PCT ORGANISATION MONDIALE DE LA PROPRIETE INTELLECTUELLE
Bureau international

DEMANDE INTERNATIONALE PUBLIEE EN VERTU DU TRAITE DE COOPERATION EN MATIERE DE BREVETS (PCT)

(51) Classification internationale des brevets 6 :		(11) Numéro de publication internationale:
G07F 7/10, 7/08	A1	WO 95/30975
		(43) Date de publication internationale: 16 novembre 1995 (16.11.95)

(21) Numéro de la demande internationale: PCT/FR95/00591

(22) Date de dépôt international: 5 mai 1995 (05.05.95)

(30) Données relatives à la priorité:
94/05615 6 mai 1994 (06.05.94) FR

(71) Déposants *(pour tous les Etats désignés sauf US)*: FRANCE TELECOM [FR/FR]; 6, place d'Alleray, F-75015 Paris (FR). LA POSTE [FR/FR]; 4, quai du Point-du-Jour, F-92777 Boulogne-Billancourt (FR). COGECOM [FR/FR]; 20, avenue Rapp, F-75007 Paris (FR).

(72) Inventeurs; et
(75) Inventeurs/Déposants *(US seulement)*: PAILLES, Jean-Claude [FR/FR]; 4, rue des Loisirs, F-14610 Epron (FR). DELABALLE, Jacques [FR/FR]; 5, rue Georges-Vogt, F-92190 Meudon (FR).

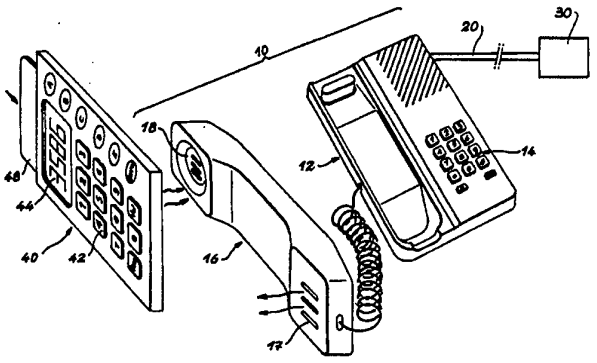
(74) Mandataire: SOCIETE DE PROTECTION DES INVENTIONS; 25, rue de Ponthieu, F-75008 Paris (FR).

(81) Etats désignés: JP, US, brevet européen (AT, BE, CH, DE, DK, ES, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Publiée
Avec rapport de recherche internationale.

(54) Title: SYSTEM FOR SECURE TELEPHONE TRANSACTIONS

(54) Titre: SYSTEME POUR TRANSACTIONS SECURISEES PAR TELEPHONE



(57) Abstract

System for secure telephone transactions comprising a telephone terminal (10) connected to a server (30) and a housing (40) comprising a keyboard (42), a microprocessor card (48) and means for generating sound signals. Card information is transmitted to the server by means of sound signals and the telephone terminal. In the other direction, information is vocally addressed to the user who responds using a keyboard (42) mounted on the housing (40). The system of the invention is suitable for secure telephone transactions, in particular, telepayments.

(57) Abrégé

Le système comprend un terminal téléphonique (10) relié à un serveur (30) et un boîtier (40) comprenant un clavier (42), une carte à microprocesseur (48), et des moyens d'émission de signaux sonores. La transmission des informations de la carte vers le serveur s'effectue par l'intermédiaire des signaux sonores et du terminal téléphonique. Dans l'autre sens, les informations sont adressées de manière vocale à l'utilisateur qui les tape sur le clavier (42) du boîtier (40). Application aux télétransactions sécurisées, notamment au télépaiement.

UNIQUEMENT A TITRE D'INFORMATION

Codes utilisés pour identifier les Etats parties au PCT, sur les pages de couverture des brochures publiant des demandes internationales en vertu du PCT.

AT	Autriche	**GB**	Royaume-Uni	**MR**	Mauritanie
AU	Australie	**GE**	Géorgie	**MW**	Malawi
BB	Barbade	**GN**	Guinée	**NE**	Niger
BE	Belgique	**GR**	Grèce	**NL**	Pays-Bas
BF	Burkina Faso	**HU**	Hongrie	**NO**	Norvège
BG	Bulgarie	**IE**	Irlande	**NZ**	Nouvelle-Zélande
BJ	Bénin	**IT**	Italie	**PL**	Pologne
BR	Brésil	**JP**	Japon	**PT**	Portugal
BY	Bélarus	**KE**	Kenya	**RO**	Roumanie
CA	Canada	**KG**	Kirghizistan	**RU**	Fédération de Russie
CF	République centrafricaine	**KP**	République populaire démocratique de Corée	**SD**	Soudan
CG	Congo			**SE**	Suède
CH	Suisse	**KR**	République de Corée	**SI**	Slovénie
CI	Côte d'Ivoire	**KZ**	Kazakhstan	**SK**	Slovaquie
CM	Cameroun	**LI**	Liechtenstein	**SN**	Sénégal
CN	Chine	**LK**	Sri Lanka	**TD**	Tchad
CS	Tchécoslovaquie	**LU**	Luxembourg	**TG**	Togo
CZ	République tchèque	**LV**	Lettonie	**TJ**	Tadjikistan
DE	Allemagne	**MC**	Monaco	**TT**	Trinité-et-Tobago
DK	Danemark	**MD**	République de Moldova	**UA**	Ukraine
ES	Espagne	**MG**	Madagascar	**US**	Etats-Unis d'Amérique
FI	Finlande	**ML**	Mali	**UZ**	Ouzbékistan
FR	France	**MN**	Mongolie	**VN**	Viet Nam
GA	Gabon				

SYSTEME POUR TRANSACTIONS SECURISEES PAR TELEPHONE

DESCRIPTION

Domaine technique

La présente invention a pour objet un système pour transactions sécurisées par téléphone. Elle trouve une application dans le télépaiement, le télévote, les jeux, les paris à distance, etc...

Etat de la technique

Les télétransactions, ou transactions à distance, se sont beaucoup développé ces dernières années. Elles utilisent le réseau téléphonique reliant un terminal téléphonique à un serveur. Ce dernier envoie des messages vocaux à l'usager, lequel répond en utilisant les touches du clavier du terminal téléphonique. Les signaux adressés en retour au serveur sont généralement du type DTMF (Dual Tone Multi-Frequency).

Dans des systèmes plus évolués, le serveur est capable d'interpréter certains mots prononcés par l'usager, pris dans un vocabulaire restreint.

Dans cette utilisation particulière du téléphone, il apparaît un besoin impérieux de sécurité lorsque la transaction est de type monétaire (télépaiement) et, d'une manière générale, lorsque des risques de fraude sont à craindre.

Pour répondre à ce besoin, on peut équiper un terminal téléphonique d'une prise supplémentaire informatique, du genre RS 232, et connecter à cette prise un lecteur de carte à microprocesseur (appareil désigné généralement par l'abréviation LECAM), ce lecteur comprenant un logiciel et des moyens appropriés d'émission et de réception de données à destination et

en provenance du serveur. Dans ce lecteur de carte, on insère une carte à microprocesseur (dite encore carte à puce), capable d'accomplir des fonctions sécuritaires, comme la vérification d'un code confidentiel, l'authentification d'une entité extérieure, l'aide à l'authentification de la carte par une entité extérieure, l'enregistrement d'un droit, etc. Ces fonctions mettent en jeu des algorithmes utilisant des clés cryptographiques, des tirages aléatoires de nombres, des comparaisons, etc...

