(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2015-528681
(P2015-528681A)
(43)公表日　平成27年9月28日(2015.9.28)

(51)Int.Cl.		F I			テーマコード（参考）
H04L 9/14	(2006.01)	H04L	9/00	641	5J104

審査請求 未請求　予備審査請求 有　（全 23 頁）

(21)出願番号	特願2015-532051 (P2015-532051)
(86)(22)出願日	平成25年9月12日 (2013.9.12)
(85)翻訳文提出日	平成27年2月27日 (2015.2.27)
(86)国際出願番号	PCT/US2013/059524
(87)国際公開番号	WO2014/043392
(87)国際公開日	平成26年3月20日 (2014.3.20)
(31)優先権主張番号	61/701,384
(32)優先日	平成24年9月14日 (2012.9.14)
(33)優先権主張国	米国 (US)
(31)優先権主張番号	13/764,524
(32)優先日	平成25年2月11日 (2013.2.11)
(33)優先権主張国	米国 (US)

(71)出願人　507364838
クアルコム，インコーポレイテッド
アメリカ合衆国　カリフォルニア　９２１２１　サン　ディエゴ　モアハウス　ドライブ　５７７５
(74)代理人　100108453
弁理士　村山　靖彦
(74)代理人　100163522
弁理士　黒田　晋平
(72)発明者　デイヴィッド・エム・ジェイコブソン
アメリカ合衆国・カリフォルニア・９２１２１・サン・ディエゴ・モアハウス・ドライヴ・５７７５

最終頁に続く

(54)【発明の名称】メッセージデータを保護するための装置および方法

(57)【要約】
メッセージデータを保護するための方法を開示する。この方法では、メッセージデータは、メッセージデータに対して実施された確定関数に基づいて生成されたパディングビットでパディングされる。パディングされたメッセージデータは、圧縮されて、圧縮データが生成される。圧縮データの長さは、パディングビットに依存する。圧縮データは暗号化されて、暗号化メッセージデータが生成される。

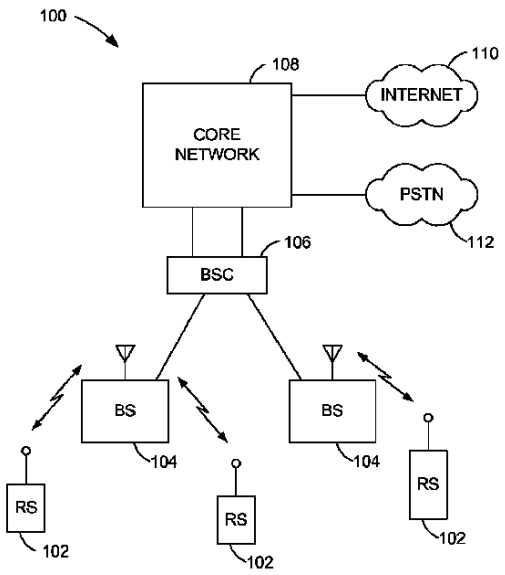


FIG. 1

【特許請求の範囲】
【請求項１】
メッセージデータを保護するための方法であって、
前記メッセージデータに対して実施された確定関数に基づいて生成されたパディングビットで、前記メッセージデータをパディングするステップと、
前記パディングされたメッセージデータを圧縮して、圧縮データを生成するステップであって、前記圧縮データの長さが前記パディングビットに依存するステップと、
前記圧縮データを暗号化して、暗号化メッセージデータを生成するステップとを含む方法。
【請求項２】
前記確定関数がハッシュ関数を含む、請求項1に記載のメッセージデータを保護するための方法。
【請求項３】
前記パディングビットが前記メッセージデータにプレフィックスされる、請求項1に記載のメッセージデータを保護するための方法。
【請求項４】
前記パディングビットが、前記パディングビットの末尾が受信機によって判断されるように制約される、請求項1に記載のメッセージデータを保護するための方法。
【請求項５】
メッセージデータに対して実施された確定関数に基づいて生成されたパディングビットで、メッセージデータをパディングするための手段と、
前記パディングされたメッセージデータを圧縮して、圧縮データを生成するための手段であって、前記圧縮データの長さが前記パディングビットに依存する手段と、
前記圧縮データを暗号化して、暗号化メッセージデータを生成するための手段とを備える遠隔局。
【請求項６】
前記確定関数がハッシュ関数を含む、請求項5に記載の遠隔局。
【請求項７】
前記パディングビットが前記メッセージデータにプレフィックスされる、請求項5に記載の遠隔局。
【請求項８】
前記パディングビットが、前記パディングビットの末尾が受信機によって判断されるように制約される、請求項5に記載の遠隔局。
【請求項９】
プロセッサを備え、前記プロセッサが、
メッセージデータに対して実施された確定関数に基づいて生成されたパディングビットで、メッセージデータをパディングし、
前記パディングされたメッセージデータを圧縮して、圧縮データを生成し、前記圧縮データの長さが前記パディングビットに依存し、
前記圧縮データを暗号化して、暗号化メッセージデータを生成するように構成された遠隔局。
【請求項１０】
前記確定関数がハッシュ関数を含む、請求項9に記載の遠隔局。
【請求項１１】
前記パディングビットが前記メッセージデータにプレフィックスされる、請求項9に記載の遠隔局。
【請求項１２】
前記パディングビットが、前記パディングビットの末尾が受信機によって判断されるように制約される、請求項9に記載の遠隔局。
【請求項１３】

コンピュータに、メッセージデータに対して実施された確定関数に基づいて生成されたパディングビットで、メッセージデータをパディングさせるためのコードと、
コンピュータに、前記パディングされたメッセージデータを圧縮させて、圧縮データを生成するためのコードであって、前記圧縮データの長さが前記パディングビットに依存するコードと、
コンピュータに、前記圧縮データを暗号化させて、暗号化メッセージデータを生成するためのコードと
を含むコンピュータプログラム。
【請求項１４】
前記確定関数がハッシュ関数を含む、請求項13に記載のコンピュータプログラム。
【請求項１５】
前記パディングビットが前記メッセージデータにプレフィックスされる、請求項13に記載のコンピュータプログラム。
【請求項１６】
前記パディングビットが、前記パディングビットの末尾が受信機によって判断されるように制約される、請求項13に記載のコンピュータプログラム。
【請求項１７】
メッセージデータを保護するための方法であって、
前記メッセージデータに対して実施された確定関数を使って、圧縮アルゴリズムの圧縮パラメータ値を選択するステップと、
前記圧縮アルゴリズムおよび前記選択された圧縮パラメータ値を使って前記メッセージデータを圧縮して、圧縮データを生成するステップであって、前記圧縮データの長さが前記圧縮パラメータ値に依存するステップと、
前記圧縮データを暗号化して、暗号化メッセージデータを生成するステップとを含む方法。
【請求項１８】
前記圧縮パラメータ値が最大チェーン長値である、請求項17に記載のメッセージデータを保護するための方法。
【請求項１９】
前記確定関数がハッシュ関数を含む、請求項17に記載のメッセージデータを保護するための方法。
【請求項２０】
前記メッセージデータを圧縮するステップが、
前記確定関数に基づいて選択された、いくつかのパディングビットで、前記メッセージデータをパディングして、パディングされたメッセージデータを生成するステップと、
前記パディングされたメッセージデータに対して前記圧縮アルゴリズムおよび前記選択された圧縮パラメータ値を使うことによって、前記圧縮データを生成するステップとを含む、請求項17に記載のメッセージデータを保護するための方法。
【請求項２１】
前記パディングビットが前記メッセージデータにプレフィックスされる、請求項20に記載のメッセージデータを保護するための方法。
【請求項２２】
前記パディングビットが、前記パディングビットの末尾が受信機によって判断されるように制約される、請求項20に記載のメッセージデータを保護するための方法。
【請求項２３】
メッセージデータに対して実施された確定関数を使って、圧縮アルゴリズムの圧縮パラメータ値を選択するための手段と、
前記圧縮アルゴリズムおよび前記選択された圧縮パラメータ値を使って前記メッセージデータを圧縮して、圧縮データを生成するための手段であって、前記圧縮データの長さが前記圧縮パラメータ値に依存する手段と、

