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

特許第4570626号
(P4570626)

(45)発行日　平成22年10月27日(2010.10.27)　(24)登録日　平成22年8月20日(2010.8.20)

(51)Int.Cl.　F I
H04L 9/08 (2006.01)　H04L 9/00 601B
H04L 9/00 601E

請求項の数 18　(全 11 頁)

(21)出願番号　特願2006-545858 (P2006-545858)
(86)(22)出願日　平成16年11月26日 (2004.11.26)
(65)公表番号　特表2007-521772 (P2007-521772A)
(43)公表日　平成19年8月2日 (2007.8.2)
(86)国際出願番号　PCT/CA2004/002043
(87)国際公開番号　WO2005/107140
(87)国際公開日　平成17年11月10日 (2005.11.10)
審査請求日　平成18年6月30日 (2006.6.30)
(31)優先権主張番号　60/567,611
(32)優先日　平成16年5月3日 (2004.5.3)
(33)優先権主張国　米国(US)

前置審査

(73)特許権者　500043574
リサーチ　イン　モーション　リミテッド
Ｒｅｓｅａｒｃｈ　Ｉｎ　Ｍｏｔｉｏｎ　Ｌｉｍｉｔｅｄ
カナダ国　エヌ２エル　３ダブリュー８　オンタリオ，　ウォータールー，　フィリップ　ストリート　２９５
２９５　Ｐｈｉｌｌｉｐ　Ｓｔｒｅｅｔ，　Ｗａｔｅｒｌｏｏ，　Ｏｎｔａｒｉｏ　Ｎ２Ｌ　３Ｗ８　Ｃａｎａｄａ
(74)代理人　100107489
弁理士　大塩　竹志

最終頁に続く

(54)【発明の名称】再生可能なセッションキーを生成するためのシステムおよび方法

(57)【特許請求の範囲】
【請求項１】
遠隔にある通信機器へセッション中に送信するためにデータ項目内のデータを暗号化するための再生可能な固有のセッションキーを、データ処理機器のプロセッサを用いて生成する方法であって、該プロセッサは、該データ項目が選択されたバッチサイズを超過する場合、該プロセッサに結合された送信器を介して該セッション中に送信される複数のデータバッチへと該データ項目を分離し、該プロセッサは、該複数のデータバッチの各々を同一のセッションキーを用いて暗号化し、
該方法は、
ａ．該プロセッサが、該データ処理機器によってアドレス可能な少なくとも１つのメモリ内に該データ項目を格納するステップと、
ｂ．該複数のデータバッチの各々に対して、該プロセッサが、該データ項目の全体または該データ項目の一部分に対して決定アルゴリズムを反復的に適用することにより、該データ項目に関連する該セッションキーとして使用するための、該データ項目のハッシュを生成するステップと
を包含する、方法。
【請求項２】
前記決定アルゴリズムが、ハッシュアルゴリズムを含む、請求項１に記載の方法。
【請求項３】
前記決定アルゴリズムが、鍵導出関数を含む、請求項１に記載の方法。

