

(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7617008号
(P7617008)

(45)発行日 令和7年1月17日(2025.1.17)

(24)登録日 令和7年1月8日(2025.1.8)

(51)国際特許分類	F I
H 0 4 L 9/32 (2006.01)	H 0 4 L 9/32 2 0 0 A
G 0 6 F 21/64 (2013.01)	H 0 4 L 9/32 2 0 0 E
	G 0 6 F 21/64

請求項の数 15 (全26頁)

(21)出願番号	特願2021-549168(P2021-549168)	(73)特許権者	521365820 ブリュノ・シングル・フェリエール フランス・7 5 0 1 6・パリ・ブルヴァ ール・ポーセジュール・4 7
(86)(22)出願日	令和2年2月17日(2020.2.17)	(74)代理人	100108453 弁理士 村山 靖彦
(65)公表番号	特表2022-521525(P2022-521525 A)	(74)代理人	100110364 弁理士 実広 信哉
(43)公表日	令和4年4月8日(2022.4.8)	(74)代理人	100133400 弁理士 阿部 達彦
(86)国際出願番号	PCT/EP2020/054126	(72)発明者	ブリュノ・シングル・フェリエール フランス・7 5 0 1 6・パリ・ブルヴァ ール・ポーセジュール・4 7
(87)国際公開番号	WO2020/169542	審査官	行田 悦資
(87)国際公開日	令和2年8月27日(2020.8.27)		
審査請求日	令和5年1月11日(2023.1.11)		
(31)優先権主張番号	1901648		
(32)優先日	平成31年2月19日(2019.2.19)		
(33)優先権主張国・地域又は機関	フランス(FR)		

最終頁に続く

(54)【発明の名称】 データを検証するための暗号方法

(57)【特許請求の範囲】

【請求項1】

送信者(A)から発信されるメッセージ(101)の整合性を装置(B)を用いて検証するための方法であって、

- i. 前記装置(B)が前記メッセージ(101)および前記メッセージの識別子を受信するステップであって、前記メッセージが第1のデータセットを形成する、ステップと、
- ii. ミキサ数と称される数を生成するステップであって、前記ミキサ数がランダムに生成される、ステップと、
- iii. 混合されたデータを取得するために、混合関数(105)を使用して、前記ミキサ数を前記第1のデータセットと混合するステップと、
- iv. ハッシュ関数(106)を使用して、前記混合されたデータをハッシュ化して、ハッシュを取得するステップと、
- v. 前記装置(B)が前記メッセージの前記識別子および前記ミキサ数を前記メッセージの前記送信者(A)に送信するステップと、
- vi. 前記装置(B)が前記送信者(A)から発信される暗号化された第2のデータセットを受信するステップと、
- vii. 前記第2のデータセットを復号するステップと、
- viii. ステップivにおいて取得された前記ハッシュを、同じ混合関数(105)を使用して、ステップiiiにおいて使用されたものと同じミキサ数と混合された前記メッセージのハッシュであると見なされる、ステップviiにおいて復号された前記第2のデータセットと比較す

るステップであって、ステップviiにおいて復号された前記第2のデータセットとステップivにおいて取得された前記ハッシュとが同一である場合、前記メッセージの前記整合性が保証される、ステップと

を含む方法。

【請求項2】

ステップvとステップviとの間に、

- 前記送信者(A)が前記メッセージの前記識別子および前記ミキサ数を受信するステップと、
 - 前記メッセージの前記識別子を使用して、前記装置(B)に送信された前記メッセージ(101)を識別するステップと、
 - 前記混合関数(105)を使用して、前記メッセージを前記ミキサ数と混合するステップと、
 - 前記ハッシュ関数(106)を使用して、先行するステップから生じるデータをハッシュ化して、ハッシュを取得するステップと、
 - 先行するステップから生じる前記ハッシュを暗号化するステップと、
 - 前記暗号化されたハッシュを前記装置(B)に送信するステップと
- を含む、請求項1に記載の方法。

【請求項3】

ステップivとステップvとの間に、前記ミキサ数を暗号化するステップを含み、
ステップvとステップviとの間に、前記ミキサ数を復号するステップを含む、請求項2に記載の方法。

【請求項4】

前記ミキサ数の前記暗号化が使い捨て鍵を使用して行われる場合、ステップviiにおける前記第2のデータセットの前記復号が対称鍵を使用して行われる、請求項3に記載の方法。

【請求項5】

前記ミキサ数の前記暗号化が対称鍵を使用して行われる場合、ステップviiにおける前記第2のデータセットの前記復号が使い捨て鍵を使用して行われる、請求項3に記載の方法。

【請求項6】

装置(A; B)内に存在するデータセットが2つの時間d1とd2との間で変更されていないことを検証するための方法であって、前記データセットが、前記時間d1において第1のデータセットを形成し、前記時間d2において第2のデータセットを形成し、前記方法が、

- i. 混合されたデータを取得するために、混合関数(105)を使用して、ミキサ数と称される数を前記第1のデータセットと混合するステップであって、前記ミキサ数がランダムに生成される、ステップと、
 - ii. ハッシュ関数(106)を使用して、前記混合されたデータをハッシュ化して、ハッシュを取得するステップと、
 - iii. 前記装置(A; B)が前記ミキサ数およびステップiiにおいて取得された前記ハッシュをセキュアに保存するステップと、
 - iv. 前記ミキサ数および前記混合関数を使用して、前記第2のデータセットの変更されたコピーを作成するステップと、
 - v. 前記ハッシュ関数を使用して、前記変更されたコピーをハッシュ化して、ハッシュを取得するステップと、
 - vi. ステップiiにおいて取得された前記ハッシュをステップvにおいて取得された前記ハッシュと比較するステップであって、前記2つのハッシュが同一である場合、前記データセットが前記2つの時間d1とd2との間で変更されていない、ステップと
- を含む方法。

【請求項7】

送信者(A)から発信される第1のデータセットを形成するメッセージ(101)の整合性を装置(B)を用いて検証するための方法であって、

- i. 前記装置(B)が前記メッセージ(101)、暗号化された第2のデータセット、およびミキ

サ数と称される暗号化された数を受信するステップであって、前記ミキサ数がランダムに生成される、ステップと、

ii. 前記ミキサ数および前記第2のデータセットを復号するステップと、

iii. 混合されたデータを取得するために、混合関数(105)を使用して、前記メッセージ(101)を前記ミキサ数と混合するステップと、

iv. ハッシュ関数(106)を使用して、前記混合されたデータをハッシュ化して、ハッシュを取得するステップと、

v. ステップivにおいて取得された前記ハッシュを、同じ混合関数(105)を使用して、ステップiiiにおいて使用されたものと同じミキサ数と混合された前記第1のデータセットのハッシュであると見なされる、ステップiiにおいて復号された前記第2のデータセットと比較するステップであって、ステップivにおいて取得された前記ハッシュとステップiiにおいて復号された前記第2のデータセットとが同一である場合、前記メッセージの前記整合性が保証される、ステップと

10

を含む方法。

【請求項 8】

ステップiの前に、

- 前記送信者(A)が前記ミキサ数を生成するステップと、

- 前記混合関数(105)を使用して、前記ミキサ数を前記メッセージ(101)と混合するステップと、

- 前記ハッシュ関数(106)を使用して、先行するステップから生じるデータをハッシュ化して、ハッシュを取得するステップと、

20

- 先行するステップから生じる前記ハッシュを暗号化し、前記第2のデータセットを形成するステップと、

- 前記ミキサ数を暗号化するステップと、

- 前記メッセージ(101)、前記暗号化された第2のデータセット、および前記暗号化されたミキサ数を前記装置(B)に送信するステップと

を含む、請求項7に記載の方法。

【請求項 9】

第1の装置(A)および第2の装置(B)によって実施される、前記第1の装置(A)内に存在する第1のデータセット(401A)と前記第2の装置(B)内に存在する第2のデータセット(401B)とを比較するための、具体的には、前記2つのデータセットが同一であるかどうかを判定することを目的とする、方法であって、

