【公報種別】特許法第１７条の２の規定による補正の掲載
【部門区分】第７部門第３区分
【発行日】平成28年3月24日(2016.3.24)

【公表番号】特表2015-510743(P2015-510743A)
【公表日】平成27年4月9日(2015.4.9)
【年通号数】公開・登録公報2015-023
【出願番号】特願2014-558887(P2014-558887)
【国際特許分類】
Ｈ０４Ｌ　9/32　(2006.01)
Ｈ０４Ｗ　84/10　(2009.01)
Ｈ０４Ｗ　12/08　(2009.01)
Ｇ０６Ｆ　21/44　(2013.01)
【ＦＩ】
Ｈ０４Ｌ　9/00　６７３Ｃ
Ｈ０４Ｗ　84/10　１１０
Ｈ０４Ｗ　12/08
Ｇ０６Ｆ　21/44

【手続補正書】
【提出日】平成28年2月3日(2016.2.3)
【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】
不明瞭にされた情報を含むメッセージの発信者をサーバが安全に識別するための方法であって、
共有秘密鍵をワイヤレス識別送信機に対応するデバイス識別子と関連付けることと、
ローリング識別子とノンスとを含む前記メッセージを受信することと、
前記受信されたメッセージから前記ローリング識別子と前記ノンスとを抽出することと、
復号されたデバイス識別子を生成するために、ストリーミングライク暗号化アルゴリズムと前記共有秘密鍵と前記ノンスとを使用して前記抽出されたローリング識別子を復号することと、
前記復号されたデバイス識別子が前記共有秘密鍵と関連付けられる前記デバイス識別子と一致するかどうかを決定することと、
前記復号されたデバイス識別子が前記ワイヤレス識別送信機と関連付けられる前記デバイス識別子と一致するとき、前記受信されたメッセージの前記発信者を前記ワイヤレス識別送信機として識別することと、
を備える方法。
【請求項２】
前記ストリーミングライク暗号化アルゴリズムはＡＥＳ－ＣＴＲ暗号である、請求項１に記載の方法。
【請求項３】
前記共有秘密鍵は１２８ビットのサイズを有する、請求項１に記載の方法。
【請求項４】
復号されたデバイス識別子を生成するために、ストリーミングライク暗号化アルゴリズ

ムと前記共有秘密鍵とを使用して前記抽出されたローリング識別子を復号することは、さらに、暗号化の前に前記デバイス識別子に連結されていたデータを復号することを備える、請求項１に記載の方法。
【請求項５】
識別情報の片方向通信を可能にするために不明瞭にされた情報を送信するワイヤレス識別送信機のための方法であって、
前記ワイヤレス識別送信機内でノンスを初期化することと、
サーバと共有される秘密鍵と前記ノンスとを使用してストリーミングライク暗号化アルゴリズムで前記ワイヤレス識別送信機と関連付けられるデバイス識別子を符号化することによって、ローリング識別子を生成することと、
短距離ワイヤレス送信を使用して、前記ローリング識別子と前記ノンスとを含むメッセージを定期的にブロードキャストすることと、
予め定義された間隔で前記ノンスをインクリメントすることと、
を備える方法。
【請求項６】
前記ノンスは、前記ワイヤレス識別送信機によって生成される繰り返されない数を表し、その値は、前記デバイス識別子の符号化が変化することが必要とされるたびに変化する、請求項５に記載の方法。
【請求項７】
前記ストリーミングライク暗号化アルゴリズムはＡＥＳ－ＣＴＲ暗号である、請求項５に記載の方法。
【請求項８】
前記メッセージは８０ビット以下のサイズを有する単一のパケットであり、前記秘密鍵は１２８ビットである、請求項５に記載の方法。
【請求項９】
不明瞭にされた情報を含むメッセージの発信者を安全に識別するように構成されるサーバであって、
共有秘密鍵をワイヤレス識別送信機に対応するデバイス識別子と関連付ける手段と、
ローリング識別子とノンスとを含む前記メッセージを受信する手段と、
前記受信されたメッセージから前記ローリング識別子と前記ノンスとを抽出する手段と、
復号されたデバイス識別子を生成するために、ストリーミングライク暗号化アルゴリズムと前記共有秘密鍵と前記ノンスとを使用して、前記抽出されたローリング識別子を復号する手段と、
前記復号されたデバイス識別子が前記共有秘密鍵と関連付けられる前記デバイス識別子と一致するかどうかを決定する手段と、
前記復号されたデバイス識別子が前記ワイヤレス識別送信機と関連付けられる前記デバイス識別子と一致するとき、前記受信されたメッセージの前記発信者を前記ワイヤレス識別送信機として識別する手段と、
を備えるサーバ。
【請求項１０】
識別情報の片方向通信を可能にするために不明瞭にされた情報を送信するように構成されるワイヤレス識別送信機であって、
前記ワイヤレス識別送信機内でノンスを初期化する手段と、
サーバと共有される秘密鍵と前記ノンスとを使用して、ストリーミングライク暗号化アルゴリズムで前記ワイヤレス識別送信機と関連付けられるデバイス識別子を符号化することによって、ローリング識別子を生成する手段と、
短距離ワイヤレス送信を使用して前記ローリング識別子と前記ノンスとを含むメッセージを定期的にブロードキャストする手段と、
予め定義された間隔で前記ノンスをインクリメントする手段と、

を備えるワイヤレス識別送信機。
【請求項１１】
サーバに、不明瞭にされた情報を含むメッセージの発信者を前記サーバが安全に識別するための動作を実行させるように構成されるサーバ実行可能命令を記憶した、非一時的サーバ可読記憶媒体であって、前記動作は、
共有秘密鍵をワイヤレス識別送信機に対応するデバイス識別子と関連付けることと、
ローリング識別子とノンスとを含む前記メッセージを受信することと、
前記受信されたメッセージから前記ローリング識別子と前記ノンスとを抽出することと、
復号されたデバイス識別子を生成するために、ストリーミングライク暗号化アルゴリズムと前記共有秘密鍵と前記ノンスとを使用して、前記抽出されたローリング識別子を復号することと、
前記復号されたデバイス識別子が前記共有秘密鍵と関連付けられる前記デバイス識別子と一致するかどうかを決定することと、
前記復号されたデバイス識別子が前記ワイヤレス識別送信機と関連付けられる前記デバイス識別子と一致するとき、前記受信されたメッセージの前記発信者を前記ワイヤレス識別送信機として識別することと、
を備える、非一時的サーバ可読記憶媒体。
【請求項１２】
識別情報の片方向通信を可能にするためにワイヤレス識別送信機が不明瞭にされた情報を送信するための動作をプロセッサに実行させるように構成される、プロセッサ実行可能ソフトウェア命令を記憶した非一時的プロセッサ可読記憶媒体であって、前記動作は、
前記ワイヤレス識別送信機内でノンスを初期化することと、
サーバと共有される秘密鍵と前記ノンスとを使用してストリーミングライク暗号化アルゴリズムで前記ワイヤレス識別送信機と関連付けられるデバイス識別子を符号化することによって、ローリング識別子を生成することと、
短距離ワイヤレス送信を使用して、前記ローリング識別子と前記ノンスとを含むメッセージを定期的にブロードキャストすることと、
予め定義された間隔で前記ノンスをインクリメントすることと、
を備える、非一時的プロセッサ可読記憶媒体。
【請求項１３】
サーバと、
ワイヤレス識別送信機と、
近隣ブロードキャスト受信機と、を備えるシステムであって、
前記ワイヤレス識別送信機は、
第１のメモリと、
前記近隣ブロードキャスト受信機によって受信されることが可能な短距離ワイヤレス信号をブロードキャストするように構成される第１の送受信機と、
前記第１のメモリおよび前記第１の送受信機に結合される第１のプロセッサと、を備え、前記第のプロセッサは、
前記ワイヤレス識別送信機内でノンスを初期化することと、
前記ワイヤレス識別送信機と関連付けられるデバイス識別子と、前記サーバと共有される秘密鍵と、前記ノンスとを、ストリーミングライク暗号化アルゴリズムで符号化することによって、ローリング識別子を生成することと、
前記第１の送受信機を介して、短距離ワイヤレス送信を使用して、前記ローリング識別子と前記ノンスとを含むメッセージを定期的にブロードキャストすることと、
予め定義された間隔で前記ノンスをインクリメントすることと、
を備える動作を実行するプロセッサ実行可能命令によって構成され、
前記近隣ブロードキャスト受信機は、
第２のメモリと、

前記ワイヤレス識別送信機と短距離ワイヤレス信号を交換するように構成される第２の送受信機と、
前記サーバと信号を交換するように構成されるネットワークデバイスと、
前記第２のメモリ、前記第２の送受信機、および前記ネットワークデバイスに結合された第２のプロセッサと、を備え、前記第２のプロセッサは、
前記第２の送受信機を介して、前記ワイヤレス識別送信機から前記ローリング識別子と前記ノンスとを含む前記メッセージを受信することと、
前記ネットワークデバイスを介して、前記ローリング識別子と前記ノンスとを含むサイティングメッセージを前記サーバに送信することと、
を備える動作を実行するプロセッサ実行可能命令によって構成され、
前記サーバは、
前記秘密鍵を前記ワイヤレス識別送信機に対応する前記デバイス識別子と関連付けることと、
前記ローリング識別子と前記ノンスとを含む前記サイティングメッセージを受信することと、
前記受信されたサイティングメッセージから前記ノンスと前記ローリング識別子とを抽出することと、
復号されたデバイス識別子を生成するために、前記ストリーミングライク暗号化アルゴリズムと、前記秘密鍵と、前記抽出されたノンスとを使用して、前記抽出されたローリング識別子を復号することと、
前記復号されたデバイス識別子が前記秘密鍵と関連付けられる前記デバイス識別子と一致するかどうかを決定することと、
前記復号されたデバイス識別子が前記ワイヤレス識別送信機と関連付けられる前記デバイス識別子と一致するとき、前記受信されたメッセージの発信者を前記ワイヤレス識別送信機として識別することと、
を備える動作を実行するサーバ実行可能命令によって構成される、システム。
【手続補正２】
【補正対象書類名】明細書
【補正対象項目名】０３２２
【補正方法】変更
【補正の内容】
【０３２２】
[0348]開示された実施形態の上記の説明は、当業者が本発明を製作または使用することを可能にするように提供されたものである。これらの実施形態への様々な修正は当業者には容易に明らかであり、本明細書で定義された一般原理は、本発明の趣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得る。したがって、本発明は、本明細書で示された実施形態に限定されるものではなく、以下の特許請求の範囲ならびに本明細書で開示される原理および新規の特徴に合致する最も広い範囲を与えられるべきである。
以下に本願出願当初の特許請求の範囲を付記する。
[Ｃ１]　不明瞭にされた情報を含むメッセージの発信者をサーバが安全に識別するための方法であって、
共有秘密鍵をワイヤレス識別送信機に対応するデバイス識別子と関連付けることと、
ローリング識別子を含む前記メッセージを受信することと、
前記受信されたメッセージから前記ローリング識別子を抽出することと、
復号されたデバイス識別子を生成するために、ストリーミングライク暗号化アルゴリズムと前記共有秘密鍵とを使用して前記抽出されたローリング識別子を復号することと、
前記復号されたデバイス識別子が前記共有秘密鍵と関連付けられる前記デバイス識別子と一致するかどうかを決定することと、
前記復号されたデバイス識別子が前記ワイヤレス識別送信機と関連付けられる前記デバイス識別子と一致するとき、前記受信されたメッセージの前記発信者を前記ワイヤレス識

