(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2010-508719
(P2010-508719A)
(43)公表日　平成22年3月18日(2010.3.18)

(51)Int.Cl.			F I			テーマコード（参考）
H04L	9/32	(2006.01)	H04L	9/00	675A	5J104
G09C	1/00	(2006.01)	G09C	1/00	640D	

審査請求 有　予備審査請求 未請求　（全 20 頁）

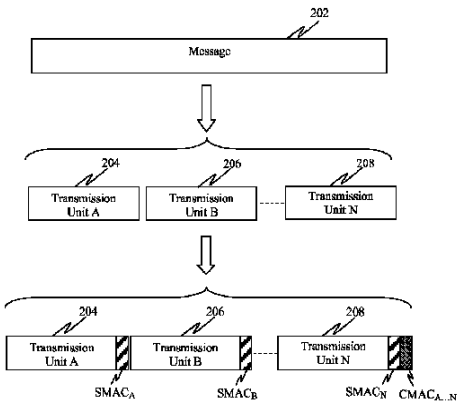
(21)出願番号　特願2009-534873 (P2009-534873)
(86)(22)出願日　平成19年10月25日 (2007.10.25)
(85)翻訳文提出日　平成21年5月25日 (2009.5.25)
(86)国際出願番号　PCT/US2007/082566
(87)国際公開番号　WO2008/052137
(87)国際公開日　平成20年5月2日 (2008.5.2)
(31)優先権主張番号　60/863,217
(32)優先日　平成18年10月27日 (2006.10.27)
(33)優先権主張国　米国 (US)
(31)優先権主張番号　11/681,117
(32)優先日　平成19年3月1日 (2007.3.1)
(33)優先権主張国　米国 (US)

(71)出願人　595020643
クゥアルコム・インコーポレイテッド
ＱＵＡＬＣＯＭＭ　ＩＮＣＯＲＰＯＲＡＴＥＤ
アメリカ合衆国、カリフォルニア州　９２１２１－１７１４、サン・ディエゴ、モアハウス・ドライブ　５７７５
(74)代理人　100058479
弁理士　鈴江　武彦
(74)代理人　100108855
弁理士　蔵田　昌俊
(74)代理人　100091351
弁理士　河野　哲
(74)代理人　100088683
弁理士　中村　誠

最終頁に続く

(54)【発明の名称】合成メッセージ認証コード

(57)【要約】
送信前に、メッセージは複数の送信ユニットに分割される。各送信ユニットのためのサブメッセージ認証コードが取得される。複数の送信ユニットのサブメッセージ認証コードに基づいて、メッセージ全体のための合成メッセージ認証コードが取得される。その後複数の送信ユニットと、合成メッセージ認証コードとが、送信される。メッセージ受信機は、メッセージに対応する複数の送信ユニットを受信する。各送信ユニットのためのローカルサブメッセージ認証コードが受信機によって計算される。複数の送信ユニットのためのローカルサブメッセージ認証コードに基づいて、ローカル合成メッセージ認証コードが受信機によって計算される。受信したメッセージの完全性及び／又は真正性を判定するために、ローカル合成メッセージ認証コードと、受信した合成メッセージ認証コードとが比較される。



【特許請求の範囲】
【請求項１】
メッセージの認証と完全性ベリフィケーションとを実行する送信デバイスで動作する方法であって、
前記メッセージを複数の送信ユニットに分割することと、
前記送信ユニットの各々のためのサブメッセージ認証コードを取得することと、
前記複数の送信ユニットの前記サブメッセージ認証コードに基づいて、前記メッセージ全体のための合成メッセージ認証コードを取得することと、
前記複数の送信ユニットと前記合成メッセージ認証コードとを送信することと
を備える方法。
【請求項２】
請求項１に記載の方法において、
送信前に、前記合成メッセージ認証コードを前記複数の送信ユニットのうちの１つに添付することを更に備える方法。
【請求項３】
請求項１に記載の方法において、
前記合成メッセージ認証コードは、前記複数の送信ユニットのサブメッセージ認証コードの関数である方法。
【請求項４】
請求項１に記載の方法において、
前記合成メッセージ認証コードは、前記サブメッセージ認証コードについて排他的ＯＲ演算を実行することによって導出される方法。
【請求項５】
請求項１に記載の方法において、
前記合成メッセージ認証コードは、複数の固定長入力を単一の固定長出力に合成する関数から得られる方法。
【請求項６】
請求項１に記載の方法において、
前記合成メッセージ認証コードは、前記サブメッセージ認証コードを合算する関数によって得られる方法。
【請求項７】
請求項１に記載の方法において、
前記合成メッセージ認証コードは、サブメッセージ認証コードを係数として備える多項式を計算する関数によって得られる方法。
【請求項８】
請求項１に記載の方法において、
前記送信ユニットが異なる長さを有する方法。
【請求項９】
請求項１に記載の方法において、
前記サブメッセージ認証コードは、対応する前記送信ユニットのコンテンツに基づいている方法。
【請求項１０】
メッセージを複数の送信ユニットに分割し、
前記送信ユニットの各々のためのサブメッセージ認証コードを取得し、
前記複数の送信ユニットの前記サブメッセージ認証コードに基づいて、前記メッセージ全体のための合成メッセージ認証コードを取得し、
前記複数の送信ユニットと前記合成メッセージ認証コードとを送信する
ように構成された送信機回路を備える送信デバイス。
【請求項１１】
請求項１０に記載のデバイスにおいて、

前記送信機は更に、前記合成メッセージ認証コードを前記複数の送信ユニットのうちの１つに添付するように構成されたデバイス。
【請求項１２】
請求項１０に記載のデバイスにおいて、
前記送信機は、複数の固定長入力を単一の固定長出力に合成する関数を含むデバイス。
【請求項１３】
請求項１０に記載のデバイスにおいて、
前記サブメッセージ認証コードは、対応する前記送信ユニットのコンテンツに基づいているデバイス。
【請求項１４】
メッセージを複数の送信ユニットに分割する手段と、
前記送信ユニットの各々のためのサブメッセージ認証コードを取得する手段と、
前記複数の送信ユニットの前記サブメッセージ認証コードに基づいて、前記メッセージ全体のための合成メッセージ認証コードを取得する手段と、
前記複数の送信ユニットと前記合成メッセージ認証コードとを送信する手段と
を備える送信デバイス。
【請求項１５】
請求項１４に記載のデバイスにおいて、
前記合成メッセージ認証コードを前記複数の送信ユニットのうちの１つに添付する手段を更に備えるデバイス。
【請求項１６】
未処理メッセージを受信する入力インタフェースと、
受信した未処理メッセージを複数の送信ユニットに分割し、
前記送信ユニットの各々のためのサブメッセージ認証コードを取得し、
前記複数の送信ユニットの前記サブメッセージ認証コードに基づいて、前記メッセージ全体のための合成メッセージ認証コードを取得し、
前記複数の送信ユニットと前記合成メッセージ認証コードとを送信する
ように構成された処理回路と
を備える処理デバイス。
【請求項１７】
請求項１６に記載のデバイスにおいて、
前記処理回路は更に、前記合成メッセージ認証コードを前記複数の送信ユニットのうちの１つに添付するように構成されたデバイス。
【請求項１８】
請求項１６に記載のデバイスにおいて、
前記送信回路は、複数の固定長入力を単一の固定長出力に合成する関数を含むデバイス。
【請求項１９】
送信デバイス上でメッセージを認証する１つ又は複数の命令群を有する機械読取可能媒体であって、前記命令群はプロセッサによって実行されると前記プロセッサに、
受信したメッセージを複数の送信ユニットに分割させ、
前記送信ユニットの各々のためのサブメッセージ認証コードを取得させ、
前記複数の送信ユニットの前記サブメッセージ認証コードに基づいて、前記メッセージ全体のための合成メッセージ認証コードを取得させ、
前記複数の送信ユニットと前記合成メッセージ認証コードとを送信させる
機械読取可能媒体。
【請求項２０】
請求項１９に記載の機械読取可能媒体において、
プロセッサによって実行されると前記プロセッサに更に、前記合成メッセージ認証コードを前記複数の送信ユニットのうちの１つに添付させる１つ又は複数の命令を有する機械読

