【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30年12月27日(2018.12.27)

【公表番号】特表2018-503323(P2018-503323A)
【公表日】平成30年2月1日(2018.2.1)
【年通号数】公開・登録公報2018-004
【出願番号】特願2017-539291(P2017-539291)
【国際特許分類】
Ｈ０４Ｌ　9/08　(2006.01)
Ｈ０４Ｌ　9/16　(2006.01)
【ＦＩ】
Ｈ０４Ｌ　9/00　６０１Ｃ
Ｈ０４Ｌ　9/00　６０１Ｅ
Ｈ０４Ｌ　9/00　６４３

【手続補正書】
【提出日】平成30年11月15日(2018.11.15)
【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デバイスであって、
データリンクグループに対応する候補グループ鍵を取得するように構成された鍵論理を含むプロセッサと、
前記データリンクグループ用に指定されたページングウィンドウ中に前記データリンクグループの１つまたは複数のデバイスに告知メッセージを送信するように構成されたワイヤレスインターフェース回路と、ここにおいて、前記告知メッセージが、前記候補グループ鍵の利用可能性を示す、ここにおいて、前記告知メッセージが、マルチキャストメッセージを備える、ここにおいて、前記ページングウィンドウが、送信ウィンドウの一部である、およびここにおいて、前記ページングウィンドウの開始が、第１の発見ウィンドウの終了の後であり、前記ページングウィンドウの終了が、第２の発見ウィンドウの開始の前である、
を備えるデバイス。
【請求項２】
前記データリンクグループが、ネイバーアウェアネットワーク（ＮＡＮ）またはワイヤレスメッシュネットワークの複数のデバイスを含む、請求項１に記載のデバイス。
【請求項３】
アクティブ鍵セット、１つまたは複数のペアワイズ鍵、候補鍵セット、またはそれらの組合せを記憶するように構成されたメモリと、ここにおいて、前記アクティブ鍵セットが、アクティブグループ鍵、アクティブ配布鍵、アクティブグループ完全性鍵、またはそれらの組合せを含む、
符号化された候補グループ鍵を生成するために前記候補グループ鍵を符号化するように構成されたエンコーダと、ここにおいて、前記エンコーダが、前記アクティブグループ鍵、前記アクティブ配布鍵、または前記１つまたは複数のペアワイズ鍵のうちの特定のペアワイズ鍵に基づいて前記候補グループ鍵を符号化するように構成された、
をさらに備える、請求項１に記載のデバイス。

【請求項４】
前記ワイヤレスインターフェース回路が、前記送信ウィンドウのデータウィンドウ中に、ユニキャストメッセージとして前記データリンクグループの第２のデバイスに前記候補グループ鍵を送信するように構成された、請求項１に記載のデバイス。
【請求項５】
前記プロセッサは、前記候補グループ鍵を含む第２のマルチキャストメッセージを生成するように構成されたメッセージ論理、前記第２のマルチキャストメッセージが、パブリックアクションフレームまたはデータリンクグループメッセージを備える、をさらに備え、ここにおいて、前記ワイヤレスインターフェース回路が、前記１つまたは複数のデバイスに前記第２のマルチキャストメッセージを送信するように構成された、請求項１に記載のデバイス。
【請求項６】
前記ワイヤレスインターフェース回路が、前記告知メッセージの送信の後に前記データリンクグループの特定のデバイスから第２の告知メッセージを受信するようにさらに構成された、前記第２の告知メッセージが、第２の候補グループ鍵を示す、および、前記鍵論理が、
前記第２の候補グループ鍵が前記候補グループ鍵よりも高い優先度を有するという決定に応答して前記第２の候補グループ鍵を選択することと、
第１のグループ鍵のアクティブグループ鍵としての満了の後に、前記第２の候補グループ鍵を前記アクティブグループ鍵として設定することと
を行うように構成された、請求項１に記載のデバイス。
【請求項７】
前記鍵論理が、
