(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第4800624号
(P4800624)
(45)発行日　平成23年10月26日(2011.10.26)　(24)登録日　平成23年8月12日(2011.8.12)

(51)Int.Cl.　F I
H04L 9/08 (2006.01)　H04L 9/00 601A
H04L 9/00 601C
H04L 9/00 601F

請求項の数 28　(全 18 頁)

(21)出願番号　特願2004-566624 (P2004-566624)
(86)(22)出願日　平成15年12月30日 (2003.12.30)
(65)公表番号　特表2006-513641 (P2006-513641A)
(43)公表日　平成18年4月20日 (2006.4.20)
(86)国際出願番号　PCT/US2003/041538
(87)国際公開番号　WO2004/064312
(87)国際公開日　平成16年7月29日 (2004.7.29)
審査請求日　平成18年12月1日 (2006.12.1)
(31)優先権主張番号　60/438,617
(32)優先日　平成15年1月7日 (2003.1.7)
(33)優先権主張国　米国(US)

(73)特許権者　595020643
クゥアルコム・インコーポレイテッド
ＱＵＡＬＣＯＭＭ　ＩＮＣＯＲＰＯＲＡＴＥＤ
アメリカ合衆国、カリフォルニア州　９２１２１－１７１４、サン・ディエゴ、モアハウス・ドライブ　５７７５
(74)代理人　100091351
弁理士　河野　哲
(74)代理人　100088683
弁理士　中村　誠
(74)代理人　100108855
弁理士　蔵田　昌俊
(74)代理人　100075672
弁理士　峰　隆司

最終頁に続く

(54)【発明の名称】暗号鍵を入れ替えるためのシステム、装置及び方法

(57)【特許請求の範囲】
【請求項１】
公開暗号システムにおける利用者機器の認証のための方法であって、
前記利用者機器が、第１のプライベート鍵と対応する第１の公開鍵とを創出すること、
前記利用者機器が、第１のプライベート鍵に関係付けられた第２のプライベート鍵を創出すること及び前記第２のプライベート鍵に対応する第２の公開鍵を創出すること、
前記利用者機器が前記第１のプライベート鍵を保持し、前記利用者機器から前記第２のプライベート鍵をアウトプットすること、前記第２のプライベート鍵をアウトプットすることは、前記第１のプライベート鍵が使用できないときに前記第２のプライベート鍵が再創出および使用可能なように、前記利用者機器から複数の異なる構成要素へ、前記第２のプライベート鍵の複数の配分を送信すること、を含み、
前記第１の公開鍵と前記第２の公開鍵とを検証者機器へアウトプットすること、
前記利用者機器が、認証のために前記第１のプライベート鍵を使用すること、
を具備する方法。
【請求項２】
前記第２のプライベート鍵の複数の配分を送信することは、
前記利用者機器が、前記第２のプライベート鍵の少なくとも２個の配分を創出すること、及び
各配分を前記利用者機器から異なる構成要素へ一回アウトプットすること、

を具備する、請求項1に記載の方法。
【請求項３】
前記利用者機器と取り替えられた利用者機器とのうちの１つが、前記複数の配分のうちの少なくともいつかを用いて、前記第２のプライベート鍵を再創出すること、及び
前記利用者機器または前記取り替えられた利用者機器の認証のために、前記第２のプライベート鍵を使用すること、
を更に具備する請求項１記載の方法。
【請求項４】
前記第２のプライベート鍵が認証のために使用される時に前記第１のプライベート鍵を使用不能にすること、
を更に具備する請求項３に記載の方法。
【請求項５】
前記第２のプライベート鍵に関係付けられた第３のプライベート鍵を創出すること及び前記第３のプライベート鍵に対応する第３の公開鍵を創出すること、及び
前記第３の公開鍵を前記検証者機器へアウトプットすること、
を更に具備する請求項３に記載の方法。
【請求項６】
前記第３のプライベート鍵をそれが再創出されることが可能であるように複数の配分として一回アウトプットすること、
前記複数の配分のうちの少なくともいくつかを用いて、前記第３のプライベート鍵を再創出すること、及び
前記第３のプライベート鍵を認証のために使用すること、
を更に具備する請求項５に記載の方法。
【請求項７】
認証のための前記第２のプライベート鍵の使用を不能にすること、
前記複数の配分のうちの少なくともいくつかを用いて、前記第３のプライベート鍵を再創出すること、
前記第３のプライベート鍵を認証のために使用すること、
を更に具備する請求項５に記載の方法。
【請求項８】
前記第２のプライベート鍵に関係付けられた第３のプライベート鍵を創出すること及び前記第３のプライベート鍵に対応する第３の公開鍵を創出すること、
前記第３のプライベート鍵に関係付けられた第４のプライベート鍵を創出すること及び前記第４のプライベート鍵に対応する第４の公開鍵を創出すること、
前記第４のプライベート鍵をそれが再創出されることが可能であるように一回アウトプットすること、及び
前記第３及び第４の公開鍵をアウトプットすること、
を更に具備する請求項３に記載の方法。
【請求項９】
認証のための前記第２のプライベート鍵の使用を不能にすること、及び
前記第３のプライベート鍵を認証のために使用すること、
を更に具備する請求項８に記載の方法。
【請求項１０】
前記第４のプライベート鍵を再創出すること、及び
前記第４のプライベートを認証のために使用すること、
を更に具備する請求項９に記載の方法。
【請求項１１】
公開暗号システムにおける認証のための利用者機器であって、
第１のプライベート鍵と対応する第１の公開鍵を創出する手段、
前記第１のプライベート鍵に関係付けられた第２のプライベート鍵を創出し、及び、前

記第２のプライベート鍵に対応する第２の公開鍵を創出する手段、
前記利用者機器で前記第１のプライベート鍵を保持し、前記利用者機器から前記第２のプライベート鍵をアウトプットする手段、前記第２のプライベート鍵をアウトプットすることは、前記第１のプライベート鍵が使用できないときに前記第２のプライベート鍵が再創出および使用可能なように、前記利用者機器から複数の異なる構成要素へ、前記第２のプライベート鍵の複数の配分を送信することを含み、
前記第１の公開鍵と前記第２の公開鍵とを検証者機器へアウトプットする手段、
前記第１のプライベート鍵を前記利用者機器の認証のために使用する手段、
を具備する利用者機器。
【請求項１２】
前記第２のプライベート鍵をアウトプットする手段は、
前記第２のプライベート鍵の少なくとも２個の配分を創出する手段、及び
各配分を異なる構成要素へ一回アウトプットする手段、
を具備する請求項１１に記載の利用者機器。
【請求項１３】
前記第２のプライベート鍵を再創出する手段、及び
前記第２のプライベート鍵を認証のために使用する手段、
を更に具備する請求項１１に記載の利用者機器。
【請求項１４】
前記第２のプライベート鍵に関係付けられた第３のプライベート鍵を創出し、及び、前記第３のプライベート鍵に対応する第３の公開鍵を創出する手段、及び
前記第３の公開鍵を前記検証者機器へアウトプットする手段、
を更に具備する請求項１３に記載の利用者機器。
【請求項１５】
前記第２のプライベート鍵に関係付けられた第３のプライベート鍵を創出し、及び、前記第３のプライベート鍵に対応する第３の公開鍵を創出する手段、
前記第３のプライベート鍵に関係付けられた第４のプライベート鍵を創出し、及び、前記第４のプライベート鍵に対応する第４の公開鍵を創出する手段、
前記第４のプライベート鍵をそれが再創出されることが可能であるように一回アウトプットする手段、及び
前記第３及び第４の公開鍵を前記検証者機器へアウトプットする手段、
を更に具備する請求項１３に記載の利用者機器。
【請求項１６】
機械に実行されると、該機械を、公開暗号システムにおいて認証を行うための利用者機器として動作させる複数のコードセグメントを備える機械可読記憶媒体であって、前記機械可読記憶媒体は、
第１のプライベート鍵と対応する第１の公開鍵とを創出するためのコードセグメントのセット、
前記第１のプライベート鍵に関係付けられた第２のプライベート鍵を創出し、および、前記第２のプライベート鍵に対応する第２の公開鍵を創出するためのコードセグメントのセット、
前記利用者機器で前記第１のプライベート鍵を保持し、前記利用者機器から前記第２のプライベート鍵をアウトプットするためのコードセグメントのセット、前記第２のプライベート鍵をアウトプットすることは、前記第１のプライベート鍵が使用できないときに前記第２のプライベート鍵が再創出および使用可能なように、前記利用者機器から複数の異なる構成要素へ、前記第２のプライベート鍵の複数の配分を送信すること、を含み、
前記第１の公開鍵と前記第２の公開鍵とを検証者機器へアウトプットするためのコードセグメントのセット、
前記第１のプライベート鍵を前記利用者機器の認証のために使用するためのコードセグメントのセット、

