(19)日本国特許庁(JP)　(12)公表特許公報(A)　(11)特許出願公表番号
特表2010-506542
(P2010-506542A)
(43)公表日　平成22年2月25日(2010.2.25)

(51)Int.Cl.		F I			テーマコード（参考）
H04L 9/32	(2006.01)	H04L	9/00	675B	5B285
H04L 9/08	(2006.01)	H04L	9/00	601C	5J104
G06F 21/20	(2006.01)	G06F	15/00	330G	

審査請求 有　予備審査請求 未請求　（全 18 頁）

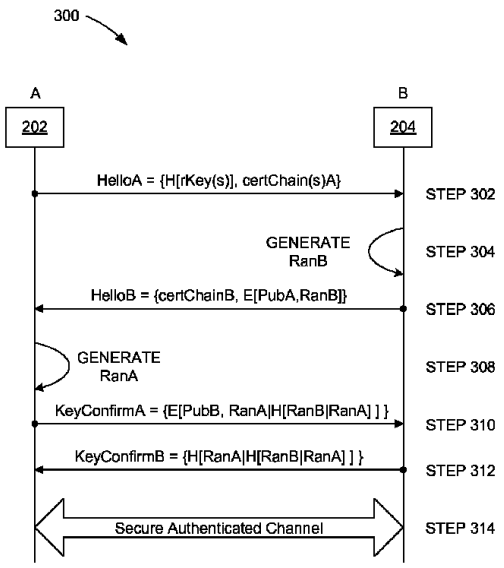
(21)出願番号　特願2009-532508 (P2009-532508)
(86)(22)出願日　平成19年10月5日 (2007.10.5)
(85)翻訳文提出日　平成21年6月10日 (2009.6.10)
(86)国際出願番号　PCT/US2007/080525
(87)国際公開番号　WO2008/045773
(87)国際公開日　平成20年4月17日 (2008.4.17)
(31)優先権主張番号　60/850,882
(32)優先日　平成18年10月10日 (2006.10.10)
(33)優先権主張国　米国 (US)
(31)優先権主張番号　11/866,946
(32)優先日　平成19年10月3日 (2007.10.3)
(33)優先権主張国　米国 (US)

(71)出願人　595020643
クゥアルコム・インコーポレイテッド
ＱＵＡＬＣＯＭＭ　ＩＮＣＯＲＰＯＲＡＴＥＤ
アメリカ合衆国、カリフォルニア州　９２１２１－１７１４、サン・ディエゴ、モアハウス・ドライブ　５７７５
(74)代理人　100058479
弁理士　鈴江　武彦
(74)代理人　100108855
弁理士　蔵田　昌俊
(74)代理人　100091351
弁理士　河野　哲
(74)代理人　100088683
弁理士　中村　誠

最終頁に続く

(54)【発明の名称】相互認証のための方法および装置

(57)【要約】
デジタル権利エージェントを有するステーションとセキュアリムーバブルメディアデバイスとの間の相互認証のための方法が開示される。デジタル権利エージェントがセキュアリムーバブルメディアデバイスにメッセージを送ることによって相互認証が開始する。セキュアリムーバブルメディアデバイスは、デジタル権利エージェントに関連した公開鍵を使用して第１の乱数を暗号化する。デジタル権利エージェントは、暗号化された第１の乱数を復号し、少なくとも第１の乱数に基づいて第２の乱数および第１のハッシュを暗号化する。セキュアリムーバブルメディアデバイスは、暗号化された第２の乱数および第１のハッシュを復号し、デジタル権利エージェントを認証するために第１のハッシュを検証し、少なくとも第２の乱数に基づいて第２のハッシュを生成する。デジタル権利エージェントは、セキュアリムーバブルメディアデバイスを認証するために第２のハッシュを検証する。
【選択図】　図３



【特許請求の範囲】
【請求項１】
第１のエンティティと第２のエンティティとの間の相互認証のための方法であって、
前記第１のエンティティが前記第２のエンティティにメッセージを送信することにより相互認証を開始することと；
前記第２のエンティティが前記第１のエンティティに関連した第１の公開鍵を検証し、第１の乱数を生成し、前記第１の公開鍵を使用して前記第１の乱数を暗号化し、前記暗号化された第１の乱数をメッセージ中で前記第１のエンティティに送信することと；
前記第１のエンティティが前記第２のエンティティに関連した第２の公開鍵を検証し、前記第１の公開鍵に対応した第１の秘密鍵を使用して前記暗号化された第１の乱数を復号し、第２の乱数を生成し、少なくとも前記第１の乱数に基づいて第１のハッシュを生成し、前記第２の公開鍵を使用して前記第２の乱数および前記第１のハッシュを暗号化し、前記暗号化された第２の乱数および第１のハッシュをメッセージ中で前記第２のエンティティに送信することと；
前記第２のエンティティが前記第２の公開鍵に対応する第２の秘密鍵を使用して前記暗号化された第２の乱数および第１のハッシュを復号し、前記第１のエンティティを認証するために前記第１のハッシュを検証し、少なくとも前記第２の乱数に基づいて第２のハッシュ生成し、前記第２のハッシュを前記第１のエンティティに送信することと；
前記第１のエンティティが前記第２のエンティティを認証するために前記第２のハッシュを検証することと；
を備える相互認証方法。
【請求項２】
前記第１のエンティティおよび前記第２のエンティティのそれぞれは、前記第１のエンティティと前記第２のエンティティとの間の通信で使用するために、前記第１の乱数および前記第２の乱数を使用して、鍵導出関数に基づいてセッション暗号鍵およびメッセージ認証コード(MAC)を導出する、請求項1に記載の相互認証方法。
【請求項３】
前記相互認証を開始するメッセージは、前記第１のエンティティのための少なくとも1つの信頼されたルート鍵および対応する証明書チェーンのハッシュを含む、請求項1に記載の相互認証方法。
【請求項４】
前記暗号化された第１の乱数を有する、前記第２のエンティティから前記第１のエンティティへの前記メッセージは、さらに、前記第２のエンティティのための証明書チェーンを含む、請求項１に記載の相互認証方法。
【請求項５】
前記第１のエンティティはデジタル権利エージェントであり、前記第２のエンティティはセキュアリムーバブルメディアデバイスである、請求項1に記載の相互認証方法。
【請求項６】
前記第１のエンティティは移動局である、請求項1に記載の相互認証方法。
【請求項７】
前記第２のエンティティは制限された処理能力を有する、請求項1に記載の相互認証方法。
【請求項８】
前記第１のハッシュはさらに少なくとも前記第２の乱数に基づき、前記第１のハッシュは少なくとも前記第２の乱数が連結された前記第１の乱数に基づいて生成される、請求項1に記載の相互認証方法。
【請求項９】
前記第２のハッシュはさらに少なくとも前記第１の乱数に基づく、請求項1に記載の相互認証方法。
【請求項１０】

