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 7 : G06F 17/17	A1	(11) Numéro de publication internationale: **WO 00/39704** (43) Date de publication internationale: 6 juillet 2000 (06.07.00)

(21) Numéro de la demande internationale: PCT/FR99/02783

(22) Date de dépôt international: 12 novembre 1999 (12.11.99)

(30) Données relatives à la priorité:
98/16518 23 décembre 1998 (23.12.98) FR

(71) Déposant *(pour tous les Etats désignés sauf US)*: GEMPLUS S.C.A. [FR/FR]; Avenue du Pic de Bertagne, Parc d'Activités de Gémenos, F–13881 Gémenos Cedex (FR).

(71)(72) Déposant et inventeur: CORON, Jean–Sébastien [FR/FR]; 45, rue d'Ulm, F–75005 Paris (FR).

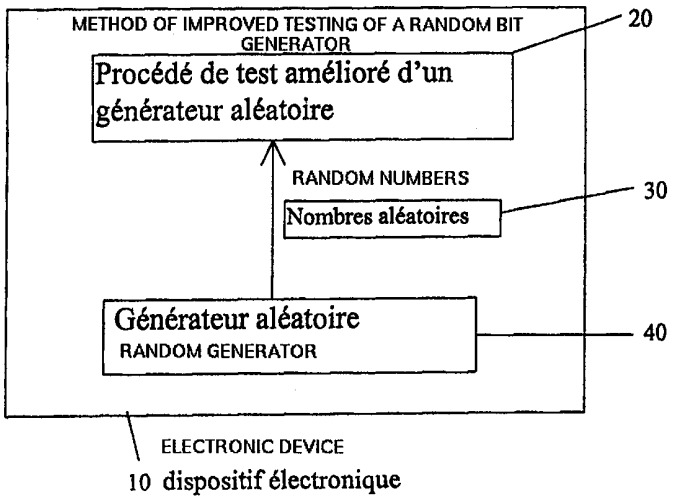
(74) Mandataire: NONNENMACHER, Bernard; Gemplus S.C.A., Avenue du Pic de Bertagne, Parc d'Activités de Gémenos, F–13881 Gémenos Cedex (FR).

(81) Etats désignés: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GE, GH, GM, HU, ID, IL, IN, IS, JP, KE, KG, KP, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZW, brevet ARIPO (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), brevet eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), brevet européen (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), brevet OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Publiée
Avec rapport de recherche internationale.

(54) Title: METHOD FOR IMPROVING A STATISTICAL TEST

(54) Titre: PROCEDE D'AMELIORATION D'UN TEST STATISTIQUE



(57) Abstract

The invention concerns a method for testing sources generating random numbers, in particular sources designed for cryptographic systems such as random number generators incorporated in chip cards. It is particularly designed to be used for testing and validating electronic devices such as chip cards, PCMCIA (Personal Computer Memory Card International Association, 1030 B East Duane Avenue Sunnyvale, California), badges, contactless cards or any other portable apparatus.

(57) **Abrégé**

La présente invention concerne un procédé de test de sources générant des nombres aléatoires, en particulier des sources mises au point dans le cadre de systèmes cryptographiques tels que les générateurs de nombres aléatoires embarqués à bord de cartes à puce. Elle est particulièrement destinée à être mise en oeuvre dans le test et la validation de dispositifs électroniques du type carte à puce, PCMCIA ("Personal Computer Memory Card International Association", 1030 B East Duane Avenue Sunnyvale, California), badges, cartes sans contact ou tout autre appareil portable.

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.

