AES-Decryption using a FPGA platform

Rapailă Vlad

Rezumat

Scopul lucrării presupune decriptarea unor texte/mesaje, acestea fiind criptate folosind algoritmul Rijndael sau mai bine zis AES.
Algoritmul AES (Advanced Encryption Standard) este cel mai cunoscut algoritm criptografic cu cheie secretă. Criptarea cu cheie secretă (SKC) foloseşte o singură cheie atât pentru criptare cât şi pentru decriptare. Expeditorul utilizează cheia pentru criptarea textului clar şi trimite textul criptat destinatarului. Destinatarul aplică aceeaşi cheie în scopul decriptării mesajului şi recuperează textul clar. Pentru că procedeul face uz de o singură cheie, acest procedeu mai este numit şi criptarea simetrică.
Algoritmul AES descriere:

Specificatia AES este un algoritm de criptare pe blocuri în care lungimea blocului și a cheii puteau fi independente, de 128 de biți, 192 de biți, sau 256 de biți. Specificația AES standardizează toate cele trei dimensiuni posibile pentru lungimea cheii, dar restrictionează lungimea blocului la 128 de biți. Astfel, intrarea și ieșirea algoritmilor de criptare și decriptare este un bloc de 128 de biți.

Descrierea problemei studiate

Operațiile AES sunt definite sub formă de operații pe matrice, unde atât cheia, cât și blocul sunt scrise sub formă de matrice. La începutul rulării cifrului, blocul este copiat într-un tablou denumit stare , primii patru octeți pe prima coloana, apoi următorii patru pe a doua coloană, și tot așa până la completarea tabloului.

În procedeul de decriptare al textului criptat, toții pașii folosiți la procesul de criptare sunt inversați în afară de ultimul pas numit AddRoundKey. Operația AddRoundKey fiind folosită atât pentru procesul de criptare cât și pentru cel de decriptare. Userul este rugat să ofere textul ce a fost criptat dar și cheia folosită în procesul de criptare a datelor. Odată oferite aceste informații, un modul de expandare a cheii începe expandarea cheii originale pentru a fi îndeajuns de mare pentru toate rundele de criptare. Dupa ce cheia a fost expandată procesul de decriptare poate incepe. În prima runda se face un XOR între data de intrare și cheia originală iar rezultatul este stocat într-un registru intermediar. După această rundă încep să se execute și rundele rămase.
Datele din registrul intermediar sunt citite și sunt aplicate la 4 Mux-uri de 32 de biți, de aici în funcție de selecție, datele sunt procesate de câte un S-box inversat, acesta va transforma datele și le va trimite mai departe procesului de AddRound.
În procesul de AddRoundKey există deja un input de 32 de biți de la cheie. Se face un Xor între acești 32 de biți și cei 32 de biți primiți de la procesul precedent, rezultatul acestei operații fiind transmis mai departe în procesul denumit Inverse Mix Column. În acest procedeu se înmulțesc cei 32 de biți primiți cu o matrice standard pentru a obține o ieșire care va fi stocată la rândul ei în registrul intermediar.
În ultima rundă etapa de Inverse Mix Column este sărită și rezultatul din AddRoundKey este stocat într-un output.

Implementarea algoritmului pentru decriptarea AES este implementată pe o placa FPGA (Field Programmable Gate Array). Aceasta este un circuit integrat digital configurabil, de către utilizator. Configurarea făcându-se prin intermediul unui limbaj de descriere hardware.