

12

DEMANDE DE BREVET D'INVENTION

A1

22 Date de dépôt : 13.02.06.

30 Priorité :

43 Date de mise à la disposition du public de la
demande : 17.08.07 Bulletin 07/33.

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

60 Références à d'autres documents nationaux
apparentés :

71 Demandeur(s) : FRANCE TELECOM Société ano-
nyme — FR.

72 Inventeur(s) : ROBSHAW MATT.

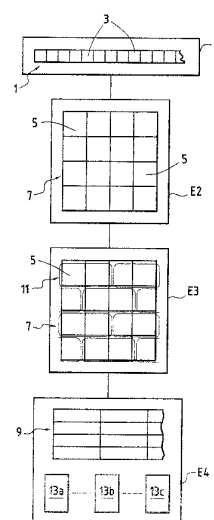
73 Titulaire(s) :

74 Mandataire(s) : CABINET BEAU DE LOMENIE.

54 DISPOSITIF ET PROCEDE DE CRYPTOGRAPHIE POUR GENERER DES NOMBRES PSEUDO-ALETOIRES.

57 L'invention concerne un dispositif et un procédé cryp-
tographique pour générer des nombres pseudo-aléatoires
(1), comportant les étapes suivantes:

- subdiviser des données initiales (1) en une pluralité de mots (3) à b-bits définis dans un corps fini GF(2^b),
- affecter lesdits mots à des cellules (5) d'un tableau d'état (7) pour former un bloc d'état initial (13a),
- regrouper les cellules (5) dudit tableau d'état (7) pour affecter un groupe (11) de cellules à chaque ensemble de d/b mots, où dest un multiple de b strictement supérieur à b, et
- générer de manière itérative à partir dudit bloc d'état initial (13a), une succession de blocs d'états (13b) pour former un bloc d'état final (13c), de sorte qu'à chaque itération chaque ensemble de d/b mots d'un bloc d'état (13b) courant est remplacé par un autre ensemble de d/b mots, en utilisant, pour former un bloc d'état suivant, au moins une table de référence (9) comportant des éléments de substitution à d-bits.



Titre de l'invention

Dispositif et procédé de cryptographie pour générer des nombres pseudo-aléatoires.

Domaine technique de l'invention

L'invention se rapporte au domaine de la cryptographie. Plus précisément, l'invention concerne l'utilisation d'un schéma de génération de nombres pseudo-aléatoires pouvant être mis en œuvre dans des dispositifs ayant une faible puissance de calcul. La technique selon l'invention peut être appliquée à la mise en œuvre d'un générateur de nombres pseudo-aléatoires (en anglais "*pseudo-random number generator*" ou PRNG) de faible coût.

Arrière-plan de l'invention

D'une manière générale, il existe deux approches pour la conception des algorithmes cryptographiques symétriques.

La première approche consiste à fournir "une preuve de sécurité" fondée sur la relation entre une méthode pour "casser" un code et la capacité à résoudre ce qui est communément considéré comme un problème difficile.

La deuxième approche plus commune dépend d'une ingénierie minutieuse d'un circuit électronique comportant plusieurs composants de type portes logiques pour réaliser un chiffrement selon le niveau de sécurité souhaité. Dans ce cas, l'efficacité peut être quantifiée par la vitesse de calcul ou le nombre de portes logiques nécessaires pour réaliser le circuit électronique.

Actuellement, et après la normalisation des algorithmes cryptographiques de type AES (Standard de chiffrement avancé, ou "*Advanced Encryption Standard*" en anglais : FIPS 197, NIST 2001), il

existe un grand intérêt à mettre en œuvre ce genre d'algorithmes dans une large gamme d'applications.

L'AES est remarquable pour son étroite observation des principes connus de Shannon et de deux notions importantes pour la mise en œuvre des algorithmes cryptographique, à savoir la "confusion" et la "diffusion". De façon simplifiée, la "confusion" correspond à l'idée de "faire des opérations difficiles" tandis que la "diffusion" correspond à l'idée de "faire propager le changement ou la transformation" pendant un calcul cryptographique.

Il est habituellement considéré qu'un des meilleurs moyens pour fournir un effet de confusion consiste à utiliser une boîte de substitution "boîte-S" (S-box Substitution box), et qu'un des meilleurs moyens pour fournir un effet de diffusion consiste à réaliser un certain type de permutation.

En effet, l'algorithme AES prend en entrée un bloc de 16 octets. Chaque octet est remplacé par un autre octet selon une boîte de substitution (boîte-S) de 8-bits vers 8-bits. Ces octets sont ensuite placés dans une matrice où chaque élément de la matrice est décalé cycliquement à gauche d'un certain nombre de colonnes. Ensuite, on effectue un produit matriciel avant d'ajouter chaque octet avec un octet correspondant d'une clé d'itération ("*round key*" en anglais) obtenue par diversification d'une clé de chiffrement.

Ainsi, la sécurité d'un algorithme du type AES dépend d'une interaction entre la boîte-S et une opération de mélange (ou de diffusion) consistant à permuter des octets et à les combiner structurellement. L'interaction entre ces octets est mise en œuvre de manière précise afin de garantir et de fournir une bonne résistance contre les attaques par cryptanalyse différentielle ou par cryptanalyse linéaire.

