(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2007-529959
(P2007-529959A)
(43)公表日　平成19年10月25日(2007.10.25)

(51)Int.Cl.			F I			テーマコード（参考）
H04L	***9/32***	***(2006.01)***	H04L	9/00	675A	4C117
A61B	***5/00***	***(2006.01)***	H04L	9/00	675Z	5J104
			A61B	5/00	102D	

審査請求 未請求　予備審査請求 未請求　（全 27 頁）

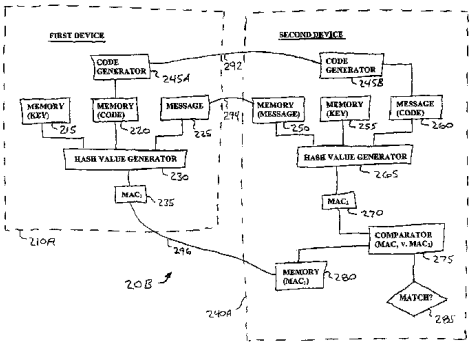
(21)出願番号　特願2007-504021 (P2007-504021)
(86)(22)出願日　平成17年3月15日 (2005.3.15)
(85)翻訳文提出日　平成18年9月15日 (2006.9.15)
(86)国際出願番号　PCT/US2005/008521
(87)国際公開番号　WO2005/091546
(87)国際公開日　平成17年9月29日 (2005.9.29)
(31)優先権主張番号　10/801,070
(32)優先日　平成16年3月15日 (2004.3.15)
(33)優先権主張国　米国 (US)

(71)出願人　505003528
カーディアック・ペースメーカーズ・インコーポレーテッド
アメリカ合衆国・５５１１２・ミネソタ州・セントポール・ハムライン　アベニュ・ノース・４１００
(74)代理人　100064621
弁理士　山川　政樹
(74)代理人　100098394
弁理士　山川　茂樹
(72)発明者　ヒーリー，スコット・ジェイ
アメリカ合衆国・５５３１１・ミネソタ州・メイプル　グローブ・ジュノウ　レーン　ノース・６２９５

最終頁に続く

(54)【発明の名称】埋込可能医療デバイスのテレメトリのための暗号認証

(57)【要約】
埋込可能医療デバイスと外部プログラマの間で通信される無線テレメトリによるメッセージの保全性が、メッセージを符号化することによって認証される。メッセージは、乱数またはタイム・スタンプ、および秘密鍵に基づいて暗号化される。メッセージは、暗号化および復号、またはハッシュ関数の実行によって認証される。



【特許請求の範囲】
【請求項１】
メッセージとそのメッセージの関数として生成された第１のハッシュ値に対応するデータを受信するように構成された受信機と、
前記受信機に結合されて、鍵と前記メッセージを格納するように構成されたメモリと、
前記メモリに結合されて、第２ハッシュ値を前記鍵と前記メッセージの関数として生成するように構成されたハッシュ値生成器と、
前記ハッシュ値生成器に結合されて、前記第１ハッシュ値が前記第２ハッシュ値と異なるかどうか判断するように構成された比較器とを備える埋込可能デバイス。
【請求項２】
前記メモリにタイム・スタンプを供給するように構成されたクロックをさらに含み、前記第２ハッシュ値が前記タイム・スタンプの関数として生成される請求項１に記載のデバイス。
【請求項３】
前記メモリに結合された数生成器をさらに含み、前記第２ハッシュ値が、前記数生成器によって供給された数の関数として生成される請求項１に記載のデバイス。
【請求項４】
前記数生成器が、乱数生成器と疑似乱数生成器の任意の組合せの少なくとも１つを含む請求項３に記載のデバイス。
【請求項５】
前記メモリに結合された鍵生成器をさらに含み、前記鍵が動的に生成される請求項１に記載のデバイス。
【請求項６】
前記受信機に結合された治療または監視回路をさらに含む請求項１に記載のデバイス。
【請求項７】
前記メモリに結合された誘導テレメトリ・チャネルをさらに含む請求項１に記載のデバイス。
【請求項８】
前記ハッシュ値生成器がＳＨＡ－１を実装するように構成される請求項１に記載のデバイス。
【請求項９】
前記ハッシュ値生成器がプロセッサと実行可能命令を含む請求項１に記載のデバイス。
【請求項１０】
埋込可能デバイス上で、メッセージとそのメッセージの関数として生成された第１のハッシュ値に対応するデータを受信するステップと、
鍵と前記メッセージを前記埋込可能デバイスのメモリ内に格納するステップと、
第２のハッシュ値を前記鍵と前記メッセージの関数として生成するステップと、
前記第１ハッシュ値と前記第２ハッシュ値を比較するステップとを備える方法。
【請求項１１】
コードを前記メモリ内に格納するステップをさらに含み、前記第２ハッシュ値が前記コードの関数として生成される請求項１０に記載の方法。
【請求項１２】
前記コードがタイム・スタンプを含む請求項１１に記載の方法。
【請求項１３】
前記鍵を格納するステップが近距離通信リンクで通信するステップを含む請求項１０に記載の方法。
【請求項１４】
埋込可能デバイスから、メッセージと前記メッセージの関数として生成された第１のハッシュ値を受信するように構成された非埋込可能トランシーバと、
前記トランシーバに結合されて、鍵と前記メッセージを格納するように構成されたメモ

リと、
前記メモリに結合されて、第２のハッシュ値を前記鍵と前記メッセージの関数として生成するように構成されたハッシュ値生成器と、
前記ハッシュ値生成器に結合されて、前記第１ハッシュ値が前記第２ハッシュ値と異なるかどうか判断するように構成された比較器とを備えるデバイス。
【請求項１５】
前記トランシーバが、前記鍵を受信するように構成された近距離テレメトリ・アンテナを含む請求項１４に記載のデバイス。
【請求項１６】
前記トランシーバが、遠距離テレメトリ用に構成される請求項１４に記載のデバイス。
【請求項１７】
前記トランシーバに結合されたコード生成器をさらに含み、前記コード生成器が後続のメッセージに鮮度コードを供給する請求項１４に記載のデバイス。
【請求項１８】
前記コード生成器が、クロックと乱数生成器の任意の組合せの少なくとも１つを含む請求項１７に記載のデバイス。
【請求項１９】
第１の遠距離トランシーバと、
前記第１遠距離トランシーバに結合された第１のプロセッサと、
前記第１プロセッサに結合された第１のメモリと、
前記プロセッサに結合された電気回路とを含む埋込可能デバイスと、
第２の遠距離トランシーバと、
前記第２遠距離トランシーバに結合された第２のプロセッサと、
前記第２プロセッサに結合された第２のメモリと、
前記プロセッサに結合されたデータ・ポートとを含む外部デバイスとを備えるシステムであって、
前記第１プロセッサと第２プロセッサの任意の組合せの少なくとも１つが、前記第１プロセッサによって生成されたコード、前記第１メモリと前記第２メモリ内に格納された鍵、メッセージに基づいて暗号文を生成するように構成された暗号化アルゴリズを実施するための命令を実行するように適応され、
前記第１プロセッサと第２プロセッサの任意の組合せの少なくとも１つが、前記コードと前記鍵に基づいて前記暗号文から前記メッセージを復号するよう構成された復号アルゴリズを実施するための命令を実行するように適応されるシステム。
【請求項２０】
前記埋込可能デバイスが、前記プロセッサに結合され、かつ前記鍵を通信するように適応された誘導テレメトリ・コイルを含む請求項１９に記載のシステム。
【請求項２１】
前記外部デバイスが、前記プロセッサに結合され、かつ前記鍵を通信するように適応された誘導テレメトリ・コイルを含む請求項１９に記載のシステム。
【請求項２２】
前記電気回路が治療回路を含む請求項１９に記載のシステム。
【請求項２３】
前記電気回路が監視回路を含む請求項１９に記載のシステム。
【請求項２４】
前記データ・ポートが、キーボード、マウス、コントローラ、データ記憶装置、ネットワーク接続、モデム、データ・バスの任意の組合せのうちの少なくとも１つを含む請求項１９に記載のシステム。
【請求項２５】
第１の遠距離トランシーバと、
前記第１遠距離トランシーバに結合された第１のプロセッサと、

前記第１プロセッサに結合された第１のメモリと、
前記プロセッサに結合された電気回路と
を含む埋込可能デバイスと、
第２の遠距離トランシーバと、
前記第２遠距離トランシーバに結合された第２のプロセッサと、
前記第２プロセッサに結合された第２のメモリと、
前記第２プロセッサに結合されたデータ・ポートと
を含む外部デバイスとを備えるシステムであって、
前記第１プロセッサと第２プロセッサの任意の組合せの少なくとも１つが、前記第１プロセッサによって生成されたコードと、前記第１メモリと前記第２メモリ内に格納された鍵と、メッセージとに基づいて第１のハッシュ値を生成するための命令を実行するように適応され、
前記第１プロセッサと第２プロセッサの任意の組合せの少なくとも１つが、前記メッセージ、前記コードと前記鍵に基づいて第２のハッシュ値を生成するための命令を実行するように適応され、また前記第１ハッシュ値と前記第２ハッシュ値を比較するように構成されるシステム。
【請求項２６】
前記第１プロセッサに結合されて、前記鍵を通信するように適応された誘導テレメトリ・コイルをさらに含む請求項２５に記載のシステム。
【請求項２７】
前記第２プロセッサに結合されて、前記鍵を通信するように適応された誘導テレメトリ・コイルをさらに含む請求項２５に記載のシステム。
【請求項２８】
前記電気回路が治療回路を含む請求項２５に記載のシステム。
【請求項２９】
前記電気回路が監視回路を含む請求項２５に記載のシステム。
【請求項３０】
前記データ・ポートが、キーボード、マウス、コントローラ、データ記憶装置、ネットワーク接続、モデム、データ・バスの任意の組合せのうちの少なくとも１つを含む請求項２５に記載のシステム。
【請求項３１】
第１デバイスからコードを受信するステップと、
前記第１デバイスと第２デバイスに鍵を格納するステップであって、前記第１デバイスと前記第２デバイスのうちの少なくとも１つが埋込可能である、格納するステップと、
前記第２デバイス上で暗号文を生成するステップであって、前記暗号文を前記コード、前記鍵とメッセージの関数として生成するステップと、
前記第１デバイス上で前記暗号文を受信するステップと、
前記メッセージを受信するために前記第１デバイス上で前記暗号文を復号するステップであって、前記メッセージを前記コードと前記鍵の関数として復号するステップと、
前記第１デバイス上で前記メッセージを認証するステップを備える方法。
【請求項３２】
前記コードを受信するステップが乱数を受信するステップを含む請求項３１に記載の方法。
【請求項３３】
前記コードを受信するステップがタイム・スタンプを受信するステップを含む請求項３１に記載の方法。
【請求項３４】
前記メッセージを認証するステップが、前記メッセージ内に含まれる識別コードをチェックするステップを含む請求項３１に記載の方法。
【請求項３５】

