Construção de S-Boxes com Valores Ótimos de Não Linearidade Baseada em uma Relação entre o Multigrafo de Ramanujan e a Matriz da Transformação Afim

Marcio Prudêncio Belleza[1]
Fábio Borges[1]

[1] Laboratório Nacional de Computação Científica (LNCC)
25651-075, Petrópolis - RJ - Brasil

{mbelleza,borges}@lncc.br

Abstract. *A substitution box (S-Box) must have at least optimal values for non-linearity (NL), differential uniformity, and algebraic degree. According to the literature, a cryptographically strong S-Box must have $NL > 100$. Advanced Encryption Standard (AES) uses a non-singular binary matrix S to generate its S-Box. Several papers choose S from approximately 2^{62} non-singular matrices or construct S-Box randomly, without guaranteeing $NL > 100$. In this paper, we identify that S can be studied as an adjacency matrix ($A(G)$) of a Ramanujan multigraph, and verify this relationship with other rotational matrices $A(G)$. Thus, we reduced the search for S to the order of 10^{11} and construct S-Boxes with $NL > 100$.*

Resumo. *Uma S-Box (caixa de substituição) deve ter pelo menos valores ótimos para não linearidade (NL), uniformidade diferencial e grau algébrico. Segundo a literatura, uma S-Box criptograficamente forte deve ter $NL > 100$. O AES (Advanced Encryption Standard) usa uma matriz binária não singular S para construir sua S-Box. Muitos trabalhos escolhem S em aproximadamente 2^{62} matrizes não singulares ou constroem S-Box aleatoriamente, sem garantir $NL > 100$. Neste trabalho, identificamos que S pode ser estudada como uma matriz de adjacência ($A(G)$) de um multigrafo de Ramanujan e verificamos esta relação com outras $A(G)$ do tipo rotacionais. Dessa forma, reduzimos a busca por S para a ordem de 10^{11} e construímos S-Boxes com $NL > 100$.*

1. Introdução

[Shannon 1949] introduziu dois princípios fundamentais que constituem a base de sistemas criptográficos: confusão e difusão. Segundo [Paar and Pelzl 2010], confusão é uma operação de encriptação onde a relação entre a chave e o texto cifrado é ocultada; e difusão é uma operação de encriptação onde a influência de um bit do texto simples é espalhada para muitos bits do texto cifrado para esconder as propriedades estatísticas do texto simples. O AES (ver [Daemen and Rijmen 2002]) usa substituição (S-Box) para alcançar a confusão [Paar and Pelzl 2010]. A S-Box do AES é uma função Booleana definida em um corpo de Galois (GF). Para [Carlet 2010], a confusão está intimamente relacionada com a complexidade das funções Booolenas envolvidas. A resistência dos sistemas criptográficos aos ataques conhecidos pode ser quantificada através de algumas características fundamentais (algumas, mais relacionadas com a confusão, e algumas, mais relacionadas

com a difusão) das funções Booleanas usadas neles [Carlet 2010]. Portanto, os ataques contra estes sistemas exigem um estudo profundo das funções Booleanas para uma criptografia mais segura.

O número de funções Boolenas de n variáveis é 2^{2^n}, o que torna muito difícil encontrar funções com boas propriedades criptográficas. Portanto, para evitar a verificação de todas as funções, aplica-se qualquer relação de equivalência sob a qual as propriedades envolvidas são invariantes [Canteaut 2016]. Uma S-Box com boas propriedades criptográficas pode garantir que a cifra resista contra uma variedade de métodos de criptoanálise. Portanto, quaisquer deficiências da S-Box enfraquecerão a segurança da cifra [Cui et al. 2011]. Aplicações criptográficas de funções Booleanas são influenciadas por muitas propriedades da S-Box [Carlet 2010], das quais, segundo [Isa et al. 2016], uma S-Box criptograficamente forte deve ter pelo menos valores ótimos nas seguintes propriedades: não linearidade ($NL > 100$), uniformidade diferencial ($2 \leqslant \delta \leqslant 6$) e grau algébrico ($AD \geq 4$). A teoria de funções não lineares perfeitas (ou funções $bent$) tem implicações interessantes em criptografia [Meier and Staffelbach 1990]. Porém, as funções $bent$ não são balanceadas [Stănică 2007]. No entanto, segundo [Meier and Staffelbach 1990], uma estratégia razoável será encontrar funções não lineares quase perfeitas que satisfaçam critérios adicionais de projeto criptográfico como, por exemplo, o balanceamento. A maioria das aplicações criptográficas usa funções Booleanas balanceadas [Canteaut 2016]. Para investigar algumas propriedades criptográficas da função Booleana f, [Stănică 2007] considerou o grafo de Cayley associado a f. [Davidoff et al. 2003] apresentaram uma relação entre o grafo de Cayley e o grafo de Ramanujan.

