(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第4006762号
(P4006762)
(45)発行日　平成19年11月14日(2007.11.14)　(24)登録日　平成19年9月7日(2007.9.7)

(51)Int.Cl.		F I		
H04L 9/32	(2006.01)	H04L	9/00	675D
G09C 1/00	(2006.01)	G09C	1/00	660B
G06Q 20/00	(2006.01)	G06F	17/60	414

請求項の数 6　(全 10 頁)

(21)出願番号	特願平9-539608
(86)(22)出願日	平成9年5月7日(1997.5.7)
(65)公表番号	特表2000-510254(P2000-510254A)
(43)公表日	平成12年8月8日(2000.8.8)
(86)国際出願番号	PCT/FR1997/000826
(87)国際公開番号	WO1997/042610
(87)国際公開日	平成9年11月13日(1997.11.13)
審査請求日	平成16年4月16日(2004.4.16)
(31)優先権主張番号	96/05706
(32)優先日	平成8年5月7日(1996.5.7)
(33)優先権主張国	フランス(FR)

(73)特許権者
フランス　テレコム
フランス国，７５０１５　パリ，プラス　ダルレイ　６番地
(73)特許権者
ラ　ポスト
フランス国，９２７７７　ブーローニュ　ビヤンクール，ケ　デュ　プワン　デュ　ジュール，４番地
(74)代理人
弁理士　山本　恵一
(72)発明者　パーユ　ジャン―クロード
フランス国，１４６１０　エプロン，リュ　デ　ルワズィール，４番地

最終頁に続く

(54)【発明の名称】二重署名安全電子トランザクションを実施するための処理手順

(57)【特許請求の範囲】

【請求項１】

カードと、該カードを受け入れるように構成された少なくとも１つの端末を有するサービス提供者と、該端末に接続されるように構成された中央システムとの間で、電子トランザクションを実施するための方法であって、前記カードはカードの秘密借方キー（ｋ）を有し、前記中央システムは前記カードの秘密借方キーを知っており、前記方法は、

ａ）前記端末から前記カードに、カード残高から借方記入された金額（ｍ）を少なくとも含むパラメータ（Ｍ）を伝送し、

ｂ）前記カードが、前記残高は前記金額より小さくないことをチェックし、

ｃ）前記カードが、前記カード残高から前記金額（ｍ）を借方記入し、

ｄ）前記カードが、前記金額は前記カード残高から借方記入されたことの証明であり、及び前記カードの秘密借方キー（ｋ）と前記パラメータ（Ｍ）との関数である署名（ｚ）を計算し、

