マルチメディア通信と分散処理　97－25
コンピュータセキュリティ　8－25
（2000．3．22）

# 関連づけ可能な匿名オフライン電子マネー

小出篤史† 多田 充† 宮地充子†
北陸先端科学技術大学院大学 情報科学研究科†

今日，インターネットをはじめとするオープン・ネットワークの普及により，電子マネーに対する期待が高まっている．しかしながら，本格的な実用化を進めるうえでは，まだ多くの課題が残っている．

従来の電子マネー方式では発行機関である銀行は不正をはたらかないと仮定していた．しかし最近では，顧客名簿の流出など行員個人による不祥事がたいへん多い．組織としての銀行の不正はあまり見かけないが，銀行を構成する行員個人の不正を考慮すべきと考えられる．

本稿では，秘密鍵を知った行員が他の不正な利用者と結託して，電子マネーの偽造を行う問題に注目する．信頼できる第三者機関を仮定することで，銀行が発行したものと還流したものの関連づけをとりつつ，利用者の匿名性を確保できるオフライン電子マネー方式を提案する．

# Linkable Anonymous Off-line E-cash

Atsushi Koide† Mitsuru Tada† and Atsuko Miyaji†
School of Information Science,
Japan Advenced Institute of Science and Technology†

The more widely open-networks such as the Internet get spread, the more remarkable E-cash becomes. In the realization of E-cash, a lot of problems have been unsolved.

In most E-cash schemes ever proposed, it has been assumed that a bank as an issuer never behave maliciously. However, in the real world, this assumption seems to be fairly artifical. Since we have frequently seen banker's illegal behaviors.

In this paper, we focus on the problem that an illegal banker may leak the secret key of the bank to forge coins. *Proposed Scheme* is an off-line E-cash scheme with a trustee in which a bank can link a coin in the withdrawal step to that in the deposit step, and which can keep user's anonymity.

## 1. はじめに

今日多くの電子マネー方式が提案され，我が国でも東京・新宿をはじめ各地で実証実験が行われている．店頭における対面販売では，電子マネーはクレジットカードなどと同様に支払い処理が煩雑になるなどの問題が残っていた．しかし，オフラインによる検証のほか非接触型 IC カードの開発により，支払い処理の点においても電子マネーは現金やクレジットカードに迫りつつある．また，インターネットを利用したコンテンツサービスが脚光をあびるなか，ネットワークおける少額の決済手段としても注目されている．

実証実験をはじめ，限定的な意味での実用化は進んでいるものの，本格的な実用化を進めるうえでは，運用上の不正対策や法改正をはじめ，まだまだ多くの課題が残っている．

例えば，従来の電子マネー方式では発行機関である銀行は不正をはたらかないと仮定していた．しかし最近では，顧客名簿の流出など行員個人による不祥事がたいへん多い．組織としての銀行の不正はあまり見かけないが，銀行を構成する行員個人の不正を考慮すべきと考えられる．

宮崎，櫻井 7), 8) は，電子マネー方式における発行機関の不正として，預け入れ済みの支払い履歴から二重使用を捏造し，正当な利用者を不正使用者として仕立て上げ違約金を請求する不正 3)，不正な行員と利用者が結託し利用証明書を偽造することで，収益をあげる不正についてとりあげ，対応策を示している．

従来提案されてきている電子マネー方式では，秘密鍵を知った行員が他の不正な利用者と結託して，偽造を行う状況はまったく考慮されていなかった．

† 北陸先端科学技術大学院大学 情報科学研究科
〒 923-1292 石川県能美郡辰口町旭台 1-1

本稿では，不正な内部行員と利用者が結託し，電子マネー発行に用いられる銀行の秘密鍵をもとに電子マネーを偽造する不正に注目する．

本論文の構成として，まずブラインドされたメッセージとブラインドされていないメッセージを共有して署名を行う部分ブラインド署名，対数が等しいことを証明するゼロ知識証明について紹介する．次に，対応策として匿名性を確保しながらも，どのようにすれば電子マネーの流れを銀行が管理することができるのかを示す．その上で，既存の電子マネー方式をもとに関連づけ可能な電子マネー方式を論じる．

