(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) **N° de publication :** **2 762 118**
(à n'utiliser que pour les commandes de reproduction)

(21) **N° d'enregistrement national :** **97 04733**

(51) Int Cl^6 : **G 07 F 7/10,** G 07 F 17/34, 7/12, G 06 K 19/067, 7/08

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt :** 11.04.97.

(30) **Priorité :**

(43) **Date de mise à la disposition du public de la demande :** 16.10.98 Bulletin 98/42.

(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) :** *GEMPLUS SOCIETE EN COMMANDITE PAR ACTIONS* — FR.

(72) **Inventeur(s) :** ORUS HERVE et FOGLINO JEAN JACQUES.

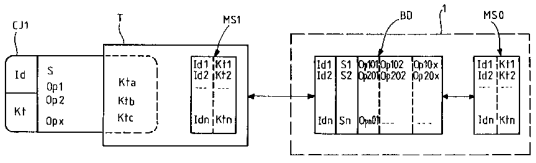
(73) **Titulaire(s) :**

(74) **Mandataire(s) :** CABINET BALLOT SCHMIT.

(54) PROCEDURE SECURISEE DE CONTROLE DE TRANSFERT D'UNITES DE VALEUR DANS UN SYSTEME DE JEU A CARTE A PUCE.

(57) L'invention concerne les machines à sous, type jackpot, black-jack, et autres machines de jeu d'argent de casino. Il est prévu que les machines de jeu fonctionnent avec des cartes de jeu (CJ1), type carte à puce, et sont reliées en réseau avec un organe central de gestion (1).

L'invention prévoit que l'organe central de gestion comporte une base de données (BD), dans laquelle sont stockées des informations correspondantes à celles stockées sur les cartes de jeu comme des informations sur le joueur ainsi que des données (Id) d'identification des cartes et des données (S, Op1, Op2) renseignant sur le solde de la valeur stockée dans la carte (CJ1). Une vérification des données de la carte par rapport aux données de la base de l'organe central de gestion permet d'assurer l'intégrité d'un tel système de machines de jeu fonctionnant avec des cartes à puce ou des cartes sans contact.



FR 2 762 118 - A1

PROCEDURE SECURISEE DE CONTROLE DE TRANSFERT D'UNITES DE VALEUR DANS UN SYSTEME DE JEU A CARTE A PUCE

La présente invention concerne le domaine des machines à sous, telles que les dispositifs de jack-pot et les autres dispositifs de jeux d'argent individuels du type de ceux que l'on trouve dans les casinos.

Elle concerne plus particulièrement des machines à sous permettant d'enregistrer des mises et des gains avec des cartes de jeu. Les cartes de jeu sont du type carte à puce ou carte sans contact. Les cartes de jeu peuvent être dédiées à cette utilisation suivant l'exemple des cartes téléphoniques. Elles sont avantageusement constituées par des cartes bancaires, permettant de transférer des sommes d'argent directement sur la machine à sous.

La présente demande vise un procédé et un système de contrôle de transfert d'unités de valeur entre une pluralité de cartes de jeu et une pluralité de machines de jeu, chaque machine étant connectée à un transcripteur de données sur cartes de jeu apte à créditer et/ou à débiter des unités de valeur en mémoire d'une carte de jeu.

Un objectif général du contrôle de transfert d'unités de valeurs entre cartes de jeu et machines de jeu est d'éviter toute malversation financière à l'aide de telle cartes.

On connaît déjà des systèmes de gestion pour des machines de jeu équipées de lecteurs de cartes à puce, adaptés à la gestion d'un parc de machines de jeux disposées dans des sites relativement fermés et contrôlés comme les casinos. Ces systèmes sont adaptés à un tel environnement, car il font l'objet de contrôles et de réglementations importants, peu

susceptibles de permettre des fraudes sur les transactions de jeux utilisant des cartes à puce.

Le document EP-A-0 360 613 décrit par exemple un système de transfert de données entre carte à puce et une pluralité de machines avec des moyens de transmission et de stockage des données machine dans la carte à puce. Un tel système permet d'effectuer un relevé des opérations de jeu avec une carte de collecte stockant une liste des opérations de jeux effectuées dans un but comptable ou fiscal.

Un inconvénient d'un tel système est qu'on ne peut pas contrôler toutes les opérations de jeu effectuées, sauf à relever toutes les machines avec la carte de collecte, ce qui occasionne des manipulations fastidieuses.

D'autre part, devant la demande croissante du public, il est envisagé d'installer des machines de jeu dans des sites moins protégés que les casinos comme des salles de jeux privées ou des bars, voire même dans des lieux d'habitation privés comme le domicile des joueurs.

Il apparaît clairement qu'une telle dispersion des machines de jeu pose d'importants problèmes de sécurité des transactions suite aux opérations de jeu.

Un but de l'invention est de permettre un développement des machines de jeu fonctionnant avec des cartes à puce dans des lieux non protégés.

Un autre but de l'invention est de renforcer l'intégrité des systèmes de machines de jeux fonctionnant avec des cartes de jeu.

L'invention prévoit que les machines de jeu sont reliées en réseau avec un organe central de gestion. Selon l'invention on a prévu que l'organe central de gestion comporte une base de données, dans laquelle

sont stockées des informations correspondantes à celles stockées sur les cartes de jeu comme des informations sur le joueur ainsi que des données d'identification des cartes et des données renseignant sur le solde de la valeur stockée dans la carte. Une vérification des données de la carte par rapport aux données de la base de l'organe central de gestion permet d'assurer l'intégrité d'un tel système de machines de jeu fonctionnant avec des cartes à puce ou des cartes sans contact.

L'invention prévoit ainsi un procédé sécurisé de contrôle de transferts d'unités de valeur entre une pluralité de cartes de jeu et une pluralité de machines de jeu, chaque machine étant connectée à un transcripteur de données sur carte de jeu, les machines étant reliées en réseau sécurisé avec un organe central de gestion par l'intermédiaire de moyens de liaison, le procédé comportant des étapes consistant, au cours d'une opération de jeu, à :

- lire des données en mémoire d'une carte de jeu, notamment un numéro d'identification de la carte et des données représentatives des unités de valeur débitées et/ou créditées au cours des opérations de jeu précédentes,

- échanger des données entre la machine et une base de données de l'organe central de gestion par l'intermédiaire des moyens de liaison du réseau sécurisé, notamment des données représentatives de solde des unités de valeur et/ou le numéro d'identification de la carte ; et,

- vérifier que les données en mémoire de la carte de jeu correspondent aux données de la base de données afin de contrôler l'intégrité d'un système constitué

par une telle carte, une telle machine, le réseau et l'organe central de gestion.