Segundo [Stănică 2007], o grafo de Cayley associado à função $bent$ é sempre um grafo de Ramanujan. Mostramos neste trabalho que a função do AES não é $bent$ (ver 2.2). Porém, o grafo associado à matriz S da transformação afim, que gera a S-Box do AES, é um multigrafo de Ramanujan. O grafo de Ramanujan é um grafo de expansão ótima, isto é, caminhos relativamente curtos no grafo de expansão se aproximam da distribuição uniforme e são frequentemente usados como uma boa fonte de aleatoriedade na ciência da computação [Costache et al. 2018]. Para estes autores, a importância desses grafos para a criptografia está na dificuldade de encontrar caminhos neles: não há algoritmo subexponencial conhecido para resolver este problema, seja classicamente ou em computador quântico. De fato, um exemplo de grafo de Ramanujan, conhecido como grafo de isogenia supersingular, está sob consideração do NIST (National Institute of Standards and Technology) para um padrão de criptografia pós-quântica [Costache et al. 2018]. Portanto, encontrar uma relação entre o grafo associado à S-Box do AES e o grafo de Ramanujan contribui para a construção de S-Boxes seguras.

Para mostrar a relação da matriz binária da transformação afim do AES com o grafo de Ramanujan, apresentamos na seção 2 conceitos para uma melhor compreensão sobre funções Booleanas, S-Box do AES e grafo de Ramanujan. Na seção 3, apresentamos trabalhos relacionados. Na seção 4, apresentamos a relação entre a S-Box do AES e o grafo de Ramanujan. Na seção 5, apresentamos uma comparação com trabalhos relacionados e suas respectivas matrizes binárias com o grafo de Ramanujan. Na seção 6, apresentamos a vantagem da relação encontrada para escolher S-Boxes mais seguras e trabalhos futuros.

2. Conceitos Básicos

Esta seção introduz funções Booleanas, a S-Box do AES e grafo de Ramanujan.

2.1. Funções Booleanas

Uma função Booleana é um mapa $f : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^m$. Considerando $m = 1$ neste parágrafo, a função pode ser representada pelo vetor binário v_f de comprimento 2^n. O peso de Hamming (H_w) de f é definido pela quantidade de 1 (uns) em v_f. A função f é balanceada se e somente se $H_w = 2^{n-1}$ [Canteaut 2016]. O número total de funções balanceadas é $\binom{2^n}{2^{n-1}}$. A distância de Hamming (H_d) entre dois vetores binários com mesmo comprimento é o número de posições para os quais as entradas correspondentes são diferentes, por exemplo, sejam $x_1 = (1, 0, 1)$ e $x_2 = (0, 1, 1)$, a distância de Hamming entre estes dois vetores é 2 (dois) porque são diferentes na primeira e segunda posições. A não linearidade (NL) de uma função f no conjunto de todas as funções Booleanas ($\mathbb{B}$) é definida como H_d mínima entre f e toda função linear em $\mathbb{B}$. Em geral, $NL(f) \leqslant 2^{n-1} - 2^{n/2-1}$, onde n é par. Uma função f é $bent$ quando $NL(f) = 2^{n-1} - 2^{n/2-1}$. A uniformidade diferencial (δ) de uma função f, de $\mathbb{F}_2^n \rightarrow \mathbb{F}_2^m$, é definida como $\delta(f) = max\{x \in \mathbb{F}_2^n : f(x + a) + f(x) = b\}$, com $a \in \mathbb{F}_2^n$, $b \in \mathbb{F}_2^m$ e $a \neq 0, b$. O grau algébrico (AD) de uma S-Box é o grau máximo de todas as suas funções componentes, onde o grau de uma função componente é o número de variáveis no maior monômio desta componente. Uma S-Box é um mapa $f : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^m$ constituído por um conjunto de m funções Booleanas. Encontrar funções Booleanas balanceadas e altamente não lineares (como funções $bent$) é um problema muito difícil e de grande importância para a construção de S-Boxes.

2.2. S-Box do AES

As S-boxes são comuns em cifras de bloco, altamente não lineares e "guardam" muito da segurança destas cifras [Nover 2005]. O AES é uma cifra de bloco baseada na cifra de Rijndael e adotado como padrão de criptografia pelo governo dos EUA. O AES foi publicado pelo NIST em 2001 para substituir o DES (Data Encryption Standard). As implementações do AES usam bloco de tamanho fixo de 128 bits com a chave podendo ter tamanhos de 128, 192 e 256 bits. O AES realiza 10, 12 e 14 rodadas (dependendo do tamanho da chave) para criptografar cada bloco de dados. Em cada rodada, quatro transformações são aplicadas no bloco, são elas: SubBytes, ShiftRows, MixColumns e AddRoundKey. Neste trabalho, nosso interesse é na SubBytes, constituída por uma transformação afim envolvendo uma matriz binária não singular S, de ordem 8. A quantidade de matrizes S, de ordem n, é igual ao número de combinações possíveis de vetores binários linearmente independentes. Portanto, a quantidade de matrizes não singulares S, de ordem n, é $\prod_{i=0}^{n-1}(2^n - 2^i)$. A transformação SubBytes é formada por duas etapas: 1) determinar o inverso multiplicativo em $GF(2^8)$ usando o polinômio irredutível $x^8 + x^4 + x^3 + x + 1$; 2) aplicar a transformação afim $z = Sy + c$, que também pode ser dada por $z = (x^7 + x^6 + x^2 + x) + y(x^7 + x^6 + x^5 + x^4 + 1) \mod (x^8 + 1)$. A matriz S é rotacional referente ao valor $0x1F$ ou 00011111. Este valor corresponde a primeira coluna de S, com o bit menos significativo igual ao elemento $s_{1,1}$ e o bit mais significativo igual a $s_{8,1}$. A segunda coluna é a rotação da primeira coluna deslocando um bit, isto é,

considerando o valor 00011111, cada bit é deslocado uma posição para a esquerda. Esta rotação é repetida para as outras colunas. Segundo [Klima and Sigmon 2016], a S-Box do AES, S-Box: $GF(2^8) \rightarrow GF(2^8)$, está associada à matriz binária S. Matricialmente, a transformação afim é dada por

$$\begin{bmatrix} z_0 \\ z_1 \\ z_2 \\ z_3 \\ z_4 \\ z_5 \\ z_6 \\ z_7 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} y_0 \\ y_1 \\ y_2 \\ y_3 \\ y_4 \\ y_5 \\ y_6 \\ y_7 \end{bmatrix} + \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix}. \quad (1)$$