前記圧縮データを暗号化して、暗号化メッセージデータを生成するための手段とを備える遠隔局。
【請求項２４】
前記圧縮パラメータ値が最大チェーン長値である、請求項23に記載の遠隔局。
【請求項２５】
前記確定関数がハッシュ関数を含む、請求項23に記載の遠隔局。
【請求項２６】
前記メッセージデータを圧縮するための前記手段が、
前記確定関数に基づいて選択された、いくつかのパディングビットで、前記メッセージデータをパディングして、パディングされたメッセージデータを生成するための手段と、
前記パディングされたメッセージデータに対して前記圧縮アルゴリズムおよび前記選択された圧縮パラメータ値を使うことによって、前記圧縮データを生成するための手段とを備える、請求項23に記載の遠隔局。
【請求項２７】
前記パディングビットが前記メッセージデータにプレフィックスされる、請求項26に記載の遠隔局。
【請求項２８】
前記パディングビットが、前記パディングビットの末尾が受信機によって判断されるように制約される、請求項26に記載の遠隔局。
【請求項２９】
プロセッサを備え、前記プロセッサが、
メッセージデータに対して実施された確定関数を使って、圧縮アルゴリズムの圧縮パラメータ値を選択し、
前記圧縮アルゴリズムおよび前記選択された圧縮パラメータ値を使って前記メッセージデータを圧縮して、圧縮データを生成し、前記圧縮データの長さが前記圧縮パラメータ値に依存し、
前記圧縮データを暗号化して、暗号化メッセージデータを生成するように構成された遠隔局。
【請求項３０】
前記圧縮パラメータ値が最大チェーン長値である、請求項29に記載の遠隔局。
【請求項３１】
前記確定関数がハッシュ関数を含む、請求項29に記載の遠隔局。
【請求項３２】
前記プロセッサが、
前記確定関数に基づいて選択された、いくつかのパディングビットで、前記メッセージデータをパディングして、パディングされたメッセージデータを生成し、
前記パディングされたメッセージデータに対して前記圧縮アルゴリズムおよび前記選択された圧縮パラメータ値を使うことによって、前記圧縮データを生成するようにさらに構成される、請求項29に記載の遠隔局。
【請求項３３】
前記パディングビットが前記メッセージデータにプレフィックスされる、請求項32に記載の遠隔局。
【請求項３４】
前記パディングビットが、前記パディングビットの末尾が受信機によって判断されるように制約される、請求項32に記載の遠隔局。
【請求項３５】
コンピュータに、メッセージデータに対して実施された確定関数を使って、圧縮アルゴリズムの圧縮パラメータ値を選択させるためのコードと、
コンピュータに、前記圧縮アルゴリズムおよび前記選択された圧縮パラメータ値を使って前記メッセージデータを圧縮させて、圧縮データを生成するためのコードであって、前

記圧縮データの長さが前記圧縮パラメータ値に依存するコードと、
コンピュータに、前記圧縮データを暗号化させて、暗号化メッセージデータを生成するためのコードと
を含むコンピュータプログラム。
【請求項３６】
前記圧縮パラメータ値が最大チェーン長値である、請求項35に記載のコンピュータプログラム。
【請求項３７】
前記確定関数がハッシュ関数を含む、請求項35に記載のコンピュータプログラム。
【請求項３８】
前記確定関数に基づいて選択された、いくつかのパディングビットで、前記メッセージデータをパディングして、パディングされたメッセージデータを生成するためのコードと、
前記パディングされたメッセージデータに対して前記圧縮アルゴリズムおよび前記選択された圧縮パラメータ値を使うことによって、前記圧縮データを生成するためのコードとをさらに含む、請求項35に記載のコンピュータプログラム。
【請求項３９】
前記パディングビットが前記メッセージデータにプレフィックスされる、請求項38に記載のコンピュータプログラム。
【請求項４０】
前記パディングビットが、前記パディングビットの末尾が受信機によって判断されるように制約される、請求項38に記載のコンピュータプログラム。
【請求項４１】
メッセージデータを保護するための方法であって、
前記メッセージデータを圧縮して、第1の数のデータバイトを含む圧縮データを生成するステップと、
前記圧縮データをパディングして、第2の数のデータバイトを含むパディングされた圧縮データを生成するステップであって、前記第2の数が、前記第1の数にデータバイトのパッド数を加えたものに等しく、データバイトの前記パッド数が、前記メッセージデータのハッシュに基づいて決定されるステップと、
前記パディングされた圧縮データを暗号化して、暗号化メッセージデータを生成するステップとを含む方法。
【請求項４２】
前記メッセージデータの前記ハッシュが、前記メッセージデータの鍵付きハッシュである、請求項41に記載のメッセージデータを保護するための方法。
【請求項４３】
前記メッセージデータの前記鍵付きハッシュが、メッセージ認証のためのハッシュ化(HMAC)暗号学的ハッシュ関数を使って実施される、請求項42に記載のメッセージデータを保護するための方法。
【請求項４４】
前記鍵付きハッシュが、鍵導出関数を使って導出された難読化鍵を使う、請求項42に記載のメッセージデータを保護するための方法。
【請求項４５】
前記難読化鍵が、交換される秘密の値から生成される、請求項44に記載のメッセージデータを保護するための方法。
【請求項４６】
前記鍵導出関数が、前記難読化鍵を生成するのに、暗号化鍵および認証鍵を使う、請求項44に記載のメッセージデータを保護するための方法。
【請求項４７】
前記暗号化鍵および前記認証鍵が、交換される秘密の値から、および複数の秘密でない

値から生成される、請求項46に記載のメッセージデータを保護するための方法。
【請求項４８】
データバイトの前記パッド数が、1から32の数を含む、請求項41に記載のメッセージデータを保護するための方法。
【請求項４９】
前記メッセージデータが、トランスポートレイヤセキュリティ(TLS)プロトコルメッセージを含む、請求項41に記載のメッセージデータを保護するための方法。
【請求項５０】
前記メッセージデータが、セキュアソケットレイヤ(SSL)プロトコルメッセージを含む、請求項41に記載のメッセージデータを保護するための方法。
【請求項５１】
メッセージデータを圧縮して、第1の数のデータバイトを含む圧縮データを生成するための手段と、
前記圧縮データをパディングして、第2の数のデータバイトを含むパディングされた圧縮データを生成するための手段であって、前記第2の数が、前記第1の数にデータバイトのパッド数を加えたものに等しく、データバイトの前記パッド数が、前記メッセージデータのハッシュに基づいて決定される手段と、
前記パディングされた圧縮データを暗号化して、暗号化メッセージデータを生成するための手段とを備える遠隔局。
【請求項５２】
前記メッセージデータの前記ハッシュが、前記メッセージデータの鍵付きハッシュである、請求項51に記載の遠隔局。
【請求項５３】
前記メッセージデータの前記鍵付きハッシュが、メッセージ認証のためのハッシュ化(HMAC)暗号学的ハッシュ関数を使って実施される、請求項52に記載の遠隔局。
【請求項５４】
前記鍵付きハッシュが、鍵導出関数を使って導出された難読化鍵を使う、請求項52に記載の遠隔局。
【請求項５５】
前記難読化鍵が、交換される秘密の値から生成される、請求項54に記載の遠隔局。
【請求項５６】
前記鍵導出関数が、前記難読化鍵を生成するのに、暗号化鍵および認証鍵を使う、請求項54に記載の遠隔局。
【請求項５７】
前記暗号化鍵および前記認証鍵が、交換される秘密の値から、および複数の秘密でない値から生成される、請求項56に記載の遠隔局。
【請求項５８】
データバイトの前記パッド数が、1から32の数を含む、請求項51に記載の遠隔局。
【請求項５９】
前記メッセージデータが、トランスポートレイヤセキュリティ(TLS)プロトコルメッセージを含む、請求項51に記載の遠隔局。
【請求項６０】
前記メッセージデータが、セキュアソケットレイヤ(SSL)プロトコルメッセージを含む、請求項51に記載の遠隔局。
【請求項６１】
プロセッサを備え、前記プロセッサが、
メッセージデータを圧縮して、第1の数のデータバイトを含む圧縮データを生成し、
前記圧縮データをパディングして、第2の数のデータバイトを含むパディングされた圧縮データを生成し、前記第2の数が、前記第1の数にデータバイトのパッド数を加えたものに等しく、データバイトの前記パッド数が、前記メッセージデータのハッシュに基づいて

