(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第6382980号
(P6382980)

(45)発行日　平成30年8月29日(2018.8.29)　(24)登録日　平成30年8月10日(2018.8.10)

(51)Int.Cl.			F I		
H04L	***9/32***	***(2006.01)***	H04L	9/00	675A
H04L	***9/36***	***(2006.01)***	H04L	9/00	685
			H04L	9/00	675B
			H04L	9/00	675D

請求項の数 28　(全 30 頁)

(21)出願番号	特願2016-536294 (P2016-536294)
(86)(22)出願日	平成26年8月11日 (2014.8.11)
(65)公表番号	特表2016-534629 (P2016-534629A)
(43)公表日	平成28年11月4日 (2016.11.4)
(86)国際出願番号	PCT/US2014/050521
(87)国際公開番号	WO2015/026551
(87)国際公開日	平成27年2月26日 (2015.2.26)
審査請求日	平成29年7月14日 (2017.7.14)
(31)優先権主張番号	61/869,429
(32)優先日	平成25年8月23日 (2013.8.23)
(33)優先権主張国	米国(US)
(31)優先権主張番号	14/148,342
(32)優先日	平成26年1月6日 (2014.1.6)
(33)優先権主張国	米国(US)

早期審査対象出願

(73)特許権者　507364838
クアルコム，インコーポレイテッド
アメリカ合衆国　カリフォルニア　９２１２１　サン　ディエゴ　モアハウス　ドライブ　５７７５
(74)代理人　100108453
弁理士　村山　靖彦
(74)代理人　100163522
弁理士　黒田　晋平
(72)発明者　ジュビン・ホセ
アメリカ合衆国・カリフォルニア・９２１２１－１７１４・サン・ディエゴ・モアハウス・ドライヴ・５７７５

最終頁に続く

(54)【発明の名称】プリコード化されたパケットのハッシュ処理を使用したセキュアなコンテンツ配信

(57)【特許請求の範囲】

【請求項１】

ワイヤレス通信におけるセキュアなコンテンツ配信の方法であって、

配信されるべきコンテンツを含む複数のパケットを取得するステップと、

コード化されたパケットのセットを生成するために、あらかじめ定義されたコードを使用して前記複数のパケットを符号化するステップと、

複数のハッシュを生成するために、前記符号化されたパケットのセットのうちの複数のパケットの各々をハッシュ処理するステップと、

通信ネットワークを介して前記複数のハッシュを送信するステップと、

前記複数のハッシュを送信することの後に、前記符号化されたパケットのセットのうちの各パケットを送信するステップと

を備え、

前記符号化されたパケットのセットのうちの各パケットを送信するステップが、

前記符号化されたパケットのセットのうちの少なくとも1つのパケットを選択するステップと、

前記複数のハッシュを送信することとは無関係に、ワイヤレス通信ネットワーク上で前記少なくとも1つの選択されたパケットをブロードキャストするステップと、

前記符号化されたパケットのセットのうちの各パケットをブロードキャストし終えるまで、前記選択することと、前記ブロードキャストすることとを繰り返すステップと

を備える、方法。

【請求項２】
前記複数のハッシュを送信するステップが、
前記複数のハッシュを少なくとも1つのハッシュのパケットに結合するステップと、
前記少なくとも1つのハッシュのパケットに電子署名で署名するステップ、または、前記少なくとも1つのハッシュのパケットを暗号化するステップのうちの少なくとも1つと、
前記通信ネットワークを介して前記少なくとも1つのハッシュのパケットを送信するステップと
をさらに備える、請求項1に記載の方法。
【請求項３】
前記符号化されたパケットのセットのうちの少なくとも1つのパケットを選択するステップが、
前記符号化されたパケットのセットのうちの少なくとも1つのパケットをランダムに選択するステップ
を備える、請求項1に記載の方法。
【請求項４】
コード化されたパケットのセットを生成するために、あらかじめ定義されたコードを使用して複数のパケットを符号化するステップが、
前記複数のパケットの中のパケットの個数(k個)を決定するステップと、
前記符号化されたパケットのセットの中のパケットの個数(m個)を決定するステップと、
前記あらかじめ定義されたコードを使用して前記k個のパケットを符号化して、前記m個の符号化されたパケットを生成するステップであって、mがkよりも大きい、ステップと
を備える、請求項1に記載の方法。
【請求項５】
前記通信ネットワークを介してk、mおよび前記あらかじめ定義されたコードを送信するステップ
をさらに備える、請求項4に記載の方法。
【請求項６】
前記通信ネットワークを介して前記複数のハッシュを送信するステップに関連付けられたオーバーヘッドに少なくとも部分的に基づいて、前記符号化されたパケットのセットの中の前記パケットの個数(m個)を決定するステップ
をさらに備える、請求項4に記載の方法。
【請求項７】
前記符号化されたパケットのセットのうちの少なくとも1つのパケットをランダムに選択するステップと、
前記ワイヤレス通信ネットワーク上での前記少なくとも1つのランダムに選択されたパケットの前記ブロードキャストに関連付けられたオーバーヘッドに少なくとも部分的に基づいて、前記符号化されたパケットのセットの中の前記パケットの個数(m個)を決定するステップと
をさらに備える、請求項4に記載の方法。
【請求項８】
前記通信ネットワークを介して前記複数のハッシュを送信するステップが、
前記複数のハッシュをワイヤレス送信するステップ
を備える、請求項1に記載の方法。
【請求項９】
前記通信ネットワークを介して前記複数のハッシュを送信するステップが、
ワイヤードバックホールを介して送信するステップ
を備える、請求項1に記載の方法。
【請求項１０】
ワイヤレス通信におけるセキュアなコンテンツ配信の装置であって、

配信されるべきコンテンツを含む複数のパケットを取得するための手段と、
コード化されたパケットのセットを生成するために、あらかじめ定義されたコードを使用して前記複数のパケットを符号化するための手段と、
複数のハッシュを生成するために、前記符号化されたパケットのセットのうちの複数のパケットの各々をハッシュ処理するための手段と、
通信ネットワークを介して前記複数のハッシュを送信するための手段と、
前記複数のハッシュを送信することの後に、前記符号化されたパケットのセットのうちの各パケットを送信するための手段と
を備え、
前記符号化されたパケットのセットのうちの各パケットを送信するための手段が、
前記符号化されたパケットのセットのうちの少なくとも1つのパケットを選択するための手段と、
前記複数のハッシュを送信することとは無関係に、ワイヤレス通信ネットワーク上で前記少なくとも1つの選択されたパケットをブロードキャストするための手段と、
前記符号化されたパケットのセットのうちの各パケットをブロードキャストし終えるまで、前記選択することと、前記ブロードキャストすることとを繰り返すための手段と
を備える、装置。
【請求項１１】
前記複数のハッシュを送信するための手段が、
前記複数のハッシュを少なくとも1つのハッシュのパケットに結合するための手段と、
前記少なくとも1つのハッシュのパケットに電子署名で署名するための手段、または、前記少なくとも1つのハッシュのパケットを暗号化するための手段のうちの少なくとも1つと、
前記通信ネットワークを介して前記少なくとも1つのハッシュのパケットを送信するための手段と
をさらに備える、請求項10に記載の装置。
【請求項１２】
前記符号化されたパケットのセットのうちの少なくとも1つのパケットを選択するための手段が、
前記符号化されたパケットのセットのうちの少なくとも1つのパケットをランダムに選択するための手段
を備える、請求項10に記載の装置。
【請求項１３】
前記複数のパケットを符号化するための手段が、
前記複数のパケットの中のパケットの個数(k個)を決定するための手段と、
前記符号化されたパケットのセットの中のパケットの個数(m個)を決定するための手段と、
前記あらかじめ定義されたコードを使用して前記k個のパケットを符号化して、前記m個の符号化されたパケットを生成するための手段であって、mがkよりも大きい、手段と
を備える、請求項10に記載の装置。
【請求項１４】
前記通信ネットワークを介してk、mおよび前記あらかじめ定義されたコードを送信するための手段
をさらに備える、請求項13に記載の装置。
【請求項１５】
前記符号化するための手段が、
通信ネットワークを介して前記複数のハッシュを送信するステップに関連付けられたオーバーヘッドに少なくとも部分的に基づいて、前記符号化されたパケットのセットの中の前記パケットの個数(m個)を決定するための手段
を備える、請求項13に記載の装置。

【請求項１６】
前記符号化されたパケットのセットのうちの少なくとも1つのパケットをランダムに選択するための手段と、
前記符号化するための手段が、
前記ワイヤレス通信ネットワーク上での前記少なくとも1つのランダムに選択されたパケットの前記ブロードキャストに関連付けられたオーバーヘッドに少なくとも部分的に基づいて、前記符号化されたパケットのセットの中の前記パケットの個数(m個)を決定するための手段
を備える、請求項13に記載の装置。
【請求項１７】
ワイヤレス通信におけるセキュアなコンテンツ配信のために構成されたデバイスであって、
プロセッサと、
前記プロセッサと電子通信しているメモリと、
前記メモリに記憶されている命令であって、
配信されるべきコンテンツを含む複数のパケットを取得することと、
コード化されたパケットのセットを生成するために、あらかじめ定義されたコードを使用して複数のパケットを符号化することと、
複数のハッシュを生成するために、前記符号化されたパケットのセットのうちの複数のパケットの各々をハッシュ処理することと、
通信ネットワークを介して前記複数のハッシュを送信することと、
前記複数のハッシュを送信することの後に、前記符号化されたパケットのセットのうちの各パケットを送信することと
を行うように前記プロセッサによって実行可能である命令と
を備え、
前記符号化されたパケットのセットのうちの各パケットを送信することを行うようにする命令が、
前記符号化されたパケットのセットのうちの少なくとも1つのパケットを選択することと、
前記複数のハッシュを送信することとは無関係に、ワイヤレス通信ネットワーク上で前記少なくとも1つの選択されたパケットをブロードキャストすることと、
前記符号化されたパケットのセットのうちの各パケットをブロードキャストし終えるまで、前記選択することと前記ブロードキャストすることとを繰り返すことと
を行うようにする命令を備える、デバイス。
【請求項１８】
ワイヤレス通信におけるセキュアなコンテンツ配信の方法であって、
第1のデバイスから配信されるべきコンテンツの符号化されたパケットのセットのうちの各パケットをハッシュ処理することによって得られる複数のハッシュを受信するステップと、
前記複数のハッシュを受信することとは無関係なブロードキャスト送信を介して、前記配信されるべきコンテンツの前記符号化されたパケットのセットのうちのあるパケットを受信するステップと、
前記受信された複数のハッシュに少なくとも部分的に基づいて前記受信されたパケットを検証するステップと、
前記受信された複数のハッシュに少なくとも部分的に基づいて前記受信されたパケットを検証することの後に、あらかじめ定義されたコードを使用して前記受信されたパケットを復号するステップと、
前記配信されるべきコンテンツを復号し終えるまで、前記符号化されたパケットのセットのうちのあるパケットを受信することと、前記受信されたパケットを検証することと、前記受信されたパケットを復号することとを繰り返すステップ

を備える方法。
【請求項１９】
前記通信ネットワークを介して前記複数のハッシュを送信するステップが、専用狭域通信(DSRC)ベースのネットワークを介して前記複数のハッシュを送信するステップを備える、請求項1に記載の方法。
【請求項２０】
認証局によって作成された証明書失効リストを取得するステップであって、前記証明書失効リストが前記符号化されるべき複数のパケットを含む、ステップをさらに備える、請求項1に記載の方法。
【請求項２１】
前記複数のハッシュを送信することの前に、
前記複数のハッシュに電子署名で署名するステップ、または、前記複数のハッシュを暗号化するステップのうちの少なくとも1つ
をさらに備える、請求項1に記載の方法。
【請求項２２】
前記通信ネットワークを介して前記複数のハッシュを送信するための手段が、専用狭域通信(DSRC)ベースのネットワークを介して前記複数のハッシュを送信するための手段を備える、請求項10に記載の装置。
【請求項２３】
認証局によって作成された証明書失効リストを取得するための手段であって、前記証明書失効リストが前記符号化されるべき複数のパケットを含む、手段をさらに備える、請求項10に記載の装置。
【請求項２４】
前記複数のハッシュを送信することの前に、
前記複数のハッシュに電子署名で署名するための手段、または、前記複数のハッシュを暗号化するための手段のうちの少なくとも1つ
をさらに備える、請求項10に記載の装置。
【請求項２５】
前記符号化されたパケットのセットのうちの前記パケットが、前記第1のデバイスとは異なる第2のデバイスから受信される、請求項18に記載の方法。
【請求項２６】
前記複数のハッシュに関連付けられた電子署名を受信するステップと、
前記受信された電子署名に少なくとも部分的に基づいて、前記受信された複数のハッシュを検証するステップと,
前記受信された電子署名を有する前記検証された複数のハッシュを別のデバイスに転送するステップ
をさらに備える、請求項18に記載の方法。
【請求項２７】
前記受信された電子署名を有する検証された複数のハッシュを前記転送するステップが、
前記あらかじめ定義されたコードと、前記符号化されたパケットのセットの中の前記パケットの個数(m個)と、前記m個の符号化されたパケットを生成するために符号化された複数のパケットの中のパケットの個数(k個)とを転送するステップであって、mがkよりも大きい、ステップ
を備える、請求項26に記載の方法。
【請求項２８】
前記検証された複数のハッシュが、専用狭域通信(DSRC)ベースのネットワークを介して前記受信された電子署名とともに転送される、請求項26に記載の方法。
【発明の詳細な説明】
【技術分野】

