オフライン型電子現金システムの分類と管理機関の内部不正に対する安全性評価

宮崎真悟† 櫻井幸一†

現在提案されている数々のオフライン電子現金方式では，現金発行用の鍵知識や利用者の関連情報といった重大な秘密情報が銀行に一点集結している．そこで今回我々は中央管理される情報，特に利用者の関連情報に焦点を当て，同情報の漏洩や悪質銀行による不正使用に対する既存電子現金システムの安全性を議論する．その指針として，既存の方式を4つの型に分類し，システム管理側の様々な不正やこれらに対する安全性の条件を考察する．

Classification of Off-line Electronic Money Systems and Evaluation of the Security against Insider Attacks

SHINGO MIYAZAKI† and KOUICHI SAKURAI†

In the traditional off-line electronic money systems, a numerous of crucial secret data such as the knowledge of key for issuing money and various information (ID, public key, etc.) related to users are centralized in a bank. So, in this paper, the security of the off-line electronic money against the malicious bank is discussed. As the guide, we classify conventional electronic money systems into four types and examine the condition of security against various insider attacks.

1. はじめに

1.1 Chaum-Fiat-Naor パラダイム

Chaum はブラインド署名を用いて，匿名なオンライン電子現金方式[9]を提案した．この方式では，支払い時に銀行がオンラインで介入し，電子現金の二重使用を検査する．しかしながら，オンラインの検査は，銀行へのアクセス渋滞といった効率性や銀行ホストコンピュータ稼働範囲に限った利用といった問題を持ち，実用的な方式とはいい難い．そこで，Chaum-Fiat-Naor [7]は支払い時に銀行へのアクセスを必要としないオフライン電子現金方式を提案した．提案されているオフライン電子現金方式の多くは同方式に基づくもので，譲渡性[11),23),28)]や分割可能性[8),11),13),27)~29)]，非常時の犯罪捜査[3),10),12),15),16),20),31)]といった機能を拡張している．

数々の方式の基盤となる Chaum-Fiat-Naor 方式では，まず顧客が銀行の預金口座から電子コインを引き出し，これを商店への支払いに当てる．このとき，顧客は銀行や認証機関といった商店以外の機関にアクセスする必要はない（オフライン性）．顧客が電子現金を不正に多重使用した場合，電子現金に埋め込まれている顧客の識別情報が銀行により検出される．顧客が電子現金を通常に使用する限りでは，匿名性が保証される仕組みになっている．本稿では，これを Chaum-Fiat-Naor パラダイムと呼ぶ．

Chaum-Fiat-Naor パラダイムに基づくオフライン電子現金方式では，支払い時のオフライン性と電子現金の二重使用検出の両方を満たすため，利用者の識別情報を電子現金に埋め込んでおく手法がとられている．この識別情報は銀行やその他機関（認証機関，登録機関など）によって管理され，銀行が電子現金を不正に多重使用した利用者を同情報から特定する仕組みになっている．特に，当該利用者と銀行のみがこの識別情報を把握している場合が多い．その秘密性・唯一性が利用者を識別する条件となっている．

1.2 オフライン電子現金方式における不正・攻撃

提案されているほとんどの方式では，銀行またはその他関連機関を信頼できると仮定して，電子現金の偽造や不正な多重使用といった利用者の不正を議論している．これらは電子現金システムとしての最低限の要

† 九州大学大学院システム情報科学研究科情報工学専攻
Graduate School of Information Science and Electrical Engineering, Kyushu University

求に関する議論である．

一方，電子現金方式における必要機能を逆手にとった不正・攻撃法が示されている．たとえば，電子現金の匿名性は利用者のプライバシを保護するための必要機能とされている．von Solms ら[34]は，この電子現金の匿名性を逆手にとったマネーロンダリングやゆすり・強盗といった完全犯罪を提示した．同問題を解決する手法がいくつかの方式[3),10),12),15),16),20),31)]で提案されている．また Jakobsson ら[20]は，悪質な敵が銀行に電子現金発行用の秘密鍵を提示するよう強制したり，特殊な引出プロトコルを実行させる銀行強盗について議論している．しかしながら，これらでは銀行自体には悪意がなく，外部からの敵や不正利用者にどう対処するかを問題としたものである．

これに対し Ferguson[14]は，管理する利用者の秘密鍵を用いて，不正な二重使用の事実を捏造するシステム管理側の銀行の不正について論じている．同方式では，電子現金を正常に使用している利用者は悪質な銀行の不正捏造を摘発することができる．また，Jakobsson ら[19]は不正捏造に対して安全な方式を提案しているが，これは Chaum-Fiat-Naor パラダイムに基づくものではない．

このように Chaum-Fiat-Naor パラダイムに基づく方式では，利用者に関する秘密情報が管理機関によって悪用・不正売買されるといった事象について議論があまりなされていない．

1.3 本稿の目的・指針・提案

電子現金の安全性を評価したものとして中山ら[26]の文献があるが，これは管理機関でなく利用者の不正を論じるものである．それに対し本稿では，これまで議論されなかった管理側の不正に対するオフライン電子現金システムの安全性を評価するものである．

その指針として，まず Chaum-Fiat-Naor パラダイムに基づく従来の提案方式を 4 つの型に分類する．そこでは，銀行や認証機関といった中央管理される利用者情報の種類や管理体系，不正なりすましを行う手間を分類基準とする．これにより，銀行やその他機関の管理情報量や仮定される信頼性の度合を明確にする．また同じ数学的想定に基づく方式間でも，その型によりシステム全体としての安全性に微妙な違いがあることも示す．

さらに，分類を基にシステム管理側の様々な不正に対する各型の安全性を考察する．今回我々は，不正捏造による賠償金超過や偽造証明書発行という新たな 2 つの攻撃法を提案する．前者は，電子現金を通常使用している利用者に二重使用の不正事実を捏造する Ferguson[14]の議論を拡張したものである．そこでは，悪質な銀行が不正な二重使用をした利用者に三重・四重使用の不正事実を捏造して賠償金を倍増することできる．後者は cut-and-choose 法を用いた方式[3),7),28)]に対する攻撃法で，銀行が利用者の許可証を偽造して第三者に売り渡すものである．

