(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第4459703号
(P4459703)
(45)発行日　平成22年4月28日(2010.4.28)　(24)登録日　平成22年2月19日(2010.2.19)

(51)Int.Cl.　　F I
G06F 3/02 (2006.01)　　G06F 3/02 390A
G09C 1/00 (2006.01)　　G09C 1/00 610B

請求項の数 20　外国語出願　(全 18 頁)

(21)出願番号　特願2004-132078 (P2004-132078)
(22)出願日　平成16年4月27日 (2004.4.27)
(65)公開番号　特開2004-355615 (P2004-355615A)
(43)公開日　平成16年12月16日 (2004.12.16)
審査請求日　平成19年4月3日 (2007.4.3)
(31)優先権主張番号　10/428,675
(32)優先日　平成15年5月2日 (2003.5.2)
(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　マーカス　ペイナード
アメリカ合衆国　９８００８　ワシントン州　ベルビュー　ノースイースト　１６８　アベニュー　７

最終頁に続く

(54)【発明の名称】キーボードまたは関連デバイスとの機密保護機能のある通信

(57)【特許請求の範囲】
【請求項１】
キーボードと通信する方法であって、
コンポーネントが、第１のナンスを前記キーボードから受信することと、
前記コンポーネントが、第２のナンスを前記キーボードに送信することと、
前記キーボードと前記コンポーネントの両方に知られているキーと定数値とを使用するトリプルＤＥＳおよび暗号ブロック連鎖を前記第１のナンスと前記第２のナンスとの組合せに適用することによって、第１の初期値、および該第１の初期値とは異なる第２の初期値を生成することと、
前記コンポーネントが前記キーボードから、前記コンポーネントと前記キーボードの両方に知られている前記キーと前記第１の初期値とを使用するトリプルＤＥＳおよび暗号ブロック連鎖を使用して前記キーボードによって暗号化された、複数のデータを受信することであって、前記複数のデータ内の各々のデータはそれぞれ、前記キーボードが受信した別個の各キー入力を含み、前記複数のデータ内の各々のデータはそれぞれ、前記トリプルＤＥＳおよび暗号ブロック連鎖の別個のブロックを使用して暗号化される、該受信することと、
前記コンポーネントが、前記キーと前記第１の初期値とに基づいて、前記複数のデータを暗号化解除することと
を備えることを特徴とする方法。
【請求項２】

前記コンポーネントが前記キーボードから、前記コンポーネントと前記キーボードの両方に知られている前記キーと前記第２の初期値とを使用するトリプルＤＥＳおよび暗号ブロック連鎖を使用して前記キーボードによって生成され、前記複数のデータに対応している、複数のメッセージ認証コードを受信することと、
前記コンポーネントが、前記複数のメッセージ認証コードを使用することによって前記複数のデータを検証することと
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３】
前記定数値は、第１の定数値と、第２の定数値とを含み、
前記第１の初期値、および該第１の初期値とは異なる第２の初期値を生成することは、
前記キーボードと前記コンポーネントの両方に知られている前記キーと前記第１の定数値とを使用するトリプルＤＥＳおよび暗号ブロック連鎖を前記第１のナンスと前記第２のナンスとの組合せに適用することによって、前記第１の初期値を生成することと、
前記キーボードおよび前記コンポーネントの両方に知られている前記キーと前記第２の定数値とを使用するトリプルＤＥＳおよび暗号ブロック連鎖を前記第１のナンスと前記第２のナンスとの組合せに適用することによって、前記第２の初期値を生成することと
を含むことを特徴とする請求項１に記載の方法。
【請求項４】
前記複数のデータは、その動作の完全性が前記コンポーネントによって信頼されていないチャネルを介して前記キーボードから前記コンポーネントに送信されることを特徴とする請求項１に記載の方法。
【請求項５】
前記コンポーネントは、コンピューティング・デバイス上でともに実行される、第１のオペレーティング・システムと、前記第１のオペレーティング・システムの動作を完全には信頼していない第２のオペレーティング・システムとを含み、前記キーボードは、前記第１のオペレーティング・システムによって制御されるドライバを介して前記第２のオペレーティング・システムと通信することを特徴とする請求項４に記載の方法。
【請求項６】
前記キーボードは、ＵＳＢキーボード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】
前記トリプルＤＥＳおよび前記暗号ブロック連鎖は、所定のサイズを有するブロック単位でデータを暗号化し、前記キーボードは、前記所定のサイズのブロック単位でデータを通信することを特徴とする請求項６に記載の方法。
【請求項８】
コンポーネントにおいてキーボードからの入力をセキュアに受信する方法を実行するためのコンピュータ実行可能命令を記憶したコンピュータ可読な記憶媒体であって、前記方法は、
コンポーネントが、第１のナンスを前記キーボードから受信することと、
前記コンポーネントが、第２のナンスを前記キーボードに送信することと、
前記キーボードと前記コンポーネントの両方に知られているキーと定数値とを使用するトリプルＤＥＳおよび暗号ブロック連鎖を前記第１のナンスと前記第２のナンスとの組み合わせに適用することによって、第１の初期値、および該第１の初期値とは異なる第２の初期値を生成することと、
前記コンポーネントが前記キーボードから、前記コンポーネントと前記キーボードの両方に知られている前記キーと前記第１の初期値とを使用するトリプルＤＥＳおよび暗号ブロック連鎖を使用して、前記キーボードが受信した複数のキー入力を暗号化することによって生成された、複数の暗号化されたキー入力を受信することであって、前記複数のキー入力の個々のキー入力はそれぞれ、前記トリプルＤＥＳおよび暗号ブロック連鎖の別個のブロックを使用して暗号化される、該受信することと、
前記コンポーネントが、前記キーと前記第１の初期値とを使用して前記複数の暗号化さ

れたキー入力を暗号化解除することと
を備えることを特徴とするコンピュータ可読な記憶媒体。
【請求項９】
前記コンポーネントは、コンピューティング・デバイス上でともに実行される、第１のオペレーティング・システムと、前記第１のオペレーティング・システムの動作を完全には信頼していない第２のオペレーティング・システムとを含み、前記キーボードは、前記第１のオペレーティング・システムによって制御されるドライバを介して前記第２のオペレーティング・システムと通信することを特徴とする請求項８に記載のコンピュータ可読な記憶媒体。
【請求項１０】
前記方法は、
前記コンポーネントが前記キーボードから、前記コンポーネントと前記キーボードの両方に知られている前記キーと前記第２の初期値とを使用するトリプルＤＥＳおよび暗号ブロック連鎖を使用して前記キーボードによって生成され、前記複数の暗号化されたキー入力に対応している、複数のメッセージ認証コードを受信することと、
前記コンポーネントが、前記複数のメッセージ認証コードを使用することによって前記複数の暗号化されたキー入力を検証することと
をさらに備えることを特徴とする請求項８に記載のコンピュータ可読な記憶媒体。
【請求項１１】
前記定数値は、第１の定数値および第２の定数値を含み、
前記第１の初期値、および該第１の初期値とは異なる第２の初期値を生成することは、
前記キーボードと前記コンポーネントの両方に知られている前記キーと前記第１の定数値とを使用するトリプルＤＥＳおよび暗号ブロック連鎖を前記第１のナンスと前記第２のナンスとの組合せに適用することによって、前記第１の初期値を生成することと、
前記キーボードと前記コンポーネントの両方に知られている前記キーと前記第２の定数値とを使用するトリプルＤＥＳおよび暗号ブロック連鎖を前記第１のナンスと前記第２のナンスとの組合せに適用することによって、前記第２の初期値を生成することと
を含むことを特徴とする請求項８に記載のコンピュータ可読な記憶媒体。
【請求項１２】
前記トリプルＤＥＳおよび前記暗号ブロック連鎖は、所定のサイズを有するブロック単位でデータを暗号化し、前記キーボードは、前記所定のサイズのブロック単位でデータを通信することを特徴とする請求項８に記載のコンピュータ可読な記憶媒体。
【請求項１３】
入力データをデータの受信側へセキュアに送信するためのキーボードであって、
キーと定数値とを格納する１つまたは複数の記憶場所と、
第１のナンスを受信側に送信し、第２のナンスを前記受信側から受信し、該キーボードと前記受信側との両方に知られている前記キーと前記定数値とを使用するトリプルＤＥＳおよび暗号ブロック連鎖を前記第１のナンスと前記第２のナンスとの組み合わせに適用することによって第１の初期値、および該第１の初期値とは異なる第２の初期値を生成し、該キーボードが受信した入力データを、該キーボードと前記受信側の両方に知られている前記キーと前記第１の初期値とを使用するトリプルＤＥＳおよび暗号ブロック連鎖を使用して暗号化することによって前記入力データに基づいた暗号化されたデータを生成する、暗号化コンポーネントであって、前記入力データ内の各入力データはそれぞれ、該キーボードが受信した別個のキー入力を表し、前記入力データ内の各入力データはそれぞれ、前記トリプルＤＥＳおよび暗号ブロック連鎖の別個のブロックを使用して暗号化される、該暗号化コンポーネントと、
前記受信側から前記第１のナンスを通信し、前記受信側へ前記第２のナンスを通信し、および前記キーと前記第１の初期値とを知っている前記受信側を宛先とする前記暗号化されたデータを前記キーボードの外部のデバイスに通信する、通信インターフェースと
を備えたことを特徴とするキーボード。

