Universidade de São Paulo
Instituto de Matemática e Estatística
Departamento de Ciência da Computação

Criptanálise Diferencial do Cifrador Rijndael

Por Mehran Misaghi

São Paulo, Novembro de 2003.

Mehran Misaghi
Doutorando em Ciência da Computação
mehran@ime.usp.br

Relatório apresentado ao Instituto de Matemática e Estatística da Universidade de São Paulo, como exigência da disciplina MAC 5701 - Tópicos em Ciência da Computação, do Programa de Pós-Graduação em Ciência da Computação.

Professor Orientador:

Routo Terada

Sumário

1. Introdução **2**

2. AES - Novo Padrão de Criptografia **3**
2.1 Histórico 3
2.2 Notação Utilizada 4
2.3 Transformações por Rodada 5
2.4 Processo de Expansão de Chaves 6
2.5 Algoritmo Rijndael 7

3. Tipos de Criptanálise **7**
3.1 Criptanálise Linear 8
3.2 Criptanálise Diferencial 9
3.2.1 Razão Sinal-Ruído 9
3.3 Variações de Ataque Diferencial 10
3.3.1 Diferencial-Linear 10
3.3.2 Diferencial Truncado 10
3.3.3 Higher Order Differentials 10
3.3.4 Square 11
3.3.5 Diferenciais Impossíveis 11
3.3.6 Bumerangue 11
3.4 Construção de Criptanálise Diferencial 12

4. Criptanálise Diferencial de Rijndael **12**
4.1 Diferencial Truncado 13
4.2 Diferencial Impossível de 6 rounds 13
4.3 Saturação 14
4.4 Probabilidade de sucesso em Criptanálise Diferencial 15
4.5 Padrões Diferenciais Consistentes de Rijndael 15

5. Considerações Finais **16**

Referências Bibliográficas **18**

1. Introdução

O aumento crescente dos sistemas de informação conectados à rede mundial de computadores tem contribuído na inovação das ferramentas de segurança de dados. Uma das mais antigas ferramentas usadas para segurança de dados é a criptografia. As ferramentas de criptografia providenciam recursos importantes contra acessos intencionais ou acidentais aos dados, os quais podem comprometer sua autenticidade e integridade.

Um cifrador de bloco permite cifrar um texto plano de n bits com uma chave de k bits, produzindo um texto cifrado de n bits. Criptanálise é equivalente a busca da chave secreta correta de tamanho K em um conjunto de 2^k chaves possíveis que permite duas soluções extremas: Busca exaustiva da chave e tabela de pré-computação. Em busca exaustiva da chave, o texto cifrado pode ser decifrado com cada chave e o resultado ser comparado com o texto plano conhecido. Se forem iguais, a chave provavelmente é a chave correta.

Existem diversos métodos de criptanálise. Criptanálise diferencial consiste em ataque ao texto plano escolhido na qual uma grande quantidade de pares de texto plano-cifrado são utilizados para descobrir alguma parte da chave. As informações estatísticas das chaves são deduzidas de blocos de textos cifrados com cifragem de pares de blocos de textos planos[2].

Este trabalha pretende abordar as técnicas de criptanálise diferencial e trabalhos relacionados com o cifrador Rijndael. O presente relatório está organizado da seguinte forma:

A seção 2 aborda o histórico do cifrador Rijndael, notação utilizada no cifrador e os detalhes das transformações por rodada e o algoritmo Rijndael. As definições de Criptanálise Linear e Diferencial e as variações de Criptanálise Diferencial são descritas na seção 3. A seção 4 descreve os tipos de ataques de Criptanálise Diferencial que podem ser aplicados com alguns rounds para o cifrador Rijndael. As considerações finais são o foco da seção 5.

2. AES - Novo Padrão de Criptografia

2.1 Histórico

O DES[1] foi instituído em 1977 como padrão de criptografia para uso oficial do governo americano. Por mais de vinte anos, o DES foi empregado amplamente em diversos sistemas. Mas com os atuais recursos computacionais, o DES tornou-se obsoleto. Foram feitas diversas tentativas de quebra do DES, através de implementações de *hardware* e *software* [11].

