(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2012-522467
(P2012-522467A)
(43)公表日　平成24年9月20日(2012.9.20)

(51)Int.Cl.		F I			テーマコード（参考）
H04L 9/08	(2006.01)	H04L	9/00	601C	5J104
H04W 12/02	(2009.01)	H04Q	7/00	181	5K067
H04W 12/04	(2009.01)	H04Q	7/00	182	5K201
H04W 12/06	(2009.01)	H04Q	7/00	183	
H04M 11/00	(2006.01)	H04M	11/00	303	

審査請求 有　予備審査請求 未請求　（全 18 頁）

(21)出願番号　特願2012-503583 (P2012-503583)
(86)(22)出願日　平成22年3月30日 (2010.3.30)
(85)翻訳文提出日　平成23年11月7日 (2011.11.7)
(86)国際出願番号　PCT/US2010/029121
(87)国際公開番号　WO2010/117746
(87)国際公開日　平成22年10月14日 (2010.10.14)
(31)優先権主張番号　12/414,630
(32)優先日　平成21年3月30日 (2009.3.30)
(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　100159651
弁理士　高倉　成男
(74)代理人　100091351
弁理士　河野　哲
(74)代理人　100088683
弁理士　中村　誠

最終頁に続く

(54)【発明の名称】受信機に向けられたチャネルにおけるプライバシー保護に対処する装置および方法

(57)【要約】
第２のワイヤレス・デバイスとプライバシーキーを共有する第１のワイヤレス・デバイスのためのプライバシー保護に対処するための方法が開示される。当該方法において、第１のレゾリューションタグは、入力引数としてシード値およびプライバシーキーをともなう擬似ランダム関数を使用して第１のワイヤレス・デバイスにおいて生成される。プライバシーキーは、第１および第２のワイヤレス・デバイスにのみ知られている。プライバシー・アドレスは、シード値および第１のレゾリューションタグに基づいて第１のワイヤレス・デバイスのために生成される。パケットは、第１のワイヤレス・デバイスから第２のワイヤレス・デバイスへ送信される。パケットは、プライバシー・アドレスおよび第１のレゾリューションタグを含む。
【選択図】　図３

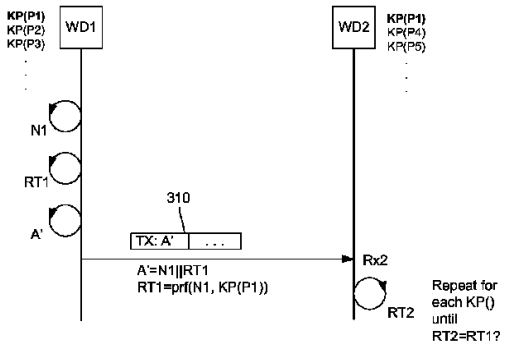


FIG. 3

【特許請求の範囲】
【請求項１】
第２のワイヤレス・デバイスとプライバシーキーを共有する第１のワイヤレス・デバイスのためのプライバシー保護に対処する方法であって、
入力セグメントとしてシード値と前記第１および第２のワイヤレス・デバイスにのみ知られている前記プライバシーキーとをともなう擬似ランダム関数を使用して前記第１のワイヤレス・デバイスにおいて第１のレゾリューションタグを生成することと、
前記シード値および前記第１のレゾリューションタグに基づいて前記第１のワイヤレス・デバイスのためのプライバシー・アドレスを生成することと、および
前記第１のワイヤレス・デバイスから前記第２のワイヤレス・デバイスへ前記プライバシー・アドレスおよび前記第１のレゾリューションタグを含むパケットを送信することとを備える方法。
【請求項２】
前記擬似ランダム関数は、短縮されたキー付きハッシュ・メッセージ認証コードを生成する、請求項１に記載のプライバシー保護に対処する方法。
【請求項３】
前記擬似ランダム関数は、暗号化ベースのメッセージ認証コードを生成する、請求項１に記載のプライバシー保護に対処する方法。
【請求項４】
前記プライバシーキーは、前記第１と第２のワイヤレス・デバイスのペアに基づいて生成されるペアにされたデバイスキーである、請求項１に記載のプライバシー保護に対処する方法。
【請求項５】
前記パケットは、前記シード値をさらに含む、請求項１に記載のプライバシー保護に対処する方法。
【請求項６】
前記シード値は、ナンス（nonce）である、請求項５に記載のプライバシー保護に対処する方法。
【請求項７】
前記シード値は、前記第１および第２のワイヤレス・デバイスによって維持されるカウンター値である、請求項１に記載のプライバシー保護に対処する方法。
【請求項８】
前記シード値は、タイムスタンプである、請求項１に記載のプライバシー保護に対処する方法。
【請求項９】
前記パケットは、前記第１と第２のワイヤレス・デバイス間の前記シード値を同期するための前記シード値の一部を含む、請求項１に記載のプライバシー保護に対処する方法。
【請求項１０】
前記プライバシー・アドレスは、前記第１のレゾリューションタグと連結した前記シード値である、請求項１に記載のプライバシー保護に対処する方法。
【請求項１１】
前記第２のワイヤレス・デバイスとのみ関連するワイヤレス受信チャネル上で前記第１のワイヤレス・デバイスから前記パケットを受信する前記第２のワイヤレス・デバイスと、
入力引数として前記シード値および前記プライバシーキーをともなう前記擬似ランダム関数を使用して第２のレゾリューションタグを生成する前記第２のワイヤレス・デバイスと、および
前記第２のレゾリューションタグが前記第１のレゾリューションタグと一致するとき、前記第１のワイヤレス・デバイスへ前記プライバシー・アドレスをマッピングする前記第２のワイヤレス・デバイスと

