(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第5579872号
(P5579872)

(45)発行日　平成26年8月27日(2014.8.27)　(24)登録日　平成26年7月18日(2014.7.18)

(51)Int.Cl.　　F I
H04L 9/08 (2006.01)　　H04L 9/00 601C
H04L 9/32 (2006.01)　　H04L 9/00 601E
　　H04L 9/00 675A

請求項の数 10　(全 14 頁)

(21)出願番号　特願2012-548017(P2012-548017)
(86)(22)出願日　平成22年12月14日(2010.12.14)
(65)公表番号　特表2013-516896(P2013-516896A)
(43)公表日　平成25年5月13日(2013.5.13)
(86)国際出願番号　PCT/US2010/060283
(87)国際公開番号　WO2011/084419
(87)国際公開日　平成23年7月14日(2011.7.14)
審査請求日　平成24年9月4日(2012.9.4)
(31)優先権主張番号　12/655,706
(32)優先日　平成22年1月6日(2010.1.6)
(33)優先権主張国　米国(US)

(73)特許権者　391030332
アルカテル－ルーセント
フランス国、９２１００・ブローニュ－ビヤンクール、ルート・ドゥ・ラ・レーヌ・１４８／１５２
(74)代理人　110001173
特許業務法人川口國際特許事務所
(72)発明者　コレスニコフ，ブラジーミル・ワイ
アメリカ合衆国、ニユー・ジヤージー・０７３０５、ジヤージー・シテイ、ウエスト・シアウオーター・コート・２０６、アパートメント・５２

審査官　青木　重徳

最終頁に続く

(54)【発明の名称】安全な複数ＵＩＭ認証および鍵交換

(57)【特許請求の範囲】
【請求項１】
装置において、
第１のランダムノンス（ＲＡＮＤ）および認証トークンを受け取ることによって認証鍵合意プロトコルを実行する通信デバイス構成要素であって、共有秘密鍵を有するように構成される、通信デバイス構成要素を備え、
通信デバイス構成要素は、ＲＡＮＤおよび共有秘密鍵に擬似ランダム関数を適用することによって派生鍵を発生し、
通信デバイス構成要素は、第２のランダムノンス（ＲＡＮＤＣ）および派生鍵に基づいてセッション鍵の第１の組を発生し、セッション鍵の第１の組は通信を暗号化するのに用いられ、
同じ加入者によって所有されている複数の装置のそれぞれに関連付けられている各通信デバイス構成要素は、同じ共有秘密鍵を有する、装置。
【請求項２】
通信デバイス構成要素が、通信デバイスに動作可能に接続されたユーザ識別モジュールであり、
セッション鍵の第１の組が、安全な通信を行うためにセッション鍵の第２の組と共に用いられ、セッション鍵の第１の組とセッション鍵の第２の組は等しく、
ユーザ識別モジュールは、派生鍵、共有秘密鍵、およびセッション鍵の第１の組を備え、ユーザ識別モジュールは、セッション鍵の第１の組を通信デバイスにエクスポートし、

共有秘密鍵および派生鍵は通信デバイスにエクスポートされない、請求項１に記載の装置。

【請求項３】

認証トークンが、シーケンス番号、第１のメッセージ認証コード、および認証管理フィールドを含み、

ユーザ識別モジュールが、共有秘密鍵、シーケンス番号、認証管理フィールド、およびＲＡＮＤに擬似ランダム関数を適用することによって第２のメッセージ認証コードを計算し、

ユーザ識別モジュールが、第２のメッセージ認証コードを第１のメッセージ認証コードと比較し、第１のメッセージ認証コードが第２のメッセージ認証コードに等しい場合は、ユーザインターフェースモジュールは、ＲＡＮＤＣおよび派生鍵に基づいて、セッション鍵および応答（ＲＥＳ）を導出し、

ユーザ識別モジュールが、セッション鍵の第１の組、ＲＡＮＤＣ、および応答を通信デバイスにエクスポートする、請求項２に記載の装置。

【請求項４】

ＲＡＮＤＣおよび派生鍵に基づいて、セッション鍵の第１の組および応答（ＲＥＳ）を導出することが、

ＲＡＮＤＣを発生すること、

擬似ランダム関数を適用することによってセッション鍵の第１の組を計算することであって、セッション鍵の第１の組は完全性鍵および暗号鍵を含む、セッション鍵の第１の組を計算すること、

ＲＡＮＤＣおよび派生鍵に擬似ランダム関数を適用することによって応答を計算すること、をさらに含み、

ユーザ識別モジュールが、ＲＡＮＤＣおよび派生鍵に擬似ランダム関数を適用することによって完全性鍵を計算し、

ユーザ識別モジュールが、ＲＡＮＤＣおよび派生鍵に擬似ランダム関数を適用することによって暗号鍵を計算し、

通信デバイスはＲＡＮＤＣおよび応答をサービングネットワークに通信し、サービングネットワークはセッション鍵の第２の組を発生し、セッション鍵の第１の組およびセッション鍵の第２の組はサービングネットワークと通信デバイスの間の通信を暗号化するために用いられる、請求項３に記載の装置。

【請求項５】

サービングネットワークノードにおいて、

通信可能に結合されたクライアントから、応答（ＲＥＳ）および第２のランダムノンス（ＲＡＮＤＣ）を受け取り、

クライアント識別子に基づいて派生鍵を取り出し、

派生鍵およびＲＡＮＤＣに擬似ランダム関数を適用することによって期待応答（ＸＲＥＳ）を計算し、

応答を期待応答と比較し、応答が期待応答に等しい場合はセッション鍵の第１の組を導出し、セッション鍵の第１の組は暗号化された通信を行うためにセッション鍵の第２の組と共に用いられ、

