

(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION
EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété
Intellectuelle
Bureau international



(43) Date de la publication internationale
27 novembre 2008 (27.11.2008)

PCT

(10) Numéro de publication internationale
WO 2008/141962 A1

(51) Classification internationale des brevets :
G06F 7/58 (2006.01) **H04L 9/06** (2006.01)

(21) Numéro de la demande internationale :
PCT/EP2008/055792

(22) Date de dépôt international : 12 mai 2008 (12.05.2008)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
07 03384 11 mai 2007 (11.05.2007) FR

(71) Déposant (pour tous les États désignés sauf US)
: **THALES** [FR/FR]; 45, rue de Villiers, F-92200
Neuilly-sur-seine (FR).

(72) Inventeurs; et

(75) Inventeurs/Déposants (pour US seulement) :
LEFRANC, David [FR/FR]; 10, rue Robert Capa,
F-95240 Corneilles-en-parisis (FR). **PAINCHAUT,**
Philippe [FR/FR]; 2, rue de la Concorde, Asnieres, 92600.

(74) Mandataire : **DUDOUIT, Isabelle**; MARKS & CLERK
France, 31-33, avenue Aristide Briand, F-94117 Arcueil
Cedex, (FR).

(81) États désignés (sauf indication contraire, pour tout titre de
protection nationale disponible) : AE, AG, AL, AM, AO,
AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH,
CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG,
ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL,
IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK,
LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW,
MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL,
PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SV, SY,
TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA,
ZM, ZW.

(84) États désignés (sauf indication contraire, pour tout titre
de protection régionale disponible) : ARIPO (BW, GH,
GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM,
ZW), eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM),
européen (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI,

[Suite sur la page suivante]

(54) Title: METHOD OF GENERATING PSEUDO-RANDOM BIT STRINGS

(54) Titre : PROCEDE DE GENERATION DE CHAINES DE BITS PSEUDO-ALEATOIRES

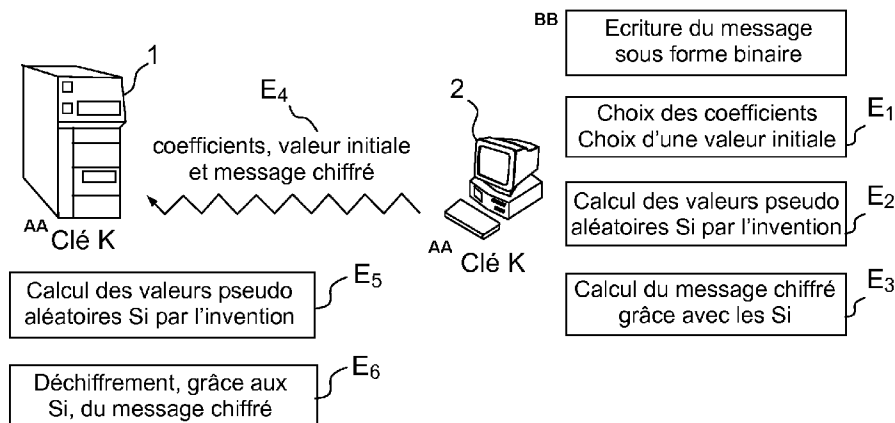


FIG.1

AA ... Key K
BB ... Writing of the message in binary form
E1 ... Choice of an initial value
E2, E5 ... Calculation of the pseudo-random values Si by the invention
E3 ... Calculation of the encrypted message using the Si
E4 ... Coefficients, initial value and encrypted message
E6 ... Decryption, using Si, of the encrypted message

(57) Abstract: Method for generating pseudo-random bit strings in a system in which the data interchanges between a first user and a second user are protected, characterized in that it comprises at least the following steps: using an application f_k of output size n bits, determining a value x and, from this value x and by applying the application f_k , generating t values v_i , from the t values v_i and, from $u \cdot t$ coefficients, determining u blocks S_i containing pseudo-random characters. Applicable to the coding or authentication domain.

[Suite sur la page suivante]

WO 2008/141962 A1



FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MT, NL,
NO, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG,
CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Publiée :

— avec rapport de recherche internationale

(57) Abrégé : Procédé pour générer des chaînes de bits pseudo-aléatoires dans un système dans lequel les échanges de données entre un premier utilisateur et un deuxième utilisateur sont protégés caractérisé en ce qu'il comporte au moins les étapes suivantes : utiliser une application f_K de taille de sortie n bits, déterminer une valeur x et à partir de cette valeur x et en appliquant l'application f_K , générer t valeurs v_i , à partir des t valeurs v_i et de $u \cdot t$ coefficients déterminer u blocs S_i contenant des caractères pseudo-aléatoires. Application au domaine du codage ou de l'authentification

PROCÉDE DE GENERATION DE CHAINES DE BITS PSEUDO-ALEATOIRES

L'objet de l'invention concerne un procédé pour générer des caractères
5 pseudo-aléatoires ou des chaînes de bits pseudo-aléatoires. Il est par
exemple utilisé pour la protection de la confidentialité de données.

L'invention s'applique, par exemple dans le domaine de la cryptographie. En
particulier, elle se rapporte aux procédés cryptographiques de protection de
la confidentialité des échanges de données entre deux applications. Elle est
10 utilisée dans tous les systèmes de codage/décodage de données qui
nécessitent de protéger les échanges de données. Elle peut être utilisée
dans le domaine de l'authentification d'utilisateurs ou de données.

A l'heure actuelle, la propriété de confidentialité peut être obtenue selon
15 différents procédés, s'inspirant tous d'un même principe. En considérant un
canal de communication supposé non sécurisé entre deux applications
notées A et B, et en supposant que A souhaite envoyer des données
confidentielles à une application B via ce canal de communication, pour ce
faire, l'application A doit « masquer » les données, puis les transmettre à
20 l'application B. Afin que l'application soit en mesure de récupérer les
données d'origine à partir des données masquées, il faut que l'application A
ait utilisé un « procédé de masquage » qui soit facilement inversible pour B
et ceci uniquement pour B, et éventuellement pour A, afin qu'aucune autre
personne ne puisse prendre connaissance des données. Pour obtenir une
25 telle technique de masquage, la cryptographie distingue deux approches
différentes : la cryptographie à clé publique, appelée aussi cryptographie
asymétrique, et la cryptographie à clé secrète, appelée aussi cryptographie
symétrique. Dans chacune de ces méthodes, les données sont représentées
sous forme d'une chaîne de caractères, les caractères généralement utilisés
30 étant des caractères 0, 1 alors appelés bits.

La cryptographie à clé publique repose sur le fait que l'application B dispose d'une paire de clé notée (P, S) telle que :

- P est une valeur connue de tout le monde et est appelée clé publique,
 - S est une valeur connue uniquement par l'application B et est appelée
- 5 clé privée,

Les valeurs de P et S sont reliées par une relation mathématique telle qu'il est difficile de retrouver S à partir de la simple connaissance de P. Ainsi, seule l'application B est à même de connaître la valeur S.

En cryptographie à clé publique, l'application A utilise la clé publique P de
10 l'application B pour coder les données. Dans ce contexte, il est nécessaire de disposer de la clé privée pour pouvoir décoder les données. Ainsi, seule l'application B est à même de connaître la valeur S.

La cryptographie à clé secrète repose, quant à elle, sur le fait que
15 l'application A et l'application B disposent d'une même valeur S connue d'elles seules. La valeur S est appelée clé secrète. Ainsi, l'application A utilise la valeur S pour coder les données de sorte que la connaissance de S soit nécessaire pour décoder les données codées. L'application B est alors la seule, avec l'application A, à pouvoir déchiffrer, ce qui garantit bien la confidentialité des données.

20 La protection de la confidentialité dans le contexte de la cryptographie à clé secrète (cryptographie symétrique) est généralement appelée méthode de *chiffrement symétrique*. Il existe deux catégories de méthodes de chiffrement. La première est appelée *chiffrement à flot* et la seconde est appelée *chiffrement par bloc*. En chiffrement à flot, les différents caractères
25 représentant la donnée sont codés successivement un à un. En chiffrement par bloc, la chaîne de caractères représentant la donnée est découpée sous forme de plusieurs blocs consécutifs de caractères et ces blocs, tous de même taille, sont ensuite codés successivement. A chaque codage d'un bloc, plusieurs caractères sont donc codés simultanément.

