



(12)

CERERE DE BREVET DE INVENȚIE

(21) Nr. cerere: **a 2021 00020**

(22) Data de depozit: **22/01/2021**

(41) Data publicării cererii:
29/07/2022 BOPI nr. **7/2022**

(71) Solicitant:
• **UNIVERSITATEA TEHNICĂ "GHEORGHE
ASACHI" DIN IAȘI, STR. PROF. DR. DOC.
DIMITRIE MANGERON NR. 67, IAȘI, IS, RO**

(72) Inventatori:
• **ANDRIESEI CRISTIAN,
BD.ROMAN MUȘAT, BL.38, AP.101,
ROMAN, NT, RO**

(54) **IMPLEMENTARE CMOS PENTRU FUNCȚIE NECLONABILĂ FIZIC (PUF)**

(57) Rezumat:

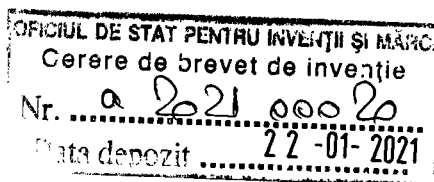
Invenția se referă la o implementare hardware în tehnologie CMOS a unei structuri PUF (physically unclonable functions) care asigură unicitatea secvenței binare de răspuns la o secvență binară de test, aplicată la intrare. Structura PUF, conform invenției, constă într-un banc de M varactori, unde M corespunde lungimii secvențelor de test și răspuns, fiecare varactor fiind implementat cu un tranzistor NMOS având terminalul grilă conectat la pinul extern de test și cu

terminalele drenă și sursă conectate împreună la masa circuitului, lățimea fiecărui tranzistor iW_1 fiind proporțională cu lățimea primului tranzistor din banc, W_1 , iar lungimea canalului L_1 fiind identică la toate tranzistoarele, unde i reprezintă indicele varactorului în banc și ia valori de la 1 la M.

Revendicări: 2
Figuri: 3



45



Implementare CMOS pentru funcție neclonabilă fizic (PUF)

Invenția **se referă la** o implementare hardware în tehnologie CMOS a unei structuri PUF care permite identificarea unică pe baza secvenței *response* furnizată la aplicarea unei secvențe *challenge*, ambele cu reprezentare pe M biți.

Deși nu există o definiție standard iar definițiile folosite de ingineri și matematicieni pot diferi, funcțiile neclonabile fizic, denumite în limba engleză PUF (*physically unclonable functions*), se referă la o clasă distinctă de implementări fizice la care perechea {semnal de intrare, semnal de ieșire} este unică pentru oricare implementare fizică distinctă a aceluiași prototip. Semnalul de intrare poate avea semnificații fizice diferite, cum ar fi parametri fizici ce țin strict de tehnologia de implementare a tranzistoarelor (de obicei CMOS), mediu optic, câmp electromagnetic (radiofrecvență) și magnetism [1]. Asemenea implementări exploatează dispersia tehnologică aferentă unei implementări fizice. Ca exemplu, din cauza toleranțelor aferente implementării fizice și dispersiei tehnologice, un lot de câteva mii de circuite integrate (fie și procesoare) produse de o fabrică pentru o aceeași schemă electronică trimisă de proiectant (*layout*) înseamnă tot atâtea variante diferite din perspectiva unor parametri de performanță, oricare două circuite integrate nefiind perfect identice. Deși dispersia tehnologică este impedimentul major în proiectarea unor circuite

integrate identice pentru un același produs vandabil, aceeași dispersie tehnologică este utilă pentru a identifica, similar unei amprente unice, chip-urile proprii cu scopul împiedicării contrafacerii, mai precis distingerea circuitelor integrate proprii de alte copii ale produsului original (clone) intrate în circuitul economic mondial (care afectează atât volumul vânzărilor produselor originale cât și brandul original prin calitatea mai slabă a produselor contrafăcute care deformează părerea clienților despre calitatea produselor proprii). Problema tehnică majoră întâmpinată la dezvoltarea unei arhitecturi PUF o constituie identificarea unui mod eficient de exploatare a dispersiei tehnologice și/sau fenomenului fizic implicat, pentru o implementare particulară.

