(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第4772965号
(P4772965)
(45)発行日　平成23年9月14日(2011.9.14)　(24)登録日　平成23年7月1日(2011.7.1)

(51)Int.Cl.　F I
H04L 9/32 (2006.01)　H04L 9/00 675C

請求項の数 9 (全 35 頁)

(21)出願番号	特願2000-596696 (P2000-596696)
(86)(22)出願日	平成12年1月27日 (2000.1.27)
(65)公表番号	特表2003-513480 (P2003-513480A)
(43)公表日	平成15年4月8日 (2003.4.8)
(86)国際出願番号	PCT/FR2000/000190
(87)国際公開番号	WO2000/045550
(87)国際公開日	平成12年8月3日 (2000.8.3)
審査請求日	平成19年1月23日 (2007.1.23)
(31)優先権主張番号	99/01065
(32)優先日	平成11年1月27日 (1999.1.27)
(33)優先権主張国	フランス(FR)
(31)優先権主張番号	99/03770
(32)優先日	平成11年3月23日 (1999.3.23)
(33)優先権主張国	フランス(FR)

(73)特許権者　509246806
ファンタム・ダイアー・エヌヴェー・エル　エルシー
アメリカ合衆国・ディーシー・１９９０４・ドヴァー・グリーントゥリー・ドライブ・１６０・スイート・１０１
(74)代理人　100079108
弁理士　稲葉　良幸
(74)代理人　100109346
弁理士　大貫　敏史
(72)発明者　ギユ，ルイ
フランス国、３５２３０　ブルバル、リュ・ドゥ・リズ　１６

最終頁に続く

(54)【発明の名称】エンティティの真正性および／またはメッセージの完全性を証明するための方法

(57)【特許請求の範囲】

【請求項１】

デモンストレータ装置の同一性またはメッセージ署名の完全性を、コントローラ装置において証明する方法であって、

前記コントローラ装置によって、コミットメントＲを受信するステップであって、該コミットメントＲは、$R \equiv r^v \mod n$であり、ｒは０＜ｒ＜ｎとなるようにランダムに選択された整数であるステップと、

前記コントローラ装置によって、ランダムに選択されたｍ個のチャレンジ$d_1, d_2, \cdots, d_m$を送信するステップと、

前記コントローラ装置によって、応答Ｄを受信するステップであって、該応答Ｄは、$D \equiv r \cdot Q_1^{d1} \cdot Q_2^{d2} \cdot \cdots \cdot Q_m^{dm} \mod n$であるステップと、

前記コントローラ装置によって、$G_1^{d1}, G_2^{d2}, \cdots, G_m^{dm}$と$D^v$とに基づいてｎを法とする計算によって得られる値が、前記コミットメントＲに等しいかどうかに基づいて、前記デモンストレータ装置の同一性または前記メッセージ署名の完全性を決定するステップであって、１以上の秘密値$Q_1, Q_2, \cdots, Q_m$とそれぞれの公開値$G_1, G_2, \cdots, G_m$との集合が、前記デモンストレータ装置または前記メッセージ署名と関連し、Q_iとG_iの値のそれぞれのペアは、式$G_i \cdot Q_i^v \equiv 1 \mod n$、または式$G_i \equiv Q_i^v \mod n$のいずれかを確認するものであり、ｍは１以上の整数であり、ｉは１とｍの間の整数であり、ｎはｆ個の素因数$p_1, p_2, \cdots, p_f$の積に等しい公開整数であり、これらの素因数の少なくとも２つは互いに異なっており、ｆは１より大きい整数であり、ｖは$v = 2^k$となる

公開指数であり、ｋは１より大きい整数値を有する機密保護パラメータであり、それぞれの公開値G_i（ｉ＝１，・・・，ｍ）は、$G_i \equiv g_i^2 \mod n$となるものであり、g_i（ｉ＝１，・・・，ｍ）は、１より大きく前記素因数p_1，p_2，…，p_fのそれぞれよりも小さい整数値を有する基数であり、前記基数g_iがモジュロｎの整数環の平方非剰余となるように前記素因数p_1，p_2，…，p_fが前記基数に基づいて選択されているステップと

を含んでなる方法。

【請求項２】

前記決定するステップは、前記コントローラ装置によって、前記コミットメントＲが、$R \equiv D^v \cdot G_1^{\varepsilon 1 d1} \cdot G_2^{\varepsilon 2 d2} \cdot \cdots \cdot G_m^{\varepsilon m dm} \mod n$となる値を前記応答Ｄが有する場合には、前記デモンストレータ装置が真正であると決定するステップを含み、ここで、ｉ＝１，・・・，ｍについて、$G_i \cdot Q_i^{\ v} \equiv 1 \mod n$の場合には$\varepsilon_i = +1$であり、$G_i \equiv Q_i^{\ v} \mod n$の場合には$\varepsilon_i = -1$である、請求項１に記載の方法。

【請求項３】

前記コミットメントＲは、コミットメント要素R_j（ｊ＝１，・・・，ｆ）の集合からチャイニーズ剰余を用いて計算された値を有し、各コミットメント要素R_jは、$R_j \equiv r_j^v \mod p_j$となる値を有し、ここで、$r_j$は、前記デモンストレータ装置によってランダムに選択され、$0 < r_j < p_j$となる整数であり、

前記応答Ｄは、チャイニーズ剰余を用いて応答要素D_jの集合から計算され、該応答要素D_jは、ｉ＝１，・・・，ｍおよびｊ＝１，・・・，ｆについて$Q_{i,j} \equiv Q_i \mod p_j$であり、ｊ＝１，・・・，ｆについて$D_j \equiv r_j \cdot Q_{1,j}^{\ d1} \cdot Q_{2,j}^{\ d2} \cdots Q_{m,j}^{\ dm} \mod p_j$となる値を有し、

前記決定するステップは、前記コントローラ装置によって、前記コミットメントＲが、$R = D^v \cdot G_1^{\varepsilon 1 d1} \cdot G_2^{\varepsilon 2 d2} \cdot \cdots \cdot G_m^{\varepsilon m dm} \mod n$となる値を前記応答Ｄが有する場合には、前記デモンストレータ装置が真正であると決定するステップを含み、ここで、ｉ＝１，・・・，ｍについて、$G_i \cdot Q_i^{\ v} \equiv 1 \mod n$の場合には$\varepsilon_i = +1$であり、$G_i \equiv Q_i^{\ v} \mod n$の場合には$\varepsilon_i = -1$である、請求項１に記載の方法。

【請求項４】

前記コントローラ装置によって、デモンストレータ装置からトークンＴを受信するステップであって、該トークンＴは、Ｔ＝ｈ（Ｍ，Ｒ）となる値を有し、ここで、ｈはハッシュ関数であり、Ｍは前記デモンストレータ装置から受信したメッセージであり、

前記応答Ｄは、$D \equiv r \cdot Q_1^{d1} \cdot Q_2^{d2} \cdot \cdots \cdot Q_m^{dm} \mod n$となるように計算された値を有し、

前記決定するステップは、前記コントローラ装置によって、前記トークンＴが、$T = h(M, D^v \cdot G_1^{\varepsilon 1 d1} \cdot G_2^{\varepsilon 2 d2} \cdot \cdots \cdot G_m^{\varepsilon m dm} \mod n)$となる値を前記応答Ｄが有する場合には、前記メッセージＭが真正であると決定するステップを含み、ここで、ｉ＝１，・・・，ｍについて、$G_i \cdot Q_i^{\ v} \equiv 1 \mod n$の場合には$\varepsilon_i = +1$であり、$G_i \equiv Q_i^{\ v} \mod n$の場合には$\varepsilon_i = -1$である、請求項１に記載の方法。

【請求項５】

前記コントローラ装置によって、前記デモンストレータ装置からトークンＴを受信するステップであって、前記コミットメントＲは、コミットメント要素R_j（ｊ＝１，・・・，ｆ）の集合からチャイニーズ剰余を用いて計算された値を有し、各コミットメント要素R_jは$R_j \equiv r_j^v \mod p_j$となる値を有し、ここで、$r_j$は、前記デモンストレータ装置によってランダムに選択され、$0 < r_j < p_j$となる整数であるステップをさらに含み、

前記応答Ｄは、チャイニーズ剰余を用いて応答要素D_jの集合から計算され、該応答要素D_jは、ｉ＝１，・・・，ｍおよびｊ＝１，・・・，ｆについて$Q_{i,j} \equiv Q_i \mod p_j$であり、ｊ＝１，・・・，ｆについて$D_j \equiv r_j \cdot Q_{1,j}^{\ d1} \cdot Q_{2,j}^{\ d2} \cdots Q_{m,j}^{\ dm} \mod p_j$となる値を有し、

前記決定するステップは、前記コントローラ装置によって、前記トークンＴが、$T = h(M, D^v \cdot G_1^{\varepsilon 1 d1} \cdot G_2^{\varepsilon 2 d2} \cdot \cdots \cdot G_m^{\varepsilon m dm} \mod n)$となる値を、前記応答Ｄ

が有する場合には、前記メッセージMが真正であると決定するステップを含み、ここで、ｉ＝１，・・・，ｍについて、$G_i \cdot Q_i^v \equiv 1 \mod n$の場合には$\varepsilon_i = +1$であり、$G_i \equiv Q_i^v \mod n$の場合には$\varepsilon_i = -1$である、請求項１に記載の方法。

【請求項６】

前記チャレンジが、ｉ＝１，・・・，ｍについて、$0 \leqq d_i \leqq 2^k - 1$である、請求項２から５のいずれかに記載の方法。

【請求項７】

前記デモンストレータによって、署名されるメッセージMを記録するステップと、

前記デモンストレータ装置によって、ｉ＝１，・・・，ｍについて、$0 < r_i < n$となるｍ個の整数r_iをランダムに選択するステップと、

前記デモンストレータ装置によって、ｉ＝１，・・・，ｍについて、$R_i \equiv r_i^v \mod n$となる値を有するコミットメントR_iを計算するステップと、

前記デモンストレータ装置によって、Ｔ＝ｈ（Ｍ、R_1，R_2，・・・，R_m）となる値を有するトークンＴを計算するステップであって、ここで、ｈは、ｍビットからなるバイナリトレインを生成するハッシュ関数であるステップと、

前記デモンストレータ装置によって、前記トークンＴのビットd_1，d_2，・・・，d_mを識別するステップと、

前記デモンストレータ装置によって、ｉ＝１，・・・，ｍについて、応答$D_i \equiv r_i \cdot Q_i^{d_i} \mod n$を計算するステップと

をさらに含む、請求項１に記載の方法。

【請求項８】

前記コントローラ装置によって、前記トークンＴおよび前記応答D_i（ｉ＝１，・・・，ｍ）を集めるステップと、

前記コントローラ装置によって、前記トークンＴが、Ｔ＝ｈ（Ｍ，$D_1^v \cdot G_1^{\varepsilon 1 d 1} \mod n$，$D_2^v \cdot G_2^{\varepsilon 2 d 2} \mod n$，…，$D_m^v \cdot G_m^{\varepsilon m dm} \mod n$）となる値を前記応答Ｄが有する場合には、前記メッセージMが真正であると決定するステップであって、ここで、ｉ＝１，・・・，ｍについて、$G_i \cdot Q_i^v \equiv 1 \mod n$の場合には$\varepsilon_i = +1$であり、$G_i \equiv Q_i^v \mod n$の場合には$\varepsilon_i = -1$であるステップと

をさらに含む、請求項７に記載の方法。

【請求項９】

コミットメントＲを受信するステップであって、該コミットメントＲは、$R \equiv r^v \mod n$であり、ｒは$0 < r < n$となるようにランダムに選択された整数であるステップと、

ランダムに選択されたｍ個のチャレンジd_1，d_2，…，d_mを送信するステップと、

応答Ｄを受信するステップであって、該応答Ｄは、$D \equiv r \cdot Q_1^{d1} \cdot Q_2^{d2} \cdot \cdots \cdot Q_m^{dm} \mod n$であるステップと、

G_1^{d1}，G_2^{d2}，…，G_m^{dm}とＤ^{v}とに基づいてｎを法とする計算によって得られる値が、前記コミットメントＲに等しいかどうかに基づいて、デモンストレータ装置の同一性またはメッセージ署名の完全性を決定するステップであって、１以上の秘密値Q_1，Q_2，…，Q_mとそれぞれの公開値G_1，G_2，…，G_mとの集合が、前記デモンストレータ装置または前記メッセージ署名と関連し、Q_iとG_iの値のそれぞれのペアは、式$G_i \cdot Q_i^v \equiv 1 \mod n$、または式$G_i \equiv Q_i^v \mod n$のいずれかを確認するものであり、ｍは１以上の整数であり、ｉは１とｍの間の整数であり、ｎはｆ個の素因数p_1，p_2，…，p_fの積に等しい公開整数であり、これらの素因数の少なくとも２つは互いに異なっており、ｆは１より大きい整数であり、ｖは$v = 2^k$となる公開指数であり、ｋは１より大きい整数値を有する機密保護パラメータであり、それぞれの公開値G_i（ｉ＝１，・・・，ｍ）は、$G_i \equiv g_i^2 \mod n$となるものであり、g_i（ｉ＝１，・・・，ｍ）は、１より大きく前記素因数p_1，p_2，…，p_fのそれぞれよりも小さい整数値を有する基数であり、前記基数g_iがモジュロｎの整数環の平方非剰余となるように前記素因数p_1，p_2，…，p_fが前記基数に基づいて選択されているステップと

をコントローラ装置に実行させる命令を記憶しているコンピュータに読み取り可能な記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、エンティティの真正性(authenticity)、および／またはメッセージの完全性(integrity)および／または真正性を証明するように設計される方法、システムおよびデバイスに関する。

【０００２】

【従来の技術】

その発明者がLouis Guillouおよび Jean－Jacques Quisquaterである欧州特許第０３１１４７０Ｂ１公報がこのような方法を説明する。これ以降、彼らの研究は用語「ＧＱ特許」または「ＧＱ方法」によって参照されるものとする。これ以降、表現「ＧＱ２」、あるいは「ＧＱ２発明」または「ＧＱ２技術」は、本発明を説明するために使用されるものとする。

【０００３】

ＧＱ方法に従って、「信頼される当局（trusted authority）」として知られているエンティティが、「証人（witness）」と呼ばれているそれぞれのエンティティにアイデンティティを割り当てる。顧客イズ化プロセスにおいて、信頼される当局は、証人にアイデンティティ(identity)およびシグナチャ(signature)を与える。それ以降、証人は以下を宣言する。つまり「ここに私のアイデンティティがある。私はそのＲＳＡシグナチャを知っている。」証人は、このシグナチャを明らかにせずに、自分が自分のアイデンティティのＲＳＡシグナチャを知っていることを証明する。ＲＳＡ公開識別鍵（RSA Public identification key）は、信頼される当局によって配布されるが、「コントローラ(controller)」として知られているエンティティが、その知識を得ずに、ＲＳＡシグナチャが宣言されたアイデンティティに一致することを確認する。ＧＱ方法を使用する機構は、「知識の移管(transfer of knowledge)」を行わずに実行する。ＧＱ方法に従って、証人は、信頼される当局が大多数のアイデンティティに署名をするＲＳＡ秘密鍵を知らない。

