(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7545490号
(P7545490)

(45)発行日　令和6年9月4日(2024.9.4)

(24)登録日　令和6年8月27日(2024.8.27)

(51)国際特許分類

		FI		
H04L 9/32 (2006.01)		H04L	9/32	200A
G06F 21/64 (2013.01)		H04L	9/32	200E
		G06F	21/64	

請求項の数　10　（全25頁）

(21)出願番号　特願2022-558876(P2022-558876)
(86)(22)出願日　令和3年8月25日(2021.8.25)
(86)国際出願番号　PCT/JP2021/031236
(87)国際公開番号　WO2022/091544
(87)国際公開日　令和4年5月5日(2022.5.5)
審査請求日　令和5年3月16日(2023.3.16)
(31)優先権主張番号　特願2020-180515(P2020-180515)
(32)優先日　令和2年10月28日(2020.10.28)
(33)優先権主張国・地域又は機関
日本国(JP)

(73)特許権者　509186579
日立Ａｓｔｅｍｏ株式会社
茨城県ひたちなか市高場２５２０番地
(74)代理人　110001678
藤央弁理士法人
(72)発明者　三宅 淳司
茨城県ひたちなか市高場２５２０番地
日立Ａｓｔｅｍｏ株式会社内
審査官　辻 勇貴

最終頁に続く

(54)【発明の名称】　情報検証装置、電子制御装置、及び情報検証方法

(57)【特許請求の範囲】

【請求項１】

情報検証装置であって、

情報発信元と当該情報検証装置で知識共有された共通鍵を外部から容易に読み取れない形式で格納しており、

前記情報発信元は、当該情報検証装置が真正性を検証すべきホスト装置宛ての配信情報と、当該情報検証装置宛ての更新情報とを配信できるように構成されており、

前記情報発信元から当該情報検証装置宛ての更新情報は、前記情報発信元と前記情報検証装置とで知識共有された共通鍵を更新するためのデータと、前記共通鍵を更新すべき前記情報検証装置の識別子と、前記共通鍵の更新タイミングの少なくとも三つを含み、

前記情報検証装置は、

前記配信情報が当該情報検証装置宛ての更新情報である場合、復号化された配信情報を出力せず、前記更新情報を用いて当該情報検証装置の内部値を変更し、

前記情報発信元から送信され、同期した時刻及び前記共通鍵によって生成されたワンタイムパスワードと、前記情報発信元から送信され、認証以外の利用価値を有する配信情報と、前記情報発信元から送信され、これらの情報から当該共通鍵を用いて計算されたメッセージ認証コードの少なくとも三つが入力されると、少なくとも前記配信情報の真正性の判定結果を出力し、

前記情報発信元から送信される配信情報の真正性判定結果が真正であり、かつ識別子が自情報検証装置のものと合致する場合、前記更新タイミングに当該検証装置内に格納され

る共通鍵を更新することを特徴とする情報検証装置。
【請求項２】
請求項１記載の情報検証装置であって、
前記情報発信元から送信されたワンタイムパスワードと当該情報検証装置内で計算されたワンタイムパスワードとが一致し、かつ、前記情報発信元から送信されたメッセージ認証コードと当該情報検証装置内で計算されたメッセージ認証コードとが一致する場合、前記配信情報が真正であると判定し、前記配信情報が真正であることを出力することを特徴とする情報検証装置。
【請求項３】
請求項１記載の情報検証装置であって、
前記情報発信元から送信されるワンタイムパスワードは、前記情報発信元から当該情報検証装置へ送信される一連の情報から送信開始時刻に基づいて生成される時刻同期型のワンタイムパスワードであることを特徴とする情報検証装置。
【請求項４】
請求項１記載の情報検証装置であって、
前記情報発信元から送信されるメッセージ認証コードは、前記情報発信元から送信されるワンタイムパスワード及び前記情報発信元から送信される配信情報に基づいて、前記共通鍵を用いて計算されることを特徴とする情報検証装置。
【請求項５】
請求項１記載の情報検証装置であって、
前記配信情報は、前記共通鍵によって暗号化されて、前記情報発信元から送信されるものであって、
前記情報検証装置は、
前記情報発信元から送信された配信情報を復号化して、
前記配信情報の真正性判定結果、及び復号化した配信情報を出力することを特徴とする情報検証装置。
【請求項６】
請求項５記載の情報検証装置であって、
前記ワンタイムパスワードを生成するための共通鍵と、前記メッセージ認証コードを生成するための共通鍵と、前記配信情報を暗号化するための共通鍵とは、同一の鍵である、又は複数の別個の鍵であることを特徴とする情報検証装置。
【請求項７】
請求項１記載の情報検証装置であって、
前記情報発信元から当該情報検証装置宛ての更新情報は、当該情報検証装置の時計を修正するための時刻データを含み、
前記情報検証装置は、前記情報発信元から送信される配信情報の真正性判定結果が真正である場合、前記時刻データを用いて当該情報検証装置の時計を修正することを特徴とする情報検証装置。
【請求項８】
請求項１記載の情報検証装置であって、
複数の前記情報検証装置が情報発信元とで知識共有した同一の共通鍵への変更によって、当該情報検証装置を格納する複数の受信機器群でクラスタを形成し、
前記クラスタを形成する複数の情報検証装置は、前記情報発信元から同一のワンタイムパスワードと同一メッセージ認証コードとを用いて、同一の配信情報を同時に受信することを特徴とする情報検証装置。
【請求項９】
請求項１から８のいずれか一つに記載の情報検証装置を含み、自動車に搭載される電子制御装置。
【請求項１０】
情報検証装置が実行する情報検証方法であって、

前記情報検証装置は、所定の処理を実行する演算装置によって構成され、情報発信元と当該情報検証装置で知識共有された共通鍵を外部から容易に読み取れない形式で格納しており、
前記情報発信元は、当該情報検証装置が真正性を検証すべきホスト装置宛ての配信情報と、当該情報検証装置宛ての更新情報とを配信できるように構成されており、
前記情報発信元から当該情報検証装置宛ての更新情報は、前記情報発信元と前記情報検証装置とで知識共有された共通鍵を更新するためのデータと、前記共通鍵を更新すべき前記情報検証装置の識別子と、前記共通鍵の更新タイミングの少なくとも三つを含み、
前記情報検証方法は、
前記情報検証装置が、前記配信情報が当該情報検証装置宛ての更新情報である場合、復号化された配信情報を出力せず、前記更新情報を用いて当該情報検証装置の内部値を変更し、
前記情報検証装置が、前記情報発信元から送信され、同期した時刻及び前記共通鍵によって生成されたワンタイムパスワードと、前記情報発信元から送信され、認証以外の利用価値を有する配信情報と、前記情報発信元から送信され、これらの情報から当該共通鍵を用いて計算されたメッセージ認証コードの少なくとも三つが入力されると、少なくとも前記配信情報の真正性の判定結果を出力し、
前記情報検証装置が、前記情報発信元から送信される配信情報の真正性判定結果が真正であり、かつ識別子が自情報検証装置のものと合致する場合、前記更新タイミングに当該検証装置内に格納される共通鍵を更新することを特徴とする情報検証方法。

【発明の詳細な説明】
【参照による取り込み】
【０００１】
本出願は、令和２年（２０２０年）１０月２８日に出願された日本出願である特願２０２０－１８０５１５の優先権を主張し、その内容を参照することにより、本出願に取り込む。
【技術分野】
【０００２】
本発明は、情報検証装置に関し、特に通信路を介して送られる情報の改竄検知技術に関する。
【背景技術】
【０００３】
ネットワークを経由して添削される情報が途中で欠落したり、改竄されていないことを検証するため、一般的にデジタル署名が採用されている。
【０００４】
しかしながら、デジタル署名は鍵配信時の盗聴による脆弱性を低減するために公開鍵暗号が使われており、組み込み機器など比較的低能力のＣＰＵ（Ｃｅｎｔｒａｌ Ｐｒｏｃｅｓｓｉｎｇ Ｕｎｉｔ）で構成された計算機には、この署名部を復号化する負担が大きくなっている。
【０００５】
また、公開鍵暗号の形式にＲＳＡ暗号が採用されている場合、量子コンピュータが実現した際には、その素因数分解計算能力によって秘密鍵が容易に発見され、この危殆化により署名部が偽造されるなどの危険性を有している。
【０００６】
本技術分野の背景技術として、特開２００２－２５９３４４号公報（特許文献１）及び特許第６０７８６８６号公報（特許文献２）がある。
特開２００２－２５９３４４号公報（特許文献１）には、ユーザ端末に接続するユーザ認証サーバと、携帯電話とからなるワンタイムパスワード認証システムであって、携帯電話は、（１）秘密情報を格納する携帯電話側秘密情報格納部と、（２）ユーザＩＤと、現在時刻情報と、携帯電話側秘密情報格納部に格納する秘密情報とを用いて、ハッシュ値を

求め、求めたハッシュ値を文字列に変換することによりワンタイムパスワードを生成する携帯電話側ハッシュ生成部と、（３）生成したワンタイムパスワードを表示するワンタイムパスワード表示部とを有し、ユーザ認証サーバは、（４）ユーザＩＤとワンタイムパスワードとを、ユーザ端末から受信するユーザＩＤ／ワンタイムパスワード受信部と、（５）携帯電話側秘密情報格納部で格納する秘密情報と同一の秘密情報を格納するサーバ側秘密情報格納部と、（６）受信したユーザＩＤと、現在時刻情報と、サーバ側秘密情報格納部に格納する秘密情報とを用いて、ハッシュ値を求め、求めたハッシュ値を文字列に変換することによりワンタイムパスワードを生成するサーバ側ハッシュ生成部と、（７）サーバ側ハッシュ生成部で生成したワンタイムパスワードと、ユーザＩＤ／ワンタイムパスワード受信部で受信したワンタイムパスワードとを比較し、一致した場合に認証結果を成功とするワンタイムパスワード検証部と、（８）認証結果を、ユーザ端末に送信する認証結果送信部とを有することを特徴とするワンタイムパスワード認証システムが記載されている（請求項１参照）。

【０００７】

また、特許第６０７８６８６号公報（特許文献２）には、車両の動作を制御する車載制御装置を維持管理するために用いる操作端末を認証する認証システムであって、前記認証システムは、通信回線を介して前記操作端末と接続され前記操作端末を操作する操作者を認証する認証装置、および前記車載制御装置を備え、前記車載制御装置は、前記操作端末が前記車載制御装置を維持管理する操作を実施することを許可するか否かを判定するように構成されており、前記認証装置と前記車載制御装置は、互いに同期して変化する変動符号を生成する変動符号生成源、前記認証装置と前記車載制御装置との間で共有する前記車両に固有の共通鍵を格納する記憶部、前記変動符号と前記共通鍵を用いて認証符号を生成する認証符号生成器、をそれぞれ備え、前記認証装置は、前記操作端末から認証要求を受け取ると前記操作者を認証し、前記操作者の認証が成功すると、前記操作端末から前記共通鍵を特定する情報を取得し、前記変動符号と前記共通鍵を用いて前記認証符号を生成して前記操作端末へ送信し、前記操作端末は、前記認証装置から受け取った前記認証符号を前記車載制御装置へ送信し、前記車載制御装置は、前記変動符号と前記共通鍵を用いて前記認証符号を生成し、生成した前記認証符号と前記操作端末から受け取った前記認証符号とが一致する場合は、前記操作端末が前記車載制御装置を維持管理する操作を実施することを許可することを特徴とする認証システムが記載されている（請求項１参照）。

