(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第5171991号
(P5171991)

(45)発行日　平成25年3月27日(2013.3.27)　(24)登録日　平成25年1月11日(2013.1.11)

(51)Int.Cl.　F I
H04L 9/08 (2006.01)　H04L 9/00 601C
H04L 9/32 (2006.01)　H04L 9/00 601E
H04L 9/00 675A

請求項の数 20　外国語出願　(全 15 頁)

(21)出願番号　特願2011-108819 (P2011-108819)
(22)出願日　平成23年5月13日 (2011.5.13)
(62)分割の表示　特願2006-529491 (P2006-529491)の分割
原出願日　平成16年5月17日 (2004.5.17)
(65)公開番号　特開2011-182454 (P2011-182454A)
(43)公開日　平成23年9月15日 (2011.9.15)
審査請求日　平成23年5月13日 (2011.5.13)
(31)優先権主張番号　10/440,486
(32)優先日　平成15年5月16日 (2003.5.16)
(33)優先権主張国　米国(US)

(73)特許権者　397071791
サーティコム　コーポレーション
カナダ国　エル４ダブリュー　Ｏビー５　オンタリオ，ミシソーガ，タホー　ブールバード　４７０１，タホー　エー，　６ティーエイチ　フロア
(74)代理人　100107489
弁理士　大塩　竹志
(72)発明者　ストルイク　マリヌス
カナダ国　オンタリオ　エム４ケイ　３ケイ８　トロント　カルロウ　アヴェニュー　７２３

審査官　中里　裕正

最終頁に続く

(54)【発明の名称】鍵合意および移送プロトコル

(57)【特許請求の範囲】
【請求項１】
データ通信システムにおける第１の通信部と第２の通信部との間での対称鍵の合意の方法であって、該第１の通信部および該第２の通信部は、それぞれ、マスター鍵Ｋを有し、該方法は、
該第１の通信部が第１の値Ｘを生成し、該第１の値Ｘを該第２の通信部に提供するステップと、
該第２の通信部が第２の値Ｙを生成し、該第１の値Ｘと該第２の値Ｙとの組み合わせにおいて鍵付き暗号関数を作用させることによって、共有鍵ｋを計算するステップであって、該第２の通信部は、該マスター鍵Ｋを、該鍵付き暗号関数に対する入力として用い、該第２の通信部により計算された該共有鍵ｋは、鍵付きハッシュ関数に対する入力として用いられ、該鍵付きハッシュ関数は、該第１の値Ｘ、該第２の値Ｙ、ならびに該第１の通信部および該第２の通信部のうちの一方の識別情報の組み合わせにおいて作用させるためのものである、ステップと、
該第２の通信部が該第２の値Ｙを該第１の通信部に提供するステップと、
該第１の通信部が、該第１の値Ｘと該第２の値Ｙとの組み合わせにおいて該鍵付き暗号関数を作用させることによって、該共有鍵ｋを計算するステップであって、該第１の通信部は、該マスター鍵Ｋを、該鍵付き暗号関数に対する入力として用い、該第１の通信部により計算された該共有鍵ｋは、該鍵付きハッシュ関数に対する入力として用いられる、ステップと

を包含する、方法。

【請求項２】

前記第２の通信部が、第１のハッシュ値を生成するために、前記第１の値Ｘ、前記第２の値Ｙ、ならびに前記第１の通信部および該第２の通信部のうちの一方の識別情報の組み合わせに、前記鍵付きハッシュ関数を適用するステップであって、該第２の通信部は、該第２の通信部によって計算された前記共有鍵ｋを、該鍵付きハッシュ関数に対する入力として用いる、ステップと、

該第２の通信部が、該第１のハッシュ値を該第１の通信部に提供するステップと、

該第１の通信部が、第２のハッシュ値を生成するために、該第１の値Ｘ、該第２の値Ｙ、ならびに該第１の通信部および該第２の通信部のうちの該一方の該識別情報の組み合わせに、該鍵付きハッシュ関数を適用するステップであって、該第１の通信部は、該第１の通信部によって計算された該共有鍵ｋを、該鍵付きハッシュ関数に対する入力として用いる、ステップと、

該第１の通信部が、該第１のハッシュ値が該第２のハッシュ値に等しいことを検証するステップと

をさらに包含する、請求項１に記載の方法。

【請求項３】

前記第１の通信部が、第３のハッシュ値を生成するために、前記第１の値Ｘ、前記第２の値Ｙ、ならびに該第１の通信部および前記第２の通信部のうちのもう一方の識別情報の組み合わせに、前記鍵付きハッシュ関数を適用するステップであって、該第１の通信部は、該第１の通信部によって計算された前記共有鍵ｋを、該鍵付きハッシュ関数に対する入力として用いる、ステップと、

該第１の通信部が、該第３のハッシュ値を該第２の通信部に提供するステップと、

該第２の通信部が、第４のハッシュ値を生成するために、該第１の値Ｘ、該第２の値Ｙ、ならびに該第１の通信部および該第２の通信部のうちの該もう一方の該識別情報の組み合わせに、該鍵付きハッシュ関数を適用するステップであって、該第２の通信部は、該第２の通信部によって計算された該共有鍵ｋを、該鍵付きハッシュ関数に対する入力として用いる、ステップと、

該第２の通信部が、該第３のハッシュ値が該第４のハッシュ値に等しいことを検証するステップと

をさらに包含する、請求項２に記載の方法。

【請求項４】

前記第１のハッシュ値および前記第２のハッシュ値は、それぞれ、h_k（Ｙ‖Ｘ‖Id_A）の形態であり、前記第３のハッシュ値および前記第４のハッシュ値は、それぞれ、h_k（Ｘ‖Ｙ‖Id_B）の形態であり、ｈは前記鍵付きハッシュ関数であり、Id_Aは、前記第１の通信部および前記第２の通信部のうちの前記一方の前記識別情報であり、Id_Bは、該第１の通信部および該第２の通信部のうちの前記もう一方の前記識別情報である、請求項３に記載の方法。

