【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26年12月25日(2014.12.25)

【公表番号】特表2014-527379(P2014-527379A)
【公表日】平成26年10月9日(2014.10.9)
【年通号数】公開・登録公報2014-056
【出願番号】特願2014-530757(P2014-530757)
【国際特許分類】
Ｈ０４Ｌ　9/08　(2006.01)
Ｈ０４Ｌ　9/14　(2006.01)
Ｈ０４Ｗ　84/12　(2009.01)
Ｈ０４Ｗ　12/04　(2009.01)
【ＦＩ】
Ｈ０４Ｌ　9/00　６０１Ｃ
Ｈ０４Ｌ　9/00　６４１
Ｈ０４Ｗ　84/12
Ｈ０４Ｗ　12/04

【手続補正書】
【提出日】平成26年11月5日(2014.11.5)
【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】
共有マスターシークレットを生成することと、
ペアワイズの一時キー（ＰＴＫ）および共有エフェメラル・キー・データのセットを生成することと、ここにおいて前記ＰＴＫは、前記共有マスターシークレットに基づいて生成され、前記共有エフェメラル・キー・データのセットは、前記共有マスターシークレットから独立して生成され、前記共有エフェメラル・キー・データのセットの有効持続期間は前記共有マスターシークレットの有効持続期間より短い、
少なくとも前記共有マスターシークレットと、前記ＰＴＫと、前記共有エフェメラル・キー・データのセットに基づく少なくとも１つの局に送信されることになる少なくとも１つのメッセージを暗号化することと、
を備える方法。
【請求項２】
前記共有マスターシークレットはペアワイズマスターキー（ＰＭＫ）を備える請求項１の方法。
【請求項３】
前記ＰＭＫは、シーケンス（ＳＥＱ）メッセージ、再認証マスターキー（ｒＭＳＫ）、アクセスポイントノンス、局ノンス、またはそれらの組み合わせに基づいて生成される請求項２の方法。
【請求項４】
前記共有エフェメラル・キー・データのセットは、アクセスポイントと前記少なくとも１つの局と関連するディフィーヘルマン（ＤＨ）キー交換を有効にする、請求項１の方法。
【請求項５】

ＤＨキー交換は、前記アクセスポイントによって指定されたＤＨグループリストから選択されたキーのセットを用いる、請求項４の方法。
【請求項６】
前記共有エフェメラル・キー・データのセットのうちの第１プライベートキー、第２プライベートキー、第１パブリックキー、及び第２パブリックキーは、前記ＤＨキー交換の前に算出され、前記第１プライベートキー及び前記第１パブリックキーは前記アクセスポイントに格納され、前記第２プライベートキー及び前記第２パブリックキーは、前記少なくとも１つの局に格納され、前記第１パブリックキー及び前記第２パブリックキーは、前記ＤＨキー交換の間に交換される、請求項５の方法。
【請求項７】
前記ＤＨキー交換には有限体演算に基づいて生成されたキーのセットを用いる、請求項４の方法。
【請求項８】
前記ＤＨキー交換には楕円曲線演算に基づいて生成されたキーのセットを用いる、請求項４の方法。
【請求項９】
前記共有エフェメラル・キー・データのセットは、アクセスポイントと前記少なくとも１つの局と関連するハンドシェイクエクスチェンジと関連づけられ、前記ハンドシェイクエクスチェンジは、前記アクセスポイントと前記少なくとも１つの局と関連する通信を認証するために実行される、請求項１の方法。
【請求項１０】
前記アクセスポイントと前記少なくとも１つの局と関連する前記ハンドシェイクエクスチェンジは、Ｗｉ－Ｆｉプロトコルを用いるハンドシェイクエクスチェンジを備える、請求項９の方法。
【請求項１１】
前記ハンドシェイクエクスチェンジは拡張可能な認証プロトコル（ＥＡＰ）交換を備える、請求項９の方法。
【請求項１２】
前記ハンドシェイクエクスチェンジと関連するアクセスポイントノンスは、ビーコンメッセージ以外のメッセージを介して送信される、請求項１１の方法。
【請求項１３】
前記ハンドシェイクエクスチェンジは４ウェイハンドシェイクを備える、請求項９の方法。
【請求項１４】
前記共有エフェメラル・キー・データのセットは、ディフィーヘルマン（ＤＨ）キー交換に基づいて生成されたパブリックキーのセットと前記ＤＨキー交換に基づくプライベートキーのセットを備える、請求項１の方法。
【請求項１５】
前記共有エフェメラル・キー・データのセットが生成された後、前記プライベートキーのセットを消去することをさらに備える、請求項１４の方法。
【請求項１６】
アクセスポイントと複数の局と関連する通信を暗号化するための複数の共有エフェメラル・キー・データのセットを生成することをさらに備え、ここにおいて、各共有エフェメラル・キー・データのセットは、前記アクセスポイントと前記複数の局のうちのそれぞれ１つと関連するそれぞれのハンドシェイクエクスチェンジを可能にし、ここにおいて、各共有エフェメラル・キー・データのセットの有効持続期間は、前記アクセスポイントと前記複数の局のうちの前記それぞれ１つと関連する対応する共有マスターシークレットの有効持続期間より短い、請求項１４の方法。
【請求項１７】
前記共有マスターシークレットと、前記ＰＴＫと、前記共有エフェメラル・キー・デー

