(19)日本国特許庁(JP)　　(12)公表特許公報(A)　　(11)公表番号
特表2022-521525
(P2022-521525A)
(43)公表日　令和4年4月8日(2022.4.8)

(51)国際特許分類
H04L 9/32 (2006.01)
G06F 21/64 (2013.01)

FI
H04L 9/32 200A
H04L 9/32 200E
G06F 21/64

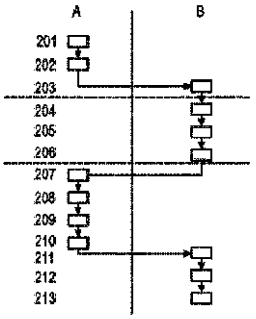
審査請求　未請求　予備審査請求　未請求　（全31頁）

(21)出願番号　特願2021-549168(P2021-549168)
(86)(22)出願日　令和2年2月17日(2020.2.17)
(85)翻訳文提出日　令和3年10月15日(2021.10.15)
(86)国際出願番号　PCT/EP2020/054126
(87)国際公開番号　WO2020/169542
(87)国際公開日　令和2年8月27日(2020.8.27)
(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)
(81)指定国・地域　AP(BW,GH,GM,KE,LR,LS,MW,MZ,NA,RW,SD,SL,ST,SZ,TZ,UG,ZM,ZW),EA(AM,AZ,BY,KG,KZ,RU,TJ,TM),EP(AL,AT,BE,BG,CH,CY,CZ,DE,DK,EE,ES,FI,FR,GB,GR,HR,HU,IE,IS,IT,LT,LU,LV,MC,
最終頁に続く

(71)出願人　521365820
ブリュノ・サングルーフェリエール
フランス・７５０１６・パリ・ブールヴァール・ボーセジュール・４７
(74)代理人　100108453
弁理士　村山 靖彦
(74)代理人　100110364
弁理士　実広 信哉
(74)代理人　100133400
弁理士　阿部 達彦
(72)発明者　ブリュノ・サングルーフェリエール
フランス・７５０１６・パリ・ブールヴァール・ボーセジュール・４７

(54)【発明の名称】　データを検証するための暗号方法

(57)【要約】
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(A; B)によって実施される方法であって、この方法は、これらの2つのデータセットが装置内に存在することを必要とせず、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(105; 405)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(106; 406)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(105; 405)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。



【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するステップと、
v. 任意選択で前記ミキサ数を暗号化するステップと、
vi. 前記装置(B)が前記メッセージの前記識別子および前記任意選択で暗号化された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、
vii. 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、
viii. 前記第2のデータセットを復号するステップと、
ix. 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前記ハッシュであると見なされる、ステップviii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viii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viとステップvii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、
- 任意選択で前記ミキサ数を復号するステップと、
- 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任意選択で復号された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vにおける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viiiにおける前記復号が対称鍵を使用して行われる、請求項1または2に記載の方法。
【請求項４】
ステップvにおける前記暗号化が対称鍵を使用して行われる場合、ステップviiiにおける前記復号が使い捨て鍵を使用して行われる、請求項1または2に記載の方法。
【請求項５】
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６】
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のデータセットの前記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
を含む方法。
【請求項７】
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6に記載の方法。
【請求項８】
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、
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、
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９】
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、
- 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8に記載の方法。
【請求項１０】
前記混合関数(105; 405)がXOR論理関数である、請求項1から9のいずれか一項に記載の方法。
【請求項１１】
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9のいずれか一項に記載の方法。
【請求項１２】
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9のいずれか一項に記載の方法。
【請求項１３】
前記ミキサ数がランダムに生成される、請求項1から12のいずれか一項に記載の方法。
【請求項１４】
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。
【請求項１５】
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】
【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。

【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。

【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。

【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。

【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。

【先行技術文献】

【特許文献】

【００１０】

【特許文献１】中国特許出願公開第１０１５４７１８４号

【特許文献２】米国特許出願公開第２０１１/０２４６４３３号

【特許文献３】欧州特許出願公開第１４２１５４８号

【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】

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。
【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を知ることは、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。
【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。
【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。
【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、
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】
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。
【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。
【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、
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。
【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】
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ず、このチャ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。

【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。

【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つのデバイスの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。