【０００４】

【発明が解決しようとする課題】

ここに前述されるＧＱ技術は、ＲＳＡ技術を利用する。しかしながら、ＲＳＡ技術は、真に係数ｎの因数分解に依存する一方で、この依存は、いわゆるＲＳＡ技術を実行するデジタル署名の多様な規格に対する倍増的に増加する攻撃に見られるように同等ではなく、実際にはそれはかなり異なっている。

【０００５】

【課題を解決するための手段】

ＧＱ２技術の目標は２つの部分を有する。つまり、第１に、ＲＳＡ技術の性能特徴を改善すること、第２にＲＳＡ技術に固有の問題を回避することである。ＧＱ２秘密鍵を知っていることは、係数ｎの因数分解を知っていることに等価である。三つ組のＧＱ２に対する攻撃は、係数ｎの因数分解につながる。このときには等価である。ＧＱ２技術を用いると、署名をする、あるいは自己認証するエンティティにとっての、および監査するエンティティにとっての作業量は削減される。機密保護と性能の両方の点での因数分解の問題をさらにうまく使用することにより、ＧＱ２技術はＲＳＡ技術の欠点を回避する。

【０００６】

ＧＱ方法は、５１２ビット以上を備える数のモジュロ計算を実行する。これらの計算は、約$2^{16}+1$乗まで累乗されたのと実質的に同じ大きさを有する数に関する。現在では、特にバンクカードの分野における既存のマイクロエレクトロニクスインフラストラクチャは、演算コプロセッサを使用しないでモノリシックな自己プログラム可能マイクロプロセッサを利用する。ＧＱ方法などの方法に関係する複数の演算アプリケーションに関する作業量は、一定の場合では、顧客が購入物を支払うためにバンクカードを使用するには不利で

あることが判明する計算時間につながっている。ここでは、支払カードの安全を高めることを求めて、銀行当局が、特に解決が困難である問題を引き起こしたことを想起することができる。実際、２つの明らかに矛盾する問題が解決されなければならない。つまり、一方では、各カードのますます冗長かつ明瞭なキーを使用することにより安全性を高めつつ、他方では、作業量がユーザにとっての過剰な計算時間につながることを妨げるのである。この問題は、既存のインフラストラクチャおよび既存のマイクロプロセッサ構成要素を考慮に入れることも必要となるため、特に激しくなる。

【０００７】

ＧＱ２技術は、安全性を高めつつ、この問題に対する解決策を提供する。

【０００８】

（方法）

さらに特に、本発明は、コントローラエンティティに対し、あるエンティティの真正性、および／または、このエンティティに関連付けられたメッセージＭの完全性とを証明するように設計された方法に関する。

【０００９】

この証明は、以下のパラメータまたはこれらのパラメータのすべてまたは一部によって確立される。ここで、パラメータは、

ｍ組の秘密値Q_1，Q_2，…Q_mおよび公開値G_1，G_2，…G_m（ｍは１以上）と、

ｆ個の素因数p_1，p_2，…p_f（ｆは２以上）の積によって構成される公開係数ｎと、

公開指数ｖとである。

前記係数、前記指数および前記値は、次のタイプの関係

$G_i . Q_i^v \equiv 1 . \mathrm{mod}\ n$ または $G_i \equiv Q_i^v \mathrm{mod}\ n .$

によって関連付けられ、

前記指数ｖは、

$v = 2^k$

であり、ここで、ｋは１より大きい機密保護パラメータである。

【００１０】

前記公開値G_iは、ｆ個の素因数p_1，p_2，…p_fより小さい基数g_iの平方g_i^2である。

基数g_iは、

２つの等式

$x^2 \equiv g_i \mathrm{mod}\ n$ および $x^2 \equiv -g_i \mathrm{mod}\ n$

が、モジュロｎの整数環のｘについて解くことができず、等式

$x^v \equiv g_i^2 \mathrm{mod}\ n$

が、モジュロｎの整数環のｘについて解くことができる。

前記方法は、以下のステップにおいて、証人と呼ばれるエンティティを実行する。前記証人エンティティは、ｆ個の素因数p_iおよび／または素因数のチャイニーズ剰余の、および公開係数ｎおよび／またはｍ個の秘密値Q_iのパラメータ、および／または秘密値Q_iのおよび公開指数ｖのｆ．ｍ個の構成要素$Q_{i,j}$（$Q_{i,j} \equiv Q_i \mathrm{mod}\ p_j$）を有する。

【００１１】

証人は、モジュロｎの整数環のコミットメントＲを計算する。各コミットメントを、

・次のタイプの演算を実行すること

$R \equiv r^v \mathrm{mod}\ n$

ここで、ｒは０＜ｒ＜ｎとなるようにランダム値であり、

・または、

・・以下のタイプの演算を実行し、

$R_i \equiv r_i^v \mathrm{mod}\ p_i$

ここで、r_iは、$0 < r_i < p_i$となるように素数p_iと関連付けられたランダム値であり、各r_iは、ランダム値｛r_1，r_2，…r_f｝の集合体に属し、

・・そして、チャイニーズ剰余法を適用すること

のどちらかによって計算する。

【００１２】
証人は、1以上のチャレンジｄを受け取る。各チャレンジｄは、これ以降初歩チャレンジと呼ばれるｍ個の整数d_iを備える。証人は、各チャレンジｄに基づき、応答Ｄを、
・以下のタイプの演算を実行すること
$D \equiv r . Q_1^{d1} . Q_2^{d2} . \cdots Q_m^{dm} \mathrm{mod}\ n$
・または、
・・以下のタイプの演算を実行し
$D_i \equiv r_i . Q_{i,1}^{d1} . Q_{i,2}^{d2} . \cdots Q_{i,m}^{dm} \mathrm{mod}\ p_i$
そして、チャイニーズ剰余法を適用すること
のどちらかによって計算する。
該方法は、コミットメントＲがあるため、チャレンジｄがあるのと同じくらい多くの応答Ｄがあり、数Ｒ，ｄ，Ｄの各群は｛Ｒ，ｄ，Ｄ｝と参照される三つ組を形成する。
【００１３】
（エンティティの真正性の証明の場合）
第１代替実施態様においては、本発明に従った方法は、デモンストレータとして知られているエンティティの真正性をコントローラとして知られているエンティティに対し証明するように設計される。前記デモンストレータエンティティは、証人を備える。前記デモンストレータエンティティおよびコントローラエンティティは、以下のステップを実行する。
・ステップ１のコミットメントＲという行為
各呼び出しでは、証人は、ここに前記に明記されたプロセスを適用することによって各コミットメントＲを計算する。デモンストレータは、コントローラに、各コミットメントＲのすべてまたは一部を送信する。
・ステップ２のチャレンジｄという行為
コントローラは、各コミットメントＲのすべてまたは一部を受け取った後、その数がコミットメントＲの数に等しいチャレンジｄを作成し、チャレンジｄをデモンストレータに送信する。
・ステップ３の応答Ｄという行為
証人は、前記に明記されたプロセスを適用することによって、チャレンジｄから応答Ｄを計算する。
・ステップ４のチェック行為
証人は、コントローラに各応答Ｄを送信する。
（第１の場合：デモンストレータが各コミットメントＲの一部を送信）
デモンストレータが各コミットメントＲの一部を送信した場合には、ｍ個の公開値G_1，G_2，．．．，G_mを有するコントローラは、各チャレンジｄおよび各応答Ｄから再構築されたコミットメントＲ’を計算し、この再構築されたコミットメントＲ’が次のタイプの関係性
$R' \equiv G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . D^v \mathrm{mod}\ n$
または、次のタイプの関係性
$R' \equiv D^v / G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . \mathrm{mod}\ n$
を満たす。
コントローラは、各再構築されたコミットメントＲ’が、それに送信された各コミットメントＲのすべてまたは一部を再現することを確認する。
（第２の場合：デモンストレータが各コミットメントＲの全体性を送信）
デモンストレータが各コミットメントＲの全体性を送信した場合、ｍ個の公開値G_1，G_2，．．．，G_mを有するコントローラは、各コミットメントＲが、次のタイプの関係性
$R \equiv G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . D^v \mathrm{mod}\ n$
または、以下のタイプの関係性
$R \equiv D^v / G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . \mathrm{mod}\ n$
を満たすことを確認する。

【００１４】
（メッセージの完全性の証明の場合）
第１代替実施態様と組み合わせることができる第２代替実施態様では、本発明の方法は、コントローラエンティティとして知られているエンティティに対し、デモンストレータエンティティと呼ばれているエンティティに関連付けられたメッセージＭの完全性の証拠を提供するように設計される。前記デモンストレータエンティティは、証人を含む。前記デモンストレータエンティティおよびコントローラエンティティは、以下のステップを実行する。
・ステップ１のコミットメントＲという行為
各呼び出しでは、証人は、ここに前記に明記されたプロセスを適用することにより、各コミットメントＲを計算する。
・ステップ２のチャレンジｄという行為
証人は、その引数がメッセージＭおよび各コミットメントＲのすべてまたは一部であるハッシュ関数ｈを適用し、少なくとも１つのトークンＴを計算する。デモンストレータは、トークンＴをコントローラに送信する。コントローラは、トークンＴを受け取った後に、コミットメントＲに数で等しいチャレンジｄを作成し、チャレンジｄをデモンストレータに送信する。
・ステップ３の応答Ｄという行為
証人は、前記に明記されたプロセスを適用することによりチャレンジｄから応答Ｄを計算する。
・ステップ４のチェック行為
証人は、各応答Ｄをコントローラに送信する。ｍ個の公開値G_1，G_2，．．．，G_mを有するコントローラは、各チャレンジｄおよび各応答Ｄから再構築されたコミットメントＲ’を計算し、この再構築されたコミットメントＲ’が、次のタイプの関係性
$R' \equiv G_1^{d1}.\ G_2^{d2}.\ .\ .\ .\ G_m^{dm}.\ D^v \bmod n$
または、次のタイプの関係性
$R' \equiv D^v / G_1^{d1}.\ G_2^{d2}.\ .\ .\ .\ G_m^{dm}.\ \bmod n$
を満たす。
そして、コントローラは、その引数がメッセージＭおよび再構築されたＲ’のすべてまたは一部であるハッシュ関数ｈを適用し、トークンＴ’を再構築する。そして、コントローラは、トークンＴ’が送信されたトークンＴと同一であることを確認する。
【００１５】
（メッセージのデジタル署名およびその真正性の証明）
前記２つと組み合わせることができる第３代替実施態様においては、本発明１に従った方法が、署名するエンティティとして知られているエンティティによってメッセージＭのデジタル署名を作成するように設計される。前記署名エンティティは証人を含む。
【００１６】
（署名動作）
前記署名エンティティは、
メッセージＭと、
チャレンジｄおよび／またはコミットメントＲと、
応答Ｄと
を含む署名済みのメッセージを得るために、署名動作を実行する。
前記署名エンティティは、以下のステップを実行することにより署名動作を実行する。
・ステップ１のコミットメントＲという行為
各呼び出しでは、証人は、ここに前記に明記されるプロセスを適用することによって各コミットメントＲを計算する。
・ステップ２のチャレンジｄという行為
署名関係者は、その引数がメッセージＭおよび各コミットメントＲであるハッシュ関数ｈを適用し、バイナリトレインを得る。このバイナリトレインから、署名関係者は、その数

がコミットメントＲの数に等しいチャレンジｄを抽出する。
・ステップ３の応答Ｄという行為
証人は、前記に明記されたプロセスを適用することによりチャレンジｄから応答Ｄを計算する。
【００１７】
（チェック動作）
メッセージＭの真正性を証明するため、コントローラと呼ばれるエンティティが、署名済みのメッセージをチェックする。証明済みのメッセージを有する前記コントローラエンティティは、以下のように進むことによってチェック動作を実行する。
・コントローラがコミットメントＲ、チャレンジｄ、応答Ｄを有する場合
コントローラがコミットメントＲ、チャレンジｄ、応答Ｄを有する場合には、コントローラは、コミットメントＲ、チャレンジｄおよび応答Ｄが、以下のタイプの関係性
$R \equiv G_1^{d1} . G_2^{d2} . . . . G_m^{dm} . D^v \bmod n$
または、以下のタイプの関係性
$R \equiv D^v / G_1^{d1} . G_2^{d2} . . . . G_m^{dm} . \bmod n$
を満たすことを確認する。
そして、コントローラは、メッセージＭ、チャレンジｄおよびコミットメントＲがハッシュ関数を満たすことを確認する。
ｄ＝ｈ（ｍｅｓｓａｇｅ，Ｒ）
・コントローラがチャレンジｄおよび応答Ｄを有する場合
コントローラがチャレンジｄおよび応答Ｄを有する場合には、コントローラは、各チャレンジｄおよび各応答Ｄに基づき、コミットメントＲ'を再構築し、以下のタイプの関係性
$R' \equiv G_1^{d1} . G_2^{d2} . . . . G_m^{dm} . D^v \bmod n$
または以下のタイプの関係性：
$R' \equiv D^v / G_1^{d1} . G_2^{d2} . . . . G_m^{dm} . \bmod n$
を満たす。
そして、コントローラは、メッセージＭおよびチャレンジｄがハッシュ関数を満たすことを確認する。
ｄ＝ｈ（ｍｅｓｓａｇｅ，Ｒ'）
・コントローラが、コミットメントＲおよび応答Ｄを有する場合
コントローラが、コミットメントＲおよび応答Ｄを有する場合には、コントローラは、ハッシュ関数を適用し、ｄ'を再構築する。
ｄ’＝ｈ（ｍｅｓｓａｇｅ，Ｒ）
そして、コントローラ装置が、コミットメントＲ、チャレンジｄ'よび応答Ｄが、以下のタイプの関係性である
$R \equiv G_1^{d'1} . G_2^{d'2} . . . . G_m^{d'm} . D^v \bmod n$
または、以下のタイプの関係性である
$R \equiv D^v / G_1^{d'1} . G_2^{d'2} . . . . G_m^{d'm} . \bmod n$
を満たすことを確認する。
【００１８】
（システム）
本発明は、コントローラサーバに対して、エンティティの真正性、および／または、このエンティティに関連付けられたメッセージＭの完全性を証明するように設計されるシステムにも関する。
この証明は、以下のパラメータまたはこれらのパラメータの派生物のすべｔまたは一部によって確立される。ここで、パラメータは、
ｍ組の秘密値Q_1，Q_2，…Q_mおよび公開値G_1，G_2，…G_m（ｍは１以上）と、
前記ｆ個の素因数p_1，p_2，…p_f（ｆは２以上）の積によって構成される公開係数ｎと、
公開指数ｖとである。

前記係数、前記指数および前記値は、以下のタイプの関係
$G_i . Q_i^v \equiv 1 . \mathrm{mod}\ n$ または $G_i \equiv Q_i^v \mathrm{mod}\ n .$
によってリンクされる。
前記指数ｖは、
$v = 2^k$
であり、ここで、ｋは、１より大きい機密保護パラメータである。
前記公開値G_iは、ｆ個の素因数p_1，p_2，…p_f．より小さい基数g_iの平方g_i^2である。基数g_iは、２つの等式
$x^2 \equiv g_i \mathrm{mod}\ n$ および $x^2 \equiv -g_i \mathrm{mod}\ n$
が、モジュロｎの整数環のｘについて解くことができず、等式
$x^v \equiv g_i^2 \mathrm{mod}\ n$
が、モジュロｎの整数環のｘについて解くことができる。

