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

特許第4612637号
(P4612637)

(45)発行日　平成23年1月12日(2011.1.12)　(24)登録日　平成22年10月22日(2010.10.22)

(51)Int.Cl.			F I		
H04L	9/32	(2006.01)	H04L	9/00	675A
G09C	1/00	(2006.01)	G09C	1/00	640E

請求項の数 14　(全 12 頁)

(21)出願番号	特願2006-538857 (P2006-538857)
(86)(22)出願日	平成16年11月10日 (2004.11.10)
(65)公表番号	特表2007-511151 (P2007-511151A)
(43)公表日	平成19年4月26日 (2007.4.26)
(86)国際出願番号	PCT/EP2004/052909
(87)国際公開番号	WO2005/046157
(87)国際公開日	平成17年5月19日 (2005.5.19)
審査請求日	平成18年5月9日 (2006.5.9)
(31)優先権主張番号	10352538.6
(32)優先日	平成15年11月11日 (2003.11.11)
(33)優先権主張国	ドイツ(DE)
(31)優先権主張番号	10358987.2
(32)優先日	平成15年12月16日 (2003.12.16)
(33)優先権主張国	ドイツ(DE)

前置審査

(73)特許権者　390039413
シーメンス　アクチエンゲゼルシヤフト
Ｓｉｅｍｅｎｓ　Ａｋｔｉｅｎｇｅｓｅｌｌｓｃｈａｆｔ
ドイツ連邦共和国　Ｄ－８０３３３　ミュンヘン　ヴィッテルスバッハープラッツ　２
Ｗｉｔｔｅｌｓｂａｃｈｅｒｐｌａｔｚ　２，　Ｄ－８０３３３　Ｍｕｅｎｃｈｅｎ，　Ｇｅｒｍａｎｙ
(74)代理人　100061815
弁理士　矢野　敏雄
(74)代理人　100094798
弁理士　山崎　利臣

最終頁に続く

(54)【発明の名称】第１の端末機器および第１のネットワークと第２の端末機器および第２のネットワークとの間でデータトラフィックを保護する方法

(57)【特許請求の範囲】

【請求項１】

第１の端末機器（１）および第１のネットワーク（２）と第２の端末機器（４）および第２のネットワーク（６）との間でデータトラフィックを保護する方法であって、

該第１の端末機器（１）は、１つまたは複数の第１のセッション鍵を使用して第１のネットワーク（２）において通信し、

該第２の端末機器（４）は、１つまたは複数の別の第２のセッション鍵を使用して第２のネットワーク（６）において通信する形式の方法において、

・該第１の端末機器（１）と第２の端末機器（４）とを、ローカルなインタフェース（３）を介して接続するステップと、

・該第１の端末機器（１）において１つまたは複数の第１のセッション鍵を求め、該１つまたは複数の第１のセッション鍵から、１つまたは複数の別の第２のセッション鍵を導出するステップと、

・前記ローカルなインタフェース（３）を介して保護プロトコルを使用して、該１つまたは複数の別の第２のセッション鍵を第２の端末機器（４）へ伝送するステップと、

・該１つまたは複数の別の第２のセッション鍵および／または該１つまたは複数の別の第２のセッション鍵から導出された鍵を使用して、認証プロトコルを介して、該第２の端末機器（４）を該第２のネットワーク（６）において認証するステップ

とを有することを特徴とする方法。

【請求項２】

認証プロトコルの一部として、前記１つまたは複数の第１のセッション鍵から導出される鍵を生成し、該鍵を使用して、第２のネットワークにおいて認証プロトコルのメッセージの保護および／または通信の保護を行う、請求項１記載の方法。

【請求項３】

第１のネットワーク（２）はＧＳＭネットワークであり、

１つまたは複数の第１のセッション鍵を、該第１の端末機器（１）上のＳＩＭ（ＳＩＭ＝Subscriber Identity Module）で生成する、請求項１または２記載の方法。

【請求項４】

認証プロトコルは、ＥＡＰ‐ＳＩＭ（ＥＡＰ＝Extensible Authentication Protocol; ＳＩＭ＝Subscriber Identity Module）である、請求項３記載の方法。

【請求項５】

第１のネットワーク（１）はＵＭＴＳネットワークであり、

１つまたは複数の第１のセッション鍵を、第１の端末機器（１）上のＵＳＩＭ（ＵＳＩＭ＝Universal Subscriber Identity Module）で生成する、請求項１または２記載の方法。

【請求項６】

認証プロトコルはＥＡＰ‐ＡＫＡ（ＥＡＰ＝Extensible Authentication Protocol; ＡＫＡ＝Authentication Key Agreement）である、請求項５記載の方法。