取可能媒体。
【請求項２１】
受信したメッセージの完全性ベリフィケーション及び認証を実行する受信デバイス上で動作する方法であって、
前記メッセージに対応する複数の送信ユニットを取得することと、
前記送信ユニットの各々のためのローカルサブメッセージ認証コードを計算することと、
前記複数の送信ユニットのための前記ローカルサブメッセージ認証コードに基づいて、ローカル合成メッセージ認証コードを計算することと、
関連するメッセージの完全性及び／又は真正性を判定するために、前記ローカル合成メッセージ認証コードと、受信した合成メッセージ認証コードとを比較することと
を備える方法。
【請求項２２】
請求項２１に記載の方法において、
前記ローカルサブメッセージ認証コードは、自身の送信ユニットが到着すると計算される方法。
【請求項２３】
請求項２１に記載の方法において、
前記送信ユニットは順不同で到着する方法。
【請求項２４】
請求項２１に記載の方法において、
前記送信ユニットが取得されると前記送信ユニットをバッファすることを更に備える方法。
【請求項２５】
請求項２１に記載の方法において、
前記ローカル合成メッセージ認証コードと前記受信した合成メッセージ認証コードとが同一であれば、前記送信ユニットを他のデバイスへ提供することを更に備える方法。
【請求項２６】
請求項２１に記載の方法において、
前記ローカル合成メッセージ認証コードと前記受信した合成メッセージ認証コードとが異なっていれば、前記送信ユニットを破棄することを更に備える方法。
【請求項２７】
メッセージに対応する複数の送信ユニットを取得し、
前記送信ユニットの各々のためのローカルサブメッセージ認証コードを計算し、
前記複数の送信ユニットのための前記ローカルサブメッセージ認証コードに基づいて、ローカル合成メッセージ認証コードを計算し、
関連するメッセージの完全性及び／又は真正性を判定するために、前記ローカル合成メッセージ認証コードと、受信した合成メッセージ認証コードとを比較する
ように構成された受信機回路を備える受信デバイス。
【請求項２８】
請求項２７に記載のデバイスにおいて、
前記受信機は更に、
前記ローカル合成メッセージ認証コードと前記受信した合成メッセージ認証コードとが同一であれば、前記送信ユニットを他のデバイスへ提供し、
前記ローカル合成メッセージ認証コードと前記受信した合成メッセージ認証コードとが異なっていれば、前記送信ユニットを破棄する
ように構成されたデバイス。
【請求項２９】
メッセージに対応する複数の送信ユニットを取得する手段と、
前記送信ユニットの各々のためのローカルサブメッセージ認証コードを計算する手段と

、
前記複数の送信ユニットのための前記ローカルサブメッセージ認証コードに基づいて、ローカル合成メッセージ認証コードを計算する手段と、
関連するメッセージの完全性及び／又は真正性を判定するために、前記ローカル合成メッセージ認証コードと、受信した合成メッセージ認証コードとを比較する手段と
を備える受信機デバイス。
【請求項３０】
請求項２９に記載の受信機デバイスにおいて、
前記ローカル合成メッセージ認証コードと前記受信した合成メッセージ認証コードとが同一であれば、前記送信ユニットを他のデバイスへ提供する手段と、
前記ローカル合成メッセージ認証コードと前記受信した合成メッセージ認証コードとが異なっていれば、前記メッセージを破棄する手段と
を更に備える受信機デバイス。
【請求項３１】
メッセージに対応する複数の送信ユニットを受信する入力インタフェースと、
前記送信ユニットの各々のためのローカルサブメッセージ認証コードを計算し、
前記複数の送信ユニットの前記ローカルサブメッセージ認証コードに基づいて、ローカル合成メッセージ認証コードを計算し、
前記メッセージの完全性及び／又は真正性を判定するために、前記ローカル合成メッセージ認証コードと、受信した合成メッセージ認証コードとを比較する
ように構成された処理回路と
を備える処理デバイス。
【請求項３２】
請求項３１に記載の処理デバイスにおいて、
前記処理回路は更に、
前記ローカル合成メッセージ認証コードと前記受信した合成メッセージ認証コードとが同一であれば、前記送信ユニットを他のデバイスへ提供し、
前記ローカル合成メッセージ認証コードと前記受信した合成メッセージ認証コードとが異なっていれば、前記送信ユニットを破棄する
ように構成された処理デバイス。
【請求項３３】
メッセージを認証する１つ又は複数の命令群を有する機械読取可能媒体であって、前記命令群はプロセッサによって実行されると前記プロセッサに、
メッセージに対応する複数の送信ユニットを取得させ、
前記送信ユニットの各々のためのローカルサブメッセージ認証コードを計算させ、
前記複数の送信ユニットのための前記ローカルサブメッセージ認証コードに基づいて、ローカル合成メッセージ認証コードを計算させ、
関連するメッセージの完全性及び／又は真正性を判定するために、前記ローカル合成メッセージ認証コードと、受信した合成メッセージ認証コードとを比較させる
機械読取可能媒体。
【請求項３４】
請求項３３に記載の機械読取可能媒体であって、
プロセッサによって実行されると前記プロセッサに更に、
前記ローカル合成メッセージ認証コードと前記受信した合成メッセージ認証コードとが同一であれば、前記送信ユニットを他のデバイスへ提供させ、
前記ローカル合成メッセージ認証コードと前記受信した合成メッセージ認証コードとが異なっていれば、前記送信ユニットを破棄させる
１つ又は複数の命令群を備える機械読取可能媒体。
【発明の詳細な説明】
【技術分野】

