(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2009-526411
(P2009-526411A)
(43)公表日　平成21年7月16日(2009.7.16)

(51)Int.Cl.			F I			テーマコード（参考）
H04L	9/32	(2006.01)	H04L	9/00	675B	5J104
G09C	1/00	(2006.01)	G09C	1/00	640D	

審査請求 有　予備審査請求 未請求　（全 36 頁）

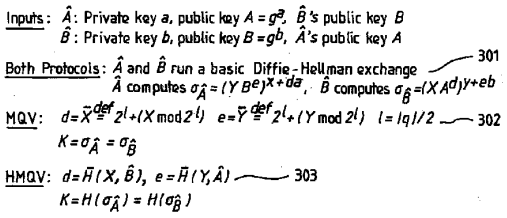
(21)出願番号　特願2007-554563 (P2007-554563)
(86)(22)出願日　平成18年2月10日 (2006.2.10)
(85)翻訳文提出日　平成19年10月5日 (2007.10.5)
(86)国際出願番号　PCT/EP2006/050841
(87)国際公開番号　WO2006/084896
(87)国際公開日　平成18年8月17日 (2006.8.17)

(71)出願人　390009531
インターナショナル・ビジネス・マシーンズ・コーポレーション
ＩＮＴＥＲＮＡＴＩＯＮＡＬ　ＢＵＳＩＮＥＳＳ　ＭＡＳＣＨＩＮＥＳ　ＣＯＲＰＯＲＡＴＩＯＮ
アメリカ合衆国１０５０４　ニューヨーク州　アーモンク　ニュー　オーチャード　ロード
(74)代理人　100108501
弁理士　上野　剛史
(74)代理人　100112690
弁理士　太佐　種一
(74)代理人　100091568
弁理士　市位　嘉宏

最終頁に続く

(54)【発明の名称】装置またはネットワークによって相互接続された２当事者間の交換の方法、信号伝送媒体、および装置（チャレンジ・レスポンス署名および高性能で安全なＤｉｆｆｉｅ－Ｈｅｌｌｍａｎプロ

(57)【要約】
【課題】　装置またはネットワークによって相互接続された２当事者間の交換の方法（および構造）を提供することにある。
【解決手段】　受信側当事者（検証者）は、値Ｘ＝Ｆ１（ｘ）を計算するために秘密の値ｘを選択し、ここでＦ１は少なくとも１つの引数を有する第１の所定の関数を含み、値ｘはＦ１の少なくとも１つの引数のうちの１つである。署名側当事者（署名者）は、値Ｙ＝Ｆ２（ｙ）を計算するために秘密の値ｙを選択し、ここでＦ２は少なくとも１つの引数を有する第２の所定の関数を含み、値ｙはＦ２の少なくとも１つの引数のうちの１つである。署名者は値Ｘを入手し、署名者は秘密鍵ｂと公開鍵Ｂとを有する。署名者は値ｓ＝Ｆ３（ｙ，ｂ，Ｘ）を計算し、ここでＦ３は少なくとも３つの引数を有する第３の所定の関数を含み、値ｙ、秘密鍵ｂ、および値ＸはＦ３の少なくとも３つの引数のうちの３つの引数である。
【選択図】　図１０



【特許請求の範囲】
【請求項１】
装置またはネットワークによって相互接続された２当事者間の交換の方法において、
受信側当事者（検証者）が値Ｘ＝Ｆ１（ｘ）を計算するために秘密の値ｘを選択し、ここでＦ１は少なくとも１つの引数を有する第１の所定の関数を含み、前記値ｘはＦ１の前記少なくとも１つの引数のうちの１つであり、
署名側当事者（署名者）が値Ｙ＝Ｆ２（ｙ）を計算するために秘密の値ｙを選択し、ここでＦ２は少なくとも１つの引数を有する第２の所定の関数を含み、前記値ｙはＦ２の前記少なくとも１つの引数のうちの１つであり、
前記署名者が前記値Ｘを入手し、前記署名者が秘密鍵ｂと公開鍵Ｂとを有し、
前記署名者が値ｓ＝Ｆ３（ｙ，ｂ，Ｘ）を計算し、ここでＦ３は少なくとも３つの引数を有する第３の所定の関数を含み、前記値ｙ、前記秘密鍵ｂ、および前記値ＸはＦ３の前記少なくとも３つの引数のうちの３つの引数であり、
値ｓ′を計算するために第４の所定の関数Ｆ４（ｘ，Ｙ，Ｂ）が存在し、Ｆ４は少なくとも３つの引数を有し、前記値ｘ、前記値Ｙ、および前記公開鍵ＢはＦ４の前記少なくとも３つの引数のうちの３つの引数であるが、値ｓはＦ４の引数ではなく、
前記検証者と前記署名者との間で共有され、前記Ｆ１、Ｆ２、Ｆ３、およびＦ４のいずれかにおいて任意の引数の基礎として働くような秘密が存在せず、
前記値ｓ′が所定の方法で前記値ｓに関連するものと判断された場合に前記検証者が前記値ｓおよびｓ′を有効な認証子と見なすことができる、方法。
【請求項２】
Ｆ１およびＦ２のうちの少なくとも１つが一方向関数を含む、請求項１に記載の方法。
【請求項３】
前記値ｓおよびｓ′が、ｓ＝ｓ′である場合に有効な認証子であると判断される、請求項１に記載の方法。
【請求項４】
ｓ′の計算ならびに前記値ｓおよびｓ′が関連するものであると判断されるかどうかの判断のうちの少なくとも一方が、前記検証者および前記署名者以外の当事者によって実行される、請求項１に記載の方法。
【請求項５】
２当事者間で共有される秘密を導出するために前記値ｓおよび前記値ｓ′が使用される、請求項１に記載の方法。
【請求項６】
前記検証者が前記値Ｙを入手し、ｓおよびｓ′が前記所定の方法で関連するかどうかを判断するために前記値ｓ′を計算するためにこれを使用すること
をさらに含む、請求項１に記載の方法。
【請求項７】
メッセージｍが、認証対象であり、Ｆ３の引数およびＦ４の引数を含み、それにより、前記値ｓおよび前記値ｓ′が前記メッセージｍ内の情報を含むことができ、
前記値ｓおよびｓ′が前記所定の方法で関連するものであると判断された場合に前記メッセージが認証される、請求項１に記載の方法。
【請求項８】
２当事者間で共有される秘密を導出するために前記値ｓおよび前記値ｓ′が使用される、請求項７に記載の方法。
【請求項９】
前記メッセージｍが、少なくとも前記交換の前記当事者の一方のＩＤを含む、請求項８に記載の方法。
【請求項１０】
前記署名者が前記値ｓを前記検証者に送信すること
をさらに含む、請求項７に記載の方法。

【請求項１１】
前記ｓ＝ｓ′である場合に前記メッセージが認証される、請求項７に記載の方法。
【請求項１２】
前記公開鍵Ｂ＝g^bであり、ｇが次数ｑの有限群の生成元であり、前記秘密鍵ｂが$0 \leq b \leq q-1$になるような整数であり、
前記値Ｘ＝g^xであり、ｘが$0 \leq x \leq q-1$になるような整数であり、前記値Ｙ＝g^yであり、ｙが$0 \leq y \leq q-1$になるような整数であり、
前記署名者が前記値ｓ＝$f_1(X)^{f2(m,Y,y,b)}$を計算し、f_1が第１の数学関数を含み、f_2が第２の数学関数を含み、引数ｍがメッセージを含む、請求項１に記載の方法。
【請求項１３】
ｑが素数である、請求項１２に記載の方法。
【請求項１４】
前記値ｓが所定の方法で前記値ｓ′に関連するものと判断された場合に前記メッセージｍが認証済みと見なされる、請求項１２に記載の方法。
【請求項１５】
前記値ｓが前記値ｓ′に等しいと判断された場合に前記メッセージｍが認証済みと見なされる、請求項１４に記載の方法。
【請求項１６】
f_1が恒等関数から構成される、請求項１２に記載の方法。
【請求項１７】
f_2が、f_2の前記引数の少なくとも１つがハッシュされるようなハッシュ関数を含む、請求項１２に記載の方法。
【請求項１８】
ハッシュされた前記引数の１つが非ヌル・メッセージｍである、請求項１７に記載の方法。
【請求項１９】
前記メッセージｍが、コンピュータまたはシステムあるいはネットワーク内の当事者のＩＤを含む、請求項１２に記載の方法。
【請求項２０】
f_2（ｍ，Ｙ，ｙ，ｂ）＝ｙ＋Ｈ（Ｙ，ｍ）ｂ　ｍｏｄ　ｑであり、ここでＨは一方向関数、暗号化関数、および暗号ハッシュ関数のうちの１つである暗号関数を含む、請求項１７に記載の方法。
【請求項２１】
前記値ｓ′＝$(YB^{\{H(Y,m)\}})^{f3(x)}$であり、ここで$f_3$（ｘ）は少なくとも１つの引数を有する数学関数を含み、前記値ｘはf_3（ｘ）の前記少なくとも１つの引数のうちの１つの引数である、請求項２０に記載の方法。
【請求項２２】
f_3（ｘ）＝ｘである、請求項２１に記載の方法。
【請求項２３】
ｓ＝ｓ′である場合のみ、前記メッセージｍを認証すること
をさらに含む、請求項２１に記載の方法。
【請求項２４】
前記検証者が、秘密鍵ａ、公開鍵Ａ＝g^a、およびメッセージｍ′を有し、前記値ｓ′がｍ上の前記署名者の署名を含むと同時に、前記値ｓがｍ′上の前記検証者の署名を含む、請求項２１に記載の方法。
【請求項２５】
前記関数ｆ３（ｘ）＝ｘ＋Ｈ（Ｘ，ｍ′）ａ　ｍｏｄ　ｑである、請求項２４に記載の方法。
【請求項２６】
ｘが前記検証者によってランダムに選択され、ｙが前記署名者によってランダムに選択

される、請求項１に記載の方法。
【請求項２７】
前記第１の値Ｘ＝ｇ^{x}が、前記証明者により検索可能になるように前記検証者によって公開された値を含み、それにより、前記認証の非対話式バージョンを可能にする、請求項１に記載の方法。
【請求項２８】
前記値ｓおよびｓ′がさらにハッシュされる、請求項２１に記載の方法。
【請求項２９】
請求項１に記載の前記方法の諸ステップの少なくとも１つを実行するためにデジタル処理装置によって実行可能な複数の機械可読命令からなるプログラムを具体的に実施する信号伝送媒体。
【請求項３０】
前記署名者について請求項１に記載した前記関数Ｆ２およびＦ３を計算するための計算機
を含む装置。
【請求項３１】
装置またはネットワークによって相互接続された２当事者間で認証鍵を確立するための方法において、
第１の当事者が秘密鍵ａと公開鍵Ａとを有する場合に、前記秘密鍵ａが$0 \leq a \leq q-1$になるような整数であり、ｑが正整数であり、ｇが次数ｑの有限群の生成元であり、Ａが前記値ｇによって生成され、Ａ＝ｇ^{a}として計算された前記群内の元であり、
第２の当事者が秘密鍵ｂと公開鍵Ｂ＝ｇ^{b}とを有し、前記秘密鍵ｂが$0 \leq b \leq q-1$になるような整数であり、
前記第１の当事者が値Ｘ＝ｇ^{x}を計算するために秘密の値ｘを選択し、ｘが$0 \leq x \leq q-1$になるような整数であり、前記値Ｘが前記第２の当事者に伝達され、
前記第２の当事者が値Ｙ＝ｇ^{y}を計算するために秘密の値ｙを選択し、ｙが$0 \leq y \leq q-1$になるような整数であり、前記値Ｙが前記第１の当事者に伝達され、
前記第１の当事者が値$s = f_1(Y, B, m)^{\{f2(x,a,m')\}}$を計算し、ここでｍ、ｍ′は前記当事者間で既知であるかまたは交換されたメッセージを含み、前記第２の当事者が値$s' = f_3(X, A, m')^{\{f4(y,b,m)\}}$を計算し、
前記関数f_2およびf_4のうちの少なくとも１つが少なくとも１つの引数を有する関数Ｈを含み、このような１つの引数が前記メッセージｍおよびｍ′のうちの少なくとも１つであり、ここでＨは一方向関数、暗号化関数、および暗号ハッシュ関数のうちの１つである暗号関数を含み、
前記第１および第２の当事者がそれぞれ前記値ｓおよびｓ′から共有鍵を導出する、方法。
【請求項３２】
（ｉ）前記値ｘおよびＸの計算が、前記第１の当事者の前記秘密鍵と、前記当事者のうちの一方または複数の前記公開鍵とを含むことと、
（ｉｉ）前記値ｙおよびＹの計算が、前記第２の当事者の前記秘密鍵と、前記当事者のうちの一方または複数の前記公開鍵とを含むこと
のうちの少なくとも一方が該当する、請求項３１に記載の方法。
【請求項３３】
ｓおよびｓ′からの共有鍵の前記導出が、一方向関数、暗号化関数、および暗号ハッシュ関数のうちの１つである暗号関数を含む、請求項３１に記載の方法。
【請求項３４】
前記メッセージｍおよびｍ′のうちの少なくとも１つが前記第１および第２の当事者のうちの一方のＩＤを含む、請求項３１に記載の方法。
【請求項３５】
$f_1(Y, B, m) = Y B^{H(Y,m)}$であり、

