現金との代替を目指した電子マネーの研究

木下研究室　200602823

工藤　護

背景

• 電子的な決済が増える中、現在普及しているのがプリベイド型電子マネーであり、一度の決済でしか利用ができないため現金との代替が不可能である。

• 印刷技術の進歩などにより偽造の問題が深刻になっているので、より強固な不正対策が必要であり、電子化が重要となっている。

目的

- 既存の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可能な電子マネーを目指す。

- 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す。

- 従来必要であった第三者機関を用いずに、決済を完了させる。

提案方式

- 基本構造として研究室で以前より研究されている離散対数問題を使用した電子マネーを用いる。
  - データベースが個々の金額、取引額が分からなくなる他、価値の分散ができる。

- データベースを分散データベース化し、階層構造をなすことでトラフィックと処理の集中を避ける。
  - 負荷が分散される他、どれか1つのシステムに障害が起きても全体は停止しない。

- 通信は全て匿名通信路を用いる
  - データベースとユーザに対し匿名性が保てる。

電子マネーの構造

- Sxを64bitの金額、Rxを448bitの乱数とする

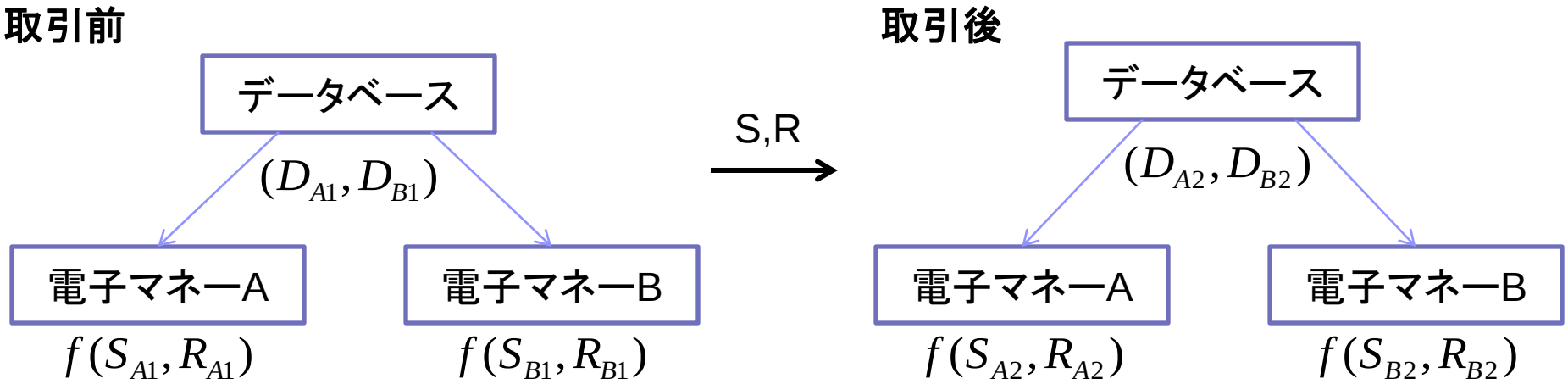
$$M_x = f(S_x, R_x) = 2^{448} S_x + R_x$$