30

i. 前記第1の装置(A)が、混合されたデータを取得するために、混合関数(405)を使用して、ミキサ数と称される数を前記第1のデータセット(401A)と混合するステップであって、前記ミキサ数がランダムに生成される、ステップと、

ii. 前記第1の装置(A)が、ハッシュ関数(406)を使用して、前記混合されたデータをハッシュ化して、ハッシュを取得するステップと、

iii. 前記第1の装置(A)が前記ミキサ数を暗号化するステップと、

iv. 前記第1の装置(A)が前記暗号化されたミキサ数を前記第2の装置(B)に送信するステップと、

40

v. 前記第1の装置(A)が前記第2のデータセット(401B)の暗号化されたハッシュを受信するステップと、

vi. 前記暗号化されたハッシュを復号するステップと、

vii. ステップiiにおいて取得された前記ハッシュをステップviにおいて復号された前記ハッシュと比較するステップと

を含む方法。

【請求項 10】

ステップivとステップvとの間に、

- 前記第2の装置(B)が前記暗号化されたミキサ数を受信するステップと、

- 前記ミキサ数を復号するステップと、

50

- 前記ミキサ数および前記混合関数(405)を使用して、前記第2のデータセット(401B)の変更されたコピーを作成するステップと、
 - 前記ハッシュ関数(406)を使用して、前記第2のデータセット(401B)の前記変更されたコピーをハッシュ化して、ハッシュを取得するステップと、
 - 先行するステップから生じる前記ハッシュを暗号化するステップと、
 - 前記第2の装置(B)が前記第2のデータセット(401B)の前記暗号化されたハッシュを前記第1の装置(A)に送信するステップと
- を含む、請求項9に記載の方法。

【請求項 1 1】

前記混合関数(105; 405)がXOR論理関数である、請求項1から10のいずれか一項に記載の方法。

10

【請求項 1 2】

前記混合関数(105; 405)が、前記ミキサ数を前記第1のデータセットの末尾に追加することから成る、請求項1から10のいずれか一項に記載の方法。

【請求項 1 3】

前記混合関数(105; 405)が、前記第1のデータセットを暗号化するための暗号化鍵として前記ミキサ数を使用する暗号化関数である、請求項1から10のいずれか一項に記載の方法。

【請求項 1 4】

前記ハッシュ関数(106; 406)が、SHA1、SHA2、SHA256、MD5およびJenkins関数の中から選ばれる、請求項1から13のいずれか一項に記載の方法。

20

【請求項 1 5】

請求項1から14のいずれか一項に記載の方法を実施するための、装置のプロセッサによって読み取り可能な命令を含むコンピュータプログラム。

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、デジタル暗号、ならびに計算デバイスおよび電子デバイスのセキュリティに関し、具体的にはデジタル署名に関する。

【背景技術】

30

【0002】

コンピュータおよび電子装置は、物理的に、ワイヤレスに、RFIDによって、または任意の他のセキュアな手段もしくは非セキュアな手段によって、ネットワークに接続されることが多く、時として、これらのコンピュータおよび電子装置に特定のデータを送信した装置のアイデンティティを知る必要があるが、これは、たとえば、これらのデータが、これらのデータを傍受し、これらのデータを正規の受信者に送信する前にこれらのデータを変更した別の装置によって伝送されていないことを保証するため、または、簡単に言えば、たとえば、道路網上の自動車もしくはスポーツイベント中に競争者によって着用されたRFIDタグである、データの送信者のアイデンティティをなんの疑いもなく識別するため、または、データの送信者のアイデンティティが受信者にとって重要である何らかの他の理由からである。

40

【0003】

伝送されるデータは、送信者に起因する鍵を用いて完全に暗号化されて送信され得る。しかしながら、データのすべての暗号化により、使い捨て鍵(ワンタイムパッド)の使用が困難になる。具体的には、データのすべての暗号化は、鍵が暗号化するデータがある間だけのものである鍵を使用する方法であり、これらの鍵は使用後に更新されなければならない。

【0004】

したがって、たとえば、テキスト、識別子、数、コンピュータプログラム、画像、またはビデオもしくはオーディオコードの交換を介して通信に入るコンピュータまたは他の電

50

子デバイスが、送信されるデータの量よりも少ない量のデータの暗号化を使用して送信デバイスのアイデンティティを検証することが必要である。データのハッシュを暗号化することから成る電子署名が使用されるのは、この理由からである。「ハッシュ」という用語は、入力として与えられた初期データに基づいて、迅速ではあるが不完全に初期データを識別するように働くフィンガープリントを計算する、ハッシュ関数の結果を指すために使用される。データとともに、暗号化されたハッシュを送信することが一般的であり、暗号化されたハッシュは次いで、受信者によって復号され、次いで、受信されたデータのハッシュと比較される。MD5、SHA1およびSHA256は、そのようなハッシュ化動作に従来使用されているアルゴリズムである。しかしながら、データハッシュは一般に元のデータよりもサイズがはるかに小さく、元のデータのハッシュに等しいハッシュを有する、元のデータと類似しているがわずかに異なる他のデータを作成することが可能である場合がある。したがって、これらのデータは、ハッシュを検証するための手順によって拒否されることなしに、元のデータと置換される可能性がある。任意のタイプのデータが置換され得るが、データの複雑性が増加する(長いテキスト、オーディオファイル、写真またはビデオ)につれて、置換のユーザによる検出可能性は低下する。置換を行うためには、暗号化されたハッシュを復号することすら必要としない。単に元のデータのハッシュを計算すれば十分である。さらに、MD5およびSHA1などのハッシュ関数は、現時点では回避することが比較的容易であるハッシュ関数である。

10

【0005】

開発中である量子コンピュータは、事前設定されたハッシュを有するように開始ファイルを最適化することが可能であるので、ハッシュ関数によって提供されるセキュリティを回避することが間もなく可能になるはずである。

20

【0006】

ハッシュ化技法を使用してシステムのセキュリティを改善するための方法が従来技術において知られている。

【0007】

中国特許出願公開第101547184号は、サーバとユーザとの間で交換される複数の補助認証値を使用する。

【0008】

米国特許出願公開第2011/0246433号において提案される方法では、送信されるべきデータのハッシュが生成され、送信されるべきデータチャンクおよび乱数タグと連結される。

30

【0009】

欧州特許出願公開第1421548号は、情報を伝送するための方法について記載しており、この方法では、送信されるべきメッセージが後でハッシュ化される乱数と連結される。ハッシュ化の結果は暗号化されずに他方の当事者に送信される。メッセージは時として、そのようにまたは暗号化されて伝送される。乱数は、常に署名されて、任意選択で暗号化されて、他方の当事者に伝送される。メッセージ自体が暗号化されないときにハッシュを暗号化しないという事実により、暗号化されていないメッセージおよびハッシュの結果に適合する乱数を計算することができる非常に強力なコンピュータまたは量子コンピュータに対して伝送が弱くなる。さらに、メッセージ全体を暗号化することは、そのような暗号化がワンタイムパッドを使用する場合に欠点を有し、ワンタイムパッドは、2つの対応する当事者の両方がそのような共有鍵にアクセスできることを必要とするものであり、クラック不可能であることになっている。

40

【先行技術文献】

【特許文献】

【0010】

【文献】中国特許出願公開第101547184号

【文献】米国特許出願公開第2011/0246433号

【文献】欧州特許出願公開第1421548号

50

【発明の概要】

【発明が解決しようとする課題】

【0011】

ハッシュ化技法のセキュリティをさらに改善して、データの検証におけるエラーの確率を低下させ、適切な場合には、これらのデータの送信者のより信頼できる認証を可能にする必要がある。

【課題を解決するための手段】

【0012】

本発明は、具体的にはこのニーズを満たすことを目的とし、第1のデータセットと第2のデータセットとを比較するための、具体的には、これらの2つのデータセットが同一であるかどうかを判定することを目的とする、少なくとも1つの装置によって実装される方法によりこの目的を達成し、この方法は、以下のステップ、すなわち、

a) 混合されたデータを取得するために、混合関数を使用して、ミキサ数と称される数を第1のデータセットと混合するステップと、

b) ハッシュ関数を使用して、混合されたデータをハッシュ化するステップと、

c) ステップb)においてこのようにして取得されたハッシュを、同じ混合関数を使用して、ステップa)において使用されたものと同じミキサ数と混合された第2のデータセットのハッシュであると見なされる第3のデータセットと比較するステップとを含む。

【0013】

本発明により、具体的にはハッシュ化の前の第1のデータセットとミキサ数との混合により、同じミキサ数と混合された後で、混合された第1のデータセットと同じハッシュを有する、この第1のデータセットに類似したデータを作成することができる可能性が非常に低くなる。

【0014】

好ましくは、本発明による方法は、2つのデータセットが装置内に同時に存在することを必要としない。

【0015】

好ましくは、ミキサ数はランダムに生成される。

【0016】

ミキサ数は、好ましくは装置によって生成される。変形形態として、ミキサ数は、別の信頼できる装置によって生成される。

【0017】

ミキサ数の生成は、たとえば、温度および時間などの、そのうちの少なくとも1つが絶えず変化する物理量である入力値のペアに、または量子現象に基づき得る。たとえば、そのような生成は、光子がプレートを通過するために2つのヤングのスリットのうちのどちらを使用することを選ぶかに基づき得る。