Si ces moyens donnent satisfaction, ils présentent néanmoins l'inconvénient de nécessiter des terminaux téléphoniques munis d'une prise périphérique informatique. Or, les terminaux téléphoniques ordinaires ne sont généralement pas équipés de telle prise. Il faut donc changer de terminal pour pouvoir mettre en oeuvre de telles transactions sécurisées.

La présente invention a justement pour but de remédier à cet inconvénient en offrant un moyen simple d'effectuer des télétransactions avec les terminaux téléphoniques habituels.

Exposé de l'invention

A cette fin, l'invention propose d'associer au terminal téléphonique habituel des moyens de sécurisation constitués par un boîtier portable muni d'un clavier à touches, d'un écran d'affichage et d'un émetteur de signaux acoustiques apte à coopérer avec le microphone du terminal téléphonique, ce boîtier pouvant accueillir une carte à microprocesseur apte à exécuter des fonctions sécuritaires. Cette carte est reliée au clavier, à l'écran et à l'émetteur de signaux acoustiques.

L'échange d'informations nécessaire à la sécurisation d'une transaction s'effectue alors de manière différente selon le sens des informations : dans le sens carte-serveur, c'est l'émetteur acoustique du boîtier et le microphone du terminal téléphonique qui assurent la liaison par le biais des signaux acoustiques émis par le boîtier ; dans le sens serveur-carte, c'est le haut-parleur du terminal téléphonique, l'utilisateur et le clavier à touches qui assurent la liaison, l'utilisateur frappant le message vocal délivré par le haut-parleur sur le clavier pour que ce message soit transmis à la carte.

On voit donc que l'utilisateur est l'un des maillons de la chaîne de transmission, dans le sens serveur-carte. Dans l'autre sens (carte-serveur), la transmission est automatique. Mais cette intervention manuelle de l'opérateur ne pose pas de problème car, dans la pratique, le message transmis par le serveur est généralement court, quelques chiffres (4 par exemple) suffisant le plus souvent à assurer les fonctions de sécurité.

On observera que des boîtiers munis d'un émetteur acoustique DTMF apte à coopérer avec un terminal téléphonique existent déjà, notamment pour composer automatiquement des numéros de téléphone. Si ces boîtiers contiennent des mémoires, ils ne contiennent pas de cartes à microprocesseur capables de mettre en oeuvre des algorithmes de sécurité et ils ne requièrent pas l'intervention de l'utilisateur dans l'un des sens de transmission.

Le boîtier portatif utilisable dans la présente invention peut être d'un type particulier que le déposant désigne par CARTULETTE (marque déposée). Il

s'agit d'un boîtier contenant une carte à puce, et qui est équipé d'un écran et d'un clavier. La CARTULETTE sert, notamment, à vérifier le contenu d'une carte à puce.

Brève description des dessins

- la figure 1 montre le schéma général du système de l'invention,
- les figures 2a et 2b montrent le boîtier en vue de face et en vue de côté,
- la figure 3 montre l'organisation fonctionnelle du boîtier,
- la figure 4 montre un premier diagramme d'échange de messages entre un serveur et une carte,
- la figure 5 montre un deuxième diagramme d'échange de messages entre un serveur et une carte,
- la figure 6 montre un troisième diagramme d'échange de messages entre un serveur et une carte,
- la figure 7 montre un quatrième diagramme d'échange de messages entre un serveur et une carte.

Exposé détaillé de modes de réalisation

On voit, sur la figure 1, un système conforme à l'invention et comprenant un terminal téléphonique 10, relié par un réseau téléphonique 20 à un serveur 30, ainsi qu'un boîtier portatif 40.

Le terminal 10 comprend classiquement un poste 12 avec un clavier à touches 14 et un combiné 16 muni d'un haut-parleur 17 et d'un microphone 18.

A ce terminal 10 est associé un boîtier portatif 40 comprenant un clavier 42, un écran d'affichage 44 et une carte à microprocesseur 48 qui, pour plus de clarté, est représentée en léger dépassement mais qui,

en fonctionnement normal, est complétement introduite dans le boîtier. Le boîtier 40 comprend, par ailleurs, à l'arrière, des moyens pour émettre des signaux acoustiques (comme on le verra sur la figure 2a). En fonctionnement, le boîtier est donc plaqué sur le microphone 18 du combiné téléphonique 16, les moyens d'émission sonore étant disposés en regard du microphone.

La figure 2a montre le boîtier en vue de face et la figure 2b montre ce même boîtier en vue de profil. Il ne s'agit naturellement que d'un exemple de réalisation. Sur la face avant, les touches A, B, C, D, E sont des touches de fonctions spécifiques de l'application envisagée : télépaiement, télévote, jeux, paris, ... La touche Ann sert à annuler les caractères frappés et affichés sur l'afficheur ; la touche Val sert à valider les caractères frappés, et à faire progresser le dialogue utilisateur-boîtier. La touche Envoi sert à provoquer l'envoi d'un message vers le serveur. En pratique, il faudra que l'émission ne commence qu'après quelques secondes, pour permettre à l'utilisateur de placer le boîtier 40 sur le microphone du combiné téléphonique.

Sur la figure 2b, on voit, à l'arrière du boîtier, des moyens 46 aptes à émettre des signaux acoustiques, par exemple de type DTMF.

La figure 3 montre l'organisation fonctionnelle du boîtier et de sa carte. On y trouve le clavier 42, l'écran d'affichage 44, les moyens 46 d'émission de signaux acoustiques DTMF. On y voit aussi un microprocesseur 50, une horloge 52, un connecteur de carte 54. Un bus 56 relie tous ces organes entre eux. Une protection physique 58 peut entourer le microprocesseur 50 et l'horloge 52.

Le microprocesseur comprend des mémoires de programme à lecture seule (ROM) et des mémoires à accès direct (RAM). L'horloge sert dans les cas où il faut horodater une opération effectuée par l'utilisateur pour permettre des vérifications ultérieures sur la date et l'heure de cette opération. Pour éviter certaines fraudes, il convient de faire en sorte qu'il soit impossible d'avancer ou retarder l'horloge. C'est le rôle de la protection physique 58 disposée autour de l'ensemble microprocesseur-horloge.

Avant de décrire quelques exemples de télétransactions pouvant être effectuées avec le système de l'invention, on va rappeler quelques fonctions sécuritaires que peut remplir une carte à puce classique. De telles cartes à puce sont généralement introduites dans un terminal muni d'un clavier et d'un afficheur, comme c'est le cas, par exemple, pour les billetteries.

Dans ce qui suit, on désignera par k une clé cryptographique, sachant que chaque carte et chaque fonction sécuritaire peut avoir une clé spécifique. Mais pour simplifier, on supposera qu'il n'y a qu'une seule clé k.