最後に，様々な金融機関の内部犯罪・不正に対する既存方式の安全性の比較から，安全な電子現金システムの条件を考察する．

本稿の構成

2 章では，Chaum-Fiat-Naor パラダイムを紹介する．3 章では既存電子現金方式の分類と不正なりすましに対する各型の安全性を議論する．4 章では，悪質な銀行による様々な不正や新たな攻撃法を記す．5 章では 3 章の分類で安全性が高いと評価された方式について，不正・攻撃に対する強度・安全性を議論する．最後に 6 章で，安全な電子現金システムに求められる条件やこれからの課題を記す．

2. Chaum-Fiat-Naor パラダイム

本章では，Chaum-Fiat-Naor パラダイムについて説明する．銀行は公開鍵 $P_{\mathcal{B}}$ に対応する秘密鍵 $S_{\mathcal{B}}$ を持っている．$S_{\mathcal{B}}$ を用いた銀行の署名は，ある金額（w 円）を持つ電子現金に相当する．電子現金の匿名性を満足するため，この署名はブラインド署名プロトコルを通して行われる．また，顧客 $\mathcal{C}$ と商店 $\mathcal{V}$ は銀行にそれぞれ口座を持っており，電子現金システムの利用者である．提案されている電子現金方式の多くはこのパラダイムに基づき，認証機関や匿名通信路を新たに設置したり，犯罪捜査の機能を拡張を計ったりしている．

電子現金システムは，主に以下の 4 つのプロトコルによって構成されている（図 1）．

引き出しプロトコル：

(1) 顧客 $\mathcal{C}$ は自分の識別情報 $S_{\mathcal{C}}$ を用いて，メッセージ $m_{\mathcal{C}}$ を作成する．$\mathcal{C}$ は $S_{\mathcal{C}}$ を示すことなく，$m_{\mathcal{C}}$ を正規の手順で作成したことを銀行に

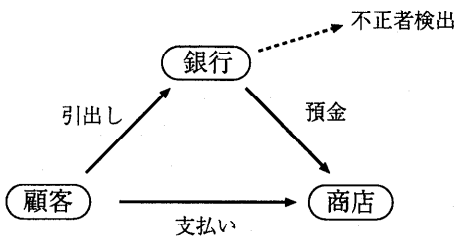


図 1 電子現金の流れと処理
Fig. 1 Flow in electronic money systems.

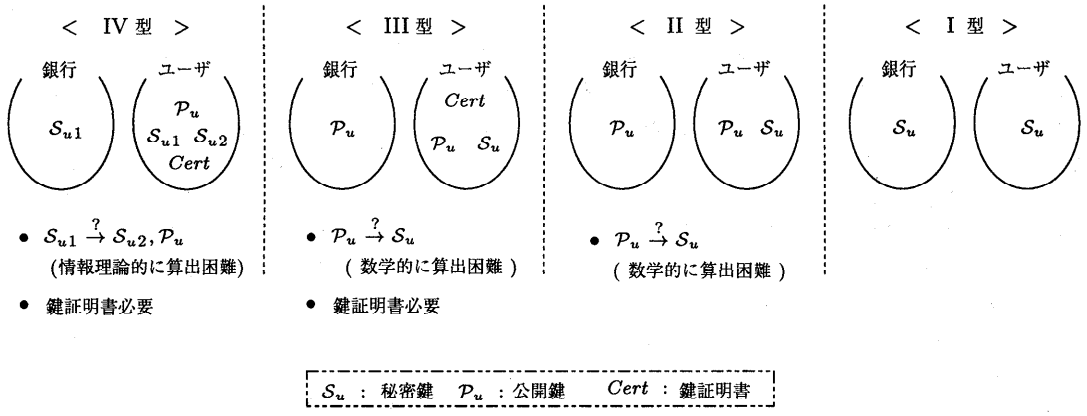


図2 利用者管理情報とその他機関の管理情報
Fig. 2 Information on customers' keys stored in authorities and in customers.

証明する.

(2) 銀行 $\mathcal{B}$ は m_C に対するブラインド署名を生成し, $\mathcal{C}$ の預金口座から w 円減額する.

(3) $\mathcal{C}$ は, m_C に対する銀行の署名 $\sigma_{\mathcal{B}}(m_C)$ を計算する.

支払いプロトコル:

(1) $\mathcal{C}$ は $(m_C, \sigma_{\mathcal{B}}(m_C))$ を商店 $\mathcal{V}$ に送信する.

(2) $\mathcal{V}$ は銀行の署名を検証し, 正当である場合のみ, ランダムな質問情報 $c_{\mathcal{V}}$ を $\mathcal{C}$ に送信する.

(3) U は $c_{\mathcal{V}}$ への応答情報 r_C を $\mathcal{V}$ に返送する.

(4) $\mathcal{V}$ は r_C の正当性を検証する.

預金プロトコル:

(1) $\mathcal{V}$ は $(m_C, \sigma_{\mathcal{B}}(m_C), c_{\mathcal{V}}, r_C)$ を $\mathcal{B}$ に送る.

(2) $\mathcal{B}$ は, 銀行の署名 $(m_C, \sigma_{\mathcal{B}}(m_C))$ の署名と質問応答 $(c_{\mathcal{V}}, r_C)$ の正当性を検証する. $\mathcal{B}$ は $(m_C, \sigma_{\mathcal{B}}(m_C), c_{\mathcal{V}}, r_C)$ をデータベースに保管し, $\mathcal{V}$ の預金口座を w 円増額する.

不正多重使用者検出プロトコル:

(1) 電子現金が不正に多重使用されている場合, $\mathcal{B}$ は異なる2つの使用履歴 $(c_{\mathcal{V}}, r_C)$ と $(c'_{\mathcal{V}}, r'_C)$ から使用者の識別情報 S_C を検出し不正者を特定する.

3. 既存オフライン電子現金方式の分類

3.1 オフライン電子現金システムと秘密鍵

オフライン電子現金システムでは, 支払い時の通信データを基に不正な二重使用者を特定する手法をとっている. その手法として, オフライン方式の発端となったChaumら[7]の方式では, 電子現金を構成するデータを受取人の要求に応じて開示する. 二重使用時にはそこに埋め込まれた識別情報が高い確率で検出される仕組みになっている. 他には, 商店からの質問データに対して署名を施す方式もある. 不正時にはその署名鍵が算出され, 犯人を特定する手法をとっている.

