論　文

2重使用を効率的に検出できる電子決済システム

光岡　　円[†*]　　山本　博資[†]

Electronic Payment Systems to Detect Duplicated Cash Efficiently

Madoka MITSUOKA[†*] and Hirosuke YAMAMOTO[†]

あらまし　現在提案されている匿名性をもつ電子決済システムの多くにおいては，現金データの不正な2重使用を検出するために，使用済の電子現金を銀行がデータベースに保存する必要がある．特にインターネットのような大規模な広域ネットワークにおいて，このようなデータベースの運用は多大なコストを要することになる．本論文では，この問題を解決するために，大規模なデータベースですべての使用済現金を検索する必要がなく，効率的に2重使用の不正を防止できる電子決済プロトコルを提案する．

キーワード　電子現金，電子決済，供託，ブラインド署名

1. まえがき

インターネットの爆発的な普及に伴い，ディジタル情報の通信のみで支払いを行う電子決済システムの確立がその商業利用のために急務となっている．

決済とは買い手と売り手の取引に伴い最終的に買い手の口座から売り手の口座に取引額が移動することである．決済に求められる条件としては，偽造不可能性，匿名性，2重使用不可能性の3点があげられる．

偽造不可能性については，銀行にしか生成できないディジタル情報である銀行のディジタル署名を「現金」とみなすことで実現できる．

また，ネットワーク上で一般消費者が利用する電子決済システムにおいては，銀行などの決済機関が消費活動を完全に把握することが極めて容易であるため，そのようなシステムは匿名性をもつべきだという意見が強い．匿名性は，消費者が得る署名と銀行が得る情報との対応が付けられない署名方式であるブラインド署名 [3] を用いて実現される．

ディジタル情報で表現された「現金」は原理的にコピーと本物の区別が無いため，支払い又は預金の時点で2重使用を防止する必要がある（2重使用不可能性）．基本的には，一度支払いに使われて銀行に戻ってきたデータを銀行のデータベースにすべて登録しておくことにより，既に使用されたデータでないか検索することで2重使用の判定が可能となる．しかし，そのようなデータベースは巨大な記憶容量が必要であり，しかもインターネットのような広域ネットワークでは，全世界に分散した支店の情報を一つに集めてデータを集中管理する必要がある．そのため，一般消費者レベルにまで電子決済システムが普及したとき，そのコストは莫大なものになると予想される．しかし，現在提案されているほとんどのシステムはそうしたデータベースを前提としている．

本論文では，匿名性をできる限り保証しながら，大規模データベースですべての使用済現金を検索する必要のない電子決済システムを提案する．基本となるアイデアは文献 [7], [9] などで用いられている「現金に通し番号を付け，その順番にのみ預金を受け入れる」という方式である．従来のシステムではこの方式を，買い手単位に適用する買い手依存形の手法が用いられていたが，本論文ではより匿名性の高い買い手依存形の手法に加えて，売り手単位に適用する売り手依存形の手法も取り上げている．これら二つの基本的な手法を用いて，支払時に銀行が関与するオンライン電子決済と関与しないオフライン電子決済を実現するプロトコルを構成する．更に文献 [8] の供託ブラインド署名を用いて，信頼できる第三者を前提とする供託電子決済システムのプロトコルも構成する．

文献 [7], [9] の方式は，利用者が銀行に対して匿名口座を開設しなければならず，また文献 [8] は電子現金

[†] 東京大学工学系研究科，東京都
School of Engineering, The University of Tokyo, 7–3–1 Hohngo, Bunkyo-ku, Tokyo, 113–8656 Japan
[*] 現在，（株）富士通研究所パーソナルシステム研究所

のデータベースをすべて保持しなければならない欠点がある．これに対して提案方式では，現金の引き出し時に銀行が利用者を特定していてもなお匿名性が保証され，データベースサイズは，買い手（又は売り手）数のオーダに削減できる特長がある．

2. と **3.** で，それぞれ電子決済システムの分類と電子決済システムで用いることのできるブラインド署名を紹介した後，**4.** で買い手依存形及び売り手依存形の新たな電子決済システムを提案する．**5.** で従来提案されている電子決済システムとの比較を行い，提案システムの特長を明らかにする．

2. 電子決済システムの分類

2.1 電子決済の枠組

電子決済システムへの参加者として，銀行，買い手，売り手の三者を考える．買い手と売り手はそれぞれ銀行に口座をもっている．

クレジットカードや小切手といった決済手段は，ネットワーク上でもディジタル署名を用いることで実現できる．だがクレジットカード会社や銀行に個々の消費者の消費活動の情報を完全に収集される可能性があり，特に本格的ネットワーク社会では個人のプライバシーを侵害される重大な危機を招く恐れがある．

そこで，かなりの匿名性を有する現金による決済を，ネットワーク上における電子決済で実現する電子現金プロトコルが近年盛んに研究されている．電子現金による決済では，基本的に引き出し（買い手が銀行から現金を引き出す），支払い（買い手が売り手に現金を支払う），預金（売り手が銀行に預金する）の 3 種類のプロトコルで構成される．

