(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2008-545163
(P2008-545163A)
(43)公表日　平成20年12月11日(2008.12.11)

(51)Int.Cl.		F I			テーマコード（参考）
G09C 1/00	(2006.01)	G09C	1/00	650Z	5B017
G06F 21/24	(2006.01)	G06F	12/14	560C	5J104
H04L 9/14	(2006.01)	G09C	1/00	640D	
		G09C	1/00	610A	
		H04L	9/00	641	

審査請求 未請求　予備審査請求 未請求　（全 18 頁）

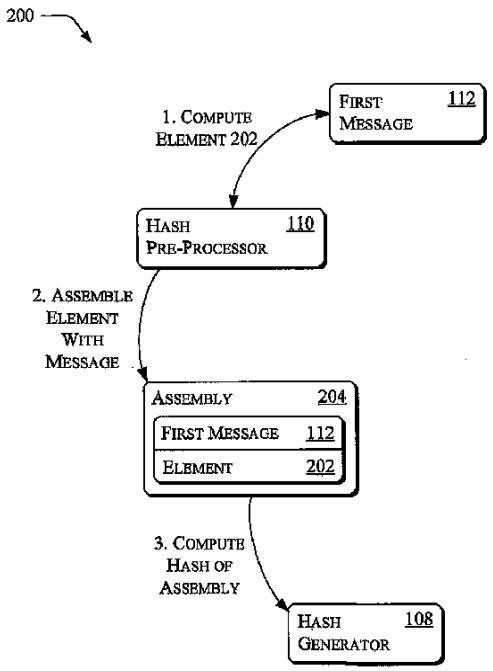
(21)出願番号　特願2008-519339 (P2008-519339)
(86)(22)出願日　平成18年6月13日 (2006.6.13)
(85)翻訳文提出日　平成19年12月28日 (2007.12.28)
(86)国際出願番号　PCT/US2006/022960
(87)国際公開番号　WO2007/001829
(87)国際公開日　平成19年1月4日 (2007.1.4)
(31)優先権主張番号　11/168,842
(32)優先日　平成17年6月28日 (2005.6.28)
(33)優先権主張国　米国 (US)

(71)出願人　500046438
マイクロソフト　コーポレーション
アメリカ合衆国　ワシントン州　９８０５２－６３９９　レッドモンド　ワン　マイクロソフト　ウェイ
(74)代理人　100077481
弁理士　谷　義一
(74)代理人　100088915
弁理士　阿部　和夫
(72)発明者　ギデオン　エー．ユバル
アメリカ合衆国　９８０５２　ワシントン州　レッドモンド　ワン　マイクロソフト　ウェイ　マイクロソフト　コーポレーション　インターナショナル　パテンツ内

最終頁に続く

(54)【発明の名称】セキュアハッシュ関数の強化

(57)【要約】
セキュアハッシュ関数を強化するシステムおよび／または方法を説明する。いくつかの実施形態では、これらのシステムおよび／または方法は、メッセージに基づいて、かつあるプロセスを用いて、無作為に現れる要素を生成し得る。次いで、この要素とメッセージを組み合わせることができる。セキュアハッシュ関数を用いてこのアセンブリをハッシュすることができる。同じプロセスおよびセキュアハッシュ関数を用いて、このメッセージを後で認証することができる。



【特許請求の範囲】
【請求項１】
コンピュータ可読命令を内部に有する１つまたは複数のコンピュータ可読媒体であって、前記命令がコンピュータによって実行されると、前記コンピュータに、
メッセージに基づいて、かつ、あるプロセスを用いて無作為に現れる要素を生成する動作と、
前記要素と前記メッセージとを組み合わせてアセンブリを提供する動作とを実行させ、前記アセンブリは、ハッシュを提供するためにセキュアハッシュ関数でハッシュすることができ、前記ハッシュは、同じセキュアハッシュ関数によって前記メッセージをハッシュして得られる第２のハッシュの長さと同じ長さを有し、
前記プロセスは、第２のメッセージに基づいて第２の無作為に現れる要素を生成することができ、前記第２の無作為に現れる要素は、前記第２のメッセージが前記第１のメッセージと同じ場合には、前記第１の無作為に現れる要素と同じであることを特徴とする媒体。
【請求項２】
前記無作為に現れる要素を生成する前記動作は、ブロック暗号を用いて前記メッセージの部分を暗号化して、暗号化された部分を提供する動作と、前記暗号化された部分と前記メッセージの部分との排他的論理和（ＸＯＲ）を計算して、前記無作為に現れる要素を提供する動作とを含むことを特徴とする請求項１に記載の媒体。
【請求項３】
組み合わせる前記動作は、前記無作為に現れる要素と前記メッセージとを連結する動作を含むことを特徴とする請求項１に記載の媒体。
【請求項４】
前記プロセスは、ブロック暗号を用いて前記メッセージの部分を暗号化して、暗号化された部分を提供する動作と、前記暗号化された部分と前記メッセージの部分との排他的論理和（ＸＯＲ）を計算して、前記無作為に現れる要素を提供する動作とを含むことを特徴とする請求項１に記載の媒体。
【請求項５】
前記無作為に現れる要素を生成する前記動作は、
前記メッセージに基づいて無作為に現れる中間要素を受け取る動作と、
前記無作為に現れる中間要素から無作為に現れる暗号キーを導出する動作と、
前記無作為に現れる暗号キーを利用する暗号関数で前記メッセージの部分を暗号化して暗号化された部分を提供する動作と、
前記暗号化された部分と前記部分との排他的論理和（ＸＯＲ）を計算して、前記無作為に現れる要素を提供する動作とを含むことを特徴とする請求項１に記載の媒体。
【請求項６】
前記暗号関数は、１２８ビットのＡＥＳ（Ａｄｖａｎｃｅｄ　Ｅｎｃｒｙｐｔｉｏｎ　Ｓｔａｎｄａｒｄ）のブロック暗号による暗号関数を含むことを特徴とする請求項５に記載の媒体。
【請求項７】
前記セキュアハッシュ関数は、セキュアハッシュアルゴリズム－１を含むことを特徴とする請求項１に記載の媒体。
【請求項８】
コンピュータ可読命令を内部に有する１つまたは複数のコンピュータ可読媒体であって、前記命令がコンピュータによって実行されると、前記コンピュータに、
データのブロックの第１のサブブロックおよび第２のサブブロックを暗号化して、暗号化された第１のサブブロックおよび暗号化された第２のサブブロックを提供する動作と、
前記第１のサブブロックと前記暗号化された第１のサブブロックとの排他的論理和（ＸＯＲ）を計算して、第１のＸＯＲサブブロックを提供する動作と、
前記第２のサブブロックと前記暗号化された第２のサブブロックとのＸＯＲを計算して

