(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第4384728号
(P4384728)
(45)発行日　平成21年12月16日(2009.12.16)　(24)登録日　平成21年10月2日(2009.10.2)

(51)Int.Cl.　F I
H04L 9/08 (2006.01)　H04L 9/00 601D
H04L 9/00 601E

請求項の数 11　(全 13 頁)

(21)出願番号	特願平10-519298
(86)(22)出願日	平成8年10月18日(1996.10.18)
(65)公表番号	特表2000-502553(P2000-502553A)
(43)公表日	平成12年2月29日(2000.2.29)
(86)国際出願番号	PCT/US1996/016608
(87)国際公開番号	WO1998/018234
(87)国際公開日	平成10年4月30日(1998.4.30)
審査請求日	平成15年10月20日(2003.10.20)
審判番号	不服2007-18363(P2007-18363/J1)
審判請求日	平成19年7月2日(2007.7.2)

(73)特許権者　397071791
サーティコム　コーポレーション
カナダ国　オンタリオ　エル４ダブリュー　５エル１，ミシソーガ，エクスプローラー・ドライブ　５５２０，フォース・フロア
(74)代理人　100089705
弁理士　社本　一夫
(74)代理人　100140109
弁理士　小野　新次郎
(74)代理人　100075270
弁理士　小林　泰
(74)代理人　100080137
弁理士　千葉　昭男

最終頁に続く

(54)【発明の名称】内在的署名を用いた鍵一致及び輸送プロトコル

(57)【特許請求の範囲】

【請求項１】

公開鍵暗号化を採用しているデータ通信システムにおいて、通信チャネル（１４）を介して第１及び第２の通信端末（Ａ及びＢ）の間で情報を交換することを可能にするために、第１及び第２の通信端末間の鍵を設定する方法であって、第１の通信端末は、第１の秘密鍵ａと、生成元α及び該秘密鍵から導かれた第１の公開鍵p_Aと、を有しており、第２の通信端末は、第２の秘密鍵ｂと、生成元α及び該秘密鍵から導かれた第２の公開鍵p_Bと、を有しており、該方法は、

ｉ）第１の通信端末（Ａ）において、第１のランダム整数ｘを選択して、該第１のランダム整数ｘを含む関数ｇ（ｘ）を、生成元αを含む第１の関数ｆ（α）のベキとする指数関数を作ることにより、第１の指数関数$f(\alpha)^{g(x)}$を提供するステップと、

ｉｉ）第１の通信端末（Ａ）において、第１のランダム整数ｘ、第１の指数関数$f(\alpha)^{g(x)}$、及び第１の秘密鍵ａから、第１のランダム整数ｘと第１の秘密鍵ａとを組み合わせるために、第１の署名s_Aを生成するステップと、

ｉｉｉ）第１の通信端末（Ａ）から、第２の通信端末（Ｂ）に、第１の指数関数$f(\alpha)^{g(x)}$を含むメッセージを送るステップと、

ｉｖ）第２の通信端末（Ｂ）において、第２のランダム整数ｙを選択して、該第２のランダム整数ｙを含む関数ｇ（ｙ）を、生成元αを含む第２の関数ｆ’（α）のベキとする指数関数を作ることにより、第２の指数関数$f'(\alpha)^{g(y)}$を提供し、第２のランダム整数ｙ、第２の指数関数$f'(\alpha)^{g(y)}$、及び第２の秘密鍵ｂから、第２のランダム整数ｙと

第２の秘密鍵ｂとを組み合わせるために、第２の署名s_Bを生成するステップと、
ｖ）第２の通信端末（Ｂ）から、第１の通信端末（Ａ）に、第２の指数関数$f'(\alpha)^{g(y)}$を含むメッセージを送るステップと、
ｖｉ）第１の通信端末（Ａ）において、第２の通信端末（Ｂ）によって公開された情報を、第１の通信端末に属する秘密情報により累乗することによって、セッション鍵Ｋを構築し、第２の通信端末（Ｂ）において、第１の通信端末（Ａ）によって公開された情報を、第２の通信端末に属する秘密情報により累乗することによって、セッション鍵Ｋを構築するステップであって、第１の通信端末（Ａ）においては第１の署名s_A及び第２の署名s_Bの一方用い、第２の通信端末（Ｂ）においてはこれら署名の他方を用いる、ステップとからなることを特徴とする方法。

【請求項２】
請求項１記載の方法において、第１の通信端末（Ａ）によって送られるメッセージは、該第１の通信端末のアイデンティフィケーション（ＩＤ）を含み、第２の通信端末（Ｂ）によって送られるメッセージは、該第２の通信端末のＩＤを含んでいることを特徴とする方法。

【請求項３】
請求項１又は２記載の方法において、生成元αを含む第１の関数ｆ（α）及び第２の関数ｆ’（α）はそれぞれ、生成元α自体であることを特徴とする方法。

【請求項４】
請求項１又は２記載の方法において、生成元αを含む第１の関数ｆ（α）は、第２の通信端末（Ｂ）の公開鍵p_Bを含み、生成元αを含む第２の関数ｆ’（α）は、第１の通信端末（Ａ）の公開鍵p_Aを含むことを特徴とする方法。