別送信機として識別することと、
を備える方法。
[Ｃ２] 前記メッセージはさらにノンスを含み、
復号されたデバイス識別子を生成するために、ストリーミングライク暗号化アルゴリズムと前記共有秘密鍵とを使用して前記抽出されたローリング識別子を復号することは、
前記復号されたデバイス識別子を生成するために、ストリーミングライク暗号化アルゴリズムと、前記メッセージから抽出された前記ノンスと、前記共有秘密鍵とを使用して前記抽出されたローリング識別子を復号することを備える、Ｃ１に記載の方法。
[Ｃ３] 前記ストリーミングライク暗号化アルゴリズムはＡＥＳ－ＣＴＲ暗号である、Ｃ１に記載の方法。
[Ｃ４] 前記共有秘密鍵は１２８ビットのサイズを有する、Ｃ１に記載の方法。
[Ｃ５] 復号されたデバイス識別子を生成するために、ストリーミングライク暗号化アルゴリズムと前記共有秘密鍵とを使用して前記抽出されたローリング識別子を復号することは、さらに、暗号化の前に前記デバイス識別子に連結されていたデータを復号することを備える、Ｃ１に記載の方法。
[Ｃ６] 識別情報の片方向通信を可能にするために不明瞭にされた情報を送信するワイヤレス識別送信機のための方法であって、
前記ワイヤレス識別送信機内でノンスを初期化することと、
サーバと共有される秘密鍵と前記ノンスとを使用してストリーミングライク暗号化アルゴリズムで前記ワイヤレス識別送信機と関連付けられるデバイス識別子を符号化することによって、ローリング識別子を生成することと、
短距離ワイヤレス送信を使用して、前記ローリング識別子を含むメッセージを定期的にブロードキャストすることと、
予め定義された間隔で前記ノンスをインクリメントすることと、
を備える方法。
[Ｃ７] 前記定期的にブロードキャストされるメッセージはさらに前記ノンスを含む、Ｃ６に記載の方法。
[Ｃ８] 前記ノンスは、前記ワイヤレス識別送信機によって生成される繰り返されない数を表し、その値は、前記デバイス識別子の符号化が変化することが必要とされるたびに変化する、Ｃ６に記載の方法。
[Ｃ９] 前記ストリーミングライク暗号化アルゴリズムはＡＥＳ－ＣＴＲ暗号である、Ｃ６に記載の方法。
[Ｃ１０] 前記メッセージは８０ビット以下のサイズを有する単一のパケットであり、前記秘密鍵は１２８ビットである、Ｃ６に記載の方法。
[Ｃ１１] 前記ローリング識別子を生成することは、送信されるべきデータを前記デバイス識別子に連結することと、サーバと共有される前記秘密鍵と前記ノンスとを使用して前記ストリーミングライク暗号化アルゴリズムで前記連結された識別子とデータとを符号化することと、を備える、Ｃ６に記載の方法。
[Ｃ１２] 不明瞭にされた情報を含むメッセージの発信者をサーバが安全に識別するための方法であって、
共有秘密鍵をワイヤレス識別送信機についてのノンスおよびデバイス識別子と関連付けることと、
ローリング識別子を含む前記メッセージを受信することと、
前記受信されたメッセージから前記ローリング識別子を抽出することと、
前記サーバの現在の時間を表すために、前記ノンスをインクリメントすることと、
サーバ暗号化データを生成するために、前記共有秘密鍵と、前記ノンスと、擬似ランダム関数とを使用して、前記デバイス識別子を符号化することと、
前記サーバ暗号化データが前記抽出されたローリング識別子と一致するかどうかを決定することと、
前記サーバ暗号化データが前記抽出されたローリング識別子と一致するとき、前記受信

されたメッセージの前記発信者を前記ワイヤレス識別送信機として識別することと、
を備える方法。
[Ｃ１３] 前記擬似ランダム関数は、鍵付きハッシュメッセージ認証コード（ＨＭＡＣ）または暗号ベースのメッセージ認証コード（ＣＭＡＣ）のうちの１つである、Ｃ１２に記載の方法。
[Ｃ１４] 前記サーバの現在の時間を表すために、前記ノンスをインクリメントすることは、前記メッセージ内に含まれる情報に基づいて、前記ワイヤレス識別送信機からのブロードキャストを近隣ブロードキャスト受信機が受信した時間に対応するように前記ノンスを計算することを備える、Ｃ１２に記載の方法。
[Ｃ１５] 前記受信されたメッセージからノンスを抽出することをさらに備え、前記デバイス識別子を符号化することは、前記受信されたメッセージから抽出された前記ノンスを使用する、Ｃ１２に記載の方法。
[Ｃ１６] 識別情報の片方向通信を可能にするために不明瞭にされた情報を送信するワイヤレス識別送信機のための方法であって、
前記ワイヤレス識別送信機内でノンスを初期化することと、
サーバと共有される秘密鍵と前記ノンスとに基づいて前記ワイヤレス識別送信機と関連付けられるデバイス識別子を符号化するために、擬似ランダム関数を使用することにより、ローリング識別子を生成することと、
短距離ワイヤレス送信を使用して前記ローリング識別子を含むメッセージを定期的にブロードキャストすることと、
前記ワイヤレス識別送信機の現在の時間を維持するために、予め定義された間隔で前記ノンスをインクリメントすることと、
を備える方法。
[Ｃ１７] 擬似ランダム関数を使用することによってローリング識別子を生成することは、送信されるべきデータを前記デバイス識別子に連結することと、サーバと共有される前記秘密鍵と前記ノンスとに基づいて前記連結されたデバイス識別子とデータとを符号化するために、前記擬似ランダム関数を使用することと、を備える、Ｃ１６に記載の方法。
[Ｃ１８] 前記擬似ランダム関数は、鍵付きハッシュメッセージ認証コード（ＨＭＡＣ）または暗号ベースのメッセージ認証コード（ＣＭＡＣ）のうちの１つである、Ｃ１６に記載の方法。
[Ｃ１９] 不明瞭にされた情報を含むメッセージの発信者をサーバが安全に識別するための方法であって、
ワイヤレス識別送信機についてのデバイス識別子を、初期ノンスと、現在ノンスと、第１の秘密鍵と、第２の秘密鍵とに関連付けることと、
前記第２の秘密鍵および前記現在ノンスとともに擬似ランダム関数を使用して、複数の符号化ノンスを予め計算することと、
ローリング識別子と符号化ノンスとを含む前記メッセージを受信することと、
前記受信されたメッセージから前記符号化ノンスを抽出することと、
前記受信されたメッセージから前記ローリング識別子を抽出することと、
前記抽出された符号化ノンスを前記複数の予め計算された符号化ノンスと比較することと、
前記抽出された符号化ノンスが前記複数の予め計算された符号化ノンスのいずれかと一致するとき、復号されたデバイス識別子を生成するために、ストリーミングライク暗号化アルゴリズムと、前記第１の秘密鍵と、前記抽出された符号化ノンスと一致する予め計算された符号化ノンスと関連付けられるノンスとを使用して、前記抽出されたローリング識別子を復号することと、
前記抽出された符号化ノンスが前記複数の予め計算された符号化ノンスのうちの１つと一致しないとき、前記復号されたデバイス識別子を生成するために、前記ストリーミングライク暗号化アルゴリズムと、前記第１の秘密鍵と、前記ワイヤレス識別送信機と関連付けられる前記初期ノンスとを使用して、前記抽出されたローリング識別子を復号すること

と、
前記復号されたデバイス識別子が前記ワイヤレス識別送信機の前記デバイス識別子と一致するとき、前記受信されたメッセージの前記発信者を前記ワイヤレス識別送信機として識別することと、
を備える方法。
[Ｃ２０] 前記第１の秘密鍵と前記第２の秘密鍵とは同じ値を有する、Ｃ１９に記載の方法。
[Ｃ２１] 識別情報の片方向通信を可能にするために不明瞭にされた情報を送信するワイヤレス識別送信機のための方法であって、
前記ワイヤレス識別送信機内でノンスを初期化することと、
前記ワイヤレス識別送信機と関連付けられるデバイス識別子と、サーバと共有される第１の秘密鍵と、前記ノンスとをストリーミングライク暗号化アルゴリズムで符号化することによって、ローリング識別子を生成することと、
前記サーバと共有される第２の秘密鍵とともに擬似ランダム関数を使用して前記ノンスを符号化することによって、符号化されたノンスを生成することと、
短距離ワイヤレス送信を使用して前記ローリング識別子と前記符号化されたノンスとを含むメッセージを定期的にブロードキャストすることと、
前記ワイヤレス識別送信機の現在の時間を維持するために、予め定義された間隔で前記ノンスをインクリメントすることと、
を備える方法。
[Ｃ２２] メッセージの発信者をサーバが安全に識別するための方法であって、
ワイヤレス識別送信機についてのデバイス識別子を、初期ノンスと、現在ノンスと、第１の秘密鍵と、第２の秘密鍵とに関連付けることと、
前記第２の秘密鍵および前記現在ノンスとともに、擬似ランダム関数を使用して、複数の符号化ノンスを予め計算することと、
前記第１の秘密鍵、前記現在ノンス、および前記デバイス識別子とともに、ストリーミングライク暗号化アルゴリズムを使用して、複数の符号化されたデバイス識別子を予め計算することと、
ローリング識別子と符号化ノンスとを含む前記メッセージを受信することと、
前記受信されたメッセージから前記符号化ノンスを抽出することと、
前記受信されたメッセージから前記ローリング識別子を抽出することと、
前記抽出された符号化ノンスを前記複数の予め計算された符号化ノンスと比較することと、
前記抽出された符号化ノンスが前記複数の予め計算された符号化ノンスのいずれかと一致するとき、前記抽出されたローリング識別子を前記複数の予め計算された符号化されたデバイス識別子と比較することと、
前記抽出されたローリング識別子が前記複数の予め計算された符号化されたデバイス識別子のいずれかと一致するとき、前記受信されたメッセージの前記発信者を前記ワイヤレス識別送信機として識別することと、
を備える方法。
[Ｃ２３] メッセージの発信者をサーバが安全に識別するための方法であって、
暗号化アルゴリズム、共有秘密鍵、初期ノンス、およびワイヤレス識別送信機と関連付けられるデバイス識別子で、複数の初期モデルペイロードを生成することと、前記暗号化アルゴリズムは前記ワイヤレス識別送信機と共有され、
前記暗号化アルゴリズム、前記共有秘密鍵、現在ノンス、および前記ワイヤレス識別送信機と関連付けられる前記デバイス識別子で、複数の現在モデルペイロードを生成することと、
不明瞭にされた識別情報をもつペイロードを含む前記メッセージを受信することと、
前記受信されたメッセージの前記ペイロードを前記複数の現在モデルペイロードと比較することと、

前記受信されたメッセージの前記ペイロードが前記複数の現在モデルペイロードのうちの１つと一致するとき、前記ワイヤレス識別送信機を識別することと、
前記受信されたメッセージの前記ペイロードが前記複数の現在モデルペイロードのいずれとも一致しないとき、前記受信されたメッセージの前記ペイロードを前記複数の初期モデルペイロードと比較することと、
前記受信されたメッセージの前記ペイロードが前記複数の初期モデルペイロードのうちの１つと一致するとき、前記ワイヤレス識別送信機を識別することと、
前記受信されたメッセージの前記ペイロードが、初期モデルペイロードと現在モデルペイロードとのうちの少なくとも１つと一致するとき、前記ワイヤレス識別送信機と関連付けられる前記現在ノンスを更新することと、
を備える、方法。
[Ｃ２４] 入来するメッセージを受信する、ワイヤレス識別送信機のための方法であって、
第１の期間に、短距離ワイヤレス送信を介して、入来する送信を受信することが可能かどうかを示すメッセージを、定期的にブロードキャストすることと、
前記第１の期間が満了したことに応答して、第２の期間の間にリンクアドバタイズメントメッセージを受信することと、
前記受信されたリンクアドバタイズメントメッセージ内の情報に基づいて、近隣ブロードキャスト受信機とのリンクをネゴシエートすることと、
前記ネゴシエートされたリンクを認証することと、
前記ネゴシエートされたリンクを介して入来するメッセージを処理することと、
を備え、
前記ネゴシエートされたリンクはＢｌｕｅｔｏｏｔｈペアリングにより実行される、方法。
[Ｃ２５] 前記入来するメッセージは、ファームウェアの更新、構成情報、トリガ信号、およびソフトウェア命令のうちの少なくとも１つを含む、Ｃ２４に記載の方法。
[Ｃ２６] 前記第１の期間は、前記ワイヤレス識別送信機上のタイマー、時計信号、および前記近隣ブロードキャスト受信機からの受信されたメッセージのうちの少なくとも１つによって定義される、Ｃ２４に記載の方法。
[Ｃ２７] 不明瞭にされた情報を含むメッセージの発信者を安全に識別するように構成されるサーバであって、
共有秘密鍵をワイヤレス識別送信機に対応するデバイス識別子と関連付ける手段と、
ローリング識別子を含む前記メッセージを受信する手段と、
前記受信されたメッセージから前記ローリング識別子を抽出する手段と、
復号されたデバイス識別子を生成するために、ストリーミングライク暗号化アルゴリズムと前記共有秘密鍵とを使用して、前記抽出されたローリング識別子を復号する手段と、
前記復号されたデバイス識別子が前記共有秘密鍵と関連付けられる前記デバイス識別子と一致するかどうかを決定する手段と、
前記復号されたデバイス識別子が前記ワイヤレス識別送信機と関連付けられる前記デバイス識別子と一致するとき、前記受信されたメッセージの前記発信者を前記ワイヤレス識別送信機として識別する手段と、
を備えるサーバ。
[Ｃ２８] 前記メッセージはさらにノンスを含み、
復号されたデバイス識別子を生成するために、ストリーミングライク暗号化アルゴリズムと前記共有秘密鍵とを使用して、前記抽出されたローリング識別子を復号する手段は、
前記復号されたデバイス識別子を生成するために、ストリーミングライク暗号化アルゴリズムと、前記メッセージから抽出された前記ノンスと、前記共有秘密鍵とを使用して、前記抽出されたローリング識別子を復号する手段を備える、Ｃ２７に記載のサーバ。
[Ｃ２９] 前記ストリーミングライク暗号化アルゴリズムはＡＥＳ－ＣＴＲ暗号である、Ｃ２７に記載のサーバ。