30 Il existe de nombreuses méthodes de chiffrement par bloc. Toutes ces solutions reposent sur l'utilisation d'une *primitive cryptographique*. Une

primitive cryptographique f est une application prenant en entrée une chaîne notée m de n caractères et une chaîne notée K de k caractères. En sortie, la primitive f fournit une chaîne de N caractères notée C vérifiant $C = f(m, K)$, avec N non nécessairement égal à n .

- 5 Chaque choix d'une entrée K définit une application f_K telle que $f_K(m) = f(m, K)$. L'entrée K est appelée *clé secrète*.

La présente invention se rapporte, notamment, au cas où la primitive cryptographique f définit, pour chaque valeur K possible, une fonction bijective f_K (en particulier $n=N$). L'application f_K ainsi obtenue est également
10 appelée permutation (terme préférentiellement utilisé dans la présente description). Ainsi, chaque clé secrète K définit une permutation f_K . En pratique, la primitive f pourra être l'AES ou le DES.

Pour coder un bloc m contenant n caractères, il suffit d'utiliser une fois la fonction f_K . Par exemple, on pourra envisager que le codé, noté C , du bloc m
15 soit calculé par $C = f_K(m)$. En pratique, la donnée confidentielle ne contiendra pas un unique bloc, mais au contraire s'écrira comme la suite de b blocs notés $m_1, \dots, m_b$. Il devient important de savoir comment coder ces b blocs. En s'inspirant du calcul $C = f_K(m)$, il est possible d'envisager que les différents blocs m_i , $1 \leq i \leq b$, soient codés en des blocs notés C_i , $1 \leq i \leq b$, vérifiant $C_i =$
20 $f_K(m_i)$.

Spécifier comment coder plusieurs blocs d'un même message consiste à définir un *mode opératoire*. Celui défini ci-dessus et consistant à coder chaque bloc indépendamment les uns des autres en les passant comme entrée de la permutation f_K est le mode ECB. La sécurité de ce mode n'est
25 pas très élevée. Le problème de ce mode est qu'un bloc m_i , quelle que soit sa position dans le message sera toujours codé par la même valeur C_i . Cela pose un réel problème en pratique.

Il existe un grand nombre de modes opératoires, certains étant standardisés par le NIST [NIS01]. Différents critères existent pour juger de la qualité de
30 ces modes. Les deux principaux sont le niveau de *sécurité* de ce mode et le *coût calculatoire* engendré par ce mode.

La sécurité d'un mode opératoire représente le fait qu'il soit difficile de décider si une chaîne de caractères donnée est le résultat du codage d'une donnée via ce mode opératoire, ou si au contraire cette chaîne de caractères est une chaîne de caractères pris au hasard. Si une telle distinction est difficile, alors il est raisonnable de penser que ce mode opératoire est relativement sûr. Toutefois, cette sécurité ne peut être garantie que lorsque le nombre de blocs codés par le mode opératoire choisi reste inférieur à une constante (dépendante du mode). Cette constante s'exprime généralement sous la forme 2^{na} avec n la taille du bloc et a une valeur comprise entre $\frac{1}{2}$ et 1. La valeur a sera généralement appelée *seuil de sécurité*. Le coût calculatoire représente le nombre d'appels à la primitive cryptographique pour coder un message de b blocs. Le coût calculatoire idéal est b appels à la permutation f_K (c'est le cas du mode ECB).

La sécurité du mode est en partie associée à la valeur a . Bien évidemment, plus la valeur a est grande, plus la valeur 2^{na} est grande et plus longtemps le mode reste sûr. Dans le tableau suivant, un rappel est donné pour la sécurité des modes standardisés par le NIST. Il est également précisé si le modèle de sécurité associé est élevé (ce qui est préférable) ou au contraire faible (ce qui est plutôt pénalisant). Les arguments formels de sécurité peuvent être trouvés dans [BDJR97] et [SLLLY01].

Mode opératoire	Constante associée à la sécurité	Référence pour la sécurité
ECB [NIST01]	$\frac{1}{2}$ (modèle de sécurité faible)	[BDJR97]
CFB [NIST01]	$\frac{1}{2}$ (modèle de sécurité élevé)	[SLLLY01]
OFB [NIST01]	$\frac{1}{2}$ (modèle de sécurité élevé)	[SLLLY01]
CBC [NIST01]	$\frac{1}{2}$ (modèle de sécurité élevé)	[BDJR97]
CTR [NIST01]	$\frac{1}{2}$ (modèle de sécurité élevé)	[BDJR97]

Les solutions existantes (et standardisées) ont une sécurité ne dépassant pas le seuil $\frac{1}{2}$.

L'art antérieur divulgue trois propositions permettant d'aller éventuellement au-delà du seuil de sécurité $\frac{1}{2}$. Les deux premières [KNU00] et [ABAG01] ont
5 été fournies avec une preuve de sécurité quasiment inexistante pour la première et dans un modèle faible pour la seconde de sorte qu'il n'est pas possible de savoir si ces modes ont effectivement une constante supérieure à $\frac{1}{2}$. La troisième solution [IWA06] parvient quant à elle à atteindre le seuil
10 de sécurité $\frac{2}{3}$ avec une preuve de sécurité complète et dans un modèle de sécurité élevé. Cette dernière proposition dispose également d'un coût calculatoire proche du coût calculatoire idéal (quasiment similaire au coût du mode ECB).

La présente invention concerne un procédé de génération de chaînes de
15 caractères pseudo-aléatoires à partir d'une application, par exemple une permutation f_K , d'une valeur initiale x et de coefficients α_i . La présente invention peut en particulier être utilisée pour le chiffrement par bloc.

L'objet de l'invention concerne un procédé pour générer des chaînes de bits
20 dans un système dans lequel les échanges de données entre un premier utilisateur et un deuxième utilisateur sont protégés caractérisé en ce qu'il comporte au moins les étapes suivantes :

- utiliser une application f_K de taille de sortie n bits,
- déterminer une valeur x et à partir de cette valeur x et en appliquant
25 plusieurs fois l'application f_K , afin de générer t valeurs v_i ,
- à partir des t valeurs v_i et de $u \cdot t$ coefficients déterminer u blocs S_i contenant des caractères pseudo-aléatoires.

Selon un mode de réalisation, l'objet de l'invention concerne un procédé pour
générer des chaînes de bits pseudo-aléatoires, au sein d'un système
30 comprenant un module de codage de données, telles qu'un message de $b = f \cdot u \cdot n + q$ bits, où f et u sont supérieurs ou égaux à 0, et q est compris entre 0

et $u*n$, peut se mettre sous la forme de f groupes de u blocs de n bits et d'un $(f+1)$ ième groupe de q bits caractérisé en ce que :

le codage d'un groupe considéré de u blocs comporte au moins les étapes suivantes :

- 5
 - pour le groupe considéré choisir une valeur initiale x ,
 - à partir des t valeurs v_i générées et de $u*t$ coefficients déterminer u blocs S_i contenant des caractères pseudo-aléatoires afin de coder les u blocs du groupe considéré,
 - combiner les u blocs du groupe considéré avec les u blocs S_i afin
- 10 d'obtenir le groupe codé,
- réitérer ces trois étapes pour les f groupes,
- pour le $(f+1)$ ième groupe de q bits,
- choisir une valeur initiale de x ,
- à partir des t valeurs v_i générées et de $u*t$ coefficients déterminer un
- 15 nombre de blocs S_i égal au moins à la partie entière supérieure de q/n ,
- combiner q bits extraits des blocs S_i déterminés avec les q bits du $(f+1)$ ième groupe.

- 20 L'invention est, par exemple, utilisée dans des applications d'authentification. Un des avantages de la présente invention est qu'elle permet de construire de nouvelles fonctions pseudo-aléatoires qui ont une sortie de taille supérieure à n . Généralement, les constructions existantes ont une sortie uniquement de n bits tout en utilisant plusieurs fois la permutation f_K . Ces
- 25 constructions ont donc un rendement très faible (au mieux, elles manipulent deux fois l'algorithme bloc pour sortir n bits, le rendement étant alors de $1/2$, ce qui en pratique n'est pas acceptable). La présente invention utilise plusieurs fois la permutation f_K , mais pour générer u blocs de n bits. De plus, le rendement obtenu est quasiment égal à 1.