を具備する機械可読記憶媒体。
【請求項１７】
前記第２のプライベート鍵を送信するためのコードセグメントのセットは、
前記第２のプライベート鍵の少なくとも２個の配分を創出するためのコードセグメントのセット、及び
各配分を異なる構成要素へ一回アウトプットするためのコードセグメントのセット、
を具備する請求項１６に記載の記憶媒体。
【請求項１８】
前記複数の配分のうちの少なくともいくつかを用いて、前記第２のプライベート鍵を再創出するためのコードセグメントのセット、及び
第２のプライベート鍵を前記利用者機器の認証のために使用するためのコードセグメントのセット、
を更に具備する請求項１６に記載の記憶媒体。
【請求項１９】
前記第２のプライベート鍵を認証のために使用することにより前記第１のプライベート鍵を使用不能にするためのコードセグメントのセット、
を更に具備する請求項１８に記載の記憶媒体。
【請求項２０】
公開暗号システムで動作する利用者機器の認証のための方法であって、
前記利用者機器が、第１のプライベート鍵及び対応する公開鍵を、関連するシステムパラメータを用いて創出すること、
前記利用者機器が、前記システムパラメータと前記公開鍵とを検証者機器へアウトプットすること、
前記利用者機器が、新しいプライベート鍵を創出すること、前記新しいプライベート鍵は前記第１のプライベート鍵と前記システムパラメータとを用いて創出される、
前記利用者機器が、認証のために前記新しいプライベート鍵を使用すること、
を具備する方法。
【請求項２１】
公開及びプライベート鍵の生成を示すカウンタ値を創出すること、及び
前記公開鍵をアウトプットする時に前記カウンタ値をアウトプットすること、
を更に具備する請求項２０記載の方法。
【請求項２２】
前記カウンタ値に基づき前記第１のプライベート鍵と前記システムパラメータとを利用して前記新しいプライベート鍵を創出すること、
を更に具備する請求項２１に記載の方法。
【請求項２３】
公開暗号システムにおける認証に適応した利用者機器装置であって、
前記利用者機器において、第１のプライベート鍵及び対応する公開鍵を、関連するシステムパラメータを用いて創出する手段、
前記利用者機器から、前記システムパラメータと前記公開鍵とを検証者機器へアウトプットする手段、
前記利用者機器において、新しいプライベート鍵を創出する手段、前記新しいプライベート鍵は前記第１のプライベート鍵と前記システムパラメータとを用いて創出される、
前記利用者機器の認証のために前記新しいプライベート鍵を使用する手段、
を具備する装置。
【請求項２４】
公開及びプライベート鍵の生成を示すカウンタ値を創出する手段、及び、
前記公開鍵をアウトプットする時に前記カウンタ値をアウトプットする手段、
を更に具備する請求項２３記載の装置。
【請求項２５】

前記カウンタ値に基づき前記第１のプライベート鍵と前記システムパラメータとを利用して前記新しいプライベート鍵を創出する手段、
を更に具備する請求項２４に記載の装置。
【請求項２６】
機械に実行されると、該機械を、公開暗号システムにおいて認証を行う利用者機器として動作させる複数のコードセグメントを備える機械可読記憶媒体であって、前記機械可読記憶媒体は、
第１のプライベート鍵及び対応する公開鍵を、関連するシステムパラメータを用いて創出するためのコードセグメントのセット、
前記システムパラメータと前記公開鍵とをアウトプットするためのコードセグメントのセット、
前記第１のプライベート鍵と前記システムパラメータとを用いて、新しいプライベート鍵を送出するためのコードセグメントのセット、
前記新しいプライベート鍵を前記利用者機器の認証のために使用するためのコードセグメントのセット、
を具備する記憶媒体。
【請求項２７】
公開及びプライベート鍵の生成を示すカウンタ値を創出するためのコードセグメントのセット、及び、
前記公開鍵をアウトプットする時に前記カウンタ値をアウトプットするためのコードセグメントのセット、
を更に具備する請求項２６に記載の記憶媒体。
【請求項２８】
前記第１のプライベート鍵が有効でない場合、前記カウンタ値に基づき前記第１のプライベート鍵と前記システムパラメータとを利用して前記新しいプライベート鍵を創出するためのコードセグメントのセット、
を更に具備する請求項２７に記載の記憶媒体。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、一般に暗号システムに係り、特に、暗号システムのための鍵の生成と入替えに関する。
【背景技術】
【０００２】
暗号化署名は、公開鍵暗号化を使用して生成され得る。公開鍵暗号化システムにおいて、利用者は、文書を認証するためにプライベート鍵と公開鍵の両者を持つ。公開鍵は共有される一方で、プライベート鍵は秘密に保たれる。利用者は、目標構成要素或いは団体に対しデジタル署名と共に通信を送ることにより利用者のプライベート鍵を用いて通信に署名する。送られる側は、その後、利用者の公開鍵を用いて通信文とデジタル署名を検証する。
【０００３】
１つの適用例では、公開鍵暗号システムは、携帯機器（以後トークンと記す）において実施されることが可能である。プライベート及び公開鍵がトークンのために生成される。プライベート鍵はトークンの中に留まり、公開鍵は１或いは１より多い目標構成要素へ送られる。その時トークンは入口への、銀行口座への、そしてコンピュータネットワーク等々へのアクセスを可能にする目標構成要素との種々の関係を樹立するため所有者によって利用されることが出来る。
【０００４】
しかしながら、トークン（従ってその中に記憶されているプライベート鍵）は盗まれるかもしれないし、或いは代わりに解読されたり、失われたり、破壊されるかもしれない。

もしトークンが盗まれるなら、トークンが盗人の手中にある間に盗人によりなされる損傷を制限することが重要である。もし、理由が何であろうと、その所有者が、これ以上それを全く利用することができないならば、問題は、トークンによって可能にされた種々の関係を再樹立しようとするとはいえ、所有者にとって主要な不便の一つどころではない。

【０００５】

それ故、トークン中の暗号鍵を入れ替えるもっと便利な、効率的な及び／又は秘密性の高い方法に対する必要性がある。

【発明の開示】

【０００６】

［サマリー］

実施形態は、秘密鍵を明かすことなく秘密鍵が入れ替えられ得る方法及び／又はシステムを述べる。より詳細には、トークン所有者は、例えば、将来のトークンの入替えのために、その時に秘密鍵を明かすことなく、備えることが出来る。例えば、入替えトークンが使用される時に、それは暗黙裡に検証されることが可能で、新しいトークンを使用する行為は、古いトークンを使用不能にするために検証者によって利用される。これは少なくとも二つの理由のために重要である。第一に、例え元のトークンが盗まれたとしても、盗人は、検証者に対して盗まれたトークンを使用することは最早できない。第二に、将来の利用のための準備がどういうわけか悪用され、そして新しいトークンがトークンの所有者が知ることなく作られたとしても、所有者は、現行のトークンを利用する認証が拒絶される時に、直ぐにこのことに気が付くであろう。それ故、所有者は他の是正措置をとることが出来る。