【請求項５】

前記第１の値Ｘは、前記第１の通信部によって生成されたランダムな整数であり、前記第２の値Ｙは、前記第２の通信部によって生成されたランダムな整数である、請求項１～４のいずれかに記載の方法。

【請求項６】

前記鍵付き暗号関数は別の鍵付きハッシュ関数である、請求項１～５のいずれかに記載の方法。

【請求項７】

前記鍵付き暗号関数は前記鍵付きハッシュ関数である、請求項１～５のいずれかに記載の方法。

【請求項８】

前記共有鍵ｋは、h_k（Ｘ‖Ｙ）の形態である、請求項６または７に記載の方法。

【請求項９】
データ通信システムにおける第１の通信部と第２の通信部との間での対称鍵の合意の方法であって、該第１の通信部および該第２の通信部は、それぞれ、マスター鍵Ｋを有し、該方法は、
該第１の通信部が、第１の値Ｘを生成し、該第１の値Ｘを該第２の通信部に提供するステップと、
該第１の通信部が、該第２の通信部によって生成された第２の値Ｙを取得するステップと、
該第１の通信部が、該第１の値Ｘと該第２の値Ｙとの組み合わせにおいて鍵付き暗号関数を作用させることによって、共有鍵ｋを計算するステップであって、該第１の通信部は、該マスター鍵Ｋを、該鍵付き暗号関数に対する入力として用い、該第１の通信部により計算された該共有鍵ｋは、鍵付きハッシュ関数に対する入力として用いられ、該鍵付きハッシュ関数は、該第１の値Ｘ、該第２の値Ｙ、ならびに該第１の通信部および該第２の通信部のうちの一方の識別情報の組み合わせにおいて作用させるためのものであり、該共有鍵ｋは、また、該マスター鍵Ｋを該鍵付き暗号関数に対する入力として用いることによって、該第１の値Ｘおよび該第２の値Ｙの該組み合わせにおいて、該第２の通信部が該鍵付き暗号関数を作用させることによって、該第２の通信部によって計算可能であり、該第２の通信部により計算可能な該共有鍵ｋは、また、該鍵付きハッシュ関数に対する入力として該第２の通信部によって用いることが可能である、ステップと
を包含する、方法。
【請求項１０】
前記第１の通信部が、前記第２の通信部から第１のハッシュ値を受信するステップであって、該第１のハッシュ値は、該第２の通信部が、該第２の通信部により計算された前記共有鍵ｋを用いて、前記第１の値Ｘ、前記第２の値Ｙ、ならびに前記第１の通信部および該第２の通信部のうちの一方の識別情報の組み合わせに前記鍵付きハッシュ関数を適用することによって、該第２の通信部により計算される、ステップと、
該第１の通信部が、第２のハッシュ値を生成するために、該第１の値Ｘ、該第２の値Ｙ、ならびに該第１の通信部および該第２の通信部のうちの該一方の該識別情報の組み合わせに、該鍵付きハッシュ関数を適用するステップであって、該第１の通信部は、該第１の通信部によって計算された該共有鍵ｋを、該鍵付きハッシュ関数に対する入力として用いる、ステップと、
該第１の通信部が、該第１のハッシュ値が該第２のハッシュ値に等しいことを検証するステップと
をさらに包含する、請求項９に記載の方法。
【請求項１１】
前記第１の通信部が、第３のハッシュ値を生成するために、前記第１の値Ｘ、前記第２の値Ｙ、ならびに該第１の通信部および前記第２の通信部のうちのもう一方の識別情報の組み合わせに、前記鍵付きハッシュ関数を適用するステップであって、該第１の通信部は、該第１の通信部によって計算された前記共有鍵ｋを、該鍵付きハッシュ関数に対する入力として用いる、ステップと、
該第１の通信部が、検証のために該第３のハッシュ値を該第２の通信部に提供するステップであって、これにより、該第２の通信部は、第４のハッシュ値を生成するために該第２の通信部により計算された該共有鍵ｋを用いて、該第１の値Ｘ、該第２の値Ｙ、ならびに該第１の通信部および前記第２の通信部のうちの該もう一方の該識別情報の組み合わせに、該鍵付きハッシュ関数を適用することによって、該第３のハッシュ値を検証し、次いで、該第３のハッシュ値が該第４のハッシュ値に等しいことを検証することが可能である、ステップと
をさらに包含する、請求項１０に記載の方法。
【請求項１２】
前記第２のハッシュ値は、h_k（Ｙ‖Ｘ‖Id_A）の形態であり、前記第３のハッシュ

値は、h_k（Ｘ‖Ｙ‖Id_B）の形態であり、ｈは前記鍵付きハッシュ関数であり、Id_Aは、前記第１の通信部および前記第２の通信部のうちの前記一方の前記識別情報であり、Id_Bは、該第１の通信部および該第２の通信部のうちの前記もう一方の前記識別情報である、請求項１１に記載の方法。

【請求項１３】

前記第１の値Ｘは、前記第１の通信部によって生成されたランダムな整数である、請求項９～１２のいずれかに記載の方法。

【請求項１４】

前記鍵付き暗号関数は別の鍵付きハッシュ関数である、請求項９～１３のいずれかに記載の方法。

【請求項１５】

前記鍵付き暗号関数は前記鍵付きハッシュ関数である、請求項９～１３のいずれかに記載の方法。

【請求項１６】

前記共有鍵ｋは、h_k（Ｘ‖Ｙ）の形態である、請求項１４または１５に記載の方法。

【請求項１７】

前記鍵付きハッシュ関数は暗号ハッシュ関数である、請求項１～１６のいずれかに記載の方法。

【請求項１８】

第１の通信部と第２の通信部とを含むシステムであって、該第１の通信部と該第２の通信部とは、共に、請求項１～８のいずれかに記載の方法を実行するように構成されている、システム。

