

12

DEMANDE DE BREVET D'INVENTION

A1

22 Date de dépôt : 17.01.02.

30 Priorité :

43 Date de mise à la disposition du public de la demande : 18.07.03 Bulletin 03/29.

56 Liste des documents cités dans le rapport de recherche préliminaire : *Se reporter à la fin du présent fascicule*

60 Références à d'autres documents nationaux apparentés :

71 Demandeur(s) : FRANCE TELECOM Société anonyme — FR.

72 Inventeur(s) : CANARD SEBASTIEN, GIRAULT MARC et TRAORE JACQUES.

73 Titulaire(s) :

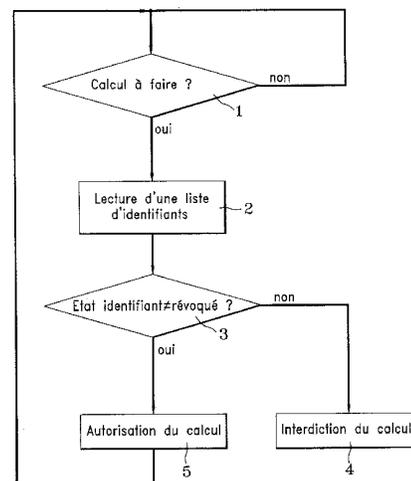
74 Mandataire(s) : FRANCE TELECOM.

54 PROCÉDE CRYPTOGRAPHIQUE DE REVOCATION A L'AIDE D'UNE CARTE A PUCE.

57 La présente invention se rapporte à un procédé cryptographique et à une carte à puce pour la mise oeuvre du procédé. Le procédé cryptographique consiste :

- avant tout calcul par un moyen de calcul de la carte à puce, à lire (2) par la carte à puce dans un moyen de mémorisation d'une seconde entité une liste d'identifiants de premières entités propriétaires d'une carte à puce, cette liste étant liée à chaque état attribué à chacune des premières entités par la seconde entité,

- à comparer (3), par la carte à puce, l'identifiant mémorisé dans un moyen de mémorisation de la carte à puce et le contenu de la liste, pour autoriser (5) ou interdire (4) tout calcul du moyen de calcul en fonction du résultat de la comparaison.



FR 2 834 841 - A1



La présente invention se rapporte au domaine des télécommunications et plus particulièrement à la sécurisation des transmissions, en particulier pour des services, qui fait appel à la cryptographie.

Pour authentifier l'origine d'un document transmis par des moyens de télécommunication, il a été développé des mécanismes de signature électronique. Il faut noter que les termes transmission sous forme électronique sont couramment utilisés pour qualifier une transmission d'un document par des moyens de télécommunication. Les documents dont il est question dans le contexte de l'invention se présentent obligatoirement sous forme numérique par opposition à une présentation sous forme papier ; le terme message est utilisé dans la suite de la demande pour désigner ce type de document. Les mécanismes de signature électronique les plus courants reposent sur des techniques de cryptographie dites à clé publique qui mettent en jeu une entité dite autorité de confiance. Habituellement, cette autorité de confiance génère des certificats pour le compte d'utilisateurs des procédés courants à clé publique ; ces certificats établissent un lien entre une clé publique et l'identité du propriétaire de cette clé. Pour mettre en œuvre un tel procédé, l'individu signataire du message doit préalablement se faire certifier auprès de l'autorité de confiance en lui communiquant au moins sa clé publique et son identité. Lors de sa mise en œuvre, le procédé de signature calcule une signature électronique du message en prenant en compte d'une part le contenu du message et d'autre part la clé privée de l'individu. Le signataire transmet au destinataire le message, la signature et son certificat. Le destinataire du message vérifie la signature électronique du message à l'aide d'au moins la clé publique et du contenu du message.

Pour des applications particulières, telles que le vote électronique, les enchères électroniques ou le paiement électronique anonyme, il est nécessaire de pouvoir disposer d'une signature électronique dite anonyme. Une signature électronique anonyme a les mêmes caractéristiques qu'une signature électronique sauf que le destinataire ne peut déterminer l'identité du signataire ; le signataire garde l'anonymat. Toutefois, le destinataire peut s'adresser à l'autorité de confiance qui dispose, par l'intermédiaire du certificat, d'un moyen pour lever l'anonymat. Parmi les différents types de signature anonyme, il existe un type particulier appelé signature anonyme de groupe. Un procédé de signature anonyme de groupe permet à chaque membre d'un

groupe de produire une signature électronique qui soit caractéristique du groupe. Le destinataire d'un message accompagné d'une signature anonyme de groupe peut vérifier que la signature a été produite par un des membres du groupe. Toutefois il ne peut déterminer, parmi les différents membres du groupe, le membre dont il s'agit.

5 Dans le contexte de l'invention, un groupe est un ensemble d'individus qui se déclarent auprès d'une autorité comme appartenant à un même groupe. Lors de cette déclaration, chaque individu interagit avec l'autorité de confiance selon un protocole déterminé à l'issue duquel l'individu obtient une clé privée, associée à une clé publique de groupe préalablement déterminée par l'autorité de confiance, et l'autorité et
10 l'individu obtiennent un identifiant de l'individu associé à cette clé privée. Chacun de ces individus est dans la suite de la demande désigné par le terme de membre. Un exemple d'un tel protocole est décrit dans l'article de J.Camenisch et M.Michels qui a pour référence "Efficient group signature schemes for large groups", In B.Kaliski, editor, *Advances in Cryptology – CRYPTO97*, volume 1296 of LNCS, pages 410 à 424, Springer-Verlag, 1997. La même interaction intervient lors de
15 l'arrivée d'un nouveau membre. L'existence d'un groupe se traduit du côté de l'autorité de confiance par l'attribution au groupe d'une clé publique dite de groupe et par l'attribution à chaque membre d'une clé privée associée à la clé publique, différente pour chaque membre, et d'un identifiant. A l'aide de sa clé privée, un membre peut
20 produire une signature anonyme de groupe d'un message de son choix. Un destinataire quelconque peut vérifier que cette signature a bien été produite par un des membres du groupe à condition d'utiliser la clé publique de groupe. A l'issue de la vérification, le destinataire a la certitude que la signature a été produite, ou pas, par un membre du groupe, mais il n'obtient aucune information sur l'identifiant de ce membre ; la
25 signature est anonyme. Le destinataire a toutefois la possibilité de s'adresser à l'autorité de confiance qui peut déterminer l'identité du signataire à partir de l'identifiant chiffré, au moyen d'une clé publique de l'autorité de confiance, qui accompagne la signature anonyme de groupe. L'autorité de confiance peut donc lever l'anonymat à tout moment.

30 Après constitution auprès de l'autorité de confiance, un groupe peut évoluer. Selon un premier type d'évolution, de nouveaux individus peuvent devenir membres du groupe. Selon un deuxième type d'évolution, des membres peuvent disparaître, soit par le départ d'un individu du groupe, soit par l'exclusion d'un individu du groupe ; pour ce type d'évolution, on parle de révocation. A chaque évolution du groupe,
35 l'autorité de confiance est confrontée au problème de donner ou de retirer à un membre

du groupe les moyens de produire une signature anonyme du groupe. Le premier problème posé, qui réside dans l'attribution des moyens de produire une signature anonyme du groupe à un nouveau membre, est résolu en utilisant un des algorithmes de génération de clé publique/clé privée connus qui permettent d'associer à une même
5 clé publique autant de clés privées que nécessaire. Un exemple d'un tel algorithme est décrit dans l'article de J.Camenisch et M.Michels qui a pour référence "Efficient group signature signature schemes for large groups", In B.Kaliski, editor, Advances in Cryptology – CRYPTO97, volume 1296 of LNCS, pages 410 à 424, Springer-Verlag, 1997.

10 Le second problème posé, qui réside dans le fait de retirer à un individu ces moyens, présente différentes solutions connues qui sont des procédés de révocation.