【０００７】

１つの実施形態においては、公開暗号システムにおける認証のための方法は、第１のプライベート鍵と対応する第１の公開鍵を創出することを具備する。第１のプライベート鍵に関係付けられた第２のプライベート鍵及び第２のプライベート鍵に対応する第２の公開鍵もまた創出される。第２のプライベート鍵は、それが再創出されるように一回アウトプットされ、そして第２の公開鍵は、第１の公開鍵をアウトプットする時にアウトプットされる。第１のプライベート鍵は、認証のために使用される。本方法は、更に第２のプライベート鍵を創出すること、そして第２のプライベート鍵を認証のために使用することを備える。

【０００８】

第１のプライベート鍵は、第２のプライベート鍵が認証に使用される時に使用不能にされることが可能である。付け加えるに、第２のプライベート鍵に関係付けられた第３のプライベート鍵及び第３のプライベート鍵に対応する第３の公開鍵が創出され得る。第３の公開鍵は、それが再創出されるように一回アウトプットされ得る。第３のプライベート鍵は、それから再創出されて、そして認証のために使用される。或いは、認証のための第２のプライベート鍵の使用は不能にされることが可能で、そして第３のプライベート鍵が認証のために使用され得る。その後、第２のプライベート鍵は、再創出されて認証のために使用されることが可能である。

【０００９】

本方法は、更に第２の鍵に関係付けられた第３のプライベート鍵を創出すること及び第３のプライベート鍵に対応する第３の公開鍵を創出すること；第３のプライベート鍵に関係付けられた第４のプライベート鍵を創出すること及び第４のプライベート鍵に対応する第４の公開鍵を創出すること；第４のプライベート鍵をそれが再創出されるように一回アウトプットすること；及び、第３及び第４の公開鍵をアウトプットすること、を備える。認証のための第２のプライベート鍵の使用は、不能とされることが可能で、そして第３のプライベート鍵が認証のために使用され得る。その後、第４のプライベート鍵が再創出され、そして認証のために使用されることが可能である。その上、第２の公開鍵をアウトプットすることは、第２の公開鍵の少なくとも２つの配分（share）を創出し、そして各配分を異なる構成要素に一回アウトプットすることを備える。

【００１０】
他の１つの実施形態において、暗号検証のための方法は、第１の公開鍵を受信すること；第１の公開鍵に関係付けられた第２の公開鍵を受信すること；第１の公開鍵を認証のために使用すること；及び、第１の公開鍵が機能しない場合に第２の公開鍵を認証のために使用すること、を備える。本方法は、更に、もし第１の公開鍵が機能せずそして第２の公開鍵が認証に成功するという結果になる場合に、第２の公開鍵に関係付けられた第３の公開鍵を受信することを備える。或いは、もし第１の公開鍵が機能せずそして第２の公開鍵が認証に成功するという結果になる場合に、本方法は、第２の公開鍵に関係付けられた第４の公開鍵と第３の公開鍵を受信することを備える。

【００１１】
また他の１つの実施形態において、認証のための方法は、プライベート鍵及び対応する公開鍵を関連するシステムパラメータを用いて創出すること；公開鍵をアウトプットする時にシステムパラメータをアウトプットすること；及び、プライベート鍵を認証のために使用すること、を備える。本方法は、更に、以前のプライベート鍵とシステムパラメータを利用して新しいプライベート鍵を創出することを備える。公開及びプライベート鍵の生成を示すカウンタ値が創出され、そして公開鍵をアウトプットする時にアウトプットされることが可能である。その後、新しいプライベート鍵は、カウンタ値に基づき以前のプライベート鍵とシステムパラメータを利用して創出されることが可能である。

【００１２】
その上、他の１つの実施形態において、検証のための方法は、公開鍵を受信すること；公開鍵に関係付けられたシステムパラメータを受信すること；公開鍵を使用して認証すること；及び、新しい公開鍵を生成し、そしてその新しい公開鍵を使用して認証すること、を備える。ここで、この新しい公開鍵は、以前の公開鍵とシステムパラメータとから導出される。本方法は、更に、以前の公開鍵の多数の冪乗を認証のために使用すること；及び新しい公開鍵として機能する１つを受け入れることを備える。或いは、本方法は、更に、プライベート及び公開鍵の生成を示すカウンタ値を受信すること；及び、カウンタ値に基づき以前の公開鍵とシステムパラメータとを用いて新しい公開鍵を生成すること、を備える。

【００１３】
更に他の１つの実施形態では、公開暗号システムにおける認証のための装置は、第１のプライベート鍵と対応する第１の公開鍵を創出するための手段；第１のプライベート鍵に関係付けられた第２のプライベート鍵を創出するための及び第２のプライベート鍵に対応する第２の公開鍵を創出するための手段；第２のプライベート鍵をそれが再創出されるように一回アウトプットするための手段；第１の公開鍵をアウトプットする時に第２のプライベート鍵をアウトプットするための手段；及び、第１のプライベート鍵を認証のために使用するための手段、を備える。或いは、公開暗号システムにおける認証のための装置は、プライベート鍵及び対応する公開鍵を関連するシステムパラメータを用いて創出するための手段；公開鍵をアウトプットする時にシステムパラメータをアウトプットするための手段；及び、プライベート鍵を認証のために使用するための手段、を備える。

【００１４】
別の１つの実施形態では、公開暗号システムにおける検証のための装置は、第１の公開鍵を受信するための手段；第１の公開鍵に関係付けられた第２の公開鍵を受信するための手段；第１の公開鍵を認証のために使用するための手段；及び、もし第１の公開鍵が機能しない場合に第２の公開鍵を認証のために使用するための手段、を備えることが可能である。或いは、公開暗号システムにおける検証のための装置は、公開鍵を受信するための手段；公開鍵に関係付けられたシステムパラメータを受信するための手段；公開鍵を使用して認証するための手段；及び、もし以前の公開鍵が機能しない場合に、新しい公開鍵を生成するためのそして新しい公開鍵を使用して認証するための手段、を備えることが可能である。ここで新しい公開鍵は、以前の公開鍵とシステムパラメータから導出される。

【００１５】

更に別の１つの実施形態では、公開暗号システムにおける機械可読媒体は、第１のプライベート鍵と対応する第１の公開鍵を創出するためのコードセグメントのセット；第１のプライベート鍵に関係付けられた第２のプライベート鍵を創出するためのそして第２のプライベート鍵に対応する第２の公開鍵を創出するためのコードセグメントのセット；第２のプライベート鍵をそれが再創出され得るように一回アウトプットするためのコードセグメントのセット；第１の公開鍵をアウトプットする時に第２の公開鍵をアウトプットするためのコードセグメントのセット；及び、第１のプライベート鍵を認証のために使用するためのコードセグメントのセット、を備えることが可能である。公開暗号システムにおける機械可読媒体は、プライベート鍵及び対応する公開鍵を関連するシステムパラメータを用いて創出するためのコードセグメントのセット；公開鍵をアウトプットする時にシステムパラメータをアウトプットするためのコードセグメントのセット；及び、プライベート鍵を認証のために使用するためのコードセグメントのセット、を備えることが可能である。

