(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第6573600号
(P6573600)
(45)発行日　令和1年9月11日(2019.9.11)　(24)登録日　令和1年8月23日(2019.8.23)

(51)Int.Cl.　F I
H04L 9/14 (2006.01)　H04L 9/00 641
H04L 9/08 (2006.01)　H04L 9/00 601E

請求項の数 13　(全 17 頁)

(21)出願番号　特願2016-510656(P2016-510656)
(86)(22)出願日　平成26年4月23日(2014.4.23)
(65)公表番号　特表2016-517248(P2016-517248A)
(43)公表日　平成28年6月9日(2016.6.9)
(86)国際出願番号　PCT/SG2014/000181
(87)国際公開番号　WO2014/175830
(87)国際公開日　平成26年10月30日(2014.10.30)
審査請求日　平成29年4月21日(2017.4.21)
(31)優先権主張番号　201303260-2
(32)優先日　平成25年4月25日(2013.4.25)
(33)優先権主張国・地域又は機関
シンガポール(SG)

前置審査

(73)特許権者　515295533
ツリーボックス・ソリューションズ・ピーティーイー・リミテッド
シンガポール・シンガポール・１４９５４４・コモンウェルス・レーン・１・＃０７－２５
(74)代理人　100108453
弁理士　村山　靖彦
(74)代理人　100110364
弁理士　実広　信哉
(74)代理人　100133400
弁理士　阿部　達彦

最終頁に続く

(54)【発明の名称】エンドツーエンド暗号化通信を許可するために第１のコンピューティングデバイスから第２のコンピューティングデバイスへのデータパケットを処理するための少なくとも１つのサーバによっ

(57)【特許請求の範囲】
【請求項１】
第1のコンピューティングデバイスから第2のコンピューティングデバイスに伝送されることになるデータパケットを処理するための、少なくとも1つのサーバによって実行される方法であって、前記方法は、
データパケットを前記第1のコンピューティングデバイスから受信するステップであって、前記データパケットは、暗号化されたメッセージを形成するために第1の暗号化鍵を使用して暗号化されたメッセージと、暗号化された識別データを形成するために第2の暗号化鍵を使用して暗号化された前記第2のコンピューティングデバイスの識別データと、前記第2のコンピューティングデバイスに関連付けられた第3の暗号化鍵を使用して前記第1の暗号化鍵を暗号化することによって形成された暗号化された第1の暗号化鍵と、前記サーバの公開鍵を使用して暗号化された第2の暗号化鍵と、前記暗号化されたメッセージに基づいて生成された認証チェックサムとを備える、ステップと、
前記サーバによって前記認証チェックサムを認証するステップと、
前記サーバの秘密鍵を使用して、前記暗号化された第2の暗号化鍵を復号するステップと、
前記復号された第2の暗号化鍵を使用して前記暗号化された識別データを復号するステップと、
前記復号された識別データに基づいて前記データパケットを前記第2のコンピューティングデバイスに伝送するステップとを含み、

前記暗号化されたメッセージおよび第1の暗号化鍵は、前記第1と前記第2のコンピューティングデバイス間でのエンドツーエンド暗号化通信を許可するために、前記サーバによる復号が不可能なように配置構成され、
前記暗号化された第1の暗号化鍵は、前記第2のコンピューティングデバイスに関連付けられた第4の暗号化鍵を使用するだけで復号が可能なように配置構成され、
前記第3および第4の暗号化鍵はそれぞれ、前記第2のコンピューティングデバイスの公開鍵および秘密鍵である、方法。
【請求項２】
前記データパケットを伝送するステップは、SMS、MMS、インスタントメッセージング、電子メール、添付、または電子文書送達サービスを介して伝送するステップを含む、請求項１に記載の方法。
【請求項３】
前記メッセージは、テキスト、イメージ、アニメーション、ビデオ、またはオーディオを含む、請求項１または２に記載の方法。
【請求項４】
前記データパケットは初期化ベクトルをさらに含む、請求項１から３のいずれか一項に記載の方法。
【請求項５】
第1と第2のコンピューティングデバイス間でのエンドツーエンド暗号化通信を許可するために、少なくとも1つのサーバを介して前記第2のコンピューティングデバイスに伝送されることになる情報を処理するための、前記第1のコンピューティングデバイスによって実行される方法であって、
第1および第2の暗号化鍵を使用して前記第2のコンピューティングデバイスのメッセージおよび識別データをそれぞれ暗号化するステップと、
前記第2のコンピューティングデバイスの公開鍵を使用して前記第1の暗号化鍵を暗号化するステップと、
前記サーバの公開鍵を使用して前記第2の暗号化鍵を暗号化するステップと、
暗号化されたメッセージに基づいて認証チェックサムを生成するステップと、
前記暗号化されたメッセージ、識別データ、第1および第2の暗号化鍵、ならびに前記認証チェックサムをまとめて、データパケットとして伝送するステップとを含む、方法。
【請求項６】
前記メッセージは、テキスト、イメージ、アニメーション、ビデオ、またはオーディオを含む、請求項５に記載の方法。
【請求項７】
前記データパケットを伝送するステップは、SMS、MMS、インスタントメッセージング、電子メール、添付、または電子文書送達サービスを介して伝送するステップを含む、請求項５または６に記載の方法。
【請求項８】
前記第1のコンピューティングデバイスのユーザが、複数のメッセージから前記メッセージを、および前記データパケットを受信できる複数のコンピューティングデバイスから前記第2のコンピューティングデバイスを、選択することを可能にするためのインターフェースを表示するステップをさらに含む、請求項５から７のいずれか一項に記載の方法。
【請求項９】
前記データパケットは、初期化ベクトルをさらに含む、請求項５から８のいずれか一項に記載の方法。
【請求項１０】
第1と第2のコンピューティングデバイス間でのエンドツーエンド暗号化通信を許可するために、少なくとも1つのサーバを介して前記第1と第2のコンピューティングデバイス間でデータパケットを交換するためのシステムであって、
前記第1のコンピューティングデバイスであって、

第1および第2の暗号化鍵を使用して、メッセージおよび前記第2のコンピューティングデバイスの識別データをそれぞれ暗号化するため、
前記第1および第2の暗号化鍵を暗号化するため、および
暗号化されたメッセージに基づいて認証チェックサムを生成するための
暗号化モジュールと、
前記暗号化されたメッセージ、識別データ、第1および第2の暗号化鍵、ならびに前記認証チェックサムをまとめて、前記データパケットとして前記サーバに伝送するための、伝送モジュールと
を含み、
前記暗号化された第1の暗号化鍵は、前記第2のコンピューティングデバイスに関連付けられた第3の暗号化鍵を使用して前記第1の暗号化鍵を暗号化することによって形成され、前記暗号化された第2の暗号化鍵は、前記サーバの公開鍵を使用して前記第2の暗号化鍵を暗号化することによって形成される、前記第1のコンピューティングデバイスと、
前記サーバであって、前記第1のコンピューティングデバイスから受信した前記データパケットを処理するように構成され、
前記認証チェックサムを認証するため、
前記サーバの秘密鍵を使用して、前記データパケットの前記暗号化された第2の暗号化鍵を復号するため、および、
前記復号された第2の暗号化鍵を使用して前記データパケットの前記暗号化された識別データを復号するための、
復号モジュールと、
前記復号された識別データに基づいて前記第2のコンピューティングデバイスに前記データパケットを伝送するための伝送モジュールと
を含み、前記暗号化されたメッセージおよび第1の暗号化鍵は、前記サーバによる復号が不可能なように配置構成される、前記サーバと、
前記第2のコンピューティングデバイスであって、前記サーバから受信した前記データパケットを処理するように構成され、
前記データパケットの前記暗号化された第1の暗号化鍵を復号するため、および
前記メッセージを取得するために前記復号された第1の暗号化鍵を使用して前記データパケットの前記暗号化されたメッセージを復号するための、
復号モジュールを含む、前記第2のコンピューティングデバイスとを含み、
前記暗号化された第1の暗号化鍵は、前記第2のコンピューティングデバイスに関連付けられた第4の暗号化鍵を使用するだけで復号が可能なように配置構成され、
前記第3および第4の暗号化鍵はそれぞれ、前記第2のコンピューティングデバイスの公開鍵および秘密鍵である、システム。