f_2（ｘ，ａ，ｍ′）＝（ｘ＋Ｈ（Ｘ，ｍ′）ａ） ｍｏｄ ｑであり、
f_3（Ｘ，Ａ，ｍ′）＝$XA^{H(X,m')}$であり、
f_4（ｙ，ｂ，ｍ）＝（ｙ＋Ｈ（Ｙ，ｍ）ｂ） ｍｏｄ ｑであり、
Ｈが一方向関数、暗号化関数、および暗号ハッシュ関数のうちの１つである暗号関数を含む、少なくとも２つの引数からなる関数である、請求項３１に記載の方法。
【請求項３６】
前記メッセージｍおよびｍ′のうちの少なくとも１つが前記第１および第２の当事者のうちの少なくとも一方のＩＤを含む、請求項３５に記載の方法。
【請求項３７】
（ｉ）前記値ｘおよびＸの計算が、前記第１の当事者の前記秘密鍵と、前記当事者のうちの一方または複数の前記公開鍵とを含むことと、
（ｉｉ）前記値ｙおよびＹの計算が、前記第２の当事者の前記秘密鍵と、前記当事者のうちの一方または複数の前記公開鍵とを含むこと
のうちの少なくとも一方が該当する、請求項３６に記載の方法。
【請求項３８】
ｓおよびｓ′からの共有鍵の前記導出が、一方向関数、暗号化関数、および暗号ハッシュ関数のうちの１つである暗号関数を含む、請求項３６に記載の方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明の諸態様は、一般に、情報交換の送信側および受信側当事者にとって立証可能に（provably）安全な署名に関する。より具体的には、チャレンジ・レスポンス署名方式（challenge-responsesignature scheme）は、検証者（verifier）と署名者（signer）の両方が同じ署名または関連署名を計算することができ、前者はチャレンジを把握することにより、後者は秘密署名鍵（privatesignature key）を把握することによりこれを行うことができ、これにより、模範的な諸実施形態では、周知のＭＱＶプロトコルの変形を含む、従来の鍵交換プロトコルの立証可能に安全な変形を可能にするという特性を有する。
【背景技術】
【０００２】
当初の提案通り、図１に図示されているＤｉｆｆｉｅ－Ｈｅｌｌｍａｎ（ＤＨ）鍵交換プロトコル１００は、盗聴専門の攻撃者（attacker）に対して安全であると考えられている。活発なマン・イン・ザ・ミドル（man-in-the-middle）攻撃に抵抗する「認証Ｄｉｆｆｉｅ－Ｈｅｌｌｍａｎ」プロトコルの探求の結果、無数のアドホック提案が行われたが、その多くは破棄されているかまたは欠点に苦しんでいることが分かっている。鍵交換のための厳格なセキュリティ・モデルに関するこの数年間の発展により、当業者は、現在、これらのプロトコルのセキュリティを判断できるとともに、現実的に活発な攻撃に立証可能に耐える設計を開発できる、かなり良好な立場にある。
【０００３】
予想通り、活発な攻撃に対する安全機能を追加すると、その結果、追加の通信および計算のいずれの点でも複雑さが追加される。後者は、通常、追加の高価な群べき乗（group exponentiation）を必要とする公開鍵技法によって認証されたプロトコルで特に重要なものである。しっかりしたセキュリティの必要性に加えて、鍵交換に対する多くの実用的な適用例のために、設計者は、認証メカニズム、特に公開鍵に基づくものに関連するパフォーマンス・コストの改善を余儀なくされてきた。
【０００４】
１９８６年に松本、高島、および今井によって着手された研究分野は、そのプロトコルに最小限の複雑さを追加することになると思われる公開鍵（ＰＫ）認証ＤＨプロトコルの探索である。理論的には、しかも保証された公開鍵の交換までは、プロトコルの通信は、正確に基本ＤＨ交換に見えることが望まれている。この技法では、プロトコルの認証は鍵導出手順を介して入手しなければならず、基本Ｄｉｆｆｉｅ－Ｈｅｌｌｍａｎ鍵g^{xy}につ

いて合意することではなく、当事者は、その当事者の公開鍵／秘密鍵とg^x、g^yを結合する鍵について合意することになるであろう。

【０００５】

一部にはこのようなプロトコルが提供すると思われる実用的な利点ために、また、一部にはこのような設計の背後にある数学的難題のために、「暗黙認証Ｄｉｆｆｉｅ－Ｈｅｌｍａｎプロトコル」と呼ばれる場合が多い多数のプロトコルが、この手法に基づいて開発されてきた。この手法は通信面で非常に効率的なプロトコルを生成できるだけでなく、認証と鍵導出手順の組み合わせにより、潜在的に大幅な計算上の節約を行うこともできる。これらの理由で、これらの「暗黙認証」プロトコルのうちのいくつかは、主要な国内および国際的セキュリティ規格によって標準化されている。

【０００６】

これらのプロトコルのうち、ＭＱＶプロトコルは広範囲にわたって標準化されているように思われる。このプロトコルは、多くの組織によって標準化され、最近、「機密扱いのまたは主幹業務の国家的セキュリティ情報」の保護を含む、「米国政府情報を保護するための次世代暗号方式」の基礎となる鍵交換メカニズムであると米国国家安全保障局（ＮＳＡ：National Security Agency）によって発表されている。

【０００７】

さらに、ＭＱＶは、多数のセキュリティ上の目標を満足するように設計されているように思われる。ＭＱＶプロトコルの基本バージョンは、たとえば、Ｖａｎｓｔｏｎｅ他に交付された米国特許第５７６１３０５号に説明されている。

【０００８】

しかし、その魅力および成功にもかかわらず、ＭＱＶはこれまで明確に定義された鍵交換のモデルにおける形式的分析を避けてきた。本発明は、このような分析を行いたいという希望が動機になっている。研究を行った際に、本発明者は、ＣａｎｅｔｔｉおよびＫｒａｗｃｚｙｋの計算鍵交換モデルで実行されるように、しかも上記の仮出願に記載されているように、明記されたＭＱＶの目標のほぼすべてが有効ではないことが証明できると気付いていた。

【０００９】

この結果、この従来のプロトコルのセキュリティに関する懸念が本発明者に提起された。したがって、従来のＭＱＶプロトコルは立証可能に安全ではなかったというこの分析に基づいて、好ましくはその既存のパフォーマンスおよび多様性を保持しながら、ＭＱＶに対する追加のセキュリティが必要になっている。

【特許文献１】米国特許第５７６１３０５号

【発明の開示】

【発明が解決しようとする課題】

【００１０】

従来のシステムの上記およびその他の模範的な問題、欠点、および不利点を考慮すると、本発明の１つの模範的な特徴は、ＭＱＶプロトコルのセキュリティ上の目標を立証可能な方法で達成し、本明細書でＨＭＱＶと呼ばれるＭＱＶの新しい変形に関する方法および構造を提供することにある。

【００１１】

本発明の他の模範的な特徴は、本明細書で「チャレンジ・レスポンス署名」と呼ばれる新しいデジタル署名方式を実証することにある。

【００１２】

本発明の他の模範的な特徴は、チャレンジャ（challenger）と署名者の両方が同じ署名または関連署名を計算することができ、前者はチャレンジを選択したことにより、後者は秘密署名鍵を把握することによりこれを行うことができるという特性を有するプロトコル・メカニズムを提供するものとして、Ｓｃｈｎｏｒｒ識別方式から導出され、本明細書で「指数チャレンジ・レスポンス」（ＸＣＲ：exponentialchallenge response）署名方式と呼ばれるバージョンを含むものとしてこのチャレンジ・レスポンス署名方式を実証する

ことにある。
【００１３】
したがって、本発明の模範的な一目的は、そこにＸＣＲ署名方式の概念を実現することによりセキュリティを立証可能に実証することができる、認証Ｄｉｆｆｉｅ－Ｈｅｌｌｍａｎプロトコルに関するセキュリティを改善するための構造および方法を提供することにある。
【課題を解決するための手段】
【００１４】
本発明の第１の模範的な態様では、上記の特徴および目的を達成するために、値Ｘ＝Ｆ１（ｘ）を計算するために秘密の値ｘを選択する受信側当事者（検証者）を含み、ここでＦ１は少なくとも１つの引数を有する第１の所定の関数を含み、値ｘはＦ１の少なくとも１つの引数のうちの１つである、装置またはネットワークによって相互接続された２当事者間の交換の方法が本明細書に記載されている。署名側当事者（署名者）は、値Ｙ＝Ｆ２（ｙ）を計算するために秘密の値ｙを選択し、ここでＦ２は少なくとも１つの引数を有する第２の所定の関数を含み、値ｙはＦ２の少なくとも１つの引数のうちの１つである。署名者は値Ｘを入手し、署名者は秘密鍵ｂと公開鍵Ｂとを有する。署名者は値ｓ＝Ｆ３（ｙ，ｂ，Ｘ）を計算し、ここでＦ３は少なくとも３つの引数を有する第３の所定の関数を含み、値ｙ、秘密鍵ｂ、および値ＸはＦ３の少なくとも３つの引数のうちの３つの引数である。値ｓ′を計算するために第４の所定の関数Ｆ４（ｘ，Ｙ，Ｂ）が存在し、Ｆ４は少なくとも３つの引数を有し、値ｘ、値Ｙ、および公開鍵ＢはＦ４の少なくとも３つの引数のうちの３つの引数であるが、値ｓはＦ４の引数ではない。検証者と署名者との間で共有され、関数Ｆ１、Ｆ２、Ｆ３、およびＦ４のいずれかにおいて任意の引数の基礎として働くような秘密はまったく存在しない。値ｓ′が所定の方法で値ｓに関連するものと判断された場合に検証者は値ｓおよびｓ′を有効な認証子（authenticator）と見なすことができる。
【００１５】
本発明の第２および第３の模範的な態様では、前の段落に記載された方法を実行する装置と、その方法を実行するためにデジタル処理装置によって実行可能な複数の機械可読命令からなるプログラムを具体的に実施する信号伝送媒体も本明細書に記載されている。
【００１６】
本発明の第４の模範的な態様では、装置またはネットワークによって相互接続された２当事者間で認証鍵（authenticated key）を確立するための方法も本明細書に記載されている。第１の当事者は秘密鍵ａと公開鍵Ａとを有し、秘密鍵ａは$0 \leq a \leq q-1$になるような整数であり、ｑは正整数であり、ｇは次数ｑの有限群（finitegroup）の生成元（generator）であり、Ａは値ｇによって生成され、$A = g^a$として計算された群内の元（element）である。第２の当事者は秘密鍵ｂと公開鍵$B = g^b$とを有し、秘密鍵ｂは$0 \leq b \leq q-1$になるような整数である。第１の当事者は値$X = g^x$を計算するために秘密の値ｘを選択し、ｘは$0 \leq x \leq q-1$になるような整数であり、値Ｘは第２の当事者に伝達される。第２の当事者は値$Y = g^y$を計算するために秘密の値ｙを選択し、ｙは$0 \leq y \leq q-1$になるような整数であり、値Ｙは第１の当事者に伝達される。第１の当事者は値$s = f_1(Y, B, m)^{\{f2(x,a,m')\}}$を計算し、ここでｍ、ｍ′は両当事者間で既知であるかまたは交換されたメッセージを含み、第２の当事者は値$s' = f_3(X, A, m')^{\{f4(y,b,m)\}}$を計算する。関数$f_2$および$f_4$のうちの少なくとも１つは少なくとも１つの引数を有する関数Ｈを含み、このような１つの引数はメッセージｍおよびｍ′のうちの少なくとも１つであり、ここでＨは一方向関数（one-way function）、暗号化関数（encryption function）、および暗号ハッシュ関数（cryptographichash function）のうちの１つである暗号関数（cryptographic function）を含む。第１および第２の当事者はそれぞれ値ｓおよびｓ′から共有鍵（sharedkey）を導出する。
【００１７】
上記およびその他の目的、態様、および利点は、図面に関連して本発明の好ましい一実

施形態に関する以下の詳細な説明からより良好に理解されるであろう。

【発明を実施するための最良の形態】

【００１８】

次に、図面、詳細には図１～図１１を参照すると、本発明による方法および構造の模範的な諸実施形態が示されている。

【００１９】

群および表記法に関する予備的注記として、本明細書で論ずるすべてのプロトコルおよび演算は、典型的には生成元ｇによって生成された素数（prime number）である次数ｑの巡回群（cyclic group）Ｇを想定している。ｑのビット長は｜ｑ｜（たとえば、

【数１】

$$|q| = \lceil \log_2 q \rceil$$

であり、最近隣数（nearestinteger）まで丸められた２を底とするｑの対数を意味する）によって表され、この数量は暗黙セキュリティ・パラメータとして使用される。パラメータＧ、ｇ、およびｑは、単純にするため、実際に一般的であるように、一定であり、あらかじめ両当事者にとって既知のものであると想定される。代わって、これらの値を証明書などに含めることもできるであろう。

【００２０】

本明細書では群演算の乗算表現が使用されるが、その処理は、楕円曲線などの加法群（additive group）、あるいは任意のその他の代数群（algebraic group）または特定の群、有限体（finitefield）、複合法（composite moduli）などに等しく適用可能である。プロトコルでは、大文字（たとえば、Ａ、Ｂ）によって表される公開鍵は群Ｇ内の元であり、対応する小文字（たとえば、ａ、ｂ）によって表される秘密鍵はZ_q内の元であり、ここでZ_qは整数０、１、・・・、ｑ－１の集合を表している。

【００２１】

たとえば、公開鍵Ａ＝g^aは秘密鍵ａに対応する。その公開鍵としてＡを有する当事者は、

【数２】

$\hat{A}$

は以降Ａハットと記載する。

によって表され、伝統的には「アリス（Alice）」と見なされることになる（第２の当事者

【数３】

$\hat{B}$

は以降Ｂハットと記載する。

は伝統的には「ボブ（Bob）」と見なされる）。一般に、「ハット表記法（hatnotation）」は、名前、電子メール・アドレス、役割など、プロトコル内の当事者の論理ＩＤまたは「識別（distinguishing）」ＩＤを表すために使用される。場合によっては、これらのＩＤはデジタル証明書で増強することができる。本明細書では繰り返さないが、仮出願で提供されるより完全な数理解析のために、攻撃者を含むプロトコル内のすべての当事者は、確率的多項式タイム・マシンを介して実現されるものと見なされる。また、攻撃者はＭによっても表され、ここでＭは「悪意のある（malicious）」ことを意味する可能性がある。

【００２２】

したがって、図１に図示されている通り、基本非認証Ｄｉｆｆｉｅ－Ｈｅｌｌｍａｎプロトコル１００に関するセッション鍵の計算は、２当事者ＡハットとＢハットとの間の交換から構成され、当事者Ａハットはまず自分の鍵Ｘ＝g^xを当事者Ｂハットに送信し、次に当事者Ｂハットは、自分の鍵Ｙ＝g^yを当事者Ａハットに返送することによって応答し、ここでｘおよびｙはそれぞれ、集合Z_qからランダムにＡハットおよびＢハットによって選択された秘密であり、共有セッション鍵はg^{xy}として計算される。

【００２３】

本明細書の説明では、ランダム選択を表すために記号$\in_R$が使用される場合があることは留意すべきである。たとえば、$x \in_R Z_q$は、典型的には乱数発生器または疑似乱数発生器を使用することにより、整数Z_qの集合からランダムに値ｘを選択することを意味する。

【００２４】

ＭＱＶプロトコル

Ａハット、ＢハットというＩＤが公開鍵証明書などの追加の情報を含む可能性があるかまたはこれらのＩＤがすべてまとめて省略される可能性があることを除いて、ＭＱＶプロトコルでの通信は、図１に描写されている基本非認証ＤＨプロトコル１００と同一である。

【００２５】

２メッセージ認証鍵交換プロトコルを設計する際の第１の難題は、第１のプロトコル・メッセージの再生に基づく攻撃の成功を防止することである。第１のメッセージは、応答側（responder）によって与えられた任意の形式のセッション固有「鮮度保証（freshness guarantee）」（たとえば、ｎｏｎｃｅまたは新鮮なＤＨ値など）を含むことができないので、これは問題のあるものである。この問題の解決策の１つは、セッション鍵の計算を介して鮮度を提供することである。