2.2 オンライン電子現金

支払いの匿名性を実現するためには，ブラインド署名と呼ばれる署名法が用いられる．これは，署名発行時に署名の依頼者である買い手が銀行に送るすべての情報にランダム要素を付加することで，買い手が得る署名と銀行が得る情報との対応が付けられない署名方式である．

しかし，ディジタル署名はディジタル情報であるためコピーして複数回の支払いに用いることが可能である．それを防ぐためには，売り手が支払いを受け入れる前に銀行のデータベースに問い合わせ，2 重使用のチェックをしてから取引を完了する方式を用いればよい．この場合，支払い時に買い手と売り手だけでなく銀行も関与することから，オンライン電子現金と呼ばれる．

このシステムでは，データベースのサイズは基本的に全システムの通算支払数の定数倍になる（ただし，現金の有効期限を設けることである程度は削減できる）．かつオンラインで売り手の問い合わせに対応できるだけの検索速度が要求されるため，そのようなデータベースのコストは莫大なものになると予想される．

2.3 オフライン電子現金

オンライン電子現金における 2 重使用防止策は，データベース検索や問い合わせの通信などへの多大な負荷をもたらす．そこで，支払いプロトコルに銀行が関与せず買い手と売り手の間のみの通信で実行できるオフライン電子現金が求められる．

オフラインでの 2 重使用防止策として，買い手と売り手との取引が完了してから時間が経過した預金時に行われる 2 重使用の検出において，不正が生じた際に限り匿名性が破れ不正者の身元が露見するシステムを，ディジタル情報の通信のみにより巧みに実現するプロトコル [4] が提案されている．以来，その枠組で，計算・通信における効率性改善 [2] や，現金の分割使用の実現 [15] などさまざまな研究が進められている．

しかし，データベースのコストの問題は，2 重使用の検索がオフライン環境下で行える点以外はオンライン電子現金と全く変わっていない．

2.4 供託電子現金

ブラインド署名により匿名性が保証された電子決済法において，マネーローンダリングや誘拐時の身代金の要求に利用されるなど，追跡不能性が悪用される恐れのあることが指摘されている．

そのため，電子現金発行時に，銀行だけでは追跡が不可能であるが，信頼できる第三者機関である受託者と銀行が協力することによって任意の電子現金を追跡できる供託機能を有する電子現金に関する研究 [8], [11] が近年進められている．

受託者と銀行の協力における電子現金の追跡には，買い手と銀行との間の引き出しプロトコルを通して銀行が得る情報から，買い手の得た署名（電子現金）を特定すること（引き出し情報 → 電子現金）と，売り手と銀行との間の預金プロトコルを通して銀行が得る情報から，預金された電子現金を誰が引き出したのか特定すること（電子現金 → 引き出し情報）の 2 種類が要求される．このうち後者の追跡を行うことによって，2 重使用された電子現金データから不正者の身元検出が可能となる．

つまり供託機能を有する電子現金では，2 重使用された事実の検出さえ行えれば，受託者と協力して不正者の身元判定が行える．しかし，データベース検索の問題については供託機能を有さないものと同様である．

2.5 オブザーバを利用するオフライン電子現金

不正にコピーされた電子現金データの使用を，銀行が関与しないオフライン環境下で，取引が成立する前に防ぐ方法として，耐タンパ性をもつデバイス（秘密情報へのアクセスが不可能なことが物理的に保証された IC カードなど）を利用して 2 重使用を防止する方式 [2] が提案されている．

この耐タンパ性をもつデバイスは特にオブザーバ [5] と呼ばれ，銀行が口座保持者に対してあらかじめ発行しておく．オブザーバの協力無しでは正当な支払いを行えないようにシステムを構成することで，支払いの事前の 2 重使用の防止を実現している．

しかし，現在の技術水準では，ディジタル署名を偽造するなどの暗号理論で困難とされている問題を解かなければならない不正にくらべ，IC カードの秘密情報の読み出しや書き換えなどのハードウェア的な不正はより容易であると考えられている．そのため, [2] ではオブザーバの耐タンパ性が破られても，預金時での 2 重使用者の検出も行えるという 2 段構えの防御策が実現されている．

3. ディジタル署名方式

3.1 ブラインド署名

銀行が発行する電子現金データは，一つ一つの電子現金データを識別するための番号に対して銀行がディジタル署名を施したものである．支払いに用いられた電子現金データは，預金時に銀行へ戻ってくる．銀行が使用済みの番号をデータベースに登録しておき，それらと新しく預金される番号を照合することで 2 重使用を検出する．

決済の匿名性を実現するためには，銀行と電子現金の使用者の間でブラインド署名を行う必要がある．ブラインド署名は，メッセージ m を保有する依頼者が，署名者との対話プロトコルにより，署名者の公開鍵で検証できる署名 $S(m)$ を得る署名方式であり，署名者がプロトコル実行の結果依頼者から得る情報と，依頼者の得る署名 $S(m)$ との対応を付けることは署名者には不可能である．