同じ加入者によって所有されている複数のクライアントのそれぞれに関連付けられている各ユーザ識別モジュールは、同じ共有秘密鍵を有する、サービングネットワークノード。

【請求項６】

セッション鍵の第１の組とセッション鍵の第２の組は等しく、

セッション鍵の第２の組は、クライアントによって発生され、

セッション鍵の第１の組は、完全性鍵および暗号鍵を含み、完全性鍵はＲＡＮＤＣおよび派生鍵に擬似ランダム関数を適用することによって計算され、

暗号鍵は、ＲＡＮＤＣおよび派生鍵に擬似ランダム関数を適用することによって計算さ

れ、
ＲＡＮＤＣおよび派生鍵に擬似ランダム関数を適用することによって期待応答を計算し、
期待応答が応答に等しい場合は、セッション鍵の第１の組を導出する、請求項５に記載のサービングネットワークノード。
【請求項７】
鍵サーバに通信可能に結合され、
鍵サーバから認証ベクトルを受け取り、認証ベクトルは第１のランダムノンス（ＲＡＮＤ）、認証トークン、および派生鍵を含み、
派生鍵を記憶し、
クライアントからの要求に応じて、ＲＡＮＤおよび認証トークンをクライアントに通信し、
クライアントが、ＲＡＮＤおよび認証トークンを用いてセッション鍵の第２の組を計算する、請求項６に記載のサービングネットワークノード。
【請求項８】
サービングネットワーク中の装置において実行される方法において、
第１のランダムノンス（ＲＡＮＤ）、第１の派生鍵、および認証トークンを含む、認証ベクトルを受け取るステップと、
認証要求メッセージを通信するステップであって、認証要求メッセージはＲＡＮＤおよび認証トークンを含む、ステップと、
第２のランダムノンス（ＲＡＮＤＣ）および応答（ＲＥＳ）をクライアントから受け取るステップと、
ＲＡＮＤＣおよび第１の派生鍵に基づいてセッション鍵の第１の組を導出するステップであって、セッション鍵の第１の組は通信を暗号化するために用いられる、ステップと
を含み、
同じ加入者によって所有されている複数のクライアントのそれぞれに関連付けられている各ユーザ識別モジュールは、同じ共有秘密鍵を有する、方法。
【請求項９】
応答が期待応答に等しいかどうかを判定するステップであって、期待応答は第１の派生鍵およびＲＡＮＤＣに擬似ランダム関数を適用することによって計算される、ステップと、
期待応答が応答に等しい場合にセッション鍵の第１の組を導出するステップであって、セッション鍵の第１の組は暗号鍵および完全性鍵を含み、暗号鍵は第１の派生鍵およびＲＡＮＤＣに擬似ランダム関数を適用することによって計算され、完全性鍵はＲＡＮＤＣおよび第１の派生鍵に擬似ランダム関数を適用することによって計算される、ステップと、
をさらに含み、第１の派生鍵が第１の共有秘密鍵およびＲＡＮＤに擬似ランダム関数を適用することによって導出され、
第１のメッセージ認証コードが、第１の共有秘密鍵、シーケンス番号、ＲＡＮＤ、および認証管理フィールドに擬似ランダム関数を適用することによって計算され、
認証トークンがシーケンス番号、認証管理フィールド、および第１のメッセージ認証コードをさらに含む、請求項８に記載の方法。
【請求項１０】
クライアントは、第２の共有秘密鍵およびＲＡＮＤに擬似ランダム関数を適用することによって第２の派生鍵を計算し、
クライアントが第１のメッセージ認証コードが第２のメッセージ認証コードに等しいことを検証し、第１のメッセージ認証コードが第２のメッセージ認証コードに等しい場合は、ＲＡＮＤＣを発生し、ＲＡＮＤＣおよび第２の派生鍵に擬似ランダム関数を適用することによって応答を計算し、セッション鍵の第２の組を計算し、
クライアントが第２の派生鍵をユーザ識別モジュール内に保持し、ユーザ識別モジュールから第２の派生鍵をエクスポートせず、

セッション鍵の第２の組を計算するステップが完全性鍵および暗号鍵を計算するステップをさらに含み、完全性鍵は第２の派生鍵およびＲＡＮＤＣに擬似ランダム関数を適用することによって計算され、暗号鍵は第２の派生鍵およびＲＡＮＤＣに擬似ランダム関数を適用することによって計算され、

第１の派生鍵は第２の派生鍵に等しい、請求項９に記載の方法。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は一般に通信デバイスの認証における、認証および安全な鍵合意に関し、より詳細には加入者が複数のユーザ識別モジュールを用いる場合の拡張認証プロトコル（ｅｘｔｅｎｓｉｂｌｅ　ａｕｔｈｅｎｔｉｃａｔｉｏｎ　ｐｒｏｔｏｃｏｌ：ＥＡＰ）－認証および鍵合意（ａｕｔｈｅｎｔｉｃａｔｉｏｎ　ａｎｄ　ｋｅｙ　ａｇｒｅｅｍｅｎｔ：ＡＫＡ）に関する。

【背景技術】

【０００２】

通信業界では安全なトランザクションを提供する必要性が十分に認められている。サービス提供者が、安全なトランザクションをサポートするシステムを提供できなければ、加入者は、購入、または安全に行われなければならない任意の他の商取引をするために無線デバイスを用いないことになる。したがって通信業界は絶えず、加入者が安全に個人的および業務上のトランザクションを行うことができる安全な環境を提供する努力をしている。たとえば、ユニバーサル移動体通信システム（Ｕｎｉｖｅｒｓａｌ　Ｍｏｂｉｌｅ　Ｔｅｌｅｃｏｍｍｕｎｉｃａｔｉｏｎｓ　Ｓｙｓｔｅｍ：ＵＭＴＳ）標準は、認証鍵合意（ａｕｔｈｅｎｔｉｃａｔｉｏｎ　ｋｅｙ　ａｇｒｅｅｍｅｎｔ：ＡＫＡ）および拡張認証プロトコル（ＥＡＰ）－ＡＫＡを提供していることが知られている。