【０００１】
相互参照
本出願は、各々が本出願の譲受人に譲渡された、2014年1月6日に出願された「Secure Content Delivery Using Hashing of Pre-coded Packets」という名称の同時係属米国特許出願第14/148,342号および2013年8月23日に出願された「Secure Content Delivery Using Hashing of Pre-coded Packets」という名称の米国仮特許出願第61/869,429号の優先権を主張する。
【背景技術】
【０００２】
以下は一般に、通信に関し、より詳細には、通信ネットワークを介してセキュアなコンテンツ配信を提供することに関する。音声、ビデオ、パケットデータ、メッセージング、ブロードキャストなどの、様々なタイプの通信コンテンツを提供するために、通信システムが広く展開されている。これらのシステムは、利用可能なシステムリソース(たとえば、時間、周波数、および電力)を共有することによって複数のユーザとの通信をサポートすることが可能な多元接続システムであり得る。ワイヤレス多元接続システムの例は、符号分割多元接続(CDMA)システム、時分割多元接続(TDMA)システム、周波数分割多元接続(FDMA)システム、および直交周波数分割多元接続(OFDMA)システムを含む。
【０００３】
本明細書で説明するように、専用狭域通信(DSRC:dedicated short range communications)ネットワークは、たとえば、認証局によって作成された証明書失効リスト(CRL:certificate revocation list)を、DSRCネットワークを使用するすべての車両に配布するために、セキュアなコンテンツ配信を必要とし得る。CRLは、車両が信頼すべきではない受信された通信を識別することができるように、失効した証明書のリストを提供する。CRLの配布(dissemination)は、悪意のあるまたは不正確なパケットがDSRCネットワークを使用する車両によって転送されないように、セキュアでなければならない。
【発明の概要】
【課題を解決するための手段】
【０００４】
説明する特徴は一般に、通信ネットワークを介して配信するためのコンテンツをセキュアにするための1つまたは複数の改善されたシステム、方法、および/または装置に関する。詳細には、説明する特徴は、専用狭域通信(DSRC)ネットワークを介したセキュアなコンテンツ配信に関する。
【０００５】
通信ネットワークを介して配信するためのコンテンツをセキュアにする方法について説明する。一構成では、方法は、コード化されたパケットのセットを生成するために、決定されたコードを使用して複数のパケットをコード化するステップと、複数のハッシュを生成するために、コード化されたパケットのセットのうちの複数のパケットをハッシュ処理するステップとを含み得る。
【０００６】
いくつかの実施形態では、方法は、コード化されたパケットのセットのうちの少なくとも1つのパケットを選択するステップを含み得る。そのような実施形態では、少なくとも1つの選択されたパケットは、ワイヤレス通信ネットワーク上でブロードキャストされ得る。さらに、少なくとも1つの署名付きおよび/または暗号化されたパケットは、選択されたパケットのブロードキャストとは無関係に送信され得る。いくつかの実施形態では、コード化されたパケットのセットのうちの少なくとも1つのパケットは、ランダムに選択され得る。
【０００７】
いくつかの実施形態では、複数のパケットのコード化は、複数のパケットの中のいくつかのパケット(k個)を決定するステップと、コード化されたパケットのセットの中のいくつかのパケット(m個)を生成するために、決定されたコードを使用してk個のパケットをコ

ード化するステップであって、mがkよりも大きい、ステップとを含み得る。そのような実施形態では、コード化されたパケットのセットの中のいくつかのパケット(m個)は、少なくともk個のパケットを有するコード化されたパケットのセットのサブセットが複数のパケットの中のk個のパケットを復元するのに十分となるように決定され得る。代替または追加として、コード化されたパケットのセットの中のいくつかのパケット(m個)は、通信ネットワークを介して複数のハッシュを送信するステップに関連付けられたオーバーヘッドに少なくとも部分的に基づいて決定され得る。

【０００８】

いくつかの実施形態では、方法は、通信ネットワークを介して複数のハッシュを送信するステップと、通信ネットワークを介してk、mおよび決定されたコードを送信するステップとを含み得る。

【０００９】

いくつかの実施形態では、方法は、コード化されたパケットのセットのうちの少なくとも1つのパケットをランダムに選択するステップを含み得る。少なくとも1つの選択されたパケットは、ワイヤレス通信ネットワーク上でブロードキャストされ得る。そのような実施形態では、コード化されたパケットのセットの中のいくつかのパケット(m個)は、ワイヤレス通信ネットワーク上での少なくとも1つのランダムに選択されたパケットのブロードキャストに関連付けられたオーバーヘッドに少なくとも部分的に基づいて決定され得る。

【００１０】

いくつかの実施形態では、複数のハッシュは、通信ネットワークを介して送信され得る。そのような実施形態では、複数のハッシュは、ワイヤレス送信され得る。代替または追加として、複数のハッシュは、ワイヤードバックホールを介して送信され得る。

【００１１】

いくつかの実施形態では、方法は、複数のハッシュを少なくとも1つのパケットに結合するステップを含み得る。そのような実施形態では、少なくとも1つのパケットは、電子署名で署名され得る。代替または追加として、少なくとも1つのパケットは暗号化され得る。さらに、そのような実施形態では、方法は、通信ネットワークを介して少なくとも1つのパケットを送信するステップを含み得る。

【００１２】

通信ネットワークを介して配信されるべきコンテンツをセキュアにするための装置について説明する。一構成では、装置は、コード化されたパケットのセットを生成するために、決定されたコードを使用して複数のパケットをコード化するための手段と、複数のハッシュを生成するために、コード化されたパケットのセットのうちの複数のパケットをハッシュ処理するための手段とを含み得る。

【００１３】

通信ネットワークを介して配信するためのコンテンツをセキュアにするように構成されたデバイスについて説明する。一構成では、デバイスは、プロセッサと、プロセッサと電子通信しているメモリとを含み得る。命令は、メモリに記憶され得る。命令は、コード化されたパケットのセットを生成するために、決定されたコードを使用して複数のパケットをコード化し、複数のハッシュを生成するために、コード化されたパケットのセットのうちの複数のパケットをハッシュ処理するように、プロセッサによって実行可能であり得る。

【００１４】

通信ネットワークを介して配信するためのコンテンツをセキュアにするためのコンピュータプログラム製品について説明する。コンピュータプログラム製品は、命令を記憶する非一時的コンピュータ可読記憶媒体であり得る。命令は、コード化されたパケットのセットを生成するために、決定されたコードを使用して複数のパケットをコード化し、複数のハッシュを生成するために、コード化されたパケットのセットのうちの複数のパケットをハッシュ処理するように、プロセッサによって実行可能であり得る。

【００１５】
通信ネットワークを介したセキュアなコンテンツ配信の方法についても説明する。一構成では、方法は、ワイヤレス通信ネットワークを介してコード化されたパケットのセットに対応する複数のハッシュを受信するステップと、複数のハッシュに関連付けられた電子署名を受信するステップとを含み得る。次いで、受信された複数のハッシュは、受信された電子署名に少なくとも部分的に基づいて検証され得る。
【００１６】
ワイヤレス通信ネットワークを介したセキュアなコンテンツ配信の別の方法について説明する。一構成では、方法は、通信ネットワークを介してコード化されたパケットのセットに対応する複数のハッシュを受信するステップと、通信ネットワークを介してコード化されたパケットのセットのうちの1つのパケットを受信するステップとを含み得る。次いで、受信されたパケットは、受信されたパケットのハッシュを生成するためにハッシュ処理され得る。次いで、受信されたパケットのハッシュは、受信されたパケットを検証するために、受信された複数のハッシュのうちの対応する1つのハッシュと比較され得る。
【００１７】
通信ネットワークを介したセキュアなコンテンツ配信のまた別の方法について説明する。一構成では、方法は、通信ネットワークを介してコード化されたパケットのセットに対応する複数のハッシュを受信するステップであって、複数のハッシュが暗号化によって暗号化される、ステップを含み得る。次いで、受信された複数のハッシュは、暗号化に少なくとも部分的に基づいて検証され得る。
【００１８】
通信ネットワークを介したセキュアなコンテンツ配信のための装置について説明する。装置は、通信ネットワークを介してコード化されたパケットのセットに対応する複数のハッシュを受信するための手段と、複数のハッシュに関連付けられた電子署名を受信するための手段と、受信された電子署名に少なくとも部分的に基づいて、受信された複数のハッシュを検証するための手段とを含み得る。
【００１９】
通信ネットワークを介したセキュアなコンテンツ配信のためのデバイスについて説明する。デバイスは、プロセッサと、プロセッサと電子通信しているメモリと、メモリに記憶された命令とを含み得る。命令は、通信ネットワークを介してコード化されたパケットのセットに対応する複数のハッシュを受信し、複数のハッシュに関連付けられた電子署名を受信し、受信された電子署名に少なくとも部分的に基づいて、受信された複数のハッシュを検証するように、プロセッサによって実行可能であり得る。
【００２０】
通信ネットワークを介したセキュアなコンテンツ配信のためのコンピュータプログラム製品について説明する。コンピュータプログラム製品は、命令を記憶する非一時的コンピュータ可読記憶媒体であり得る。命令は、ワイヤレス通信ネットワークを介してコード化されたパケットのセットに対応する複数のハッシュを受信し、複数のハッシュに関連付けられた電子署名を受信し、受信された電子署名に少なくとも部分的に基づいて、受信された複数のハッシュを検証するように、プロセッサによって実行可能であり得る。
【００２１】
通信ネットワークを介したセキュアなコンテンツ配信のための別の装置について説明する。装置は、通信ネットワークを介してコード化されたパケットのセットに対応する複数のハッシュを受信するための手段と、通信ネットワークを介してコード化されたパケットのセットのうちの1つのパケットを受信するための手段と、受信されたパケットのハッシュを生成するために、受信されたパケットをハッシュ処理するための手段と、受信されたパケットを検証するために、受信されたパケットのハッシュを受信された複数のハッシュのうちの対応する1つのハッシュと比較するための手段とを含み得る。
【００２２】
通信ネットワークを介したセキュアなコンテンツ配信のための別のデバイスについて説

明する。デバイスは、プロセッサと、プロセッサと電子通信しているメモリと、メモリに記憶された命令とを含み得る。命令は、通信ネットワークを介してコード化されたパケットのセットに対応する複数のハッシュを受信し、通信ネットワークを介してコード化されたパケットのセットのうちの1つのパケットを受信し、受信されたパケットのハッシュを生成するために、受信されたパケットをハッシュ処理し、受信されたパケットを検証するために、受信されたパケットのハッシュを受信された複数のハッシュのうちの対応する1つのハッシュと比較するように、プロセッサによって実行可能であり得る。

【００２３】

通信ネットワークを介したセキュアなコンテンツ配信のための別のコンピュータプログラム製品について説明する。コンピュータプログラム製品は、命令を記憶する非一時的コンピュータ可読記憶媒体であり得る。命令は、通信ネットワークを介してコード化されたパケットのセットに対応する複数のハッシュを受信し、通信ネットワークを介してコード化されたパケットのセットのうちの1つのパケットを受信し、受信されたパケットのハッシュを生成するために、受信されたパケットをハッシュ処理し、受信されたパケットを検証するために、受信されたパケットのハッシュを受信された複数のハッシュのうちの対応する1つのハッシュと比較するように、プロセッサによって実行可能であり得る。

【００２４】

通信ネットワークを介したセキュアなコンテンツ配信のための別の装置について説明する。装置は、通信ネットワークを介してコード化されたパケットのセットに対応する複数のハッシュを受信するための手段を含み得る。複数のハッシュは、暗号化によって暗号化され得る。装置は、暗号化に少なくとも部分的に基づいて、受信された複数のハッシュを検証するための手段をさらに含み得る。

【００２５】

通信ネットワークを介したセキュアなコンテンツ配信のための別のデバイスについて説明する。デバイスは、プロセッサと、プロセッサと電子通信しているメモリと、メモリに記憶された命令とを含み得る。命令は、通信ネットワークを介してコード化されたパケットのセットに対応する複数のハッシュを受信するように、プロセッサによって実行可能であり得る。複数のハッシュは、暗号化によって暗号化され得る。命令は、暗号化に少なくとも部分的に基づいて、受信された複数のハッシュを検証するように、プロセッサによってさらに実行可能であり得る。

【００２６】

通信ネットワークを介したセキュアなコンテンツ配信のための別のコンピュータプログラム製品について説明する。コンピュータプログラム製品は、命令を記憶する非一時的コンピュータ可読記憶媒体であり得る。命令は、通信ネットワークを介してコード化されたパケットのセットに対応する複数のハッシュを受信するように、プロセッサによって実行可能であり得る。複数のハッシュは、暗号化によって暗号化され得る。命令は、暗号化に少なくとも部分的に基づいて、受信された複数のハッシュを検証するように、プロセッサによってさらに実行可能であり得る。

【００２７】

説明する方法および装置の適用可能性のさらなる範囲は、以下の発明を実施するための形態、特許請求の範囲、および図面から明らかとなろう。説明の趣旨および範囲内の様々な変更および修正が当業者に明らかとなるので、発明を実施するための形態および具体的な例は、例示として与えられるものにすぎない。