【請求項１１】

前記サーバの前記伝送モジュールは、SMS、MMS、インスタントメッセージング、電子メール、添付、または電子文書送達サービスを使用して前記データパケットを伝送するように構成されることを含む、請求項１０に記載のシステム。

【請求項１２】

前記メッセージは、テキスト、イメージ、アニメーション、ビデオ、またはオーディオを含む、請求項１０または１１に記載のシステム。

【請求項１３】

前記データパケットは、初期化ベクトルをさらに含む、請求項１０から１２のいずれか一項に記載のシステム。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、エンドツーエンド暗号化通信を許可するために第1のコンピューティングデバイスから第2のコンピューティングデバイスへのデータパケットを処理するための少な

くとも1つのサーバによって実行される方法、および対応するシステムに関する。
【背景技術】
【０００２】
現在、あるメッセージングソリューションは、たとえば通信ネットワーク内の2つのコンピューティングデバイス、送信者と受信者との間にサーバが配置構成されたシナリオにおいて、2つの異なる暗号化-復号方法を実行する。送信者は、ランダムに生成された対称鍵を使用してメッセージを暗号化する。次いで送信者は、サーバの公開鍵を使用して対称鍵を暗号化した後、暗号化されたメッセージおよび対称鍵を含むデータパッケージをサーバに伝送する。サーバは、暗号化された対称鍵をそれ独自の秘密鍵を使用して復号した後、受信者の公開鍵を用いて対称鍵を再暗号化し、再フォーマットされたデータパッケージは受信者に転送される。しかしながら、サーバは対称鍵を有するため、暗号化されたメッセージにアクセスできることを理解されよう。受信者はデータパッケージを受信すると、暗号化されたメッセージを復号するために使用される対称鍵を取り出すために、暗号化された対称鍵をそれ独自の秘密鍵を用いて復号する。こうしたシナリオのために、サーバは対称鍵のコピーを有し、監査目的または復号されたメッセージの保管のために、暗号化されたメッセージを復号することができる。しかしながら、サーバはメッセージの内容にアクセスできるため、これは真のエンドツーエンドの暗号化通信とはみなされない。
【０００３】
他の従来の実装では、サーバは新しい対称鍵を再生成し、新しい対称鍵を用いてメッセージを再暗号化し、受信者の公開鍵を用いて新しい対称鍵を暗号化するように構成することができる。この状況において、それでもなおサーバは暗号化されたメッセージにアクセスできるため、真のエンドツーエンド暗号化通信を実行することはできない。
【発明の概要】
【発明が解決しようとする課題】
【０００４】
したがって本発明の一目的は、従来技術の問題のうちの少なくとも1つに対処すること、および/または、当分野で有用な選択肢を提供することである。
【課題を解決するための手段】
【０００５】
本発明の第1の態様によれば、第1のコンピューティングデバイスから第2のコンピューティングデバイスに伝送されることになるデータパケットを処理するための、少なくとも1つのサーバによって実行される方法が提供され、データパケットは、暗号化されたメッセージを形成するために第1の暗号化鍵を使用して暗号化されるメッセージと、暗号化された識別データを形成するために第2の暗号化鍵を使用して暗号化される第2のコンピューティングデバイスの識別データと、暗号化された第1および第2の暗号化鍵とを含む。方法は、暗号化された第2の暗号化鍵を復号すること、復号された第2の暗号化鍵を使用して暗号化された識別データを復号すること、および、復号された識別データに基づいてデータパケットを伝送することを含む。暗号化されたメッセージおよび第1の暗号化鍵は、第1と第2のコンピューティングデバイス間でのエンドツーエンド暗号化通信を許可するために、サーバによる復号が不可能なように配置構成される。
【０００６】
方法は、有利なことに、データパケットの再ルーティングを実行するために暗号化されたメッセージを中間サーバを介して転送することによって、送信者が暗号化されたメッセージを受信者に送信できるようにする、複数鍵暗号化方式の実現を可能にするが、サーバは、この能力を用いて暗号化されたメッセージを復号することはできない。これにより、送信者と受信者の間に真のエンドツーエンド暗号化が達成されることが有利に保証される。
【０００７】
好ましくは、暗号化された第2の暗号化鍵を復号することは、復号を実行するためにサーバの秘密鍵を使用することを含み得る。また、データパケットを伝送することは、SMS

、MMS、インスタントメッセージング、電子メール、添付または電子文書送達サービスを介して伝送することを含み得る。メッセージは、テキスト、イメージ、アニメーション、ビデオ、またはオーディオを含むことができる。第1の暗号化鍵が第2のコンピューティングデバイスの公開鍵を使用して暗号化され得るか、または代替として、第1の暗号化鍵がサーバの公開鍵を使用して暗号化され得ることを理解されよう。より好ましくは、第2の暗号化鍵はサーバの公開鍵を使用して暗号化され得る。さらに好ましくは、データパケットは初期化ベクトル、および暗号化されたメッセージに基づいて生成されたデジタル署名を、さらに含むことができる。

【０００８】

本発明の第2の態様によれば、第1と第2のコンピューティングデバイス間でのエンドツーエンド暗号化通信を許可するために、少なくとも1つのサーバを介して第2のコンピューティングデバイスに伝送されることになる情報を処理するための、第1のコンピューティングデバイスによって実行される方法が提供される。方法は、第1および第2の暗号化鍵を使用して第2のコンピューティングデバイスのメッセージおよび識別データをそれぞれ暗号化すること、第1および第2の暗号化鍵を暗号化すること、および、暗号化されたメッセージ、識別データ、第1および第2の暗号化鍵をまとめて、データパケットとして伝送することを含む。

【０００９】

好ましくは、メッセージは、テキスト、イメージ、アニメーション、ビデオ、またはオーディオを含むことができる。さらに、データパケットを伝送することは、SMS、MMS、インスタントメッセージング、電子メール、添付または電子文書送達サービスを介して伝送することを含むことができる。より好ましくは、第1の暗号化鍵を暗号化することは、第2のコンピューティングデバイスの暗号化鍵またはサーバの暗号化鍵を使用して暗号化することを含むことができる。加えて、第2のコンピューティングデバイスの暗号化鍵はその公開鍵を含むことができ、サーバの暗号化鍵はその公開鍵を含むことができる。第2の暗号化鍵を暗号化することは、サーバの暗号化鍵を使用して暗号化することを含むことができる。サーバの暗号化鍵は、その公開鍵を含むことができる。

【００１０】

好ましくは、方法は、第1のコンピューティングデバイスのユーザが、複数のメッセージからメッセージを、およびデータパケットを受信できる複数のコンピューティングデバイスから第2のコンピューティングデバイスを、選択することを可能にするためのインターフェースを表示することをさらに含むことができる。データパケットは、初期化ベクトル、および暗号化されたメッセージに基づいて生成されたデジタル署名を、さらに含むことができる。

