

12

DEMANDE DE BREVET D'INVENTION

A1

22 Date de dépôt : 01.07.92.

30 Priorité :

71 Demandeur(s) : T.R.T. TELECOMMUNICATIONS
RADIOELECTRIQUES ET TELEPHONIQUES Société
Anonyme — FR.

72 Inventeur(s) : Goudard Jean-Louis.

43 Date de la mise à disposition du public de la
demande : 07.01.94 Bulletin 94/01.

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

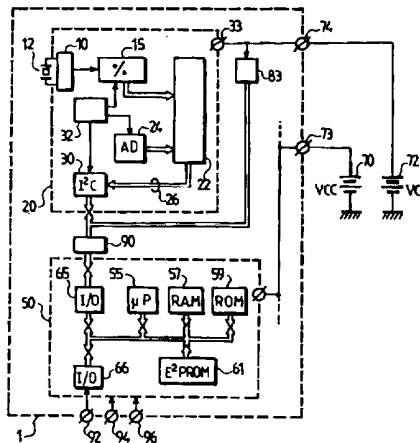
60 Références à d'autres documents nationaux
apparentés :

73 Titulaire(s) :

74 Mandataire : Chaffraix Jean.

54 Circuit d'horloge pour dispositif de jeu.

57 Ce circuit d'horloge est formé d'un oscillateur (10-12)
couplé à un circuit compteur-diviseur (15) muni d'accès de
lecture (30). Pour éviter que ses données soient falsifiées
ce circuit se présente sous la forme d'un boîtier protégé et il
est prévu un circuit d'accès protégé (50) connecté entre
lesdits accès et le circuit compteur-diviseur.
Application au jeu.



FR 2 693 295 - A1



"Circuit d'horloge pour dispositif de jeu".

Description :

La présente invention concerne un circuit d'horloge pour dispositif de jeu notamment, formé d'un oscillateur-générateur de fréquence d'horloge couplé à un circuit compteur-diviseur.

5 Ce genre de circuit est bien connu et trouve d'importantes applications.

Cependant il y a certaines applications où des exigences nouvelles sont imposées, notamment dans le domaine des jeux. On pourra à ce sujet consulter le brevet
10 US 5 073 931.

Dans ce brevet, on propose à des joueurs un dispositif qui permet d'enregistrer des paris sur l'issue d'un événement qui se déroule devant leurs yeux. Le moment du pari ne peut donc pas être postérieur à cette issue. Si le montant
15 de l'enjeu est important, un tel dispositif risque d'être la proie de fraudes. Notamment il importe que le moment du pari ne soit pas falsifié ; un joueur malhonnête peut essayer d'affecter un moment antérieur à son pari, alors qu'il l'a fait en connaissant l'issue du jeu.

20 L'invention propose donc un circuit d'horloge qui a pour but de s'opposer à ce genre de fraude.

Pour cela, un tel circuit est remarquable en ce qu'il est intégré et qu'il est muni d'un circuit de sécurité qui protège ses données en sortie.

25 La description suivante, accompagnée des dessins ci-annexés, le tout donné à titre d'exemple non limitatif, fera bien comprendre comment l'invention peut être réalisée.

La figure 1 montre le schéma du circuit conforme à l'invention.

La figure 2 montre une variation du circuit conforme à l'invention.

Le circuit d'horloge proposé par l'invention porte, à la figure 1, la référence 1. Il est constitué essentiellement par un oscillateur 10 piloté par un quartz 12 et par un compteur-diviseur 15. Ces composants peuvent faire partie d'un circuit intégré 20 du genre immatriculé sous le n° PCF8583. Le contenu de ce compteur-diviseur fournit différentes informations de date à une mémoire RAM 22 adressée par un organe d'adressage 24. Ces informations de sortie sont : l'année, le mois, le jour, les heures, les minutes, les secondes, etc... D'autres informations peuvent être contenues dans cette mémoire : des informations d'alarmes, de statut, etc... Les informations contenues dans cette mémoire peuvent être lues sur une ligne 26 connectée à sa sortie. Une interface 30 permet une communication du genre I²C vers l'extérieur du circuit 20. Un organe de logique 32 permet de commander tout le fonctionnement de ce circuit 20. Ce circuit 20 est alimenté par une tension appliquée à une borne 33.

