(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2018-503322
(P2018-503322A)
(43)公表日　平成30年2月1日(2018.2.1)

(51)Int.Cl.			F I			テーマコード（参考）
H04L	***9/08***	***(2006.01)***	H04L	9/00	601C	5J104
H04L	***9/16***	***(2006.01)***	H04L	9/00	601E	
			H04L	9/00	643	

審査請求 未請求　予備審査請求 未請求　（全 76 頁）

(21)出願番号　特願2017-539288 (P2017-539288)
(86)(22)出願日　平成28年1月27日 (2016.1.27)
(85)翻訳文提出日　平成29年9月25日 (2017.9.25)
(86)国際出願番号　PCT/US2016/015198
(87)国際公開番号　WO2016/123256
(87)国際公開日　平成28年8月4日 (2016.8.4)
(31)優先権主張番号　62/108,374
(32)優先日　平成27年1月27日 (2015.1.27)
(33)優先権主張国　米国 (US)
(31)優先権主張番号　62/209,326
(32)優先日　平成27年8月24日 (2015.8.24)
(33)優先権主張国　米国 (US)
(31)優先権主張番号　15/006,908
(32)優先日　平成28年1月26日 (2016.1.26)
(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　100108855
弁理士　蔵田　昌俊
(74)代理人　100109830
弁理士　福原　淑弘
(74)代理人　100158805
弁理士　井関　守三
(74)代理人　100112807
弁理士　岡田　貴志

最終頁に続く

(54)【発明の名称】データリンクグループのためのグループ鍵告知および配布

(57)【要約】
ワイヤレス通信のためのデバイスは、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。デバイスはまた、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を含む。告知メッセージは、マルチキャストメッセージを含み、候補グループ鍵の利用可能性と告知メッセージとを示す。

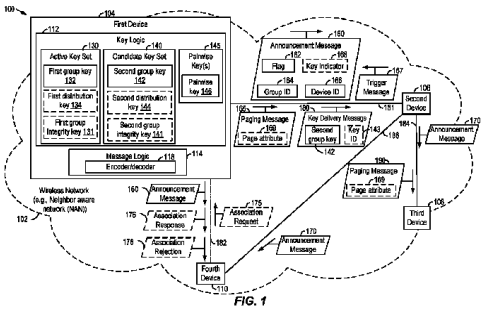

FIG. 1

【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。
【請求項２】
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、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、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、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、請求項１に記載のデバイス。
【請求項５】
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、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、
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】
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。
【請求項１１】
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１０に記載の方法。
【請求項１２】
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１０に記載の方法。
【請求項１３】
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１０に記載の方法。
【請求項１４】
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１３に記載の方法。
【請求項１５】
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１０に記載の方法。
【請求項１６】
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１０に記載の方法。
【請求項１７】
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１６に記載の方法。
【請求項１８】
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。
【請求項１９】
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、請求項１８に記載のデバイス。
【請求項２０】
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、請求項１９に記載のデバイス。
【請求項２１】
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。
【請求項２２】
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２１に記載の方法。
【請求項２３】
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２１に記載の方法。
【請求項２４】
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、請求項２１に記載の方法。
【請求項２５】
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２１に記載の方法。
【請求項２６】
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、請求項２１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２１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２１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、
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２１に記載の方法。
【発明の詳細な説明】
【技術分野】
【０００１】
優先権の主張
[0001]本出願は、下記の出願の各々の内容全体が参照により本明細書に明確に組み込まれる、同一出願人が所有する、２０１５年１月２７日に出願された「ＧＲＯＵＰ　ＫＥＹ　ＡＮＮＯＵＮＣＥＭＥＮＴ　ＡＮＤ／ＯＲ　ＤＩＳＴＲＩＢＵＴＩＯＮ　ＦＯＲ　Ａ　ＧＲＯＵＰ」と題する米国仮特許出願番-号第６２／１０８，３７４号、２０１５年８月２４日に出願された「ＧＲＯＵＰ　ＫＥＹ　ＡＮＮＯＵＮＣＥＭＥＮＴ　ＡＮＤ　ＤＩＳＴＲＩＢＵＴＩＯＮ　ＦＯＲ　Ａ　ＧＲＯＵＰ」と題する米国仮特許出願番号第６２／２０９，３２６号、および２０１６年１月２６日に出願された「ＧＲＯＵＰ　ＫＥＹ　ＡＮＮＯＵＮＣＥＭＥＮＴ　ＡＮＤ　ＤＩＳＴＲＩＢＵＴＩＯＮ　ＦＯＲ　Ａ　ＤＡＴＡ　ＬＩＮＫ　ＧＲＯＵＰ」と題する米国非仮特許出願番号第１５／００６，９０８号の優先権を主張する。

【０００２】
[0002]本開示は、概して、グループ鍵の告知および配布に関する。
【背景技術】
【０００３】
[0003]ネイバーアウェアネットワーク（ＮＡＮ：neighbor aware network）またはワイヤレスメッシュネットワークのデータリンクグループ中に含まれるデバイスは、グループアドレス指定されたトラフィックを暗号化するためにグループ鍵（たとえば、共通グループ鍵）などのセキュリティ証明を使用する。セキュリティの理由のために、データリンクグループのデバイスによって使用される特定のグループ鍵（たとえば、アクティブグループ鍵）は、対応する時間期間の後に満了する。周期的に、新しいグループ鍵が、生成され、データリンクグループの各デバイスにセキュアに配布される。例示のために、新しいグループ鍵を生成する特定のデバイスは、データリンクグループの他のデバイスに鍵告知メッセージを送り得、ピア交換メッセージング（たとえば、ポイントツーポイント（Ｐ２Ｐ）通信）を使用してデータリンクグループの１つまたは複数のデバイス（たとえば、１つまたは複数の隣接デバイス）に新しいグループ鍵を送り得る。新しいグループ鍵は、追加の関連付け動作とデータリンクグループ中のデバイス間のユニキャストメッセージ交換とを使用してデータリンクグループの各デバイスに配布され得る。グループ鍵を配布するために関連付け動作またはユニキャストメッセージ交換を実行することは、ＮＡＮまたはワイヤレスメッシュネットワークに有意なトラフィックおよびオーバーヘッドを追加し得る。
【発明の概要】
【０００４】
[0004]特定の態様では、デバイスは、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。本デバイスはまた、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を含む。告知メッセージは、マルチキャストメッセージを含み、候補グループ鍵の利用可能性を示す。
【０００５】
[0005]別の特定の態様では、方法は、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を含む。本方法は、データリンクグループの第１のデバイスから第２のデバイスに、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をさらに含む。告知メッセージは、マルチキャストメッセージを含み、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。
【０００６】
[0006]特定の態様では、デバイスは、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。本デバイスはまた、ページングウィンドウ中に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を含む。告知メッセージは、マルチキャストメッセージを含み、候補グループ鍵の利用可能性を示す。
【０００７】
[0007]別の特定の態様では、方法は、データリンクグループの第２のデバイスにおいて、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ことを含む。本方法は、ページングウィンドウ中にデータリンクグループの第１のデバイスから第２のデバイスにおいて告知メッセージを受信することをさらに含む。告知メッセージは、マルチキャストメッセージを含み、候補グループ鍵の利用可能性を示す。
【０００８】
[0008]別の特定の態様では、デバイスは、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。本デバイスはまた、第１の通信チャネル

の発見ウィンドウ中に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を含む。告知メッセージは、マルチキャストメッセージを含み、候補グループ鍵の利用可能性を示す。

【０００９】

[0009]別の特定の態様では、方法は、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を含む。本方法は、データリンクグループの第１のデバイスからデバイスに、利用可能性候補グループ鍵を示す告知メッセージを送信することをさらに含む。告知メッセージは、マルチキャストメッセージを含み、発見ウィンドウ中に第１の通信チャネルを介して送信される。

【００１０】

[0010]別の特定の態様では、デバイスは、データリンクグループに対応する発見ウィンドウ中に第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。本デバイスはまた、発見ウィンドウ中に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を含む。告知メッセージは、マルチキャストメッセージを含み、候補グループ鍵の利用可能性を示す。

【００１１】

[0011]別の特定の態様では、方法は、データリンクグループの第２のデバイスにおいて、データリンクグループに対応する発見ウィンドウ中に第１の通信チャネルを監視することを含む。本方法は、発見ウィンドウ中にデータリンクグループの第１のデバイスから第２のデバイスにおいて告知メッセージを受信することをさらに含む。告知メッセージは、マルチキャストメッセージを含み、候補グループ鍵の利用可能性を示す。

【図面の簡単な説明】

【００１２】

【図１】[0012]告知メッセージの送信とデータリンクグループのグループ鍵の配布とをサポートするシステムの特定の実装形態の図。

【図２】[0013]候補グループ鍵を生成するように構成されたデバイスのブロック図。

【図３】[0014]データリンクグループに対応する通信の例示的な例のタイミング図。

【図４】[0015]配布鍵を使用する例示的な方法のラダー図。

【図５】[0016]データリンクグループに対応する通信の例示的な例のタイミング図。

【図６】[0017]ページ属性フィールドの態様の例示的な例の図。

【図７】[0018]データリンクグループのデバイスにおける動作の第１の例示的な方法のフロー図。

【図８】[0019]データリンクグループのデバイスにおける動作の第２の例示的な方法のフロー図。

【図９】[0020]データリンクグループのデバイスにおける動作の第３の例示的な方法のフロー図。

【図１０】[0021]データリンクグループのデバイスにおける動作の第４の例示的な方法のフロー図。

【図１１】[0022]データリンクグループのデバイスにおける動作の第５の例示的な方法のフロー図。

【図１２】[0023]データリンクグループのデバイスにおける動作の第６の例示的な方法のフロー図。

【図１３】[0024]本明細書で開示する１つまたは複数の方法、システム、装置、およびコンピュータ可読媒体の様々な実装形態をサポートするように動作可能であるワイヤレスデバイスの図。

【発明を実施するための形態】

【００１３】

[0025]本開示の特定の実装形態について、図面を参照しながら以下で説明する。説明では、共通の特徴は、図面全体にわたって共通の参照番号によって指定される。本明細書では、構造、構成要素、動作などの要素を修正するのに使用される順序を示す用語（たとえ

ば、「第１の」、「第２の」、「第３の」など）は、それ自体、別の要素に関する要素の優先順位または順序を示しておらず、要素を、（順序を示す用語の使用を別にすれば）同じ名前を有する別の要素から区別しているだけである。

【００１４】

[0026]本明細書では、様々な用語は、特定の実装形態を記述するためのものにすぎず、実装形態を制限するものではない。たとえば、単数形「ａ」、「ａｎ」および「ｔｈｅ」は、文脈が別段に明確に示すのでなければ、複数形をも含むものとする。さらに、「備える」および「備えている」という用語が、「含む」または「含んでいる」と互換的に使用され得ることが理解され得る。さらに、「ここにおいて」という用語が「ここで」という用語と互換的に使用され得ることを理解されよう。

【００１５】

[0027]本開示では、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データリンクグループ中のデバイスは、新しいグループ鍵（または候補グループ鍵）などのグループ鍵を告知し、配布し得る。データリンクグループの第１のデバイスは、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し得る。たとえば、第１のデバイスは、データリンクグループに対応するグループ送信ウィンドウのページングウィンドウ中にマルチキャストメッセージとして告知メッセージを送り得る。別の例として、告知メッセージは、ＮＡＮに対応する発見ウィンドウ中に送られ得る。告知メッセージは、候補グループ鍵（たとえば、潜在的に「次の」アクティブグループ鍵）の利用可能性を示すフラグを含み得る。データリンクグループの各デバイスは、ページングウィンドウ中に起動している（たとえば、アクティブモードにある）ことがあり、これは、第１のデバイスの隣接デバイスが告知メッセージを受信する可能性を増加させ得る。

【００１６】

[0028]データリンクグループの第２のデバイスは、第１のデバイスから告知メッセージを受信し得、告知メッセージに応答して、第２のデバイスは、第２のデバイスが第１のデバイスに関連するのかどうかを決定し得る。第２のデバイスが第１のデバイスに関連する（たとえば、第１のデバイスと第２のデバイスとが、認証プロシージャなどのセキュリティ関連付けをうまく完了し、セキュアなピアツーピア（Ｐ２Ｐ）通信のためのペアワイズ鍵を確立した）場合、第２のデバイスは、Ｐ２Ｐ通信を介して第１のデバイスから候補グループ鍵を受信し得る。

【００１７】

[0029]第１のデバイスと第２のデバイスとが関連しない場合、第２のデバイスは、第２のデバイスに関連する第３のデバイスから（候補グループ鍵に対応する）第２の告知メッセージを受信するのを待ち得る。たとえば、第２のデバイスに関連しない第１のデバイスから告知メッセージを受信した後に、第２のデバイスは、第２のデバイスに関連する第３のデバイスから第２の告知メッセージを受信するのを待ち得る。第２の告知メッセージを受信したことに応答して、第２のデバイスは、第３のデバイスに候補グループ鍵を要求し得る。第２のデバイスは、データリンクグループのアクティブグループ鍵が満了するよう設定される前の所定の時間まで、関連するデバイスから第２の告知メッセージを受信するのを待ち得る。例示のために、所定の時間が検出されると、アクティブグループ鍵の満了が間近であると見なされ、第２のデバイスは、第１のデバイスなどの関連しないデバイスとセキュリティ関連付けを開始し得、新たに関連したデバイス（たとえば、第１のデバイス）に候補グループ鍵を要求し得る。所定の時間が検出されるまで、関連するデバイスから告知メッセージを受信するのを待つことによって、第２のデバイスは、告知メッセージに応答して第１のデバイスとのセキュリティ関連付けを自動的に開始しない。したがって、候補グループ鍵を取得するためにセキュリティ関連付けを行う（たとえば、認証プロシージャを実行する）１つまたは複数のデバイスに対応するトラフィックの量は、告知メッセージを送ったデバイスに自動的に関連付けられ、それにグループ鍵を要求するデータリンクグループのデバイスと比較して低減され得る。

【００１８】
[0030]図１を参照すると、データリンクグループの１つまたは複数のデバイスを含むシステム１００の特定の実装形態が示されている。システム１００は、データリンクグループのグループ鍵の配布とグループ鍵に対応する告知メッセージの送信とをサポートするＮＡＮまたはワイヤレスメッシュネットワークなどのワイヤレスネットワーク１０２を含む。ワイヤレスネットワーク１０２はまた、１つまたは複数のデータリンクグループを含むかまたはそれに対応し得る。

【００１９】
[0031]ワイヤレスネットワーク１０２は、第１のデバイス１０４、第２のデバイス１０６、第３のデバイス１０８、および第４のデバイス１１０などの１つまたは複数のデバイスを含み得る。デバイス１０４～１１０の各々は、ワイヤレスネットワーク１０２中に含まれる１つまたは複数の他のワイヤレス通信デバイスにデータを送信し、それからデータを受信するように構成されたワイヤレス通信デバイスであり得る。各ワイヤレスデバイスは、ワイヤレスネットワーク１０２の無線局またはワイヤレス通信デバイスなどの局を含むか、またはそれに対応し得る。ワイヤレスネットワーク１０２は、インフラストラクチャネットワークまたはピアツーピアネットワーク（たとえば、アドホックネットワーク）などのインフラストラクチャを伴わないネットワークであり得る。たとえば、ワイヤレスネットワーク１０２（たとえば、ＮＡＮ）のデバイス１０４～１１０の各々は、ＮＡＮに対応する１つまたは複数のワイヤレスチャネルを介して、関連付け動作（たとえば、セキュリティ関連付け動作）、セキュリティ情報交換動作、同期動作、および他の動作を実行するように構成され得る。いくつかの実装形態では、デバイス１０４～１１０は、例示的な非限定的な例として、電気電子技術者協会（ＩＥＥＥ）８０２．１１規格（たとえば、ＩＥＥＥ８０２．１１ｓの規格）、Ｗｉ－Ｆｉ　Ａｌｌｉａｎｃｅ（登録商標）規格、ＮＡＮ規格、またはそれらの組合せなどの１つまたは複数の規格に従ってそのような動作を実行し得る。ワイヤレスネットワーク１０２が４つのデバイスを含むものとして示されているが、他の実装形態では、ワイヤレスネットワーク１０２は５つ以上のデバイスを含むことも、３つ以下のデバイスを含むこともある。

【００２０】
[0032]ワイヤレスネットワーク１０２は、１つまたは複数のデータリンクグループ（たとえば、１つまたは複数のメッシュ）を含むか、またはそれに対応し得る。本明細書で使用するデータリンクグループは、アドホックネットワークなど、インフラストラクチャを伴わないピアツーピアネットワークを含み得る。データリンクグループは、分散型ワイヤレスネットワークなどのネットワークを形成することができる複数のデバイスを含み得る。さらに、データリンクグループの各デバイスは、データリンクグループによって使用される１つまたは複数の通信チャネルとともにインバンドでまたはアウトオブバンドで交換され得る共通のセキュリティ証明を使用し得る。いくつかの実装形態では、データリンクグループのデバイスは、トラフィックおよび他のメッセージを広告および受信するためにデバイスの各々が起動する時間期間などの周期的な起動時間を有するように同期され得る。

【００２１】
[0033]ワイヤレスネットワーク１０２は、デバイス１０４～１１０などの１つまたは複数のデバイスを含むデータリンクグループを含むか、またはそれに対応し得る。データリンクグループは、データリンク、データリンクネットワーク、グループネットワーク、ＮＡＮデータリンク（ＮＤＬ）、ＮＤＬネットワーク、データパスグループ、データパスグループネットワーク、ＮＡＮデータパス、ＮＡＮデータパスグループ、またはＮＡＮデータパスグループネットワークと呼ばれることもある。いくつかの実装形態では、データリンクグループは、例示的な非限定的な例として、「ソーシャルＷｉ－Ｆｉ（登録商標）メッシュネットワーク」または米国電気電子学会（ＩＥＥＥ）８０２．１１ｓメッシュネットワークなどのメッシュネットワーク中に含まれるメッシュグループであり得る。別の例として、データリンクグループは、インフラストラクチャ不要のピアツーピア（ｐ２ｐ）

ネットワークを含み得る。

【００２２】

[0034]データリンクグループの一部として、データリンクグループのデバイス１０４～１１０は、（たとえば、１つまたは複数のワイヤレスキャリア、１つまたは複数のＷｉ－Ｆｉアクセスポイント、インターネット、またはそれらの組合せを伴うことなしに）ワイヤレス通信を介してデータ交換を実行し得る。たとえば、データリンクグループのデバイス１０４～１１０は、通信を可能にするためにグループ鍵（たとえば、共通のグループ鍵）などのセキュリティ証明を共有し得る。例示のために、データリンクグループの各デバイスは、グループメッセージを符号化および復号するためにグループ鍵を使用し得る。いくつかの実装形態では、音楽サービス、ソーシャルメディア共有サービス、ファイル共有サービス、ゲームサービス、または他のサービスなどの１つまたは複数のサービスが、データリンクグループのデバイス１０４～１１０のうちの１つまたは複数によって与えられ得る。いくつかの実装形態では、データリンクグループのデバイス１０４～１１０は、デバイス１０４～１１０の各々がサービスを広告するために、トラフィックまたは他のメッセージを受信するために、あるいはそれらの組合せのために（たとえば、アクティブ動作モードで）「起動」している時間期間などの周期的な起動時間を有するように同期され得る。いくつかの実装形態では、ワイヤレスネットワーク１０２は、複数のデータリンクグループを含み得、ワイヤレスネットワーク１０２の各データリンクグループは、一意の値（たとえば、バイト値、グループアドレス、またはそれらの組合せ）などの対応するグループ識別子を有し得る。ワイヤレスネットワーク１０２が複数のデータリンクグループを含むとき、特定のデバイスは、２つ以上のデータリンクグループ中に含まれ得る。ワイヤレスネットワーク１０２がデータリンクグループ中に含まれる４つのデバイスを有するものとして記述されているが、他の実装形態では、ワイヤレスネットワーク１０２は５つ以上のデバイスを含むことも、３つ以下のデバイスを含むこともある。

【００２３】

[0035]第１のデバイス１０４は、鍵論理１１２とメッセージ論理１１４とを含み得る。鍵論理１１２は、アクティブ鍵セット１３０と、候補鍵セット１４０と、１つまたは複数のペアワイズ鍵１４５とを含むこと（または記憶すること）を行い得る。アクティブ鍵セット１３０は、データリンクグループに対応する、データリンクグループのデバイスによって使用されるように設定される１つまたは複数の鍵を含み得る。例示のために、アクティブ鍵セット１３０は、第１のグループ鍵１３２、第１の配布鍵１３４、第１のグループ完全性鍵１３１、またはそれらの組合せを含み得る。特定の実装形態では、アクティブ鍵セット１３０は、鍵１３１、１３２、および１３４のうちの２つを含み得、２つの鍵は、鍵ペアと呼ばれることがある。別の特定の実装形態では、アクティブ鍵セット１３０は、鍵１３１、１３２、および１３４のすべてを含み得、３つの鍵は、鍵トリオと呼ばれることがある。同様に、候補鍵セット１４０は、第２のグループ鍵１４２、第２の配布鍵１４４、第２のグループ完全性鍵１４１、またはそれらの組合せを含み得る。単一のアクティブ鍵セット１３０および単一の候補鍵セット１４０として説明されるが、いくつかの実装形態では、鍵論理１１２は、複数のアクティブ鍵セット、複数の候補鍵セット、またはその両方を記憶するように構成され得る。たとえば、鍵論理１１２は、第１のデータリンクグループに対応する第１のアクティブ鍵セットと第２のデータリンクグループに対応する第２のアクティブ鍵セットとを記憶するように構成され得る。

【００２４】

[0036]アクティブ鍵セット１３０は、データリンクグループのアクティブグループ鍵として設定される第１のグループ鍵１３２を含み得る。第１のグループ鍵１３２により、データリンクグループのデバイス間で通信されるデータリンクグループメッセージの暗号化（または符号化）と解読（または復号）とが可能になり得る。

【００２５】

[0037]随意に、アクティブ鍵セット１３０は、データリンクグループのアクティブ配布鍵として設定される第１の配布鍵１３４を含み得る。第１の配布鍵１３４は、第１のグル

ープ鍵１３２と第１の配布鍵１３４とが第１の鍵ペアを構成するように第１のグループ鍵１３２に対応し得る。第１の配布鍵１３４がアクティブ配布鍵として設定されると、第１の配布鍵１３４は、本明細書でさらに説明するように、データリンクグループの他のデバイスに通信されるべき候補グループ鍵、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暗号化するために使用され得る。

【００２６】

[0038]さらに、アクティブ鍵セット１３０は、データリンクグループのアクティブ完全性グループ鍵として設定される第１の完全性グループ鍵１３１を含み得る。第１の完全性グループ鍵１３１は、第１のグループ鍵１３２、第１の配布鍵１３４、またはその両方に対応し得る。アクティブ鍵セット１３０が、第１のグループ鍵１３２と、第１の配布鍵１３４と、第１の完全性グループ鍵１３１とを含む実装形態では、第１のグループ鍵１３２と、第１の配布鍵１３４と、第１の完全性グループ鍵１３１とは第１の鍵トリオを構成する。第１の完全性グループ鍵１３１がアクティブ完全性グループ鍵として設定されると、第１の完全性グループ鍵１３１は、暗号化されていない（または符号化されていない）グループアドレス指定されたトラフィックの完全性保護のために使用され得る。たとえば、暗号化されていないグループアドレス指定されたメッセージとして送るべきメッセージをもつデバイスは、メッセージと第１の完全性グループ鍵１３１とに基づいて値を生成し得る。値は、メッセージの特定のフィールド中に含まれ得る。特定の実装形態では、値は、ＩＥＥＥ８０２．１１規格によるメッセージ完全性コード（ＭＩＣ）フィールド中に含まれる。暗号化されていないグループアドレス指定されたメッセージを受信するデバイスは、暗号化されていない（または符号化されていない）グループアドレス指定されたメッセージを検証するために第１のグループ完全性鍵１３１を使用し得、これは、デバイスが、グループアドレス指定されたトラフィックを改変し、改変されたグループアドレス指定されたトラフィックを中継することに対するセキュリティを与え得る。例示のために、第１のデバイス１０４の鍵論理１１２は、第１のグループ完全性鍵１３１と受信された第１の暗号化されていない（または符号化されていない）マルチキャストメッセージとに基づいて第１の値を生成し得、鍵論理１１２は、受信された暗号化されていない（または符号化されていない）マルチキャストメッセージのＭＩＣフィールド中の特定の値などのメッセージ中の特定の値と第１の値を比較し得る。第１の値が特定の値に一致する場合、鍵論理１１２は、第１の暗号化されていないマルチキャストメッセージを検証し得る。第１の値が特定の値に一致しない場合、鍵論理１１２は、第１の暗号化されていないマルチキャストメッセージを検証することができないことがある。特定の実装形態では、検証されないメッセージは、転送されず、破棄されるかあるいは消去される。

【００２７】

[0039]１つまたは複数のペアワイズ鍵１４５は、第１のデバイス１０４と第１のデバイス１０４に関連するデバイスとの間のピアツーピア（Ｐ２Ｐ）通信のために使用され得る。たとえば、１つまたは複数のペアワイズ鍵１４５は、本明細書でさらに説明するように、第１のデバイス１０４と第２のデバイス１０６（第１のデバイス１０４に関連するデバイス）との間のＰ２Ｐ通信のために使用され得るペアワイズ鍵１４６を含み得る。デバイスと第１のデバイス１０４とは、関連付けられるために関連付けプロセスを実行し得る。第１のデバイス１０４に関連するデバイスは、第１のデバイス１０４と関連する状態にあると呼ばれることもある。

【００２８】

[0040]アクティブ鍵セット１３０中に含まれる各鍵は、対応する時間期間の間アクティブ鍵として設定され得る。たとえば、第１のグループ鍵１３２は、アクティブグループ鍵として設定され得、第１の時間期間の間アクティブ鍵セット１３０中に含まれ得る。別の例として、第１の配布鍵１３４は、アクティブ配布鍵として設定され得、第２の時間期間の間アクティブ鍵セット１３０中に含まれ得る。別の例として、第１のグループ完全性鍵１３１は、第３の時間期間の間アクティブ鍵セット１３０中に含まれ得る。他の実装形態では、第１の時間期間と、第２の時間期間と、第３の時間期間とは、同じ時間期間であり

得る。第１の時間期間、第２の時間期間、第３の時間期間、またはそれらの組合せは、データリンクグループ中に含まれる各デバイスによって知られている（または決定可能である）所定の時間期間であり得る。いくつかの実装形態では、第１の時間期間、第２の時間期間、または第３の時間期間は、鍵有効時間期間の別のものと部分的に重複し得る。特定の実装形態では、第１の時間期間は、ＩＥＥＥ８０２．１１規格、Ｗｉ－Ｆｉ　Ａｌｌｉａｎｃｅ規格、ＮＡＮ規格、またはそれらの組合せなどのワイヤレス通信規格において定義されている。他の実装形態では、第１の時間期間と第２のものとは、データリンクグループのデバイスによってネゴシエートされ得る。いくつかの実装形態では、第１の時間期間は、他のグループ鍵の時間期間と重複し得る。特定の実装形態では、第１のグループ鍵１３２と第１の時間期間とは満了しない。たとえば、第１の時間期間は、無制限の寿命を示し得るか、または終了時間を示さないことがあり、したがって、第１のグループ鍵１３２は、無制限の寿命を有し得、満了しないことがある。第１のグループ鍵１３２が満了しないと、デバイス１０４～１１０は、第１のグループ鍵１３２を置き換えるために候補鍵を生成しないことがある。

【００２９】

[0041]候補鍵セット１４０は、アクティブ鍵セット１３０のアクティブ鍵として設定されるために利用可能である１つまたは複数の鍵を含み得る。候補鍵セット１４０は、第２のグループ鍵１４２（たとえば、候補グループ鍵）、第２の配布鍵１４４（たとえば、候補配布鍵）、第２のグループ完全性鍵１４１（たとえば、候補グループ完全性）、またはそれらの組合せを含み得る。第２の配布鍵１４４は、第２のグループ鍵１４２と第２の配布鍵１４４とが第２の鍵ペアを構成するように第２のグループ鍵１４２に対応し得る。第２のグループ鍵１４２は、アクティブグループ鍵として使用され得（たとえば、設定され得）、第１の時間期間の満了時にアクティブ鍵セット１３０中に含まれ得る。したがって、第２のグループ鍵１４２は、アクティブグループ鍵として第１のグループ鍵１３２に続き得る（たとえば、それを置き換え得る）。第２の配布鍵１４４は、アクティブ配布鍵として使用され得（たとえば、設定され得）、第２の時間期間の満了時にアクティブ鍵セット１３０中に含まれ得る。したがって、第２の配布鍵１４４は、アクティブ配布鍵として第１の配布鍵１３４に続き得る（たとえば、それを置き換え得る）。第２のグループ完全性鍵１４１は、第３の時間期間の満了時に第１のグループ完全性鍵１３１に続き得る（たとえば、それを置き換え得る）。

【００３０】

[0042]第２のグループ完全性鍵１４１（たとえば、候補グループ完全性鍵）は、第２のグループ鍵１４２と、第２の配布鍵１４４と、第２のグループ完全性鍵１４１とが第２の鍵トリオを構成するように第２のグループ鍵１４２、第２の配布鍵１４４、またはその両方に対応し得る。第２のグループ完全性鍵１４１は、第１のグループ完全性鍵１３１に続き得（たとえば、それを置き換え得）、暗号化されていない（または符号化されていない）グループアドレス指定されたトラフィックのための完全性保護のために使用され得る。

【００３１】

[0043]候補鍵セット１４０は、アクティブ鍵セット１３０の満了より前に第１のデバイス１０４によって取得され得る。たとえば、第２のグループ鍵１４２は、第１の時間期間の満了の前に（たとえば、アクティブグループ鍵として第１のグループ鍵１３２の満了より前に）第１のデバイス１０４によって取得され得る。候補鍵セット１４０を取得するために、第１のデバイス１０４は、図２を参照しながら説明するように、候補鍵セット１４０を生成するように構成され得る。追加または代替として、候補鍵セット１４０は、本明細書でさらに説明するように、データリンクグループの別のデバイスによって生成され、鍵配信メッセージ１８０を使用して第１のデバイス１０４に通信され得る（たとえば、配布され得る）。

【００３２】

[0044]メッセージ論理１１４は、ワイヤレスネットワーク１０２のデバイス間で通信されるメッセージを生成し、処理するように構成され得る。メッセージ論理１１４は、ワイ

ヤレスネットワーク１０２のデバイス１０４～１１０の間で通信されるメッセージを符号化および復号するように構成されるエンコーダ／デコーダ１１８を含み得る。たとえば、エンコーダ／デコーダ１１８は、データリンクグループの別のデバイスに通信されるべきメッセージを符号化（たとえば、暗号化）するために、１３２または１３４などのアクティブ鍵セット１３０のうちの１つを使用し得る。他の実装形態では、メッセージ論理１１４は、エンコーダと、エンコーダとは別個であるデコーダとを含み得る。