AL	Albanie	**ES**	Espagne	**LS**	Lesotho	**SI**	Slovénie
AM	Arménie	**FI**	Finlande	**LT**	Lituanie	**SK**	Slovaquie
AT	Autriche	**FR**	France	**LU**	Luxembourg	**SN**	Sénégal
AU	Australie	**GA**	Gabon	**LV**	Lettonie	**SZ**	Swaziland
AZ	Azerbaïdjan	**GB**	Royaume-Uni	**MC**	Monaco	**TD**	Tchad
BA	Bosnie-Herzégovine	**GE**	Géorgie	**MD**	République de Moldova	**TG**	Togo
BB	Barbade	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tadjikistan
BE	Belgique	**GN**	Guinée	**MK**	Ex-République yougoslave de Macédoine	**TM**	Turkménistan
BF	Burkina Faso	**GR**	Grèce			**TR**	Turquie
BG	Bulgarie	**HU**	Hongrie	**ML**	Mali	**TT**	Trinité-et-Tobago
BJ	Bénin	**IE**	Irlande	**MN**	Mongolie	**UA**	Ukraine
BR	Brésil	**IL**	Israël	**MR**	Mauritanie	**UG**	Ouganda
BY	Bélarus	**IS**	Islande	**MW**	Malawi	**US**	Etats-Unis d'Amérique
CA	Canada	**IT**	Italie	**MX**	Mexique	**UZ**	Ouzbékistan
CF	République centrafricaine	**JP**	Japon	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Pays-Bas	**YU**	Yougoslavie
CH	Suisse	**KG**	Kirghizistan	**NO**	Norvège	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	République populaire démocratique de Corée	**NZ**	Nouvelle-Zélande		
CM	Cameroun			**PL**	Pologne		
CN	Chine	**KR**	République de Corée	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Roumanie		
CZ	République tchèque	**LC**	Sainte-Lucie	**RU**	Fédération de Russie		
DE	Allemagne	**LI**	Liechtenstein	**SD**	Soudan		
DK	Danemark	**LK**	Sri Lanka	**SE**	Suède		
EE	Estonie	**LR**	Libéria	**SG**	Singapour		

PROCEDE D'AMELIORATION D'UN TEST STATISTIQUE

L'invention concerne une amélioration d'un procédé de test statistique de générateurs de nombres aléatoires appelés aussi sources générant des nombres aléatoires, en particulier des sources mises au point dans le cadre de systèmes cryptographiques tels que les générateurs de nombres aléatoires embarqués à bord de cartes à puce.

Elle est particulièrement destinée à être mise en oeuvre dans le test et la validation de dispositifs électroniques du type carte à puce, PCMCIA ("Personal Computer Memory Card International Association", 1030 B East Duane Avenue Sunnyvale, California) badges, cartes sans contact ou tout autre appareil portable.

La plupart des systèmes de cryptographie à clé publique (dite aussi cryptographie asymétrique) et clé secrète (dite aussi cryptographie symétrique) nécessitent le tirage d'aléas secrets. Il est primordial que de tels aléas, ou nombres, destinés à servir comme clés ultérieurement , soient à priori imprévisibles et ne présentent pas de régularités permettant de les retrouver par des stratégies de recherche exhaustive ou exhaustive améliorée pour laquelle les clés les plus probables sont cherchées en premier lieu.

A ce titre, il existe plusieurs procédés permettant de tester les aléas générés par une source aléatoire et de s'assurer que ladite source fonctionne correctement et ne présente pas de dérive suite à des changements de paramètres externes d'origine malveillante telle qu'une altération par des radiations induites.

Chacun de ces procédés s 'applique à une suite, appelée aussi séquence, de nombres entiers compris entre 0 et une valeur d, ladite suite étant générée par la source aléatoire.

Le procédé de test le plus connu est le test dit de "fréquence". Il s'agit de compter le nombre d'apparitions de chaque entier compris entre 0 et une valeur d dans ladite séquence. Le nombre d'apparitions de chaque entier est ensuite évalué statistiquement.

Un second procédé de test dit de "séries" consiste en un comptage et une évaluation statistique du nombre d'apparitions de tous

les couples possibles d'entiers compris entre 0 et une valeur d. Ce procédé de test peut être généralisé au comptage des triplets, quadruplets d'entiers, etc...

Un troisième procédé de test dit de "trou" existe. Un trou dans une séquence est une suite de nombres à l'extérieur d'un intervalle prédéterminé. Il s'agit d'une évaluation statistique de la longueur desdits trous dans la séquence.

Un quatrième procédé de test, dit test du "poker", existe. Le test consiste à grouper les nombres de la séquence par groupe de cinq nombres et à compter dans chaque quintuplet combien de valeurs différentes apparaissent.

Un cinquième procédé de test dit de "collecte de coupons" consiste à évaluer statistiquement la taille de séquence nécessaire pour que toutes les valeurs entières comprises entre 0 et d apparaissent dans ladite séquence.

Le détail de ces procédés se trouve dans l'ouvrage intitulé: " Knuth, The art of computer programming, vol. 2, Seminumerical algorithms ".