前記第２のハッシュはさらに少なくとも前記第１のハッシュに基づき、前記第２のハッシュは少なくとも前記第１のハッシュが連結された前記第２の乱数に基づいて生成される、請求項1に記載の相互認証方法。

【請求項１１】

相互認証のための装置であって、

相互認証を開始する手段と;

第１の公開鍵を検証し、第１の乱数を生成し、前記第１の公開鍵を使用して前記第１の乱数を暗号化する手段と;

第２の公開鍵を検証し、前記第１の公開鍵に対応する第１の秘密鍵を使用して前記暗号化された第１の乱数を復号し、第２の乱数を生成し、少なくとも前記第１の乱数に基づいて第１のハッシュを生成し、前記第２の公開鍵を使用して前記第２の乱数および前記第１のハッシュを暗号化する手段と;

前記第２の公開鍵に対応する第２の秘密鍵を使用して前記暗号化された第２の乱数および第１のハッシュを復号し、認証のために前記第１のハッシュを検証し、少なくとも前記第２の乱数に基づいて第２のハッシュを生成する手段と;

認証のために前記第２のハッシュを検証する手段と；

を備えた相互認証装置。

【請求項１２】

前記第１のエンティティと前記第２のエンティティとの間の通信で使用するために、前記第１の乱数および前記第２の乱数を使用して、鍵導出関数に基づいてセッション暗号鍵およびメッセージ認証コード(MAC)を導出する手段をさらに備えた、請求項11に記載の相互認証装置。

【請求項１３】

前記第１のハッシュはさらに少なくとも前記第２の乱数に基づき、前記第１のハッシュは少なくとも前記第２の乱数が連結された前記第１の乱数に基づいて生成される、請求項11に記載の相互認証装置。

【請求項１４】

前記第２のハッシュはさらに少なくとも前記第１の乱数に基づく、請求項11に記載の相互認証装置。

【請求項１５】

前記第２のハッシュはさらに前記１のハッシュに基づき、前記第２のハッシュは前記第１のハッシュが連結された前記第２の乱数に基づいて生成される、請求項11に記載の相互認証装置。

【請求項１６】

セキュアリムーバブルメディアデバイスとの相互認証を有するステーションであって、デジタル権利エージェントを備え、

前記デジタル権利エージェントは、前記セキュアリムーバブルメディアデバイスにメッセージを送ることにより相互認証を開始し、なお、前記セキュアリムーバブルメディアデバイスは、前記デジタル権利エージェントに関連した第１の公開鍵を検証し、第１の乱数を生成し、前記第１の公開鍵を使用して前記第１の乱数を暗号化し、前記暗号化された第１の乱数をメッセージ中で前記デジタル権利エージェントに送る;

前記デジタル権利エージェントは、前記セキュアリムーバブルメディアデバイスに関連した第２の公開鍵を検証し、前記第１の公開鍵に対応する第１の秘密鍵を使用して前記暗号化された第１の乱数を復号し、第２の乱数を生成し、少なくとも前記第１の乱数に基づいて第１のハッシュを生成し、前記第２の公開鍵を使用して前記第２の乱数および前記第１のハッシュを暗号化し、前記暗号化された第２の乱数および第1のハッシュをメッセージ中で前記セキュアリムーバブルメディアデバイスに送り、なお、前記セキュアリムーバブルメディアデバイスは、前記第２の公開鍵に対応する第２の秘密鍵を使用して前記暗号化された第２の乱数および第1のハッシュを復号し、前記デジタル権利エージェントを認証するために前記第１のハッシュを検証し、少なくとも前記第２の乱数に基づいて第２のハ

ッシュを生成し、前記第２のハッシュを前記デジタル権利エージェントに送る;
前記デジタル権利エージェントは、前記セキュアリムーバブルメディアデバイスを認証するために前記第２のハッシュを検証する；
ステーション。
【請求項１７】
前記デジタル権利エージェントおよびセキュアリムーバブルメディアデバイスの各々は、前記デジタル権利エージェントとセキュアリムーバブルメディアデバイスとの間の通信で使用するために、前記第１の乱数および前記第２の乱数を使用して、鍵導出関数に基づいてセッション暗号鍵およびメッセージ認証コード(MAC)を導出する、請求項16に記載の相互認証を有するステーション。
【請求項１８】
前記相互認証を開始するために前記デジタル権利エージェントによって送られたメッセージは、前記デジタル権利エージェントのための少なくとも1つの信頼されたルート鍵および対応する証明書チェーンのハッシュを含む、請求項16に記載の相互認証を有するステーション。
【請求項１９】
前記デジタル権利エージェントのための前記証明書チェーンは、前記デジタル権利エージェントに関連した前記公開鍵を含む、請求項18に記載の相互認証を有するステーション。
【請求項２０】
前記暗号化された第１の乱数を有し前記セキュアリムーバブルメディアデバイスによって前記デジタル権利エージェントに送られる前記メッセージは、さらに、前記セキュアリムーバブルメディアデバイスのための証明書チェーンを含む、請求項16に記載の相互認証を有するステーション。
【請求項２１】
前記セキュアリムーバブルメディアデバイスのための前記証明書チェーンは、前記セキュアリムーバブルメディアデバイスに関連した前記公開鍵を含む、請求項20に記載の相互認証を有するステーション。
【請求項２２】
前記ステーションは移動局である、請求項16に記載の相互認証を有するステーション。
【請求項２３】
前記第１のハッシュはさらに少なくとも第２の乱数に基づき、前記デジタル権利エージェントは少なくとも前記第２の乱数が連結された前記第１の乱数に基づいて前記第１のハッシュを生成する、請求項16に記載の相互認証を有するステーション。
【請求項２４】
コンピュータが読取り可能な媒体を備えたコンピュータプログラム製品であって、
前記コンピュータが読取り可能な媒体は、
前記コンピュータに、デジタル権利エージェントをして、セキュアリムーバブルメディアデバイスにメッセージを送ることによって相互認証を開始させるためのコードと、なお、前記セキュアリムーバブルメディアデバイスは、前記デジタル権利エージェントに関連した第１の公開鍵を検証し、第１の乱数を生成し、前記第１の公開鍵を使用して前記第１の乱数を暗号化し、前記暗号化された第１の乱数をメッセージ中で前記デジタル権利エージェントに送る;
前記コンピュータに、前記デジタル権利エージェントをして、前記セキュアリムーバブルメディアデバイスに関係した第２の公開鍵を検証させ、前記第１の公開鍵に対応する第１の秘密鍵を使用して前記暗号化された第１の乱数を復号させ、第２の乱数を生成させ、少なくとも前記第１の乱数に基づいて第１のハッシュを生成させ、前記第２の公開鍵を使用して前記第２の乱数および前記第１のハッシュを暗号化させ、前記暗号化された第２の乱数および第１のハッシュをメッセージ中で前記セキュアリムーバブルメディアデバイスに送らせるためのコードと、なお、前記セキュアリムーバブルメディアデバイスは、前記