【００３３】

[0045]いくつかの実装形態では、メッセージ論理１１４は、第１のデバイス１０４と、（実線１８１によって示されるように）第１のデバイス１０４に関連する第２のデバイス１０６などのデバイスとの間で通信されるセキュアなメッセージを符号化および復号するように構成され得る。例示のために、第１のデバイス１０４と第２のデバイス１０６とは、第１のデバイス１０４と第２のデバイス１０６との間のピアツーピア（Ｐ２Ｐ）通信を可能にするためにセキュリティ関連付けを行うか、またはそれを実行し得る（たとえば、認証プロセスを実行し得る）。認証プロセスの一部として、ペアワイズ鍵１４６は、第１のデバイス１０４と第２のデバイス１０６との間のセキュアな通信を可能にするために生成され得る。ペアワイズ鍵１４６は、第１のデバイス１０４と第２のデバイス１０６との各々に記憶され得る。たとえば、第１のデバイス１０４は、１つまたはペアワイズの鍵１４５中にペアワイズ鍵１４６を含み得る。第１のデバイス１０４が第２のデバイス１０６に関連する限り、１つまたは複数のペアワイズ鍵１４５は、ペアワイズ鍵１４６を含み得る。メッセージ論理１１４は、第１のデバイス１０４と第２のデバイス１０６との間で通信される１つまたは複数のＰ２Ｐメッセージを符号化および復号するためにペアワイズ鍵１４６を使用し得る。

【００３４】

[0046]追加または代替として、ワイヤレスネットワーク１０２のデバイス１０４～１１０の間で通信されるメッセージのうちの１つまたは複数は、符号化されないことがある（たとえば、暗号化されないことがある）。たとえば、メッセージ論理１１４は、メッセージを生成し得、第１のデバイス１０４は、エンコーダ／デコーダ１１８を使用してメッセージを符号化することなしにワイヤレスネットワーク１０２の別のデバイスにメッセージを送り得る。例示のために、第１のデバイス１０４は、（破線１８２によって示されるように）第４のデバイス１１０に関連しないことがあり、第１のデバイス１０４は、第４のデバイス１１０に非セキュアなメッセージ（たとえば、符号化されていないメッセージまたは暗号化されていないメッセージ）を送り得る。さらに、第１のデバイス１０４は、１つまたは複数の関連するデバイスに非セキュアなメッセージを送り得る。

【００３５】

[0047]動作中、第１のデバイス１０４は、第１のグループ鍵１３２の満了より前に第２のグループ鍵１４２を生成するように構成され得る。たとえば、第１のデバイス１０４は、図２を参照しながらさらに説明するように、ランダム値または擬似ランダム値からのカウントダウンを完了したことに応答して、第２のグループ鍵１４２を生成し得る。第２のグループ鍵１４２は、データリンクグループ中の各デバイスがグループメッセージ（たとえば、グループ送信）を暗号化および解読することを可能にするために第１のグループ鍵１３２をデータリンクグループのアクティブグループ鍵として置き換え得る。

【００３６】

[0048]いくつかの実装形態では、データリンクグループのデバイス１０４～１１０は、乱数発生によってグループ鍵を生成し得る。たとえば、第１のデバイス１０４は、乱数発生器、擬似乱数生成器、または他の乱数発生方法を使用することによって第２のグループ鍵１４２を生成するように構成され得る。第２のグループ鍵１４２は、ランダムに生成されたまたは擬似ランダムに生成された２５６ビットを含み得る。ワイヤレスネットワーク１０２の各データリンクグループは、一意のグループ鍵を含み得る。データリンクグループのデバイスは、前に使用されたグループ鍵を使用しないことがある。たとえば、データリンクグループのデバイスは、グループ鍵の再利用を防げるために、満了した鍵（たとえ

ば、満了したアクティブ鍵セット）と候補鍵（たとえば、候補鍵セット）とを記憶し得る。例示のために、第１のデバイス１０４は、第１のグループ鍵１３２を生成し、第２のグループ鍵１４２が一意であるのかどうかを決定するために第１のグループ鍵１３２を第２のグループ鍵１４２と比較し得る。第２のグループ鍵１４２が一意でないと決定したことに応答して、第１のデバイス１０４は、第２の候補グループ鍵などの別の候補鍵をランダムに生成し得る。第２のグループ鍵１４２が一意であると決定したことに応答して、第１のデバイス１０４は、第２のグループ鍵１４２の生成に対応するかまたはそれを示す告知メッセージを送信し得る。特定の実装形態では、第２のグループ鍵１４２は、ランダム値からのカウントダウンに応答して生成され得る。

【００３７】

[0049]いくつかの実装形態では、データリンクグループの専用デバイスは、候補グループ鍵を生成するように構成され得る。デバイスは、データリンクグループの鍵生成器デバイスと呼ばれることがある。例示のために、特定のデバイスが、鍵生成器デバイスとして動作する間に、データリンクグループの他のデバイスは、グループ鍵（または候補グループ鍵）を生成しないことがある。鍵生成器デバイスはまた、データリンクグループの「リーダー」デバイスと呼ばれることもある。いくつかの実装形態では、鍵生成器デバイスは、１対１のサービス、１対多のサービス、またはその両方など、データリンクグループのサービスのプロバイダであり得る。いくつかの実装形態では、データリンクグループの特定のデバイスは、１つまたは複数の基準を満たすことに基づいて鍵生成器デバイスとして動作することを決定し得る。たとえば、第１のデバイス１０４は、第１のデバイス１０４がデータリンクグループの発信者であることに基づいて、第１のデバイス１０４が、データリンクグループの任意の他のデバイスと比べてデータリンクグループのより多くのデバイスと関連する状態にあることに基づいて、第１のデバイス１０４が、データリンクグループの他のデバイスと比べてＮＡＮ中でより多くの時間を費やしたことに基づいて、第１のデバイス１０４と関連する状態にあるデバイスの数に基づいて、ＮＡＮのトポロジーに基づいて、第１のデバイス１０４がＮＡＮ中に含まれていた持続時間に基づいて、ＮＡＮ内の第１のデバイス１０４のランクに基づいて、第１のデバイス１０４のバッテリーレベルに基づいて、またはそれらの組合せで、鍵生成器デバイスとして動作することを決定し得る。特定の実装形態では、鍵生成器デバイスは、データリンクグループの発信者によるデータリンクグループの作成後に示され得る。たとえば、発信者は、特定のデバイスが鍵生成器デバイスとして動作すべきであることを示すメッセージをデータリンクグループのデバイスに送信し得る。

【００３８】

[0050]別の特定の実装形態では、データリンクグループの特定のデバイスは、データリンクグループのデバイスによって鍵生成器デバイスとして動作するように選択され得る。選択は、上に列挙した基準のうちの１つまたは複数に基づき得る。たとえば、特定のデバイスは、データリンクグループの他のデバイスと比べて特定のデバイスがデータリンクトポロジー中でより「有利な」位置を有することに基づいて鍵生成器デバイスとして動作するように選択され得る。データリンクグループのトポロジー中の有利な位置は、データリンクグループの互いのデバイスからのホップのしきい値数と比べて特定のデバイスがより少ないことに対応し得る。別の例として、特定のデバイスは、特定のデバイスがデータリンクグループの任意の他のデバイスよりも多くのデバイスと関連する状態にあることに基づいて鍵生成器デバイスとして動作するように選択され得る。

【００３９】

[0051]特定の実装形態では、現在の鍵生成器デバイスが、利用不可能になるか、または鍵生成動作の実行を終了する場合、候補鍵を生成するように構成されたデバイスが鍵生成器デバイスになり得る。たとえば、鍵生成器デバイスとして現在動作している特定のデバイスが、データリンクグループまたはＮＡＮとの関連付けを解除する場合、または特定のデバイスが、鍵生成動作を実行する能力がないことを示す場合、データリンクグループの異なるデバイスが鍵生成器デバイスとして動作するように選択され得る。特定の実装形態

では、利用不可能になるより前に、特定のデバイスは、鍵生成器デバイスとして動作すべき異なるデバイスを選択し得、特定のデバイスは、選択されたデバイスにメッセージを送信し得る。別の実装形態では、デバイスは、特定のデバイスが鍵生成動作をもはや実行していないと決定し得、デバイスは、鍵生成動作を実行し始め得る。代替的に、データリンクグループの異なるデバイスは、鍵生成器デバイスとして動作するようにデータリンクグループのデバイスによって選択され得る。

【００４０】

[0052]データリンクグループのデバイスはまた、グループ鍵に対応するメッセージを送信または受信するように構成され得る。例示のために、メッセージ論理１１４は、データリンクグループのデバイス間で通信されるメッセージを生成し、処理するように構成され得る。いくつかの実装形態では、メッセージ論理１１４は、第１のデバイス１０４と、（実線１８１によって示されるように）第１のデバイス１０４に関連する第２のデバイス１０６などのデバイスとの間で通信されるセキュアなメッセージを符号化および復号するかまたは暗号化および解読するように構成され得る。いくつかの実装形態では、第１のグループ鍵１３２は、マルチキャストデータまたはブロードキャストデータなどのグループアドレス指定されたデータを暗号化または解読するために使用され得る。

【００４１】

[0053]第１のデバイス１０４は、第２のグループ鍵１４２の生成に対応する告知メッセージ１６０を生成するように構成され得る。たとえば、メッセージ論理１１４は、告知メッセージ１６０を生成するように構成され得る。告知メッセージ１６０は、候補鍵セット１４０の少なくとも１つの鍵が利用可能であることを示し得る。たとえば、候補グループ鍵（たとえば、第２のグループ鍵１４２）が、利用可能であり、アクティブグループ鍵として第１のグループ鍵１３２を置き換えるべきである告知メッセージ１６０。告知メッセージ１６０は、第２のグループ鍵１４２を生成したことに応答して、データリンクグループの他のデバイス１０６～１１０に第２のグループ鍵１４２を配布する前に第１のデバイス１０４によって生成され得る。代替的に、第２のグループ鍵１４２は、カウントダウンの完了後に生成され得、告知メッセージ１６０は、カウントダウンの完了に応答して、第２のグループ鍵１４２の生成または配布より前に生成され得る。いくつかの実装形態では、告知メッセージ１６０は、第１のグループ鍵１３２またはペアワイズ鍵１４６などの鍵を使用してメッセージ論理１１４によって符号化（または暗号化）され得る。他の実装形態では、メッセージ論理１１４は、告知メッセージ１６０を符号化（または暗号化）しないことがある。

【００４２】

[0054]告知メッセージ１６０は、フラグ１６２と、グループ識別子（ＩＤ）１６４と、デバイスＩＤ１６６とを含み得る。フラグ１６２は、告知メッセージがグループ鍵告知メッセージであることを示す１つまたは複数のビット、フィールド、またはそれらの組合せを含み得る。グループＩＤ１６４は、データリンクグループを一意に識別するデータリンクグループの識別子であり得る。たとえば、グループＩＤ１６４は、データリンクグループに対応するバイト値またはグループアドレスなどの１つまたは複数のビットを含み得る。デバイスＩＤ１６６は、候補グループ鍵を生成したデバイスに対応する媒体アクセス制御（ＭＡＣ）アドレスであり得る。たとえば、告知メッセージ１６０のデバイスＩＤ１６６は、第１のデバイス１０４のＭＡＣアドレスであり得る。いくつかの実装形態では、告知メッセージ１６０は、第２のグループ鍵１４２（または候補鍵セット１４０）が生成されたとき、または第２のグループ鍵１４２（または候補鍵セット１４０）の生成が開始されたときに対応するタイムスタンプを含み得る。追加または代替として、告知メッセージ１６０は、告知メッセージ１６０を送信する特定のデバイスに対応する第２のデバイスＩＤを含み得る。たとえば、第２のデバイスＩＤは、第１のデバイス１０４など、告知メッセージ１６０を送信するデバイスのＭＡＣアドレスであり得る。

【００４３】

[0055]いくつかの実装形態では、告知メッセージ１６０はまた、鍵インジケータ１６８

を含む。鍵インジケータ１６８は、第２のグループ鍵１４２に関係する情報を与え得る。たとえば、鍵インジケータ１６８は、第２のグループ鍵１４２、第２のグループ鍵１４２の生成に対応するタイムスタンプ、第１のデバイス１０４のＭＡＣアドレス、またはそれらの組合せに基づいて生成されるハッシュ値を含み得る。鍵インジケータ１６８は、本明細書でさらに説明するように、告知メッセージ１６０を受信するデバイスが、第２のグループ鍵１４２がデータリンクグループのための次のアクティブ鍵になるべきであるのかどうかを決定することを可能にし得る。

【００４４】

[0056]告知メッセージ１６０の生成の後に、第１のデバイス１０４は、告知メッセージ１６０をデータリンクグループの他のデバイスに送信し得る。告知メッセージ１６０は、セキュアなメッセージとして、または非セキュアなメッセージとして送られ得る。告知メッセージ１６０がセキュアなメッセージとして送られる場合、告知メッセージ１６０は、暗号化されたメッセージであり得、告知メッセージ１６０が非セキュアなメッセージとして送られる場合、告知メッセージ１６０は、暗号化されていないメッセージであり得る。たとえば、告知メッセージ１６０を送るより前に、エンコーダ／デコーダ１１８は、第１のグループ鍵１３２などのアクティブ鍵セット１３０の特定の鍵を使用して告知メッセージ１６０を暗号化し得る。代替的に、エンコーダ／デコーダ１１８は、告知メッセージ１６０を暗号化しないことがある。告知メッセージ１６０が暗号化されない場合、エンコーダ／デコーダ１１８は、第１のグループ完全性鍵１３１を使用して告知メッセージ１６０を保護し得る。

【００４５】

[0057]第１のデバイス１０４は、データリンクグループのデバイス１０６～１１０のうちの少なくとも１つにマルチキャストメッセージとして告知メッセージ１６０を送信するように構成され得る。告知メッセージ１６０は、第１のワイヤレスチャネルを介して送信され得る。告知メッセージ１６０は、第１のデバイス１０４に関連するデバイスと第１のデバイス１０４に関連しないデバイスとに送信され得る。たとえば、告知メッセージ１６０は、（実線１８１によって示されるように）第１のデバイス１０４に関連する第２のデバイス１０６に送信され得る。さらに、告知メッセージ１６０は、（破線１８２によって示されるように）第１のデバイス１０４に関連しない第４のデバイス１１０に送信され得る。第１のワイヤレスチャネルは、ＮＡＮ通信チャネル、データリンクグループチャネル、またはその両方に対応し得る。

【００４６】

[0058]特定の実装形態では、第１のデバイス１０４は、第１の通信チャネルのページングウィンドウ中に告知メッセージ１６０を送信し得る。ページングウィンドウは、データリンクグループ用に指定され得、ページングウィンドウは、ＮＡＮ通信チャネルまたはデータリンクグループチャネルに対応し得る。例示のために、ページングウィンドウは、ＮＡＮ通信チャネルまたはデータリンクグループチャネルを介した特定の通信用に指定された特定の時間期間を含み得る。別の特定の実装形態では、第１のデバイス１０４は、第１の通信チャネルの発見ウィンドウ中に告知メッセージ１６０を送信し得る。発見ウィンドウは、ＮＡＮ通信チャネルに対応し得る。追加または代替として、第１のデバイス１０４は、第１のデバイス１０４に関連する第２のデバイス１０６などの特定のデバイスにピアツーピア（Ｐ２Ｐ）通信として告知メッセージ１６０を送り得る。

【００４７】

[0059]データリンクグループのデバイス１０４～１１０の各々は、ページングウィンドウ、発見ウィンドウ、またはその両方中にアクティブモードにあり得、これは、第１のデバイス１０４の隣接デバイスが告知メッセージ１６０を受信する可能性を増加させ得る。第１のデバイス１０４から１ホップだけ離れているデバイスなど、第１のデバイス１０４の通信範囲内にあるデバイスが告知メッセージ１６０を受信し得る。たとえば、第２のデバイス１０６と第４のデバイス１１０とは、告知メッセージ１６０を受信し得、デバイス１０６および１１０が、ＩＥＥＥ８０２．１１ｓ規格、Ｗｉ－Ｆｉ　Ａｌｌｉａｎｃｅ規

格、またはそれらの組合せによって記述されているように、第１のデバイス１０４の特定の通信範囲（たとえば、１ホップの範囲）内にあるので、第１のデバイス１０４の「隣接」デバイスと呼ばれることがある。第３のデバイスは、第１のデバイス１０４から複数ホップだけ離れているので、第３のデバイス１０８は、特定の通信範囲内になく、第１のデバイス１０４の隣接デバイスであるとは考えられない。

【００４８】

[0060]告知メッセージ１６０がデータリンクグループ中の各デバイスに達するように、１つまたは複数のデバイスは、告知メッセージ１６０を受信し、転送し得る。たとえば、第２のデバイス１０６が第１のデバイス１０４から告知メッセージ１６０を受信したことに応答して、第２のデバイス１０６は、データリンクグループの他のデバイスに告知メッセージ１７０（たとえば、転送された告知メッセージ）として告知メッセージ１６０を転送し得る。例示のために、第２のデバイス１０６は、第３のデバイス１０８と第４のデバイス１１０とに告知メッセージ１７０を送り得る。いくつかの実装形態では、他のデバイスが、告知メッセージ１６０に対応する第２のグループ鍵１４２（または候補鍵セット１４０）を受信する後まで、第１のデバイス１０４から告知メッセージ１６０を受信する別のデバイスは、告知メッセージ１６０を転送しないことがある。

【００４９】

[0061]いくつかの実装形態では、メッセージ論理１１４は、告知メッセージ１６０が送信された後にページングメッセージ１６５を生成するようにさらに構成され得る。ページングメッセージ１６５は、第１のデバイス１０４などの特定のデバイスからデータリンクグループの他のデバイスに送信するようにデータをスケジュールしたことを示し得る。送信するようにスケジュールしたデータは、第２のグループ鍵１４２など、候補鍵セット１４０の少なくとも１つの鍵を含み得る。いくつかの実装形態では、ページングメッセージ１６５はマルチキャストメッセージであり得る。たとえば、ページングメッセージ１６５は、データリンクグループの複数のデバイスに送信され得、ページングメッセージ１６５は、データリンクグループの複数のデバイスに送信するようにデータをスケジュールしたことを示し得る。いくつかの実装形態では、ページングメッセージ１６５は、第１のグループ鍵１３２を使用して暗号化され得る。ページングメッセージ１６５は、ページ属性１６９を随意に含み得る。ページ属性１６９の詳細について、図６を参照しながらさらに説明する。

【００５０】

[0062]第１のデバイス１０４は、第１のデバイス１０４に関連するデータリンクグループの隣接デバイスにページングメッセージ１６５を送信するように構成され得る。たとえば、第１のデバイス１０４は、第２のデバイス１０６にページングメッセージ１６５を送信し得る。いくつかの実装形態では、ページングメッセージ１６５は、第１のワイヤレスチャネル（ＮＡＮ通信チャネル）を介して送信され得る。他の実装形態では、ページングメッセージ１６５は、第２のワイヤレスチャネル（データリンクグループチャネル）を介して送信され得る。ページングメッセージ１６５は、データリンクグループ用に指定された（またはそれに対応する）送信ウィンドウのページングウィンドウ中に送信され得る。データリンクグループの各デバイスは、ページングメッセージが受信および送信され得るように、ページングウィンドウ中にアクティブ動作モードで動作するように構成され得る。

【００５１】

[0063]いくつかの実装形態では、第２のデバイス１０６は、ページングメッセージ１６５を受信したことに応答して第１のデバイス１０４にトリガメッセージ１６７を送信するように構成され得る。トリガメッセージ１６７は、現在の送信ウィンドウまたは後続の送信ウィンドウのデータウィンドウ中にアクティブ動作モードで動作するように第２のデバイス１０６がスケジュールされることを示す。たとえば、データウィンドウ中に第２のデバイス１０６に送信するようにスケジュールされたデータを第１のデバイス１０４が有することを示すページングメッセージ１６５を受信したことに応答して、第２のデバイス１

０６はトリガメッセージ１６７を送信し得る。さらに、第２のデバイス１０６は、第１のデバイス１０４からデータを受信するために、データウィンドウ中にアクティブ動作モードで動作したままであり得る。トリガメッセージ１６７は、ページングウィンドウまたはデータウィンドウ中に第２のワイヤレスチャネル（データリンクグループチャネル）を介して送信され得る。代替的に、トリガメッセージ１６７は、第１のワイヤレスチャネル（ＮＡＮ通信チャネル）を介して送信され得る。

【００５２】

[0064]トリガメッセージ１６７を受信した後に、第１のデバイス１０４は、鍵配信メッセージ１８０を生成し得る。鍵配信メッセージ１８０は、データリンクグループのデバイス１０６～１１０に配布されるべき第２のグループ鍵１４２を含み得る。いくつかの実装形態では、鍵配信メッセージ１８０は、候補鍵セット１４０の１つまたは複数の鍵を含み得る。第１のデバイス１０４は、第１のグループ鍵１３２（たとえば、アクティブグループ鍵）の満了より前に第２のデバイス１０６に鍵配信メッセージ１８０を送信し得る。いくつかの実装形態では、鍵配信メッセージ１８０は、図１中で鍵ＩＤとして示された鍵識別子１４３をさらに含み得る。鍵識別子１４３は、第２のグループ鍵１４２の寿命または有効期限を示し得る。いくつかの実装形態では、鍵配信メッセージ１８０は、セキュアなメッセージであり得、第１のデバイス１０４から第２のデバイス１０６にユニキャストメッセージとして送信され得る。たとえば、鍵配信メッセージ１８０は、ペアワイズ鍵１４６に基づいて暗号化され得、ユニキャスト送信を介して第１のデバイス１０４から第２のデバイス１０６に送信され得る。鍵配信メッセージ１８０は、データウィンドウ中に第２のワイヤレスチャネル（データリンクグループチャネル）を介して送信され得る。代替的に、鍵配信メッセージ１８０は、第１のワイヤレスチャネル（ＮＡＮ通信チャネル）を介して送信され得る。

【００５３】

[0065]第１のデバイス１０４がトリガメッセージ１６７を受信しない場合、たとえば、ページングメッセージ１６５またはトリガメッセージ１６７が宛先に達しない場合、または第２のデバイス１０６がページングメッセージ１６５に応答することができない場合、第１のデバイス１０４は鍵配信メッセージ１８０を送信しない。この例では、第１のデバイス１０４は、第２のページングウィンドウ中に第２のデバイス１０６に第２のページングメッセージを送信し得る。このようにして、第１のデバイス１０４は、第２のデバイス１０６からトリガメッセージ１６７などのトリガメッセージを受信するまで鍵配信メッセージ１８０を送信しないことがある。他の実装形態では、ページングメッセージ、トリガメッセージまたはその両方が使用されないことがある。たとえば、第１のデバイス１０４は、ページングメッセージ１６５を送信することまたはトリガメッセージ１６７を受信することなしに鍵配信メッセージ１８０を生成し得る。特定の実装形態では、第１のデバイス１０４は、告知メッセージ１６０が発見ウィンドウ中に送信された後に鍵配信メッセージ１８０を生成し、送信し得る。別の特定の実装形態では、第１のデバイス１０４は、カウントダウンの完了に応答して鍵配信メッセージ１８０を生成し、送信し得る。カウントダウンは、アクティブグループ鍵の満了に関係し得、アクティブグループ鍵の満了の前に行なわれ得る。

【００５４】

[0066]第２のデバイス１０６は、データリンクグループの他のデバイスに第２のグループ鍵１４２を伝搬するように構成され得る。たとえば、鍵配信メッセージ１８０（または候補鍵セット１４０の少なくとも１つの鍵）を受信したことに応答して、第２のデバイス１０６は、データリンクグループの隣接デバイスにページングメッセージ１９０を送信し得る。例示のために、第２のデバイス１０６が、（実線１８４によって示されるように）第３のデバイス１０８に関連し、第２のデバイス１０６は、第３のデバイス１０８にページングメッセージ１９０を送信し得る。ページングメッセージ１９０は、第２のデバイス１０６が、第３のデバイス１０８に送信するようにスケジュールされた（第２のグループ鍵１４２などの候補鍵セット１４０の少なくとも１つの鍵に対応する）データを有するこ

とを示し得る。第３のデバイス１０８からトリガメッセージ（図示せず）を受信したことに応答して、第２のデバイス１０６は、第３のデバイス１０８に鍵配信メッセージ１８０を転送し得る。このようにして、第２のグループ鍵１４２は、データリンクグループのデバイスに伝搬し得る。

【００５５】

[0067]単一の候補グループ鍵（たとえば、第２のグループ鍵１４２）の生成について説明されるが、いくつかの実装形態では、第２のグループ鍵１４２に関係する告知メッセージが特定の時間までに受信されていない場合、データリンクグループの複数のデバイスは、候補グループ鍵（または候補鍵セット）を生成するように構成され得る。たとえば、デバイス１０４～１１０の各々は、ランダム値からタイマーを開始し、タイマーが特定の値に達すると、新しい候補グループ鍵（または新しい候補鍵セット）を生成するように構成され得る。デバイス１０４～１１０の各々は、（第１のグループ鍵１３２などの）前のグループ鍵が満了したことまたは（第２のグループ鍵１４２などの）候補グループ鍵がアクティブグループ鍵になったことに応答してタイマーを開始するように構成され得る。タイマーが特定の値に達する前に告知メッセージが特定のデバイスによって受信される場合、特定のデバイスのタイマーが停止され得、候補グループ鍵が特定のデバイスによって生成される。タイマーが特定の値に達した場合、特定のデバイスは、候補グループ鍵の生成を開始する。

【００５６】

[0068]複数の告知メッセージまたは複数のグループ鍵（たとえば、複数の候補鍵セット）がデータリンクグループのデバイスによって受信される場合、データリンクグループのデバイスは、鍵インジケータに基づいて次のアクティブグループ鍵（または次のアクティブ鍵セット）として特定の候補グループ鍵（または特定の候補鍵セット）を設定し得る。例示のために、特定の候補グループ鍵は、他の候補グループ鍵に対応する他の鍵インジケータよりも高い優先度を有する特定の候補グループ鍵に対応する鍵インジケータに基づいて次のアクティブグループ鍵として選択され得る。例示的な例として、最古のタイムスタンプを有する候補グループ鍵が次のアクティブグループ鍵として設定され得る。例示のために、第２のデバイス１０６は、第１のタイムスタンプ（たとえば、第１の優先度）と第２のタイムスタンプ（たとえば、第２の優先度）との間の比較を実行し得る。第２のデバイス１０６は、第１のタイムスタンプが第２のタイムスタンプよりも前のものであることに基づいて、第１のタイムスタンプに対応する候補グループ鍵を選択し得る。別の例として、最大の（または最低の）ハッシュ値を有する候補グループ鍵が次のアクティブグループ鍵として設定され得る。別の例として、最も優先度の高いＭＡＣアドレスを有するデバイスによって生成された候補グループ鍵が次のアクティブグループ鍵として設定され得る。

【００５７】

[0069]選択されない候補グループ鍵に対応する告知メッセージは、データリンクグループのデバイスによって転送されない。たとえば、第２のデバイス１０６が、告知メッセージ１６０を受信した後に第２の告知メッセージを受信し、第２の告知メッセージが、別の候補グループ鍵に対応する後のタイムスタンプを含む場合、第２のデバイス１０６は、第２の告知メッセージを転送しない。いくつかの実装形態では、第２のデバイス１０６は、第２の告知メッセージを受信したことに応答して、または第２の告知メッセージに対応するページングメッセージを受信したことに応答して拒絶メッセージを送り得る。

【００５８】

[0070]いくつかの実装形態では、第１のデバイス１０４は、データリンクグループの１つまたは複数のデバイスに鍵配信メッセージ１８０をマルチキャストメッセージとして通信し得る。マルチキャストメッセージは、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含むか、またはそれに対応し得る。鍵配信メッセージ１８０がマルチキャストメッセージとして通信されると、第１のデバイス１０４は、データリンクグループの特定のアクティブ鍵を使用して鍵配信メッセージ１８０を符号化（または暗号

化）し得る。たとえば、アクティブ鍵セット１３０が、データリンクグループのアクティブ配布鍵として設定された第１の配布鍵１３４を含むとき、エンコーダ／デコーダ１１８は、第１の配布鍵１３４を使用して鍵配信メッセージ１８０を符号化（または暗号化）し得る。鍵配信メッセージ１８０を暗号化するために第１の配布鍵１３４を使用することは、鍵配信メッセージ１８０を送信するときに追加のセキュリティを与え得る。例示のために、第１の配布鍵１３４は、鍵配信メッセージ１８０などの鍵配信メッセージを符号化および復号（または暗号化および解読）するためにのみ使用され得、第１のグループ鍵１３２は、他のセキュアなグループ通信のために使用され得る。第１のグループ鍵１３２が第１の配布鍵１３４よりも頻繁に使用されるので、第１のグループ鍵１３２は、より漏洩しやすい（たとえば、データリンクグループの一部でないデバイスによってより識別されやすい）。したがって、データリンクグループのデバイスにマルチキャストメッセージとして第２のグループ鍵１４２、第２の配布鍵１４４、またはその両方を配布するために第１の配布鍵１３４を使用することは、データリンクグループのデバイスに第２のグループ鍵１４２、第２の配布鍵１４４、またはその両方を配布するために第１のグループ鍵１３２を使用することよりもセキュアであり得る。

【００５９】

[0071]第１のデバイス１０４は、第２のグループ鍵１４２を生成することによって、またはデータリンクグループの別のデバイスから第２のグループ鍵１４２を受信することによって、第１のデバイス１０４が第２のグループ鍵１４２を取得したかどうかにかかわらず、マルチキャストメッセージとして鍵配信メッセージ１８０を配布し得る。第１の配布鍵１３４を使用して第２のグループ鍵１４２を符号化（または暗号化）し、符号化された第２のグループ鍵を含むマルチキャストメッセージを送ることによって、符号化された第２のグループ鍵（たとえば、第２のグループ鍵１４２）は、第１のデバイス１０４とデータリンクグループの別のデバイスとの間でセキュリティ関連付け手順、Ｐ２Ｐ通信、またはそれらの組合せを実行することなしにデータリンクグループの１つまたは複数のデバイスに配布され得るたとえば、第１のデバイス１０４は、複数のデバイスが第１のデバイス１０４に関連するか関連しないかにかかわらず、複数のデバイスに符号化（または暗号化）された第２のグループ鍵１４２を同時に配布するためにマルチキャストメッセージを送信し得る。例示のために、第１のデバイス１０４は、第１のデバイス１０４に関連する第２のデバイス１０６に、および第１のデバイス１０４に関連しない第４のデバイス１１０に符号化（または暗号化）された第２のグループ鍵１４２をマルチキャストし得る。したがって、符号化された第２のグループ鍵（第２のグループ鍵１４２）をマルチキャストするために第１の配布鍵１３４を使用することは、ワイヤレスネットワーク１０２内での候補グループ鍵配布に関係する鍵関連のトラフィックとオーバーヘッドとを低減し得る。

