(19)日本国特許庁(JP)　(12)公表特許公報(A)　(11)特許出願公表番号
特表2005-532723
(P2005-532723A)
(43)公表日　平成17年10月27日(2005.10.27)

(51)Int.Cl.[7]	F I		テーマコード（参考）
H04L 9/10	H04L	9/00　621A	5J104

審査請求 未請求　予備審査請求 有　（全 30 頁）

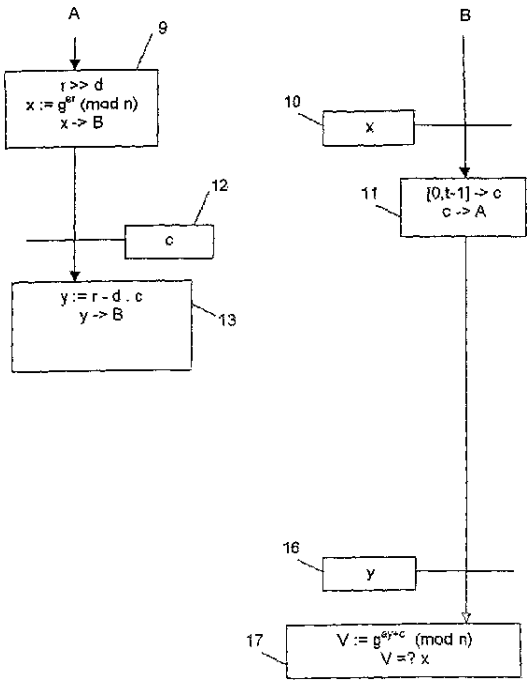
(21)出願番号	特願2004-518844 (P2004-518844)
(86)(22)出願日	平成15年6月27日 (2003.6.27)
(85)翻訳文提出日	平成16年12月27日 (2004.12.27)
(86)国際出願番号	PCT/FR2003/002000
(87)国際公開番号	WO2004/006497
(87)国際公開日	平成16年1月15日 (2004.1.15)
(31)優先権主張番号	02/08474
(32)優先日	平成14年7月5日 (2002.7.5)
(33)優先権主張国	フランス(FR)

(71)出願人　591034154
フランス　テレコム
ＦＲＡＮＣＥ　ＴＥＬＥＣＯＭ
フランス国、７５０１５　パリ、プラス・ダルレ、６
(74)代理人　100064908
弁理士　志賀　正武
(74)代理人　100089037
弁理士　渡邊　隆
(74)代理人　100108453
弁理士　村山　靖彦
(74)代理人　100110364
弁理士　実広　信哉

最終頁に続く

(54)【発明の名称】処理中の計算を容易にするための暗号化方法、及び装置

(57)【要約】
本発明は、第２の構成要素(B)により前記秘密鍵に関連付けられたＲＳＡ公開鍵を用いて照合可能な証明書を、第１の構成要素(A)がＲＳＡ秘密鍵(d)を用いて生成する処理において使用するための暗号化方法に関するものである。公開鍵は、第１の指数(e)、及び係数(n)を含む。前記方法において、第１の構成要素(A)は、処理の計算とは無関係に１つの計算が獲得され得る証明書の第１の要素(x)と、証明書の第１の要素(x)に関連付けられると共に、処理のために第１及び第２の構成要素に明確に共有された共通数(c)に依存する証明書の第２の要素(y)とを生成する。第２の構成要素(B)は、証明書の第１の要素(x)が、係数(n)を法として求められた総称数(g)の第１の累乗と、関係式によって関連付けられていることを照合する。



【特許請求の範囲】
【請求項１】
ＲＳＡ秘密鍵(d)に関連付けられたＲＳＡ公開鍵を用いて第２の構成要素(B)によって照合可能な証明書を、第１の構成要素(A)が前記ＲＳＡ秘密鍵(d)を用いて生成するための処理に使用され得る暗号化方法であって、
前記公開鍵が第１の指数(e)と係数(n)とを有すると共に、
－　第１の構成要素(A)が証明書の第１の要素(x)を生成し、かなりの資源を消費するその第１の計算が処理とは無関係に実行され得る過程と、
－　第１の構成要素(A)が、第１の要素(x)に関連付けられると共に、処理のために第１と第２の構成要素により明確に共有された共通数(c)に依存する証明書の第２の要素(y)を生成し、その第２の計算がほとんど資源を消費しない過程と、
－　証明書の第１の要素(x)が、共通数(c)の全部または一部と証明書の第２の要素(y)が乗算された公開鍵の第１の指数(e)との一次結合に等しい第２の指数を有すると共に、係数(n)を法とする総称数(g)の第１の累乗と、関係式を通して関連付けられることを、第２の構成要素(B)が照合する過程とを有する
ことを特徴とする暗号化方法。
【請求項２】
第１の構成要素(A)が識別されることを可能にするために、
－　第１の構成要素(A)により秘密の状態に維持された任意の整数(r)が乗算された公開鍵の第１の指数(e)と等しい第３の指数を有すると共に、係数(n)を法とする総称数(g)の第２の累乗を計算することにより、証明書の第１の要素(x)が第１の構成要素(A)によって生成され、
－　第２の構成要素(B)によって、共通数(c)が安全期間“[0,t-1]”の中から任意に選択されると共に、その場合には証明書の第１の要素(x)が受信された後で送信され、
－　第２の構成要素(B)により照合される関係式が、証明書の第１の要素(x)の累乗と総称数(g)の第１の累乗との間の関係の等式である
ことを特徴とする請求項１に記載の暗号化方法。
【請求項３】
メッセージ(M)が署名されることを可能にするために、
－　メッセージ(M)と、第１の構成要素(A)により秘密の状態に維持された任意の整数(r)が乗算された公開鍵の第１の指数(e)と等しい第３の指数を有すると共に、係数(n)を法とする第２の累乗が計算された総称数(g)とに標準のハッシュ関数を適用することにより、証明書の第１の要素(x)が第１の構成要素(A)によって生成され、
－　共通数(c)が証明書の第１の要素(x)に等しく、
－　第２の構成要素(B)により照合される関係式が、証明書の第１の要素(x)と、メッセージ(M)及び総称数(g)の第１の累乗に適用された標準のハッシュ関数の結果との間の関係の等式である
ことを特徴とする請求項１に記載の暗号化方法。
【請求項４】
第２の構成要素(B)により受信されるメッセージ(M)が第１の構成要素(A)からくることを認証するために、
－　メッセージ(M)と、第１の構成要素(A)により秘密の状態に維持された任意の整数(r)が乗算された公開鍵の第１の指数(e)と等しい第３の指数を有すると共に、係数(n)を法とする第２の累乗が計算された総称数(g)とに標準のハッシュ関数を適用することにより、証明書の第１の要素(x)が第１の構成要素(A)によって生成され、
－　第２の構成要素(B)によって、共通数(c)が安全期間“[0,t-1]”の中から任意に選択されると共に、その場合には証明書の第１の要素(x)が受信された後で送信され、
－　第２の構成要素(B)により照合される関係式が、証明書の第１の要素(x)と、メッセージ(M)及び総称数(g)の第１の累乗に適用された標準のハッシュ関数の結果との間の関係の等式である

ことを特徴とする請求項１に記載の暗号化方法。
【請求項５】
－　任意の整数(r)から共通数(c)が乗算された秘密鍵(d)を減算することにより、証明書の第２の要素(y)が第１の構成要素(A)によって生成され、
－　第２の指数に等しい一次結合が、共通数(c)に関する単一の正の係数と、証明書の第２の要素(y)が乗算された公開鍵の第１の指数(e)に関する単一の正の係数とを有し、
－　照合される関係式において、証明書の第１の要素が単一の指数による累乗とみなされる
ことを特徴とする請求項２から請求項４のいずれか１項に記載の暗号化方法。
【請求項６】
－　共通数(c)が第１の共通数元素(a)と第２の共通数元素(b)とに分割されるので、第１の共通数元素(a)が乗算された任意の整数(r)から第２の共通数元素(b)が乗算された秘密鍵(d)を減算することにより、証明書の第２の要素(y)が第１の構成要素(A)によって生成され、
－　第２の指数に等しい一次結合が、第１の共通数元素(a)に関するゼロの係数と、第２の共通数元素(b)に関する単一の正の係数と、証明書の第２の要素(y)が乗算された公開鍵の第１の指数(e)に関する単一の正の係数とを有し、
－　照合される関係式において、証明書の第１の要素が第１の共通数元素(a)に等しい単一の指数による累乗とみなされる
ことを特徴とする請求項２と請求項４のいずれかに記載の暗号化方法。
【請求項７】
　証明書の第２の要素(y)が、カーマイケル関数(λ)による係数(n)の写像を法として計算されるか、または係数(n)を法として求められた総称数(g)の次数の倍数を法として計算される
ことを特徴とする請求項５と請求項６のいずれかに記載の暗号化方法。
【請求項８】
　任意の数(r)が秘密鍵(d)の値より非常に大きい
ことを特徴とする請求項５と請求項６のいずれかに記載の暗号化方法。
【請求項９】
　任意の整数(r)が、カーマイケル関数(λ)による係数(n)の写像より小さいか、または係数(n)を法として求められた総称数(g)の次数の倍数より小さい
ことを特徴とする請求項７に記載の暗号化方法。
【請求項１０】
　第３の指数が、カーマイケル関数(λ)による係数(n)の写像を法として計算されるか、または係数(n)を法として求められた総称数(g)の次数の倍数を法として計算される
ことを特徴とする請求項５から請求項９のいずれか１項に記載の暗号化方法。
【請求項１１】
　秘密鍵(d)を指数とすると共に、係数(n)を法として累乗された単純な数(G)に等しい総称数(g)が、公開鍵と共に送信される
ことを特徴とする請求項１から請求項１０のいずれか１項に記載の暗号化方法。
【請求項１２】
－　第３の構成要素(C)が、証明書の第２の要素(y)を受信し、証明書の第２の要素(y)を指数とし係数(n)を法として総称数(g)を累乗することによって証明書の第３の要素(Y)を生成すると共に、証明書の第３の要素(Y)を第２の構成要素(B)に送信し、
－　証明書の第１の要素を証明書の第２の要素に関連付ける関係式を照合するために、第２の構成要素(B)が、係数(n)を法として証明書の第３の要素(Y)を第１の指数(e)で累乗すると共に、それの結果に共通数(c)を指数として累乗された総称数(g)を乗算する
ことを特徴とする請求項１から請求項１１のいずれか１項に記載の暗号化方法。
【請求項１３】
　秘密の状態に維持されたＲＳＡ秘密鍵(d)を与えられると共に侵入から保護され、認証

