(19)日本国特許庁(JP)　(12)公表特許公報(A)　(11)特許出願公表番号
特表2006-528874
(P2006-528874A)
(43)公表日　平成18年12月21日(2006.12.21)

(51)Int.Cl.		F I			テーマコード（参考）
H04L 9/08	(2006.01)	H04L	9/00	601D	5J104
		H04L	9/00	601F	

審査請求 未請求　予備審査請求 未請求　（全 27 頁）

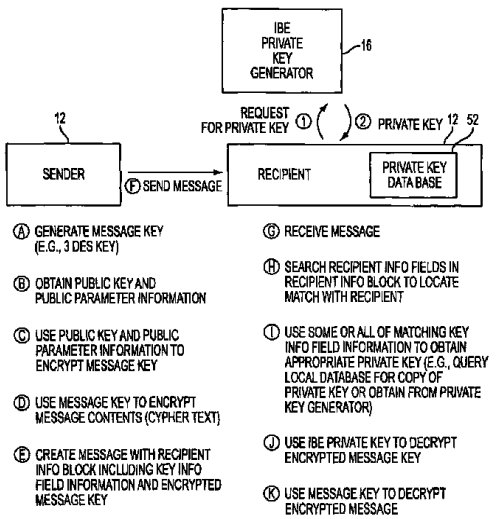
(21)出願番号	特願2006-532326 (P2006-532326)
(86)(22)出願日	平成16年3月12日 (2004.3.12)
(85)翻訳文提出日	平成17年10月31日 (2005.10.31)
(86)国際出願番号	PCT/US2004/007829
(87)国際公開番号	WO2005/010732
(87)国際公開日	平成17年2月3日 (2005.2.3)
(31)優先権主張番号	10/390,058
(32)優先日	平成15年3月14日 (2003.3.14)
(33)優先権主張国	米国 (US)

(71)出願人　505295547
ボルテージ　セキュリティー，　インコーポレイテッド
アメリカ合衆国　カリフォルニア　９４３０４，　パロ　アルト，　アラストラデロ　ロード　１０７０，　スイート　１００
(74)代理人　100078282
弁理士　山本　秀策
(74)代理人　100062409
弁理士　安村　高明
(74)代理人　100113413
弁理士　森下　夏樹

最終頁に続く

(54)【発明の名称】同一性ベースの暗号化メッセージングシステム

(57)【要約】
再生セルロースにカプセル封入している活性物質、および再生セルロースマトリックス内に活性物質をカプセル封入する方法が開示されている。活性物質は、再生セルロースのマトリックス内に実質的に均一に分布しているのが好ましい。再生セルロースは、（ｉ）再生セルロースが調製された最初のセルロースと実質的に同じ分子量を有し、（ｉｉ）出発セルロースと比べて追加された置換基を実質的に含まず、捕捉されたイオン性液体分解生成物も実質的に含まない。



【特許請求の範囲】
【請求項１】
ユーザ装置でユーザが通信網を介して通信するシステムにおいて暗号化通信をサポートするために、同一性ベースの暗号化を用いる方法であって、前記システムは複数の同一性ベースの暗号化用の秘密鍵生成器を有し、該複数の秘密鍵生成器はそれぞれ、前記ユーザに対して秘密鍵を生成し、該複数の秘密鍵生成器はそれぞれ、その秘密鍵生成器に関連付けられたユーザに送られるメッセージの前記同一性ベースの暗号化に用いられる各公開パラメータ情報を生成し、前記システムにおけるメッセージの送信者は、（１）目的のメッセージ受信者と関連付けられた前記秘密鍵生成器に関連する前記公開パラメータ情報と、（２）該目的の受信者の前記アイデンティティに基づく同一性ベースの暗号化の公開鍵とを入力とする同一性ベースの暗号化アルゴリズムを用いて、前記メッセージそれぞれを暗号化し、ユーザは２つ以上の前記秘密鍵生成器と関連を持ってもよく、そのため所与の受信者が所与の送信者から所与の暗号化されたメッセージを受け取る場合に、前記所与の受信者は、前記所与の送信者が前記所与のメッセージを暗号化するために、どの秘密鍵生成器およびどの関連する公開パラメータ情報を用いたのかを事前に知らなくてもよく、前記所与の暗号化されたメッセージを復号化するために該所与の受信者の対応する秘密鍵のうちどれを用いればよいのか事前に知らなくてもよい方法であり、該方法は、
前記所与の送信者から前記所与の受信者へ前記所与の暗号化されたメッセージとともに送られた秘密鍵識別情報を前記受信者側で受け取るステップと、
前記暗号化されたメッセージを復号化するための前記所与の受信者の秘密鍵のうち前記適切な鍵を取得するために、前記所与の受信者側で前記秘密鍵識別情報を用いるステップと、
を含む、方法。
【請求項２】
前記所与の送信者から送られた前記秘密鍵識別情報を前記受信者側で受け取るステップは、前記所与のメッセージの受信者情報フィールドに置かれた秘密鍵識別情報を受け取ることを含む、請求項１に記載の方法。
【請求項３】
前記所与の送信者から送られた前記秘密鍵識別情報を前記受信者側で受け取るステップは、前記所与のメッセージの鍵情報フィールドに置かれた秘密鍵識別情報を受け取ることを含む、請求項１に記載の方法。
【請求項４】
前記所与のメッセージを復号化するために前記適切な秘密鍵を用いるステップであって、前記暗号化されたメッセージの暗号化されたメッセージ鍵フィールドに含まれて、前記所与の送信者から送られた暗号化されたメッセージ鍵を復号化し、次に、前記メッセージ鍵を用いて前記所与の送信者によって暗号化されたメッセージペイロードを前記メッセージ鍵を用いて復号化することによって行われるステップをさらに含む、請求項３に記載の方法。
【請求項５】
前記所与の送信者から送られた前記秘密鍵識別情報を前記受信者側で受け取るステップは、前記所与のメッセージの鍵情報フィールドに置かれた秘密鍵識別情報を受け取ることを含み、前記鍵情報フィールドは前記受信者の電子メールアドレスに基づく受信者識別子を有する、請求項１に記載の方法。
【請求項６】
前記所与の送信者から送られた前記秘密鍵識別情報を前記受信者側で受け取るステップは、前記所与のメッセージの鍵情報フィールドに置かれた秘密鍵識別情報を受け取ることを含み、前記鍵情報フィールドは有効期間と連結された前記受信者の電子メールアドレスに基づく受信者識別子を有する、請求項１に記載の方法。
【請求項７】
前記所与の送信者から送られた前記秘密鍵識別情報を前記受信者側で受け取るステップは

、前記所与のメッセージの鍵情報フィールドに置かれた秘密鍵識別情報を受け取ることを含み、前記鍵情報フィールドは前記所与の受信者の受信者識別子と秘密鍵生成器識別子とを有する、請求項１に記載の方法。

【請求項８】

前記所与の送信者から送られた前記秘密鍵識別情報を前記受信者側で受け取るステップは、前記所与のメッセージの鍵情報フィールドに置かれた秘密鍵識別情報を受け取ることを含み、前記鍵情報フィールドは前記所与の受信者の受信者識別子とサーバ名に基づく秘密鍵生成器識別子とを有する、請求項１に記載の方法。

【請求項９】

前記所与の送信者から送られた前記秘密鍵識別情報を前記受信者側で受け取るステップは、前記所与の受信者の秘密鍵のうち前記適切な鍵に関連する前記秘密鍵生成器を識別する秘密鍵生成器識別子を前記送信者から受け取ることを含む、請求項１に記載の方法。

【請求項１０】

前記所与の送信者から送られた前記秘密鍵識別情報を前記受信者側で受け取るステップは、前記所与の受信者の秘密鍵のうち前記適切な鍵に関連する前記秘密鍵生成器を識別する秘密鍵生成器識別子を前記送信者から受け取ることを含み、前記暗号化されたメッセージを復号化するための前記所与の受信者の秘密鍵のうち前記適切な鍵を取得するために、前記所与の受信者側で前記秘密鍵識別情報を用いるステップは、前記受信者側のローカルデータベースで前記所与の受信者の秘密鍵のうち前記適切な鍵の位置を特定するローカルデータベースクエリを作成するために、前記秘密鍵生成器識別子を用いることを含む、請求項１に記載の方法。

【請求項１１】

前記所与の送信者から送られた前記秘密鍵識別情報を前記受信者側で受け取るステップは、前記所与の送信者によって前記所与のメッセージを暗号化するために用いられた前記公開パラメータ情報の前記バージョンについての情報を有する秘密鍵識別情報を受け取ることを含む、請求項１に記載の方法。

【請求項１２】

前記秘密鍵識別情報を受け取るステップは、前記所与の送信者によって前記所与のメッセージの暗号化に用いられた前記公開パラメータ情報を受け取ることを含む、請求項１に記載の方法。

【請求項１３】

前記秘密鍵識別情報を受け取るステップは、ハッシュ関数によって処理された情報を受け取ることを含む、請求項１に記載の方法。

【請求項１４】

前記秘密鍵識別情報を受け取るステップは、ハッシュ関数によって処理された秘密鍵生成器識別情報を受け取ることを含む、請求項１に記載の方法。

【請求項１５】

前記所与の受信者の秘密鍵のうち前記適切な鍵を取得するために、前記所与の受信者側で前記秘密鍵識別情報を用いるステップは、ローカルストレージから前記適切な秘密鍵を検索するために、前記受信者側で前記秘密鍵識別情報を用いることをさらに含む、請求項１に記載の方法。

【請求項１６】

前記所与の受信者の秘密鍵のうち前記適切な鍵を取得するために、前記所与の受信者側で前記秘密鍵識別情報を用いるステップは、前記通信網上で適切な秘密鍵生成器から前記適切な秘密鍵を検索するために、前記所与の受信者側で前記秘密鍵識別情報を用いることをさらに含む、請求項１に記載の方法。

【請求項１７】

前記送信者が、前記受信者側で前記メッセージの復号化に用いるべき同一性ベースの暗号化アルゴリズムを識別するアルゴリズム識別子情報を前記メッセージとともに提供し、前記方法は、前記受信者側で前記メッセージを復号化する際に前記アルゴリズム識別子情報