このような識別情報や署名鍵は, 支払い時に電子現金の受取相手からのランダムな質問データに対する応答データ作成に使用される. 本稿では, こういった不正利用者の特定を促す識別情報や署名鍵を "秘密鍵" として議論する. 利用者識別の機能を持つことで, この "秘密鍵" の悪用・漏洩が悪質銀行による不正の捏造や入手した第三者による不正ななりすましを招く.

3.2 従来方式の分類

"秘密鍵" の管理体系や不正の実行難易度を大きな目安として, 従来の方式を以下4つの型☆に分類する (**図2, 表1** を参照).

I型:

識別情報そのものを秘密鍵または電子現金に埋め込む方式. 銀行そのものが同情報を知っているため, 様々な不正・攻撃にさらされやすい.

II型:

秘密鍵は利用者自身で管理し, 公開鍵だけを銀行に預ける方式. 引き出し時, 銀行はこの公開鍵をIDとして電子現金に埋め込む. よって公開鍵に対応する秘密鍵を入手・算出できれば, 当該利用者へのなりすましが可能となる.

III型:

公開鍵をIDとして登録し, これに対する証明書とともに支払いを行ってゆく方式. 当該利用者のなりすましを行うためには, 対応する秘密鍵情報

☆ 方式自体の特性が型を決定している. そのため, ある型に属する方式を別の上位型 (数字の大きい方) に変えるためには, 方式におけるプロトコルを修正する必要がある.

表1 既存オフライン電子現金方式の分類
Table 1 Our classification of previous off-line electronic money systems.

出典	型	保管場所	犯罪捜査機能	備考
[Yac94] [35]	IV	銀行・認証機関	無	対話型ゼロ知識証明
[Bra94] [5]	IV (→ II)	銀行・耐タンパー装置	無	耐タンパー性
[MS98] [24]	IV	登録機関	無	
[FO96] [15]	III$^+$	信頼第三機関（複数）	有り	匿名通信路または分散構造
[OO91] [28]	III	銀行	無	
[EO95] [13]	III	銀行	無	
[Oka95] [27]	III	銀行	無	
[PP97] [31]	III	信頼第三機関	有り	
[MAFN97] [23]	III	登録機関	無	
[Bra93] [4]	II	銀行	無	
[DdC94] [11]	II	公開ファイル	無	非対話型ゼロ知識証明
[BGK95] [3]$-\alpha$	II	銀行	有り	Brands 方式[4]ベース
[CMS96] [10]	II	銀行	有り	
[FTY96] [16]	II	銀行	有り	匿名通信路
[NMV97] [25]	II	銀行	無	
[dST98] [12]	II	銀行	有り	
[Pai92] [30]	I$^+$	銀行	無	
[Fer93] [14]	I$^+$	銀行	無	
[CFN88] [7]	I	銀行	無	
[FY93] [18]	I	銀行	無	
[Sch95] [33]	I	銀行	無	
[BGK95] [3]$-\beta$	I	銀行	有り	Franklin-Yung 方式[17]ベース
[JY96] [20]	III, II, I	銀行	有り	

の入手・算出に加え，証明書の入手・偽造が必要である．

IV 型：

機関に預けられる利用者の識別情報は秘密鍵の一部だけである．秘密鍵を構成するもう一部分や対応する公開鍵，鍵証明書は当該利用者しか知らない・計算できない方式．公開鍵でさえ明かされないことで，完全な秘密鍵を算出する術が困難である．

表1のその他の項目として，“保管場所”は秘密鍵や公開鍵，部分鍵情報といった利用者の識別情報をどの機関に預けるまたは知られているかを示したものである．“犯罪捜査機能”は，誘拐や銀行強盗などの非常時に，電子現金の匿名性を強制的に解除する機能の有無を示したものである．これにより，電子現金の使用者や特定利用者の使用履歴を捜査することができる．

注意： “+”の付いている方式は，同じ型の他の方式に比べ，なりすましといった不正に対してより安全なものである☆．

3.3 管理情報と不正なりすまし

図2に示すように，銀行にはすべての利用者の様々な情報が管理されている．よって，銀行が利用者の関連情報リストを多額の金額で売り渡したり，強力なマシンパワーを持つ団体の攻撃によって同情報が盗まれたりした場合，当該利用者への不正なりすましが発生する危険性がある．

特にI型の方式では秘密鍵そのものが銀行に管理されているため，この状況に直結してしまう．III型やII型の方式では，銀行には公開鍵しか管理されていないので，数学的な難問を解決しなければ利用者の秘密鍵

☆ III$^+$ 型の方式は識別情報と公開鍵の対応づけが難しいため，不正なりすましがより困難な方式である．また I$^+$ 型の方式では，支払い時の質問応答用の秘密鍵とは別に，引き出し時の通信データへの署名を行う鍵が必要である．この署名用鍵は当該利用者しか知らないので，他のI型の方式に比べ，悪質な銀行による陥れや不正なりすましをを行うことが困難である．

は露呈しない．しかし，銀行に悪意がある場合，鍵生成時に影響を及ぼしたり☆，システム変数を巧みに設定して秘密鍵を算出しやすい形に導くかもしれない．

またここで，秘密鍵が選出される空間 Z_q^* において，ある部分的な空間を $A \subset Z_q^*$ とする．今，ある不正者が（地道な線形探索によって）A におけるすべての要素 $x \in A$ と $g^x \pmod p$ の関係を知っている．このとき，II型のようにすべての利用者公開鍵と所有者の関係を一覧できる表が1点に管理されているのとされていないのとでは，利用者の秘密鍵を入手する手間は大きく違う．II型では，管理されたリストを奪取すれば鍵の対応を効率的に検索してゆくことが可能である．これに対し，IV型では利用者と支払いプロトコルを実行したりして公開鍵を地道に入手して鍵関係を比較するといった作業が必要である．

このようにII型は銀行の不正や敵の持つ情報量によって一瞬にしてI型に変化する危険性を持っている．一方，III型の方式で不正になりすましを行うにはさらに鍵証明書を入手・偽造する必要がある．IV型では，秘密鍵の部分情報しか銀行に預けられない．数学的な難問により秘密鍵を導出する公開鍵でさえ与えられないので，他の型に比べてなりすましの必要情報はより入手困難となっている．