## 2. 準　　備

### 2.1 部分ブラインド署名

ブラインド署名は，利用者が作成した電子マネーであることを示すメッセージを銀行に知られることなく，署名を行うことができる．しかしながら，不正をするかもしれない利用者が他人の識別情報を埋め込んだり，引き出し金額とは違う金額情報を埋め込んだりしようとすることも考えられる．

そこで，署名依頼者 $\mathcal{C}$ は識別情報や金額情報などの一部のメッセージを部分的に署名者 $\mathcal{S}$ と共有して署名を行うことによって，利用者の不正をできないようにする必要がある．

部分ブラインド署名は，署名依頼者 $\mathcal{C}$ と署名者 $\mathcal{S}$ との間でブラインドされたメッセージとブラインドされていない特定のメッセージを共有して署名を生成する方法である．

離散対数問題を安全性の根拠としている Schoenmakers ブラインド署名 9) をベースにした部分ブラインド署名が提案されている．1) まず，署名依頼者 $\mathcal{C}$ は，ブラインド化されたメッセージと共に共有メッセージを署名者 $\mathcal{S}$ に送る．次に，署名者 $\mathcal{S}$ は共有情報を確認し，ブラインドされたメッセージと共有情報の両方に対して署名を生成するものである．

**【初期設定】**

**Step1.** 署名者 $\mathcal{S}$ は，素数 $p$, $q$ $(q|p-1)$ を生成し，乗法群 $\mathbb{Z}_p^*$ での位数が $q$ となるような $g$ を定める．$\mathcal{H}$ は適切なハッシュ関数，$\|$ は連結とする．演算は特に断りのない限り $(\mathrm{mod}\ p)$ で行われる．

**Step2.** 署名者 $\mathcal{S}$ は秘密鍵 $x_1$, $x_2 \in \mathbb{Z}_q$ を定め，対応する公開鍵 $h_1 = g^{x_1}$, $h_2 = g^{x_2}$ を計算する．

《秘密鍵》　$x_1$, $x_2$

《公開鍵》　$h_1$, $h_2$, $g$, $p$, $q$

《共有メッセージ》　$c$

《メッセージ》　$m$

**【署名生成】**

**Step1.** 署名依頼者 $\mathcal{C}$ は共有メッセージ $c$ を署名者 $\mathcal{S}$ へ送る．

**Step2.** 署名者 $\mathcal{S}$ は乱数 $k \in \mathbb{Z}_q$ を生成し，$\delta = g^k$ を計算する．署名者 $\mathcal{S}$ は $\delta$ を署名依頼者 $\mathcal{C}$ へ送る．

**Step3.** 署名依頼者 $\mathcal{C}$ は乱数 $a$, $b \in \mathbb{Z}_q$ を生成し，$t = \delta g^a (h_1^c h_2)^b$ を計算する．

**Step4.** 署名依頼者 $\mathcal{C}$ は $r = \mathcal{H}(c\|m\|t)$, $r' = r - a \pmod q$ を計算し，$r'$ を署名者 $\mathcal{S}$ へ送る．

**Step5.** 署名者 $\mathcal{S}$ は $s' = \frac{k - r'}{cx_1 + x_2} \pmod q$ を署名依頼者 $\mathcal{C}$ へ送る．

**Step6.** 署名依頼者 $\mathcal{C}$ は $s = s' + b \pmod q$ を計算し，本来の署名 $s$ を求める．

**【署名検証】**

**Step1.** 署名依頼者 $\mathcal{C}$ は $[\alpha, c, m, r, s]$ を署名検証者 $\mathcal{V}$ に送る．

**Step2.** 署名検証者 $\mathcal{V}$ は $r = \mathcal{H}(c\|m\|g^r (h_1^c h_2)^s)$ を満たすかどうかを確認することで，署名 $(r, s)$ の正当性を検証する．

[安全性について] 離散対数問題が困難であると仮定し，ハッシュ関数 $\mathcal{H}$ が仮想的なランダム関数として振る舞い，署名依頼者 $\mathcal{C}$ によって乱数 $a$, $b$ がランダムに選ばれたものであるならば，署名者 $\mathcal{S}$ はメッセージ $m$ を推測することができず，たとえ署名者 $\mathcal{S}$ と署名検証者 $\mathcal{V}$ が結託しても $s'$ と $s$ の対応関係を知ることができない．

