# PROPUNEREA UNOR SOLUŢII DE ACCELERARE A ALGORITMULUI AES CU AJUTORUL UNUI PROCESOR GRAFIC

**REZUMAT**

Teză destinată obţinerii
titlului ştiinţific de doctor inginer
la
Universitatea „Politehnica” din Timişoara
în domeniul CALCULATOARE şi TEHNOLOGIA INFORMAŢIEI
de către

**Ing. Tomoiagă Radu-Daniel**

| | |
|---|---|
| Conducător ştiinţific: | prof. univ. dr.ing. Stratulat Mircea |
| Referenţi ştiinţifici : | prof. univ. dr. ing. Victor-Valeriu Patriciu |
| | prof. univ. dr. ing. Daniela Elena Popescu |
| | prof. univ. dr. ing. Mircea Popa |

Ziua susţinerii tezei: 11.03.2011

Este indiscutabil faptul că domeniul tehnologiei informației a devenit o componentă de bază a societății actuale şi că el face parte, într-o manieră din ce în ce mai evidentă, din realitatea pe care o trăim. Evoluția permanentă a tehnologiei de înaltă performanță a permis accesul unor categorii de utilizatori din ce mai largi şi în acelaşi timp din ce în ce mai diversificați. Pe de altă parte, acumulările teoretice şi experimentale au determinat mutații tehnologice semnificative în cele mai diverse domenii ale vieții ştiințifice, economice, sociale şi chiar culturale.

Actualitatea şi importanța temei rezultă din modul cum a evoluat tehnologia modernă privind protecția şi transmiterea informațiilor pe diferite canale de comunicații publice. În acest context, este firească dorința fiecăruia dintre noi de a avea acces la servicii de comunicație cu grad ridicat de securitate. Securitatea informației este un subiect mult discutat şi dezbătut în prezent. Există mai multe domenii ale securității informației, dar indiferent de modelul de securitate ales, ca punct central, toate au ca ultimă măsură asigurarea confidențialității datelor.

Teza de doctorat se încadrează în domeniul protecției datelor prin abordarea unui model de securitate ce are ca scop protejarea datelor clasificate ținând cont şi de cadrul legislativ național. Acest model se bazează pe mai multe straturi de protecție, iar punctul central este criptografia, care are rolul de asigurare a confidențialității datelor. Una dintre problemele curente ar fi absența unor metode performante care sa permită implementarea unor algoritmi criptografici consacrați pentru o gamă largă de date de capacitate variabilă şi cu un grad ridicat de securitate şi care să conducă la obținerea unor timpi de execuție acceptabili. Pe baza problemelor identificate, autorul îşi propune ca în cadrul tezei de doctorat să atingă următoarele mari obiective:

- Să identifice, prin metode experimentale, algoritmii criptografici cu performanțele cele mai bune de a fi folosiți în aplicații ce impun utilizarea unor date de intrare de capacitate variabilă şi memorate pe diferite medii de stocare.
- Să identifice platformele şi mediile de programare care prezintă soluțiile de implementare a algoritmilor criptografici în condițiile cele mai bune.
- Să identifice arhitecturile hardware care sunt cele mai adecvate implementării unor algoritmi criptografici.
- Dezvoltarea unor metode de accelerare a unor algoritmi criptografici consacrați care să fie validate atât teoretic cât şi prin experimente practice şi care să permită obținerea unor rezultate comparabile sau mai bune decât cele mai utilizate metode existente în prezent.

Teza de doctorat este structurată pe şase capitole care se extind pe 145 de pagini şi este organizată în trei părți logice. Prima parte constituită din primele două capitole ale lucrării este alocată prezentării algoritmilor criptografici consacrați, cu scoaterea în evidență a caracteristicilor acestora.

Partea a doua a lucrării ce cuprinde capitolele trei şi patru din teză este dedicată experimentelor şi testelor efectuate pe diferite medii de programare a celor mai cunoscuți algoritmi criptografici în vederea obținerii unor răspunsuri privind performanțele acestora, dar şi identificarea mediului de programare care are comportamentul cel mai potrivit pentru asfel de aplicații. Au utilizat date stocate în memorie cât şi pe hard disc. În

continuare, s-au efectuat experimente pe un număr de platforme hardware, având diferite arhitecturi şi configuraţii. Rezultatele experimentelor au fost prezentate sub formă tabelară şi/sau grafică exprimându-se o serie de obseraţii cu privire la aceste seturi de teste.