Un autre procédé de test populaire est le test universel de Maurer décrit dans l'ouvrage " Journal of Cryptology, vol. 5, n° 2, 1992, pp. 89-105 ". Ce test présente l'avantage de révéler tous les défauts décelables par les procédés de tests précédemment cités ainsi que d'autres défauts statistiques non détectés par ces mêmes procédés de test.

Le procédé de test, dit de Maurer, également dénommé universel, comprend les étapes suivantes:

Première étape: Génération d'une séquence de (Q+K)*L bits par la source aléatoire. Q, K et L sont des paramètres d'entrée. Les bits de la séquence sont groupés par bloc de L bits, formant une séquence d'entiers compris entre 0 et 2^L-1 de longueur Q+K. La longueur est mémorisée dans le tableau block[n], où n est compris entre 1 et Q+K.

Deuxième étape: Calcul du paramètre du test, noté fTU; cette deuxième étape comprenant les étapes suivantes, appelées sous-étapes 2.1 à 2.5 , Sum étant une variable utilisée à partir de l'étape 2.3:

2.1 Création et initialisation d'un tableau tab [i] de taille 2^L;

2.2 Pour n variant de 1 à Q, faire le calcul: tab[block[n]]=n;

2.3 Initialiser le nombre Sum à 0;

2.4 Pour n variant de Q+1 à Q+K, exécuter le calcul :

Ajouter log(n-tab[block[n]] à Sum;

Faire le calcul: tab[block[n]]=n;

2.5 Le paramètre fTU du test est donné par:

fTU=(Sum/K)/Log(2);

Troisième étape: Calcul de la variance par block de paramètre du test, notée Var. Son expression précise est donnée dans l'article publié par Maurer dans l'ouvrage " Journal of Cryptology, vol. 5, n° 2, 1992, pp. 89-105 ", qui est :

$$Var = (1-z)^* \sum_{i=1}^{\infty} \log2(i)^2 * z^{i-1} - ((1-z)^* \sum_{i=1}^{\infty} \log2(i) * z^{i-1})^2 ,$$

avec $\log2(z)=\log(z)/\log(2)$ et $z=1-2^{-L}$

Quatrième étape: Calcul de la fonction c(L,K). Une expression approchée de cette fonction est donnée dans l'article de l'ouvrage précédent, qui est:

$c(L,K)=0,7-0,8/L+(1,6+12,8/L)*K^{(-4/L)}$;

Cinquième étape: Calcul de l'écart type du paramètre de test, noté σ: $\sigma=c(L,K)*\sqrt{(Var/K)}$;

Sixième étape: Calcul du paramètre y; y est déterminé à partir du taux de rejet du test fixé en entrée, noté ρ. y doit vérifier l'équation:

$N(-y)= \rho$.

N est la fonction de densité normale décrite dans l'ouvrage " R. Langley, Practical statistics, Dover publications, New-York, 1968 ". L'équation $N(-y)= \rho$ peut être résolue en utilisant une table de valeurs de N. Une telle table est fournie dans l'article précédent;

Septième étape: Calcul de la valeur moyenne du test, notée E[fTU]. Son expression est donnée dans l'article publié par Maurer dans l'ouvrage " Journal of Cryptology, vol. 5, n°2, 1992, pp. 89-105 ", et vaut :

$$E[fTU] = (1-z)^* \sum_{i=1}^{\infty} \log2(i) * z^{i-1}$$

avec log2(z)=log(z)/log(2) et $z=1-2^{-L}$

Huitième étape: Calcul des bornes t1 et t2. Elles sont données par l'équation: $t1=E[fTU]-y*\sigma$ et $t2=E[fTU]+y*\sigma$;

Neuvième étape: Résultat du test:

Si le paramètre du test fTU est compris entre t1 et t2, alors le générateur de nombre aléatoire est accepté. Dans le cas contraire, il est refusé.

L'intérêt de ce procédé de test universel est que le paramètre du test fTU est relié de façon asymptotique à l'entropie de la source aléatoire testée. L'entropie d'une source aléatoire mesure la qualité cryptographique de cette source. Il est possible d'établir la relation asymptotique suivante entre le paramètre du test fTU et l'entropie par blocks de taille L de la source notée K(L) , qui est:

E[fTU] – K(L) converge vers C quand L tend vers l'infini,

où C est une constante calculable.

La présente invention a pour objet un procédé de test amélioré permettant d'atteindre une meilleure précision dans l'estimation de l'entropie.