D'autres caractéristiques et avantages apparaîtront à la lecture de la description détaillée donnée à titre d'exemple et non limitative qui suit faite en regard des figures qui représentent

- La figure 1, un exemple d'échanges de données de manière sécurisée entre un serveur bancaire et un utilisateur,
- La figure 2, un exemple d'utilisation du procédé selon l'invention dans un système d'authentification.

L'un des buts de l'invention est de créer de nouvelles fonctions pseudo-aléatoires, en utilisant, notamment, des permutations dont la sortie est un bloc de n bits; la sortie de la nouvelle fonction étant de taille égale à un multiple de n bits, notée $u*n$ bits, u étant un nombre entier.

Le principe de l'invention consiste, notamment, à considérer t appels à l'algorithme bloc générant en sortie un bloc de n bits afin d'obtenir t chaînes de n bits qui seront alors organisées de manière adéquate selon des coefficients fournis en paramètre pour obtenir les $u \leq t$ blocs de n bits en sortie de la fonction.

Afin de mieux faire comprendre l'objet de la présente invention, l'exemple donné est relatif à la mise en œuvre du procédé pour un cas où les coefficients utilisés pour organiser les t chaînes de n bits sont les coefficients d'une matrice génératrice d'un code linéaire. Les codes linéaires ont une distance associée notée d . Cette distance se concrétise dans les coefficients de la matrice génératrice associée. Ainsi, ces coefficients permettent d'organiser les t chaînes de sorte que les $u \leq t$ blocs de n bits de la sortie de la fonction soient alors suffisamment différents (« distants ») les uns des autres. Ainsi, même en tentant des combinaisons de ces u blocs de sortie, il reste difficile de mettre à mal le caractère pseudo-aléatoire de la sortie (de u blocs de n bits) de la nouvelle fonction. Fort logiquement, plus la distance du code est grande, plus cette mise à mal est difficile et plus la fonction ainsi créée est fortement pseudo-aléatoire. Le niveau de sécurité obtenu par la mise en œuvre du procédé est égale à $d/d+1$.

Comme il a été précédemment annoncé, de telles fonctions peuvent être également utilisées pour définir de nouveaux modes opératoires, tels que leur sécurité soit identique à la sécurité de la fonction sous-jacente utilisée. Ainsi, en utilisant les fonctions pseudo-aléatoires paramétrées par des matrices de codes linéaires obtenues par la présente invention, il est possible d'obtenir des modes opératoires avec un niveau de sécurité égal à $d/d+1$, où d est la distance du code linéaire utilisé. En particulier, en utilisant des codes linéaires de distance supérieure ou égale à 3, il est alors possible d'obtenir des modes opératoires ayant une sécurité très élevée, non décrite dans l'art antérieur.

Selon un exemple de mise en œuvre, le procédé selon l'invention concerne un procédé de génération de chaînes de caractères pseudo-aléatoires à partir d'une permutation f_K , d'une valeur initiale x et de coefficients α_i . La présente invention peut en particulier être utilisée pour coder un message découpé en bloc.

Dans un tel contexte, deux considérations sont possibles.

- Si l'on souhaite coder u blocs d'un message, il est alors suffisant de disposer (en plus de la valeur initiale et de la permutation) de $u*t$ coefficients α_i pour une valeur $t \geq 1$ quelconque.
- Si l'on dispose de la donnée de $u*t$, $t \geq 1$ coefficients α_i (en plus de la valeur initiale et de la permutation), il est alors possible de coder u blocs.

La valeur de t étant variable, le produit des coefficients $u*t$ est variable et peut varier selon la valeur de t .

Les $u*t$ coefficients sont répartis en u séquences de t valeurs. Pour plus de clarté, cette répartition peut être représentée sous la forme d'une matrice contenant u lignes et t colonnes comme décrite ci-dessous. La représentation sous forme matricielle est utilisée à titre illustratif, afin d'améliorer la compréhension de l'exemple donné pour illustrer le procédé,

mais n'est en aucun cas indispensable pour le bon fonctionnement de l'invention.

	$\alpha_{1,1}$	$\alpha_{1,2}$	$\alpha_{1,3}$	...	$\alpha_{1,t}$
5	$\alpha_{2,1}$	$\alpha_{2,2}$	$\alpha_{2,3}$	...	$\alpha_{2,t}$
	.				
	.				
	.				
	$\alpha_{u-1,1}$	$\alpha_{u-1,2}$	$\alpha_{u-1,3}$	...	$\alpha_{u-1,t}$
10	$\alpha_{u,1}$	$\alpha_{u,2}$	$\alpha_{u,3}$	...	$\alpha_{u,t}$

Selon l'invention, la donnée initiale x peut être une valeur stockée dans l'application, ou une valeur issue d'un processus aléatoire ou pseudo-aléatoire ou déterministe.

- 15 A partir de cette valeur x , il est possible de générer t valeurs, représentées à titre d'exemple dans la présente description sous la forme d'une suite v contenant t valeurs notées v_i , $1 \leq i \leq t$. Un exemple pour v est :

$$v = (v_1 = f_K(x+1), v_2 = f_K(x+2), v_3 = f_K(x+3), \dots, v_{t-1} = f_K(x+t-1), v_t = f_K(x+t))$$

- Selon l'invention, l'application choisira, selon ses ressources, de calculer tout
20 ou partie des t valeurs notées v_i , $1 \leq i \leq t$ et de les stocker; ou au contraire de calculer la valeur v_i lorsque cette valeur est nécessaire.

- Le procédé selon l'invention accepte plus généralement l'utilisation de t valeurs obtenues par un calcul de la forme $g_i(f_K, x)$, $1 \leq i \leq t$, où les applications g_i sont des applications quelconques (LFSR, transformation affine, transformation linéaire, registre diviseur, addition modulaire...). Ainsi,
25 l'exemple précédent correspond à $g_i(f_K, x) = f_K(x+i)$.

D'autres exemples sont choisis parmi la liste non exhaustive suivante :

- $g_i(f_K, x) = f_K(x + i - 1)$,
- 30 • $g_i(f_K, x) = f_K(L^i(x))$ où L^i correspond à la $i^{\text{ème}}$ itération d'un LFSR ou d'un registre diviseur,

- $g_i(f_K, x) = f_K(a_i x + b_i)$ où a_i et b_i sont des coefficients d'une transformation affine,
- $g_i(f_K, x) = f_K(a_i x + b_i \bmod 2^n)$ où a_i et b_i sont des coefficients d'une transformation affine,
- 5 • $g_i(f_K, x) = f_K(x + i) \oplus d_i$, où $\oplus$ représente l'opération de xor bit à bit et d_i est une chaîne de bits,
- $g_i(f_K, x) = f_K(x + i - 1) \oplus d_i$, où $\oplus$ représente l'opération de xor bit à bit et d_i est une chaîne de bits,
- 10 • $g_i(f_K, x) = f_K(L^i(x)) \oplus d_i$, où L^i correspond à la $i^{\text{ème}}$ itération d'un LFSR ou d'un registre diviseur, $\oplus$ représente l'opération de xor bit à bit et d_i est une chaîne de bits.

A partir des t valeurs notées v_i , $1 \leq i \leq t$ et des $u \cdot t$ coefficients

$$\begin{array}{cccccc}
 & \alpha_{1,1} & \alpha_{1,2} & \alpha_{1,3} & \dots & \alpha_{1,t} \\
 15 & \alpha_{2,1} & \alpha_{2,2} & \alpha_{2,3} & \dots & \alpha_{2,t} \\
 & . & & & & \\
 & \alpha_{u-1,1} & \alpha_{u-1,2} & \alpha_{u-1,3} & \dots & \alpha_{u-1,t} \\
 & \alpha_{u,1} & \alpha_{u,2} & \alpha_{u,3} & \dots & \alpha_{u,t}
 \end{array}$$

- le procédé détermine u blocs S_i contenant des caractères pseudo-aléatoires.
- 20 Le codage de u blocs notés $m_1, m_2, \dots, m_u$ en u blocs codés notés $C_1, C_2, \dots, C_u$ sera alors facilement obtenu à partir des u blocs S_i . Plus précisément, pour tout i , $1 \leq i \leq u$, coder les différents blocs m_i revient à calculer

$$\begin{aligned}
 S_i &= (\alpha_{i,1} \otimes v_1) \oplus (\alpha_{i,2} \otimes v_2) \oplus (\alpha_{i,3} \otimes v_3) \oplus \dots \oplus (\alpha_{i,t} \otimes v_t) \\
 C_i &= m_i \oplus S_i
 \end{aligned}$$

- 25 Où $\otimes$ peut représenter :

- La multiplication si elle est définie. En particulier,
 - Dans le cas $\alpha_{i,j} = 1$, $\alpha_{i,j} \otimes v_j = v_j$
 - Dans le cas $\alpha_{i,j} = 0$, $\alpha_{i,j} \otimes v_j = 0$ (chaîne de n bits tous égaux à 0). Cela revient au même d'ignorer le terme $\alpha_{i,j} \otimes v_j$

- La sélection d'une proportion de bits. En particulier, si $0 \leq \alpha_{i,j} \leq 1$, $a_{i,j} \otimes v_j$ représente la sélection de $a_{i,j}$ % des n bits, selon un critère de sélection connu de l'application.