、第２のＸＯＲサブブロックを提供する動作と、
前記第１のＸＯＲサブブロックおよび前記第２のＸＯＲサブブロックと、前記第１のサブブロックおよび前記第２のサブブロックとを組み合わせて、第１の組み合わされたブロックおよび第２の組み合わされたブロックを提供する動作とを実行させることを特徴とする媒体。
【請求項９】
暗号化する前記動作は、前記第１のサブブロックおよび前記第２のサブブロックに対してブロック暗号を実施する動作を含むことを特徴とする請求項８に記載の媒体。
【請求項１０】
暗号化する前記動作は、
前記第２のサブブロックから導出される第１の暗号キーを用いて前記第１のサブブロックを暗号化する動作と、
前記第１のサブブロックから導出される第２の暗号キーを用いて前記第２のサブブロックを暗号化する動作とを含むことを特徴とする請求項８に記載の媒体。
【請求項１１】
暗号化する前記動作は、第３のサブブロックおよび第４のサブブロックを暗号化する動作を含み、前記第１、第２、または第４のサブブロックから導出される第３の暗号キーを用いて前記第３のサブブロックを暗号化する動作と、前記第１、第２、または第３のサブブロックから導出される第４の暗号キーを用いて前記第４のサブブロックを暗号化する動作とをさらに含むことを特徴とする請求項１０に記載の媒体。
【請求項１２】
前記第１の組み合わされたブロックまたは前記第２の組み合わされたブロックは、前記第１のＸＯＲブロック、前記第２のＸＯＲブロック、前記第３のサブブロック、および前記第４のサブブロックの連結体であることを特徴とする請求項１１に記載の媒体。
【請求項１３】
暗号化する前記動作は、ＡＥＳ（Ａｄｖａｎｃｅｄ　Ｅｎｃｒｙｐｔｉｏｎ　Ｓｔａｎｄａｒｄ）のブロック暗号による暗号関数を実施する動作を含むことを特徴とする請求項８に記載の媒体。
【請求項１４】
前記ブロックはメッセージの一部であり、前記媒体は、前記ブロックを前記第１のサブブロックおよび前記第２のサブブロックに分割する動作をさらに含むことを特徴とする請求項８に記載の媒体。
【請求項１５】
前記メッセージを複数のブロックに分割する動作をさらに含み、前記ブロックは、前記複数のブロックの１つであることを特徴とする請求項１４に記載の媒体。
【請求項１６】
前記ブロックの長さは５１２ビットであり、前記サブブロックの長さは１２８ビットであることを特徴とする請求項８に記載の媒体。
【請求項１７】
前記第１および第２の組み合わされたブロックのハッシュを計算する動作をさらに含むことを特徴とする請求項８に記載の媒体。
【請求項１８】
Ａ、Ｂ、Ｃ、およびＤそれぞれをメッセージのある部分とし、Ｅを暗号関数、$_{cd}$を前記部分ＣおよびＤから導出される暗号キー、$_{ab}$を前記部分ＡおよびＢから導出される暗号キーとして、

【数１】

$$C \oplus E_{ab}(C)$$

$$D \oplus E_{ab}(D)$$

$$A \oplus E_{cd}(A)$$

$$B \oplus E_{cd}(B)$$

を計算する動作と、

Ｈをセキュアハッシュ関数として、

【数２】

$$H(C \oplus P \| D \oplus Q \| A \| B \| A \oplus R \| B \oplus S \| C \| D) = h.$$

を計算してハッシュｈを提供する動作とを含むことを特徴とする方法。

【請求項１９】

Ｅは、１２８ビットのＡＥＳ（Ａｄｖａｎｃｅｄ Ｅｎｃｒｙｐｔｉｏｎ Ｓｔａｎｄａｒｄ）による暗号関数を含むことを特徴とする請求項１８に記載の方法。

【請求項２０】

Ｈはセキュアハッシュアルゴリズム－１（ＳＨＡ－１）を含むことを特徴とする請求項１８に記載の方法。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明はセキュアハッシュ関数の強化に関するものである。

【背景技術】

【０００２】

セキュアハッシュ関数は、メッセージを認証するのにしばしば用いられる。例えば、デジタル署名は、セキュアハッシュ関数に依存している。ある人は、セキュアハッシュ関数を使用して計算したドキュメントのハッシュに署名することによって、そのドキュメントにデジタル的に署名することができる。その後、このデジタル署名は、その人が署名したということになっているドキュメントのハッシュを同じハッシュ関数を用いて計算することによって認証することができる。これら第１のハッシュと第２のハッシュが同じであれば、これらのドキュメントは同じものとみなされる。これらのドキュメントが同じであれば、このデジタル署名は信頼できる。

【０００３】

これら２つのドキュメントは、同じものとみなされるだけであり、同じものとわかっているわけではない。というのは、２つの異なるドキュメントのハッシュが同じになることがあり得るからである。これを「衝突」と呼ぶ。

【０００４】

衝突の例を数学用語で示すことができる。セキュアハッシュ関数「Ｈ（Ｍ）」は任意長のメッセージ「Ｍ」に対して演算を行うことができ、固定長のハッシュ「ｈ」を戻すこと

ができると仮定する。そのため、「ｈ＝Ｈ（Ｍ）」になる。ここで、「ｈ」の長さは固定されている。しかし、この場合、メッセージ「$Ｍ_{1}$」が固定長ハッシュ「ｈ」よりも大きければ、２つの異なるメッセージ「$Ｍ_{1}$」および「$Ｍ_{2}$」が等価なハッシュ「ｈ」を有し、「Ｈ（$Ｍ_{1}$）＝Ｈ（$Ｍ_{2}$）」となる可能性が残る。「Ｈ（$Ｍ_{1}$）＝Ｈ（$Ｍ_{2}$）」となる場合、衝突が起こったことになる。