【0018】

好ましくは、ステップa)における混合動作は装置によって行われる。変形形態として、混合は別の信頼できる装置によって行われる。

【0019】

混合関数は、第1のデータセットとミキサ数を組み合わせる。好ましくは、第1のデータセットのビットおよびミキサ数のビットを1つずつ追加するのは、XOR論理関数である。ミキサ数のサイズは一般に第1のデータセットのサイズよりも小さいので、XORを介してミキサ数のビットを第1のデータセットの最初のビットまたは最後のビットに追加することが可能である。

【0020】

ミキサ数は、第1のデータセットと同じサイズを有し得る。この場合、XOR関数を介した追加は、1つずつ、すべてのビットに対して行われる。

【0021】

10

20

30

40

50

代替として、混合関数は、ミキサ数を第1のデータセットの末尾に追加することから成る。

【0022】

混合関数は、第1のデータセットを暗号化するための暗号化鍵としてミキサ数を使用する暗号化関数でさえあり得る。

【0023】

好ましくは、ステップb)におけるデータは装置によってハッシュ化される。変形形態として、ハッシュ化は別の信頼できる装置によって行われる。

【0024】

好ましくは、ハッシュ関数はSHA1、SHA2、SHA256およびMD5ならびにJenkins関数の中から選ばれる。

【0025】

本発明による方法の第1の変形形態は、送信者から発信されるメッセージの整合性を装置を用いて検証するための方法であり、この方法は、

i. 装置がメッセージおよびメッセージの識別子を受信するステップであって、前記メッセージが第1のデータセットを形成する、ステップと、

ii. ミキサ数を生成するステップと、

iii. メッセージがミキサ数と混合され、次いでハッシュ化される、ステップa)およびステップb)を実施するステップと、

iv. 任意選択でミキサ数を暗号化するステップと、

v. 装置がメッセージの識別子および任意選択で暗号化されたミキサ数をメッセージの送信者に送信するステップと、

vi. 装置が送信者から発信される暗号化された第3のデータセットを好ましくはメッセージの識別子とともに受信するステップと、

vii. 第3のデータセットを復号するステップと、

viii. ステップc)を実施するステップであって、ステップviiにおいて復号された第3のデータセットとステップb)において取得されたハッシュとが同一である場合、メッセージの整合性が保証される、ステップと

を含む。

【0026】

メッセージの「整合性」とは、たとえば、メッセージの伝送中にメッセージを傍受した悪意のある第三者による改変がないことであると理解されなければならない。

【0027】

メッセージの識別子は、とりわけASCIIコードを介してデジタル語に変換されることが可能な一連の英数字および/または記号であり得る。

【0028】

メッセージの識別子は、送信者の識別子およびメッセージの順序数を含み得る。

【0029】

送信者の認証は、具体的には、ステップviiにおける復号動作によって保証される。

【0030】

本発明のこの第1の変形形態は、受信されたメッセージの整合性とメッセージの送信者のアイデンティティの整合性の両方を保証することを可能にする。

【0031】

データを送信することおよびデータを受信することに関するステップは、同じ通信プロトコルを使用してまたは異なる通信プロトコルを使用して行われ得る。たとえば、ステップiにおいて受信されるデータはWi-Fiを介して受信され、ステップvにおいて送信されるデータは4Gを介して送信され、ステップviにおいて受信されるデータはWiMAXを介して受信される。

【0032】

ステップiにおいて、装置は送信者の識別子も受信し得る。この識別子は、装置が様々な

10

20

30

40

50

送信者からのメッセージを受信することができる場合に有用であり、そのような識別子は、本発明のこの第1の変形形態において説明された暗号化動作および復号動作の間に送信者と交換される情報を暗号化または復号するために使用されるべき暗号化鍵を選ぶことを可能にする。

【0033】

好ましくは、この第1の変形形態による方法は、ステップvとステップviとの間に、

- 送信者がメッセージの識別子および任意選択で暗号化されたミキサ数を受信するステップと、

- 任意選択でミキサ数を復号するステップと、

- メッセージの識別子を使用して、装置に送信されたメッセージを識別するステップと、

- 混合関数を使用して、メッセージを任意選択で復号されたミキサ数と混合するステップと、

- ハッシュ関数を使用して、先行するステップから生じるデータをハッシュ化するステップと、

- 先行するステップから生じるハッシュを暗号化するステップと、

- 暗号化されたハッシュを好ましくはメッセージの識別子とともに装置に送信するステップと

を含む。

【0034】

ステップivにおけるミキサ数の任意選択の暗号化は、好ましくは装置によって行われる。

【0035】

ミキサ数の任意選択の暗号化は、この数が悪意のある第三者によって傍受および改変されるのを防止することを可能にする。

【0036】

好ましくは、ミキサ数の任意選択の暗号化は、少なくともその数のサイズに等しいサイズの使い捨て鍵を使用して行われる。鍵は使い捨てであるので、ミキサ数が送信されるたびに新しい鍵が使用される。

【0037】

暗号化はまた、対称鍵を使用して行われ得る。対称暗号化鍵は送信者と装置との間で秘密にしておかれるものであり、好ましくは特定の数の伝送の後で更新される。

【0038】

代替として、ミキサ数の任意選択の暗号化は非対称であり、関連する秘密鍵を使用した送信者による復号を可能にするために、装置に知られている送信者の公開鍵を使用して、または、その公開鍵が送信者に知られている装置の秘密鍵を使用して、のいずれかで行われる。

【0039】

したがって、第三者がミキサ数を知るまたは改変することが防止される。

【0040】

好ましくは、ステップviiにおける復号は装置によって行われる。

【0041】

好ましくは、ステップivにおける暗号化が使い捨て鍵を使用して行われる場合、ステップviiにおける復号は対称鍵を使用して行われる。

【0042】

代替として、ステップivにおける暗号化が対称鍵を使用して行われる場合、ステップviiにおける復号は使い捨て鍵を使用して行われる。

【0043】

ステップviiにおける復号はまた、他の方法を使用して、たとえば、ステップviにおいて受信されたハッシュを暗号化するように働いた送信者の秘密鍵に関連付けられた、装置に知られている公開鍵を使用して行われ得る。したがって、装置は送信者のアイデンティティを認定することが可能である。

10

20

30

40

50

【0044】

ミキサ数は、ミキサ数を暗号化するように働く対称鍵が使用される場合、そのような対称鍵と同じサイズを有し、ハッシュと同じサイズも有し得る。

【0045】

好ましくは、秘密で対称の使い捨て暗号化鍵およびミキサ数は、送信者または装置によって送信されたデータをリッスンすることが、装置によって受信されたが前記鍵を正規に保持することになっている者以外の送信者によって伝送されたメッセージの整合性を誤って認識させることになる不正な第2のデータセットを生成および伝送することを可能にするのを防止するために、第三者デバイスによって推測できず、観測できない。

【0046】

ミキサ数 x の暗号化鍵 X が知られている場合、 x の暗号化を復号し、メッセージをハッシュ化する前にメッセージの混合を計算すれば十分であるので、混合されたメッセージのハッシュが知られていることがある。次いで、ハッシュを暗号化する鍵 Y はまた、小さい母集団に属することが推測されるかまたは知られていることがあり、混合されたメッセージのハッシュおよび Y を用いたその暗号化は両方とも、知られているかまたは観測可能である。したがって暗号化鍵 Y は暗号化鍵 X の関数 F であるか、またはさもなければ、暗号化鍵 Y は暗号化鍵 X に依存する母集団に属する。複数の伝送の観測は複数の関数 F を出現させ、鍵 X および鍵 Y の値はこれらの関数の共通部分にある。この状況を回避することが好ましい。したがって、鍵 X または鍵 Y について、伝送の間に変化する値を使用すること、または「メッセージ、暗号化された数、暗号化されたハッシュ」という3つ組の交換の観測ごとに、可能な X ごとの鍵 Y の母集団が大きくなる(このことにより、各観測において推論できるこれらの母集団の共通部分から生じる母集団が大きくなる)ような暗号化関数を使用することのいずれかが推奨される。鍵 Y について、ランダムに生成されたミキサ数 x を取ることは推奨されない。具体的には、ミキサ数 x が暗号化鍵 Y として使用される場合、または実際に鍵 Y が定義された式を使用してミキサ数 x に応じて計算される場合、鍵 X 、ミキサ数 x 、およびしたがって Y で暗号化されたミキサ数 x の暗号化された値 C を知ることが、鍵 X の別の関数 G になり、鍵 X および鍵 Y は、関数 F およびこの新しい関数 G の共通部分にあることになる。好ましくは、鍵 X または鍵 Y は各交換の後に更新される。