【請求項１９】

請求項９～１６のいずれかに記載の方法を実行するように構成されている暗号ユニットを有する通信部。

【請求項２０】

請求項９～１６のいずれかに記載の方法を実行する複数のコンピュータ読み取り可能命令を格納したコンピュータ読み取り可能媒体。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は暗号鍵の移送および認証用の鍵合意（共有）プロトコルに関する。

【背景技術】

【０００２】

情報交換中にプライバシーを保護するために、鍵を使用して、データを暗号化することは良く知られている。鍵は通信者がメッセージを暗号化し復号できるようなものであって、横取りする人がメッセージのコンテンツを決定することができないようなものを選ばなければならない。

【０００３】

秘密鍵の暗号のプロトコルでは、通信者は、それらに秘密の共通鍵を共有する。これは通信者間で鍵を合意（即ち共有）しておく必要があり、また、鍵の秘密を保持するための設備も必要であり、基礎をなすセキュリティが危険にさらされた場合には鍵の変更をもたらすものである。

【０００４】

公開鍵暗号のプロトコルは、Diffie-Hellmanによって1976年に最初に提案されたものであって、潜在的な全ての通信者に利用可能になった公開鍵、および、意図した受信者にのみ知らされる秘密鍵を利用するものである。公開鍵と秘密（私用）鍵は、受信者の公開鍵で暗号化されたメッセージが、平文、暗号テキストおよび公開鍵についての知識で導出できないような秘密鍵で容易に解読することができる、ことに関するものである。

【０００５】

鍵の確立は、2つの(あるいはより多くの)関係者がセッション鍵と呼ばれる共有の秘密鍵を確立するプロセスである。続いてセッション鍵がプライバシーのようなある暗号のゴールを達成するために使用される。以下の2種類の鍵合意（共有）プロトコルがある。

・鍵が一方の当事者によって作成され、安全に第二の当事者に送信される鍵移送プロトコル。

・共有秘密鍵を一緒に確立するような情報を双方の当事者が与える鍵合意（共有）プロトコル。

当事者間で要求されるメッセージ交換の数は、パスの数と呼ばれる。鍵確立プロトコルでは、具体的に識別された第二当事者から他の相手方がセッション鍵の値を知ることが無いことを一方の当事者が保証される場合には、暗黙の鍵認証（あるいは単に鍵認証）を提供すると考えられる。暗黙の鍵認証の性質は、第二当事者が実際にセッション鍵を所有することを必ずしも意味しない。鍵確立プロトコルでは、具体的に識別された第二当事者が特別のセッション鍵を実際に所有していることを一方の当事者が保証された場合には、鍵の確認をもたらすものであると考えられる。認証がプロトコルに関連する両当事者に供給される場合は、鍵認証は相互のものであると考えられ、ただ１つの当事者に供給される場合には、認証は一方的であると考えられる。

【０００６】

暗黙の鍵認証を提供することを主張する様々な従来提案がある。

【０００７】

例えば、鍵合意（共有）のためのNyberg-Rueppelの1パスプロトコル、および、マツモトータカシマーイマイ(MTI)およびGossおよびYacobiの２パスプロトコルがある。

【０００８】

従来の提案は、共通鍵を確立する通信者間の伝送が安全で、中途介在者がセッション鍵を取得することができず、暗号文を解読することができないことを保証する。このようにして、資金移動のようなセンシティブなトランザクション（取引）のためのセキュリティ（安全）が提供される。

【０００９】

例えば、MTI/AO鍵合意プロトコルは、次の方法で、2つの通信者に知られていた共有秘密鍵Kを確立、即ち設定する。

1. 最初、即ち、一度だけのセットアップのときに、鍵生成および公開が、確実性を保証するやり方で適切な系(system)の素数(prime)pおよび生成元(generator)

$$\alpha \in Z_p^*$$

を選択し公表することにより行われる。通信者Aは、長期的な秘密鍵として、ランダム（無作為）な整数「a」（但し、$1 \leqq a \leqq p-2$）を選択し、長期的な公開鍵$Z_A = \alpha^a \mod p$を計算する。Ｂは同様の鍵b、z_Bを生成する。ＡとＢは互いの長期的な公開鍵の認証されたコピーにそれぞれアクセスする。

【００１０】

2.プロトコルは、次のメッセージの交換を要求する。

$$A \rightarrow B : \alpha^x \mod p \quad (1)$$

$$A \leftarrow B : \alpha^y \mod p \quad (2)$$

xとyの値は、もちろんｐが十分に大きなものが選択されるという前提であるが、指数やαの値の値が知られた場合でさえも、指数を決定することが非実用的であるような伝送の間は安全な状態にされる。

【００１１】

3.プロトコルを実施するために、共有鍵が必要とされる度に、次のステップが行なわれる。

(a)Ａは無作為の整数x（但し$1 \leqq x \leqq p-2$）を選択し、Ｂにメッセージ(1)、即ち、$\alpha^x \mod p$を送る。

(b)Ｂは無作為の整数y（但しl≦y≦p-2）を選択し、Ａにメッセージ(2)、即ち、$\alpha^{y} \mod p$を送る。
(c)Aは鍵K=$(\alpha^{y})^{a} z_B^{X} \mod p$を計算する。
(d)Ｂは鍵K=$(\alpha^{x})^{b} z_B^{y} \mod p$を計算する。
(e)両方が、鍵$K-\alpha^{bx+ay}$を共有する。

【００１２】

鍵Kを計算するために、Aは自分の秘密鍵aおよび無作為（ランダム）の整数ｘを使用しなければならず、そして、それらの両方はＡにのみに知られている。同様に、Bは、セッション鍵Kを計算するために自分の秘密鍵bおよび無作為の整数yを使用しなければならない。秘密鍵a、ｂが危険にさらされず安全なものであるという前提で、中途介在者は他の通信者と同一のセッション鍵を生成することができない。従って、どんな暗号テキストも両方の通信者によって判読可能になることはない。