を用いるステップをさらに含む、請求項１に記載の方法。
【請求項１８】
ユーザ装置でユーザが通信網を介して通信するシステムにおいて暗号化通信をサポートするために、同一性ベースの暗号化を用いる方法であって、前記システムが複数の秘密鍵生成器を有し、該複数の秘密鍵生成器はそれぞれ、前記ユーザに対して秘密鍵を生成し、該方法は、
送信者側で、複数の関連する秘密鍵を持つ受信者宛てのメッセージを暗号化するステップであって、該複数の関連する秘密鍵はそれぞれ、前記秘密鍵生成器の各１つによって生成され、前記送信者は、メッセージペイロードを暗号化するためにメッセージ鍵を使用し、前記メッセージ鍵を暗号化するために同一性ベースの暗号化アルゴリズムを使用することによって、前記メッセージを暗号化し、前記同一性ベースの暗号化アルゴリズムの入力として、前記各秘密鍵生成器の所与の１つによって生成される公開パラメータと、前記受信者の前記アイデンティティに基づく同一性ベースの暗号化の公開鍵とを用いるステップと、
前記暗号化されたメッセージ鍵、暗号化されたメッセージペイロード、および前記受信者が、該受信者どの秘密鍵が前記暗号化されたメッセージ鍵の復号化に適しているのかを識別するための秘密鍵識別情報とともに前記メッセージを前記送信者から前記受信者へ送信するステップと、
を含む、方法。
【請求項１９】
前記適切な秘密鍵を取得するために、前記受信者側で前記秘密鍵識別情報を用いるステップと、
前記適切な秘密鍵を用いて、前記暗号化されたメッセージ鍵を復号化するステップと、
前記暗号化されたメッセージペイロードを復号化するために、前記復号化されたメッセージ鍵を用いるステップと、
をさらに含む、請求項１８に記載の方法。
【請求項２０】
前記メッセージを暗号化するステップは、複数の受信者に宛てた前記メッセージを暗号化することを含み、前記メッセージを送るステップは、前記送信者から前記複数の受信者それぞれに対して、該受信者が、該受信者のどの秘密鍵が前記暗号化されたメッセージ鍵の復号化に適切であるのかを識別するための秘密鍵識別情報とともに前記メッセージを送ることを含む、請求項１８に記載の方法。
【発明の詳細な説明】
【背景技術】
【０００１】
（発明の背景）
本発明は暗号化に関し、特に、セキュアなメッセージを送るための同一性ベースの暗号化（Ｉｄｅｎｔｉｔｙ－Ｂａｓｅｄ－Ｅｎｃｒｙｐｔｉｏｎ）スキームに関する。
【０００２】
セキュア電子メールサービスおよびセキュアウェブブラウジングなど、セキュアな通信サービスを提供するために暗号システムが用いられている。
【０００３】
対称鍵暗号システムでは、メッセージの送信者は、メッセージの受信者が該メッセージを復号化するために使用する鍵と同一の鍵を用いて、メッセージを暗号化する。対称鍵システムでは、送信者および受信者はそれぞれ、セキュアな方法で共有鍵を交換する必要がある。
【０００４】
公開鍵暗号システムでは、２種類の鍵、すなわち公開鍵と秘密鍵とを用いる。送信者は、受信者の公開鍵を用いてメッセージを暗号化することもできる。各受信者は、自分宛てのメッセージの復号化に用いる秘密鍵を持つ。

【０００５】
現在使用されている公開鍵暗号システム１つが、ＲＳＡ（ＲｉＶｅｓｔ－Ｓｈａｍｉｒ－Ａｄｌｅｍａｎ）暗号システムである。このシステムでは、各ユーザは、一意の公開鍵と一意の秘密鍵とを持つ。このシステムを使用する送信者は、インターネットに接続されている鍵サーバから、所与の受信者の公開鍵を取得することもできる。公開鍵の信憑性を保証し、これによって、起こり得るマンインザミドル攻撃を無効化するために、信頼できる認証局によって署名された証明書を付けて公開鍵を送信者に提供してもよい。公開鍵が送信者のメッセージの宛て先である受信者のものであることを検証するために、該証明書を用いてもよい。

【０００６】
従業員が組織を離職した際、組織が該従業員のセキュア電子メールの権限を無効にすることができるように、いくつかの組織では、毎日一日の終わりに全従業員の公開鍵を自動的に失効させるように構成する場合もある。就業中の従業員の新たな公開鍵を毎日生成してもよく、これを公開鍵サーバに置くことによって、新たな公開鍵を公的に利用できるようにしてもよい。

【０００７】
公開鍵暗号化アルゴリズムを用いる暗号化は計算量が膨大になってしまう。このため、いくつかのシステムでは、ユーザが共有対称鍵をセキュアに交換するために、公開鍵暗号化を使用できるようにしている。対称鍵の交換後、セキュアな通信セッションをサポートするために、該対称鍵を用いてもよい。

【０００８】
公開鍵暗号化システムでは、メッセージを暗号化できるようになるためには、送信者はまずメッセージ受信者の公開鍵を取得しなければならない。ある送信者がポータブルコンピュータを持って旅行していて、そのコンピュータに一時的に記憶しておいた電子メールメッセージに返信したいと思ったとする。該メッセージを送った人物の公開鍵のコピーを送信者がまだ持っていない場合、送信者は公開鍵サーバから該公開鍵を取得する必要がある。しかし、送信者が電子メールへの返信メールを作成したいと思ったときに、送信者のポータブルコンピュータはネットワークに接続されていない場合もある。そのため、送信者はオンラインの公開鍵サーバにアクセスできず、メッセージ作成後すぐにこれを暗号化できない場合もある。送信者のコンピュータは盗まれる危険性もあるため、コンピュータ上の暗号化されてないメッセージを盗み見ることができる場合もある。

【０００９】
同一性ベースの暗号化スキームは公開鍵システムと異なる動作をする。同一性ベースの暗号化システムでは、送信者および受信者は、公開パラメータ情報と秘密鍵とを用いてセキュアに通信する。各ユーザは、メッセージを復号化するためのユーザの同一性に基づく一意の秘密鍵を持つが、暗号化および復号化プロセス中に使用する公開パラメータ情報を多くのユーザで共有することもできる。特定のユーザの電子メールアドレスなど、ユーザ固有の同一性情報が同一性ベースの暗号化アルゴリズムの入力の１つとして用いられる。このため、これらのスキームは「同一性ベースの」と呼ばれる。

【００１０】
適切な構成の１つでは、ユーザの電子メールアドレスまたは日付スタンプと連結したユーザの電子メールアドレスを各ユーザの識別に用いることもできる。このアプローチによって、現在オフラインであるために従来の公開鍵システムの公開鍵サーバにアクセスできない送信者であっても、ユーザの公開パラメータ情報を入手できれば、機密事項を含むメッセージをさらに迅速に暗号化することもできるのである。組織内の全ユーザが同一の公開パラメータ情報を共有することもできるため、たとえ送信者が受信者と以前に全く通信したことがない場合でも、多くの場合送信者は所与の受信者に対して用いる正しい公開パラメータ情報を入手することもできる。ネットワークにアクセスできる場合、暗号化されたメッセージを受信者に伝送することもできる。受信者は自身の秘密鍵を用いて該メッセージを復号化することができる。

【００１１】
同一性ベースの暗号システムでは、秘密鍵生成器によって秘密鍵を生成してもよい。秘密鍵を生成する際に、秘密鍵生成器は秘密情報（すなわち、いわゆる「マスタシークレット」）を入力として用いる。システムのセキュリティは、マスタシークレットを保有している組織がその機密性を維持する能力にかかっている。
【００１２】
同一性ベースの暗号システムでは、マスタシークレットの機密性を維持することが重要なため、ある組織ではマスタシークレットを保管する責務を第三者に依託することを望まない場合もある。この結果、システムには、固有のマスタシークレットをそれぞれが持っている秘密鍵生成器が複数存在する場合もある。
【００１３】
複数の秘密鍵生成器が存在するか、あるいはユーザが複数の秘密鍵を持つ他の機会が存在する同一性ベースの暗号化環境では、ユーザが所与のメッセージの復号化に用いるべき正しい秘密鍵の位置を特定することは難しい場合もある。
【発明の開示】
【課題を解決するための手段】
【００１４】
（発明の要旨）
本発明に従って、通信網においてメッセージをセキュアに交換することができるシステムを提供する。メッセージを暗号化するために、同一性ベースの暗号化技術を用いてもよい。該システムは、同一性ベースの暗号化の秘密鍵生成器を複数持つこともできる。各秘密鍵生成器は、各生成器に固有のマスタシークレットを持つこともでき、各生成器に固有の関連する公開パラメータ関連情報を生成することもできる。時折、秘密鍵生成器は様々なバージョンの公開パラメータ情報と、これに対応する様々なバージョンの適合する秘密鍵とを生成することもできる。
【００１５】
該システムのユーザが２つ以上の秘密鍵生成器と関連を持つ場合もある。例えば、ユーザは自身の銀行において、ある秘密鍵生成器と関連を持つこともできるし、自身の雇用主において、別の秘密鍵生成器と関連を持つこともできる。この種の構成を用いると、銀行の秘密鍵生成器からユーザが受け取る秘密鍵は、雇用主の秘密鍵生成器からユーザが受け取る秘密鍵とは異なるマスタシークレットから生成されることとなり、したがって、ユーザは複数の秘密鍵を持つようになる。
【００１６】
個々のユーザに関連付けられている複数の秘密鍵が存在する場合、メッセージの受信者は、所与のメッセージの復号化にどの秘密鍵を用いるべきか判断するために、受信メッセージとともに提供される情報を処理することもできる。必要に応じて、送信者は、受信者がどの秘密鍵を使用すべきかを判断するために使用可能な秘密鍵識別情報を受信者に提供することもできる。
【００１７】
一例として、暗号化されたメッセージの送信者は、メッセージとともに、自身がメッセージを暗号化するために入力として用いた公開パラメータ情報の生成に、どの秘密鍵生成器が使用されたのかを特定する情報を提供することもできる。例えば、該情報は、サーバ名、ＩＰアドレスなどによって、秘密鍵生成器を識別する情報であってもよい。この例では、識別された秘密鍵生成器は、送信者がメッセージの暗号化に用いた公開パラメータ情報を作成するために使用されたものである。したがって、この識別された秘密鍵生成器は、受信者が該メッセージを復号化するために用いるべき対応する秘密鍵を生成するのに適した秘密鍵生成器となる。このように、適切な秘密鍵を取得するために、受信者は秘密鍵生成器を識別する情報を用いることもできる。
【００１８】
別の例として、「バージョン」付きの公開パラメータ情報が生成される環境では、メッ

セージとともに秘密鍵の識別情報を提供し、使用すべき適切な秘密鍵（すなわち、暗号化中に用いられた公開パラメータ情報のバージョンに対応する秘密鍵）を受信者が識別する手助けをすることもできる。

【００１９】

通信網において秘密鍵生成器から秘密鍵を取得することもできる。また、秘密鍵をローカル（例えば、受信者の装置の秘密鍵データベース）に記憶させることもできる。送信者から受け取った秘密鍵の識別情報を用いて、メッセージを復号化するために用いる適切な秘密鍵を受信者が取得するのを支援してもよい。例えば、秘密鍵の識別情報を用いて、コンタクトを取るべき正しい秘密鍵生成器を、またはメッセージの暗号化に用いられた正しいバージョンの公開パラメータ情報を受信者が識別するのを手助けしてもよい。秘密鍵の識別情報を用いて、適切な秘密鍵をローカルで（以前に記憶されていれば）取得してもよいし、あるいは通信網上で秘密鍵生成器から取得してもよい（その後、次回の復号化のためにローカルに記憶させてもよい）。

【００２０】

必要であれば、電子メールメッセージの受信者フィールドに、秘密鍵の識別情報を提供してもよい。例えば、電子メールメッセージの受信者フィールドに含まれる鍵情報フィールドの一部として、所与の秘密鍵生成器を実装するために用いられているサーバの名前または公開パラメータのバージョン番号情報を提供することもできる。また、公開パラメータ情報そのものなど、その他の情報を受信者情報フィールドに提供することもできる。