決定され、
前記パディングされた圧縮データを暗号化して、暗号化メッセージデータを生成するように構成された遠隔局。
【請求項６２】
前記メッセージデータの前記ハッシュが、前記メッセージデータの鍵付きハッシュである、請求項61に記載の遠隔局。
【請求項６３】
前記メッセージデータの前記鍵付きハッシュが、メッセージ認証のためのハッシュ化(HMAC)暗号学的ハッシュ関数を使って実施される、請求項62に記載の遠隔局。
【請求項６４】
前記鍵付きハッシュが、鍵導出関数を使って導出された難読化鍵を使う、請求項62に記載の遠隔局。
【請求項６５】
前記難読化鍵が、交換される秘密の値から生成される、請求項64に記載の遠隔局。
【請求項６６】
前記鍵導出関数が、前記難読化鍵を生成するのに、暗号化鍵および認証鍵を使う、請求項64に記載の遠隔局。
【請求項６７】
前記暗号化鍵および前記認証鍵が、交換される秘密の値から、および複数の秘密でない値から生成される、請求項66に記載の遠隔局。
【請求項６８】
データバイトの前記パッド数が、1から32の数を含む、請求項61に記載の遠隔局。
【請求項６９】
前記メッセージデータが、トランスポートレイヤセキュリティ(TLS)プロトコルメッセージを含む、請求項61に記載の遠隔局。
【請求項７０】
前記メッセージデータが、セキュアソケットレイヤ(SSL)プロトコルメッセージを含む、請求項61に記載の遠隔局。
【請求項７１】
コンピュータに、メッセージデータを圧縮させて、第1の数のデータバイトを含む圧縮データを生成するためのコードと、
コンピュータに、前記圧縮データをパディングさせて、第2の数のデータバイトを含むパディングされた圧縮データを生成するためのコードであって、前記第2の数が、前記第1の数にデータバイトのパッド数を加えたものに等しく、データバイトの前記パッド数が、前記メッセージデータのハッシュに基づいて決定されるコードと、
コンピュータに、前記パディングされた圧縮データを暗号化させて、暗号化メッセージデータを生成するためのコードと
を含むコンピュータプログラム。
【請求項７２】
前記メッセージデータの前記ハッシュが、前記メッセージデータの鍵付きハッシュである、請求項71に記載のコンピュータプログラム。
【請求項７３】
前記メッセージデータの前記鍵付きハッシュが、メッセージ認証のためのハッシュ化(HMAC)暗号学的ハッシュ関数を使って実施される、請求項72に記載のコンピュータプログラム。
【請求項７４】
前記鍵付きハッシュが、鍵導出関数を使って導出された難読化鍵を使う、請求項72に記載のコンピュータプログラム。
【請求項７５】
前記難読化鍵が、交換される秘密の値から生成される、請求項74に記載のコンピュータ

プログラム。
【請求項７６】
前記鍵導出関数が、前記難読化鍵を生成するのに、暗号化鍵および認証鍵を使う、請求項74に記載のコンピュータプログラム。
【請求項７７】
前記暗号化鍵および前記認証鍵が、交換される秘密の値から、および複数の秘密でない値から生成される、請求項76に記載のコンピュータプログラム。
【請求項７８】
データバイトの前記パッド数が、1から32の数を含む、請求項71に記載のコンピュータプログラム。
【請求項７９】
前記メッセージデータが、トランスポートレイヤセキュリティ(TLS)プロトコルメッセージを含む、請求項71に記載のコンピュータプログラム。
【請求項８０】
前記メッセージデータが、セキュアソケットレイヤ(SSL)プロトコルメッセージを含む、請求項71に記載のコンピュータプログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
関連出願の相互参照
本出願は、参照により本明細書に組み込まれている、2012年9月14日に出願した米国仮出願第61/701,384号の利益を主張するものである。
【０００２】
本発明は概して、圧縮および暗号化されているメッセージデータの保護に関する。
【背景技術】
【０００３】
暗号化および圧縮されたメッセージの長さは、情報を発見するのに活用することができるので、圧縮を使うセキュアな接続(たとえば、SSL/TLS)に対して、攻撃が行われる場合がある。攻撃者が、非圧縮メッセージ中の何らかのテキストをコントロールすることができるとき、攻撃者は、最も短い暗号化メッセージを生じるものを見つけるまで、数字(またはバイト)を循環すればよい。たとえば、暗号化メッセージは、「秘密=4528715」のようなタグを含み得る。攻撃者が挿入した非圧縮メッセージが「秘密=4」であるとき、「秘密=0」など、他の可能な数字に対してよりも圧縮が向上するので、暗号化メッセージの長さは短くなる。最初の数字を発見した後、攻撃者は、より短い長さ、たとえば「秘密=45」を生じるものを見つけるまで、次の可能な数字(またはバイト)を循環すればよい。攻撃者は次いで、機密情報がすべて発見されるまで、次の数字(またはバイト)を循環すればよい。
【発明の概要】
【発明が解決しようとする課題】
【０００４】
したがって、圧縮メッセージの長さを、圧縮および暗号化されたデータストリームから判断することができないように、圧縮と暗号化の両方がなされているメッセージを保護するための技法が必要である。
【課題を解決するための手段】
【０００５】
本発明の一態様は、メッセージデータを保護するための方法に存在し得る。この方法では、メッセージデータは、メッセージデータに対して実施された確定関数に基づいて生成されたパディングビットでパディングされる。パディングされたメッセージデータは、圧縮されて、圧縮データが生成される。圧縮データの長さは、パディングビットに依存する。圧縮データは暗号化されて、暗号化メッセージデータが生成される。

【０００６】
本発明のより詳細な態様では、確定関数は、ハッシュ関数を含み得る。パディングビットは、メッセージデータにプレフィックスまたはプリペンドされてよい。パディングビットは、パディングビットの末尾が受信機によって判断されるように制約され得る。
【０００７】
本発明の別の態様は、メッセージデータに対して実施された確定関数に基づいて生成されたパディングビットで、メッセージデータをパディングするための手段と、パディングされたメッセージデータを圧縮して、圧縮データを生成するための手段であって、圧縮データの長さがパディングビットに依存する手段と、圧縮データを暗号化して、暗号化メッセージデータを生成するための手段とを備える遠隔局に存在し得る。
【０００８】
本発明の別の態様は、メッセージデータに対して実施された確定関数に基づいて生成されたパディングビットでメッセージデータをパディングし、パディングされたメッセージデータを圧縮して、圧縮データを生成し、圧縮データの長さがパディングビットに依存し、圧縮データを暗号化して、暗号化メッセージデータを生成するように構成されたプロセッサを備える遠隔局に存在し得る。
【０００９】
本発明の別の態様は、コンピュータに、メッセージデータに対して実施された確定関数に基づいて生成されたパディングビットでメッセージデータをパディングさせるためのコードと、コンピュータに、パディングされたメッセージデータを圧縮させて、圧縮データを生成するためのコードであって、圧縮データの長さがパディングビットに依存するコードと、コンピュータに、圧縮データを暗号化させて、暗号化メッセージデータを生成するためのコードとを含むコンピュータ可読媒体を含むコンピュータプログラム製品に存在し得る。
【００１０】
本発明の別の態様は、メッセージデータを保護するための方法に存在し得る。この方法では、圧縮アルゴリズムの圧縮パラメータ値が、メッセージデータに対して実施された確定関数を使って選択される。メッセージデータは、圧縮アルゴリズムおよび選択された圧縮パラメータ値を使って圧縮されて、圧縮データが生成される。圧縮データの長さは、圧縮パラメータ値に依存する。圧縮データは暗号化されて、暗号化メッセージデータが生成される。
【００１１】
本発明のより詳細な態様では、圧縮パラメータ値は、最大チェーン長値であってよい。確定関数は、ハッシュ関数を含み得る。メッセージデータを圧縮するステップは、確定関数に基づいて選択されたいくつかのパディングビットでメッセージデータをパディングして、パディングされたメッセージデータを生成するステップと、パディングされたメッセージデータに対して圧縮アルゴリズムおよび選択された圧縮パラメータ値を使って、圧縮データを生成するステップとを含み得る。パディングビットは、メッセージデータにプレフィックスされてよい。パディングビットは、パディングビットの末尾が受信機によって判断されるように制約され得る。
【００１２】
本発明の別の態様は、メッセージデータに対して実施された確定関数を使って、圧縮アルゴリズムの圧縮パラメータ値を選択するための手段と、圧縮アルゴリズムおよび選択された圧縮パラメータ値を使ってメッセージデータを圧縮して、圧縮データを生成するための手段であって、圧縮データの長さが圧縮パラメータ値に依存する手段と、圧縮データを暗号化して、暗号化メッセージデータを生成するための手段とを備える遠隔局に存在し得る。
【００１３】
本発明の別の態様は、メッセージデータに対して実施された確定関数を使って圧縮アルゴリズムの圧縮パラメータ値を選択し、圧縮アルゴリズムおよび選択された圧縮パラメー

タ値を使ってメッセージデータを圧縮して、圧縮データを生成し、圧縮データの長さが圧縮パラメータ値に依存し、圧縮データを暗号化して、暗号化メッセージデータを生成するように構成されたプロセッサを備える遠隔局に存在し得る。