【請求項１４】
前記暗号化コンポーネントは、さらに、前記暗号化されたデータまたは前記入力データに対応する複数のメッセージ認証コードを、該キーボードと前記受信側の両方に知られている前記キーと前記第２の初期値とを使用するトリプルＤＥＳおよび暗号ブロック連鎖を使用して生成することを特徴とする請求項１３に記載のキーボード。
【請求項１５】
前記キーボードは、ＵＳＢキーボードを含むことを特徴とする請求項１３に記載のキーボード。
【請求項１６】
前記通信インターフェースが、前記暗号化されたデータを、前記デバイス上で実行される第１のオペレーティング・システムによって制御されるドライバに通信すると、前記暗号化されたデータは、前記デバイス上で前記第１のオペレーティング・システムとともに実行され、前記第１のオペレーティング・システムの動作を完全には信頼していない、第２のオペレーティング・システムである前記受信側に通信されることを特徴とする請求項１３に記載のキーボード。
【請求項１７】
キーボードが該キーボードの外部のコンポーネントとのセキュリティで保護された通信を行うことができるようにする方法を実行するためのコンピュータ実行可能命令を記憶したコンピュータ可読な記憶媒体であって、前記方法は、前記キーボードが、
第１のナンスを前記コンポーネントに送信することと、
第２のナンスを前記コンポーネントから受信することと、
該キーボードと前記コンポーネントの両方に知られているキーと定数値とを使用するトリプルＤＥＳおよび暗号ブロック連鎖を前記第１のナンスと前記第２のナンスとの組み合わせに適用することによって、第１の初期値、および該第１の初期値とは異なる第２の初期値を生成することと、
複数の入力されたキー入力を受信することと、
前記複数の入力されたキー入力のそれぞれを、該キーボードと前記コンポーネントの両方に知られている前記キーと前記第１の初期値とを使用するトリプルＤＥＳおよび暗号ブロック連鎖を使用して暗号化することであって、前記複数の入力されたキー入力の各キー入力がそれぞれ、前記トリプルＤＥＳおよび暗号ブロック連鎖の別個のブロックを使用して暗号化される、該暗号化することと、
前記複数の暗号化されたキー入力を前記コンポーネントに伝送することと
を備えることを特徴とするコンピュータ可読な記憶媒体。
【請求項１８】
前記トリプルＤＥＳおよび暗号ブロック連鎖は、所定のサイズを有するブロック単位でデータを暗号化し、前記キーボードは、前記所定のサイズのブロック単位でデータを通信することを特徴とする請求項１７に記載のコンピュータ可読な記憶媒体。
【請求項１９】
前記方法は、前記キーボードが、
該キーボードと前記コンポーネントの両方に知られている前記キーと前記第２の初期値とを使用するトリプルＤＥＳおよび暗号ブロック連鎖を使用して、前記複数の暗号化されたキー入力に対応する複数のメッセージ認証コードを生成することと、
前記複数のメッセージ認証コードを前記コンポーネントに伝送することと
をさらに備えることを特徴とする請求項１７に記載のコンピュータ可読な記憶媒体。
【請求項２０】
キーボードと通信する方法であって、
コンポーネントが、第１のナンスを前記キーボードから受信することと、
前記コンポーネントが、第２のナンスを前記キーボードに送信することと、
前記キーボードと前記コンポーネントの両方に知られているキーと定数値とを使用するトリプルＤＥＳおよび暗号ブロック連鎖を前記第１のナンスと前記第２のナンスとの組み

合わせに適用することによって、第１の初期値、および該第１の初期値とは異なる第２の初期値を生成することと、
前記コンポーネントが前記キーボードから、前記コンポーネントと前記キーボードの両方に知られている前記キーと前記第１の初期値とを使用するトリプルＤＥＳおよび暗号ブロック連鎖を使用して前記キーボードによって暗号化された、複数のデータを受信することであって、前記複数のデータ内の各データはそれぞれ、前記キーボードから受信した別個の各キー入力を含み、前記複数のデータ内の各データはそれぞれ、前記トリプルＤＥＳおよび暗号ブロック連鎖の別個のブロックを使用して暗号化される、該受信することと、
前記コンポーネントが、前記コンポーネントと前記キーボードの両方に知られている前記キーと前記第２の初期値とを使用するトリプルＤＥＳおよび暗号ブロック連鎖を使用して前記キーボードによって生成され、前記複数のデータに対応している、複数のメッセージ認証コードを受信することと、
前記コンポーネントが、前記キーと前記第１の初期値とに基づいて、前記複数のデータを暗号化解除することと
前記コンポーネントが、前記複数のメッセージ認証コードを使用することによって前記複数のデータを検証することと
を備えたことを特徴とする方法。

【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・セキュリティの分野に関する。より詳細には、本発明は、傍受または他のタイプの不正操作（tampering）を受ける可能性がある通信チャネルを介するキーボードのセキュリティで保護された使用に関する。
【背景技術】
【０００２】
キーボードは、ユーザが入力したデータをコンピュータなどの電子デバイスに通信する。ユーザがキーボード上のキーを押した際、キーボードは、押された特定のキーを表すデータ（例えば、文字「ｅ」のＡＳＣＩＩコード）を生成し、このデータが、デバイス・ドライバなどのコンピュータ内部のコンポーネントによって受け取られる。次に、デバイス・ドライバが、そのデータを、どのようなプログラムであれ、現在、入力を受け取っているコンピュータ上で実行されているプログラムに送る（たとえば、そのデータを、いずれのアプリケーション・プログラムであれ、アクティブであるアプリケーション・プログラムの入力バッファに入れることにより）。
【０００３】
データの受け取りにキーボードを使用するときに生じる１つの問題は、データが機密扱いの場合、または、秘密にしておかれる必要がある場合である。たとえば、セキュリティで保護されたアプリケーション（またはオペレーティング・システムのセキュリティで保護されたサービス）が、一般に、公衆に漏らされてはならないパスワードを入力するようにユーザに求めることがある。しかし、キーボードからデータを受け取るソフトウェア・コンポーネントに至るパスは、このデータを傍受するいくつかの機会が存在すると理由で、セキュリティで保護されていない。たとえば、このデータは、しばしば、スヌーピング（snooping）を受けるバスを介して伝送され、不正操作を受ける可能性があるデバイス・ドライバによって扱われる（または、そのオペレーティング・システムが、そのドライバが扱う情報を格納したり、漏洩させたりする、セキュリティで保護されていないデバイス・ドライバに、置き換えられること許すことがある）。言い換えれば、キーボードから最終の宛先に向かう途中の秘密データを観察する、または不正操作するいくつかの機会が存在する。
【発明の開示】
【発明が解決しようとする課題】
【０００４】