【００２１】

ハッシュ関数を用いて、鍵情報フィールドに含まれる情報を変換することもできる。この構成は、鍵サーバの同一性情報、ユーザがセキュア電子メール（ユーザの通常の電子メールアドレスとは異なる場合もある）を送るためだけに使用することができる特別な「暗号化」同一性情報など、鍵情報フィールドに含まれる機密情報である可能性もある情報を隠蔽するのに役立つ場合もある。また、ハッシュ関数の出力は通常、入力よりも短くなるため、ハッシュ関数を用いるアプローチでは鍵情報フィールドが短くなりやすい。

【００２２】

メッセージの暗号化に用いられる同一性ベースの暗号化の暗号技術に、受信者の電子メールアドレス、有効期間を連結した受信者の電子メールアドレス、またはその他の適切な受信者識別子など、受信者識別子情報に基づく同一性ベースの暗号化の公開鍵を用いてもよい。また、暗号化中に使用される公開鍵は、公開パラメータのバージョン番号、秘密鍵生成器の識別情報など、他の情報に基づくものであってもよい。

【００２３】

本発明の更なる特徴、本質、および種々の利点は添付の図面ならびに以下の好ましい実施形態の詳細な説明から、明確になるであろう。

【発明を実施するための最良の形態】

【００２４】

（好ましい実施形態の詳細な説明）

図１に、本発明に従った例示的な同一性ベースの暗号化の暗号システム１０の一部を示す。システム１０において、同一性ベースの暗号化スキームを用いて、様々な場所にいるユーザがセキュアに通信することができる。システムのユーザは、個人、組織、あるいはその他の任意の適切な者またはエンティティであってもよい。ユーザは、ユーザ装置デバイス１２を用いて相互に通信することもできる。例えば、装置１２には、パーソナルコンピュータ、ポータブルコンピュータ、メインフレームコンピュータ、ネットワークでつながれたコンピュータまたは端末、電気通信装置、ハンドヘルドコンピュータまたはパーソナルデジタルアシスタント、あるいは携帯電話などのコンピューティング装置を含めることもできる。複数のユーザが同一のデバイスを使用してもよい。例えば、ユーザの集合は、ローカルエリアネットワークでホストコンピュータに接続されている１台のコンピュータ端末を共同で使用することもできる。これらは、システム１０のユーザが使用可能であるプラットフォームの種類の単なる具体例に過ぎず、必要であれば、ユーザ装置１２は任

意の適切な電子装置を基づくものであってもよい。

【００２５】

ユーザ装置デバイスは通信網１４によって相互に接続されてもよい。例えば、ネットワーク１４はインターネット、ローカルエリアネットワーク、ワイドエリアネットワーク、公衆交換電話網、仮想プライベートネットワーク、有線ネットワーク、無線ネットワーク、専用回線、光ファイバでつながれている経路またはケーブルでつながれている経路あるいは他の有線または無線の経路を基盤としたネットワーク、もしくはその他の任意の適切なネットワーク技術またはこのようなネットワークの組み合わせを用いて形成されているネットワークであってもよい。

【００２６】

同一性ベースの暗号化スキームの特徴をサポートするために、種々のコンピューティングデバイスをネットワーク１４に接続することもできる。例えば、秘密鍵生成器１６にあるコンピューティング装置を用いて、秘密鍵を配布してもよい。いくつかの構成において、クライアントサーバアーキテクチャのサーバの機能を提供するために、このようなコンピューティング装置を用いることもできる。明確にするために、時にはこのようなサーバベースの構成に即して、本発明を説明することとする。しかしながら、これは単なる例示に過ぎず、必要であれば、システム１０において暗号化通信をサポートするための秘密鍵および他の情報の配布に、任意の適切なコンピューティングデバイスの構成を用いてもよい。通常のサーバベースの構成では、サーバの機能を提供するために１台以上のコンピュータを使用することもできる。サーバは、１台のコンピュータ用いて形成される場合もあるし、あるいは複数のコンピュータを用いて形成される場合もある。必要であれば、物理的に異なる複数の場所に分散しているコンピュータによって、１台のサーバの機能を提供することもできる。

【００２７】

秘密鍵生成器１６は、通信網１４に接続されているサーバベースのプラットフォームなど、適切なコンピューティングプラットフォームを基盤とするものであってもよい。必要であれば、１つ以上の場所にある複数のコンピュータ（各コンピュータが秘密鍵を生成するのに必要な秘密情報の一部だけを持つこともできる）間で、秘密鍵生成器１６の鍵生成機能を分割してもよい。明確にするために、本論考は主に秘密鍵生成器の構成に焦点を当てることとする。該構成において、各秘密鍵生成器１６は、各生成器に固有に関連付けられたユーザに対して各生成器に固有の秘密鍵を個別に生成する。

【００２８】

個人間での電子メールメッセージの送信など、いくつかのユーザ活動は手動で行う必要がある。例えば、このようなメッセージを送信したいと思う人物は、メッセージを暗号化して適切な受信者に送る前に、メッセージを作成しなければならない。

【００２９】

システム１０における他のユーザ活動を自動化したり、あるいは半自動化したりすることもできる。これらのユーザ活動は手動操作をほとんど介さずに、あるいは全く介さずに行われる場合もある。単なる一例として、デバイス１２のユーザは、通信網１４上で暗号化通信を使用し、他方のデバイス１２の口座名義人に対して暗号化された銀行取引明細の配送を所望する銀行であってもよい。配布プロセスを自動化してもよい。これによってシステムが適切にセットアッされてしまえば、銀行の装置では通常オペレータを介する必要がなくなる。また、ユーザによる取引明細書の受け取りも自動化することができる。

【００３０】

多くの異なる暗号アルゴリズムを用いて、同一性ベースの暗号化スキームを実装することができる。このようなスキームの１つが平方余剰に基づくものである（例えば、「An Identity Based Encryption Scheme Based on Quadratic Residues,」 Eighth IMA International Conference on Cryptography and Coding, Dec. 2001, Royal Agricultural Co

llege, Cirencester, UK, by Clifford Cocksを参照のこと）。別の適切なスキームは楕円曲線に基づくものである（例えば、「Identity－Based Encryption from the Weil Pairing,」 by Dan Boneh and Matthew Franklin, extended abstract in AdVances in Cryptology － Crypto 2001, Lecture Notes in Computer Science, Vol. 2139, Springer－Verlag, pp. 231－229, Aug. 2001.また、http：／／eprint.iacr.org／2001／090 by Dan Boneh and Matthew Franklinも参照のこと)。BonehおよびFranklinの研究で説明されているアプローチを用いると、同一性ベースの暗号化は、ベイユペアリング（Weil Pairing）またはテイトパーリング（Tate Paring）などの双線形写像の性質に基づいたものになる。明確にするために、例えばBonehおよびFranklinによって説明された楕円曲線を実装する同一性ベースの暗号化に即して、本発明の態様を説明する場合もある。しかしながら、これは単なる例示に過ぎず、必要であれば、システム１０とともに同一性ベースの暗号化の任意の適切なアプローチを用いてもよい。

【００３１】

一方のデバイス１２の送信者から別のデバイス１２の受信者へ送られるメッセージは、セキュアな方法で電子的に伝えられるものであればいかなるデジタル情報（例えば、テキスト、グラフィック、オーディオ、ビデオ、コマンド、実行可能なコード、データなど）であってもよい。システムがセットアップされると、図１の秘密鍵生成器１６は最初に、マスタシークレットｓを取得したり、あるいは生成したりする。例えば、秘密鍵生成器は、不正操作ができない格納装置内に格納されているプロセッサによって、秘密鍵生成器においてランダムに生成される番号からマスタシークレットを作成することもできる。また、マスタシークレットを別の場所で作り、秘密鍵生成器１６に配送することもできる。マスタシークレット（時には、秘密マスタ鍵またはマスタ鍵とも呼ばれる）は秘密情報である。秘密鍵生成器は、これを生成または取得後、このマスタシークレットを使用して、システムの受信者がメッセージの復号化に用いる秘密鍵を生成したり、また送信者がメッセージの暗号化に用いる公開パラメータ情報を生成したりする。

【００３２】

マスタシークレットｓの取得後、秘密鍵生成器は公開パラメータ情報を生成する。Boneh等の前述の研究の同一性ベースの暗号化アプローチにおいて生成される公開パラメータ情報は、公開パラメータＰとｓＰとを含む。秘密鍵生成器によって（例えば、乱数発生器を用いて）パラメータＰを最初に生成してもよい。その後、秘密鍵生成器によってパラメータｓＰを生成してもよい。BonehおよびFranklinの研究のｓとＰの「乗算」は、楕円曲線上の点と整数との乗算を用いることによって行われる。乗算（ｓＰの算出）は容易であるが、逆算（既知のＰとｓＰからｓを求めること）は実質的に不可能である。

【００３３】

公開パラメータ情報（例えば、楕円曲線に基づく同一性ベースの暗号化プロセスでは、パラメータＰとｓＰ）は数字であってもよい。一般に、数字、文字、シンボルおよび情報を表現する他のこのようなスキームは等価である。時にはある種の情報（例えば、マスタシークレットまたは公開パラメータ）は数字の形で記載される場合もあるだろうし、また時にはある種の情報（例えば、ユーザの同一性）は少なくとも一部が文字の形（例えば、電子メールアドレスの形）で記載される場合もある。これらの表現の異なるスキームは本来等価であるため、本明細書中では、文字またはシンボルから数字への変換に関連する技術、複数の数字または文字列を1つの数字として表す技術、あるいは他のこのような操作を詳しく説明しない。

【００３４】

公開パラメータ情報（例えば、公開パラメータＰとｓＰ）を求めた後、秘密鍵生成器によってこの情報を公開してもよい。例えば、秘密鍵生成器１６にあるコンピューティング装置（例えば、サーバ）を用いて、通信網１４上でこの情報を利用可能にしてもよい。公開パラメータ情報を電子メールでユーザに送ることもできる。必要であれば、公開パラメータ情報を要求に応じてユーザに提供する（例えば、サーバからダウンロードすることによって、メッセージの形で、あるいはその他の任意の適切な構成を用いることによって）こともできる。ダウンロード可能なソフトウェアモジュールまたはパッケージの一部として、あるいはプリインストールされているソフトウェアモジュールまたはパッケージの一部として、公開パラメータ情報（例えば、公開パラメータＰとｓＰ）を配布することもできる。例えば、電子メールアプリケーション、ウェブブラウザ、もしくはユーザのパーソナルコンピュータまたは他のユーザ装置１２とともに配布されるか、あるいは後刻にダウンロードされる（例えば、プラグインまたはスタンドアロンのパッケージの形で）その他の通信用アプリケーションまたはインターネット用アプリケーションに、公開パラメータ情報を組み込むこともできる。

【００３５】

公開パラメータ情報が２つ以上のパラメータを含む場合、パラメータを同時に配布してもよいし、あるいは個別に配布してもよい。例えば、パラメータＰとｓＰとを同時に配布してもよいし、あるいは個別に配布してもよい。パラメータＰおよびｓＰを個別に配布する場合、異なる配布メカニズムを用いて各パラメータを配布することもできる。例えば、Ｐをユーザのソフトウェアに盛り込むこともでき、ｓＰをインターネットで配布することもできる。さらに、ＰとｓＰを結合して、これらに相当する１つの番号またはパラメータを形成してもよいし、あるいはＰとｓＰをさらに分割してもよい（例えば、３つ以上の公開パラメータのサブパーツを作るように）。必要であれば、公開パラメータ情報（例えば、公開パラメータＰとｓＰ）を手動で（例えば、手紙によって、あるいはディスケットまたはコンピュータで読み取りが可能な他の媒体をユーザに配布することによって）配布してもよい。