【０００１】
様々な構成が通信、特に、メッセージを認証する方法に関する。
【背景技術】
【０００２】
メッセージ認証コード（ＭＡＣ）は、送信メッセージに添付された又は組み込まれた短い情報の断片であり、多くの通信プロトコルに共通する特徴である。ＭＡＣの目的は、（秘密鍵も有する）ベリファイアが、メッセージ及び／又はＭＡＣに対する任意の変更を検出することを可能にすることによって、メッセージの完全性及び真正性の両方を保護することである。典型的なＭＡＣアルゴリズムは、秘密鍵及び任意の長さのメッセージを入力として受け入れ、結果として得られるＭＡＣを計算する。メッセージを受信すると、メッセージのＭＡＣが受信機によって計算され、送信されたＭＡＣに対してチェックされる。もし２つのＭＡＣが一致すればメッセージは処理され、そうでなければ、メッセージは（通常）破棄される。
【０００３】
メッセージは移動時、送信ユニット（ＴＵ）に分解されうる。これは一般に、通信リンクの最大送信ユニット（ＭＴＵ）が元のメッセージの長さより短い場合に起こる。いくつかの状況において、メッセージを構成するＴＵは、順不同で受信機に到着しうる。
【０００４】
一般に、従来のＭＡＣの計算を完了するためにはメッセージ全体が存在しなくてはならない。もしメッセージがＴＵに分解されると、ＭＡＣの計算前に、まずメッセージが受信機によって再構築され（reassembled）ねばならない。例えば、ルータによって送信ユニット又はフラグメントに分解されたデータパケットや、リンク層によってフレームに分解されたデータパケットは、ＭＡＣの計算前に再構築されねばならない。
【０００５】
ＭＡＣ計算は、比較的高価で時間のかかる処理である。従って、レイテンシを最小化し、スループットを最大化するために、可能な限り早くメッセージのＭＡＣ計算を開始することが望ましい。また、このような計算を専用ハードウェアに委託することもしばしば望ましい。
【０００６】
従来のＭＡＣは、メッセージを始めから終わりまで処理することによって、メッセージ全体に対して計算される。もしメッセージが複数の送信ユニット（ＴＵ）（例えばパケット、セグメント等）に分解され、ＴＵが順不同で到着すれば、受信機は、更なるＴＵが到着するまでＭＡＣ計算を実行することができないいくつかのＴＵを有するであろう。最悪の場合、受信機はメッセージのほとんどを有しているが、メッセージの１つ又はごく一部のＴＵを受信していないためにどのＭＡＣ計算も開始できないことがある。もしＭＡＣを計算するためにＴＵを独立して処理することができれば、著しく効率が向上する。
【０００７】
更に、ＴＵが順不同で到着しうる場合、受信ハードウェアは一般に、ＴＵを再構築及びＭＡＣ計算のために汎用処理要素へ渡す。もしＴＵを独立して（例えば、順不同で、及び／又は特定のメッセージのＴＵ全てが到着するのを待たずに）処理することができれば、これらの計算は、受信ハードウェア内で直接実現することができる。
【発明の概要】
【０００８】
本願は、本願の譲受人に譲渡され、参照によって本願に明確に組み込まれた“Composed Message Authentication Code”と題された米国特許仮出願第６０／８６３，２１７号に対する優先権を主張する。
【０００９】
メッセージの完全性ベリフィケーション及び認証を実行するために、送信デバイス上で動作する方法が提供される。送信前、メッセージは複数の送信ユニットに分割される。サブメッセージ認証コードが、各送信ユニットのために取得される。複数の送信ユニットの

サブメッセージ認証コードに基づいて、メッセージ全体のための、合成メッセージ認証コードが取得される。次に、複数の送信ユニットと合成メッセージ認証コードとが送信される。合成メッセージ認証コードは、送信前、複数の送信ユニットのうちの１つに添付されうる。合成メッセージ認証コードは、複数の送信ユニットのサブメッセージ認証コードの関数であることができる。例えば合成メッセージ認証コードは、（１）サブメッセージ認証コードに排他的ＯＲ演算を実行することによって導出される、（２）複数の固定長入力を単一の固定長出力に合成する関数から得られる、（３）サブメッセージ認証コードを合算する関数によって得られる、及び／又は（４）サブメッセージ認証コードを係数として備える多項式を計算する関数によって得られる。サブメッセージ認証コードは、対応する送信ユニットのコンテンツに基づくことができる。

【００１０】

また、（１）メッセージを複数の送信ユニットに分割し、（２）各送信ユニットのためのサブメッセージ認証コードを取得し、（３）複数の送信ユニットのサブメッセージ認証コードに基づいて、メッセージ全体のための合成メッセージ認証コードを取得し、（４）複数の送信ユニットのうちの１つに合成メッセージ認証コードを添付し、及び／又は（５）複数の送信ユニットと合成メッセージ認証コードとを送信するように構成された送信機回路を備える送信デバイスも提供される。サブメッセージ認証コードは、対応する送信ユニットのコンテンツに基づくことができる。

【００１１】

また別の構成は、（１）メッセージを複数の送信ユニットに分割する手段、（２）各送信ユニットのためのサブメッセージ認証コードを取得する手段、（３）複数の送信ユニットのサブメッセージ認証コードに基づいて、メッセージ全体のための合成メッセージ認証コードを取得する手段、（４）複数の送信ユニットのうちの１つに合成メッセージ認証コードを添付する手段、及び／又は（５）複数の送信ユニットと合成メッセージ認証コードとを送信する手段、を備える送信デバイスを提供する。

【００１２】

また、（１）未処理メッセージを受信する入力インタフェース、及び（２）処理回路、を備える処理デバイスも提供される。処理回路は、（ａ）受信した未処理メッセージを複数の送信ユニットに分割し、（ｂ）各送信ユニットのためのサブメッセージ認証コードを取得し、（ｃ）複数の送信ユニットのサブメッセージ認証コードに基づいて、メッセージ全体のための合成メッセージ認証コードを取得し、（ｄ）複数の送信ユニットのうちの１つに合成メッセージ認証コードを添付し、及び／又は（ｅ）複数の送信ユニットと合成メッセージ認証コードとを送信するように構成されうる。

【００１３】

また、送信デバイスでメッセージを認証する１つ又は複数の命令群を有する機械読取可能媒体も提供される。命令群は、プロセッサによって実行されるとプロセッサに、（１）受信したメッセージを複数の送信ユニットに分割させ、（２）各送信ユニットのためのサブメッセージ認証コードを取得させ、（３）複数の送信ユニットのサブメッセージ認証コードに基づいて、メッセージ全体のための合成メッセージ認証コードを取得させ、（４）複数の送信ユニットのうちの１つに合成メッセージ認証コードを添付させ、及び／又は（５）複数の送信ユニットと合成メッセージ認証コードとを送信させる。

【００１４】

受信したメッセージの完全性ベリフィケーション及び認証を実行するために、受信デバイス上で動作する方法が提供される。メッセージに対応する複数の送信ユニットが取得される。各送信ユニットのためにローカルサブメッセージ認証コードが計算される。複数の送信ユニットのためのローカルサブメッセージ認証コードに基づいて、ローカル合成メッセージ認証コードが計算される。関連するメッセージの完全性及び／又は真正性を判定するために、ローカル合成メッセージ認証コードと、受信した合成メッセージ認証コードとが比較される。ローカルサブメッセージ認証コードは、自身が関連する送信ユニットが到着すると計算される。送信ユニットは、順不同で到着することができ、取得されるとバッ