Et où $\oplus$ peut représenter :

- 5
 - l'opération xor égale au « ou exclusif » bit à bit.
 - L'addition modulaire modulo 2^n

La définition des opérandes peut varier au sein du calcul d'un bloc S_i .

10 Selon l'invention, pour coder $f \cdot u$ blocs, il suffit d'itérer le processus décrit précédemment f fois. Chaque itération nécessite les paramètres suivants :

- la donnée d'une valeur initiale x ,
- la donnée de $u \cdot t$ coefficients,
- la donnée de la permutation f_K ou d'une application choisie.

15 Selon l'invention, si l'application y voit un intérêt, elle pourra coder b blocs d'un message, b quelconque, en considérant $b = u_1 + u_2 + \dots + u_s$ et coder les u_1 blocs selon le procédé décrit dans la présente description, puis les u_2 blocs avec une nouvelle itération du procédé et ainsi de suite, les différentes valeurs $u_1, u_2, \dots, u_s$ pouvant être différentes les unes des autres, ou
 20 certaines égales, ou encore toutes égales. A chaque itération du procédé de génération de chaînes pseudo-aléatoires, l'application pourra choisir de conserver tout ou partie des paramètres de précédentes itérations ou au contraire d'utiliser des paramètres tous différents.

Premier exemple de mise en œuvre de l'invention

25 Supposons la donnée d'une valeur initiale x , d'une permutation f_K et de la suite de coefficients présentée sous la forme de la matrice $u^* u$ ($t = u$).

$$\begin{array}{ccccccc} 1 & 0 & 0 & \dots & 0 & 0 & 0 \\ 0 & 1 & 0 & \dots & 0 & 0 & 0 \\ 0 & 0 & 1 & \dots & 0 & 0 & 0 \\ & & & \dots & & & \\ 0 & 0 & 0 & \dots & 1 & 0 & 0 \end{array}$$

0 0 0 0 1 0

0 0 0 0 0 1

En considérant la donnée de t valeurs v_i obtenues par $v_i = f_K(x + i - 1)$, pour tout i , $1 \leq i \leq t=u$, l'opérande $\oplus$ sera à tout moment de l'itération le ou exclusif bit à bit et l'opérande $\otimes$ sera la multiplication par 0 ou 1 (les valeurs des coefficients) comme défini précédemment.

Soit un message de b bits, b égal à $f^*u^*n + q$ bits avec f et u supérieurs ou égaux à 0, et q supérieur ou égal à 0 et strictement inférieur à u^*n , devant être codé. La suite de coefficients et la permutation f_K seront, par exemple, constantes à chaque itération, et la valeur initiale sera x pour la première itération, puis $x+t$ pour la seconde, puis $x+2t$ pour la troisième et plus généralement $x+(i-1)^*t$ pour la $i^{\text{ème}}$ itération. Les u premiers blocs de n bits, ceux du premier groupe, seront codés grâce à la première itération (avec x comme valeur initiale) de la présente invention. Pour tout i , $1 \leq i \leq u$, le codage du bloc i noté m_i s'obtient alors par l'application de la formule

$$S_i = (\alpha_{i,1} \otimes v_1) \oplus (\alpha_{i,2} \otimes v_2) \oplus (\alpha_{i,3} \otimes v_3) \oplus \dots \oplus (\alpha_{i,t} \otimes v_t)$$

$$C_i = m_i \oplus S_i$$

Or, tous les coefficients de la ligne i de la matrice sont nuls, sauf le $i^{\text{ème}}$, (matrice identité). Par conséquent, S_i se réduit à

$$S_i = \alpha_{i,i} \otimes v_i = v_i = f_K(x + i - 1)$$

de sorte que

$$C_i = m_i \oplus S_i = m_i \oplus f_K(x + i - 1).$$

Lors de la seconde itération de l'invention, pour le codage du second groupe de u blocs de n bits, les u blocs m_{u+i} suivants, $1 \leq i \leq u$, seront codés en calculant

$$S_i = \alpha_{i,i} \otimes v_i = v_i = f_K(x + u + i - 1)$$

de sorte que

$$C_{u+i} = m_{u+i} \oplus S_i = m_i \oplus f_K(x + u + i - 1).$$

Les deux itérations peuvent s'exprimer sous la forme commune suivante.

Pour tout i , $1 \leq i \leq 2u$,

$$S_i = f_K(x + i - 1)$$

$$C_i = m_i \oplus S_i$$

Au final, après f différentes itérations, le processus de codage des u^*f premiers blocs du message se résume sous la forme pour $1 \leq i \leq u^*f$,

5 $S_i = f_K(x + i - 1)$ coefficient à utiliser pour coder le bloc d'indice i

$C_i = m_i \oplus S_i$ valeur du bloc d'indice i codé.

Les derniers q bits, notés sous la forme d'un unique bloc m'_{u^*f+1} seront codés en générant suffisamment de blocs S_i pour pouvoir en extraire q bits, afin de former le bloc S'_{u^*f+1} . Le $(f+1)$ ième groupe est codé en un groupe $C'_{u^*f+1} =$

10 $m'_{u^*f+1} \oplus S'_{u^*f+1}$.

Second exemple d'application

En supposant la donnée d'une valeur initiale x , d'une permutation f_K et de la suite de coefficients présentée sous la forme de la matrice $u^*(u+1)$ ($t = u+1$).

	1 1 0 0 0 0 0
15	1 0 1 0 0 0 0
	1 0 0 1 0 0 0
	
	1 0 0 0 1 0 0
	1 0 0 0 0 1 0
20	1 0 0 0 0 0 1

En considérant la donnée de valeurs v_i obtenues par $v_i = f_K(x + i - 1)$, pour tout i , $1 \leq i \leq t = u + 1$. L'opérande $\oplus$ sera à tout moment de l'itération le ou exclusif bit à bit et l'opérande $\otimes$ sera la multiplication par 0 ou 1 (les valeurs des coefficients) comme définie précédemment.

25 Soit un message $b = f^*u^*n + q$ bits, avec f et u supérieurs ou égaux à 0, et q supérieur ou égal à 0 et strictement inférieur à u^*n , devant être codé. La suite de coefficients et la permutation f_K seront constantes à chaque itération, et la valeur initiale sera x pour la première itération, puis $x+u+1$ pour la seconde, puis $x+2(u+1)$ pour la troisième et plus généralement $x + (i - 1)^*(u+1)$ pour la

30 $i^{\text{ème}}$ itération. Les u premiers blocs seront codés grâce à la première itération

(avec x comme valeur initiale) de la présente invention. Pour tout i , $1 \leq i \leq u$, le codage du bloc i noté m_i s'obtient alors par l'application de la formule

$$S_i = (\alpha_{i,1} \otimes v_1) \oplus (\alpha_{i,2} \otimes v_2) \oplus (\alpha_{i,3} \otimes v_3) \oplus \dots \oplus (\alpha_{i,t} \otimes v_t)$$

$$C_i = m_i \oplus S_i$$

- 5 Or, tous les coefficients de la ligne i sont nuls, sauf le 1^{er} et le $(i+1)$ ^{ème}. Par conséquent, cette formule se réduit à

$$S_i = (\alpha_{i,1} \otimes v_1) \oplus (\alpha_{i,i+1} \otimes v_{i+1}) = v_1 \oplus v_{i+1} = f_K(x) \oplus f_K(x+i-1)$$

de sorte que

$$C_i = m_i \oplus f_K(x) \oplus f_K(x+i-1)$$

- 10 Lors de la seconde itération de l'invention, les u blocs m_{u+i} pour tout i , $1 \leq i \leq u$, sont codés par

$$C_{u+i} = m_{u+i} \oplus f_K(x+u-1) \oplus f_K(x+u+1+i-1)$$

Et ainsi de suite pour les f premiers groupes.