【００３６】

システム１０には、複数の秘密鍵生成器があってもよい。さらに、秘密鍵生成器は、複数のバージョンの公開パラメータ情報（例えば、異なるＰの値、すなわち$P_{VERSION-1}$、$P_{VERSION-2}$などに基づいて）を生成してもよい。前述の配布技術のいずれか、またはこのような技術の組み合わせ、あるいはその他の適切な配布技術を用いて、様々なバージョンを持つ各秘密鍵生成器の公開パラメータ情報を配布してもよい。これらの配布方法は単なる例示に過ぎず、必要であれば、公開パラメータ情報を公開するために任意の適切な技術を用いてもよい。

【００３７】

別のユーザ（すなわち、受信者）へ暗号化されたメッセージを送信したいと思っているユーザ（すなわち、送信者）に公開パラメータ情報（例えば、公開パラメータＰおよびｓＰ）が提供されると、送信者はメッセージを暗号化して受信者に送ることもできる。受信者が暗号化されたメッセージを受け取ったときに、あるいはメッセージを受け取る以前、すなわち受信者が自分の位置にある装置をセットアップしたときまたは更新したときなどに、受信者は秘密鍵生成器から自身の秘密鍵を取得する。

【００３８】

送信者側の暗号化プロセスでは、入力として（１）公開パラメータ情報、および（２）受信者の同一性に基づく公開鍵Ｑを用いるため、このような暗号化は同一性ベースの暗号化（ＩＢＥ：Ｉｄｅｎｔｉｔｙ－Ｂａｓｅｄ　Ｅｎｃｒｙｐｔｉｏｎ）と呼ばれている。ユーザの同一性を任意の適切な文字列、数字、またはシンボルによって表してもよい。例えば、受信者の電子メールアドレス、名前、また社会保障番号によって、メッセージ受信者の同一性を表すこともできる。従来の公開鍵暗号スキームでは、目的の受信者のＲＳＡ公開鍵を取得するのに様々な煩わしさが必ず伴う。ＩＢＥスキームの利点は、送信者は通常このような煩わしさが伴うことなく目的の受信者の同一性（例えば、電子メールアドレ

ス）を求めることができることである。例えば、ＩＢＥ公開鍵は、ユーザの電子メールアドレスと同一の（または、これに基づく）ものであってもよく、これは容易に取得可能である。

【００３９】

秘密鍵生成器１６は、該秘密鍵生成器に関連付けられている複数のユーザそれぞれに対して、これらのユーザそれぞれの公開鍵（Ｑの）に基づいて（すなわち、ユーザの同一性に基づいて）秘密鍵を生成することもできる。

【００４０】

システム１０で用いる公開鍵Ｑの形式は所望される安全対策に依存する。例えば、ユーザの同一性（すなわち、電子メールアドレス）だけでなく有効期間情報にも基づくＱの値を形成するために、有効期間（例えば、現在の年月日、現在の月、２００３年１月２日－２００３年１月１０日などの開始および終了年月日、あるいは、その他の任意の適切な時間関連の日付スタンプ情報などの日付または期間）を各ユーザの電子メールアドレスに自動的に連結することによって、システム１０でユーザの権限が自動的に失効するようにもできる。

【００４１】

別の例として、公開鍵Ｑ（すなわち、Ｑ＝ｊｏｅ＠ｎａＶｙ．ｃｏｍ｜ｔｏｐ＿ｓｅｃｒｅｔなど）を形成する際に、セキュリティクリアランスレベル情報を各ユーザの電子メールアドレスと連結するか、または別の方法で付加することによって、セキュリティクリアランスレベルに基づいて、ユーザの権限を制限することもできる。これらのアプローチは、各ユーザ用の公開鍵（例えば、各ユーザ用のＱ）を形成する際に、ユーザの電子メールアドレスなどのユーザ同一性に追加の基準を付加できる方法の単なる例示であって、必要であれば、公開鍵を形成するために任意の適切なアプローチを用いてもよい。

【００４２】

所与の受信者に対して暗号化されたメッセージを送信したいとき、送信者は通常、受信者の同一性（例えば、受信者の電子メールアドレス）を知っておく必要がある。また、場合によっては、追加の公開鍵情報（例えば、有効期間、セキュリティレベルなど）からユーザの公開鍵Ｑを構築する方法も知っておく必要がある。さらに、送信者は、公開パラメータ情報（例えば、ＰとｓＰ）を取得する必要もある。メッセージを伝送する前に、送信者は、受信者に宛てたメッセージのコンテンツを暗号化するために、同一性ベースの暗号化（ＩＢＥ）プロセス（例えば、前述のＢｏｎｅｈおよびＦｒａｎｋｌｉｎの研究のプロセス）を用いてもよい。ＩＢＥプロセスでは、入力として（１）暗号化するメッセージ、（２）公開パラメータ情報（例えば、ＰとｓＰ）、および（３）メッセージが送られる所与の受信者の同一性に基づく公開鍵Ｑを取り込むこともできる。ＩＢＥプロセスは出力として、暗号化されたバージョンのメッセージを作る。

【００４３】

通信網１４上で、送信者が受信者に暗号化されたメッセージを伝送した後、該受信者はこれを受け取り、受け取ったメッセージを適切な秘密鍵を用いて復号化してもよい。メッセージの復号化に用いられる秘密鍵は、メッセージを暗号化する際に用いられた同一性ベースの暗号化の公開鍵Ｑと公開パラメータ情報（例えば、ＰおよびｓＰ）とに関連する。メッセージの復号化には、公開鍵に適合する秘密鍵のみを用いてもよい。秘密鍵を生成するためには、マスタシークレットｓを知っておく必要がある。そのため、秘密鍵生成器１６のみが受信者の公開鍵Ｑに基づく受信者の秘密鍵を生成することができる。

【００４４】

適切なアプローチの１つでは、ｓＱの値を算出するために適切な数学関数（例えば、楕円曲線上の点と整数との乗算）を用いることによって、受信者の同一性Ｑとマスタシークレットｓとから受信者用の秘密鍵を生成してもよい。秘密鍵を受信者に発行する前に、受信者からの認証情報を用いて受信者の同一性を検証することもできる。

【００４５】

任意の適切な手動または自動の認証技術を用いてもよい。例えば、受信者の公的なレタ

ーヘッドについての手紙を秘密鍵生成器１６へファックスあるいは郵便で送るように受信者に求め、担当者または秘密鍵生成器の自動化された装置が、認証のために該レターヘッドを検査してもよい。別の例として、バイオメトリック識別技術（例えば、指紋分析、目のスキャニング、掌紋または声紋分析、顔認証方法、または、対面の身元確認）を用いることもできる。認証プロセスに受信者と秘密鍵生成器との間の電気通信が伴う場合、受信者と秘密鍵生成器との間の通信経路はセキュアなものでなければならない。信頼できない者が通信経路を使用できない場合、該通信経路をセキュアなものとみなすこともできる。例えば、秘密鍵生成器１６と受信者との間のネットワークは、秘密鍵生成器または別の信頼できるエンティティによって制御されているプライベート回線であってもよい。別の例として、セキュアなウェブブラウザリンク用いて（例えば、セキュアソケットレイヤプロトコルを用いて）、セキュアなチャンネルをサポートすることもできる。

【００４６】

秘密鍵生成器１６が受信者の同一性を認証して該受信者の秘密鍵を生成する方法はどのようなものであってもよいが、受信者には、メッセージの復号化に使用する該秘密鍵が提供されなければならない。受信者に秘密鍵を提供するために、任意の適切な技術を用いてもよい。例えば、電子メールまたは他の適切なメッセージで、受信者に秘密鍵を伝送してもよい。また、インターネット上で、該秘密鍵をダウンロード（スタンドアロンのダウンロードが可能なアプリケーションまたはダウンロード可能なプラグインモジュールの一部として、あるいは、スタンドアロンの鍵として、など）できるようにしてもよい。秘密鍵生成器１６と受信者の装置１２との間の電気通信に、セキュアな通信チャネルを用いることもできる。必要であれば、受信者の装置に秘密鍵をプリインストールしてもよく、こうすると、受信者が該装置を初めて使う際に、受信者はこの秘密鍵を使用することができる。また、郵便または宅配便によって（例えば、コンピュータディスクまたはメモリチップなどのコンピュータで読み取り可能な媒体に記録して）秘密鍵を配布することもできる。

【００４７】

必要であれば、受信者は秘密鍵をローカルに（例えば、受信者の装置の記憶回路またはハードドライブなどのストレージデバイス上のデータベースに）記憶させてもよい。秘密鍵をローカルに記憶させておけば、受信者は次回メッセージを復号化する必要が生じたときに、この秘密鍵を検索することができ、通信網上で秘密鍵の新たなコピーを取得するために、秘密鍵生成器にコンタクトを取る必要はない。秘密鍵がローカルに置かれていない場合は、以前に記憶された秘密鍵生成器についてローカルリストを調べたり、ディレクトリにリストアップされている秘密鍵生成器を調べたり、メッセージとともに提供された情報に基づいて１つ以上の秘密鍵生成器とコンタクトを取ったり、あるいは、その他の任意の適切な技術を用いたりして、受信者は適切な秘密鍵生成器から秘密鍵を取得することもできる。

【００４８】

復号化および暗号化のプロセスの効率をよくするために、２段階の復号化技術を用いてもよい。該技術では、受信者に伝送する前に、メッセージのコンテンツを暗号化するために、メッセージ鍵（例えば、対称メッセージ鍵）を用いる。その後、この対称メッセージ鍵を暗号化するためにＩＢＥプロセスを用いる。送信者から受信者に送られるメッセージは、ＩＢＥで暗号化されたメッセージ鍵とメッセージ鍵で暗号化されたメッセージのコンテンツとを含む。受信者側で、受信者はＩＢＥ秘密鍵を用いてメッセージ鍵を復号化し、次に受信者は該メッセージ鍵を用いて残りのメッセージを復号化することもできる。

【００４９】

「純粋な」または「一段階の」同一性ベースの暗号化アルゴリズムでは、該ＩＢＥアルゴリズムを単独で用いて、メッセージペイロード全体を暗号化する。しかし、該アルゴリズムは計算量が膨大になることがある。例えば、純粋な同一性ベースの暗号化スキームでは、おおよそ１０００バイト／秒のレートでデータを暗号化することができる一方で、ＤＥＳ３（３－ＤＥＳ－－データ暗号化標準（Ｄａｔａ　Ｅｎｃｒｙｐｔｉｏｎ　Ｓｔａｎｄａｒｄ））などの対称暗号化アルゴリズムでは、およそ１００メガバイト／秒のレート