【0047】

装置は、定義された数に達したときに検証試行の阻止をトリガする連続した検証試行の失敗のカウンタをさらに含んでもよく、装置は、場合によっては、ミキサ数を暗号化するために使用される暗号化鍵またはハッシュを暗号化するために使用される暗号化鍵の更新の間にブロックされない。

【0048】

本発明による方法の第2の変形形態は、送信者から発信されるメッセージの整合性を装置を用いて検証するための方法であり、この方法は、

- i. 装置がメッセージ、暗号化された第3のデータセット、および暗号化されたミキサ数を受信するステップと、
- ii. ミキサ数および第3のデータセットを復号するステップと、
- iii. ステップa)~ステップc)を実施するステップであって、ステップb)において取得されたハッシュとステップiiにおいて復号された第3のデータセットとが同一である場合、メッセージの整合性が保証される、ステップとを含む。

【0049】

好ましくは、本発明のこの第2の変形形態による方法は、ステップiの前に、

- 送信者がミキサ数を生成するステップと、
- 混合関数を使用して、ミキサ数をメッセージと混合するステップと、
- ハッシュ関数を使用して、先行するステップから生じるデータをハッシュ化するステップと、
- 先行するステップから生じるハッシュを暗号化し、第3のデータセットを形成するス

10

20

30

40

50

テップと、

- ミキサ数を暗号化するステップと、
- メッセージ、暗号化された第3のデータセット、および暗号化されたミキサ数を装置に送信するステップとを含む。

【0050】

これらのステップは、本物の送信者によって行われ、無許可の第三者によるメッセージの改変が検出されることを可能にする。

【0051】

ミキサ数および第3のデータセットのステップiiにおける復号は、好ましくは装置によって行われる。

10

【0052】

好ましくは、ミキサ数の暗号化は使い捨て鍵を使用して行われ、第3のデータセットの暗号化は対称鍵を使用して行われ、対称鍵は好ましくは時々更新される。

【0053】

代替として、ミキサ数の暗号化は対称鍵を使用して行われ、第3のデータセットの暗号化は使い捨て鍵を使用して行われ、対称鍵は好ましくは時々更新される。

【0054】

ミキサ数の暗号化および第3のデータセットの暗号化はまた、同じタイプであるか、または異なるタイプであってもよく、これらのタイプの暗号化は、場合によっては、対称鍵または非対称鍵を用いる。

20

【0055】

非対称鍵のペアがミキサ数の暗号化に使用される場合、前記ペアの秘密鍵は好ましくは装置によって保持され、次いで、対応する公開鍵が送信者に知られる。

【0056】

第3のデータセットの暗号化は、好ましくは、送信者によって保持された秘密鍵を使用して行われ、次いで、対応する公開鍵が装置に知られる。

【0057】

したがって、ミキサ数および第3のデータセットを復号することによって、装置は送信者のアイデンティティを認定することが可能である。

30

【0058】

ミキサ数の暗号化および第3のデータセットの暗号化は、同じ暗号化関数を使用して、具体的にはミキサ数の暗号化が非対称であるときに行われ得る。

【0059】

代替として、ミキサ数の暗号化および第3のデータセットの暗号化は、2つの異なる暗号化関数によって行われる。

【0060】

好ましくは、使用されるべき暗号化関数のタイプは、送信者と装置との間の通信のセットアップの前に、送信者および装置の構成の一部を形成する。

【0061】

本発明による方法の第3の変形形態は、第1のデータセットが装置内に存在し、第2のデータセットが第2の装置内に存在する方法であり、この方法は、

40

- i. ステップa)およびステップb)を実施するステップと、
- ii. ミキサ数を暗号化するステップと、
- iii. 装置が暗号化されたミキサ数を第2の装置に送信するステップと、
- iv. 装置が第2のデータセットの暗号化されたハッシュを受信するステップと、
- v. 暗号化されたハッシュを復号するステップと、
- vi. ステップc)を実施するステップと

を含む。

【0062】

50

好ましくは、本発明のこの第3の変形形態による方法は、ステップiiiとステップivとの間に、

- 第2の装置が暗号化されたミキサ数を受信するステップと、
- ミキサ数を復号するステップと、
- ミキサ数および混合関数を使用して、第2のデータセットの変更されたコピーを作成するステップと、
- ハッシュ関数を使用して、第2のデータセットの変更されたコピーをハッシュ化するステップと、
- 先行するステップから生じるハッシュを暗号化し、第3のデータセットを形成するステップと、
- 第2の装置が第2のデータセットの暗号化されたハッシュを装置に送信するステップとを含む。

10

【0063】

ステップiiにおけるミキサ数の暗号化およびステップvにおける暗号化されたハッシュの復号は、好ましくは装置によって行われる。

【0064】

好ましくは、ミキサ数の暗号化は、第2の装置と共有される対称暗号化鍵を使用して行われる。

【0065】

好ましくは、ハッシュの暗号化は使い捨て鍵を使用して行われ、ミキサ数の暗号化は時々更新される対称鍵を使用して行われる。

20

【0066】

代替として、ミキサ数の暗号化は使い捨て鍵を使用して行われ、ハッシュの暗号化は時々更新される対称鍵を使用して行われる。

【0067】

ミキサ数の暗号化およびハッシュの暗号化はまた、同じタイプであるか、または異なるタイプであってもよく、これらのタイプの暗号化は、場合によっては、対称鍵、具体的には使い捨て鍵、または非対称鍵を用いる。

【0068】

本発明による方法の第4の変形形態は、装置内に存在するデータセットが2つの時間d1とd2との間で変更されていないことを検証するための方法であり、このデータセットは時間d1において第1のデータセットを形成し、時間d2において第2のデータセットを形成し、この方法は、

30

- i. ステップa)およびステップb)を実施するステップと、
 - ii. 装置がミキサ数およびステップb)において取得されたハッシュをセキュアに保存するステップと、
 - iii. ミキサ数および混合関数を使用して、第2のデータセットの変更されたコピーを作成するステップと、
 - iv. 第3のデータセットを形成するために、ハッシュ関数を使用して、変更されたコピーをハッシュ化するステップと、
 - v. ステップc)を実施するステップと
- を含む。

40

【0069】

有利には、この第4の変形形態による方法は、データセットがセキュアに保持されることを必要としない。

【0070】

本発明の別の主題は、上記で定義された変形形態のうちのいずれか1つによる本発明による方法を実施するための装置のプロセッサによって読み取り可能な命令を含むコンピュータプログラム製品である。

【0071】

50

本発明は、その実装形態の非限定的な例の以下の詳細な説明を読み、添付の図面を検討すれば、より良く理解される可能性がある。

【図面の簡単な説明】

【0072】

【図1】本発明の第1の変形形態または本発明の第2の変形形態による、本発明を実施するために必要なデータおよび関数を概略的に示す図である。

【図2】本発明の第1の変形形態による、本発明の実装形態の一例を概略的に示す図である。

【図3】本発明の第2の変形形態による、本発明の実装形態の一例を概略的に示す図である。

【図4】本発明の第3の変形形態による、本発明を実施するために使用されるデータおよび関数を概略的に示す図である。

【図5】本発明の第3の変形形態による、本発明の実装形態の一例を概略的に示す図である。

【図6】本発明の第4の変形形態による、本発明の実装形態の方式を示す図である。

【図7】図8の例を実施するために使用されるデータを概略的に示す図である。

【図8】ソフトウェアパッケージの検証に適用される、本発明の実装形態の第1の例を示す図である。

【図9】ソフトウェアパッケージの検証に適用される、本発明の実装形態の第2の例を示す図である。

【図10】図11の例を実施するために使用されるデバイスおよびデータを概略的に示す図である。

【図11】インターネットブラウザのセキュリティの強化に適用される本発明の実装形態の一例を示す図である。

【図12】図13の例を実施するために使用されるデバイスおよびデータを概略的に示す図である。

【図13】電子メールのセキュリティの強化に適用される本発明の実装形態の一例を示す図である。

【発明を実施するための形態】

【0073】

図1は、本発明の第1の変形形態または本発明の第2の変形形態による、本発明を実施するために使用されるデータおよび関数を概略的に示し、図1において、メッセージ101はデータ伝送チャンネル109を介してデバイスAによってデバイスBに送信されなければならない、このチャンネルはセキュアまたは非セキュアであり得る。