ファされる。送信ユニットは、もしローカル合成メッセージ認証コードと受信した合成メッセージ認証コードとが同一であれば、他のデバイスへ提供されうる。もしローカル合成メッセージ認証コードと受信した合成メッセージ認証コードとが異なっていれば、送信ユニットは破棄されうる。

【００１５】

また、（１）メッセージに対応する複数の送信ユニットを取得し、（２）各送信ユニットのためのローカルサブメッセージ認証コードを計算し、（３）複数の送信ユニットのためのローカルサブメッセージ認証コードに基づいて、合成メッセージ認証コードを計算し、（４）関連するメッセージの完全性及び／又は真正性を判定するために、ローカル合成メッセージ認証コードと、受信した合成メッセージ認証コードとを比較し、（５）もしローカル合成メッセージ認証コードと受信した合成メッセージ認証コードとが同一であれば、送信ユニットを他のデバイスへ提供し、及び／又は（６）もしローカル合成メッセージ認証コードと受信した合成メッセージ認証コードとが異なっていれば、送信ユニットを破棄するように構成された受信機回路を備える受信デバイスが提供される。

【００１６】

また、（１）メッセージに対応する複数の送信ユニットを取得する手段、（２）各送信ユニットのためのローカルサブメッセージ認証コードを計算する手段、（３）複数の送信ユニットのためのローカルサブメッセージ認証コードに基づいて、合成メッセージ認証コードを計算する手段、（４）関連するメッセージの完全性及び／又は真正性を判定するために、ローカル合成メッセージ認証コードと、受信した合成メッセージ認証コードとを比較する手段、（５）もしローカル合成メッセージ認証コードと受信した合成メッセージ認証コードとが同一であれば、送信ユニットを他のデバイスへ提供する手段、及び／又は（６）もしローカル合成メッセージ認証コードと受信した合成メッセージ認証コードとが異なっていれば、メッセージを破棄する手段、を備える受信デバイスが提供される。

【００１７】

また、（１）メッセージに対応する複数の送信ユニットを受信する入力インタフェース、及び（２）処理回路、を備える処理デバイスが提供される。処理回路は、（ａ）各送信ユニットのためのローカルサブメッセージ認証コードを計算し、（ｂ）複数の送信ユニットのためのローカルサブメッセージ認証コードに基づいて、合成メッセージ認証コードを計算し、（ｃ）メッセージの完全性及び／又は真正性を判定するために、ローカル合成メッセージ認証コードと、受信した合成メッセージ認証コードとを比較し、（ｄ）もしローカル合成メッセージ認証コードと受信した合成メッセージ認証コードとが同一であれば、送信ユニットを他のデバイスへ提供し、及び／又は（ｅ）もしローカル合成メッセージ認証コードと受信した合成メッセージ認証コードとが異なっていれば、送信ユニットを破棄するように構成されうる。

【００１８】

受信デバイスでメッセージを認証する１つ又は複数の命令群を有する機械読取可能媒体が提供される。命令群は、プロセッサによって実行されるとプロセッサに、（１）メッセージに対応する複数の送信ユニットを取得させ、（２）各送信ユニットのためのローカルサブメッセージ認証コードを計算させ、（３）複数の送信ユニットのためのローカルサブメッセージ認証コードに基づいて、合成メッセージ認証コードを計算させ、（４）関連するメッセージの完全性及び／又は真正性を判定するために、ローカル合成メッセージ認証コードと、受信した合成メッセージ認証コードとを比較させ、（５）もしローカル合成メッセージ認証コードと受信した合成メッセージ認証コードとが同一であれば、送信ユニットを他のデバイスへ提供させ、（６）もしローカル合成メッセージ認証コードと受信した合成メッセージ認証コードとが異なっていれば、送信ユニットを破棄させる。

【図面の簡単な説明】

【００１９】

【図１】図１は、１つの例に従う合成メッセージ認証コードスキームを実現する送信デバイスの機能構成要素、論理構成要素、ソフトウェア構成要素、及び／又はハードウェア構

成要素を示すブロック図である。
【図２】図２は、１つの例に従う合成メッセージ認証コードスキームを実現するメッセージの処理を示すブロック図である。
【図３】図３は、合成メッセージ認証コードスキームを実現する送信デバイスの例を示すブロック図である。
【図４】図４は、合成メッセージ認証コードスキームを実現する送信デバイス上で動作する方法を示す。
【図５】図５は、１つの例に従う合成メッセージ認証コードスキームを実現する受信デバイスの機能構成要素、論理構成要素、ソフトウェア構成要素、及び／又はハードウェア構成要素を示すブロック図である。
【図６】図６は、合成メッセージ認証コードスキームを実現する受信デバイスの例を示すブロック図である。
【図７】図７は、合成メッセージ認証コードスキームを実現する受信デバイス上で動作する方法を示す。
【図８】図８は、１つの例に従っていかにしてメッセージが送信デバイスから受信デバイスへ送信されるかのネットワーク概観を示すブロック図である。
【発明を実施する形態】
【００２０】
以下の説明において、具体的な詳細が、例及び構成の完全な理解を提供するために与えられる。しかし、例及び構成はこれら具体的詳細なしでも実現されうることが、当業者によって理解されるであろう。例えば、不必要な詳細で例及び構成を不明確にしないために、回路はブロック図内に示されない。
【００２１】
また、例及び構成は、フローチャート、フロー図、構成図、又はブロック図として示される処理として説明されうる。フローチャートは動作を連続した処理として示すが、動作の多くは、並行して又は同時に実行することができる。更に、動作の順番は並べ替えることができる。処理は、その動作が完了すると終了する。処理は、方法、関数、手順、サブルーチン、サブプログラム等に対応しうる。処理が関数に対応する場合、処理の終了は、呼び出し関数やメイン関数へ関数が戻ることに対応する。
【００２２】
更に、記憶媒体は、データを格納する１つ又は複数のデバイスを表し、読取専用メモリ（ＲＯＭ）、ランダム・アクセス・メモリ（ＲＡＭ）、磁気ディスク記憶媒体、光記憶媒体、フラッシュメモリデバイス、及び／又は情報を格納するその他の機械読取可能媒体を含む。「機械読取可能媒体」という用語は、移動式又は固定式記憶デバイス、光記憶デバイス、無線チャネル、及び、命令及び／又はデータを格納、包含、あるいは搬送することができるその他様々な媒体を含むことができるが、それらに限定されない。
【００２３】
更に、構成は、ハードウェア、ソフトウェア、ファームウェア、ミドルウェア、マイクロコード、又はそれらの組合せによって実現することができる。ソフトウェア、ファームウェア、ミドルウェア、又はマイクロコードによって実現される場合、必要なタスクを実行するプログラムコードやコードセグメントは、例えば記憶媒体又はその他の記憶手段のような機械読取可能媒体に格納されうる。プロセッサは、必要なタスクを実行することができる。コードセグメントは、手順、関数、サブプログラム、プログラム、ルーチン、サブルーチン、モジュール、ソフトウェアパッケージ、クラス、又は命令、データ構成、あるいはプログラム文の組合せを表すことができる。コードセグメントは、情報、データ、引数、パラメータ、又はメモリコンテンツを渡し、受け取ることによって、別のコードセグメント又はハードウェア回路に接続されることができる。情報、引数、パラメータ、データ等は、メモリ共有、メッセージパッシング、トークンパッシング、及びネットワーク送信を特に含む適切な手段を介して、パス、転送、又は送信されることができる。
【００２４】