În partea treia a lucrării, pe baza concluziilor rezultate din experimentele efectuate, se propun două metodă de accelerare a executării algoritmilor criptografici prin adaptarea acestora în vederea efectuării anumitor paşi de execuţie în paralel. Soluţiile alese diferă de cele propuse în literatura de specialitate, ceea ce-i conferă o notă de originalitate. În urma testelor efectuate cu noua metodă, implementată pentru algoritmul criptografic AES pe un procesor grafic (GPU) folosind mediul de dezvoltare CUDA (Compute Unified Device Architecture), s-au obţinut rezultate deosebit de promiţătoare, ceea ce conferă soluţiilor alese un grad ridicat de încredere. În final, au fost comparate rezultatele experimentale obţinute cu alte  din literatura de specialitate.

În finalul lucrării sunt punctate concluziile, contribuţiile personale şi direcţiile de cercetare viitoare.

Capitolul 1 de introducere pune accentul pe aspecte legate de metrici şi testele de evaluare a performanţelor algoritmilor de criptare. Testele selectate au avut ca scop generarea unor concluzii privind performanţele oferite de platformele tradiţionale de programare cât şi cele legate de eficienţa unor arhitecturi de calculatoare. Totodată, s-a urmărit determinarea unor difernţe între mediile de programare. Pentru o mai bună analiză, s-a apelat la alegerea unor valori de intrare diverse. Scopul urmărit în alegerea testelor a constat în determinarea performanţelor sistemelor de operare, a sistemelor de calcul şi a limbajelor de programare privind implementarea algoritmilor de criptare. Pentru a înlătura o serie de obiecţii ridicate de testele efectuate în literatura de specialitate autorul lucrării a recurs la efectuarea acestor teste pe un număr mare de date, folosind un număr mare de platforme şi rulând  un număr mare de algorimi. Faţă de testele din literatură ce au adoptat un număr de repetare a unui algoritm, în vederea testelor de 100.000 de ori, autorul tezei a repetat acelaşi test de 1.000.000 de ori în vederea obţinerii unor rezultate mai exacte. Volumul mare de date de intrare, numărul mare de algoritmi testaţi, utilizarea unui număr sporit de sisteme de calcul cu arhitecturi diverse pe care s-au executat testele şi varietatea mediilor de dezvoltare au permis autorului lucrării o mai fină observaţie asupra comportamentului algoritmilor criptografici. Pe baza acestor concluzii s-a reuşit dezvoltarea unor metode mai bune în ceea ce priveşte implementarea algoritmilor criptografici.

Plecând de la evaluările performanţelor funcţiilor criptografice, autorul lucrării s-a oprit în capitolul 2 asupra a trei categorii de algoritmi criptografici standard: algoritmi bazaţi pe coduri de autentificare a mesajelor (MAC) ce folosesc primitive criptografice de tipul funcţiilor hash (HMAC), algoritmi simetrici cum ar fi algoritmul DES (Data Encryption Standard), 3DES (Triple DES), AES (Advanced Encryption Standard) şi funcţii hash.

În urma descrierilor teoretice a primitivelor criptografice şi pe baza unor justificări pertinente, s-au ales 11 algoritmi pentru a fi testaţi în capitolele următoare şi anume patru algoritmi din clasa primitivelor HMAC, trei algoritmi simetrici şi patru algoritmi din categoria funcţiilor hash.

În capitolul 3 sunt descrise aplicaţiile de testare.  O primă categorie de teste se referă la date stocate pe hard disc. Dimensiunea fişierelor alese este de la 100MB, şi ajung până

la 10GB. La aceste teste, la timpul de criptare pentru cei 11 algoritmi mai trebuie avut în vedere şi timpul de acces la datele care se află pe hard disc. Testele au fost realizate pe sistemul de operare Windows pe care au fost dezvoltate aplicații de test pentru algoritmi criptografici menționați mai sus în Visual Basic şi Visual C#. Tot în aceaşi categorie de test s-a dezvoltat o aplicație pe sistemul de operare UNIX optându-se pentru bibliotecile din OpenSSL.