### 2.2 対数が等しいことの証明

支払いプロトコルで，マネー情報に同じ識別情報が埋め込まれていることを証明する場合に用いる．$A = a^x \pmod p$, $B = b^x \pmod p$ としたとき，対数が等しいこと $\log_a A = \log_b B$ を対数 $x$ を示さずに証明するゼロ知識証明が提案されている．4) このプロトコルは証明者 $\mathcal{P}$ と検証者 $\mathcal{V}$ の二者からなる．

**【初期設定】**

**Step1.** 証明者 $\mathcal{P}$ は素数 $p$, $q$ $(q|p-1)$ を生成し，乗法群 $\mathbb{Z}_p^*$ での位数が $q$ となるような $g$ を定める．

**Step2.** 証明者 $\mathcal{P}$ は $(A, a)$, $(B, b)$ を検証者 $\mathcal{V}$ に送る．

《秘密》　$x$

《公開》　$A(=a^x)$, $a$, $B(=b^x)$, $b$, $p$, $q$, $g$

《証明すること》　$\log_a A = \log_b B$

**【証明】**

**Step1.** 証明者 $\mathcal{P}$ は乱数 $i \in \mathbb{Z}_q$ を生成し，$A' = a^i$, $B' = b^i$ を計算し，$A', B'$ を検証者 $\mathcal{V}$ へ送る．

**Step2.** 検証者 $\mathcal{V}$ は乱数 $d \in \mathbb{Z}_q$ を生成し，証明者 $\mathcal{P}$ へ送る．

**Step3.** 証明者 $\mathcal{P}$ は $j = dx + i$ を計算し，$j$ を検証者 $\mathcal{V}$ へ送る．

**Step4.** 検証者 $\mathcal{V}$ は $a^j = A^d \cdot A'$，$b^j = B^d \cdot B'$ を満たすことを確認する．

## 3. 対 応 策

従来提案されてきている電子マネー方式では，秘密鍵を知った行員が他の不正な利用者と結託して，偽造を行う状況はまったく考慮されていなかった．

不正な内部行員と利用者が結託し，内部行員が利用者に銀行の秘密鍵を漏えいさせて電子マネーを偽造した場合に次のようなことが考えられる．

利用者は引き出しプロトコルを通すことなく，秘密鍵をもとにマネー情報を偽造することができる．偽造したマネー情報は検証式を満たすため，支払いプロトコルでも店は受け入れ，受け入れた店は預け入れプロトコルでも銀行は受け入れる．銀行はマネー情報の正当性を検証式によってのみしか判定することができないため，偽造があったことがわからない．

対応策として，マネー情報に ID（マネー ID）を挿入することにより電子マネーを管理することが必要である．引出プロトコルにおいて発行したもののと，預入プロトコルにおいて還流したものを関連づける．これにより，偽造による引出プロトコルを通していないマネー情報を識別することができるため，偽造がなされたことが非常に高い確率で検出できる．

オンライン電子マネー 2) の教訓でもみられるように，マネー情報にマネー ID で関連づけを行うことは，匿名性を阻害することでもあった．しかしながら，信頼できる第三者機関を仮定することで，銀行は発行したものと還流したものの関連づけをとりつつ，利用者の匿名性を確保できるオフライン電子マネーを既存方式 6) をもとに提案する．

具体的には，匿名性を損なうような情報を銀行に与えないという方針から，支払いプロトコルによりマネー情報を利用者 $\mathcal{U}$ から受け取った店 $\mathcal{S}$ は直接銀行へ預け入れずに，信頼できる第三者機関に $\mathcal{T}$ を通して預け入れを行う．信頼できる第三者機関は $\mathcal{T}$ は秘密鍵を用いて，マネー ID を復号し，マネー ID と金額情報のみを銀行 $\mathcal{B}$ へ預け入れを行う．