A matriz S pode ser representada por $[8F, C7, E3, F1, F8, 7C, 3E, 1F]^T$. A função $F(x) = x^{2^n-2}$, com n par, é usada na S-Box do AES com $NL(F) = 2^{n-1} - 2^{n/2}$ [Carlet and Ding 2007]. Para $n = 8$, a S-Box do AES tem $NL(F) = 112$. Logo, F não é $bent$.

A matriz S constitui uma simples estrutura matemática que substitui a tabela 1 apresentada por [Klima and Sigmon 2016]. Esta estrutura é descrita pela fórmula $z = Sy + c$, onde $y = [y_0y_1y_2y_3y_4y_5y_6y_7]^T$, $c = [11000110]^T$ e $z = [z_0z_1z_2z_3z_4z_5z_6z_7]^T$.

Apresentamos uma aplicação da S-Box do AES, usando a tabela 1 no exemplo a seguir.

Tabela 1. S-Box do AES (em hexadecimal).

63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
D0	EF	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8
51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB
E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E
E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16

Exemplo 1: Considere o polinômio $x^5 + x^3 + x$. Podemos representar este polinômio por 00101010. Os quatro primeiros e os quatro últimos bits correspondem, respectivamente, às representações de inteiros que especificam a linha e a coluna na tabela

1, apresentada em [Klima and Sigmon 2016]. Isto é, o byte 00101010 determina linha 2 e coluna 10. Esta posição corresponde à entrada 229 na S-Box (linhas e colunas enumeradas de 0 a 15). O valor 229 (E5) é representado pelo byte 11100101, que representa o polinômio $x^7 + x^6 + x^5 + x^2 + 1$. Logo, a S-Box transformou $x^5 + x^3 + x$ em $x^7 + x^6 + x^5 + x^2 + 1$.

A transformação apresentada no exemplo 1 pode ser implementada pela estrutura formada pela matriz S, descrita pela equação 1.

Exemplo 2: Considere $f(x) = x^5 + x^3 + x$ (mesmo do exemplo 1). Inicialmente, aplicamos o algoritmo Euclidiano para determinar o inverso multiplicativo de $f(x)$ em $F = \mathbb{Z}_2/(p(x))$. Então, $f^{-1}(x) = x^7 + x^4 + x^3$ e sua representação binária é 10011000. Para $y = [00011001]^T$ obtemos $z = [10100111]^T$. Logo, o byte 11100101 representa o polinômio de saída $x^7 + x^6 + x^5 + x^2 + 1$.

Muitos dos critérios de difusão e não linearidade descritos na literatura de criptologia são apenas critérios que uma cifra de bloco deve satisfazer para ser segura. São condições necessárias para a segurança, mas não suficientes [Daemen and Rijmen 2002]. Neste trabalho, apresentamos uma condição que pode ser suficiente através de restrições matemáticas e busca exaustiva.

2.3. Grafo de Ramanujan

Analisamos a matriz S por meio de um grafo associado a ela. Um grafo G é um par ordenado (V, E), onde V é um conjunto não vazio de vértices e E é um conjunto, disjunto de V, de arestas. Para um grafo G, podemos associá-lo a uma matriz n x n conhecida como matriz de adjacência $A(G) = (a_{ij})$, onde a_{ij} é o número de arestas conectando o vértice v_i ao vértice v_j. O grau de um vértice v em G é o número de arestas de G incidentes com v, onde cada loop é contado como duas arestas. Um grafo G é k-regular se o grau de v é igual a k para todo $v \in V$. Um grafo direcionado D é um par ordenado (V, A) constituído de um conjunto não vazio V de vértices e um conjunto A, disjunto de V, de arcos, onde cada arco de D é um par ordenado de vértices de D. O arco associado a (v_i, v_j) é representado por uma seta saindo de v_i e apontando para v_j. Um grafo direcionado é dito balanceado se $d_e(v_i) = d_s(v_i)$, para todo $v_i \in V$, onde $d_e(v_i)$ e $d_s(v_i)$ são, respectivamente, os graus de entrada e de saída do vértice v_i. Para mais detalhes sobre grafos ver [Bondy 1976].

Um grafo de Ramanujan é um grafo k-regular satisfazendo $\lambda \leqslant 2\sqrt{k-1}$, onde λ é o máximo dos valores absolutos de todos os autovalores não triviais ($\pm k$) da matriz de adjacência associada ao grafo. Se este grafo tiver arestas múltiplas ou loops, então é chamado de multigrafo de Ramanujan. Consulte [Murty 2003] e [Lubotzky et al. 1988] para mais detalhes sobre grafos de Ramanujan.