[Ｃ３０] 前記共有秘密鍵は１２８ビットのサイズを有する、Ｃ２７に記載のサーバ。
[Ｃ３１] 復号されたデバイス識別子を生成するために、ストリーミングライク暗号化アルゴリズムと前記共有秘密鍵とを使用して、前記抽出されたローリング識別子を復号する手段は、さらに、暗号化の前に前記デバイス識別子に連結されていたデータを復号する手段を備える、Ｃ２７に記載のサーバ。
[Ｃ３２] 識別情報の片方向通信を可能にするために不明瞭にされた情報を送信するように構成されるワイヤレス識別送信機であって、
前記ワイヤレス識別送信機内でノンスを初期化する手段と、
サーバと共有される秘密鍵と前記ノンスとを使用して、ストリーミングライク暗号化アルゴリズムで前記ワイヤレス識別送信機と関連付けられるデバイス識別子を符号化することによって、ローリング識別子を生成する手段と、
短距離ワイヤレス送信を使用して前記ローリング識別子を含むメッセージを定期的にブロードキャストする手段と、
予め定義された間隔で前記ノンスをインクリメントする手段と、
を備えるワイヤレス識別送信機。
[Ｃ３３] 前記定期的にブロードキャストされるメッセージは、さらに前記ノンスを含む、Ｃ３２に記載のワイヤレス識別送信機。
[Ｃ３４] 前記ノンスは、前記ワイヤレス識別送信機によって生成される繰り返されない数を表し、その値は、前記デバイス識別子の符号化が変化することが必要とされるたびに変化する、Ｃ３２に記載のワイヤレス識別送信機。
[Ｃ３５] 前記ストリーミングライク暗号化アルゴリズムはＡＥＳ－ＣＴＲ暗号である、Ｃ３２に記載のワイヤレス識別送信機。
[Ｃ３６] 前記メッセージは８０ビット以下のサイズを有する単一のパケットであり、前記秘密鍵は１２８ビットである、Ｃ３２に記載のワイヤレス識別送信機。
[Ｃ３７] 前記ローリング識別子を生成する手段は、送信されるべきデータを前記デバイス識別子に連結し、サーバと共有される前記秘密鍵と前記ノンスとを使用して前記ストリーミングライク暗号化アルゴリズムで前記連結された識別子とデータとを符号化する手段を備える、Ｃ３２に記載のワイヤレス識別送信機。
[Ｃ３８] 不明瞭にされた情報を含むメッセージの発信者を安全に識別するように構成されるサーバであって、
共有秘密鍵をワイヤレス識別送信機についてのノンスおよびデバイス識別子と関連付ける手段と、
ローリング識別子を含む前記メッセージを受信する手段と、
前記受信されたメッセージから前記ローリング識別子を抽出する手段と、
前記サーバの現在の時間を表すために、前記ノンスをインクリメントする手段と、
サーバ暗号化データを生成するために、前記共有秘密鍵と、前記ノンスと、擬似ランダム関数とを使用して、前記デバイス識別子を符号化する手段と、
前記サーバ暗号化データが前記抽出されたローリング識別子と一致するかどうかを決定する手段と、
前記サーバ暗号化データが前記抽出されたローリング識別子と一致するとき、前記受信されたメッセージの前記発信者を前記ワイヤレス識別送信機として識別する手段と、
を備える、サーバ。
[Ｃ３９] 前記擬似ランダム関数は、鍵付きハッシュメッセージ認証コード（ＨＭＡＣ）または暗号ベースのメッセージ認証コード（ＣＭＡＣ）のうちの１つである、Ｃ３８に記載のサーバ。
[Ｃ４０] 前記サーバの現在の時間を表すために、前記ノンスをインクリメントする手段は、前記メッセージ内に含まれる情報に基づいて、前記ワイヤレス識別送信機からのブロードキャストを近隣ブロードキャスト受信機が受信した時間に対応するように前記ノンスを計算する手段を備える、Ｃ３８に記載のサーバ。
[Ｃ４１] 前記受信されたメッセージからノンスを抽出する手段をさらに備え、前記デバ

イス識別子を符号化する手段が、前記受信されたメッセージから抽出された前記ノンスを使用する、Ｃ３８に記載のサーバ。
[Ｃ４２] 識別情報の片方向通信を可能にするために不明瞭にされた情報を送信するように構成されるワイヤレス識別送信機であって、
前記ワイヤレス識別送信機内でノンスを初期化する手段と、
サーバと共有される秘密鍵と前記ノンスとに基づいて前記ワイヤレス識別送信機と関連付けられるデバイス識別子を符号化するために、擬似ランダム関数を使用することにより、ローリング識別子を生成する手段と、
短距離ワイヤレス送信を使用して前記ローリング識別子を含むメッセージを定期的にブロードキャストする手段と、
前記ワイヤレス識別送信機の現在の時間を維持するために、予め定義された間隔で前記ノンスをインクリメントする手段と、
を備える、ワイヤレス識別送信機。
[Ｃ４３] 擬似ランダム関数を使用することによってローリング識別子を生成する手段は、送信されるべきデータを前記デバイス識別子に連結し、サーバと共有される前記秘密鍵と前記ノンスとに基づいて前記連結されたデバイス識別子とデータとを符号化するために、前記擬似ランダム関数を使用する手段を備える、Ｃ４２に記載のワイヤレス識別送信機。
[Ｃ４４] 前記擬似ランダム関数は、鍵付きハッシュメッセージ認証コード（ＨＭＡＣ）または暗号ベースのメッセージ認証コード（ＣＭＡＣ）のうちの１つである、Ｃ４２に記載のワイヤレス識別送信機。
[Ｃ４５] 不明瞭にされた情報を含むメッセージの発信者を安全に識別するように構成されるサーバであって、
ワイヤレス識別送信機についてのデバイス識別子を、初期ノンスと、現在ノンスと、第１の秘密鍵と、第２の秘密鍵とに関連付ける手段と、
前記第２の秘密鍵および前記現在ノンスとともに、擬似ランダム関数を使用して、複数の符号化ノンスを予め計算する手段と、
ローリング識別子と符号化ノンスとを含む前記メッセージを受信する手段と、
前記受信されたメッセージから前記符号化ノンスを抽出する手段と、
前記受信されたメッセージから前記ローリング識別子を抽出する手段と、
前記抽出された符号化ノンスを前記複数の予め計算された符号化ノンスと比較する手段と、
前記抽出された符号化ノンスが前記複数の予め計算された符号化ノンスのいずれかと一致するとき、復号されたデバイス識別子を生成するために、ストリーミングライク暗号化アルゴリズムと、前記第１の秘密鍵と、前記抽出された符号化ノンスと一致する予め計算された符号化ノンスと関連付けられるノンスとを使用して、前記抽出されたローリング識別子を復号する手段と、
前記抽出された符号化ノンスが前記複数の予め計算された符号化ノンスのうちの１つと一致しないとき、前記復号されたデバイス識別子を生成するために、前記ストリーミングライク暗号化アルゴリズムと、前記第１の秘密鍵と、前記ワイヤレス識別送信機と関連付けられる前記初期ノンスとを使用して、前記抽出されたローリング識別子を復号する手段と、
前記復号されたデバイス識別子が前記ワイヤレス識別送信機の前記デバイス識別子と一致するとき、前記受信されたメッセージの前記発信者を前記ワイヤレス識別送信機として識別する手段と、
を備えるサーバ。
[Ｃ４６] 前記第１の秘密鍵と前記第２の秘密鍵とは同じ値を有する、Ｃ４５に記載のサーバ。
[Ｃ４７] 識別情報の片方向通信を可能にするために不明瞭にされた情報を送信するように構成されるワイヤレス識別送信機であって、

前記ワイヤレス識別送信機内でノンスを初期化する手段と、
前記ワイヤレス識別送信機と関連付けられるデバイス識別子と、サーバと共有される第１の秘密鍵と、前記ノンスとをストリーミングライク暗号化アルゴリズムで符号化することによって、ローリング識別子を生成する手段と、
前記サーバと共有される第２の秘密鍵とともに擬似ランダム関数を使用して前記ノンスを符号化することによって、符号化されたノンスを生成する手段と、
短距離ワイヤレス送信を使用して前記ローリング識別子と前記符号化されたノンスとを含むメッセージを定期的にブロードキャストするための手段と、
前記ワイヤレス識別送信機の現在の時間を維持するために、予め定義された間隔で前記ノンスをインクリメントする手段と、
を備える、ワイヤレス識別送信機。
[Ｃ４８] メッセージの発信者を安全に識別するように構成されるサーバであって、
ワイヤレス識別送信機についてのデバイス識別子を、初期ノンスと、現在ノンスと、第１の秘密鍵と、第２の秘密鍵とに関連付ける手段と、
前記第２の秘密鍵および前記現在ノンスとともに、擬似ランダム関数を使用して、複数の符号化ノンスを予め計算する手段と、
前記第１の秘密鍵、前記現在ノンス、および前記デバイス識別子とともに、ストリーミングライク暗号化アルゴリズムを使用して、複数の符号化されたデバイス識別子を予め計算する手段と、
ローリング識別子と符号化ノンスとを含む前記メッセージを受信する手段と、
前記受信されたメッセージから前記符号化ノンスを抽出する手段と、
前記受信されたメッセージから前記ローリング識別子を抽出する手段と、
前記抽出された符号化ノンスを前記複数の予め計算された符号化ノンスと比較する手段と、
前記抽出された符号化ノンスが前記複数の予め計算された符号化ノンスのいずれかと一致するとき、前記抽出されたローリング識別子を前記複数の予め計算された符号化されたデバイス識別子と比較する手段と、
前記抽出されたローリング識別子が前記複数の予め計算された符号化されたデバイス識別子のいずれかと一致するとき、前記受信されたメッセージの前記発信者を前記ワイヤレス識別送信機として識別する手段と、
を備えるサーバ。
[Ｃ４９] メッセージの発信者を識別するように構成されるサーバであって、
暗号化アルゴリズム、共有秘密鍵、初期ノンス、およびワイヤレス識別送信機と関連付けられるデバイス識別子で、複数の初期モデルペイロードを生成する手段と、前記暗号化アルゴリズムは前記ワイヤレス識別送信機と共有され、
前記暗号化アルゴリズム、前記共有秘密鍵、現在ノンス、および前記ワイヤレス識別送信機と関連付けられる前記デバイス識別子で、複数の現在モデルペイロードを生成する手段と、
不明瞭にされた識別情報をもつペイロードを含む前記メッセージを受信する手段と、
前記受信されたメッセージの前記ペイロードを前記複数の現在モデルペイロードと比較する手段と、
前記受信されたメッセージの前記ペイロードが前記複数の現在モデルペイロードのうちの１つと一致するとき、前記ワイヤレス識別送信機を識別する手段と、
前記受信されたメッセージの前記ペイロードが前記複数の現在モデルペイロードのいずれとも一致しないとき、前記受信されたメッセージの前記ペイロードを前記複数の初期モデルペイロードと比較する手段と、
前記受信されたメッセージの前記ペイロードが前記複数の初期モデルペイロードのうちの１つと一致するとき、前記ワイヤレス識別送信機を識別する手段と、
前記受信されたメッセージの前記ペイロードが、初期モデルペイロードと現在モデルペイロードのうちの少なくとも１つと一致するとき、前記ワイヤレス識別送信機と関連付け

られる前記現在ノンスを更新する手段と、
を備えるサーバ。
[Ｃ５０] 入来するメッセージを受信するように構成されるワイヤレス識別送信機であって、
第１の期間に、短距離ワイヤレス送信を介して、入来する送信を受信することが可能かどうかを示すメッセージを、定期的にブロードキャストする手段と、
前記第１の期間が満了したことに応答して、第２の期間の間にリンクアドバタイズメントメッセージを受信する手段と、
前記受信されたリンクアドバタイズメントメッセージ内の情報に基づいて、近隣ブロードキャスト受信機とのリンクをネゴシエートする手段と、
前記ネゴシエートされたリンクを認証する手段と、
前記ネゴシエートされたリンクを介して入来するメッセージを処理する手段と、
を備え、
前記ネゴシエートされたリンクはＢｌｕｅｔｏｏｔｈペアリングにより実行される、ワイヤレス識別送信機。
[Ｃ５１] 前記入来するメッセージは、ファームウェアの更新、構成情報、トリガ信号、およびソフトウェア命令のうちの少なくとも１つを含む、Ｃ５０に記載のワイヤレス識別送信機。
[Ｃ５２] 前記第１の期間は、前記ワイヤレス識別送信機上のタイマー、時計信号、および前記近隣ブロードキャスト受信機からの受信されたメッセージのうちの少なくとも１つによって定義される、Ｃ５０に記載のワイヤレス識別送信機。
[Ｃ５３] 不明瞭にされた情報を含むメッセージの発信者を安全に識別するように構成されるサーバであって、
メモリと、
前記メモリに結合されたサーバプロセッサと、を備え、前記サーバプロセッサは、
共有秘密鍵をワイヤレス識別送信機に対応するデバイス識別子と関連付けることと、
ローリング識別子を含む前記メッセージを受信することと、
前記受信されたメッセージから前記ローリング識別子を抽出することと、
復号されたデバイス識別子を生成するために、ストリーミングライク暗号化アルゴリズムと前記共有秘密鍵とを使用して、前記抽出されたローリング識別子を復号することと、
前記復号されたデバイス識別子が前記共有秘密鍵と関連付けられる前記デバイス識別子と一致するかどうかを決定することと、
前記復号されたデバイス識別子が前記ワイヤレス識別送信機と関連付けられる前記デバイス識別子と一致するとき、前記受信されたメッセージの前記発信者を前記ワイヤレス識別送信機として識別することと、
を備える動作を実行する、サーバプロセッサ実行可能命令によって構成される、サーバ。
[Ｃ５４] 前記メッセージはさらにノンスを含み、
前記サーバプロセッサは、
復号されたデバイス識別子を生成するために、ストリーミングライク暗号化アルゴリズムと前記共有秘密鍵とを使用して、前記抽出されたローリング識別子を復号することが、
前記復号されたデバイス識別子を生成するために、ストリーミングライク暗号化アルゴリズムと、前記メッセージから抽出された前記ノンスと、前記共有秘密鍵とを使用して、前記抽出されたローリング識別子を復号することを備えるように、動作を実行するサーバプロセッサ実行可能命令によって構成される、Ｃ５３に記載の方法。
[Ｃ５５] 前記ストリーミングライク暗号化アルゴリズムはＡＥＳ－ＣＴＲ暗号である、Ｃ５３に記載のサーバ。
[Ｃ５６] 前記共有秘密鍵は１２８ビットのサイズを有する、Ｃ５３に記載のサーバ。
[Ｃ５７] 前記サーバプロセッサは、