Chaum によって，RSA 署名に対するブラインド署名方式 [3] が提案された．更に，離散対数問題の困難さに基づく Schnorr 署名 [16] に対するブラインド署名方式 [13], [14] が提案されている．本論文のプロトコルでは，供託を行わないシステムではどの署名方式に基づくブラインド署名でも利用できるが，オブザーバを用いるプロトコルや供託機能をもつプロトコルで用いるブラインド署名への拡張は Schnorr 署名に基づくプロトコルが便利である．論文の自己完結性をよくするために，そのプロトコルを**付録**で述べる．

3.2 供託ブラインド署名

供託機能をもつブラインド署名を構成するためには，署名者に送るブラインド化した変数と実際に依頼者が得る署名との対応を表す情報を，信頼できる第三者機関である受託者と銀行が協力したときのみ求められるようにすればよい．

つまり，供託ブラインド署名実行時に供出される（銀行又は受託者が保持する）情報を T とすると，依頼者が得る署名 S との対応が受託者のみに付けられればよい．つまり，T から S に関連付けられた情報を求めることと，S から T に関連付けられた情報を求めることが受託者のみに可能となるプロトコルを構成すればよいことになる．

この供託ブラインド署名を公開鍵証明書の発行に用いることで，電子現金の 2 重使用者を検出するシステムを実現できる．電子現金使用者の公開鍵に対する銀行の署名を公開鍵証明書とする．支払いの際に，使用者が支払金額に対しこの公開鍵でディジタル署名を行い，公開鍵証明書を署名に添付することにより，銀行が確認した人物の署名であることが誰にでも検証できる．ブラインド署名の性質により，銀行は証明書発行時に得る情報と公開鍵証明書の対応を付けることはできない．これは，銀行から匿名 ID（身元保証はされているが，特定の個人とは対応付けられない）を発行してもらう手続きとみなせる．

使用者の実際の身元に対応する ID 情報を署名実行時に供出すれば，支払が不正に行われた場合，銀行と受託者の協力により不正者の ID を検出することができる．

本論文では, [8] で提案されている，署名時に一切受託者が関与する必要の無い供託ブラインド署名を用いる．これは Schnorr 署名に基づくブラインド署名を拡張したものである（具体的なプロトコルは**付録**に示す）．

4. 2重使用を効率的に検出できる電子決済

4.1 2重使用を効率的に検出する方法

現在研究されている電子現金システムの枠組では，2重使用検出のためのデータベースのサイズは，システム内の通算の全取引数の規模にまで巨大化する．

預金を受け入れる順番の通し番号を現金データの署名されたメッセージに含めておき，その順番にしか預金を受け付けないようにすれば，2重使用の検出のためにすべての使用済データを検索する必要はなくなる．しかも記憶しておく必要があるのは最近に預金された現金データの通し番号のみで，使用済データを捨てていくことが可能である．つまり，現在銀行のデータベースに登録されている番号より大きい番号をもつ現金のみ預金を受け付け，登録番号以下なら拒否する．

しかし，分散ネットワーク上を流通するすべての現金データに統一した通し番号を付け，その順番にしか預金を受け付けないとすることは当然不可能である．そこで本論文では，預金を行う売り手ごとに通し番号を付ける売り手依存形，銀行から引き出しを行うそれぞれの買い手ごとに通し番号を付ける買い手依存形の二つの通し番号の管理法を適用した電子決済プロトコルを提案する．

4.2 売り手依存形オンライン電子決済

売り手がすべての取引に通し番号を付けておき，その番号を買い手に示し，それに対する銀行の署名をオンラインでブラインド発行してもらうことにより，売り手は通し番号順にその番号の署名（電子現金）を手に入れることができ，番号順に銀行に預金することが可能になる．

【引き出し・支払い】

（1） **売り手**：$m = (SID \parallel n)$ を買い手に送る（$\parallel$ は連結を表す）．ここで，SID は売り手の ID，n は売り手が取引に付ける通し番号である．

（2） **買い手**：銀行との間で m に対するブラインド署名プロトコルを実行し，支払い金額に対応した銀行の公開鍵で検証できる m についての署名 $S_B(m)$ を得る．

（3） **銀行**：買い手の口座から支払い金額分を差し引く．

（4） **買い手**：$S_B(m)$ を売り手に送る．

（5） **売り手**：$S_B(m)$ を確認し，正当であれば買い手の支払いを受け入れる．通し番号 n を 1 増加させる．

【預金】

（1） **売り手**：$S_B(m)$ と m を銀行に送る（通し番号順に処理）．

（2） **銀行**：売り手の口座に一番最近に預金された現金データの通し番号より，m に含まれる通し番号 n が大きいことを確認する．更に $S_B(m)$ の正当性を確認し，売り手の口座を所定金額増やす（End.）．

このプロトコルにおいては，銀行は売り手の口座ごとに最近に預金された現金データの通し番号を記憶するだけでよいので，データベースのサイズは各銀行が自分の所に口座を開いている売り手の数の定数倍に抑えられる．また，地理的に離れた銀行の支店間でデータベースを共有する必要もなく，分散化が可能である利点を有する．

問題点は，引き出しと支払いの時刻が非常に近いことから銀行と売り手の結託（売り手が取引の成立した時刻を銀行に教える）により匿名性がオンライン電子現金に比べ弱まることである．しかし，クレジットカードなどでは銀行が得る情報だけで匿名性が破られるのに対し，この枠組では売り手が情報を漏らさない限り，銀行が得る情報だけでは電子現金の追跡は不可能である．

