(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) **N° de publication :** **2 842 679**
(à n'utiliser que pour les commandes de reproduction)

(21) **N° d'enregistrement national :** **03 08396**

(51) Int Cl[7] : **H 04 L 9/22**

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt :** 09.07.03.

(30) **Priorité :** 19.07.02 GB 02167708.

(43) **Date de mise à la disposition du public de la demande :** 23.01.04 Bulletin 04/04.

(56) **Liste des documents cités dans le rapport de recherche préliminaire :** *Ce dernier n'a pas été établi à la date de publication de la demande.*

(60) **Références à d'autres documents nationaux apparentés :**

(71) **Demandeur(s) :** *RITECH INTERNATIONAL LIMITED* — HK.

(72) **Inventeur(s) :** LIM BOON LUM.

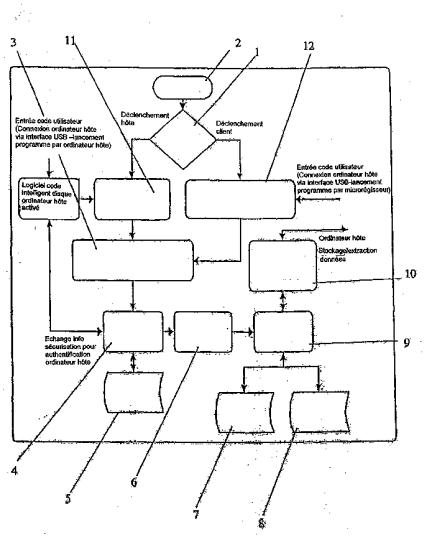
(73) **Titulaire(s) :**

(74) **Mandataire(s) :** CABINET MALEMONT.

(54) DISPOSITIF DE STOCKAGE DE DONNEES PORTABLE COMPORTANT UNE ARCHITECTURE DE MEMOIRE EN COUCHES ET PROCEDE DE CRYPTAGE/DECRYPTAGE D'UN CODE D'ENTREE D'UTILISATEUR.

(57) L'invention concerne un dispositif de stockage de données portable apte à sécuriser des données conformément à un code polynomial créé à l'aide de paramètres générés de manière pseudoaléatoire, qui peut agir en tant qu'hôte ou client en ce qui concerne l'accès d'utilisateurs aux données stockées en lui, et qui stocke les données selon une architecture de mémoire en couches. Ce dispositif comprend une interface de communication (10), un microrégisseur (1) comportant un moyen d'entrée commutable (2) intégré, des moyens formant mémoire primaire et secondaire (7, 8), une unité de traitement de données (9), un moyen de décision (3), une unité de traitement de code de sécurisation (4), une unité de décision de commande d'accès (6) et une unité de stockage de code intelligent crypté (5).

L'invention concerne également un procédé de cryptage/décryptage de code d'entrée d'utilisateur mis en oeuvre dans ce dispositif.



FR 2 842 679 - A1

La présente invention concerne un dispositif de stockage de données portable capable de stocker et de transporter facilement de grandes quantités de données et dans lequel un accès aux données peut être sécurisé par un code polynomial créé à l'aide de paramètres générés de manière pseudoaléatoire. Le dispositif peut agir en tant qu'hôte ou en tant que client relativement à un accès aux données pour ainsi assurer une protection non seulement en ce qui concerne les données qu'il contient mais également vis-à-vis d'un ordinateur auquel il est relié, les données étant stockées selon une architecture de mémoire en couches offrant une structure à compartiments primaire et secondaire sécurisée.

Cette invention propose en fait un disque de stockage de données pourvu d'une interface de communication faisant appel à une technique de cryptage et à une technique de commutation hôte/client pour créer une architecture nouvelle et un protocole de communication nouveau, afin d'assurer une sécurisation des données stockées sur le disque au moyen de paramètres générés de manière pseudoaléatoire, l'architecture en couches offrant en même temps à l'utilisateur une protection des couches grâce à l'utilisation d'un organe de commande à commutation hôte/client à autodéclenchement qui sécurise un accès non seulement aux données mais également à tout ordinateur hôte auquel le disque est relié.

