**I.O.S.U.D. Universitatea Politehnica Timişoara 2013/2014**

**Şcoala doctorală de studii inginereşti**

**CONTRIBUTIONS IN THE FIELD OF INFORMATION SECURITY. ERROR-DETECTION ARCHITECTURES**

**[CONTRIBUTII IN DOMENIUL SECURIZARII INFORMATIEI. ARHITECTURI DE DETECTIE A ERORILOR]**

**Teză susţinută pentru obţinerea titlului de doctor în domeniul de doctorat**

*Calculatoare si Tehnologia Informatiei*

**(sinteza)**

**Autor: *Andreea BOZEŞAN***

**Data susţinerii:** *9.04.2015*

**Conducător ştiinţific: Prof. dr. ing. Mircea VLADUŢIU**

**Referenţi ştiinţifici: Prof. dr. ing. Horia CIOCÂRLIE**

***Conf. dr. ing. Lucian PRODAN***

***Conf. dr. ing. Mihai UDRESCU***

**Rezumat:**

 Sistemele de comunicare cu calculatoare interconectate sunt viitorul în comunicatiile globale. Dar, odata cu extinderea prelucrarii electronice a datelor si transmiterea acestora prin intermediul retelelor informatice si pe web, importanta acordată securitătii acestor aspecte a crescut considerabil. Nevoia de securitate si autenticitate apare la toate nivelurile arhitecturale ale retelelor de calculatoare conectate la Internet, pentru a preveni accesul neautorizat la retea, care ar putea duce la deteriorarea sau distrugerea de date. Orice persoana care doreste sa transmita informatii prin web poate fi supusa unor atacuri malitioase care doresc sa ajunga la informatie  (de exemplu furtul de parole, de informatii de pe card din tranzactii bancare online, citire neautorizata de emailuri, conversatii, etc). O alta ramura este cea a telefoniei mobile care in lipsa unor metode de securizare este supusa ascultarilor ne-autorizate sau a citirii mesajelor de catre terte persoane. O serie de atacuri asupra ATM-urilor au fost inregistrate in ultimii ani, de catre persoane care doreau sa ajunga la datele cardului persoanelor care il foloseau pentru a le putea goli ulterior conturile. Aceste atacuri si brese in securitate pot avea consecinte dintre cele mai grave, de la incalcarea intimitatii, la furtul de bani, de identitate si esuarea unor tranzactii sau chiar sisteme informatice. Toate acestea justifica nevoia investigarii in profunzime in domeniul securitatii precum si al testarii dispozitivelor care asigura aceasta securitate. Notiunile de fiabilitate, mentenabilitate si disponibilitate in cadrul unui sistem de calcul, aparute in cartea „Design of Fault Tolerant Systems” de Barry Johnson, 1989, si fortificat in lucrarile notabile a lui A. Avizienis, J.C. Laprie, B. Randell si C. Landwehr in articolul pilot al IEEE Transactions on Dependable and Secure Computing , prin care actualitatea preocuparilor de dependabilitate este extinsa asupra noilor tehnologii corespunzatoare nano-sistemelor, bio-chipurilor, calculelor cuantice si a noilor concepte “cloud” si calculul ambiental. Cu cat paleta potentialelor defecte ce pot aparea intr-un sistem informatic devine tot mai variata, aceasta cuprinzand malfunctionarile provocate intentionat, erorile de design sau implementare, defectarea prin uzura a unor componente fizice, etc, cu atat identificarea si incorporarea mijloacelor adecvate de crestere a dependabilitatii si securitatii devine o preocupare tot mai importanta ce a fost studiata in profunzime si in aceasta teza.

In Introducerea lucrarii se incadreaza cercetarile intreprinse in domeniile din care fac parte, aratand ca se refera la modalitati de securizare a informatiilor prin algoritmii de criptare si in special algoritmul IDEA NXT, care constituie principalul subiect al investigatiilor intreprinse in lucrare. Este subliniata importanta cercetarilor referitoare la prevederea dispozitivelor criptografice cu facilitaiti de testare, diminuandu-le vulnerabilitatea la posibilele atacuri precum si cresterea imunitatii la defecte. Sunt amintite principalele contributii personale in domeniul criptografiei si testabilitatii, contributii discutate pe larg in urmatoarele capitole.