【発明の概要】

【発明が解決しようとする課題】

【００１３】

上記および関連するプロトコルは、鍵確立に十分で従来の盗聴者あるいは途中に介在する者の攻撃に強い、と考えられていた。

【００１４】

いくつかの状況では、敵が、第２の通信者の真実の同一性に関して1つの通信者を誤解させることが有利かもしれない。

【００１５】

そのような攻撃では、活動的な敵、即ち、途中介在者（interloper）Eは、AとBの間で交換されるメッセージを修正すると、その結果として、Bは、彼がEと鍵Kを共有すると信じ、一方で、AがBと同じ鍵Kを共有すると信じる。たとえＥがＫの値を知らないとしても、通信者の同一性に関する偽の情報は有用となり得る。

【００１６】

そのような攻撃が成功裡に始められるかもしれない場合、実際的なシナリオは下記である。Bが銀行支店で、Aが口座所有者である、と仮定する。証明書は銀行本部によって出され、証明書内には、所有者の口座情報がある。資金の電子預金用のプロトコルは、相互に認証された鍵合意によって銀行支店で鍵を交換することであると仮定する。一旦Bが送信するものを認証したならば、暗号化された資金は証明書にある口座番号に預け入れられる。それ以上、認証が、暗号化された預金メッセージ（帯域幅を保存するその場合かもしれない）中でそのとき行われなければ、預金はEの口座に為されるだろう。

【００１７】

従って、上記の損失が除去される、或いは軽減されるプロトコルを提供することが本発明の目的である。

【課題を解決するための手段】

【００１８】

よって、本発明によれば、通信者A，Ｂの組の間で認証する方法であって、その間で情報の交換を可能にする方法であり、前記通信者の各々は、それぞれの秘密鍵ａ，ｂと、これらの秘密鍵の各々と生成元（器）（generator）αから得られる公開鍵p^{A}とp^{B}とを持ち、下記のステップを含む方法が提供される。

i)はじめに第１の通信者が、第１の無作為の整数xを選択し、前記生成元を含む関数$f(\alpha)$を指数$g^{(x)}$でべき乗して、第１の（べき乗された）指数関数$f(\alpha)^{g^{(x)}}$を提供するステップ。

ii)前記第1の通信者Aが、前記第１の指数関数$f(\alpha)^{g^{(x)}}$を含むメッセージを第２の通信者Bへ移送するステップ。

iii)前記通信者Bが、第２の無作為の整数ｙを選択し、前記生成元を含む関数$f(\alpha)$を指数$g^{(y)}$でべき乗して、第２の（べき乗された）指数関数$f(\alpha)^{g^{(y)}}$を提供するステップ。

iv)前記第２の通信者Bが、前記第１の通信者Aによって公開された情報と、前記第２の通信者Bの秘密（即ちＢだけが知る私用）の情報とからセッション鍵Kを構築するステップであり、また、このセッション鍵が、前記第１の通信者Aによっても、Ｂによって公開された情報と、前記第１の通信者Aの秘密の情報のために構築されるステップ。
v)前記第2の通信者Bが、関数

F[ð, K]

の値hを生成するステップ（但し、関数

F[ð, K]

は

ð

とKとを共に用いた暗号関数であり、

ð

はＢによって与えられた公開情報のサブセット、即ち部分集合であり、これによって

ð

とKの値を結びつける）。
vi)前記第２の通信者Bが、前記第１の通信者Aに、前記第２の指数関数f(α)ｇ（ｙ）と、関数

F[ð, K]

の値hとをを含むメッセージを移送するステップ。
vii)前記第1の通信者が、前記メッセージを受取り、前記第１の通信者の秘密と、前記第２の通信者Bによって公開されたものによる情報からセッション鍵K’を計算するステップ。
viii)前記第1の通信者Aが、暗号関数

h,h’ F[ð, K]

の値h’を計算するステップ。
ix)これらの通信を検証（即ち、認証）するために、前記暗号関数Fから得られた前記値を比較するステップ。
【００１９】
セッション鍵Kが、ＡかBのいずれかに秘密の情報を使ってのみ生成させることができるため、Ｋを

ð

と暗号関数hとに結合することによって、ＥがＫを抽出すること、或いは、Ａによって得られるものと一致させるような新たな値の関数を差し挟むことを防止する。
本発明は、例えば、以下を提供する。