【００２８】

以下の図面を参照することにより、本発明の性質および利点のさらなる理解が得られ得る。添付の図面では、類似の構成要素または特徴は、同じ参照ラベルを有する場合がある。さらに、同じタイプの様々な構成要素は、参照ラベルの後に、ダッシュと、それらの同様の構成要素同士を区別する第2のラベルとを続けることによって区別され得る。第1の参照ラベルのみが本明細書で使用される場合、その説明は、第2の参照ラベルとは無関係に、同じ第1の参照ラベルを有する類似の構成要素のうちのいずれか1つに適用可能である。

【図面の簡単な説明】
【００２９】
【図１】ワイヤレス通信システムのブロック図である。
【図２Ａ】基地局の一例のブロック図である。
【図２Ｂ】基地局の別の例のブロック図である。
【図３】基地局のまた別の例のブロック図である。
【図４Ａ】ユーザ機器(UE)の一例のブロック図である。
【図４Ｂ】UEの別の例のブロック図である。
【図５】UEのまた別の例のブロック図である。
【図６】ソースにおいて実施される、配信するためのコンテンツをセキュアにする方法のフローチャートである。
【図７】ソースにおいて実施される、配信するためのコンテンツをセキュアにする別の方法のフローチャートである。
【図８】ソースにおいて実施される、セキュアなコンテンツ配信の方法のフローチャートである。
【図９】UEにおいて実施される、セキュアなコンテンツ配信の方法のフローチャートである。
【図１０】UEにおいて実施される、セキュアなコンテンツ配信の別の方法のフローチャートである。
【図１１】UEにおいて実施される、セキュアなコンテンツ配信のまた別の方法のフローチャートである。
【図１２】UEにおいて実施される、セキュアなコンテンツ配信のさらに別の方法のフローチャートである。
【図１３】UEにおいて実施される、セキュアなコンテンツ配信の方法の最後の例のフローチャートである。
【発明を実施するための形態】
【００３０】
以下の説明は、専用狭域通信(DSRC)ネットワークに関して行われる。ただし、説明する特徴は一般的に、ワイヤレスか、ワイヤードか、またはそれらの組合せかにかかわらず、他の通信ネットワークにも適用可能であり得ることを理解されたい。特にDSRCネットワークのコンテキストでは、セキュアなコンテンツ配信は、DSRCネットワーク内の車両によって悪意のあるおよび/または不正確な情報パケットが受信され、転送されることを回避するために重要である。車両の各々は、より総称的にはユーザ機器(UE)であるものとして理解され得る。
【００３１】
DSRCネットワークの特定の目標は、証明書失効リスト(CRL)の配布である。情報のどの送信者を信頼することができないかをDSRCネットワーク内の車両が正確に知ることができるように、CRLの配布はセキュアでなければならない。したがって、セキュアなコンテンツ配信を提供するための様々な技法について説明する。一般的な技法は、セルラー基地局において、またはDSRCネットワークのロードサイド(roadside)基地局においてなど、CRLを配布することになっているソースにおいてコード化し、ハッシュ処理することであり得る。
【００３２】
そのような手法では、(この例ではCRLを含む)複数のパケットは、コード化されたパケットのセットを生成するために、決定されたコードを使用してコード化され得る。次いで、コード化されたパケットのセットのうちの複数のパケットは、複数のハッシュを生成するために、ハッシュ処理され得る。このようにして、コンテンツ(たとえば、CRL)は、DSRCネットワークを介して配信するためにセキュアにされ得る。次いで、複数のハッシュはネットワークを介して送信され得る。さらなるセキュリティを提供するために、複数のハッシュは少なくとも1つのパケットに結合され、次いで、電子署名で署名されるか、また

は暗号化され得る。電子署名、または場合によっては、暗号化は、パケットを検証するために少なくとも1つのパケットを受信する車両によって使用され得る。ソースによって使用されるコードは車両によって知られていることがあるので、車両は検証されたパケットをネットワーク内の別の車両を転送すること、ならびに検証されたパケットを復号して転送することができる。

【００３３】

加えて、ソースはコード化されたパケットのセットから1つのパケットをランダムに選択し、次いで、選択されたパケットをブロードキャストし得る。ソースは、必要に応じて、またはそれ以外に所望される通りに、パケットをランダムに選択し、ブロードキャストすることを継続することができる。次いで、コード化されハッシュ処理されたパケットを受信した任意の車両は、選択されブロードキャストされたパケットを受信し、次いで、(1つまたは複数の)ハッシュを生成するために受信されたパケットをハッシュ処理し、生成されたハッシュを以前に受信されたハッシュのうちの対応する(1つまたは複数の)ハッシュと比較することによって、受信されたパケットを検証し得る。

【００３４】

以下の説明は例を提供するものであり、特許請求の範囲に記載した範囲、適用可能性、または構成を限定するものではない。本開示の趣旨および範囲から逸脱することなく、説明する要素の機能および構成において変更が行われ得る。様々な実施形態は、様々な手順または構成要素を、適宜に省略、置換、または追加することができる。たとえば、説明する方法は、説明する順序とは異なる順序で実行され得、様々なステップが追加、省略、または組み合わせられ得る。また、いくつかの実施形態に関して説明する特徴は、他の実施形態において組み合わせられ得る。

【００３５】

最初に図1を参照すると、図は、ワイヤレス通信システム100の一例を示している。システム100は、DSRC基地局(たとえば、ロードサイド基地局)105と、(たとえば、DSRCシステム中の)DSRCスペクトル内で動作するDSRCデバイス(たとえば、車両)115-a～115-dとを含む。システム100は、(たとえば、Wi-Fi通信システム中の)U-NIIスペクトルにおいて動作し得るセルラー基地局130も含み得る。説明する様々な実施形態では、DSRC基地局105またはセルラー基地局130のいずれか1つはソースとして動作し得る。さらに、DSRCデバイス115の各々はユーザ機器(UE)と呼ばれることがあり、デバイス/UEに関して本明細書で説明する様々な機能を実行するための手段であるものとして見なされることがある。

【００３６】

DSRCデバイス115はワイヤレス通信システム100全体にわたって分散され得、各DSRCデバイス115は固定またはモバイルであり得る。DSRCデバイス115は、車両、交通信号、踏切、基地局、セルラーフォン、携帯情報端末(PDA)などであり得る。DSRCデバイス115は、DSRC基地局105および他のDSRCデバイス115と通信することが可能であり得る。各DSRC基地局105は、それぞれのDSRC地理的カバレージエリア110に通信カバレージを提供することができる。

【００３７】

FCCは当初、自動車用途(たとえば、インテリジェントトランスポーテーションシステム)のDSRCスペクトルを割り振った。DSRC通信の例は、車両用の緊急警報、協調型適応走行制御(cooperative adaptive cruise control)、協調型衝突警報(cooperative collision warning)、交差点衝突回避(intersection collision avoidance)、電子駐車支払(electronic parking payments)、車載シグナリング(in vehicle signaling)、自動料金収受(electronic toll collection)などを含む。DSRC通信リンク120は、DSRCデバイス115とDSRC基地局105との間、またはDSRCデバイス115と別のDSRCデバイス115との間であり得る。場合によっては、DSRCデバイス115間のDSRC通信リンク120は、DSRCデバイス115-aと115-bとの間に示すものなど、DSRC基地局105のカバレージエリア110の外で生じ得る。いくつかの実施形態では、DSRC基地局105は、直接的にまたは間接的にのいずれかで、ワイヤードまたはワイヤレス通信リンクであり得るバックホールリンク125上で互いに通信し得る。

【００３８】
ワイヤレス通信システム100はまた、複数のキャリア(異なる周波数の波形信号)上での動作をサポートし得る。マルチキャリア送信機は、変調された信号を複数のキャリア上で同時に送信することができる。たとえば、各DSRC通信リンク120は、様々な無線技術に従って変調されたマルチキャリア信号であり得る。各変調された信号は、異なるキャリア上で送られ得、制御情報(たとえば、基準信号、制御チャネルなど)、オーバーヘッド情報、データなどを搬送し得る。
【００３９】
上述したように、DSRC基地局105またはセルラー基地局130のうちの1つはソースとして動作し得、基地局またはソースに関して本明細書で説明する様々な機能を実行するための手段であるものと見なされ得る。セルラー基地局130の場合、局130は複数のパケットの形で生成局から証明書失効リスト(CRL)を取得するように構成され得る。次いで、セルラー基地局130は、コード化されたパケットのセットを生成するために、決定されたコードを用いてコード化することによって、複数のパケットを処理し得る。次いで、局130は、複数のハッシュを生成するために、コード化されたパケットのセットをハッシュ処理し得る。さらに、セルラー基地局130は複数のハッシュに電子署名で署名し得るか、または複数のハッシュを暗号化し得るか、またはその両方を行い得る。次いで、署名付きおよび/または暗号化された複数のハッシュは基地局130によって送信され得る。
【００４０】
セルラー基地局130は、たとえば、WiFiを介して、適宜にまたは所望される通りに、DSRC基地局105のうちの1つにおよび/またはDSRCデバイス115-aなどのDSRCデバイス115のうちの1つに送信し得る。いくつかの実施形態では、セルラー基地局130から1人または数人の受信者への送信を制限することは、セルラーなどのセカンダリワイヤレスネットワークに完全に依存することに関連付けられた比較的高いコストを回避するのに役立ち得る。これはまた、車両用のDSRCのより早い展開を容易にし得る。DSRCデバイス115-aがこの送信を受信したとき、デバイス115-aは、電子署名、または暗号化、またはその両方に基づいて、受信された複数のハッシュを検証し得る。検証されると、DSRCデバイス115-aは、複数のハッシュを、DSRCデバイス115-bおよび115-cなどの、範囲内にあるDSRCデバイス115のうちの1つまたは複数に転送するか、または復号して転送し得る。
【００４１】
DSRC基地局105がセルラー基地局130から署名付きおよび/または暗号化された複数のハッシュの送信を受信したとき、またはDSRC基地局105がソースとして動作するとき、DSRC基地局は、署名付きおよび/または暗号化された複数のハッシュを、DSRCデバイス115-dなどの、そのカバレージエリア110内のDSRCデバイス115に送信し得る。DSRC基地局はまた、適宜にまたは所望される通りに、署名付きおよび/または暗号化された複数のハッシュを別のDSRC基地局に送信し得、次いで、別のDSRC基地局はそのハッシュをさらに送信し得る。
【００４２】
DSRCデバイス115-dがこの送信を受信したとき、デバイス115-dは、電子署名、または暗号化、またはその両方に基づいて、受信された複数のハッシュを検証し得る。検証されると、DSRCデバイス115-dは、複数のハッシュを、範囲内にあるDSRCデバイス115のうちの1つまたは複数に転送するか、または復号して転送し得る。
【００４３】
いずれの場合も、DSRCデバイス115からDSRCデバイス115への転送は、検証された複数のハッシュをDSRCネットワーク全体にわたって効率的に配布し得る。
【００４４】
次いで、セルラー基地局130またはDSRC基地局105のいずれかであるソースは、たとえば、コード化されたパケットのセットのうちの1つのパケットをランダムに選択し、選択されたパケットをブロードキャストし得る。ブロードキャストされたパケットを、検証された複数のハッシュを受信した(または受信された複数のハッシュを検証した)DSRCデバイス

によって受信すると、DSRCデバイスはブロードキャストされたパケットを検証し得る。たとえば、受信されたパケットに対してハッシュを実行し、生成されたハッシュを検証された複数のハッシュのうちの対応する1つのハッシュと比較することによって、ブロードキャストされたパケットが検証され得る。コード化されたCRLのパケットのセット全体がDSRCデバイスにおいて受信され、検証され、復号され得るように、ソースはランダムに選択し、ブロードキャストすることを継続し得、DSRCデバイスは検証することを継続し得る。したがって、CRLはDSRCネットワーク全体にわたってセキュアにかつ効率的に配布され得る。

【００４５】

図2Aは、図1に関して説明したように本開示の態様を実行し得るDSRC基地局105-aの一例を示すブロック図200である。上記で説明したように、特定の実装形態に応じて、図2A(ならびに図2Bおよび図3)もセルラー基地局の一例を示すと見なされ得ることを理解されたい。DSRC基地局105-aは、セルラー基地局130またはDSRCデバイス115から通信を受信するように構成された受信モジュール205を含み得る。特に、受信モジュール205は、(認証局によって作成された証明書失効リストを取得するために)複数のパケットの形で認証局から通信を受信するように構成され得る。したがって、受信モジュール205または受信機は、受信するための手段および/または取得するための手段であり得る。

【００４６】

デバイス105-aの構成要素は、個別にまたは集合的に、適用可能な機能の一部または全部をハードウェアで実行するように適合された1つまたは複数の特定用途向け集積回路(ASIC)を用いて実装され得る。代替的に、それらの機能は、1つまたは複数の他の処理ユニット(またはコア)によって、1つまたは複数の集積回路上で実行され得る。他の実施形態では、当技術分野で知られている任意の方法でプログラムされ得る他のタイプの集積回路(たとえば、ストラクチャード/プラットフォームASIC、フィールドプログラマブルゲートアレイ(FPGA)、および他のセミカスタムIC)が使用され得る。各ユニットの機能はまた、全体的または部分的に、1つまたは複数の汎用プロセッサまたは特定用途向けプロセッサによって実行されるようにフォーマットされた、メモリ内で具体化された命令を用いて実装され得る。