第２の公開鍵に対応する第２の秘密鍵を使用して前記暗号化された第２の乱数および第1のハッシュを復号し、前記デジタル権利エージェントを認証するために前記第１のハッシュを検証し、少なくとも前記第２の乱数に基づいて第２のハッシュを生成し、前記第２のハッシュを前記デジタル権利エージェントに送る；

前記コンピュータに、前記デジタル権利エージェントをして、前記セキュアリムーバブルメディアデバイスを認証するために前記第２のハッシュを検証させるためのコードと；

を備えたコンピュータプログラム製品。

【請求項２５】

コンピュータが読取り可能な媒体を備えたコンピュータプログラム製品であって、 前記コンピュータが読取り可能な媒体は、

前記コンピュータに、セキュアリムーバブルメディアデバイスをして、デジタル権利エージェントに関連した第１の公開鍵を検証させ、第１の乱数を生成させ、前記第１の公開鍵を使用して前記第１の乱数を暗号化させ、前記暗号化された第１の乱数をメッセージ中で前記デジタル権利エージェントに送らせるためのコードと、なお、前記デジタル権利エージェントは、前記セキュアリムーバブルメディアデバイスに関連した第２の公開鍵を検証し、前記第１の公開鍵に対応する第１の秘密鍵を使用して前記暗号化された第１の乱数を復号し、第２の乱数を生成し、少なくとも前記第１の乱数に基づいて第１のハッシュを生成し、前記第２の公開鍵を使用して前記第２の乱数および前記第１のハッシュを暗号化し、前記暗号化された第２の乱数および第１のハッシュをメッセージ中で前記セキュアリムーバブルメディアデバイスに送る；

前記コンピュータに、前記セキュアリムーバブルメディアデバイスをして、前記第２の公開鍵に対応する第２の秘密鍵を使用して前記暗号化された第２の乱数および第１のハッシュを復号させ、前記デジタル権利エージェントを認証するために前記第１のハッシュを検証させ、少なくとも前記第２の乱数に基づいて第２のハッシュを生成させ、前記第２のハッシュを前記デジタル権利エージェントに送らせるためのコードと、なお、前記デジタル権利エージェントは前記セキュアリムーバブルメディアデバイスを認証するために前記第２のハッシュを検証する；

を備えたコンピュータプログラム製品。

【発明の詳細な説明】

【米国特許法の下での優先権主張】

【０００１】

本出願は、2006年10月10日に申請された「METHOD AND APPARATUS FOR MUTUAL AUTHENITICATION」と題する仮出願第60/850,882号への優先権を主張する。この仮出願は本願の譲受人に譲渡され、参照により本願に明確に組込まれる。

【技術分野】

【０００２】

本発明は、一般に無線通信に関し、特に相互認証(mutual authentication)に関する。

【背景技術】

【０００３】

モバイル加入者は、別のエンティティ(entity)あるいはエージェントによる、認証を必要とするシステムによって保護された内容へのアクセスを望む。普及している認証プロトコルは、RFC 4306に記述されたインターネット鍵交換(Internet Key Exchange)(IKE)プロトコルである。しかしながら、IKEプロトコルは、認証プロセスにおいてエンティティが、認証の速度は問題にしない程に十分な計算あるいは処理能力を有するものと仮定する。

【０００４】

したがって、処理能力に制限のある装置に対する効率的な相互認証の技術が必要とされる。

【発明の概要】

【０００５】

本発明の一態様は、第１のエンティティと第２のエンティティとの間の相互認証のため

の方法に存する。その方法では、第１のエンティティが第２のエンティティにメッセージを送ることにより相互認証を開始する。第２のエンティティは、第１のエンティティに関連した第１の公開鍵(public key)を検証(verify)し、第１の乱数を生成し、第１の公開鍵を使用して第１の乱数を暗号化(encrypt)し、暗号化された第１の乱数をメッセージ中で第１のエンティティに送る。第１のエンティティは、第２のエンティティに関連した第２の公開鍵を検証し、第１の公開鍵に対応する第１の秘密鍵(private key)を使用して、暗号化された第１の乱数を復号(decrypt)し、少なくとも第１の乱数に基づいて第１のハッシュを生成する第２の乱数を生成し、第２の公開鍵を使用して第２の乱数および第１のハッシュを暗号化し、暗号化された第２の乱数および第１のハッシュをメッセージ中で第２のエンティティに送る。第２のエンティティは、第２の公開鍵に対応する第２の秘密鍵を使用して、暗号化された第２の乱数および第１のハッシュを復号し、第１のエンティティを認証するために第１のハッシュを検証し、少なくとも第２の乱数に基づいて第２のハッシュを生成し、第２のハッシュを第１のエンティティに送る。第１のエンティティは、第２のエンティティを認証するために第２のハッシュを検証する。

【０００６】

本発明のより詳細な態様では、第１のエンティティおよび第２のエンティティは各々、第１のエンティティと第２のエンティティとの間のコミュニケーションで使用するために、鍵導出関数(key derivation function)に基づいて、第１の乱数および第２の乱数を使用して、セッション暗号鍵(session encryption key)およびメッセージ認証コード(message authentication code)(MAC)キーを導出する。

【０００７】

さらに、相互認証を開始するメッセージは、第１のエンティティのための少なくとも1個の信頼されたルート鍵(root key)のハッシュおよび対応する証明書チェーン(certificate chain)を含む。第１のエンティティのための証明書チェーンは、第１のエンティティに関連した公開鍵を含む。また、暗号化された第１の乱数を有する第２のエンティティから第１のエンティティへのメッセージは、さらに第２のエンティティのための証明書チェーンを含む。第２のエンティティのための証明書チェーンは、第２のエンティティに関連した公開鍵を含む。

