(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
16 août 2007 (16.08.2007)

PCT

(10) Numéro de publication internationale
WO 2007/090961 A1

(51) Classification internationale des brevets :
H04L 9/06 (2006.01)

(21) Numéro de la demande internationale :
PCT/FR2007/000222

(22) Date de dépôt international : 7 février 2007 (07.02.2007)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
0601135 8 février 2006 (08.02.2006) FR

(71) Déposant *(pour tous les États désignés sauf US)* : **SAGEM DEFENSE SECURITE** [FR/FR]; Le Ponant de Paris, 27, rue Leblanc, F-75015 Paris (FR).

(72) Inventeurs; et

(75) Inventeurs/Déposants *(pour US seulement)* : **CHABANNE, Hervé** [FR/FR]; Sagem Défense Sécurité, Le Ponant de Paris, 27, rue Leblanc, F-75015 Paris (FR). **BRINGER, Julien** [FR/FR]; Sagem Défense Sécurité, Le Ponant de Paris, 27, rue Leblanc, F-75015 Paris (FR). **DOTTAX, Emmanuelle** [FR/FR]; Sagem Défense Sécurité, Le Ponant de Paris, 27, rue Leblanc, F-75015 Paris (FR).

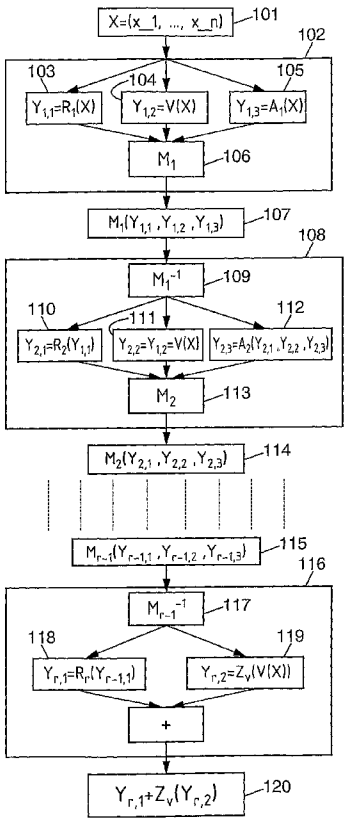
(74) Mandataires : **LOISEL, Bertrand** etc.; Cabinet Plasseraud, 52, rue de la Victoire, F-75440 Paris Cedex 09 (FR).

(81) États désignés *(sauf indication contraire, pour tout titre de protection nationale disponible)* : AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, 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, LV, LY, MA, MD, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU,

[Suite sur la page suivante]

(54) **Title:** PROTECTION OF A CRYPTOGRAPHIC ALGORITHM

(54) **Titre :** PROTECTION D'UN ALGORITHME CRYPTOGRAPHIQUE



(57) Abstract: An algorithm includes a first and a second cryptographic operation. A first operational system (102) is applied to an initial data block and a first intermediate data block is obtained, said first operational system corresponding to a combination of the first cryptographic operation (103), a first random operation (104) which provides a determined value with a defined probability value, a second random operation (105), and a bijective operation (106). Next, a second operational system (116) is applied to the intermediate data block and a second intermediate data block is obtained, said second operational system corresponding to a combination of the inverse operation (117) to the bijective operation of the previous operational system, the second cryptographic operation (118), and an operation which provides the zero value for a value associated with said determined value (119). The application of the first and second operational systems is repeated N times, N being determined as a function of the probability value, and the encrypted data block is determined on the basis of the second intermediate data blocks, as a function of the probability value.

(57) Abrégé : Un algorithme inclut une première et une deuxième opération cryptographique. On applique un premier système opératoire (102) sur un bloc de données initial et on obtient un premier bloc de données intermédiaire, ledit premier système opératoire correspondant à une combinaison de la première opération cryptographique (103), une première opération aléatoire (104) qui fournit une valeur déterminée avec une valeur de probabilité définie, une seconde opération aléatoire (105), et une opération bijective (106). Puis, on applique un deuxième système opératoire (116) sur le bloc de données intermédiaire et on obtient un deuxième bloc de données intermédiaire, ledit deuxième système opératoire correspondant à une combinaison de l'opération inverse (117) de l'opération bijective du système opératoire précédent, la deuxième opération cryptographique (118), et une opération qui fournit la valeur nulle pour une valeur associée à ladite valeur déterminée (119). On répète l'application des premier et deuxième systèmes opératoires N fois, N étant déterminé en fonction de la valeur de probabilité, et on détermine le bloc de données crypté à partir du ou des deuxièmes blocs de données intermédiaires, en fonction de la valeur de probabilité.

WO 2007/090961 A1

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, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Déclaration en vertu de la règle 4.17 :

— *relative à la qualité d'inventeur (règle 4.17.iv))*

Publiée :

— *avec rapport de recherche internationale*

En ce qui concerne les codes à deux lettres et autres abréviations, se référer aux "Notes explicatives relatives aux codes et abréviations" figurant au début de chaque numéro ordinaire de la Gazette du PCT.