【００１９】

前記システムは、特に、例えば、マイクロプセッサベースのバンクカードの形を取るノマッドオブジェクトに含まれる証人装置を含む。証人装置は、ｆ個の素因数p_iおよび／または素因数のチャイニーズ剰余の、および／または公開係数ｎおよび／またはｍ個の秘密値Q_iのパラメータ、および／または秘密値Q_iおよび公開指数ｖのｆ．ｍ個の構成要素$Q_{i,j}$（$Q_{i,j} \equiv Q_i \mathrm{mod}\ p_j$）を含むメモリゾーンを含む。また、証人装置は、
証人装置のこれ以降ランダム値生成手段と呼ばれるランダム値生成手段と、
これ以降証人装置のコミットメントＲの計算用手段と呼ばれる計算手段、
を含む。
計算手段は、モジュロｎの整数環でコミットメントＲを計算する。各コミットメントを、
・以下のタイプの演算を実行することによって、
$R \equiv r^v \mathrm{mod}\ n$
ここで、ｒは、ランダム値生成手段によって作成されるランダム値であり、ｒは０＜ｒ＜ｎである。
・または、以下のタイプの演算を実行し、
$R_i \equiv r_i^v \mathrm{mod}\ p_i$
ここで、r_iは、$0 < r_i < p_i$となるように素数p_iに関連付けられたランダム値であり、各r_iはランダム値｛r_1，r_2，…r_f｝の集合体に属し、そしてチャイニーズ剰余法を適用することのどちらかによって、
計算する。

【００２０】

証人装置は、
証人装置のチャレンジｄの受信用装置と呼ばれる1以上のチャレンジｄを受け取るための受信手段であって、各チャレンジｄが、初歩チャレンジと呼ばれるｍ個の整数d_iを備える受信手段と、
・以下のタイプの演算を実行することによって、
$D \equiv r . Q_1^{d1} . Q_2^{d2} . \cdots Q_m^{dm} \mathrm{mod}\ n$
・または、以下のタイプの演算を実行し、
$D_i \equiv r_i . Q_{i,1}^{d1} . Q_{i,2}^{d2} . \cdots Q_{i,m}^{dm} \mathrm{mod}\ p_i$
そして、チャイニーズ剰余法を適用することのどちらかによって、
応答Ｄの各チャレンジｄに基づき、計算用の証人装置の応答Ｄの計算用手段と呼ばれる計算手段と
を含む。
証人装置は、1以上のコミットメントＲおよび1以上の応答Ｄを送信するための送信手段も含む。コミットメントＲがあるので、チャレンジｄと同じくらい多くの応答Ｄがあり、Ｒ，ｄ，Ｄの各群が｛Ｒ，ｄ，Ｄ｝と参照される三つ組を形成する。

【００２１】

（エンティティの真正性の証明の場合）

第１実施態様では、デモンストレータと呼ばれているエンティティの真正性をコントローラと呼ばれているエンティティに証明するように、本発明に従ったシステムを設計する。前記システムは、それがデモンストレータエンティティと関連付けられたデモンストレータ装置を含んでいる。前記デモンストレータ装置は、相互接続手段によってデモンストレータ装置と相互接続される。それは、特に、例えば、マイクロプロセッサベースのバンクカード内のマイクロプロセッサの形式などのノマッドオブジェクトの論理マイクロ回路の形を取る。

前記システムは、コントローラエンティティに関連付けられたコントローラ装置も含む。前記コントローラ装置は、特に、端末または遠隔サーバの形を取る。前記コントローラ装置は、特にデータ処理通信網を通して、デモンストレータ装置へのその電気的、電磁的、光学的、または音響的な接続のための接続手段を含む。

【００２２】

前記システムは、以下のステップを実行するために使用される。

・ステップ１のコミットメントＲという行為

各呼び出しでは、証人装置のコミットメントＲの計算の手段が、ここに前記に明記されたプロセスを適用することによって、各コミットメントＲを計算する。証人装置は、各コミットメントＲのすべてまたは一部を相互接続手段を通してデモンストレータ装置に送信するために、証人装置の送信手段と呼ばれる送信の手段を有する。デモンストレータ装置は、各コミットメントＲのすべてまたは一部を接続手段を通してコントローラ装置に送信するために、デモンストレータの送信手段と呼ばれる送信手段も有する。

・ステップ２のチャレンジｄという行為

コントローラ装置は、コミットメントＲのすべてまたは一部を受け取った後、コミットメントＲの数に数で等しいチャレンジｄの生成のためのチャレンジ生成手段を含む。コントローラ装置は、接続手段を通してデモンストレータにチャレンジｄを送信するために、コントローラの送信手段として知られている送信手段も有する。

・ステップ３の応答Ｄという行為

証人装置のチャレンジｄの受信手段は、相互接続手段を通してデモンストレータ装置から着信する各チャレンジｄを受信する。証人装置の応答Ｄの計算手段は、ここに前記に明記されたプロセスを適用することによってチャレンジｄから応答Ｄを計算する。

・ステップ４のチェックという行為

デモンストレータの送信手段は、各応答Ｄをコントローラに送信する。コントローラは、
コントローラ装置の計算手段と呼ばれる計算手段と、
コントローラ装置の比較手段と呼ばれる比較手段と
を含む。

【００２３】

（第１の場合：デモンストレータが各コミットメントＲの一部を送信）

デモンストレータの送信手段が、各コミットメントＲの一部を送信した場合には、ｍ個の公開値G_1，G_2，．．．，G_mを有するコントローラ装置の計算手段は、各チャレンジｄおよび各応答Ｄから再構築されたコミットメントＲ’を計算し、この再構築されたコミットメントＲ’が、以下のタイプの関係

$R' \equiv G_1^{d1} . G_2^{d2} . . . . G_m^{dm} . D^v \bmod n$

または、次のタイプの関係

$R' \equiv D^v / G_1^{d1} . G_2^{d2} . . . . G_m^{dm} . \bmod n$

を満たす。

コントローラ装置の比較手段は、それぞれの再構築されたコミットメントＲ’を受信された各コミットメントＲのすべてまたは一部と比較する。

【００２４】

（第２の場合：デモンストレータが、各コミットメントＲの全体性を送信）

デモンストレータの送信手段が各コミットメントＲの全体性を送信した場合には、ｍ個の公開値G_1，G_2，．．．，G_mを有するコントローラ装置の計算手段および比較手段が、

各コミットメントＲが次のタイプの関係性
$R \equiv G_1^{d1} . G_2^{d2} . . . . G_m^{dm} . D^v \bmod n$
または、次のタイプの関係性
$R \equiv D^v / G_1^{d1} . G_2^{d2} . . . . G_m^{dm} . \bmod n$
を満たすことを確認する。
【００２５】
（メッセージの完全性の証明の場合）
第１代替実施態様と組み合わせることができる第２代替実施態様においては、本発明に従ったシステムは、コントローラとして知られているエンティティに対し、デモンストレータとして知られているエンティティに関連付けられたメッセージＭの完全性の証明を与えるように設計される。前記システムは、それがデモンストレータエンティティに関連付けられたデモンストレータ装置を含んでいる。前記デモンストレータ装置は相互接続手段によって証人装置と相互接続される。前記デモンストレータ装置は、特に、マイクロプロセッサベースのバンクカード内のマイクロプロセッサの形などのノマッドオブジェクト内の論理マイクロ回路の形を取りうる。前記システムは、コントローラエンティティに関連付けられたコントローラ装置も含む。前記コントローラ装置は、特に、端末または遠隔サーバの形を取る。前記コントローラ装置は、特にデータ処理通信網を通して、デモンストレータ装置へのその電気的、電磁的、光学的、または音響的な接続のための接続手段を含む。
【００２６】
前記システムは、以下のステップを実行するために使用される。
・ステップ１のコミットメントＲという行為
各呼び出しでは、証人装置のコミットメントＲの計算手段が、ここに前記に明記されたプロセスを適用することによって各コミットメントＲを計算する。証人装置は、相互接続手段を通してデモンストレータ装置に各コミットメントＲのすべてまたは一部を送信するために、証人装置の送信手段と呼ばれる送信手段を有する。
・ステップ２のチャレンジｄという行為
デモンストレータ装置は、デモンストレータの計算手段と呼ばれる計算手段を含み、その引数がメッセージＭおよびコミットメントＲのすべてまたは一部であるハッシュ関数ｈを適用し、少なくとも１つのトークンＴを計算する。デモンストレータ装置は、接続手段を通してコントローラ装置へ各トークンＴを送信するために、デモンストレータ装置の送信手段として知られる送信手段も含む。コントローラ装置は、トークンＴを受信した後、コミットメントＲの数に数で等しいチャレンジｄの生成のためのチャレンジ生成手段も有する。コントローラ装置は、接続手段を通してデモンストレータにチャレンジｄを送信するために、これ以降、コントローラの送信手段と呼ばれる送信手段も有する。
・ステップ３の応答Ｄという行為
証人装置のチャレンジｄの受信手段は、相互接続手段を通してデモンストレータ装置から着信する各チャレンジｄを受信する。証人装置の応答Ｄの計算手段は、ここに前記に明記されたプロセスを適用することによって、チャレンジｄから応答Ｄを計算する。
・ステップ４のチェックという行為
デモンストレータの送信手段は、コントローラに各応答Ｄを送信する。コントローラ装置は、第１に、各チャレンジｄおよび各応答Ｄから再構築されたコミットメントＲ’を計算するために、第２に、引数として、メッセージＭおよび各再構築されたコミットメントＲ’のすべてまたは一部を有するハッシュ関数ｈを適用することによって、トークンＴ’を計算するために、ｍ個の公開値G_1，G_2，．．．，G_mを有する、これ以降、コントローラ装置の計算手段と呼ばれる計算手段も備え、この再構築されたコミットメントＲ’が、次のタイプの関係性
$R' \equiv G_1^{d1} . G_2^{d2} . . . . G_m^{dm} . D^v \bmod n$
または、次のタイプの関係性
$R' \equiv D^v / G_1^{d1} . G_2^{d2} . . . . G_m^{dm} . \bmod n$

を満たす。
コントローラ装置は、計算されたトークンＴ’を受信されたトークンＴと比較するために、これ以降、コントローラ装置の比較手段として知られる比較手段も有する。
【００２７】
（メッセージのデジタル署名およびその真正性の証明）
第１の２つの実施態様のどちらかまたは両方と組み合わせることができる第３代替実施態様においては、本発明に従ったシステムは、署名エンティティと呼ばれているエンティティによって、これ以降、署名済みのメッセージとして知られているメッセージＭのデジタル署名を証明するように設計される。署名済みメッセージは、
メッセージＭと、
チャレンジｄおよび／またはコミットメントＲと、
応答Ｄと
を含む。
【００２８】
（署名動作）
前記システムは、それが署名エンティティと関連付けられた署名デバイスを含んでいる。前記署名デバイスは、相互接続手段によって証人装置と相互接続される。それは、特に、例えば、マイクロプロセッサベースのバンクカード内のマイクロプロセッサの形などのノマッドオブジェクト内の論理マイクロ回路の形を取りうる。
【００２９】
前記システムは、以下のステップを実行するために使用される。
・ステップ１のコミットメントＲという行為
各呼び出しでは、証人装置のコミットメントＲの計算手段が、ここに前記に明記されたプロセスを適用することによって各コミットメントＲを計算する。証人装置は、相互接続手段を通してデモンストレータ装置に各コミットメントＲのすべてまたは一部を送信するために、これ以降、証人装置の送信手段と呼ばれる送信手段を有する。
・ステップ２のチャレンジｄという行為
署名デバイスは、これ以降、署名デバイスの計算手段と呼ばれる計算手段を含み、その引数がメッセージＭおよびコミットメントＲのすべてまたは一部であるハッシュ関数ｈを適用し、バイナリトレインを計算し、このバイナリトレインから、その数がコミットメントＲの数に等しいチャレンジｄを抽出する。
・ステップ３の応答Ｄという行為
証人装置のチャレンジｄの受信手段は、相互接続手段を通して署名デバイスから着信する各チャレンジｄを受信する。証人装置の応答Ｄを計算するための手段は、ここに前記に明記されたプロセスを適用することによって、チャレンジｄから応答Ｄを計算する。
証人装置は、相互接続手段を通して署名デバイスに応答Ｄを送信するために、これ以降、証人装置の送信の手段と呼ばれる送信手段を含む。
【００３０】
（チェック動作）
メッセージＭの真正性を証明するために、コントローラとして知られているエンティティは、署名済みメッセージをチェックする。
システムは、コントローラエンティティと関連付けられたコントローラ装置を含む。前記コントローラ装置は、特に、端末または遠隔サーバの形を取る。前記コントローラ装置は、特に、データ処理通信網を通して署名デバイスへのその電気的、電磁的、光学的、または音響の接続のための接続手段を含む。
【００３１】
署名エンティティと関連付けられた署名デバイスは、接続手段を通した署名済みメッセージの、コントローラ装置への送信のための、署名デバイスの送信手段として知られている送信手段を含む。このようにして、コントローラ装置は、
メッセージＭと、

チャレンジｄおよび／またはコミットメントＲと、
応答Ｄと
を含む署名済みのメッセージを有する。
【００３２】
コントローラ装置は、
－これ以降、コントローラ装置の計算手段と呼ばれる計算手段と、
－これ以降、コントローラ装置の比較手段と呼ばれる比較手段と
を含む。
【００３３】
・コントローラ装置がコミットメントＲ、チャレンジｄ、応答Ｄを有する場合　コントローラ装置がコミットメントＲ、チャレンジｄ、応答Ｄを有する場合には、コントローラ装置の計算手段および比較手段は、コミットメントＲ、チャレンジｄおよび応答Ｄが、次のタイプの関係性
$R \equiv G_1^{d1} . G_2^{d2} . . . . G_m^{dm} . D^v \bmod n$
または次のタイプの関係性
$R \equiv D^v / G_1^{d1} . G_2^{d2} . . . . G_m^{dm} . \bmod n$
を満たすことを確認する。
そして、コントローラ装置の計算手段および比較手段は、メッセージＭ、チャレンジｄおよびコミットメントＲが、ハッシュ関数
ｄ＝ｈ（ｍｅｓｓａｇｅ，Ｒ）
を満たすことを確認する。
【００３４】
・コントローラ装置が、チャレンジｄおよび応答Ｄを有する場合
コントローラがチャレンジｄおよび応答Ｄを有する場合には、コントローラは、各チャレンジｄおよび各応答Ｄに基づき次のタイプの関係性
$R' \equiv G_1^{d1} . G_2^{d2} . . . . G_m^{dm} . D^v \bmod n$
または、次のタイプの関係性
$R' \equiv D^v / G_1^{d1} . G_2^{d2} . . . . G_m^{dm} . \bmod n$
を満たすコミットメントＲ'を再構築する。
そして、コントローラが、メッセージＭおよびチャレンジｄが以下のハッシュ関数
ｄ＝ｈ（ｍｅｓｓａｇｅ，Ｒ'）
を満たすことを確認する。
【００３５】
・コントローラがコミットメントＲおよび応答Ｄを有する場合
コントローラが、コミットメントＲおよび応答Ｄを有する場合には、コントローラ装置の計算手段は、ハッシュ関数を適用し
ｄ’＝ｈ（ｍｅｓｓａｇｅ，Ｒ）
となるようにｄ'を計算する。
そして、コントローラ装置の計算手段および比較手段は、コミットメントＲ、チャレンジｄ'および応答Ｄが、次のタイプの関係性
$R \equiv G_1^{d1} . G_2^{d2} . . . . G_m^{dm} . D^v \bmod n$
または、次のタイプの関係
$R \equiv D^v / G_1^{d1} . G_2^{d2} . . . . G_m^{dm} . \bmod n$
を満たすことを確認する。
【００３６】
（端末装置）
本発明は、エンティティに関連付けられた端末装置にも関する。端末装置は、特に、例えば、マイクロプロセッサベースのバンクカード内のマイクロプロセッサの形など、ノマッドオブジェクトの形を取る。端末装置は、コントローラサーバに対し、あるエンティティの真正性、および／または、このエンティティに関連付けられたメッセージＭの完全性を