Toate testele au fost rulate pe cinci sisteme de calcul având performanțe diferite şi chiar arhitecturi de calcul diferite. Alegerea sistemelor de calcul a constat în verificarea algoritmilor pe platforme de calcul având procesoare din categorii diferite, memorii interne cu caracteristici diferite şi furnizate de producători diferiți.

O a doua categorie de teste a contat în furnizarea datelor pentru criptare să se facă de pe memoria internă a sistemului de calcul. Sistemul de operare utilizat în acest caz a fost Windows, iar aplicațiile s-au dezvoltat în Visual Basic, C# şi Java. Pentru acestă categorie de teste s-au utilizat trei sisteme de calcul. Pentru configurația aleasă s-au adoptat aceleaşi principii ca la testele din categoria întâi şi anume să prezinte procesoare şi memorie cu caracteristici diferite. Producătorii, de asemenea, au fost aleşi diferit.

Pentru toate testele din memorie s-a rulat fiecare algoritm de un milion de ori. Rezultatele rulării s-au exprimat prin timpul mediu de rulare al algoritmului pentru o iterație.

În capitolul 4 sunt prezentate rezultatele obținute în urma efectuării testelor descrise în capitolul precedent şi o serie de evaluări ale performanțelor algoritmilor criptografici. Pentru o evaluare cât mai corectă rezultatele au fost interpretate pe mai multe planuri. Un prim set de analize s-a efectuat pentru fişiere de intrare de dimensiuni de 1MB şi 100MB, respectiv fişiere cuprinse între 1GB şi 10GB. Pentru cele două studii de caz s-au analizat performanțele în timp ale algoritmilor criptografici pe durata efectuării procesului de criptare.

O primă remarcă legată de sistemele de calcul utilizate a constat în faptul că, comportamentul în timp al algoritmilor nu este unitar existând nişe în care un anumit algoritm este mai performant pe un sistem de calcul dar mai puțin performant pentru alte date de intrare.

În ceea ce priveşte evaluarea performanțelor algoritmilor din punctul de vedere al mediilor de dezvoltare, se constată un grad mai mare de uniformitate al rezultatelor, dar care nu sunt suficient de concludente pentru întreaga plajă a valorilor de intrare.

În urma analizei realizate între sistemele de operare, se poate spune că sistemul de operare Unix oferă stabilitate mai bună din punctul de vedere al păstrării caracterului crescător pe cele zece fişiere testate. Sistemul de operare Windows nu a oferit o astfel de stabilitate pe întregul set de fişiere în testele efectuate, fiind cazuri în care primitivele criptografice au avut nevoie de mai mult timp în cazul fişierelor mai mici decât în cazul fişierelor mai mari. Unix poate fi considerat mai stabil decât Windows, dar din punctul de vedere al performanței, niciunul din cele două sisteme de operare nu este un câştigător.

Un ultim set de evaluare al performanțelor s-a efectuat asupra celor trei categorii de algoritmi. În acest caz, rezultatele evaluărilor s-au apropiat de estimările inițiale efectuate.

În final, se poate spune că numărul mare de variabile de intrare şi-au pus amprenta asupra rezultatelor. Acestea au fost în anumite situații atipice. Teste efectuate au acoperit mai multe tipuri de: sisteme de calcul, sisteme de operare, limbaje de programare şi date

de intrare. Ca o concluzie se poate spune că, în final, s-a putut obține o imagine de ansamblu asupra performanțelor oferite de primitivele criptografice şi anume că o imbunătățire a timpilor de execuție nu poate fi obținută cu metode clasice. Ca urmare, autorul lucrării a propus o nouă metodă de accelerare a performanțelor algoritmilor criptografici.

Soluția propusă constă în rularea algoritmilor criptografici pe un procesor neconvențional care să ajute procesorul dedicat la operația de criptare. O soluție ar fi utilizarea unui coprocesor criptografic, care ar implica costuri suplimentare, sau utilizarea unui procesor existent într-un sistem de calcul, cum ar fi procesorul grafic. S-a ales cea de-a doua soluție din motive economice şi care, după cum se va vedea în continuare, conduce la rezultate apreciabile.