【００１４】

本発明の別の態様は、コンピュータに、メッセージデータに対して実施された確定関数を使って、圧縮アルゴリズムの圧縮パラメータ値を選択させるためのコードと、コンピュータに、圧縮アルゴリズムおよび選択された圧縮パラメータ値を使ってメッセージデータを圧縮させて、圧縮データを生成するためのコードであって、圧縮データの長さが圧縮パラメータ値に依存するコードと、コンピュータに、圧縮データを暗号化させて、暗号化メッセージデータを生成するためのコードとを含むコンピュータ可読媒体を含むコンピュータプログラム製品に存在し得る。

【００１５】

本発明の別の態様は、メッセージデータを保護するための方法に存在し得る。この方法では、メッセージデータは、圧縮されて、第1の数のデータバイトを含む圧縮データが生成される。圧縮データはパディングされて、第2の数のデータバイトを含む、パディングされた圧縮データが生成され、第2の数は、第1の数にデータバイトのパッド数を加えたものに等しく、データバイトのパッド数は、メッセージデータのハッシュに基づいて決定される。パディングされた圧縮データは暗号化されて、暗号化メッセージデータが生成される。

【００１６】

本発明のより詳細な態様では、メッセージデータのハッシュは、メッセージデータの鍵付きハッシュであってよい。メッセージデータの鍵付きハッシュは、メッセージ認証のためのハッシュ化(HMAC)という暗号学的ハッシュ関数を使って実施することができ、鍵導出関数を使って導出された難読化鍵を使うことができる。難読化鍵は、交換される秘密の値から生成することができる。鍵導出関数は、難読化鍵を生成するのに、暗号化鍵および認証鍵を使うことができる。暗号化鍵および認証鍵は、交換される秘密の値から、および複数の秘密でない値から生成することができる。データバイトのパッド数は、1から32の数を含み得る。

【００１７】

他のより詳細な本発明の態様では、圧縮データをパディングして、パディングされた圧縮データを生成するステップは、メッセージデータの確定関数に基づいて修正された圧縮アルゴリズムを使うステップを含み得る。メッセージデータは、トランスポートレイヤセキュリティ(TLS)プロトコルメッセージ、またはセキュアソケットレイヤ(SSL)プロトコルメッセージを含み得る。

【００１８】

本発明の別の態様は、メッセージデータを圧縮して、第1の数のデータバイトを含む圧縮データを生成するための手段と、圧縮データをパディングして、第2の数のデータバイトを含むパディングされた圧縮データを生成するための手段であって、第2の数が、第1の数にデータバイトのパッド数を加えたものに等しく、データバイトのパッド数が、メッセージデータのハッシュに基づいて決定される手段とを備える遠隔局に存在し得る。

【００１９】

本発明の別の態様は、メッセージデータを圧縮して、第1の数のデータバイトを含む圧縮データを生成し、圧縮データをパディングして、第2の数のデータバイトを含むパディングされた圧縮データを生成し、第2の数は、第1の数にデータバイトのパッド数を加えたものに等しく、データバイトのパッド数は、メッセージデータのハッシュに基づいて決定されるように構成されたプロセッサを備える遠隔局に存在し得る。

【００２０】

本発明の別の態様は、コンピュータに、メッセージデータを圧縮させて、第1の数のデータバイトを含む圧縮データを生成するためのコードと、コンピュータに、圧縮データをパディングさせて、第2の数のデータバイトを含むパディングされた圧縮データを生成す

るためのコードであって、第2の数が、第1の数にデータバイトのパッド数を加えたものに等しく、データバイトのパッド数が、メッセージデータのハッシュに基づいて決定されるコードとを含むコンピュータ可読媒体を含むコンピュータプログラム製品に存在し得る。

【図面の簡単な説明】

【００２１】

【図１】ワイヤレス通信システムの一例のブロック図である。

【図２】本発明による、メッセージデータを保護するための方法の流れ図である。

【図３】メッセージデータを保護するための方法におけるデータの流れ図である。

【図４】プロセッサとメモリとを含むコンピュータのブロック図である。

【図５】本発明による、メッセージデータを保護するための別の方法の流れ図である。

【図６】メッセージデータを保護するための別の方法におけるデータの流れ図である。

【図７】本発明による、メッセージデータを保護するための別の方法の流れ図である。

【図８】メッセージデータを保護するための別の方法におけるデータの流れ図である。

【図９】メッセージデータを保護するための別の方法におけるデータの流れ図である。

【図１０】メッセージデータを保護するための別の方法におけるデータの流れ図である。

【発明を実施するための形態】

【００２２】

「例示的」という単語は、本明細書では「例、事例、または例示の働きをすること」を意味するために使用する。「例示的」として本明細書で説明するいかなる実施形態も、必ずしも他の実施形態よりも好ましいまたは有利であると解釈されるべきではない。

【００２３】

図2および図3を参照すると、本発明の一態様は、メッセージデータ310を保護するための方法200に存在し得る。この方法では、メッセージデータは、メッセージデータに対して実施された確定関数330に基づいて生成されたパディングビット320でパディングされる(ステップ210)。パディングされたメッセージデータ335は、圧縮されて、圧縮データ340が生成される(ステップ220)。圧縮データの長さは、パディングビットに依存する。圧縮データは暗号化されて、暗号化メッセージデータ350が生成される(ステップ230)。暗号化関数380は、圧縮データを暗号化するのに、暗号化鍵を使う。この方法は、圧縮メッセージの長さを、圧縮および暗号化されたデータストリームから判断することができないように、圧縮と暗号化の両方がなされているメッセージを安全にする。

【００２４】

本発明のより詳細な態様では、確定関数330は、ハッシュ関数を含み得る。パディングジェネレータ360は、ハッシュ関数から数ビットを取り出して、パディングされたメッセージの長さを決定する。ハッシュ関数からのビットは、ランダム状である。その結果、圧縮データ340は、ランダム状の長さを有する。また、ハッシュ関数からのビットは、ハッシュ関数からのこれらのビットのランダム状の性質により、圧縮されて、ほぼなくなるわけではない。パディングビット320は、メッセージデータ310にプレフィックスまたはプリペンドされてよい。

【００２５】

パディングビット320は、パディングビットの末尾が受信機によって判断されるように制約され得る。たとえば、最終ビットを除くすべてのパディングバイトの最上位ビットは、強制的に0にされてよく、最終バイトの最上位ビットは、強制的に1にされてよい。メッセージ受信機は、このパターンによってパディングの末尾を判断することができる。別の例として、パディングの長さは、最初の5ビットに入れることができる。(最大長さが32バイトであると仮定する)。ビットの残りは、ハッシュ関数330から生じ得る。圧縮関数370および圧縮パラメータ値390については、図6を参照して後で説明する。

【００２６】

図4をさらに参照すると、本発明の別の態様は、メッセージデータに対して実施された確定関数330に基づいて生成されたパディングビット320でメッセージデータ310をパディングするための手段410と、パディングされたメッセージデータ335を圧縮して、圧縮デー

タ340を生成するための手段410であって、圧縮データの長さがパディングビットに依存する手段と、圧縮データを暗号化して、暗号化メッセージデータ350を生成するための手段410とを備える遠隔局102に存在し得る。

【００２７】

本発明の別の態様は、メッセージデータに対して実施された確定関数330に基づいて生成されたパディングビット320でメッセージデータ310をパディングし、パディングされたメッセージデータ335を圧縮して、圧縮データ340を生成し、圧縮データの長さがパディングビットに依存し、圧縮データを暗号化して、暗号化メッセージデータ350を生成するように構成されたプロセッサ410を備える遠隔局102に存在し得る。

【００２８】

本発明の別の態様は、コンピュータ400に、メッセージデータに対して実施された確定関数に基づいて生成されたパディングビット320でメッセージデータ310をパディングさせるためのコードと、コンピュータに、パディングされたメッセージデータ335を圧縮させて、圧縮データ340を生成するためのコードであって、圧縮データの長さがパディングビットに依存するコードと、コンピュータ400に、圧縮データを暗号化させて、暗号化メッセージデータ350を生成するためのコードとを含むコンピュータ可読媒体420を含むコンピュータプログラム製品に存在し得る。

【００２９】

図5および図6を参照すると、本発明の別の態様は、メッセージデータ610を保護するための方法500に存在し得る。この方法では、圧縮関数670の圧縮アルゴリズムの圧縮パラメータ値690が、メッセージデータに対して実施された確定関数630を使って選択される(ステップ510)。メッセージデータは、圧縮アルゴリズムおよび選択された圧縮パラメータ値を使って圧縮されて、圧縮データ640が生成される(ステップ520)。圧縮データの長さは、圧縮パラメータ値に依存する。圧縮データは暗号化されて、暗号化メッセージデータ650が生成される(ステップ530)。暗号化関数680は、圧縮データを暗号化するのに、暗号化鍵および暗号化アルゴリズムを使う。