L'invention prévoit avantageusement des moyens de sécurisation qui permettent d'authentifier les messages de données échangées sur le réseau, c'est-à-dire de signer de tels messages.

L'invention prévoit en outre un système sécurisé de contrôle de transferts d'unités de valeur entre une pluralité de cartes de jeu et une pluralité de machines de jeu, chaque machine étant pourvue d'un transcripteur apte à débiter des unités de valeur d'une carte de jeu, les machines étant reliées en réseau sécurisé avec un organe central de gestion par l'intermédiaire de moyens de liaison, une carte de jeu stockant en mémoire des données représentatives d'opérations de jeu effectuées, notamment des données d'identification de la carte et des données représentatives de solde des valeurs débitées et/ou créditées au cours des opérations de jeu précédentes, caractérisé en ce que l'organe central de gestion comporte une base de données stockant parallèlement en mémoire les données représentatives des opérations de jeu effectuées, notamment les données d'identification des cartes et les données représentatives des soldes des valeurs débitées et/ou créditées au cours des opérations de jeu précédentes et en ce que des moyens de contrôle vérifient que, pour une carte identifiée, les données de la base et les données de la carte correspondent, notamment que les données représentatives du solde correspondent, afin de vérifier l'intégrité du système.

Un module de sécurisation pour l'authentification des messages de données peut avantageusement être prévu dans le réseau, au niveau d'un transcripteur, d'une

machine, de l'organe central, ou même des moyens de liaison du réseau.

L'invention sera mieux comprise à la lecture de la description et des dessins qui suivent, donnés uniquement à titre d'exemples non limitatifs ; sur les dessins annexés :

- la figure 1 représente un système sécurisé de contrôle de transfert d'unités de valeurs entre une pluralité de cartes de jeu et une pluralité de machines de jeu apte à mettre en oeuvre l'invention ;

- la figure 2 représente un schéma d'échange et de vérification des données selon l'invention ; et,

- la figure 3 représente un calcul de certificat d'authentification par des moyens de sécurisation selon l'invention.

Sur la figure 1 on a représenté un système sécurisé de machines de jeu tel que proposé par l'invention, et qui comprend une ou plusieurs machines de jeu 200, 200', 200" et 200'".

Une telle machine de jeu 200, semblable aux machines à sous que l'on trouve dans les casinos dispose d'un monnayeur électronique 210 que l'on appellera par la suite transcripteur de données sur carte de jeu CJ.

Le transcripteur de données sur carte 210 est relié à l'électronique de la machine 200, par exemple par une liaison série de type RS 485. La machine et le lecteur comportent des interfaces entrée-sortie adaptées à cette liaison.

De façon classique, la machine est équipée d'un écran d'affichage 211 qui permet aux joueurs de savoir à tout instant quel est le solde dont il dispose pour jouer et le montant des mises et des gains réalisés.

La machine 200 qui a été représentée peut bien sûr être une machine à monnayeur électronique exclusivement, mais aussi une machine à double monnayeur, c'est-à-dire une machine qui comporte outre ce monnayeur électronique, un monnayeur à pièces (ou à jetons) symbolisé par la référence 201.

Dans le cas d'une machine à double monnayeur, le joueur aura la possibilité de jouer avec des pièces ou jetons et de se faire restituer ses gains uniquement sous la forme de pièces.

Les cartes de jeu CJ représentées sous forme de cartes à puce comportent une mémoire morte effaçable électriquement, par exemple une mémoire de type EEPROM.

Il peut s'agir également de cartes à puce comportant un microprocesseur, une mémoire de programmes et une mémoire de travail de type RAM.

Ces cartes à puce peuvent également être des cartes à chargement d'unités de type rechargeable. Ces cartes comportent pour cela une mémoire électriquement programmable du genre boulier.

En outre les cartes de jeu peuvent être constituées par des cartes sans contact, la carte comportant un circuit intégré à mémoire et microprocesseur, et un circuit électronique de transmission de données sans contact électrique. On peut par exemple utiliser un transpondeur tel que décrit dans la demande de brevet FR - 96 16061.

La réalisation des machines de jeu 200 et leur connexion à des transcripteurs de données sur cartes de jeu ne sera pas détaillée ici. Des exemples de réalisations de machines de jeu sont détaillés par exemple dans la demande de brevet FR - 96 10031 dont la description est incorporée à la présente.

Afin de contrôler les opérations de jeux et les transactions avec les cartes, il est prévu de relier les machines 200, 200', 200", 200'" en réseau, avec un organe central de gestion représentés sous la référence 1 à la figure 1. Les machines du réseau sont reliées à l'organe central de gestion 1 par des moyens de liaison 123. Comme représentées à la figure 1, les machines 200, 200', 200", 200'" peuvent également être reliées entre elles par le réseau.

Les moyens de liaison 123 sont constitués dans le cas d'un réseau local comme celui d'un casino par une liaison locale. La liaison locale est par exemple une liaison série de type RS 485, un bus de liaison parallèle , une fibre optique, une liaison radio ou tout autre support de transmission.

Dans le cas d'un réseau joignant des salles de jeu dispersées, les moyens de liaisons peuvent être constitués par des canaux de transmission propres au réseau ou par des lignes téléphoniques.

Pour établir des liaisons téléphoniques, le réseau comporte des modulateurs-démodulateurs de type MODEM 120, 120', 120" et 120"', disposés en interface entre les moyens de liaison 123 et une machine de jeux 200, 200', 200", 200"' respectivement.

L'organe central de gestion 1 est constitué par exemple d'un ordinateur central relié également aux moyens de liaison 123 par un MODEM 101 de façon à faire partie du réseau.

Sur la figure 1 on a représenté des moyens de liaison 123 sous la forme schématique d'une ligne annulaire à laquelle les machines de jeux 200, 200', 200" et 200"' sont connectées. Les machines sont ainsi reliées entre elles et à l'organe central de gestion 1.

La liaison peut cependant prendre toutes sortes de formes équivalentes.

Dans le cas de liaisons téléphoniques, les machines sont reliées individuellement aux moyens centralisés de gestion, les machines n'étant pas nécessairement reliées entre elles. Le MODEM 101 des moyens de gestion 1 peut comporter avantageusement un standard de plusieurs lignes téléphoniques.