【００４７】

DSRC基地局105-aは、コード化されたパケットのセットを生成するために、あらかじめ定義されたコードを使用して複数のパケットをコード化するように構成されたコード化モジュール210を含み得る。加えて、DSRC基地局105-aは、複数のハッシュを生成するために、コード化されたパケットのセットのうちのパケットをハッシュ処理するように構成されたハッシュ処理モジュール215を含み得る。次いで、ハッシュは、任意選択で、結合モジュール220によって1つまたは複数のパケットに結合され得る。次いで、1つまたは複数のパケットは、DSRC基地局105-aの送信モジュール225によって送信され得る。したがって、コード化モジュール210またはコーダはコード化するための手段であり得、ハッシュ処理モジュール215またはハッシャはハッシュ処理するための手段であり得、送信モジュール225または送信機は送信するための手段であり得る。

【００４８】

図2Bは、図1に関して説明したように本開示の態様を実行し得るDSRC基地局105-bの別の例を示すブロック図200-aである。図2Aの例と同様に、DSRC基地局105-bは、受信モジュール205-aと、ハッシュ処理モジュール215-aと、結合モジュール220-aと、送信モジュール225-aとを含み得る。これらのモジュールの各々は、上記で説明したものと同様の機能を含み得る。

【００４９】

デバイス105-bの構成要素は、個別にまたは集合的に、適用可能な機能の一部または全部をハードウェアで実行するように適合された1つまたは複数の特定用途向け集積回路(ASIC)を用いて実装され得る。代替的に、それらの機能は、1つまたは複数の他の処理ユニット(またはコア)によって、1つまたは複数の集積回路上で実行され得る。他の実施形態で

は、当技術分野で知られている任意の方法でプログラムされ得る他のタイプの集積回路(たとえば、ストラクチャード/プラットフォームASIC、フィールドプログラマブルゲートアレイ(FPGA)、および他のセミカスタムIC)が使用され得る。各ユニットの機能はまた、全体的または部分的に、1つまたは複数の汎用プロセッサまたは特定用途向けプロセッサによって実行されるようにフォーマットされた、メモリ内で具体化された命令を用いて実装され得る。

【００５０】

DSRC基地局105-bはまた、コード化モジュール210-aを含み得る。この例では、コード化モジュール210-aは、k決定サブモジュール230と、m決定サブモジュール235とを含み得る。k決定サブモジュール230は、受信モジュール205-aによって受信された複数のパケットの中のいくつかのパケット(k個)を決定するように構成され得る。m決定サブモジュール235は、複数のパケットがコード化モジュール210-aによってコード化されるべき、いくつかのパケット(m個)を決定するように構成され得る。したがって、k決定サブモジュール230またはカウンタはkを決定するための手段であり得、m決定サブモジュール235はmを決定するための手段であり得る。

【００５１】

いくつかの実施形態では、mは決定されたkよりも大きくなるように決定され得る。いくつかの実施形態では、いくつかのパケット(m個)は、少なくともk個のパケットを有するコード化されたパケットのセットのサブセットが複数のパケットの中のk個のパケットを復元するのに十分となるように決定され得る。代替または追加として、いくつかのパケット(m個)は、ネットワークを介した複数のハッシュの送信に関連付けられたオーバーヘッドに少なくとも部分的に基づいて決定され得る。したがって、m決定サブモジュール235は、そのような決定を行うように構成された論理を含み得る。

【００５２】

送信モジュール225-aは、k、mおよび決定されたコードを送信するようにさらに構成され得る。これは、たとえば、複数のハッシュを送信するために使用される1つまたは複数のパケットのヘッダにk、mおよび決定されたコードを含めることによって達成され得る。

【００５３】

図2Bに示すように、DSRC基地局105-bはまた、パケット選択モジュール240を含み得る。このモジュールは、送信モジュール225-aによってブロードキャストされるべき、コード化されたパケットのセットのパケットのうちの1つを選択するように構成され得る。そのような場合、コード化されたパケットのセットの中のいくつかのパケット(m個)は、ネットワーク上でのランダムに選択されたパケットのブロードキャストに関連付けられたオーバーヘッドに少なくとも部分的に基づいて、m決定サブモジュール235によって決定され得る。パケット選択モジュール240は、コード化されたパケットのセットのうちのパケットのすべてが、少なくとも1回で、そうでない場合は複数回で、送信モジュール225-aによって最終的に送信されるように、コード化されたパケットのセットのうちのパケットをランダムに選択することを継続し得る。したがって、パケット選択モジュール240またはパケット選択器は、選択するための手段であり得る。

【００５４】

図3は、セキュアなコンテンツ配信を提供するように構成され得るDSRC基地局105-cのまた別の例を示すブロック図300である。DSRC基地局105-cは、図1に示すDSRC基地局105またはセルラー基地局130の一例であり得る。DSRC基地局105-cは、1つまたは複数のトランシーバモジュール310と協働してワイヤレス信号を受信および送信するように構成された1つまたは複数のアンテナ305を含み得る。DSRC基地局は、通信管理モジュール315と、(DSRC基地局105-cがセルラー基地局130であるときは特に)ロードサイド(DSRC)局通信モジュール320と、プロセッサモジュール325と、ネットワーク通信モジュール330と、メモリ335とをさらに含み得、これらの各々は、直接的にまたは間接的に、(たとえば、1つまたは複数のバス上で)互いに通信していてもよい。

【００５５】

トランシーバモジュール310は、アンテナ305を介して、ロードサイド(DSRC)局通信モジュール320による制御下で(他の)DSRC基地局と通信するように構成され得る。また、トランシーバモジュール310は、アンテナ305を介して、通信管理モジュール315による制御下でDSRCデバイスと通信するように構成され得る。さらに、トランシーバモジュール310は、たとえば、生成局からCRLを受信するために、アンテナ305を介して、ネットワーク通信モジュール330の制御下で別のネットワーク(たとえば、セルラー)と通信するように構成され得る。したがって、トランシーバモジュール310またはトランシーバは、単独であるいはモジュール315、320および/もしくは330、ならびに/またはアンテナと組み合わせて、送信するための手段、ブロードキャストするための手段および/または取得するための手段であり得る。

【００５６】

メモリ335は、ランダムアクセスメモリ(RAM)と読取り専用メモリ(ROM)とを含み得る。メモリ335はまた、実行されると、本明細書で説明する様々な機能(たとえば、コード化、ハッシュ処理など)をプロセッサモジュール325に実行させるように構成される命令を含む、コンピュータ可読のコンピュータ実行可能ソフトウェアコード340を記憶し得る。代替的に、ソフトウェアコード340は、プロセッサモジュール325によって直接的に実行可能でないことがあるが、たとえば、コンパイルされ実行されたとき、本明細書で説明する機能をコンピュータに実行させるように構成され得る。したがって、プロセッサモジュール325またはプロセッサは、単独でまたはメモリ335およびソフトウェアコード340と組み合わせて、コード化するための手段、ハッシュ処理するための手段、結合するための手段、署名するための手段および/または暗号化するための手段であり得る。

【００５７】

プロセッサモジュール325は、インテリジェントハードウェアデバイス、たとえば、中央処理ユニット(CPU)、マイクロコントローラ、特定用途向け集積回路(ASIC)などを含み得る。トランシーバモジュール310は、パケットを変調し、変調されたパケットを送信のためにアンテナ305に与え、アンテナ305から受信されたパケットを復調するように構成されたモデムを含み得る。

【００５８】

通信管理モジュール315は別個に示されているが、通信管理モジュール315の機能は、トランシーバモジュール310の構成要素として、コンピュータプログラム製品として、および/またはプロセッサモジュール325の1つまたは複数のコントローラ要素として実装され得る。同様に、ロードサイド(DSRC)局通信モジュール320およびネットワーク通信モジュール330は、トランシーバモジュール310の構成要素として、コンピュータプログラム製品として、および/またはプロセッサモジュール325の1つまたは複数のコントローラ要素として実装され得る。

【００５９】

図4Aは、図1に関して説明したように本開示の態様を実行し得るDSRCデバイス115-eの一例を示すブロック図400である。DSRCデバイス115-eは、セルラー基地局130、DSRC基地局105、および/または別のDSRCデバイス115から通信を受信するように構成された受信モジュール405を含み得る。したがって、受信モジュール405または受信機は、受信するための手段であり得る。

【００６０】

DSRCデバイス115-eの構成要素は、個別にまたは集合的に、適用可能な機能の一部または全部をハードウェアで実行するように適合された1つまたは複数の特定用途向け集積回路(ASIC)を用いて実装され得る。代替的に、それらの機能は、1つまたは複数の他の処理ユニット(またはコア)によって、1つまたは複数の集積回路上で実行され得る。他の実施形態では、当技術分野で知られている任意の方法でプログラムされ得る他のタイプの集積回路(たとえば、ストラクチャード/プラットフォームASIC、フィールドプログラマブルゲートアレイ(FPGA)、および他のセミカスタムIC)が使用され得る。各ユニットの機能はまた、全体的または部分的に、1つまたは複数の汎用プロセッサまたは特定用途向けプロセ

ッサによって実行されるようにフォーマットされた、メモリ内で具体化された命令を用いて実装され得る。

【００６１】

DSRCデバイス115-eはまた、ソースから受信された複数のハッシュを検証するように構成された検証モジュール410を含み得る。上記で説明したように、検証は、複数のハッシュとともに受信された署名付き証明書もしくは電子署名、または複数のハッシュの暗号化、またはその両方を必要とし得る。検証モジュール410は、2つの機能、すなわち、(1)証明書または署名をチェックすることと、(2)ランダムなパケットをハッシュ処理し、取得されたハッシュを複数のハッシュの中の対応するハッシュと比較する(たとえば、一致によって検証する)こととを実行することによって、複数のハッシュを検証し得る。検証モジュール410は、あらかじめ定義されたコードを使用してコード化されたパケットのセットを復号するように構成された復号モジュール415に、複数のハッシュが検証されたことを通信するように構成され得る。DSRCデバイス115-eは、パケットの復号されたセットを別のDSRCデバイス115に送信する(たとえば、復号して転送する)ように構成された送信モジュール225を含み得る。代替または追加として、送信モジュール225は、(場合によっては、電子署名および/または暗号化を有する)検証された複数のハッシュを別のDSRCデバイス115に送信する(たとえば、転送する)ように構成され得る。したがって、検証モジュール410、証明書/署名チェッカーまたは暗号化チェッカーは検証するための手段であり得、復号モジュール415またはデコーダは復号するための手段であり得る。同様に、送信モジュール225または送信機は、送信するための手段であり得る。

【００６２】

受信モジュール405はまた、ソースからコード化されたパケットのセットのうちのランダムに選択されたパケットを受信するように構成され得る。検証モジュール410はまた、これらのパケットを検証するように構成され得る。検証されると、これらのパケットは復号モジュール415によって復号され得る。DSRCデバイス115-eは、元の複数のパケット(たとえば、証明書失効リスト(CRL))を取得するために、ランダムに受信された復号されたパケットを組み立てるように構成されたパケット組立てモジュール425をさらに含み得る。したがって、パケット組立てモジュール425またはパケットアセンブラは、組み立てるための手段であり得る。

【００６３】

図4Bは、図1に関して説明したように本開示の態様を実行し得るDSRCデバイス115-fの別の例を示すブロック図400-aである。図4Aの例と同様に、DSRCデバイス115-fは、受信モジュール405-aと、復号モジュール415-aと、パケット組立てモジュール425-aと、送信モジュール420-aとを含み得る。これらのモジュールの各々は、上記で説明したものと同様の機能を含み得る。

【００６４】

デバイス115-fの構成要素は、個別にまたは集合的に、適用可能な機能の一部または全部をハードウェアで実行するように適合された1つまたは複数の特定用途向け集積回路(ASIC)を用いて実装され得る。代替的に、それらの機能は、1つまたは複数の他の処理ユニット(またはコア)によって、1つまたは複数の集積回路上で実行され得る。他の実施形態では、当技術分野で知られている任意の方法でプログラムされ得る他のタイプの集積回路(たとえば、ストラクチャード/プラットフォームASIC、フィールドプログラマブルゲートアレイ(FPGA)、および他のセミカスタムIC)が使用され得る。各ユニットの機能はまた、全体的または部分的に、1つまたは複数の汎用プロセッサまたは特定用途向けプロセッサによって実行されるようにフォーマットされた、メモリ内で具体化された命令を用いて実装され得る。

【００６５】

DSRCデバイス115-fはまた、検証モジュール410-aを含み得る。この例では、検証モジュール410-aは、電子署名検証サブモジュール430と、暗号化検証サブモジュール435と、ハッシュ検証モジュール440とを含み得る。これらのサブモジュールは、それぞれ、電子署

名、暗号化およびランダムなパケットのハッシュに基づいて複数のハッシュを検証するために、図4Aに関して上記で説明した機能を実行するように構成され得る。したがって、電子署名検証サブモジュール430または署名検証器、暗号検証サブモジュール435または暗号検証器、およびハッシュ検証モジュール440またはハッシュ検証器は、それぞれ、電子署名、暗号およびハッシュを検証するための手段であり得る。

