(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété Intellectuelle
Bureau international

(43) Date de la publication internationale
27 août 2020 (27.08.2020)

WIPO | PCT

(10) Numéro de publication internationale
WO 2020/169542 A1

(51) Classification internationale des brevets :
G06F 21/44 (2013.01) *H04L 9/08* (2006.01)
G06F 21/64 (2013.01) *H04L 9/32* (2006.01)
H04L 9/06 (2006.01) *H04L 29/06* (2006.01)

(21) Numéro de la demande internationale :
PCT/EP2020/054126

(22) Date de dépôt international :
17 février 2020 (17.02.2020)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
FR1901648 19 février 2019 (19.02.2019) FR

(72) Inventeur; et

(71) Déposant : **SANGLE-FERRIERE, Bruno** [FR/FR] ; 47 Boulevard Beauséjour, 75016 Paris (FR).

(74) Mandataire : **CABINET NONY** ; **11** rue Saint-Georges, 75009 PARIS (FR).

(81) États désignés *(sauf indication contraire, pour tout titre de protection nationale disponible)* : 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.

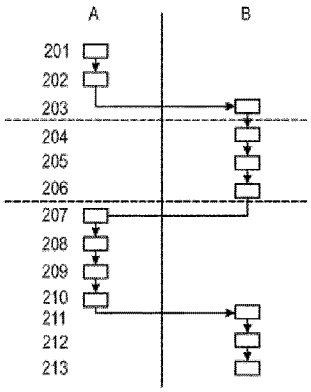
(84) États désignés *(sauf indication contraire, pour tout titre de protection régionale disponible)* : ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), eurasien (AM, AZ, BY, KG, KZ, RU, TJ, TM), européen (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Publiée:
— *avec rapport de recherche internationale (Art. 21(3))*

(54) **Title:** CRYPTOGRAPHIC DATA VERIFICATION METHOD

(54) **Titre** : MÉTHODE CRYPTOGRAPHIQUE DE VÉRIFICATION DES DONNÉES

[Fig. 2]



(57) Abstract: The invention relates to a comparison method implemented by at least one apparatus (A; B), between a first and a second dataset, in particular with a view to determining whether these two datasets are identical, this method not requiring the presence of these two datasets on the apparatus, and comprising the following steps: a) mixing a number, referred to as the mixing number, with the first dataset, using a mixing function (105; 405), in order to obtain mixed data, b) hashing the mixed data using a hash function (106); 406), and c) comparing the hash thus obtained in step b) with a third dataset assumed to be the hash of the second dataset mixed with the same mixing number as that used in step a) and with the same mixing function (105; 405).

(57) **Abrégé** : Procédé de comparaison mis en œuvre par au moins un appareil (A; B), entre un premier et deuxième ensemble de données, en vue notamment de déterminer si ces deux ensembles de données sont identiques, ce procédé ne nécessitant pas la présence de ces deux ensembles de données sur l'appareil, et comportant les étapes suivantes: a) le mélange d'un nombre, dit nombre de mélange, au premier ensemble de données, à l'aide d'une fonction de mélange (105; 405), pour obtenir des données mélangées, b) le hachage des données mélangées à l'aide d'une fonction de hachage (106; 406), et c) la comparaison du haché ainsi obtenu à l'étape b) avec un troisième ensemble de données supposé être le haché du deuxième ensemble de données mélangé au même nombre de mélange que celui utilisé à l'étape a) et avec la même fonction de mélange (105; 405).

WO 2020/169542 A1

Description

Titre : Méthode cryptographique de vérification des données

Domaine technique

La présente invention concerne la cryptographie numérique et la sécurité des dispositifs informatiques et électroniques, en particulier les signatures numériques.

Technique antérieure

Les ordinateurs et les appareils électroniques sont souvent connectés sur un réseau, physiquement, sans fil, par RFID, ou par tout autre moyen sécurisé ou non, et ont parfois besoin de connaître l'identité de l'appareil qui leur a envoyé certaines données, par exemple pour s'assurer que ces données ne sont pas transmises par un autre appareil, qui les aurait interceptées et modifiées avant de les renvoyer au destinataire légitime, ou tout simplement pour identifier sans aucun doute l'identité de l'expéditeur des données, qui est par exemple une voiture sur un réseau routier ou une étiquette RFID portée par un concurrent lors d'un événement sportif, ou pour toute autre raison pour laquelle l'identité de l'expéditeur des données est importante pour le destinataire.

Les données transmises peuvent être envoyées entièrement chiffrées avec une clé attribuée à l'expéditeur. Cependant, le cryptage de l'intégralité des données rend difficile l'utilisation des clés à usage unique, appelées *« One Time Pads »* en anglais. En effet, le cryptage de l'intégralité des données est une méthode qui utilise des clés aussi longues que les données qu'elles cryptent, et ces clés doivent être renouvelées après utilisation.

Il est donc nécessaire que les ordinateurs ou autres dispositifs électroniques entrant en communication, par exemple par l'échange de textes, d'identifiants, de numéros, de programmes informatiques, d'images ou de codes vidéo ou audio, vérifient l'identité du dispositif d'envoi en utilisant le cryptage d'une quantité de données inférieure à la quantité de données envoyées. C'est pour cela qu'on utilise une signature électronique consistant à chiffrer un haché des données. On appelle « haché » le résultat d'une fonction de hachage qui, à partir d'une donnée initiale fournie en entrée, calcule une empreinte servant à identifier rapidement, bien qu'incomplètement, la donnée initiale. Il est courant d'envoyer avec les données un haché chiffré, qui sera ensuite déchiffré par le destinataire, puis comparé au haché des données reçues. MD5, SHA1 et SHA256 sont des algorithmes classiquement utilisés pour de tels hachages. Toutefois, les hachés de données sont de taille généralement beaucoup plus petite que celle des données d'origine, et il peut être possible

de créer d'autres données similaires, mais légèrement différentes des données d'origine, ayant un haché égal au haché des données d'origine. Ces données pourraient donc être substituées aux données d'origine, sans être rejetées par la procédure de vérification du haché. La substitution peut être effectuée sur tout type de données, mais est d'autant moins détectable par l'utilisateur que les données sont complexes, comme un texte long, un fichier audio, une photo ou une vidéo. Pour effectuer la substitution, il ne serait même pas nécessaire de décrypter le haché crypté. Un simple calcul du haché des données d'origine suffirait. En outre, les fonctions de hachage telles que MD5 et SHA1 sont des fonctions de hachage actuellement relativement faciles à contourner.

Les ordinateurs quantiques en cours de développement devraient bientôt être capables de contourner la sécurité offerte par les fonctions de hachage, étant capables d'optimiser des fichiers de départ pour qu'ils aient un haché prédéterminé.

Des méthodes d'amélioration de la sécurité des systèmes utilisant des techniques de hachage sont connues de l'art antérieur.

La demande CN101547184 utilise plusieurs valeurs d'authentification auxiliaires échangées entre un serveur et des utilisateurs.

Dans la méthode proposée par la demande US201 1/0246433, un haché des données à envoyer est généré et concaténé avec le bloc de données à envoyer et l'étiquette d'un nombre aléatoire.

La demande EP 1 421 548 décrit une méthode de transmission d'informations dans laquelle un message à envoyer est concaténé avec un nombre aléatoire puis haché. Le résultat du hachage est envoyé non crypté à l'autre partie. Le message est parfois transmis tel quel ou crypté. Le nombre aléatoire est toujours transmis signé, et éventuellement crypté, à l'autre partie. Le fait de ne pas crypter le haché quand le message n'est lui-même pas crypté rend la transmission vulnérable aux ordinateurs très puissants ou quantiques qui peuvent calculer des nombres aléatoires compatibles avec le message non crypté et le résultat du hachage. Par ailleurs, le cryptage du message entier a l'inconvénient, si un tel cryptage utilise des clés à usage unique réputées inviolables, de nécessiter la présence chez les deux parties en correspondance de telles clés partagées.