L'utilisation de liaisons téléphoniques présente l'avantage de permettre d'étendre le réseau au lieu d'habitation des joueurs. Les machines de jeux sont de préférence constituées par des ordinateurs personnels 300 et 300' de type PC. Les machines peuvent ainsi être connectées chacune à un transcripteur de données sur carte de jeu 310 ou 310' intégrant de préférence un MODEM 130 ou 130', par exemple du type "GEMTEL" commercialisé par la demanderesse.

Le réseau utilisé peut être notamment un réseau de communication ouvert du type "INTERNET".

Il est prévu en outre que le système et le réseau comportent au moins un terminal de chargement représenté à la figure 1 sous forme d'une caisse enregistreuse 100. Le terminal de chargement 100 comporte alors un transcripteur 110. Le terminal 100 et le transcripteur 110 sont alors reliés au réseau par l'intermédiaire d'un MODEM 111 connecté aux moyens de liaison 123.

Classiquement, il est prévu que les cartes à puce dédiées aux jeux sont des cartes non-rechargeables, à l'instar des cartes téléphoniques, et elles sont fabriquées et chargées uniquement par un organisme central.

Dans une application avec des cartes non-rechargeables, il est prévu que la base de données BD

des moyens centralisés de gestion 1 dispose des soldes S1, S2, ..., Sn initiaux des valeurs créditées sur les cartes CJ1, CJ2, ..., CJn avant leur mise en circulation.

Cependant, selon une variante avantageuse, il est prévu que les cartes sont rechargées en unités de valeurs par l'intermédiaire de terminaux de chargement.

En pratique, ce terminal peut être celui d'un caissier du casino. De façon alternative, on peut prévoir une multitude de terminaux de chargements disposés dans des débits de tabac ou dans d'autres commerces accessibles aux joueurs.

Ainsi lorsqu'un joueur désire obtenir la délivrance d'un crédit, il donne sa carte de jeu CJ1 à l'opérateur habilité à utiliser le terminal 100 qui insère cette carte dans la partie transcripteur 110 de ce terminal 100 et qui au moyen du clavier de la caisse va rentrer le montant du crédit que désire avoir le joueur. Ce montant est transféré au transcripteur 110 qui enregistre alors sur la carte à puce CJ1 l'information significative correspondant au crédit désiré par le joueur.

Selon l'invention, le terminal de rechargement peut alors communiquer à l'organe central de gestion 1, par l'intermédiaire des moyens de liaison du réseau 123, les données lues sur la carte à recharger, notamment son numéro d'identification Id et son solde S d'unités de valeur. La vérification du numéro d'identification Id de la carte de jeu CJ1 peut être faite directement par le terminal de rechargement 100 ou par son transcripteur de données 110 ou de manière alternative par l'organe central de gestion 1. L'invention prévoit ainsi une étape préliminaire aux opérations de jeu, consistant à inscrire dans la base de données de

l'organe central de gestion 1 et dans la mémoire d'une carte de jeu CJ1, des données représentatives d'une valeur de solde initial lors d'une opération préliminaire de chargement de la carte CJ1.

Selon la première alternative, il est prévu comme visible à la figure 2 que le terminal de rechargement ou son transcripteur T dispose des clefs d'identification secrètes Kt1, Kt2, ..., Ktn de toutes les cartes de jeu CJ1, CJ2, ..., CJn en circulation. Ces clés secrètes sont de préférence stockées dans un module de sécurisation MS1 comportant une mémoire et une unité de calcul, les données stockées n'étant pas accessibles de l'extérieur. Le terminal 100 vérifie alors que l'identification Id1 de la carte à puce CJ1 est correcte avec la clef Kt1 correspondante, en appliquant un algorithme d'authentification ou de cryptage selon les méthodes connues.

Selon la seconde alternative, cette authentification de la carte est effectuée au niveau de l'organe central de gestion 1, les numéros d'identification Id1,Id2,...,Idn et les clefs d'authentification correspondantes Kt1, Kt2, ..., Ktn étant stockées dans la base de données BD de l'organe central de gestion ou de préférence dans un module de sécurité MS0 similaire à MS1. Cette seconde alternative présente l'avantage d'éviter toute dissémination des clefs d'authentification secrètes.

L'invention prévoit en outre un échange de données entre le terminal et l'organe central de gestion portant sur les données stockées dans la base de données de l'organe central de gestion 1. De préférence, cet échange de données est accompagné d'un certificat d'authentification. Un protocole de sécurisation permettant d'émettre de tels certificats

sera détaillé ci-après. Ce protocole évite avantageusement qu'une machine parasite du réseau ne crédite abusivement la base de donnée. Le terminal T peut ainsi communiquer le solde S des valeurs débitées et/ou créditées précédemment sur la carte de jeu CJ1 à l'organe central de gestion 1. Après avoir authentifié le numéro d'identification Id1 de la carte ou le certificat accompagnant les données de solde, on peut ainsi vérifier que le solde S inscrit en mémoire de la carte de jeu CJ1 correspond bien au solde S1 stocké dans la base de données BD. Si la vérification est positive, il est prévu que l'organe central de gestion 1 émet un signal d'accord pour le rechargement de la carte CJ1 par le terminal et le transcripteur T. En cas de vérification négative, une procédure ou un signal d'alerte peuvent être mis en oeuvre au niveau de l'organe central de gestion 1, ou au niveau du terminal de chargement. Dans un réseau de machines à sous de casino par exemple, le caissier pourra être alerté par le terminal de chargement afin de découvrir l'origine d'un tel dysfonctionnement. Dans un réseau plus étendu, on peut prévoir que la carte CJ1 soit avalée par le transcripteur T du terminal afin d'enquêter sur le dysfonctionnement.

On peut prévoir en outre que la base de données ou la mémoire des cartes de jeu CJ comportent des informations sur le joueur, par exemple sur son âge, ses habitudes de jeu pour des applications de fidélisation des joueurs, de remise de parties gratuites, etc.

Nous allons présenter maintenant des protocoles de contrôle de transferts d'unités de valeur au cours d'opérations de jeu effectuées avec le procédé ou le système selon l'invention.

Au début des opérations de jeu, le transcripteur de données sur carte 210 de la machine de jeu lit le numéro d'identification en mémoire de la carte de jeu CJ1. Comme exposé précédemment au vu de la figure 2, ce numéro d'identification Id est de préférence authentifié par un module de sécurité MS1 prévu dans le transcripteur T. Le numéro Id peut éventuellement être communiqué à l'organe central de gestion 1 en vue d'authentifier la carte CJ1 avec la clef d'identification Kt1 contenue dans le module de sécurité MS0. Cette étape d'identification est de préférence effectuée une seule fois pour plusieurs opérations de jeu avec la même carte sur la même machine, la machine ou le terminal mémorisant éventuellement ce numéro d'identification Id pour les opérations suivantes.