証明するように設計される。
この証明は、以下のパラメータまたはこれらのパラメータの派生物のすべてまたは一部によって確立される。
m組の秘密値Q_1，Q_2，…Q_mおよび公開値G_1，G_2，…G_m（mは１以上）と、
前記ｆ個の素因数p_1，p_2，…p_f（ｆは２以上）によって構成される公開係数ｎと、
公開指数ｖとであり、
前記係数、前記指数、および前記値は、次のタイプの関係
$G_i . Q_i^v \equiv 1 . \mathrm{mod}\ n$または$G_i \equiv Q_i^v \mathrm{mod}\ n .$
によって関係付けられる。
前記指数ｖは、
$v = 2^k$
であり、ここで、ｋは、１より大きい機密保護パラメータである。
前記公開値G_iは、ｆ個の素因数p_1，p_2，…p_f．より小さい基数g_iの平方g_i^2である。基数g_iは、
２つの等式
$x^2 \equiv g_i \mathrm{mod}\ n$　および　$x^2 \equiv -g_i \mathrm{mod}\ n$
が、モジュロｎの整数環のｘについて解くことができず、等式
$x^v \equiv g_i^2 \mathrm{mod}\ n$
が、モジュロｎの整数環のｘの中で解くことができる。
前記端末装置は、ｆ個の素因数p_iおよび／または素因数のチャイニーズ剰余の、および／または公開係数ｎおよび／またはｍ個の秘密値Q_iのパラメータ、および／または秘密値Q_iの、および公開指数ｖのｆ．ｍ個の構成要素$Q_{i,j}$（$Q_{i,j} \equiv Q_i \mathrm{mod}\ p_j$）を含むメモリゾーンを備える証人装置を含む。
【００３７】
証人装置は、
証人装置のランダム値生成手段と呼ばれるランダム値生成手段と、
モジュロｎの整数環のコミットメントＲを計算するために、これ以降、証人装置のコミットメントＲを計算するために、これ以降、証人装置のコミットメントＲのための計算手段と呼ばれる計算手段と
を含む。各コミットメントが、
・以下のタイプの演算を実行することによって、
$R \equiv r^v \mathrm{mod}\ n$
ここで、ｒは、ランダム値生成手段によって作成されるランダム値であり、ｒは０＜ｒ＜ｎとなる。
・または、以下のタイプの演算を実行することによって、
$R_i \equiv r_i^v \mathrm{mod}\ p_i$
ここで、r_iは、$0 < r_i < p_i$となるように、素数p_iと関連付けられたランダム値であって、各r_iは、ランダム値生成手段によって生じるランダム｛r_1，r_2，…r_f｝の集合体に属し、そして、チャイニーズ剰余を適用することのどちらかによって、計算される。
【００３８】
証人装置は、
1以上のチャレンジｄを受信するために、これ以降、証人装置のチャレンジｄの受信のための主だと呼ばれる受信手段であって、各チャレンジｄが、これ以降初歩チャレンジと呼ばれるｍ個の整数d_iを備える受信手段と、
・以下のタイプの演算を実行すること、
$D \equiv r . Q_1^{d1} . Q_2^{d2} . \cdots Q_m^{dm} \mathrm{mod}\ n$
・または、以下のタイプの演算を実行し、
$D_i \equiv r_i . Q_{i,1}^{d1} . Q_{i,2}^{d2} . \cdots Q_{i,m}^{dm} \mathrm{mod}\ p_i$
そして、チャイニーズ剰余法を適用すること
のどちらかによって、

応答Ｄの各チャレンジｄに基づく、計算のための証人装置の応答Ｄの計算のための手段と呼ばれる計算手段と
も含む。
前記証人装置は、1以上のコミットメントＲおよび1以上の応答Ｄを送信するために送信手段も含む。コミットメントＲがあるため、チャレンジｄと同じくらい多くの応答Ｄがある。数Ｒ，ｄ，Ｄの各群は、｛Ｒ，ｄ，Ｄ｝と参照される三つ組を形成する。
【００３９】
（エンティティの真正性の証明の場合）
第１代替実施態様においては、本発明に従った端末装置は、デモンストレータと呼ばれているエンティティの真正性をコントローラと呼ばれているエンティティに証明するように設計される。
前記端末装置は、それがデモンストレータエンティティに関連付けられたデモンストレータ装置を含んでいる。前記デモンストレータ装置は、相互接続手段によってデモンストレータ装置と相互接続している。それは、特に、例えば、マイクロプロセッサベースのバンクカード内のマイクロプロセッサという形などのノマッドオブジェクト内の論理マイクロ回路という形を取りうる。
前記デモンストレータ装置は、特にデータ処理通信網を通して、コントローラエンティティに関連付けられたコントローラ装置へのその電気的、電磁的、光学的または音響の接続のための接続手段も含む。
【００４０】
前記コントローラ装置は、特に端末または遠隔サーバの形を取る。
前記コントローラ装置は、以下のステップを実行するために使用される。
・ステップ１のコミットメントＲという行為
各呼び出しでは、証人装置のコミットメントＲの計算手段が、ここに前記に明記されたプロセスを適用することによって各コミットメントＲを計算する。
証人装置は、各コミットメントＲのすべてまたは一部を相互接続手段を通してデモンストレータ装置に送信するために、これ以降、証人装置の送信手段と呼ばれる送信手段を有する。デモンストレータ装置は、各コミットメントＲのすべてまたは一部をコントローラ装置に送信するために、これ以降、デモンストレータの送信手段と呼ばれる送信手段も有する。
・ステップ２および３のチャレンジｄという行為および応答Ｄという行為
証人装置のチャレンジｄの受信手段は、コントローラ装置とデモンストレータ装置の間の接続手段を通して、およびデモンストレータ装置と証人装置の間の相互接続手段を通して、コントローラ装置から着信する各チャレンジｄを受信する。証人装置の応答Ｄの計算手段は、ここに前記に明記されるプロセスを適用することにより、チャレンジｄから応答Ｄを計算する。
・ステップ４のチェックという行為
デモンストレータの送信手段は、各応答Ｄをチェックを実行するコントローラに送信する。
【００４１】
（メッセージの完全性の証明の場合）
第１代替実施態様と組み合わせることのできる第２代替実施態様においては、本発明に従った端末装置は、コントローラとして知られるエンティティに対し、デモンストレータとして知られるエンティティに関連付けられたメッセージＭの完全性の証明を与えるように設計される。前記端末装置は、それがデモンストレータエンティティに関連付けられたデモンストレータ装置を含んでいる。前記デモンストレータ装置は、相互接続手段によって証人装置と相互接続されている。それは、特に、例えば、マイクロプロセッサベースのバンクカード内のマイクロプロセッサの形などの、ノマッドオブジェクト内の論理マイクロ回路の形を取りうる。前記デモンストレータ装置は、特に、データ処理通信網を通したコントローラエンティティに関連付けられたコントローラ装置へのその電気的、電磁的、光

学的または音響の接続のための接続手段を含む。前記コントローラ装置は、特に、端末または遠隔サーバの形を取る。

【００４２】

前記端末装置は、以下のステップを実行するために使用される。

・ステップ１のコミットメントＲという行為

各呼び出しでは、証人装置のコミットメントＲの計算手段が、ここに前記に明記されたプロセスを適用することによって、各コミットメントＲを計算する。証人装置は、相互接続手段を通してデモンストレータ装置に各コミットメントＲのすべてまたは一部を送信するために、これ以降、証人装置の送信手段と呼ばれる送信の手段を有する。

・ステップ２および３のチャレンジｄという行為および応答Ｄという行為

デモンストレータ装置は、これ以降、デモンストレータの計算手段と呼ばれる計算手段を含み、その引数が、メッセージＭおよび各コミットメントＲのすべてまたは一部であるハッシュ関数ｈを適用し、少なくとも１つのトークンＴを計算する。デモンストレータ装置は、コントローラ装置に、接続手段を通して、各トークンＴを送信するために、これ以降、デモンストレータ装置の送信手段として知られている送信手段も有する。

前記コントローラは、トークンＴを受信した後、コミットメントＲの数に等しい数のチャレンジｄを作成する。

証人装置のチャレンジｄの受信手段は、コントローラ装置とデモンストレータ装置の間の接続手段を通して、およびデモンストレータ装置と証人装置の間の相互接続手段を通して、コントローラ装置から着信する各チャレンジｄを受信する。証人装置の応答Ｄの計算の手段は、ここに前記に明記されたプロセスを適用することによって、チャレンジｄから応答Ｄを計算する。

・ステップ４のチェックという行為

デモンストレータの送信手段は、各応答Ｄを、チェックを実行するコントローラ装置に送信する。

【００４３】

（メッセージのデジタル署名およびその真正性の証明）

第１の２つの実施態様のどちらかまたは両方と組み合わせることのできる第３代替実施態様においては、本発明に従った端末装置が、署名エンティティと呼ばれるエンティティによる、これ以降、署名済みメッセージとして知られるメッセージＭのデジタル署名を作成するように設計される。署名済みメッセージは、

メッセージＭと、

チャレンジｄおよび／またはコミットメントＲと、

応答Ｄと

を含む。

前記端末装置は、それが署名エンティティと関連付けられた署名デバイスを含んでいる。前記署名デバイスは、相互接続手段によって証人装置と相互接続される。それは、特に、例えば、マイクロプロセッサベースのバンクカード内のマイクロプロセッサの形などの、ノマッドオブジェクト内の論理マイクロ回路の形を取りうる。前記デモンストレータ装置は、データ処理通信網を通したコントローラエンティティと関連付けられたコントローラ装置への、その電気的、電磁的、光学的、または音響の接続のための接続手段を含む。前記コントローラ装置は、特に、端末または遠隔サーバの形を取る。

【００４４】

（署名動作）

前記端末装置は、以下のステップを実行するために使用される。

・ステップ１のコミットメントＲという行為

各呼び出しでは、証人装置のコミットメントＲの計算の手段が、ここに前記に明記されたプロセスを適用することによって、各コミットメントＲを計算する。証人装置は、相互接続手段を通して署名デバイスに各コミットメントＲのすべてまたは一部を送信するために、これ以降、証人装置の送信手段と呼ばれる送信の手段を有する。

・ステップ２のチャレンジｄという行為
署名デバイスは、これ以降、署名デバイスの計算手段と呼ばれる計算手段を含み、その引数がメッセージＭおよび各コミットメントＲのすべてまたは一部であるハッシュ関数ｈを適用し、バイナリトレインを計算し、このバイナリトレインから、その数がコミットメントＲの数に等しいチャレンジｄを抽出する。
・ステップ３の応答Ｄという行為
証人装置のチャレンジｄの受信のための手段は、相互接続手段を通して署名デバイスから着信する各チャレンジｄを受信する。証人装置の応答Ｄを計算するための手段は、ここに前記に明記されたプロセスを適用することによって、チャレンジｄから応答Ｄを計算する。証人装置は、相互接続手段を通して、署名デバイスに応答Ｄを送信するために、これ以降、証人装置の送信の手段と呼ばれる送信手段を含む。

【００４５】
（コントローラ装置）
本発明は、コントローラ装置にも関する。コントローラ装置は、特に、コントローラエンティティに関連付けられた端末または遠隔サーバの形を取る。コントローラ装置は、エンティティの真正性、および／または、このエンティティに関連付けられたメッセージＭの完全性をチェックするように設計される。
この証明は、以下のパラメータまたはこれらのパラメータの派生物のすべてまたは一部によって確立される。
ｍ組の公開値G_1，G_2，…G_m（ｍは１以上）と、
コントローラ装置にとって、および関連付けられたコントローラエンティティにとって未知である前記ｆ個の素因数p_1，p_2，…p_f（ｆは２以上）の積によって構成される公開係数ｎと、
公開指数ｖと
前記係数、前記指数、および前記値は、次のタイプの関係
$G_i \cdot Q_i^v \equiv 1 \mod n$ または $G_i \equiv Q_i^v \mod n$.
によって関連付けられ、ここで、Q_iは、公開値G_Iに関連付けられたコントローラ装置にとって未知の秘密値を指定する。
指数ｖは、
$v = 2^k$
であり、ここで、ｋは、１より大きい機密保護パラメータである。
前記公開値G_iは、ｆ個の素因数p_1，p_2，…p_fより小さい基数g_iの平方g_i^2である。
基数g_iは、
２つの等式
$x^2 \equiv g_i \mod n$ および $x^2 \equiv -g_i \mod n$
が、モジュロｎの整数環のｘについて解くことができず、
等式
$x^v \equiv g_i^2 \mod n$
が、モジュロｎの整数環のｘについて解くことができる。

【００４６】
（エンティティの真正性の証明の場合）
第１代替実施態様においては、本発明に従ったコントローラ装置は、デモンストレータと呼ばれるエンティティおよびコントローラと呼ばれるエンティティの真正性を証明するように設計される。
前記コントローラ装置は、デモンストレータエンティティと関連付けられたデモンストレータ装置への、特にデータ処理通信網を通した、その電気的、電磁的、光学的、または音響の接続のための接続手段を含む。
前記コントローラ装置は、以下のステップを実行するために使用される。
・ステップ１および２のコミットメントＲという行為およびチャレンジｄという行為
前記コントローラ装置は、接続手段を通して、デモンストレータ装置から着信するコミッ