【請求項５】
請求項１～３いずれかに記載の方法において、第１及び第２の署名s_A及びs_Bは、
$s_A = x - r_A a \alpha^a \mod (p-1)$
$s_B = y - r_B b \alpha^b \mod (p-1)$
ただし、$r_A = \alpha^x = f(\alpha)^{g(x)}$
$r_B = \alpha^y = f'(\alpha)^{g(y)}$
ｐ：素数
であることを特徴とする方法。

【請求項６】
請求項１、２又は４記載の方法において、第１及び第２の署名s_A及びs_Bは、
$s_A = x + a \alpha^a (p_B)^x \mod (p-1)$
$s_B = y + b \alpha^b (p_A)^y \mod (p-1)$
ただし、ｐ：素数
であることを特徴とする方法。

【請求項７】
請求項１～３いずれかに記載の方法において、第１及び第２の署名s_A及びs_Bは、
$s_A = x r_{x1} - (r_A)^{r x1} a \alpha^a \mod (p-1)$
$s_B = y r_{y1} - (r_B)^{r y1} b \alpha^b \mod (p-1)$
ただし、x_1：第１の通信端末において選択された第２のランダム整数
y_1：第２の通信端末において選択された第２のランダム整数
$r_{x1} = \alpha^{x1}$
$r_{y1} = \alpha^{y1}$
ｐ：素数
であることを特徴とする方法。

【請求項８】
請求項１～３いずれかに記載の方法において、該方法はさらに、
第１の通信端末において、第３のランダム整数x_1を選択してα^{x1}を生成し、該α^{x1}を第２の通信端末に送るステップと、

第２の通信端末において、第４のランダム整数y_1を選択してα^{y1}を生成し、該α^{y1}を第１の通信端末に送るステップと、
第１及び第２の通信端末において、一対の鍵k_1及びk_2を
$k_1 = \alpha^{x \cdot y}$
$k_2 = \alpha^{x1 \cdot y1}$
を計算するステップと
を備え、これら鍵k_1及びk_2のＸＯＲを計算することにより、セッション鍵Ｋを生成することを特徴とする方法。
【請求項９】
請求項１～８いずれかに記載の方法において、第１の指数関数ｆ（α）$^{g(x)}$を含んでいるメッセージは第１の署名s_Aをさらに含み、第２の指数関数ｆ’（α）$^{g(x)}$を含んでいるメッセージは第２の署名s_Bをさらに含んでいることを特徴とする方法。
【請求項１０】
請求項９記載の方法において、ステップｖｉ）はさらに、
第１の通信端末（Ａ）において、該通信端末によって受信したメッセージの完全性（インテグリティ）の有効性を、該メッセージに含まれる第２の署名及び第２の指数関数から該第２の指数関数と等価な値を計算し、該計算された値を、受信したメッセージ中の第２の指数関数と対比することによって、評価するステップと、
第２の通信端末（Ｂ）において、該通信端末によって受信したメッセージの完全性（インテグリティ）の有効性を、該メッセージに含まれる第１の署名及び第１の指数関数から該第１の指数関数と等価な値を計算し、該計算された値を、受信したメッセージ中の第１の指数関数と対比することによって、評価するステップと
を備えていることを特徴とする方法。
【請求項１１】
請求項１～３いずれかに記載の方法において、第１の通信端末（Ａ）に属する秘密情報は第１の署名s_Aであり、第２の通信端末（Ｂ）に属する秘密情報は第２の署名s_Bであることを特徴とする方法。
【発明の詳細な説明】
本発明は、暗号鍵の転送及び認証のための鍵一致（key agreement）プロトコルに関する。
情報の交換の際にプライバシを維持するために、データを鍵を用いて暗号化することが、広く知られている。この鍵は、通信者がメッセージを暗号化及び復号化できるが介入者にはメッセージの内容を判断できないように、選択されなければならない。
秘密鍵暗号プロトコルでは、通信者は、彼らにとって秘密である共通鍵を共有（share）する。このためには、この鍵が通信者の間で一致しており、この鍵の秘密性を維持するために条項（provision）が作成され、基礎となる安全性が万一危険にさらされた場合には、鍵の交換がなされることが要求される。
公開鍵暗号プロトコルは、１９７６年にDiffie-Hellmanによって最初に提案され、すべての潜在的な通信者に利用可能とされている公開鍵と、意図された受信者にだけ知られている秘密鍵（private key）とを用いる。公開鍵と秘密鍵とは、受信者の公開鍵を用いて暗号化されたメッセージは、秘密鍵を用いて容易に復号化できるが、秘密鍵は、平文（plaintext）、暗号文（ciphertext）及び公開鍵の知識からは導くことはできないような、相互関係になっている。
鍵の確立（establishment）は、二人以上の当事者が、セッション（session）鍵と称される、共有される秘密鍵（secret key）を確立するプロセスである。セッション鍵は、プライバシなどの何らかの暗号上の目的を達成するために、後で用いられる。鍵一致プロトコルには、２つの種類が存在する。すなわち、鍵が第１の当事者によって作成され、第２の当事者に安全に送信されるという鍵輸送（transport）プロトコルと、両方の当事者が、共有される秘密鍵を共同して確立する情報を出し合う鍵一致プロトコルと、である。当事者の間で必要となるメッセージ交換の数は、パス数（number of passes）と称される。鍵