Exposé de l'invention

Il existe un besoin pour perfectionner encore la sécurité des techniques de hachage, réduisant la probabilité d'erreur dans la vérification des données, et le cas échéant, permettant une authentification plus sûre de l'expéditeur de ces données.

L'invention vise notamment à y répondre, et elle y parvient grâce à un procédé de comparaison, mis en œuvre par au moins un appareil, d'un premier et deuxième ensemble de données, en vue notamment de déterminer si ces deux ensembles de données sont identiques, comportant les étapes suivantes :

a) le mélange d'un nombre, dit nombre de mélange, au premier ensemble de données, à l'aide d'une fonction de mélange, pour obtenir des données mélangées,

b) le hachage des données mélangées à l'aide d'une fonction de hachage, et

c) la comparaison du haché ainsi obtenu à l'étape b) avec un troisième ensemble de données supposé être le haché du deuxième ensemble de données mélangé au même nombre de mélange que celui utilisé à l'étape a) et avec la même fonction de mélange.

Grâce à l'invention, notamment au mélange du premier ensemble de données avec un nombre de mélange préalablement au hachage, il devient très improbable de pouvoir créer des données similaires à ce premier ensemble de données qui, après avoir été mélangées au même nombre de mélange, auront le même haché que le premier ensemble de données mélangé.

De préférence, le procédé selon l'invention ne nécessite pas la présence simultanée des deux ensembles de données sur l'appareil.

De préférence, le nombre de mélange est généré aléatoirement.

Le nombre de mélange est préférentiellement généré par l'appareil. En variante, la génération du nombre de mélange est effectuée par un autre appareil de confiance.

La génération du nombre de mélange peut reposer sur un couple de valeurs d'entrée qui sont des grandeurs physiques dont l'une au moins varie continuellement, comme par exemple la température et l'heure, ou sur un phénomène quantique. Par exemple, le choix d'un photon de traverser une plaque par une ou l'autre de deux fentes d'Young constitue la base d'une telle génération.

De préférence, l'opération de mélange à l'étape a) est effectuée par l'appareil. En variante, le mélange est effectué par un autre appareil de confiance.

La fonction de mélange combine le premier ensemble de données et le nombre de mélange. Elle est, de préférence, une fonction logique de type XOR, additionnant les bits du premier ensemble de données et ceux du nombre de mélange, un par un. La taille du nombre de mélange étant généralement inférieure à la taille du premier ensemble de données, il est possible d'additionner par un XOR les bits du nombre de mélange aux premiers ou aux derniers bits du premier ensemble de données.

Le nombre de mélange peut avoir la même taille que le premier ensemble de données. Dans ce cas, l'addition par la fonction XOR s'opère sur tous les bits, un par un.

Alternativement, la fonction de mélange consiste à ajouter le nombre de mélange à la fin du premier ensemble de données.

La fonction de mélange peut encore être une fonction de cryptage utilisant le nombre de mélange comme clé de chiffrement du premier ensemble de données.

De préférence, le hachage des données à l'étape b) est effectué par l'appareil. En variante, le hachage est effectué par un autre appareil de confiance.

De préférence, la fonction de hachage est choisie parmi SHA1, SHA2, SHA256 et MD5 et la fonction de Jenkins.

Une première variante du procédé selon l'invention est un procédé pour la vérification par l'appareil de l'intégrité d'un message provenant d'un émetteur, le procédé comportant:

i. la réception par l'appareil du message constituant le premier ensemble de données et d'un identifiant du message,
ii. la génération du nombre de mélange,
iii. la mise en œuvre des étapes a) et b) où le message est mélangé au nombre de mélange puis haché,
iv. le cryptage éventuel du nombre de mélange,
v. l'envoi par l'appareil de l'identifiant du message et du nombre de mélange éventuellement crypté à l'émetteur du message,
vi. la réception par l'appareil du troisième ensemble de données crypté, avec préférentiellement l'identifiant du message, en provenance de l'émetteur,
vii. le décryptage du troisième ensemble de données, et

viii. la mise en œuvre de l'étape c), l'intégrité du message étant assurée si le troisième ensemble de données décrypté à l'étape vii et le haché obtenu à l'étape b) sont identiques.

Par « intégrité » du message, il faut entendre sa non altération, par exemple par un tiers malveillant qui l'aurait intercepté au cours de sa transmission.

L'identifiant du message peut être une suite de caractères alphanumériques et/ou de signes pouvant être convertie en un mot numérique par le biais d'un code ASCII ou autre.

L'identifiant du message peut comporter l'identifiant de l'émetteur et un numéro d'ordre du message.

L'authentification de l'émetteur est notamment assurée par l'opération de décryptage à l'étape vii.

Cette première variante de l'invention permet à la fois de s'assurer de l'intégrité du message reçu et de l'identité de l'émetteur du message.

Les étapes relatives à l'envoi et à la réception des données peuvent être réalisées selon le même protocole de communication, ou selon des protocoles de communication différents. Par exemple, la réception à l'étape i se fait par WiFi, l'envoi à l'étape v se fait par 4G et la réception à l'étape vi se fait par WiMAX.

A l'étape i, l'appareil peut également recevoir un identifiant de l'émetteur. Cet identifiant est utile si l'appareil peut recevoir des messages de différents émetteurs, un tel identifiant lui permettant de choisir les clés de cryptage à utiliser pour crypter ou décrypter les informations échangées avec l'émetteur lors des opérations de cryptage et décryptage décrites dans cette première variante de l'invention.

De préférence, le procédé selon cette première variante comporte entre les étapes v et vi :

- la réception par l'émetteur de l'identifiant du message et du nombre de mélange éventuellement crypté,
- le décryptage éventuel du nombre de mélange,
- l'identification, à l'aide de l'identifiant du message, du message envoyé à l'appareil,
- le mélange du message au nombre de mélange éventuellement décrypté à l'aide de la fonction de mélange,
- le hachage des données résultant de l'étape précédente à l'aide de la fonction de hachage,

- le cryptage du haché résultant de l'étape précédente, et
- l'envoi à l'appareil du haché crypté avec de préférence l'identifiant du message.

Le cryptage éventuel du nombre de mélange à l'étape iv est préférentiellement effectué par l'appareil.

Le cryptage éventuel du nombre de mélange permet d'éviter que ce nombre ne soit intercepté et altéré par un tiers malveillant.

De préférence, le cryptage éventuel du nombre de mélange s'effectue à l'aide d'une clé à usage unique d'une taille au moins égale à celle du nombre. La clé étant à usage unique, une nouvelle clé est utilisée à chaque envoi d'un nombre de mélange.

Le cryptage peut aussi être effectué à l'aide d'une clé symétrique. La clé de cryptage symétrique est gardée secrète entre l'émetteur et l'appareil, et est de préférence renouvelée après un certain nombre de transmissions.

Alternativement, le cryptage éventuel du nombre de mélange est asymétrique, s'effectuant, soit à l'aide d'une clé publique de l'émetteur connue de l'appareil, de sorte à permettre le décryptage par l'émetteur en utilisant sa clé privée associée, soit à l'aide d'une clé privée de l'appareil dont l'émetteur connaît la clé publique.

Ainsi, un tiers est empêché de connaître ou d'altérer le nombre de mélange.

De préférence, le décryptage à l'étape vii est effectué par l'appareil.

De préférence, le décryptage à l'étape vii s'effectue à l'aide d'une clé symétrique, si le cryptage à l'étape iv est fait par une clé à usage unique.

Alternativement, le décryptage à l'étape vii s'effectue à l'aide d'une clé à usage unique, si le cryptage à l'étape iv est fait par une clé symétrique.

Le décryptage à l'étape vii peut aussi être effectué par d'autres méthodes, par exemple à l'aide d'une clé publique connue de l'appareil, associée à une clé privée de l'émetteur ayant servi au cryptage du haché reçu à l'étape vi. Ainsi, l'appareil est capable de certifier l'identité de l'émetteur.

Le nombre de mélange peut avoir la même taille que la clé symétrique qui sert à le crypter, si une telle clé symétrique est utilisée, et aussi la même taille que le haché.

