(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 2 983 156 A1

(12) DEMANDE DE BREVET EUROPEEN

(43) Date de publication:
10.02.2016 Bulletin 2016/06

(51) Int Cl.:
G09C 1/00 *(2006.01)* ***H04L 9/00*** *(2006.01)*

(21) Numéro de dépôt: **14306247.9**

(22) Date de dépôt: **06.08.2014**

(84) Etats contractants désignés:
AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO RS SE SI SK SM TR
Etats d'extension désignés:
BA ME

(71) Demandeur: **Secure-IC SAS**
35000 Rennes (FR)

(72) Inventeurs:
- **Guilley, Sylvain**
  75013 Paris (FR)
- **Porteboeuf, Thibault**
  75013 Paris (FR)
- **Danger, Jean-Luc**
  92160 Antony (FR)

(74) Mandataire: **Hnich-Gasri, Naïma et al**
Marks & Clerk France
Immeuble Visium
22, avenue Aristide Briand
94117 Arcueil Cedex (FR)

(54) Système et procédé de protection de circuit

(57) L'invention propose un procédé de protection d'un circuit booléen associé à une description structurelle du circuit comprenant des variables booléennes élémentaires, chacune représentée par un bit, le procédé comprenant les étapes consistant à:
- sélectionner un ensemble de k variables booléennes élémentaires du circuit en fonction de critères de sélection prédéfinis,
- construire une variable x représentée par k bits par concaténation des k variables sélectionnées, selon un ordre choisi,
- déterminer un code binaire C, comprenant un ensemble de mots de code et appartenant à un espace vectoriel donné, et le code supplémentaire D du code binaire C, en fonction d'une condition portant sur la distance duale du code supplémentaire D, le code binaire C ayant une longueur n et une taille 2^k, où k désigne le nombre de bits représentant la variable x;
- substituer la variable x dans la description structurelle du circuit booléen par une variable protégée z représentée par n bits de telle sorte que :
- toute opération d'écriture sur la variable x dans le circuit soit substituée par une opération d'écriture sur la variable z, la variable z étant générée par ajout de la variable x encodée par ledit code C à un vecteur de bit d'aléas y encodé par le code supplémentaire D, et
- toute opération de lecture de la variable x dans le circuit soit substituée par une opération de lecture de la valeur de la variable protégée z et d'une opération de décodage de ladite valeur lue de la variable protégée z en utilisant une matrice de décodage J de taille $(n \times k)$ déterminée à partir du code binaire C et du code supplémentaire D du code binaire C.

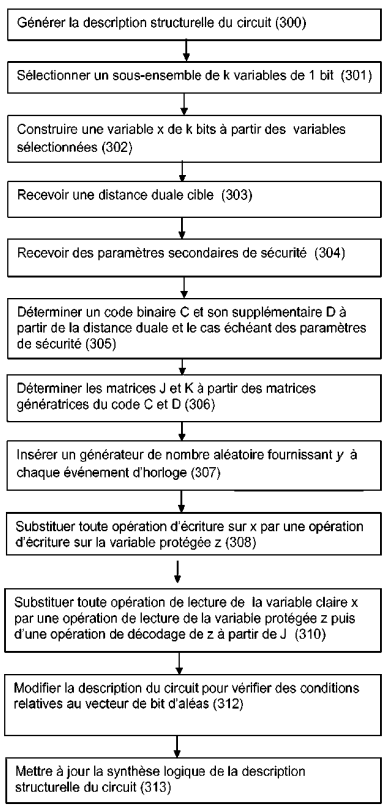

FIGURE 3

EP 2 983 156 A1