4. 悪質な銀行による様々な不正・攻撃

4.1 不正捏造による賠償金請求

支払い時の ElGamal 署名や Okamoto-Schnorr 署名から二重使用者を検出する方式（文献3)〜5), 12)〜14), 24), 25), 33), 35)）では悪質な銀行の不正捏造にさらされる危険性がある．ElGamal 署名を用いた二重使用者検出は，以下のアルゴリズム☆☆に基づいている．今，顧客の秘密鍵を U，引き出し時に顧客の生成した乱数を k，そしてある商店からの質問データを m とする．ある顧客が電子現金を二重使用するとき，銀行は支払い時の署名からなる二次方程式：

$$r_1 = Um_1 + k$$
$$r_2 = Um_2 + k$$

より，U を算出し，使用者を特定する．このとき，悪質な銀行は k を求めることができるので，適当に生成した m_3 と U を使って，$r_3 = Um_3 + k$ なる署名を計算する．この不正捏造した履歴を用いて，電子現金を二重使用した利用者に三重使用の罰金を請求することが可能である．

ここで，このアルゴリズムを使用している Schoenmakers の方式[33]では，銀行が電子現金を通常使用している利用者に対する二重使用の不正捏造を行うことが可能である．I型に属す Schoenmakers 方式では U 自身を最初から銀行は知っている．

Step 1：銀行はある商店と結託し，預金する電子現金をだれから受けとったかを把握する．支払い時の署名を $r = Um + k$ とする（論文と厳密には異なる）．

Step 2：支払い時の署名 r とその顧客の秘密鍵 U から，乱数部分 k を計算する．

Step 3：偽造文書 m' を生成し，計算した k と U を用いて，偽造署名 $r' = Um' + k$ を計算する．

Step 4：当該顧客に (r, r') を提示し，二重使用の罰金を請求する．

ここでは，匿名性を打開するため商店の協力が必要であるが，不正を犯していない利用者にも罪を着せることが可能である．Ferguson[14]は，同攻撃法に対する1つの解決策を提案している．しかしながら，利用者が不正な二重使用を行った場合，銀行の不正捏造による賠償金の超過請求を防ぐことはできない．

4.2 偽造証明書発行

文献 28) では cut-and-choose 法を用いて，電子現金を使用するための許可証を発行する．利用者は内容を乱数によりブラインドした K 個の情報のうち，銀行が適当に選んだ $K/2$ 個（この集合を L とする）に対しその構成データを開示する．$K/2$ 個すべての内容が正当な手順で作成されている場合にのみ，残り $K/2$ 個（この集合を $\tilde{L}$ とする）を合成して銀行は署名を施す．利用者はこの値から乱数を引き抜いたものを許可証として使用する．銀行が不正である場合，廃棄されるべき集合 L を用いて，当該利用者の偽造許可証を作成することが可能である．この処理を以下に簡単に示す（図 **3** 参照）．

利用者 $\mathcal{U}$ は銀行 $\mathcal{B}$ から電子許可証 $B = \{B_i | i \in \tilde{L}\}$ を発行してもらうため以下の処理を行う．利用者 $\mathcal{U}$ の RSA 公開鍵を (e_U, N_U) かつ秘密鍵を d_U，銀行 $\mathcal{B}$ の RSA 公開鍵を (e_B, N_B) かつ秘密鍵を d_B とする．

Step 1：$\mathcal{U}$ は $i = 1, \ldots, K$ に対し，乱数 a_i と Williams 数 N_i を選ぶ．ここで，N_i の素因数 P_i, Q_i は，$P_i = 3 \pmod 8$ かつ $Q_i = 7 \pmod 8$ を満たす．

Step 2：$\mathcal{U}$ は K 個のブラインド値 $W_i (1 \le i \le K)$ を作成し，銀行に送信する．

$$W_i = r_i^{e_B} g(I_i \| N_i) \mod n_B$$

☆ たとえば，莫大な金額を口座に預金するような顧客に対しては，銀行が秘密鍵と公開鍵との関係を把握している空間から鍵を選ぶように利用者に勧めたりするかもしれない．

☆☆ Okamoto-Schnorr 署名を用いた処理もこれに類似している．

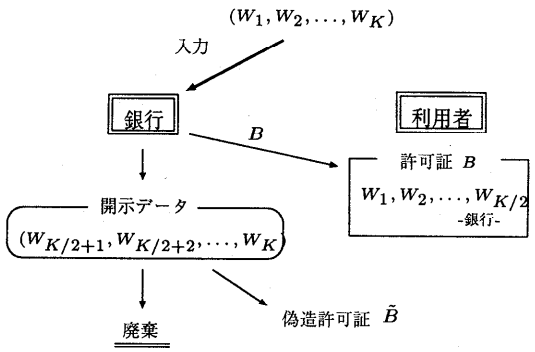


図3 偽造証明書発行
Fig. 3 Forging the certification in the issuing protocol.

ここで，$r_i \in_R Z_{N_B}$ で，g は適当な一方向性ハッシュ関数とする．また，

$$S_i = ID_U \parallel a_i \parallel (g(ID_U \| a_i))^{d_U} \bmod N_U$$
$$= S_{1,i} \parallel S_{2,i}$$
$$I_i = S_{1,i}^2 \bmod N_i \parallel S_{2,i}^2 \bmod N_i$$

とし，$\parallel$ はビット連結（concatenation）を示す．

Step 3：$\mathcal{B}$ は適当に $K/2$ 個（$\in L$）を選び，W_i の開示要求を行う．

Step 4：$\mathcal{U}$ は開示要求された L に属するすべての W_i に対し，これを構成する $(a_i, P_i, Q_i, (g(ID_U \| a_i))^{d_U} \bmod N_U, ID_U, r_i)$ を $\mathcal{B}$ に送信する．

Step 5：$\mathcal{B}$ は開示された L の正当性を検証し，正当な場合は残り $K/2$ 個（$\in \tilde{L}$）に対し，

$$\tilde{W} = \left(\prod_{i \in \tilde{L}} W_i \right)^{d_B} \bmod N_B$$

を計算して $\mathcal{U}$ に送信する．

Step 6：$\mathcal{U}$ は許可証 B を計算する．

$$B = \tilde{W} / \left(\prod_{i \in \tilde{L}} r_i \right)$$
$$= \left(\prod_{i \in \tilde{L}} g(I_i \| N_i) \right)^{d_B} \bmod N_B$$