Un premier de ces procédés est décrit dans l'article suivant de E. Bresson et J. Stern, « Efficient Revocation in group Signatures », in K. Kim, editor, Public Key Cryptography – PKC 2001, volume 1992 of LNCS, pages 190-206, Springer-Verlag,
15 2001. Ce procédé repose sur le fait que chaque membre d'un groupe possède un identifiant qui lui est propre. Etant donné que la signature doit rester anonyme, il n'est pas possible de dévoiler cet identifiant. Toutefois, selon le procédé, l'identifiant du signataire est divisé par celui de chaque membre révoqué ; le résultat de la division est toujours différent de 1 si et seulement si le signataire n'est pas lui-même un membre
20 révoqué. Ensuite, le procédé chiffre, avec un algorithme de chiffrement, chacun des résultats de ces divisions et transmet au destinataire ces résultats chiffrés accompagnés d'éléments déterminés. Le destinataire exploite les éléments déterminés et les résultats chiffrés pour vérifier d'une part que les divisions ont été correctement effectuées et d'autre part que tous les résultats sont différents de 1 ; c'est-à-dire pour s'assurer que
25 la signature a été produite par un membre non révoqué.

Ce procédé a pour inconvénient de générer une signature anonyme de groupe dont la longueur et le temps de calcul augmentent proportionnellement au nombre de membres révoqués, étant donné qu'il y a autant de résultats chiffrés et d'éléments déterminés que de membres révoqués.

30 Un deuxième de ces procédés de révocation est décrit dans l'article de H.J. Kim, J.I. Lim et D.H. Lee qui a pour référence « Efficient and Secure Member Deletion in Group Signature Schemes », In D. Won, editor. Information Security and Cryptology – ICISC 2000, volume 2015 of LNCS, pages 150 et s. Springer-Verlag
35 2000. Ce procédé consiste à utiliser trois clés supplémentaires en plus des clés nécessaires à la réussite de la signature de groupe : une clé privée de propriété pour

chaque membre, une clé publique de propriété pour permettre à chaque membre de vérifier la validité de sa clé et une clé publique de renouvellement permettant à chaque membre de modifier sa clé privée de propriété à chaque fois qu'un membre rejoint ou quitte le groupe. Pour chaque nouveau membre et pour chaque révocation d'un

5 membre, l'autorité de confiance modifie la clé publique de propriété et la clé de renouvellement. Chaque membre restant du groupe modifie sa propre clé privée de propriété à l'aide de la clé de renouvellement et vérifie sa validité grâce à la clé publique de propriété. Lors de la signature électronique d'un message, le membre

10 signataire utilise sa clé privée de propriété. Ainsi, le destinataire peut vérifier la signature électronique à l'aide de la clé publique de propriété. Ce procédé a pour inconvénient d'être d'application particulière car il est prouvé sûre uniquement dans un schéma de signature de groupe particulier qui correspond à celui présenté dans l'article de J. Camenisch, M. Michels, ayant pour référence « A group Signature Scheme with Improved Efficiency », In K. Ohta et D. Pei, editors, *Advances in Cryptology – ASIACRYPT'98*, volume 1514 of LNCS, pages 160-174. Springer-Verlag, 1998. En

15 outre, ce procédé est désavantageux en ce qu'il impose des calculs à chaque membre à chaque fois qu'un membre rejoint ou quitte le groupe ; or, ces calculs peuvent devenir fréquents si la dynamique du groupe est importante.

20 Un des objectifs de l'invention est de remédier aux inconvénients des méthodes connues et précédemment décrites.

A cet effet, l'invention a pour objet un procédé cryptographique mis en œuvre par une carte à puce d'un ensemble de cartes à puce appartenant chacune à une première entité qui peut être différente pour chaque carte à puce, chaque carte à puce étant équipée d'une puce comprenant un moyen de mémorisation dans lequel sont

25 mémorisés une clé secrète et un identifiant de la première entité propriétaire de la carte à puce et comprenant un moyen de calcul dans lequel est implanté un algorithme de cryptographie ayant pour arguments d'entrée au moins la clé secrète. Le procédé cryptographique selon l'invention comprend les étapes qui consistent :

- avant tout calcul par le moyen de calcul de la puce de la carte à puce, à lire
- 30 par la puce dans un moyen de mémorisation d'une seconde entité une liste d'identifiants des premières entités propriétaires d'une carte à puce, cette liste étant liée à chaque état attribué à chacune des premières entités par la seconde entité,

- à comparer par la puce l'identifiant mémorisé dans le moyen de mémorisation de la puce et le contenu de la liste, pour autoriser ou interdire tout calcul du moyen de calcul en fonction du résultat de la comparaison.

L'invention a en outre pour objet une carte à puce pour la mise en œuvre d'un tel procédé.

Le procédé selon l'invention consiste à interdire par la puce de la carte à puce tout calcul cryptographique implanté dans la puce, lorsque le propriétaire de la carte à puce est dans un état positionné à révoqué par la seconde entité. Dans le cas contraire, le propriétaire de la carte à puce est dans un état positionné à non révoqué, la puce autorise le calcul. La seconde entité, qui est typiquement une autorité de confiance, met à jour une liste des identifiants de chaque propriétaire de carte à puce dont l'état est révoqué ou non révoqué. Cette liste est mémorisée par la seconde entité dans un moyen de mémorisation connecté à un réseau de télécommunication. Ce moyen est accessible par la carte à puce via un lecteur de carte à puce associé à un ordinateur tel un ordinateur personnel, lui-même connecté au réseau de télécommunication.

Ainsi, un membre révoqué ne peut pas effectuer de calcul cryptographique s'il est révoqué. Si l'algorithme de cryptographie implanté dans la puce est un algorithme de calcul de signature anonyme, le propriétaire de la carte à puce ne peut pas signer un fichier au moyen de sa carte à puce s'il est révoqué.

Le procédé selon l'invention peut être réalisé de manière particulière ; certaines réalisations sont listées ci-après de façon non-exhaustive.

Selon une réalisation particulière, la liste comprend les identifiants des entités révoquées, dans ce cas la liste est dite liste noire.

Selon une autre réalisation particulière, la liste comprend les identifiants des entités non révoquées, dans ce cas la liste est dite liste blanche.

Selon une autre réalisation particulière, la liste est signée par la seconde entité ; la seconde entité calcule cette signature au moyen d'un algorithme de signature. Cet algorithme peut-être un algorithme asymétrique à clé publique tel que RSA, RSA étant les initiales des inventeurs. Avant toute autorisation, la puce vérifie la validité de la signature. Dans le cas d'un algorithme de signature à clé publique, la puce vérifie la signature au moyen du même algorithme asymétrique en prenant comme argument d'entrée la clé publique. Cette vérification permet d'authentifier la liste dans son ensemble et donc de vérifier son intégrité.

Selon une autre réalisation particulière, chaque identifiant de la liste est associé à une valeur de comptage, chaque ensemble formé de l'identifiant et de la valeur de

comptage associé étant signé par la seconde entité ; la liste comprend une valeur du nombre d'identifiants listés dans la liste ainsi que la signature de cette valeur. Chaque signature est calculée de la même manière que dans la réalisation précédente. Avant toute autorisation, la puce vérifie la validité de chaque signature. Cette vérification permet d'authentifier chaque identifiant de la liste, la valeur de comptage associé et la valeur lue du nombre d'identifiants. En outre, la puce incrémente un compteur à chaque lecture d'un identifiant en prenant en compte la valeur de comptage associée à l'identifiant lu puis elle compare ce compteur à la valeur authentifiée avant toute autorisation de calcul par la puce. Cette comparaison permet de vérifier l'intégrité du nombre d'identifiants lus.

Selon une autre réalisation particulière, la puce n'a accès par lecture dans le moyen de mémorisation de la seconde entité qu'à une trace des identifiants de la liste et à une signature de cette trace. Cette trace est une chaîne de bits plus courte que la liste et est obtenue par un codage particulier de la liste. Selon cette réalisation, la comparaison porte sur l'identifiant mémorisé dans le moyen de mémorisation de la puce et la trace et, avant autorisation par la puce de tout calcul du moyen de calcul, la puce vérifie la validité de la signature pour authentifier la trace.

D'autres caractéristiques et avantages de l'invention apparaîtront lors de la description qui suit et qui est faite en regard des figures suivantes annexées de modes particuliers de réalisation donnés à titre d'exemples non limitatifs.

La figure 1 est un organigramme d'un procédé cryptographique selon l'invention.

La figure 2 est un organigramme d'un premier mode de réalisation d'un procédé cryptographique selon l'invention.

La figure 3 est un organigramme d'un deuxième mode de réalisation d'un procédé cryptographique selon l'invention.

La figure 4 est un organigramme d'un exemple de mise en œuvre par une puce du deuxième mode de réalisation d'un procédé cryptographique selon l'invention.

La figure 5 est un schéma d'une carte à puce selon l'invention.

La figure 1 est un organigramme d'un procédé cryptographique selon l'invention.