Les données stockées sur le disque sont sécurisées au moyen d'une architecture de mémoire cloisonnée ainsi que d'un protocole et d'une procédure de protection de données tels que les données stockées dans la mémoire sont disposées en couches et cryptées conformément à un code généré de manière pseudoaléatoire. Grâce à ce

système de sécurité, il est impossible à quiconque d'accéder aux données sans le code d'entrée primaire.

Selon un premier aspect de la présente invention, il est donc proposé un dispositif de stockage de données portable pouvant être connecté à un ordinateur à distance, tel qu'un ordinateur personnel de bureau ou un ordinateur portable, caractérisé en ce qu'il est capable de sécuriser des données conformément à un code polynomial créé à l'aide de paramètres générés de manière pseudoaléatoire, en ce qu'il peut agir en tant qu'hôte ou en tant que client en ce qui concerne l'accès d'utilisateurs aux données stockées en lui, en ce qu'il stocke les données selon une architecture de mémoire en couches, et en ce qu'il est équipé d'une interface de communication, d'un microrégisseur comportant un moyen d'entrée commutable intégré, de moyens de stockage formant couches de mémoire primaire et secondaire, d'une unité de traitement de données, d'un moyen de décision en fonction de données, d'une unité de traitement de code de sécurisation, d'une unité de décision de commande d'accès et d'une unité de stockage de code intelligent crypté.

L'interface de communication, qui peut être une interface de type à bus série universel (USB) ou d'un autre type, permet à des utilisateurs d'accéder aux données stockées dans les moyens formant mémoire du dispositif. Elle permet aussi un accès réversible aux données stockées sur le disque.

Le microrégisseur est pourvu d'une entrée commutable reliée au moyen de décision en fonction de données en vue d'un accès aux couches primaire et secondaire de la mémoire. Le microrégisseur et le moyen de décision en fonction de données sont chargés d'établir une interface entre un ordinateur hôte et les moyens de stockage formant mémoire et, en tant que

tels, créent une passerelle permettant le stockage et l'extraction de données ainsi que des opérations vers et à partir des moyens de stockage sous la forme d'une mémoire flash, par exemple, par des utilisateurs autorisés.

Les moyens de stockage primaire et secondaire servent à stocker des données de manière à permettre un accès sélectif à des utilisateurs en fonction de l'autorisation accordée à ceux-ci, l'accès à ces données étant sécurisé conformément à un code crypté de sécurisation.

L'entrée commutable peut être déclenchée par un ordinateur hôte auquel le dispositif est relié, le dispositif agissant alors en tant que client, ou bien l'entrée peut être déclenchée par le microrégisseur lui-même, auquel cas le dispositif agit en tant qu'hôte. L'entrée du code peut se faire à partir de l'ordinateur hôte ou directement à partir du dispositif lui-même. Cette entrée de code peut ensuite être analysée par le moyen de décision en fonction de données pour permettre un accès aux couches primaire et secondaire de la mémoire.

L'unité de traitement de code de sécurisation est reliée de manière réversible à l'unité de stockage de code intelligent crypté et est également reliée à l'unité de décision de commande d'accès qui est elle-même reliée à l'unité de traitement de données.

L'unité de traitement de données est reliée de manière réversible aux moyens formant mémoire flash primaire et secondaire et est reliée à l'interface de communication par l'intermédiaire de laquelle il est possible d'y avoir accès. L'unité de traitement de données permet un accès bidirectionnel aux moyens formant mémoire en couches.

Les moyens formant mémoire peuvent être non rémanents ou rémanents, et peuvent recevoir et stocker de manière réversible des données pour permettre de multiples applications de lecture/écriture.