Conformément à l'invention, pour éviter que les informations élaborées par ce circuit 20 soient falsifiées, on a prévu un circuit de sécurité 50 intégré, sous forme hybride ou non, sur le même substrat que le circuit 20.

L'intégration évite qu'une intervention puisse s'effectuer à l'intérieur du circuit 1. Cette intégration peut s'accompagner d'un enrobage de tout le circuit, ce qui rend toute intrusion encore plus improbable.

Le circuit de sécurité est par exemple constitué par un circuit du genre immatriculé sous le n° MC6805SC24. Ce circuit est formé d'un microprocesseur 55 auquel sont rattachées une mémoire RAM 57, une mémoire ROM 59 qui contient les instructions pour le fonctionnement du microprocesseur 55 et également une mémoire EEPROM 61 qui peut contenir différentes données non effaçables par coupure de l'alimentation.

Ce circuit est utilisé habituellement dans les cartes à puce du genre décrit dans l'ouvrage :

LES CARTES A MICROCIRCUIT
TECHNIQUES ET APPLICATIONS

5 de F. GUEZ, C. ROBERT et A. LAURET
paru en France aux éditions MASSON.

Pour communiquer, ce circuit comporte un ensemble d'accès 65 et 66 dont une partie 65 est affectée aux communications à l'intérieur du circuit 1 et l'autre partie 66
10 aux communications vers l'extérieur.

Selon un premier mode de réalisation le circuit 1 est alimenté par deux sources de tension 70 et 72 par l'intermédiaire de deux bornes d'alimentation 73 et 74. La source 72 est prévue pour alimenter uniquement le circuit 20.

15 Selon un deuxième mode de réalisation, le circuit 1 est alimenté par les deux mêmes bornes de tension 70 et 72. Mais, de préférence, c'est la source 70 qui alimente les circuits, même le circuit 20. Si cette source manifeste une défaillance, ceci est détecté par un analyseur de tension
20 d'alimentation 80 (figure 2) qui, dans ce cas, connecte un commutateur de tension 82 pour que le circuit 20 soit alimenté par la source de tension 70.

L'intérêt de ces mesures est que l'on peut garantir une certaine autonomie de ce circuit d'horloge (quelques années compte tenu de sa faible consommation) alors que l'alimentation
25 de l'environnement pour lequel il travaille peut nécessiter plusieurs changements de piles (source 70).

Cependant si la tension d'alimentation du circuit 20 vient à être interrompue, ceci est détecté par un autre
30 analyseur de tension 83 connecté à la borne d'alimentation 33. L'information de rupture de tension peut être reflétée par l'état des données contenues dans la mémoire 22. L'état de cette tension d'alimentation peut également être analysé par le circuit 50 en lui communiquant la détection faite par
35 l'analyseur 83 lors de ses accès I²C au circuit 20.

Pour permettre une communication entre ce bus et le circuit de sécurité 50, un circuit d'interface 90 a été prévu. Le programme assure la communication sur ce bus en respectant le protocole défini par les mesures relatives au bus I²C.

5 L'information concernant l'horloge est rendue accessible via le circuit 50 sur un accès 92. Le circuit 1 porte, outre les bornes d'alimentation 73 et 74, deux autres accès 94 et 96 pour, respectivement, la re-initialisation du circuit et l'application des signaux d'horloge nécessaires au
10 processeur 55.

Le circuit 50 opère, selon un mode de fonctionnement préférentiel, selon l'algorithme de cryptage-décryptage DES, tel que défini, par exemple, dans la publication :

15 Federal Information Processing Standards Publication
(FIPS PUB46) du 15 janvier 1977
du Bureau National des Standards du Ministère du Commerce américain.