O grafo de Ramanujan é um grafo de expansão. Grafos de expansão são grafos esparsos e possuem propriedades muito importantes, como baixo diâmetro, alta conectividade e alto número cromático [Tao 2015]. Para saber mais sobre grafos de expansão e suas aplicações consulte [Hoory et al. 2006]. Uma aplicação em criptografia pode ser encontrada em [Charles et al. 2009], onde apresentam a construção de funções hash resistentes à provável colisão a partir de grafos de expansão.

3. Trabalhos Relacionados

Recentemente, [de la Cruz Jiménez 2019] afirmou que a construção de S-Boxes com propriedades criptográficas próximas do ótimo é um problema em aberto. Ele apresentou um novo método para construir S-Boxes de dimensão $n = 2k$, com $k \geq 2$. Este método usa permutação polinomial sobre $GF(2^k)$ e permutações arbitrárias para a construção de uma função Booleana vetorial e sua inversa. A principal vantagem dessa construção é a realização de uma busca baseada na geração aleatória de permutações de k bits para encontrar S-Boxes de n bits com valores quase ótimos para propriedades criptográficas. A melhor S-Box encontrada tem $NL = 108$, $\delta = 6$ e $AD = 7$. Todas as S-Boxes encontradas pelo método não apresentaram suas respectivas matrizes da transformação afim.

[Das et al. 2013] geraram S-Boxes do AES usando o polinômio irredutível $\{11D\}$ e apresentaram 8 S-Boxes, selecionadas arbitrariamente, com as constantes aditivas de 8 bits $(0A, 31, 4A, 74, 9D, CA, D5$ e $F0)$. Eles observaram que estas escolhas podem melhorar a randomização nos textos cifrados, podendo prevenir a criptoanálise linear e diferencial. Porém, não apresentaram a não linearidade e sugeriram novos estudos para encontrar S-Boxes seguras.

Para gerar boas S-Boxes do AES, [Waqas et al. 2014] encontraram 46 S-Boxes com propriedades que garantem uma criptografia segura e confiável, substituindo somente a matriz da transformação afim por matrizes rotacionais com a primeira linha gerada aleatoriamente. Porém, apresentaram apenas 10 matrizes, escolhidas aleatoriamente e denotadas por A_n, com $n = 1, 2, ..., 10$. Para os autores, estas S-Boxes são boas porque satisfazem as seguintes propriedades: efeito avalanche, critério de independência de bit, critério de avalanche estrita e não linearidade. O software construído por eles também garante a geração de S-Boxes sem repetição de elementos, sem ponto fixo e algumas delas mais resistentes do que a S-Box original do AES.

Em sua tese, [Chandrasekharappa 2012] apresentou um AES modificado, substituindo a S-Box original por S-box dinâmica. Ele verificou que algumas S-Boxes dinâmicas alcançaram valor máximo de critério de avalanche, sem considerar o intervalo ótimo para a não linearidade ($NL > 100$). Em seu trabalho, também gerou função hash baseada na S-Box dinâmica e obteve resultados satisfatórios.

Para estudar o efeito da construção algébrica de S-Boxes em suas propriedades criptográficas, [Deva Sinha and Arya 2012] propuseram mudanças em cada componente da transformação afim do AES. Primeiro, apresentaram o efeito de cada um dos 30 polinômios irredutíveis (incluindo o do AES), de grau 8, em algumas propriedades da S-Box. Eles observaram que a escolha por um destes polinômios afeta propriedades criptográficas. Depois, eles apresentam o impacto da mudança da matriz binária da transformação nestas propriedades, sem considerar o efeito na não linearidade. Como a quantidade de matrizes é muito grande, uma pesquisa aleatória foi executada. Para isso, uma matriz binária de ordem 8 é aleatoriamente gerada. A matriz é descartada se for singular e outra matriz é gerada novamente. Este processo foi repetido 500 vezes em uma implementação em MatLab. Após este processo, três matrizes foram apresentadas com seus respectivos efeitos sobre parâmetros da S-Box. Porém, uma destas matrizes gerou uma S-Box com elementos repetidos. Finalmente, [Deva Sinha and Arya 2012] realizaram uma mudança na constante aditiva da transformação e observaram seu efeito somente na quantidade de pontos fixos na S-Box.

Para aumentar a complexidade e a segurança da S-Box do AES, [Cui et al. 2011] modificaram a transformação afim e adicionaram outra transformação afim. Eles apresentaram uma análise de desempenho e constataram, por exemplo, um aumento do período iterativo de 88 para 256. Ao comparar os resultados obtidos com a S-Box original do AES, [Cui et al. 2011] concluíram que a S-Box proposta tem melhor desempenho e pode ser facilmente aplicada ao AES.

4. Relação entre a S-Box do AES e o Grafo de Ramanujan

Nós afirmamos que se G_S é um multigrafo direcionado associado à matriz S do AES, então G_S é um multigrafo de Ramanujan.

Para vermos esta relação, considere que $A(G_S)$ é a matriz de adjacência de G_S. Como G_S é um grafo com loops e arestas múltiplas em todos os seus vértices (figura 1), então G_S é 5-regular ($d_e(v_i) = d_s(v_i)$) e o λ da matriz $A(G_S)$ satisfaz $\lambda = 2.4142 \leqslant 4$. Logo, G_S é um multigrafo de Ramanujan.

$$A(G_S) = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}$$

Como $d_e(v_i) = d_s(v_i) = 5$ para todo $v_i \in V$, então G_S é balanceado (ver figura 1).