【請求項４】
前記ステップａの後に、前記プロセッサが、前記データ項目の前記一部分を追加のデータと連結するさらなるステップを包含し、
前記ステップｂ．において、該プロセッサは、該データ項目および追加のデータの連結された部分を含め、該データ項目の全体または該データ項目の一部分に対して決定アルゴリズムを適用することにより、該データ項目のハッシュを生成する、請求項１に記載の方法。
【請求項５】
前記追加のデータが、前記データ項目外にあるソースからのものである、請求項４に記載の方法。
【請求項６】
ｃ．前記プロセッサが、公開鍵を用いて前記セッションキーを暗号化することにより、暗号化されたセッションキーを生成するさらなるステップを包含する、請求項１に記載の方法。
【請求項７】
遠隔にある通信機器へセッション中に送信するためにデータ項目内のデータを暗号化するための再生可能な固有のセッションキーを生成するシステムであって、該データ項目が選択されたバッチサイズを超過する場合、複数のデータバッチが、該セッション中に送信され、同一のセッションキーを用いて暗号化され、該システムは、該データ項目を格納するための少なくとも１つのメモリと通信するデータ処理機器と、該複数のデータバッチの各々に対して、該データ項目の全体または該データ項目の一部分に対して決定アルゴリズムを反復的に適用することにより、該データ項目に関連する該セッションキーとして使用するための、該データ項目のハッシュを生成するプロセッサとを備える、システム。
【請求項８】
前記決定アルゴリズムが、ハッシュアルゴリズムを含む、請求項７に記載のシステム。
【請求項９】
前記決定アルゴリズムが、鍵導出関数を含む、請求項７に記載のシステム。
【請求項１０】
前記データ項目の前記一部分は、追加のデータと連結され、
前記決定アルゴリズムは、該データ項目および追加のデータの連結された部分を含め、該データ項目の全体または該データ項目の一部分に対して適用されて、該データ項目のハッシュを生成する、請求項７に記載のシステム。
【請求項１１】
前記追加のデータが、前記データ項目外にあるソースからのものである、請求項１０に記載のシステム。
【請求項１２】
前記プロセッサが、さらに、公開鍵を用いて前記セッションキーを暗号化することにより、暗号化されたセッションキーを生成するために用いられる、請求項７に記載のシステム。
【請求項１３】
コンピュータプログラムコードを格納しているコンピュータ使用可能な媒体であって、該コンピュータプログラムコードは、実行されたときに、プロセッサに、
ａ．メッセージデータを暗号化するための再生可能な固有のセッションキーを生成することと、
ｂ．該複数のデータバッチの各々に対して、少なくとも１つのメモリから該データ項目を読み出すことと、
ｃ．該データ項目の全体または該データ項目の一部分に対して決定アルゴリズムを反復的に適用することにより、該データ項目に関連する該セッションキーとして使用するための、該データ項目のハッシュを生成することと
を実行させる、コンピュータ使用可能な媒体。

【請求項１４】
前記コンピュータプログラムコードが前記プロセッサに前記データ項目の全体または該データ項目の前記一部分に適用させる前記決定アルゴリズムが、ハッシュアルゴリズムを含む、請求項１３に記載のコンピュータ使用可能な媒体。
【請求項１５】
前記コンピュータプログラムコードが前記プロセッサに前記データ項目の全体または該データ項目の前記一部分に適用させる前記決定アルゴリズムが、鍵導出関数を含む、請求項１３に記載のコンピュータ使用可能な媒体。
【請求項１６】
前記コンピュータプログラムコードは、前記プロセッサに、前記データ項目の前記一部分を追加のデータと連結させ、該プログラムコードが、該プロセッサに、該データ項目および追加のデータの連結された部分を含め、該データ項目の全体または該データ項目の一部分に該決定アルゴリズムを適用することにより、該データ項目のハッシュを生成させる前に、該連結させることは実行される、請求項１３に記載のコンピュータ使用可能な媒体。
【請求項１７】
前記追加のデータが、前記データ項目外にあるソースからのものである、請求項１６に記載のコンピュータ使用可能な媒体。
【請求項１８】
前記コンピュータプログラムコードは、前記プロセッサに、公開鍵を用いて前記セッションキーを暗号化することにより、暗号化されたセッションキーを生成させる、請求項１３に記載のコンピュータ使用可能な媒体。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、無線通信機器に関する。特に、本発明は、移動体通信機器とネットワークサーバまたはゲートウェイとの間の通信を安全にするためにセッションキーを生成するためのシステムおよび方法に関する。
【背景技術】
【０００２】
Ｅメール、電話、ＳＭＳメッセージング、インターネット、イントラネットベースのアプリケーションのうちの１つ以上を介して通信可能な無線移動体通信機器は、ビジネス上のアプリケーションおよび個人的なアプリケーションにおいて広く利用されている。これらの機器は、自蔵機器、およびポータブルコンピュータに一体化され得る無線モデムを含む。複数のユーザを伴う一般的なビジネス環境において、複数の移動体通信機器がローカルサーバを介して通信している。ローカルサーバは、通信量を管理し、通信信号を遠距離通信のキャリアへリレーする。
【０００３】
このような無線通信システムにおいて、安全性は主要な関心事である。したがって、ローカルサーバは、移動体通信機器へ送信する前に全てのメッセージを暗号化する。移動体通信機器へ送信された、暗号化されたメッセージは、その移動体通信機器内の適切なソフトウェアまたはハードウェアによって復号される。
【０００４】
暗号化プロセスおよび復号プロセスは、一般的に「公開鍵」のインフラストラクチャを用いて動作する。「公開鍵」のインフラストラクチャでは、信用のある第三者が、ユーザによって生成された公開鍵／秘密鍵のペアの信頼性を証明する。公開鍵は、メッセージを暗号化したりデジタル署名を確証したりするために用いられ、秘密鍵は、メッセージを復号したりドキュメントにデジタル署名をしたりするために用いられる。公開鍵と秘密鍵とのこの組み合わせは、一般的に「非対称暗号」として知られており、当業者には既知であるように、効果的にメッセージを暗号化したりデジタル署名を作成したりするために利用

