ROMÂNIA

(19) OFICIUL DE STAT
PENTRU INVENŢII ŞI MĂRCI
Bucureşti

(11) **RO 135861 A2**
(51) **Int.Cl.**
G06F 21/72 (2013.01)

(12) # CERERE DE BREVET DE INVENŢIE

(21) Nr. cerere: **a 2020 00848**

(22) Data de depozit: **21/12/2020**

(41) Data publicării cererii:
30/06/2022 BOPI nr. **6/2022**

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

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

(54) CRIPTOSISTEM CU PROTECŢIE LA ANALIZA PUTERII CONSUMATE

(57) **Rezumat:**

Invenţia se referă la un criptosistem pentru care efectuarea operaţiilor algoritmului criptografic este protejată de atacurile hardware neinvazive ce fac uz de analiza puterii instantanee consumate de criptoprocesor. Criptosistemul conform invenţiei cuprinde un criptoprocesor (**2**) şi un bloc (**3**) de ecranare a consumului de putere, criptoprocesorul (**2**) având aplicate un bus de intrare (**11**) cu p biţi şi un bus de ieşire (**12**) cu q biţi, iar un pin (**13**) de intrare pentru semnalul de tact este aplicat ca intrare distinctă a criptoprocesorului (**2**) şi blocului (**3**) de ecranare, atât criptoprocesorul (**2**) cât şi blocul (**3**) de ecranare fiind polarizate în curent continuu de la o sursă de tensiune conectată galvanic la nişte pini (**14** şi **15**) de masă.

Revendicări: 1
Figuri: 3

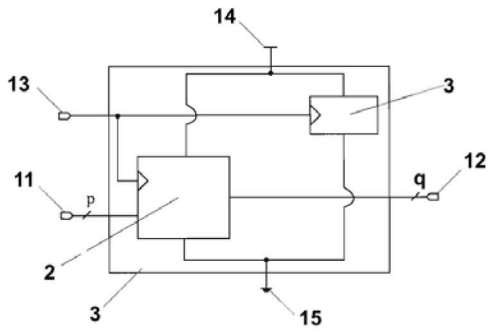

Fig. 1

RO 135861 A2

34

Criptosistem cu protecţie la analiza puterii consumate

Invenţia **se referă la** un criptosistem pentru care efectuarea operaţiilor algoritmului criptografic este protejată de atacurile hardware neinvazive ce fac uz de analiza puterii instantanee consumate de criptoprocesor.

Toţi algoritmii criptografici standardizaţi de NIST şi utilizaţi comercial în aplicaţiile practice (AES, RSA, ECC) sunt vulnerabili la atacuri neinvazive atât timp cât sunt implementaţi hardware (ASIC, FPGA) ori software (în sistemele embedded cu microcontrolere) fără contramăsuri dedicate de protecţie. Asemenea atacuri neinvazive se împart în 3 clase distincte:

- atacuri bazate pe analiza fluctuaţiei puterii consumate, de tip SPA (simple power analysis), DPA (differential power analysis) şi CPA (correlation power analysis);
- atacuri bazate pe analiza câmpului magnetic radiat neintenţionat de către criptoprocesor în timpul executării operaţiilor matematice criptografice, denumite şi DEMA (differential electromagnetic analysis), acest tip de atac necesitând, comparativ cu analiza puterii consumate, prelevarea unui număr mai mic de eşantioane pentru extragerea unei chei secrete sau date intermediare;

- atacuri bazate pe analiza întârzierilor inerente implementării algoritmului criptografic, denumite și *time analysis*, putându-se stabili corelații între o întârziere particulară măsurată practic și o adresă de memorie utilizată pentru scrierea sau citirea unei valori intermediare, implementările software și embedded fiind mai predispuse la asemenea atacuri.

Se cunosc contramăsuri pentru implementările software [1] și hardware la nivel de tranzistor [2]. Dincolo de avantajele evidente, există și dezavantaje asociate acestor contramăsuri, după cum urmează:

- viteză mai mică de comutație a porților logice din cauza complicării structurii interne a acestora prin adăugarea de tranzistoare suplimentare, având ca efect negativ frecvență de lucru (*clock*) mai mică, *throughput* (biți criptați pe secundă) mai mic față de variantă neprotejată, respectiv arie mai mare, uneori chiar de 4 ori mai mare față de varianta neprotejată la atacuri [3], puterea consumată crescând proporțional;
- proiectarea mai complicată în cazul protecției implementate la nivel de tranzistor din cauza necesității echilibrării capacităților parazite din circuit pentru asigurarea unor timpi de comutație similari în toate nodurile de interes ale circuitului;
- număr mai mare de locații de memorie necesare pentru implementarea algoritmului în cazul variantei software.