確立プロトコルは、ある当事者が、特別に識別された第２の当事者以外のどの当事者もセッション鍵の値を知ることを許されないことが保証されている場合に、「内在的」（implicit）鍵認証（又は、単に、鍵認証）を提供すると称される。内在的鍵認証の性質は、第２の当事者が実際のセッション鍵を有していることを必ずしも意味しない。次に、鍵確立プロトコルは、ある当事者が、特別に識別された第２の当事者が特定のセッション鍵を実際に所持していることを保証されている場合には、鍵確認（confirmation）を提供すると称される。プロトコルに関係する両方の当事者に認証が提供される場合には、鍵認証は、相互的（mutual）と称され、一人の当事者にだけ提供される場合には、認証は、一方的（unilateral）と称される。

内在的な鍵認証を提供すると主張する提案は、これまでに、いくつかなされている。

例としては、鍵一致に関する、Nyberg-Rueppelによる１パス（one-pass）プロトコル、Matsumoto-Takashima-Imai（MTI）及びGoss and Yacobiによる２パス・プロトコルがある。

従来の提案は、共通鍵を確立するための通信者の間の送信が安全であり、侵入者がセッション鍵をリトリーブし暗号文を復号化することはでｆきないことを保証している。このようにして、資金の移動などの注意を要するトランザクションに対する安全性が提供されている。

例えば、MTI/A0鍵一致プロトコルでは、二人の通信者に知られている、共有される秘密鍵を、次のようにして確立している。

１．当初の、一時的な（one-time）セットアップの間に、鍵の発生と公開とが、適切なシステム・プライム（system prime）ｐと生成元（generator）$\alpha \in Z^*_p$とを真正であることが補償されるように、選択され公開される。通信者Ａは、長期の秘密鍵として$1 < a < p-1$であるランダムな整数ａを選択し、長期の公開鍵$z_A = \alpha^a \bmod p$を計算する。Ｂも、同様のｂとz_Bとを生成する。ＡとＢとは、相互の長期公開鍵の認証されたコピーへのアクセスを有することになる。

２．このプロトコルは、次のメッセージの交換を要求する。すなわち、

ＡからＢ：$\alpha^x \bmod p$　（１）

ＢからＡ：$\alpha^y \bmod p$　（２）

ｘ及びｙの値は、その送信の間は安全に保たれるが、その理由は、ｐが十分に大きくとられていれば、αの値と指数化とが知られているとしても、指数を決定するのは実際的ではないからである。

３．このプロトコルを実現するには、次のステップが、共有されている鍵が要求される度に実行される。

（ａ）Ａは、$1 \leqq x \leqq p-2$であるランダムな整数ｘを選び、Ｂに向けて、メッセージ（１）、すなわち、$\alpha^x \bmod p$を送る。

（ｂ）Ｂは、$1 \leqq y \leqq p-2$であるランダムな整数ｙを選び、Ａに向けて、メッセージ（２）、すなわち、$\alpha^y \bmod p$を送る。

（ｃ）Ａは、鍵Ｋ＝$(\alpha^y)^a z_B^x \bmod p$を計算する。

（ｄ）Ｂは、鍵Ｋ＝$(\alpha^x)^b z_A^y \bmod p$を計算する。

（ｅ）両者は、鍵Ｋ＝α^{bx+ay}を共有する。

鍵Ｋを計算するためには、Ａは、自分の秘密鍵ａとランダムな整数ｘとを使わなければならない。これらは、共に、Ａ本人だけに知られているものである。同様にして、Ｂは、セッション鍵Ｋを計算するためには、自分の秘密鍵ｂとランダムな整数ｙとを使わなければならない。秘密鍵ａ及びｂが、危険にさらされていないと仮定すると、侵入者は、他方の通信者と同一のセッション鍵を生成することはできない。従って、任意の暗文は、どちらの通信者にも復号化が不可能である。

従って、このプロトコル及び関連するプロトコルは、鍵確立には十分なものであると考えられてきたし、従来型の盗聴や、中間者（man-in-the-middle）による攻撃に対して抵抗できると考えられてきた。

