



*Implementări Fiabile ale Dispozitivelor Criptografice
cu Facilități de Testare*

Teză susținută pentru obținerea titlului de doctor în domeniul de doctorat
Știința Calculatoarelor

(sinteză)

Autor: *Flavius Oprîtoiu*

Data susținerii: *16 iulie 2010*

Conducător științific: *Prof. dr. ing. Mircea Vlăduțiu*

Referenți științifici: *Prof. dr. ing. Mircea Petrescu*
Prof. dr. ing. Daniela Popescu
Prof. dr. ing. Liviu Miclea

Rezumat: *Criptografia urmărește asigurarea securității datelor în contextul în care modulele criptografice sunt incluse în tot mai multe sisteme digitale. Păstrarea integrității acestor unități, și a securității cheilor în prezența atacurilor premeditate, a metodelor criptanalitice precum și a deteriorării naturale a substratului semiconductor este o necesitate. Teza de doctorat detaliază modelele de defecte la diferite nivele ale descrierii circuitelor. Investighează de asemenea gradul de acoperire al defectelor fizice prin modelul stuck-at. Strategiile convenționale de testare, atât on-line cât și off-line sunt introduse ca o extensie a necesității de detecție a modelelor de erori prezentate. Algoritmul criptografic asupra căruia este focalizată această lucrare este Advanced Encryption Standard, pentru care autorul construiește o arhitectură de mare viteză, exploatând reutilizarea hardware la nivelul operațiilor rundelor de criptare și decriptare AES. Această structură este apoi extinsă prin mecanismele de test propuse de autor, dovedite experimental a fi eficiente pentru detecția atât a erorilor permanente cât și a celor intermitente.*

Principalele contribuții revendicate: *1.Recenzia exhaustivă a literaturii de specialitate; 2.Prezentarea unei arhitecturi AES de mare viteză, iterativă, exploatând reutilizarea hardware; 3.Proiectarea unei soluții de test on-line, bazată pe predicția prin paritate, destinată protecției rundeii AES; 4.Construirea unei structuri BIST non-concurente pentru protejarea operațiilor neliniare ale algoritmului; 5.Dezvoltarea unei soluții de testare a modulului de inversie în câmpuri finite bazată pe o proprietate matematică convenabilă.*

Nr. Pagini: *126*

Nr. Figuri: *65*

Nr. Tabele: *9*

Nr. de titluri bibliografice: *123*

Valorificări până la momentul susținerii tezei:

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

Nr. lucrări comunicate la conferințe și congrese: *5*

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

Catalogarea în seriile Teze de doctorat ale UPT – Editura Politehnica:

Seria: *10* **Nr:** *29*

ISSN: *1842-7707*

ISBN: *978-606-554-129-0*