Em 1977, uma máquina de busca paralela, com custo de 20 milhões de dólares, foi proposta com um tempo estimado de 12 horas de pesquisa. Em 1980, este valor foi corrigido para 50 milhões de dólares e 2 dias de pesquisa. Em 1993, este custo baixou para um milhão de dólares e 3,5 horas de pesquisa. Em 1998, uma máquina de 130.000 dólares foi montada com uma expectativa de tempo de pesquisa de 112 horas [11].

Em 1997, o NIST[2] abriu um concurso internacional chamado AES[3] para algoritmos candidatos que satisfizessem os seguintes critérios [6]:

1. Tamanho de bloco 128 bits na entrada e na saída.
2. Tamanho da chave de 128 ou 192 ou 256 bits.
3. Segurança e velocidade do algoritmo igual ou superior a 3-DES.
4. Implementação em *software*, *hardware* e *smart-card* de forma eficiente.
5. Código fonte do algoritmo disponível sem custo algum.

Em abril de 1999, foram escolhidos cinco candidatos:

1. **MARS**, desenvolvido por Nevenko Zunic (IBM).
2. **RC6**, desenvolvido por Burt Kaliski (RSA Laboratories).
3. **RIJNDAEL**, desenvolvido por Joan Daemen e Vincent Rijmen.
4. **SERPENT**, desenvolvido por Ross Anderson, Eli Biham e Lars Knudsen.
5. **TWOFISH**, desenvolvido por Bruce Schneier, J. Kelsey, D. Whiting, D. Wagner, Chris Hall e Niels Ferguson.

[1] Data Encryption Standard
[2] National Institute of Standards and Tenchnology of USA
[3] Advanced Encryption Standard

Em 2 de outubro de 2000, foi escolhido RIJNDAEL como novo padrão de criptografia que substituiu oficialmente o DES, a partir de junho de 2001.

O cifrador de bloco Rijndael é designado para realizar as operações sobre um byte, providenciando a flexibilidade requerida para os candidatos de AES, no qual tamanho da chave e tamanho do bloco podem ser escolhidos entre 128, 192 e 256 bits. Número de *rounds* varia conforme o tamanho da chave:

- 9 *rounds*, se a chave e o bloco sejam do tamanho de 128 bits.
- 11 *rounds*, se a chave ou o bloco sejam do tamanho de 192 bits.
- 13 *rounds*, se a chave ou o bloco sejam do tamanho de 256 bits.

2.2 Notação Utilizada

- Todos os valores do byte do algoritmo de Rijndael são apresentados por uma notação de vetor $(b_7, b_6, b_5, b_4, b_3, b_2, b_1 \; e \; b_0)$ que corresponde a representação de um polinômio como:

$$b_7x^7 + b_6x^6 + b_5x^5 + b_4x^4 + b_3x^3 + b_2x^2 + b_1x + b_0 = \sum_{i=0}^{7} b_i x^i$$

  Um exemplo seria $(01001011) \rightarrow x^6 + x^3 + x + 1$.

- Conjuntos de bytes, $a_0, a_1, a_2, \ldots, a_{15}$ são definidos a partir da seqüência de entrada, de 128 bits, $ip_0, ip_1, ip_2, \ldots, ip_{126}, ip_{127}$, como segue:

$$a_0 = (ip_0, ip_1, \ldots, \; ip_7)$$

$$a_1 = (ip_8, ip_9, \ldots, \; ip_{15})$$

$$\vdots$$

$$a_0 = (ip_{120}, ip_{121}, \ldots, \; ip_{127})$$

  onde ip_k é $entrada_k$ para $k = 0, 1, 2, \ldots, \; 127$.

2.3 Transformações por Rodada

As transformações por rodada são uma seqüência de quatro transformações que ocorrem no processo de cifragem:

1. **SubBytes**: É uma simples substituição de byte que utiliza uma tabela de 16x16 contendo a permutação de todos os valores de 256 bits. Cada byte é substituido pelo byte correspondente na linha (esquera 4 bits) e na coluna (direita 4 bits). Por exemplo, byte **95** é substituido pelo byte da linha **9** e coluna **5**. A S-Box[4] é construída usando uma transformação definida de valores em $GF(2^8)$.