状況によっては、相手方が、一方の通信者を他方の通信者であるとミスリードするのが効果的である。

そのような攻撃では、アクティブな相手方、すなわち、侵入者Ｅは、ＡとＢとの間で交換されるメッセージを修正し、その結果として、Ｂは、Ｅと鍵Ｋを共有していると信じ、他方で、Ａは、同じ鍵をＢと共有していると信じることになる。ＥがＫの値を知らない場合であっても、通信者の識別（ＩＤ）に関する偽の情報が、有用となる。
そのような攻撃が成功するであろう実際的なシナリオは、次のようなものである。Ｂは、銀行の支店であり、Ａは、口座保持者であると仮定する。銀行の本部によって証明書が発行され、その証明書の中には、保持者の口座情報が書かれている。資金の電子的支払い（デポジット）のためのプロトコルは、相互認証された鍵一致を介して、銀行の支店との鍵の交換であると仮定する。Ｂがいったん送信者を認証すると、暗号化された資金がその証明書の口座番号に払い込まれる。それ以上の認証が暗号化された支払いメッセージにおいてなされない場合（これは、帯域幅を節約するためになされるかもしれない）には、支払いは、Ｅの口座になされる。
本発明の目的は、上述の短所が回避される又は解消されるようなプロトコルを提供することである。
従って、本発明によると、１対の通信者Ａ及びＢが相互に情報を交換することを認証する方法であって、前記通信者は、それぞれが、秘密鍵ａ及びｂと、生成元αと前記秘密鍵ａ及びｂのそれぞれとから導かれた公開鍵p_A及びp_Bと、を有している方法が提供される。この方法は、
ｉ）前記通信者の第１の者Ａが、第１のランダムな整数ｘを選択し、前記生成元を含む関数ｆ（α）のｇ$^{(x)}$をベキとする指数関数を作ることにより、第１の指数関数ｆ（α）$^{g(x)}$を提供するステップと、
ｉｉ）前記第１の通信者Ａが、前記ランダムな整数ｘと前記指数関数ｆ（α）$^{g(x)}$とから第１の署名s_Aを生成するステップと、
ｉｉｉ）前記第１の通信者Ａが、第２の通信者Ｂに向けて、前記第１の指数関数ｆ（α）$^{g(x)}$と署名s_Aとを含むメッセージを送るステップと、
ｉｖ）前記通信者Ｂが、第２のランダムな整数ｙを選択し、前記生成元を含む関数ｆ’（α）のｇ$^{(y)}$をベキとする指数関数を作ることにより、第２の指数関数ｆ’（α）$^{g(y)}$と、前記第２の整数ｙと前記第２の指数関数ｆ（α）$^{g(x)}$とから得られるs_Bとを提供するステップと、
ｖ）前記第２の通信者Ｂが、第１の通信者Ａに向けて、前記第２の指数関数ｆ’（α）$^{g(y)}$と前記署名s_Bとを含むメッセージを送るステップと、
ｖｉ）前記通信者のそれぞれが、受け取ったメッセージの中の前記署名と前記指数関数とから、前記指数関数と等しい値を計算し、前記計算された値と前記送信された値とを比較することによって、自分たちが受け取ったメッセージの真正を検証するステップと、
ｖｉｉ）前記通信者Ａ及びＢのそれぞれが、前記他方の通信者によって彼ら自身にとって秘密である前記ランダムな整数を用いて、公開された情報を指数化することによって、セッション鍵を構成するステップと、を含む。
従って、侵入者Ｅが自らの公開鍵$p_E = \alpha^{ac}$をメッセージの一部として送信の中に入れることはできるが、Ｂは、メッセージを認証する際には、p_Aではなくp_Eを用いることになる。従って、指数関数の計算され送信された値は、対応しない。
本発明の実施例を次の添付した図面を参照することによって、これから説明することにする。
図１には、本発明による認証方法が用いられるデータ通信システムの概略図が示されている。
そこで、図１を参照すると、通信者Ａ及び通信者Ｂとして表される１対の通信者１０、１２が、通信チャネル１４上で情報を交換する（なお、この出願において通信者Ａ及び通信者Ｂ、通信者１０及び通信者１２などと表現されているのは、図１に示されているデータ通信システムの中に存在する通信機能を有するコンピュータである通信端末を意味する）。暗号ユニット１６、１８が、通信者１０、１２とチャネル１４とのそれぞれの間に配置されている。鍵２０は、暗号ユニット１６、１８のそれぞれに関連し、それぞれのユニッ

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、チャネル１４上で運ばれる暗文に変換する。
動作においては、Ａの通信者１０によって生成されるメッセージは、ユニット１６によって、鍵２０を用いて暗号化され、チャネル１４上の暗文として、ユニット１８まで送信される。
鍵２０は、ユニット１８において暗文に作用して、Ｂの通信者１２のために平文のメッセージを生成する。鍵２０が対応する場合には、通信者１２によって受け取られたメッセージは、通信者１０によって送られたものである。
図１に示されたシステムが動作するためには、鍵２０が同一であり、従って、公開的な態様での情報の移動を可能にする鍵一致（agreement）プロトコルが確立されていることが必要である。そのような鍵の生成には多数のプロトコルが利用可能であり、また、Diffie-Hellman鍵交換の変形も存在する。その目的は、当事者Ａ及びＢが秘密セッション鍵Ｋを確立することである。
これらのプロトコルのためのシステム・パラメータは、素数ｐと乗法群Z^*_pの生成元αとである。通信者Ａは、秘密鍵ａと、公開鍵$p_A=\alpha^a$とを有する。通信者Ｂは、秘密鍵ｂと、公開鍵$p_B=\alpha^b$とを有する。以下で例を挙げるプロトコルでは、$text_A$は、当事者Ａを識別する情報のストリングを意味する。他方の当事者Ｂが通信者Ａの公開鍵の真正のコピーを有しており、更に、$text_A$がＡの信用のおけるセンターによって発行された公開鍵証明書を含む場合には、通信者Ｂは、その信用のおけるセンターの公開鍵の真正のコピーを用いて、通信者Ａの証明書を検証でき、従って、通信者Ａの公開鍵の真正のコピーを得ることができる。
以下のそれぞれの例では、侵入者Ｅは、Ａからのメッセージが Ｅ自身から生じたものとして識別されることを望んでいると仮定する。これを達成するには、Ｅは、$1 \leqq e \leqq p-2$であるランダムな整数ｅを選択し、$p_E=(p_A)^e=\alpha^{ae} \mod p$を計算し、これがＥ自身の公開鍵であることを証明させる。Ｅは、ｅを知ってはいるが、指数ａｅは知らない。ｔｅｘｔＡをｔｅｘｔＥによって代替することによって、通信者Ｂは、メッセージがＡからではなくＥからのものであると考え、Ｅの公開鍵を用いてセッション鍵Ｋを生成する。Ｅはまた、Ｂからのメッセージを中間奪取（インターセプト）し、その秘密のランダムな整数ｅを用いて、その内容を修正する。Ａは、次に、その情報を用いて、ＡがＢと通信できるようにする同じセッション鍵を生成する。
侵入者ＥがＢに、ＢはＥと通信しているということを信じさせようとしているのを妨害するには、次のプロトコルが採用される。
このプロトコルの目的は、当事者Ａ及びＢがセッション鍵Ｋを確立することである。ここで挙げたプロトコルは、役割対称的（role-symmetric）であり、対話的（interactive）ではない。
このプロトコルのためのシステム・パラメータは、素数ｐと乗法群Z^*_pの生成元αとである。通信者Ａは、秘密鍵ａと、公開鍵$p_A=\alpha^a$とを有する。通信者Ｂは、秘密鍵ｂと、公開鍵$p_B=\alpha^b$とを有する。