をさらに具備する、請求項１に記載のプライバシー保護に対処する方法。
【請求項１２】
前記第１のワイヤレス・デバイスは、ブロードキャスト匿名ページング・チャネル上で前記第２のワイヤレス・デバイスに前記パケットを送信し、
前記方法は、前記第１のワイヤレス・デバイスの前記プライバシー・アドレスによって定義されるワイヤレス受信チャネル上で前記第１のワイヤレス・デバイスへ第２のパケットを転送する前記第２のワイヤレス・デバイスをさらに備える、請求項１１に記載のプライバシー保護に対処する方法。
【請求項１３】
第２のワイヤレス・デバイスとプライバシーキーを共有する、プライバシー保護に対処する装置であって、
入力引数としてシード値と前記装置および前記第２のワイヤレス・デバイスにのみ知られている前記プライバシーキーとをともなう擬似ランダム関数を使用して第１のレゾリューションタグを生成する手段と、
前記シード値および前記第１のレゾリューションタグに基づいて前記装置のためのプライバシー・アドレスを生成する手段と、および
前記第２のワイヤレス・デバイスに前記プライバシー・アドレスおよび前記第１のレゾリューションタグを含むパケットを送信する手段と
を備える装置。
【請求項１４】
前記擬似ランダム関数は、短縮されたキー付きハッシュ・メッセージ認証コードを生成する、請求項１３に記載のプライバシー保護に対処する装置。
【請求項１５】
前記擬似ランダム関数は、暗号化ベースのメッセージ認証コードを生成する、請求項１３に記載のプライバシー保護に対処する装置。
【請求項１６】
前記プライバシーキーは、前記第１と第２のワイヤレス・デバイスのペアに基づいて生成されるペアにされたデバイスキーである、請求項１３に記載のプライバシー保護に対処する装置。
【請求項１７】
前記パケットは、前記シード値をさらに含む、請求項１３に記載のプライバシー保護に対処する装置。
【請求項１８】
前記シード値は、ナンスである、請求項１７に記載のプライバシー保護に対処する装置。
【請求項１９】
前記シード値は、前記装置および前記第２のワイヤレス・デバイスによって維持されるカウンター値である、請求項１３に記載のプライバシー保護に対処する装置。
【請求項２０】
前記シード値は、タイムスタンプである、請求項１３に記載のプライバシー保護に対処する装置。
【請求項２１】
前記パケットは、前記第１と第２のワイヤレス・デバイス間の前記シード値を同期するための前記シード値の一部を含む、請求項１３に記載のプライバシー保護に対処する装置。
【請求項２２】
前記プライバシー・アドレスは、前記第１のレゾリューションタグと連結した前記シード値である、請求項１３に記載のプライバシー保護に対処する装置。
【請求項２３】
コンピュータ・プログラム・プロダクトであって、

入力引数としてシード値とコンピュータおよび第２のワイヤレス・デバイスにのみ知られているプライバシーキーとをともなう擬似ランダム関数を使用する第１のレゾリューションタグを前記コンピュータに生成させるためのコードと、
前記シード値および前記第１のレゾリューションタグに基づいてプライバシー・アドレスをコンピュータに生成させるためのコードと、および
前記第２のワイヤレス・デバイスに前記プライバシー・アドレスおよび前記第１のレゾリューションタグを含むパケットをコンピュータに送信させるためのコードと
を具備するコンピュータ可読媒体を具備するコンピュータ・プログラム・プロダクト。
【請求項２４】
前記擬似ランダム関数は、短縮されたキー付きハッシュ・メッセージ認証コードを生成する、請求項２３に記載のコンピュータ・プログラム・プロダクト。
【請求項２５】
前記擬似ランダム関数は、暗号化ベースのメッセージ認証コードを生成する、請求項２３に記載のコンピュータ・プログラム・プロダクト。
【請求項２６】
前記プライバシーキーは、前記コンピュータおよび前記第２のワイヤレス・デバイスのペアに基づいて生成されるペアにされたデバイスキーである、請求項２３に記載のコンピュータ・プログラム・プロダクト。
【請求項２７】
前記パケットは、前記シード値をさらに含む、請求項２３に記載のコンピュータ・プログラム・プロダクト。
【請求項２８】
前記シード値は、ナンスである、請求項２７に記載のコンピュータ・プログラム・プロダクト。
【請求項２９】
前記シード値は、前記コンピュータおよび前記第２のワイヤレス・デバイスによって維持されるカウンター値である、請求項２３に記載のコンピュータ・プログラム・プロダクト。
【請求項３０】
前記シード値は、タイムスタンプである、請求項２３に記載のコンピュータ・プログラム・プロダクト。
【請求項３１】
前記パケットは、前記コンピュータと第２のワイヤレス・デバイスとの間の前記シード値を同期するための前記シード値の一部を含む、請求項２３に記載のコンピュータ・プログラム・プロダクト。
【請求項３２】
前記プライバシー・アドレスは、前記第１のレゾリューションタグと連結した前記シード値である、請求項２３に記載のコンピュータ・プログラム・プロダクト。
【請求項３３】
第２のワイヤレス・デバイスとプライバシーキーを共有する、プライバシー保護に対処する時計であって、
入力引数としてシード値と前記時計および前記第２のワイヤレス・デバイスにのみ知られている前記プライバシーキーとをともなう擬似ランダム関数を使用して第１のレゾリューションタグを生成する手段と、
前記シード値および前記第１のレゾリューションタグに基づいて前記時計のためのプライバシー・アドレスを生成する手段と、および
前記第２のワイヤレス・デバイスに前記プライバシー・アドレスおよび前記第１のレゾリューションタグを含むパケットを送信する手段と
を備える、時計。
【請求項３４】