Soit fTM la fonction de test améliorée décrite dans la suite de ce document, il est possible d'établir que :

E[fTM]=K(L)

Contrairement au test de Maurer original pour lequel il existe seulement une relation asymptotique entre la fonction du test fTU et l'entropie de la source K(L), l'avantage du procédé de test amélioré est que la fonction du test amélioré fTM est exactement égale à l'entropie de la source K(L). En conséquence, tout défaut statistique induisant une variation de l'entropie de la source sera détecté de manière plus fiable par le procédé de test amélioré. Ce test amélioré sert notamment à évaluer la sécurité de dispositifs portables du type carte à puce

Le procédé de test amélioré comprend les étapes suivantes:

Première étape: Elle consiste en une génération d'une séquence de (Q+K)*L bits par la source aléatoire, Q, K et L étant des paramètres d'entrée; les bits de la séquence sont groupés par bloc de L bits, formant une séquence d'entiers compris entre 0 et 2^L-1 de longueur Q+K; la longueur est mémorisée dans le tableau block[n], où n est compris entre 1 et Q+K.

Deuxième étape: elle consiste en un calcul du paramètre du test amélioré, noté fTM qui comprend les étapes suivantes, appelées sous-étapes 2.1 à 2.5 :

2.1 Création et initialisation d'un tableau tab [i] de taille 2^L;

2.2 Pour n variant de 1 à Q, calcul de : tab[block[n]]=n;

2.3 Initialisation du nombre Sum à 0;

2.4 Pour n variant de Q+1 à Q+K, exécution du calcul suivant:

Calcul de j=n-tab[block[n]] .

Si j est inférieur ou égal à 23 alors exécuter le calcul :

Pour k variant de 1 à j-1

Ajouter 1/(k*Log(2)) à Sum

Sinon, pour j supérieur à 23, exécuter le calcul

Ajouter log(j-1)/log(2)+0.8327462+1/(2*(j-1))/log(2) à Sum,

Exécution du calcul: tab[block[n]]=n;

2.5 Le paramètre fTM du test est donné par:

fTM=Sum/K

Troisième étape: elle consiste en un calcul de la variance par block de paramètre du test, notée Var; son expression précise est donnée par l'expression suivante :

$$Var = (1-z)^* \sum_{i=1}^{\infty} g(i)^2 * z^{i-1} - L^2$$

avec $z=1-2^{-L}$ et g(i) une fonction définie de la manière suivante :

$$g(i)= \sum_{k=1} 1/k$$

Quatrième étape: elle consiste en un calcul de la fonction c(L,K); une expression approchée de cette fonction est donnée par la formule :

$$c(L,K)=0,7-0,8/L+(1,6+12,8/L)*K^{(-4/L)};$$

Cinquième étape: elle consiste en un calcul de l'écart type du paramètre de test, noté σ: $\sigma=c(L,K)*\sqrt{(Var/K)}$;

Sixième étape: elle consiste en un calcul du paramètre y; y est déterminé à partir du taux de rejet du test fixé en entrée, noté ρ. y doit vérifier l'équation:

$N(-y)= \rho$.

N est la fonction de densité normale décrite dans l'ouvrage " R. Langley, Practical statistics, Dover publications, New-York, 1968 " qui est:

$$N(-y)=\int_{-\infty}^{y} 1/\sqrt{(2*\pi)}*\exp(-x^2/2)\, dx$$

L'équation $N(-y)= \rho$ peut être résolue en utilisant une table de valeurs de N. Une telle table est fournie dans l'article précédent;

Septième étape: elle consiste en un calcul des bornes t1 et t2. Elles sont données par l'équation: $t1=L-y*\sigma$ et $t2=L+y*\sigma$;

Huitième étape: elle consiste à donner le résultat du test:

Si le paramètre du test fTM est compris entre t1 et t2, alors le générateur de nombre aléatoire est accepté; dans le cas contraire, il est refusé.

Par conséquent, le procédé de l'invention consiste en un calcul modifié de la fonction du test de Maurer fTM. L'intérêt de ce calcul modifié est qu'il permet d'avoir une estimation beaucoup plus précise de l'entropie K(L) de la source, puisque la valeur moyenne de la fonction de test modifiée E[fTM] est égale à K(L). Grâce à cette estimation plus précise de l'entropie de la source, le procédé de l'invention permet une détection plus fiable des éventuels défauts statistiques de la source aléatoire testée.