【００３０】

本発明のより詳細な態様では、圧縮パラメータ値は、最大チェーン長値であってよい。確定関数は、ハッシュ関数630を含み得る。圧縮関数670は、圧縮中に多くの選定を行い得る。DEFLATE関数は、ウェブ上でのデータの圧縮において一般に使われ、圧縮がどの程度積極的であるべきかを、0～9の範囲で示すパラメータを有する。数ビットがハッシュ関数から取り出され、その範囲に変えられ、圧縮関数に対する呼出しに渡され得る。こうすることにより、圧縮関数は、メッセージデータ中で何かが変更された場合、異なる振舞いをすることになる。

【００３１】

DEFLATE関数では、いくつかの値、すなわちgood_length、max_lazy、nice_length、およびmax_chainが、内部調整パラメータとして使われ得る。max_chain値は、たとえば、関数が探す最も長いチェーンのコントロールなどを行う。DEFLATE関数は、これらの調整パラメータを、テーブルから選択される、0と9との間の単一整数としてではなく、個々に受諾するように修正されてよい。調整パラメータは、ハッシュ関数630の出力からのビットの一部を使って選択すればよい。

【００３２】

メッセージデータ610の圧縮は、確定関数に基づいて選択されたいくつかのパディングビットでメッセージデータをパディングして、パディングされたメッセージデータを生成すること、ならびにパディングされたメッセージデータに対して圧縮アルゴリズムおよび選択された圧縮パラメータ値を使って、圧縮データ640を生成することを含み得る。パディングビットは、メッセージデータにプレフィックスされてよい。パディングビットは、パディングビットの末尾が受信機によって判断されるように制約され得る。パディングのランダム化および/または圧縮の有効性により、そのような長さ漏洩タイプの攻撃から保護することができる。

【００３３】
本発明の別の態様は、メッセージデータ610に対して実施された確定関数630を使って、圧縮アルゴリズムの圧縮パラメータ値690を選択するための手段410と、圧縮アルゴリズムおよび選択された圧縮パラメータ値を使ってメッセージデータを圧縮して、圧縮データ640を生成するための手段410であって、圧縮データの長さが圧縮パラメータ値に依存する手段と、圧縮データを暗号化して、暗号化メッセージデータ650を生成するための手段とを備える遠隔局102に存在し得る。
【００３４】
本発明の別の態様は、メッセージデータ610に対して実施された確定関数630を使って圧縮アルゴリズムの圧縮パラメータ値690を選択し、圧縮アルゴリズムおよび選択された圧縮パラメータ値を使ってメッセージデータを圧縮して、圧縮データ640を生成し、圧縮データの長さが圧縮パラメータ値に依存し、圧縮データを暗号化して、暗号化メッセージデータ650を生成するように構成されたプロセッサ410を備える遠隔局102に存在し得る。
【００３５】
本発明の別の態様は、コンピュータ400に、メッセージデータ610に対して実施された確定関数630を使って、圧縮アルゴリズムの圧縮パラメータ値690を選択させるためのコードと、コンピュータに、圧縮アルゴリズムおよび選択された圧縮パラメータ値を使ってメッセージデータを圧縮させて、圧縮データ640を生成するためのコードであって、圧縮データの長さが圧縮パラメータ値に依存するコードと、コンピュータに、圧縮データを暗号化させて、暗号化メッセージデータ650を生成するためのコードとを含むコンピュータ可読媒体420を含むコンピュータプログラム製品に存在し得る。
【００３６】
図7～図10を参照すると、本発明の別の態様は、メッセージデータ810を保護するための方法700に存在し得る。この方法では、メッセージデータは、圧縮されて、第1の数のデータバイトを含む圧縮データ840が生成される(ステップ710)。圧縮データはパディングされて、第2の数のデータバイト837を含む、パディングされた圧縮データ835が生成され、第2の数は、第1の数にデータバイトのパッド数を加えたものに等しく、データバイトのパッド数は、メッセージデータのハッシュに基づいて決定される(ステップ720)。パディングされた圧縮データは暗号化されて、暗号化メッセージデータ850が生成される(ステップ730)。
【００３７】
本発明のより詳細な態様では、メッセージデータ810のハッシュ830は、メッセージデータの鍵付きハッシュ935であってよい。メッセージデータの鍵付きハッシュは、メッセージ認証のためのハッシュ化(HMAC)という暗号学的ハッシュ関数を使って実施することができ、鍵導出関数を使って導出された難読化鍵を使うことができる。難読化鍵は、交換される秘密の値から生成することができる。鍵導出関数は、難読化鍵を生成するのに、暗号化鍵および認証鍵を使うことができる。暗号化鍵および認証鍵は、交換される秘密の値から、および複数の秘密でない値から生成することができる。データバイトのパッド数は、1から32の数を含み得る。
【００３８】
非圧縮テキスト810のハッシュまたは類似の関数を計算することができる。ハッシュ値から、ある程度のパディング837の長さを、何らかの算術または論理演算によって決定することができる。たとえば、演算は、ハッシュの最後の有効な5ビットを使うだけでよい。これは、0と31との間の数であり、追加することができるパディング837のバイトの数である。この技法により、このタイプの攻撃が阻止され、というのは、長さは、各試行数字における多くのバイトによって変わり、正しいものが最も短いものである可能性は低いからである。ハッシュ関数は、難読化鍵などの秘密を含み得る。HMACは、秘密を含む、ハッシュのような関数である(HMACは、鍵付きハッシュと呼ばれることがある)。
【００３９】
秘密は、セッション確立の一部として導出することができる。セッション確立中に暗号

化鍵および認証鍵を導出することが一般的であり、これらの鍵は、長さ難読化鍵を導出するのに使うことができる。長さ難読化鍵は、パディングの長さの計算の一部である。攻撃者は、長さ難読化鍵を知らないので、パディングの長さを計算することはできない。

【００４０】

ある態様は、圧縮関数の演算の修正を伴い得る。圧縮関数は概して、多くの決断を行う。たとえば、圧縮関数はしばしば、最近遭遇したストリングの「辞書」を構築する。ただし、ストレージは限られているので、頻繁な間隔で、辞書中の1つまたは複数のエントリが破棄されなければならない。最も過去に見かけたストリングはしばしば、破棄するために選ばれる。ただし、この選定は、メッセージのハッシュに依存させられ得る。実際の圧縮アルゴリズムでは、行われ得る多くの他の選定があり得る。これらの選択の一部または全部を、メッセージのハッシュ(または鍵付きハッシュ)に依存させることにより、長さにたくさんの「ノイズ」がもたらされる場合がある。

【００４１】

実際のセキュア通信システムでは、一般にプリマスターシークレットと呼ばれる秘密の値を交換し、次いで、鍵導出関数を使って、その値をいくつかの秘密でない値と組み合わせて、暗号化鍵および認証鍵を生成するプロトコルが存在する。パディング難読化鍵など、第3の鍵が、暗号化鍵および認証鍵から導出され得る。

【００４２】

他のより詳細な本発明の態様では、圧縮データ840をパディングして、パディングされた圧縮データを生成するステップは、メッセージデータ810の確定関数に基づいて修正された圧縮アルゴリズム845を使うステップを含み得る。メッセージデータは、トランスポートレイヤセキュリティ(TLS)プロトコルメッセージ、またはセキュアソケットレイヤ(SSL)プロトコルメッセージを含み得る。ハッシュ関数830、パディングジェネレータ860、および暗号化関数880については、図3を参照して上述した。パッド数は、乱数ジェネレータ1035からの乱数に基づいて決定することができる。

【００４３】

本発明の別の態様は、メッセージデータ810を圧縮して、第1の数のデータバイトを含む圧縮データ840を生成するための手段410と、圧縮データをパディングして、第2の数のデータバイトを含むパディングされた圧縮データ835を生成するための手段410であって、第2の数が、第1の数にデータバイトのパッド数を加えたものに等しく、データバイトのパッド数が、メッセージデータのハッシュに基づいて決定される手段と、パディングされた圧縮データを暗号化して、暗号化メッセージデータ850を生成するための手段410とを備える遠隔局102に存在し得る。

【００４４】

本発明の別の態様は、メッセージデータ810を圧縮して、第1の数のデータバイトを含む圧縮データ840を生成し、圧縮データをパディングして、第2の数のデータバイトを含むパディングされた圧縮データ835を生成し、第2の数は、第1の数にデータバイトのパッド数を加えたものに等しく、データバイトのパッド数は、メッセージデータのハッシュに基づいて決定され、パディングされた圧縮データを暗号化して、暗号化メッセージデータ850を生成するように構成されたプロセッサ410を備える遠隔局102に存在し得る。