【００６０】

[0072]追加または代替として、第１のデバイス１０４は、Ｐ２Ｐ通信として鍵配信メッセージ１８０を通信し得る。例示のために、告知メッセージ１６０の送信の後に、第１のデバイス１０４は、関連するデバイスから第２のグループ鍵１４２についての要求を受信し得る。いくつかの実装形態では、第２のグループ鍵１４２についての要求は、候補鍵セット１４０についての要求を含み得る。第２のデバイス１０６が告知メッセージ１６０を受信すると、第２のデバイス１０６は、第１のデバイス１０４に関連し得、第２のデバイス１０６は、告知メッセージ１６０に応答して第２のグループ鍵１４２についての要求を送り得る。第２のデバイス１０６は、Ｐ２Ｐメッセージとして要求を送り得る。要求に応答して、第１のデバイス１０４は、Ｐ２Ｐメッセージとして第２のデバイス１０６に鍵配信メッセージ１８０を送り得る。いくつかの実装形態では、第１のデバイス１０４は、第１のデバイス１０４に関連する１つまたは複数のデバイスにＰ２Ｐメッセージとして鍵配信メッセージ１８０を自動的に送り得る。たとえば、第１のデバイス１０４は、関連するデバイスから第２のグループ鍵１４２についての要求を受信することなしにＰ２Ｐメッセージとして鍵配信メッセージ１８０を自動的に送り得る。

【００６１】

[0073]いくつかの実装形態では、第１のデバイス１０４に関連しない特定のデバイスに告知メッセージ１６０を送った後に、第１のデバイス１０４は、特定のデバイスに関連付けられるためにセキュリティ関連付け手順を実行し得る。たとえば、第４のデバイス１１０が告知メッセージ１６０を受信するとき、第４のデバイス１１０は、第１のデバイス１０４に関連しないことがある。告知メッセージ１６０を受信した後に、第４のデバイス１１０は、第１のデバイス１０４に関連付けられるために第１のデバイス１０４とのセキュリティ関連付け手順を開始し得る。第４のデバイス１１０が第１のデバイス１０４に関連した後、第１のデバイス１０４は、第４のデバイス１１０に第２のグループ鍵１４２を含むＰ２Ｐ通信を送り得る。たとえば、第１のデバイス１０４は、第４のデバイス１１０に第２のグループ鍵１４２を自動的に送り得、または第１のデバイス１０４は、第２のグループ鍵１４２についての、第４のデバイス１１０から受信された要求に応答して第２のグループ鍵１４２を送り得る。

【００６２】

[0074]特定の実装形態では、第１のデバイス１０４から告知メッセージ１６０を受信する特定のデバイスが、第１のデバイス１０４に関連しないとき、特定のデバイスは、データリンクグループの第１のグループ鍵１３２などのアクティブグループ鍵が満了するように設定される前の所定の時間まで関連するデバイスから別の告知メッセージ（たとえば、告知メッセージ１７０）を受信するのを待ち得る。所定の時間が検出されると、アクティブグループ鍵の満了が間近であると見なされる。特定のデバイスが無関連のデバイスから告知メッセージ１６０を受信するのと所定の時間の検出との間の時間期間は待ち期間と呼ばれることがある。待ち期間中に、特定のデバイスは、特定のデバイスに関連するデバイスから第２の告知メッセージを受信するのを待ち得、したがって、特定のデバイスは、第２のグループ鍵１４２を受信することができる。特定のデバイスが、待ち期間中に第２の告知メッセージを受信しない場合、特定のデバイスは、所定の時間が検出された後に無関連のデバイスとのセキュリティ関連付け手順を開始し得、したがって、特定のデバイスは、第２のグループ鍵１４２を収集することができる。

【００６３】

[0075]例示のために、第４のデバイス１１０が告知メッセージ１６０を受信するとき、第４のデバイス１１０は、第１のデバイス１０４に関連しないことがある。告知メッセージ１６０を受信したことに応答して第１のデバイス１０４に関連するためにセキュリティ関連付けプロセスを開始するのではなく、第４のデバイス１１０は、第４のデバイス１１０が関連するデータリンクグループの別のデバイスから告知メッセージ１７０などの告知メッセージ１６０の転送バージョンを受信するのを待ち得る。例示のために、第４のデバイス１１０は、（実線１８６によって示されるように）第２のデバイス１０６に関連し得、第１のデバイス１０４から告知メッセージ１６０を受信した後に第２のデバイス１０６から告知メッセージ１７０を受信し得る。第２のデバイス１０６から告知メッセージ１７０を受信した後に、第４のデバイス１１０は、Ｐ２Ｐ通信として第２のデバイス１０６から第２のグループ鍵１４２（または候補鍵セット１４０）を受信し得る。たとえば、第２のデバイス１０６は、自動的に、または第２のグループ鍵１４２についての、第４のデバイス１１０から受信された要求に応答して、第４のデバイス１１０に第２のグループ鍵１４２を送り得る。関連するデバイス１０６から別の告知メッセージ１７０を受信するのを待つことによって、第４のデバイス１１０は、第１のデバイス１０４から告知メッセージ１６０を受信したことに応答して第１のデバイス１０４とのセキュリティ関連付けを自動的に開始しない。

【００６４】

[0076]第４のデバイス１１０は、データリンクグループの第１のグループ鍵１３２などのアクティブグループ鍵が満了するように設定される前の所定の時間まで、関連するデバイスから第２の告知メッセージ（たとえば、告知メッセージ１７０）を受信するのを待ち得る。例示のために、所定の時間が検出されると、アクティブグループ鍵の満了が間近であると見なされる。第４のデバイス１１０が、関連するデバイスから第２の告知メッセー

ジを受信しなかった場合、第４のデバイス１１０は、第２のグループ鍵１４２（または候補鍵セット１４０）を受信するために、第１のデバイス１０４などの無関連のデバイスとのセキュリティ関連付け手順を開始し得る。例示のために、第４のデバイス１１０は、第１のデバイス１０４とのセキュリティ関連付け手順を開始し得、セキュリティ関連付け手順の完了の後に、第４のデバイス１１０は、第１のデバイス１０４から第２のグループ鍵１４２（または候補鍵セット１４０）を受信し得る。たとえば、第１のデバイス１０４は、自動的に、または第２のグループ鍵１４２についての、第４のデバイス１１０から受信された要求に応答して、第４のデバイス１１０に第２のグループ鍵１４２を送り得る。

【００６５】

[0077]別の特定の実装形態では、データリンクグループの各デバイスは、アクティブグループ鍵の満了を予想して候補グループ鍵の生成を開始するように構成され得る。例示のために、各デバイスは、図２を参照しながら説明するように、ランダム値を生成し、アクティブグループ鍵の時間期間が満了に近づくと、生成されたランダム値からカウントダウンを開始するように構成され得る。特定のデバイスにおけるカウントダウンが完了すると、特定のデバイスは、候補グループ鍵を生成し、他のデバイスに告知メッセージを送信し得る。たとえば、第１のデバイス１０４は、対応するカウントダウンを完了し、第２のグループ鍵１４２を生成し、告知メッセージ１６０を送信し得る。第２のデバイス１０６および第４のデバイス１１０などの他のデバイスは、告知メッセージ（たとえば、告知メッセージ１６０）を受信したことに応答してそれらのそれぞれのカウントダウンを停止し（、追加の候補グループ鍵を生成するのを控え）得る。告知メッセージ１６０または告知メッセージ１７０を受信すると、特定のデバイスはまた、１つまたは複数の追加の告知メッセージ、候補グループ鍵、またはそれらの組合せの伝搬を（抑制基準に基づいて）条件付きで抑制し得る。たとえば、抑制基準は、例示的な非限定的な例として、より古いタイムスタンプ、またはより高い値のＭＡＣアドレスを有するデバイスによって生成されたタイムスタンプに対応する特定の候補グループ鍵を選択するために適用され得る。告知メッセージ、候補グループ鍵、またはそれらの組合せを抑制することによって、データリンクグループは、複数の（競合する）候補グループ鍵がアクティブグループ鍵として設定されることを回避し得る。

【００６６】

[0078]いくつかの実装形態では、データリンクグループの２つのデバイスは、隣接デバイスであり得、無関連であり得る。たとえば、図１に示したように、第１のデバイス１０４は、第４のデバイス１１０の通信範囲（たとえば、１ホップ範囲）内にあり得、（破線１８２によって示されるように）第４のデバイス１１０に関連しないことがある。第４のデバイス１１０は、（実線１８６によって示されるように）第２のデバイス１０６など、データリンクグループの異なるデバイスに関連し得る。デバイスは関連しないが、マルチキャストメッセージなどのいくつかのメッセージは、デバイス間で共有され得る。たとえば、告知メッセージ１６０がマルチキャストされると、第１のデバイス１０４は、第４のデバイス１１０に告知メッセージ１６０を送信し得る。

【００６７】

[0079]いくつかの実装形態では、データリンクグループのデバイスは、データリンクグループの他のデバイスから候補グループ鍵を受信するために特定の時間まで待つように構成され得る。候補グループ鍵が、現在のグループ鍵の満了より前の特定の量の時間などの特定の時間までに受信されない場合、デバイスは、候補グループ鍵を受信するためにデータリンクグループの別のデバイスに関連するように構成され得る。現在のグループ鍵の満了より前の特定の量の時間は、グループ鍵更新ウィンドウの終了、関連付けウィンドウの開始、またはその両方を示し得るかまたはそれに対応し得る。グループ鍵更新ウィンドウは、鍵更新動作（たとえば、特定の候補グループ鍵を選択し、データリンクグループのデバイスに特定の候補グループ鍵を配布すること）の実行に対応する特定の時間間隔を含み得る。第１のグループ鍵１３２がアクティブグループ鍵として設定されると、データリンクグループのデバイスは、カウントダウンを開始し得る。カウントダウンは、第１のグル

ープ鍵１３２の有効期間よりも短い継続時間を有し得る。カウントダウンの継続時間（または最初のカウントダウン値）は、カウントダウンの満了と第１のグループ鍵１３２の満了との間の時間期間が、デバイスがデータリンクグループの他のデバイスとの１つまたは複数の関連付け動作を実行するのに十分であるように選択され得る。カウントダウンについて説明されるが、カウントダウンに対応する時間期間を追跡するために任意の形態のタイマーまたはタイミング回路が使用され得る。

【００６８】

[0080]図１に示す例では、第１のグループ鍵１３２がアクティブ鍵として設定されると、第４のデバイス１１０は、（第１の継続時間を有する）カウントダウンを開始し得る。他の実装形態では、カウントダウンは、告知メッセージ１６０が第１のデバイス１０４から受信されたときに開始され得、カウントダウンは、第１の継続時間とは異なる継続時間を有し得る。カウントダウンが満了し、第４のデバイス１１０が、たとえば、鍵配信メッセージを受信することによって、第２のグループ鍵１４２を受信しなかった場合、第４のデバイス１１０は、「パニックモード」に入り得、第４のデバイス１１０が告知メッセージを受信したデバイスに関連しようと試み得る。たとえば、第４のデバイス１１０が、第１のデバイス１０４から告知メッセージ１６０を受信したので、第４のデバイス１１０は、第１のデバイス１０４に関連しようと試み得る。

【００６９】

[0081]第１のデバイス１０４に関連するために、第４のデバイス１１０は、第１のデバイス１０４に関連付け要求１７５を送信し得る。関連付け要求１７５は、第４のデバイス１１０を識別し得、第４のデバイス１１０が第１のデバイス１０４との関連付けを実行することを望むことを示し得る。関連付け要求１７５を受信したことに応答して、第１のデバイス１０４は、少なくとも１つの基準に基づいて第４のデバイス１１０に関連すべきかどうかを決定し得る。一例として、基準は、第１のデバイス１０４が現在関連するいくつかの他のデバイスを含み得る。例示のために、第１のデバイス１０４は、データリンクグループのしきい値数以下の他のデバイスに関連するように構成され得る。この例では、第１のデバイス１０４は、第１のデバイス１０４がしきい値数の他のデバイスに現在関連するのかどうかを決定し得る。第１のデバイス１０４が、少なくともしきい値数のデバイスに関連する場合、第１のデバイス１０４は、第４のデバイス１１０に関連しないことを決定し得る。第１のデバイス１０４が、しきい値数未満のデバイスに関連する場合、第１のデバイス１０４は、第４のデバイス１１０に関連することを決定し得る。

【００７０】

[0082]追加または代替として、少なくとも１つの基準は、「必要ベースの」関連付けに関係し得る。たとえば、第１のデバイス１０４は、「必要」に応じて他のデバイスに関連するように構成され得る。一例として、必要ベースの関連付けは、データリンクグループの任意の他のデバイスに現在関連しないデバイスとの関連付けを含み得る。別の例として、必要ベースの関連付けは、アクティブトラフィックセッションに基づいて決定され得る。例示のために、第１のデバイス１０４は、第１のデバイス１０４が次回のページングウィンドウ中に第２のデバイス１０６のためのアクティブトラフィックセッションを有しないと決定したことに応答して、第２のデバイス１０６との関連付けを解除し得る。別の例として、第１のデバイス１０４は、第２のデバイス１０６が第２のグループ鍵１４２をすでに受信したと決定したことに応答して第２のデバイス１０６との関連付けを解除し得る。このようにして、第１のデバイス１０４は、「必要性」がより大きいであろう他のデバイスに関連するためにデータリンクグループのいくつかのデバイスとの関連付けを解除するように構成され得る。

【００７１】

[0083]第１のデバイス１０４が、第４のデバイス１１０に関連することを決定する場合、第１のデバイス１０４は第４のデバイス１１０に関連付け応答１７６を送信し得る。関連付け応答１７６は、第４のデバイス１１０が第１のデバイス１０４に関連することを可能にする情報を含み得る。関連付け応答１７６を受信したことに応答して、第４のデバイ

ス１１０は、第１のデバイス１０４に関連し得る。たとえば、第４のデバイス１１０は、第１のデバイス１０４との１つまたは複数の関連付け動作を実行し得る。特定の実装形態では、１つまたは複数の関連付け動作は、２ウェイハンドシェイク、４ウェイのハンドシェイク、セキュリティ情報の交換、またはそれらの組合せを含み得る。他の実装形態では、他の関連付け動作が実行され得る。関連付け動作の実行中に、第１のデバイス１０４と第４のデバイス１１０との間でペアワイズ鍵が発生され得る。

【００７２】

[0084]第１のデバイス１０４が、第４のデバイス１１０に関連しないことを決定する場合、第１のデバイス１０４は第４のデバイス１１０に関連付け拒絶１７８を送信し得る。関連付け拒絶１７８は、第１のデバイス１０４が、この時点で第４のデバイス１１０との関連付け動作を実行することができないことを示し得る。関連付け拒絶１７８は、第１のデバイスに関連するデバイスのセット（たとえば、第２のグループ鍵１４２を持っているデバイスのセット）を示し得る。たとえば、関連付け拒絶１７８は、第１のデバイス１０４が第２のデバイス１０６に関連することを示し得る。追加または代替として、関連付け拒絶１７８は、第２のグループ鍵１４２をすでに受信しているか、またはそれをすでに持っているデバイスのセットを示し得る。たとえば、関連付け拒絶１７８は、第２のデバイス１０６が第２のグループ鍵１４２をすでに受信しているか、またはそれをすでに持っていることを示し得る。第４のデバイス１１０は、関連付け拒絶１７８中に第２のデバイス１０６が示されたことに応答して第２のデバイス１０６に第２の関連付け要求を送信し得る。関連付け要求１７５と、関連付け応答１７６と、関連付け拒絶１７８とは、第１のワイヤレスチャネルまたは第２のワイヤレスチャネルを介して送信され得る。

【００７３】

[0085]いくつかの実装形態では、第４のデバイス１１０は、関連付けが実行されるまで、または第１のグループ鍵１３２が満了するまで、第１のデバイス１０４に関連しようと試み続けるように構成され得る。たとえば、第４のデバイス１１０が、第２のグループ鍵１４２を受信している別のデバイスに関連しない場合、第４のデバイス１１０は、第１のデバイス１０４に第２の関連付け要求（図示せず）を送信し得る。別の例として、第４のデバイス１１０が第２のデバイス１０６から告知メッセージ１７０を受信する場合、第４のデバイス１１０は、第２のデバイス１０６に関連しようと試み得る。

【００７４】

[0086]いくつかの実装形態では、第４のデバイス１１０は、第１のデバイス１０４に関連しようと試みるより前に、カウントダウンの満了を待たない。代わりに、第４のデバイス１１０は、告知メッセージ１６０を受信したことに応答して第１のデバイス１０４に関連するように構成され得る。たとえば、第４のデバイス１１０は、第１のデバイス１０４から告知メッセージ１６０を受信したことに応答して第１のデバイス１０４に関連付け要求１７５を送信し得る。追加または代替として、第４のデバイス１１０が、第２のデバイス１０６に関連しないとき、第４のデバイス１１０は、第２のデバイス１０６から告知メッセージ１７０を受信したことに応答して第２のデバイス１０６に関連付け要求を送信し得る。第１のデバイス１０４（または第２のデバイス１０６）は、上記で説明されるように、第４のデバイス１１０に関連すべきかどうかを決定し得る。第４のデバイス１１０は、データリンクグループの他のデバイスに関連しようと試みるより前にカウントダウンの満了を待たないので、関連付け試みが失敗した場合、第４のデバイス１１０は、異なるデバイスに関連するためにより多くの時間を有し、それによって、第４のデバイス１１０が、異なるデバイスに関連し、第１のグループ鍵１３２の満了より前に第２のグループ鍵１４２を受信することができる可能性が増加し得る。

【００７５】

[0087]いくつかの実装形態では、データリンクグループのデバイス１０４～１１０は、ユニキャストメッセージとしてデータリンクグループの別のデバイスに鍵配信メッセージと候補グループ鍵（または候補鍵セット）とを通信し得る。特定の実装形態では、ユニキャストメッセージを使用してデータリンクグループの２つの無関連のデバイス間で候補グ

ループ鍵（または候補鍵セット）を交換するために４ウェイハンドシェイクが使用され得る。４ウェイハンドシェイクは、鍵暗号化鍵（ＫＥＫ：key encryption key）を使用して暗号化され、鍵確認鍵（ＫＣＫ：key confirmation key）を使用して完全性を保護されるローカルエリアネットワークを介した拡張認証プロトコル（ＥＡＰＯＬ：extension authentication protocol over local area network）鍵フレームを含み得る。ＫＥＫとＫＣＫとは、ペアワイズ鍵中に含まれ得る。ＥＡＰＯＬ鍵フレームは、第２のグループ鍵１４２などの候補グループ鍵を含み得る。いくつかの実装形態では、ＥＡＰＯＬ鍵フレームは、候補鍵セット１４０を含み得る。ＥＡＰＯＬ鍵フレームは、２つの無関連のデバイス間の第３のメッセージ（または通信）に対応するか、またはそれの中に含まれ得る。

【００７６】

[0088]４ウェイハンドシェイクを実行することの例示的な例として、第１のデバイス１０４と第４のデバイス１１０とは無関連であり得、第１のデバイス１０４は、第４のデバイス１１０に第１のメッセージを送信し得る。第１のメッセージにより、第４のデバイス１１０は、ペアワイズ鍵を生成することが可能になり得る。第１のデバイス１０４は、第４のデバイス１１０から第２のメッセージを受信し、第２のメッセージに基づいてペアワイズ鍵を生成し得る。第１のデバイス１０４は、第４のデバイス１１０にＥＡＰＯＬ鍵フレームを含む第３のメッセージを送信し、ＥＡＰＯＬ鍵フレームは、第２のグループ鍵１４２を含み得る。ＥＡＰＯＬ鍵フレームは、ＫＥＫに基づいて暗号化され、ＫＣＫに基づいて完全性を保護され得る。第１のデバイス１０４は、第４のデバイス１１０から第４のメッセージを受信し得る。第４のメッセージは、第４のデバイス１１０が第２のグループ鍵１４２を受信したことと、第４のデバイス１１０が第１のデバイス１０４に現在関連することとを示す肯定応答メッセージを含み得る。

【００７７】

[0089]別の特定の実装形態では、ユニキャストメッセージを使用してデータリンクグループの２つの関連するデバイス間で候補グループ鍵を交換するためにグループ鍵ハンドシェイク（たとえば、２ウェイハンドシェイク）が使用され得る。グループ鍵ハンドシェイクは、暗号化され、完全性を保護され得るＥＡＰＯＬ鍵フレームを含み得る。ＥＡＰＯＬ鍵フレームは、２つの関連するデバイス間で第１のメッセージ（または通信）として送信され得る。グループ鍵ハンドシェイクを実行することの例示的な例として、第１のデバイス１０４と第２のデバイス１０６とは、関連し得、第１のデバイス１０４と第２のデバイス１０６とは、ペアワイズ鍵１４６をすでに所有していることがある。たとえば、ペアワイズ鍵１４６は、グループハンドシェイクより前に行なわれた関連付け動作中に生成されていることがある。ペアワイズ鍵１４６は、ＫＥＫとＫＣＫとを含み得る。第１のデバイス１０４は、第２のデバイス１０６に、第２のグループ鍵１４２を有するＥＡＰＯＬ鍵フレームを含む第１のメッセージを送信し得る。（または候補鍵セット１４０）ＥＡＰＯＬ鍵フレームは、ペアワイズ鍵１４６のＫＥＫに基づいて暗号化され、ペアワイズ鍵１４６のＫＣＫに基づいて完全性を保護され得る。第１のデバイス１０４は、第２のデバイス１０６から第２のメッセージを受信し得る。第２のメッセージは、肯定応答メッセージを含み得、第２のデバイス１０６が第２のグループ鍵１４２を受信していることを示し得る。

【００７８】

[0090]別の特定の実装形態では、鍵配信メッセージ１８０は、ＮＡＮ管理フレームを含むか、またはそれに対応し得、これは、ユニキャストメッセージを使用してデータリンクグループの２つのデバイス間で候補グループ鍵を交換するために使用され得る。ＮＡＮ管理フレームは、ＥＡＰＯＬ鍵フレームをカプセル化し得る（または含み得る）。ＮＡＮ管理フレーム、ＥＡＰＯＬ鍵フレーム、またはその両方は、ＫＥＫに基づいて暗号化され、ＫＣＫに基づいて完全性を保護され得る。たとえば、第１のデバイス１０４は、第２のグループ鍵１４２など、候補鍵セット１４０の少なくとも１つの鍵を有するＥＡＰＯＬ鍵フレームを含むＮＡＮ管理フレームとして鍵配信メッセージ１８０を送信し得る。第１のデバイス１０４は、第２のデバイス１０６など、第１のデバイス１０４に関連する別のデバイスにＮＡＮ管理フレームを送信し得る。

【００７９】
[0091]別の特定の実装形態では、鍵配信メッセージ１８０は、パブリックアクションフレームを含むか、またはそれに対応し得、これは、ユニキャストメッセージを使用してデータリンクグループの２つのデバイス間で候補グループ鍵を交換するために使用され得る。パブリックアクションフレームは、時間鍵（ＴＫ）を使用して保護され得る。ＴＫは、ペアワイズ鍵中に含まれ得る。グループ鍵を搬送するために、パブリックアクションフレームの特定の属性（たとえば、特定のフィールド）が規定され得る。たとえば、１つまたは複数のワイヤレス通信規格においてなど、グループ鍵を搬送するために、パブリックアクションフレームの第１の属性が規定され得る。第１のデバイス１０４は、パブリックアクションフレームの第１の属性中に、第２のグループ鍵１４２など、候補鍵セット１４０の少なくとも１つの鍵を含むパブリックアクションフレームとして鍵配信メッセージ１８０を送信し得る。鍵配信メッセージ１８０は、第２のデバイス１０６など、第１のデバイス１０４に関連する別のデバイスに送信され得る。

【００８０】
[0092]いくつかの実装形態では、第１のデバイス１０４は、告知メッセージ１６０などの告知メッセージを送信しない。これらの実装形態では、第２のグループ鍵１４２を生成したことに応答して、第１のデバイス１０４は、データリンクグループの隣接デバイスにページングメッセージ１６５を送信し得る。上記で説明されるように、ページングメッセージ１６５は、第１のワイヤレスチャネル（ＮＡＮ通信チャネル）または第２のワイヤレスチャネル（データリンクグループチャネル）のページングウィンドウ中に送信され得る。これらの実装形態では、ページングメッセージ１６５は、第２のグループ鍵１４２の生成を示すページ属性１６９を含む。ページ属性１６９の詳細について、図６を参照しながら本明細書でさらに説明する。いくつかの実装形態ではまた、ページングメッセージ１６５は、グループＩＤ１６４、デバイスＩＤ１６６、鍵インジケータ１６８、またはそれらの組合せを含み得る。告知メッセージ１６０などの告知メッセージを使用する代わりにページングメッセージを使用してグループ鍵を告知することは、第１のワイヤレスチャネル、第２のワイヤレスチャネル、またはその両方上でトラフィックを低減し得る。

【００８１】
[0093]ページングメッセージ１６５を受信したことに応答して、第２のデバイス１０６は、上記で説明されるように、第１のデバイス１０４にトリガメッセージ１６７を送信し得る。第１のデバイス１０４は、トリガメッセージ１６７を受信したことに応答して第２のデバイス１０６に第２のグループ鍵１４２を含む鍵配信メッセージ１８０を送信し得る。第２のグループ鍵１４２を受信した後に、第２のデバイス１０６は、第３のデバイス１０８にページングメッセージを送信し得、第２のデバイス１０６と第３のデバイス１０８とは、第１のデバイス１０４と第２のデバイス１０６とに関して説明されるように、トリガメッセージと鍵配信メッセージとを交換し得る。さらに、第２のデバイス１０６は、（第２のグループ鍵１４２を含む）鍵配信メッセージ１８０を受信したことに応答して第１のデバイス１０４にＭＡＣ　ＡＣＫなどの肯定応答（ＡＣＫ）を送り得る。さらに、ページングメッセージは、マルチキャストであり得、暗号化されていないことがあるので、第４のデバイス１１０などの第１のデバイス１０４に関連しない隣接デバイスは、ページングメッセージ１６５を受信し得、候補鍵セット１４０の少なくとも１つの鍵（たとえば、第２のグループ鍵１４２）など、ページングメッセージ１６５に関連するデータを受信するために第１のデバイス１０４に関連しようと試み得る。

【００８２】
[0094]ページングメッセージ１６５は、複数のページングウィンドウ中に再送信されるか、または繰り返され得る。たとえば、第１のデバイス１０４は、第１のグループ鍵１３２が満了するまで、複数のページングウィンドウ中にページングメッセージ１６５を送信し得る。いくつかの実装形態では、第１のデバイス１０４と関連する状態にある各隣接デバイスが第２のグループ鍵１４２を受信した場合、第１のデバイス１０４は、第１のグループ鍵１３２の満了より前にページングメッセージ１６５を送信することを停止し得る。

例示のために、第１のデバイス１０４は、第２のデバイス１０６が第２のグループ鍵１４２を受信するまで、複数のページングウィンドウ中にページングメッセージ１６５を送信し得る。第１のデバイス１０４は、鍵配信メッセージ１８０を送信したことに応答して第２のデバイス１０６からＡＣＫを受信することに基づいて第２のデバイス１０６が第２のグループ鍵１４２を受信したと決定し得る。したがって、第１のデバイス１０４が、データリンクグループの各隣接デバイスからＡＣＫを受信する場合、第１のデバイス１０４は、ページングメッセージ１６５を送信することを停止し得る。

【００８３】

[0095]追加または代替として、グループ鍵（アクティブ鍵セット１３０および候補鍵セット１４０）は、鍵インデックス、鍵識別番号、またはその両方に関連し得る。鍵インデックス、鍵識別番号、またはその両方は、サービス情報フィールド、鍵配信メッセージ１８０、またはその両方の中などのＮＡＮサービス発見フレーム中に含まれ得る。鍵インデックス、鍵識別番号、またはその両方は、アクティブグループ鍵がデータリンクグループのためのトラフィックを暗号化するために使用されることを示し得る。鍵識別番号は、グループ鍵を識別するために使用され得る数値または英数字文字列を含み得る。鍵インデックスは、非アクティブグループ鍵とアクティブグループ鍵との表を含み得る。いくつかの実装形態では、鍵インデックスの表は、各非アクティブグループ鍵とアクティブグループ鍵とのための鍵識別番号を含み得る。

【００８４】

[0096]鍵インデックス、鍵識別番号、またはそれらの組合せにより、データリンクグループのデバイスは、アクティブグループ鍵を決定することが可能になり得る。たとえば、特定のデータリンクグループを離れ、後で、特定のデータリンクグループに再加入するデバイスは、前のアクティブグループ鍵が、鍵インデックス、鍵識別番号、またはそれらの組合せに基づいて依然として有効であるのかどうかを決定し得る。前のアクティブグループ鍵が依然として有効である場合、デバイスは、データリンクグループのアクティブグループ鍵を受信するためにデータリンクグループの別のデバイスと認証する必要がない。別の例として、アクティブグループ鍵としての第１のグループ鍵１３２からの第２のグループ鍵１４２への遷移中に、デバイスは、データを暗号化するためにデバイスがどのグループ鍵（たとえば、第１のグループ鍵１３２または第２のグループ鍵１４２）を使用しているのかを示し得る。たとえば、第１のデバイス１０４は、メッセージ中に、データを暗号化するために第１のデバイス１０４が使用している第１のグループ鍵１３２に関連する鍵識別番号を含み得る。

【００８５】

[0097]システム１００のいくつかの動作および機能について、対応するデバイスに関して説明されたが、デバイス１０４～１１０の各々は、デバイス１０４～１１０の別のものを参照しながら説明される１つまたは複数の動作、機能、またはそれらの組合せを実行するように構成され得る。たとえば、デバイス１０４～１１０の各々は、第１のデバイス１０４の、それぞれ、鍵論理１１２およびメッセージ論理１１４を参照しながら説明されるように対応する鍵論理と対応するメッセージ論理とを含み得る。追加または代替として、１つまたは複数の例について第２のグループ鍵１４２の配布に関して説明されたが、そのような例は、候補鍵セット１４０の１つまたは複数の鍵の配布に適用され得る。