De préférence, les clés de cryptage privées, symétriques et à usage unique ainsi que les nombres de mélange sont indevinables et inobservables par des dispositifs tiers, pour éviter que l'écoute des données émises par l'émetteur ou l'appareil ne rende possible la

génération et la transmission de deuxièmes ensembles de données, frauduleux, qui engendreraient à tort une reconnaissance d'intégrité de messages reçus par l'appareil mais transmis par un émetteur autre que celui censé porter légitimement lesdites clés.

Si la clé de cryptage X du nombre de mélange x est connue, alors le haché du message mélangé peut être connu, car il suffit de décrypter le crypté de x et de calculer le mélangé du message avant de le hacher. La clé Y cryptant le haché peut être alors aussi devinée ou être connue pour appartenir à un univers restreint, le haché du message mélangé et son cryptage par Y étant tous deux connus ou observables. La clé de cryptage Y est donc une fonction F de la clé de cryptage X, ou bien la clé de cryptage Y appartient à un univers dépendant de la clé de cryptage X. L'observation de plusieurs transmissions fait apparaître plusieurs fonctions F, et les valeurs des clés X et Y sont à l'intersection de ces fonctions. Il est préférable d'éviter cette situation. Il est donc recommandé soit d'utiliser pour la clé X ou la clé Y des valeurs changeantes au fil des transmissions, soit d'utiliser des fonctions de cryptage telles que pour chaque observation d'échanges du triplet « message, nombre crypté, haché crypté», l'univers des clés Y pour chaque X possible est grand ; ceci rendant grand l'univers résultant de l'intersection de ces univers déductibles à chaque observation. Il n'est pas recommandé de prendre pour clé Y le nombre de mélange x généré aléatoirement. En effet, si on se sert du nombre de mélange x comme clé de chiffrage Y, ou bien si on calcule la clé Y en fonction du nombre de mélange x par une formule déterminée, connaissant la valeur cryptée C du nombre de mélange x par la clé X, le nombre de mélange x, et donc Y deviennent une autre fonction G de la clé X ; et les clés X et Y seraient à l'intersection de la fonction F et de cette nouvelle fonction G. De préférence, la clé X ou la clé Y est renouvelée après chaque échange.

L'appareil peut en outre comporter un compteur de tentatives de vérifications négatives consécutives déclenchant un blocage de celui-ci lorsqu'un nombre déterminé est atteint, le déblocage pouvant être effectué lors du renouvellement de la clé de cryptage du nombre de mélange ou de la clé de cryptage du haché.

Une deuxième variante du procédé selon l'invention est un procédé pour la vérification par l'appareil de l'intégrité d'un message provenant d'un émetteur, le procédé comportant :

i. la réception par l'appareil du message, du troisième ensemble de données crypté et du nombre de mélange crypté,

ii. le décryptage du nombre de mélange et du troisième ensemble de données, et

iii. la mise en œuvre des étapes a) à c), l'intégrité du message étant assurée si le haché obtenu à l'étape b) et le troisième ensemble de données décrypté à l'étape ii sont identiques.

De préférence, le procédé selon cette deuxième variante de l'invention comporte avant l'étape i :

- la génération par l'émetteur du nombre de mélange,
- le mélange du nombre de mélange au message, à l'aide de la fonction de mélange,
- le hachage des données résultant de l'étape précédente à l'aide de la fonction de hachage,
- le cryptage du haché résultant de l'étape précédente et constituant le troisième ensemble de données,
- le cryptage du nombre de mélange, et
- l'envoi à l'appareil du message, du troisième ensemble de données crypté et du nombre de mélange crypté.

Ces étapes sont effectuées par l'émetteur authentique et permettent de détecter l'altération du message par un tiers non autorisé.

Le décryptage à l'étape ii du nombre de mélange et du troisième ensemble de données est préférentiellement effectué par l'appareil.

De façon préférentielle, le cryptage du nombre de mélange s'effectue à l'aide d'une clé à usage unique, et le cryptage du troisième ensemble de données s'effectue à l'aide d'une clé symétrique, la clé symétrique étant de préférence renouvelée occasionnellement.

Alternativement, le cryptage du nombre de mélange s'effectue à l'aide d'une clé symétrique, et le cryptage du troisième ensemble de données s'effectue à l'aide d'une clé à usage unique, la clé symétrique étant de préférence renouvelée occasionnellement.

Le cryptage du nombre de mélange et le cryptage du troisième ensemble de données peuvent aussi être de même type, ou de types différents, ces types de cryptage pouvant être par clés symétriques, ou par clés asymétriques.

Si une paire de clés asymétriques est utilisée pour le cryptage du nombre de mélange, celle-ci a de préférence sa clé privée détenue par l'appareil, la clé publique correspondante étant alors connue de l'émetteur.

Le cryptage du troisième ensemble de données est, de préférence, effectué à l'aide d'une clé privée détenue par l'émetteur, la clé publique correspondante étant alors connue de l'appareil.

Ainsi, par le décryptage du nombre de mélange et du troisième ensemble de données, l'appareil est capable de certifier l'identité de l'émetteur.

Le cryptage du nombre de mélange et celui du troisième ensemble de données peuvent être effectués par le biais de la même fonction de cryptage, notamment lorsque le cryptage du nombre de mélange est asymétrique.

Alternativement, le cryptage du nombre de mélange et celui du troisième ensemble de données sont effectués par le biais de deux fonctions de cryptage différentes.

De préférence, les types de fonctions de cryptage à utiliser font partie de la configuration de l'émetteur et de l'appareil, préalablement à l'établissement de la communication entre ces deux derniers.

Une troisième variante du procédé selon l'invention est un procédé dans lequel le premier ensemble de données est présent sur l'appareil et le deuxième ensemble de données est présent sur un deuxième appareil, le procédé comportant :

i. la mise en œuvre des étapes a) et b),
ii. le cryptage du nombre de mélange,
iii. l'envoi par l'appareil au deuxième appareil du nombre de mélange crypté,
iv. la réception par l'appareil d'un haché crypté du deuxième ensemble de données,
v. le décryptage du haché crypté, et
vi. la mise en œuvre de l'étape c).

De préférence, le procédé selon cette troisième variante de l'invention comporte entre les étapes iii et iv :

- la réception par le deuxième appareil du nombre de mélange crypté,
- le décryptage du nombre de mélange,

- la création d'une copie modifiée du deuxième ensemble de données à l'aide du nombre de mélange et de la fonction de mélange,
- le hachage de la copie modifiée du deuxième ensemble de données à l'aide de la fonction de hachage,
- le cryptage du haché résultant de l'étape précédente et constituant le troisième ensemble de données, et
- l'envoi par le deuxième appareil à l'appareil du haché crypté du deuxième ensemble de données.

Le cryptage du nombre de mélange à l'étape ii et le décryptage du haché crypté à l'étape v sont préférentiellement effectués par l'appareil.

De préférence, le cryptage du nombre de mélange s'effectue à l'aide d'une clé de cryptage symétrique partagée avec le deuxième appareil.

De préférence, le cryptage du haché s'effectue à l'aide d'une clé à usage unique et le cryptage du nombre de mélange s'effectue à l'aide d'une clé symétrique renouvelée occasionnellement.

Alternativement, le cryptage du nombre de mélange s'effectue à l'aide d'une clé à usage unique et le cryptage du haché s'effectue à l'aide d'une clé symétrique renouvelée occasionnellement.

Le cryptage du nombre de mélange et le cryptage du haché peuvent aussi être de même type, ou de types différents, ces types de cryptage pouvant être par clés symétriques, notamment par clés à usage unique, ou par clés asymétriques.

Une quatrième variante du procédé selon l'invention est un procédé pour la vérification qu'un ensemble de données présent sur l'appareil n'a pas été modifié entre deux dates d1 et d2, cet ensemble de données constituant à la date d1 le premier ensemble de données et à la date d2 le deuxième ensemble de données, le procédé comportant :

i. la mise en œuvre des étapes a) et b),
ii. la sauvegarde de manière sécurisée par l'appareil du nombre de mélange et du haché obtenu à l'étape b),
iii. la création d'une copie modifiée du deuxième ensemble de données à l'aide du nombre de mélange et de la fonction de mélange,
iv. le hachage de la copie modifiée à l'aide de la fonction de hachage pour former le troisième ensemble de données, et

v. la mise en œuvre de l'étape c).