ｅ）前記カードが、前記署名の関数であるデータ（ｙ、ｂ）を計算し、

ｆ）少なくとも前記署名（ｚ）と前記データ（ｙ、ｂ）を前記カードから前記端末に伝送し、

ｇ）前記端末が、前記データ（ｙ、ｂ）をチェックし、

ｈ）前記署名（ｚ）を前記端末に記憶し、

ｉ）前記中央システムが、前記署名（ｚ）を収集し、

ｊ）前記中央システムが、前記カードの秘密借方キー（ｋ）で前記署名（ｚ）をチェック

し、
ｋ）前記中央システムが、前記署名の前記チェック操作が正であるという条件でサービス提供者に金額（ｍ）の貸方記入する、
各ステップを含むことを特徴とする方法。
【請求項２】
前記カードが秘密及び公開カードキー（ｓ、ｐ）の組み合わせを有し、前記データが前記カードの秘密キー（ｓ）を使用した前記署名の関数であり、前記端末が前記データのチェックに前記カードの公開キー（ｐ）を使用することを特徴とする請求の範囲第１項に記載の方法。
【請求項３】
前記中央システムが、さらに当局の秘密及び公開キー（S_A、P_A）の組み合わせを知っており、及び前記カードは、当局の秘密キー（S_A）を使用して計算されたカード証明書（ｃｅｒ）を有し、前記方法は、
前記カード証明書（ｃｅｒ）を前記カードから前記端末に伝送し、
前記端末が当局の公開キー（P_A）を使用し、前記カード証明書をチェックする、
各ステップをさらに含むことを特徴とする請求の範囲第２項に記載の方法。
【請求項４】
前記カードが秘密及び公開カードキー（ｓ、ｐ）の組み合わせと、カード識別（ｉ）と、前記カードの公開キー（ｐ）を定義する２つのカードパラメータ（ｎ，ｅ）を有し、前記ステップｅ）は、
前記カードがカード乱数（ｘ）を選択し、
前記カードが第１の数$t = x^e \bmod n$を計算する、
各ステップをさらに含み、
前記データ（ｂ）は、前記パラメータ（Ｍ）と、前記署名（ｚ）と、前記第１の数（ｔ）を下位ビットに制限した第２の数（t^*）と、の関数（ｈ）であり（$b = h(t^*, M, z)$）、
前記端末が、チャレンジ乱数（ｃ）を選択し、前記端末から前記カードに伝送し、
前記端末が、前記カードから、チャレンジ乱数（ｃ）と前記乱数（ｘ）との関数であるデータ（ｙ）を受け取り、
前記端末が、前記カード識別の拡張関数$I = g(i)$を計算し、
前記端末が、数$u = (y^e I^c \bmod n)$を計算し、
前記端末が、$b = h(u, M, z)$であることをチェックする
各ステップを含んでいることを特徴とする請求の範囲第１項に記載の方法。
【請求項５】
前記中央システムが、さらに当局の秘密及び公開キー（S_A、P_A）の組み合わせを知っており、及び前記カードは、当局の秘密キー（S_A）を使用して計算されたカード証明書（ｃｅｒ）を有し、前記方法は、
前記カード証明書（ｃｅｒ）を前記カードから前記端末に伝送し、
前記端末が当局の公開キー（P_A）を使用し、前記カード証明書をチェックする、
各ステップをさらに含み、チャレンジ乱数（ｃ）が、前記カード証明書のチェックが正のときのみ前記カードに伝送されることを特徴とする請求の範囲第４項に記載の方法。
【請求項６】
前記チャレンジ乱数（ｃ）の長さを変化するステップをさらに含むことを請求の範囲第４項または第５項に記載の方法。
【発明の詳細な説明】
発明の分野
本発明は、二重署名電子トランザクションを実施するための処理手順に関する。
本発明は、端末がチップ・カードを所持する利用者と安全なトランザクションを実施することを必要とし、この端末が、中央処理システムに常時接続されているのではなく、最近の収集以降に実施されたトランザクションの収集中に周期的にのみ接続される、あらゆる

分野に適用することができる。

背景技術

下記の説明をわかりやすくするために、「電子財布（wallet）」として知られている形式のトランザクションの状況を使用する。この技術は、１９９４年第４四半期に発行された「L'Echo des Recherches」誌の増刊号（第１５８号）の主題であった。とくに興味をひくものは、「Signature electronique et application au paiement electronique」と題するMarc Girauld Luc Valleeによる論文である。

電子財布技術は近年著しく発達したが、このタイプの適用例の安全保護にはなお問題があり、これに対する研究が続けられている。これらの問題に対しては様々な解決策が可能であり、安全保護とコストに基づいて検討することができる。

このタイプのシステムでは、電子財布（ＥＷ）カードは、残高、すなわちある量の価値（通貨、トークン、消費単位など）を載せている。金額ｍの支払いに応じてこの残高はｍ単位だけ減少し、カードは、ｍ単位だけ借方記入されたという証明を生成し、これが、使用者がトランザクションを行う相手である端末またはサーバを備えた商人に対する支払い証明となる。この証明は、電子財布を発行した当局から商人が正規の通貨で支払いを受け取る条件であり、この当局を「銀行」と呼ぶこともできる。

証明は、偽造カードの使用を防止するために検証しなければならない。つまり無から、すなわちカードなしで、本物として受け入れできる証明を構築することが不可能でなければならない。証明はまた、金額ｍをｍより大きな金額ｍ’に変換するか、または同じ証明を再使用して支払うべき金額を商人に二度支払ったり、またはさらに支払うべきではない金額を他の商人に支払うなどの操作も防止しなければならない。

下記の説明では、これらのシステムにおける様々な関係者を「利用者」、「サービス提供者」、「銀行」として記載する。利用者は、サービス提供に支払うためにＥＷカードを有し、また銀行はカードを発行する組織である。