【００８６】

[0098]開示する態様のうちの少なくとも１つによって与えられる１つの利点は、ワイヤレスネットワーク内の鍵関係のトラフィックおよびオーバーヘッドの低減である。たとえば、ＮＡＮのデバイスがアクティブ動作モードにある（たとえば、起動している）とき、鍵関連のトラフィックは、ページングウィンドウまたは発見ウィンドウ中に告知メッセージ１６０を送ることによって低減され得る。ページングウィンドウまたは発見ウィンドウ中に告知メッセージ１６０を送ることは、第１のデバイス１０４の隣接デバイスが告知メッセージ１６０を受信する可能性を増加させ得、これは、再送信を低減し得る。別の例として、データリンクグループ中のデバイスがアクティブ動作モードにあるとき、鍵関連の

トラフィックは、ページングウィンドウ中にページ属性１６９を有するページングメッセージ１６５を送ることによって低減され得る。ページ属性１６９は、次回のデータウィンドウ中に特定のデバイスからトラフィックを受信するようにスケジュールされた複数のデバイスを示し得、グループ鍵伝搬のために必要とされるページングメッセージの数を低減し得る。

【００８７】

[0099]別の例示的な利点は、告知メッセージ１６０（またはそれの転送バージョン）を受信するデバイスが、アクティブグループ鍵の満了より前の所定の時間までの待ち期間を実装し得ることである。待ち期間中に、告知メッセージ１６０（またはそれの転送バージョン）を受信した特定のデバイスは、告知メッセージ１６０（またはそれの転送バージョン）に対応する第２のグループ鍵１４２を取得するためにセキュリティ関連付け手順を開始するのを控え得る（自制し得る）。第２のグループ鍵１４２を収集するために別のデバイスに関連するのを控えることによって、第２のグループ鍵１４２を取得するためにセキュリティ関連付け手順を実行する１つまたは複数のデバイスに対応するトラフィックの量が低減され得る。別の例として、第２のグループ鍵１４２を符号化（または暗号化）するために第１の配布鍵１３４などのアクティブ配布鍵が使用され得、符号化された第２のグループ鍵が、データリンクグループの１つまたは複数のデバイスに送られ得る（たとえば、マルチキャストされ得る）。符号化された第２のグループ鍵を送ることによって、第２のグループ鍵１４２は、第２のグループ鍵１４２を有する別のデバイスと第２のグループ鍵１４２を有しないデータリンクグループのデバイスとの間でセキュリティ関連付け手順、Ｐ２Ｐ通信、またはそれらの組合せを実行することなしにデータリンクグループの１つまたは複数のデバイスに配布され得る。

【００８８】

[0100]図２は、候補グループ鍵を生成するシステム２００の特定の例示的な実装形態である。システム２００は、ワイヤレスネットワーク中に含まれるデバイスなどのデバイス２０２を含む。デバイス２０２は、図１のワイヤレスネットワーク１０２のデバイス１０４～１１０のうちの１つを含むか、またはそれに対応し得る。

【００８９】

[0101]デバイス２０２は、カウンタ２０４と、鍵生成器２０６と、鍵記憶装置２０８と、受信機２１０と、送信機２１２とを含み得る。受信機２１０と送信機２１２とは、それぞれ、ワイヤレスネットワークの他のデバイスから１つまたは複数の信号を受信し、それに１つまたは複数の信号を送信するように構成され得る。いくつかの実装形態では、受信機２１０と送信機２１２とは、トランシーバなどの単一の構成要素を含み得る。鍵記憶装置２０８は、メモリなどのストレージデバイスを含むか、またはそれに対応し得る。カウンタ２０４は、鍵生成器２０６と受信機２１０とに結合され得、鍵生成器２０６は、鍵記憶装置２０８と送信機２１２とに結合され得、鍵記憶装置２０８は、受信機２１０と送信機２１２とに結合され得る。いくつかの実装形態では、カウンタ２０４は、タイマーを含むか、またはそれに対応し得る。

【００９０】

[0102]カウンタ２０４は、本明細書でさらに説明するように、グループ鍵２１４の生成より前にランダム値２２０からカウントダウンを実行するように構成され得る。鍵生成器２０６は、グループ鍵２１４、配布鍵（図示せず）、グループ完全性鍵、またはそれらの組合せなどの１つまたは複数の鍵を生成することと、鍵記憶装置２０８と送信機２１２とに１つまたは複数の鍵を与えることとを行うように構成され得る。たとえば、鍵生成器は、グループ鍵２１４を生成し、鍵記憶装置２０８と送信機２１２とにグループ鍵２１４を与え得る。グループ鍵２１４は、図１の第１のグループ鍵１３２または第２のグループ鍵１４２を含むか、またはそれに対応し得る。配布鍵は、図１の第１の配布鍵１３４または第２の配布鍵１４４を含むか、またはそれに対応し得る。鍵生成器２０６は、ハードウェア、ソフトウェア、またはそれらの組合せを含み得る。いくつかの実装形態では、鍵生成器２０６は、グループ鍵２１４を生成するためにメモリ中に含まれる１つまたは複数の命

令を実行するように構成されたプロセッサを含むか、またはそれに対応し得る。
【００９１】
[0103]鍵記憶装置２０８は、グループ鍵２１４、配布鍵、ペアワイズ鍵、グループ完全性鍵、またはそれらの組合せなどの１つまたは複数の鍵を記憶するように構成され得る。別の例として、鍵記憶装置２０８は、データリンクグループの１つまたは複数の満了したグループ鍵などの１つまたは複数の前のグループ鍵、あるいは別のデバイスによって生成され、受信機２１０を介してデバイス２０２において受信された１つまたは複数の候補グループ鍵を記憶し得る。
【００９２】
[0104]動作中、鍵生成器２０６は、グループ鍵２１４の形成を開始し得る。特定の実装形態では、アクティブグループ鍵の満了の前の特定の所定の量の時間（たとえば、アクティブグループ鍵として設定された前のグループ鍵が満了に近づいていること）を検出することに基づいて、鍵記憶装置２０８は、前のグループ鍵（たとえば、アクティブグループ鍵）を記憶し得、鍵生成器４０６は、グループ鍵２１４の形成を開始し得る。たとえば、特定の所定の量の時間は、アクティブグループ鍵に関連するタイミング情報に基づいて、カウンタ２０４、鍵生成器２０６、またはそれらの組合せによって検出され得る。特定の所定の量の時間は、アクティブグループ鍵の満了の前に残された時間量が、アクティブグループ鍵の満了より前に候補グループ鍵が生成され、データリンクグループの各デバイスに伝搬されるのに十分であるように選択され得る。
【００９３】
[0105]図２に、タイミング図２３０中のデータリンクグループのグループ鍵（たとえば、アクティブグループ鍵）の満了に対応するタイミングをも示す。図示のように、時間ｔ１に第１のグループ鍵（鍵１）が生成され得る（または、生成が開始され得る）。第１のグループ鍵（鍵１）は、時間ｔ１に、または時間ｔ１のすぐ後にアクティブグループ鍵として設定され得る。第１のグループ鍵（鍵１）がデータリンクグループのデバイスの間で送信されるとき、第１のグループ鍵（鍵１）に対応するタイムスタンプが、生成され、第１のグループ鍵（鍵１）とともに、図１の鍵配信メッセージ１８０などのメッセージ中に含まれ得る。
【００９４】
[0106]時間ｔ２に、第２のグループ鍵（鍵２）の生成が開始される。いくつかの実装形態では、時間ｔ２は、第１のグループ鍵（鍵１）の満了の前の特定の所定の量の時間（または第１のグループ鍵（鍵１）の生成の後のある量の時間）に関連し得る。時間ｔ３に、第１のグループ鍵（鍵１）が満了する。時間ｔ２に生成されるものとして示されているが、他の例では、第２のグループ鍵（鍵２）の生成は、時間ｔ２に開始され得、第２のグループ鍵（鍵２）の生成は、時間ｔ２と時間ｔ３との間にある時間に行なわれ得る。第２のグループ鍵（鍵２）の生成の後に、第２のグループ鍵（鍵２）は、第１のグループ鍵（鍵１）の満了より前にデータリンクグループの１つまたは複数のデバイスに与えられ得る。第２のグループ鍵（鍵２）は、第１の候補グループ鍵であり得、図１の候補鍵セット１４０に対応し得る。第２のグループ鍵（鍵２）は、時間ｔ２と時間ｔ３との間の時間期間中にアクティブグループ鍵になり得る。特定の実装形態では、第２のグループ鍵（鍵２）は、時間ｔ３にアクティブグループ鍵として設定される。
【００９５】
[0107]第３のグループ鍵（鍵３）の生成は、時間ｔ４に開始され得、これは、第２のグループ鍵（鍵２）の満了の前の特定の所定の量の時間に対応する。第２のグループ鍵（鍵２）は、時間ｔ５に満了し得、第３のグループ鍵（鍵３）は、アクティブグループ鍵として設定され得る。図示されていないが、第４のグループ鍵は、時間ｔ６に第３のグループ鍵（鍵３）の満了より前に生成され得る。さらに、特定の所定の量の時間が、アクティブグループ鍵の各々の満了の前の同じ時間量であるものとして説明されたが、他の実装形態では、特定の所定の量の時間は、アクティブグループ鍵の各々ごとに異なる量の、満了の前の時間であり得る。第３のグループ鍵（鍵３）は、第２の候補グループ鍵であり得、図

１の候補鍵セット１４０に対応し得る。

【００９６】

[0108]デバイス２０２を参照すると、アクティブグループ鍵の満了より前に特定の所定の量の時間を検出したことに応答して、鍵生成器２０６は、グループ鍵２１４の生成を開始することを決定し得る。鍵生成器２０６は、カウンタ２０４に、ランダム値２２０からカウントダウンを開始すること（またはランダム値２２０までカウントアップするカウンタを開始すること）を行わせることによってグループ鍵２１４の生成を開始し得る。ランダム値２２０は、デバイス２０２に記憶された特定の範囲の値内から生成（または選択）され得る。たとえば、製造中に、デバイス２０２は、１つまたは複数の規格に対応する範囲の値などの特定の範囲の値を示すデータを用いてプログラムされ得る。別の例として、デバイス２０２は、デバイス２０２がデータリンクグループに加わるときに実行されるセキュリティ関連付け手順（たとえば、関連付け手順）中にデータリンクグループの別のデバイスから特定の範囲の値を示すデータを受信し得る。

【００９７】

[0109]カウントダウンが０に達すると（またはカウントアップがランダム値２２０に達すると）、鍵生成器２０６は、グループ鍵２１４を生成し、鍵記憶装置２０８、送信機２１２、またはそれらの組合せにグループ鍵２１４を与え得る。さらに、鍵生成器２０６は、図１の告知メッセージ１６０などの告知メッセージを生成するか、またはそれの生成を開始し得、鍵生成器２０６は、グループ鍵２１４の送信より前に告知メッセージを送信機２１２によって送信することを行わせ得る。グループ鍵２１４は、データリンクグループのデバイス２０２から他のデバイスに送られるグループメッセージを暗号化すること、データリンクグループの他のデバイスからデバイス２０２において受信されたグループメッセージを解読すること、またはそれらの組合せを行う際に使用するアクティブグループ鍵として鍵記憶装置２０８中に記憶され得る。追加または代替として、グループ鍵２１４は、候補グループ鍵として鍵記憶装置２０８中に記憶され得、アクティブグループ鍵として後で設定され得る。グループ鍵２１４（および告知メッセージ）は、（たとえば、シングルホップまたはマルチホップルートを介して）グループ中の１つまたは複数の他のデバイスに送信機２１２によって送信され得る。いくつかの実装形態では、告知メッセージは、カウントダウンが０に達した（またはカウントアップがランダム値２２０に達した）後に、グループ鍵２１４の生成より前に送られ得る。

【００９８】

[0110]鍵生成器２０６は、グループ鍵２１４の生成より前に別の告知メッセージまたは別のグループ鍵が受信されるときにグループ鍵４１４の生成を防げる（たとえば、禁止する）ように構成され得る。たとえば、カウンタ２０４は、別の告知メッセージまたは別の候補グループ鍵（たとえば、異なるデバイスによって生成された告知メッセージ、異なるデバイスによって生成された候補グループ鍵、またはそれらの組合せ）が受信機２１０によって受信される場合にカウントダウンを停止し得る。さらに、グループ鍵２１４が生成され、デバイス２０２が、別のデバイスから別のグループ鍵が生成されたことを示す特定の告知メッセージを受信する場合、デバイス２０２は、グループ鍵２１４または他のグループ鍵を既存のアクティブグループ鍵の満了の後に潜在的な「次の」アクティブグループ鍵として使用すべきであるのかどうかを決定するために抑制基準を適用し得る。たとえば、抑制基準は、例示的な非限定的な例として、より古いタイムスタンプに対応する特定の候補グループ鍵、またはより高い値のＭＡＣアドレスを有するデバイスによって生成された候補グループ鍵を選択するために適用され得る。

【００９９】

[0111]図２に、単一のデバイス２０２を示すが、データリンクグループ中の各デバイスがデバイス２０２として同様に構成され得る。したがって、データリンクグループ中の任意のデバイスは、データリンクグループの他のデバイスによって使用されるべき対応する候補グループ鍵を生成し得る。データリンクグループの各デバイスが対応する候補グループ鍵を生成することを可能にすることによって、データリンクグループは、データリンク

グループのデバイスによって使用されるべき候補グループ鍵を生成するように単一の中央デバイスを構成することなしにデータを交換することを可能にし得る。（中央デバイスを含む）各デバイスが任意の時間にワイヤレスネットワークを離れ得るので、単一の中央デバイスの使用はワイヤレスネットワークにおいて望ましくないことがある。

【０１００】

[0112]図３は、データリンクグループ中で通信されるメッセージのタイミング図３００の特定の例示的な実装形態である。データリンクグループは、デバイス１０４～１１０を含む図１のデータリンクグループを含むか、またはそれに対応し得る。データリンクグループは、第１のデバイス（ＳＴＡ１）、第２のデバイス（ＳＴＡ２）、および第３のデバイス（ＳＴＡ３）などの複数のデバイスを含み得る。たとえば、第１のデバイスと、第２のデバイスと、第３のデバイスとは、図１のデバイス１０４～１１０または図２のデバイス２０２を含むか、またはそれに対応し得る。

【０１０１】

[0113]タイミング図３００に、ＮＡＮ通信チャネル３０２とデータリンクグループチャネル３０４とを示す。ＮＡＮ通信チャネル３０２は、第１の発見ウィンドウ３１０と第２の発見ウィンドウ３１２などの複数の発見ウィンドウを含む。データリンクグループチャネル３０４は、複数のグループ送信ウィンドウ３２０～３２６を含む。いくつかの実装形態では、グループ送信ウィンドウ３２０～３２６は、ＮＡＮ通信チャネル３０２に関して発生する。たとえば、データリンクグループチャネル３０４がないとき、グループ送信ウィンドウ３２０～３２６は、ＮＡＮ通信チャネル３０２に関して発生し、第１の発見ウィンドウ３１０と第２の発見ウィンドウ３１２との間にあり得る。

【０１０２】

[0114]他の実装形態では、データリンクグループチャネル３０４は、（発見ウィンドウ３１０、３１２と同様の）発見ウィンドウを含み得、グループ送信ウィンドウ３２０～３２６は、データリンクグループチャネル３０４の２つの発見ウィンドウ間に発生する。いくつかの実装形態では、データリンクグループチャネル３０４の発見ウィンドウは、ＮＡＮ通信チャネル３０２の第１の発見ウィンドウ３１０と第２の発見ウィンドウ３１２とに加えたものであり得る。他の実装形態では、ＮＡＮ通信チャネル３０２がないことがある。これらの実装形態では、データリンクグループチャネル３０４は、対応する発見ウィンドウを有し得るか、または有し得る。

【０１０３】

[0115]いくつかの実装形態では、データリンクグループは、ＮＡＮ中に含まれ得、データリンクグループのデバイスは、ＮＡＮ通信チャネル３０２を介して通信し得る。ＮＡＮのデバイスは、ＮＡＮのマスタデバイスによって、またはＮＡＮの特定のグループのマスタデバイスによって通信される１つまたは複数の同期ビーコンを介して同期され得る。たとえば、データリンクグループのデバイスのうちの１つは、マスタデバイスとして動作し得、ＮＡＮ通信チャネル３０２を介してＮＡＮ中に含まれる他のデバイスに１つまたは複数の同期ビーコンをブロードキャストし得る。

【０１０４】

[0116]追加または代替として、データリンクグループ中に含まれるデバイスは、データリンクグループチャネル３０４を介して通信し得る。データリンクグループのデバイスは、データリンクグループのマスタデバイスまたはデータリンクグループを含むＮＡＮのマスタデバイスによって通信される１つまたは複数の同期ビーコンを介して同期され得る。たとえば、データリンクグループのデバイスのうちの１つは、マスタデバイスとして動作し得、ＮＡＮ通信チャネル３０２、データリンクグループチャネル３０４、またはその両方を介してデータリンクグループの他のデバイス、ＮＡＮの他のデバイス、またはそれらの組合せに１つまたは複数の同期ビーコンをブロードキャストし得る。

【０１０５】

[0117]デバイスは、データリンクグループチャネル３０４に対応するグループ送信ウィンドウを検出するために同期され得る。たとえば、データリンクグループのデバイスの各

々は、本明細書でさらに説明するように、グループ送信ウィンドウ、ページングウィンドウ、データパスウィンドウ、またはそれらの組合せの開始と終了との正しい決定を可能にするために、ＩＥＥＥ８０２．１１ｓ規格、Ｗｉ－Ｆｉ　Ａｌｌｉａｎｃｅ規格、またはそれらの組合せによって記述されているように同期クロックを有し得る。グループ送信ウィンドウは、第１のグループ送信ウィンドウ３２０と、第２のグループ送信ウィンドウ３２２と、第３のグループ送信ウィンドウ３２４と、第４のグループ送信ウィンドウ３２６とを含み得る。データパス送信ウィンドウの各々は、対応するページングウィンドウと対応するデータウィンドウとを含み得る。例示のために、第１のグループ送信ウィンドウ３２０は、第１のページングウィンドウ３３２と第１のデータウィンドウ３３４とを含み得、第２のグループ送信ウィンドウ３２２は、第２のページングウィンドウ３４２と第２のデータウィンドウ３４４とを含み得、第３のグループ送信ウィンドウ３２４は、第３のページングウィンドウ３５２と第３のデータウィンドウ３５４とを含み得、第４のグループ送信ウィンドウ３２６は、第４のページングウィンドウ３６２と第４のデータウィンドウ３６４とを含み得る。

【０１０６】

[0118]いくつかの実装形態では、各グループ送信ウィンドウは、第１の発見ウィンドウ３１０など、ＮＡＮ通信チャネルの発見ウィンドウからのオフセットを含む。デバイスは、第１の発見ウィンドウ３１０からのオフセットに基づいてグループ送信ウィンドウ、ページングウィンドウ、またはデータパスウィンドウの開始または終了を決定し得る。第１の発見ウィンドウ３１０と第２の発見ウィンドウ３１２との間の継続時間は、グループ鍵更新ウィンドウを含むか、またはそれに対応し得る。

【０１０７】

[0119]発見ウィンドウ中に、データリンクグループのデバイスの各々は、起動している（たとえば、省電力モード、低電力モード、またはスリープモードにない）ことがあり、ビーコン、メッセージ、またはその両方を監視し得る。いくつかの実装形態では、ビーコン、メッセージ、またはその両方は、後続のデータウィンドウ中に送られるべきトラフィックを示し得る。発見ウィンドウ中に送られるビーコン、メッセージ、またはそれらの組合せは、セキュアである（たとえば、符号化または暗号化されている）ことも、セキュアでない（たとえば、符号化または暗号化されていない）こともある。セキュアなビーコン、セキュアなメッセージ、またはその両方が発見ウィンドウ中に送信されるとき、セキュアなビーコン、セキュアなメッセージ、またはその両方は、アクティブグループ鍵、アクティブ配布鍵、または完全性グループ鍵などの鍵を使用して符号化され得る。たとえば、アクティブグループ鍵およびアクティブ配布鍵は、それぞれ、図１の第１のグループ鍵１３２と図１の第１の配布鍵１３４とを含むか、またはそれに対応し得る。完全性グループ鍵は、図１の完全性グループ鍵を含むか、またはそれに対応し得る。特定のデバイスが、発見ウィンドウ中に受信されたビーコン、メッセージ、またはその両方に基づいて特定のデバイスがデータを受信し得ると決定する場合、特定のデバイスは、後続のデータウィンドウ中に起動したままでいることがある。特定のデバイスが、発見ウィンドウ中にビーコン、メッセージ、またはその両方を受信しない場合、特定のデバイスは、後続のデータウィンドウ中に「スリープに移行する」（たとえば、スリープモードまたは省電力モードに入る）。

【０１０８】

[0120]ページングウィンドウ中に、データリンクグループのデバイスの各々は、起動している（たとえば、省電力モード、低電力モード、またはスリープモードにない）ことがあり、ビーコン、メッセージ、またはその両方を監視し得る。いくつかの実装形態では、ビーコン、メッセージ、またはその両方は、後続のデータウィンドウ中に送られるべきトラフィックを示し得る。ページングウィンドウ中に送られるビーコン、メッセージ、またはその両方は、セキュアである（たとえば、符号化または暗号化されている）ことも、セキュアでない（たとえば、符号化または暗号化されていない）こともある。セキュアなビーコン、セキュアなメッセージ、またはその両方がページングウィンドウ中に送信される

とき、セキュアなビーコン、セキュアなメッセージ、またはその両方は、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などの鍵を使用して符号化され得る。たとえば、アクティブグループ鍵およびアクティブ配布鍵は、それぞれ、図１の第１のグループ鍵１３２と図１の第１の配布鍵１３４とを含むか、またはそれに対応し得る。ペアワイズ鍵は、図１のペアワイズ鍵１４６を含むか、またはそれに対応し得る。特定のデバイスが、ページングウィンドウ中に受信されたビーコン、メッセージ、またはそれらの組合せに基づいてそれがデータを受信し得ると決定する場合、特定のデバイスは、後続のデータウィンドウ中に起動したままでいることがある。特定のデバイスが、ページングウィンドウ中にビーコン、メッセージ、またはその両方を受信しない場合、特定のデバイスは、後続のデータウィンドウ中に「スリープに移行する」（たとえば、スリープモードまたは省電力モードに入る）。

【０１０９】

[0121]第１のグループ送信ウィンドウ３２０の第１のページングウィンドウ３３２を参照すると、第１のデバイスは、データリンクグループの１つまたは複数のデバイスにデータリンクグループチャネル３０４を介して告知メッセージ３３６を送信し得る。告知メッセージ３３６は、第１のデバイスが、データリンクグループのデバイスに配布されるべき図１の第２のグループ鍵１４２または図２のグループ鍵２１４などの候補グループ鍵を有することを示し得る。たとえば、告知メッセージ３３６は、図１の告知メッセージ１６０または告知メッセージ１７０を含むか、またはそれに対応し得る。告知メッセージ３３６に応答して、第２のデバイスは、候補グループ鍵を要求するために第１のデバイスに要求３３８を送り得る。要求３３８は、告知メッセージ３３６と同じページングウィンドウ中に送られるものとして示されているが、他の実装形態では、要求３３８は、後のページングウィンドウまたは発見ウィンドウ中に第２のデバイスから送られ得る。

【０１１０】

[0122]第１のデータウィンドウ３３４中に、要求３３８に応答して、第１のデバイスと第２のデバイスとは、第１のデバイスが第２のデバイスに候補グループ鍵を送ることを可能にするためにＰ２Ｐ通信を実行し得る。データリンクグループの他のデバイスは、第１のデータウィンドウ３３４中に起動していない（たとえば、スリープモードまたは省電力モードにある）ことがある。

【０１１１】

[0123]第２のページングウィンドウ３４２中に、第２のデバイスは、データリンクグループの１つまたは複数のデバイスにデータリンクグループチャネル３０４を介して告知メッセージ３４６を送信し得る。たとえば、告知メッセージ３４６は、第１のデバイスによって発行された告知メッセージ３３６に基づき得るか、または第１のデバイスによって発行された告知メッセージ３３６の転送バージョンであり得る。告知メッセージ３４６に応答して、第３のデバイスは、候補グループ鍵を要求するために第２のデバイスに要求３４８を送り得る。第２のデータウィンドウ３４４中に、第２のデバイスと第３の第２のデバイスとは、第２のデバイスが第３のデバイスに候補グループ鍵を送ることを可能にするためにＰ２Ｐ通信を実行し得る。データリンクグループの第１のデバイスなどの他のデバイスは、第２のデータウィンドウ３４４中に起動していない（たとえば、スリープモードまたは省電力モードにある）ことがある。

【０１１２】

[0124]第３のページングウィンドウ３５２中に、ビーコンまたはメッセージは、通信されないことがある。したがって、第３のデータウィンドウ３５４中に、データリンクグループのデバイスのすべてが起動していないことがある。第４のページングウィンドウ３６２中に、第１のデバイスは、データリンクグループの１つまたは複数のデバイスにマルチキャスト告知メッセージ３６６を送信し得る。したがって、告知メッセージ３６６を受信したデータリンクグループのデバイスのすべては、第１のデバイスがデータリンクグループの他のデバイスにメッセージをマルチキャストすることを可能にするために、第４のデータウィンドウ３６４中に起動していることがある。

【０１１３】
[0125]このようにして、図３に、送信されるべきデータトラフィックのデータリンクグループを他のデバイスに通知するためにページングウィンドウまたは発見ウィンドウ中にデバイスがビーコン、メッセージ、またはそれらの組合せをどのように送り得るのかについて示す。送信されるべきデータトラフィックを他のデバイスに通知することによって、データトラフィックを受信することを目的としない１つまたは複数のデバイスは、データウィンドウ中に起動しない（たとえば、スリープモードまたは省電力モードに入り）、したがって、電力を節約し得る。
【０１１４】
[0126]図４を参照すると、第１の代表的なデバイス４０２と第２の代表的なデバイス４０４との間で通信する方法４００の例示的な実装形態が示されている。方法４００は、ラダー図によって示されている。第１のデバイス４０２と第２のデバイス４０４とは、ＮＡＮの同じデータリンクグループなどの同じデータリンクグループ中に含まれ得る。たとえば、第１のデバイス４０２と第２のデバイス４０４とは、図１のデバイス１０４～１１０、図２のデバイス２０２、または図３を参照しながら説明されるデバイスを含むか、またはそれに対応し得る。データリンクグループが２つのデバイス（たとえば、第１のデバイス４０２と第２のデバイス４０４と）を含むものとして説明されるが、他の実装形態では、データリンクグループは３つ以上のデバイスを含み得る。
【０１１５】
[0127]第１のデバイス４０２は、４１２において、第１のデバイス４０２の第１のアクティブ鍵（たとえば、第１のアクティブ鍵セット）として第１のグループ鍵と第１の配布鍵とを設定し得る。第１のグループ鍵および第１の配布鍵は、それぞれ、図１の第１のグループ鍵１３２と第１の配布鍵１３４とを含むか、またはそれに対応し得る。第２のデバイス４０４は、４１４において、第２のデバイス４０４の第２のアクティブ鍵（たとえば、第２のアクティブ鍵セット）として第１のグループ鍵と第１の配布鍵とを設定し得る。第１のデバイス４０２は、第２のデバイス４０４が第２のアクティブ鍵を設定する前に、その後に、またはそれと同時に第１のアクティブ鍵を設定し得る。
【０１１６】
[0128]第１のデバイス４０２は、４２２において、第１のランダム値を使用して第１のカウントダウンを開始し得、第２のデバイス４０４は、４２４において、第２のランダム値を使用して第２のカウントダウンを開始し得る。たとえば、第１のランダム値、第２のランダム値、またはその両方は、図２のランダム値２２０を含むか、またはそれに対応し得る。第１のカウントダウンは、第１のデバイス４０２において実行される候補グループ鍵（たとえば、候補鍵セット）生成手順に対応し得、第２のカウントダウンは、第２のデバイス４０４において実行される候補グループ鍵生成手順に対応し得る。第１のデバイス４０２は、第２のデバイス４０４が第２のカウントダウンを開始する前に、その後に、またはそれと同時に第１のカウントダウンを開始し得る。
【０１１７】
[0129]第１のデバイス４０２は、４３２において、第１のカウントダウンの終了を検出し、第２のグループ鍵と第２の配布鍵とを生成し得る。たとえば、第１のデバイス４０２は、図２のカウンタ２０４などのカウンタの値に基づいて第１のカウントダウンの終了を検出し得る。第２のグループ鍵は、図１の第２のグループ鍵１４２または図２のグループ鍵２１４を含むか、またはそれに対応し得る。第２の配布鍵は、図１の第２の配布鍵１４４を含むか、またはそれに対応し得る。第２のグループ鍵と第２の配布鍵とを生成するために、第１のデバイス４０２は、図１の鍵論理１１２または図２の鍵生成器２０６などの１つまたは複数の鍵生成器を含み得る。
【０１１８】
[0130]第１のデバイス４０２は、４３３において、第２のデバイス４０４に告知メッセージを送り得る。たとえば、告知メッセージは、図１の告知メッセージ１６０を含むか、またはそれに対応し得る。告知メッセージは、第１のデバイス４０２が配布されるべき第

２のグループ鍵を有することを第２のデバイス４０４に示し得る。いくつかの実装形態では、告知メッセージは、マルチキャストトラフィック告知メッセージなどのマルチキャストメッセージを含み得る。告知メッセージは、第２のグループ鍵が生成された後に送られるものとして説明されるが、他の実装形態では、告知メッセージは、第１のカウントダウンの終了が検出された後の、第２のグループ鍵が生成される前に送られ得る。

【０１１９】

[0131]第２のデバイス４３４は、４３４において、第２のカウントダウンを終了し得る。たとえば、第２のデバイス４３４は、第１のデバイス４０２から告知メッセージを受信したことに応答して候補グループ鍵生成手順を抑制し得る。

【０１２０】

[0132]第１のデバイス４０２は、４４２において、第１の配布鍵を使用して第２のグループ鍵と第２の配布鍵とを符号化（または暗号化）し得る。第１のデバイス４０２は、４４３において、第２のデバイス４０４に鍵配信メッセージを送り得る。たとえば、鍵配信メッセージは、図１の鍵配信メッセージ１８０を含むか、またはそれに対応し得る。鍵配信メッセージは、符号化（または暗号化）された第２のグループ鍵と符号化（または暗号化）された第２の配布鍵とを含み得る。いくつかの実装形態では、第１のデバイス４０２は、第１のデバイス４０２に関連するかまたは関連しないデータリンクグループのデバイスによって受信され得るマルチキャストメッセージとして第２のデバイス４０４に鍵配信メッセージを送り得る。符号化（または暗号化）された第２のグループ鍵と符号化（または暗号化）された第２の配布鍵とが、単一の鍵配信メッセージ中に含まれるものとして説明されるが、他の実装形態では、符号化（または暗号化）された第２のグループ鍵と符号化（または暗号化）された第２の配布鍵とは別個のメッセージ中で送られ得る。