（項目１）
　データ通信システムで第１および第２の通信者を認証する方法において、
a)前記第１の通信者が、第１の値G_Aを生成し、前記第１の値を前記第２の通信者に送出するステップと、
b)前記第２の通信者が、第２の値G_Bを生成するステップと、
c)前記通信者が各々、共有鍵Kを得るステップと、
d)前記第２の通信者が、前記第１の通信者の識別情報および前記第１および第２の値の第１の鍵付きハッシュを計算するステップであって、前記第１の鍵付きハッシュが前記共有鍵Kを使用するステップと、
e)前記第2の通信者が、前記第1の鍵付きハッシュ、前記識別情報、および前記第２の値を、前記第１の通信者に送出するステップと、
f)前記第１の通信者が、前記第１の通信者の識別情報、および前記第１および第２の値の第１の検証鍵付きハッシュを計算するステップであって、前記第１の検証鍵付きハッシュが前記共有鍵Kを使用するステップと、
g)前記第１の通信者が、前記第1の鍵付きハッシュが前記第１の検証鍵付きハッシュと同じであることを検証するステップと、
を含む方法。
（項目２）
　項目１に記載の方法において、
h)前記第１の通信者が、前記第２の通信者の識別情報、および、前記第１および第２の値の第２の鍵付きハッシュを計算するステップであって、前記第2の鍵付きハッシュが前記共有鍵Kを使用するステップと、
i)前記第１の通信者が、前記第２の通信者の前記識別情報および前記第2の鍵付きハッシュを前記第2の通信者に送出するステップと、
j)前記第2の通信者が、前記第２の通信者の識別情報および前記第１および第２の値の第２の検証鍵付きハッシュを計算するステップであって、前記第2の鍵付きハッシュが前記共有鍵Kを使用するステップと、
k)前記第2の通信者が、前記第２の検証鍵付きハッシュが前記第２の鍵付きハッシュと同じであるかを検証するステップと、
をさらに含むことを特徴とする方法。
（項目３）
　データ通信システムで第１の通信者と第２の通信者との間で認証された鍵の合意の方法であって、前記通信者の各々は公開鍵暗号システムにおける公開鍵と秘密鍵とのペアを有し、前記方法が、
a)前記第１の通信者が、第１の値G_Aを生成し、この第１の値を前記第2の通信者に送出するステップと、
b)前記第2の通信者が、第２の値G_Bを生成するステップと、
c)前記通信者の各々は、自分だけの秘密である情報および他の通信者に公開されている情報から共有鍵Kを計算するステップと、
d)前記第2の通信者が、前記第1の通信者の識別情報および前記第１および第２の値の第１の鍵付きハッシュを計算するステップであって、前記鍵付きハッシュが前記共有鍵Kを使用するステップと、
e)前記2の通信者が、前記第1の鍵付きハッシュ、前記識別情報、および、前記第２の値を前記第１の通信者に送出するステップと、
f）前記第1の通信者が、前記第１の通信者の識別情報、前記第１および第２の値の第１の検証鍵付きハッシュを計算するステップであって、前記検証鍵付きハッシュが前記共有鍵Ｋを使用するステップと、
g)前記第１の通信者が、前記第１の鍵付きハッシュが前記第１の検証鍵付きハッシュと同じであるかを検証するステップと、
を含む方法。

（項目４）
項目１に記載の方法において、
h)前記第１の通信者が、前記第２の通信者の識別情報、前記第1および第2の値の第２の鍵付きハッシュを計算するステップであって、前記第2の鍵付きハッシュが前記共有鍵Kを使用するステップと、
i)前記第１の通信者が、前記第2の鍵付きハッシュ、および、前記第2の通信者の識別情報を前記第２の通信者に送出するステップと、
j)前記第2の通信者が、前記第２の通信者の識別情報、および、前記第1および第2の値の第2の検証鍵付きハッシュを計算するステップであって、前記第２の鍵付きハッシュが共有鍵Kを使用するステップと、
k)前記第2の通信者が、前記第2の検証鍵付きハッシュが前記第２の鍵付きハッシュと同じであるかを検証するステップと、
をさらに含むことを特徴とする方法。
（項目５）
項目１，２，３，４のいずれか１項に記載の方法を実装する暗号ユニット。
【図面の簡単な説明】
【００２０】
発明の実施例は、付属の図面を参照して説明するが、これらの図面は例示に過ぎない。
【図１】図1はデータ通信システムの説明図である。
【図２】図2－図8は種々のプロトコルの実装の説明図である。
【図３】図2－図8は種々のプロトコルの実装の説明図である。
【図４】図2－図8は種々のプロトコルの実装の説明図である。
【図５】図2－図8は種々のプロトコルの実装の説明図である。
【図６】図2－図8は種々のプロトコルの実装の説明図である。
【図７】図2－図8は種々のプロトコルの実装の説明図である。
【図８】図2－図8は種々のプロトコルの実装の説明図である。
【発明を実施するための形態】
【００２１】
したがって、図1を参照すると、通信者A(10)、通信者B(12)のペアは、通信チャネル14を介して情報を交換する。暗号ユニット16および18は、通信者10、12の各々と、チャネル14との間に置かれる。鍵20は、各ユニット16,18とそれぞれの通信者10,12との間で運ばれる平文を変換して、チャネル１４で運ばれる暗号文にするために、暗号ユニット16および18の各々に関連付けられる。
【００２２】
操作においては、通信者A(10)によって生成されたメッセージは、鍵20を備えたユニット16によって暗号化され、ユニット18にチャネル14上、暗号テキスト（暗文）として送信される。
【００２３】
鍵20はユニット18の暗号テキストを操作して、通信者B(12)のために平文メッセージを生成する。鍵20が通信者に与えられている場合には、通信者12が受け取ったメッセージは通信者10によって送られたものに変換される。
【００２４】
図1で示したシステムが作動するためには、それぞれの鍵20は同一のもにする必要があり、したがって、同一の鍵を確立するたに、公開された方法で情報の移送を可能にする鍵合意（共有）プロトコルは確立される。その実装を、図2－図7に図解で示す。
【００２５】
図2を参照して、相互公開鍵・認証鍵合意プロトコルは、図の左側に示された、通信者Aと、右側に示された通信者Bの間で補間しあうものである。通信者Aは、公開－秘密（私用）鍵のペア、P_A、S_Aををそれぞれ持ち、同様に通信者Bは、公開－秘密（私用）鍵のペア、P_B、S_Bををそれぞれ持つ。

