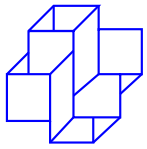
Aplicações de $GF(2^8)$ no algoritmo AES

Raquel de Araujo de Souza
Fábio Borges de Oliveira
Laboratório Nacional de Computação Científica
{rasouza,borges}@lncc.br



1. Introdução

O algoritmo de criptografia AES *(Advanced Encryption Standard)*, conhecido também como Rijndael [Daemen and Rijmen 2002], trabalha sobre o Corpo de Galois $GF(2^8)$. Todas as operações matemáticas utilizadas são realizadas sobre este corpo, construído a partir do polinômio irredutível $m(x) = x^8 + x^4 + x^3 + x + 1$.

2. $GF(2^8)$ no algoritmo AES

Todas as etapas, exceto a **ShiftRows**, que é um rotacionamento circular dos bytes do estado, utilizam os conceitos algébricos de corpos finitos [Klima et al. 2000], usando o corpo $GF(2^8)$.

SubBytes - Consiste em uma substituição dos bytes do estado por outros contidos em uma caixa de substituição (S-box). A S-box do Rijndael (S_{RD}) é gerada pela composição de duas funções f e g, tais que

$$g(a) = a^{-1} \text{ e } f(a) = b,$$

onde

$$\begin{aligned} b_i &= a_i \oplus a_{(i+4) \bmod 8} \oplus a_{(i+5) \bmod 8} \\ &\oplus a_{(i+6) \bmod 8} \oplus a_{(i+7) \bmod 8} \oplus c_i. \end{aligned}$$

Acima, c_i é o i-ésimo bit do byte 63h = 01100011. Sendo a um byte qualquer do estado, temos:

$$S_{RD}[a] = f(g(a)).$$

A operação inversa da SubBytes chama-se **InvSubBytes** e usa uma S-box inversa (S_{RD}^{-1}). Temos

$$S_{RD}^{-1}[b] = g^{-1}(f^{-1}(b)) = g(f^{-1}(b)),$$

onde $f^{-1}(b) = b'$ e

$$\begin{aligned} b'_i &= b_{(i+2) \bmod 8} \oplus b_{(i+5) \bmod 8} \\ &\oplus b_{(i+7) \bmod 8} \oplus d_i. \end{aligned}$$

Acima, d_i representa o $i-$ésimo bit do byte 05h = 00000101.

MixColumns - Pode ser representada como uma multiplicação de matrizes, onde os elementos do estado são considerados polinômios sobre $GF(2^8)$. Multiplica-se a matriz fixa

$$C = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix}$$

pela matriz S que representa o estado inicial, e obtemos o estado cifrado S', ou seja,

$$S' = C \odot S,$$

onde $\odot$ é o produto matricial em $GF(2^8)$, ou seja, a multiplicação é feita módulo $m(x)$ e a soma corresponde ao XOR. A operação inversa de MixColumns é chamada **InvMixColumns** e consiste na multiplicação da matriz fixa

$$C^{-1} = \begin{bmatrix} 0E & 0B & 0D & 09 \\ 09 & 0E & 0B & 0D \\ 0D & 09 & 0E & 0B \\ 0B & 0D & 09 & 0E \end{bmatrix},$$

que é a inversa de C, pelo estado cifrado S', voltando ao estado inicial S, isto é,

$$S = C^{-1} \odot S'.$$

AddRoundKey - É um XOR byte a byte entre o estado e a chave de rodada. Isto quer dizer que se $s_{x,y}$ é um byte do estado S e $k_{x,y}$ um byte da chave, o byte $s'_{x,y}$ do novo estado S' será igual a $s_{x,y} \oplus k_{x,y}$. A transformação inversa à AddRoundKey também consiste em um XOR entre o estado e a chave de rodada, ou seja, AddRoundKey é sua própria inversa, visto que $(s_{x,y} \oplus k_{x,y}) \oplus k_{x,y} = s_{x,y}$.

3. Conclusões

Este trabalho apresentou as aplicações de $GF(2^8)$ no algoritmo criptográfico AES, servindo de motivação ao estudo dos corpos finitos e mostrando sua importância na área de criptografia.

Referências

Daemen, J. and Rijmen, V. (2002). *The design of Rijndael: AES — The Advanced Encryption Standard*. Springer-Verlag.

Klima, R. E., Sigmon, N., and Stitzinger, E. (2000). *Applications of abstract algebra with Maple*. CRC Press, Boca Raton, FL.

Agradecemos ao apoio financeiro oferecido pelo PIBIC/CNPq.