【０００５】

衝突の確率は、任意の特定のメッセージが信頼できる確率を確認するのに重要である。例えば、１６０ビットのハッシュを生成するセキュアハッシュ関数では、２つの無作為なメッセージが同じハッシュを有する確率は$２^{１６０}$分の１である。しかし、一群の無作為なメッセージがあり、この中の任意の２つのメッセージのハッシュが同じになり得るには、このメッセージの集合の大きさは、思うほど大きくなくてよい。ある集合の任意の２つのメッセージが同じハッシュを有することがあり得るためには、この集合は、１６０ビットのハッシュでは、約$２^{８０}$個のメッセージを有するだけでよい。

【０００６】

したがって、衝突を起こさせようとする場合、すなわち、２つのドキュメントが同じハッシュをもつようにしようとする場合、１６０ビットのハッシュでは、約$２^{８０}$回またはそれよりも少ない試みでこのような衝突を１回起こすことができる。例えば、ウィリーがジョージを詐欺にかけたいとする。ウィリーは、２つの契約書を作成することができるはずである。一方はジョージに有利なものであり、他方はウィリーに極めて有利なものである。ウィリーは、これらのドキュメントにそれぞれ小さな変更を加え（例えば、スペースを追加し）、各ドキュメントについてハッシュを計算することができる。ウィリーは、このように変更を加えたウィリーに有利な契約書の１つについてのハッシュ値がジョージに有利な契約書の１つについてのハッシュ値と一致するまで、この操作を継続することができる。こうすることによって、ウィリーは、ジョージに有利な契約書「$Ｍ_{g}$」とウィリーに有利な契約書「$Ｍ_{w}$」の間で衝突を起こすことができ、その結果「Ｈ（$Ｍ_{g}$）＝Ｈ（$Ｍ_{w}$）」になる。ウィリーは、そうした後で、ジョージに、ある手順を用いてジョージに有利な契約書に署名させ、ここでジョージはハッシュ値「ｈ」に署名することになる。その後なんらかの時点で、ウィリーは、ジョージが署名したジョージに有利な契約書を、ジョージが署名していないウィリーに有利な契約書にすり替える。これで、ウィリーは、審判者（例えば、司法裁判所の裁判官）に、ウィリーに有利な契約書にジョージが署名したことを納得させることができる。というのは、ウィリーに有利な契約書のハッシュが、ジョージに有利な契約書についてのジョージの署名のハッシュ値「ｈ」と一致するからである。

【０００７】

１６０ビットのハッシュのような大きなハッシュでこのような衝突を起こさせることは、最近まで極めて困難であると考えられていた。$２^{８０}$個のメッセージについてハッシュを改変し計算するには、何百台ものコンピュータでも、現在の処理スピードでは何百年ないし何千年もかかる。しかし、最近では、制御された小さな変更をメッセージのビットに加えることによって、$２^{６９}$個のメッセージで衝突は可能であると言う人もいる。これが本当なら、現在の処理スピードでも数ヶ月で、数百台のコンピュータを使用して衝突を起こすことが可能になり得る。今後、５年ないし１０年のうちに、おそらくは、１台のコンピュータで１年もかからずに衝突を起こすことができるようになるかもしれない。

【発明の開示】

【発明が解決しようとする課題】

【０００８】

このようなことが具体的に可能であり、また、他の種類の攻撃では、潜在的には理想よりも簡単に衝突が起こるので、人々は、ある種のセキュアハッシュ関数の安全性および有用性を疑うようになった。

【課題を解決するための手段】

【０００９】

セキュアハッシュ関数を強化するシステムおよび／または方法（「ツール」）を説明する。いくつかの実施形態では、これらのツールは、メッセージに基づいて無作為に現れる要素を生成し得る。次いで、これらのツールは、要素とメッセージを組み合わせることができる。セキュアハッシュ関数を用いてこの組合せ体（アセンブリ）をハッシュすることができる。ここで、得られたハッシュは、同じセキュアハッシュ関数で、要素を伴わないメッセージから計算されたハッシュと同じ長さのものである。こうすることにより、これらのツールは、衝突を起こそうとするある種の攻撃の有効性を削減することによりセキュアハッシュ関数を強化することができる。

【００１０】

いくつかの他の実施形態では、これらのツールは、メッセージのサブブロックを暗号化し、これらのサブブロックと暗号化されたサブブロックの排他的論理和（ＸＯＲ）を計算し、これらのサブブロックとＸＯＲサブブロックを組み合わせることができる。こうすることによって、メッセージのビット操作では容易に制御可能にならないビットの再現可能なアセンブリをハッシュすることができる。こうして得られたハッシュは、メッセージそのものから計算されたハッシュよりも安全になり得る。

【００１１】

この「発明の開示」は、「発明を実施するための最良の形態」で以下にさらに説明する概念を抜粋し簡略化して紹介するためのものである。この「発明の開示」は、特許請求の範囲に記載された主題の主要な、または不可欠な特徴を特定することを意図するものではなく、また、特許請求の範囲に記載された主題の範囲を決定する助けとして用いることを意図するものでもない。

【００１２】

以下の開示および図を通して、同じ番号を用いて同様の構成要素および特徴を参照する。

【発明を実施するための最良の形態】

【００１３】

概要

以下、セキュアハッシュ関数を強化し得る１つ（または複数）のシステムおよび／または１つ（または複数）の方法（「ツール」）を説明する。これらのツールは、衝突を起こさせようとするある種の攻撃の有効性を削減することによってセキュアハッシュ関数を強化し得る。例えば、これらのツールは、制御された小さな変更をメッセージのビットに加えることに基づく攻撃に対してセキュアハッシュ関数を強化し得る。

【００１４】

いくつかの実施形態では、これらのツールは、メッセージに基づいて、かつ、あるプロセスを用いて、無作為に現れる要素を生成し得る。次いで、これらのツールは、この要素とメッセージを組み合わせることができる。このアセンブリはセキュアハッシュ関数を用いてハッシュすることができ、得られたハッシュは、同じセキュアハッシュ関数で、このメッセージから計算されたハッシュと同じ長さのものである。別のメッセージに基づいて、かつ、同じプロセスを用いて、別の無作為に現れる要素を生成することもでき、得られた別の無作為に現れる要素は、これらのメッセージが同じであれば、最初の無作為に現れる要素と同じある。こうすることによって、将来のある時点で、この別のメッセージから別のアセンブリを生成し得る。ここで、この別のアセンブリから計算されたハッシュは、これらのメッセージが同じ場合には、最初のアセンブリから計算されたハッシュと同じになる。こうすることによってメッセージが認証される。