Le procédé est mis en œuvre par une carte à puce d'un ensemble de cartes à puce appartenant chacune à une première entité. Chaque première entité, typiquement une personne physique, peut être différente pour chaque carte à puce. Chaque carte à puce est équipée d'une puce qui comprend un moyen de mémorisation et un moyen de

calcul. Une clé secrète et un identifiant de la première entité propriétaire de la carte à puce sont mémorisés dans le moyen de mémorisation. Un algorithme de cryptographie ayant pour arguments d'entrée au moins la clé secrète est implanté dans le moyen de calcul.

5 Cet algorithme de cryptographie peut tout aussi bien être un algorithme de calcul de signature de groupe, un algorithme de chiffrement ou un algorithme de déchiffrement.

10 Un exemple d'algorithme de calcul de signature de groupe est décrit dans l'article de J.Camenisch et M.Stadler qui a pour référence "Efficient group signature schemes for large groups", In B.Kaliski, editor, Advances in Cryptology – CRYPTO97, volume 1296 of LNCS, pages 410 à 424, Springer-Verlag, 1997. Une autre description est donnée dans l'article de J.Camenisch et M.Michels qui a pour référence "A group signature scheme with improved efficiency. In K.Ohta et D.Pei, editors, Advances in cryptology- ASIACRYPT'98, volume 1514 of LNCS, pages 160-174. Springer-Verlag, 1998. L'algorithme RSA peut être utilisé comme algorithme de
15 chiffrement / déchiffrement.

Le procédé comprend plusieurs étapes ci-après décrites. Pour signer, chiffrer ou déchiffrer, la puce active le moyen de calcul qui calcule une donnée de sortie en fonction d'arguments d'entrée présentés en entrée de l'algorithme de cryptographie.

20 Avant tout calcul 1 par le moyen de calcul de la puce de la carte à puce, le procédé consiste à lire 2 par la puce dans un moyen de mémorisation d'une seconde entité une liste d'identifiants des premières entités propriétaires d'une carte à puce. De manière totalement équivalente, le procédé peut écrire dans la puce une liste lue dans le moyen de mémorisation d'une seconde entité. Dans la suite de la description, toute
25 opération de lecture peut être remplacée de manière totalement équivalente par une opération d'écriture. La liste est liée à chaque état attribué à chacune des premières entités par la seconde entité ; l'état est positionné à révoqué ou non révoqué par la seconde entité. La liste contient soit les premières entités révoquées, il s'agit d'une liste noire, soit les premières entités non révoquées, il s'agit d'une liste blanche. La seconde
30 entité mémorise cette liste dans un moyen de mémorisation qui est accessible via un réseau de télécommunication. Il peut s'agir d'un espace mémoire sur un serveur ou sur une mémoire de masse par exemple.

Le procédé consiste ensuite à comparer 3 par la puce l'identifiant mémorisé dans le moyen de mémorisation de la puce et le contenu de la liste. Si, à l'issue de la
35 comparaison, la puce trouve que la première entité est révoquée alors la puce interdit 4

tout calcul du moyen de calcul. Par contre, si, à l'issue de la comparaison, la puce trouve que la première entité est non révoquée alors la puce autorise 5 tout calcul du moyen de calcul.

Pour mettre en œuvre par une puce la comparaison, le processus est le suivant.

5 La puce initialise un témoin à un. Elle compare successivement chaque identifiant lu à l'identifiant mémorisé dans la puce ; s'il n'y a pas identité la puce positionne le témoin à un sinon elle positionne le témoin à zéro. A l'issue de la comparaison entre chaque identifiant lu et l'identifiant mémorisé dans la puce, la puce interdit tout calcul du moyen de calcul si le témoin est à un. Par contre si le témoin est à zéro, la puce

10 autorise tout calcul du moyen de calcul.

Un premier mode de réalisation d'un procédé cryptographique selon l'invention est illustré par la figure 2. Ce mode comprend les étapes décrites en regard de la figure 1, elles ne sont pas re-décrites, et des étapes complémentaires ci-après décrites. La puce lit 10 en outre, en même temps que la liste et dans la même zone mémoire, une

15 signature de cette liste. La signature est préalablement calculée par un moyen de calcul de la seconde entité. Avant autorisation 5 par la puce de tout calcul du moyen de calcul, la puce vérifie 11 la validité de la signature pour authentifier la liste et pour vérifier son intégrité. Si la signature n'est pas valide, la puce interdit 4 tout calcul du moyen de calcul, sinon elle autorise 5 le calcul.

20 Un deuxième mode de réalisation d'un procédé cryptographique selon l'invention est illustré par la figure 3. Ce mode comprend les étapes décrites en regard de la figure 1, elle ne sont pas re-décrites, et des étapes complémentaires ci-après décrites. La puce lit 12, 13, 14 en outre, en même temps que la liste et dans la même zone mémoire, une valeur de comptage associée à chaque identifiant, une signature

25 pour chaque ensemble composé d'un identifiant de cette liste et d'une valeur de comptage associée, la valeur du nombre d'identifiants de cette liste ainsi qu'une signature de cette valeur. La signature de chaque identifiant et de sa valeur de comptage associée, la valeur du nombre d'identifiants et la signature de cette valeur sont préalablement calculées par un moyen de calcul de la seconde entité et

30 mémorisées dans la même zone mémoire que la liste. La puce incrémente 15 un compteur à chaque lecture par la puce d'un identifiant en prenant en compte la valeur de comptage associée à l'identifiant, pour compter le nombre d'identifiants. Avant autorisation 5 par la puce de tout calcul du moyen de calcul, la puce vérifie 16, 17 la validité de chacune des signatures pour authentifier respectivement chaque identifiant

de la liste et le nombre d'identifiants. Si une des signatures n'est pas valide, la puce interdit 4 le calcul.

A l'issue de la lecture de la liste des identifiants, la puce compare 18 la valeur de son compteur à la valeur lue du nombre d'identifiants. Si ces valeurs sont différentes, la puce interdit 4 tout calcul du moyen de calcul. Si ces valeurs sont identiques, la puce vérifie 17 la validité de la signature de la valeur du nombre d'identifiants. La figure 5 illustre une mise en œuvre par une puce de ce deuxième mode. La puce initialise 19 un témoin à un et un compteur à zéro. La puce lit 20 un identifiant de la liste et la valeur de comptage associée, lit leur signature et incrémente le compteur. La puce compare 21 le témoin à zéro. Si le témoin est différent de zéro, la puce compare 22 l'identifiant lu à l'identifiant mémorisé dans la puce ; s'il n'y a pas identité la puce positionne 23 le témoin à un sinon elle positionne 24 le témoin à zéro. A l'issue de la comparaison entre l'identifiant lu et l'identifiant mémorisé dans la puce ou si le témoin est égal à zéro, la puce vérifie 25 la validité de la signature de l'ensemble composé de l'identifiant lu et de la valeur de comptage associée. Si la signature n'est pas valide, la puce interdit 4 tout calcul du moyen de calcul. Par contre si la signature est valide, la puce se met en attente de l'identifiant suivant ou 26, s'il n'y a plus d'identifiant dans la liste, la puce lit 27 la valeur du nombre d'identifiants et sa signature. La puce compare 18 la valeur du nombre d'identifiants avec la valeur de son compteur. Si ces valeurs sont différentes, la puce interdit 4 tout calcul du moyen de calcul, sinon la puce vérifie 17 la validité de la signature de la valeur du nombre lu. Si la signature n'est pas valide, la puce interdit 4 tout calcul du moyen de calcul. Par contre si la signature est valide, la puce teste 28 la valeur du nombre d'identifiants. Si le témoin est différent de un, la puce interdit 4 tout calcul du moyen de calcul ; le membre est révoqué. Sinon, la puce autorise 5 tout calcul du moyen de calcul.

Selon une variante au premier mode décrit en regard de la figure 2, la puce n'a accès par lecture dans le moyen de mémorisation de la seconde entité qu'à une trace des identifiants de la liste et à une signature de cette trace. La trace est une chaîne de bits plus courte que la liste et est obtenue par un codage de la liste selon par exemple une méthode dite du "Superimposed Coding". Cette méthode est décrite dans l'article de D.E. Knuth, "The Art of Computer Programming, Volume 3 / Sorting and searching. Addison-Wesley Publishing Company, pages 559-563, 1973. Une mise en œuvre par une puce de cette variante est décrite au moyen de l'exemple qui suit.