前記候補グループ鍵に関係する第１の鍵インジケータに基づいて前記候補グループ鍵の第１の優先度を決定することと、ここにおいて、前記第１の鍵インジケータが、媒体アクセス制御（ＭＡＣ）アドレス、ハッシュ値、タイムスタンプ、またはそれらの組合せを含む、ここにおいて、前記ハッシュ値が、前記ＭＡＣアドレス、前記候補グループ鍵、またはその両方に基づいて生成される、
前記第２の告知メッセージ中に含まれる鍵インジケータに基づいて前記第２の候補グループ鍵の第２の優先度を決定することと、
前記第１の優先度と前記第２の優先度との比較に基づいて前記第２の候補グループ鍵が前記候補グループ鍵よりも高い優先度を有することを決定することと
を行うように構成された、請求項６に記載のデバイス。
【請求項８】
前記ワイヤレスインターフェース回路が、前記候補グループ鍵を含む鍵配信メッセージを送信するようにさらに構成された、ここにおいて、前記鍵配信メッセージが、前記候補グループ鍵の有効期限を示す鍵識別子を含む、および、前記鍵論理が、前記有効期限より前に第２の候補グループ鍵を生成するように構成された、請求項１に記載のデバイス。
【請求項９】
前記候補グループ鍵が、鍵配信メッセージ中に含まれる、および、前記鍵配信メッセージが、鍵識別番号、鍵インデックス、またはその両方を含む、ここにおいて、前記鍵インデックスが、非アクティブグループ鍵とアクティブグループ鍵とを示す、およびここにおいて、前記鍵インデックスにより、前記データリンクグループのデバイスが前記アクティブグループ鍵を決定することが可能になる、請求項１に記載のデバイス。
【請求項１０】
前記鍵論理が、次のアクティブグループ鍵として、複数の候補グループ鍵から、特定の候補グループ鍵を選択するようにさらに構成された、前記複数の候補グループ鍵が、前記候補グループ鍵を含む、請求項１に記載のデバイス。
【請求項１１】
ワイヤレス通信のための方法であって、

データリンクグループの第１のデバイスにおいて候補グループ鍵を取得することと、
前記データリンクグループの前記第１のデバイスから第２のデバイスに、前記候補グループ鍵の利用可能性を示す告知メッセージを送信することと、ここにおいて、前記告知メッセージが、前記データリンクグループ用に指定されたページングウィンドウ中に送信される、ここにおいて、前記告知メッセージが、マルチキャストメッセージを備える、ここにおいて、前記ページングウィンドウが、送信ウィンドウの一部である、およびここにおいて、前記ページングウィンドウの開始が、第１の発見ウィンドウの終了の後であり、前記ページングウィンドウの終了が、第２の発見ウィンドウの開始の前である、
を備える方法。
【請求項１２】
前記第１のデバイスが、前記第１のデバイスにおいて前記候補グループ鍵を生成することによって、または前記データリンクグループの別のデバイスから前記第１のデバイスにおいて前記候補グループ鍵を受信することによって前記候補グループ鍵を取得する、および、前記候補グループ鍵により、前記データリンクグループに対応するグループアドレス指定されたデータメッセージの暗号化または解読のうちの少なくとも１つが可能になる、請求項１１に記載の方法。
【請求項１３】
前記候補グループ鍵を取得するより前に、
前記データリンクグループの第３のデバイスから第２の告知メッセージを受信することと、ここにおいて、前記第２の告知メッセージは、前記候補グループ鍵が利用可能であることを示す、
前記候補グループ鍵を要求するために前記データリンクグループに対応する要求を送ることと
を行うことをさらに備える、請求項１１に記載の方法。
【請求項１４】
前記告知メッセージが、鍵インジケータ、前記データリンクグループのデータリンクグループ識別子、前記候補グループ鍵を生成した特定のデバイスのデバイス識別子、またはそれらの組合せを含む、請求項１１に記載の方法。
【請求項１５】
前記鍵インジケータが、前記第１のデバイスの媒体アクセス制御（ＭＡＣ）アドレス、ハッシュ値、前記候補グループ鍵の生成に対応するタイムスタンプ、またはそれらの組合せを備える、ここにおいて、前記ハッシュ値が、前記ＭＡＣアドレス、前記候補グループ鍵、またはその両方に基づいて生成される、および、前記デバイス識別子が、前記特定のデバイスの第２のＭＡＣアドレスを含む、請求項１４に記載の方法。
