(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第4896537号
(P4896537)
(45)発行日　平成24年3月14日(2012.3.14)　(24)登録日　平成24年1月6日(2012.1.6)

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

請求項の数 18 (全 17 頁)

(21)出願番号　特願2006-30252(P2006-30252)
(22)出願日　平成18年2月7日(2006.2.7)
(65)公開番号　特開2006-254423(P2006-254423A)
(43)公開日　平成18年9月21日(2006.9.21)
審査請求日　平成21年1月28日(2009.1.28)
(31)優先権主張番号　11/074,885
(32)優先日　平成17年3月7日(2005.3.7)
(33)優先権主張国　米国(US)

(73)特許権者　500046438
マイクロソフト　コーポレーション
アメリカ合衆国　ワシントン州　９８０５２－６３９９　レッドモンド　ワン　マイクロソフト　ウェイ
(74)代理人　100077481
弁理士　谷　義一
(74)代理人　100088915
弁理士　阿部　和夫
(72)発明者　アンドリュー　ボルツ
アメリカ合衆国　９８０５２　ワシントン州　レッドモンド　ワン　マイクロソフト　ウェイ　マイクロソフト　コーポレーション内

最終頁に続く

(54)【発明の名称】非対称キーセキュリティのための方法およびシステム

(57)【特許請求の範囲】
【請求項１】
複数のサーバの各々との、クライアントの先の相互作用を認証する非対称セキュリティキーを作成する方法において、
前記クライアントが、
前記複数のサーバの第１のサーバに関連付けられている第１のＩＤキーを受け取るステップと、
前記第１のサーバに対応している第１のマスターキーを生成するステップと、
前記第１のＩＤキーおよび前記第１のマスターキーの暗号化関数を利用することによって、１つ以上のシードを作成するステップと、
前記１つ以上のシードを利用して、前記第１のサーバに対応している、非対称公開キーおよび非対称秘密キーのペアを作成するステップと、
前記非対称公開キーを格納するよう前記第１のサーバに要求するステップと、
前記クライアントで、前記非対称秘密キーを格納するステップと、
前記第１のサーバとの先の相互作用を認証するステップであって、
前記先の相互作用の結果として前記非対称公開キーを知っていることの証明が前記第１のサーバによって要求されたとき、前記非対称公開キーを知っていることの前記証明を前記第１のサーバに提示し、および、前記非対称秘密キーを送信することなく、前記第１のサーバにアクセスすること、ならびに、
前記非対称公開キーを知っていることの前記証明に加えて、前記非対称秘密キーの保

有の証明が、前記第１のサーバによって要求されたとき、前記非対称秘密キーの保有の証明を前記第１のサーバに提示し、および、前記第１のサーバにアクセスすることを含む、認証するステップと
を備えることを特徴とする方法。
【請求項２】
前記１つ以上のシードを作成するステップは、１つ以上の定数を利用することをさらに含むことを特徴とする請求項１に記載の方法。
【請求項３】
前記クライアントが、前記非対称公開キーを利用して、前記クライアントが以前に前記第１のサーバにアクセスしたことがあるかどうかを判定するステップをさらに備えることを特徴とする請求項１に記載の方法。
【請求項４】
前記クライアントが以前に前記第１のサーバにアクセスしたことがあると判定したことに応答して、前記第１のサーバにアクセスするステップをさらに備えることを特徴とする請求項１に記載の方法。
【請求項５】
前記クライアントが、前記非対称公開キーを利用して、前記第１のサーバを認証するステップをさらに備えることを特徴とする請求項１に記載の方法。
【請求項６】
前記第１のマスターキーを生成するステップは、乱数を生成することを含むことを特徴とする請求項１に記載の方法。
【請求項７】
前記１つ以上のシードを作成するステップは、前記第１のＩＤキー、前記第１のマスターキー、および定数のハッシュ関数を利用することを含むことを特徴とする請求項１に記載の方法。
【請求項８】
前記第１のサーバは、ウェブサーバを含むことを特徴とする請求項１に記載の方法。
【請求項９】
前記クライアントが、前記非対称キーのペアをシードとして利用して対称キーを作成するステップをさらに備えることを特徴とする請求項１に記載の方法。
【請求項１０】
前記非対称公開キーは、前記第１のＩＤキーに少なくとも部分的に基づくことを特徴とする請求項１に記載の方法。
【請求項１１】
前記第１のＩＤキーを受け取るステップは、前記第１のサーバによって提供されるウェブサイトに関連付けられている証明書を受け取ることを含むことを特徴とする請求項１に記載の方法。
【請求項１２】
非対称キーのペアを利用する、通信チャネルを経由した１つ以上のサーバとの先の相互作用を認証するシステムにおいて、
プロセッサと、
前記プロセッサに結合され、前記プロセッサによって読み取り可能なメモリを含むクライアントとを備え、
前記メモリは、前記プロセッサによって実行されると、前記プロセッサに
第１のサーバに関連付けられている第１のＩＤキーを受け取るステップと、
第１のマスターキーを生成するステップと、
前記第１のＩＤキーおよび前記第１のマスターキーの暗号化関数を利用することによってシードを作成するステップと、
前記シードを利用して非対称秘密キーおよび非対称公開キーのペアを作成するステップと、

前記第１のサーバに、前記非対称公開キーを格納するよう要求するステップと、
クライアントで、前記非対称秘密キーを格納するステップと、
前記第１のサーバとの先の相互作用を認証するステップであって、
前記第１のサーバから、前記先の相互作用の結果として前記非対称公開キーを知っていることの証明を要求し、
前記非対称公開キーを知っていることの前記証明の要求を受けたときに、前記第１のサーバにアクセスする、認証するステップと
を行なわせる一連の命令を収容していること
を特徴とするシステム。

【請求項１３】
第１のマスターキーを生成するステップは、乱数を生成することを含むことを特徴とする請求項１２に記載のシステム。

【請求項１４】
シードを作成するステップは、前記第１のＩＤキー、前記第１のマスターキー、および１つ以上の定数のハッシュ関数を利用することを含むことを特徴とする請求項１２に記載のシステム。

【請求項１５】
前記非対称公開キーに少なくとも部分的に基づいて、前記第１のサーバから、認証に対する要求を受信するステップをさらに含むことを特徴とする請求項１２に記載のシステム。

【請求項１６】
１つ以上のサーバとの先の相互作用を認証する、コンピュータに実装される方法を実行するための命令のコンピュータプログラムを格納したコンピュータ読取り可能記憶媒体であって、前記コンピュータは、少なくとも中央処理装置（ＣＰＵ）、メモリ、および前記１つ以上のサーバと通信する手段を有し、クライアントとして動作可能であって、前記方法は、
クライアントが、
第１のサーバに関連付けられている第１のＩＤキーを受け取るステップと、
第１のマスターキーを生成するステップと、
前記第１のＩＤキー、前記第１のマスターキーおよび１つ以上の定数の暗号化関数を利用することによって１つ以上のシードを作成するステップと、
前記１つ以上のシードを利用して、非対称秘密キーおよび非対称公開キーのペアを作成するステップと、
前記第１のサーバに、前記非対称公開キーを格納するよう要求するステップと、
前記クライアントで、前記非対称秘密キーを格納するステップと、
前記第１のサーバとの先の相互作用を認証するステップであって、
前記先の相互作用の結果として前記非対称公開キーを知っていることの証明を前記第１のサーバに提示し、
前記第１のサーバから、前記非対称秘密キーの保有の証明に対する要求を受信し、
前記非対称秘密キーの保有の証明を前記第１のサーバに提示し、および、
前記クライアントが認証され、および、アクセスが許可されることの表示を、前記第１のサーバから受信することを含む、認証するステップと
を含むことを特徴とするコンピュータ読取り可能記憶媒体。