20 Dans la mémoire EEPROM est enregistrée une clé de chiffrement C.

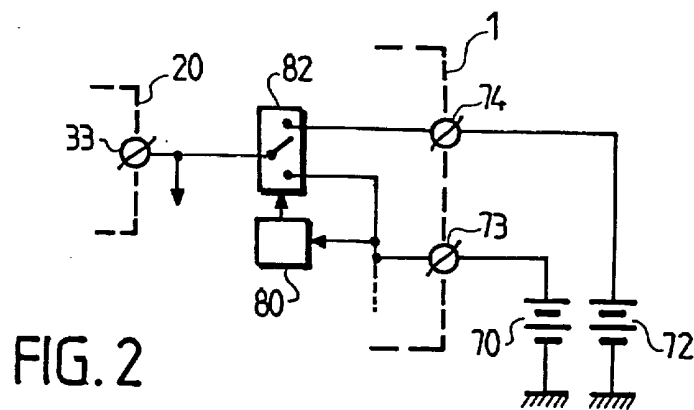
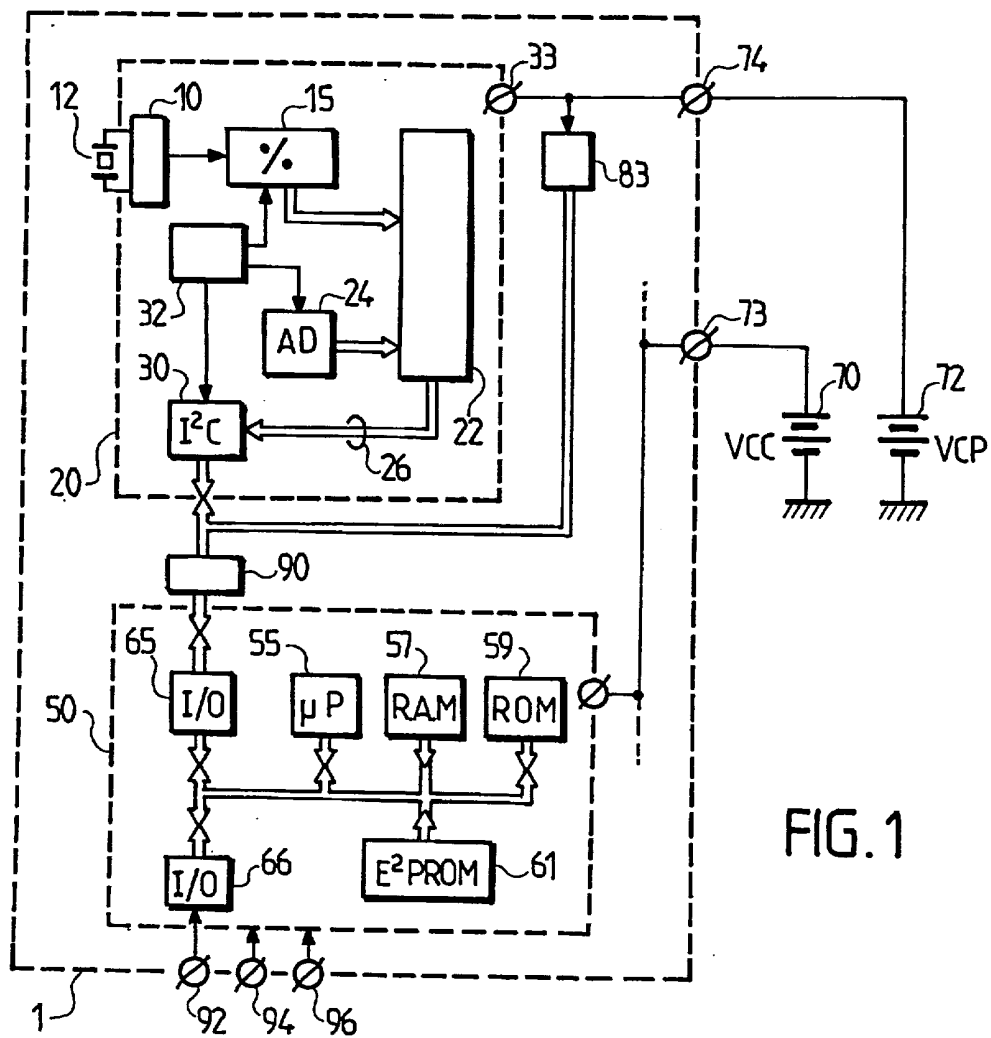
Ainsi, à l'accès 92 la date DAT peut être en clair, mais elle est accompagnée d'un code DES (C, DAT). Ainsi, on peut vérifier l'intégrité de cette date DAT, si bien entendu on connaît C, toute précaution étant prise pour que cette clé C
25 demeure inconnue à tout fraudeur potentiel.

