【公報種別】特許法第１７条の２の規定による補正の掲載
【部門区分】第７部門第３区分
【発行日】平成29年11月30日(2017.11.30)

【公表番号】特表2016-534629(P2016-534629A)
【公表日】平成28年11月4日(2016.11.4)
【年通号数】公開・登録公報2016-062
【出願番号】特願2016-536294(P2016-536294)
【国際特許分類】
Ｈ０４Ｌ　9/32　(2006.01)
Ｈ０４Ｌ　9/36　(2006.01)
【ＦＩ】
Ｈ０４Ｌ　9/00　６７５Ａ
Ｈ０４Ｌ　9/00　６８５

【手続補正書】
【提出日】平成29年10月19日(2017.10.19)
【手続補正１】
【補正対象書類名】特許請求の範囲
【補正対象項目名】全文
【補正方法】変更
【補正の内容】
【特許請求の範囲】
【請求項１】
ワイヤレス通信のための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識別するステップと、
コード化されたパケットのセットを生成するために、決定されたコードを使用して前記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、前記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、
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、前記コード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、
前記コード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、
前記コード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が、
前記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、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が、
前記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、
前記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、前記決定されたコードを使用して前記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
を備える、請求項1に記載の方法。
【請求項５】
少なくともk個のパケットを有する前記コード化されたパケットのセットのサブセットが前記複数のパケットの中の前記k個のパケットを復元するのに十分となるように前記コード化されたパケットのセットの中の前記いくつかのパケット(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６】
前記通信ネットワークを介してk、mおよび前記決定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７】
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、前記コード化されたパケットのセットの中の前記いくつかのパケット(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８】
前記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、前記コード化されたパケットのセットの中の前記いくつかのパケット(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、
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１０】
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１１】
ワイヤレス通信のための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識別するための手段と、
コード化されたパケットのセットを生成するために、決定されたコードを使用して前記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、前記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、

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、前記コード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、
前記コード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、
前記コード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１２】
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11に記載の装置。
【請求項１３】
前記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ための手段が、
前記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ための手段
を備える、請求項11に記載の装置。
【請求項１４】
前記複数のパケットをコード化するための手段が、
前記複数のパケットの中のいくつかのパケット(k個)を決定するための手段と、
前記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、前記決定されたコードを使用して前記k個のパケットをコード化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11に記載の装置。
【請求項１５】
前記コード化するための手段が、
少なくともk個のパケットを有する前記コード化されたパケットのセットのサブセットが前記複数のパケットの中の前記k個のパケットを復元するのに十分となるように前記コード化されたパケットのセットの中の前記いくつかのパケット(m個)を決定するための手段
を備える、請求項14に記載の装置。
【請求項１６】
前記通信ネットワークを介してk、mおよび前記決定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14に記載の装置。
【請求項１７】
前記コード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、前記コード化されたパケットのセットの中の前記いくつかのパケット(m個)を決定するための手段
を備える、請求項14に記載の装置。

【請求項１８】
前記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ための手段と、
前記コード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、前記コード化されたパケットのセットの中の前記いくつかのパケット(m個)を決定するための手段
を備える、請求項14に記載の装置。
【請求項１９】
ワイヤレス通信のための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識別することと、
コード化されたパケットのセットを生成するために、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ことと、
複数のハッシュを生成するために、前記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、前記コード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、
前記コード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、
前記コード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２０】
ワイヤレス通信のための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、
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コード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、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、前記コード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２１】

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２２】
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コード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２３】
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２４】
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11に記載の装置。
【請求項２５】
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コード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11に記載の装置。
【請求項２６】
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11に記載の装置。
【請求項２７】
前記コード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20に記載の方法。
【請求項２８】
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20に記載の方法。
【請求項２９】
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、前記いくつかのパケット(m個)とを転送するステップ
を備える、請求項28に記載の方法。
【請求項３０】
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28に記載の方法。