



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

(21) Numéro de la demande internationale :

PCT/FR2011/052602

(22) Date de dépôt international :

8 novembre 2011 (08.11.2011)

(25) Langue de dépôt :

français

(26) Langue de publication :

français

(30) Données relatives à la priorité :

1059208 8 novembre 2010 (08.11.2010) FR

(71) Déposant (pour tous les États désignés sauf US) :
MORPHO [FR/FR]; 27, rue Leblanc, F-75015 Paris (FR).

(72) Inventeurs; et

(75) Inventeurs/Déposants (pour US seulement) :
CHABANNE, Hervé [FR/FR]; c/o Morpho, 27, rue Leblanc, F-75015 Paris (FR). **BRINGER, Julien**

[FR/FR]; c/o Morpho, 27, rue Leblanc, F-75015 Paris (FR). **LE, Thanh, Ha** [VN/FR]; c/o Morpho, 27, rue Leblanc, F-75015 Paris (FR).

(74) Mandataires : **WLODARCZYK, Lukasz** et al.; 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, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, 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, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, 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,

[Suite sur la page suivante]

(54) Title : PROTECTION AGAINST PASSIVE SNIFFING

(54) Titre : PROTECTION CONTRE LES ECOUTES PASSIVES

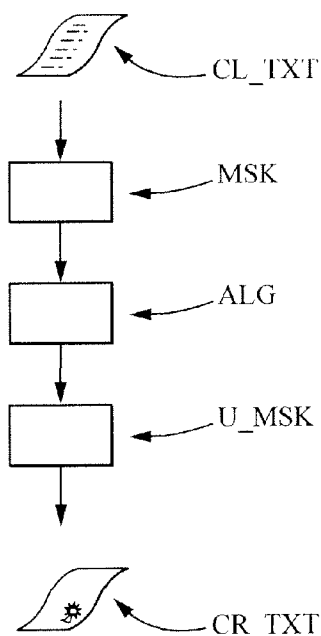


FIG. 1

(57) Abstract : The invention relates in particular to a method for securing the execution of a cryptographic algorithm (ALG) against passive sniffing, the method implementing masking (MSK) of data processed by the cryptographic algorithm. The masking (MSK) of said data includes a linear encoding step such as $x' = x.L + c$, in which x is the data to be masked, x' is the corresponding masked data, c is a code word included in a linear code C , and L is a matrix made up of linearly independent vectors not included in the linear code C . The invention also relates to a device (SC) implementing such a method.

(57) Abrégé : L'invention se rapporte notamment à un procédé de sécurisation de l'exécution d'un algorithme cryptographique (ALG) contre des écoutes passives, le procédé mettant en œuvre un masquage (MSK) de données traitées par l'algorithme cryptographique. Le masquage (MSK) desdites données comprend une étape de codage linéaire de type $x' = x.L + c$, x étant une donnée à masquer, x' étant une donnée masquée correspondante, c étant un mot de code compris dans un code linéaire C , et L étant une matrice composée de vecteurs linéairement indépendants non compris dans le code linéaire C . L'invention concerne également un dispositif (SC) mettant en œuvre un tel procédé.



GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), européen (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Déclarations en vertu de la règle 4.17 :

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

Publiée :

— *avec rapport de recherche internationale (Art. 21(3))*