【００１１】

本発明の第3の態様によれば、第1と第2のコンピューティングデバイス間でのエンドツーエンド暗号化通信を許可するために、少なくとも1つのサーバを介して転送された第2のコンピューティングデバイスからのデータパケットを処理するための、第1のコンピューティングデバイスによって実行される方法が提供され、データパケットは、暗号化されたメッセージを形成するために第1の暗号化鍵を使用して暗号化されるメッセージと、暗号化された識別データを形成するために第2の暗号化鍵を使用して暗号化される第1のコンピューティングデバイスの識別データと、暗号化された第1および第2の暗号化鍵とを含む。方法は、暗号化された第1の暗号化鍵を復号すること、および、メッセージを取得するために復号された第1の暗号化鍵を使用して暗号化されたメッセージを復号することを含む。

【００１２】

好ましくは、暗号化された第1の暗号化鍵を復号することは、復号を実行するために第1のコンピューティングデバイスの秘密鍵を使用することを含むことができる。

【００１３】

本発明の第4の態様によれば、第1と第2のコンピューティングデバイス間でのエンドツ

ーエンド暗号化通信を許可するために、少なくとも1つのサーバを介して第1と第2のコンピューティングデバイス間でデータパケットを交換するためのシステムが提供される。システムは、第1および第2のコンピューティングデバイスと、サーバとを備える。第1のコンピューティングデバイスは、第1および第2の暗号化鍵を使用して、メッセージおよび第2のコンピューティングデバイスの識別データをそれぞれ暗号化するため、ならびに第1のおよび第2の暗号化鍵を暗号化するための、暗号化モジュールと、暗号化されたメッセージ、識別データ、ならびに第1のおよび第2の暗号化鍵をまとめて、データパケットとしてサーバに伝送するための、伝送モジュールとを含む。サーバは、第1のコンピューティングデバイスから受信したデータパケットを処理するように構成され、データパケットの暗号化された第2の暗号化鍵を復号するため、および復号された第2の暗号化鍵を使用してデータパケットの暗号化された識別データを復号するための、復号モジュールと、復号された識別データに基づいて第2のコンピューティングデバイスにデータパケットを伝送するための伝送モジュールとを含み、暗号化されたメッセージおよび第1の暗号化鍵は、サーバによる復号が不可能なように配置構成される。第2のコンピューティングデバイスは、サーバから受信したデータパケットを処理するように構成され、データパケットの暗号化された第1の暗号化鍵を復号するため、およびメッセージを取得するために復号された第1の暗号化鍵を使用してデータパケットの暗号化されたメッセージを復号するための、復号モジュールを含む。

【００１４】

好ましくは、サーバの復号モジュールは、暗号化された第2の暗号化鍵を復号するために、サーバの秘密鍵を使用するように構成されることを含むことができる。他方で、サーバの伝送モジュールは、SMS、MMS、インスタントメッセージング、電子メール、添付または電子文書送達サービスを使用してデータパケットを伝送するように構成されることを含むことができる。メッセージは、テキスト、イメージ、アニメーション、ビデオ、またはオーディオを含むことができる。第1の暗号化鍵を暗号化するために第1のコンピューティングデバイスの暗号化モジュールによって使用される第2のコンピューティングデバイスの暗号化鍵は、好ましくは第2のコンピューティングデバイスの公開鍵を含むことができる。

【００１５】

好ましくは、第1のコンピューティングデバイスの暗号化モジュールは、第2のコンピューティングデバイスの暗号化鍵またはサーバの暗号化鍵を使用して、第1の暗号化鍵を暗号化するようにさらに構成され得る。加えて、第1のコンピューティングデバイスの暗号化モジュールは、サーバの暗号化鍵を使用して、第2の暗号化鍵を暗号化するようにさらに構成され得る。

【００１６】

好ましくは、第2の暗号化鍵を暗号化するために第1のコンピューティングデバイスの暗号化モジュールによって使用されるサーバの暗号化鍵は、サーバの公開鍵を含むことができる。データパケットは、初期化ベクトルと、暗号化されたメッセージに基づいて生成されたデジタル署名とを、さらに含むことができる。

【００１７】

本発明の第5の態様によれば、暗号化デバイスとコンピューティングデバイスとの間でのエンドツーエンド暗号化通信を許可するために、少なくとも1つのサーバを介してコンピューティングデバイスに伝送されることになる情報を処理するための、暗号化デバイスが提供される。暗号化デバイスは、第1および第2の暗号化鍵を使用して、メッセージおよびコンピューティングデバイスの識別データをそれぞれ暗号化するため、ならびに、第1および第2の暗号化鍵を暗号化するための、暗号化モジュールと、暗号化されたメッセージ、識別データ、第1および第2の暗号化鍵をまとめて、データパケットとして伝送するための、伝送モジュールとを備える。

【００１８】

本発明の第6の態様によれば、復号デバイスとコンピューティングデバイスとの間での

エンドツーエンド暗号化通信を許可するために、少なくとも1つのサーバを介して転送されたコンピューティングデバイスからのデータパケットを処理するための、復号デバイスが提供され、データパケットは、暗号化されたメッセージを形成するために第1の暗号化鍵を使用して暗号化されるメッセージと、暗号化された識別データを形成するために第2の暗号化鍵を使用して暗号化される第1のコンピューティングデバイスの識別データと、暗号化された第1および第2の暗号化鍵とを含む。復号デバイスは、暗号化された第1の暗号化鍵を復号するため、および、メッセージを取得するために復号された第1の暗号化鍵を使用して暗号化されたメッセージを復号するための、復号モジュールを備える。

【００１９】

本発明の第7の態様によれば、第2のコンピューティングデバイスに伝送されることになる第1のコンピューティングデバイスからのデータパケットを処理するために、少なくとも1つのサーバによって実行される方法が提供され、データパケットは、暗号化されたメッセージを形成するために第1の暗号化鍵を使用して暗号化されるメッセージと、暗号化された識別データを形成するために第2の暗号化鍵を使用して暗号化される第2のコンピューティングデバイスの識別データと、第2のコンピューティングデバイスに関連付けられた第3の暗号化鍵を使用して第1の暗号化鍵を暗号化することによって形成される、暗号化された第1の暗号化鍵と、サーバに関連付けられた暗号化鍵を使用して第2の暗号化鍵を暗号化することによって形成される、暗号化された第2の暗号化鍵とを含む。方法は、暗号化された第2の暗号化鍵を復号すること、復号された第2の暗号化鍵を使用して暗号化された識別データを復号すること、および、復号された識別データに基づいてデータパケットを伝送することを含む。暗号化された第1の暗号化鍵は、第2のコンピューティングデバイスに関連付けられた第4の暗号化鍵を使用してのみ復号され得るように配置構成され、第2のコンピューティングデバイスの第3および第4の暗号化鍵は、非対称鍵のペアとして構成される。

【００２０】

好ましくは、サーバに関連付けられた暗号化鍵はサーバの公開鍵を含むことができる。続いて、暗号化された第2の暗号化鍵を復号することは、復号を実行するためにサーバの秘密鍵を使用することを含むことができる。さらに、データパケットを伝送することは、SMS、MMS、インスタントメッセージング、電子メール、添付または電子文書送達サービスを介して伝送することを含むことができる。メッセージは、テキスト、イメージ、アニメーション、ビデオ、またはオーディオを含むことができる。さらに好ましくは、第3および第4の暗号化鍵は、それぞれ、第2のコンピューティングデバイスの公開鍵および秘密鍵を含むことができる。データパケットは、初期化ベクトル、および暗号化されたメッセージに基づいて生成されたデジタル署名を、さらに含むことができる。

