Rezumatul Tezei de Doctorat

"Reliable Implementations for Cryptographic Systems with Testability Facilities"

Elaborată de ing. Flavius Opriţoiu

Circuitele integrate cu funcţie de securitate joacă un rol cu o importanţă crescândă în viaţa cotidiană. În principal, utilitatea acestora se defineşte în contextul asigurării securităţii informaţiilor sensibile. Printre multele aplicaţii ale metodelor criptografice se pot aminti: comunicarea sigură în reţele de calculatoare, distribuţia media în cadrul televiziunilor digitale în sistem pay-per-view, carduri bancare, plaţi electronice precum şi paşaport biometric.

Atât actualitatea cât mai ales oportunitatea temei de cercetare alese pot fi justificate aducând în discuţie interesul manifestat de comunitatea europeană asupra domeniului securităţii. În acest sens, amintim demersurile continue de finanţare a cercetării colaborative între instituţiile academice şi segmentul industrial. În acest sens, proiectul Stork, urmat de Ecrypt şi de actualul Ecrypt II, fundamentează cercetarea europeană în domeniul criptografic, ridicând-o la nivel de activitate finanţată prin proiecte cadru de cercetare.

Actualitatea domeniului testării in tehnologie VLSI în general şi a cryptocipurilor în particular, este justificată de interesul acordat ingineriei testării, de către Asociaţia Industriilor Semiconductoare în rapoartele întocmite periodic de către acest for internaţional.

Eficienţa facilităţilor de testarea integrate într-un dispozitiv influenţează direct costul de producţie prin intermediul ratei de defectare. Cunoscând că înlocuirea unei componente defecte este cu atât mai puţin costisitoare cu cât este mai rapid identificată în procesul de asamblare a sistemului final, este pe deplin justificată integrarea unor mecanisme de testare în interiorul designului, care să permită verificarea integrităţii dispozitivului atat după fabricaţie, cât şi pe durata exploatării lui.

Problematica testării în contextul dispozitivelor criptografice capăta valenţe noi. Pe de o parte facilităţile de testarea sunt esenţiale pentru orice dispozitiv integrat, iar pe de altă parte, sunt absolut esenţiale pentru un sistem vulnerabil în fata atacurilor. Rafinarea metodele criptanalitice a dus la construirea unor strategii de atac a sistemelor criptografice dintre cele mai variate: de la metode pasive, bazate pe analiza informaţiilor oferite inerent de către dispozitivele integrate (radiaţie termică, radiaţie electromagnetică) până la soluţii invazive, ţintind modificarea stării interne a circuitului. În acest context, integrarea facilităţilor de verificare a integrităţii modulelor criptografice devine o prioritate a oricărui design criptografic. Pot fi alese însă soluţii de testare necorespunzătoare, care să constitue tocmai punctul de pornire al unor atacuri reuşite.

Aparenta contradicţie între necesitatea integrării facilităţilor de testare şi vulnerabilitatea pe care o pot introduce, este uşor depăşită luând în considerare soluţiile de autotestare. Conferind autonomie procesului de testare şi reducând volumul de informaţii transmise spre exterior pe durata testului, aceste soluţii îmbunătăţesc securitatea implementării.

Concluzia evidentă a comentariilor anterioare recomanda ingineria testării hardware ca fiind o disciplină cu oportunităţi şi provocări actuale, semnificative, în contextul cercetării ştiinţifice.

În teză, este introdusă tematica modelelor de defecte, prezentate ierarhic în concordanţă cu nivelele de descriere hardware ale circuitelor digitale. Modelele de defecte sunt diferenţiate

gradual începând cu cele de la nivelul algoritmilor, continuând cu cele specifice nivelului de descriere Register Transfer Level, prezentând apoi modelele caracteristice nivelului de descriere logică al circuitelor şi finalizând cu mai specializatele modele de defecte la nivelul tranzistorilor şi al substratului semiconductor. Prezentarea investighează de asemenea, posibilitatea de mapare a defectelor la nivelul tranzistorilor şi al substratului fizic în termenii defectelor logice. Ipotezele de acoperire a defectelor de nivel jos prin tehnici de testare specific defectelor stuck-at sunt validate prin simulări la nivelul transistorului în tehnologie CMOS, utilizând mediul de simulare SPICE. Sunt detaliate şi modelele de defect de tip bridging şi cele de tip întârziere, specifice tehnologiei VLSI, oferind o discuție a metodelor de detecție a acestora la nivelul logic.

Lucrarea abordează în continuare problematica ingineriei testării hardware, pornind de la premisele de natură economică asociate procesului de testare. Strategiile de testare autonomă, utile în asigurarea integrității sistemelor criptografice, sunt detaliate, începând cu metodele de testare off-line, non-concurentă. Paradigma Built-In Self-Test este introdusă, împreună cu detaliile de implementare ale unei soluții off-line caracteristice, aşa cum sunt prezentate în literatură şi cum sunt implementate practic de către fabricanții de circuite. Sunt discutate soluțiile convenabile de implementare a unităților de generare a vectorilor de test precum şi a modulelor de compactare a răspunsurilor, bazate pe elemente Linear Feedback Shift Registers, împreună cu problemele de selecție a configurației acestora pentru reducerea probabilității de aliasing. Strategia Built In Logic Block Observer este descrisă de asemenea, reprezentând o soluție algoritmică de transformare a unui design VLSI într-o structură care încorporează facilități Built-In Self-Test. Lucrarea analizează şi strategiile de testare concurenta: mecanismele convenționale de testare on-line, cum sunt cele bazate pe duplicarea hardware, a utilizării codurilor detectoare de erori şi a metodelor redundantei de timp sunt detaliate, urmărind modelul referințelor autoritative din literatură. Sunt prezentate soluțiile concurente pentru detecția defectele care nu sunt detectate prin modelele de la nivelul logic sau cel al tranzistorului, cum sunt cele bazate pe monitorizarea parametrilor fizici ai implementării.