トメントＲのすべてまたは一部の受信のための手段も有する。
コントローラ装置は、各コミットメントＲのすべてまたは一部を受信した後、コミットメントＲの数に等しい数のチャレンジｄの生成のためのチャレンジ生成手段を有し、各チャレンジｄは、初歩チャレンジと呼ばれるｍ個の整数d_iを備える。
コントローラ装置は、接続手段を通してデモンストレータにチャレンジｄを送信するために、コントローラの送信手段と呼ばれる送信手段も有する。
・ステップ３および４の応答Ｄという行為およびチェック行為
コントローラ装置は、
接続手段を通して、デモンストレータ装置から着信する応答Ｄの受信のための手段と、
これ以降、コントローラ装置の計算手段と呼ばれる計算手段と、
これ以降、コントローラ装置の比較手段と呼ばれる比較手段と
を含む。
（第１の場合：デモンストレータが各コミットメントＲの一部を送信）
デモンストレータの受信手段が各コミットメントＲの一部を受信すると、ｍ個の公開値$G_1, G_2, \ldots, G_m$を有するコントローラ装置の計算手段が、各チャレンジｄおよび各応答Ｄから、再構築されたコミットメントＲ’を計算し、この再構築されたコミットメントは、次のタイプの関係性

$$R' \equiv G_1^{d1} . G_2^{d2} . \ldots . G_m^{dm} . D^v \bmod n$$

または、次のタイプの関係性

$$R' \equiv D^v / G_1^{d1} . G_2^{d2} . \ldots . G_m^{dm} . \bmod n$$

を満たす。
コントローラ装置の比較手段は、受信された各コミットメントＲのすべてまたは一部と、各再構築されたコミットメントＲ’を比較する。
（第２の場合：デモンストレータが各コミットメントＲの全体性を送信）
デモンストレータの送信手段が、各コミットメントＲの全体性を送信した場合には、ｍ個の公開値$G_1, G_2, \ldots, G_m$を有するコントローラ装置の計算手段および比較手段が、各コミットメントＲが、次のタイプの関係性

$$R \equiv G_1^{d1} . G_2^{d2} . \ldots . G_m^{dm} . D^v \bmod n$$

または、次のタイプの関係性

$$R \equiv D^v / G_1^{d1} . G_2^{d2} . \ldots . G_m^{dm} . \bmod n$$

を満たすことを確認する。
【００４７】
（メッセージの完全性の証明の場合）
第１代替実施態様と結び付けることができる第２代替実施態様においては、本発明に従ったコントローラ装置が、コントローラとして知られるエンティティに対し、デモンストレータとして知られているエンティティと関連付けられたメッセージＭの完全性の証明を与えるように設計される。
前記コントローラ装置は、特にデータ処理通信網を通した、デモンストレータエンティティと関連付けられたデモンストレータ装置へのその電気的、電磁的、光学的、または音響の接続のための接続手段を含む。
前記システムは、以下のステップを実行するために使用される。
・ステップ１および２のコミットメントＲという行為およびチャレンジｄという行為
前記コントローラ装置は、接続手段を通してデモンストレータ装置から着信するトークンＴの受信のための手段も有する。コントローラ装置は、トークンＴを受信した後、コミットメントＲの数に数で等しいチャレンジｄの生成のためのチャレンジ生成手段を有し、各チャレンジｄは、呼び出された初歩チャレンジの後にここにｍ個の整数d_iを備える。コントローラ装置は、接続手段を通してデモンストレータへチャレンジｄを送信するために、これ以降、コントローラの送信手段と呼ばれる送信手段も有する。
・ステップ３および４の応答Ｄという行為およびチェック行為
コントローラ装置は、接続手段を通してデモンストレータ装置から着信する応答Ｄの受信

のための手段も含む。前記コントローラ装置は、第１に、各チャレンジｄおよび各応答Ｄから再構築されたコミットメントＲ’を計算するために、および第２に、メッセージＭおよび各再構築されたコミットメントＲ’のすべておよび一部として有するハッシュ関数ｈを適用することによってトークンＴ’を計算するために、ｍ個の公開値G_1，G_2，．．．，G_mを有する、これ以降、コントローラ装置の計算手段と呼ばれる計算手段も含み、この再構築されたコミットメントＲ’は、次のタイプの関係性

$R' \equiv G_1^{d1} . G_2^{d2} . . . . G_m^{dm} . D^v \bmod n$

または、次のタイプの関係性

$R' \equiv D^v / G_1^{d1} . G_2^{d2} . . . . G_m^{dm} . \bmod n$

を満たす。

コントローラ装置は、計算されたトークンＴ’を受信されたトークンＴと比較するために、これ以降、コントローラ装置の比較手段と呼ばれる比較手段も有する。

【００４８】

（メッセージのデジタル署名およびその真正性の証明）

第１の２つの実施態様のどちらか、または両方と組み合わせることのできる第３代替実施態様のいては、本発明に従ったコントローラ装置は、コントローラと呼ばれるエンティティによって署名済みのメッセージをチェックすることによって、メッセージＭの真正性を証明するように設計される。

ハッシュ関数ｈ（メッセージ，Ｒ）を有する署名エンティティに関連付けられた署名デバイスによって送信される署名済みメッセージは、

メッセージＭと、

チャレンジｄおよび／またはコミットメントＲと、

応答Ｄと

を含む。

【００４９】

（チェック動作）

前記コントローラ装置は、署名エンティティに関連付けられた署名デバイスへの、特にデータ処理通網を通した、その電気的、電磁的、光学的または音響の接続のための接続手段を備える。前記コントローラ装置は、接続手段を通して、署名済みメッセージを、署名されたデバイスから受信する。

コントローラ装置は、

コントローラ装置の計算手段と呼ばれる計算手段と、

コントローラ装置の比較手段と呼ばれる比較手段と

を含む。

・コントローラ装置が、コミットメントＲ、チャレンジｄ、応答Ｄを有する場合

コントローラがコミットメントＲ、チャレンジｄ、応答Ｄを有する場合、コントローラ装置の計算手段および比較手段は、コミットメントＲ、チャレンジｄおよび応答Ｄが、次のタイプの関係性

$R \equiv G_1^{d1} . G_2^{d2} . . . . G_m^{dm} . D^v \bmod n$

または、次のタイプの関係性

$R \equiv D^v / G_1^{d1} . G_2^{d2} . . . . G_m^{dm} . \bmod n$

を満たすことを確認する。

そして、監査デバイスの計算手段および比較手段は、メッセージＭ、チャレンジｄおよびコミットメントＲが、ハッシュ関数

ｄ’＝ｈ（ｍｅｓｓａｇｅ，Ｒ）

を満たすことを確認する。

・コントローラ装置がチャレンジｄおよび応答Ｄを有する場合

コントローラ装置が、チャレンジｄおよび応答Ｄを有する場合には、コントローラの計算手段は、各チャレンジｄおよび各応答Ｄに基づいて、次のタイプの関係性

$R' \equiv G_1^{d1} . G_2^{d2} . . . . G_m^{dm} . D^v \bmod n$

または、次のタイプの関係性
$R' \equiv D^{v} / G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . \mathrm{mod}\ n$
を満たすコミットメントR'を計算する。
そして、コントローラ装置の計算手段および比較手段は、メッセージMおよびチャレンジdが、ハッシュ関数
d＝h（ｍｅｓｓａｇｅ，R'）
を満たすのを確認する。
・コントローラ装置がコミットメントRおよび応答Dを有する場合
コントローラ装置が、コミットメントRおよび応答Dを有する場合、コントローラ装置の計算手段は、ハッシュ関数を適用し、
d＝h（ｍｅｓｓａｇｅ，R）
となるように、d'を計算する。
そして、コントローラ装置の計算手段および比較手段は、コミットメントR、チャレンジd'および応答Dが、次のタイプの関係性
$R \equiv G_1^{d'1} . G_2^{d'2} . \ldots G_m^{d'm} . D^{v} \mathrm{mod}\ n$
または、次のタイプの関係性
$R \equiv D^{v} / G_1^{d'1} . G_2^{d'2} . \ldots G_m^{d'm} . \mathrm{mod}\ n$
を満たすのを確認する。

【００５０】

（説明）

ＧＱ技術の目標を想起することができる。つまり、それはメッセージのデジタル署名だけではなくエンティティおよび関連付けられたメッセージの動的認証である。

【００５１】

ＧＱ技術の標準バージョンは、ＲＳＡ技術を利用する。しかしながら、ＲＳＡ技術は、真に因数分解に依存するが、この依存は、ＲＳＡ技術を実行しているデジタル署名の多様な規格に対するいわゆる倍数的に増加する攻撃に見られるように、同等ではなく、実際にはかなりそれと異なっている。

【００５２】

ＧＱ２技術という文脈では、本発明のこの部分は、さらに明確には動的認証およびデジタル署名という文脈でのＧＱ２鍵の集合の使用に関する。ＧＱ２技術はＲＳＡ技術を使用しない。目標は２つの部分を有する。つまり、第１に、ＲＳＡ技術に関して性能を改善し、第２にＲＳＡ技術に固有の問題を妨げることである。ＧＱ２秘密鍵は、係数ｎの因数分解である。ＧＱ２三つ組に対する攻撃は、係数ｎの因数分解に相当する。このときには同等がある。ＧＱ２技術を使用すると、署名をするエンティティまたは認証されるエンティティ、およびチェックを行うエンティティの両方にとっての作業量が削減される。機密保護およぎ性能という点での、因数分解の問題の改善された使用を通して、ＧＱ２技術はＲＳＡ技術に匹敵する。

【００５３】

ＧＱ２技術は、１より大きい1以上の小さな整数、例えば、基数と呼ばれ、g_iと参照されるｍ個の小さい整数（ｍ≧１）を使用する。基数はｍ＞１でg_iからg_mで固定されるため、公開検鍵＜ｖ，ｎ＞が、以下のように選択される。公開認証指数ｖは2^{k}であり、ここで、ｋは１（ｋ≧２）を上回る小さい整数である。公開係数ｎは、基数より大きい少なくとも２つの素因数、例えばp_jによって$p_1 \cdots p_f$から参照されるｆ個の素因数（ｆ≧２）の積である。ｆ個の素因数は、公開係数ｎが、g_1からg_mｍ個の基数のそれぞれに関して以下の特性を有するように選択される。
第１に、等式（数１）および（数２）は、モジュロｎの整数環のｘについて解くことができない。つまり、g_iおよび？g_iは２つの非平方剰余（ｍｏｄ　ｎ）である。
【数１】

$$x^2 \equiv g_i \pmod{n}$$

【数２】

$$x^2 \equiv -g_i \pmod{n}$$

第２に、等式（数３）は、モジュロｎの整数環のｘについて解くことができる。

【数３】

$$x^{2^k} \equiv g_i^2 \pmod{n}$$

【００５４】

公開認証鍵＜ｖ，ｎ＞は、ｍ≧１でg_1からg_mの基数に従って固定されているため、各基数g_iが公開値G_iと秘密値Q_Iを備える値ＧＱ２の組を決定する。ｍ組の参照されたG_1Q_1からG_mQ_mを指定する。公開値G_iは、基数g_Iの平方である。つまり、$G_i = g_i^2$を指定する。秘密値Q_iは、等式（数３）に対する解の１つであるか、さもなければこのような解の逆数（ｍｏｄ　ｎ）である。

【００５５】

ちょうど係数ｎがｆ個の素数に分解されるように、モジュロｎの整数環はＣＧ（p_1）からＣＧ（p_f）というｆ個のガロア体（Galois field）に分解される。ここにＣＧ（p_j）での等式（数１）、（数２）、および（数３）の投射がある。

【数４】

$$x^2 \equiv g_i \pmod{p_j}$$

【数５】

$$x^2 \equiv -g_i \pmod{p_j}$$

【数６】

$$x^{2^k} \equiv g_i^2 \pmod{p_j}$$

【００５６】

各秘密値Q_iは、素因数あたり１個づつｆ個の秘密構成要素によって一意に表すことができる。$Q_{i,j} \equiv Q_i$（ｍｏｄ　p_j）．各秘密構成要素$Q_{i,j}$は等式（数６）に対する解であるか、またはさもなければこのような解の逆数（ｍｏｄ　p_j）である。各等式（数６）に対するすべての考えられる解が計算された後に、チャイニーズ剰余技法が、等式（数３）に対するすべての考えられる解を得るために$Q_{i,1}$から$Q_{i,f}$：Q_iというｆ個の構成要素＝チャイニーズ剰余（$Q_{i,1}$，$Q_{i,2}$，…$Q_{i,f}$）に基づき、秘密値Q_iごとにすべての考えられる値をセットアップする。

【００５７】

以下は、チャイニーズ剰余技法である。０＜ａ＜ｂとなるように相互に素数ａとｂである２つの正の整数、および０からａ－１のX_aおよび０からｂ－１のX_bという２つの構成要素があるとする。$X_a \equiv X$（ｍｏｄ　ａ）および$X_b \equiv X$（ｍｏｄ　ｂ）となるように、Ｘ＝チャイニーズ剰余（X_a，X_b）、つまり０からａ．ｂ－１の一意のＸを決定することが必要とされる。以下は、チャイニーズ剰余パラメータである。つまり、$\alpha \equiv \{b \pmod{a}\}^{-1}$（ｍｏｄ　ａ）。以下はチャイニーズ剰余演算である。つまり、$\varepsilon \equiv X_b \pmod{a}$、$\delta = X_a \cdot \varepsilon$、δが負である場合には、δをδ＋ａと、$\gamma \equiv \alpha . \delta \pmod{a}$

）と、$X = \gamma . b + X_b$とに置換する。

【００５８】

素因数が最小のp_1から大きい方のp_fへと昇順で並べられるとき、チャイニーズ剰余パラメータは以下となることがある（それらのｆ－１がある、つまり素因数より１少ない）。第１チャイニーズ剰余パラメータは、$\alpha \equiv \{p_2 (\mathrm{mod}\ p_1)\}^{-1} (\mathrm{mod}\ p_1)$である。第２チャイニーズ剰余パラメータは$\beta \equiv \{p_1 . p_2 (\mathrm{mod}\ p_3)\}^{-1} (\mathrm{mod}\ p_3)$である。ｉ番目のチャイニーズ剰余パラメータは、$\lambda \equiv \{p_1 . p_2 . \cdots p_{i-1} (\mathrm{mod}\ p_i)\}^{-1} (\mathrm{mod}\ p_i)$である。等々。最後に、ｆ－１個のチャイニーズ剰余演算で第１結果（ｍｏｄ p_2にp_1をかける）が第１パラメータで得られてから、第２結果（ｍｏｄ $p_1 . p_2$にp_3をかける）が第２パラメータで得られ、結果（ｍｏｄ $p_1 . \cdots p_{f-1}$にp_fをかける）、すなわち（ｍｏｄ ｎ）が得られまで等々である。

【００５９】

秘密鍵ＧＱ２の多様な性質を表す、秘密鍵ＧＱ２のいくつかの考えられる描写がある。多様な描写は同等であることが判明する。つまり、それらはすべて、真の秘密ＧＱ２件である係数ｎの因数分解の知識に相当する。描写が真に署名エンティティまたは自己認証エンティティの動きに影響を及ぼすのであれば、それはコントローラエンティティの動きには影響を及ぼさない。

ここに、ＧＱ２秘密鍵の考えられる３つの主要な描写がある。

１）ＧＱ技術での標準表記は、ｍ個の秘密値Q_iと公開認証鍵＜ｖ，ｎ＞の記憶から成り立つ。ＧＱ２においては、この描写には、以下の２つが匹敵する。２）作業量という点での最適表記は、公開指数ｖ、ｆ個の素因数p_j、ｍ．ｆ個の秘密構成要素Q_{ij}およびチャイニーズ剰余のｆ－１個のパラメータを記憶することにある。３）秘密鍵サイズという点での最適表記は、公開指数ｖ、ｍ個の基数g_iおよびｆ個の素因数p_jを記憶すること、そして、ｍ個の秘密値Q_iおよび係数ｎをセットアップして、第１描写に戻るか、またはさもなければｍ．ｆ個の秘密構成要素$Q_{i,j}$およびチャイニーズ剰余のｆ－１個のパラメータをセットアップして第２描写に戻るかのどちらかによって各使用を開始することにある。

【００６０】

署名または自己認証エンティティは、すべて同じ基数を使用できる。それ以外に示されていない限り、g_1からg_mのｍ個の基数は、有利なことにｍ個の第１素数となることがある。