2. **ShiftRows**: Os bytes são rotacionados em grupos de quatro bytes, de modo que cada grupo irá interferir em outro, através do emprego de técnicas de difusão de dados. Shift circular de byte em cada linha, sendo que:

   - 1^a linha não é trocada;
   - 2^a linha faz 1 shift circular de byte para esquerda;
   - 3^a linha faz 2 shift circular de byte para esquerda;
   - 4^a linha faz 3 shift circular de byte para esquerda.

   O processo de decifragem faz shift para direita. Este passo permuta os bytes entre as colunas.

3. **MixColumns**: Cada grupo de quatro bytes passa por uma multiplicação linear, através do emprego de técnicas de difusão de dados. Cada coluna é processada separadamente e cada byte é substituido por um valor dependente aos 4 bytes na coluna. A figura 1 mostra esta operação.

4. **AddRoundKey**: Nesta etapa, o bloco de dados é alterado através da subchave da rodada, a qual possui o mesmo tamanho do bloco, que realiza uma operação XOR com o bloco inteiro.

A figura 2 mostra o funcionamento das transformações em rodadas do cifrador Rijndael.

[4]S-Box ou Caixa-S é uma tabela de substituição.

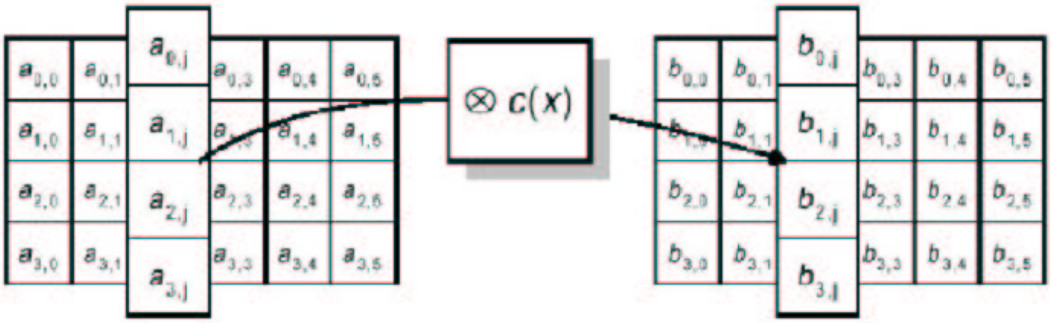

Figura 1: Operação de MixColumns no cifrador Rijndael

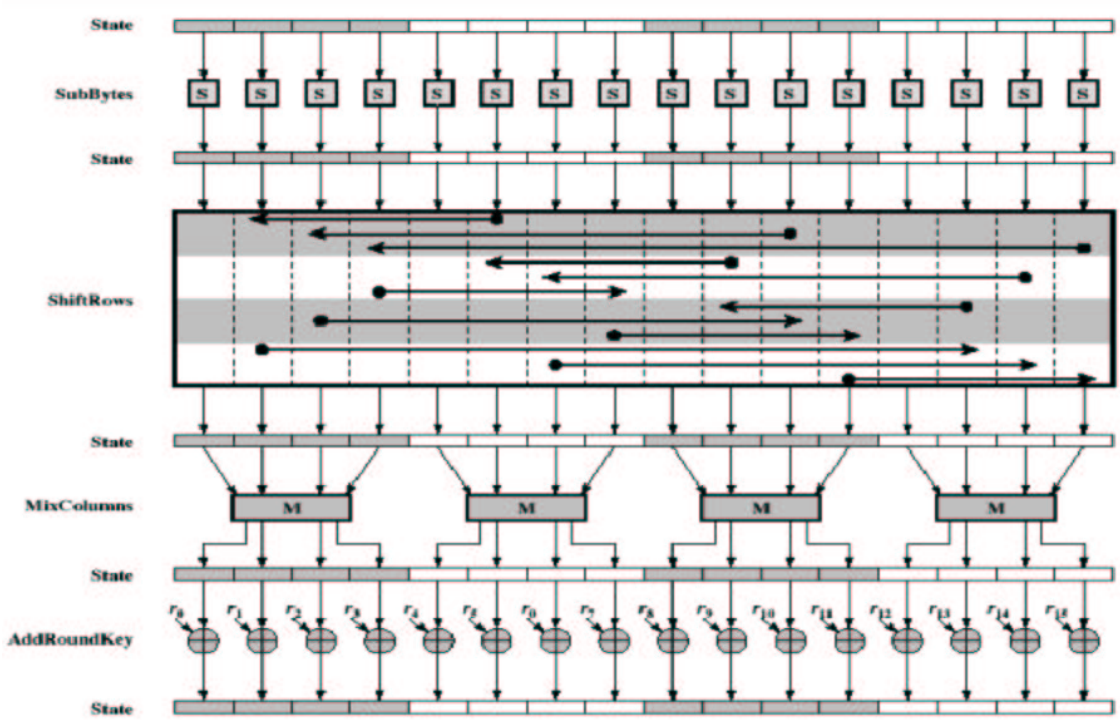

Figura 2: As Rodadas de Rijndael.

2.4 Processo de Expansão de Chaves

Este processo também é conhecido como algoritmo de geração de chaves. Este algoritmo gera uma quantidade de sub-chaves igual a quantidade de rounds mais um, a partir da