Actuellement, on essaie d'introduire des fonctionnalités cryptographiques dans des environnements de calcul très restreints comme par exemple dans des puces RFID.

Cependant, des algorithmes pour ce genre d'environnement sont réalisés au coup par coup et utilisent des composants cryptographiques de faible capacité. En effet, il est très difficile de réaliser des composants cryptographiques ayant une qualité comparable à ceux utilisés pour la mise en œuvre d'un algorithme de type AES dans un environnement très restreint.

Objet et résumé de l'invention

La présente invention concerne un procédé cryptographique pour générer des nombres pseudo-aléatoires comportant les étapes suivantes :

- subdiviser des données initiales en une pluralité de mots à b -bits définis dans un corps fini $GF(2^b)$,
- affecter lesdits mots à des cellules d'un tableau d'état pour former un bloc d'état initial,
- regrouper les cellules dudit tableau d'état pour affecter un groupe de cellules à chaque ensemble de d/b mots, où d est un multiple de b strictement supérieur à b , et
- générer de manière itérative à partir dudit bloc d'état initial, une succession de blocs d'états pour former un bloc d'état final, de sorte qu'à chaque itération chaque ensemble de d/b mots d'un bloc d'état courant est remplacé par un autre ensemble de d/b mots, en utilisant, pour former un bloc d'état suivant, au moins une table de référence comportant des éléments de substitution à d -bits.

Le fait d'utiliser une table de référence ayant des éléments de longueur d strictement supérieure à b introduit un effet de diffusion en

plus de l'effet de confusion, réalisant ainsi une génération de nombres pseudo-aléatoires de qualité avec un coût de calcul très réduit.

On notera qu'un algorithme de type AES utilise une boîte-S ayant des éléments de la même taille que les mots d'un bloc d'état interne faisant correspondre un mot d'entrée de b -bits à un autre mot de sortie de b -bits, et les mots sont utilisés un par un. Ainsi, le remplacement des mots par substitution selon la boîte-S réalisée par ce genre d'algorithme engendre un effet de confusion mais aucun effet de diffusion.

En revanche, l'opération de substitution selon la table de référence de l'invention n'utilise pas les mots un par un, mais par regroupement. Par ailleurs, on notera que l'utilisation d'une table de référence ou boîte-S ayant des éléments plus grands que les mots de l'état interne est tout à fait contraire aux habitudes de l'homme du métier.

Ainsi, la configuration selon l'invention permet d'assurer à la fois la diffusion et la confusion tout en économisant du temps de calcul pour le même niveau de sécurité. Ceci permet d'améliorer le niveau de sécurité tout en diminuant le nombre de portes logiques ("*gates equivalent*" ou GE en anglais) dans la réalisation d'un circuit électronique mettant en œuvre ce procédé de chiffrement. Ainsi, la technique selon l'invention peut être facilement appliquée pour la mise en œuvre d'un générateur de nombres pseudo-aléatoires de faible coût et dans un environnement très restreint comme une cellule ou puce RFID. En outre, cette technique peut être appliquée à une variété d'algorithmes cryptographiques du type codage par blocs, codage par flux, fonctions de hachage, ou codes d'authentification de messages. De plus, l'utilisation de ce genre de table de référence avec d strictement supérieure à b permet de réaliser un générateur de nombres pseudo-aléatoires plus robuste aux attaques par cryptanalyse de type "*square attacks*" auxquelles les algorithmes de type AES sont réputés être sensibles.

Avantageusement, la génération itérative de ladite succession de blocs d'états comporte en outre une étape pour mélanger les mots dudit bloc d'état courant selon une transformation de mélange prédéterminée.

Cette transformation de mélange garantit une meilleure diffusion ou propagation des bits d'un bloc d'état améliorant ainsi la sécurité du cryptage et la qualité des nombres pseudo-aléatoires générés sans trop alourdir les étapes de calcul.

Cette transformation de mélange prédéterminée peut comporter une multiplication dans le corps fini $GF(2^b)$ d'une colonne dudit bloc d'état courant par une matrice prédéfinie dans ledit corps fini. Cette multiplication matricielle est une transformation linéaire assez simple à mettre en œuvre.

Avantageusement, la génération itérative de ladite succession de blocs d'états comporte en outre une permutation entre des mots sur au moins une partie dudit bloc d'état courant.

Ceci permet d'augmenter encore davantage la propagation des bits, ce qui améliore la sécurité.

Selon une particularité de la présente invention, la génération itérative de ladite succession de blocs d'états comporte en outre une modification d'au moins une partie d'un mot situé dans une cellule prédéterminée du tableau d'état.

Ceci permet de réduire toute symétrie pouvant s'installer lors des itérations successives, ce qui complique toute tentative de prédiction et améliore par conséquent la sécurité du procédé.

Selon une autre particularité de la présente invention, le procédé comporte une combinaison par addition dans le corps fini de chaque mot dudit bloc d'état initial avec un mot correspondant dans une clé de chiffrement améliorant ainsi le niveau de sécurité.