用装置との処理中に前記秘密鍵に関連付けられた公開鍵を用いて、認証要求者用装置(30)が証明書を発行したことの保証をその認証が可能にする証明書を生成するための認証要求者用装置(30)であって、
前記ＲＳＡ公開鍵が第１の指数(e)と係数(n)とを有すると共に、
－　処理とは無関係に、証明書の第１の要素(x)を完全にまたは部分的に生成するように設計されると共に、証明書の第１の要素に関連付けられ、かつ処理に特有の共通数(c)に依存する証明書の第２の要素(y)を生成するように設計される計算手段(37)と、
－　少なくとも証明書の第１及び第２の要素を送信するように設計されると共に、前記共通数(c)を認証者用装置に送信する、または前記共通数を認証者用装置から受信するように設計される通信手段(34)とを有する
ことを特徴とする認証要求者用装置。
【請求項１４】
－　計算手段(37)が、一方で、第１の任意の数(r)を生成すると共に、任意の整数(r)が乗算された公開鍵の第１の指数(e)に等しい第３の指数を有し、係数(n)を法とする総称数(g)の第２の累乗を計算するように設計され、
－　計算手段(37)が、他方で、任意の整数(r)と共通数(c)が乗算された秘密鍵(d)との間の差分を取ることによって、または共通数(c)が共通数元素(a,b)に分割され、第１の共通数元素(a)が乗算された任意の整数(r)から第２の共通数元素(b)が乗算された秘密鍵(d)を減算することによって、証明書の第２の要素(y)を生成するように設計される
ことを特徴とする請求項１３に記載の認証要求者用装置。
【請求項１５】
計算手段(37)が、カーマイケル関数(λ)による係数(n)の写像を法とする操作を実行するか、または係数(n)を法として求められた総称数(g)の次数の倍数を法とする操作を実行するように設計される
ことを特徴とする請求項１４に記載の認証要求者用装置。
【請求項１６】
認証要求者用装置により秘密の状態に維持されたＲＳＡ秘密鍵(d)を与えられて認証要求者用装置から発行された証明書を前記秘密鍵に関連付けられた公開鍵を用いて照合するための認証者用装置(31)であって、
前記ＲＳＡ公開鍵が第１の指数(e)と係数(n)とを有すると共に、
－　証明書の第１の要素(x)と、証明書の第２の要素(y)または第３の要素(Y)とを受信すると共に、証明書の第１の要素と第２または第３の要素とが受信される処理に特有の共通数(c)を、受信または送信するように設計される通信手段(35)と、
－　証明書の第１の要素(x)が、共通数(c)の全部または一部と証明書の第２の要素(y)が乗算された公開鍵の第１の指数(e)との一次結合に等しい第２の指数を有すると共に、係数(n)を法とする総称数(g)の第１の累乗と、関係式を通して関連付けられることを照合するように設計される計算手段(38)とを有する
ことを特徴とする認証者用装置。
【請求項１７】
通信手段が、証明書の第２の要素(y)を受信するように設計されると共に、
計算手段(38)が、第２の指数と総称数(g)の第１の累乗とを計算するように設計される
ことを特徴とする請求項１６に記載の認証者用装置。
【請求項１８】
通信手段が、証明書の第３の要素(Y)を受信するように設計されると共に、
計算手段(38)が、それの結果に共通数(c)を指数として有する第２の累乗が計算された総称数(g)を乗算するために、証明書の第３の要素(Y)を公開鍵の第１の指数(e)で累乗するように設計される
ことを特徴とする請求項１６に記載の認証者用装置。

【発明の詳細な説明】

【技術分野】
【０００１】
この発明は、暗号方式の技術分野に関し、より明確にはいわゆる公開鍵暗号方式に関するものである。
【背景技術】
【０００２】
このタイプの暗号方式において、利用者は、所定の使用に対して一組のキーを所有する。前記キーのペアは、この利用者が秘密の状態に維持する秘密鍵、及びこの利用者が他の利用者に通知する可能性がある関連付けられた公開鍵から構成される。例えば、秘密保持専用の一組のキーの場合、その場合に公開鍵はデータを暗号に変えるために使用され、一方、秘密鍵はそれを解読するため、すなわち、このデータを平文に回復するために使用される。
【０００３】
秘密鍵暗号方式と異なり、安全に保護された通信を確立するために同じ秘密を共有する対話者を必要としない限り、公開鍵暗号方式は非常に広く使用される。しかしながら、セキュリティに関するこの利点には、公開鍵スキーム（schemes）とも呼ばれる公開鍵暗号化方法が、多くの場合秘密鍵スキーム（schemes）とも呼ばれる秘密鍵暗号化方法より１００倍、あるいは１０００倍更に遅いので、性能に関する欠点がつきものである。非常に重要な目標は、従って、標準のマイクロプロセッサカードのような、資源が制限された接触方式または非接触方式の環境においてそれらを使用することができるように、迅速に実行され得る公開鍵暗号化方法を発見することである。
【０００４】
現存する大部分の公開鍵スキームは、演算(または、数論)の分野における数学の問題の難しさに依存している。このように、ＲＳＡ(Rivest, Shamir, Adleman)の数字による署名、及び暗号化スキームの安全性は、同程度のサイズの２個かそれ以上の素数をお互いに掛け合わせることによって非公開で獲得された非常に大きな整数（５００桁を超える）を与えられると共に、これらの素数を回復するための効果的な方法が現存しないという、その整数を因数分解することに対する問題の難しさに基づいている。
【０００５】
特許文献１において説明されたデジタル署名スキームのような他の公開鍵スキームは、それらの安全性に関して、いわゆる“離散的対数問題（discrete logarithm problem）”の難しさに依存している。この問題は、以下のような、その最も一般的な場合に表される。例えば“Ｅ”は演算（すなわち、２つの要素“ａ”と“ｂ”とを有し、“a.b”または“ab”と表示されると共に「“ａ”と“ｂ”との積」と呼ばれるように要素を結合させる関数）が与えられたセットであるとし、更にそれぞれ“ｇ”は“Ｅ”の要素、“ｒ”は大きな整数、“ｙ”は“$y = g^r$”で定義される整数（すなわち、“ｇ・ｇ・．．．．・ｇ”と“ｇ”が“ｒ”回出現する積）とすると、その場合に、“ｇ”及び“ｙ”から“ｒ”を回復することは実行不可能である。多くの場合、使用されるセット“Ｅ”は“ｎ”を法とする整数（整数を“ｎ”で割った余り）のセットであり、ここで“ｎ”は整数、素数、または素数から構成される数である。
【０００６】
本発明は、更に特に、“識別”とも呼ばれる構成要素の認証に関係すると共に、同様にメッセージの認証の技術分野、及び公開鍵の暗号化技術を用いたそのデジタル署名の技術分野に関係する。そのような方法において、“認証要求者（prover）”と呼ばれる認証された構成要素は、秘密鍵または非公開鍵と、関連付けられた公開鍵とを所有する。その認証要求者は、認証値またはデジタル署名を生成するために秘密鍵を使用する。“認証者”と呼ばれる認証を行う構成要素は、認証値またはデジタル署名を照合するのに認証要求者の公開鍵だけを必要とする。
【０００７】
本発明の分野は、それに加えて、更に特にいわゆる“ゼロ知識証明（zero-knowledge）

”と呼ばれた認証方法の分野である。これは、その認証が、それが使用される回数にかかわりなく、認証された構成要素の秘密鍵について何も明らかにしない、証明された方法におけるプロトコルを用いて実行されることを意味する。メッセージ及びこのメッセージのデジタル署名の認証に関して、このタイプのスキームから、標準の技術を用いてどのようにスキームを推論するかが知られている。

【０００８】

本発明の分野は、それに加えて、特にその安全性が、更に整数を因数分解することに対する問題の難しさ、及び離散的対数問題の難しさの両方に依存する方法の分野である。

【０００９】

例えばセントラルサーバの場合、または他の理由により、公開鍵暗号方式を使用するあらゆるシステムにおいて、更に特に、様々な当事者によって実行された多くの計算が、少なくともそれらのうちの１つに対して臨界のパラメータを形成するシステムにおいて、それが、計算の速度を加速するために、多くの場合“暗号用プロセッサ（cryptoprocessor）”と呼ばれる暗号化計算を専門に実行する利用可能なコプロセッサを備えていないか、またはそれが、多くの計算を同時に実行することが可能であるので、本発明は、それらの要素及び／またはそれらの処理の安全性を保護するために適用できる。

【００１０】

主な用途は、クレジットカード（バンクカード）または電子財布による電子決済である。近接通信決済の場合、共通鍵を蓄積しないように、決済端末は公開鍵暗号化方法の使用を促す公共の場所にある。そのようなシステムの総コストを減少させるために、標準のマイクロプロセッサカードであるカード、すなわち、暗号用プロセッサを供給されなかったカード、または標準型である端末自身に含まれる安全性が保護されたマイクロプロセッサ、またはこれらの両方のいずれかにとって、それは望ましいかもしれない。その状況及び採用された暗号化方法によって、現在知られている従来技術は、これらの目的の一方または他方を達成するが、しかし、システムの制限に従いながら、容易に両方が同時に達成されることを可能にするとは限らない。そのような制限の例としては、その決済が１秒未満で達成される、または非接触処理の場合に１５０ミリ秒未満で達成される、または高速道路通行料金の場合に数ミリ秒で達成されることが挙げられる。

【００１１】

現在最も広く使用される暗号化方法は、ＲＳＡ方法である。それは、因数分解の問題に基づいている。様々な場合において標準化されたこのアルゴリズムは、デファクト・スタンダードになった。それは、今後とも優勢なアルゴリズムとして残ることになる。ＰＫＩ基盤（Public Key Infrastructure：公開鍵基盤）のような、多くの製品、システム、及びインフラ基盤が、このアルゴリズムから、及びアルゴリズムが使用する鍵の形式から設計された。

【００１２】

知られているように、このアルゴリズムによれば、公開鍵は、一組の整数“(n,e)”から構成されると共に、秘密鍵は整数“d”から構成される。係数“n”（法“n”）は、それを因数分解することができない十分に大きい整数である。公開鍵“(n,e)”を知るあらゆる構成要素“B”が、“n”を法として整数“W'”を“e”乗する（整数“W'”を“e”乗して“n”で割った余りを取る）ことによって整数“W”を回復することを可能にするために、単独で秘密鍵“d”を保持する構成要素“A”が、「“n”を法とする整数“W”の“d”乗（整数“W”の“d”乗を“n”で割った余り）」に等しい整数“W'”を生成する。

【００１３】

メッセージ署名“M”を使用する方法において、整数“W”は、一般に既知のハッシュ関数のような関数によるメッセージの写像である。その認証要求者は、その署名が整数“W'”である構成要素“A”であって、その認証者は、署名“W'”に基づいて発見された整数が既知の関数によるメッセージの写像であるかを照合する構成要素“B”である。