chave principal, sendo que cada sub-chave possui o mesmo tamanho da chave principal. O processo de geração de chaves resulta em um vetor unidimensional com palavras (w) de 4 bytes. A figura 3 ilustra o processo de expansão de chaves no cifrador Rijndael. Nesta figura cada byte é nomeado de w_x, onde x é a posição do byte dentro do vetor.

Figura 3: Processo de Expansão de Chaves

2.5 Algoritmo Rijndael

O processo de cifragem do algoritmo de Rijndael é a execução da seqüência das transformações por rodada. O processo de decifragem consiste na execução de transformações inversas. No processo de decifragem são utilizadas as formas inversas das funções SubBytes, ShiftRows e MixColumns. A função AddRoundKey continua sendo a mesma função no processo de cifragem e decifragem. A figura 4 ilustra o processo de cifragem e decifragem do cifrador Rijndael.

3. Tipos de Criptanálise

A criptanálise consiste no estudo estudo das ferramentas que avaliam vulnerabilidades de um cifrador para garantir um certo nível de segurança e até reduzir a complexidade do cifrador em alguns casos. A criptanálise trabalha com hipóteses. Por exemplo conhecimento de alguma parte da chave, do texto plano, do texto cifrado, do algoritmo de cifragem ou alguma combinação entre estas partes. Existem diversos métodos de criptanálise, como por exemplo Criptanálise Linear e Criptanálise Diferencial.