【０００３】

ＡＫＡおよびＥＡＰ－ＡＫＡでは通信デバイスは、共有秘密鍵を用いて認証される。共有秘密鍵は、通信デバイスの一部であるユーザ識別モジュール（ｕｓｅｒ　ｉｄｅｎｔｉｔｙ　ｍｏｄｕｌｅ：ＵＩＭ）内に常駐することができる。ネットワーク内に常駐する通信デバイスおよびサーバは、通信デバイスとアクセスネットワークの間の安全な通信リンクを確保するために、秘密鍵を用いて他の様々な鍵を計算することができる。この枠組みは、１つのＵＩＭしかないときは有効に働く。

【発明の概要】

【発明が解決しようとする課題】

【０００４】

しかし加入者は、通常、２つ以上の通信デバイスを有する。たとえば加入者は、携帯電話、携帯情報端末、ラップトップ、および他の通信デバイスを有し得る。これらのデバイスのそれぞれは、アクセスネットワークを通して無線サービスを受けることができる。またこれらのデバイスのそれぞれは、安全なトランザクションをもたらすために認証される必要がある。複数の通信デバイスを有する加入者をサポートするための有効な方法は、加入者が所有する各デバイス用のＵＩＭカードを加入者に与えることであり、各ＵＩＭカードは同じ共有秘密鍵を有する。しかし加入者が複数のＵＩＭを有する場合は、ＡＫＡおよびＥＡＰ－ＡＫＡプロトコルにセキュリティホールが生じる。サービス提供者が、安全な通信リンクを提供し、かつ加入者が同じ共有秘密鍵を有する複数のＵＩＭカードをもつことを可能にすることを望むならば、複数のＵＩＭカードをもつことに関連するセキュリティホールに対処しなければならない。

【課題を解決するための手段】

【０００５】

一実施形態では装置が提供される。装置は、第１のランダムノンス（ＲＡＮＤ）および認証トークンを受け取ることによって認証鍵合意プロトコルを実行する通信デバイス構成要素を備え、通信デバイス構成要素は共有秘密鍵を有するように構成される。通信デバイ

ス構成要素は、ＲＡＮＤおよび共有秘密鍵に擬似ランダム関数を適用することによって派生鍵を発生する。通信デバイス構成要素は、第２のランダムノンス（ＲＡＮＤＣ）および派生鍵に基づいて、セッション鍵の第１の組を発生し、セッション鍵の第１の組は通信を暗号化するのに用いられる。

【０００６】

他の実施形態では装置が提供される。装置は、応答および第１のランダムノンス（ＲＡＮＤＣ）を受け取るように構成される。装置はまた、クライアント識別子に基づいて派生鍵を取り出し、派生鍵およびＲＡＮＤＣから期待応答を計算するように構成される。さらに装置は、応答を期待応答と比較し、応答が期待応答に等しい場合は、セッション鍵の第１の組を導出し、セッション鍵の第１の組は、暗号化された通信を行うためにセッション鍵の第２の組と共に用いられる。

【０００７】

他の実施形態は方法が提供される。方法は、第１のランダムノンス（ＲＡＮＤ）、第１の派生鍵、および認証トークンを含む認証ベクトルを受け取るステップを含む。方法はまた、認証要求メッセージを通信するステップであって、認証要求メッセージはＲＡＮＤおよび認証トークンを含む、ステップと、第２のランダムノンス（ＲＡＮＤＣ）および応答を受け取るステップとを含む。方法はさらに、ＲＡＮＤＣに基づいてセッション鍵の第１の組、および第１の派生鍵を導出するステップを含み、セッション鍵の第１の組は通信を暗号化するために用いられる。

【０００８】

本発明の例示の実装形態の特徴は、説明、特許請求の範囲、および添付の図面から明らかになるであろう。

【図面の簡単な説明】

【０００９】

【図１】従来技術の認証および鍵合意プロトコルを示すメッセージフローの一実装形態を示す図である。

【図２ａ】従来技術の認証および鍵合意プロトコルに関連する計算を表す図である。

【図２ｂ】従来技術の認証および鍵合意プロトコルに関連する計算を表す図である。

【図３】安全な複数ＵＩＭ認証および鍵交換プロトコルに対する例示のメッセージフローを示す図である。

【図４ａ】安全な複数ＵＩＭ認証鍵交換プロトコルの一実施形態に関連する計算を表す図である。

【図４ｂ】安全な複数ＵＩＭ認証鍵交換プロトコルの一実施形態に関連する計算を表す図である。

【図５】安全な複数ＵＩＭ認証鍵交換方法の一実施形態を示す例示のフローチャートである。

【発明を実施するための形態】

【００１０】

図１を参照すると、一実施例におけるメッセージフロー１００は、安全なアクセスチャネルをもたらすためのＡＫＡ／ＥＡＰ－ＡＫＡメッセージフローの図を含む。ここからは簡潔にするためにＡＫＡのみについて述べるが、ＡＫＡに関するすべての説明はＡＫＡ／ＥＡＰにも当てはまる。ＡＫＡ認証プロトコルは、事前共有または共有秘密鍵（ｐｒｅ－ｓｈａｒｅｄ　ｏｒ　ｓｈａｒｅｄ　ｓｅｃｒｅｔ　ｋｅｙ：ＰＳＫ）を有する、プロトコル内のいくつかの参加者に基づく鍵交換（ｋｅｙ　ｅｘｃｈａｎｇｅ：ＫＥ）プロトコルである。プロトコルにおける主参加者は通常は、サービングネットワーク（Ｓ）１１０へのアクセスを要求する通信デバイスすなわちクライアント（Ｃ）１０５である。サービングネットワークは、ホームネットワークである場合もあり、サービングネットワークはクライアントが訪問しているネットワークである場合もある。以下の説明ではメッセージは、サービングネットワーク１１０に送られる。一実施形態ではこれらのメッセージは、ホーム位置レジスタ、訪問者位置レジスタ、または他のサービングネットワークの構成要