前記識別コードのチェックが、前記識別コードと格納された値とを比較するステップを含む請求項３４に記載の方法。

【請求項３６】

前記メッセージを認証するステップが、前記メッセージ内に含まれる誤り検出符号をチェックするステップを含む請求項３１に記載の方法。

【請求項３７】

前記誤り検出符号をチェックするステップが、

前記メッセージの関数として計算値を生成するステップと、

前記計算値と前記誤り検出符号を比較するステップとを含む請求項３６に記載の方法。

【請求項３８】

前記誤り検出符号のチェックが巡回冗長符号をチェックするステップを含む請求項３６に記載の方法。

【請求項３９】

前記鍵を格納するステップが鍵を生成するステップを含む請求項３１に記載の方法。

【請求項４０】

前記鍵を生成するステップが、鍵を前記第１デバイス内に格納されたデータの関数として計算するステップを含む請求項３９に記載の方法。

【請求項４１】

前記鍵を格納されたデータの関数として計算するステップが、デバイス・シリアル番号、製造日付、製造時刻、デバイス・モデル番号、前記デバイスの測定された特性の任意の組合せの少なくとも１つに基づいて格納されたデータを含むメモリにアクセスするステップを含む請求項４０に記載の方法。

【請求項４２】

前記鍵を計算するステップがハッシュ・アルゴリズムを実行するステップを含む請求項４０に記載の方法。

【請求項４３】

前記鍵を前記第１デバイス内に格納するステップが誘導結合を介して通信するステップを含む請求項３１に記載の方法。

【請求項４４】

前記鍵を前記第２デバイス内に格納するステップが誘導結合を介して通信するステップを含む請求項３１に記載の方法。

【請求項４５】

前記鍵を格納するステップが前記鍵を暗号化するステップを含む請求項３１に記載の方法。

【請求項４６】

前記第１暗号文を生成するステップが、データ暗号化規格（ＤＥＳ）、トリプル・データ暗号化規格（３ＤＥＳ）、拡張暗号化規格（ＡＥＳ）、国際データ暗号化アルゴリズム（ＩＤＥＡ）、ＢｌｏｗｆｉｓｈとＣＡＳＴの任意の組合せの少なくとも１つから選択されたアルゴリズムを実行するステップを含む請求項３１に記載の方法。

【請求項４７】

第１デバイスからコードを受信するステップと、

前記第１デバイスと第２デバイスに鍵を格納するステップであって、前記第１デバイスと前記第２デバイスのうちの少なくとも１つが埋込可能である、前記鍵を格納するステップと、

前記第２デバイス上で、前記コード、前記鍵、メッセージの関数として生成される第１のハッシュ値を生成するステップと、

前記第１デバイス上で前記メッセージと前記第１ハッシュ値を受信するステップと、

前記第１デバイス上で、前記コード、前記鍵、前記メッセージの関数として生成される第２のハッシュ値を生成するステップと、

前記第１デバイス上で前記第１ハッシュ値と前記第２ハッシュ値を比較するステップと

を備える方法。
【請求項４８】
前記コードを受信するステップが乱数を受信するステップを含む請求項４７に記載の方法。
【請求項４９】
前記コードを受信するステップが、タイム・スタンプの受信とタイム・スタンプの生成の任意の組合せの少なくとも１つを含む請求項４７に記載の方法。
【請求項５０】
前記鍵を格納するステップが鍵を生成するステップを含む請求項４７に記載の方法。
【請求項５１】
前記鍵を生成するステップが、鍵を前記第１デバイス内に格納されたデータの関数として計算するステップを含む請求項５０に記載の方法。
【請求項５２】
前記鍵を計算するステップが第３のハッシュ値を計算するステップを含む請求項５１に記載の方法。
【請求項５３】
前記第１デバイス内へ前記鍵を格納するステップが、誘導結合を介して通信するステップを含む請求項４７に記載の方法。
【請求項５４】
前記第２デバイス内へ前記鍵を格納するステップが、誘導結合を介して通信するステップを含む請求項４７に記載の方法。
【請求項５５】
前記鍵を格納するステップが前記鍵を暗号化するステップを含む請求項４７に記載の方法。
【請求項５６】
前記第１ハッシュ値の生成と前記第２ハッシュ値の生成の任意の組合せの少なくとも１つが、ハッシュ・アルゴリズムを実行するステップを含む請求項４７に記載の方法。
【請求項５７】
前記ハッシュ・アルゴリズムの実行が、セキュア・ハッシュ標準アルゴリズムとメッセージ・ダイジェスト・アルゴリズムの任意の組合せの少なくとも１つを実行するステップを含む請求項５６に記載の方法。
【請求項５８】
セキュア・ハッシュ標準アルゴリズムの実行が、ＳＨＡ－１とＳＨＡ－２５６の任意の組合せの少なくとも１つを実行するステップを含む請求項５７に記載の方法。
【請求項５９】
メッセージ・ダイジェスト・アルゴリズムの実行が、ＭＤ２、ＭＤ４、ＭＤ５の任意の組合せの少なくとも１つを実行するステップを含む請求項５７に記載の方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本主題は、心臓ペースメーカや埋込可能除細動器などの埋込可能医療デバイスに関する。具体的には、本主題は、埋込可能医療デバイスを使用したテレメトリのためのデータ認証に関する。
【背景技術】
【０００２】
ペースメーカや埋込可能除細動器などの心調律管理デバイスを含めて、埋込可能医療デバイスは通常、外部プログラマと呼ばれるデバイスと無線周波数テレメトリ・リンクを介して通信する能力を有する。
【０００３】
従来の埋込可能医療デバイスは、誘導テレメトリ・コイルまたは他の短距離通信チャネ

ルを用いてリモート・プログラマとデータを交換する。手持ち型のワンドが埋込可能デバイスから数インチ以内に置かれ、データが誘導結合によって転送される。

【０００４】

メッセージの長距離テレメトリが登場し、またそれに付随して通信範囲が増加するのに伴い、メッセージが損なわれるリスクが増加する。たとえば、メッセージまたはメッセージの一部が捕捉され、後に悪意のあるやり方で使用されるという再生攻撃が行われる。

【発明の開示】

【発明が解決しようとする課題】

【０００５】

改良型テレメトリのためのシステムおよび方法が求められている。

【課題を解決するための手段】

【０００６】

本主題は、メッセージで通信されるデータを認証するための方法とシステムを含む。具体的には、本主題は、メッセージの保全性が損なわれていないことと、通信セッションが許可されていることを検証するための方法とシステムを提供する。

【０００７】

ある実施態様では、メッセージは、同じ鍵を使用してメッセージが暗号化され、復号される対称暗号化アルゴリズムを使用して伝達される。ある実施態様では、メッセージは、送信側と受信側の両方によって使用される一方向ハッシュ・アルゴリズムを使用して伝達され、受信側がメッセージの保全性が保たれていることを検証することを可能にする。

【０００８】

他の態様は、以下の詳細な説明を読み、またその一部を形成する図面を見ると明らかになる。

【発明を実施するための最良の形態】

【０００９】

以下の詳細な説明では、本明細書の一部を形成しており、また本主題が実施される特定の実施形態が例として示されている諸図面を参照する。これらの実施形態は、当業者が本主題を実施できるようにするのに十分なほど詳細に述べられており、諸実施形態は組み合わされることができ、または他の実施形態が使用されることができ、また本主題の範囲から逸脱せずに構造、機械、論理、電気に関する変更が加えることができることを理解されたい。したがって、以下の詳細な説明は限定的な意味で解釈されるべきでなく、本主題の範囲は、添付の特許請求の範囲およびその均等物によって定められる。

【００１０】

上述したように、心臓ペースメーカなどの埋込可能医療デバイスに使用される従来のテレメトリ・システムは、信号を送受信するために、埋込可能デバイスと外部プログラマのアンテナ間の誘導結合を使用する。送信側アンテナによって生成される誘導磁界が距離と共に急速に低下するので、デバイス間の通常およそ数インチの距離で適切に働くためにこうしたシステムは、埋込可能デバイスと外部プログラマのワンド・アンテナとの間が非常に近いことを必要とする。

【００１１】

一方、本主題は、遠距離放射を使用した埋込可能医療デバイスでのテレメトリを可能にするための装置と方法を含む。遠距離放射を使用した通信は、さらに大きい距離に渡って行われる。これによって、患者の遠隔監視など、テレメトリ・システムの他の応用や他のタイプの外部デバイスとの通信が可能となる。遠距離放射に基づくテレメトリには、無線周波数テレメトリ、音響テレメトリ、電界テレメトリが含まれる。

【００１２】

図１Ａは、外部デバイス３０と埋込可能デバイス６０とを含むシステム２０Ａを示している。外部デバイス３０は、プログラマまたはリピータと称されることがある。様々な実施形態において、プログラマは、表示画面、プリンタ、あるいはオペレータにデータを運び、操作者によって入力され、または入力インターフェースから受信されたデータまたは