第１のプロトコル

１．Ａは、$1 \leqq x \leqq p-2$であるランダムな整数ｘを選び、$r_A=\alpha^x$と、署名$s_A=x-r_A a \alpha^a \mod (p-1)$と、を計算する。Ａは、Ｂに向けて、$\{r_A, s_A, text_A\}$を送る。
２．Ｂは、$1 \leqq y \leqq p-2$であるランダムな整数ｙを選び、$r_B=\alpha^y$と、署名$s_B=y-r_B b \alpha^b \mod (p-1)$と、を計算する。Ａは、Ｂに向けて、$\{r_B, s_B, text_B\}$を送る。
３．Ａは、
$\alpha^{s_B}(p_B)^{r_B}\alpha^b$
を計算し、これが、r_Bに等しいことを検証する。Ａは、次に、セッション鍵$K=(r_B)^x=\alpha^{xy}$を計算する。
４．Ｂは、

$\alpha^{s_A}(p_A)^{r_A}\alpha^{a}$
を計算し、これが、r_Aに等しいことを検証する。Bは、次に、セッション鍵K＝（r_A）$^y=\alpha^{xy}$を計算する。
Eが、$text_A$を$text_B$に交換する場合には、Bは、r_Aの送信された値には対応しない
$\alpha^{s_A}(p_E)^{r_A}\alpha^{a}$
を計算する。Bは、従って、侵入者Eに関する警告を受け、別のセッション鍵を開始することになる。
第１のプロトコルの短所は、完全な前方向の秘密性（守秘性）（perfect forward secrecy）が得られないことである。すなわち、相手側が当事者Aの長期の秘密鍵aを知る場合には、この相手側は、Aの過去のセッション鍵すべてを導き出せることになる。完全な前方向の秘密性は、プロトコル１を次のようにして修正することによって、達成される。
修正された第１のプロトコル
ステップ１では、Aはまた、
α^{x_1}
をBに送る。ここで、x_1は、Aによって生成された第２のランダムな整数である。同様にして、上述のステップ２では、Bはまた、
α^{y_1}
をAに送る。ここで、y_1は、ランダムな整数である。A及びBは、鍵
$K=\alpha^{xy}\ \alpha^{x_1y_1}$
を計算する。
第１のプロトコルの別の短所は、相手側がAの秘密のランダムな整数xを知る場合には、この相手側は、当事者Aの長期の秘密鍵を、方程式$s_A=x-r_Aa\alpha^a \bmod (p-1)$から求めることができる点である。このプロトコルのうまく設計された実現例では、秘密の整数の開示は回避されるので、この短所は、基本的に理論的性格を有するものである。
第２のプロトコル
次に述べる第２のプロトコルは、これら２つの短所を解決する。
１．Aは、$1\leqq x\leqq p-2$であるランダムな整数xを選び、（p_B）^{x}と、α^xと署名$s_A=x+a\alpha^a$（p_B）$^x \bmod (p-1)$と、を計算する。Aは、Bに向けて、{α^x，s_A，$text_A$}を送る。
２．Bは、$1\leqq y\leqq p-2$であるランダムな整数yを選び、（p_A）^{y}と、α^yと署名$s_B=y+b\alpha^b$（p_A）$^y \bmod (p-1)$と、を計算する。Bは、Aに向けて、{α^y，s_B，$text_B$}を送る。
３．Aは、（α^y）^{a}を計算して、
$\alpha^{s_B}(p_B)^{-\alpha^b}\alpha^{ay}=\alpha^y$

であることを検証する。Aは、次に、セッション鍵K＝α^{ay}（p_B）^{x}を計算する。
４．Bは、（α^x）^{b}を計算して、
$\alpha^{s_A}(p_A)^{-\alpha^a}\alpha^{bx}=\alpha^x$

であることを検証する。Aは、次に、セッション鍵K＝α^{by}（p_A）^{y}を計算する。
第２のプロトコルが第１のプロトコルとの比較で優れているのは、それが、完全な前方向の秘密性（forward secrecy）を提供するからである。秘密であるランダムな整数xの開示によって、相手側が秘密鍵aを知ることができるのではあるが、これは実際上は問題ではない。なぜならば、Aは、自分がこのプロトコルのステップ１においてxを用いた直後に、xを廃棄することができるからである。
AがBの公開鍵の認証されたコピーを有していない場合には、Bは、自らの鍵の真正（certified）なコピーを、プロトコルの開始時に、Aに送信しなければならない。この場合には、第２のプロトコルは、３パス・プロトコルである。
量S_Aは、値α^xに対して、Aの署名として機能する。この署名は、当事者Bだけに確認が