以下の説明において、ある用語が、１つ又は複数の例のある特徴を説明するために用いられる。「メッセージ認証コード」という用語は、メッセージの完全性及び真正性の両方を保護することができる、送信メッセージに組み込まれた又は添付された情報の任意の断片を称する。

【００２５】

１つの新規な特徴は、サブメッセージ認証コード（ＳＭＡＣ）が各ＴＵに関して独立して計算される、合成メッセージ認証コード（composed message authentication code）（ＣＭＡＣ）を提供する。

【００２６】

図１は、１つの例に従う合成メッセージ認証コードスキームを実現する送信デバイスの機能構成要素、論理構成要素、ソフトウェア構成要素、及び／又はハードウェア構成要素を示すブロック図である。長さＬＭのメッセージ１０２が取得される。（従来のシステムによって行われるように）メッセージ全体のためのＭＡＣを計算するのではなく、メッセージセグメンタ１０４が、メッセージを複数の送信ユニット（ＴＵ）に分割する。ＴＵは、等しい又は異なる長さＬＳであることができ、ＬＳ＜ＬＭである。認証コード生成器１０８がその後、各ＴＵのためのサブメッセージ認証コード（ＳＭＡＣ）を生成する。各ＴＵのためのＳＭＡＣは、それらを結合させて合成メッセージ認証コード（ＣＭＡＣ）１１６を形成する合成ＭＡＣ生成器１１４へ送られる。送信ユニット１０６は、受信者１１８へ送信される。ＣＭＡＣ１１６もまた、受信者１１８へ送信される。例えばＣＭＡＣ１１６は、受信者１１８へ送信される最後のＴＵに添付することができる。

【００２７】

また別の実現形態において、メッセージのためのＳＭＡＣとＣＭＡＣとの両方が、メッセージの完全性及び／又は真正性をベリファイするために受信者へ送られる。

【００２８】

図２は、１つの例に従う合成メッセージ認証コードスキームを実現するメッセージの処理を示すブロック図である。メッセージ２０２は、複数の短い長さの送信ユニット（ＴＵ）Ａ　２０４、Ｂ　２０６、乃至Ｎ　２０８に分割、セグメント化、又は区切られる。各ＴＵについてサブメッセージ認証コード（ＳＭＡＣ）が取得される。ＳＭＡＣは、関連するＴＵ内のデータ又は情報に基づいて計算された値であることができる。例えば$SMAC_A$は、ＴＵ　Ａ　２０４内の情報から計算することができる。

【００２９】

１つの実現形態において、ＣＭＡＣは、特定のメッセージのためのＳＭＡＣ全てに基づいて取得することができる。例えば、値$CMAC_{A...N}$は、ＴＵ　Ａ　２０４、ＴＵ　Ｂ　２０６、乃至ＴＵ　Ｎ　２０８のためのＳＭＡＣ（すなわち$SMAC_A$、$SMAC_B$、乃至$SMAC_N$）に基づいて取得することができる。$CMAC_{A...N}$は、メッセージ全体の完全性及び／又は真正性をベリファイするためにそれを用いる受信者へ送信することができる。

【００３０】

いくつかの実現形態において、ＳＭＡＣは、送信のために、自身が対応するＴＵに添付されうる。このように、ＴＵを受信すると、受信者は、添付されたＳＭＡＣに基づいてＴＵの完全性及び／又は真正性をベリファイすることができる。

【００３１】

自身のＳＭＡＣを有する小さいサイズのＴＵを送信することによって、受信者は、各ＴＵを受信するとそれを前処理することが可能となり、それによって特定のメッセージのベリファイ又は認証の遅延が低減される。従来技術において、一般にメッセージ全体が、そのＭＡＣの計算前に受信されるが、本特徴は、メッセージのＴＵ又はセグメントの各々が受信されると、それらのＳＭＡＣを計算する。最後のセグメント又はＴＵを受信すると、受信者は単に、以前計算されたＳＭＡＣに基づいて、受信したメッセージのＣＭＡＣを計算する。ＣＭＡＣの計算は、メッセージ全体に対するＭＡＣの計算よりも時間消費が少ない。これは、いったん全ての部分が受信されるとメッセージ全体を分析しなくてはならな

いのではなく、予め計算されたコード（ＳＭＡＣ）を用いるためである。

【００３２】

ＳＭＡＣは、送信のために必ずしも各ＴＵに添付される必要はない。代わりに、ＳＭＡＣは、ＴＵとともに受信者へ送信されるＣＭＡＣを生成するために、送信デバイスによって（内部で）用いられる。ＣＭＡＣは、ＴＵに添付して、あるいはＴＵとは別に送信することができる。受信者はその後、（各ＴＵを受信すると）自身のＳＭＡＣを計算し、受信したＣＭＡＣとその後比較することができるローカルＣＭＡＣを生成することによって、メッセージの完全性及び／又は真正性をベリファイすることができる。

【００３３】

メッセージのＣＭＡＣは、メッセージの関連するＴＵのＳＭＡＣの関数として計算される。すなわち、メッセージＭがＮ個の送信ユニットを有する場合、ＣＭＡＣは、

【数１】

$$CMAC(M) = F(SMAC(TU_0), SMAC(TU_1), \ldots SMAC(TU_{N-1}))$$

【００３４】

と表される。ここでＦは、複数の固定長入力（例えばＳＭＡＣ）を、単一の固定長出力（例えばＣＭＡＣ）に合成する関数である。関数Ｆの１つの実現形態は、自身の入力（ＳＭＡＣ）全ての排他的ｏｒを計算する関数であることができる。別の実現形態は、自身の入力（ＳＭＡＣ）を望まれる出力長さ（ＣＭＡＣ）で割ったときの剰余の全てを合計する関数Ｆを提供する。また別の実現形態は、係数として入力（ＳＭＡＣ）を用いて多項式を計算する関数を提供する。これらは、複数のＳＭＡＣに基づいてＣＭＡＣを計算するために用いられうる関数のほんのいくつかの例である。他のタイプの関数Ｆも、本スキームによって包含される。