【０００８】

本発明のより詳細な態様では、第１のエンティティは移動局のデジタル権利エージェント(digital rights agent)であり、また、第２のエンティティはセキュア(secure)なリムーバブルメディアデバイスである。第２のエンティティは制限された処理能力を有する。また、第１のハッシュはさらに第２の乱数に基づき、第１のハッシュが第２の乱数と連結された第１の乱数に基づいて生成される。第２のハッシュはさらに第１の乱数を基づき、あるいはさらに第１のハッシュに基づき、第２のハッシュは第１のハッシュと連結された第２の乱数に基づく。

【０００９】

本発明の他の態様は相互認証のための装置にあり、その装置は、相互認証を開始する手段と、第１の公開鍵を検証し、第１の乱数を生成し、第１の公開鍵を使用して第１の乱数を暗号化する手段と、第２の公開鍵を検証し、暗号化された第１の乱数を第１の公開鍵に対応する第１の秘密鍵を使用して復号し、第２の乱数を生成し、少なくとも第１の乱数に基づいて第１のハッシュを生成し、第２の公開鍵を使用して第２の乱数および第１のハッシュを暗号化する手段と、暗号化された第２の乱数および第１のハッシュを第２の公開鍵に対応する第２の秘密鍵を使用して復号し、認証のための第１のハッシュを検証し、少なくとも第２の乱数に基づいて第２のハッシュを生成する手段と、認証のための第２のハッシュを検証する手段とを含む。

【００１０】

本発明の他の態様は、セキュアなリムーバブルメディアデバイスとの相互認証を有し、かつデジタル権利エージェントを含む移動局に存する。デジタル権利エージェントは、メッセージをセキュアリムーバブルメディアデバイスに送ることによって相互認証を開始す

る。ここで、セキュアリムーバブルメディアデバイスは、デジタル権利エージェントに関連した第１の公開鍵を検証し、第１の乱数を生成し、第１の公開鍵を使用して第１の乱数を暗号化し、メッセージ中の暗号化された第１の乱数をデジタル権利エージェントに送る。デジタル権利エージェントは、セキュアリムーバブルメディアデバイスに関連した第２の公開鍵を検証し、第１の公開鍵に対応する第１の秘密鍵を使用して、暗号化された第１の乱数を復号し、第２の乱数を生成し、少なくとも第１の乱数に基づいて第１のハッシュを生成し、第２の公開鍵を使用して第２の乱数および第１のハッシュを暗号化し、暗号化された第２の乱数および第１のハッシュをメッセージ中でセキュアリムーバブルメディアデバイスに送る。ここで、セキュアリムーバブルメディアデバイスは、第２の公開鍵に対応する第２の秘密鍵を使用して、暗号化された第２の乱数および第１のハッシュを復号し、デジタル権利エージェントを認証するために第１のハッシュを検証し、少なくとも第２の乱数に基づいて第２のハッシュを生成し、デジタル権利エージェントに第２のハッシュを送る。デジタル権利エージェントは、セキュアリムーバブルメディアデバイスを認証するために第２のハッシュを検証する。

【００１１】

本発明のさらに他の態様はコンピュータ読取り可能な媒体を備えるコンピュータプログラム製品にあり、コンピュータ読取り可能な媒体は、デジタル権利エージェントを有するステーションのコンピュータに、メッセージをセキュアリムーバブルメディアデバイスに送ることによって相互認証を開始させるためのコードと（なお、セキュアリムーバブルメディアデバイスは、デジタル権利エージェントに関連した第１の公開鍵を検証し、第１のの乱数を生成し、第１の公開鍵を使用して第１の乱数を暗号化し、暗号化された第１の乱数をメッセージ中でデジタル権利エージェントに送る）、コンピュータがデジタル権利エージェントに、セキュアリムーバブルメディアデバイスに関連した第２の公開鍵を検証させ、第１の公開鍵に対応する第１の秘密鍵を使用して、暗号化された第１の乱数を復号させ、第２の乱数を生成させ、少なくとも第１の乱数に基づいて第１のハッシュを生成させ、第２の公開鍵を使用して第２の乱数および第１のハッシュを暗号化させ、暗号化された第２の乱数および第１のハッシュをメッセージ中でセキュアリムーバブルメディアデバイスに送らせるためのコードと（なお、セキュアリムーバブルメディアデバイスは、第２の公開鍵に対応する第２の秘密鍵を使用して、暗号化された第２の乱数および第１のハッシュを復号し、デジタル権利エージェントを認証するために第１のハッシュを検証し、少なくとも第２の乱数に基づいて第２のハッシュを生成し、デジタル権利エージェントに第２のハッシュを送る）、コンピュータがデジタル権利エージェントに、セキュアリムーバブルメディアデバイスを認証するために第２のハッシュを検証させるためのコードとを備える。

【００１２】

本発明のさらに他の態様はコンピュータ読取り可能な媒体を備えるコンピュータプログラム製品にあり、コンピュータ読取り可能な媒体は、コンピュータがセキュアリムーバブルメディアデバイスに、デジタル権利エージェントに関連した第１の公開鍵を検証させ、第１の乱数を生成させ、第１の公開鍵を使用して第１の乱数を暗号化させ、暗号化された第1の乱数をメッセージ中でデジタル権利に送らせるためのコードと（なお、デジタル権利エージェントは、セキュアリムーバブルメディアデバイスに関連した第２の公開鍵を検証し、第１の公開鍵に対応する第１の秘密鍵を使用して、暗号化された第１の乱数を復号し、第２の乱数を生成し、少なくとも第１の乱数に基づいて第１のハッシュを生成し、第２の公開鍵を使用して第２の乱数および第１のハッシュを暗号化し、暗号化された第２の乱数および第１のハッシュをメッセージ中でセキュアリムーバブルメディアデバイスに送る）、コンピュータがセキュアリムーバブルメディアデバイスに、第２の公開鍵に対応する第２の秘密鍵を使用して暗号化された第２の乱数および第１のハッシュを復号させ、デジタル権利エージェントを認証するために第１のハッシュを検証させ、少なくとも第２の乱数に基づいて第２のハッシュを生成させ、第２のハッシュをデジタル権利エージェントに送らせるためのコード（なお、デジタル権利エージェントはセキュアリムーバブルメデ