Une carte à puce disposée dans un terminal peut accomplir au moins les cinq fonctions suivantes :

a) contrôle d'un code confidentiel (CC)

Le terminal envoie à la carte un code confidentiel CC. La carte vérifie que le code reçu est identique au code mémorisé. Si ce n'est pas le cas, la carte positionne un indicateur interne pour ne pas accepter d'autres ordres. Un comptage permet ainsi un blocage définitif, si trois codes faux ont été présentés successivement. Dans tous les cas, une réponse est envoyée à l'extérieur.

b) authentification de la carte et de tout ou partie de son contenu par une entité externe

Le terminal demande à la carte d'authentifier son contenu M, défini par exemple par une adresse et par une longueur. Le terminal envoie également (pour éviter des fraudes par rejeu), un aléa x. La carte calcule y=Fk(M,x), où k est une clé dédiée à cette fonction de sécurité, et F est la fonction cryptographique de la carte (algorithme DES par exemple).

c) authentification de la carte et de données externes

L'opération est analogue à l'opération b), où l'on ajoute au contenu M une donnée T fournie en même temps que x à la carte.

d) authentification par la carte d'une entité distante

L'entité extérieure demande à la carte un aléa. La carte calcule un aléa x à l'aide d'un générateur pseudo-aléatoire et l'envoie à l'entité extérieure. Cette entité effectue un calcul y=Fk(x), où k est la clé dédiée à cette fonction. L'entité extérieure connaît cette clé si elle est authentique. L'entité envoie le résultat "y" du calcul à la carte pour vérification. La carte effectue le même calcul y'=Fk(x), où k est la clé dédiée à cette fonction, clé qu'elle connaît également. La carte vérifie alors que le résultat "y" qu'elle a trouvé est identique au résultat "y" que l'entité extérieure lui avait transmis. La carteque envoie une réponse en conséquence. Si le test est négatif, la carte peut interdire les ordres qui suivent.

e) enregistrement d'un droit dans la carte, conditionné à l'authentification de l'entité extérieure à la carte

L'entité extérieure demande à la carte un aléa. La carte calcule un aléa x à l'aide d'un générateur pseudo-aléatoire et l'envoie à l'entité extérieure.

L'entité extérieure effectue un calcul y=Fk(D,x), où k est la clé dédiée à cette fonction et D un droit qu'elle connaît, si elle est authentique. La connaissance de la clé nécessite en général la connaissance, par l'entité, du numéro de la carte, pour qu'elle puisse reconstituer la clé spécifique à cette fonction. Le droit D est une information indiquant à la carte qu'il faut, par exemple, modifier un certain nombre d'octets, à telle adresse, et la nouvelle valeur de ces octets. C'est ce genre de fonctions que l'on trouve par exemple lorsqu'il s'agit de recharger un porte-monnaie. L'entité envoie "y" et D à la carte pour exécution. La carte effectue le même calcul et trouve un résultat y'=Fd(D,x) où k est la clé dédiée à cette fonction, clé que la carte connaît également. La carte vérifie que y'=y et, dans l'affirmative, exécute l'ordre de mise à jour, puis envoie une réponse en conséquence.

Toutes ces fonctions classiques peuvent être reprises et/ou adaptées dans le cas de l'invention :

a) Contrôle d'un code confidentiel

Le code en question est saisi sur le clavier du boîtier et présenté à la carte contenue dans le boîtier. L'écran affiche un message qui est fonction de la réponse fournie par la carte. La mise en oeuvre de cette fonction n'est donc vraiment pas spécifique de l'invention.

b) Authentification de la carte et de son contenu

Le serveur vérifie que la carte avec laquelle la communication est établie est authentique.

Un exemple où cette fonction est requise est une transaction bancaire, où M est le montant de la transaction enregistrée dans la mémoire de la carte. Cette transaction est illustrée sur la figure 4. Sur

cette figure, comme sur les suivantes, la transmission d'informations dans le boîtier est symbolisée par une flèche en trait continu, ce qui signifie que l'utilisateur utilise le clavier pour introduire ladite information. Les autres transmissions d'information sont représentées par des flèches en trait interrompu et représentent des signaux acoustiques (DTMF).

Les opérations mises en oeuvre sur la figure 4 sont les suivantes :

- le serveur envoie un message vocal x ;
- l'utilisateur tape le message x sur le clavier du boîtier ;
- le boîtier demande à la carte qu'elle contient d'effectuer un certain calcul propre à la transaction M, laquelle est repérée par une adresse aM dans la mémoire de la carte ; le boîtier transmet donc M et aM à la carte ;
- la carte calcule une quantité "y" égale à Fk(M,x) où k est la clé et F une fonction cryptographique paramètrée par k ;
- la carte envoie "y" au boîtier, qui l'émet par un signal acoustique directement vers le serveur sans intervention de l'utilisateur ;
- le serveur vérifie que "y" est bien égale à la quantité Fk(M,x) qu'il a pu calculer par ailleurs, si l'égalité est obtenue le serveur envoie un message sonore d'accord m à destination de l'utilisateur.

c) Authentification de la carte et de données externes

Un exemple d'utilisation de cette fonction est le cas où le serveur veut authentifier qu'une action a bien eu lieu dans le boîtier de l'utilisateur avant un instant donné D. Cette action a été mémorisée dans la carte à un instant T=T1. Il peut s'agir d'un vote par exemple, ou d'un pari, ou d'un jeu. La quantité M

contient donc le résultat de cette action et T1 l'instant indiqué par l'horloge. On suppose que le boîtier n'a pas forcément la même heure que le serveur, en raison, par exemple, d'une désynchronisation des horloges. Le serveur va donc tester les durées relatives au boîtier et au serveur entre l'instant du vote et l'instant de la télétransaction. Lors de la transaction avec le serveur, l'indication de l'horloge du boîtier est T=T2 ; celle du serveur est D'. Le serveur testera alors, après vérification du calcul effectué dans la carte, que la durée T2-T1 est supérieur à D'-D.

La suite des opérations est illustrée sur la figure 5. Elle est la suivante :

- le serveur envoie un message vocal x ;
- l'utilisateur tape x sur le clavier ;
- le boîtier demande à la carte d'effectuer un calcul propre à M d'adresse aM, et transmet donc à la carte x, aM et T ;
- la carte calcul y=Fk(M,T,x),
- le boîtier émet y, M, T par signaux acoustiques ;
- le serveur vérifie que le "y" reçu est bien égal à la quantité Fk(M,T,x) précalculée ;
- en cas d'accord, le serveur envoie un message d'accord m à destination de l'utilisateur.

d) Authentification par la carte d'une entité distante

L'utilisateur veut vérifier que le serveur est authentique, c'est-à-dire qu'il a été habilité par une autorité supérieure qui lui a communiqué la clé secrète k, laquelle est contenue également dans la carte. Le serveur montre qu'il connaît cette clé en effectuant le même calcul que la carte, sur un nombre x tiré aléatoirement par celle-ci. Le résultat obtenu par le serveur, soit y', est envoyé à l'utilisateur, qui le

tape sur le clavier. Le boîtier peut alors informer l'utilisateur du succès ou de l'échec de l'authentification du serveur.

