UNIVERSIDADE DO ESTADO DO RIO DE JANEIRO
Centro de Tecnologia e Ciências
Faculdade de Engenharia
Programa de Pós-Graduação em Engenharia Eletrônica

Arquiteturas de Alto Desempenho

Projeto

Arquitetura Pipeline para Implementação do Sistema Criptográfico AES

Profª. Luiza de Macedo Mourelle

email: ldmm@eng.uerj.br

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 decriptografar 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 seqüências de 128 bits. Essas seqüências 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 <= r < 4 e sua coluna c no intervalo 0 <= 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 abaixo. As transformações individuais – SubBytes(), ShiftRows(), MixColumns() e AddRoundKey() – processam o State.

```
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
```

Bibliografia

[1] Federal Information Processing Standards Publications, Advanced Encryption Standard (AES), National Institute of Standards and Technolgy (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.