他の命令を受信する他の出力デバイスを含む。様々な実施形態において、リピータは、遠隔監視またはプログラミングを可能にする、通信ネットワークとのインターフェースを備えるデバイスを含む。様々な実施形態において、リピータは、埋込可能デバイスと通信ネットワークの間で通信し、通信範囲を有効に拡張するデバイスを指す。ある実施形態では、リピータは、家庭内の電話回線に接続されており、したがって医療関係者が旧来の電話サービス（ＰＯＴＳ：ｐｌａｉｎ　ｏｌｄ　ｔｅｌｅｐｈｏｎｅ　ｓｅｒｖｉｃｅ）網を介してその家の住居者の埋込可能デバイスを監視することを可能にする。ある実施形態では、リピータは、ケーブル・モデムまたは他のインターフェースを用いてインターネットなどのネットワークに通信可能に結合される。

【００１３】

埋込可能デバイス６０は、ペースメーカ、心臓除細動器、細動除去器、あるいは生理学的な状態を監視し、電気エネルギー、薬またはその任意の組合せを用いて治療を行うように構成された他の埋込可能デバイスを含む。

【００１４】

外部デバイス３０は、メモリ３２、プロセッサ３４、データ入力ポート３６、データ出力ポート３８、テレメトリ４０、テレメトリ４２を含む。

【００１５】

メモリ３２は、本主題によるアルゴリズムを実装するためのデータ、ファームウェア、ソフトウェアを格納するように適応される。様々な実施形態において、メモリ３２は、読出し専用メモリ、ランダム・アクセス・メモリまたは他のタイプの記憶装置を含む。

【００１６】

プロセッサ３４は、メモリ３２内に格納された認証アルゴリズムを実行するように構成される。

【００１７】

データ入力ポート３６は、プロセッサ３４に結合される。様々な実施形態において、データ入力ポート３６は、キーボード、マウス、コントローラ、データ記憶装置または他のデータ入力手段を含む。ある実施形態では、データ入力ポートは、有線または無線ネットワーク接続、モデムまたはデータ・バスを含む。データ入力ポート３６は、受信側デバイスに通信されるメッセージとして直接的にまたは間接的に働くデータまたは命令を受信する。ある実施形態では、プロセッサ３４は、測定されまたは計算されたパラメータに基づいて埋込可能デバイス６０のためのメッセージを独立に生成する。

【００１８】

データ出力ポート３８はプロセッサ３４に結合される。様々な実施形態において、データ出力ポート３８は、プリンタ、表示装置、オーディオ・トランスジューサ、データ記憶装置または他の出力デバイスを含む。データ出力ポート３８によって、埋込可能デバイスまたは外部デバイスからの結果、データまたはメッセージは、操作者により知覚可能なものとなる。

【００１９】

テレメトリ４０は遠距離トランシーバを含み、遠距離放射を送受信するように構成されたアンテナに結合される。テレメトリ４２は、短距離無線テレメトリ・トランシーバを含み、またある実施形態では、誘導アンテナを含む。遠距離無線周波数結合などの遠距離無線通信手段や誘導結合などの近距離無線通信手段は、参照により本明細書に組み込まれている、２００１年１２月１９日に出願された、同一出願人による米国特許出願第１０／０２５１８３号、「ＡＮ　ＩＭＰＬＡＮＴＡＢＬＥ　ＭＥＤＩＣＡＬ　ＤＥＶＩＣＥ　ＷＩＴＨ　ＴＷＯ　ＯＲ　ＭＯＲＥ　ＴＥＬＥＭＥＴＲＹ　ＳＹＳＴＥＭＳ」、発明人Ｊｅｆｆｒｅｙ　Ａ．Ｖｏｎ　Ａｒｘ他に開示されている。

【００２０】

埋込可能デバイス６０は、メモリ６２とプロセッサ６４と電気回路６６とテレメトリ６８とテレメトリ７０とを含む。

【００２１】

メモリ６２は、本主題によるアルゴリズムを実装するためのデータ、ファームウェア、ソフトウェアを格納するように適応される。様々な実施形態において、メモリ６２は、読出し専用メモリ、ランダム・アクセス・メモリまたは他のタイプの記憶装置を含む。

【００２２】

プロセッサ６４は、メモリ６２内に格納された認証アルゴリズムを実行するように構成される。

【００２３】

様々な実施形態において、電気回路６６は、パルス発生器、ペースメーカ、除細動器、治療回路、監視回路、換気量センサ、インピーダンス測定回路、呼吸センサ、あるいは治療を行うように構成され、または生理学的な状態または事象を監視するように構成された他の回路を含む。

【００２４】

テレメトリ６８は、トランシーバを含み、遠距離放射を送受信するように構成されたアンテナに結合され、外部デバイス３０のテレメトリ４０と協働する。テレメトリ７０は、近距離無線テレメトリ・トランシーバを含み、ある実施形態では誘導アンテナを含み、また外部デバイス３０のテレメトリ４２と協働する。ループの形の誘導アンテナに加えて、たとえばソレノイドを含めて、他のアンテナの形も企図されている。

【００２５】

外部デバイス３０と埋込可能デバイス６０は、無線周波数伝送を使用してテレメトリ４０とテレメトリ６８の間の遠距離通信を可能にするように構成される。さらに、外部デバイス３０と埋込可能デバイス６０は、誘導結合されたアンテナを使用してテレメトリ４２とテレメトリ７０の間の近距離通信を可能にするように構成される。

【００２６】

ある実施形態では、遠距離通信セッションが、まず誘導結合された通信セッションを確立することによって開始される。図１Ａに示す実施形態では、外部デバイス３０は、近距離アンテナを使用して埋込可能デバイス６０と通信するためのテレメトリ４２を含む。図１Ｂに示す実施形態では、補助または外部デバイス８０が、誘導結合アンテナを使用して埋込可能デバイス６０と通信するために使用される。補助デバイス８０は、テレメトリ４０とテレメトリ６８の間の遠距離通信への移行が後に続いて行われる、誘導アンテナを介したテレメトリ７０との通信を確立するために使用される。デバイス８０は、プロセッサ８２と誘導テレメトリ８４とアンテナ８６と電気回路２４とメモリ２６とを含む。デバイス８０は、リンク３７を介して外部デバイス３０のプロセッサ３４と通信状態にある。リンク３７は、安全なデータを通信するためのチャネルを含む。たとえばある実施形態では、リンク３７は、デバイス８０からデバイス３０に暗号鍵を中継するために使用される。様々な実施形態において、リンク３７は、有線接続と無線通信チャネルとを含む。

【００２７】

図２は、第１のデバイス２１０Ａと第２のデバイス２４０Ａとを含むシステム２０Ｂを示しており、これらのデバイスのうちの１つは体内に埋め込み可能であり、もう１つは外部にある。たとえばある実施形態では、デバイス２１０Ａはリピータまたはプログラマを含み、デバイス２４０Ａは埋込可能パスル生成器を含む。図２のデバイス２１０Ａまたは２４０Ａが、図１Ａの外部デバイス３０または埋込可能デバイス６０に対応するデバイス内で実装される。

【００２８】

通常、埋込可能デバイスと外部デバイスは使用可能な電源と処理容量が互いに異なる。具体的には、プログラマであれリピータであれ、外部デバイスの電源は、置換可能なまたは充電可能なバッテリを含み、あるいは従量制の回線サービスへの有線接続を含む。それとは異なり、埋込可能デバイスの電源は一般に、取り替えるには外科的な処置を必要とするバッテリであり、簡単には充電することができない。得られる電源が限られていること、また物理的サイズへの考慮により、埋込可能デバイスの処理容量は一般に、外部デバイスのそれと比べて小さい。

【００２９】
デバイス２１０Ａは、他の要素もあるが特に挙げると、メモリ２１５、メモリ２２０、メッセージ・モジュール２２５、ハッシュ値生成器２３０を含む。デバイス２１０Ａの選択された要素は、別個のものとして示されているが、組み合わされることがあるのを理解できるであろう。たとえば、メモリ２１５とメモリ２２０が単一の物理メモリ・デバイス内に存在してもよく、メッセージ・モジュール２２５とハッシュ値生成器２３０がプロセッサ内に単独に実装され、あるいはネットワーク接続やキーボードなどデータ入力デバイスと共にプロセッサ内に実装されることもある。
【００３０】
メモリ２１５は、秘密鍵の記憶域を提供する。鍵は、秘密に保たれた文字列である。長い鍵は一般に、より短い鍵に比べて大きい安全性をもたらす。
【００３１】
メモリ２２０は、コードの記憶域を提供する。ある実施形態では、コードは、通信セッション内の特定のメッセージの通信を可能にするためのメッセージ鍵の働きをする文字列である。通信セッションは、たとえば医療施設への事後の訪問時に発生する一連の交換を指す。ある実施形態では、セッションの各メッセージは一意のコードで認証される。様々な実施形態において、コードは、図に示されるように第２デバイス２４０Ａによって生成され、または第１デバイス２１０Ａによって生成されるタイム・スタンプまたは乱数を含む。コードは、メッセージ（またはメッセージの断片）が無許可のユーザによって捕捉され、通信システムを危険にさらすために後に使用される再生攻撃を阻止するための鮮度の尺度（ｍｅａｓｕｒｅ　ｏｆ　ｆｒｅｓｈｎｅｓｓ）を提供する。
【００３２】
図示する実施形態では、メッセージ・モジュール２２５は、第２デバイス２４０Ａに伝達されるメッセージを表している。ある実施形態では、メッセージ・モジュール２２５は、キーボードなどのデータ入力デバイスを含み、またはそれに結合される。ある実施形態では、メッセージ・モジュール２２５は、プロセッサ上で実行されるアルゴリズムの関数として生成されるデータを格納するためのメモリを含む。ある実施形態では、メッセージ・モジュール２２５は、第２デバイス２４０Ａへの引渡しのために命令をリモート・プロセッサから受信するためのネットワーク接続を含む。ある実施形態では、メッセージ・モジュール２２５は、測定された生理学的パラメータ、または埋込可能デバイスによって決定された他のパラメータに基づいてメッセージを生成する。
【００３３】
メモリ２１５から受信された鍵、メモリ２２０から受信されたコード、メッセージ・モジュール２２５から受信されたメッセージを使用してハッシュ値生成器２３０は、ハッシュ関数に従って一意の値を計算する。ハッシュ関数は、可変長の入力文字列を取り、ハッシュ値、メッセージ・ダイジェストまたは指紋と呼ばれる固定長、一般にはより短い出力文字列に入力文字列を変換する一方向関数である。具体的には、ハッシュ値生成器２３０への入力のうちの１つは秘密鍵なので、出力ハッシュ値はメッセージ認証コード（ＭＡＣ）またはデータ認証コード（ＤＡＣ）と称される。図では、デバイス２１０Ａによって生成されるメッセージ認証コードは、MAC_1　２３５と示されている。
【００３４】
ハッシュ・アルゴリズムは、所与のメッセージ・ダイジェストに対応するメッセージを見つけること、または同じメッセージ・ダイジェストを生成する２つの異なるメッセージを見つけることが計算的に実行不可能であるので、安全であるとされている。したがって、変更されたメッセージでは、メッセージ・ダイジェストにおいて検出可能な変化がもたらされる。
【００３５】
様々なハッシュ・アルゴリズムが、ハッシュ値、したがってメッセージ認証コードの生成のために使用される。たとえば、セキュア・ハッシュ・アルゴリズム（ＳＨＡ－１）は、メッセージまたはデータ・ファイルの圧縮表現を生成する。アルゴリズムＳＨＡ－１は