【請求項１７】
前記非対称キーのペアをシードとして利用して対称キーが作成されることを特徴とする請求項１６に記載のコンピュータ読取り可能記憶媒体。

【請求項１８】
前記暗号化関数は、前記第１のＩＤキー、前記第１のマスターキー、および１つ以上の定数のハッシュ関数であることを特徴とする請求項１６に記載のコンピュータ読取り可能記憶媒体。

【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、一般に、コンピュータおよびネットワークのセキュリティなど、電子セキュリティの分野に関する。より詳細には、本発明は、コンピュータシステムおよびユーザのＩＤ（ｉｄｅｎｔｉｔｙ）を認証することに関する。
【背景技術】
【０００２】
典型的な電子セキュリティは、インターネットなどのネットワークを介してリソースにアクセスする当事者を認証するために、公開キー／秘密キーのシステムを利用することができる。これらの公開キー／秘密キーのシステムは、不変であり、ウェブサイトなどの多くの異なるリソースのために利用される１つの公開キーと、リソースにアクセスするクライアントコンピュータなどのオリジネータのみによってアクセス可能な１つの秘密キーと共に動作する。
【発明の開示】
【発明が解決しようとする課題】
【０００３】
この電子セキュリティキーシステムには、著しい不都合があり、これには、オリジネータを識別する固定のキーがオリジネータに関する多くの情報、およびオリジネータの習性、照会などを得るために、多くの異なるウェブサイトによって利用される可能性があることが含まれる。これは、さまざまなウェブサイトの運営者が、公開キーをマッチさせ、そのマッチした公開キーに対応する情報を交換することによって行うことができる。さらに、ウェブサイトの運営者は、いったん公開キーがマッチすれば、オリジネータに関する情報を自由にオンゴーイングのベースで交換して、ユーザの習性などに関してより多くの情報を得ることができる。
【課題を解決するための手段】
【０００４】
本明細書で開示される例示的な実施形態は、前述ならびにその他の不都合を軽減するための方法およびシステムを含むことができる。本明細書で開示される例示的な実施形態は、マスターキーを生成することと、サーバからＩＤキーを受け取ることと、ＩＤキー、マスターキー、および（１つまたは複数の）定数（ｃｏｎｓｔａｎｔ）の暗号化またはハッシング関数を利用することによってシードを作成することと、キーまたはキーのペアを作成するプロセスへの入力としてこのシードを使用することとを備える（１つまたは複数の）非対称キーのペアを作成するための方法およびシステムを伴う。本明細書で開示される例示的な一実施形態では、このシードを使用して非対称キーのペアを生成し、結果として得られる非対称公開キーをサーバに格納する。
【０００５】
他の実施形態は、クライアントコンピュータ上で非対称公開キーを生成することと、その非対称公開キーがサーバ上で利用可能な対応する非対称キーにマッチするかどうかを判定することと、その非対称キーがマッチする場合にサーバおよび／またはクライアントを認証することとを備えるウェブサイトおよび／またはサーバあるいはユーザシステムを認証するためのシステムおよび方法を伴う。
【０００６】
さらに他の実施形態は、マスターキーを生成することと、サーバからＩＤキーを受け取ることと、ＩＤキー、マスターキー、および（１つまたは複数の）定数の暗号化関数を利用することによってシードを作成することと、安全な対称キーを作成するプロセスへの入力としてこのシードを使用することと、サーバとクライアントの間で対称的な認証プロセスを開始することによって、その対称キーがサーバ上で利用可能な対応する対称キーにマッチするかどうかを判定することとを備えるウェブサイトおよび／またはサーバあるいはユーザシステムを認証するためのシステムおよび方法を伴う。

【０００７】
本明細書で開示される例示的な実施形態は、コンピュータプロセスやコンピューティングシステムとして、またはコンピュータプログラム製品などの製品として実装することができる。このコンピュータプログラム製品は、コンピュータプロセスを実行するための命令のコンピュータプログラムを符号化したコンピュータシステムによって読み取り可能なコンピュータストレージメディアとすることができる。このコンピュータプログラム製品は、コンピュータプロセスを実行するための命令のコンピュータプログラムを符号化したコンピューティングシステムによって読み取り可能な搬送波上で伝搬される信号とすることもできる。
【０００８】
本開示およびその改良形態についてのより完全な理解は、以降で簡単に説明されている添付の図面と、以下の本発明の現在の好ましい実施形態に関する詳細な説明と、添付の特許請求の範囲とを参照することによって得ることができる。
【発明を実施するための最良の形態】
【０００９】
図１は、全体的に１００において、例示的な一実施形態に従って（１つまたは複数の）非対称キーのペアを作成し、ＩＤを認証するために利用できるシステムのブロック図である。この実施形態では、システム１００は、クライアント１０２、１０４を有する。クライアント１０２、１０４は、ネットワーク１１２に接続され、これは次に、サーバ１　１０６、サーバ２　１０８、およびサーバ３　１１０に接続されている。ネットワーク１１２は、インターネット、またはその他の通信チャネルとすることができ、これを利用して、クライアント１０２および１０４と、サーバ１０６、１０８、１１０との間で通信を行うことができる。システム１００は、クライアントおよびサーバとの例示的な通信システムであるにすぎず、多くの異なる代替的な構成を利用できることを当業者は理解するであろう。
【００１０】
この実施形態では、クライアント１０２および１０４は、それぞれキー作成モジュール１１４および１１５を有する。キー作成モジュール１１４および１１５は、（１つまたは複数の）対称キーおよび／または（１つまたは複数の）非対称キーのペアを作成することができる。
【００１１】
非対称キーを伴う例示的な一実施形態では、（１つまたは複数の）非対称キーのペアは、既知の入力に基づいて計算される一意の値であり、そのためそれらの値は、同じ入力値を用いて同じ関数を繰り返すことによって再現することができる。そしてサーバの固定のＩＤキーおよび／またはクライアント上のキー作成モジュールによって生成された公開キーを使用して、相互認証を行う。すなわち、クライアントはサーバを認証することができ、サーバもクライアントを認証することができる。
【００１２】
クライアント１０２および１０４は、サーバ１０６、１０８、１１０に対して情報の要求および送信を行う。同様にサーバ１０６、１０８、１１０は、情報についての要求を受信し、応答を試みる。さらに、サーバは、自らクライアントからの情報を要求することができる。時には、機密の情報がサーバに送信される。サーバおよびクライアントを保護するために、システム１００は、対称キーまたは非対称キーのセキュリティを組み込んでいる。これらのセキュリティ機能を使用して、クライアントシステムは、情報を盗もうと試みる不正なサーバ技術からかなり保護される。
【００１３】
クライアント１０２は、サーバ１　１０６に関連付けられているＩＤキー１１６を要求することができる。そしてクライアント１０２は、キー作成モジュール１１４を利用して、マスターキーを作成し、ＩＤキー１１６、マスターキー、および（１つまたは複数の）定数を利用して、非対称公開キー（ＡＰＫ）１　１２０を含む非対称キーのペアを作成す