【0074】

デバイスAはパーソナルコンピュータまたはスマートフォンであってもよく、デバイスBは電子メールサーバであってもよく、メッセージ101は、たとえば、インターネットを介してコンピュータまたは電話によって送信される電子メールであってもよい。

【0075】

デバイスAはまた、電子メールまたはウェブページを送信するサーバであってもよく、デバイスBは、今度は前記電子メールまたはウェブページを受信するパーソナルコンピュータまたはスマートフォンであってもよい。

【0076】

デバイスAは、たとえば、電気、ガスまたは水の消費量を測定するための、または機械内の部品の摩耗を測定するための測定装置でさえであってもよく、メッセージ101は、今度はそのような測定の結果であってもよく、デバイスBは、測定値を収集し、電気通信ネットワーク、たとえば、モノのインターネット、Wi-FiネットワークまたはLTEネットワークを介して測定装置と通信するサーバであってもよい。

【0077】

デバイスAおよびデバイスBはまた、パーソナルコンピュータまたはスマートフォンであ

10

20

30

40

50

ってもよい。

【0078】

デバイスAはウェブブラウザであってもよく、デバイスBはウェブサーバであってもよく、メッセージ101はブラウザAのユーザによって記入されるフォームであってもよく、メッセージの受信はその伝送に関して差別化されることを必要としなくてもよい。

【0079】

デバイスAおよびデバイスBはそれぞれ、本発明による方法のステップを実行するためのプロセッサと、この実行に必要とされるデータを保存するためのメモリとを備えてもよい。

【0080】

デバイスBは、秘密鍵などの暗号化/復号データ102Bを入手することができる。デバイスAは、秘密鍵102Bに関連付けられた公開鍵などの暗号化/復号データ102Aを入手することができる。

10

【0081】

デバイスAはまた、デバイスB内に存在する公開鍵103Bに関連付けられた秘密鍵などの暗号化/復号データ103Aを入手することができる。

【0082】

デバイスAおよびデバイスBは、それぞれ乱数生成器104Aおよび104Bと、共通の混合関数105と、共通のハッシュ関数106とを所有する。

【0083】

デバイスAおよびデバイスBはまた、それぞれ暗号化関数107Aおよび107Bと、それぞれ復号関数108Aおよび108Bとを有する。

20

【0084】

図2は、本発明の第1の変形形態による方法の実装形態の一例を示す。

【0085】

ステップ201において、メッセージ101を識別するために使用される第1の数が、デバイスAによって生成される。第1の数は、任意選択で、乱数生成器104Aを使用して生成され得る。

【0086】

ステップ202において、第1の数がメッセージ101に追加される。この追加は、2つのデバイス間で使用される通信プロトコルによって定義される任意の順序での連結であり得る。

30

【0087】

ステップ203において、デバイスAが、ステップ202から生じるデータをデバイスBにデータ伝送チャンネル109を介して送信する。

【0088】

ステップ204において、データの受信時に、デバイスBが、乱数生成器104Bを使用して第2の数をランダムに生成する。

【0089】

ステップ205において、デバイスBが、第2の数をメッセージ101と混合するために混合関数105を利用する。例として、この混合関数は第2の数のビットとメッセージ101の同じ数のビットとの間で演算するXORである。混合関数105はデバイスAによって知られている。

40

【0090】

ステップ206において、デバイスBが、先行するステップにおいて取得されたデータをハッシュ化するためにハッシュ関数106を使用する。デバイスBはまた、第2の数を暗号化するために公開暗号化鍵103Bおよび暗号化関数107Bを使用する。

【0091】

ステップ207において、デバイスBが、第1の数および暗号化された第2の数をデバイスAにチャンネル109を介して送信する。

【0092】

50

ステップ208において、2つの数の受信時に、デバイスAが、暗号化に必然的に使用された公開鍵103Bに関連付けられた秘密暗号化鍵103Aおよび暗号化関数107Bに関連付けられた復号関数108Aを使用して第2の数を復号する。第2の数がデバイスBによって暗号化されなかった場合、その復号は誤ったものになる。

【0093】

第1の数があれば、デバイスAはメッセージ101を識別し、混合関数105を使用して、復号された第2の数を識別されたメッセージ101と混合することができる。

【0094】

ステップ209において、デバイスAが、先行するステップから生じるデータをハッシュ化するためにハッシュ関数106を使用する。

【0095】

ステップ210において、デバイスAが、先行するステップにおいて取得されたハッシュを暗号化するために秘密暗号化鍵103Aおよび暗号化関数107Aを使用する。

【0096】

ステップ211において、デバイスAが、暗号化されたハッシュをデバイスBにチャンネル109を介して送信する。

【0097】

ステップ212において、暗号化されたハッシュの受信時に、デバイスBが、暗号化に必然的に使用された秘密鍵103Aに関連付けられた公開暗号化鍵103Bおよび暗号化関数107Aに関連付けられた復号関数108Bを使用して、暗号化されたハッシュを復号する。

【0098】

ステップ213において、デバイスBが、ステップ212において取得された復号されたハッシュをステップ206において計算されたハッシュと比較する。2つのハッシュが同一である場合、デバイスBは、メッセージ101が改変されていないと結論付ける。

【0099】

好ましくは、混合において使用される第2の数は、検証を行うためにハッシュが比較されるまで秘密にされていなければならないが、このミキサ数は、ミキサ数が明らかにされる時点とハッシュの比較との間でデータが変更されないようにハッシュを計算するデバイスを信頼することが可能である場合、その前に明らかにされることがある。

【0100】

図3は、本発明の第2の変形形態による方法の実装形態の第2の例を示し、メッセージ101は、デバイスAによってデバイスBに送信されることを必要とする。

【0101】

デバイスAおよびデバイスBはパーソナルコンピュータまたはスマートフォンであってもよく、メッセージ101は電子メールであってもよい。

【0102】

デバイスAおよびデバイスBは、隣接する自動車であってもよく、交換されるデータは、今度はそれらの動きに関する情報であってもよく、接続は、2つの車両の間のデータリンク、たとえば、5Gリンク、低エネルギーBluetoothリンク、超高周波数RFIDリンク、LoraリンクまたはSigfoxリンクを介して達成されてもよい。

【0103】

ステップ301において、乱数生成器104Aを使用して、乱数がデバイスAによって生成される。

【0104】

ステップ302において、デバイスAが、混合関数105を使用して、メッセージ101を乱数と混合する。

【0105】

ステップ303において、デバイスAが、ハッシュ関数106を使用して、先行するステップから生じる混合されたデータをハッシュ化する。

【0106】

10

20

30

40

50

ステップ304において、デバイスAが、暗号化関数107Aおよび秘密暗号化鍵103Aを使用して、先行するステップにおいて取得されたハッシュを暗号化する。

【0107】

ステップ305において、デバイスAが、暗号化関数107Aおよび公開暗号化鍵102Aを使用して、乱数を暗号化する。

【0108】

ステップ306において、メッセージ101、暗号化された乱数、および暗号化されたハッシュが、2つのデバイス間で同意された通信プロトコルを使用して、デバイスBに伝送チャネル109を介して送信される。

【0109】

ステップ307において、データの受信時に、デバイスBが、ハッシュを復号するために復号関数108Bおよび公開暗号化鍵103Bを使用し、乱数を復号するために秘密暗号化鍵102Bを使用する。

【0110】

このようにして、デバイスBはデバイスAを認証することができる。

【0111】

ステップ308において、デバイスBが、混合関数105を使用して、メッセージ101を乱数と混合する。

【0112】

ステップ309において、デバイスBが、ハッシュ関数106を使用して、先行するステップから生じる混合されたデータをハッシュ化する。

【0113】

ステップ310において、デバイスBが、デバイスBが計算したハッシュを復号されたハッシュと比較し、メッセージ101の整合性に関する結論を出す。

【0114】

この例では、デバイスBはデバイスAから受信されたデータを第3のデバイスに転送してもよい。デバイスBは、デバイスBがデバイスAから受信した乱数を第3のデバイスの公開鍵を使用して再び暗号化する前に、その乱数を秘密鍵102Bを使用して復号する。次いで、デバイスBは、暗号化された乱数およびデバイスAによって暗号化されたハッシュを第3のデバイスに伝送する。デバイスAの公開鍵を入手することができる第3のデバイスは、デバイスBがデバイスAによって暗号化されたハッシュを変更しなかった限り、このハッシュが実際にデバイスAから来たことを検証することができる。したがって、所与のデータセットは、多くのユーザによって本物として検証され得る。しかしながら、このオプションは認定のセキュリティをむき出しにし、不正なデバイスは、乱数を復号し、場合によっては、メッセージが初期ハッシュと同じランダムハッシュを有するようにメッセージを変更することができる。したがって、この実装形態は好ましくは、そのような不正な使用から保護された要素から形成されたコンピュータシステム間の通信を認定するために使用される。