、参照により本明細書に組み込まれている、ＦＩＰＳ　ＰＵＢ　１８０－１　Ｓｅｃｕｒｅ　Ｈａｓｈ　Ｓｔａｎｄａｒｄ、１９９５年４月に規定されている。アルゴリズムＳＨＡ－１は、最大2^{64}ビットのメッセージを圧縮し、２０バイトのメッセージ・ダイジェストを生成することができる。ハッシュ・アルゴリズムの追加の例にはメッセージ・ダイジェスト・アルゴリズムが含まれ、このアルゴリズムの一部は、ＭＤ２、ＭＤ４、ＭＤ５として知られている。アルゴリズムＭＤ２、ＭＤ４、ＭＤ５はそれぞれ、１２８ビット長の圧縮されたメッセージ・ダイジェストを提供する。ＭＤ２、ＭＤ４、ＭＤ５についての説明とソース・コードは、それぞれが参照により本明細書に組み込まれている、Ｉｎｔｅｒｎｅｔ　Ｒｅｑｕｅｓｔ　Ｆｏｒ　Ｃｏｍｍｅｎｔ　ＲＦＣ１３１９、ＲＦＣ１３２０やＲＦＣ１３２１において見ることができる。

【００３６】

第２デバイス２４０Ａは、様々な実施形態においてタイム・スタンプ、乱数、または新鮮度の何らかの他の尺度を生成するコード生成器２４５Ｂを含む。コード生成器２４５Ｂの出力は、第２デバイス２４０Ａのメモリ２６０内に格納される。ある実施形態では、コード生成器２４５Ｂによって生成されるコードは、通信リンク２９２によって示されるように、デバイス２１０Ａのコード生成器２４５Ａによって生成されるコードと同期される。一例として、コードは、乱数生成器で使用される同じシードを使用するように調整することによって同期される。コード生成器２４５Ａは、デバイス２１０Ａのメモリ２２０内に格納するのためのコードを提供する。ある実施形態では、通信リンク２９２は、暗号化せずに通信する有線または無線の平文リンクである。別の実施形態では、コードは、暗号化または他の安全な通信手法を使用して送信される。図に示された実施形態では、コード生成器２４５Ａとコード生成器２４５Ｂは、互いに同期されたリアルタイム・クロックを含み、それぞれがタイム・スタンプを供給する。

【００３７】

ある実施形態では、コードはタイム・スタンプを含み、第１デバイス２１０Ａと第２デバイス２４０Ａの両方が、コードを生成するように構成されたリアルタイム・クロックを含む。ある実施形態では、乱数がコードのために使用され、メッセージを受信するデバイスは、コードを選択し、メッセージ送信の前にメッセージ送信側デバイスにそのコードを送信する。双方向リンクの場合、第１デバイス２１０Ａと第２デバイス２４０Ａの両方が、コード生成器を含む。

【００３８】

ある実施形態によれば、鍵は、通信セッションの最初に通信参加者に配布される。ある実施形態によれば、鍵は、誘導テレメトリ・システムを使用して外部デバイスによって埋込可能デバイスから受信される。誘導テレメトリ・リンクが、通信セッションを開始し、鍵を配布するために使用される。

【００３９】

様々な実施形態において、鍵は、所定の期間の間、所定の数の交換の間、あるいは他のやり方で取り消されまたは別の鍵で置き換えられるまで有効なままである。ある実施形態では、鍵は、通信セッションの継続時間の間有効なままであり、誘導リンクによって通信参加者間で交換される。たとえば、埋込可能デバイスの鍵は、１日、１週間、１ヶ月、１年またはデバイスの寿命の間有効のままであってもよい。ある実施形態では、初期の鍵は埋込可能デバイスによって生成され、その後のコードは、埋込可能デバイスまたは外部デバイスによって確立される。ある実施形態では、埋込可能デバイス用の鍵は、プログラマを使用した暗号化された交換によって変更される。

【００４０】

コードがリンクの片側によって選択される（タイム・スタンプ以外のコードが使用される場合などの）ある実施形態では、メッセージ受信側は、そのメッセージのためのコードを選択する。一方、メッセージ送信側がコードの選択を許可される場合、通信セッションは再生攻撃を受けやすい。再生攻撃では、正当な送信側がコードを選択し、受信側にコードを通信し、次いで有効なコマンドを送信する。敵意のある送信側は、この交換を記録し

、後にこのセッションを乗っ取る。次に、悪意のある送信側は、前の交換を再現することができ、メッセージ受信側は、正当なコード（前に受信したのと同じコード）、次いで正当なコマンド（前に受信したのと同じコマンド）を受信する。

【００４１】

再生攻撃を防止するため、シーケンスは以下の通りである。まず、メッセージ発信元デバイスは、メッセージ受信側デバイスにコードを要求する。メッセージ受信側デバイスは、そのメッセージのコードをランダムに選択し、そのコードを（平文または暗号文として）メッセージ発信元デバイスに通信する。次いで、メッセージ送信側デバイスは、鍵とコードで生成されたハッシュと共にメッセージを送信する。このイベント・シーケンスでは、前のコードを再現する敵意ある送信側は、受信側をだますことができない。

【００４２】

第２デバイス２４０Ａは、鍵を格納するように構成されたメモリ２５５を含む。鍵は、安全なやり方で通信参加者に配布される。ある実施形態では、鍵は、デバイスの製造またはデバイスの移植時に確立される。さらに、鍵は、無許可のデバイスからはアクセス不可能であるように保存される。ある実施形態では、鍵は、誘導結合された通信リンクによりテレメトリ・セッションの最初に交換される。

【００４３】

ある実施形態では、鍵は、特定のデバイスに固有のデータに基づいてハッシュ関数を実行することによって生成される。たとえば、埋込可能デバイスの製造時刻、製造日付、モデル番号、シリアル番号の任意の組合せが、ハッシュ・アルゴリズムへの入力として使用され、鍵はメッセージ・ダイジェストの関数として決定される。データに固有の他のデバイスもまた、メッセージ・ダイジェスト、したがって鍵の生成に使用される。たとえばある実施形態では、測定されまたは計算された、デバイスの性能に固有のパラメータまたは特性が、ハッシュ・アルゴリズムへの入力として使用される。ある実施形態では、ハッシュ関数の入力に使用されるデータは、外部の読取り装置または他のデバイスからは一般にアクセス不可能であるメモリ位置に格納される。ある実施形態では、ハッシュ関数の入力に使用されるデータは、たとえばループ・アンテナを使用した誘導結合リンクを用いて読み取られるメモリ位置に格納される。ある実施形態では、鍵を生成するのに使用されるハッシュ関数はメッセージ認証コードを生成するのに実行されるハッシュ関数とは異なる。

【００４４】

第２デバイス２４０Ａはメッセージを格納するように構成されたメモリ２５０を含む。ある実施形態では、メッセージは、通信リンク２９４で示すように第１デバイス２１０Ａから第２デバイス２４０Ａに平文で送信される。ある実施形態では、メッセージは暗号化された形で送信される。

【００４５】

第２デバイス２４０Ａは、メモリ２５０、メモリ２５５、メモリ２６０に結合されたハッシュ値生成器２６５を含む。ある実施形態では、単一のメモリ・デバイスが、本明細書では２５０、メモリ２５５、メモリ２６０と示された記憶レジスタの任意の組合せの少なくとも１つを含む。ハッシュ値生成器２６５は、メモリ２５０からメッセージ、メモリ２５５から鍵、メモリ２６０からコードを受信し、ハッシュ関数に従って一意のハッシュ値を計算する。ハッシュ値生成器２６５によって生成されたハッシュ値は、MAC_2 ２７０と示されたメッセージ認証コードである。ある実施形態では、ハッシュ値生成器２６５は、第２デバイス２４０Ａ内のメモリ内に格納されたアルゴリズムを実行するプロセッサを含む。ハッシュ値生成器２６５によって実行されるハッシュ関数は、ハッシュ値生成器２３０によって実行されるハッシュ関数と同じである。

【００４６】

第２デバイス２４０Ａは、MAC_1 ２３５とMAC_2 ２７０の比較に基づいて出力を生成する比較器２７５を含む。通信リンク２９６は、メモリ２８０への格納のためMAC_1 ２３５を第２デバイス２４０Ａに提供するための通信チャネルを備える。様々な実施形態において、通信リンク２９６は、平文または暗号文を伝達する。ある実施形態では、