【請求項７】

ローカルなインタフェース（３）は無線インタフェースであり、たとえばブルートゥースインタフェースおよび／または赤外線インタフェースである、請求項１から６までのいずれか１項記載の方法。

【請求項８】

第２のネットワーク（６）の一部は、ローカルなネットワークであり、たとえばＬＡＮネットワークおよび／またはＷＬＡＮネットワークである、請求項１から７までのいずれか１項記載の方法。

【請求項９】

保護プロトコルは、

・第１の指示メッセージが第２の端末機器（４）から第１の端末機器（１）へ送信され、第１の端末機器（１）において該第１の指示メッセージによって、第１のセッション鍵から前記１つまたは複数の別の第２のセッション鍵の導出が開始され、

・該第１の指示メッセージに対する応答で、第２の指示メッセージが第１の端末機器（１）から第２の端末機器（４）へ送信され、該第２の指示メッセージによって前記１つまたは複数の別の第２のセッション鍵が伝送される

ように構成されている、請求項１から８までのいずれか１項記載の方法。

【請求項１０】

第１の指示メッセージによって、認証プロトコルからのパラメータを伝送する、請求項１から９までのいずれか１項記載の方法。

【請求項１１】

保護プロトコルは、前記第１の指示メッセージおよび第２の指示メッセージを含む拡張されたブルートゥースＳＩＭアクセスプロフィールプロトコルである、請求項９または１０記載の方法。

【請求項１２】

端末機器において、

請求項１から１１までのいずれか１項記載の方法において第１の端末機器（１）として使用可能であるように構成されていることを特徴とする端末機器。

【請求項１３】

１つまたは複数のセッション鍵を求めるための手段と、１つまたは複数の別の第２のセッション鍵を該第１のセッション鍵から導出するための手段とを有する、請求項１２記載の端末機器。

【請求項１４】
端末機器において、
請求項１から１１までのいずれか１項記載の方法において第２の端末機器として使用可能であるように構成されていることを特徴とする端末機器。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、第１の端末機器および第１のネットワークと第２の端末機器および第２のネットワークとの間でデータトラフィックを保護する方法に関する。さらに本発明は、本発明による方法を実施するために構成された相応の第１の端末機器および相応の第２の端末機器に関する。
【０００２】
現在、移動電話機のユーザに対して、適切なアクセスネットワークを介して移動無線網にアクセスするだけでなく、たとえばインターネット等の別のネットワークにアクセスできるようにする必要性が生じている。インターネットにアクセスする際にはとりわけ、伝送されるデータが移動電話機に表示されるだけでなく、たとえばラップトップ等の別の端末機器でも表示されるのが望ましい。
【０００３】
従来技術から次のような方法が公知になっている。すなわち、移動電話機の形態である第１の端末機器がＳＩＭモジュールまたはＵＳＩＭモジュール（ＳＩＭ＝Subscriber Identity Module；ＵＳＩＭ＝Universal Subscriber Identity Module）を有し、ローカルのインタフェースを介してラップトップの形態の第２の端末機器と接続する方法が公知になっている。ここではラップトップは、たとえばＷＬＡＮネットワークおよび／またはインターネット等の別のネットワークにアクセスすることができる。ここで第２の端末機器は、認証プロトコルを介して別のネットワークで認証される。この認証プロトコルでは、ＳＩＭモジュールないしはＵＳＩＭモジュールに由来する鍵が使用される。適切な認証プロトコルとして、たとえばＥＡＰ‐ＳＩＭ（ＥＡＰ＝Extensible Authentication Protocol；ＳＩＭ＝Subscriber Identity Module；文献［１］参照）またはＥＡＰ‐ＡＫＡ（ＥＡＰ＝Extensible Authentication Protocol；ＡＫＡ＝Authentication Key Agreement；文献［２］参照）というプロトコルが使用される。ＥＡＰ‐ＳＩＭプロトコルはＧＳＭ移動電話において使用され、ＥＡＰ‐ＡＫＡプロトコルはＵＭＴＳ移動電話に使用される。
【０００４】
認証プロトコルＥＡＰ‐ＳＩＭおよびＥＡＰ‐ＡＫＡでは、ネットワークとの通信接続が必要とされ、認証時にはＳＩＭモジュールまたはＵＳＩＭモジュールの関与が必要とされる。したがって、第２の端末機器も第１の端末機器も、認証プロトコルの実行に関与する。それゆえ、第２の端末機器と第１の端末機器との間で、たとえばブルートゥースインタフェース等のローカルなインタフェースを介してデータ交換を行う必要がある。その際には認証を行うために、インタフェースを介して適切なプロフィールによって、認証データが伝送される。従来技術からは、適切なプロフィールとしてとりわけブルートゥースプロフィールが公知となっている。これはたとえば、ブルートゥースＳＩＭアクセスプロフィール（文献［３］参照）である。ローカルなインタフェースを介して、第１のセッション鍵が伝送される。この第１のセッション鍵は本来、移動電話機と相応の移動無線網との通信を行うために使用されるものである。この第１のセッション鍵から、第２の端末機器で新たなセッション鍵が計算される。このセッション鍵によって、認証が認証プロトコルを介して実行される。ここで、第１のセッション鍵が第２の端末機器において既知であることが問題的であると判明している。それゆえ、攻撃者が第２の端末機器に対して管理権を取得すると、第１のセッション鍵にもアクセスすることができ、第１の端末機器のユーザのふりをして、本来のユーザの負担で第１のネットワークで通話を行うことができる。
【０００５】
したがって本発明の課題は、第１の端末機器および第１のネットワークと第２の端末機