【０１２１】

[0133]第２のデバイス４０４は、４４４において、第１の配布鍵を使用して符号化（または暗号化）された第２のグループ鍵と符号化（または暗号化）された第２の配布鍵とを復号（または解読）し得る。第１のデバイス４０２は、４５２において、第１のアクティブ鍵として第２のグループ鍵と第２の配布鍵とを設定し得、第２のデバイス４０４は、４５４において、第２のアクティブ鍵として第２のグループ鍵と第２の配布鍵とを設定し得る。配布鍵を使用するものとして説明されるが、他の実装形態では、候補グループ鍵を符号化（または暗号化）するために配布鍵が使用されないことがある。たとえば、第１のデバイス４０２は、第１のグループ鍵に基づいて第２のグループ鍵を符号化（または暗号化）し得る。

【０１２２】

[0134]第２のグループ鍵を符号化（または暗号化）するために第２の第１の配布鍵を使用することによって、第１のデバイス４０２は、第２のグループ鍵を符号化（または暗号化）し、マルチキャストメッセージとしてデータリンクグループの１つまたは複数のデバイス（たとえば、第２のデバイス４０４）に第２のグループ鍵を配布し得る。第１の配布鍵が、データリンクグループの各デバイス（たとえば、第２のデバイス４０４）に知られるので、マルチキャストメッセージは、１つまたは複数のデバイスが第１のデバイス４０２に関連するのか関連しないのかにかかわらず、１つまたは複数のデバイスに符号化（または暗号化）された第２のグループ鍵を直接送るために使用され得る。したがって、第２のグループ鍵を配布するために、追加のセキュリティ関連付け手順、Ｐ２Ｐ通信、またはそれらの組合せがデータリンクグループの他のデバイスと第１のデバイスによって実行されない。したがって、配布鍵がデータリンクグループによって使用されるとき、第２のグループ鍵を配布するデータトラフィックの量は、第２のグループ鍵を配布するために配布鍵が使用されないときと比較して低減され得る。

【０１２３】

[0135]図５を参照すると、データリンクグループ内の通信を示す特定の例示的なタイミング図５００が示されている。図５に、データリンクグループのグループ鍵（アクティブグループ鍵など）の寿命および満了を示す。時間ｔ０（図示せず）に、第１のグループ鍵

（鍵１）の生成が開始され得るか、または第１のグループ鍵（鍵１）が生成され得る。第１のグループ鍵（鍵１）の生成について、少なくとも図２を参照しながら説明される。第１のグループ鍵（鍵１）に対応するタイムスタンプが、生成され、図１の鍵配信メッセージ１８０などのメッセージ中に含まれ得る。特定の実装形態では、鍵識別子１４３は、タイムスタンプを含み得る。第１のグループ鍵（鍵１）が、第１のグループ鍵（鍵１）に対応するデータリンクグループのデバイス間で送信されるとき、タイムスタンプは、第１のグループ鍵（鍵１）とともにメッセージ中に含まれ得る。図示のように、鍵１は、時間ｔ１にアクティブ鍵になる。データリンクグループのデバイスは、時間ｔ１にカウントダウンを開始し得る。カウントダウンは、第１のグループ鍵（鍵１）の存続期間、関連付けウィンドウまでの時間期間、または他のタイミング情報を示し得る。単一のカウントダウンについて説明されるが、いくつかの実装形態では、複数のカウントダウンが使用され得る。他の実装形態では、カウントダウンは、デバイスが告知メッセージを受信するのに対応する時間などの前の時間に開始し得る。

【０１２４】

[0136]時間ｔ２に開始し、時間ｔ３に終了する発見ウィンドウ中に、第２のグループ鍵（鍵２）に対応する告知メッセージ５１０は、データリンクグループのデバイスによって送信される。告知メッセージ５１０は、データリンクグループのデバイスが第２のグループ鍵（鍵２）を生成するのに応答して送信され得る。告知メッセージ５１０は、図１の告知メッセージ１６０、告知メッセージ１７０、またはそれらの組合せを含むか、またはそれに対応し得る。発見ウィンドウ中に送信される告知メッセージとして説明されるが、他の実装形態では、第２のグループ鍵（鍵２）は、図１および図３を参照しながら説明されるように、データリンクグループのページングウィンドウ中に送信されるページングメッセージによって告知され得る。

【０１２５】

[0137]告知メッセージ５１０が特定のデバイスによって送信された後、特定のデバイスは、図１を参照しながら説明されるように、データリンクグループの他のデバイスに第２のグループ鍵（鍵２）を配布するために、ページングメッセージと鍵配信メッセージとを送信し得る。さらに、第２のグループ鍵（鍵２）を受信するデバイスはまた、第２のグループ鍵（鍵２）がデータリンクグループ全体にわたって伝搬するように、他のデバイスに第２のグループ鍵（鍵２）を伝搬し得る。しかしながら、データリンクグループの１つまたは複数のデバイスは、時間ｔ４に発生する関連付けウィンドウの開始時に第２のグループ鍵（鍵２）を受信していないことがある。たとえば、デバイスは、鍵生成器デバイスから複数ホップ離れていることがあり得、第２のグループ鍵（鍵２）は、デバイスに達していないことがあるか、またはデバイスは、特定のデバイスに関連しないことがあり、特定のデバイスは、関連付けウィンドウの開始時にデバイスに第２のグループ鍵（鍵２）を送信していない。関連付けウィンドウは、図１中の第１のデバイス１０４など、候補グループ鍵（鍵２）を有するデータリンクグループのデバイスに関連しようと１つまたは複数のデバイスが試みる時間に対応し得る。

【０１２６】

[0138]関連付けウィンドウは、データリンクグループの各デバイスに知られる所定の時間（関連付けしきい値時間）に開始し得る。関連付けウィンドウは、時間ｔ６に第１のグループ鍵（鍵１）の寿命の満了より前に発生し得、時間ｔ６にまたはその前に第２のグループ鍵（鍵２）がアクティブグループ鍵として設定されるより前に発生し得る。特定の実装形態では、関連付けしきい値時間は、ＩＥＥＥ８０２．１１規格、Ｗｉ－Ｆｉ　Ａｌｌｉａｎｃｅ規格、ＮＡＮ規格、またはそれらの組合せなどのワイヤレス通信規格において定義されている。いくつかの実装形態では、関連付けしきい値時間は、図１の鍵配信メッセージ１８０などの鍵配信メッセージによって示され得る。たとえば、関連付けしきい値時間は、鍵識別子１４３によって示され得る。他の実装形態では、関連付けしきい値時間は、データリンクグループのデバイスによってネゴシエートされ得る。

【０１２７】

[0139]関連付けウィンドウ中に、１つまたは複数のデバイスが関連付け動作５２０を実行し得る。例示的な例として、図１を参照すると、第４のデバイス１１０は、第１のデバイス１０４に関連付け要求１７５を送り得、第１のデバイス１０４は、関連付けウィンドウ中に第４のデバイス１１０に関連付け応答１７６または関連付け拒絶１７８を送り得る。時間ｔ５に、ＮＡＮの第２の発見ウィンドウが開始する。１つまたは複数の告知メッセージが第２の発見ウィンドウ中に送信され得る。時間ｔ６に、第２の発見ウィンドウが終了する。いくつかの実装形態では、関連付けウィンドウは、図５に示すように、時間ｔ６に終了し、第２の発見ウィンドウを含む。他の実装形態では、関連付けウィンドウは、時間ｔ５に終了し得る。

【０１２８】

[0140]ｔ２からｔ６までの時間期間は、グループ鍵更新ウィンドウに対応し得る。グループ鍵更新ウィンドウは、データリンクグループの１つまたは複数のデバイスがデータリンクのデバイスに第２のグループ鍵（鍵２）などの候補グループ鍵を配布する時間期間に対応し得る。第２のグループ鍵（鍵２）を含む鍵配信メッセージ（図示せず）は、グループ鍵更新ウィンドウ中にデータリンクグループのデバイス間で送信され得る。たとえば、図１を参照すると、鍵配信メッセージ１８０は、データリンクグループのデバイスに送信され得る。第１の発見ウィンドウの開始と第２の発見ウィンドウの終了との間に起こるものとして示されているが、グループ鍵更新ウィンドウは、複数の発見ウィンドウの間に起こり得る。たとえば、告知メッセージ５１０は、複数の発見ウィンドウ中に送信（または、再送信）され得る。複数の発見ウィンドウ中に告知メッセージ５１０を送信することは、データリンクグループの各デバイスが告知メッセージ５１０を受信する可能性を増加させ得る。

【０１２９】

[0141]第３のグループ鍵（鍵３）の生成は、時間ｔ７に開始され得、これは、第２のグループ鍵（鍵２）の満了の前の特定の所定の量の時間に対応し得る。第２のグループ鍵（鍵２）は、時間ｔ８に満了し得る。いくつかの実装形態では、時間ｔ２と時間ｔ６との間の持続時間は、時間ｔ７と時間ｔ８との継続時間と同じである。他の実装形態では、時間ｔ２および時間ｔ６との間の持続時間は、時間ｔ７と時間ｔ８との継続時間とは異なる。いくつかの実装形態では、第１のグループ鍵（鍵１）と、第２のグループ鍵（鍵２）と、第３のグループ鍵（鍵３）とは、同じ寿命を有する。他の実装形態では、第１のグループ鍵（鍵１）と、第２のグループ鍵（鍵２）と、第３のグループ鍵（鍵３）とは、異なる寿命を有する。

【０１３０】

[0142]このようにして、図５に、グループ鍵に関係するタイミングと関係する告知メッセージとについて説明する。発見ウィンドウ中に告知メッセージを送信することは、データリンクグループのデバイスがアクティブ動作モードで動作しており、告知メッセージを受信することが可能である可能性を増加させ得る。さらに、関連付けウィンドウの開始までに候補グループ鍵（たとえば、潜在的な「次の」アクティブグループ鍵）を受信しなかった１つまたは複数のデバイスは、他のデバイスとの関連付け動作を実行するための指定された時間を有し得る。関連付け動作は、デバイスを、候補グループ鍵を有する別のデバイスに関連付け得、それによって、デバイスが候補グループ鍵を受信することが可能になる。関連付けウィンドウの継続時間は、データリンクグループの各デバイスが候補グループ鍵を有するデバイスに関連する時間を有するターゲット可能性を達成するように設定され得る。

【０１３１】

[0143]図６を参照すると、例示的なページ属性６００の図。ページ属性６００は、ページングメッセージ中に含まれ得る。特定の実装形態では、ページ属性６００は、図１のページ属性１６９を含むか、またはそれに対応し得る。ページ属性６００が、特定のフィールドを含むものとして図６に示されているが、例示は限定するものではない。他の実装形態では、ページ属性６００のフィールドは、異なる順序で構成され得、図６に示すものよ

りも少ないフィールドまたは多くのフィールドを含み得る。

【０１３２】

[0144]ページ属性６００は、属性ＩＤフィールド６０２を含み得る。ページ属性６００は、ページ属性６００の長さを特定する値を含む長さフィールド６０４を含み得る。ページ属性６００はまた、データリンクグループを特定する値を含むデータリンクグループＩＤフィールド６０６を含み得る。データリンクグループＩＤフィールド６０６は、ＮＡＮデータリンク（ＮＤＬ）識別子と呼ばれることもある。

【０１３３】

[0145]ページ属性６００は、ページ制御フィールド６０８とトラフィックインジケータまたはグループ鍵生成器ＩＤフィールド６１０をさらに含む。ページ属性６００は、随意に、トラフィックタイプインジケータ６１２を含む。ページ制御フィールド６０８は、ページ属性６００に関係する情報を示す。ページ制御フィールド６０８のビットの第１のセット６２０は、本明細書でさらに説明するように、ページ属性６００がトラフィックインジケータを含むのか、またはグループ鍵生成器ＩＤを含むのかを示し得る。さらに、トラフィックインジケータがページ属性６００中に含まれる場合、ビットの第１のセット６２０は、本明細書でさらに説明するように、トラフィックインジケータのタイプを示し得る。ある特定の実装形態では、ビットの第１のセット６２０は３ビットを含む。ページ制御フィールド６０８のビットの第２のセット６２２は、トラフィックタイプインジケータ６１２がページ属性６００に含まれるのかどうかを示し得る。ページ制御フィールド６０８のビットの第３のセット６２４は予備であり得る。他の実装形態では、ページ制御フィールド６０８中のビットは、別様に分割され得る。

【０１３４】

[0146]ビットの第１のセット６２０によって提供される指示を例示すると、ビットの第１のセット６２０が第１の特定の値を有する場合、ページ属性６００を含むページングメッセージを送信するデバイスによる送信をスケジュールされるデータは、マルチキャストデータである。特定の実装形態では、データがマルチキャストデータである場合、トラフィックインジケータまたはグループ鍵生成器ＩＤフィールド６１０はページ属性６００中に含まれないことがある。この場合、ページ属性６００を含むページングメッセージを受信する各デバイスは、ページ制御フィールド６０８のビットの第１のセット６２０が第１の特定の値を有することを検出することに基づいて、アクティブ動作モードにとどまり得る。ビットの第１のセット６２０が、第２の特定の値、第３の特定の値、または第４の特定の値を有する場合、トラフィックインジケータまたはグループ鍵生成器ＩＤフィールド６１０は、トラフィックインジケータを含む。ビットの第１のセット６２０が第２の特定の値を有する場合、データは、ユニキャストデータであり得、トラフィックインジケータは、トラフィックインジケータマップ（ＴＩＭ：traffic indicator map）によって表され得る。ビットの第１のセット６２０が第３の特定の値を有する場合、データは、ユニキャストデータであり得、トラフィックインジケータは、ブルームフィルタによって表され得る。ビットの第１のセット６２０が第４の特定の値を有する場合、データは、ユニキャストデータであり得、トラフィックインジケータは、ＭＡＣアドレスのリストによって表され得る。ビットの第１のセット６２０が第５の特定の値を有する場合、トラフィックインジケータまたはグループ鍵生成器ＩＤフィールド６１０は、グループ鍵生成器ＩＤを含む。この場合、ビットの第１のセット６２０は、候補グループ鍵を生成したデバイスの識別子を示す。この場合、グループ鍵生成器ＩＤは、候補グループ鍵を生成したデバイスのＭＡＣアドレス（または他の識別子）を含み、トラフィックタイプインジケータ６１２が、ページ属性６００中に含まれる場合、トラフィックタイプインジケータ６１２は、最も優先度の高いトラフィックタイプを示す。たとえば、トラフィックタイプインジケータ６１２は、トラフィックに対応する最高のサービス品質（ＱｏＳ）カテゴリを示し得る。

【０１３５】

[0147]ページ属性６００がトラフィックインジケータを含む場合、トラフィックインジケータは、可変サイズを有し、次回のデータウィンドウ中に特定のデバイスからトラフィ

ックを受信するようにスケジュールされたデバイスのサブセットを示す。トラフィックインジケータは、ＴＩＭ、ブルームフィルタ、またはＭＡＣアドレスのリストによって表され得る。トラフィックインジケータは、図１の第１のデバイス１０４からのトラフィックなどのトラフィックを受信するようにスケジュールされた各デバイスを識別し得る。いくつかの実装形態では、ページングメッセージは、複数のページ属性６００を含み得る。たとえば、ページングメッセージは、（トラフィックインジケータまたはグループ鍵生成器ＩＤフィールド６１０とページ制御フィールド６０８とに基づいて）グループ鍵生成器ＩＤを示す第１のページ属性とデータリンクグループの１つまたは複数のデバイスへの送信のためにスケジュールされた他のデータに対応する第２のページ属性とを含み得る。

【０１３６】

[0148]このようにして、図６に、トラフィックを受信するかまたは鍵生成器デバイスのＩＤを示すようにスケジュールされたデバイスのリストを示すために、サービス発見フレーム（ＳＤＦ）、（ＩＥＥＥ８０２．１１に記載されている）パブリックアクションフレーム、管理フレーム、またはＮＡＮ管理フレームなどのフレーム中に含まれ得るページ属性６００を示す。追加または代替として、ページ属性６００は、候補グループ鍵の生成を告知するためにページングメッセージ中に含まれ得る。

【０１３７】

[0149]図７を参照すると、データリンクグループのデバイスにおける動作の方法７００の第１の実装形態が示されている。データリンクグループは、インフラストラクチャ不要のピアツーピアネットワークを含み得る。たとえば、データリンクグループは、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み得る。複数のデバイスは、それら自体の間の（たとえば、複数のデバイスの間の）データ接続性を形成し得る。方法７００は、デバイス１０４～１１０のいずれか、図２のデバイス２０２、図３を参照しながら説明されるデバイスのいずれか、または図４のデバイス４０２、４０４のいずれかにおいて実行され得る。

【０１３８】

[0150]方法７００は、７０２において、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生成することを含む。たとえば、候補グループ鍵は、図１の第２のグループ鍵１４２または図２のグループ鍵２１４を含むか、またはそれに対応し得る。候補グループ鍵は、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、解読、またはその両方を可能にするためにアクティブグループ鍵として設定され得る。第２のグループ鍵１４２は、図１を参照しながら説明されるように、第１のデバイス１０４によって生成され得る。

【０１３９】

[0151]方法７００は、７０４において、データリンクグループの第１のデバイスから第２のデバイスに、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、ここで、告知メッセージは、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、およびここで、告知メッセージは、マルチキャストメッセージを含む、を含む。たとえば、ページングウィンドウは、グループ送信ウィンドウの一部であり得る。例示のために、ページングウィンドウは、図３のページングウィンドウ３３２、３４２、３５２、３６２のうちの１つであり得る。告知メッセージは、図１の告知メッセージ１６０または告知メッセージ１７０を含むか、またはそれに対応し得る。

【０１４０】

[0152]いくつかの実装形態では、告知メッセージは、候補グループ鍵を生成したことに応答して送信され得る。たとえば、告知メッセージは、第１のデバイスがデータリンクグループの別のデバイスから候補グループ鍵を受信したことに応答して送信され得る。別の例として、告知メッセージは、第１のデバイスが候補グループ鍵の生成を開始したことに応答して、または第１のデバイスが候補グループ鍵を生成したことに応答して送信され得る。マルチキャストメッセージ（たとえば、告知メッセージ）は、告知メッセージがグループ鍵告知メッセージであることを示す１つまたは複数のビットを含み得る。たとえば、

１つまたは複数のビットは、図１のフラグ１６２を含むか、またはそれに対応し得る。１つまたは複数のビットは、告知メッセージの特定のフィールド中に含まれ得る。告知メッセージはまた、データリンクグループのグループ識別子と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とを含み得る。いくつかの実装形態では、第１のデバイスと特定のデバイスとは同じデバイスであり、他の実装形態では、第１のデバイスと特定のデバイスとは異なるデバイスである。グループ識別子およびデバイス識別子は、図１の、それぞれ、グループ識別子１６４およびデバイス識別子１６６、を含むか、またはそれに対応し得る。デバイス識別子は、特定のデバイスのＭＡＣアドレスであり得る。さらに、告知メッセージは、特定のデバイスによる候補グループ鍵の生成に関連するタイムスタンプを含み得る。

【０１４１】

[0153]いくつかの実装形態では、第１のデバイスは、告知メッセージを送った後に、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送り得る。第２のマルチキャストメッセージは、図１の第１の配布鍵１３４などの配布鍵を使用して保護され得る。データリンクグループの各デバイスは、配布鍵の対応するコピーを含む。配布鍵は、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符号化、復号、またはその両方を行うためだけに使用されるように構成され得る。

【０１４２】

[0154]いくつかの実装形態では、第１のデバイスが告知メッセージを送信するとき、第１のデバイスは、データリンクグループの第２のデバイスに関連し得る。たとえば、第１のデバイスが図１の第１のデバイス１０４であるとき、第２のデバイスは、図１の第２のデバイス１０６であり得る。第１のデバイスは、第１のデバイスから第２のデバイスに候補グループ鍵に送りたいという第２のデバイスからの要求を受信し得る。第１のデバイスは、第１のデバイスが第２のデバイスに関連することに対応するペアワイズ鍵を使用して候補グループ鍵を暗号化した後に、第２のデバイスに候補グループ鍵を送り得る。たとえば、ペアワイズ鍵は、第１のデバイスと第２のデバイスとの間に実行されるセキュリティ関連付け手順中に生成され得る。ペアワイズ鍵は、セキュリティ関連付け手順の後に第１のデバイスと第２のデバイスとの間のセキュアな通信を可能にし得る。ペアワイズ鍵は、図１のペアワイズ鍵１４６を含むか、またはそれに対応し得る。

【０１４３】

[0155]他の実装形態では、告知メッセージを送信した後に、第１のデバイスは、データリンクグループの第３のデバイスに関連することを第１のデバイスに求める要求を受信し得る。たとえば、第３のデバイスは、図１の第４のデバイス１１０を含むか、またはそれに対応し得る。第１のデバイスは、第３のデバイスとのセキュリティ関連付けを行い得、第１のデバイスと第３のデバイスとに対応するペアワイズ鍵は、セキュリティ関連付け中に生成（たとえば、確立）され得る。セキュリティ関連付けの完了の後に、第１のデバイスは、第３のデバイスに候補グループ鍵を送ることを第１のデバイスに求める第２の要求を受信し得る。代替的に、セキュリティ関連付けの完了の後に、第１のデバイスは、第３のデバイスに候補グループ鍵を自動的に送り得る。

【０１４４】

[0156]いくつかの実装形態では、第１のデバイスは、告知メッセージが送信された後に第４のデバイスからメッセージを受信し得る。メッセージは、ザットザメッセージが第２のグループ鍵告知メッセージであることを示し得る。メッセージは、データリンクグループの特定のデバイスによって生成された第２の候補グループ鍵に対応し得る。特定のデバイスと第２のデバイスとは同じデバイスであり得、または特定のデバイスと第２のデバイスとは異なるデバイスであり得る。特定のデバイスと第２のデバイスとが異なるデバイスであるとき、第２のデバイスは、第１のデバイスから１ホップだけ離れていることがあり、特定のデバイスは、第１のデバイスから複数ホップだけ離れていることがある。いくつかの実装形態では、第２の候補グループ鍵は、第１のデバイスによって生成されたアクティブグループ鍵に取って代わり得る。第２の候補グループ鍵を受信する前に、第１のデバ

イスは、データリンクグループの１つまたは複数のデバイスにマルチキャスト要求を送り得る。マルチキャスト要求に応答して、第１のデバイスは、データリンクグループの特定のデバイスから第２の候補グループ鍵を受信し得る。

【０１４５】

[0157]第１のデバイスが候補グループ鍵を有する特定のデバイスに関連しないという決定に応答して、第１のデバイスは、第１のデバイスに関連する、候補グループ鍵を有するデータリンクグループの第５のデバイスを識別し得る。第１のデバイスは、データリンクグループの図１の第１のグループ鍵１３２など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第５のデバイスを識別し得る。時間期間は、第２の告知メッセージが受信された後に開始し得、アクティブグループ鍵の満了の前の所定の時間に終了し得る。たとえば、第１のデバイスは、特定のメッセージが第５のデバイスから第１のデバイスにおいて受信されたことに応答して候補グループ鍵を有するものとして第５のデバイスを識別し得る。特定のメッセージは、第２の告知メッセージが第１のデバイスにおいて受信された後に、その時間期間の終了より前に受信され得る。第１のデバイスは、第５のデバイスに候補グループ鍵を要求し得、アクティブグループ鍵の満了より前に第５のデバイスから候補グループ鍵を受信し得る。いくつかの実装形態では、第１のデバイスは、第２の告知メッセージが受信されると、第５のデバイスに関連し得、第１のデバイスが第５のデバイスから候補グループ鍵を受信すると、第５のデバイスと関連しないことがある。たとえば、第５のデバイスは、配布鍵を使用してマルチキャストメッセージとして第１のデバイスに候補グループ鍵を送信し得る。

【０１４６】

[0158]方法７００により、データリンクグループのデバイスへの候補グループ鍵の配布が可能になる。候補グループ鍵は、データリンクグループを含むＮＡＮ内での鍵関連のトラフィックとオーバーヘッドとが低減された状態で配布され得る。たとえば、鍵関連のトラフィックは、データリンクグループのデバイスが起動しているときにページングウィンドウ中にグループ鍵告知メッセージなどの告知メッセージを送ることによって低減され得る。別の例として、候補グループ鍵を符号化するためにアクティブ配布鍵が使用され得、符号化された候補グループ鍵が、データリンクグループの１つまたは複数のデバイスにマルチキャストメッセージとして送られ得る。マルチキャストメッセージとして候補グループ鍵を送ることによって、候補グループ鍵は、データリンクグループの第１のデバイスと別のデバイスとの間でセキュリティ関連付け、Ｐ２Ｐ通信、またはそれらの組合せを実行することなしにデータリンクグループの１つまたは複数のデバイスに配布され得る。

【０１４７】

[0159]図８を参照すると、データリンクグループのデバイスにおける動作の方法８００の第２の実装形態が示されている。方法８００は、ワイヤレス通信のための方法を含むかまたはそれに対応し、デバイス１０４～１１０のいずれか、図２のデバイス２０２、図３を参照しながら説明されるデバイスのいずれか、または図４のデバイス４０２、４０４のいずれかにおいて実行され得る。

【０１４８】

[0160]方法８００は、８０２において、データリンクグループの第１のデバイスにおいて、グループ鍵と配布鍵とを生成することを含み得る。たとえば、グループ鍵および配布鍵は、図１の第２のグループ鍵１４２と第２の配布鍵１４４とを含むか、またはそれに対応し得る。

【０１４９】

[0161]方法８００は、８０４において、第２の配布鍵を使用してグループ鍵と配布鍵とを符号化すること、ここで、第２の配布鍵は、データリンクグループのアクティブグループ鍵に対応する、を含み得る。たとえば、第２の配布鍵は、図１の第１の配布鍵１３４を含むか、またはそれに対応し得る。いくつかの実装形態では、第２の配布鍵は、アクティブグループ鍵に対応し得（たとえば、アクティブ鍵セットなどの鍵のセットの一部であり得）、第２の配布鍵は、グループ鍵がアクティブグループ鍵として設定されるまで、鍵配

信メッセージを符号化および復号するために使用可能であり得る。

【０１５０】

[0162]方法８００は、８０６において、データリンクグループの１つまたは複数のデバイスに符号化されたグループ鍵と符号化された配布鍵とを送信することをさらに含む。いくつかの実装形態では、符号化されたグループ鍵と符号化された配布鍵とは、図１のワイヤレスネットワーク１０２などのＮＡＮ中に含まれる複数のデバイスに符号化されたグループ鍵と符号化された配布鍵とをマルチキャストすることによって送信され得る。データリンクグループの各デバイスは、第２の配布鍵を含み得、第２の配布鍵を使用して符号化されたグループ鍵と符号化された配布鍵とを復号するように構成され得る。

【０１５１】

[0163]いくつかの実装形態では、グループ鍵と配布鍵とを生成するより前に、第２のグループ鍵（たとえば、候補グループ鍵）と第２の配布鍵とがデータリンクグループの別のデバイスから第１のデバイスにおいて受信され得る。たとえば、第２のグループ鍵は、図１の第１のグループ鍵１３２を含むか、またはそれに対応し得る。第１のデバイスは、（たとえば、第２の候補グループ鍵がアクティブグループ鍵である間に生成される）グループ鍵を生成するより前に第２のグループ鍵をアクティブグループ鍵として設定し得る。第１のデバイスは、アクティブグループ鍵としての第２のグループ鍵の満了を検出したことに応答してグループ鍵をアクティブグループ鍵として設定し得る。したがって、グループ鍵は、データリンクグループのアクティブグループ鍵として第２のグループ鍵を置き換え得る。

【０１５２】

[0164]いくつかの実装形態では、グループ鍵と配布鍵とを符号化するより前に、図１の告知メッセージ１６０などの告知メッセージが１つまたは複数のデバイスに送信され得る。告知メッセージは、グループ鍵に対応し得る。たとえば、告知メッセージは、グループ鍵が配布のために利用可能であることを示し得る。告知メッセージは、グループ送信ウィンドウのページングウィンドウ中に送信され得る。グループ送信ウィンドウは、図３のグループ送信ウィンドウ３２０～３２６のうちの１つを含むか、またはそれに対応し得る。符号化されたグループ鍵と符号化された配布鍵とは、グループ送信ウィンドウのデータウィンドウ中に、またはグループ送信ウィンドウの後に発生する別のグループ送信ウィンドウ中に送信され得る。

【０１５３】

[0165]方法８００により、アクティブ配布鍵（たとえば、第１の配布鍵１３４）をグループ鍵を符号化するために使用することが可能になり、符号化されたグループ鍵は、データリンクグループの１つまたは複数のデバイスにマルチキャストメッセージとして送られ得る。グループ鍵（たとえば、「次の」アクティブグループ鍵として設定するために利用可能な候補鍵）を含むマルチキャストメッセージを送ることによって、グループ鍵は、データリンクグループの第１のデバイスと別のデバイスとの間でセキュリティ関連付け、Ｐ２Ｐ通信、またはそれらの組合せを行うことなしにデータリンクグループの１つまたは複数のデバイスに配布され得る。

【０１５４】

[0166]図９を参照すると、ワイヤレスネットワークのデバイスにおける動作の方法９００の第３の実装形態が示されている。方法９００は、図１のデバイス１０４～１１０のいずれか、図２のデバイス２０２、図３を参照しながら説明されるデバイスのいずれか、または図４のデバイス４０２、４０４のいずれかにおいて実行され得る。

【０１５５】

[0167]方法９００は、９０２において、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を含む。たとえば、図１を参照すると、第１のデバイス１０４は、第２のグループ鍵１４２を取得し得る。候補グループ鍵は、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、解読、またはその両方を可能にするために潜在的な「次の」アクティブグループ鍵として設定され得る。

いくつかの実装形態では、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は、データリンクグループの別のデバイスから候補グループ鍵を受信することを含み得る。他の実装形態では、候補グループ鍵を取得することは、第１のデバイスにおいて候補グループ鍵を生成することを含み得る。

【０１５６】

[0168]方法９００は、９０４において、データリンクグループの第１のデバイスから第２のデバイスに、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を含む。告知メッセージは、ページングウィンドウ中に、データリンクグループに対応するワイヤレスチャネルを介して送信され得る。いくつかの実装形態では、告知メッセージは、マルチキャストメッセージを含み得る。

