



(51) Classification internationale des brevets :
G06F 21/02 (2006.01) **G06F 21/00** (2006.01)

(21) Numéro de la demande internationale :
PCT/EP2009/059886

(22) Date de dépôt international :
30 juillet 2009 (30.07.2009)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
0855537 12 août 2008 (12.08.2008) FR

(71) Déposant (pour tous les États désignés sauf US) :
**GROUPE DES ECOLES DES
TELECOMMUNICATIONS - ECOLE NATIONALE
SUPERIEURE DES TELECOMMUNICATIONS**
[FR/FR]; 46, rue Barrault, F-75013 Paris (FR).

(72) Inventeurs; et

(75) Inventeurs/Déposants (pour US seulement) : **DANGER,
Jean-Luc** [FR/FR]; 21, Avenue de la Concorde, F-62160
Antony (FR). **GUILLEY, Sylvain** [FR/FR]; 84, rue
Bobillot, F-75013 Paris (FR). **FLAMENT, Florent** [FR/
FR]; 8, rue Auguste Vitu, F-75015 Paris (FR).

(74) Mandataires : **LUCAS, Laurent** et al.; Immeuble
Visium, 22, 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, 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, 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), eurasién (AM, AZ, BY, KG, KZ, MD, RU, TJ,
TM), européen (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, SE, SI, SK, SM,
TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW,
ML, MR, NE, SN, TD, TG).

Publiée :

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

[Suite sur la page suivante]

(54) Title : METHOD FOR DETECTING ABNORMALITIES IN A CRYPTOGRAPHIC CIRCUIT PROTECTED BY DIFFERENTIAL LOGIC, AND CIRCUIT FOR IMPLEMENTING SAID METHOD

(54) Titre : PROCEDE DE DETECTION D'ANOMALIES DANS UN CIRCUIT DE CRYPTOGRAPHIE PROTEGE PAR LOGIQUE DIFFERENTIELLE ET CIRCUIT METTANT EN OEUVRE UN TEL PROCEDE

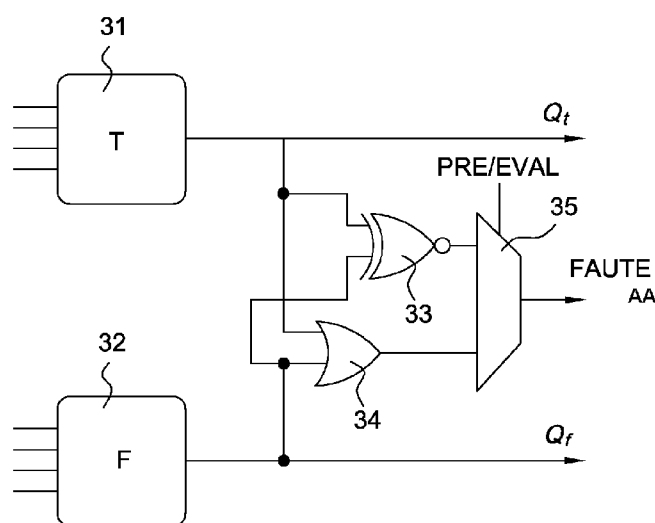


FIG.3

AA ERROR

(57) Abstract : The invention relates to a method for detecting abnormalities in a circuit protected by differential logic and processing logic variables represented by a pair of components (a_i , a_j), a first network of cells (T) carrying out logic functions on the first component of said pairs, a second network of dual cells (F) operating as a complementary logic on the second component, the logic functions being carried out by each pair of cells (T, F) in a preload phase (21) placing the variables in a known state at the cell input, followed by an evaluation phase (22) in which a calculation is carried out by the cells, wherein said method is characterised in that an abnormality is detected by at least one inconsistency state. The invention also relates to a circuit protected by differential logic, comprising means for testing the consistency of the two components of the logic variables during the preload or evaluation phases at the monitored nodes of the circuit.

(57) Abrégé :

[Suite sur la page suivante]



La présente invention a pour objet un procédé de détection d'anomalies dans un circuit protégé par logique différentielle et traitant des variables logiques représentées par un couple de composantes (a_i , a_j), un premier réseau de cellules (T) réalisant des fonctions logiques sur la première composante desdits couples, un deuxième réseau de cellules duales (F) fonctionnant en logique complémentaire sur la deuxième composante, les fonctions logiques étant réalisées par chaque couple de cellules (T, F) en une phase de précharge (21) mettant les variables dans un état connu à l'entrée des cellules suivie d'une phase d'évaluation (22) où un calcul est effectué par les cellules, ledit procédé étant caractérisé en ce qu'une anomalie est détectée par au moins un état non cohérent. L'invention a aussi pour objet un circuit protégé par logique différentielle comportant des moyens pour tester la cohérence entre les deux composantes des variables logiques durant les phases de précharge ou d'évaluation aux nœuds surveillés du circuit.