【００２６】

たとえば、図２に図示されている２メッセージＤｉｆｆｉｅ－Ｈｅｌｌｍａｎプロトコル２００は、ＩＳＯ（国際標準化機構：International Standards Organization）９７９３プロトコルから採用されたデジタル署名を使用して認証される。Ｂハットの署名の下にg^xを含めることによって認証に鮮度が提供されるが、この安全機能はＡハットのメッセージには存在しない。しかし、セッション鍵g^{xy}は、新鮮なｙによってランダム化されるので、新鮮であること（ならびに他のセッション鍵から独立していること）が保証される。しかし、攻撃者がＢハットとのセッションにおいてＡハットによって使用される単一のペア（ｘ，g^x）を見つけることができる場合、プロトコルのセキュリティが途切れ、その場合、攻撃者は

【数４】

$$\mathrm{SIG}_{\hat{A}}(g^x, \hat{B})$$

も学習する。これにより、攻撃者は、Ａハットの長期秘密署名鍵を学習する必要なしに、同じメッセージとｘに関する知識を使用して、漠然とＢハットに対してＡハットを詐称することができる。

【００２７】

これは、一時（ephemeral）セッション固有情報（たとえば、ペア（ｘ，g^x））の開示によって他のセッションを破壊してはならないという基本原理に違反する重大な脆弱性である。多くの適用例がこのペア（ｘ，g^x）をオフラインで計算し、たとえば、長期秘密鍵ほど保護されていない記憶域にそれを保持することになることを考慮すると、これは特に重大である。

【００２８】

したがって、一時情報が漏れた場合でもリプレイ・アタック（replay attack）に影響されない２メッセージ・プロトコルをどのように設計できるかが問題である。セッション鍵の計算に長期秘密鍵を含めることは当然の答えである。これは、ＭＱＶを含む、Ｄｉｆｆｉｅ－Ｈｅｌｌｍａｎのいわゆる「暗黙認証」変種の多くの動機になっている、松本、高島、および今井による１９８６年の研究で着手された手法であった。この手法では、各当事者は長期ＤＨ公開鍵とそれに対応する秘密の指数（exponent）とを有し、セッション固有の一時ＤＨ値と両当事者の公開鍵および秘密鍵とを組み合わせることによってセッションが生成される。したがって、このようなプロトコルのセキュリティは全体として、この鍵の組み合わせの正確な詳細に依存する。意外なことに、この表面上単純な考え方は確実に実現するには困難なものであり、これまでの提案はいずれもいくつかの短所を抱えて

いる。

【００２９】

次に、セッション鍵計算において一時鍵と長期鍵を組み合わせることの問題に対する以下のような当然の解決策を考慮すると、ＡハットおよびＢハットが鍵を交換したいと希望する場合、両者は基本Ｄｉｆｆｉｅ－Ｈｅｌｌｍａｎプロトコルを実行し、$K=g^{(x+a)(y+b)}=(YB)^{x+a}=(XA)^{y+b}$としてセッション鍵を計算する。この場合、攻撃者がａではなくｘを学習すると、攻撃者はＫを計算することができない。

【００３０】

しかし、以下の単純な攻撃によって実証される通り、プロトコルは依然として安全ではなく、すなわち、Ｍは値$x^{*}\in_{R}Z_{q}$を選択し、$X^{*}=g^{X^{*}}/A$を計算し、Ａハットからの初期メッセージの詐称としてＢハットにX^{*}を送信する。ＢハットはＹ＝ｇｙを送信し、セッション鍵$K=(X^{*}A)^{y+b}$を計算する。残念なことに、ＭはＫを$(BY)^{x^{*}}$として計算することもできる。したがって、このプロトコルは安全ではない。

【００３１】

そのうえ、Ｋの計算が定数ｄ、ｅに関する$K=g^{(x+da)(y+eb)}$になるように変更された場合でも、攻撃は依然として可能である。これに対して、攻撃者がｅおよびＹを個別に制御できないように定数ｄ、ｅがＸ、Ｙにつれて変化することができる場合、上記の単純な攻撃は機能しない可能性がある。この考え方は我々をＭＱＶの設計に戻すものであり、ここでｄ＝

【数５】

$\overline{X}$

は以降Ｘバーと記載する。

およびｅ＝

【数６】

$\overline{Y}$

は以降Ｙバーと記載する。

である。

【００３２】

ＭＱＶにおけるセッション鍵Ｋの計算３０１、３０２は図３に図示されており、ここで当事者Ａハットは長期秘密鍵$a\in Z_{q}$と対応する公開鍵$A=g^{a}$とを所有している。同様に、Ｂの秘密鍵／公開鍵のペアは（ｂ，$B=g^{b}$）であり、一時ＤＨ値は$X=g^{x}$、$Y=g^{y}$であり、ここでｘ、ｙはそれぞれＡ、Ｂによって選択されたものである。セッション鍵の計算では、ｄ＝Ｘバーおよびｅ＝Ｙバーという値も使用し、ここで、ｌ＝｜ｑ｜／２の場合に、Ｘバー$=2^{l}+(X \bmod 2^{l})$およびＹバー$=2^{l}+(Y \bmod 2^{l})$である。

【００３３】

Ａハットによるセッション鍵の計算は、$X=g^{x}$を計算するためのオフラインべき乗（off-lineexponentiation）と、B^{e}を計算するためのオンラインべき乗（on-line exponentiation）と、$(YB^{e})^{x+da}$に関する追加のオンラインべき乗とを必要とすることは留意すべきである。しかし、第２のべき乗は長さ｜ｑ｜／２の指数ｅを使用し、したがって、それが「半べき乗（halfexponentiation）」（たとえば、ｇという正規べき乗（regular exponentiation）に対してモジュラ乗算の回数が半分である）と見なされることも留意すべきである。Ｂハットについても同じ演算カウントが有効である。

【００３４】

全体として、ＭＱＶのパフォーマンスは本当に印象的であり、基本非認証ＤＨプロトコルと同じ通信（両当事者のＩＤの一部として証明書を伝送する可能性を除く）であり、基本プロトコルより半べき乗だけ多く、認証交換を達成するための計算において２５％の増加に過ぎない。これは、認証のためにデジタル署名または公開鍵暗号化に依存する証明されたＤＨプロトコルのいずれよりも大幅に良好なものであり、より高価な演算と帯域幅の増加を伴うものである。また、これは、暗黙認証ＤＨプロトコルのうちの最も効率的なも

のであり、最も近いものは、３つの完全べき乗（full exponentiation）を必要とするが、実質的により少ないセキュリティ上の特徴を提供する「統一モデル（UnifiedModel）」プロトコルである。

【００３５】

この例外的パフォーマンスおよびセキュリティの約束により、認証ＤＨプロトコルを選択するときにＭＱＶが魅力的な候補になる。これらの理由で、このプロトコルは、多くの規格に採用され、広く文献で論じられてきた。しかし、鍵交換セキュリティの形式モデルのいずれでもＭＱＶプロトコルのいかなる形式的分析も正常に実行されなかったので、これまで回答されていない質問の１つは、ＭＱＶプロトコルが実際にどの程度安全であるのかということである。

【００３６】

これに対して、ＭＱＶ設計者は、設計の背後にあるセキュリティ上の目標について明確であった。これらは、詐称および既知の鍵の攻撃（「未知の鍵の共有（ＵＫＳ：unknown key share）」攻撃に対する抵抗を含む）に対する本質的なセキュリティならびに完全転送秘密（ＰＦＳ：perfectforward secrecy）およびＫＣＩ（鍵漏洩詐称：key-compromise impersonation）攻撃に対する抵抗などのより具体的な特徴を含む。既知の鍵の攻撃に対する抵抗は、一時セッション固有秘密情報の開示によって他のセッションのセキュリティを破壊してはならないという原理を表している。

【００３７】

ＰＦＳおよびＫＣＩ特性は、ある当事者の秘密鍵が攻撃者Ｍに漏れた場合にセキュリティ上の損害を閉じこめることを指す。より具体的には、ＰＦＳは、破壊されていない２当事者間で確立された任意のセッション鍵が両当事者のメモリから消去された後で両当事者が破壊された場合でも、そのセッション鍵をＭが学習できないことを意味する。ＫＣＩ攻撃に対する抵抗は、ある当事者Ａハットの長期秘密鍵を学習し、このため、明らかに他の当事者に対してＡハットを詐称できる攻撃者が、Ａハットに対して他の破壊されていない当事者を詐称できないことを必要とする。

【００３８】

残念なことに、上記の仮出願にさらに記載されているように、本発明者の分析の結果は、形式的に研究すると、これらの特性のいずれもＭＱＶプロトコルによって満足されないことを示している。具体的には、Ｃａｎｅｔｔｉおよびｋｒａｗｃｚｙｋのセキュリティ・モデルでは、このプロトコルは、ＭＱＶによって満足されると言われている上述のセキュリティ特性と矛盾する、ある範囲の攻撃に対して無防備であることが実証されている。

【００３９】

ＨＭＱＶプロトコル

ＨＭＱＶプロトコル（「Ｈ」は「ハッシュ」を意味するものと見なすことができる）は、いくつかの模範的な実施形態では、比較のためにステップ３０２に示されている従来のＭＱＶプロトコルへの追加であり、図３のステップ３０３に示されているようなハッシュを含むことができる、ＭＱＶの単純だが強力な変種である。しかし、ハッシュを行わず、ハッシュ以外の技法を使用しない代替諸実施形態が本明細書で論じられ、本発明の概念にも含まれるので、最初の問題として、これらの模範的な実施形態の１つまたは複数のハッシュ・ステップが本発明にとって前提条件ではないことも留意すべきである。本発明のより基本的な概念は、ＭＱＶプロトコルの模範的なハッシュ・バージョンを含む、いくつかの適用例および実施形態がそこから進化したチャレンジ・レスポンス署名方式に関するものである。

【００４０】

当技術分野で周知の通り、ハッシュは、出力として文字ストリングを数値、固定長ストリング（たとえば、ハッシュまたはメッセージ・ダイジェスト）などに変換するためにハッシュ関数を使用することを必要とする。暗号方式におけるハッシュ関数の基本機能は、元のデータを検索することが実行不可能であり、所与のハッシュ値に一致するデータ・ブロックを構築することも実行不可能でなければならないことを意味する、「一方向（one-

way）」または「非可逆（irreversible）」変換を提供することである。ハッシュ関数は、単純な「混合（mixing）」関数から、純粋にランダムなスクランブルに似ている変換まで及ぶ可能性がある。後者は、「強い暗号ハッシュ関数」と呼ばれ、理想的な確率関数（randomfunction）（または「ランダム・オラクル（random oracle）」によって暗号分析でモデル化される場合が多い。

【００４１】

いくつかのハッシュ関数は、強い暗号ハッシュに広く使用される。たとえば、ＭＤ５は、任意のサイズのデータ・ブロックを入力として取り、ビット単位演算、加算、および６４バイト・ブロック単位でデータを処理するための正弦関数（sine function）に基づく値の表を使用することによって、１２８ビット（１６バイト）のハッシュを生成する。もう１つの主要なハッシュ関数は、１６０ビット・ハッシュを提供するＮＩＳＴ（国立標準技術研究所：NationalInstitute of Standards and Technology）のセキュア・ハッシュ・アルゴリズム（ＳＨＡ：Secure Hash Algorithm）である。

【００４２】

典型的には、ハッシュ関数は暗号化に直接使用されないが、暗号化関数は一方向変換を提供し、このため、本発明のいくつかの模範的な実施形態を含む、いくつかのハッシュ用途に適用可能である。また、ハッシュ関数は、データ認証にも適切なものであり、秘密鍵（これらの設定では、メッセージ認証コード（Message Authentication Codeの場合にＭＡＣ）と呼ばれ、疑似確率関数（Pseudo-RandomFunction）の場合にＰＲＦと呼ばれる場合が多い）または署名方式（この場合、ハッシュ値は「メッセージ・ダイジェスト」に使用される）とともに、このような目的に使用される。

【００４３】

本発明の様々な模範的な実施形態では、上記の仮出願により詳細に記載されているセキュリティ分析において理想的なランダム・オラクルとして要約される少なくとも１つのハッシュ関数Ｈを使用する。これらの模範的な実施形態で関数Ｈが使用される２つのタスクは、第１に指数ｄ、ｅの計算であり、第２にセッション鍵そのものの導出である。

【００４４】

第１のタスクは例示的に、Ｈへの２つの引数を使用し、長さが｜ｑ｜／２のストリングを出力し、第２のタスクは、単一の引数にＨを適用し、指定の長さ（たとえば、１２８ビット）の鍵を出力する。表記法を単純にするために、同じ記号Ｈを使用して、ハッシュ関数の両方の適用例を表す。実際には、可変長入力を処理することができ、おそらく、ハッシュ結果を生成する際に短縮／拡張（truncation/expansion）の何らかの組み合わせを使用して、上記の２つのタスクに適合するようにその出力サイズを調整できる、単一のＨ、たとえば、ＳＨＡ－１を使用することになるであろう。

【００４５】

しかし、第１のタスクのようにハッシュを使用する場合、メッセージまたは当事者のＩＤのみをハッシュするのではなく、タイムスタンプ、ｎｏｎｃｅなどの追加の引数をハッシュ関数への入力として含めることができるので、必ずしも２つの引数に制限されないことも留意すべきである。

【００４６】

ハッシュを使用する場合、指数ｄ、ｅを生成するために使用されるハッシュ関数（典型的にはｌ＝｜ｑ｜／２ビットの出力を有する）は、

【数７】

$\overline{H}$

は以降Ｈバーと記載する。

で表される場合が多く、ｋビットの出力を有し、σ値に適用されるハッシュ関数はＨで表される。実際には、異なる出力長を有する同じハッシュ関数を使用することができ、このため、Ｈバーの代わりに記号Ｈが使用されることもある。ニーモニックとして、Ｈバー内のバーは、この関数の出力が指数として使用されることを示している。

【００４７】

ＭＱＶのように、ＨＭＱＶプロトコルの通信は、以前、図１に図示されている基本ＤＨ交換と同一であるが、証明書が追加される可能性がある。図３に例証されている通り、セッション鍵Ｋの計算は、値ｄおよびｅの計算におけるＭＱＶのものとは異なり、当事者自身のＤＨ値とピア（peer）のＩＤのハッシュを必要とする。このハッシュの典型的な出力はｌ＝｜ｑ｜／２ビットである。加えて、模範的な一実施形態では、ＨＭＱＶは、

【数８】

$$\sigma_{\hat{A}} = \sigma_{\hat{B}}$$

という値からｋビットの鍵へのハッシュを指定し、ここでｋは所望のセッション鍵の長さである。代替実施形態では、１つまたは両方のσ関数はハッシュされない。

【００４８】

この説明から、ＨＭＱＶは、通信および計算の両方の点でＭＱＶの優れたパフォーマンスを保持していることが分かる。同時に、ＨＭＱＶは、上記の仮特許出願で論じられているＭＱＶのすべてのセキュリティ上の短所を、そこでさらに論じられ証明される２メッセージ・プロトコルで最大限可能な範囲で、克服するものである。ＨＭＱＶおよびその変種のセキュリティ上の特性および利点に関するより完全な説明については、本出願で後で提示する。