ることができる。次いで非対称公開キー１　１２０をサーバ１　１０６上に格納することができ、対応する非対称秘密キーをクライアント１０２に格納することができ、これによって、クライアント１０２がサーバ１　１０６を再び訪問するとき、および／またはクライアント１０２のユーザがサーバ１　１０６を再び訪問するとき、非対称公開キー１　１２０について知っていることの証明を要求することができ、これによって、以前にサーバ１　１０６にアクセスしたことがあるかどうかを判定することができる。この実施形態を利用して、非対称公開キー１　１２０を介してサーバ１　１０６および／または関連付けられているウェブサイトの認証性を判定することもできる。さらに、クライアント１０２は、非対称秘密キーを破棄し、後で再びサーバにアクセスするときに非対称キーのペアを再作成し、非対称公開キーを提示して、サーバに対して継続中のデジタル関係（ｏｎ　ｇｏｉｎｇ　ｄｉｇｉｔａｌ　ｒｅｌａｔｉｏｎｓｈｉｐ）が存在することをサーバに対して証明することができる。

【００１４】

クライアント１０２は、サーバ１　１０６に再びアクセスするときに再作成した非対称公開キーを提示して、サーバ１　１０６に対してクライアント１０２を検証することができる。クライアント１０２とサーバ１　１０６は双方とも、他方からのさらなる保証を要求してＩＤを認証することができる。これらのさらなる保証は、ペアの公開キーまたは秘密キーのいずれかの所有者のみが復号、理解でき、および／または応答できるような形態とすることができる。

【００１５】

非対称キーのメカニズムを使用する場合、クライアント１０２は、それぞれのサーバ１０６、１０８、および１１０ごとに異なるキーのペアを生成し、暗号化されたチャネルを使用して公開キーを通信するため、ＩＤを認証するには、非対称公開キーについて知っていることの証明を提示するだけで十分かもしれない。これは非対称公開キーが都合に応じて対称キーとして機能することができることを意味する。他の場合、サーバは、関連付けられている秘密キーを所有している旨の証明を要求することを選択することができる。

【００１６】

同様に別のクライアント１０４も、サーバ１　１０６にアクセスし、サーバ１のＩＤキー１１６を要求することができる。サーバ１のＩＤキー１１６は、サードパーティーからの証明書またはセキュリティ証明書を要求し、その証明書をパースしてＩＤキーまたはその他のＩＤ情報を得ることによって入手することもできる。本明細書で開示されているコンセプトから逸脱することなくＩＤキーおよび／またはセキュリティ証明書を得るためのその他の方法およびシステムを利用することもできることが理解されるであろう。同様に、クライアント１０４も、ＩＤキー１１６、異なるマスターキー、および任意選択で（１つまたは複数の）定数を利用して、非対称公開キー（ＡＰＫ）２　１２２を作成することができる。そしてクライアント２　１０４は、非対称公開キー２　１２２をサーバ１　１０６に関連付けることができる。次いでクライアント１０４は、対応する非対称秘密キーを保存するか、またはそれを破棄し、その後にサーバにアクセスするときにキーのペアを再作成することができる。

【００１７】

非対称公開キー２　１２２は、クライアント１０４に関連付けられているキー作成モジュール１１４によって作成することができる。前述の方法と同様に、クライアント１０４がその後にサーバ１　１０６にアクセスするとき、以前にサーバ１　１０６にアクセスしたことがあるかどうか、および／または何らかのＩＤ情報をサーバ１　１０６に提供したことがあるかどうかを判定することができるように非対称公開キー２　１２２について知っていることの証明を要求することができる。同様に、クライアント１０４は、非対称公開キー２　１２２について知っていることの証明を再作成し、サーバ１　１０６に実証して、クライアント１０４のＩＤを認証することができ、あるいは関連付けられている秘密キーを所有していることの証明を要求することができる。

【００１８】

さらに、クライアント１　１０２は、サーバ２　１０８にアクセスし、サーバ２のＩＤキー１１８を要求することができる。ＩＤキー１１８を受け取った後、クライアント１０２は次に、ＩＤキー１１８、および別のまたは同じマスターキー、ならびに（１つまたは複数の）定数を利用して、対称キー３（ＳＫ）１２４を作成することができる（この場合、非対称キーのペアではなく対称キーを作成するモジュールにシードが提供される）。この対称キーは次いで、暗号化されたチャネルを使用してサーバ２　１０８に伝達される。

【００１９】

クライアント１０２は次に、サーバ２　１０８に再びアクセスするときに対称キー３　１２４について知っていることの証明を要求することができる。同様に、サーバは、クライアントによるそのキーについて知っていることの証明を要求することができる。そのユーザのみが、対称キーを作成するために使用されたマスターキーなどを有しているであろう。クライアント１０２は、訪問したあらゆるウェブサイトおよび／またはサーバごとに異なる対称キーを格納することができ、それらのキーについて知っていることの証明を要求して、サーバが以前にアクセスされたことがあるかどうかを判定できるかもしれない。さらに、対称キーを利用して、サーバ、クライアント、および／またはウェブサイトを認証することができる。これは、その対称キーをサーバに格納した特定のクライアントまたはユーザのみが、要求された相互認証を渡すことができるであろうためである。

【００２０】

同様に、クライアント１０４も、サーバ３　１１０にアクセスし、サーバ３のＩＤキー１２０を要求することができる。クライアント１０４は次いで、キー作成モジュール１１４を利用してランダムなマスターキーを作成することができ、このマスターキーをサーバ３のＩＤキー１２０および任意選択で定数と共に利用して非対称公開キー（ＡＰＫ）４　１２６を作成し、これをサーバ３　１１０に格納するか、またはサーバ３　１１０に関連付けることができる。次いでクライアント１０４は、マスターキー、サーバ３のＩＤキー、および何らかの定数から得られたものなどの対称キーの下で非対称キーのペアを暗号化することもでき、非対称キーのペアをシード（ＳＫＡＫ）１２７として利用して作成されたこの対称キーを、非対称公開キーＡＰＫ４　１２６およびサーバの関連付けられているＩＤと関連付けてサーバ３上に格納する。非対称キー１２７を利用する対称キーが暗号化されるので、クライアント１０４のみがそれを復号することができるか、またはその情報を利用して非対称キーのペアを取り出すことができるであろう。それゆえ、非対称キー１２７を利用する対称キーがクライアント１０４によって利用されて、クライアント１０４が以前にサーバ３　１１０にアクセスしたことがあるかどうかを判定することができる。さらに、この構成を利用してウェブサイトおよび／またはサーバを認証することができる。これは、以前に訪問したサーバのみが、特定のクライアントからの非対称キーを利用する、関連付けられている対称キーを有するであろうためである。またさらに、サーバを訪問するときに非対称キーを利用する対称キーを復号できるクライアントは、非対称公開キーを利用してサーバに対して自分自身のＩＤを認証することができる。