Avantageusement, le procédé selon cette quatrième variante ne nécessite pas une conservation sécurisée de l'ensemble de données.

L'invention a aussi pour objet un produit programme d'ordinateur comprenant des instructions lisibles par un processeur d'un appareil pour la mise en œuvre du procédé selon l'invention, selon l'une quelconque des variantes définies ci-dessus.

Brève description des dessins

L'invention pourra être mieux comprise à la lecture de la description détaillée qui va suivre, d'exemples non limitatifs de mise en œuvre de celle-ci, et à l'examen du dessin annexé, sur lequel :

[Fig 1] la figure 1 représente schématiquement les données et fonctions nécessaires à la mise en œuvre de l'invention selon sa première ou sa deuxième variante,

[Fig 2] la figure 2 illustre schématiquement un exemple de mise en œuvre de l'invention selon sa première variante,

[Fig 3] la figure 3 représente schématiquement un exemple de mise en œuvre de l'invention selon sa deuxième variante,

[Fig 4] la figure 4 illustre schématiquement des données et fonctions utiles à la mise en œuvre de l'invention selon sa troisième variante,

[Fig 5] la figure 5 représente schématiquement un exemple de mise en œuvre de l'invention selon sa troisième variante,

[Fig 6] la figure 6 illustre un schéma de mise en œuvre de l'invention selon sa quatrième variante,

[Fig 7] la figure 7 illustre schématiquement des données utiles à la mise en œuvre de l'exemple de la figure 8,

[Fig 8] la figure 8 représente un premier exemple de mise en œuvre de l'invention appliquée à la vérification de logiciels,

[Fig 9] la figure 9 représente un deuxième exemple de mise en œuvre de l'invention appliquée à la vérification de logiciels,

[Fig 10] la figure 10 illustre schématiquement des dispositifs et données utiles à la mise en œuvre de l'exemple de la figure 11,

[Fig 11] la figure 11 illustre un exemple de mise en œuvre de l'invention appliquée à la sécurisation des navigateurs internet,

[Fig 12] la figure 12 représente schématiquement des dispositifs et données utiles à la mise en œuvre de l'exemple de la figure 13, et

[Fig 13] la figure 13 représente un exemple de mise en œuvre de l'invention appliquée à la sécurisation des courriers électroniques.

Description détaillée

La figure 1 représente schématiquement des données et fonctions utiles à la mise en œuvre de l'invention selon sa première ou sa deuxième variante, où un message 101 doit être envoyé par un dispositif A à un dispositif B via un canal de transmission de données 109, lequel peut être sécurisé ou non.

Le dispositif A peut être un ordinateur personnel ou un téléphone intelligent, et le dispositif B un serveur de courrier électronique, le message 101 étant par exemple un courrier électronique envoyé par l'ordinateur ou le téléphone via le réseau internet.

Le dispositif A peut aussi être un serveur envoyant un courrier électronique ou une page web, le dispositif B étant alors un ordinateur personnel ou un téléphone intelligent recevant ledit courrier électronique ou la page web.

Le dispositif A peut encore être un appareil de mesure, par exemple de la consommation de courant électrique, de gaz ou d'eau, ou pour mesurer l'usure d'une pièce dans une machine, le message 101 étant alors le résultat d'une telle mesure, et le dispositif B un serveur regroupant la mesure et communiquant avec l'appareil de mesure via un réseau de télécommunications, par exemple un réseau d'internet des objets, un réseau WiFi ou un réseau LTE.

Les dispositifs A et B peuvent aussi être des ordinateurs personnels ou des téléphones intelligents.

Le dispositif A peut être un navigateur web, le dispositif B un serveur web et le message 101 un formulaire rempli par l'utilisateur du navigateur A, la réception du message devant ne pas être différée par rapport à son envoi.

Les dispositifs A et B peuvent être chacun équipés d'un processeur pour l'exécution des étapes du procédé selon l'invention, et d'une mémoire pour sauvegarder les données nécessaires à cette exécution.

Le dispositif B dispose de données de chiffrement/déchiffrement 102B, telles qu'une clé privée. Le dispositif A dispose de données de chiffrement/déchiffrement 102A, telles que la clé publique associée à la clé privée 102B.

Le dispositif A dispose également de données de chiffrement/déchiffrement 103A, telles qu'une clé privée associée à une clé publique 103B présente sur le dispositif B.

Les dispositifs A et B possèdent des générateurs de nombres aléatoires 104A et 104B respectivement, une fonction de mélange commune 105 et une fonction de hachage commune 106.

Les dispositifs A et B ont également des fonctions de cryptage 107A et 107B respectivement, ainsi que des fonctions de décryptage 108A et 108B respectivement.

On a illustré à la figure 2 un exemple de mise en œuvre du procédé selon la première variante de l'invention.

A l'étape 201, un premier nombre, utilisé pour identifier le message 101, est généré par le dispositif A. Il peut être optionnellement généré à partir du générateur de nombres aléatoires 104A.

A l'étape 202, le premier nombre est ajouté au message 101. Cet ajout peut être une concaténation dans un ordre quelconque défini par le protocole de communication entre les deux dispositifs.

A l'étape 203, le dispositif A envoie les données résultant de l'étape 202 au dispositif B via le canal 109 de transmission des données.

A l'étape 204, à la réception des données, le dispositif B génère aléatoirement un deuxième nombre à partir du générateur de nombres aléatoires 104B.

A l'étape 205, le dispositif B se sert de la fonction de mélange 105 pour mélanger le deuxième nombre avec le message 101. A titre d'exemple, cette fonction de mélange est un XOR opérant entre les bits du deuxième nombre et un même nombre de bits du message 101. La fonction de mélange 105 est connue par le dispositif A.

A l'étape 206, le dispositif B utilise la fonction de hachage 106 pour hacher les données obtenues à l'étape précédente. Le dispositif B utilise également la clé de chiffrement publique 103B et la fonction de cryptage 107B, pour crypter le deuxième nombre.

A l'étape 207, le dispositif B envoie au dispositif A via le canal 109 le premier nombre ainsi que le deuxième nombre crypté.

A l'étape 208, à la réception des deux nombres, le dispositif A décrypte le deuxième nombre à l'aide de la clé de chiffrement privée 103A associée à la clé publique 103B qui devait servir au cryptage, et de la fonction de décryptage 108A associée à la fonction de

cryptage 107B. Si le deuxième nombre n'a pas été crypté par le dispositif B, son décryptage sera inexact.

Avec le premier nombre, le dispositif A peut identifier le message 101, et mélanger, à l'aide de la fonction de mélange 105, le deuxième nombre décrypté au message 101 identifié.

A l'étape 209, le dispositif A utilise la fonction de hachage 106 pour hacher les données résultantes de l'étape précédente.

A l'étape 210, le dispositif A utilise la clé de chiffrement privée 103A et la fonction de cryptage 107A, pour crypter le haché obtenu à l'étape précédente.

A l'étape 211, le dispositif A envoie le haché crypté au dispositif B via le canal 109.

A l'étape 212, à la réception du haché crypté, le dispositif B le décrypte à l'aide de la clé de chiffrement publique 103B associée à la clé privée 103A qui devait servir au cryptage, et de la fonction de décryptage 108B associée à la fonction de cryptage 107A.

A l'étape 213, le dispositif B compare le haché décrypté obtenu à l'étape 212 avec le haché calculé à l'étape 206. Si les deux hachés sont identiques, le dispositif B conclut que le message 101 n'a pas été altéré.

De préférence, le deuxième nombre servant au mélange doit être gardé secret jusqu'à ce que les hachés aient été comparés pour effectuer la vérification, mais ce nombre de mélange peut être révélé avant, si l'on peut faire confiance aux dispositifs calculant les hachés pour que les données ne soient pas modifiées entre le moment où le nombre de mélange est révélé et la comparaison des hachés.