比較器２７５は、第２デバイス２４０Ａのプロセッサを含む。

【００４７】

比較器２７５の出力は、MAC_1 ２３５がMAC_2 ２７０に一致するかどうか判断される問合せ２８５で評価される。MAC_1 ２３５とMAC_2 ２７０の比較によって差が認められない場合は、メッセージは認証されたものとして扱われ、比較によって差が認められる場合は、メッセージは認証されていないものとして扱われる。メッセージが認証される場合は、メッセージのさらなる処理が、第２デバイス２４０Ａの他の要素によって実施され、この要素のうちのいくつかは図に示されていない。メッセージが認証されない場合、ある実施形態では、さらなる措置は取られない。ある実施形態では、メッセージが認証されない場合、エラー・フラグが設定され、それに応じてさらなる措置が取られる。ある実施形態では、問合せ２８５は、第２デバイス２４０Ａのプロセッサ上で実行されるアルゴリズムを含む。

【００４８】

様々な実施形態において、代表的な通信リンク２９２、２９４、２９６は、無線通信チャネルである。たとえば、通信リンク２９２、２９４、２９６は、誘導テレメトリ・チャネルと遠距離テレメトリ・チャネルの任意の組合せの少なくとも１つを含む。他の通信リンクも企図されている。たとえばある実施形態では、ループ・アンテナを含むリンクが、短距離テレメトリを使用して鍵を交換するために設けられる。さらに、ある実施形態によれば、コードは、リンク２９２を使用した通信セッション内で交換されるメッセージ毎に交換される。ある実施形態では、通信リンク２９２、２９４、２９６は、遠距離リンクであり、遠距離送信機を含む。たとえば、通信リンク２９４はメッセージを平文で伝達し、通信リンク２９６は、第１デバイス２１０Ａによって生成されたメッセージ認証コード２３５をはやり平文で伝達する。

【００４９】

ある実施形態では、リンク２９２は、第１デバイス２１０Ａと第２デバイス２４０Ａの両方が、コード生成器の働きをするリアルタイム・クロックを含むので省かれる。ある実施形態では、送信されるメッセージ毎に新しいコードがリアルタイム・クロックを使用して生成され、そのコードは遠距離送信を使用して平文で送信される。

【００５０】

図３は、本主題の一実施形態によって実施される方法３００を示している。イベント・シーケンスが変更され、一部のイベントが省略される他の方法も企図されている。方法３００は、メッセージを第１デバイスから第２デバイスに通信することを伴い、メッセージが本物であることが第２デバイスによって検証される。３０５で開始し、この方法は３１０に進み、秘密鍵が第１デバイスと第２デバイスの両方に格納される。鍵は、その識別が通常秘密に保たれており、第２デバイスと許可された第１デバイスだけに知られている所定の文字列を含む。ある実施形態では、鍵は、無許可のアクセスを防ぐためにリモート手段による読取りが不可能にされた第２デバイスのメモリ内に格納される。ある実施形態では、鍵は、誘導リンクにより交換される。鍵は、暗号化されて交換されることも、平文として交換されることもある。

【００５１】

３１５で、コードが、第１デバイスによって第２デバイスから受信される。コードは、たとえば遠距離テレメトリ・リンクなどの通信リンクで、第１デバイスによって受信される。様々な実施形態において、コードは、第２デバイスによって生成されたタイム・スタンプまたは乱数を含む。３１５の後に、第１デバイスと第２デバイスの両方が、メモリ内に格納されたコードを有する。ある実施形態では、コードは平文で交換される。

【００５２】

３２０で、第１デバイスは、鍵、コード、メッセージに基づいてメッセージ認証コードを生成する。メッセージ認証コードは、一方向ハッシュ値を含む。様々な実施形態において、メッセージは、命令、データまたは他のコンテンツを含む。

【００５３】

３２５で、第１デバイスによって生成されたハッシュ値が第２デバイスに通信される。さらに、メッセージが、第１デバイスから第２デバイスに送信される。ある実施形態では、ハッシュ値とメッセージは、遠距離送信機を使用して平文で送信される。

【００５４】

３３０で、ハッシュ値とメッセージが第２デバイスによって受信され、メモリ内に格納される。

【００５５】

３３５で、第２デバイスは、格納された鍵、格納されたコード、第１デバイスから受信されたメッセージに基づいて第２ハッシュ値を独立に生成する。ある実施形態では、第２ハッシュ値は、第１デバイスのアルゴリズムに一致するアルゴリズムを使用して計算されたメッセージ認証コードである。

【００５６】

３４０で、第１デバイスから受信されたハッシュ値と第２デバイスによって計算されたハッシュ値が、第２デバイス上で比較される。メッセージが本物であることは、ハッシュ値が一致する場合に確認される。

【００５７】

方法３００は３４５で終了するが、しかし、他の処理が行われてもよい。たとえばある実施形態では、ハッシュ値の比較の結果に応じて、後続のアルゴリズムまたは手順が実行される。具体的には、ある実施形態によれば、メッセージが本物であることが確認される場合はメッセージ内のいずれかの命令が実行され、メッセージが本物であることが確認されない場合はメッセージは廃棄される。

【００５８】

図４は、第１デバイス２１０Ｂと第２デバイス２４０Ｂの間で通信されるメッセージを認証するために対称暗号化アルゴリズムが使用されるシステム２０Ｃを示している。本文献の他所で述べたように、第１デバイス２１０Ｂのメモリ２１５と第２デバイス２４０Ｂのメモリ２５５はそれぞれ、秘密鍵の記憶域を提供する。さらに、第１デバイス２１０Ｂのメモリ２２０と第２デバイス２４０Ｂのメモリ２６０はそれぞれ、第２デバイス２４０Ｂのコード生成器２４５Ｃから鮮度コードを受信する。このコードは、通信リンク２９２を経由して第２デバイス２４０Ｂから第１デバイス２１０Ｂに送信される。図に示す実施形態では、単一のコード生成器２４５Ｃが、デバイス２４０Ｂ内に置かれており、第１デバイス２１０Ｂと第２デバイス２４０Ｂにコードを提供する。

【００５９】

図に示す実施形態によれば、メッセージは、第１デバイス２１０Ｂのメッセージ・モジュール２２５内から生じる。メッセージは、キーボード、記憶装置または他のデータ入力手段を使用して受信されるデータに基づいて生成される。さらに、メッセージは、リモート・デバイスから受信され、ネットワークまたは他の通信手段によって第１デバイス２１０Ｂに通信されたデータに基づいて生成される。様々な実施形態において、メッセージはデータと命令を含む。

【００６０】

図示する実施形態では、第１デバイス２１０Ｂは、プロセッサによって実行される暗号化アルゴリズム４３０を含む。暗号化アルゴリズム４３０は、暗号文４３５を、鍵、コード、メッセージの関数として生成する。鍵とコードなしでは、無許可の受信側は、暗号文だけに基づいてメッセージの内容を判断することはできないと仮定されている。

【００６１】

様々な対称暗号化方法が使用可能である。例には、それぞれの規格が参照により本明細書に組み込まれている、データ暗号化規格（ＤＥＳ）、トリプル・データ暗号化規格（３ＤＥＳ）、拡張暗号化規格（ＡＥＳ、連邦情報処理規格刊行１９７）、国際データ暗号化アルゴリズム（ＩＤＥＡ）、Ｂｌｏｗｆｉｓｈ（１９９３年、Ｂｒｕｃｅ Ｓｃｈｎｅｉｅｒによる設計）、ＣＡＳＴ（Ｅｎｔｒｕｓｔ（登録商標） Ｔｅｃｈｎｏｌｏｇｉｅｓ社）が含まれる。これらの方法の一部に関する追加の情報は、１９８７年のコンピュータ

・セキュリティ法（ＰＬ　１００－２３５）のもとで確立された組織である、情報技術研究所（ＩＴＬ：Ｉｎｆｏｒｍａｔｉｏｎ　Ｔｅｃｈｎｏｌｏｇｙ　Ｌａｂｏｒａｔｏｒｙ）のコンピュータ・セキュリティ部門から入手可能である。

【００６２】

暗号文４３５は、通信リンク４３７を使用して、第１デバイス２１０Ｂから第２デバイス２４０Ｂに無線で通信される。ある実施形態では、通信リンク４３７は、遠距離通信チャネルを含む。

【００６３】

第２デバイス２４０Ｂは、暗号文４３５を格納するように構成されたメモリ４４０を含み、また復号アルゴリズム４６５を実行するように構成されたプロセッサを含む。復号アルゴリズム４６５は、平文メッセージ４７０を鍵、コード、暗号文４３５の関数として生成する。

【００６４】

第２デバイス２４０Ｂは、認証チェック・アルゴリズム４７５を実行するように構成されたプロセッサを含む。様々な実施形態において、認証チェック・アルゴリズム４７５は、巡回冗長検査値を計算し、次いでこの巡回冗長検査値は、格納されまたは受信された値と比較される。ある実施形態では、認証チェック・アルゴリズム４７５は、送信側の識別を確認するために、受信されたメッセージ内に含まれる送信機の識別コードを検証する。

【００６５】

図５は、本主題の一実施形態によって実施される方法５００を示している。イベント・シーケンスが変更され、一部のイベントが省略される他の方法も企図されている。方法５００は、メッセージを第１デバイスから第２デバイスに通信することを伴い、メッセージが本物であることが第２デバイスによって検証される。この方法は、５０５で開始し、５１０に進む。そこでは秘密鍵が第１デバイスと第２デバイスの両方に格納される。鍵は所定の文字列を含み、通常、この文字列の識別は秘密に保たれており、第２デバイスと許可された第１デバイスだけに知られている。ある実施形態では、鍵は、無許可のアクセスを防ぐためリモート手段による読取りが不可能にされた第２デバイスのメモリ内に格納される。ある実施形態では、鍵は、誘導的に交換され、平文の形であることも、暗号文の形であることもある。

【００６６】

５１０で、コードが、第１デバイスによって第２デバイスから受信される。ある実施形態では、コードは、遠距離アンテナを含む通信リンクで、第２デバイスによって受信される。様々な実施形態において、コードは、第２デバイスによって生成されたタイム・スタンプまたは乱数を含む。５１５の後には、第１デバイスと第２デバイスの両方が、メモリ内に格納されたコードを有する。ある実施形態ではコードは平文で交換され、セッション内のメッセージ毎に新しいコードが選択される。