復号されたデバイス識別子を生成するために、ストリーミングライク暗号化アルゴリズムと前記共有秘密鍵とを使用して、前記抽出されたローリング識別子を復号することが、さらに、暗号化の前に前記デバイス識別子に連結されていたデータを復号することを備えるように、動作を実行するサーバプロセッサ実行可能命令によって構成される、Ｃ５３に記載のサーバ。

[Ｃ５８] 識別情報の片方向通信を可能にするために不明瞭にされた情報を送信するように構成されるワイヤレス識別送信機であって、

メモリと、

前記メモリに結合されたプロセッサと、を備え、前記プロセッサは、

前記ワイヤレス識別送信機内でノンスを初期化することと、

サーバと共有される秘密鍵と前記ノンスとを使用してストリーミングライク暗号化アルゴリズムで前記ワイヤレス識別送信機と関連付けられるデバイス識別子を符号化することによって、ローリング識別子を生成することと、

短距離ワイヤレス送信を使用して前記ローリング識別子を含むメッセージを定期的にブロードキャストすることと、

予め定義された間隔で前記ノンスをインクリメントすることと、

を備える動作を実行する、プロセッサ実行可能命令によって構成される、ワイヤレス識別送信機。

[Ｃ５９] 前記定期的にブロードキャストされるメッセージは、さらに前記ノンスを含む、Ｃ５８に記載のワイヤレス識別送信機。

[Ｃ６０] 前記ノンスは、前記デバイス識別子の符号化が変化することが必要とされるたびに値が変化する、前記ワイヤレス識別送信機によって生成される繰り返されない数を表す、Ｃ５８に記載のワイヤレス識別送信機。

[Ｃ６１] 前記ストリーミングライク暗号化アルゴリズムはＡＥＳ－ＣＴＲ暗号である、Ｃ５８に記載のワイヤレス識別送信機。

[Ｃ６２] 前記メッセージは８０ビット以下のサイズを有する単一のパケットであり、前記秘密鍵は１２８ビットである、Ｃ５８に記載のワイヤレス識別送信機。

[Ｃ６３] 前記プロセッサは、

前記ローリング識別子を生成することが、送信されるべきデータを前記デバイス識別子に連結することと、サーバと共有される前記秘密鍵と前記ノンスとを使用して前記ストリーミングライク暗号化アルゴリズムで前記連結された識別子とデータとを符号化することとを備えるように、動作を実行するプロセッサ実行可能命令によって構成される、Ｃ５８に記載のワイヤレス識別送信機。

[Ｃ６４] 不明瞭にされた情報を含むメッセージの発信者を安全に識別するように構成されるサーバであって、

メモリと、

前記メモリに結合されたサーバプロセッサと、を備え、前記サーバプロセッサは、

共有秘密鍵をワイヤレス識別送信機に対するノンスおよびデバイス識別子と関連付けることと、

ローリング識別子を含む前記メッセージを受信することと、

前記受信されたメッセージから前記ローリング識別子を抽出することと、

前記サーバの現在の時間を表すために、前記ノンスをインクリメントすることと、

サーバ暗号化データを生成するために、前記共有秘密鍵と、前記ノンスと、擬似ランダム関数とを使用して、前記デバイス識別子を符号化することと、

前記サーバ暗号化データが前記抽出されたローリング識別子と一致するかどうかを決定することと、

前記サーバ暗号化データが前記抽出されたローリング識別子と一致するとき、前記受信されたメッセージの前記発信者を前記ワイヤレス識別送信機として識別することと、

を備える動作を実行するサーバプロセッサ実行可能命令によって構成される、サーバ。

[Ｃ６５] 前記擬似ランダム関数は、鍵付きハッシュメッセージ認証コード（ＨＭＡＣ）

または暗号ベースのメッセージ認証コード（ＣＭＡＣ）のうちの１つである、Ｃ６４に記載のサーバ。
[Ｃ６６] 前記サーバプロセッサは、
前記サーバの現在の時間を表すために、前記ノンスをインクリメントすることが、
前記メッセージ内に含まれる情報に基づいて、前記ワイヤレス識別送信機からのブロードキャストを近隣ブロードキャスト受信機が受信した時間に対応するように前記ノンスを計算することを備えるように、動作を実行するサーバプロセッサ実行可能命令によって構成される、Ｃ６４に記載のサーバ。
[Ｃ６７] 前記サーバプロセッサは、
前記受信されたメッセージからノンスを抽出することをさらに備える動作を実行するサーバプロセッサ実行可能命令によって構成され、
前記デバイス識別子を符号化することは、前記受信されたメッセージから抽出された前記ノンスを使用する、Ｃ６４に記載のサーバ。
[Ｃ６８] 識別情報の片方向通信を可能にするために不明瞭にされた情報を送信するように構成されるワイヤレス識別送信機であって、
メモリと、
前記メモリに結合されたプロセッサと、を備え、前記プロセッサは、
前記ワイヤレス識別送信機内でノンスを初期化することと、
前記ワイヤレス識別送信機と関連付けられるデバイス識別子と、サーバと共有される秘密鍵と、前記ノンスとを擬似ランダム関数により符号化することによって、ローリング識別子を生成することと、
短距離ワイヤレス送信を使用して前記ローリング識別子を含むメッセージを定期的にブロードキャストすることと、
前記ワイヤレス識別送信機の現在の時間を維持するために、予め定義された間隔で前記ノンスをインクリメントすることと
を備える動作を実行する、プロセッサ実行可能命令によって構成される、ワイヤレス識別送信機。
[Ｃ６９] 前記サーバプロセッサは、
擬似ランダム関数を使用することによってローリング識別子を生成することが、
送信されるべきデータを前記デバイス識別子に連結し、サーバと共有される前記秘密鍵と前記ノンスとに基づいて前記連結されたデバイス識別子とデータとを符号化するために、前記擬似ランダム関数を使用すること、を備えるように、動作を実行するサーバプロセッサ実行可能命令によって構成される、Ｃ６８に記載のワイヤレス識別送信機。
[Ｃ７０] 前記擬似ランダム関数は、鍵付きハッシュメッセージ認証コード（ＨＭＡＣ）または暗号ベースのメッセージ認証コード（ＣＭＡＣ）のうちの１つである、Ｃ６８に記載のワイヤレス識別送信機。
[Ｃ７１] 不明瞭にされた情報を含むメッセージの発信者を識別するように構成されるサーバであって、
メモリと、
前記メモリに結合されたサーバプロセッサと、を備え、前記サーバプロセッサは、
ワイヤレス識別送信機に対するデバイス識別子を、初期ノンスと、現在ノンスと、第１の秘密鍵と、第２の秘密鍵とに関連付けることと、
前記第２の秘密鍵および前記現在ノンスとともに、擬似ランダム関数を使用して、複数の符号化ノンスを予め計算することと、
ローリング識別子と符号化ノンスとを含む前記メッセージを受信することと、
前記受信されたメッセージから前記符号化ノンスを抽出することと、
前記受信されたメッセージから前記ローリング識別子を抽出することと、
前記抽出された符号化ノンスを前記複数の予め計算された符号化ノンスと比較することと、
前記抽出された符号化ノンスが前記複数の予め計算された符号化ノンスのいずれかと

一致するとき、復号されたデバイス識別子を生成するために、ストリーミングライク暗号化アルゴリズムと、前記第１の秘密鍵と、前記抽出された符号化ノンスと一致する予め計算された符号化ノンスと関連付けられるノンスとを使用して、前記抽出されたローリング識別子を復号することと、

前記抽出された符号化ノンスが前記複数の予め計算された符号化ノンスのうちの１つと一致しないとき、前記復号されたデバイス識別子を生成するために、前記ストリーミングライク暗号化アルゴリズムと、前記第１の秘密鍵と、前記ワイヤレス識別送信機と関連付けられる前記初期ノンスとを使用して、前記抽出されたローリング識別子を復号することと、

前記復号されたデバイス識別子が前記ワイヤレス識別送信機の前記デバイス識別子と一致するとき、前記受信されたメッセージの前記発信者を前記ワイヤレス識別送信機として識別することと、

を備える動作を実行するサーバプロセッサ実行可能命令によって構成される、サーバ。

[Ｃ７２] 前記第１の秘密鍵と前記第２の秘密鍵とは同じ値を有する、Ｃ７１に記載のサーバ。

[Ｃ７３] 識別情報の片方向通信を可能にするために不明瞭にされた情報を送信するように構成されるワイヤレス識別送信機であって、

メモリと、

前記メモリに結合されたプロセッサと、を備え、前記プロセッサは、

前記ワイヤレス識別送信機内でノンスを初期化することと、

前記ワイヤレス識別送信機と関連付けられるデバイス識別子と、サーバと共有される第１の秘密鍵と、前記ノンスとをストリーミングライク暗号化アルゴリズムで符号化することによって、ローリング識別子を生成することと、

前記サーバと共有される第２の秘密鍵とともに擬似ランダム関数を使用して前記ノンスを符号化することによって、符号化されたノンスを生成することと、

短距離ワイヤレス送信を使用して前記ローリング識別子と前記符号化されたノンスとを含むメッセージを定期的にブロードキャストすることと、

前記ワイヤレス識別送信機の現在の時間を維持するために、予め定義された間隔で前記ノンスをインクリメントすることと、

を備える動作を実行するプロセッサ実行可能命令によって構成される、ワイヤレス識別送信機。

[Ｃ７４] メッセージの発信者を安全に識別するように構成されるサーバであって、

メモリと、

前記メモリに結合されたサーバプロセッサと、を備え、前記サーバプロセッサは、

ワイヤレス識別送信機についてデバイス識別子を、初期ノンスと、現在ノンスと、第１の秘密鍵と、第２の秘密鍵とに関連付けることと、

前記第２の秘密鍵および前記現在ノンスとともに、擬似ランダム関数を使用して、複数の符号化ノンスを予め計算することと、

前記第１の秘密鍵、前記現在ノンス、および前記デバイス識別子とともに、ストリーミングライク暗号化アルゴリズムを使用して、複数の符号化されたデバイス識別子を予め計算することと、

ローリング識別子と符号化ノンスとを含む前記メッセージを受信することと、

前記受信されたメッセージから前記符号化されたノンスを抽出することと、

前記受信されたメッセージから前記ローリング識別子を抽出することと、

前記抽出された符号化ノンスを前記複数の予め計算された符号化ノンスと比較することと、

前記抽出された符号化ノンスが前記複数の予め計算された符号化ノンスのいずれかと一致するとき、前記抽出されたローリング識別子を前記複数の予め計算された符号化デバイス識別子と比較することと、