On a illustré à la figure 3 un deuxième exemple de mise en œuvre du procédé selon la deuxième variante de l'invention, le message 101 devant être envoyé par le dispositif A au dispositif B.

Les dispositifs A et B peuvent être des ordinateurs personnels ou des téléphones intelligents, et le message 101 peut être un courrier électronique.

Les dispositifs A et B peuvent être des automobiles voisines, les données échangées étant alors des informations relatives à leurs mouvements, et la connexion s'effectuant par une liaison de données entre les deux véhicules, par exemple une liaison de type 5G, Bluetooth Low Energy, une liaison RFID ultra haute fréquence, une liaison Lora ou Sigfox.

A l'étape 301, un nombre aléatoire est généré par le dispositif A, à l'aide du générateur de nombres aléatoires 104A.

A l'étape 302, le dispositif A mélange le message 101 au nombre aléatoire à l'aide de la fonction de mélange 105.

A l'étape 303, le dispositif A procède au hachage des données mélangées résultant de l'étape précédente, à l'aide de la fonction de hachage 106.

A l'étape 304, le dispositif A crypte le haché obtenu à l'étape précédente à l'aide de la fonction de cryptage 107A et de la clé de chiffrement privée 103A.

A l'étape 305, le dispositif A crypte le nombre aléatoire à l'aide de la fonction de cryptage 107A et de la clé de chiffrement publique 102A.

A l'étape 306, le message 101, le nombre aléatoire crypté et le haché crypté sont envoyés au dispositif B via le canal de transmission 109, selon le protocole de communication établi entre les deux dispositifs.

A l'étape 307, à la réception des données, le dispositif B utilise la fonction de décryptage 108B ainsi que la clé de chiffrement publique 103B pour décrypter le haché, et la clé de chiffrement privée 102B pour décrypter le nombre aléatoire.

Le dispositif B est ainsi en mesure d'authentifier le dispositif A.

A l'étape 308, le dispositif B mélange le message 101 au nombre aléatoire, à l'aide de la fonction de mélange 105.

A l'étape 309, le dispositif B hache les données mélangées résultant de l'étape précédente, à l'aide de la fonction de hachage 106.

A l'étape 310, le dispositif B compare le haché qu'il a calculé au haché décrypté, et conclut quant à l'intégrité du message 101.

Dans cet exemple, le dispositif B peut faire suivre les données reçues du dispositif A à un troisième dispositif. Le dispositif B décrypte à l'aide de la clé privée 102B le nombre aléatoire qu'il a reçu du dispositif A avant de le crypter à nouveau à l'aide de la clé publique du troisième dispositif. Le dispositif B transmet alors au troisième dispositif le nombre aléatoire crypté ainsi que le haché crypté par le dispositif A. Le troisième dispositif, disposant de la clé publique du dispositif A, pourra vérifier que ce haché provient bien du dispositif A, dans la mesure où le dispositif B n'a pas modifié le haché crypté par le dispositif A. Un même ensemble de données peut donc être vérifié comme authentique par de nombreux utilisateurs. Cette possibilité expose cependant la sécurité de la certification, un dispositif frauduleux pouvant décrypter le nombre aléatoire, et éventuellement modifier le message pour qu'il ait le même haché aléatoire que le haché

initial. Cette mise en œuvre est donc utilisée de préférence pour certifier la communication entre systèmes informatiques formés d'éléments protégés contre une telle utilisation frauduleuse.

La figure 4 illustre schématiquement les données et fonctions nécessaires à la mise en œuvre de l'invention selon sa troisième variante, pour vérifier qu'un fichier 401A présent sur un dispositif A est identique à un fichier 401B présent sur un dispositif B.

Les dispositifs A et B communiquent via un canal de transmission 409 qui est par exemple un réseau WiFi.

Le dispositif A possède un générateur de nombres aléatoires 404.

Les dispositifs A et B disposent en commun d'une fonction de mélange 405, d'une fonction de hachage 406 et d'une clé symétrique de cryptage 410.

Le dispositif B dispose d'une fonction de cryptage 407.

Le dispositif A dispose d'une fonction de décryptage 408.

On a illustré à la figure 5 un troisième exemple de mise en œuvre du procédé selon la troisième variante de l'invention.

A l'étape 501, un nombre aléatoire est généré sur le dispositif A à l'aide du générateur de nombres aléatoires 404.

A l'étape 502, une copie modifiée du fichier 401A est créée en utilisant la fonction de mélange 405 et le nombre aléatoire.

A l'étape 503, la copie modifiée du fichier 401A est hachée à l'aide de la fonction de hachage 406.

A l'étape 504, le nombre aléatoire est crypté à l'aide d'un algorithme de cryptage symétrique et de la clé de chiffrement symétrique 410, et est envoyé au dispositif B via le canal de transmission 409.

A l'étape 505, à la réception du nombre aléatoire crypté, le dispositif B le décrypte et l'utilise dans une fonction de mélange 405 pour créer une copie modifiée du fichier 401B.

En décryptant le nombre aléatoire, le dispositif B peut vérifier l'identité du dispositif A.

A l'étape 506, la copie modifiée du fichier 401B est hachée avec la même fonction de hachage 406.

A l'étape 507, le haché de la copie modifiée est crypté à l'aide de la fonction de cryptage 407 et de la clé de chiffrement 410.

A l'étape 508, le haché crypté est envoyé au dispositif A.

A l'étape 509, à la réception du haché crypté, le dispositif A le décrypte à l'aide de la fonction de décryptage 408 et de la clé 410.

A l'étape 510, le dispositif A compare le haché décrypté à celui qu'il a calculé à l'étape 503, et ainsi est en mesure de vérifier si les deux fichiers 401A et 401B sont identiques.

On a illustré à la figure 6 un quatrième exemple de mise en œuvre du procédé selon la quatrième variante de l'invention, pour vérifier qu'un fichier n'a pas été modifié entre deux dates d1 et d2, en conservant en toute sécurité un jeu de données réduit entre les deux dates, ce jeu comprenant un nombre conservé intact et secret et un haché conservé intact et préférentiellement secret.

A l'étape 601, un nombre aléatoire est généré.

A l'étape 602, à la date dl, une copie modifiée du fichier est créée en utilisant le nombre aléatoire généré et une fonction de mélange, cette fonction consistant par exemple à ajouter le nombre aléatoire à la fin du fichier.

A l'étape 603, un haché de la copie modifiée est créé, par exemple en utilisant la fonction SHA2.

A l'étape 604, le nombre aléatoire et le haché sont conservés de manière sécurisée et secrète, afin qu'ils ne puissent pas être modifiés et que le nombre aléatoire ne soit pas divulgué à une partie tierce.

A l'étape 605, à la date d2, la personne ou le dispositif ayant accès aux informations sauvegardées à l'étape 604 souhaite comparer le fichier à la date d2 avec le fichier utilisé aux étapes 601 à 604. Pour ce faire, le nombre aléatoire sauvegardé est utilisé pour créer une deuxième copie modifiée du fichier à la date d2, en utilisant la même fonction de mélange qu'à l'étape 602.

A l'étape 606, un haché de la deuxième copie modifiée est créé en utilisant la même fonction de hachage qu'à l'étape 603.

A l'étape 607, le haché créé à l'étape précédente est comparé avec le haché sauvegardé pour s'assurer que le fichier n'a pas été modifié entre les dates d1 et d2.

On a illustré schématiquement à la figure 7 les clés nécessaires à la mise en œuvre d'un cinquième exemple, représenté à la figure 8, du procédé selon l'invention appliquée à la vérification de logiciels.

Dans la suite de la description, on appellera « hachage aléatoire » d'une donnée, l'opération de mélange de cette donnée avec un nombre de mélange aléatoire suivie de l'opération de hachage.

L'exemple représenté à la figure 8 est réalisé entre deux dispositifs : un dispositif A dit distributeur de logiciels et un dispositif B dit client.

Le dispositif A possède deux clés 701 et 702.

701 est une clé servant à chiffrer un haché, et est de préférence privée.