【請求項１６】
前記第１のデバイスが前記告知メッセージを送信するとき、前記第１のデバイスが、前記第２のデバイスに関連する、
前記第２のデバイスから前記第１のデバイスにおいて、前記第１のデバイスから前記第２のデバイスに前記候補グループ鍵を送ることを求める要求を受信することと、
ペアワイズ鍵を使用して前記候補グループ鍵を暗号化した後に前記第１のデバイスから前記第２のデバイスに前記候補グループ鍵を送ることと、ここにおいて、前記ペアワイズ鍵により、前記第１のデバイスと前記第２のデバイスとの間のセキュアな通信が可能になる、
をさらに備える、請求項１１に記載の方法。
【請求項１７】
前記告知メッセージを送信した後に、前記第２のデバイスに関連付けることを前記第１のデバイスに求める要求を受信することと、
前記第２のデバイスとのセキュリティ関連付けを行うことと、ここにおいて、前記第１のデバイスと前記第２のデバイスとに対応するペアワイズ鍵が、前記セキュリティ関連付け中に生成される、

前記セキュリティ関連付けの完了の後に、前記第２のデバイスに前記候補グループ鍵を送ることを前記第１のデバイスに求める第２の要求を受信することと
をさらに備える、請求項１１に記載の方法。
【請求項１８】
前記第１のデバイスが、前記データリンクグループの鍵生成器デバイスとして動作する、および、前記データリンクグループの他のデバイスは、前記第１のデバイスが前記鍵生成器デバイスとしての動作を中止するより前に鍵生成器デバイスとして動作しない、
前記データリンクグループの前記第１のデバイスから前記第２のデバイスにメッセージを送信することと、前記メッセージは、前記第２のデバイスが、前記データリンクグループの前記鍵生成器デバイスとして動作すべきであることを示す、
前記第１のデバイスにおいて鍵生成動作を終了することと、
前記第１のデバイスによって前記データリンクグループとの関連付けを解除すること、前記第１のデバイスにおいて低電力動作モードに遷移すること、またはその両方を行うことと
を行うことをさらに備える、請求項１７に記載の方法。
【請求項１９】
ワイヤレス通信のためのデバイスであって、
データリンクグループ用に指定されたページングウィンドウ中に第１の通信チャネルを監視するように構成された鍵論理を含むプロセッサと、ここにおいて、前記ページングウィンドウが、送信ウィンドウの一部である、およびここにおいて、前記ページングウィンドウの開始が、第１の発見ウィンドウの終了の後であり、前記ページングウィンドウの終了が、第２の発見ウィンドウの開始の前である、
前記ページングウィンドウ中に前記データリンクグループの第１のデバイスから告知メッセージを受信するように構成されたワイヤレスインターフェース回路と、前記告知メッセージが、候補グループ鍵の利用可能性を示す、ここにおいて、前記告知メッセージが、マルチキャストメッセージを備える、
を備えるデバイス。
【請求項２０】
前記ワイヤレスインターフェース回路が、符号化された候補グループ鍵を含む鍵配信メッセージを受信するようにさらに構成された、
アクティブ鍵セット、１つまたは複数のペアワイズ鍵、候補鍵セット、またはそれらの組合せを記憶するように構成されたメモリと、ここにおいて、前記候補鍵セットが、前記候補グループ鍵、候補配布鍵、候補グループ完全性鍵、またはそれらの組合せを含む、
アクティブグループ鍵、アクティブ配布鍵、または前記１つまたは複数のペアワイズ鍵のうちの特定のペアワイズ鍵に基づいて前記候補グループ鍵を生成するために前記符号化された候補グループ鍵を復号するように構成されたデコーダと
をさらに備える、請求項１９に記載のデバイス。
【請求項２１】
前記符号化された候補グループ鍵を生成するために前記候補グループ鍵を符号化するように構成されたエンコーダをさらに備える、ここにおいて、前記エンコーダが、前記アクティブグループ鍵、前記アクティブ配布鍵、または前記特定のペアワイズ鍵に基づいて前記候補グループ鍵を符号化するように構成された、およびここにおいて、前記鍵論理が、前記アクティブ鍵セット中に含まれるアクティブ完全性グループ鍵に基づいてグループアドレス指定されたトラフィックを検証するようにさらに構成された、請求項２０に記載のデバイス。