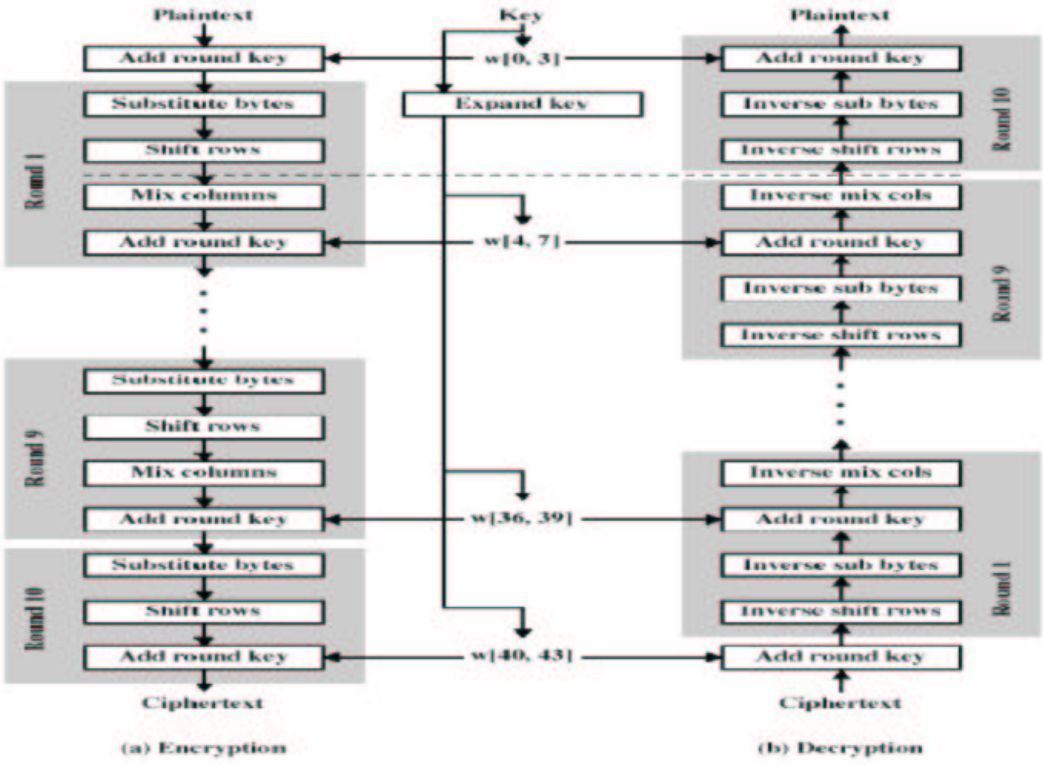

Figura 4: Processo Cifragem e Decifragem de Rijndael

3.1 Criptanálise Linear

O método de Criptanálise Linear foi inicialmente apresentado por M. Matsui na conferência Eurocrypt'93 como um ataque estatístico de texto legível conhecido, onde se explora combinações de bits do texto legível, bits do texto cifrado e bits de subchave, através de operações de ou-exclusivo (XOR), chamadas de operações lineares, resultando em um bit de paridade, para obter um provável candidato para alguns bits de subchave, envolvendo nesta combinação linear entre esses bits [2].

A estratégia utilizada neste método é criar uma aproximação mais simples para um cifrador de bloco, ao invés de verificar pontos isolados, no qual o cifrador de bloco tem um comportamento mais simples. Para encontrar alguns bits da chave, o criptanalista deve processar um conjunto muito grande de pares de texto plano e texto cifrado.

3.2 Criptanálise Diferencial

Criptanálise diferencial foi desenvolvido por Biham e Shamir[3] para variantes do cifrador **DES** e depois foi aplicada para o DES com 16 *rounds*[4]. Criptanálise diferencial também pode ser aplicada em cifradores com estrutura SPN[5], tais como SAFER[5], Lucifer e funções de *hash*.

Criptanálise diferencial consiste em ataque ao texto plano escolhido na qual uma grande quantidade de pares de texto plano-cifrado são utilizados para descobrir alguma parte da chave. As informações estatísticas das chaves são deduzidas de blocos de textos cifrados com cifragem de pares de blocos de textos planos[2].

Este tipo de ataque se baseia na utilização de pares de texto plano(P, P^*) que satisfazem a relação ($\Delta P = P \oplus P^*$) e pares de texto cifrado (C, C^*) correspondentes. A relação existente é chamada de **diferença no par** de textos planos ou textos cifrados[6].

A criptanálise diferenical de cifradores iterativas baseia-se na observação de que determinados pares de texto plano, que foram cifrados com a mesma chave, resultam em pares de texto cifrado, cuja diferença é previsível com certa probabilidade, dependente do número de iterações consideradas.

Além disso, a criptanálise diferencial examina as propriedades de S-Box para determinar as características diferenciais, considera as diferenças de entrada e saída de S-box, combinando pares de diferenças de S-Box de um round para outro, de forma que, os bits de diferença de saída não zero correspendam aos bits de diferença de entrada do outro round.

3.2.1 Razão Sinal-Ruído

Uma propriedade muito importante em criptanálise diferencial é chamada Razão Sinal-Ruído ou simplesmente S/N[7]. A razão entre o número de pares corretos e a contagem média de subchaves incorretas em uma esquema de contagem é chamada de S/N, sendo que:

- S/N > 1 indica que o valor da subchave correta é entre as mais sugeridas.
- S/N < 1 indica que o valor da subchave correta é entre as menos sugeridas.