Un accès aux données stockées dans le dispositif est possible conformément à un code polynomial crypté généré en fonction d'une entrée de code d'utilisateur en combinaison avec un code prédéfini en usine. Pour accéder aux données contenues dans les moyens formant mémoire, un utilisateur enregistré doit entrer son code directement dans le dispositif ou dans un ordinateur hôte auquel le dispositif est relié. Cette possibilité de commande d'accès d'entrée commutable, permet à l'utilisateur du dispositif d'autoriser des tiers à accéder aux données contenues dans le dispositif par l'intermédiaire d'un ordinateur hôte homologué.

Le code d'entrée est converti en un code généré de manière pseudoaléatoire par une technique de cryptage. Ce code d'entrée d'utilisateur crypté est stocké dans les moyens formant mémoire. A ce code crypté, l'unité de traitement de code de sécurisation ajoute, selon une procédure d'adjonction polynomiale, un code prédéfini en usine pour produire un code de sécurisation. Ainsi, le code polynomial de sécurisation est créé à partir d'un code d'entrée d'utilisateur et d'un code prédéfini en usine. Ce code polynomial crypté de sécurisation est stocké dans les moyens formant mémoire.

Un accès aux données suppose que l'utilisateur entre le code d'entrée approprié soit par l'intermédiaire du dispositif soit par l'intermédiaire d'un ordinateur hôte homologué auquel le dispositif est relié. Une authentification du code d'entrée permet à l'utilisateur de procéder à la création d'un code de cryptage et d'accéder aux moyens formant mémoire primaire et secondaire.

L'enregistrement des utilisateurs nécessite que ceux-ci entrent un code de leur choix soit directement dans le dispositif soit par l'intermédiaire de l'ordinateur hôte auquel le dispositif est relié. Le code d'utilisateur est crypté conformément à des paramètres générés de manière pseudoaléatoire et est stocké dans les moyens formant mémoire. Ce code crypté est ensuite combiné à un code prédéfini en usine pour former un code polynomial de sécurisation. Ce code est pointé et accessible à l'aide d'un code connu sous le nom de pointeur de cryptage. L'accès d'un utilisateur peut être sélectivement limité à la couche de mémoire primaire ou à la couche de mémoire secondaire ou autorisé pour les deux couches.

Pour accéder aux données, l'utilisateur introduit son code d'entrée. Le moyen qui décide en fonction des données d'un accès à la couche primaire et/ou secondaire de la mémoire authentifie l'entrée de l'utilisateur. Puis, un pointeur de cryptage est préparé pour permettre d'extraire le code de cryptage de la mémoire à cloisonnement de sécurisation. Le code de cryptage est ensuite combiné au code prédéfini en usine pour créer le code polynomial de sécurisation. Ce code polynomial est alors décrypté par l'unité de traitement de code de sécurisation, après quoi l'unité de décision de commande d'accès autorise un accès aux données qui sont traitées par l'unité de traitement de données.

Le cloisonnement de la mémoire permet de limiter sélectivement l'accès que peuvent avoir des utilisateurs aux données contenues dans la mémoire. Ceci est rendu possible par l'architecture à cryptage en couches. Le plus haut niveau d'autorisation permet à un utilisateur d'accéder à l'ensemble des données stockées dans les différents compartiments de la

mémoire, tandis que le niveau le plus bas limite l'accès de celui-ci aux données contenues dans l'une ou l'autre couche. L'utilisateur peut ainsi permettre à des tiers d'avoir accès à certaines ou à la totalité des données contenues dans le dispositif grâce à une procédure d'enregistrement sélectif. Ces tiers peuvent accéder aux données par l'intermédiaire d'un ordinateur hôte homologué en entrant leur code d'utilisateur.