Les opérations correspondantes sont illustrées sur la figure 6 :

- l'utilisateur frappe sur la touche correspondant à la focntion "authentification du serveur" ;
- le boîtier demande à la carte de tirer un nombre aléatoire ;
- la charte choisit un nombre x aléatoire, et transmet ce nombre au boîtier ;
- le boîtier émet un signal sonore permettant de transmettre x au serveur ;
- le serveur calcule un nombre "y" égal à Fk(x,D) ;
- le serveur transmet par message vocal le nombre y ;
- l'utilisateur frappe "y" sur le clavier ;
- le boîtier transmet "y" à la carte et demande de vérifier avec le nombre y' calculé par la carte avec y'=Fk(D,x) ;
- la carte commande l'affichage sur l'écran du résultat de la comparaison : correct ou incorrect.

En variante, cette fonction pourrait être aussi réalisée en utilisant la fonction b) de la carte : le boîtier demanderait à la carte d'effectuer le même calcul que celui qui a été demandé au serveur, et vérifierait elle-même l'égalité des deux résultats (au lieu que ceci soit fait dans la carte).

e) Inscription d'un droit dans la carte

Il s'agit d'inscrire dans la carte une information sensiblen par exemple un droit D, que seul un serveur habilité à le droit d'écrire ou de mettre à jour, et ceci grâce à une clé appropriée. Un exemple de cette

fonction est le rechargement d'une carte porte-monnaie. Les opérations sont illustrées sur la figure 7 :

- l'utilisateur frappe sur le clavier la touche appropriée à cette fonction ;
- le boîtier demande à la carte de tirer un nombre aléatoire ;
- la carte tire un aléa x et le transmet au boîtier ;
- le boîtier envoie vers le serveur, par les signaux acoustiques, à la fois x et le droit D ;
- le serveur calcule un nombre "y" égal à Fk(x,D) et envoie "y" par message vocal ;
- l'utilisateur tape "y" sur le clavier ;
- le boîtier demande à la carte une mise à jour du droit D et lui transmet D et y ;
- la carte calcule y'=Fk(D,x) et vérifie si "y'" est égal à "y" ; dans l'affirmative la carte met à jour D et renvoie une réponse au boîtier ;
- le boîtier affiche la réponse : correct (ou incorrect).

REVENDICATIONS

1. Système pour transactions sécurisées par téléphone comprenant :

a) un terminal téléphonique (10) avec un haut-parleur (17) et un microphone (18), ce terminal téléphonique (10) étant relié par un réseau téléphonique (20) à au moins un serveur (30),

b) des moyens de sécurisation contenant une carte à microprocesseur apte à sécuriser une transaction entre l'utilisateur du dispositif et un serveur, la sécurisation étant obtenue par échange bidirectionnel d'informations entre le serveur et la carte,

ce dispositif étant caractérisé par le fait que les moyens de sécurisation sont constitués par un boîtier portatif (40) muni d'un clavier à touches (42), d'un écran d'affichage (44), d'un émetteur de signaux acoustiques (46) apte à coopérer avec le microphone (18) du terminal téléphonique (10), ce boîtier portatif comprenant en outre une carte à microprocesseur (48) apte à exécuter des fonctions sécuritaires, cette carte (48) étant reliée au clavier (42), à l'écran (44) et à l'émetteur de signaux acoustiques (46), l'échange d'informations nécessaire à la sécurisation d'une transaction s'effectuant :

- dans le sens serveur (30)-carte (48) par le haut-parleur (17) du terminal téléphonique (10) et par le clavier à touches (42) sur lequel l'utilisateur frappe des données provenant du message vocal envoyé par le serveur (30) et émis par le haut-parleur (17) du terminal téléphonique (10),
- dans le sens carte (48)-serveur (30) par les signaux acoustiques émis par l'émetteur (46) de

signaux acoustiques et le microphone (18) du terminal téléphonique (10).

2. Système selon la revendication 1, caractérisé par le fait que l'émetteur des signaux acoustiques (46) est un émetteur de signaux DTMF.