Para gerar uma S-Box melhorada para implementação do AES, [Cui et al. 2011] mudaram a matriz da transformação afim. Vamos verificar se esta matriz, denotada por M, é uma matriz de adjacência de um multigrafo de Ramanujan.

A S-Box proposta por [Cui et al. 2011] pode ser representada pela matriz

$$M = \begin{pmatrix} 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$$

Seja G_M um multigrafo direcionado associado a matriz M e apresentado pela figura 2. A matriz de adjacência de G_M, denotada por $A(G_M)$, é diferente de $A(G_S)$. Porém, está associada ao 5-regular e satisfaz a definição de multigrafo de Ramanujan. Logo, G_M também é um multigrafo de Ramanujan. Verificamos que as matrizes S e M têm o mesmo polinômio característico $P(\lambda) = \lambda^8 - 8\lambda^7 + 24\lambda^6 - 64\lambda^5 + 114\lambda^4 - 104\lambda^3 +$

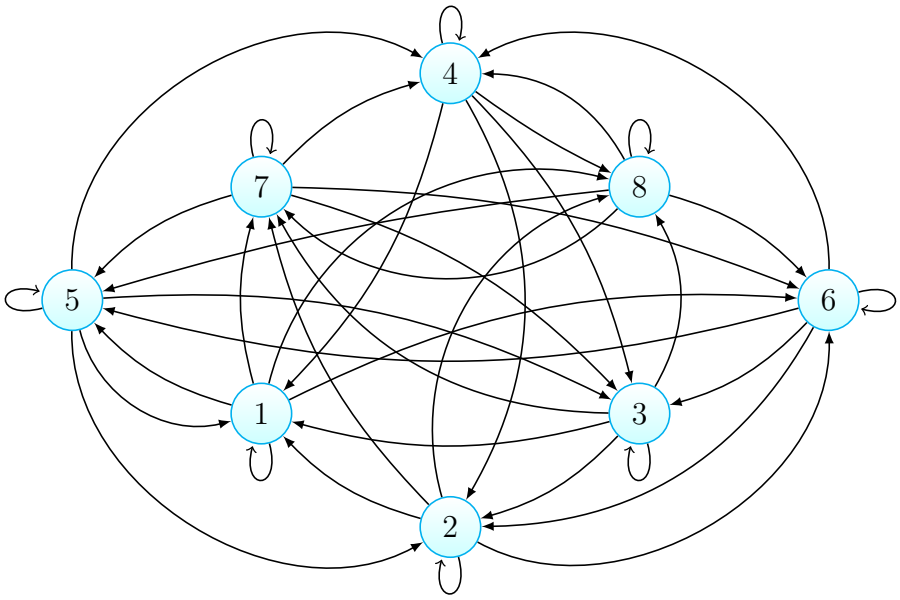

Figura 1. Multigrafo direcionado G_S.

$48\lambda^2 - 16\lambda + 5$. A S-Box proposta por [Cui et al. 2011] tem não linearidade igual a 112, mesmo valor da não linearidade da S-Box do AES. A matriz M também é rotacional.

No trabalho de [Chandrasekharappa et al. 2011], uma S-Box com 100% de critério de avalanche é apresentada, porém observamos que a sua matriz A não está associada ao grafo de Ramanujan. Estes autores consideram $[1B, 24, 37, 52, 6F, 92, DF]^T$ para formar a matriz A, a partir da qual a S-Box é gerada usando $c = B5$ e o polinômio irredutível $14D$. Segundo eles, a S-Box é projetada para fornecer um bom efeito de avalanche. Porém, não consideraram outras propriedades relevantes, tais como a não linearidade.

$$A = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 1 & 1 & 1 & 1 \end{pmatrix} \quad \text{e} \quad B = \begin{pmatrix} 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 \end{pmatrix}$$

A matriz B é uma matriz de adjacência de um multigrafo de Ramanujan. Porém, B é singular. Logo, ser uma matriz de adjacência de um grafo de Ramanujan não garante a construção de uma boa S-Box. Esta matriz deveria ser não singular.

Em sua tese de doutorado, [Chandrasekharappa 2012] apresentou quatro S-Boxes com suas respectivas matrizes binárias, denotadas neste trabalho por S_1, S_2, S_3 e S_4.

