(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) N° de publication : **2 591 007**
(à n'utiliser que pour les commandes de reproduction)

(21) N° d'enregistrement national : **85 17778**

(51) Int Cl⁴ : G 06 K 19/06.

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt :** 2 décembre 1985.

(30) **Priorité :**

(43) **Date de la mise à disposition du public de la demande :** BOPI « Brevets » n° 23 du 5 juin 1987.

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

(71) **Demandeur(s) :** *REMERY Patrick et BOULE Jean Pierre.* — FR.

(72) **Inventeur(s) :** Patrick Remery et Jean Pierre Boule.

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

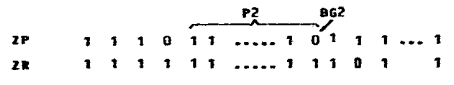
(74) **Mandataire(s) :** Brevatome.

(54) Procédé de paiement électronique à l'aide d'une carte à mémoire.

(57) Procédé de paiement électronique à l'aide d'une carte à mémoire.

Selon l'invention, pour effectuer un paiement, on grille des bits dans une mémoire EPROM. Cette mémoire est partagée en deux zones : une zone de paiement ZP et une zone de rechargement ZR. Le montant d'une transaction est défini par le nombre de bits à 1 situés entre le bit que l'on grille et le dernier bit grillé lors de la transaction précédente.

Application au paiement électronique.



FR 2 591 007 - A1

PROCEDE DE PAIEMENT ELECTRONIQUE A L'AIDE D'UNE CARTE A MEMOIRE

La présente invention a pour objet un procédé de paiement électronique à l'aide d'une carte à mémoire.

Le fonctionnement actuel des systèmes de paiement électronique de petites sommes consiste en l'utilisation de cartes à mémoire dites "porte-jetons".

On sait que la carte à mémoire est un support plastique dont les dimensions sont conformes aux normes ISO 2894 et 3554. Sur ce support est implanté un composant électronique contenant un microprocesseur. Celui-ci contient une mémoire de données de plusieurs centaines de bits réalisée en technologie "EPROM". On sait qu'il s'agit là d'une mémoire à lecture seulement, programmable électriquement une fois (Electrically Programmable Read Only Memory).

Le traitement effectué dans la carte à mémoire "porte-jetons" consiste à faire correspondre à chaque bit d'une zone de la mémoire de données, une unité de paiement dite "jeton". Un terminal point de vente, muni d'un lecteur de cartes, exécute une transaction par "grillage" de bits dans la mémoire de données. Le "grillage" d'un bit consiste à faire passer électriquement un élément binaire de la mémoire de l'état binaire "1" correspondant au crédit d'une unité à l'état binaire "0" correspondant à un crédit nul. La mémoire de données étant réalisée en technologie "EPROM", ce changement d'état est électriquement irréversible.

Les défauts de ce système sont multiples : d'une part, il n'est pas possible de recharger la carte, et d'autre part, la consommation de bits est élevée : le nombre de bits grillés est en effet égal au nombre d'unités à débiter.

Le but de l'invention est de remédier à ces inconvénients. A cette fin, la mémoire EPROM est parta-

gée en deux zones d'égale capacité. La structure physique et logique de l'EPROM permet d'associer à chaque bit un rang. Deux bits sont dits homologues s'ils ont même rang dans les deux zones ; ils forment un couple noté (x, y) où x est la valeur binaire (0 ou 1) du bit de la première zone, dite "zone de paiement" et où y est la valeur binaire du bit de la deuxième zone, dite "zone de rechargement". Selon l'invention le crédit disponible dans la carte s'exprime en unités, le nombre d'unités disponibles étant égal au nombre de couples (1,1) dont le rang est à la fois supérieur à 1 ou au rang du couple (0,1) de rang le plus élevé, si un tel couple (0,1) existe, et inférieur au rang d'un couple limite déterminé.

Selon une première variante, ce couple déterminé limitant le nombre d'unités disponibles est le dernier couple (1,1) de la mémoire. Autrement dit le crédit disponible est limité par la capacité de la mémoire.

Selon une deuxième variante le couple déterminé limitant le nombre d'unités disponibles est un couple butée (1,0) obtenu en écrivant un 0 dans la zone de rechargement.

Enfin, selon une troisième variante le couple déterminé limitant le nombre d'unités disponibles est, parmi des couples butées (1,0), celui qui a le rang le plus élevé.

Selon l'invention, pour effectuer une opération de débit de la carte de p unités, on grille un bit et un seul dans la zone de paiement selon la procédure suivante :

- on recherche le couple (0,1) de rang r_0 le plus élevé,

- on recherche le $p^{ième}$ couple (1,1) de rang r_p supérieur à r_0,

- on grille le bit de rang r_p en zone de paiement si ce rang est inférieur au rang du couple limite, lequel est défini selon l'une des trois variantes définies plus haut.