【０００８】

また、Specification of Module Secure Onboard Communication（非特許文献１）には、ＭＡＣ認証でやり取りする情報の改竄検知を行い、配信情報に含ませたＦＶカウンターで再生攻撃を検知することが記載されている。

【先行技術文献】

【特許文献】

【０００９】

【文献】特開２００２－２５９３４４号公報

【文献】特許第６０７８６８６号公報

【非特許文献】

【００１０】

【文献】"Specification of Module Secure Onboard Communication"、[online]、AUTOSAR、https://www.autosar.org/fileadmin/user_upload/standards/classic/4-2/AUTOSAR_SWS_SecureOnboardCommunication.pdf

【発明の概要】

【発明が解決しようとする課題】

【００１１】

デジタル署名の署名部を処理するための公開鍵暗号等の非対称鍵暗号は計算量が大きく、大きな処理能力が必要とされるので、他の方式に変更して処理負荷を軽減することが求められている。

【００１２】
例えば、ＲＳＡなどの公開鍵暗号では巨大な冪剰余の算術計算が必要である。一方、ＭＡＣ認証に用いられるハッシュ関数の計算は、論理演算とシフト演算で実装可能であり、組込み用途の車載ＥＣＵ（Ｅｌｅｃｔｒｉｃ Ｃｏｎｔｒｏｌ Ｕｎｉｔ）やＩｏＴ（Ｉｎｔｅｒｎｅｔ ｏｆ Ｔｈｉｎｇｓ）機器に使用される低能力のＣＰＵでも簡単に取り扱える。

【００１３】
特許文献１及び特許文献２では、ＭＡＣ認証を用いて時刻同期型ワンタイムパスワードを生成しているが、認証の元となる情報が時刻と機器の識別情報以外に利用価値のある情報を含んでいない。すなわち、認証情報だけのやり取りに限定される発明であり、配信情報など認証以外のＭＡＣ認証技術には対応していない。

【００１４】
本発明は、認証以外に利用価値のある配信情報にＭＡＣ認証を使用し、同時に再生攻撃も検知可能な方法を提案する、という二つの課題を掲げてこの解決を計っている。ここで再生攻撃とは、通信路の盗聴者が通信路に流れる過去の情報を記録し、後に、記録した情報やシーケンスをそのまま攻撃対象に送信して攻撃対象を騙そうとする方法である。デジタル署名では署名部が時間情報を含まないため、再生攻撃を検出できない。

【００１５】
非特許文献１（Ｓｐｅｃｉｆｉｃａｔｉｏｎ ｏｆ Ｍｏｄｕｌｅ Ｓｅｃｕｒｅ Ｏｎｂｏａｒｄ Ｃｏｍｍｕｎｉｃａｔｉｏｎ）では、ＭＡＣ認証でやり取りする情報の改竄検知を行い、配信情報に含まれるカウンターであるＦＶ（Ｆｒｅｓｈｎｅｓｓ Ｖａｌｕｅ）を用いて再生攻撃を検知している。

【００１６】
ＦＶは、送信元が情報を送出する都度に値が更新されるカウンターであり、受信側では同一のＦＶ値の情報を受理しないことによって再生攻撃を排除している。

【００１７】
しかしながら、非特許文献１ではＭＡＣ認証を行う共通鍵を予め車載ＬＡＮを通じて配信するので、この共通鍵が盗聴されるリスクがある。従って、Ｏｎｂｏａｒｄ Ｃｏｍｍｕｎｉｃａｔｉｏｎ、すなわち、車載ＬＡＮなどの限定された範囲における通信では実用性があるが、インターネットを経由して鍵を配信できるほどセキュアではない。また、送信側と受信側の両方でＦＶ値を管理すると、配信先が増えた場合にＦＶ値の管理が煩雑になる。

【００１８】
本発明では、前述した鍵配信時の漏洩問題を解決して、インターネットを経由して送られる配信情報の改竄を検知することを目的とする。さらに、デジタル署名では不可能な再生攻撃を検知し、しかも配信先が増えた場合でも管理が煩雑にならない方法を提案することを目的とする。

【課題を解決するための手段】

【００１９】
本願において開示される発明の代表的な一例を示せば以下の通りである。すなわち、情報検証装置であって、情報発信元と当該情報検証装置で知識共有された共通鍵を外部から容易に読み取れない形式で格納しており、前記情報発信元は、当該情報検証装置が真正性を検証すべきホスト装置宛ての配信情報と、当該情報検証装置宛ての更新情報とを配信できるように構成されており、前記情報発信元から当該情報検証装置宛ての更新情報は、前記情報発信元と前記情報検証装置とで知識共有された共通鍵を更新するためのデータと、前記共通鍵を更新すべき前記情報検証装置の識別子と、前記共通鍵の更新タイミングの少なくとも三つを含み、前記情報検証装置は、前記配信情報が当該情報検証装置宛ての更新情報である場合、復号化された配信情報を出力せず、前記更新情報を用いて当該情報検証装置の内部値を変更し、前記情報発信元から送信され、同期した時刻及び前記共通鍵によって生成されたワンタイムパスワードと、前記情報発信元から送信され、認証以外の利用

価値を有する配信情報と、前記情報発信元から送信され、これらの情報から当該共通鍵を用いて計算されたメッセージ認証コードの少なくとも三つが入力されると、少なくとも前記配信情報の真正性の判定結果を出力し、前記情報発信元から送信される配信情報の真正性判定結果が真正であり、かつ識別子が自情報検証装置のものと合致する場合、前記更新タイミングに当該検証装置内に格納される共通鍵を更新することを特徴とする。

【発明の効果】

【００２０】

本発明の一態様によれば、配信情報の改竄及び再生攻撃を検知できる。前述した以外の課題、構成及び効果は、以下の実施例の説明によって明らかにされる。

【図面の簡単な説明】

【００２１】

【図１】前提となるＯＴＰ照合チップのユースケースを示す図である。

【図２】前提となるＯＴＰ照合チップ、及びその施錠装置内に格納される形態を示すブロック図である。

【図３】実施例１に係る拡張されたＯＴＰ照合チップの詳細を示すブロック図である。

【図４】実施例１の方式と従来のデジタル署名と比較して示す図である。

【図５】実施例１の配信情報検証処理を示すフローチャートである。

【図６】実施例１の情報転送におけるＯＴＰの時刻の基準を示すタイミング図である。

【図７】実施例１でＭＡＣ値の範囲にＯＴＰを含まない場合の情報送出プロセスと中間者攻撃を示すタイミング図である。

【図８】実施例２に係る拡張されたＯＴＰ照合チップの詳細を示すブロック図である。

【図９】実施例２の配信情報検証処理を示すフローチャートである。

【図１０】実施例３に係る拡張されたＯＴＰ照合チップの詳細を示すブロック図である。

【図１１】実施例３の配信情報検証処理を示すフローチャートである。

【図１２】実施例３の定時割込み処理のフローチャートである。

【図１３】実施例３の受信クラスタを動的に拡大や縮小する受信機器群を示す図である。

【発明を実施するための形態】

【００２２】

以下、本発明の実施形態について、図面を参照して説明する。なお、以下に説明する実施形態は請求の範囲に係る発明を限定するものではなく、また実施形態の中で説明されている諸要素及びその組み合わせの全てが発明の解決手段として必須であるとは限らない。

【００２３】

なお、実施例を説明する図において、同一の機能を有する箇所には同一の符号を付し、その繰り返しの説明は省略する。

【００２４】

また、以下の説明では、情報の一例として「ｘｘｘレジスタ」、「ｘｘｘメモリ」という情報記憶域に関する表現を用いる場合があるが、記憶域の特性に関する属性、すなわちロケーションの指定方法、アクセス速度に関する優劣、電源操作もしくはリフレッシュ動作に対する揮発性か不揮発性か、もしくは読み書き可か読み出し専用かなどの属性をその文言により分類するものでは無い。加えて、情報のデータ構造はどのようなものでもよい。すなわち、情報が記憶域の構造に依存しないことを示すために、「ｘｘｘレジスタ内容」を「ｘｘｘメモリ内容」と言うことができる。さらに、「ｘｘｘメモリ内容」を単に「ｘｘｘの内容」と言うこともある。そして、以下の説明において、各情報の構成は一例であり、情報を分割して保持したり、結合して保持したりしても良い。

【００２５】

＜前提となる構成＞

本願に先行する形でＯＴＰ（Ｏｎｅ　Ｔｉｍｅ　Ｐａｓｓｗｏｒｄ:ワンタイムパスワード）照合チップの内容を以下に簡単に説明する。

【００２６】

図１は、前提となるＯＴＰ照合チップ１１０のユースケースを示す図である。

【００２７】
施錠装置１０３の内部に実装されたＯＴＰ照合チップ１１０は、ユーザ１０２を認証するために、所定の処理を実行する演算部と演算部がアクセス可能な記憶部とを有するデバイスである。演算部は、所定の手順に従って演算処理を実行するものであり、プロセッサが所定のプログラムを実行するものでも、ハードウェア（ＦＰＧＡ、ＡＳＩＣなど）でもよい。施錠装置１０３は、ＯＴＰ照合チップ１１０の認証結果によって施錠装置１０３の施錠・開錠動作を引き起こす機能を有する。
【００２８】
ユーザ１０２は、厳格なユーザ認証１０７を経てユーザ認証＆ＯＴＰ発行サーバ１００にログオンし、権限が認められるとユーザ認証＆ＯＴＰ発行サーバ１００から時刻同期型ＯＴＰ１０８が発行される。
【００２９】
ユーザ１０２は、発行されたＯＴＰ１０８を、所定時間内に施錠装置１０３に開示する（発行されたＯＴＰ１０８と施錠装置１０３に開示されるＯＴＰ１０９は、符号が異なるのみで同じものである）。施錠装置１０３は、内部のＯＴＰ照合チップ１１０にＯＴＰ１０９の真正性の判定を依頼し、判定によって認証に成功すれば（真正性が認められれば）所定の動作を行う。
【００３０】
ＯＴＰ照合チップ１１０は、製造段階でユーザ認証＆ＯＴＰ発行サーバ１００とパスフレーズ１０６という共通鍵を共有し、情報が漏洩することなく、製品の製造段階から稼働段階まで共通鍵を秘匿できる。鍵情報を通信路に流さない極めて物理的な鍵配信と言える。
【００３１】
ＯＴＰ照合チップ１１０は、タンパー性に優れており、外部より物理的に中の共通鍵を探ることは不可能であり、ＯＴＰ照合チップ内部のファームウェアのみが共通鍵情報にアクセスできる構造となっている。従って、ＯＴＰ照合チップ１１０は一種のＨＳＭ（Ｈａｒｄｗａｒｅ　Ｓｅｃｕｒｉｔｙ　Ｍｏｄｕｌｅ）とみなすことができる。
【００３２】
サーバ１００の時計１０４とＯＴＰ照合チップ１１０内の時計１０５は同期しており、パスフレーズ１０６という共通鍵はサーバ１００とＯＴＰ照合チップ１１０で共有されているので、サーバ１００の時計１０４の時刻とパスフレーズ１０６を用いてハッシュ関数（後述）によって計算した値（ＯＴＰ１０８、１０９）と、ＯＴＰ照合チップ１１０内の時計１０５とパスフレーズ１０６を用いて同一のハッシュ関数によって計算した比較用の値（図示せず）の一致によって認証が成功する。
【００３３】
ここで、本実施例のために、ユーザ認証＆ＯＴＰ発行サーバ１００を情報配信サーバ（図１３の１３００）に拡張して考える。さらに、ユーザ１０２の中間関与を排除し、情報配信サーバ１３００自体がオンデマンドで配信情報を加えて拡張したＯＴＰ（図４の４２２）を直に施錠装置１０３、さらにはＯＴＰ照合チップ１１０まで送信する場合を考える。
【００３４】
この時、ＯＴＰ照合チップ１１０内部のパスフレーズ１０６という情報配信サーバ１３００と共有した共通鍵をＭＡＣ認証に流用でき、ＭＡＣ認証を用いて配信情報の改竄を検知できる。
【００３５】
また、前述のように、この共通鍵はＯＴＰ照合チップ１１０内に隠蔽された鍵情報の物理配布に相当するので、非特許文献１のような通信媒体上の鍵配信に基づく盗聴リスクがなく、またデジタル署名のように公開鍵暗号を使わなくてもよい。
【００３６】
さらに、配信情報の先頭に、元々の機能である時刻同期型ワンタイムパスワードをヘッダとして付加することによって、グローバル時間と関連付けて該当時刻に発信された情報である（記録された後に再生された情報ではない）ことを検証でき、再生攻撃を検知でき