【００４９】

チャレンジ・レスポンス署名

ＨＭＱＶプロトコルがＭＱＶプロトコルとはどのように異なるかは明らかでなければならないが、ある意味でより基本的な本発明のもう１つの態様が存在する。すなわち、ＨＭＱＶの背後にある中心的設計および分析要素として存在する主なテクニカル・ツールは、「チャレンジ・レスポンス署名」と呼ばれ、Ｆｉａｔ－Ｓｈａｍｉｒ方法を使用するＳｃｈｎｏｒｒの識別方式の新しい変種を基礎として実現される、新しい形の対話式署名である。その結果として、本発明の「指数チャレンジ・レスポンス」（ＸＣＲ）署名が得られる。ＳｃｈｎｏｒｒおよびＦｉａｔ－Ｓｈａｍｉｒ方法とＸＣＲ署名との関係については以下に論じる。

【００５０】

これらのＸＣＲ署名は、ランダム・オラクル・モデル（計算Ｄｉｆｆｉｅ－Ｈｅｌｌｍａｎ（Computational Diffie-Hellman）またはＣＤＨ仮説に基づくもの－以下を参照）において安全なものであり、検証者と署名者の両方が例示的に同じ署名を計算できるという特性を有する。前者はチャレンジを把握することによってこれを達成し、後者は秘密署名鍵を把握することによってこれを行うことができる。同一の署名の計算に関する変形は、署名者および検証者によって異なるが関連のある署名を計算することを含む。

【００５１】

たとえば、一方によって計算された署名値は、もう一方によって計算された署名のハッシュ変種である可能性があるか、あるいは両方の署名は何らかの特定の代数特性などによって関連している可能性がある。本発明の様々なＨＭＱＶプロトコルは、これらのＸＣＲ署名を使用する模範的なメカニズムの１つであり、これらは（ＤＨ値およびピアＩＤの）認証ならびにセッション鍵の計算を提供する。

【００５２】

したがって、ＸＣＲ署名ならびにその「二重バージョン（dual version）」（たとえば、ＤＣＲ）は、簡潔に論じると、ＨＭＱＶ設計および分析の基礎となる考え方について、技術ならびに概念の両面で当然の解釈を提供するものである。

【００５３】

加えて、ＨＭＱＶプロトコルを超える適用例ではＸＣＲ署名も使用できることは留意すべきである。それぞれの基本的形式では、ＸＣＲ署名は、対話式で、チャレンジ固有であり、移転不能であるので、デジタル署名の古典的機能を提供しない。すなわち、これらは、否認防止（non-repudiation）のために使用することができない。

【００５４】

これに対して、これらは、鍵交換を含む、何らかの適用例の場合に重要な特性である「

否認可能認証（deniable authentication）」を提供し、それにより、ＸＣＲ署名の受信側に対して、メッセージまたは鍵の発信元および保全性を保証することができるが、第三者に対してこの発信元を証明することはできない。とりわけ、これらの署名および結果として生じる鍵交換プロトコルは理想的には「非公式の（off-therecord）」の通信およびプライバシ保護に適している。加えて、ＸＣＲの非対話式バージョンは、後述の通りに存在し、何らかの場合に周知のデジタル署名アルゴリズム（ＤＳＡ：DigitalSignature Algorithm）などの確立された署名方式に代わるものを提供する。

【００５５】

正規のデジタル署名方式のように、チャレンジ・レスポンス署名方式では、署名者は、署名の生成および検証にそれぞれ使用する秘密鍵と公開鍵のペアを有し、検証者は署名者の真正公開鍵を入手するものと想定されている。とりわけ、両当事者は署名プロトコルの開始前に秘密を共有しているものとは想定されておらず、署名の計算にこのような共有秘密は必要ではない。しかし、正規の署名とは対照的に、その基本的な形式では、チャレンジ・レスポンス署名は対話式であり、署名者が所与のメッセージ上に署名を生成する前に署名の受信側（たとえば、検証者）が署名者に対してチャレンジを発行する必要がある。安全なチャレンジ・レスポンス署名方式は、正当な署名者以外の人は誰も、その署名を有効なものとして受け入れるようチャレンジャを納得させるような署名を生成できないことを保証する必要がある。とりわけ、署名は、メッセージ固有であるだけでなく、チャレンジ固有のものでもある。

【００５６】

これに対して、チャレンジャによる署名の検証可能性を保証することは関心のあることであり、したがって、署名の転送可能性または第三者による検証可能性に関する想定または要件はまったく存在しない。その上、後述の特定の方式は、チャレンジを選択する当事者が、その特定のチャレンジに関して有効な署名をどのメッセージ上でも必ず生成できるという特性を有する。本出願に関してより重要であり、この方式を他の対話式署名から区別するものは、検証者がチャレンジを使用して、署名者と同じ（または関連する）署名ストリングを計算できることである。

【００５７】

上記の通り、ｇは（通常は素数）次数ｑの群Ｇの生成元である。また、Ｈは｜ｑ｜／２ビット

【数９】

$$(|q| = \lceil \log_2 q \rceil)$$

を出力するハッシュ関数であるが、この場合も、「素数次数（prime order）」の使用およびＨの出力の特定の長さは、模範的な諸実施形態の模範的な設計の詳細に過ぎず、本発明に不可欠なものではない。

【００５８】

ＸＣＲ署名方式の定義

図４に例示されている指数チャレンジ・レスポンス（ＸＣＲ）署名方式５００は以下のように定義される。すなわち、Ｂハットで表されるＸＣＲ方式内の署名者は、秘密鍵$b \in_R Z_q$と公開鍵$B = g^b$とを所有する。Ａハットで表される検証者（またはチャレンジャ）は、$x \in_R Z_q$の場合にＡハットが$X = g^x$として計算する最初のチャレンジＸを提供し、ここでｘはＡハットによって選択され、秘密に保持される。チャレンジＸを使用する所与のメッセージｍ上のＢハットの署名は、

【数１０】

$$(Y, X^{y+\bar{H}(Y,m)b})$$

というペアとして定義され、ここで$Y = g^y$であり、$y \in_R Z_q$はＢハットによって選択され、指数ｙ＋Ｈバー（Ｙ，ｍ）ｂはｑを法として換算される。検証者Ａハットは、それが

【数１１】

$$(YB^{\bar{H}(Y,m)})^x = \sigma$$

であると判断した場合のみ、（メッセージｍおよびチャレンジ$X = g^x$について）有効な

ものとして署名ペア（Ｙ，σ）を受け入れる。

【００５９】

ここで以下の表記法を使用する。すなわち、所与のメッセージｍ、チャレンジＸ、および値Ｙの場合に、

【数１２】

$$XSIG_B(Y,m,X) = X^{y+\bar{H}(Y,m)b}$$

と定義する。すなわち、

【数１３】

$$XSIG_{\hat{B}}$$

は、ＸＣＲ署名ペア内の第２の元を表している。一般的な注記として、「メッセージ」という単語の上記の使用が、送信データ、ファイル、媒体などを含むビット・ストリームによって表すことができ、それ自体がより長いメッセージのハッシュ・バージョンになりうる任意の形式のデータまたは情報を表すことは注目する価値がある。このメッセージは、図５に図示されているように両当事者に対して入力できるか、ある当事者から他の当事者に伝送できるか、あるいは第三者、外部ソースなどから提供することができる。

【００６０】

本出願に記載されている通り、ＸＣＲ署名の利点としては、分析の健全性（立証可能性）、検証者と証明者の両方による計算可能性、二重性（単一の計算は２当事者以上による署名の結合を表す）、「ハッシュ可能性（hashability）」（すなわち、ハッシュ署名を処理し検証する能力）、鍵または共通値の導出、転送不能性および否認可能性、（否認可能な署名から伝統的な否認不能な署名への）変換可能性、（特に対話環境で）ＤＳＳより堅固な代替策を提供すること、ならびに非対話式変種の存在を含む。

【００６１】

そこからＸＣＲ署名が導出されるＳｃｈｎｏｒｒの識別方式に対する関連を介してＸＣＲ方式の設計の動機になることは、例証となる可能性がある。Ｓｃｈｎｏｒｒの（対話式）識別方式は、所与の入力Ｂ＝g^bに関する離散対数ｂを把握していることの証明から構成される。Ｂハットがこの方式の証明者（ｂを所有するもの）を表し、Ａハットが検証者（入力Ｂが与えられるもの）を表すものとする。基本的なＳｃｈｎｏｒｒの識別は以下の３つのメッセージから構成される。

（ｉ）Ｂハットは$y \in_R Z_q$を選択し、Ｙ＝g^yをＡハットに送信する。

（ｉｉ）Ａハットはランダム値$e \in_R Z_q$で応答する。

（ｉｉｉ）Ｂハットは値ｓ＝ｙ＋ｅｂをＡハットに送信する。Ａハットは、g^s＝ＹB^eが有効である場合のみ、受け入れる。

【００６２】

このプロトコルは、正直な検証者Ａハット（たとえば、ランダムに一律にｅを選択する人）に対する（ｂの）知識のパブリックコイン型ゼロ知識証明（public-coin zero-knowledge proof）である。したがって、これは、周知のＦｉａｔ－Ｓｈａｍｉｒ方法を介してランダム・オラクル・モデルで立証可能に安全な署名方式、すなわち、

【数１４】

$$SIG_{\hat{B}}(m) = (Y, y + H(Y,m)b)$$

に変換することができる。

【００６３】

次に、ＡハットからＢハットへの第１のメッセージが追加される、以下のＳｃｈｎｏｒｒプロトコルの４メッセージ変種について検討する。この第１のメッセージで、Ａハットは値Ｘ＝g^xをＢハットに送信する。次に、Ｓｃｈｎｏｒｒの方式からの３つのメッセージが続くが、メッセージ（ｉｉｉ）、すなわち、変更済みプロトコルの第４のメッセージでは、ｓ＝ｙ＋ｅｂをＡハットに送信するのではなく、ＢハットがＳ＝X^sを送信する。Ａハットは、Ｓ＝（ＹB^e）^{x}である場合のみ、受け入れる。このプロトコルは任意の値Ｘ∈ＧについてＤｉｆｆｉｅ－Ｈｅｌｌｍａｎ値ＣＤＨ（Ｂ，Ｘ）を計算するＢハットの「能力」の証明であることが分かる。その上、このプロトコルはランダムにｅを選択する検

証者Ａハットに対するゼロ知識であり、Ｘは任意に選択することができる。

【００６４】

Ｆｉａｔ－Ｓｈａｍｉｒ変換をこのプロトコルに適用することにより、本発明のチャレンジ・レスポンス署名ＸＣＲが得られる。また、これは、ＸＣＲ方式を命名する際に「指数」という用語が使用される理由も説明しており、Ｓｃｈｎｏｒｒ方式のｓ＝ｙ＋ｅｂをこのプロトコルの最後のメッセージのX^sで置き換えることを指している。

【００６５】

ＣＤＨ仮説に基づくＸＣＲ署名方式のセキュリティの追加の態様については上記の仮出願でさらに論じられている。

【００６６】

上記の用語のいくつかを説明する際に、Ｇ内の２つの元であるＵ＝g^u、Ｖ＝g^vの場合、Ｄｉｆｆｉｅ－Ｈｅｌｌｍａｎ計算をＵおよびＶに適用した結果をＣＤＨ（Ｕ，Ｖ）によって表す（たとえば、ＣＤＨ（Ｕ，Ｖ）＝g^{uv}）。このアルゴリズムは、入力としてＧ内の元（Ｕ，Ｖ）のペアを取り、Ｄｉｆｆｉｅ－Ｈｅｌｌｍａｎ結果ＣＤＨ（Ｕ，Ｖ）を出力する場合、「Ｇに関するＣＤＨ求解ルーチン（solver）」と呼ばれる。仮出願でさらに提供される分析で使用される主な至難性仮説（intractability assumption）は計算Ｄｉｆｆｉｅ－Ｈｅｌｌｍａｎ（ＣＤＨ）仮説である。Ｇに関するすべての効率的なＣＤＨ求解ルーチンの場合、Ｕ，Ｖ$\in_R$Ｇに関するペア（Ｕ，Ｖ）について求解ルーチンが正しい値ＣＤＨ（Ｕ，Ｖ）を計算する確率が無視できるものである場合（この確率は求解ルーチンのランダム・コインについて取られ、Ｕ，Ｖの選択はＧ内でランダムに独立して行われる）、ＣＤＨ仮説は群Ｇで有効であると言える。

【００６７】

Ｈバー（Ｙ，ｍ）内のビット数

ｌはＨバー（Ｙ，ｍ）内のビット数とする。明らかなことに、ｌが小さくなるほど署名方式の効率が高くなることを示す。これに対して、指数Ｈバー（Ｙ，ｍ）が予測可能であると、署名方式が不安定になるので、ｌが小さすぎる場合、セキュリティ・バウンド（security bound）が不良であることを示す。しかし、セキュリティのためにどの程度の大きさのｌが必要であるかが問題である。

【００６８】

ｌ＝１／２｜ｑ｜という設定によって良好なセキュリティ・パフォーマンスのトレードオフが得られ、このため、ＸＣＲ署名の模範的な指定で（しかも本発明のＨＭＱＶプロトコルへのその模範的な適用のために）この値が使用されることが分かる（上記の仮出願の考察を参照されたい）。

【００６９】

Ｂとの対話の順序の変更

とりわけ、ＨＭＱＶプロトコルの分析に適用されるＸＣＲ署名のいくつかの適用例では、チャレンジャＡハットと署名者Ｂハットとの対話の順序を変更することができる。

【００７０】

ＸＣＲ方式の上記の定義では、Ａハットは、Ｂハットにチャレンジ Ｘを提供すると同時にＢハットにメッセージｍを提示し、その結果、Ｂハットは署名ペア

【数１５】

$$(Y, XSIG_{\hat{B}}(Y,m,X))$$

で直ちに応答することができる。現在検討している変更済みバージョンでは、以下の順序の対話が行われる。

（ｉ）ＡハットはＢハットにメッセージｍを提示し、ＢハットはＹを出力し、その後の何らかの時点で

（ｉｉ）ＡハットはＢハットに（Ｙ，ｍ，Ｘ）を提供し、Ｂハットは

【数１６】

$$XSIG_{\hat{B}}(Y,m,X)$$

を出力する。

【００７１】

次に、当事者Ｆがこの変更済み順序を取るようＢハットに照会するものと想定する。とりわけ、ＦはＢハットとの種々の対話をインターリーブすることができ、すなわち、Ｆは、対応するステップ（ｉｉ）を実行する前にステップ（ｉ）のいくつかのインスタンスを実行することができる。これは、ＢハットがＹ、ｙ、およびｍという値でステップ（ｉ）後の状態を保持することを必要とする。その後、Ｆがステップ（ｉｉ）で（Ｙ，ｍ，Ｘ）を提示すると、Ｂハットは、それがその状態内にペア（Ｙ，ｍ）を有することをチェックし、有する場合に