Capitolul urmator, intitulat „Fundamentals of Cryptography” cuprinde 12 pagini si constituie o trecere in revista a notiunilor de baza si a taxonomiilor in ceea ce priveste dependabilitatea si securitatea calculelor. Capitolul incepe prin a da o definitie a dependabilitatii si securitatii  si a atributelor care dau masura acestora. Apoi se prezinta amenintarile la adresa dependabilitatii si securitatii unui sistem, si anume lantul fault-error-failure, care scoate in relief modul de propagare al defectelor prin scheme, pana in locurile in care acestea sunt observate. Dupa aceea se prezinta o serie de notiuni generale ale securitatii informatiei si se introducere notiunea de criptografie, ca si solutie consacrata a atingerii dezideratului securitatii sistemelor informatice. Dupa o scurta trecere in revista a principalilor algoritmi cu chei publice (asimetrici) si a celor cu cheie privata (simetrici) si a tehnicilor pe care acestia se bazeaza, se prezinta diversele tipuri de atacuri asupra algoritmilor criptografici, printre care atacurile liniare, diferentiale, prin forta bruta, etc. Aceste atacuri dovedite care slabesc dependabilitatea cripto-algoritmilor au dus la nevoia indreptatita a cercetarilor intreprinse pentru a gasi noi directii in criptografie. Exista mai multe organisme care reglementeaza recomandarile pentru marimi de chei, parametrii si nivele minime de securitate, printre care ECYPT si ECRYPT2 (European Union Agency for Network and Information Security Agency).

Capitolul al doilea intitulat ”THE IDEA NXT CRYPTO-ALGORITHM” are 9 pagini si prezinta noua directie in criptografie sub forma familiei de algoritmi criptografici IDEA NXT, fundamentate de matematicienii Pascal Junod and Serge Vaudenav in 2001 in Elvetia. In lucrarea de prezentare a algoritmului se ilustreaza domeniile deosebit de actuale in care acest nou algoritm este folosit, printre care se numara securizarea sistemelor home-cinema, a downloadurilor de internet pentru a scadea pirateria audio si video de pe internet precum si in securizarea documentelor secrete ale guvernului american si a comunicatiilor digitale. In urma analizei amanuntite a structurii algoritmului, s-a remarcat ca modalitatea in care e construit generatorul de numere pseudo-aleatoare care se vor constitui in cheile de runda folosite la criptarea textului poate fi imbunatatia. Solutia personala gasita pentru a spori viteza de calcul a unitatii de generare a cheii, si implicit a intregului  algoritm, a fost sa se shifteze LFSR-ul cu cate 6 pozitii dintr-o data, astfel incat o cheie de runda sa fie generata direct intr-un singur ciclu de tact. Dovada matematica folosind operatii de inmultire in Campul Galois (28 ) si substitutie asupra polinomului generator al LFSR-ului sunt oferite amanuntit in acest capitol. Capitolul se incheie cu prezentarea detaliata a schemei bloc  construita pentru a implementa intr-o maniera pur hardware algoritmul IDEA NXT, atat in versiunea originala cat si in versiune sa modificata, pentru a demonstra de maniera experimentala sporirea vitezei prin modificarea LFSR-ului din generatorul de chei de runda.