Selon un autre aspect de l'invention, il est également proposé un procédé de cryptage de code d'entrée d'utilisateur, caractérisé en ce qu'il comprend les étapes de conversion d'un code entré par un utilisateur en un code généré de manière pseudoaléatoire conformément à des algorithmes prédéfinis; de combinaison de ce code avec un code prédéfini en usine selon une procédure d'adjonction de séquence polynomiale pour produire un code de sécurisation; et de pointage du code de sécurisation qui n'est accessible que par un code pointeur de cryptage.

L'invention propose aussi un procédé de décryptage de code d'entrée d'utilisateur, caractérisé en ce qu'il comprend les étapes d'évaluation et d'authentification d'un code d'entrée d'utilisateur par un moyen de décision en fonction de données; de préparation d'un pointeur de cryptage par une unité de traitement de code de sécurisation pour extraire le code de cryptage de sécurisation de moyens formant mémoire sécurisés; de génération d'un code de sécurisation par l'unité de traitement de code de sécurisation selon une procédure d'adjonction de séquence polynomiale; de combinaison du code d'utilisateur crypté avec un code prédéfini en usine; et de décryptage de ce code de sécurisation par une unité de traitement de données. Ce qui précède, ainsi que d'autres caractéristiques et avantages de la

présente invention, ressortira plus clairement de la description détaillée suivante d'un mode de réalisation donnée à titre d'exemple nullement limitatif en référence aux dessins annexés dans lesquels:

la figure 1 est un schéma fonctionnel d'un dispositif de stockage de données portable selon l'invention; et

la figure 2 est un organigramme d'un procédé de cryptage/décryptage d'un code d'accès à des moyens formant mémoire primaire et secondaire, selon l'invention.

Le schéma fonctionnel de la figure 1 représente les organes constitutifs du dispositif. Le dispositif comporte une interface de communication 10 qui le relie à un ordinateur hôte et qui est en communication bidirectionnelle avec une unité de traitement de données 9. L'unité de traitement de données est en communication avec une unité de décision de commande d'accès 6 et une unité de stockage de données primaire 7 et une unité de stockage de données secondaire 8. L'unité de décision de commande d'accès 6 est en communication avec une unité de traitement de code de sécurisation 4 et reçoit une entrée de celle-ci.

L'unité de traitement de code de sécurisation 4 est en communication bidirectionnelle avec une unité de stockage de code intelligent crypté 5 ainsi qu'avec un moyen 3 de décision en fonction de données duquel elle reçoit une entrée, en vue de permettre un accès à la couche primaire et/ou la couche secondaire des moyens formant mémoire et à l'interface de communication.

Le moyen 3 de décision en fonction de données est en communication avec un ordinateur hôte et reçoit un code d'entrée 11 de celui-ci et/ou un code d'entrée 12 du dispositif proprement dit. L'entrée de code est en

communication avec un microrégisseur 1 qui est en communication avec une entrée commutable 2.

La figure 2 représente l'organigramme d'un procédé de cryptage/décryptage de code en vue d'accéder aux moyens formant mémoire. Un utilisateur commence par entrer son code d'entrée (étape 20). Ce code d'entrée d'utilisateur est ensuite authentifié (étape 21) par le moyen 3 de décision en fonction de données. Le code d'entrée d'utilisateur est ensuite évalué pour permettre de déterminer si l'utilisateur est habilité ou non à accéder aux moyens formant mémoire de niveau primaire et/ou secondaire (étape 22). Cette étape est également exécutée par le moyen 3 de décision en fonction de données.

Une fois que le code d'entrée d'utilisateur a été authentifié et que son type d'accès a été déterminé, un code pointeur de cryptage est préparé (étape 23). Le code de cryptage relatif à des utilisateurs enregistrés est extrait des moyens formant mémoire sécurisés en ce qui concerne un accès au niveau primaire et un accès au niveau secondaire par la préparation d'un code pointeur de cryptage primaire ou secondaire (étape 24, 25).

