(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
25 novembre 2021 (25.11.2021)

WIPO | PCT

(10) Numéro de publication internationale
WO 2021/234307 A1

(51) Classification internationale des brevets :
G07C 9/20 (2020.01) *E05B 17/18* (2006.01)
E05B 47/00 (2006.01)

(21) Numéro de la demande internationale :
PCT/FR2021/050909

(22) Date de dépôt international :
20 mai 2021 (20.05.2021)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
FR 2005372 20 mai 2020 (20.05.2020) FR

(71) Déposant : **CARAX** [FR/FR] ; 1 rue des Capucines, 40140 Soustons (FR).

(72) Inventeur : **GAUBERT, Bernard** ; 1 Rue des Capucines, 40140 Soustons (FR).

(74) Mandataire : **TOUROUDE, Magali** ; TOUROUDE & ASSOCIATES, 2bis rue Alfred Nobel, Marne La Vallée 77420 (FR).

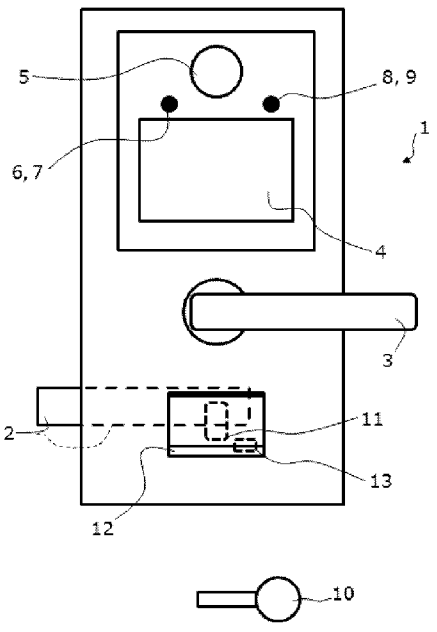
(81) États désignés *(sauf indication contraire, pour tout titre de protection nationale disponible)* : AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, IT, 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).

(54) **Title:** CONNECTED LOCK SYSTEM

(54) **Titre :** SYSTÈME DE SERRURE CONNECTÉE

Fig. 1



(57) **Abstract:** The invention relates to a connected lock system (1) for a door in the form of a housing, comprising at least one secure unlocking means (4, 5) connected to a door bolt (2), a camera (6) and a detector (7) connected to the camera (6), a module for connection to an access management application, a communication module comprising a microphone (8) and a loudspeaker (9), that can be connected to the camera (6). The invention also relates to a kit, a method and a corresponding assembly.

(57) **Abrégé :** L'invention concerne un système de serrure (1) connectée pour porte sous forme de boîtier, comprenant au moins un moyen de déverrouillage sécurisé (4, 5) connecté à un verrou de porte (2), une caméra (6) et un détecteur (7) connecté à la caméra (6), un module de connexion à une application de gestion d'accès, un module de communication comprenant microphone (8) et un haut-parleur (9), pouvant être connecté à la caméra (6). L'invention concerne en outre un kit, un procédé et un ensemble correspondant.

WO 2021/234307 A1

[Suite sur la page suivante]

Publiée:

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

— *avant l'expiration du délai prévu pour la modification des revendications, sera republiée si des modifications sont reçues (règle 48.2(h))*

Système de serrure connectée

L'invention se rapporte au domaine des systèmes de serrures connectées pour des portes, en particulier pour une porte d'entrée d'une habitation (maison, appartement...etc) ou autres bâtiments ou constructions similaires.

Dans ce domaine, il est connu de proposer des serrures connectées couvrant le verrou uniquement et pouvant être activées par un code numérique ou une application téléphonique.
Malheureusement, les serrures connectées classiques de l'art antérieur ne sont pas pleinement satisfaisantes en cas de décharge de batterie pour éviter un blocage du verrou.
En outre, les serrures connectées de l'art antérieur ne permettent pas de savoir en détail quelle personne utilise effectivement le moyen d'accès.
De plus, les moyens de déverrouillage de la serrure connectée ont des failles en termes de piratage, de sorte qu'un tiers peut pirater la connexion internet ou le signal de déverrouillage et avoir accès aux contrôles de la serrure.

US2014265359 décrit un système de serrure connecté pour porte, comprenant un boîtier et communiquant avec une application de gestion d'accès. Cependant, le boîtier comprend peu de fonctionnalités de communication.

US2019178003 décrit un autre système de serrure connecté pour porte, comprenant un boîtier et communiquant avec une application de gestion d'accès. Le boîtier présente une forme cylindrique et une grande compacité, qui limite le nombre de fonctions pouvant être intégrées au système de serrure.

Ainsi, un premier objectif de l'invention est de proposer un système de serrure connectée ayant des moyens permettant d'éviter le blocage du verrou en cas de décharge de la batterie du système.
Un deuxième objectif est de proposer un système de serrure connectée permettant de savoir qui utilise effectivement le moyen d'accès.
Un troisième objectif est de proposer un système de serrure connectée davantage sécurisé vis-à-vis du piratage des moyens d'accès.

Pour atteindre ces objectifs, l'invention propose un système de serrure connectée pour porte, ledit système étant configuré sous forme de boîtier, ledit boîtier comprenant au moins :
- un moyen de déverrouillage sécurisé apte à être connecté à un verrou de porte,
- une caméra configurée pour interagir avec un utilisateur ;
- un détecteur connecté à la caméra et configuré pour détecter une présence ;
- un module de connexion à une application de gestion d'accès ;
- un module de communication comprenant microphone et un haut-parleur configuré pour interagir avec l'utilisateur.