【００１４】

識別の方法において、整数“W”は、一般に認証者である構成要素“B”により送信され

た要求を構成する。認証要求者である構成要素“Ａ”によって生成された数“Ｗ'”は、この要求に対する応答を構成する。

【００１５】

メッセージ“Ｍ”を認証する方法において、整数“Ｗ”は、一般的にメッセージ“Ｍ”の写像と、構成要素“Ｂ”で構成される認証者によって送信された要求との結合から生じる。認証要求者である構成要素“Ａ”によって生成された数“Ｗ'”は、この要求に応答して本物の署名を構成する。

【特許文献１】仏国特許出願公開第716058号明細書

【発明の開示】

【発明が解決しようとする課題】

【００１６】

しかしながら、ＲＳＡアルゴリズムは、認証要求者または署名者によって実行されるべき多くの処理から生じる問題を有している。これらの処理を実行するマイクロプロセッサカード上で、１秒未満で完全な計算を実行するために、暗号用プロセッサをカードに加えることが必要である。しかしながら、暗号用プロセッサの製作及び導入には、マイクロプロセッサカードのコストを増大させる多大なコストがかかる。同様に暗号用プロセッサが多量の電流を消費するということも知られている。端末によるカードを供給することは、非接触インタフェースの場合に技術的難しさをもたらす可能性がある。同様に暗号用プロセッサの追加が、技術的解決法を発見することが難しい欠点を提示する、消費された電流のスペクトル解析による物理的攻撃を容易にするということが知られている。更に、もしカードが暗号用プロセッサを与えられるとしても、上述の例にあるように、処理時間が非常に短いことが必要とされるアプリケーションにおいて、その計算はまだ遅すぎると証明される可能性がある。

【００１７】

本発明の目的は、認証及びデジタル署名方法のような公開鍵の暗号化方法を具体的に述べることである。より正確には、本発明の目的は、更に暗号用プロセッサを使用する必要性を回避する計算の大部分が前もって実行されることを可能にする一方で、少なくともＲＳＡアルゴリズムの安全性のレベルと等しい安全性のレベルで、ＲＳＡアルゴリズムと同じ鍵を使用することである。

【課題を解決するための手段】

【００１８】

ＲＳＡ秘密鍵に関連付けられたＲＳＡ公開鍵を用いて第２の構成要素によって照合可能な証明書を、第１の構成要素が前記ＲＳＡ秘密鍵を用いて生成するための処理に使用され得ると共に、前記公開鍵が第１の指数と係数とを有する暗号化方法を考慮すると、本発明による方法は、

－　第１の構成要素が証明書の第１の要素を生成し、かなりの資源を消費するその第１の計算が処理とは無関係に実行され得る過程と、

－　第１の構成要素が、第１の要素に関連付けられると共に、処理のために第１と第２の構成要素により明確に共有された共通数に依存する証明書の第２の要素を生成し、その第２の計算がほとんど資源を消費しない過程と、

－　証明書の第１の要素が、共通数の全部または一部と証明書の第２の要素が乗算された公開鍵の第１の指数との一次結合に等しい第２の指数を有すると共に、係数を法とする総称数の第１の累乗と、関係式を通して関連付けられることを、第２の構成要素が照合する過程と

を有するという点で注目すべきである。

【００１９】

鍵がＲＳＡタイプの鍵であるという事実は、何の変更も加えることなく、鍵生成ソフトウェア、マイクロプロセッサのメモリ領域の記述、公開鍵証明書フォーマット等のような多くの既存製品、開発物、またはインフラストラクチャを使用することができるという利点を有する。

【００２０】
処理とは無関係に、証明書の第１の要素が完全にまたは部分的に計算され得るので、第１の構成要素は、安全性を保証するために、この複合的計算の実行を秘密の状態に維持しながら、処理の前に複合的な計算を実行する可能性を有する。このように、第１の構成要素が、暗号用プロセッサの資源のような強力な資源を必要とせずに、処理の初めから直ちにそのような証明書の第１の要素を迅速に生成するということが理解される。その場合には、単純な処理を通じて、処理によって明確に共有された共通数に証明書の第２の要素を依存させるために、証明書の第１の要素と関係づけることにより、第１の構成要素のみが証明書の第２の要素を生成することができる。短時間におけるこれらの単純な処理の第１の構成要素による可能な限りの実行は、更に高いレベルの安全を保ちながら、処理が減速することを回避する。

【００２１】
処理の目的は、メッセージに署名するため、またはメッセージを認証するために、制限されることなく第１の構成要素を識別することであっても良い。

【００２２】
特に、第１の構成要素が識別されることを可能にするために、
－　第１の構成要素により秘密の状態に維持された任意の整数が乗算された公開鍵の第１の指数と等しい第３の指数を有すると共に、係数を法とする総称数の第２の累乗を計算することにより、証明書の第１の要素が第１の構成要素によって生成され、
－　第２の構成要素によって、共通数が安全期間の中から任意に選択されると共に、その場合には証明書の第１の要素が受信された後で送信され、
－　第２の構成要素により照合される関係式が、証明書の第１の要素の累乗と総称数の第１の累乗との間の関係の等式である
ことを特徴とする。

【００２３】
その実行が秘密の状態に維持される複合的な計算は、この場合、証明書の第１の要素を生成するために総称数の第２の累乗を計算することと関連付けられる。処理中に任意に選択された共通数の選択は、この処理のスピードを損なわない。

【００２４】
特に、メッセージが署名されることを可能にするために、
－　メッセージと、第１の構成要素により秘密の状態に維持された任意の整数が乗算された公開鍵第１指数と等しい第３の指数を有すると共に、係数を法とする第２の累乗が計算された総称数とに標準のハッシュ関数を適用することにより、証明書の第１の要素が第１の構成要素によって生成され、
－　共通数が証明書の第１の要素に等しく、
－　第２の構成要素により照合される関係式が、共通数と、メッセージ及び総称数の第１の累乗に適用された標準のハッシュ関数の結果との間の関係の等式である
ことを特徴とする。

【００２５】
その実行が秘密の状態に維持される複合的な計算は、この場合、証明書のポテンシャルを生成するために総称数の第２の累乗を計算することと関連付けられる。メッセージ及びこの証明書のポテンシャルに対する標準のハッシュ関数の応用は、もはや多量の資源を消費しない。この場合、証明書の第２の要素の伝送、及び第２の構成要素と共有された共通数に等しい証明書の第１の要素の伝送を行う処理の前に、第１の構成要素は証明書のポテンシャルを計算しても良く、その場合には、第１の構成要素はメッセージの署名の伝送を実行する。

【００２６】
特に、第２の構成要素により受信されるメッセージが第１の構成要素からくることを認証するために、
－　メッセージと、第１の構成要素により秘密の状態に維持された任意の整数が乗算され

た公開鍵第１指数と等しい第３の指数を有すると共に、係数を法とする第２の累乗が計算された総称数とに標準のハッシュ関数を適用することにより、証明書の第１の要素が第１の構成要素によって生成され、
－　第２の構成要素によって、共通数が安全期間の中から任意に選択されると共に、その場合には証明書の第１の要素が受信された後で送信され、
－　第２の構成要素により照合される関係式が、証明書の第１の要素と、メッセージ及び総称数の第１の累乗に適用された標準のハッシュ関数の結果との間の関係の等式であることを特徴とする。

【００２７】

秘密の状態に維持される複合的な計算は、この場合、証明書の第１の要素を生成するために総称数の第２の累乗を計算することと関連付けられる。第２の構成要素によって処理中に任意に選択された共通数の選択は、この処理のスピードを損なわない。

【００２８】

一般的に、処理の前に実行され得る複合的な計算は、条件として直接秘密鍵を伴わないと共に、従ってその結果は秘密鍵に関する情報を与えない。

【００２９】

更に特に、暗号化方法は、
－　任意の整数から共通数が乗算された秘密鍵(d)を減算することにより、証明書の第２の要素が第１の構成要素によって生成され、
－　第２の指数に等しい一次結合が、共通数に関する単一の正の係数と、証明書の第２の要素が乗算された公開鍵第１指数に関する単一の正の係数とを有し、
－　照合される関係式において、証明書の第１の要素が単一の指数による累乗とみなされる
という点で注目すべきである。

【００３０】

もう一つの方法として、好ましくは、共通数が第２の構成要素によって選択されるとき、暗号化方法は
－　共通数が第１の共通数元素と第２の共通数元素とに分割されるので、第１の共通数元素が乗算された任意の整数から第２の共通数元素が乗算された秘密鍵を減算することにより、証明書の第２の要素が第１の構成要素によって生成され、
－　第２の指数に等しい一次結合が、第１の共通数元素に関するゼロの係数と、第２の共通数元素に関する単一の正の係数と、証明書の第２の要素が乗算された公開鍵第１指数に関する単一の正の係数とを有し、
－　照合される関係式において、証明書の第１の要素が第１の共通数元素に等しい単一の指数による累乗とみなされる
という点で注目すべきである。

【００３１】

上述の単純な減算処理及び乗算処理は、処理中に証明書の第２の要素を迅速に計算すると共に、異なった証明書の第１の要素に関係する証明書の第２の要素を、異なる任意の数によって毎回生成することにより、秘密鍵に関するあらゆる情報を与えることなく処理を数回繰り返すことを可能にする。

【００３２】

暗号化方法は、都合良く、証明書の第２の要素がカーマイケル（Carmichael）関数による係数の写像を法として計算されるか、または係数を法として求められた総称数の次数の倍数を法として計算されるという点で、注目すべきである。

【００３３】

任意の整数は、秘密鍵より非常に大きくなるように選択されても良い。もし前の段落において言及された利点が適用されないならば、秘密鍵の値より非常に大きな値であることが任意の整数には必要である。都合良く、任意の数を指数として有する指数計算のために必要とされる処理の数を減少させるために、任意の整数は、カーマイケル関数による係数

の写像より小さいか、または係数を法として求められた総称数の次数の倍数より小さい。そのような任意の数は、秘密鍵に関して攻撃可能な情報を全く与え得ない。

【００３４】

このように獲得された証明書の第２の要素のサイズを減少させることにより、安全性を損なわずに第２の構成要素によって実行されるべき計算をスピードアップすることが可能である。

【００３５】

暗号化方法は、同様に都合良く、第３の指数がカーマイケル関数による係数の写像を法として計算されるか、または係数を法として求められた総称数の次数の倍数を法として計算されるという点で、注目すべきである。

【００３６】

このように獲得された第３の指数のサイズを減少させることにより、安全性を損なわずに第１の構成要素によって実行されるべき計算をスピードアップすることが可能である。

【００３７】

総称数に割り当てられる値“２”は、あらゆる総称数の累乗に対する指数計算を容易にする。既知のハッシュ関数を、係数及び公開鍵の第１の指数に適用することにより、各第１の構成要素を区別することを可能にする総称数に、小さな値が同様に割り当てられても良い。