一般に、セキュリティで保護されていないチャネルで接続された２つのコンポーネントの間で伝送するためにデータを暗号化することが可能である。しかし、色々な要因に起因して、たとえば、キー管理問題、リプレー攻撃の可能性、ならびに、暗号化テキストの程々のサイズのサンプルを傍受することができる場合、キーボードによって生成される可能性があるデータの範囲が比較的小さいことにより、キーボード通信上の通常の暗号を破ることが比較的容易になっていること、などの要因に起因して、キーボードのコンテキストにおいて、多くの暗号化技術を容易に適用することができない。

【０００５】

以上に鑑みて、キーボードとのセキュリティで保護された通信を円滑にする技術の必要性が存在する。

【課題を解決するための手段】

【０００６】

本発明は、セキュリティで保護されていない通信チャネルを介する２つのコンポーネント間におけるセキュリティで保護された通信のための技術を提供する。本技術は、キーボードに特によく適しており、標準の暗号化スキームをキーボードに適用する際に存在する問題に対処する暗号化スキームを使用する。

【０００７】

本発明によるキーボードは、キーと、暗号化スキームの初期化のために使用される定数値と、を格納する。コンポーネント（たとえば、コンピュータ上で実行されているアプリケーション）が、キーボードにおいて格納されているのと同じキーおよび同じ定数値を格納する。コンポーネントとキーボードの間でセキュリティで保護されたセッションを開始するため、それぞれが、ナンス（nonce）を生成し、次に、互いとナンスを交換して、キーボードおよびコンポーネントがそれぞれ両方のナンスを所有しているようにする。次に、キーボードおよびコンポーネントは、２つのナンス、キー、および定数値にそれぞれが基づく２つの初期値を計算する。たとえば、第１の初期値は、ＣＢＣ－３ＤＥＳＭＡＣアルゴリズムを使用して生成されることが可能であり、ＣＢＣ－３ＤＥＳＭＡＣは、格納された定数値を初期連鎖値として使用し、前述のキーを、２つのナンスに基づいて生成されたメッセージに適用する。（ＣＢＣ－３ＤＥＳＭＡＣとは、暗号ブロック連鎖を伴うデータ暗号化標準（Data Encryption Standard）（ＤＥＳ）アルゴリズムによるトリプル暗号化を適用し、最終の暗号化テキスト・ブロックを使用してメッセージ認証コード（Message Authentication Code）（ＭＡＣ）を生成することを指す。好ましくは、第２の初期値は、第１の初期値のビットを反転させる（すなわち、第１の初期値と、数０ｘｆｆｆｆｆｆｆｆｆｆｆｆｆｆｆｆの間で「排他ＯＲ」演算を実行する）ことによって生成される。キーボードとコンポーネントは、第１の初期値および第２の初期値を同じやり方で計算するので、共に、同じ２つの初期値を所有する。

【０００８】

代替の好ましい実施形態では、キーボードおよびコンポーネントは、２つの定数値を備え、第１の初期値および第２の初期値は、第１の初期値を生成するために第１の定数を使用し、第２の初期値を生成するために第２の定数を使用するＣＢＣ－３ＤＥＳＭＡＣを、両方のナンスに基づくメッセージに対して適用することによって、生成されることが可能である。

【０００９】

第１の初期値および第２の初期値が生成されると、キーボードは、暗号化されたデータを通信する準備ができ、データを受け取るコンポーネントは、そのデータを暗号化解除し、検証する準備ができる。データがキーボードに入力されると、キーボードは、第１の初期値およびキーに基づいてそのデータを暗号化する。好ましくは、キーボードは、暗号ブロック連鎖を準備する（prime）のに使用される第１の初期値と共に、ＣＢＣ－３ＤＥＳ（暗号ブロック連鎖を伴うトリプルＤＥＳ）を使用して、前述したキーでデータを暗号化する。キーボードは、好ましくは、ＣＢＣ－３ＤＥＳＭＡＣを使用して各データ単位に関するＭＡＣも生成する。ここで、ＣＢＣ－３ＤＥＳＭＡＣは、前述したキーを適用し、第

２の初期値を使用して暗号ブロック連鎖を準備する。好ましくは、各キー入力が、別個の暗号ブロックの中に暗号化され、セッション中にキーボードにおいて生成されたデータストリーム全体が、暗号ブロックの連鎖を構成する。というのは、この技術は、同じキー入力（例えば、文字「ｅ」）が、先行するキー入力に依存して異なる暗号化テキストとして出現することを可能にするからである。

【００１０】

暗号化されたデータおよびＭＡＣが受信側コンポーネントにおいて受け取られると、受信側コンポーネントは、前述したキー、ならびに第１の初期値および第２の初期値を使用して受け取られたデータを暗号化解除し、検証する。

【００１１】

本発明のその他の特徴を以下に説明する。

【００１２】

以上の概要、および好ましい実施形態の以下の詳細な説明は、添付の図面に関連して読むことでよりよく理解される。本発明を例示するため、図面では、本発明の例示的な構成を示しているが、本発明は、本明細書に開示する特定の方法および手段（instrumentalities）に限定されない。

【発明を実施するための最良の形態】

【００１３】

例示的なコンピューティング構成

図１は、本発明の態様を実装することができる例示的なコンピューティング環境を示している。コンピューティング・システム環境１００は、適切なコンピューティング環境の一例に過ぎず、本発明の用途または機能の範囲に関する限定を何ら示唆するものではない。また、コンピューティング環境１００が、例示的な動作環境１００に示したコンポーネントのいずれか１つ、またはいずれの組合せに関連する依存関係または要件を有していると解釈してはならない。

【００１４】

本発明は、多数の他の汎用または専用のコンピューティング・システム環境またはコンピューティング・システム構成で機能する。本発明で使用するのに適する可能性がある周知のコンピューティング・システム、コンピューティング環境、および／またはコンピューティング構成の例には、パーソナル・コンピュータ、サーバ・コンピュータ、ハンドヘルド・デバイスまたはラップトップ・デバイス、マルチ・プロセッサ・システム、マイクロ・プロセッサベースのシステム、セットトップボックス、プログラマブル家庭用電化製品、ネットワークＰＣ、ミニ・コンピュータ、メインフレーム・コンピュータ、組み込みシステム、以上のシステムまたはデバイスのいずれかを含む分散コンピューティング環境などが含まれるが、以上には限定されない。

【００１５】

本発明は、コンピュータによって実行される、プログラム・モジュールなどのコンピュータ実行可能命令の一般的な文脈において説明することができる。一般に、プログラム・モジュールには、特定のタスクを実行する、または特定の抽象データ型を実装するルーチン、プログラム、オブジェクト、コンポーネント、データ構造などが含まれる。本発明は、通信ネットワークまたは他のデータ伝送媒体を介してリンクされたリモート処理デバイスによってタスクが実行される分散コンピューティング環境において実施してもよい。分散コンピューティング環境では、プログラム・モジュールおよび他のデータは、メモリ記憶装置を含むローカル・コンピュータ記憶媒体とリモート・コンピュータ記憶媒体の両方の中に配置されることが可能である。

【００１６】

図１を参照すると、本発明を実装するための例示的なシステムが、コンピュータ１１０の形態で汎用コンピューティング・デバイスを含んでいる。コンピュータ１１０のコンポーネントには、処理ユニット１２０、システム・メモリ１３０、ならびにシステム・メモリから処理ユニット１２０までを含む様々なシステム・コンポーネントを結合するシステ

ム・バス１２１が含まれることが可能であるが、以上には限定されない。システム・バス１２１は、様々なバス・アーキテクチャのいずれかを使用するメモリバスまたはメモリ・コントローラ、周辺バス、およびローカル・バスを含むいくつかのタイプのバス構造のいずれかであることが可能である。例として、限定としてではなく、そのようなアーキテクチャには、インダストリ・スタンダード・アーキテクチャ（Industry Standard Architecture）（ＩＳＡ）バス、マイクロ・チャネル・アーキテクチャ（Micro Channel Architecture）（ＭＣＡ）バス、エンハンストＩＳＡ（Enhanced ISA）（ＥＩＳＡ）バス、ビデオ・エレクトロニクス・スタンダーズ・アソシエーション（Video Electronics Standards Association）（ＶＥＳＡ）ローカル・バス、および（メザニン（Mezzanine）バスとしても知られる）ペリフェラル・コンポーネント・インターコネクト（Peripheral Component Interconnect）（ＰＣＩ）バスが含まれる。また、システム・バス１２１は、通信デバイスのなかでもとりわけ、ポイント・ツー・ポイント接続、交換ファブリックなどとして実装してもよい。