でデータを暗号化することができる。さらに、純粋なＩＢＥアルゴリズムを用いた場合、ＩＢＥで暗号化されたデータブロックのサイズは、暗号化されていないバージョンの同一データブロックよりも何オーダも大きくなることもある。したがって、送信者と受信者とが対称メッセージ鍵などのメッセージ鍵をセキュアに交換できるようにするために、２段階の同一性ベースの暗号化スキームを用いることが望ましい場合もある。この種の２段階のＩＢＥ暗号スキームでは、ＩＢＥを用いてメッセージ鍵をセキュアに交換する一方で、効率のよいメッセージ鍵暗号プロセス（例えば、３－ＤＥＳまたはアドバンストエンクリプションスタンダード（ＡＥＳ：ＡｄＶａｎｃｅｄ　Ｅｎｃｒｙｐｔｉｏｎ　Ｓｔａｎｄａｒｄ）)を用いて、大部分のメッセージデータの暗号化および復号化をする。

【００５０】

２段階の暗号化法では、「純粋な」ＩＢＥと効率のよい暗号化技術（例えば、３－ＤＥＳまたはＡＥＳなどの対称鍵暗号化技術）とを組み合わせて用いる。２段階の暗号化法は、システム１０の全体的なＩＢＥ暗号化の効率を改善させることができる。明確にするために、本明細書中では、時にはこのようなハイブリッドのあるいは「２段階の」ＩＢＥ暗号化スキームを単に「同一性ベースの暗号化」スキーム、または「ＩＢＥ」スキームという場合もある。同様に、本明細書中では、時には純粋なＩＢＥスキーム（このスキームではＩＢＥのみが暗号化および復号化に用いられる）を「同一性ベースの暗号化」、または「ＩＢＥ」スキームという場合もある。

【００５１】

２段階のＩＢＥアルゴリズムでは、データ暗号化における効率化のためにメッセージ鍵暗号化技術（例えば、３－ＤＥＳ技術または他の対称鍵技術）を選択することができる。これによって、２段階のＩＢＥアルゴリズムような混合アルゴリズムでは、ＩＢＥ暗号化アルゴリズムを用いてすべてのメッセージデータを暗号化する「純粋な」ＩＢＥ暗号化法を用いた場合に比べ、効率を大幅に改善することができる。以下に詳述する適切な２段階のアプローチの１つでは、暗号化されたメッセージ鍵フィールドにＩＢＥで暗号化されたメッセージ鍵を含ませて、メッセージの受信者に伝送することもできる。

【００５２】

図２に示すように、システム１０には２つ以上の秘密鍵生成器１６があってもよい。例えば、様々な機関（例えば、様々な銀行、仲買店、企業、軍事基地、政府の支局、教育機関など）はそれぞれ、関連する秘密鍵生成器を個別に持つこともできる。一般に、各秘密鍵生成器は各生成器に固有のマスタシークレットと、各生成器に固有の公開パラメータ情報（例えば、ＢｏｎｅｈおよびＦｒａｎｋｌｉｎの前述の研究で説明されている種類のアプローチを用いる環境においては、各生成器に固有の公開パラメータ情報ＰとｓＰのセット）とを持つ。

【００５３】

送受信者間で適切な通信を行うために、送信者および受信者の動作を調整する必要がある。特に、送信者はメッセージの暗号化をする際に、受信者が秘密鍵を取得するために使用する秘密鍵生成器と同一の秘密鍵生成器に由来する公開パラメータ情報を用いる必要がある。システム１０において、任意の所与のユーザに関連付けられている可能な秘密鍵生成器１６が複数存在する場合、所与のユーザにどの秘密鍵生成器が関連付けられているのかを送信者に知らせるために、ディレクトリまたは他の適切なメカニズムを提供することが有益である。

【００５４】

例えば、所与の受信者宛てのメッセージを適切に暗号化するために、送信者は、ネットワーク１４に接続されているディレクトリサービス１８または他の適切な装置を調べて、該受信者の秘密鍵生成器の所属を調査することもできる。例えば、送信者が、関連する秘密鍵生成器を持つ組織のメンバに対して暗号化されたメッセージを送信したい場合、この送信者はディレクトリ１８を調べて、該組織のメンバ用秘密鍵生成器情報の位置を特定してもよい。この情報は、名前またはインターネット上の位置、あるいはその他の適切な識別子によって、秘密鍵生成器の識別をすることもできる。次に、送信者はこの識別情報を

用いて、この秘密鍵生成器（または、その他の適切なソース）にコンタクトを取り、該受信者宛てのメッセージを暗号化する際に用いる適切な公開パラメータ情報を取得することもできる。必要であれば、適切な公開パラメータ情報そのものをディレクトリ１８に直接提供することもできる。

【００５５】

この種のディレクトリ構成によって、送信者は、所与のユーザに宛てたメッセージの暗号化にどのＩＢＥ公開パラメータ情報を用いるべきか判断できるようになる。また、別の適切な構成を用いて公開パラメータ情報を公開することによって、これを配布することもできる。送信者のメッセージを暗号化するために用いる適切な公開パラメータ情報（例えば、パラメータＰとｓＰ）は、目的の受信者のＩＢＥ秘密鍵（ｓＱ）を生成するために使用されたマスタシークレットと同一のマスタシークレット（ｓ）を用いて生成された公開パラメータ情報である。公開パラメータ情報と秘密鍵との間に対応がある場合、ＩＢＥスキームを用いてメッセージを適切に暗号化および復号化できる。

【００５６】

システム１０のいくらかのユーザは２つ以上の秘密鍵生成器と関連を持つこともできる。例えば、あるユーザは第１の秘密鍵生成器を持つ銀行からＩＢＥで暗号化された通信を受ける場合もあるし、また第２の秘密鍵生成器を持つ雇用主からＩＢＥで暗号化された通信を受ける場合もある。

【００５７】

この種の複数の秘密鍵生成器を有する環境では、受信者は、複数の秘密鍵を持つこともでき、そのため、どの秘密鍵が所与の受信メッセージを復号化するために用いるべき正しい秘密鍵であるのか判断しなければならない場合もある。

【００５８】

さらに、複数の秘密鍵生成器を備えるシステム環境では、メッセージ送信者はメッセージを暗号化する前に、どの公開パラメータ情報が使用に適した公開パラメータ（例えば、銀行の秘密鍵生成器に関連する公開パラメータ情報、雇用主の秘密鍵生成器に関連する公開パラメータ情報、あるいは他のエンティティに関連する公開パラメータ情報）であるのか通常判断する必要がある。

【００５９】

送信者は、ユーザのディレクトリ（例えば、ディレクトリ１８などのディレクトリ）に含まれる目的の受信者についての情報を調査することによって、メッセージの暗号化に用いる公開パラメータを判断することもできる。また、送信者は秘密鍵生成器から、受信者から、あるいはその他の適切なソースから、使用すべき適切な公開パラメータ情報についての情報を取得することもできる。

【００６０】

受信者がメッセージを受け取ると、受信者は自身の各秘密鍵を用いてメッセージの復号化を試みることができる。これによって、更なる動作を伴わずにメッセージの復号化に成功することができる。しかし、時には多数のステップが必要となる場合（例えば、秘密鍵を取得するプロセスに、試みを行う度にポップアップパスワードウィンドウまたは他の認証ステップに応答するなどのユーザステップが伴う場合）もある。

【００６１】

必要であれば、受信者はディレクトリ内の秘密鍵生成器についての情報を調べることができる。一例として、受信者が復号化されたメッセージを受け取ると、ユーザはディレクトリにリストアップされている秘密鍵生成器のいくつか、あるいはすべてにおいて、適切な秘密鍵の取得を試みてもよい。このアプローチは、種々の秘密鍵生成器の数が多くないシステム１０で特に満足な結果を得ることができる。

【００６２】

別の適切な構成では、送信者は、メッセージとともに秘密鍵の識別情報を提供することによって、受信者が正しい秘密鍵の位置を特定するのを支援することもできる。受信者は、自身の秘密鍵のうちどれがメッセージの復号化に用いるべき正しい秘密鍵であるのかを

識別するために、この秘密鍵の識別情報を用いることができる。図３に、秘密鍵の識別情報２２を含む例示的なメッセージ２０の図を示す。

【００６３】

秘密鍵の識別情報２２として、送信者の電子メールアドレスについての情報など、メッセージ２０のヘッダに含まれる情報を用いることもできる。この場合、受信者は、送信者の電子メールアドレスによって提供される情報から使用すべき適切な秘密鍵を判断することもできる。例えば、送信元が自身の銀行であることがわかるメッセージを受信者が受け取ると（例えば、メッセージヘッダに含まれる送信者情報が受信者の銀行のものと一致すると）、受信者は、自身の銀行の秘密鍵生成器がメッセージに関連しており、また自身の秘密鍵のうちメッセージを復号化するために用いるべき適切な鍵は、銀行の秘密鍵生成器に関連する秘密鍵であることを推測することができる。銀行が受信者に宛てたメッセージを暗号化するために用いた公開パラメータ情報は、秘密鍵の生成に用いられた秘密鍵生成器と同一の秘密鍵生成器によって生成されているので、該秘密鍵を用いればメッセージを正しく復号化することができる。

【００６４】

送受信者間には、事前に関連が存在しない場合もあれば、あるいは通常のメッセージヘッダ情報から送信者の同一性を突き止めることが難しい場合もある。したがって、メッセージ２０とともに、他の種類の秘密鍵の識別情報を提供することが有効である場合もある。例えば、秘密鍵の識別情報として、暗号化されたメッセージに関連する秘密鍵生成器の名前を用いてもよい。テキスト文字列として、数字として、ネットワーク１４上で秘密鍵生成器１６の位置を特定するＵＲＬまたはＩＰアドレスとして、あるいは秘密鍵生成器１６を一意にまたは正確に識別するために使用可能なその他の任意の適切な識別子として、この名前を提供してもよい。この情報を用いると、所与のメッセージの受信者は適切な秘密鍵生成器１６の位置を容易に特定でき、該秘密鍵生成器から秘密鍵を請求することができる。その後、所与のメッセージの復号化に該秘密鍵を用いることができる。

【００６５】

図４に、システム１０において、セキュアなメッセージの送受をするための秘密鍵の識別情報の使用に関わる例示的なステップを示す。ステップ２４において、ＩＢＥで暗号化されたメッセージと、関連する秘密鍵の識別情報とを送信者側で生成する。例えば、メッセージペイロードを暗号化するためにメッセージ鍵を用いてもよいし、また、該メッセージ鍵を暗号化するためにＩＢＥ暗号化プロセスを用いてもよい。ネットワークで伝送されるメッセージは、暗号化されたメッセージペイロードと暗号化されたメッセージ鍵とから構成される。ＩＢＥ暗号化プロセスではメッセージ鍵を暗号化する際に、入力として、目的の受信者の公開鍵Ｑと、該受信者に関連付けられた所与の秘密鍵生成器から受け取る公開パラメータ情報とを用いてもよい。送信者はメッセージに秘密鍵の識別情報（例えば、関与する所与の秘密鍵生成器を具体的に識別するサーバ名または他の情報）を付加することもできる。