【００３８】

第１の構成要素の区別に関して、暗号化方法に対する評価できる改善は、公開鍵と共に、秘密鍵を指数とし係数を法として累乗された単純な数に等しい総称数が送信されることである。

【００３９】

その場合に第１の構成要素が実行しなければならない全てのことは、任意の整数が乗算された公開鍵第１指数に等しい第３の指数を有すると共に、係数を法とする総称数の第２の累乗を計算することによる結果と同じ結果を獲得するために、任意の数を指数とし係数を法として単純な数を累乗することである。単純な数に値“２”を割り当てることによって、複合的計算が処理の前または処理中に実行されるか否かに拘らず、複合的計算はかなりスピードアップされる。

【００４０】

暗号化方法に対する更に評価できる改善は、

－　第３の構成要素が、証明書の第２の要素を受信し、証明書の第２の要素を指数とし係数を法として総称数を累乗することによって証明書の第３の要素を生成すると共に、証明書の第３の要素を第２の構成要素に送信し、

－　証明書の第１の要素を証明書の第２の要素に関連付ける関係式を照合するために、第２の構成要素が、係数を法として証明書の第３の要素を第１の指数で累乗すると共に、それの結果に共通数を指数として累乗された総称数を乗算する

ことによる改善である。

【００４１】

第３の構成要素は、認証の完全性を損なわずに第２の構成要素の負担を軽減することを可能にする。

【００４２】

秘密の状態に維持されたＲＳＡ秘密鍵を与えられると共に、認証用装置との処理中に前記秘密鍵に関連付けられた公開鍵を用いて、認証要求者用装置が前記証明書の発行元であることの保証をその認証が可能にする証明書を生成するために、侵入から保護された認証要求者用装置を考慮すると、前記ＲＳＡ公開鍵は第１の指数と係数とを有し、本発明による認証要求者用装置は、

－　かなりの資源を消費するその第１の計算が処理とは無関係に実行され得て、証明書の第１の要素を生成するように設計されると共に、証明書の第１の要素に関連付けられ、かつ処理に特有の共通数に依存する証明書の第２の要素を生成するように設計される計算手

段と、
－　少なくとも証明書の第１及び第２の要素を送信するように設計されると共に、前記共通数を認証者用装置に送信する、または前記共通数を認証者用装置から受信するように設計される通信手段とを有する
という点で注目すべきである。
【００４３】
本発明による認証要求者用装置は、
－　計算手段が、一方で、任意の数を生成すると共に、任意の整数が乗算された公開鍵第１指数に等しい第３の指数を有し、係数を法とする総称数の累乗を計算するように設計され、
－　計算手段が、他方で、任意の整数(r)と共通数(c)が乗算された秘密鍵(d)との間の差分を取ることによって、証明書の第２の要素(y)を生成するように設計される
という点で注目すべきである。
【００４４】
もう一つの方法として、計算手段は、カーマイケル関数による係数の写像を法とする操作を実行するか、または係数を法として求められた総称数の次数の倍数を法とする操作を実行するように設計される。
【００４５】
認証要求者用装置により秘密の状態に維持されたＲＳＡ秘密鍵(d)を与えられて認証要求者用装置から発行された証明書を前記秘密鍵に関連付けられた公開鍵によって照合するための認証者用装置を考慮すると、前記ＲＳＡ公開鍵は第１の指数と係数とを有し、本発明による認証者用装置は、
－　証明書の第１の要素と、証明書の第２の要素または第３の要素とを受信すると共に、証明書の第１の要素と第２または第３の要素とが受信される処理に特有の共通数を、受信または送信するように設計される通信手段と、
－　証明書の第１の要素が、共通数の全部または一部と証明書の第２の要素が乗算された公開鍵第１指数との一次結合に等しい第２の指数を有すると共に、係数を法とする総称数の第１の累乗と、関係式を通して関連付けられることを照合するように設計される計算手段とを有する
という点で注目すべきである。
【００４６】
特に、認証者用装置は、通信手段が証明書の第２の要素を受信するように設計されると共に、計算手段が第２の指数、及び総称数の前記第１の累乗を計算するように設計されるという点で注目すべきである。
【００４７】
もう一つの方法として、認証装置は、通信手段が証明書の第３の要素を受信するように設計されると共に、計算手段は、それの結果に共通数を指数として有する第２の累乗が計算された総称数を乗算するために、証明書の第３の要素を公開鍵第１指数で累乗するように設計されるという点で注目すべきである。
【００４８】
本発明は、添付された図を参照して以下に示された実施例から更によく理解されることになる。
【発明を実施するための最良の形態】
【００４９】
ここに示された実施例は、構成要素の認証方法、または構成要素の識別方法である。それによって認証要求者“Ａ”はその信頼性を認証者“Ｂ”に証明することが可能となる。この方法は、以下で説明されるように、メッセージ、またはデジタルメッセージ署名を認証する方法に変更されても良い。その安全性は、大きな整数を因数分解することの難しさに依存している。この難しさは、ＲＳＡアルゴリズムの安全性が依存する問題の難しさと少なくとも同じくらい難しいとして当業者に知られている。照合のタスク（作業）が促進さ

れることを可能にする１つのオプションにおいて、方法の安全性はＲＳＡの安全性に相当する。

【００５０】

素数は“１”及びそれ自身のみで割り切れる数であるということが思い出されることになる。あらゆる正の整数“ｚ”のオイラー関数“φ(z)”は、“ｚ”より小さいと共に“ｚ”と互いに素である、すなわち“ｚ”に関して“１”以外の公約数を持たない正の整数のセットの基数を与えることも同様に思い出されることになる。あらゆる整数“ｕ”が関係式“{u^v = 1 modulo w}”、すなわち、知られているように、“ｗ”による“u^v”の整数分割の残りが“１”に等しいという関係を満たすように、あらゆる正の整数“ｗ”のカーマイケル関数“λ(w)”が正確に正の整数“ｖ”の最小値を与えるということが同じく思い出されることになる。

【００５１】

上述の目的及び結果によれば、この方法はＲＳＡの鍵を使用する。認証要求者用装置を構成するために、第１の構成要素“Ａ”は、第一に、認証者用装置を構成するあらゆる第２の構成要素“Ｂ”に対して公開された公開鍵を所有する。第１の構成要素“Ａ”は、第二に、秘密の状態に維持された秘密鍵を所有する。公開鍵は、係数“ｎ”及び第１の指数“ｅ”を有する。秘密鍵は、第２の指数“ｄ”を有する。係数“ｎ”は、２個か、またはそれ以上の素数の積に等しい整数である。数“ｎ”が２個の素数“ｐ”及び“ｑ”の積であるとき、その場合、“φ(n) = (p-1)(q-1)”である。多くのＲＳＡの記述は、係数“ｎ”、第１の指数“ｅ”、及び第２の指数“ｄ”が方程式“{ed = 1 modulo φ(n)}”を満足させることを指定する。方程式“{ed = 1 modulo φ(n)}”が満足されているとき、その場合には方程式“{ed = 1 modulo λ(n)}”が満足されていることは当業者に良く知られている。

【００５２】

更に一般的に、その方法は、方程式“{ed = 1 modulo λ(n)}”を満たす秘密鍵“ｄ”と関連付けられたあらゆる公開鍵“(n,e)”に対する安全性と同じレベルで機能する。

【００５３】

全てのオプションにおいて、認証要求者“Ａ”の証明書、すなわちその身元、その公開鍵、その公開鍵証明書等が第１の構成要素によって与えられるということを照合するのに必要とされる全ての公のパラメータを、認証者“Ｂ”が既に知っていると仮定されている。

【００５４】

構成要素“Ｂ”による構成要素“Ａ”の識別は、図１を参照してここで説明されたプロトコルを“ｋ”回繰り返すことによって実行される。数“ｋ”は、指数“ｅ”より小さいかまたは等しい整数“ｔ”と共に一組の安全性のパラメータを定義する、正の整数である。

【００５５】

第１のステップ９において、構成要素“Ａ”は、“ｄ”より非常に大きい第１の任意の整数“ｒ”を生成し、“$x = g^{er} \pmod n$”を計算すると共に“ｘ”を構成要素“Ｂ”に送信する。既知の方法において、構成要素“Ａ”及び構成要素“Ｂ”は、コンピュータ、またはチップカードタイプの構成要素である。整数“ｇ”は、構成要素“Ａ”及び構成要素“Ｂ”によって知られている総称数である。“２”に等しい総称数“ｇ”の値は、指数計算を容易にする。総称数“ｇ”は、同様に、例えば“ｈ”が全てに知られているハッシュ関数である“g = h(n,e)”のような、認証要求者の公開鍵の関数でも良い。総称数“ｇ”は、同様に、構成要素“Ａ”によって決定され、その後その公開鍵と共に送信されても良い。例えば、構成要素“Ａ”は、単純な数“Ｇ”を“ｄ”乗すると共に、その結果は“$g^e \pmod n = G$”のような数“ｇ”を与える。総称数“ｇ”が構成要素“Ａ”によって最終的に計算されるので、この場合“$x = G^r \pmod n$”のように“ｘ”の計算は単純化される。指数計算を容易にする“２”に等しい単純な数“Ｇ”の値は、更に特に有利である。すなわち、式“(mod n)”は“ｎ”を法とすること、すなわち知られているように、計算の結果が、一般的に係数と呼ばれる整数“ｎ”による問題の演算の結果の整数分割の残りに等しいことを意味する。ここで、任意の数“ｒ”を生成する構成要素のみが数“ｘ”を生成することが可能であるの

で、整数“ｘ”は、証明書の第１の要素を構成する。任意の数“ｒ”は、それを生成する構成要素によって通知されない。既知の数論から、総称数“ｇ”または単純な数“Ｇ”の認識、及び係数“ｎ”の認識が、数“ｘ”から数“ｒ”が回復されることを可能にしないように、数“ｒ”は十分に大きいものに選ばれる。

【００５６】

構成要素“Ｂ”による証明書の第１の要素“ｘ”の受信は遷移１０を有効とし、その場合にそれは第２のステップ１１をアクティブにする。

【００５７】

ステップ１１において、構成要素“Ｂ”は、安全期間（the security interval）と呼ばれる期間“[0,t-1]”の中から任意に選択された整数“ｃ”を構成要素“Ａ”に送信する。このように、数“ｃ”は、構成要素“Ａ”及び構成要素“Ｂ”、更に対話を構成要素“Ａ”及び構成要素“Ｂ”の間に浸透させている他の構成要素に共通である。