Puis, un code de sécurisation est généré (étape 26) par l'unité de traitement de code de sécurisation 4 par une procédure d'adjonction polynomiale au cours de laquelle un code crypté en usine, stocké dans l'unité de stockage de code intelligent crypté 5, et le code d'entrée d'utilisateur crypté sont combinés (étape 27).

Ce code de sécurisation est ensuite décrypté (étape 28) par l'unité de traitement de données 9 pour permettre à l'utilisateur d'accéder aux moyens formant mémoire de niveau primaire (étape 29) et/ou de niveau secondaire (étape 30). Un accès aux données est alors possible par l'intermédiaire de l'interface de communication 10 reliée à l'ordinateur hôte (étape 31).

Bien que la description précédente ait porté sur un mode de réalisation particulier de la présente invention, celle-ci n'est bien entendu pas limitée à l'exemple spécifique décrit et illustré ici, et l'homme de l'art comprendra aisément qu'il est possible d'y apporter de nombreuses variantes et modifications sans pour autant sortir du cadre de l'invention.

REVENDICATIONS

1. Dispositif de stockage de données portable pouvant être connecté à un ordinateur à distance, tel qu'un ordinateur personnel de bureau ou un ordinateur portable, caractérisé en ce qu'il est capable de sécuriser des données conformément à un code polynomial créé à l'aide de paramètres générés de manière pseudoaléatoire, en ce qu'il peut agir en tant qu'hôte ou en tant que client en ce qui concerne l'accès d'utilisateurs aux données stockées en lui, en ce qu'il stocke les données selon une architecture de mémoire en couches, et en ce qu'il est équipé d'une interface de communication (10), d'un microrégisseur (1) comportant un moyen d'entrée commutable (2) intégré, de moyens de stockage formant couches de mémoire primaire et secondaire (7, 8), d'une unité de traitement de données (9), d'un moyen (3) de décision en fonction de données, d'une unité de traitement de code de sécurisation (4), d'une unité de décision de commande d'accès (6) et d'une unité de stockage de code intelligent crypté (5).

2. Dispositif selon la revendication 1, caractérisé en ce que l'interface de communication (10) est en communication bidirectionnelle avec l'unité de traitement de données (9).

3. Dispositif selon la revendication 1, caractérisé en ce que l'unité de traitement de données (9) est en communication avec l'unité de décision de commande d'accès (6) et en communication bidirectionnelle avec les moyens formant mémoire primaire et secondaire (7, 8).

4. Dispositif selon la revendication 1, caractérisé en ce que l'unité de traitement de code de sécurisation (4) est reliée de manière réversible à l'unité de stockage de code intelligent crypté (5) et est

également en communication avec l'unité de décision de commande d'accès (6).

5. Dispositif selon la revendication 1, dans lequel le microrégisseur (1) comportant le moyen d'entrée commutable (2) intégré est en communication avec le moyen (3) de décision en fonction de données.

6. Dispositif selon la revendication 1, caractérisé en ce que le moyen (3) de décision en fonction de données est en communication avec l'unité de traitement de code de sécurisation (4).

7. Dispositif selon la revendication 1, caractérisé en ce que les moyens formant mémoire (7, 8) peuvent être non rémanents ou rémanents, et en ce qu'ils peuvent recevoir et stocker de manière réversible des données pour permettre de multiples applications de lecture/écriture.

8. Dispositif selon la revendication 1, caractérisé en ce que l'unité de décision de commande d'accès (6) détermine si un utilisateur peut avoir ou non accès aux moyens formant couches de mémoire primaire et/ou secondaire (7, 8) en fonction d'un code d'entrée d'utilisateur (11, 12).

9. Dispositif selon la revendication 1, caractérisé en ce que l'unité de traitement de code de sécurisation (4) est chargée de la fonction de cryptage et de décryptage des codes d'entrée d'utilisateurs (11, 12).

10. Dispositif selon la revendication 1, caractérisé en ce que l'unité de traitement de données (9) traite des données stockées dans les moyens formant mémoire primaire et secondaire (7, 8) avant qu'un utilisateur n'accède à celles-ci par l'intermédiaire de l'interface de communication (10).