現在使用されている技法を、この技法が使用する署名が秘密キーを有するか、公開キーを有するか、または対話キーを有するかにしたがって、３種に大別することができる。

第１のタイプでは、端末は銀行から切断することができ（オフラインと呼ばれる）、また銀行に直接接続することもできる。第１の構成（オフライン）は、様々な既存の電子財布システムで最も普通のものである。これは、ＥＷカードの番号を表すパラメータｉと、下記のすべてのパラメータを代表するパラメータＭとに適用される秘密キー・アルゴリズムｆを使用して、証明ｚを計算することにある。

ｍ：トランザクションの金額、

ｊ：通常安全アプリケーション・モジュールすなわちＳＡＭとして知られている安全保護モジュールの番号、

ｒ：乱数値、さらに簡単には、カウンタの読み、

これによりｚ＝ｆ（ｋ，ｍ，ｊ，ｒ）が得られる。ただしｋは識別がｉであるＥＷカードの秘密キーである。このキーは、カードの番号ｉに従ってキーを多様化する機構のため、ｉに依存している。ＳＡＭは端末中に置かれたチップ・カードであり、この物理的特徴から、端末が安全な保護された金銭登録機として活動することが可能になる。したがってＳＡＭは、証明書ｚをチェックし、受け取った金額を累計する。これは規則的に空にされるので、サービス提供者の収益は銀行によって貸方記入される。これはＳＡＭと銀行との間の安全な処理手順を使用して行われる。この処理手順には特に困難なものは含まれておらず、したがってこれについてはここでは説明しない。

証明書ｚをチェックするために、ＳＡＭはすべてのＥＷカードのキーを知る必要がある。実際問題として、これは多様化式ｋ＝ｇ（ＫＭ，ｉ）を使用して、ＥＷカードのキーｋを計算することによって行われる。ただしＫＭはマスタ・キーであって、システム全体について有効であり、すべてのＳＡＭ中に存在する。

この方法を添付の図１に示すが、ここでは利用者のＥＷカードには１０の番号、サービス提供者の端末には２０の番号、そのＳＡＭには２５の番号、そして銀行には３０の番号が付けられている。端末２０からカード１０に向う矢印はパラメータＭのカードへの伝送を

表し、逆方向に向う矢印は証明書ｚの端末への伝送を表す。
この第１の方法は、低コストのカードを使用するという利点がある。しかしながら次のような欠点を持っている。すなわち、
－ＳＡＭは、非常に広範囲に及ぶすべての端末に設置されているので、安全保護は、ＳＡＭにおけるマスタ・キーＫＭが読取り不可能なことに基づき、したがってＳＡＭの物理的安全保護に基づいている。したがって、この安全保護は保存が困難である。マスタ・キーＫＭを所有すると大規模な不正行為が可能になり、ブラックリスト・システムが阻止できない任意の識別ｉを有するカードを作成することができることになる。
－ＳＡＭは、端末中またはサービス提供者の構内に位置する。このため、各々それ自体のＳＡＭを有するいくつかの形式のＥＷカードを受け入れなければならないという実用上の問題が生じる。これは、複数の銀行がそれ自体のＥＷカードを発行する場合に、付随的に実際上非常に広範に見られる事例である。
ここで、サービス提供者端末が銀行に接続されている構成（すなわちオンライン）に目を向けると、ＳＡＭはもはや端末の内部にはなく、証明書は銀行でチェックしなければならない。この処理手順を添付の図２に示すが、番号付けは図１におけるものと同じである。実際問題として、遠隔通信コストが非常に高いので、このシステムは余り関心がもたれない。電子財布システムは、非常に小さな金額を伴うトランザクションにもコスト効果がよくなければならない。
公開キー・アルゴリズムを使用する署名処理手順を組み込んだシステムは、安全アプリケーション・モジュール（ＳＡＭ）を使用するか否かに応じて２つのタイプに分けることができる。
ＳＡＭが使用されない場合には、前述の秘密キー・システムの証明書ｚは、ＲＳＡ（Rivest-Shamir-Adleman）アルゴリズムなどの公開キー・アルゴリズムに基づく署名で置き代えられる。各カードは、それぞれｓとｐである秘密キーと公開キーとの対を有し、パラメータＭによって定義された借方証明は、署名ｙ＝ｓ（Ｍ）を計算することによって得られる。
サービス提供者は、公開キーを使用してこの署名をチェックすることができる。すべての署名を周期的な収集のために記憶して、銀行による支払いを記録することができる。このタイプの構成では、秘密キーｓと公開キーｐとの対を単に保持することは、ＥＷカードが本物であることを証明することにはならないので、公開キーｐはまた、カードを発行する当局によって本物であることが認証されなければならない。このタイプの対を、例えば適切なソフトウェアをインストールしたパーソナル・コンピュータを使用して容易に検出することができる。したがってＥＷカードは端末に、その公開キーｐのみでなく、公開キーｐにリンクされた証明書も提供しなければならない。この証明書を、以下「ｃｅｒ」と称することにする。証明書「ｃｅｒ」は銀行の公開キーＰＡによってチェックされる。
添付の図３にこの構成を示す。番号付けは図１および図２のものと同じであるが、サービス提供者の端末２０がカード番号ｉ、パラメータＭ、証明書ｃｅｒ、および署名ｙを収集または記録する手段２６を備えていることに注目されたい。
このシステムの利点は、リスクが関与するＳＡＭまたは秘密マスタ・キーが端末中に存在しないことである。したがって、このシステムはより安全であり、より高い順応性を有する。
しかしながら、このシステムは次の欠点を有する。すなわち、
－所与の応答時間で必要な計算力が大きいので、ＲＳＡ型公開キー・アルゴリズムに基づく計算を実行できるカードのコストが高い。
－大量のデータを端末に記憶し、端末から収集する必要があり、Ｍとｙを各トランザクションごとに記憶しなければならない。公開キー（５１２ビット）の現在長が与えられた場合、このデータ・セットは１．５キロビット程度になる。
安全アプリケーション・モジュールによるバージョンでは、トランザクションは、後続の銀行による収集のために端末に累積される。意図的な何らかの不正がサービス提供者によって累積された金額の変更の企てを含むとすれば、累積操作は安全保護上のリスクを有す