され得る。通信システムの無線コンポーネントはこのように安全にされる。そのため、無線信号が悪意のあるアタッカーによって傍受される場合、その信号を復号することはできない。

【０００５】

移動体通信システムにおいて安全性を最大にするために、ユーザの移動体通信機器がローカルサーバからその移動体通信機器へのメッセージの転送をリクエストする度にセッションキーが生成される。移動体通信機器は、各メッセージ転送セッションの開始において、ローカルサーバと移動体通信機器との間にリンクをもたらすために、「署名のみされている」メッセージを暗号化し得る。このプロセスの一部として、セッションキーが生成され、ユーザの公開鍵を用いて暗号化される。

【０００６】

移動体通信機器内のメモリは貴重であり、時には、メッセージが大きすぎて移動体通信機器へ都合よく全体のメッセージをダウンロードできない。したがって、ローカルサーバは、一般的に、一度につきデータのバッチまたはブロック（たとえば２ＫＢ）を移動体通信機器へ送信する。たとえば一部のメッセージについては、第１のブロックは全体のメッセージを含み、したがって、メッセージの送信が完了するとセッションは終了する。しかし、より大きなメッセージについては、さらなるメッセージデータを求めＭＯＲＥリクエストがローカルサーバへ送信されるまで、メッセージデータの残りが移動体通信機器に秘密にされる。たとえばユーザが、ダウンロード済みのデータブロックの終了に移動体通信機器が近づく点までメッセージをスクロールダウンすると、機器は自動的にＭＯＲＥリクエストをローカルサーバへ送信する。ＭＯＲＥリクエストを受信すると、メッセージ内にある次のデータブロックが移動体通信機器へ送信される。

【０００７】

ＭＯＲＥリクエストが移動体通信機器から受信されるたびに、復号されたメッセージにおけるエラーを防ぐために、ローカルサーバは、先のデータブロックに用いたのと同じセッションキーを用いて次のデータブロックを暗号化する必要がある。しかしながら、セッションキーをローカルサーバ内に保存しておくことは望ましくない。それは、保存することによって追加のメモリが無駄に使用されるためでもあり、ローカルサーバ上に保存されなければならないシークレット情報の量を限定するのが好都合なためでもある。

【０００８】

したがって、安全かつ再生可能なセッションキーを作成する方法、およびこのような方法を利用したシステムが提供されることが好都合といえよう。

【発明の開示】

【課題を解決するための手段】

【０００９】

本発明は、再生可能なセッションキーを生成するためのシステムおよび方法を提供する。

【００１０】

本発明によると、セッションキーはメッセージ自体のハッシュに少なくとも部分的に基づいて生成される。少なくともセッションが完了するまではローカルサーバがメッセージを保存しているため、各ＭＯＲＥリクエストに応答して同一のキーを容易に再生成することができる。

【００１１】

好ましい実施形態において、そのキーが固有のものであることを保証するために、追加データがハッシュに追加される。追加データとは、たとえば、ユーザのＥメールアドレス、ローカルサーバに保存されている一部のランダムバイト、あるいは増加式カウンタである（そのため、たとえば同一のメッセージがユーザへ複数回送信される場合、セッションキーはその都度異なる）。追加データが利用されない場合、セッションキーはメッセージ自体のハッシュにのみ基づいて生成される。

【００１２】

したがって、本発明は、再生可能なセッションキーを生成するためのシステムおよび方法を提供する。さらに、本発明の方法は、保存されている元のメッセージ、公開鍵、およびメッセージのハッシュに基づいてセッションキーを生成するアルゴリズムと共にのみ実施され得る。