- 15 Les derniers q bits, notés sous la forme d'un unique bloc m'_{u*f+1} seront codés en générant suffisamment de blocs S_i pour pouvoir en extraire q bits, afin de former le bloc S'_{u*f+1} . Le $(f+1)$ ^{ème} groupe est codé en un groupe $C'_{u*f+1} = m'_{u*f+1} \oplus S'_{u*f+1}$.

Obtention de nouveaux modes opératoires

- 20 Dans les deux précédents exemples d'application de l'invention permettant d'illustrer le fait que l'invention rend certaines solutions existantes comme des cas particuliers, les coefficients fournis sous forme matricielle ne correspondent pas à des valeurs quelconques.

- Concernant le mode compteur, premier exemple, la matrice de coefficient
25 fournie correspond à la matrice identité, qui peut être considérée comme la matrice génératrice du code linéaire identité auquel est associée une distance $d=1$.

- Dans le second exemple, la matrice ayant uniquement des 1 sur la première
30 colonne correspond à la matrice génératrice du code linéaire de parité auquel est associé la distance $d=2$.

A tout code correcteur est associée une *dimension* qui correspond à la taille d'origine des mots (selon les notations de l'exemple u), une *taille* qui correspond à la taille des mots du code (selon les notations de l'exemple t) et une distance notée d .

- 5 La présente invention est tout particulièrement intéressante lorsque les coefficients fournis correspondent aux coefficients d'une matrice génératrice d'un code linéaire de dimension u , de taille t et de distance d . Une telle matrice aura alors u lignes et t colonnes.

Ainsi, l'utilisation d'une matrice génératrice de taille $u \times t$ comme donnée de
10 coefficients, d'une valeur initiale x et d'une permutation f_K permet, en une itération de coder u blocs. Chaque itération conserve les mêmes coefficients et la même permutation. Seule la donnée initiale change. Ainsi, lors de la $i^{\text{ème}}$ itération $2 \leq i$, la donnée initiale vaut $x + (i - 1) \cdot t$.

En utilisant de cette sorte la présente invention, il est alors possible de
15 prouver la sécurité du mode opératoire ainsi obtenu dans un modèle de sécurité élevé, et en particulier, la distance d du code est directement impliquée dans l'analyse de sécurité. Ainsi, il est possible de montrer que ce mode opératoire, consistant en l'itération du procédé décrit précédemment, reste sûr tant que le nombre de blocs chiffrés reste inférieur à $2^{nd/d+1}$. Ainsi,
20 en considérant la matrice génératrice d'un code linéaire de distance 3, la sécurité du mode opératoire décrit ci-dessus est alors garantie tant que le nombre de blocs codés reste inférieur à $2^{3n/4}$, nombre qu'aucune autre solution de codage connue de l'art antérieur ne peut espérer.

- 25 Pour un code linéaire de distance 4, la sécurité pourra être garantie dans que le nombre de blocs codés est inférieur à $2^{4n/5}$, ce qui est supérieur à $2^{3n/4}$.

En résumé, et de façon générale, il est possible d'utiliser la présente invention pour générer des chaînes de bits pseudo-aléatoires, non nécessairement dédiées à la problématique du codage de message.

Exemple de mise en œuvre du procédé selon l'invention au sein d'un système permettant à un utilisateur d'effectuer des transactions avec un serveur bancaire.

- 5 Considérons une connexion entre un serveur de banque 1 et un client 2. Ces deux entités ont pour objectif de dialoguer ensemble de façon confidentielle (demande de virement, par exemple...).

Supposons que le serveur et le client disposent tous deux d'une même clé secrète K de 128 bits. La présente invention permet de réaliser cette communication confidentielle.

En effet, considérons que le client souhaite transmettre à la banque un ordre de virement et supposons que cet ordre soit représenté par un message électronique M de taille $8 \times 128 = 1024$ bits. Un tel message peut donc s'écrire sous la forme

$$15 \quad M = m_1 m_2 m_3 m_4 m_5 m_6 m_7 m_8$$

Où chaque m_i représente un bloc de 128 bits.

Pour transmettre son ordre de façon confidentielle, le client va utiliser le procédé selon l'invention décrit ci-dessus. Pour cela, le serveur et le client conviennent alors publiquement (i.e. de façon non secrète) :

- 20 • d'un algorithme de codage par bloc utilisant des clés de 128 bits, disons l'AES. Nous noterons $AES(K, t)$ le codage du mot de 128 bits t en utilisant la clé secrète K .
- d'une suite de valeurs binaires pouvant être représentée sous la forme d'une matrice G ayant 4 lignes et 5 colonnes définie par

$$25 \quad G = \begin{matrix} & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 \end{matrix}$$

Dans la suite, l'opérande $\oplus$ représente l'opération de « ou exclusif » bit à bit.

- 30 Cette opérande vérifie

$$A \oplus A = 0; A \oplus B = B \oplus A; (A \oplus B) \oplus B = A \oplus (B \oplus B) = A \oplus 0 = A$$

Le client 2 choisit (étape E₁) ensuite une première valeur initiale x de taille 128 bits et applique une première fois la présente invention en utilisant G pour calculer (étape E₂) 4 (le nombre de lignes de G) blocs S_i de 128 bits

5 définis par

$$S_1 = \text{AES}(K, x) \oplus \text{AES}(K, x+4)$$

$$S_2 = \text{AES}(K, x+1) \oplus \text{AES}(K, x+4)$$

$$S_3 = \text{AES}(K, x+2) \oplus \text{AES}(K, x+4)$$

$$S_4 = \text{AES}(K, x+3) \oplus \text{AES}(K, x+4)$$

10 A partir de ces quatre blocs S_i , le client peut coder (étape E₃) les 4 premiers blocs du message M en 4 blocs codés c_i définis par

$$c_1 = m_1 \oplus S_1; c_2 = m_2 \oplus S_2; c_3 = m_3 \oplus S_3; c_4 = m_4 \oplus S_4$$

Ensuite, le client peut considérer une seconde valeur initiale x' . Le client peut
15 une nouvelle fois appliquer la présente invention avec la valeur initiale x' et la matrice G représentant la suite de coefficients. Le client obtient alors 4 nouveaux blocs S_i de 128 bits définis par

$$S_5 = \text{AES}(K, x') \oplus \text{AES}(K, x'+4)$$

$$S_6 = \text{AES}(K, x'+1) \oplus \text{AES}(K, x'+4)$$

20 $S_7 = \text{AES}(K, x'+2) \oplus \text{AES}(K, x'+4)$

$$S_8 = \text{AES}(K, x'+3) \oplus \text{AES}(K, x'+4)$$

Le client peut alors coder les 4 derniers blocs du message M en utilisant ces 4 nouveaux blocs S_i . En effet, le client calcule alors

$$c_5 = m_5 \oplus S_5; c_6 = m_6 \oplus S_6; c_7 = m_7 \oplus S_7; c_8 = m_8 \oplus S_8$$

25

Ainsi, en appliquant deux fois la présente invention, le client a été capable de coder le message M en un message codé C défini par

$$C = c_1 c_2 c_3 c_4 c_5 c_6 c_7 c_8$$

A partir de C , il est impossible de retrouver la valeur de M sans la connaissance de la clé secrète K partagée uniquement par le serveur et le client.

Le client envoie (étape E_4) alors au serveur le message C ainsi que le couple
 5 (x, x') de données initiales.