タのセットに基づくパーフェクト・フォワード・シークレシーペアワイズの一時的なキー（ＰＦＳ－ＰＴＫ）を生成することをさらに備える、請求項１の方法。

【請求項１８】
アクセスポイントと前記少なくとも１つの局と関連する前記少なくとも１つのメッセージの前記暗号化は、ｐｅｒｆｅｃｔ　ｆｏｒｗａｒｄ　ｓｅｃｒｅｃｙ（ＰＦＳ）を実行する、請求項１の方法。

【請求項１９】
少なくとも１つの局に対する無線ネットワークインターフェース、
前記無線ネットワークインターフェースを介して前記少なくとも１つの局と通信するように構成されるプロセッサ、
を備える装置であって、
前記プロセッサは、
共有マスターシークレットを生成し、
ペアワイズの一時的なキー（ＰＴＫ）及び共有エフェメラル・キー・データのセットを生成し、ここにおいて、前記ＰＴＫは、前記共有マスターシークレットに基づいて生成され、ここにおいて、前記共有エフェメラル・キー・データのセットは、前記共有マスターシークレットから独立して生成され、ここにおいて、前記共有エフェメラル・キー・データのセットの有効持続期間は、前記共有マスターシークレットの有効持続期間より短い、
少なくとも前記共有マスターシークレットと、前記ＰＴＫ、と前記共有エフェメラル・キー・データのセットを用いて、前記少なくとも１つの局に送信されることになる少なくとも１つのメッセージを暗号化する、
ように構成される、装置。

【請求項２０】
前記共有マスターシークレットはペアワイズマスターキーを備える、請求項１９の装置。

【請求項２１】
前記共有エフェメラル・キー・データのセットはディフィーヘルマン（ＤＨ）キー交換を可能にする、請求項１９の装置。

【請求項２２】
前記ＤＨキー交換は、アクセスポイントよって指定されたＤＨグループリストから選択されたキーのセットを用いる、請求項２１の装置。

【請求項２３】
前記共有エフェメラル・キー・データのセットのうちの第１プライベートキー、第２プライベートキー、第１パブリックキー、及び第２パブリックキーは、前記ＤＨキー交換の前に算出され、ここにおいて、前記第１プライベートキー及び前記第１パブリックキーは前記アクセスポイントに格納され、ここにおいて、前記第２プライベートキー及び前記第２パブリックキーは、前記少なくとも１つの局に格納され、ここにおいて、前記第１パブリックキー及び前記第２パブリックキーは、前記ＤＨキー交換の間交換される、請求項２２の装置。