【0115】

図4は、デバイスA上に存在するファイル401AがデバイスB上に存在するファイル401Bと同一であることを検証するための、本発明の第3の変形形態による、本発明を実施するために必要とされるデータおよび関数を概略的に示す。

【0116】

デバイスAおよびデバイスBは、たとえばWi-Fiネットワークである伝送チャネル409を介して通信する。

【0117】

デバイスAは乱数生成器404を所有する。

【0118】

デバイスAおよびデバイスBは共通して混合関数405、ハッシュ関数406、および対称暗号化鍵410を有する。

10

20

30

40

50

【0119】

デバイスBは暗号化関数407を入手することができる。

【0120】

デバイスAは復号関数408を入手することができる。

【0121】

図5は、本発明の第3の変形形態による方法の実装形態の第3の例を示す。

【0122】

ステップ501において、乱数生成器404を使用して、デバイスAにおいて乱数が生成される。

【0123】

ステップ502において、混合関数405および乱数を使用して、ファイル401Aの変更されたコピーが作成される。

【0124】

ステップ503において、ハッシュ関数406を使用して、ファイル401Aの変更されたコピーがハッシュ化される。

【0125】

ステップ504において、対称暗号化アルゴリズムおよび対称暗号化鍵410を使用して、乱数が暗号化され、デバイスBに伝送チャネル409を介して送信される。

【0126】

ステップ505において、暗号化された乱数の受信時に、デバイスBが暗号化された乱数を復号し、暗号化された乱数を混合関数405において使用して、ファイル401Bの変更されたコピーを作成する。乱数を復号することによって、デバイスBはデバイスAのアイデンティティを検証することができる。

【0127】

ステップ506において、ファイル401Bの変更されたコピーが同じハッシュ関数406でハッシュ化される。

【0128】

ステップ507において、暗号化関数407および暗号化鍵410を使用して、変更されたコピーのハッシュが暗号化される。

【0129】

ステップ508において、暗号化されたハッシュがデバイスAに送信される。

【0130】

ステップ509において、暗号化されたハッシュの受信時に、復号関数408および鍵410を使用して、デバイスAが暗号化されたハッシュを復号する。

【0131】

ステップ510において、デバイスAが復号されたハッシュをデバイスAがステップ503において計算したハッシュと比較し、このようにして、2つのファイル401Aおよび401Bが同一であるかどうかを検証することができる。

【0132】

図6は、2つの時間d1とd2との間でより小さいデータセットを完全にセキュアに保ちながら、ファイルがその2つの時間の間で変更されていないことを検証するための、本発明の第4の変形形態による方法の実装形態の第4の例を示し、このセットは、そのまま秘密にされている数と、そのまま好ましくは秘密にされているハッシュとを含む。

【0133】

ステップ601において、乱数が生成される。

【0134】

ステップ602において、時間d1で、生成された乱数および混合関数を使用して、ファイルの変更されたコピーが作成され、この関数は、たとえば、乱数をファイルの末尾に追加することから成る。

【0135】

10

20

30

40

50

ステップ603において、たとえばSHA2関数を使用して、変更されたコピーのハッシュが作成される。

【0136】

ステップ604において、乱数およびハッシュを変更することができないように、かつ乱数が第三者に開示されないように、乱数およびハッシュがセキュアかつ秘密に記憶される。

【0137】

ステップ605において、時間d2で、ステップ604において記憶された情報にアクセスできる人またはデバイスが、時間d2におけるファイルをステップ601～604において使用されたファイルと比較することを望む。これを行うために、保存された乱数が、ステップ602の場合と同じ混合関数を使用して、時間d2におけるファイルの第2の変更されたコピーを作成するために使用される。

10

【0138】

ステップ606において、ステップ603の場合と同じハッシュ関数を使用して、第2の変更されたコピーのハッシュが作成される。

【0139】

ステップ607において、ファイルが時間d1とd2との間で変更されていないことを保証するために、先行するステップにおいて作成されたハッシュが記憶されたハッシュと比較される。

【0140】

図7は、ソフトウェアパッケージの検証に適用される本発明による方法の、図8に示される第5の例を実施するために必要な鍵を概略的に示す。

20

【0141】

説明の残りの部分では、ハッシュ化動作が後に続く、データをランダムミキサ数と混合する動作は、このデータの「ランダムハッシュ化」と称される。

【0142】

図8に示される例は、2つのデバイス、すなわち、ソフトウェアディストリビュータと称されるデバイスAとクライアントデバイスと称されるデバイスBとの間で実施される。

【0143】

デバイスAは2つの鍵701および702を所有する。

【0144】

701は、ハッシュを暗号化するように働く鍵であり、好ましくは秘密である。

30

【0145】

702は、乱数を暗号化するように働く鍵であり、好ましくは公開である。

【0146】

デバイスBは2つの鍵703および704を所有する。

【0147】

703は、鍵701を使用して暗号化されたハッシュを復号するために使用される鍵であり、好ましくは公開である。

【0148】

704は、鍵702を使用して暗号化された乱数を復号するために使用される鍵であり、好ましくは秘密である。

40

【0149】

鍵(701、703)のペアは、ソフトウェアディストリビュータの鍵のペアと称されることがあるものであり、ソフトウェアディストリビュータは、ソフトウェアディストリビュータが配布するソフトウェアパッケージのうちの1つがインストールされるすべての装置と通信するために、その鍵のペアを使用することができる。

【0150】

鍵(704、702)のペアは、クライアントの鍵のペアと称されることがあるものであり、クライアントは、ダウンロード中にクライアントが検証するすべてのソフトウェアパッケージについて、その鍵のペアを使用することができる。

50

【0151】

ステップ801において、ソフトウェアディストリビュータAが、図3を参照しながら上記で説明されたステップ301～305において、クライアントBに伝送されるべきソフトウェアパッケージのランダムハッシュ化を実施する。

【0152】

ソフトウェアディストリビュータAは、乱数を暗号化するために鍵702を使用し、ソフトウェアパッケージのランダムハッシュを暗号化するために鍵701を使用する。

【0153】

ステップ802において、ソフトウェアディストリビュータAが、クライアントBに、ソフトウェアパッケージと、ソフトウェアパッケージの暗号化されたハッシュと、暗号化された乱数とを含むデータセットを、セキュアまたは非セキュアであり得る伝送線路を介して送信する。

10

【0154】

ステップ803において、データセットの受信時に、クライアントBが、鍵703でハッシュを復号し、鍵704で乱数を復号する。次いで、クライアントBは、受信されたソフトウェアパッケージのランダムハッシュ化を実施するためにその乱数を使用する。

【0155】

ステップ804において、計算されたハッシュが受信されたハッシュと同一である場合、クライアントBは、受信されたソフトウェアパッケージの実行を許可するか、またはソフトウェアパッケージの前のバージョンをクライアントBが受信したばかりのバージョンと置き換える。

20

【0156】

ステップ805において、より良いセキュリティのために、ステップ803および804が、ソフトウェアパッケージの真正性を検証するために、事前にプログラムされた時間間隔で再実行される。

【0157】

図9は、ダウンロード中であるソフトウェアパッケージが装置上で実行中であるソフトウェアパッケージによって許可されることを検証するための、ランダムハッシュ化の別の可能な実装形態について説明する。

【0158】

ステップ901において、装置が、受信されたソフトウェアパッケージが信頼できるソースから発信されていることを検証するために、図2に示された方法を使用する。

30

【0159】

ステップ902において、装置においてソフトウェアパッケージのセキュアな署名を作成するために、図6のステップ601～604が実行される。

【0160】

ステップ903において、ソフトウェアパッケージを使用する前に、ステップ902以降にソフトウェアパッケージが変更されていないことを検証するために、図6のステップ605～607が実行される。

【0161】

図10は、ウェブブラウザによって表示されるデータのセキュリティを高めることを可能にする、図11に示される例を実施するために必要なオブジェクトを示す。

40

【0162】

ウェブブラウザ1001は、秘密鍵1002pおよび公開鍵1002uから成る非対称鍵のペアを入手することができる。

【0163】

セキュアなインターネットサイト1004sの公開鍵をブラウザに配布するサーバ1003sは、秘密鍵1003pおよび公開鍵1003uから成る非対称鍵のペア1003を所有する。