【００２１】

前述のように、不正な人間が、クライアントおよび／またはクライアントのユーザをだまして個人情報を提供させようと試みることがある。正体不明の不正人物１３０が、正当なサーバおよび／またはウェブサイトを模造するか、またはそれになりすまして、クライアント１０２、１０４からのＩＤおよび／またはその他の情報を入手しようと試みることがある。本明細書で開示される例示的な実施形態では、クライアントがＩＤキーを要求するとき、正体不明の不正人物のＩＤキー１３２がそのクライアントに提供されることになり、したがってそのクライアントは、それが以前に訪問したサーバではないことを見分けることができる。さらに、クライアントが非対称公開キーを要求する場合、クライアントおよび／またはユーザは以前にその正体不明の不正人物のウェブサイトにアクセスしたことがないので、その正体不明の不正人物は（１つまたは複数の）非対称公開キー（ＡＰＫ）１３４を有していないことになる。これらのシナリオのいずれによっても、クライアント１０２、１０４のユーザは、そのウェブサイトおよび／またはサーバが信頼されるべき

ではなく、ＩＤまたはその他の情報を開示するにあたって警戒すべきであることを警告されることになる。

【００２２】

同様に、正体不明の不正人物１３０は、サーバのいずれかにアクセスしてクライアントのＩＤ情報を入手しようと試みる場合、クライアントまたはサーバとして装うのに必要とされる対称キーまたは非対称キーについて知っていることを実証できないことになる。

【００２３】

この例示的な実施形態では、サーバ、ユーザ、および／またはクライアントは、正体不明の不正人物がウェブサイトになりすますことによって個人情報を入手することを禁止できる別の１つまたは２つのレベルのセキュリティを有することができる。さらに、これは、「マン・イン・ザ・ミドル（ｍａｎ　ｉｎ　ｔｈｅ　ｍｉｄｄｌｅ）」による情報の傍受を禁止して、さらなるセキュリティを提供することもできる。

【００２４】

サイトに固有の非対称公開キーまたは対称キーがサーバおよび／またはウェブサイトに格納されるので、ユーザは、自分のマスターキーを多くの異なるクライアントに用い、ウェブサイトにアクセスし、それでもなおそれらが真正なウェブサイトとやり取りしているという点でいくらか安全であることができる。この場合もやはり、それらは、自分の（１つまたは複数の）マスターキーおよび（１つまたは複数の）定数と共にサーバのＩＤキーを利用して、サイトの対称または非対称公開キーについて知っていることの証明を要求することができ、あるいはウェブサイトに保存されているかまたは関連付けられている隠されたキーブロブ（ｏｐａｑｕｅ　ｋｅｙ　ｂｌｏｂ）を要求および復号して、以前にそのサーバおよび／またはウェブサイトを訪問したことがあるかどうかを判定することもできる。これはまた、家庭、職場、図書館などで複数のマシンを使用するユーザにとってウェブサイトとやり取りする際により大きな安心を持つことができるという点で魅力的かもしれない。ある時点でマスターキーを新しいデバイスまたはコンピュータに移すだけでよいという点が、このシステムの特筆すべき中心的な特徴である。そのマスターキーから、継続中のデジタル関係のすべてのサイトに固有のキーおよび証明を演繹することができる。これによって、オンゴーイングの再同期が不要となる。

【００２５】

これは、不正行為について懸念を抱いている可能性のあるサーバおよびウェブサイトの運営者にとって魅力的かもしれない。これは、正体不明のユーザが機密情報を入手するのを禁止することができる特別なレベルのユーザ生成のセキュリティを提供する。

【００２６】

図２は、本発明の実施形態を実装できる適切なコンピューティングシステム環境の一例を示している。このシステム２００は、前述のようにクライアントおよび／またはサーバとして機能するために使用できるシステムの代表である。その最も基本的な構成において、システム２００は通常、少なくとも１つの処理装置２０２およびメモリ２０４を含む。コンピューティングデバイスの厳密な構成およびタイプに応じて、メモリ２０４は、（ＲＡＭなどの）揮発性、（ＲＯＭ、フラッシュメモリなどの）不揮発性、またはこれら２つの何らかの組合せとすることができる。この最も基本的な構成が、破線２０６によって図２に示されている。さらに、システム２００は、追加の特徴／機能を有することもできる。たとえば、デバイス２００は、磁気ディスク、光ディスク、テープなどの追加のストレージ（リムーバブルおよび／または非リムーバブル）を含むこともできるが、これらには限定されない。このような追加のストレージは、リムーバブルストレージ２０８および非リムーバブルストレージ２１０として図２に示されている。コンピュータストレージメディアは、コンピュータ可読命令、データ構造、プログラムモジュール、その他のデータなどの情報を記憶するための任意の方法または技術において実装される揮発性および不揮発性メディア、ならびにリムーバブルおよび非リムーバブルメディアを含む。メモリ２０４、リムーバブルストレージ２０８、および非リムーバブルストレージ２１０は、すべてコンピュータストレージメディアの例である。コンピュータストレージメディアは、ＲＡＭ

、ＲＯＭ、ＥＥＰＲＯＭ、フラッシュメモリもしくはその他のメモリ技術、ＣＤ－ＲＯＭ、デジタル多用途ディスク（ＤＶＤ）もしくはその他の光ストレージ、磁気カセット、磁気テープ、磁気ディスクストレージもしくはその他の磁気ストレージデバイス、または希望の情報を記憶するために使用でき、システム２００によってアクセスできるその他の任意のメディアを含むが、これらには限定されない。任意のこのようなコンピュータストレージメディアは、システム２００の一部とすることができる。

【００２７】

システム２００は、システムがその他のデバイスと通信することができるようにする（１つまたは複数の）通信接続２１２を含むこともできる。（１つまたは複数の）通信接続２１２は、通信メディアの一例である。通信メディアは通常、搬送波やその他のトランスポートメカニズムなどの変調されたデータ信号にコンピュータ可読命令、データ構造、プログラムモジュール、その他のデータを具現し、任意の情報伝達メディアを含む。「変調されたデータ信号」という用語は、情報をその信号に符号化するような方法でその特性の１つまたは複数を設定または変更した信号を意味する。例として、限定ではなく、通信メディアは、有線ネットワークや直接配線接続などの有線メディアと、音響メディア、ＲＦメディア、赤外線メディア、その他の無線メディアなどの無線メディアとを含む。本明細書で使用するコンピュータ可読メディアという用語は、ストレージメディアおよび通信メディアの両方を含む。

【００２８】

システム２００は、キーボード、マウス、ペン、音声入力デバイス、タッチ入力デバイスなどの（１つまたは複数の）入力デバイス２１４を有することもできる。ディスプレイ、スピーカ、プリンタなどの（１つまたは複数の）出力デバイス２１６を含むこともできる。これらのデバイスはすべて、当技術分野でよく知られており、本明細書で詳細に論じる必要はない。

【００２９】

システム２００など、コンピューティングデバイスは通常、少なくとも何らかの形態のコンピュータ可読メディアを含む。コンピュータ可読メディアは、システム２００によってアクセスすることができる任意の利用可能なメディアとすることができる。例として、限定ではなく、コンピュータ可読メディアは、コンピュータストレージメディアおよび通信メディアを備えることができる。