素に向かうことができる。実施された場合は、これらのメッセージはサービングネットワークの特定のノードに向かうことができるが、以下では一般にメッセージはサービングネットワーク１１０に向かうものとして説明する。サービングネットワーク１１０は通常は、クライアント（１０５）、および鍵サーバ（ｋｅｙ　ｓｅｒｖｅｒ：ＫＳ）１１５と対話する。鍵サーバ１１５は通常は、クライアント（１０５）のホームネットワーク内に常駐する。

【００１１】

クライアント１０５がネットワーク１１０にアクセスするときは、クライアント１０５は、アクセス要求１２０をサービングネットワーク１１０に送ることができる。アクセス要求１２０は、クライアントデバイス（モバイル通信デバイス）の電源投入、バーストデータに対する要求、またはクライアント１０５がサービングネットワーク１１０との接続の確立を望む場合がある任意の他の理由の結果として生じ得る。クライアント１０５および鍵サーバ１１５は、ネットワークを通して安全にデータを転送するのに用いられる完全性鍵（ｉｎｔｅｇｒｉｔｙ　ｋｅｙ：ＩＫ）と、暗号鍵（ｃｉｐｈｅｒ　ｋｅｙ：ＣＫ）とを発生する。通常はＩＫおよびＣＫは、共有秘密鍵を用いて発生される。共有秘密鍵は、サービングネットワーク１１０に無線で渡されず、通常はその代わりに共有秘密鍵は鍵サーバ１１５上に記憶される。また共有秘密鍵は、鍵サーバ１１５からサービングネットワークに送出されず、その代わりに鍵サーバ１１５は、様々な変数を含む認証ベクトル（ａｕｔｈｅｎｔｉｃａｔｉｏｎ　ｖｅｃｔｏｒ：ＡＶ）をサービングネットワーク１１０に渡す。サービングネットワーク１１０は、認証ベクトルの内容を用いてクライアント１０５を認証し、クライアント１０５とサービングネットワーク１１０の間の安全なチャネルを確立する。したがってクライアント１０５がサービングネットワーク１１０にアクセスしたときは、サービングネットワーク１１０は鍵サーバ１１５がどこに常駐するかを判定し、認証データ要求メッセージ１２２を鍵サーバ１１５に送る。

【００１２】

認証データ要求１２２を受け取るとすぐに鍵サーバ１１５は、クライアント１０５の識別情報に基づいて共有秘密鍵を検索し、認証ベクトルに用いるべき値を決定する。一実施形態では認証ベクトルは、ランダムノンス（ＲＡＮＤ）、期待応答（ＸＲＥＳ）、ＣＫ、ＩＫ、および認証トークン（ＡＵＴＮ）の連接を含むことができる。これらの値に到達するために鍵サーバ１１５は、擬似ランダム関数f_1からf_5を使用することができる。これらの関数は異なる擬似ランダム関数でもよく、ＡＥＳなどの同じ関数でもよい。後者の場合は関数が呼ばれたときに、関数特有の引数が先頭に追加されなければならない。したがってたとえば、$f_i(x) = AES(i, x)$である。本明細書では擬似ランダム関数とは、ＡＥＳ、ハッシュ関数、擬似ランダム関数、Ｒｉｊｎｄａｅｌ、または任意の他の擬似ランダム関数また準擬似ランダム関数を指す。

【００１３】

ＡＶを含む値に導出には、ＡＶの他の変数を計算するのに、ＲＡＮＤ、シーケンス番号（ｓｅｑｕｅｎｃｅ　ｎｕｍｂｅｒ：ＳＱＮ）、匿名鍵（ａｎｏｎｙｍｉｔｙ　ｋｅｙ：ＡＫ）、およびメッセージ認証コード（ｍｅｓｓａｇｅ　ａｕｔｈｅｎｔｉｃａｔｉｏｎ　ｃｏｄｅ：ＭＡＣ）を用いることができる。鍵サーバ１１５は、ＲＡＮＤおよびＳＱＮを発生することができる。ＲＡＮＤは、たとえばＳＱＮなどの様々なパラメータを用いて発生することができる。ＳＱＮは、一時的なＡＶを追跡し、クライアント１０５がリプレイを検出するのを補助するために用いることができる。ＡＫ匿名鍵は、

【００１４】

【数１】

$$f5_k$$

を用いて発生されるオプションのパラメータである。以降では、ＡＫが用いられておらず、したがって

【００１５】

【数２】

$f5_k=0$

であるものとする。またＭＡＣの計算には、認証管理フィールド（ａｕｔｈｅｎｔｉｃａｔｉｏｎ　ｍａｎａｇｅｍｅｎｔ　ｆｉｅｌｄ：ＡＭＦ）が関連する。当業者には容易に理解されるように通常はＡＭＦは、タイムアウト値などの技術的パラメータを選択するために用いられる。ＳＱＮ、ＲＡＮＤ、ＡＭＦを所与としてＭＡＣは、関数