Pour effectuer une opération de crédit de la carte, on grille des bits dans la zone de rechargement pour annuler des opérations de débit antérieures et ceci en faisant passer les couples (0,1) à l'état (0,0), ces couples étant ignorés par la suite.

Pour limiter le crédit rechargé dans la carte, on peut faire passer un couple (1,1) à l'état (1,0) - couple butée - sans annuler ou en annulant les couples butées précédents, c'est-à-dire en faisant passer un couple butée (1,0) à l'état (0,0) ignoré par la suite. Si les couples butées ne sont pas utilisés, on peut limiter le crédit rechargé par un paiement fictif, en faisant passer un couple (1,1) à l'état (0,1).

Par rapport à l'art antérieur (porte-jetons), la consommation de bits se trouve réduite quand le paiement moyen dépasse deux unités. En effet, un paiement implique le grillage d'un bit en zone de paiement, et le réemploi des couples inutilisés implique le grillage du bit homologue en zone de rechargement, soit 2 bits au total.

En fait, lors du rechargement la limitation de la somme rechargée conduit à griller des bits supplémentaires. En pratique on peut considérer que le nombre de bits grillés par opération est compris entre 2 et 3.

Les caractéristiques de l'invention apparaîtront mieux après la description qui suit, d'un exemple de réalisation de l'invention. Cette description se réfère à des dessins annexés sur lesquels :

- la figure 1 illustre l'état initial de la mémoire ;

- la figure 2 illustre l'écriture d'une butée dans la zone de chargement ;

- la figure 3 illustre une opération de premier paiement ;

- la figure 4 illustre une opération de deuxième paiement ;

- la figure 5 montre l'état de la mémoire en fin de première utilisation ;

- la figure 6 illustre l'opération de détermination du montant à recharger dans une carte ;

- la figure 7 illustre l'opération de mise à (0,0) des couples (0,1) et (1,0) lors du rechargement ;

- la figure 8 montre l'état de la mémoire après écriture d'une nouvelle butée (1,0).

Dans la description qui suit on se placera dans la variante où le crédit disponible est limité par un couple butée (1,0) et un seul.

L'état initial de la mémoire avec ses zones de paiement ZP et de rechargement ZR est représenté sur la figure 1. Tous les bits sont à 1. Un bit à 0 dans la zone de rechargement ZR définit une butée BB1 comme représenté sur la figure 2.

Une première transaction d'un montant P1 est effectuée par un terminal point de vente dans lequel est introduite la carte, en comptant, depuis le début de la zone ZP, un nombre de 1 égal à P1 (ici P1=4). Ce comptage définit le bit à griller BG1. Ce bit est mis à 0 (figure 3).

Une deuxième transaction correspondant à un paiement d'un montant P2 est obtenue en grillant le bit BG2 situé à P2 emplacements de BG1 (figure 4).

Ces paiements sont possibles puisque le rang du bit mis à 0 est inférieur au rang de la butée BB1. Mais la transaction est impossible dès que le rang r_p du bit que l'on devrait griller est supérieur au rang du couple de butée.

Dans la pratique, la zone de rechargement est protégée. Lorsque la carte est introduite dans un terminal point de vente, celui-ci n'a accès qu'à la zone de paiement ZP au moyen d'une première clé et ne peut griller que les bits de cette zone. Seul l'organisme émetteur de la carte est habilité à griller des bits dans la zone de rechargement ZR. Ces opérations de rechargement s'effectuent donc en introduisant la carte dans un terminal spécial, qui est un terminal de chargement. Cette protection est obtenue par l'utilisation d'une clé connue du seul terminal de rechargement. Ce terminal calcule d'abord le montant résiduel MR de la carte. C'est le nombre de couples (1, 1) qui subsiste entre le dernier couple (0, 1) et le couple définissant la butée (1, 0). (Figure 5). Puis il calcule le nouveau montant à recharger : c'est la somme du montant résiduel MR et de la somme versée SV par le titulaire de la carte. Le terminal cherche ensuite le bit de butée à griller. Pour cela, il compte, depuis le début des zones, un nombre de couples (1, 1) égal au montant à recharger SV+MR (figure 6). Les couples à l'état (1, 0), (0, 1) et (0, 0) sont ignorés dans ce comptage. Si le nombre de couples à l'état (1, 1) est inférieur au montant à recharger, plus 1, l'opération est impossible.