【００５８】

構成要素“Ａ”による共通数“ｃ”の受信は遷移１２を有効とし、その場合にそれは第３のステップ１３をアクティブにする。

【００５９】

ステップ１３において構成要素“Ａ”は、“ｙ＝ｒ-ｄｃ”を計算する。このように、構成要素“Ａ”は、数“ｒ”と、掛け算の係数が共通数“ｃ”である数“ｄ”との一次結合の形式で表された秘密鍵の写像“ｙ”を生成する。任意の数“ｒ”が非常に大きいと共に通知されないので、写像“ｙ”の認識は積“ｄｃ”が回復されることを可能にせず、従って、その結果構成要素“Ａ”により秘密の状態に維持されたままである秘密鍵数“ｄ”の回復を防止する。構成要素“Ａ”のみが数“ｄ”を知っているので、構成要素“Ａ”のみが、共通数“ｃ”を結びつける写像を生成し得る。

【００６０】

ここで説明されたプロトコルを考慮すると、偽物は、秘密鍵“ｄ”の秘密を知らずに構成要素“Ａ”になりすまそうと試みる構成要素である。整数の因数分解が難しい問題であるとき、検出されない偽物の確率が“1/kt”に等しいということが証明され得る。これらのプロトコルの安全性は、従ってＲＳＡの安全性と少なくとも同じくらい高い。多くのアプリケーションに対して、積“kt”は、例えば“2^{16}”の次数の認証文脈の中で、比較的小さいものに選ばれても良い。

【００６１】

安全性のパラメータのペアである“ｋ”及び“ｔ”のあらゆる値が見込まれる。好ましくは、“ｋ＝１”及び“ｔ＝ｅ”であり、その場合に、上で定義された確率は“1/e”に等しいと共に、適用されるべき認証方程式は１つだけである。“ｅ＝65537”のようなＲＳＡの公の指数の値、すなわち“2^{16}+1”は多くのアプリケーションに適している。

【００６２】

構成要素“Ｂ”による証明書の第２の要素“ｙ”の受信は遷移１６を有効とし、その場合にそれは第４のステップ１７をアクティブにする。

【００６３】

ステップ１７において、構成要素“Ｂ”は、“$g^{ey+c} = x(\mathrm{mod}\ n)$”であるかどうかを照合する。上述のように、証明書の第２の要素が秘密鍵“ｄ”に関する情報を通知しないが、証明書の第２の要素“ｙ”は“ey + c = e(r - dc) + c”のようになる。従って、指数を共通数“ｃ”と積“ey”の一次結合として総称数を累乗することにより、その場合には“$g^{ey+c} = g^{er}(g^{-ed+1})^{c} = x(\mathrm{mod}\ n)$”となる。更に、数論によれば総称数“ｇ”が秘密鍵に関する情報を通知しないが、総称数“ｇ”は、実際“$(g^{dc})^{e} = g^{c}(\mathrm{mod}\ n)$”のようになる。

【００６４】

このように、どんな場合も“ｒ”の通知なしで、等式“$(g^{y})^{e}g^{c} = (g^{r})^{e} = x(\mathrm{mod}\ n)$”は、構成要素“Ａ”が“ｄ”を知っていることを証明する。

【００６５】

この照合は、ステップ１１の終わりまたはそれの前にでも、前もって“$v' = g^{c} (mod\ n)$”を計算することによってスピードアップされる。

【００６６】

このように、第４のステップにおいて、“Ｂ”は、もはや“$g^{ey} v' = x (mod\ n)$”であるかどうかを照合する必要はない。“Ｂ”が“ｙ”を受信するとき、ステップ１１において“$G^{y} v' = x (mod\ n)$”であるかどうかを照合するために、最終的に“$G = g^{e} (mod\ n)$”を計算することは“Ｂ”にとって有利である。認証計算を最適化する他の可能な方法は、以下の説明において与えられることになる。

【００６７】

この基礎的プロトコルを最適化する多くの異なる方法が実行できる。例えば、“$x = g^{e^{r}} (mod\ n)$”は、“$x = g^{-er} (mod\ n)$”と交換されても良く、その場合に、認証方程式は“$g^{ey+c} x = 1 (mod\ n)$”となる。

【００６８】

更に、例えば、“ｃ”を一組の正または負の整数“(a,b)”と交換すると共に“$y = r - dc$”を“$y = ar - bd$”と交換することが可能であり、その場合に、認証方程式は“$g^{ey+b} = x^{a} (mod\ n)$”となる。

【００６９】

もし係数“ｎ”の素数因数が“Ａ”から分かる場合、第１のステップは、いわゆる“中国人剰余（Chinese remainders）”技術を用いてスピードアップされても良い。

【００７０】

第１のステップは、前もって実行されても良い。更に、“ｘ”の“ｋ”値は、“Ａ”の公開鍵の一部を形成しても良く、その場合に、プロトコルは直接第２のステップにおいて開始する。“ｘ”のこれらの値は、信頼するに足る外部の構成要素によって計算されると共に、構成要素“Ａ”に記憶されても良い。

【００７１】

証明書の第１の要素の事前の計算値が公開鍵に結合されるとき、処理の中のプロトコルは、直接ステップ１１と同時に開始する。ステップ１７において、“Ｖ”に等しい証明書の第１の要素“ｘ”の値が存在するかどうかを、構成要素“Ｂ”がそれぞれに対して照合する、ステップ１１及びステップ１３の反復の数“ｋ”を決定するのは構成要素“Ｂ”である。更に構成要素“Ａ”は、証明書の第１の要素と対応する任意の数を知る唯一の構成要素である。

【００７２】

事前の計算値の最大の数を構成要素“Ａ”のメモリに記憶することができるように、特に、構成要素“Ａ”がチップカードの超小型回路に統合されるとき、クレジットカード、または携帯電話の場合には、数“ｘ”は、“ｆ”が例えば暗号化ハッシュ関数に等しい（または暗号化ハッシュ関数を含む）関数である値“$f(x)$”と交換されても良く、その場合に、認証方程式は“$f(g^{ey+c} (mod\ n)) = f(x)$”となる。

【００７３】

全ての、またはいくらかの上述の変形例は結合されても良い。

【００７４】

方法に対する１つの有益な改良は、カーマイケル関数による係数ｎの写像“$\lambda(n)$”を構成要素“Ａ”のメモリに記憶することである。

【００７５】

それによって認証方程式を修正せずに認証時間を減少させるために、証明書の第２の要素“ｙ”のサイズを減少させるように、証明書の第２の要素“ｙ”はステップ１３において“$\lambda(n)$”を法とする計算が実行される。この実施方法において、任意の数“ｒ”は、“$\lambda(n)$”より小さくなるように、ステップ１１において有利に選択される。更に一般的に、式“$\{y = r - dc\}$”は、あらゆる式“$\{y = r - dc - i\lambda(n)\}$”と交換されても良く、ここで“ｉ”はあらゆる整数、好ましくは正の整数である。

【００７６】

ステップ１１の実行をスピードアップするために、総称数“ｇ”に適用される指数の演算より前に、積“ｅｒ”が“λ(n)”を法として計算される。

【００７７】

同等の手段は、“λ(n)”を“ｎ”を法とする“ｇ”の次数と交換すること、すなわち“ｎ”を法として“g^l=1（gの「エル」乗＝「数字の１」）”となるような最も小さいゼロでない整数“ｌ「エル」”、または、より一般的には、この次数“ｌ”のあらゆる倍数と交換することから構成される。

【００７８】

図５を参照すると、構成要素“Ｂ”によって実行された認証計算は、いかなる安全性の損失もなしに、同様に“Ｂ”以外のあらゆる構成要素に部分的に委託されても良い。この場合、“Ａ”は、証明書の第２の要素“ｙ”を、これ以外の他の構成要素“Ｃ”に供給する。構成要素“Ｃ”は、証明書の第２の要素“ｙ”から証明書の第３の要素“Ｙ”を生成すると共に、証明書の第３の要素“Ｙ”を構成要素“Ｂ”に送信する。第一に、積“ｄｃ”が任意の数“ｒ”によって“マスクされている”ので、“ｙ”を知ることは“ｄ”に関する情報を提供しない。第二に、詐欺師が全ての部分から、すなわち、第１の構成要素“Ａ”によって排他的に生成された証明書の第２の要素“ｙ”なしで、“Ｙ”を生成することは実質的に不可能である。こういうわけで、もしその因数分解が難しい問題であるならば、“ｎ”，“ｅ”，“ｘ”，及び“ｃ”を与えられて第４のステップの認証方程式を満たす“Ｙ”の値を求めることは実行可能ではない。

【００７９】

公開鍵は、ペア“(n,e)”であると共に、構成要素“Ｂ”による構成要素“Ａ”の認証または識別は、ここで説明されたプロトコルを“ｋ”回繰り返すことによって実行され、ここでは“Ｃ”は“Ｂ”以外のあらゆる構成要素を意味する。従来技術の他のプロトコルと比較すると、例えば、離散的対数の場合において、公開鍵は“(n，e，g，v)”の四つ組であり、公開鍵のコンポーネントの数の減少は、安全性を損なわずに、実行されるべき演算の数を減少する。都合良く、本発明によれば、ここで使用される公開鍵はＲＳＡタイプの鍵であり、記述されたプロトコルは、広く開発されたＲＳＡの文脈に容易に統合される。

【００８０】

その方法は、図１を参照してステップ１３に至るまでに説明された方法と同じ方法で実行される。図５を参照すると、構成要素“Ａ”が秘密鍵“ｄ”の写像“ｙ”を中間の構成要素“Ｃ”に送信するという点でステップ１３は修正される。上述のように、写像“ｙ”は秘密鍵に関する情報を与えない。

【００８１】

構成要素“Ｃ”による写像“ｙ”の受信は遷移１４を有効とし、従ってそれは第５のステップ１５をアクティブにする。

【００８２】

ステップ１５において、証明書の第３の要素“$Y = g^y \pmod n$”を計算すると共に、“Ｙ”を“Ｂ”に送信するのは、この場合中間の構成要素“Ｃ”である。

【００８３】

その手続きは、図１を参照して遷移１６及びステップ１７によって説明されたのと同じ方法で継続される。しかしながら、第２の構成要素“Ｂ”が、直ちに証明書の第３の要素“Ｙ”を指数“ｅ”で累乗すると共に、それの結果に“$g^c \pmod n$”を乗算しさえすればよいように、ステップ１７は修正される。

【００８４】

物理的に、中間の構成要素“Ｃ”は、例えば、必ずしも安全性が保護されているとは限らない、チップカードのような認証要求者のセキュリティ装置（保護装置）、決済端末のような認証者のセキュリティ装置、さもなければコンピュータのような別の装置に含まれているチップに組み込まれる。その安全性は、構成要素“Ｃ”がそれ自身により適当な値“Ｙ”、すなわち認証方程式が満足されていることを発見することができないという事実に依存している。