A chaque opération de jeu suivante, le solde S des unités de valeur affecté au joueur est revu à la suite des mises ou des gains réalisés.

Selon un premier mode de réalisation de l'invention, il est prévu de communiquer simplement à l'organe central de gestion 1 des données relatives à l'opération de jeu effectuée, notamment le nouveau solde d'unités de valeur obtenu au cours de cette opération de jeu. L'organe central de gestion 1 peut ainsi stocker la liste des opérations effectuées, sous forme d'une liste des crédits ou des débits successifs enregistrés sur la carte CJ1. Cette liste des opérations Op101,Op102,... , Op10x est par exemple enregistrée dans la base de données BD sous le numéro d'identification Id1 de la carte CJ1 en cours d'utilisation.

La recopie du solde S1 ou des opérations Op101, Op102, ... , Op10x dans la base de données BD de

l'organe central de gestion 1 sert alors à établir un relevé comptable des opérations ou à effectuer des vérifications fiscales. Un tel historique des opérations permet également lors d'une vérification d'une carte falsifiée de mesurer l'étendue de la fraude.

Selon un deuxième mode de réalisation de l'invention, il est prévu une étape supplémentaire consistant à vérifier que les données en mémoire de la carte CJ1 et les données de la base de données BD correspondent afin de contrôler l'intégrité d'un système constitué par une telle carte CJ1, une telle machine 200, le réseau 123 et l'organe central de gestion 1.

Deux types de vérification peuvent être prévues, la vérification pouvant porter sur le numéro d'identification Id ou sur le solde S de la carte.

La vérification du numéro d'identification Id1 de la carte CJ1 est effectuée avec une clé d'identification Kt1 comme on l'a vu précédemment. Selon ce deuxième mode de réalisation, le numéro d'identification Id est communiqué à l'organe central 1 via les moyens de liaison 123 du réseau. L'organe central 1 stocke les clés d'identification Kt1, Kt2, ..., Ktn des cartes CJ1, CJ2, ..., CJn en circulation, dans sa base de donnée BD ou de préférence dans un module de sécurisation MS0. Le module de sécurisation MS0 effectue ainsi les calculs d'identification en interne.

De plus, la vérification peut porter sur le solde d'unités de valeur de la carte CJ1. Dans ce cas, le transcripteur T lit sur la carte les données de solde S des unités de valeur et les envoie à l'organe central de gestion 1 par l'intermédiaire des moyens de liaison

du réseau 123. La vérification du solde S de la carte CJ1 est alors effectuée par rapport au solde S1 indiqué dans la base de données BD sous le numéro d'identification Id1. Si les deux soldes S et S1 correspondent, l'opération de jeu est autorisée par l'organe central de gestion 1.

Selon une autre alternative, la vérification peut porter sur la certification des données échangées à partir de la carte de jeu CJ1. Des algorithmes standards d'encryptage de données type algorithme DES permettent en effet de certifier les données numériques échangées entre la carte CJ1, le transcripteur T, la machine de jeu et l'organe central de gestion 1. Le cryptage et le décryptage du certificat accompagnant les données transmises n'est possible et cohérent que si on utilise une clé secrète.

Les algorithmes de cryptage de donnés de type DES comportent des séries de calculs complexes qui ne seront pas détaillés dans la présente.

Un exemple de mise en oeuvre d'algorithme DES sera exposé en considérant simplement que l'algorithme fournit un nombre crypté, appelé clef de session K', à partir d'un premier nombre donné, appelé clef d'identification K et d'un nombre aléatoire Rnd, selon l'exemple de la formule suivante :

$$K' = DES(K, Rnd)$$

La complexité des algorithmes DES rend impossible la découverte d'une clef d'identification secrète K à partir de la clef de session K' et du nombre aléatoire Rnd.

La figure 3 montre un exemple d'application d'un algorithme DES. Il permet d'illustrer des moyens de sécurisation du réseau, en particulier la sécurisation

des échanges de données effectuées via les moyens de liaison du réseau. La carte de jeu dispose dans une zone mémoire inaccessible d'au moins une clé d'identification secrète Kt. Le microprocesseur de la carte génère un nombre pseudo aléatoire Rnd1. A partir de ces deux nombres Rnd1 et Kt, l'algorithme DES mis en oeuvre par le microprocesseur calcule une clef de session Kt'.

Cette clef de session Kt' peut servir de certificat d'authentification et être envoyée avec le nombre aléatoire Rnd1 et les données à certifier. Cependant, pour rendre toute découverte des clefs impossible, il est prévu d'appliquer une seconde fois l'algorithme DES. Comme visible figure 3, la carte de jeu, organe émetteur du message à certifier, demande à l'organe destinataire, l'organe central 1 par exemple, de lui fournir un second nombre aléatoire Rnd2.

L'algorithme DES est à nouveau appliqué à la clef de session Kt' et au second nombre aléatoire Rnd2 par le microprocesseur de la carte pour calculer un certificat C.

Le message de données est alors envoyé à l'organe destinataire accompagné du certificat C et du nombre aléatoire Rnd1 calculés par la carte. Ainsi les clefs utilisées, en particulier la clef d'identification secrète Kt, ne sont pas échangées.

L'authentification du message de données est effectué en recalculant un certificat C' à partir des même données. L'organe central de gestion 1 dispose dans son module sécurisé MSO de la clef d'identification secrète Kt. Le module sécurisé MSO peut donc calculer la clef de session Kt' à partir de la clef d'identification Kt et du nombre aléatoire Rnd1.

Le module sécurisé MS0 dispose encore du nombre aléatoire Rnd2 qu'il a fourni précédemment à la carte de jeu. A partir de ces deux nombres Rnd2 et Kt', le module de sécurité MS0 calcule à nouveau un certificat C' en appliquant une seconde fois l'algorithme DES.

En vérifiant que le certificat C calculé par la carte correspond au certificat C' recalculé par son module de sécurité, l'organe central peut authentifier le message de donnée reçu.

Notons que la clé de session Kt' et le certificat C sont recalculés à chaque certification de message désirée. On évite ainsi que une machine pirate du réseau obtienne l'accès à la base de donnée ou à la mémoire de la carte en recopiant une certification précédente.