可能であるという新規な性質を有している。このアイデアは、ElGamalライクな署名方式のすべてに一般化できる。
上述の第１及び第２のプロトコルは、帯域幅の要件と、鍵一致の計算上の効率とを向上させるように修正が可能である。修正されたプロトコルは、次に、プロトコル１’及びプロトコル２’として、示してある。それぞれの場合に、Ａ及びＢは、共通鍵$\alpha^{S_A S_B}$を共有している。

プロトコル１’

１．Ａは、$1 \leqq x \leqq p-2$であるランダムな整数ｘを選び、$r_A = \alpha^a$と、$s_A = x + r_A a \alpha^a \bmod (p-1)$と、を計算する。Ａは、Ｂに向けて、$\{r_A, text_A\}$を送る。
２．Ｂは、$1 \leqq y \leqq p-2$であるランダムな整数ｙを選び、$r_B = \alpha^y$と、$s_B = y + r_B b \alpha^b \bmod (p-1)$と、を計算する。Ａは、Ｂに向けて、$\{r_B, text_B\}$を送る。
３．Ａは、
$\alpha^{S_A S_B}$
に等しい
$$K = (r_B (p_B)^{r_B} \alpha^b)^{s_A}$$
を計算する。
４．Ｂは、
$\alpha^{S_A S_B}$
に等しい
$$K = (r_A (p_A)^{r_A} \alpha^a)^{s_B}$$
を計算する。
このようにして、Ａ及びＢは、共通鍵を共有するが、署名ｓＡ及びｓＢは、送信される必要がないことに注意すべきである。

プロトコル２’

１．Ａは、$1 \leqq x \leqq p-2$であるランダムな整数ｘを選び、$(p_B)^x$と、α^xと署名$s_A = x + a (p_B)^x \bmod (p-1)$と、を計算する。Ａは、Ｂに向けて、$\{\alpha^x, text_A\}$を送る。
２．Ｂは、$1 \leqq y \leqq p-2$であるランダムな整数ｙを選び、$(p_A)^y$と、α^yと署名$s_B = y + b (p_A)^y \bmod (p-1)$と、を計算する。Ｂは、Ａに向けて、$\{\alpha^y, text_B\}$を送る。
３．Ａは、$(\alpha^y)^a$と、
$(\alpha^y (p_B)^{\alpha^b \alpha^{ay}})^{s_A}$
を、すなわち、
$\alpha^{S_A S_B}$
を計算する。
４．Ｂは、$(\alpha^x)^b$と、
$$K = (\alpha^x (p_A)^{\alpha^a \alpha^{bx}})^{s_B}$$
を、すなわち、
$\alpha^{S_A S_B}$
を計算する。
従って、やはり、s_A及びs_Bの送信が回避された。
Ａ及びＢがセッション鍵Ｋを確立するために、別のプロトコルが利用可能である。

第３のプロトコル

このプロトコルに対するシステム・パラメータは、乗法群Z^*_pの素数ｐと生成元αである。ユーザＡは、秘密鍵ａと公開鍵$p_A = \alpha^a$とを有している。ユーザＢは、秘密鍵ｂと公開鍵$p_B = \alpha^b$とを有している。
１．Ａは、$1 \leqq x, x_1 \leqq p-2$である２つのランダムな整数ｘ，x_1を選び、
$r_{x_1} = \alpha^{x_1}$
と、$r_A = \alpha^x$と、

$(r^A)^{r_{x_1}}$
とを計算し、更に、署名
$S_A = x r_{x_1} - (r_A)^{r_{x_1}} a \alpha^a \mod (p-1)$
を計算する。Aは、Bに向けて、
$\{r_A, s_A, \alpha^{x_1}, text_A\}$
を送る。
2．Bは、$1 \leqq y, y_1 \leqq p-2$である2つのランダムな整数y，y_1を選び、
$r_{y_1} = \alpha^{y_1}$
と、$r_B = \alpha^y$と、
$(r_B)^{r_{y_1}}$
とを計算し、更に、署名
$S_B = y r_{y_1} - (r_B)^{r_{y_1}} b \mod (p-1)$
を計算する。Bは、Aに向けて、
$\{r_B, s_B, \alpha^{y_1}, text_B\}$
を送る。
3．Aは、
$\alpha^{s_B} (p_B)^{(r_B)^{r_{y_1}}}$
を計算し、これが、
$(r^B)^{r_{y_1}}$
に等しいことを確認する。Aは、セッション鍵
$K = (\alpha^{y_1})^{x_1} = \alpha^{x_1 y_1}$
を計算する。
4．Bは、
$\alpha^{s_A} (p_A)^{(r_A)^{r_{x_1}}}$
を計算し、これが、
$(r_A)^{r_{x_1}}$
に等しいことを確認する。Bは、セッション鍵
$K = (\alpha^{x_1})^{y_1} = \alpha^{x_1 y_1}$
を計算する。
これらのプロトコルでは、（r_A，s_A）は、Aだけがメッセージ
r_{x_1}
に署名できるという性質を有する
r_{x_1}
の署名であると考えることができる。