【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。
【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にチャネル１０９を介して送信する。
【００９２】
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】
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つのデバイスの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。

【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、そのままで秘密にされている数と、そのままで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】
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。
【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。
【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。
【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。
【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。
【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。
【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。
【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。
【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。

【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。

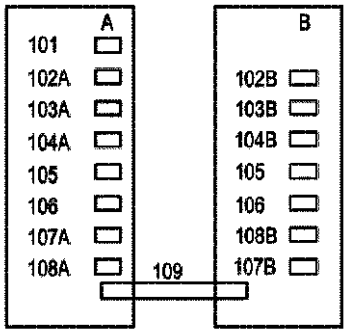
【０１７３】
この第1のデバイスAは、公開鍵1201uおよび秘密鍵1201pから成る非対称鍵のペア1201cにアクセスできる。
【０１７４】
第2の電子デバイスBは、電子メール1200が送信、受信、アーカイブ、編集、および表示されることを可能にする。
【０１７５】
この第2のデバイスBは、公開鍵1202uおよび秘密鍵1202pから成る非対称鍵のペア1202cにアクセスできる。
【０１７６】
サーバ1203は、受信された電子メールの整合性および本発明によるランダムハッシュ化方法に関連付けられた乱数の機密性を維持することが認定された、AおよびBなどの電子デバイスの識別番号および公開鍵を収集する。
【０１７７】
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。
【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。
【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。
【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信し得る。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信する。
【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。
【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
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
409　伝送チャネル
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
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
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
1205　宛先アドレス

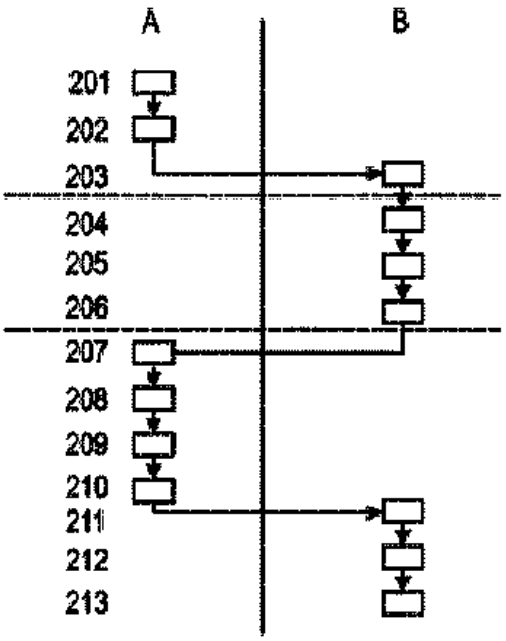
【図面】
【図１】

[Fig. 1]



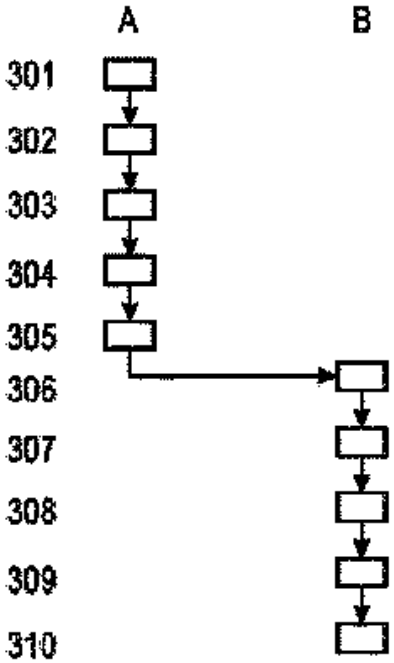
【図２】

[Fig. 2]

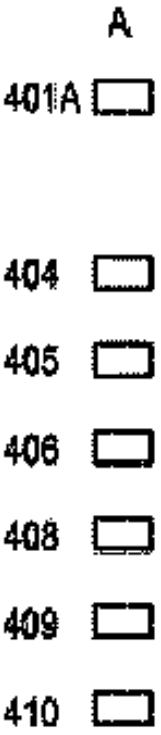


【図３】

[Fig. 3]