【請求項２４】
前記ＤＨキー交換には有限体演算又は楕円曲線演算に基づいて生成されるキーのセットを用いる、請求項２１の装置。

【請求項２５】
前記共有エフェメラル・キー・データのセットは、アクセスポイントと前記少なくとも１つの局と関連するハンドシェイクエクスチェンジと関連し、前記ハンドシェイクエクスチェンジは、前記アクセスポイントと前記少なくとも１つの局と関連する通信を認証するために実行される、請求項１９の装置。

【請求項２６】
前記ハンドシェイクエクスチェンジはアクセスポイントシステムと前記少なくとも１つ

の局と関連し、前記ハンドシェイクエクスチェンジはＷｉ－Ｆｉプロトコルを用いる、請求項２５の装置。
【請求項２７】
前記ハンドシェイクエクスチェンジはＥＡＰ交換を備え、前記ハンドシェイクエクスチェンジと関連するアクセスポイントノンスはビーコンメッセージ以外のメッセージを介して送信される、請求項２５の装置。
【請求項２８】
前記ハンドシェイクエクスチェンジは４ウェイハンドシェイクを備える、請求項２５の装置。
【請求項２９】
前記共有エフェメラル・キー・データのセットは、ディフィーヘルマン（ＤＨ）キー交換に基づいて生成されるパブリックキー及び前記ＤＨキー交換に基づいて生成されるプライベートキーのセットを備える、請求項１９の装置。
【請求項３０】
前記プロセッサは、前記共有エフェメラル・キー・データのセットが生成された後、前記プライベートキーのセットを消去するように構成される、請求項２９の装置。
【請求項３１】
前記プロセッサは、複数の共有エフェメラル・キー・データのセットを生成してアクセスポイントシステムと複数の局と関連する通信を暗号化するように構成され、ここにおいて、各共有エフェメラル・キー・データのセットは、前記アクセスポイントと前記複数の局のうちのそれぞれ１つと関連するハンドシェイクエクスチェンジを可能にし、ここにおいて、各共有エフェメラル・キー・データのセットの有効持続期間は、前記アクセスポイントと前記複数の局のうちの前記それぞれ１つと関連する対応する共有マスターシークレットの有効持続期間より短い、請求項２９の装置。
【請求項３２】
前記少なくとも１つの局と関連する前記少なくとも１つのメッセージの前記暗号化は、ｐｅｒｆｅｃｔ　ｆｏｒｗａｒｄ　ｓｅｃｒｅｃｙ（ＰＦＳ）を実行する、請求項１９の装置。
【請求項３３】
無線ネットワークインターフェースを介して少なくとも１つの局と通信するための手段と、
共有マスターシークレット、ペアワイズの一時キー（ＰＴＫ）、および共有エフェメラル・キー・データを生成するための手段を備える装置であって、ここにおいて前記ＰＴＫは、前記共有マスターシークレットに基づいて生成され、ここにおいて前記共有エフェメラル・キー・データのセットは、前記共有マスターシークレットから独立して生成され、ここにおいて、前記共有エフェメラル・キー・データのセットの有効持続期間は前記共有マスターシークレットの有効持続期間より短く、ここにおいて、前記少なくとも１つの局に送信されることになる少なくとも１つのメッセージは、少なくとも前記共有マスターシークレットと、前記ＰＴＫと、前記共有エフェメラル・キー・データのセットに基づいて暗号化される、装置。
【請求項３４】
前記命令がプロセッサによって実行される場合、前記プロセッサに、
共有マスターシークレットを生成することと、
ペアワイズの一時キー（ＰＴＫ）と、共有エフェメラル・キー・データのセットを生成することと、ここにおいて、前記ＰＴＫは、前記共有マスターシークレットに基づいて生成され、ここにおいて、前記共有エフェメラル・キー・データのセットは前記共有マスターシークレットから独立して生成され、ここにおいて、前記共有エフェメラル・キー・データのセットの有効持続期間は、前記共有マスターシークレットの有効持続期間より短く、
少なくとも前記共有マスターシークレットと、前記ＰＴＫと、前記共有エフェメラル・

