UNIVERSITETI I PRISHTINES FAKULTETI I SHKENCAVE MATEMATIKO-NATYRORE

Tema: Gjenerimi i qelsave tek AES i thjeshtuar

Lënda: Siguria e te dhenave

Punoi: Florian Shabani, Jon Sadikaj, Syard Dauti

Permbajtja:

Abstrakti:
Ky punim synon të thjeshtësojë algoritmin Advanced Encryption Standard (AES) duke përdorur qëllimisht qeleshe 32-bit në vend të celsave standard 128-bit. Punimi synon të përdorë një lloj AES me celsa 32-bit në vend të AES standarde me qeleshe 128-bit. Për ta bërë këtë, është zhvilluar një metodë thjeshtësimi të AES që do të reduktojë madhësinë e qelesit nga 128-bit në 32-bit. Gjithashtu diskutojme për mënyrën e gjenerimit të celsave të 7 rundeve të enkriptimit te AES të thjeshtuar

1.Definimi i detyrës

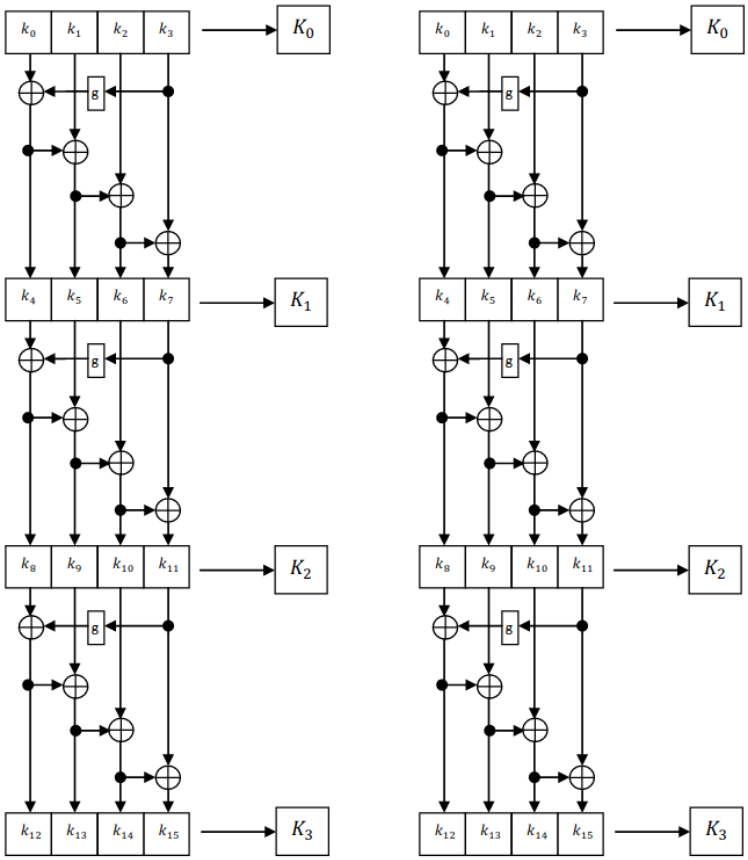
Përshkrimi i problematikës së ndryshimit të AES thjeshtësuar që ka një gjatësi çelësi prej 16 në një me gjatësi çelësi prej 32 është në thelb problemi i zgjerimit të madhësisë së çelësit të kriptografisë. AES-i i thjeshtësuar origjinal me një madhësi çelësi prej 16 bajtësh është projektuar për të siguruar një nivel të caktuar sigurie kundër sulmeve, ndërsa ndryshimi i madhësisë së çelësit në 32 bajta do të rritej teorikisht sigurinë e cifrës.

Megjithatë, ndryshimi i madhësisë së çelësit të algoritmës nga 16 në 32 bit nuk është një detyrë triviale, pasi kjo përfshin ndryshime në algoritmin e zgjerimit të çelësit dhe funksionin e rundeve të cifrës. Këto ndryshime duhet të sigurojnë që algoritmi irezultuese mbetet i sigurt dhe që çelësi i zgjeruar ofron përmasa të mjaftueshme të rastësisë dhe shpërndarjes.

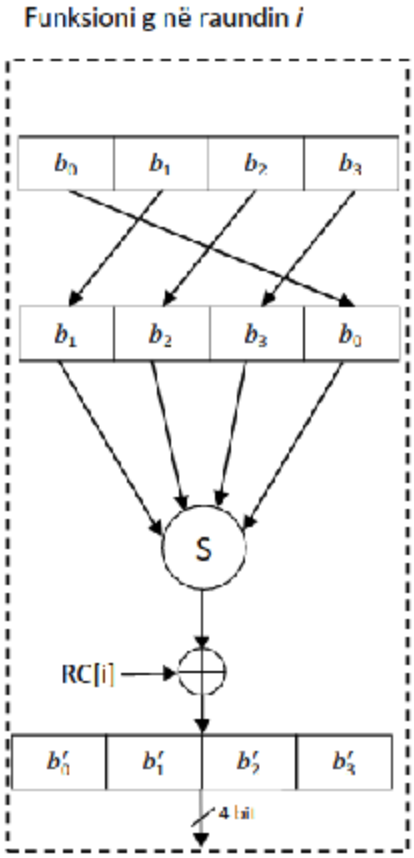
Për më tepër, rritja e madhësisë së çelësit të cifrës mund të ndikojë edhe në performancën dhe efikasitetin e saj, pasi madhësitë e mëdha të çelësve shpesh kërkojnë më shumë burime kalkulimi dhe kohë më të gjatë për të kriptuar dhe dekriptuar.

Për rrjedhojë, problematika e ndryshimit të madhësisë së çelësit të AES-it të thjeshtësuar nga 16 në 32 është një problem kriptografik kompleks që kërkon analizë, projektim dhe testime të kujdesshme për të siguruar sigurinë dhe efikasitetin e cifrës së rezultuar.

2.Procesi i gjenerimit te celsave



Procesi i ndryshimit të celsave nga 16 bit në 32 bit mbetet tejet i ngjajshem. Procedura e gjenerimit mbeten e njejte, ku së pari bëhet ndarja e bitve ne grupe me 4, gu secili grup gjeneron një celës. Menyra se si gjenerohet ky cels bëhet duke XOR në mënyrë sekuenciale celsat paraprak dhe të ardhshëm, gjithashtu duke aplikuar funksionin g në secilin celës të gjeneruar.



$$RC[1] = x^0 = (0001)_2$$
$$RC[2] = x^1 = (0010)_2$$
$$RC[3] = x^2 = (0100)_2$$

Funksioni g

Funksioni g ka nje rendesi mjafte te veqante ne gjenerimin e celsave dhe perdoret ne secilin round te gjenerimit te subcelsave.Implementimi i funksionit g behet ashtu qe fillimisht behet rrotullimi i fjales per nje byte ne te majte.Pas rrotullimit aplikohet S-AES S-box qe eshte zevendesim fiks i shifrave.Figura 3,paraqet S_Box qe perdoret ne S-AES

Nibbles	00	01	10	11
00	9	4	A	B
01	D	1	8	5
10	6	2	0	3
11	C	E	F	7

Figura 3.S-Box Simplified AES

Pas keti veprimi rezultati behet XOR me nje round konstant qe derivon nga nje vlere fikse dhe numri i tanishem i roundit.