【００１７】

コンピュータ１１０は、通常、様々なコンピュータ可読媒体を含む。コンピュータ可読媒体は、コンピュータ１１０がアクセスすることができる任意の利用可能な媒体であることが可能であり、揮発性媒体と不揮発性媒体、リムーバブルな媒体とリムーバブルでない媒体が共に含まれる。例として、限定としてではなく、コンピュータ可読媒体は、コンピュータ記憶媒体および通信媒体を含むことが可能である。コンピュータ記憶媒体には、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、または他のデータなどの情報の格納のために任意の方法または技術で実装された揮発性媒体と不揮発性媒体、リムーバブルな媒体とリムーバブルでない媒体が共に含まれる。コンピュータ記憶媒体には、ＲＡＭ、ＲＯＭ、ＥＥＰＲＯＭ、フラッシュ・メモリまたは他のメモリ技術、ＣＤ－ＲＯＭ、デジタル・バーサタイル・ディスク（ＤＶＤ）または他の光ディスク・ストレージ、磁気カセット、磁気テープ、磁気ディスク・ストレージまたは他の磁気記憶装置、あるいは所望の情報を格納するのに使用することができ、コンピュータ１１０がアクセスすることができる任意の他の媒体が含まれるが、以上には限定されない。通信媒体は、通常、搬送波などの変調されたデータ信号、または他のトランスポート機構で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、または他のデータを実体化し、あらゆる情報配信媒体が含まれる。「変調されたデータ信号」という用語は、信号内に情報をエンコードするような仕方で特性の１つまたは複数が設定または変更されている信号を意味する。例として、限定としてではなく、通信媒体には、有線ネットワークまたは直接配線接続などの有線媒体、ならびに音響媒体、ＲＦ媒体、赤外線媒体、およびその他の無線媒体などの無線媒体が含まれる。また、前述した媒体のいずれかの組合せも、コンピュータ可読媒体の範囲に含められなければならない。

【００１８】

システム・メモリ１３０は、読み取り専用メモリ（ＲＯＭ）１３１およびランダム・アクセス・メモリ（ＲＡＭ）１３２などの揮発性メモリおよび／または不揮発性メモリの形態でコンピュータ記憶媒体を含む。始動中などにコンピュータ１１０内部の要素間で情報を転送するのを助ける基本ルーチンを含む基本入出力システム１３３（ＢＩＯＳ）が、通常、ＲＯＭ１３１の中に格納されている。ＲＡＭ１３２は、通常、処理ユニット１２０によって即時にアクセス可能であり、かつ／または現在、処理されているデータおよび／またはプログラム・モジュールを含む。例として、限定としてではなく、図１は、オペレーティング・システム１３４、アプリケーション・プログラム１３５、その他のプログラム・モジュール１３６、およびプログラム・データ１３７を示している。

【００１９】

また、コンピュータ１１０は、他のリムーバブルな／リムーバブルでない、揮発性／不揮発性のコンピュータ記憶媒体も含むことが可能である。単に例として、図１は、リムーバブルでない不揮発性の磁気媒体に対して読み取りまたは書き込みを行うハード・ディスク・ドライブ１４１、リムーバブルな不揮発性の磁気ディスク１５２に対して読み取りま

たは書き込みを行う磁気ディスク・ドライブ１５１、およびＣＤ－ＲＯＭまたは他の光媒体などのリムーバブルな不揮発性の光ディスク１５６に対して読み取りまたは書き込みを行う光ディスク・ドライブ１５５を示している。例示的な動作環境において使用することができる他のリムーバブルな／リムーバブルでない揮発性／不揮発性のコンピュータ記憶媒体には、磁気テープカセット、フラッシュ・メモリ・カード、デジタル・バーサタイル・ディスク、デジタル・ビデオ・テープ、ソリッド・ステートＲＡＭ、ソリッド・ステートＲＯＭなどが含まれるが、以上には限定されない。ハード・ディスク・ドライブ１４１は、通常、インターフェース１４０のようなリムーバブルでないメモリ・インターフェースを介してシステム・バス１２１に接続され、磁気ディスク・ドライブ１５１および光ディスク・ドライブ１５５は、通常、インターフェース１５０のようなリムーバブルなメモリ・インターフェースでシステム・バス１２１に接続される。

【００２０】

前述し、図１に示すドライブおよび関連するコンピュータ記憶媒体により、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、およびその他のデータのストーレッジがコンピュータ１１０に提供される。図１では、たとえば、ハード・ディスク・ドライブ１４１が、オペレーティング・システム１４４、アプリケーション・プログラム１４５、他のプログラム・モジュール１４６、およびプログラム・データ１４７を格納しているのを示している。以上のコンポーネントは、オペレーティング・システム１３４、アプリケーション・プログラム１３５、他のプログラム・モジュール１３６、およびプログラム・データ１３７と同じであることも、異なることも可能であることに留意されたい。オペレーティング・システム１４４、アプリケーション・プログラム１４５、他のプログラム・モジュール１４６、およびプログラム・データ１４７に、ここでは、少なくともそれらが異なるコピーであることを示すために異なる符号を付けている。ユーザは、キーボード１６２や、マウス、トラック・ボール、またはタッチ・パッドと一般に呼ばれるポインティング・デバイス１６１などの入力デバイスを介して、コマンドおよび情報をコンピュータ２０に入力することができる。その他の入力デバイス（図示せず）には、マイク、ジョイスティック、ゲーム・パッド、サテライト・ディッシュ、スキャナなどが含まれることが可能である。以上の入力デバイス、およびその他の入力デバイスは、しばしば、システム・バスに結合されたユーザ入力インターフェース１６０を介して処理ユニット１２０に接続されるが、パラレル・ポート、ゲーム・ポート、またはユニバーサル・シリアル・バス（ＵＳＢ）などの他のインターフェースおよびバス構造で接続してもよい。また、モニタ１９１、または他のタイプのディスプレイ・デバイスも、ビデオ・インターフェース１９０などのインターフェースを介してシステム・バス１２１に接続される。モニタに加えて、コンピュータは、出力周辺インターフェース１９０を介して接続することができるスピーカ１９７やプリンタ１９６などの他の周辺出力デバイスも含むことが可能である。

【００２１】

コンピュータ１１０は、リモート・コンピュータ１８０のような１つまたは複数のリモート・コンピュータに対する論理接続を使用するネットワーク化された環境において動作することが可能である。リモート・コンピュータ１８０は、パーソナル・コンピュータ、サーバ、ルータ、ネットワークＰＣ、ピア・デバイス、または他の一般的なネットワーク・ノードであることが可能であり、通常、コンピュータ１１０に関連して前述した要素の多く、またはすべてを含むが、メモリ記憶装置１８１だけを図１に示している。図１に示した論理接続は、ローカル・エリア・ネットワーク（ＬＡＮ）１７１およびワイド・エリア・ネットワーク（ＷＡＮ）１７３を含むが、その他のネットワークを含むことも可能である・。そのようなネットワーキング環境は、オフィス、企業全体のコンピュータ・ネットワーク、イントラネット、およびインターネットで一般的である。

【００２２】

ＬＡＮネットワーキング環境で使用される場合、コンピュータ１１０は、ネットワーク・インターフェースまたはネットワーク・アダプタ１７０を介してＬＡＮ１７１に接続される。ＷＡＮネットワーキング環境で使用される場合、コンピュータ１１０は、通常、イ

