

①②

DEMANDE DE BREVET D'INVENTION

A1

②② Date de dépôt : 18.11.03.

③① Priorité :

④③ Date de mise à la disposition du public de la
demande : 20.05.05 Bulletin 05/20.

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

⑥① Références à d'autres documents nationaux
apparentés :

⑦① Demandeur(s) : ATMEL GRENOBLE S.A. Société ano-
nyme — FR.

⑦② Inventeur(s) : MAINGUET JEAN FRANCOIS et
FRANCIOLI FABRICE.

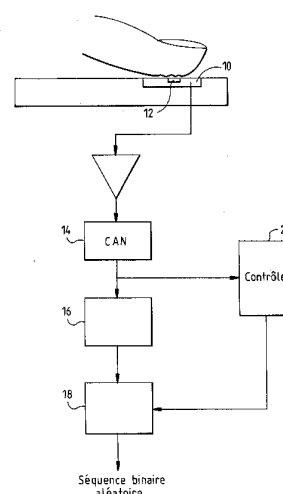
⑦③ Titulaire(s) :

⑦④ Mandataire(s) : THALES "INTELLECTUAL PRO-
PERTY".

⑤④ GENERATEUR DE SEQUENCES BINAIRES ALEATOIRES.

⑤⑦ L'invention concerne la génération de séquences bi-
naires ou nombres aléatoires.

On prévoit que la séquence est produite à partir d'un
capteur d'empreinte digitale (10) et d'un convertisseur ana-
logique-numérique (14). La séquence binaire aléatoire
est produite à partir des bits de poids faible issus du convertis-
seur (lequel a une résolution suffisamment fine pour que le
niveau de bruit du signal issu du capteur fasse basculer
aléatoirement le bit de poids faible. Le capteur comporte
une matrice de détecteurs qui sont de préférence des détec-
teurs pyroélectriques. L'ordre des bits est brouillé par un cir-
cuit de réorganisation et des moyens (18) sont prévus pour
équilibrer la distribution des 0 et des 1 dans la séquence
produite.



GENERA TEUR DE SEQUENCES BINAIRES ALEATOIRES

L'invention concerne la génération de nombres ou séquences binaires aléatoires, dont l'utilité se manifeste principalement pour les applications de cryptographie : beaucoup de logiciels de cryptage nécessitent de générer une clé la plus aléatoire possible.

5 Les générateurs de nombres aléatoires purement algorithmiques sont en fait des générateurs de nombres pseudo-aléatoires ; ces nombres ne sont pas suffisamment aléatoires, comme le montrent des tests qui permettent de mesurer le caractère plus ou moins aléatoire de séquences qui ont toutes les apparences de séquences aléatoires mais qui ne sont pas
10 complètement aléatoires.

Pour mieux rendre aléatoire des séquences binaires, on a déjà proposé de faire intervenir un opérateur humain en lui demandant d'effectuer des mouvements aléatoires enregistrés électroniquement : un exemple de création de nombre aléatoire pour un logiciel de cryptage consiste à
15 demander à l'utilisateur, devant son ordinateur, de faire des mouvements manuels arbitraires avec sa souris ; ces mouvements sont enregistrés et permettent de définir une séquence aléatoire. Mais l'expérience montre que la séquence n'est pas encore suffisamment aléatoire.

Il existe encore des générateurs fondés sur une source physique
20 d'aléas, telle que le bruit thermique. Cette source physique est appliquée à une circuiterie de mise en forme qui la convertit en séquence aléatoire. Ces générateurs ne sont malheureusement pas très bons en termes statistiques, car souvent des corrélations apparaissent, liées à des conditions externes ; par exemple, la fréquence de 50 Hz ou 60 Hz du réseau électrique qui sert à
25 alimenter les appareils se retrouve sous forme résiduelle dans les circuits électroniques et engendre une composante clairement non aléatoire dans la séquence supposée aléatoire.

On peut envisager aussi de combiner un générateur pseudo-aléatoire et une source physique aléatoire, la source physique générant une
30 "graine" momentanée pour démarrer le générateur pseudo-aléatoire qui prend le relais pour générer les bits d'une séquence. Mais il faut alors utiliser

un système relativement complexe pour faire cette combinaison entre la source physique et le générateur pseudo-aléatoire.