Après avoir effectué une ou plusieurs de ces vérifications, l'organe central 1 envoie un signal d'accord qui peut être crypté ou encodé. Avec un tel signal d'accord, le joueur peut utiliser sa carte de jeu CJ1, effectuer des mises, des opérations de jeu et recharger sa carte avec ses gains.

Dans ces deux premiers modes de réalisation, on a vu que la carte a une fonction d'identification, son numéro Id permettant à l'organe central 1 ou à la machine de jeu de la reconnaître voire de reconnaître le joueur dans certaines applications de fidélisation de clientèle. De plus, la carte a une fonction de porte-monnaie, le solde d'unités de valeur étant stocké dans la carte et connu essentiellement par la carte, la recopie de solde dans l'organe central 1 servant aux fins de vérification.

Selon un troisième mode de réalisation, la fonction porte-monnaie n'est plus assurée par la carte mais par l'organe central de gestion lui-même. La carte

ne comporte alors aucune donnée relative au solde du joueur mais uniquement des données d'identification, telles que le numéro d'identification Id, plusieurs clefs Kta, Ktb, Ktc d'authentification et éventuellement des informations sur le joueur. Les données de solde S1 des unités de valeur sont alors uniquement stockées dans la base de données BD de l'organe central de gestion 1. Ce compte d'unités de valeur se trouve par exemple dans la base de données sous le numéro d'identification Id1.

Lors d'une opération de jeu, le numéro d'identification Id de la carte CJ1 est envoyé à l'organe central de gestion 1 via les moyens de liaison 123 du réseau. Le numéro d'identification Id peut être envoyé directement par la machine de jeu 200 ou par son transcripteur 210 s'il a été mémorisé par la machine ou par son transcripteur. Le numéro d'identification Id peut aussi être lu sur la carte et envoyé à l'organe central de gestion 1 par le transcripteur 210 à chaque opération de jeu.

Après vérification du numéro d'identification Id, l'organe central de gestion 1 consulte la base de données BD et envoie à la machine de jeu 200 le solde S1 des unités de valeur affecté à la carte CJ1.

De préférence le transfert des données de solde d'unités de valeur est effectué avec un certificat selon le protocole de sécurisation des échanges de données présenté précédemment.

Un avantage de ce troisième mode de réalisation est que les montants mis en jeu sont stockés dans l'organe central de gestion 1, ce qui évite toute mémorisation de valeur au niveau des cartes de jeu.

Selon ce troisième mode de réalisation, il est donc prévu de stocker, dans la base de données des

moyens centralisés de gestion, les données représentatives du solde des valeurs débitées et/ou créditées afin d'éviter une fraude à partir d'une carte à puce.

Le contrôle consiste simplement dans ce troisième mode de réalisation à vérifier le numéro d'identification Id de la carte de jeu CJ1 avec une clé d'identification Kt1 lue dans la base de données BD de l'organe central de gestion 1 afin de contrôler l'intégrité de la carte.

Avec ces trois modes de réalisation de l'invention on a vu qu'on peut avantageusement contrôler l'intégrité des cartes de jeu utilisées sur les machines de jeu.

De plus, en mettant en oeuvre des moyens de sécurisation des échanges de données, l'invention permet avantageusement de vérifier l'intégrité d'un système formé par les cartes de jeu, le réseau de machines de jeu et la base de données de l'organe central de gestion, l'intégrité d'un des trois éléments du système, soit une carte de jeu, soit le réseau, soit la base de données étant vérifiée à l'aide des deux autres éléments.

L'invention prévoit en effet un système apte à mettre en oeuvre le procédé selon l'invention.

Un tel système comporte une pluralité de machines de jeu, chaque machine étant pourvue d'un transcripteur apte à débiter des unités de valeur d'une carte de jeu, les machines étant reliées en réseau avec un organe central de gestion par l'intermédiaire de moyens de liaison.

Selon l'invention, les données représentatives des opérations de jeu effectuées avec une carte à puce sur une machine de jeu sont stockées en mémoire de la carte

de jeu et parallèlement dans une base de données prévue dans l'organe central de gestion.

Les données stockées sont notamment les données d'identification de la carte et le solde ou les soldes successifs d'unités de valeur débitées et/ou créditées avec la carte.

Des moyens de contrôle tels qu'un programme d'ordinateur effectuant l'authentification du numéro d'identification de la carte ou la comparaison des valeurs de solde stockées sur la carte et dans la base ou encore la certification des données échangées sont prévus afin de vérifier l'intégrité du système.

De préférence, pour sécuriser les échanges de données sur le réseau, il est prévu qu'un module de sécurisation calcule un certificat d'authentification à partir de données secrètes stockées en mémoire du module et en ce que les moyens de contrôle vérifient que le certificat d'authentification calculé par le module de sécurisation correspond au certificat d'authentification calculé par la carte de jeu ou par un autre module de sécurisation.

De tels modules de sécurisation MS0, MS1 peuvent être disposés dans les cartes du jeu CJ1, CJ2, ..., CJn, ou au niveau des transcripteurs 10, 110, 210, 210', 210'', 210''', 310, des machines de jeu 200, 200', 200'', 200''', de l'organe central de gestion 1 ou même sur les moyens de liaison 123 du réseau.

On peut en particulier prévoir plusieurs modules ou des moyens répartis de sécurisation au sein du réseau. Chaque transcripteur 10, 210, 210', 210", 210"', ou chaque interface 11, 120, 120', 120", 120"' comprend par exemple un module de sécurisation de sorte que les échanges de données sur les moyens de liaison 123 son accompagnés de certificat d'authentification.

Par exemple le transcripteur 10 émetteur ajoute à son message son certificat qui est authentifié par le transcripteur 210 destinataire avant d'être transmis à la machine 200 correspondante.

D'autres variantes de réalisation, avantages et caractéristiques de l'invention, apparaîtront à l'homme du métier sans sortir du cadre des revendications ci-après.