ンターネットなどのＷＡＮ１７３を介して通信を確立するためのモデム１７２、またはその他の手段を含む。内部にあることも、外部にあることも可能なモデム１７２は、ユーザ入力インターフェース１６０、またはその他の適切な機構を介してシステム・バス１２１に接続することができる。ネットワーク化された環境では、コンピュータ１１０に関連して示したプログラム・モジュール、またはプログラム・モジュールの部分は、リモートメモリ記憶装置の中に格納されることが可能である。例として、限定としてではなく、図１は、リモート・アプリケーション・プログラム１８５が、メモリ・デバイス１８１上に常駐しているのを示している。図示したネットワーク接続は、例示的であり、コンピュータ間で通信リンクを確立する他の手段も使用できることが認められよう。

【００２３】

キーボードとコンポーネントの間における通信のセキュリティ

本発明は、キーボードからの入力を要するコンポーネントとセキュリティで保護された形で通信するためにキーボードをどのように使用することができるかという問題を扱う。図２は、このような通信のシナリオを示している。図２では、キーボード１６２が、コンポーネント２０４と通信している。コンポーネント２０４は、任意のタイプのコンポーネント、たとえば、コンピュータ上で実行されているプログラム、あるいはハードウェアなどであることが可能である。キーボード１６２からコンポーネント２０２への通信は、少なくとも何らかのセキュリティで保護されていない部分２０４を含む通信チャネルを経由する。つまり、キー入力を表すデータがキーボード１６２からコンポーネント２０２に向かう途中で何らかのチャネルを経由する際、第三者がそのデータを傍受する、または不正操作する何らかの機会が存在する、可能性がある。たとえば、キーボード１６２で入力されている情報が、公衆に明かされてはならない秘密パスワードである場合、この傍受または不正操作は問題である可能性がある。

【００２４】

図３は、キーボードとコンポーネントの間でセキュリティで保護された通信が所望される特定のシナリオを示している。図３では、キーボード１６２を使用して、コンピュータ１１０上で実行されているソフトウェアに入力が与えられる。図３の例では、キーボード１６２は、ユニバーサル・シリアル・バス（ＵＳＢ）３０２で使用するように適合されたキーボードである。（略して、そのようなキーボードをＵＳＢキーボードと呼ぶ。）キーボード１６２は、キー入力を受け取り、そのキー入力を表すバイトをＵＳＢ３０２に乗せ、ＵＳＢ３０２においてバイトがＵＳＢドライバ３０４によってピックアップされる。次に、ドライバ３０４が、図３の例では、ソフトウェア３０６である最終的な宛先にそのバイトを伝達する。ソフトウェア３０６は、コンポーネント２０２（図２に示す）の例である。

【００２５】

図３では、コンピュータ１１０上で実行されている２つのオペレーティング・システム１３４（１）および１３４（２）が存在する。オペレーティング・システム１３４（１）は、ＭＩＣＲＯＳＯＦＴ　ＷＩＮＤＯＷＳ（登録商標）ＸＰ、Ｕｎｉｘ（登録商標）、Ｌｉｎｕｘ、Ｓｏｌａｒｉｓなどの通常のオペレーティング・システムである。オペレーティング・システム１３４（２）は、信頼されるアプリケーション用に使用されるハイ・アシュアランス（high　assurance：高信頼）オペレーティング・システムである。たとえば、オペレーティング・システム１３４（２）は、オペレーティング・システム１３４（２）の外部ではアクセス可能でないｃｕｒｔａｉｎｅｄメモリに関連付けられていることが可能であり、オペレーティング・システム１３４（２）は、オペレーティング・システム１３４（２）の下で実行されることが許されているある特別な信頼されるアプリケーションだけが秘密情報を読み取ることができるように、そのｃｕｒｔａｉｎｅｄメモリの中に秘密情報（例えば、暗号化キー、パスワードなど）を格納することができる。オペレーティング・システム１３４（２）は、オペレーティング・システム１３４（２）が自らの機能を正しく実行するという非常に高いレベルのアシュアランスを受ける権利が与えられるという意味で、ハイ・アシュアランスである。すなわち、秘密情報を保護することが、

オペレーティング・システム１３４（２）の意図される機能の１つである場合、オペレーティング・システム１３４（２）がその秘密情報を漏らさないという非常に高いレベルのアシュアランス信頼を受ける権利を与えられる。秘密情報を保護することができることの一部には、をその秘密を外部世界に漏らすことなく入力された秘密（例えば、パスワード）を受け取ることができることが含まれる。オペレーティング・システム１３４（２）は、ドライバ３０４がオペレーティング・システム１３４（１）の制御下にある（および、そのオペレーティング・システム１３４（１）が、ハッカーがＵＳＢ３０２から直接に情報を読み取ったり、または秘密情報を格納して外部に公表する不正なドライバに置き換えることを許容する可能性がある）ので、ドライバ３０４がそのような秘密情報を扱うのを信頼しない可能性がある。したがって、オペレーティング・システム１３４（２）は、オペレーティング・システム１３４（１）において引き起こされる動作（acts）によって秘密情報が漏らされる懸念なしに、オペレーティング・システム１３４（１）を介してキーボード１６２から情報を受け取る方法を必要とする。

【００２６】

図３の例は、キーボード１６２がユニバーサル・シリアル・バス３０２を介してコンピュータ１１０と通信しているのを示しているが、前述したシナリオは、キーボード１６２がコンピュータ１１０と通信する厳密な手段に関わりなく該当し、したがって、本発明は、ＵＳＢキーボードに限定されない。

【００２７】

図４は、セキュリティで保護されていないチャネルを介してセキュリティで保護された通信に参加するようにキーボード１６２およびコンポーネント２０２を構成することができるやり方を示している。キーボード１６２およびコンポーネント２０２はそれぞれ、暗号化キー４０２のコピーを格納する。キーボード１６２およびコンポーネント２０２は、好ましくは、以下により詳細に説明するように、特定の好ましい暗号化技術のための初期値として使用される定数値４０４も格納する。さらに好ましい実施形態では、キーボード１６２およびコンポーネント２０２は、（キーに加えて）１つではなく２つの定数値を格納してもよい。この２つの定数値は、以下に説明するように、暗号化技術において使用することができる。キーボード１６２は、たとえば、キー４０２および定数４０４を格納する基板に実装した（onboard）不揮発性半導体を含むこと、またはキー４０２および定数４０４が格納されたリムーバブル記憶媒体を受けるポートを有することが可能である。コンポーネント２０２がソフトウェア・コンポーネントである場合、キー４０２および定数４０４は、コンポーネント２０２のデータ空間の中に格納することができる。ただし、本発明は、キー４０２および定数４０４を格納するいずれの特定の仕方にも限定されないことを理解されたい。

【００２８】

キーボード１６２とコンポーネント２０２の間におけるセキュリティで保護された通信の初めに、キーボード１６２およびコンポーネント２０２は、ナンスを生成し、交換する。つまり、キーボード１６２が、ナンス４１２を生成し、ナンス４１２をコンポーネント２０２に送る。コンポーネント２０２が、ナンス４１４を生成し、ナンス４１４をキーボード１６２に送る。当技術分野で周知のとおり、ナンスは、暗号化アプリケーション（暗号化の申し込み）において使用されるデータであり、しばしば、あるエンティティを暗号法において（crytographically）認証するのに使用され、あるいは暗号化を依存させることができる、容易に再現されない、要素を使用して暗号化セッションを初期化するのに使用される。ナンス４１２および４１４は、以下により詳細に説明するとおり、キーボード１６２とコンポーネント２０２の間で伝送されるデータの暗号化および認証のための初期値を生成するのに使用することができる。

【００２９】

キーボードからコンポーネントにデータをセキュリティで保護された形で送るプロセス

図５は、コンポーネント２０２がキーボード１６２からデータをセキュリティで保護された形で受け取るセッションに、キーボード１６２およびコンポーネント２０２が関与す

ることができるプロセスを示している。図５のプロセスは、暗号化（送信データの傍受から保護する）と認証（送信データの変更から保護する）を共に提供する。ただし、伝送のセキュリティ要件に応じて、暗号化または認証を単独で使用することもできることを理解されたい。たとえば、データの変更を許容することができるが、傍受は許容することができない場合、暗号化を単独で使用することができる。逆に、データの傍受を許容することができるが、データの変更は許容することができない場合、認証だけを使用することができる。