ここで，開示された L から銀行は利用者 U の偽造証明証 $\tilde{B}$ を発行することができる．

$$\tilde{B} = \left(\prod_{i \in L} g(I_i \| N_i) \right)^{d_B} \bmod N_B$$

銀行は L に属する W_i の構成要素を知っているので，$(a_i, P_i, Q_i, (g(ID_U \| a_i))^{d_U} \bmod N_U, ID_U)$ と偽造証明書 $\tilde{B}$ を対にして売り渡す．偽造証明書を購入した不正者は，当該利用者へのなりすましが可能となる．

この不正は，cut-and-choose 法を用いた方式[7]や文献3)で提案された2つの方式のうちの1つである β 方式（Franklin-Yung 方式ベース）にも適用することができる．これらの方式では偽造証明書ではなく，利用者の ID を埋め込んだ偽造電子現金に相当する．

4.3 商店との結託

文献15)，24)，28)，35)の方式では，顧客は毎回固定の署名鍵・検証鍵・鍵証明書を用いて，商店への支払いを行う．この際，商店☆は相手がだれであるかを管理することができるので，識別情報と検証鍵を関連させることができる．そこで，銀行と商店が結託する場合，銀行は預金されてくる電子現金にある検証鍵から，当該顧客の使用履歴を把握することが可能となる．

このように支払い時に毎回同じ鍵を使用する方式では，商店と銀行の結託により電子現金の匿名性が失われる危険性がある．これに対し文献31)では，利用者が複数の鍵を使い分けることで，電子現金の匿名性を高めている．

5. 安 全 性

5.1 耐タンパー性装置と相互検証

耐タンパー性装置は，利用者が制御できない信頼第三機関と見なすことができる[3]．

Brands[5]の提案した方式では，銀行が利用者に配る装置の耐タンパー性を仮定して方式が構築されている．この装置には利用者を識別する情報 x_{1i} が埋め込んであり，銀行と装置のみが同情報を知っている．他方式と異なるのは，利用者自身が秘密鍵の一部をなす同情報を知ることができない点にある．電子現金引き出しの際，顧客は秘密鍵のもう一部分 x_{0i} をランダムに生成し，装置の保持情報とあわせて，その電子現金に対する顧客秘密鍵 (x_{0i}, x_{1i}) とする．

ここで，銀行が管理する利用者の識別情報 x_{1i} のリストが，敵の手に渡った場合を考える．引き出し時や支払い時，装置本体の正当性が厳密に検証される場合☆☆，敵はリストにある利用者の部分秘密鍵を手に入れてもこれを使用するための正当な装置を持たない．銀行管理情報の漏洩が直接，利用者への被害とならない点では，この方式は IV 型に分類される．

☆ 電子現金の流入量が大きいほど，情報量は大きくなる．大手デパートなど物品流出・電子現金流入の激しい機関ほど効果は大きい．

☆☆ 引き出し時，銀行は引出者の装置に埋め込んだ利用者識別情報の有無を検証するのではなく，装置そのものの正当性検証を行う必要がある．また支払い時も，顧客と商店の間で装置本体の正当性検証を行う．正当な装置でない場合処理は中断される．

ここで，装置そのものを埋め込まれた識別情報の正当性を示す証明書と見なすことができる．よって，装置検証が厳密でない場合，敵は奪取した利用者の部分鍵 x_{1i} を用いて当該利用者になりすますことができる．

引き出し時：正規装置の行う乱数生成を自分で行う．また秘密鍵のもう一部分 x'_{0i} をランダムに生成し，正規の処理を用いて当該利用者 i の口座から電子現金を引き出す．

支払い時：秘密鍵 (x_{1i}, x'_{0i}) を用いて署名を行う．

この場合，銀行管理情報の漏洩が登録された利用者への莫大な被害を引き起こすことから，方式はI型に分類される．

5.2 IV型の安全性

前節にも触れたように，IV型に属するBrands[5]の方式は装置本体の正当性検証を行わない場合，管理リスト漏洩がそのまま被害に直結するI型に分別されることになる．

次に，認証（登録）機関が鍵の証明書を発行する文献24), 35)の二方式について考える．Yacobi[35]の方式では，秘密鍵を構成する利用者の識別情報 $\mathcal{ID}_U$☆を銀行と認証機関の両方が知っている．

ここで悪質な銀行が何らかの経路で，秘密鍵のもう一方を構成する乱数情報 R を入手して秘密鍵を算出した場合を考える．不正なりすましを可能とするためには，$\mathcal{ID}_U$ を含む秘密鍵の証明書を認証機関に発行してもらう必要がある．認証機関が信頼できる場合，認証機関が識別情報を唯一に設定し，乱数と識別情報のビットサイズが異なる☆☆場合のみ証明書を発行することで，不正なりすましを防ぐことができる．

しかしながら，文献24), 35)の両方式において認証機関が悪質である場合，認証機関は自己生成した乱数と保持する利用者の識別情報から秘密鍵を生成し，これに対する証明書を発行することができる．当該利用者の識別情報を含む秘密鍵と対応する証明書を不正売買する場合，I型における銀行の不正と同じ状況に陥ってしまう．ただし認証機関は電子現金の引き出し・預金に関与する銀行と異なり，処理は鍵証明書発行時のみである．そこで，閾値法などを適用して同機関を分散化し，認証機関としての信頼性を高める有効な解決策が考えられる．

☆ 利用者の秘密鍵 S は識別情報 $\mathcal{ID}_U$ と乱数 R のビット連結で構成される（$S = \mathcal{ID}_U \| R$）．

☆☆ 制限がない場合，不正者 $\mathcal{F}$ はある利用者 $\mathcal{T}$ の識別情報 $\mathcal{ID}_\mathcal{T}$ を乱数のように扱い，$S_\mathcal{F} = \mathcal{ID}_\mathcal{F} \| \mathcal{ID}_\mathcal{T}$ に対する証明書を発行してもらうことができる．この場合，引き出し時は $\mathcal{ID}_\mathcal{T}$ を用いて利用者 $\mathcal{T}$ になりすまして電子現金を引き出すことができる．