ィアデバイスを認証するために第２のハッシュを検証する）とを備える。
【図面の簡単な説明】
【００１３】
【図１】図１は無線通信システムの例である。
【図２】図２は、移動局、および相互認証を有するセキュアリムーバブルメディアデバイスのブロックダイヤグラムである。
【図３】図３は、移動局とセキュアリムーバブルメディアデバイスとの間の相互認証のための方法のフローチャートである。
【発明の詳細な説明】
【００１４】
「典型的」という語は「例、インスタンスあるいは実例として役立つ」を意味するためにここに使用される。ここで「典型的である」と記述されたいかなる実施例も、必ずしも他の実施例よりも好ましい、あるいは有利であると解釈されるものではない。
【００１５】
移動局(MS)、アクセスターミナル(AT)、ユーザ設備あるいは加入者ユニットとしても知られている遠隔ステーションは、モバイルであっても静止してもよく、基地トランシーバステーション(BTS)あるいはノードBとしても知られている1つ以上の基地局と通信する。遠隔ステーションは、1つ以上の基地局を介して、無線ネットワークコントローラ(RNC)としても知られている基地局コントローラにデータパケットを送受信する。基地局および基地局コントローラはアクセスネットワークと呼ばれるネットワークの部分である。アクセスネットワークは、複数の遠隔ステーション間でデータパケットを輸送する。アクセスネットワークは、さらに、企業イントラネットあるいはインターネットのようなアクセスネットワークの外部で追加のネットワークに接続され、各遠隔ステーションとそのような外部ネットワークとの間でデータパケットを輸送する。1つ以上の基地局とのアクティブなトラヒックチャンネル接続を確立した遠隔ステーションは、アクティブ遠隔ステーションと呼ばれ、トラヒック状態にあると言われる。1つ以上の基地局とのアクティブなトラヒックチャンネル接続を確立する過程にある遠隔ステーションは、接続セットアップ状態であると言われる。遠隔ステーションは、無線チャンネルを介して通信する任意のデータ装置であり得る。遠隔ステーションは、さらに、PCカード、コンパクトフラッシュ（登録商標）、外部あるいは内蔵モデム、あるいは無線電話を含む、これらに限定されない様々な形式の任意のデバイスであり得る。遠隔ステーションが基地局に信号を送る通信リンクはアップリンクと呼ばれ、逆方向リンクとしても知られている。基地局が遠隔ステーションに信号を送る通信リンクはダウンリンクと呼ばれ、順方向リンクとしても知られている。
【００１６】
図１に関して、無線通信システム100は、1つ以上の無線移動局(MS)102、1つ以上の基地局(BS)104、1つ以上の基地局コントローラ(BSC)106、および、1つのコアネットワーク108を含む。コアネットワークは、適切なバックホールを介してインターネット110および公衆スイッチ電話ネットワーク(PSTN)112に接続されている。典型的な無線移動局は、携帯型の電話、あるいはラップトップコンピュータを含む。無線通信システム100は、符号分割多元接続(CDMA)、時分割多元接続(TDMA)、周波数分割多元接続(FDMA)、空間分割多元接続(SDMA)、極分割多元接続(PDMA)あるいは当該技術分野において既知の他の変調技術のような多くの多元接続技術のうちの任意のものを使用し得る。
【００１７】
計算能力が制限されている多くの低価格装置が、スマートカードおよびフラッシュメモリ(様々なフォームファクターで）のような市場に導入されている。そのような装置は認証を要求する。例えば、デジタル著作権管理(DRM)システムによってこれらの装置に使用権を所有させるという要求がある。これらの装置で使用権を交換する前に、交換を認可されたエンティティに制限するために、交換に関与する両方のエンティティの相互認証が必要である。これらの実施例は、相互認証を遂行するための効率的な方法を提供し、また、関与するエンティティ間での更なる通信において使用することができる、承認された秘密

の交換(confirmed exchange of a secret)を提供する。効率は、計算能力と速度の両方の観点にある。

【００１８】

当業者には明白なように、相互認証スキームは、２つのエンティティ間で相互認証が要求されるいかなるときも使用することができる。相互認証スキームは、ここにおいて実施例を説明するために使用される特定のアプリケーション(デジタル権利管理のような)、システム、およびデバイスに制限されない。

【００１９】

本発明の1つの実施例は、4つのメッセージの交換を使用して、確認鍵交換(confirmed key exchange)による相互認証を実行する。それは、２つの公開鍵署名検証(すべての中間証明用に＋1)、２つの公開鍵暗号化、２つの公開鍵復号、２つのハッシュ生成、および２つのハッシュ検証を必要とする。メッセージ交換、公開鍵検証、公開鍵復号、ハッシュ生成およびハッシュ検証の特定の数は、要求された量のセキュリティおよび効率を達成するために、分割あるいは変更されてもよい。

【００２０】

プロトコルの効率は、公開鍵暗号のオペレーション数を最小化し、また、交換された鍵材料の所有の証拠を提供するためにハッシュ関数を使用することによって増強される。

【００２１】

効率的な相互認証と確認鍵交換プロトコルは、計算バウンドデバイス(compute-bound device)での使用のために記述される。効率は、公開鍵オペレーションの数を最小化し、所有の証拠を提供するために暗号ハッシュ(cryptographic hashes)を使用することによって達成される。

【００２２】

プロトコルは、相互認証のための方法300(図3)を示す図2および図3に関して例証される。下記のステップは図3中の番号が付けられた矢印に相当する。

【００２３】

方法300では、エンティティＡ(例えばMS 102のDRMエージェント202)が、エンティティＢ(例えばSRMエージェント206を有するセキュアリムーバブルメディア(SRM)デバイス204)にHelloAメッセージを送信する(ステップ302)。SRMエージェントは、SRMデバイス中のセキュアストレージ208へのアクセスを管理する。(MSのオペレーティングシステム210は、SRM装置のゼネラルストレージ212に直接アクセスする。) HelloAは、信頼されたルート鍵(あるいはルート鍵のそれら自身)および対応する証明書チェーンのハッシュから成る。このメッセージを受け取ると、エンティティＢは、それがメッセージから信頼するルート鍵を見つけ、選択されたルート鍵の下での証明書チェーンを見つける。それは、選択されたルート鍵の下でのエンティティＡの証明書チェーンを検証する。

【００２４】

エンティティＢは乱数RanBを生成する(ステップ304)。

【００２５】

エンティティＢはエンティティＡにHelloBメッセージを送信する(ステップ306)。HelloBは、選択されたルート鍵の下でのＢの証明書チェーンと、ステップ302の後に選択された証明書チェーンからのエンティティＡの公開鍵で暗号化されたRanBとから成る。エンティティＡがこのメッセージを受け取ると、エンティティＢの証明書チェーンを検証する。有効な場合、それはその秘密鍵(選択されたルート鍵に対応する)でRanBを復号する。