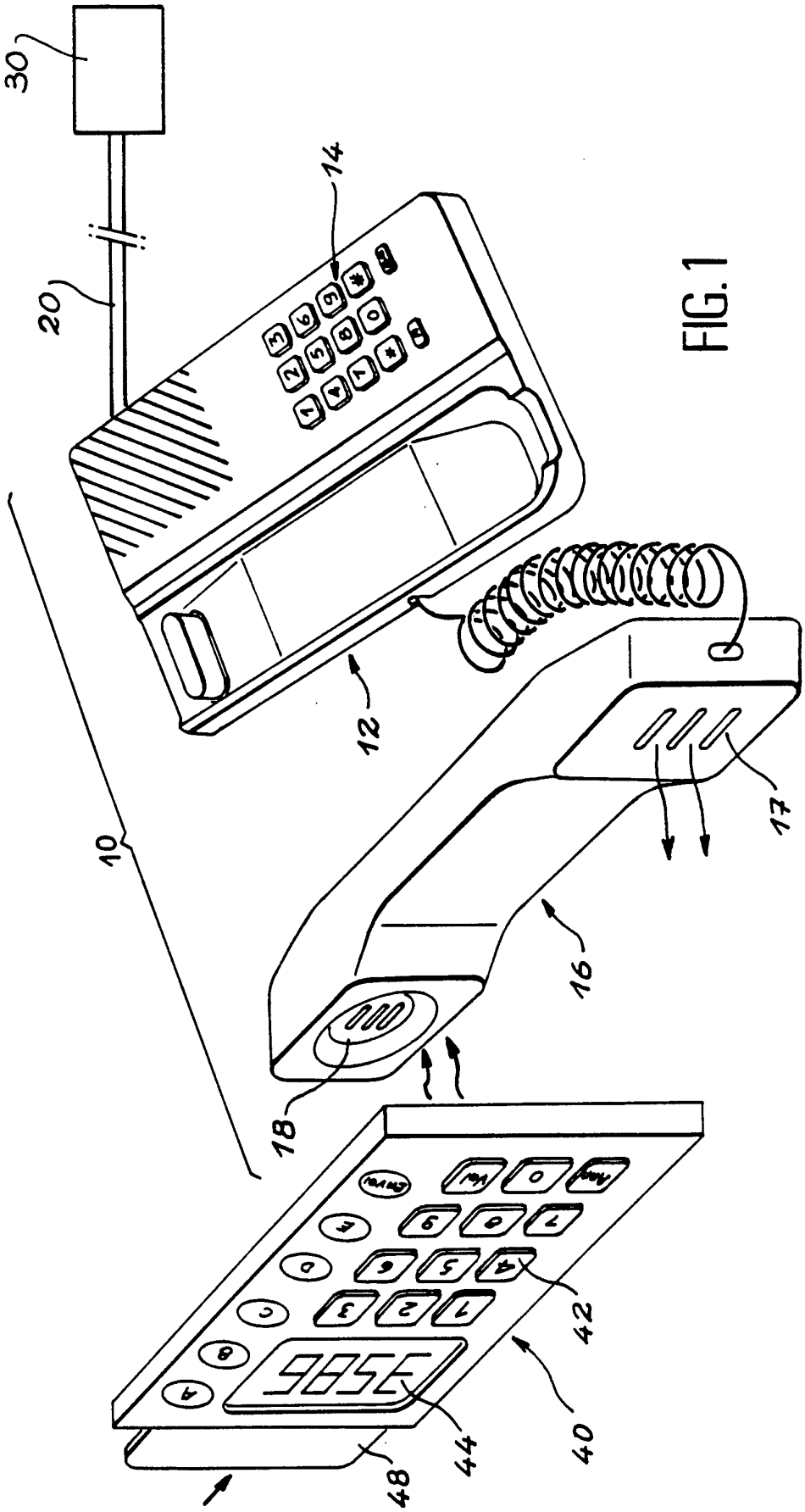


FIG. 1

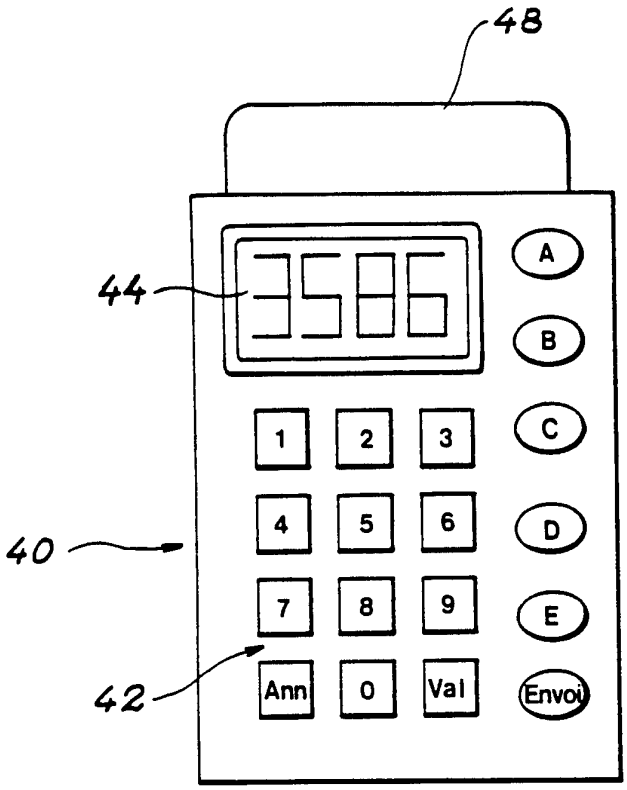


FIG. 2a

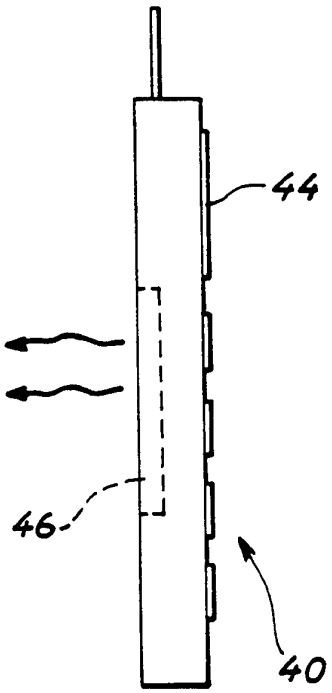


FIG. 2b

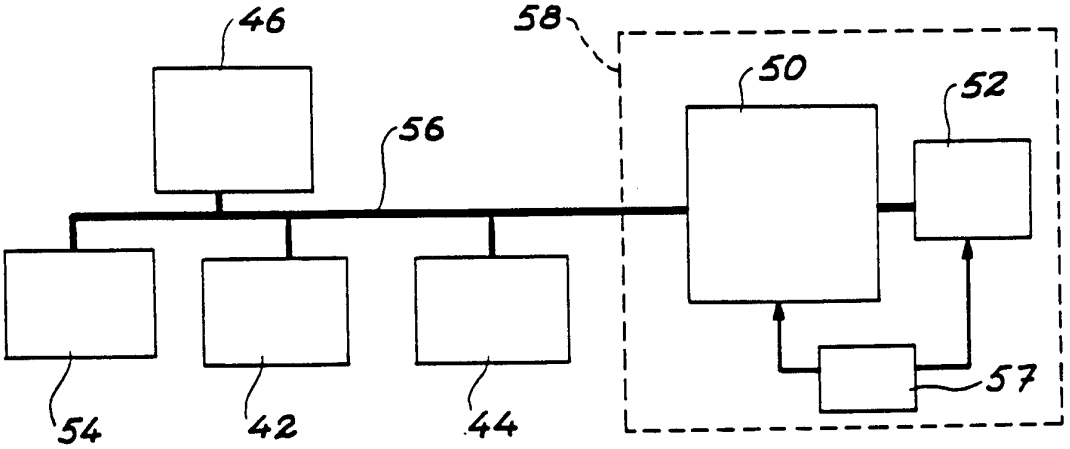


FIG. 3

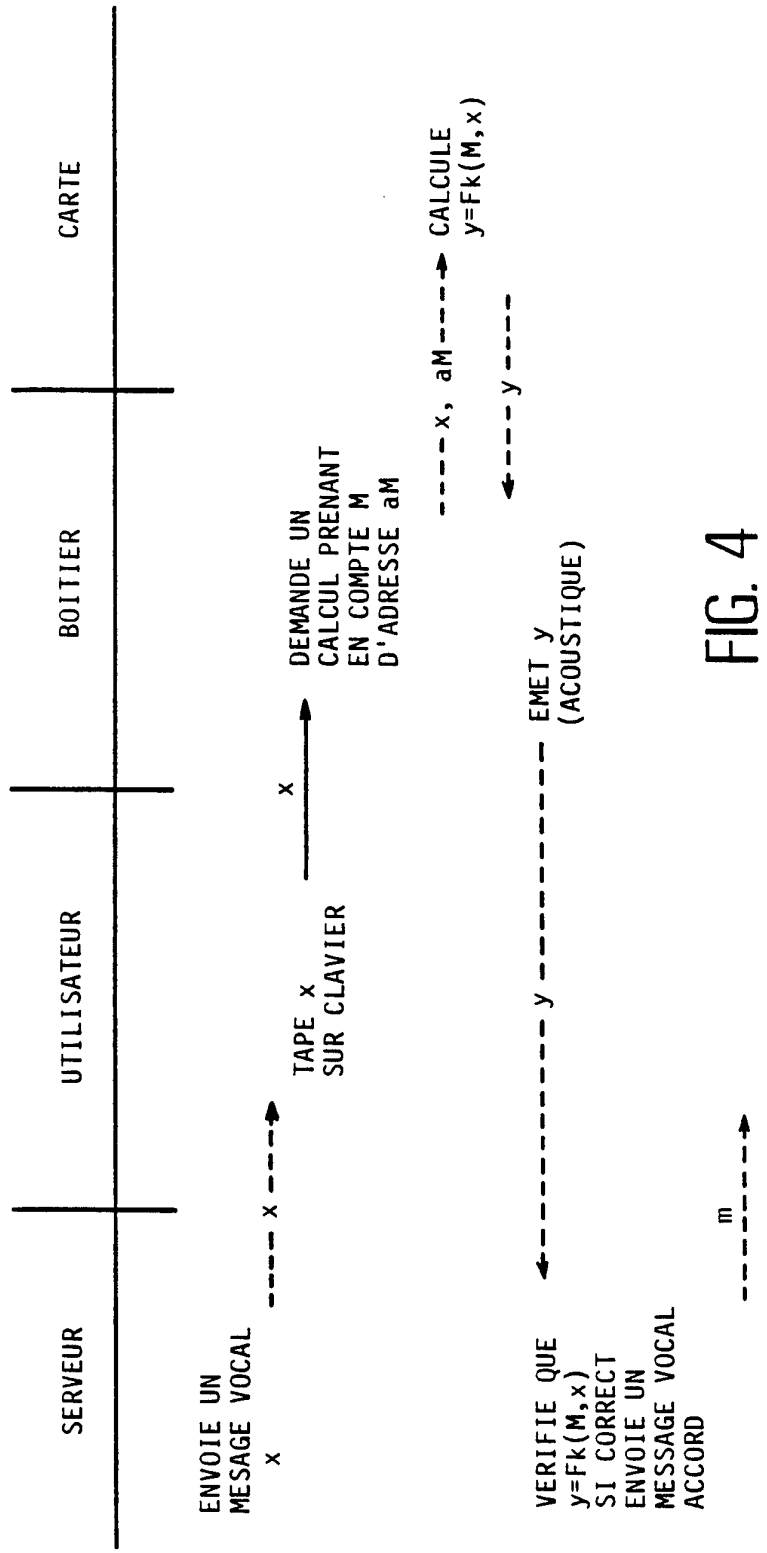

SERVEUR
UTILISATEUR
BOITIER
CARTE
ENVOIE UN MESAGE VOCAL x
x
TAPE x SUR CLAVIER
x
DEMANDE UN CALCUL PRENANT EN COMPTE M D'ADRESSE aM
x, aM
CALCULE y=Fk(M,x)