るので、ＳＡＭは、トランザクション署名をチェックし、これらを累積することが必要となる。
図４に、このバージョンを先の図と同じ番号付けを使用して示す。
このバージョンの利点は、端末が秘密マスタ・キーを含まず、これによって安全保護が改善することである。しかしながら２つの欠点が残っている。すなわち、
－所与の応答時間で必要な計算力が大きいので、公開キー・アルゴリズムに基づく計算処理を実行できるカードのコストが高い。
－ＳＡＭを必要とする。
第３のタイプの処理手順は対話型署名システムを使用する。この技法を使うと、カードが必要とする計算力を、現在使用されているパラメータ設定で１０～２０分の１に著しく減少することが可能になる。したがって、同じ計算力の場合、応答時間が改善される。同じ応答時間で、ＥＷカードの構成要素のコストは低い。
概して、２つの認証システム、すなわちGuillou-Quisquater（ＱＲ）およびFiat-Shamir（ＦＳ）が使用される。上述の「L'Echo des Recherches」誌増刊号は、これら２つのシステムに関する参考文献をすべて含んでいる。
この形式の署名処理手順の概要を、一例としてＣＱシステムを使用して説明する。この例で、Ｃｉとして示されるカードは次の関数またはパラメータを使用する。
ｇ：６４～５１２ビットの拡張関数、
ｈ：６４ビットの結果を出すハッシュ関数、
＊：１２８最低位ビットに制限する操作、
S_AおよびP_A：当局の秘密キーと公開キー：７６８ビット、
ｉ：カードの識別：６４ビット、
ｎ：モジュール：５１２ビット、
ｃｅｒ：S_A（ｉ，ｎ，ｅ）：７６８ビット、
ｅ：ｎ第１数：１６ビット、
ｖ：$1／I^{1/e}$ ｍｏｄ ｎ：５１２ビット。
セキュア端末Ｔｊは、公開キーP_A、ｇ、ｈを有し、６４ビットのｊで証明される。
処理手順は次の通りである。
１）端末は、トランザクションの金額ｍを設定し、乱数ｒを引き、ｍ、ｊ、ｒを組み合わせるパラメータＭを構成する。次いでＭをカードに伝送する。
２）カードは、残高がトランザクションの金額ｍより大きいことをチェックする。その通りであれば、カードは乱数ｘを引き、$t＝x^e$ ｍｏｄ ｎとｂ＝ｈ（t^*，Ｍ）とを計算し、ｉ、ｂ、および証明書ｃｅｒ＝S_A（ｉ，ｎ，ｅ）を端末に伝送する。
３）端末は証明書をチェックして、ｉ、ｎ、ｅを得、ｅより小さな乱数ｃを選択して、ｃをカードに送る。
４）カードは$y＝x v^c$ ｍｏｄ ｎを計算し、残高をｍだけ減らし、ｙとt^*を端末に伝送する。
５）端末は$I＝g（i）$、量$u＝（y^e I^c$ ｍｏｄ ｎ$）^*$、次いでｈ（ｕ、Ｍ）を計算し、ｂがｈ（ｕ、Ｍ）に等しいことをチェックする。次いで端末は残高をｍだけ増やす。
この処理手順は次のように要約することができる。
－カードは乱数ｘを選択して、$t＝x^e$ ｍｏｄ ｎを計算し、ｂ＝ｈ（Ｍ，ｔ）を端末に送り、
－端末は、０＜ｃ＜ｅになるように乱数ｃを選択して、これをカードに送り、
－カードは、$y＝x v^c$ ｍｏｄ ｎに応答し、
－次いで端末は、$u＝y^e I^c$ならば、$v^e I＝1$ ｍｏｄ ｎであるからｂ＝ｈ（Ｍ，ｕ）であることをチェックする。
この処理手順を添付の図５に示す。この利点は、必要な計算力がＲＳＡ型の処理手順よりも低いことにある。しかしこの処理手順には、ＳＡＭを必要とするという欠点が残っている。対話型署名は、乱数値ｃが所与の順序で正しくカードに提供されないかぎり価値はない。この理由で対話型署名は、「使い捨て」として知られており、これらが得られるとき