Selon un aspect, le système comprend une clé de secours physique et une serrure de secours sur le boîtier, pour déverrouiller le verrou de l'extérieur avec la clé de secours. Avantageusement, cela permet de pouvoir ouvrir le verrou de l'extérieur même si l'électronique du système n'est pas fonctionnelle.

Selon un autre aspect, le système comprend, côté extérieur, un port USB de recharge du système, de préférence derrière un volet de masquage. Avantageusement, cela permet de pouvoir recharger le système de l'extérieur, et ne pas être bloqué par le verrou.

Selon un autre aspect, au moins un moyen de déverrouillage sécurisé comprend un contrôle de déverrouillage du verrou pilotable par un ou plusieurs protocoles de communication IoT choisis parmi le NB-IoT, Lifi, UNB (Ultra narrow Band), un protocole mixte double fréquence (twin band). Avantageusement, ces protocoles permettent un déverrouillage à distance, et sont pour l'heure sensiblement inviolables. En outre, ils consomment peu d'énergie électrique.

Selon d'autres aspects pris isolément, ou combinés selon toutes les combinaisons techniquement réalisables :
- le boîtier s'étend sous forme de cadre autour du verrou et d'une poignée de porte associée ; et/ou
- le boîtier présente un profil plan apte à être installé contre une face extérieure de la porte ; et/ou

- le détecteur est configuré pour déclencher le fonctionnement de la caméra en cas de détection d'une présence ; et/ou
- le système comprend un volet de masquage amovible masquant la serrure de secours ; et/ou
- le moyen de déverrouillage sécurisé comprend un lecteur d'empreinte ; et/ou
- le moyen de déverrouillage sécurisé comprend un clavier numérique ; et/ou
- le moyen de déverrouillage sécurisé comprend un module de déverrouillage par badge ; et/ou
- le système est alimenté par une batterie lithium-ion rechargeable par résonance magnétique ; et/ou
- le module de connexion est configuré pour être connecté à l'application de gestion d'accès via un serveur, lequel intègre le programme de fonctionnement du système de serrure ; et/ou
- le système de serrure est connecté à un réseau Blockchain ; et/ou
- le système de serrure est connecté au réseau Holochain ; et/ou
- le système comprend un module de sécurité anti-arrachage, configuré pour notifier une alerte via l'application de gestion d'accès ; et/ou
- le système comprend un module de sécurité anti-intrusion, configuré pour notifier une alerte via l'application de gestion d'accès.

Un autre objet de l'invention concerne un kit de serrure connectée comprenant :
- un système de serrure connectée selon l'invention
- un serveur connecté au système de serrure via un protocole de communication sans fil,
- une application de gestion d'accès configurée pour piloter le système de serrure via le serveur.

L'invention concerne également un procédé de mise en œuvre d'un système de serrure connectée. Le procédé comprend les étapes suivantes :
a) installer le système de serrure sur un verrou de porte ;
b) connecter le système de serrure à un serveur via un protocole de communication sans fil;
c) connecter une application de gestion d'accès au système de serrure via le serveur.

Selon un mode de réalisation particulier, le système de serrure et l'application mobile sont connectés via un réseau Blockchain ou Holochain.

L'invention concerne également un ensemble de serrures connectées, comprenant plusieurs systèmes de serrure tel que décrits ci-dessus, chaque système de serrure étant connecté à un réseau Blockchain ou réseau Holochain. Chaque système de serrure 1 connectée constitue un point relais du réseau.

L'invention sera davantage détaillée par la description de modes de réalisation non-limitatifs, et sur la base de la figure annexée [Fig.1] illustrant une vue en plan de l'extérieur d'un système de serrure connectée selon un mode de réalisation préféré de l'invention.

L'invention concerne un système de serrure connectée 1, en particulier pour une porte de bâtiment, habitation ou autre construction similaire, plus particulièrement une porte d'entrée.
Le système de serrure connectée 1 est réalisé sous forme de boîtier. En particulier, le boîtier s'étend sous forme de cadre autour d'un verrou 2 et d'une poignée de porte 3 associée. Avantageusement, le boîtier peut être conformé en bloc rigide difficile à forcer. De préférence, le boîtier présente un profil plan apte à être installé contre une face extérieure de la porte.
Le système de serrure 1 comprend en outre des moyens de déverrouillage sécurisé connectés mécaniquement au verrou de porte 2. Il s'agit d'un moyen de contrôle d'accès pour actionner le verrou 2.
En particulier, les moyens de déverrouillage sécurisé peuvent comprendre un lecteur d'empreinte 4 et/ou un clavier numérique 5. Ainsi, le déverrouillage peut être réalisé par un code numérique via le clavier 5 du système de serrure 1, ou via une lecture d'une empreinte digitale sur le lecteur 4.
D'autres moyens de déverrouillage peuvent être envisagés. De préférence, ces moyens peuvent aussi être utilisés pour le verrouillage.
Dans une variante préférée, le système de serrure 1 est configuré de sorte que son verrouillage peut être réalisé en levant la poignée 3 vers le haut. Le déverrouillage du système de serrure 1 de l'intérieur peut se faire fera via un bouton installé sur la platine du système de serrure 1 électriquement ou mécaniquement.

Le système de serrure 1 comprend un module de connexion à une application de gestion d'accès. Il s'agit d'une application web ou d'une application mobile chargeable dans un appareil du gestionnaire d'accès, c'est à dire le propriétaire du système 1 ou un opérateur, situés à distance.
L'application de gestion d'accès peut être installée sur un ou plusieurs appareils du propriétaire du système 1, tels que smartphone, montre, tablette, ordinateur, etc.
L'application peut être utilisée pour verrouiller ou déverrouiller le système de serrure 1 à distance.
Le module de connexion se connecte à l'application via un protocole de communication sans fil, par exemple en WIFI ou par un module de données mobiles. Ce module peut intégrer des composants matériels à cet effet. Avantageusement, la connexion en données mobiles (3G, 4G, 5G...) permet de pouvoir maintenir une connexion même en cas de coupure d'internet domestique (WIFI).
Le protocole de communication peut être sélectionné via l'application mobile automatiquement.