【００１５】

別の実施形態では、これらのツールは、メッセージのブロックに対してブロック暗号を実施し、その結果、暗号化されたブロックが得られる。次いで、これらのツールは、暗号化されたブロックと上記ブロックの加算、減算、または排他的論理和（「ＸＯＲ」）などの演算を行い、その結果、加算、減算、またはＸＯＲによるブロックが得られる。その後、これらのツールは、加算、減算、またはＸＯＲによるブロックと、上記ブロックとを組

み合わせ、その結果、組み合わされたブロックが得られる。次いで、これらの組み合わされたブロックをハッシュすることができる。こうして組み合わされたブロックのビットは、メッセージのビットを改変することによって容易に制御できるようにはならず、メッセージのビットを注意深く改変することによって衝突を起こそうとする試みが潜在的に妨げられる。

【００１６】

別の実施形態では、これらのツールは、メッセージのブロックをサブブロックに分割することもできる。次いで、これらのツールは、これらのサブブロックの１つまたは複数に基づいて暗号キーを計算する。これらのツールは、このキーを含む暗号関数でサブブロックを暗号化し、それによって、暗号化されたサブブロックが提供される。ここで、このキーは、暗号化されるサブブロックとは異なるサブブロックから計算する。この操作は、暗号化されたサブブロックの数が上記サブブロックの数に等しくなるまで繰り返すことができる。次いで、暗号化されたサブブロックと上記サブブロックを連結する。この連結の結果、上記ブロックと同じサイズの２つの連結されたブロックが得られる。これらの連結されたブロックはそれぞれ、サブブロックおよび暗号化されたサブブロックを備える。これらのツールはまた、サブブロックと暗号化されたサブブロックを備えるように、連結された各ブロックを構築することができ、これら暗号化されたサブブロックは、これら２つの連結されたブロックの他方のブロックのサブブロックから計算されたキーを用いて暗号化される。これらの連結されたブロックをセキュアハッシュ関数でハッシュすることができる。

【００１７】

動作環境の例

これらのツールを詳細に説明する前に、以下に動作環境の例を論じて、どこで、かつどうやってこれらのツールを採用し得るかを理解する助けとする。以下の説明は一例を示しているが、これらのツールを１つの特定の動作環境にだけ限定して応用することを意図するものではない。

【００１８】

図１に、１つのこのような動作環境を全体的に１００で示す。動作環境１００は、１つ（または複数）のプロセッサ１０４およびコンピュータ可読媒体１０６を含むコンピュータ１０２を備える。これらのプロセッサは、コンピュータ可読媒体１０６にアクセスし、かつ／またはそれらを実行することができる。コンピュータ可読媒体は、セキュアハッシュを計算し得るハッシュ生成器１０８と、セキュアハッシュ関数を強化し得るハッシュプリプロセッサ１１０と、第１メッセージ１１２および第２メッセージ１１４の２つのメッセージとを備えるか、あるいはこれらにアクセスし得る。

【００１９】

メッセージの前処理

以下の説明では、動作環境１００の要素が、あるメッセージのハッシュを計算する前に、このメッセージを処理することによってセキュアハッシュ関数を強化し得る方法の例を論じる。このプロセスは、敵対者によるハッシュ計算対象ビット制御を削減するのに有効である。

【００２０】

図２を参照すると、第１メッセージ１１２を処理するための流れ図の例２００が示されている。流れ図２００には、環境１００の要素による１組の動作と、これらの動作に付随する要素間の通信とを示す。これらの動作および付随する通信を矢印で示す。この流れ図は、任意の適切なハードウエア、ソフトウエア、ファームウエア、またはこれらの組合せで実施し得る。ソフトウエアおよびファームウエアの場合、この図は、コンピュータが実行可能な命令として実施される演算の組を表す。

【００２１】

矢印１のところで、ハッシュプリプロセッサ１１０は、第１メッセージ１１２に基づいて、再現性があり、無作為に現れる要素２０２を計算する。この要素は、先のツールによ

り、このメッセージの一部およびこのメッセージの暗号化部分の論理演算、例えば、以下の実施形態で説明する論理演算を行うことによって計算することができる。要素２０２は、実際には無作為ではないが、第１メッセージのビットの変更では容易に制御されない程度に十分に無作為に現れる。この要素は再現可能である。すなわち、同じメッセージと、要素を生成するための同じ手順とに基づいて同じ要素を生成することができる。従って、２つの同じメッセージを同じやり方で処理し、得られるアセンブリを同じハッシュ関数を用いてハッシュすると、これらの同じメッセージのハッシュは同じになる。このようにして、このハッシュを用いてメッセージを認証することができる。

【００２２】

矢印２のところで、ハッシュプリプロセッサ１１０は、第１メッセージ１１２および要素２０２を含むアセンブリ２０４を構築する。このアセンブリは、容易には制御し得ないビットを含む。そのため、このアセンブリは、第１メッセージ１１２のビットと、これらのビットに依存するビット（要素２０２）とを含み、このアセンブリのビットは、第１メッセージを操作することによる悪意のある操作を容易には受けない。この実施形態では、このアセンブリは、第１メッセージに基づいてこのアセンブリが再現し得るように上記要素と第１メッセージを任意に組み合わせたものとし得る。

【００２３】

矢印３のところで、ハッシュ生成器１０８は、このアセンブリのハッシュを計算する。このハッシュは、ハッシュ生成器のハッシュ関数と同じハッシュ関数および同じ要素を用いて第１メッセージを認証するのに有効である。この要素は、ハッシュプリプロセッサによって同じやり方で同じ第１メッセージを処理することによって同じものになる。

【００２４】

この実施形態では、ハッシュ生成器１０８は改変されない。そうではなくて、ハッシュ計算の対象であるビットを改変するのであり、ハッシュ関数自体を改変するのではない。こうすると、標準のセキュアハッシュ関数およびシステム、例えば、セキュアハッシュアルゴリズム－１（「ＳＨＡ－１」）およびセキュアハッシュシステム（ＳＨＳ）を使用し続けることができる。