第２のワイヤレス・デバイスとプライバシーキーを共有する、プライバシー保護に対処するヘッドセットであって、
入力引数としてシード値と前記ヘッドセットおよび前記第２のワイヤレス・デバイスにのみ知られている前記プライバシーキーとをともなう擬似ランダム関数を使用する第１のレゾリューションタグを生成する手段と、
前記シード値および前記第１のレゾリューションタグに基づいて前記ヘッドセットのためのプライバシー・アドレスを生成する手段と、および
前記第２のワイヤレス・デバイスに前記プライバシー・アドレスおよび前記第１のレゾリューションタグを含むパケットを送信する手段と
を備える、ヘッドセット。
【請求項３５】
第２のワイヤレス・デバイスとプライバシーキーを共有する、プライバシー保護に対処するセンシング・デバイスであって、
入力引数としてシード値と前記センシングおよび前記第２のワイヤレス・デバイスにのみ知られている前記プライバシーキーとをともなう擬似ランダム関数を使用して第１のレゾリューションタグを生成する手段と、
前記シード値および前記第１のレゾリューションタグに基づいて前記センシング・デバイスのためのプライバシー・アドレスを生成する手段と、および
前記第２のワイヤレス・デバイスに前記プライバシー・アドレスおよび前記第１のレゾリューションタグを含むパケットを送信する手段と
を備えるセンシング・デバイス。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、一般に、受信機に向けられた（oriented）ワイヤレス・チャネルにおけるプライバシー保護に対処することに関係する。
【背景技術】
【０００２】
短距離にわたってデータをワイヤレスに伝送するピア・ツー・ピア・ネットワークは、ケーブルを使用する従来の有線の接続に対する利点により普及しつつある。ブルートゥースおよびZipBeeは、短距離ピア・ネットワークの標準の事例である。
【０００３】
しかしながら、ピア・デバイス間のワイヤレス通信は、追跡および攻撃の対象になり得る。無線上でワイヤレスに送信されるパケットは、一般に、正しく搬送されるためにそのソースおよび宛先を識別する。ソースおよび宛先は、一般に、それぞれのアドレスによって識別される。結果として、盗聴者は、受信チャネルを受動的に盗聴し、そのソースアドレスまたは宛先アドレスが含まれる受信チャネルを追跡し得る。盗聴者は、したがって、１つのエンティティがパケットを送信または受信していることを知っている。
【０００４】
短距離のワイヤレス通信において、アドレス追跡のそのような可能性は望ましくない。パケット内のソースアドレスまたは宛先アドレスは、通常特定のデバイスと関連されている。デバイスの存在は、デバイスの所有者の位置および時間パターンのような有用な情報を開示し得る。
【０００５】
したがって、プライバシー保護に対処するための技術に対するニーズがある。
【発明の概要】
【０００６】
本発明の態様は、第２のワイヤレス・デバイスとプライバシーキーを共有する第１のワイヤレス・デバイスのためのプライバシー保護に対処する方法に属することができる。当該方法において、第１のレゾリューションタグ（resolution tag）は、入力引数としてシ

ード値およびプライバシーキーをともなう擬似ランダム関数を使用して第１のワイヤレス・デバイスにおいて生成される。プライバシーキーは、第１および第２のワイヤレス・デバイスにのみ知られている。プライバシー・アドレスは、シード値および第１のレゾリューションタグに基づいて第１のワイヤレス・デバイスのために生成される。パケットは、第１のワイヤレス・デバイスから第２のワイヤレス・デバイスに送信される。パケットは、プライバシー・アドレスおよび第１のレゾリューションタグを含む。

【０００７】

本発明のより詳細な態様において、擬似ランダム関数は、短縮されたキー付きハッシュ・メッセージ認証コード（a truncated keyed hash message authentication code）または暗号化ベースのメッセージ認証コード（a cipher-based message authentication code）を生成することができる。プライバシーキーは、第１および第２のワイヤレス・デバイスのペアに基づいて生成されるペアにされたデバイスキーであり得る。

【０００８】

パケットは、シード値をさらに含む。シード値は、ナンス（nonce）であり得る。代替的に、シード値は、第１および第２のワイヤレス・デバイスによって維持されるタイムスタンプ、またはカウンター値であり得る。したがって、パケットは、第１と第２のワイヤレス・デバイス間のシード値を同期するためのシード値の一部を含み得る。プライバシー・アドレスは、第１のレゾリューションタグと連結したシード値であり得る。プライバシー・アドレスは、第２のデバイスが他の方法でシード値を知っている場合、単に第１のレゾリューションタグを含み得る。

【０００９】

本発明の他のより詳細な態様において、第２のワイヤレス・デバイスは、第２のワイヤレス・デバイスとのみ関連するワイヤレス受信チャネル上で第１のワイヤレス・デバイスからパケットを受信することができる。第２のワイヤレス・デバイスは、入力引数としてシード値およびプライバシーキーをともなう擬似ランダム関数を使用して第２のレゾリューションタグを生成することができる。第２のレゾリューションタグが第１のレゾリューションタグと一致するとき、第２のワイヤレス・デバイスは、第１のワイヤレス・デバイスにプライバシー・アドレスをマップすることができる。さらに、第１のワイヤレス・デバイスは、ブロードキャスト匿名ページング・チャネル（a broadcast anonymous paging channel）上で第２のワイヤレス・デバイスにパケットを送信することができ、第２のワイヤレス・デバイスは、第１のワイヤレス・デバイスのプライバシー・アドレスによって定義されるワイヤレス受信チャネル上で第１のワイヤレス・デバイスに第２のパケットを転送することができる。

【００１０】

本発明の他の態様は、第２のワイヤレス・デバイスとプライバシーキーを共有する、プライバシー保護に対処する装置に属することができる。当該装置は、入力としてシード値と当該装置および第２のワイヤレス・デバイスにのみ知られているプライバシーキーとをともなう擬似ランダム関数を使用して第１のレゾリューションタグを生成する手段と、シード値および第１のレゾリューションタグに基づいて装置のためのプライバシー・アドレスを生成する手段と、および第２のワイヤレス・デバイスにプライバシー・アドレスおよび第１のレゾリューションタグを含むパケットを送信する手段とを含むことができる。当該装置は、時計、ヘッドセット、またはセンシング・デバイスを具備することができる。