Selon un mode de réalisation préféré, le système de serrure 1 est couplé à un serveur. Tous deux sont commandés par l'application de gestion d'accès installée sur un ou plusieurs appareils du gestionnaire du système 1, tels que smartphone, montre, tablette, ordinateur, etc.
Le programme de fonctionnement du système de serrure 1, constituant son « cerveau », se trouve sur le serveur. Le principe de fonctionnement est comparable à un système d'alarme, comme la relation entre un détecteur d'intrusion et la centrale d'alarme.
Le système de serrure 1 est connecté au serveur via un protocole de communication sans fil, tel que le protocole WIFI. Le serveur transmet via le réseau installé les informations du système de serrure 1, sur l'application de gestion.
L'application passe obligatoirement par le serveur pour communiquer avec le système de serrure 1, c'est la même procédure dans l'autre sens. Cela enlève toutes contraintes distancielles ou de performances dans la communication entre la serrure et l'application.
L'installation (serrure, serveur, application) peut fonctionner sur un réseau décentralisé de type Blockchain (tels que Filecoin, Storj, Sia, MaidSafe) ou

Holochain, qui est une nouvelle technologie permettant d'aller vers un Internet réellement décentralisé et ultra performant, différent de l'internet (http) comme on le connaît ou de la Blockchain. Le réseau Holochain a l'avantage d'être moins énergivore et plus sécurisé.

L'invention peut présenter deux applications bien distinctes :
- La première spécifique au fonctionnement de la serrure pour les particuliers.
- La deuxième uniquement réservée à certains secteurs professionnels, tel que la poste ou autres services de livraison, services de secours (pompiers, samu...etc), forces de l'ordre (gendarmerie, police....) certains services d'aide à domicile (aide à la personne...). Chaque secteur professionnel aura, au niveau de l'application de gestion, les spécificités liées à son cœur de métier. Le tout sera réalisé dans le respect des normes défini par les autorités compétentes, comme la CNIL pour la France. Cette application d'accès, pour des raisons de sécurité, ne se trouvera pas en téléchargement sur le web (http).

Selon un aspect de l'invention, les moyens de déverrouillage sécurisé peuvent comprendre un contrôle de déverrouillage du verrou pilotable par un ou plusieurs protocoles de communication IoT choisis parmi le M2M (machine to machine), NB-IoT, Lifi, UNB (Ultra narrow Band), un protocole mixte double fréquence (twin band). Ainsi, la commande de déverrouillage est acheminée vers le système par un ou plusieurs de ces protocoles. Des composants nécessaires sont prévus dans le boîtier à cet effet. Avantageusement, ces protocoles permettent un déverrouillage à distance, et sont pour l'heure sensiblement inviolable. Le twin band est une mesure de sécurité supplémentaire dans son mode communication. Selon un éventuel embouteillage d'une fréquence, il permettra à l'autre fréquence de donner l'information plus rapidement.
En outre, la technologie UNB (Ultra Narrow Band) utilise des bandes de fréquences (onde radio) libres de droit disponibles dans le monde entier comme les bande ISM (bande industrielle, scientifique et médical) pour exemple en Europe il s'agit de l'ISL à 868 Mhz. Cette fréquence est radio ultra rapide et de longue portée.
Le système de serrure 1 selon une variante est équipé de cette technologie en mode protocole Mixte double fréquence 433Mhz / 868Mhz / 902Mhz ou twin band. Cette variante est très sécurisante et performante en cas d'encombrement des canaux. Par

ailleurs, cette technologie installée sur le système de serrure 1 lui permettra d'être toujours fonctionnel en cas de coupure électrique, d'internet...etc.
Le protocole de communication peut être choisi en fonction du lieu géographique où est installé le système de serrure 1.

Les moyens de déverrouillage sécurisé peuvent en outre comprendre un module de déverrouillage par badge. Ainsi, un lecteur de badge (non-représenté) peut être prévu sur le boîtier à cet effet.

De préférence, le système de serrure 1 pourra être connecté à plusieurs appareils au sein d'un même réseau domestique, voire tous, en utilisant le même protocole de transmission par onde radio.

De préférence, l'application comprend une fonction indiquant le niveau de charge des piles (batteries) du système de serrure 1.
Dans une variante, par sécurité dans le cas où les piles (batteries) ont une charge faible et que la serrure est sur position déverrouillée, alors la serrure se verrouille automatiquement.
En cas de verrouillage, pour déverrouiller le système de serrure 1, plusieurs options sont possibles : charger les batteries/changer les piles de l'intérieur, déverrouiller mécaniquement depuis l'intérieur ou via une clé de secours, comme détaillé plus bas.

Selon une variante, le système de serrure 1 peut être alimenté par une batterie lithium-ion rechargeable par résonance magnétique.
Le dispositif de recharge par résonance magnétique comprend un émetteur et un récepteur (soit un élément connecté à la batterie à charger, soit la batterie elle-même).
Par exemple, l'émetteur peut être installé sur une face intérieure de la porte et le récepteur dans le boîtier du système de serrure 1 connectée, du coté de la porte plutôt que vers l'extérieur, pour réduire la distance entre l'émetteur et le récepteur.
En alternative, l'émetteur peut être installé dans le serveur, qui peut être placé à plusieurs mètres du système de serrure 1.