【００１６】

更にまた別の１つの実施形態では、公開暗号システムにおける機械可読媒体は、第１の公開鍵を受信するためのコードセグメントのセット；第１の公開鍵に関係付けられた第２の公開鍵を受信するためのコードセグメントのセット；第１の公開鍵を認証のために使用するためのコードセグメントのセット；及び、第１の公開鍵が機能しない場合に第２の公開鍵を認証のために使用するためのコードセグメントのセット、を備えることが可能である。公開暗号システムにおける機械可読媒体は、公開鍵を受信するためのコードセグメントのセット；公開鍵に関係付けられたシステムパラメータを受信するためのコードセグメントのセット；公開鍵を使用して認証するためのコードセグメントのセット；及び、もし以前の公開鍵が機能しない場合に、新しい公開鍵を生成するためのそして新しい公開鍵を使用して認証するためのコードセグメントのセット、を備えることが可能である。ここで新しい公開鍵は、以前の公開鍵とシステムパラメータから導出される。

【詳細な説明】

【００１７】

様々な実施形態が、図面を参照して詳細に述べられる。図面において同じ参照番号は同じ要素を指している。

【００１８】

一般に、記載されている実施形態は、秘密鍵を明かすことなく秘密鍵の将来の入替えのための準備を可能にする。以下の記載において、本発明の完全な理解を提供するために、具体的な詳細が与えられる。しかしながら、本発明は、これ等の具体的な詳細がなくても実施されることが可能であることは、当業者により理解される。例えば、回路は、本発明を無用な瑣末で不明瞭にならないようにブロック図で示されることができる。他の例では、周知の回路、構造及び技術が、本発明を不明瞭にしないために詳細に示されることができる。

【００１９】

本発明が、フローチャート、流れ図、構造図、或いはブロック図として表現されるプロセスとして記載され得ることを特に注意する。フローチャートは、作業を順次的に起こるプロセスとして記述することがあるが、多くの工程は並行して或いは同時に実行されることが可能である。その上、工程の順序は、再配列されることが可能である。あるプロセスは、その工程が完了された時に終了される。プロセスは、方法、機能、処理手順、サブルーチン、サブプログラム、等々に対応することが可能である。プロセスが機能に対応する時、その終了は呼び出し機能或いは主機能への機能の回帰に対応している。

【００２０】

図１は、利用者機器１１０と検証者機器１２０とを備えた暗号システム１００の一実施形態である。利用者機器１１０は、トークン、携帯電話機、個人のデータアシスタント、パソコン（デスクトップ或いはラップトップ）或いは他の電子機器、において実行され得る。検証者機器１２０は、例えば、銀行、弁護士、或いはバリサイン（Verisign）社のよ

うな信用されている第三者機関のような構成要素により実行され得る。図１は、１つの検証者機器１２０を示しているけれども、１或いは１より多い検証者機器があり得ることは当業者により理解される。

【００２１】

利用者機器１１０は、暗号鍵を生成し操作するプロセッサ１１２と、生成された暗号鍵を記憶する記憶媒体１１４と、通信を送る送信機１１６とを備える。公開鍵暗号システムでは、プライベート鍵は、利用者機器１１０内にとどまる秘密鍵である。それに対し公開鍵は送信機１１６を使用して検証者機器１２０へ送信される。通信は、その後、プライベート鍵を用いて署名され、認証のために検証者機器１２０へ送られる。

【００２２】

検証者機器１２０は、利用者機器１１０からの通信を受信する受信機１２２、受信された通信を記憶する記憶媒体１２４、及び通信を認証するためのプロセッサ１２６とを備える。記憶媒体１２４は、また利用者機器１１０から送信された公開鍵を記憶するために認証データベースを実行することも可能である。より詳しくは、受信機１２２は、公開鍵を受信しそして記憶媒体１２４に記憶される認証データベースを創出する。検証者機器１２０が署名された通信を認証のために受信した時に、対応する公開鍵が認証データベースから取得され、そして通信を検証するために使用される。認証データベースは、記憶媒体１２４及び／或いは検証者機器１２０とは異なる場所で、及び／或いは、外部的に、与えられ得るということは注意すべきである。

【００２３】

図２は、公開鍵暗号システムのための鍵を生成するための方法２００を示している。プロセッサ１１４は、第１の鍵のセット、すなわち第１のプライベート鍵及び対応する第１の公開鍵、を創出する（２１０）。プロセッサ１１４は、また第２の鍵のセット、すなわち第２のプライベート鍵及び対応する第２の公開鍵、も創出する（２２０）。第２の鍵のセットは、第１の鍵のセットに関係付けられる。しかしながら、第２のセットは第１のセットとは独立に創出される。鍵は業界で公知の種々のアルゴリズムを用いて生成され得る。

【００２４】

例えば、鍵は周知のデジタル署名標準（Digital Signature Standard）（ＤＳＳ）に基づいて生成され得る。ここで、プロセッサ１１４は、ＤＳＳのために使用されるべきプライベート或いは秘密鍵ｘを創出するために乱数（randomness）の内部源を使用する。対応する公開鍵Ｘは、それから以下のように計算される。ここで、Ｐはそこで数学的な操作が起こる数学的体を規定する大きな、例えば１０２４ビットの、素数であり、Ｑは典型的には１６０ビット或いはそれ以上の素数であり、その結果Ｑ｜（Ｐ－１）になり、そして、ｇは数学的体の元であり、そしてＱ次の部分群Ｆ＊（Ｐ）の生成元である。

【００２５】

$$X = g^{x} \pmod{P}$$

それ等の鍵は、当初記憶媒体１１４に記憶され得る。第１のプライベート鍵は、利用者機器１１０内に保持され、そして第２のプライベート鍵は、例え利用者機器１１０が盗まれたり紛失したり解読されたりしても再創出され得るようにアウトプットされる。ここで、第２のプライベート鍵が利用者機器１１０の内部に保持され、そして第１の鍵は、それが再創出され得るようにアウトプットされることが可能である。しかしながら、説明の目的で、第２のプライベート鍵がアウトプットされると仮定する。利用者機器１１０内部で保持されている鍵は、認証のために使用される主要な鍵であり、そして有効になる。アウトプットされたプライベート鍵は将来の入替え鍵であり、そして無効になる。

【００２６】

第２のプライベート鍵は、利用者機器１１０の所有者の要請で一回アウトプットされる（２３０）。その後では、利用者機器１１０は、そのような要請に応答しない。第２の公開鍵も、また第１の公開鍵がアウトプットされる時アウトプットされる（２４０）。ここで、第２のプライベート及び公開鍵は、送信機１１６を使用してアウトプットされ得る。