- データベースに蓄積する電子マネーxの認証子Dxは原子元をgとすると

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

- 離散対数問題を使用しているためDxからMxを求めることが困難である

支払処理の原理



- 取引前のデータベースの情報は、

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

- 取引後のデータベース情報は

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

- 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。

$$g^{M_{A1}} g^{M_{B1}} = g^{M_{A2}} g^{M_{B2}} \bmod n$$

電子マネーの発行

・中央銀行がデータベースに空の電子マネーを作る。

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

・Mxに任意の電子マネーの金額を入れる。

・Dxにはデータベースに登録する電子マネーの金額が入る。

・通常の銀行は中央銀行から電子マネーを受け取る。

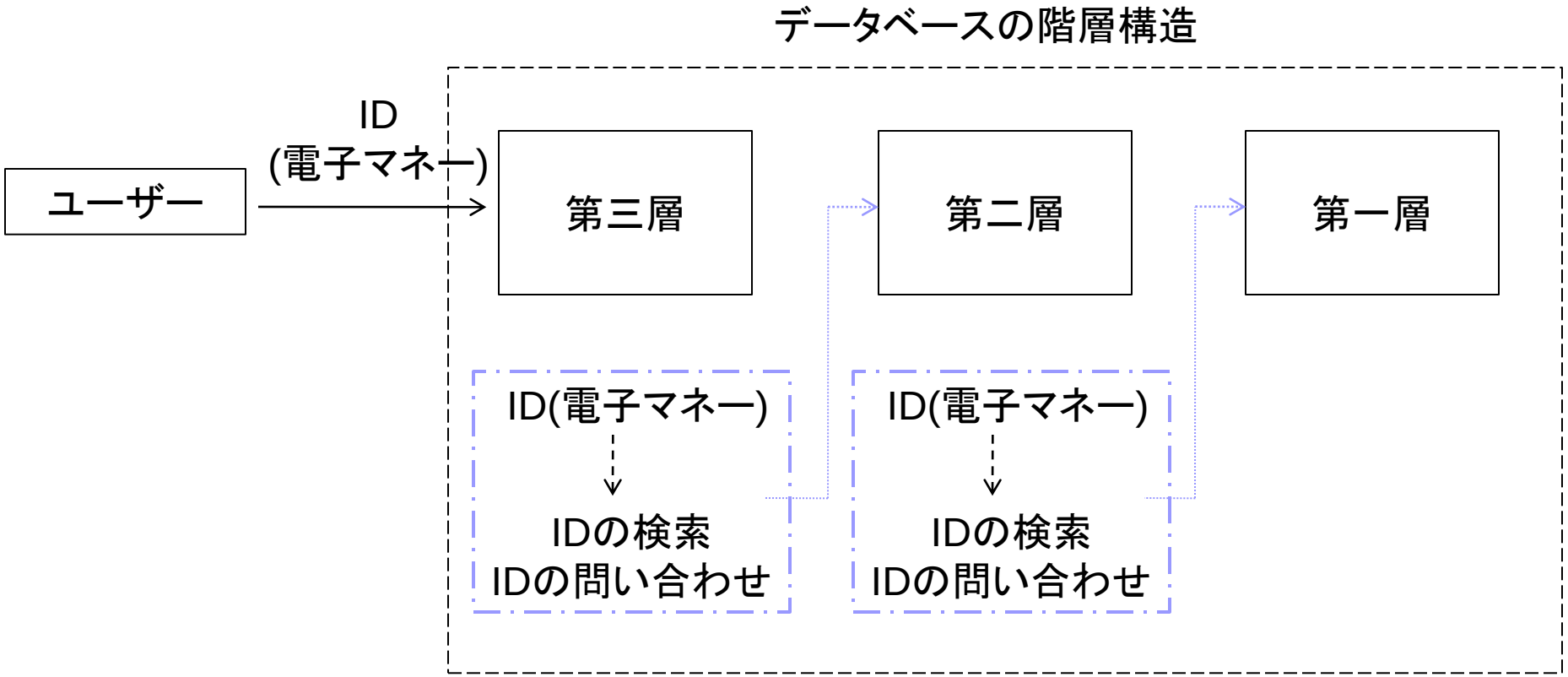
・このことから現金と同じようにマネーサプライのコントロールが可能となる。

提案方式について

- データベースをトラフィックや処理の集中を避けるために分散データベース化し、検索を効率的に行えるように識別子を設定する。

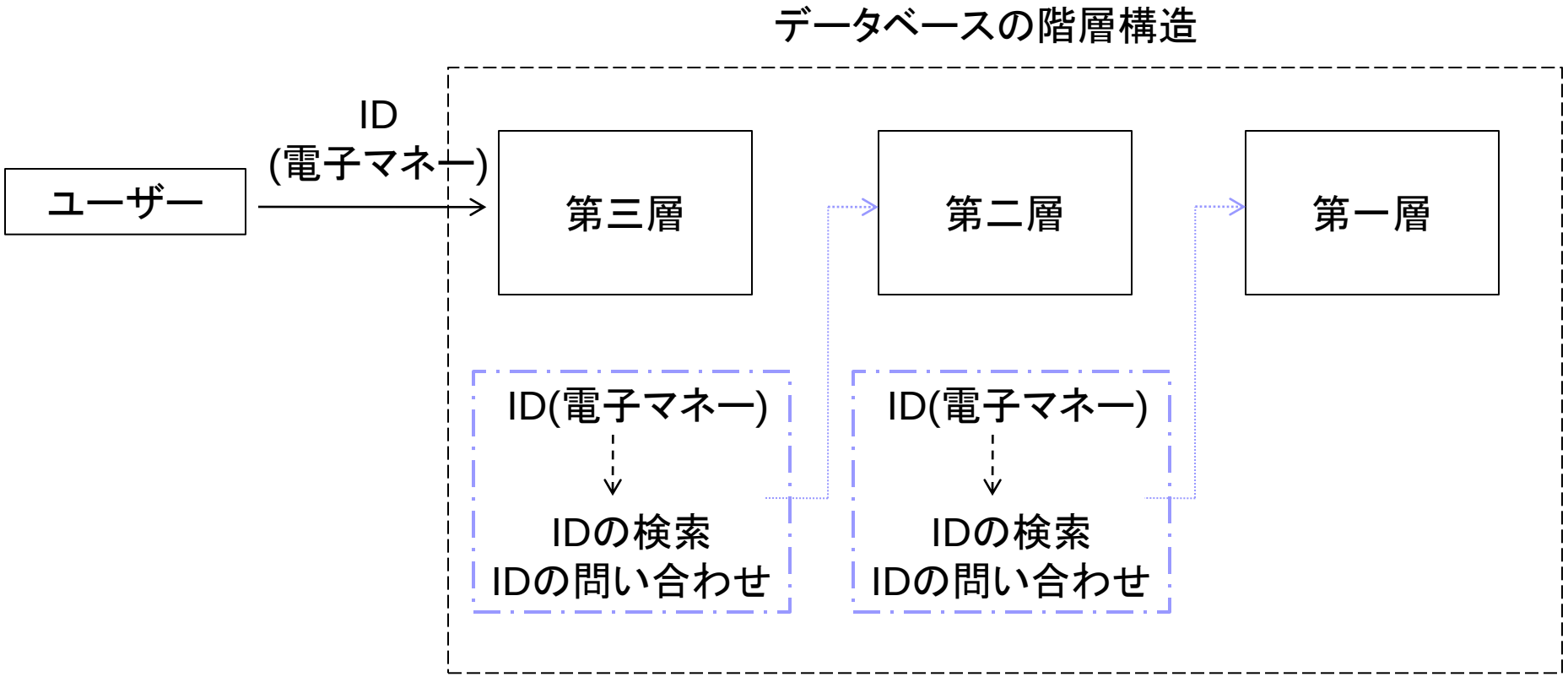
- 今回、従来の方式でユーザの手持ちの金額が支払い後に負の値になるのを防ぐために設置していた第三者機関に頼らずに、決済を終える方式を二通り提案する。