【００１６】

【数３】

$f1_k$

を通して導出され、ただし

【００１７】

【数４】

$$MAC = f1_k(SQN \| RAND \| AMF)$$

である。

【００１８】

【数５】

$f1_k$

のｋは、共有秘密鍵（ＰＳＫ）であることに留意されたい。

【００１９】

さらにＸＲＥＳは、

【００２０】

【数６】

$f2_k$

を用いて導出することができ、ただし

【００２１】

【数７】

$$XRES = f2_k(RAND)$$

である。ＣＫは、

【００２２】

【数８】

$f3_k$

を用いて導出することができ、ただし

【００２３】

【数９】

$$CK = f3_k(RAND)$$

である。ＩＫは、

【００２４】

【数１０】

$f4_k$

を用いて導出することができ、ただし

【００２５】

【数１１】

$$IK = f4_k(RAND)$$

である。オプションのＡＫは、

【００２６】

【数１２】

$$f5_k$$

を用いて導出することができ、ただし

【００２７】

【数１３】

$$AK = f5_k(RAND)$$

である。および、

【００２８】

【数１４】

$$AUTN = SQN \oplus AK \,||\, AMF \,||\, MAC$$

である。ＡＶは、ＲＡＮＤ、ＸＲＥＳ、ＣＫ、ＩＫ、およびＡＵＴＮの連接として構成され、したがって、ＡＶ＝ＲＡＮＤ｜｜ＸＲＥＳ｜｜ＣＫ｜｜ＩＫ｜｜ＡＵＴＮである。鍵サーバ１１５で関連する計算を示すものとして図２Ａを参照されたい。ＡＶ１２５は、鍵サーバ１１５からサービングネットワーク１１０に通信される。ＡＶ１２５を受け取るとすぐにサービングネットワークは、ＣＫおよびＩＫを記憶し、認証要求１３０をクライアント１０５に通信することができる。認証要求１３０は、ＲＡＮＤと、鍵サーバ１１５によって計算されたＡＵＴＮとを含むことができる。

【００２９】

認証要求１３０を受け取るとすぐにクライアントは、ＩＫおよびＣＫの導出を試みることができる。クライアント１０５は、認証要求１３０にてＲＡＮＤおよびＡＵＴＮを受け取っている。この例では０のＡＫが用いられているので、ＡＵＴＮ＝ＳＱＮ｜｜ＡＭＦ｜｜ＭＡＣである。クライアント１０５は、ＡＶを導出するのに用いられた共有秘密鍵（ｋ）を有するように構成されるので、図２Ｂに示されるようにクライアント１０５は、応答（ｒｅｓｐｏｎｓｅ：ＲＥＳ）、ＣＫ、ＩＫ、および期待されるＭＡＣ（ＸＭＡＣ）を導出することができる。クライアント１０５は、ＳＱＮの有効性をチェックし、ＭＡＣがＸＭＡＣに等しいことを検証する。チェックが合格した場合は、クライアントはＡＫＡが成功したと見なし、クライアントは導出したＣＫおよびＩＫをサービングネットワーク１１０との安全な通信に用いる。クライアント１０５はさらに、呼掛けに対する応答ＲＥＳを計算し、サービングネットワーク１１０に送る。サービングネットワーク１１０は、ＲＥＳ＝ＸＲＥＳであることを検証し、そうであればＡＫＡが成功したと見なし、ＣＫおよびＩＫを通信に用いる。これは第３世代パートナーシッププロジェクト（３ｒｄ Ｇｅｎｅｒａｔｉｏｎ Ｐａｒｔｎｅｒｓｈｉｐ Ｐｒｏｊｅｃｔ：３ＧＰＰ）標準に準拠してＡＫＡがどのように動作するかの概観である。

【００３０】

前述したように、ネットワークに接続するために加入者が用いることができるデバイスの数が増えるのに従ってサービス提供者は、加入者のデバイスのそれぞれに対してＵＩＭを発行することを望む場合があり、この場合は各ＵＩＭは同じ共有秘密鍵を有する。３ＧＰＰ標準は、同じ共有秘密鍵を有する複数のＵＩＭを可能にすることを留意されたい。しかし、加入者が複数のデバイスを有し各デバイスが同じ共有秘密鍵を有するそれ自体のＵＩＭを有する環境で、知られている鍵交換プロトコルが用いられる場合は、セキュリティ脆弱性が現れる。このセキュリティ脆弱性を示す２つの攻撃シナリオについて述べる。

【００３１】

第１のシナリオでは、第１のクライアント（Ｃ１）と第２のクライアント（Ｃ２）がサ

ービングネットワークへの接続を試みる。Ｃ１およびＣ２は同じ加入者によって所有されるデバイスであるが、各デバイスはそれ自体のＵＩＭを有することに留意されたい。したがってＣ１はＵＩＭ１を有し、Ｃ２はＵＩＭ２を有することができ、ＵＩＭ１とＵＩＭ２は同じ共有秘密鍵を有する。鍵交換プロトコルの一部としてサービングネットワークは、ＲＡＮＤおよびＡＵＴＮをＣ１に送ることができ、これを敵（Ａ）が漏れ聞く。次いでＣ２は、サービングネットワークとの接続の確立を試みる。しかしＡは、Ｃ２のサービングネットワークとの通信を阻止することができ、漏れ聞いたＲＡＮＤおよびＡＵＴＮをＣ２に繰り返す。Ｃ１およびＣ２は、同じセッション鍵ＣＫおよびＩＫを導出することになる。ここでＣ１とＣ２はサービングネットワークと安全に通信していると考えるが、Ｃ１とＣ２は共に同じセッション鍵を用いて接続される。このシナリオではＡは、Ｃのアカウント上で意図されていないトランザクションを作成することができる。たとえばＣ１によって実行されるトランザクションが、Ｃ１のＵＩＭによって維持されるアカウント上の引き落とし額を伴う場合は、Ａはこのトランザクションをｃ２に対してリプレイすることができる（これは、Ｃ１がＣ２と同じセッション鍵を有するので可能である）。このリプレイは、対応するＣ２のＵＩＭ上の引き落とし額に影響を及ぼし得ることになり、これは明らかに意図されていないトランザクションであり、攻撃の成功である。

【００３２】

第２の攻撃シナリオは、Ａが、共有秘密鍵を含んだＣのデバイスの１つを借用（または捕捉、または遠隔的にセキュリティを侵害する）する場合に生じ得る。秘密鍵は安全にＵＩＭに記憶される。しかしＵＩＭによって生成されるセッション鍵は、Ｃ２の主メモリにエクスポートされる。Ｃ２がセキュリティの侵害を受けたと仮定する。次いでＡは、Ｃ１に向かうＲＡＮＤおよびＡＵＴＮを漏れ聞き、ＲＡＮＤおよびＡＵＴＮをＣ２のＵＩＭに転送する。Ｃ２のＵＩＭは、セッション鍵ＩＫおよびＣＫを発生し、主メモリにセッション鍵を置く。これらは、Ｃ１によって発生された同じセッション鍵であることに留意されたい。ここでＡは、サービングネットワークとＣ１の間に確立された安全なセッションを支配する。