Deși soluții împotriva copierii ilegale a circuitelor integrate erau brevetate încă din 1988 [2], arhitecturile de tip PUF își au începutul în jurul anului 2000, odată cu dezvoltarea unui formalism matematic și mai ales generalizare a conceptului pe fondul posibilității exploatării mai multor fenomene fizice distincte. Astfel, prima soluție de identificare a circuitelor integrate electronice în scop de protecție a fost propusă spre brevetare în anul 1999, cu brevet acordat în 2000 [3], redepus spre brevetare în variantă îmbunătățită în anul 2002 și acceptat în 2008 [4]. O soluție tehnică alternativă care face uz de imperfecțiunile tehnologiei CMOS a fost publicată de același autor în 2000 [5]. În paralel, în anul 2001 compania Hitachi ULSI Systems Co., Ltd. propune spre brevetare o arhitectură utilă pentru identificarea circuitelor integrate, implementată la nivel de poartă logică [6]. În aceeași perioadă se derulează și prima cercetare de doctorat [7], [8] focalizată pe implementarea fizică a funcțiilor greu inversabile (*one-way functions*), adică ușor de calculat ca și răspuns ($Y=f(X)$) pentru o valoare de intrare (x) dar greu (ideal imposibil) de calculat valoarea X de intrare a funcției cunoscând ieșirea Y a acesteia, cu aplicabilitate directă în criptografie. Implementarea practică a exploatat mediul optic ca și modalitate de protecție criptografică, cu aplicabilitate la autentificare. Primul articol științific care a lansat ideea exploatării dispersiei la tehnologia CMOS în scopuri de securitate a fost

43

publicat în 2002, moment care marchează începutul unui nou domeniu de interes la nivel global, dedicat în întregime conceptului de PUF [9]. Soluția propusă de PUF se bazează pe exploatarea întârzierii diferite a căii de semnal intrare - ieșire funcție de secvența aplicată la intrare (denumită *challenge*) pentru un același circuit și diferită, pentru același *challenge*, la un alt circuit fabricat cu schema internă identică. La acest moment există peste 300 brevete/aplicații de brevet și peste 600 de articole indexate la IEEE [10] care propun arhitecturi de PUF ori înglobează asemenea structuri în aplicații de securitate, acestea ajungând să fie văzute ca soluție chiar și pentru protocoalele RFID [11], unde interesează implementările digitale (cu porți logice) pentru PUF.

Dincolo de avantajele evidente din perspectiva securității, asigurând unicitatea răspunsului, există și dezavantaje asociate acestor soluții:

- conceptul de PUF fiind gândit pentru identificarea chip-urilor, extinderea acestuia la alte clase de aplicații de securitate poate introduce vulnerabilitate;
- implementat inițial la nivel de tranzistor, integrat fiind în chiar structura chip-ului, s-a încercat translarea conceptului de PUF la implementări FPGA, implementându-se scheme cu porți logice care, pe fondul dezvoltării tehnologiei și studiilor raportate în literatură, au devenit vulnerabile la analize statistice și *machine learning*;
- din considerente de automatizare a procesului de proiectare și mai degrabă din perspectiva implementărilor FPGA, este necesară construirea unui setup experimental care să testeze multiple secvențe de biți (*challenge*) pentru construirea bazei de date aferentă perechii *challenge-response*, această constrângere vizând mai degrabă implementările digitale, nu și alte tipuri de implementări fizice (cum ar fi cele RF) ;
- implementările în tehnologie CMOS, fiind implementate cu tranzistoare, manifestă o dependență puternică cu temperatura, ceea ce conduce la

42

eronarea perechii *challenge-response* măsurată inițial odată cu modificarea temperaturii, mai precis un același PUF implementat fizic putând răspunde cu două sau mai multe secvențe *response* distincte pentru aceeași secvență *challenge* (motiv pentru care multe structuri PUF au circuite de corecție a erorilor, complicând structura)

Pe fondul numărului mare de referințe, a existenței unor clase distincte de implementări fizice, precum și a unor aplicații distincte de securitate care pot fi vizate (autenticitatea unui chip, protocoale RFID, generatoare de chei aleatoare, etc), respectiv interpătrunderii cu cercetarea efectuată de matematicieni care lucrează doar la nivel matematic fără să aibă contact cu implementarea fizică, acest domeniu stă adesea sub semnul confuziei. Din această perspectivă, soluția propusă în acest brevet vizează o implementare fizică distinctă de PUF, implicând o modalitate proprie de evaluare a perechii *challenge-response* mai sigură din perspectiva securității doar dacă este înglobată ca atare într-un sistem, fără a se încerca adaptarea la o altă perspectivă de implementare.