【００６６】

ステップ２６において、暗号化されたメッセージを、それに関連する秘密鍵の識別情報とともに送信者から受信者へ伝送することができる。

【００６７】

ステップ２８において、受信者は暗号化されたメッセージと秘密鍵の識別情報とを受け取ることができる。

【００６８】

ステップ３０において、受信者は、秘密鍵の識別情報を用いて、メッセージの復号化に自身のどの秘密鍵を用いるべきかを識別することができ、該秘密鍵の識別情報を用いて秘密鍵のコピーを取得することもできる。

【００６９】

例えば、秘密鍵の識別情報によって、メッセージの暗号化に用いられた（または、メッセージ鍵の暗号化に用いられた）ＩＢＥ公開パラメータ情報を生成するために用いられた

特定の秘密鍵生成器のネットワーク上での位置を識別することもできる。秘密鍵の識別情報によって、秘密鍵を直接的に（例えば、秘密鍵に直接関連する識別子によって）識別することもできるし、あるいは間接的に（例えば、秘密鍵に関連する秘密鍵生成器を識別することによって、または秘密鍵に関連する秘密鍵生成器に関連付けられた公開パラメータを識別することによって）識別することもできる。これらは単なる具体例に過ぎず、受信者が自身のどの秘密鍵を使用すべきかということを識別できるように、任意の適切な秘密鍵の識別情報を用いてもよい。

【００７０】

受信者側にあるローカル秘密鍵データベースから、特定された秘密鍵を検索してもよい。ローカルデータベースから該秘密鍵を入手できない場合、受信者は適切な秘密鍵生成器から該秘密鍵を取得してもよい。例えば、受信者は手動で、自動で、あるいは手動と自動のステップの組み合わせを用いて、ネットワーク１４上で適切な秘密鍵生成器１６にコンタクトを取り、該秘密鍵を取得してもよい。秘密鍵生成器は、適切な秘密鍵（例えば、受信者の同一性ベースのＩＢＥの公開鍵と該秘密鍵生成器のマスタシークレットとに基づく鍵ｓＱ）を生成する前に、受信者の同一性を認証し、受信者がメッセージの内容にアクセス権限を持つことを検証してもよい。必要であれば、受信者は秘密鍵を保存することもできる（例えば、ローカルの秘密鍵データベースに）。記憶装置、ハードドライブ、あるいは受信者の装置の他のローカルストレージを用いて、ローカル秘密鍵データベースを実装することもできる。同一の秘密鍵生成器に関連する新たなメッセージを受け取り受信者が秘密鍵を必要とするまで、記憶させた秘密鍵を保存しておいてもよい。

【００７１】

ステップ３２において、受信者（すなわち、メッセージを受信する装置１２）はメッセージを復号化するために、取得した秘密鍵を用いてもよい。純粋なＩＢＥの構成では、ＩＢＥで暗号化されたペイロードの復号化に該秘密鍵を用いることもできる。２段階のＩＢＥスキームでは、ＩＢＥで暗号化されたメッセージ鍵の復号化に該秘密鍵を用いることもできる。その後、メッセージ鍵で暗号化されたペイロードの復号化に、復号化されたメッセージ鍵を用いることもできる。

【００７２】

システム１０において交換されるメッセージは、インスタントメッセージ、電子メールメッセージ、またはその他の任意の適切な種類のメッセージであってもよい。図５に、例示的なメッセージフォーマットを示す。図５の例において、メッセージ２０は、ヘッダ３４、受信者情報ブロック３６、およびペイロード部３８を有する。ヘッダ３４は、受信者の電子メールアドレス情報、送信者の電子メールアドレス情報、件名情報、伝送日時情報などのプロトコルに固有の情報を含むことができる。ペイロード３８は、任意の適切なテキスト、メディア、コード、または他の内容であってもよい。メッセージ鍵（例えば、３－ＤＥＳ鍵またはＡＥＳ鍵などの対称メッセージ鍵）を用いて、ペイロードを暗号化してもよい。またＩＢＥを用いて、該メッセージ鍵を暗号化してもよい。ＩＢＥで暗号化されたメッセージ鍵を受信者情報ブロック３６に置くこともできる。

【００７３】

受信者情報ブロック３６は受信者情報フィールドを含み、該受信者情報フィールドはメッセージの各受信者に対して、鍵情報フィールド３６ａと、暗号化されたメッセージ鍵フィールド３６ｂとを有する。例えば、受信者が１人だけである場合、受信者情報ブロック３６には１つの鍵情報フィールドとこれに対応する１つの暗号化されたメッセージ鍵フィールドとを含ませてもよい。

【００７４】

暗号化されたメッセージ鍵フィールドに、ＩＢＥで暗号化されたメッセージ鍵を置くこともできる。複数の受信者がいる場合、各暗号化されたメッセージ鍵フィールド用にメッセージ鍵を個別に暗号化してもよい。例えば、受信者１の公開鍵と、秘密鍵生成器１から取得する公開パラメータ情報とに基づくＩＢＥを用いて、受信者１が使用するメッセージ鍵のコピーを暗号化してもよく、また一方で、受信者２の公開鍵と、秘密鍵生成器２から

取得する公開パラメータ情報とに基づくＩＢＥを用いて、受信者２が使用するメッセージ鍵のコピーを暗号化してもよい。結果として得られる暗号化されたメッセージ鍵を対応する暗号化されたメッセージ鍵フィールドに格納することもできる。どの受信者がどの受信者情報フィールドに関連付けられているのかを識別するために、各受信者フィールドに含まれる鍵情報フィールド３６ａを用いてもよい。必要であれば、受信者に関連付けられている鍵情報フィールドに各受信者用の秘密鍵の識別情報を提供することもできる。

【００７５】

図６に示すように、メッセージ２０は、標準的なＳ／ＭＩＭＥ（Ｓｅｃｕｒｅ Ｍｕｌｔｉｐｕｒｐｏｓｅ Ｉｎｔｅｒｎｅｔ Ｍａｉｌ Ｅｘｔｅｎｓｉｏｎｓ）電子メールメッセージに基づくフォーマットを用いる電子メールメッセージとすることができる。図６の図に示すように、メッセージ２０はＳ／ＭＩＭＥメールヘッダ３４を含んでもよい。送信者の同一性など、図５または図６のメールヘッダ３４に含まれる情報を秘密鍵の識別情報として用いることもできる。例えば、受信者は、ヘッダ３４のヘッダ情報を用いて、所与のメッセージが自身の銀行から送られたのかを判断することもできる。次に受信者はこの情報を用いて、ローカルストレージまたは自身の銀行の秘密鍵生成器から秘密鍵を取得してもよい。受信者情報ブロック３６に（例えば、各鍵情報フィールド３６ａに）秘密鍵の識別情報を提供することもできる。

【００７６】

メッセージ２０の暗号化コンテンツの位置（例えば、暗号文４４の位置）を識別するために、暗号文開始位置マーカ４０および暗号文終了位置マーカ４２を用いてもよい。必要であれば、メッセージ２０に添付物４６を１つ以上含め、必要に応じて該添付物を暗号化してもよい。

【００７７】

メッセージ２０に署名がしたければ、送信者は、デジタル署名ブロック４８にデジタル署名を置くことによって署名することもできる。送信者は任意の適切な技術を用いて、デジタル署名を生成してもよい。例えば、送信者は、受信者が秘密鍵に対応するＲＳＡ公開鍵で検証することのできるＲＳＡ秘密鍵を用いて、デジタル署名を生成してもよい。

【００７８】

メッセージ２０の暗号化にどの暗号化アルゴリズムまたはアルゴリズム類が使用されたのかを特定するアルゴリズム識別子を保持するために、アルゴリズム識別子ブロック５０を用いることもできる。例えば、アルゴリズム識別子によって、メッセージ鍵の暗号化にＩＢＥアルゴリズムバージョン２．２が使われていることと、メッセージペイロード暗号化アルゴリズムとして、メッセージのペイロードの暗号化に３－ＤＥＳ暗号化アルゴリズムが使われていること（すなわち、メッセージ鍵が３－ＤＥＳメッセージ鍵である）とを特定することもできる。他の例示的なアルゴリズムＩＤには、ＩＢＥ＋３－ＤＥＳ、ＩＢＥ＋ＡＥＳ、ＩＢＥＶ．３＋３－ＤＥＳ、ＩＢＥＶ．４＋３－ＤＥＳなどが含まれる。英数字の文字列、バイナリコード、あるいはその他の適切な表現を用いて、アルゴリズムＩＤを表現することもできる。各受信者に対して個別のアルゴリズム識別子エントリがあってもよいし、あるいはすべての受信者に対して使用されている暗号アルゴリズム（類）を特定するアルゴリズム識別子が１つあってもよい。必要であれば、アルゴリズム識別子ブロック５０のフォーマットはＳ／ＭＩＭＥ電子メール標準に従ってもよい。

【００７９】

図７の図は、送受信者間でセキュアなメッセージングをサポートするために、ＩＢＥ暗号技術をどのように使用することができるのかを示す。

【００８０】

適切なタイミングで（例えば、セットアッププロセスのとき、または後刻の受信者がメッセージを復号化する必要があるとき）、ＩＢＥ秘密鍵を受信者に提供することができる。例示的なアプローチの１つにおいて、受信者は秘密鍵を請求してもよく（ステップ１）、秘密鍵生成器１６から受信者に該鍵が配送されてもよい（ステップ２）。受信者は、秘密鍵データベース５２に秘密鍵を格納することもできる。メッセージを復号化する場合、

ネットワーク上での鍵の電子配送を請求する前に、受信者はデータベース５２に問い合わせて秘密鍵のローカルコピーの位置を特定してみることもできる。

【００８１】

メッセージを送信するために、送信者はメッセージ鍵（例えば、３－ＤＥＳまたはＡＥＳメッセージ鍵）を生成してもよい（ステップＡ）。次に、送信者は目的の受信者の公開パラメータ情報（例えば、公開パラメータＰとｓＰ）および目的の受信者のＩＢＥ公開鍵Ｑを取得する（ステップＢ）。公開パラメータ情報は、ディレクトリサービスによって、受信者に関連付けられた秘密鍵生成器によって、受信者によって、あるいはその他の任意の適切なエンティティによって、インターネット上で公開されてもよい。公開鍵は受信者の同一性に基づく。例えば、公開鍵は受信者の電子メールアドレスに基づくものであってもよい。システム１０に更なる安全対策を付加するために、公開鍵に追加情報を提供することもできる。例えば、電子メールアドレスに有効期間を付加して公開鍵を形成してもよい。

【００８２】

送信者は、自身の側で実行するＩＢＥ暗号化アルゴリズムへの入力としてＩＢＥ公開鍵とＩＢＥ公開パラメータとを用いて、メッセージ鍵を暗号化する（ステップＣ）。

【００８３】

メッセージ鍵（暗号化されていない形で）を用いて、メッセージペイロード（例えば、テキストまたはメディアファイル、コードなど）を暗号化する（ステップＤ）。

【００８４】

ステップＥでは、暗号化されたペイロードからメッセージを構成してもよい。受信者情報ブロックの暗号化されたメッセージフィールドにＩＢＥで暗号化されたバージョンのメッセージ鍵を置いてもよい。複数の受信者（各受信者は、各自に適切に対応する同一性ベースの公開鍵と、各情報が異なり得る公開パラメータ情報とを用いて暗号化されたメッセージ鍵を受け取ることもできる）にメッセージを宛てることもできる。受信者情報ブロックは複数の受信者情報フィールドを含んでもよく、各受信者情報フィールドは、各受信者情報フィールドに関連する暗号化されたメッセージ鍵フィールドのコンテンツにどの受信者が関連付けられているかを識別するための情報を含む。また、受信者情報フィールドには、複数存在し得る受信者の秘密鍵のうちどれを暗号化されたメッセージ鍵の復号化に用いるべきなのか受信者が識別できる情報（秘密鍵の識別情報）を含むこともできる。