にのみ使用することができる。対話型署名は、データM、ｃｅｒ、ｂ、ｃ、ｙを含む。したがって、無からこのデータを作り出すことは容易であり、ｃｅｒとMが既知であれば、ｐとｉを得ることができ、残っているのはｙとｃを選択すること、およびｔ＝$y^e I^c$とｂ＝ｈ（Ｍ，ｔ）を計算することである。得られたデータM、ｃｅｒ、ｂ、ｃ、ｙは有効な署名を構成する。

本発明の目的は、これらの欠点を正確に克服することである。

発明の開示

本発明は、一方の署名が公開キーまたは秘密キー形式のもので（上記のｙを参照）、他方の署名が秘密キー・アルゴリズムに基づく（上記のｚを参照）、二重署名処理手順を提案する。この二重署名は、２つの技法の利点を組み合わせるために設計されたもので、したがって所望の利点を得るために２つの署名を署名情報に賢明に組み合わせることからなる。

先に説明したように、ＲＳＡ型署名においては、カードの借方証明は、サービス提供者がチェックすることのできる署名ｙ＝ｓ（Ｍ）を計算することによって得られ、この署名がなければ、サービス提供者は、公開キーを使用して操作するので秘密の情報を含まなければならない。これを図３に示す。

秘密キー処理手順では、証明ｚは、ｚ＝ｆ（ｋ，ｍ，ｊ，ｒ）を計算するための秘密キー・アルゴリズムを使用して得られる。ただしｋは秘密キーであり、ＳＡＭを含まない変更例では、ｚをサービス提供者がチェックすることはできないが、銀行のみがチェックすることができる。証明ｚはｉおよびMとともにサービス提供者によって記憶され、続いて銀行によって収集される。

本発明によれば、これら２つの処理手順は、サービス提供者がチェックすることのできる署名ｙが、サービス提供者がチェックすることのできない署名ｚに従属するように組み合わされる。これによって、ｙ＝ｓ（Ｍ）の代わりにｙ＝ｓ（Ｍ，ｚ）が得られる。したがって利用者がｚをｚ’に変更するには、ｙをｙ’＝ｓ（Ｍ，ｚ’）に変更することが必要であるが、これは、関数ｓがカードにしか知られていないので不可能である。