【0164】

インターネットサイト1004sは、秘密鍵1004pおよび公開鍵1004uから成る非対称鍵

50

のペア1004を所有する。

【0165】

ステップ1101において、ユーザが、ユーザが閲覧することを望むサイトのURLアドレスをブラウザ1001のアドレスバーに入力する。

【0166】

ステップ1102において、ブラウザ1001が、鍵のペア1002を使用し、以下の情報、すなわち、

- ユーザが閲覧することを望むサイトのURLアドレス、
- ブラウザの公開鍵1002u、および
- サーバがそれに応答することができるようなブラウザ1001のURLアドレス

をサーバ1003sに送信する。

【0167】

ステップ1103において、サーバ1003sが、サイト1004sの公開鍵1004uをブラウザにセキュアに送信するために、図2に示された本発明による方法を使用する。

【0168】

公開鍵1002uは、ナビゲータが交換の間にサーバに送信する第2の数を復号するためにサーバによって使用される。

【0169】

ステップ1104において、ブラウザ1001は、以下の情報、すなわち、

- ユーザが閲覧することを望むサイトのページの名前、
- ブラウザの公開鍵1002u、および
- サイトがそれに応答することができるようなブラウザのURLアドレス

をサイト1004sに送信する。

【0170】

ステップ1105において、サーバ1004sが、要求されたページをブラウザにセキュアに送信するために、図2に示された本発明による方法を使用する。

【0171】

図12は、電子メールのセキュリティを高めることを可能にする、図13に示される例を実施するために必要とされるオブジェクトを示す。

【0172】

場合によってはコンピュータまたはスマートフォンであり得る第1の電子デバイスAは、電子ファイルの形態を取る電子メール1200が送信、受信、アーカイブ、編集、および表示されることを可能にする。

【0173】

この第1のデバイスAは、公開鍵1201uおよび秘密鍵1201pから成る非対称鍵のペア1201cにアクセスできる。

【0174】

第2の電子デバイスBは、電子メール1200が送信、受信、アーカイブ、編集、および表示されることを可能にする。

【0175】

この第2のデバイスBは、公開鍵1202uおよび秘密鍵1202pから成る非対称鍵のペア1202cにアクセスできる。

【0176】

サーバ1203は、受信された電子メールの整合性および本発明によるランダムハッシュ化方法に関連付けられた乱数の機密性を維持することが認定された、AおよびBなどの電子デバイスの識別番号および公開鍵を収集する。

【0177】

サーバ1203は、公開鍵1203uおよび秘密鍵1203pから成る鍵のペア1203cにアクセスできる。このサーバは、各ペアが1つの明確に定義された電子デバイスとの通信に特化したものである複数の鍵のペアを有してもよいことに留意されたい。

10

20

30

40

50

【0178】

サーバ1204は、1つまたは複数の電子デバイスを電子メールの宛先アドレス1205に関連付ける。

【0179】

サーバ1204は、公開鍵1204uおよび秘密鍵1204pから成る鍵のペア1204cにアクセスできる。このサーバは、各々が1つの明確に定義された電子デバイスとの通信に特化したものである複数の鍵のペアを有してもよいことに留意されたい。

【0180】

ステップ1301において、ユーザが、第1のデバイスAが電子メール1200を宛先アドレス1205に送信することを要求する。

10

【0181】

ステップ1302において、第1のデバイスAが、アドレス1205に関連付けられたデバイスBの識別子および公開鍵を判定するために、図2に示された本発明による方法を使用して、第1のデバイスAが知っている公開鍵をサーバ1204と通信する。サーバ1204による第1のデバイスAの認証の後、サーバ1204が、デバイスBの識別子および公開鍵を第1のデバイスAに送信する。これはまた、図2に示された方法、デバイスAの公開鍵を知っているサーバ1204、およびサーバ1204の公開鍵を知っているデバイスAを使用して行われる。この方法は、デバイスAがサーバ1204から変更されていないデータを受信することを可能にする。サーバ1204自体は、サーバ1203からデバイスBの公開鍵を取得し、それと同時に、デバイスAの公開鍵を検証することができるようになっている。

20

【0182】

ステップ1303において、第1のデバイスAがその識別子をデバイスBに通信する。

【0183】

ステップ1304において、ステップ1303において通信された識別子を受信したデバイスBが、第1のデバイスAの公開鍵を判定するためにサーバ1203と通信する。この情報は図2の方法を使用してデバイスBに送信され、このことはデバイスBが変更されていない情報を受信することを可能にする。デバイスBは、受信確認をデバイスAに送信することによって、この情報の受信をデバイスAに通知する。

【0184】

ステップ1305において、ステップ1304において送信された受信確認の受信時に、第1のデバイスAが、電子メール1200をデバイスBに送信するために、図2に示された本発明による方法を使用し、デバイスBは次いで、この情報がデバイスAによって送信されたものであり、改変されずに受信されたものであるということを確認し得る。加えて、デバイスAは、この情報がデバイスBのみによって認定されたものであるということを確認する。

30

【0185】

非対称鍵および対称鍵を用いる暗号化方法は量子コンピュータに対して弱いことがあるので、これらの暗号化方法は、上記で説明された例では、使い捨て鍵を使用する暗号化方法と置き換えられ得る。

【0186】

本発明は、上記で説明された実施形態の例にも、例示された適用例にも限定されない。本発明は、具体的には、金融取引のセキュリティを高めるために使用され得る。

40

【符号の説明】

【0187】

- 101 メッセージ
- 102A 暗号化/復号データ、公開暗号化鍵
- 102B 暗号化/復号データ、秘密暗号化鍵
- 103A 暗号化/復号データ、秘密暗号化鍵
- 103B 公開暗号化鍵
- 104A, 104B 乱数生成器
- 105 混合関数

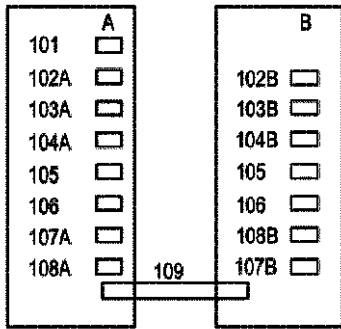
50

106	ハッシュ関数	
107A, 107B	暗号化関数	
108A, 108B	復号関数	
109	データ伝送チャンネル	
401A, 401B	ファイル	
404	乱数生成器	
405	混合関数	
406	ハッシュ関数	
407	暗号化関数	
408	復号関数	10
409	伝送チャンネル	
410	対称暗号化鍵	
701, 702, 703, 704	鍵	
1001	ウェブブラウザ	
1002	鍵のペア	
1002p	秘密鍵	
1002u	公開鍵	
1003	非対称鍵のペア	
1003p	秘密鍵	
1003s	サーバ	20
1003u	公開鍵	
1004	非対称鍵のペア	
1004p	秘密鍵	
1004s	インターネットサイト、サーバ	
1004u	公開鍵	
1200	電子メール	
1201c	非対称鍵のペア	
1201p	秘密鍵	
1201u	公開鍵	
1202c	非対称鍵のペア	30
1202p	秘密鍵	
1202u	公開鍵	
1203	サーバ	
1203c	鍵のペア	
1203p	秘密鍵	
1203u	公開鍵	
1204	サーバ	
1204c	鍵のペア	
1204p	秘密鍵	
1204u	公開鍵	40
1205	宛先アドレス	

【 図 面 】

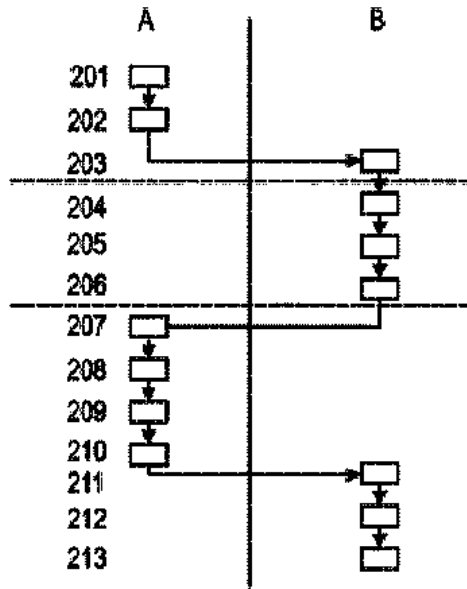
【 図 1 】

[Fig. 1]



【 図 2 】

[Fig. 2]