11. Dispositif selon la revendication 1, caractérisé en ce que le microrégisseur (1) comportant l'entrée commutable intégrée (2) forme une passerelle

qui permet une interface d'un utilisateur avec le dispositif de stockage de données par l'intermédiaire d'un ordinateur hôte, en ce que l'entrée commutable (2) permet au dispositif d'agir en tant qu'hôte auquel cas le dispositif protège un accès aux données stockées dans les moyens formant mémoire, et en tant que client, auquel cas le dispositif peut être relié à un ordinateur hôte, et en ce que le dispositif peut permettre à des utilisateurs autorisés d'accéder à l'ordinateur auquel il est relié.

12. Dispositif selon la revendication 1, caractérisé en ce qu'un code crypté prédéfini en usine est stocké dans l'unité de stockage de code intelligent crypté.

13. Dispositif selon la revendication 1, caractérisé en ce que le moyen (3) de décision en fonction de données authentifie le code (11, 12) entré par l'utilisateur et détermine si l'utilisateur sera autorisé ou non à accéder aux données stockées dans les moyens formant couches de mémoire primaire et/ou secondaire (7, 8).

14. Procédé de cryptage de code d'entrée d'utilisateur, utilisable dans le dispositif selon la revendication 1, caractérisé en ce qu'il comprend les étapes de :

conversion d'un code entré par un utilisateur en un code généré de manière pseudoaléatoire conformément à des algorithmes prédéfinis;

combinaison de ce code avec un code prédéfini en usine selon une procédure d'adjonction de séquence polynomiale pour produire un code de sécurisation; et

pointage du code de sécurisation qui n'est accessible que par un code pointeur de cryptage.

15. Procédé selon la revendication 14, caractérisé en ce que le code polynomial crypté de sécurisation est stocké dans un moyen formant mémoire.

16. Procédé de décryptage de code d'entrée d'utilisateur, utilisable dans le dispositif selon la revendication 1, caractérisé en ce qu'il comprend les étapes de :

évaluation et authentification d'un code d'entrée d'utilisateur par un moyen de décision en fonction de données;

préparation d'un pointeur de cryptage par une unité de traitement de code de sécurisation pour extraire le code de cryptage de sécurisation de moyens formant mémoire sécurisés;

génération d'un code de sécurisation par l'unité de traitement de code de sécurisation selon une procédure d'adjonction de séquence polynomiale;

combinaison du code d'utilisateur crypté avec un code prédéfini en usine; et

décryptage de ce code de sécurisation par une unité de traitement de données.