【００２１】

本発明の一態様に関する機能は、本発明の他の態様にも適用可能であり得ることが明らかとなろう。

【００２２】

本発明のこれらおよび他の態様は、以下で説明する実施形態に関して明らかとなり、解明されるであろう。

【００２３】

本発明の実施形態は、添付の図面に関して以下で開示される。

【図面の簡単な説明】

【００２４】

【図１】本発明の実施形態に従った、エンドツーエンド暗号化通信を許可するために、サーバを介して第1と第2のコンピューティングデバイス間でデータパケットを交換するためのシステムを示す、概略図である。

【図２】図1の第1および第2のコンピューティングデバイスならびにサーバの構成を示す、図2aから図2cを含む図である。

【図３】データパケットとして第2のコンピューティングデバイスに伝送されることにな

る情報を処理するための、図1の第1のコンピューティングデバイスによって実行される方法を示すフロー図である。
【図４】データパケットのフォーマットを示す図である。
【図５】第1のコンピューティングデバイスから受信したデータパケットを処理するための、図1のサーバによって実行される方法を示すフロー図である。
【図６】サーバから受信したデータパケットを処理するための、図1の第2のコンピューティングデバイスによって実行される方法を示すフロー図である。
【発明を実施するための形態】
【００２５】
第1の実施形態に従い、エンドツーエンド暗号化通信を許可するために、少なくとも1つのサーバ108を介して第1と第2とのコンピューティングデバイス104、106(すなわち2つのパーティ)間でデータパケット102を交換するための、システム100(すなわち図1を参照)および対応する方法500(すなわち図5を参照)が開示される。システム100は、第1および第2のコンピューティングデバイス104、106、ならびに、第1および第2のコンピューティングデバイス104、106の中間に立体的に配置構成されたサーバ108を含む。サーバ108は、公開鍵インフラストラクチャ(すなわち非対称鍵暗号化)用語のように、公開鍵および秘密鍵に関連付けて構成されることを理解されよう。同様に、第2のコンピューティングデバイス106も、公開鍵および秘密鍵に関連付けて構成される。図1との関連において、第1のコンピューティングデバイス104はデータパケット102の送信者であり、第2のコンピューティングデバイス106はデータパケット102の最終的に意図された受信者である。しかし他の例では、反対の関係、すなわち第2のコンピューティングデバイス106が送信者になり、第1のコンピューティングデバイス104が受信者になることが可能であることも理解されよう。特に、システム100は、送信者と受信者との間での真のエンドツーエンド暗号化通信を可能にし、さらにサーバ108がデータパケット102をセキュアにルーティングできるようにするが、メッセージのコンテンツにアクセスするためにデータパケット102に埋め込まれたセキュアメッセージを復号することはできない。また、図示および説明を簡略化するために、図1には1つのサーバ102のみが示されているが、データパケット102は、第2のコンピューティングデバイス106によって受信される前に、複数のサーバ108(すなわちサーバクラスタ)を介して転送され得ることを理解されよう。複数のサーバ108の当該シナリオでは、サーバ108の各々が、公開鍵および秘密鍵の共通セット(たとえば、各サーバ108上にローカルに記憶され得るか、またはすべての複数のサーバ108によって等しくアクセス可能なストレージサーバ上に記憶され得る)にアクセスできるように構成されることを理解されよう。具体的に言えば、公開鍵および秘密鍵の共通セットは、以下で詳述される、第2のコンピューティングデバイス106の識別データを暗号化および復号する目的で使用されることになる。第1および第2のコンピューティングデバイス104、106、ならびにサーバ108は、通信ネットワーク内に常駐することをさらに理解されよう。
【００２６】
第1および第2のコンピューティングデバイス104、106の例は、モバイルコンピューティングデバイス(たとえばiPhone(商標)などのスマートフォンまたはiPad(商標)などのタブレット)、ワイヤードコンピュータ(たとえばデスクトップパーソナルコンピュータ)などを含む。しかしながら、本実施形態では、第1および第2のコンピューティングデバイス104、106は、所定の好適なモバイルオペレーティングシステム(たとえばApple Inc(商標)からのiOS(商標))上で実行するモバイルコンピューティングデバイスである。以下で参照しやすくするために、特に明示的に示されていない限り、第1および第2のコンピューティングデバイス104、106は、(真のエンドツーエンド暗号化通信関係との関連において)それぞれ暗号化デバイス104および復号デバイス106と呼ばれる。互いに異なるデータパケット102を交換するために、通信ネットワークのシステム100内に複数の暗号化デバイス104および復号デバイス106が配置され得るが、簡潔にするために、このインスタンスでは図1内に具体的に示されていないことも理解されよう。サーバ108に関して、例は、暗号化デバイス104と復号デバイス106との間でデータパケット102のルーティングのタスクを実行する

ために好適に構成された、任意のタイプのサーバを含む。

【００２７】

図2を参照すると、暗号化デバイス104は、復号デバイス106に提供されることになるデータパケット102内に情報を処理するための暗号化プログラムコード(図示せず)を実行するように構成され、復号デバイス106は、受信したデータパケット102を処理するための復号プログラムコード(図示せず)を実行するように構成される。他方で、サーバ108は、暗号化デバイス104によって復号デバイス106に送信されたデータパケット102を処理するために、図5の方法500に基づく、データパケット処理コード(図示せず)を実行するように構成される。本実施形態において、暗号化および復号のプログラムコードは、暗号化デバイスおよび復号デバイス104、106上にローカルにインストールされ、さらに暗号化および復号のプログラムコードは、ネイティブなモバイルアプリケーションとして(たとえばユーザによる使用が可能なソフトウェアとして)具体化されることを理解されよう。具体的に言えば、暗号化デバイス104は、暗号化モジュール1042、表示モジュール1046、伝送モジュール1048、およびプロセッサモジュール10410の、モジュールを含み、復号デバイス106は、受信側モジュール1062および復号モジュール1064の、モジュールを含む。同様に、データパケット処理コードは、特定用途向けプログラム(背景プロセスとして実行するように構成され得る)として実装され、サーバ108上にローカルにインストールされる。サーバ108については、受信側モジュール1082、復号モジュール1084、および伝送モジュール1086の、モジュールが内部に配置構成される。この例において、暗号化デバイス204および復号デバイス206のそれぞれの当該モジュールはソフトウェア内に実装され、したがってそれぞれが暗号化プログラムコードおよび復号プログラムコード内に組み込まれることを理解されよう。これは、サーバ108の当該モジュールに準用する。

【００２８】

次に、図3および図4を参照して、エンドツーエンド暗号化通信を許可するために、サーバ108を介して復号デバイス106(すなわち受信者)に伝送されることになる情報を処理するための、暗号化デバイス104(すなわち送信者)によって実行される方法300を説明する。方法300のステップ302で、表示モジュール1046は、暗号化デバイス104のユーザ(図示せず)が、復号デバイス106に送信されることになる複数のメッセージから所望のメッセージ(すなわち入力データ)を選択できるようにするための、ソフトウェアインターフェース(図示せず)を表示するように配置構成される。メッセージは、テキスト、イメージ、アニメーション、ビデオ、オーディオなどを含むことを理解されよう。加えて、ステップ302で、ユーザはソフトウェアインターフェースを使用して、選択されたメッセージの受信者も(複数のデバイスから)選択するが、この状況では復号デバイス106である。さらに、インターフェースは、エンドツーエンド暗号化をユーザが所望しているかどうかに関するオプションも表示する。ユーザがエンドツーエンド暗号化オプションを選択すると、暗号化デバイス104は図4に示されるようなセキュアなパケットフォーマット400に基づいて、選択されたメッセージを埋め込むためのデータパケット102の準備に進む。また、エンドツーエンド暗号化通信を進めるために、次いで暗号化デバイス104は、対称型メッセージ暗号化鍵(図示せず)および受信者情報暗号化鍵(図示せず)をランダムに生成するように構成され、その目的は以下で詳述する。加えて、メッセージ暗号化鍵および受信者情報暗号化鍵の新しい固有セットが、暗号化デバイス104によって伝送されるように各データパケット102に対して生成される。データパケット102は標準IPパケットのペイロードとして埋め込まれ得ることを、さらに理解されよう。