【請求項２２】
ワイヤレス通信のための方法であって、
データリンクグループの第２のデバイスにおいて、前記データリンクグループ用に指定されたページングウィンドウ中に第１の通信チャネルを監視することと、ここにおいて、前記ページングウィンドウが、送信ウィンドウの一部である、およびここにおいて、前記

ページングウィンドウの開始が、第１の発見ウィンドウの終了の後であり、前記ページングウィンドウの終了が、第２の発見ウィンドウの開始の前である、
前記ページングウィンドウ中に前記データリンクグループの第１のデバイスから前記第２のデバイスにおいて告知メッセージを受信することと、前記告知メッセージが、候補グループ鍵の利用可能性を示す、ここにおいて、前記告知メッセージが、マルチキャストメッセージを備える、
を備える方法。
【請求項２３】
前記候補グループ鍵を取得することをさらに備える、ここにおいて、前記候補グループ鍵を取得することが、
前記ページングウィンドウ中に前記告知メッセージを受信したことに応答して前記第１のデバイスにトリガメッセージを送信することと、
データウィンドウ中に前記第１のデバイスから前記候補グループ鍵を受信することと
を備える、請求項２２に記載の方法。
【請求項２４】
カウンタを更新することと、前記カウンタが、前のグループ鍵の満了に関係する、
前記カウンタが特定の値に達するより前に前記告知メッセージを受信したことに応答して前記カウンタを更新することを停止することと、前記特定の値が、前記第２のデバイスによる新しいグループ鍵の生成に関係する、
をさらに備える、請求項２２に記載の方法。
【請求項２５】
前記告知メッセージ中に含まれる第１の鍵インジケータを識別することと、
前記ページングウィンドウ中に前記データリンクグループの第３のデバイスから第２の告知メッセージを受信することと、前記第２の告知メッセージが、第２の鍵インジケータを含み、第２の候補グループ鍵の生成を示す、
前記告知メッセージの前記第１の鍵インジケータが前記第２の鍵インジケータよりも高い優先度を有することに基づいて前記第１のデバイスにトリガメッセージを送信することと、
前記第１のデバイスから前記候補グループ鍵を受信することと
をさらに備える、請求項２２に記載の方法。
【請求項２６】
前記告知メッセージを受信する前に、第２の候補グループ鍵の生成を開始することと、
前記告知メッセージを受信したことに応答して、前記第２の候補グループ鍵の生成を停止することと
をさらに備える、請求項２２に記載の方法。
【請求項２７】
前記告知メッセージを受信したことに応答して、前記第２のデバイスが前記第１のデバイスに関連するのかどうかを決定することと、
前記第１のデバイスが前記第２のデバイスに関連するという決定に応答して、前記第１のデバイスに前記候補グループ鍵を要求することと
をさらに備える、請求項２２に記載の方法。
【請求項２８】
前記告知メッセージを受信したことに応答して、前記第２のデバイスが前記第１のデバイスに関連するのかどうかを決定することと、
前記第２のデバイスが前記第１のデバイスに関連しないという決定に応答して、
前記候補グループ鍵を受信した、前記第２のデバイスに関連する前記データリンクグループの第３のデバイスを識別することと、ここにおいて、前記第３のデバイスが、前記データリンクグループのアクティブグループ鍵の満了より前に終了する時間期間中に識別される、ここにおいて、前記時間期間が、前記告知メッセージが受信された後に開始し、前記アクティブグループ鍵の前記満了の前の所定の時間に終了する、

前記第３のデバイスに前記候補グループ鍵を要求することと、
前記アクティブグループ鍵の前記満了より前に前記第３のデバイスから前記候補グループ鍵を受信することと
をさらに備える、請求項２２に記載の方法。
【請求項２９】
前記第２のデバイスが前記第１のデバイスに関連しないという決定に応答して前記第３のデバイスとのセキュリティ関連付けを実行することと、ここにおいて、前記セキュリティ関連付けがペアワイズ鍵を確立する、
前記第３のデバイスから符号化された候補グループ鍵を受信することと、