【０１５７】

[0169]いくつかの実装形態では、告知メッセージは、候補グループ鍵を取得したことに応答して送信され得る。たとえば、図１を参照すると、告知メッセージ１６０は、第１のデバイス１０４がデータリンクグループの別のデバイスから第２のグループ鍵１４２を受信したことに応答して送信され得る。別の例として、告知メッセージ１６０は、第１のデバイス１０４が第２のグループ鍵１４２の生成を開始したことに応答して、または第１のデバイス１０４が第２のグループ鍵１４２を生成したことに応答して送信され得る。マルチキャストメッセージ（たとえば、告知メッセージ１６０）は、告知メッセージがグループ鍵告知メッセージであることを示す１つまたは複数のビットを含み得る。１つまたは複数のビットは、告知メッセージ１６０の特定のフィールド中に含まれ得る。告知メッセージ１６０はまた、データリンクグループのグループＩＤ１６４と第２のグループ鍵１４２を生成した特定のデバイスのデバイスＩＤ１６６とを含み得る。

【０１５８】

[0170]いくつかの実装形態では、第１のデバイスは、データリンクグループの第２のデバイスからトリガメッセージを受信し得、ここで、第２のデバイスは、第１のデバイスと関連する状態にある。たとえば、第１のデバイス１０４は、第２のデバイス１０６からトリガメッセージ１６７を受信し得る。第１のデバイスは、トリガメッセージを受信したことに応答して第２のデバイスに候補グループ鍵を送信し得る。たとえば、第１のデバイス１０４は、第２のデバイス１０６に第２のグループ鍵１４２を含む鍵配信メッセージ１８０を送信し得る。候補グループ鍵は、ペアワイズ鍵に基づいて暗号化され得る。ペアワイズ鍵は、第１のデバイスと第２のデバイスとの間の関連付けプロセス中に生成され得る。たとえば、第２のグループ鍵１４２は、ペアワイズ鍵１４６に基づいて暗号化され得る。特定の実装形態では、候補グループ鍵は、鍵配信メッセージ中に含まれ、鍵配信メッセージは、候補グループ鍵の有効期限を示す鍵識別子を含む。たとえば、鍵配信メッセージ１８０は、第２のグループ鍵１４２と鍵識別子１４３とを含み得る。

【０１５９】

[0171]いくつかの実装形態では、アクティブ鍵セットは、アクティブグループ鍵と、アクティブ配布鍵と、アクティブグループ完全性鍵とを含み得る。たとえば、アクティブ鍵セット１３０は、図１の第１のグループ鍵１３２と、第１の配布鍵１３４と、第１のグループ完全性鍵１３１とを含み得る。いくつかの実装形態では、候補鍵セットは、候補グループ鍵と、候補配布鍵と、候補グループ完全性鍵とを含み得る。たとえば、候補鍵セット１４０は、図１の第２のグループ鍵１４２と、第２の配布鍵１３４と、第２のグループ完全性鍵１４１とを含み得る。

【０１６０】

[0172]いくつかの実装形態では、候補グループ鍵は、アクティブグループ鍵、（アクティブ鍵セットの）アクティブ配布鍵、またはペアワイズ鍵に基づいて符号化され得る。たとえば、第２のグループ鍵１４２は、第１のグループ鍵１３２、第１の配布鍵１３４、またはペアワイズ鍵１４６に基づいて暗号化され得る。（暗号化された第２のグループ鍵１４２を含む）鍵配信メッセージ１８０は、第１のグループ鍵１３２、第１の配布鍵１３４、またはペアワイズ鍵１４６に基づいて暗号化され得る。方法９００は、符号化された候

補グループ鍵を送信することを含み得る。符号化された候補グループ鍵は、アクティブグループ鍵、（アクティブ鍵セットの）アクティブ配布鍵、またはペアワイズ鍵に基づいて復号され得る。たとえば、第２の鍵１４２は、第１のグループ鍵１３２、第１の配布鍵１３４、またはペアワイズ鍵１４６に基づいて解読され得る。特定の実装形態では、グループアドレス指定されたトラフィックは、アクティブ鍵セット中に含まれるアクティブグループ完全性鍵に基づいて検証され得る。

【０１６１】

[0173]ある実装形態では、第１のデバイスは、グループ鍵更新ウィンドウが満了した後にデータリンクグループの特定のデバイスから関連付け要求を受信し得る。特定の実装形態では、第１のデバイスは、関連付け要求を受信したことに応答して特定のデバイスに関連付け応答を送信し得る。関連付け応答により、特定のデバイスが、第１のデバイスに関連することが可能になり得る。たとえば、第１のデバイス１０４は、第４のデバイス１１０から関連付け要求１７５を受信し得、関連付け要求１７５を受信したことに応答して第４のデバイス１１０に関連付け応答１７６を送信し得る。別の実装形態では、第１のデバイスは、基準が満たされないと決定したことに応答して特定のデバイスに関連付け拒絶を送信し得る。たとえば、基準が満たされない場合、第１のデバイス１０４は、第４のデバイス１１０に関連付け拒絶１７８を送信し得る。

【０１６２】

[0174]いくつかの実装形態では、第１のデバイスは、データリンクグループの第２のデバイスから第２の告知メッセージを受信し得る。第２の告知メッセージは、候補グループ鍵の生成を示し得る。

【０１６３】

[0175]いくつかの実装形態では、第１のデバイスは、候補グループ鍵をランダムに生成することによって候補グループ鍵を取得し得る。特定の実装形態では、グループ候補鍵は、ランダムに生成された２５６ビットを含む。いくつかの実装形態では、候補グループ鍵は、ランダム値からのカウントダウンの満了に応答して生成され得る。

【０１６４】

[0176]いくつかの実装形態では、告知メッセージは、鍵インジケータ、データリンクグループのデータリンクグループ識別子、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み得る。たとえば、告知メッセージ１６０は、鍵インジケータ１６８と、グループＩＤ１６４と、デバイスＩＤ１６６とを含み得る。特定の実装形態では、鍵インジケータ１６８は、タイムスタンプ、ハッシュ値、またはその両方を含み得る。

【０１６５】

[0177]いくつかの実装形態では、鍵インジケータは、第１のデバイスのＭＡＣアドレス、ハッシュ値、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含み得る。ハッシュ値は、ＭＡＣアドレス、候補グループ鍵、またはその両方に基づいて生成され得る。たとえば、告知メッセージ１７０の鍵インジケータは、第２のデバイス１０６のＭＡＣアドレスを含み得る。デバイス識別子は、第２のグループ鍵１４２を生成した第１のデバイス１０４の第２のＭＡＣアドレスを含み得る。

【０１６６】

[0178]いくつかの実装形態では、第１のデバイスは、データリンクグループの第２のデバイスから第２の告知メッセージを受信し得る。第２の告知メッセージは、第２のグループ鍵と第２のタイムスタンプとを含み得る。第１のデバイスは、告知メッセージ中に含まれる第１のタイムスタンプが第２のタイムスタンプよりも前のものであると決定することに基づいて第２のデバイスに候補グループ鍵を送信し得る。特定の実装形態では、第１のデバイス１０４は、告知メッセージ１６０の送信の後に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し得る。

【０１６７】

[0179]いくつかの実装形態では、第１のデバイスは、データリンクグループの鍵生成器

デバイスとして動作し、データリンクグループの他のデバイスは、鍵生成器デバイスとして動作しないが、第１のデバイスは、鍵生成器デバイスとして動作するように指定される。第１のデバイスが鍵生成器デバイスとしての動作を中止する前に、方法９００は、データリンクグループの第１のデバイスから第２のデバイスにメッセージを送信すること、メッセージは、第２のデバイスが、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べきであることを示す、を含み得る。たとえば、第１のデバイス１０４は、図１を参照しながら説明されるように、第２のデバイスが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べきであることを示すメッセージを第２のデバイス１０６に送信し得る。方法９００はまた、第１のデバイスにおいて鍵生成動作を終了することを含み得る。方法９００は、第１のデバイスによってデータリンクグループとの関連付けを解除すること、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をさらに含み得る。たとえば、第１のデバイス１０４は、図１を参照しながら説明されるように、鍵生成動作を終了し、低電力動作モードに遷移し得る。

【０１６８】

[0180]いくつかの実装形態では、第１のデバイスは、データリンクグループの第１のデバイスから第２のデバイスにメッセージを送信し得る。メッセージは、第２のデバイスが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べきであることを示し得る。第１のデバイスは、メッセージを送った後にデータリンクグループとの関連付けを解除し得る。メッセージを受信したことに応答して、第２のデバイスは、データリンクグループの鍵生成器デバイスとして動作し得る。

【０１６９】

[0181]他の実装形態では、第１のデバイスは、第２の発見ウィンドウ中に第２の告知メッセージを受信し得、第２の告知メッセージは、データリンクグループの第２のデバイスが第２のグループ鍵を生成したことを示し得る。

【０１７０】

[0182]いくつかの実装形態では、第１のデバイスは、カウンタを更新し得る。カウンタは、候補グループ鍵の満了に関係し得る。第１のデバイスは、カウンタが特定の値に達したことに応答して新しいグループ鍵を生成し得る。第１のデバイスは、カウンタが特定の値に達するより前に第２の告知メッセージを受信したことに応答してカウンタを更新するのを停止し得る。

【０１７１】

[0183]いくつかの実装形態では、第１のデバイスは、しきい値数以下のデバイスに関連するように構成され得る。他の実装形態では、第１のデバイスは、必要に応じて他のデバイスに関連する。

【０１７２】

[0184]いくつかの実装形態では、第１のデバイスは、データリンクグループの第４のデバイスから関連付け要求を受信したことに応答してデータリンクグループの第３のデバイスと関係をたち得る。特定の実装形態では、第１のデバイスが第２のページングウィンドウの終了より前に第３のデバイスにトランスポートされるべきデータをバッファしていないので、第１のデバイスは、第３のデバイスとの関連付けを解除することを決定し得る。別の特定の実装形態では、第１のデバイスは、第４のデバイスから関連付け要求を受信するより前にデータリンクグループの第２のデバイスと関連する状態にあり得、第２のデバイスは、第３のデバイスと関連する状態にあり得る。第４のデバイスは、データリンクグループのデバイスと関連する状態にないことがある。この特定の実装形態では、第１のデバイスは、第３のデバイスが第２のデバイスと関連する状態にあることに基づいて第３のデバイスとの関連付けを解除することを決定し得る。

【０１７３】

[0185]図１０を参照すると、ワイヤレスネットワークのデバイスにおける動作の方法１０００の第４の実装形態が示されている。ワイヤレスネットワークは、複数のデータリンクグループを含み得る。方法１０００は、デバイス１０４～１１０のいずれか、図２のデ

バイス２０２、図３を参照しながら説明されるデバイスのいずれか、または図４のデバイス４０２、４０４のいずれかにおいて実行され得る。

【０１７４】

[0186]方法１０００は、１００２において、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を含む。たとえば、候補グループ鍵は、図１の第２のグループ鍵１４２、図２のグループ鍵２１４、または図３～図５を参照しながら説明される鍵のいずれかを含むか、またはそれに対応し得る。図１を参照すると、第１のデバイス１０４は、第２のグループ鍵１４２を取得し得る。いくつかの実装形態では、第１のデバイスは、第１のデバイスにおいて候補グループ鍵を生成することによって候補グループ鍵を取得する。他の実装形態では、第１のデバイスは、データリンクグループの別のデバイスから第１のデバイスにおいて候補グループ鍵を受信することによって候補グループ鍵を取得する。候補グループ鍵により、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つが可能になり得る。

【０１７５】

[0187]方法１０００は、１００４において、データリンクグループの第１のデバイスからデバイスに、利用可能性候補グループ鍵を示す告知メッセージを送信すること、ここで、告知メッセージは、発見ウィンドウ中に、第１の通信チャネルを介して送信される、およびここで、告知メッセージは、マルチキャストメッセージを含む、を含む。たとえば、告知メッセージ１６０は、図１の告知メッセージ１６０、告知メッセージ１７０、または図５の告知メッセージ５１０を含むか、またはそれに対応し得る。いくつかの実装形態では、告知メッセージは、発見ウィンドウ中に、ＮＡＮ通信チャネルを介して送信され得、告知メッセージは、マルチキャストメッセージであり得る。

【０１７６】

[0188]いくつかの実装形態では、第１の通信チャネルは、図３のネイバーアウェアネットワーク（ＮＡＮ）通信チャネル３０２などのＮＡＮ通信チャネルに対応し、グループ鍵更新ウィンドウは、発見ウィンドウの終了と第２の発見ウィンドウの開始との間の継続時間を含む。図３の第１の発見ウィンドウ３１０と第２の発見ウィンドウ３１２との間の継続時間などのグループ鍵更新ウィンドウは、複数の送信ウィンドウを含み得る。図１および図３を参照しながら説明されるように、複数の送信ウィンドウの第１の送信ウィンドウは、発見ウィンドウの終了からの第１のオフセットを有し得、複数の送信ウィンドウの第２の送信ウィンドウは、発見ウィンドウの終了からの第２のオフセットを有する。

【０１７７】

[0189]いくつかの実装形態では、方法１０００は、ページングウィンドウ中にＮＡＮの第１のデバイスから第２のデバイスに、第１のデバイスが第２のデバイスに送信すべき第１のグループ鍵に対応するデータを有することを示すページングメッセージを送信することを含み得る。ページングウィンドウは、グループ送信ウィンドウの一部であり得る。例示のために、ページングウィンドウは、図３のページングウィンドウ３３２、３４２、３５２、３６２のうちの１つであり得る。

【０１７８】

[0190]いくつかの実装形態では、方法１０００は、第２のデバイスからトリガメッセージを受信することと、トリガメッセージを受信したことに応答して候補グループ鍵を送信することとを含み得る。たとえば、トリガメッセージは、図１のトリガメッセージ１６７、図３の３３８の要求、または図３の要求３４８を含むか、またはそれに対応し得る。候補グループ鍵は、ペアワイズ鍵に基づいて暗号化され得、ペアワイズ鍵は、第１のデバイスと第２のデバイスとの間の関連付けプロセス中に生成され得る。たとえば、ペアワイズ鍵は、図１のペアワイズ鍵１４６を含むか、またはそれに対応し得る。肯定応答メッセージは、第１のデバイスによって受信され得る。肯定応答メッセージは、第２のデバイスが候補グループ鍵を受信したことを示し得る。

【０１７９】

[0191]いくつかの実装形態では、アクティブ鍵セットは、アクティブグループ鍵と、アクティブ配布鍵と、アクティブグループ完全性鍵とを含み得る。たとえば、アクティブ鍵セット１３０は、図１の第１のグループ鍵１３２と、第１の配布鍵１３４と、第１のグループ完全性鍵１３１とを含み得る。いくつかの実装形態では、候補鍵セットは、候補グループ鍵と、候補配布鍵と、候補グループ完全性鍵とを含み得る。たとえば、候補鍵セット１４０は、図１の第２のグループ鍵１４２と、第２の配布鍵１３４と、第２のグループ完全性鍵１４１とを含み得る。

【０１８０】

[0192]いくつかの実装形態では、候補グループ鍵は、アクティブグループ鍵、（アクティブ鍵セットの）アクティブ配布鍵、またはペアワイズ鍵に基づいて符号化され得る。たとえば、第２のグループ鍵１４２は、第１のグループ鍵１３２、第１の配布鍵１３４、またはペアワイズ鍵１４６に基づいて暗号化され得る。（暗号化された第２のグループ鍵１４２を含む）鍵配信メッセージ１８０は、第１のグループ鍵１３２、第１の配布鍵１３４、またはペアワイズ鍵１４６に基づいて暗号化され得る。方法１０００は、符号化された候補グループ鍵を送信することを含み得る。符号化された候補グループ鍵は、アクティブグループ鍵、（アクティブ鍵セットの）アクティブ配布鍵、またはペアワイズ鍵に基づいて復号され得る。たとえば、第２の鍵１４２は、第１のグループ鍵１３２、第１の配布鍵１３４、またはペアワイズ鍵１４６に基づいて解読され得る。特定の実装形態では、グループアドレス指定されたトラフィックは、図１の第１のグループ完全性鍵１３１など、アクティブ鍵セット中に含まれるアクティブグループ完全性鍵に基づいて検証され得る。

【０１８１】

[0193]他の実装形態では、候補グループ鍵は、関連付け要求を受信したことに応答して送信され得る。たとえば、（第２のグループ鍵１４２を含む）鍵配信メッセージ１８０は、関連付け要求１７５を受信したことに応答して第１のデバイス１０４から第４のデバイス１１０に送信され得る。方法１０００はまた、グループ鍵更新ウィンドウが満了した後にＮＡＮの特定のデバイスから関連付け要求を受信することを含み得る。グループ鍵更新ウィンドウは、データリンクグループ中での鍵更新動作の実行に対応する特定の時間間隔を含み得る。たとえば、グループ鍵更新ウィンドウは、データリンクグループ中での告知メッセージ、鍵配信メッセージ、またはその両方の生成、送信、受信、またはそれらの組合せに対応し得る。別の実装形態では、方法１０００は、関連付け要求を受信したことに応答して特定のデバイスに関連付け応答を送信することを含み、ここで、関連付け応答により、特定のデバイスが、第１のデバイスに関連することが可能になる。たとえば、図１を参照すると、第１のデバイス１０４は、告知メッセージ１６０を送信したことに応答して第４のデバイス１１０から関連付け要求１７５を受信し得る。第１のデバイス１０４は、関連付け要求１７５を受信したことに応答して第４のデバイス１１０に関連付け応答１７６を送信し得る。

【０１８２】

[0194]いくつかの実装形態では、方法１０００は、グループ鍵更新ウィンドウが満了した後にデータリンクグループの特定のデバイスから関連付け要求を受信することを含み得る。たとえば、関連付け要求は、図１の関連付け要求１７５を含むか、またはそれに対応し得る。図３の第１の発見ウィンドウ３１０と第２の発見ウィンドウ３１２との間の継続時間などのグループ鍵更新ウィンドウは、データリンクグループ中でのグループ鍵更新動作の実行に対応する特定の時間間隔を含み得る。方法１０００はまた、第１の基準を満たすと決定したことに応答して特定のデバイスに関連付け拒絶を送信することを含み得る。たとえば、関連付け拒絶は、図１の関連付け拒絶１７８を含むか、またはそれに対応し得る。第１の基準は、第１のデバイスに関連するデバイスの数がしきい値以上であるときに満たされ得る。

【０１８３】

[0195]いくつかの実装形態では、方法１０００は、告知メッセージを送信したことに応答して、データリンクグループの特定のデバイスから関連付け要求を受信することを含み

得る。たとえば、第１のデバイス１０４は、図１を参照しながら説明されるように、第１のデバイス１０４が告知メッセージ１６０を送信したことに応答して第４のデバイス１１０から関連付け要求１７５を受信し得る。方法１０００はまた、第２の基準を満たすと決定したことに応答して特定のデバイスに関連付け応答を送信することを含み得る。たとえば、関連付け応答は、図１の関連付け応答１７６を含むか、またはそれに対応し得る。第２の基準は、第１のデバイスに関連するデバイスの数がしきい値以下であるときに満たされ得る。たとえば、第１のデバイス１０４は、第１のデバイス１０４がしきい値よりも小さい数のデバイスに関連すると決定したことに応答して、関連付け応答１７６を送信し得る。

【０１８４】

[0196]方法１０００は、データリンクグループのデバイスにデータを送信することを含み得る。例示のために、第１のデバイスは、データリンクグループのデバイスにデータを送信し得、ここで、データは、候補グループ鍵がアクティブグループ鍵として設定された後に候補グループ鍵に基づいて暗号化される。たとえば、図１を参照すると、第１のデバイス１０４は、第２のデバイス１０６にデータを送信し得、データは、第２のグループ鍵１４２がアクティブグループ鍵として設定された後に第２のグループ鍵１４２に基づいて暗号化され得る。

【０１８５】

[0197]方法１０００は、アクティブグループ鍵の満了の前に第２の候補グループ鍵を生成することを含み得る。たとえば、第１のデバイス１０４は、第１のグループ鍵１３２の満了より前に第２のグループ鍵１４２を生成し得る。

【０１８６】

[0198]いくつかの実装形態では、方法１０００は、アクティブグループ鍵として候補グループ鍵を設定することを含み得る。たとえば、第１のデバイス１０４は、図１を参照しながら説明されるように、第１のグループ鍵１３２のアクティブグループ鍵としての満了の後に、第２のグループ鍵１４２をアクティブグループ鍵として設定し得る。方法１０００はまた、データリンクグループのデバイスにてアクティブグループ鍵に基づいて暗号化されたデータなどのデータを送信することを含み得る。例示のために、第１のデバイス１０４は、図１を参照しながら説明されるように、１つまたは複数のサービスを提供し、ワイヤレスネットワーク１０２のデバイスにグループアドレス指定されたトラフィックを送信し得る。方法１０００はまた、アクティブグループ鍵の満了の前に第２の候補グループ鍵を生成することを含み得る。方法１０００はまた、データリンクグループの複数の発見ウィンドウ中に第２の告知メッセージを送信することを含み得る。第２の告知メッセージは、第２の候補グループ鍵の利用可能性を示し得る。

【０１８７】

[0199]方法１０００は、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データリンクグループのデバイスに第２の候補グループ鍵を配布することを含み得る。方法１０００はまた、第１のデバイスに関連する各デバイスから対応する肯定応答メッセージを受信することに基づいて第１のデバイスに関連する各デバイスが第２の候補グループ鍵を受信したと決定することを含み得る。たとえば、肯定応答メッセージは、図１のＡＣＫを含むか、またはそれに対応し得る。方法１０００は、第１のデバイスに関連する各デバイスが第２の候補グループ鍵を受信したと決定したことに応答して第２の告知メッセージの送信を中止することをさらに含み得る。第１のデバイス１０４は、図１を参照しながら説明されるように、第１のデバイス１０４が第１のデバイス１０４に関連する各デバイスからＭＡＣ　ＡＣＫを受信したと決定したことに応答して告知メッセージ１７０を送信することを停止し得る。

【０１８８】

[0200]いくつかの実装形態では、候補グループ鍵は、図１の鍵インジケータ１６８などの第１の鍵インジケータに関係する。たとえば、鍵インジケータ１６８は、第２のグループ鍵１４２に関係する情報を与え得、鍵インジケータ１６８は、第２のグループ鍵１４２

または第２のグループ鍵１４２の生成に対応するタイムスタンプに基づいて生成されるハッシュ値を含み得る。方法１０００は、データリンクグループの第２のデバイスから第２の候補グループ鍵と第２の鍵インジケータとを含む第２の告知メッセージを受信することを含み得る。方法１０００は、鍵インジケータと第２の鍵インジケータとの比較に基づいて伝搬のために候補グループ鍵を選択することをさらに含み得る。

【０１８９】

[0201]いくつかの実装形態では、第１のデバイスは、第１のデバイスがデータリンクグループの発信者であることに基づいて、第１のデバイスがデータリンクグループの他のデバイスの各デバイスよりも多くのデバイスに関連することに基づいて、第１のデバイスが、データリンクグループの他のデバイスの各デバイスよりも長い時間をデータリンクグループ中で過ごしたことに基づいて、第１のデバイスに関連するデバイスの数に基づいて、データリンクグループのトポロジーに基づいて、第１のデバイスがデータリンクグループ中に含まれた持続時間に基づいて、データリンクグループ内の第１のデバイスのランクに基づいて、第１のデバイスのバッテリーレベルに基づいて、またはそれらの組合せで、鍵生成器デバイスとして動作することを決定する。たとえば、第１のデバイス１０４は、図１を参照しながら説明されるように、１つまたは複数の基準に基づいて鍵生成器デバイスとして動作することを決定し得る。

【０１９０】

[0202]図１１を参照すると、ワイヤレスネットワークのデバイスにおける動作の方法１１００の第５の実装形態が示されている。ワイヤレスネットワークは、複数のデータリンクグループを含み得る。方法１１００は、デバイス１０４～１１０のいずれか、図２のデバイス２０２、図３を参照しながら説明されるデバイスのいずれか、または図４のデバイス４０２、４０４のいずれかにおいて実行され得る。

【０１９１】

[0203]方法１１００は、１１０２において、データリンクグループの第２のデバイスにおいて、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ことを含む。たとえば、第１の通信チャネルは、図３のＮＡＮ通信チャネル３０２またはデータリンクグループチャネル３０４を含むか、またはそれに対応し得る。ページングウィンドウは、図３のページングウィンドウ３３２、３４２、３５２、３６２のうちの１つを含むか、またはそれに対応し得る。

【０１９２】

[0204]方法１１００は、１１０４において、ページングウィンドウ中にデータリンクグループの第１のデバイスから第２のデバイスにおいて告知メッセージを受信すること、告知メッセージは、候補グループ鍵の利用可能性を示す、ここで、告知メッセージは、マルチキャストメッセージを含む、を含む。たとえば、告知メッセージは、図１の告知メッセージ１６０または告知メッセージ１７０を含むか、またはそれに対応し得る。ページングウィンドウは、図３のグループ送信ウィンドウ３２０、３２２、３２４、３２６などのグループ送信ウィンドウの一部であり得る。

【０１９３】

[0205]いくつかの実装形態では、第２のデバイスは、候補グループ鍵を取得し得る。第２のデバイスは、ページングウィンドウ中に告知メッセージを受信したことに応答して第１のデバイスにトリガメッセージを送信することによって、およびデータウィンドウ中に第１のデバイスから候補グループ鍵を受信することによって候補グループ鍵を取得し得る。図１を参照すると、トリガメッセージは、図１のトリガメッセージ１６７を含むか、またはそれに対応し得る。

【０１９４】

[0206]他の実装形態では、第２のデバイスは、告知メッセージを受信したことに応答して第１のデバイスにトリガメッセージを送信し得る。たとえば、図１を参照すると、第２のデバイス１０６は、告知メッセージ１６０を受信したことに応答して第１のデバイス１０４にトリガメッセージ１６７を送信し得る。告知メッセージは、図１の鍵インジケータ

１６８などの鍵インジケータを含み得る。鍵インジケータは、タイムスタンプ、ハッシュ値、またはその両方を含み得る。

【０１９５】

[0207]いくつかの実装形態では、第２のデバイスは、ページングウィンドウ中に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し得る。第２の告知メッセージは、第２のタイムスタンプを含み得、第２のグループ鍵の生成を示し得る。第２のデバイスは、告知メッセージの第１のタイムスタンプが第２のタイムスタンプよりも前のものであることに基づいて第１のデバイスにトリガメッセージを送信し得る。第２のデバイスは、トリガメッセージを送信したことに応答して、第１のデバイスから候補グループ鍵を受信し得る。

【０１９６】

[0208]他の実装形態では、第２のデバイスは、第１のデバイスがデータリンクグループとの関連付けを解除すると決定したことに応答して第２のグループ鍵を生成し得る。たとえば、図１を参照すると、第２のデバイス１０６は、第１のデバイス１０４がデータリンクグループとの関連付けを解除すると決定したことに応答してグループ鍵を生成し得る。

【０１９７】

[0209]いくつかの実装形態では、方法１１００は、カウンタを更新すること、カウンタは、前のグループ鍵の満了に関係する、を含み得る。たとえば、カウンタは、図２のカウンタ２０４を含むか、またはそれに対応し得る。方法１１００はまた、カウンタが、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特定の値に達するより前に告知メッセージを受信したことに応答してカウンタを更新することを停止することを含み得る。

【０１９８】

[0210]いくつかの実装形態では、方法１１００は、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を含み得る。たとえば、第２のデバイス１０６は、図１を参照しながら説明されるように、告知メッセージ１６０中の鍵インジケータ１６８を識別し得る。方法１１００はまた、ページングウィンドウ中に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を含み得る。第２の告知メッセージは、第２の鍵インジケータを含み得、第２の候補グループ鍵の生成を示し得る。方法１１００は、第２の鍵インジケータよりも高い優先度を有する告知メッセージの第１の鍵インジケータに基づいて第１のデバイスにトリガメッセージを送信することを含み得る。たとえば、第２のデバイス１０６は、告知メッセージ１６０の鍵インジケータ１６８に基づいて第１のデバイス１０４にトリガメッセージ１６７を送り得る。方法１１００は、トリガメッセージを送信したことに応答して第１のデバイスから候補グループ鍵を受信することをさらに含み得る。

【０１９９】

[0211]いくつかの実装形態では、方法１１００は、告知メッセージを受信するより前に、第２の候補グループ鍵の生成を開始することを含み得る。たとえば、第２のデバイス１０６は、図１を参照しながら説明されるように、第１のデバイス１０４から告知メッセージ１６０を受信するより前に候補グループ鍵を生成し得る。方法１１００はまた、告知メッセージを受信したことに応答して、第２の候補グループ鍵の生成を停止することを含み得る。たとえば、第２のデバイス１０６は、第１のデバイス１０４から告知メッセージ１６０などの告知メッセージを受信したことに応答して、候補グループ鍵の生成を停止するかまたは候補グループ鍵を抑制し得る。

【０２００】

[0212]いくつかの実装形態では、方法１１００は、告知メッセージを受信したことに応答して、データリンクグループのデバイスに告知メッセージを再送信することを含み得る。たとえば、第２のデバイス１０６は、第１のデバイス１０４から告知メッセージ１６０を受信したことに応答して第３のデバイス１０８と第４のデバイス１１０とに告知メッセージ１７０を送信し得る。

【０２０１】

[0213]いくつかの実装形態では、方法１１００は、告知メッセージを受信したことに応答して、第２のデバイスが第１のデバイスに関連するのかどうかを決定することを含み得る。方法１１００はまた、第１のデバイス１０４が第２のデバイス１０６に関連するという決定に応答して、第１のデバイス１０４に候補グループ鍵を要求することを含み得る。たとえば、第２のデバイス１０６は、図１を参照しながら説明されるように、第２のデバイス１０６が第１のデバイス１０４に関連すると決定し得る。

【０２０２】

[0214]いくつかの実装形態では、方法１１００は、告知メッセージを受信したことに応答して、第２のデバイスが第１のデバイスに関連するのかどうかを決定することを含み得る。方法１１００はまた、第２のデバイスが第１のデバイスに関連しないという決定に応答して、候補グループ鍵を受信し、第２のデバイスに関連する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を含み得る。たとえば、第４のデバイス１１０は、図１を参照しながら説明されるように、第４のデバイス１１０が第１のデバイス１０４に関連しないと決定し得る。第４のデバイス１１０は、第２のグループ鍵１４２がページングメッセージ１６５または告知メッセージ１７０をベースされたものとして第２のデバイス１０６を識別し得る。第３のデバイスは、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得る。時間期間は、告知メッセージが受信された後に開始し、アクティブグループ鍵の満了の前の所定の時間に終了し得る。方法１１００は、第３のデバイスに候補グループ鍵を要求することを含み得る。方法１１００は、アクティブグループ鍵の満了より前に第３のデバイスから候補グループ鍵を受信することをさらに含み得る。たとえば、第４のデバイス１１０は、トリガメッセージ１６７を送信することによって第２のグループ鍵１４２を要求し得、第２のグループ鍵１４２を含む鍵配信メッセージ１８０を受信し得る。