Initialisation :

Soit Y l'ensemble des éléments dont on veut obtenir une trace, par exemple la liste des identifiants. Y est initialisé à l'ensemble vide \emptyset .

On veut que les éléments de Y soient tous représentés dans une chaîne (la trace) de taille fixe. On fixe cette taille à $M = 16$ bits.

5 On fixe trois fonctions de hachage (h_1 , h_2 et h_3). Ces trois fonctions prennent en entrée un élément de taille quelconque, par exemple un identifiant, et donnent en sortie un élément de taille fixe. Pour l'exemple la taille est telle que l'élément est un nombre compris entre 0 et 15 $\Rightarrow h_i : \{0,1\}^* \rightarrow \{0,1\}^4$ si on parle en terme de bits ; un nombre codé sur quatre bits est compris entre 0 = 0000 et 15 = 1111. On suppose en outre, à
10 priori, que les trois fonctions de hachage ne donnent jamais le même résultat sur un même élément d'entrée.

Soit B la chaîne résultante. Elle a donc une longueur de 16 bits. C'est la trace de l'ensemble Y que lit la puce. On initialise $B = 0000000000000000$ ($= b_{15}b_{14}b_{13}\dots b_1b_0$, c'est-à-dire que chaque i -ème bit de B est noté b_i).

15 Etape 1 : $y_{258} \rightarrow Y (Y = \{y_{258}\})$; on ajoute un élément à Y .

$h_1(y_{258}) = 2$, $h_2(y_{258}) = 13$, $h_3(y_{258}) = 12$; on calcule les condensés du nouvel élément selon les trois fonctions de hachage, on obtient trois nombres distincts compris entre 0 et 15.

20 On met des 1 aux endroits de B correspondants aux trois nombres précédemment obtenus. Les nombres précédemment obtenus sont 2, 13 et 12, par conséquent on place les bits 2, 13 et 12 de B à 1, $B = 001100000000100$.

Etape 2 : $y_{21} \rightarrow Y (Y = \{y_{258}, y_{21}\})$; on ajoute un deuxième élément à Y .

25 $h_1(y_{21}) = 5$, $h_2(y_{21}) = 2$, $h_3(y_{21}) = 8$; on calcule les condensés du nouvel élément selon les trois fonctions de hachage, on obtient trois nombres distincts compris entre 0 et 15.

On met des 1 aux endroits de B correspondants aux trois nombres précédemment obtenus. Les nombres précédemment obtenus sont 2, 13 et 12, par conséquent on place les bits 2, 13 et 12 de B à 1, $B = 0011000100100100$.

Etape 3 : $y_{928} \rightarrow Y (Y = \{y_{258}, y_{21}, y_{928}\})$; on ajoute un troisième élément à Y .

30 $h_1(y_{928}) = 9$, $h_2(y_{928}) = 0$, $h_3(y_{928}) = 1$.

Trois nouveaux bits sont mis à 1, $B = 0011001100100111$.

A l'issue de cette étape, on possède un ensemble Y contenant trois valeurs. La représentation de Y est la chaîne (la trace) B qui est 0011001100100111 ($= 13095$ en décimal ou 3327 en hexadécimal). La puce lit B et est capable de déterminer si son

propre identifiant est contenu dans Y ou non avec une probabilité plus ou moins faible en mettant en œuvre un test particulier.

Soit la puce dont l'identifiant est y_{822} . Cette puce veut tester si elle a le droit d'effectuer le calcul cryptographique. La puce effectue les opérations suivantes.

5 $h_1(y_{822}) = 8, h_2(y_{822}) = 14, h_3(y_{822}) = 7$; la puce calcule des condensés liés à son identifiant. On peut considérer que la puce les garde en mémoire même si le calcul n'est pas long. Ensuite, la puce teste si chacun des bits correspondant aux trois nombres résultant des fonctions de hachage est à 0 ou à 1. S'ils sont tous à 1, alors il y a des chances pour que l'identifiant soit dans la liste, auquel cas elle refuse de faire
10 l'opération cryptographique (mais elle peut se tromper...). Par contre, si elle tombe sur un 0, alors elle est sûre que l'identifiant n'est pas dans la liste ; en effet, dans le cas contraire, le bit correspondant au résultat de la fonction de hachage est mis à 1 lors du rajout de l'identifiant correspondant dans Y .

$b_7 = 1$? Oui \Rightarrow on continue

15 $b_{14} = 1$? Non $\Rightarrow y_4 \notin Y$. C'est vrai. Dès que la puce tombe sur un 0, elle est sûre que son identifiant n'est pas dans Y .

Soit la puce dont l'identifiant est y_{258} . Cette puce veut tester si elle a le droit d'effectuer le calcul cryptographique. La puce effectue les opérations suivantes.

$h_1(y_{422}) = 2, h_2(y_{422}) = 13, h_3(y_{422}) = 12.$

20 $b_2 = 1$? Oui \Rightarrow on continue

$b_{13} = 1$? Oui \Rightarrow on continue

$b_{12} = 1$? Oui $\Rightarrow y_{422} \in Y$. C'est vrai. Dans cet exemple, la puce trouve trois 1. La puce considère donc qu'elle est révoquée, ce qui est vrai puisqu'on a mis y_{258} dans Y à l'étape 1.

25 La figure 5 illustre de manière schématique une carte à puce selon l'invention.

La carte 30 à puce est équipée d'une puce 31 qui comprend au moins un moyen 32 de mémorisation, un moyen 33 de calcul et un moyen 34 de lecture dans un moyen de mémorisation d'une seconde entité via un réseau de télécommunication et un moyen 35 d'autorisation du moyen de calcul.

30 Le moyen 32 de mémorisation mémorise une clé secrète et un identifiant d'une première entité propriétaire de la carte à puce.

Dans le moyen 33 de calcul est implanté un algorithme de cryptographie ayant pour arguments d'entrée au moins la clé secrète. Le moyen 33 de calcul est en liaison avec le moyen 32 de mémorisation.

Le moyen 34 de lecture permet de lire une liste d'identifiants dans le moyen de mémorisation d'une seconde entité, via un réseau de télécommunication. Le moyen 34 de lecture transmet les données lues au moyen 33 de calcul ou/et au moyen 35 d'autorisation par des liaisons avec chacun de ces moyens.

5 Le moyen 35 d'autorisation autorise tout calcul par le moyen 33 de calcul en fonction du résultat d'une comparaison entre l'identifiant et le contenu de la liste.

Une telle carte 30 à puce permet la mise en œuvre d'un procédé selon l'invention.

10 Une première application d'un procédé selon l'invention est le vote électronique. Le vote électronique se déroule en deux phases :

- une inscription sur une liste électorale auprès d'une autorité administrative,
- une opération de vote auprès d'une urne connectée via un réseau de communication à un serveur d'une administration des votes.

15 Lors de l'inscription, l'électeur obtient dans une carte à puce, une clé privée personnelle et une clé privée de groupe. La signature anonyme que peut produire l'électeur au moyen de sa carte à puce, et à partir de sa clé privée personnelle, est dite "corrélable". Ceci signifie que, dans le cas où l'électeur tenterait de signer de manière anonyme un second bulletin de vote en produisant une signature anonyme, ce bulletin serait rejeté par l'urne. En effet, la signature anonyme étant corrélable, l'urne est en
20 mesure de vérifier qu'il s'agit d'une seconde signature anonyme.

Un électeur malveillant ne peut pas prétendre avoir perdu sa clé privée de groupe, en recevoir une autre et être en mesure de voter deux fois. En effet, la mise en œuvre d'un procédé selon l'invention permet de lui interdire l'utilisation de la première clé privée de groupe ; cette clé privée de groupe est mise à jour au moment où il
25 déclare avoir perdu la première clé privée de groupe. Cette perte est gérée par la mise en œuvre d'un procédé selon l'invention comme une révocation du membre.

Une seconde application d'un procédé selon l'invention est un service d'enchères électroniques. Les enchères font appel à trois protagonistes : un serveur d'enchères, une autorité de confiance et un client. L'ensemble des clients forme un
30 groupe dit groupe des clients. Un utilisateur désirant s'inscrire au groupe des clients doit s'adresser à l'autorité de confiance qui lui fournit sa clé privée personnelle dans une carte à puce. Il obtient ainsi le droit de produire une signature anonyme de groupe. Muni de ce droit, il peut signer à l'aide de sa carte à puce chacune de ses enchères de manière anonyme. Lors d'une enchère pour un certain produit, chaque membre du
35 groupe des clients peut enchérir en signant un message contenant notamment le produit

mis en vente et le montant de son enchère. Le serveur d'enchères peut vérifier l'appartenance au groupe et donc la validité de l'enchère en vérifiant la signature anonyme de groupe. Le vainqueur est celui qui donne la dernière enchère avant l'adjudication. Le dernier message reçu par le serveur d'enchères est donc celui du vainqueur. Le serveur adresse alors ce message et la signature anonyme de groupe correspondante à l'autorité de confiance qui est la seule capable d'en lever l'anonymat et donc de déterminer l'identité physique de l'acheteur du produit mis aux enchères.