6. 安全な電子現金システム

不正なりすましや多重使用への陥れは，銀行に管理されている情報が当該利用者の持つ情報にほぼ匹敵することに起因している．つまり，こういった保管情報による不正を防ぐには，利用者が銀行やその他機関に正当なユーザを識別するための最低限の情報のみを与えることが望ましい．数学的に難しいとされる問題を解ければ，秘密鍵を導く公開鍵でさえも直接的に預けない．

預ける知識量はそのままでもなりすまし実行の手間を高めることが可能である．たとえば，証明書を用いて支払いを行うような方式では，証明書を発行する機関を分散させ，発行機関としての信頼性を高めることが考えられる．結託によって偽造証明書を発行する状況をおさえることができるし，引き出しに比べ証明書発行は発生頻度が低いので決済の効率を損なうことはない．不正なりすましを困難にする効果的な手法といえる．

最後に我々は，秘密重要情報を意識した安全な電子現金システムへの一アプローチと検討すべき未解決問題を示す．

(1) 文献20)と本稿のアプローチの合成．銀行の権力分散と利用者情報の分散により，不正な電子現金発行や預託鍵悪用の危険性をおさえる．

(2) 離散対数問題や因数分解問題といった暗号系そのもの（または部分的）の崩壊による方式への被害を最小限に食い止めるため，様々な暗号系を用いて構築する．これにより，一暗号系が破られた場合にも他の暗号系で代替し，正常な運営を持続することができる．

(3) 証明書の変動性．4章で触れたように，証明書を用いた方式では，支払い時に固定鍵と対応する証明書を使用するため，プライバシの侵害に結びつきやすい．また，不正なりすましを行おうとする敵は，当該利用者と一度商取引を行うことで証明書を入手できてしまう．何らかの解決策が課題としてあげられる．

(4) 犯罪捜査機能付きIV型方式の設計．本稿での分類では上位であればあるほど，ユーザ以外の機関への情報量は低くなる．最小限度の情報しか他機関に与えないIV型は，機関に預託されたできる限りのユーザ情報を連結し強制的捜査を実行する機能とは方向性を異にするものである．しかしながら，犯罪捜査機能は実用的方式に必要な要素と考えられる．必要最小限の情報

で同機能を果たすような技術・方式の設計が今後の課題となっている．

このように，システム管理者側の不正や情報漏洩といった仮定の裏側に隠蔽されていた事実を掘り出し議論することが，これからの電子現金実用化に向けて必要である．

参考文献

1) Bank for Internatinal Settlements: *Risk management for electronic banking and electronic money activities*, Basle Committee on Banking Supervision, No.35 (Mar. 1998). http://www.bis.org/publ/index.htm
2) Bank for Internatinal Settlements: *Security of electronic money*, Committee on Payment and Settlement Systems, No.18 (Aug. 1996). http://www.bis.org/publ/index.htm
3) Brickell, E., Gemmell, P. and Kravitz, D.: Trustee-based tracing extensions to anonymous cash and the making of anonymous change, *6th Annual ACM-SIAM Symposium on Discrete Algorithms*, pp.457–466 (1995).
4) Brands, S.: Untraceable off-line cash in wallet with observers, *Advances in Cryptology – CRYPTO '93*, LNCS 773, pp.302–318 (1993).
5) Brands, S.: Off-Line Electronic Cash Based on Secret-Key Certificates, *Proc. 2nd International Symposium of Latin American Theoretical Informatics* (1995). http://www.cwi.nl/cwi/publications/
6) Chan, A., Frankel, Y., MacKenzie, P. and Tsiounis, Y.: Mis-representation of identities in e-cash schemes and how to prevent it, *Advances in Cryptology – ASIACRYPT '96*, LNCS 1163, pp.276–285 (1996).
7) Chaum, D., Fiat, A. and Naor, M.: Untraceable Electronic Cash, *Advances in Cryptology – CRYPTO '88*, pp.319–327 (1988).
8) Chan, A., Frankel, Y. and Tsiounis, Y.: Easy come – easy go divisible cash, *Advances in Cryptology – EUROCRYPT '98*, LNCS 1403, pp.561–575 (1998).
9) Chaum, D.: Blind Signature for Untraceable Payments, *Proc. Crypto '82*, pp.199–203, Plenum Press (1983).
10) Camenisch, J., Maurer, U. and Stadler, M.: Digital payment systems with passive anonymity-revoking trustees, *Computer Security – ESORICS 96*, LNCS 1146, pp.33–43 (1996).
11) D'Amiano, S. and di Crescenzo, G.: Methodlogy for digital money based on general cryptographic tools, *Advances in Cryptology – EUROCRYPTO '94*, LNCS 950, pp.156–170 (1994).
12) de Solages, A. and Traoré, J.: An efficient fair off-line electronic cash system, *Financial Cryptography '98*, LNCS 1465 (1998).
13) Eng, T. and Okamoto, T.: Single-term divisible electric coins, *Advances in Cryptology – EUROCRYPT '95*, LNCS 950, pp.306–319 (1995).
14) Ferguson, N.: Single term off-line coins, *Advances in Cryptology – EUROCRYPT '93*, LNCS 765, pp.319–328 (1993).
15) Fujisaki, E. and Okamoto, T.: Practical escrow cash systems, *Security Protocols*, LNCS 1189, pp.33–48 (1996).
16) Frankel, Y., Tsiounis, Y. and Yung, M.: Indirect discourse proofs: achieving efficient fair off-line e-cash, *Advances in Cryptology – ASIACRYPT '96*, LNCS 1163, pp.286–300 (1996).
17) Franklin, M. and Yung, M.: Towards provably secure efficient electronic cash, Columbia Univ. Dept. of C.S. TR CUCS-018-92 (1992).
18) Franklin, M. and Yung, M.: Secure and efficient off-line digital money, *Proc. ICALP '93*, LNCS 700, pp.265–276 (1993).
19) Jakobsson, M. and M'Raihi, D.: Mix-based electronic payments, *SAC '98* (1998).
20) Jakobsson, M. and Yung, M.: Revokable and versatile electronic money, *3rd ACM Conference on Computer and Communications Security*, pp.76–87 (1996).
21) Jakobsson, M. and Yung, M.: Applying anti-trust policies to increase trust in a versatile e-money system, *Financial Cryptography*, LNCS 1318, pp.217–238 (1997).
22) Lelieveldt, S.L.: Evaluating the security of electronic money, *Financial Cryptography*, LNCS 1318, pp.91–94 (1997).
23) Moribatake, H., Abe, M., Fujisaki, E. and Nakayama, Y.: Electronic cash scheme, *Proc. 1997 Symposium on Cryptography and Information Security*, SCIS97-3C (1997).
24) Miyazaki, S. and Sakurai, K.: A more efficient untraceable e-cash system with partially blind signatures based on the discrete logarithm problem, *Financial Cryptography*, LNCS 1465 (1998).
25) Nguyen, K.Q., Mu, Y. and Varadharajan, V.: A new digital cash scheme based on blind Nyberg-Rueppel digital signature, *Information Security*, LNCS 1396, pp.313–320 (1997).
26) 中山靖司，太田和夫，松本 勉：電子現金の安全性評価について，SCIS'98-3.1.A (1998).
27) Okamoto, T.: An efficient divisible elec-