前記抽出されたローリング識別子が前記複数の予め計算された符号化されたデバイス

識別子のいずれかと一致するとき、前記受信されたメッセージの前記発信者を前記ワイヤレス識別送信機として識別することと、
を備える動作を実行するサーバプロセッサ実行可能命令によって構成される、サーバ。
[Ｃ７５] メッセージの発信者を安全に識別するように構成されるサーバであって、
メモリと、
前記メモリに結合されたサーバプロセッサと、を備え、前記サーバプロセッサは、
暗号化アルゴリズム、共有秘密鍵、初期ノンス、およびワイヤレス識別送信機と関連付けられるデバイス識別子で、複数の初期モデルペイロードを生成することと、前記暗号化アルゴリズムは前記ワイヤレス識別送信機と共有され、
前記暗号化アルゴリズム、前記共有秘密鍵、現在ノンス、および前記ワイヤレス識別送信機と関連付けられる前記デバイス識別子で、複数の現在モデルペイロードを生成することと、
不明瞭にされた識別情報をもつペイロードを含む前記メッセージを受信することと、
前記受信されたメッセージの前記ペイロードを前記複数の現在モデルペイロードと比較することと、
前記受信されたメッセージの前記ペイロードが前記複数の現在モデルペイロードのうちの１つと一致するとき、前記ワイヤレス識別送信機を識別することと、
前記受信されたメッセージの前記ペイロードが前記複数の現在モデルペイロードのいずれとも一致しないとき、前記受信されたメッセージの前記ペイロードを前記複数の初期モデルペイロードと比較することと、
前記受信されたメッセージの前記ペイロードが前記複数の初期モデルペイロードのうちの１つと一致するとき、前記ワイヤレス識別送信機を識別することと、
前記受信されたメッセージの前記ペイロードが、初期モデルペイロードと現在モデルペイロードのうちの少なくとも１つと一致するとき、前記ワイヤレス識別送信機と関連付けられる前記現在ノンスを更新することと、
を備える動作を実行するサーバプロセッサ実行可能命令によって構成される、サーバ。
[Ｃ７６] 入来するメッセージを受信するように構成されるワイヤレス識別送信機であって、
メモリと、
前記メモリに結合されたプロセッサと、を備え、前記プロセッサは、
第１の期間に、短距離ワイヤレス送信を介して、入来する送信を受信することが可能かどうかを示すメッセージを、定期的にブロードキャストすることと、
前記第１の期間が満了したことに応答して、第２の期間の間にリンクアドバタイズメントメッセージを受信することと、
前記受信されたリンクアドバタイズメントメッセージ内の情報に基づいて、近隣ブロードキャスト受信機とのリンクをネゴシエートすることと、
前記ネゴシエートされたリンクを認証することと、
前記ネゴシエートされたリンクを介して前記入来するメッセージを処理することと、
を備える動作を実行するプロセッサ実行可能命令によって構成され、
前記ネゴシエートされたリンクはＢｌｕｅｔｏｏｔｈペアリングにより実行される、ワイヤレス識別送信機。
[Ｃ７７] 前記入来するメッセージは、ファームウェアの更新、構成情報、トリガ信号、およびソフトウェア命令のうちの少なくとも１つを含む、Ｃ７６に記載のワイヤレス識別送信機。
[Ｃ７８] 前記第１の期間は、前記ワイヤレス識別送信機上のタイマー、時計信号、および前記近隣ブロードキャスト受信機からの受信されたメッセージのうちの少なくとも１つによって定義される、Ｃ７６に記載のワイヤレス識別送信機。
[Ｃ７９] サーバに、不明瞭にされた情報を含むメッセージの発信者を前記サーバが安全に識別するための動作を実行させるように構成されるサーバ実行可能命令を記憶した、非一時的サーバ可読記憶媒体であって、前記動作は、

共有秘密鍵をワイヤレス識別送信機に対応するデバイス識別子と関連付けることと、
ローリング識別子を含む前記メッセージを受信することと、
前記受信されたメッセージから前記ローリング識別子を抽出することと、
復号されたデバイス識別子を生成するために、ストリーミングライク暗号化アルゴリズムと前記共有秘密鍵とを使用して、前記抽出されたローリング識別子を復号することと、
前記復号されたデバイス識別子が前記共有秘密鍵と関連付けられる前記デバイス識別子と一致するかどうかを決定することと、
前記復号されたデバイス識別子が前記ワイヤレス識別送信機と関連付けられる前記デバイス識別子と一致するとき、前記受信されたメッセージの前記発信者を前記ワイヤレス識別送信機として識別することと、
を備える、非一時的サーバ可読記憶媒体。
[Ｃ８０] 前記メッセージはさらにノンスを含み、
前記記憶されたサーバ実行可能命令は、
復号されたデバイス識別子を生成するために、ストリーミングライク暗号化アルゴリズムと前記共有秘密鍵とを使用して前記抽出されたローリング識別子を復号することが、
前記復号されたデバイス識別子を生成するために、ストリーミングライク暗号化アルゴリズムと、前記メッセージから抽出された前記ノンスと、前記共有秘密鍵とを使用して前記抽出されたローリング識別子を復号すること、を備えるように、
サーバに動作を実行させるように構成される、Ｃ７９に記載の非一時的サーバ可読記憶媒体。
[Ｃ８１] 前記ストリーミングライク暗号化アルゴリズムはＡＥＳ－ＣＴＲ暗号である、Ｃ７９に記載の非一時的サーバ可読記憶媒体。
[Ｃ８２] 前記共有秘密鍵が１２８ビットのサイズを有する、Ｃ７９に記載の非一時的サーバ可読記憶媒体。
[Ｃ８３] 前記記憶されたサーバ実行可能命令は、
復号されたデバイス識別子を生成するために、ストリーミングライク暗号化アルゴリズムと前記共有秘密鍵とを使用して前記抽出されたローリング識別子を復号することが、さらに、暗号化の前に前記デバイス識別子に連結されていたデータを復号することを備えるように、
サーバに動作を実行させるように構成される、Ｃ７９に記載の非一時的サーバ可読記憶媒体。
[Ｃ８４] 識別情報の片方向通信を可能にするためにワイヤレス識別送信機が不明瞭にされた情報を送信するための動作をプロセッサに実行させるように構成される、プロセッサ実行可能ソフトウェア命令を記憶した非一時的プロセッサ可読記憶媒体であって、前記動作は、
前記ワイヤレス識別送信機内でノンスを初期化することと、
サーバと共有される秘密鍵と前記ノンスとを使用してストリーミングライク暗号化アルゴリズムで前記ワイヤレス識別送信機と関連付けられるデバイス識別子を符号化することによって、ローリング識別子を生成することと、
短距離ワイヤレス送信を使用して、前記ローリング識別子を含むメッセージを定期的にブロードキャストすることと、
予め定義された間隔で前記ノンスをインクリメントすることと、
を備える、非一時的プロセッサ可読記憶媒体。
[Ｃ８５] 前記定期的にブロードキャストされるメッセージはさらに前記ノンスを含む、Ｃ８４に記載の非一時的プロセッサ可読記憶媒体。
[Ｃ８６] 前記ノンスは、前記ワイヤレス識別送信機によって生成される繰り返されない数を表し、その値は、前記デバイス識別子の符号化が変化することが必要とされるたびに変化する、Ｃ８４に記載の非一時的プロセッサ可読記憶媒体。
[Ｃ８７] 前記ストリーミングライク暗号化アルゴリズムはＡＥＳ－ＣＴＲ暗号である、Ｃ８４に記載の非一時的プロセッサ可読記憶媒体。

[Ｃ８８] 前記メッセージは８０ビット以下のサイズを有する単一のパケットであり、前記秘密鍵は１２８ビットである、Ｃ８４に記載の非一時的プロセッサ可読記憶媒体。
[Ｃ８９] 前記記憶されたサーバ実行可能命令は、
前記ローリング識別子を生成することが、送信されるべきデータを前記デバイス識別子に連結することと、サーバと共有される前記秘密鍵と前記ノンスとを使用して前記ストリーミングライク暗号化アルゴリズムにより前記連結された識別子とデータとを符号化することと、を備えるように、
サーバに動作を実行させるように構成される、Ｃ８４に記載の非一時的プロセッサ可読記憶媒体。
[Ｃ９０] 不明瞭にされた情報を含むメッセージの発信者をサーバが安全に識別するための動作を前記サーバに実行させるように構成されるサーバ実行可能命令を記憶した、非一時的サーバ可読記憶媒体であって、前記動作は、
共有秘密鍵をワイヤレス識別送信機についてのノンスおよびデバイス識別子と関連付けることと、
ローリング識別子を含む前記メッセージを受信することと、
前記受信されたメッセージから前記ローリング識別子を抽出することと、
前記サーバの現在の時間を表すために、前記ノンスをインクリメントすることと、
サーバ暗号化データを生成するために、前記共有秘密鍵と、前記ノンスと、擬似ランダム関数とを使用して、前記デバイス識別子を符号化することと、
前記サーバ暗号化データが前記抽出されたローリング識別子と一致するかどうかを決定することと、
前記サーバ暗号化データが前記抽出されたローリング識別子と一致するとき、前記受信されたメッセージの前記発信者を前記ワイヤレス識別送信機として識別することと、
を備える、非一時的サーバ可読記憶媒体。
[Ｃ９１] 前記擬似ランダム関数は、鍵付きハッシュメッセージ認証コード（ＨＭＡＣ）または暗号ベースのメッセージ認証コード（ＣＭＡＣ）のうちの１つである、Ｃ９０に記載の非一時的サーバ可読記憶媒体。
[Ｃ９２] 前記サーバ実行可能命令は、
前記サーバの現在の時間を表すために、前記ノンスをインクリメントすることが、前記メッセージ内に含まれる情報に基づいて、前記ワイヤレス識別送信機からのブロードキャストを近隣ブロードキャスト受信機が受信した時間に対応するように前記ノンスを計算することを備えるように、前記サーバに動作を実行させるように構成される、Ｃ９０に記載の非一時的サーバ可読記憶媒体。
[Ｃ９３] 前記サーバ実行可能命令は、前記受信されたメッセージからノンスを抽出することをさらに備える動作を前記サーバに実行させるように構成され、
前記デバイス識別子を符号化することは、前記受信されたメッセージから抽出された前記ノンスを使用する、Ｃ９０に記載の非一時的サーバ可読記憶媒体。
[Ｃ９４] 識別情報の片方向通信を可能にするためにワイヤレス識別送信機が不明瞭にされた情報を送信するための動作をプロセッサに実行させるように構成される、プロセッサ実行可能ソフトウェア命令を記憶した非一時的プロセッサ可読記憶媒体であって、前記動作は、
前記ワイヤレス識別送信機内でノンスを初期化することと、
前記ワイヤレス識別送信機と関連付けられるデバイス識別子と、サーバと共有される秘密鍵と、前記ノンスとを、擬似ランダム関数で符号化することによって、ローリング識別子を生成することと、
短距離ワイヤレス送信を使用して前記ローリング識別子を含むメッセージを定期的にブロードキャストすることと、
前記ワイヤレス識別送信機の現在の時間を維持するために、予め定義された間隔で前記ノンスをインクリメントすることと、
を備える、非一時的プロセッサ可読記憶媒体。

[Ｃ９５] 前記プロセッサ実行可能命令は、
擬似ランダム関数を使用することによってローリング識別子を生成することが、送信されるべきデータを前記デバイス識別子に連結することと、サーバと共有される前記秘密鍵と前記ノンスとに基づいて前記連結されたデバイス識別子とデータとを符号化するために、前記擬似ランダム関数を使用することと、を備えるように、
プロセッサに動作を実行させるように構成される、Ｃ９４に記載の非一時的サーバ可読記憶媒体。
[Ｃ９６] 前記擬似ランダム関数は、鍵付きハッシュメッセージ認証コード（ＨＭＡＣ）または暗号ベースのメッセージ認証コード（ＣＭＡＣ）のうちの１つである、Ｃ９４に記載の非一時的プロセッサ可読記憶媒体。
[Ｃ９７] 不明瞭にされた情報を含むメッセージの発信者をサーバが安全に識別するための動作を前記サーバに実行させるように構成されるサーバ実行可能命令を記憶した、非一時的サーバ可読記憶媒体であって、前記動作は、
ワイヤレス識別送信機に対するデバイス識別子を、初期ノンスと、現在ノンスと、第１の秘密鍵と、第２の秘密鍵とに関連付けることと、
前記第２の秘密鍵および前記現在ノンスとともに、擬似ランダム関数を使用して、複数の符号化ノンスを予め計算することと、
ローリング識別子と符号化ノンスとを含む前記メッセージを受信することと、
前記受信されたメッセージから前記符号化ノンスを抽出することと、
前記受信されたメッセージから前記ローリング識別子を抽出することと、
前記抽出された符号化ノンスを前記複数の予め計算された符号化ノンスと比較することと、
前記抽出された符号化ノンスが前記複数の予め計算された符号化ノンスのいずれかと一致するとき、復号されたデバイス識別子を生成するために、ストリーミングライク暗号化アルゴリズムと、前記第１の秘密鍵と、前記抽出された符号化ノンスと一致する予め計算された符号化ノンスと関連付けられるノンスとを使用して、前記抽出されたローリング識別子を復号することと、
前記抽出された符号化ノンスが前記複数の予め計算された符号化ノンスのうちの１つと一致しないとき、前記復号されたデバイス識別子を生成するために、前記ストリーミングライク暗号化アルゴリズムと、前記第１の秘密鍵と、前記ワイヤレス識別送信機と関連付けられる前記初期ノンスとを使用して、前記抽出されたローリング識別子を復号することと、
前記復号されたデバイス識別子が前記ワイヤレス識別送信機の前記デバイス識別子と一致するとき、前記受信されたメッセージの前記発信者を前記ワイヤレス識別送信機として識別することと、
を備える、非一時的サーバ可読記憶媒体。
[Ｃ９８] 前記第１の秘密鍵と前記第２の秘密鍵とは同じ値を有する、Ｃ９７に記載の非一時的サーバ可読記憶媒体。
[Ｃ９９] 識別情報の片方向通信を可能にするためにワイヤレス識別送信機が不明瞭にされた情報を送信するための動作をプロセッサに実行させるように構成される、プロセッサ実行可能ソフトウェア命令を記憶した非一時的プロセッサ可読記憶媒体であって、前記動作は、
前記ワイヤレス識別送信機内でノンスを初期化することと、
前記ワイヤレス識別送信機と関連付けられるデバイス識別子と、サーバと共有される第１の秘密鍵と、前記ノンスとをストリーミングライク暗号化アルゴリズムにより符号化することによって、ローリング識別子を生成することと、
前記サーバと共有される第２の秘密鍵とともに擬似ランダム関数を使用して前記ノンスを符号化することによって、符号化されたノンスを生成することと、
短距離ワイヤレス送信を使用して前記ローリング識別子と前記符号化されたノンスとを含むメッセージを定期的にブロードキャストすることと、