【００１３】

したがって、本発明は、遠隔にある通信機器へセッション中に送信するためにデータ項目内のデータを暗号化するための、再生可能なセッションキーを生成する方法であって、データ項目が選択されたバッチサイズを超過する場合、複数のデータバッチがセッション中に送信され、同一のセッションキーを用いて暗号化され、ａ．データ処理機器によってアドレス可能な少なくとも１つのメモリ内に該データ項目を格納する、ステップと、ｂ．該データ項目の全体、あるいはその一部分に対して決定アルゴリズムを適用することによって、該データ項目に関連する固有のセッションキーとして使用するための、該データ項目のハッシュを生成する、ステップとを包含する、方法を提供する。

【００１４】

本発明は、遠隔にある通信機器へセッション中に送信するためにデータ項目内のデータを暗号化するための、再生可能なセッションキーを生成するシステムであって、データ項目が選択されたバッチサイズを超過する場合、複数のデータバッチがセッション中に送信され、同一のセッションキーを用いて暗号化され、システムは、データ項目を格納するための少なくとも１つのメモリと通信する、データ処理機器と、データ項目の全体、あるいはその一部分に対して決定アルゴリズムを適用することによって、データ項目に関連する固有のセッションキーとして使用するための、データ項目のハッシュを生成する、プロセッサとを備える、システムをさらに提供する。

【００１５】

本発明は、コンピュータと共に利用するためのコンピュータプログラム製品であって、コンピュータ使用可能な媒体を備え、コンピュータ使用可能な媒体は、媒体に組み込まれた、メッセージデータを暗号化するための再生可能なセッションキーを再生する、コンピュータ読み取り可能なプログラムコード手段を有し、また、コンピュータプログラム製品は、ａ．少なくとも１つのメモリからデータ項目を読み出すためのコンピュータ読み取り可能なプログラムコード手段と、ｂ．データ項目の全体またはその一部分に対して決定アルゴリズムを適用して、データ項目に関連する固有のセッションキーとして使用すべきデータのハッシュを生成するための、コンピュータ読み取り可能なプログラムコード手段とを備える、コンピュータプログラム製品をさらに提供する。

【００１６】

図は、例として、本発明の好適な実施形態のみを示す。

【発明を実施するための最良の形態】

【００１７】

本発明のシステムおよび方法を、図１に示すハンドヘルド移動体通信機器１０のような遠距離通信機器の関連で、例示のみによって以下に詳細に記載する。このようなハンドヘルド移動体通信機器１０は、当業者にとっては周知である。しかしながら、本発明の原理はその他の無線通信機器に適用され、本システムがそれによって限定されるようには意図されていないという点が認識されよう。また、本発明が、用いられている特定の通信方法（たとえば、Ｅメール、電話、ＳＭＳ、ＭＭＳ等）によって限定されるわけではないという点も認識されよう。

【００１８】

一般に、ハンドヘルド移動体通信機器１０は、ハウジングと、キーボード１４と、出力機器１６とを含む。図示されている出力デバイスはディスプレイ１６であり、好ましくはフルグラフィックＬＣＤである。その他のタイプの出力デバイスが代替的に利用され得る。図１に概略的に示すプロセッサ１８は、ハウジング内に含まれており、キーボード１４とディスプレイ１６との間に結合されている。プロセッサ１８は、ユーザがキーボード１４上のキーを作動することに応答して、モバイル機器１０の全体の動作と同様にディスプ

レイ１６の動作を制御する。

【００１９】

ハウジングは縦長であり得、あるいはその他の寸法および形状をとり得る（クラムシェルハウジング構造）。キーボード１４は、モード選択キー、あるいは、テキスト入力と電話入力とを切り替えるための他のハードウェアまたはソフトウェアを含み得る。

【００２０】

プロセッサ１８に加え、モバイル機器１０のその他のパーツを図１に概略的に示す。これらのパーツは、通信サブシステム１００と、短距離通信サブシステムと、他の入力／出力デバイス１０６、１０８、１１０、および１１２を伴うキーボード１４およびディスプレイ１６と、メモリデバイス１１６、１１８およびその他の多様な機器サブシステム１２０を含む。モバイル機器１０は、好ましくは、音声通信の性能とデータ通信の性能とを有する、送受信兼用のＲＦ通信機器である。また、モバイル機器１０は、好ましくは、インターネットを介してその他のコンピュータシステムと通信する性能を有する。