REVENDICATIONS

1. Procédé sécurisé de contrôle de transferts d'unités de valeur entre une pluralité de cartes de jeu (CJ, CJ1, CJ2, CJn) et une pluralité de machines de jeu (200, 200', 200", 200''', 300, 300', 300"), chaque machine étant connectée à un transcripteur (210) de données sur carte de jeu (CJ2), les machines étant reliées en réseau sécurisé avec un organe central de gestion (1) par l'intermédiaire de moyens de liaison (123), le procédé comportant des étapes consistant, au cours d'une opération de jeu, à :

- lire des données en mémoire d'une carte de jeu, notamment un numéro d'identification (Id) de la carte (CJ1) et/ou des données (S, Op1, Op2, Opx) représentatives des unités de valeur débitées et/ou créditées au cours des opérations de jeu précédentes,

le procédé étant caractérisé en ce qu'il comporte des étapes consistant à :

- échanger des données entre la machine (200) et une base de données (BD) de l'organe central de gestion (1) par l'intermédiaire des moyens de liaison (123) du réseau sécurisé, notamment des données représentatives de solde (S) des unités de valeur et/ou le numéro d'identification (Id) de la carte ; et,

- vérifier que les données en mémoire de la carte de jeu (CJ1) correspondent aux données de la base de données (BD) afin de contrôler l'intégrité d'un système constitué par une telle carte, une telle machine, le réseau et l'organe central de gestion.

2. Procédé selon la revendication 1, caractérisé par une étape préliminaire aux opérations de jeu, consistant à :

- inscrire, dans la base de données (BD) de l'organe central de gestion (1) et dans la mémoire d'une carte de jeu (CJ1), des données représentatives d'un solde (S, S1) initial d'unités de valeur lors d'une opération préliminaire de chargement de la carte.

3. Procédé selon l'une des revendications précédentes, caractérisé par une étape consistant, au cours d'une opération de jeu, à :

- inscrire, dans la base de données (BD) de l'organe central de gestion (1), des données représentatives du solde (S1) des unités de valeur de la carte de jeu (CJ1).

4. Procédé selon l'une des revendications précédentes, caractérisé par une étape consistant, au cours d'une opération de jeu, à :

- recevoir les données représentatives du solde (S1) des unités de valeur à partir de l'organe central de gestion (1) afin d'éviter une fraude à partir d'une carte (CJ2) ou d'une machine de jeu (200).

5. Procédé selon l'une des revendications précédentes, caractérisé en ce que l'étape de vérification consiste à :

- vérifier les données représentatives de solde (S) des unités de valeur lues en mémoire de la carte de jeu (CJ1) par rapport aux données (S1) lues dans la base de données (BD) afin de contrôler l'intégrité de la carte de jeu (CJ1).

6. Procédé selon l'une des revendications précédentes, caractérisé en ce que l'étape de vérification consiste à :

- vérifier le numéro d'identification (Id) de la carte de jeu (CJ1) avec une clé d'identification (Kt1) lue dans la base de données (BD) de l'organe central de

gestion (1) afin de contrôler l'intégrité de la carte de jeu (CJ1).

7. Procédé selon l'une des revendications précédentes caractérisé en ce que le réseau comporte en outre des moyens de sécurisation (MS0), le procédé comportant une étape supplémentaire consistant à :

- prévoir que les moyens de sécurisation (MS0) du réseau calculent un certificat d'authentification (C') à partir de données secrètes (Kt, Kt') en mémoire des moyens de sécurisation.

8. Procédé selon la revendication 7, caractérisé par une étape supplémentaire consistant à :

- lire un certificat d'authentification (C) calculé par la carte de jeu (CJ1) à partir de données secrètes (Kt, Kt1) en mémoire de la carte.

9. Procédé selon la revendication 8 caractérisé en ce que l'étape de vérification consiste à :

- vérifier que le certificat d'authentification (C) calculé par la carte de jeu (CJ1) correspond au certificat d'authentification (C') calculé par les moyens de sécurisation (MSO) du réseau.

10. Procédé selon l'une des revendications précédentes caractérisé en ce que le réseau comporte en outre des moyens de sécurisation répartis (MSO, MS1), le procédé comportant des étapes supplémentaires consistant à :

- prévoir que des premiers moyens de sécurisation (MS0) du réseau calculent un premier certificat d'authentification (C') à partir de données secrètes (Kt, Kt') en mémoire des premiers moyens de sécurisation (MS0), et

- prévoir que des seconds moyens de sécurisation (MS1) du réseau calculent un second certificat d'authentification à partir de données secrètes en mémoire des seconds moyens de sécurisation (MS1), et

- vérifier que le premier certificat d'authentification (C') calculé par les premiers moyens de sécurisation (MS0) du réseau correspond au second certificat d'authentification calculé par les seconds moyens de sécurisation (MS1) du réseau.

11. Procédé selon l'une des revendications 7 à 10 caractérisé en ce que les données (Id, S) échangées entre la machine (200) et la base de données (BD) de l'organe central de gestion (1) sont accompagnées d'un certificat d'authentification (C, C').

12. Procédé selon l'une des revendications précédentes caractérisé en ce que des moyens de sécurisation (MS1) sont associés au transcripteur (T, 10, 110, 210) de données sur carte de jeu (CJ1) afin de contrôler l'intégrité d'une telle carte.

13. Procédé selon l'une des revendications précédentes caractérisé en ce que des moyens de sécurisation (MS1) sont associés à une machine de jeu (T, 200, 300).

14. Procédé selon l'une des revendications précédentes caractérisé en ce que des moyens de sécurisation sont associés aux moyens de liaison du réseau.

15. Procédé selon l'une des revendications précédentes caractérisé en ce que des moyens de sécurisation (MS0) sont associés à l'organe central de gestion (1) afin de contrôler l'intégrité du réseau.

16. Système sécurisé de contrôle de transferts d'unités de valeur entre une pluralité de cartes de jeu (CJ) et une pluralité de machines de jeu (200, 300), chaque machine étant pourvue d'un transcripteur (210, 310) apte à débiter des unités de valeur d'une carte de jeu (CJ), les machines étant reliées en réseau sécurisé avec un organe central de gestion (1) par l'intermédiaire de moyens de liaison (123), une carte de jeu (CJ1) stockant en mémoire des données (S, Op1,

Op2, Opx) représentatives d'opérations de jeu effectuées, notamment des données d'identification (Id) de la carte et des données représentatives de solde (S) des unités de valeurs débitées et/ou créditées au cours des opérations de jeu précédentes, caractérisé en ce que l'organe central de gestion (1) comporte une base de données (BD) stockant parallèlement en mémoire les données (S1, Op101, Op102, Op10x) représentatives des opérations de jeu effectuées, notamment les données d'identification (Id1, Id2, Idn) des cartes et les données représentatives des soldes (S1, S2, Sn) des unités de valeur débitées et/ou créditées au cours des opérations de jeu précédentes et en ce que des moyens de contrôle (BD) vérifient que, pour une carte identifiée, les données de la base (BD) et les données de la carte (CJ1) correspondent, notamment que les données (S, S1) représentatives du solde d'unités de valeur correspondent, afin de vérifier l'intégrité du système.