前記ワイヤレス識別送信機の現在の時間を維持するために、予め定義された間隔で前記ノンスをインクリメントすることと、
を備える、非一時的プロセッサ可読記憶媒体。
[Ｃ１００] メッセージの発信者をサーバが安全に識別するための動作を前記サーバに実行させるように構成されるサーバ実行可能命令を記憶した、非一時的サーバ可読記憶媒体であって、前記動作は、
ワイヤレス識別送信機に対するデバイス識別子を、初期ノンスと、現在ノンスと、第１の秘密鍵と、第２の秘密鍵とに関連付けることと、
前記第２の秘密鍵および前記現在ノンスとともに、擬似ランダム関数を使用して、複数の符号化ノンスを予め計算することと、
前記第１の秘密鍵、前記現在ノンス、および前記デバイス識別子とともに、ストリーミングライク暗号化アルゴリズムを使用して、複数の符号化されたデバイス識別子を予め計算することと、
ローリング識別子と符号化ノンスとを含む前記メッセージを受信することと、
前記受信されたメッセージから前記符号化ノンスを抽出することと、
前記受信されたメッセージから前記ローリング識別子を抽出することと、
前記抽出された符号化ノンスを前記複数の予め計算された符号化ノンスと比較することと、
前記抽出された符号化ノンスが前記複数の予め計算された符号化ノンスのいずれかと一致するとき、前記抽出されたローリング識別子を前記複数の予め計算された符号化されたデバイス識別子と比較することと、
前記抽出されたローリング識別子が前記複数の予め計算された符号化されたデバイス識別子のいずれかと一致するとき、前記受信されたメッセージの前記発信者を前記ワイヤレス識別送信機として識別することと、
を備える、非一時的サーバ可読記憶媒体。
[Ｃ１０１] メッセージの発信者をサーバが安全に識別するための動作を前記サーバに実行させるように構成されるサーバ実行可能命令を記憶した、非一時的サーバ可読記憶媒体であって、前記動作は、
暗号化アルゴリズム、共有秘密鍵、初期ノンス、およびワイヤレス識別送信機と関連付けられるデバイス識別子で、複数の初期モデルペイロードを生成することと、前記暗号化アルゴリズムは前記ワイヤレス識別送信機と共有され、
前記暗号化アルゴリズム、前記共有秘密鍵、現在ノンス、および前記ワイヤレス識別送信機と関連付けられる前記デバイス識別子で、複数の現在モデルペイロードを生成することと、
不明瞭にされた識別情報をもつペイロードを含む前記メッセージを受信することと、
前記受信されたメッセージの前記ペイロードを前記複数の現在モデルペイロードと比較することと、
前記受信されたメッセージの前記ペイロードが前記複数の現在モデルペイロードのうちの１つと一致するとき、前記ワイヤレス識別送信機を識別することと、
前記受信されたメッセージの前記ペイロードが前記複数の現在モデルペイロードのいずれとも一致しないとき、前記受信されたメッセージの前記ペイロードを前記複数の初期モデルペイロードと比較することと、
前記受信されたメッセージの前記ペイロードが前記複数の初期モデルペイロードのうちの１つと一致するとき、前記ワイヤレス識別送信機を識別することと、
前記受信されたメッセージの前記ペイロードが、初期モデルペイロードと現在モデルペイロードとのうちの少なくとも１つと一致するとき、前記ワイヤレス識別送信機と関連付けられる前記現在のノンスを更新することと、
を備える、非一時的サーバ可読記憶媒体。
[Ｃ１０２] 入来するメッセージを受信する、ワイヤレス識別送信機のための動作をプロセッサに実行させるように構成される、プロセッサ実行可能ソフトウェア命令を記憶した

非一時的プロセッサ可読記憶媒体であって、前記動作は、
第１の期間に、短距離ワイヤレス送信を介して、入来する送信を受信することが可能かどうかを示すメッセージを、定期的にブロードキャストすることと、
前記第１の期間が満了したことに応答して、第２の期間の間にリンクアドバタイズメントメッセージを受信することと、
前記受信されたリンクアドバタイズメントメッセージ内の情報に基づいて、近隣ブロードキャスト受信機とのリンクをネゴシエートすることと、
前記ネゴシエートされたリンクを認証することと、
前記ネゴシエートされたリンクを介して入来するメッセージを処理することと、
を備え、
前記ネゴシエートされたリンクがＢｌｕｅｔｏｏｔｈペアリングを介して実行される、非一時的プロセッサ可読記憶媒体。
[Ｃ１０３] 前記入来するメッセージは、ファームウェアの更新、構成情報、トリガ信号、およびソフトウェア命令の少なくとも１つを含む、Ｃ１０２に記載の非一時的プロセッサ可読記憶媒体。
[Ｃ１０４] 前記第１の期間が、前記ワイヤレス識別送信機上のタイマー、時計信号、および前記近隣ブロードキャスト受信機からの受信されたメッセージのうちの少なくとも１つによって定義される、Ｃ１０２に記載の非一時的プロセッサ可読記憶媒体。
[Ｃ１０５] サーバと、
ワイヤレス識別送信機と、
近隣ブロードキャスト受信機と、を備えるシステムであって、
前記ワイヤレス識別送信機は、
第１のメモリと、
前記近隣ブロードキャスト受信機によって受信されることが可能な短距離ワイヤレス信号をブロードキャストするように構成される第１の送受信機と、
前記第１のメモリおよび前記第１の送受信機に結合される第１のプロセッサと、を備え、前記第のプロセッサは、
前記ワイヤレス識別送信機内でノンスを初期化することと、
前記ワイヤレス識別送信機と関連付けられるデバイス識別子と、前記サーバと共有される秘密鍵と、前記ノンスとを、ストリーミングライク暗号化アルゴリズムで符号化することによって、ローリング識別子を生成することと、
前記第１の送受信機を介して、短距離ワイヤレス送信を使用して、前記ローリング識別子と前記ノンスとを含むメッセージを定期的にブロードキャストすることと、
予め定義された間隔で前記ノンスをインクリメントすることと、
を備える動作を実行するプロセッサ実行可能命令によって構成され、
前記近隣ブロードキャスト受信機は、
第２のメモリと、
前記ワイヤレス識別送信機と短距離ワイヤレス信号を交換するように構成される第２の送受信機と、
前記サーバと信号を交換するように構成されるネットワークデバイスと、
前記第２のメモリ、前記第２の送受信機、および前記ネットワークデバイスに結合された第２のプロセッサと、を備え、前記第２のプロセッサは、
前記第２の送受信機を介して、前記ワイヤレス識別送信機から前記ローリング識別子と前記ノンスとを含む前記メッセージを受信することと、
前記ネットワークデバイスを介して、前記ローリング識別子と前記ノンスとを含むサイティングメッセージを前記サーバに送信することと、
を備える動作を実行するプロセッサ実行可能命令によって構成され、
前記サーバは、
前記秘密鍵を前記ワイヤレス識別送信機に対応する前記デバイス識別子と関連付けることと、

前記ローリング識別子と前記ノンスとを含む前記サイティングメッセージを受信することと、
前記受信されたサイティングメッセージから前記ノンスと前記ローリング識別子とを抽出することと、
復号されたデバイス識別子を生成するために、前記ストリーミングライク暗号化アルゴリズムと、前記秘密鍵と、前記抽出されたノンスとを使用して、前記抽出されたローリング識別子を復号することと、
前記復号されたデバイス識別子が前記秘密鍵と関連付けられる前記デバイス識別子と一致するかどうかを決定することと、
前記復号されたデバイス識別子が前記ワイヤレス識別送信機と関連付けられる前記デバイス識別子と一致するとき、前記受信されたメッセージの発信者を前記ワイヤレス識別送信機として識別することと、
を備える動作を実行するサーバ実行可能命令によって構成される、システム。
[Ｃ１０６] 前記ストリーミングライク暗号化アルゴリズムはＡＥＳ－ＣＴＲ暗号である、Ｃ１０５に記載のシステム。
[Ｃ１０７] 前記秘密鍵は１２８ビットのサイズを有する、Ｃ１０５に記載のシステム。
[Ｃ１０８] 前記ノンスは、前記ワイヤレス識別送信機によって生成される繰り返されない数を表し、その値は、前記デバイス識別子の符号化が変化することが必要とされるたびに変化する、Ｃ１０５に記載のシステム。
[Ｃ１０９] サーバと、
ワイヤレス識別送信機と、
近隣ブロードキャスト受信機と、を備えるシステムであって、
前記ワイヤレス識別送信機は、
第１のメモリと、
前記近隣ブロードキャスト受信機によって受信されることが可能な短距離ワイヤレス信号をブロードキャストするように構成される第１の送受信機と、
前記第１のメモリおよび前記第１の送受信機に結合される第１のプロセッサと、を備え、前記第１のプロセッサは、
前記ワイヤレス識別送信機内でノンスを初期化することと、
前記ワイヤレス識別送信機と関連付けられるデバイス識別子と、前記サーバと共有される秘密鍵と、前記ノンスとを擬似ランダム関数で符号化することによって、ローリング識別子を生成することと、
前記第１の送受信機を介して、短距離ワイヤレス送信を使用して、前記ローリング識別子を含むメッセージを定期的にブロードキャストすることと、
前記ワイヤレス識別送信機の現在の時間を維持するために、予め定義された間隔で前記ノンスをインクリメントすることと、
を備える動作を実行するプロセッサ実行可能命令によって構成され、
前記近隣ブロードキャスト受信機は、
第２のメモリと、
前記ワイヤレス識別送信機と短距離ワイヤレス信号を交換するように構成される第２の送受信機と、
前記サーバと信号を交換するように構成されるネットワークデバイスと、
前記第２のメモリ、前記第２の送受信機、および前記ネットワークデバイスに結合された第２のプロセッサと、を備え、前記第２のプロセッサは、
前記第２の送受信機を介して、前記ワイヤレス識別送信機から前記ローリング識別子を含む前記メッセージを受信することと、
前記ネットワークデバイスを介して、前記ローリング識別子を含むサイティングメッセージを前記サーバに送信することと、
を備える動作を実行するプロセッサ実行可能命令によって構成され、
前記サーバは、

前記秘密鍵を前記ワイヤレス識別送信機に対する前記ノンスおよび前記デバイス識別子とに関連付けることと、
前記ローリング識別子を含む前記サイティングメッセージを前記近隣ブロードキャスト受信機から受信することと、
前記受信されたサイティングメッセージから前記ローリング識別子を抽出することと、
前記サーバの現在の時間を表すために、前記ノンスをインクリメントすることと、
サーバ暗号化データを生成するために、前記秘密鍵と、前記ノンスと、前記擬似ランダム関数とを使用して、前記デバイス識別子を符号化することと、
前記サーバ暗号化データが前記抽出されたローリング識別子と一致するかどうかを決定することと、
前記サーバ暗号化データが前記抽出されたローリング識別子と一致するとき、前記受信されたメッセージの発信者を前記ワイヤレス識別送信機として識別することと、
を備える動作を実行するサーバ実行可能命令によって構成される、システム。
[Ｃ１１０] 前記擬似ランダム関数は、鍵付きハッシュメッセージ認証コード（ＨＭＡＣ）または暗号ベースのメッセージ認証コード（ＣＭＡＣ）のうちの１つである、Ｃ１０９に記載のシステム。
[Ｃ１１１] 前記サーバは、
前記サーバの現在の時間を表すために、前記ノンスをインクリメントすることが、前記サイティングメッセージ内に含まれる情報に基づいて、前記ワイヤレス識別送信機からの前記メッセージを前記近隣ブロードキャスト受信機が受信した時間に対応するように前記ノンスを計算することを備えるように、動作を実行するサーバ実行可能命令によって構成される、Ｃ１０９に記載のシステム。
[Ｃ１１２] サーバと、
ワイヤレス識別送信機と、
近隣ブロードキャスト受信機と、を備えるシステムであって、
前記ワイヤレス識別送信機は、
第１のメモリと、
前記近隣ブロードキャスト受信機によって受信されることが可能な短距離ワイヤレス信号をブロードキャストするように構成される第１の送受信機と、
前記第１のメモリおよび前記第１の送受信機に結合される第１のプロセッサと、を備え、
前記第１のプロセッサは、
前記ワイヤレス識別送信機内でノンスを初期化することと、
前記ワイヤレス識別送信機と関連付けられるデバイス識別子と、前記サーバと共有される第１の秘密鍵と、前記ノンスとをストリーミングライク暗号化アルゴリズムで符号化することによって、ローリング識別子を生成することと、
前記サーバと共有される第２の秘密鍵とともに擬似ランダム関数を使用して前記ノンスを符号化することによって、符号化されたノンスを生成することと、
前記第１の送受信機を介して、短距離ワイヤレス送信を使用して、前記ローリング識別子と前記符号化されたノンスとを含むメッセージを定期的にブロードキャストすることと、
前記ワイヤレス識別送信機の現在の時間を維持するために、予め定義された間隔で前記ノンスをインクリメントすることと、
を備える動作を実行するプロセッサ実行可能命令によって構成され、
前記近隣ブロードキャスト受信機は、
第２のメモリと、
前記ワイヤレス識別送信機と短距離ワイヤレス信号を交換するように構成される第２の送受信機と、
前記サーバと信号を交換するように構成されるネットワークデバイスと、