これにより，信頼できる第三者機関を仮定することで，銀行 $\mathcal{B}$ と店 $\mathcal{S}$ が単独あるいは結託したとしても利用者 $\mathcal{U}$ の匿名性を確保することができる．

## 4. 提 案 方 式

**【初期設定】**

**Step1.** 銀行 $\mathcal{B}$ は素数 $p$，$q$ $(q|p-1)$ を生成し，$\mathbb{G}_q$ を $\mathbb{Z}_p^*$ の位数が $q$ となるような $\mathbb{Z}_p^*$ の部分集合とし，$g \in \mathbb{G}_q$ を定める．$\mathcal{H}$ は $\{0,1\}$ から $\{0,1\}^l$ $(l \approx 160)$ への適切なハッシュ関数，$\|$ は連結とする．演算は特に断りのない限り $(\mathrm{mod}\ p)$ で行われる．

**Step2.** $\mathcal{B}$ は秘密鍵 $x_1, x_2, x_3, x_4 \in \mathbb{Z}_q^*$ を定め，公開鍵 $h_1 = g^{x_1}$，$h_2 = g^{x_2}$，$h_3 = g^{x_3}$，$h_4 = g^{x_4}$ を計算する．銀行 $\mathcal{B}$ は信頼できる第三者機関 $\mathcal{T}$ に安全な通信路を用いて秘密鍵 $x_2$ を送る．

**Step3.** 信頼できる第三者機関 $\mathcal{T}$ は秘密鍵 $x_\mathcal{T} \in \mathbb{Z}_q^*$ を定め，公開鍵 $h_\mathcal{T} = g^{x_\mathcal{T}}$ を計算する．

**【登録プロトコル】**

電子マネーを利用するにあたり，利用者 $\mathcal{U}$ および店 $\mathcal{S}$ は事前に銀行 $\mathcal{B}$ に登録を行う必要がある．

**Step1.** 利用者 $\mathcal{U}$（または店 $\mathcal{S}$）はそれぞれ銀行 $\mathcal{B}$ に対し，電子マネー口座の開設要求をして，何らかの方法により身分証明を行う．

**Step2.** 銀行 $\mathcal{B}$ は各人に固有のユーザ ID （$ID_\mathcal{U} \in \mathbb{Z}_{\lfloor\sqrt{q}\rfloor}$），（または店 ID （$ID_\mathcal{S} \in \mathbb{Z}_{\lfloor\sqrt{q}\rfloor}$））を生成し，対応する電子マネー口座を登録する．

**Step3.** 銀行 $\mathcal{B}$ はユーザ ID （$ID_\mathcal{U}$）（または店 ID （$ID_\mathcal{S}$））を付与する．

**【引き出しプロトコル】**

引き出しプロトコルによって，利用者 $\mathcal{U}$ は電子マネー口座 $ID_\mathcal{U}$ の預金から電子マネーに変える．

**Step1.** 利用者 $\mathcal{U}$ は，ユーザ ID （$ID_\mathcal{U}$）および引き出し金額（$w$ 円）を何らかの方法によって銀行 $\mathcal{B}$ へ示す．

**Step2.** 銀行 $\mathcal{B}$ は乱数 $f$，$k \in \mathbb{Z}_q$，マネー ID （$ID_M \in \mathbb{Z}_{\lfloor\sqrt{q}\rfloor}$）を生成し，識別情報 $u = (ID_\mathcal{U} \| ID_M)$ を計算する．有効期限 ExpDate，引き出し金額（$w$ 円）から金額情報 $c = (w \| \mathrm{ExpDate})$ を計算する．

**Step3.** 銀行 $\mathcal{B}$ は $\delta = (h_1^u h_2 (h_3^c h_4)^f)^k$ を計算し，マネー ID （$ID_M$），金額情報 $c$，乱数 $f$ および $\delta$ を $\mathcal{U}$ へ送る．