【００８５】
上述のプロトコルは、メッセージ認証プロトコル、またはディジタル署名スキームに変えられても良い。図３は、第２の構成要素“Ｂ”によって受信されたメッセージ“Ｍ”が第１の構成要素“Ａ”により送信されたことを認証するのを可能にする方法のステップを示す。
【００８６】
第１のステップ２０において、構成要素“Ａ”は、“ｄ”より非常に大きい第１の任意の整数“ｒ”を生成すると共に、証明書の第１の要素の場合には、ステップ９と同様に“$P = g^{er} \pmod n$”のような式を使用して証明書のポテンシャル“Ｐ”を計算する。“Ｐ”を構成要素“Ｂ”に送信する代りに、構成要素“Ａ”は、例えば暗号化ハッシュ関数に等しい関数“ｈ”を数“Ｐ”と共同でメッセージ“Ｍ”に適用するか、または“$x = h(P,M)$”のような暗号化ハッシュ関数を組み込むことによって証明書の第１の要素“ｘ”を生成する。
【００８７】
次に、構成要素“Ａ”は、メッセージ“Ｍ”及び証明書の第１の要素“ｘ”を構成要素“Ｂ”に送信する。
【００８８】
構成要素“Ｂ”によるメッセージ“Ｍ”及び証明書の第１の要素“ｘ”の受信は遷移２１を有効とし、それは第２のステップ１１をアクティブにする。その手続きは、その場合には、図１または図５のいずれかを参照して説明されたのと同じ方法で続く。
【００８９】
ステップ１１において、構成要素“Ｂ”は、安全期間と呼ばれる期間“[0,t-1]”の中から任意に選択された整数“ｃ”を構成要素“Ａ”に送信する。このように、数“ｃ”は、構成要素“Ａ”及び構成要素“Ｂ”、更に対話を構成要素“Ａ”及び構成要素“Ｂ”の間に浸透させている他の構成要素に共通である。
【００９０】
構成要素“Ａ”による共通数“ｃ”の受信は遷移１２を有効とし、その場合にそれは第３のステップ１３をアクティブにする。
【００９１】
ステップ１３において構成要素“Ａ”は“$y = r - dc$”を計算する。このように、構成要素“Ａ”は、数“ｒ”と、掛け算の係数が共通数“ｃ”である数“ｄ”との一次結合の形式で表された秘密鍵の写像“ｙ”を生成する。任意の数“ｒ”が非常に大きいと共に通知されないので、写像“ｙ”の認識は積“ｄｃ”が回復されることを可能にせず、従って、その結果構成要素“Ａ”により秘密の状態に維持されたままである秘密鍵数“ｄ”の回復を可能にしない。構成要素“Ａ”のみが数“ｄ”を知っているので、構成要素“Ａ”のみが、共通数“ｃ”を結びつける写像を生成し得る。図３に示された例において、構成要素“Ａ”は、秘密鍵写像“ｙ”を構成要素“Ｂ”に送信するが、しかし、図５における例と同様にそれを中間の構成要素“Ｃ”に送信しても良い。上述のように、写像“ｙ”は秘密鍵に関する情報を与えない。
【００９２】
構成要素“Ｂ”による写像“ｙ”の受信は遷移１６を有効とし、その場合にそれは第４のステップ２２をアクティブにする。
【００９３】
ステップ２２において、構成要素“Ｂ”は、ステップ１７と同様に、式“$V = g^{c+ey} \pmod n$”によって認証値“Ｖ”を計算すると共に、その場合には、認証方程式“$h(V,M) = x$”によって証明書の第２の要素が証明書の第１の要素と適合することを照合する。
【００９４】
関数“ｆ”を使用する変形例において、認証方程式は“$h(f(g^{c+ey} \pmod n),M) = x$”となる。
【００９５】
関数“ｆ”を使用すると共に、中間の構成要素“Ｃ”を包含する変形例において、認証方

程式は、“$h(f(Y^e g^c (\mathrm{mod}\ n)),M) = x$”となる。

【００９６】

メッセージ認証と異なり、もし構成要素“Ｂ”があらゆる他の構成要素からメッセージ“Ｍ”を受信するならば、構成要素“Ａ”によるメッセージ“Ｍ”の署名が有効な状態を維持するという意味において、メッセージ署名は送り手とは無関係である。安全性の許容レベルを保証するために、公開鍵指数“ｅ”に関して少なくとも２４ビット以上のサイズが推奨される。

【００９７】

図２を参照すると、第１のステップ１８において、構成要素“Ａ”は、第１の任意の整数“ｒ”を生成すると共に、証明書のポテンシャル“$P = g^{er} (\mathrm{mod}\ n)$”を計算する。

【００９８】

ステップ１のすぐ後の第２のステップ２３において、構成要素“Ａ”は、例えば暗号化ハッシュ関数に等しい関数“ｈ”を数“Ｐ”と共同でメッセージ“Ｍ”に適用するか、または“$x = h(P,M)$”のような暗号化ハッシュ関数を組み込むことによって証明書の第１の要素“ｘ”を生成する。

【００９９】

ステップ２３において、構成要素“Ａ”は、証明書の第１の要素“ｘ”に等しいとみなされる共通数“ｃ”を生成する。

【０１００】

ステップ２３のすぐ後の第３のステップ２４において、構成要素“Ａ”は“$y = r - dc$”を計算する。このように、構成要素“Ａ”は、数“ｒ”と、掛け算の係数が共通数“ｃ”である数“ｄ”との一次結合の形式で表された秘密鍵の写像“ｙ”を生成する。任意の数“ｒ”が非常に大きいと共に通知されないので、写像“ｙ”の認識は積“ｄｃ”が回復されることを可能にせず、従って、その結果構成要素“Ａ”により秘密の状態に維持されたままである秘密鍵数“ｄ”の回復を可能にしない。構成要素“Ａ”のみが数“ｄ”を知っているので、構成要素“Ａ”のみが、共通数“ｃ”を結びつける写像を生成し得る。上述のように、写像“ｙ”は秘密鍵に関する情報を与えない。ペア“(x,y)”は、このペアが、メッセージ“Ｍ”と、構成要素“Ａ”がこの署名の発信元（ソース）であることを保証する秘密鍵の要素との双方を統合するので、メッセージ“Ｍ”の署名を構成する。

【０１０１】

その場合に構成要素“Ａ”は、構成要素“Ｂ”へ、またはその後に署名されたメッセージを構成要素“Ｂ”に送ることができるであろう他の構成要素へ、メッセージ“Ｍ”及び署名“(x,y)”を送信する。

【０１０２】

ステップ２４においてメッセージ“Ｍ”が必ずしも送信されるとは限らないことに留意すべきである。メッセージ“Ｍ”のあらゆる変形がその署名と互換性を有する機会は殆どないので、メッセージ“Ｍ”は、その署名とは無関係にステップ１９において送信されても良い。

【０１０３】

構成要素“Ｂ”による、構成要素“Ａ”または他の構成要素から発行している署名“(x,y)”を伴うメッセージ“Ｍ”の受信は遷移２５を有効とし、その場合にそれはステップ２６をアクティブにする。

【０１０４】

ステップ２６において、構成要素“Ｂ”は、共通数“ｃ”を証明書の第１の要素“ｘ”に等しいとみなす。

【０１０５】

ステップ２６において、構成要素“Ｂ”は、ステップ１７と同様に、式“$V = g^{c+ey} (\mathrm{mod}\ n)$”によって認証値“Ｖ”を計算すると共に、その場合には、認証方程式“$h(V,M) = x$”によって証明書の第２の要素が証明書の第１の要素と適合することを照合する。

【０１０６】

この場合、証明書の第１の要素と適合することは、ステップ２３自身において生成された共通数“ｃ”自身が証明書の第１の要素に適合するという事実に基づくこの等式によって照合される。

【０１０７】

関数“ｆ”を使用する変形例において、認証方程式は“$h(f(g^{c+ey} \pmod n),M) = x$”となる。

【０１０８】

本発明の方法の特に効率的な１つの実施例は、図４を参照してこれから説明されることになる。

【０１０９】

ステップ２７は、そのそれぞれと関連付けられたものが証明書のポテンシャル“P(j')”となる、１つ以上の任意の数の値“r(j')”を生成すると共に、構成要素“Ａ”のメモリに記憶する。インデックス“j'”は、テーブルにおいて、各任意の数“r(j')”と関連付けられた証明書のポテンシャル“P(j')”との間の一致を証明する役目をする。各任意の数“r(j')”は、上述のように、秘密鍵“ｄ”より実質的に大きいか、または“λ(n)”より小さいか、または“λ(n)”に等しいか、のいずれかとなるように生成される。証明書の各ポテンシャル“p(j')”は、“r(j')”を指数とする単純な数“Ｇ”の累乗（“$G^{r(j')}$”）として計算される。ステップ２７は、“P(j')”の各計算後に、インデックス“j'”の各列に対して、長さ“k'”を法としてインデックス“j'”をインクリメントすることにより実行される。長さ“k'”は、テーブルの第１の列に“j' = 0”のインデックスが付けられ、“j'”が再びゼロの状態になるときステップ２７の実行が停止するか、またはテーブルに含まれる値を更新するためにステップ２７の実行が継続するような、テーブルの段数（列数）を表す。長さ“k'”は、“ｋ”以上の値を有する。

【０１１０】

“P(j')”の計算は、“λ(n)”より小さいかまたは“λ(n)”に等しい任意の数“r(j')”を選ぶために、構成要素“Ａ”、あるいは構成要素“Ａ”から任意の数“r(j')”または値“λ(n)”を受信する信用のある構成要素によって実行される。“P(j')”の計算が構成要素“Ａ”によって実行されるとき、ステップ２７の各実行は、構成要素“Ａ”のデジタル処理手段が接続されていないことが検出されるときに有効とされる遷移２８によってアクティブにされる。

【０１１１】

単純な数“Ｇ”は、第１のステップ２９において決定される。総称数“ｇ”がセットされ、その結果全てに知られたとき、構成要素“Ａ”は単に公開鍵“(n,e)”を通知する必要があると共に、単純な数“Ｇ”が“ｎ”を法として“$G = g^e$”のように計算される。総称数“ｇ”がセットされないとき、構成要素“Ａ”は、“Ｇ”の値、例えば“G = 2”を選択すると共に、“ｎ”を法として“$g = G^d$”を生成する。その場合に、総称数“ｇ”は公開鍵と共に送信される。インデックス“j'”は、テーブルの第１の列に対してステップ２７の最初の実行を始めるように、ゼロにセットされる。ステップ２７の実行の各終りは、遷移２８、及び優先順位に従って遷移４０，４１，４２を調べるために、ステップ２９の出力に戻すように接続される。

【０１１２】

遷移４２は、識別処理によって有効とされ、その場合にそれはステップ４３及びステップ４５の一組をアクティブにする。

【０１１３】

ステップ４３は、例えば任意の数を含むテーブルの現在のインデックス“j'”、及び関連づけられた証明書のポテンシャルに等しい、繰り返しインデックス“ｊ”を配置する。

【０１１４】

ステップ４５において、構成要素“Ａ”は、テーブルから証明書のポテンシャル“P(j)”を単に読み取ることによって第１の要素“ｘ”を生成する。その結果、遷移４２の検証によって検出された処理中に、証明書の第１の要素の生成は累乗計算を必要としない。証