る。
【００３７】
図２は、前提となるＯＴＰ照合チップ１１０、及びその施錠装置１０３内に格納される形態を示すブロック図である。
【００３８】
施錠装置１０３は、ホストＣＰＵ２１０及びＯＴＰ照合チップ１１０から構成される。ホストＣＰＵ２１０とＯＴＰ照合チップ１１０とは通信可能に接続されている。
【００３９】
従来、セキュリティに関する演算は、本体チップ（前述のホストＣＰＵ２１０）と別体のセキュリティチップ（前述のＯＴＰ照合チップ１１０）に集約されることがある。これはセキュリティチップに格納された秘匿すべき秘密鍵（公開鍵暗号方式で称するところの情報）、又は共通鍵（共通鍵暗号方式で称するところの情報）などの情報漏洩を防ぐためである。セキュリティチップが、本体チップと別体になり、ハードウェア的に完全に独立したモジュールをＨＳＭ（Ｈａｒｄｗａｒｅ　Ｓｅｃｕｒｉｔｙ　Ｍｏｄｕｌｅ）と呼ぶことは前述の通りである。
【００４０】
セキュリティチップと本体チップとを別体とすることによって、セキュリティチップのメモリ空間を本体チップから完全に観測不能にでき、秘匿情報の漏洩を防止できる。また、耐タンパー性の観点からも封止開放で情報が消えるシリコンプロセス（フローティング・キャパシタンス）などの秘匿化方法をセキュリティチップのみに採用できるようになる。
【００４１】
ホストＣＰＵ２１０とＯＴＰ照合チップ１１０を別体にすることによって、前述の通りＯＴＰ照合チップ１１０そのものにより耐タンパー性を確保でき、ホストＣＰＵ２１０を通じてＯＴＰ照合チップ１１０内部に秘匿され保護された共通鍵（例えば、図１のユーザ認証＆ＯＴＰ発行サーバ１００と知識共有したパスフレーズ１０６）の情報を読み出されることを防止できる。
【００４２】
ワンタイムパスワード１０９は、ホストＣＰＵ２１０を介し、通信路２１１を経由してＯＴＰ照合チップ１１０に送られる。検証結果は、ＯＴＰ照合チップ１１０より通信路２１２を経由してホストＣＰＵ２１０に送り返される、この結果によって、ホストＣＰＵ２１０は次に実行する処理を決定する。
【００４３】
ホストＣＰＵ２１０からＯＴＰ照合チップ１１０への通信路２１１では、ホストＣＰＵ２１０からＯＴＰ照合チップ１１０に与えられるコマンド、ＯＴＰ照合チップ１１０内の時計の時刻合わせデータ、及び、外部からの被認証ＯＴＰデータが伝送される。
【００４４】
また、ＯＴＰ照合チップ１１０からホストＣＰＵ２１０への通信路２１２では、ＯＴＰ照合チップ１１０からホストＣＰＵ２１０に返送される認証結果、及び、種々のステータス報告値が伝送される。
【００４５】
ＯＴＰ照合チップ１１０とホストＣＰＵ２１０との間の通信路２１１及び２１２は、シリアル伝送でもよいし、バスのようなパラレル伝送でもよい。また、シリアルやパラレル以外の高度なプロトコルによって制御されたネットワークでもよい。通信路２１１及び２１２は、ＯＴＰ照合チップ１１０内部のＩ／Ｏ部２０７によって制御される。
【００４６】
ＯＴＰ照合チップ１１０は、制御部２００、時計部２０１、パスフレーズ保管庫２０２、比較用ＯＴＰ生成部２０３、受信ＯＴＰを一時的に記憶する受信ＯＴＰバッファ２０４、ＯＴＰ比較器２０５、出力用の判定結果レジスタ２０６、及び前述したＩ／Ｏ部２０７で構成される。
【００４７】

制御部２００は、ＯＴＰ照合チップ１１０の全体の動作を制御する部分で、ＰＬＣ（Ｐｒｏｇｒａｍｍａｂｌｅ　Ｌｏｇｉｃ　Ｃｏｎｔｒｏｌｌｅｒ）によって実装されてもよいし、一般のＣＰＵによるソフトウェア又はファームウェアで実装されてもよい。

【００４８】

時計部２０１は、初回動作時にホストＣＰＵ２１０から通信路２１１を経由して時刻初期値を設定された後、自律的に時を刻む時計を内蔵している。施錠装置１０３の全体の電源供給が途切れても、時計部２０１のみが稼働し続けるようなバックアップ電源が供給されている。

【００４９】

バックアップ電源が断たれて時計が停止した場合や、ＯＴＰ照合チップ１１０のリセット操作によって時計が初期化された場合、その旨のステータスを通信路２１２を経由してホストＣＰＵ２１０に報告して、時刻値の再設定を依頼する。

【００５０】

パスフレーズ保管庫２０２は、ユーザ認証＆ＯＴＰ発行サーバ１００と知識共有したパスフレーズ１０６を保管する部分で、高度の耐タンパー性が確保されており、保管された内容をチップ外部からの破壊読出しに対しても保護する（破壊読み出しに対する保護によって、エミュレーションチップの作成を阻止できる）。もちろん、ホストＣＰＵ２１０は、パスフレーズ保管庫２０２に保管された内容を読み出せない。

【００５１】

ＯＴＰ照合チップ１１０の動作を簡単に説明すると、外部から送られたＯＴＰ１０９は、ホストＣＰＵ２１０を経由してＯＴＰ照合チップ１１０の受信ＯＴＰバッファ２０４に格納される。ＯＴＰ１０９と共に、ホストＣＰＵ２１０よりＯＴＰ照合依頼が指令される。

【００５２】

ＯＴＰ照合チップ１１０の比較用ＯＴＰ生成部２０３は、ユーザ認証＆ＯＴＰ発行サーバ１００と同期した時計部２０１より読み出した現在時刻と、パスフレーズ保管庫２０２より読み出したパスフレーズ１０６から比較用ＯＴＰ値を算出する。

【００５３】

ＯＴＰ比較器２０５は、比較用ＯＴＰ生成部２０３が算出した値と、受信ＯＴＰバッファ２０４に格納された値を比較し、両者が一致すれば認証成功と判定し、両者が不一致であれば認証失敗と判定する。判定結果は、判定結果レジスタ２０６に送られ、通信路２１２を経由してホストＣＰＵ２１０に通知される。ＯＴＰ照合チップ１１０から出力される判定結果は、単に０又は１のフラグなどの固定値ではなく、予めホストＣＰＵ２１０との間で取り決めた形式で出力することが想定されている。これは偽のＯＴＰ照合チップに付け替える改造や、通信路２１２に偽情報を注入される攻撃から認証システム（ホストＣＰＵ２１０とＯＴＰ照合チップ１１０との連係動作）を保護するためである。

【００５４】

＜実施例１＞

図３は、実施例１に係る拡張されたＯＴＰ照合チップ３００の詳細を示すブロック図である。

【００５５】

ちなみに、ＯＴＰ照合チップ３００を格納した本体装置３０７は、ＯＴＰ認証の機能のみを有する施錠装置１０３とは異なり、例えば車載用途の場合、車載ＬＡＮの中核を成し、各ＥＣＵ間の中継（データ中継、周期変換、プロトコル変換、データ組み替え等）を行うＣＧＷ（Ｃｅｎｔｒａｌ　Ｇａｔｅｗａｙ：セントラルゲートウェイ）として動作する装置を想定している。なお、拡張されたＯＴＰ照合チップ３００において、前述したＯＴＰ照合チップ１１０と同じ機能の構成要素には同じ符号を付し、それらの説明は省略する。

【００５６】

本体装置３０７に入力される配信情報３１０は、該ＣＧＷ直下に車載ＬＡＮ（図示せず）を通じて接続され、ＯＴＡ（Ｏｖｅｒ－ｔｈｅ－Ａｉｒ）により更新されるＥＣＵ（図示せず）のデータ（更新用制御ソフトウェア、更新パッチ、制御パラメータ、制御ルール

）などを想定している。
【００５７】
ＥＣＵは、制御系、安全系、ボディ系、情報系などの系統別の専用ネットワークに分けて複数が接続されている。ＣＧＷは、これらの専用ネットワークで構成されるスター型ネットワークのハブとなる装置であり、無線（ＬＴＥ（Ｌｏｎｇ Ｔｅｒｍ Ｅｖｏｌｕｔｉｏｎ）、Ｗｉ－Ｆｉ（Ｗｉｒｅｌｅｓｓ Ｆｉｄｅｌｉｔｙ）、スマートフォン）や有線（故障診断ツール、充電ターミナル）などの通信手段によって車外と通信するインタフェースとしても機能する。
【００５８】
ＣＧＷは、本発明を利用してＯＴＡ送信元たる外部アクティビティを厳格に認証し、送信された配信情報の改竄を厳格に検査し、各ＥＣＵに車載ＬＡＮを通じてデータを配布する形態とする。
【００５９】
図３に示す実施例では、受信した配信情報を一時的に記憶する配信情報ＤＩ（Ｄｅｌｉｖｅｒｙ Ｉｎｆｏｒｍａｔｉｏｎ）バッファ３０１、受信したＭＡＣ値（メッセージ認証コード：Ｍｅｓｓａｇｅ Ａｕｔｈｅｎｔｉｃａｔｉｏｎ Ｃｏｄｅ）を一時的に記憶する受信ＭＡＣ値バッファ３０２、ＭＡＣ値にＯＴＰを含めるかを選択するための切り替えスイッチ３０３（通常は「閉」）、比較用ＭＡＣ値生成部３０４、ＭＡＣ値比較器３０５、ＯＴＰが一致しかつＭＡＣ値が一致する場合のみ判定結果レジスタ２０６内容をＯＫとするＡＮＤ論理３０６が、図２に示す例に追加されている。
【００６０】
図４は、実施例１の情報配信プログラムの形態及びチェックコード（署名又はＭＡＣ値）の生成原理と検証原理を、従来のデジタル署名と比較して示す図である。
【００６１】
表の縦列では左から順に送り出し側の情報配信サーバにおける処理４００、伝送路（有線、無線）４０１での情報形態、受信端末（車、ＩｏＴ）での受信検証処理４０２を示す。表の横行は、上が従来のデジタル署名４１０、下が本実施例の方法４２０を示す。
【００６２】
上部４１０に示す従来のデジタル署名の動作から説明する。欄４１１は、サーバ側からデジタル署名を付して送信する情報の生成手順を示す。配信情報を一方向性ハッシュ関数に入力し、ハッシュ値（メッセージダイジェスト）を計算する。ここで、一方向性ハッシュ関数（以下、名称を略してハッシュ関数、数学関数としてｈａｓｈ（）と記載する）とは、任意の長さのデータを固定長（１２８～５１２ビット程度）のデータに圧縮する、以下の（１）～（３）の性質を有する暗号学的関数である。
（１）一方向性：出力値から入力値の発見が困難である。すなわち、あるハッシュ値ｈが与えられたとき、ｈ＝ｈａｓｈ（ｍ）を満たす任意のｍを求める逆演算が困難でなければならない。
（２）第２原像計算困難性：ある入力値と同じハッシュ値が得られる別の入力を求めることが困難である。すなわち、ｍが与えられたとき、ｈａｓｈ（ｍ）＝ｈａｓｈ（ｍ’）となるようなｍ’（ただし、ｍ≠ｍ’）を求めるのが困難でなければならない。
（３）衝突困難性：同じ出力値を生成する二つの入力値の発見が困難である。すなわち、ｈａｓｈ（ｍ）＝ｈａｓｈ（ｍ’）を満たすｍとｍ’（ただし、ｍ≠ｍ’）を求めることが困難でなければならない。
【００６３】
すなわち、一方向性ハッシュ関数とは、入力が与えられれば、確かな再現性をもって簡単に出力を計算できるが、出力から入力の逆演算が困難な（膨大な時間コストが必要である）暗号学的関数である。
【００６４】
また、如何なる大きさのデータも固定長の出力となるハッシュ値に圧縮して纏めることができるので、このハッシュ値はメッセージダイジェストとも呼称される。サーバは、こ