D’autres agencements de l’émetteur et du récepteur sont possibles dans sortir du cadre de l’invention.

De préférence, un contrôleur de charge est intégré au système de serrure 1 pour surveiller en permanence l’état de charge de la batterie. Le contrôleur a une fonction de régulation, consistant à assurer la charge complète de la batterie et prévenir de tout risque de surcharge de la batterie en stoppant son alimentation lorsqu’elle atteint un niveau de charge prédéterminé. Le contrôleur coupe l’alimentation du générateur lorsque l’état de charge de la batterie atteint l’une des valeurs limites correspondant au déclenchement de la sécurité. Cette surveillance et cette protection permanente permettent ainsi de prolonger de façon importante les performances et la durée de vie de la batterie.

La résonance magnétique permet le chargement de la batterie à des distances importantes. Cette technique repose sur une bobine et un condensateur qui fait office de résonateur. L'énergie électrique est transmise par résonance électromagnétique entre la bobine de l'émetteur et celle du récepteur. Ce procédé s’accommode ainsi de plus grandes distances de charge. Le couplage magnétique entre les deux bobines peut en effet être faible, à condition que les fréquences de résonance se correspondent entre les deux bobines. Cette technique donne donc plus de souplesse quant à la disposition entre l’émetteur et le récepteur.

En terme de fréquences, les ondes électromagnétiques (WPT : Wireless Power Transfer en anglais) seront dans des bandes de fréquences inférieures à 30 MHz.

Selon un aspect, outre le contrôle d’accès, le système de serrure 1 comprend une caméra 6 et un détecteur 7 connecté à la caméra 6. La caméra 6 est configurée pour capturer des images de l’extérieur du boîtier. La caméra 6 peut être fixe et dirigée selon une unique direction, ou bien orientable selon différentes directions, par rapport au boîtier. Le détecteur 7 est configuré pour détecter toute présence devant la porte d'entrée, à proximité du boîtier.

De préférence, la caméra 6 est à vision nocturne. De préférence, le détecteur 7 est également à vision nocturne.

Selon une variante, le détecteur 7 est intégré dans la caméra 6.

De préférence, le détecteur 7 est configuré pour déclencher le fonctionnement de la caméra 6 en cas de détection d’une présence. Cela permet de limiter la consommation d’énergie de la caméra 6.

De préférence, le détecteur 7 est configuré pour signaler la détection d'une présence via une alerte sonore, vibreur ...etc envoyé sur au moins un appareil du propriétaire (sur un smartphone, une montre connectée, une tablette, un ordinateur, etc) ou de l'opérateur, et quel que soit le lieu où l'on se trouve (travail, vacance, sur son canapé.....etc) à une très longue portée.
Dans la variante préférée, cette fonctionnalité est activée dès qu'une présence est détectée (temps minimum arrêté devant la porte, par exemple un temps de deux secondes) et à partir d'une certaine distance de la serrure, moins d'un mètre par exemple. La personne est par exemple vue en gros plan.
Selon le réglage choisi dans l'application par le propriétaire, la personne pourra être filmée, prise en photo...etc, et enregistrée sur au moins un appareil du gestionnaire d'accès, notamment le smartphone du propriétaire.

Le système de serrure 1 comprend en outre un module de communication comprenant un microphone 8 et un haut-parleur 9. Avantageusement, cela permet de pouvoir interagir avec un tiers voulant entrer en entrant en communication avec le gestionnaire d'accès, c'est à dire le propriétaire ou un opérateur.
De préférence, le module de communication peut être utilisé en association avec la caméra 6, permettant de voir ledit tiers situé à proximité du boîtier.
De préférence, le module de communication et ses composants (microphone 8 et un haut-parleur 9, et caméra 6 le cas échéant) fonctionne en WIFI.
On pourra communiquer avec cette personne, déverrouiller ou verrouiller la porte à distance et quel que soit le lieu où l'on se trouve à une très longue portée. Il peut être nécessaire d'avoir une connexion internet mobile pour faire fonctionner la communication.

Selon une variante, le système 1 comprend une clé de secours 10 physique et une serrure de secours 11 sur le boîtier, pour déverrouiller le verrou 2 de l'extérieur avec la clé de secours 10.

Selon une variante, le système 1 comprend un volet de masquage 12 amovible masquant la serrure de secours 11. Par exemple, le volet 12 peut être coulissé ou pivoté verticalement ou horizontalement. La serrure de secours 11 est connectée au même verrou 2 que la serrure connectée par une liaison mécanique. La serrure de

secours 11 est configurée pour pouvoir déverrouiller le verrou 2 lorsque la serrure connectée est défaillante. Par exemple, l'insertion de la clé de secours 10 désaccouple le cylindre des moyens d'actuation du verrou 2 ou lesdits moyens ne sont pas accouplés au verrou 2 en situation standard. Avantageusement, la serrure de secours 11 permet de déverrouiller le verrou 2 même si la serrure connectée n'est pas fonctionnelle ou est déchargée.
Le volet de masquage 12 est équipé d'un loqueteau à pression, comprenant un ressort avec aimant. Son ouverture et fermeture se fera par pression. Derrière le volet de masquage 12 se trouve de préférence un détecteur de positionnement, ce qui permet via l'application de gestion d'accès installée sur au moins un appareil du gestionnaire d'accès, de connaître l'état du volet de masquage 12 et de recevoir une alerte en cas d'ouverture de ce dernier.