Capitolul trei se numeste „VLSI TEST PRINCIPLES AND ARCHITECTURES: DESIGN FOR TESTABILITY” si are 16 pagini. In preambul, autorul se refera la necesitatea testarii echipamentelor VLSI pentru a detecta eventualele defecte ce pot aparea in sistem inca din cele mai incipiente stadii. Sunt descrise de asemena si principiile de baza ale testarii si dependabilitatii, iar in continuare sunt introduse cateva principii ale designului pentru testabilitate. Urmatorul sub-capitol constituie o trecere in revista a modelelor de defecte VLSI la toate stagiile in care acestea ar putea aparea: nivel de layout, tranzistor, nivel de porti logice rudimentare, nivelul registrului de transfer si chiar defecte la nivelul algoritmului insusi, precum si a unor tipuri uzuale de defecte. In continuare, autoarea introduce unul din conceptele fundamentale in stiinta testarii si anume toleranta la defectare, care se refera la functionarea unui sistem sau algoritm in prezenta defectelor, prin preluarea de catre componentele ne-afectate de erori a taskurilor ce trebuiau facute de componentele defecte. Domeniul tolerantei la defecte a fost intens studiat in ultimii 20-30 de ani, studii ce au dus la construirea unor masini tolerante la defecte, (Rifle, Focus, Messaline, etc) si a unor concepte noi: mascarea defectelor si revenirea dinamica dupa erori. Tot in acest capitol se introduce conceptul de injectie a erorilor intr-un circuit sau sistem, metoda ce presupune inserarea de defecte la diferite nivele si verificarea comportamentului sistemului testat cand un defect atunci este simulat in interiorul sau prin compararea iesirii sistemului cu o valoarea despre care se stie s-ar obtine la functionarea corecta a sistemului. Se amintesc toate cele 5 categorii de injectie de defecte: la nivel hardware, software,simulate, emolate si hibride, cu accent pe primele doua, oferindu-se si informatia ca detalii mai multe despre utilizarea metodelor de injectare a defectelor in cadrul cercetarii de fata vor fi date in capitolul urmator.