17. Système sécurisé selon la revendication 16, caractérisé en ce que la carte de jeu (CJ1) calcule un certificat d'authentification (C) à partir de données secrètes (Kt, Kt') stockées en mémoire de la carte (CJ1).

18. Système sécurisé selon la revendication 16 ou la revendication 17, caractérisé en ce qu'il comporte en outre au moins un module de sécurisation (MS0, MS1), le module de sécurisation calculant un certificat d'authentification (C') à partir de données secrètes (Kt, Kt') stockées en mémoire du module (MS0) et en ce que les moyens de contrôle (MS0) vérifient que le certificat d'authentification (C') calculé par le module de sécurisation correspond au certificat

d'authentification (C') calculé par la carte de jeu ou par un autre module de sécurisation (MS1).

19. Système sécurisé selon la revendication 18, caractérisé en ce qu'un module de sécurisation (MS1) est disposé dans le transcripteur (T, 10, 210, 310).

20. Système sécurisé selon l'une des revendications 18 et 19, caractérisé en ce qu'un module de sécurisation (MS0) est disposé dans une machine de jeu (200).

21. Système sécurisé selon l'une des revendications 18 à 20, caractérisé en ce qu'un module de sécurisation est disposé sur les moyens de liaison du réseau.

22. Système sécurisé selon l'une des revendications 18 à 21, caractérisé en ce qu'un module de sécurisation (MS0) est disposé dans l'organe central de gestion (1).

23. Système sécurisé selon l'une des revendications 16 à 22, caractérisé en ce qu'une carte de jeu est une carte à puce.

24. Système sécurisé selon l'une des revendications 16 à 23, caractérisé en ce qu'une carte de jeu est une carte sans contact.

25. Système sécurisé selon l'une des revendications 16 à 24, caractérisé en ce qu'une carte de jeu est une carte bancaire.

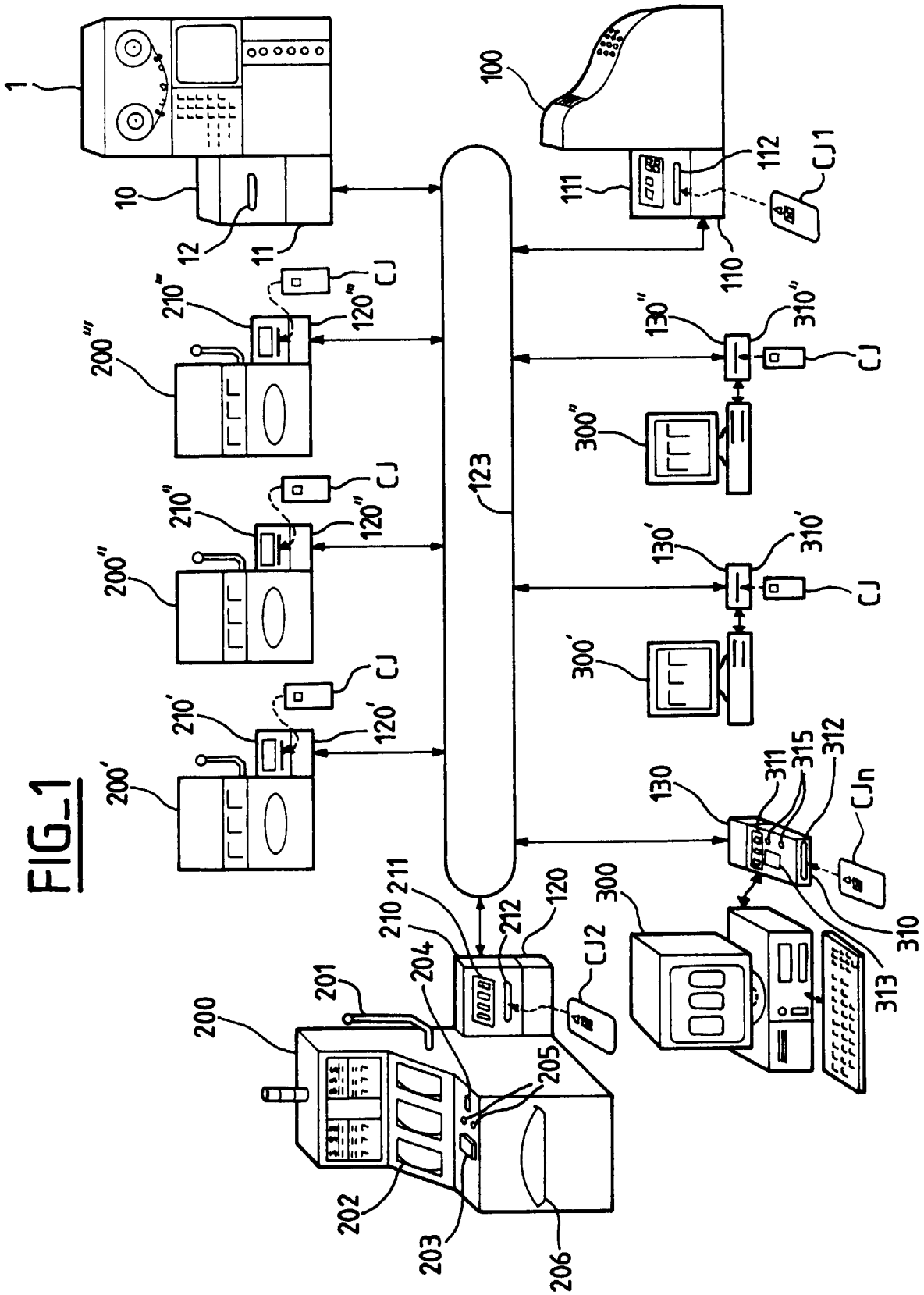

1
10
11
12
100
111
112
CJ1
110
123
200
201
202
203
204
205
206
210
211
212
120
CJ2
300
130
311
315
312
CJn
310
313
200'
210'
120'
CJ
300'
130'
310'
200''
210''
120''
300''
130''
310''
200'''
210'''
120'''