明書の第１の要素“ｘ”は、このように迅速に送信される。

【０１１５】

遷移１は、共通数“ｃ”の受信によって有効とされ、その場合にそれはステップ２をアクティブにする。

【０１１６】

ステップ２において、構成要素“Ａ”は、上述のように証明書の第２の要素“ｙ”を生成する。その操作がわずかな乗算、及び加算または減算に限定されるので、それらは計算時間をほとんど必要としない。証明書の第２の要素“ｙ”は、このように共通数“ｃ”の受信の後で迅速に送信される。

【０１１７】

ステップ４５の“ｋ”回実行後にステップ２９の出力に戻るために、“ｊ”が“ｋ”を法とする“ｊ'”と異なることが遷移３において検知される限り、“ｊ”が“ｋ”を法とする“ｊ'”に等しいことを遷移４が検知するまで、ステップ４５及びステップ２を繰り返すように、ステップ２においてインデックス“ｐ”は単一の増分で増加させられる。

【０１１８】

遷移４１は、メッセージ“Ｍ”の署名処理によって有効とされる。その場合に、遷移４１はステップ４４及びステップ４６の一組をアクティブにする。

【０１１９】

ステップ４４は、例えば任意の数を含むテーブルの現在のインデックス“ｊ'”、及び関連づけられた証明書のポテンシャルに等しい繰り返しインデックス“ｊ”を配置する。メッセージ“Ｍ”はステップ４４において送信される。

【０１２０】

ステップ４６において、構成要素“Ａ”は、標準のハッシュ関数“ｈ()”をメッセージ“Ｍ”、及びテーブルからの証明書のポテンシャル“Ｐ(ｊ)”の単なる読み取り結果に適用することによって、証明書の第１の要素“ｘ”を生成する。共通数“ｃ”は、証明書の第１の要素“ｘ”に等しいとみなされる。

【０１２１】

ステップ４６において、構成要素“Ａ”は、上述のように証明書の第２の要素“ｙ”を生成する。その操作がわずかな乗算、及び加算または減算に限定されるので、それらは計算時間をほとんど必要としない。その結果、遷移４１の検証によって検出された処理中に、証明書の第１の要素“ｘ”及び証明書の第２の要素“ｙ”から構成される署名の生成は累乗計算を必要としない。署名“(ｘ,ｙ)”は、このように迅速に送信される。

【０１２２】

ステップ４６の“ｋ”回実行後にステップ２９の出力に戻るために、“ｊ”が“ｋ”を法とする“ｊ'”と異なることが遷移３において検知される限り、“ｊ”が“ｋ”を法とする“ｊ'”に等しいことを遷移４が検知するまで、ステップ４６を繰り返すように、状況に応じて、ステップ４６においてインデックス“ｊ”は単一の増分で増加させられる。

【０１２３】

遷移４０は、メッセージ“Ｍ”を認証するための処理によって有効とされる。その場合に、遷移４０はステップ４３及びステップ４７の一組をアクティブにする。

【０１２４】

ステップ４３は、例えば任意の数を含むテーブルの現在のインデックス“ｊ'”、及び関連づけられた証明書のポテンシャルに等しい繰り返しインデックス“ｊ”を配置する。

【０１２５】

ステップ４７において、構成要素“Ａ”は、メッセージ“Ｍ”、及び証明書の第１の要素“ｘ”を送信する。証明書の第１の要素“ｘ”は、標準のハッシュ関数“ｈ()”をメッセージ“Ｍ”、及びテーブルからの証明書のポテンシャル“Ｐ(ｊ)”の単なる読み取り結果に適用することによって生成される。

【０１２６】

その結果、遷移４０の検証によって検出された処理中に、証明書の第１の要素の生成は

累乗計算を必要としない。証明書の第１の要素“ｘ”はこのように迅速に送信される。

【０１２７】

遷移１は、共通数“ｃ”の受信によって有効とされ、その場合にそれはステップ４８をアクティブにする。

【０１２８】

ステップ４８において、構成要素“Ａ”は、上述のように証明書の第２の要素“ｙ”を生成する。その操作がわずかな乗算、及び加算または減算に限定されるので、それらは計算時間をほとんど必要としない。証明書の第２の要素“ｙ”は、このように共通数“ｃ”の受信の後で迅速に送信される。

【０１２９】

ステップ４７の“ｋ”回実行後にステップ２９の出力に戻るために、“ｊ”が“ｋ”を法とする“ｊ'”と異なることが遷移３において検知される限り、“ｊ”が“ｋ”を法とする“ｊ'”に等しいことを遷移４が検知するまで、ステップ４７及びステップ４８を繰り返すように、ステップ４８においてインデックス“ｐ”は単一の増分で増加させられる。

【０１３０】

図６を参照すると、上述の構成要素“Ａ”、構成要素“Ｂ”、及び構成要素“Ｃ”は、認証要求者用装置３０、認証者用装置３１、及び中間装置３２によってそれぞれ物理的に形成される。

【０１３１】

認証要求者用装置３０は、例えばクレジットカード、または携帯電話加入者身分証明カード（mobile telephone subscriber identification card）のようなマイクロプロセッサカードである。認証者用装置３１は、例えば銀行端末（bank terminal）、または電子商取引サーバ（electronic commerce server）、または移動体通信オペレータ装置（mobile telecommunication operator equipment）である。中間装置３２は、例えばマイクロプロセッサカード付属装置（microprocessor card extension）、クレジットカード読み取り端末（credit card read terminal）、または、携帯電話の電子カード（mobile telephone electronic card）である。認証要求者用装置３０は、通信手段３４、及び計算手段３７を有する。認証要求者用装置３０は、侵入から保護される。通信手段３４は、実行されるべき方法のバージョンに応じて、図１、図３、または図４を参照して説明されたステップ９、ステップ４５、またはステップ４７に従って証明書の第１の要素“ｘ”、図１、及び図３を参照して説明されたステップ１３に従って、図２を参照して説明されたステップ２４、または図４を参照して説明されたステップ２、及びステップ４８において証明書の第２の要素“ｙ”、図１から図４を参照して説明されたステップ１９、ステップ２０、ステップ４４、またはステップ４７に従ってメッセージ“Ｍ”、または図２、及び図４を参照して説明されたステップ２４、ステップ４６に従って共通数“ｃ”を送信するように設計される。通信手段３４は、実行されるべき方法のバージョンが識別、または認証に相当するとき、同様に、図１から図４を参照して説明された遷移１２、または遷移１に従って、共通数“ｃ”を受信するように設計される。署名に相当する実行されるべき方法のバージョンに関して、通信手段３４は共通数“ｃ”を受信するように設計される必要はない。

【０１３２】

計算手段３７は、実行されるべき方法のバージョンに応じて、図１、または図５を参照して説明されたステップ９、及びステップ１３、図２を参照して説明されたステップ１８、ステップ１９、ステップ２３、及びステップ２４、図３を参照して説明されたステップ１３、及びステップ２０、または図４を参照して説明されたステップを実行するように設計される。既知の方法において、計算手段３７は、上述のような計算専用のマイクロプロセッサ及びマイクロプログラム、または結合回路を有する。

【０１３３】

認証者用装置３１は、通信手段３５、及び計算手段３８を有する。通信手段３５は、実行されるべき方法のバージョンが認証に相当するとき、図１、図３、及び図５を参照して

説明されたステップ１１に従って、１つ以上の共通数“ｃ”を送信するように設計される。署名に相当する実行されるべき方法のバージョンに関して、通信手段３５は共通数“ｃ”を送信するように設計される必要はない。通信手段３５は、同様に、図１から図３、及び図５を参照して説明された遷移１０、及び遷移１６に従って、証明書の２つの要素“ｘ”と“ｙ”、図３を参照して説明された遷移２１、及び遷移１６に従って、証明書の第１の要素“ｘ”、及び証明書の第２の要素“ｙ”を伴うメッセージ“Ｍ”、または図５を参照して説明された遷移２、及び遷移８に従って、１つ以上の共通数“ｃ”と秘密鍵の写像“ｙ”を伴う証明書の第２の要素とメッセージ“Ｍ”を受信するように設計される。

【０１３４】

計算手段３８は、実行されるべき方法のバージョンに応じて、図１、及び図５を参照して説明されたステップ１１、及びステップ１７、図２を参照して説明されたステップ２６、または図３を参照して説明されたステップ１１、及びステップ２２を実行するように設計される。既知の方法において、計算手段３８は、上述のような計算専用のマイクロプロセッサ及びマイクロプログラム、または結合回路を有する。

【０１３５】

中間装置３２は、通信手段３６、及び計算手段３９を有する。通信手段３６は、図５を参照して説明されたステップ１５に従って、証明書の第３の要素“Ｙ”を送信するように設計される。通信手段３６は、同様に、図５を参照して説明された遷移１４に従って、証明書の第２の要素“ｙ”を受信するように設計される。

【０１３６】

計算手段３９は、図５を参照して説明されたステップ１５を実行するように設計される。既知の方法において、計算手段３９は、上述のような計算専用のマイクロプロセッサ及びマイクロプログラム、または結合回路を有する。

【０１３７】

改良として、上述の計算手段、及び通信手段は、毎回異なる証明書の第１の要素、及び証明書の第２の要素に関して、上述のステップの実行を“ｋ”回繰り返すように設計される。