【００１１】

本発明の他の態様は、入力引数としてシード値とコンピュータおよび第２のワイヤレス・デバイスにのみ知られているプライバシーキーとをともなう擬似ランダム関数を使用する第１のレゾリューションタグをコンピュータに生成させるためのコードと、シード値および第１のレゾリューションタグに基づいてプライバシー・アドレスをコンピュータに生成させるためのコードと、および第２のワイヤレス・デバイスにプライベート・アドレスおよび第１のレゾリューションタグを含むパケットをコンピュータに送信させるためのコードとを具備するコンピュータ可読媒体を具備するコンピュータ・プログラム・プロダク

トに属することができる。
【図面の簡単な説明】
【００１２】
【図１】図１は、ワイヤレス通信システムの一例のブロック図である。
【図２】図２は、第２のワイヤレス・デバイスとプライバシーキーを共有する第１のワイヤレス・デバイスのプライバシー保護に対処する方法のフロー図である。
【図３】図３は、プライバシー保護に対処する方法を例示するフロー図である。
【図４】図４は、プライバシー保護に対処する方法を例示する他のフロー図である。
【図５】図５は、プロセッサおよびメモリを含むコンピュータのブロック図である。
【発明の詳細な説明】
【００１３】
「典型的な(exemplary)」という用語は、本明細書において、「事例、例、または例示として役に立つ(serving as an example, instance, or illustration)」ことを意味するために使用される。本明細書において、「典型的な（exemplary）」として説明される任意の実施形態は、必ずしも他の実施形態に対して好ましいまたは有利であるものとして解釈されない。
【００１４】
図１－３を参照して、本発明の態様は、第２のワイヤレス・デバイス、WD２および１１４、とプライバシーキーKPを共有するモバイル局１０２のような第１のワイヤレス・デバイスWD１のためのプライバシー保護に対処する方法２００に属することができる。当該方法において、第１のレゾリューションタグRT１は、入力引数としてシード値Ｓ１およびプライバシーキーをともなう擬似ランダム関数を使用して第１のワイヤレス・デバイスにおいて生成される（ステップ２１０）。プライバシーキーは、第１および第２のワイヤレス・デバイスにのみ知られている。プライバシー・アドレスA’は、シード値および第１のレゾリューションタグに基づいて第１のワイヤレス・デバイスのために生成される（ステップ２２０）。パケット３１０は、第１のワイヤレス・デバイスから第２のワイヤレス・デバイスへ送信される（ステップ２３０）。パケットは、プライバシー・アドレスおよび第１のレゾリューションタグを含む。
【００１５】
擬似ランダム関数は、短縮されたキー付きハッシュ・メッセージ認証コード（HMAC）（a truncated keyed hash message authentication code）または暗号化ベースのメッセージ認証コード（CMAC）（a cipher-based message authentication code）を生成することができる。擬似ランダム関数は、暗号的に強いものであるべきであるので、プライバシー・アドレスA’から共有されたプライバシーキーKPを導き出すことは実行不可能である。プライバシーキーは、第１および第２のワイヤレス・デバイスのペアに基づいて生成されるペアにされたデバイスキーであり得る。デバイスをペアにするために、ユーザは、コードを各デバイスに手動で入力するか、または他の方法でこれらの２個のデバイス間のセキュリティ関連性を確立し得る。シード値Ｓ１は、ナンス（nonce）Ｎ１、カウンター値、またはタイムスタンプであり得る。プライバシー・アドレスA’は、第１のレゾリューションタグと連結したシード値であり得るので、A’ = Ｓ１||RT１である。なお、RT１ = prf(Ｓ１、KP)である。シード値Ｓ１がカウンター値またはタイムスタンプであるとき、受信デバイスが他の方法でシード値の正確な値を得ることができるかどうかに依拠して、シード値は、プライバシー・アドレスに含まれる、部分的に含まれる、または省略されることができる。シード値がナンスＮ１であるとき、ナンスは、図３において図示されるように第１のワイヤレス・デバイスWD１において生成され、プライバシー・アドレスA’の一部としてパケット３１０において送信される。
【００１６】
さらに、第２のワイヤレス・デバイスWD２は、第２のワイヤレス・デバイスとのみ関連するワイヤレス受信チャネルＲｘ２上で第１のワイヤレス・デバイスＷＤ１からパケットを受信することができる。第２のワイヤレス・デバイスは、入力引数としてシード値（例

えば、ナンスＮ１）およびプライバシーキーをともなう擬似ランダム関数を使用して第２のレゾリューションタグＲＴ２を生成することができる。第２のワイヤレス・デバイスは、第２のレゾリューションタグが第１のレゾリューションタグと一致するとき、第１のワイヤレス・デバイスへプライバシー・アドレスをマップすることができる。第１および第２のワイヤレス・デバイスは、複数の他のデバイスとペアにされることができる。各々のペア（Ｐ１、．．．、ＰＮ）は、関連するプライバシーキーＫＰ（）を有する。デバイスは、レゾリューションタグにおける一致が見つけ出されるまで、プライバシーキーＫＰ（Ｐ１、．．．、ＰＮ）ごとにレゾリューションタグを生成することによってプライバシー・アドレスをマップする。

【００１７】

図４を参照して、第１のワイヤレス・デバイスＷＤ１は、ブロードキャスト匿名ページング・チャネル（a broadcast anonymous paging channel）Ｒｘ０上で第２のワイヤレス・デバイスにパケット３１０を送信することができ、第２のワイヤレス・デバイスＷＤ２は、第１のワイヤレス・デバイスのプライバシー・アドレスＡ’によって定義されるワイヤレス受信チャネルＲｘＡ’上で第１のワイヤレス・デバイスに第２のパケット３２０を転送することができる。さらに、第２のワイヤレス・デバイスは、第２のナンスと、第２のナンスおよびプライバシーキーＰＫを使用して生成される第３のレゾリューションタグＲＴ３とに基づいて自身のプライバシー・アドレスＡ２’を生成するための第２のシード値（例えば、ナンスＮ２）を生成することができる。第１のワイヤレス・デバイスは、第４のレゾリューションタグＲＴ４を生成し、第３のレゾリューションタグＲＴ３に一致させることによって、第２のワイヤレス・デバイスに第２のプライバシー・アドレスＡ２’をマップすることができる。