データベースの分散



- 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。

データベースの分散



- 支払い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。

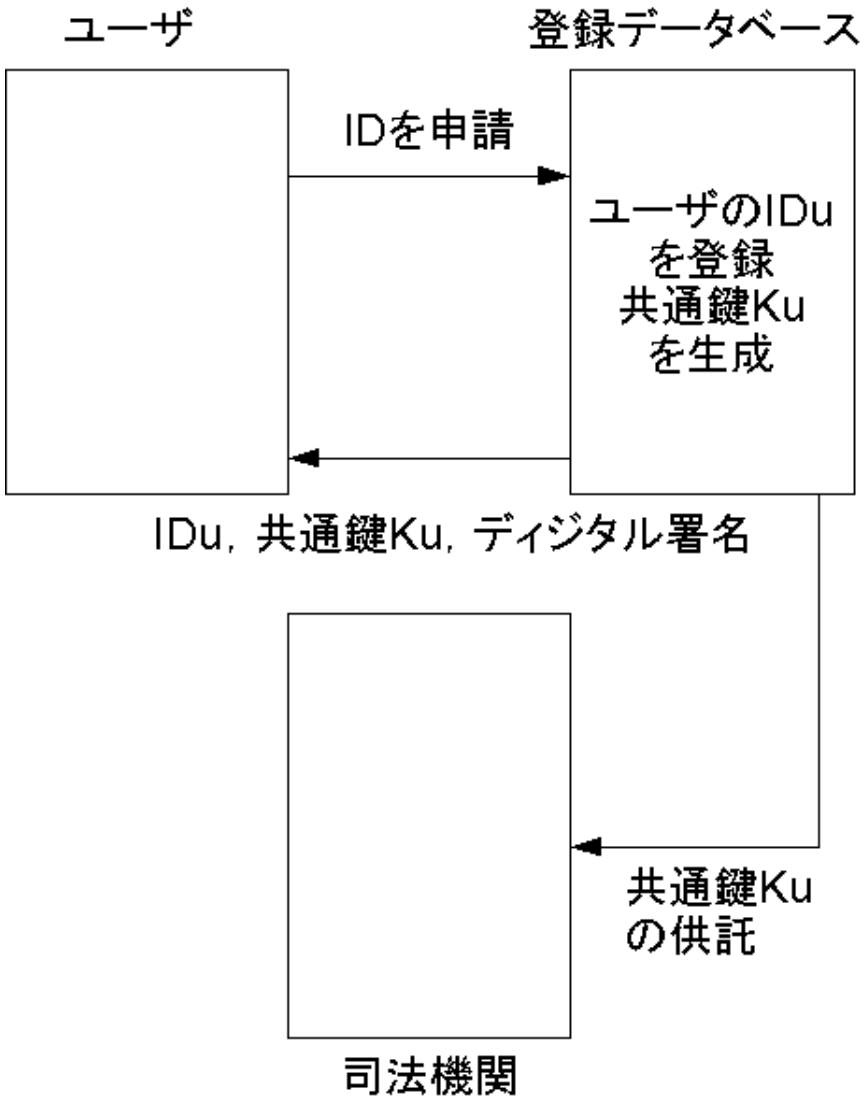
データベースの分散

- 識別子はどのデータベースに存在するかを容易に見つけることができるように割り当てる。

例－XX$AA.BB.CC.centralbank.YY.ZZ

- 赤字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の区切り文字を示す。

登録プロトコル

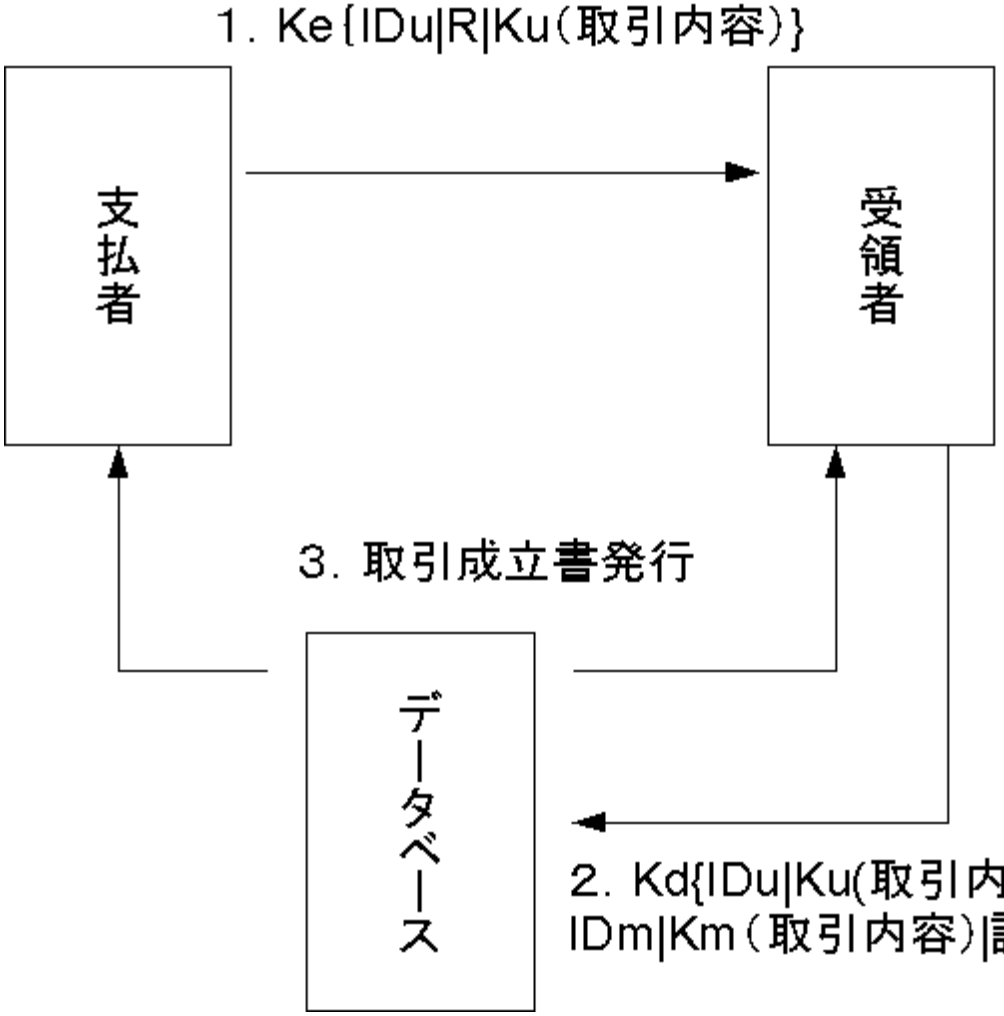