4.3 買い手依存形オンライン電子決済

銀行が各ユーザの口座とともに，支払いの順番を表す通し番号を保持しておき，預金時に支払いを行ったユーザの通し番号を参照してその順番にのみ預金を受け入れることにすれば，2重使用の防止は実現できる．更に匿名性を導入するには，実際のユーザの ID の代わりに，ブラインド発行された公開鍵証明書を匿名 ID として用いればよい．この方針に基づき，オンライン電子決済プロトコルを構築する．

匿名 ID のもとでの支払い回数を，対応する公開鍵で検証できるよう署名して売り手に送れば，その回数が銀行のデータベースの匿名 ID のフィールドに登録されている支払い回数より大きいかを問い合わせることで，支払いの正当性を検証できる．

このプロトコルでは，まとまった金額の商品券という形で口座から現金を引きだし，プリペイドカードのように任意の金額に分割して用いることができる．

【公開鍵証明書の取得】

（1） **買い手**：秘密鍵を生成し，対応する公開鍵 y を計算する．

（2） **買い手**：銀行との間で y に対するブラインド署名プロトコルを実行し，署名 $S_B(y)$ を得る．

【商品券の購入】

（1） **買い手**：公開鍵 y の元での商品券の通算購入回数を n_g とし，商品券番号と呼ぶ．購入したい商品券の額面 v_g を銀行に送り，$g = (n_g \parallel v_g \parallel y)$ とする．

（2） **買い手**：銀行との間で g に対するブラインド署名プロトコルを実行し，額面に対応した銀行の公開鍵で検証できる署名 $S_B(g)$ を得る．

（3） **銀行**：商品券の額面分を買い手の口座から差し引く．

【支払い・預金】

（1） **買い手**：商品券番号 n_g の商品券を用いた支払い回数を n_p，支払いたい金額を v_p とする．$m = (n_p \parallel v_p \parallel g)$ として公開鍵 y で検証できる署名 $S_y(m)$ を計算し，$m, S_y(m), S_B(g), S_B(y)$ を売り手に送る．

（2） **売り手**：$m, S_y(m), S_B(g), S_B(y)$ を銀行に送る．

（3） **銀行**：$S_y(m), S_B(g), S_B(y)$ の正当性を確認する．銀行のデータベース上の公開鍵 y（買い手の匿名 ID）のフィールドに登録されている商品券の番号を ${n_g}'$，それを用いた支払い回数を ${n_p}'$，その商品券での支払総額を v' として，

- $n_g > {n_g}'$ の場合：$v_g \geqq v_p$ を確かめ，正当なら $v' := v_p$，${n_g}' := n_g$，${n_p}' := n_p$ に更新する．
- $n_g = {n_g}'$ の場合：$n_p > {n_p}'$ かつ $v_g \geqq v' + v_p$ を確かめ，正当なら $v' := v' + v_p$ とする．正当な支払いなら ${n_p}' := n_p$ に更新し，売り手の口座を v_p だけ増やす．
- $n_g < {n_g}'$ の場合：不正が生じたとみなす．

（4） **売り手**：銀行から正当性の検証結果を受け取り正当なら支払いを成立させる（End.）．

買い手は，商品券を番号順に用い，使い切ってから次の番号の商品券を使う必要がある．商品券番号 n_g や支払い回数 n_p において正当な値を用いなかったとしても，買い手や売り手が利益を得たり，銀行が損をすることはない．

一つの公開鍵のもとでの支払いのすべてが対応付けられているため，何らかの手段で公開鍵の所有者の身元が露見するとその所有者のすべての支払い記録が追跡可能になる．そのため，公開鍵証明書（匿名 ID）を複数取得しそれらを使い分けた方がよい．

このプロトコルではデータベースのサイズは買い手のもつ匿名 ID の数の定数倍の規模に抑えられる．売り手依存のプロトコルと比べると，データベースの分散化ができず銀行の各支店からデータを集めた統一的データベースを必要とするという短所がある．しかし，これまでのオンライン電子現金のように全取引数の定数倍のデータベースを検索することと比較すれば，特にオンライン検証においては有利であると考えられる．

4.4 買い手依存供託オフライン電子決済

供託機能をもつ電子決済においては，銀行と受託者が協力することで電子現金データを引き出した者の ID を求めることができる．これを買い手依存オンライン電子決済のプロトコルに直接適用することで，2 重使用検出の際の不正者の特定が受託者と銀行の協力により行える．

そのプロトコルは，買い手依存オンライン電子決済プロトコルにおける公開鍵のブラインド発行を，受託者と署名者の協力で匿名性を取り消せる供託ブラインド署名を用いたものに変更することで実現できる．オンラインプロトコルでは取引完了前にデータベースへの問い合わせをして 2 重使用を検出する必要があったが，供託機能を用いると事後に不正者を特定できるので，取引が終了してから預金を行うオフライン決済が可能である．