Il est possible de compliquer le processus en envoyant au circuit d'horloge 1 un aléa "a", de sorte que la date soit accompagnée d'un code DES (C, a, DAT).

Revendications :

1. Circuit d'horloge pour dispositif de jeu notamment, formé d'un oscillateur-générateur de fréquence d'horloge couplé à un circuit compteur-diviseur munis d'accès de lecture,
5 caractérisé en ce que ce circuit se présente sous la forme d'un boîtier protégé, en ce qu'il est prévu un circuit d'accès protégé connecté entre lesdits accès et le circuit de compteur-diviseur.
2. Circuit d'horloge selon la revendication 1,
10 caractérisé en ce que le boîtier protégé est réalisé par l'intégration de tout le circuit d'horloge.
3. Circuit d'horloge selon la revendication 1, caractérisé en ce que le boîtier protégé est réalisé par l'intégration hybride de composants disponibles dans le
15 commerce.
4. Circuit d'horloge selon l'une des revendications 1 à 3, caractérisé en ce que le circuit d'accès protégé est un circuit de carte à puce.
5. Circuit d'horloge selon la revendication 4,
20 caractérisé en ce que le circuit de carte à puce met en oeuvre l'algorithme DES.
6. Circuit d'horloge selon l'une des revendications 1 à 5, caractérisé en ce qu'il comporte un circuit de détection de présence de tension d'alimentation pour fournir une
25 information d'interruption de tension d'alimentation si elle se produit.
7. Circuit d'horloge selon l'une des revendications 1 à 6, caractérisé en ce qu'il comporte deux bornes d'alimentation, une première étant affectée à l'alimentation de

l'oscillateur et de son circuit de compteur associé, quand
l'autre est défaillante.



INSTITUT NATIONAL
de la
PROPRIETE INDUSTRIELLE

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

N° d'enregistrement
national

FR 9208099
FA 478057

DOCUMENTS CONSIDERES COMME PERTINENTS		Revendications concernées de la demande examinée
Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes	
A,D	US-A-5 073 931 (AUDEBERT) * colonne 2, ligne 39 - colonne 4, ligne 22 * * colonne 7, ligne 26 - colonne 8, ligne 18; figures *	1-5
A	US-A-3 806 874 (EHRAT) * abrégé; figures * * colonne 13, ligne 41 - colonne 14, ligne 39 *	1-5
A	DE-A-3 023 427 (GRETAG) * page 7, ligne 7 - page 11, ligne 5 * * page 13, ligne 4 - page 18, ligne 10; figures *	1,3,5,6
A	GB-A-2 148 135 (IGT) * page 7, ligne 122 - page 8, ligne 108; figures *	1,5
A	EP-A-0 418 098 (NCR) * abrégé; revendication 1; figures * * colonne 13, ligne 47 - colonne 14, ligne 4 *	1,3
A	GB-A-2 189 059 (DISTRIMEX) * abrégé; revendications; figures *	1,6
A	US-A-4 592 546 (FASCENDA)	
A	US-A-4 365 810 (RICHARDSON)	
		DOMAINES TECHNIQUES RECHERCHES (Int. Cl.5)
		G07C G07B G06F G06K G04C G04G A63F G07F G07D
Date d'achèvement de la recherche 19 MARS 1993		Examineur MEYL D.
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		