キー・データのセットに基づく少なくとも１つの局に送信されることになる少なくとも１つのメッセージを暗号化すること、を前記プロセッサにさせる複数のプロセッサ実行可能命令を備える、非一時的コンピュータ可読媒体。
【手続補正２】
【補正対象書類名】明細書
【補正対象項目名】００５７
【補正方法】変更
【補正の内容】
【００５７】
[0061]請求項は上記で例示された厳密な構成及び構成要素に限定されないことが理解されるべきである。開示された実施例の先の説明は、当業者が開示された実施例を作成又は利用するのを可能にするために提供される。前述のものは本開示の態様に関するが、本開示の別の及びさらなる態様は、その基本的な範囲から逸脱することなく考案されており、またその範囲は、次に続く請求項によって決定される。種々の修正、変更、及び変形は、本開示又は請求項の範囲から逸脱することなく、ここで説明された実施例の構成、動作、及び詳細において行われる。従って、本開示は、ここでの実施例に限定されることを意図するものではないが、下記の請求項及びそれと同等なものによって定義されるように、原則及び新規の特徴と一致可能なより広い範囲に調和する。
以下に本件出願当初の特許請求の範囲に記載された発明を付記する。
[Ｃ１]共有マスターシークレットを生成することと、
共有エフェメラル・キー・データのセットを生成することと、前記共有エフェメラル・キー・データのセットは、前記共有マスターシークレットから独立して生成され、前記共有エフェメラル・キー・データのセットの有効持続期間は前記共有マスターシークレットの有効持続期間より短い、
少なくとも前記共有マスターシークレットと前記共有エフェメラル・キー・データのセットに基づく少なくとも１つの局に送信されることになる少なくとも１つのメッセージを暗号化することと、
を備える方法。
[Ｃ２]前記共有マスターシークレットはペアワイズマスターキー（ＰＭＫ）を備える、Ｃ１の方法。
[Ｃ３]前記共有エフェメラル・キー・データのセットは、アクセスポイントと前記少なくとも１つの局と関連するディフィーヘルマン（ＤＨ）キー交換を可能にする、Ｃ１の方法。
[Ｃ４]前記ＤＨキー交換は、前記アクセスポイントよって指定されたＤＨグループリストから選択されたキーのセットを用いる、Ｃ３の方法。
[Ｃ５]前記共有エフェメラル・キー・データのセットのうちの第１プライベートキー、第２プライベートキー、第１パブリックキー、及び第２パブリックキーは、前記ＤＨキー交換の前に算出され、前記第１プライベートキー及び前記第１パブリックキーは前記アクセスポイントに格納され、第２プライベートキー及び第２パブリックキーは、前記少なくとも１つの局に格納され、前記第１パブリックキー及び前記第２パブリックキーは、前記ＤＨキー交換の間に交換される、Ｃ４の方法。
[Ｃ６]前記ＤＨキー交換には有限体演算に基づいて生成されたキーのセットを用いる、Ｃ４の方法。
[Ｃ７]前記ＤＨキー交換には楕円曲線演算に基づいて生成されたキーのセットを用いる、Ｃ４の方法。
[Ｃ８]前記共有エフェメラル・キー・データのセットは、アクセスポイントと前記少なくとも１つの局と関連するハンドシェイクエクスチェンジと関連づけられ、前記ハンドシェイクエクスチェンジは、前記アクセスポイントと前記少なくとも１つの局と関連する通信を認証するために実行される、Ｃ１の方法。
[Ｃ９]前記アクセスポイントと前記少なくとも１つの局と関連する前記ハンドシェイ