【００６７】

５２０で、第１デバイスは鍵、コード、平文メッセージに基づいて暗号文を生成する。メッセージは、様々な実施形態において、命令、データまたは他のコンテンツを含む。

【００６８】

５２５で、第１デバイスによって生成される暗号文が第２デバイスに通信される。ある実施形態では、暗号文は遠距離送信機を使用して送信される。

【００６９】

５３０で、平文メッセージの生成のため、格納された鍵と格納されたコードの関数として受信された暗号文が復号される。

【００７０】

５３５で、平文メッセージが、メッセージの内容を解析することによって認証される。たとえばある実施形態では、メッセージの発信元が本物であることを検証するため、メッセージ発信元に関連する識別コードが格納された値と比較される。ある実施形態では、メッセージの発信元が本物であることを検証するため、メッセージ発信元に関連する識別コ

ードがメッセージで受信された値と比較される。ある実施形態では、誤り検出符号が、メッセージ認証のために計算される。ある実施形態では、誤り検出符号は巡回冗長符号を含む。メッセージで受信された誤り検出符号はメッセージの関数として計算された値と比較される。

【００７１】

方法５００は５４０で終了するが、しかし、他の処理が行われてもよい。たとえばある実施形態では、認証の結果に応じて、後続のアルゴリズムまたは手順が実行される。具体的には、ある実施形態によれば、メッセージが本物であることが確認される場合はメッセージ内のいずれかの命令が実行され、メッセージが本物であることが確認されない場合はメッセージは廃棄される。

【００７２】

代替実施形態

ある実施形態では、メッセージ認証コードは、第１デバイス上で動作するハッシュ値生成器によって生成され、第２デバイス上で動作するハッシュ値生成器によって生成されたメッセージ認証コードと比較される。ある実施形態では、アルゴリズムは互いに同じである。

【００７３】

ある実施形態では、パルス生成器（埋込可能デバイス）とプログラマ（外部デバイス）の両方が秘密鍵を所有している。通信セッションの最初に、パルス生成器は、プログラマにタイム・スタンプまたは乱数を送信する。次いで、プログラマは、秘密鍵に基づく第１のメッセージ認証コード、乱数（またはタイム・スタンプ）、パルス生成器に送信されるメッセージを計算する。プログラマは、メッセージと第１メッセージ認証コードをパルス生成器に送信する。次いで、パルス生成器は、秘密鍵、乱数（またはタイム・スタンプ）、受信されたメッセージに基づいて第２のメッセージ認証コードを計算する。メッセージが本物かどうか判断するために、パルス生成器は第１と第２のメッセージ認証コードを比較する。

【００７４】

ある実施形態では、本主題は、埋込可能デバイスから外部デバイスに送信されるデータの認証に適用される。ある実施形態では、本主題は、外部デバイスから埋込可能デバイスに送信されるデータの認証に適用される。

【００７５】

ある実施形態では、第１デバイスと第２デバイスの間で通信されるすべてのデータが認証される。ある実施形態では、第１デバイスと第２デバイスの間で通信される所定のフレームまたは他のデータ・サブセットが認証を受ける。

【００７６】

ある実施形態では、秘密鍵またはコードの長さは、安全性への考慮または他の要因に基づいて調整される。

【００７７】

本明細書で示される諸実施例では、コード生成器は、第２デバイスの一部として述べられている。しかし、ある実施形態では、コード生成器は第１デバイスの一部であり、結果として生じるコードは第２デバイスに伝達される。

【００７８】

ある実施形態では、通信されるメッセージは、ハッシュ・アルゴリズムを使用してメッセージ・ダイジェストが計算される前にパディングされる。メッセージは、ハッシュ・アルゴリズムで使用するのに適したメッセージ長をもたらすように追加のビットを加えることによってパディングされる。

【００７９】

ある実施形態では、特定の暗号化アルゴリズムが、安全性向上のため、複数回繰り返される。ある実施形態では、メッセージ認証コードは送信または比較の前に追加のハッシュ関数にかけられる。ある実施形態では、メッセージ認証コードは、あるデバイスから別の

デバイスへの送信の前に暗号化される。ある実施形態では、１つの暗号化アルゴリズムまたは異なるアルゴリズムの複数のラウンドが暗号化テキストを送信する前に実行される。

【００８０】

ある実施形態では、鍵は通信する前に暗号化される。

【００８１】

ある実施形態では、このシステムは、セッション鍵とコードを使用するのではなく、時間と共に変化するメッセージ鍵を使用する。たとえばある実施形態では、そのメッセージ鍵は、セッション鍵とコードを使用して排他的論理和などの論理操作を実施することによって取得される。したがって、ハッシュ値が、時間的に変化するメッセージ鍵とメッセージを使用して生成される。

【００８２】

ある実施形態では、タイム・スタンプがコードとして使用される。たとえば、１秒の分解能では、コードは１秒毎に変化する。通信セッションの最初に、２つのデバイス（たとえば埋込可能デバイスと外部プログラマなど）のリアルタイム・クロックを合わせる。クロックは一般に、通信の継続時間を通して、だんだん互いに離れていく。メッセージ発信元は、メッセージとタイム・スタンプの両方を受信側に平文で送信する。メッセージの送信の後に続いて、メッセージ発信元は、セッション鍵に対して（たとえばハッシュ・アルゴリズムとしてＳＨＡ－１を使用して）ハッシュ関数を実行することによって生成された、暗号化されていない（平文の）メッセージ認証コード、タイム・スタンプ、メッセージを送信する。次いで、メッセージ受信側は、（暗号化されていない形で送信された）受信されたタイム・スタンプを、メッセージ受信側のコード生成器（またはリアルタイム・クロック）によって生成されたタイム・スタンプと比較する。受信されたタイム・スタンプが、生成されたタイム・スタンプと所定の値より大きい量だけ異なる場合は、メッセージはさらなる処理をせずに廃棄される。受信されたタイム・スタンプと生成されたタイム・スタンプとが十分に近い（たとえば、それらが所定の値より小さい量だけ互いに異なる）場合は、メッセージはさらに処理される。ある実施形態では、所定の値は８秒である。タイム・スタンプが十分に近い場合は、メッセージ受信側はメッセージ認証コードを生成し、次いでこのメッセージ認証コードは、メッセージ発信元から受信されたメッセージ認証コードと比較される。メッセージ認証コードが一致する場合、メッセージは認証される。

【００８３】

ある実施形態では、ハッシュ関数は、ＨＭＡＣと称され、またＦＲＣ２１０４に記載された認証アルゴリズムを含む。このアルゴリズムは、参照により本明細書に組み込まれている、ＦＩＰＳ ＰＵＢ １９８、Ｆｅｄｅｒａｌ Ｉｎｆｏｒｍａｔｉｏｎ Ｐｒｏｃｅｓｓｉｎｇ Ｓｔａｎｄａｒｄｓ Ｐｕｂｌｉｃａｔｉｏｎ、Ｔｈｅ Ｋｅｙｅｄ－Ｈａｓｈ Ｍｅｓｓａｇｅ Ａｕｔｈｅｎｔｉｃａｔｉｏｎ Ｃｏｄｅ（ＨＭＡＣ）；Ｃａｔｅｇｏｒｙ：Ｃｏｍｐｕｔｅｒ Ｓｅｃｕｒｉｔｙ Ｓｕｂｃａｔｅｇｏｒｙ：Ｃｒｙｐｔｏｇｒａｐｈｙ；Ｉｎｆｏｒｍａｔｉｏｎ Ｔｅｃｈｎｏｌｏｇｙ Ｌａｂｏｒａｔｏｒｙ、Ｎａｔｉｏｎａｌ Ｉｎｓｔｉｔｕｔｅ ｏｆ Ｓｔａｎｄａｒｄｓ ａｎｄ Ｔｅｃｈｎｏｌｏｇｙ、Ｇａｉｔｈｅｒｓｂｕｒｇ、ＭＤ ２０８９９－８９００、２００２年３月６日発行、に記載されている。

【００８４】

ＨＭＡＣに従って秘密鍵が、データ保全性とデータ発行元の認証を可能にする。ＨＭＡＣは、ＭＤ５、ＳＨＡ－１他など、反復暗号ハッシュ関数を使用して実装される。さらに、ＨＭＡＣは、メッセージ認証値の計算と検証のために秘密鍵を使用する。

【００８５】

ＨＭＡＣに従って、暗号ハッシュ関数はＨと表され、秘密鍵はＫと表される。関数Ｈは、データ・ブロックに対して基本の圧縮関数を反復することによってデータがハッシュされる暗号ハッシュ関数である。さらに、Ｂはこうしたブロックのバイト長を表し、Ｌはハッシュ出力のバイト長を表す。秘密鍵Ｋは、最大Ｂの任意の長さである。Ｂより長い鍵では、最初にＨを使用してＫをハッシュし、次いで、結果として生じるＬバイト列をＨＭＡ

Ｃへの実際の鍵として使用する。また２つの異なる固定文字列ｉｐａｄ（内）とｏｐａｄ（外）は、ｉｐａｄ＝バイト０×３６をＢ回繰り返した文字列と定義され、ｏｐａｄ＝バイト０×５ＣをＢ回繰り返した文字列と定義される。したがって、データ「ｔｅｘｔ」に対するＨＭＡＣは、Ｈ（Ｋ　ＸＯＲ　ｏｐａｄ，Ｈ（Ｋ　ＸＯＲ　ｉｐａｄ，ｔｅｘｔ））と計算される。具体的には、ＨＭＡＣ法は、以下の一連のステップを伴う。
（１）Ｋの最後にゼロを追加してＢバイトの文字列を作成する（たとえば、Ｋが２０バイトの長さで、Ｂ＝６４であれば、Ｋに４４個のゼロのバイト０×００が追加される）。
（２）ステップ（１）で計算されたＢバイトの文字列とｉｐａｄとのＸＯＲ（ビット毎の排他的論理和）を計算する。
（３）ステップ（２）の結果として得られたＢバイトの文字列にデータ「ｔｅｘｔ」のストリームを追加する。
（４）ステップ（３）で計算されたストリームにＨを適用する。
（５）ステップ（１）で計算されたＢバイトの文字列とｏｐａｄとのＸＯＲ（ビット毎の排他的論理和）を計算する。
（６）ステップ（５）の結果として得られたＢバイトの文字列に、ステップ（４）のＨの結果を追加する。
（７）ステップ（６）で生成されたストリームにＨを適用し、その結果を出力する。