【００２９】

図4を参照すると、パケットフォーマット400は、合計で7つのデータフィールド401～407を含むが、必要であれば、追加の必要データフィールドを追加することができる。具体的に言えば、7つのデータフィールド401～407は(パケットフォーマット400内のデータシーケンスの配置構成された順序に基づいて)、バージョン数フィールド401、暗号化されたメッセージ鍵フィールド402、暗号化された受信者情報鍵フィールド403、初期化ベクトルフィールド404、暗号化された受信者情報フィールド405、暗号化されたメッセージフィー

ルド406、およびデジタル署名フィールド407を含む。簡潔に言えば、バージョン数フィールド401は、使用中のパケットフォーマット400の現在のバージョンを定義し、暗号化されたメッセージ鍵フィールド402は、復号デバイス106の公開鍵を使用して暗号化されたメッセージ暗号化鍵を記憶するが、暗号化された受信者情報鍵フィールド403は、サーバ108の公開鍵を使用して暗号化された受信者情報暗号化鍵を記憶する。複数サーバ108を含むシナリオの場合、暗号化された受信者情報鍵フィールド403は、前述のように、すべてのサーバ108によるアクセスが可能な共通公開鍵を代わりに使用して暗号化された、受信者情報暗号化鍵を記憶する。初期化ベクトルフィールド404は、(当業者によって理解されるような)暗号化に使用される初期変数を定義し、暗号化された受信者情報フィールド405は、受信者情報暗号化鍵を使用して暗号化された復号デバイス106の識別データを記憶するが、暗号化されたメッセージフィールド406は、メッセージ暗号化鍵を使用して暗号化された選択されたメッセージを記憶し、デジタル署名フィールド407は、(暗号化されたメッセージフィールド406内に記憶されたような)暗号化されたメッセージに基づいて生成された認証チェックサムを記憶する。復号デバイス106の識別データは、サーバ108が、データパケット102を識別し、暗号化デバイス104から復号デバイス106へと転送およびルーティングできるようにする、復号デバイス106のIPアドレスなどの、関連付けられた位置情報を指すことを理解されよう。したがって、この例では復号デバイス106はデータパケット102の受信者であるため、識別データは受信者に関連付けられた位置情報である。暗号化デバイス104は、別々の通信チャネル/手段を介してサーバ108によって配布されるような、復号デバイス106の識別データを取得するが、これは本発明の考察の焦点ではないことを理解されよう。

【００３０】

暗号化デバイス104の表示モジュール1046によって表示されるソフトウェアインターフェースは、識別データがメッセージ(同じく暗号化される)とは別に暗号化され得るようにするために、メッセージから識別データを(なんらのユーザ介入も必要とせずに)自動的に分離することを理解されよう。次にこれについて、以下で詳述する。

【００３１】

図3の方法300について再度説明すると、ステップ304で、(暗号化デバイス104の)暗号化モジュール1042は、メッセージ暗号化鍵および受信者情報暗号化鍵を使用して、選択されたメッセージおよび復号デバイス106の識別データをそれぞれ暗号化し、暗号化されたメッセージおよび識別データをそれぞれ、(データパケット102の)暗号化されたメッセージフィールド406および暗号化された受信者情報フィールド405内に記憶する。(任意の好適な既存のチェックサムアルゴリズムを使用して)暗号化されたメッセージに基づき、(暗号化デバイス104の)プロセッサモジュール10410によって、対応する認証チェックサムも生成され、デジタル署名フィールド407に記憶される。その後、ステップ306で、(暗号化デバイス104の)暗号化モジュール1042は、復号デバイス106の公開鍵およびサーバ108の公開鍵をそれぞれ使用して、メッセージ暗号化鍵および受信者情報暗号化鍵を暗号化する。複数のサーバ108を備えるシナリオの場合、受信者情報暗号化鍵は代わりに、前述のように、すべてのサーバ108によるアクセスが可能な共通公開鍵を使用して暗号化されることを理解されよう。暗号化されたメッセージ暗号化鍵および受信者情報暗号化鍵は、次に、(データパケット102の)暗号化されたメッセージ鍵フィールド402および暗号化された受信者情報鍵フィールド403内に、それぞれ記憶される。データパケット102は、次に、暗号化デバイス104によって完全な形にアセンブルされる。ステップ308で、(暗号化デバイス104の)伝送モジュール1048は、(アセンブルされた)データパケット102をサーバ108に伝送する。データパケットは、SMS、MMS、インスタントメッセージング(IM)、電子メール、添付、電子文書送達サービスを使用するなど、好適なデジタルメッセージング方式を介して伝送され得ることを理解されよう。

【００３２】

サーバ108は、次に、暗号化デバイス104と復号デバイス106との間での真のエンドツーエンド暗号化通信を許可する、暗号化デバイス104から受信したデータパケット102を処理

するための(図5に示されたような)方法500を実行する。特に、サーバ108は第1に、ステップ502で、(サーバ108の)受信側モジュール1082を介してデータパケット102を受信する。サーバ108は、暗号化されたメッセージフィールド406内の暗号化されたメッセージが、暗号化デバイス104からサーバ108への移行中に、いかなる地点でも改ざんされていないことを保証するために、受信したデータパケット102のデジタル署名フィールド407から取り出したデータを使用して、認証チェックを実行する。次に、ステップ504で、サーバ108の復号モジュール1084は、受信したデータパケット102の暗号化された受信者情報鍵フィールド403内に記憶されたような、暗号化された受信者情報暗号化鍵を、サーバ108の秘密鍵を使用して復号するように構成される。これにより、受信者情報暗号化鍵の「プレーンテキストでの」(すなわち、暗号化されていない形での)取り出しが可能になる。複数のサーバ108を備えるシナリオの場合、暗号化された受信者情報暗号化鍵は、代わりに、上記で既に説明したように、すべてのサーバ108によるアクセスが可能な共通秘密鍵を使用して復号されることを理解されよう。その後、サーバ108の復号モジュール1084は、ステップ504で取得された受信者情報暗号化鍵を使用する、データパケット102の暗号化された受信者情報フィールド405内に記憶されたような、暗号化された識別データの復号に進む。これにより、「プレーンテキストでの」識別データの取り出しが可能になる。サーバ108が、前述のステップ506で取得された識別データに基づいて、データパケット102が次にどこにルーティングされる必要があるかを決定すると、次にサーバ108の伝送モジュール1086は、データパケット102を、識別データ内に指定された宛先に伝送および転送する。もちろん、本考察との関連において、識別データは復号デバイス106に関連付けられているため、データパケットは復号デバイス106に転送されることになる。重要なことに、データパケット102は、サーバ108によって逐語的に復号デバイス106に転送されること、すなわちサーバ108は、暗号化デバイス104から受信するデータパケット102を(いかなる方法でも)変更、再暗号化、または再フォーマット化しないことを理解されよう。