【００３３】

複数ＵＩＭでのＡＫＡを用いた上述の脆弱性を克服する１つの方法は、クライアントにランダム性を発生させて、確立されたセッション鍵に与えることである。これはすでに確立されたＣＫおよびＩＫを中間鍵として用いることによって行うことができ、ＵＩＭによってサンプルされたランダム性に基づいてセッション鍵を導出する。この提案に関連するメッセージフローを図３に示す。

【００３４】

次に図３を参照すると、これは複数ＵＩＭのＡＫＡプロトコルの一実施形態のメッセージフローを示す。メッセージフローにおける主参加者は、クライアント３０５、サービングネットワーク３１０、および鍵サーバ３１５である。クライアント３０５は、移動電話、携帯情報端末、ラップトップ、またはサービングネットワーク３１０へのアクセスを試みることができる任意の他のタイプのデバイスとすることができる。サービングネットワーク３１０は、クライアント３０５がアクセスするネットワークであるが、クライアント３０５のホームネットワークでもよくそうでなくてもよい。鍵サーバ３１５は、クライアント３０５のホームネットワーク内に常駐することができる。

【００３５】

図１と同様に最初にクライアント３０５は、アクセス要求１２０をサービングネットワーク３１０に送ることによってネットワーク３１０との接続の確立を試みる。また図１と同様にサービングネットワーク３１０は、認証データ要求１２２を鍵サーバ３１５に送り、鍵サーバは、複数ＵＩＭ鍵交換のために必要な情報の導出を開始する。ＵＩＭ　ＡＫＡプロトコルとは対照的に鍵サーバは、ＡＶのためのＣＫおよびＩＫを生成せず、その代わりに鍵サーバ３１５は、共有秘密鍵およびＲＡＮＤから派生鍵（ＫＤ）を計算する。図１と同様にクライアント３０５および鍵サーバ３１５は、共有鍵を有するように構成され、クライアント３０５の共有鍵は、鍵サーバ３１５の共有鍵と等しくまたは同じである。Ｃ

ＫおよびＩＫは、ＫＤから導出することができる。したがって鍵サーバ３１５によって生成されるＡＶは、ＲＡＮＤ、ＡＵＴＮ、およびＫＤの連接を含む（すなわち、ＡＶ＝ＲＡＮＤ｜｜ＡＵＴＮ｜｜ＫＤである）。

【００３６】

ＡＶ３１７を生成するために必要な変数の計算には、擬似ランダム関数発生器ｆ１、Ｆ、Ｆ１、およびＦ２が用いられる。先に述べたようにこれらの関数は異なる関数でもよく、ＡＥＳなどの同じ関数でもよい。後者の場合は関数が呼ばれたときに、関数特有の引数が先頭に追加されなければならない。先に述べたように複数ＵＳＩＭ　ＡＫＡでは、鍵サーバ３１５は、セッション鍵ＣＫおよびＩＫをサービングネットワーク３１０に送らない。その代わりに鍵サーバ３１２は、ＫＤをサービングネットワーク３１０に送る。ＫＤは、共有秘密鍵と、鍵サーバ３１５によって発生されたＲＡＮＤとから導出することができ、したがって、ＫＤ＝F_k（ＲＡＮＤ）である。鍵サーバ３１５は、ＡＫＡプロトコルの場合のようにＭＡＣを計算し、したがって

【００３７】

【数１５】

$$MAC = f_{1_k}(SQN \| RAND \| AMF)$$

である。図１に関連して述べたようにＡＭＦは、通常は技術的パラメータを選択するために用いられる。ＸＲＥＳは、サービングネットワーク３１０がＫＤおよびＲＡＮＤＣに基づいてＸＲＥＳを計算することになるので、省略される。鍵サーバ３１５はまた、ＡＫＡプロトコルの場合のようにＡＵＴＮを構成し、したがって、ＡＵＴＮ＝ＳＱＮ｜｜ＡＭＦ｜｜ＭＡＣである。上述のように、ＡＶ＝ＲＡＮＤ｜｜ＡＵＴＮ｜｜ＫＤである。次いで鍵サーバ３１５は、ＡＶ３１７をサービングネットワーク３１０に送出する。ＡＶ３１７を受け取るとすぐにサービングネットワークは、ＡＶ３１７および具体的にはＫＤを記憶することができる。サービングネットワークは、記憶したＫＤに一意のクライアント識別子を関連付けることができ、一意のクライアント識別子は、モバイル識別表示、電子シリアル番号、または別の他の、通信デバイスの一意の識別子とすることができる。

【００３８】

サービングネットワーク３１０は、ＡＵＴＮとＲＡＮＤとを含む認証要求３２０をクライアント３０５に送る。ＡＫＡの場合と同様にクライアント３０５は、ＡＵＴＮを構成するＭＡＣおよびＳＱＮを検証する。すなわちクライアント３０５は、ＭＡＣが期待されるＭＡＣに等しいかどうかを判定することができる。ＭＡＣが検証された場合は、クライアント３０５はＫＤを計算し、ただしＫＤ＝F_k（ＲＡＮＤ）である。次いでクライアントはＲＡＮＤＣを発生し、ＲＥＳ＝F_{KD}（ＲＡＮＤＣ）を計算する。クライアント３０５はまた、ＣＫおよびＩＫを計算することができ、ただし、ＣＫ＝$F1_{KD}$（ＲＡＮＤＣ）、およびＩＫ＝$F2_{KD}$（ＲＡＮＤＣ）である。これらのクライアントの計算は、図４ａに示される。この時点でクライアント３０５は、サービングネットワーク３１０との安全な通信セッションを行うために必要なセッション鍵（ＣＫおよびＩＫ）を有する。クライアント３０５は、認証応答３３０をフォーマットし、サービングネットワーク３１０に通信する。認証応答３３０は、ＲＡＮＤＣおよびＲＥＳを含むことができる。これらのクライアントの計算は、クライアントのＵＩＭ内で行われることに留意されたい。共有秘密鍵および派生鍵は、ＵＩＭから出ることはない。しかしＵＩＭは、ＵＩＭの外部のメモリにセッション鍵（ＣＫおよびＩＫ）をエクスポートすることができ、セッション鍵はクライアントとサービングネットワーク３１０の間の通信を暗号化するのに用いることができる。