器および第２のネットワークとの間でデータトラフィックを保護する方法において、高くなった保護要件を満たす方法を提供することである。とりわけ本方法では、上記の攻撃から保護を行わなければならない。

【０００６】

前記課題は独立請求項によって解決される。本発明の発展形態が、従属請求項に記載されている。

【０００７】

本発明による方法では、１つまたは複数のセッション鍵を使用して第１のネットワークで通信するように構成された第１の端末機器と、１つまたは複数のセッション鍵を使用して第２のネットワークで通信するように構成された第２の端末機器とが使用される。本方法では、第１の端末機器は第２の端末機器と、ローカルなインタフェースを介して接続されている。第１の端末機器で第１のセッション鍵を検出し、第２のセッション鍵を第１のセッション鍵から導出する。第２のセッション鍵は、ローカルなネットワークを介して保護プロトコルを使用して、第２の端末機器へ伝送される。最後に第２の端末機器は、第２のセッション鍵および／または第２のセッション鍵から導出された鍵を使用して、認証プロトコルを介して第２のネットワークで認証される。本発明による方法の基礎となっている思想は、第２の端末機器に第１のセッション鍵が供給されないことである。したがって、本来は第２の端末機器によって実施される機能が、第１の端末機器に移される。とりわけ、第１の端末機器ですでに、第２のセッション鍵が第１のセッション鍵から導出される。それゆえ、第２の端末機器に対して管理権を取得した攻撃者は、第１のセッション鍵にアクセスできなくなり、第１のネットワークにアクセスすることはできない。

【０００８】

有利な変形形態では認証プロトコルは、該認証プロトコルの一部として、第２のセッション鍵から導出される鍵が生成され、これを使用して第２のネットワークにおいて認証プロトコルのメッセージの保護および／または通信の保護が行われるように構成されている。

【０００９】

１つの実施形態では、第１のネットワークはＧＳＭネットワークであり、第１のセッション鍵は第１の端末機器上のＳＩＭモジュールで生成される。この場合、認証プロトコルは有利にはＥＡＰ‐ＳＩＭプロトコル（ＥＡＰ＝Extensible Authentication Protocol；ＳＩＭ＝Subscriber Identity Module）である。択一的な実施形態では、第１のネットワークはＵＭＴＳネットワークであり、第１のセッション鍵は第１の端末機器上のＵＳＩＭモジュール（ＵＳＩＭ＝Universal Subscriber Identity Module）で生成される。この場合、認証プロトコルは有利にはＥＡＰ‐ＡＫＡ（ＥＡＰ＝Extensible Authentication Protocol；ＡＫＡ＝Authentication Key Agreement）である。

【００１０】

第１の端末機器と第２の端末機器との間のローカルなインタフェースは、有利には無線インタフェースを介して実現される。ここではとりわけ、ブルートゥースインタフェースおよび／または赤外線インタフェースが考えられる。

【００１１】

本発明による方法において第２の端末機器と通信する第２のネットワークは、有利にはローカルなネットワークであり、とりわけＬＡＮネットワークおよび／またはＷＬＡＮネットワークである。このローカルなネットワークは、たとえばインターネット等の別のネットワークに接続することもできる。

【００１２】

本発明の別の有利な変形形態では、情報を第１の端末機器と第２の端末機器との間で交換するために使用される保護プロトコルは、以下のように構成されている：

・第２の端末機器からの第１の指示メッセージが第１の端末機器へ送信され、第１の指示メッセージにより、第１の端末機器において第１のセッション鍵から第２のセッション鍵の導出が開始される。