前記第２のメモリ、前記第２の送受信機、および前記ネットワークデバイスに結合された第２のプロセッサと、を備え、前記第２のプロセッサは、
前記第２の送受信機を介して、前記ワイヤレス識別送信機から、前記ローリング識別子と前記符号化されたノンスとを含む前記メッセージを受信することと、
前記ネットワークデバイスを介して、前記ローリング識別子と前記符号化されたノンスとを含むサイティングメッセージを前記サーバに送信することと、
を備える動作を実行するプロセッサ実行可能命令によって構成され、
前記サーバは、
前記ワイヤレス識別送信機についての前記デバイス識別子を、初期ノンスと、現在ノンスと、前記ワイヤレス識別送信機と共有される前記第１の秘密鍵と、前記第２の秘密鍵とに関連付けることと、
前記第２の秘密鍵および前記現在ノンスとともに前記擬似ランダム関数を使用して、複数の符号化ノンスを予め計算することと、
前記ローリング識別子と前記符号化ノンスとを含む前記サイティングメッセージを、前記近隣ブロードキャスト受信機から受信することと、
前記受信されたサイティングメッセージから前記符号化ノンスを抽出することと、
前記受信されたサイティングメッセージから前記ローリング識別子を抽出することと、
前記抽出された符号化ノンスを前記複数の予め計算された符号化ノンスと比較することと、
前記抽出された符号化ノンスが前記複数の予め計算された符号化ノンスのいずれかと一致するとき、復号されたデバイス識別子を生成するために、前記ストリーミングライク暗号化アルゴリズムと、前記第１の秘密鍵と、前記抽出された符号化ノンスと一致する予め計算された符号化ノンスと関連付けられる記憶されたノンスとを使用して、前記抽出されたローリング識別子を復号することと、
前記抽出された符号化ノンスが前記複数の予め計算された符号化ノンスのうちの１つと一致しないとき、前記復号されたデバイス識別子を生成するために、ストリーミングライク暗号化アルゴリズムと、前記第１の秘密鍵と、前記ワイヤレス識別送信機と関連付けられる前記初期ノンスとを使用して、前記抽出されたローリング識別子を復号することと、
前記復号されたデバイス識別子が前記ワイヤレス識別送信機の前記デバイス識別子と一致するとき、前記受信されたメッセージの発信者を前記ワイヤレス識別送信機として識別することと、
を備える動作を実行するサーバ実行可能命令によって構成される、システム。
[Ｃ１１３] 前記第１の秘密鍵と前記第２の秘密鍵とは同じ値を有する、Ｃ１１２に記載のシステム。
[Ｃ１１４] サーバと、
ワイヤレス識別送信機と、
近隣ブロードキャスト受信機と、を備えるシステムであって、
前記ワイヤレス識別送信機は、
第１のメモリと、
前記近隣ブロードキャスト受信機によって受信されることが可能な短距離ワイヤレス信号をブロードキャストするように構成される第１の送受信機と、
前記第１のメモリおよび前記第１の送受信機に結合される第１のプロセッサと、を備え、前記第１のプロセッサは、
前記ワイヤレス識別送信機内でノンスを初期化することと、
前記ワイヤレス識別送信機と関連付けられるデバイス識別子と、前記サーバと共有される第１の秘密鍵と、前記ノンスとをストリーミングライク暗号化アルゴリズムで符号化することによって、ローリング識別子を生成することと、
前記サーバと共有される第２の秘密鍵とともに擬似ランダム関数を使用して前記ノ

ンスを符号化することによって、符号化されたノンスを生成することと、
前記第１の送受信機を介して、短距離ワイヤレス送信を使用して、前記ローリング識別子と前記符号化されたノンスとを含むメッセージを定期的にブロードキャストすることと、
前記ワイヤレス識別送信機の現在の時間を維持するために、予め定義された間隔で前記ノンスをインクリメントすることと、
を備える動作を実行するプロセッサ実行可能命令によって構成され、
前記近隣ブロードキャスト受信機は、
第２のメモリと、
前記ワイヤレス識別送信機と短距離ワイヤレス信号を交換するように構成される第２の送受信機と、
前記サーバと信号を交換するように構成されるネットワークデバイスと、
前記第２のメモリ、前記第２の送受信機、および前記ネットワークデバイスに結合された第２のプロセッサと、を備え、前記第２のプロセッサは、
前記第２の送受信機を介して、前記ワイヤレス識別送信機から前記ローリング識別子と前記符号化されたノンスとを含む前記メッセージを受信することと、
前記ネットワークデバイスを介して、前記ローリング識別子と前記符号化されたノンスとを含むサイティングメッセージを前記サーバに送信することと、
を備える動作を実行するプロセッサ実行可能命令によって構成され、
前記サーバは、
前記ワイヤレス識別送信機についての前記デバイス識別子を、初期ノンスと、現在ノンスと、前記第１の秘密鍵と、前記第２の秘密鍵とに関連付けることと、
前記第２の秘密鍵および前記現在ノンスとともに、前記擬似ランダム関数を使用して複数の符号化ノンスを予め計算することと、
前記第１の秘密鍵、前記現在ノンス、および前記デバイス識別子とともに、前記ストリーミングライク暗号化アルゴリズムを使用して、複数の符号化されたデバイス識別子を予め計算することと、
前記ローリング識別子と前記符号化されたノンスとを含む前記サイティングメッセージを、前記近隣ブロードキャスト受信機から受信することと、
前記受信されたサイティングメッセージから前記符号化されたノンスを抽出することと、
前記受信されたサイティングメッセージから前記ローリング識別子を抽出することと、
前記抽出された符号化されたノンスを前記複数の予め計算された符号化ノンスと比較することと、
前記抽出された符号化されたノンスが前記複数の予め計算された符号化ノンスのいずれかと一致するとき、前記抽出されたローリング識別子を前記複数の予め計算された符号化されたデバイス識別子と比較することと、
前記抽出されたローリング識別子が前記複数の予め計算された符号化されたデバイス識別子のいずれかと一致するとき、前記受信されたメッセージの発信者を前記ワイヤレス識別送信機として識別することと、
を備える動作を実行するサーバ実行可能命令によって構成される、システム。
[Ｃ１１５]　サーバと、
ワイヤレス識別送信機と、
近隣ブロードキャスト受信機と、を備えるシステムであって、
前記ワイヤレス識別送信機は、
第１のメモリと、
前記近隣ブロードキャスト受信機によって受信されることが可能な短距離ワイヤレス信号をブロードキャストするように構成される第１の送受信機と、
前記第１のメモリおよび前記第１の送受信機に結合される第１のプロセッサと、を備

え、前記第１のプロセッサは、
前記ワイヤレス識別送信機内でノンスを初期化することと、
前記ワイヤレス識別送信機と関連付けられるデバイス識別子と、前記サーバと共有される秘密鍵と、前記ノンスとをストリーミングライク暗号化アルゴリズムで符号化することによって、ローリング識別子を生成することと、
前記第１の送受信機を介して、短距離ワイヤレス送信を使用して、前記ローリング識別子を含むメッセージを定期的にブロードキャストすることと、
予め定義された間隔で前記ノンスをインクリメントすることと、
を備える動作を実行するプロセッサ実行可能命令によって構成され、
前記近隣ブロードキャスト受信機は、
第２のメモリと、
前記ワイヤレス識別送信機と短距離ワイヤレス信号を交換するように構成される第２の送受信機と、
前記サーバと信号を交換するように構成されるネットワークデバイスと、
前記第２のメモリ、前記第２の送受信機、および前記ネットワークデバイスに結合された第２のプロセッサと、を備え、前記第２のプロセッサは、
前記第２の送受信機を介して、前記ワイヤレス識別送信機から前記ローリング識別子を含む前記メッセージを受信することと、
前記ネットワークデバイスを介して、前記ローリング識別子を含むサイティングメッセージを前記サーバに送信することと、
を備える動作を実行するプロセッサ実行可能命令によって構成され、
前記サーバは、
前記暗号化アルゴリズム、前記秘密鍵、初期ノンス、および前記ワイヤレス識別送信機と関連付けられる前記デバイス識別子で、複数の初期モデルペイロードを生成することと、前記暗号化アルゴリズムは前記ワイヤレス識別送信機と共有され、
前記暗号化アルゴリズム、前記秘密鍵、現在ノンス、および前記ワイヤレス識別送信機と関連付けられる前記デバイス識別子で、複数の現在モデルペイロードを生成することと、
不明瞭にされた識別情報をもつペイロードを含む前記サイティングメッセージを、前記近隣ブロードキャスト受信機から受信することと、
前記受信されたサイティングメッセージの前記ペイロードを前記複数の現在モデルペイロードを比較することと、
前記受信されたサイティングメッセージの前記ペイロードが前記複数の現在モデルペイロードのうちの１つと一致するとき、前記ワイヤレス識別送信機を識別することと、
前記受信されたサイティングメッセージの前記ペイロードが前記複数の現在モデルペイロードのいずれとも一致しないとき、前記受信されたサイティングメッセージの前記ペイロードを前記複数の初期モデルペイロードと比較することと、
前記受信されたサイティングメッセージの前記ペイロードが前記複数の初期モデルペイロードの１つと一致するとき、前記ワイヤレス識別送信機を識別することと、
前記受信されたメッセージの前記ペイロードが初期モデルペイロードと現在モデルペイロードのうちの少なくとも１つと一致するとき、前記ワイヤレス識別送信機と関連付けられる前記現在ノンスを更新することと、
を備える動作を実行するサーバ実行可能命令によって構成される、システム。
[Ｃ１１６] サーバと、
ワイヤレス識別送信機と、
近隣ブロードキャスト受信機と、を備えるシステムであって、
前記ワイヤレス識別送信機は、
第１のメモリと、
前記近隣ブロードキャスト受信機によって受信されることが可能な短距離ワイヤレス信号をブロードキャストするように構成される第１の送受信機と、

前記第１のメモリおよび前記第１の送受信機に結合される第１のプロセッサと、を備え、前記第１のプロセッサは、
第１の期間に、前記第１の送受信機を使用して、入来する送信を受信することが可能かどうかを示すメッセージを、短距離ワイヤレス送信を介して定期的にブロードキャストすることと、
前記第１の期間が満了したことに応答して、第２の期間の間にリンクアドバタイズメントメッセージを受信することと、
前記受信されたリンクアドバタイズメントメッセージ内の情報に基づいて、前記近隣ブロードキャスト受信機とのリンクをネゴシエートすることと、前記ネゴシエートされたリンクがＢｌｕｅｔｏｏｔｈペアリングを介して実行され、
前記ネゴシエートされたリンクを認証することと、
前記ネゴシエートされたリンクを介して入来するメッセージを処理することと、
を備える動作を実行するプロセッサ実行可能命令によって構成され、
前記近隣ブロードキャスト受信機は、
第２のメモリと、
前記ワイヤレス識別送信機と短距離ワイヤレス信号を交換するように構成される第２の送受信機と、
前記サーバと信号を交換するように構成されるネットワークデバイスと、
前記第２のメモリ、前記第２の送受信機、および前記ネットワークデバイスに結合された第２のプロセッサと、を備え、前記第２のプロセッサは、
前記ネットワークデバイスを使用して前記サーバからメッセージを受信することと、
前記ワイヤレス識別送信機が前記入来する送信を受信する可能性を示すブロードキャストメッセージを受信することと、
前記受信されたブロードキャストメッセージにおいて示される前記可能性に基づいて、前記リンクアドバタイズメントメッセージを送信することと、
前記リンクアドバタイズメントメッセージ内の前記情報に基づいて、前記ワイヤレス識別送信機との前記リンクをネゴシエートすることと、前記ネゴシエートされたリンクは前記Ｂｌｕｅｔｏｏｔｈペアリングを介して実行され、
前記ネゴシエートされたリンクを認証することと、
前記ネゴシエートされたリンクを介して、前記メッセージを前記サーバから前記ワイヤレス識別送信機に送信することと、
を備える動作を実行するプロセッサ実行可能命令によって構成され、
前記サーバは、前記メッセージを前記近隣ブロードキャスト受信機に送信することを備える動作を実行するサーバ実行可能命令によって構成される、システム。
[Ｃ１１７] 前記ワイヤレス識別送信機に送信される前記メッセージは、ファームウェアの更新、構成情報、トリガ信号、およびソフトウェア命令のうちの少なくとも１つを含む、Ｃ１１６に記載のシステム。
[Ｃ１１８] 前記第１の期間は、前記ワイヤレス識別送信機上のタイマー、時計信号、および前記近隣ブロードキャスト受信機からの第２のメッセージのうちの少なくとも１つによって定義される、Ｃ１１６に記載のシステム。
[Ｃ１１９] Ｂｌｕｅｔｏｏｔｈを使用して、向上されたセキュリティで通信する第１の通信デバイスのための方法であって、
第２の通信デバイスとの通信リンクを確立することと、
前記第２の通信デバイスと共有されるノンスを記憶することと、
前記通信リンクを介して、ローリングＢｌｕｅｔｏｏｔｈマシンアドレスを示すメッセージを受信することと、
前記ノンスと、前記第２の通信デバイスと共有される暗号化アルゴリズムとを使用して、前記第２の通信デバイスの予想されるＢｌｕｅｔｏｏｔｈマシンアドレスを生成することと、