【００３０】

図３は、全体的に３００において、例示的な一実施形態に従って非対称セキュリティキーの交換のためのシステムを概念的なレベルで示している。この例は、ネットワーク３１４またはその他のチャネルを介して接続されているクライアント３０１およびサーバ３０６を含むシステム３００を例示している。明らかになるであろうが、ほとんどのデバイスは、その時々に応じてクライアント３０１およびサーバ３０６のどちらとしても機能することができる。しかし、説明を簡単にするために、ここではこれらの機能を別々に示している。さらに、ネットワーク３１４は、インターネットを含むほぼいかなるタイプのネットワークとすることもでき、あるいはクライアント３０１とサーバ３０６の間で通信を確立するのに適したその他の何らかのタイプのチャネルとすることができる。

【００３１】

クライアント３０１は、インターネットを介してウェブサイトまたはサーバ３０６にアクセスするパーソナルＰＣなどのクライアントとすることができる。しかし、本明細書で開示されているコンセプトから逸脱することなくその他のデバイスおよび構成を利用できることが理解されるであろう。同様に、サーバ３０６は、ウェブサイト、デバイス、またはその他のシステム、あるいはその他の構成のホストとすることができる。

【００３２】

サーバ３０６は、関連付けられているＩＤキー３０７を有する。ＩＤキー３０７は、数ある情報の中でもサーバに関する情報を有する。一実施形態では、それらの情報は、ＵＲＬのコンポーネント、システムを所有または運営しているプリンシパルの名前、および／

またはその他の「ＩＤ」情報に関係する。サーバ３０６にアクセスするとき、クライアント３０１は、ＩＤキー３０７を要求することができ、および／またはＩＤキー３０７は、サーバまたはその他のエンティティによってクライアント３０１に提供することができる。ＩＤキー３０７は、ここではサーバ３０６に属するかまたは由来するものとして示されているが、ＩＤキー３０７は、これには限定されないが、数ある中でも検証エンティティを含む別のソースに属するかまたは由来することもできることが理解されるであろう。

【００３３】

別の例示的な実施形態では、クライアント３０１は、サーバ３０６に関する情報を収容する証明書を受け取る。この証明書内に収容された情報は、ＩＤキー３０７またはその他のＩＤ情報を含む。クライアント３０１は、この証明書をパースしてＩＤキー３０７にアクセスする。前述のように、この証明書は、サーバ、検証エンティティ、および／またはその他のエンティティに由来することができる。

【００３４】

次いで、ＩＤ情報はクライアントによって使用されて一意の非対称公開キー（または対称キー）３０９を作成し、これはサーバに格納される。このキー３０９は、サーバのＩＤ情報、クライアントによって生成されたマスターキー、および任意選択で（１つまたは複数の）定数の関数である。この関数は、その関数を作成するために利用されるコンポーネントが最終製品から識別可能とすることができないように（すなわち暗号化されるように）することができる。

【００３５】

クライアント３０１は、以前にマスターキー３０２を作成したことがあるかもしれない。マスターキー３０２は、ランダムに生成された数、および／またはこれらには限定されないが、タイムスタンプ、ＩＤ情報など、もしくはその他の情報、あるいはそれらの組合せを含むさまざまな異なるタイプの情報とすることができる。クライアント３０１は次に、マスターキー３０２、およびＩＤキー３０７、ならびに（１つまたは複数の）定数の組合せの暗号化関数を利用して、秘密キー３０８および公開キー３０９を含む非対称キーのペアを生成するために使用される１つまたは複数のシードを作成することができる。このようにして、非対称キー３０８および３０９は、訪問されたそれぞれのサーバ３０６および／またはウェブサイトごとに作成することができる。あるいは、１つまたは複数のシードを使用して、暗号化されたチャネルを介して伝達できる対称キーを作成することができ、これも３０９として示されている。

【００３６】

キー３０９は次いで、サーバ３０６上に格納することができる。非対称の場合、非対称秘密キーをクライアント３０１に格納するか、またはこれを破棄し、その後にサーバにアクセスするときにキーを再作成することができる。クライアント３０１は、サーバ３０６に再びアクセスするとき、サーバ３０６によってキー３０９について知っていることの証明を要求および／または受信し、それを自分自身のシステム上で再作成されたキーと比較して、クライアント３０１が以前にサーバ３０６にアクセスしたことがあるかどうかを判定することができる。サーバ３０６も、この方法を利用して、クライアント３０１が以前にサーバ３０６にアクセスしたことがあるかどうかを判定することができ、あるいは非対称の場合は、秘密キー３０８について知っていることの証明を示すようクライアントに要求することもできる。

【００３７】

この情報を利用してサーバ３０６の認証性を判定することもでき、これによってクライアント３０１、およびそのクライアント３０１を使用するプリンシパルは、サーバ３０６および／または関連付けられているウェブサイトが真正および／または正当なものであることをさらに確信することができる。これによって不正行為を低減することができ、ユーザがＩＤ情報またはその他の情報をサーバ３０６に開示する前にユーザの確信だけでなく、その他の多くの利点を増大することができる。

【００３８】

知っていることの証明は、秘密を用いた何らかの情報に対するデジタル署名をサブミットすることを含むことができ、これは、その秘密を知っているエンティティおよび／または（１つまたは複数の）シードおよびキーを有するエンティティによって検証および／または理解することができる。以前にサーバに格納されたキーについて知っていることの証明を要求することによって、ユーザはサーバ／ウェブサイトを識別することができ、そしてサーバに情報を開示するときにより確信することができる。例示的な実施形態は、正体不明のシステム３１２が、以前にアクセスしサーバ３０６になりすますことによってクライアント３０１からＩＤ情報を入手しようと試みる可能性を低減することができる。さらに、サーバ３０６は、非対称秘密キー３０８を利用して、サーバ３０６へのアクセスを試みるおよび／または特定のクライアントに関する情報を変更または入手するクライアント３０１の認証性を判定することもできる。

【００３９】

非対称公開キーまたは対称キーは、作成されると、ウェブサーバ上に格納されるか、またはそのキーが作成されたウェブサイトに関連付けて格納される。その結果、ユーザは、そのサイトに再び訪問し、サイトの問いかけを介してそのサイトを迅速に検証／認識してキーを知っていることを実証することができる。さらに、訪問されたそれぞれのシステムには一意のペアワイズ（ｐａｉｒ－ｗｉｓｅ）のキーが与えられ得るので、異なるシステムの運営者がキーを比較して、クライアントまたはユーザに関する情報を共有することはできない。

【００４０】

知っていることの証明のために使用される暗号化は、状況に応じて、ＡＥＳ２５６関数とすることもでき、あるいはＲＳＡなどの公開キーアルゴリズムに基づくこともできる。しかし、本明細書で開示されているコンセプトから逸脱することなくその他の暗号化アルゴリズム、関数、および構成を利用することもできることが理解されるであろう。

【００４１】

この情報を利用してサーバ３０６の認証性を判定することもでき、これによってクライアント３０１、およびそのクライアント３０１のユーザは、サーバ３０６および／または関連付けられているウェブサイトおよびシステムが真正および／または正当なものであることをさらに確信することができる。これによって、数ある利点の中でも、不正行為を低減することができ、ユーザがＩＤ情報またはその他の機密情報をサーバ３０６に開示する前にユーザの確信を増大することができる。この認証は、継続中のデジタル関係の首尾一貫した認識を提供することができる。