Ainsi, une sécurité similaire à celle d'un algorithme de type AES peut être garantie avec un nombre optimal de calculs.

Avantageusement, lesdites données initiales sont générées par un compteur. Ainsi, on peut facilement générer des nombres pseudo-aléatoires avec un nombre minimal d'opérations.

L'invention vise aussi un dispositif cryptographique pour générer des nombres pseudo-aléatoires, comportant :

- un moyen de subdivision pour subdiviser des données initiales en une pluralité de mots à b -bits définis dans un corps fini $GF(2^b)$,
- un moyen d'affectation pour affecter lesdits mots à des cellules d'un tableau d'état pour former un bloc d'état initial,
- un moyen de définition pour définir et mémoriser au moins une table de référence comportant des éléments de substitution à d -bits, où d -est un multiple de b strictement supérieur à b ,
- un moyen de regroupement pour regrouper les cellules dudit tableau d'état pour affecter un groupe de cellules à chaque ensemble de d/b mots, et
- un moyen de génération pour générer de manière itérative à partir dudit bloc d'état initial, une succession de blocs d'états pour former un bloc d'état final, de sorte qu'à chaque itération chaque ensemble de d/b mots d'un bloc d'état courant est remplacé par un autre ensemble de d/b mots en fonction de ladite table de référence pour former un bloc d'état suivant.

L'invention vise également un générateur de nombres pseudo-aléatoires comportant un compteur et une pluralité de portes logiques pour la mise en œuvre du procédé décrit succinctement ci-dessus.

L'invention vise aussi un dispositif RFID comportant un générateur tel que décrit succinctement ci-dessus.

Brève description des dessins

D'autres particularités et avantages de l'invention ressortiront à la lecture de la description faite, ci-après, à titre indicatif mais non limitatif, en référence aux dessins annexés, sur lesquels :

- la figure 1 est un organigramme illustrant les différentes étapes d'un procédé cryptographique selon l'invention ;
- la figure 2 est un exemple illustrant l'action d'une table de référence selon le procédé de la figure 1 ;
- la figure 3 illustre très schématiquement un dispositif mettant en œuvre le procédé de la figure 1 ;
- la figure 4 est un mode particulier de réalisation du procédé de la figure 1 ; et
- la figure 5 illustre très schématiquement un générateur de nombres pseudo-aléatoires mettant en œuvre le procédé de la figure 4.

Description détaillée de modes de réalisation

Conformément à l'invention, la figure 1 est un organigramme illustrant les différentes étapes d'un procédé cryptographique pour générer des nombres pseudo-aléatoires à partir de données initiales.

L'étape E1 comporte le découpage ou la subdivision du message ou des données initiales 1 en une pluralité de mots 3 à b -bits définis dans un corps fini $GF(2^b)$, où b peut par exemple être égal à 2, 4, 8, 16, 32, 64 ou 128.

A l'étape E2, ces mots 3 sont affectés à des cellules 5 d'un tableau d'état 7 pour former un bloc d'état initial. On notera qu'on peut ne placer qu'une partie de ces mots 3 dans le tableau d'état 7.

A l'étape E3, on regroupe les cellules 5 du tableau d'état 7 de manière à affecter un groupe 11 de cellules à chaque ensemble de d/b mots, où d est un multiple de b , avec $d > b$. Chaque ensemble de mots correspond alors à un élément de d -bits.

Finalement, à l'étape E4, on génère de manière itérative à partir du bloc d'état initial 13a, une succession de blocs d'états 13b courants pour former un dernier bloc ou un bloc d'état final 13c. Pour ce faire, on utilise au moins une table de référence ou de substitution 9 prédéfinie comportant des éléments de substitution à d -bits. Ainsi, cette table de référence 9 permet de remplacer un élément d'entrée de d -bits par un élément de sortie de d -bits.

A chaque itération, chaque ensemble de d/b mots d'un bloc d'état 13b courant est remplacé par un autre ensemble de d/b mots en fonction de la table de référence 9 pour former un bloc d'état suivant. Ainsi, le dernier bloc d'état 13c représente le nombre pseudo-aléatoire généré.

Le fait d'utiliser une table de référence ayant des éléments de longueur $d > b$ introduit un effet de diffusion en plus de l'effet de confusion et permet de réaliser un bon niveau de sécurité d'une manière plus rapide qu'une table de substitution (boîte-S) de l'état de l'art où $d = b$.

La figure 2 est un exemple illustrant l'action d'une table de référence 9 sur un tableau d'état 7 comportant quatre colonnes et quatre lignes (4×4). Selon cet exemple le bloc d'état initial 13a comporte les mots $A_{00}, \dots, A_{33}$ à 4-bits (c'est-à-dire $b = 4$) et la table de référence 9 comporte des éléments à 8-bits (c'est-à-dire $d = 8$). Dans ce cas, on peut utiliser une table de référence du type boîte-S d'un algorithme AES.