Lors de la réception du couple (x, x') , le serveur peut, en appliquant également deux fois la présente invention recalculer (étape E_5) les valeurs

$$\begin{aligned} S_1 &= \text{AES}(K, x) \oplus \text{AES}(K, x+4) \\ 10 \quad S_2 &= \text{AES}(K, x+1) \oplus \text{AES}(K, x+4) \\ S_3 &= \text{AES}(K, x+2) \oplus \text{AES}(K, x+4) \\ S_4 &= \text{AES}(K, x+3) \oplus \text{AES}(K, x+4) \end{aligned}$$

et

$$\begin{aligned} S_5 &= \text{AES}(K, x') \oplus \text{AES}(K, x'+4) \\ 15 \quad S_6 &= \text{AES}(K, x'+1) \oplus \text{AES}(K, x'+4) \\ S_7 &= \text{AES}(K, x'+2) \oplus \text{AES}(K, x'+4) \\ S_8 &= \text{AES}(K, x'+3) \oplus \text{AES}(K, x'+4) \end{aligned}$$

et ensuite calculer

$$\begin{aligned} c_1 \oplus S_1 &= (m_1 \oplus S_1) \oplus S_1 = m_1 \oplus (S_1 \oplus S_1) = m_1 \oplus 0 = m_1 \\ 20 \quad c_2 \oplus S_2 &= (m_2 \oplus S_2) \oplus S_2 = m_2 \oplus (S_2 \oplus S_2) = m_2 \oplus 0 = m_2 \\ c_3 \oplus S_3 &= (m_3 \oplus S_3) \oplus S_3 = m_3 \oplus (S_3 \oplus S_3) = m_3 \oplus 0 = m_3 \\ c_4 \oplus S_4 &= (m_4 \oplus S_4) \oplus S_4 = m_4 \oplus (S_4 \oplus S_4) = m_4 \oplus 0 = m_4 \\ c_5 \oplus S_5 &= (m_5 \oplus S_5) \oplus S_5 = m_5 \oplus (S_5 \oplus S_5) = m_5 \oplus 0 = m_5 \\ c_6 \oplus S_6 &= (m_6 \oplus S_6) \oplus S_6 = m_6 \oplus (S_6 \oplus S_6) = m_6 \oplus 0 = m_6 \\ 25 \quad c_7 \oplus S_7 &= (m_7 \oplus S_7) \oplus S_7 = m_7 \oplus (S_7 \oplus S_7) = m_7 \oplus 0 = m_7 \\ c_8 \oplus S_8 &= (m_8 \oplus S_8) \oplus S_8 = m_8 \oplus (S_8 \oplus S_8) = m_8 \oplus 0 = m_8 \end{aligned}$$

Le serveur a ainsi pu recalculer (étape E_6) le message décodé

$M = m_1 m_2 m_3 m_4 m_5 m_6 m_7 m_8$ grâce à sa connaissance de K . Le serveur
 30 connaît alors l'ordre de virement qu'il peut maintenant exécuter.

Exemple d'utilisation du procédé utilisé dans un dispositif d'authentification

Considérons un distributeur 3 de contenus numériques payants, disposant de différents clients. Pour qu'un client du distributeur puisse avoir accès à un contenu, il doit d'abord prouver au distributeur qu'il a le droit d'obtenir ce contenu.

Pour ce faire, le distributeur fournit au client un terminal 4 et une carte à puce 5 dans laquelle se trouve :

- Une zone mémoire en lecture seule, 5_1 contenant
 - Une clé secrète K connue uniquement par le distributeur (qui aura par exemple fabriqué la carte lui-même) et propre à la carte. Par exemple, nous considérons qu'il s'agit d'une clé de taille 128 bits utilisable pour l'AES. Nous noterons $AES(K, t)$ le chiffrement du mot de 128 bits t en utilisant la clé secrète K .
 - $u \cdot t$ coefficients binaires (pouvant être identique pour chaque carte). Par exemple $u=4$ et $t=5$. On pourra supposer que ces coefficients sont représentés dans la ROM 5_1 sous la forme d'une matrice G de taille $4 \cdot 5$ définie par

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 \end{pmatrix}$$

- une zone de logique câblée ou un processeur 5_2 capable de réaliser les calculs associés à l'invention, en particulier, capable de mettre en œuvre des calculs AES pour cet exemple.
 - Une interface 5_3 de communication pour pouvoir échanger des données.
- Pour authentifier le client, le distributeur peut envoyer au client une valeur initiale x (étape E_{10}). La carte à puce, à la réception de x , va alors mettre en

œuvre les étapes du procédé selon l'invention, en prenant comme paramètre la clé K et la matrice G stockées en ROM et la valeur initiale x envoyée par le distributeur. La carte à puce calcule (étape E_{11}) les 4 blocs de 128 bits définis par

5

$$S_1 = \text{AES}(K, x) \oplus \text{AES}(K, x+4)$$

$$S_2 = \text{AES}(K, x+1) \oplus \text{AES}(K, x+4)$$

$$S_3 = \text{AES}(K, x+2) \oplus \text{AES}(K, x+4)$$

$$S_4 = \text{AES}(K, x+3) \oplus \text{AES}(K, x+4)$$

10

La carte à puce renvoie alors les 4 blocs S_i , (pouvant être considérés comme un unique bloc de 512 bits) étape E_{12} . A la réception de ces 4 blocs, le distributeur calcule également, selon l'invention et avec les paramètres K , G et x , 4 blocs de 128 bits (étape E_{13}). Si ces 4 blocs sont identiques aux
15 quatre reçus, alors le client est authentifié auprès du distributeur et peut logiquement obtenir le contenu auquel il a légitimement accès (étapes E_{14} et E_{15}).

Sans sortir du cadre de l'invention, le procédé peut aussi être utilisé pour authentifier des données échangées dans un système.

20

Bibliographie :

[ABAG01] 2D-Encryption Mode, A. A. Belal and M. A. Abdel-Gawad, SPIE, volume 4793, 2003, 64-75.

25

[BDJR97] A Concrete Security Treatment of Symmetric Encryption, M Bellare, A. Desai, E. Jorjani et P. Rogaway, FOCS 1997, 394-403.

30

[IWA06] New Blockcipher Modes of Operation with Beyond the Birthday Bound Security, T. Iwata, Fast Secure Encryption 2006, 331-348.

[KNU00] Block Chaining Modes of Operation, L. R. Knudsen, NIST call for new modes of operation, 2000.

5 [NIST01] Recommendation for Block Cipher Modes of Operation, Methodes and Techniques. M Dworkin, NIST Special Publication 800-38A, 2001.

10 [SLLLY01] Concrete Security Analysis of CTR-OFB and CTR-CFB Modes of Operation. J. Sung, S. Lee, J. Lim, W. Lee et O. Yi. 4th International Conference of Information Security and rypology 2001, 103-113.

REVENDICATIONS

- 1 – Procédé pour générer des chaînes de bits pseudo-aléatoires dans un système dans lequel les échanges de données entre un premier utilisateur et un deuxième utilisateur sont protégés caractérisé en ce qu'il comporte au moins les étapes suivantes :
- utiliser une application f_K de taille de sortie n bits,
 - déterminer une valeur x et à partir de cette valeur x et en appliquant plusieurs fois l'application f_K , afin de générer t valeurs v_i ,
 - à partir des t valeurs v_i et de $u \cdot t$ coefficients déterminer u blocs S_i contenant des caractères pseudo-aléatoires.
- 2 - Procédé selon la revendication 1 pour générer des chaînes de bits pseudo-aléatoires, au sein d'un système comprenant un module de codage de données, telles qu'un message de $b = f \cdot u \cdot n + q$ bits, où f et u sont supérieurs ou égaux à 0, et q est compris entre 0 et $u \cdot n$, peut se mettre sous la forme de f groupes de u blocs de n bits et d'un $(f+1)$ ième groupe de q bits caractérisé en ce que :
- le codage d'un groupe considéré de u blocs comporte au moins les étapes suivantes :
- pour le groupe considéré choisir une valeur initiale x ,
 - à partir des t valeurs v_i générées et de $u \cdot t$ coefficients déterminer u blocs S_i contenant des caractères pseudo-aléatoires afin de coder les u blocs du groupe considéré,
 - combiner les u blocs du groupe considéré avec les u blocs S_i afin d'obtenir le groupe codé,
 - réitérer ces trois étapes pour les f groupes,
- pour le $(f+1)$ ième groupe de q bits,
- choisir une valeur initiale de x ,

- à partir des t valeurs v_i générées et de $u \cdot t$ coefficients déterminer un nombre de blocs S_i égal au moins à la partie entière supérieure de q/n ,
 - combiner q bits extraits des blocs S_i déterminés avec les q bits du
- 5 $(f+1)$ ème groupe.

3 – Procédé selon la revendication 2 caractérisé en ce que l'on fait varier les $u \cdot t$ coefficients en faisant varier la valeur de t .

