(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) N° de publication : **2 707 027**
(à n'utiliser que pour les commandes de reproduction)

(21) N° d'enregistrement national : **93 07875**

(51) Int Cl[5] : G 06 K 19/073

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt** : 25.06.93.

(30) **Priorité** :

(43) **Date de la mise à disposition du public de la demande :** 30.12.94 Bulletin 94/52.

(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) :** *SCHLUMBERGER INDUSTRIES* — FR.

(72) **Inventeur(s) :** Rhelimi Alain et Rigal Vincent.

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

(74) **Mandataire :** Schlumberger Technologies Propriété Intellectuelle.

(54) Dispositif électronique et portatif de comptage d'unités.

(57) La présente invention concerne un dispositif portatif de comptage d'unités en bits avec une mémoire électronique effaçable et ré-inscriptible pour stocker lesdites unités consommables qui donnent à un utilisateur des titres à des services ou produits.

Pour éviter des actions frauduleuses, l'invention propose un dispositif portatif qui permet une gestion améliorée des unités et qui ne nécessite aucune redondance mais qui évite tout résultat aberrant en cas de retrait anticipé.

FR 2 707 027 - A1

DISPOSITIF ELECTRONIQUE ET PORTATIF DE COMPTAGE D'UNITES

La présente invention concerne un dispositif portatif de comptage d'unités en bits avec une mémoire électronique effaçable et ré-inscriptible pour stocker lesdites unités.

De façon plus précise, l'invention concerne particulièrement un tel dispositif portatif comme par exemple une carte avec une mémoire contenant des unités consommables qui donnent à un utilisateur des titres à des services ou produits.

On connaît de telles télécartes pour des publiphones par exemple dont la première génération utilisait la méthode de comptage dite "à jeton", consistant à changer de manière irréversible l'état d'un bit pour compter une unité. Cette méthode correspondait aux possibilités des mémoires dites EPROM. Elle présentait l'avantage d'être facilement sécurisée, un compteur d'unités ne pouvant progresser que dans un sens.

Ladite méthode présente toutefois trois inconvénients. D'une part un rechargement est impossible. D'autre part, le nombre d'unités a été limité sévèrement par la taille mémoire du composant. Enfin, l'accès à la mémoire se fait de manière séquentielle, ce qui impose un logiciel relativement complexe dans le publiphone et, dans certains cas, un temps d'accès aux bits pertinents relativement long.

Un autre génération de carte a permis de remédier à ces problèmes. Elle utilise des cellules mémoire EEPROM et une méthode de comptage dite "par boulier".

Cette seconde génération présente également des inconvénients.

En premier lieu, le nombre d'unités possible dans une cellule mémoire EEPROM est souvent limité (typiquement 10 000 cycles d'écriture effacement). Compter un nombre plus élevé suppose donc une redondance, qui augmente de nouveau la taille mémoire, ainsi qu'un circuit logique complexe.

En second lieu, ces cartes sont généralement apparentes dans le lecteur, et peuvent être retirées par un utilisateur à tout moment. Si cela se produit pendant le processus d'écriture, le résultat peut être profondément altéré. Dans certains cas, la mémoire est effacée par mots avant d'être réécrite, le compteur peut donc être remis à zéro. Dans certaines configurations du compteur, il faut d'une part écrire des bits, d'autre part en effacer. Le retrait de la carte entre ces deux moments peut conduire à un résultat aberrant : rechargement partiel de la carte, consommation d'un nombre d'unités trop important. Il est donc fait appel, là encore, à des redondances et à des circuits spécialisés coûteux.

Pour éviter ces problèmes énoncés ci-dessus, l'objet de l'invention est de fournir un dispositif portatif qui permet une gestion améliorée des unités et qui ne nécessite aucune redondance mais qui évite tout résultat aberrant en cas de retrait anticipé.

Afin d'atteindre ce but l'invention propose un tel dispositif portatif de comptage d'unités en bits, avec une mémoire électronique effaçable et ré-inscriptible pour stocker lesdites unités, comportant également un circuit logique qui compte les unités d'une manière que le comptage

d'une unité ne fait intervenir qu'un changement d'état d'un seul bit et en ce que la mémoire de comptage et le circuit logique d'incrémentation (ou de décrémentation) sont sur un composant électronique unique.

Egalement, le dispositif portatif selon l'invention donne d'autres avantages supplémentaires :

- On obtient aussi toujours sans redondance, une capacité de comptage supérieure au nombre de cycles d'effacement-écriture des cellules mémoire.
- Enfin, l'invention permet de simplifier les ordres d'écriture vers la carte, et dans certains cas de les accélérer.

D'autres caractéristiques de l'invention appraîtront aux revendications.

L'invention sera mieux comprise à la lecture de la description de plusieurs modes de réalisation de l'invention donnés à tire d'exemples non limitatifs.

Le dispositif de comptage comporte n bits d'EEPROM ou de tout autre type de mémoire effaçable électriquement. Plutôt que d'utiliser la méthode usuelle de comptage, où le bit de rang p pèse 2p, le dispositif selon l'invention utilise un code réfléchi. L'avantage essentiel de ce système est que l'incrémentation du compteur (ou sa décrémentation) se fait par changement d'un bit unique.