Problema tehnică pe care o rezolvă invenția este implementarea unei funcționalități de tip PUF în tehnologie CMOS care să manifeste o dependență mai scăzută cu temperatura și să îngreuneze procesul de clonare sau analiză statistică.

Structura PUF, conform invenției, constă dintr-un banc de M varactori, unde M corespunde lungimii secvențelor *challenge* și *response*, fiecare varactor fiind implementat cu un tranzistor NMOS având terminalul grilă conectat la pinul extern de test și cu terminalele drenă și sursă conectate împreună la masa circuitului, lățimea fiecărui tranzistor $i \cdot W_1$ fiind proporțională cu lățimea primului tranzistor din banc W_1 iar lungimea canalului L_1 identică la toate tranzistoarele, unde i reprezintă indexul varactorului din banc și ia valori de la 1 la M .

41

Invenția poate fi exploatată industrial pentru asigurarea proprietății de autenticitate a unui produs sau echipament.

Implementarea PUF, conform invenției, prezintă următoarele avantaje:

- făcând uz de capacitățile parazite ale tranzistorului MOSFET și nu de transconductanța g_m a acestuia, implementarea prezintă o dependență cu temperatura mai scăzută față de alte implementări digitale raportate până acum, ceea ce asigură fiabilitate crescută și probabilitate mai mică de eronare a unei perechi challenge-response pe fondul deviației cu temperatura;
- implementarea face uz de frecvențe ridicate de lucru, necesitând astfel expertiză tehnică și un setup de test care limitează mai ales probabilitatea de analiză statistică automată și atacurile care fac uz de *machine learning*;
- metoda de testare asociată acestei arhitecturi impune păstrarea circuitului PUF de test la compania producătoare, care, fiind distinct de alte implementări PUF identice nu poate fi clonat și, pe de altă parte, permite reluarea testelor cu același setup de test inițial și în aceleași condiții de test.

Se dă, în continuare, un exemplu de aplicare a invenției, în legătură cu Figurile 1-3 a implementării PUF propuse, care reprezintă :

- Figura 1, celulă PUF elementară;
- Figura 2, structura PUF generalizată (banc de varactori);
- Figura 3, metoda de testare a unei celule PUF elementare.

Celula PUF elementară 1, conform invenției, este constituită dintr-un tranzistor NMOS 2 având terminalul grilă 21 conectat galvanic la pinul extern de test 3 și terminalele drenă 22 și sursă 23 conectate galvanic împreună masa

40

(ground) 4 a circuitului, așa cum este ilustrat în Figura 1. Conform teoriei circuitelor, această topologie implementează un varactor [12], cu aplicabilitate mai ales în implementarea oscilatoarelor RF [13], adică un condensator a cărui capacitate parazită echivalentă (măsurată între terminalul grilă 21 și masa circuitului 4) este dependentă neliniar de tensiunea de polarizare (de curent continuu) aplicată pe grila 21 a tranzistorului, mai precis la pinul extern 3. Pentru o asemenea implementare capacitatea varactorului are valoarea aproximativă $W_1 \cdot L_1 \cdot C_{ox}$ când tensiunea V_3 este nulă (asimilată valorii logice '0' pentru bitul *challenge* aplicat la intrarea 3 de test), respectiv o valoare C_{max} când tensiunea depășește cu mult tensiunea de prag V_{th} a tranzistorului 2 (valoare ce poate fi asimilată valorii logice '1' pentru bitul *challenge* aplicat la intrarea 3 de test). Cu această asociere, o asemenea arhitectură poate fi utilizată ca celulă PUF elementară, furnizând răspunsuri diferite funcție de tensiunea de test. În cazul cel mai simplu de test, se poate testa o celulă PUF elementară doar cu aplicarea bitului '0'. Funcționalitatea specifică unui PUF se datorează exclusiv toleranțelor de implementare a layout-ului tranzistorului 2, acestea generând variații mici (dar sesizabile) ale capacității parazite echivalente. W , L și C_{ox} reprezintă lățimea și lungimea canalului tranzistorului, respectiv capacitatea echivalentă a stratului de oxid (SiO_2), W_1 și L_1 fiind, conform acestei invenții, valorile implicite stabilite pentru prima celulă PUF elementară (și singurii parametri de proiectare).