前記受信されたメッセージの前記ローリングＢｌｕｅｔｏｏｔｈマシンアドレスを前記予想されるＢｌｕｅｔｏｏｔｈマシンアドレスと比較することと、
前記受信されたメッセージの前記ローリングＢｌｕｅｔｏｏｔｈマシンアドレスが前記第１の通信デバイスによって生成された前記予想されるＢｌｕｅｔｏｏｔｈマシンアドレスと一致するとき、前記受信されたメッセージを処理することと、
ノンスの更新が必要であると決定したことに応答して、前記ノンスをインクリメントすることと、を備える方法。
[Ｃ１２０] 前記受信されたメッセージの前記ローリングＢｌｕｅｔｏｏｔｈマシンアドレスが前記予想されるＢｌｕｅｔｏｏｔｈマシンアドレスと一致しないとき、予め定義されたオフセット値のセットにより、前記ノンスを変更することと、
前記変更されたノンスに基づいて、ある期間の間、前記受信されたメッセージの前記ローリングＢｌｕｅｔｏｏｔｈマシンアドレスと比較するための、複数の新たな予想されるＢｌｕｅｔｏｏｔｈマシンアドレスを生成することと、
前記期間の間に一致が発見されないとき、前記受信されたメッセージを無視することと、
をさらに備える、Ｃ１１９に記載の方法。
[Ｃ１２１] Ｂｌｕｅｔｏｏｔｈを使用して、向上されたセキュリティで通信するように構成される第１の通信デバイスであって、
第２の通信デバイスとの通信リンクを確立する手段と、
前記第２の通信デバイスと共有されるノンスを記憶する手段と、
前記通信リンクを介して、ローリングＢｌｕｅｔｏｏｔｈマシンアドレスを示すメッセージを受信する手段と、
前記ノンスと、前記第２の通信デバイスと共有される暗号化アルゴリズムとを使用して、前記第２の通信の予想されるＢｌｕｅｔｏｏｔｈマシンアドレスを生成する手段と、
前記受信されたメッセージの前記ローリングＢｌｕｅｔｏｏｔｈマシンアドレスを前記予想されるＢｌｕｅｔｏｏｔｈマシンアドレスと比較する手段と、
前記受信されたメッセージの前記ローリングＢｌｕｅｔｏｏｔｈマシンアドレスが前記第１の通信デバイスによって生成された前記予想されるＢｌｕｅｔｏｏｔｈマシンアドレスと一致するとき、前記受信されたメッセージを処理する手段と、
ノンスの更新が必要であると決定したことに応答して、前記ノンスをインクリメントする手段と、
を備える、第１の通信デバイス。
[Ｃ１２２] 前記受信されたメッセージの前記ローリングＢｌｕｅｔｏｏｔｈマシンアドレスが前記予想されるＢｌｕｅｔｏｏｔｈマシンアドレスと一致しないとき、予め定義されたオフセット値のセットにより、前記ノンスを変更する手段と、
前記変更されたノンスに基づいて、ある期間の間、前記受信されたメッセージの前記ローリングＢｌｕｅｔｏｏｔｈマシンアドレスと比較するための、複数の新たな予想されるＢｌｕｅｔｏｏｔｈマシンアドレスを生成する手段と、
前記期間の間に一致が発見されないとき、前記受信されたメッセージを無視する手段と、
をさらに備える、Ｃ１２１に記載の第１の通信デバイス。
[Ｃ１２３] Ｂｌｕｅｔｏｏｔｈを使用して、向上されたセキュリティで通信するように構成される第１の通信デバイスであって、
メモリと、
前記メモリに結合されたプロセッサと、を備え、前記プロセッサは、
第２の通信デバイスとの通信リンクを確立することと、
前記第２の通信デバイスと共有されるノンスを記憶することと、
前記通信リンクを介して、ローリングＢｌｕｅｔｏｏｔｈマシンアドレスを示すメッセージを受信することと、
前記ノンスと、前記第２の通信デバイスと共有される暗号化アルゴリズムとを使用し

て、前記第２の通信デバイスの予想されるＢｌｕｅｔｏｏｔｈマシンアドレスを生成することと、
前記受信されたメッセージの前記ローリングＢｌｕｅｔｏｏｔｈマシンアドレスを前記予想されるＢｌｕｅｔｏｏｔｈマシンアドレスと比較することと、
前記受信されたメッセージの前記ローリングＢｌｕｅｔｏｏｔｈマシンアドレスが前記第１の通信デバイスによって生成された前記予想されるＢｌｕｅｔｏｏｔｈマシンアドレスと一致するとき、前記受信されたメッセージを処理することと、
ノンスの更新が必要であると決定したことに応答して、前記ノンスをインクリメントすることと、
を備える動作を実行するプロセッサ実行可能命令によって構成される、第１の通信デバイス。
[Ｃ１２４] 前記プロセッサは、
前記受信されたメッセージの前記ローリングＢｌｕｅｔｏｏｔｈマシンアドレスが前記予想されるＢｌｕｅｔｏｏｔｈマシンアドレスと一致しないとき、予め定義されたオフセット値のセットにより、前記ノンスを変更することと、
前記変更されたノンスに基づいて、ある期間の間、前記受信されたメッセージの前記ローリングＢｌｕｅｔｏｏｔｈマシンアドレスと比較するための、複数の新たな予想されるＢｌｕｅｔｏｏｔｈマシンアドレスを生成することと、
前記期間の間に一致が発見されないとき、前記受信されたメッセージを無視することと、
をさらに備える動作を実行するプロセッサ実行可能命令によって構成される、Ｃ１２３に記載の第１の通信デバイス。
[Ｃ１２５] Ｂｌｕｅｔｏｏｔｈを使用して向上されたセキュリティで第１の通信デバイスが通信するための動作をプロセッサに実行させるように構成される、プロセッサ実行可能ソフトウェア命令を記憶した非一時的プロセッサ可読記憶媒体であって、前記動作は、
第２の通信デバイスとの通信リンクを確立することと、
前記第２の通信デバイスと共有されるノンスを記憶することと、
前記通信リンクを介して、ローリングＢｌｕｅｔｏｏｔｈマシンアドレスを示すメッセージを受信することと、
前記ノンスと、前記第２の通信デバイスと共有される暗号化アルゴリズムとを使用して、前記第２の通信デバイスの予想されるＢｌｕｅｔｏｏｔｈマシンアドレスを生成することと、
前記受信されたメッセージの前記ローリングＢｌｕｅｔｏｏｔｈマシンアドレスを前記予想されるＢｌｕｅｔｏｏｔｈマシンアドレスと比較することと、
前記受信されたメッセージの前記ローリングＢｌｕｅｔｏｏｔｈマシンアドレスが前記第１の通信デバイスによって生成された前記予想されるＢｌｕｅｔｏｏｔｈマシンアドレスと一致するとき、前記受信されたメッセージを処理することと、
ノンスの更新が必要であると決定したことに応答して、前記ノンスをインクリメントすることと、
を備える、非一時的プロセッサ可読記憶媒体。
[Ｃ１２６] 前記プロセッサ実行可能ソフトウェア命令は、
前記受信されたメッセージの前記ローリングＢｌｕｅｔｏｏｔｈマシンアドレスが前記予想されるＢｌｕｅｔｏｏｔｈマシンアドレスと一致しないとき、予め定義されたオフセット値のセットにより、前記ノンスを変更することと、
前記変更されたノンスに基づいて、ある期間の間、前記受信されたメッセージの前記ローリングＢｌｕｅｔｏｏｔｈマシンアドレスと比較するための、複数の新たな予想されるＢｌｕｅｔｏｏｔｈマシンアドレスを生成することと、
前記期間の間に一致が発見されないとき、前記受信されたメッセージを無視することと、
をさらに備える動作を実行する、Ｃ１２５に記載の非一時的プロセッサ可読記憶媒体。

[Ｃ１２７] Ｂｌｕｅｔｏｏｔｈを使用して、向上されたセキュリティで通信するための方法であって、
第１の通信デバイスにおいて、第２の通信デバイスとの通信リンクを確立することと、
前記第２の通信デバイスと共有されるノンスを記憶することと、
前記第２の通信デバイスにおいて、前記ノンスと、前記第１の通信デバイスと共有される暗号化アルゴリズムとを使用して、ローリングＢｌｕｅｔｏｏｔｈマシンアドレスを生成することと、
前記ローリングＢｌｕｅｔｏｏｔｈマシンアドレスを使用して、メッセージを前記第２の通信デバイスから前記第１の通信デバイスに送信することと、
前記第１の通信デバイスにおいて、前記通信リンクを介して、前記ローリングＢｌｕｅｔｏｏｔｈマシンアドレスを示す前記メッセージを受信することと、
前記第１の通信デバイスにおいて、前記ノンスと、前記第２の通信デバイスと共有される前記暗号化アルゴリズムとを使用して、前記第２の通信デバイスの予想されるＢｌｕｅｔｏｏｔｈマシンアドレスを生成することと、
前記受信されたメッセージの前記ローリングＢｌｕｅｔｏｏｔｈマシンアドレスを前記予想されるＢｌｕｅｔｏｏｔｈマシンアドレスと比較することと、
前記受信されたメッセージの前記ローリングＢｌｕｅｔｏｏｔｈマシンアドレスが前記第１の通信デバイスによって生成された前記予想されるＢｌｕｅｔｏｏｔｈマシンアドレスと一致するとき、前記受信されたメッセージを前記第１の通信デバイスにおいて処理することと、
ノンスの更新が必要であると決定したことに応答して、前記ノンスをインクリメントすることと、
を備える方法。
[Ｃ１２８] 第１の通信デバイスと、
第２の通信デバイスと、を備えるシステムであって、
前記第１の通信デバイスは、
第１のメモリと、
前記第２の通信デバイスによって受信されることが可能な短距離ワイヤレス信号をブロードキャストするように構成される第１の送受信機と、を備え、前記第１の送受信機は、
前記第２の通信デバイスとの通信リンクを確立することと、
前記第２の通信デバイスと共有されるノンスを記憶することと、
前記通信リンクを介して、ローリングＢｌｕｅｔｏｏｔｈマシンアドレスを示すメッセージを受信することと、
前記ノンスと、前記第２の通信デバイスと共有される暗号化アルゴリズムとを使用して、前記第２の通信デバイスの予想されるＢｌｕｅｔｏｏｔｈマシンアドレスを生成することと、
前記受信されたメッセージの前記ローリングＢｌｕｅｔｏｏｔｈマシンアドレスを前記予想されるＢｌｕｅｔｏｏｔｈマシンアドレスと比較することと、
前記受信されたメッセージの前記ローリングＢｌｕｅｔｏｏｔｈマシンアドレスが前記第１の通信デバイスによって生成された前記予想されるＢｌｕｅｔｏｏｔｈマシンアドレスと一致するとき、前記受信されたメッセージを処理することと、
ノンスの更新が必要であると決定したことに応答して、前記ノンスをインクリメントすることと
を備える動作を実行するプロセッサ実行可能命令によって構成され、
前記第２の通信デバイスは、
第２のメモリと、
前記第１の通信デバイスによって受信されることが可能な短距離ワイヤレス信号をブロードキャストするように構成される第２の送受信機と、を備え、前記第２の送受信機は、

前記第１の通信デバイスとの前記通信リンクを確立することと、
前記第１の通信デバイスと共有される前記ノンスを記憶することと、
前記ノンスと、前記第１の通信デバイスと共有される前記暗号化アルゴリズムとを使用して、前記ローリングＢｌｕｅｔｏｏｔｈマシンアドレスを生成することと、
前記ローリングＢｌｕｅｔｏｏｔｈマシンアドレスを使用して、前記メッセージを前記第１の通信デバイスに送信することと、
前記通信リンクを介して、入来するメッセージを前記第２の通信デバイスから受信することと、
前記ノンスの更新が必要であると決定したことに応答して、前記ノンスをインクリメントすることと、
を備える動作を実行するプロセッサ実行可能命令によって構成される、システム。