- 10 4 – Procédé selon l'une des revendications 1 à 3 caractérisé en ce que les blocs S_i sont obtenus de la manière suivante

$$S_i = (\alpha_{i,1} \otimes v_1) \oplus (\alpha_{i,2} \otimes v_2) \oplus (\alpha_{i,3} \otimes v_3) \oplus \dots \oplus (\alpha_{i,t} \otimes v_t)$$

Où $\otimes$ est la multiplication avec

- Dans le cas $\alpha_{i,j} = 1$, $a_{i,j} \otimes v_j = v_j$
- 15 ○ Dans le cas $\alpha_{i,j} = 0$, $a_{i,j} \otimes v_j = 0$

5 - Procédé selon l'une des revendications 1 à 3 caractérisé en ce que les blocs S_i sont obtenus de la manière suivante

$$S_i = (\alpha_{i,1} \otimes v_1) \oplus (\alpha_{i,2} \otimes v_2) \oplus (\alpha_{i,3} \otimes v_3) \oplus \dots \oplus (\alpha_{i,t} \otimes v_t)$$

- 20 avec, pour les $\alpha_{i,j}$ tels que $0 \leq \alpha_{i,j} \leq 1$, $a_{i,j} \otimes v_j$ représentant la sélection de $a_{i,j}$ % des n bits, selon un critère de sélection connu de l'application.

6 – Procédé selon l'une des revendications 2 à 5 caractérisé en ce que l'on détermine la valeur du bloc m_i d'indice i codé par $C_i = m_i \oplus S_i$

- 25 où $\oplus$ correspond soit à l'opération xor égale au « ou exclusif » bit à bit ou à l'addition modulaire modulo 2^n

7 – Procédé selon l'une des revendications 1 à 6 caractérisé en ce que les valeurs t peuvent être obtenues en appliquant une fonction g choisie parmi la

- 30 liste suivante :

- $g_i(f_K, x) = f_K(x + i - 1)$,
- $g_i(f_K, x) = f_K(L^i(x))$ où L^i correspond à la $i^{\text{ème}}$ itération d'un LFSR ou d'un registre diviseur,
- $g_i(f_K, x) = f_K(a_i x + b_i)$ où a_i et b_i sont des coefficients d'une transformation affine,
- $g_i(f_K, x) = f_K(a_i x + b_i \bmod 2^n)$ où a_i et b_i sont des coefficients d'une transformation affine,
- $g_i(f_K, x) = f_K(x + i) \oplus d_i$, où $\oplus$ représente l'opération de xor bit à bit et d_i est une chaîne de bits,
- $g_i(f_K, x) = f_K(x + i - 1) \oplus d_i$, où $\oplus$ représente l'opération de xor bit à bit et d_i est une chaîne de bits,
- $g_i(f_K, x) = f_K(L^i(x)) \oplus d_i$, où L^i correspond à la $i^{\text{ème}}$ itération d'un LFSR ou d'un registre diviseur, $\oplus$ représente l'opération de xor bit à bit et d_i est une chaîne de bits.

15

8 – Procédé selon l'une des revendications 1 à 7 caractérisé en ce que la fonction f_K est une permutation.

20

9 - Procédé selon l'une des revendications précédentes caractérisé en ce que les $u \cdot t$ coefficients correspondent aux coefficients d'une matrice d'un code linéaire.

25

10 - Procédé selon l'une des revendications précédentes caractérisé en ce que la valeur x est stockée ou générée en exécutant un processus aléatoire ou pseudo-aléatoire ou déterministe.

30

11 – Utilisation du procédé selon la revendication 1 ou l'une des revendications 4 à 5 ou 7 pour l'authentification d'utilisateurs d'un système ou l'authentification de données.

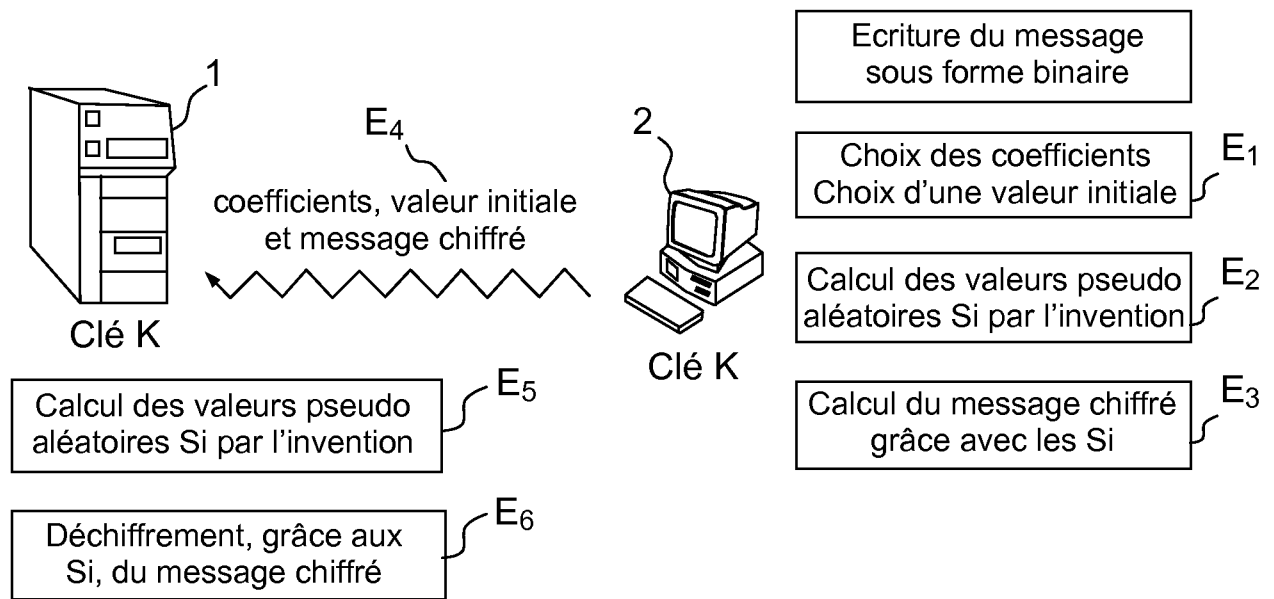


FIG.1

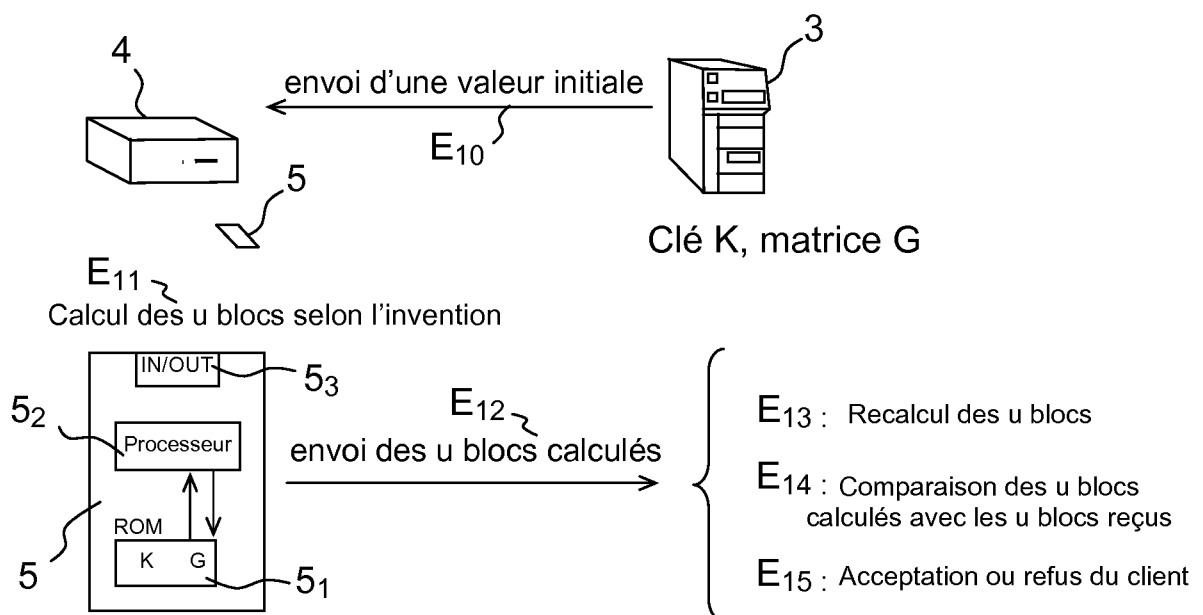


FIG.2

INTERNATIONAL SEARCH REPORT

International application No

PCT/EP2008/055792

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06F7/58 H04L9/06

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)

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)

EP0-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	TETSU IWATA ED - MATTHEW ROBshaw: "New Blockcipher Modes of Operation with Beyond the Birthday Bound Security" FAST SOFTWARE ENCRYPTION LECTURE NOTES IN COMPUTER SCIENCE, vol. 4047, 2006, pages 310-327, XP019041659 SPRINGER, BERLIN HEIDELBERG ISBN: 978-3-540-36597-6 cited in the application page 316 - page 317; figures 2-4	1,2,4-11

☐ Further documents are listed in the continuation of Box C.