のように計算されたハッシュ値（メッセージダイジェスト）を、サーバ秘密鍵による公開鍵暗号化を施し署名を作成する。

【００６５】

欄４１２は、デジタル署名における配信情報の伝送路で送信されるデータを示す。すなわち、伝送路では配信情報と署名とがペアになって伝送される。署名には時刻成分が含まれていないので、再生攻撃に対して無力となる。すなわち、この配信情報と署名とのペアを盗聴すれば、盗聴によって記録された配信情報と署名とのペアを何回でも受信端末に送信できる。受信端末は、正しい署名が付されているので、配信情報を正当なものとして受信する。

【００６６】

欄４１３は、受信端末側の処理を示す。受信端末は、送信された署名を、サーバ公開鍵を用いて公開鍵復号化をして、復号化した送信配信情報のハッシュ値を求める。また、受信端末は同一のハッシュ関数を用いて独自に受信配信情報からハッシュ値を求める。これら二つのハッシュ値を比較し、ハッシュ値が一致すれば送信側と受信側とで情報が正しく送られているのでＯＫと判定し、ハッシュ値が不一致であれば情報の欠落や改竄が発生しているのでＮＧと判定する。

【００６７】

下部４２０に、本実施例のサーバ、及び受信端末の動作を示す。欄４２１は情報配信サーバ側の動作を示す。受信側と共有した共通鍵であるパスフレーズと時刻情報からＯＴＰ（ワンタイムパスワード）を生成する。従って、このＯＴＰは「時刻情報のＭＡＣ認証値」であると言える。続いて、ＯＴＰと配信情報とパスフレーズからハッシュ関数を用いて全体のＭＡＣ値を計算する。

【００６８】

欄４２２は、本実施例における配信情報の伝送路で送信されるデータを示す。すなわち、伝送路では、ＯＴＰ、配信情報、及びＭＡＣ値の三つの値が組で伝送される。従来のデジタル署名と異なり、ＯＴＰに時刻情報が含まれているので、再生攻撃が検出可能となる利点がある。

【００６９】

欄４２３は、受信端末側の処理を示す。まず、受信端末は、サーバの時計と同期した時計から得た時刻とパスフレーズからＯＴＰを計算する。計算されたＯＴＰと受信したＯＴＰが異なれば、サーバとパスフレーズが異なり、配信情報の宛先がこの受信端末ではないか、又は再生攻撃を受けている可能性があるので、配信情報を受信しないで破棄する。以上の手順４２４は、本実施例の前提となる構成であるＯＴＰ照合チップ１１０の機能である。

【００７０】

一方、計算されたＯＴＰと受信したＯＴＰが一致していれば、このＯＴＰと配信情報とパスフレーズからハッシュ関数を用いてＭＡＣ値を計算する。この計算したＭＡＣ値と受信したＭＡＣ値が一致すれば、情報が正しく伝送されているのでＯＫと判定し、計算したＭＡＣ値と受信したＭＡＣ値が一致しなければ、情報の欠落や改竄が発生しているのでＮＧと判定する。ＭＡＣ値の生成に用いるハッシュ関数は、手順４２４に内包するハッシュ関数を使用できる。このように現有する計算資源を流用でき、コストの上昇を抑制できる。

【００７１】

以上に述べたように、本実施例の方法４２０では、基本的な能力として再生攻撃を常に検知できる。また、受信端末側での計算量を両手法で比較し、計算量の大小を不等号で表現すると、一般的に、

公開鍵暗号復号化処理＞＞ハッシュ関数処理

となるので、

デジタル署名（公開鍵暗号復号化１回＋ハッシュ関数１回）＞＞本実施例（ハッシュ関数２回）

と本実施例の方法４２０の方が圧倒的に小さくなる。

【００７２】
従って、計算能力が低い廉価なＣＰＵでも実行でき、本実施例のようにＯＴＰ照合チップ１１０でもＭＡＣ認証値の演算と照合処理を追加実装できる。また、それによってＯＴＰ照合チップ１１０を拡張するための製造コストの上昇も抑制できる。
【００７３】
図３のホストＣＰＵ２１０は、図４の伝送路４０１上の値の組み４２２、すなわちＯＴＰと配信情報３１０とＭＡＣ値を受信すると、通信路２１１を経由して、拡張されたＯＴＰ照合チップ３００内部の受信ＯＴＰバッファ２０４、配信情報ＤＩバッファ３０１、受信ＭＡＣ値バッファ３０２に、それぞれの値を格納する。その後、ホストＣＰＵ２１０は、同様に通信路２１１を経由して拡張されたＯＴＰ照合チップ３００に対して配信情報検証依頼（図示せず）を発行する。
【００７４】
図５は、実施例１の配信情報検証処理Ｓ５００を示すフローチャートである。
【００７５】
判定Ｓ５０１では、ＯＴＰ照合チップ３００は、ホストＣＰＵ２１０より配信情報の検証依頼を受けたかを判定し、配信情報の検証依頼を受けていればステップＳ５０２に進み、配信情報の検証依頼を受けていなければステップＳ５０９に進んで、配信情報検証処理を終了する。
【００７６】
ステップＳ５０２では、ＯＴＰ照合チップ３００は、内蔵時計デバイスを参照する。内蔵時計デバイスの特定レジスタＲｅｇ（ｔｉｍｅ）にはＯＴＰを受信し始めた時刻がキャプチャされており、その時刻を変数ｔｉｍｅにセットする。この時刻キャプチャ機能の必要性については、図６で後述する。
【００７７】
ステップＳ５０３では、ＯＴＰ照合チップ３００は、比較用のＯＴＰを計算する。図中記号∪はデータの結合を表し、時刻情報ｔｉｍｅとパスフレーズをデータストリーム的に結合することを意味する。時刻情報のフォーマット、及びパスフレーズとの結合方式（順番など）は情報配信サーバ側と統一される。
【００７８】
判定ステップＳ５０４では、ＯＴＰ照合チップ３００は、受信したＯＴＰと内部計算したＯＴＰとを比較する。比較の結果、ＯＴＰが一致すれば次のステップＳ５０５に進み、ＯＴＰが一致しなければステップＳ５０８で判定結果ＮＧとして、ステップＳ５０９に進んで、配信情報検証処理を終了する。
【００７９】
ステップＳ５０５では、ＯＴＰ照合チップ３００は、受信情報のＭＡＣ値を独自に計算する。ステップＳ５０３と同様に図中記号∪はデータの結合を表している。受信したＯＴＰ内容（ＯＴＰ　Ｂｕｆｆ．）、受信した配信情報内容（Ｄ．Ｉ．Ｂｕｆｆ．）、パスフレーズの三つのデータストリーム的な結合方式（順番など）が情報配信サーバ側と統一されることはステップＳ５０３と同じである（ここでは、記憶域の名称を括弧（）で囲みその記憶域の内容を表している。以下同じ。）。
【００８０】
判定ステップＳ５０６では、ＯＴＰ照合チップ３００は、受信したＭＡＣ値と独自に計算されたＭＡＣ値とを比較する。比較の結果、ＭＡＣ値が一致すれば次のステップＳ５０７で判定結果ＯＫとして、ステップＳ５０９に進んで、配信情報検証処理を終了する。一方、ＭＡＣ値が一致しなければステップＳ５０８で判定結果ＮＧとして、ステップＳ５０９に進んで、配信情報検証処理を終了する。
【００８１】
ステップＳ５０７における判定結果ＯＫの情報及びステップＳ５０８における判定結果ＮＧの情報は、図３の判定結果レジスタ２０６に送られ、通信路２１２を経由してホストＣＰＵ２１０に通知される。