Problema tehnică pe care o rezolvă invenția este implementarea unui sistem criptografic care efectuează operațiile criptografice într-o manieră securizată, protejată contra analizei puterii consumate de criptosistem.

Criptosistemul, conform invenției, constă dintr-un procesor criptografic implementat hardware cu porți logice sau direct la nivel de tranzistor, o matrice de inversoare cu dimensiunea M x N și un divizor de frecvență, procesorul

criptografic, matricea de inversoare şi divizorul de frecvenţă fiind conectate galvanic la terminalele sursei de alimentare a criptosistemului.

Invenţia poate fi exploatată industrial pentru securizarea implementării hardware CMOS a algoritmilor criptografici, în variantă ASIC sau FPGA.

Criptosistemul, conform invenţiei, prezintă următoarele avantaje:

- securizarea implementării operaţiilor criptografice faţă de analizele SPA, DPA şi CPA;
- gradul mare de generalitate, aleatorizarea puterii consumate de procesorul criptografic păstrându-şi eficienţa indiferent de algoritmul criptografic implementat de procesorul principal (cu cheie publică sau secretă).

Se dă, în continuare, un exemplu de aplicare a invenţiei, în legătură cu Figurile 1–3 ale criptosistemului propus.

Criptosistemul **1**, conform invenţiei, este constituit dintr-un criptoprocesor **2** şi un bloc **3** de ecranare a consumului de putere, având un bus de intrare **11** cu **p** biţi aplicat ca intrare blocului **2**, un bus de ieşire **12** cu **q** biţi care este ieşire a blocului **2** şi un pin de intrare **13** pentru semnalul de tact (*clock*) aplicat ca intrare distinctă blocurilor **2** şi **3**, blocurile **1**, **2** şi **3** fiind polarizate în curent continuu de la o sursă de tensiune conectată galvanic la pinii **14** şi **15** (pin de masă / *ground*).

Criptoprocesorul **2** implementează operaţii matematice criptografice şi nu are contramăsuri de protecţie la atacurile hardware externe neinvazive, fiind proiectat la nivel de tranzistor (specific unui circuit integrat dedicat de tip ASIC) sau la nivel de porţi logice (specific unei implementări FPGA) pentru a avea performanţe maxime din perspectiva frecvenţei de lucru, ariei şi puterii consumate. Bus-ul de intrare **11** al criptosistemului **1** permite aplicarea paralel pe **p** biţi la intrarea criptoprocesorului **2** a datelor de intrare necriptate, cheii de criptare şi

altor semnale de comandă. Criptoprocesorul **2** furnizează datele criptate pe **q** biți la ieșirea **12** a criptosistemului **1**, în format paralel. De regulă **p** < **q**, bus-ul de ieșire livrând doar datele de ieșire criptate în timp ce bus-ul de intrare include datele de intrare necriptate (cu aceeași dimensiune / număr de biți ca și datele de intrare necriptate), cheia de criptare și alte semnale de comandă și control a funcționării criptosistemului. Structura internă a criptoprocesorului **2** și algoritmul particular implementat nu sunt de interes din perspectiva acestei invenții și nici nu afectează aplicarea și/sau validitatea invenției. Intrarea **13** a criptosistemului **1** aplică același semnal de tact blocurilor **2** și **3**, asigurând funcționarea sincronă.

Blocul **3**, conform invenției, constă dintr-un bloc **4** și un bloc **5**, ambele conectate galvanic la intrarea **13** aferentă semnalului de tact a criptosistemului **1**, așa cum este ilustrat în Figura 2.

Blocul **4**, conform invenției, este un divizor în frecvență care divide frecvența semnalului de tact cu valori de la 2 la M, asigurând generarea unor semnale distincte, cu perioade de 2 până la M ori mai mari decât cea de tact. Ieșirea fiecărui divizor de frecvență este conectată galvanic la intrarea unui banc de inversoare al blocului **5**. Un avantaj suplimentar al utilizării unui asemenea bloc este și acela că poate oferi semnale cu perioade diferite care pot fi utile chiar blocului **2**.

