Matrizes de Hardamard como Transformações Armadilhas Aplicadas em um Criptossistema de Chave Pública Baseado no Problema da Mochila

Polyane Alves Santos, Yuzo Iano, Lucas Gomes S. Silva & Domingos T. S. Neto

IFBA, UNICAMP & USP

polyane@ifba.edu.br

Resumo

O presente trabalho apresenta os resultados obtidos a partir da utilização de as matrizes de Hadamard como transformações armadilhas para códigos ótimos de memória unitária com taxas $R = 2/4$ e $R = 2/8$, respectivamente, no sistema criptográfico de chave pública que, ao serem aplicadas às submatrizes reduzem a capacidade de correção de erros do código. Este processo proporciona um aumento no grau de privacidade da informação enviada devido a dois fatores: para a determinação de códigos ótimos de memoria unitária é necessário resolver o Problema da Mochila e a redução da capacidade de correção de erro dos códigos[1].

Introdução

O sistema criptográfico de chave pública que faz uso do método do Problema da Mochila aqui atrabalhado é baseado nos códigos convolucionais clássicos de memória unitária [2], onde busca-se explorar todo seu grau de complexidade inerente ao processo de determinação de códigos ótimos e ao processo de decodificação. As funções armadilhas são transformações aplicadas às submatrizes geradoras do código, G_0 e G_1, com a finalidade de reduzir o poder de correção deste código a um valor desejado. Este processo proporciona um aumento no grau de privacidade da informação a ser enviada devido a dois fatores: para a determinação de códigos otimos de memória unitária é necessário resolver o Problema da Mochila e a redução da capacidade de correção de erro dos códigos ocasionada pelo embaralhamento das colunas das submatrizes geradoras [1].

A Matriz de Hadamard é uma matriz quadrada de ordem $n \times n$ composta de $+1'$s e $-1'$s tal que $HH^T = nI$. Em outras palavras, o produto interno de duas linhas distintas de H é zero, ou seja, linhas distintas são ortogonais e o produto interno de qualquer linha com ela mesma é n. Dado que $H^{-1} = (1/n)H^T$, temos também que $H^T H = nI$, e deste modo as colunas tem as mesmas propriedades. Se trocarmos $+1$ por 0 e -1 por 1 conduz a uma matriz de Hadamard binária de ordem$n$ e, é nesta forma que utilizaremos ao longo deste trabalho.

Nas tabelas aqui apresentadas, todas as matrizes, as transformações armadilha e as submatrizes geradoras, estão representadas na forma octal, onde cada linha da matriz é separada por dois pontos$(:)$. Como exemplo, considere a seguinte matriz:

$$G_0 = \left[13 : 03 : 06\right]$$

Sua representaçãoo octal é dada por,

$$G_0 = \begin{bmatrix} 1\,0\,1\,1 \\ 0\,1\,1\,0 \\ 0\,0\,1\,1 \end{bmatrix}$$

Resultados

O procedimento utilizado foi aplicar as transformações armadilhas A e B em cada submatriz geradora, G_0 e G_1 separadamente, obtendo novas submatrizes G'_0 e G'_1, da seguinte forma:

$$G'_0 = AG_0B \quad e \quad G'_1 = AG_1B.$$

Os resultados são apresentados nas tabelas e . Para o código de memória unitária $(4, 2, 1)$, com taxa $R = 2/4$ e matriz geradoras dadas por $G_0 = 15 : 3$ e $G_1 = 14 : 07$, o d_{free} obteve uma considerável redução de 5 para 2 independentemente de qual seja a transformação armadilha A. Porém apesar de ter alcançado o objetivo de redução da capacidade de correção, todos os códigos obtidos tiveram uma redução na dimensão do espaço de operação, pois uma ou mais colunas das submatrizes G'_0 e G'_1 são nulas. Outro fato observado, é que dois dos três códigos resultantes são códigos de memória unitária parcial.

A	B	G'_0	G'_1	d_{free}	$d'free$
A	B	G'_0	G'_1	d_{free}	$d'free$
A_1	H_4	$03 : 05$	$05 : 00$	5	2
A_2		$06 : 05$	$05 : 00$	5	2
A_3		$03 : 06$	$05 : 05$	5	2

Tabela 1: Transformação Hadamard de ordem 4, Código de taxa $r = 2/4$

O mesmo padrão ocorre com o código convolucional de memória unitária $(8, 2, 1)$, com taxa $R = 2/8$ e as matrizes geradoras $G_0 = (370 : 037)$ e $G_1 = (174 : 237)$ o qual perde a capacidade de correção de erro resultando em um d_{free} menor que o do código original. Neste caso, a distância livre inicial era $d_{free} = 10$ e, após a aplicação das transformaçõees passou a ser $d'_{free} = 8$, indiferentemente de quais fossem as matrizes A e B. Neste caso, também ocorre uma redução na dimensão do espaço em todos os casos observados.

A	B	G'_0	G'_1	d_{free}	$d'free$
A_1	H_8	$360 : 231$	$252 : 146$	10	8
A_2		151:231	314:146	10	8
A_3		360:151	252:314	10	8
A_1	H_{p8}	232:321	306:056	10	8
A_2		113:321	350:056	10	8
A_3		360:151	252:314	10	8

Tabela 2: Transformação Hadamard de ordem 8, Código de taxa $r = 2/8$

Conclusão

A transformação armadilha aqui proposta, matriz de Hadamard, foi aplicada no criptossistema baseado no problema da mochila que utiliza códigos convolucionais de memória unitária e os resultados obtidos foram analisados. Foram obtidos bons resultados na redução da capacidade de correção de erros dos códigos com taxa $r = 2/4$ e$r = 2/8$, pois forneceram códigos com capacidade de correção menor que a dos códigs originais e concluimos que tais reduções são causadas pela aplicação da transformação B, já que a transformação A não apresentou influência no resultado.

Referências

[1] SANTOS, P. A. , *Uma proposta de um sistema criptográfico de chave pública utilizando códigos convolucionais clássicos e quânticos* , Campinas: UNICAMP,2008

[2] YOUNG, M. C. P.,*Obtenção de códigos convolucionais ótimos de memória unitária por programação matemática*. Campinas: UNICAMP, 1989