La présente invention concerne également, comme cela a été dit au début de la description un dispositif électronique représenté à la figure unique jointe à la présente description.

Ce dispositif électronique 10 est un dispositif d'auto-vérification d'intégrité physique d'un circuit intégré s'auto-vérifiant et contrôlant l'intégrité de son générateur aléatoire 40 produisant des nombres aléatoires 30 à partir du procédé de test amélioré 20 décrit précédemment, ceci afin de s'assurer que ledit générateur 40 fonctionne correctement en général et ne présente pas de dérive suite à des changements de paramètres externes d'origine malveillante telle qu'une altération par des radiations induites en particulier.

De manière préférentielle, le dispositif électronique effectuant le test est un dispositif portable, plus particulièrement il consiste, par exemple, en une carte à puce, une carte sans contact, une carte PCMCIA ("Personal Computer Memory Card International Association", 1030 B East Duane Avenue Sunnyvale, California), un badge, une montre "intelligente".

Enfin, le dispositif électronique de l'invention peut être un dispositif extérieur constitué d'une machine ou installation destinée à tester le bon fonctionnement de générateurs aléatoires embarqués à bord desdits dispositifs portables. Ce dispositif extérieur permet un échange d'informations avec le dispositif portable de manière à vérifier que le générateur aléatoire fonctionne correctement. Le dispositif extérieur inter-agit avec le dispositif portable pour vérifier l'intégrité de son générateur aléatoire.

REVENDICATIONS

1. Procédé de test de sources de nombres aléatoires embarqué à bord d'un système cryptographique, du type carte à puce, comprenant les étapes suivantes:

Première étape: Génération d'une séquence de (Q+K)*L bits par la source aléatoire, Q, K et L étant des paramètres d'entrée; les bits de la séquence étant groupés par bloc de L bits, formant une séquence d'entiers compris entre 0 et 2^L-1 de longueur Q+K; la longueur étant mémorisée dans le tableau block[n], où n est compris entre 1 et Q+K,

ledit procédé de test de source étant caractérisé en ce que les étapes deux à huit sont les suivantes:

Deuxième étape: Calcul du paramètre du test amélioré, noté fTM; cette deuxième étape comprenant les étapes suivantes, appelées sous-étapes 2.1 à 2.5 , Sum étant une variable utilisée à partir de l'étape 2.3,

2.1 Création et initialisation d'un tableau tab [i] de taille 2^L;

2.2 Pour n variant de 1 à Q, calcul de tab[block[n]]=n;

2.3 Initialisation du nombre Sum à 0;

2.4 Pour n variant de Q+1 à Q+K, exécution du calcul :

Calculer j=n-tab[block[n]] .

Si j est inférieur ou égal à 23 alors exécution du calcul :

Pour k allant de 1 à i-1

Ajouter 1/(k*Log(2)) à Sum

Sinon, pour j supérieur à 23, exécution du calcul

Ajouter log(j-1)/log(2)+0.8327462+1/(2*(j-1))/log(2) à Sum

Faire le calcul: tab[block[n]]=n;

2.5 Le paramètre fTM du test est donné par:

fTM=Sum/K

Troisième étape: Calcul de la variance par block de paramètre du test, notée Var; son expression précise étant donnée par l'expression suivante :

$$Var = (1-z)^* \sum_{i=1}^{\infty} g(i)^2 * z^{i-1} - L\hat{}2$$

avec $z=1-2^{-L}$ et g(i) qui est une fonction définie de la manière suivante :

$$g(i)=\sum_{k=1}^{i-1} 1/k$$

Quatrième étape: Calcul de la fonction c(L,K); son expression approchée étant donnée par la formule :

$$c(L,K)=0,7-0,8/L+(1,6+12,8/L)*K^{(-4/L)};$$

Cinquième étape: Calcul de l'écart type du paramètre de test, noté σ, donné par la formule

$$\sigma=c(L,K)*\sqrt{(Var/K)};$$

Sixième étape: Calcul du paramètre y; y état déterminé à partir du taux de rejet du test fixé en entrée, noté ρ; y devant vérifier l'équation:

$N(-y)=\rho$;

N étant la fonction de densité normale sous la forme:

$$N(-y)=\int_{-\infty}^{y} 1/\sqrt{(2*\pi)}*\exp(-x^2/2)\,dx$$

Septième étape: Calcul des bornes t1 et t2 qui sont données par l'équation: $t1=L-y*\sigma$ et $t2=L+y*\sigma$;

Huitième étape: Résultat du test:

Si le paramètre du test fTM est compris entre t1 et t2, alors le générateur de nombre aléatoire est accepté et dans le cas contraire, il est refusé.