Voici un exemple de compteur de ce type, sur 3 bits

VALEUR	CODIFICATION USUELLE	CODIFICATION INVENTIVE
0	000	000
1	001	001
2	010	011
3	011	010

4	100	110
5	101	111
6	110	101
7	111	100

En cas de retrait pendant le comptage, l'unité peut ne pas être consommée mais l'erreur reste limitée à cette seule unité. On voit également, sur cet exemple, que le dernier bit ne change que 4 fois, contrairement à la méthode classique où il change 8 fois. Pour cette raison, il est ainsi possible d'augmenter le nombre d'unités comptées pour un même nombre de cycles d'écriture effacement. A une capacité de 10 000 cycles correspond une capacité maximale de comptage de 40 000 unités.

Avec ce type de compteur selon l'invention, on peut atteindre une plus grande capacité mémoire : un compteur de n bits permet de compter jusqu'à 2^n unités 32 000 pour 15 bits par exemple.

Plusieurs types de codage connus offrent l'avantage d'une telle codification décrite. Pour certains d'entre eux, par exemple pour celui qui est décrit dans le tableau ci-dessus (GRAY CODE), l'algorithme d'incrémentation (ou de décrémentation) est trop simple. Il peut avantageusement être réalisé sous forme de logique câblée dans le dispositif portatif, ou sous la forme d'un programme très simple pour un microprocesseur.

Ceci met en évidence un autre avantage anti-fraude de l'invention : la gestion du compteur peut se faire de manière sécurisée. Il est ainsi possible de concevoir un dispositif portatif qui ne connait qu'un seul ordre, l'ordre d'incrémentation ; dans ce cas, aucun accès direct

à la mémoire n'est possible. Le temps de réaction du dispositif peut ainsi être raccourci.

Il est également possible de donner des accès directs à la mémoire, sans perdre cet avantage de sécurité. On peut ainsi prévoir une instruction de lecture du contenu du compteur. On peut également prévoir une instruction de rechargement, ou plus généralement d'écriture directe dans la mémoire, conditionnée par un mécanisme de sécurisation : présentation d'une clé secrète de rechargement ou de personnalisation, présentation d'un "PIN code", etc.

Il est également possible de doter le dispositif de plusieurs compteurs du type proposé.

Ceci présente plusieurs avantages. On peut par exemple gérer plusieurs compteurs ayant chacun une valeur monétaire différente. Cela permet de débiter en une fois (une seule instruction d'incrémentation) une valeur importante ou au contraire une valeur faible.
On peut aussi gérer plusieurs applications dans le même objet portatif, pour en faire une carte multi-services par exemple.

On obtient ainsi un avantage de coût (lié à la simplicité du circuit de comptage) d'autant plus important que le nombre d'applications gérées est grand. Dans ce dernier cas, il peut-être important que chaque application bénéficie de sa propre protection. Les différents prestataires des services qui gèrent ces applications n'ont en effet alors pas besoin de partager des secrets (des clés de rechargement par exemple).

REVENDICATIONS

1. Dispositif portatif de comptage d'unités en bits, avec une mémoire électronique effaçable et ré-inscriptible pour stocker lesdites unités caractérisé en ce que le dispositif comporte également un circuit logique qui compte les unités d'une manière que le comptage d'une unité ne fait intervenir qu'un changement d'état d'un seul bit et en ce que la mémoire de comptage et le circuit logique d'incrémentation (ou de décrémentation) sont sur un composant électronique unique.

2. Dispositif selon la revendication 1, caractérisé en ce que le composant électronique comporte un circuit électronique supplémentaire qui permet que chaque bit peut-être écrit ou effacé individuellement.

3. Dispositif selon la revendication 1, caractérisé en ce que le circuit logique d'incrémentation (ou de décrémentation) est un microprocesseur programmable.

4. Dispositif selon l'une des revendications précédentes, caractérisé en ce que le dispositif portatif comporte des moyens qui contrôlent que l'accès à la fonction de comptage n'est rendue possible que sous conditions d'une clé secrète ou de l'identification d'une application.

5. Dispositif selon l'une des revendications précédentes, caractérisé en ce que le dispositif est muni des moyens qui contrôlent que l'accès direct au compteur, sans passage par la fonction d'incrémentation (ou de décrémentation) est rendu possible sous conditions d'une clé secrète ou de l'identification d'une application.

6. Dispositif selon l'une des revendications précédentes, caractérisé en ce qu'il dispose de plusieurs compteurs.

7. Dispositif selon la revendication 6, caractérisé en ce que les compteurs ont des valeurs différentes.

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

2707027

N° d'enregistrement national

FA 487060
FR 9307875

DOCUMENTS CONSIDERES COMME PERTINENTS		Revendications concernées de la demande examinée
Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes	
Y	EP-A-0 268 106 (GAO) * abrégé; revendications; figures 1-3 * * colonne 4, ligne 25 - colonne 6, ligne 32 *	1
A		2,3

Y	CH-A-607 799 (ATO) * abrégé; revendications; figures * * page 3, colonne de gauche, ligne 31 - colonne de droite, ligne 20 *	1
A		5

A	DE-A-35 33 740 (ROBERT BOSCH) * abrégé; revendications; figures * * colonne 3, ligne 35 - colonne 4, ligne 65 *	1-7

A	EP-A-0 421 409 (IBM) * abrégé; figures 2,4 * * page 4, ligne 19 - page 5, ligne 37 *	1-3

A	EP-A-0 423 035 (GEMPLUS CARD INTERNATIONAL)	

A	FR-A-2 667 192 (GEMPLUS CARD INTERNATIONAL)	

A	GB-A-2 180 083 (MOTOROLA)	

DOMAINES TECHNIQUES RECHERCHES (Int.Cl.5)
G07F H03K

1

Date d'achèvement de la recherche	Examinateur
17 Mars 1994	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)