Implementarea PUF generalizată 5, conform invenției, constă din implementarea într-un singur chip a unui număr M de celule PUF elementare similare cu cea reprezentată în Figura 1, numerotate 5-1, 5-2, ... 5-M. Indexul fiecărei celule reprezintă și factor de multiplicare pentru lățimea canalului W , tranzistorul aferent ultimei celule 5-M având o arie de M ori mai mare decât a tranzistorului primei celule 5-1, ca în Figura 2. În acest fel se asigură o capacitate a varactorului mai mare, frecvență de test tot mai mică (baleindu-se un domeniu mai mare de frecvențe testate) și asigură o dispersie tehnologică mai mare. Dimensiunea M este liber aleasă de producător, o dimensiune mai mare permițând

o secvență de test (*challenge*) mai lungă deci și probabilitate mai mare de a individualiza unic oricare două structuri PUF identice fizic (simultan cu îngreunarea analizei statistice). Pinii de test sunt disponibili extern iar masa circuitului (*ground*) este comună. Testarea acestei implementări generalizate se poate face fie individual pentru fiecare celulă (cu avantajul unui gabarit mai mic pentru circuitul de test) fie pentru toate celulele simultan (cu dezavantajul unui gabarit mare pentru circuitul de test).

Metoda de test pentru testarea celulei PUF elementare, conform invenției, constă din parcurgerea următorilor pași, așa cum este ilustrat în Figura 3:

1. Se implementează o celulă PUF elementară **PUF 1** (test), identică din perspectiva datelor de proiectare cu celula PUF care va fi asociată produsului comercial, **PUF 2** (produs fizic). Celula de test va fi păstrată de compania producătoare și utilizată ca celulă PUF de referință pentru testarea tuturor celulelor PUF identice fizic (adică W_1 și L_1 identice) fabricate și atașate fizic produselor lansate pe piață. Din cauza toleranțelor aferente implementării fizice, capacitatea varactorului aferent produsului comercial, notat C_{var2} , va fi mai mare sau mai mică față de C_{var1} al celulei PUF de test, dar niciodată egale, pentru aceeași tensiune $V_{challenge}$ aplicată pe grilele ambelor tranzistoare.

2. Se aplică $V_{challenge} = '0'$ (echivalent cu 0V).

3. Se cuplează consecutiv, la pinul de test al ambelor celule PUF, o bobină de test cu inductanța asociată L_{test} . Fiind implementată SMD sau în tehnologie microstrip pentru a funcționa la frecvențe de ordinul GHz, valoarea exactă a acestei inductanțe nu este necesară a fi prestabilită, de interes fiind valoarea frecvenței de rezonanță pe care o are la conectarea în paralel cu varactorul celulei PUF, notată f_{01} și respectiv f_{02} . Ca și **PUF 1**, această bobină va fi păstrată de compania producătoare pentru a fi folosită la testarea curentă sau ulterioară a celulelor PUF atașate unor produse comerciale. Bobina este conectată la celula PUF prin intermediul unui condensator de decuplare C_{dec} .

4. Se măsoară cu un analizor de spectru frecvențele f_{01} și respectiv f_{02} .

38

5. Dacă f_{02} este mai mare ca valoare decât f_{01} se decide că bitul *response* pentru **PUF 2** este '1', în caz contrar este '0'.

6. Se aplică $V_{\text{challenge}} = '1'$ (echivalent cu tensiune mult mai mare decât V_{th}) și se reiau pașii 3-5.

7. Perechile *challenge – response* se memorează și păstrează într-o bază de date internă, pentru eventuale teste ulterioare.

REFERINȚE

- [1] *A PUF taxonomy*, Thomas McGrath et al., Applied physics reviews, Vol. 6, 011303 (2019)
- [2] *Method and apparatus for securing integrated circuits from unauthorized copying and use*, Faik S. Ozdemir et al., US Patent application, 4 766 516, 1988
- [3] *System for providing an integrated circuit with a unique identification*, Keith Lofstrom, US Patent application, 6 161 213, 2000
- [4] *IC Identification Circuit using Device Mismatch*, Keith Lofstrom et al., IEEE International Solid-State Circuits Conference (ISSCC), 2000
- [5] *System and method for providing an integrated circuit with a unique identification*, Keith Lofstrom, US Reissued Patent, US RE40,188 E, 2008
- [6] *Method for identifying semiconductor integrated circuit device, method for manufacturing semiconductor integrated circuit device, semiconductor integrated circuit device and semiconductor chip*, Masaya Muranaka, Hitachi Ltd., European Patent Application, EP 1 341 214 A1, 2001
- [7] *Physical One-Way Functions*, Pappu Srinivasa Ravikanth, PhD Thesis, Massachusetts Institute of Technology, Martie 2001
- [8] *Physical One-Way Functions*, Ravikanth Pappu et al., Science 297, 2026 (2002)
- [9] Massachusetts Institute of Technology, *Silicon Physical Random Functions*, Blaise Gassend et al., Proceedings of the 9th ACM conference on Computer and communications security (CCS'02), 2002
- [10] www.ieeexplore.org