【００６６】

ハッシュ検証モジュール440は、ソースから受信されたコード化されたパケットのセットのうちのランダムに選択されたパケットを検証するために、図4Aに関して上記で説明した機能を実行するように構成され得る。より詳細には、ハッシュ検証モジュール440は、ハッシュ処理サブモジュール445と、比較サブモジュール450とを含み得る。ハッシュ処理サブモジュール445は、各パケットのハッシュを生成するために、ソースから受信されたコード化されたパケットのセットのうちのランダムに選択されたパケットをハッシュ処理するように構成され得る。比較サブモジュール450は、生成されたハッシュを以前に受信された複数のハッシュのうちの対応する1つのハッシュと比較するように構成され得る。たとえば、所与のパケットについての2つのハッシュ間の一致は、そのパケットを検証し得る。したがって、ハッシュ処理サブモジュールまたはハッシャおよび比較サブモジュール450または比較器は、それぞれ、ハッシュ処理するための手段および比較するための手段であり得る。上記のように、パケットが検証されると、パケットは復号モジュール415-aによって復号され得、元の複数のパケット(たとえば、証明書失効リスト(CRL))を取得するために、パケット組立てモジュール425-aによって組み立てられ得る。

【００６７】

図5は、セキュアなコンテンツ配信を提供するように構成され得るDSRCデバイス115-gのまた別の例を示すブロック図500である。DSRCデバイス115-gは、図1に示すDSRCデバイス115の一例であり得る。DSRCデバイス115-gは、1つまたは複数のトランシーバモジュール510と協働してワイヤレス信号を受信および送信するように構成された1つまたは複数のアンテナ505を含み得る。DSRCデバイスは、セルラー通信管理モジュール515と、DSRC通信管理モジュール520と、プロセッサモジュール525と、メモリ530とをさらに含み得、これらの各々は、直接的にまたは間接的に、(たとえば、1つまたは複数のバス上で)互いに通信していてもよい。

【００６８】

トランシーバモジュール510は、アンテナ505を介して、DSRC通信管理モジュール520による制御下で他のDSRCデバイス115およびDSRC基地局105と通信するように構成され得る。また、トランシーバモジュール510は、アンテナ505を介して、セルラー通信管理モジュール515による制御下で他のセルラー基地局130と通信するように構成され得る。したがって、トランシーバモジュール510またはトランシーバは、単独であるいはモジュール515および/もしくは520、ならびに/またはアンテナと組み合わせて、送信するための手段、ブロードキャストするための手段および/または取得するための手段であり得る。

【００６９】

メモリ530は、ランダムアクセスメモリ(RAM)と読取り専用メモリ(ROM)とを含み得る。メモリ530はまた、実行されると、本明細書で説明する様々な機能(たとえば、検証、復号など)をプロセッサモジュール525に実行させるように構成される命令を含む、コンピュータ可読のコンピュータ実行可能ソフトウェアコード535を記憶し得る。代替的に、ソフトウェアコード535は、プロセッサモジュール525によって直接的に実行可能でないことがあるが、たとえば、コンパイルされ実行されたとき、本明細書で説明する機能をコンピュータに実行させるように構成され得る。したがって、プロセッサモジュール525またはプロセッサは、単独でまたはメモリ530およびソフトウェアコード535と組み合わせて、コード化するための手段、ハッシュ処理するための手段、結合するための手段、署名するための手段および/または暗号化するための手段であり得る。

【００７０】

プロセッサモジュール525は、インテリジェントハードウェアデバイス、たとえば、中

央処理ユニット(CPU)、マイクロコントローラ、特定用途向け集積回路(ASIC)などを含み得る。トランシーバモジュール510は、パケットを変調し、変調されたパケットを送信のためにアンテナ505に与え、アンテナ505から受信されたパケットを復調するように構成されたモデムを含み得る。

【００７１】

セルラー通信管理モジュール515は別個に示されているが、セルラー通信管理モジュール515の機能は、トランシーバモジュール510の構成要素として、コンピュータプログラム製品として、および/またはプロセッサモジュール525の1つまたは複数のコントローラ要素として実装され得る。同様に、DSRC通信管理モジュール520は、トランシーバモジュール510の構成要素として、コンピュータプログラム製品として、および/またはプロセッサモジュール525の1つまたは複数のコントローラ要素として実装され得る。

【００７２】

図6は、通信ネットワークを介して配信するためのコンテンツをセキュアにするための方法600の一実施形態を示すフローチャートである。明快のために、図1、図2A、図2Bおよび/または図3を参照しながら説明するDSRC基地局105のうちの1つまたは複数の態様に関して、方法600について以下で説明する。一実装形態では、図3を参照しながら説明するプロセッサモジュール325は、以下で説明する機能を実行するために、DSRC基地局105の機能要素を制御するための1つまたは複数のコードのセットを実行し得る。

【００７３】

ブロック605において、DSRC基地局105は、コード化されたパケットのセットを生成するために、複数のパケットをコード化するように動作し得る。これは、決定されたコードを使用して行われ得る。コードは、上記で説明したように決定され得る。特に、コード化は、複数のパケットの中のいくつかのパケット(k個)を決定することと、コード化されたパケットのセットの中のいくつかのパケット(m個)を生成するために、決定されたコードを使用してk個のパケットをコード化することとを含み得る。いくつかの実施形態では、mはkよりも大きくてもよい。コード化されたパケットのセットの中のいくつかのパケット(m個)は、少なくともk個のパケットを有するコード化されたパケットのセットのサブセットが複数のパケットの中のk個のパケットを復元するのに十分となるように決定され得る。さらに、コード化されたパケットのセットの中のいくつかのパケット(m個)は、ワイヤレス通信ネットワークを介した複数のハッシュの送信に関連付けられたオーバーヘッドに少なくとも部分的に基づいて決定され得る。

【００７４】

ブロック610において、DSRC基地局105は、コード化されたパケットのセットのうちの複数のパケットをハッシュ処理するように動作し得る。ハッシュは、所望される通りに、任意の適切なハッシュ処理アルゴリズムを使用して実行され得る。このようにして、複数のパケットのコンテンツは配信のためにセキュアにされ得る。図示されていないが、複数のハッシュは、通信ネットワークを介して送信され得る。したがって、ソースにおいてコード化することおよびハッシュ処理することは、配信するためのセキュアなコンテンツを効率的な方法で提供するように実行され得る。

【００７５】

図7は、通信ネットワークを介して配信するためのコンテンツをセキュアにするための方法700の別の実施形態を示すフローチャートである。明快のために、図1、図2A、図2Bおよび/または図3を参照しながら説明するDSRC基地局105のうちの1つまたは複数の態様に関して、方法700について以下で説明する。一実装形態では、図3を参照しながら説明するプロセッサモジュール325は、以下で説明する機能を実行するために、DSRC基地局105の機能要素を制御するための1つまたは複数のコードのセットを実行し得る。

【００７６】

ブロック705において、DSRC基地局105は、認証局からCRLを取得するように動作し得る。これは、たとえば、任意の適切な手段を介して認証局からの送信を受信するDSRC基地局105によって達成され得る。

【００７７】
ブロック710において、DSRC基地局105は、コード化されたパケットのセットを生成するために、CRLを含む複数のパケットをコード化し得る。上記のように、これは決定されたコードを使用して行われ得る。
【００７８】
ブロック715において、DSRC基地局105は、コード化されたパケットのセットのうちの複数のパケットをハッシュ処理するように動作し得る。やはり、ハッシュは、所望される通りに、任意の適切なハッシュ処理アルゴリズムを使用して実行され得る。このようにして、コンテンツ(CRL)は配信のためにセキュアにされ得る。
【００７９】
ブロック720において、DSRC基地局105は、複数のハッシュを少なくとも1つのパケットに結合するように動作し得る。次いで、ブロック725において、DSRC基地局105は、少なくとも1つのパケットに電子署名で署名するように動作し得る。代替または追加として、ブロック730において、DSRC基地局105は、少なくとも1つのパケットを暗号化するように動作し得る。最後に、ブロック735において、少なくとも1つの署名付きおよび/または暗号化されたパケットが送信され得る。この実施形態によれば、ソースにおいてコード化することおよびハッシュ処理することは、配信するためのコンテンツを効率的な方法でセキュアにするように実行され得る。さらに、電子署名で署名することまたは暗号化することは、送信の受信者が少なくとも1つのパケットを検証するための効率的な機構を提供し得る。
【００８０】
図8は、通信ネットワークを介したセキュアなコンテンツ配信のための方法800の一実施形態を示すフローチャートである。明快のために、図1、図2A、図2Bおよび/または図3を参照しながら説明するDSRC基地局105のうちの1つまたは複数の態様に関して、方法800について以下で説明する。一実装形態では、図3を参照しながら説明するプロセッサモジュール325は、以下で説明する機能を実行するために、DSRC基地局105の機能要素を制御するための1つまたは複数のコードのセットを実行し得る。
【００８１】
ブロック805において、DSRC基地局105は、コード化されたパケットのセットを生成するために、複数のパケットをコード化するように動作し得る。上記のように、これは決定されたコードを使用して行われ得る。
【００８２】
ブロック810において、DSRC基地局105は、コード化されたパケットのセットのうちの複数のパケットをハッシュ処理するように動作し得る。やはり、ハッシュは、所望される通りに、任意の適切なハッシュ処理アルゴリズムを使用して実行され得る。このようにして、コンテンツ(CRL)は配信のためにセキュアにされ得る。
【００８３】
ブロック815において、DSRC基地局105は、ハッシュ処理した複数のパケットを送信するように動作し得る。次いで、ブロック820において、DSRC基地局105は、コード化されたパケットのセットのうちの少なくとも1つのパケットを選択するように動作し得る。これはランダムに行われ得る。最後に、ブロック825において、DSRC基地局105は、少なくとも1つの選択されたパケットをブロードキャストするように動作し得る。この実施形態によれば、ソースにおいてコード化することおよびハッシュ処理することは、配信するためのコンテンツを効率的な方法でセキュアにするように実行され得る。さらに、コード化されたパケットのセットのうちのパケットを選択することおよびブロードキャストすることは、元の複数のパケットのセキュアになったコンテンツをネットワーク全体にわたって配信するための効率的な機構を提供し得る。
【００８４】
図9は、ワイヤレス通信ネットワークにおけるセキュアなコンテンツ配信のための方法900の一実施形態を示すフローチャートである。明快のために、図1、図4A、図4Bおよび/ま

たは図5を参照しながら説明するDSRCデバイス115のうちの1つまたは複数の態様に関して、方法900について以下で説明する。一実装形態では、図5を参照しながら説明するプロセッサモジュール525は、以下で説明する機能を実行するために、DSRCデバイス115の機能要素を制御するための1つまたは複数のコードのセットを実行し得る。

【００８５】

ブロック905において、DSRCデバイス115は、コード化されたパケットのセットに対応する複数のハッシュを受信するように動作し得る。たとえば、これは、図6のブロック615におけるまたは図7のブロック735における送信を受信することによって実行され得る。

【００８６】

ブロック910において、DSRCデバイス115は、複数のハッシュに関連付けられた電子署名を受信するように動作し得る。たとえば、これは、図7のブロック735における送信を受信することによって実行され得る。

【００８７】

次いで、ブロック915において、DSRCデバイス115は、受信された電子署名に少なくとも部分的に基づいて、受信された複数のハッシュを検証するように動作し得る。この実施形態によれば、ソースにおいてコード化されハッシュ処理されたデータを受信することは、セキュアなコンテンツを効率的な方法で配信させるように実行され得る。さらに、データは電子署名に基づいて効率的に検証され得る。

【００８８】

図10は、通信ネットワークを介したセキュアなコンテンツ配信のための方法1000の別の実施形態を示すフローチャートである。明快のために、図1、図4A、図4Bおよび/または図5を参照しながら説明するDSRCデバイス115のうちの1つまたは複数の態様に関して、方法1000について以下で説明する。一実装形態では、図5を参照しながら説明するプロセッサモジュール525は、以下で説明する機能を実行するために、DSRCデバイス115の機能要素を制御するための1つまたは複数のコードのセットを実行し得る。

【００８９】

ブロック1005において、DSRCデバイス115は、コード化されたパケットのセットに対応する複数のハッシュを受信するように動作し得る。たとえば、これは、図6のブロック615におけるまたは図7のブロック735における送信を受信することによって実行され得る。

【００９０】

ブロック1010において、DSRCデバイス115は、複数のハッシュに関連付けられた電子署名を受信するように動作し得る。たとえば、これは、図7のブロック735における送信を受信することによって実行され得る。

【００９１】

次いで、ブロック1015において、DSRCデバイス115は、受信された電子署名に少なくとも部分的に基づいて、受信された複数のハッシュを検証するように動作し得る。

【００９２】

ブロック1020において、DSRCデバイス115は、電子署名を有する検証された複数のハッシュを1つまたは複数の他のDSRCデバイス115に転送するように動作し得る。さらに、ブロック1025において、DSRCデバイス115は、コード化されたパケットのセットをコード化するコードと、いくつかのパケット(m個)を生成するためにコード化される複数のパケットの中のいくつかのパケット(k個)と、いくつかのパケット(m個)とを転送するように動作し得る。上記で説明したように、これは、たとえば、転送されるハッシュのヘッダにコード、kおよびmを含めることによって達成され得る。この実施形態によれば、ソースにおいてコード化されハッシュ処理されたデータを受信することは、セキュアなコンテンツを効率的な方法で配信させるように実行され得る。また、データは電子署名に基づいて効率的に検証され得る。さらに、検証されたデータは、ネットワーク全体にわたってセキュアなコンテンツ配信を提供するために、他のDSRCデバイス115に転送され得る。