【数１７】

$$XSIG_{\beta}(Y,m,X)$$

で応答し、その状態から（Ｙ，ｍ）を消去する（Ｂハットがその状態内にペア（Ｙ，ｍ）を持っていない場合、それはその署名を発行しない）。

【００７２】

Ｂハットのアクションのこの指定によって、Ｂハットが２つの異なる署名に同じＹ値を使用しないことを保証することに留意されたい。ＢハットによるＹの選択のシミュレーションがＸの知識を必要としないが、Ｈバー（Ｙ，ｍ））を決定するためにｍの値のみが必要であるという理由だけで、ＸＣＲ署名のセキュリティの証明がこの変更済み順序について引き続き有効であることは、容易に検証することができる。

【００７３】

ハッシュＸＣＲ変種（ＨＣＲ）

ＸＣＲ署名（Ｙ，σ）のペアをペア（Ｙ，Ｈ（σ））で置き換えることが可能であり、ここでＨはハッシュ関数であり、このような「ハッシュＸＣＲ」署名は「ＨＣＲ」と略記される。ＸＣＲ特性によって検証者がＹのついてσを再計算できるので、Ｙが与えられると、Ｈ（σ）も計算することができ、このため、変更済みＨＣＲ署名を検証できることに留意されたい。

【００７４】

ＨＣＲ署名は、いくつかの設定で重要な、所定の範囲の特性を有する。たとえば、その署名は正規のＸＣＲ署名より短い場合もあれば、結果的にランダム値または疑似ランダム値になる場合もあり、攻撃者がσ内の代数構造を学習するのを防止する場合などもある。

【００７５】

とりわけ、対話式および検証者固有の認証環境（鍵交換プロトコルなど）では、ＨＣＲ署名は、ＤＳＡ署名に代わるより安全なものを提供する。実際に、ＤＳＡでは、単一の一時指数（たとえば、ＤＳＡ署名の成分ｒ＝g^k内のｋ）を開示すると、秘密署名鍵を明かすことにより、署名方式が完全に不安定になり、一時指数ｙが攻撃者に明かされた場合でも、ＨＣＲ署名は捏造不能である（ただし、この場合、署名者がチャレンジＸの順序をテストするかまたは余因数べき乗（co-factor exponentiation）を使用して強制的にその値を少なくとも次数ｑのものにすることを条件とする）。

【００７６】

非対話式ＸＣＲ変種

ＸＣＲ（およびＨＣＲ）署名は、Ｘ＝Ａを書き込むことにより、非対話式だが検証者固有のものにすることができ、ここでＡは、図６に図示されている通り、検証者の公開鍵である。これは、非常に効率的な非対話式で検証者固有の否認可能認証メカニズムを提供する。ある変形では、当事者Ａハットの固有の公開鍵Ａを使用するのではなく、後者は署名者が使用するために１つまたは複数のチャレンジを公表する（たとえば、Ｗｅｂサイトでポストする）ことができ、したがって、Ａハット自体が署名時に使用可能ではない場合でも、これらのチャレンジが使用可能になる。

【００７７】

変換可能ＸＣＲ署名

ＸＣＲ署名の顕著な特性（とりわけ、共有秘密および公開鍵暗号化に基づくものを含み

、他の「否認可能」チャレンジ・レスポンス・メカニズムからそれを区別するもの）は、これらの署名を正規の否認不能な署名に「変換」する能力である。変換可能署名は、否認可能認証の特性を有し、すなわち、意図された受信側のみによって検証することができるが、署名者も自分の秘密署名鍵を明かさずに自分が所与の署名の作成者であることを最終的に証明することができる。

【００７８】

秘密署名から公開署名へのこの変換可能性は、たとえば、数年後に検証可能な公開記録に変換しなければならない職務上の非公式通信のために必要である可能性がある。ＸＣＲ署名の場合、チャレンジＸに基づくメッセージｍ上の署名（Ｙ，σ）は、値ｙ＋Ｈバー（Ｙ，ｍ）ｂを明かすことにより、正当な署名者によって正規の否認不能な署名に変換することができる。

【００７９】

他の（受信側固有の）変換可能署名は文献に提示されているが、そのいずれでも、意図された受信側（またはチャレンジャ）は独力で署名を再計算することができず、このため、以下の二重ＸＣＲ署名によって例示されている通り、この再計算特性がＸＣＲ署名に提供する多くの利点を共有しない。

【００８０】

二重ＸＣＲ署名（ＤＣＲ）

ＸＣＲ署名の重要な特性の１つは、チャレンジを選択したチャレンジャが独力で署名を計算できることである。ここで、任意の２当事者Ａハット、Ｂハットがチャレンジャと署名者という二重の役割で互いに対話でき、それぞれがいかなる第三者も捏造できない署名を生成するという特性を備えた関連チャレンジ・レスポンス署名方式（本明細書では「二重ＸＣＲ方式」または略してＤＣＲという）を導出するためにこの特性を利用する方法が示される。その上、これは、この方式をＨＭＱＶプロトコルにとって重要なものにするものであり、結果として得られるＡハットおよびＢハットによる署名は同じ値を有する。より正確には、それらはＸＣＲ署名ペア内に同じＸＳＩＧ成分を有する。

【００８１】

定義：　二重（指数）チャレンジ・レスポンス（ＤＣＲ）署名方式。ＡハットおよびＢハットは、それぞれ公開鍵Ａ＝g^a、Ｂ＝g^bを有する２当事者とする。m_1、m_2は２つのメッセージとする。それぞれメッセージm_1、m_2上のＡハットおよびＢハットの二重ＸＣＲ署名（略してＤＣＲ）は、Ｘ、Ｙ、および

【数１８】

$$DSIG_{\hat{A},\hat{B}}(m_1,m_2,X,Y) \doteq g^{(x+da)(y+eb)}$$

という３つ組の値として定義され、ここでＸ＝g^xおよびＹ＝g^yはそれぞれＡハットおよびＢハットによって選択されたチャレンジであり、記号ｄおよびｅはそれぞれＨバー（Ｘ，m_1）およびＨバー（Ｙ，m_2）を表している。（図７を参照されたい。）

【００８２】

このため、ＤＣＲ署名の基本的な特性は、値ＸおよびＹ（それぞれＡハットおよびＢハットによって選択されたｘおよびｙを含む）を交換した後、ＡハットとＢハットの両方が同じ署名

【数１９】

$$DSIG_{\hat{A},\hat{B}}(m_1,m_2,X,Y)$$

を計算（および検証）できることである。これは、

【数２０】

$$DSIG_{\hat{A},\hat{B}}(m_1,m_2,X,Y) = g^{(x+da)(y+eb)} = (YB^e)^{x+da} = (XA^d)^{y+eb}$$

という等値（equivalence）から分かり、ここでｘ＋ｄａおよびｙ＋ｅｂはｑを法として換算される。

【００８３】
その上、上記の仮出願の考察に実証されている通り、攻撃者はこの署名を実行できるように計算することができない。
【００８４】
大ざっぱに言えば、二重署名は、チャレンジＹＢ^{e}に基づくメッセージｍ$_{1}$上のＡハットによるＸＣＲ署名であると同時にチャレンジＸＡ^{d}に基づくメッセージｍ$_{2}$上のＢハットによるＸＣＲ署名である。より正確には、値ｄおよびｅは署名プロセス中に（メッセージｍ$_{1}$、ｍ$_{2}$のおそらく敵対的な選択により）決定されるので、ＢハットのＤＣＲ署名は攻撃者によって選択されたわけではない任意の値Ａ＝ｇ^{a}に関して安全であることを実証することができる。
【００８５】
基本ＨＭＱＶプロトコルの形式的説明
ＨＭＱＶプロトコルは、その基本的２メッセージ交換において、そこから両当事者ＡハットおよびＢハットが
【数２１】

$$DSIG_{\hat{A},\hat{B}}("\hat{A}","\hat{B}",X,Y)=g^{(x+da)(y+eb)}$$

という二重ＸＣＲ署名を計算するためのチャレンジとして機能するＤｉｆｆｉｅ－Ｈｅｌｌｍａｎ値Ｘ＝ｇ^{x}およびＹ＝ｇ^{y}の両当事者間の交換から構成される。次に、この値をハッシュすることにより、セッション鍵が導出される。このように、署名自体は伝送する必要がなく、セッション鍵の共通導出値を保証するのは署名の一意性（uniqueness）であり、主張された当事者Ａハット、Ｂハットによって交換が実行されたという証明を可能にするのは鍵（同等に、署名）を計算する固有の能力である。
【００８６】
基本的に、署名が計算されるメッセージｍ$_{1}$、ｍ$_{2}$はピアのＩＤ（すなわち、Ａハット、Ｂハット）であるので、両当事者は、自分が計算した鍵が正しいＩＤに一意的に拘束されるという保証を得る。署名の元に（とりわけ、値ｄおよびｅの計算において）一時Ｄｉｆｆｉｅ－Ｈｅｌｌｍａｎ値だけでなく、両当事者のＩＤをこのように含めることは、ＵＫＳ攻撃などの何らかの認証障害を回避するために不可欠である。
【００８７】
したがって、２当事者Ａハット、Ｂハット間のＨＭＱＶプロトコルのセッションは、Ｈ（π）として計算されたセッション鍵によるＤＨ値Ｘ＝ｇ^{x}およびＹ＝ｇ^{y}（図１）の基本Ｄｉｆｆｉｅ－Ｈｅｌｌｍａｎ交換から構成され、ここで
【数２２】

$$\pi = DSIG_{\hat{A},\hat{B}}(m_1=\hat{B},m_2=\hat{A},X,Y)$$

である。すなわち、πは互いのＩＤに関するＡハットおよびＢハットの二重署名として計算される。上記の署名は、省略表現π（Ａハット，Ｂハット，Ｘ，Ｙ）によって表され、すなわち、
【数２３】

$$\pi(\hat{A},\hat{B},X,Y) \doteq DSIG_{\hat{A},\hat{B}}(m_1=\hat{B},m_2=\hat{A},X,Y)=g^{(x+da)(y+eb)}$$

であり、ここでｄ＝Ｈバー（Ｘ，Ｂハット）、ｅ＝Ｈバー（Ｙ，Ａハット）であり、Ａ＝ｇ^{a}、Ｂ＝ｇ^{y}はそれぞれ両当事者Ａハット、Ｂハットの公開鍵である。π（Ａハット，Ｂハット，Ｘ，Ｙ）＝π（Ｂハット，Ａハット，Ｙ，Ｘ）であることは、この時点で留意すべきである。ある変形では、Ｈ（π）はπの異なる関数で置き換えることができ、とりわけ、ハッシュは両当事者のＩＤなどの追加の情報を含むことができる。
【００８８】
ＨＭＱＶプロトコルは典型的には、そのプロトコルを実行するために全当事者のいずれかを呼び出すことができるマルチパーティ・ネットワークで実行される。ある当事者側で

プロトコルを呼び出すたびにセッション（プロトコルのこの特定のインスタンスに関連する情報を含むローカル状態）が作成され、それにより、完了時に発信メッセージとセッション鍵の出力を生成することができる。セッション中に以下のように３通りのタイプの起動によってある当事者を起動することができる（以下の説明では、Ａハットは起動される当事者のＩＤを表し、Ｂハットはセッションに対する意図されたピアのＩＤを表している）。

１．Ｉｎｉｔｉａｔｅ（Ａハット，Ｂハット）：　Ａハットは、値$X = g^x$、$x \in_R Z_q$を生成し、（不完全な）セッション（Ａハット，Ｂハット，Ｘ）として識別するＨＭＱＶのローカル・セッションを作成し、その発信メッセージとして値Ｘを出力する。

この起動の意味は、ＡハットがＢハットとのセッションの起動側（initiator）として起動されていることであり、Ｘはこのセッションの一部としてピアＢハットに配信する予定のメッセージである。当事者Ａハットはセッションの「保有者（holder）」（または「所有者（owner）」）と呼ばれ、Ｂハットはセッションに対する「ピア」と呼ばれ、Ｘは発信（ＤＨ）値と呼ばれる。

２．Ｒｅｓｐｏｎｄ（Ａハット，Ｂハット，Ｙ）：　ＡハットはＹ≠０であることをチェックする。そうである場合、Ａハットは、値$X = g^x$、$x \in_R Z_q$を生成し、Ｘを出力し、ＩＤ（Ａハット，Ｂハット，Ｘ，Ｙ）およびセッション鍵Ｈ（π（（Ａハット，Ｂハット，Ｘ，Ｙ））を有するセッションを完了する。ここで、Ａハットは、ピアＢハットおよび着信値Ｙを有するセッションにおいて応答側として起動されている。この場合、Ａハットは直ちにそのセッションを完了する（それ以上の着信メッセージはまったく存在しない）。着信値Ｙがゼロである場合、Ａハットが起動を無視することに留意されたい。

３．Ｃｏｍｐｌｅｔｅ（Ａハット，Ｂハット，Ｘ，Ｙ）：　Ａハットは、Ｙ≠０であることと、ＩＤ（Ａハット，Ｂハット，Ｘ）を有する公開セッションを有することをチェックする。これらの条件のいずれかが適合しない場合、Ａハットは起動を無視し、適合する場合、ＡハットはセッションＩＤ（Ａハット，Ｂハット，Ｘ，Ｙ）およびセッション鍵Ｋ＝Ｈ（π（（Ａハット，Ｂハット，Ｘ，Ｙ））を有するセッションを完了する。これは、（申し立てによると）ピアＢハットからの応答である着信値Ｙによる、このプロトコルにおける第２のメッセージの配信を表している。

【００８９】

３メッセージＨＭＱＶ－Ｃプロトコル

３メッセージＨＭＱＶ－Ｃ（Ｃは「鍵確認（key Confirmation）」を意味する）プロトコルは図８に描写されている。このプロトコルは、ＨＭＱＶのすべてのセキュリティ特性、特に同じ計算コストを享受する。しかし、これは、第３のメッセージをプロトコルに追加し、プロトコル・メッセージの長さをわずかに増加させるものである。

【００９０】

代わりに、ＨＭＱＶ－Ｃは、鍵確認、ＰＦＳ、および汎用構成可能性（universal composability）を含む、基本ＨＭＱＶプロトコルで欠けているいくつかの特性を提供する。

【００９１】

鍵確認

ＨＭＱＶプロトコルは、ピアＢハットおよびセッション鍵Ｋを有するセッションを完了する当事者Ａハットに基本的な保証を提供し、Ｂハットが破壊されていない場合、Ｂハットのみがおそらくを把握することができる。このプロトコルが提供しないものは、Ｂハットがセッションを完了したかまたはセッション鍵を計算したというＡハットに対する保証である。その上、Ｂハットは、セッションの実行中に「活動中」ではなかった可能性がある。

【００９２】

（典型的な公開鍵シナリオのように、ＡハットとＢハットとの間のそれ以前の通信で、いかなる事前共有状態も作成されなかったと想定すると）いずれの２メッセージ公開鍵ベースのプロトコルについても同じことが当てはまるので、これはＨＭＱＶのみの欠点ではない。さらに、Ｓｈｏｕｐによって指摘されたように、その鍵を使用してそれぞれが開始