以下，具体的にプロトコルを記述する．

【公開鍵証明書の取得】

（1） 銀行との間で供託ブラインド署名を実行する．買い手の公開鍵 y に対する供託された署名を得て，それを公開鍵証明書 $S_B(y)$ とする．

【商品券の購入】

（1） 買い手依存オンラインプロトコルと同様の構成となる．買い手は銀行の署名 $S_B(g)$ を得る．

【支払い】

（1） **売り手**：$m_S = (SID \parallel n)$ を買い手に送る．ここで，SID は売り手の ID，n は売り手が取引すべてに付ける通し番号である．

（2） **買い手**：商品券番号 n_g の商品券を用いて支払いたい金額を v_p とする．$m = (m_S \parallel v_p \parallel g)$ として公開鍵 y で検証できる署名 $S_y(m)$ を計算し，m，$S_y(m)$，$S_B(g)$，$S_B(y)$ を売り手に送る．

（3） **売り手**：$S_y(m)$，$S_B(g)$，$S_B(y)$ が正当であれば買い手の支払いを受け入れる．

【預金】

（1） **売り手**：m，$S_y(m)$，$S_B(g)$，$S_B(y)$ を銀行に送る．

（2） **銀行**：署名 $S_y(m)$，$S_B(g)$，$S_B(y)$ の正当性を確認する．一番最近に預金された同一売り手の通し

番号より，m_S に含まれる n が大きいことを確認する．銀行のデータベース上の公開鍵 y（買い手の匿名 ID）のフィールドに登録されている商品券の番号を検索する．

（case 1）送られてきた商品券の n_g がデータベースに登録されている商品券の番号のどれよりも小さい場合，不正が生じたとみなす（データベースに商品券番号が全く登録されていなければ case 3）．

（case 2）送られてきた商品券の n_g が既にデータベースに登録されている場合，その番号の商品券で支払われた総額が商品券の額面を超えていれば，不正が生じたとみなす．超えていなければ，今までにその商品券で払われた総額を更新する．額面がちょうど満額支払われたら，データベースからその番号を削除する．

（case 3）商品券の n_g がデータベースに登録されていない場合（case 1 を除く），データベースの y のフィールドに商品券番号と支払い総額 (n_g, v_p) を登録．以上，正当な支払いなら売り手の口座を v_p だけ増やす．不正が行われた場合，受託者と銀行が協力して不正者の ID を検出する（End.）．

供託を行う場合，買い手の匿名 ID ごとの通し番号に加え，売り手の口座ごとに最近に預金された現金データの通し番号を記憶する必要がある．

すなわち，データベースのサイズは（買い手のもつ匿名 ID の数の定数倍）＋（売り手の数の定数倍）の規模となる．また，現在の商品券を使い切る前に，新しい商品券での支払いデータが預金される場合を考慮して，データベースに複数の番号を登録しなければならない．だが，商品券の額面がある程度大きければ，短い期間に連続して複数の異なった商品券を使うことは少ないので，複数番号登録によるデータベースサイズ増大はほとんど問題にならないと考えられる．

更に前節の方式をオブザーバと組み合せることで，その耐タンパ性の仮定のもとで支払いにおける事前の不正防止が構成できる．

この場合，オブザーバが破られたとしても，事後に不正者の身元検出が可能である．これは，[2] と同様に，オブザーバの耐タンパ性というハードウェア的な第 1 段階の防御，更に 2 重使用者を事後に特定する第 2 段階の防御という，2 段構えの不正防止策をもつプロトコルとなっている．更に，オブザーバを破る不正者がいなければ 2 重使用は生じないことから，不正者特定のために受託者が関与する局面を減らすことができる．これは，現金の追跡性に関して強力な権限をもつ受託者自身の不正や受託者の秘密情報への攻撃を防ぐ点からも重要である．

5. 従来方式との比較

2 重使用の不正を検出するためのデータベースの量を削減することを特徴とする，他の電子決済システムとの比較を行う．

現金データに通し番号を付け，その順番にのみ預金を受け入れるというアイデアは，[7], [9] においても見られる．しかし，これらの方式は，利用者が自分の身元を明かさずに銀行と接触し，匿名口座を開設することを前提としている．だが，銀行との接触時に完全に匿名性が保証されるという仮定は，実際に銀行の店舗や端末を利用する場合はもちろん，ネットワークを介した通信においても現実的でない．これに対して，本論文における提案方式は，銀行が引出し時に利用者を特定していてもなお，匿名性が保証される．

また，[1] において，有効期限を定めることが可能なブラインド署名を利用してデータベースの量を制限する電子決済プロトコルが提案されているが，これも利用者が銀行と匿名で接触することを前提としている．

[12] では，次のような方式が提案されている．利用者が金融機関からブラインド署名を用いて電子現金発行依頼書を取得した後，この依頼書を実名などの情報を提示することなく電子現金発行機関に送信して電子現金を取得する．この方式では，利用者が発行機関に身元を明かさず接触するという前提のもとに匿名性が実現されているため，この匿名性が確保できない場合は，預金された電子現金データが 2 重使用の不正検出のために発行機関へ戻ってくることから，売り手の預金する金融機関と発行機関が結託することにより匿名性が破られる．これに対し，本論文での提案方式では銀行は受託者の協力なしに不正検出を行い，受託者は不正が生じた場合の不正者の身元の特定のみを行う．したがって，銀行と受託者が通信を行うのは不正が行われた稀な場合であり，通信量の削減と，銀行と受託者の接触が少ないことが情報漏れの可能性を低下させるという 2 点において優れている．