【００１３】
・第１の指示メッセージに対する応答で、第２の指示メッセージが第１の端末機器から第２の端末機器へ送信される。この第２の指示メッセージによって、第２のセッション鍵が転送される。
【００１４】
このような構成によって、第２のセッション鍵が第１の端末機器から第２の端末機器へ簡単に転送される。有利な変形形態では、ここで第１の指示メッセージによって、認証プロトコルからのパラメータが伝送される。有利にはこの保護プロトコルは、拡張されたブルートゥースＳＩＭアクセスプロフィールプロトコルであり、これは第１の指示メッセージおよび第２の指示メッセージを含む。本明細書では、このような拡張されたプロトコルに関する詳細な仕様および要件を特定する。
【００１５】
本発明によるデータトラフィック保護方法の他に、本発明はさらに、本発明によるデータトラフィック保護方法において第１の端末機器として使用可能に構成された端末機器も含む。この端末機器は有利には、第１のセッション鍵を求めるための手段と、該第１のセッション鍵から第２のセッション鍵を導出するための手段とを有する。
【００１６】
さらに本発明は、本発明によるデータトラフィック保護方法において第２の端末機器として使用可能に構成された端末機器も含む。
【００１７】
本発明の実施例を以下で、添付図面に基づいて詳述する。
【００１８】
図面
図１　本発明によるデータトラフィック保護方法が適用されるシナリオの一例を示している。
【００１９】
図１に、移動電話機の形態の第１の端末機器１が示されている。この端末機器１は、ローカルのブルートゥースインタフェース３を介して、ラップトップ４の形態の第２の端末機器４に接続されている。この第２の端末機器４はまた、別の無線インタフェース５を介して、第２のネットワーク６にも接続されている。このネットワーク６は、図１ではＷＬＡＮネットワークである。ＷＬＡＮネットワークで認証を行うためには、ラップトップ４とネットワーク６との間で認証プロトコルが実行される。ＷＬＡＮネットワーク６は別のネットワーク７にも接続されており、このネットワーク７は、たとえばインターネットである。移動電話機１は、エアインタフェースを介して移動無線網２にも接続されている。この移動無線網２は、たとえばＧＳＭネットワークまたはＵＭＴＳネットワークである。移動電話機は移動無線網において、識別モジュールを介して識別される。この識別モジュールは、ＧＳＭの場合にはＳＩＭモジュールであり、ＵＭＴＳの場合にはＵＳＩＭモジュールである。移動電話機と移動無線網との通信を行うために、１つまたは複数の第１のセッション鍵が使用される。このセッション鍵は、移動電話機の識別モジュールで生成される。同様に、ラップトップ４とＷＬＡＮネットワーク６との間で通信を行うために、１つまたは複数の第２のセッション鍵が使用される。
【００２０】
図１のシナリオでは、移動電話機のユーザがラップトップ４を介して、該移動電話機の識別モジュールで生成された第１のセッション鍵を使用して、ＷＬＡＮネットワークにおいて認証されるようにしなければならない。こうするために第２のセッション鍵は、第１のセッション鍵から導出される。ここで、第１のセッション鍵がブルートゥースインタフェース３を介してラップトップ４へ伝送され該ラップトップで取り出される場合、攻撃者がラップトップ４に対して管理権を有する攻撃が問題になる。この場合、攻撃者は第１のセッション鍵に関する知識を得て、移動無線網２においてユーザのふりをすることができるようになる。このような攻撃を回避するため、本発明によるデータ保護方法では、第２

のセッション鍵をラップトップ４で導出するのではなく、移動電話機１においてすでに、第１のセッション鍵から導出する。導出された第２のセッション鍵はその後、ブルートゥースインタフェース３を介して保護プロトコルを使用して、ラップトップへ転送される。ラップトップは、この第２のセッション鍵または第２のセッション鍵から導出された別の鍵を使用して、ＷＬＡＮネットワークにおいて認証プロトコルを使用して認証を行う。このようにして、第１のセッション鍵はラップトップに記憶されなくなるので、ラップトップの管理権を有する攻撃者が、第１のセッション鍵を使用して移動無線接続を確立する可能性はない。

【００２１】

以下で本発明を、２つの実施例に基づいて詳細に説明する。第１の実施例では、ＳＩＭモジュールを有するＧＳＭ移動電話機を第１の端末機器とし、第２の実施例では、ＵＳＩＭモジュールを有するＵＭＴＳ移動電話機を第１の端末機器とする。

【００２２】

第１の実施例では、ＷＬＡＮネットワークにおいて認証を行うための認証プロトコルとして、従来技術から公知のＥＡＰ‐ＳＩＭプロトコル（文献［１］参照）が使用される。ここでは、移動電話機のＳＩＭモジュールはいわゆる「全認証（Full Authentication）」（文献［１］第３パラグラフを参照されたい）にのみ関与し、いわゆる「再認証（Re-Authentication）」（文献［１］第４．３パラグラフを参照されたい）には関与しないことが前提とされる。認証プロセスの詳細なメッセージフローは、文献［１］の第３パラグラフ（とりわけ図１を参照されたい）に記載されている。認証時には、以下のステップが実施される。