【００４２】

クライアント３０１が、キー３０９を所有していることの予期される証明以外の何かを受け取った場合、これは、クライアント３０１が以前にこのサーバ３０６にアクセスしたことがないことを示している可能性がある。これはまた、数あるシナリオの中でも、正当なサイトが偽造されているか、またはサーバ３０６がそのキーを失ったことを示しているかもしれない。これは、クライアント３０１のユーザに対して、サーバ３０６が信頼できないこと、およびユーザはサーバ３０６との接続を解除すべきであること、もしくは注意して進むか、および／またはいかなる機密情報、秘密情報、および／またはＩＤ情報も明かすべきではないことを示しているかもしれない。

【００４３】

図３に示されている実施形態のさらなる利点は、ユーザが、オリジナルのマスターキーで多くの異なるクライアントからウェブサイトおよび／またはサーバ３０６にアクセスすることができ、なおそのウェブサイトが正当なものであるというあるレベルの保証を有することができることである。

【００４４】

図４は、全体的に４００において、例示的な一実施形態に従ってペアワイズのセキュリティキーを作成する方法の例示的な一実施形態を例示するフローチャートである。方法４００は、受信オペレーション４０２を含む。受信オペレーション４０２は、サーバまたは

その他のエンティティからＩＤキーを受け取ることを含む。ＩＤキーは、サーバに関するＩＤ情報を含むことができ、これには、一意のＵＲＬ、システムを所有しているプリンシパル、および／またはその他のＩＤ情報などが含まれるが、これらには限定されない。さらに、ＩＤキーは、サーバに関連付けられているセキュリティ証明書やその他の証明書などの証明書の一部とすることができる。ＩＤキーは、証明書からパースすることができる。そして制御は、生成オペレーション４０４に渡る。

【００４５】

生成オペレーション４０４は、マスターキーを生成することを含むことができる。マスターキーは、乱数、ＩＤ情報、もしくはその他の一意の情報、および／またはそれらの組合せとすることができる。マスターキーは、以前に生成され、別のアプリケーションに再利用されていたかもしれない。マスターキーは、無許可の人間またはエンティティが侵入し、情報を見ることおよび／または盗むことができないであろう非常に安全な場所に格納すべきであることが理解されるであろう。そして制御は、取得オペレーション４０６に渡る。

【００４６】

取得オペレーション４０６は、（１つまたは複数の）定数を取得することを含む。この（１つまたは複数の）定数は、ランダムに作成された数、もしくはその他の情報、および／またはそれらの組合せとすることができる。この（１つまたは複数の）定数は、必要なときに後で再生できるように、その定数を作成するユーザに知られるだけでよい。そして制御は、作成関数４０８に渡る。

【００４７】

作成オペレーション４０８は、ＩＤキー、マスターキー、および（１つまたは複数の）定数の関数としてシードを作成することを含むことができる。本明細書で開示されているコンセプトから逸脱することなくその他の情報および／または情報の組合せを利用することができることが理解されるであろう。この関数は、元の情報は、結果として得られるシードから判定できないように上記の情報を一方向の暗号化とすることができる。この関数は、ＡＥＳ暗号化関数、あるいはその他の暗号化関数もしくはアルゴリズム、および／またはそれらの組合せとすることができる。ある範囲のシードを生成する必要がある場合は、制御を取得関数４０６に戻して、異なる定数を利用して別のシードを作成する際に利用することになる別の定数を取得することができる。そしてこの（１つまたは複数の）シードは、（１つまたは複数の）非対称キーのペアを作成するための非対称キーペアジェネレータによって、または対称キーを作成するための対称キー作成／認証関数によって利用することができる。

【００４８】

図５は、全体的に５００において、例示的な一実施形態に従って（１つまたは複数の）非対称キーのペアを作成し、継続中のデジタル関係を認識することを伴うさらなるオペレーション上の特徴を示す流れ図である。

【００４９】

方法５００は、５０２において受信関数を含む。受信オペレーション５０２は、以前に作成された（１つまたは複数の）シードを受け取ることを含む。（１つまたは複数の）シードは、上述のように作成される。そして制御は、作成関数５０４に渡る。

【００５０】

作成関数５０４は、受信した（１つまたは複数の）シードを利用して非対称キーのペアを作成することを含む。１つまたは複数のシードは、非対称キーのペアの作成において利用することができる。使用されるシードの数は、使用する非対称キーペアジェネレータの特定のタイプに依存することができる。そして制御は、格納関数５０６に渡る。

【００５１】

格納オペレーション５０６は、非対称公開キーをサーバに格納すること、および／またはその非対称公開キーをサーバもしくはウェブサイトに関連付けることを含むことができる。この非対称公開キーは、クライアントがサーバに再びアクセスするときにこのクライ

アントによってアクセスすることができるようにサーバに関連付けられる。さらに、この非対称公開キーは、ユーザが多くの異なるデバイスまたはシステムからシステムまたはウェブサイトを認証または認識することができるように別のシステムからのユーザによってアクセスすることができる。クライアントは、非対称公開キーを再作成し、その後にサーバに再びアクセスするときに提示して、そのクライアントのＩＤを検証することもできる。このようにして、クライアントは、以前にそのサーバにアクセスしたことがあるかどうかを判定することができる。さらに、この情報を利用して、サーバおよび／またはクライアントの認証性および／または正当性を判定することができる。

【００５２】

図６は、全体的に６００において、例示的な一実施形態に従ってサーバ、クライアント、システム、またはウェブサイトの認証性を判定する方法を示すフローチャートである。方法６００の態様によれば、生成オペレーション６０２で処理が始まる。生成オペレーション６０２は、ユーザ／クライアントが、ユーザ／クライアントのＩＤを検証するためにサーバに対して非対称公開キーについて知っていることの証明を生成することを含むことができる。クライアントおよび／またはサーバによる非対称公開キーについて知っていることの証明の生成により、継続中の関係の証明を構成することができる。これは、クライアントおよびサーバが以前に情報を交換したことがあるということである。クライアントは、対応する非対称秘密キーを利用して、サーバとの以前の訪問および／または情報の交換を示すこともできる。さらに、クライアントは、キーのペアを格納しておくことによって、または最初に非対称公開キーを作成するために使用した情報を利用して非対称キーのペアを再作成することによって、非対称公開キーを知っていることを実証することができる。そして制御は、クエリーオペレーション６０４に渡る。

【００５３】

クエリーオペレーション６０４は、生成された非対称公開キーが、クライアントによって保存されている、および／または再作成された、および／または復号された、および／または以前に格納された非対称公開キーにマッチするかどうかを判定することを含む。クライアントは、対応する非対称公開キーを保存していたかもしれないので、その非対称公開キーを比較して、サーバが以前にアクセスされたことがあるかどうかを判定することができる。さらに、クライアントは、数ある情報の中でもＩＤキーおよびオリジナルのマスターキーを利用して、サーバが以前にアクセスされたことがあるかどうかを判定するために非対称公開キーを再作成することができる。