【００８６】

ある実施形態では、ハッシュ関数はＳＨＡ－１を含み、アルゴリズムは、ＭＡＣ＝Ｈ（Ｋ＋ＯＰＡＤ‖Ｈ（Ｋ＋ＩＰＡＤ‖Ｍ）によって近似される。ただし、Ｋはある長さの鍵であり、Ｋ＋は鍵へのいくらかのパディングであり、Ｈ（）はハッシュ関数の適用であり、符号‖は連結を指す。値ＯＰＡＤとＩＰＡＤは定数である。ある実施形態では、ハッシュ・アルゴリズムはメッセージ認証コードを生成するために２度実行され、結果は切り捨てられる。ある実施形態では、メッセージ認証コードは、１２８ビットの長さへと切り捨てられる。

【００８７】

ある実施形態では、コード生成器はクロックを含む。クロックによって生成されるタイム・スタンプ値が、コードの働きをする。

【００８８】

ある実施形態では、埋込可能デバイスと外部デバイスの両方がそれぞれ、内部クロックを含む。通信セッションの最初に、クロックが近距離通信リンクを使用して同期させられる。ある実施形態では、クロックは、誘導リンクを使用して同期される。送信側デバイスは、各メッセージまたはフレーム毎にタイム・スタンプ値を平文の形で送信する。さらに、送信側デバイスは、タイム・スタンプ値とメッセージの関数として生成されたメッセージ認証コードを送信する。受信側デバイスは、受信されたタイム・スタンプ値を、その自体の内部クロックによって供給された現在の時間値と比較する。受信されたタイム・スタンプ値と、受信側デバイスの内部クロックによって供給された現在の時間値が十分に近くない場合、メッセージは再生攻撃であるとされ、メッセージが廃棄される。ある実施形態では、８秒しか差がない時間値は、時宜を得たものとされる。受信側デバイスは、受信されたタイム・スタンプ値を使用して、受信されたメッセージ認証コードとの比較のためメッセージ認証コードを生成する。

【００８９】

ある実施形態では、タイム・スタンプ値の平文のコピーを交換するのではなく、通信セッションの最初に、埋込可能デバイスと外部デバイスの内部クロックが同期される。クロックは所定の精度レベル内で同期され、送信される各メッセージは、送信側デバイスによって生成された現在のタイム・スタンプ値を含む。メッセージを認証するために受信側デバイスは、受信されたタイム・スタンプ値をそれ自体の内部クロック値と比較する。クロックの誤差を補償するために、時間値は所定のレベルへと丸められまたは切り捨てられ、クロック値がクロック遷移の所定の範囲内であれば、早い時間値と遅い時間値の両方がチェックされる。たとえば、ある実施形態では、時間値は直近の８秒値に丸められ、遷移端

が次の値から１秒以内にある場合、早い値と遅い値の両方が比較される。

【００９０】

ある実施形態では、それぞれのデバイスは、コード生成器として働く乱数（または疑似乱数）生成器を含む。これらの数生成器は互いに同じシード値を使用する。シードは、乱数または疑似乱数の数列を生成するのに使用される開始値である。ある実施形態では、シード値は、近距離通信リンクを使用して通信セッションの最初に交換され、そのセッションの後続の交換については、コード生成器によって供給される値は各フレームと共に送信される必要はない。ある実施形態では、コード生成器によって供給される値は、各フレームと共に平文で送信される。

【００９１】

ある実施形態では、通信リンクが双方向性であり、埋込可能デバイスと外部デバイスの両方からのメッセージが認証される対象であれば、両方のデバイスがコード生成器を含む。

【００９２】

ある実施形態ではメッセージを認証するために、メッセージを受信しているデバイスによってコードが選択される。認証される対象のデータが単一の送信で通信される場合、その送信の前に、受信デバイスは、まずコードを要求するように構成される。通信リンクが双方向性であり、また埋込可能デバイスと外部デバイスの両方がメッセージを認証するセッションでは、いずれかの特定のメッセージのコードが事前の交換で伝達される。

【００９３】

ある実施形態では、静的な鍵が識別を提供するために使用され、動的なコードが鮮度の尺度を提供するために使用される。ある実施形態では、鍵は動的であり、鍵の値を時間の関数として変更することにより、鮮度の尺度がもたらされる。動的な鍵が鍵生成器によって供給され、様々な実施形態において、鍵生成器は、数生成器またはクロックを含む。こうした実施形態では、鍵は、ハッシュ・アルゴリズムで使用される。ある実施形態では、鍵は、タイム・スタンプと組み合わされる。鍵とコードの任意の組合せのうちの少なくとも１つは、メッセージと組み合わされる。たとえば、ある実施形態では、鍵とコードは、論理的に組み合わされ、ＨＡＳＨアルゴリズムで使用される。他の組合せ方法も企図されている。ある実施形態では、埋込可能デバイスと外部デバイスは、同じ初期値がシードとして与えられ（ｓｅｅｄ）、それらの乱数生成器は、一致する数列を提供する。ある実施形態では、コードは省かれ、動的な鍵だけが使用される。

【００９４】

上記の説明は、限定的なものではなく、例示的なものであることを理解されたい。たとえば、上記で述べた諸実施形態またはその任意の部分は、互いに組合せて使用される。添付の特許請求の範囲では、語句「任意の組合せ」は、複数の要素だけでなく、単一の要素をも含むものである。本文献を精査すると、当業者には他の実施形態が明らかになろう。

【図面の簡単な説明】

【００９５】

【図１Ａ】埋込可能デバイス用の誘導テレメトリおよび長距離テレメトリを提供するシステムを示す図である。

【図１Ｂ】誘導テレメトリ・デバイスを示す図である。

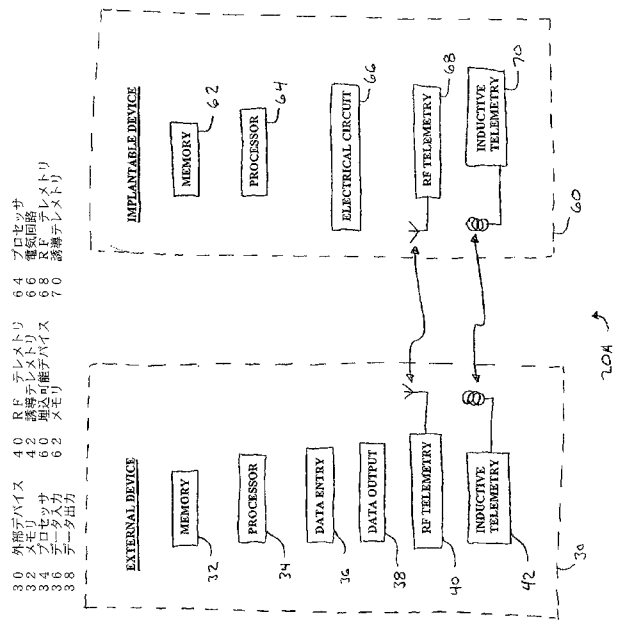
【図２】一実施形態によるハッシュベースの暗号化アルゴリズムを含むテレメトリ・システムを示す図である。

【図３】一実施形態による方法のフローチャートである。

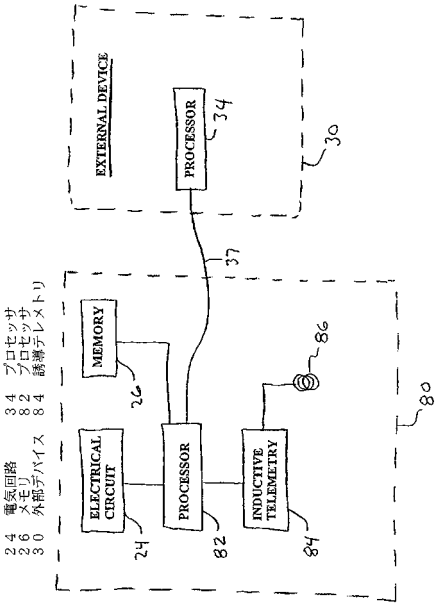
【図４】一実施形態による対称暗号化アルゴリズムを含むテレメトリ・システムを示す図である。