【００２６】

一旦ルート鍵選択と証明書チェーン交換が生じたならば、エンティティＡおよびエンティティＢは互いの証明書チェーンを持つことに注意されたい。したがって、これらのパラメータは、将来の相互認証のためにエンティティＡとエンティティＢとの間での将来のHelloAおよびHelloBメッセージ中で送られる必要はない。その場合、ステップ302および306の証明書チェーン交換はオプションである。

【００２７】

エンティティＡはRanAを生成する(ステップ308)。

【００２８】

エンティティＡはエンティティＢにKeyConfirmAメッセージを送信する(ステップ310)。KeyConfirmAは、RanA、それに連結したRanBのハッシュ、それに連結したRanA(H[RanA|RanB])およびＢの公開鍵で暗号化したこのすべてから成る。このメッセージを受け取ると、エンティティＢはそれを復号する。復号されたRanAを使用して、それは、RanAと連結されたRanBのハッシュを検証する。注:このステップでは、エンティティＢはエンティティＡを認証しており、エンティティＡがRanBを知っていることが保証される。

【００２９】

エンティティＢはエンティティＡにKeyConfirmBメッセージを送信する(ステップ312)。KeyConfirmBは、KeyConfirmAメッセージの復号された部分のハッシュから成る。このメッセージを受け取ると、エンティティＡはハッシュを検証する。注:このステップでは、エンティティＡはエンティティＢを認証しており、エンティティＢがRanAを知っていることが保証される。

【００３０】

この時点で、両方のエンティティは互いを認証し、それらが各々同じRanAおよびRanBを共有することを確認している。RanAとRanBは、パーティー間のさらなる通信での使用のために、鍵導出関数(KDF)に基づいて、セッション暗号鍵(SK)およびMAC鍵(MK)を導出するために使用することができる(ステップ314)。

【００３１】

メッセージの詳細が以下に与えられる。HelloAメッセージは、相互認証を開始するために鍵確認プロトコル(key confirmation protocol)と共に送信される。HelloAメッセージは「バージョン」パラメータと「rootAndChains[ ]」パラメータを有する。バージョンパラメータは8ビット値で、このメッセージのプロトコルバージョンを含む。それは、主バージョン用の5つのMSBと、小さなバージョン用の3つのLSBとして写像される。

【００３２】

rootAndChains[ ]パラメータは、エンティティAによって支持されたすべての信頼モデルの下での、エンティティAのためのルート・ハッシュ配列(an array of the root hashes)および証明書チェーンである。パラメータのための構造、RootHashAndCertChainは、パラメータrootHashであり、それは信頼モデルのルート公開鍵のSHA-1ハッシュである。またパラメータcertChainは、ルート公開鍵の下でのエンティティの証明書チェーンである。エンティティの証明書が最初に来て、それに任意のCA証明書(署名の順に）がルート証明書（それは含まない）まで続く。

【００３３】

HelloBメッセージは、エンティティＢによる鍵確認プロトコルを備えた相互認証を継続する。次のテーブルはパラメータについて記述する。HelloBはパラメータとして次のものを有する。「バージョン」、「ステータス」、「certChain」および「encRanB」バージョンパラメータは8ビット値で、このメッセージのプロトコルバージョンを含む。それは、主バージョン用の5つのMSBと、小さなバージョン用の3つのLSBとして写像される。ステータスパラメータは、HelloAメッセージを処理するエンティティＢのステータスを含む、8ビット値である。ステータスパラメータの値は、成功は0（前のメッセージでエラーに遭遇しなかった）、noSharedRootKeyは１（エンティティBがエンティティＡと共有するルート鍵を発見できなかった）である。値2-255が将来の使用のためにリザーブされる。

【００３４】

certChainパラメータは、HelloAメッセージから選択されたルート鍵の下でのエンティティＢの証明書チェーンである。ステータスパラメータの値が成功でない場合、certChainパラメータは存在しない。encRanBパラメータは、エンティティＡの公開鍵(選択された証明書チェーンからの)を使用した、RSA-OAEP 暗号化ranBである。ranBはエンティティＢによって生成された20バイトの乱数である。ステータスの値が成功でない場合、encRanBパラメータは存在しない。

【００３５】
KeyConfirmAメッセージは、エンティティＡによる鍵確認プロトコルを備えた相互認証を継続する。KeyConfirmAメッセージは「バージョン」パラメータと「encRanB」パラメータを有する。バージョンパラメータは、このメッセージのプロトコルバージョンを含んでいる8ビット値である。それは、主バージョン用の5つのMSBと、小さなバージョン用の3つのLSBとして写像される。encRanBパラメータは、「ranA」パラメータと「hashBA」パラメータを有するRSA-OAEP 暗号化 KeyConfirmData 構造である。ranAパラメータは、エンティティＡによって生成された20バイトの乱数であり、また、ハッシュBAパラメータは、ranAと連結されたranBのSHA-1ハッシュである。

【００３６】
KeyConfirmBメッセージは、エンティティＢによる鍵確認プロトコルを備えた相互認証を終了させる。KeyConfirmBメッセージは「バージョン」パラメータ、ステータスパラメータおよび「hashKeyConfirm」パラメータを有する。バージョンパラメータは、このメッセージのプロトコルバージョンを含んでいる8ビット値である。それは、主バージョン用の5つのMSBと、小さなバージョン用の3つのLSBとして写像される。ステータスパラメータは、メッセージを処理するエンティティＢのステータスを含んでいる8ビット値である。hashKeyConfirmパラメータは、エンティティＢによって復号されたKeyConfirmData 構造のSHA-1ハッシュである。ステータスパラメータの値が成功でない場合、このパラメータは存在しない。

【００３７】
本発明の他の態様は、DRMエージェント202に方法300を実現させるために、制御プロセッサ216およびOS 210を含む移動局102に存する。本発明のさらに他の態様は、コンピュータに方法300のステップをDRMエージェントに行なわせるためのコードを含む、コンピュータ読取り可能な媒体(メモリデバイス218のような)を含むコンピュータプログラム製品に存する。

【００３８】
当業者は、情報および信号が様々な異なる技術および技法のうちのいずれを使用して表わされてもよいことを理解するであろう。例えば、上の記述の全体にわたって参照されたデータ、命令、コマンド、情報、信号、ビット、シンボルおよびチップは、電圧、電流、電磁波、磁界またはパーティクル、光学フィールドまたはパーティクル、あるいはそれの任意の組み合わせによって表わされてもよい。