【００２５】

敵対者は、あるメッセージ自体のビットを完全に制御し得ることがあるが、流れ図２００で説明したようにこのメッセージを前処理することによって、敵対者は、ハッシュ計算の対象であるこれらのビットの多くを制御することができなくなる。というのは、ハッシュは、メッセージそのものからではなく、前処理したメッセージから計算されるからである。現在は、衝突（２つの異なるメッセージで同じハッシュ）を起こしたい敵対者は、メッセージのハッシュ予定ブロックの開始ビットに、制御された小さな変更を加えることによって衝突を起こそうとし得る。しかし、先のツールは、流れ図２００に従って、敵対者のメッセージと別のメッセージの衝突の確率を上げる敵対者の能力を削減することができる。敵対者がメッセージに小さな変更を加えると、前処理されたメッセージは大きく改変されることになり、敵対者の衝突生成能力は潜在的に減る。

【００２６】

ブロック暗号化および排他的論理和演算

以下の節では、先のツールがブロック暗号化および排他的論理和演算を用いてセキュアハッシュ関数を強化する方法の例を説明する。以下の説明は特許請求する主題の適用範囲を限定するものではないことを理解されたい。

【００２７】

図３に、プロセスの例３００を示す。ここで、プロセスの例３００は、個々の演算または動作を表す一連のステップとして示されている。以下で説明する実施形態では、ハッシュプリプロセッサ１１０などの図１の動作環境１００の要素がこのプロセスを実施する。本明細書で開示する上記その他のプロセスは、任意の適切なハードウエア、ソフトウエア、ファームウエア、またはこれらの組合せで実施し得る。ソフトウエアおよびファームウエアの場合、これらのプロセスは、コンピュータが実行可能な命令として実施される１組

の演算を表し、これらの命令は、コンピュータ可読媒体１０６に格納され、１つ（または複数）のプロセッサ１０４によって実行可能なものである。

【００２８】

ステップ３０２では、メッセージがブロックに分割される。これらのブロックは、セキュアハッシュ関数が扱い得るサイズのものとし得る。図４に示す実施形態では、ハッシュプリプロセッサ１１０は、第１メッセージ１１２を一連の５１２ビットのブロックに分割する。これらのブロックのうち３つを４０２で示す。

【００２９】

ステップ３０４では、メッセージがサブブロックに分割される。各サブブロックは、ブロック４０２などのより大きなブロックから分割することができる。図に示す実施形態では、各ブロック４０２から４つの１２８ビットのサブブロック４０４に分割される。これらのブロックの１つから分割されたサブブロックを「Ａ」、「Ｂ」、「Ｃ」、および「Ｄ」と名付けて示す。

【００３０】

ステップ３０６では、メッセージのサブブロックが暗号化されて、暗号化されたサブブロックが得られる。一実施形態では、ステップ３０６で、メッセージのサブブロックが暗号化されて、暗号化されたサブブロックが得られるが、サブブロックの数は任意とし得る。

【００３１】

「Ｋ」、「Ｌ」、および「Ｔ」と称する３つの演算を実施し得る。関数Ｋはキーを生成する。関数Ｌは、このキーが公開された場合でも暗号を不可逆性にするパッドを生成する。関数Ｔは、サブブロックの変換が高い確率で１対１のままであることを保証するタグ（「ｔ」）を生成する。上記は、４つのサブブロックＡ、Ｂ、Ｃ、およびＤで数学的に以下のように表し得る。

Ｋ（Ａ，Ｂ，Ｃ，Ｄ）＝α，β，γ，δ

Ｌ（Ａ，Ｂ，Ｃ，Ｄ）＝Ａ’，Ｂ’，Ｃ’，Ｄ’

T_{key}（Ａ，Ｂ，Ｃ，Ｄ）＝ｔ

より一般には、上記は、次のように数学的に表し得る。

E_{α}（Ａ）＝Ｒ、E_{β}（Ｂ）＝Ｓ、E_{γ}（Ｃ）＝Ｐ、E_{δ}（Ｄ）＝Ｑ

Ｕ＝Ｒ＋Ａ’、Ｖ＝Ｓ＋Ｂ’、Ｗ＝Ｐ＋Ｃ’、Ｘ＝Ｑ＋Ｄ’

$T_{U,V,W,X}$（Ａ，Ｂ，Ｃ，Ｄ）＝ｔ

上記出力ｔ、Ｕ、Ｖ、Ｗ、およびＸを用いて、あるケースを示すことができる。ここで、

Ｋ（Ａ，Ｂ，Ｃ，Ｄ）＝ＣＤ，ＣＤ，ＡＢ，ＡＢ

Ｌ（Ａ，Ｂ，Ｃ，Ｄ）＝Ａ，Ｂ，Ｃ，Ｄ

T_{key}（Ａ，Ｂ，Ｃ，Ｄ）＝Ａ，Ｂ，Ｃ，Ｄ

である。

【００３２】

敵対者にキーとしてＡＢを選択させないように、関数Ｋを次のようにし得る。

Ｋ（Ａ，Ｂ，Ｃ，Ｄ）＝ＣＤ，ＣＤ，ＲＳ，ＲＳ

これらのブロックをさらに混ぜ合わせるには、別の全単射関数を用いることもできる。

【００３３】

上記プロセスの例を以下に示す。ここで、ステップ３０６では、元のサブブロックＡ、Ｂ、Ｃ、およびＤがブロック暗号で暗号化される。ステップ３０６では、ハッシュプリプロセッサ１１０を使用してそうすることができ、それによって、暗号キー「$_{n}$」を含む暗号関数「E_{n}」を用いてサブブロックＡが暗号化される。ここで、「Ｒ」は、サブブロックＡを暗号化した結果であり、暗号化されたサブブロックと呼ぶ。暗号キーは、同じブロックから分割された別のサブブロックのビットから導出され、この場合は、サブブロックＢ、Ｃ、Ｄ、またはＢ、Ｃ、および／またはＤの組合せのいずれかである。この実施形態では、このキーは、サブブロックＣおよびＤから導出され、そのため、「$_{cd}$」と名付け

