【公報種別】特許公報の訂正
【部門区分】第７部門第３区分
【発行日】令和4年5月31日(2022.5.31)

【特許番号】特許第7041162号(P7041162)
【登録日】令和4年3月14日(2022.3.14)
【特許公報発行日】令和4年3月23日(2022.3.23)
【年通号数】登録公報(特許)2022-049
【出願番号】特願2019-551651(P2019-551651)
【訂正要旨】特許権者の住所の誤載により、下記のとおり全文を訂正する。
【国際特許分類】
Ｈ０４Ｌ　9/32(2006.01)
Ｈ０４Ｌ　9/08(2006.01)
Ｈ０４Ｗ　12/04(2021.01)
【ＦＩ】
Ｈ０４Ｌ　9/32　２００Ｚ
Ｈ０４Ｌ　9/08　Ｆ
Ｈ０４Ｗ　12/04
【記】別紙のとおり

(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7041162号
(P7041162)

(45)発行日　令和4年3月23日(2022.3.23)

(24)登録日　令和4年3月14日(2022.3.14)

(51)国際特許分類

H04L	*9/32*	*(2006.01)*	H04L	9/32
H04L	*9/08*	*(2006.01)*	H04L	9/08
H04W	*12/04*	*(2021.01)*	H04W	12/04

FI

	200Z
	F

請求項の数　18　（全35頁）

(21)出願番号　特願2019-551651(P2019-551651)
(86)(22)出願日　平成30年3月15日(2018.3.15)
(65)公表番号　特表2020-516118(P2020-516118A)
(43)公表日　令和2年5月28日(2020.5.28)
(86)国際出願番号　PCT/EP2018/056491
(87)国際公開番号　WO2018/172171
(87)国際公開日　平成30年9月27日(2018.9.27)
審査請求日　令和3年3月11日(2021.3.11)
(31)優先権主張番号　17161856.4
(32)優先日　平成29年3月20日(2017.3.20)
(33)優先権主張国・地域又は機関
欧州特許庁(EP)

(73)特許権者　590000248
コーニンクレッカ フィリップス エヌヴェ
Koninklijke Philips N.V.
オランダ国 5656 アーヘー アインドーフェン ハイテック キャンパス 5
(74)代理人　110001690
特許業務法人M&Sパートナーズ
(72)発明者　バーンセン ヨハネス アーノルダス コーネリス
オランダ国 5656 アーエー アインドーフェン ハイ テック キャンパス 5
(72)発明者　ヴァン デ ラール フランシスカス アントニウス マリア

最終頁に続く

(54)【発明の名称】　相互認証システム

(57)【特許請求の範囲】
【請求項１】
通信プロトコルに従うレスポンダデバイスとのワイヤレス通信のためのイニシエータデバイスであって、
前記通信プロトコルが、
前記イニシエータデバイスによる前記レスポンダデバイスの片側認証、並びに
前記イニシエータデバイスによる前記レスポンダデバイスの及び前記レスポンダデバイスによる前記イニシエータデバイスの相互認証
のうちの１つである認証を適応させるための認証プロトコルを含み、
前記レスポンダデバイスが、
前記通信プロトコルに従うワイヤレス通信のためのレスポンダトランシーバと、
前記通信プロトコルを処理するためのレスポンダプロセッサとを備え、
前記イニシエータデバイスが、
前記通信プロトコルに従うワイヤレス通信のためのイニシエータトランシーバと、
前記通信プロトコルを処理するためのイニシエータプロセッサとを備え、
前記イニシエータプロセッサが、
前記レスポンダデバイスに送られることになるメッセージを作成することと、前記認証プロトコルに従って前記レスポンダデバイスから受信されたメッセージを分解することとを行うためのイニシエータメッセージユニットと、
ユーザ対話と前記レスポンダデバイスから受信されたメッセージとに応じて前記認証プロ

トコルに従ってイニシエータ状態を与えるためのイニシエータステートマシンとを備え、
前記イニシエータ状態は、
イニシエータ帯域外アクションを介して前記レスポンダデバイスからレスポンダ公開鍵を取得することによるブートストラッピングのための初期状態（ＩＳＴ）と、
前記ブートストラッピングが前記レスポンダ公開鍵を取得することによって正常に実行されたことを示すブートストラップ済み状態（ＢＳＴ）と、
前記認証が正常に実行されたことを示す認証済み状態（ＡＴＤ）と
を含み、
前記イニシエータメッセージユニットは、
前記ブートストラップ済み状態で送られることになり、イニシエータ公開鍵を検証するためのイニシエータベリファイアと前記レスポンダ公開鍵を検証するためのレスポンダベリファイアとを含む認証要求
を含むメッセージを作成し、
前記レスポンダ公開鍵に対応するレスポンダプライベート鍵に基づくレスポンダ片側認証データと、前記レスポンダデバイスがレスポンダ帯域外アクションを介して前記イニシエータデバイスから前記イニシエータ公開鍵を取得することを可能にするための前記相互認証が進行中であることを示す相互進行ステータスとを含む認証応答
を含むメッセージを分解し、
前記イニシエータステートマシンが、待機中相互認証のために、前記相互進行ステータスを受信するとつくことになる、相互認証中状態を与え、
前記イニシエータメッセージユニットが、
前記イニシエータ公開鍵と前記レスポンダプライベート鍵とに基づく相互レスポンダ認証データを含む相互認証応答
を分解し、
前記相互認証の確認を示す相互確認ステータスと、前記レスポンダ公開鍵と前記イニシエータ公開鍵に対応するイニシエータプライベート鍵とに基づく相互イニシエータ認証データとを含む相互認証確認
を作成する、イニシエータデバイス。
【請求項２】
前記イニシエータステートマシンは、前記相互認証応答を受信し、前記イニシエータプロセッサが前記レスポンダ公開鍵と前記イニシエータ公開鍵に対応するイニシエータプライベート鍵とに基づく前記相互レスポンダ認証データを正常に処理すると、前記認証済み状態につく、請求項１に記載のイニシエータデバイス。
【請求項３】
前記イニシエータメッセージユニットが、前記片側認証の場合、前記レスポンダ公開鍵に対応するレスポンダプライベート鍵に基づく片側レスポンダ認証データと、前記片側認証を示す片側ステータスとを含む片側認証応答を分解し、
前記イニシエータステートマシンは、前記イニシエータプロセッサが前記レスポンダ公開鍵とイニシエータ公開鍵に対応するイニシエータプライベート鍵とに基づく前記片側レスポンダ認証データを正常に処理すると、前記認証済み状態につく、
請求項１に記載のイニシエータデバイス。
【請求項４】
前記イニシエータステートマシンは、前記認証応答を受信し、前記イニシエータプロセッサが前記レスポンダ片側認証データを正常に処理しないと、前記ブートストラップ済み状態又は前記初期状態につく、
請求項２又は３に記載のイニシエータデバイス。
【請求項５】
前記イニシエータステートマシンは、前記相互認証応答を受信し、前記イニシエータプロセッサが前記相互レスポンダ認証データを正常に処理しないと、前記ブートストラップ済み状態又は前記初期状態につく、

請求項２に記載のイニシエータデバイス。
【請求項６】
前記イニシエータメッセージユニットが、前記相互進行ステータスを受信すると、相互待機中ステータスを含む待機中認証確認を作成する、
請求項２又は５に記載のイニシエータデバイス。
【請求項７】
通信プロトコルに従うイニシエータデバイスとのワイヤレス通信のためのレスポンダデバイスであって、
前記通信プロトコルが、
前記イニシエータデバイスによる前記レスポンダデバイスの片側認証、並びに
前記イニシエータデバイスによる前記レスポンダデバイスの及び前記レスポンダデバイスによる前記イニシエータデバイスの相互認証
のうちの１つである認証を適応させるための認証プロトコルを含み、
前記イニシエータデバイスが、
前記通信プロトコルに従うワイヤレス通信のためのイニシエータトランシーバと、
前記通信プロトコルを処理するためのイニシエータプロセッサとを備え、
前記レスポンダデバイスが、
前記通信プロトコルに従うワイヤレス通信のためのレスポンダトランシーバと、
前記通信プロトコルを処理するためのレスポンダプロセッサとを備え、前記レスポンダプロセッサが、
前記イニシエータデバイスに送られることになるメッセージを作成することと、前記認証プロトコルに従って前記イニシエータデバイスから受信されたメッセージを分解することとを行うためのレスポンダメッセージユニットと、
ユーザ対話と前記イニシエータデバイスから受信されたメッセージとに応じて前記認証プロトコルに従ってレスポンダ状態を与えるためのレスポンダステートマシンとを備え、前記レスポンダ状態は、
前記イニシエータデバイスからメッセージを受信するための待機中状態と、
前記認証が正常に実行されたことを示すレスポンダ認証済み状態と
を含み、
前記レスポンダステートマシンは、前記レスポンダデバイスがレスポンダ帯域外アクションを介して前記イニシエータデバイスからイニシエータ公開鍵を取得することを可能にするための相互レスポンダ認証中状態を与え、
前記レスポンダメッセージユニットは、
レスポンダ公開鍵に対応するレスポンダプライベート鍵に基づく片側レスポンダ認証データと、前記相互認証が進行中であることを示す相互進行ステータスとを含む認証応答
を含むメッセージを作成し、
イニシエータ公開鍵を検証するためのイニシエータベリファイアと前記レスポンダ公開鍵を検証するためのレスポンダベリファイアとを含む認証要求
を含むメッセージを分解し、
前記レスポンダステートマシンは、前記レスポンダプロセッサが前記イニシエータ公開鍵と前記レスポンダプライベート鍵とに基づくイニシエータ認証データを正常に処理すると、前記レスポンダ認証済み状態につく、レスポンダデバイス。
【請求項８】
前記レスポンダメッセージユニットが、
前記相互レスポンダ認証中状態で送られるべき相互認証応答であって、前記イニシエータ公開鍵と前記レスポンダ公開鍵に対応するレスポンダプライベート鍵とに基づく相互レスポンダ認証データを含む相互認証応答
を作成し、
前記相互認証の確認を示す相互確認ステータスと、前記レスポンダ公開鍵と前記イニシエータ公開鍵に対応するイニシエータプライベート鍵とに基づく相互イニシエータ認証デー

タとを含む相互認証確認
を分解する、請求項７に記載のレスポンダデバイス。
【請求項９】
前記レスポンダメッセージユニットが、前記片側認証の場合、前記レスポンダ公開鍵に対応するレスポンダプライベート鍵に基づく片側レスポンダ認証データと、前記片側認証を示す片側ステータスとを含む片側認証応答を作成し、
前記レスポンダステートマシンは、前記片側認証の場合、片側認証確認を受信し、前記レスポンダプロセッサが片側イニシエータ認証データを正常に処理すると、前記レスポンダ認証済み状態につく、
請求項７又は８に記載のレスポンダデバイス。
【請求項１０】
前記レスポンダステートマシンは、前記相互認証確認を受信し、前記レスポンダプロセッサが前記相互イニシエータ認証データを正常に処理しないと、前記待機中状態につく、
請求項８に記載のレスポンダデバイス。
【請求項１１】
前記レスポンダメッセージユニットが、相互待機中ステータスを含む待機中相互認証確認を分解し、
前記レスポンダステートマシンが、前記相互待機中ステータスを受信すると、前記相互レスポンダ認証中状態につく、
請求項８又は１０に記載のレスポンダデバイス。
【請求項１２】
前記レスポンダメッセージユニットが、片側イニシエータ認証データを含む前記待機中相互認証確認をさらに分解し、
前記レスポンダステートマシンは、前記レスポンダプロセッサが前記片側イニシエータ認証データを正常に処理しないと、前記待機中状態につく、
請求項１１に記載のレスポンダデバイス。
【請求項１３】
前記レスポンダデバイスが、
前記イニシエータデバイスから前記イニシエータ公開鍵を取得するために前記レスポンダ帯域外アクションを実行するためにユーザ対話を適応させるスポンダユーザインターフェース
を備える、請求項７から１２のいずれか一項に記載のレスポンダデバイス。
【請求項１４】
請求項１から６のいずれか一項に記載のイニシエータデバイスと、請求項７から１３のいずれか一項に記載のレスポンダデバイスとを備える、ワイヤレス通信システム。
【請求項１５】
通信プロトコルに従うレスポンダデバイスとのワイヤレス通信のためにイニシエータデバイスにおいて使用するためのイニシエータ方法であって、
前記通信プロトコルが、
前記イニシエータデバイスによる前記レスポンダデバイスの片側認証、並びに
前記イニシエータデバイスによる前記レスポンダデバイスの及び前記レスポンダデバイスによる前記イニシエータデバイスの相互認証
のうちの１つである認証を適応させるための認証プロトコルを含み、
前記イニシエータ方法は、
ユーザ対話と前記レスポンダデバイスから受信されたメッセージとに応じて前記認証プロトコルに従ってイニシエータ状態を与えるステップであって、前記イニシエータ状態が、
イニシエータ帯域外アクションを介して前記レスポンダデバイスからレスポンダ公開鍵を取得することによるブートストラッピングのための初期状態と、
前記ブートストラッピングが前記レスポンダ公開鍵を取得することによって正常に実行されたことを示すブートストラップ済み状態と、

前記認証が正常に実行されたことを示す認証済み状態と
を含む、与えるステップと、
前記ブートストラップ済み状態で送られることになり、イニシエータ公開鍵を検証するためのイニシエータベリファイアと前記レスポンダ公開鍵を検証するためのレスポンダベリファイアとを含む認証要求を作成するステップと、
前記レスポンダ公開鍵に対応するレスポンダプライベート鍵に基づく片側レスポンダ認証データと、前記レスポンダデバイスがレスポンダ帯域外アクションを介して前記イニシエータデバイスから前記イニシエータ公開鍵を取得することを可能にするための前記相互認証が進行中であることを示す相互進行ステータスとを含む認証応答を分解するステップと、
待機中相互認証のために、前記相互進行ステータスを受信するとつくことになる、相互認証中状態を与えるステップと、
前記イニシエータ公開鍵と前記レスポンダプライベート鍵とに基づく相互レスポンダ認証データを含む相互認証応答を分解するステップと、
前記相互認証の確認を示す相互確認ステータスと、前記レスポンダ公開鍵と前記イニシエータ公開鍵に対応するイニシエータプライベート鍵とに基づく相互イニシエータ認証データとを含む相互認証確認を作成するステップと、
前記相互認証応答を受信し、前記レスポンダ公開鍵と前記イニシエータ公開鍵に対応するイニシエータプライベート鍵とに基づく前記相互レスポンダ認証データを正常に処理すると、前記認証済み状態につくステップと
を有する、イニシエータ方法。
【請求項１６】
通信プロトコルに従うイニシエータデバイスとのワイヤレス通信のためにレスポンダデバイスにおいて使用するためのレスポンダ方法であって、
前記通信プロトコルが、
前記イニシエータデバイスによる前記レスポンダデバイスの片側認証、並びに
前記イニシエータデバイスによる前記レスポンダデバイスの及び前記レスポンダデバイスによる前記イニシエータデバイスの相互認証
のうちの１つである認証を適応させるための認証プロトコルを含み、
前記レスポンダ方法は、
ユーザ対話と前記イニシエータデバイスから受信されたメッセージとに応じて前記認証プロトコルに従ってレスポンダ状態を与えるステップであって、前記レスポンダ状態が、
前記イニシエータデバイスからメッセージを受信するための待機中状態と、
前記認証が正常に実行されたことを示すレスポンダ認証済み状態と
を含む、与えるステップと、
レスポンダ公開鍵に対応するレスポンダプライベート鍵に基づく片側レスポンダ認証データと、前記相互認証が進行中であることを示す相互進行ステータスとを含む認証応答を作成するステップと、
前記レスポンダデバイスがレスポンダ帯域外アクションを介して前記イニシエータデバイスからイニシエータ公開鍵を取得することを可能にするための相互レスポンダ認証中状態を与えるステップと、
前記相互レスポンダ認証中状態で送られることになり、前記イニシエータ公開鍵と前記レスポンダ公開鍵に対応するレスポンダプライベート鍵とに基づく相互レスポンダ認証データを含む相互認証応答を作成するステップと、
イニシエータ公開鍵を検証するためのイニシエータベリファイアと前記レスポンダ公開鍵を検証するためのレスポンダベリファイアとを含む認証要求を分解するステップと、
前記認証要求を正常に処理すると、レスポンダ認証中状態につくステップと
を有する、レスポンダ方法。
【請求項１７】
前記レスポンダ方法は、
前記相互認証の確認を示す相互確認ステータスと、前記レスポンダ公開鍵と前記イニシ