【００２３】

移動電話機１はラップトップ４から、プロトコル識別子（ＥＡＰ‐ＳＩＭ）と、２つまたは３つのＧＳＭチャレンジＲＡＮＤと、パラメータ "Identity"、"NONCE_MT"、"Version List" および "Selected Version" とを受信する。パラメータ "Identity"、"NONCE_MT"、"Version List" および "Selected Version" は、文献［１］に詳述されている。移動電話機１は連続して、受信された各ＲＡＮＤを所属のＳＩＭモジュールへ伝送する。次のＲＡＮＤは、ＳＩＭモジュールによって先行するＲＡＮＤに対して応答が完了された際に初めて、ＳＩＭモジュールへ伝送される。

【００２４】

ＳＩＭモジュール上では、各ＲＡＮＤごとに次の機能が実行される：

文献［４］に記載されているような、ＧＳＭアルゴリズムＡ３／Ａ８の実行、すなわち、レスポンスＳＲＥＳおよびＧＳＭセッション鍵Ｋｃの導出。パラメータＳＲＥＳおよびＫｃは、ＳＩＭによって移動電話機へ伝送される。このようにして移動電話機は、ＳＩＭとの通信の終了後には、受信されたＲＡＮＤの数に応じて、２つまたは３つのレスポンスＳＲＥＳと２つまたは３つのセッション鍵Ｋｃとを有する。セッション鍵Ｋｃは、請求項の記載によれば第１のセッション鍵である。

【００２５】

これに基づいて移動電話機は、文献［１］の第４．６パラグラフに記載されたようなＥＡＰ‐ＳＩＭマスタキーＭＫを、以下の数式にしたがって算出する（ここでＭＫは、請求項よれば第２のセッション鍵である）：

MK = SHA1 (Identity|n*Kc| NONCE_MT| Version List| Selected Version)

その後、移動電話機はＭＫおよびレスポンスＳＲＥＳをラップトップへ送信する。

【００２６】

上記の式において、「｜」は結合を意味する。Identityは、最後にゼロシンボルを有さないストリングのピア識別子を意味する。これはここでは、最後のＥＡＰ‐レスポンス／ＳＩＭ／スタート‐パケットのAT_IDENTITY属性の識別子であるか、またはAT_IDENTITYが使用されなかった場合には、ＥＡＰ‐レスポンス／識別子‐パケットの識別子である。この識別子ストリングは変更なしで使用され、可能な識別子修飾部（Dekoration）を有する。n*KC という表記は、結合されたｎ個のＫｃ値を示す。Ｋｃ鍵は、ＡＴ＿ＲＡＮＤ属性

においてＲＡＮＤチャレンジと同じ順序で使用される。NONCE_MT は、ＮＯＮＣＥ＿ＭＴ値（ＡＴ＿ＮＯＮＣＥ＿ＭＴ属性ではなく、ＮＯＮＣＥ値のみである）を示す。"Version List" は、AT_VERSION_LISTの２バイトのバージョン番号を含む。しかもこのバージョン番号は、属性と同じ順序になっている。"Selected Version" は、AT_SELECTED_VERSIONの２バイトのバージョンである。ネットワークのバイトのオーダは、属性と同じように使用される。ハッシュ関数ＳＨＡ－１は、文献［５］において詳述されている。複数のＥＰＡ／ＳＩＭ／スタート－ループがＥＡＰ／ＳＩＭ交換で使用される場合、パラメータNONCE_MT、"Version List" および "Selected Version" は最後のＥＡＰ／ＳＩＭ／スタート－ループによって使用され、先行のＥＡＰ／ＳＩＭ／スタート－ループは無視される。

【００２７】

ここでラップトップは、ＭＫ、とりわけいわゆる「セッションキー（session key）」から、別のすべての鍵を算出する。ラップトップはまた、文献［１］の第３パラグラフの図１に示されたテスト "verifies AT_MAC" を実行する。ラップトップがセッション鍵Ｋｃを推定できるようになるのを阻止するためには、セッション鍵ＫｃからＭＫを計算するための鍵導出で十分である。

【００２８】

移動電話機１においてマスタキーを計算するために必要とされるパラメータを伝送するためには、拡張されたブルートゥースＳＩＭアクセスプロフィールが使用される。ここでは、既存のＳＩＭアクセスプロフィールで使用されるメッセージ "TRANSFER_APDU_REQ" が、パラメータ "AuthProt"、"EAP-Id"、"NONCE_MT"、"Version List" および "Selected Version" によって拡張される。ＥＡＰ－Ｉｄの伝送は、移動電話機がＥＡＰ－Ｉｄを固有のデータから導出できる場合には、オプションである。さらに、２つまたは３つのＧＳＭチャレンジＲＡＮＤが伝送される。このＧＳＭチャレンジの伝送は、文献［３］ですでに考察されている。