【００１８】

ワイヤレス・デバイスは、時間期間の後にそのプライバシー・アドレスを変更するべきである。従って、デバイスと関連する共通の受信チャネルは、例えば、ＲｘＡ’からＲｘＡ”へ変更し得る。

【００１９】

本技術は、Bluetooth（登録商標） Low-Energy（ＬＥ）におけるような、１つのデバイスとペアにされた全てのデバイスによって共有されるアイデンティティ・ルート（ＩＲ）のような秘密に依存しない。代わりに、アドレスのプライバシーは、ペアにする方法で保護される。したがって、デバイスとペアにされた１つのデバイスが危険にさらされるとしても、攻撃者は、セキュリティ破壊をされたものを除いて他のデバイスによるアクティビティを追跡することができない。

【００２０】

図５を参照して、本発明の他の態様は、第２のワイヤレス・デバイスＷＤ２とプライバシーキーＫＰを共有する、プライバシー保護に対処する装置５００に属することができる。当該装置は、入力引数としてシード値と当該装置および第２のワイヤレス・デバイスにのみ知られているプライバシーキーとをともなう擬似ランダム関数を使用して第１のレゾリューションタグＲＴ１を生成する手段（プロセッサ５１０）と、シード値および第１のレゾリューションタグに基づいて当該装置のためのプライバシー・アドレスＡ’を生成する手段と、および第２のワイヤレス・デバイスにプライベート・アドレスおよび第１のレゾリューションタグを含むパケット３１０を送信する手段とを含むことができる。当該装置は、時計、ヘッドセット、センシング・デバイス、またはモバイル局１０２を具備することができる。

【００２１】

当該装置は、メモリ、ディスプレイ５３０、およびキーボードのような入力デバイス５４０のような記録媒体５２０をさらに含むことができる。当該装置は、ワイヤレス接続５５０を含むことができる。

【００２２】

本発明の他の態様は、入力引数としてシード値と当該コンピュータおよび第２のワイヤ

レス・デバイスにのみ知られているプライバシーキーＫＰとをともなう擬似ランダム関数を使用して第１のレゾリューションタグＲＴ１をコンピュータ５００に生成させるためのコードと、シード値および第１のレゾリューションタグに基づいてプライバシー・アドレスＡ’をコンピュータに生成させるためのコードと、および第２のワイヤレス・デバイスにプライベート・アドレスおよび第１のレゾリューションタグを含むパケット３１０をコンピュータに送信させるためのコードとを具備するコンピュータ可読媒体５２０を具備するコンピュータ・プログラム・プロダクトに属することができる。

【００２３】

ワイヤレス・デバイスは、ワイヤレス・デバイスによって送信されるまたはワイヤレス・デバイスにおいて受信される信号に基づいて機能を実行するさまざまなコンポーネントを含むことができる。例えば、ワイヤレス・ヘッドセットは、受信機を通して受信される信号に基づいてオーディオ出力を提供するのに適したトランスデューサを含むことができる。ワイヤレス時計は、受信機を通して受信された信号に基づいて表示を提供するのに適したユーザ・インターフェースを含むことができる。ワイヤレス・センシング・デバイスは、他のデバイスへ送信されることとなるデータを提供するのに適したセンサーを含むことができる。

【００２４】

図１を再度参照して、ワイヤレス・モバイル局（ＭＳ）１０２は、ワイヤレス通信システム１００の１つまたは複数の基地局（ＢＳ）１０４と通信することができる。ワイヤレス通信システム１００は、１つまたは複数の基地局コントローラ（ＢＳＣ）１０６、およびコアネットワーク１０８をさらに含むことができる。コアネットワークは、適切なバックホール（backhaul）を通してインターネット１１０および公衆交換電話ネットワーク（ＰＳＴＮ）１１２に接続されることができる。典型的なワイヤレス・モバイル局は、ハンドヘルド電話、またはラップトップ・コンピュータを含むことができる。ワイヤレス通信システム１００は、符号分割多元接続（ＣＤＭＡ）、時分割多元接続（ＴＤＭＡ）、周波数分割多元接続（ＦＤＭＡ）、空間分割多元接続（ＳＤＭＡ）、偏波多元接続（ＰＤＭＡ）、または当該技術分野において既知の他の変調技術のようないくつかの多元接続技術のうちのいずれか１つを採用することができる。

【００２５】

ワイヤレス・デバイス１１４は、任意の適切なワイヤレス通信技術に基づいてまたはそうでなければ任意の適切なワイヤレス通信技術をサポートする１つまたは複数のワイヤレス通信リンクを通して通信することができる。例えば、いくつかの態様において、ワイヤレス・デバイスは、ネットワークと関連することができる。いくつかの態様において、ネットワークは、ボディエリア・ネットワークまたはパーソナルエリア・ネットワーク（例えば、超広帯域ネットワーク）を具備することができる。いくつかの態様において、ネットワークは、ローカルエリア・ネットワークまたは広域ネットワークを具備することができる。ワイヤレス・デバイスは、例えば、ＣＤＭＡ、ＴＤＭＡ、ＯＦＤＭ、ＯＦＤＭＡ、ＷｉＭＡＸ、およびＷｉ－Ｆｉのようなさまざまなワイヤレス通信技術、プロトコル、または標準のうちの１つまたは複数をサポートすることができるか、そうでなければ使用することができる。同様に、ワイヤレス・デバイスは、さまざまな対応する変調方式または多重化方式のうちの１つまたは複数をサポートすることができるか、またはそうでなければ使用することができる。ワイヤレス・デバイスは、したがって、上記のまたは他のワイヤレス通信技術を使用して１つまたは複数のワイヤレス通信リンクを通して確立および通信するための適切なコンポーネント（例えば、無線インターフェース）を含むことができる。例えば、デバイスは、ワイヤレス媒体上の通信を容易にするさまざまなコンポーネント（例えば、信号生成器および信号プロセッサ）を含むことができる関連する送信機および受信機コンポーネント（例えば、送信機および受信機）を備えるワイヤレス・トランシーバを具備することができる。