鍵輸送プロトコル

上述のプロトコルによれば、セッション鍵の確立と認証とが可能になる。Aがセッション鍵を当事者Bに輸送（transport）することを可能にするプロトコルを確立することが望まれる。そのようなプロトコルを次に述べる。
1．Aは、$1 \leqq x \leqq p-2$であるランダムな整数xを選び、$r_A = \alpha^x$と、署名$s_A = x - r_A a \alpha^a \mod (p-1)$と、を計算する。Aは、Bに向けて、$\{r_A, s_A, text_A\}$を送る。
2．Bは、
$\alpha^{s_A} (p_A)^{r_A \alpha^a}$
を計算し、この量が、r_Aに等しいことを検証する。Bは、次に、セッション鍵$K = (r_A)^b$を計算する。

修正された鍵輸送プロトコル

上述のプロトコルは、署名sAを送信する必要をなくすことによって、帯域幅を減少させ

るように修正が可能である。
１．Ａは、１≦ｘ≦ｐ－２であるランダムな整数ｘを選び、$r_A = \alpha^x$と、署名$s_A = x - r_A a \alpha^a \mod (p-1)$と、を計算する。Ａは、更に、
$K = (p^B)^{s_A}$
を計算して、Ｂに向けて、$\{r_A, text_A\}$を送る。
２．Ｂは、
$(\alpha^x (p_A)^{-r_A \alpha^a})^b = \alpha^{b s_A}$
を計算し、この量が、r_Aに等しいことを検証する。Ｂは、次に、セッション鍵$K = (\alpha^x (p_A)^{-rA \alpha a})^b = \alpha^{bSA}$を計算する。
すべての１パス鍵輸送プロトコルは、次に述べるリプレイの問題を有する。１パス鍵輸送プロトコルを用いてセッション鍵ＫをＡからＢへ、このセッション鍵を用いて暗号化された何らかのテキストと共に送信することを考える。Ｅが、ＡからＢへの送信を記録すると仮定する。もし、Ｅが、後に、Ｂの復号化装置へのアクセス（ただし、Ｂの秘密鍵など、その装置の内部的な内容へのアクセスではない）を、その装置への送信をリプレイすることによって得ることになる場合には、Ｅは、元のテキストを回復することができる。この状況では、Ｅは、セッション鍵を知らない。
このリプレイによるアタックは、タイムスタンプの使用などの、通常の方法によって失敗させることができる。しかし、Ｂの計算資源が限定されていて、それぞれのセッションの開始時に、Ｂがランダムなビット・ストリングｋをＡに送信する方がより適切であるようなこともあり得る。テキストを暗号化するのに用いられるセッション鍵は、その場合には、ｋ▲＋▼ｋ、すなわち、ｋとｋとのＸＯＲを計算したものとなる。
署名（signing）方程式$s_A = x - r_A a \alpha^a$と、プロトコル２における鍵輸送プロトコル$r_A = \alpha^{xb}$とは、いくつかの変形例で代替することができる。いくつか例を挙げると、次の通りである。
$r_A = s_A x + z$
$s_A = x \alpha^a + a r_A$
$s_A = x r_A + A \alpha^a$
$1 = a r_A + x s_A$
既に述べたプロトコルは、すべて、乗法群Z^*_pの設定において、説明された。しかし、これらのプロトコルは、離散対数問題が困難を生じさせるように見える任意の有限群において機能するように容易に修正することができる。適切な選択肢としては、有限体の乗法群（特に、有限体ＧＦ（2^n））、位数（order）ｑのZ^*_pの部分群、有限体上で定義される楕円曲線上の点から成る群などがある。それぞれの場合に、適切な生成元（generator）αを用いて公開鍵を定義する。
上述したプロトコルは、また、直接的な方法で修正して、それぞれのユーザが自分自身のシステム・パラメータｐ及びα（又は、Z^*_p以外の群が用いられる場合には、類似のパラメータ）を選択できるような状況を扱えるようにできる。
上述のプロトコルでは、一般形式$s_A = x + r_a \cdot a \cdot \alpha^a$の署名成分が用いられていた。これらのプロトコルは、安全性を損ねることなく、より単純な一般形式$s_A = x + r_a \cdot a$の署名成分を用いるように修正が可能である。
これらのプロトコルの例を、同じ記号（notation）を用いて以下に与えるが、望むのであれば、別の記号を用いてこれらのプロトコルを表現することができることを理解すべきである。
プロトコル１”
このプロトコルは、乗法群Z^*_pにおける次の記号を用いて説明される。
ｐは、素数である。
αは、Z^*_pの生成元である。
ａ及びｂは、当事者Ａ及びＢのそれぞれの長期的な秘密鍵である。
$\alpha^a \mod p$は、当事者Ａの長期的な秘密鍵である。
$\alpha^b \mod p$は、当事者Ｂの長期的な秘密鍵である。

ｘは、Ａによって短期の秘密鍵として選択されるランダムな整数である。
$r_a = \alpha^x \mod p$は、当事者Ａの短期の公開鍵である。
ｙは、Ｂによって短期の秘密鍵として選択されるランダムな整数である。
$r^b = \alpha^y \mod p$は、当事者Ａの短期の公開鍵である。