エータ公開鍵に対応するイニシエータプライベート鍵とに基づく相互イニシエータ認証データとを含む相互認証確認を分解するステップと、
前記イニシエータ公開鍵と前記レスポンダプライベート鍵とに基づく前記相互イニシエータ認証データを正常に処理すると、前記レスポンダ認証済み状態につくステップと
をさらに有する、請求項１６に記載のレスポンダ方法。
【請求項１８】
ネットワークからダウンロード可能な、並びに／或いはコンピュータ可読媒体及び／又はマイクロプロセッサ実行可能媒体に記憶されたコンピュータプログラムであって、前記コンピュータプログラムは、コンピュータ上で実行されたときに請求項１５に記載のイニシエータ方法又は請求項１６に記載のレスポンダ方法のいずれかを実施するためのプログラムコード命令を含む、コンピュータプログラム。

【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、通信プロトコルに従うワイヤレス通信のために構成されたイニシエータデバイス及びレスポンダデバイス、並びに、そのようなデバイスにおいて使用するための方法及びコンピュータプログラム製品に関する。通信プロトコルは、
－　イニシエータデバイスによるレスポンダデバイスの片側認証、並びに
－　イニシエータデバイスによるレスポンダデバイスの及びレスポンダデバイスによるイニシエータデバイスの相互認証
のうちの１つである認証を適応させるための認証プロトコルを含む。レスポンダデバイスは、通信プロトコルに従うワイヤレス通信のために構成されたレスポンダトランシーバと、通信プロトコルを処理するために構成されたレスポンダプロセッサとを備える。イニシエータデバイスは、通信プロトコルに従うワイヤレス通信のために構成されたイニシエータトランシーバと、通信プロトコルを処理するために構成されたイニシエータプロセッサとを備える。
【０００２】
本発明は、短距離ワイヤレス通信システム、たとえば屋内通信システムの分野に関し、より詳細には、レスポンダデバイス及び／又はイニシエータデバイスを認証することに基づいてワイヤレス接続をセキュアにセットアップするための様々なデバイス及び方法を提供する。Ｗｉ－Ｆｉ（登録商標）（参考文献［１］参照）は、ワイヤレスデバイス接続を確立するための通信プロトコル及び機構の一例を与える。
【背景技術】
【０００３】
ワイヤレス通信においてデバイスを識別し、認証するための手段として、公開鍵が使用される。公開鍵に関連付けられたプライベート鍵は、各デバイス内で生成され、暴露から保護されるべきである。デバイスはピアデバイスを認証するために公開鍵暗号技術を使用し、ここで、デバイスは、それらの公開鍵に対応するプライベート鍵の所有を証明し、さらなるセキュアな通信のために共有鍵を確立しなければならない。このセキュリティアーキテクチャは、デバイス間のセキュアな接続性の確立を簡略化し、デバイスをプロビジョニング及び接続する際のユーザビリティの改善のための基礎を与える。
【０００４】
認証プロトコルを開始するデバイスは、イニシエータの役割を果たす。イニシエータ要求に応答するデバイスは、レスポンダの役割を果たす。認証プロトコルは、イニシエータにレスポンダの認証を与え、随意に、レスポンダにイニシエータの認証を与える。これは、イニシエータが単方向認証を実行するためにレスポンダのブートストラッピング鍵を取得し、両方の当事者が随意に相互認証を実行するために互いのブートストラッピング鍵を取得したと仮定する。
【０００５】
Ｄｉｆｆｉｅ－Ｈｅｌｌｍａｎ（参考文献［６］参照）は、２つの当事者間の秘密鍵を確立するためのよく知られている技術であり、ここで、当事者間の通信は、確立された秘密鍵に関するいかなる情報も第三者に明らかにしない。２つの当事者は各々、それら自体の公開／プライベート鍵ペアを使用し、公開鍵を互いと交換する。各当事者は、それ自体のプライベート鍵と、他方の当事者の公開鍵と、場合によっては何らかの他の情報、たとえば各当事者からのナンス（乱数）とを使用して秘密鍵を計算することが可能である。各当事者は、それがＤｉｆｆｉｅ－Ｈｅｌｌｍａｎを実行するか、又はそれがより古い鍵ペアを再使用するたびに、新たに鍵ペアを生成する。
【０００６】
ネットワークを介してＤｉｆｆｉｅ－Ｈｅｌｌｍａｎを実行するとき、Ｄｉｆｆｉｅ－Ｈｅｌｌｍａｎを実行するための公開鍵を受信したデバイスは、この公開鍵がどのデバイスからのものであるかを知らない。これは、いわゆる中間者攻撃において攻撃者によって利

用される。攻撃者Ｅは、デバイスＡが接続することを希望する現実のデバイスＢになりすます。攻撃者Ｅは、デバイスＡとのＤｉｆｆｉｅ－Ｈｅｌｌｍａｎを実行し、デバイスＡとの秘密鍵Ｋａｅを確立する。同様に、攻撃者は、デバイスＢに対してデバイスＡになりすまし、デバイスＢとの秘密鍵Ｋｂｅを確立する。デバイスＡ又はデバイスＢの一方からメッセージが来たとき、攻撃者は、一方の秘密鍵を用いてメッセージを解読し、他方の秘密鍵を用いてそれを暗号化し、それを他方のデバイスにフォワーディングする。このようにして、デバイスＡとデバイスＢとは、いくらかの余分な遅延を除いて、それらの通信における妙な点に気づかない。しかし、攻撃者は、それらが何を通信するかに関する完全な知識を有する。

【０００７】

ワイヤレス通信のセキュリティを高めるために、プロトコルが、通信プロトコルに従うセキュアなワイヤレス通信に参加しているデバイスのうちの１つ又は複数の認証のために使用される。そのような認証プロトコルは第１の参加しているデバイスによって開始され、第１の参加しているデバイスは、通常、第２の参加しているデバイスと通信しているイニシエータデバイスと呼ばれ、第２の参加しているデバイスは、通常、レスポンダデバイスと呼ばれる。現在のコンテキストでは、イニシエータデバイスは、ワイヤレス通信を使用して接続をセットアップするための能力を有する任意の電子デバイスである。イニシエータデバイスは、ＰＣ、アクセスポイント、ワイヤレスドッキングステーション、ワイヤレスＵＳＢハブ、或いはワイヤレスビデオ又はＡＶモニターのような固定デバイスであるが、ラップトップ又はモバイルフォンのようなポータブルデバイスでもある。レスポンダデバイスは、同様に、ワイヤレス通信を使用して接続をセットアップするための能力を有する任意のタイプの電子デバイスである。

【０００８】

したがって、通信プロトコルは、レスポンダ及び／又はイニシエータの認証を適応させるための認証プロトコルを含む。認証は、イニシエータデバイスによるレスポンダデバイスの片側認証である。また、認証は、イニシエータデバイスによるレスポンダデバイスの認証とレスポンダデバイスによるイニシエータデバイスの認証とを伴う、相互認証である。

【発明の概要】

【発明が解決しようとする課題】

【０００９】

そのような認証プロトコルにおいて、たとえばＤｉｆｆｉｅ－Ｈｅｌｌｍａｎを使用するときの中間者攻撃を防ぐために、通信の他のやり方、すなわち、通常、帯域内通信と呼ばれる、ワイヤレス通信プロトコルに従って使用されるワイヤレス通信チャネル以外のやり方が、公開鍵又は公開鍵のハッシュを交換するために使用される。通信の他のやり方は、一般に帯域外（ＯＯＢ）通信と呼ばれ、それは、たとえば、バーコードのような視覚マーカーを使用するか、又はユーザにコードを入力させる。

【００１０】

その上、通信プロトコルは、一般に、メッセージのワイヤレス交換の雑音及び妨害に対処するための機構を有する。たとえば、返答が所定のタイムアウト期間内に受信されなかったとき、メッセージは再び送信される。所定の数の再試行の後に、通信プロトコルはアボートされる。

【００１１】

本発明の目的は、認証中の過度に長いタイムアウト期間を回避しながら、イニシエータデバイスとレスポンダデバイスとの間の接続を確実にセットアップするためのセキュアなワイヤレス通信システムを与えることである。

【課題を解決するための手段】

【００１２】

この目的で、添付の特許請求の範囲において定義されているデバイス及び方法が提供される。

【００１３】

本発明の一態様によれば、イニシエータデバイスが、通信プロトコルに従うレスポンダデバイスとのワイヤレス通信のために構成され、
通信プロトコルが、
－　イニシエータデバイスによるレスポンダデバイスの片側認証、並びに
－　イニシエータデバイスによるレスポンダデバイスの及びレスポンダデバイスによるイニシエータデバイスの相互認証
のうちの１つである認証を適応させるための認証プロトコルを含み、
レスポンダデバイスが、
－　通信プロトコルに従うワイヤレス通信のために構成されたレスポンダトランシーバと、
－　通信プロトコルを処理するために構成されたレスポンダプロセッサとを備え、
イニシエータデバイスが、
－　通信プロトコルに従うワイヤレス通信のために構成されたイニシエータトランシーバと、
－　通信プロトコルを処理するために構成されたイニシエータプロセッサとを備え、イニシエータプロセッサが、
－　レスポンダデバイスに送られることになるメッセージを作成することと、認証プロトコルに従ってレスポンダデバイスから受信されたメッセージを分解することとを行うためのイニシエータメッセージユニットと、
－　ユーザ対話とレスポンダデバイスから受信されたメッセージとに応じて認証プロトコルに従ってイニシエータ状態を与えるためのイニシエータステートマシンと
を備え、イニシエータ状態は、
イニシエータ帯域外アクションを介してレスポンダデバイスからレスポンダ公開鍵を取得することによるブートストラッピングのための初期状態と、
ブートストラッピングがレスポンダ公開鍵を取得することによって正常に実行されたことを示すブートストラップ済み状態（ｂｏｏｔｓｔｒａｐｐｅｄ　ｓｔａｔｅ）と、
認証が正常に実行されたことを示す認証済み状態（ａｕｔｈｅｎｔｉｃａｔｅｄ　ｓｔａｔｅ）と
を含み、
イニシエータメッセージユニットは、
－　ブートストラップ済み状態で送られることになり、イニシエータ公開鍵を検証するためのイニシエータベリファイアとレスポンダ公開鍵を検証するためのレスポンダベリファイアとを含む認証要求
を含むメッセージを作成するように構成され、
－　レスポンダ公開鍵に対応するレスポンダプライベート鍵に基づくレスポンダ片側認証データと、レスポンダデバイスがレスポンダ帯域外アクションを介してイニシエータデバイスからイニシエータ公開鍵を取得することを可能にするための相互認証が進行中であることを示す相互進行ステータス（ｍｕｔｕａｌ　ｐｒｏｇｒｅｓｓ　ｓｔａｔｕｓ）とを含む認証応答
を含むメッセージを分解するように構成され、
－　相互認証の確認を示す相互確認ステータスと、レスポンダ公開鍵とイニシエータ公開鍵に対応するイニシエータプライベート鍵とに基づく相互イニシエータ認証データとを含む相互認証確認
を作成するように構成される。
【００１４】
本発明のさらなる態様によれば、片側認証方法に加えて、又はその代替として、イニシエータデバイスによるレスポンダデバイスの及びレスポンダデバイスによるイニシエータデバイスの相互認証が実行され得る。この態様によれば、イニシエータステートマシンは、待機中相互認証（ａｗａｉｔｉｎｇ　ｍｕｔｕａｌ　ａｕｔｈｅｎｔｉｃａｔｉｏｎ）のために、相互進行ステータスを受信するとつくことになる（ｅｎｇａｇｅ）、相互認証中状態（ａｕｔｈｅｎｔｉｃａｔｉｎｇ　ｓｔａｔｅ）を与えるように構成され、

イニシエータメッセージユニットが、
－　イニシエータ公開鍵とレスポンダプライベート鍵とに基づく相互レスポンダ認証データを含む相互認証応答
を分解するように構成され、
イニシエータステートマシンは、相互認証応答を受信し、イニシエータプロセッサがレスポンダ公開鍵とイニシエータ公開鍵に対応するイニシエータプライベート鍵とに基づく相互レスポンダ認証データを正常に処理すると、認証済み状態につくように構成される。
【００１５】
本発明のさらなる態様によれば、レスポンダデバイスが、通信プロトコルに従うイニシエータデバイスとのワイヤレス通信のために構成され、
通信プロトコルが、
－　イニシエータデバイスによるレスポンダデバイスの片側認証、並びに
－　イニシエータデバイスによるレスポンダデバイスの及びレスポンダデバイスによるイニシエータデバイスの相互認証
のうちの１つである認証を適応させるための認証プロトコルを含み、
イニシエータデバイスが、
－　通信プロトコルに従うワイヤレス通信のために構成されたイニシエータトランシーバと、
－　通信プロトコルを処理するために構成されたイニシエータプロセッサとを備え、
レスポンダデバイスが、
－　通信プロトコルに従うワイヤレス通信のために構成されたレスポンダトランシーバと、
－　通信プロトコルを処理するために構成されたレスポンダプロセッサとを備え、レスポンダプロセッサが、
－　イニシエータデバイスに送られることになるメッセージを作成することと、認証プロトコルに従ってイニシエータデバイスから受信されたメッセージを分解することとを行うためのレスポンダメッセージユニットと、
－　ユーザ対話とイニシエータデバイスから受信されたメッセージとに応じて認証プロトコルに従ってレスポンダ状態を与えるためのレスポンダステートマシンとを備え、レスポンダ状態は、
イニシエータデバイスからメッセージを受信するための待機中状態（ａｗａｉｔｉｎｇ　ｓｔａｔｅ）と、
認証が正常に実行されたことを示すレスポンダ認証済み状態と
を含み、
レスポンダメッセージユニットは、
－　レスポンダ公開鍵に対応するレスポンダプライベート鍵に基づく片側レスポンダ認証データと、相互認証が進行中であることを示す相互進行ステータスとを含む認証応答
を含むメッセージを作成するように構成され、
－　イニシエータ公開鍵を検証するためのイニシエータベリファイアとレスポンダ公開鍵を検証するためのレスポンダベリファイアとを含む認証要求
を含むメッセージを分解するように構成される。
【００１６】
本発明のさらなる態様によれば、片側認証方法に加えて、又はその代替として、イニシエータデバイスによるレスポンダデバイスの及びレスポンダデバイスによるイニシエータデバイスの相互認証が実行され得る。この態様によれば、レスポンダステートマシンは、
－　レスポンダデバイスがレスポンダ帯域外アクションを介してイニシエータデバイスからイニシエータ公開鍵を取得することを可能にするための相互レスポンダ認証中状態を与えるように構成され、
レスポンダメッセージユニットが、
－　相互レスポンダ認証中状態で送られることになり、イニシエータ公開鍵とレスポンダ公開鍵に対応するレスポンダプライベート鍵とに基づく相互レスポンダ認証データを含む