【００３９】

認証応答３３０を受け取るとすぐにサービングネットワーク３１０は、ＫＤおよびＲＡＮＤＣから期待応答ＸＲＥＳを計算し、ただしＸＲＥＳ＝F_{KD}（ＲＡＮＤＣ）である。次いでサービングネットワークは、ＸＲＥＳが認証応答３３０のＲＥＳに等しいことを検証する。ＸＲＥＳの検証が成功した場合はサービングネットワーク３１０は、ＫＤを取り

出し、セッション鍵ＣＫおよびＩＫを導出し、ただし、ＣＫ＝Ｆ１$_{KD}$（ＲＡＮＤＣ）、およびＩＫ＝Ｆ２$_{KD}$（ＲＡＮＤＣ）である。ＸＲＥＳ、ＣＫ、およびＩＫの導出は、図４ｂに示される。この時点でサービングネットワーク３１０は、クライアント３０５との安全な通信セッションを行うために用いることができるセッション鍵（ＩＫおよびＣＫ）を有する。

【００４０】

次に図５を参照すると、この図は複数ＵＩＭのＡＫＡプロトコルの方法５００を示すフローチャートである。ステップ５１０では、クライアント、典型的にはＵＩＭを備えた通信デバイスは、サービングネットワークへのアクセスを要求する。図１および図３に関連して述べたようにこれは、クライアントがアクセス要求メッセージをサービングネットワークに通信すること、およびサービングネットワークが認証データ要求を鍵サーバに通信することを引き起こし得る。５２０で鍵サーバはＡＶを発生することによって応答し、ＡＶをサービングネットワークに通信する。ＡＶの構成、およびどのようにＡＶのフィールドが計算されるかについては、図３に関連する説明で開示された。

【００４１】

認証を求めるクライアントの要求に応じて、５３０でサービングネットワークは、認証要求をクライアントに通信する。認証要求は、ＲＡＮＤおよびＡＵＴＮを含むことができる。図３に関連して述べたように５４０でクライアントは、ＭＡＣがＸＭＡＣに等しいことを検証することができる。ＭＡＣがＸＭＡＣに等しくない場合は、５９０で方法は終了する。ＭＡＣがＸＭＡＣに等しい場合は、５５０でクライアントは、複数ＵＳＩＭ　ＡＫＡにおいて必要な他の変数を導出する。ステップ５５０はさらに、クライアントがＲＡＮＤＣを発生し、ＲＥＳ、ＣＫ、およびＩＫを計算することを含むことができる。クライアントがＲＡＮＤＣを発生し、ＲＥＳ、ＣＫ、およびＩＫを計算するやり方は、図３に関連して述べた。

【００４２】

５６０でクライアントは、認証応答をサービングネットワークに通信する。認証応答は、ＲＡＮＤＣおよびＲＥＳを含むことができる。図３に関連して述べたように、５７０でサービングネットワークは、ＸＲＥＳを計算し、ＸＲＥＳがＲＥＳに等しいかどうかを判定することができる。ＲＥＳがＸＲＥＳに等しくない場合は、方法５００は５９０で終了する。ＸＲＥＳがＲＥＳに等しい場合は、５８０で複数ＵＳＩＭ　ＡＫＡのために必要な他の変数が導出される。ステップ５８０ではサービングネットワークは、図３に関連して述べたようにＩＫおよびＣＫを計算する。この時点でサービングネットワークおよびクライアントは、サービングネットワークとクライアントの間の安全な通信に用いることができるＩＫおよびＣＫを有する。

【００４３】

一実施例におけるメッセージフロー５００に関連する装置は、１つまたは複数の電子構成要素、ハードウェア構成要素、およびコンピュータ構成要素などの、複数の構成要素を備える。このような構成要素のいくつかは、装置内で組み合わせるまたは分割することができる。装置の例示の構成要素は、当業者には理解されるように、いくつかのプログラミング言語のいずれかを用いて書かれたまたは実現された１組の、および／または一連のコンピュータ命令を使用かつ／または備える。一実施例での装置は、任意の方向（たとえば水平、斜め、垂直）を有することができ、本明細書での説明および図面は、説明のために装置の１つの例示の方向を示す。

【００４４】

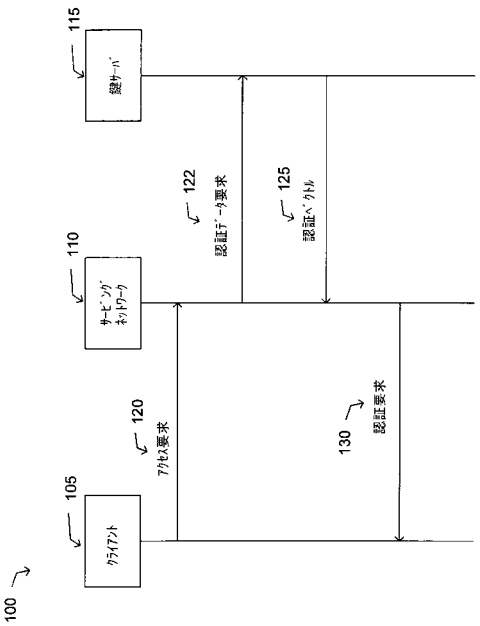
本明細書で述べたステップまたは動作は、例示のためのみである。本発明の趣旨から逸脱せずに、これらのステップまたは動作に多くの変形例が存在し得る。たとえばステップは異なる順序で実行することができ、またはステップは追加、削除、または変更することができる。