する前にピアがセッションを完了しているという保証を両当事者が有するという表面上当然の目標は、いずれの鍵交換プロトコルでも達成することができない。実際に、攻撃者は、最後のプロトコル・メッセージがその宛先に到着しないようにすることにより、この相互保証を必ず阻止することができる。

【００９３】

しかし、ピアが鍵を計算できたという両当事者のそれぞれに対する保証が弱い場合（しかし、必ずしも、呼び出し側アプリケーションに鍵を出力するという保証ではない）、その保証は達成可能であり、文献では鍵確認特性と呼ばれる。鍵交換の基本セキュリティにとって決定的なものではないが（たとえば、鍵確認の欠如は鍵によって保護された通信のプライバシまたは確実性にとって脅威ではない）、この特性はいくつかの適用例に有用な「動作上の健全性のチェック（operational sanity check）」を提供することができる。

【００９４】

この場合、追加のＭＡＣ値が鍵確認を可能にするので、プロトコルＨＭＱＶ－ＣはＨＭＱＶより適している。その上、ＭＡＣ妥当性検査は、セッションに対する識別済みピアの積極的な関わりとともに、このピアが一致セッション（すなわち、同じピアおよび同じセッション鍵を有する）を所有するという事実を確認する。これらの特性を達成するために、ＨＭＱＶ－ＣのＭＡＣは、任意の特定のセッション情報に適用する必要はないが、単にメッセージの「方向」を示すためならびに反射を防止するために使用される単一ビットに適用する必要があることに留意されたい。また、ＨＭＱＶ－Ｃの最初の２つのメッセージのみから構成されるプロトコルが起動側に鍵確認を提供すること（それにより、プロトコル・メッセージの数を増加せずにＨＭＱＶに有用な特徴を追加する可能性がある）も留意する価値がある。

【００９５】

鍵交換の多くの適用例では、鍵確認の欠如の結果、たとえば、Ｂハットに保護情報を送信するために、当事者Ａハットが鍵を使用し始めるが、Ｂハットはまだその鍵を確立していないので、この情報を処理することができないという、ある形の「サービス妨害」（ＤｏＳ：denial of service）攻撃が行われる可能性がある。言われている通り、相互「セッション完了」確認は達成不能なので、この状況は完全に回避することができない。

【００９６】

その上、ある当事者がピアの無効性を発見する前に相当な計算サイクルを費やすこと（およびセッション状態を作成すること）を強要されるという、公開鍵動作に基づくプロトコルに対してより深刻な形のＤｏＳ攻撃が存在する。プロトコル・メッセージの追加という犠牲を払って任意の鍵交換プロトコル（ＨＭＱＶを含む）に適用でき、ＤｏＳ攻撃に対して有用だが範囲が限られた対策がいくつか存在する。

【００９７】

完全転送秘密（ＰＦＳ）

完全転送秘密は、それにより長期秘密鍵が漏洩しても古いセッション鍵のセキュリティを危険にさらさない、鍵交換プロトコルの非常に望ましい特性である。より形式的には、破壊されていない当事者Ａハットが破壊されていないピアＢハットとの鍵交換セッションを確立する場合、ＡハットでＫが満了した後で攻撃者がＡハットを破壊するかまたはＢハットでＫが満了した後で攻撃者がＢハットを破壊しても、セッション鍵Ｋは引き続き安全である。ＨＭＱＶを含む、暗黙認証を伴う２メッセージ・プロトコルはいずれも、活発な攻撃者に対する完全な完全転送秘密を提供することができない。その代わりに、望むことができる最良のものは、ＨＭＱＶによって提供される弱い形のＰＦＳである。基本的な２メッセージＨＭＱＶに対するＨＭＱＶ－Ｃの主な利点は、仮出願にさらに説明されている通り、それがＨＭＱＶの固有の制限を引き上げ、完全なＰＦＳを提供することである。

【００９８】

汎用構成可能性セキュリティ

鍵交換に関するＣａｎｅｔｔｉ／Ｋｒａｗｃｚｙｋのモデルは、仮出願におけるＭＱＶおよびＨＭＱＶの分析の基礎であり、実社会環境の場合のように、他のアプリケーション

と同時に実行されたときに鍵交換プロトコルのセキュリティを保証することを目標とする、より意欲的なモデルに拡張されている。このモデルは、鍵交換の汎用構成可能性（ＵＣ：Universal-Composability）モデルとして知られている。

【００９９】

ＨＭＱＶ－Ｃの場合、セッションを完了すべき第１の当事者がそのセッション鍵を出力すると、ピアの状態は、プロトコルおよびセッション鍵内の公開情報から「シミュレート」可能な情報のみを含むことが分かる。Ｃａｎａｔｔｉ／Ｋｒａｗｃｚｙｋは、仮出願に示されているＨＭＱＶの他のセキュリティ特性とともに、この特性がＨＭＱＶプロトコルの汎用構成可能性を保証するために十分であることを示している。

【０１００】

１パスＨＭＱＶ

図９に示されている１パス鍵交換プロトコルは、送信側Ａハットから受信側Ｂハットに送信された単一メッセージから構成され、両当事者およびセッションが以下に定義するように破壊されていない限り、そこから両当事者はそれぞれの秘密鍵と公開鍵を使用して、ＡハットおよびＢハットのみがおそらく把握できる固有の鍵を導出する。

【０１０１】

確立された鍵からの要件は、Ｂハットによって受信されたメッセージがＡハットからの古いメッセージの再生である可能性を除いて、正規の鍵交換プロトコルと同じである。この再生は、１パス・プロトコルで避けられないものであるが、同期時間または共有状態などのその他の手段によって検出可能である可能性がある。

【０１０２】

加えて、Ｂハットからのセッション固有の入力の欠如により、その鍵はＢハットの秘密鍵の単独知識で計算可能でなければならないので、このようなプロトコルはＰＦＳを提供することができない。

【０１０３】

本発明の一実施形態では、それぞれ公開鍵$A=g^a$、$B=g^b$を有する当事者ＡハットとＢハットとの間の１パスＨＭＱＶプロトコルは、ＡハットからＢハットに伝送された単一値$X=g^x$から構成され、ここで$x\in_R Z_q$はＡハットによって選択される。セッション鍵Ｋは以下のようにＡハットによって計算される。

（ｉ）（Ａハット，Ｂハット）は２つのＩＤ　ＡハットおよびＢハットを含むメッセージを表すものとし、ｄ＝Ｈバー（Ｘ，（Ａハット，Ｂハット））の結果になるようにｄを設定する。

（ｉｉ）

【数２４】

$$XSIG_{\hat{A}}(X,(\hat{A},\hat{B}),B)=B^{x+da}$$

を計算する。

（ｉｉｉ）Ｋ＝Ｈ（σ，Ａハット）を設定し、ここでＨは必要な鍵の長さに等しいビット数を出力する。同じ鍵Ｋは、Ｘ≠０であることをチェックした後、ＢハットによってＫ＝Ｈ（（XA^d）^{b}）として計算される。変形では、Ｋ＝Ｈ（σ，Ａハット，Ｂハット）である。

【０１０４】

換言すれば、１パスＨＭＱＶのこの実施形態の鍵は、Ｂハットの公開鍵をチャレンジとして使用して、非対話式ＸＣＲ著名から導出される。

【０１０５】

１パス・プロトコルは認証選択暗号文セキュア（ＣＣＡ：chosen-ciphertext secure）暗号化方式として使用できることも指摘されている。すなわち、Ａハットは、（選択暗号文攻撃に対して）暗号化されるとともに（Ａハットにより）認証されたメッセージｍをＢハットに伝送することができる。一実施形態では、Ａハットは、３つ組（Ｘ，ｃ，ｔ）を送信することになり、ここで$X=g^x$であり、ｃは鍵K_1に基づいてメッセージｍの対称選

択平文セキュア（ＣＰＡ：chosen-plaintextsecure）暗号化として得られる暗号文であり、ｔは鍵K_2に基づいてｃについて計算されたＭＡＣ値である。鍵K_1およびK_2は、１パスＨＭＱＶプロトコルのようにＸから計算された鍵Ｋから導出される。

【０１０６】

この手順の全体的なコストは、Ａハットについては２つのべき乗（一方はオフライン）であり、Ｂハットについては１．５である。これは、ＤＨＩＥＳ（Ｄｉｆｆｉｅ－Ｈｅｌｌｍａｎ統合暗号化方式：Diffie-Hellman Integrated Encryption Scheme）などの代替ＣＣＡ暗号化方式と比較してＢハットについて１／２べき乗多いだけであるが、代わりに、Ａハットからの認証を提供する（ＤＨＩＥＳの場合、この認証はＡハットから完全な追加の署名を返すことになるであろう）。この効率的な認証ＣＣＡ暗号化は、一般的な「プリティグッド・プライバシ（ＰＧＰ：Pretty-GoodPrivacy）」アプリケーションなどの「蓄積交換（store-and-forward）」アプリケーションにとって非常に魅力的であり、通常の署名暗号化（sign-and-encrypt）パラダイムよりかなり安価である。この場合、唯一の警告は、暗号化解除動作に必要であるので、ＩＤ　Ａハット（およびおそらくその証明書）は平文で伝送する必要があることである。

【０１０７】

上記のプロトコルのさらに他の特性のうち、留意する価値のあるものは、必ずしも暗号化部分を追加せずにメッセージｍ上のＡハットの検証者固有の署名としてのみ使用できることである。しかし、この署名は、受信側固有のものであり、したがって、否認防止を提供しない。その代わりに、ＰＧＰなどの多くの適用例で非常に価値ある特徴である否認可能性を提供する。

【０１０８】

ＭＱＶを採用した規格の多くはその１パス変種も採用していることは留意すべきである。その種々の形（１メッセージ、２メッセージ、および３メッセージ）でのＨＭＱＶの採用に関心のある規格の場合、ＨＭＱＶの他の変種の導出と同様に、１パス・プロトコルで鍵の導出を定義することは意味をなすであろう。

【０１０９】

具体的には、ＨＭＱＶプロトコルを定義する二重署名においてＹをＢで置き換えることにより、１パス鍵について以下の値が得られ、ＡハットおよびＢハットはそれぞれ、

【数２５】

$$\sigma_{\hat{A}} = (BB^{e})^{x+da}$$

および

【数２６】

$$\sigma_{\hat{B}} = (XA^{d})^{b+eb}$$

を計算し、鍵Ｋをこれらの（等しい）値のハッシュに設定する。この場合、他の変種と互換性のあるものにすることを除き、指数ｅはいかなる値もプロトコルに追加しないことに留意されたい。これは、実際に、プロトコル効率をいくらか減ずるものである。

【０１１０】

しかし、ＨＭＱＶの１パス・バージョンのｄ＝Ｈバー（Ｘ，（Ａハット，Ｂハット））という値と２メッセージ・バージョンのｄ＝Ｈバー（Ｘ，Ｂハット）という値の間には追加の矛盾が存続する。３つのモード間の互換性を提供する方法は、これらのいずれでもｄ＝Ｈバー（Ｘ，Ｂハット）、ｅ＝Ｈバー（Ｙ，Ａハット）を有し、ここで１パスの場合にＹ＝Ｂであり、セッション鍵導出関数、すなわち、Ｋ＝Ｈ（σ，Ａハット，Ｂハット）（何らかの固定基準を使用して定義されたＡハットおよびＢハットの次数を有する）にＩＤ　Ａハット、Ｂハットを追加することになるであろう。これは、ｄの計算においてＡハットを追加する必要性に取って代わるものである。また、事前計算ＤＨ値が漏洩した場合にＨＭＱＶを強化し、潜在的に未知の鍵共有攻撃を回避するという利点も有する。

【０１１１】

ＨＭＱＶのセキュリティ態様の要約

従来のＭＱＶプロトコルに比較して、ＨＭＱＶプロトコルは、以下のものを含む、いくつかのパフォーマンス上の利点を提供する。ＨＭＱＶは、このプロトコルで伝送されるＤＨ値に関する高価な素数次数テストの必要性を立証可能に省くものである。仮出願で実証されている通り、攻撃者がローグ（rogue）ＤＨ値の選択の恩恵を受けうる唯一の方法は、ゼロになるようにそれらを選択することであり、したがって、単純な非ゼロ・チェックがＨＭＱＶで必要なすべてである。このため、素数次数テストの必要性またはＭＱＶプロトコルで同時に使用される余因数ｈの必要性はまったくない。

【０１１２】

ＨＭＱＶプロトコルが数学的に立証可能な方法で達成する特性のリストは以下の通りである。

（１）ＨＭＱＶは、ＣａｎｅｔｔｉおよびＫｒａｗｃｚｙｋの強い形式的鍵交換モデルで安全なものである。

（２）ＨＭＱＶは、両当事者の秘密鍵にアクセスできない攻撃者による詐称に耐えるものである。

（３）ＨＭＱＶは、交換の当事者のＩＤにＸＣＲ署名を適用し、その結果、ＵＫＳおよびその他の認証攻撃を回避することにより、これらの当事者のＩＤと鍵との間に固有の結合を確立する。

（４）ＨＭＱＶは、セッション鍵およびその他のセッション情報の部分漏洩が存在しても安全であり、換言すれば、ＨＭＱＶはいわゆる「既知の鍵（known key）」の攻撃に対する抵抗力がある。とりわけ、異なるセッション鍵は、互いに「計算上独立」するように保証される。

（５）このプロトコルは、「鍵漏洩詐称（ＫＣＩ：key-compromise impersonation）」攻撃に対する抵抗力として知られる追加レベルの保護を提供し、すなわち、これは、Ａに対して他の当事者を詐称できるように当事者Ａの秘密鍵を学習する攻撃者を阻止する。

（６）鍵確認を有する３メッセージＨＭＱＶプロトコルは、立証可能な完全転送秘密（ＰＦＳ）を提供し、すなわち、２当事者の長期秘密鍵が最終的に開示された場合でも、漏洩前にこれらの当事者によって作成されたセッション鍵は引き続き安全である。

（７）鍵確認を有する３メッセージ・プロトコルは、いわゆる「汎用構成可能」鍵交換プロトコルの追加のセキュリティ上の利点を享受し、すなわち、他のプロトコルによって安全に構成することができる。

（８）ＨＭＱＶのセキュリティは、静的公開鍵の形式および構造に関する特別なテストに依存せず、対応する秘密鍵のいわゆる「所有証明（proof of possession）」を必要としない。ＭＱＶを含む、同様のプロトコルを上回るＨＭＱＶのこのような利点により、認証局（ＣＡ：certificationauthority）は、登録公開鍵についてこのような特別なチェックを実行する負担から解放され、その結果、より現実的で実用的なセキュリティの保証が得られるが、とりわけ、多くのローカルＣＡがこのようなチェックを実行できないかまたは実行するように構成されていないためである。その上、ＣＡによるこのようなテスト（たとえば、所有証明）の正当な実行により、追加のセキュリティ上の脆弱性に対してプロトコルを開放することは、留意する価値がある。