【００３９】
熟練者はまた、ここに示された実施例に関して記述された様々な例示的な論理ブロック、モジュール、回路、およびアルゴリズム・ステップは、電子ハードウェア、コンピュータ・ソフトウェアあるいはその両方の組み合わせとしてインプリメントされてもよいことを認識するであろう。 このハードウェアとソフトウェアの互換性を明白に例証するために、上では様々な例示となるコンポーネント、ブロック、モジュール、回路およびステップが、それらの機能性の点から概論的に説明された。 そのような機能性がハードウェアとしてインプリメントされるかソフトウェアとしてインプリメントされるかは、全体システムに課された特定のアプリケーションおよび設計制約に依存する。 熟練した職人は記述された機能性を各特定のアプリケーション用に変更してインプリメントしてもよいが、そのようなインプリメンテーションの決定が本発明の範囲からの離脱を引き起こすと解釈されるべきでない。

【００４０】
ここに示された実施例に関して記述された様々な例示的な論理ブロック、モジュールおよび回路は、汎用プロセッサ、デジタル信号プロセサ(DSP)、特定用途向けIC(ASIC)、フィールドプログラム可能なゲートアレイ(FPGA)あるいは他のプログラム可能な論理回路、個別ゲートあるいはトランジスタ・ロジック、個別のハードウェア・コンポーネント、あるいはここに記述された機能を実行するために設計されたそれらの任意の組み合わせによってインプリメントあるいは実行することができる。 汎用プロセッサはマイクロプロセ

ッサであり得る。しかし、代替では、プロセッサは任意の従来のプロセッサ、コントローラ、マイクロコントローラあるいは状態マシンであってもよい。また、プロセッサは、例えばDSPとマイクロプロセッサの組み合わせ、複数のマイクロプロセッサ、DSPコアと協働する1個以上のマイクロプロセッサ、あるいは他のそのような構成のような計算装置の組み合わせとしてインプリメントすることができる。

【００４１】

ここに示された実施例に関して記述された方法あるいはアルゴリズムのステップは、ハードウェアに直接、あるいはプロセッサによって実行されるソフトウェアモジュールに、あるいはそれら2つの組み合わせ中で具現化することができる。ソフトウェアモジュールは、RAMメモリ、フラッシュメモリ、ROMメモリ、EPROMメモリ、EEPROMメモリ、レジスタ、ハードディスク、リムーバブルディスク、CD-ROM、あるいは当該技術分野で既知の他の形式の記憶メディアに存在することができる。典型的な記憶メディアはプロセッサに結合され、プロセッサが記憶メディアから情報を読むことができ、記憶メディアに情報を書くことができる。代替では、記憶メディアはプロセッサと一体であり得る。プロセッサと記憶メディアはASICに存在してもよい。 ASICはユーザ端末に存在してもよい。代替では、プロセッサと記憶メディアはユーザ端末中に個別のコンポーネントとして存在してもよい。

【００４２】

1つ以上の典型的な実施例では、記述された機能は、ハードウェア、ソフトウェア、ファームウェアあるいはそれの任意のコンビネーション中でインプリメントされ得る。もしコンピュータプログラム製品としてソフトウェア中でインプリメントされるならば、機能は、コンピュータが読み取り可能な媒体上の1つ以上の命令あるいはコードとして、格納され、あるいは送信され得る。コンピュータが読み取り可能な媒体は、コンピュータ記憶媒体およびある場所から別の場所へコンピュータプログラムの転送を促進する任意の媒体を含む通信媒体の両方を含む。記憶媒体は、コンピュータによってアクセスすることができるあらゆる利用可能な媒体であり得る。制限ではなく例示として、そのようなコンピュータ可読媒体はRAM、ROM、EEPROM、CD-ROMまたは他の光ディスク記憶装置、磁気ディスク記憶装置または他の磁気記憶装置、あるいは、命令もしくはデータ構造の形で所要のプログラムコードを運びもしくは格納するために使用することができ、コンピュータによってアクセスされることができる他の媒体を含む。さらに、いかなる接続もコンピュータが読み取り可能な媒体と適切に名付けられる。例えば、ソフトウェアがウェブサイト、サーバーあるいは他の遠隔の出所から、同軸ケーブル、光ファイバケーブル、撚り対線、デジタル加入者線(DSL)あるいは赤外線、無線およびマイクロ波のような無線技術を使用して送信される場合、同軸ケーブル、光ファイバケーブル、撚り対線、DSLあるいは赤外線、無線およびマイクロ波のような無線技術は、媒体の定義に含まれる。ここで使用されたディスクは、磁気的にデータを再生し、あるいはレーザーでデータを光学上に再生する、コンパクト・ディスク(CD)、レーザーディスク（登録商標）、光ディスク、ディジタル・バーサタイル・ディスク(DVD)、フロッピー（登録商標）ディスクおよびブルーレイ・ディスクを含む。 上記のもののコンビネーションもまた、コンピュータが読み取り可能な媒体の範囲内に含まれるべきである。

【００４３】

開示された実施例の以上の記述は、いかなる当業者も本発明を製造あるいは使用することを可能にするために提供される。 これらの実施例への様々な変更は当業者に容易に明白であり、またここに定義された総括的な本質は、開示の精神あるいは範囲から逸脱することなく、他の実施例に適用することができる。したがって、本開示は、ここに示された実施例に制限されるようには意図されず、ここに示された本質と新規な特徴と合致する最も広い範囲が与えられるべきものである。