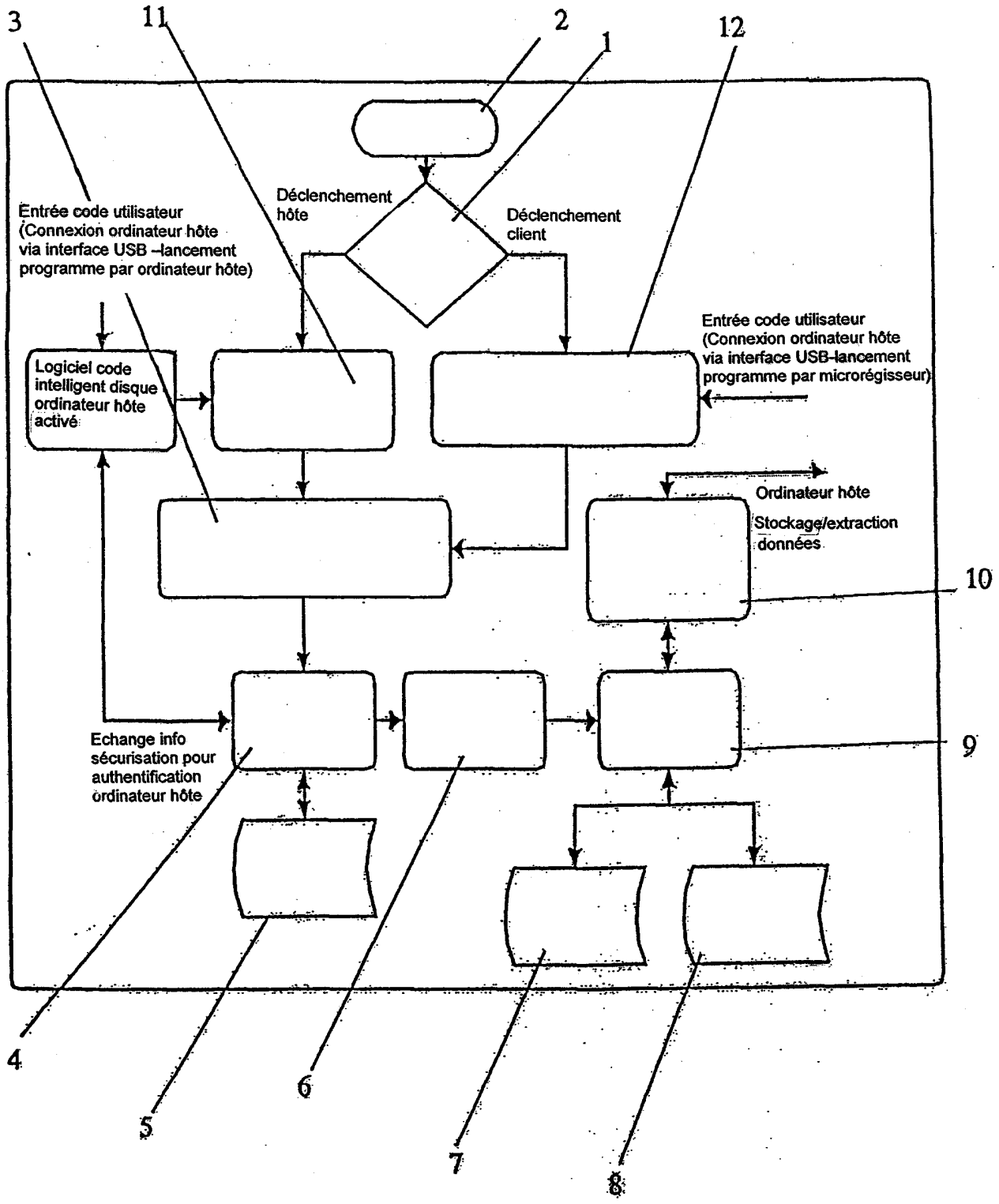

3
11
2
1
12
Entrée code utilisateur (Connexion ordinateur hôte via interface USB –lancement programme par ordinateur hôte)
Déclenchement hôte
Déclenchement client
Logiciel code intelligent disque ordinateur hôte activé
Entrée code utilisateur (Connexion ordinateur hôte via interface USB-lancement programme par microrégisseur)
Ordinateur hôte
Stockage/extraction données
10
Echange info sécurisation pour authentification ordinateur hôte
9
4
5
6
7
8