前記第２のデバイスにおいて前記候補グループ鍵を生成するために前記ペアワイズ鍵に基づいて前記符号化された候補グループ鍵を復号することと、
メモリにおいて前記候補グループ鍵を記憶することと
をさらに備える、請求項２８に記載の方法。
【請求項３０】
前記第２のデバイスが前記第１のデバイスに関連しないという決定に応答して、
前記データリンクグループのアクティブグループ鍵の満了の前の所定の時間を識別することと、
前記所定の時間の前に、前記データリンクグループの少なくとも１つのデバイスに前記候補グループ鍵についてのマルチキャスト要求を送ることと、
前記マルチキャスト要求に応答して前記データリンクグループの第３のデバイスから前記候補グループ鍵を受信することと
を行うことをさらに備える、請求項２２に記載の方法。
【手続補正２】
【補正対象書類名】明細書
【補正対象項目名】０２４１
【補正方法】変更
【補正の内容】
【０２４１】
[0253]開示した実装形態の前の説明は、開示した実装形態を当業者が製作または使用することを可能にするために与えられる。これらの実装形態に対する様々な修正が、当業者には容易に明らかになり、本明細書において定義される原理は、本開示の範囲から逸脱することなく、他の実装形態に適用され得る。したがって、本開示は、本明細書で示した実装形態に限定されるものではなく、以下の特許請求の範囲によって定義される原理および新規の特徴に一致する可能な最も広い範囲を与えられるべきである。
以下に本願発明の当初の特許請求の範囲に記載された発明を付記する。
［Ｃ１］
ワイヤレス通信のためのデバイスであって、
データリンクグループに対応する候補グループ鍵を取得するように構成された鍵論理と、
前記データリンクグループ用に指定されたページングウィンドウ中に前記データリンクグループの１つまたは複数のデバイスに告知メッセージを送信するように構成されたワイヤレスインターフェースと、ここにおいて、前記告知メッセージが、前記候補グループ鍵の利用可能性を示す、およびここにおいて、前記告知メッセージが、マルチキャストメッセージを備える、
を備えるデバイス。
［Ｃ２］
前記ページングウィンドウが、送信ウィンドウの一部である、および、前記データリンクグループが、ネイバーアウェアネットワーク（ＮＡＮ）またはワイヤレスメッシュネットワークの複数のデバイスを含む、Ｃ１に記載のデバイス。
［Ｃ３］

アクティブ鍵セット、ペアワイズ鍵、候補鍵セット、またはそれらの組合せを記憶するように構成されたメモリと、ここにおいて、前記アクティブ鍵セットが、アクティブグループ鍵、アクティブ分布鍵、アクティブグループ完全性鍵、またはそれらの組合せを含む、
符号化された候補グループ鍵を生成するために前記候補グループ鍵を符号化するように構成されたエンコーダと、ここにおいて、前記エンコーダが、前記アクティブグループ鍵、前記アクティブ配布鍵、または前記ペアワイズ鍵に基づいて前記候補グループ鍵を符号化するように構成された、
をさらに備える、Ｃ１に記載のデバイス。
［Ｃ４］
前記ワイヤレスインターフェースが、ユニキャストメッセージとして前記データリンクグループの第２のデバイスに前記候補グループ鍵を送信するように構成された、Ｃ１に記載のデバイス。
［Ｃ５］
前記候補グループ鍵を含む第２のマルチキャストメッセージを生成するように構成されたメッセージ論理、前記第２のマルチキャストメッセージが、パブリックアクションフレームまたはデータリンクグループメッセージを備える、をさらに備え、ここにおいて、前記ワイヤレスインターフェースが、前記１つまたは複数のデバイスに前記第２のマルチキャストメッセージを送信するように構成された、Ｃ１に記載のデバイス。
［Ｃ６］
前記ワイヤレスインターフェースが、前記告知メッセージの送信の後に前記データリンクグループの特定のデバイスから第２の告知メッセージを受信するようにさらに構成された、前記第２の告知メッセージが、第２の候補グループ鍵を示す、および、前記鍵論理が、
前記第２の候補グループ鍵が前記候補グループ鍵よりも高い優先度を有するという決定に応答して前記第２の候補グループ鍵を選択することと、