Selon une variante, le système 1 comprend un port USB 13 de recharge du système. Ce port USB 13 est connecté à l'électronique du système de serrure connectée. Ce port 13 est disposé côté extérieur, par exemple l'extérieur du bâtiment ou de l'habitation ou autre… Le port USB 13 est de préférence disposé derrière le volet de masquage 12. Avantageusement, le volet de masquage 12 permet de protéger le port USB 13 de la poussière et de l'humidité. Il en est de même pour la serrure de secours 11.

Selon une variante, le système comprend un module de sécurité anti-arrachage, configuré pour notifier une alerte via l'application de gestion d'accès. En particulier, il s'agit d'un système électronique permettant de détecter l'arrachage par exemple via une détection de séparation de deux pièces du boîtier, et transmettre une notification à cet effet au gestionnaire d'accès via l'application de gestion d'accès.

Selon une variante, le système comprend un module de sécurité anti-intrusion, configuré pour notifier une alerte à l'application de gestion d'accès. En particulier, il s'agit d'un système électronique permettant de détecter une intrusion par exemple via une détection de perçage, et transmettre une notification à ce sujet au gestionnaire d'accès via l'application de gestion d'accès.
En particulier, le système de serrure 1 en mode "verrouillé" active les systèmes de sécurité d'arrachage et de détection de vibration aussi bien sur la porte

correspondante que sur le système de serrure 1 (tentative de perçage de la serrure... dégondage de la porte... etc).

En utilisation, un tiers déclenche le détecteur de mouvement 7 de la caméra 6, et une alerte est notifiée dans l'application. Si ce tiers a obstrué la caméra 6, et essaye de fracturer la porte, le système de serrure 1… une deuxième alerte spécifique est envoyée via l'application. Cette transmission de signal se fait par onde radio via le canal le plus approprié. Ainsi, une coupure électrique ou web n'empêchera pas la transmission d'alerte.

Un autre objet de l'invention concerne un kit de serrure connectée comprenant :
- un système de serrure 1 tel que décrit précédemment
- un serveur connecté au système de serrure 1 via un protocole de communication sans fil, par exemple WIFI ;
- une application de gestion d'accès configurée pour piloter le système de serrure 1 via le serveur.
Optionnellement, le kit peut aussi inclure un badge d'accès.

Selon un mode de réalisation particulier, le système de serrure 1 peut être connecté au réseau Holochain. Chaque système de serrure 1 connectée constitue un point relais du réseau Holochain.
Les architectures centralisées traditionnelles sont faciles à comprendre, à entretenir et à sécuriser, mais elles créent des points de défaillance centraux.
Le réseau Holochain transforme l'architecture des applications à l'envers : les utilisateurs sont au centre de leur présence en ligne, en charge de leur propre identité, de leurs données et de leur traitement.
Dans une application Holochain, le traitement, le stockage et la surface de sécurité sont répartis sur l'ensemble du réseau. Cela réduit les points de défaillance centraux, les goulots d'étranglement et les cibles d'attaque attrayantes.
Les deux piliers de l'intégrité des applications sont l'intégrité intrinsèque des données et la réplication / validation par les pairs.
Le réseau Holochain ne comprend de base de données mondiale unique; les données proviennent de nombreuses sources individuelles.

Chaque utilisateur d'une application participe également à la construction de l'infrastructure de l'application, en fournissant ses propres ressources de calcul et de stockage et en prenant la responsabilité de valider et de stocker une petite partie des données des autres utilisateurs.
Le tout est plus grand que la somme de ses parties de nombreux agents, jouant selon des règles simples, se combinent pour former un organisme social qui maintient sa propre santé.

Une fois le réseau Holochain fonctionnel, l'application de gestion d'accès est configurée pour réaliser une mise à jour, permettant au système de serrure 1 de fonctionner sur le réseau Holochain, présentant de nombreux avantages : plus sécurisé, plus rapide, moins énergivore, zone blanche réduite comparer aux réseaux actuels. La mise à jour se fera automatiquement entre l'application et le système de serrure 1 connectée. Un réseau privé entre le système de serrure 1 et l'application sera crée, et une clé cryptographique unique sera attribuée à ce réseau privé. L'application et le système de serrure 1 seront appairées (« peer-to-peer » en anglais). Cette clé cryptographique pourra être transmise à des tierces personnes.
Le système de serrure 1 connectée fonctionnant sur le réseau Holochain servira de relais au réseau au même titre que l'Holoport, que des appareils du type smartphone, montre, tablette, ordinateur, ce qui permettra au propriétaire de la serrure d'être rémunéré en cryptomonnaie du réseau Holochain (retour sur investissement).
Avantageusement, un outil de surveillance et de gestion de l'utilisation de la bande passante peut être installé dans le serveur afin de prioriser la bande passante du réseau privé pour supporter les applications du système de serrure connectée 1 et du foyer.
Ainsi cela permettra d'optimiser les performances du réseau (Holochain, IPFS, SafeNetwork, Storj...) selon le choix fait du réseau et d'augmenter la rentabilité (points gagnés pour l'hébergement du réseau).

L'application de gestion d'accès du système de serrure 1 pourra, via le serveur, commander l'ouverture d'ouvrants, par exemple un portail (pour une maison ou une copropriété), ou la porte d'entrée d'un immeuble dans le cas d'un immeuble équipé de cette serrure connectée.

L'application de gestion d'accès peut être configurée pour détecter les systèmes de serrures connectées qui se trouvent dans un certain périmètre.

L'application ne permet pas de piloter directement chaque serrure, il faudra au préalable faire la demande d'accès auprès du propriétaire de cette dernière. Celui-ci aura l'option de refuser la demande, de l'accepter temporairement ou définitivement. Cette autorisation peut permettre de déverrouiller le verrou (2), ou bien simplement donner la possibilité de «sonner à la porte» pour que le propriétaire déverrouille le verrou (2).