相互認証応答
を作成するように構成され、
－　相互認証の確認を示す相互確認ステータスと、レスポンダ公開鍵とイニシエータ公開鍵に対応するイニシエータプライベート鍵とに基づく相互イニシエータ認証データとを含む相互認証確認
を分解するように構成され、
レスポンダステートマシンは、レスポンダプロセッサがイニシエータ公開鍵とレスポンダプライベート鍵とに基づくイニシエータ認証データを正常に処理すると、レスポンダ認証済み状態につくように構成される。
【００１７】
本発明のさらなる態様によれば、通信プロトコルに従うレスポンダデバイスとのワイヤレス通信のためにイニシエータデバイスにおいて使用するためのイニシエータ方法が提供され、
通信プロトコルが、
－　イニシエータデバイスによるレスポンダデバイスの片側認証、並びに
－　イニシエータデバイスによるレスポンダデバイスの及びレスポンダデバイスによるイニシエータデバイスの相互認証
のうちの１つである認証を適応させるための認証プロトコルを含み、
イニシエータ方法は、
－　ユーザ対話とレスポンダデバイスから受信されたメッセージとに応じて認証プロトコルに従ってイニシエータ状態を与えるステップであって、イニシエータ状態が、
イニシエータ帯域外アクションを介してレスポンダデバイスからレスポンダ公開鍵を取得することによるブートストラッピングのための初期状態と、
ブートストラッピングがレスポンダ公開鍵を取得することによって正常に実行されたことを示すブートストラップ済み状態と、
認証が正常に実行されたことを示す認証済み状態と
を含む、与えるステップと、
－　ブートストラップ済み状態で送られることになり、イニシエータ公開鍵を検証するためのイニシエータベリファイアとレスポンダ公開鍵を検証するためのレスポンダベリファイアとを含む認証要求を作成するステップと、
－　レスポンダ公開鍵に対応するレスポンダプライベート鍵に基づく片側レスポンダ認証データと、レスポンダデバイスがレスポンダ帯域外アクションを介してイニシエータデバイスからイニシエータ公開鍵を取得することを可能にするための相互認証が進行中であることを示す相互進行ステータスとを含む認証応答を分解するステップと、
－　待機中相互認証のために、相互進行ステータスを受信するとつくことになる、相互認証中状態を与えるステップと、
－　イニシエータ公開鍵とレスポンダプライベート鍵とに基づく相互レスポンダ認証データを含む相互認証応答を分解するステップと、
－　相互認証の確認を示す相互確認ステータスと、レスポンダ公開鍵とイニシエータ公開鍵に対応するイニシエータプライベート鍵とに基づく相互イニシエータ認証データとを含む相互認証確認を作成するステップと、
－　相互認証応答を受信し、レスポンダ公開鍵とイニシエータ公開鍵に対応するイニシエータプライベート鍵とに基づく相互レスポンダ認証データを正常に処理すると、認証済み状態につくステップと
を有する。
【００１８】
本発明のさらなる態様によれば、通信プロトコルに従うイニシエータデバイスとのワイヤレス通信のためにレスポンダデバイスにおいて使用するためのレスポンダ方法が提供され、
通信プロトコルが、
－　イニシエータデバイスによるレスポンダデバイスの片側認証、並びに

－　イニシエータデバイスによるレスポンダデバイスの及びレスポンダデバイスによるイニシエータデバイスの相互認証
のうちの１つである認証を適応させるための認証プロトコルを含み、
レスポンダ方法は、
－　ユーザ対話とイニシエータデバイスから受信されたメッセージとに応じて認証プロトコルに従ってレスポンダ状態を与えるステップであって、レスポンダ状態が、
イニシエータデバイスからメッセージを受信するための待機中状態と、
認証が正常に実行されたことを示すレスポンダ認証済み状態と
を含む、与えるステップと、
－　レスポンダ公開鍵に対応するレスポンダプライベート鍵に基づく片側レスポンダ認証データと、相互認証が進行中であることを示す相互進行ステータスとを含む認証応答を作成するステップと、
－　イニシエータ公開鍵を検証するためのイニシエータベリファイアとレスポンダ公開鍵を検証するためのレスポンダベリファイアとを含む認証要求を分解するステップと、
－　認証要求を正常に処理すると、レスポンダ認証中状態につくステップと、
－　レスポンダデバイスがレスポンダ帯域外アクションを介してイニシエータデバイスからイニシエータ公開鍵を取得することを可能にするための相互レスポンダ認証中状態を与えるステップと、
－　相互レスポンダ認証中状態で送られることになり、イニシエータ公開鍵とレスポンダ公開鍵に対応するレスポンダプライベート鍵とに基づく相互レスポンダ認証データを含む相互認証応答を作成するステップと、
－　相互認証の確認を示す相互確認ステータスと、レスポンダ公開鍵とイニシエータ公開鍵に対応するイニシエータプライベート鍵とに基づく相互イニシエータ認証データとを含む相互認証確認を分解するステップと、
－　イニシエータ公開鍵とレスポンダプライベート鍵とに基づく相互イニシエータ認証データを正常に処理すると、レスポンダ認証済み状態につくステップと
を有する。
【００１９】
本発明のさらなる態様によれば、ネットワークからダウンロード可能な、並びに／或いはコンピュータ可読媒体及び／又はマイクロプロセッサ実行可能媒体に記憶されたコンピュータプログラム製品が提供され、コンピュータプログラム製品は、コンピュータ上で実行されたときに上記の方法を実施するためのプログラムコード命令を含む。
【００２０】
上記の特徴は、認証プロトコルが片側認証と相互通信の両方をサポートするという効果を有する。プロトコルは様々なメッセージを交換することによって実行され、メッセージは、それぞれイニシエータメッセージユニット及びレスポンダメッセージユニットによって作成され、分解される。さらに、メッセージを交換することとメッセージ中の要素を処理することとのシーケンスは、それぞれイニシエータステートマシン及びレスポンダステートマシンを介して制御され、イニシエータステートマシンとレスポンダステートマシンとは、認証プロトコルを実行する間のイニシエータデバイス及びレスポンダデバイスの状態を決定する。
【００２１】
さらに、認証プロトコルは、レスポンダデバイスからレスポンダ公開鍵を取得するために帯域外（ＯＯＢ）通信を使用することを可能にする。イニシエータ側における帯域外アクションは、レスポンダ公開鍵自体、或いは、さらなる通信アクションを介して受信された、たとえば、帯域内メッセージを受信したか又は以前の通信セッションにおいて記憶されたレスポンダ公開鍵を検証するための符号化されたレスポンダ公開鍵データを受信することを伴う。鍵材料の初期量を取得するプロセスは、ブートストラッピングと呼ばれる。ブートストラッピングが成功した後に、イニシエータは、レスポンダデバイスの認証を実行するために認証中状態につく。

【００２２】
しかしながら、相互認証の場合、レスポンダデバイスは、レスポンダ帯域外アクションを介してイニシエータデバイスからイニシエータ公開鍵を取得しなければならない。たとえばユーザ対話を伴う場合、イニシエータデバイス上のコードを読み取り、それをレスポンダデバイスに入力するか、或いはイニシエータデバイス上のバーコード又はＱＲコード（登録商標）などの機械可読コードの写真を撮ることなど、ＯＯＢ通信を介してコードを交換することは、長い時間を要する（数十秒程度）。そのような時間は、ワイヤレス通信を介してメッセージを交換する時間（通常、数ミリ秒以下）と比較して長い。イニシエータデバイスは、認証要求を送った後に、認証応答を待ち続ける。相互認証を可能にするために、完全な認証応答は、イニシエータ公開鍵にも基づいてレスポンダ認証データを与えることを必要とする。発明者は、完全な認証応答が、レスポンダＯＯＢアクションに十分な比較的長い時間の後にのみ送信されることがわかった。したがって、旧来の相互認証プロトコルでは長いタイムアウト期間が必要とされる。不利なことに、たとえば雑音により認証要求が受信されなかった場合、再送信は、長いタイムアウト期間の後にのみ行われる。
【００２３】
また、認証要求が受信されなかった場合、又は、認証応答が誤ったデータを含んでおり、それにより認証が失敗した場合、ユーザは、イニシエータデバイスがユーザに認証が失敗したことを知らせるまで長い時間待たなければならない。そのような長いタイムアウト期間を回避するために、レスポンダ公開鍵に対応するレスポンダプライベート鍵に基づくレスポンダ認証データを含んでいる認証応答が与えられており、それには、いかなるイニシエータ鍵をも伴わない。有利なことに、そのような認証応答は、認証要求を処理した直後に送信され、認証要求を送ったときのイニシエータデバイスにおける短いタイムアウトを可能にする。したがって、雑音の場合、再送信は短いタイムアウトに基づいて行われることになり、ユーザは、認証試みがいつ失敗したかをはるかに迅速に知ることになる。
【００２４】
その上、発明者は、そのような認証応答が片側認証のための応答と同様であることがわかった。しかしながら、相互認証が実行されることになる。したがって、さらに、上記の拡張された認証応答は、相互認証が進行中であることを示す相互進行ステータスをさらに含んでいる。また、イニシエータステートマシンは、待機中相互認証のために、相互進行ステータスを受信するとつくことになる、相互認証中状態を与えるように構成される。有利なことに、相互認証中状態では、イニシエータデバイスは相互認証に気づいており、それは、イニシエータ公開鍵とレスポンダプライベート鍵とに基づく相互レスポンダ認証データを含む相互認証応答を後で受信することを可能にする。その後、受信された相互レスポンダ認証データの処理が成功した場合、イニシエータは、相互認証の確認を示す相互確認ステータスと、レスポンダ公開鍵とイニシエータ公開鍵に対応するイニシエータプライベート鍵とに基づくイニシエータ認証データとを含む相互認証確認を送信する。
【００２５】
したがって、第１の認証応答メッセージ中で追加の相互認証状態及び相互進行ステータスを与えることによって、相互認証は、長いタイムアウト期間を必要とすることなしに実行され、同じ認証プロトコルにおいて、片側認証をも可能にする。有利なことに、ワイヤレス通信のための条件が悪い場合、必要とされるメッセージの再送信は、短いタイムアウト期間により、比較的高速である。
【００２６】
本発明による方法は、コンピュータ上でコンピュータ実施方法として、又は専用ハードウェアで、又はその両方の組合せで実施される。本発明による方法のための実行可能コードが、コンピュータプログラム製品に記憶される。コンピュータプログラム製品の例は、メモリスティックなどのメモリデバイス、光ディスクなどの光記憶デバイス、集積回路、サーバ、オンラインソフトウェアなどを含む。コンピュータプログラム製品は、コンピュータプログラム製品がコンピュータ上で実行されるとき、本発明による方法を実行するためのコンピュータ可読媒体に記憶された非一時的プログラムコード手段を含む。一実施形態

では、コンピュータプログラムは、コンピュータプログラムがコンピュータ上で実行されるとき、本発明による方法のすべてのステップ又は段階を実行するように適応されたコンピュータプログラムコード手段を含む。好ましくは、コンピュータプログラムは、コンピュータ可読媒体上で具現される。ネットワークからダウンロード可能な、並びに／或いはコンピュータ可読媒体及び／又はマイクロプロセッサ実行可能媒体に記憶されたコンピュータプログラム製品が提供され、コンピュータプログラム製品は、コンピュータ上で実行されたときに上記で説明された方法を実施するためのプログラムコード命令を含む。

【００２７】

本発明の別の態様は、コンピュータプログラムをダウンロードのために利用可能にする、たとえばアプリケーションに含まれるようにする方法を提供する。この態様は、コンピュータプログラムが、たとえば、ＡｐｐｌｅのＡｐｐ　Ｓｔｏｒｅ、ＧｏｏｇｌｅのＰｌａｙ　Ｓｔｏｒｅ、又はＭｉｃｒｏｓｏｆｔのＷｉｎｄｏｗｓ　Ｓｔｏｒｅにアップロードされるとき、及びコンピュータプログラムが、そのようなストアからダウンロードするために利用可能であるとき、使用される。

【００２８】

本発明によるデバイス及び方法のさらなる好ましい実施形態が添付の特許請求の範囲において与えられ、それの開示は参照により本明細書に組み込まれる。

【００２９】

本発明のこれら及び他の態様は、以下の説明において例として及び添付の図面を参照しながら説明される実施形態から明らかになり、さらにそれらを参照して解明されよう。

【図面の簡単な説明】

【００３０】

【図１】ワイヤレス通信及び認証のためのデバイスを示す図である。
【図２】認証プロトコルの概略図である。
【図３】イニシエータステートマシンの一例を示す図である。
【図４】レスポンダステートマシンの一例を示す図である。
【図５】イニシエータのための方法を示す図である。
【図６】レスポンダのための方法を示す図である。
【図７ａ】コンピュータ可読媒体を示す図である。
【図７ｂ】プロセッサシステムの概略表現を示す図である。

【発明を実施するための形態】

【００３１】

図は、単に概略であり、一定の縮尺で描かれていない。図において、すでに説明された要素に対応する要素は同じ参照番号を有する。

【００３２】

以下の略語が使用される。

状態：

ＩＳＴ　初期状態
ＢＳＴ　ブートストラップ済み
ＡＧ１　認証中（イニシエータ、片方向）
ＡＧ２　相互認証中（イニシエータ、相互）
ＡＴＤ　認証済み（イニシエータ）
ＡＷＧ　待機中（Ａｗａｉｔｉｎｇ）（レスポンダ）
ＡＲ１　認証中（レスポンダ、片方向）
ＡＲ２　相互認証中（レスポンダ、相互）
ＡＲＤ　認証済み（レスポンダ）

メッセージ：

ＡＲＱ　認証要求
ＡＲＰ　認証応答
ＡＣＦ１　認証確認（片方向）

ＡＣＦ２　相互認証確認
ＡＲＰ１　認証応答（片方向）
ＡＲＰ２　相互認証応答
イベント／アクション／ステータス：
ＯＯＢ　帯域外（通信アクション）
ＯＯＢ＿Ｉ　帯域外（イニシエータによる通信アクション）
ＯＯＢ＿Ｒ　帯域外（レスポンダによる通信アクション）
ＢＡ　不正な認証（Ｂａｄ　Ａｕｔｈｅｎｔｉｃａｔｉｏｎ）（イベント）
ＢＴＧ　ブートストラッピング（イベント）
ＮＰ　ピアなし（Ｎｏ　Ｐｅｅｒ）（イベント）
ＴＯ　タイムアウト（イベント）
ＴＲ　トリガ（イベント）
ＭＰＳ　相互進行ステータス
ＭＡＳ　相互待機中ステータス
ＭＣＳ　相互確認ステータス
鍵：
B_I　イニシエータの公開ブートストラッピング鍵
B_R　レスポンダの公開ブートストラッピング鍵
P_I　イニシエータの公開鍵
P_R　レスポンダの公開鍵
b_I　B_Iに対応するイニシエータプライベート鍵
b_R　B_Rに対応するレスポンダプライベート鍵

【００３３】

図１は、ワイヤレス通信及び認証のためのデバイスを示す。ワイヤレス通信のためのシステム１００は、イニシエータデバイス１１０とレスポンダデバイス１２０とを備え、それらのデバイスは物理的に離れている。イニシエータデバイスは、通信プロトコルに従うワイヤレス通信のために構成されたイニシエータトランシーバ１１１と、通信プロトコルを処理するために構成されたイニシエータプロセッサ１１２とを備える。同様に、レスポンダデバイスは、通信プロトコルに従うワイヤレス通信のために構成されたレスポンダトランシーバ１２１と、通信プロトコルを処理するために構成されたレスポンダプロセッサ１２２とを備える。それらのデバイスは、トランシーバ１１１とトランシーバ１２１とを接続する形状１３０及び矢印によって概略的に示されているように、ワイヤレス通信のために装備される。イニシエータデバイスはユーザインターフェース１１３を備え、ユーザインターフェース１１３は、１つ又は複数のボタン１１５、キーボード、ディスプレイ、タッチスクリーンなど、よく知られている要素を含む。レスポンダデバイスも、ユーザインターフェース１２３を備える。レスポンダユーザインターフェースは、イニシエータデバイスからイニシエータ公開鍵を取得するためにレスポンダ帯域外アクションを実行するためにユーザ対話を適応させるために構成される。