【００２９】

以下で、拡張されたブルートゥースＳＩＭアクセスプロフィールにおいて使用されるパラメータを詳細に記述する。

【００３０】

パラメータ：AuthProt

このパラメータは、使用される認証プロトコルを示す。

長さ：１バイト

パラメータＩＤ：ブルートゥーススペシャルインタレストグループ（ＳＩＧ）によって定義される（本発明では重要でない）

パラメータ値：ＥＡＰ－ＳＩＭ値＝0x01

パラメータ：ＥＡＰ－Ｉｄ

このパラメータは、マスタキーの導出で使用されるユーザのＥＡＰ識別子（文献［１］の第４．６パラグラフに記載されているような、永続的な識別子または仮の識別子）を含む。

長さ：可変

パラメータＩＤ：ブルートゥーススペシャルインタレストグループ（ＳＩＧ）によって定義される（本発明では重要でない）

パラメータ値：ＥＡＰ識別子の適切な符号化（符号化は本発明では重要でない）

パラメータ："NONCE_MT"

このパラメータは、マスタキーの導出で使用されるＥＡＰピアのＮＯＮＣＥ＿ＭＴ値を含む（文献［１］第４．６パラグラフに記載されたようなもの）。

長さ：１６バイト

パラメータＩＤ：ブルートゥーススペシャルインタレストグループ（ＳＩＧ）によって定義される（本発明では重要でない）

パラメータ値：ＮＯＮＣＥ＿ＭＴ値の適切な符号化（符号化は本発明では重要でない）

パラメータ："Version List"

このパラメータは、マスタキーの導出で使用されるバージョンリスト（文献［１］第４．６パラグラフに記載されたようなもの）を含む。
長さ：２バイト
パラメータＩＤ：ブルートゥーススペシャルインタレストグループ（ＳＩＧ）によって定義される（本発明では重要でない）
パラメータ値：バージョンリストの適切な符号化（符号化は本発明では重要でない）
パラメータ："Selected Version"
このパラメータは、マスタキーの導出で使用されるＥＡＰピアの選択されたバージョンを含む（文献［１］第４．６パラグラフに記載されたようなもの）。
長さ：２バイト
パラメータＩＤ：ブルートゥーススペシャルインタレストグループ（ＳＩＧ）によって定義される（本発明では重要でない）
パラメータ値：選択されたバージョンの適切な符号化（符号化は本発明では重要でない）
メッセージ "TRANSFER_APDU_RESP" は、ＳＩＭアクセスプロフィールの現在の仕様に含まれている（文献［３］第５．２パラグラフを参照されたい）。このメッセージは、パラメータ "MK" によって拡張される。さらに、２つまたは３つのＧＳＭレスポンスＳＲＥＳが伝送される。このＧＳＭレスポンスの伝送は、文献［３］ですでに考察されている。

【００３１】

パラメータ：ＭＫ
このパラメータは、文献［１］第４．６パラグラフに記載のように移動電話機で算出されたマスタキーを含む。
長さ：２０バイト
パラメータＩＤ：ブルートゥーススペシャルインタレストグループ（ＳＩＧ）によって定義される（本発明では重要でない）
パラメータ値：マスタキーＭＫの適切な符号化（符号化は本発明では重要でない）
ＵＭＴＳ移動電話機が使用される場合、ＷＬＡＮネットワーク６において認証を行うための認証プロトコルとして、従来技術から公知のＥＡＰ‐ＡＫＡプロトコルが使用される（文献［２］を参照されたい）。この認証はここでは、文献［２］第３パラグラフ（ここでは、とりわけ図を参照されたい）に記載のように行われる。ここでは、ＵＳＩＭモジュールおよび移動電話機は「全認証（Full Authentication）」（文献［２］第３パラグラフを参照されたい）にのみ関与し、「再認証（Re-Authentication）」（文献［２］第３パラグラフを参照されたい）には関与しないことが前提とされる。この移動電話機は、以下のような機能を実行する。以下のパラメータは、文献［２］に詳細に記載されている。

【００３２】

移動電話機はラップトップから、プロトコル識別子（ＥＡＰ‐ＡＫＡ）と、ＡＫＡチャレンジ RAND|AUTNと、パラメータ "Identity" とを受け取り、ＲＡＮＤおよびＡＵＴＮをＵＳＩＭモジュールへ伝送する。パラメータ "Identity" はここでは、ユーザによってＥＡＰにおいて使用される識別子を示す。この識別子は、文献［２］第４．２パラグラフに詳細に記載されている。