REVENDICATIONS

1) Système de serrure (1) connectée pour porte, ledit système étant configuré sous forme de boîtier, ledit boîtier comprenant au moins :
- un moyen de déverrouillage sécurisé (4, 5) apte à être connecté à un verrou de porte (2) ;
- une caméra (6) configurée pour interagir avec un utilisateur ;
- un détecteur (7) connecté à la caméra (6) et configuré pour détecter une présence;
- un module de connexion à une application de gestion d'accès ;
- un module de communication comprenant un microphone (8) et un haut-parleur (9) configurés pour interagir avec l'utilisateur.

2) Système selon la revendication précédente, caractérisé en ce que le boîtier s'étend sous forme de cadre autour du verrou (2) et d'une poignée de porte (3) associée.

3) Système selon l'une des revendications précédentes, caractérisé en ce que le boîtier présente un profil plan apte à être installé contre une face extérieure de la porte.

4) Système selon l'une des revendications précédentes, caractérisé en ce qu'il comprend une clé de secours (10) physique et une serrure de secours (11) sur le boîtier, pour déverrouiller le verrou (2) de l'extérieur avec la clé de secours (10).

5) Système selon la revendication précédente, caractérisé en ce qu'il comprend un volet de masquage (12) amovible masquant la serrure de secours (10).

6) Système selon l'une des revendications précédentes, caractérisé en ce qu'il comprend, côté extérieur, un port USB (13) de recharge du système, de préférence derrière le volet de masquage (12).

7) Système selon l'une des revendications précédentes, caractérisé en ce que le moyen de déverrouillage sécurisé comprend un lecteur d'empreinte (4).

8) Système selon l'une des revendications précédentes, caractérisé en ce que le moyen de déverrouillage sécurisé comprend un clavier numérique (5).

9) Système selon l'une des revendications précédentes, caractérisé en ce qu'il est alimenté par une batterie lithium-ion rechargeable par résonance magnétique.

10) Système selon l'une des revendications précédentes, caractérisé en ce que le module de connexion est configuré pour être connecté à l'application de gestion d'accès via un serveur, lequel intègre le programme de fonctionnement du système de serrure (1).

11) Système selon l'une des revendications précédentes, caractérisé en ce qu'il est connecté à un réseau Blockchain.

12) Système selon l'une des revendications précédentes, caractérisé en ce qu'il est connecté au réseau Holochain.

13) Système selon l'une des revendications précédentes, caractérisé en ce que le moyen de déverrouillage sécurisé comprend un contrôle de déverrouillage du verrou pilotable par un ou plusieurs protocoles de communication IoT choisis parmi le NB-IoT, Lifi, UNB (Ultra narrow Band), un protocole mixte double fréquence (twin band).

14) Système selon la revendication précédente, caractérisé en ce qu'au moins un moyen de déverrouillage sécurisé comprend un module de déverrouillage par badge.

15) Système selon l'une des revendications précédentes, caractérisé en ce qu'il comprend un module de sécurité anti-arrachage, configuré pour notifier une alerte via l'application de gestion d'accès.

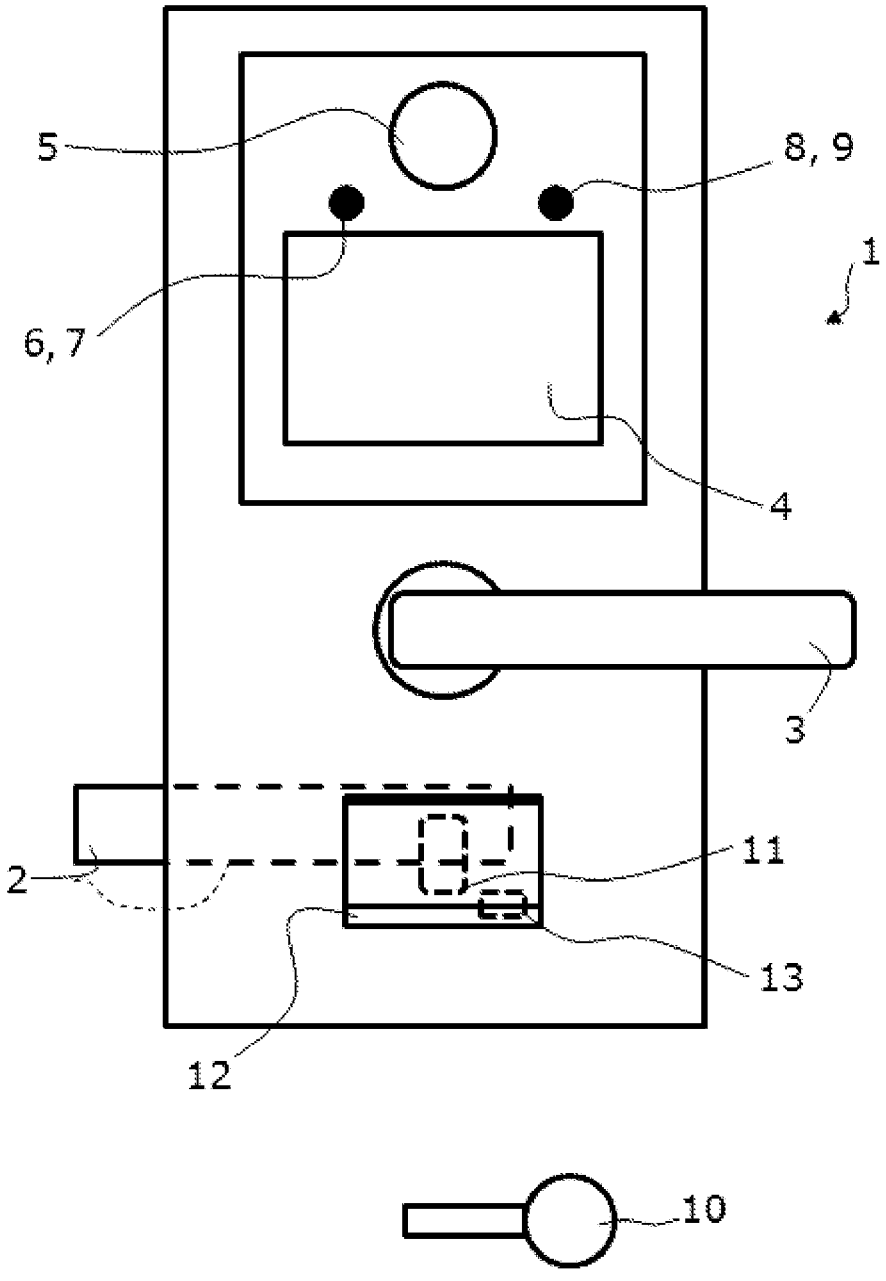
16) Système selon l'une des revendications précédentes, caractérisé en ce qu'il comprend un module de sécurité anti-intrusion, configuré pour notifier une alerte via l'application de gestion d'accès.