【００３４】

それらのデバイスは、イニシエータデバイスとレスポンダデバイスとの間の通信プロトコルに従うワイヤレス通信のために構成される。それらのデバイスは、イニシエータデバイスによるレスポンダデバイスの片側認証、並びに、イニシエータデバイスによるレスポンダデバイスの及びレスポンダデバイスによるイニシエータデバイスの相互認証のうちの１つである認証を適応させるための認証プロトコルを実行するために構成され、一例について図２を参照しながら以下で詳述する。通信プロトコルは認証プロトコルを含む。例では、通信プロトコルは、ＩＥＥＥ８０２．１１に従うＷｉ－Ｆｉ（登録商標）である［参考文献１］が、以下で解明されるようなシステムに基づく適切な認証プロトコルを与えられたとき、Ｂｌｕｅｔｏｏｔｈ（登録商標）など、他のワイヤレスプロトコルも使用される。

【００３５】

イニシエータプロセッサ１１２は、レスポンダデバイスに送られることになるメッセージ

を作成することと、認証プロトコルに従ってレスポンダデバイスから受信されたメッセージを分解することとを行うためのイニシエータメッセージユニット１１６を備える。イニシエータプロセッサは、ユーザ対話とレスポンダデバイスから受信されたメッセージとに応じて認証プロトコルに従ってイニシエータ状態を与えるためのイニシエータステートマシン１１７をも備え、一例について図３を参照しながら以下で詳述する。

【００３６】

レスポンダプロセッサ１２２は、イニシエータデバイスに送られることになるメッセージを作成することと、認証プロトコルに従ってイニシエータデバイスから受信されたメッセージを分解することとを行うためのレスポンダメッセージユニット１２６を備える。レスポンダプロセッサは、ユーザ対話とイニシエータデバイスから受信されたメッセージとに応じて認証プロトコルに従ってレスポンダ状態を与えるためのレスポンダステートマシン１２７をも備える。

【００３７】

それぞれのメッセージユニット及びステートマシンを使用して、それぞれのメッセージ並びにそれぞれのイニシエータ状態及びレスポンダ状態に基づいて認証プロトコルを適応させるためのイニシエータプロセッサ及びレスポンダプロセッサの機能は、図２、図３及び図４を参照しながら以下で解明される。

【００３８】

認証のために、提案するシステムは、ＲＳＡ、［７］参照、又は楕円曲線暗号（ＥＣＣ）、［８］参照、など、任意の形態の公開鍵暗号法を使用する。

【００３９】

図２は、認証プロトコルの概略図を示す。認証プロトコル２００に従って、第１のデバイスＩＮＩＴ＿ＤＥＶは、下方向で時間の進行を表す２つの垂直タイムライン間の矢印によって示されているように、メッセージを第２のデバイスＲＥＳＰ＿ＤＥＶと交換する。第１のデバイスは、ＩＳＴにおいて開始するイニシエータデバイスであり、第２のデバイスは、ＡＷＧにおいて開始するレスポンダデバイスであるが、そのような役割は逆転される。メッセージは、送信側におけるメッセージユニットによって作成され、受信側におけるメッセージユニットによって分解される。

【００４０】

本明細書では、B_Iはイニシエータの公開ブートストラッピング鍵を示し、b_Iは対応するプライベート鍵を示す。同様に、B_Rはレスポンダの公開ブートストラッピング鍵を示し、b_Rは対応するプライベート鍵を示す。Ｈはハッシュ関数を示し、たとえば、そのようなものとして知られている適切なハッシュ片方向アルゴリズムに基づく。ハッシュ関数の好適な例は、参考文献［４］において見つけられ得る。

【００４１】

イニシエータ公開鍵のハッシュ値は、Ｈ（B_I）によって示される。ハッシュ値は、ハッシュ保護値（ｈａｓｈ－ｐｒｏｔｅｃｔｅｄ　ｖａｌｕｅ）に対応することが容易に検証され得るが、同じハッシュを維持しながらそのような値を操作することはほぼ不可能である。認証データは、１つ又は複数の鍵、すなわち、それぞれの公開鍵及びプライベート鍵に基づいて算出され、たとえば$\{auth1\}_{k1}$によって示され、$\{auth1\}_{k1}$は、鍵ｋ１によって暗号化されたａｕｔｈ１の値を意味し、｛ａｕｔｈ１｝はａｕｔｈ１の値を意味する。たとえば前述のＤｉｆｆｉｅ－Ｈｅｌｌｍａｎ暗号化システムから、そのような鍵は生成され、そのようによく知られているように、符号化及び復号すること、シグネチャ又は制御値を生成すること、並びにそのような値を検証することのために使用される。

【００４２】

最初に、イニシエータデバイスは、イニシエータ帯域外アクションを介してレスポンダデバイスからレスポンダ公開鍵を取得することによるブートストラッピングを実行する。ＯＯＢアクションは、ＯＯＢアクションとマークされた破線矢印によって示されている（対応して図１において矢印１４０によって示されている）。ＯＯＢアクションの様々な例は

、参考文献［２］、第１０章に記載されている。他の例は、ユーザが、イニシエータデバイス上のコードを読み取り、それをレスポンダデバイスに入力すること、ユーザが、イニシエータデバイスのカメラを用いて、レスポンダデバイスにプリントされた又はレスポンダデバイスによって表示されたバーコード又はＱＲコード（登録商標）などの機械可読コードの写真を撮ることである。

【００４３】

その後、イニシエータメッセージユニットは、ブートストラップ済み状態で送られることになる認証要求ＡＲＱを作成する。認証要求は、イニシエータ公開鍵を検証するためのイニシエータベリファイアＨ（B_I）とレスポンダ公開鍵を検証するためのレスポンダベリファイアＨ（B_R）とを含んでいる。ＡＲＱは、イニシエータ公開鍵P_Iと、イニシエータナンスＩ－ｎｏｎｃｅ及びイニシエータ能力データＩ－ｃａｐａｂｉｌｉｔｉｅｓのようなさらなるイニシエータデータとをさらに含んでおり、さらなるイニシエータデータは第１の鍵K_1を使用して符号化され、｛Ｉ－ｎｏｎｃｅ｜Ｉ－ｃａｐａｂｉｌｉｔｉｅｓ｝$_{K_1}$によって示される。第１の鍵K_1は、レスポンダ公開鍵B_Rとイニシエータ公開鍵P_Iに対応するイニシエータプライベート鍵p_Iとから、Ｄｉｆｆｉｅ－Ｈｅｌｌｍａｎ様式でイニシエータによって導出される。第１の鍵K_1は、イニシエータ公開鍵P_Iとレスポンダ公開鍵B_Rに対応するレスポンダプライベート鍵b_Rとから、Ｄｉｆｆｉｅ－Ｈｅｌｌｍａｎ様式でレスポンダによって導出される。対応して、レスポンダメッセージユニットは、認証要求ＡＲＱを分解するように構成される。

【００４４】

タイムアウトＴＯの後に、応答が受信されなかったとき、ＡＲＱは、たとえば３回まで再び送信される。応答ＡＲＰ１が時間内に受信されると仮定される。

【００４５】

レスポンダメッセージユニットは、認証応答ＡＲＰ１を作成するように構成され、認証応答ＡＲＰ１は、片側レスポンダ認証データ｛Ｒ－ａｕｔｈ１｝$_{k_1}$を含んでいる。ＡＲＰ１は、レスポンダ公開鍵P_Rと、レスポンダナンスＲ－ｎｏｎｃｅのようなさらなるレスポンダデータとをさらに含んでいる。第１の中間鍵k_1は、イニシエータ公開鍵P_Iに基づき、（P_RがＡＲＰ１中に存在していた場合）レスポンダ公開鍵（P_R）に対応するレスポンダプライベート鍵（p_R）に基づき、レスポンダ公開鍵（B_R）に対応するレスポンダプライベート鍵（b_R）に基づく。第１の中間鍵は、レスポンダデバイスの片側認証に適している。Ｒ－ａｕｔｈ１の値は、イニシエータナンスＩ－ｎｏｎｃｅ、レスポンダナンスＲ－ｎｏｎｃｅ、及び／又はP_R、B_R及びP_Iなどの使用される公開鍵など、認証プロトコルにおいて使用される値のうちの任意の選ばれた値の連結（のハッシュ）である。ナンスのランダム性により、Ｒ－ａｕｔｈ１の値はプロトコルが実行されるたびに異なり、それにより、リプレイアタックから保護する。相互認証の場合、ＡＲＰ１は、レスポンダデバイスがレスポンダ帯域外アクションを介してイニシエータデバイスからイニシエータ公開鍵を取得することを可能にするための、相互認証が進行中であることを示す相互進行ステータスをも含む。対応して、イニシエータメッセージユニットは、認証応答ＡＲＰ１を分解するように構成される。

【００４６】

随意に、イニシエータメッセージユニットは、認証中状態で相互進行ステータスを受信すると、相互待機中ステータスを含んでいる待機中認証確認ＡＣＦ１を作成するように構成される。ＡＣＦ１は、レスポンダ公開鍵（B_R）とイニシエータ公開鍵P_Iに対応するイニシエータプライベート鍵（p_I）とに基づく片側イニシエータ認証データ｛Ｉ－ａｕｔｈ１｝$_{k_1}$を含んでいる。｛Ｉ－ａｕｔｈ１｝の値は、同じ入力を使用して｛Ｒ－ａｕｔｈ１｝と同様の様式で計算される。しかしながら、リプレイアタックから守るために、｛Ｉ－ａｕｔｈ１｝の値は｛Ｒ－ａｕｔｈ１｝の値とは異なるべきである。したがって、ハッシュを計算するときの入力の順序は別様に選択されるべきであり、及び／又は、｛Ｒ－ａｕｔｈ１｝についてのハッシュの計算におけるものとは異なる一定値がハッシュに含まれるべきである。対応して、レスポンダメッセージユニットは、待機中認証確認ＡＣＦ１

を分解するように構成される。

【００４７】

その後、レスポンダデバイスは、レスポンダ帯域外アクションを介してイニシエータデバイスからイニシエータ公開鍵を取得することを実行するか、又は、それをすでに実行している。ＯＯＢアクションは、ＯＯＢアクションとマークされた破線矢印によって示されている（対応して図１において矢印１４０によって示されている）。取得することを完了すると、レスポンダステートマシンは、相互認証応答ＡＲＰ２を送るために、以下で解明されるように進む。

【００４８】

レスポンダメッセージユニットは、相互レスポンダ認証データ｛Ｒ－ａｕｔｈ２｝$_{k2}$を含む相互認証応答ＡＲＰ２を作成するように構成される。ＡＲＰ２は、レスポンダ公開鍵P_Rと、レスポンダナンスＲ－ｎｏｎｃｅのようなさらなるレスポンダデータとをさらに含んでいる。第２の中間鍵k_2は、イニシエータ公開鍵（B_I）とレスポンダ公開鍵（B_R）に対応するレスポンダプライベート鍵（b_R）とに基づく。第２の中間鍵は、レスポンダデバイスとイニシエータデバイスとの相互認証に適している。第２の中間鍵は、レスポンダにおける｛b_R、p_R、B_I及びP_I｝、又はイニシエータにおける｛p_I、b_I、B_R及びP_R｝を使用して決定される。Ｒ－ａｕｔｈ２の値は、イニシエータナンスＩ－ｎｏｎｃｅ、レスポンダナンスＲ－ｎｏｎｃｅ、及びB_I、B_R、P_R及びP_Iなどの使用される公開鍵など、認証プロトコルにおいて使用される値の連結のハッシュである。ナンスのランダム性により、｛Ｒ－ａｕｔｈ２｝の値はプロトコルが実行されるたびに異なり、それにより、リプレイアタックから保護する。対応して、イニシエータメッセージユニットは、認証応答ＡＲＰ２を分解するように構成される。正常に処理することは、イニシエータプロセッサがレスポンダと同じk_2についての値に達することと、イニシエータが、Ｒ－ａｕｔｈ２自体を計算することによって、及びメッセージＡＲＰ２中で受信された値｛Ｒ－ａｕｔｈ２｝$_{k2}$の鍵k_2を用いた解読によって、｛Ｒ－ａｕｔｈ２｝についての同じ値を見つけることとを意味する。

【００４９】

イニシエータメッセージユニットは、相互認証の確認を示す相互確認ステータスと、レスポンダ公開鍵（B_R）とイニシエータ公開鍵（B_I）に対応するイニシエータプライベート鍵（b_I）とに基づく相互イニシエータ認証データ｛Ｉ－ａｕｔｈ２｝$_{k2}$とを含む相互認証確認ＡＣＦ２を作成するように構成される。第２の中間鍵k_2は、イニシエータにおける｛p_I、b_I、B_R及びP_R｝を使用して決定され得る。｛Ｉ－ａｕｔｈ２｝の値は、同じ入力を使用して｛Ｒ－ａｕｔｈ２｝と同様の様式で計算される。しかしながら、リプレイアタックから守るために、｛Ｉ－ａｕｔｈ２｝の値は｛Ｒ－ａｕｔｈ２｝の値とは異なるべきである。したがって、ハッシュを計算するときの入力の順序は別様に選択されるべきであり、及び／又は、｛Ｒ－ａｕｔｈ２｝についてのハッシュの計算におけるものとは異なる一定値がハッシュに含まれるべきである。対応して、レスポンダメッセージユニットは、相互認証確認ＡＣＦ２を分解するように構成される。レスポンダが、同じ中間鍵k_2に達し、Ｉ－ａｕｔｈ２自体を計算することによって、及び鍵k_2を用いた受信された｛Ｉ－ａｕｔｈ２｝$_{k2}$の解読によって、データＩ－ａｕｔｈ２についての同じ値を取得した場合、レスポンダはB_Iを認証し、相互イニシエータ認証データ｛Ｉ－ａｕｔｈ２｝$_{k2}$の処理は成功した。

【００５０】

図３は、イニシエータステートマシンの一例を示す。イニシエータステートマシン３００は、ユーザ対話とレスポンダデバイスから受信されたメッセージとに応じて認証プロトコルに従ってイニシエータ状態を与える。イニシエータ状態は、