Le rechargement précédent est remis à zéro en faisant passer tous les couples (1, 0) et (0, 1) à l'état (0, 0) (figure 7). Ces couples (0, 0) seront ensuite ignorés dans toutes les opérations ultérieures. Finalement, le terminal grille le bit BB2 qui définit la nouvelle butée (figure 8).

A titre d'exemple, on peut utiliser des mémoires de 50 mots de 32 bits, dont 28 sont utiles (4 bits sont réservés pour le système d'exploitation de la carte). Les tailles des zones de paiement et de rechar-

gement sont donc de 50x14=700 bits. Le nombre de bits grillés par paiement étant de 1, le nombre théorique de paiements est de 700. En fait, il est inférieur à ce nombre car les bits grillés pour définir des butées et les bits restant en fin de validité de la carte, sont perdus. De façon plus précise, on peut prendre l'exemple d'un rechargement constant minimum de 100 unités et de paiements moyens de 10 unités. Les bits inutilisables car leur nombre ne permet pas un rechargement sont donc au nombre de 100. On ne peut donc effectuer que 545 paiements. D'où une consommation moyenne de 2,56 bits par opération. Le montant global de ces paiements s'élève ainsi à 545x10=5450 unités.

Si l'on veut améliorer la précision des paiements en multipliant par 2 le nombre de bits comptés par paiement, soit 20 unités, les rechargements seront de 200 unités. Le nombre de paiements sera alors de 455 d'où une consommation moyenne de 3,07 bits par opération. Le montant global des paiements sera de 455x20=9100 unités.

En conséquence, la précision sur les unités est doublée au détriment du nombre total de paiements diminué de 20%.

L'invention apporte des protections spécifiques vis-à-vis des agressions possibles de la part d'un porteur de carte essayant de masquer des paiements ou de faire des rechargements illicites. A cet égard, les points suivants doivent être soulignés :

- la lecture des zones de paiement et de rechargement est libre,

- l'écriture de 0 dans la zone de chargement n'est possible que sous présentation d'une clé : tout passage des couples à l'état (1, 1) et (0,1) à l'état (1,0) ou (0,0) est impossible sans présenter à la carte une clé détenue par l'organisme émetteur et lui seul,

- l'écriture de 0 en zone de paiement a pour conséquence, pour le couple (1,1) qui passe à (0,1) :

- d'être sans effet sur le montant disponible dans la carte, si elle est faite sur des couples précédant le dernier couple à l'état (0,1) ou situés après le couple butée à l'état (1,0),

- d'ajouter des paiements fictifs dans la carte si elle est faite sur des couples situés entre le dernier couple à l'état (0,1) et le couple butée à l'état (1,0).

Pour le couple butée à l'état (1,0), le passage à l'état (0,0) aura pour conséquence de rendre invalide la carte car au prochain paiement, plus aucune butée n'apparaîtra.

En conséquence, une écriture indue en zone de paiement ne peut jamais avoir pour conséquence la création de monnaie ; la carte ne peut être créditée que par des écritures en zone de rechargement sous contrôle de la clé de l'organisme émetteur.

REVENDICATIONS

1. Procédé de paiement électronique utilisant une carte à mémoire EPROM chargée à l'origine de bits à l'état 1 pouvant être grillés, c'est-à-dire mis à l'état 0 de façon irréversible, ce procédé étant caractérisé par le fait que :

- la mémoire est divisée en deux zones d'égales capacités, une première zone dite zone de paiement et une seconde zone dite zone de rechargement, les bits ayant, dans ces deux zones, un rang déterminé, un bit de valeur x dans la première zone étant dit homologue d'un bit de valeur y dans la seconde zone, s'ils ont même rang, ces deux bits définissant alors un couple (x, y), des couples (1,1), (1,0), (0,1) et (0,0) pouvant être ainsi écrits dans la mémoire,

- le crédit disponible dans la carte s'exprime en unités, le nombre d'unités disponibles étant égal au nombre de couples (1,1) dont le rang est supérieur à 1 ou au rang du couple (0,1) de rang le plus élevé, lorsqu'un tel couple (0,1) existe, et inférieur au rang d'un couple limite déterminé.

2. Procédé selon la revendication 1, caractérisé par le fait que le couple limite déterminé limitant le nombre d'unités disponibles est le dernier couple (1,1) de la mémoire.

3. Procédé selon la revendication 1, caractérisé par le fait que le couple déterminé limitant le nombre d'unités disponibles est un couple butée (1,0) obtenu en écrivant un 0 dans la zone de rechargement.

4. Procédé selon la revendication 1, caractérisé par le fait que le couple déterminé limitant le nombre d'unités disponibles est, parmi des couples butées (1,0), celui qui a le rang le plus élevé.