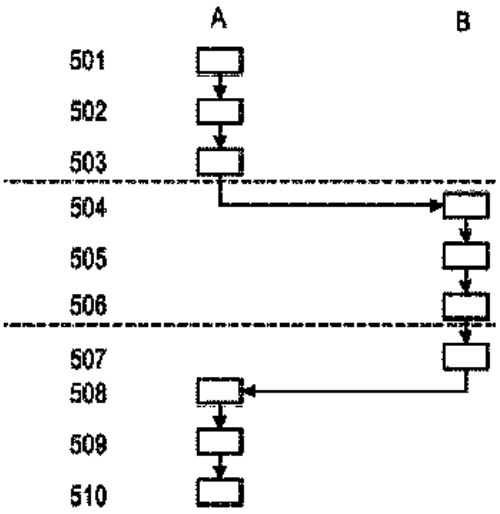
【図４Ａ】



【図４Ｂ】

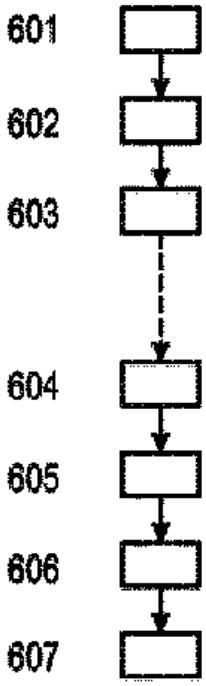
【図５】

[Fig. 5]

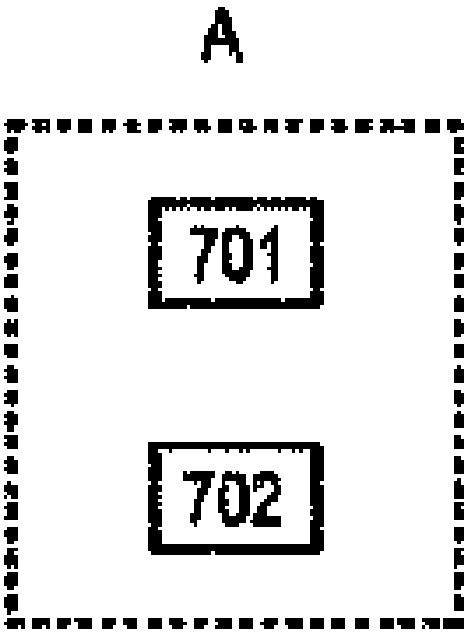


【図６】

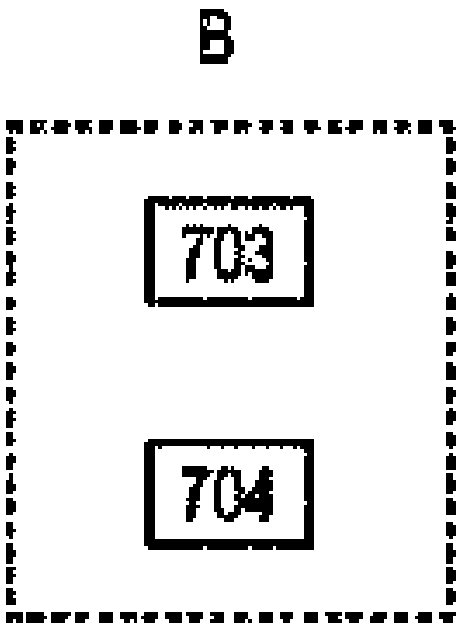
[Fig. 6]



【図７Ａ】

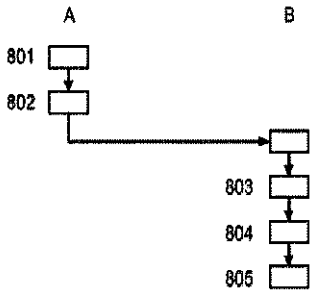


【図７Ｂ】



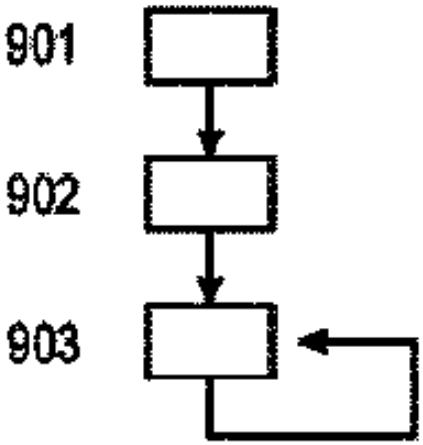
【図８】

[Fig. 8]