La présente invention a pour but de proposer un nouveau type de générateur aléatoire fondé sur une source physique, qui présente en soi un caractère fortement aléatoire et qui ne nécessite pas ou pratiquement pas de
5 générateur pseudo-aléatoire car les séquences de bits générées sont déjà satisfaisantes du point de vue de la plupart des tests statistiques.

Selon l'invention, on propose un générateur de séquence aléatoire comportant comme élément essentiel de génération de séquence aléatoire
10 d'origine physique un capteur d'empreinte digitale à matrice de détecteurs élémentaires, ce capteur comportant un convertisseur analogique-numérique pour convertir en numérique des niveaux de tension détectés par les détecteurs élémentaires, et les bits de poids faible de cette conversion servant à constituer les bits de la séquence pseudo-aléatoire.

15 Le capteur est de préférence un capteur à balayage, dont la matrice est constituée par quelques lignes de nombreux détecteurs, permettant de détecter une empreinte digitale lors du glissement d'un doigt contre la surface du capteur. Un tel capteur est décrit dans le brevet FR-A-2 749 955.

20 Le capteur est de préférence un capteur dont les détecteurs élémentaires sont des éléments pyroélectriques.

L'utilisation d'un capteur d'empreinte digitale comme générateur aléatoire est particulièrement indiquée du fait que les applications visées (notamment les applications de cryptage) sont destinées à fonctionner en
25 environnement sécurisé et qu'un capteur d'empreinte digitale est particulièrement recommandé pour assurer la sécurité. On combine donc avantageusement grâce à un seul capteur la fonction de sécurité par reconnaissance d'empreinte et la fonction de génération de signal aléatoire pour une sécurité de nature différente (sécurité par cryptage notamment).
30 Mieux encore, l'invention peut permettre de crypter l'empreinte digitale elle-même (avant transmission à un système de décryptage et de reconnaissance et authentification), le relevé de l'empreinte elle-même servant à établir la séquence aléatoire servant au cryptage de l'empreinte.

De préférence, l'ordre des bits de poids faible issus du convertisseur analogique-numérique est brouillé pour limiter les corrélations entre détecteurs (ou pixels) voisins ou entre lignes voisines.

5 D'autres caractéristiques et avantages de l'invention apparaîtront à la lecture de la description détaillée qui suit et qui est faite en référence aux dessins annexés dans lesquels la figure unique représente le générateur de séquence aléatoire selon l'invention.

10 Un détecteur élémentaire pyroélectrique est constitué par une couche pyroélectrique (ou piézoélectrique, ce qui revient au même) céramique ou plastique tel que du PVDF (fluorure de polyvinyle) ou céramique, formant une capacité élémentaire connectée à un circuit de lecture qui amplifie le signal. Le signal est ensuite converti en numérique par
15 le convertisseur. Les signaux des différents détecteurs ou pixels d'une ligne sont lus séquentiellement et les signaux des différentes lignes sont également lus séquentiellement.

Lorsque aucun doigt ne touche le capteur, chaque pixel est approximativement en équilibre thermique avec son environnement, tenant
20 compte de la température extérieure et de la consommation de puissance de la puce de circuit intégré qui porte les détecteurs.

Mais les couches pyroélectriques sont extrêmement sensibles aux perturbations extérieures ; un souffle d'air, un bruit, une vibration, viennent facilement modifier le niveau de charges et donc le niveau du signal lu et
25 converti. Le bruit électronique s'y rajoute. Ces perturbations existent en l'absence de signal principal dû à la présence d'un doigt, mais elles se rajoutent au signal principal lorsqu'il existe.

La source de bruit aléatoire sera constituée par le bit de poids faible de la conversion analogique-numérique, en présence ou en l'absence
30 de signal principal. De plus, les différents pixels, nombreux puisqu'il s'agit de lire une empreinte digitale, seront utilisés, les signaux de ces pixels étant largement décorrélés entre eux et ceci d'autant plus lorsqu'ils ne sont pas juxtaposés.

La figure représente le système selon l'invention. Le capteur
35 d'empreinte digitale 10 est vu en coupe ; c'est une puce de silicium

comportant une matrice de capacités pyroélectriques dans une zone 10 sur laquelle on peut poser ou glisser un doigt. La puce comporte ses propres moyens d'adressage de la matrice, de lecture des signaux issus de la matrice, d'amplification, et de conversion analogique-numérique. Ces
5 moyens sont représentés en dehors de la puce pour une plus grande commodité de représentation.