【００９３】

図11は、通信ネットワークを介したセキュアなコンテンツ配信のための方法1100の別の

実施形態を示すフローチャートである。明快のために、図1、図4A、図4Bおよび/または図5を参照しながら説明するDSRCデバイス115のうちの1つまたは複数の態様に関して、方法1100について以下で説明する。一実装形態では、図5を参照しながら説明するプロセッサモジュール525は、以下で説明する機能を実行するために、DSRCデバイス115の機能要素を制御するための1つまたは複数のコードのセットを実行し得る。

【００９４】

ブロック1105において、DSRCデバイス115は、コード化されたパケットのセットに対応する複数の暗号化されたハッシュを受信するように動作し得る。たとえば、これは、図7のブロック735における送信を受信することによって実行され得る。

【００９５】

次いで、ブロック1110において、DSRCデバイス115は、暗号化に少なくとも部分的に基づいて、受信された複数のハッシュを検証するように動作し得る。この実施形態によれば、ソースにおいてコード化されハッシュ処理されたデータを受信することは、セキュアなコンテンツを効率的な方法で配信させるように実行され得る。さらに、データは暗号化に基づいて効率的に検証され得る。

【００９６】

図12は、通信ネットワークを介したセキュアなコンテンツ配信のための方法1200の別の実施形態を示すフローチャートである。明快のために、図1、図4A、図4Bおよび/または図5を参照しながら説明するDSRCデバイス115のうちの1つまたは複数の態様に関して、方法1200について以下で説明する。一実装形態では、図5を参照しながら説明するプロセッサモジュール525は、以下で説明する機能を実行するために、DSRCデバイス115の機能要素を制御するための1つまたは複数のコードのセットを実行し得る。

【００９７】

ブロック1205において、DSRCデバイス115は、コード化されたパケットのセットに対応する複数の暗号化されたハッシュを受信するように動作し得る。たとえば、これは、図7のブロック735における送信を受信することによって実行され得る。

【００９８】

次に、ブロック1210において、DSRCデバイス115は、暗号化に少なくとも部分的に基づいて、受信された複数のハッシュを検証するように動作し得る。ブロック1215において、DSRCデバイス115は、検証された複数の暗号化されたハッシュを1つまたは複数の他のDSRCデバイス115に転送するように動作し得る。さらに、ブロック1220において、DSRCデバイス115は、コード化されたパケットのセットをコード化するコードと、いくつかのパケット(m個)を生成するためにコード化される複数のパケットの中のいくつかのパケット(k個)と、いくつかのパケット(m個)とを転送するように動作し得る。上記で説明したように、これは、たとえば、転送されるハッシュのヘッダにコード、kおよびmを含めることによって達成され得る。この実施形態によれば、ソースにおいてコード化されハッシュ処理されたデータを受信することは、セキュアなコンテンツを効率的な方法で配信させるように実行され得る。また、データは暗号化に基づいて効率的に検証され得る。さらに、検証されたデータは、ネットワーク全体にわたってセキュアなコンテンツ配信を提供するために、他のDSRCデバイス115に転送され得る。

【００９９】

図13は、通信ネットワークを介したセキュアなコンテンツ配信のための方法1300の別の実施形態を示すフローチャートである。明快のために、図1、図4A、図4Bおよび/または図5を参照しながら説明するDSRCデバイス115のうちの1つまたは複数の態様に関して、方法1300について以下で説明する。一実装形態では、図5を参照しながら説明するプロセッサモジュール525は、以下で説明する機能を実行するために、DSRCデバイス115の機能要素を制御するための1つまたは複数のコードのセットを実行し得る。

【０１００】

ブロック1305において、DSRCデバイス115は、コード化されたパケットのセットに対応する複数のハッシュを受信するように動作し得る。たとえば、これは、図6のブロック615

におけるまたは図7のブロック735における送信を受信することによって実行され得る。

【０１０１】

ブロック1310において、DSRCデバイス115は、コード化されたパケットのセットのうちの1つのパケットを受信するように動作し得る。たとえば、これは、図8のブロック825におけるブロードキャストを受信することによって実行され得る。

【０１０２】

次いで、ブロック1315において、DSRCデバイス115は、受信されたパケットのハッシュを生成するために、受信されたパケットをハッシュ処理するように動作し得る。

【０１０３】

ブロック1320において、DSRCデバイス115は、受信されたパケットを検証するために、受信されたパケットのハッシュを受信された複数のハッシュのうちの対応する1つのハッシュと比較するように動作し得る。この実施形態によれば、ソースにおいてコード化されハッシュ処理されたデータを受信することは、セキュアなコンテンツを効率的な方法で配信させるように実行され得る。また、受信されたパケットは、単に受信されたパケットに対してハッシュを実行することによって、受信された複数のハッシュのうちの対応する1つのハッシュに基づいて効率的に検証され得る。

【０１０４】

添付の図面に関して上記に記載した発明を実施するための形態は、例示的な実施形態について説明しており、実装され得るまたは特許請求の範囲内に入る実施形態のみを表すものではない。本明細書全体にわたって使用される「例示的」という用語は、「一例、実例、または例示として役立つ」ことを意味し、「好ましい」または「他の実施形態よりも有利な」を意味するものではない。発明を実施するための形態は、説明した技法の理解を与えるための具体的な詳細を含む。しかしながら、これらの技法は、これらの具体的な詳細なしに実践され得る。場合によっては、説明した実施形態の概念を曖昧にするのを回避するために、よく知られている構造およびデバイスはブロック図の形態で示されている。

【０１０５】

本明細書で説明する技法は、CDMA、TDMA、FDMA、OFDMA、SC-FDMA、および他のシステムなどの様々なワイヤレス通信システムに使用され得る。「システム」および「ネットワーク」という用語は、しばしば互換的に使用される。CDMAシステムは、CDMA2000、Universal Terrestrial Radio Access(UTRA)などの無線技術を実装し得る。CDMA2000は、IS-2000規格、IS-95規格、およびIS-856規格をカバーする。IS-2000リリース0およびAは、通常、CDMA2000 1X、1Xなどと呼ばれる。IS-856(TIA-856)は、通常、CDMA2000 1xEV-DO、高速パケットデータ(HRPD)などと呼ばれる。UTRAは、広帯域CDMA(WCDMA(登録商標))およびCDMAの他の変形形態を含む。TDMAシステムは、モバイル通信用グローバルシステム(GSM(登録商標):Global System for Mobile Communications)などの無線技術を実装し得る。OFDMAシステムは、ウルトラモバイルブロードバンド(UMB:Ultra Mobile Broadband)、発展型UTRA(E-UTRA:Evolved UTRA)、IEEE802.11(Wi-Fi)、IEEE802.16(WiMAX)、IEEE802.20、Flash-OFDMなどの無線技術を実装し得る。UTRAおよびE-UTRAは、Universal Mobile Telecommunication System(UMTS)の一部である。3GPPロングタームエボリューション(LTE:Long Term Evolution)およびLTEアドバンスト(LTE-A:LTE-Advanced)は、E-UTRAを使用するUMTSの新しいリリースである。UTRA、E-UTRA、UMTS、LTE、LTE-A、およびGSM(登録商標)は、「第3世代パートナーシッププロジェクト」(3GPP:3rd Generation Partnership Project)という名称の組織からの文書に記載されている。CDMA2000およびUMBは、「第3世代パートナーシッププロジェクト2」(3GPP2:3rd Generation Partnership Project 2)という名称の組織からの文書に記載されている。本明細書で説明する技法は、上述のシステムおよび無線技術、ならびに他のシステムおよび無線技術に使用され得る。ただし、上記の説明では、例としてLTEシステムについて説明し、上記の説明の大部分においてLTE用語が使用されるが、本技法はLTE適用例以外に適用可能である。

【０１０６】

したがって、以下の説明は例を提供するものであり、特許請求の範囲に記載した範囲、

適用可能性、または構成を限定するものではない。本開示の趣旨および範囲から逸脱することなく、説明する要素の機能および構成において変更が行われ得る。様々な実施形態は、様々な手順または構成要素を、適宜に省略、置換、または追加することができる。たとえば、説明する方法は、説明する順序とは異なる順序で実行され得、様々なステップが追加、省略、または組み合わせられ得る。また、いくつかの実施形態に関して説明する特徴は、他の実施形態において組み合わせられ得る。

【０１０７】

添付の図面に関して上記に記載した発明を実施するための形態は、例示的な実施形態について説明しており、実装され得るまたは特許請求の範囲内に入る実施形態のみを表すものではない。本明細書全体にわたって使用される「例示的」という用語は、「一例、実例、または例示として役立つ」ことを意味し、「好ましい」または「他の実施形態よりも有利な」を意味するものではない。発明を実施するための形態は、説明した技法の理解を与えるための具体的な詳細を含む。しかしながら、これらの技法は、これらの具体的な詳細なしに実践され得る。場合によっては、説明した実施形態の概念を曖昧にするのを回避するために、よく知られている構造およびデバイスはブロック図の形態で示されている。

【０１０８】

情報および信号は、様々な異なる技術および技法のいずれかを使用して表され得る。たとえば、上記の説明全体にわたって言及され得るデータ、命令、コマンド、情報、信号、ビット、シンボル、およびチップは、電圧、電流、電磁波、磁場もしくは磁性粒子、光学場もしくは光学粒子、またはそれらの任意の組合せによって表され得る。

【０１０９】

本明細書の開示に関して説明した様々な例示的なブロックおよびモジュールは、汎用プロセッサ、デジタル信号プロセッサ(DSP)、特定用途向け集積回路(ASIC)、フィールドプログラマブルゲートアレイ(FPGA)もしくは他のプログラマブル論理デバイス、個別ゲートもしくはトランジスタ論理、個別ハードウェア構成要素、または本明細書で説明した機能を実行するように設計されたそれらの任意の組合せを用いて実装または実行され得る。汎用プロセッサは、マイクロプロセッサであり得るが、代替として、プロセッサは、任意の従来のプロセッサ、コントローラ、マイクロコントローラ、または状態機械であり得る。プロセッサはまた、コンピューティングデバイスの組合せ、たとえば、DSPとマイクロプロセッサとの組合せ、複数のマイクロプロセッサ、DSPコアと連携する1つまたは複数のマイクロプロセッサ、または任意の他のそのような構成として実装され得る。

【０１１０】

本明細書で説明した機能は、ハードウェア、プロセッサによって実行されるソフトウェア、ファームウェア、またはそれらの任意の組合せで実装され得る。プロセッサによって実行されるソフトウェアで実装される場合、機能は、1つまたは複数の命令またはコードとしてコンピュータ可読媒体上に記憶されるか、またはコンピュータ可読媒体を介して送信され得る。他の例および実装形態は、本開示および添付の特許請求の範囲の範囲および趣旨内にある。たとえば、ソフトウェアの性質により、上記で説明した機能は、プロセッサ、ハードウェア、ファームウェア、ハードワイヤリング、またはこれらのうちのいずれかの組合せによって実行されるソフトウェアを使用して実装され得る。機能を実装する特徴はまた、機能の部分が、異なる物理的な場所において実装されるように分散されることを含めて、様々な位置に物理的に配置され得る。また、特許請求の範囲を含めて、本明細書で使用する場合、「のうちの少なくとも1つ」で終わる項目の列挙中で使用される「または」は、たとえば、「A、B、またはCのうちの少なくとも1つ」の列挙がAまたはBまたはCまたはABまたはACまたはBCまたはABC(すなわち、AおよびBおよびC)を意味するように、選言的列挙を示している。

【０１１１】

コンピュータ可読媒体は、ある場所から別の場所へのコンピュータプログラムの転送を容易にする任意の媒体を含む、コンピュータ記憶媒体と通信媒体の両方を含む。記憶媒体は、汎用または専用コンピュータによってアクセスされ得る任意の利用可能な媒体であり

得る。限定ではなく例として、コンピュータ可読媒体は、RAM、ROM、EEPROM、CD-ROMもしくは他の光ディスクストレージ、磁気ディスクストレージもしくは他の磁気ストレージデバイス、または命令もしくはデータ構造の形態の所望のプログラムコード手段を搬送もしくは記憶するために使用され得、汎用もしくは専用コンピュータまたは汎用もしくは専用プロセッサによってアクセスされ得る、任意の他の媒体を備えることができる。また、いかなる接続もコンピュータ可読媒体と適切に呼ばれる。たとえば、ソフトウェアが同軸ケーブル、光ファイバケーブル、ツイストペア、デジタル加入者回線(DSL)、または赤外線、無線、およびマイクロ波などのワイヤレス技術を使用してウェブサイト、サーバ、または他のリモートソースから送信される場合、同軸ケーブル、光ファイバケーブル、ツイストペア、DSL、または赤外線、無線、およびマイクロ波などのワイヤレス技術は、媒体の定義に含まれる。ディスク(disk)およびディスク(disc)は、本明細書で使用する場合、コンパクトディスク(disc)(CD)、レーザーディスク(登録商標)(disc)、光ディスク(disc)、デジタル多用途ディスク(disc)(DVD)、フロッピー(登録商標)ディスク(disk)およびブルーレイディスク(disc)を含み、ディスク(disk)は通常、データを磁気的に再生し、ディスク(disc)は、レーザーを用いてデータを光学的に再生する。上記の組合せも、コンピュータ可読媒体の範囲内に含まれる。