【００３３】

ＵＳＩＭ上では、以下の機能が実行される：
文献［６］に記載されているようなＵＭＴＳアルゴリズムのｆ１～ｆ５＊の実行。とりわけ、ＡＵＴＮおよびＭＡＣの確認、ならびにレスポンスＲＥＳおよびＡＫＡセッション鍵ＣＫおよびＩＫの導出。これらの鍵は、請求項の記載によれば第１のセッション鍵である。パラメータＲＥＳ、ＣＫおよびＩＫは、ＵＳＩＭモジュールから移動電話機へ伝送される。

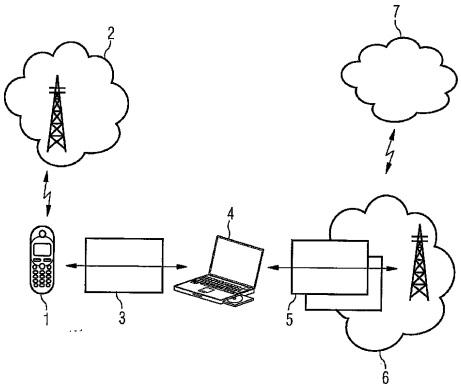
【００３４】

移動電話機はこれに基づいて、文献［２］第４．５パラグラフに記載されたようなＥＡＰ‐ＡＫＡマスタキーＭＫを、以下の数式にしたがって算出する（ＭＫはここでは、請求

項によれば第２のセッション鍵である）：
ＭＫ＝ＳＨＡ１（Identity|IK|CK）
移動電話機はこのＭＫおよびＲＥＳを、ラップトップへ送信する。
【００３５】
上記の数式において、「｜」は結合を意味する。Identityは、最後にゼロシンボルを有さないピア識別子ストリングを表す。この識別子は、最後のＥＡＰ‐レスポンス／ＡＫＡ‐識別子パケットのAT_IDENTITY属性の識別子であるか、または、AT_IDENTITYが使用されなかった場合にはＥＡＰ‐レスポンス／識別子‐パケットの識別子である。この識別子ストリングは変更なしで使用され、可能な識別子修飾部のみを有する。ハッシュ関数ＳＨＡ‐１は、文献［５］に詳述されている。
【００３６】
ラップトップはその後、ＭＫからすべての別の鍵を計算し、とりわけ、文献［２］の第３パラグラフ中の図で言及されている「セッション鍵（session keys）」を計算する。ラップトップがＣＫおよびＩＫを推定するのが可能になるのを阻止するためには、ＭＫをＣＫおよびＩＫから計算するための鍵導出を行うので十分である。
【００３７】
移動電話機においてマスタキーを計算するのに必要とされるパラメータを伝送するためには、ローカルのブルートゥースインタフェースを介してパラメータを伝送するために使用される拡張されたブルートゥースＳＩＭアクセスプロトコルが定義される。以下で、拡張されたブルートゥースＳＩＭアクセスプロフィールで使用されるパラメータを詳細に定義する：
メッセージ "TRANSFER_APDU_REQ" は、ＳＩＭアクセスプロフィールの現在の仕様に含まれている。ここで、文献［３］第５．２パラグラフを参照されたい。このメッセージは、パラメータ "AuthProt" および "EAP-Id" によって拡張される。EAP-Idの伝送は、移動電話機が固有のデータからEAP-Idを導出できる場合には、オプションである。さらに、ＡＫＡチャレンジRAND|AUTNが伝送される。ＡＫＡチャレンジの伝送は、文献［３］ですでに考察されている。
【００３８】
パラメータ：AuthProt
このパラメータは、使用される認証プロトコルを示す。
長さ：１バイト
パラメータＩＤ：ブルートゥーススペシャルインタレストグループ（ＳＩＧ）によって定義される（本発明では重要でない）
パラメータ値：ＥＡＰ‐ＡＫＡ：値＝０ｘ００
パラメータ：EAP-Id
このパラメータは、マスタキーの導出で使用されるユーザのＥＡＰ識別子を含む（文献［２］第４．５パラグラフによれば、持続的な識別子または仮の識別子）。
長さ：可変
パラメータＩＤ：ブルートゥーススペシャルインタレストグループ（ＳＩＧ）によって定義される（本発明では重要でない）
パラメータ値：ＥＡＰ識別子の適切な符号化（符号化はここでは重要でない）
メッセージ "TRANSFER_APDU_RESP" は、ＳＩＭアクセスプロフィールの現在の仕様に含まれている。ここで、文献［３］第５．２パラグラフを参照されたい。このメッセージは、パラメータ "MK" によって拡張される。さらに、ＡＫＡレスポンスＲＥＳが伝送される。このＡＫＡレスポンスの伝送は、文献［３］ですでに考察されている。
【００３９】
パラメータ：MK
このパラメータは、文献［２］第４．５パラグラフの記載にしたがって移動電話機において計算されたマスタキーを含む。
長さ：２０バイト