対話型署名処理手順では、上記のようにカードが関数ｂ＝ｈ（Ｍ，ｔ）を計算する代りに、ｔ＝x^e　ｍｏｄ　ｎによって、証明ｚを含む関数ｂすなわちｂ＝ｈ（Ｍ，ｔ，ｚ）が計算される。ｚが利用者によってｚ’に変更された場合、サービス提供者のソフトウェアはこの変更を検出する。実際に、ｔのみがトランザクションの完了時に間接的に明かされる。したがって、ｂ’をサービス提供者に送らなければならないときに、利用者はｂ’＝ｈ（Ｍ，ｔ，ｚ）を計算することはできない。

さらに正確には、本発明の目的は、カードを所有する利用者と、前記カードを受け入れることのできる端末を所有するサービス提供者と、端末に周期的に接続することのできる中央システムとの間で、電子トランザクションを実施するための処理手順であって、

－端末は、少なくともトランザクションの金額を含むパラメータをカードに伝送し、

－カードは、前記金額を残高から借方記入し、

－カードと端末は様々なデータを計算し、交換し、これらのデータのいくらかは公開または秘密アルゴリズムを使用してカードによって署名され、

－端末は、前記公開または秘密アルゴリズムによって署名されたデータをチェックし、実施された様々なトランザクションの個々のパラメータを記憶し、

－中央システムは、端末に接続されたとき、記憶されたデータを周期的に収集し、該当する金額をサービス提供者に貸方記入する、

という処理手順を提供することであり、

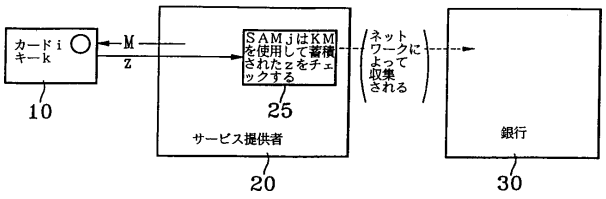
この処理手順は、これが二重署名処理手順であり、公開または秘密アルゴリズムを使用してカードによって署名されたデータは、カードが借方記入されたという証明ｚを含み、この証明ｚはパラメータと秘密借方キーとの関数であり、これによって端末はまた、前記証明をチェックすることができずに、実施されたトランザクションの種々の証明を記憶し、中央システムはまた前記証明を収集し、秘密借方キーを使用してこれらの証明をチェックし、チェック操作が肯定であるという条件でサービス提供者に貸方記入することを特徴と

する。
支払いがサービス提供者とオンラインで行われる場合には、アルゴリズムを秘密キー形式にすることもできる。
【図面の簡単な説明】
図１は、秘密キー・アルゴリズムとオフライン端末とを使用する、公知の署名処理手順を示す図である（上述）。
図２は、秘密キー・アルゴリズムと銀行に接続された端末とを使用する、公知の署名処理手順を示す図である（上述）。
図３は、安全アプリケーション・モジュールのない公開キー・アルゴリズムを使用する、公知の署名処理手順を示す図である（上述）。
図４は、安全アプリケーション・モジュールのある公開キー・アルゴリズムを使用する、公知の署名処理手順を示す図である（上述）。
図５は、公知の対話型署名処理手順を示す図である（上述）。
図６は、公開キー署名を使用する処理手順における、本発明の第１の実施形態を示す図である。
図７は、対話型署名を使用する処理手順における、本発明の第２の実施形態を示す図である。
実施形態の詳細な開示
対話型署名を使用する本発明の一実施形態を、一例としてこれから説明する。下記の省略形を使用する。
ｇ：４８～５１２ビットの拡張関数、
ｈ：１２８ビットの結果を出すハッシュ関数、
ｆ：秘密キー（例えばＤＥＳ）署名計算関数：６４ビット、
＊：ｋ．６４下位ビットに制限する操作、ｋは４～８に設定できる
S_AおよびP_A：当局の秘密キーと公開キー：７６８ビット、
カードに含まれるデータは次の通りである。
ｉ：カードの識別：４８ビット、
ｎ：モジュール：５１２ビット、
ｃｅｒ：S_A（ｉ，ｎ，ｅ）：７６８ビットの証明書
ｅ：$2^{16}+1$、
ｖ：$1/I^{1/e}$ ｍｏｄ ｎ：５１２ビット、
ｋ：秘密借方キー：６４ビット、
ｂａｌ：カード上の残高：３２ビット
ｈ，ｆ
サービス提供者の端末に含まれるデータは次の通りである。
P_A、ｇ、ｈ
ｊ：端末の識別：４８ビット、
ｍ：金額：１６ビット、
ｒ：カウンタの読み：３２ビット。
したがって、続くオプションは下記の通りである。
１）サービス提供者の端末は、トランザクションの金額ｍを設定し、ｍ、ｊ、およびカウンタの読みｒからＭを構成し、この読みをｒ＋１に設定する。サービス提供者はＭをカードに伝送する。
２）カードは、残高が金額ｍより少なくないことをチェックする。このチェックが正であれば、カードは５１２ビットの乱数ｘを選択し、$t=x^e \bmod n$を計算し、秘密借方キーｋを使用して証明ｚ、すなわち$z=f(k,M)$を計算し、また$b=h(t^*,M,z)$、すなわち金額ｍを残高と記録Ｍから計算する。カードは認証証明書$cer=S_A(i,n,e)$を含む。ただし、S_Aは当局の秘密キーである。カードは最終的に、証明ｚ、関数ｂ、および証明書ｃｅｒをサービス提供者の端末に伝送する。
３）サービス提供者の端末は、当局の公開キーP_Aを使用して証明書ｃｅｒをチェックし