【００２１】

プロセッサ１８によって実行されるオペレーティングシステムソフトウェアは、好ましくは、フラッシュメモリ１１６のような持続性の記憶装置内に格納されるが、読み取り専用メモリ（ＲＯＭ）または同様の記憶装置要素のようなその他のタイプのメモリデバイス内にも格納され得る。また、システムソフトウェア、特定の機器アプリケーション、またはその一部は、ランダムアクセスメモリ（ＲＡＭ）１１８のような揮発性メモリ内に一時的にロードされ得る。モバイル機器が受信した通信信号も、ＲＡＭ１１８内に格納され得る。

【００２２】

プロセッサ１８は、オペレーティングシステム機能に加え、機器１０上のソフトウェアアプリケーション１３０Ａ～１３０Ｎを実行できる。データ通信１３０Ａおよび音声通信１３０Ｂのような機器の基本動作を制御する、所定のアプリケーションのセットは、製造中に機器１０上にインストールされ得る。また、パーソナルインフォメーションマネジャー（ＰＩＭ）アプリケーションが製造中にインストールされ得る。ＰＩＭは、好ましくは、Ｅメール、カレンダーイベント、音声メール、アポイントメント、タスクアイテム等のデータ項目を編集し管理することができる。ＰＩＭアプリケーションは、好ましくは、無線ネットワーク１４０を介してデータ項目を送受信することもできる。好ましくは、ＰＩＭデータ項目は、無線ネットワーク１４０を介して、格納されているおよび／またはホストコンピュータシステムと関連する、機器のユーザの関連データ項目と、シームレスに統合され、同期され、更新される。

【００２３】

データ通信および音声通信を含む通信機能は、通信サブシステム１００と、場合によっては短距離通信サブシステムとを介して実行される。通信サブシステム１００は、受信器１５０と、送信器１５２と、１つ以上のアンテナ１５４および１５６とを含む。また、通信サブシステム１００は、デジタル信号プロセッサ（ＤＳＰ）１５８およびローカル発振器（ＬＯ）１６０のような、処理モジュールをも含む。通信サブシステム１００の詳細な設計および実施は、モバイル機器１０が動作するように意図される通信ネットワークに依存する。たとえば、モバイル機器１０は、通信サブシステム１００であって、Ｍｏｂｉｔｅｘ™、ＤａｔａＴＡＣ™、またはＧｅｎｅｒａｌ Ｐａｃｋｅｔ Ｒａｄｉｏ Ｓｅｒｖｉｃｅ（ＧＰＲＳ）の移動体データ通信ネットワークと共に動作するように設計されており、ＡＭＰＳ、ＴＤＭＡ、ＣＤＭＡ、ＰＣＳ、ＧＳＭ等の多様な音声通信ネットワークとも共に動作するように設計されている、通信サブシステム１００を含み得る。その他のタイプのデータ通信および音声通信もまた、モバイル機器１０と共に利用され得る。データ通信と音声通信とは、個別であってもよいし、一体化されていてもよい。

【００２４】

通信システムのタイプに応じて、ネットワークアクセスの要件は異なる。たとえば、ＭｏｂｉｔｅｘネットワークおよびｄａｔａＴＡＣネットワークにおいて、モバイル機器は

、各機器に付随する固有の個人識別番号すなわちＰＩＮを用いてネットワーク上に登録される。しかしながら、ＧＰＲＳネットワークにおいては、ネットワークアクセスは加入者または機器のユーザに関連する。したがって、ＧＰＲＳ機器は、ＧＰＲＳネットワーク上で動作するために、一般にＳＩＭカードと呼ばれる加入者識別モジュールを必要とする。

【００２５】

要求されたネットワーク登録手順またはネットワーク起動手順が完了すると、モバイル機器１０は通信ネットワーク１４０を介して通信信号を送受信し得る。通信ネットワーク１４０を介してアンテナ１５４によって受信された信号は、受信器１５０へルーティングされる。受信器１５０は、信号増幅、周波数ダウンコンバージョン、フィルタリング、チャネル選択等を提供し得、アナログ－デジタル変換をも提供し得る。受信した信号のアナログ－デジタル変換によって、復調およびデコーディングといったより複雑な機能をＤＳＰ１５８が実行することが可能になる。ネットワーク１４０へ送信される信号は同様の方法でＤＳＰ１５８によって処理され（たとえば変調され、デコーディングされる）、次いで、デジタル－アナログ変換、周波数アップコンバージョン、フィルタリング、増幅、アンテナ１５６を介しての通信ネットワーク１４０への送信のために、送信器１５２へ提供される。