【００３０】

最初、キーボード１６２とコンポーネント２０２が、ナンスを交換する（５０２）。たとえば、図４に関連して前述したとおり、キーボード１６２が、ナンス４１２を生成して、コンポーネント２０２に送ることが可能であり、コンポーネント２０２が、ナンス４１４を生成して、キーボード１６２に送ることが可能である。ナンスを生成するための技術は、当技術分野では周知であり、したがって、本明細書で詳述することはしない。一部の例として、ナンス４１２および４１４は、乱数、メモリの何らかの領域の内容、時刻、温度、月相（phase of the moon）等、あるいはしばしば変化する可能性が高くてキーボード１６２またはコンポーネント２０２が同じナンスを２回生成する可能性が低くなるだけ十分な範囲を有する任意の他の要因、に基づいて生成することが可能である。

【００３１】

ナンス４１２および４１４が交換される（５０２）と、キーボード１６２およびコンポーネント２０２はそれぞれ、両方のナンスを所有する。次に、キーボード１６２およびコンポーネント２０２は、共に合意した数式を使用して、両方のナンスおよびキー４０２の関数として２つの初期値、すなわち、ＩＶ＿ｃおよびＩＶ＿ｍを計算する（５０４）。つまり、Ｋ＝キー４０２、$Ｎ_1$＝ナンス４１２、および$Ｎ_2$＝ナンス４１４である場合、

ＩＶ＿ｃ＝ｆ（Ｋ，$Ｎ_1$，$Ｎ_2$）、および

ＩＶ＿ｍ＝ｇ（Ｋ，$Ｎ_1$，$Ｎ_2$）である。

【００３２】

機能ｆおよびｇは、あらゆる関数であることが可能である。好ましい実施形態では、

ｆ（Ｋ，$Ｎ_1$，$Ｎ_2$）＝$ＣＢＣ－３ＤＥＳＭＡＣ_Ｋ$（ｃｏｎｓｔ＿ＩＶ，$Ｎ_1$｜$Ｎ_2$）、および

ｇ（Ｋ，$Ｎ_1$，$Ｎ_2$）＝ｆ（Ｋ，$Ｎ_1$，$Ｎ_2$）ｘｏｒ　０ｘｆｆｆｆｆｆｆｆｆｆｆｆｆｆｆｆであり、

ここで、ｃｏｎｓｔ＿ＩＶは、定数値４０４（図４に示す）に等しい。キーボードとコンポーネントが２つの定数値（たとえば、ｃｏｎｓｔ＿ＩＶ＿１およびｃｏｎｓｔ＿ＩＶ＿２）を共有するさらなる好ましい実施形態では、関数ｆおよびｇは、代替として、以下のとおり計算することができる。

【００３３】

ｆ（Ｋ，$Ｎ_1$，$Ｎ_2$）＝$ＣＢＣ－３ＤＥＳＭＡＣ_Ｋ$（ｃｏｎｓｔ＿ＩＶ＿１，$Ｎ_1$｜$Ｎ_2$）、および

ｇ（Ｋ，$Ｎ_1$，$Ｎ_2$）＝$ＣＢＣ－３ＤＥＳＭＡＣ_Ｋ$（ｃｏｎｓｔ＿ＩＶ＿２，$Ｎ_1$｜$Ｎ_2$）

【００３４】

（演算子「｜」は連結を意味し、したがって、$Ｎ_1$｜$Ｎ_2$は、$Ｎ_1$と$Ｎ_2$を連結することからもたらされる値である。「ｘｏｒ」は、ビット単位の「排他ＯＲ」演算であり、したがって、Ａ　ｘｏｒ　Ｂは、ＡまたはＢのどちらかで「１」であるビットを「１」に設定するが、ＡとＢの両方で「１」であるビットは「１」に設定せず、他のすべてのビットをゼロに設定することからもたらされる値である。）$ＣＢＣ－３ＤＥＳＭＡＣ_Ｋ$（ｃｏｎｓｔ＿ＩＶ，$Ｎ_1$｜$Ｎ_2$）は、暗号化関数であり、この関数の意味は、当技術分野で周知であり、以下により詳細に説明する。

【００３５】

ＩＶ＿ｃおよびＩＶ＿ｍが計算された後、キーボード１６２とコンポーネント２０２の

間における通信を開始することができる。キーボード１６２が、キー入力、すなわち、操作者がキーの１つを押すことによるキー入力（あるいは＜ＳＨＩＦＴ＞と「Ａ」、または＜ＣＴＲＬ＞と「Ａ」などのキーのある組合せ）を受け取る（ステップ５０６）。次に、キーボードは、キー入力を暗号化し（５０８）、暗号化は、好ましくは、キー４０２およびＩＶ＿ｃに基づく。好ましい実施形態では、キー入力は、キー４０２をキーとし、ＩＶ＿ｃを初期値として、ＣＢＣ－３ＤＥＳを使用して暗号化される。ＣＢＣ－３ＤＥＳは、当技術分野で周知の暗号化アルゴリズムであり、以下により詳細に説明する。さらに、キーボード１６２は、好ましくは、キー４０２およびＩＶ＿ｍに基づき、キー入力に関するメッセージ認証コード（ＭＡＣ）を計算する（５１０）。好ましい実施形態では、メッセージ認証コードは、キー４０２をキーとし、ＩＶ＿ｍを初期値としてＣＢＣ－３ＤＥＳＭＡＣを使用して生成される。前述したとおり、ＣＢＣ－３ＤＥＳＭＡＣは、当技術分野で周知であり、以下により詳細に説明する。

【００３６】

キーボードが暗号化されたキー入力データとＭＡＣの両方を生成した後、コンポーネント２０２が、その暗号化されたキー入力データおよびＭＡＣをキーボード１６２から受け取る５１２（ステップ５１２）。次に、コンポーネント２０２は、キー４０２およびＩＶ＿ｃを使用してデータを暗号化解除し（５１４）、キー４０２およびＩＶ＿ｍを使用してデータの検証も行う（ステップ５１４）。次に、処理は、ステップ５０６に戻り、キーボードにおける次の入力を受け取る。

【００３７】

暗号化関数ＣＢＣ－３ＤＥＳおよびＣＢＣ－３ＤＥＳＭＡＣ

ＣＢＣ－３ＤＥＳは、データ暗号化標準（ＤＥＳ）と暗号ブロック連鎖（ＣＢＣ）と組み合わせる暗号化関数である。「３ＤＥＳ」とは、ＤＥＳ暗号化アルゴリズムが所与のデータ・ブロックに３回、適用されることを意味する（「トリプルＤＥＳ」）。ＤＥＳは、キーをデータに周知のやり方で適用することによってデータを暗号化する。ＤＥＳは、メッセージを、より小さいブロックに分割し、個々のブロックを暗号化することによって長いメッセージを暗号化する。（「トリプルＤＥＳ」が使用される場合、ＤＥＳアルゴリズムは、各ブロックに対して３回、そのブロックに関する暗号化テキストを生成するために適用される。）ＤＥＳ（およびトリプルＤＥＳ）は、キーだけを使用して各データ・ブロックを暗号化することができるが、暗号ブロック連鎖が使用される場合、１つのブロックの暗号化は、そのキーだけにではなく、直前のブロックを暗号化することによって生成された暗号化テキストにも基づく。したがって、所与のブロックの暗号化は、２つの入力に、すなわち、キー、および先行のブロックを暗号化したことによりもたらされた暗号化テキストに基づく。暗号化される第１のデータ・ブロックは、「先行の」ブロックを有さないので、暗号ブロック連鎖プロセスは、「初期値」を準備しなければならない。つまり、第１のデータ・ブロックは、キーおよび何らかの初期値に基づいて暗号化される。初期値は、後続のブロックの暗号化では使用されないが、どのようにそれらのブロックが暗号化されるかに間接的に影響を与えることができる（第１のブロックの暗号化テキストが初期値に基づき、第２のブロックの暗号化テキストが第１のブロックの暗号化テキストに基づき、以下同様であるため）。