第１のグループ鍵のアクティブグループ鍵としての満了の後に、前記第２の候補グループ鍵を前記アクティブグループ鍵として設定することと
を行うように構成された、Ｃ１に記載のデバイス。
［Ｃ７］
前記鍵論理が、
前記候補グループ鍵に関係する第１の鍵インジケータに基づいて前記候補グループ鍵の第１の優先度を決定することと、ここにおいて、前記第１の鍵インジケータが、媒体アクセス制御（ＭＡＣ）アドレス、ハッシュ値、タイムスタンプ、またはそれらの組合せを含む、ここにおいて、前記ハッシュ値が、前記ＭＡＣアドレス、前記候補グループ鍵、またはその両方に基づいて生成される、
前記第２の告知メッセージ中に含まれる鍵インジケータに基づいて前記第２の候補グループ鍵の第２の優先度を決定することと、
第１の優先度と前記第２の優先度との比較に基づいて前記第２の候補グループ鍵が前記候補グループ鍵よりも高い優先度を有することを決定することと
を行うように構成された、Ｃ６に記載のデバイス。
［Ｃ８］
前記ワイヤレスインターフェースが、前記候補グループ鍵を含む鍵配信メッセージを送信するようにさらに構成された、ここにおいて、前記鍵配信メッセージが、前記候補グループ鍵の有効期限を示す鍵識別子を含む、および、前記鍵論理が、前記有効期限より前に第２の候補グループ鍵を生成するように構成された、Ｃ１に記載のデバイス。
［Ｃ９］
前記候補グループ鍵が、鍵配信メッセージ中に含まれる、および、前記鍵配信メッセージが、鍵識別番号、鍵インデックス、またはその両方を含む、ここにおいて、前記鍵インデックスが、非アクティブグループ鍵とアクティブグループ鍵とを示す、およびここにお

いて、前記鍵インデックスにより、前記データリンクグループのデバイスが前記アクティブグループ鍵を決定することが可能になる、Ｃ１に記載のデバイス。
［Ｃ１０］
ワイヤレス通信のための方法であって、
データリンクグループの第１のデバイスにおいて候補グループ鍵を取得することと、
前記データリンクグループの前記第１のデバイスから第２のデバイスに、前記候補グループ鍵の利用可能性を示す告知メッセージを送信することと、ここにおいて、前記告知メッセージが、前記データリンクグループ用に指定されたページングウィンドウ中に送信される、およびここにおいて、前記告知メッセージが、マルチキャストメッセージを備える、
を備える方法。
［Ｃ１１］
前記第１のデバイスが、前記第１のデバイスにおいて前記候補グループ鍵を生成することによって、または前記データリンクグループの別のデバイスから前記第１のデバイスにおいて前記候補グループ鍵を受信することによって前記候補グループ鍵を取得する、および、前記候補グループ鍵により、前記データリンクグループに対応するグループアドレス指定されたデータメッセージの暗号化または解読のうちの少なくとも１つが可能になる、Ｃ１０に記載の方法。
［Ｃ１２］
前記候補グループ鍵を取得するより前に、
前記データリンクグループの第３のデバイスから第２の告知メッセージを受信することと、ここにおいて、前記第２の告知メッセージは、前記候補グループ鍵が利用可能であることを示す、
前記候補グループ鍵を要求するために前記データリンクグループに対応する要求を送ることと
を行うことをさらに備える、Ｃ１０に記載の方法。
［Ｃ１３］
前記告知メッセージが、鍵インジケータ、前記データリンクグループのデータリンクグループ識別子、前記候補グループ鍵を生成した特定のデバイスのデバイス識別子、またはそれらの組合せを含む、Ｃ１０に記載の方法。
［Ｃ１４］
前記鍵インジケータが、前記第１のデバイスの媒体アクセス制御（ＭＡＣ）アドレス、ハッシュ値、前記候補グループ鍵の生成に対応するタイムスタンプ、またはそれらの組合せを備える、ここにおいて、前記ハッシュ値が、前記ＭＡＣアドレス、前記候補グループ鍵、またはその両方に基づいて生成される、および、前記デバイス識別子が、前記特定のデバイスの第２のＭＡＣアドレスを含む、Ｃ１３に記載の方法。
［Ｃ１５］
前記第１のデバイスが前記告知メッセージを送信するとき、前記第１のデバイスが、前記第２のデバイスに関連する、