る。これは数学的に次のように表すことができる。
E_{cd}（Ａ）＝Ｒ
使用する暗号関数は、１２８ビットの新暗号規格（Ａｄｖａｎｃｅｄ　Ｅｎｃｒｙｐｔｉｏｎ　Ｓｔａｎｄａｒｄ）（「ＡＥＳ」）による暗号関数とし得る。このキーは、このキーが１つまたは複数の他のサブブロックに基づき、かつ再現可能にもなるように、他のサブブロックから導出し得る。

【００３４】

同様に、ステップ３０６では、他の暗号化されたサブブロックを提供するのに有効な他のサブブロックＢ、Ｃ、およびＤを暗号化し得る。これらは数学的に以下のように表される。
E_{cd}（Ｂ）＝Ｓ
E_{ab}（Ｃ）＝Ｐ
E_{ab}（Ｄ）＝Ｑ
このように、いくつかの暗号化されたサブブロックが構築される。これらのサブブロックはそれぞれ、再現可能であり、１つまたは複数のサブブロックのビットに基づくものである。

【００３５】

ステップ３０８では、サブブロックと暗号化されたサブブロックの排他的論理和（ＸＯＲ）が計算され、それによって、ＸＯＲサブブロックが得られる。

【００３６】

ここでは、ハッシュプリプロセッサ１１０が、排他的論理和（数学的な表記ではＸＯＲまたは

【００３７】

【数１】

“⊕”

【００３８】

）を計算し、以下の結果が得られる。

【００３９】

【数２】

$C \oplus P$

$D \oplus Q$

$A \oplus R$

$B \oplus S$

【００４０】

これらの結果はそれぞれ無作為に現れ、敵対者の制御下には簡単には入らない。そのため、敵対者が悪意をもってＡ、Ｂ、Ｃ、またはＤのビットを、例えば、制御された小さな変更で改変したとしても、ＸＯＲサブブロックを、Ａ、Ｂ、Ｃ、またはＤのビットを改変する際に許されるような制御レベルで悪意をもって選択することはできない。

【００４１】

ステップ３１０では、サブブロックとＸＯＲサブブロックが組み合わされて、組み合わされたブロックが得られる。組み合わされた各ブロックのビットサイズは、上記ブロックのビットサイズと同じとし得る。ただし、組み合わされたブロックの数は、それらの基になるブロックの数の２倍になり得る。

【００４２】

図に示すように、サブブロックＡ、Ｂ、Ｃ、およびＤは、ＸＯＲブロック

【００４３】

【数３】

$$C \oplus P,\ D \oplus Q,\ A \oplus R,\ \text{および}\ B \oplus S$$

【００４４】

に連結される。これらは組み合わされて、ここでは、

【００４５】

【数４】

$$C \oplus P \| D \oplus Q \| A \| B$$

【００４６】

および

【００４７】

【数５】

$$A \oplus R \| B \oplus S \| C \| D$$

【００４８】

の２つの組み合わされたブロックになる。

【００４９】

図４に、これらのブロックを４０６で示す。これらの組み合わされたブロックはそれぞれ、メッセージのビットに加えられる制御された小さな変更では容易に制御可能にならない要素を含む。また、これらの要素により、メッセージのビットに制御された小さな変更を加えて衝突を起こそうとすることがより難しくなる。

【００５０】

これらの組み合わされたブロックはそれぞれ、これらのブロックの基となるメッセージのブロックと同じやり方でハッシュすることができるサイズのものとし得る。セキュアハッシュ関数の多くは、より長い計算時間が必要にはなるものの、同じサイズの追加のブロックを容易に扱うことができる。

【００５１】

ステップ３０４、３０６、３０８、および／または３１０は、メッセージの各ブロック、あるいは１つまたは複数の他のブロックに対して繰り返すことができる。これらの動作を繰り返すことによって、メッセージの大部分または全部を前処理して、図に示す実施形態のＸＯＲブロックなどの再現可能な無作為に現れる要素を備えることができる。

【００５２】

ステップ３１２では、サブブロックとＸＯＲサブブロックのアセンブリに対してセキュアハッシュ関数の計算を行う。メッセージが２つ以上のブロックを含む場合（そうなることが多いが）、セキュアハッシュ関数の計算は、サブブロックとＸＯＲサブブロックの複数のアセンブリに対して行われる。図に示す実施形態では、ハッシュ生成器１０８は、ＳＨＡ－１を利用して、サブブロックとＸＯＲサブブロックのアセンブリの１６０ビットのハッシュを計算する。そうすることによって、メッセージに基づいており、かつこのメッ

セージから再現可能なハッシュを計算することができる。

【００５３】

例えば、図３に示したやり方で第２メッセージ１１４を処理する場合、第２メッセージについて得られるハッシュは、第２メッセージ１１４と第１メッセージ１１２が同じであれば、第１メッセージ１１２のハッシュと同じになる。これらのハッシュが同じに場合に、第１メッセージまたは第２メッセージを認証することができる。これらが同じでない場合、第１メッセージと第２メッセージは同じでないことがわかる。

【００５４】

暗号キー

以下の説明では、メッセージを前処理する際に用いる暗号キーに対する潜在的な制御性を削減することによって先のツールがセキュアハッシュ関数を強化する方法の例を論じる。図２または図３で説明したように、これらのツールは、１つには、ある要素を生成することによってセキュアハッシュ関数を強化する。この要素は、敵対者が、この要素を導出するメッセージのビットを操作することによっては容易に制御可能にならないものである。

【００５５】

図５に、暗号キーに対する制御を削減するためのプロセスの例５００を示す。プロセス５００は、ハッシュプリプロセッサ１１０などの図１の動作環境１００の要素によって実施される個々の演算または動作を表す一連のステップとして示されている。

【００５６】

ステップ５０２では、メッセージから再現可能な無作為に現れる要素が導出される。図６に示す実施形態では、ステップ３０８から得られたＸＯＲサブブロック６０２が提供される。この実施形態では、これらのＸＯＲサブブロックおよびそれらの構成要素である暗号化されたサブブロックＰ、Ｑ、Ｒ、およびＳは中間物である。というのは、これらの中間物を用いて要素を構築し、これらの要素を組み合わせてハッシュするためのブロックにするが、これら自体はハッシュすることはできないからである。