17) Kit de serrure connectée comprenant :
- un système de serrure (1) connectée selon l'une des revendications 1 à 16,
- un serveur connecté au système de serrure (1) via un protocole de communication sans fil,
- une application de gestion d'accès configurée pour piloter le système de serrure (1) via le serveur.

18) Procédé de mise en œuvre d'un système de serrure (1) connectée selon l'une des revendications 1 à 16, le procédé comprend les étapes suivantes :
a) installer le système de serrure (1) sur un verrou de porte (2) ;
b) connecter le système de serrure (1) à un serveur via un protocole de communication sans fil ;
c) connecter une application de gestion d'accès au système de serrure (1) via le serveur.

19) Ensemble de serrures connectées, caractérisé en ce qu'il comprend plusieurs systèmes de serrure (1) connectée selon l'une des revendications 1 à 16, chaque système de serrure étant connecté à un réseau Blockchain ou Holochain.

Fig. 1



INTERNATIONAL SEARCH REPORT

International application No.
PCT/FR2021/050909

A. CLASSIFICATION OF SUBJECT MATTER

G07C 9/20(2020.01)i; ***E05B 47/00***(2006.01)i; *E05B 17/18*(2006.01)n

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)

G07C; E05B; E05C

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	US 2014265359 A1 (CHENG SHIH YU THOMAS [US] ET AL) 18 September 2014 (2014-09-18)	1-11,13-19
A	the whole document	12
X	WO 2016085529 A1 (HENDERSON KEVIN [US]) 02 June 2016 (2016-06-02)	1-11,13-19
A	the whole document	12
X	WO 2017117137 A1 (BOT HOME AUTOMATION INC [US]) 06 July 2017 (2017-07-06)	1-11,13-19
A	the whole document	12
X	US 2019178003 A1 (MARTIN JOHN H [US] ET AL) 13 June 2019 (2019-06-13)	1-11,13-19
A	paragraph [0049] paragraph [0057] - paragraph [0064]	12
X	CN 105100187 A (YUAN YUCHAO) 25 November 2015 (2015-11-25)	1-11,13-19
A	the whole document	12
A	CN 108979338 A (CHEN LI) 11 December 2018 (2018-12-11) abstract	1,3

☑ 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
10 September 2021	**21 September 2021**

Name and mailing address of the ISA/EP	Authorized officer
European Patent Office **p.b. 5818, Patentlaan 2, 2280 HV Rijswijk** **Netherlands**	**Robelin, Fabrice**
Telephone No. **(+31-70)340-2040** Facsimile No. **(+31-70)340-3016**	Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/FR2021/050909

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	EP 3366872 A1 (XIAMEN AEROLITE TECH CO LTD [CN]) 29 August 2018 (2018-08-29) paragraph [0035]	1,5
A	FR 3049635 A1 (ETABLISSEMENTS DECAYEUX [FR]) 06 October 2017 (2017-10-06) page 8, line 36 - page 9, line 2	1,7
A	FR 3048714 A1 (CHEN [FR]) 15 September 2017 (2017-09-15) page 8, lines 1-3	1,7
A	EP 3505710 A1 (NETATMO [FR]) 03 July 2019 (2019-07-03) paragraph [0002]	1,8
A	WO 2018129915 A1 (SHENZHEN IKMAK TECH CO LTD [CN]) 19 July 2018 (2018-07-19) paragraph [0016]	1,9
A	CN 110533807 A (HANGZHOU YULIAN TECH CO LTD) 03 December 2019 (2019-12-03) the whole document	1,11