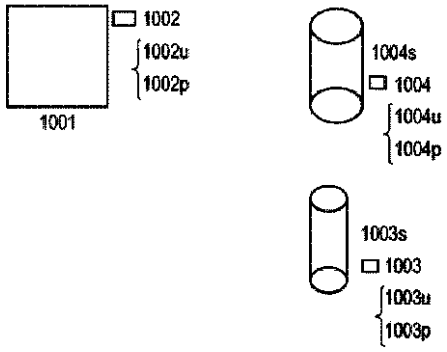
【図９】

[Fig. 9]



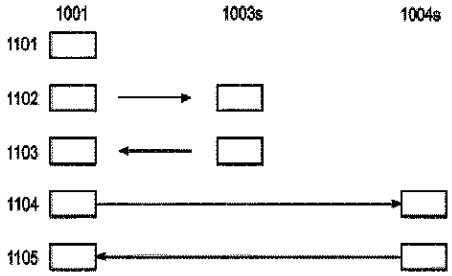
【図１０】

[Fig. 10]



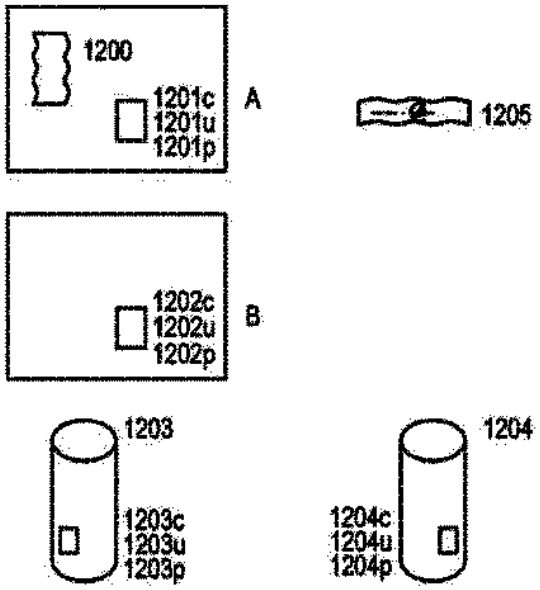
【図１１】

[Fig. 11]



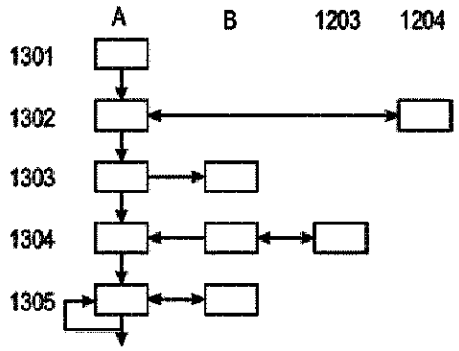
【図１２】

[Fig. 12]



【図１３】

[Fig. 13]



【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No.
PCT/EP2020/054126

A. CLASSIFICATION OF SUBJECT MATTER

G06F 21/44(2013.01)i; ***G06F 21/64***(2013.01)i; ***H04L 9/06***(2006.01)i; ***H04L 9/08***(2006.01)i; ***H04L 9/32***(2006.01)i; ***H04L 29/06***(2006.01)i

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)

G06F; 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 practicable, search terms used)

EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EP 1421548 A1 (ANOTO AB [SE]) 26 May 2004 (2004-05-26) paragraph [0028] - paragraph [0034]; figures 2,3	1-15
A	US 2012057702 A1 (MINEMATSU KAZUHIKO [JP]) 08 March 2012 (2012-03-08) paragraph [0103] - paragraph [0120]; figures 6,7	1-15
A	US 2018324152 A1 (JARCHAFJIAN HAROUT [US] ET AL) 08 November 2018 (2018-11-08) paragraph [0020] - paragraph [0052]; figures 4,5	1-15

☐ Further documents are listed in the continuation of Box C. ☑ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
15 April 2020	**21 April 2020**
Name and mailing address of the ISA/EP **European Patent Office** **p.b. 5818, Patentlaan 2, 2280 HV Rijswijk** **Netherlands** Telephone No. **(+31-70)340-2040** Facsimile No. **(+31-70)340-3016**	Authorized officer **Jardak, Christine** Telephone No.