**Step4.** 利用者 $\mathcal{U}$ は乱数 $y \in \mathbb{Z}_q^*$ を生成し，識別情報 $u = (ID_\mathcal{U} \| ID_M)$，$e = fy \ (\mathrm{mod}\ q)$，$\alpha = (h_1^u h_2)^y$ を計算する．

**Step5.** 利用者 $\mathcal{U}$ はまた乱数 $a, b, z_1, z_2 \in \mathbb{Z}_q$ を生成し，$t = \delta g^a (\alpha (h_3^c h_4)^e)^b$，$m = h_1^{z_1} h_2^{z_2}$

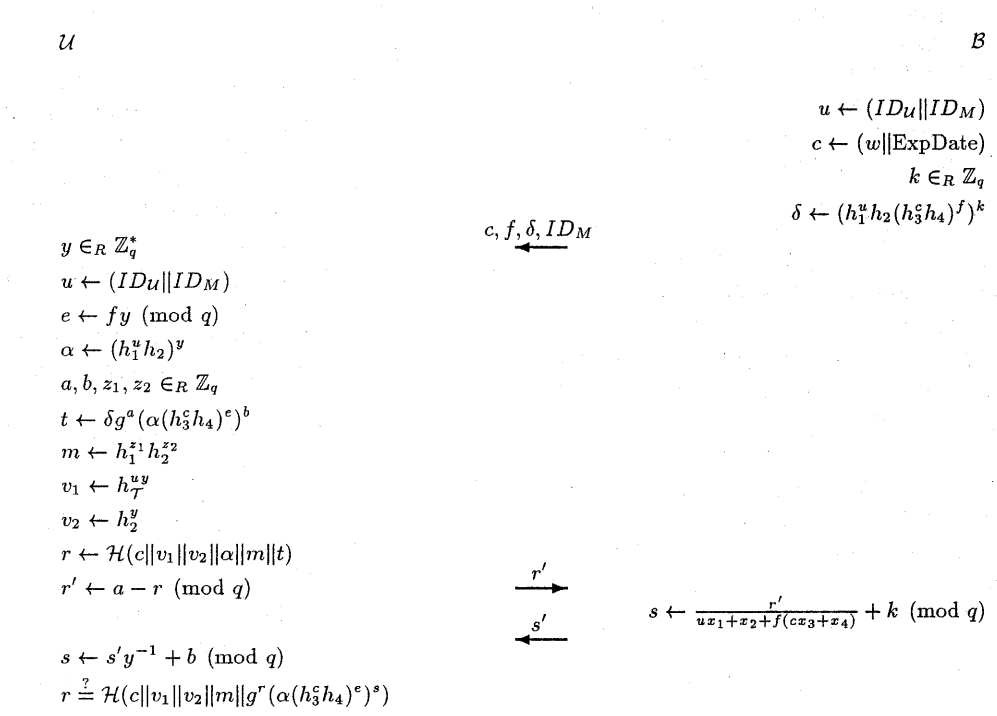


図 1　引き出しプロトコル

$v_1 = h_{\mathcal{T}}^{uy}$, $v_2 = h_2^y$ および $r = \mathcal{H}(c \| v_1 \| v_2 \| m \| t)$ を計算する.

**Step6.** 利用者 $\mathcal{U}$ は $r' = a - r \pmod q$ を計算し, $r'$ を銀行 $\mathcal{B}$ へ送る.

**Step7.** 銀行 $\mathcal{B}$ は署名 $s' = \frac{r'}{ux_1 + x_2 + f(cx_3 + x_4)} + k \pmod q$ を計算し, $\mathcal{U}$ へ送る.

**Step8.** 利用者 $\mathcal{U}$ は本来の署名 $s = s' y^{-1} + b \pmod q$ を計算する.

**Step9.** 利用者 $\mathcal{U}$ は検証式 $r = \mathcal{H}(c \| v_1 \| v_2 \| m \| g^r (\alpha (h_3^c h_4)^e)^s)$ を満たすかどうか確認する.

**【支払いプロトコル】**

利用者 $\mathcal{U}$ はマネー情報 $M = [\alpha, c, e, m, r, s, v_1, v_2]$ を用いて店 $\mathcal{S}$ に対し次のようにして支払を行う.