FIGURE 1

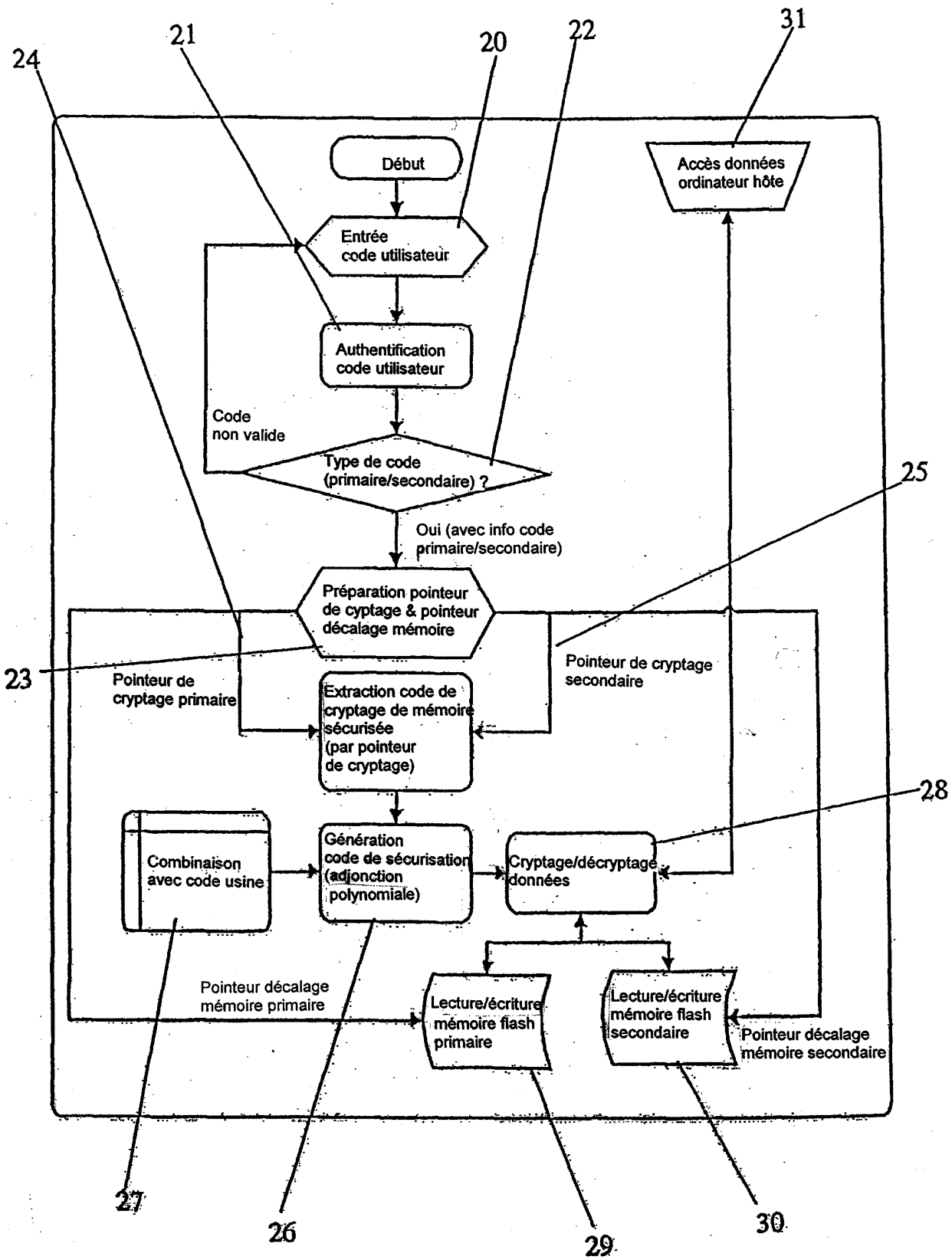

21
20
22
31
24
Début
Accès données ordinateur hôte
Entrée code utilisateur
Authentification code utilisateur
Code non valide
Type de code (primaire/secondaire) ?
25
Oui (avec info code primaire/secondaire)
Préparation pointeur de cyptage & pointeur décalage mémoire
23
Pointeur de cryptage primaire
Pointeur de cryptage secondaire
Extraction code de cryptage de mémoire sécurisée (par pointeur de cryptage)
28
Combinaison avec code usine
Génération code de sécurisation (adjonction polynomiale)
Cryptage/décryptage données
Pointeur décalage mémoire primaire
Lecture/écriture mémoire flash primaire
Lecture/écriture mémoire flash secondaire
Pointeur décalage mémoire secondaire
27
26
29
30

FIGURE 2