La matrice comporte par exemple huit lignes de 280 pixels chacune et elle est lue périodiquement en une milliseconde. Le signal lu est amplifié et converti en numérique par le convertisseur. Un convertisseur de 4
10 bits de résolution est suffisant pour la prise d'image d'empreinte, mais on peut prévoir un convertisseur de plus grande résolution pour accroître le caractère aléatoire du bit de poids le plus faible.

De manière générale, on s'assure, lors de la conception du système, que le niveau d'amplification du signal lu est suffisant pour que le
15 bruit naturel (thermique, électronique, etc.) soit supérieur au niveau du bit de poids le plus faible afin que celui-ci bascule aléatoirement.

C'est ce bit de poids faible en sortie du convertisseur analogique-numérique 14 qui permet de former une séquence de bits aléatoire.

Toutefois, de préférence, la séquence n'est pas prélevée
20 directement en sortie du convertisseur 14. Elle est plutôt prise en sortie d'un circuit de réorganisation de pixels 16. Le circuit de réorganisation 16 est de préférence aussi situé sur la puce du capteur d'empreinte.

Le circuit de réorganisation 16 prend successivement les bits de poids faible issus du convertisseur 14, qui arrivent dans l'ordre d'adressage
25 de la matrice de détection d'empreinte, c'est-à-dire ligne par ligne et, à l'intérieur d'une ligne, dans l'ordre des colonnes de la matrice. Le circuit de réorganisation 16 brouille l'ordre des bits reçus du convertisseur afin que des bits issus de pixels voisins dans la matrice ne soient pas voisins dans l'ordre de la séquence aléatoire. Ceci évite des corrélations dans la séquence.

30 Le circuit de réorganisation a en tous cas pour rôle d'éliminer la plupart des corrélations connues, corrélation entre pixels voisins ou autres corrélations. Par exemple, le circuit de réorganisation ne devrait pas laisser passer successivement les bits d'une même colonne issus de plusieurs lignes de la matrice. En effet, il y a par principe une corrélation entre les

différentes lignes puisqu'elles doivent voir la même image à des instants différents.

De plus, le circuit de réorganisation est suivi par un circuit ou des moyens logiciels 18 d'ajustement de la distribution moyenne des bits, c'est-à-dire que sur une période moyenne, la séquence doit comporter autant de bits
5 zéro que de bits 1. Ceci est fait par un algorithme relativement simple. Les bits issus de la première réorganisation (résultant du brouillage de l'ordre des pixels) sont lus deux par deux. Lorsque les bits sont tous les deux à 0 ou tous les deux à 1, on les ignore purement et simplement. Lorsqu'ils sont le
10 premier à zéro, le deuxième à 1, on génère un bit 1, lorsque c'est le contraire on génère un bit 0 (ou l'inverse bien sûr).

Ceci permet, au moins en première approximation d'obtenir autant de zéro que de 1 car si la source aléatoire est mal distribuée et produit plus de 0 que de 1 (par exemple) alors la combinaison 00 devrait apparaître
15 statistiquement plus souvent et la combinaison 11 moins souvent. Comme ces deux combinaisons sont éliminées, ne reste que les deux autres qui n'ont pas de raison d'être distribuées anormalement.

Mais pour le cas où la distribution serait quand même anormale, on prévoit de préférence en outre d'alterner périodiquement la conversion ci-dessus ; ainsi, pour une série de couples reçus, 01 ou 10, la conversion
20 transformera 01 en bit 1 et 10 en bit zéro, mais pour la série de couples suivants, la conversion transformera 01 en bit 0 et 10 en bit 1, et ainsi de suite. La conversion peut même être alternée à chaque couple, c'est-à-dire qu'elle est inversée pour chaque bit de la séquence aléatoire produite.

25 La sélection de pixels pour produire un couple de bits successifs est faite par le circuit de réorganisation de manière à éviter les corrélations et on propose avantageusement pour cela d'utiliser pour chaque couple une paire de pixels éloignés ; par exemple le pixel d'une extrémité gauche d'une ligne de la matrice est pris en même temps que le pixel du centre de la ligne,
30 puis on décale d'un pas vers la gauche pour prendre un nouveau couple, deuxième pixel en partant de la gauche avec deuxième pixel en partant du centre, et ainsi de suite.