【００２６】

本明細書における技術は、さまざまな装置（例えば、デバイス）に組み込まれる（例え

ば、さまざまな装置内で実装される、またはさまざまな装置によって実行される）ことができる。例えば、本明細書において教示される１つまたは複数の態様は、電話（例えば、セルラ電話）、携帯情報端末（「ＰＤＡ」）、娯楽デバイス（例えば、音楽またはビデオデバイス）、ヘッドセット（例えば、ヘッドフォン、イヤフォンなど）、マイクロフォン、メディカル・デバイス（例えば、バイオメトリックセンサ、心拍数モニタ、歩数計、ＥＫＧデバイスなど）、ユーザＩ／Ｏデバイス（例えば、時計、遠隔コントロール、電灯のスイッチ、キーボード、マウスなど）、タイヤ圧力モニタ、コンピュータ、ＰＯＳシステムのデバイス、娯楽デバイス、補聴器、セットトップ・ボックス、または任意の他の適切なデバイスに組み込まれることができる。

【００２７】

これらのデバイスは、異なる電力およびデータ要件を有し得る。いくつかの態様において、本明細書における技術は、低電力アプリケーションにおける使用（例えば、インパルス・ベースの信号方式および低デューティー・サイクル・モードの使用による）に適していることができ、比較的高いデータレートを含むさまざまなデータレート（例えば、高帯域パルスの使用による）をサポートすることができる。

【００２８】

いくつかの態様において、ワイヤレス・デバイスは、通信システムのためのアクセスデバイス（例えば、Ｗｉ－Ｆｉアクセスポイント）を具備することができる。そのようなアクセスデバイスは、例えば、有線のまたはワイヤレス通信リンクを通して他のネットワーク（例えば、インターネットまたはセルラ・ネットワークのような広域ネットワーク）への接続性を提供することができる。したがって、アクセスデバイスは、他のデバイス（例えば、Ｗｉ－Ｆｉ局）がその他のネットワークまたはいくつかの他の機能性にアクセスすることを可能にすることができる。加えて、１つまたは両方のデバイスは、持ち運び可能であるか、またはある場合には、比較的持ち運び不能であり得ることが認識されるべきである。

【００２９】

当業者であれば、情報および信号は、さまざまな異なる技術および技法のうちのいずれかを使用して表されることができることを理解するだろう。例えば、上記の説明の全体にわたって言及されたデータ、命令、コマンド、情報、信号、ビット、シンボル、およびチップは、電圧、回路、電磁波、磁場または磁粒子、光波動場または光粒子、またはこれらのものの任意の組み合わせによって表されることができる。

【００３０】

当業者は、本明細書において開示された実施形態に関して説明された様々な例示的な論理ブロック、モジュール、回路、およびアルゴリズムステップは、電子的ハードウェア、コンピュータソフトウェア、または両方の組み合わせとして実装されることができることをさらに認識するだろう。ハードウェアおよびソフトウェアのこの互換性を明白に例示するために、様々な例示的なコンポーネント、ブロック、モジュール、回路、およびステップは、それらの機能性の観点から一般に上で説明されている。そのような機能性がハードウェアまたはソフトウェアとして実装されるかどうかは、全体のシステム上で課される特定のアプリケーションおよび設計の制約に依拠する。当業者は、各々の特定のアプリケーションについて様々な方法で、説明された機能性を実装することができるが、そのような実装決定は、本発明の範囲から逸脱していると解釈されるべきではない。

【００３１】

本明細書において開示された実施形態に関して説明された様々な例示的な論理ブロック、モジュール、および回路は、汎用目的プロセッサ、デジタル信号プロセッサ（DSP）、特定用途集積回路（ASIC）、フィールドプログラマブルゲートアレイ（FPGA）または他のプログラマブル論理デバイス、離散ゲートまたはトランジスタ論理、離散ハードウェア・コンポーネント、またはこれらのものの任意の組み合わせであって、本明細書に記載の機能を実行するように設計されたものによって実装または実行されることができる。汎用目的プロセッサは、マイクロプロセッサであってもよいが、その代わりに、任意の従来のプ

ロセッサ、コントローラ、マイクロコントローラ、または状態機械であってもよい。プロセッサはまた、コンピュータ計算デバイスの組み合わせ（例えば、DSPとマイクロプロセッサとの組み合わせ、複数のマイクロプロセッサ、DSPコアと結合した１つまたは複数のマイクロプロセッサ、または任意の他のそのような構成）として実装されることもできる。

【００３２】

本明細書において開示される実施形態と関係して説明された方法またはアルゴリズムのステップは、ハードウェア、プロセッサによって実行されるソフトウェア・モジュール、またはその２つの組み合わせにおいて直接具体化されることができる。ソフトウェア・モジュールは、RAMメモリ、フラッシュメモリ、ＲＯＭメモリ、ＥＰＲOMメモリ、EEPROMメモリ、レジスタ、ハードディスク、リムーバルディスク、CD-ROM、または当該技術分野において既知の記録媒体の任意の他の形式に存在してもよい。典型的な記録媒体は、プロセッサが記録媒体から情報を読み出す、または記録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ていてもよい。その代わりに、記録媒体は、プロセッサと一体化されていてもよい。プロセッサおよび記録媒体は、ASICに存在してもよい。ASICは、ユーザ端末に存在してもよい。代替的に、プロセッサおよび記録媒体は、ユーザ端末内の離散コンポーネントとして存在してもよい。