【００３５】

図３は、合成メッセージ認証コードスキームを実現する送信デバイスの例を示すブロック図である。送信デバイス３０２は、送信機３０４と、汎用プロセッサ３０６とを含むことができる。送信機３０４によって、送信デバイス３０２は、通信リンクを介して情報（例えばメッセージ）を送信することが可能となる。１つの実現形態によると、送信機３０４は、メッセージを複数のＴＵに分割し、各ＴＵのＳＭＡＣを取得し、ＳＭＡＣに基づいて各メッセージのＣＭＡＣを取得し、ＴＵとＣＭＡＣとを送信するように構成されたハードウェア部品及び／又はソフトウェア構成要素を含むことができる。例えば送信機３０４ハードウェアは、図１及び／又は２に示す動作及び機能を実現することができる。これらの動作及び機能を送信機３０４ハードウェア上で実現することによって、汎用プロセッサ３０６の処理負担が軽減される。

【００３６】

図４は、合成メッセージ認証コードスキームを実現する送信デバイス上で動作する方法を示す。メッセージが複数の送信ユニット（ＴＵ）に分割される（４０２）。サブメッセージ認証コード（ＳＭＡＣ）が、各送信ユニットについて取得される（４０４）。１つの実現形態において、ＳＭＡＣは、自身が対応するＴＵに添付されることができる（４０６）。複数のＴＵが受信者へ送信される（４０８）。受信者はその後、受信した各ＴＵのためのローカルＳＭＡＣを計算し、ローカルＳＭＡＣと、各ＴＵとともに受信したＳＭＡＣとを比較することによって、メッセージの完全性及び／又は真正性をベリファイすることができる。

【００３７】

ＳＭＡＣは、必ずしも各ＴＵに添付される必要、及び／又は各ＴＵとともに送信される必要はない。代わりに、合成メッセージ認証コード（ＣＭＡＣ）を、送信ユニットのＳＭＡＣに基づいて、メッセージ全体について取得することができる（４１０）。ＳＭＡＣは、ＣＭＡＣを計算するために、送信機デバイスによって内部で用いられる。ＣＭＡＣが受

信者へ送信される（４１２）。例えばＣＭＡＣは、最後のＴＵに添付され、その後送信されることができる。受信者はその後、受信した各ＴＵのためのローカルＳＭＡＣを計算し、ローカルＳＭＡＣに基づいてローカルＣＭＡＣを計算し、ローカルＣＭＡＣと受信したＣＭＡＣとを比較することによって、メッセージの完全性及び／又は真正性をベリファイすることができる。

【００３８】

図５は、１つの例に従う合成メッセージ認証コードスキームを実現する受信機デバイスの機能構成要素、論理構成要素、ソフトウェア構成要素、及び／又はハードウェア構成要素を示すブロック図である。複数のメッセージ送信ユニット（ＴＵ）５０２が受信される。各ＴＵが受信されると、サブメッセージ認証コード生成器５０４は、ＴＵのコンテンツに基づいてＳＭＡＣを生成する。すなわち、生成器５０４は、ＴＵ内のペイロードや情報に基づいて、自身のローカルＳＭＡＣを生成する。合成ＭＡＣ生成器５１２は、受信したＴＵのためのローカルＳＭＡＣを取得し、いったん全てのＴＵを受信すると、ローカルＳＭＡＣに基づいてローカルＣＭＡＣを計算する。ＣＭＡＣ認証器５１４はその後、ローカルＣＭＡＣと、（一般に最後に送信されたＴＵに添付される）受信したＣＭＡＣとを比較し、メッセージ全体の完全性及び／又は真正性を判定する。もし、ローカルＣＭＡＣと受信したＣＭＡＣとが同一であれば、ＣＭＡＣ認証は成功であり（５１６）、受信メッセージを構成しているＴＵは、メッセージバッファ５１０からアップストリームで受信機デバイスの他の構成要素へ渡される。もしローカルＣＭＡＣと受信したＣＭＡＣが同一でなければ、認証は失敗であり（５１８）、メッセージのためのＴＵは破棄することができる。

【００３９】

図６は、合成メッセージ認証コードスキームを実現する受信デバイスの例を示すブロック図である。受信デバイス６０２は、受信機６０４と、汎用プロセッサ６０６とを含むことができる。受信機６０４によって、受信デバイス６０２は、通信リンクを介して情報（例えばメッセージ）を受信することが可能となる。１つの実現形態によると、受信機６０４は、複数のＴＵを受信し、各ＴＵのためのローカルＳＭＡＣを取得し、ローカルＳＭＡＣに基づいてローカルＣＭＡＣを取得し、受信したメッセージの完全性及び／又は真正性を判定するためにローカルＳＭＡＣ／ＣＭＡＣと受信したＳＭＡＣ／ＣＭＡＣを比較するように構成されたハードウェア部品及び／又はソフトウェア構成要素を含むことができる。例えば受信機６０４ハードウェアは、図５に示す動作及び機能を実現することができる。これらの動作及び機能を受信機６０４ハードウェア上で実現することによって、汎用プロセッサ６０６の処理負荷が軽減される。

【００４０】

図７は、合成メッセージ認証コードスキームを実現する受信デバイス上で動作する方法を示す。メッセージに対応する複数の送信ユニットが取得される（７０２）。これらの送信ユニットは、順不同で受信することができ、異なるサイズであることができる。各送信ユニットのためのローカルサブメッセージ認証コード（ＳＭＡＣ）が計算又は取得される（７０４）。各送信ユニットが受信されると、送信ユニットが、順番が狂って、すなわち順不同で受信されても、各送信ユニットのためのローカルサブメッセージ認証コード（ＳＭＡＣ）を計算することができる。ローカル合成メッセージ認証コード（$CMAC_{Local}$）が、複数の送信ユニットのためのローカルサブメッセージ認証コード（ＳＭＡＣ）に基づいて計算又は取得される（７０６）。ローカル合成メッセージ認証コード（$CMAC_{Local}$）は、受信した送信ユニットの合成メッセージ認証コード（$CMAC_{Received}$）と比較され、関連するメッセージの完全性及び／又は真正性が判定される（７０８）。もしローカルメッセージ認証コードと受信したメッセージ認証コードとが異なっていれば、メッセージは破棄される（７１０）。

【００４１】

図８は、１つの例に従っていかにしてメッセージが送信デバイスから受信デバイスへ送信されうるかのネットワーク概観を示すブロック図である。送信デバイス８０２は、メッセージを複数の送信ユニットTU_0、TU_1、TU_2、TU_3、TU_4、TU_{N-1}（こ

こでＮは整数である）に分割し、例えばインターネットや無線通信ネットワークのようなネットワーク８０６を介してそれらを受信デバイス８０４へ送信する。送信前に、送信デバイス８０２は、各ＴＵのためのＳＭＡＣを計算し、ＳＭＡＣに基づいてメッセージのためのＣＭＡＣを計算する。ＣＭＡＣはＴＵのうちの１つに添付される。送信デバイス８０２は、ＴＵを、順番通りに又は順不同で送信することができる。しかし、ネットワーク８０６を移動中、ＴＵは異なる送信経路を通り、順不同で到着することがある。例えばいくつかのＴＵは、ルータ８０８やその他のネットワークデバイスによって遅延させられ、後から送信されたＴＵより後に到着することがある。

