ROMÂNIA

(19) OFICIUL DE STAT
PENTRU INVENŢII ŞI MĂRCI
Bucureşti

(11) **RO 135240 A2**
(51) **Int.Cl.**
G06F 21/72 (2013.01)

(12) # CERERE DE BREVET DE INVENŢIE

(21) Nr. cerere: **a 2020 00165**

(22) Data de depozit: **31/03/2020**

(41) Data publicării cererii:
30/09/2021 BOPI nr. **9/2021**

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

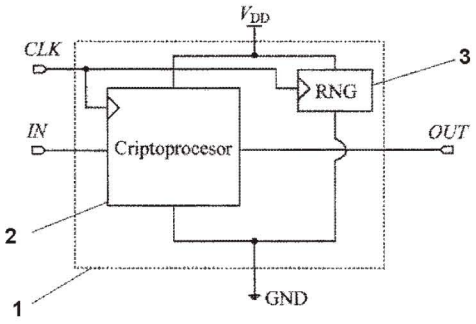
(72) Inventatori:
• **ANDRIESEI CRISTIAN**,
BD.ROMAN MUŞAT, BL.38, AP.101, ROMAN, NT, RO

(54) # CRIPTOSISTEM CU PROTECŢIE CONTRA ATACURILOR HARDWARE NEINVAZIVE

(57) **Rezumat:**

Invenţia se referă la un criptosistem cu protecţie contra atacurilor hardware neinvazive. Criptosistemul conform invenţiei este constituit dintr-un criptoprocesor (**2**) şi dintr-un generator (**3**) de numere aleatoare, ambele conectate galvanic la aceeaşi sursă (V_{DD}) de alimentare şi masă (**GND**) a sistemului, astfel încât consumul instantaneu de putere al generatorului (**3**) să mascheze consumul instantaneu de putere al criptoprocesorului (**2**).

Revendicări: 1
Figuri: 1



RO 135240 A2

14

Criptosistem cu protecție contra atacurilor hardware neinvazive

Invenția **se referă la** un criptosistem care protejează efectuarea operațiilor algoritmului criptografic de atacurile hardware neinvazive.

Toți algoritmii criptografici neclasificați utilizați comercial la ora actuală (3DES, AES, RSA, criptare pe curbe eliptice) sunt vulnerabili la atacuri hardware neinvazive atât timp cât sunt implementați fără contramăsuri dedicate de protecție. Asemenea atacuri se bazează pe analiza fluctuației puterii consumate sau câmpului magnetic radiat neintenționat de către procesor în timpul executării operațiilor matematice criptografice și vizează ambele tipuri de implementări, adică software (microcontroler, microprocesor, placă de dezvoltare de tip Arduino / Raspberry PI / FPGA) sau hardware direct la nivel de tranzistor (în tehnologie CMOS). Se cunosc contramăsuri atât pentru implementările software [1] cât și cele hardware la nivel de tranzistor [2]. Dezavantajele asociate acestor contramăsuri sunt următoarele:

- durata mai mare de efectuare a operațiilor și deci frecvență de lucru (clock) și throughput (biți criptați pe secundă) mai mici;
- număr mai mare de locații de memorie necesare pentru implementarea software;

- arie mai mare necesară în cazul algoritmilor criptografici implementați la nivel de tranzistor, 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.

Problema tehnică pe care o rezolvă invenția este implementarea unui sistem criptografic care să asigure securizarea efectuării operațiilor criptografice, fără deteriorarea frecvenței de lucru a procesorului criptografic principal.

Criptosistemul, conform invenției, constă dintr-un procesor criptografic implementat la nivel de tranzistor, care execută optim un algoritm de securitate, și un generator de numere aleatoare implementat pe același chip, ambele fiind conectate galvanic la aceeași sursă de alimentare și masa sistemului.

Invenția poate fi exploatată industrial pentru securizarea implementării algoritmilor criptografici.

Criptosistemul, conform invenției, prezintă următoarele avantaje:

- securizarea implementării operațiilor criptografice față de analiza externă a puterii consumate de sistem și a câmpului magnetic radiat;
- gradul mare de generalitate, aleatorizarea puterii consumate de procesorul criptografic și emisiilor magnetice păstrându-și eficiența indiferent de algoritmul criptografic implementat de procesorul principal.

Se dă, în continuare, un exemplu de aplicare a invenției, în legătură cu Figura 1, care reprezintă perspectiva sistemică, de tip black-box, a criptosistemului propus.

Criptosistemul 1, conform invenției, este constituit dintr-un criptoprocesor 2 și un generator de numere aleatoare 3, ambele conectate galvanic la sursa de alimentare V_{DD} și masa GND a sistemului.

Criptoprocesorul 2 este implementat la nivel de tranzistor cu blocuri logice pentru implementarea operațiilor matematice criptografice și nu are contramăsuri de protecție la atacurile hardware externe neinvazive. Intrarea de date IN a criptosistemului 1, care permite aplicarea datelor de intrare serial sau paralel, este conectată la intrarea criptoprocesorului 2. Ieșirea criptoprocesorului 2 este conectată la ieșirea criptosistemului 1, notată OUT care, de asemenea, livrează la ieșire datele în format serial sau paralel.

Generatorul de numere aleatoare 3, notat RNG, este conectat în paralel cu criptoprocesorul 2 la sursa de alimentare V_{DD} și masa GND a sistemului, neavând porturi de intrare-ieșire, doar o singură intrare pentru semnalul de tact (CLK).