【００４５】

本発明の別の態様は、コンピュータ400に、メッセージデータ810を圧縮させて、第1の数のデータバイトを含む圧縮データ840を生成するためのコードと、コンピュータに、圧縮データをパディングさせて、第2の数のデータバイトを含むパディングされた圧縮データ835を生成するためのコードであって、第2の数が、第1の数にデータバイトのパッド数を加えたものに等しく、データバイトのパッド数が、メッセージデータのハッシュに基づいて決定されるコードと、コンピュータに、パディングされた圧縮データを暗号化させて、暗号化メッセージデータ850を生成するためのコードとを含むコンピュータ可読媒体420を含むコンピュータプログラム製品に存在し得る。

【００４６】

遠隔局102は、プロセッサ410と、メモリおよび/またはディスクドライブなどの記憶媒体420と、ディスプレイ430と、キーパッドなどの入力440と、ワイヤレス接続450とを含むコンピュータ400を備え得る。

【００４７】

図1を参照すると、ワイヤレス遠隔局(RS)102(移動局MSなど)は、ワイヤレス通信システム100の1つまたは複数の基地局(BS)104と通信することができる。ワイヤレス通信システム100は、1つまたは複数の基地局コントローラ(BSC)106と、コアネットワーク108とをさらに含み得る。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および公衆交換電話網(PSTN)112に接続されてもよい。典型的なワイヤレス移動局は、ハンドヘルド電話またはラップトップコンピュータを含み得る。ワイヤレス通信システム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)、偏波分割多元接続(PDMA)、または当技術分野で知られている他の変調技法などのいくつかの多元接続技法のうちのいずれか1つを採用することができる。

【００４８】

当業者は、情報および信号は様々な異なる技術および技法のいずれかを使用して表され得ることを理解されよう。たとえば、上記の説明全体にわたって言及され得るデータ、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、磁界もしくは磁性粒子、光場もしくは光学粒子、またはそれらの任意の組合せによって表され得る。

【００４９】

当業者は、本明細書で開示する実施形態に関して説明し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が、電子ハードウェア、コンピュータソフトウェア、または両方の組合せとして実装され得ることをさらに諒解されよう。ハードウェアとソフトウェアのこの互換性を明確に示すために、様々な例示的な構成要素、ブロック、モジュール、回路、およびステップについて、上記では概してそれらの機能性に関して説明した。そのような機能性をハードウェアとして実装するか、ソフトウェアとして実装するかは、特定の適用例および全体的なシステムに課される設計制約に依存する。当業者は、説明された機能を特定の適用例ごとに様々な方法で実装し得るが、そのような実装の決定は、本発明の範囲からの逸脱を生じるものと解釈すべきではない。

【００５０】

本明細書で開示される実施形態に関して説明される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ッサ(DSP)、特定用途向け集積回路(ASIC)、フィールドプログラマブルゲートアレイ(FPGA)もしくは他のプログラマブル論理デバイス、個別ゲートもしくはトランジスタ論理、個別ハードウェア構成要素、または、本明細書で説明される機能を実施するように設計されたそれらの任意の組合せによって、実装または実施され得る。汎用プロセッサはマイクロプロセッサであり得るが、代替として、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、または状態機械であり得る。プロセッサはまた、コンピューティングデバイスの組合せ、たとえば、DSPとマイクロプロセッサとの組合せ、複数のマイクロプロセッサ、DSPコアと連携する1つもしくは複数のマイクロプロセッサ、または任意の他のそのような構成として実装することができる。

【００５１】

本明細書で開示された実施形態に関して記載された方法またはアルゴリズムのステップは、直接ハードウェアで具現化されるか、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で具現化されるか、またはその2つの組合せで具現化され得る。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、または当技術分野で知られている任意の他の形態の記憶媒体中に存在し得る。例示的な記憶媒体は、プロセッサが記憶媒体から情報を読み取り、かつ記憶媒体に情報を書き込むことができるように、プロセッサに結合される。代替として、記憶媒体は、プロセッサと一体であり得る。プロセッサ

および記憶媒体はASIC中に常駐し得る。ASICは、ユーザ端末内に常駐し得る。代替として、プロセッサおよび記憶媒体は、ユーザ端末内の個別構成要素として存在することができる。

【００５２】

1つまたは複数の例示的な実施形態では、記載された機能は、ハードウェア、ソフトウェア、ファームウェア、またはそれらの任意の組合せに実装することができる。コンピュータプログラム製品としてソフトウェアに実装された場合、機能は、1つまたは複数の命令またはコードとして、コンピュータ可読媒体上に記憶されるか、またはコンピュータ可読媒体を介して送信され得る。コンピュータ可読媒体は、ある場所から別の場所へのコンピュータプログラムの転送を容易にする任意の媒体を含む、非一時的コンピュータ可読記憶媒体と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され得る任意の利用可能な媒体であり得る。限定ではなく例として、そのようなコンピュータ可読媒体は、RAM、ROM、EEPROM、CD-ROMもしくは他の光ディスク記憶装置、磁気ディスク記憶装置もしくは他の磁気記憶デバイス、または、命令もしくはデータ構造の形態の所望のプログラムコードを搬送もしくは記憶するために用いることができ、コンピュータによってアクセス可能である、任意の他の媒体を含むことができる。また、当然、あらゆる接続がコンピュータ可読媒体と呼ばれる。たとえば、ソフトウェアが、同軸ケーブル、光ファイバケーブル、ツイストペア、デジタル加入者回線(DSL)、または赤外線、無線、およびマイクロ波などのワイヤレス技術を用いて、ウェブサイト、サーバ、または他のリモートソースから送信される場合には、同軸ケーブル、光ファイバケーブル、ツイストペア、DSL、または赤外線、無線、およびマイクロ波などのワイヤレス技術は、媒体の定義に含まれる。本明細書において用いられるとき、ディスク(disk)およびディスク(disc)は、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、デジタル多用途ディスク(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み、ディスク(disk)は、通常、磁気的にデータを再生し、ディスク(disc)は、レーザーで光学的にデータを再生する。上記の組合せもコンピュータ可読媒体の範囲の中に含まれるべきである。

【００５３】

開示された実施形態の上記の説明は、任意の当業者が本発明を作製または使用することを可能にするために提供される。これらの実施形態への様々な修正が当業者には容易に明らかになり、本明細書に定義された一般原理は、本発明の趣旨または範囲を逸脱することなしに他の実施形態に適用することができる。したがって、本発明は、本明細書に示す実施形態に限定されるものではなく、本明細書で開示する原理および新規の特徴に一致する最大の範囲を与えられるものである。

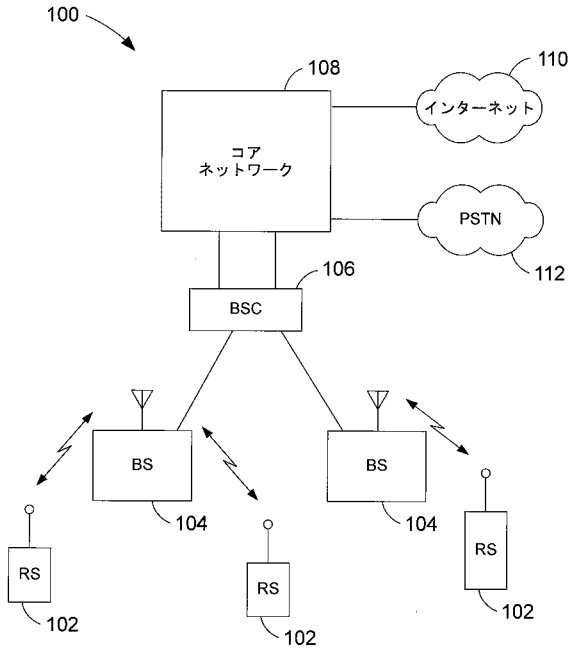
【符号の説明】

【００５４】

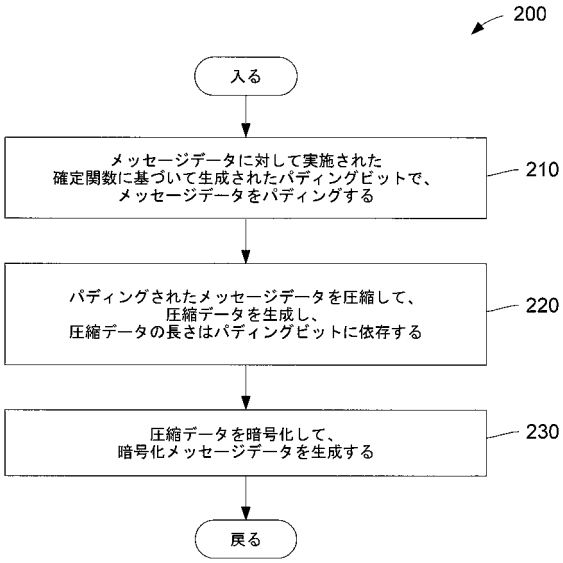
100 ワイヤレス通信システム
102 遠隔局
104 基地局(BS)
106 基地局コントローラ(BSC)
108 コアネットワーク
110 インターネット
112 公衆交換電話網(PSTN)
310 メッセージデータ
320 パディングビット
330 確定関数、ハッシュ関数
335 パディングされたメッセージデータ
340 圧縮データ
350 暗号化メッセージデータ
360 パディングジェネレータ
370 圧縮関数