【００２６】
最初に、通信者Aは乱数RND_Aとしてセッション秘密鍵を生成し、対応する公開セッション鍵$G_A=F(RND_A)$を計算する。関数F_Aは、暗号の一方向性関数であり、典型的には、楕円暗号系のポイント乗算(point multiplication)のような集合の生成元（器）による指数(exponetion)である。
【００２７】
公開セッション鍵G_Aは、セッション秘密鍵RND_Bおよび公開セッション鍵G_Bの対応するパラメーターを生成する通信者Bへ移送される。
【００２８】
通信者Bは、Ａの公開情報G_A、P_Aと、,Bの秘密情報RND_B、S_Bの関数としてセッション鍵Kを計算する。対応する鍵K'は、Aの秘密（プライベート）情報およびBの公開情報(すなわち$f(RND_A、G_B、S_A、P_B)$の公開情報を使用して、Aによって計算することができる。
【００２９】
通信者Bが鍵Kを生成した後、彼はストリング（文字列）$(G^A \| G_B \| Id_A)$をコンパイル(compile)、即ち１つにまとめるが、ここで、Id_AはＡを識別するストリングである。この連結されたストリングは、ストリング$hash_B$を生成するために鍵Kを使用する、鍵付きハッシュ関数である暗号関数h_kでハッシュされる。
【００３０】
ストリング$hash_B$はId_AとG_Bと共に通信者Ａに移送される。
【００３１】
Bからのメッセージを受けて、通信者Aは、上述したように鍵K'を計算する。通信者Aは、さらに、鍵K'による鍵が付いたハッシュ関数を使用して、ストリング$(G_B//G_A//Id_A)$からハッシュ$hashverifiy_B$を計算する。通信者Aは、ハッシュを検証して鍵K、K'の同一性が確認（証明）できるかどうかを検査する。
【００３２】
その後、通信者Aは、ストリング$(G_A//G_B//Id_B)$において鍵K'を使用して、ハッシュ$h_{K'}$を計算し、通信者BのId_Bと一緒のそれを移送する。同様に、通信者Ｂは、同じストリング上で、鍵Kを使用する鍵付きハッシュ関数h_Kを使用して、$hashverify_A$を計算し、$hash_A=hashverifiy_A$であるかを検証する。
【００３３】
図３に相互の実体認証プロトコルを実装するための同様のプロトコルを示す。このプロトコルでは、通信者は、安全なチャネルを介して得られた鍵Kを共有する。通信者A、Bは、各々、AとBのセッション公開鍵としてそれぞれ使用される無作為（ランダムな）の整数を生成する。その後、鍵付きハッシュ関数で利用されている共有秘密鍵と共に図2に示したように、情報交換と検証が進む。
【００３４】
十分な相互公開鍵・認証鍵交換プロトコルを図4に示す。信頼を認証されたチャネルを介した公開鍵P_A、P_Bの最初の交換が行われた後に、図4のプロトコル中で示されるような情報交換が続く。この場合、通信者Ａは、ＡがＢによる受信を確認することと所望するストリングx_2と一緒に、図2を参照して説明したように計算されたG_Aを送信する。通信者Ｂは図2のような鍵Kを計算し、ペアのストリングy_1,y_2を生成するが、これらのストリングは、Ｂが、Ａによって認証されること、および、Ａによって受信されたことを確認（検証）することを所望するものである。これらのストリングは、ハッシュ$hash_B$と識別情報Id_Aと共に、Ａに送信される。ハッシュ$hash_B$は、認証されるべきストリングy_1とメッセージx_2とを含むストリング上で実施される。
【００３５】
通信者Aは鍵Kを計算し、ハッシュが前のものと同じであるか検証する。これは、また、Bによるx_2の受領を確認（検証）する。
【００３６】
通信者Aは、次に、ストリングz_1,z_2を生成し、ここで、z_1は、ＡがＢによって認証され

ることを所望するようなストリング（文字列）であり、z_2は、後で述べるプロトコルの後続の実行によって使用することができるようなストリングである。Bの識別情報Id_Bと一緒のストリングz_1およびy_2は、ストリング$hash_A$を提供するために鍵Kでハッシュされるストリングに含まれている。これは、ストリングz_1,z_2およびBの識別情報と共に、ハッシュが前のものであるのかを検証するものである通信者Bに送信され、これによって、通信者Aによる、z_1の認証およびy_2の受信を確認する。

【００３７】

したがって、情報は、認証された仕組みで交換され、得られた共通鍵は、安全なチャネル上での後続の通信の交換を可能にする。

【００３８】

図4で説明したプロトコルを用いて、ストリングx_2、y_1、y_2、z_1、z_2をすべて空のストリング（文字列）にすることによって、相互公開鍵認証鍵合意（共有）プロトコルを実装することが可能である。あるいは、暗黙の鍵を用いて相互公開鍵・認証鍵合意プロトコルを、kの値を鍵Kと共に暗号関数Eに適用した結果である$E_K(k)$を表わすと仮定されるストリングとしてx_2を使用することによって実装することができる。通信者Bは、Kの値を計算することができ、よって、ストリングからkの名目上（即ち理論上）の値が取り出される。彼は、通信者Aと共に共有セッション鍵としてこれを使用することができる。y_1の値は、$E_K(k_{12})$としてのz_1および$E_K(k_{21})$を表わすために使用することができ、ここでk_{12}、k_{21}は、通信のための異なる鍵、即ち、通信者間で共有される他の秘密情報である。この場合、y_2、Z_2とが空のストリング（文字列）である。このように、通信者の間における鍵k21およびkl2の認証された鍵輸送と一緒に共有鍵K_{AB}についての鍵合意、および、kについての認証された鍵合意がなされる。さらに、追加情報がそのときストリングx_2,y_2で提供される場合、適正な受信の確認も得られる。

【００３９】

図4のプロトコルも、次のセッションの第１のパス中で交換される情報を渡すためにストリングz_2を使用することにより、連続セッションの効率を増加させるために使用することもできる。したがって、図5で示すように、ストリングG_A、x_2は、前のセッションのz_2として送られる。その後、以前のように、プロトコルは通信者Bから進行する。図5で見られるように、3番目の伝送は任意に省略することができる。通信者Bは、さらに、y_2として交換に次のセッションのため情報G_B、y_1を含めることによりこの機能の利点を利用することもできる。

【００４０】

相互公開鍵認証鍵合意プロトコルも、図6で示すような実体認証実装(entity authentication implementation)に適応することができる。この場合、図3でのように、通信者が安全なチャネル上で共有鍵を得たものであるとして、鍵生成が省略される。