【００８２】
ホストＣＰＵ２１０が発行する配信情報検証依頼（図示せず）は、受信ＯＴＰバッファ２０４、配信情報ＤＩバッファ３０１及び受信ＭＡＣ値バッファ３０２のセットの送信が完了した後に発行するとよいが、スループットを向上させるために、受信ＯＴＰのデータ先頭がＯＴＰ照合チップ３００に到来した直後に配信情報検証依頼を発行してもよい。その場合、ＯＴＰの比較（Ｓ５０４）の直前に受信ＯＴＰバッファ２０４の転送完了までの待機処理を追加し、比較用ＭＡＣ値計算（Ｓ５０５）の直前に配信情報ＤＩバッファ３０１の転送完了までの待機処理を追加し、ＭＡＣ値比較（Ｓ５０６）の直前に受信ＭＡＣ値バッファ３０２の転送完了までの待機処理を追加するとよい。
【００８３】
図６は、サーバから受信端末への情報転送におけるＯＴＰの時刻の基準を示すタイミング図である。
【００８４】
結論から言えば、一連の情報はＯＴＰを先頭にして通信路６１０に送出され、ＯＴＰが送出され始める先頭時刻をＯＴＰ生成の基準時刻とする。これは、一連の情報の全体の伝送時間が長い場合、ＯＴＰ値の切り替わり時間の超過を避けるためである。
【００８５】
図６では、上からサーバ内処理６００、通信路６１０、ＯＴＰチップ内処理６２０を並行する時間座標で示す。図中、時間は左から右に流れる。
【００８６】
サーバ内処理６００では、一連の情報を通信路６１０に送出し始める予定時刻６３０を基準にして、ＯＴＰを計算する（プロセス６０１）。
【００８７】
予定時刻６３０が到来すると、ＯＴＰ６１１を通信路６１０に送出し始める。
【００８８】
続いて、サーバ内処理６００では、配信情報を構成し（プロセス６０２）、構成された配信情報６１２を通信路６１０に送出する。
【００８９】
続いて、サーバ内処理６００では、ＯＴＰと配信情報からＭＡＣ値を計算し（プロセス６０３）、計算されたＭＡＣ値６１３を通信路６１０に送出する。
【００９０】
ＯＴＰチップ内処理６２０では、通信路６１０を経由して伝送されたＯＴＰ６１１、配信情報６１２及びＭＡＣ値６１３の各々を、受信ＯＴＰバッファ２０４へ格納６２１し、配信情報ＤＩバッファ３０１へ格納６２２し、受信ＭＡＣ値バッファ３０２へ格納６２３する。
【００９１】
ＯＴＰチップ内処理６２０では、ＯＴＰ６１１が到着すると、比較用ＯＴＰ計算プロセス６３２が起動可能となる。比較用ＯＴＰ計算プロセス６３２ではＯＴＰの受信を開始した時刻をキャプチャして比較用ＯＴＰを算出するが、通信路６１０の遅延及びホストＣＰＵ２１０による情報伝達の遅延によって、多少の時間遅延Δｔ（６３１）が発生する。しかし、この時間遅延Δｔ（６３１）はＯＴＰの切り替わり時間より十分小さいので、その影響を無視できる。
【００９２】
受信ＯＴＰバッファ２０４へのＯＴＰ６１１の格納６２１が完了しており、比較用ＯＴＰ計算プロセス６３２が終了していれば、ＯＴＰ検証プロセス６３３が実行可能となる。
【００９３】
受信配信情報用ＤＩバッファへの配信情報６１２の格納６２２が完了していれば、比較用ＭＡＣ値計算プロセス６３４が実行可能となる。
【００９４】
受信ＭＡＣ値バッファ３０２へのＭＡＣ値６１３の格納６２３が完了しており、比較用

ＭＡＣ値計算プロセス６３４が終了していれば、ＭＡＣ値検証プロセス６３５で配信情報全体の検証（受信ＭＡＣ値と独自計算した比較用ＭＡＣ値との比較）が実行可能となる。

【００９５】

ここまで、ＭＡＣ認証の範囲をＯＴＰと配信情報を結合したものとして説明したが、特定の用途においてはＭＡＣ認証の範囲からＯＴＰを除外して配信情報のみに限定できる。これは、図３のブロック図において切り替えスイッチ３０３を「開」にすることに相当する。また、図５の処理フロー図では、ステップＳ５０５の比較用ＭＡＣ値計算を、

MAC_ref = hash((D.I. Buff.)∪パスフレーズ)

とすることに相当する。

【００９６】

これにより、ＯＴＰと配信情報の結合性がＭＡＣ値に反映されなくなり、ＯＴＰ計算とＭＡＣ値計算とを独立したプロセスとして扱うことができる。この変更に伴うメリットとデメリットを図７のタイミングチャートに示す。

【００９７】

図７では、上からサーバ内処理７００、サーバ出力７１０、サーバと受信端末の間に割り込んで通信路を偽装した中間者攻撃の出力７２０、ＯＴＰチップの認識７３０を並行する時間座標で示す。図中、時間は左から右に流れる。

【００９８】

サーバ内処理７００で、時刻ｔ１（７４０）を起点とする配信情報Ｘと時刻ｔ２（７４１）を起点とする配信情報Ｙとを送る場合を考える。

【００９９】

図示するように、ＯＴＰ（ｔ１）の計算プロセス７０１と配信情報Ｘの構成及びＭＡＣ（Ｘ）の計算プロセス７０２、７０３とを独立して並行に実行できる。ＯＴＰ（ｔ２）の計算プロセス７０４と配信情報Ｙの構成及びＭＡＣ（Ｙ）の計算プロセス７０５、７０６も同様に独立して並行に実行できる。

【０１００】

従って、この並行プロセスによるスループットの向上は、種々の端末に異なる配信情報を送る配信情報サーバにとってメリットとなる。

【０１０１】

しかし、ＯＴＰと配信情報及びＭＡＣ値を分離したために、中間者攻撃を受けるリスクがあるというデメリットもある。以下、このデメリットを説明する。

【０１０２】

サーバ出力７１０は、時刻ｔ１（７４０）を起点として、ＯＴＰ（ｔ１）（７１１）－配信情報Ｘ（７１２）－ＭＡＣ（Ｘ）（７１３）の順で並んでいる。また、時刻ｔ２（７４１）を起点として、ＯＴＰ（ｔ２）（７１４）－配信情報Ｙ（７１５）－ＭＡＣ（Ｙ）（７１６）の順で並んでいる。図７の説明において、記号「－」はデータ並びのシーケンスを表す接続記号である。

【０１０３】

中間者攻撃では、その出力７２０として、配信情報Ｘ（７１２）とＭＡＣ（Ｘ）（７１３）の組を記憶し、別のＯＴＰヘッダＯＴＰ（ｔ２）（７１４）の時の後続データを配信情報Ｙ（７１５）の代わりに配信情報Ｘ（７１２）で書き換え（７２１）、ＭＡＣ（Ｙ）（７１６）の代わりにＭＡＣ（Ｘ）（７１３）で書き換え（７２２）というデータを送信する攻撃が実行可能である。サーバから発信された情報配信情報Ｙ（７１５）とＭＡＣ（Ｙ）（７１６）は通信経路の途中で失われる。

【０１０４】

ＯＴＰチップの認識処理では、ＯＴＰ（ｔ１）（７１１）－配信情報Ｘ（７１２）－ＭＡＣ（Ｘ）（７１３）の順に並んだデータと、ＯＴＰ（ｔ２）（７１４）－配信情報Ｘ（７１２）－ＭＡＣ（Ｘ）（７１３）の順に並んだデータがサーバから到達したことになり、配信情報とＭＡＣ値の組が合っているので改竄を検出できない。すなわち、この中間者攻撃は、配信情報Ｘ（７１２）－ＭＡＣ（Ｘ）（７１３）の再生攻撃を行うことになる。

これは配信情報と、その正しいＭＡＣ値の対が、時刻的に正しいＯＰＴヘッダの下に付いていれば、矛盾なく情報を受け入れるためである。

【０１０５】

以上、ＭＡＣ認証範囲が異なる別方式も例示したが、前述したメリットとリスクを加味して採否の判断をすることが肝要となる。

【０１０６】

＜実施例２＞

図８は、本発明の実施例２に係る拡張されたＯＴＰ照合チップ３００の詳細を示すブロック図である。実施例２では、配信情報の共通鍵暗号化に対応するように、ＯＴＰ照合チップが拡張されている。この拡張によって、盗聴による配信情報の内容漏洩を防止できる。

【０１０７】

図８に示す実施例２の構成と図３に示す実施例１の構成との差分は、復号化した配信情報をホストＣＰＵ２１０に送信するための復号データバッファ８０２が追加された点である。ホストＣＰＵ２１０は、通信路２１２を経由して、復号化された配信情報を取得できるようになっている。

【０１０８】

配信情報の真正性が確認された場合、すなわちＯＴＰ一致かつＭＡＣ値一致でＡＮＤ論理３０６がアクティブの場合、暗号復号器８０１がアクティブとなる。暗号復号器８０１は、パスフレーズ保管庫２０２に格納されているパスフレーズを共通鍵として配信情報ＤＩバッファ３０１の内容を復号化し、復号データバッファ８０２に転送する。

【０１０９】

ここまでの説明で、情報配信サーバと知識共有した共通鍵は、全てパスフレーズという呼称で記述してきたが、同一のものに限定されなくてもよい。すなわち、ＯＴＰを生成する共通鍵、ＭＡＣ値を生成する共通鍵、及び配信情報を暗号復号化する共通鍵の各々を別の鍵として、複数の個別鍵で構成されてもよい。複数の個別鍵で構成される場合、各々の鍵は用途別に情報配信サーバとの間で知識共有されており、拡張されたＯＴＰ照合チップ３００の中では、耐タンパー性に優れたパスフレーズ保管庫２０２の中に保管されることは言うまでもない。

【０１１０】

図９は、実施例２の配信情報検証処理Ｓ５００を示すフローチャートである。

【０１１１】

実施例２の処理フローと、配信情報を共通鍵暗号化しない実施例１の処理フロー（図５）との差分は、ステップ５０７で判定結果ＯＫの場合の「ステップＳ９０１：配信データの復号化」、「ステップＳ９０２：復号化されたデータの復号データバッファ８０２への格納」が追加された点である。

【０１１２】

判定Ｓ５０６でＭＡＣ値を比較し配信情報の改竄が無いと判定されると、ステップＳ５０７で判定結果ＯＫとする点は実施例１と同じであるが、実施例２では、判定結果ＯＫとした後にステップＳ９０１で配信データを復号化する。

【０１１３】

図９の処理フローでは、以下の３ステップでパスフレーズを使用する。「ステップＳ５０３：比較用ＯＴＰ計算」、「ステップＳ５０６：比較用ＭＡＣ値計算」、「ステップＳ９０１：配信データの復号化」の３ステップである。これらのパスフレーズは同一のものを用いてもよいし、用途別に別のパスフレーズを用いてもよいことは前述の通りである。