【００５４】

非対称公開キーがマッチした場合、制御は、認証されたシステム６０６に渡る。これは、そのクライアントが以前にそのサーバにアクセスしたことがあり、非対称公開キーを保存し、および／またはそのサーバに関連付けていたことを示している。認証されるシステムは、サーバおよび／またはクライアントとすることができる。クライアントおよび／またはサーバは、他方のＩＤを認証する前に、任意選択で他方のＩＤのさらなる保証を要求することができる。これは、正体不明の不正人物がキーを捕捉したかどうかを判定するためにすることができる。このさらなる保証は、対応するキー、または数ある情報の中でも以前に開示された情報を利用しなければ復号および／または回答できないメッセージまたは問いかけを他方に送信することを含むことができる。

【００５５】

非対称公開キーがマッチしない場合、または非対称公開キーが生成されていない場合、制御は要求関数６１０に渡る。要求関数６１０は、サーバからＩＤキーを要求すること、またはサーバによってクライアントからより多くの情報を要求することを含むことができる。クライアントが以前にサーバ、またはウェブサイト、にアクセスしたことがあり、この関数が開始される場合、ユーザおよび／またはサーバは、ウェブサイトが真正なものではないこと、またはクライアントと称しているものが実はそうではないことの何らかの表示を有することができる。これは、ユーザまたはサーバに対して、別のエンティティがそのプリンシパルからＩＤ情報を入手しようと試みていることを示しているかもしれない。

これは、サーバまたはクライアントが非対称公開キーまたは非対称秘密キーを失ったか、あるいはサーバまたはクライアントが不正行為を被ったことを示しているかもしれない。これらのシナリオのいずれにおいても、クライアントのユーザまたはサーバは、このシステムは信頼できないものであり、相手方に何らかの情報を開示するときに警戒すべきであることの表示を有することができる。

【００５６】

例示的な実施形態のさまざまな具体化の論理オペレーションは、（１）コンピュータで実施されたアクトのシーケンスや、コンピューティングシステム上で稼働するプログラムモジュールとして、および／または（２）コンピューティングシステム内で相互に接続されたマシンロジック回路または回路モジュールとして実装することができる。この実装は、本発明を実装するコンピューティングシステムのパフォーマンス要件に応じた選択の問題である。したがって、本明細書に記載の例示的な実施形態の具体化を構成する論理オペレーションは、オペレーション、構造的なデバイス、アクト、あるいはモジュールなど、さまざまに呼ばれる。これらのオペレーション、構造的なデバイス、アクト、およびモジュールは、本明細書に添付されている特許請求の範囲内に記載された本開示の趣旨および範囲から逸脱することなく、ソフトウェア、ファームウェア、専用のデジタルロジック、および／またはそれらの任意の組合せにおいて実装できることが当業者によって認識されるであろう。

【００５７】

例示的な実施形態について、コンピュータの構造的な特徴、方法論的なアクト、およびコンピュータ可読メディアに特有の言葉で説明したが、添付の特許請求の範囲において定義される例示的な実施形態は、説明した特定の構造、アクト、またはメディアに必ずしも限定されるものではないことを理解されたい。一例として、ＸＭＬ以外の異なるフォーマットを使用して、ＩＤ情報を符号化することができる。それゆえ、それらの特定の構造的な特徴、アクト、およびメディアは、特許請求されている本発明を実装する例示的な実施形態として開示されている。

【００５８】

上述のさまざまな実施形態は、例示としてのみ提供され、本開示を限定するものとして解釈すべきではない。本明細書で例示および説明されている例示的な実施形態および用途に従うことなく、また添付の特許請求の範囲に示された本開示の真の趣旨および範囲から逸脱することなく、本開示に対して行うことができるさまざまな修正および変更について当業者は容易に認識するであろう。

【図面の簡単な説明】

【００５９】

【図１】例示的な一実施形態に従って（１つまたは複数の）非対称キーのペアを作成し、継続中のデジタル関係を認識するためのシステムを示すブロック図である。

【図２】例示的な実施形態を実装できる適切なコンピューティングシステム環境の一例を示す図である。

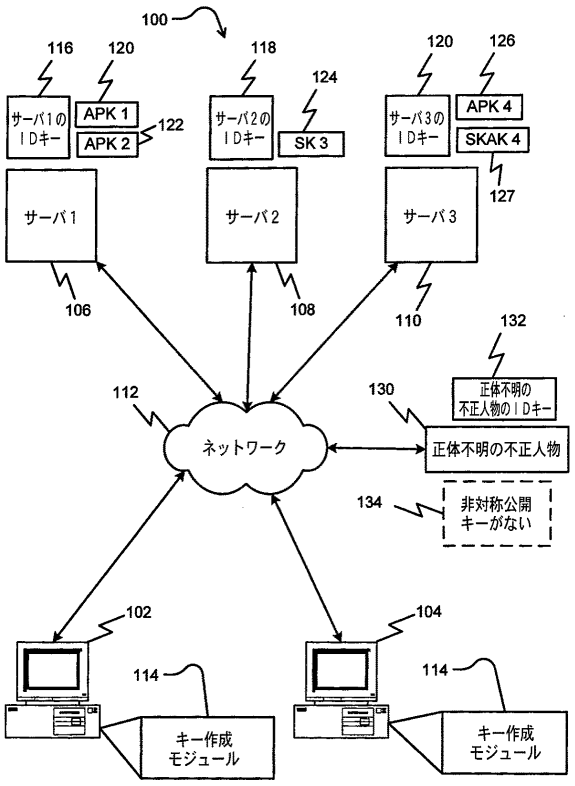
【図３】例示的な一実施形態に従って（１つまたは複数の）非対称キーのペアを作成し、システムを認証するためのシステムを示すブロック図である。

【図４】例示的な一実施形態に従って（１つまたは複数の）非対称キーのペアを作成し、継続中のデジタル関係を認識することに伴うオペレーション上の特徴を例示する流れ図である。

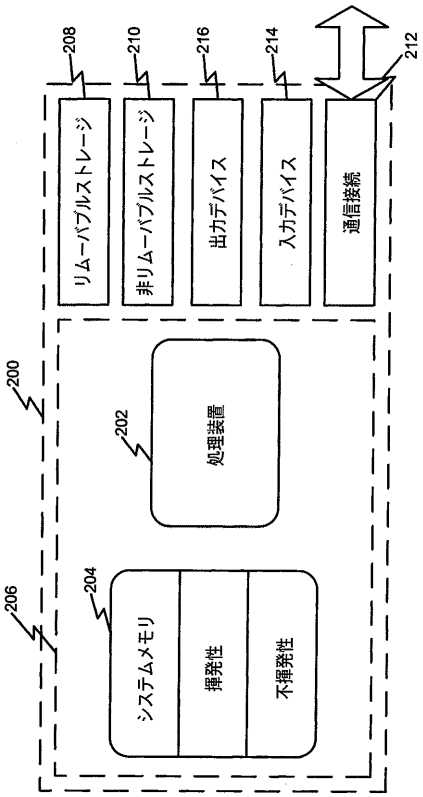
【図５】例示的な一実施形態に従って（１つまたは複数の）非対称キーのペアを作成し、継続中のデジタル関係を認識することに伴うさらなるオペレーション上の特徴を例示する流れ図である。