【００３３】

図5の方法500の実行中、サーバ108は、データパケット102の暗号化されたメッセージフィールド406および暗号化されたメッセージ鍵フィールド402を復号できないことを理解されよう。これは、サーバ108が、暗号化されたメッセージ鍵フィールド402を復号するために必要な、復号デバイス106の秘密鍵のコピーを有するように構成されていないためである。「プレーンテキストでの」メッセージ暗号化鍵の取り出しによってのみ、暗号化されたメッセージフィールド406を復号し、「プレーンテキストでの」メッセージを取得することが可能となる。すなわち、サーバ108は、復号デバイス106に向けられたメッセージを復号およびアクセスすることはできず、これは有利なことに、送信者と所期の受信者との間でのセキュアなエンドツーエンド暗号化通信を許可する。

【００３４】

次に、図6は、サーバ108から受信したデータパケット102を処理するために復号デバイス106によって実行される方法600を示す。ステップ602で、(復号デバイス106の)受信側モジュール1062は、サーバ108によって転送されたデータパケット102を受信し、ステップ604で、(復号デバイス106の)復号モジュール1064は、「プレーンテキストでの」メッセージ暗号化鍵を取得するために、データパケット102の暗号化されたメッセージ鍵フィールド402を復号するように構成される。復号されたメッセージ暗号化鍵を正常に取り出すと、次いで(復号デバイス106の)復号モジュール1064は、ステップ606で、(ステップ604で取得された)メッセージ暗号化鍵を使用して、復号されたメッセージを取得するためにデータパケット102の暗号化されたメッセージフィールド406を復号するように配置構成される。その後、復号デバイス106は、暗号化デバイス104によって伝送されたメッセージにアクセスし、これを読み取ることができる。

【００３５】

以下で、本発明の他の実施形態について説明する。簡潔にするために、実施形態間で共通の同様の要素、機能、および動作の説明は反復しない代わりに、関連する実施形態の同様の部分には言及する。

【００３６】
第2の実施形態によれば、複数の復号デバイス106(すなわち、グループ通信用の複数の受信者)が存在するシナリオにおいて、(暗号化デバイス104の)暗号化モジュール1042は、対応する復号デバイス106に関連付けられた受信者情報暗号化鍵を使用して、各復号デバイス106の識別データを暗号化した後、暗号化された識別データのすべてを、伝送されることになる新しいデータパケット102の暗号化された受信者情報フィールド405内に記憶する。特に、暗号化された識別データのすべては、新しいデータパケット102の暗号化された受信者情報フィールド405内に記憶されるデータ文字列に連結される。その後、複数の復号デバイス106のすべての受信者情報暗号化鍵は、サーバ108の公開鍵を使用して(暗号化デバイス104の暗号化モジュール1042によって)暗号化されるように配置構成され、データパケット102の暗号化された受信者情報鍵フィールド403内にまとめて記憶される。さらに、(暗号化デバイス104の)暗号化モジュール1042は、各復号デバイス106の公開鍵を使用してメッセージ暗号化鍵を暗号化もし、これがその後、データパケット102の暗号化されたメッセージ鍵フィールド402内に記憶される。より具体的に言えば、メッセージ暗号化鍵は、関連付けられた暗号化されたメッセージ暗号化鍵を形成するために、各復号デバイス106の対応する公開鍵を使用して、独立および単独に暗号化される。理解されるように、このプロセスは、すべての復号デバイス106の公開鍵に対して実行され、結果として生成される暗号化されたメッセージ暗号化鍵は、その後、データ文字列に連結され、これがデータパケット102の暗号化されたメッセージ鍵フィールド402内に記憶される。この実施形態において、図3の方法300におけるステップ302～ステップ308は依然として暗号化デバイス104によって同様に実行され、データパケット102内に記憶されるデータのタイプおよび量のみが、第1の実施形態について変化することを理解されよう。

【００３７】
サーバ108が暗号化デバイス104によって伝送されたデータパケット102を受信すると、次いでサーバ108の復号モジュール1084は、サーバ108の秘密鍵を使用して、受信したデータパケット102の暗号化された受信者情報鍵フィールド403に記憶されたような、暗号化された受信者情報暗号化鍵を復号する。これによってサーバ108は、複数の復号デバイス106のすべての復号された受信者情報暗号化鍵を取り出すことが可能になり、その後これらはそれぞれ、複数の復号デバイス106のすべての復号された識別データを取得するために、データパケット102の暗号化された受信者情報フィールド405に記憶されたようなデータ文字列の対応するセグメントを復号するためにさらに使用される。その後サーバ108は、復号された識別データを用いて、データパケット102を所期の復号デバイス106の各々に再ルーティングすることができる。データパケット102が各々の復号デバイス106に送達されると、それぞれの復号デバイス106は、メッセージ暗号化鍵のコピーを取得するために、それぞれの復号デバイス106の関連付けられた秘密鍵を使用して、(受信されたデータパケット102の暗号化されたメッセージ鍵フィールド402内のデータ文字列に記憶された)対応する暗号化されたメッセージ暗号化鍵を復号する。メッセージ暗号化鍵を用いて、各復号デバイス106は、復号されたメッセージを取得するために、データパケット102の暗号化されたメッセージフィールド406を復号することができる。本実施形態において、図5の方法500におけるステップ502～ステップ508は、依然としてサーバ108によって同様に実行されることを理解されよう。サーバ108はメッセージを再暗号化する必要がなく、第1の実施形態で既に述べられ、簡潔にするために反復されない理由により、サーバ108はメッセージを再暗号化することもできないことを、またさらに理解されよう。

【００３８】
第1の実施形態のわずかな変形である第3の実施形態によれば、復号デバイス106の公開鍵の代わりにサーバ108の公開鍵をここで使用して、(暗号化デバイス104のユーザによって選択されるような)図3の方法300内のステップ306で、メッセージ暗号化鍵が暗号化される。これは、サーバ108がその後、サーバ108の秘密鍵を使用して、暗号化されたメッセージ暗号化鍵を復号できるため、その後サーバ108は暗号化されたメッセージにアクセスできることを意味する。実際に、メッセージ暗号化鍵の取り出しにより、サーバ108は暗号

化されたメッセージを復号して、これにアクセスすることができる。すなわちこれは、(セキュリティ検証の目的で)暗号化されたメッセージのコンテンツへのアクセスをサーバ108に認めることも、暗号化デバイス104のユーザが希望し得ることを意味する。上記の変形以外に、第1の実施形態の詳細な説明の残りの部分が、その他の変更なしに第3の実施形態に適用されることを理解されよう。

【００３９】

要約すると、提案されたシステム100(および対応する方法)は、送信者が、再ルーティングを実行するために、少なくとも1つの(中間)サーバを介して暗号化されたメッセージを転送することにより、暗号化されたメッセージを1人または複数の受信者に送信できるようにするが、サーバには暗号化されたメッセージを復号する能力を有することを許可しない、複数鍵暗号化方式の具体化および実装が可能である。これは有利なことに、暗号化されたメッセージの復号を実際にサーバに許可することなく、送信者と受信者との間での真のエンドツーエンド暗号化が保持および達成されることを保証する。