【００８５】

ステップＦにおいて、メッセージを送ることができる。例えば、電子メールプログラムまたは電子メール機能を備えるアプリケーションを用いて、メッセージを送ってもよい。

【００８６】

ステップＧにおいて、受信者はメッセージを受け取ることができる。例えば、受信者は、電子メールプログラムまたは電子メール機能を備えるアプリケーションを用いて、メッセージを受け取ってもよい。

【００８７】

ステップＨにおいて、受信者は各受信者情報フィールド３６ａを検索し、フィールド内の情報のいずれかが自身のものと一致するか否かを判断することができる。一致しない場合、メッセージは該受信者に向けられたものではないので、破棄することができる。

【００８８】

一致する場合、受信者は、一致する鍵情報フィールドの情報のいくつかあるいはすべてを用いて、暗号化されたメッセージ鍵を復号化するために必要となる適切な秘密鍵を取得することができ（ステップＩ）、それによって、メッセージのコンテンツにアクセスすることができる（すなわち、受信者は鍵情報フィールドの秘密鍵の識別情報を用いて、適切な秘密鍵を取得することができる）。受信者は、データベース５２から事前に記憶されている秘密鍵を取得してもよいし、あるいは適切なＩＢＥ秘密鍵生成器１６から秘密鍵を取得してもよい。秘密鍵の識別情報には、データベース５２において受信者が正しい秘密鍵を識別したり、および／または、正しい秘密鍵生成器１６（例えば、複数の秘密鍵生成器

がある環境で）から正しい秘密鍵を請求したりする（ステップ１）のに十分な情報を含めることもできる。

【００８９】

ステップＪでは、受信者のＩＢＥ秘密鍵を用いて、該受信者の暗号化されたメッセージ鍵（受信者の暗号化されたメッセージ鍵フィールドから取得される）を復号化することができる。

【００９０】

ステップＫでは、復号化されたバージョンのメッセージ鍵を用いて、暗号化されたペイロード（例えば、図６の暗号文４４）を復号化することができる。これによって受信者はメッセージのコンテンツにアクセスできるようになる。

【００９１】

先に説明したように、メッセージ２０とともに秘密鍵の識別情報を送ることもできる。例えば、電子メールメッセージの鍵情報フィールド３６ａに、秘密鍵の識別情報と他のメッセージ情報とを提供することもできる。受信者情報フィールド３６、およびこれに関連する鍵情報フィールド３６ａと暗号化されたメッセージ鍵フィールド３６ｂに対して、任意の適切な構成を用いてもよい。図８ａ、８ｂ、８ｃ、８ｄ、８ｅ、および８ｆに、例示的な鍵情報フィールド３６ａを示す。メッセージ２０には、これらの例示的な鍵情報フィールド３６ａのいずれかを1つ以上含めることもできるし、あるいはその他の適切な受信者情報フィールドを１つ以上含めることもできる。通常、各鍵情報フィールド３６ａは特定の受信者に関連付けられており、受信者がこの関連を確認するのに十分な情報を含んでいる。受信者は自身に一致する鍵情報フィールド３６ａの位置を特定すると、メッセージペイロードを復号化するために、これに対応する暗号化されたメッセージ鍵フィールド３６ｂに提供された暗号化されたメッセージ鍵を用いることができる。

【００９２】

図８ａに示すように、メッセージ２０の鍵情報フィールド３６ａには、受信者の電子メール名に基づく受信者識別子情報を含むこともできる。例えば、受信者情報フィールド３６ａに、「ｂｏｂ＠ａｏｌ．ｃｏｍ」を置くこともできる。この種の受信者情報フィールド３６ａを用いる場合、各受信者は電子メール名情報を用いて、該フィールドに対応する暗号化メッセージ鍵のうちどれが自分用のものであるのか識別することもできる。

【００９３】

図８ｂに示すように、鍵情報フィールド３６ａの受信者識別子は、受信者の電子メールアドレスと有効期間との両方に基づくものであってもよい。有効期間は日付（例えば、２００３年２月１０日）、期間（例えば、２００３年１月２日－２００３年２月２２日）、あるいは、受信者が暗号化されたメッセージの内容を復号化する権限を持つその他の任意の適切な時間ベースの期間であってもよい。このアプローチを用いると、鍵を自動的に失効させることもできるし、あるいは鍵をある日付以降にだけ有効にすることもできる。各受信者は図８ｂの受信者識別子情報を用いて、これに対応する暗号化されたメッセージ鍵フィールドのうちどれが自分に関連するものであるのか識別してもよい。

【００９４】

図８ｃに示すように、鍵情報フィールド３６ａに秘密鍵識別情報を含めてもよい。メッセージ受信者は秘密鍵識別情報を用いて、メッセージの復号化に自身のどの秘密鍵を用いるか（また、ネットワーク１４上で秘密鍵を請求する必要がある場合は、該秘密鍵を取得するためにどの秘密鍵生成器に、またはどの場所にコンタクトを取るべきか）判断してもよい。

【００９５】

図８ｃの例では、秘密鍵識別情報は秘密鍵生成器の識別情報（例えば、サーバ名の形をとる秘密鍵生成器ＩＤ）に基づくものであり、これは受信者ＩＤとともに提供される。この秘密鍵生成器情報によって、各受信者は自身のどの秘密鍵を用いるべきなのか十分に識別できる。秘密鍵生成器ＩＤを用いて、受信者の装置のローカル秘密鍵データベースに記憶されている多数の秘密鍵の中から、該秘密鍵の位置を特定するローカルデータベースク

エリを作成してもよい。あるいは、秘密鍵生成器ＩＤを用いて、正しい秘密鍵生成器に対して、受信者が暗号化されたメッセージ鍵を復号化するために（それによって、受信者はメッセージのコンテンツを復号化できる）必要とする秘密鍵を生成するように指示する請求を作成してもよい。

【００９６】

メッセージの受信者は、受信者ＩＤ（図８ｃの例では、これは電子メールと有効期間情報に基づいている）を用いて、どの秘密鍵識別情報がどの受信者に対応しているのか判断してもよい。適切な構成の１つでは、所与の受信者は最初に、該当する電子メールアドレスがある鍵情報フィールドの受信者ＩＤ部の位置を特定する。次に、所与の受信者は添付の秘密鍵識別情報（例えば、図８の例ではサーバ名）を用いて、自身のローカル秘密鍵データベースから自分が使用すべき適切な秘密鍵の検索を試みる。秘密鍵データベースで秘密鍵の位置が特定できない場合は、サーバ名を用いて、ネットワーク１４上で適切な秘密鍵のコピーを取得するために、自分がどの秘密鍵生成器にコンタクトを取るべきか識別してもよい。所与の受信者は正しい秘密鍵を取得すると、この秘密鍵を用いて、該当する電子メールアドレスが見つかった鍵情報フィールドに関連する暗号化されたメッセージ鍵フィールドに位置する暗号化されたメッセージ鍵を復号化することができる。復号化されたメッセージ鍵を用いて、メッセージの内容を復号化し、メッセージの復号化プロセスは完了する。

【００９７】

図８ｄに示すように、鍵情報フィールドは、公開パラメータのバージョン番号情報などの秘密鍵識別情報を含んでもよい。時折（例えば、定期的に、あるいは秘密鍵生成器のマスタシークレットの秘密が漏洩したときに）、秘密鍵生成器１６によって生成される公開パラメータを変更してもよい。一例として、秘密鍵生成器１６はバージョン番号１．０の公開パラメータ情報を最初に生成してもよく、しばらく経った後にバージョン番号２．０の公開パラメータ情報を生成してもよい。復号化動作を適切に行うために、受信者は公開パラメータの正しいバージョン番号に一致する秘密鍵を使用する必要がある。このため、受信者は、正しい秘密鍵が取得され使用されていることを確認するために、バージョン番号情報を含む秘密鍵識別情報を用いることができる。図８ｄに、公開パラメータのバージョン番号情報を含む鍵情報フィールドの一例を示す。公開パラメータのバージョン番号は秘密鍵識別情報の形の１つであり、サーバ名に基づく秘密鍵生成器ＩＤ（あるいは、他の適切な秘密鍵生成器ＩＤ）などの秘密鍵識別情報とともに提供されてもよい。

【００９８】

図８ｅに示すように、鍵情報フィールド３６ａには、公開パラメータ情報（例えば、ＢｏｎｅｈおよびＦｒａｎｋｌｉｎの前述の研究で説明されている種類のシステム環境では、公開パラメータＰとｓＰとのセット）を含むこともできる。鍵情報フィールド３６ａに含まれる公開パラメータ情報は、該鍵情報フィールドに対応する暗号化されたメッセージフィールド３６ｂのメッセージ鍵を暗号化する際に、送信者が用いた公開パラメータ情報と同一のＩＢＥ公開パラメータ情報であってもよい。受信者が、受信者ＩＤを用いてメッセージに含まれる適切な鍵情報フィールドの位置を特定することができるように、図８ｅの公開パラメータ情報を受信者ＩＤとともに提供してもよい。公開パラメータ情報を用いて、暗号化されたメッセージ鍵を復号化するために受信者が用いるべき秘密鍵を判断することができるので、公開パラメータ情報は秘密鍵識別情報の形の１つと言える。

【００９９】

図８ｆに示すように、送信者は、図８ａ、８ｂ、８ｃ、８ｄ、および８ｅ、あるいはその他の任意の適切な鍵情報フィールド情報のうち任意の鍵情報フィールド情報を、鍵情報フィールド３６ａに挿入する前にハッシュ関数を用いて処理してもよい。ハッシュ関数Ｈは、Ｈ（ｓ）＝Ｖという性質を持つ。ここで、ｓは任意の文字列長を持つ英数字の文字列であり、Ｖは固定長の２進数である。例えば、Ｖの長さは１２８ビット、１６０ビット（例えば、１６バイトまたは２０バイト）、あるいはその他の適切な長さであってもよい。ハッシュ関数は衝突のないものであり、したがって、Ｈ（ｓ１）＝Ｈ（ｓ２）となるよう

なｓ１とｓ２を見つけることはできない（妥当な時間内には）。また、ハッシュ関数は一方向関数であるため、Ｖ１を所与として、Ｈ（ｓ３）＝Ｖ１となるようなｓ３を見つけることはできない（妥当な時間内には）。

