



(51) Classification internationale des brevets :
G01R 31/317 (2006.01) G06F 21/00 (2006.01)

(21) Numéro de la demande internationale :
PCT/EP2011/050234

(22) Date de dépôt international :
10 janvier 2011 (10.01.2011)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
10 50297 18 janvier 2010 (18.01.2010) FR

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

(72) Inventeur; et

(75) Inventeur/Déposant (pour US seulement) : DANGER,
Jean-Luc [FR/FR]; 21, Avenue de la Concorde, F-92160
Antony (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, 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, GM, KE, LR, LS, MW, MZ, NA, 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).

Publiée :

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

[Suite sur la page suivante]

(54) Title : INTEGRATED SILICON CIRCUIT COMPRISING A PHYSICALLY NON-REPRODUCIBLE FUNCTION, AND METHOD AND SYSTEM FOR TESTING SUCH A CIRCUIT

(54) Titre : CIRCUIT INTEGRE EN SILICIUM COMPORTANT UNE FONCTION PHYSIQUEMENT NON COPIABLE, PROCEDE ET SYSTEME DE TEST D'UN TEL CIRCUIT

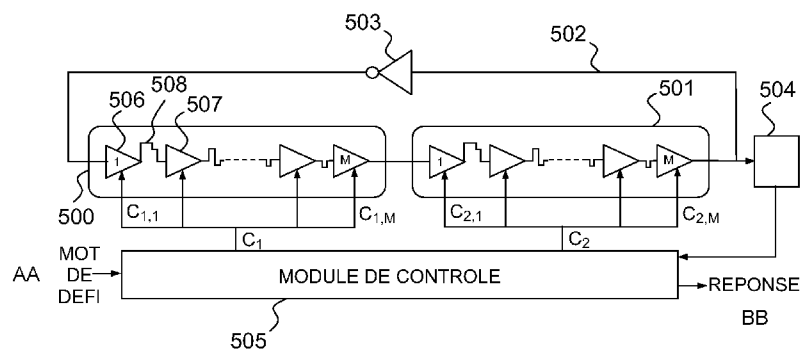


FIG.5

AA CHALLENGE WORD
505 CONTROL MODULE
BB RESPONSE

(57) Abstract : The invention relates to an integrated silicon circuit that comprises a physically non-reproducible LPUF function enabling the generation of a signature specific to said circuit. Said function comprises a ring oscillator consisting of a loop (502) through which a signal e flows, said loop consisting of N topologically identical delay channels (500, 501), connected to each other in series and an inversion gate (503), wherein a delay channel (500, 501) consists of M lag elements (506, 507) connected to each other in series. The function also comprises a control module (505) that generates N control words (C1, C2), said words being used for configuring the value of the lag inserted by the delay channels on the signal e flowing therethrough. A measuring module (504) measures the signal frequency at the output of the last delay channel (501) after updating the control words, and means for deriving the measurements of the frequencies of the bits forming the circuit signature. The invention also relates to a method and system for testing such circuits.

(57) Abrégé :

[Suite sur la page suivante]



L'invention a pour objet un circuit intégré en silicium comportant une fonction physiquement non copiable LPUF permettant la génération d'une signature propre audit circuit. Ladite fonction comporte un oscillateur en anneau composé d'une boucle (502) parcourue par un signal e , ladite boucle étant formée de N chaînes de délais (500, 501) topologiquement identiques, connectées en série les unes aux autres et d'une porte d'inversion (503), une chaîne de délais (500, 501) étant composée de M éléments de retard (506, 507) connectés en série les uns aux autres. La fonction comporte aussi un module de contrôle (505) générant N mots de contrôle (C_1 , C_2), lesdits mots étant utilisés pour configurer la valeur des retards introduits par les chaînes de délais sur le signal e les parcourant. Un module de mesure (504) mesure la fréquence du signal en sortie de la dernière chaîne de délais (501) après la mise à jour des mots de contrôle, et des moyens permettent de déduire des mesures de fréquence les bits composant la signature du circuit. L'invention a aussi pour objets un procédé et un système de test de tels circuits.