$\overline{r}_a$

は、r_aから導かれる整数である。

$\overline{r}_b$

は、r_bから導かれる整数である。
プロトコルを実現するには、次のようにする。
１．Ａは、r_aをＢに送る。
２．Ｂは、r_bをＡに送る。
３．Ａは、

$$s_A = x + \overline{r}_a \cdot a \bmod (p-1)$$

を計算する。
４．Ａは、セッション鍵

$$K = (\alpha^y (\alpha^b)^{\overline{r}_b})^{s_A} \bmod p$$

を計算する。
５．Ｂは、

$$s_B = y + \overline{r}_b \cdot b \bmod (p-1)$$

を計算する。
６．Ｂは、セッション鍵

$$K = (\alpha^x (\alpha^a)^{\overline{r}_a})^{s_B} \bmod p$$

を計算する。
７．共有される秘密は、$\alpha^{s_A s_B} \bmod p$である。
このプロトコルでは、待機幅の要件が再び緩和されているが、署名成分は、通信者の短期及び長期の鍵を組み合わせて、侵入者からの攻撃を禁止している。
このプロトコルは、また、Z^*_pの部分群を用いても実現できる。この場合には、ｑは、（ｐ－１）の素約数（prime divisor）であり、ｇは、Z^*_pの中の位数ｐの要素である。
Ａ及びＢの公開鍵は、それぞれが、g^a及びg^bの形式を有し、短期の鍵r_a及びr_bは、g^x及びg^yの形式を有している。
署名成分であるs_A及びs_Bは、ｍｏｄｑで計算され、セッション鍵は、従前のように、ｍｏｄｑで計算される。この場合には、共有の秘密は、

$$g^{s_A s_B} \bmod p$$

である。
既に述べたように、これらのプロトコルは、Z^*_p以外の群においても実現が可能であり、特に、ローバスト（robust）群は、有限体上の楕円曲線上の点から成る群である。このような実現例は、次にプロトコル１”’として挙げてある。

プロトコル１”’

次の記号を用いる。
Ｅは、Ｆｑ上で定義される楕円曲線である。
Ｐは、Ｅ（Ｆｑ）内の素数位数の点である。
d_a（$1 < d_a < n-1$）は、当事者Ａの長期の秘密鍵である。
d_b（$1 < d_b < n-1$）は、当事者Ｂの長期の秘密鍵である。
$Q_a = d_a P$は、当事者Ａの長期の公開鍵である。
$Q_b = d_b P$は、当事者Ｂの長期の公開鍵である。
ｋ（$1 < k < n-1$）は、当事者Ａの短期の秘密鍵である。
ｍ（$1 < m < n-1$）は、当事者Ｂの短期の秘密鍵である。

$r_b = mP$は、当事者Ｂの短期の公開鍵である。
ｒａ及びｒｂは、ビット・ストリングであり、例えば、r_a及びr_bのｘ座標の８０最下位ビットである。
このプロトコルを実現するには、次のようにする。
１．Ａは、r_aをＢに送る。
２．Ｂは、r_bをＡに送る。
３．Ａは、

$$s_A = (k + \tilde{r}_a \cdot d_a) \bmod n$$

を計算する。
４．Ａは、セッション鍵

$$K = s_A (r_b + \tilde{r}_b Q_b)$$

を計算する。
５．Ｂは、

$$s_B = (m + \tilde{r}_b \cdot d_b) \bmod n$$

を計算する。
６．Ｂは、セッション鍵

$$K = s_b (r_a + \tilde{r}_a Q_a)$$

を計算する。
７．共有される秘密は、$s_a s_b P$である。
再び、通信者の間では署名成分ｓＡ及びｓＢを送る必要はないことに注意すべきである。
しかし、通信者の短期及び長期の鍵が成分の形式で組み合わされる。
先の例におけるｘ及びｙに対して、記号ｍを用いているのは、曲線上の点の座標（ｘ，ｙ）との混乱を回避するためである。

【図１】

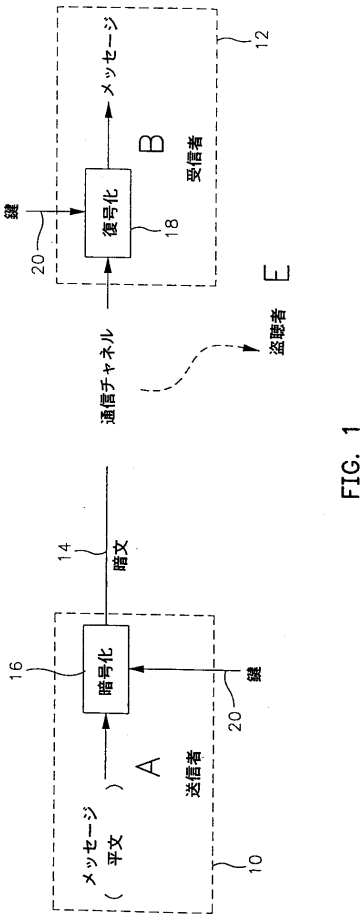

FIG. 1

フロントページの続き

(74)代理人 100096013
弁理士 富田 博行
(74)代理人 100096068
弁理士 大塚 住江
(72)発明者 ヴァンストーン，スコット・エイ
カナダ国 エヌ２ティー・２エイチ４ オンタリオ，ウォータールー，サンドブルック・コート ５３９
(72)発明者 メネゼス，アルフレッド・ジョン
アメリカ合衆国アラバマ州３６８３０，オーバーン，ペイン・ストリート ２５４
(72)発明者 キュー，ミングァ
カナダ国 エヌ２エル・３イー５ オンタリオ，ウォータールー，ユニバーシティ・アベニュー・ウエスト １５７，ナンバー １１２

合議体
審判長 吉岡 浩
審判官 石田 信行
審判官 冨吉 伸弥

(58)調査した分野(Int.Cl.，ＤＢ名)
H04L 9/08