tronic cash scheme, *Advances in Cryptology – CRYPTO '95*, LNCS 963, pp.438–451 (1995).
28) Okamoto, T. and Ohta, K.: Universal electronic cash, *Advances in Cryptology – CRYPTO '91*, LNCS 576, pp.324–337 (1991).
29) Okamoto, T. and Yung, M.: Lower bounds on term-based divisible cash systems, *Public Key Cryptography*, LNCS 1431, pp.72–82 (1998).
30) Pailles, J.C.: New protocols for electronic money, *Advances in Cryptology – AUSCRYPT '92*, LNCS 718, pp.263–274 (1992).
31) Petersen, H. and Poupard, G.: Efficient scalable fair cash with off-line extortion prevention, *Proc. ICICS '97*, LNCS 1334, pp.463–477 (1997).
32) Pfitzmann, B., Shunter, M. and Waidner, M.: How to break another "provably secure" payment system, *Advances in Cryptology – EUROCRYPT '95*, LNCS 921, pp.121–132 (1995).
33) Schoenmakers, B.: An efficient electronic payment system with standing parallel attacks, Technical report, CWI (1995). http://www.cwi.nl/cwi/publications/
34) von Solms, S. and Naccache, D.: On blind signatures and perfect crimes, *Computer and Security*, Vol.11, No.6, pp.581–583 (1992).
35) Yacobi, Y.: Efficient electronic money, *Advances in Cryptology – ASIACRYPT '94*, LNCS 917, pp.153–163 (1994).

付　　録

A.1 従来方式への所見

[FO96][15] **– III$^+$ 型**

この方式ではIII型の他方式と異なり，利用者情報と公開鍵情報を関連させて保管しない．手法は2つ提案されており，1つは匿名通信路を用いて，利用者情報を管理する機関と公開鍵を管理する機関が別々になっている．この場合，公開鍵リストを得たにしても所有者の情報がないので，なりすましといった不正を行うことができない．所有者情報を入手するためには，複数存在する信頼第三機関すべての協力が必要となる．

もう1つは公開鍵を複数に分割し，その部分情報を各機関に利用者情報と連結させて寄託する手法である．この場合，ある1つの機関の管理リストを入手しても，利用者情報と関連させて保管されてある情報は公開鍵の部分的情報だけである．よって，上と同様にすべての信頼第三機関の協力が必要となる．このように，公開鍵が利用者情報と関連させて管理されてある他のIII型の方式に比べ，公開鍵から秘密鍵を算出して当該利用者へのなりすましを行う不正に対して安全性の高い方式といえる．

[PP97][31] **– III型**

利用者は仮名に対応する秘密鍵 $\mathcal{S}_U$ と公開鍵 $\mathcal{P}_U$ を生成し，信頼第三機関に $\mathcal{P}_U$ に対応する証明書を発行してもらう．よって，信頼できる第三機関のみが利用者と仮名との関係を把握している．支払い時，利用者はこの仮名を使って質問応答プロトコルを行う．しかし，仮名と利用者との関係が明らかになったとき，銀行は預金時に入手する同情報から引出者を特定することが可能である．このとき，預金される電子現金から流通履歴がすべて把握され，顧客のプライバシが侵されてしまう．そこで，この方式では顧客は複数の仮名を保持し異なる仮名を使い分ける☆．これにより，一部の仮名からの履歴露呈を最小限にし，プライバシの保護を強化することができる．

[DdC94][11] **– II型**

この方式では，電子コインのサイズが増加しない譲渡可能な電子現金方式が提案されている．そこでは，銀行の署名を施した電子コインのみが転々と流通してゆき，支払人の署名（支払い履歴）は各受取人側で保管する手法をとっている．二重使用を検知した際，銀行は公開ファイルにその電子コイン情報を提示し，これを受け取ったすべての受取人に支払い履歴の提出を促す．提示された流通履歴から二重使用者を検出する仕組みをとっている．預金されるまでの譲渡回数によらず，電子コインのサイズが一定である点では効果的な手法といえる．

しかしながら，支払い履歴を各利用者で保管する分，利用者における負担が大きくなり，また以下のような問題も生じてくる．Pfitzmann ら[32]の言及に対し，D'Amiano ら[11]は，対象の電子現金を使用したすべての利用者から履歴を回収して，完全に復元した流通履歴より二重使用者を検出する，と述べている．

ここで，二重使用の検出処理の際，支払い履歴を提示できない利用者がいて電子現金の流通経路が回復できない状況を考える．そこで検出処理が中止されるのであれば，わざと履歴を提示しない利用者が考えられる．逆に履歴を提示できない利用

☆ 商店・銀行との結託などにより，顧客と仮名との関係が明らかになっている場合を考える．このとき，顧客は他の支払いに別の仮名を使用すればその仮名による電子現金の匿名性は保持される．

者にすべての罪を着せるのであれば，犯人が適当な受取人へのクラッキングにより，罪をなすりつける状況も考えられる．また利用者が支払い履歴を紛失してしまう状況はおおいに考えられる．支払い履歴は各自，安全な情報金庫または（複数の）サービス機関に預けておくことが望ましい．

支払人の署名に対して，受取人は正当な検証鍵を事前に入手しておくか，オンラインで公開ファイルにアクセスする必要がある．公開ファイルにアクセスできないことや公開ファイルそのものをダウンロードするコストを考えると，オフラインで鍵認証を与える証明書による認証方式が効果的である．