☐ See patent family 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

11 août 2008

Date of mailing of the international search report

27/08/2008

Name and mailing address of the ISA/

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

Authorized officer

Verhoof, Paul

INTERNATIONAL SEARCH REPORT

International application No.

PCT/EP2008/055792

Box No. II Observations where certain claims were found unsearchable (Continuation of item 2 of first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☒ Claims Nos.: **3**
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:
see FURTHER INFORMATION sheet PCT/ISA/210

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box No. III Observations where unity of invention is lacking (Continuation of item 3 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

1. ☐ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.
2. ☐ As all searchable claims could be searched without effort justifying additional fees, this Authority did not invite payment of additional fees.
3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest

- ☐ The additional search fees were accompanied by the applicant's protest and, where applicable, the payment of a protest fee.
- ☐ The additional search fees were accompanied by the applicant's protest but the applicable protest fee was not paid within the time limit specified in the invitation.
- ☐ No protest accompanied the payment of additional search fees.

Continuation of Box II.2I**Claim 3**

The additional feature of claim 3 is not supported by the description. The method according to claim 2 is explained on pages 12 and 13. Neither this passage nor any other relates to "varying the u*t coefficients". A meaningful search consequently appears to be neither necessary nor feasible. The aforementioned feature is very vague and ambiguous. (How and when are the coefficients varied? Which coefficients? those according to claim 1? the first coefficients according to claim 2? the second group of coefficients according to claim 2? What is the technical advantage?) Even had a clear definition been provided, a search would not have been possible because of the lack of support provided by the description.

The applicant is advised that claims relating to inventions in respect of which no international search report has been established cannot normally be the subject of an international preliminary examination (PCT Rule 66.1(e)). The applicant is further advised that, in its capacity as International Preliminary Examining Authority, the EPO generally will not carry out a preliminary examination for subjects in respect of which no search has been carried out. This applies regardless of whether were amended after receipt of the international search report (PCT Article 19) or in the course of the procedure under PCT Chapter II. However, if the application enters the regional phase before the EPO, an additional search can be carried out in the course of the examination (cf. EPO Guidelines, C-VI, 8.2) if the defects that led to the declaration under PCT Article 17(2) have been remedied.

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale n°

PCT/EP2008/055792

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
INV. G06F7/58 H04L9/06

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)
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 cela est réalisable, termes de recherche utilisés)
EPO-Internal

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie*	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
X	TETSU IWATA ED - MATTHEW ROBshaw: "New Blockcipher Modes of Operation with Beyond the Birthday Bound Security" FAST SOFTWARE ENCRYPTION LECTURE NOTES IN COMPUTER SCIENCE, vol. 4047, 2006, pages 310-327, XP019041659 SPRINGER, BERLIN HEIDELBERG ISBN: 978-3-540-36597-6 cité dans la demande page 316 - page 317; figures 2-4	1,2,4-11

☐ 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'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

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

Date à laquelle la recherche internationale a été effectivement achevée

11 août 2008

Date d'expédition du présent rapport de recherche internationale

27/08/2008

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

Fonctionnaire autorisé

Verhoof, Paul

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale n°
PCT/EP2008/055792

Cadre n°. II Observations – lorsqu'il a été estimé que certaines revendications ne pouvaient pas faire l'objet d'une recherche (suite du point 2 de la première feuille)

Le rapport de recherche internationale n'a pas été établi en ce qui concerne certaines revendications conformément à l'article 17.2)a) pour les raisons suivantes :

1. ☐ Les revendications n°s
se rapportent à un objet à l'égard duquel l'administration chargée de la recherche internationale n'est pas tenue de procéder à la recherche, à savoir :

2. ☒ Les revendications n°s 3
parce qu'elles se rapportent à des parties de la demande internationale qui ne remplissent pas suffisamment les conditions prescrites pour qu'une recherche significative puisse être effectuée, en particulier :

voir FEUILLE ANNEXÉE PCT/ISA/210

3. ☐ Les revendications n°s
parce qu'elles sont des revendications dépendantes et ne sont pas rédigées conformément aux dispositions de la deuxième et de la troisième phrases de la règle 6.4.a).

Cadre n°. III Observations – lorsqu'il y a absence d'unité de l'invention (suite du point 3 de la première feuille)

L'administration chargée de la recherche internationale a trouvé plusieurs inventions dans la demande internationale, à savoir :

1. ☐ Comme toutes les taxes additionnelles exigées ont été payées dans les délais par le déposant, le présent rapport de recherche internationale porte sur toutes les revendications pouvant faire l'objet d'une recherche.

2. ☐ Comme toutes les revendications qui se prêtent à la recherche ont pu faire l'objet de cette recherche sans effort particulier, justifiant des taxes additionnelles, l'administration chargée de la recherche internationale n'a sollicité le paiement d'aucunes taxes de cette nature.

3. ☐ Comme une partie seulement des taxes additionnelles demandées a été payée dans les délais par le déposant, le présent rapport de recherche internationale ne porte que sur les revendications pour lesquelles les taxes ont été payées, à savoir les revendications n°s :

4. ☐ Aucunes taxes additionnelles demandées n'ont été payées dans les délais par le déposant. En conséquence, le présent rapport de recherche internationale ne porte que sur l'invention mentionnée en premier lieu dans les revendications; elle est couverte par les revendications n°s :

Remarque quant à la réserve ☐ Les taxes additionnelles étaient accompagnées d'une réserve de la part du déposant et, le cas échéant, du paiement de la taxe de réserve.

☐ Les taxes additionnelles étaient accompagnées d'une réserve de la part du déposant mais la taxe de réserve n'a pas été payée dans le délai prescrit dans l'invitation.

☐ Le paiement des taxes additionnelles n'était assorti d'aucune réserve.

SUITE DES RENSEIGNEMENTS INDICUES SUR PCT/ISA/ 210

Suite du cadre II.2

Revendications nos.: 3

La caractéristique supplémentaire de la revendication 3 manque un fondement dans la description. Le procédé de la revendication 2 est expliqué aux pages 12 et 13. Ni dans ce passage ni dans le reste de l'exposé il est question de "faire varier les u*t coefficients". Une recherche significative n'est, par conséquent, ni requise ni possible. Cette caractéristique est très vague est équivoque (comment et quand on fait varier les coefficients ? Quels coefficients : ceux de revendication 1 ? Les premiers de revendication 2 ? Les deuxièmes de revendication 2 ? Quel est l'avantage technique ?). Une définition claire n'aurait pas permis de faire une recherche, à cause du manque d'un fondement dans la description.

L'attention du déposant est attirée sur le fait que les revendications ayant trait aux inventions pour lesquelles aucun rapport de recherche n'a été établi ne peuvent faire obligatoirement l'objet d'un rapport préliminaire d'examen (Règle 66.1(e) PCT). Le déposant est averti que la ligne de conduite adoptée par l'OEB agissant en qualité d'administration chargée de l'examen préliminaire international est, normalement, de ne pas procéder à un examen préliminaire sur un sujet n'ayant pas fait l'objet d'une recherche. Cette attitude restera inchangée, indépendamment du fait que les revendications aient ou n'aient pas été modifiées, soit après la réception du rapport de recherche, soit pendant une quelconque procédure sous le Chapitre II. Si la demande devait être poursuivie dans la phase régionale devant l'OEB, il est rappelé au déposant qu'une recherche pourrait être effectuée durant la procédure d'examen devant l'OEB (voir Directive OEB C-VI, 8.2) à condition que les problèmes ayant conduit à la déclaration conformément à l'Article 17(2) PCT aient été résolus.