Les enchères mettent en jeu des groupes dynamiques : de nouvelles personnes peuvent chaque jour s'inscrire au groupe, un membre peut quitter le groupe ou être exclu pour fraude à tout moment. Il est donc indispensable de mettre en place un système de révocation pour empêcher qu'un membre révoqué ne puisse se servir de sa signature de manière frauduleuse. En effet, le membre révoqué pourrait continuer à utiliser sa clé pour participer aux enchères et fausser le bon déroulement de ces dernières par exemple en faisant monter le montant. Et, s'il prend soin de se retirer suffisamment tôt du processus de façon à ne pas remporter les enchères en question, alors cette fraude n'est pas détectée puisque seule l'identité du gagnant est finalement révélée. La mise en œuvre d'un procédé selon l'invention permet de résoudre le problème de révocation d'un ou de membre(s) du groupe.

Une troisième application d'un procédé selon l'invention est le paiement électronique. Elle met en jeu quatre protagonistes : un client, un commerçant, une banque et une autorité de confiance. Chaque client doit se faire identifier par le système et obtenir une clé privée de groupe mémorisée dans une carte à puce, avant de pouvoir effectuer sa première transaction. Pour effectuer un paiement, le client doit retirer des pièces électroniques auprès de sa banque. Les pièces qu'il retire sont anonymes grâce à l'utilisation d'un mécanisme dit de signature aveugle. La dépense d'une pièce C chez un commerçant se fait de la manière suivante : le client génère au moyen de sa carte à puce une signature de groupe portant sur les pièces C et transmet l'ensemble signature et pièces C au commerçant. Le commerçant vérifie la signature de la banque attachée à chaque pièce C et vérifie la signature de groupe. Si chacune des deux signatures est valide, le commerçant accepte la transaction. A un moment donné du jour, le commerçant transmet à sa banque les signatures et les pièces reçues en paiement pour virement à son compte. En cas de fraude, par exemple par la réutilisation d'une même pièce dans plusieurs transactions, la banque envoie la signature de groupe portant sur la pièce litigieuse à l'autorité de confiance afin qu'elle identifie le client indélicat et sanctionne le contrevenant.

5 Un mécanisme fiable de révocation des clés compromises est nécessaire afin d'éviter une fraude du type suivant : un client malhonnête signale à l'autorité de confiance la perte de sa clé privée s et décline alors toute responsabilité pour les fraudes qui pourraient être commises avec s . Le client remet sa clé à son complice, lequel peut alors utiliser s pour signer les pièces c qu'il a légitimement retirées à la banque, puis les dépenser autant de fois qu'il le souhaite. Un procédé selon l'invention permet de résoudre le problème de la révocation des clés s .

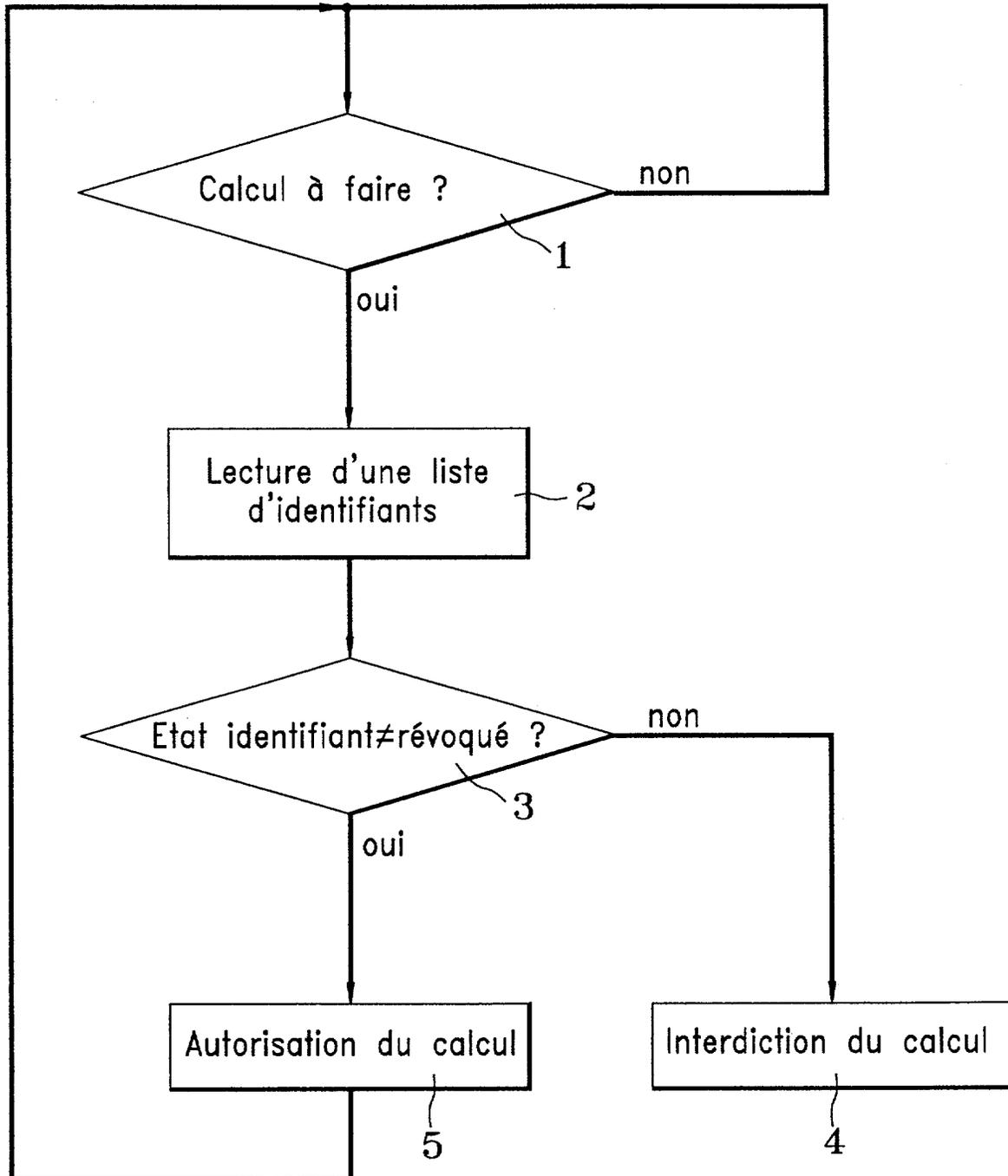
REVENDICATIONS

1. Procédé cryptographique mis en œuvre par une carte (30) à puce d'un ensemble de cartes à puce appartenant chacune à une première entité qui peut être différente
5 pour chaque carte à puce, chaque carte à puce étant équipée d'une puce (31) comprenant un moyen (32) de mémorisation dans lequel sont mémorisés une clé secrète et un identifiant de la première entité propriétaire de la carte (30) à puce et comprenant un moyen (33) de calcul dans lequel est implanté un algorithme de cryptographie ayant pour arguments d'entrée au moins la clé secrète, caractérisé
10 en ce qu'il comprend les étapes qui consistent :
 - avant tout calcul par le moyen (33) de calcul de la puce (31) de la carte (30) à puce, à lire (2) par la puce (31) dans un moyen de mémorisation d'une seconde entité une liste d'identifiants des premières entités propriétaires d'une carte à puce, cette liste étant liée à chaque état attribué à chacune des
15 premières entités par la seconde entité,
 - à comparer (3) par la puce (31) l'identifiant mémorisé dans le moyen (32) de mémorisation de la puce (31) et le contenu de la liste, pour autoriser (5) ou interdire (4) tout calcul du moyen (33) de calcul en fonction du résultat de la comparaison.
20
2. Procédé cryptographique selon la revendication 1, dans lequel la liste comprend l'ensemble des premières entités dont l'état est positionné à révoqué par la seconde entité et dans lequel l'autorisation (5) de calcul est donnée par la puce (31) uniquement si l'identifiant mémorisé dans le moyen (32) de mémorisation de la
25 puce (31) n'appartient pas à la liste.
3. Procédé cryptographique selon la revendication 1, dans lequel la liste comprend l'ensemble des premières entités dont l'état est positionné à non révoqué par la seconde entité et dans lequel l'autorisation (5) de calcul est donnée par la puce
30 (31) uniquement si l'identifiant mémorisé dans le moyen (32) de mémorisation de la puce (31) appartient à la liste.
4. Procédé cryptographique selon l'une des revendications 1 à 3, comprenant en outre les étapes qui consistent :