【００５７】

そのため、以下のものを受け取ることができる。

【００５８】

【数６】

$$C \oplus P$$

$$D \oplus Q$$

$$A \oplus R$$

$$B \oplus S$$

【００５９】

ステップ５０４では、メッセージから導出された再現可能な無作為に現れる要素から、無作為に現れる暗号キーが導出される。ここでは、ハッシュプリプロセッサ１１０が、図６に示すＸＯＲサブブロック６０２に基づいて無作為に現れる暗号キー「$RAE-n$」を構築する。ここで、「n」は、キーを導出する１つ（または複数）の要素を表す。これは、次のように表し得る。

【００６０】

【数７】

$$C \oplus P \,\|\, D \oplus Q \rightarrow \text{RAE-cpdq}$$

$$A \oplus R \,\|\, B \oplus S \rightarrow \text{RAE-arbs}$$

【００６１】

ステップ５０６では、無作為に現れる暗号キー（「ＲＡＥキー」）を用いてメッセージの一部が暗号化される。ここでは、図３のステップ３０４から得られたサブブロック４０４　Ａ、Ｂ、Ｃ、およびＤが、ステップ５０４でＸＯＲサブブロック６０２から導出されたＲＡＥキーを用いて暗号化される。これにより、ＲＡＥキーにより暗号化されたサブブロック６０４が得られ、これらをＶ、Ｗ、Ｔ、およびＵと名付ける。このように、サブブロック４０４は、ＲＡＥキー$_{RAE-n}$を含む暗号関数Ｅ$_{n}$を用いて暗号化され、それによって、ＲＡＥキーにより暗号化されたサブブロックが得られる。

【００６２】

これは、数学的に次のように表される。

$E_{RAE-cpdq}$（Ａ）＝Ｖ
$E_{RAE-cpdq}$（Ｂ）＝Ｗ
$E_{RAE-arbs}$（Ｃ）＝Ｔ
$E_{RAE-arbs}$（Ｄ）＝Ｕ

その結果、これらのＲＡＥキーにより暗号化されたサブブロックは、図３のプロセス３００に従う暗号化ブロックとして扱うことができる。ここで、Ｐ＝Ｔ、Ｑ＝Ｕ、Ｒ＝Ｖ、およびＳ＝Ｗである。例えば、図３のステップ３０８およびステップ３１０に従って、以下の組み合わされたブロック６０６

【００６３】

【数８】

$$C \oplus T \,\|\, D \oplus U \,\|\, A \,\|\, B$$

【００６４】

および

【００６５】

【数９】

$$A \oplus V \,\|\, B \oplus W \,\|\, C \,\|\, D$$

【００６６】

が得られる。

【００６７】

結論

以上説明したシステムおよび方法により、セキュアハッシュ関数が強化される。これらのシステムおよび方法により、メッセージ間で衝突を起こさせようとするある種の攻撃の有効性を著しく低減し得る。そうすることによって、セキュアハッシュ関数を用いて、より高度の確かさでメッセージを認証することができる。構造的な特徴および／または方法上の動作に固有の用語でこうしたシステムおよび方法を説明してきたが、添付の特許請求

の範囲で定義されるシステムおよび方法は、上記で説明した特定の特徴または動作に必ずしも限定されないことを理解されたい。そうではなくて、これら特定の特徴および動作は、特許請求の範囲に記載されたシステムおよび方法を実施する形態の例として開示されるものである。

【図面の簡単な説明】

【００６８】

【図１】様々な実施形態が動作し得る動作環境の例を示す図である。

【図２】メッセージを処理するための流れ図の例である。

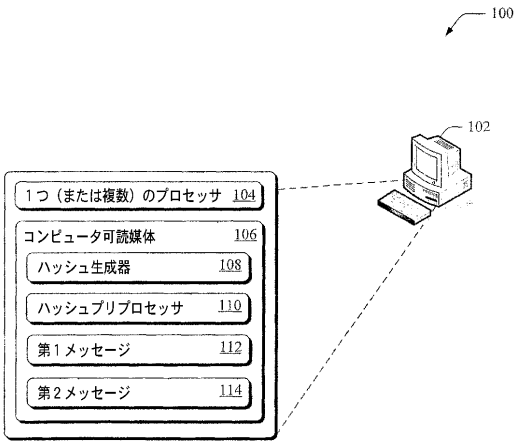
【図３】ブロック暗号化および排他的論理和演算を用いてハッシュ関数を安全なものにするためのプロセスの例を示す図である。