（９）２メッセージおよび３メッセージＨＭＱＶプロトコルは、一時公開鍵（すなわち、値ＸおよびＹ）の次数のテストを必要とせず、その結果、場合によっては高価なものになりうるテストを回避する。しかし、両当事者の一時秘密鍵を学習する可能性のある攻撃者に耐えることがプロトコルのセキュリティである場合、このようなテストは必要である。また、１パスＨＭＱＶプロトコルのセキュリティについても、このテストは必要である。ＭＱＶのように、これらのテストは、プロトコル内のσ値の「余因数べき乗」で置き換えることができる。基礎となる代数群に応じて、所定の群内の帰属関係など、群の元に関する追加のテストが必要になる場合もある。

【０１１３】

本発明のＨＭＱＶプロトコルの重要な利点の１つは、形式的に数学的に有効であること

を証明できる広範囲のセキュリティ上の特性が存在するときに、それがほぼ間違いなく最も効率的な認証Ｄｉｆｆｉｅ－Ｈｅｌｌｍａｎ鍵交換プロトコルであることである。実際に、この形式的な立証可能性は、ＨＭＱＶとその先行ＭＱＶとの間の主な相違点の１つである。

【０１１４】

ＭＱＶはセキュリティの証明を備えることができなかっただけでなく、上記の仮出願に初めて記載されたいくつかの弱点を含む、このプロトコルの明示的な弱点が時間の経過につれて明らかになっている（たとえば、Ｋａｌｉｓｋｉによる研究およびＲｏｇａｗａｙ他による報告）。このような弱点または攻撃は、その発明者によって行われたＭＱＶに関するセキュリティ上の主張のいくつかを無効にしており、とりわけ、ＭＱＶが安全なものであることを証明できないことが示されている。

【０１１５】

ＸＣＲ署名とＭＱＶの「暗黙署名（Implicit Signature）」との比較

比較のやり方として、特許および学術論文に記載されているＭＱＶはプロトコルの設計および説明でも署名の概念を使用することは、留意する価値がある。これは、ＭＱＶに関連して「暗黙署名」と呼ばれ、秘密署名鍵の所有者のみが署名値を生成できるデジタル署名のより伝統的な概念に従うものである（具体的には、ＭＱＶは、秘密署名鍵と、一時秘密鍵および公開鍵との１次結合によって形成されるＥｌＧａｍａｌのような署名を指す）。しかし、プロトコルは、これらの署名の特性を完全に使用するまでには至らない。とりわけ、ＭＱＶプロトコルは、そのプロトコルの当事者のＩＤを明示的に認証する方法として署名を使用せず、これにより、Ｋａｌｉｓｋｉによって発見された有名な「未知の鍵の共有（ＵＫＳ：unknown key share）」などの重大な認証障害が発生する。

【０１１６】

対照的に、ＨＭＱＶは、２つの重要な要素をその設計に採り入れている。１つは、ＸＣＲの使用であり、これはＥｌＧａｍａｌ署名の指数バージョンである。より具体的には、これはＳｃｈｎｏｒｒの署名の指数バージョンであり、次にこれはＥｌＧａｍａｌ署名の特定のインスタンス化である。もう１つは、ピアのＩＤの明示的な署名であり、これは、セッションのピアに対するセッション鍵の安全な結合を保証し、とりわけ、ＵＫＳなどの認証障害を防止する。

【０１１７】

ＸＣＲ署名の重要な新規性は、署名者と検証者（またはチャレンジャ）の両方が同じ署名を計算できるという特性である。この特性は、通常、共有鍵暗号方式に基づく認証メカニズムに見られる（すなわち、署名者と検証者の両方が事前（a-priori）共有鍵を有する場合）が、公開鍵ベースの署名では新しいものである。ＸＣＲ署名は、ＨＭＱＶのように、共有鍵の導出に完全に適しているだけでなく、認証ツールとして様々な利点を提示し、そのうちのいくつかについては上述した通りである。

【０１１８】

本発明が様々な実施形態を包含することは当業者にとって明白であるはずである。

【０１１９】

したがって、模範的な一実施形態では、検証者Ｖと署名者Ｓという２当事者が存在する。署名者Ｓは秘密鍵ｂと公開鍵Ｂとを有し、検証者ＶはＳの真正公開鍵Ｂを所有するかまたは（たとえば、Ｓから送信されたデジタル証明書を介して）入手するものと想定される。所与のメッセージｍに関する認証プロトコルは以下のものを含む。

（１）Ｖは、秘密の値ｘを選択し、値$X = F_1(x)$を計算し、ここでF_1は所与の関数であり、次にＸをＳに送信する。

（２）Ｓは、秘密の値ｙを選択し、値$Y = F_2(y)$を計算し、ここでF_2は所与の関数であり、次にＹをＶに送信する。

（３）Ｓは、値$s = F_3(y, b, X, m)$を計算し、ここでF_3は所与の関数であり、次にｓをＶに送信する。

（４）Ｖは、値$s' = F_4(x, Y, B, m)$を計算し、値ｓ′と受信した値ｓに対する

その関連とを基礎として、ｍの確実性を決定する。
【０１２０】
この実施形態のいくつかの模範的な変種は以下のものを含む。
（ａ）F_1、F_2は一方向関数である。ＸＣＲでは、これらの一方向関数は$X = g^x$および$Y = g^y$である。
（ｂ）ＸＣＲ署名では、この関数は
【数２７】

$$s = F_3(y,b,X,m) = X^{(y+\bar{H}(Y,m)b)}$$

および
【数２８】

$$s' = F_4(x,Y,B,m) = (YB^{(\bar{H}(Y,m))})^x$$

である。
（ｃ）ｓ′＝ｓである場合のみ、ｍを認証として受け入れる。この最後の変種は、それにより、チャレンジＸの背後にある秘密を把握することによって検証者が署名を再計算できる、典型的なＸＣＲ署名の特性を利用する。
（ｄ）
【数２９】

$$s = F_3(y,b,X,m) = X^{(y+\bar{H}(Y,m)b)}$$

を計算し、Ｈ（ｓ′）＝ｓなどをテストする。
【０１２１】
ＨＭＱＶに対するＸＣＲの適用例の少なくとも１つの実施形態では、ステップ（３）でＳによって計算された値ｓはけっしてＶに送信されない。その代わりに、Ｖは、（Ｓが詐称者（impostor）である場合を除き）ｓと同一になるはずの値ｓ′を計算し、ｓ（これはＨＭＱＶではσである）を使用してそこからセッション鍵を導出する。とりわけ、Ｖは明示的検証をけっして実行しない。この実施形態では、メッセージｍの確実性を検証するための方法ではなく、それにより両当事者が共通の「認証値（authenticatedvalue）」（すなわち、両当事者のみが計算できる値）を計算し、この値がそれぞれのＩＤに一意に結合される（二重ＸＣＲ署名を介して両当事者のＩＤを署名することによりＨＭＱＶで達成される典型的な鍵交換プロトコルにおける本質的な条件である）方法が存在することになるであろう。
【０１２２】
追加の変形例については上記の説明および特許請求の範囲に記載されている。
【０１２３】
模範的なハードウェア実現例
図１０は、本発明による情報処理／コンピュータ・システムの典型的なハードウェア構成を例示しており、このシステムは好ましくは少なくとも１つのプロセッサまたは中央演算処理装置（ＣＰＵ：central processing unit）１０１１を有する。
【０１２４】
ＣＰＵ１０１１は、システム・バス１０１２を介して、ランダム・アクセス・メモリ（ＲＡＭ：random access memory）１０１４、読み取り専用メモリ（ＲＯＭ：read-only memory）１０１６、入出力（Ｉ／Ｏ）アダプタ１０１８（ディスク装置１０２１およびテープ・ドライブ１０４０などの周辺装置をバス１０１２に接続するため）、ユーザ・インターフェース・アダプタ１０２２（キーボード１０２４、マウス１０２６、スピーカ１０２８、マイクロホン１０３２、またはその他のユーザ・インターフェース・デバイス、あるいはこれらの組み合わせをバス１０１２に接続するため）、情報処理システムをデータ処理ネットワーク、インターネット、イントラネット、パーソナル・エリア・ネットワーク（ＰＡＮ：personalarea network）などに接続するための通信アダプタ１０３４、および

バス１０１２をディスプレイ装置１０３８またはプリンタ１０３９（たとえば、デジタル・プリンタなど）あるいはその両方に接続するためのディスプレイ・アダプタ１０３６に相互接続される。

【０１２５】

上述のハードウェア／ソフトウェアの実施形態に加えて、本発明の異なる一態様は、上記の方法を実行するためのコンピュータで実行される方法を含む。一例として、この方法は、上記で論じた特定の実施形態で実現することができる。

【０１２６】

このような方法は、たとえば、一連の機械可読命令を実行するように、デジタル・データ処理装置によって実施されるコンピュータを操作することによって実現することができる。これらの命令は、様々なタイプの信号伝送媒体に常駐することができる。

【０１２７】

したがって、本発明のこの態様は、本発明の方法を実行するために、ＣＰＵ１０１１および上記のハードウェアを組み込むデジタル・データ・プロセッサによって実行可能な複数の機械可読命令からなるプログラムを具体的に実施する信号伝送媒体を含むプログラム式製品を対象とする。

【０１２８】

この信号伝送媒体としては、たとえば、高速アクセス記憶装置によって表される、たとえば、ＣＰＵ１０１１内に収容されたＲＡＭを含むことができる。代わって、命令は、ＣＰＵ１０１１によって直接または間接的にアクセス可能な磁気データ記憶ディスケット１１００（図１１）などの他の信号伝送媒体に収容することもできる。

【０１２９】

ディスケット１１００に収容されているか、コンピュータ／ＣＰＵ１０１１に収容されているか、またはその他の場所に収容されているかにかかわらず、命令は、ＤＡＳＤ記憶装置（たとえば、従来の「ハード・ディスク」またはＲＡＩＤアレイ）、磁気テープ、電子読み取り専用メモリ（たとえば、ＲＯＭ、ＥＰＲＯＭ、またはＥＥＰＲＯＭ）、光学記憶装置（たとえば、ＣＤ－ＲＯＭ、ＷＯＲＭ、ＤＶＤ、デジタル光テープなど）、紙の「パンチ」カード、または、デジタルおよびアナログの通信リンクおよび無線などの伝送媒体を含むその他の適切な信号伝送媒体などの様々な機械可読データ記憶媒体に保管することができる。本発明の例示的な一実施形態では、機械可読命令は、ソフトウェア・オブジェクト・コードを含むことができる。

【図面の簡単な説明】

【０１３０】

【図１】基本（非認証）Ｄｉｆｆｉｅ－Ｈｅｌｌｍａｎプロトコル１００を示す図である。

【図２】デジタル署名を使用することによって認証された２メッセージＤｉｆｆｉｅ－Ｈｅｌｌｍａｎプロトコル２００を示す図である。

【図３】本発明のＨＭＱＶプロトコルのセッション鍵の計算に対する従来のＭＱＶプロトコルのセッション鍵Ｋの計算の比較３００を示し、ＭＱＶで使用されるハッシュへの追加である模範的な一実施形態のハッシュをＨＭＱＶがどのように使用するかを実証する図である。

【図４】図３に示されているＨＭＱＶプロトコルの異なるグラフィック表現４００である。

【図５】ＸＣＲの計算５００を例示的に示す図である。

【図６】非対話式ＸＣＲ署名の計算６００の一例を示す図である。

【図７】２当事者による二重ＸＣＲ署名の計算７００を示す図である。

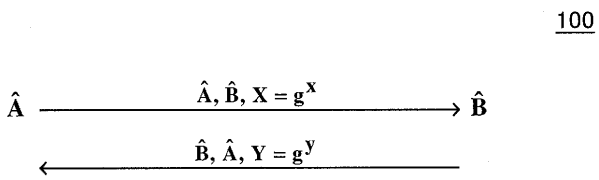
【図８】３メッセージ鍵確認（ＨＭＱＶ－Ｃ）プロトコル８００で例示的に実施されたＨＭＱＶを示す図である。

【図９】１パス鍵交換９００で例示的に実施されたＨＭＱＶを示す図である。

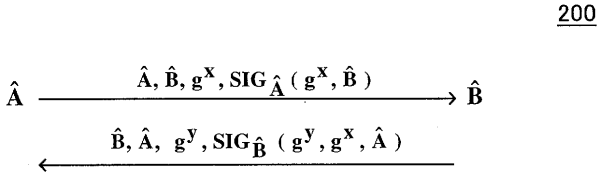
【図１０】そこに本発明を組み込むための模範的なハードウェア／情報処理システム１０

００を例示する図である。
【図１１】本発明による方法のプログラムの諸ステップを保管するための信号伝送媒体１１００（たとえば、記憶媒体）を例示する図である。

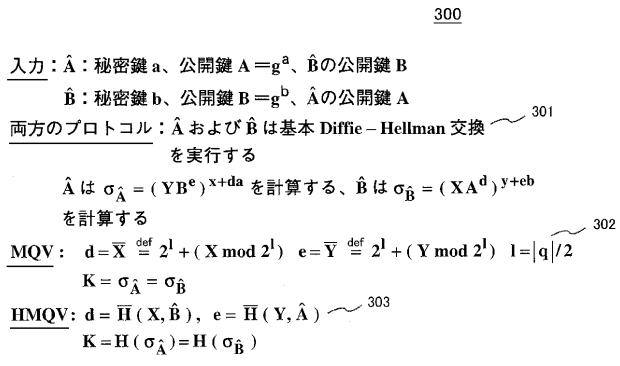
【図１】



【図２】



【図３】



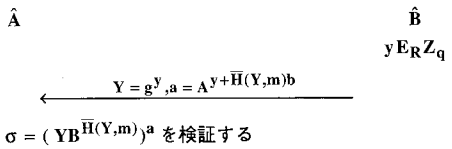
【図４】

【図５】

【図６】

600

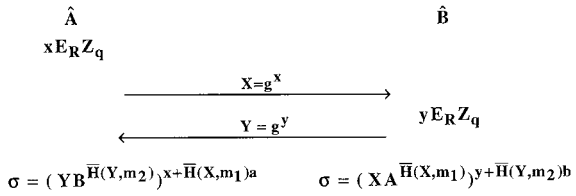
入力：署名者$\hat{B}$：秘密鍵b、公開鍵$B=g^b$、$\hat{A}$の公開鍵A、メッセージ m
検証者$\hat{A}$：秘密鍵a、公開鍵$A=g^a$、$\hat{B}$の公開鍵B、メッセージ m
署名プロトコル：



【図７】

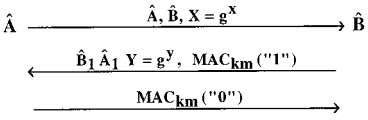
700

入力：$\hat{A}$ 秘密鍵a、公開鍵$A=g^a$、$\hat{B}$の公開鍵B、メッセージ m_1, m_2
$\hat{B}$ 秘密鍵b、公開鍵$B=g^b$、$\hat{A}$の公開鍵A、メッセージ m_1, m_2
署名プロトコル：