供託機能をもつ電子決済システムとして [8], [11] がある．本論文の提案方式は [8] における供託ブラインド署名を用いており，供託に関する特徴は同一である．[11] の供託の手法と比較すると，本論文の方式でも，[8] の方式と同様に利用者は受託者の公開情報を利用するだけでよく，受託者と通信する必要がない点が

優れている．[8], [11] のいずれにおいても，2 重使用を検出するために使用された電子現金をデータベースに保持する必要がある．

6. むすび

買い手単位で電子現金の通し番号を付ける買い手依存形のプロトコルと，売り手単位で番号を付けを行う売り手依存形のプロトコルを用いて，オンライン電子決済・オフライン電子決済・供託電子決済のそれぞれの枠組で 2 重使用を効率的に検出できる電子決済システムを提案した．

売り手依存形のプロトコルではデータベースのサイズは売り手数の規模となり，またデータベースの分散化が実現される．ただし，売り手と銀行の結託で匿名性が弱まる問題点がある．

買い手依存形のプロトコルではデータベースのサイズは買い手数の規模となる．売り手依存形と比較するとデータベースの分散化は不可能であるが，匿名性は強化される．買い手依存形の供託オフライン電子決済においては，2 重使用の不正者の身元検出が預金時に可能である．更にオブザーバとの組合せで耐タンパ性による支払い前の不正防止と支払い後の不正検出の 2 段構えの防御が実現できる．

文　献

[1] M. Abe and E. Fujisaki, “How to Date Blind Signatures,” Advances in Cryptology—ASIACRYPTO ’96, LNCS 1163, Springer-Verlag, Berlin, pp.244–251, 1996.

[2] S. Brands, “Untraceable Off-line Cash in Wallet with Observers,” Advances in Cryptology—CRYPTO ’93, LNCS 765, Springer-Verlag, pp.302–318, 1994.

[3] D. Chaum, “Security without identification: Transaction systems to make big brother obsolete,” Commun. ACM, vol.28, no.10, pp.1030–1044, Oct. 1985.

[4] D. Chaum, A. Fiat, and M. Naor, “Untraceable Electronic Cash,” Advances in Cryptology—CRYPTO ’88, LNCS 403, Springer-Verlag, pp.319–327, 1990.

[5] D. Chaum and T.P. Pedersen, “Wallet Databases with Observers,” Advances in Cryptology—CRYPTO ’92, LNCS 740, Springer-Verlag, pp.89–105, 1993.

[6] R.J.F. Cramer and T.P. Pederson, “Improved Privacy in Wallet with Observers,” Advances in Cryptology—EUROCRYPTO ’93, LNCS 756, Springer-Verlag, pp.329–343, 1994.

[7] J. Camenisch, J-M. Piveteau, and M. Stadler, “An Efficient Electronic Payment System Protecting Privacy,” Computer Security—ESORICS ’94, LNCS 875, Springer-Verlag, pp.207–215, 1994.

[8] J. Camenisch, U. Maurer, and M. Stadler, “Digital Payment Systems with Passive Anonymity – Revoking Trustees,” Computer Security—ESORICS ’96, LNCS 1146, Springer-Verlag, pp.31–43, 1996.

[9] J. Camenisch, J-M. Piveteau, and M. Stadler, “An Efficient Fair Payment System,” Proc. of 3rd ACM Conference on Computer Communications Security, ACM press, pp.88–94, 1996.

[10] T. ElGamal, “A public key cryptosystem and a signature scheme based on discrete logarithms,” IEEE Trans. on IT, vol.IT-31, no.4, pp.469–472, July 1985.

[11] 藤崎英一郎，岡本龍明，“エスクロー電子現金方式,” 信学技報，IT95-51, 1996.

[12] 森畠秀実，阿部正幸，藤崎英一郎，中山靖司，“電子現金方式,” 1997 年暗号と情報セキュリティ・シンポジウム講演論文集，SCIS97-3C, 1997.

[13] T. Okamoto, “Provable Secure and Practical Identification Schemes and Coresponding Signature Schemes,” Advances in Cryptology—CRYPTO ’92, LNCS 740, Springer-Verlag, pp.31–53, 1993.

[14] T. Okamoto and K. Ohta, “Divertible Zero-Knowledge Interactive Proofs and Commutative Random Self-Reducibility,” Advances in Cryptology—EUROCRYPTO ’89, LNCS 434, Springer-Verlag, pp.134–149, 1994.

[15] T. Okamoto and K. Ohta, “Universal Electronic Cash,” Advances in Cryptology—CRYPTO ’91, LNCS 576, Springer-Verlag, pp.324–337, 1992.

[16] C. Schnorr, “Efficient Signature Generation by Smart Cards,” Journal of Cryptology, vol.4, no.3, pp.161–174, 1991.