D'autres possibilités peuvent être prévues, avec pour principe d'éviter une corrélation identifiée comme possible.

Si la séquence aléatoire ne nécessite pas une production rapide, on peut éviter d'utiliser tous les pixels de la ligne et n'utiliser que certains d'entre eux, en changeant le groupe de pixels utilisés à chaque balayage de ligne d'image. Ceci augmente le caractère aléatoire (au détriment de la
5 vitesse puisqu'il faut plus de lignes pour une même longueur de séquence aléatoire).

Afin de protéger le générateur de séquence aléatoire contre tout effet externe parasite, on ajoutera de préférence un circuit ou des moyens logiciels de contrôle 20 qui sont un circuit ou un logiciel d'auto-test périodique
10 qui permettra de vérifier le bon fonctionnement. L'auto-test repose sur la vérification périodique de la distribution des valeurs de signal issues des pixels de l'empreinte. Cela peut être fait par un calcul de la moyenne du signal sur l'image qui ne devrait être ni nulle ni tellement élevée qu'elle résulte probablement d'une saturation du capteur. Egalement on peut faire
15 un calcul d'écart-type entre les valeurs de signal issus des différents pixels : l'écart-type doit avoir une valeur ni trop faible (les pixels n'ont pas de raison de fournir tous le même niveau de signal) ni trop élevée (signifiant que quelque chose d'anormal agit sur le capteur). On peut également contrôler un histogramme de valeurs (contrôle de l'absence de trous ou de
20 discontinuités dans l'histogramme, etc.).

Enfin, on peut vérifier que les valeurs des pixels varient au cours du temps, c'est-à-dire que ce n'est pas toujours le même motif d'image qui est lu par le capteur.

On vérifiera de cette manière qu'il n'y a pas de pixel mort dans
25 l'image, et s'il en existe, on s'assurera qu'ils sont éliminés du processus de fabrication de la séquence aléatoire.

Bien que le capteur d'empreinte digitale préféré selon l'invention soit un capteur à éléments pyroélectriques, on peut envisager à la rigueur que ce soit un capteur capacitif, voire même optique. Dans un cas limite, on
30 pourrait n'utiliser, pour la fabrication d'une séquence pseudo-aléatoire, qu'un seul élément détecteur et non l'ensemble de la matrice, mais cette réalisation est beaucoup moins intéressante.

Le générateur de séquence aléatoire ainsi décrit est particulièrement utilisable dans un système utilisant des moyens de cryptage.
35 Notamment des moyens de cryptage de l'empreinte digitale qui a été

détectée par le capteur d'empreinte. La lecture de l'empreinte sert alors elle-même à établir la séquence pseudo-aléatoire qui permet de crypter la transmission de cette empreinte.

REVENDICATIONS

1. Générateur de séquence binaire aléatoire comportant comme élément essentiel de génération d'une séquence aléatoire d'origine physique un capteur d'empreinte digitale (10) à matrice de détecteurs élémentaires, ce capteur comportant un convertisseur analogique-numérique (14) pour
5 convertir en numérique des niveaux de tension détectés par les éléments pyroélectriques, et les bits de poids faible de cette conversion servant à constituer les bits de la séquence pseudo-aléatoire.

2. Générateur de séquence aléatoire selon la revendication 1,
10 caractérisé en ce que les détecteurs élémentaires sont des éléments pyroélectriques.

3. Générateur de séquence aléatoire selon l'une des revendications 1 et 2, caractérisé en ce que le capteur est un capteur à
15 balayage, dont la matrice est constituée par quelques lignes de nombreux détecteurs, permettant de détecter une empreinte digitale lors du glissement d'un doigt contre la surface du capteur.

4. Générateur selon l'une des revendications 1 à 3, caractérisé en
20 ce qu'il comporte des moyens pour brouiller l'ordre des bits pour renforcer le caractère aléatoire de la séquence.

5. Générateur selon la revendication 4, caractérisé en ce qu'il comporte des moyens pour prélever des couples successifs de bits de poids
25 faible, pour éliminer les couples 00 et les couples 11, et pour convertir un couple 01 en un premier bit et un couple 10 en un bit inverse, pour constituer une séquence mieux distribuée entre 0 et 1.