【０１１２】

本開示の上記の説明は、当業者が本開示を作成または使用できるようにするために提供される。本開示への様々な修正が当業者には容易に明らかとなり、本明細書に定義する一般原理は、本開示の趣旨または範囲を逸脱することなしに他の変形形態に適用され得る。本開示全体にわたって、「例」または「例示的」という用語は、一例または実例を示し、言及する例についてのいかなる選好をも暗示または必要としない。したがって、本開示は、本明細書で説明した例および設計に限定されるべきでなく、本明細書で開示する原理および新規の特徴に合致する最も広い範囲を与えられるべきである。

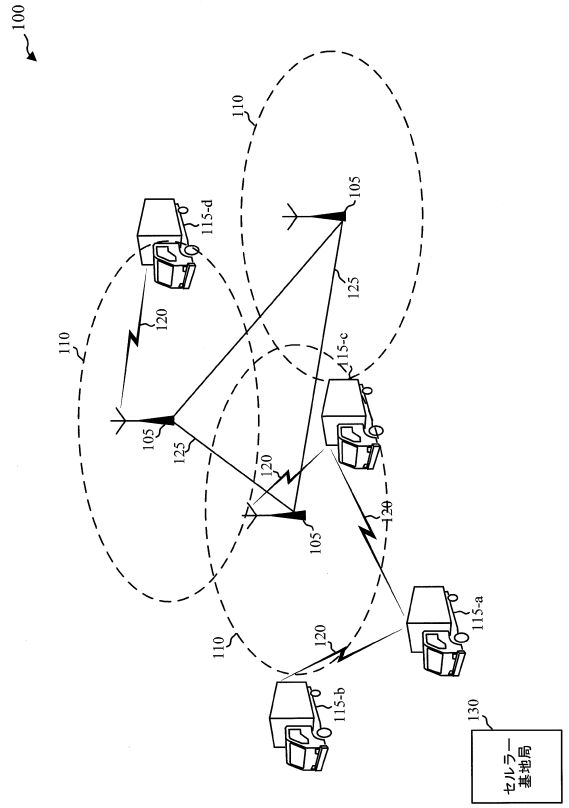
【符号の説明】

【０１１３】

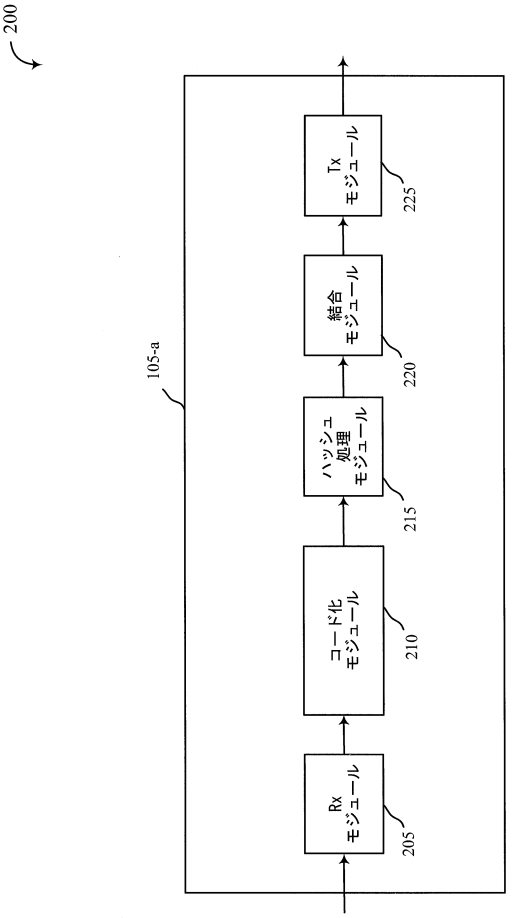
100　ワイヤレス通信システム、システム
105　DSRC基地局
110　カバレージエリア
115、115-a～115-g　DSRCデバイス
120　DSRC通信リンク
125　バックホールリンク
130　セルラー基地局
200、200-a　ブロック図
205、205-a　受信モジュール
210、210-a　コード化モジュール
215、215-a　ハッシュ処理モジュール
220、220-a　結合モジュール
225、225-a　送信モジュール
230　k決定サブモジュール
235　m決定サブモジュール
240　パケット選択モジュール
300　ブロック図
305　アンテナ
310　トランシーバモジュール
315　通信管理モジュール
320　ロードサイド(DSRC)局通信モジュール
325　プロセッサモジュール
330　ネットワーク通信モジュール
335　メモリ

340　ソフトウェアコード
400、400-a　ブロック図
405、405-a　受信モジュール
410、410-a　検証モジュール
415、415-a　復号モジュール
420、420-a　送信モジュール
425、425-a　パケット組立てモジュール
430　電子署名検証サブモジュール
435　暗号検証サブモジュール
440　ハッシュ検証モジュール
445　ハッシュ処理サブモジュール
450　比較サブモジュール
500　ブロック図
505　アンテナ
510　トランシーバモジュール
515　セルラー通信管理モジュール
520　DSRC通信管理モジュール
525　プロセッサモジュール
530　メモリ
535　ソフトウェアコード
600　方法
700　方法
800　方法
900　方法
1000　方法
1100　方法
1200　方法
1300　方法

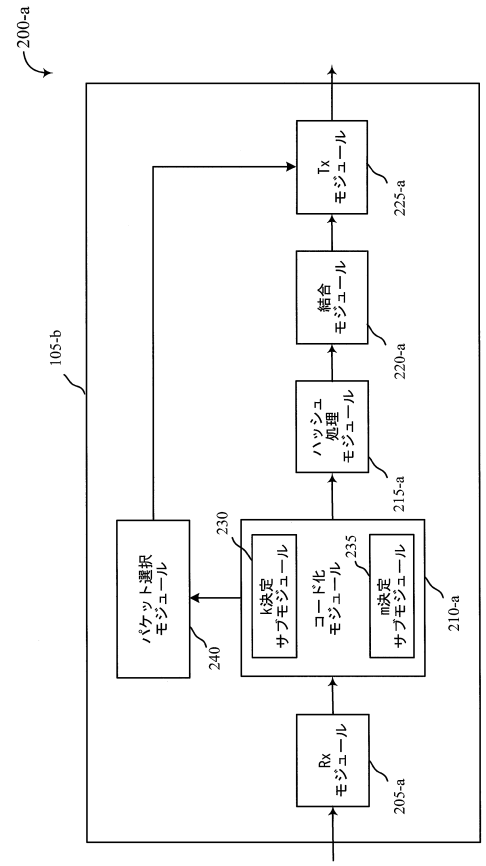
【図１】


100
110
105
115-d
120
125
115-c
115-a
115-b
130
セルラー基地局

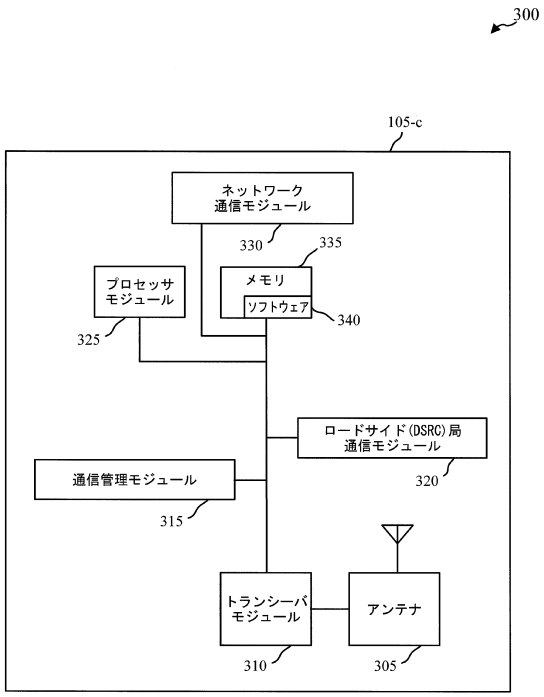
【図２Ａ】


200
105-a
Rx モジュール
205
コードル化 モジュール
210
ハッシュ 処理 モジュール
215
結合 モジュール
220
Tx モジュール
225

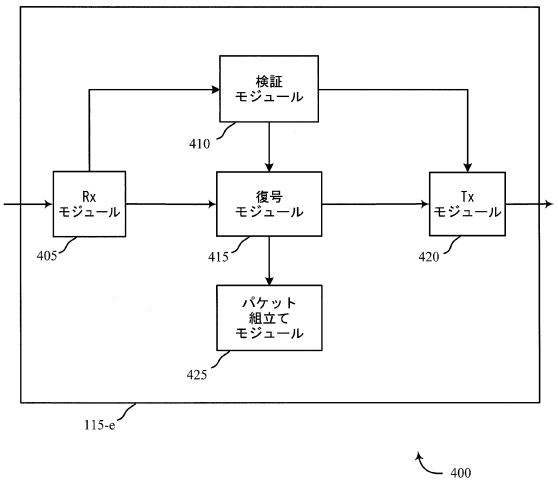
【図２Ｂ】


200-a
105-b
Rx モジュール
205-a
コードル化 モジュール
210-a
k決定 サブモジュール
m決定 サブモジュール
230
235
パケット選択 モジュール
240
ハッシュ 処理 モジュール
215-a
結合 モジュール
220-a
Tx モジュール
225-a

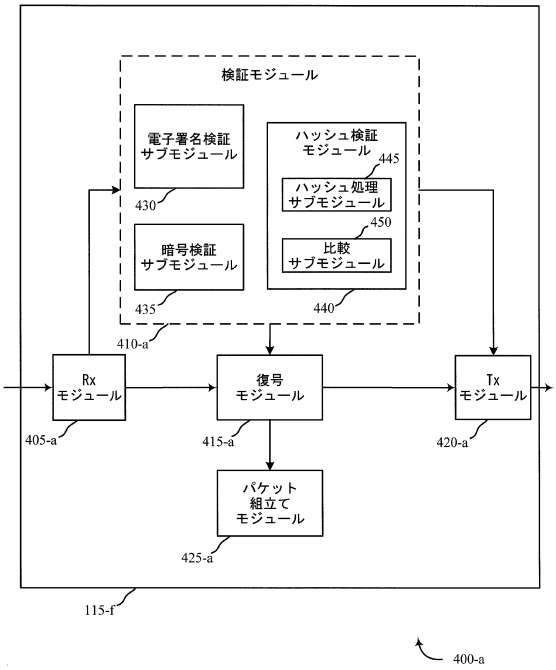
【図３】


300
105-c
ネットワーク 通信モジュール
330
335
メモリ
ソフトウェア
340
プロセッサ モジュール
325
ロードサイド(DSRC)局 通信モジュール
320
通信管理モジュール
315
トランシーバ モジュール
310
アンテナ
305

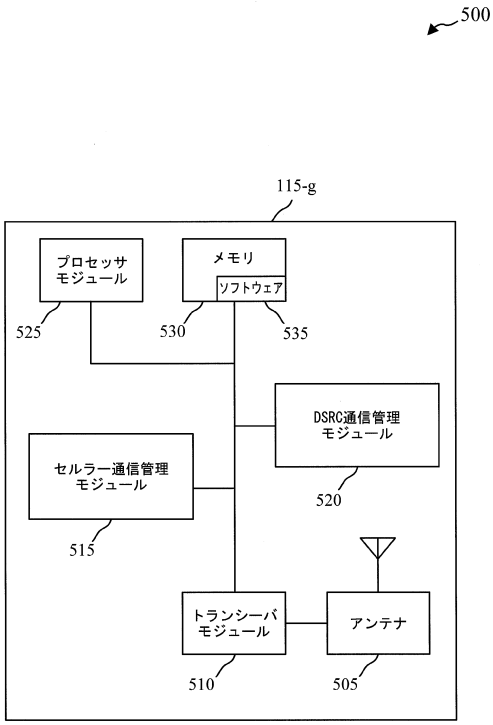
【図４Ａ】


検証
モジュール
410
Rx
モジュール
405
復号
モジュール
415
Tx
モジュール
420
パケット
組立て
モジュール
425
115-e
400

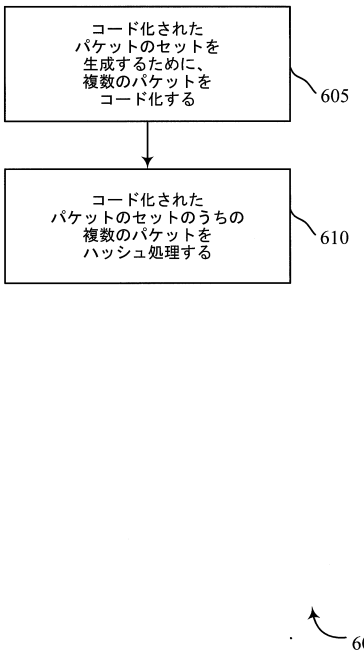
【図４Ｂ】


検証モジュール
電子署名検証
サブモジュール
430
ハッシュ検証
モジュール
445
ハッシュ処理
サブモジュール
450
比較
サブモジュール
暗号検証
サブモジュール
435
440
410-a
Rx
モジュール
405-a
復号
モジュール
415-a
Tx
モジュール
420-a
パケット
組立て
モジュール
425-a
115-f
400-a