【００４２】

受信デバイス８０２は、順不同（TU_3、TU_0、TU_2、TU_1、TU_{N-1}、TU_4）でＴＵを受信しうる。ＳＭＡＣは、各ＴＵが受信されると、各ＴＵについて受信デバイス８０４によって計算される。最後のＴＵを受信すると、ローカルＣＭＡＣが、受信デバイス８０４によって計算される。このローカルＣＭＡＣは、メッセージの完全性及び／又は真正性を判定するために、送信デバイス８０２によって送信されたＣＭＡＣと比較される。もしローカルＣＭＡＣが送信されたＣＭＡＣと一致すれば、メッセージの完全性がベリファイされ、そのメッセージは真正であると見なされる。もしローカルＣＭＡＣと受信したＣＭＡＣが一致しなければ、メッセージを破棄することができる。

【００４３】

様々な実現形態において、送信デバイス８０２及び／又は受信デバイス８０４は、無線電話、基地局、アクセスポイント、コンピュータサーバ、ネットワークルータ、及び／又は無線ネットワーク及び／又は有線ネットワークを介して通信するその他の通信デバイスであることができる。

【００４４】

図１乃至図８に示す構成要素、ステップ、及び／又は機能のうちの１つ又は複数は、本発明から逸脱することなく、単一の構成要素、ステップ、又は機能に再配置及び／又は結合されうる、あるいはいくつかの構成要素、ステップ、又は機能において具現化されうる。更なる要素、構成要素、ステップ、及び／又は機能もまた、本発明から逸脱することなく追加することができる。図１、３、５、６、及び／又は８に示す装置、デバイス、及び／又は構成要素は、図２、４、及び／又は７に示す方法、特徴、又はステップのうちの１つ又は複数を実行するように構成されうる。

【００４５】

当業者は更に、本明細書に開示された例及び構成に関連して記述された様々な例示的論理ブロック、モジュール、回路、及びアルゴリズムステップが、電子工学的ハードウェア、コンピュータソフトウェア、又はそれらの組合せとして実現されうることをよく理解するであろう。ハードウェアとソフトウェアとの相互置換性を明確に説明するために、様々な例示的構成要素、ブロック、モジュール、回路、及びステップが、それらの機能の観点から一般的に説明された。このような機能が、ハードウェアとして実現されるかソフトウェアとして実現されるかは、システム全体に課された設計制約及び特定のアプリケーションによる。

【００４６】

上述した例及び構成は単に例であり、本発明を限定するものとして解釈されないことが留意されるべきである。この例及び構成の説明は、例示的であることが意図されており、特許請求の範囲の範囲を限定することは意図されていない。このように、本教示は、他のタイプの装置に容易に適用可能であり、多くの代替例、修正例、及び変形例が当業者には明らかであるだろう。