702 est une clé servant à chiffrer un nombre aléatoire, et est de préférence publique.

Le dispositif B possède deux clés 703 et 704.

703 est une clé servant à déchiffrer un haché crypté à l'aide de la clé 701, et est de préférence publique.

704 est une clé servant à déchiffrer un nombre aléatoire crypté à l'aide de la clé 702, et est de préférence privée.

La paire de clés (701, 703) peut être appelée paire de clés du distributeur de logiciels, ce dernier pouvant l'utiliser pour communiquer avec tous les appareils sur lesquels un des logiciels qu'il distribue est installé.

La paire de clés (704, 702) peut être appelée paire de clés du client, celui-ci pouvant l'utiliser pour tous les logiciels qu'il vérifie lors de leur chargement.

A l'étape 801, le distributeur de logiciels A procède au hachage aléatoire d'un logiciel à transmettre au client B selon les étapes 301 à 305 décrites précédemment à la figure 3.

Le distributeur de logiciels A utilise la clé 702 pour crypter le nombre aléatoire et la clé 701 pour crypter le haché aléatoire du logiciel.

A l'étape 802, le distributeur de logiciels A envoie au client B un ensemble de données contenant le logiciel, le haché crypté du logiciel et le nombre aléatoire crypté, sur une ligne de transmission sécurisée ou non.

A l'étape 803, à la réception de l'ensemble de données, le client B décrypte le haché avec la clé 703 et le nombre aléatoire avec la clé 704. Le client B se sert alors du nombre aléatoire pour procéder au hachage aléatoire du logiciel reçu.

A l'étape 804, si le haché calculé est identique au haché reçu, le client B autorise l'exécution du logiciel reçu, ou remplace la version précédente de ce logiciel par la version qu'il vient de recevoir.

A l'étape 805, pour plus de sécurité, les étapes 803 et 804 sont ré-exécutées à des intervalles de temps préprogrammés afin de vérifier l'authenticité du logiciel.

La figure 9 décrit une autre mise en œuvre possible du hachage aléatoire pour vérifier que le logiciel en cours de chargement est autorisé par un logiciel en cours d'exécution sur un appareil.

A l'étape 901, l'appareil utilise le procédé décrit à la figure 2 pour vérifier qu'un logiciel reçu provient d'une source fiable.

A l'étape 902, les étapes 601 à 604 de la figure 6 sont exécutées pour créer sur l'appareil une signature sécurisée du logiciel.

A l'étape 903, avant d'utiliser le logiciel, les étapes 605 à 607 de la figure 6 sont exécutées pour vérifier que le logiciel n'a pas été modifié depuis l'étape 902.

La figure 10 présente les objets nécessaires à la mise en œuvre de l'exemple illustré à la figure 11 permettant la sécurisation des données affichées par les navigateurs internet.

Un navigateur internet 1001 dispose d'une paire de clés asymétriques constituée d'une clé privée 1002p et d'une clé publique 1002u.

Un serveur 1003s, fournissant au navigateur les clés publiques de sites internet sécurisés 1004s, possède une paire de clés asymétriques 1003 constituée d'une clé privée 1003p et d'une clé publique 1003u.

Le site internet 1004s possède une paire de clés asymétriques 1004 constituée d'une clé privée 1004p et d'une clé publique 1004u.

A l'étape 1101, un utilisateur entre dans la barre d'adresse du navigateur 1001 l'adresse URL du site qu'il souhaite consulter.

A l'étape 1102, le navigateur 1001 utilise la paire de clés 1002 et envoie au serveur 1003s les informations suivantes :

- l'adresse URL du site que l'utilisateur souhaite consulter,
- la clé publique 1002u du navigateur, et
- l'adresse URL du navigateur 1001 pour que le serveur puisse lui répondre.

A l'étape 1103, le serveur 1003s utilise le procédé selon l'invention décrit à la figure 2 pour envoyer de façon sécurisée au navigateur la clé publique 1004u du site 1004s.

La clé publique 1002u sera utile au serveur pour le décryptage du deuxième nombre que le navigateur lui aura envoyé lors des échanges.

A l'étape 1104, le navigateur 1001 envoie au site 1004s les informations suivantes :

- le nom de la page du site que l'utilisateur souhaite consulter,
- la clé publique 1002u du navigateur, et
- l'adresse URL du navigateur pour que le site puisse lui répondre.

A l'étape 1105, le serveur 1004s utilise le procédé selon l'invention décrit à la figure 2 pour envoyer au navigateur de façon sécurisée la page demandée.

La figure 12 présente les objets nécessaires à la mise en œuvre de l'exemple illustré à la figure 13 permettant la sécurisation des courriers électroniques.

Un premier dispositif électronique A, pouvant être un ordinateur ou un téléphone intelligent, permet l'envoi, la réception, l'archivage, l'édition et l'affichage de courriers électroniques 1200 qui sont sous forme de fichiers électroniques.

Ce premier dispositif A a accès à une paire de clés asymétriques 1201c constituée d'une clé publique 1201u et d'une clé privée 1201p.

Un deuxième dispositif électronique B permet l'envoi, la réception, l'archivage, l'édition et l'affichage des courriers électroniques 1200.

Ce deuxième dispositif B a accès à une paire de clés asymétriques 1202c constituée d'une clé publique 1202u et d'une clé privée 1202p.

Un serveur 1203 regroupe les numéros d'identification et les clés publiques des dispositifs électroniques, tels que A et B, certifiés conserver l'intégrité des messages électroniques reçus et la confidentialité des nombres aléatoires associés au procédé de hachage aléatoire selon l'invention.

Le serveur 1203 a accès à une paire de clés 1203c constituée d'une clé publique 1203u et d'une clé privée 1203p. Il est à noter que ce serveur peut avoir plusieurs paires de clés, chacune dédiée à la communication avec un dispositif électronique bien déterminé.

Un serveur 1204 associe le ou les dispositifs électroniques à l'adresse 1205 destinataire du courrier électronique.

Le serveur 1204 a accès à une paire de clés 1204c constituée d'une clé publique 1204u et d'une clé privée 1204p. Il est à noter que ce serveur peut avoir plusieurs paires de clés, chacune dédiée à la communication avec un dispositif électronique bien déterminé.

A l'étape 1301, un utilisateur demande au premier dispositif A d'envoyer le courrier électronique 1200 à l'adresse destinataire 1205.

A l'étape 1302, le premier dispositif A communique avec le serveur 1204 dont il connaît la clé publique, en utilisant le procédé selon l'invention décrit à la figure 2, afin de connaître

l'identifiant et la clé publique du dispositif B associé à l'adresse 1205. Après authentification du premier dispositif A auprès du serveur 1204, ce dernier envoie au premier dispositif A l'identifiant et la clé publique du dispositif B. Cet envoi se fait aussi suivant le procédé décrit à la figure 2, le serveur 1204 connaissant la clé publique du dispositif A et ce dernier connaissant la clé publique du serveur 1204. Ce procédé permet au dispositif A de recevoir du serveur 1204 des données non modifiées. Le serveur 1204 aura lui-même pu obtenir la clé publique du dispositif B auprès du serveur 1203 et, par la même occasion, vérifié la clé publique du dispositif A.

A l'étape 1303, le premier dispositif A communique son identifiant au dispositif B.

A l'étape 1304, le dispositif B, ayant reçu l'identifiant communiqué à l'étape 1303, communique avec le serveur 1203 pour connaître la clé publique du premier dispositif A. Cette information lui est envoyée selon le procédé de la figure 2 permettant au dispositif B de recevoir une information non modifiée. Le dispositif B informe le dispositif A de la réception de cette information en lui envoyant un accusé de réception.

A l'étape 1305, à la réception de l'accusé de réception envoyé à l'étape 1304, le premier dispositif A utilise le procédé selon l'invention décrit à la figure 2 pour envoyer le courrier 1200 au dispositif B qui peut alors être certain que ces informations ont été envoyées par le dispositif A et ont été reçues non altérées. De plus, le dispositif A est certain de n'avoir certifié ces informations qu'auprès du dispositif B.