【００２６】

ＤＳＰ１５８は、通信信号を処理するだけでなく受信器１５０および送信器１５２の制御をも提供する。たとえば、受信器１５０および送信器１５２において通信信号に適用されるゲインは、ＤＳＰ１５８内で実施される自動ゲイン制御アルゴリズムを通じて適合するように制御され得る。

【００２７】

データ通信モードにおいて、テキストメッセージまたはウェブページのダウンロード等の受信された信号は、通信サブシステム１００によって処理され、プロセッサ１８へ入力される。次いで、受信された信号は、ディスプレイ１６へ、または代替的に他の一部の補助Ｉ／Ｏデバイス１０６へ、出力されるために、プロセッサ１８によってさらに処理される。機器のユーザは、キーボード１４、および／あるいは、タッチパッド、ロッカースイッチ、サムホイール（ｔｈｕｍｂｗｈｅｅｌ）、または他の一部のタイプの入力デバイスのような補助Ｉ／Ｏデバイス１０６を用いて、たとえばＥメールメッセージ等のデータ項目を作成することもできる。作成されたデータ項目は、次いで通信サブシステム１００を介して通信ネットワーク１４０上へ送信され得る。各データ項目は、「セッション」中、暗号化された形式で通信ネットワーク１４０上で送信される。この送信は、データ項目が機器１０へ完全に送信されるまで、１つ以上のバッチのデータを送信することを含む。好ましい実施形態において、このような各セッションの間に送信されたデータは、共通の「セッションキー」を用いて暗号化される。これについては以下に詳述する。

【００２８】

音声通信モードにおいては、受信された信号がスピーカ１１０へ出力され、送信される信号がマイクロフォン１１２によって生成されるという点を除けば、機器の全体的な動作は実質的に同様である。音声メッセージ録音サブシステムのような代替的な声または音声のＩ／Ｏサブシステムも機器１０上で実施され得る。また、音声通信モードにおいて、たとえば電話をかけた当事者の識別、音声通話の長さ、または音声通話関連のその他の情報を提供するために、ディスプレイ１６も利用され得る。

【００２９】

短距離通信サブシステムは、モバイル機器１０と近辺にある他のシステムまたは機器との間の通信を可能にする。これらは必ずしも同様の機器である必要はない。たとえば、短距離通信サブシステムは、赤外線機器やそれに関連する回路およびコンポーネント、あるいは、同様に可能であるシステムや機器との通信を提供するＢｌｕｅｔｏｏｔｈ™通信モジュールを含み得る。

【００３０】

本発明は、たとえば通信ネットワーク１４０を介したＥメールメッセージデータ項目の

送信に適用される。ネットワーク１４０の効率的な動作のために、データ項目は、全体のメッセージが機器１０に送信されるまで、たとえば２ｋｂのバッチ（ただし、任意の適切なバッチサイズが選択され得る）というように、データバッチとして送信される。これは「セッション」として知られている。セキュリティ目的のため、セッションの間、データ項目は暗号化された形式で送信される。

【００３１】

本発明によると、メッセージのハッシュを生成するために決定性アルゴリズムが採用される。一般的な用語において、ハッシュとは、圧縮機能を用いてデータバッチを処理した結果である。圧縮機能は、データバッチを取り、それを圧縮してより小さな固有の識別子にする。

【００３２】

本方法の好ましい実施形態において、決定アルゴリズム、たとえば、ハッシュアルゴリズム（たとえば、２００２年８月１日に刊行されたＦｅｄｅｒａｌ　Ｉｎｆｏｒｍａｔｉｏｎ　Ｐｒｏｃｅｓｓｉｎｇ　Ｓｔａｎｄａｒｄｓ（ＦＩＰＳ）の刊行物１８０－２（本明細書中に援用する）において定義されている、ＳＨＡ－２５６等）または鍵導出関数（データを反復的にハッシュして特定の長さの鍵を作成するために、他のデータと共にハッシュアルゴリズムを利用する一般的な構造）が、暗号化されるメッセージｍに適用される。例示のみの目的で、ハッシュアルゴリズムＨ（）としてＳＨＡ－２５６を用いた本発明の実施について記載する。Ａｄｖａｎｃｅｄ　Ｅｎｃｒｙｐｔｉｏｎ　Ｓｔａｎｄａｒｄ（ＡＥＳ）を用いてメッセージｍを暗号化すると、ＳＨＡ－２５６は、２５６ビットの出力を提供し、そのため機能が良い。本明細書中では、メッセージｍのハッシュをＨ（ｍ）によって表す。