- [11] *Security and Privacy of PUF-Based RFID Systems*, Ferucio Laurențiu Țiplea, Cristian Andriesei, Cristian Hristea, IntechOpen, pp. 1-23, 2020, DOI: 10.5772/intechopen.94018
- [12] *Digital Integrated Circuits*, Jan M. Rabaey, Prentice Hall (1st edition), 1995
- [13] *Design of CMOS Phase-Locked Loops*, Behzad Razavi, Cambridge University Press, 2020

REVENDICĂRI

34

1. Metodă de test, **caracterizată prin aceea că**, pentru testarea unei celule PUF elementare, metoda constă din parcurgerea următorilor pași:

1.1 Se implementează o celulă PUF elementară **PUF 1** (test), identică din perspectiva datelor de proiectare cu celula PUF care va fi asociată produsului comercial, **PUF 2** (produs fizic). Celula de test va fi păstrată de compania producătoare și utilizată ca celulă PUF de referință pentru testarea tuturor celulelor PUF identice fizic (adică W_1 și L_1 identice) fabricate și atașate fizic produselor lansate pe piață. Din cauza toleranțelor aferente implementării fizice, capacitatea varactorului aferent produsului comercial, notat C_{var2} , va fi mai mare sau mai mică față de C_{var1} al celulei PUF de test, dar niciodată egale, pentru aceeași tensiune $V_{challenge}$ aplicată pe grilele ambelor tranzistoare.

1.2 Se aplică $V_{challenge} = '0'$ (echivalent cu 0V).

1.3 Se cuplează consecutiv, la pinul de test al ambelor celule PUF, o bobină de test cu inductanța asociată L_{test} . Fiind implementată SMD sau în tehnologie microstrip pentru a funcționa la frecvențe de ordinul GHz, valoarea exactă a acestei inductanțe nu este necesară a fi prestabilită, de interes fiind valoarea frecvenței de rezonanță pe care o are la conectarea în paralel cu varactorul celulei PUF, notată f_{01} și respectiv f_{02} . Ca și **PUF 1**, această bobină va fi păstrată de compania producătoare pentru a fi folosită la testarea curentă sau ulterioară a celulelor PUF atașate unor produse comerciale.

1.4 Se măsoară cu un analizor de spectru frecvențele f_{01} și respectiv f_{02} .

1.5 Dacă f_{02} este mai mare ca valoare decât f_{01} se decide că bitul *response* pentru **PUF 2** este '1', în caz contrar este '0'.

1.6 Se aplică $V_{challenge} = '1'$ (echivalent cu tensiune mult mai mare decât V_{th}) și se reiau pașii 3-5.

1.7 Perechile *challenge* – *response* se memorează și păstrează într-o bază de date internă, pentru eventuale teste ulterioare.

2. Structură PUF în tehnologie CMOS, **caracterizată prin aceea că**, pentru asigurarea unicității secvenței binare răspuns (*response*) la o secvență binară de test aplicată la intrare (*challenge*), constă dintr-un banc **5** de M varactori notați **5-1**, **5-2**, ... **5-M** și implementați fiecare cu tranzistor NMOS **2** având terminalul grilă **21** conectat la pinul extern **2** iar terminalele drenă **22** și sursă **23** conectate galvanic împreună la masa circuitului **4**, lungimea canalului L_1 fiind identică la toate tranzistoarele iar lățimea tranzistorului este $i \cdot W_1$, unde i este indexul i al varactorului din banc iar W_1 lățimea tranzistorului primului varactor din banc.