－　イニシエータ帯域外アクションを介してレスポンダデバイスからレスポンダ公開鍵を取得することによるブートストラッピングのための初期状態ＩＳＴと、

－　ブートストラッピングがレスポンダ公開鍵を取得することによって正常に実行されたことを示すブートストラップ済み状態ＢＳＴと、

－　認証を実行するための認証中状態ＡＧ１と、
－　相互認証を実行するための相互認証中状態ＡＧ２と、
－　認証が正常に実行されたことを示す認証済み状態ＡＴＤと
を含む。
【００５１】
最初に、ステートマシンは、開始状態ＩＳＴにおいて開始する。矢印は、状態遷移を示し、状態遷移に対応するメッセージ又はイベントを示す頭字語によってマークされる。イニシエータステートマシンは、レスポンダ公開鍵を取得することによってブートストラッピングＢＴＧを正常に実行すると、ブートストラップ済み状態ＢＳＴにつくように構成される。
【００５２】
イニシエータステートマシンは、ＡＲＱを送ると、及び／或いはユーザ又は別のイベントによるトリガイベントＴＲを介して、或いは成功したブートストラッピングの直後に、認証中状態ＡＧ１にその後関与するように構成される。タイムアウトＴＯの後に、認証中状態ＡＧ１は、試行回数を計数しながら、ＡＲＱを再送信した後に再関与され、所定の数の試行を超えた後に、ブートストラップ済み状態ＢＳＴに、又は初期状態ＩＳＴにフォールバックする。状態ＢＳＴ及びＡＧ１はまた、組み合わせられる。
【００５３】
イニシエータステートマシンは、待機中相互認証のために、ＡＲＰ１中で相互進行ステータスを受信すると、相互認証中状態ＡＧ２につくように構成される。随意に、相互待機中ステータスを含んでいる待機中認証確認ＡＣＦ１が送られる。
【００５４】
イニシエータステートマシンは、相互認証応答ＡＲＰ２を受信し、イニシエータプロセッサがレスポンダ公開鍵とイニシエータ公開鍵（B_I）に対応するイニシエータプライベート鍵（b_I）とに基づく相互レスポンダ認証データ｛Ｒ－ａｕｔｈ２｝$_{k2}$を正常に処理すると、認証済み状態ＡＴＤにつくように構成される。次いで、相互確認ステータスを含む相互認証確認ＡＣＦ２も送られる。
【００５５】
随意に、イニシエータステートマシンは、認証中状態ＡＧ１で相互認証応答ＡＲＰ２を受信し、イニシエータプロセッサが相互レスポンダ認証データ｛Ｒ－ａｕｔｈ２｝$_{k2}$を正常に処理すると、認証済み状態につくように構成される。次いで、相互確認ステータスを含む相互認証確認ＡＣＦ２も送られる。非常に効果的に、相互認証中状態はスキップされる。
【００５６】
随意に、イニシエータメッセージユニットは、片側認証の場合、レスポンダ公開鍵B_Rに対応するレスポンダプライベート鍵b_Rに基づく片側レスポンダ認証データ｛Ｒ－ａｕｔｈ１｝$_{k1}$と、片側認証を示す片側ステータスとを含む片側認証応答（ＡＲＰ１）を分解するように構成される。また、イニシエータステートマシンは、イニシエータプロセッサがレスポンダ公開鍵とイニシエータ公開鍵B_Iに対応するイニシエータプライベート鍵b_Iとに基づく片側レスポンダ認証データ｛Ｒ－ａｕｔｈ１｝$_{k1}$を正常に処理すると、認証済み状態につくように構成される。正常に処理することは、イニシエータプロセッサがレスポンダと同じk_1についての値に達することと、イニシエータが、Ｒ－ａｕｔｈ１自体を計算することによって、及びメッセージＡＲＰ１中で受信された値｛Ｒ－ａｕｔｈ１｝$_{k1}$の鍵k_1を用いた解読によって、｛Ｒ－ａｕｔｈ１｝についての同じ値を見つけることとを意味する。
【００５７】
随意に、イニシエータステートマシンは、認証応答ＡＲＰ１を受信し、イニシエータプロセッサが片側レスポンダ認証データ｛Ｒ－ａｕｔｈ１｝$_{k1}$を正常に処理しないと、ブートストラップ済み状態又は初期状態につくように構成される。正常に処理しないことは、いわゆる不正な認証ＢＡによるか、又は、ピアデバイスが見つけられないときＮＰである

。そのような場合、イニシエータステートマシンは、ブートストラップ済み状態ＢＳＴに、又は初期状態ＩＳＴにフォールバックするように構成され、それは、検出されたイベントにさらに依存する。

【００５８】

随意に、イニシエータステートマシンは、相互認証応答ＡＲＰ２を受信し、イニシエータプロセッサが相互レスポンダ認証データ｛Ｒ－ａｕｔｈ２｝$_{K2}$を正常に処理しないと、ブートストラップ済み状態又は初期状態につくように構成される。正常に処理しないことは、いわゆる不正な認証ＢＡによるか、又は、ピアデバイスが見つけられないときＮＰである。そのような場合、イニシエータステートマシンは、ブートストラップ済み状態ＢＳＴに、又は初期状態ＩＳＴ（図示せず）にフォールバックするように構成され、それは、検出されたイベントにさらに依存する。

【００５９】

図４は、レスポンダステートマシンの一例を示す。レスポンダステートマシン４００は、ユーザ対話とレスポンダデバイスから受信されたメッセージとに応じて認証プロトコルに従ってレスポンダ状態を与える。レスポンダ状態は、

－　イニシエータデバイスからメッセージを受信するための待機中状態（ＡＷＧ）と、

－　認証を実行するためのレスポンダ認証中状態（ＡＲ１）と、

－　レスポンダデバイスがレスポンダ帯域外アクションを介してイニシエータデバイスからイニシエータ公開鍵を取得することを可能にするための相互レスポンダ認証中状態（ＡＲ２）と、

－　認証が正常に実行されたことを示すレスポンダ認証済み状態（ＡＲＤ）と

を含む。

【００６０】

最初に、レスポンダステートマシンは、待機中状態ＡＷＧにおいて開始する。待機中状態ＡＷＧは、ユーザ対話、又は、レスポンダデバイスをオンに切り替えることなど、任意の他のイベント時に、関与される。矢印は、状態遷移を示し、状態遷移に対応するメッセージ又はイベントを示す頭字語によってマークされる。

【００６１】

レスポンダステートマシンは、認証要求ＡＲＱを受信し、正常に処理すると、レスポンダ認証中状態ＡＲ１につくように構成される。状態ＡＷＧ及びＡＲ１はまた、単一の状態に組み合わせられる。

【００６２】

ＡＲＱを正常に処理しないことは、レスポンダが、受信されたＡＲＱ中のレスポンダベリファイアＨ（B_R）がその公開鍵B_Rのハッシュでないこと、又は、受信されたＡＲＱ中の｛Ｉ－ｎｏｎｃｅ｜Ｉ－ｃａｐａｂｉｌｉｔｉｅｓ｝$_{K1}$を解読することがエラーにつながることを決定したことを意味する。間違った鍵が解読のために使用されていること、又は、暗号化されたデータが暗号化の後に変更されたことを解読中に検出することが可能である暗号化／解読アルゴリズムの一例は、ＡＥＳ－ＳＩＶ、［３］参照、である。ＡＲＱを正常に処理すると、相互認証が進行中であることを示す相互進行ステータスを含んでいる認証応答ＡＲＰ１がイニシエータに送信される。

【００６３】

レスポンダステートマシンは、レスポンダデバイスがレスポンダ帯域外アクションを介してイニシエータデバイスからイニシエータ公開鍵を取得すると、相互レスポンダ認証中状態ＡＲ２を与え、それにつく。取得すると、相互認証応答ＡＲＰ２もイニシエータに送られる。

【００６４】

随意に、レスポンダステートマシンは、相互待機中ステータスを含む待機中相互認証確認ＡＣＦ１を受信し、処理するように構成される。

【００６５】

レスポンダステートマシンは、次いで、相互待機中ステータスを受信すると、及びレスポ

ンダＯＯＢアクション時にのみ、相互レスポンダ認証中状態ＡＲ２につくように構成される。ＡＣＦ１が所定のタイムアウトＴＯ内に受信されなかった場合、状態は、レスポンダ認証中状態ＡＲ１のままであり、ＡＲＰ１は、所定の数の再試行まで再び送信される。

【００６６】

レスポンダステートマシンは、相互認証確認ＡＣＦ２を受信すると、及びレスポンダプロセッサがイニシエータ公開鍵B_Iとレスポンダプライベート鍵b_Rとに基づく相互イニシエータ認証データ｛Ｉ－ａｕｔｈ２｝$_{k2}$を正常に処理すると、レスポンダ認証済み状態ＡＲＤにつくように構成される。

【００６７】

随意に、レスポンダステートマシンは、レスポンダ認証中状態ＡＲ１で相互認証確認ＡＣＦ２を受信すると、及びレスポンダプロセッサが相互イニシエータ認証データ｛Ｉ－ａｕｔｈ２｝$_{k2}$を正常に処理すると、レスポンダ認証済み状態ＡＲＤにつくように構成される。ＡＣＦ２を受信することは、たとえばレスポンダが以前のセッションからのイニシエータ公開鍵をすでに所有していることに基づいて、レスポンダが直接、ＡＲＱの受信時に、相互認証応答ＡＲＰ２をイニシエータに送ると行われる。

【００６８】

随意に、メッセージユニットが、片側認証の場合、レスポンダ公開鍵B_Rに対応するレスポンダプライベート鍵b_Rに基づく片側レスポンダ認証データ｛Ｒ－ａｕｔｈ１｝$_{k1}$と、片側認証が完了したことを示す片側ステータスとを含む片側認証応答ＡＲＰ１を作成するように構成される。また、レスポンダステートマシンは、片側認証の場合、片側認証確認ＡＣＦ１を受信し、レスポンダプロセッサが片側イニシエータ認証データ｛Ｉ－ａｕｔｈ１｝$_{k1}$を正常に処理すると、レスポンダ認証済み状態につくように構成される。正常に処理することは、レスポンダプロセッサがイニシエータと同じk_1についての値に達することと、レスポンダデバイスが、Ｉ－ａｕｔｈ１自体を計算することによって、及びメッセージＡＣＦ１中で受信された値｛Ｉ－ａｕｔｈ１｝$_{k1}$の鍵k_1を用いた解読によって、Ｉ－ａｕｔｈ１についての同じ値を見つけることとを意味する。

【００６９】

随意に、レスポンダステートマシンは、相互認証確認ＡＣＦ２を受信し、レスポンダプロセッサが相互イニシエータ認証データ｛Ｉ－ａｕｔｈ２｝$_{k2}$を正常に処理せず、不正な認証イベントＢＡが生じると、待機中状態につくように構成される。

【００７０】

随意に、レスポンダメッセージユニットは、片側イニシエータ認証データ｛Ｉ－ａｕｔｈ１｝$_{k1}$を含み、相互待機中ステータスを含む待機中認証確認ＡＣＦ１をさらに分解するように構成される。また、レスポンダステートマシンは、レスポンダプロセッサが片側イニシエータ認証データを正常に処理せず、不正な認証イベントＢＡが生じると、待機中状態につくように構成される。

【００７１】

概して、相互認証は、片方向認証をも指定する認証プロトコルにおいて適応され得る。片方向認証では、レスポンダ（のユーザ）は、それがどのデバイスから認証要求を受信したかを確かめることを望まない。レスポンダは、帯域外でイニシエータの公開鍵B_Iをキャプチャせず、したがって、認証応答メッセージ中でイニシエータにB_Iのハッシュを送ることができず、それを送らない。レスポンダが、イニシエータが帯域外でキャプチャした公開鍵B_Rに対応するプライベート鍵b_Rの所有をイニシエータに証明したとき、片側認証のみが行われる。たとえば、イニシエータへのメッセージを暗号化するための鍵を作るために、Ｄｉｆｆｉｅ－Ｈｅｌｌｍａｎ様式（参考文献［６］参照）でb_Rを使用することによって。そのようなプロトコルは、各当事者のための２つ又はそれ以上の鍵ペアを使用し、たとえば、１つの鍵ペアは、互いに対する信頼をブートストラップするための鍵ペアであり、さらなる鍵ペアは、さらなる動作のために公開鍵がそこから認証される鍵ペアである。

【００７２】

ユーザが、Ｗｉ－Ｆｉ（登録商標）を介した要求及び応答並びにメッセージのさらなる交換を伴って、プロトコルの実行をトリガするアクションを実行するとき、ユーザは、すべてのメッセージの交換を伴うこのアクションが終了するまで長く待っているのを好まない。しかしながら、いくつかの理由で、たとえばメッセージがＲＦ干渉によって破損した場合に、他方の当事者はメッセージの各々を受信することに失敗することがある。したがって、デバイスがＷｉ－Ｆｉ（登録商標）を介して要求を送るとき、デバイスは、応答を待つためのタイマーを設定する。応答がタイムアウト内に到着しなかった場合、デバイスは、再び要求を送ることを試みる。数回の試行の後に応答が受信されなかった場合、デバイスは断念し、これをユーザに報告する。待ち時間がより長く、許容される試行の数がより多いとき、成功の見込みは増加するが、ユーザはまた、プロトコルが成功しなかったという確認を得るまでより長く待たなければならない。

【００７３】

旧来の相互認証に関する問題は、レスポンダデバイスのユーザが最初に公開鍵ＢＩをキャプチャしなければならないので、レスポンダが相互認証のために認証応答メッセージで応答するのに、片方向認証の場合よりも長い時間がかかることである。また、イニシエータデバイスは、レスポンダデバイスが相互認証を行うことを希望するか否かを知らない。したがって、イニシエータデバイスは、これに適応するように、イニシエータデバイスの待ち時間及び試行の数を高く設定しなければならない。これは、Ｗｉ－Ｆｉ（登録商標）問題、たとえば、あまりに多くの雑音、又はイニシエータとレスポンダとの間の不正なＷｉ－Ｆｉ（登録商標）転送の何らかの他の理由がある場合、イニシエータデバイスが、断念し、これをそのユーザに報告するまで非常に長く待たなければならないことを意味する。

【００７４】

提案するシステムは、イニシエータの公開ＯＯＢ鍵ＢＩをキャプチャするために必要とされるユーザ対話があるとき、効果的である。そのようなレスポンダＯＯＢアクションの例は、以下の通りである。

・　ＢＩが機械可読コード（たとえばＱＲコード（登録商標）又はバーコード）として表示され、ユーザがＢＩを読み取るために（カメラ又はレーザースキャナなどの）機械可読コードリーダーを使用しなければならないとき、

・　ＢＩが、人間が読み取れる形式で表示され、ユーザが何らかの入力デバイス（キーボード、キー、キーボードがその上に表示されるタッチディスプレイ、マウス、及びスクリーン上に表示されるキーボードなど）を使用してレスポンダデバイスにコードを入力しなければならないとき、

・　ユーザがレスポンダデバイスのためのＮＦＣリーダーと接触させなければならないＮＦＣタグ（参考文献［５］参照）を使用してＢＩが転送されるとき。ここで、ＢＩをもつＮＦＣタグは、レスポンダデバイスにＢＩを転送すると同時にイニシエータデバイスにＢＲを転送するために使用され得ない。

【００７５】

上記の問題を解決するために、レスポンダが相互認証を行うことを希望する場合、レスポンダは、レスポンダが片方向認証を行うことを希望するかのように、最初に第１の認証応答を作る。レスポンダは、レスポンダが片方向認証を行うことを希望するかのように、すべての暗号化アクション及び他のアクションを実行する。ただし、レスポンダは、その応答中で、レスポンダが後で相互認証を行うことを希望することを指示する。この指示は特殊なステータスであり、たとえば「ステータスＯＫ」の代わりに、レスポンダは、認証応答中でステータス「相互認証進行中」を送る。

【００７６】

そのようなＡＲＰを受信すると、イニシエータデバイスは、Ｗｉ－Ｆｉ（登録商標）問題がないとき、イニシエータデバイスの認証要求に対する迅速な応答を得る。イニシエータデバイスは、レスポンダデバイスに対する信頼を構築するためにレスポンダデバイスについての片方向認証検査を実行する。片方向認証検査を行うこと、たとえば、Ｄｉｆｆｉｅ－Ｈｅｌｌｍａｎ鍵を使用して、返されたステータスに対して完全性検査を実行すること

はまた、攻撃者がステータスコード「相互認証進行中」又は認証応答メッセージの他の部分を変更することを防ぐ。

【００７７】

イニシエータデバイスは、受信された認証応答に対するすべての暗号化検査に関する問題がないとわかった後に、特殊なステータス「待機中相互認証応答」をもつ認証確認メッセージで応答する。

【００７８】

レスポンダデバイス（のユーザ）は、次いで、都合のよいときに公開鍵ＢＩをキャプチャし、終わったとき、イニシエータの公開鍵ＢＩのハッシュとさらなるステータス「ステータスＯＫ」とを含んでいる相互認証応答で応答する。