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/FR2021/050909

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
US 2014265359 A1	18 September 2014	AU 2014236999 A1	15 October 2015
		CA 2905009 A1	25 September 2014
		US 9322201 B1	26 April 2016
		US 9470017 B1	18 October 2016
		US 9470018 B1	18 October 2016
		US 9528296 B1	27 December 2016
		US 9534420 B1	03 January 2017
		US 9624695 B1	18 April 2017
		US 9644398 B1	09 May 2017
		US 9644400 B1	09 May 2017
		US 9683392 B1	20 June 2017
		US 2014265359 A1	18 September 2014
		US 2016189502 A1	30 June 2016
		US 2016189503 A1	30 June 2016
		US 2018261029 A1	13 September 2018
		WO 2014151692 A2	25 September 2014
WO 2016085529 A1	02 June 2016	US 2017332055 A1	16 November 2017
		WO 2016085529 A1	02 June 2016
WO 2017117137 A1	06 July 2017	NONE	
US 2019178003 A1	13 June 2019	AU 2018383754 A1	14 May 2020
		CA 3080639 A1	20 June 2019
		CN 111512009 A	07 August 2020
		US 2019178003 A1	13 June 2019
		WO 2019118559 A1	20 June 2019
CN 105100187 A	25 November 2015	NONE	
CN 108979338 A	11 December 2018	NONE	
EP 3366872 A1	29 August 2018	EP 3366872 A1	29 August 2018
		US 2020248479 A1	06 August 2020
		WO 2017067475 A1	27 April 2017
FR 3049635 A1	06 October 2017	FR 3049635 A1	06 October 2017
		US 2017284126 A1	05 October 2017
FR 3048714 A1	15 September 2017	NONE	
EP 3505710 A1	03 July 2019	CN 109972920 A	05 July 2019
		EP 3505710 A1	03 July 2019
		US 2019203504 A1	04 July 2019
WO 2018129915 A1	19 July 2018	CN 206378916 U	04 August 2017
		WO 2018129915 A1	19 July 2018
CN 110533807 A	03 December 2019	NONE	

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale n°
PCT/FR2021/050909

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
INV. G07C9/20 E05B47/00
ADD. E05B17/18

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)
G07C E05B E05C

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	US 2014/265359 A1 (CHENG SHIH YU THOMAS [US] ET AL) 18 septembre 2014 (2014-09-18)	1-11, 13-19
A	le document en entier	12
X	WO 2016/085529 A1 (HENDERSON KEVIN [US]) 2 juin 2016 (2016-06-02)	1-11, 13-19
A	le document en entier	12
X	WO 2017/117137 A1 (BOT HOME AUTOMATION INC [US]) 6 juillet 2017 (2017-07-06)	1-11, 13-19
A	le document en entier	12
X	US 2019/178003 A1 (MARTIN JOHN H [US] ET AL) 13 juin 2019 (2019-06-13)	1-11, 13-19
A	alinéa [0049] alinéa [0057] - alinéa [0064]	12

-/--

[X] Voir la suite du cadre C pour la fin de la liste des documents

[X] 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
10 septembre 2021	21/09/2021

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	Robelin, Fabrice

1

C(suite). DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie*	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
X	CN 105 100 187 A (YUAN YUCHAO) 25 novembre 2015 (2015-11-25)	1-11, 13-19
A	le document en entier	12

A	CN 108 979 338 A (CHEN LI) 11 décembre 2018 (2018-12-11) abrégé	1,3

A	EP 3 366 872 A1 (XIAMEN AEROLITE TECH CO LTD [CN]) 29 août 2018 (2018-08-29) alinéa [0035]	1,5

A	FR 3 049 635 A1 (ETABLISSEMENTS DECAYEUX [FR]) 6 octobre 2017 (2017-10-06) page 8, ligne 36 - page 9, ligne 2	1,7

A	FR 3 048 714 A1 (CHEN [FR]) 15 septembre 2017 (2017-09-15) page 8, lignes 1-3	1,7

A	EP 3 505 710 A1 (NETATMO [FR]) 3 juillet 2019 (2019-07-03) alinéa [0002]	1,8

A	WO 2018/129915 A1 (SHENZHEN IKMAK TECH CO LTD [CN]) 19 juillet 2018 (2018-07-19) alinéa [0016]	1,9

A	CN 110 533 807 A (HANGZHOU YULIAN TECH CO LTD) 3 décembre 2019 (2019-12-03) le document en entier	1,11

1

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Demande internationale n°
PCT/FR2021/050909

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
US 2014265359 A1	18-09-2014	AU 2014236999 A1	15-10-2015
		CA 2905009 A1	25-09-2014
		US 9322201 B1	26-04-2016
		US 9470017 B1	18-10-2016
		US 9470018 B1	18-10-2016
		US 9528296 B1	27-12-2016
		US 9534420 B1	03-01-2017
		US 9624695 B1	18-04-2017
		US 9644398 B1	09-05-2017
		US 9644400 B1	09-05-2017
		US 9683392 B1	20-06-2017
		US 2014265359 A1	18-09-2014
		US 2016189502 A1	30-06-2016
		US 2016189503 A1	30-06-2016
		US 2018261029 A1	13-09-2018
		WO 2014151692 A2	25-09-2014
WO 2016085529 A1	02-06-2016	US 2017332055 A1	16-11-2017
		WO 2016085529 A1	02-06-2016
WO 2017117137 A1	06-07-2017	AUCUN	
US 2019178003 A1	13-06-2019	AU 2018383754 A1	14-05-2020
		CA 3080639 A1	20-06-2019
		CN 111512009 A	07-08-2020
		US 2019178003 A1	13-06-2019
		WO 2019118559 A1	20-06-2019
CN 105100187 A	25-11-2015	AUCUN	
CN 108979338 A	11-12-2018	AUCUN	
EP 3366872 A1	29-08-2018	EP 3366872 A1	29-08-2018
		US 2020248479 A1	06-08-2020
		WO 2017067475 A1	27-04-2017
FR 3049635 A1	06-10-2017	FR 3049635 A1	06-10-2017
		US 2017284126 A1	05-10-2017
FR 3048714 A1	15-09-2017	AUCUN	
EP 3505710 A1	03-07-2019	CN 109972920 A	05-07-2019
		EP 3505710 A1	03-07-2019
		US 2019203504 A1	04-07-2019
WO 2018129915 A1	19-07-2018	CN 206378916 U	04-08-2017
		WO 2018129915 A1	19-07-2018
CN 110533807 A	03-12-2019	AUCUN	