【００４１】

同様に、図5のそれと同様に、前のセッションにおける情報交換を利用するために図7で例示するように、図6のプロトコルを修正することもできる。

【００４２】

従って、特別のニーズを満たすために一般的なプロトコルから多くの汎用で柔軟なプロトコルを開発し得ることがわかる。これらのプロトコルは、楕円曲線暗号手法を実装する、即ち、Z_pで操作することができるようにすることが好適である。

【００４３】

図３に示した公開鍵認証鍵合意プロトコルのメッセージフローと、図２で示した実体認証プロトコルのものとは同一の構造を持っていることが、容易に分るであろう。さらに、それの検証と同様に、通信者AおよびBによるハッシュ値$hash_A$および$hash_B$の計算も、それぞれ入力として同一の構造のストリングをとる。実際、両方のプロトコルは、プロトコルの中で使用される鍵Kを導出する方法だけにおいて異なる。したがって、両方のプロトコルを結合した実装は、メッセージ送受信、エラー処理、同様のものを含む通信フローの共通の取り扱いという利点を得ることができ、また鍵検証ステップ(即ちハッシュ値の生成

および処理)の共通の取り扱いの利点を利用することもできる。

【００４４】

同様の論法は、は、図4で示した公開鍵認証鍵合意プロトコルの公開鍵の処理ステップ、および、メッセージフロー、および図５に示したそれらのものの形式に適用できる。前者の一部だけの実行から、後者のものが形成されることが認識されるだろう。図4で示した公開鍵認証鍵合意プロトコルを用いて、図３に示したものを実装、即ち実行することができ、そして同様に、図6で示した拡張された実体認証プロトコルを用いて、図２に示したものを実装、即ち実行することができることに注意されたい。したがって、説明したプロトコルはすべて、これらプロトコルの全ておよび各々のプロトコルステップの実装（実行）のほとんど共通で通信（テレコミュニケーション）とメッセージフローを扱うための大規模な共通ルーチンで実装（実施）することができる

【００４５】

本発明は、公開鍵ベースの合意プロトコルおよび実体認証プロトコルに言及しながら記述したが、それが対称な鍵合意プロトコル上で等しく利用することができることが認識されるであろう。そのような実施態様では、共有鍵Kの計算は、鍵付きハッシュ関数への1つの入力としてマスター鍵k_mを使用して行なうことができる。暫定の鍵G_AとG_Bとの結合は別の入力として使用され、結果として生じる出力は共有鍵Kとして使用される。そのような構成は図８に示してある。