Intrarea de tact CLK a criptosistemului este aplicată ambelor blocuri constitutive 2 și 3 pentru a asigura funcționarea sincronă, respectiv aceeași perioadă pentru circuitele secvențiale.

Principiul de securizare a rulării algoritmului criptografic este sintetizat după cum urmează. Criptoprocesorul 2 nefiind securizat contra atacurilor neinvazive, va fi proiectat de asemenea manieră încât va avea arie ocupată minimă, consum minim și frecvență de tact maximă (asigurând throughput maxim). În schimb, nefiind securizate operațiile, tranziția logică '0'-'1' la ieșirea porții logice poate fi identificată în masa circuitului [4], prin măsurarea curentului instantaneu care intră în masa circuitului. Pentru îngreunarea efectuării de către potențialul atacator a oricăror corelații între fluctuațiile de curent măsurate și operațiile logice efectuate de criptoprocesor, se folosește blocul 3 (RNG) care, prin tranzițiile

logice suplimentare pe care le efectuează sincron, introduce fluctuații suplimentare de curent în masa circuitului, care pot îneca în zgomot fluctuațiile de curent ale criptoprocesorului 2, ecranând astfel operațiile criptografice. Blocul 3 este implementat cu celule de deplasare (bistabile de tip D) ca în teoria codurilor corectoare de erori, fiind un registru de deplasare cu reacție, liniar (LFSR – linear feedback shift register) sau neliniar (NLFSR). În teoria clasică a codurilor se dorește ca un LFSR să aibă, dacă se poate, o lungime cât mai mică, adică număr de celule de întârziere cât mai mic, dar lungime a secvenței (pseudo)aleatoare cât mai mare. În securizarea comunicațiilor mobile 2G [5], algoritmul A5-1 folosea 3 astfel de registre de deplasare tip LFSR, cu lungimi diferite de 19, 22 și 23. A avea o secvență pseudoaleatoare lungă nu este de interes, pentru această invenție este de dorit un număr cât mai mare de tranziții '0'-'1'. În concluzie, blocul 3 RNG trebuie să fie un LFSR, ori NLFSR după caz, care să aibă la bază un polinom generator cu grad suficient de mare cât să sintetizeze un număr mare de celule de întârziere. Un număr mai mare de celule de întârziere crește probabilitatea de a avea un număr mai mare de tranziții '0'-'1' pentru fiecare celulă de întârziere. În acest fel este asigurată securizarea efectuării operațiilor criptografice contra atacurilor ce se bazează pe analiza puterii consumate.

Pentru securizarea operațiilor criptografice contra atacurilor ce fac uz de radiația emisă de criptoprocesor, se va avea în vedere intercalarea la nivel de layout a celulelor de întârziere ale blocului 3 între porțile logice ale blocului 2, respectiv alăturarea traseelor încât emisiile radiative ale blocului 3 să se interpătrundă cu cele ale blocului 2. În acest fel, atacatorul nu va putea stabili corelații între operațiile logice efectuate și fluctuațiile câmpului magnetic.

17

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

[4] Kris Tiri, Moonmoon Akmal, Ingrid Verbauwhede, *A Dynamic and Differential CMOS Logic with Signal Independent Power Consumption to Withstand Differential Power Analysis on Smart Cards*, ESSCIRC 2002, pag. 403-406

[5] https://asecuritysite.com/encryption/a5

REVENDICĂRI

1. Criptosistem care, în scopul securizării operațiilor algoritmului criptografic contra atacurilor hardware neinvazive, este **caracterizat prin aceea că** este compus dintr-un procesor criptografic 2 și un generator de numere aleatoare 3, cuplate galvanic la aceeași sursă de alimentare și masă, intrarea și ieșirea procesorului criptografic 2 fiind conectate la intrarea IN și ieșirea OUT a criptosistemului.

19

FIGURI

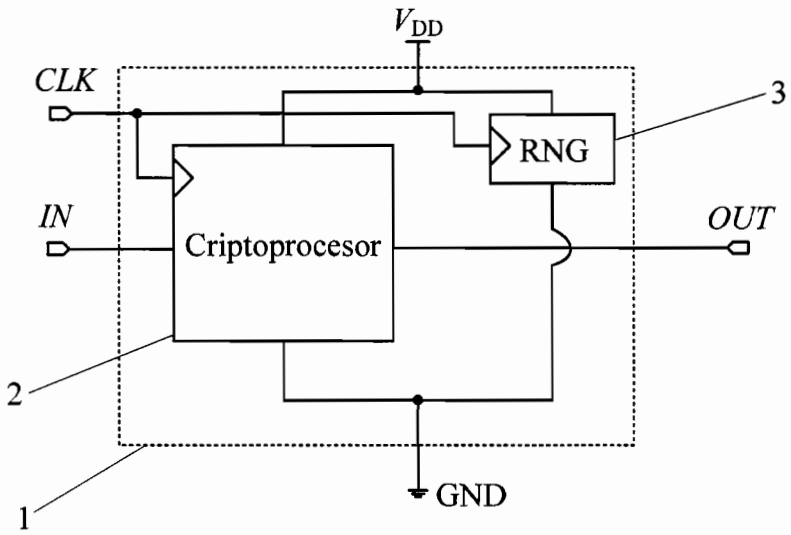


Figura 1