【００３３】

セッションキーは、メッセージのハッシュに少なくとも一部基づいて生成される。メッセージ自体のハッシュにのみ基づいてセッションキーを生成することができるが、好ましい実施形態において、そのハッシュが固有のものであるということを保証するために、追加のデータがハッシュに追加される。したがって、たとえば、同一のメッセージが２度送信されると、２つの異なるセッションは、異なるセッションキーを有する。このように、本発明の好ましい実施形態は、追加情報ｒを利用するというオプションを可能にする。この追加情報ｒは、ハッシュが固有のものであるということを保証するために、メッセージｍに追加される。追加データｒは、たとえば、ユーザのＥメールアドレス、ランダムに生成されローカルサーバに保存されているバイト、または増加式カウンタであり得る。代替実施形態において、追加データｒのハッシュはメッセージｍのハッシュと結び付けられ得る。追加データｒの様々な活用方法が存在するということが認識されよう。追加データｒの利用は選択的であるため、ｒは空白の場合もある。

【００３４】

メッセージの復号を所望する悪意のアタッカーは、セッションキーを決定しなければならない。これを行うためには、アタッカーは元のメッセージを読まなければならないが、元のメッセージはセッションキーを用いて暗号化されているため、セッションキーがないとそれを読むことはできない。あるいは、セッションキーを復号しなければならないが、セッションキーはユーザの公開鍵を用いて暗号化されており、悪意のアタッカーは対応する秘密鍵へのアクセスを有していないため、復号を行うことはできない。

【００３５】

セッションキーｋは、ｋ＝Ｈ（ｍ‖ｒ）と表される、ｍとｒとの連結のハッシュによって作成される。ｒが空白である場合、すなわちセッションキーｋがメッセージｍの内容のみから作成される場合、これはｋ＝Ｈ（ｍ）と表され得る。

【００３６】

次いで、セッションキーｋは、ユーザの公開鍵ｐを用いて、演算E_p（ｋ）によって暗号化され、セッションキー$e_k = E_p$（ｋ）が作成される。この公開鍵は、たとえばＲＳＡキーであり得る。

【００３７】
メッセージｍ（あるいは、選択されたバッチサイズよりもメッセージｍが大きい場合、メッセージｍからのデータバッチ）は、セッションキーｋを用いて、たとえばＡＥＳを用いて、暗号化され、それによって暗号化されたメッセージe_mは、$e_m = E_k$（ｍ）になる。暗号化されたセッションキーe_kおよび暗号化されたメッセージe_mは、ユーザの移動体通信機器１０へ送信される。移動体通信機器１０は、次いで、公開鍵ｐに対応する秘密鍵を用いて、好都合な方式でセッションキーを復号することができ、それによって、そのセッションキーを用いてメッセージを復号することができる。セッション継続の間、セッションキーはモバイル機器１０上に保存され得る。
【００３８】
図２に示すように、メッセージが第１のデータバッチ内に完全に含まれている場合、セッションは完了である。メッセージデータの第１のバッチがメッセージ全体を含んでいない場合、移動体通信機器１０はＭＯＲＥリクエストをローカルサーバへ送信する。これは、たとえばユーザがメッセージデータの第１のバッチの終了部分へとメッセージをスクロールダウンするときに送信される。次いで、メッセージデータのうちの次のバッチに対して上記のプロセスが反復される。ローカルサーバが、メッセージデータのハッシュからセッションキーを再現（使用されていれば、外部データｒからも再現する）し、公開鍵を用いてセッションキーを再暗号化し、暗号化されたセッションキーを再現し、同一のセッションキーを用いてメッセージデータのうちの次のバッチを暗号化し、暗号化されたメッセージデータのうちの次のバッチを同様の方式でモバイル機器１０へ送信する。
【００３９】
本発明の原則は、採用される通信方法にかかわらず適用され得、暗号化のプラットフォームおよび公開鍵システムは選択事項であるという点が認識されよう。
【００４０】
以上のように、本発明の多様な実施形態を例示によって詳細に説明したが、本発明から逸脱することなく多様な変更および修正がなされ得るということは、当業者にとっては明白であろう。本発明は、このような変更および修正を全て添付の請求項の範囲内にあるものとして含む。
【図面の簡単な説明】
【００４１】
【図１】従来のハンドヘルド無線通信機器のシステムの概要のブロック図である。
【図２】本発明の方法を用いたメッセージの暗号化および復号方法を示すフローチャートである。