FIG_1

FIG_2

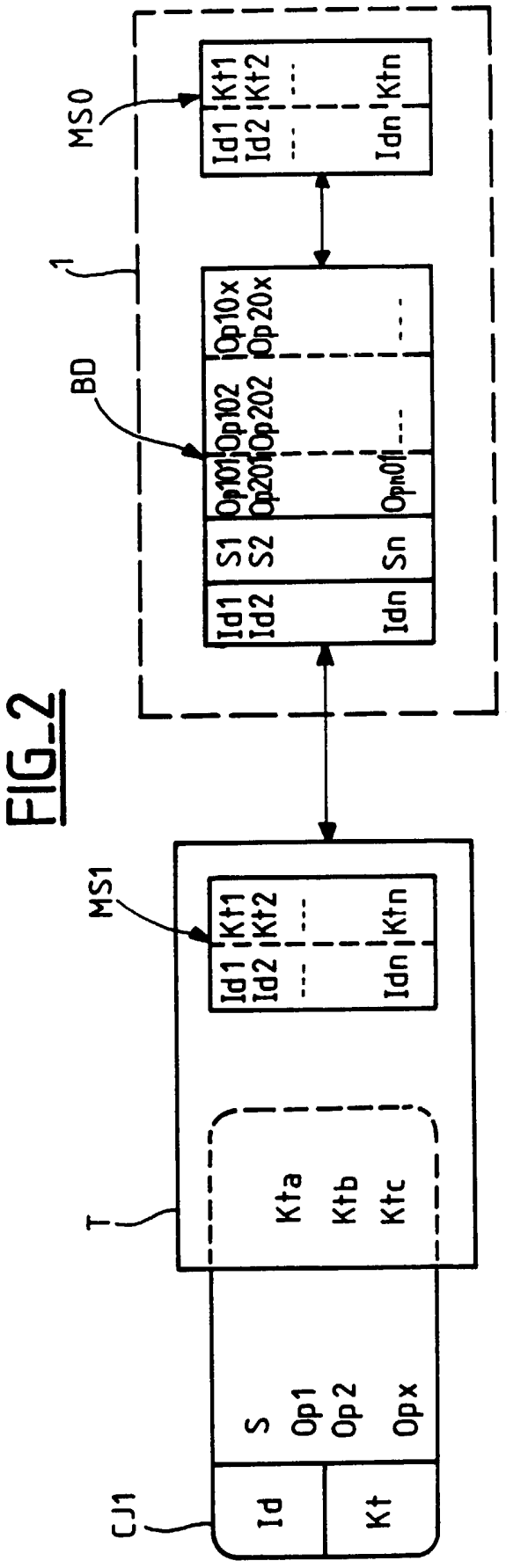
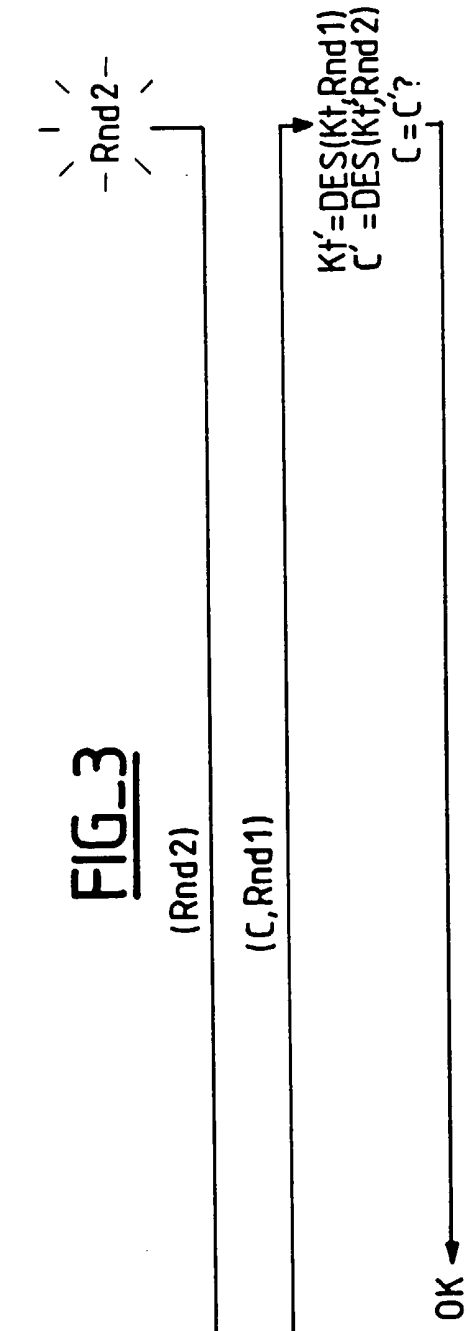

MS0
Id1 Id2 Idn
Kt1 Kt2 Ktn
1'
BD
Op10x Op20x
Op101 Op102 Op201 Op202 Opm01
S1 S2 Sn
Id1 Id2 Idn
MS1
Id1 Id2 Idn
Kt1 Kt2 Ktn
T
Kta Ktb Ktc
CJ1
Id
Kt
S Op1 Op2 Opx

FIG_3


Rnd2
(Rnd2)
(C,Rnd1)
Kt'=DES(Kt,Rnd1)
C' =DES(Kt',Rnd2)
C=C'?
Rnd1
Kt'=DES(Kt,Rnd1)
C=DES(Kt',Rnd2)
OK

2762118

REPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
de la
PROPRIETE INDUSTRIELLE

RAPPORT DE RECHERCHE PRELIMINAIRE

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

N° d'enregistrement national

FA 543256
FR 9704733

DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes	Revendications concernées de la demande examinée
Y	WO 93 17403 A (NSM) * abrégé; revendications 13-24; figures * * page 6, alinéa 2 - page 9, alinéa 1 *	1-5,16, 23
Y	DE 44 27 039 A (GIESECKE & DEVRIENT) * abrégé; revendications; figures 1,2 * * colonne 3, ligne 32 - colonne 4, ligne 41 *	1-5,16, 23
A	EP 0 589 545 A (BALLY GAMING INTERNATIONAL) * abrégé; revendications; figure * * colonne 4, ligne 8 - colonne 8, ligne 56 *	1-6,16, 23
A	WO 96 08798 A (GEMPLUS) * abrégé; revendications; figures *	1,2,6-23
A	EP 0 762 333 A (TEXAS INSTRUMENTS)	
A	EP 0 619 564 A (PITNEY BOWES)	
A	WO 97 02547 A (KONINKLIJKE PTT NEDERLAND)	

DOMAINES TECHNIQUES RECHERCHES (Int.CL.6)

G07F

1

Date d'achèvement de la recherche	Examinateur
18 février 1998	David, J

CATEGORIE DES DOCUMENTS CITES

X : particulièrement pertinent à lui seul
Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie
A : pertinent à l'encontre d'au moins une revendication ou arrière-plan technologique général
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

EPO FORM 1503 03.82 (P04C13)