- en même temps que la lecture (2) de la liste, à lire (10) une signature de cette liste par la puce (31) dans le moyen de mémorisation de la seconde entité, la signature ayant été préalablement calculée par un moyen de calcul de la seconde entité,
 - 5 - avant autorisation (5) par la puce de tout calcul du moyen (33) de calcul, à vérifier (11) par la puce (31) la validité de la signature.
5. Procédé cryptographique selon l'une des revendications 1 et 2, comprenant en outre les étapes qui consistent :
- 10 - en même temps que la lecture (2) de la liste, à lire (12) des signatures des identifiants de la liste par la puce (31) dans le moyen de mémorisation de la seconde entité, chaque identifiant ayant donné lieu à une signature préalablement calculée par un moyen de calcul de la seconde entité,
 - en même temps que la lecture (2) de la liste, à lire (13, 14) par la puce (31)
15 dans le moyen de mémorisation de la seconde entité, une valeur du nombre d'identifiants listés dans cette liste ainsi qu'une signature de cette valeur, la valeur et sa signature ayant été préalablement calculées par un moyen de calcul de la seconde entité,
 - avant autorisation (5) par la puce (31) de tout calcul du moyen (33) de
20 calcul, à vérifier (16, 17) par la puce (31) la validité de chacune des signatures,
 - à compter (15) par la puce (31) le nombre d'identifiants contenus dans la liste lue,
 - avant autorisation (5) par la puce (31) de tout calcul du moyen (33) de
25 calcul, à vérifier (18) l'égalité entre la valeur du compteur et la valeur lue.
6. Procédé cryptographique selon l'une des revendications 1 et 2, dans lequel la puce (31) n'a accès par lecture dans le moyen de mémorisation de la seconde entité qu'à une trace des identifiants de la liste et à une signature de cette trace, cette trace
30 étant une chaîne de bits plus courte que la liste et étant obtenue par un codage particulier de la liste, et dans lequel la comparaison (3) porte sur l'identifiant mémorisé dans le moyen (32) de mémorisation de la puce (31) et la trace, et en ce que le procédé comprend en outre l'étape qui consiste :

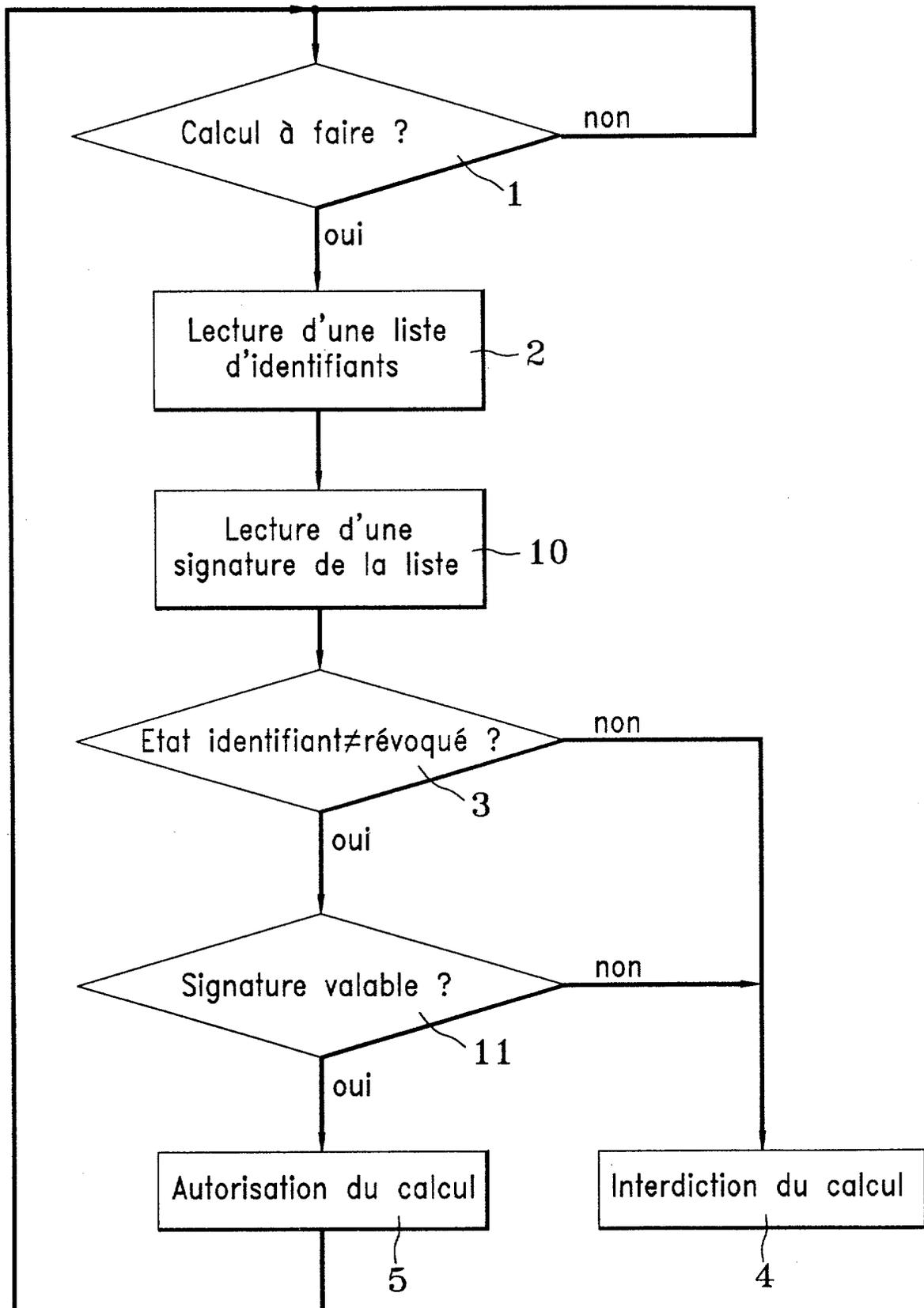
- avant autorisation (5) par la puce (31) de tout calcul du moyen (33) de calcul, à vérifier (11) par la puce (31) la validité de la signature pour authentifier la trace.
- 5 7. Carte (30) à puce pour la mise en œuvre d'un procédé selon l'une des revendications 1 à 7, caractérisée en ce qu'elle (30) est équipée d'une puce (31) qui comprend au moins :
- un moyen (32) de mémorisation d'une clé secrète et d'un identifiant d'une première entité propriétaire de la carte à puce,
 - 10 - un moyen (33) de calcul dans lequel est implanté un algorithme de cryptographie ayant pour arguments d'entrée au moins la clé secrète,
 - un moyen (34) pour lire une liste d'identifiants dans un moyen de mémorisation d'une seconde entité, via un réseau de télécommunication,
 - un moyen (35) pour autoriser tout calcul par le moyen (33) de calcul en
15 fonction du résultat d'une comparaison entre l'identifiant et le contenu de la liste.