【００４０】

また、提案されたシステム100は、暗号化されたメッセージへのサーバのアクセスを可能にすることを送信者が希望するかどうかに関して、送信者が決定できるように構成される。送信者が、当該暗号化されたメッセージへのサーバのアクセスを希望する場合、送信者は、メッセージ暗号化鍵を暗号化するためにサーバの公開鍵が代わりに使用され得るオプション(すなわち第3の実施形態)を、選択することができる。しかしながら、代わりに送信者が、暗号化されたメッセージをサーバが復号できない真のエンドツーエンド暗号化を希望する場合、第1および第2の実施形態が適用される。

【００４１】

繰り返し述べると、提案されたシステム100および方法は、(少なくとも1つの)サーバを介して送信者と複数の受信者との間での真のエンドツーエンド暗号化通信を可能にし、サーバは、複数の暗号化フィールドを有するカスタマイズされたセキュアなパケットフォーマットを用いて配置構成されたデータパケットをルーティング(および保管)するように構成される。暗号化フィールドのうちの1つが、送信者による受信者向けの暗号化されたメッセージを記憶し、サーバは、暗号化された(受信者の公開鍵を使用して暗号化された)メッセージを復号およびアクセスすることができない。具体的に言えば、セキュアなパケットフォーマットは、保管、再ルーティング、または実際に意図される受信者のいずれかの目的で、異なるパーティによって求められる情報を定義する。受信者の識別データは、受信者の識別情報への未許可のアクセスを防止するために暗号化される。特に、データパケットは、カスタマイズされた暗号化ソフトウェアアプリケーションを使用する提案された複数鍵暗号化方式を使用して暗号化され、デジタルメッセージングプラットフォームを介して受信者に送信され、同じタイプのデジタルメッセージングプラットフォーム上で受信者によって受信される。メッセージにアクセスするために、その後受信者は、メッセージを見るために(受信者独自の秘密鍵を使用して)暗号化されたメッセージを復号する。サーバは、データパケットを受信者に転送するプロセスにおいて同じデータパケットを受信し、データパケットを再ルーティングするかまたはデータパケットを保管するかを決定するために、データパケットの特定の暗号化フィールド、すなわちデータパケットの暗号化された受信者情報フィールド405を復号できることを理解されよう。しかしながらサーバは、データパケット内に記憶された暗号化されたメッセージを復号するための暗号化鍵(すなわち受信者の秘密鍵)を用いて構成されていない。これにより、(中間転送)サーバが送信者と受信者との間でメッセージをルーティングするための重要な役割を実行する、デジタルメッセージングシステムにおいて、サーバは、暗号化されたメッセージを復号すること、および関連付けられたコンテンツにアクセスすることができないことが保証される。したがって、提案されたシステムは、送信者および受信者のための真のエンドツーエンド暗号化システムおよび方式を可能にするが、依然としてサーバは、送信者によって受信者に伝送される暗号化されたメッセージのコンテンツのセキュリティおよび信頼性を損なうことなく、通信の転送/ルーティングに関与することができる。

【００４２】
提案された方法を広義に要約するためにも、第1のコンピューティングデバイスから第2のコンピューティングデバイスに伝送されることになるデータパケットを処理するために、少なくとも1つのサーバによって実行される方法が開示され、データパケットは、暗号化されたメッセージを形成するために第1の暗号化鍵を使用して暗号化されるメッセージと、暗号化された識別データを形成するために第2の暗号化鍵を使用して暗号化される第2のコンピューティングデバイスの識別データと、第2のコンピューティングデバイスに関連付けられた第3の暗号化鍵を使用して第1の暗号化鍵を暗号化することによって形成される暗号化された第1の暗号化鍵と、サーバに関連付けられた暗号化鍵を使用して第2の暗号化鍵を暗号化することによって形成される暗号化された第2の暗号化鍵とを含む。方法は、暗号化された第2の暗号化鍵を復号すること、復号された第2の暗号化鍵を使用して暗号化された識別データを復号すること、および、復号された識別データに基づいてデータパケットを伝送することを含む。具体的に言えば、暗号化された第1の暗号化鍵は、第2のコンピューティングデバイスに関連付けられた第4の暗号化鍵を使用してのみ復号可能なように配置構成され、第2のコンピューティングデバイスの第3および第4の暗号化鍵は、非対称鍵のペアとして構成される。すなわち、非対称鍵のペアは、確立された公開鍵暗号化方式の概念に従って、公開鍵(すなわち第3の暗号化鍵)および秘密鍵(すなわち第4の暗号化鍵)を含む。

【００４３】
しかしながら、説明した実施形態は限定的なものとして解釈されるべきではない。たとえば、暗号化および復号のデバイス104、106は、モバイルコンピューティングデバイス以外の任意の他のタイプの好適なデバイスとできることが理解されよう。また、暗号化デバイス104および復号デバイス106のそれぞれのモジュール(ソフトウェア内に実装されている場合)は、プログラムで統合され、それぞれ、データパケット102を処理するように想定され得る同様のコンピューティングデバイスにインストールされ得、これによって実行可能な、単一の完全なソフトウェアアプリケーションとして提供され得る。オプションとして、単一の完全なソフトウェアアプリケーションは、ハードウェア内に全体として実装され得、こうした実装されたハードウェアのコピーが、暗号化デバイス104および復号デバイス106の各々に組み込まれる。直前の2文で説明した代替の構成は、サーバ108の当該モジュールにも準用可能である。さらに代替として、暗号化および復号のプログラムコードは外部記憶デバイス上に記憶することが可能であり、必要な場合に、それぞれ暗号化デバイスおよび復号デバイス104、106上で実行するために「オンデマンド」でダウンロードすることが可能である。さらに、ソフトウェアインターフェースにおいて、暗号化デバイス104の表示モジュール1046によって表示されるように、ユーザが復号デバイス106の代わりにサーバ108を受信者として選択できるようにするオプションも、表示することができる。複数のサーバ108のシナリオの場合、サーバ108は、データパケット102が転送されることになる場所を決定するロードバランシング規則のセットと共に、集合的に構成され得ることも理解されよう。さらに、図4に示されるようなパケットフォーマット400は、必要に応じて、所期のアプリケーションの要件に基づき、新しいデータフィールドを含むかまたは既存のデータフィールドを除去するように修正することができる。

【００４４】
本発明を図面および上記の説明で詳細に例示および説明してきたが、こうした例示および説明は例示的または典型例であって、制限的ではないものとみなされ、本発明は開示された実施形態に限定されない。当業者であれば、請求された本発明を実施する際に、開示された実施形態に対する他の変形が理解および実行可能であろう。

【符号の説明】

【００４５】
100　システム
102　データパケット
104　第1のコンピューティングデバイス、暗号化デバイス

106　第2のコンピューティングデバイス、復号デバイス
108　サーバ
1042　暗号化モジュール
1046　表示モジュール
1048　伝送モジュール
10410　プロセッサモジュール
1062　受信側モジュール
1064　復号モジュール
1082　受信側モジュール
1084　復号モジュール
1086　伝送モジュール
204　暗号化デバイス
206　復号デバイス
400　パケットフォーマット
401　バージョン数フィールド
402　暗号化されたメッセージ鍵フィールド
403　暗号化された受信者情報鍵フィールド
404　初期化ベクトルフィールド
405　暗号化された受信者情報フィールド
406　暗号化されたメッセージフィールド
407　デジタル署名フィールド