【図８】

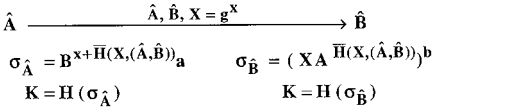
800



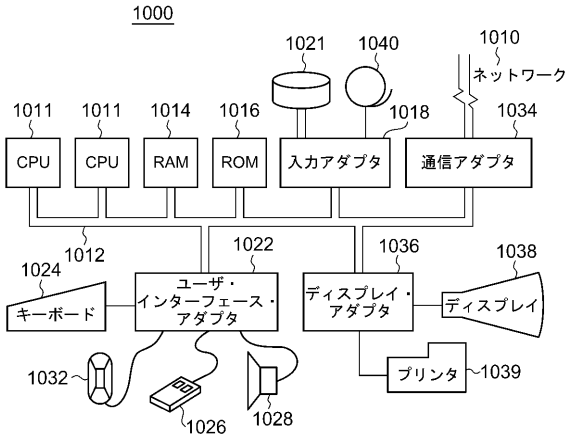
鍵計算（$\hat{A}$および$\hat{B}$による）：
HMQVのようにσを計算する；$K_m = H(\sigma, 0)$および
$K = H(\sigma, 1)$を計算する

【図９】

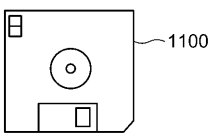
900



【図１０】



【図１１】



【手続補正書】
【提出日】平成20年12月17日(2008.12.17)
【手続補正１】
【補正対象書類名】特許請求の範囲
【補正対象項目名】全文
【補正方法】変更
【補正の内容】
【特許請求の範囲】
【請求項１】
装置またはネットワークによって相互接続された２当事者間の交換の方法において、
受信側当事者（検証者）が値Ｘ＝Ｆ１（ｘ）を計算するために秘密の値ｘを選択し、ここでＦ１は少なくとも１つの引数を有する第１の所定の関数を含み、前記値ｘはＦ１の前記少なくとも１つの引数のうちの１つであり、
署名側当事者（署名者）が値Ｙ＝Ｆ２（ｙ）を計算するために秘密の値ｙを選択し、ここでＦ２は少なくとも１つの引数を有する第２の所定の関数を含み、前記値ｙはＦ２の前記少なくとも１つの引数のうちの１つであり、
前記署名者が前記値Ｘを入手し、前記署名者が秘密鍵ｂと公開鍵Ｂとを有し、
前記署名者が値ｓ＝Ｆ３（ｙ，ｂ，Ｘ）を計算し、ここでＦ３は少なくとも３つの引数を有する第３の所定の関数を含み、前記値ｙ、前記秘密鍵ｂ、および前記値ＸはＦ３の前記少なくとも３つの引数のうちの３つの引数であり、
値ｓ′を計算するために第４の所定の関数Ｆ４（ｘ，Ｙ，Ｂ）が存在し、Ｆ４は少なくとも３つの引数を有し、前記値ｘ、前記値Ｙ、および前記公開鍵ＢはＦ４の前記少なくとも３つの引数のうちの３つの引数であるが、値ｓはＦ４の引数ではなく、
前記検証者と前記署名者との間で共有され、前記Ｆ１、Ｆ２、Ｆ３、およびＦ４のいずれかにおいて任意の引数の基礎として働くような秘密が存在せず、
前記値ｓ′が所定の方法で前記値ｓに関連するものと判断された場合に前記検証者が前記値ｓおよびｓ′を有効な認証子と見なすことができる、方法。
【請求項２】
Ｆ１およびＦ２のうちの少なくとも１つが一方向関数を含む、請求項１に記載の方法。
【請求項３】
前記値ｓおよびｓ′が、ｓ＝ｓ′である場合に有効な認証子であると判断される、請求項１に記載の方法。
【請求項４】
ｓ′の計算ならびに前記値ｓおよびｓ′が関連するものであると判断されるかどうかの判断のうちの少なくとも一方が、前記検証者および前記署名者以外の当事者によって実行される、請求項１に記載の方法。
【請求項５】
２当事者間で共有される秘密を導出するために前記値ｓおよび前記値ｓ′が使用される、請求項１に記載の方法。
【請求項６】
前記検証者が前記値Ｙを入手し、ｓおよびｓ′が前記所定の方法で関連するかどうかを判断するために前記値ｓ′を計算するためにこれを使用すること
をさらに含む、請求項１に記載の方法。
【請求項７】
メッセージｍが、認証対象であり、Ｆ３の引数およびＦ４の引数を含み、それにより、前記値ｓおよび前記値ｓ′が前記メッセージｍ内の情報を含むことができ、
前記値ｓおよびｓ′が前記所定の方法で関連するものであると判断された場合に前記メッセージが認証される、請求項１に記載の方法。
【請求項８】
２当事者間で共有される秘密を導出するために前記値ｓおよび前記値ｓ′が使用される

、請求項７に記載の方法。
【請求項９】
前記メッセージｍが、少なくとも前記交換の前記当事者の一方のＩＤを含む、請求項８に記載の方法。
【請求項１０】
前記署名者が前記値ｓを前記検証者に送信すること
をさらに含む、請求項７に記載の方法。
【請求項１１】
前記ｓ＝ｓ′である場合に前記メッセージが認証される、請求項７に記載の方法。
【請求項１２】
前記公開鍵$B=g^{b}$であり、ｇが次数ｑの有限群の生成元であり、前記秘密鍵ｂが$0\leq b\leq q-1$になるような整数であり、
前記値$X=g^{x}$であり、ｘが$0\leq x\leq q-1$になるような整数であり、前記値$Y=g^{y}$であり、ｙが$0\leq y\leq q-1$になるような整数であり、
前記署名者が前記値$s=f_1(X)^{f2(m,Y,y,b)}$を計算し、f_1が第１の数学関数を含み、f_2が第２の数学関数を含み、引数ｍがメッセージを含む、請求項１に記載の方法。
【請求項１３】
ｑが素数である、請求項１２に記載の方法。
【請求項１４】
前記値ｓが所定の方法で前記値ｓ′に関連するものと判断された場合に前記メッセージｍが認証済みと見なされる、請求項１２に記載の方法。
【請求項１５】
前記値ｓが前記値ｓ′に等しいと判断された場合に前記メッセージｍが認証済みと見なされる、請求項１４に記載の方法。
【請求項１６】
f_1が恒等関数から構成される、請求項１２に記載の方法。
【請求項１７】
f_2が、f_2の前記引数の少なくとも１つがハッシュされるようなハッシュ関数を含む、請求項１２に記載の方法。
【請求項１８】
ハッシュされた前記引数の１つが非ヌル・メッセージｍである、請求項１７に記載の方法。
【請求項１９】
前記メッセージｍが、コンピュータまたはシステムあるいはネットワーク内の当事者のＩＤを含む、請求項１２に記載の方法。
【請求項２０】
$f_2(m, Y, y, b)=y+H(Y, m)b \mod q$であり、ここでＨは一方向関数、暗号化関数、および暗号ハッシュ関数のうちの１つである暗号関数を含む、請求項１７に記載の方法。
【請求項２１】
前記値$s'=(YB^{\{H(Y,m)\}})^{f3(x)}$であり、ここで$f_3(x)$は少なくとも１つの引数を有する数学関数を含み、前記値ｘは$f_3(x)$の前記少なくとも１つの引数のうちの１つの引数である、請求項２０に記載の方法。
【請求項２２】
$f_3(x)=x$である、請求項２１に記載の方法。
【請求項２３】
ｓ＝ｓ′である場合のみ、前記メッセージｍを認証すること
をさらに含む、請求項２１に記載の方法。
【請求項２４】
前記検証者が、秘密鍵ａ、公開鍵$A=g^{a}$、およびメッセージｍ′を有し、前記値ｓ′

がｍ上の前記署名者の署名を含むと同時に、前記値ｓがｍ′上の前記検証者の署名を含む、請求項２１に記載の方法。

【請求項２５】

前記関数ｆ３（ｘ）＝ｘ＋Ｈ（Ｘ，ｍ′）ａ　ｍｏｄ　ｑである、請求項２４に記載の方法。

【請求項２６】

ｘが前記検証者によってランダムに選択され、ｙが前記署名者によってランダムに選択される、請求項１に記載の方法。

【請求項２７】

前記第１の値$X = g^x$が、前記証明者により検索可能になるように前記検証者によって公開された値を含み、それにより、前記認証の非対話式バージョンを可能にする、請求項１に記載の方法。

【請求項２８】

前記値ｓおよびｓ′がさらにハッシュされる、請求項２１に記載の方法。

【請求項２９】

装置またはネットワークによって相互接続された２当事者間で認証鍵を確立するための方法において、

第１の当事者が秘密鍵ａと公開鍵Ａとを有する場合に、前記秘密鍵ａが$0 \leq a \leq q-1$になるような整数であり、ｑが正整数であり、ｇが次数ｑの有限群の生成元であり、Ａが前記値ｇによって生成され、$A = g^a$として計算された前記群内の元であり、

第２の当事者が秘密鍵ｂと公開鍵$B = g^b$とを有し、前記秘密鍵ｂが$0 \leq b \leq q-1$になるような整数であり、

前記第１の当事者が値$X = g^x$を計算するために秘密の値ｘを選択し、ｘが$0 \leq x \leq q-1$になるような整数であり、前記値Ｘが前記第２の当事者に伝達され、

前記第２の当事者が値$Y = g^y$を計算するために秘密の値ｙを選択し、ｙが$0 \leq y \leq q-1$になるような整数であり、前記値Ｙが前記第１の当事者に伝達され、

前記第１の当事者が値$s = f_1(Y, B, m)^{\{f2(x,a,m')\}}$を計算し、ここでｍ、ｍ′は前記当事者間で既知であるかまたは交換されたメッセージを含み、前記第２の当事者が値$s' = f_3(X, A, m')^{\{f4(y,b,m)\}}$を計算し、

前記関数f_2およびf_4のうちの少なくとも１つが少なくとも１つの引数を有する関数Ｈを含み、このような１つの引数が前記メッセージｍおよびｍ′のうちの少なくとも１つであり、ここでＨは一方向関数、暗号化関数、および暗号ハッシュ関数のうちの１つである暗号関数を含み、

前記第１および第２の当事者がそれぞれ前記値ｓおよびｓ′から共有鍵を導出する、方法。

【請求項３０】

（ｉ）前記値ｘおよびＸの計算が、前記第１の当事者の前記秘密鍵と、前記当事者のうちの一方または複数の前記公開鍵とを含むことと、

（ｉｉ）前記値ｙおよびＹの計算が、前記第２の当事者の前記秘密鍵と、前記当事者のうちの一方または複数の前記公開鍵とを含むこと

のうちの少なくとも一方が該当する、請求項２９に記載の方法。

【請求項３１】

ｓおよびｓ′からの共有鍵の前記導出が、一方向関数、暗号化関数、および暗号ハッシュ関数のうちの１つである暗号関数を含む、請求項２９に記載の方法。

【請求項３２】

前記メッセージｍおよびｍ′のうちの少なくとも１つが前記第１および第２の当事者のうちの一方のＩＤを含む、請求項２９に記載の方法。

【請求項３３】

$f_1(Y, B, m) = Y B^{H(Y,m)}$であり、

$f_2(x, a, m') = (x + H(X, m')a)$　ｍｏｄ　ｑであり、

f_3（Ｘ，Ａ，ｍ′）＝$XA^{H(X,m')}$であり、
f_4（ｙ，ｂ，ｍ）＝（ｙ＋Ｈ（Ｙ，ｍ）ｂ）　ｍｏｄ　ｑであり、
Ｈが一方向関数、暗号化関数、および暗号ハッシュ関数のうちの１つである暗号関数を含む、少なくとも２つの引数からなる関数である、請求項２９に記載の方法。
【請求項３４】
前記メッセージｍおよびｍ′のうちの少なくとも１つが前記第１および第２の当事者のうちの少なくとも一方のＩＤを含む、請求項３３に記載の方法。
【請求項３５】
（ｉ）前記値ｘおよびＸの計算が、前記第１の当事者の前記秘密鍵と、前記当事者のうちの一方または複数の前記公開鍵とを含むことと、
（ｉｉ）前記値ｙおよびＹの計算が、前記第２の当事者の前記秘密鍵と、前記当事者のうちの一方または複数の前記公開鍵とを含むこと
のうちの少なくとも一方が該当する、請求項３４に記載の方法。
【請求項３６】
ｓおよびｓ′からの共有鍵の前記導出が、一方向関数、暗号化関数、および暗号ハッシュ関数のうちの１つである暗号関数を含む、請求項３４に記載の方法。
【請求項３７】
請求項１～３６のいずれか１項に記載の方法の各ステップをコンピュータに実行させるための方法。

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2006/050841

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L9/08

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

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 practical, search terms used)
EPO-Internal, PAJ, WPI Data, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
P,X	KRAWCZYK H: "HMQV: a high-performance secure Diffie-Hellman protocol (extended abstract)" ADVANCES IN CRYPTOLOGY CRYPTO 2005. 25TH ANNUAL INTERNATIONAL CRYPTOLOGY CONFERENCE. PROCEEDINGS. LECTURE NOTES IN COMPUTER SCIENCE, SPRINGER-VERLAG, vol. 3621, 18 August 2005 (2005-08-18), pages 546-566, XP002380812 Santa Barbara, CA, USA ISBN: 3-540-28114-2 the whole document -/--	1-38

[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 document 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
16 May 2006	26/05/2006

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, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Carnerero Álvaro, F

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

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2006/050841

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	BLAKE-WILSON S; MENEZES A: "AUTHENTICATED DIFFIE-HELLMAN KEY AGREEMENT PROTOCOLS" SELECTED AREAS IN CRYPTOGRAPHY. 5TH ANNUAL INTERNATIONAL WORKSHOP, SAC'98. PROCEEDINGS. SPRINGER-VERLAG, 18 August 1998 (1998-08-18), pages 339-361, XP002380813 Kingston, Ont., Canada ISBN: 3-540-65894-7 page 346 - page 351 page 354 - page 359	29
A	-----	1,30,31

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,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,RU,SC,SD,SE,SG,SK,SL,SM,SY,TJ,TM,TN,TR,TT,TZ,UA,UG,US,UZ,VC,VN,YU,ZA,ZM,ZW

(74)代理人 100086243
弁理士 坂口 博
(72)発明者 クラフチック、ヒューゴ
アメリカ合衆国１０５９１ ニューヨーク州タリータウン ユーニス・コート２５

Ｆターム(参考) 5J104 AA08 AA09 JA21 LA03 LA06 NA02 NA27 NA37 NA38

(54)【発明の名称】装置またはネットワークによって相互接続された２当事者間の交換の方法、信号伝送媒体、および装置（チャレンジ・レスポンス署名および高性能で安全なＤｉｆｆｉｅ－Ｈｅｌｌｍａｎプロトコルに関する方法および構造）