【００２７】
１つの実施形態では、秘密共有方式が使用されることが可能で、それによって秘密情報のｎ個の配分（share）が、利用者機器１１０内部で創出され、そして信頼の置ける共有者（shareholder）に独立に割り当てられる。その結果、後になってｋ個の共有者（ｋ＜ｎ）は、秘密情報を再創出することが出来る。信頼の置ける共有者は、これに限られるわけではないが、利用者機器１１０の所有者であるかも知れないし、或いは、所有者の信頼されている友人や、例えば銀行、会計士或いは他の金融機関のような所有者の秘密情報を既に持っている者や、或いはバリサイン社のような「信頼されている第三者機関」であり得る。
【００２８】
例えば、利用者機器１１０のプロセッサ１１４は、プライベート鍵の３個の配分を創出し得る。これ等は、利用者の要請で送信機１１６を用いて、一度に１個ずつ、アウトプットされる。各配分は、３個の団体の指定された１つに一回アウトプットされる。全ての配分がアウトプットされてしまった後で、利用者機器１１０は、もはやこのような要請に応答しない。しかしながら、利用者は３団体のうち何れか２つの協力を得て秘密鍵を再創出することが出来る。他方、一団体でも信頼を置けないということになれば、３団体のうち誰もプライベート鍵を単独で再創出することは出来ない。その上、もし１つの団体が彼等の配分を紛失した場合、他の２つはなお入替えを創出するのに必要とされる情報を提供できる。もし秘密共有方式が実行される場合、第１のプライベート鍵は利用者機器１１０内にとどまり、そして第２のプライベート鍵が再創出され得るように、第２のプライベート鍵が配分としてアウトプットされる。３個より多い又は少ないプライベート鍵の配分が創出され得て、そして対応する数の団体にアウトプットされることが可能であることは、理解されるべきである。
【００２９】
図２に戻って参照して、第１のプライベート鍵は、もしそれが有効ならば、認証する時に使用される（２５０及び２６０）。換言すると、利用者機器１１０は、第１のプライベート鍵を用いて通信に署名し、目標とされる関係先に関係付けられた署名を添えて通信を送る。関係先は、その後、第１の公開鍵を用いて通信を検証する。もし第１のプライベート鍵が有効でなければ、代わりのプライベート鍵、すなわち、第２のプライベート鍵が認証のために使用される（２７０）。
【００３０】
第１のプライベート鍵は、様々な理由で有効でないことがあり得る。例えば、利用者機器１１０の所有者は、利用者機器１１０及び／或いは第１のプライベート鍵が盗まれたり、解読されたり、紛失されたり及び／或いは破壊されたりしたという理由で、第１のプライベート鍵を入れ替えた可能性がある。より詳しくは、利用者機器１１０の所有者は、第１のプライベート鍵を無効にする及び／或いは不能にすることができる。そのような場合、第２のプライベート鍵が再創出されそして認証のために使用される。或いは、１つのプライベート鍵がある暗号システムの中で期限切れになることがある。もし第１のプライベート鍵が期限切れした場合、第２のプライベート鍵が、利用者機器１１０により再創出されて認証のために使用される。ある実施形態においては、利用者機器１１０は、入替えプライベート鍵の使用が既存の主プライベート鍵、この場合第１のプライベート鍵であるが、を不能にするように設計されることが可能である。ここでは、もしプライベート鍵が盗まれたり、解読されたり、紛失されたり及び／或いは破壊されたりした場合、プライベート鍵を再創出することは、利用者機器１１０を、例えば旧トークンから新トークンへと入れ替えることを意味する可能性がある。さもなければ、ただ単に秘密鍵が、盗まれたり、紛失されたり、及び／或いは期限切れになったというだけで、プライベート鍵を再創出するということは、利用者機器１１０内部におけるプライベート鍵の交換を意味する可能性がある。
【００３１】
第２のプライベート鍵が再創出されそして認証のために使用される時、第２のプライベ

ート鍵は、第１のプライベート鍵に入れ替わりそして有効になる。それ故、プロセッサ１１２は、第２のプライベート鍵に関係付けられた入替え鍵の新しいセットを創出し（２８０）アウトプットする（２９０）。換言すれば、第３の鍵のセットが創出されそして、将来の入替え鍵としてアウトプットされる。第１と第２の鍵のセットの場合と同様、第３の鍵のセットは第２の鍵のセットに関係付けられているとはいえ、第３のセットは第２のセットとは独立に創出される。しかも、第２のプライベート鍵は、利用者機器１１０内部に保持されるが、他方、第３のプライベート鍵はそれが再創出され得るようにアウトプットされる。ここで、第３のプライベート鍵は、例えば業界で周知のシャミール（Shamir）の共有方式を利用して、１或いは１より多い同じ或いは異なる構成要素に一回アウトプットされる。第３の公開鍵は、第２の公開鍵がアウトプットされる時、例えば送信機１１６を使用してアウトプットされることが可能である。

【００３２】

もし第２のプライベート鍵が無効になった場合、第３のプライベート鍵が第２のプライベート鍵を入れ替えるために再創出され、そして認証のために使用されることが出来る。その場合では、もう１つの新しい入替え鍵のセット、例えば第４の鍵のセット、が創出され、そして将来の入替え鍵としてアウトプットされる。より詳しくは、入替えのプライベート鍵が再創出されそして以前の主プライベート鍵に入れ替わって新しい主要鍵になる時、入替え鍵のセットが創出され、将来の入替え鍵としてアウトプットされる。もし第３のプライベート鍵が無効になった場合、第４のプライベート鍵が再創出され、そして認証のために使用されることが出来るが、他方で、第５の鍵のセット、が創出されそして将来の入替え鍵としてアウトプットされる。秘密鍵のこの創出、アウトプット及び再創出は、上述のようにそして必要に応じて繰り返し発生し、以前の秘密鍵と入れ替わることが可能である。ある実施形態では、秘密鍵が入れ替えられ得る回数は、制限されることがある。しかも、プロセッサ１１４が入替えのプライベート鍵を再創出し、そしてその再創出された鍵を認証のために使用することも可能である。各々の新しい主プライベート鍵のための入替え鍵のセットを、前もって、創出することによって、プライベート鍵は、明らかにされることなく入れ替えられることが可能である。

【００３３】

図３は、通信を認証するための方法２００に対応する方法３００を示す。検証者機器１２０は、利用者機器１１０から第１の公開鍵と第２の公開鍵を受信する（３１０）、ここで、第１の公開鍵は、第１のプライベート鍵に対応し、そして第２の公開鍵、は第２のプライベート鍵に対応する。第２のプライベート鍵は、第１のプライベート鍵に関係付けられ、そしてそれ故、第２の公開鍵は、第１の公開鍵に関係付けられる。公開鍵は、記憶媒体１２４の認証データベースの中に記憶される。ここでは、１つの公開鍵が有効である主公開鍵として記憶される一方、他の公開鍵は無効である入替え公開鍵として記憶される。この例では、第１の公開鍵は主要鍵であり、そして第２の公開鍵は入替え鍵である。しかも、第１の公開鍵と第２の公開鍵は、受信機１２２を使用して受信されることが出来る。

【００３４】

署名された通信が利用者機器１１０から認証のために受信される時に、プロセッサ１２６は主要鍵、すなわちこの例では第１公開鍵、を用いて認証を試みる（３２０及び３３０）。換言すれば、第１の公開鍵が認証データベースから取り出されて、通信を検証するために使用される。もし通信が第１の公開鍵を使用して検証されることが出来ない場合、プロセッサ１２６は、署名された通信の認証を試みるために、入替え公開鍵、すなわちこの例では第１の公開鍵に関係付けられた第２の公開鍵、を使用する（３４０及び３６０）。もし成功すれば、検証者機器１２０は、第１のプライベート鍵が入れ替えられていたとみなすことが出来る。

【００３５】

検証者機器１２０は、しかも新しい入替え公開鍵、すなわち第３の公開鍵、を利用者機器１１０から受信し（３６０）、そして認証データベースを更新する（３７０）。検証者機器１２０は、署名された検証を用いて第３の公開鍵を受信することが出来る。しかしな

がら、検証者機器１２０は、第２の公開鍵を使用して認証に成功した後に、第３の公開鍵を受け取ることが出来る。これは、以前の公開鍵の不正な所有者がもっともらしく見える入替え鍵を創出することを防止する。或いは、検証者機器１２０は、第２の公開鍵を使用して認証に成功した後に入替え鍵を要請することが出来る。