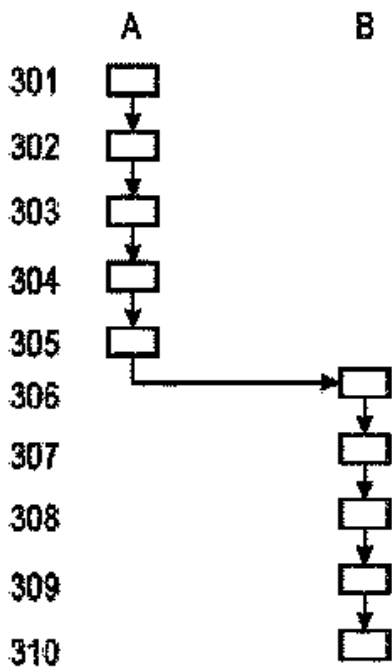


10

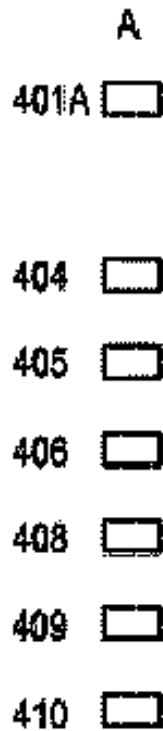
20

【 図 3 】

[Fig. 3]



【 図 4 A 】



30

40

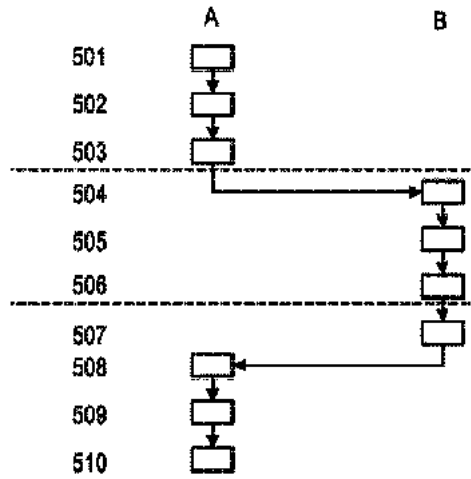
50

【 図 4 B 】



【 図 5 】

[Fig. 5]

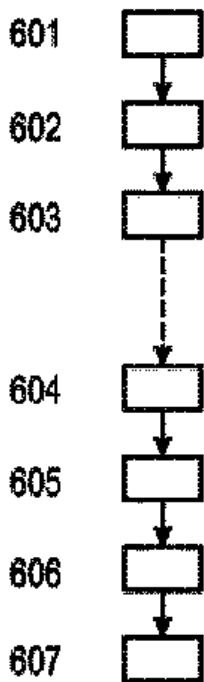


10

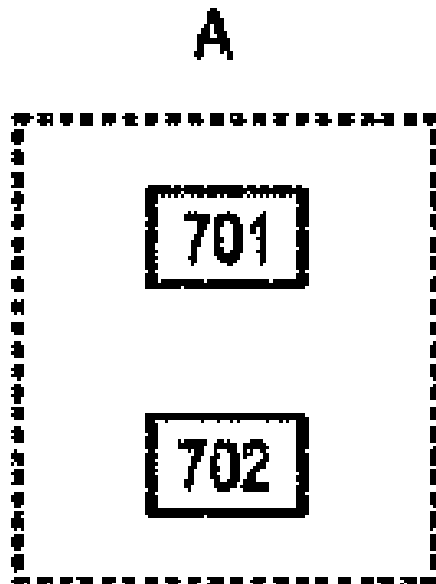
20

【 図 6 】

[Fig. 6]



【 図 7 A 】

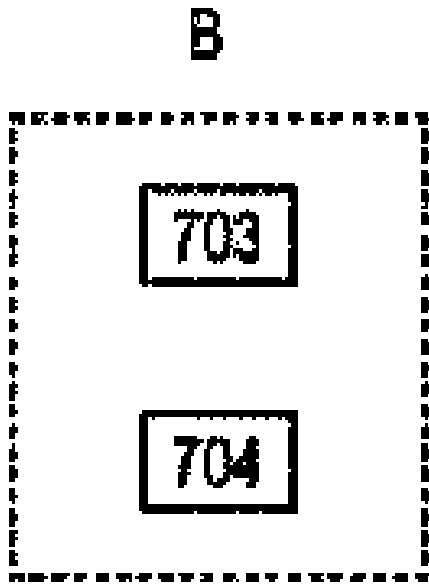


30

40

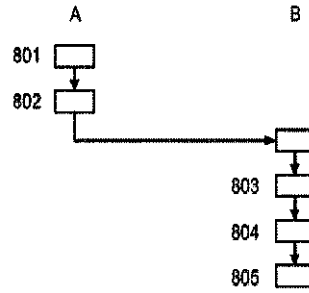
50

【 図 7 B 】



【 図 8 】

[Fig. 8]

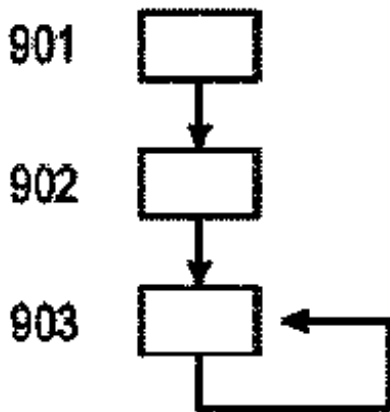


10

20

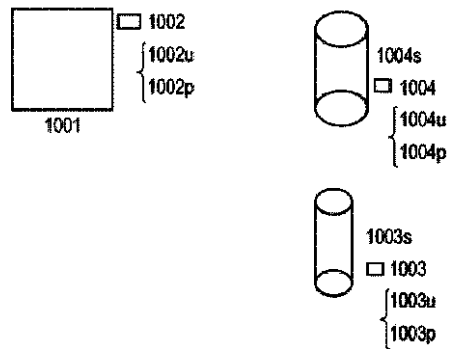
【 図 9 】

[Fig. 9]



【 図 1 0 】

[Fig. 10]



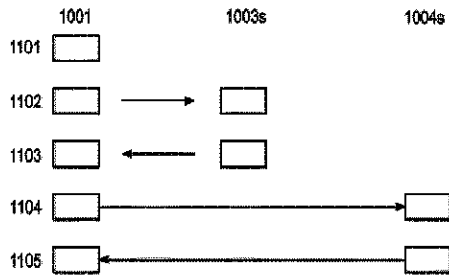
30

40

50

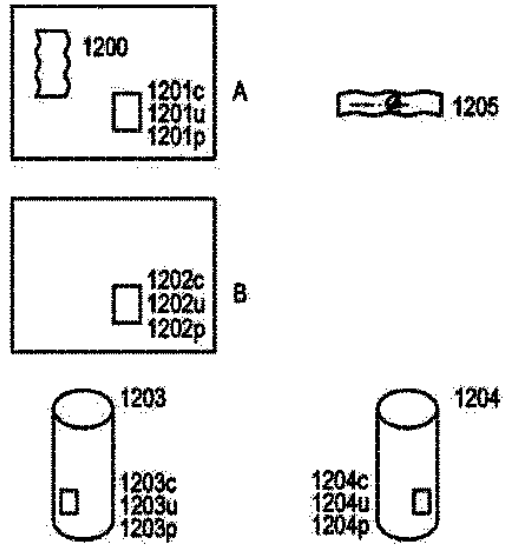
【 図 1 1 】

[Fig. 11]



【 図 1 2 】

[Fig. 12]

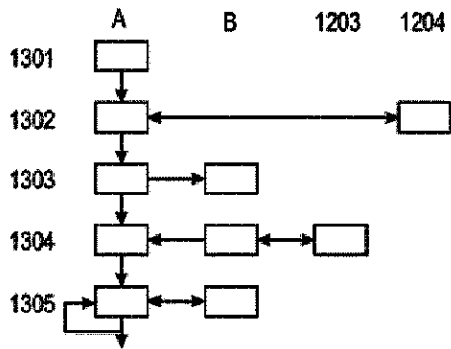


10

20

【 図 1 3 】

[Fig. 13]



30

40

50

フロントページの続き

- (56)参考文献 特開平 1 0 - 2 4 0 8 2 6 (J P , A)
特開 2 0 0 4 - 1 4 4 8 1 0 (J P , A)
特開 2 0 1 6 - 1 5 4 0 3 3 (J P , A)
米国特許出願公開第 2 0 0 3 / 0 0 2 1 4 1 9 (U S , A 1)
- (58)調査した分野 (Int.Cl. , D B 名)
H 0 4 L 9 / 3 2
G 0 6 F 2 1 / 6 4