【００７９】

次に、詳細な認証プロトコルが説明される。プロトコルは、公開鍵が帯域外（ＯＯＢ）で使用されることを可能にし、それらの公開鍵は、完全に表示又は転送されるが、Ｗｉ－Ｆｉ（登録商標）を介してそのようなものとして使用されない。代わりに、Ｗｉ－Ｆｉ（登録商標）を介して、公開ＯＯＢ鍵のハッシュ値が使用され、その結果、これらの公開鍵は、交換されたＷｉ－Ｆｉ（登録商標）メッセージをリッスンしている他のものに知られないままである。これは、ＯＯＢ鍵が静的である場合、有用である。静的なＯＯＢ鍵は、ＱＲコード（登録商標）のためのディスプレイなど、ＯＯＢでデータを出力する手段を有しないデバイスによって使用される。プロトコルが、レスポンダに、帯域内で、したがってＷｉ－Ｆｉ（登録商標）を介して公開鍵を受信するように要求したとき、イニシエータは、Ｗｉ－Ｆｉ（登録商標）を介してさらなる異なる公開鍵ＰＩを送る。

【００８０】

公開鍵の転送のために、代替実施形態が可能である。Ｗｉ－Ｆｉ（登録商標）を介して公開鍵のハッシュを使用する代わりに、公開鍵の限られた数のビットのみを表示する／送ることなど、値を不明瞭にする他のやり方が使用される。また、完全な値の代わりに、公開鍵のハッシュがＯＯＢで表示／転送される。これは、ＯＯＢで表示又は転送することになるビット数を少なくすることができ、したがって、より小さいＱＲコード（登録商標）又はより小さいＮＦＣタグ（参考文献［５］参照）が使用され得ることを利点として有する。そのような場合、公開鍵の完全な値は、帯域内で、すなわちＷｉ－Ｆｉ（登録商標）を介して送られなければならない。この場合、ＰＩとＢＩとは同じである。それらの公開鍵は両方とも、ＯＯＢで使用して、及びＷｉ－Ｆｉ（登録商標）を介して完全に表示／転送される。

【００８１】

今説明された例示的なプロトコルでは、ＯＯＢ公開鍵は、ＱＲコード（登録商標）として表示され、カメラによってキャプチャされるが、ＯＯＢチャネルについての他の実施形態も可能である。上記の例参照。

【００８２】

第１の段階において、イニシエータデバイスのユーザは、イニシエータデバイスと特定のレスポンダデバイスとの間のセキュアな接続をセットアップすることを希望する。ユーザは、イニシエータデバイス上で認証プロトコルを開始する。イニシエータデバイスは、公開鍵ペアＢＩ／ｂＩ及びＰＩ／ｐＩを使用するか、又は、新しい鍵ペアＢＩ／ｂＩ及びＰＩ／ｐＩを生成する。

【００８３】

いくつかの実施形態では、レスポンダデバイスは、レスポンダモードでアクティブに設定される。他の実施形態では、レスポンダデバイスは、第１の時間の間に又は工場出荷時の値へのリセットの後にそれがオンに切り替えられたとき、レスポンダモードで設定される。Ｒをレスポンダモードに設定することは、新しい公開鍵ペアＢＲ／ｂＲを生成することをトリガする。レスポンダデバイスは、プロトコルに参加するためにレスポンダモードでなければならない。レスポンダモードでは、レスポンダデバイスは、Ｄｉｆｆｉｅ－Ｈｅｌｌｍａｎにおいて公開鍵又は公開鍵のうちの１つとして使用するための公開鍵ＢＲを表

示する。B_Rは静的であり、レスポンダデバイスに、又はそのマニュアルにプリントされる。B_Rに対応するプライベート鍵はb_Rである。ペアB_R／b_Rは、Ｄｉｆｆｉｅ－Ｈｅｌｌｍａｎの新しい実行ごとに、又はｘ分の時間間隔ごとに、新たに生成される。B_Rの表示は、人間が読み取れる形式のもの、又は機械可読形式（ＱＲコード（登録商標）、バーコード）のもの、或いはその両方であり得る。ここでは、カメラを用いて読み取ることができるコンピュータ可読コードを仮定する。

【００８４】

第２の段階において、イニシエータデバイスのユーザは、認証プロトコルを開始し、イニシエータデバイスのカメラをレスポンダデバイスの機械可読公開鍵B_Rに向け、イニシエータデバイスにそれをキャプチャさせる。これらのユーザアクションは、もちろん、ある程度の時間を要する。

【００８５】

第３の段階において、イニシエータデバイスは、イニシエータデバイスがＭＡＣアドレスを知っている場合は直接レスポンダデバイスをアドレス指定することによって、又は、Ｗｉ－Ｆｉ（登録商標）を介して認証要求をブロードキャストすることによって、Ｗｉ－Ｆｉ（登録商標）を介して認証要求をレスポンダデバイスに送る。認証要求は、イニシエータデバイスの公開鍵B_Iのハッシュ及びレスポンダデバイスの公開鍵B_Rのハッシュと、レスポンダによってＤｉｆｆｉｅ－Ｈｅｌｌｍａｎ鍵を導出する際に使用されることになるイニシエータの公開鍵P_Iと、他のイニシエータ情報、たとえばイニシエータナンスとを含んでおり、それらは、B_Rとp_Iとを使用してＤｉｆｆｉｅ－Ｈｅｌｌｍａｎを使用して導出される鍵ｋ１を用いて暗号化される。暗号化は、対称暗号を用いて行われ得る。ただし、その暗号化されたペイロードの完全性検査を行うことと、また、そのペイロードの他の暗号化されていない部分の完全性検査を行うこととをも採用する暗号、たとえばＡＥＳ－ＳＩＶ（参考文献［３］参照）が使用されるとき、レスポンダデバイスは、「他のイニシエータ情報」の解読中に、それが正しいＤｉｆｆｉｅ－Ｈｅｌｌｍａｎ鍵を生成したかどうかと、ステータスコードなど、メッセージ中の暗号化されていない値が攻撃者によって変更されなかったかどうかとを検査することができる。ＡＥＳ－ＳＩＶがエラーなしで解読した場合、レスポンダデバイスは、イニシエータデバイスが、P_Iに対応するプライベート鍵を使用したことと、したがって、イニシエータデバイスが、P_Iに対応するプライベート鍵の所有をレスポンダデバイスに証明したこととを確実に知る。

【００８６】

次の段階において、レスポンダは、その公開鍵B_Rのハッシュを用いてＷｉ－Ｆｉ（登録商標）メッセージを参照し、したがって、レスポンダは、Ｗｉ－Ｆｉ（登録商標）メッセージがレスポンダに向けられていることを知る。レスポンダはまた、特に認証プロトコルのこの実行の直前にB_Rが新たに生成されたとき、このメッセージの送信側がB_Rをキャプチャしたことをその表示から知る。しかしながら、レスポンダデバイスは、どのデバイスが送信側であるかの手がかりを有しない。したがって、レスポンダデバイス（のユーザ）は、さらなる認証を希望し、それに加えて、イニシエータデバイスの公開鍵B_Iを帯域外でキャプチャする。レスポンダデバイスのユーザは、相互認証を実行するようにユーザのデバイスをセットアップする。レスポンダは、次に、イニシエータデバイスに迅速なフィードバックを与え、したがって、イニシエータデバイスは、Ｗｉ－Ｆｉ（登録商標）リンクが動作しており、今のところ暗号学的にすべてがＯＫであることを知る。応答メッセージは、相互認証応答がレスポンダデバイスから来るが、この応答がある程度の時間（数秒～数十秒程度）を要することを示す。したがって、レスポンダは、ステータス「相互認証進行中」をもつイニシエータへの認証応答メッセージで直ちに返答し、メッセージ中のさらなるデータが、片方向認証応答の場合のように生成される。後者は、このメッセージの構成において、認証要求からの「他のイニシエータ情報」、たとえばイニシエータナンスが、P_I及びb_Rを使用してレスポンダデバイスによって解読され、認証応答メッセージの構成において使用され、その結果、レスポンダが、正しい「他のイニシエータ情報」、たとえばイニシエータナンスを実際使用し、したがって、レスポンダＯＯＢ公開鍵B_R

に対応するプライベート鍵ｂ$_R$の所有を証明したかどうかをイニシエータが検査することができることを意味する。

【００８７】

認証応答メッセージの構成において他のイニシエータ情報を使用する様々なやり方としては、以下がある。

・　「他のイニシエータ情報」は、平文でメッセージ中に入れられ得る。

・　「他のイニシエータ情報」は、たとえばＡＥＳ－ＳＩＶとともにＡＡＤ（認証済み関連データ（Ａｕｔｈｅｎｔｉｃａｔｅｄ　Ａｓｓｏｃｉａｔｅｄ　Ｄａｔａ）、又は認証済み追加データ（Ａｕｔｈｅｎｔｉｃａｔｅｄ　Ａｄｄｉｔｉｏｎａｌ　Ｄａｔａ））として「他のイニシエータ情報」を使用することによって、Ｄｉｆｆｉｅ－Ｈｅｌｌｍａｎを使用して導出される鍵によって完全性について保護されながら、平文でメッセージ中に入れられ得る。

・　「他のイニシエータ情報」は、たとえば、最初にＤｉｆｆｉｅ－Ｈｅｌｌｍａｎを使用して鍵を導出し、Ｄｉｆｆｉｅ－Ｈｅｌｌｍａｎ鍵と「他のイニシエータ情報」とを鍵導出関数のための入力として使用することによって、さらなる鍵を導出するために使用され得る。そのように導出された鍵がＡＥＳ－ＳＩＶとともに使用される場合、又は、そのように導出された鍵が、イニシエータに知られている何かを暗号化するために使用される場合、イニシエータは、レスポンダが正しい「他のイニシエータ情報」を知っているかどうかを検査することができる。

【００８８】

随意に、ステータスフィールドもＡＥＳ－ＳＩＶのためのＡＡＤとして使用され、したがって、それは、イニシエータデバイスが知ることなしに改ざんされ得ない。

【００８９】

次の段階において、イニシエータは認証応答メッセージを受信する。イニシエータは、すべての暗号化検査を実行し、レスポンダデバイスが「他のイニシエータ情報」を正しく解読したかどうか、したがって、イニシエータデバイスがそのカメラを用いてレスポンダデバイスからキャプチャした公開ＯＯＢ鍵Ｂ$_R$に対応するプライベート鍵ｂ$_R$をレスポンダデバイスが所有するかどうかを知ることができる。これらの検査が失敗した場合、イニシエータデバイスはプロトコルをアボートする。検査がＯＫであることが判明した場合、イニシエータデバイスはステータスフィールドを点検する。イニシエータデバイスは、「相互認証進行中」を参照する。ここで、イニシエータデバイスは、それがレスポンダデバイスからの第２の応答を数秒～数十秒待たなければならないことを知る。

【００９０】

随意に、イニシエータデバイスは、イニシエータが相互認証応答を待っていることを示すステータスをもつ待機中認証確認メッセージを伴う認証応答メッセージの正しい受信を確認する。そのメッセージは、片方向認証のために構成される。

【００９１】

次の段階において、レスポンダデバイスのユーザは、レスポンダデバイスのカメラをイニシエータデバイスによって表示された公開鍵Ｂ$_I$に向ける。イニシエータデバイスからのそのようにキャプチャされた公開鍵のハッシュが、認証要求メッセージ中でＷｉ－Ｆｉ（登録商標）を介して受信されたイニシエータデバイスの公開鍵のハッシュに一致するとき、レスポンダデバイスは、それがイニシエータデバイスとのＤｉｆｆｉｅ－Ｈｅｌｌｍａｎを実行するために正しい公開鍵を使用しようとしていることを確信することができる。レスポンダデバイスは、プロトコルにおいて後で、イニシエータデバイスが、対応するプライベート鍵ｂ$_I$の所有を証明したとき、レスポンダデバイスが、Ｂ$_I$をそこからキャプチャしたデバイスと通信していることを確実に知ることになる。

【００９２】

次の段階において、公開鍵Ｂ$_I$をキャプチャした後に、レスポンダデバイスは、相互認証応答として作成された、相互認証応答メッセージでイニシエータデバイスに応答する。メッセージは、ステータス「相互ＯＫ」、又は単に「ＯＫ」と、Ｂ$_I$のハッシュと、他のレ

スポンダ情報とを含んでおり、これは、認証要求メッセージ中でＷｉ－Ｆｉ（登録商標）を介して受信された公開鍵ＰＩとイニシエータデバイスから帯域外で取得されたＢＩとを使用してＤｉｆｆｉｅ－Ｈｅｌｌｍａｎを使用して導出された鍵を用いて暗号化される。イニシエータデバイスによって送られた「他のイニシエータ情報」は、前に説明されたように、レスポンダデバイスによって、そのプライベート鍵ｂＲと受信された公開鍵ＰＩとを使用して解読され、認証応答メッセージの構成において使用され、したがって、レスポンダデバイスは、ｂＲの所有をイニシエータデバイスに証明することができる。片方向認証応答とのいくつかの差は、レスポンダが、Ｄｉｆｆｉｅ－Ｈｅｌｌｍａｎ鍵を導出するためにＢＩをも使用すること、及び応答中のＢＩのハッシュの存在である。

【００９３】

レスポンダデバイスがイニシエータからの２つの公開鍵ＢＩ及びＰＩを使用することができる異なるやり方がある。たとえば、レスポンダは、それ自体の１つ又は２つのプライベート鍵とともにこれらの２つの公開鍵の各々を使用して、ｋ３及びｋ４とともに、２つのＤｉｆｆｉｅ－Ｈｅｌｌｍａｎ鍵を導出する。

【００９４】

第１の実施形態では、レスポンダは、たとえば、ＰＩ及びそのプライベート鍵ｂＲ又は新しいプライベート鍵ｐＲ或いはｂＲとｐＲとの和を使用してｋ３を導出することができる。レスポンダがｐＲを使用する場合、レスポンダは、対応する公開鍵ＰＲを、イニシエータがそれを取り出すことができるようなやり方で認証応答中に含めなければならない。それは、平文のＰＲ、又は、イニシエータが導出することが可能である鍵、たとえば上記の鍵ｋ１を用いて暗号化されたＰＲを送ることによって行われ得る。

【００９５】

第２の実施形態では、レスポンダは、たとえば、ＢＩ及びそのプライベート鍵ｂＲ又は新しいプライベート鍵ｐＲ或いはｂＲとｐＲとの和を使用してｋ４を導出する。レスポンダがｐＲを使用する場合、レスポンダは、対応する公開鍵ＰＲを、イニシエータがそれを取り出すことができるようなやり方で認証応答中に含めなければならない。それは、平文のＰＲ、又は、イニシエータが導出することが可能である鍵、たとえば上記の鍵ｋ１を用いて暗号化されたＰＲを送ることによって行われ得る。２つのプライベート鍵の和がｋ３又はｋ４のいずれかのために使用される場合、他の鍵の導出は、ｐＲとｂＲとの和ではなく、これらの鍵のうちのただ１つを使用するべきである。このようにして、レスポンダデバイスは、プライベート鍵ｂＲとｐＲとの和だけではなく、プライベート鍵の所有を証明することが可能である。

【００９６】

さらなる実施形態では、レスポンダは、イニシエータが知っている異なる値、たとえばイニシエータナンスを各々暗号化するために鍵ｋ３と鍵ｋ４の両方を使用し、したがって、イニシエータは、レスポンダが使用したプライベート鍵をレスポンダデバイスが知っているかどうかを検査することができる。さらに、レスポンダは、認証確認メッセージを検査することが可能であるために、それ自体の「他のレスポンダ情報」、たとえばレスポンダナンスを暗号化する。

【００９７】

さらなる実施形態では、異なる値を暗号化するために鍵ｋ３及びｋ４を使用する代わりに、それらのうちの一方、すなわち「第１の鍵」が、第１の値を暗号化するために使用され得、他方の鍵、すなわち「第２の鍵」が、別の値と暗号化された第１の値との連結を暗号化するために使用される。第２の鍵は、レスポンダがこの鍵を生成することができるようなものであるべきである。第２の鍵を用いて暗号化された値は、第１の鍵を生成するために必要とされる情報を含んでおり、したがって、信頼を構築するのを助ける。