【００６１】

動的認証機構またはデジタル署名機構の機密保護は係数の分解の知識に同等であるため、ＧＱ２技術は同じ係数を使用する２つのエンティティを単に区別するために使用することはできない。一般的に、それ自体を認証するまたは署名する各エンティティは専用のＧＱ２係数を有する。しかしながら、４つの素因数でＧＱ２係数を指定することは可能であり、その内の２つはあるエンティティによって知られており、他の２つは別のエンティティによって知られている。

【００６２】

ここでは、ｋ＝６がｖ＝６４を示し、ｍ＝３が３つの基数、$g_1 = 3$，$g_2 = 5$および、$g_3 = 7$を示し、ｆ＝３、つまり２つが３（ｍｏｄ ４）に一致し、１つが５（ｍｏｄ ８）に一致する３つの素因数を含む係数であるＧＱ２鍵の第１集合がある。ｇ＝２が、５（ｍｏｄ ８）に一致する素因数と相容れないことを注意しなければならない。

p_1＝０３ＣＤ２Ｆ４Ｆ２１Ｅ０ＥＡＤ６０２６６Ｄ５ＣＦＣＥＢＢ６９５４６８３４９３Ｅ２Ｅ８３３

p_2＝０５８３Ｂ０９７Ｅ８Ｄ８Ｄ７７７ＢＡＢ３８７４Ｆ２Ｅ７６６５９ＢＢ６１４Ｆ９８５ＥＣ１Ｂ

p_3＝０Ｃ３６３ＣＤ９３Ｄ６Ｂ３ＦＥＣ７８ＥＥ１３Ｄ７ＢＥ９Ｄ８４３５４Ｂ８ＦＤＤ６ＤＡ１ＦＤ

$n = p_1 . p_2 . p_3$＝ＦＦＦＦ８１ＣＥＡ１４９ＤＣＦ２Ｆ７２ＥＢ４４９Ｃ５７２４７

４２ＦＥ２Ａ３６３０Ｄ９
０２ＣＣ００ＥＡＦＥＥ１Ｂ９５７Ｆ３ＢＤＣ４９ＢＥ９ＣＢＤ４Ｄ９４４６７Ｂ７２Ａ
Ｆ２８ＣＦＢＢ２６１４４
ＣＤＦ４ＢＢＤＢＡ３Ｃ９７５７８Ｅ２９ＣＣ９ＢＢＥＥ８ＦＢ６ＤＤＤＤ
$Q_{1,1}$＝０２７９Ｃ６０Ｄ２１６６９６ＣＤ６Ｆ７５２６Ｅ２３５１２ＤＡＥ０９０ＣＦ
Ｆ８７９ＦＤＤＥ
$Q_{2,1}$＝７Ｃ９７７ＦＣ３８Ｆ８４１３Ａ２８４Ｅ９ＣＥ４ＥＤＥＦ４ＡＥＦ３５ＢＦ７
７９３Ｂ８９
$Q_{3,1}$＝６ＦＢ３Ｂ９ＣＯ５Ａ０３Ｄ７ＣＡＤＡ９Ａ３４２５５７１ＥＦ５ＥＣＣ５４Ｄ
７Ａ７Ｂ６Ｆ
$Q_{1,2}$＝０３８８ＥＣ６ＡＡ１Ｅ８７６１３Ｄ８３２Ｅ２Ｂ８０Ｅ５ＡＥ８Ｃ１ＤＦ２Ｅ
７４ＢＦＦ５０２
$Q_{2,2}$＝０４７９２ＣＥ７０２８４Ｄ１６Ｅ９Ａ１５８Ｃ６８８Ａ７Ｂ３ＦＥＡＦ９Ｃ４
００５６４６９Ｅ
$Q_{3,2}$＝ＦＤＣ４Ａ８Ｅ５３Ｅ１８５Ａ４ＢＡ７９３Ｅ９３ＢＥＥ５Ｃ６３６ＤＡ７３１
ＢＤＣＡ４Ｅ
$Q_{1,3}$＝０７ＢＣ１ＡＢ０４８Ａ２ＥＡＦＤＡＢ５９ＢＤ４０ＣＣＦ２Ｆ６５７ＡＤ８Ａ
６Ｂ５７３ＢＤＥ
$Q_{2,3}$＝０ＡＥ８５５１Ｅ１１６Ａ３ＡＣ０８９５６６ＤＦＤＢ３ＡＥ００３ＣＦ１７４
ＦＣ４Ｅ４８７７
$Q_{3,3}$＝０１６８２Ｄ４９００４１９１３Ａ４ＥＡ５Ｂ８０Ｄ１６Ｂ６８５Ｅ４Ａ６ＤＤ
８８０７０５０１
Q_{1}＝Ｄ７Ｅ１ＣＡＦ２８１９２ＣＥＤ６５４９ＦＦ４５７７０８Ｄ５０Ａ７４８１５７
２ＤＤ５Ｆ２Ｃ３３５Ｄ８
Ｃ６９Ｅ２２５２１Ｂ５１０Ｂ６４４５４ＦＢ７Ａ１９ＡＥＣ８Ｄ０６９８５５５８Ｅ７
６４Ｃ６９９１Ｂ０５ＦＣ２Ａ
Ｃ７４Ｄ９７４３４３５ＡＢ４Ｄ７ＣＦ０ＦＦ６５５７
Q_{2}＝ＣＢ１ＥＤ６Ｂ１ＤＤ６４９Ｂ８９Ｂ９６３８ＤＣ３３８７６Ｃ９８ＡＣ７ＡＦ６
８９Ｅ９Ｄ１３５９Ｅ４
ＤＢ１７５６３Ｂ９Ｂ３ＤＣ５８２Ｄ５２７１９４９Ｆ３ＤＢＡ５Ａ７０Ｃ１０８Ｆ５６
１Ａ２７４４０５Ａ５ＣＢ８
８２２８８２７３ＡＤＥ６７３５３Ａ５ＢＣ３１６Ｃ０９３
Q_{3}＝０９ＡＡ６Ｆ４９３０Ｅ５１Ａ７０ＣＣＤＦＡ７７４４２Ｂ１０７７０ＤＤ１ＣＤ
７７４９０Ｅ３３９８Ａ
ＡＤ９ＤＣ５０２４９Ｃ３４３１２９１５Ｅ５５９１７Ａ１ＥＤ４Ｄ８３ＡＡ３Ｄ６０７
Ｅ３ＥＢ５Ｃ８Ｂ１９７
６９７２３８５３７ＦＥ７Ａ０１９５Ｃ５Ｅ８３７３ＥＢ７４Ｄ

【００６３】

以下は、ｋ＝９、すなわちｖ＝５１２、ｍ＝２、すなわち２つの基数、g_1＝２とg_2＝３、およびｆ＝３が３（ｍｏｄ　４）に一致する３つの素因数を含む係数を示すＧＱ２鍵の第２集合である。

p_1＝０３８５２１０３Ｅ４０ＣＤ４Ｆ０６ＦＡ７ＢＡＡ９ＣＣ８Ｄ５ＢＣＥ９６Ｅ３９
８４５７０ＣＢ
p_2＝０６２ＡＣ９ＥＣ４２ＡＡ３Ｅ６８８ＤＣ２ＢＣ８７１Ｃ８３１５ＣＢ９３９０８
９Ｂ６１ＤＤ７
p_3＝０ＢＣＡＤＥＣ２１９Ｆ１ＤＦＢＢ８ＡＢ５ＦＥ８０８Ａ０ＦＦＣＢ５３４５８２
８４ＥＤ８Ｅ３
ｎ＝p_1．p_2．p_3＝ＦＦＦＦ５４０１ＥＣＤ９Ｅ５３７Ｆ１６７Ａ８０Ｃ０Ａ９１１１
９８６Ｆ７Ａ８ＥＢＡ４Ｄ
６６９８ＡＤ６８ＦＦ６７０ＤＥ５Ｄ９Ｄ７７ＤＦＦ００７１６ＤＣ７５３９Ｆ７ＣＢＢ

ＣＦ９６９Ｅ７３Ａ０Ｃ４９
７６１Ｂ２７６Ａ８Ｅ６Ｂ６９７７Ａ２１Ｄ５１６６９Ｄ０３９Ｆ１Ｄ７
$Q_{1,1}$＝０２６０ＢＣ７２４３Ｃ２２４５０Ｄ５６６Ｂ５Ｃ６ＥＦ７４ＡＡ２９Ｆ２Ｂ９２７ＡＦ６８Ｅ１
$Q_{2,1}$＝０３２６Ｃ１２ＦＣ７９９１ＥＣＤＣ９ＢＢ８Ｄ７Ｃ１Ｃ４５０１ＢＥ１ＢＡＥ９４８５３００Ｅ
$Q_{1,2}$＝０２Ｄ０Ｂ４ＣＣ９５Ａ２ＤＤ４３５Ｄ０Ｅ２２ＢＦＢＢ２９Ｃ５９４１８３０６Ｆ６ＣＤ００Ａ
$Q_{2,2}$＝Ｏ４５ＥＣＢ８８１３８７５８２Ｅ７Ｃ５５６８８７７８４Ｄ２６７１ＣＡ１１８Ｅ２２ＦＣＦ２
$Q_{1,3}$＝Ｂ０Ｃ２Ｂ１Ｆ８０８Ｄ２４Ｆ６３７６Ｅ３Ａ５３４ＥＢ５５５ＥＦ５４Ｅ６ＡＥＦ５９８２
$Q_{2,3}$＝０ＡＢ９Ｆ８１ＤＦ４６２Ｆ５８Ａ５２Ｄ９３７Ｅ６Ｄ８１Ｆ４８ＦＦＡ４Ａ８７Ａ９９３５ＡＢ
Q_{1}＝２７Ｆ７Ｂ９ＦＣ８２Ｃ１９ＡＣＡＥ４７Ｆ３ＦＥ９５６０Ｃ３５３６Ａ７Ｅ９０Ｆ８Ｃ３Ｃ５１Ｅ１３Ｃ
３５Ｆ３２ＦＤ８Ｃ６８２３ＤＦ７５３６８５ＤＤ６３５５５Ｄ２１４６ＦＣＤＢ９Ｂ２８ＤＡ３６７３２７ＤＤ６
ＥＤＤＡ０９２Ｄ０ＣＦ１０８Ｄ０ＡＢ７０８４０５ＤＡ４６
Q_{2}＝２３０Ｄ０Ｂ９５９５Ｅ５ＡＤ３８８Ｆ１Ｆ４４７Ａ６９９１８９０５ＥＢＦＢ０５９１０５８２Ｅ５ＢＡ６４
９Ｃ９４Ｂ０Ｂ２６６１Ｅ４９ＤＦ３Ｃ９Ｂ４２ＦＥＦ１Ｆ３７Ａ７９０９Ｂ１Ｃ２ＤＤ５４１１３ＡＣＦ８７Ｃ６
Ｆ１１Ｆ１９８７４ＤＥ７ＤＣ５Ｄ１ＤＦ２Ａ９２５２Ｄ

【００６４】

（動的認証）

動的認証機構は、コントローラとして知られているエンティティに対し、考えられる関連付けられたメッセージＭの真正性だけではなく、デモンストレータとして知られているエンティティの真正性も証明し、その結果、コントローラは、それが真にデモンストレータであり、場合によっては唯一のデモンストレータである旨、およびデモンストレータが真に同じメッセージＭを話している旨を確信できる。関連付けられたメッセージＭはオプションである。つまり、それは空である可能性がある。

【００６５】

動的認証機構は、４つの行動のシーケンスである。つまり、コミットメントという行為と、チャレンジという行為と、応答という行為と、チェックという行為とである。デモンストレータは、コミットメントおよび応答という行為を達成する。コントローラは、チャレンジおよび管理という行為を達成する。

【００６６】

デモンストレータの中では、デモンストレータの最も要注意なパラメータおよび機能、つまりコミットメントおよび応答の作成を隔離するために、証人を隔離することが可能である。証人はパラメータｋおよび秘密鍵ＧＱ２、つまりここに前記に参照された３つの描写の内の１つに従った係数ｎの因数分解を有する。つまり、・ｆ個の素因数およびｍ個の基数と、・ｍ．ｆ個の秘密構成要素と、ｆ個の素因数およびチャイニーズ剰余のｆ－１個のパラメータと、・ｍ個の秘密値および係数ｎとである。

【００６７】

証人は、例えば、・デモンストレータ全体を形成するＰＣに接続されているチップカード、または再び、・ＰＣ内で特別に保護されているプログラム、または再び、・スマートカード内で特別に保護されているプログラムなどの部分的な実施態様に対応することができる。そして、このようにして隔離された証人は、署名関係者内でここに以下に定義される証人に類似している。機構の実行のたびに、証人は、1以上のコミットメントＲを作成し

てから、チャレンジｄと同じくらい多くの応答Ｄを作成する。各集合｛Ｒ，ｄ，Ｄ｝は、ＧＱ２三つ組である。

【００６８】

証人を備えることとは別に、デモンストレータは、必要な場合、ハッシュ関数およびメッセージＭも有する。

【００６９】

コントローラは、係数ｎおよびパラメータｋとｍを有する。必要な場合には、それは同じハッシュ関数およびメッセージＭ’も有する。コントローラは、任意のチャレンジｄおよび任意の応答Ｄからコミットメント Ｒ’を再構築することができる。パラメータｋおよびｍがコントローラに知らせる。逆に表示できない場合には、g_1からg_mのｍ個の基数がｍ個の第１素因数である。各チャレンジｄは、基数ごとに１つ、d_1からd_mと参照されるｍ個の初歩チャレンジを有さなければならない。d_1からd_mと参照されるこの初歩チャレンジは、０から$2^{k-1}-1$（ｖ／２からｖ－１の値は使用されていない）という値を取りうる。典タイプ的には、各チャレンジは、ｍかけるｋ－１ビットで（ｍかけるｋビットではなく）で符号化される。例えば、ｋ＝６およびｍ＝３ならびに基数３，５、および７では、各チャレンジが２バイトで１５ビットを送信させる。ｋ＝９，ｍ＝２および基数２と３では、各チャレンジは２バイトで１６ビットを送信させる。（ｋ－１）．ｍ個の考えられるチャレンジも可能であるとき、値（ｋ－１）．ｍが、各ＧＱ２三つ組によって提供される機密保護を決定する。つまり、定義により、係数ｎの因数分解を知らない詐称者は、まさに$2^{(k-1)\cdot m}$に１回の成功の確率を有する。（ｋ－１）．ｍが１５から２０に等しいとき、動的認証に妥当に備えるためには１つの三つ組で十分である。任意の機密保護レベルを達成するには、三つ組を平行して作成することができる。また、連続して作成する、つまり機構の実行を繰り返すことも可能である。

【００７０】

１）コミットメントという行為は、以下の動作を備える。

証人がQ_1からQ_mのｍ個の秘密値、および係数ｎを有するとき、それは1以上のランダム値ｒ（０＜ｒ＜ｎ）をランダムにかつ秘密裏に引き出す。それからｋ回の連続二乗（ｍｏｄｎ）演算により、それは各ランダム値ｒをコミットメントＲに変換する。