【００３３】

１つまたは複数の典型的な実施形態において、説明された機能は、ハードウェア、ソフトウェア、ファームウェア、またはそれらのものの任意の組み合わせにおいて実装されることができる。コンピュータ・プログラム・プロダクトとしてソフトウェアにおいて実装される場合、当該機能は、１つまたは複数の命令またはコードとしてコンピュータ可読媒体上に記憶されるか、または送信されることができる。コンピュータ可読媒体は、ある場所から他の場所へのコンピュータ・プログラムの転送を容易にする任意の媒体を含むコンピュータ記憶媒体および通信媒体の両方を含む。記録媒体は、コンピュータによってアクセスされることができる任意の利用可能な媒体であってもよい。事例として、かつ非制限的例として、そのようなコンピュータ可読媒体は、RAM、ROM、EEPROM、CD-ROMまたは他の光ディスク記憶装置、磁気ディスク記憶装置または他の磁気記憶デバイス、もしくは、任意の他の媒体であって、命令またはデータ構成の形式において所望のプログラムコードを伝達または記憶するために使用可能で、かつコンピュータによってアクセス可能な媒体を具備することができる。さらに、いかなる接続もコンピュータ可読媒体と適切に呼ばれる。例えば、もしソフトウェアがウェブサイト、サーバ、または他の遠くの情報源から、同軸ケーブル、光ファイバケーブル、ツイストペアケーブル、デジタル加入者線(DSL)またはワイヤレス技術（例えば、赤外線、無線およびマイクロ波など）を使用して送信されるのであれば、そうした同軸ケーブル、光ファイバケーブル、ツイストペアケーブル、ＤＳＬまたはワイヤレス技術（例えば、赤外線、無線およびマイクロ波など)もまた、媒体の定義に含まれる。本明細書において使用されるように、ディスク（disk and disc）は、コンパクトディスク（CD）、デジタルバーサタイルディスク(DVD)、フロッピー（登録商標）ディスクおよびブルーレイ(登録商標)ディスクを含む。ここで、diskは、通常、データを磁気的に再生するものをいい、discは、レーザを用いてデータを光学的に再生するものをいう。上記のものの組み合わせはまた、コンピュータ可読媒体の範囲内に含まれるべきである。

【００３４】

開示された実施形態の以前の説明は、当業者の誰もが本発明を作るまたは使用することができるように提供される。これらの実施形態に対する様々な修正は、当業者に直ちに明確となり、本明細書において定義された一般原則は、本発明の要旨または範囲から逸脱することなく他の実施形態に適用されることができる。したがって、本発明は、本明細書において示される実施形態に制限されるよう意図されないが、本明細書において開示された原則および新規の特徴と一致する最も広い範囲を与えられる。