【０２０３】

[0215]いくつかの実装形態では、方法１１００は、第２のデバイスが第１のデバイスに関連しないという決定に応答して第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を含み得る。特定の実装形態では、セキュリティ関連付けは、図１のペアワイズ鍵１４６などのペアワイズ鍵を確立する。

【０２０４】

[0216]方法１１００はまた、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を含み得る。方法１１００は、第２のデバイスにおいて候補グループ鍵を生成するためにペアワイズ鍵に基づいて符号化された候補グループ鍵を復号することを含み得る。たとえば、ペアワイズ鍵は、図１のペアワイズ鍵１４６を含むか、またはそれに対応し得る。方法１１００は、メモリに候補グループ鍵を記憶することをさらに含み得る。たとえば、メモリは、図２の鍵記憶装置２０８を含むか、またはそれに対応し得る。

【０２０５】

[0217]いくつかの実装形態では、方法１１００は、第２のデバイスが第１のデバイスに関連しないという決定に応答して、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を含み得る。方法１１００はまた、所定の時間の前に、データリンクグループの少なくとも１つのデバイスに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を含み得る。方法１１００は、マルチキャスト要求に応答してデータリンクグループの第３のデバイスから候補グループ鍵を受信することをさらに含み得る。

【０２０６】

[0218]図１２を参照すると、ワイヤレスネットワークのデバイスにおける動作の方法１２００の第６の実装形態が示されている。ワイヤレスネットワークは、複数のデータリンクグループを含み得る。方法１２００は、図１のデバイス１０４～１１０のいずれか、図２のデバイス２０２、図３を参照しながら説明されるデバイスのいずれか、または図４のデバイス４０２、４０４のいずれかにおいて実行され得る。

【０２０７】

[0219]方法１２００は、１２０２において、データリンクグループの第２のデバイスにおいて、データリンクグループに対応する発見ウィンドウ中に第１の通信チャネルを監視することを含む。たとえば、第１の通信チャネルは、図３のＮＡＮ通信チャネル３０２またはデータリンクグループチャネル３０４を含むか、またはそれに対応し得る。発見ウィンドウは、図３の第１の発見ウィンドウ３１０と第２の発見ウィンドウ３１２とを含むか、またはそれに対応し得る。図１を参照すると、ワイヤレスネットワーク１０２（たとえば、ＮＡＮ）のデータリンクグループの第２のデバイス１０６は、データリンクグループの発見ウィンドウ中にデータリンクグループに対応するワイヤレスチャネルを監視し得る。

【０２０８】

[0220]方法１２００は、１２０４において、発見ウィンドウ中にデータリンクグループの第１のデバイスから第２のデバイスにおいて告知メッセージを受信すること、ここで、告知メッセージは、候補グループ鍵の利用可能性を示す、およびここで、告知メッセージは、マルチキャストメッセージを含む、を含む。たとえば、告知メッセージは、図１の告知メッセージ１６０、告知メッセージ１７０、または図５の告知メッセージ５１０を含むか、またはそれに対応し得る。

【０２０９】

[0221]特定の実装形態では、第２のデバイスは、図２のカウンタ２０４に基づくカウントダウンなどのカウントダウンの満了に応答して第１のデバイスに関連付け要求を送信し得る。たとえば、第４のデバイス１１０は、第１のデバイス１０４に関連付け要求１７５を送信し得る。

【０２１０】

[0222]いくつかの実装形態では、第２のデバイスは、データリンクグループのページングウィンドウ中に第１のデバイスからページングメッセージを受信したことに応答して第１のデバイスにトリガメッセージを送信し得る。第２のデバイスは、トリガメッセージに応答して第２のデバイスにおいて第１のデバイスから候補グループ鍵を受信し得る。たとえば、第２のデバイス１０６は、図１を参照しながら説明されるように、第１のデバイスからページングメッセージ１６５を受信したことに応答して第１のデバイス１０４にトリガメッセージ１６７を送信し得る。第２のデバイス１０６は、第１のデバイス１０４から第２のグループ鍵１４２を受信し得る。

【０２１１】

[0223]他の実装形態では、第２のデバイスは、告知メッセージを受信したことに応答して第１のデバイスに関連付け要求を送信し得る。たとえば、図１を参照すると、第２のデバイス１０６が第１のデバイス１０４に関連しないとき、告知メッセージ１６０を受信したことに応答して第１のデバイス１０４に関連付け要求１７５を送信し得る。

【０２１２】

[0224]特定の実装形態では、第２のデバイスは、第１のデバイスから関連付け応答を受信したことに応答して第１のデバイスに関連し得る。図１の関連付け応答１７６などの関連付け応答は、第１のデバイスが関連するために利用可能であることを示し得る。第２のデバイスは、第２のデバイスにおいて第１のデバイスから候補グループ鍵を受信し得る。第２のデバイスは、第１のデバイスから図１の関連付け拒絶１７８などの関連付け拒絶を受信したことに応答して第１のデバイスに第２の関連付け要求を送信し得る。

【０２１３】

[0225]いくつかの実装形態では、告知メッセージは、第１の通信チャネルを介して受信され得る。たとえば、第１の通信チャネルは、図３のＮＡＮ通信チャネル３０２を含み得る。方法１２００はまた、第２の通信チャネルのページングウィンドウ中に第１のデバイスからページングメッセージを受信したことに応答して、第２の通信チャネルを介して、第１のデバイスにトリガメッセージを送信することを含み得る。たとえば、第２の通信チャネルは、図３のデータリンクグループチャネル３０４を含み得る。ページングメッセージは、図１のページングメッセージ１６５またはページングメッセージ１９０を含むか、

またはそれに対応し得る。方法１２００は、第２のデバイスにおいて第１のデバイスから候補グループ鍵を受信することと、完全性グループ鍵に基づいて候補グループ鍵を検証することとをさらに含み得る。

【０２１４】

[0226]いくつかの実装形態では、方法１２００は、告知メッセージを受信した後に、カウントダウンを開始することを含み得る。方法１２００はまた、カウントダウンの満了に応答して、第２のデバイスによって、第２のデバイスが候補グループ鍵を受信しなかったと決定することを含み得る。方法１２００は、第２のデバイスがカウントダウンの満了までに候補グループ鍵を受信しなかったと決定したことに応答して第１のデバイスに関連付け要求を送信することをさらに含み得る。たとえば、第４のデバイス１１０は、図１を参照しながら説明されるように、それが第２のグループ鍵１４２を受信しなかったと決定し得、第１のデバイス１０４に関連付け要求１７５を送信し得る。

【０２１５】

[0227]いくつかの実装形態では、方法１２００は、第１の鍵インジケータを含む告知メッセージを受信するより前に、第２のデバイスにおいて第２の候補グループ鍵と第２の候補グループ鍵の第２の鍵インジケータとを生成することを含み得る。たとえば、第１のデバイス１０４は、図１を参照しながら説明されるように、ワイヤレスネットワーク１０２の別のデバイスから告知メッセージを受信するより前に第２のグループ鍵１４２と鍵インジケータ１６８とを生成し得る。方法１２００はまた、第２の鍵インジケータが第１の鍵インジケータよりも高い優先度を示すことに基づいて伝搬のために第２の候補グループ鍵を選択することを含み得る。たとえば、第１のデバイスは、図１を参照しながら説明されるように、告知メッセージ１６０中に含まれる鍵インジケータ１６８に基づいて伝搬のために第２のグループ鍵１４２を選択し得る。方法１２００は、告知メッセージを受信した後に、第２の通信チャネルを介してページングウィンドウ中にデータリンクグループの第４のデバイスにページングメッセージを送信すること、第４のデバイスは、第２のデバイスに関連する、をさらに含み得る。ページングメッセージは、第２の候補グループ鍵が第２のデバイスから入手可能であることを示し得る。たとえば、第１のデバイス１０４は、図１を参照しながら説明されるように、第４のデバイス１１０にページングメッセージ１６５を送信し得る。

【０２１６】

[0228]いくつかの実装形態では、方法１２００は、１つまたは複数の条件に基づいて第２の鍵インジケータが第１の鍵インジケータよりも高い優先度を有すると決定することを含み得る。１つまたは複数の条件は、第２の鍵インジケータがより高い優先度の媒体アクセス制御（ＭＡＣ）アドレスを示すとき、第２の鍵インジケータがより前のタイムスタンプを示すとき、または第２の鍵インジケータがより高い優先度のハッシュ値を示すときを含み得る。たとえば、第２のデバイス１０６は、図１を参照しながら説明されるように、ＭＡＣアドレス、タイムスタンプ、またはハッシュ値に基づいて（第２のデバイス１０６によって生成された候補グループ鍵に対応する）第２の鍵インジケータが告知メッセージ１６０中に含まれる鍵インジケータ１６８よりも高い優先度を有すると決定し得る。

【０２１７】

[0229]図７の方法７００、図８の方法８００、図９の方法９００、図１０の方法１０００、図１１の方法１１００、図１２の方法１２００、またはそれらの組合せにより、データリンクグループのデバイスへのグループ鍵の配布が可能になる。候補グループ鍵は、データリンクグループを含むＮＡＮまたはメッシュネットワーク内での鍵関連のトラフィックとオーバーヘッドとが低減された状態で配布され得る。たとえば、鍵関連のトラフィックは、データリンクグループのデバイスが起動しているときにページングウィンドウまたは発見ウィンドウ中にグループ鍵告知メッセージなどの告知メッセージを送ることによって低減され得る。別の例として、候補グループ鍵（たとえば、潜在的な「次の」アクティブグループ鍵）を暗号化するためにアクティブ配布鍵が使用され得、暗号化された候補グループ鍵が、データリンクグループの１つまたは複数のデバイスにマルチキャストメッセ

ージとして送られ得る。マルチキャストメッセージとして候補グループ鍵を送ることによって、候補グループ鍵は、データリンクグループの２つのデバイス間でセキュリティ関連付け、Ｐ２Ｐ通信、またはそれらの組合せを実行することなしにデータリンクグループの１つまたは複数のデバイスに配布され得る。

【０２１８】

[0230]図７の方法７００、図８の方法８００、図９の方法９００、図１０の方法１０００、図１１の方法１１００、図１２の方法１２００、またはそれらの組合せに示すプロセスは、中央処理ユニット（ＣＰＵ）、コントローラ、フィールドプログラマブルゲートアレイ（ＦＰＧＡ）デバイス、特定用途向け集積回路（ＡＳＩＣ）、別のハードウェアデバイス、ファームウェアデバイス、またはそれらの任意の組合せなどの処理ユニットによって制御され得る。一例として、図７の方法７００、図８の方法８００、図９の方法９００、図１０の方法１０００、図１１の方法１１００、図１２の方法１２００、またはそれらの組合せは、告知メッセージを送信すること、グループ鍵を配布すること、またはそれらの組合せを行うための命令を実行する１つまたは複数のプロセッサによって実行され得る。さらに、図７～図１２の方法のうちの１つの第１の部分は、図７～図１２の方法の別の１つの少なくとも第２の部分と組み合わされ得る。たとえば、図７の方法７００の第１の部分は、図８の方法８００、図９の方法９００、図１０の方法１０００、図１１の方法１１００、図１２の方法１２００、またはそれらの組合せのうちの１つの第２の部分と組み合わされ得る。

【０２１９】

[0231]図１３を参照すると、ワイヤレス通信デバイスの特定の例示的な実装形態が示され、全体的に１３００と称される。デバイス１３００は、メモリ１３３２に結合されたデジタル信号プロセッサなどのプロセッサ１３１０を含む。デバイス１３００またはそれの構成要素は、図１のデバイス１０４～１１０、図２のデバイス２０２、図３を参照しながら説明されるデバイス、図４のデバイス４０２、４０４またはそれらの構成要素に対応し得る。

【０２２０】

[0232]非一時的コンピュータ可読媒体などのメモリ１３３２は、１つまたは複数の鍵１３６０と命令１３６８とを含み得る。命令は、プロセッサ１３１０によって実行可能であり得る。たとえば、メモリ１３３２は、図２の鍵記憶装置２０８を含むか、またはそれに対応し得る。１つまたは複数の鍵１３６０は、デバイス１３００を含むデータリンクグループのグループ鍵１３６２を含み得る。たとえば、グループ鍵１３６２は、図１の第１のグループ鍵１３２、第２のグループ鍵１４２または図２のグループ鍵２１４を含むか、またはそれに対応し得る。随意に、１つまたは複数の鍵１３６０は、データリンクグループの配布鍵１３６４を含み得る。たとえば、配布鍵１３６４は、図１の第１の配布鍵１３４または第２の配布鍵１４４を含むか、またはそれに対応し得る。いくつかの実装形態では、１つまたは複数の鍵１３６０は、アクティブグループ鍵および候補グループ鍵などの複数のグループ鍵を含み得る。さらに、１つまたは複数の鍵１３６０は、アクティブ配布鍵および候補配布鍵などの複数の配布鍵を含み得る。

【０２２１】

[0233]プロセッサ１３１０は、鍵論理１３１２とメッセージ論理１３１４とを含み得る。鍵論理１３１２は、図１の鍵論理１１２、カウンタ２０４、図２の鍵生成器２０６、またはそれらの組合せを含むか、またはそれに対応し得る。メッセージ論理１３１４は、図１のメッセージ論理１１４を含むか、またはそれに対応し得る。メッセージ論理１３１４は、図１の告知メッセージ１６０または告知メッセージ１７０などの告知メッセージ１３１６を生成するように構成され得る。告知メッセージ１３１６は、グループ鍵１３６２に対応し得る（たとえば、それを含み得る）。

【０２２２】

[0234]プロセッサ１３１０は、メモリ１３３２中に記憶されたソフトウェア（たとえば、１つまたは複数の命令１３６８のプログラム）を実行するように構成され得る。たとえ

ば、プロセッサ１３１０は、図７の方法７００、図８の方法８００、図９の方法９００、図１０の方法１０００、図１１の方法１１００、図１２の方法１２００、またはそれらの組合せに従って動作するように構成され得る。例示のために、プロセッサ１３１０は、データリンクグループの取得されたグループ鍵１３６２を識別することと、ページングウィンドウ中にデータリンクグループの１つまたは複数のデバイスへの告知メッセージ１３１６の送信を開始することとをプロセッサ１３１０に行わせる命令１３６８を実行するように構成され得る。告知メッセージ１３１６は、グループ鍵１３６２に対応し得、告知メッセージ１３１６がグループ鍵告知メッセージであることを示すマルチキャストメッセージとして送信され得る。

【０２２３】

[0235]別の例として、プロセッサ１３１０は、データリンクグループに対応するグループ鍵１３６２と配布鍵１３６４とを生成することと、アクティブ配布鍵などの第２の配布鍵（図示せず）を使用してグループ鍵１３６２と配布鍵１３６４とを符号化することとをプロセッサ１３１０に行わせる命令１３６８を実行するように構成され得る。第２の配布鍵は、データリンクグループのアクティブグループ鍵に対応し得る。命令１３６８は、データリンクグループの１つまたは複数のデバイスへの暗号化されたグループ鍵と暗号化された配布鍵との送信を開始することをプロセッサにさらに行なわせ得る。

【０２２４】

[0236]図１３に、同じく、プロセッサ１３１０とディスプレイ１３２８とに結合されたディスプレイコントローラ１３２６を示す。コーダ／デコーダ（コーデック）１３３４も、プロセッサ１３１０に結合され得る。スピーカー１３３６とマイクロフォン１３３８とが、コーデック１３３４に結合され得る。図１３はまた、ワイヤレスインターフェース１３４０がプロセッサ１３１０とアンテナ１３４２とに結合され得ることを示す。たとえば、ワイヤレスインターフェース１３４０は、トランシーバ１３４１を介してアンテナ１３４２に結合され得る。トランシーバ１３４１は、送信機、受信機、またはその両方を含み得る。トランシーバ１３４１は、メッセージ論理１３１４によって生成された１つまたは複数のメッセージを送信することと、データリンクグループのデバイスなどの他のデバイスによってデバイス１３００に送信された１つまたは複数のメッセージを受信することとを行うように構成され得る。

【０２２５】

[0237]いくつかの実装形態では、プロセッサ１３１０、ディスプレイコントローラ１３２６、メモリ１３３２、コーデック１３３４、ワイヤレスインターフェース１３４０、およびトランシーバ１３４１は、システムインパッケージまたはシステムオンチップデバイス１３２２中に含まれる。特定の実装形態では、入力デバイス１３３０と電源１３４４とが、システムオンチップデバイス１３２２に結合される。さらに、別の特定の実装形態では、図１３に示すように、ディスプレイ１３２８、入力デバイス１３３０、スピーカー１３３６、マイクロフォン１３８、アンテナ１３４２、および電源１３４４は、システムオンチップデバイス１３２２の外部にある。ただし、ディスプレイ１３２８、入力デバイス１３３０、スピーカー１３３６、マイクロフォン１３３８、アンテナ１３４２、および電源１３４４の各々は、インターフェースまたはコントローラなど、システムオンチップデバイス１３２２の構成要素に結合され得る。

【０２２６】

[0238]図１～図１３の説明される実装形態のうちの１つまたは複数に関連して、第１の装置は、データリンクグループの第１のデバイスにおいてグループ鍵を取得するための手段を含む。たとえば、グループ鍵を取得するための手段は、図１の鍵論理１１２、図２の鍵生成器２０６、受信機２１０、図１３の鍵論理１３１２、ワイヤレスインターフェース１３４０、トランシーバ１３４１、命令１３６８を実行するようにプログラムされたプロセッサ１３１０、グループ鍵を取得するための１つまたは複数の他の構造、デバイス、回路、モジュール、または命令、あるいはそれらの任意の組合せを含むか、またはそれに対応し得る。グループ鍵は、図１の第１のグループ鍵１３２、図１の第２のグループ鍵１４

２、図２のグループ鍵２１４、または図３～図５を参照しながら説明されるグループ鍵のいずれかを含むか、またはそれに対応し得る。

【０２２７】

[0239]第１の装置はまた、ページングウィンドウ中にデータリンクグループの１つまたは複数のデバイスにグループ鍵に対応する告知メッセージを送信するための手段を含む。告知メッセージは、グループ鍵に対応し得、告知メッセージがグループ鍵告知メッセージであることを示すマルチキャストメッセージとして送信され得る。たとえば、告知メッセージを送信するための手段は、図１のメッセージ論理１１４、図２の送信機２１２、図１３のワイヤレスインターフェース１３４０、トランシーバ１３４１、アンテナ１３４２、命令１３６８を実行するようにプログラムされたプロセッサ１３１０、告知メッセージを送信するための１つまたは複数の他の構造、デバイス、回路、モジュール、または命令、あるいはそれらの任意の組合せを含むか、またはそれに対応し得る。

【０２２８】

[0240]１つまたは複数の説明される実装形態に関連して、第２の装置は、データリンクグループに対応するグループ鍵と配布鍵とを生成するための手段を含む。たとえば、生成するための手段は、図１の鍵論理１１２、図２の鍵生成器２０６、図１３の鍵論理１３１２、命令１３６８を実行するようにプログラムされたプロセッサ１３１０、グループ鍵と配布鍵とを生成するための１つまたは複数の他の構造、デバイス、回路、モジュール、または命令、あるいはそれらの任意の組合せを含むか、またはそれに対応し得る。

【０２２９】

[0241]第２の装置は、第２の配布鍵を使用してグループ鍵と配布鍵とを符号化するための手段を含む。第２の配布鍵は、データリンクグループのアクティブグループ鍵に対応し得る。たとえば、符号化するための手段は、図１のメッセージ論理１１４、エンコーダ／デコーダ１１８、図１３のメッセージ論理１３１４、命令１３６８を実行するようにプログラムされたプロセッサ１３１０、グループ鍵と配布鍵とを符号化するための１つまたは複数の他の構造、デバイス、回路、モジュール、または命令、あるいはそれらの任意の組合せを含むか、またはそれに対応し得る。

【０２３０】

[0242]第２の装置はまた、データリンクグループの１つまたは複数のデバイスに符号化されたグループ鍵と符号化された配布鍵とを送信するための手段を含む。たとえば、送信するための手段は、図１のメッセージ論理１１４、ワイヤレスデバイス１３４０、図２の送信機２１２、図１３のトランシーバ１３４１、アンテナ１３４２、命令１３６８を実行するようにプログラムされたプロセッサ１３１０、符号化されたグループ鍵と符号化された配布鍵とを送信するための１つまたは複数の他の構造、デバイス、回路、モジュール、または命令、あるいはそれらの任意の組合せを含むか、またはそれに対応し得る。

【０２３１】

[0243]１つまたは複数の説明する実装形態に関連して、第３の装置は、データリンクグループの第１のデバイスにおいてグループ鍵を取得するための手段を含む。たとえば、取得するための手段は、図１の鍵論理１１２、図１３の鍵論理１３１２、命令１３６８を実行するようにプログラムされたプロセッサ１３１０、グループ鍵を取得するための１つまたは複数の他の構造、デバイス、回路、モジュール、または命令、あるいはそれらの任意の組合せを含むか、またはそれに対応し得る。

【０２３２】

[0244]第３の装置は、データリンクグループの第１のデバイスからデバイスに送信するための手段、告知メッセージはグループ鍵に対応する、を含む。たとえば、符号化するための手段は、図１のメッセージ論理１１４、第１のデバイス１０４、図１３のメッセージ論理１３１４、ワイヤレスインターフェース１３４０、トランシーバ１３４１、アンテナ１３４２、命令１３６８を実行するようにプログラムされたプロセッサ１３１０、告知メッセージを送信するための１つまたは複数の他の構造、デバイス、回路、モジュール、または命令、あるいはそれらの任意の組合せを含むか、またはそれに対応し得る。告知メッ

セージは、マルチキャストメッセージを含み得、ＮＡＮ通信チャネルなどの通信チャネルを介して、またはデータリンクグループチャネルを介してページングウィンドウ中に送信され得る。

【０２３３】

[0245]１つまたは複数の説明する実装形態に関連して、第４の装置は、データリンクグループの第２のデバイスにおいて、発見ウィンドウ中に第１のワイヤレスチャネルを監視するための手段を含む。たとえば、監視するための手段は、図１のメッセージ論理１１４、第１のデバイス１０４、図１３のメッセージ論理１３１４、ワイヤレスインターフェース１３４０、トランシーバ１３４１、アンテナ１３４２、命令１３６８を実行するようにプログラムされたプロセッサ１３１０、ワイヤレスチャネルを監視するための１つまたは複数の他の構造、デバイス、回路、モジュール、または命令、あるいはそれらの任意の組合せを含むか、またはそれに対応し得る。第１のワイヤレスチャネルは、図３のＮＡＮ通信チャネル３０２またはデータリンクグループチャネル３０４を含むか、またはそれに対応し得る。

【０２３４】

[0246]第４の装置は、発見ウィンドウ中にデータリンクグループの第１のデバイスから第２のデバイスにおいて告知メッセージを受信するための手段を含む。たとえば、受信するための手段は、図１のメッセージ論理１１４、第１のデバイス１０４、図１３のメッセージ論理１３１４、ワイヤレスインターフェース１３４０、トランシーバ１３４１、アンテナ１３４２、命令１３６８を実行するようにプログラムされたプロセッサ１３１０、告知メッセージを受信するための１つまたは複数の他の構造、デバイス、回路、モジュール、または命令、あるいはそれらの任意の組合せを含むか、またはそれに対応し得る。

【０２３５】

[0247]１つまたは複数の説明される実装形態に関連して、第５の装置は、ＮＡＮのデータリンクグループの第２のデバイスにおいて、データリンクグループのページングウィンドウ中にデータリンクグループに対応するワイヤレスチャネルを監視するための手段を含む。たとえば、監視するための手段は、図１のメッセージ論理１１４、図１３のメッセージ論理１３１４、ワイヤレスインターフェース１３４０、トランシーバ１３４１、アンテナ１３４２、命令１３６８を実行するようにプログラムされたプロセッサ１３１０、ワイヤレスチャネルを監視するための１つまたは複数の他の構造、デバイス、回路、モジュール、または命令、あるいはそれらの任意の組合せを含むか、またはそれに対応し得る。

【０２３６】

[0248]第５の装置は、ページングウィンドウ中にデータリンクグループの第１のデバイスから第２のデバイスにおいて告知メッセージを受信するための手段、告知メッセージは、グループ鍵の生成を示す、を含む。たとえば、受信するための手段は、図１のメッセージ論理１１４、第１のデバイス１０４、図１３のメッセージ論理１３１４、ワイヤレスインターフェース１３４０、トランシーバ１３４１、アンテナ１３４２、命令１３６８を実行するようにプログラムされたプロセッサ１３１０、告知メッセージを受信するための１つまたは複数の他の構造、デバイス、回路、モジュール、または命令、あるいはそれらの任意の組合せを含むか、またはそれに対応し得る。告知メッセージは、マルチキャストメッセージを含み得る。

【０２３７】

[0249]開示される実装形態のうちの１つまたは複数は、通信デバイス、固定ロケーションデータユニット、モバイルロケーションデータユニット、モバイル電話、セルラー電話、衛星電話、コンピュータ、タブレット、ポータブルコンピュータ、ディスプレイデバイス、メディアプレーヤ、またはデスクトップコンピュータを含み得る、デバイス１３００などのシステム、デバイスまたは装置において実装され得る。代替または追加として、デバイス１３００は、セットトップボックス、エンターテインメントユニット、ナビゲーションデバイス、携帯情報端末（ＰＤＡ）、モニタ、コンピュータモニタ、テレビジョン、チューナー、ラジオ、衛星ラジオ、音楽プレーヤ、デジタル音楽プレーヤ、ポータブル音

楽プレーヤ、ビデオプレーヤ、デジタルビデオプレーヤ、デジタルビデオディスク（ＤＶＤ）プレーヤ、ポータブルデジタルビデオプレーヤ、衛星、車両または車両内に組み込まれたデバイス、プロセッサを含むか、または、データもしくはコンピュータ命令を記憶するかもしくは取り出す任意の他のデバイス、あるいはそれらの組合せを含み得る。別の例示的な、非限定的な例として、システム、デバイス、または装置は、ハンドヘルドパーソナル通信システム（ＰＣＳ）ユニットなどのリモートユニット、全地球測位システム（ＧＰＳ）対応デバイスなどのポータブルデータユニット、メーター読取り機器、あるいは、プロセッサを含むか、または、データもしくはコンピュータ命令を記憶するかもしくは取り出す任意の他のデバイス、あるいはそれらの任意の組合せを含み得る。

【０２３８】

[0250]図１～図１３の１つまたは複数は、本開示の教示によるシステム、装置、方法、またはこれらの組合せを示し得るが、本開示は、これらの示されたシステム、装置、方法、またはこれらの組合せに限定されない。本明細書で示され、または説明される図１～図１３のいずれかの１つまたは複数の機能または構成要素は、図１～図１３の別の機能または構成要素の１つまたは複数の他の部分と組み合わされ得る。したがって、本明細書で説明されるいずれの単一の実装形態も限定的と解釈されるべきではなく、本開示の実装形態は、本開示の教示から逸脱することなく適切に組み合わされ得る。

【０２３９】

[0251]さらに、本明細書で開示された実装形態に関連して説明された様々な例示的な論理ブロック、構成、モジュール、回路、およびアルゴリズムステップは、電子ハードウェア、プロセッサによって実行されるコンピュータソフトウェア、または両方の組合せとして実装され得ることを当業者は諒解されよう。様々な例示的な構成要素、ブロック、構成、モジュール、回路、およびステップについて、上記では概してそれらの機能に関して説明した。そのような機能がハードウェアとして実装されるか、プロセッサ実行可能命令として実装されるかは、具体的な適用例および全体的なシステムに課された設計制約に依存する。当業者は、説明した機能を具体的な適用例ごとに様々な方法で実装し得るが、そのような実装決定は、本開示の範囲からの逸脱を生じるものと解釈すべきではない。

【０２４０】

[0252]本明細書で開示した実装形態に関して説明される方法またはアルゴリズムのステップは、直接ハードウェアに含まれ、プロセッサによって実行されるソフトウェアモジュールに含まれ、またはその２つの組合せであり得る。ソフトウェアモジュールは、ランダムアクセスメモリ（ＲＡＭ）、フラッシュメモリ、読取り専用メモリ（ＲＯＭ）、プログラマブル読取り専用メモリ（ＰＲＯＭ）、消去可能プログラマブル読取り専用メモリ（ＥＰＲＯＭ）、電気消去可能プログラマブル読取り専用メモリ（ＥＥＰＲＯＭ（登録商標））、レジスタ、ハードディスク、リムーバブルディスク、コンパクトディスク読取り専用メモリ（ＣＤ－ＲＯＭ）、または当技術分野で知られている任意の他の形態の非一時的（ｎｏｎ－ｔｒａｎｓｉｅｎｔ）（たとえば、非一時的（ｎｏｎ－ｔｒａｎｓｉｔｏｒｙ））記憶媒体中に存在し得る。例示的な記憶媒体は、プロセッサが記憶媒体から情報を読み取り、記憶媒体に情報を書き込むことができるようにプロセッサに結合される。代替的に、記憶媒体はプロセッサと一体化され得る。プロセッサおよび記憶媒体は特定用途向け集積回路（ＡＳＩＣ）中に存在し得る。ＡＳＩＣは、コンピューティングデバイスまたはユーザ端末中に存在し得る。代替的に、プロセッサおよび記憶媒体は、コンピューティングデバイスまたはユーザ端末内の個別の構成要素として存在し得る。