【図６】例示的な一実施形態に従ってシステムを認証することに伴うオペレーション上の特徴を例示する流れ図である。

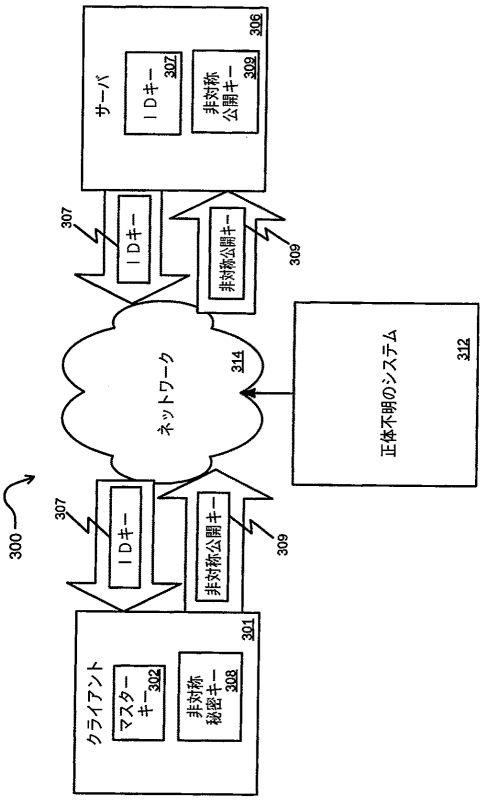
【図１】


100
116
120
118
124
120
126
サーバ1のIDキー
APK 1
APK 2
122
サーバ2のIDキー
SK 3
サーバ3のIDキー
APK 4
SKAK 4
127
サーバ1
サーバ2
サーバ3
106
108
110
132
正体不明の不正人物のIDキー
112
130
ネットワーク
正体不明の不正人物
134
非対称公開キーがない
102
104
114
114
キー作成モジュール
キー作成モジュール

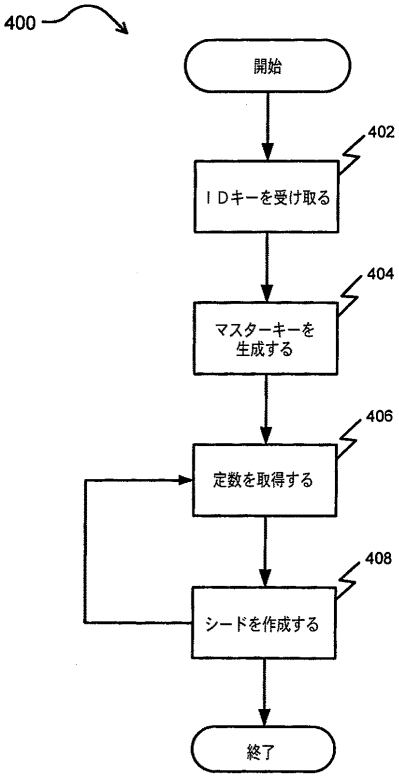
【図２】


208
210
216
214
212
リムーバブルストレージ
非リムーバブルストレージ
出力デバイス
入力デバイス
通信接続
200
202
処理装置
206
204
システムメモリ
揮発性
不揮発性

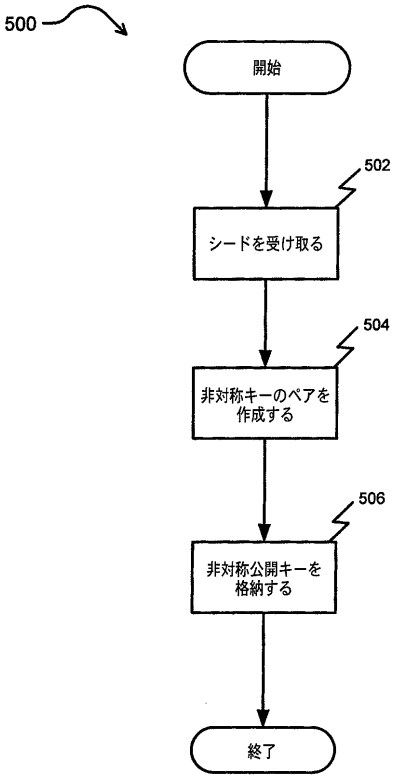
【図３】


306
サーバ
IDキー
307
非対称公開キー
309
307
IDキー
非対称公開キー
309
ネットワーク
314
正体不明のシステム
312
300
307
IDキー
非対称公開キー
309
301
クライアント
マスターキー
302
非対称秘密キー
308

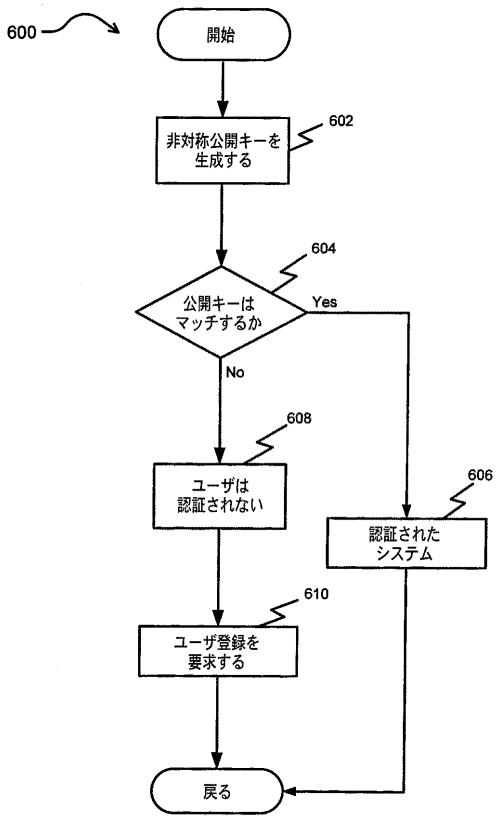
【図４】


400
開始
402
IDキーを受け取る
404
マスターキーを生成する
406
定数を取得する
408
シードを作成する
終了

【図５】


500
開始
502
シードを受け取る
504
非対称キーのペアを作成する
506
非対称公開キーを格納する
終了

【図６】


600
開始
602
非対称公開キーを生成する
604
公開キーはマッチするか
Yes
No
608
ユーザは認証されない
606
認証されたシステム
610
ユーザ登録を要求する
戻る

フロントページの続き

(72)発明者　アルン　ケー．ナンダ
アメリカ合衆国　９８０５２　ワシントン州　レッドモンド　ワン　マイクロソフト　ウェイ　マイクロソフト　コーポレーション内
(72)発明者　ダニエル　アール．シモン
アメリカ合衆国　９８０５２　ワシントン州　レッドモンド　ワン　マイクロソフト　ウェイ　マイクロソフト　コーポレーション内
(72)発明者　ジョン　ピー．シューチュク
アメリカ合衆国　９８０５２　ワシントン州　レッドモンド　ワン　マイクロソフト　ウェイ　マイクロソフト　コーポレーション内
(72)発明者　ジョシュ　ディー．ベナロー
アメリカ合衆国　９８０５２　ワシントン州　レッドモンド　ワン　マイクロソフト　ウェイ　マイクロソフト　コーポレーション内
(72)発明者　キム　キャメロン
アメリカ合衆国　９８０５２　ワシントン州　レッドモンド　ワン　マイクロソフト　ウェイ　マイクロソフト　コーポレーション内

審査官　金沢　史明

(56)参考文献　特表２００５－５００７４０（ＪＰ，Ａ）
特開２００４－３３６７９４（ＪＰ，Ａ）

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