て、ｎ、ｅ、ｉを得る。端末は、チャレンジとも呼ばれる１６ビットの乱数ｃを選択して、ｃをカードに伝送する。
４）カードは、$y = x v^{c} \mod n$を計算して、ｙをサービス提供者の端末に伝送する。
５）サービス提供者の端末は、Ｉ＝ｇ（ｉ）、次いで$u = (y^{e} I^{c} \mod n)$を計算する。端末は、ｂがｈ（ｕ，Ｍ，ｚ）に等しいことをチェックし、このチェックが正であると証明した場合には、トランザクションを有効にする。端末はｉ、Ｍ、ｚを収集して、このデータを銀行に送る。
６）銀行は、ｉを使用して秘密借方キーｋを得て、証明ｚ＝ｆ（ｋ，Ｍ）をチェックする。銀行は、サービス提供者の端末のカウンタｒが進んだことをチェックし、そうであれば、サービス提供者の計算書に金額ｍを貸方記入する。
この処理手順は、対話型署名の使い捨ての性格をなくすことによって修正することもできる。この修正は、ｚ＝ｆ（ｋ，Ｍ）をｚ＝ｆ（ｋ，Ｍ，t^{*}）に変更することによって行われる。上述の対話型署名（ｉ，Ｍ，ｃｅｒ，ｙ，ｚ）を生成する方法はもはや働かない。すなわちｙ、ｃ、Ｍが選択され、$t^{*} = (y^{e} I^{c} \mod n)$が計算され、ｂ＝ｈ（$t^{*}$，Ｍ，ｚ）が計算されるが、ｔはｚ＝ｆ（ｋ，Ｍ，$t^{*}$）を満足しない。データ項目ｉ、Ｍ、ｚ、$t^{*}$、ｂ、ｃ、ｙはサービス提供者によって記憶されなければならない。
上記のプロトコルの安全保護レベルは、チャレンジｃのサイズによって決定される。例えば、ｃが１６ビットのサイズを有する場合には、カード偽造者がｃを推察して人為的にトランザクションを作り出す機会は、$2^{16} = 65,536$回に１回となる。カードの計算時間もまた、この安全保護レベルに直接比例する。安全保護レベルは、署名が対話型であるカードに端末が伝送する乱数ｃの長さを変更することによって変えることもできる。したがって１つの改善策は、トランザクションのサイズ、接触支払いよりも遠隔支払いの方が高い偽造カードが使用される可能性、などのパラメータにしたがって、サービス提供者が安全保護レベルを調節できるようにすることからなる。
この説明から、本発明の処理手順が下記の通り多くの利点を有することが明らかになろう。すなわち：
－極くわずかな計算力しか必要としないので、ＥＷカードは低コストで同等の性能をもたらすことができ、あるいは、同等の計算力で応答時間が改善される。
－サービス提供者がＳＡＭを必要とせずに、使用することができる。
－サービス提供者が必要とする記録保持メモリを５：１０の比率で減少させる。
－サービス提供者から銀行へ転送されるデータの量を上記と同じ比率で減少させる。
－トランザクションがサービス提供者によって累積されることが好ましい場合には、これをＳＡＭとともに使用することができる。しかしながら、使用されるＳＡＭは秘密キーを含んでいないので、安全保護上のリスクはほとんどない。
トランザクションの特徴に応じて、安全保護レベルを調節することができる。
2^{16}の安全保護レベルは、暗号法において通常見られる６４ビット、さらに５１２ビットさえもあるレベルと比較すれば低い。しかしながら、キーを見つけるコストに関して言えば（この場合にはｖ）、すなわちチャレンジ応答対を使用してキーを見つけるために必要な繰り返し回数に関しては、ここの提唱するシステムは標準システムと全く同じ安全保護特性を有している。この2^{16}の安全保護レベルの利点を利用するために、偽造カードは、１つの受け入れがなされるまでにに平均３２，０００回の拒絶トランザクションを試みることになる。