【００３６】

また、検証者機器１２０が第３の公開鍵を受信する及び／或いは受け入れることが可能であるけれども、認証データベースは、第２の公開鍵が入れ替えられていたことを示さないことがある。これは、検証者機器１２０が、認証データベースを定期的に或いはある時間間隔に基づいて更新し得るためである。その結果、もし第２のプライベート鍵が無効になり、そして認証データベースが更新される前に、第３のプライベート鍵を使用する通信が利用者機器１１０から受信された場合、検証者機器１２０は、通信を認識することが出来ずそれ故検証することが出来ない。従って、主要鍵と関係付けられた１個より多くの入替え鍵のセットが前もって創出され、そして将来の入替え鍵としてアウトプットされることが可能である。

【００３７】

図３では、第２の公開鍵を使用する認証が成功すると仮定している。しかしながら、種々の理由により第２の公開鍵が認証不成功に終わることがあり得る。１つの理由は、不正な所有者が主要鍵を入れ替えることを試みていることがあり得る。もう１つの理由は、第２のプライベート鍵が第３のプライベート鍵により入れ替えられていた、この場合検証者機器１２０は、既に第３の公開鍵を受信していたはずである、ということであり得る。それ故に、もし第２の公開鍵が認証不成功に終わる場合、検証者機器１２０は、もし利用可能ならば新しい入替え鍵、すなわち第３の公開鍵、を使用して認証を試みることが可能である。さもなければ、認証は失敗する。検証者機器１２０は、もし第３のプライベート鍵が第４のプライベート鍵により入れ替えられている場合第４の公開鍵を使用して認証を試みること、もし第４のプライベート鍵が第５のプライベート鍵により入れ替えられている場合第５の公開鍵を使用して認証を試みること、等々が可能であることは理解される。ある実施形態では、公開鍵が入れ替えられ得る回数が、与えられた許容入替え回数或いは与えられた期間に基づいて制限されることが可能である。

【００３８】

上述のように、第２の鍵のセットが有効でその後の認証のために使用されている間に、第３の鍵のセットが創出され、そして無効である入替え鍵としてアウトプットされる。その後の認証のために第３の鍵のセットを使用することも可能である。例えば、利用者機器１１０は、第３の鍵のセットを創出し、そして第２のプライベート鍵を再創出する。第２のプライベート鍵は、通信の認証のために最初に使用される。これは、検証者機器１２０が第３の鍵が創出されていたことを未だ認識できないためである。第３の公開鍵は、署名された通信とともにアウトプットされ得る。通信が首尾よく検証される時、検証者機器１２０は、第３のセットがその後の認証のために使用されるように、認証データベースを更新することが可能である。

【００３９】

もし認証データベースが定期的に或いはある時間間隔に基づいて更新されるならば、例え第３の公開鍵がアウトプットされていたとしても、第２のプライベート鍵は、一時的に有効を維持し、そして認証のために使用されることが可能である。第３のプライベート鍵は、その後、検証者機器１２０の更新スケジュールに基づいて選択された時間間隔の後で有効になり得る。或いは、認証データベースが更新される時に、検証者機器１２０は、利用者機器１１０に制御信号を送ることが可能であり、認証データベースが更新されたということを指示する。利用者機器１１０は、それから第３のプライベート鍵を使用し、そして検証者機器１２０は、認証のために第３の公開鍵を使用する。更にそれに代わって、検証者機器１２０は、認証データベースが入替え鍵を記憶するために更新されることが可能になるように、一度に入替え鍵を要請することが可能である。ここで、利用者機器１１０は、要請が検証者機器１２０から受信されるまでは、第３の公開鍵をアウトプットしない

。

【００４０】

利用者機器１１０が認証のために第３のプライベート鍵を使用し始める時、第２のプライベート鍵は、たとえ利用者機器１１０が紛失されたり或いは盗まれたりしても、第２のプライベート鍵が再創出され得ないように、廃棄されることが可能である。その上、利用者機器１１０は、第２のプライベート鍵が既にアウトプットされてしまったので、第２或いは第３のプライベート鍵どちらもアウトプットしないことを注意する。しかしながら、利用者機器１１０は、第２のプライベート鍵が再創出される場合に、利用者機器の所有者が第２のプライベート鍵を再びアウトプットすることが出来るように設計されることが可能である。第２のプライベート鍵は、それから１或いは１より多い同じ或いは異なる構成要素に対し、例えば共有方式を使用して一回アウトプットされることが可能である。

【００４１】

従って、第２のプライベート鍵は、利用者機器１１０の所有者を認証しそして第１のプライベート鍵の新しいプライベート鍵、すなわち第３のプライベート鍵、での入替えを可能にする一時的なプライベート鍵として作用することができる。第３のプライベート鍵は、その後、それが無効になるまで認証のために使用される。無効になった時、第２のプライベート鍵が再び再創出され、そして利用者機器１１０の所有者を認証して第３のプライベート鍵の新しいプライベート鍵での入替えを可能にするために使用される。ここで、第４の入替え鍵のセットは、第３のプライベート鍵を入れ替えるために創出される。

【００４２】

他の１つの実施形態においては、第３及び第４の鍵のセットは、第１及び第２の鍵のセットに対する入替え鍵として創出されることが可能である。１つのセットのプライベート鍵は、その後の認証のために使用されるが、他方、その他のセットのプライベート鍵は、それが再創出され得るように利用者機器１１０の所有者の要請で一回アウトプットされる。例えば、第３のプライベート鍵は、その後の認証のために使用されることが可能であるが、他方で、第４のプライベート鍵はそれが再創出され得るようにアウトプットされる。ここで、第２のプライベート鍵は、利用者機器１１０の所有者を認証し、そして第１のプライベート鍵の新しいプライベート鍵、すなわち第３のプライベート鍵、での入替えを可能にする一時的なプライベート鍵として依然として作用することができる。第２のプライベート鍵は、第１のプライベート鍵が入れ替えられた後に廃棄されることができる。第３のプライベート鍵は、その後、それが無効になるまで認証のために使用される、その時、第４のプライベート鍵が再創出されそして利用者機器１１０の所有者を認証して、第３のプライベート鍵の新しいプライベート鍵のセットでの入替えを可能にするために使用される。この場合、第５及び６の鍵のセットが、新しい入替え鍵のセットとして創出される。

【００４３】

暗号鍵の複数のセットは、上述のように独立に生成されることが可能であり、そこでは１つの鍵は認証のための主要鍵として作用する一方、別の１つの鍵は入替え鍵として作用し、それにより主要鍵が無効になった場合の予備鍵として作用する。他の１つの実施形態においては、入替え鍵のセットは、以前の暗号鍵のセットから導出されることが可能である。

【００４４】

図４は公開暗号システムのための鍵を生成するための別の１つの方法４００を示す。プロセッサ１１２は、プライベート鍵及びシステムパラメータに関係付けられた対応する公開鍵を創出する（４１０）。鍵とシステムパラメータは、最初は記憶媒体１１４内に記憶されることが可能である。プライベート鍵は、利用者機器１１０内部に保持されるが、他方公開鍵及びシステムパラメータは、送信機１１６を使用してアウトプットされる（４３０）。

【００４５】

認証する時に、プライベート鍵が、もしそれが有効ならば使用される（４４０，４５０及び４６０）。換言すれば、利用者機器１１０は、プライベート鍵を用いて通信に署名し

、そして通信及びそれに関係付けられた署名を目標団体或いは機器へ送り、その後、団体或いは機器は、対応する公開鍵を用いて通信を検証する。もしプライベート鍵が有効でなければ、新しい或いは入替えのプライベート鍵がシステムパラメータ及び旧の或いは以前のプライベート鍵を使用して創出される（４７０）。ここで、以前のプライベート鍵は種々の理由で有効でないことがあり得る。例えば、利用者機器１１０が盗まれたり、解読されたり、紛失されたり或いは破壊されたりしたという理由で、利用者機器１１０の所有者がプライベート鍵を無効にしてしまうことがあり得る。或いは、プライベート鍵がある暗号システムの中で期限切れになることがあり得る。新しいプライベート鍵は、その時はもしそれが有効であれば（４５０及び４６０）、認証のために使用される。新しいプライベート鍵の使用は、以前のプライベート鍵を使用不能にする。