【図１】

図 1

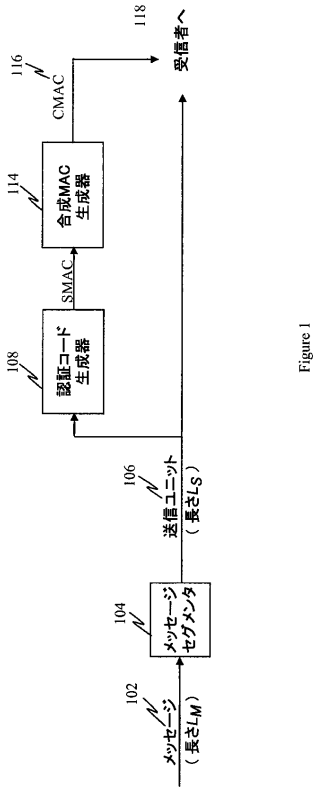


Figure 1

【図２】

図 2

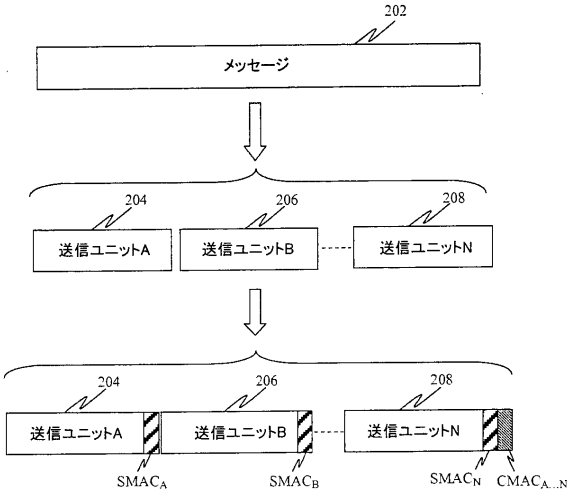


Figure 2

【図３】

図 3

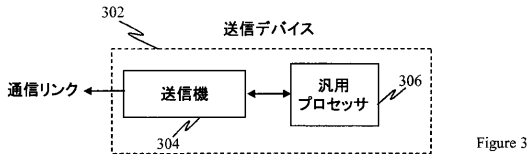


Figure 3

【図４】

図 4

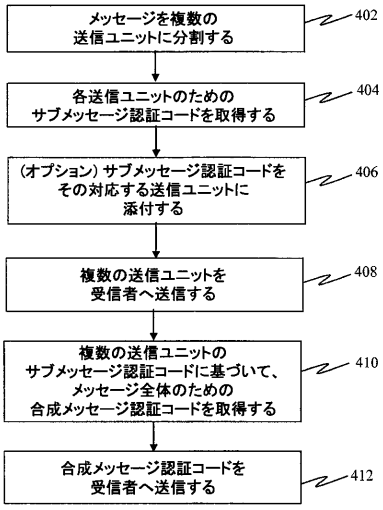


Figure 4

【図５】

図 5

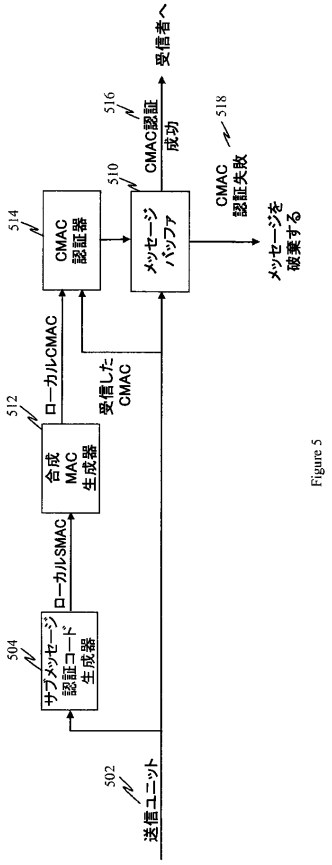


Figure 5

【図６】

図 6

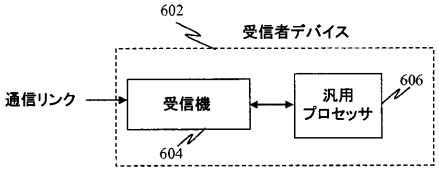


Figure 6

【図７】

図 7

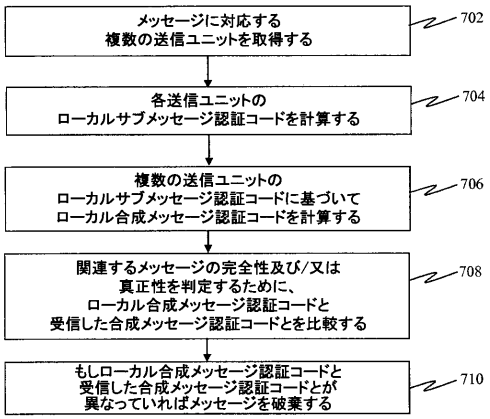


Figure 7

【図８】

図 8

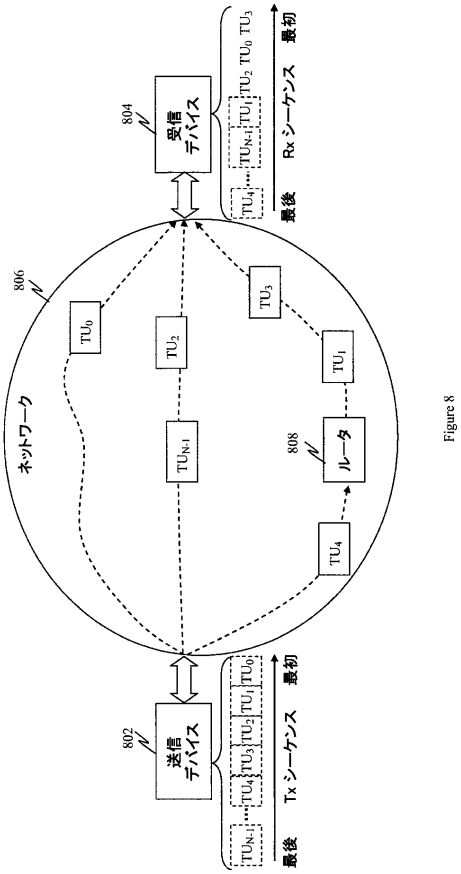


Figure 8

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2007/082566

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04Q7/38 H04L29/06 H04L9/32

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)
H04L H04Q

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, WPI Data, PAJ, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 98/47264 A (SIEMENS AG [DE]; HANCK MARTINA [DE]; HOFFMANN GERHARD [DE]; LUKAS KLAU) 22 October 1998 (1998-10-22)	1,3-7,9, 10, 12-14, 16,18, 19,21, 23-34
Y	page 1, line 12 - page 2, line 12 page 3, line 4 - line 18 page 5, line 1 - line 8 page 5, line 19 - page 6, line 5 page 7, line 1 - page 9, line 20 page 10, line 9 - line 10 figure 1	2,8,11, 15,17,20

-/--

[X] Further documents are listed in the continuation of Box C. [X] See patent family 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 May 2008	29/05/2008

Name and mailing address of the ISA/	Authorized officer
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	Hartweg, Norman

Form PCT/ISA/210 (second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2007/082566

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	WO 2006/086554 A (SINETT CORP [US]; CHOUDHURY ABHIJIT K [US]; SHUKLA HIMANSHU [US]; LEWI) 17 August 2006 (2006-08-17)	2,8,11, 15,17,20
A	paragraph [0006] - paragraph [0009] paragraph [0026]	1,10,14, 16,19, 21,27, 29,31,33
A	US 2003/126303 A1 (KADAKIA VIRAL [US] ET AL) 3 July 2003 (2003-07-03) paragraph [0013] paragraph [0029] - paragraph [0033] figure 4	1,10,14, 16,19, 21,27, 29,31,33
A	US 2004/142710 A1 (LIANG JIE [US]) 22 July 2004 (2004-07-22) paragraph [0015] - paragraph [0021]	1,10,14, 16,19, 21,27, 29,31,33

Form PCT/ISA/210 (continuation of second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/US2007/082566

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9847264 A	22-10-1998	AU 723002 B2	17-08-2000
		AU 7028298 A	11-11-1998
		EP 0976221 A1	02-02-2000
		ES 2219883 T3	01-12-2004
		ID 22750 A	09-12-1999
		JP 2000513115 T	03-10-2000
WO 2006086554 A	17-08-2006	NONE	
US 2003126303 A1	03-07-2003	NONE	
US 2004142710 A1	22-07-2004	NONE	

Form PCT/ISA/210 (patent family annex) (April 2005)

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,LV,MC,MT,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,BH,BR,BW,BY,BZ,CA,CH,CN,CO,CR,CU,CZ,DE,DK,DM,DO,DZ,EC,EE,EG,ES,FI,GB,GD,GE,GH,GM,GT,HN,HR,HU,ID,IL,IN,IS,JP,KE,KG,KM,KN,KP,KR,KZ,LA,LC,LK,LR,LS,LT,LU,LY,MA,MD,ME,MG,MK,MN,MW,MX,MY,MZ,NA,NG,NI,NO,NZ,OM,PG,PH,PL,PT,RO,RS,RU,SC,SD,SE,SG,SK,SL,SM,SV,SY,TJ,TM,TN,TR,TT,TZ,UA,UG,US,UZ,VC,VN,ZA,ZM,ZW

(74)代理人 100109830
弁理士 福原 淑弘
(74)代理人 100075672
弁理士 峰 隆司
(74)代理人 100095441
弁理士 白根 俊郎
(74)代理人 100084618
弁理士 村松 貞男
(74)代理人 100103034
弁理士 野河 信久
(74)代理人 100119976
弁理士 幸長 保次郎
(74)代理人 100153051
弁理士 河野 直樹
(74)代理人 100140176
弁理士 砂川 克
(74)代理人 100100952
弁理士 風間 鉄也
(74)代理人 100101812
弁理士 勝村 紘
(74)代理人 100070437
弁理士 河井 将次
(74)代理人 100124394
弁理士 佐藤 立志
(74)代理人 100112807
弁理士 岡田 貴志
(74)代理人 100111073
弁理士 堀内 美保子
(74)代理人 100134290
弁理士 竹内 将訓
(74)代理人 100127144
弁理士 市原 卓三
(74)代理人 100141933
弁理士 山下 元
(72)発明者 パッドン、マイケル
アメリカ合衆国、カリフォルニア州 ９２１２１、サン・ディエゴ、モアハウス・ドライブ ５７７５
(72)発明者 エスコット、エイドリアン
アメリカ合衆国、カリフォルニア州 ９２１２１、サン・ディエゴ、モアハウス・ドライブ ５７７５
(72)発明者 ローズ、グレゴリー・ゴードン

アメリカ合衆国、カリフォルニア州　９２１２１、サン・ディエゴ、モアハウス・ドライブ　５７７５
(72)発明者　ホークス、フィリップ・エム.
アメリカ合衆国、カリフォルニア州　９２１２１、サン・ディエゴ、モアハウス・ドライブ　５７７５

Ｆターム(参考) 5J104 AA08　AA12　AA16　EA02　EA10　EA16　LA06　NA02　NA38　PA07