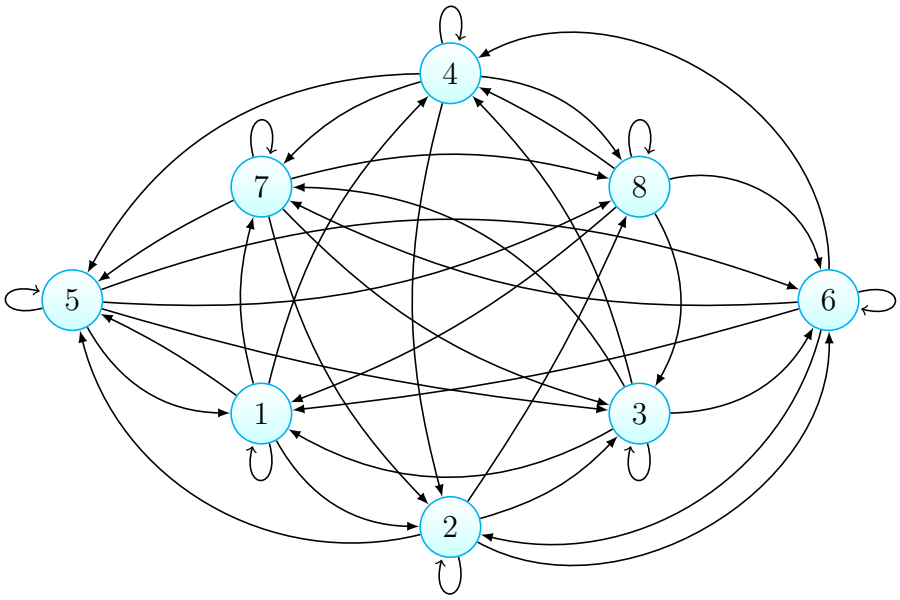

Figura 2. Multigrafo direcionado G_M.

$$S_1 = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \end{pmatrix} \quad \text{e} \quad S_2 = \begin{pmatrix} 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \end{pmatrix}$$

O polinômio irredutível usado para a S-Box associada à matriz S_1 é $x^8 + x^7 + x^3 + x^2 + 1$. Os autovalores absolutos de S_1 são $\{4.1160, 1.6138, 1.6138, 0.7196, 0.7196, 0.8034, 0.8034, 0.2791\}$. A S_1 não corresponde a uma matriz de adjacência de uma grafo de Ramanujan.

O polinômio irredutível usado para a S-Box associada à matriz S_2 é $x^8 + x^4 + x^3 + x + 1$. Os autovalores absolutos de S_2 são $\{4.3123, 1.2456, 1.2456, 1.2373, 1.4474, 1.4474, 0.9300, 0.9300\}$. A S_2 não corresponde a uma matriz de adjacência de um grafo de Ramanujan.

$$S_3 = \begin{pmatrix} 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 \end{pmatrix} \quad \text{e} \quad S_4 = \begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 1 & 0 & 1 & 1 \end{pmatrix}$$

O polinômio irredutível usado para a S-Box associada à ma-

triz S_3 é $x^8 + x^7 + x^3 + x^2 + 1$. Os autovalores absolutos de S_3 são $\{4.3406, 1.5602, 1.5602, 1.2884, 1.2884, 0.8081, 0.8081, 0.2619\}$. A S_3 não corresponde a uma matriz de adjacência de uma grafo de Ramanujan.

O polinômio irredutível usado para a S-Box associada à matriz S_4 é $x^8 + x^4 + x^3 + x + 1$. Os autovalores absolutos de S_4 são $\{4.7993, 1.8084, 1.7380, 1.2598, 1.2598, 0.8884, 0.2358, 0.1994\}$. A S_4 não corresponde a uma matriz de adjacência de uma grafo de Ramanujan.

Propomos algumas S-Boxes geradas por uma implementação escrita no software $SAGE$ [The Sage Developers 2009]. Nossos dados de entrada são: a matriz binária (S), o polinômio irredutível ($p(x)$) e a constante aditiva (c). Observamos que uma boa escolha de c evita qualquer ponto fixo na S-Box, isto é, $S\text{-Box}[a] = a$. A saída são dois vetores, um que determina a posição dos elementos da S-Box (de 0 a 255) e outro com estes elementos. As matrizes usadas na implementação são:

$$A_1 = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{pmatrix} \quad \text{e} \quad A_2 = \begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 \end{pmatrix}$$

A matriz A_1 está associada ao multigrafo 3-regular e a matriz A_2 está associada ao multigrafo 7-regular.

$$A_3 = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \end{pmatrix} \quad \text{e} \quad A_4 = \begin{pmatrix} 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \end{pmatrix}$$

As matrizes A_3 e A_4 não estão associadas a um k-regular. Estas matrizes foram geradas aleatoriamente por uma implementação proposta por [Deva Sinha and Arya 2012].

Realizando uma busca exaustiva, veja algoritmo 1, também analisamos matrizes de adjacência de multigrafos de Ramanujan que geraram S-Boxes com elementos repetidos. Esta repetição ocorreu porque as matrizes não eram rotacionais, como descrito para a matriz S do AES. Esta condição destaca a relevância da posição dos zeros e dos uns na matriz de adjacência para verificar se a matriz com k $1's$ em cada linha e coluna é também uma matriz rotacional. Portanto, o algoritmo 1 verifica apenas matrizes com k $1's$ em cada linha e coluna para construir S-Boxes com $NL > 100$. Estas matrizes devem ser rotacionais, não singulares e matrizes de adjacência de multigrafos de Ramanujan.

Como as matrizes estudadas neste trabalho são de ordem 8, a quantidade k de 1's em cada linha e coluna destas matrizes varia de 1 a 8. Para $k = 1$, não temos uma matriz

de adjacência de multigrafo de Ramanujan (1-regular). Para $k = 8$, a matriz é singular. Portanto, o algoritmo 1 testa somente matrizes de adjacência de grafos k-regulares, para $2 \leqslant k \leqslant 7$.