クエクスチェンジは、Ｗｉ－Ｆｉプロトコルを用いるハンドシェイクエクスチェンジを備える、Ｃ８の方法。
[Ｃ１０]前記ハンドシェイクエクスチェンジは拡張可能な認証プロトコル（ＥＡＰ）エクスチェンジを備える、Ｃ８の方法。
[Ｃ１１]前記ハンドシェイクエクスチェンジと関連するアクセスポイントノンスは、ビーコンメッセージ以外のメッセージを介して送信される、Ｃ１０の方法。
[Ｃ１２]前記ハンドシェイクエクスチェンジは４ウェイハンドシェイクを備える、Ｃ８の方法。
[Ｃ１３]前記共有エフェメラル・キー・データのセットは、ディフィーヘルマン（ＤＨ）キー交換に基づいて生成されたパブリック及びプライベートキーのセットを備える、Ｃ１の方法。
[Ｃ１４]前記共有エフェメラル・キー・データのセットが生成された後、前記プライベートキーのセットを消去することをさらに備える、Ｃ１３の方法。
[Ｃ１５]
アクセスポイントと複数の局のうちのそれぞれと関連する通信を暗号化するための複数の共有エフェメラル・キー・データのセットを生成することをさらに備え、ここにおいて、共有エフェメラル・キー・データのセットのそれぞれは、前記アクセスポイントと前記複数の局のうちの前記それぞれ１つと関連するそれぞれのハンドシェイクエクスチェンジを可能にし、共有エフェメラル・キー・データのセットのうちのそれぞれの有効持続期間は、前記アクセスポイントと前記複数の局のうちの前記それぞれ１つと関連する対応する共有マスターシークレットの有効持続期間より短い、Ｃ１３の方法。
[Ｃ１６]
前記アクセスポイントと前記少なくとも１つの局と関連する前記少なくとも１つのメッセージの前記暗号化は、perfect forward secrecy（ＰＦＳ）を実行する、Ｃ１の方法。
[Ｃ１７]少なくとも１つの局に対する無線ネットワークインターフェースと、
前記無線ネットワークインターフェースを介して前記少なくとも１つの局と通信するように構成されるプロセッサと、
を備える装置であって、
前記プロセッサは、
共有マスターシークレットを生成し、
共有エフェメラル・キー・データのセットを生成し、
前記共有エフェメラル・キー・データのセットは、前記共有マスターシークレットから独立して生成され、前記共有エフェメラル・キー・データのセットの有効持続期間は前記共有マスターシークレットの有効持続期間より短い、
少なくとも前記共有マスターシークレットと前記共有エフェメラル・キー・データのセットを用いて、前記少なくとも１つの局に送信されることになる少なくとも１つのメッセージを暗号化する、
ように構成された前記プロセッサ、
を備える装置。
[Ｃ１８]前記共有マスターシークレットはペアワイズマスターキーを備える、Ｃ１７の装置。
[Ｃ１９]前記共有エフェメラル・キー・データのセットはディフィーヘルマン（ＤＨ）キー交換を可能にする、Ｃ１７の装置。
[Ｃ２０]前記ＤＨキー交換は、アクセスポイントよって指定されたＤＨグループリストから選択されたキーのセットを用いる、Ｃ１９の装置。
[Ｃ２１]前記共有エフェメラル・キー・データのセットのうちの第１プライベートキー、第２プライベートキー、第１パブリックキー、及び第２パブリックキーは、前記ＤＨキー交換の前に算出され、前記第１プライベートキー及び前記第１パブリックキーは前記アクセスポイントに格納され、第２プライベートキー及び第２パブリックキーは、前記少なくとも１つの局に格納され、前記第１パブリックキー及び前記第２パブリックキーは、