Les procédés de cryptage à clés asymétriques et à clés symétriques pouvant être vulnérables aux ordinateurs quantiques, ces procédés de cryptage peuvent être remplacés, dans les exemples décrits ci-dessus par des procédés de cryptage utilisant des clés à usage unique.

L'invention n'est pas limitée aux exemples de réalisation décrits ci-dessus, ni aux applications exemplifiées. L'invention peut être utilisée notamment pour sécuriser les transactions financières.

Revendications

1. Procédé de vérification par un appareil (B) de l'intégrité d'un message (101) provenant d'un émetteur (A), le procédé comportant:

i. la réception par l'appareil du message (101) constituant un premier ensemble de données et d'un identifiant du message,

ii. la génération d'un nombre, dit nombre de mélange,

iii. le mélange du nombre de mélange, au premier ensemble de données, à l'aide d'une fonction de mélange (105), pour obtenir des données mélangées,

iv. le hachage des données mélangées à l'aide d'une fonction de hachage (106),

v. le cryptage éventuel du nombre de mélange,

vi. l'envoi par l'appareil (B) de l'identifiant du message et du nombre de mélange éventuellement crypté à l'émetteur (A) du message,

vii. la réception par l'appareil (B) d'un deuxième ensemble de données crypté, en provenance de l'émetteur (A),

viii. le décryptage du deuxième ensemble de données, et

ix. la comparaison du haché obtenu à l'étape iv avec le deuxième ensemble de données décrypté à l'étape viii et supposé être le haché du message mélangé au même nombre de mélange que celui utilisé à l'étape iii et avec la même fonction de mélange (105), l'intégrité du message étant assurée si le deuxième ensemble de données décrypté à l'étape viii et le haché obtenu à l'étape iv sont identiques.

2. Procédé selon la revendication précédente, comportant entre les étapes vi et vii :

- la réception par l'émetteur (A) de l'identifiant du message et du nombre de mélange éventuellement crypté,
- le décryptage éventuel du nombre de mélange,
- l'identification, à l'aide de l'identifiant du message, du message (101) envoyé à l'appareil (B),
- le mélange du message au nombre de mélange éventuellement décrypté à l'aide de la fonction de mélange (105),

- le hachage des données résultant de l'étape précédente à l'aide de la fonction de hachage (106),
- le cryptage du haché résultant de l'étape précédente, et
- l'envoi à l'appareil (B) du haché crypté.

3. Procédé selon l'une des deux revendications précédentes, le décryptage à l'étape viii s'effectuant à l'aide d'une clé symétrique, si le cryptage à l'étape v est fait par une clé à usage unique.

4. Procédé selon l'une des deux revendications 1 et 2, le décryptage à l'étape viii s'effectuant à l'aide d'une clé à usage unique, si le cryptage à l'étape v est fait par une clé symétrique.

5. Procédé de vérification qu'un ensemble de données présent sur un appareil (A; B) n'a pas été modifié entre deux dates d1 et d2, cet ensemble de données constituant à la date d1 un premier ensemble de données et à la date d2 un deuxième ensemble de données, le procédé comportant :

i. le mélange d'un nombre, dit nombre de mélange, au premier ensemble de données, à l'aide d'une fonction de mélange (105), pour obtenir des données mélangées,
ii. le hachage des données mélangées à l'aide d'une fonction de hachage (106),
iii. la sauvegarde de manière sécurisée par l'appareil (A; B) du nombre de mélange et du haché obtenu à l'étape ii,
iv. la création d'une copie modifiée du deuxième ensemble de données à l'aide du nombre de mélange et de la fonction de mélange,
v. le hachage de la copie modifiée à l'aide de la fonction de hachage, et
vi. la comparaison du haché obtenu à l'étape ii avec le haché obtenu à l'étape v, l'ensemble de données n'ayant pas été modifié entre les deux dates d1 et d2 si les deux hachés sont identiques.

6. Procédé de vérification par un appareil (B) de l'intégrité d'un message (101) constituant un premier ensemble de données provenant d'un émetteur (A), le procédé comportant :

i. la réception par l'appareil (B) du message (101), d'un deuxième ensemble de données crypté et d'un nombre, dit nombre de mélange, crypté,

ii. le décryptage du nombre de mélange et du deuxième ensemble de données, et

iii. le mélange du message (101) au nombre de mélange, à l'aide d'une fonction de mélange (105), pour obtenir des données mélangées,

iv. le hachage des données mélangées à l'aide d'une fonction de hachage (106), et

v. la comparaison du haché obtenu à l'étape iv avec le deuxième ensemble de données décrypté à l'étape ii et supposé être le haché du premier ensemble de données mélangé au même nombre de mélange que celui utilisé à l'étape iii et avec la même fonction de mélange (105), l'intégrité du message étant assurée si le haché obtenu à l'étape iv et le deuxième ensemble de données décrypté à l'étape ii sont identiques.

7. Procédé selon la revendication précédente, comportant avant l'étape i :

- la génération par l'émetteur (A) du nombre de mélange,
- le mélange du nombre de mélange au message (101), à l'aide de la fonction de mélange (105),
- le hachage des données résultant de l'étape précédente à l'aide de la fonction de hachage (106),
- le cryptage du haché résultant de l'étape précédente et constituant le deuxième ensemble de données,
- le cryptage du nombre de mélange, et
- l'envoi à l'appareil (B) du message (101), du deuxième ensemble de données crypté et du nombre de mélange crypté.

8. Procédé de comparaison, mis en œuvre par un premier appareil (A) et un deuxième appareil (B), d'un premier ensemble de données (401A) présent sur le premier appareil (A) et un deuxième ensemble de données (40IB) présent sur le deuxième appareil (B), en vue notamment de déterminer si ces deux ensembles de données sont identiques, le procédé comportant :

i. le mélange par le premier appareil (A) d'un nombre, dit nombre de mélange, au premier ensemble de données (401A), à l'aide d'une fonction de mélange (405), pour obtenir des données mélangées,

ii. le hachage par le premier appareil (A) des données mélangées à l'aide d'une fonction de hachage (406),

iii. le cryptage par le premier appareil (A) du nombre de mélange,

iv. l'envoi par l'appareil (A) au deuxième appareil (B) du nombre de mélange crypté,

v. la réception par l'appareil (A) d'un haché crypté du deuxième ensemble de données (40 IB),

vi. le décryptage du haché crypté, et

vii. la comparaison du haché obtenu à l'étape ii avec le haché décrypté à l'étape vi.

9. Procédé selon la revendication précédente, comportant entre les étapes iv et v :

- la réception par le deuxième appareil (B) du nombre de mélange crypté,
- le décryptage du nombre de mélange,
- la création d'une copie modifiée du deuxième ensemble de données (40 IB) à l'aide du nombre de mélange et de la fonction de mélange (405),
- le hachage de la copie modifiée du deuxième ensemble de données à l'aide de la fonction de hachage (406),
- le cryptage du haché résultant de l'étape précédente, et
- l'envoi par le deuxième appareil (B) à l'appareil (A) du haché crypté du deuxième ensemble de données (40 IB).

10. Procédé selon l'une quelconque des revendications précédentes, la fonction de mélange (105 ; 405) étant une fonction logique de type XOR.

11. Procédé selon l'une quelconque des revendications 1 à 9, la fonction de mélange (105 ; 405) consistant à ajouter le nombre de mélange à la fin du premier ensemble de données.

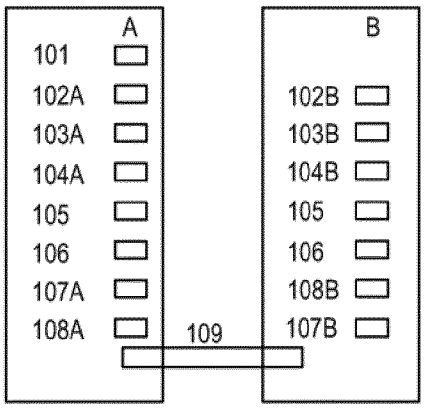
12. Procédé selon l'une quelconque des revendications 1 à 9, la fonction de mélange (105 ; 405) étant une fonction de cryptage utilisant le nombre de mélange comme clé de chiffrement du premier ensemble de données.