Blocul **5**, conform invenției, constă dintr-o matrice de dimensiune M x N de inversoare cascadate, unde M este numărul de bancuri de inversoare cascadate și N este numărul de inversoare aferent fiecărui banc. N este număr par pentru a asigura generarea unei perioade complete, aceasta însemnând existența unui palier aferent valorii logice '1' și al unuia aferent valorii logice '0'. Număr par de inversoare asigură și faptul că oricare pereche de inversoare generează o dublă comutație, din '1' în '0' și din '0' în '1', adică probabilitate maximă de ½ de a avea tranziții logice generatoare de ripluri (creșteri) ale consumului instantaneu (monitorizate în masa circuitului în cazul unui atac neinvaziv), ecranând astfel riplurile mai mici aferente unui consum optimizat (ideal minim) al

criptoprocesorului **2**. Blocul **5** nu are pini de ieşire deoarece nu are semnale de ieşire, inversoarele fiind utilizate nu pentru a genera semnale logice complementare (funcţionalite generică) ci pentru a exploata riplurile introduse suplimentar în bilanţul instantaneu al puterii consumate, generate de tranziţia logică '0' → '1' la ieşirea unui inversor. Numărul N trebuie ales adecvat, pe baza contextului real şi măsurătorilor fizice efectuate, fiind într-o aplicaţie reală dependent de consumul instantaneu al criptoprocesorului **2**. Numărul de bancuri M trebuie ales astfel încât să asigurăm că prin suprapunerea riplurilor fiecărui banc, lucru care se întâmplă doar la anumite momente de timp, funcţie de perioada de tact aferentă fiecărui banc, se asigură o ecranare uniformă a consumului instantaneu de putere al criptosistemului **2**. Semnalul de intrare aplicat fiecărui banc este fie semnalul de tact aplicat criptosistemului 1 în cazul primului banc (nu se doreşte întârziere), fie semnalul de tact cu frecvenţa divizată generată de divizorul de frecvenţă **4**. Conform Figurii 2, conexiunea galvanică asigură că semnalul de tact aplicat criptosistemului este aplicat bancului 1, semnalul de tact divizat cu 2 este aplicat bancului 2, semnalul de tact divizat cu 3 este aplicat bancului 3, etc, semnalul de tact divizat cu M este aplicat bancului M.

Fiecare inversor **51** inclus în structura blocului **5** are structura clasică din Figura 3, cu o intrare **5111** conectată la blocul precedent sau intrarea **13** a circuitului (cazul primului banc), o ieşire **5112** conectată la inversorul următor sau lăsată neconectată (dacă este ultimul inversor dintr-un banc de inversoare, caz în care se inserează o capacitate suplimentară la ieşirea acestuia), inversorul fiind conectat galvanic la terminalele **14** şi **15** ale sursei de alimentare a criptosistemului. Inversoarele sunt implementate cu două tranzistoare de tip MOSFET, **511** (PMOS) şi **512** (NMOS), care prin dimensiunea fizică asigură timpii de comutaţie doriţi. Inversoarele aferente unui banc sunt identice. Pentru a asigura ripluri mai mari, alese astfel încât să se asigure un consum optim de putere, întrucât bancurile de ordin superior de la 2 la M funcţionează cu semnale având frecvenţă mai mică, acestea pot fi implementate cu inversoare având tranzistoare mai mari, asigurând

astfel capacităţi parazite mai mari. Doar primul banc de inversoare funcţionează la frecvenţa de lucru a criptosistemului care este astfel, conform invenţiei, şi cea mai mare utilizată de criptosistem. Generându-se un riplu global mai mare pentru puterea instantanee, fluctuaţiile individuale ale consumului de putere instantanee al criptoprocesorului **2** sunt acoperite în întregime, nemaiputându-se stabili o corelaţie între fluctuaţiile puterii consumate aferente criptosistemului **1** şi operaţiile matematice efectuate de criptoprocesorul **2**.

REFERINȚE

[1] Pitu, Ciprian-Leonard, *PREVENTING SIDE CHANNEL ATTACKS ON A CPU*, EP 3 214 566 B1, 2016

[2] Ingrid M. Verbauwhede, *Dynamic and differential CMOS logic with signal-independent power consumption to withstand differential power analysis*, US 2007/0057698 A1, 2007

[3] David D. Hwang, Kris Tiri, Alireza Hodjat, Bo-Cheng Lai, Shenglin Yang, Patrick Schaumont, Ingrid Verbauwhede, *AES-Based Security Coprocessor IC in 0.18-μm CMOS With Resistance to Differential Power Analysis Side-Channel Attacks*, IEEE Journal of Solid-State Circuits, vol. 41, nr. 4, pag. 781-791, 2006

28

REVENDICĂRI

1. Criptosistem **1** care, în scopul securizării operațiilor algoritmului criptografic contra atacurilor hardware neinvazive care fac uz de analiza puterii consumate instantanee, este **caracterizat prin aceea că** este compus dintr-un criptoprocesor **2** și un bloc **3** folosit pentru ecranarea fluctuațiilor puterii consumate instantanee, ambele cuplate galvanic la pinii **14** și **15** ai sursei de alimentare, bus-ul **11** fiind aplicat la intrarea blocului **2**, bus-ul **12** conectat la ieșirea blocului **2** și intrarea **13** a criptosistemului, aferentă semnalului de tact, aplicată blocurilor **2** și **3**.