1．ユーザはIDを登録データベースに申請する．

2．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．

3．データベースは司法機関に共通鍵Kuを供託する．

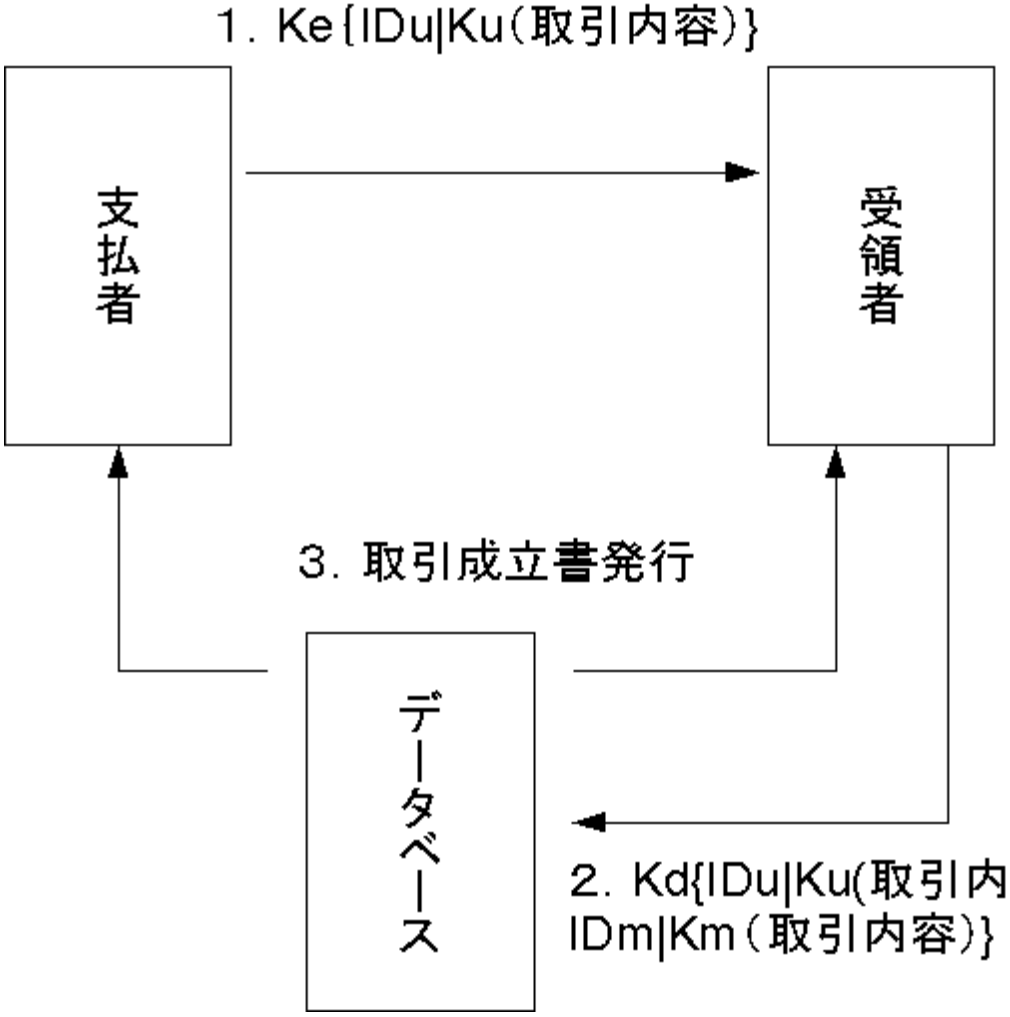
支払プロトコル1



・受領者に支払者の乱数Rを開示し，受領者側で取引後の支払者の金額が一の値にならないことを確認し，証明書を発行してデータベースに送る方式.

Ku,Km：登録した際の権利者の鍵
Ke：受領者の公開鍵
Kd：データベース内の公開鍵

支払プロトコル2



・データベースに金額と乱数の組み合わせを全て登録しておき，該当するものがあるかどうかを判断し，それにより支払者の金額がプラスであると判断し決済を完了する方式．

Ku,Km：登録した際の権利者の鍵
Ke：受領者の公開鍵
Kd：データベース内の公開鍵

まとめ

- マネーサプライのコントロールや現金との代替については中央銀行発行にし、離散対数問題を用いた基本構造にすることで実現する。

- マネーロンダリングなどへの対応は司法機関へ鍵を供託し、提案方式2のように一度の使用額を限定することで解決する。

- 第三者機関を用いずに決済を完了させることについては、方式1では乱数Rを受領者に開示することで、方式2は金額と乱数の組み合わせをあらかじめ登録することで解決する。

今後の課題

- 今回は2種類の支払い方式を考案したが，方式1では個人情報が必要な場合の取引では，受領者と銀行が結託すると個人と使用目的の結び付けが可能になるという欠点がある．また，方式2では乱数との組み合わせを全パターン登録しなければならないため，上限金額をある程度制限しなければならない．

- 以上の問題点を解決できるよりよい方式を考案し，ポイント経済や地域通貨との対応も考えていきたい．