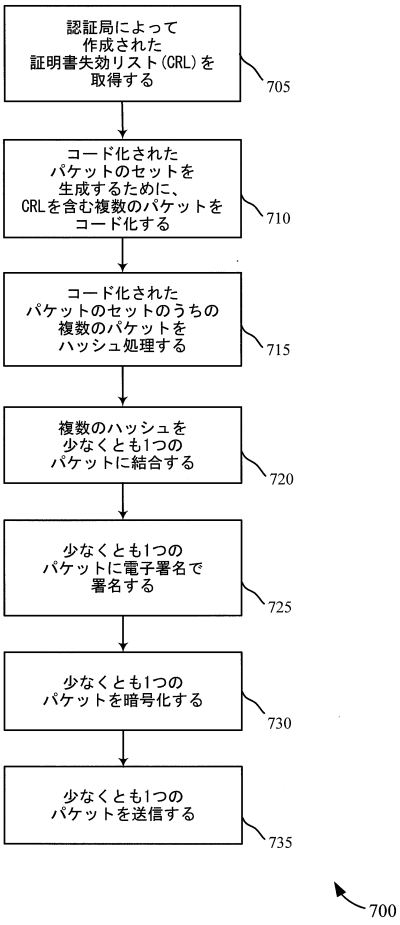
【図５】


500
115-g
プロセッサ
モジュール
525
メモリ
ソフトウェア
530
535
DSRC通信管理
モジュール
520
セルラー通信管理
モジュール
515
トランシーバ
モジュール
510
アンテナ
505

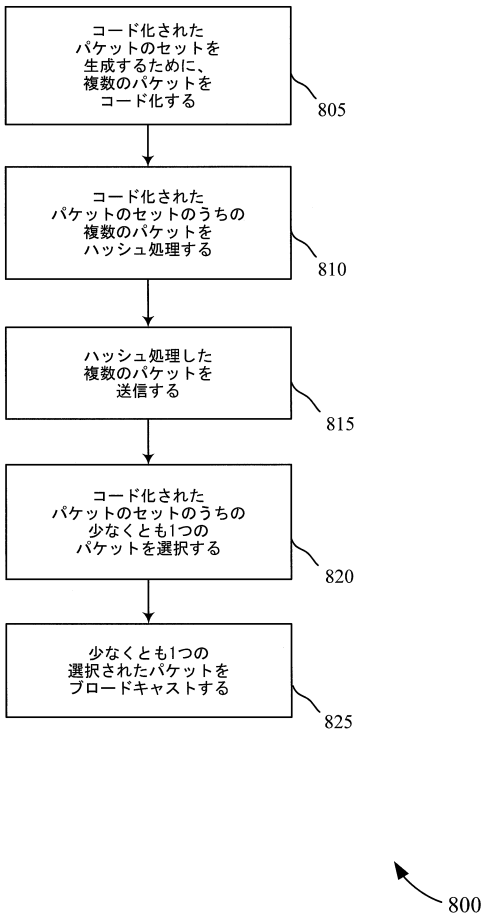
【図６】


コード化された
パケットのセットを
生成するために、
複数のパケットを
コード化する
605
コード化された
パケットのセットのうちの
複数のパケットを
ハッシュ処理する
610
600

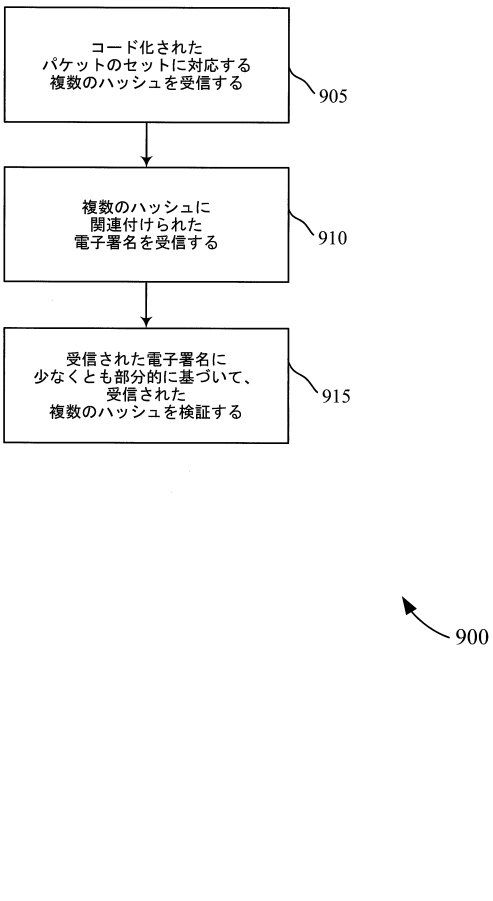
【図７】


認証局によって
作成された
証明書失効リスト(CRL)を
取得する
705
コード化された
パケットのセットを
生成するために、
CRLを含む複数のパケットを
コード化する
710
コード化された
パケットのセットのうちの
複数のパケットを
ハッシュ処理する
715
複数のハッシュを
少なくとも1つの
パケットに結合する
720
少なくとも1つの
パケットに電子署名で
署名する
725
少なくとも1つの
パケットを暗号化する
730
少なくとも1つの
パケットを送信する
735
700

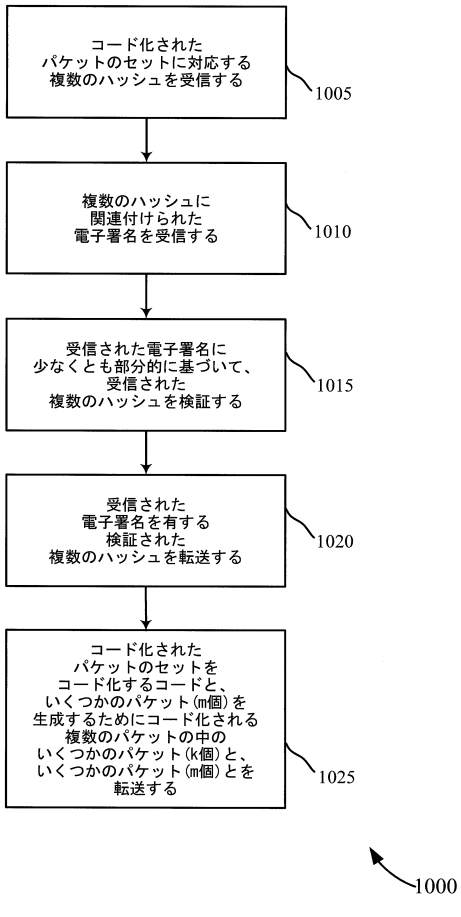
【図８】


コード化された
パケットのセットを
生成するために、
複数のパケットを
コード化する
805
コード化された
パケットのセットのうちの
複数のパケットを
ハッシュ処理する
810
ハッシュ処理した
複数のパケットを
送信する
815
コード化された
パケットのセットのうちの
少なくとも1つの
パケットを選択する
820
少なくとも1つの
選択されたパケットを
ブロードキャストする
825
800

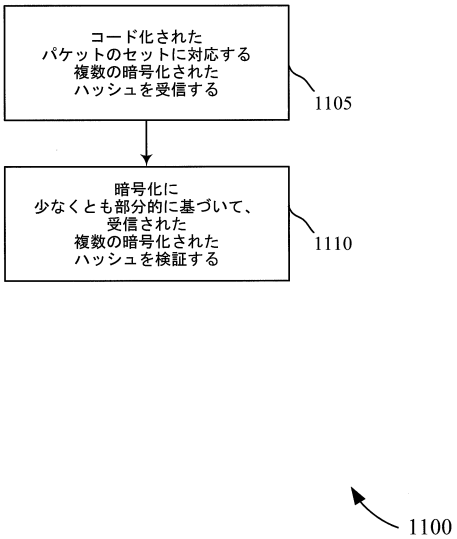
【図９】


コード化された
パケットのセットに対応する
複数のハッシュを受信する
905
複数のハッシュに
関連付けられた
電子署名を受信する
910
受信された電子署名に
少なくとも部分的に基づいて、
受信された
複数のハッシュを検証する
915
900

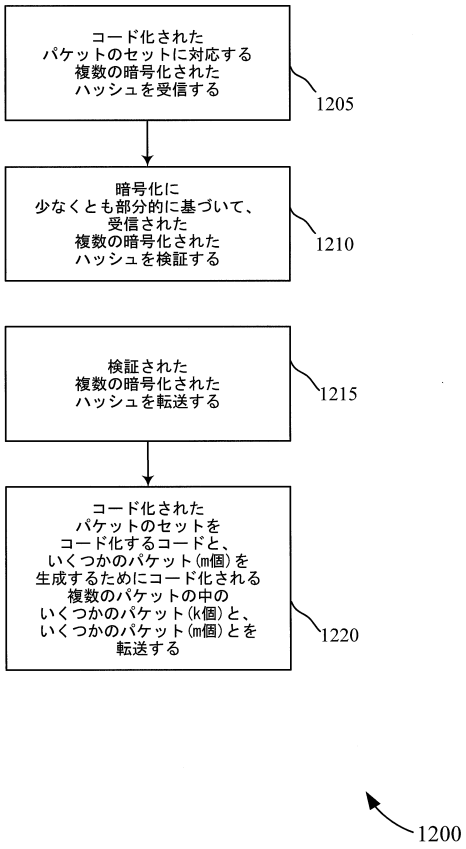
【図１０】


コード化された
パケットのセットに対応する
複数のハッシュを受信する
1005
複数のハッシュに
関連付けられた
電子署名を受信する
1010
受信された電子署名に
少なくとも部分的に基づいて、
受信された
複数のハッシュを検証する
1015
受信された
電子署名を有する
検証された
複数のハッシュを転送する
1020
コード化された
パケットのセットを
コード化するコードと、
いくつかのパケット(m個)を
生成するためにコード化される
複数のパケットの中の
いくつかのパケット(k個)と、
いくつかのパケット(m個)とを
転送する
1025
1000

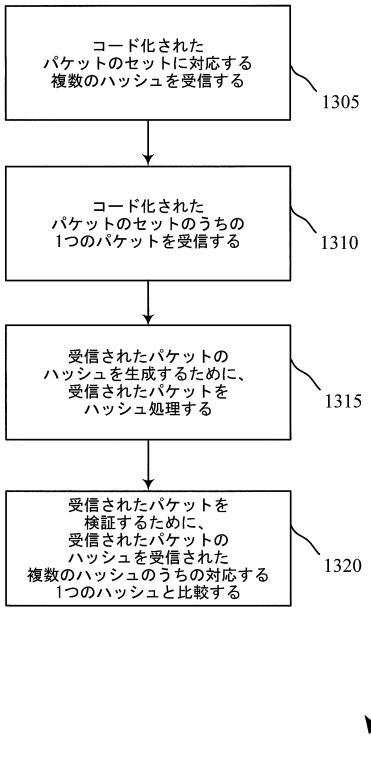
【図１１】


コード化された
パケットのセットに対応する
複数の暗号化された
ハッシュを受信する
1105
暗号化に
少なくとも部分的に基づいて、
受信された
複数の暗号化された
ハッシュを検証する
1110
1100

【図１２】


コード化された
パケットのセットに対応する
複数の暗号化された
ハッシュを受信する
1205
暗号化に
少なくとも部分的に基づいて、
受信された
複数の暗号化された
ハッシュを検証する
1210
検証された
複数の暗号化された
ハッシュを転送する
1215
コード化された
パケットのセットを
コード化するコードと、
いくつかのパケット(m個)を
生成するためにコード化される
複数のパケットの中の
いくつかのパケット(k個)と、
いくつかのパケット(m個)とを
転送する
1220
1200

【図１３】


コード化された
パケットのセットに対応する
複数のハッシュを受信する
1305
コード化された
パケットのセットのうちの
1つのパケットを受信する
1310
受信されたパケットの
ハッシュを生成するために、
受信されたパケットを
ハッシュ処理する
1315
受信されたパケットを
検証するために、
受信されたパケットの
ハッシュを受信された
複数のハッシュのうちの対応する
1つのハッシュと比較する
1320
1300

フロントページの続き

(72)発明者　シンゾウ・ウ
アメリカ合衆国・カリフォルニア・９２１２１－１７１４・サン・ディエゴ・モアハウス・ドライヴ・５７７５
(72)発明者　トーマス・ジェイ・リチャードソン
アメリカ合衆国・カリフォルニア・９２１２１－１７１４・サン・ディエゴ・モアハウス・ドライヴ・５７７５

審査官　金木　陽一

(56)参考文献　特開平１１－３４０９６８（ＪＰ，Ａ）
特開２００４－２６６６５２（ＪＰ，Ａ）
特表２００８－５０７１５４（ＪＰ，Ａ）
特表２００８－５２９４１９（ＪＰ，Ａ）
特開２０１３－１２６１５５（ＪＰ，Ａ）
特表２０１３－５１４５８７（ＪＰ，Ａ）
米国特許出願公開第２００１／００５３２２６（ＵＳ，Ａ１）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ　　９／３２
Ｈ０４Ｌ　　９／３６