



UNIVERSIDADE DO ESTADO DO RIO DE JANEIRO
Centro de Tecnologia e Ciências
Faculdade de Engenharia
Departamento de Engenharia de Sistemas e Computação

Arquiteturas de Computadores

Prof^a. Luiza de Macedo Mourelle

Pesquisa

Arquitetura Pipeline para Implementação do Sistema Criptográfico AES

Aluno:

Email:

mês/ano

1. Introdução

O sistema criptográfico Advanced Encryption Standard (AES) especifica um algoritmo criptográfico, aprovado como padrão pelo National Institute of Standards and Technology (NIST), que pode ser usado para proteger dados eletrônicos. O algoritmo AES é um cifrador de bloco simétrico que pode criptografar e decifrar informação. O AES especifica o algoritmo de Rijndael, um cifrador de bloco simétrico que pode processar bloco de dados de 128 bits, utilizando chaves cifradoras de 128, 192 e 256 bits. Rijndael foi projetado para tratar tamanhos de bloco e de chaves adicionais, mas eles não são adotados neste padrão. De acordo com o tamanho da chave, o algoritmo recebe o nome AES-128, AES-192 e AES-256. A entrada e a saída do algoritmo AES consistem, cada uma, de sequências de 128 bits. Essas sequências serão referidas como blocos. A entrada, saída e chave cifradora são processadas como arranjos de bytes. Internamente, as operações do algoritmo AES são realizadas num arranjo de bytes de duas dimensões chamado State. O State consiste de quatro linhas de bytes, cada uma contendo Nb bytes, onde Nb é o tamanho do bloco dividido por 32. No arranjo State denominado pelo símbolo s, cada byte tem dois índices, com sua linha r no intervalo $0 \leq r < 4$ e sua coluna c no intervalo $0 \leq c < Nb$. Isto permite que um byte do State seja referenciado ou como sr,c ou s[r,c]. O cifrador é descrito em pseudo-código no Algoritmo Cipher, abaixo. As transformações individuais – SubBytes(), ShiftRows(), MixColumns() e AddRoundKey() – processam o State. Na Seção 2, será descrito o modelo de cada component, juntamente com a respectiva validação funcional. Na Seção 3, serão apresentadas as informações necessárias à utilização do simulador.

```
Algoritmo Cipher (byte in [4*Nb], byte out [4*Nb], word w[Nb *
(Nr + 1)])
begin
    byte State [4,Nb]
    State = in
    AddRoundKey (State, w[0, Nb - 1])
    for round = 1 step 1 to Nr - 1
        SubBytes (State)
        ShiftRows (State)
        MixColumns (State)
        AddRoundKey (State, w[round * Nb, (round + 1) * Nb -
1])
    end for
    SubBytes (State)
    ShiftRows (State)
    AddRoundKey (State, w[Nr * Nb, (Nr + 1) * Nb - 1])
    out = State
end
```

2. Descrição do trabalho

Pesquise e apresente uma descrição sobre a implementação em *hardware* do AES, baseada em *pipeline*. O relatório deverá conter a arquitetura proposta, identificando os estágios correspondentes. Caso seja interessante, subdivida o relatório em sub-seções. Inclua, no texto, as referências utilizadas. O relatório deverá ter em torno de 5 páginas.

3. Conclusão

Faça uma análise sobre o que entendeu da arquitetura estudada. Utilize a folha anterior como folha de rosto do seu trabalho e substitua esta segunda folha pelo seu relatório, mantendo a estrutura apresentada. Boa sorte!

4. Referências

Inclua outras referências que tenha utilizado.

- [1] Federal Information Processing Standards Publications, Advanced Encryption Standard (AES), National Institute of Standards and Technology (NIST), Novembro, 2001.
- [2] J. Daemen e V. Rijmen, AES Proposal: Rijndael, AES Algorithm Submission, Setembro, 1999.
- [3] J. Nechvatal et. al., Report on the Development of the Advanced Encryption Standard (AES), National Institute of Standards and Technology, <http://www.nist.gov/CryptoToolkit>, Outubro, 2000.