FIG. 1

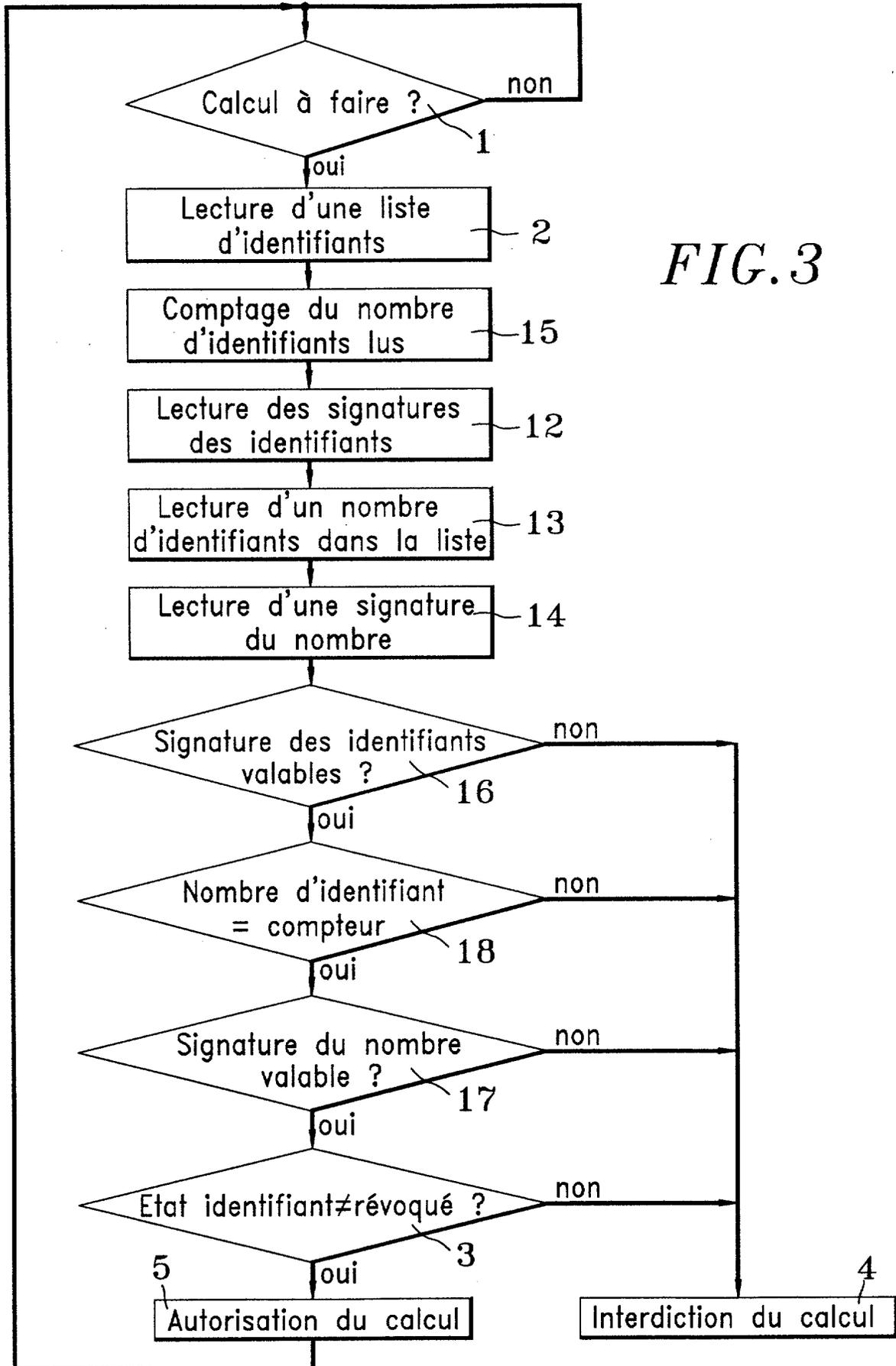


2/5

FIG. 2



3/5



4/5

FIG. 4

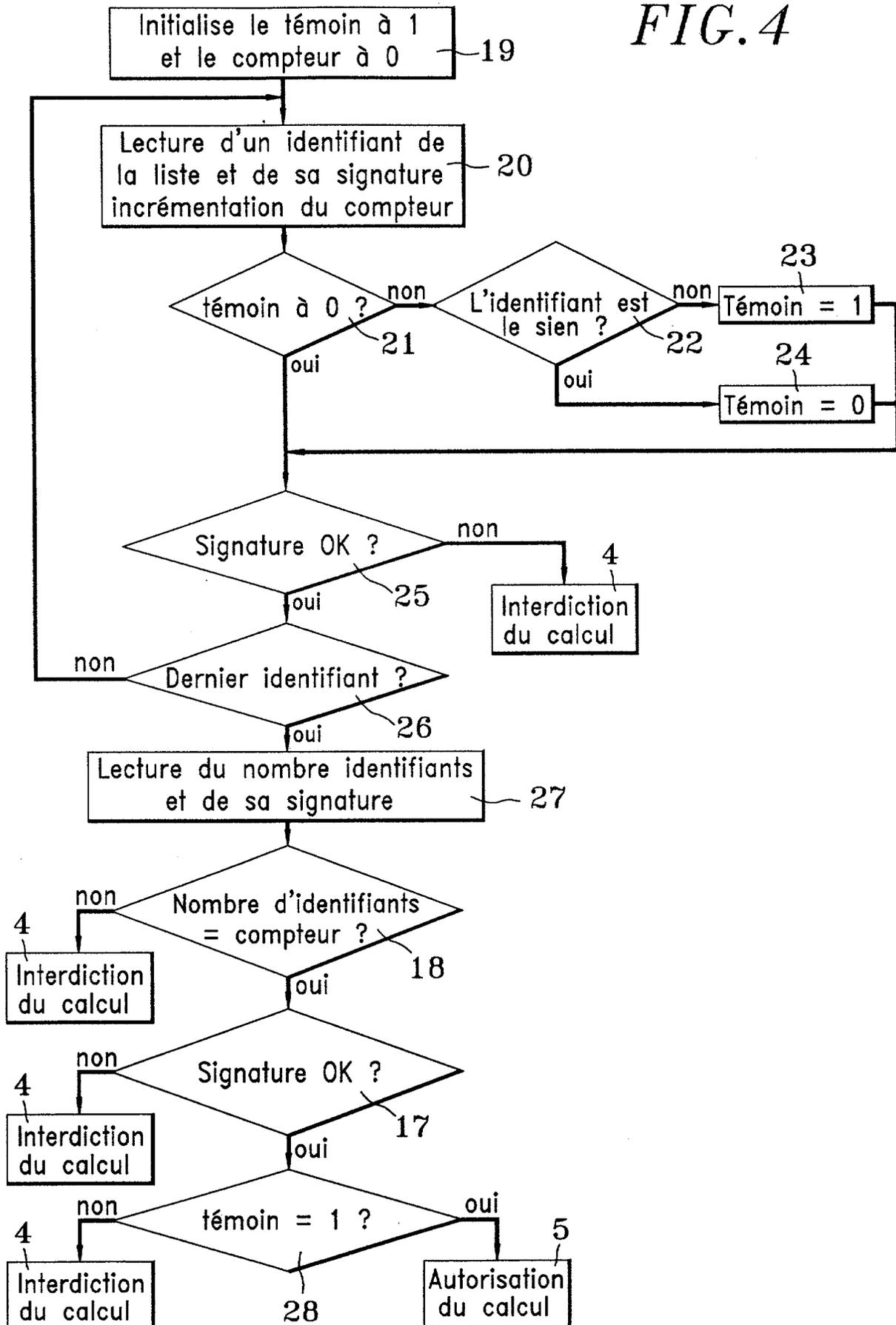
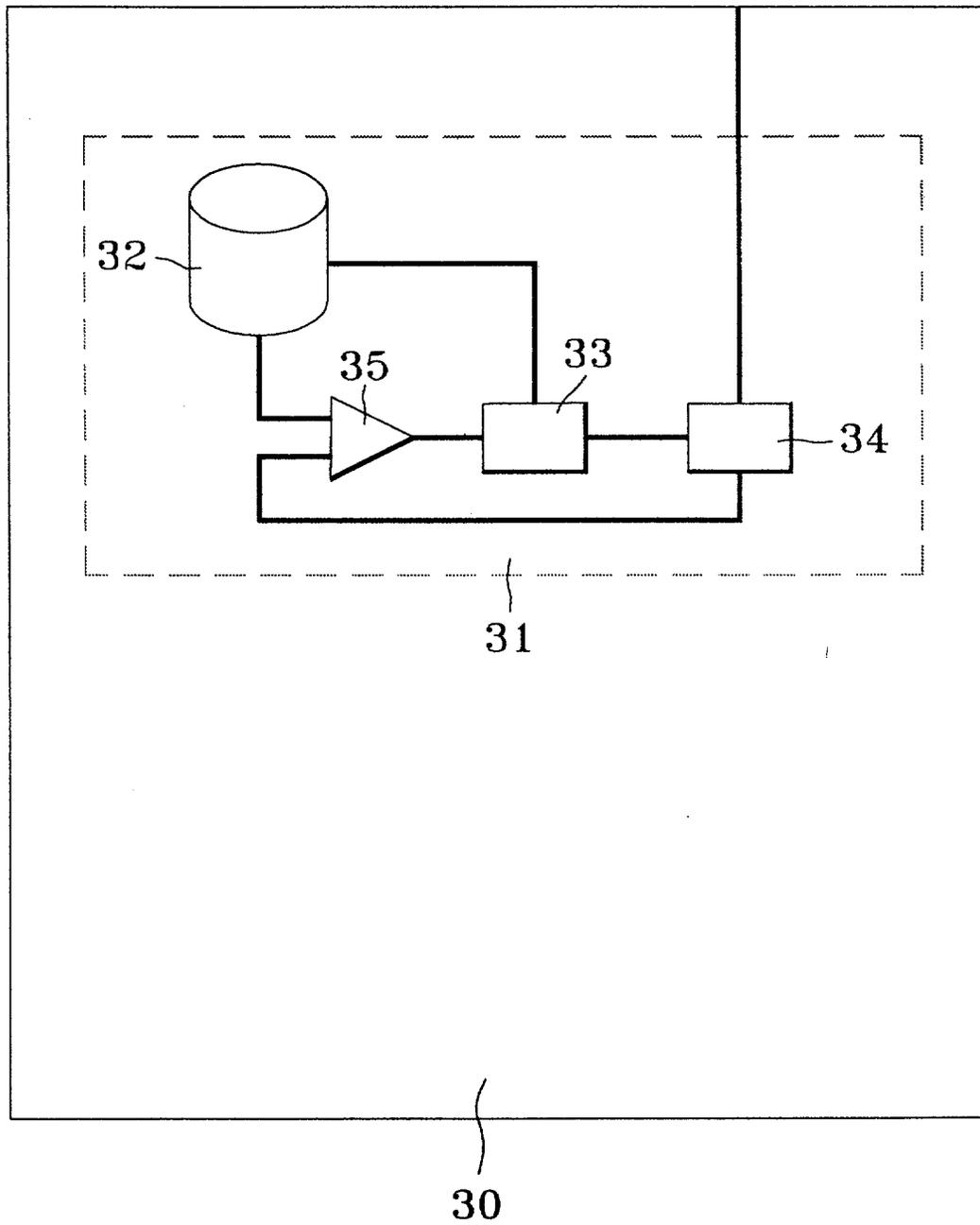