【図４】メッセージのブロック、ブロックのサブブロック、および組み合わされたブロックの例を示す図である。

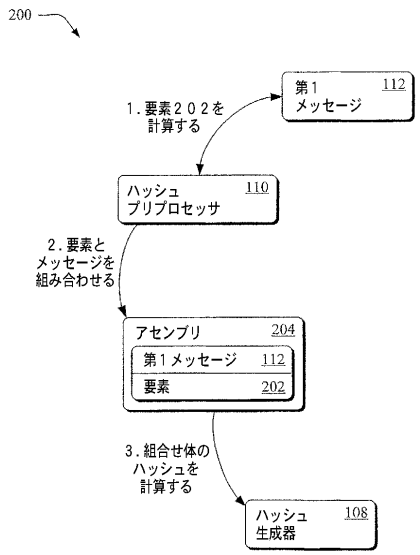
【図５】暗号キーに対する制御を削減するためのプロセスの例を示す図である。

【図６】メッセージのＸＯＲブロック、暗号化されたサブブロック、および組み合わされたブロックの例を示す図である。

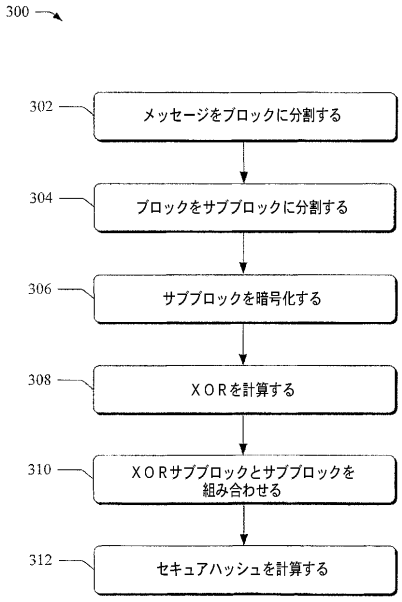
【図１】



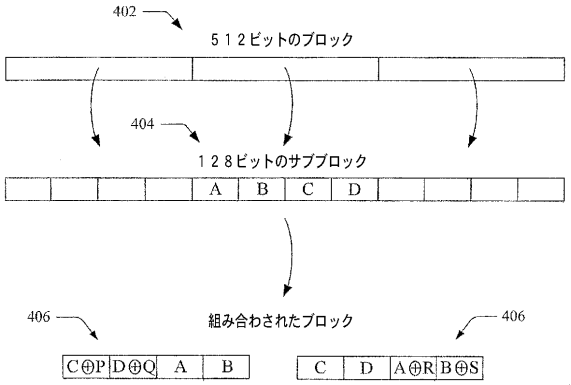
【図２】



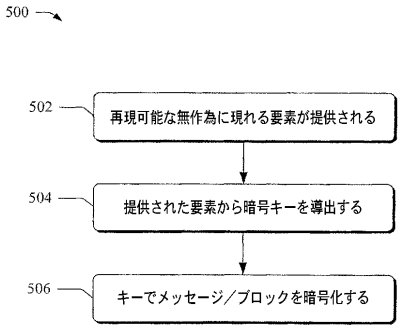
【図３】


300
302
メッセージをブロックに分割する
304
ブロックをサブブロックに分割する
306
サブブロックを暗号化する
308
ＸＯＲを計算する
310
ＸＯＲサブブロックとサブブロックを組み合わせる
312
セキュアハッシュを計算する

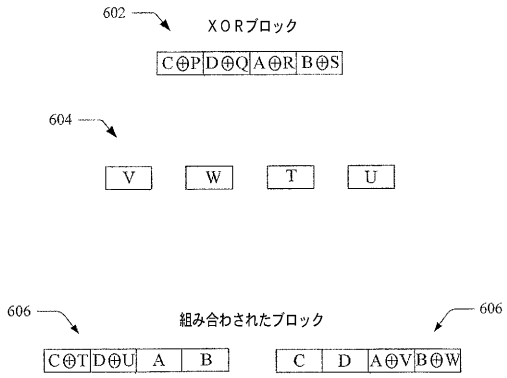
【図４】


402
５１２ビットのブロック
404
１２８ビットのサブブロック
A
B
C
D
406
組み合わされたブロック
406
C⊕P
D⊕Q
A
B
C
D
A⊕R
B⊕S

【図５】


500
502
再現可能な無作為に現れる要素が提供される
504
提供された要素から暗号キーを導出する
506
キーでメッセージ／ブロックを暗号化する

【図６】


602
ＸＯＲブロック
C⊕P
D⊕Q
A⊕R
B⊕S
604
V
W
T
U
606
組み合わされたブロック
606
C⊕T
D⊕U
A
B
C
D
A⊕V
B⊕W

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US 06/22960

A. CLASSIFICATION OF SUBJECT MATTER
IPC(8) - H04L 1/00 (2007.01), G06Q 99/00 (2007.01)
USPC - 380/28
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)
USPC: 380/28

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
USPC: 370/395.32, 380/59 705/50, 713/170, 713/176 (keyword limited - see terms below)

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
WEST(USPT,PGPB,EPAB,JPAB)
Keywords searched: (hash, secure, digital signature, block cipher, sub-block, encryption, pre-process, message, assembly)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 5,892,829 A (AIELLO et al.) 06 April 1999 (06.04.1999) (col 2., ln 18-42 and col 1, ln 57-63).	1-17
Y	US 6,578,144 B1 (GENNARO et al) 10 June 2003 (10.06.2003) (col 8, ln 32-64).	1-7
Y	US 6,314,186 B1 (LEE et al.) 06 November 2001 (06.11.2001) (col 3, ln 35-57 and col 6, ln 9 to col 7, ln 27).	2, 4-6, 8-17

☐ Further documents are listed in the continuation of Box C. ☐

* 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
8 January 2007 (08.01.2007)	22 FEB 2007
Name and mailing address of the ISA/US Mail Stop PCT, Attn: ISA/US, Commissioner for Patents P.O. Box 1450, Alexandria, Virginia 22313-1450 Facsimile No. 571-273-3201	Authorized officer: Lee W. Young PCT Helpdesk: 571-272-4300 PCT OSP: 571-272-7774

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

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US 06/22960

Box No. II Observations where certain claims were found unsearchable (Continuation of item 2 of first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☒ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:
Claims 18-20 appear to be unsearchable as they appear to recite a mathematical algorithm.

2. ☐ Claims Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box No. III Observations where unity of invention is lacking (Continuation of item 3 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

1. ☐ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.

2. ☐ As all searchable claims could be searched without effort justifying additional fees, this Authority did not invite payment of additional fees.

3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest

☐ The additional search fees were accompanied by the applicant's protest and, where applicable, the payment of a protest fee.

☐ The additional search fees were accompanied by the applicant's protest but the applicable protest fee was not paid within the time limit specified in the invitation.

☐ No protest accompanied the payment of additional search fees.

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,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,BR,BW,BY,BZ,CA,CH,CN,CO,CR,CU,CZ,DE,DK,DM,DZ,EC,EE,EG,ES,FI,GB,GD,GE,GH,GM,HR,HU,ID,IL,IN,IS,JP,KE,KG,KM,KN,KP,KR,KZ,LC,LK,LR,LS,LT,LU,LV,LY,MA,MD,MG,MK,MN,MW,MX,MZ,NA,NG,NI,NO,NZ,OM,PG,PH,PL,PT,RO,RS,RU,SC,SD,SE,SG,SK,SL,SM,SY,TJ,TM,TN,TR,TT,TZ,UA,UG,US,UZ,VC,VN,ZA,ZM,ZW

(72)発明者 ラマラスナム ベンカテサン
アメリカ合衆国 ９８０５２ ワシントン州 レッドモンド ワン マイクロソフト ウェイ マイクロソフト コーポレーション インターナショナル パテンツ内

Ｆターム(参考) 5B017 AA08 BA09
5J104 AA08 AA18 JA03 LA06 NA12 NA27