【０１１４】

続くステップＳ９０２では、復号化されたデータ（Ｄｃｒｐｔ＿Ｄａｔａ）を復号データバッファ８０２に転送し、ステップＳ５０９で処理を終了する。

【０１１５】

以上に説明したように、実施例２では、配信情報を公開鍵暗号と比べて計算量が少ない共通鍵暗号方式によって容易に暗号化でき、盗聴を防止できる。

【０１１６】
＜実施例３＞
図１０は、本発明の実施例３に係る拡張されたＯＴＰ照合チップ３００の詳細を示すブロック図である。実施例３では、配信情報の共通鍵暗号化に対応するように、ＯＴＰ照合チップがさらに拡張されている。実施例３の拡張されたＯＴＰ照合チップによって、配信情報がホストＣＰＵ２１０向けの配信情報とＯＴＰ照合チップ向けの配信情報とを兼ねるように構成し、同一プロトコルで別用途の情報を統合的に配信できる。
【０１１７】
ＯＴＰ照合チップ向けの配信情報は、共通鍵暗号化が必須であり、配信内容を盗聴から守る必要がある。また、復号化したＯＴＰ照合チップ向けの配信内容を、復号データバッファ８０２を経由してホストＣＰＵ２１０に開示することは、情報漏洩リスクとなるので避けるべきである。
【０１１８】
図１０に示す実施例３の構成と図８に示す実施例２の構成との差分は、指令解釈部１００１と２方向データ切り替えスイッチ１００２が追加された点である。
【０１１９】
配信情報がホストＣＰＵ２１０向けかＯＴＰ照合チップ３００向けかを示すコマンドは、配信情報に格納されている。指令解釈部１００１は、復号化された配信情報から抽出されるコマンドによって切り替えスイッチ１００２を切り替える。例えば、配信情報がホストＣＰＵ２１０向けであれば、図８に示す実施例２と同様に、復号化されたデータは復号データバッファ８０２送られる。一方、配信情報がＯＴＰ照合チップ３００向けであれば、２方向データ切り替えスイッチ１００２が切り替わり、復号化されたデータは制御部２００に直接送られ、復号データバッファ８０２には送られない。ＯＴＰ照合チップ向けのデータとは、例えば、時計部２０１の時刻合わせ情報、パスフレーズ保管庫２０２のパスフレーズ更新情報などがある。
【０１２０】
パスフレーズの更新は、ＯＴＰ照合チップ製造時に設定された初期鍵を保存した状態で使用せず、情報配信サーバから配信された共通鍵を一時的に使用する。初期鍵を保存しておく理由は、何か障害が発生した場合、又はＯＴＰ照合チップ３００がマスターリセットされた場合、初期鍵に戻る方がシステムとしてロバストだからである。
【０１２１】
一時的に更新されるパスフレーズは、配信情報データ中に格納されてＯＴＰ照合チップ３００まで送られるが、前述した通り初期鍵で共通鍵暗号化されているため、更新されるパスフレーズの漏洩リスクは低く、インターネットを経由して鍵を配信しても十分にセキュアである。
【０１２２】
図１１は、実施例３の配信情報検証処理Ｓ５００を示すフローチャートである。
【０１２３】
実施例３の処理フローと実施例１の処理フロー（図５）との差分は、Ｓ９０１、Ｓ９０２、Ｓ１１０１～Ｓ１１０６の処理ステップが追加された点であり、実施例２の処理フロー（図９）との差分は、Ｓ１１０１～Ｓ１１０６の処理ステップが追加された点である。
【０１２４】
判定Ｓ５０６でＭＡＣ値を比較し配信情報の改竄が無いと判定されると、ステップＳ５０７で判定結果ＯＫとし、続くステップＳ９０１で配信データを復号化する点は実施例２と同じである。その後、配信情報がホストＣＰＵ２１０向けか、ＯＴＰ照合チップ３００向けかが判定される（Ｓ１１０１）。
【０１２５】
復号化された配信情報の中に、ホストＣＰＵ２１０向けであるかＯＴＰ照合チップ３００向けであるのかのコマンドが含まれており、このコマンドに基づいて処理が切り替えられる。この仕組みは、ブロック図（図１０）において、指令解釈部１００１と切り替えス

イッチ１００２で構成される。
【０１２６】
配信情報がホストＣＰＵ２１０向けである場合、ステップＳ９０２で復号化されたデータ（Ｄｃｒｐｔ＿Ｄａｔａ）を復号データバッファ８０２に転送し、ステップＳ５０９で処理を終了する。この処理は実施例２と同じである。
【０１２７】
一方、配信情報がＯＴＰ照合チップ向けである場合、Ｓ１１０２～Ｓ１１０６の処理を実行する。
【０１２８】
まず、配信情報が時刻更新指令であるかが判定される（Ｓ１１０２）。配信情報が時刻更新指令であれば、配信情報中の時刻更新値ｔｉｍｅ＿ｒｎｗを引数にしてシステム関数ｔｉｍｅｓｅｔ（）を呼び出して、時計デバイスの現在時刻を変更する（ステップ１１０３）。その後ステップ５０９で処理を終了する。
【０１２９】
配信情報が時刻更新指令でなければ、配信情報がパスフレーズ更新指令であるか（Ｓ１１０４）、及び配信情報の更新対象機器ＩＤ（ＩＤｅｎｔｉｆｉｃａｔｉｏｎ：識別子）が一致するか（Ｓ１１０５）を判定する。配信情報がパスフレーズ更新指令でなく又は更新対象機器ＩＤが一致していなければ、ステップＳ５０９で処理を終了する。
【０１３０】
配信情報がパスフレーズ更新指令であり、かつ更新対象機器ＩＤが一致していれば、イベントフラグであるパスフレーズ更新フラグに”１”をセットし、更新設定時刻を配信情報から抽出してシステム変数ｔｉｍｅ＿ｃｈｇにセットし、更新用パスフレーズを配信情報から抽出してシステム変数Ｐｐ＿ｎｅｗにセットして、ステップＳ５０９で処理を終了する。
【０１３１】
実際には、パスフレーズの更新は、図１２で示す時間更新用の定時割込み処理Ｓ１２００で実行される。図１２は、拡張されたＯＴＰ照合チップ３００で実行される定時割込み処理のフローチャートである。定時割込み処理は、所定の時間分解能で毎回サイクリックに起動し、ハウスキーピングタスクを行う制御部２００の割り込み処理である。
【０１３２】
まず、パスフレーズ更新用フラグが設定されているか（値が１であるか）を判定する（Ｓ１２０１）。パスフレーズ更新用フラグが設定されていなければ、イベントが発生していないので、何も行わずにステップ１２０６で処理を終了する。
【０１３３】
パスフレーズ更新用フラグが設定されていれば（値が１であれば）パスフレーズ更新イベントが発生中なので、時計デバイスを参照し、現在時刻（Ｒｅｇ＿ｎｏｗの内容）をｔｉｍｅ変数に入力する（Ｓ１２０２）。続いて、現在時刻ｔｉｍｅが更新設定時刻ｔｉｍｅ＿ｃｈｇを経過しているかを判定する（Ｓ１２０３）。その結果、現在時刻ｔｉｍｅが更新設定時刻ｔｉｍｅ＿ｃｈｇを経過していれば、ステップ１２０４に進む。現在時刻ｔｉｍｅが更新設定時刻ｔｉｍｅ＿ｃｈｇを経過していなければ、何も行わずにステップ１２０６で処理を終了する。
【０１３４】
ステップ１２０４では、更新用パスフレーズＰｐ＿ｎｅｗをパスフレーズ保管庫２０２に送って、今までのパスフレーズの変更値として設定する。続いてステップＳ１２０５では、パスフレーズ更新フラグをクリア（”０”に設定）し、ステップＳ１２０６で処理を終了する。
【０１３５】
図１３は、前述したパスフレーズ変更機能を利用して受信クラスタを動的に拡大や縮小する受信機器群を示す図である。
【０１３６】

パスフレーズを決定すればグローバル時間における一つの時刻において唯一のＯＴＰが決定するので、情報配信サーバ１３００が一つのＯＴＰを選択すれば、唯一の宛先を決定することになる。従って、パスフレーズは宛先選別（アドレッシング）の機能を持っているといえる。よって、複数の受信端末に暫定的に同一パスフレーズを付与することによって、当該複数の受信端末群で受信クラスタを形成できる。情報配信サーバ１３００は、この受信クラスタに対して一時期に一括して配信情報をブロードキャストでき、効率的に情報を配信できる。

【０１３７】

状態１３０１は、初期鍵のパスフレーズで構成された受信機器群を示しており、○の中の数字は受信機の個別ＩＤ、すなわち設定されたパスフレーズの識別番号を示す。

【０１３８】

状態１３０２は、状態１３０１から時間ｔ１が経過した状態である。前述したパスフレーズ更新機能を利用して、端末３、５、６に暫定パスフレーズ０が付与され、受信クラスタ１３１０を形成する。情報配信サーバ１３００は、この受信クラスタ１３１０の端末に一括して配信情報のブロードキャストできる。

【０１３９】

状態１３０３は、状態１３０２から時間ｔ２が経過した状態である。再び前述したパスフレーズ更新機能を利用して、受信クラスタ１３１０中の元々は端末６であった端末０の暫定的なパスフレーズを解除し、初期鍵６に戻す。従って受信クラスタ１３１１は受信クラスタ１３１０と比べて小さくなる。

【０１４０】

このように、実施例３では、パスフレーズの更新機能を用いて受信クラスタを拡大や縮小でき、効率的に情報を配信できる。

【０１４１】

以上、実施例１、実施例２、実施例３で述べたように、本明細書に開示した手段によれば、デジタル署名というリソース消費が大きい方式を使わずに配信情報を検証でき、低い処理能力で廉価なＯＴＰ照合チップの内部で実行でき、高い信頼性の情報配信機構を実現できる。

【０１４２】

また、ＯＴＰ照合チップ自体のパラメータも配信情報としてサーバから配信して変更できる。この仕組みに基づいて、同一宛先の受信クラスタを動的かつ容易に形成し解消できる。すなわち、同一受信クラスタに位置づけられた機器には、情報配信サーバから同時に同一情報をブロードキャスト配信でき、車載機器、ＩｏＴ機器などのＯＴＡ（Ｏｖｅｒ－ｔｈｅ－Ａｉｒ：無線による情報配信）に適応した仕組みを提供できる。

【０１４３】

以上に説明したように、本実施例の情報検証装置（ＯＴＰ照合チップ３００）は、情報発信元（情報配信サーバ１３００）から送信され、同期した時刻及び共通鍵によって生成されたワンタイムパスワードと、情報発信元から送信され、認証以外の利用価値を有する配信情報と、情報発信元から送信され、これらの情報から当該共通鍵を用いて計算されたメッセージ認証コード（ＭＡＣ値）の少なくとも三つが入力されると、少なくとも配信情報の真正性の判定結果を出力するので、配信情報の改竄を検知できると共に、再生攻撃を検知できる。また、既存のＯＴＰ照合チップの基本的構成を維持した改造によって、配信情報の改竄検知及び再生攻撃検知を実現できる。しかも、機能追加によるコストアップを最小化でき、ＯＴＰ照合チップ自体の付加価値を向上できる。すなわち、現有計算資源（例えばハッシュ関数）を流用して、新たに追加されるＭＡＣ認証機能を実現できる点でコストアップを最小化できる。

【０１４４】

また、処理負荷が軽いことから、ＯＴＰ照合チップ内で検証処理を実行でき、ホストＣＰＵ２１０の負担を増大させず、車載用途及びＩｏＴ用途の低能力のホストＣＰＵ２１０であっても本来の処理を圧迫せずにセキュリティ対応能力を向上できる。

【０１４５】
また、通信路を経由して共通鍵が送信されず、物理的に配布されるので、盗聴リスクを低減でき、インターネットを経由した情報配信に適用しても、十分にセキュアである。
【０１４６】
また、情報検証装置は、前記情報発信元から送信されたワンタイムパスワードと当該情報検証装置内で計算されたワンタイムパスワードとが一致し、かつ、前記情報発信元から送信されたメッセージ認証コードと当該情報検証装置内で計算されたメッセージ認証コードとが一致する場合、前記配信情報が真正であると判定し、前記配信情報が真正であることを出力するので、配信情報の改竄を検知できると共に、再生攻撃を検知できる。
【０１４７】
また、情報発信元から送信されるワンタイムパスワードは、前記情報発信元から当該情報検証装置へ送信される一連の情報から送信開始時刻に基づいて生成される時刻同期型のワンタイムパスワードとしたので、ワンタイムパスワードを生成するための時刻の切れ目を考慮する必要がなくなり、装置の設計自由度が向上する。
【０１４８】
また、前記情報発信元から送信されるメッセージ認証コードは、前記情報発信元から送信されるワンタイムパスワード及び前記情報発信元から送信される配信情報に基づいて、前記共通鍵を用いて計算されるので、高いセキュリティを実現できる。
【０１４９】
また、前記情報発信元から送信されるメッセージ認証コードは、前記情報発信元から送信される配信情報に基づいて、前記共通鍵を用いて計算されるので、ワンタイムパスワードの計算プロセスと配信情報の構成及びＭＡＣ値の計算プロセスを独立して並行に実行し、処理のスループットを向上させることができる。
【０１５０】
また、前記配信情報は、前記共通鍵によって暗号化されて、前記情報発信元から送信されるものであって、前記演算装置は、前記情報発信元から送信された配信情報を復号化して、前記配信情報の真正性判定結果、及び復号化した配信情報を出力するので、盗聴による配信情報の内容漏洩を防止できる。
【０１５１】
また、前記ワンタイムパスワードを生成するための共通鍵と、前記メッセージ認証コードを生成するための共通鍵と、前記配信情報を暗号化するための共通鍵とは、同一の鍵である、又は複数の別個の鍵としたので、鍵を変えるときに適用プロセスを自由に設定できる。また、共通鍵を同一とした場合、別の共通鍵を設定することなく、配信情報を暗号化でき、配信情報の漏洩を防止できる。
【０１５２】
また、前記情報発信元は、当該情報検証装置が真正性を検証すべきホスト装置宛ての配信情報と、当該情報検証装置宛ての更新情報とを配信できるように構成されており、前記情報検証装置は、前記配信情報が当該情報検証装置宛ての更新情報である場合、前記復号化された配信情報を出力せず、前記更新情報を用いて当該情報検証装置の内部値を変更するので、ホストＣＰＵ２１０に提供される配信情報に加えて、ＯＴＰ照合チップ３００が必要とする情報（例えば、内部時計の時刻合わせ情報、共通鍵の更新情報）を同一プロトコルで統合的に配信できる。
【０１５３】
また、前記情報発信元から当該情報検証装置宛ての更新情報は、当該情報検証装置の時計を修正するための時刻データを含み、前記演算装置は、前記情報発信元から送信される配信情報の真正性判定結果が真正である場合、前記時刻データを用いて当該情報検証装置の時計を修正するので、高いセキュリティで時刻を更新できる。
【０１５４】
また、前記情報発信元から当該情報検証装置宛ての更新情報は、前記情報発信元と前記情報検証装置とで知識共有された共通鍵を更新するためのデータと、前記共通鍵を更新す