**Step1.** 利用者 $\mathcal{U}$ は乱数 $i \in \mathbb{Z}_q$ を生成し, $A' = v_1^i$, $B' = (\alpha v_2^{-1})^i$ を計算し, $A', B'$ をマネー情報 $M$ と共に店 $\mathcal{S}$ へ送る.

**Step2.** 店 $\mathcal{S}$ は検証式 $r = \mathcal{H}(c \| v_1 \| v_2 \| m \| g^r (\alpha (h_3^c h_4)^e)^s)$ を満たすかどうか確認する.

**Step3.** 店 $\mathcal{S}$ はチャレンジ $d = \mathcal{H}(M \| ID_{\mathcal{S}} \| \mathrm{Date/Time})$ を計算し, チャレンジ $d$ を利用者 $\mathcal{U}$ へ送る.

**Step4.** 利用者 $\mathcal{U}$ は $r_1 = z_1 + udy \pmod q$, $r_2 = z_2 + dy \pmod q$, $j = duy + i \pmod q$ を計算し, $r_1$, $r_2$, $j$ を店 $\mathcal{S}$ へ送る.

**Step5.** 店 $\mathcal{S}$ は検証式 $h_1^{r_1} h_2^{r_2} = \alpha^d m$, $h_{\mathcal{T}}^j = v_1^d A'$, $h_1^j = (\alpha v_2^{-1})^d B'$ を満たすかどうか確認する.

**【預け入れプロトコル1】**

店 $\mathcal{S}$ はマネー情報 $M$ を信頼できる第三者機関 $\mathcal{T}$ へ次のようにして預け入れを行う.

**Step1.** 店 $\mathcal{S}$ はマネー情報および支払履歴 $(M, A', B', ID_{\mathcal{S}}, \mathrm{Date/Time}, r_1, r_2, j)$ を $\mathcal{B}$ へ送る.

**Step2.** 信頼できる第三者機関 $\mathcal{T}$ は検証式 $r = \mathcal{H}(c \| v_1 \| v_2 \| m \| g^r (\alpha (h_3^c h_4)^e)^s)$ を満たすかどうか確認する.

**Step3.** 信頼できる第三者機関 $\mathcal{T}$ はチャレンジ情報 $d = \mathcal{H}(M \| ID_{\mathcal{S}} \| \mathrm{Date/Time})$ を計算する.

**Step4.** 信頼できる第三者機関 $\mathcal{T}$ は検証式 $h_1^{r_1} h_2^{r_2} = \alpha^d m$, $h_{\mathcal{T}}^j = v_1^d A'$, $h_1^j = (\alpha v_2^{-1})^d B'$ を満たすかどうか確認する.