【図５】一実施形態による方法のフローチャートである。

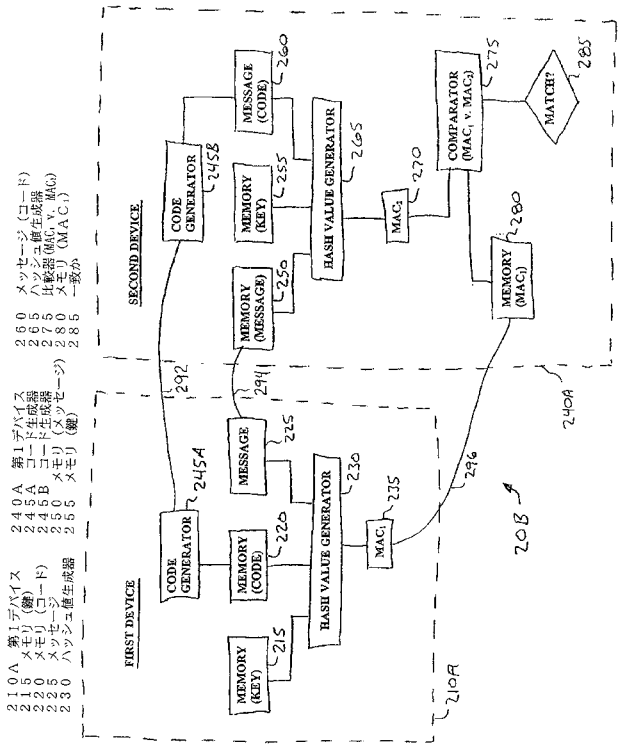
【図１Ａ】



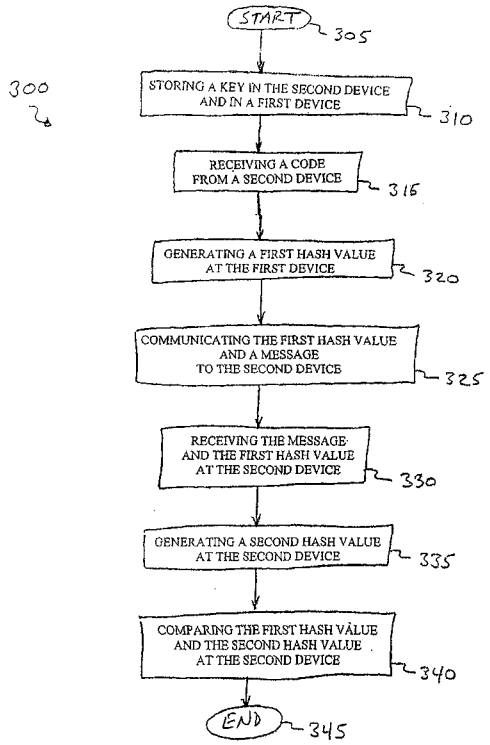
【図１Ｂ】



【図２】

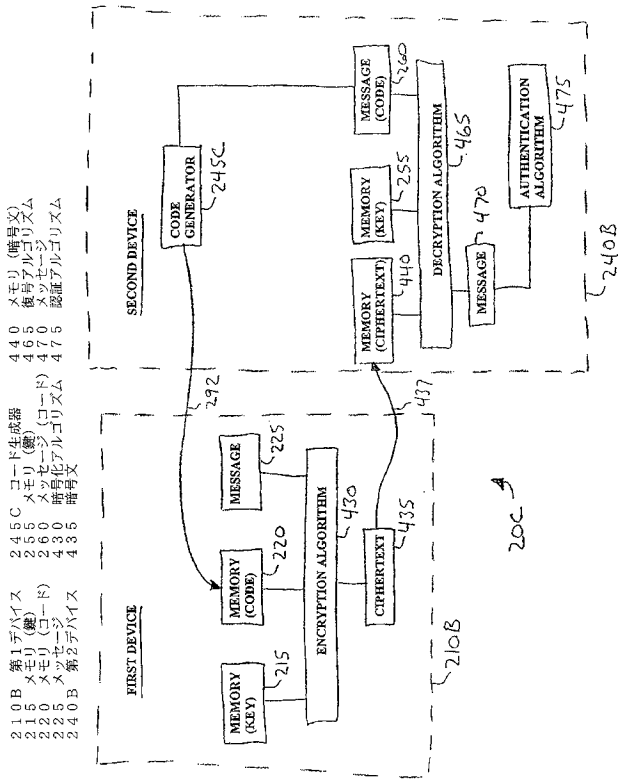


【図３】



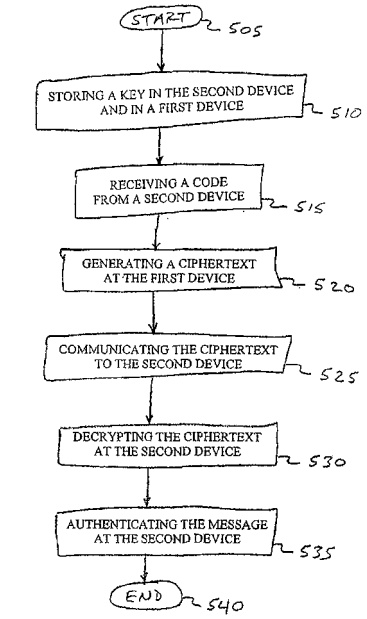
310 鍵を第２デバイスと第１デバイス内に格納する
315 第２デバイスからコードを受信する
320 第１デバイス上で第１ハッシュ値を生成する
325 第１ハッシュ値とメッセージを第２デバイスに通信する
330 第２デバイス上でメッセージと第１ハッシュ値を受信する
335 第２デバイスで第２ハッシュ値を生成する
340 第２デバイス上で第１ハッシュ値と第２ハッシュ値を比較する

【図４】



２１０Ｂ　第１デバイス　　２４５Ｃ　コード生成器　　４４０　メモリ（暗号文）
２１５　メモリ（鍵）　　２５５　メモリ（鍵）　　４６５　復号アルゴリズム
２２０　メモリ（コード）　　２６０　メッセージ（コード）　　４７０　メッセージ
２２５　メッセージ　　４３０　暗号化アルゴリズム　　４７５　認証アルゴリズム
２４０Ｂ　第２デバイス　　４３５　暗号文

【図５】



５１０　鍵を第２デバイスと第１デバイス内に格納する
５１５　第２デバイスからコードを受信する
５２０　第１デバイス上で暗号文を生成する
５２５　暗号文を第２デバイスに通信する
５３０　第２デバイス上で暗号文を復号する
５３５　第２デバイス上でメッセージを認証する

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International Application No
US2005/008521

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L9/00 A61N1/372

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)
IPC 7 H04L A61N

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 practical, search terms used)
EPO-Internal, PAJ, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 2003/074036 A1 (PRUTCHI DAVID ET AL) 17 April 2003 (2003-04-17) paragraph '0047!	1-18
Y	PATENT ABSTRACTS OF JAPAN vol. 2003, no. 05, 12 May 2003 (2003-05-12) & JP 2003 022008 A (SONY CORP), 24 January 2003 (2003-01-24) abstract	1-18
Y	US 2003/114897 A1 (VON ARX JEFFREY A ET AL) 19 June 2003 (2003-06-19) paragraphs '0035!, '0074!; figure 1	19-59
Y	US 5 737 419 A (GANESAN ET AL) 7 April 1998 (1998-04-07) column 5, paragraph 2	19-24, 31-46

-/--

[X] Further documents are listed in the continuation of box C. [X] Patent family members are listed in 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 document but 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
21 September 2005	11 10. 2005
Name and mailing address of the ISA European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Authorized officer Edward, V

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

INTERNATIONAL SEARCH REPORT

'onal Application No
JS2005/008521

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 2003/065919 A1 (ALBERT ROY DAVID ET AL) 3 April 2003 (2003-04-03) paragraph '0065! - paragraph '0072!	25-30, 47-59
A	US 2003/159048 A1 (MATSUMOTO TSUTOMU ET AL) 21 August 2003 (2003-08-21) paragraph '0050!	1-59
A	US 6 028 527 A (SOENEN ET AL) 22 February 2000 (2000-02-22) column 18, paragraph 1 column 21, line 1 - line 5	1-59
A	US 2002/120838 A1 (ABDULKADER BARBIR) 29 August 2002 (2002-08-29) paragraphs '0006!, '0018!	1-59
A	US 5 898 397 A (MURRAY ET AL) 27 April 1999 (1999-04-27) column 3, paragraph 8	1-59

INTERNATIONAL SEARCH REPORT

ernational application No.
PCT/US2005/008521

Box II Observations where certain claims were found unsearchable (Continuation of item 2 of first sheet)

This International Search Report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☐ Claims Nos.:
because they relate to parts of the International Application that do not comply with the prescribed requirements to such an extent that no meaningful International Search can be carried out, specifically:

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box III Observations where unity of invention is lacking (Continuation of item 3 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

see additional sheet

1. ☒ As all required additional search fees were timely paid by the applicant, this International Search Report covers all searchable claims.

2. ☐ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.

3. ☐ As only some of the required additional search fees were timely paid by the applicant, this International Search Report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this International Search Report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest

☐ The additional search fees were accompanied by the applicant's protest.

☐ No protest accompanied the payment of additional search fees.

International Application No. PCT/US2005/008521

FURTHER INFORMATION CONTINUED FROM PCT/ISA/ 210

This International Searching Authority found multiple (groups of) inventions in this international application, as follows:

1. claims: 1-18

A device with communications of high data integrity achieved by hash value comparison.

---

2. claims: 19-24, 31-46

A system with communications of high secrecy and immunity to replay attacks achieved by the use of encryption in combination with a code.

---

3. claims: 25-30, 47-59

A system with communications of high data integrity and immunity to replay attacks achieved by use of hash value comparison in combination with a code.

INTERNATIONAL SEARCH REPORT

nformation on patent family members

onal Application No
US2005/008521

Patent document cited in search report		Publication date	Patent family member(s)		Publication date
US 2003074036	A1	17-04-2003	NONE		
JP 2003022008	A	24-01-2003	NONE		
US 2003114897	A1	19-06-2003	AU	2002364179 A1	09-07-2003
			EP	1458444 A1	22-09-2004
			WO	03053515 A1	03-07-2003
US 5737419	A	07-04-1998	US	5535276 A	09-07-1996
US 2003065919	A1	03-04-2003	EP	1386444 A1	04-02-2004
			JP	2004532468 T	21-10-2004
			WO	02087143 A1	31-10-2002
US 2003159048	A1	21-08-2003	CN	1439982 A	03-09-2003
			JP	2003244139 A	29-08-2003
			SG	108889 A1	28-02-2005
US 6028527	A	22-02-2000	NONE		
US 2002120838	A1	29-08-2002	CA	2330166 A1	29-06-2002
US 5898397	A	27-04-1999	US	5699065 A	16-12-1997

Form PCT/ISA/210 (patent family annex) (January 2004)

フロントページの続き

(81)指定国 AP(BW,GH,GM,KE,LS,MW,MZ,NA,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,IS,IT,LT,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,SM,SY,TJ,TM,TN,TR,TT,TZ,UA,UG,US,UZ,VC,VN,YU,ZA,ZM,ZW

(72)発明者 クイレス, シルビア
アメリカ合衆国・５５４３９・ミネソタ州・エディナ・ウィリアン アベニュ・６５１２
(72)発明者 ヴォン アーックス, ジェフリー・エイ
アメリカ合衆国・５５４０５・ミネソタ州・ミネアポリス・エマーソン アベニュ サウス・２１１５

Ｆターム(参考) 4C117 XA01 XB04 XB11 XB15 XC15 XC21 XD24 XE52 XE59 XE60
XE62 XH02 XH07 XH16 XH27 XJ03 XL03 XL27
5J104 AA08 AA11 LA01 PA07