【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。

【図１】

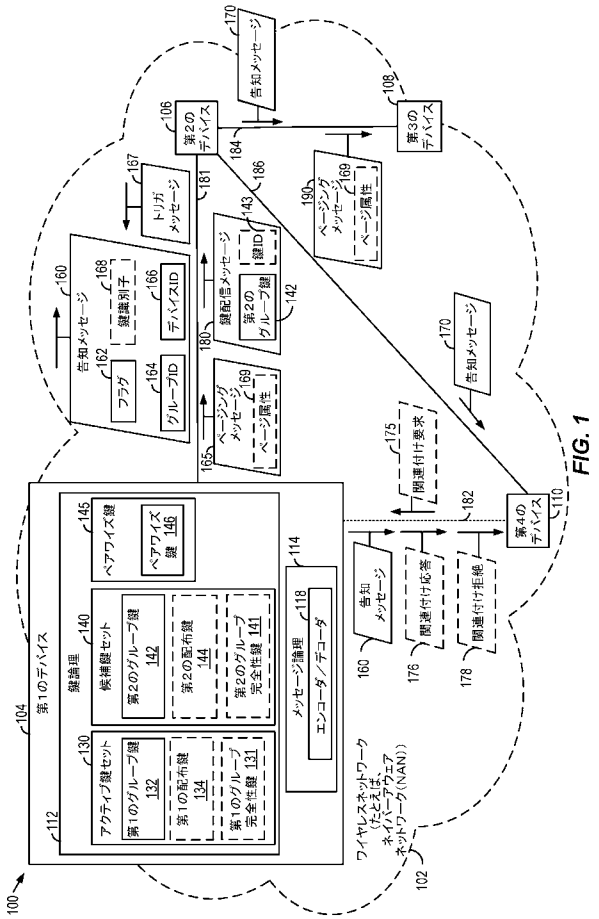

FIG. 1

【図２】

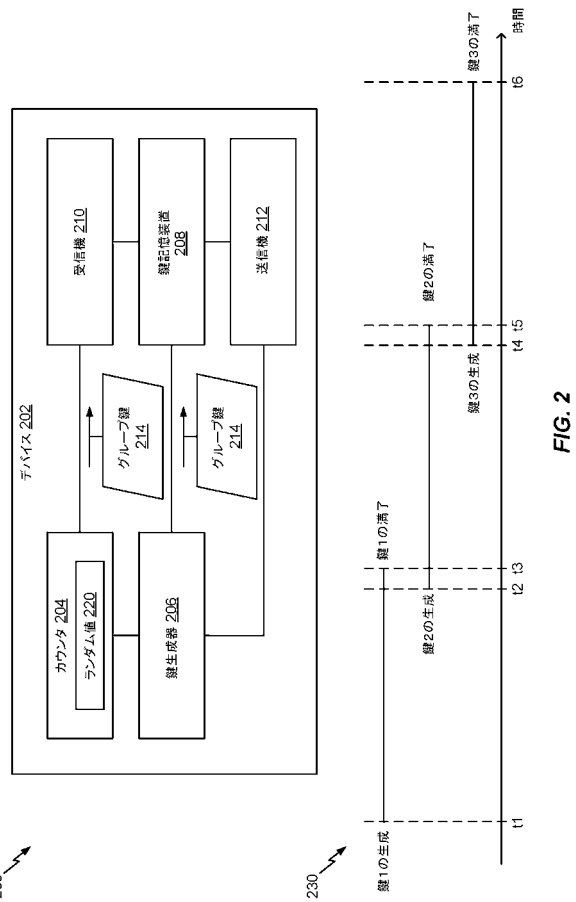

FIG. 2

【図３】

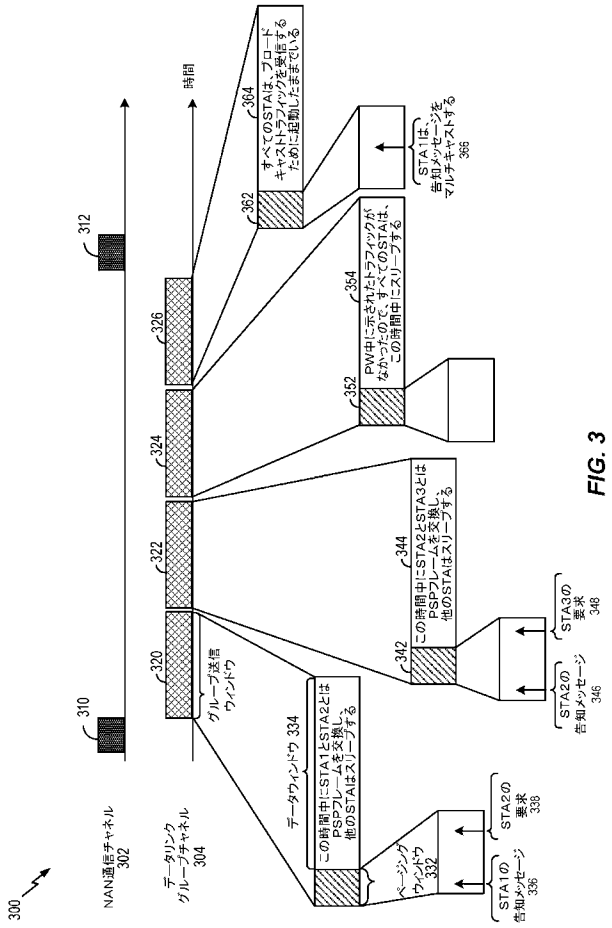

FIG. 3

【図４】

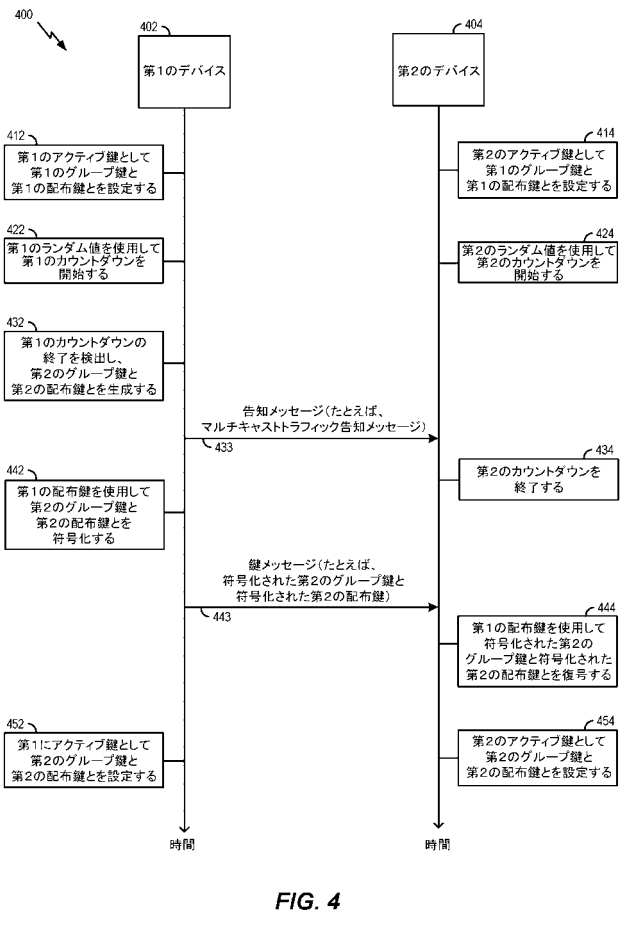

FIG. 4

【図５】

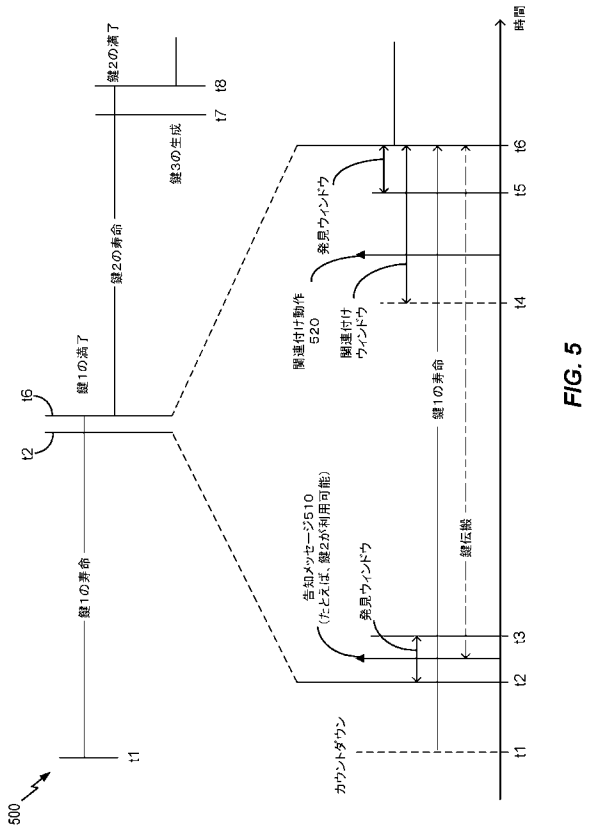

FIG. 5

【図６】

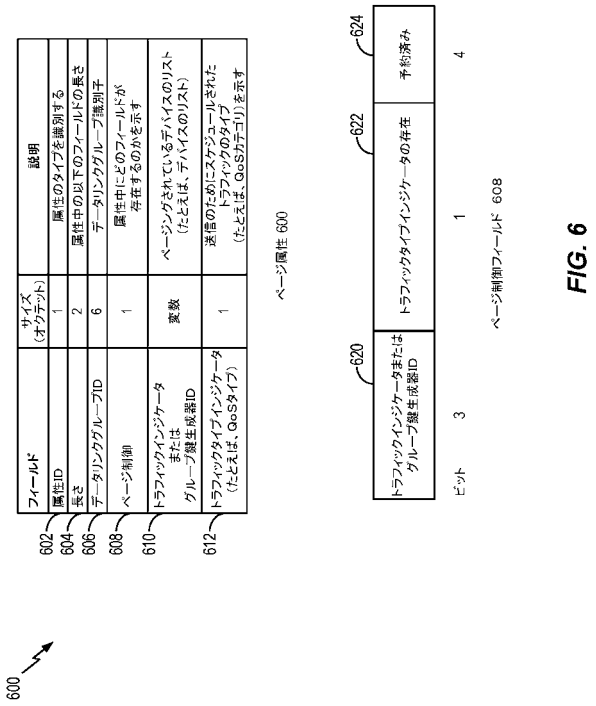

FIG. 6

【図７】

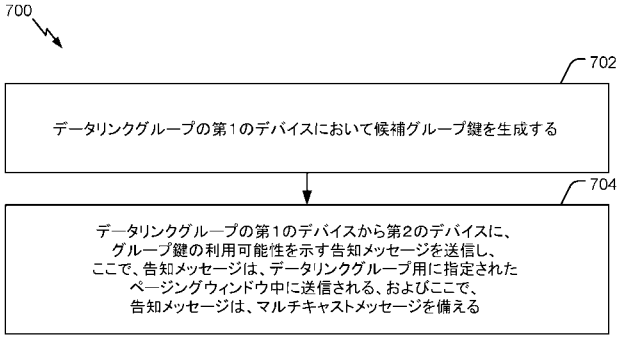

FIG. 7

【図８】

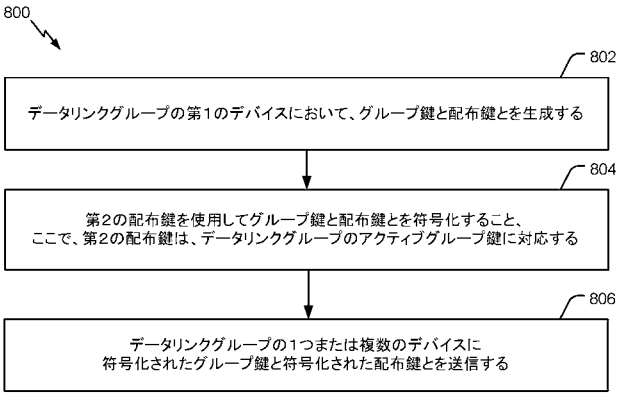

FIG. 8

【図９】

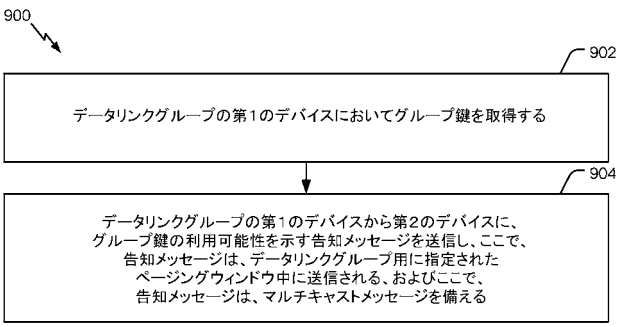

FIG. 9

【図１０】

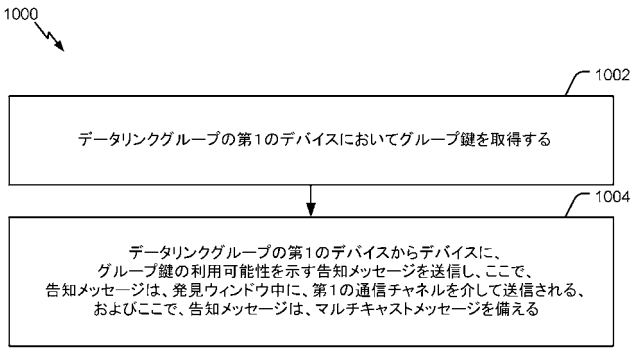

FIG. 10

【図１１】

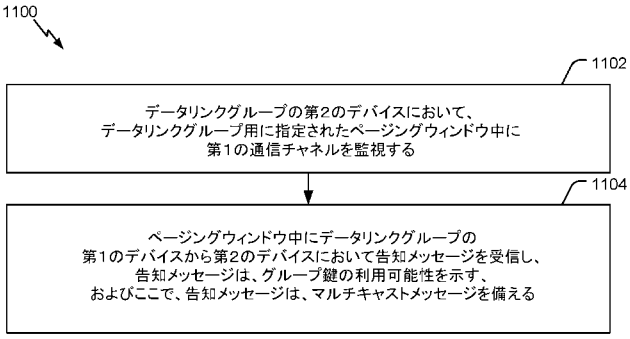

FIG. 11

【図１２】

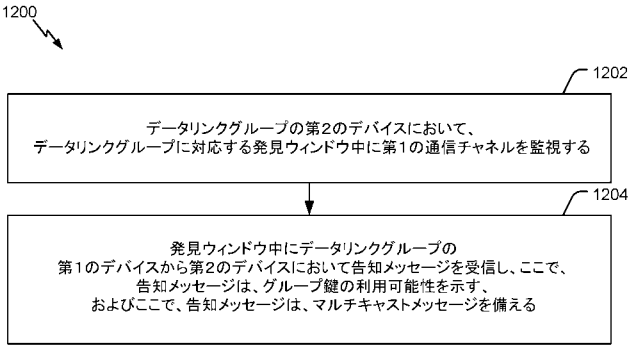

FIG. 12

【図１３】

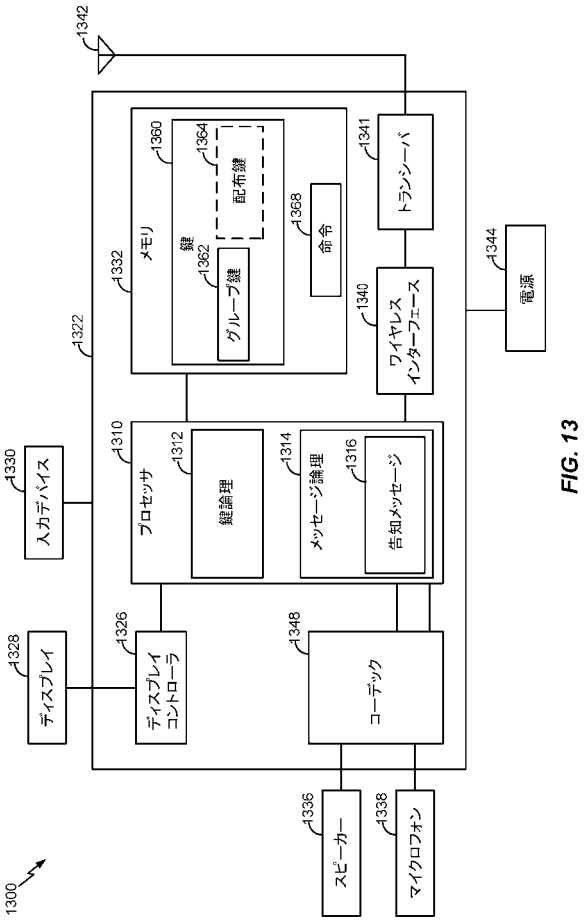

FIG. 13

【手続補正書】
【提出日】平成29年10月16日(2017.10.16)
【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と、
第１の通信チャネルの発見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し、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】
前記第１の通信チャネルは、ネイバーアウェアネットワーク（ＮＡＮ）通信チャネルに対応し、グループ鍵更新ウィンドウは、前記発見ウィンドウの終了と第２の発見ウィンドウの開始との間の継続時間を備え、前記グループ鍵更新ウィンドウは、複数の送信ウィンドウを含み、前記複数の送信ウィンドウの第１の送信ウィンドウは、前記発見ウィンドウ

の前記終了からの第１のオフセットを有し、前記複数の送信ウィンドウの第２の送信ウィンドウは、前記発見ウィンドウの前記終了からの第２のオフセットを有する、請求項１に記載のデバイス。

【請求項４】

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５】

前記ワイヤレスインターフェースが、

ページングウィンドウ中、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ページングメッセージを送信することと、

データウィンドウ中、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鍵配信メッセージを送信することと

を行うようにさらに構成された、請求項１に記載のデバイス。

【請求項６】

前記告知メッセージは、データリンクグループ識別子、鍵インジケータ、またはそれらの組合せを含む、請求項１に記載のデバイス。

【請求項７】

前記鍵インジケータが、媒体アクセス制御（ＭＡＣ）アドレス、前記候補グループ鍵のハッシュ値、前記ＭＡＣアドレス、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、請求項６に記載のデバイス。

【請求項８】

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、

前記第１のデバイスから前記データリンクグループの複数のデバイスに、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、第１の通信チャネルを介して、および、発見ウィンドウ中に送信され、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９】

ページングウィンドウ中に、前記第１のデバイスから前記データリンクグループの第２のデバイスに、前記第１のデバイスが、前記第２のデバイスに送信すべき前記候補グループ鍵を有することを示すページングメッセージを送信することと、ここにおいて、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のデバイスからトリガメッセージを受信することと、

前記トリガメッセージを受信したことに応答して、前記第２のデバイスに前記候補グループ鍵を送信することと、ここにおいて、前記候補グループ鍵が、ペアワイズ鍵に基づいて暗号化され、前記ペアワイズ鍵が、前記第１のデバイスと前記第２のデバイスとの間の関連付けプロセス中に生成される、

をさらに備える、請求項８に記載の方法。

【請求項１０】

符号化された候補グループ鍵を生成するために、アクティブ配布鍵に基づいて前記候補グループ鍵を符号化することと、

前記データリンクグループの前記複数のデバイスの１つまたは複数にマルチキャストメ

ッセージとして鍵配信メッセージを送信することと、ここにおいて、前記鍵配信メッセージが、前記符号化された候補グループ鍵を含む、
をさらに備える、請求項８に記載の方法。
【請求項１１】
グループ鍵更新ウィンドウが満了した後に、前記データリンクグループの特定のデバイスから関連付け要求を受信することと、ここにおいて、前記グループ鍵更新ウィンドウが、前記データリンクグループにおけるグループ鍵更新動作の実行に対応する特定の時間間隔を含む、
第１の基準を満たすと決定したことに応答して、前記特定のデバイスに関連付け拒絶を送信することと、ここにおいて、前記第１の基準は、前記第１のデバイスに関連するデバイスの数が、しきい値以上であるときに満たされる、
をさらに備える、請求項８に記載の方法。
【請求項１２】
前記関連付け拒絶は、前記データリンクグループのデバイスのセットを示し、前記デバイスのセットの各デバイスは、前記第１のデバイスに関連する、または、前記候補グループ鍵を持っている第２のデバイスを示し、前記関連付け拒絶により、前記特定のデバイスが、前記デバイスのセットの特定のデバイスに関連することが可能になる、請求項１１に記載の方法。
【請求項１３】
前記告知メッセージを送信したことに応答して、前記データリンクグループの特定のデバイスから関連付け要求を受信することと、
第２の基準を満たすと決定したことに応答して、前記特定のデバイスに関連付け応答を送信することと、ここにおいて、前記第２の基準は、前記第１のデバイスに関連するデバイスの数がしきい値よりも小さいときに満たされる、
をさらに備える、請求項８に記載の方法。
【請求項１４】
アクティブグループ鍵の満了より前に、第２の候補グループ鍵を生成することと、ここにおいて、前記アクティブグループ鍵により、グループアドレス指定されたデータの解読が可能になる、
前記アクティブグループ鍵の前記満了より前に、前記データリンクグループの複数の発見ウィンドウ中に、第２の告知メッセージを送信することと、ここにおいて、前記第２の告知メッセージが、前記第２の候補グループ鍵の利用可能性を示す、
前記アクティブグループ鍵の前記満了時に、前記第２の告知メッセージの送信を中止することと
をさらに備える、請求項８に記載の方法。
【請求項１５】
アクティブグループ鍵として前記候補グループ鍵を設定することと、
前記データリンクグループの前記複数のデバイスにデータを送信することと、ここにおいて、前記データが、前記アクティブグループ鍵に基づいて暗号化される、
前記アクティブグループ鍵の満了より前に、第２の候補グループ鍵を生成することと、
前記データリンクグループの複数の発見ウィンドウ中に、第２の告知メッセージを送信することと、ここにおいて、前記第２の告知メッセージが、前記第２の候補グループ鍵の利用可能性を示す、
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前記複数のデバイスに前記第２の候補グループ鍵を配布することと、
前記第１のデバイスに関連する各デバイスから対応する確認応答メッセージを受信することに基づいて、前記第１のデバイスに関連する各デバイスが前記第２の候補グループ鍵を受信したと決定することと、
前記第１のデバイスに関連する各デバイスが前記第２の候補グループ鍵を受信したと決定したことに応答して、前記第２の告知メッセージの送信を中止することと

をさらに備える、請求項８に記載の方法。
【請求項１６】
前記候補グループ鍵は、第１の鍵インジケータに関係し、前記方法は、
前記データリンクグループの第２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の候補グループ鍵および第２の鍵インジケータを示す、
前記鍵インジケータと前記第２の鍵インジケータとの比較に基づいて、伝搬のために前記候補グループ鍵を選択することと
をさらに備える、請求項８に記載の方法。
【請求項１７】
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し、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、請求項８に記載の方法。
【請求項１８】
前記第１のデバイスは、前記第１のデバイスが前記データリンクグループの発信者であることに基づいて、前記第１のデバイスが前記データリンクグループの他のデバイスの各デバイスよりも多くのデバイスに関連することに基づいて、前記第１のデバイスが、前記データリンクグループの前記他のデバイスの各デバイスよりも長い時間を前記データリンクグループ中で過ごしたことに基づいて、前記第１のデバイスに関連するデバイスの数に基づいて、前記データリンクグループのトポロジーに基づいて、前記第１のデバイスが前記データリンクグループ中に含まれた持続時間に基づいて、前記データリンクグループ内の前記第１のデバイスのランクに基づいて、前記第１のデバイスのバッテリーレベルに基づいて、またはそれらの組合せで、前記鍵生成器デバイスとして動作することを決定する、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に対応する発見ウィンドウ中に第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、
前記発見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、ここにおいて、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し、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、前記デバイスは、
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、前記候補グループ鍵セットが、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、請求項１９に記載のデバイス。
【請求項２１】
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１９に記載のデバイス。
【請求項２２】
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は、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、ここにおいて、前記ワイヤレスインターフェースは、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、
をさらに備える、請求項１９に記載のデバイス。
【請求項２３】
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に対応する発見ウィンドウ中に第１の通信チャネルを監視することと、
前記発見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、ここにおいて、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し、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２４】
前記告知メッセージが、第１の通信チャネルを介して受信され、前記方法は、
第２の通信チャネルのページングウィンドウ中に前記第１のデバイスからページング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前記第２の通信チャネルを介して送信することと、
前記第２のデバイスにおいて前記第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、
アクティブ完全性グループ鍵に基づいて前記候補グループ鍵を検証することと
をさらに備える、請求項２３に記載の方法。
【請求項２５】
前記告知メッセージを受信した後に、カウントダウンを開始することと、
前記カウントダウンの満了に応答して、前記第２のデバイスによって、前記第２のデバイスが前記候補グループ鍵を受信しなかったと決定することと、
前記カウントダウンの前記満了までに前記第２のデバイスが前記候補グループ鍵を受信しなかったと決定したことに応答して、前記第１のデバイスに関連付け要求を送信することと
をさらに備える、請求項２３に記載の方法。
【請求項２６】
前記第１のデバイスから関連付け応答を受信したことに応答して、前記第１のデバイスに関連することと、前記関連付け応答は、前記第１のデバイスが関連するために利用可能であることを示す、
前記第２のデバイスにおいて、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２５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１のデバイスに関連付け要求を送信することと、
前記第１のデバイスから関連付け拒絶を受信したことに応答して、前記第１のデバイスに第２の関連付け要求を送信することと
をさらに備える、請求項２５に記載の方法。
【請求項２８】
前記告知メッセージを受信した後に、前記第１のデバイスに関連付け要求を送信することと、
前記第１のデバイスから関連付け拒絶を受信したことに応答して、第３のデバイスに第２の関連付け要求を送信することと、ここにおいて、前記関連付け拒絶は、前記第３のデバイスが前記候補グループ鍵を持っていることを示す、

をさらに備える、請求項２５に記載の方法。
【請求項２９】
第１の鍵インジケータを含む前記告知メッセージを受信するより前に、前記第２のデバイスにおいて、第２の候補グループ鍵と前記第２の候補グループ鍵の第２の鍵インジケータとを生成することと、
前記第２の鍵インジケータが第１の鍵インジケータよりも高い優先度を示すことに基づいて、伝搬のために前記候補グループ鍵を選択することと、
前記告知メッセージを受信した後に、第２の通信チャネルを介して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４のデバイスにページングメッセージを送信することと、前記第４のデバイスは、前記第２のデバイスに関連し、ここにおいて、前記ページングメッセージは、前記第２の候補グループ鍵が前記第２のデバイスから入手可能であることを示す、
をさらに備える、請求項２３に記載の方法。
【請求項３０】
前記第２の鍵インジケータがより高い優先度の媒体アクセス制御（ＭＡＣ）アドレスを示すとき、前記第２の鍵インジケータがより前のタイムスタンプを示すとき、または、前記第２の鍵インジケータがより高い優先度のハッシュ値を示すとき、前記第２の鍵インジケータが前記第１の鍵インジケータよりも高い優先度を有すると決定することをさらに備える、請求項２９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】０００１
【補正方法】変更
【補正の内容】
【０００１】
優先権の主張
[0001]本出願は、下記の出願の各々の内容全体が参照により本明細書に明確に組み込まれる、同一出願人が所有する、２０１５年１月２７日に出願された「ＧＲＯＵＰ　ＫＥＹ　ＡＮＮＯＵＮＣＥＭＥＮＴ　ＡＮＤ／ＯＲ　ＤＩＳＴＲＩＢＵＴＩＯＮ　ＦＯＲ　Ａ　ＧＲＯＵＰ」と題する米国仮特許出願番-号第６２／１０８，３７４号、２０１５年８月２４日に出願された「ＧＲＯＵＰ　ＫＥＹ　ＡＮＮＯＵＮＣＥＭＥＮＴ　ＡＮＤ　ＤＩＳＴＲＩＢＵＴＩＯＮ　ＦＯＲ　Ａ　ＧＲＯＵＰ」と題する米国仮特許出願番号第６２／２０９，３２６号、および２０１６年１月２６日に出願された「ＧＲＯＵＰ　ＫＥＹ　ＡＮＮＯＵＮＣＥＭＥＮＴ　ＡＮＤ　ＤＩＳＴＲＩＢＵＴＩＯＮ　ＦＯＲ　Ａ　ＤＡＴＡ　ＬＩＮＫ　ＧＲＯＵＰ」と題する米国非仮特許出願番号第６２／２０９，３３６号の優先権を主張する。
【手続補正３】
【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。
以下に本願の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］

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。

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2016/015198

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L9/08 H04L29/06 H04W12/04 H04W84/18
ADD.

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 H04W

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 practicable, search terms used)
EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 6 049 878 A (CARONNI GERMANO [US] ET AL) 11 April 2000 (2000-04-11) column 6, line 51 - column 9, line 24; figures 5,6	1-5, 8-23, 25-30
Y	US 2014/082185 A1 (ABRAHAM SANTOSH PAUL [US] ET AL) 20 March 2014 (2014-03-20) paragraph [0064]; figure 5	1-5, 8-23, 25-30
A	US 2008/175387 A1 (EASTHAM W BRYANT [US]) 24 July 2008 (2008-07-24) paragraphs [0030], [0039], [0064]; figure 7 paragraphs [0053] - [0056]; figures 4,5 paragraphs [0045] - [0050]; figures 2,3	1-30

-/--

[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 application or patent 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
22 March 2016	04/04/2016

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, Fax: (+31-70) 340-3016	Horbach, Christian

1

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

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2016/015198

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 2009/118268 A2 (IBM [US]; IBM UK [GB]; SAYRE JOHANNES [US]; BAE MYUNG [US]; KNOP FELIP) 1 October 2009 (2009-10-01) page 17, lines 15-25	1-30

1

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

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/US2016/015198

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 6049878 A	11-04-2000	NONE	
US 2014082185 A1	20-03-2014	CN 104662937 A	27-05-2015
		JP 2015530058 A	08-10-2015
		US 2014082185 A1	20-03-2014
		WO 2014047125 A1	27-03-2014
US 2008175387 A1	24-07-2008	CN 101641903 A	03-02-2010
		EP 2104989 A1	30-09-2009
		JP 5033188 B2	26-09-2012
		JP 2010517330 A	20-05-2010
		KR 20090110334 A	21-10-2009
		RU 2009131314 A	27-02-2011
		TW 200840297 A	01-10-2008
		US 2008175387 A1	24-07-2008
		WO 2008088084 A1	24-07-2008
WO 2009118268 A2	01-10-2009	CN 101981889 A	23-02-2011
		EP 2258093 A2	08-12-2010
		KR 20100133448 A	21-12-2010
		US 2009245518 A1	01-10-2009
		WO 2009118268 A2	01-10-2009

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,LR,LS,MW,MZ,NA,RW,SD,SL,ST,SZ,TZ,UG,ZM,ZW),EA(AM,AZ,BY,KG,KZ,RU,TJ,TM),EP(AL,AT,BE,BG,CH,CY,CZ,DE,DK,EE,ES,FI,FR,GB,GR,HR,HU,IE,IS,IT,LT,LU,LV,MC,MK,MT,NL,NO,PL,PT,RO,RS,SE,SI,SK,SM,TR),OA(BF,BJ,CF,CG,CI,CM,GA,GN,GQ,GW,KM,ML,MR,NE,SN,TD,TG),AE,AG,AL,AM,AO,AT,AU,AZ,BA,BB,BG,BH,BN,BR,BW,BY,BZ,CA,CH,CL,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,IR,IS,JP,KE,KG,KN,KP,KR,KZ,LA,LC,LK,LR,LS,LU,LY,MA,MD,ME,MG,MK,MN,MW,MX,MY,MZ,NA,NG,NI,NO,NZ,OM,PA,PE,PG,PH,PL,PT,QA,RO,RS,RU,RW,SA,SC,SD,SE,SG,SK,SL,SM,ST,SV,SY,TH,TJ,TM,TN,TR,TT,TZ,UA,UG,US

(72)発明者 パティル、アビシェク・プラモド
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
(72)発明者 チェリアン、ジョージ
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
(72)発明者 リ、ス・ボム
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
(72)発明者 マリネン、ジョウニ・カレビ
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
(72)発明者 アブラハム、サントシュ・ポール
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
(72)発明者 ライシニア、アリレザ
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

Ｆターム(参考) 5J104 AA16 AA34 EA18 NA02 NA37 PA07