**【預け入れプロトコル2】**

信頼できる第三者機関 $\mathcal{T}$ はマネー情報および支払

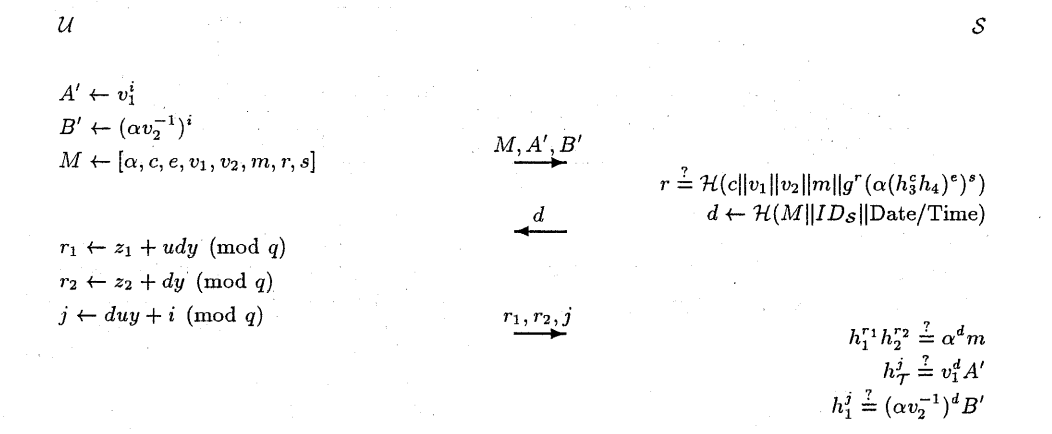


**図 2** 支払いプロトコル

い履歴 ($M$, $A'$, $B'$, $ID_{\mathcal{S}}$, Date/Time, $r_1$, $r_2$, $j$) を用いて $\mathcal{B}$ へ次のようにして銀行 $\mathcal{B}$ へ預け入れを行う.

**Step1.** 信頼できる第三者機関 $\mathcal{T}$ は秘密鍵 $x_{\mathcal{T}}$, $x_2$ を用いて, $I = v_1^{x_{\mathcal{T}}^{-1}} / v_2^{x_2^{-1}}$ を計算する.

**Step2.** 信頼できる第三者機関 $\mathcal{T}$ は $I$ を銀行 $\mathcal{B}$ へ送る.

**Step3.** 銀行 $\mathcal{B}$ は発行済みの $u$ から, $g^u = I$ を満たすマネー情報を特定・照合する.

## 5. 安全性の考察

### 5.1 完 全 性

提案方式が完全であるということは以下の属性を満たすことである.

(1) 利用者 $\overline{\mathcal{U}}$ が引き出しプロトコルに従い, 支払いプロトコルにおいてもマネー情報を送り, チャレンジに対する応答を返すならば, 店 $\overline{\mathcal{S}}$ は受け入れる.

(2) 店 $\overline{\mathcal{S}}$ が支払いプロトコルを受け入れ, 預け入れプロトコルにおいても支払い履歴を受け入れるならば, 銀行 $\overline{\mathcal{B}}$ は受け入れる.

**Proposition 1** 提案方式は完全である.

*Proof.* 検証式

$$\begin{cases} r = \mathcal{H}(c\|v_1\|v_2\|m\|g^r(\alpha(h_3^c h_4)^e)^s) \\ h_1^{r_1} h_2^{r_2} = \alpha^d m \\ h_{\mathcal{T}}^j = v_1^d A' \\ h_1^j = (\alpha v_2^{-1})^d B' \end{cases}$$

から, 検証式の健全性条件により 4) と同様に証明される. ∎

### 5.2 匿 名 性

匿名性とは次のことをいう.

- もし利用者 $\mathcal{U}$ は電子マネープロトコルに従い, 多重使用をしないならば, たとえ引出プロトコルや支払プロトコルにおいて銀行 $\mathcal{B}$ と店 $\mathcal{S}$ が結託しても利用者 $\mathcal{U}$ に関する情報は何もわからない.

信頼できる第三者機関 $\mathcal{T}$ がプロトコルに従うならば, 4) と同様に証明される.

∎

### 5.3 安 全 性

- 偽造不可能性

偽造をするには次の検証式を満たすように, マネー情報 $M$ を作らなければならない.

$$\begin{cases} r = \mathcal{H}(c\|v_1\|v_2\|m\|g^r(\alpha(h_3^c h_4)^e)^s) \\ h_1^{r_1} h_2^{r_2} = \alpha^d m \\ h_{\mathcal{T}}^j = v_1^d A' \\ h_1^j = (\alpha v_2^{-1})^d B' \end{cases}$$