Ainsi, les cellules 5 du tableau d'état 7 sont regroupées par groupes de deux cellules. Selon cet exemple, les cellules 5 comportant les mots A_{00} et A_{01} forment un premier groupe 11a, ceux comportant les mots A_{02} et A_{03} forment un deuxième groupe 11b, et ceux comportant les mots A_{11} et A_{12} forment un troisième groupe 11c, etc. Dans ce cas, la table de référence 9 substitue les mots deux par deux. Par exemple les mots A_{00} et A_{01} sont remplacés par B_{00} et B_{01} et les mots A_{02} et A_{03} sont remplacés par

B_{02} et B_{03} . Alors un autre bloc d'état 13b est formé comportant les mots $B_{00}, \dots, B_{33}$ définis par une fonction "S" déterminée par la table de référence 9 de la manière suivante :

$$B_{00}||B_{01} = S[A_{00}||A_{01}], \quad B_{02}||B_{03} = S[A_{02}||A_{03}]$$

$$B_{11}||B_{12} = S[A_{11}||A_{12}], \quad B_{13}||B_{10} = S[A_{13}||A_{10}]$$

$$B_{20}||B_{21} = S[A_{20}||A_{21}], \quad B_{22}||B_{23} = S[A_{22}||A_{23}]$$

$$B_{31}||B_{32} = S[A_{31}||A_{32}], \quad B_{33}||B_{30} = S[A_{33}||A_{30}],$$

où le symbole "||" entre deux mots représente leur concaténation.

Ainsi, on peut générer de manière itérative une succession de blocs d'état 13b en fonction d'une ou de plusieurs tables de référence 9. On notera que dans un milieu restreint (par exemple RFID), il est préférable (quoique non obligatoire) d'utiliser une seule table de référence 9 pour toutes les opérations.

Afin de garantir une meilleure propagation, les mots 3 d'un bloc d'état 13b courant peuvent être mélangés selon une transformation "MIX" de mélange prédéterminée.

Ainsi, à chaque itération, l'opération de substitution en fonction de la table de référence 9 peut être suivie par un mélange de mots à b -bits, en utilisant par exemple une technique similaire à celle utilisée par l'algorithme AES.

Selon l'exemple de la figure 2, ce mélange MIX peut être réalisé de la manière suivante :

$$C_{00}||C_{10}||C_{20}||C_{30} = \text{MIX} [B_{00}||B_{10}||B_{20}||B_{30}]$$

$$C_{01}||C_{11}||C_{21}||C_{31} = \text{MIX} [B_{01}||B_{11}||B_{21}||B_{31}]$$

$$C_{02}||C_{12}||C_{22}||C_{32} = \text{MIX} [B_{02}||B_{12}||B_{22}||B_{32}]$$

$$C_{03}||C_{13}||C_{23}||C_{33} = \text{MIX} [B_{03}||B_{13}||B_{23}||B_{33}]$$

Selon les propriétés de l'opération de mélange MIX qui dépendent des matrices choisies, il peut être avantageux de permuter des mots 3 sur au moins une partie du bloc d'état 13b courant selon une opération de permutation "Echanger" ("*swap*" en anglais).

Selon l'exemple de la figure 2, cette permutation " Echanger " peut être réalisée de la manière suivante :

Echanger $C_{02}||C_{12}$ avec $C_{22}||C_{32}$

Echanger $C_{03}||C_{13}$ avec $C_{23}||C_{33}$

En outre, selon les caractéristiques des composants électroniques utilisés pour la fabrication d'un dispositif mettant en œuvre le procédé selon l'invention, un simple compteur d'incrémentation ou un tout autre mécanisme similaire peut être utilisé pour réduire toute symétrie pouvant s'installer lors des itérations successives. A titre d'exemple, ceci peut comporter une simple modification d'au moins une partie d'un mot situé dans une cellule 5 prédéterminée du tableau d'état 7. Par exemple, il suffit de compléter quelques bits situés dans une seule cellule 5 bien déterminée et à un moment bien déterminé du calcul.

De plus, le procédé selon l'invention peut comporter une combinaison par addition (opération "ou-exclusif") dans le corps fini de chaque mot 3 du bloc d'état initial 13a avec un mot correspondant d'une clé de chiffrement prédéfinie ou avec des suites alternées de mots secrets.

La figure 3 illustre très schématiquement un dispositif 21 mettant en œuvre le procédé selon la figure 1. Ce dispositif 21 comporte un moyen de subdivision 23, un moyen d'affectation 25, un moyen de définition 27, un moyen de regroupement 29 et un moyen de génération 31.

Le moyen de subdivision 23 est destiné à subdiviser le message ou les données initiales en une pluralité de mots 3 à b -bits. Le moyen d'affectation 25 est destiné à affecter ces mots 3 aux cellules 5 du tableau d'état 7 pour former le bloc d'état initial 13a. Le moyen de définition 27 est destiné à définir et mémoriser la ou les tables de référence 9 ou de substitution comportant les éléments de substitution à d -bits avec $d > b$. Le moyen de regroupement 29 est destiné à regrouper les cellules 5 du tableau d'état pour affecter un groupe 11 de cellules à

chaque ensemble de d/b mots. Le moyen de génération 31 est destiné à générer de manière itérative à partir du bloc d'état initial 13a, une succession de blocs d'états 13b pour former un bloc d'état final 13c représentatif d'un nombre pseudo-aléatoire.

