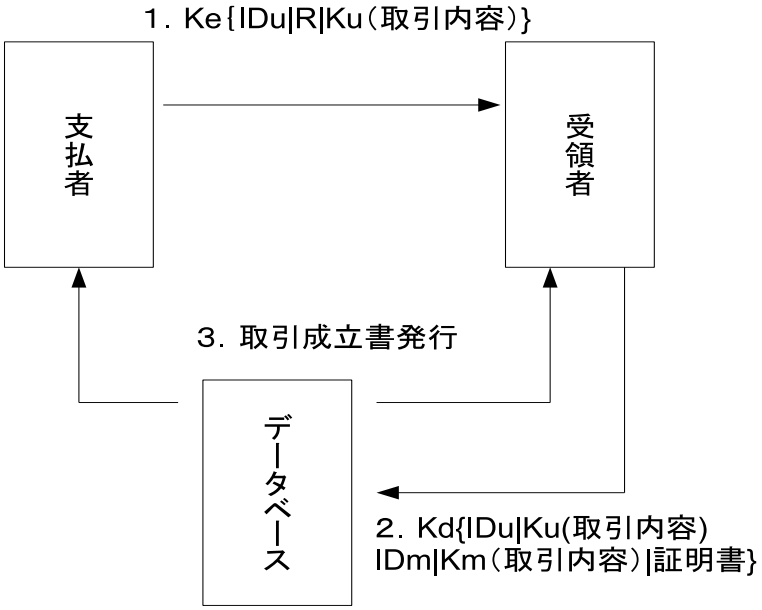

図 3.3　支払いの流れ

支払い初めから終わりまでの手順 [12] として以下に示す．

- 支払者は中央銀行より受け取った電子マネー及び共有鍵 Ku で暗号化した取引内容と IDu，乱数 R を受領者の公開鍵 Ke で暗号化し受領者に送る．
- 受領者は受信した情報を秘密鍵 K’e で複合化し，ユーザの支払い後の金額がプラスであることを確認したのち結果と登録した鍵 Km で暗号化した取引内容と IDm をデータベースの公開鍵 Kd で暗号化し，証明書と共にデータベースに送る．
- データベースでは受信した情報を秘密鍵 K’d により複合化し，データベース内の鍵 Ku,Km で取引内容を複合化し決済を行う．データベースは証明書より支払者の支払い後の金額がプラスであることを確認し，決済を完了する．その後，支払者と受領者に取引成立書を送る．

3.2.5 支払プロトコル2

図3.4は支払の流れを示す．この方式では電子マネーの上限金額を1万円程度とする．

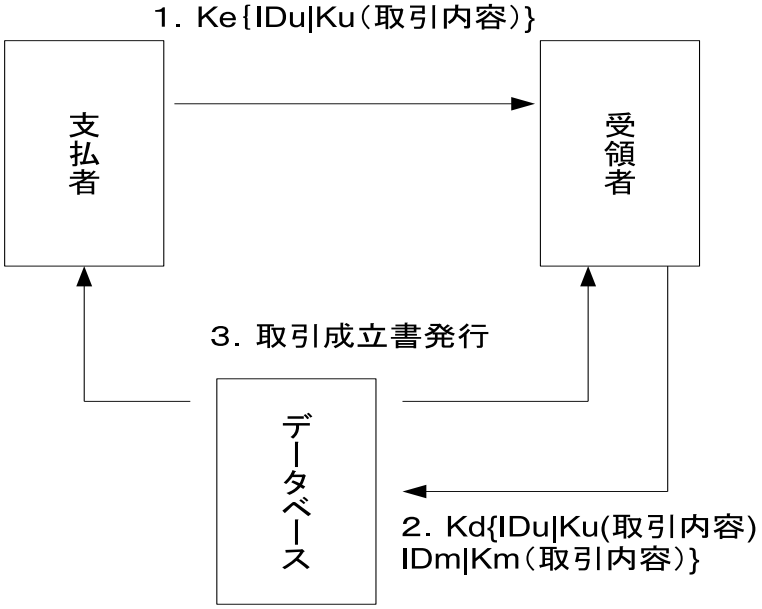

図 3.4 支払いの流れ

- 支払者は中央銀行より受け取った電子マネー及び共有鍵Kuで暗号化した取引内容とIDuを受領者の公開鍵Keで暗号化し受領者に送る．
- 受領者は受信した情報を秘密鍵K'eで複合化し，結果と登録した鍵Kmで暗号化した取引内容とIDmをデータベースの公開鍵Kdで暗号化し，データベースに送る．
- データベースでは受信した情報を秘密鍵K'dにより複合化し，データベース内の鍵Ku,Kmで取引内容を複合化し決済を行う．データベースは支払い後の金額が，あらかじめ登録した全ての乱数との組み合わせと該当するものがあるかを判断し，該当する組み合わせがあった場合，支払者の支払い後の金額がプラスであると判断し，決済を完了する．その後，支払者と受領者に取引成立書を送る．