【図１】

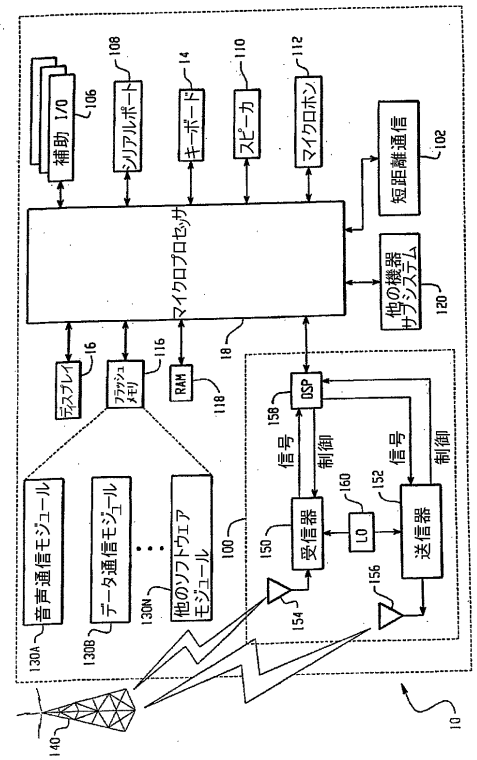

FIG. 1

【図２】

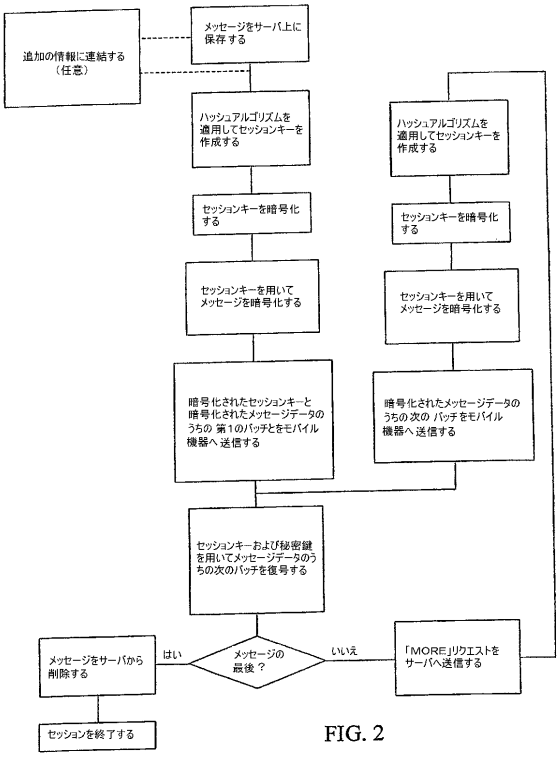

FIG. 2

フロントページの続き

(72)発明者 ブラウン, マイケル ケー.
カナダ国 エヌ２エム ２ゼット２ オンタリオ, キッチナー, ファーンウッド プレイス ８
(72)発明者 ブラウン, マイケル エス.
カナダ国 エヌ２ケー ４ビー１ オンタリオ, ウォータールー, ユニバーシティ ダウンズ クレセント ３５０
(72)発明者 リトル, ハーバート エー.
カナダ国 エヌ２ティー ２ブイ８ オンタリオ, ウォータールー, オールド オーク プレイス ５０４

審査官 速水 雄太

(56)参考文献 特開平０９－０４６３３０（ＪＰ，Ａ）
特開２００２－３５８２２６（ＪＰ，Ａ）
特開平１１－３２７４３７（ＪＰ，Ａ）
特開２００４－００５１７４（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
H04L 9/08