Data: matriz binária 8x8 com k 1's em cada linha e coluna, para $2 \leqslant k \leqslant 7$
Result: matriz binária 8x8 para construir S-Box com $NL > 100$

```
inicialização;
while a matriz binária for de adjacência do multigrafo de Ramanujan do
    if a matriz for rotacional then
        verifique se a matriz é não singular;
    else
        escolha outra matriz binária;
    end
end
```

Algoritmo 1: Teste para escolher S-Boxes com $NL > 100$

Vejamos três matrizes de adjacência associadas a multigrafos de Ramanujan que geraram S-Boxes com elementos repetidos. Destacamos os zeros e uns que tornaram a matriz não rotacional.

$$R_1 = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ \mathbf{0} & \mathbf{1} & 0 & 0 & 0 & 1 & 0 & 0 \\ \mathbf{1} & \mathbf{0} & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \end{pmatrix} \quad \text{e} \quad R_2 = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & \mathbf{0} & \mathbf{1} & 0 & 1 & 1 & 1 & 0 \\ 0 & \mathbf{1} & \mathbf{0} & 0 & 0 & 1 & 1 & 1 \end{pmatrix}$$

A matriz R_1 está associada ao multigrafo 2-regular. E a matriz R_2 está associada ao multigrafo 4-regular.

$$R_3 = \begin{pmatrix} 0 & 1 & 1 & 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 & 1 & 1 & \mathbf{1} & \mathbf{0} \\ 1 & 1 & 0 & 1 & 1 & 1 & \mathbf{0} & \mathbf{1} \end{pmatrix}$$

A matriz R_3 está associada ao multigrafo 6-regular.

5. Comparação com Trabalhos Relacionados

A tabela 2 mostra duas propriedades relevantes que estão relacionadas com a resistência a ataques linear e diferencial, a não linearidade e a uniformidade diferencial, respectivamente. O grau algébrico de todas as S-Boxes comparadas na tabela 2 é igual a 7.

Nenhum dos trabalhos anteriores mostra a relação da matriz binária com o multigrafo de Ramanujan para a construção de S-Boxes resistentes a ataque linear. Tomando a

Tabela 2. Relação de Propriedades das S-Boxes com Grafo de Ramanujan.

Artigos	S-Boxes	NL	δ	Multigrafo de Ramanujan
AES [Daemen and Rijmen 2002]	S	112	4	Sim
[Cui et al. 2011]	M	112	4	Sim
[Chandrasekharappa 2012]	S_1	94	10	Não
[Chandrasekharappa 2012]	S_2	92	10	Não
[Chandrasekharappa 2012]	S_3	92	10	Não
[Chandrasekharappa 2012]	S_4	92	12	Não
Este trabalho	A_1	112	4	Sim
Este trabalho	A_2	112	4	Sim
[Deva Sinha and Arya 2012]	A_3	112	4	Não
[Deva Sinha and Arya 2012]	A_4	112	4	Não
[Waqas et al. 2014]	A_n	112	-	Sim

matriz binária como sendo a matriz de adjacência de um grafo, observamos que a matriz S definida no AES é uma matriz de adjacência de um grafo 5-regular e satisfaz a definição de multigrafo de Ramanujan. Dessa forma, construímos S-Boxes com $NL > 100$ via implementação no $SAGE$. Realizamos testes em matrizes de adjacência, de ordem 8, que estão associadas a multigrafos de Ramanujan, desde que estes multigrafos sejam k-regulares com $2 \leqslant k \leqslant 7$. Portanto, não precisamos buscar por uma S entre aproximadamente 2^{62} matrizes não singulares possíveis. Nossa busca é restrita ao conjunto de todas as matrizes binárias com k $1's$ em cada linha e coluna.

Tabela 3. Número de matrizes de adjacência, de ordem 8, de grafos k-regulares

k	Quantidade	Referências
2	187530840	A001499 [Sloane 2019]
3	24046189440	A001501 [Sloane 2019]
4	116963796250	A058528 [Sloane 2019]
5	24046189440	A075754 [Sloane 2019]
6	187530840	Este trabalho
7	40320	Este trabalho

O total referente à tabela 3 é de 165431277130 matrizes binárias. Porém, nem todas são não singulares. Este valor é nosso limitante para o algoritmo 1. Os valores para $k = 6$ e $k = 7$ são iguais aos valores para $k = 2$ e $k = 1$, respectivamente.

6. Conclusão e Trabalhos Futuros

Muito da segurança do AES está presente na sua S-Box, cuja construção depende de uma matriz binária não singular de uma transformação afim. Isto é, devemos escolher matrizes binárias não singulares de forma otimizada para construir S-Boxes resistentes a ataques. Porém, muitos trabalhos relacionados escolhem as matrizes da transformação realizando buscas em um conjunto com 10160459763342013440 (ver [Sloane 2019]) matrizes binárias não singulares, sem a garantia de construção de S-Boxes com $NL > 100$. Para resolver este problema, identificamos uma relação entre a matriz da transformação afim e

a matriz de adjacência de um multigrafo de Ramanujan. Esta relação permitiu a construção de S-Boxes com $NL > 100$, escolhendo matrizes de adjancência de multigrafos de Ramanujan que são rotacionais e não singulares. Matrizes não singulares garantem a inversa da S-Box e matrizes rotacionais evitam elementos repetidos na S-Box. O algoritmo 1 garante a construção de S-Boxes com $NL > 100$, considerando as condições descritas anteriormente.

Como um trabalho futuro, estudaremos a relação entre o grafo de Ramanujan e outras propriedades da S-Box como, por exemplo, a uniformidade diferencial e o efeito avalanche. Também trabalharemos para diminuir o intervalo para k e pretendemos escrever um algoritmo para gerar a matriz da transformação afim, dada uma S-Box.