2. Dispositif électronique d'auto-vérification d'intégrité physique d'un circuit intégré s'auto-vérifiant et contrôlant l'intégrité de son générateur aléatoire, afin de s'assurer que ce dernier fonctionne correctement en général et ne présente pas de dérive suite à des changements de paramètres externes d'origine malveillante telle qu'une altération par des radiations induites en particulier, caractérisé en ce que ledit dispositif met

en oeuvre le procédé de test amélioré selon la revendication 1.

3. Dispositif électronique selon la revendication 2 caractérisé en ce que le dispositif effectuant le test est un dispositif portable.

4. Dispositif électronique selon la revendication 3 caractérisé en ce que le dispositif est une carte à puce.

5. Dispositif électronique selon la revendication 3 caractérisé en ce que le dispositif est une carte sans contact.

6. Dispositif électronique selon la revendication 3 caractérisé en ce que le dispositif est une carte PCMCIA ("Personal Computer Memory Card International Association", 1030 B East Duane Avenue Sunnyvale, California).

7. Dispositif électronique selon la revendication 3 caractérisé en ce que le dispositif est un badge.

8. Dispositif électronique selon la revendication 3 caractérisé en ce que le dispositif est une montre.

9. Dispositif électronique selon la revendication 1 caractérisé en ce qu'un dispositif extérieur effectuant le test est constitué d'une machine ou installation destinée à tester le bon fonctionnement de générateurs aléatoires embarqués à bord desdits dispositifs portables.