y
EMET y (ACOUSTIQUE)
y
VERIFIE QUE y=Fk(M,x) SI CORRECT ENVOIE UN MESSAGE VOCAL ACCORD
m

FIG. 4

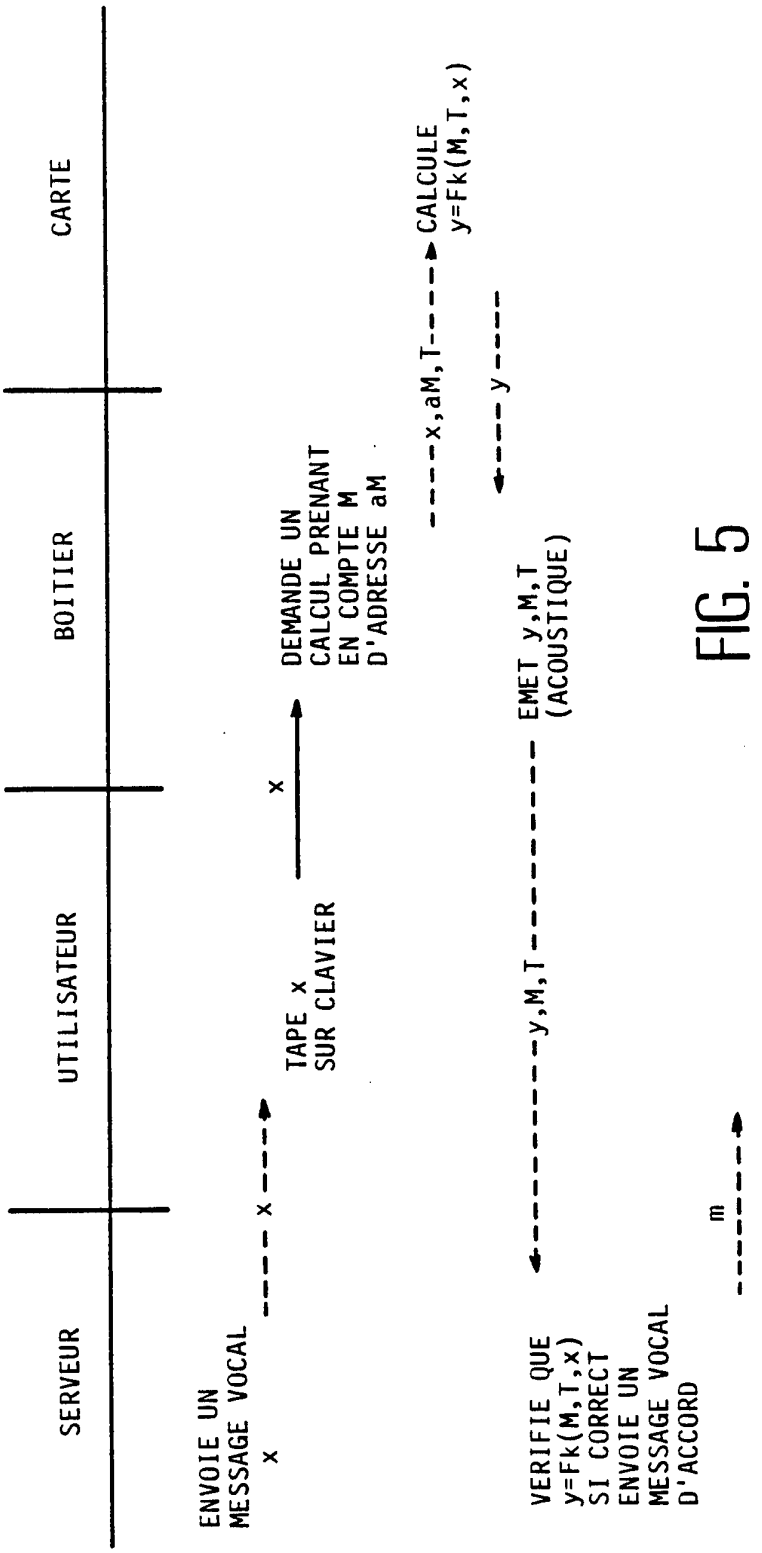

SERVEUR
UTILISATEUR
BOITIER
CARTE
ENVOIE UN MESSAGE VOCAL x
x
TAPE x SUR CLAVIER
x
DEMANDE UN CALCUL PRENANT EN COMPTE M D'ADRESSE aM
x,aM,T
CALCULE y=Fk(M,T,x)
y
EMET y,M,T (ACOUSTIQUE)
y,M,T
VERIFIE QUE y=Fk(M,T,x) SI CORRECT ENVOIE UN MESSAGE VOCAL D'ACCORD
m