前記ＤＨキー交換の間に交換される、Ｃ２０の装置。
[Ｃ２２]前記ＤＨキー交換には有限体演算に基づいて生成されるキーのセットを用いる、Ｃ２０の装置。
[Ｃ２３]前記ＤＨキー交換は楕円曲線演算に基づいて生成されるキーのセットを用いる、Ｃ２０の装置。
[Ｃ２４]前記共有エフェメラル・キー・データのセットは、アクセスポイントと前記少なくとも１つの局と関連するハンドシェイクエクスチェンジと関連し、前記ハンドシェイクエクスチェンジは、前記アクセスポイントと前記少なくとも１つの局と関連する通信を認証するために実行される、Ｃ１６の装置。
[Ｃ２５]前記ハンドシェイクエクスチェンジはアクセスポイントシステムと前記少なくとも１つの局と関連し、前記ハンドシェイクエクスチェンジはＷｉ－Ｆｉプロトコルを用いる、Ｃ２３の装置。
[Ｃ２６]前記ハンドシェイクエクスチェンジはＥＡＰエクスチェンジを備える、Ｃ２３の装置。
[Ｃ２７]前記ハンドシェイクエクスチェンジと関連するアクセスポイントノンスはビーコンメッセージ以外のメッセージに送信される、Ｃ２６の装置。
[Ｃ２８]前記ハンドシェイクエクスチェンジは４ウェイハンドシェイクを備える、Ｃ２３の装置。
[Ｃ２９]前記共有エフェメラル・キー・データのセットは、ディフィーヘルマンキー交換に基づいて生成されるパブリック及びプライベートキーのセットを備える、Ｃ１７の装置。
[Ｃ３０]前記プロセッサは、前記共有エフェメラル・キー・データのセットが生成された後、前記プライベートキーのセットを消去するように構成される、Ｃ２８の方法。
[Ｃ３１]前記プロセッサは、複数の共有エフェメラル・キー・データのセットを生成して前記アクセスポイントシステムと複数の局のうちのそれぞれと関連する通信を暗号化するように構成され、ここにおいて、それぞれの共有エフェメラル・キー・データのセットは、前記アクセスポイントと前記複数の局のうちの前記それぞれ１つと関連するハンドシェイクエクスチェンジを可能にし、それぞれの共有エフェメラル・キー・データのセットの有効持続期間は、前記アクセスポイントと前記複数の局のうちの前記各１つと関連する対応する共有マスターシークレットの有効持続期間より短い、Ｃ１３の方法。
[Ｃ３２]前記少なくとも１つの局と関連する前記少なくとも１つのメッセージの前記暗号化は、perfect forward secrecy（ＰＦＳ）を実行する、Ｃ１６の方法。
[Ｃ３３]無線ネットワークインターフェースを介して少なくとも１つの局と通信するための手段と、
共有マスターシークレットを生成し、
共有エフェメラル・キー・データのセットを生成し、前記共有エフェメラル・キー・データのセットは、前記共有マスターシークレットから独立して生成され、前記共有エフェメラル・キー・データのセットの有効持続期間は前記共有マスターシークレットの有効持続期間より短い、
少なくとも前記共有マスターシークレットと前記共有エフェメラル・キー・データのセットに基づいて、前記少なくとも１つの局に送信されることになる少なくとも１つのメッセージを暗号化するように、
構成された処理のための手段、
を備える装置。
[Ｃ３４]プロセッサによって実行される場合、前記プロセッサに、
共有マスターシークレットを生成させ、
共有エフェメラル・キー・データのセットを生成させ、前記共有エフェメラル・キー・データのセットは前記共有マスターシークレットから独立して生成され、前記共有エフェメラル・キー・データのセットの有効持続期間は前記共有マスターシークレットの有効持続期間より短い、

少なくとも前記共有マスターシークレットと前記共有エフェメラル・キー・データのセットに基づく少なくとも１つの局に送信されることになる少なくとも１つのメッセージを暗号化させる、

複数のプロセッサ実行可能命令を備える、非一時的コンピュータ可読媒体。