付　録

1. 記　法

p: Z_p^* 上の離散対数問題が困難であるような大きな素数 ($p \geqq 2^{512}$)

q: $p-1$ の約数である大きな素数 ($q \geqq 2^{140}$)

g: Z_p^* 上の位数 q の要素（原始元の $(p-1)/q$ 乗）

G_q: g によって生成される群

H: 任意の文字列を入力として，Z_q への写像である 1 方向性ハッシュ関数

と定義する．署名を行うメッセージ文字列を m で表す．

2. Schnorr 署名

【鍵生成】署名者は秘密鍵 $x \in Z_q$ と生成元 $g \in G_q$ を選び，$y = g^x$ を計算して公開鍵 (g, y) を公開する．

【署名生成】

（1） $w \in Z_q$ をランダムに選び，$a = g^w$ とする．

（2） $c = H(m \parallel a)$（$\parallel$ は文字列の連結を表す）を計算し，$r = w + cx \pmod q$ とする．

このプロトコルで得られる署名を

$\mathrm{Sig1}(m, g, y) = (c, r)$

と定義する．

【署名検証】

$c = H(m \parallel g^r y^{-c})$

が成立すれば，署名 (c, r) を m に対する，公開鍵 (g, y) の所有者による署名とみなす．

この署名は，離散対数 $\log_g y$（$y = g^x$ を満たす x の値）を知っていることを，x に関する有効な知識を与えないようにしながら証明しているものとみなすことができる．

3. ブラインド署名

Schnorr 署名に対するブラインド署名の生成について述べる（鍵生成と検証式はブラインド署名でないものと同一である）．

【署名生成】

（1） **署名者**：$w' \in Z_q$ をランダムに選び，$a' = g^{w'}$ を計算して依頼者に送る（$'$ が付いた変数は署名者に知られてもよいものを表す）．

（2） **依頼者**：$c_R, r_R \in Z_q$ をランダムに選び，$a = a' g^{r_R} y^{c_R}, c = H(m \parallel a), c' = c + c_R$ を計算して，c' を署名者に送る．

（3） **署名者**：$r' = w' + c'x \pmod q$ を計算して依頼者に送る．

（4） **依頼者**：$r = r' + r_R \pmod q$ を計算する．

このプロトコルにより署名

$\mathrm{Sig1}(m, g, y) = (c, r)$

が得られる．

4. Schnorr 署名の拡張

Schnorr 署名の拡張として，離散対数 $\log_{g_1} y_1$ の知識の証明だけでなく，その値ともう一つの離散対数 $\log_{g_2} y_2$ が等しいことも同時に証明するプロトコルを構成することができる．

そうした二つの離散対数の値が等しいことを示す Schnorr 署名の拡張 [5] について記述する．

【鍵生成】 署名者は秘密鍵 $x \in Z_q$ と二つの生成元 $g_1, g_2 \in G_q$ を選び，$y_1 = g_1^x, y_2 = g_2^x$ を計算して公開鍵 (g_1, y_1) を公開する．

【署名生成】

（1） $w \in Z_q$ をランダムに選び，$a_1 = g_1^w, a_2 = g_2^w$ とする．

（2） $c = H(m \parallel a_1 \parallel a_2)$ を計算し，$r = w + cx \pmod q$ とする．

このプロトコルで得られた署名を

$\mathrm{Sig2}(m, g_1, y_1, g_2, y_2) = (c, r)$

と定義する．

【署名検証】

$c = H(m \parallel g_1^r y_1^{-c} \parallel g_2^r y_2^{-c})$

が成立すれば，署名 $\mathrm{Sig2}(m, g_1, y_1, g_2, y_2)$ を m に対する，公開鍵 (g_1, y_1, g_1, y_2) の所有者による署名とみなす．

g_2 を署名者に明かさずに，$y_2 = g_2^x$ を依頼者が得ることができるブラインド署名プロトコルについて記述する．

【署名生成】

（1） **依頼者**：g_2 をブラインド要素 b でブラインド化した $g_2' = g_2 g_1^b$ を署名者に送る．

（2） **署名者**：$w' \in Z_q$ をランダムに選び，$a_1' = g_1^{w'}, a_2' = {g_2'}^{w'}, y_2' = {g_2'}^x$ を計算して依頼者に送る．

（3） **依頼者**：$c_R, r_R \in Z_q$ をランダムに選び，$y_2 = y_2' y_1^{-b}, a_1 = a_1' g_1^{r_R} y_1^{c_R}, a_2 = {a_1'}^{-b} a_2' g_2^{r_R} y_2^{c_R}$ $c = H(m \parallel g_2 \parallel y_2 \parallel a_1 \parallel a_2), c' = c + c_R$ を計算して，c' を署名者に送る．

（4） **署名者**：$r' = w' + c'x \pmod q$ を計算して依頼者に送る．

（5） **依頼者**：$r = r' + r_R \pmod q$ を計算する．

このプロトコルにより署名 $\mathrm{Sig2}(m, g_1, y_1, g_2, y_2)$ が得られる．

5. 供託ブラインド署名

署名者 B，受託者 T の生成元を $g_B, g_T \in G_q$，秘密鍵を $x_B, x_T \in Z_q$，公開鍵を $y_B = g_B^{x_B}, y_T = g_T^{x_T} \in G_q$ とする．