5. Procédé selon les revendications 1 à 4, caractérisé par le fait que, pour effectuer une opéra-

tion de débit de la carte de p unités, on grille un bit et un seul dans la zone de paiement selon la procédure suivante :

- on recherche le couple (0,1) de rang r_0 le plus élevé,
- on recherche le $p^{ième}$ couple (1,1) de rang r_p supérieur à r_0,
- on grille le bit de rang r_p en zone de paiement si ce rang est inférieur au rang du couple limite, sinon l'opération est impossible.

6. Procédé selon la revendication 1, caractérisé par le fait qu'on effectue une opération de crédit de la carte en grillant des bits dans la zone de rechargement pour annuler des opérations de débit antérieures et ceci en faisant passer les couples (0,1) à l'état (0,0), ces couples étant ignorés par la suite.

7. Procédé selon les revendications 2, 5 et 6, caractérisé par le fait que, lors d'une opération de crédit de la carte, le montant du crédit est ajusté en faisant passer un couple (1,1) à l'état (0,1) (paiement fictif).

8. Procédé selon les revendications 3, 4 et 6, caractérisé par le fait que, lors d'une opération de crédit de la carte, le montant du crédit est ajusté en faisant passer un couple (1,1) à l'état (1,0) pour créer un couple butée.

9. Procédé selon la revendication 8, caractérisé par le fait que l'on annule un couple butée (1,0) précédent en grillant le bit à 1 de la zone de paiement pour faire passer le couple (1,0) à l'état (0,0), ce couple étant ignoré par la suite.

10. Procédé selon la revendication 1, caractérisé par le fait que l'écriture en zone de paiement est effectuée dans des automates de paiement acceptant la carte, et n'est possible que sur présentation d'une première clé connue par tous ces automates de paiement.

11. Procédé selon la revendication 1, caractérisé par le fait que l'écriture en zone de rechargement est effectuée dans un automate de rechargement sous contrôle de l'organisme délivrant la carte et n'est possible que sur présentation d'une seconde clé connue par les automates de rechargement agréés par cet organisme.

FIG. 1

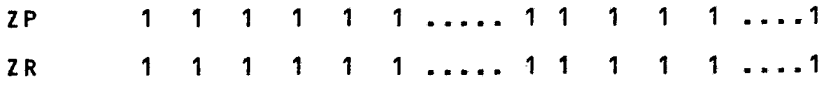


FIG. 2

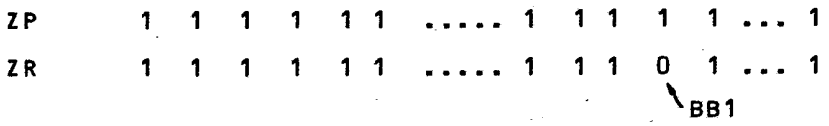


FIG. 3

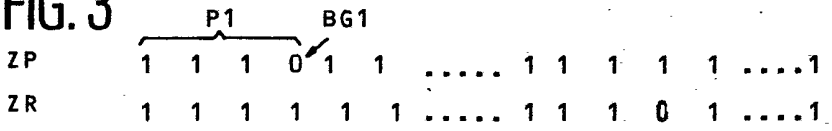


FIG. 4

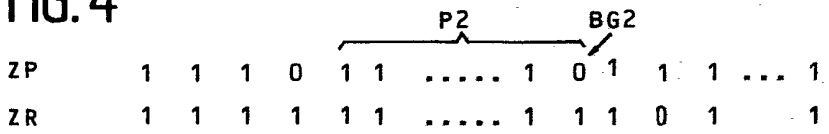


FIG. 5

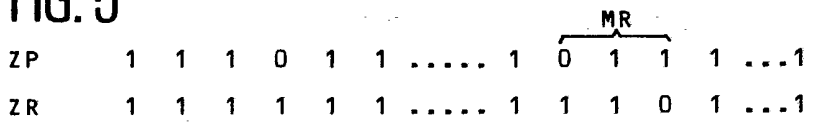


FIG. 6

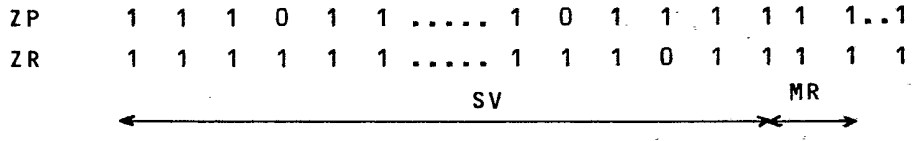


FIG. 7

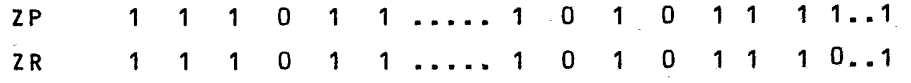


FIG. 8