前記第２のデバイスから前記第１のデバイスにおいて、前記第１のデバイスから前記第２のデバイスに前記候補グループ鍵を送ることを求める要求を受信することと、
ペアワイズ鍵を使用して前記候補グループ鍵を暗号化した後に前記第１のデバイスから前記第２のデバイスに前記候補グループ鍵を送ることと、ここにおいて、前記ペアワイズ鍵により、前記第１のデバイスと前記第２のデバイスとの間のセキュアな通信が可能になる、
をさらに備える、Ｃ１０に記載の方法。
［Ｃ１６］
前記告知メッセージを送信した後に、前記第２のデバイスに関連付けることを前記第１のデバイスに求める要求を受信することと、
前記第２のデバイスとのセキュリティ関連付けを行うことと、ここにおいて、前記第１

のデバイスと前記第２のデバイスとに対応するペアワイズ鍵が、前記セキュリティ関連付け中に生成される、
前記セキュリティ関連付けの完了の後に、前記第２のデバイスに前記候補グループ鍵を送ることを前記第１のデバイスに求める第２の要求を受信することと
をさらに備える、Ｃ１０に記載の方法。
［Ｃ１７］
前記第１のデバイスが、前記データリンクグループの鍵生成器デバイスとして動作する、および、前記データリンクグループの他のデバイスは、前記第１のデバイスが前記鍵生成器デバイスとしての動作を中止するより前に鍵生成器デバイスとして動作しない、
前記データリンクグループの前記第１のデバイスから前記第２のデバイスにメッセージを送信することと、前記メッセージは、前記第２のデバイスが、前記データリンクグループの前記鍵生成器デバイスとして動作すべきであることを示す、
前記第１のデバイスにおいて鍵生成動作を終了することと、
前記第１のデバイスによって前記データリンクグループとの関連付けを解除すること、前記第１のデバイスにおいて低電力動作モードに遷移すること、またはその両方を行うことと
を行うことをさらに備える、Ｃ１６に記載の方法。
［Ｃ１８］
ワイヤレス通信のためのデバイスであって、
データリンクグループ用に指定されたページングウィンドウ中に第１の通信チャネルを監視するように構成された鍵論理と、
前記ページングウィンドウ中に前記データリンクグループの第１のデバイスから告知メッセージを受信するように構成されたワイヤレスインターフェースと、前記告知メッセージが、候補グループ鍵の利用可能性を示す、ここにおいて、前記告知メッセージが、マルチキャストメッセージを備える、
を備えるデバイス。
［Ｃ１９］
前記ワイヤレスインターフェースが、符号化された候補グループ鍵を含む鍵配信メッセージを受信するようにさらに構成された、
アクティブ鍵セット、ペアワイズ鍵、候補鍵セット、またはそれらの組合せを記憶するように構成されたメモリと、ここにおいて、前記候補鍵セットが、前記候補グループ鍵、候補配布鍵、候補グループ完全性鍵、またはそれらの組合せを含む、
アクティブグループ鍵、アクティブ配布鍵、またはペアワイズ鍵に基づいて前記候補グループ鍵を生成するために前記符号化された候補グループ鍵を復号するように構成されたデコーダと
をさらに備える、Ｃ１８に記載のデバイス。
［Ｃ２０］
前記符号化された候補グループ鍵を生成するために前記候補グループ鍵を符号化するように構成されたエンコーダをさらに備える、ここにおいて、前記エンコーダが、前記アクティブグループ鍵、前記アクティブ配布鍵、または前記ペアワイズ鍵に基づいて前記候補グループ鍵を符号化するように構成された、およびここにおいて、前記鍵論理が、前記アクティブ鍵セット中に含まれるアクティブ完全性グループ鍵に基づいてグループアドレス指定されたトラフィックを検証するようにさらに構成された、Ｃ１９に記載のデバイス。
［Ｃ２１］
ワイヤレス通信のための方法であって、
データリンクグループの第２のデバイスにおいて、前記データリンクグループ用に指定されたページングウィンドウ中に第１の通信チャネルを監視することと、
前記ページングウィンドウ中に前記データリンクグループの第１のデバイスから前記第２のデバイスにおいて告知メッセージを受信することと、前記告知メッセージが、候補グループ鍵の利用可能性を示す、ここにおいて、前記告知メッセージが、マルチキャストメ

ッセージを備える、
を備える方法。
［Ｃ２２］