35

FIGURI

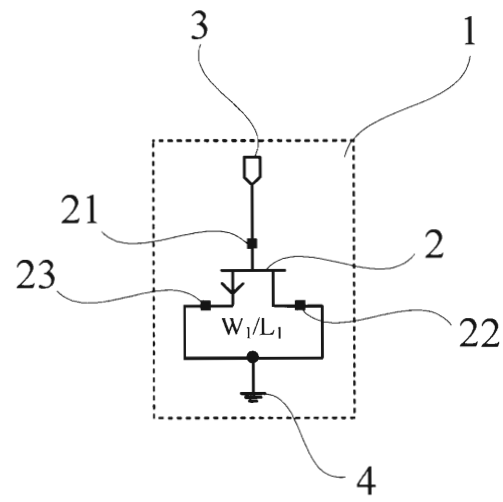


Figura 1

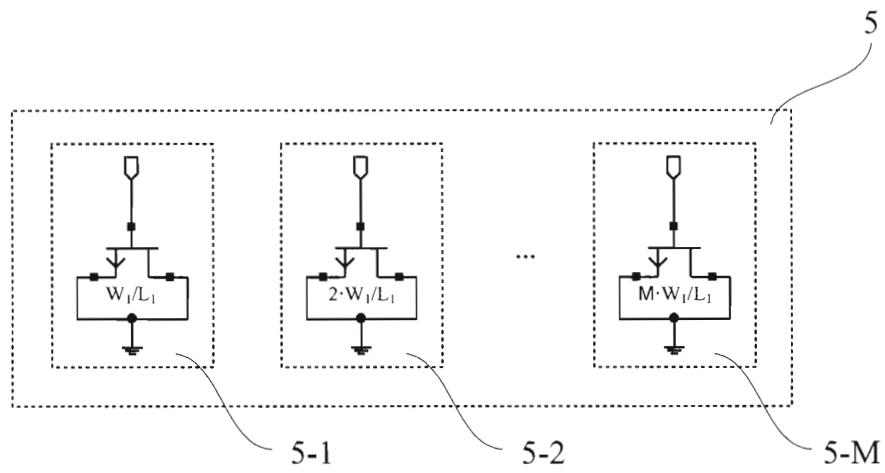


Figura 2

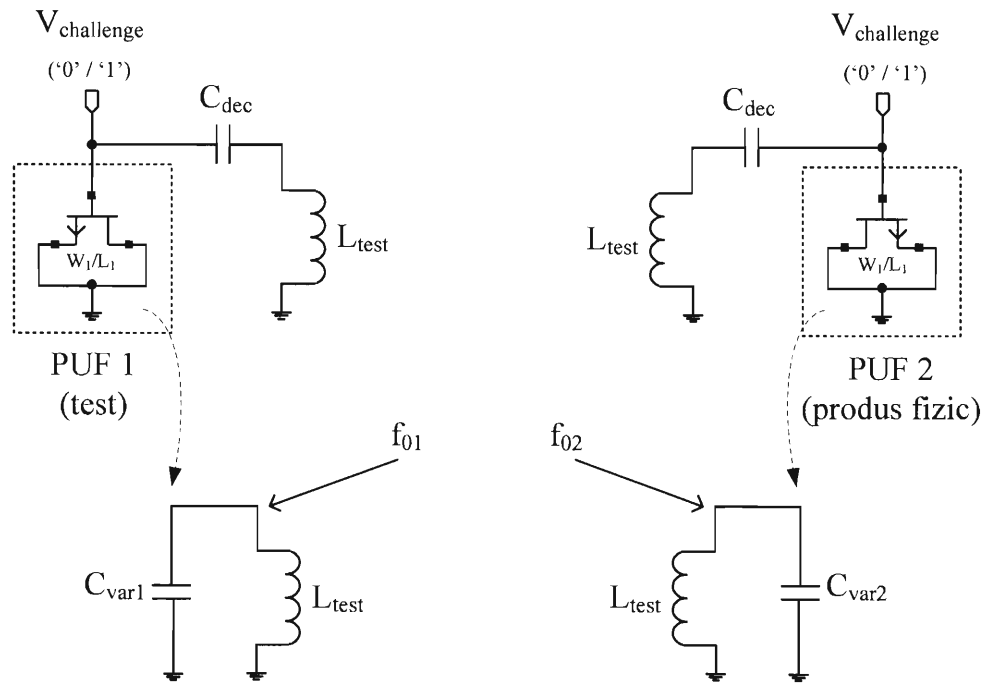


Figura 3