380 暗号化関数
390 圧縮パラメータ値
400 コンピュータ
410 手段、プロセッサ
420 コンピュータ可読媒体、記憶媒体
430 ディスプレイ
440 入力
450 ワイヤレス接続
610 メッセージデータ
630 確定関数、ハッシュ関数
640 圧縮データ
650 暗号化メッセージデータ
670 圧縮関数
680 暗号化関数
690 圧縮パラメータ値
810 メッセージデータ、非圧縮テキスト
830 ハッシュ、ハッシュ関数
835 パディングされた圧縮データ
837 データバイト、パディング
840 圧縮データ
845 圧縮アルゴリズム
850 暗号化メッセージデータ
860 パディングジェネレータ
880 暗号化関数
935 鍵付きハッシュ
1035 乱数ジェネレータ

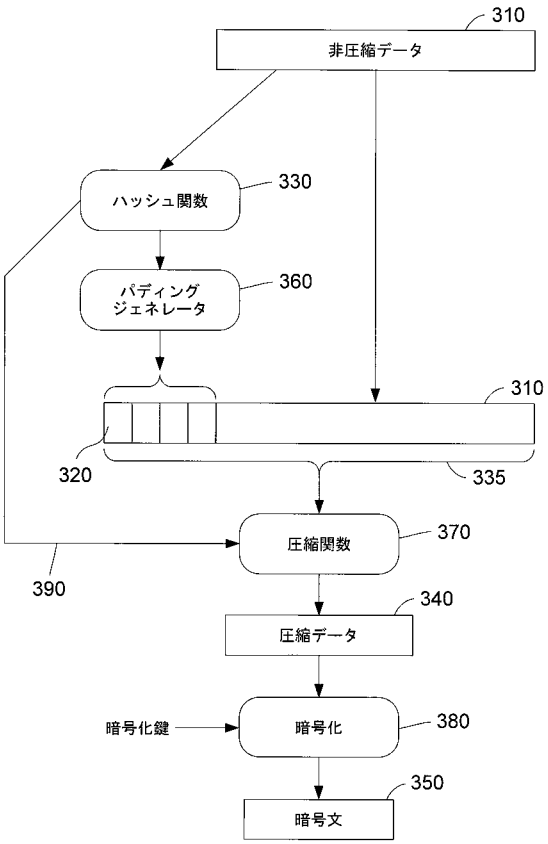
【図１】


100
108
110
インターネット
コア
ネットワーク
PSTN
112
106
BSC
BS
BS
104
104
RS
RS
RS
102
102
102

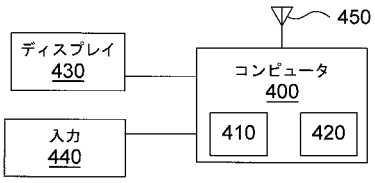
【図２】


200
入る
メッセージデータに対して実施された
確定関数に基づいて生成されたパディングビットで、
メッセージデータをパディングする
210
パディングされたメッセージデータを圧縮して、
圧縮データを生成し、
圧縮データの長さはパディングビットに依存する
220
圧縮データを暗号化して、
暗号化メッセージデータを生成する
230
戻る

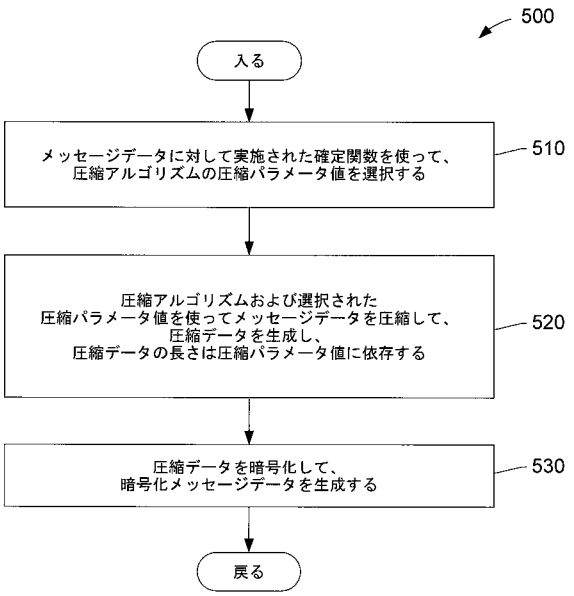
【図３】


310
非圧縮データ
ハッシュ関数
330
パディング
ジェネレータ
360
310
320
335
圧縮関数
370
390
340
圧縮データ
暗号化鍵
暗号化
380
350
暗号文

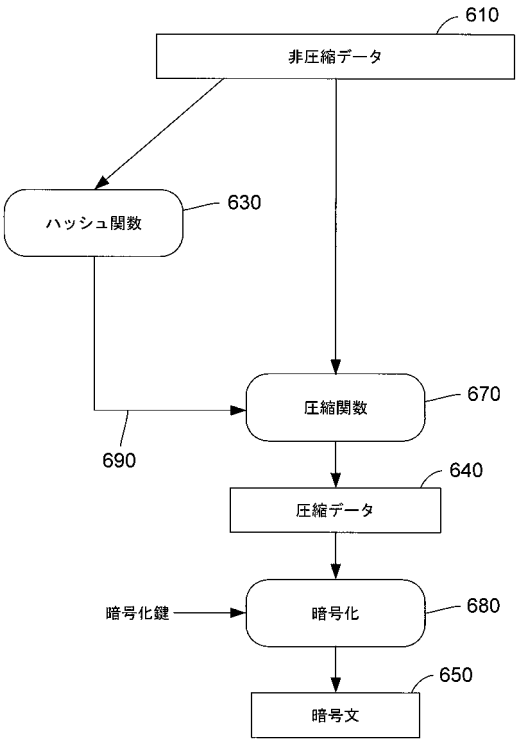
【図４】


450
ディスプレイ
430
コンピュータ
400
410
420
入力
440

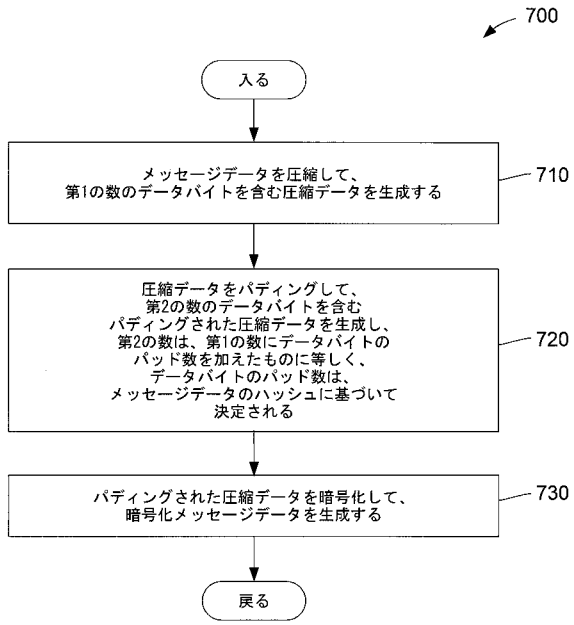
【図５】


500
入る
メッセージデータに対して実施された確定関数を使って、
圧縮アルゴリズムの圧縮パラメータ値を選択する
510
圧縮アルゴリズムおよび選択された
圧縮パラメータ値を使ってメッセージデータを圧縮して、
圧縮データを生成し、
圧縮データの長さは圧縮パラメータ値に依存する
520
圧縮データを暗号化して、
暗号化メッセージデータを生成する
530
戻る