13. Procédé selon l'une quelconque des revendications précédentes, le nombre de mélange étant généré aléatoirement.

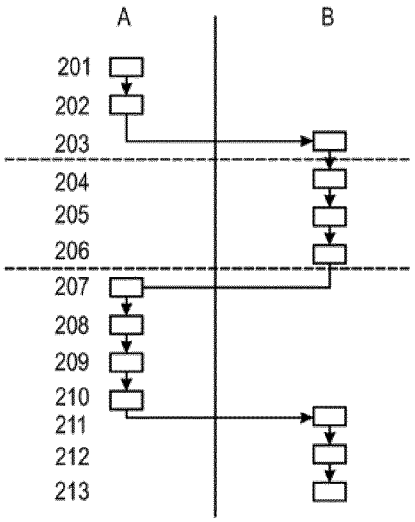
14. Procédé selon l'une quelconque des revendications précédentes, la fonction de hachage (106 ; 406) étant choisie parmi SHA1, SHA2, SHA256, MD5 et la fonction de Jenkins.

15. Produit programme d’ordinateur comprenant des instructions lisibles par le processeur d’un appareil pour la mise en œuvre du procédé selon l’une quelconque des revendications précédentes.

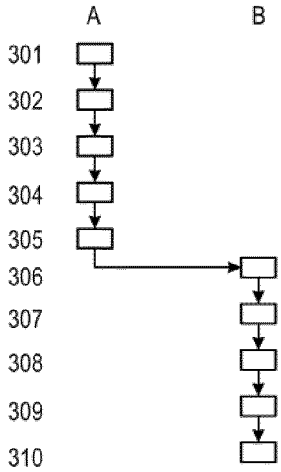
[Fig. 1]



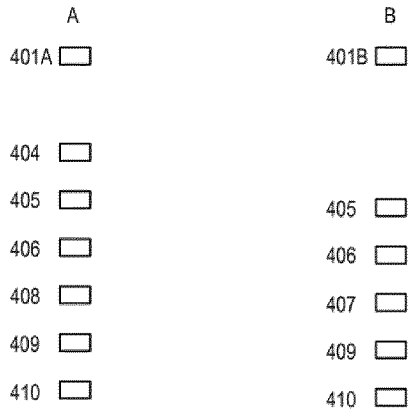
[Fig. 2]



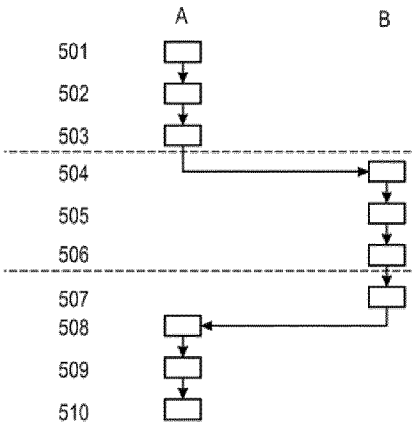
[Fig. 3]



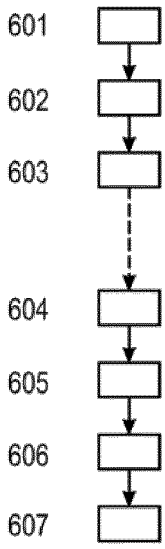
[Fig. 4]



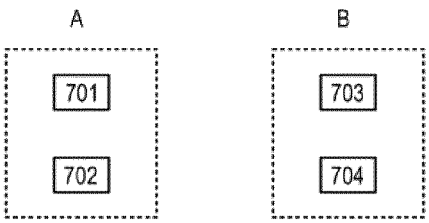
[Fig. 5]



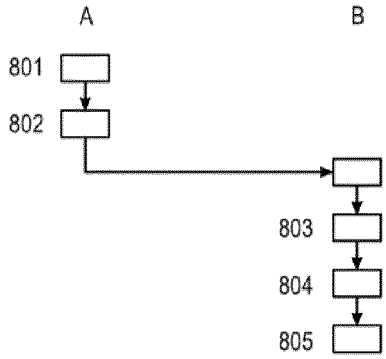
[Fig. 6]



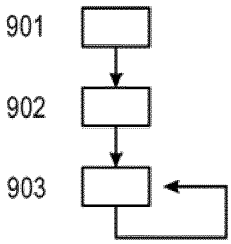
[Fig. 7]



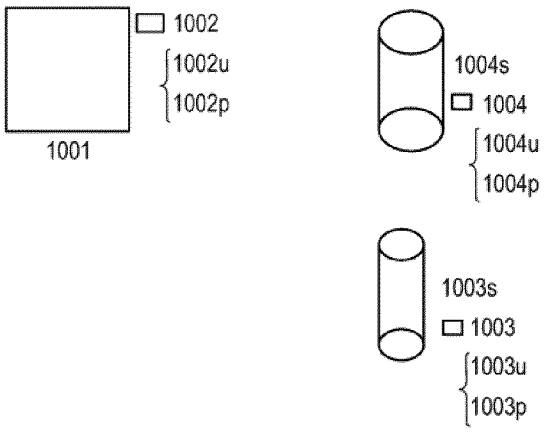
[Fig. 8]



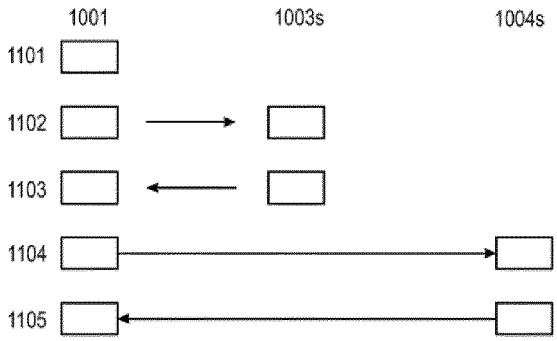
[Fig. 9]



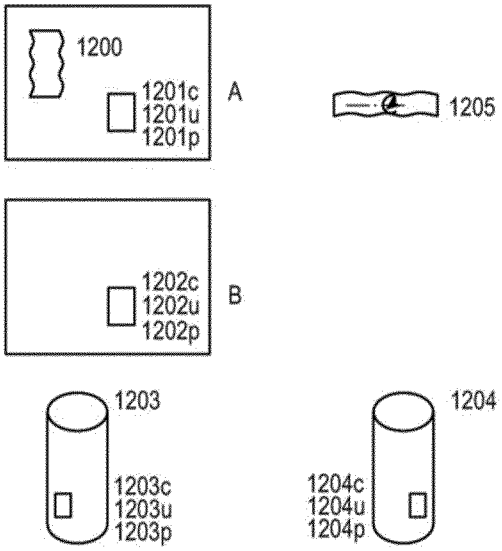
[Fig. 10]



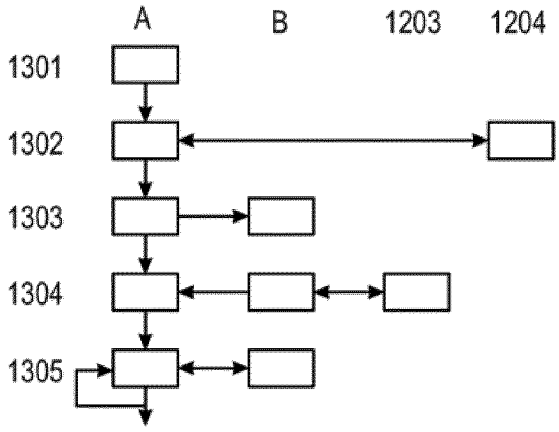
[Fig. 11]



[Fig. 12]



[Fig. 13]



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	Authorized officer
European Patent Office **p.b. 5818, Patentlaan 2, 2280 HV Rijswijk** **Netherlands** Telephone No. **(+31-70)340-2040** Facsimile No. **(+31-70)340-3016**	**Jardak, Christine** Telephone No.

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	

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'appartenant 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 avri l 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, Chri sti ne**

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	