Dans la mise en œuvre d'un générateur de nombres pseudo-aléatoires, les données initiales 1 utilisées pour former le bloc d'état initial 13a peuvent être générées par un simple compteur.

En effet, la figure 4 est un organigramme illustrant un mode particulier de réalisation d'un générateur de nombres pseudo-aléatoires PRNG à 64-bits et comportant dix itérations. Ce générateur peut être utilisé dans une puce RFID comportant une clé secrète de 128-bits. La clé secrète peut par exemple être représentée par un couple de données (s_0 , s_1) où s_0 et s_1 ont tous deux une longueur de 64 bits.

A chaque séquence d'itérations définie par un compteur c_i de 16-bits, une valeur de sortie v_i de 64-bits est générée par le PRNG en fonction de c_i , s_0 et s_1 (c'est-à-dire $v_i = f(c_i, s_0, s_1)$ pour $1 \leq i < 2^{16}$).

L'étape E11 est l'état initial d'une séquence d'itérations (le compteur $c_i = 1$). A cette étape, les 64-bits des données initiales 1 sont rangées dans un tableau d'état 7 (4×4) comportant seize mots $A_{00}, \dots, A_{33}$ à 4-bits comme illustré sur l'exemple de la figure 2.

A l'étape E12, la première ligne du tableau d'état 7 est additionnée (selon un ou-exclusif) avec la valeur courante du compteur ordonnée en quatre fois 4-bits, c'est-à-dire $c_i = [c_{i0} || c_{i1} || c_{i2} || c_{i3}]$.

A l'étape E13, on réalise trois itérations d'opérations du type "mixtable". Chaque itération "mixtable" comporte des substitutions selon une fonction S déterminée par une table de référence 9 réalisant des permutations à 8-bits (par exemple une boîte-S de type AES), et/ou un mélange "MIX" à l'intérieur d'une ou plusieurs colonnes, et/ou des permutations "Echanger".

A une itération numéro r donnée, le bloc d'état 13b courant est alors défini en fonction du tableau de référence 9 de la manière suivante :

$$B_{00}||B_{01} = S[A_{00}||A_{01}], \quad B_{02}||B_{03} = S[A_{02}||A_{03}]$$

$$B_{11}||B_{12} = S[A_{11}||A_{12}], \quad B_{13}||B_{10} = S[A_{13}||A_{10}]$$

$$B_{20}||B_{21} = S[A_{20}||A_{21}], \quad B_{22}||B_{23} = S[A_{22}||A_{23}]$$

$$B_{31}||B_{32} = S[A_{31}||A_{32} \oplus r], \quad B_{33}||B_{30} = S[A_{33}||A_{30}]$$

On notera qu'à l'itération numéro r , la valeur prise par r est ajoutée à un mot (par exemple le mot A_{32}) afin de réduire tout effet de symétrie pouvant se produire entre les itérations.

L'opération de mélange MIX est un mélange à l'intérieur d'une colonne utilisant une matrice M prédéterminée de dimension 4×4 dans un corps fini $GF(2^4)$. Cette opération consiste à multiplier chaque colonne du tableau d'état (7) par cette matrice M .

L'opération de mélange MIX peut être suivie par une permutation des mots sur les deux dernières lignes du bloc d'état 13b courant de la manière suivante :

$$C_{02}||C_{12} \text{ échangé avec } C_{22}||C_{32}, \text{ et}$$

$$C_{03}||C_{13} \text{ échangé avec } C_{23}||C_{33}.$$

A l'étape E14, on combine par une addition ou-exclusif, les 64-bits du bloc d'état 13b courant avec les seize demi-octets (16 fois 4-bits) dans s_1 de la clé secrète.

A l'étape E15, on réalise encore quatre itérations d'opérations du type "*mixtable*".

A l'étape E16, on combine par une addition ou-exclusif, les 64-bits du bloc d'état 13b courant avec les seize demi-octets (16 fois 4-bits) dans s_0 de la clé secrète.

A l'étape E17, on réalise encore trois itérations d'opérations du type "*mixtable*".

A l'étape E18, on recombine par une addition ou-exclusif, les 64-bits du bloc d'état 13b courant avec les seize demi-octet (4-bits) dans s_1 de la clé secrète.

L'étape E19 donne la valeur de sortie v_i à la $i^{\text{ème}}$ séquence d'itérations de la manière suivante :

$$v_i = [V_{00}||\dots||V_{03}||V_{10}||\dots||V_{13}||\dots||V_{33}].$$

L'étape E20 est un test pour vérifier si la valeur c_i du compteur est égale à $(2^{16}-1)$. Si oui, la puce est détruite à l'étape E21, sinon, on incrémente c_i à l'étape E22 avant de recommencer les étapes ci-dessus.

La figure 5 illustre très schématiquement un générateur 41 de nombres pseudo-aléatoires PRNG mettant en œuvre le procédé selon la figure 4. Ce générateur 41 comporte un compteur 43 et une pluralité de portes logiques 45. Ce générateur PRNG peut être facilement utilisé dans une puce RFID.

On notera qu'une implémentation d'un algorithme du type AES est déterminée par une boîte-S et une mémoire RAM nécessitant 395 et 2337 portes logiques (GE) respectivement.