【００９８】

次の段階において、イニシエータは、今やステータス「ＯＫ」をもつ認証応答メッセージを受信する。イニシエータデバイスは、その中のハッシュをその公開鍵ＢＩのハッシュと比較する。それが一致するとき、イニシエータデバイスはまた、レスポンダデバイスがそ

の公開鍵ＢＩをキャプチャしたことをその表示から知る。イニシエータデバイスはすべての必要とされる鍵を生成し、そのためにイニシエータデバイスは、そのプライベート鍵ｂＩ及びｐＩを必要とし、イニシエータデバイスはすべての暗号化検査を実行する。これらの検査がすべてＯＫである場合、イニシエータデバイスは、それが、プライベート鍵ｂＲと、ｐＲも使用された場合、場合によってはｐＲとを所有するデバイスと通信していたことと、レスポンダデバイスが正しいＢＩを正常に取得したこととを知る。

【００９９】

次の段階において、前の段階における検査がすべてＯＫである場合、イニシエータデバイスは、ステータス「ＯＫ」をもつ確認応答メッセージをレスポンダデバイスに送り、ここで、特に、ｂＩからＤｉｆｆｉｅ－Ｈｅｌｌｍａｎ様式で導出された鍵が使用され、その結果、イニシエータデバイスはｂＩの所有をレスポンダデバイスに証明することができる。イニシエータデバイスは、「他のレスポンダ情報」、たとえばレスポンダナンスをも使用し、その結果、レスポンダは、イニシエータがこれらを解読することに成功したことがわかる。

【０１００】

上記のシステムは、ポータブルデバイス、ラップトップ、ＰＣ、Ｗｉ－Ｆｉ（登録商標）アクセスポイント、Ｗｉ－Ｆｉ（登録商標）ピアツーピアデバイス、Ｂｌｕｅｔｏｏｔｈ（登録商標）デバイス、Ｚｉｇｂｅｅ（登録商標）デバイスにおいて実装される。Ｗｉ－Ｆｉ（登録商標）が使用される場合、本発明は、一般に、ｗｐａ＿ｓｕｐｐｌｉｃａｎｔソフトウェア、たとえばｈｔｔｐｓ：／／ｅｎ．ｗｉｋｉｐｅｄｉａ．ｏｒｇ／ｗｉｋｉ／ｗｐａ＿ｓｕｐｐｌｉｃａｎｔ参照、において実装される。

【０１０１】

一実施形態では、第１のデバイスと第２のデバイスとの間の認証プロトコルは、追加の属性又は追加のメッセージを含み、追加の属性又は追加のメッセージは、たとえば、証明（たとえば公開鍵）、証明のハッシュ又は暗号化された証明を含んでいる、ＩＥＥＥ８０２．１１（参考文献［１］参照）において定義されている認証プロトコルに追加される。第２のデバイスは、認証プロトコルのためのメッセージ交換の一部として、そのような証明、証明のハッシュ又は暗号化された証明を含まなければならない。対称であるために、第１のデバイスも、そのような証明、証明のハッシュ又は暗号化された証明を含まなければならない。認証プロトコルのメッセージ中に、証明、証明のハッシュ又は暗号化された証明を含んでいる好ましいフィールドは、そのメッセージの送信又は到着時間を測定するために、そのフィールドを転送する信号又は信号の少なくとも一部が使用されるフィールドであり、その結果、別のデバイスが、その証明、その証明のハッシュ、又はその暗号化された証明をメッセージ中に挿入することは、不可能ではないにしても極めて困難である。

【０１０２】

一実施形態では、第１のメッセージプロセッサは、この証明、証明のハッシュ又は暗号化された証明を処理するように構成され、その証明が、第１のメッセージプロセッサが、Ｗｉ－Ｆｉ（登録商標）プロテクテッドセットアッププロトコル（Ｗｉ－Ｆｉ（登録商標）Ｐｒｏｔｅｃｔｅｄ Ｓｅｔｕｐ Ｐｒｏｔｏｃｏｌ）、デバイスプロビジョニングプロトコル（Ｄｅｖｉｃｅ Ｐｒｏｖｉｓｉｏｎｉｎｇ Ｐｒｏｔｏｃｏｌ）、Ｄｉｆｆｉｅ－Ｈｅｌｌｍａｎ鍵交換及び／又は４ウェイＷＰＡ２ハンドシェイク（４－ｗａｙ ＷＰＡ２ ｈａｎｄｓｈａｋｅ）を使用することなどによって、正常にデバイス認証を実行し、相互信頼を確立した、デバイスによって前に使用された証明に一致するかどうかを検証する（参考文献［１］参照）。一致が見つかった場合、第１のデバイスは、第２のデバイスを信頼し、信頼性が高いと見なすことができると仮定する。一致が見つからなかった場合、第１のデバイスは、第２のデバイスを信頼せず、信頼性を検証するために追加のステップを実行する。

【０１０３】

代替実施形態では、第２のデバイスは、後の接続セットアップ中に使用される証明、証明のハッシュ又は暗号化された証明を含まなければならない。第１のメッセージプロセッサ

は、受信された証明、証明のハッシュ又は暗号化された証明を、その証明と接続する特定のデバイスとセキュアに相関するために、第２のデバイスの他のパラメータとともに処理し、記憶するように構成される。第１のデバイスと第２のデバイスとの間の接続をセットアップすると、第１のデバイスは、Ｗｉ－Ｆｉ（登録商標）プロテクテッドセットアッププロトコル、デバイスプロビジョニングプロトコル、Ｄｉｆｆｉｅ－Ｈｅｌｌｍａｎ鍵交換を実行する間に及び／又は４ウェイＷＰＡ２ハンドシェイクを実行する間になど、デバイス認証を実行する間に、同じ証明又はそれの派生物が使用されるかどうかを検証する。そうすることによって、第１のデバイスは、それが接続しているデバイスが、以前の認証が行われたデバイスと同じデバイスであると決定することができる。特に、証明が公開鍵であった場合、及び第１のデバイスと第２のデバイスとの間の接続をセットアップすることが、第２のデバイスがその公開鍵に属するプライベート鍵の所有を証明として有することを第２のデバイスが第１のデバイスに正常に証明したことを含んでいた場合、第１のデバイスは、第２のデバイスが、そうであると主張するデバイスであり、偽造者（ｉｍｐｏｓｔｅｒ）でないことを確信することができる。

【０１０４】

図５は、イニシエータのための方法を示す。本方法は、通信プロトコルと、認証を適応させるための認証プロトコルとに従うレスポンダデバイスとのワイヤレス通信のためにイニシエータデバイスにおいて使用するための方法である。プロトコルは、ユーザ対話とレスポンダデバイスから受信されたメッセージとに応じて認証プロトコルに従うイニシエータ状態を必要とする。

【０１０５】

本方法は、ノードＳＴＡＲＴ５０１において開始する。第１の段階において、本方法は、ブートストラッピングのための初期状態を設定する。

【０１０６】

次のステップＡＣＲＰＫ５０２において、本方法は、イニシエータ帯域外アクションを介してレスポンダデバイスからレスポンダ公開鍵B_Rを取得することにつく。B_Rを正常に取得すると、本方法は、ステップＳＡＲＱ５０３において、ブートストラッピングがレスポンダ公開鍵を取得することによって正常に実行されたことを示すブートストラップ済み状態につく。次いで、本方法は、イニシエータ公開鍵を検証するためのイニシエータベリファイア（Ｈ（B_I））とレスポンダ公開鍵を検証するためのレスポンダベリファイア（Ｈ（B_R））とを含む認証要求ＡＲＱを作成することによって続く。メッセージＡＲＱは、ブートストラップ済み状態で送られる。次いで、本方法は、認証応答を受信することを待機する。所定の時間内に受信されなかった場合、本方法は、矢印５１３によって示されるように、ＡＲＱを再び送る。

【０１０７】

次の段階ＲＡＲＰ１　５０４において、認証を実行するための認証中状態につく。その後、本方法は、レスポンダ公開鍵B_Rに対応するレスポンダプライベート鍵b_Rに基づく片側レスポンダ認証データ｛Ｒ－ａｕｔｈ１｝$_{k1}$を含む認証応答ＡＲＰ１を受信し、分解する。ＡＲＰ１は、レスポンダデバイスがレスポンダ帯域外アクションを介してイニシエータデバイスからイニシエータ公開鍵を取得することを可能にするための、相互認証が進行中であることを示す相互進行ステータスを含む。

【０１０８】

次の段階ＡＷＭＵＴ５０５において、待機中相互認証のために、相互進行ステータスを受信すると、相互認証中状態につく。次に、相互認証応答ＡＲＰ２を受信し、分解する。ＡＲＰ２は、イニシエータ公開鍵B_Iとレスポンダプライベート鍵b_Rとに基づく相互レスポンダ認証データ｛Ｒ－ａｕｔｈ２｝$_{k2}$を含む。

【０１０９】

次の段階ＭＵＴＣ５０６において、認証が正常に実行されたことを示す認証済み状態につく。これは、相互認証応答ＡＲＰ２を受信することと、レスポンダ公開鍵とイニシエータ公開鍵（B_I）に対応するイニシエータプライベート鍵（b_I）とに基づく相互レスポン

ダ認証データ｛Ｒ－ａｕｔｈ２｝ｋ２を正常に処理することとを伴う。次いで、本方法は、相互認証の確認を示す相互確認ステータスを含む相互認証確認ＡＣＦ２を作成することによって続く。ＡＣＦ２は、レスポンダ公開鍵ＢＲとイニシエータ公開鍵ＢＩに対応するイニシエータプライベート鍵ｂＩとに基づく相互イニシエータ認証データ｛Ｉ－ａｕｔｈ２｝ｋ２をも含む。本方法は、次いで、ノードＥＮＤ５０７において終了する。

【０１１０】

図６は、レスポンダのための方法を示す。本方法は、通信プロトコルと、認証を適応させるための認証プロトコルとに従うイニシエータデバイスとのワイヤレス通信のためにレスポンダデバイスにおいて使用するための方法である。プロトコルは、ユーザ対話とイニシエータデバイスから受信されたメッセージとに応じて認証プロトコルに従うレスポンダ状態を必要とする。

【０１１１】

本方法は、ノードＳＴＡＲＴ６０１において開始する。第１の段階ＲＡＲＱ６０２において、レスポンダは、イニシエータからメッセージを受信するための待機中状態につく。認証要求ＡＲＱを受信し、分解する。ＡＲＱは、イニシエータ公開鍵を検証するためのイニシエータベリファイアＨ（ＢＩ）とレスポンダ公開鍵を検証するためのレスポンダベリファイアＨ（ＢＲ）とを含む。

【０１１２】

次の段階ＳＡＲＰ１　６０３において、本方法は、認証を実行するためのレスポンダ認証中状態につく。認証要求を正常に処理すると、レスポンダ認証中状態につく。次いで、レスポンダ公開鍵ＢＲに対応するレスポンダプライベート鍵ｂＲに基づく片側レスポンダ認証データ｛Ｒ－ａｕｔｈ１｝ｋ１と、相互認証が進行中であることを示す相互進行ステータスとを含む認証応答ＡＲＰ１を作成する。

【０１１３】

次の段階ＭＵＴＡ６０４において、相互レスポンダ認証中状態につく。次に、レスポンダ（のユーザ）は、レスポンダ帯域外アクションを介してイニシエータデバイスからイニシエータ公開鍵を取得することを可能にされる。これは、その状態に再び入る矢印６１４によって示されているように、ある程度の時間を要する。イニシエータ公開鍵を正常に取得した後に、相互認証応答ＡＲＰ２を作成し、相互レスポンダ認証中状態で送る。ＡＲＰ２は、イニシエータ公開鍵ＢＩとレスポンダ公開鍵ＢＲに対応するレスポンダプライベート鍵ｂＲとに基づく相互レスポンダ認証データ｛Ｒ－ａｕｔｈ２｝ｋ２を含む。

【０１１４】

次の段階ＷＭＵＣ６０５において、認証が正常に実行されたことを示すレスポンダ認証済み状態につく。相互認証確認ＡＣＦ２を受信し、分解する。ＡＣＦ２は、相互認証の確認を示す相互確認ステータスと、レスポンダ公開鍵ＢＲとイニシエータ公開鍵（ＢＩ）に対応するイニシエータプライベート鍵ｂＩとに基づく相互イニシエータ認証データ｛Ｉ－ａｕｔｈ２｝ｋ２とを含む。イニシエータ公開鍵（ＢＩ）とレスポンダプライベート鍵（ｂＲ）とに基づく相互イニシエータ認証データを正常に処理すると、認証済み状態につく。本方法は、次に、ノードＥＮＤ６０６において終了する。

【０１１５】

以下でさらに解明されるように、ロケーション情報を保護するためにコンピュータ上で実行されたときに上記の方法を実施するためのプログラムコード命令を含む、ネットワークからダウンロード可能な、並びに／或いはコンピュータ可読媒体及び／又はマイクロプロセッサ実行可能媒体に記憶されたコンピュータプログラム製品が提供される。

【０１１６】

上記のシステムは、たとえば、屋内及び屋外短距離ワイヤレス通信システムにおいて適用され、ここで、認証プロトコルを介して認証がサポートされる。たとえば、システムは、Ｗｉ－Ｆｉ（登録商標）、Ｗｉ－Ｆｉ（登録商標）　Ａｗａｒｅ、又はＷｉ－Ｆｉ（登録商標）　Ｄｉｒｅｃｔをサポートするポータブルデバイス及び固定デバイスにおいて適用され得る。

【０１１７】
一般に、対話するイニシエータデバイス及びレスポンダデバイスは、各々、デバイスにおいて記憶された適切なソフトウェアを実行するプロセッサを備え、たとえば、そのソフトウェアは、ダウンロードされ、及び／又は対応するメモリ、たとえば、ＲＡＭなどの揮発性メモリ又はフラッシュなどの不揮発性メモリ（図示せず）に記憶される。デバイス及びサーバは、たとえば、マイクロプロセッサ及びメモリ（図示せず）を装備する。代替的に、デバイス及びサーバは、全体的に又は部分的に、プログラマブル論理で、たとえば、フィールドプログラマブルゲートアレイ（ＦＰＧＡ）として実装される。デバイス及びサーバは、全体的に又は部分的に、いわゆる特定用途向け集積回路（ＡＳＩＣ）、すなわち、それらの特定の用途のためにカスタマイズされた集積回路（ＩＣ）として実装される。たとえば、回路は、たとえば、Ｖｅｒｉｌｏｇ、ＶＨＤＬなど、ハードウェア記述言語を使用して、ＣＭＯＳにおいて実装される。
【０１１８】
当業者に明らかであるように、方法を実行する多くの異なるやり方が可能である。たとえば、段階又はステップの順序が変動され得るか、又はいくつかの段階が並列に実行される。その上、ステップの中間に、他の方法ステップが挿入される。挿入されたステップは、本明細書で説明されるような方法の改良を表すか、又はそのような方法に関係しない。
【０１１９】
本発明による方法は、ソフトウェアを使用して実行され、ソフトウェアは、プロセッサシステムに、それぞれの方法を実行させるための命令を含む。ソフトウェアは、システムの特定のサブエンティティによってとられるステップのみを含む。ソフトウェアは、ハードディスク、フロッピー、メモリなど、好適な記憶媒体に記憶される。ソフトウェアは、ワイヤに沿って、又はワイヤレス、或いはデータネットワーク、たとえば、インターネットを使用して、信号として送られる。ソフトウェアは、ダウンロードのために及び／又はサーバ上でのリモート使用のために利用可能にされる。本発明による方法は、方法を実行するためにプログラマブル論理、たとえば、フィールドプログラマブルゲートアレイ（ＦＰＧＡ）を設定するように構成された、ビットストリームを使用して実行される。ソフトウェアは、ソースコード、オブジェクトコード、コード中間ソース及び部分的にコンパイルされた形態などのオブジェクトコードの形態、又は本発明による方法の実装形態において使用するのに好適な任意の他の形態であることが諒解されよう。コンピュータプログラム製品に関係する実施形態は、記載された方法のうちの少なくとも１つの処理ステップの各々に対応するコンピュータ実行可能命令を含む。これらの命令は、サブルーチンに再分割され、及び／或いは静的に又は動的にリンクされる１つ又は複数のファイルに記憶される。コンピュータプログラム製品に関係する別の実施形態は、記載されたシステム及び／又は製品のうちの少なくとも１つの手段の各々に対応するコンピュータ実行可能命令を含む。
【０１２０】
図７ａは、コンピュータプログラム１０２０を備える書込み可能部分１０１０を備えるコンピュータ可読媒体１０００を示し、コンピュータプログラム１０２０は、プロセッサシステムに、上記で説明されたシステムにおいて上記の方法のうちの１つ又は複数を実行させるための命令を含む。コンピュータプログラム１０２０は、物理的マークとして又はコンピュータ可読媒体１０００の要素の磁化によって、非一時的コンピュータ可読媒体１０００上で具現される。しかしながら、他の好適な実施形態が、同様に考えられる。さらに、コンピュータ可読媒体１０００は、ここでは光ディスクとして示されているが、コンピュータ可読媒体１０００は、ハードディスク、ソリッドステートメモリ、フラッシュメモリなど、任意の好適なコンピュータ可読媒体であり、記録不可能又は記録可能であることが諒解されよう。コンピュータプログラム１０２０は、プロセッサシステムに方法を実行させるための命令を含む。
【０１２１】
図７ｂは、上記で説明されたデバイス又はサーバの一実施形態による、プロセッサシステム１１００の概略表現を示す。プロセッサシステムは、回路１１１０、たとえば１つ又は