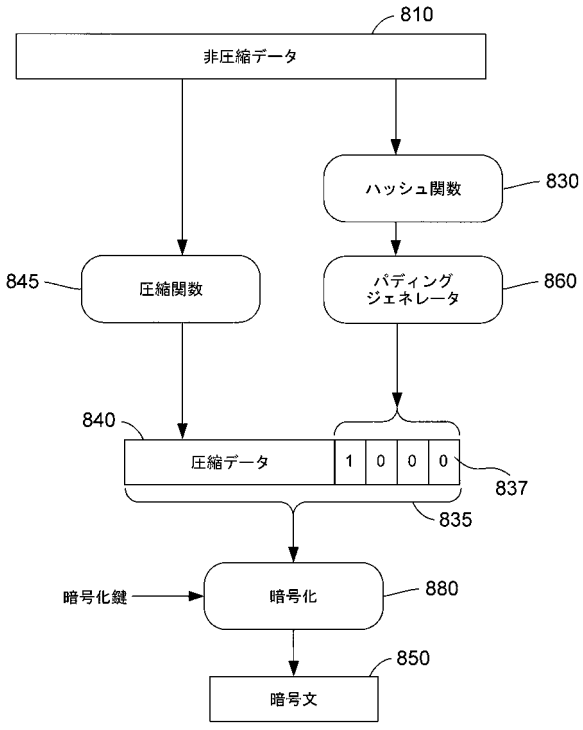
【図６】


610
非圧縮データ
ハッシュ関数
630
690
圧縮関数
670
640
圧縮データ
暗号化鍵
暗号化
680
650
暗号文

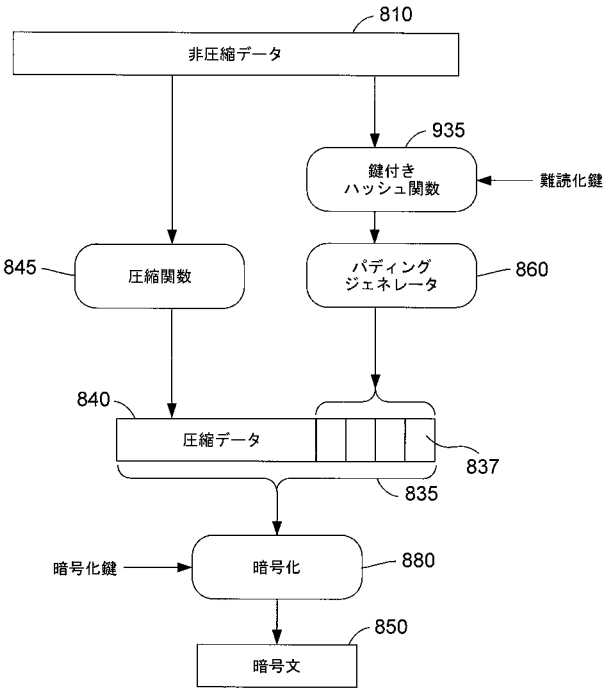
【図７】


700
入る
メッセージデータを圧縮して、
第1の数のデータバイトを含む圧縮データを生成する
710
圧縮データをパディングして、
第2の数のデータバイトを含む
パディングされた圧縮データを生成し、
第2の数は、第1の数にデータバイトの
パッド数を加えたものに等しく、
データバイトのパッド数は、
メッセージデータのハッシュに基づいて
決定される
720
パディングされた圧縮データを暗号化して、
暗号化メッセージデータを生成する
730
戻る

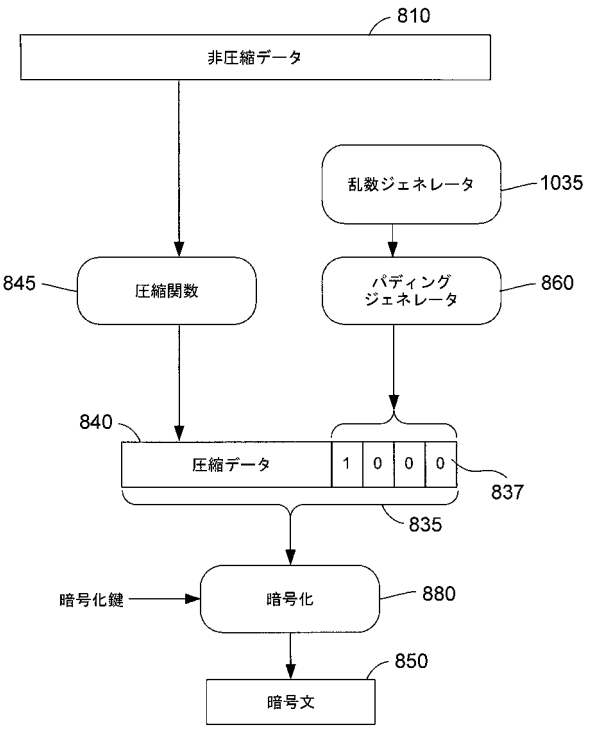
【図８】


810
非圧縮データ
ハッシュ関数
830
845
圧縮関数
パディング
ジェネレータ
860
840
圧縮データ
1
0
0
0
837
835
暗号化鍵
暗号化
880
850
暗号文

【図９】


810
非圧縮データ
935
鍵付き
ハッシュ関数
難読化鍵
845
圧縮関数
パディング
ジェネレータ
860
840
圧縮データ
837
835
暗号化鍵
暗号化
880
850
暗号文

【図１０】


810
非圧縮データ
乱数ジェネレータ
1035
845
圧縮関数
パディング
ジェネレータ
860
840
圧縮データ
1
0
0
0
837
835
暗号化鍵
暗号化
880
850
暗号文

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2013/059524

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L29/06 H04L9/00 H04W12/02 H04W28/06
ADD.

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 H04W

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 practicable, search terms used)
EPO-Internal, WPI Data, INSPEC, COMPENDEX, IBM-TDB

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	John Kelsey ET AL: "Compression and Information Leakage of Plaintext" In: "Fast Software Encryption", 1 January 2002 (2002-01-01), Springer Berlin Heidelberg, Berlin, Heidelberg, XP55095581, ISBN: 978-3-54-044009-3 vol. 2365, pages 263-276, DOI: 10.1007/3-540-45661-9_21, abstract section 1. Introduction section 7. Caveats and Countermeasures ----- -/--	1-80

[X] Further documents are listed in the continuation of Box C. [ ] 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 application or patent 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
13 January 2014	30/01/2014

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, Fax: (+31-70) 340-3016	Poppe, Fabrice

3

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

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2013/059524

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	TURNER S ET AL: "RFC 6151: Updated Security Considerations for the MD5 Message-Digest and the HMAC-MD5 Algorithms", INTERNET ENGINEERING TASK FORCE, 7 March 2011 (2011-03-07), XP015075904, [retrieved on 2011-03-07] section 2. Security Considerations	1-80
A	HOLLENBECK S ET AL: "RFC 3749: Transport Layer Security Protocol Compression Methods", INTERNET ENGINEERING TASK FORCE, 1 May 2004 (2004-05-01), XP015009529, section 6. Security Considerations	1-80
A,P	Ivan Ristic: "CRIME: Information Leakage Attack against SSL/TLS", Security Labs, Qualys Community , 14 September 2012 (2012-09-14), XP55095627, Retrieved from the Internet: URL:https://community.qualys.com/blogs/securitylabs/2012/09/14/crime-information-leakage-attack-against-ssltls [retrieved on 2014-01-09] the whole document	1-80
A,P	Tom Ritter: "Details on the "Crime" Attack", iSEC Partners , 14 September 2012 (2012-09-14), XP55095572, Retrieved from the Internet: URL:https://isecpartners.com/blog/2012/september/details-on-the-crime-attack.aspx [retrieved on 2014-01-09] the whole document	1-80

3

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

フロントページの続き

(81)指定国 AP(BW,GH,GM,KE,LR,LS,MW,MZ,NA,RW,SD,SL,SZ,TZ,UG,ZM,ZW),EA(AM,AZ,BY,KG,KZ,RU,TJ,TM),EP(AL,AT,BE,BG,CH,CY,CZ,DE,DK,EE,ES,FI,FR,GB,GR,HR,HU,IE,IS,IT,LT,LU,LV,MC,MK,MT,NL,NO,PL,PT,RO,RS,SE,SI,SK,SM,TR),OA(BF,BJ,CF,CG,CI,CM,GA,GN,GQ,GW,KM,ML,MR,NE,SN,TD,TG),AE,AG,AL,AM,AO,AT,AU,AZ,BA,BB,BG,BH,BN,BR,BW,BY,BZ,CA,CH,CL,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,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,PA,PE,PG,PH,PL,PT,QA,RO,RS,RU,RW,SA,SC,SD,SE,SG,SK,SL,SM,ST,SV,SY,TH,TJ,TM,TN,TR,TT,TZ,UA,UG,US,UZ

(72)発明者 ビリー・ビー・ブラムリー
アメリカ合衆国・カリフォルニア・９２１２１・サン・ディエゴ・モアハウス・ドライヴ・５７７５

Ｆターム(参考) 5J104 AA08 AA16 AA32 EA04 EA08 EA18 JA03 JA31 LA05 NA02
NA12 NA37 NA38 PA14