$R \equiv r^v \pmod n$

ここに、ｋ＝６での鍵の第１集合の例がある。

ｒ＝Ｂ８ＡＤ４２６Ｃ１Ａ１０１６５Ｅ９４Ｂ８９４ＡＣ２４３７Ｃ１Ｂ１７９７ＥＦ５６２ＣＦＡ５３Ａ４ＡＦ８

４３１３１ＦＦ１Ｃ８９ＣＦＤＡ１３１２０７１９４７１０ＥＦ９Ｃ０１０Ｅ８Ｆ０９Ｃ６０Ｄ９８１５１２１９８１２６０

９１９９６７Ｃ３Ｅ２ＦＢ４Ｂ４５６６０８８Ｅ

Ｒ＝ＦＦＤＤ７３６Ｂ６６６Ｆ４１ＦＢ７７１７７６Ｄ９Ｄ５０ＤＢ７ＣＤＦ０３Ｆ３Ｄ９７６４７１Ｂ２５Ｃ５６

Ｄ３ＡＦ０７ＢＥ６９２ＣＢ１ＦＥ４ＥＥ７０ＦＡ７７０３２ＢＥＣＤ８４１１Ｂ８１３Ｂ４Ｃ２１２１０Ｃ６Ｂ０４

４９ＣＣ４２９２Ｅ５ＤＤ２ＢＤＢ００８２８ＡＦ１８

【００７１】

証人が、p_1からp_fまでｆ個の素因数、およびｍ．ｆ個の秘密構成要素Q_{ij}を有するとき、それはランダムに、および秘密裏に、ｆ個のランダム値の1以上の集合体を引き出す。各集合体は、素因数p_i（$0 < r_i < p_i$）ごとに１つのランダム値r_iを有する。それから、（ｍｏｄp_i）を二乗するｋ回の連続演算によって、それは各ランダム値r_iをコミットメントR_iの構成要素に変換する。

$R_i \equiv r_i^v \pmod{p_i}$

ここに、ｋ＝９での鍵の第２集合の例がある。

r_1＝Ｂ０４１８ＥＡＢＥＢＡＤＦ０５５３Ａ２８９０３Ｆ７４４７２ＣＤ４９ＤＤ８Ｃ８２Ｄ８６

R_1＝０２２Ｂ３６５Ｆ０ＢＥＡ８Ｅ１５７Ｅ９４Ａ９ＤＥＢ０５１２８２７ＦＦＤ５１４９８８０Ｆ１
r_2＝７５Ａ８ＤＡ８ＦＥ０Ｅ６０ＢＤ５５Ｄ２８Ａ２１８Ｅ３１３４７７３２３３９Ｆ１Ｄ６６７
R_2＝０５７^{E}４３Ａ２４２Ｃ４８５ＦＣ２０ＤＥＥＦ２９１Ｃ７７４ＣＦ１Ｂ３０Ｆ０１６３ＤＥＣ２
r_3＝０Ｄ７４Ｄ２ＢＤＡ５３０２ＣＦ８ＢＥ２Ｆ６Ｄ４０６２４９Ｄ１４８Ｃ６９６０Ａ７Ｄ２７
R_3＝０６^{E}１４Ｃ８ＦＣ４ＤＤ３１２ＢＡ３Ｂ４７５Ｆ１Ｆ４０ＣＦ０１ＡＣＥ２Ａ８８Ｄ５ＢＢ３Ｃ

【００７２】

ｆ個のコミットメント構成要素の集合体ごとに、証人は、チャイニーズ剰余の儀容に従ってコミットメントをセットアップする。ランダム値の集合体と同じくらい多くのコミットメントがある。

Ｒ＝チャイニーズ剰余（R_1，R_2，．．．，R_j）
Ｒ＝２８ＡＡ７Ｆ１２２５９ＢＦＢＡ８１３６８ＥＢ４９Ｃ９３ＥＥＡＢ３Ｆ３ＥＣ６ＢＦ７３Ｂ０ＥＢＤ７
Ｄ３ＦＣ８３９５ＣＦＡ１ＡＤ７ＦＣ０Ｆ９ＤＡＣ１６９Ａ４Ｆ６Ｆ１Ｃ４６ＦＢ４Ｃ３４５８Ｄ１Ｅ３７Ｃ９
９１２３Ｂ５６４４６Ｆ６Ｃ９２８７３６Ｂ１７Ｂ４ＢＡ４Ａ５２９

【００７３】

両方の場合で、デモンストレータは、コントローラに各コミットメントＲのすべてまたは一部、あるいは各コミットメントＲをハッシュ化することによって得られる少なくとも１つのハッシュコードＨおよび１つのメッセージＭを送信する。

【００７４】

２）チャレンジという行為は、ランダムに、それぞれが、ｍ個の初歩チャレンジd_1｜d_2｜…｜d_mから成り立つ1以上のチャレンジｄを引き出すことにある。各初歩チャレンジd_iは、０からｖ／２－１の値の１つを取る。

ｄ＝d_1｜d_2｜．．．｜d_m

ここに、ｋ＝６およびｍ＝３である鍵の第１集合の例がある。
d_1＝１０１１０＝２２＝’１６’；d_2＝００１１１＝７；d_3＝０００１０＝２
ｄ＝０｜｜d_1｜｜d_2｜｜d_3＝０１０１１０００１１１０００１０＝５８Ｅ２
ここに、ｋ＝９およびｍ＝２である鍵の第２集合の例がある。
ｄ＝d_1｜｜d_2＝５８Ｅ２、すなわち、小数点表記８８および２２６である
コントローラは、デモンストレータに各チャレンジｄを送信する。

【００７５】

３）応答という行為は、以下の演算を有する。
証人は、Q_1からQ_mのｍ個の秘密値および係数ｎを有するとき、それはコミットメントという行為の各ランダム値ｒおよび初歩チャレンジに従った秘密値を使用して、1以上の応答Ｄを計算する。

Ｘ≡Q_1^{d1}．Q_2^{d2}…Q_m^{dm}（ｍｏｄ ｎ）
Ｄ≡ｒ．Ｘ（ｍｏｄ ｎ）
ここに、鍵の第１集合の例がある。
Ｄ＝ＦＦ２５７４２２ＥＣＤ３Ｃ７Ａ０３７０６Ｂ９Ａ７Ｂ２８ＥＥ３ＦＣ３Ａ４Ｅ９７４ＡＥＤＣＤＦ３８６
５ＥＥＦ３８７６０Ｂ８５９ＦＤＢ５３３３Ｅ９０４ＢＢＤＤ３７Ｂ０９７Ａ９８９Ｆ６９０８５ＦＥ８ＥＦ６４８０
Ａ２Ｃ６Ａ２９０２７３４７９ＦＥＣ９１７１９９０Ａ１７

【００７６】

証人は、p_iからp_fのｆ個の素因数およびｍ．ｆ個の秘密構成要素$Q_{i,j}$を有するとき、それはコミットメントという行為のランダム値の各集合体を使用してｆ個の応答構成要素を計算する。応答構成要素の各集合体は、素因数ごとに１つの構成要素を備える

$X_i \equiv Q_1^{d1} . Q_2^{d2} \cdots Q_m^{dm}, _i \pmod{p_i}$

$D_i \equiv r_i . X_i \pmod{p_1}$

ここに鍵の第２集合の例がある。

$D_1 = r_1 . Q_{1.1}^{d1} . Q_{2.1}^{d2} \pmod{p_1} =$

Ｏ２６６０ＡＤＦ３Ｃ７３Ｂ６ＤＣ１５Ｅ１９６１５２３２２ＤＤＥ８ＥＢ５Ｂ３５７７５Ｅ３８

$D_2 = r_2 . Q_{1.2}^{d1} . Q_{2.2}^{d2} \pmod{p_2} =$

０４Ｃ１５０２８Ｅ５ＦＤ１１７５７２４３７６Ｃ１１ＢＥ７７０５２２０５Ｆ７Ｃ６２ＡＥ３Ｂ

$D_3 = r_3 . Q_{1.3}^{d1} . Q_{2.3}^{d2} \pmod{p_3} =$

０９０３Ｄ２０Ｄ０Ｃ３０６Ｃ８ＥＤＡ９Ｄ８ＦＢ５Ｂ３ＢＥＢ５５Ｅ０６１ＡＢ３９ＣＣＦ５２

【００７７】

応答構成要素の集合体ごとに、証人は、チャイニーズ剰余技法に従った応答を作成する。チャレンジと同じくらい多くの応答がある。

$D = チャイニーズ剰余 (D_1, D_2, \ldots, D_f)$

Ｄ＝８５Ｃ３Ｂ００２９６４２６Ｅ９７８９７Ｆ７３Ｃ７ＤＣ６３４１ＦＢ８ＦＦＥ６Ｅ８７９ＡＥ１２ＥＦ１Ｆ３６

４ＣＢＢ５５ＢＣ４４ＤＥＣ４３７２０８ＣＦ５３０Ｆ８４０２ＢＤ９Ｃ５１１Ｆ５ＦＢ３Ｂ３Ａ３０９２５７Ａ００

１９５Ａ７３０５Ｃ６ＦＦ３３２３Ｆ７２ＤＣ１ＡＢ

両方の場合で、デモンストレータは各応答Ｄをコントローラに送信する。

【００７８】

４）チェック行為は、各三つ組｛Ｒ，ｄ，Ｄ｝が、非零値に関して以下のタイプの等式を検証することを確認することにあるか、

【数７】

$$R \cdot \prod_{i=1}^{m} G_i^{d_i} \equiv D^{2^t}$$ 、あるいはまた、 $$R \equiv D^{2^t} \cdot \prod_{i=1}^{m} G_i^{d_i}$$

または、さもなければ、各コミットメントをセットアップすることにある。何もゼロであってはならない。

【数８】

$$R' \equiv D^{2^t} / \prod_{i=1}^{m} G_i^{d_i}$$ 、あるいはまた、 $$R' \equiv D^{2^t} \cdot \prod_{i=1}^{m} G_i^{d_i}$$

【００７９】

必要な場合、コントローラは、それぞれの再確立されたコミットメントＲ’およびメッセージＭ’をハッシュ化する際にハッシュコードＨ’を計算する。動的認証は、コントローラが、このようにして、それがコミットメントの最初の行為の最後に受信したもの、つまり各コミットメントＲのすべてまたは一部、あるいはさもなければハッシュコードＨを検索するときに成功する。

【００８０】

例えば、初歩動作のシーケンスが、応答Ｄをコミットメント Ｒ’に変換する。シーケンスは、ｋ－１回の除算によって、あるいは基数による乗算（ｍｏｄ　ｎ）によって分離されるｋ個の平方（ｍｏｄ　ｎ）を有する。ｉ番目の平方とｉ＋１番目の平方の間で実行され

るｉ番目の除算または乗算の場合には、初歩チャレンジd_iのｉ番目のビットはg_iを使用する必要があることを示し、初歩チャレンジd_2のｉ番目のビットは、g_2を使用するのが必要かどうかを示し、初歩チャレンジd_mのｉ番目のビットまで、g_mを使用することが必要であるかどうかを示す。
ここに、鍵の第１集合の例がある。
【表１】

$D^2 \pmod n$ = FD12E8E1F1370AEC9C7BA2E05C80AD2B692D341D46F3
2B93948715491F0EB091B7606CA1E744E0688367D7BB998F7B73D5F7
FDA95D5BD6347DC8B978CA217733

3 . $D^2 \pmod n$ = F739B708911166DFE715800D8A9D78FC3F332FF622D
3EAB8E7977C68AD44962BEE4DAE3C0345D1CB34526D3B67EBE8BF
987041B4852890D83FC6B48D3EF6A9DF

【表２】

$3^{1} \cdot D^{4} \pmod{n}$ = 682A7AF280C49FE230BEE354BF6FFB30B7519E3C8
92DD07E5A781225BBD33920E5ADABBCD7284966D71141EAA17AF
8826635790743EA7D9A15A33ACC7491D4A7

$3^{4} \cdot D^{8} \pmod{n}$ = BE9D828989A2C184E34BA8FE0F384811642B7B548F
870699E7869F8ED851FC3DB3830B2400C516511A0C28AFDD210EC3
939E69D413F0BABC6DEC441974B1A291

$3^{3} \cdot 5 \cdot D^{8} \pmod{n}$ = 2B40122E225CD858B26D27B768632923F2BBE5
DB15CA9EFA77EFA667E554A02AD1A1E4F6B59BD9E1AE4A537D
4AC1E89C2235C363830EBF4DB42CEA3DA98CFE00

$3^{10} \cdot 5^{2} \cdot D^{16} \pmod{n}$ = BDD3B34C90ABBC870C604E27E7F2E9DB2D383
68EA46C931C66F6C7509B118E3C162811A98169C30D4DEF768397DD
B8F6526B6714218DEB627E11FACA4B9DB268

$3^{11} \cdot 5^{3} \cdot 7 \cdot D^{16} \pmod{n}$ = DBFA7F40D338DE4FBA73D42DBF427BBF195
C13D02AB0FA5F8C8DDB5025E342823 11CEF80BACDCE5D0C433444
A2AF2B15318C36FE2AE02F3C8CB25637C9AD712F

$3^{22} \cdot 5^{6} \cdot 7^{2} \cdot D^{32} \pmod{n}$ = C60CA9C4A11F8AA89D9242CE717E3DC6C1
A95D5D09A2278F8FEE1DFD94EE84D09D000EA8633B53C4A0E7F0A
EECB70509667A3CB052029C94EDF27611FAE286A7

$3^{22} \cdot 5^{7} \cdot 7^{2} \cdot D^{32} \pmod{n}$ = DE40CB6B41C01E722E4F312AE7205F18CDD
0303EA52261CB0EA9F0C7E0CD5EC53D42E5CB645B6BB1A3B00C77
886F4AC5222F9C863DACA440CF5F1A8E374807AC

$3^{44} \cdot 5^{14} \cdot 7^{4} \cdot D^{64} \pmod{n}$, namely $3^{2C} \cdot 5^{E} \cdot 7^{4} \cdot D^{40}$ with the exponents in hexadecimal notation = FFDD736B666F41FB771776D9D50DB7CDF03F3D9
76471B25C56D3AF07BE692CB1FE4EE70FA77032BECD8411B813B4C
21210C6B0449CC4292E5DD2BDB00828AF18

We find the commitment R. The authentication is successful.

Here is an example for the second set of keys.