【図１】

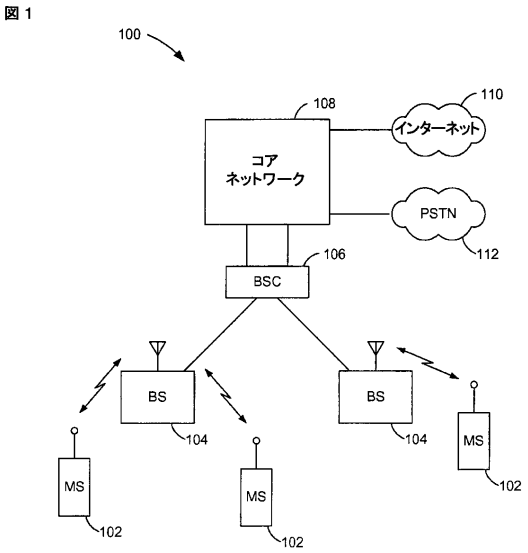


FIG. 1

【図２】

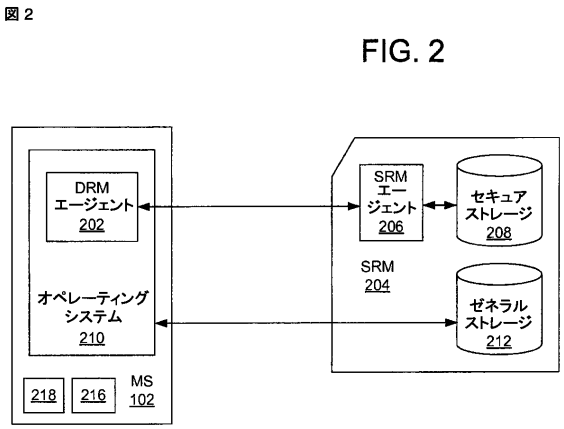


FIG. 2

【図３】

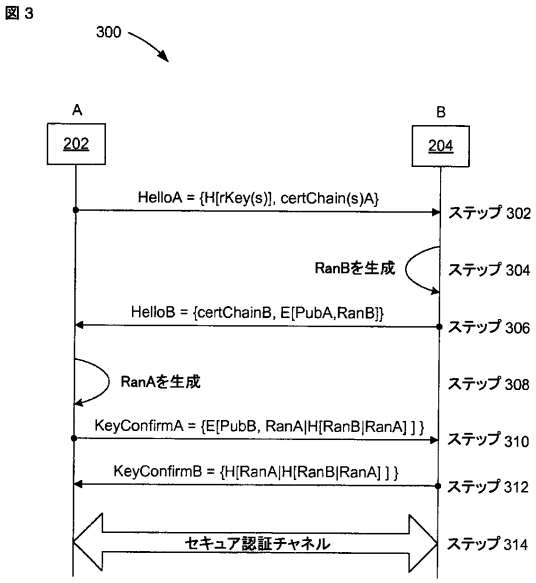


FIG. 3

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2007/080525

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L9/32

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, INSPEC, IBM-TDB, COMPENDEX

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	MENEZES ET AL: "HANDBOOK OF APPLIED CRYPTOGRAPHY" HANDBOOK OF APPLIED CRYPTOGRAPHY, CRC PRESS SERIES ON DISCRETE MATHEMATICES AND ITS APPLICATIONS, BOCA RATON, FL, CRC PRESS, US, 1997, pages 403-405,506, XP002165287 ISBN: 0-8493-8523-7 page 403 - page 405	1-25
Y	US 6 769 060 B1 (DENT PAUL W [US] ET AL) 27 July 2004 (2004-07-27) column 6, line 32 - column 8, line 17; figure 4	1-25

-/--

[X] Further documents are listed in the continuation of Box C. [X] See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
14 April 2008	21/04/2008

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Cretaine, Philippe

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

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2007/080525

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 7 024 690 B1 (YOUNG ALBERT [US] ET AL) 4 April 2006 (2006-04-04) column 5, line 1 - column 6, line 50; figure 3	1-25
A	WO 2005/091551 A (SAMSUNG ELECTRONICS CO LTD [KR]; LEE BYUNG-RAE [KR]; KIM TAE-SUNG [KR]) 29 September 2005 (2005-09-29) paragraphs [0042] - [0047]; figure 3	1-25

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

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/US2007/080525

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 6769060 B1	27-07-2004	NONE	
US 7024690 B1	04-04-2006	NONE	
WO 2005091551 A	29-09-2005	AU 2005223902 A1	29-09-2005
		CA 2560570 A1	29-09-2005
		EP 1733504 A1	20-12-2006
		JP 2007529975 T	25-10-2007

フロントページの続き

(81)指定国 AP(BW,GH,GM,KE,LS,MW,MZ,NA,SD,SL,SZ,TZ,UG,ZM,ZW),EA(AM,AZ,BY,KG,KZ,MD,RU,TJ,TM),EP(AT,BE,BG,CH,CY,CZ,DE,DK,EE,ES,FI,FR,GB,GR,HU,IE,IS,IT,LT,LU,LV,MC,MT,NL,PL,PT,RO,SE,SI,SK,TR),OA(BF,BJ,CF,CG,CI,CM,GA,GN,GQ,GW,ML,MR,NE,SN,TD,TG),AE,AG,AL,AM,AT,AU,AZ,BA,BB,BG,BH,BR,BW,BY,BZ,CA,CH,CN,CO,CR,CU,CZ,DE,DK,DM,DO,DZ,EC,EE,EG,ES,FI,GB,GD,GE,GH,GM,GT,HN,HR,HU,ID,IL,IN,IS,JP,KE,KG,KM,KN,KP,KR,KZ,LA,LC,LK,LR,LS,LT,LU,LY,MA,MD,ME,MG,MK,MN,MW,MX,MY,MZ,NA,NG,NI,NO,NZ,OM,PG,PH,PL,PT,RO,RS,RU,SC,SD,SE,SG,SK,SL,SM,SV,SY,TJ,TM,TN,TR,TT,TZ,UA,UG,US,UZ,VC,VN,ZA,ZM,ZW

(74)代理人 100109830
弁理士 福原 淑弘
(74)代理人 100075672
弁理士 峰 隆司
(74)代理人 100095441
弁理士 白根 俊郎
(74)代理人 100084618
弁理士 村松 貞男
(74)代理人 100103034
弁理士 野河 信久
(74)代理人 100119976
弁理士 幸長 保次郎
(74)代理人 100153051
弁理士 河野 直樹
(74)代理人 100140176
弁理士 砂川 克
(74)代理人 100100952
弁理士 風間 鉄也
(74)代理人 100101812
弁理士 勝村 紘
(74)代理人 100070437
弁理士 河井 将次
(74)代理人 100124394
弁理士 佐藤 立志
(74)代理人 100112807
弁理士 岡田 貴志
(74)代理人 100111073
弁理士 堀内 美保子
(74)代理人 100134290
弁理士 竹内 将訓
(74)代理人 100127144
弁理士 市原 卓三
(74)代理人 100141933
弁理士 山下 元
(72)発明者 ペレズ、アラム
アメリカ合衆国、カリフォルニア州 ９２１２１、サン・ディエゴ、モアハウス・ドライブ ５７７５
(72)発明者 ドンデティ、ラクシュミナス・レディー
アメリカ合衆国、カリフォルニア州 ９２１２１、サン・ディエゴ、モアハウス・ドライブ ５７７５

Ｆターム(参考) 5B285 AA01 BA08 CA43 CA44 CA47 CB09 CB47 CB63 CB64 CB74

CB75 CB76
5J104 AA07 AA16 EA04 EA18 FA00 JA21 KA02 KA05 NA02 NA03
NA12 NA37 NA38 PA07