【００４６】

図５は、通信を認証するための方法４００に対応する方法５００を示す。検証者機器１２０は、利用者機器１１０からプライベート鍵に対応する公開鍵を受信する（５１０）。検証者機器１２０は、しかも、利用者機器１１０から秘密及び公開鍵に関係付けられたシステムパラメータも受信する（５２０）。公開鍵とシステムパラメータは、記憶媒体１２４の認証データベースの中に記憶される。

【００４７】

署名された通信が認証のために利用者機器１１０から受信された時に、プロセッサ１２６は、対応する公開鍵を用いて認証する（５３０及び５４０）。換言すれば、対応する公開鍵が認証データベースから引き出され、そして通信と関連する署名を検証するために使用される。もし通信が公開鍵を使用して検証されることが出来ないならば、プロセッサ１２６は、以前の公開鍵とシステムパラメータを用いて新しい公開鍵を導出する（５６０）。その後、検証者機器１２０は、新しい公開鍵を使用して認証を試みる（５４０）。この導出と新しい又は入替え公開鍵を使用した試行は、認証成功が起こるまで上述のようにそして必要に応じて繰り返し起こる。ある実施形態においては、秘密鍵が入れ替えられ得る回数は、与えられた許容入替え回数又は与えられた期間に基づいて限定されることが可能である。

【００４８】

方法４００及び５００において、システムパラメータは、実行される暗号システムに依存する。例えば、もし暗号システムがＤＳＳに基づいているならば、システムパラメータは乱数である。

【００４９】

より詳しくは、秘密鍵ｘが創出される時に、利用者機器は、ｍｏｄ Ｑの部分群の１つの元でもある乱数ｒ及びオプションのカウンタ値ｃを創出し、それ等は公開及び秘密鍵にそれから関係付けられる。公開鍵がアウトプットされそして検証者機器１２０内に記憶される時に、ｒ及びｃもまたアウトプットされる。オリジナルな利用者機器１１０がｃ＝０を有すると仮定して、利用者機器１１０は、入替え秘密鍵の配分を以下のように創出する：

$$y = x * r \pmod{P}$$

対応する公開鍵Ｙは、以下のようになる：

$$Y = g^{y} = g^{(x*r)} = (g^{x})^{r} = X^{r} \pmod{P}$$

新しい公開鍵は、旧の公開鍵とｒの知識から導出されることができる。新しい鍵ｙを与えられた、例えばトークンのような、新たに創出された利用者機器１１０は、ｃを増加し、そして同じｒを保有する。いずれかの利用者機器１１０により生成された署名は、ｃを含むはずであり、検証者機器１２０が検証のためにどの公開鍵を使用すべきかを容易に決定することを可能にしている。更に、検証者機器１２０は、例え所有者が最後に認証して以来多数の入替えが起こったとしても、署名を受け取って検証することが出来る。もしｃが署名の中に含まれているならば、それは旧の公開鍵をｃに基づいて適当な回数冪乗するために使用される。もしｃが含まれていないならば、検証者機器１２０は、単純にＸの多数の冪乗回を試みることが出来る。ここで、試行の回数に対する制限はセットされること

が可能である。もしこれ等の導出された公開鍵の１つが、署名を認証するために機能するならば、それは新しい公開鍵として受け入れられる。

【００５０】

それ故、利用者機器の所有者は、入替え時に秘密鍵を明かすことなく将来の入替えに備えることが出来る。しかも、入れ替えた利用者機器及び／或いは秘密鍵が使用される時に、それは暗黙裡に検証される。換言すれば、新しい利用者機器及び／或いは秘密鍵を使用する行為は、検証者により旧の利用者機器及び／或いは秘密鍵を使用不能にするために利用されることが可能である。

【００５１】

本実施形態は、ＤＳＳに基づいて記述されたが、その範囲はＤＳＳに制限されないことが、注意されるべきである。この技術において公知の異なる数学とプロセスを一般に用いるとしても、本実施形態は、他の公開鍵システムにも適用できる。また、ある実施形態はシャミールの秘密共有方法によって記述されているが、その他の公知の方法も同等に適用可能である。その上、利用者機器１１０が、各プライベート、公開、及び入替え鍵を生成し、そして生成された（複数の）鍵を認証のために使用するように設計された１つのプロセッサ１１２を示しているけれども、１より多いプロセッサが装備されて、鍵を生成し及び／或いは生成された（複数の）鍵を認証のために使用することが可能である。同様に、検証者機器１２０は、適用可能であるとして、各公開鍵を生成し、そして生成された（複数の）鍵を認証のために使用するように設計された１つのプロセッサ１２４を示しているけれども、１より多いプロセッサが装備されて（複数の）鍵を生成し、そして生成された（複数の）鍵を認証のために使用することが可能である。加えるに、利用者機器１１０の諸要素は、利用者機器１１０の操作と機能に影響を与えずに、好きなように、配置し直すことが可能であることは当業者によって理解される。同様に、検証者機器１２０の諸要素は、検証者機器１２０の操作と機能に影響を与えずに、好きなように、配置し直すことが可能である。

【００５２】

更に、実施形態は、ハードウエア、ソフトウエア、ファームウエア、ミドルウエア、マイクロコード又はそれ等の任意の組合せにより実行されることができる。ソフトウエア、ファームウエア、ミドルウエア又はマイクロコードの中で実行される時、必要なタスクを実行するためプログラムコード又はコードセグメントは、例えばそれぞれ記憶媒体１１４及び／或いは記憶媒体１２４のような機械可読媒体の中に、或いは示されていない独立した記憶媒体の中に記憶されることができる。プロセッサ１１２及び／或いは１２６は、望まれたタスクを実行できる。コードセグメントは、手順、機能、サブプログラム、プログラム、ルーチン、サブルーチン、モジュール、ソフトウエアパッケージ、クラス、或いは命令、データ構造或いはプログラムステートメントの任意の組合せを表すことが出来る。コードセグメントは、情報、データ、引数、パラメータ或いはメモリ内容を伝える及び／或いは受け取ることにより、他のコードセグメント或いはハードウエア回路に結合されることが出来る。情報、引数、パラメータ、データ等々はメモリ共有、メッセージパッシング、トークンパッシング或いはネットワーク伝送等々を含むいずれかの適当な手段を使用しても伝えられ、転送され或いは送信されることが可能である。

【００５３】

それ故、前述の実施形態は、単なる例示であって発明を限定すると解されるべきではない。記述は説明的になるように意図されており、本発明の請求範囲を制限するように意図されてはいない。かくして、本発明の教えるところは、他の型の装置に容易に適用されることが可能で、そして多くの代替、修正そして変形が当業者にとって明白である。