FIG. 5



**RAPPORT DE RECHERCHE
PRÉLIMINAIRE**

N° d'enregistrement
national

établi sur la base des dernières revendications
déposées avant le commencement de la recherche

FA 615175
FR 0200569

DOCUMENTS CONSIDÉRÉS COMME PERTINENTS		Revendication(s) concernée(s)	Classement attribué à l'invention par l'INPI
Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes		
X	WO 00 08610 A (MICROSOFT CORP) 17 février 2000 (2000-02-17) * abrégé * * page 12, ligne 23 - page 19, ligne 2 * * page 9, ligne 21 - page 11, ligne 3 * * page 11, ligne 24 - page 12, ligne 7 * * figures 1-5 * ---	1,2,4,6, 7	H04L9/28 G06K19/07
X	US 5 191 193 A (LE ROUX JEAN-YVES) 2 mars 1993 (1993-03-02) * abrégé * * colonne 1, ligne 24 - colonne 2, ligne 42 * * colonne 3, ligne 38 - colonne 4, ligne 51 * * colonne 5, ligne 30 - ligne 35 * * colonne 5, ligne 52 - colonne 6, ligne 2 * * figures 1-4 * ---	1,2,7	
X	EP 0 378 349 A (VISA INT SERVICE ASS) 18 juillet 1990 (1990-07-18) * abrégé * * page 3, ligne 19 - page 4, ligne 12 * * page 5, ligne 22 - page 6, ligne 27 * * page 13, ligne 4 - ligne 20 * ---	1,2,7	DOMAINES TECHNIQUES RECHERCHÉS (Int.CL.7)
A	* abrégé * * page 3, ligne 19 - page 4, ligne 12 * * page 5, ligne 22 - page 6, ligne 27 * * page 13, ligne 4 - ligne 20 *	6	H04L G07F
A	US 4 734 564 A (BOSTON VINCENT ET AL) 29 mars 1988 (1988-03-29) * abrégé * * colonne 3, ligne 33 - colonne 4, ligne 6 * * colonne 5, ligne 38 - ligne 52 * * colonne 6, ligne 14 - ligne 24 * ---	1,7	
	-/--		
Date d'achèvement de la recherche		Examineur	
4 novembre 2002		Dujardin, C	
CATÉGORIE DES DOCUMENTS CITÉS			
X : particulièrement pertinent à lui seul Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie A : arrière-plan technologique O : divulgation non-écrite P : document intercalaire		T : théorie ou principe à la base de l'invention E : document de brevet bénéficiant d'une date antérieure à la date de dépôt et qui n'a été publié qu'à cette date de dépôt ou qu'à une date postérieure. D : cité dans la demande L : cité pour d'autres raisons & : membre de la même famille, document correspondant	

3

EPO FORM 1503 12.99 (P04C14)

**RAPPORT DE RECHERCHE
PRÉLIMINAIRE**

N° d'enregistrement
national

établi sur la base des dernières revendications
déposées avant le commencement de la recherche

FA 615175
FR 0200569

DOCUMENTS CONSIDÉRÉS COMME PERTINENTS		Revendication(s) concernée(s)	Classement attribué à l'invention par l'INPI
Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes		
D,A	KNUTH: "Art of Computer Programming. Volume 3. Sorting and Searching. " 1973 , ADDISON-WESLEY , READING, MASSACHUSETTS XP001109108 * page 559, ligne 19 - page 563, ligne 2 *	6	
			DOMAINES TECHNIQUES RECHERCHÉS (Int.CL.7)
		Date d'achèvement de la recherche	Examineur
		4 novembre 2002	Dujardin, C
<p>CATÉGORIE DES DOCUMENTS CITÉS</p> <p>X : particulièrement pertinent à lui seul Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie A : arrière-plan technologique O : divulgation non-écrite P : document intercalaire</p> <p>T : théorie ou principe à la base de l'invention E : document de brevet bénéficiant d'une date antérieure à la date de dépôt et qui n'a été publié qu'à cette date de dépôt ou qu'à une date postérieure. D : cité dans la demande L : cité pour d'autres raisons & : membre de la même famille, document correspondant</p>			

3

EPO FORM 1503 12.99 (P04C14)

**ANNEXE AU RAPPORT DE RECHERCHE PRÉLIMINAIRE
RELATIF A LA DEMANDE DE BREVET FRANÇAIS NO. FR 0200569 FA 615175**

La présente annexe indique les membres de la famille de brevets relatifs aux documents brevets cités dans le rapport de recherche préliminaire visé ci-dessus.
Les dits membres sont contenus au fichier informatique de l'Office européen des brevets à la date du 04-11-2002
Les renseignements fournis sont donnés à titre indicatif et n'engagent pas la responsabilité de l'Office européen des brevets, ni de l'Administration française

Document brevet cité au rapport de recherche		Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
WO 0008610	A	17-02-2000	WO 0008610 A1	17-02-2000
US 5191193	A	02-03-1993	FR 2653248 A1	19-04-1991
			CA 2027344 A1	14-04-1991
			DE 69014817 D1	19-01-1995
			DE 69014817 T2	22-06-1995
			EP 0423035 A1	17-04-1991
			ES 2066169 T3	01-03-1995
			JP 1884135 C	10-11-1994
			JP 3241463 A	28-10-1991
			JP 6009051 B	02-02-1994
			KR 147360 B1	01-12-1998
EP 0378349	A	18-07-1990	US 4908521 A	13-03-1990
			AT 110868 T	15-09-1994
			AU 613574 B2	01-08-1991
			AU 4708389 A	19-07-1990
			CA 2007234 A1	10-07-1990
			DE 69011877 D1	06-10-1994
			DE 69011877 T2	20-04-1995
			EP 0378349 A2	18-07-1990
			ES 2063911 T3	16-01-1995
			JP 2226362 A	07-09-1990
			JP 2714869 B2	16-02-1998
			NO 900103 A	11-07-1990
US 4734564	A	29-03-1988	AT 69903 T	15-12-1991
			AU 589851 B2	19-10-1989
			AU 5654686 A	06-11-1986
			CA 1252566 A1	11-04-1989
			DE 3682608 D1	09-01-1992
			EP 0200343 A2	05-11-1986
			US 4812628 A	14-03-1989