Form PCT/ISA/210 (second sheet) (January 2015)

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/EP2020/054126

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
EP 1421548 A1	26 May 2004	AT 446543 T	15 November 2009
		EP 1421548 A1	26 May 2004
		WO 03007228 A1	23 January 2003
US 2012057702 A1	08 March 2012	JP 5447510 B2	19 March 2014
		JP WO2010131563 A1	01 November 2012
		US 2012057702 A1	08 March 2012
		WO 2010131563 A1	18 November 2010
US 2018324152 A1	08 November 2018	NONE	

Form PCT/ISA/210 (patent family annex) (January 2015)

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale n°
PCT/EP2020/054126

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
INV. G06F21/44 G06F21/64 H04L9/06 H04L9/08 H04L9/32
H04L29/06
ADD.
Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)
G06F H04L

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si cela est réalisable, termes de recherche utilisés)
EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie*	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
X	EP 1 421 548 A1 (ANOTO AB [SE]) 26 mai 2004 (2004-05-26) alinéa [0028] - alinéa [0034]; figures 2,3	1-15
A	US 2012/057702 A1 (MINEMATSU KAZUHIKO [JP]) 8 mars 2012 (2012-03-08) alinéa [0103] - alinéa [0120]; figures 6,7	1-15
A	US 2018/324152 A1 (JARCHAFJIAN HAROUT [US] ET AL) 8 novembre 2018 (2018-11-08) alinéa [0020] - alinéa [0052]; figures 4,5	1-15

☐ Voir la suite du cadre C pour la fin de la liste des documents

☒ Les documents de familles de brevets sont indiqués en annexe

* Catégories spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent
"E" document antérieur, mais publié à la date de dépôt international ou après cette date
"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)
"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens
"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée
"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention
"X" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément
"Y" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier
"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée	Date d'expédition du présent rapport de recherche internationale
15 avril 2020	21/04/2020

Nom et adresse postale de l'administration chargée de la recherche internationale	Fonctionnaire autorisé
Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Jardak, Christine

Formulaire PCT/ISA/210 (deuxième feuille) (avril 2005)

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Demande internationale n°
PCT/EP2020/054126

Document brevet cité au rapport de recherche		Date de publication	Membre(s) de la famille de brevet(s)		Date de publication
EP 1421548	A1	26-05-2004	AT	446543 T	15-11-2009
			EP	1421548 A1	26-05-2004
			WO	03007228 A1	23-01-2003
US 2012057702	A1	08-03-2012	JP	5447510 B2	19-03-2014
			JP	WO2010131563 A1	01-11-2012
			US	2012057702 A1	08-03-2012
			WO	2010131563 A1	18-11-2010
US 2018324152	A1	08-11-2018	AUCUN		

Formulaire PCT/ISA/210 (annexe familles de brevets) (avril 2005)

フロントページの続き

MK,MT,NL,NO,PL,PT,RO,RS,SE,SI,SK,SM,TR),OA(BF,BJ,CF,CG,CI,CM,GA,GN,GQ,GW,KM,ML,MR,NE,SN,TD,TG),AE,AG,AL,AM,AO,AT,AU,AZ,BA,BB,BG,BH,BN,BR,BW,BY,BZ,CA,CH,CL,CN,CO,CR,CU,CZ,DE,DJ,DK,DM,DO,DZ,EC,EE,EG,ES,FI,GB,GD,GE,GH,GM,GT,HN,HR,HU,ID,IL,IN,IR,IS,JO,JP,KE,KG,KH,KN,KP,KR,KW,KZ,LA,LC,LK,LR,LS,LU,LY,MA,MD,ME,MG,MK,MN,MW,MX,MY,MZ,NA,NG,NI,NO,NZ,OM,PA,PE,PG,PH,PL,PT,QA,RO,RS,RU,RW,SA,SC,SD,SE,SG,SK,SL,ST,SV,SY,TH,TJ,TM,TN,TR,TT,TZ,UA,UG,US,UZ,VC,VN,WS,ZA,ZM,ZW

（特許庁注：以下のものは登録商標）

１．ＢＬＵＥＴＯＯＴＨ