【図１】

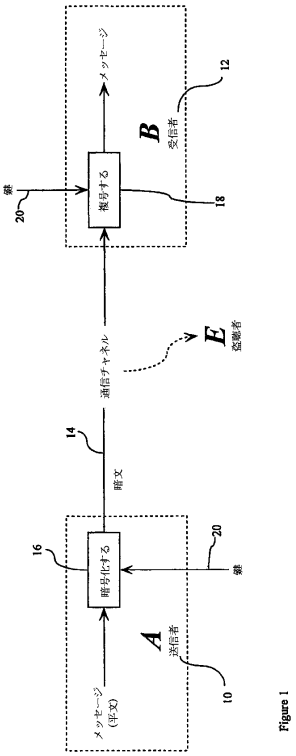

Figure 1

【図２】

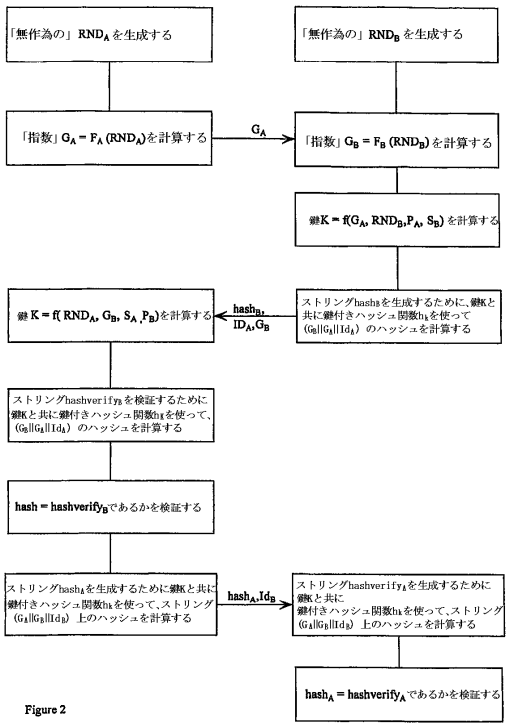

Figure 2

【図３】

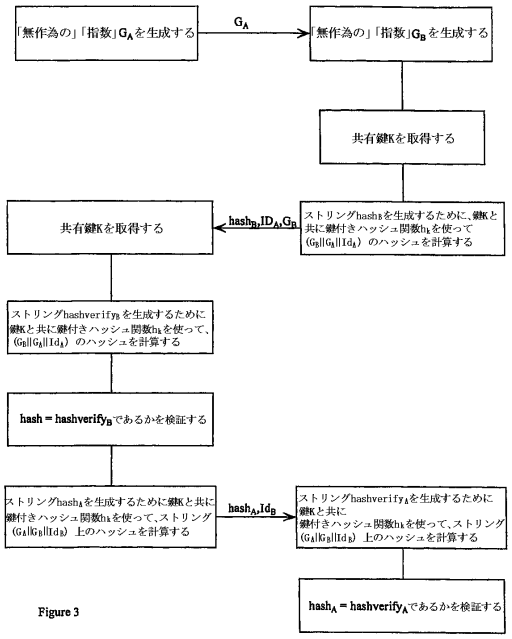

Figure 3

【図４】

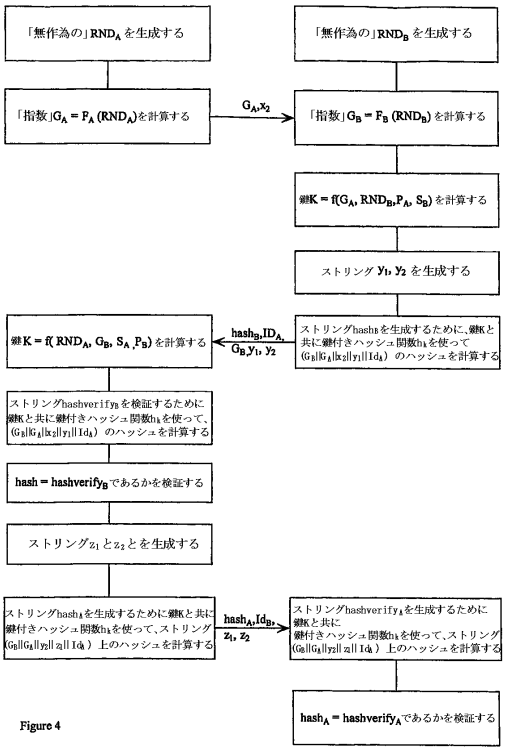

Figure 4

【図５】

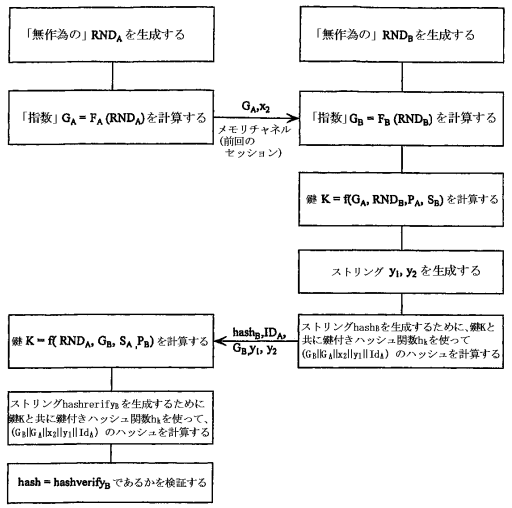

Figure 5

【図６】

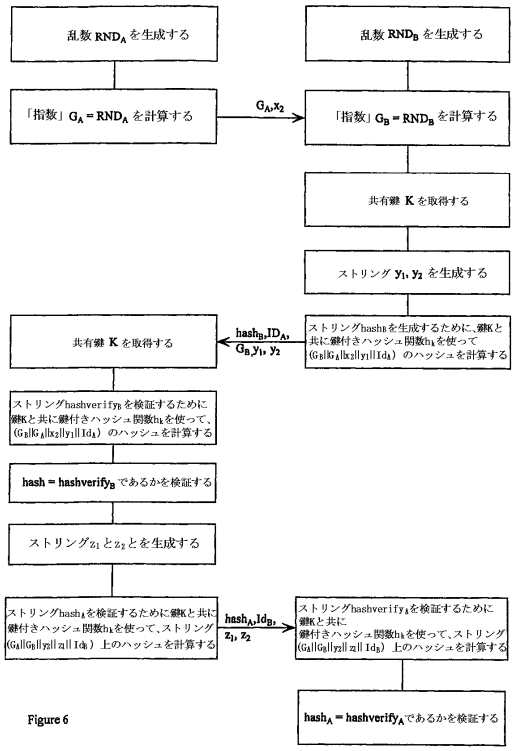

Figure 6

【図７】

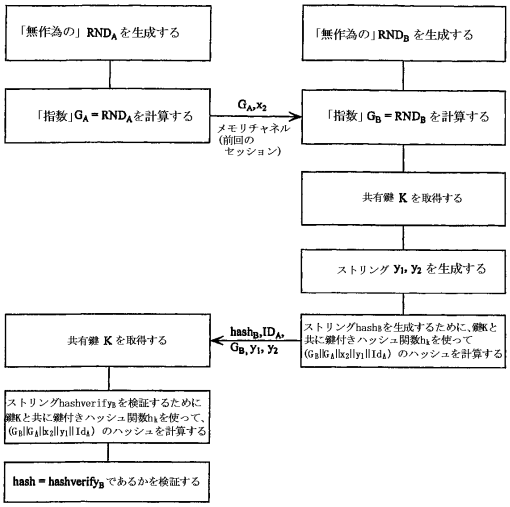

Figure 7

【図８】

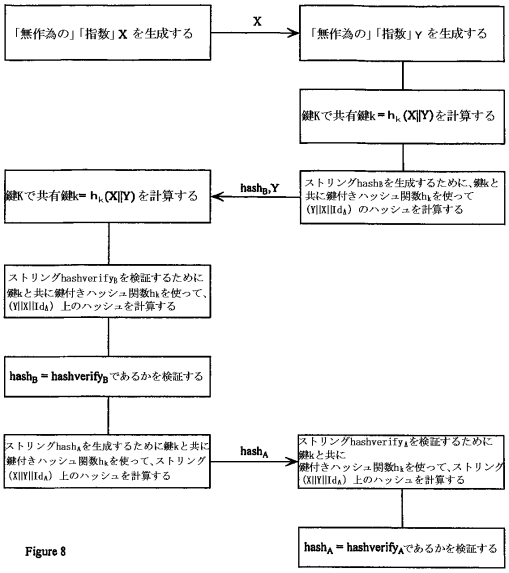

Figure 8

フロントページの続き

(56)参考文献 特開２００１－３１３６３４（ＪＰ，Ａ）
特開２００２－３３５２３８（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ　　９／０８
Ｈ０４Ｌ　　９／３２
ＪＳＴＰｌｕｓ／ＪＭＥＤＰｌｕｓ／ＪＳＴ７５８０（ＪＤｒｅａｍＩＩ）