În capitolul 5 , după o trecere în revistă a unor realizări similare de utilizare a unui procesor grafic (GPU) pe post de cooprocesor criptografic, autorul constată că soluțiile prezentate au performanțe scăzute. Pentru a accelera performanțele algoritmilor criptografici, s-a plecat de la principiul utilizării acelui procesor grafic cu mai multe nuclee şi care să suporte ca mediu de dezvoltare arhitectura paralelă CUDA (Compute Unified Device Architecture). Această arhitectură permite utilizatorilor să folosească limbajul C şi din punct de vedere operațional procesorul principal consideră procesorul grafic ca pe un cooprocesor. Pentru accelerarea algoritmilor criptografici utilizând procesorul grafic, autorul a dezvoltat două soluții. În prima fază, s-a impus adaptarea algoritmilor criptografici la procesorele grafice. Aceştia sunt proiectați pentru calcul paralel şi în principiu nu sunt adecvați procesului criptografic, care, în general, se bazează pe date anterioare pentru criptare. Pentru verificarea conceptelor ce urmează a fi abordate, autorul lucrării a ales pentru adaptarea executării paralele pe procesorul grafic algoritmul de criptare simetrică AES. Algoritmul AES executat pe procesoare seriale se bazează pe tabele de căutare care, teoretic, la procesoarele grafice, ar încetini procesul de execuție. Pentru verificarea aspectelor teoretice, algoritmul AES a fost implementat în varianta utilizării tabelelor de căutare, respectiv în varianta executării operațiilor aritmetice. Prin identificarea tuturor operațiilor ce pot fi executate în paralel pe procesorul grafic, s-a reuşit ca procesul de criptare să fie executat în paralel fie prin căutare în tabele fie prin operații aritmetice. O atenție deosebită s-a acordat modului de acces la memoria privată, memoria partajată sau memoria globală, luându-se în considerare timpul de acces la aceste tipuri de memorie.

Pentru validarea soluțiilor alese, s-au efectuat de asemenea două seturi de teste, primul cu datele stocate în memoria principală şi al doilea set de teste pentru date stocate pe hard disc. Fiecare test a fost repetat de un milion de ori. Rezultatele testelor au fost comparate cu datele din literatura de specialitate cât şi rezultatele testelor efectuate pe sisteme de calcul cu procesoare seriale. Pentru ambele seturi de teste, cu date stocate în memorie, respectiv cu datele de intrare stocate pe hard disc s-au obținut rezultate net inferioare, în cazul utilizării procesoarelor grafice față de cazul utilizării procesoarelor clasice. În unele cazuri rezultatele au fost peste aşteptări. Astfel, dacă în literatura de specialtate se preconiza o accelerare a performanțelor de peste 14,5 ori mai bună, în cazul soluțiilor adoptate de către autorul lucrării s-au obținut rezultate mai bune cuprinse între 2 până la 134 de ori mai bune, în funcție de mărimea datelor de intrare.

Ultimul capitol al tezei prezintă concluziile finale, contribuțiile personale şi perspective de continuare a cercetării în direcția tezei. Având în vedere că o mare parte

din contribuțiile aduse de către autor au fost evidențiate pe parcursul analizei tezei, în continuare se prezintă o sinteză a acestora.

- Evaluarea performanțelor a 11 algoritmi criptografici, cei mai reprezentativi, pentru două seturi de date de intrare stocate în memoria principală a calculatoarelor, respectiv pe hard disc;
- Evaluarea performanțelor algoritmilor criptografici pe mai mult sisteme de calcul având procesoare cu performanțe diferite;
- Testatea şi evaluarea algoritmilor criptografici pe mai multe medii de dezvoltare şi utilizând mai multe sisteme de operare;
- Propunerea unor soluții privind accelerarea performanțelor algoritmilor criptografici prin utilizarea prelucrării paralele a procesului de criptare;
- Adaptarea algoritmului AES pentru a fi implementat pe un procesor grafic (GPU);
- Adoptarea modului de prelucrare paralelă Counter Mode (CTR) în comparație cu soluția clasică descrisă în literatură şi anume Electronic Codebook – ECB;
- Verificarea soluțiilor propuse pe baza testelor efectuate asupra algoritmului AES paralel implementat pe un GPU, în vederea accelerării procesului de criptare/decriptare.
- Efectuarea a două seturi de teste pentru algoritmul AES pentru date socate în memoria principală, respectiv pe hard disc. Soluțiile alese au fost pe baza tabelelor de căutare, respectiv pe baza executării operațiilor aritmetice;