FIG. 5

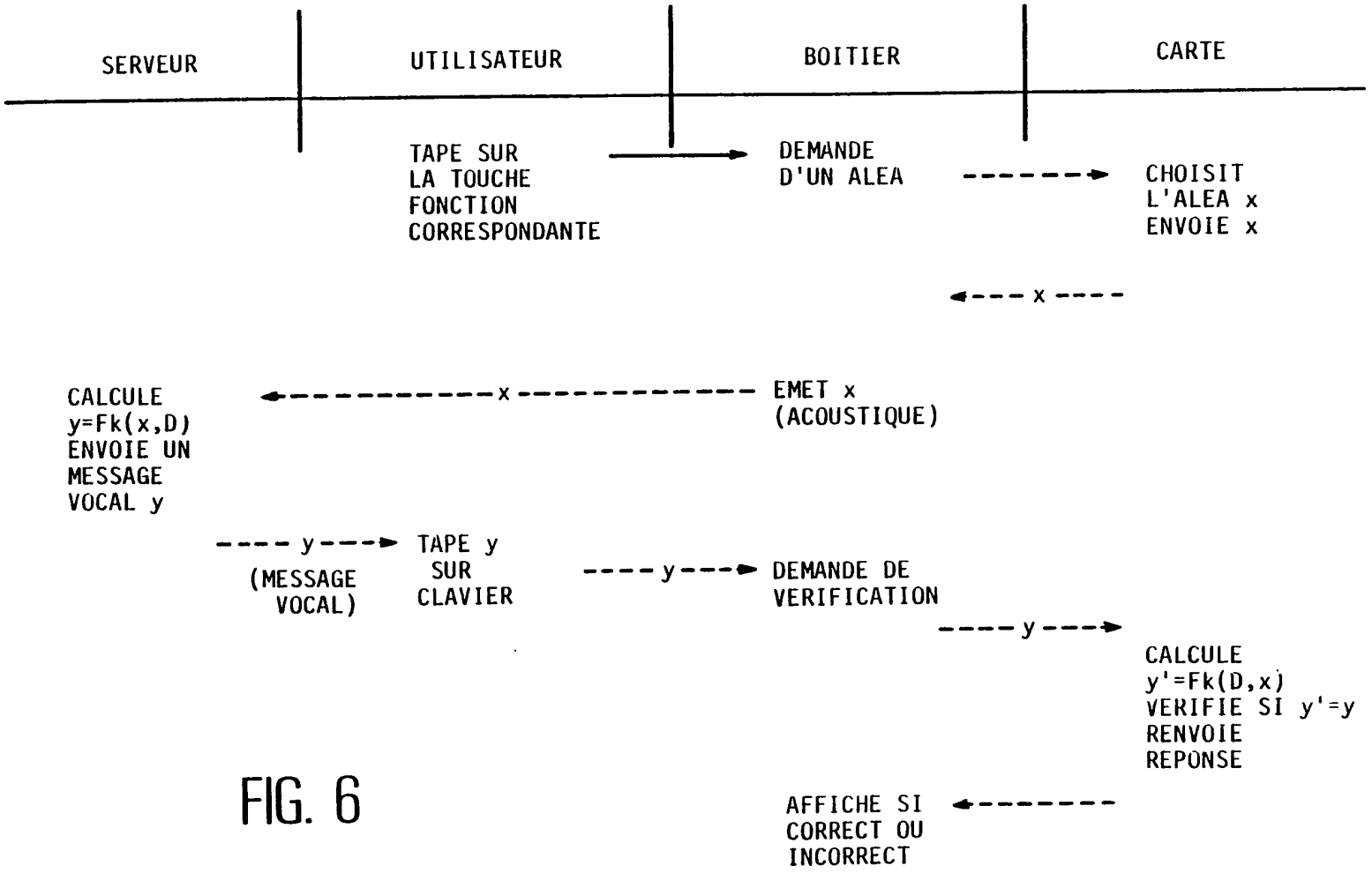

SERVEUR
UTILISATEUR
BOITIER
CARTE
TAPE SUR LA TOUCHE FONCTION CORRESPONDANTE
DEMANDE D'UN ALEA
CHOISIT L'ALEA x
ENVOIE x
x
CALCULE y=Fk(x,D) ENVOIE UN MESSAGE VOCAL y
x
EMET x (ACOUSTIQUE)
y (MESSAGE VOCAL)
TAPE y SUR CLAVIER
y
DEMANDE DE VERIFICATION
y
CALCULE y'=Fk(D,x) VERIFIE SI y'=y RENVOIE REPONSE
AFFICHE SI CORRECT OU INCORRECT

FIG. 6

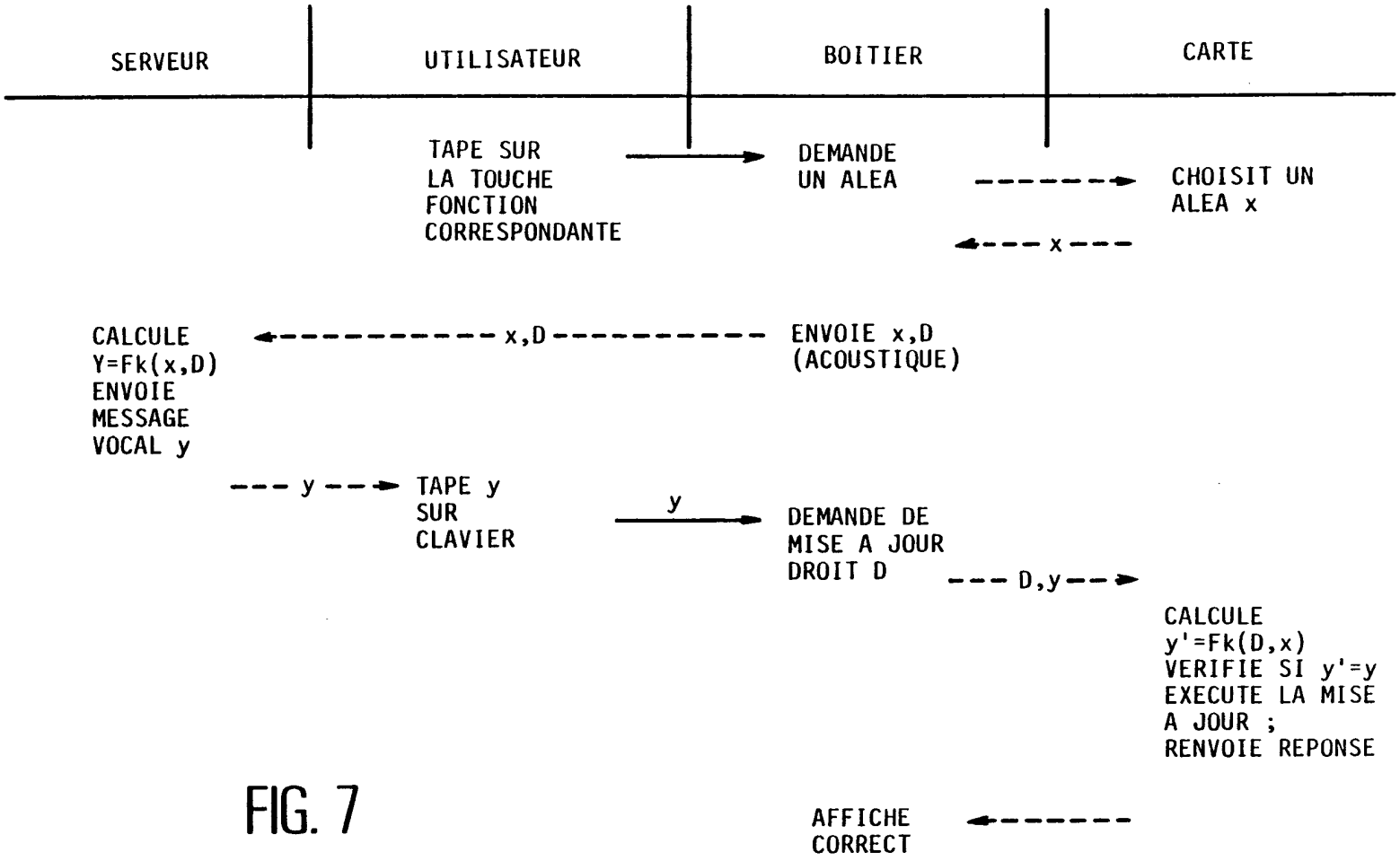

SERVEUR
UTILISATEUR
BOITIER
CARTE
TAPE SUR LA TOUCHE FONCTION CORRESPONDANTE
DEMANDE UN ALEA
CHOISIT UN ALEA x
x
CALCULE Y=Fk(x,D) ENVOIE MESSAGE VOCAL y
x,D
ENVOIE x,D (ACOUSTIQUE)
y
TAPE y SUR CLAVIER
y
DEMANDE DE MISE A JOUR DROIT D
D,y
CALCULE y'=Fk(D,x) VERIFIE SI y'=y EXECUTE LA MISE A JOUR ; RENVOIE REPONSE
AFFICHE CORRECT