前記候補グループ鍵を取得することをさらに備える、ここにおいて、前記候補グループ鍵を取得することが、
前記ページングウィンドウ中に前記告知メッセージを受信したことに応答して前記第１のデバイスにトリガメッセージを送信することと、
データウィンドウ中に前記第１のデバイスから前記候補グループ鍵を受信することと
を備える、Ｃ２１に記載の方法。
［Ｃ２３］
カウンタを更新することと、前記カウンタが、前のグループ鍵の満了に関係する、
前記カウンタが特定の値に達するより前に前記告知メッセージを受信したことに応答して前記カウンタを更新することを停止することと、前記特定の値が、前記第２のデバイスによる新しいグループ鍵の生成に関係する、
をさらに備える、Ｃ２１に記載の方法。
［Ｃ２４］
前記告知メッセージ中に含まれる第１の鍵インジケータを識別することと、
前記ページングウィンドウ中に前記データリンクグループの第３のデバイスから第２の告知メッセージを受信することと、前記第２の告知メッセージが、第２の鍵インジケータを含み、第２の候補グループ鍵の生成を示す、
前記第２の鍵インジケータよりも高い優先度を有する前記告知メッセージの前記第１の鍵インジケータに基づいて前記第１のデバイスにトリガメッセージを送信することと、
前記第１のデバイスから前記候補グループ鍵を受信することと
をさらに備える、Ｃ２１に記載の方法。
［Ｃ２５］
前記告知メッセージを受信する前に、第２の候補グループ鍵の生成を開始することと、
前記告知メッセージを受信したことに応答して、前記第２の候補グループ鍵の生成を停止することと
をさらに備える、Ｃ２１に記載の方法。
［Ｃ２６］
前記告知メッセージを受信したことに応答して、前記データリンクグループのデバイスに前記告知メッセージを再送信することをさらに備える、Ｃ２１に記載の方法。
［Ｃ２７］
前記告知メッセージを受信したことに応答して、前記第２のデバイスが前記第１のデバイスに関連するのかどうかを決定することと、
前記第１のデバイスが前記第２のデバイスに関連するという決定に応答して、前記第１のデバイスに前記候補グループ鍵を要求することと
をさらに備える、Ｃ２１に記載の方法。
［Ｃ２８］
前記告知メッセージを受信したことに応答して、前記第２のデバイスが前記第１のデバイスに関連するのかどうかを決定することと、
前記第２のデバイスが前記第１のデバイスに関連しないという決定に応答して、
前記候補グループ鍵を受信した、前記第２のデバイスに関連する前記データリンクグループの第３のデバイスを識別することと、ここにおいて、前記第３のデバイスが、前記データリンクグループのアクティブグループ鍵の満了より前に終了する時間期間中に識別される、ここにおいて、前記時間期間が、前記告知メッセージが受信された後に開始し、前記アクティブグループ鍵の前記満了の前の所定の時間に終了する、
前記第３のデバイスに前記候補グループ鍵を要求することと、
前記アクティブグループ鍵の前記満了より前に前記第３のデバイスから前記候補グループ鍵を受信することと

をさらに備える、Ｃ２１に記載の方法。
［Ｃ２９］
前記第２のデバイスが前記第１のデバイスに関連しないという決定に応答して前記第３のデバイスとのセキュリティ関連付けを実行することと、ここにおいて、前記セキュリティ関連付けがペアワイズ鍵を確立する、
前記第３のデバイスから符号化された候補グループ鍵を受信することと、
第２のデバイスにおいて前記候補グループ鍵を生成するために前記ペアワイズ鍵に基づいて前記符号化された候補グループ鍵を復号することと、
メモリにおいて前記候補グループ鍵を記憶することと
をさらに備える、Ｃ２８に記載の方法。
［Ｃ３０］
前記第２のデバイスが前記第１のデバイスに関連しないという決定に応答して、
前記データリンクグループのアクティブグループ鍵の満了の前の所定の時間を識別することと、
前記所定の時間の前に、前記データリンクグループの少なくとも１つのデバイスに前記候補グループ鍵についてのマルチキャスト要求を送ることと、
前記マルチキャスト要求に応答して前記データリンクグループの第３のデバイスから前記候補グループ鍵を受信することと
を行うことをさらに備える、Ｃ２１に記載の方法。