

(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
19 mai 2011 (19.05.2011)

PCT

(10) Numéro de publication internationale
WO 2011/057991 A1

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

DANGER, Jean-Luc [FR/FR]; 21, Avenue de la Concorde, F-92160 Antony (FR).

(21) Numéro de la demande internationale :
PCT/EP2010/067064

(74) Mandataires : DUDOUIT, Isabelle et al.; Immeuble Visium, 22, Avenue Aristide Briand, F-94117 Arcueil (FR).

(22) Date de dépôt international :
8 novembre 2010 (08.11.2010)

(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, RO, RS, RU, 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.

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
0958030 13 novembre 2009 (13.11.2009) FR

(71) Déposant (pour tous les États désignés sauf US) :
INSTITUT TELECOM - TELECOM PARISTECH
[FR/FR]; 46, rue Barrault, F-75013 Paris (FR).

(72) Inventeurs; et

(75) Inventeurs/Déposants (pour US seulement) : GUILLEY, Sylvain [FR/FR]; 84, rue Bobillot, F-75013 Paris (FR).

(84) États désignés (sauf indication contraire, pour tout titre de protection régionale disponible) : ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ,

[Suite sur la page suivante]

(54) Title : LOW-COMPLEXITY ELECTRONIC CIRCUIT PROTECTED BY CUSTOMIZED MASKING

(54) Titre : CIRCUIT ELECTRONIQUE DE FAIBLE COMPLEXITE PROTEGE PAR MASQUAGE PERSONNALISE

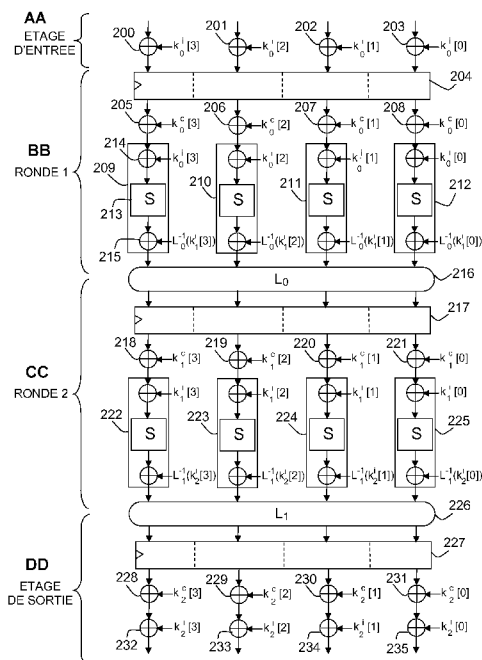


FIG.2

AA ... INPUT STAGE
BB ... ROUND 1
CC ... ROUND 2
DD ... OUTPUT STAGE

(57) Abstract : The invention relates to a masking-protected cryptographic circuit, said circuit comprising a means for encrypting binary words through the use of at least one key k_r^c , a means for applying linear processing (216) and nonlinear processing (226) to said words, and a means for masking said words. The binary words are unmasked (214) upstream from the nonlinear processing through the use of a mask k_r^i and are masked (215) downstream from said processing through the use of a mask k_{r+1}^i , the masks k_r^i and k_{r+1}^i being selected from within a set of masks that are specific to each instance of the circuit.

(57) Abrégé : L'invention a pour objet un circuit de cryptographie protégé par masquage, ledit circuit comportant des moyens pour chiffrer des mots binaires à l'aide d'au moins une clé k_r^c , des moyens pour appliquer des traitements linéaires (216) et des traitements non linéaires (226) auxdits mots et des moyens pour masquer lesdits mots. Les mots binaires sont démasqués (214) en amont des traitements non linéaires en utilisant un masque k_r^i et masqués (215) en aval desdits traitements en utilisant un masque k_{r+1}^i , les masques k_r^i et k_{r+1}^i étant choisis dans un ensemble de masques étant propres à chaque instance du circuit.

WO 2011/057991 A1



TM), européen (AL, AT, BE, BG, CH, CY, CZ, DE, DK, **Publiée :**

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).

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