Capitolul al patrulea, initulat „TESTING ARCHITECTURES FOR THE IDEA NXT ENCRYPTION ALGORITHM”, se extinde pe 24 de pagini prezinta schemele de detectie a erorilor construite pentru IDEA NXT precum si justificarea creeari acestora, subliniindu-se cresterea costului, timpului si al efortului de testare cu cat se descopera o eroare intr-un stadiu mai avansat. O alta justificare a crearii unor arhitecturi de testare o reprezinta numeroasele atacuri la algoritmii existenti, unele din atacuri injectand defecte intr-un sistem prin diverse moduri: injectia fizica a erorii printr-o raza laser, insertia unui glitch rapid variind frecventa tactului, inserarea unui spike de curent, supra-incalzirea sau inghetarea unitatii, etc. Mecanismele de detectie a erorii imaginate sunt construite in mod custom, pe tiparul acestui algoritm si constituie singurele arhitecturi de testare pentru NXT pana in momentul de fata. Primul tip de arhitecturi construite si prezentate in lucrare este cel off-line, care implica testarea algotimului in timp ce acesta nu este operational. Punctul de pornire in designul mecanismelor off-line l-a constituit schema tipica Built-In Self-Test din literatura, care a stat si la baza arhitecturilor de testare construite pentru algoritmul AES. Aceasta schema, ilustrata si in mod vizual in teza, presupune stimularea circuitului cu un vector de test, generat de un modul dedicat numit Test pattern Generator (TPG)  si analizarea iesirii circuitului dupa ce un anumit numar de runde al algoritmului sau toate rundele au fost rulate si compararea lor cu o asa-numita „semnatura de aur”, care este o valoare apriori considerata corecta si obtinuta prin simulari succesive. Rezultatele partiale de la iesirea circuitului sunt compactate de fiecare data cu rezultatele anterioare intr-o semnatura si in final, semnatura respectiva este comparata cu semnatura de aur. Sunt amintite si avantajele unei astfel de testari, si anume faptul ca ele pot fi rulate atat pe o runda cat si pe un anumit numar de runde, fara ajutor din partea unui testor uman, astfel reducandu-se costul, timpul de test, nevoile de memorie. Autoarea propune 3 modele principale de arhitecturi de testare off-line si anume: feedback loop interconnection, in care exista o conexiune in bucla prin care rezultatul intermediar al criptarii devine intrare pentru urmatoarea runda de criptare, arhitecture pura BIST, in care test Pattern Generator-ul este construit pe rand ca si counter, LFSR si Cellular Automata pentru a vedea care din variante este mai eficienta iar rezultatul iesirii dupa fiecare iteratie a algoritmului este compactata cu rezultatele anterioare, si dupa ce numarul de runde stocat intr-un counter au fost rulate, rezultatul se compara cu semnatura de aur si un semnal de eroare se seteaza sau nu, in functie de rezultatul comparatiei. Unitatea care realizeaza aceasta comparatie, Output Response Analyzer (ORA) a fost de asemena implementata ca Multiple Input Signature Register (MISR) pentru a putea compacta iesirile fiecarei runde.  O a treia varianta de arhitectura offline a fost construita cu un Built In Logic Block Observer (BILBO), care este un caz special de BIST in care registrul simplu (pentru stocarea fluxului utilizat intr-o runda de criptare) utilizat in schema BIST construita anterior a fost inlocuit printr-un Pseudo-random Pattern Generator (PRPG) si al doilea registru, ce stoca in schema initiala rezultatul compactat al iesirilor circuitului a devenit un Multiple Input Signature Register (MISR). S-a observat ca aceasta varianta de arhitectura de testare este cea mai putin eficienta din cauza overheadului introdus de PRPG si MISR. Urmatorul tip de arhitectura de testare construita este cea on-line, ce opereaza concomitent cu rularea algoritmului, bazata de predictia paritatii. Principiul care sta la baza unei astfel de arhitecturi este cel al anticiparii paritatii de la iesirea algoritmului in mod iterativ, calculat dupa executia fiecarei operatii in parte, in functie de intrarea fiecarui modul. Prin verificarea egalitatii dintre paritatea prezisa si paritatea calculata, se va detecta numarul impar de erori ce afecteaza rezultatul modulului protejat, ramanand totusi complet independent de modului testat. Arhitectura concurenta bazata pe paritate construita de autoare merge in paralel cu executia algoritmului, ne-intervenind in nici un fel in functionarea acestuia. S-au construit doua arhitecturi distincte pentru calea de date si pentru unitatea de generare a cheii, singurele diferente intre cele doua fiind aparitia ortomorfismului la finalul unitatii de generare a cheii si LFSR-ul ce produce sirul de numere pseudo-aleatoare pentru construirea cheilor de runda. Schema concurenta a fost construita prin adaugarea a 2 biti de paritate, fiecare protejand cate o jumatate a inputului caii de date, si adaugarea a 2 biti de paritate corespunzatori celor doua jumatati a inputului modulului de generare a cheii de runda. Prima operatie a algoritmului este un SAU EXCLUSIV intre cele 2 jumatati a inputului, ceea ce corespunde la efectuarea aceleeasi operatii intre cei doi biti de paritate. Dificultatea aparela calculul paritatii operatiilor mai complexe, cum sunt sigma, mu, ortomorfismul sau LFSR, care fac uz de tabele de substitutie si operatii de adunare si inmultire in Campul Galois (28). Pentru acestea, autoarea a construit module dedicate care calculeaza paritatea in functie de operatiile specifice care au loc in fiecare modul. Pe langa verificarea paritatii iesirii, a fost  verificata si paritatea de la intrarea unui modul, deoarece si aceasta poate fi afectata de erori. Pentru aceasta au fost construite niste module speciale numite verificatoare care compara intrarea unui anumit modul al algoritmului de criptare cu bitii de paritate obtinuti pana in momentul respectiv si daca se observa o discrepanta, se seteaza un semnal de eroare. Schemele de predictie a paritatii au fost ilustrate si in maniera grafica, printr-o serie de figuri extrem, de clare si explicite. Toate aceste arhitecturi de testare originale construite pentru cripto-algoritmul IDEA NXT au fost cuprinse in doua lucrari de mare valoare, prezentate la conferintele SOFA si ICSTCC, ambele facand parte din circuitul IEEE: ”Parity-based Concurrent Error-detection Architecture applied to the IDEA NXT Crypto-algorithm” si “Offline Self-Testing Architectures for the IDEA NXT Crypto-Algorithm”.