Domeniul algoritmilor de criptare este de asemenea investigat în teză, fiind oferind un scurt istoric al dezvoltării acestora precum şi modalitățile curente de utilizare şi adaptare a lor la nevoile de securitate curente. Accentul este pus pe algoritmi de criptare simetrică, considerând algoritmul Advanced Encryption Standard. Pe lângă prezentarea propriu-zisă a algoritmului, teza investighează soluțiile oferite în literatură, pentru accelerarea procesului de criptare respectiv de decriptare. Culminarea observațiilor acumulate prin studiul literaturii de specialitate o reprezintă arhitectura AES duala, capabilă să execute atât procesul de criptare cât şi pe cel de decriptare, a cărei sintetiză urmăreşte reducerea dimensiunii designului prin partajarea resurselor hardware comune celor 2 procese, în condițiile obținerii unei viteze de operare ridicate. Sunt detaliate diferențele notabile între structura propusă şi soluțiile întâlnite în literatură.

Lucrarea prezintă soluțiile de testare, atât on-line cât şi off-line, propuse de autor, soluții care cumulativ protejează toate elementele constitutive ale algoritmului AES împotriva defectelor în general şi a atacurilor invazive în particular. Este inclusă o secțiune destinată inventarierii soluțiilor de testare aplicabile algoritmului AES, aşa cum au fost întâlnite în literatură, şi continuă cu prezentarea a doua mecanisme de testare on-line, unul destinat operațiilor rundei AES, iar altul operației de inversie în câmpul Galois, şi a unei arhitecturi BIST de testare off-line, ca o soluție alternativă de protejare a operatiilor nelinieare ale algoritmului.

Prima soluție de testare aparține clasei de mecanisme de detecție concurentă a erorilor. Ea permite identificarea erorilor care afectează operațiile rundei AES, bazându-se pe mecanisme de detecție a erorilor prin predicția parității. Arhitectura propusă a fost construită pornind de la o

structură de bază, proiectată pe baza soluțiilor de testare on-line propuse în literatură. Dezavantajul arhitecturii de bază constă în neuniformitatea predicției parității pentru transformarea ShiftRows, impediment înlăturat în structura propusă de autor, care calculează octeții de paritate transversal, în matricea de stare. Lucrarea prezintă detaliile matematice de predicție a parității pentru transformările AES. Se remarcă caracterul non-intruziv al soluției construite, permițându-i să fie aplicată independent de modalitatea de implementare a căii de date AES. În plus, pentru noua structură, complexitatea predicție parității în cazul modulului de generare a cheilor de rundă este semnificativ redusă. Structura realizată este comparată în raport cu arhitectura de bază, rezultatele evidențiind superioritatea ei privind dimensiunile designului, puterea consumată şi latența procesului de test.

A doua soluție de testare urmăreste detecția erorilor ce pot afecta cele 3 operații neliniare ale AES, prin metode de autotestare non-concurentă. Este construită o arhitectură BIST utilizând elemente LFSR care să asigure detecția oricărui defect stuck-at singular. Alegerea polinoamelor caracteristice pentru structurile LFSR de generare a vectorilor de test şi respectiv, de compactare a răspunsurilor, a fost ghidată de simulări. În cadrul aceleaşi soluții este analizată adaptare tehnicii prezentate prin monitorizarea continuă a intrărilor unității protejate, în vederea identificării vectorilor relevanți procesului de testare. Experimentele indică o rată de detecție a defectelor multiple, mai mare de 99.77% pentru prima soluție BIST propusă.

Ultima arhitectură de test introduce o soluție on-line de detecție a defectelor intermitente în unitatea de inversie AES. Testarea se bazează pe o proprietate matematică convenabilă a operației, demonstrată în lucrare, pe baza căreia suma între un element al câmpului şi inversul său poate fi unul din 128 de posibile rezultate. În acest sens modulul de verificare a integrității inversiei efectuează suma în câmpul finit între intrarea şi ieşirea modulului verificând dacă rezultatul este unul din cele 128 de configurații corecte. Rezultatele experimentale indică aplicabilitatea acestei metodei în detecția defectelor intermitente singulare sau duble. Adaptarea mecanismului prezentat într-o arhitectură de testare non-concurentă, permite reducerea latenței testului la numai 4 cicluri, spre deosebire de soluțiile BIST convenționale, necesitând între 152 şi 255 de cicluri, după cum documentează anterioara soluție de testare.

Datorită efectului aliasingului, metoda de test on-line nu este potrivită pentru detecția defectelor intermitente multiple. Soluția la această problemă se rezuma la includerea redundantei de cod, asociind suma dintre intrarea şi ieşirea unității de inversie cu o semnătură calculata pentru configurația de intrare. Semnătura, în soluția analizată, este obținută prin compactare spațială pe 4 biti a intrarii. Noua arhitectură obținută, detectează cu probabilitate mai mare de 93% defecte intermitente cu multiplicitate de până la 100. Pentru evaluarea eficienței structurilor construite a fost considerată tehnica duplicării hardware, față de care designurile propuse au o complexitate semnificativ redusă, oferind în acelaşi timp o rată de detecție mai mare de 93%.

În încheierea lucrarii sunt prezentate concluziile activității de cercetare si sunt marcate punctual contribuțiile acesteia împreuna cu posibilele direcții de continuare a cercetării.