【００４５】

本発明の例示の実装形態について本明細書で示し詳細に説明してきたが、当業者には、

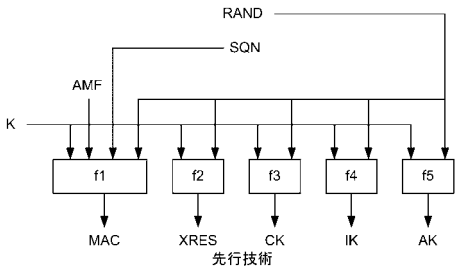
本発明の趣旨から逸脱せずに、様々な変更、追加、置換などを行うことができることが明らかとなり、したがってこれらは添付の特許請求の範囲において定義される本発明の範囲内であると見なされる。

【図１】



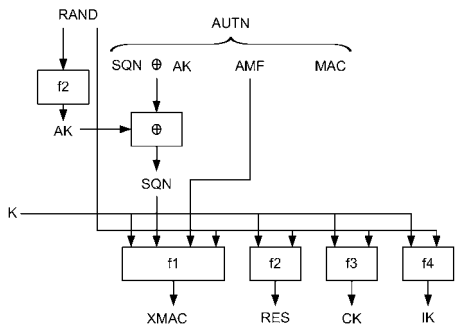
先行技術
FIG. 1

【図２ａ】



先行技術
FIG. 2a

【図２ｂ】



先行技術
FIG. 2b

【図３】

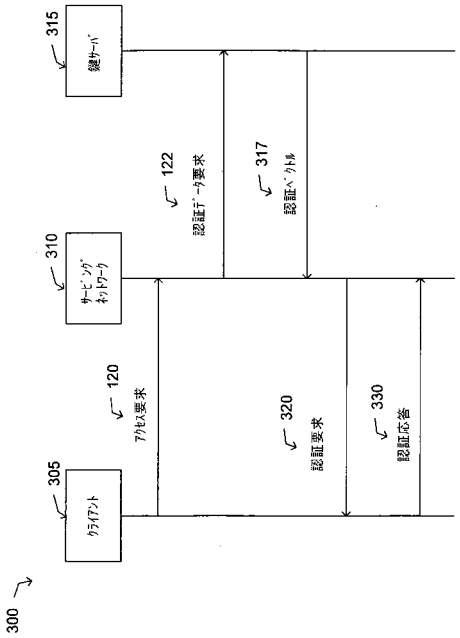


FIG. 3

【図４ａ】

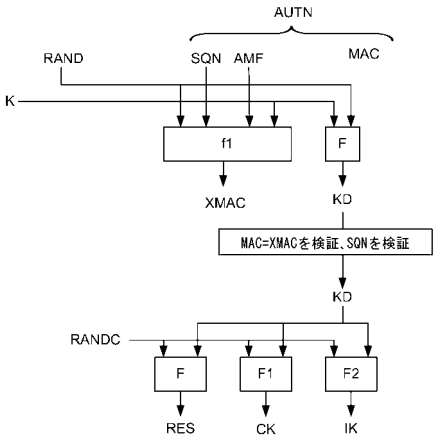


FIG. 4a

【図４ｂ】

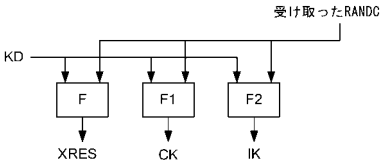


FIG. 4b

【図５】

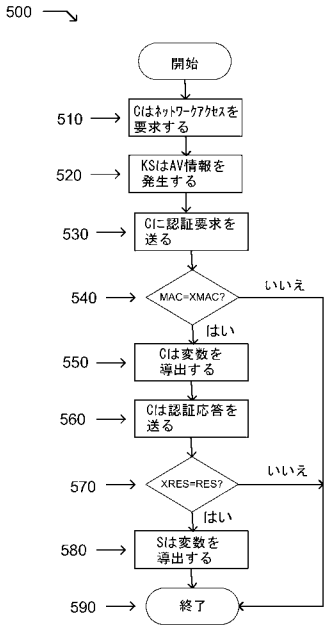


FIG. 5

フロントページの続き

(56)参考文献 特開平０５－３４７６１７（ＪＰ，Ａ）
特開２００３－１４３１２８（ＪＰ，Ａ）
特表２００６－５１８１２１（ＪＰ，Ａ）
特表２００９－５２４３６９（ＪＰ，Ａ）
特表２００７－５１１１７２（ＪＰ，Ａ）
特表２００７－５０８６１４（ＪＰ，Ａ）
特表２００５－５３０４２９（ＪＰ，Ａ）
国際公開第２００９／１４６７２９（WO，Ａ１）
国際公開第２００９／０４８５７４（WO，Ａ１）
国際公開第２００９／０４５２８２（WO，Ａ１）
国際公開第２００９／０２９１６９（WO，Ａ１）
米国特許出願公開第２００９／０１７２３９７（ＵＳ，Ａ１）
Vladimir Kolesnikov, “A Security Enhancement and Proof for Authentication and Key Agreement (AKA)”, Cryptology ePrint Archive: Report 2010/350, [online], ２０１０年 ６月１８日, Version: 20100618:183819, p.1-22, [retrieved on 2013-09-17]. Retrieved from the Internet, ＵＲＬ, <http://eprint.iacr.org/2010/350.pdf>

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ ９／０８
Ｈ０４Ｌ ９／３２
ＪＳＴＰｌｕｓ／ＪＭＥＤＰｌｕｓ／ＪＳＴ７５８０（ＪＤｒｅａｍＩＩＩ）
ＩＥＥＥ Ｘｐｌｏｒｅ