【００３８】

以上の説明に鑑みて、「ＣＢＣ－３ＤＥＳ$_K$（ＩＶ，メッセージ」という語句は、トリプルＤＥＳおよび暗号ブロック連鎖を使用してキーＫで「メッセージ」を暗号化することを意味し、ＩＶは、暗号ブロック連鎖のための初期値である。

【００３９】

ＣＢＣ－３ＤＥＳＭＡＣは、ＣＢＣ－３ＤＥＳを使用してメッセージ認証コード（message authentication code：ＭＡＣ）を生成するやり方である。詳細には、ＣＢＣ－３ＤＥＳＭＡＣ$_K$（ＩＶ，メッセージ）という語句は、トリプルＤＥＳおよび暗号ブロック連鎖を使用し、ＩＶを暗号ブロック連鎖のための初期値として使用してキーＫで「メッセージ」が暗号化されることを意味する。ただし、ＣＢＣ－３ＤＥＳＭＡＣの目的は、メッ

セージに関する複雑な暗号化テキストではなく、メッセージに関するＭＡＣを生成することだけであるため、最後の暗号化テキスト・ブロックだけが保存され、残りの暗号化テキスト・ブロックは、破棄されることが可能である。この最後の暗号化テキスト・ブロックをＭＡＣとして使用することができる。というのは、定数のキーおよび定数のＩＶが与えられても、異なるメッセージによって同じ最終ブロックが生成される可能性は低いからである（あるいは、より正確には、各ブロックが2^n個の異なる値を表すことが可能である場合、任意の２つのメッセージが同じ最終ブロックを有する確率は$1/2^n$だけしかない）。

【００４０】

ＣＢＣ－３ＤＥＳについての上記の特定の選択、ならびにＣＢＣ－３ＤＥＳを使用する上記のやり方は、暗号化されたキーボード通信に特に有利であることに留意されたい。暗号化されるべきメッセージの領域は小さい（たとえば、１２８個の異なるＡＳＣＩＩ文字程度）ので、暗号ブロック連鎖は、暗号が破られないようにするのに特に役立つ。直線的（straight）暗号化が（連鎖なしで）使用された場合、所与のセッション内で、各文字は、入力されるたびに毎回、同じ暗号化テキストに暗号化されることになる。たとえば、「ｅ」を入力することにより、同じ暗号化テキストが常に生成されることになる。経験に基づく推測を行うことにより（たとえば、「ｅ」が英語において最もよく出現する文字であるという事実を使うことにより）、そのような暗号をより容易に破ることが可能である。セッション内の入力のすべてを連鎖させることは、同じデータが、入力ストリームの中でどこに現れるかに応じて異なる暗号化テキストが出現することを確実にすることにより、暗号を破ることをより困難にする（たとえば、「ｅ」が、同じ暗号化テキストを常にもたらさない可能性がある）。さらに、ナンスに基づいて新しい初期値を生成することによって各セッションに関する暗号化を変更することにより、観察者が、セキュリティを危うくするのに使用する可能性がある使用パターンを検出することを防止する（たとえば、毎回のセッションで入力される最初のテキストがパスワードである場合、観察者は、そのパスワードに関する暗号化テキストをキャプチャし、リプレー攻撃を開始することができる）。さらに、ＤＥＳによって使用される暗号ブロックのサイズは、ＤＥＳが８バイトブロックを扱い、ほとんどのキーボード・プロトコルは、このサイズに収まることが可能なブロックでデータを伝送するため（たとえば、ＵＳＢ標準も８バイト・ブロックを扱い、したがって、各ＵＳＢブロックは、無駄な領域なしに１つのＤＥＳブロックの中に収まることが可能である）、特によく適している。ただし、任意の他の暗号も使用することが可能であり、ＣＢＣと同様の連鎖概念をそのようブロック暗号に適用することも可能であることに留意されたい。

【００４１】

さらに、本明細書で説明する暗号化スキームがキーボードに特によく適しているのと同じ理由で、この暗号化スキームは、マウス（または他のポインティング・デバイス）などの他のあるタイプの入力デバイスにもよく適していることにさらに留意されたい。それらの入力デバイスは、少量のボキャブラリ（vocabulary）や、複雑な暗号化アルゴリズムを実行する能力が限られていることなどの、様々な特徴をキーボードと共有している。

【００４２】

データを暗号化するキーボードの例示的な用法

図６は、暗号化を実行するキーボードをセキュリティで保護された通信を要するコンポーネントと共に使用することができる例示的な環境を示している。図６の例では、製造業者６０２が、複数のキーボード１６２（１）、１６２（２）、…１６２（ｎ）を製造し、一般の使用のためにそれらのキーボードを流通させる。キーボード１６２（１）、１６２（２）、…１６２（ｎ）のそれぞれは、（図４に示す）キー４０２および定数値４０４を組み込んでいる（または、リムーバブル半導体メモリ用のポートによるなどの、キー４０２および定数値４０４に外部でアクセスするのに使用することができる何らかの手段、を組み込んでいる）。製造業者６０４は、キーボードとセキュリティで保護された形で通信することに役立つコンポーネント２０２（１）、２０２（２）、…２０２（ｍ）を製造す

る。コンポーネント２０２（１）、２０２（２）、…２０２（ｍ）のそれぞれは、キー４０２および定数値４０４を組み込んでいる（または、何からの仕方でキーおよび定数値を受け取ることができる）。したがって、コンポーネント２０２（１）、２０２（２）、…２０２（ｍ）は、前述した技術を介して、キーボード１６２（１）、１６２（２）、…１６２（ｎ）から入力を受け取ることが可能である。

【００４３】

製造業者６０２は、両方の製造業者は、セキュリティで保護された通信のために組み込まれるべきキー４０２および定数４０４について合意することができるように、製造業者６０４と前から存在する関係を有することが可能である。一例では、製造業者６０２と６０４は、同一のエンティティである。別の例では、製造業者６０４は、コンポーネント２０２（１）、２０２（２）、…２０２（ｍ）がセキュリティで保護されたキーボードからデータを受け取ることができることを望むコンポーネント２０２（１）、２０２（２）、…２０２（ｍ）の製造業者であり、製造業者６０２は、コンポーネント２０２（１）、２０２（２）、…２０２（ｍ）とセキュリティで保護された通信を行うためのキーボードを製造し、キー４０２および／または定数４０４を保持するのに十分なだけ信頼できると製造業者６０４が考えたキーボードの製造業者である。

【００４４】

以上の例は、単に説明のために提示しており、本発明を決して限定するものと解釈すべきではないことに留意されたい。本発明を様々な実施形態に関連して説明してきたが、本明細書で使用してきた言葉は、限定する言葉ではなく、説明し、例示する言葉であるものと理解されたい。さらに、本発明を特定の手段、材料、および実施形態に関連して説明してきたが、本発明は、本明細書で開示した詳細に限定されるものではない。むしろ、本発明は、特許請求の範囲に含まれるようなすべての機能的に等価の構造、方法、および用途を範囲に含む。本明細書の教示を利用できる当分野の技術者は、教示に多数の変更を加えることができ、変更は、本発明の態様の範囲および趣旨を逸脱することなく行うことができる。

【図面の簡単な説明】

【００４５】

【図１】本発明の態様を実装することができる例示的なコンピューティング環境を示すブロック図である。

【図２】キーボードとコンポーネントの間の通信がセキュリティで保護されていないチャネルを介して行われる可能性がある第１の例示的な環境を示すブロック図である。

【図３】キーボードとコンポーネントの間の通信がセキュリティで保護されていないチャネルを介して行われる可能性がある第２の例示的な環境を示すブロック図である。

【図４】本発明の態様によるセキュリティで保護された通信のために構成されており、ナンスを交換するキーボードとコンポーネントを示すブロック図である。

【図５】キーボードとコンポーネントの間でセキュリティで保護された通信セッションを行うためのプロセスを示す流れ図である。

【図６】本発明の態様によるセキュリティで保護された通信を行うようにキーボードおよびコンポーネントを分散させることができる第１の例示的な環境を示すブロック図である。