ElGamal 暗号 [10] を用いた，受託者による平文 e の暗号化は，$C_1 = g_T^k, C_2 = e y_T^k$（$k \in Z_q$ はランダム）として，(C_1, C_2) が暗号文となる．

このとき，ElGamal 暗号の復号化により，受託者が (C_1, C_2) から e を求めることができる．

$e = C_2 / C_1^{x_T}$

また，C_2 と e から，受託者は

$C_1 = (C_2/e)^{x_T^{-1}}$

より C_1 を求めることもできる．

そこで，C_2 をシステム共通の値とし，依頼者はランダムに $k \in Z_q$ を選び $e = C_2 y_T^{-k}$ を計算する．依頼者は e をブラインド化し，署名者に対してブラインド署名を依頼する．また，依頼者は C_1 を署名者に送付し，署名者は依頼者の ID と組で C_1 を保管してお

く．更に，依頼者は (C_1, C_2) が e の暗号文となっていることを，e を明かさないようにしながら署名者に対して示す．

こうして得たブラインド署名は，署名者と受託者が協力することにより匿名性をはくだつすることが可能である．署名者が保管するデータ C_1 を受託者に提供し，受託者が復号化を行い e を求めることで，対応する署名の追跡が可能となる．また，e から対応する C_1 が受託者により求められるので，署名自体からその依頼者の ID も判明する．

以上の供託の原理をもとに，署名者が依頼者の選んだメッセージ m に対するブラインド署名を発行するが，受託者が協力したときのみ追跡が行えるプロトコルを構成する．

【鍵生成】まず生成元

$$g_B, g_T \in Z_q$$

を受託者が選ぶ．ただし，g_B と g_T は，互いの要素に対する離散対数の値を受託者以外に知られないようにする必要がある．署名者，受託者はそれぞれ秘密鍵

$$x_B, x_T \in Z_q$$

を選び，公開鍵として

$$y_B(= g_B^{x_B}), y_T(= g_T^{x_T})$$

と生成元を公開する．

また，上述したようにシステムに共通な値として $C_2 \in G_q$ を選んで公開する．

【署名生成】

（1） **依頼者**：

$k \in Z_q$ をランダムに選ぶ．$e = C_2 y_T^{-k}$，$e' = e g_B^k$（e をブラインド化したもの），$C_1 = g_T^k$，$P1$ =Sig2$(\epsilon, g_T, C_1, (g_B/y_T), (e'/C_2))$ を計算し（ϵ は空の文字列），$e', C_1, P1$ を署名者に送る．

（2） **署名者**：署名 $P1$ を確認する．C_1 を依頼者の ID とともに保管する．

（3） **依頼者・署名者**：ブラインド要素を k として，Schnorr 署名の拡張形式のブラインド署名プロトコルを実行し，メッセージ m に対する署名者の署名 Sig2$(m, g_B, y_B, e, z) = (c, r)$ を得る（z はブラインド署名により得る $z = e^x$ を満たす値である）．

（4） **依頼者**：$P2$ =Sig$(\epsilon, y_T, C_2/e)$ を計算する．

m についての署名 Sig2(m, g_B, y_B, e, z) と，$P2$ を合わせて，供託済みの署名とする．

【署名検証】

$$c = H(m \parallel g_B^r y_B^{-c} \parallel e^r z^{-c})$$

かつ署名 $P2$ が成立していれば，公開鍵 (g_B, y_B) のもとでの m に対する署名として受け入れる．

【受託者と署名者による追跡】

1. 署名発行時の履歴から対応する署名を求める．

署名者は C_1 を保持しているので，受託者は秘密鍵 x_T を用いて

$$e = C_2/C_1^{x_T}$$

を計算することで対応する署名を見つけることが可能である．

2. 署名から依頼者の ID を求める．

署名に含まれる e から，受託者は秘密鍵 x_T を用いて

$$C_1 = (C_2/e)^{x_T^{-1}}$$

を計算することで C_1 を見つけることが可能であり，署名者は C_1 と ID の組を保持していることから，署名の依頼者の ID を求めることが可能である．

（平成 9 年 11 月 10 日受付，10 年 6 月 3 日再受付）

光岡　　円　（正員）

平 7 東大・工・計数卒．平 9 同大大学院修士課程了．同年富士通研究所入社．在学中，電子現金に関する研究に従事．インターネット上の社会システムの構築に興味をもつ．情報処理学会会員．

山本　博資　（正員）

昭 50 静大・工・電気卒．昭 55 東大大学院博士課程了．工博．同年徳島大・工・電子助手．同講師，助教授を経て，昭 62 電通大・電子情報助教授．平 5 東大・工・計数助教授，現在に至る．平 6 年度情報処理学会 Best Author 賞受賞．情報理論（Shannon 理論，多端子情報理論，データ圧縮アルゴリズムなど），通信理論，暗号理論などの研究に従事．IEEE，情報理論とその応用学会，日本応用数理学会各会員．