【図１】

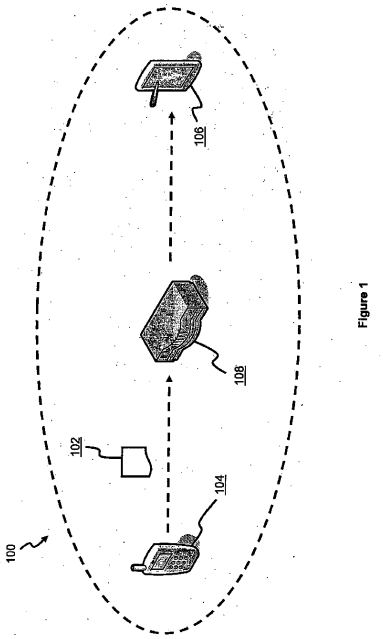
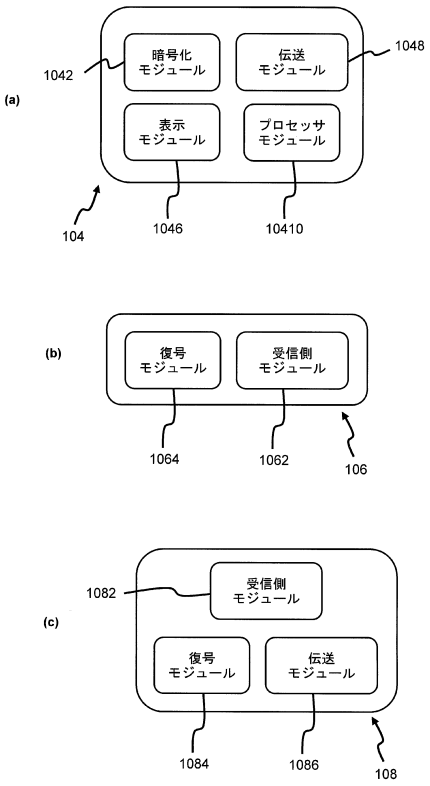
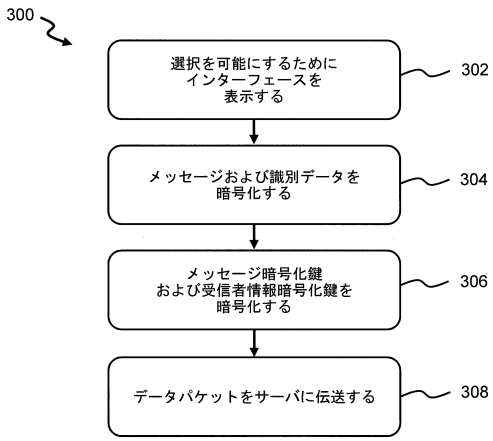


Figure 1

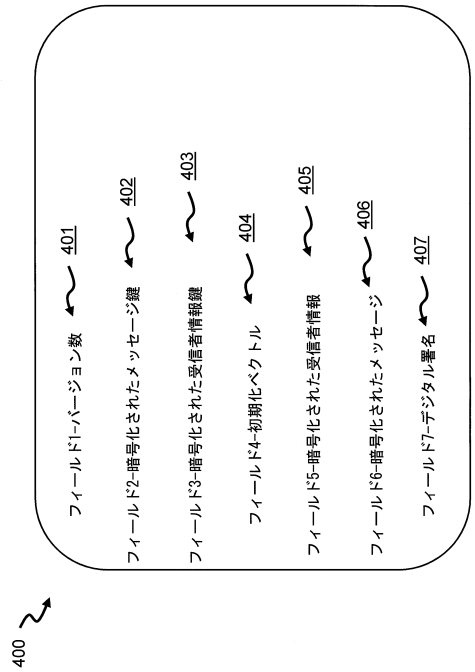
【図２】



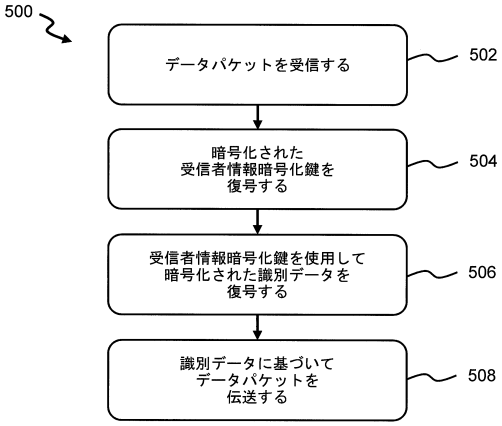
【図３】


300
選択を可能にするために
インターフェースを
表示する
302
メッセージおよび識別データを
暗号化する
304
メッセージ暗号化鍵
および受信者情報暗号化鍵を
暗号化する
306
データパケットをサーバに伝送する
308

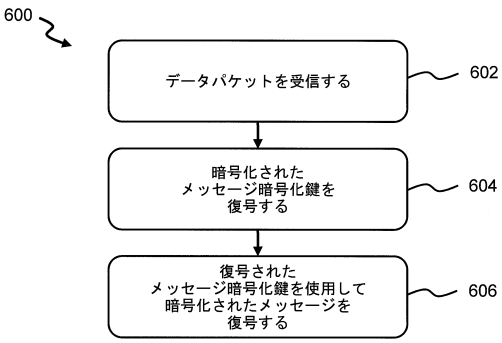
【図４】


フィールド1-バージョン数
401
フィールド2-暗号化されたメッセージ鍵
402
フィールド3-暗号化された受信者情報鍵
403
フィールド4-初期化ベクトル
404
フィールド5-暗号化された受信者情報
405
フィールド6-暗号化されたメッセージ
406
フィールド7-デジタル署名
407
400

【図５】


500
データパケットを受信する
502
暗号化された
受信者情報暗号化鍵を
復号する
504
受信者情報暗号化鍵を使用して
暗号化された識別データを
復号する
506
識別データに基づいて
データパケットを
伝送する
508

【図６】


600
データパケットを受信する
602
暗号化された
メッセージ暗号化鍵を
復号する
604
復号された
メッセージ暗号化鍵を使用して
暗号化されたメッセージを
復号する
606

フロントページの続き

(72)発明者　ツェ・チン・テオ
シンガポール・シンガポール・１３００１８・ドーヴァー・クレセント・１８・＃０３－３８
(72)発明者　チー・ワー・チョン
シンガポール・シンガポール・２７０００７・ギム・モー・ロード・７・＃２２－２６９
(72)発明者　ンガイ・カイン・イプ
シンガポール・シンガポール・６４２６５８・ジュロン・ウエスト・ストリート・６５・６５８ビー・＃０３－６０８
(72)発明者　ホン・タト・ラウ
シンガポール・シンガポール・３２９６１０・ブーン・テック・ロッジ・ブーン・テック・ロード・４６・＃０５－０１
(72)発明者　リ・ファン・ング
シンガポール・シンガポール・７３０６１８・ウッドランズ・アヴェニュー・４・６１８・＃０３－５３３
(72)発明者　シュー・イェン・ウェンディー・チャン
シンガポール・シンガポール・７３０８５８・ウッドランズ・ストリート・８３・８５８・＃０４－２１８

審査官　青木　重徳

(56)参考文献　特開平１１－１１２４９１（ＪＰ，Ａ）
特開２００８－０２８８４９（ＪＰ，Ａ）
特開平１０－１２６４０６（ＪＰ，Ａ）
David L. Chaum, et al., Untraceable Electronic Mail Return Addresses, and Digital Pseudonyms, Communications of the ACM, 米国, ACM, １９８１年　2月, Volume 24 Issue 2, pp. 84-88

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ　　９／１４
Ｈ０４Ｌ　　９／０８

(54)【発明の名称】エンドツーエンド暗号化通信を許可するために第１のコンピューティングデバイスから第２のコンピューティングデバイスへのデータパケットを処理するための少なくとも１つのサーバによって実行される方法