べき前記情報検証装置の識別子と、前記共通鍵の更新タイミングの少なくとも三つを含み、前記演算装置は、前記情報発信元から送信される配信情報の真正性判定結果が真正であり、かつ識別子が自情報検証装置のものと合致する場合、前記更新タイミングに当該検証装置内に格納される共通鍵を更新するので、高いセキュリティで共通鍵を更新できる。

【０１５５】

また、複数の前記情報検証装置が情報発信元とで知識共有した同一の共通鍵への変更によって、当該情報検証装置を格納する複数の受信機器群でクラスタを形成し、前記クラスタを形成する複数の情報検証装置は、前記情報発信元から同一のワンタイムパスワードと同一メッセージ認証コードとを用いて、同一の配信情報を同時に受信するので、クラスタに対して一時期に一括して配信情報を一対多でブロードキャストでき、効率的に情報を配信できる。

【０１５６】

なお、本発明は前述した実施例に限定されるものではなく、添付した特許請求の範囲の趣旨内における様々な変形例及び同等の構成が含まれる。例えば、前述した実施例は本発明を分かりやすく説明するために詳細に説明したものであり、必ずしも説明した全ての構成を備えるものに本発明は限定されない。また、ある実施例の構成の一部を他の実施例の構成に置き換えてもよい。また、ある実施例の構成に他の実施例の構成を加えてもよい。また、各実施例の構成の一部について、他の構成の追加・削除・置換をしてもよい。

【０１５７】

また、前述した各構成、機能、処理部、処理手段等は、それらの一部又は全部を、例えば集積回路で設計する等により、ハードウェアで実現してもよく、プロセッサがそれぞれの機能を実現するプログラムを解釈し実行することにより、ソフトウェアで実現してもよく、集積回路と密接に関連したデバイス制御言語又はファームウェアとして実現してもよい。

【０１５８】

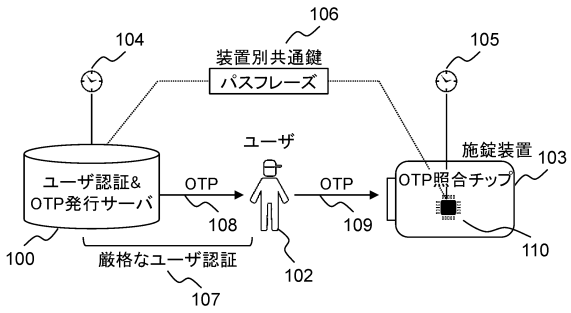
各機能を実現するプログラム、テーブル、ファイル等の情報は、メモリ、ハードディスク、ＳＳＤ（Ｓｏｌｉｄ　Ｓｔａｔｅ　Ｄｒｉｖｅ）等の記憶装置、又は、ＩＣカード、ＳＤカード、ＤＶＤ等の記録媒体に格納することができる。

【０１５９】

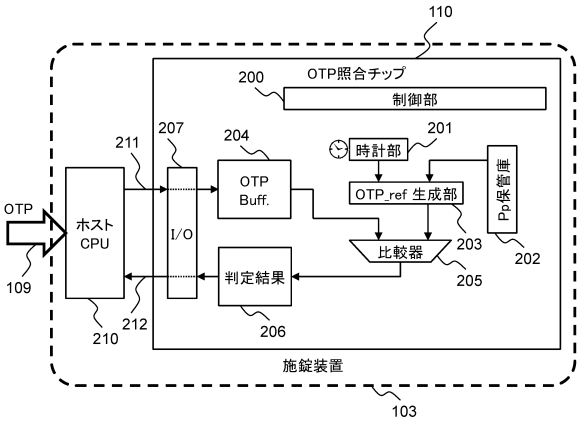
また、制御線や情報線は説明上必要と考えられるものを示しており、実装上必要な全ての制御線や情報線を示しているとは限らない。実際には、ほとんど全ての構成が相互に接続されていると考えてよい。

【図面】

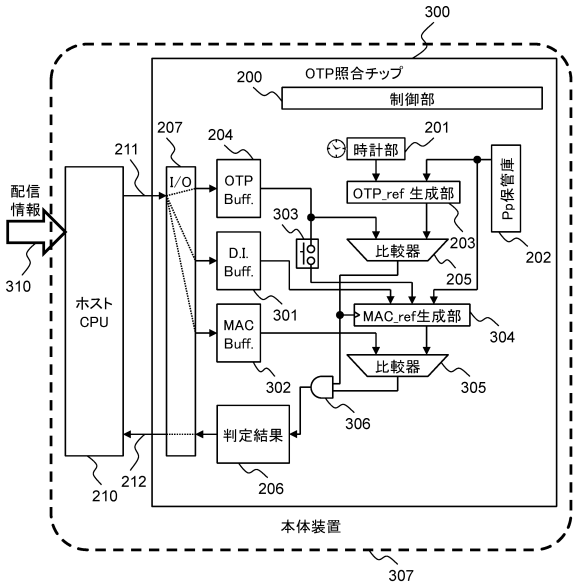
【図１】


104
106
装置別共通鍵
パスフレーズ
105
施錠装置
103
ユーザ
ユーザ認証&
OTP発行サーバ
OTP
108
OTP
109
OTP照合チップ
100
厳格なユーザ認証
107
102
110

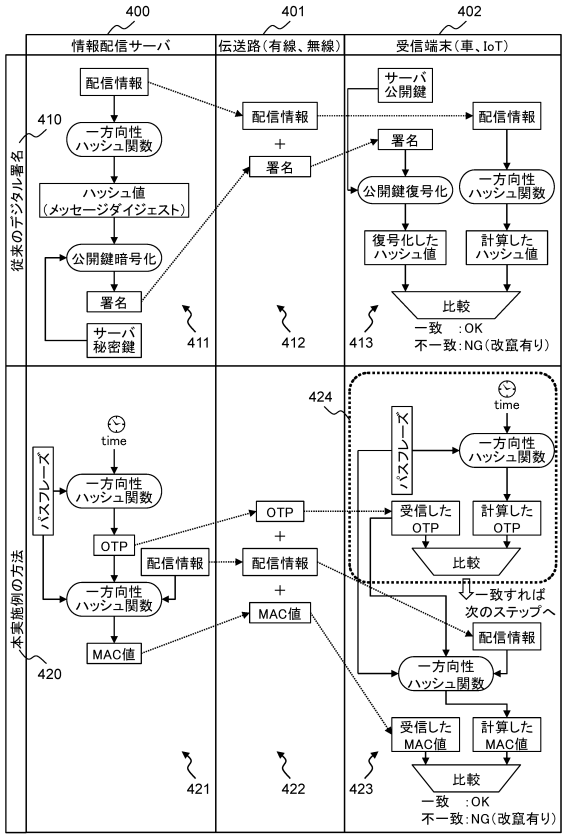
【図２】


110
OTP照合チップ
200
制御部
211
207
204
201
時計部
OTP
Buff.
OTP_ref 生成部
Pp保管庫
OTP
ホスト
CPU
I/O
比較器
203
202
判定結果
205
109
212
206
210
施錠装置
103

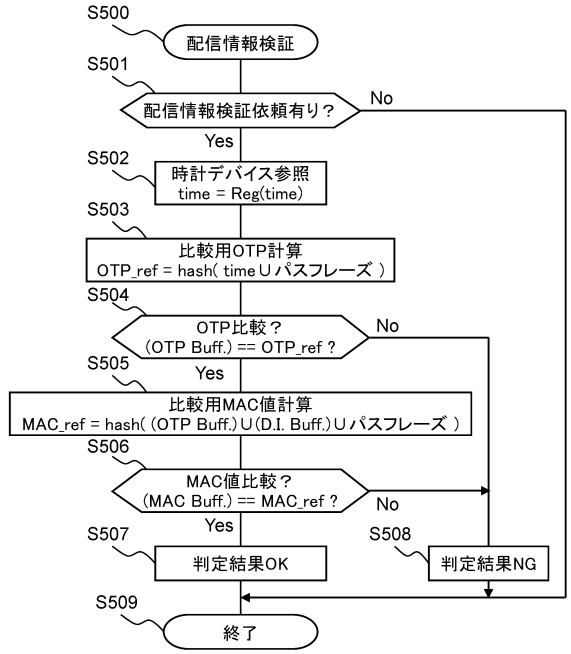
【図３】


300
200
OTP照合チップ
制御部
207
204
211
201
時計部
I/O
OTP
Buff.
OTP_ref 生成部
Pp保管庫
303
D.I.
Buff.
比較器
203
202
205
配信
情報
MAC_ref生成部
301
304
MAC
Buff.
比較器
302
305
306
ホスト
CPU
判定結果
310
212
206
210
本体装置
307

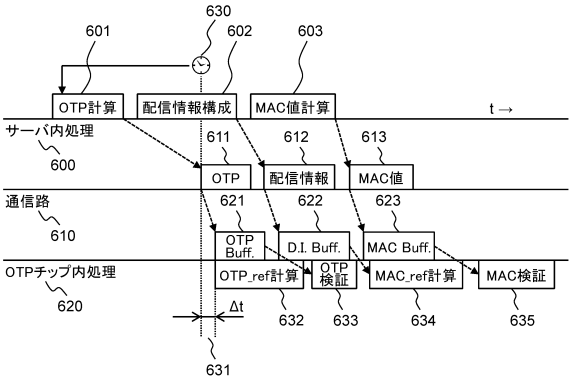
【図４】


400
401
402
情報配信サーバ
伝送路(有線、無線)
受信端末(車、IoT)
従来のデジタル署名
配信情報
サーバ
公開鍵
410
一方向性
ハッシュ関数
配信情報
署名
署名
ハッシュ値
(メッセージダイジェスト)
公開鍵復号化
一方向性
ハッシュ関数
公開鍵暗号化
復号化した
ハッシュ値
計算した
ハッシュ値
署名
比較
サーバ
秘密鍵
411
412
413
一致 :OK
不一致:NG(改竄有り)
本実施例の方法
424
time
パスフレーズ
一方向性
ハッシュ関数
time
パスフレーズ
一方向性
ハッシュ関数
OTP
受信した
OTP
計算した
OTP
OTP
+
配信情報
比較
配信情報
+
MAC値
一致すれば
次のステップへ
一方向性
ハッシュ関数
配信情報
MAC値
受信した
MAC値
計算した
MAC値
比較
420
421
422
423
一致 :OK
不一致:NG(改竄有り)