【図面の簡単な説明】

【０１３８】

【図１】第１の構成要素を識別するための本発明による方法のステップを示す図である。

【図２】メッセージに署名するための本発明による方法のステップを示す図である。

【図３】メッセージを認証するための本発明による方法のステップを示す図である。

【図４】多くの処理を容易にするための認証方法の第１の変形例を示す図である。

【図５】中間の構成要素を関与させる認証方法の第２の変形例を示す図である。

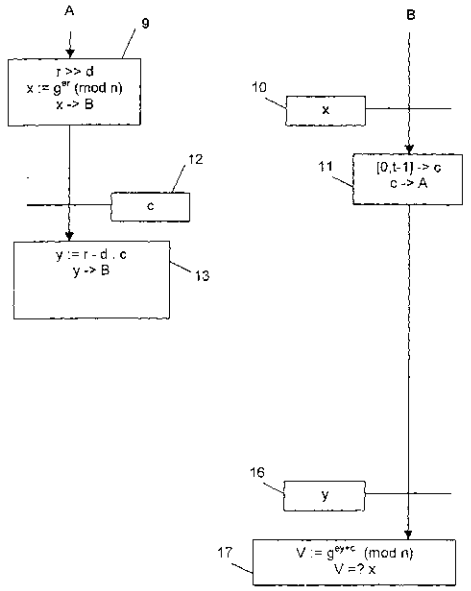
【符号の説明】

【０１３９】

３０　認証要求者用装置
３１　認証者用装置
３２　中間装置
３４，３５，３６　通信手段
３７，３８，３９　計算手段

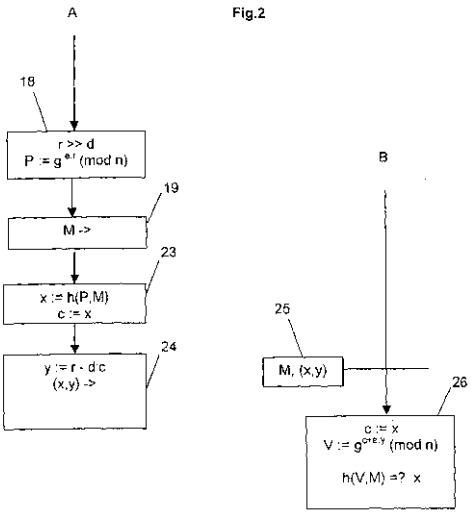
【図１】

Fig.1



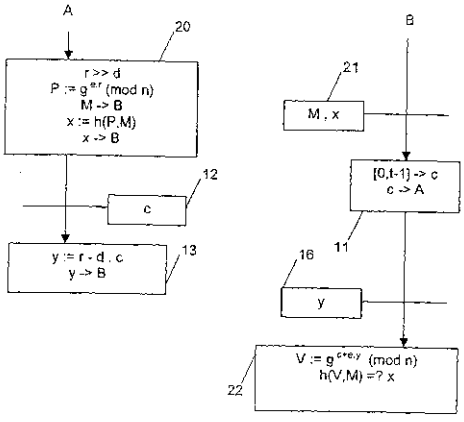
【図２】

Fig.2



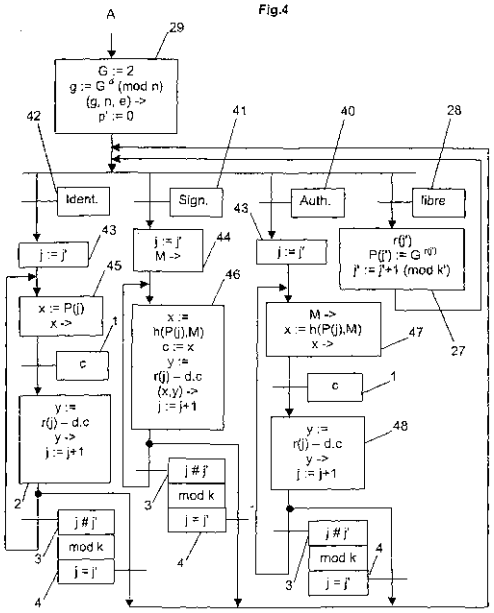
【図３】

Fig.3



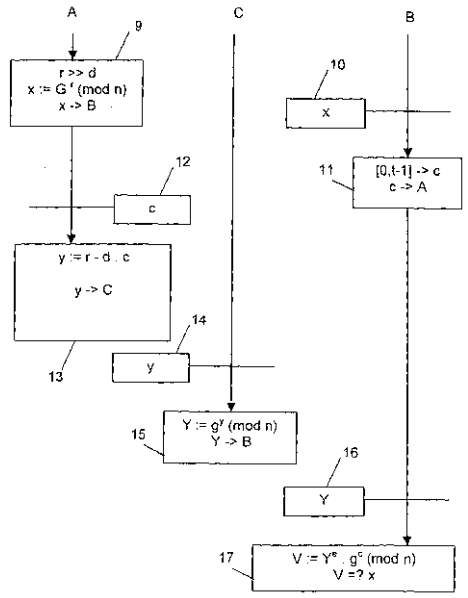
【図４】

Fig.4



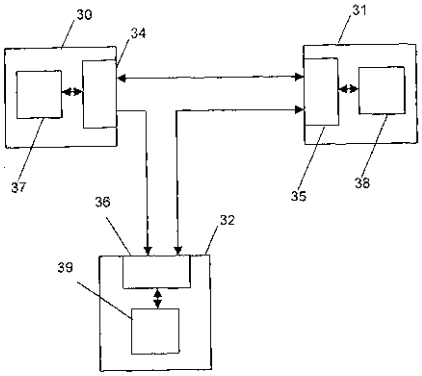
【図５】

Fig.5



【図６】

Fig.6



【国際調査報告】

INTERNATIONAL SEARCH REPORT

International Application No
PCT/FR 03/02000

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L9/32

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	SCHNORR C P: "EFFICIENT IDENTIFICATION AND SIGNATURES FOR SMART CARDS" LECTURE NOTES IN COMPUTER SCIENCE, SPRINGER VERLAG, NEW YORK, NY, US, 20 August 1989 (1989-08-20), pages 239-252, XP002052048 ISSN: 0302-9743 page 239, line 1 - line 17 page 240, line 7 -page 241, line 13 page 242, line 28 -page 243, line 8 page 249, line 1 - line 24 ---	1-18
A	US 4 995 082 A (SCHNORR CLAUS P) 19 February 1991 (1991-02-19) abstract column 2, line 3 -column 3, line 61; figures 1,2,4 --- -/--	1-18

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

'A' document defining the general state of the art which is not considered to be of particular relevance

'E' earlier document but published on or after the international filing date

'L' document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

'O' document referring to an oral disclosure, use, exhibition or other means

'P' document published prior to the international filing date but later than the priority date claimed

'T' later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

'X' document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

'Y' document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

'&' document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
12 November 2003	21/11/2003

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Post, K

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

International Application No
PCT/FR 03/02000

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
A	FR 2 718 311 A (TRT TELECOM RADIO ELECTR) 6 October 1995 (1995-10-06) abstract page 2, line 20 -page 3, line 24	1-18

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/FR 03/02000

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 4995082 A	19-02-1991	EP 0383985 A1	29-08-1990
		AT 106643 T	15-06-1994
		DE 59005851 D1	07-07-1994
		EP 0384475 A1	29-08-1990
		ES 2054120 T3	01-08-1994
		JP 2666191 B2	22-10-1997
		JP 3001629 A	08-01-1991
FR 2718311 A	06-10-1995	FR 2718311 A1	06-10-1995
		DE 69521641 D1	16-08-2001
		DE 69521641 T2	02-05-2002
		EP 0675614 A1	04-10-1995
		JP 7287514 A	31-10-1995
		US 5748782 A	05-05-1998

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale No
PCT/FR 03/02000

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
CIB 7 H04L9/32

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)
CIB 7 H04L

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si réalisable, termes de recherche utilisés)
EPO-Internal, WPI Data, INSPEC

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie °	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	SCHNORR C P: "EFFICIENT IDENTIFICATION AND SIGNATURES FOR SMART CARDS" LECTURE NOTES IN COMPUTER SCIENCE, SPRINGER VERLAG, NEW YORK, NY, US, 20 août 1989 (1989-08-20), pages 239-252, XP002052048 ISSN: 0302-9743 page 239, ligne 1 - ligne 17 page 240, ligne 7 -page 241, ligne 13 page 242, ligne 28 -page 243, ligne 8 page 249, ligne 1 - ligne 24 ---	1-18
A	US 4 995 082 A (SCHNORR CLAUS P) 19 février 1991 (1991-02-19) abrégé colonne 2, ligne 3 -colonne 3, ligne 61; figures 1,2,4 ---	1-18

-/--

[X] Voir la suite du cadre C pour la fin de la liste des documents

[X] Les documents de familles de brevets sont indiqués en annexe

° Catégories spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent

"E" document antérieur, mais publié à la date de dépôt international ou après cette date

"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)

"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens

"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention

"X" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément

"Y" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier

"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée	Date d'expédition du présent rapport de recherche internationale
12 novembre 2003	21/11/2003

Nom et adresse postale de l'administration chargée de la recherche internationale	Fonctionnaire autorisé
Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Post, K

Formulaire PCT/ISA/210 (deuxième feuille) (juillet 1992)

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale No
PCT/FR 03/02000

C.(suite) DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie *	Identification des documents cités, avec,le cas échéant, l'indicationdes passages pertinents	no. des revendications visées
A	FR 2 718 311 A (TRT TELECOM RADIO ELECTR) 6 octobre 1995 (1995-10-06) abrégé page 2, ligne 20 -page 3, ligne 24	1-18

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Demande internationale No
PCT/FR 03/02000

Document brevet cité au rapport de recherche		Date de publication	Membre(s) de la famille de brevet(s)		Date de publication
US 4995082	A	19-02-1991	EP	0383985 A1	29-08-1990
			AT	106643 T	15-06-1994
			DE	59005851 D1	07-07-1994
			EP	0384475 A1	29-08-1990
			ES	2054120 T3	01-08-1994
			JP	2666191 B2	22-10-1997
			JP	3001629 A	08-01-1991
FR 2718311	A	06-10-1995	FR	2718311 A1	06-10-1995
			DE	69521641 D1	16-08-2001
			DE	69521641 T2	02-05-2002
			EP	0675614 A1	04-10-1995
			JP	7287514 A	31-10-1995
			US	5748782 A	05-05-1998

フロントページの続き

(81)指定国 AP(GH,GM,KE,LS,MW,MZ,SD,SL,SZ,TZ,UG,ZM,ZW),EA(AM,AZ,BY,KG,KZ,MD,RU,TJ,TM),EP(AT,BE,BG,CH,CY,CZ,DE,DK,EE,ES,FI,FR,GB,GR,HU,IE,IT,LU,MC,NL,PT,RO,SE,SI,SK,TR),OA(BF,BJ,CF,CG,CI,CM,GA,GN,GQ,GW,ML,MR,NE,SN,TD,TG),AE,AG,AL,AM,AT,AU,AZ,BA,BB,BG,BR,BY,BZ,CA,CH,CN,CO,CR,CU,CZ,DE,DK,DM,DZ,EC,EE,ES,FI,GB,GD,GE,GH,GM,HR,HU,ID,IL,IN,IS,JP,KE,KG,KP,KR,KZ,LC,LK,LR,LS,LT,LU,LV,MA,MD,MG,MK,MN,MW,MX,MZ,NI,NO,NZ,OM,PG,PH,PL,PT,RO,RU,SC,SD,SE,SG,SK,SL,SY,TJ,TM,TN,TR,TT,TZ,UA,UG,US,UZ,VC,VN,YU,ZA,ZM,ZW

(72)発明者 マルク・ジロール
フランス・Ｆ－１４０００・カーン・リュ・ヴィヴィアーヌ・４
(72)発明者 ジャン－クロード・パイル
フランス・Ｆ－１４６１０・ウプロン・リュ・デ・ロワシル・４

Ｆターム(参考) 5J104 AA18 AA22 AA32 AA41 AA43 AA47 JA21 JA28 NA02 NA18 NA39 NA42