パラメータＩＤ：ブルートゥーススペシャルインタレストグループ（ＳＩＧ）によって定義される（本発明では重要でない）
パラメータ値：マスタキーＭＫの適切な符号化（符号化は本発明では重要でない）
文献リスト：
［１］H.Haverinen, J.Salowey "EAP SIM Authentication", Internet Draft, draft-haverinen-pppext-eap-sim-12, October 2003;
http://www.ietf.org/internet-drafts/draft-haverinen-pppext-eap-sim-12.txt
［２］J.Arkko, H.Haverinen, "EAP AKA Authentication", Internet Draft, draft-arkko-pppext-eap-aka-11, October 2003;
http://www.ietf.org/internet-drafts/draft-arkko-pppext-eap-aka-11.txt
［３］"SIM access via 'SIM Access Profile' and Bluetooth link", 3GPP meeting SA3#29に対する寄稿, San Francisco, 15.-18. July 2003;
ftp://ftp.3gpp.org/TSG_SA/WG3_Security/TSGS3_29_SanFran/Docs/ZIP/S3-030436.zip; Version 0.95VD_d、付録att2の改訂版
［４］GSM Technical Specification GSM 03.20 (ETSI TS 100 929): "Digital cellular telecommunication system (Phase 2+); Security related network functions", European Telecommunications Standards Institute, July 1999
［５］Federal Information Processing Standard (FIPS) Publication 180-1, "Secure Hash Standard", National Institute of Standards and Technology, U.S. Department of Commerce, April 17, 1995
［６］3GPP Technical Specification 3GPP TS 33.102 V5.3.0: "Technical Specification Group Services and System Aspects; 3G Security; Security Architecture (Release 5)", 3rd Generation Partnership Project, September 2003;
ftp://ftp.3gpp.org/Specs/latest/Rel-5/33_series/
【図面の簡単な説明】
【００４０】
【図１】本発明によるデータトラフィック保護方法が適用されるシナリオの一例を示している。

【図１】



フロントページの続き

(74)代理人 100099483
弁理士 久野 琢也
(74)代理人 100110593
弁理士 杉本 博司
(74)代理人 100128679
弁理士 星 公弘
(74)代理人 100135633
弁理士 二宮 浩康
(74)代理人 100114890
弁理士 アインゼル・フェリックス＝ラインハルト
(72)発明者 ギュンター ホルン
ドイツ連邦共和国 ミュンヘン エドゥアルトーシュミットーシュトラーセ １６

審査官 青木 重徳

(56)参考文献 米国特許出願公開第２００２／０１６９９５８（ＵＳ，Ａ１）
特開平０５－０７５５９８（ＪＰ，Ａ）
特開２００１－００５７８２（ＪＰ，Ａ）
特表２００２－５２８９７８（ＪＰ，Ａ）
H. Haverinen, J. Salowey, “EPA SIM Authentication”, Network Working Group Internet Draft, [online], ２００３年１０月２７日, draft-haverinen-pppext-eap-sim-12.txt, p.1-72, [検索日：平成２１年１０月６日]、インターネット，ＵＲＬ，http://tools.ietf.org/html/draft-haverinen-pppext-eap-sim-12
J. Arkko, H. Haverinen, “EAP AKA Authentication”, Network Working Group Internet Draft, [online], ２００３年１０月２７日, draft-arkko-pppext-eap-aka-11.txt, p.1-61, [検索日：平成２１年１０月６日]、インターネット，ＵＲＬ，http://tools.ietf.org/html/draft-arkko-pppext-eap-aka-11
Yuh-Ren Tsai and Cheng-Ju Chang, “SIM-based Subscriber Authentication for Wireless Local Area Networks”, 37th ANNUAL 2003 International Carnahan Conference on Security Technology, ２００３年１０月, p.468-473, Proceedings THE INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS
Sarvar Patel, “Analysis of EAP-SIM Session Key Agreement”, eap Mailing List, [online], ２００３年　３月２９日, Re:submitting EAP-SIM document, Attachment: AnalyisOfEAP.pdf, [検索日：平成２１年１０月６日]、インターネット，ＵＲＬ，http://lists.frascone.com/pipermail/eap/pdf00006.pdf
Guenter Horn and Bart Praneel, “Authentication and Payment in Future Mobile Systems”, Lecture Notes in Computer Science, １９９８年１０月　５日, Vol.1485, Computer Security - ESORICS 98, p.277-293

(58)調査した分野(Int.Cl., ＤＢ名)
H04L 9/32
G09C 1/00