6. Générateur selon la revendication 5, caractérisé en ce que la
30 conversion est inversée entre deux séries successives de couples 01 et 10,

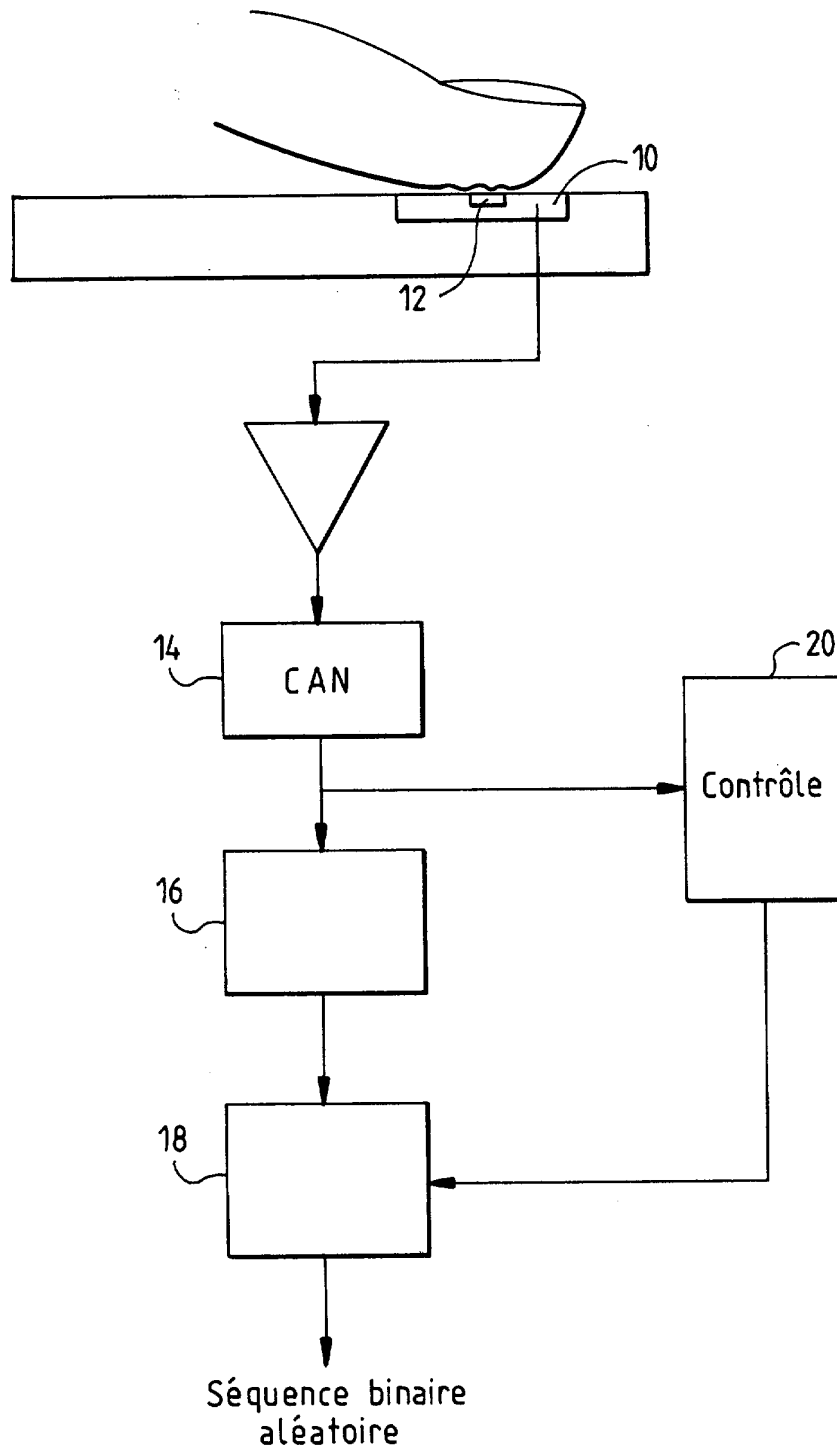
une première conversion faisant correspondre le couple 01 à un bit 0 et une conversion inverse faisant correspondre le couple 01 à 1.