$D^{2} \pmod{n}$ = C66E585D8F132F7067617BC6D00BA699ABD74FB9D13E
24E6A6692CC8D2FC7B57352D66D34F5273C13F20E3FAA228D70AEC
693F8395ACEF9206B172A8A2C2CCBB

【表３】

$3 \cdot D^{2} \pmod{n}$ = 534C6114D385C3E15355233C5B00D09C2490D1B8D8E
D3D59213CB83EAD41C309A187519E5F501C4A45C37EB2FF38FBF20
1D6D138F3999FC1D06A2B2647D48283

$3^{2} \cdot D^{4} \pmod{n}$ = A9DC8DEA867697E76B4C18527DFFC49F4658473D03
4EC1DDE0EB21F6F65978BE477C4231AC9B1EBD93D5D49422408E47
15919023B16BC3C6C46A92BBD326AADF

$2 \cdot 3^{3} \cdot D^{4} \pmod{n}$ = FB2D57796039DFC4AF9199CAD44B66F257A1FF
3F2BA4C12B0A8496A0148B4DFBAFE838E0B5A7D9FB4394379D72A
107E45C51FCDB7462D03A35002D29823A2BB5

$2^{3} \cdot 3^{6} \cdot D^{8} \pmod{n}$ = 4C210F96FF6C77541910623B1E49533206DFB9E91
6521F305F12C5DB054D4E1BF3A37FA293854DF02B49283B6DE5E5D
82ACB23DAF1A0D5A721A1890D03A00BD8

$2^{2} \cdot 3^{7} \cdot D^{8} \pmod{n}$ = E4632EC4FE4565FC4B3126B15ADBF996149F2D
BB42F65D911D3851910FE7EA53DAEA7EE7BA8FE9D081DB78B249
B1B18880616B90D4E280F564E49B270AE02388

$2^{4} \cdot 3^{14} \cdot D^{16} \pmod{n}$ = ED3DDC716AE3D1EA74C5AF935DE814BCC
2C78B12A6BB29FA542F9981C5D954F53D153B9F0198BA82690EF
665C17C399607DEA54E218C2C01A890D422EDA16FA3

$2^{5} \cdot 3^{14} \cdot D^{16} \pmod{n}$ = DA7C64E0E8EDBE9CF823B71AB13F17E1161487
6B000FBB473F5FCBF5A5D8D26C7B2A05D03BDDD588164E562D0F5
7AE94AE0AD3F35C61C0892F4C91DC0B08ED6F

$2^{10} \cdot 3^{28} \cdot D^{32} \pmod{n}$ = 6ED6AFC5A87D2DD117B0D89072C99FB9DC9
5D558F65B6A1967E6207D4ADBBA32001D3828A35069B256A07C3D
722F17DA30088E6E739FBC419FD7282D16CD6542

$2^{11} \cdot 3^{28} \cdot D^{32} \pmod{n}$ = DDAD5F8B50FA5BA22F61B120E5933F73B92
BAAB1ECB6D432CFCC40FA95B774644003A705146A0D364AD40F8
7AE45E2FB460111CDCE73F78833FAE505A2D9ACA84

$2^{22} \cdot 3^{56} \cdot D^{64} \pmod{n}$ = A466D0CB17614EFD961000BD9EABF4F021
36F8307101882BC1764DBAACB715EFBF5D8309AE001EB5DEDA
8F000E44B3D4578E5CA55797FD4BD1F8E919BE787BD0

$2^{44} \cdot 3^{112} \cdot D^{128} \pmod{n}$ = 925B0EDF5047EFEC5AFABDC03A830919761

【表４】

B8FBDD2BF934E2A8A31E29B976274D513007EF1269E4638B4F65F
8FDEC740778BDC178AD7AF2968689B930D5A2359
$2^{44} \cdot 3^{113} \cdot D^{128} \pmod{n}$ = B711D89C03FDEA8D1F889134A4F809B3F2D
8207F2AD8213D169F2E99ECEC4FE08038900F0C203B55EE4F4C803
BFB912A04F11D9DB9D076021764BC4F57D47834
$2^{88} \cdot 3^{226} \cdot D^{256} \pmod{n}$ = 41A83F119FFE4A2F4AC7E5597A5D0BEB4D4C
08D19E597FD034FE720235894363A19D6BC5AF323D24B1B7FCFD8D
FCC628021B4648D7EF757A3E461EF0CFF0EA13
$2^{176} \cdot 3^{452} \cdot D^{512} \pmod{n}$ that is $4^{88} \cdot 9^{226} \cdot D^{512} \pmod{n}$ = 28AA7F12259BFBA8
1368EB49C93EEAB3F3EC6BF73B0EBD7D3FC8395CFA1AD7FC0F9D
AC169A4F6F1C46FB4C3458D1E37C99123B56446F6C928736B17B4BA
4A529

私達は、コミットメントＲを発見する。認証は無事に終了した。

【００８１】

（デジタル署名）

デジタル署名機構によって、署名関係者と呼ばれるエンティティは、署名済みのメッセージを作成し、コントローラと呼ばれるエンティティは署名済みのメッセージを確認することができるようになる。メッセージＭは、任意のバイナリシーケンスである。それは空である場合がある。メッセージＭは、それにシグナチャ付録を追加することによって署名される。このシグナチャ付録は、対応する応答だけではなく、1以上のコミットメントおよび／またはチャレンジも備える。

【００８２】

コントローラは同じハッシュ関数、パラメータｋとｍ、および係数ｎを有する。パラメータｋおよびｍは、コントローラに対し情報を提供する。第１に、d_1からd_mの各初歩チャレンジは、０から$2_{k-1}-1$（ｖ／２からｖ－１という値は使用されない）の値を取らなければならない。第２に、各チャレンジｄは、d_1からd_mと参照されるｍ個の初歩チャレンジ、つまり基数と同じくらい多くの初歩チャレンジを含まなければならない。さらに、逆に表示することができないと、g_1からg_mのｍ個の基数はｍ個の第１素数である。（ｋ－１）．ｍが１５から２０に等しいので、平行して作成された４個の三つ組ＧＱ２で署名することが可能である。（ｋ－１）．ｍが６０以上に等しい場合、単一の三つ組ＧＱ２で署名することが可能である。例えばｋ＝９およびｍ＝８の場合には、単一の三つ組ＧＱ２で十分である。各チャレンジは８バイトであり、基数は２、３、５、７、１１、１３、１７および１９である。

【００８３】

署名動作は、３つの行為、つまりコミットメントという行為と、チャレンジという行為と、応答という行為とのシーケンスである。それぞれの行為から、コミットメントＲ（≠０）、d_1，d_2，．．．，d_mと参照されるｍ個の初歩チャレンジから成り立つチャレンジｄ、および応答Ｄ（≠０）をそれぞれ含む1以上のＧＱ２三つ組が生じる。

【００８４】

署名関係者は、ハッシュ関数、パラメータｋおよびＧＱ２秘密鍵、つまりここに前記に参照された３つの描写の内の１つに従った係数ｎの因数分解を有する。署名関係者内で、デモンストレータにとって最も要注意である関数およびパラメータを隔離するために、コミットメントおよび応答という行為を実行する証人を隔離することが可能である。コミットメントおよび応答を計算するために、証人はパラメータｋおよびＧＱ２秘密鍵、つまりこ

こに前記に参照された３つの描写の内の１つに従った係数ｎの因数分解を有する。このようにして隔離された証人は、デモンストレータ内で定義された証人に類似する。それは、ある特定の実施態様、例えば、・署名関係者全体を形成するＰＣに接続されているチップカード、または再び、・ＰＣ内で特に保護されているプログラム、または再び、・チップカード内で特に保護されているプログラムに対応することができる。

【００８５】

１）コミットメントという行為は、以下の演算を含む。

証人がQ_1からQ_mというｍ個の秘密値、および係数ｎを有するとき、それはランダムにおよび秘密裏に1以上のランダム値ｒ（０＜ｒ＜ｎ）を引き出す。それから、ｋ回の無事終了した二乗（ｍｏｄ　ｎ）演算によって、それは各ランダム値ｒをコミットメントＲに変換する。

$R \equiv r^v$（ｍｏｄ　ｎ）

【００８６】

証人がp_1からp_fのｆ個の素因数およびｍ．ｆ個の秘密構成要素Q_{ij}を有するとき、それは、秘密裏にかつランダムにｆ個ののランダム値の1以上の集合体を引き出す。各集合体は、素因数p_i（$0 < r_i < p_i$）ごとに１つのランダム値を有する。それから、ｋ回の無事終了した二乗（ｍｏｄp_i）演算によって、それは各ランダム値r_iをコミットメントR_iの構成要素に変換する。

$R_i \equiv r_i^v$（ｍｏｄ　p_i）

【００８７】

ｆ個のコミットメント構成要素ごとに、証人は、チャイニーズ剰余技法にしたがってコミットメントをセットアップする。ランダム値の集合体と同じくらい多くのコミットメントがある。

Ｒ＝チャイニーズ剰余（R_1，R_2，．．．，R_f）

【００８８】

２）チャレンジという行為は、すべてのコミットメントＲおよび署名関係者が、それぞれがｍ個の初歩チャレンジを含む1以上のチャレンジを形成するハッシュコードを得るためにＭと署名されるメッセージをハッシュ化することにある。各初歩チャレンジは、例えば、ｋ＝９およびｍ＝８で０からｖ／２－１から任意の値を取る。各チャレンジは８バイトを有する。コミットメントと同じくらい多くのチャレンジがある。

ｄ＝$d_1/d_2/.../d_m$，結果ハッシュ（Ｍ，Ｒ）から抽出

【００８９】

３）応答という行為は、以下の動作を含む。

証人は、Q_1からQ_mのｍ個の秘密値および係数ｎを有するとき、それは、コミットメントという行為の各ランダム値ｒおよび初歩チャレンジに従った秘密値を使用して、1以上の応答Ｄを計算する。

$X./\equiv Q_1^{d1}.\ Q_2^{d2} \cdots Q_m^{dm}$（ｍｏｄ　ｎ）

$D/\equiv r./X./$（ｍｏｄ　ｎ）

【００９０】

証人は、p_1からp_fのｆ個の素因数、およびｍ．ｆ個の秘密構成要素Q_{ij}を有するとき、それはコミットメントという行為のランダム値の書く集合体を使用する際にｆ個の応答構成要素を計算する。応答構成要素の各集合体は、素因数ごとに１つの構成要素を含む。

$X_i \equiv Q_1^{d1,\ i}.\ Q_2^{d2,\ i} \cdots Q_m^{dm,\ i}$（ｍｏｄ　p_i）

$D_i \equiv r_i.\ X_i$（ｍｏｄ　p_i）

【００９１】

応答構成要素の集合体ごとに、証人は、チャイニーズ剰余技法に従って応答をセットアップする。チャレンジと同じくらい多くの応答がある。

Ｄ＝チャイニーズ剰余（D_1，D_2，．．．，D_f）

【００９２】

署名関係者はそれに以下を含むシグナチャ付録を追加する際に、メッセージＭに署名する

。
各ＧＱ２三つ組、つまり各コミットメントＲ、各チャレンジｄおよび各応答Ｄと、
または、さもなければ、各コミットメントＲおよび各対応する応答Ｄか、
または、さもなければ、各チャレンジｄおよび各対応する応答Ｄ
【００９３】
検証動作の実行は、シグナチャ付録の内容に依存する。３つの考えられる場合がある。
【００９４】
付録が1以上の三つ組を含む場合には、チェック動作は、年代順配列が重要ではない２つの独立したプロセスを有する。コントローラは、以下の２つの条件が満たされる場合および満たされる場合にだけ署名済みのメッセージを受け入れる。
【００９５】
第１に、各三つ組は、一貫（以下のタイプに関する適切な関係性が検証されなければならない）し、許容（非零値で比較が実行されなければならない）できなければならない。
【数９】

$$R\cdot\prod_{i=1}^{m}G_i^{d_i}\equiv D^{2^t}\pmod{n}$$、あるいはまた、$$R\equiv D^{2^t}\cdot\prod_{i=1}^{m}G_i^{d_i}\pmod{n}$$

【００９６】
例えば、応答Ｄは、初歩動作のシーケンスによって変換される。つまり、基数によるｋ－１回の乗算または除算演算によって分離されるｋ個の平方済み（ｍｏｄ　ｎ）。ｉ番目の平方とｉ＋１番目の平方の間で実行されるｉ番目の乗算または除算の場合には、初歩チャレンジd_1のｉ番目のビットは、g_1を使用することが必要であるかどうかを示し、初歩チャレンジd_2のｉ番目のビットは、g_2を使用するのが必要かどうかを示し、初歩チャレンジd_mのｉ番目のビットまで、g_mを使用することが必要であるかどうかを示す。このようにして、シグナチャ付録に存在する各コミットメントＲを検索することが必要である。
【００９７】
さらに、1以上の三つ組は、メッセージＭにリンクされなければならない。すべてのコミットメントＲおよびメッセージＭをハッシュ化することによって、各チャレンジｄが回復されなければならないハッシュコードが得られる。
$d=d_1/d_2/\ldots/d_m$,結果ハッシュ（Ｍ，Ｒ）から抽出されるものと同一
【００９８】
付録にチャレンジがない場合には、チェック動作が、すべてのコミットメントＲおよびメッセージＭをハッシュ化することによって、1以上のチャレンジｄ’の再構築で開始する。
$D'=d'_1/d'_2/\ldots/d'_m$，結果ハッシュ（Ｍ，Ｒ）から抽出
【００９９】
そして、コントローラは、各三つ組が一貫（以下のタイプの適切な関係性が検証される）し、許容（非零値で比較が実行される）できる場合に、および場合にだけ署名済みメッセージを受け入れる。
【数１０】

$$R\cdot\prod_{i=1}^{m}G_i^{d_i}\equiv D^{2^t}\pmod{n}$$または、さもなければ$$R\equiv D^{2^t}\cdot\prod_{i=1}^{m}G_i^{d_i}\pmod{n}$$、

【０１００】
付録がコミットメントを備えない場合には、チェック動作は、以下の２つの公式の一方、つまり適切である公式に従って、1以上のコミットメントＲ’を再構築することによって開始する。確立し直されたコミットメントはゼロであってはならない。
【数１１】

$R' \equiv D^{2^k} / \prod_{i=1}^{m} G_i^{d_i} \pmod{n}$、あるいはまた、$R' \equiv D^{2^k} \cdot \prod_{i=1}^{m} G_i^{d_i} \pmod{n}$

【０１０１】
そして、コントローラは、各チャレンジｄを再構成するために、すべてのコミットメントＲ’およびメッセージＭをハッシュ化しなければならない。
$d = d_1 / d_2 / \ldots / d_m$，結果ハッシュ（Ｍ，Ｒ）から抽出されたものと同一
【０１０２】
コントローラは、各再構築されたチャレンジが付録内の対応するチャレンジに同一である場合および場合にだけ署名済みのメッセージを受け入れる。
【０１０３】
本出願においては、それぞれ、エンティティの真正性、および／またはメッセージの完全性および／または真正性を証明するように設計される本発明に従って方法、システムおよびデバイスを実行するために使用される秘密値と公開値ＱとＧの組がある。
【０１０４】
その発明者がLouis Guillouおよび Jean-Jacques Quisquaterであるフランステレコム、ＴＤＦ、およびMath RiZK社によって本出願と同日に提出された係属出願において、ＧＱ２鍵の集合、つまり指数ｖが2^kに等しいときに、それぞれ係数ｎおよび公開値と秘密値ＧとＱの組を生成するための方法が説明されている。これらを引用することにより本明細書の一部をなすものとする。

フロントページの続き

(31)優先権主張番号 99/12465
(32)優先日 平成11年10月1日(1999.10.1)
(33)優先権主張国 フランス(FR)
(31)優先権主張番号 99/12467
(32)優先日 平成11年10月1日(1999.10.1)
(33)優先権主張国 フランス(FR)
(31)優先権主張番号 99/12468
(32)優先日 平成11年10月1日(1999.10.1)
(33)優先権主張国 フランス(FR)

(72)発明者 キスクワテル, ジャン‐ジャック
ベルギー国、１６４０ ロード・サン・ジェネス、アヴニュ・デ・カナール ３

審査官 中里 裕正

(56)参考文献 欧州特許出願公開第００５１８３６５（ＥＰ，Ａ１）
特開平０５－０２０３４４（ＪＰ，Ａ）
Victor Shoup, On the Security of a Practical Identification Scheme, Lecture Notes in Computer Science, １９９６年, Vol.1070, p.344-353

(58)調査した分野(Int.Cl., ＤＢ名)
H04L 9/32
JSTPlus/JMEDPlus/JST7580(JDreamII)