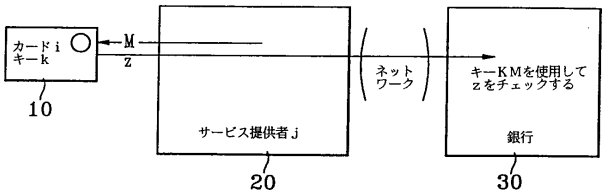
【図１】

FIG.1



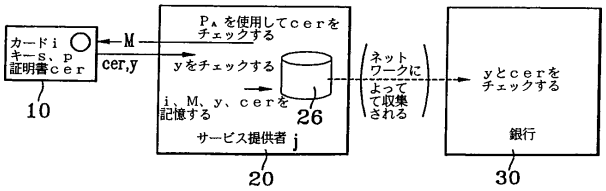
【図２】

FIG.2



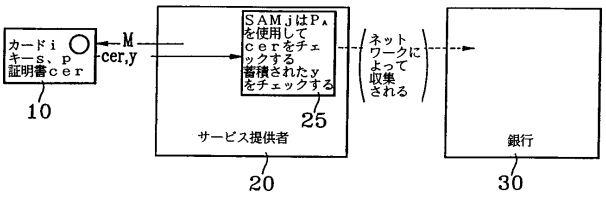
【図３】

FIG.3



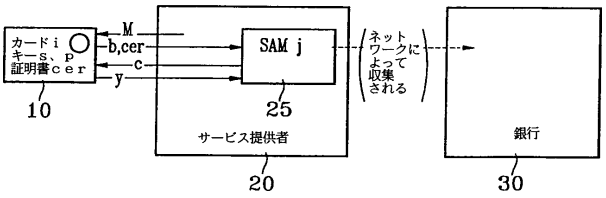
【図４】

FIG.4



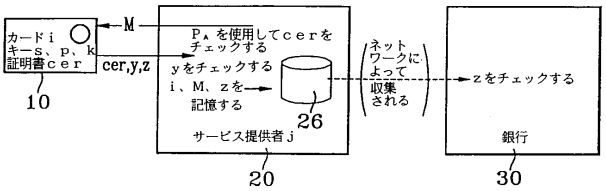
【図５】

FIG.5



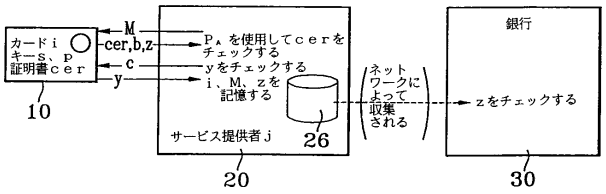
【図６】

FIG.6



【図７】

FIG.7



フロントページの続き

(72)発明者 ジロー マルク
フランス国, １４０００ カーン, リュ ベルナール ヴァニエ, ９番地
(72)発明者 ルメリー パトリック
フランス国, １４０００ カーン, リュ ドゥ コルヌアーユ, ４３番地

審査官 中里 裕正

(56)参考文献 特開平０３－０９２９６６（ＪＰ, Ａ）
特開平０８－０７９２３８（ＪＰ, Ａ）

(58)調査した分野(Int.Cl., ＤＢ名)
H04L 9/32
G06Q 20/00
G09C 1/00