5 7. Générateur selon la revendication 6, caractérisé en ce que la conversion est inversée à chaque nouveau couple de bits.

10 8. Générateur selon l'une des revendications 1 à 7, caractérisé en ce qu'il comporte un moyen de vérification de l'image de l'empreinte, ce moyen comportant notamment un moyen de vérification de la valeur de la moyenne et/ou l'écart-type des valeurs de signal issues des différents détecteurs élémentaires.

15 9. Système utilisant un générateur selon l'une des revendications 1 à 8 et comportant des moyens de cryptage d'une empreinte digitale détectée par le capteur d'empreinte, ces moyens utilisant le générateur de séquence aléatoire.

1/1





RAPPORT DE RECHERCHE PRÉLIMINAIRE

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

N° d'enregistrement
national

FA 641352
FR 0313491

DOCUMENTS CONSIDÉRÉS COMME PERTINENTS		Revendication(s) concernée(s)	Classement attribué à l'invention par l'INPI
Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes		
Y	EP 0 903 665 A (TOKYO SHIBAURA ELECTRIC CO) 24 mars 1999 (1999-03-24) * abrégé * * alinéas [0072] - [0074] * * alinéa [0082] *	1-9	G06F7/58 H04L9/32
Y	US 5 680 460 A (SCHMIDT GREGORY J ET AL) 21 octobre 1997 (1997-10-21) * abrégé * * colonne 2, ligne 40 - ligne 51 * * colonne 3, ligne 34 - ligne 54 * * figure 2 *	1-9	
D,A	EP 0 813 164 A (THOMSON CSF) 17 décembre 1997 (1997-12-17) * abrégé * * figure 5 *	1-3	
A	WO 98/33075 A (SAGE TECHNOLOGY INC) 30 juillet 1998 (1998-07-30) * abrégé * * page 10, ligne 1 - ligne 16 *	4-7	
			DOMAINES TECHNIQUES RECHERCHÉS (Int.CL.7)
			G06F H03K H04L
Date d'achèvement de la recherche		Examineur	
15 juillet 2004		Post, K	
CATÉGORIE DES DOCUMENTS CITÉS X : particulièrement pertinent à lui seul Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie A : arrière-plan technologique 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			

ANNEXE AU RAPPORT DE RECHERCHE PRÉLIMINAIRE**RELATIF A LA DEMANDE DE BREVET FRANÇAIS NO. FR 0313491 FA 641352**

La présente annexe indique les membres de la famille de brevets relatifs aux documents brevets cités dans le rapport de recherche préliminaire visé ci-dessus.

Les dits membres sont contenus au fichier informatique de l'Office européen des brevets à la date du **15-07-2004**

Les renseignements fournis sont donnés à titre indicatif et n'engagent pas la responsabilité de l'Office européen des brevets, ni de l'Administration française

Document brevet cité au rapport de recherche		Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
EP 0903665	A	24-03-1999	JP 2980576 B2	22-11-1999
			JP 11085472 A	30-03-1999
			EP 0903665 A2	24-03-1999
			US 6195669 B1	27-02-2001

US 5680460	A	21-10-1997	US 5541994 A	30-07-1996
			AU 689946 B2	09-04-1998
			AU 3339095 A	27-03-1996
			BR 9509002 A	02-06-1998
			CA 2199034 A1	14-03-1996
			WO 9608093 A1	14-03-1996
			CN 1157677 A	20-08-1997
			EP 0780040 A2	25-06-1997
			JP 10505474 T	26-05-1998
			US 5737420 A	07-04-1998
			US 5832091 A	03-11-1998

EP 0813164	A	17-12-1997	FR 2749955 A1	19-12-1997
			AT 235718 T	15-04-2003
			CA 2206825 A1	14-12-1997
			CN 1172308 A ,B	04-02-1998
			DE 69720109 D1	30-04-2003
			DE 69720109 T2	23-10-2003
			EP 0813164 A1	17-12-1997
			ES 2191816 T3	16-09-2003
			IL 121045 A	10-02-2002
			JP 10091769 A	10-04-1998
			US 6289114 B1	11-09-2001
			US 2001026636 A1	04-10-2001
			ZA 9705193 A	05-01-1998

WO 9833075	A	30-07-1998	AU 6433198 A	18-08-1998
			US 5987483 A	16-11-1999
			WO 9833075 A2	30-07-1998