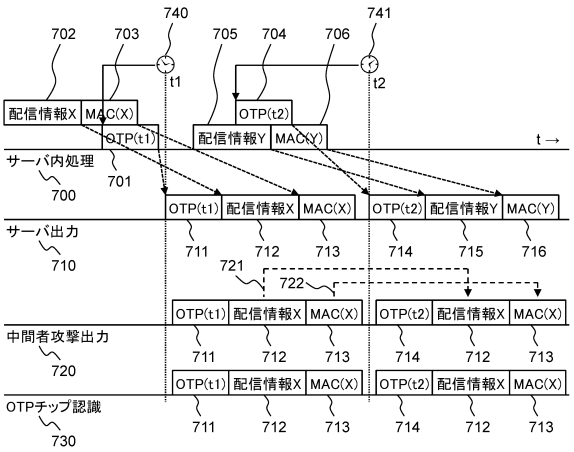
【図５】


S500
配信情報検証
S501
配信情報検証依頼有り？
No
Yes
S502
時計デバイス参照
time = Reg(time)
S503
比較用OTP計算
OTP_ref = hash(time∪パスフレーズ)
S504
OTP比較？
(OTP Buff.) == OTP_ref ?
No
S505
Yes
比較用MAC値計算
MAC_ref = hash((OTP Buff.)∪(D.I. Buff.)∪パスフレーズ)
S506
MAC値比較？
(MAC Buff.) == MAC_ref ?
No
Yes
S507
判定結果OK
S508
判定結果NG
S509
終了

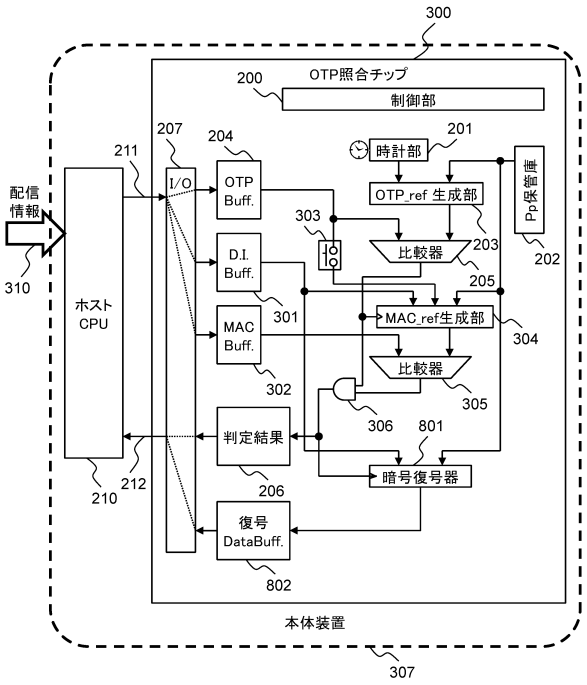
【図６】


630
601
602
603
OTP計算
配信情報構成
MAC値計算
t →
サーバ内処理
600
611
612
613
OTP
配信情報
MAC値
通信路
610
621
622
623
OTP Buff.
D.I. Buff.
MAC Buff.
OTPチップ内処理
620
OTP_ref計算
OTP 検証
MAC_ref計算
MAC検証
Δt
632
633
634
635
631

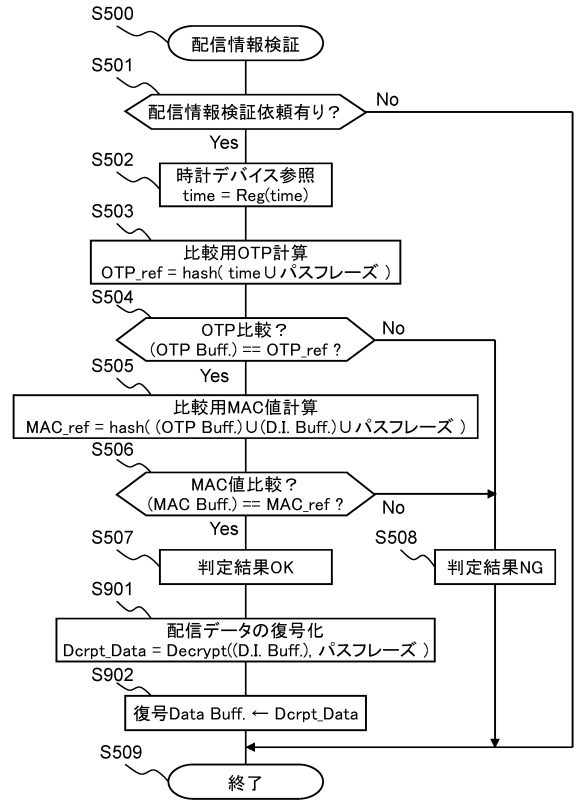
【図７】


740
741
702
703
705
704
706
t1
t2
配信情報X
MAC(X)
OTP(t1)
OTP(t2)
配信情報Y
MAC(Y)
t →
サーバ内処理
700
701
サーバ出力
710
711
712
713
714
715
716
721
722
中間者攻撃出力
720
OTPチップ認識
730

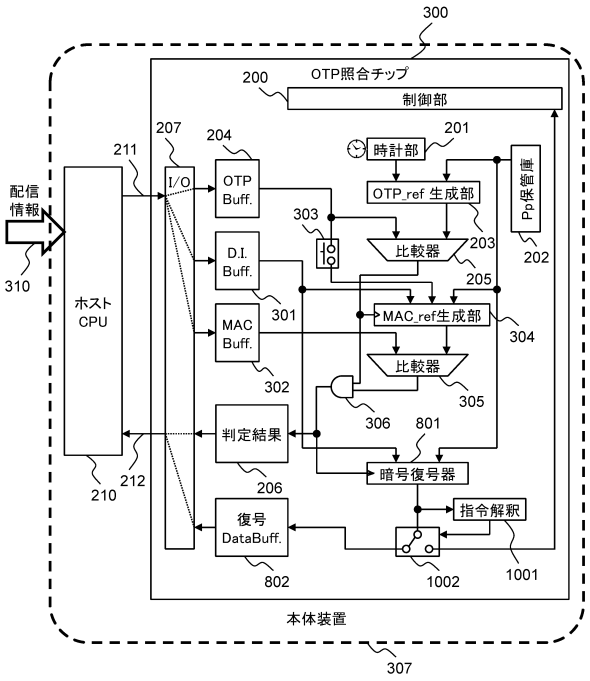
【図８】


300
200
OTP照合チップ
制御部
207
204
201
211
時計部
I/O
OTP Buff.
OTP_ref 生成部
Pp保管庫
配信情報
303
D.I. Buff.
比較器
203
202
205
ホスト CPU
301
MAC_ref生成部
304
MAC Buff.
比較器
302
305
306
801
判定結果
暗号復号器
206
210
212
復号 DataBuff.
802
本体装置
310
307

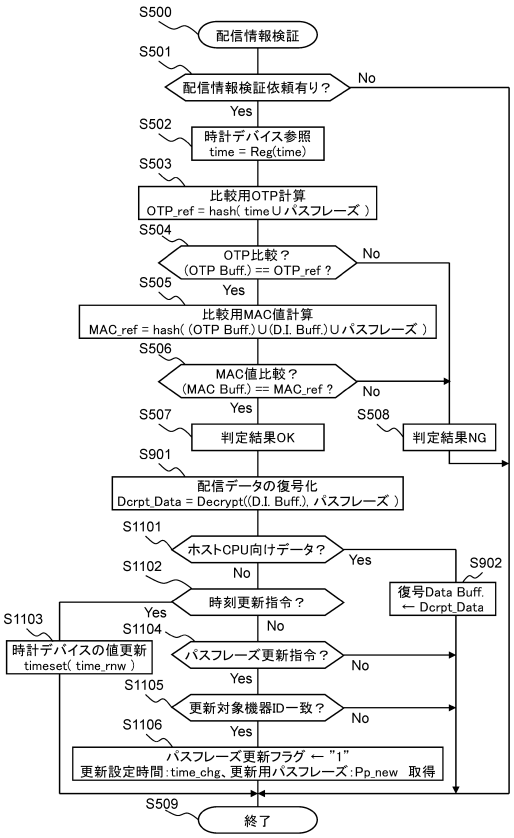
【図９】



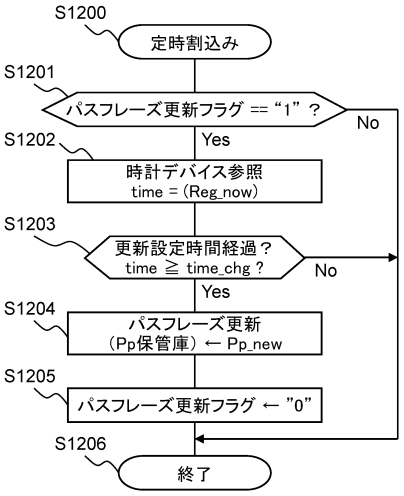
【図１０】



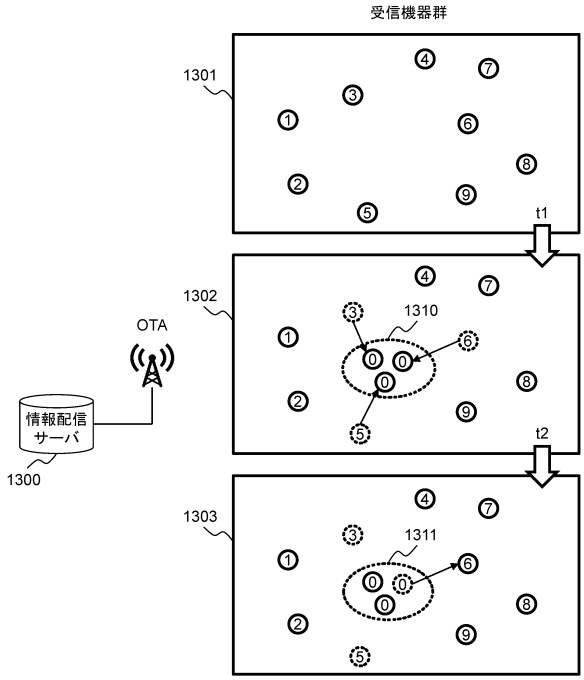
【図１１】



【図１２】



【図１３】



フロントページの続き

(56)参考文献　欧州特許出願公開第０３１０１５３５（ＥＰ，Ａ１）
特開２０１８－１０７５１４（ＪＰ，Ａ）
特表２０１７－５０５０４８（ＪＰ，Ａ）
特開２００２－２５９３４４（ＪＰ，Ａ）
特開２０２０－０７２３３９（ＪＰ，Ａ）

(58)調査した分野　(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ　９／３２
Ｇ０６Ｆ　２１／６４