【０１００】

図８ｆに示すように、鍵情報フィールド３６ａにハッシュ関数Ｈを用いると、これらの性質によっていくつかの利点が提供される。例えば、ハッシュ関数の一方向性によって、鍵情報フィールドに含まれる機密情報である可能性もある情報は、ネットワーク１４上でのメッセージ２０の伝送中隠蔽される。たとえメッセージが盗聴されたとしても、盗聴者は受信者の電子メール名を判断することはできない。これは、電子メール名が社会一般に利用可能になることを受信者が望まない場合に、有益となり得る。さらに、秘密鍵サーバ名情報（図８ｃおよび８ｄで示すように）あるいは、他の機密情報である可能性もある秘密鍵識別子情報または鍵情報フィールド情報を盗聴者から隠すこともできる。ハッシュ関数を用いる別の利点は、ハッシュ関数の出力は通常入力として渡される文字列よりも短いため、ハッシュ関数によって鍵情報フィールドをコンパクト化させることができる点である。したがって、ハッシュ関数への文字列入力が受信者ＩＤ、あるいは受信者ＩＤと公開パラメータ情報（図８ｅに示すように）だけであっても、メッセージ２０の鍵情報フィールド３６ａにこの情報を置く前に、ハッシュ関数を用いるほうが、依然として都合がよいだろう。

【０１０１】

電子メール通信あるいはその他の任意の適切な種類のメッセージ用のメッセージ鍵を暗号化するために、ＩＢＥスキームを用いてもよい。インスタントメッセージに伴うセキュアな通信をサポートする場合、通常メッセージ鍵を続けて再送する必要はない。インスタントメッセージングでは通常、後続のインスタントメッセージの復号化に用いるために、最初のインスタントメッセージのメッセージ鍵を保存しておくことも可能である。したがって、インスタントメッセージセッションの最初のインスタントメッセージに、受信者情報ブロック（鍵情報フィールドと暗号化されたメッセージ鍵フィールドとを有する）と、暗号化されたメッセージペイロードとを含めてもよい。受信者はＩＢＥを用いて暗号化されたメッセージ鍵を復号化してもよい。その後、セッション中後続のインスタントメッセージを復号化するために、復号化されたメッセージ鍵を保存してもよい。このような後続のメッセージを送信者から受信者へ伝送する際、暗号化されたメッセージペイロードを一緒に送るが、受信者ブロックの情報を全く送らない（例えば、暗号化されたメッセージ鍵を含まない）ようにしてもよい。

【０１０２】

前述の内容は本発明の本質の単なる例示に過ぎず、本発明の範囲および精神から逸脱することなく、当業者は種々の変更を行うことができる。

【図面の簡単な説明】

【０１０３】

【図１】図１は、本発明に従ってセキュアな電子メッセージングをサポートする、例示的な同一性ベースの暗号化システムの図である。

【図２】図２は、本発明に従ってセキュアな電子メッセージングをサポートするために複数の秘密鍵生成器を持つ、例示的な同一性ベースの暗号化システムの図である。

【図３】図３は、本発明に従った秘密鍵識別情報に関連する例示的なメッセージの図である。

【図４】図４は、本発明に従った同一性ベースの暗号化の暗号技術を用いた、セキュア電子メールメッセージの送信に伴うステップに伴う例示的なステップのフローチャートである。

【図５】図５は、本発明に従った例示的なメッセージを一般化した図である。

【図６】図６は、本発明に従って使用可能である適切なメッセージフォーマットについての例示的な実施形態の図である。

【図７】図７は、本発明に従って送受信者間でセキュアなメッセージを送るために、同一

性ベースの暗号化をどのように使用することができるのかを示す図である。
【図８】図８ａ、８ｂ、８ｃ、８ｄ、８ｅおよび８ｆは、本発明に従って使用可能である例示的な受信者情報フィールドの図である。

【図１】

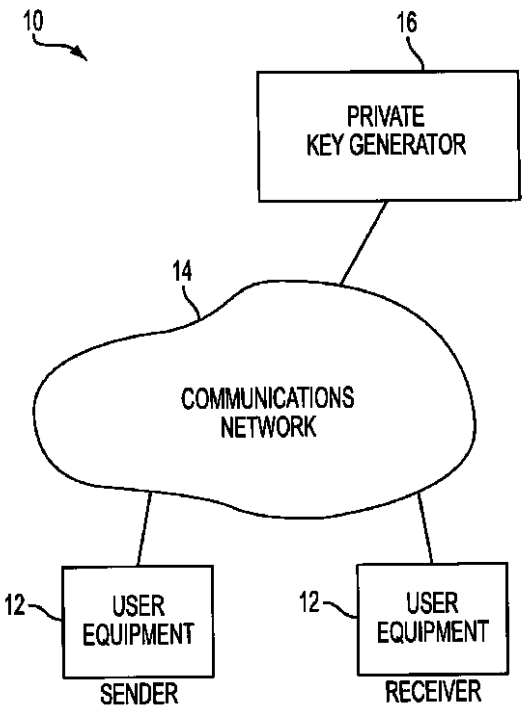


FIG. 1

【図２】

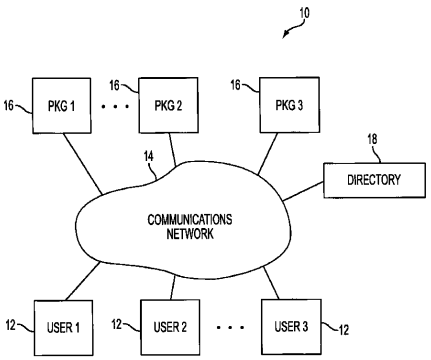


FIG. 2

【図３】

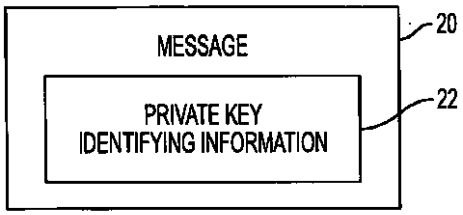


FIG. 3

【図４】

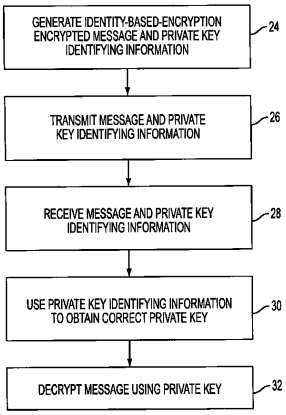


FIG. 4

【図５】

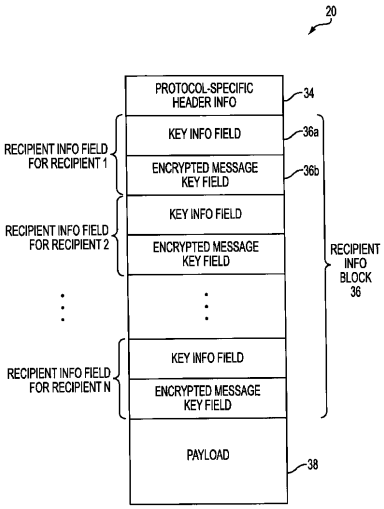


FIG. 5

【図６】

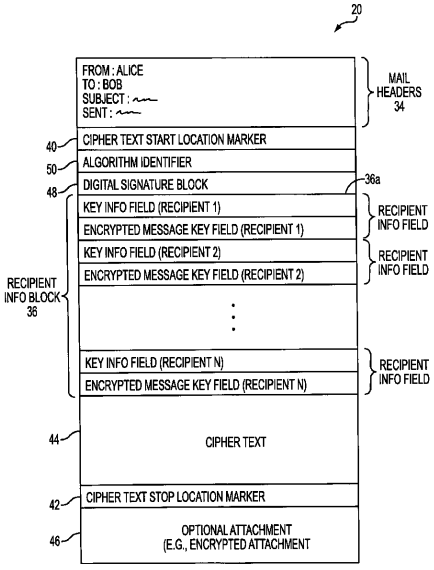


FIG. 6

【図７】

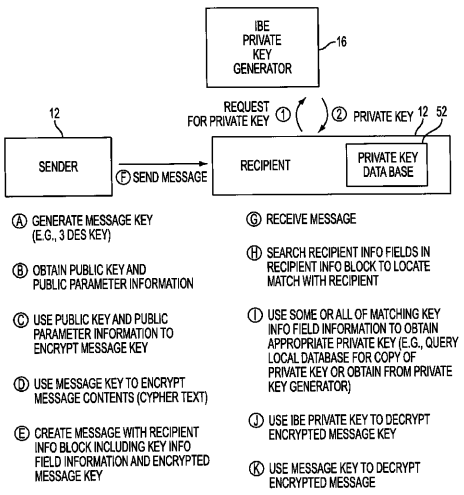


FIG. 7

【図８ａ】

FIG. 8a

【図８ｂ】

FIG. 8b

【図８ｃ】

FIG. 8c

【図８ｄ】

FIG. 8d

【図８ｅ】

FIG. 8e

【図８ｆ】

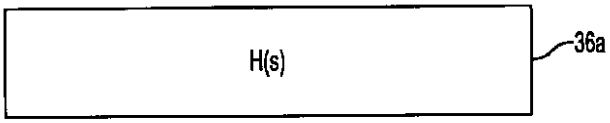


FIG. 8f

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US04/07829

A. CLASSIFICATION OF SUBJECT MATTER
IPC(7) : H04L 9/00
US CL : 713/171; 380/44
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
U.S. : 713/171; 380/44

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

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
Please See Continuation Sheet

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X --- Y	BONEH. D. and FRANKLIN. M. Identity Based Encryption from the Weil Pairing. Advances in Cryptology - Crypto 2001, LNCS 2139, Springer, pages 213-229, especially pages 213-217, 221-223, and 226.	1-3, 5, 6, and 11-17 --- 4, 7-10, and 18-20
Y	SCHNEIER. B. Applied Cryptography: Protocols, Algorithms, and Source Code in C. Second Edition, John Wiley & Sons, 1996, pages 31-34, especially page 32-33.	4 and 18-20
Y	BONEH. D. et al. Identity-Based Encryption. http://crypto.stanford.edu/ibe. April 8, 2002, whole document.	7-10

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:

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

"E" earlier application or patent published on or after the international filing date

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

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

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

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

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

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

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
24 May 2005 (24.05.2005)	07 JUN 2005
Name and mailing address of the ISA/US Mail Stop PCT, Attn: ISA/US Commissioner for Patents P.O. Box 1450 Alexandria, Virginia 22313-1450 Facsimile No. (703) 305-3230	Authorized officer Ayaz R Sheikh Telephone No. 571-272-2100

Form PCT/ISA/210 (second sheet) (January 2004)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US04/07829

Continuation of B. FIELDS SEARCHED Item 3:
Google search for "identity based encryption"
ACM and IEEE for "identity based encryption"

フロントページの続き

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

(72)発明者 アペンゼラー, グイド
アメリカ合衆国 カリフォルニア ９４０２５, メンロ パーク, イースト クリーク ドライブ １７１
(72)発明者 パウカー, マシュー ジェイ.
アメリカ合衆国 カリフォルニア ９４０２５, メンロ パーク, コールマン アベニュー ８０６, ナンバー７
(72)発明者 シュピース, テレンス
アメリカ合衆国 カリフォルニア ９４３０１, パロ アルト, ホーソーン ３７５エー
(72)発明者 カッカー, リシ アール.
アメリカ合衆国 カリフォルニア ９４０２５, メンロ パーク, コールマン アベニュー ８０６, ナンバー７

Ｆターム(参考) 5J104 AA01 AA16 AA32 EA04 EA15 EA16 EA19 EA26 JA21 NA02
NA27 NA36 NA37 PA08