3.2.6 支払方法の比較

支払いの提案方式1および2において，登録プロトコルは共通のものを使用する．

- **提案方式1**

  利点

  現金の特徴である完結性，匿名性，汎用性，流通性，譲渡性などを受け継いだ上で電子マネーの短所である電子データの偽造，改竄などの問題はディジタル署名や公開鍵暗号によって解決している．

  欠点

  匿名性の確保が限定的で，ユーザの個人情報が必要な取引の場合，受領者と銀行が結託すると個人情報と使用目的が結び付けられる可能性が出てくる．

- **提案方式2**

  利点

  限度額を設定するので，マネーロンダリングなどの不正で大金を送ろうとするには，何度も送金をする必要があるので，不正の検出が容易になる．

  欠点

  乱数と金額の組み合わせを全パターン，データベースに登録しておく必要があるので，限度額を大きく設定すると管理するデータ量が膨大なものとなり，運用が困難なものとなってしまう．

第4章

結論

本研究では支払時の処理に第3者を介入させない方法を2通り提案した．2つの提案方式に共通して，司法機関に鍵の供託をしているため，何らかの不正があった場合匿名性を保ちつつ，ユーザの特定をすることも可能である．また，中央銀行のデータベースで電子マネーを管理するのでユーザの不注意による紛失や盗難がない，二重支払いが起こらない，転々流通性があり，現金と同様にマネーサプライのコントロールが可能などの利点があるが，提案方式１では，基本的には匿名性があるが，ネットショッピングなどでユーザの個人情報（住所や電話番号）が必要な場合，商店と銀行が結託すると使用目的が分かってしまうという欠点がある． また，提案方式２では，乱数との組み合わせを全パターン，データベースに登録しなくてはならないため，使用限度額をあまり大きく設定すると管理するデータ量が膨大になり，運用が難しくなるという欠点がある．

今後の課題としては，今回の提案方式の欠点を改善できるより良い方法を検討する．一つの例としては金額bitを分解することなどが挙げられるが，具体的な方法はまだ検討段階である．また，地域通貨やポイント経済との対応も考えていきたい．

謝辞

本研究を行うにあたり，終始熱心に御指導していただいた木下宏揚教授と鈴木一弘助手に心から感謝致します．また，公私にわたり良き研究生活を送らせていただいた木下研究室の方々に感謝致します．

2010年2月

工藤　護

参考文献

[1] 岡田仁志：”電子マネーがわかる”，日経文庫,（2008）

[2] 木下宏揚，森住哲也：”中央銀行の発行に適した電子マネー”，神奈川大学，東洋通信機

[3] 熊本壮修：”中央銀行の超分散データベースによる貨幣システム”

[4] 相澤英孝，岩下直行，宇根正志，中山靖司，本多松前，亘理光：”電子マネーと特許法”，弘文堂

[5] 磯部朝彦：”電子マネーとオープン・ネットワーク社会”，東洋経済（1996）

[6] 岩村充：”電子マネー入門”，日経文庫（1996）

[7] 楠田浩二，櫻井幸一：”公開鍵暗号方式に関する現状と課題”，日本銀行金融研究所

[8] 松尾真一郎，森田光：”電子取引を実現する安全なプロトコル”，暗号と情報セキュリティ・シンポジウム,SCIS2000-C34

[9] 小森:”公開鍵基盤を用いた電子マネーシステムの研究”, http://csai03.is.noda.sut.ac.jp/akira/ronbun.pdf

[10] 竹村:”電子マネープロトコル研究の動向”, http://www.e.u-tokyo.ac.jp/item/dp/dp36.pdf

[11] 谷口:”通信ネットワークセキュリティ”, 日本実業出版社（1998）

[12] ”初等整数論, アルゴリズム入門, 暗号”, http://www2.cc.niigata-u.ac.jp/takeuchi/tbasic/BackGround/

[13] 高木貞治:”初等関数論講義 第2版”, 共立出版株式会社（1994）

[14] ベルナルド・リエター, 小林一紀, 福本初男, 加藤敏春:”新しいコミュニティ通貨の誕生　マネー崩壊”, 日本経済評論社（2000）

[15] 舘龍一郎:”電子マネー・電子商取引と金融政策”, 日本銀行金融研究所（2000）

[16] 小西英行:”ポイント経済と電子マネー, 地域通貨に関する考察”, 富山国際大学地域学部紀要　第7巻（2007）

[17] 中山靖司, 森畠秀美, 阿部正幸, 藤崎英一郎:”電子マネーの一実現方式について, ―安全性, 利便性に配慮した新しい電子マネー実現方式の提案―”, 日本銀行金融研究所, 金融研究（1997）

質疑応答

能登先生より

Q：実装は考えていますか？

現在の段階では提案のみであり，実装は電子マネーの管理が中央銀行のものとなっているので難しく，また別の方法で試験を行っていきたい．

豊島先生より

Q：電子マネーの管理はどうなっていますか？

電子マネーの管理は各国，各通貨毎に中央銀行が行います．