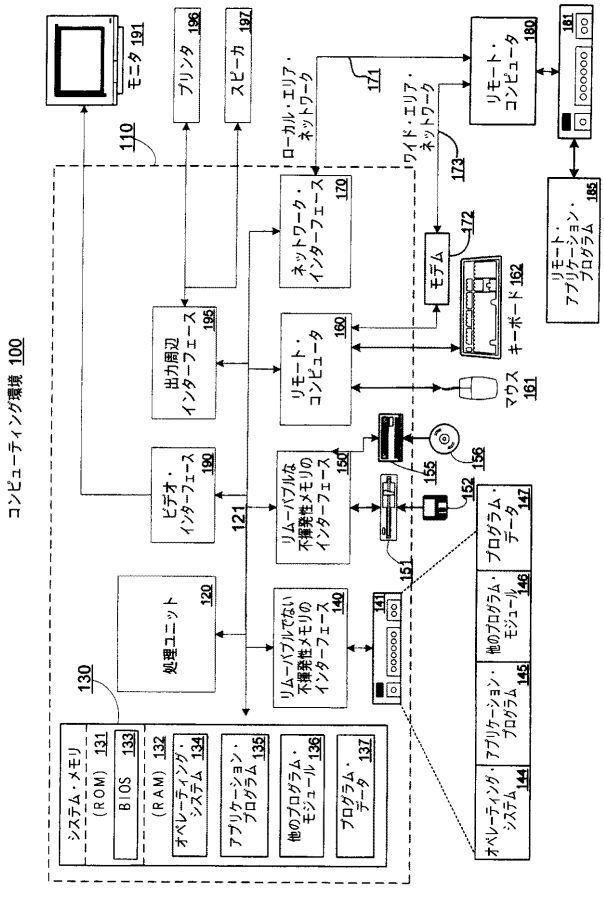
【符号の説明】

【００４６】

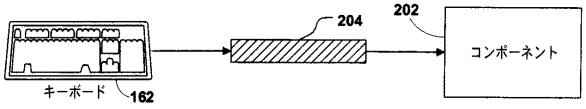
１１０　コンピュータ
１３４（１）、１３４（２）　オペレーティング・システム
１６２（１）、１６２（２）、１６２（ｎ）　キーボード
２０２（１）、２０２（２）、２０２（ｍ）、２０４　コンポーネント
３０２　ユニバーサル・シリアル・バス
３０４　ユニバーサル・シリアル・バス・ドライバ
３０６　ソフトウェア

４０２　キー
４０４　定数
４１２　ナンス
４１４　ナンス
６０２、６０４　製造業者

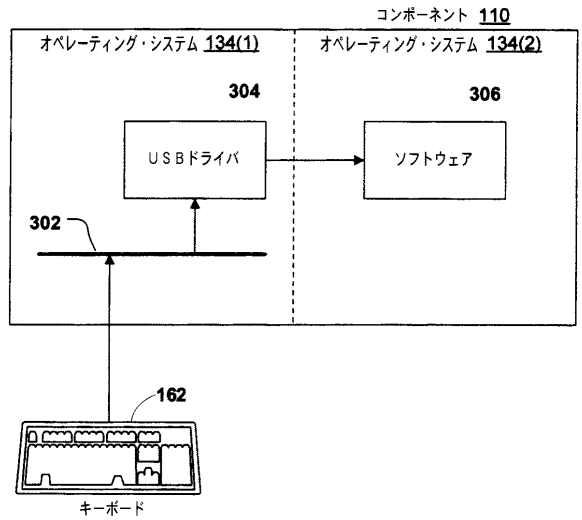
【図１】



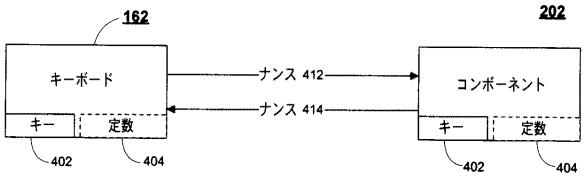
【図２】



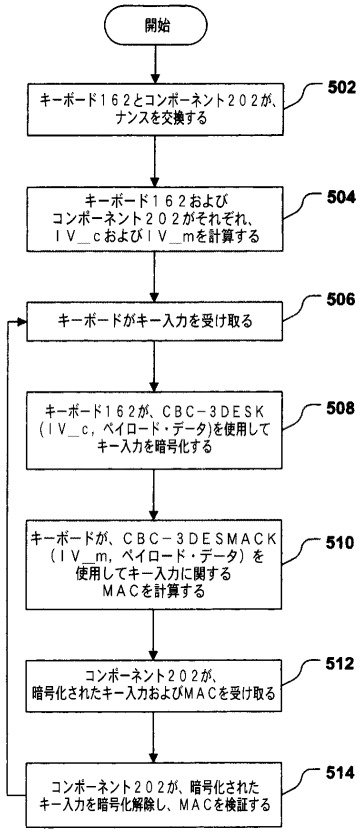
【図３】



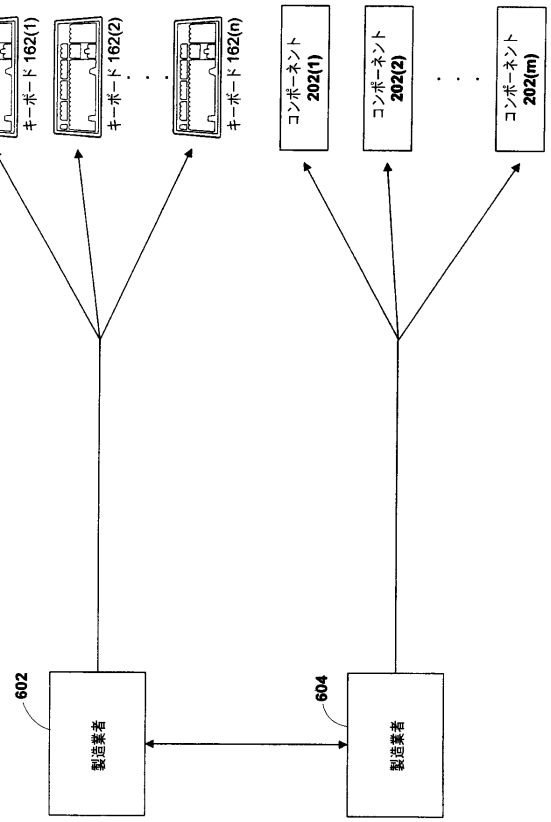
【図４】



【図５】


開始
キーボード１６２とコンポーネント２０２が、ナンスを交換する
502
キーボード１６２およびコンポーネント２０２がそれぞれ、ＩＶ＿ｃおよびＩＶ＿ｍを計算する
504
キーボードがキー入力を受け取る
506
キーボード１６２が、ＣＢＣ－３ＤＥＳＫ（ＩＶ＿ｃ，ペイロード・データ）を使用してキー入力を暗号化する
508
キーボードが、ＣＢＣ－３ＤＥＳＭＡＣＫ（ＩＶ＿ｍ，ペイロード・データ）を使用してキー入力に関するＭＡＣを計算する
510
コンポーネント２０２が、暗号化されたキー入力およびＭＡＣを受け取る
512
コンポーネント２０２が、暗号化されたキー入力を暗号化解除し、ＭＡＣを検証する
514

【図６】


キーボード162(1)
キーボード162(2)
キーボード162(n)
コンポーネント202(1)
コンポーネント202(2)
コンポーネント202(m)
602
製造業者
604
製造業者

フロントページの続き

(72)発明者　ジョシュ　ベナロー
アメリカ合衆国　９８０５２　ワシントン州　レッドモンド　１５９　コート　ノースイースト　５０２８

審査官　岩橋　龍太郎

(56)参考文献　特開平１１－０３９０８２（ＪＰ，Ａ）
国際公開第０２／０４４８７５（WO，Ａ１）
特開２００３－０９９３３２（ＪＰ，Ａ）
特開２００３－０８７２４３（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　１／００
Ｇ０６Ｆ　１／２０
Ｇ０６Ｆ　３／０２－　３／０２７
Ｇ０９Ｃ　１／００－　５／００
Ｈ０３Ｍ　１１／０４－１１／２４
Ｈ０４Ｋ　１／００－　３／００
Ｈ０４Ｌ　９／００－　９／３８