【図面の簡単な説明】

【００５４】

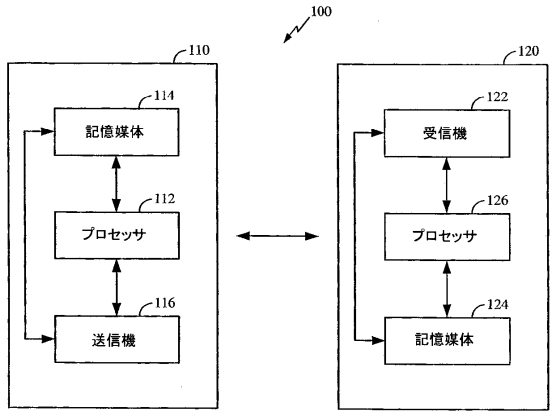
【図１】図１は暗号システムの１つの実施形態を示す。

【図２】図２は利用者機器からの認証のための方法を示す。

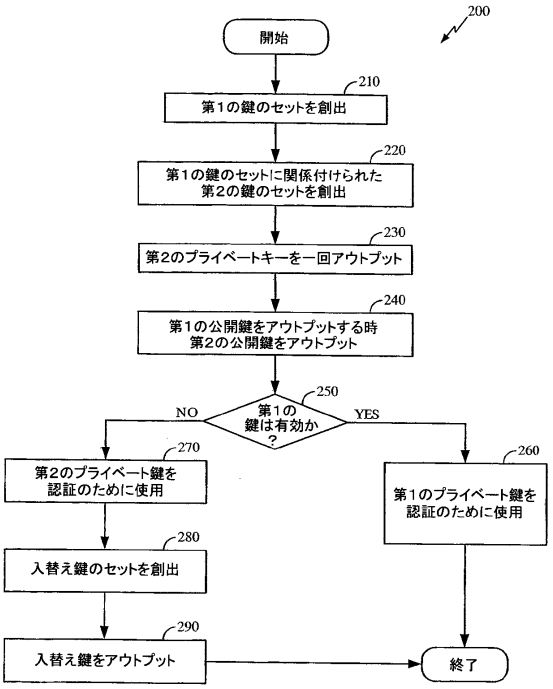
【図３】図３は検証者機器からの検証のための方法を示す。

【図４】図４は利用者機器からの認証のための別の方法を示す。
【図５】図５は検証者機器からの検証のための別の方法を示す。
【符号の説明】
【００５５】
１００…暗号システム，１１０…利用者機器，１２０…検証者機器，２００…方法，３００…方法，４００…方法，５００…方法。

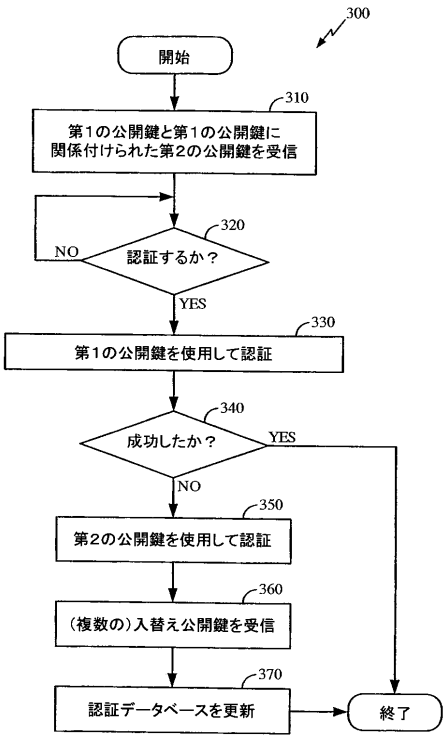
【図１】



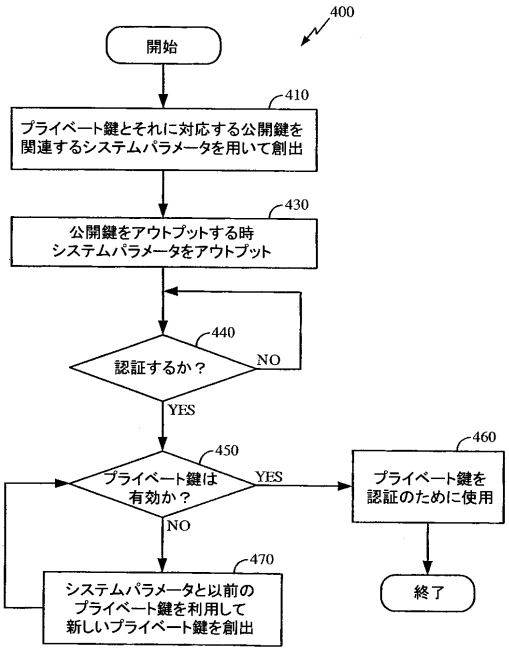
【図２】



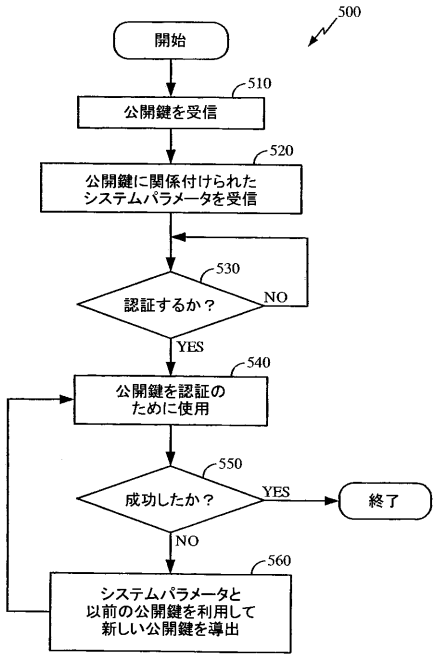
【図３】


300
開始
310
第１の公開鍵と第１の公開鍵に
関係付けられた第２の公開鍵を受信
320
NO
認証するか？
YES
330
第１の公開鍵を使用して認証
340
成功したか？
YES
NO
350
第２の公開鍵を使用して認証
360
（複数の）入替え公開鍵を受信
370
認証データベースを更新
終了

【図４】


400
開始
410
プライベート鍵とそれに対応する公開鍵を
関連するシステムパラメータを用いて創出
430
公開鍵をアウトプットする時
システムパラメータをアウトプット
440
認証するか？
NO
YES
450
プライベート鍵は
有効か？
YES
NO
460
プライベート鍵を
認証のために使用
470
システムパラメータと以前の
プライベート鍵を利用して
新しいプライベート鍵を創出
終了

【図５】


500
開始
510
公開鍵を受信
520
公開鍵に関係付けられた
システムパラメータを受信
530
認証するか？
NO
YES
540
公開鍵を認証の
ために使用
550
成功したか？
YES
終了
NO
560
システムパラメータと
以前の公開鍵を利用して
新しい公開鍵を導出

フロントページの続き

(74)代理人 100109830
弁理士 福原 淑弘
(74)代理人 100095441
弁理士 白根 俊郎
(74)代理人 100084618
弁理士 村松 貞男
(74)代理人 100103034
弁理士 野河 信久
(74)代理人 100092196
弁理士 橋本 良郎
(74)代理人 100100952
弁理士 風間 鉄也
(72)発明者 ローズ、グレゴリー・ジー.
オーストラリア国、ニュー・サウス・ウェールズ州 ２１３７、コンコード、アーチャー・ストリート ４０
(72)発明者 ガントマン、アレクサンダー
アメリカ合衆国、カリフォルニア州 ９２１２９、サン・ディエゴ、クリークウッド・レーン ８７０４
(72)発明者 ノエレンバーグ、ジョン・ダブリュ.
アメリカ合衆国、カリフォルニア州 ９２１３１、サン・ディエゴ、フィグ・トゥリー・ストリート １２３４３

審査官 青木 重徳

(56)参考文献 特表２００１－５０７５２８（ＪＰ，Ａ）
特開２０００－１７４７４６（ＪＰ，Ａ）
特開２００１－１０３０４５（ＪＰ，Ａ）
特開平０５－２２４６０４（ＪＰ，Ａ）
特開２００２－３７４２４０（ＪＰ，Ａ）
特開２０００－３０７５８８（ＪＰ，Ａ）
米国特許第０５６７５６４９（ＵＳ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
H04L 9/08