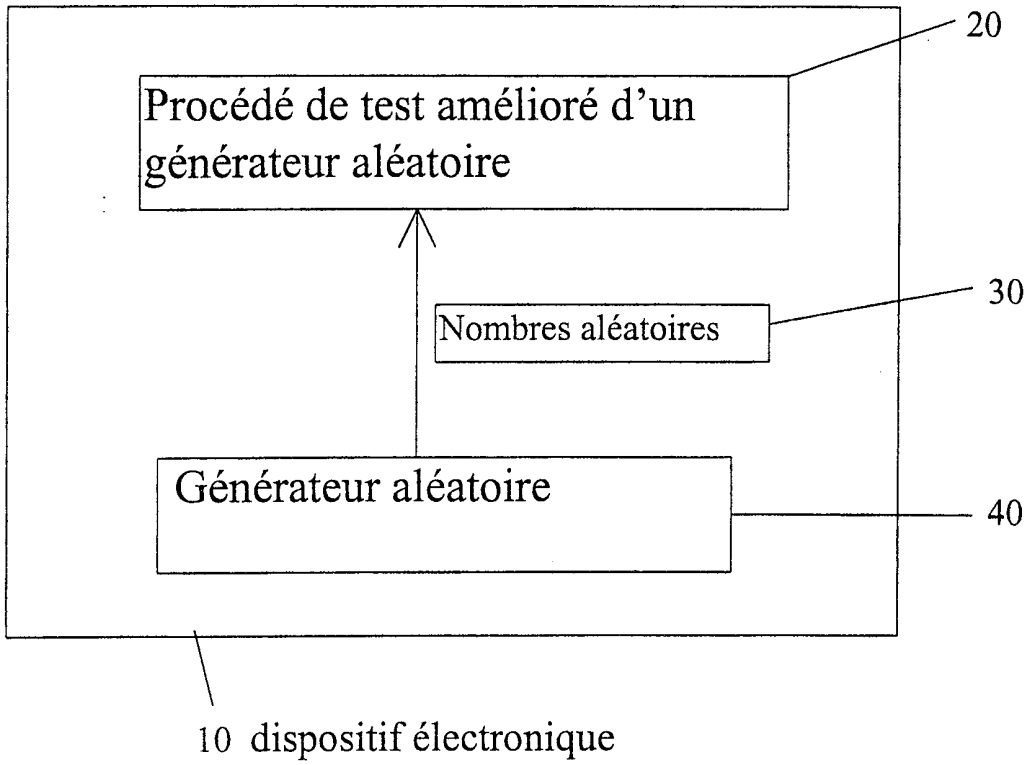


Figure unique

INTERNATIONAL SEARCH REPORT

Internati . Application No
PCT/FR 99/02783

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G06F17/17

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 7 G06F

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 indication, where appropriate, of the relevant passages	Relevant to claim No.
A	CORON JS, NACCACHE D: "AN ACCURATE EVALUATION OF MAURER'S UNIVERSAL TEST" GEMPLUS' CORPORATE PRODUCT R&D DIVISION - TECHNICAL REPORT IT01-1998,1998, pages 1-13, XP002101030 http://www.gemplus.fr/smart/r_d/publications/download/it01.pdf the whole document ---	1-9
A	MAURER U M: "A universal statistical test for random bit generators" JOURNAL OF CRYPTOLOGY, 1992, USA, vol. 5, no. 2, pages 89-105, XP002101031 ISSN 0933-2790 cited in the application the whole document ---	1-9

-/--

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

[ ] 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
11 January 2000	17/01/2000

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	Pierfederici, A

1

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

INTERNATIONAL SEARCH REPORT

Internat. .l Application No
PCT/FR 99/02783

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
A	SADEGHIYAN B ET AL: "A new universal test for bit strings" INFORMATION SECURITY AND PRIVACY. FIRST AUSTRALASIAN CONFERENCE, ACISP'96. PROCEEDINGS, INFORMATION SECURITY AND PRIVACY. FIRST AUSTRALASIAN CONFERENCE, ACISP'96. PROCEEDINGS, WOLLONGONG, NSW, AUSTRALIA, 24-26 JUNE 1996, pages 311-319, XP002101032 ISBN 3-540-61991-7, 1996, Berlin, Germany, Springer-Verlag, Germany ---	
A	DALLE MOLLE J W ET AL: "Higher-order cumulant spectral-based statistical tests of pseudo-random variate generators" 1992 WINTER SIMULATION CONFERENCE PROCEEDINGS (CAT. NO.92CH3202-9), ARLINGTON, VA, USA, 13-16 DEC. 1992, pages 618-625, XP002101033 ISBN 0-7803-0798-4, 1992, New York, NY, USA, IEEE, USA -----	

1

RAPPORT DE RECHERCHE INTERNATIONALE

Demand. ternationale No
PCT/FR 99/02783

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
CIB 7 G06F17/17

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 7 G06F

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 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
A	CORON JS, NACCACHE D: "AN ACCURATE EVALUATION OF MAURER'S UNIVERSAL TEST" GEMPLUS' CORPORATE PRODUCT R&D DIVISION - TECHNICAL REPORT IT01-1998,1998, pages 1-13, XP002101030 http://www.gemplus.fr/smart/r_d/publications/download/it01.pdf le document en entier ---	1-9
A	MAURER U M: "A universal statistical test for random bit generators" JOURNAL OF CRYPTOLOGY, 1992, USA, vol. 5, no. 2, pages 89-105, XP002101031 ISSN 0933-2790 cité dans la demande le document en entier ---	1-9

-/--

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

[ ] 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'appartenenant 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'inven tion revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément

"Y" document particulièrement pertinent; l'inven tion 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
11 janvier 2000	17/01/2000

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	Pierfederici, A

1

Formulaire PCT/ISA/210 (deuxième feuille) (juillet 1992)

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale No
PCT/FR 99/02783

C.(suite) DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie °	Identification des documents cités, avec,le cas échéant, l'indicationdes passages pertinents	no. des revendications visées
A	SADEGHIYAN B ET AL: "A new universal test for bit strings" INFORMATION SECURITY AND PRIVACY. FIRST AUSTRALASIAN CONFERENCE, ACISP'96. PROCEEDINGS, INFORMATION SECURITY AND PRIVACY. FIRST AUSTRALASIAN CONFERENCE, ACISP'96. PROCEEDINGS, WOLLONGONG, NSW, AUSTRALIA, 24-26 JUNE 1996, pages 311-319, XP002101032 ISBN 3-540-61991-7, 1996, Berlin, Germany, Springer-Verlag, Germany	
A	DALLE MOLLE J W ET AL: "Higher-order cumulant spectral-based statistical tests of pseudo-random variate generators" 1992 WINTER SIMULATION CONFERENCE PROCEEDINGS (CAT. NO.92CH3202-9), ARLINGTON, VA, USA, 13-16 DEC. 1992, pages 618-625, XP002101033 ISBN 0-7803-0798-4, 1992, New York, NY, USA, IEEE, USA	

1