[BGK95] [3] – III型 & II型

文献3)では，二重使用者の検出に用いられる利用者の識別情報とは別に，政府が電子現金の強制的な使用履歴調査に用いる利用者の秘密情報を設定している．裁判所の許可のもと，政府は同情報を用いて強制的に電子現金の匿名性を解除し，当該利用者の使用履歴を調査する．また同情報は，複数の信頼できる機関によって分割保管されている．本稿では，二重使用者検出に用いられる秘密情報を秘密鍵として型分別を行うもので，強制的履歴調査に用いられる秘密情報は別としている．強制調査用の秘密情報を（分散）寄託することは，少なくともユーザのプライバシを損なう方向にある．

[Pai92] [30] – I^+ 型

この方式では，cut-and-choose法を用いて利用者の識別情報 id_U が電子現金に埋め込まれているかを銀行が検査する．id_U は銀行と利用者のみが知る情報で，不正な二重使用が行われると同情報が検出され犯人が特定される．銀行が id_U を直接知る点では他の型と変わらないが，引き出しの際，ユーザは銀行に転送する K 個すべてのデータに対して署名を施す．この署名用の秘密鍵はユーザのみが知る情報となっており，不正なりすましを行うには同情報が必要となる．つまり銀行データベースに保管されている id_U を不正使用するには，さらに署名用秘密鍵を入手する必要がある．この分，他のI型の方式よりも安全性は高いと評価できる．

[Fer93] [14] – I^+ 型

文献14)では，銀行が正当ユーザを不正な二重使用の事実を捏造する不正について議論を行っている．型としてはI型に分類するが，論じられている銀行の不正捏造を防ぐ手段を適用すると，他のI型の方式よりも不正なりすましに対して高い安全性を持つ．そのため，I^+ 型として分類している．

手法として，まず，秘密鍵 U の構成を $U =$ (識別情報 $\|$ コイン番号) とすることで，U が電子コインごとに異なるようにする．次に引き出し時に，利用者は通信されるデータに対し署名を施し，銀行に転送する．この署名用鍵は本稿で論議した質問応答用の鍵とは異なるもので，電子現金システムと独立に設定することができる．銀行が利用者の二重使用を訴える場合，算出される U からコイン番号を抜き出し，この電子コインを発行した引き出しプロトコルを検索する．そこで利用者が通信データに対して行った署名を証拠として罰金を請求する．このとき，銀行は利用者の署名鍵を知らないので，悪質銀行による不正な二重使用の捏造は，証拠不十分により不可能となっている．この署名鍵の導入は不正捏造を防ぐことと同時に，不正なりすましに対する安全性の強度を増す機能もある．同情報を知らない不正者が不正なりすましを行うと必ず証拠が残ってしまうのである☆．しかし，利用者・銀行双方でそれぞれ引き出し時の通信データを保管しておく必要がある点において両者への負荷が大きい．

[JY96] [20] – III, II, I型

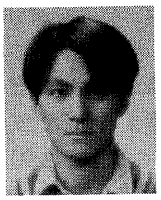
この方式がどの型に属するかは，引き出し時に行う個人認証方式による．論文には引き出し時，銀行に送るセッション鍵 K_B を用いて個人認証を行うと記述してある．今，敵が銀行に管理されている識別情報 id を入手できる環境にあるとする．ここで，K_B に関する知識保持が利用者の個人認証を与えるものとすると，以下のような状況が考えられる．1つは，口座開設時に銀行からセッション鍵を与えられ，これを利用者・銀行の共通情報として個人認証を行う場合である．引き出しの際，銀行が暗号化されたセッション鍵を復号し，これが登録時に発行した当該利用者の鍵であれば，本

☆ たとえば，不正者 X が銀行から不正取引により，ある利用者 A の識別情報を手に入れたとする．ここで，署名鍵を知らない X がある日時 D に A になりすまして口座から電子現金を引き出す場合を考える．通帳を見て不思議に思った A は，その日時 D に行われた電子現金の引き出しプロトコルのログ（通信データとそれへの署名）の開示を銀行に要請する．そこでは，正当な A の鍵による署名がなされていないので，A は銀行に不正な口座引き落としの責任を問うことが可能である．ここで，銀行はログを見せないわけにはいかないので，不正取引した X に A の口座からの引き落としを許した場合の証拠は必ず残る．

人と見なす．この場合，K_B は id と関連させて管理されるため，敵は銀行の管理する (id, K_B) を入手することで，当該利用者へのなりすましが可能となる．これは，管理情報そのものがなりすましへと直結する（**I型**）に等しい．

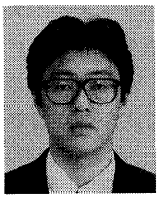
他には，公の公開鍵リストに記載されている銀行・利用者の公開鍵を利用する方法もある．1つは，銀行がリストにある利用者の公開鍵と自分の秘密鍵から Diffie-Hellman 型の K_B を計算し，送られてきたセッション鍵に一致するかどうかで認証を行う方法がある．または，質問応答プロトコルで，リストにある当該利用者の公開鍵を用いて，その署名を検証する方法もある．これらの場合，敵がリストの公開鍵に対応する利用者の秘密鍵を入手・算出できた段階で，当該利用者へのなりすましが可能となる．これは，II型の方式と等価である．リストに管理されているのはなく，認証機関などの証明書を用いて個人認証を行う場合，III型の方式として分類することができる．この場合，敵は対応する証明書を入手する必要がある．

(平成10年10月16日受付)
(平成10年12月 7 日採録)



宮崎 真悟

平成9年九州大学工学部情報工学科卒業．現在，同大学院システム情報科学研究科修士課程2年．暗号理論，情報セキュリティの研究に従事．平成9年度電子情報通信学会学術奨励賞受賞．電子情報通信学会会員．



櫻井 幸一（正会員）

昭和61年九州大学理学部数学科卒業．昭和63年同大学院工学研究科応用物理専攻修了．同年三菱電機（株）入社．現在，九州大学大学院システム情報科学研究科助教授．平成9年9月より1年間コロンビア大学計算機科学科客員として在籍．計算複雑性理論，暗号理論，情報セキュリティの研究に従事．「暗号理論の基礎」（平8年共立出版，監訳），「数論アルゴリズムと楕円暗号理論入門」（平成9年シュプリンガー東京，訳），工学博士．電子情報通信学会，日本数学会各会員．