複数の集積回路を備える。回路１１１０のアーキテクチャは、図に概略的に示されている。回路１１１０は、一実施形態による方法を実行し、及び／或いはそのモジュール又はユニットを実装するために、コンピュータプログラム構成要素を実行するための処理ユニット１１２０、たとえば、ＣＰＵを備える。回路１１１０は、プログラミングコード、データなどを記憶するためのメモリ１１２２を備える。メモリ１１２２の一部は、読取り専用である。回路１１１０は、通信要素１１２６、たとえば、アンテナ、コネクタ、又はその両方などを備える。回路１１１０は、方法において定義された処理の一部又は全部を実行するための専用集積回路１１２４を備える。プロセッサ１１２０、メモリ１１２２、専用ＩＣ１１２４及び通信要素１１２６は、相互接続１１３０、たとえばバスを介して、互いに接続される。プロセッサシステム１１００は、それぞれ、アンテナ及び／又はコネクタを使用して、接触及び／又は非接触通信のために構成される。

【０１２２】

要約すれば、ワイヤレス通信システムが、ワイヤレス通信のために構成されたイニシエータデバイス及びレスポンダデバイスを備える。ワイヤレス通信システムは、イニシエータデバイスによるレスポンダデバイスの片側認証と、両方のデバイスの相互認証とを可能にする。イニシエータの実施形態は、メッセージユニットとステートマシンとを備える。イニシエータは、帯域外アクションを介してレスポンダ公開鍵を取得することによって開始し、認証要求を送る。レスポンダは、レスポンダプライベート鍵に基づくレスポンダ認証データと、レスポンダデバイスがレスポンダ帯域外アクションを介してイニシエータ公開鍵を取得することを可能にするための相互認証が進行中であることを示す相互進行ステータスとを含む認証応答を送る。イニシエータステートマシンは、待機中相互認証のために、相互進行ステータスを受信するとつくことになる、相互認証中状態を与えるように構成される。それにより、ワイヤレス通信中の長いタイムアウト期間が回避され、また、イニシエータが短い時間内にユーザに通信エラーを報告することを可能にする。

【０１２３】

明快のために、上記の説明では、異なる機能ユニット及びプロセッサに関して本発明の実施形態について説明したことが諒解されよう。しかしながら、本発明から逸脱することなく、異なる機能ユニット又はプロセッサ間の機能の任意の好適な分散が使用されることは明らかであろう。たとえば、別個のユニット、プロセッサ又はコントローラによって実行されるものとして示された機能は、同じプロセッサ又はコントローラによって実行される。したがって、特定の機能ユニットへの言及は、厳密な論理的又は物理的構造或いは編成を示すのではなく、説明された機能を提供するための好適な手段への言及としてのみ参照されるべきである。本発明は、ハードウェア、ソフトウェア、ファームウェア又はこれらの任意の組合せを含む任意の好適な形態で実装され得る。

【０１２４】

本明細書では、「含む／備える／有する（ｃｏｍｐｒｉｓｉｎｇ）」という単語は、記載されたもの以外の要素又はステップの存在を除外せず、要素に先行する「１つの（ａ）」又は「１つの（ａｎ）」という単語は、複数のそのような要素の存在を除外しないこと、いかなる参照符号も特許請求の範囲の範囲を限定しないこと、本発明は、ハードウェアとソフトウェアの両方によって実装されること、及びいくつかの「手段」又は「ユニット」は、ハードウェア又はソフトウェアの同じアイテムによって表され、プロセッサは、場合によってはハードウェア要素と協働して、１つ又は複数のユニットの機能を満たすことに留意されたい。さらに、本発明は実施形態に限定されず、本発明は、上記で説明された、又は相互に異なる従属請求項に記載の、あらゆる新規の特徴又は特徴の組合せにある。

参考文献:

[1] IEEE Computer Society, “IEEE Standard for Information Technology-Telecommunications and Information Exchange Between Systems-Local and Metropolitan Area Networks-Specific requirements Part 11:Wireless LAN Medium Access Control(MAC)and Physical Layer(PHY)Specifications,” (IEEE Std.802.11-2016),December 2016

[2] Wi-Fi Simple Configuration-Technical Specification-Version 2.0.5“Specification for easy,secure setup and introduction of devices into WPA2-enabled 802.11 networks”,Wi-Fi Alliance,2014.
[3] RFC 5297,Synthetic Initialization Vector(SIV)Authenticated Encryption Using the Advanced Encryption Standard(AES),October 2008,(https://datatracker.ietf.org/doc/rfc5297/)
[4] FIPS180-4,"Secure Hash Standard",United States of America,National Institute of Standards and Technology,Federal Information Processing Standard (FIPS)180-4
[5] NFC Forum Connection Handover Candidate Technical Specification,December 2015,(http://nfc-forum.org/product/nfc-forum-connection-handover-candidate-technical-specification-version-1-4/)
[6] Diffie,W.;Hellman,M.(1976),"New directions in cryptography",IEEE Transactions on Information Theory,22(6):644-654
[7] Rivest,R.;Shamir,A.;Adleman,L.(February 1978)."A Method for Obtaining Digital Signatures and Public-Key Cryptosystems",Communications of the ACM.21(2):120-126.
[8] Koblitz,N.(1987)."Elliptic curve cryptosystems".Mathematics of Computation.48(177):203-209.

【図面】

【図１】

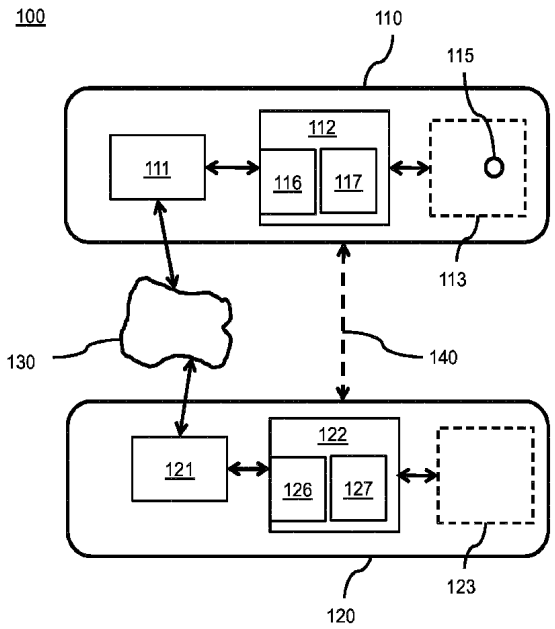

Fig. 1

【図２】

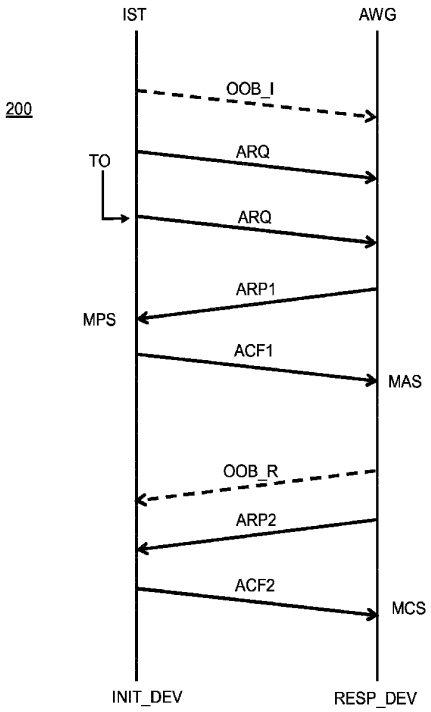

Fig. 2

【図３】

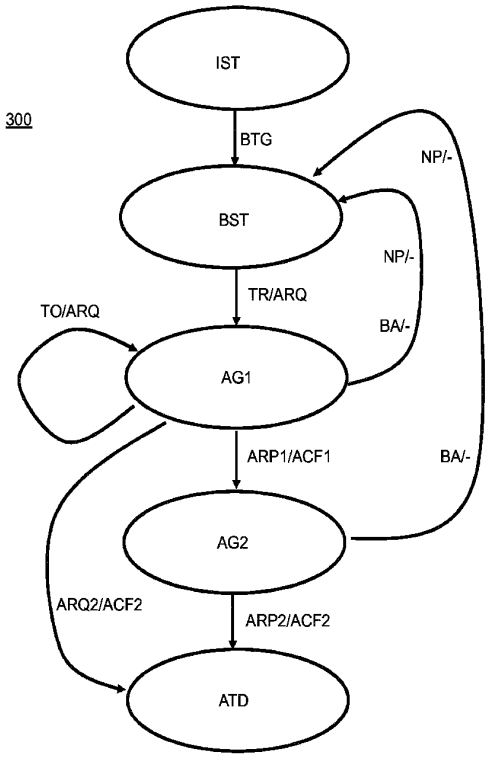

Fig. 3

【図４】

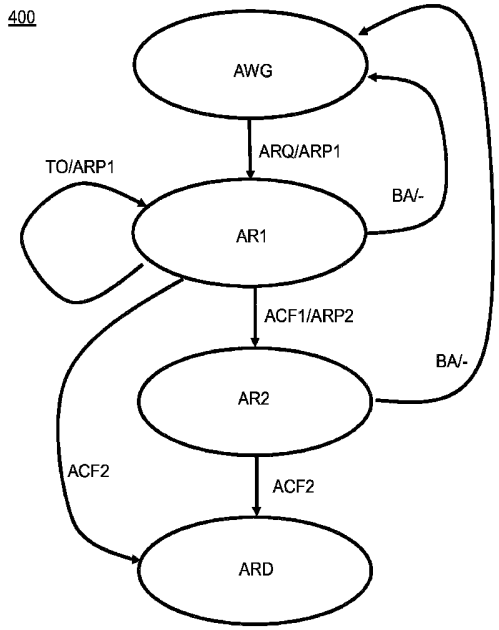

Fig. 4

【図５】

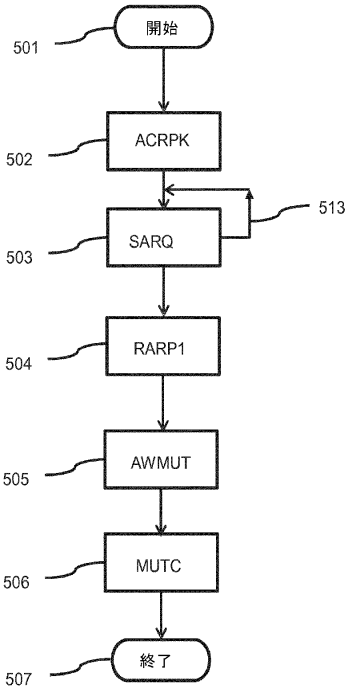

図５

【図６】

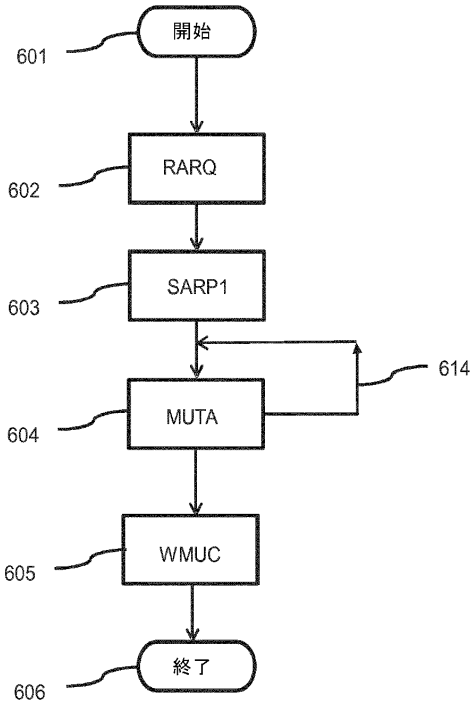

図６

【図７ａ】

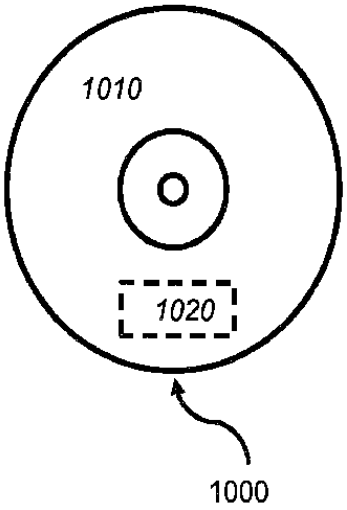

Fig. 7a

【図７ｂ】

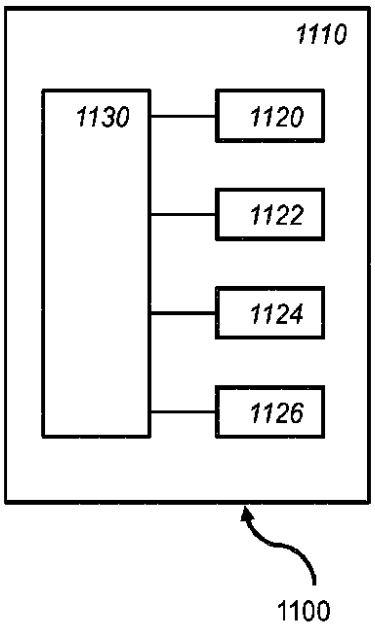

Fig. 7b

フロントページの続き

オランダ国 ５６５６ アーエー アインドーフェン ハイ テック キャンパス ５
(72)発明者 リンデルス ロナルド フェリックス アルベルトゥス
オランダ国 ５６５６ アーエー アインドーフェン ハイ テック キャンパス ５

審査官 青木 重徳

(56)参考文献 特開２００５－２０２３６４（ＪＰ，Ａ）
米国特許出願公開第２０１６／０２４２０３０（ＵＳ，Ａ１）
米国特許出願公開第２０１０／００４２８３８（ＵＳ，Ａ１）
米国特許出願公開第２０１７／００７０８８１（ＵＳ，Ａ１）

(58)調査した分野 (Int.Cl.，ＤＢ名)
Ｈ０４Ｌ ９／３２
Ｈ０４Ｌ ９／０８
Ｈ０４Ｗ １２／０４