27

FIGURI

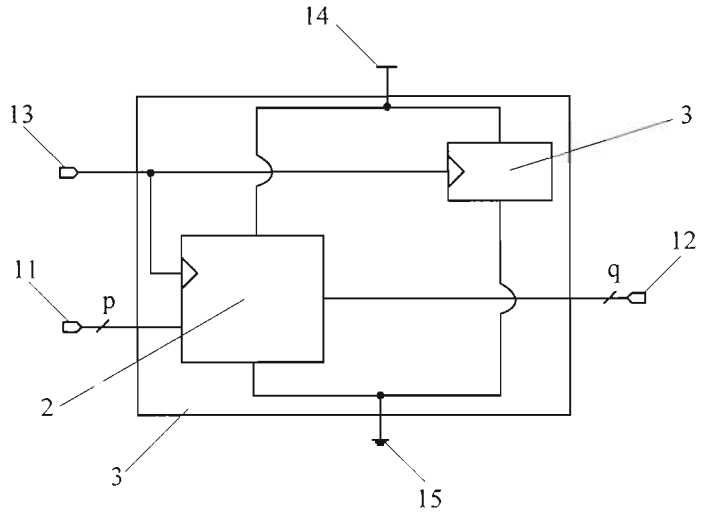

Figura 1

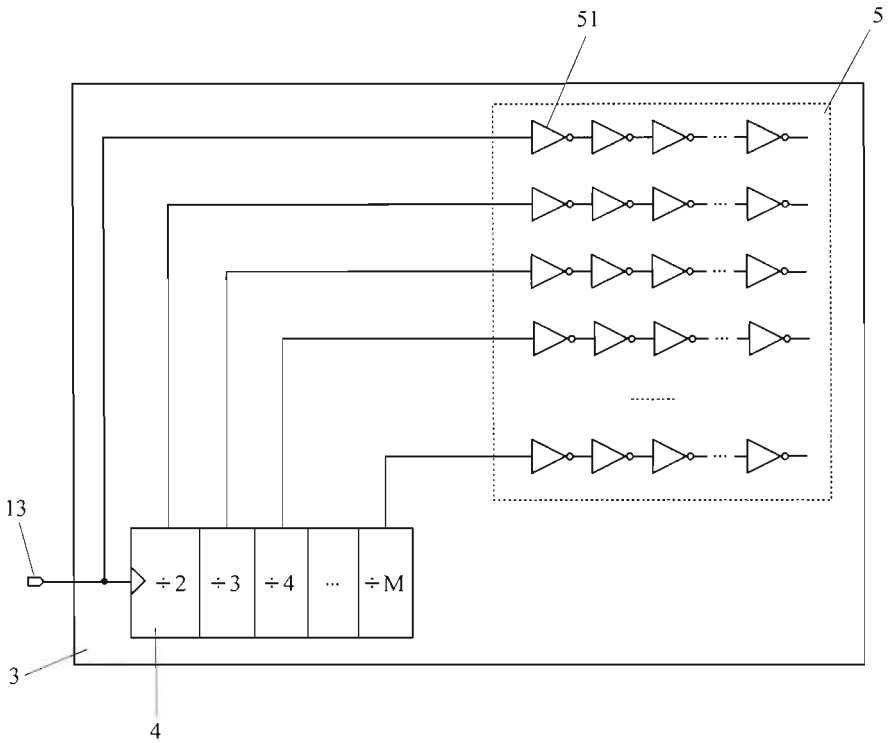

Figura 2

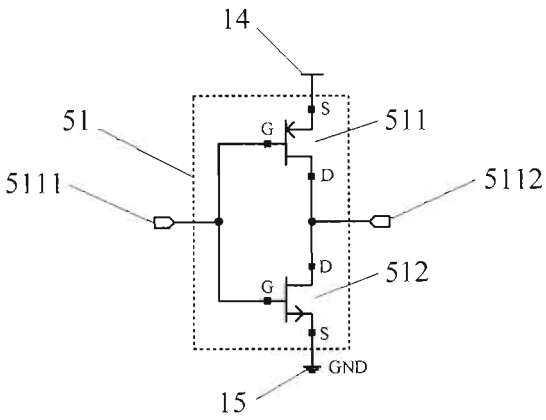

Figura 3