En revanche, en comparaison avec l'algorithme AES, un PRNG 41 selon l'exemple des figures 4 et 5 divise le nombre d'états par deux et ne comporte pas des clés d'itération obtenues par diversification. Par ailleurs, les opérations de mélange à l'intérieur des colonnes nécessitent très peu de portes logiques.

Ainsi, on obtient, grâce à l'invention, un générateur PRNG 41 efficace avec un bon niveau de sécurité et un nombre de portes (GE) réduit par rapport à l'algorithme AES.

REVENDEICATIONS

1. Procédé cryptographique pour générer des nombres pseudo-aléatoires (1), caractérisé en ce qu'il comporte les étapes suivantes :

- subdiviser des données initiales (1) en une pluralité de mots (3) à b -bits définis dans un corps fini $GF(2^b)$,
- affecter lesdits mots à des cellules (5) d'un tableau d'état (7) pour former un bloc d'état initial (13a),
- regrouper les cellules (5) dudit tableau d'état (7) pour affecter un groupe (11) de cellules à chaque ensemble de d/b mots, où d est un multiple de b strictement supérieur à b , et
- générer de manière itérative à partir dudit bloc d'état initial (13a), une succession de blocs d'états (13b) pour former un bloc d'état final (13c), de sorte qu'à chaque itération chaque ensemble de d/b mots d'un bloc d'état (13b) courant est remplacé par un autre ensemble de d/b mots, en utilisant, pour former un bloc d'état suivant, au moins une table de référence (9) comportant des éléments de substitution à d -bits.

2. Procédé selon la revendication 1, caractérisé en ce que la génération itérative de ladite succession de blocs d'états (13b) comporte en outre une étape pour mélanger les mots dudit bloc d'état courant selon une transformation de mélange prédéterminée.

3. Procédé selon la revendication 2, caractérisé en ce que ladite transformation de mélange prédéterminée comporte une multiplication dans le corps fini $GF(2^b)$ d'une colonne dudit bloc d'état courant par une matrice prédéfinie dans ledit corps fini.

4. Procédé selon l'une quelconque des revendications 1 à 3, caractérisé en ce que la génération itérative de ladite succession de blocs d'états comporte en outre une permutation entre des mots sur au moins une partie dudit bloc d'état courant.

5. Procédé selon l'une quelconque des revendications 1 à 4, caractérisé en ce que la génération itérative de ladite succession de blocs d'états comporte en outre une modification d'au moins une partie d'un mot situé dans une cellule (5) prédéterminée du tableau d'état (7).

6. Procédé selon l'une quelconque des revendications 1 à 5, caractérisé en ce qu'il comporte une combinaison par addition dans le corps fini de chaque mot dudit bloc d'état initial (13a) avec un mot correspondant dans une clé de chiffrement.

7. Procédé selon l'une quelconque des revendications 1 à 6, caractérisé en ce que lesdites données initiales (1) sont générés par un compteur.

8. Dispositif cryptographique pour générer des nombres pseudo-aléatoires, caractérisé en ce qu'il comporte :

- un moyen de subdivision (23) pour subdiviser des données initiales (1) en une pluralité de mots (3) à b -bits définis dans un corps fini $GF(2^b)$,
- un moyen d'affectation (25) pour affecter lesdits mots à des cellules (5) d'un tableau d'état (7) pour former un bloc d'état initial (13a),
- un moyen de définition (27) pour définir et mémoriser au moins une table de référence (9) comportant des éléments de substitution à d -bits, où d est un multiple de b strictement supérieur à b ,
- un moyen de regroupement (29) pour regrouper les cellules dudit tableau d'état pour affecter un groupe de cellules à chaque ensemble de d/b mots, et

- un moyen de génération (31) pour générer de manière itérative à partir dudit bloc d'état initial (13a), une succession de blocs d'états pour former un bloc d'état final (13c) de sorte qu'à chaque itération chaque ensemble de d/b mots d'un bloc d'état courant est remplacé par un autre ensemble de d/b mots en fonction de ladite table de référence (9) pour former un bloc d'état suivant.

9. Générateur de nombres pseudo-aléatoires caractérisé en ce qu'il comporte un compteur (43) et une pluralité de portes logiques (45) pour la mise en œuvre du procédé selon les revendications 1 à 8.