Capitolul se incheie cu observatia ca este necesara si o verificare a ratei detectie a erorilor (au fost considerate cele de tip stuck-at). In acest sens, s-a  transformat implementarea hardware a arhitecturilor de testare intr-una ce foloseste numai porti logice primitive si registre si a aplicat tehnica sabotorilor pentru a injecta defecte de tip stuck-at-0 la intrarile respectivelor porti. S-au considerat cazurile cu fanout 1, cand iesirea unei porti va constitui intrare pentru o singura alta poarta, si a blocat acel semnatul la valoarea ‚0’ logic, si cazul cu fanout mai mare decat 1, pentru acele iesiri care se constitie in intrari pentru mai multe porti. In acel caz, a ales intr-un mod aleator una dintre intrare si a blocat-o pe ‚0’ logic. Prin analiza corectitudinii iesirii algoritmului dupa rularea acestuia se constata daca erorile au fost detectate sau nu.

Capitolul cinci denumit „Experimental Results” are 25 de pagini si cuprinde toate  experimentele desfasurate in cadrul cercetarii intreprinse. Sunt prezentate toate experimentele intreprinse in cadrul cercetarii, atat in ceea ce priveste implementarea hardware a algoritmului original IDEA NXT si a variantei sale modificate , cat si in ceea ce priveste metodele de detectie a erorilor construite pentru acest algoritm, comparativ unele la celelalte in lipsa altor scheme similare. Sunt subliniate avantajele folosirii unui anumit tip de arhitecturi in detrimentul altora, avantaje ce reies din analiza rezultatelor experimentale obtinute in termeni ai hardware-ului ocupat, ai vitezei caii critice, al throughputului si al metricii composite arie/throughput.

In final, un capitol de Concluzii extins pe 3 pagini reitereaza contributiile principale ale tezei, relevate pe tot parcursul ei si prezinta viitoarele directii posibile de cercetare, plecand de la rezultatele obtinute in lucrare. Sunt mentionate de asemena si articolele suport publicate si sustinute la diverse conferinte.

**Principalele contribuţii revendicate:**

                               I. Recenzia literaturii de specialitate in contextul implementarii facilitatilor de testare fara degradarea securitatii pentru protectia algoritmului IDEA NXT

                             II. O solutie de testare on-line atat a caii de date a algoritmului cat si a generatorului de chei de runda a algoritmului de criptare IDEA NXT , bazata pe predictia paritatii iesirilor fiecarei operatii a algoritmului

                           III. O serie de strategii de testare off-line, atat folosind o interconexiune in bucla, cat si folosind o structura Built-In Self-Test pentru algoritmul IDEA NXT, aplicabile atat la nivel de runda, cat si la nivelul intregului algoritm

                          IV. O modalitate de verificare a eficientei arhitecturilor de testare mai sus mentionate de detectare a defectelor de tip stuck-at-0 folosind tehnicile saboteur/mutant

                            V. O implementare pur hardware a cripto-algoritmului IDEA NXT, prima de genul acesta implementata pentru un FPGA

                          VI. O imbunatatire a vitezei  algoritmului adusa prin modificarea modulului de generare a numerelor pseudo-aleatoare ce se vor constitui in chei de runda pentru algoritm prin furnizarea unei chei de runda intr-un singur ciclu de clock in loc de 6 cicluri de tact, cum era in varianta originala a algoritmului

**Nr. Pagini:** 102 **Nr. Figuri:** 60 **Nr. Tabele:** 7 **Nr. De titluri bibliografice:** 123

**Valorificări până la momentul susţinerii tezei:**

**Nr. articole publicate în reviste de specialitate:** *0*

**Nr. lucrări comunicate la conferinţe şi congrese:** 6

**Nr. rapoarte de cercetare (referate de doctorat, granturi ş.a.):** 2