しかしながら, 検証式を満たすようにマネー情報を生成するには, 銀行の秘密鍵 $x_1$, $x_2$, $x_3$, $x_4$, 信頼できる第三者機関の秘密鍵 $x_{\mathcal{T}}$ を知る必要がある. 銀行の公開鍵 $h_1 = g^{x_1}$, $h_2 = g^{x_2}$, $h_3 = g^{x_3}$, $h_4 = g^{x_4}$ 信頼できる第三者機関の公開鍵 $h_{\mathcal{T}} = g^{x_{\mathcal{T}}}$ との関係から秘密鍵を求めることは離散対数問題を計算することになるため, マネー情報を偽造することは非常に困難である.

| | 通信量 [ビット] | | 時間 [乗算回数] | | | |
|---|---|---|---|---|---|---|
| | | | 引き出し | | 支払い | |
| | 引き出し | 支払い | $\mathcal{U}$ | $\mathcal{B}$ | $\mathcal{U}$ | $\mathcal{S}$ |
| 既存方式 6) | 1664 | 3168 | 2400 | 780 | 0 | 1440 |
| 提案方式 | +80 | +4256 | +480 | 0 | +480 | +960 |

**図 3** 性能評価

- 再利用不可能性
  マネー情報のコピーによる再利用を行うことを考える．同じマネー情報における複数の支払い履歴から，

$$\begin{cases} r_1 - r_1' = u(d - d')y \\ r_2 - r_2' = (d - d')y \end{cases}$$

  より，銀行 $\mathcal{B}$ は利用者 $\mathcal{U}$ の識別情報 $u = (ID_U||ID_M)$ を計算し，ユーザ ID ($ID_U$) を求めることで，多重使用者を特定することができる．

### 5.4 性能評価

効率性の点で既存方式 6) との比較をする．効率性として総通信量（ビット）および，時間（乗算回数）によって比較を行った．$|\cdot|$ をビット長としたとき，$|p| = 1024$, $|q| = 160$, $|u| = 160$, $|c| = 160$ とする．時間（乗算回数）は $|p| = 1024$ ビットを法とする mod 演算の乗算回数を 240 としたときの値である．

## 6. 結　　論

本稿では，発行機関の不正として秘密鍵を知った行員が他の不正な利用者と結託して，電子マネーの偽造を行う問題に注目した．信頼できる第三者機関を仮定することで，銀行は発行したものと還流したものの関連づけをとりつつ，利用者の匿名性を確保できるオフライン電子マネー方式を提案した．

## 参 考 文 献


1) M. Abe and J. Camenisch. Partially Blind Signature Schemes, Proc. of the 1999 Symposium on Cryptogyaphy and Information Security, 1997, SCIS '97 33D.
2) D. Chaum. Security Without Identification: Transaction Systems to Make Big Brother Olsolete, Commnunications of the ACM, Vol. 28 No.10, pages 1030-1044, 1985.
3) N. Ferguson. Single-term off-line coins, Advances in Cryptology - Eurocrypt '93, LNCS 765, pages 318-328, 1994. Springer-Verlag.
4) Y. Frankel, Y. Tsiounis, and M. Yung. Indirect discouse proofs: achieving fair off-line e-cash. In Advances in Cryptology, Proc. of Asiacrypt '96 *(Lecture Notes in Computer Science 1163)*, pages 286-300, Kyongju, South Korea, November 3-7 1996. Springer-Verlag.
5) K. Hirohashi, M. Tada and E. Okamoto. Study on a new e-cash systems using two bline signatures. Proc. of the 1999 Symposium on Cryptogyaphy and Information Security, 1999, SCIS '99 W1-3.1.
6) A. Koide, K.Hirohashi, M. Tada and A. Miyaji. Study on off-line e-cash. Computer Security Symposium '99. pages 111-116.
7) S. Miyazaki and K. Sakurai. Notes on Malicious Insider Attacks in Electronic money Systems. Proc. of the 1999 Symposium on Cryptogyaphy and Information Security, 1999, SCIS '99 W1-3.2.
8) S. Miyazaki and K. Sakurai. Classfication of the Off-line Electronic Money Systems and Evaluation of the Security against Insider Attacks. IPSJ, Vol. 40, No.3 pages 1294-1304.
9) B. Schoenmakers. An efficient electronic payment system with standing parallel attacks, CWI, 1995.