10. Dispositif RFID caractérisé en ce qu'il comporte un générateur (41) selon la revendication 9.

1/3

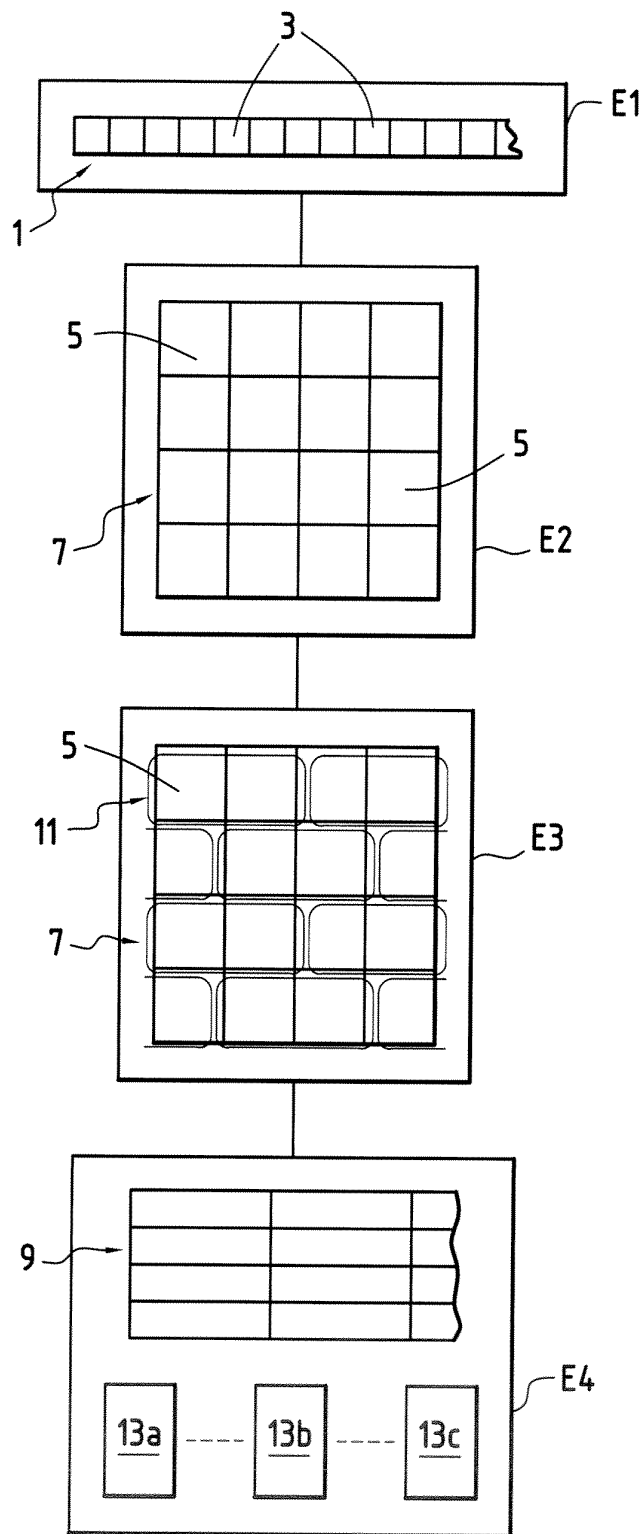


FIG.1

FIG. 2

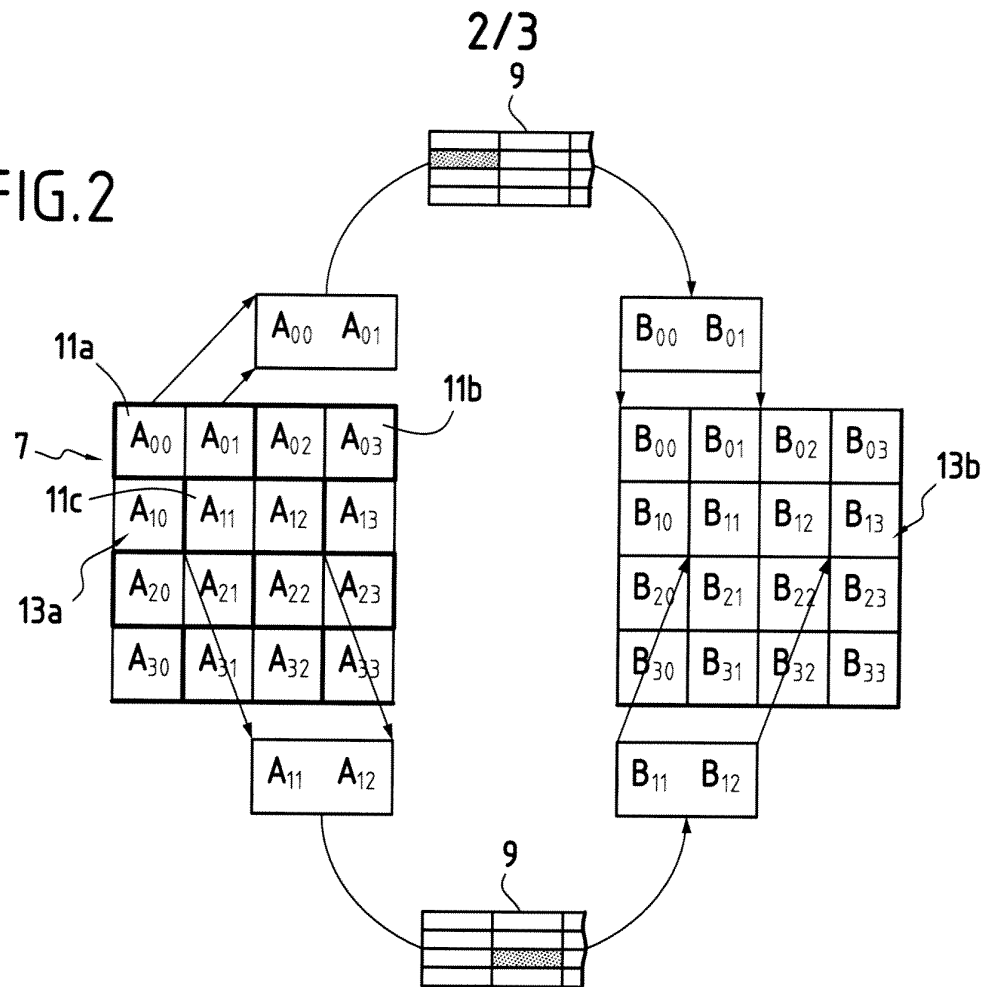


FIG. 3

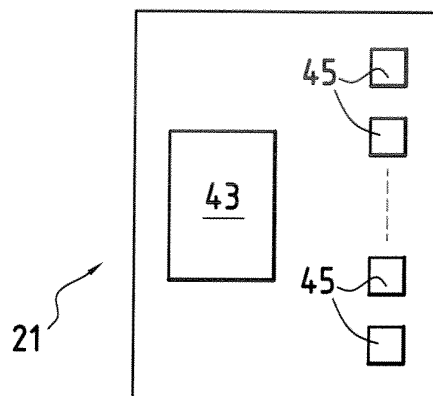
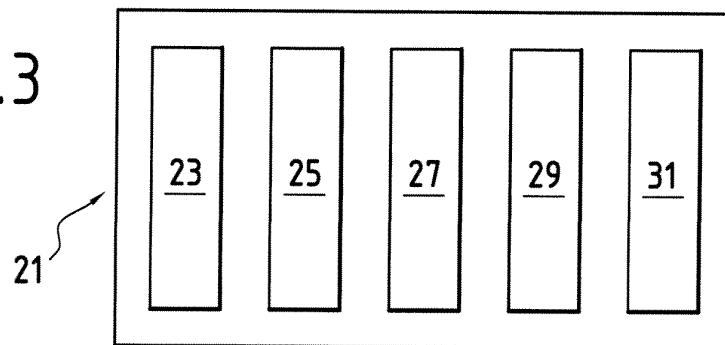


FIG. 5

3/3

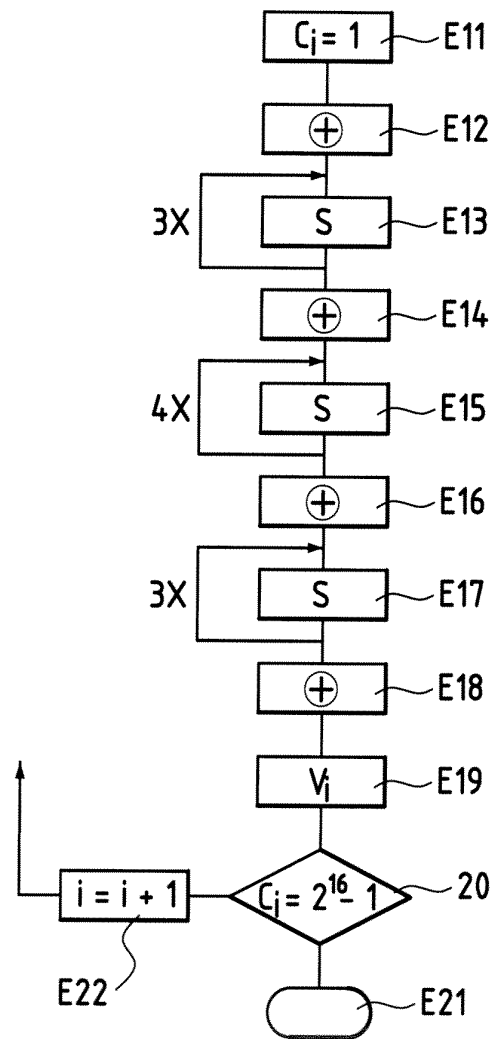


FIG. 4



RAPPORT DE RECHERCHE PRÉLIMINAIRE

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

N° d'enregistrement
national

FA 679357
FR 0650506

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		
A	PATENT ABSTRACTS OF JAPAN vol. 2003, no. 12, 5 décembre 2003 (2003-12-05) & JP 2006 024140 A (SONY CORP), 26 janvier 2006 (2006-01-26) * abrégé *	1-10	G06F7/58 H04L9/28
A	US 2002/051534 A1 (MATCHETT NOEL D ET AL) 2 mai 2002 (2002-05-02) * figures 1,3 *	1-10	
A	WO 01/13218 A (SIEMENS AKTIENGESELLSCHAFT; HESS, ERWIN; SERF, PASCALE) 22 février 2001 (2001-02-22) * abrégé *	1-10	
			DOMAINES TECHNIQUES RECHERCHÉS (IPC)
			G06F H04L
Date d'achèvement de la recherche		Examineur	
25 septembre 2006		Pfab, Stefan	
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 0650506 FA 679357

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 **25-09-2006**

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
JP 2006024140 A	26-01-2006	AUCUN	
US 2002051534 A1	02-05-2002	AUCUN	
WO 0113218 A	22-02-2001	CA 2381937 A1	22-02-2001
		EP 1222527 A1	17-07-2002
		JP 2003507761 T	25-02-2003