Agradecimentos

Gostaríamos de agradecer à Petrobras (processo 2018/00528-9) pelo apoio no desenvolvimento deste trabalho.

Referências

Bondy, J. A. (1976). *Graph Theory With Applications*. Elsevier Science Ltd., Oxford, UK, UK.

Canteaut, A. (2016). Lecture notes on cryptographic Boolean functions. *Inria, Paris, France*.

Carlet, C. (2010). *Boolean Functions for Cryptography and Error-Correcting Codes*, page 257–397. Encyclopedia of Mathematics and its Applications. Cambridge University Press.

Carlet, C. and Ding, C. (2007). Nonlinearities of s-boxes. *Finite Fields and Their Applications*, 13(1):121 – 135.

Chandrasekharappa, T. (2012). *Enhancement of confidentiality and integrity using cryptographic techniques*. PhD thesis, Manipal University, Manipal - India.

Chandrasekharappa, T., Prema, K., and Kumara, S. (2011). S-boxes generated using affine transformation giving maximum avalanche effect. *Int. J. Comput. Sci. Eng.*, 3(9):3185–3193.

Charles, D. X., Lauter, K. E., and Goren, E. Z. (2009). Cryptographic hash functions from expander graphs. *Journal of Cryptology*, 22(1):93–113.

Costache, A., Feigon, B., Lauter, K. E., Massierer, M., and Puskás, A. (2018). Ramanujan graphs in cryptography. *IACR Cryptology ePrint Archive*, 2018:593.

Cui, J., Huang, L., Zhong, H., Chang, C., and Yang, W. (2011). An improved AES s-box and its performance analysis. *International Journal of Innovative Computing, Information and Control*, 7:2291–2302.

Daemen, J. and Rijmen, V. (2002). *The Design of Rijndael*. Springer-Verlag, Berlin, Heidelberg.

Das, S., Zaman, J. U., and Ghosh, R. (2013). Generation of AES s-boxes with various modulus and additive constant polynomials and testing their randomization. *Procedia Technology*, 10:957 – 962. First International Conference on Computational Intelligence: Modeling Techniques and Applications (CIMTA) 2013.

Davidoff, G., Sarnak, P., and Valette, A. (2003). *Elementary Number Theory, Group Theory and Ramanujan Graphs*. Number 55 in London Mathematical Society Student Texts. Cambridge University Press.

de la Cruz Jiménez, R. A. (2019). Generation of 8-bit s-boxes having almost optimal cryptographic properties using smaller 4-bit s-boxes and finite field multiplication. In Lange, T. and Dunkelman, O., editors, *Progress in Cryptology – LATINCRYPT 2017*, pages 191–206, Cham. Springer International Publishing.

Deva Sinha, S. and Arya, C. (2012). Algebraic construction and cryptographic properties of Rijndael substitution box. *Defence Science Journal*, 62:32–37.

Hoory, S., Linial, N., and Wigderson, A. (2006). Expander graphs and their applications. *BULL. AMER. MATH. SOC.*, 43(4):439–561.

Isa, H., Jamil, N., and Reza Z 'aba, M. (2016). Hybrid heuristic methods in constructing cryptographically strong s-boxes. *International Journal of Cryptology Research*, 6:1–15.

Klima, R. and Sigmon, N. (2016). *Applied abstract algebra with MAPLE and MATLAB*. Textbook in mathematics. CRC Press, London, 3rd ed. edition.

Lubotzky, A., Phillips, R., and Sarnak, P. (1988). Ramanujan graphs. *Combinatorica*, 8(3):261–277.

Meier, W. and Staffelbach, O. (1990). Nonlinearity criteria for cryptographic functions. In Quisquater, J.-J. and Vandewalle, J., editors, *Advances in Cryptology — EUROCRYPT '89*, pages 549–562, Berlin, Heidelberg. Springer Berlin Heidelberg.

Murty, M. R. (2003). Ramanujan graphs. *J. Ramanujan Math. Soc*, 18:1–20.

Nover, H. (2005). Algebraic Cryptanalysis of AES: An Overview. *University of Wisconsin, USA*, pages 1–16.

Paar, C. and Pelzl, J. (2010). *The Data Encryption Standard (DES) and Alternatives*, pages 55–86. Springer Berlin Heidelberg, Berlin, Heidelberg.

Shannon, C. E. (1949). Communication theory of secrecy systems. *The Bell System Technical Journal*, 28(4):656–715.

Sloane, N. J. A. (2019). The on-line encyclopedia of integer sequences. http://oeis.org.

Stănică, P. (2007). Graph eigenvalues and Walsh spectrum of Boolean functions. *Integers: Electronic Journal of Combinatorial Number Theory*, 7(2).

Tao, T. (2015). *Expansion in Finite Simple Groups of Lie Type*. Graduate Studies in Mathematics: 164. American Mathematical Society, United States of America.

The Sage Developers (2009). *SageMath, the Sage Mathematics Software System (Version 4.3)*. `https://www.sagemath.org`.

Waqas, U., Afzal, S., Mir, M. A., and Yousaf, M. (2014). Generation of AES-like s-boxes by replacing affine matrix. In *2014 12th International Conference on Frontiers of Information Technology*, pages 159–164.