【図１】

図 1

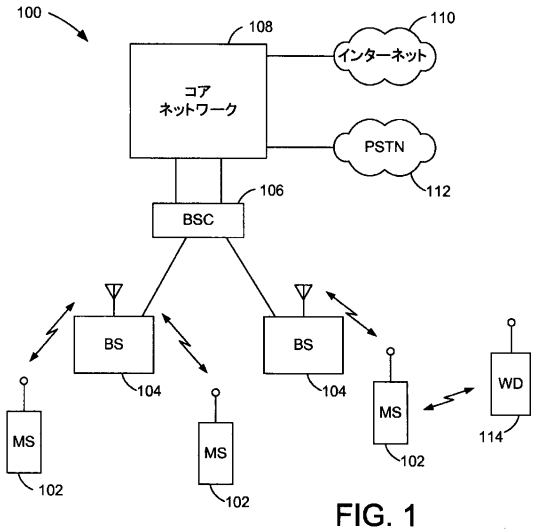


FIG. 1

【図２】

図 2

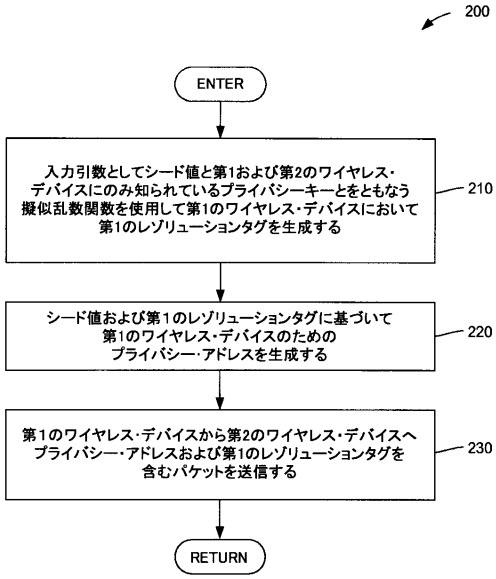


FIG. 2

【図３】

図 3

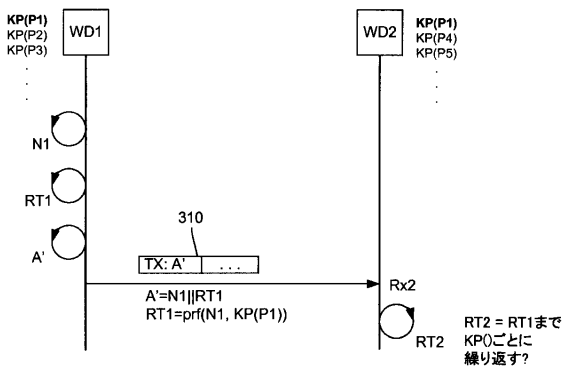


FIG. 3

【図４】

図 4

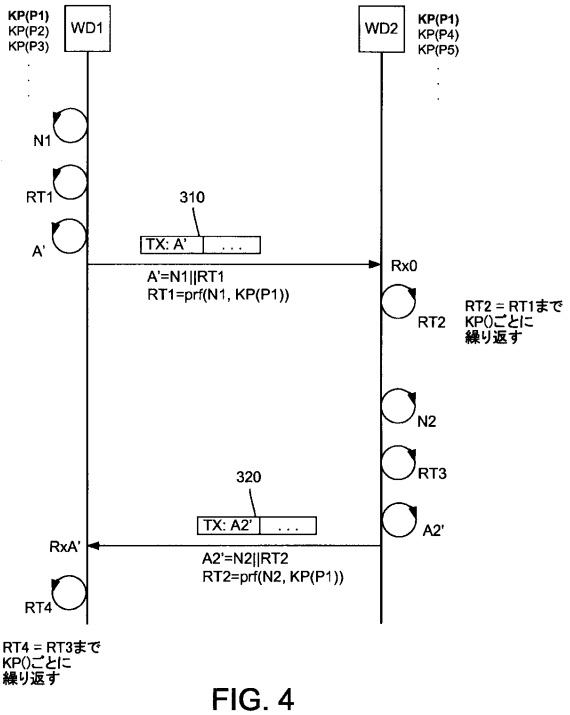
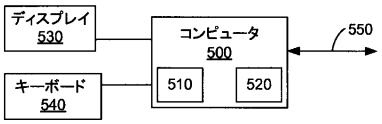


FIG. 4

【図５】

図５

FIG. 5



【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2010/029121

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L29/06 H04L29/12 H04W12/02
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 practical, search terms used)
EPO-Internal, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EP 1 871 135 A2 (NOKIA CORP [FI]) 26 December 2007 (2007-12-26) * abstract; figures 6a, 6b paragraph [0007] paragraph [0010] - paragraph [0013] paragraph [0057] - paragraph [0072] -----	1-35
X	WO 02/19599 A2 (LUCENT TECHNOLOGIES INC [US]; JAKOBSSON BJORN MARKUS [US]; WETZEL SUSA) 7 March 2002 (2002-03-07) * abstract page 2, line 19 - page 3, line 26 page 5, line 18 - page 7, line 10 page 13, line 8 - page 16, line 19 -----	1-35
	-/--	

[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 document 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
28 July 2010	04/08/2010

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	Figiel, Barbara

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

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2010/029121

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JAKOBSSON M ET AL: "Security weaknesses in Bluetooth" TOPICS IN CRYPTOLOGY - CT-RSA. THE CRYPTOGRAPHERS TRACK AT RSACONFERENCE. PROCEEDINGS, XX, XX, 8 April 2001 (2001-04-08), pages 176-191, XP002211423 the whole document	1-35

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/US2010/029121

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 1871135 A2	26-12-2007	US 2007293197 A1	20-12-2007
WO 0219599 A2	07-03-2002	AU 8531301 A	13-03-2002
		AU 8683701 A	13-03-2002
		DE 60129714 T2	30-04-2008
		EP 1314286 A2	28-05-2003
		EP 1329060 A2	23-07-2003
		JP 2004528735 T	16-09-2004
		JP 3860113 B2	20-12-2006
		JP 2004512709 T	22-04-2004
		WO 0219641 A2	07-03-2002

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,SD,SL,SZ,TZ,UG,ZM,ZW),EA(AM,AZ,BY,KG,KZ,MD,RU,TJ,TM),EP(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,SE,SI,SK,SM,TR),OA(BF,BJ,CF,CG,CI,CM,GA,GN,GQ,GW,ML,MR,NE,SN,TD,TG),AE,AG,AL,AM,AO,AT,AU,AZ,BA,BB,BG,BH,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,IS,JP,KE,KG,KM,KN,KP,KR,KZ,LA,LC,LK,LR,LS,LT,LU,LY,MA,MD,ME,MG,MK,MN,MW,MX,MY,MZ,NA,NG,NI,NO,NZ,OM,PE,PG,PH,PL,PT,RO,RS,RU,SC,SD,SE,SG,SK,SL,SM,ST,SV,SY,TH,TJ,TM,TN,TR,TT,TZ,UA,UG,US,UZ,VC,VN,ZA,ZM,ZW

(74)代理人 100109830
弁理士 福原 淑弘
(74)代理人 100075672
弁理士 峰 隆司
(74)代理人 100095441
弁理士 白根 俊郎
(74)代理人 100084618
弁理士 村松 貞男
(74)代理人 100103034
弁理士 野河 信久
(74)代理人 100119976
弁理士 幸長 保次郎
(74)代理人 100153051
弁理士 河野 直樹
(74)代理人 100140176
弁理士 砂川 克
(74)代理人 100158805
弁理士 井関 守三
(74)代理人 100124394
弁理士 佐藤 立志
(74)代理人 100112807
弁理士 岡田 貴志
(74)代理人 100111073
弁理士 堀内 美保子
(74)代理人 100134290
弁理士 竹内 将訓
(72)発明者 シャオ、ル
アメリカ合衆国、カリフォルニア州 ９２１２１、サン・ディエゴ、モアハウス・ドライブ ５７７５
(72)発明者 キム、ヨン・ジン
アメリカ合衆国、カリフォルニア州 ９２１２１、サン・ディエゴ、モアハウス・ドライブ ５７７５
(72)発明者 ジャ、ジャンフェン
アメリカ合衆国、カリフォルニア州 ９２１２１、サン・ディエゴ、モアハウス・ドライブ ５７７５
(72)発明者 ジュリアン、デイビッド・ジョナサン
アメリカ合衆国、カリフォルニア州 ９２１２１、サン・ディエゴ、モアハウス・ドライブ ５７７５

Ｆターム(参考) 5J104 AA12 AA16 AA32 EA04 EA08 EA18 FA00 JA03 LA01 NA02
NA12 NA37 PA07

5K067 AA30 BB04 BB21 CC08 DD11 DD17 EE02 EE10 EE25 FF02
FF07 HH22 HH23 HH36
5K201 AA08 AA10 CD09 EA07 ED05