FIG. 7

INTERNATIONAL SEARCH REPORT

Intern ıal Application No
PCT/FR 95/00591

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 G07F7/10 G07F7/08

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 G07F H04M

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indicatic where appropriate, of the relevant passages	Relevant to claim No.
Y	FR,A,2 663 442 (TOSHIBA) 20 December 1991 see abstract; claims; figures 1-5 see page 9, line 2 - page 10, line 29	1
Y	US,A,4 601 011 (A. GRYNBERG) 15 July 1986 see abstract; figures 1,6 see column 4, line 1 - column 5, line 51	1
A	EP,A,0 374 012 (ETAT FRANCAIS) 20 June 1990 see the whole document	1,2
A	EP,A,0 451 057 (A. BERNARD) 9 October 1991 see abstract; claims; figures	1
A	FR,A,2 621 199 (A.E.T.A.) 31 March 1989 see abstract; claims; figures 1,2	1,2

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
22 August 1995	1. 09. 95

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax (+31-70) 340-3016	David, J

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Inten al Application No
PCT/FR 95/00591

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	EP,A,0 565 279 (AMERICAN TELEPHONE AND TELEGRAPHE) 13 October 1993 ---	
A	EP,A,0 117 124 (FUJITSU) 29 August 1984 ---	
A	WO,A,91 07042 (TRANSACTION NETWORK) 16 May 1991 ---	
A	US,A,4 482 802 (K. AIZAWA) 13 November 1984 ---	
A	GB,A,2 211 050 (THE GENERAL ELECTRIC COMPANY) 21 June 1989 -----	

INTERNATIONAL SEARCH REPORT

Information on patent family members

Intern. al Application No
PCT/FR 95/00591

Patent document cited in search report	Publication date	Patent family member(s)		Publication date
FR-A-2663442	20-12-91	JP-A-	4024888	28-01-92
US-A-4601011	15-07-86	DE-A-	3248400	28-07-83
		GB-A-	2114791	24-08-83
EP-A-0374012	20-06-90	FR-A-	2640835	22-06-90
EP-A-0451057	09-10-91	FR-A-	2660771	11-10-91
		AT-T-	114066	15-11-94
		DE-D-	69105024	15-12-94
		DE-T-	69105024	24-05-95
		ES-T-	2065629	16-02-95
		JP-A-	6054088	25-02-94
		US-A-	5136632	04-08-92
FR-A-2621199	31-03-89	NONE		
EP-A-0565279	13-10-93	AU-B-	3533093	07-10-93
		JP-A-	6046162	18-02-94
		US-A-	5406619	11-04-95
EP-A-0117124	29-08-84	JP-A-	59151261	29-08-84
		US-A-	4675815	23-06-87
WO-A-9107042	16-05-91	US-A-	5050207	17-09-91
		AU-A-	5187590	31-05-91
		US-A-	5157717	20-10-92
US-A-4482802	13-11-84	JP-C-	1290736	29-11-85
		JP-A-	58050066	24-03-83
		JP-B-	60014385	12-04-85
GB-A-2211050	21-06-89	NONE		

RAPPORT DE RECHERCHE INTERNATIONALE

Dem. Internationale No
PCT/FR 95/00591

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
CIB 6 G07F7/10 G07F7/08

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)
CIB 6 G07F H04M

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si cela est réalisable, termes de recherche utilisés)

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie *	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
Y	FR,A,2 663 442 (TOSHIBA) 20 Décembre 1991 voir abrégé; revendications; figures 1-5 voir page 9, ligne 2 - page 10, ligne 29	1
Y	US,A,4 601 011 (A. GRYNBERG) 15 Juillet 1986 voir abrégé; figures 1,6 voir colonne 4, ligne 1 - colonne 5, ligne 51	1
A	EP,A,0 374 012 (ETAT FRANCAIS) 20 Juin 1990 voir le document en entier	1,2
A	EP,A,0 451 057 (A. BERNARD) 9 Octobre 1991 voir abrégé; revendications; figures	1

-/--

[X] Voir la suite du cadre C pour la fin de la liste des documents

[X] Les documents de familles de brevets sont indiqués en annexe

* Catégories spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent

"E" document antérieur, mais publié à la date de dépôt international ou après cette date

"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)

"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens

"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention

"X" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément

"Y" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier

"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée	Date d'expédition du présent rapport de recherche internationale
22 Août 1995	- 1. 09. 95

Nom et adresse postale de l'administration chargée de la recherche internationale	Fonctionnaire autorisé
Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+ 31-70) 340-2040, Tx. 31 651 epo nl, Fax (+ 31-70) 340-3016	David, J

RAPPORT DE RECHERCHE INTERNATIONALE

Dem . Internationale No
PCT/FR 95/00591

C.(suite) DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie *	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	FR,A,2 621 199 (A.E.T.A.) 31 Mars 1989 voir abrégé; revendications; figures 1,2	1,2
A	EP,A,0 565 279 (AMERICAN TELEPHONE AND TELEGRAPHE) 13 Octobre 1993	
A	EP,A,0 117 124 (FUJITSU) 29 Août 1984	
A	WO,A,91 07042 (TRANSACTION NETWORK) 16 Mai 1991	
A	US,A,4 482 802 (K. AIZAWA) 13 Novembre 1984	
A	GB,A,2 211 050 (THE GENERAL ELECTRIC COMPANY) 21 Juin 1989	

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Dem. Internationale No
PCT/FR 95/00591

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)		Date de publication
FR-A-2663442	20-12-91	JP-A-	4024888	28-01-92
US-A-4601011	15-07-86	DE-A-	3248400	28-07-83
		GB-A-	2114791	24-08-83
EP-A-0374012	20-06-90	FR-A-	2640835	22-06-90
EP-A-0451057	09-10-91	FR-A-	2660771	11-10-91
		AT-T-	114066	15-11-94
		DE-D-	69105024	15-12-94
		DE-T-	69105024	24-05-95
		ES-T-	2065629	16-02-95
		JP-A-	6054088	25-02-94
		US-A-	5136632	04-08-92
FR-A-2621199	31-03-89	AUCUN		
EP-A-0565279	13-10-93	AU-B-	3533093	07-10-93
		JP-A-	6046162	18-02-94
		US-A-	5406619	11-04-95
EP-A-0117124	29-08-84	JP-A-	59151261	29-08-84
		US-A-	4675815	23-06-87
WO-A-9107042	16-05-91	US-A-	5050207	17-09-91
		AU-A-	5187590	31-05-91
		US-A-	5157717	20-10-92
US-A-4482802	13-11-84	JP-C-	1290736	29-11-85
		JP-A-	58050066	24-03-83
		JP-B-	60014385	12-04-85
GB-A-2211050	21-06-89	AUCUN		