[5]Subtitution Permutations Network
[6]no caso de texto cifrado temos: $\Delta C = C \oplus C^*$
[7]S/N = Signal-to-Noise Ratio

- S/N = 1 não permite distinguir a subchave correta com subchave errada.

3.3 Variações de Criptanálise Diferencial

Como ataques derivados do ataque de Criptanálise Diferencial podemos comentar os seguinte ataques [12], dentre os existentes:

1. **Diferencial-Linear** por Langford-Hellman em 1995,
2. **Diferencial Truncado** por Knudsen em 1995,
3. **Higher Order Differentials** por Knudsen em 1995,
4. **Square** por Daemen et al. em 1997,
5. **Diferenciais Impossíveis** por Biham et al. em 1998,
6. **Bumerangue** por Wagner em 1999.

3.3.1 Diferencial-Linear

Langford e Hellman utilizaram a concatenação das características diferenciais e lineares e criaram o ataque Diferencial-Linear em 1995. Esta técnica é baseada na cifragem de vários pares com diferença de entrada conhecida. Cada par é cifrado e a paridade do subconjunto de saída é computada para ambos os textos cifrados.

3.3.2 Diferencial Truncado

Este ataque foi publicado inicialmente por Knudsen em 1995 e explora o fato que em alguns cifradores, os rastos diferenciais tendem a se agrupar. O agrupamento ocorre quando, se para um certo conjunto de modelos de diferenças de entrada e modelos de diferenças de saída, o número de rastos diferenciais seja excessivamente grande. A probabilidade esperada para que um rasto diferencial fique em fronteiras de agrupamento, pode ser computada independentemente de razões de apoio de rastos diferenciais de forma individual. Cifradores na qual, todas as transformações operam em um estado de blocos bem ordenados, tendem a ser suscetível a este tipo de ataque.

3.3.3 Higher Order Differentials

Este ataque é a generalização de ataque diferencial utilizando diferenças de texto repetido. As diferenças de texto também são definidas como derivada das funções discretas, e a sua generalização como derivadas de *higher order*.

3.3.4 Square

Este ataque explora a estrutura baseada na palavra do cifrador, onde todos os blocos de dados são particionados e processados em palavras de 8 bits. Pode ser aplicado para estrutura de Feistel ou SPN. É um ataque de texto plano escolhido que tem semelhanças com *higher order*, no sentido que uma diferença repetida de diversas palavras com alguma operação de grupo como uma propriedade invariante através de diversos rounds de um cifrador, em uma configuração semelhante como um par de textos, com um operador de diferença.

3.3.5 Diferenciais Impossíveis

No ataque convencional de Criptanálise Diferencial, as características ou as diferenças de alta probabilidade são procuradas para distinguir um cifrador de uma permutação aleatória e eventualmente montar um ataque de recuperação da chave.

Nestes ataques, as subchaves são advinhadas em diversos rounds, cercando as diferenças. As subchaves mais sugeridas (após de cifragem/decifragem) pela diferença podem ser os valores corretos. A nova técnica (sugerida pelo Biham), ao contrário, procura diferenças que sugerem valores que nunca ocorrem, quer dizer, com probabilidade zero. Desta forma a S/N=0, desde que a chave correta nunca seja sugerida. Estas diferenças com probabilidade zero são chamadas de Diferenças Impossíveis[8].

3.3.6 Bumerangue

Este ataque é como um bumerangue[9], ou seja, a arma que volta a quem a lançou. Utiliza duas características não relacionadas para atacar duas metades de um cifrador de bloco. Começa com um bloco de texto plano aleatório e baseado nas características conhecidas na primeira metade de cifrador.

O resultado depois de uma meia cifragem de dois blocos de texto plano, antes e depois de XOR, terá diferenças. Desde que as características sejam aplicadas somente a primeira metade do cifrador, os resultados depois de cifragem de todo bloco, não terão relação entre eles. Este ataque aumenta o potencial de Criptanálise Diferencial, pois pode utilizar características que não são espalhadas através do cifrador. A figura 5 ilustra este tipo de ataque.

[8]Impossible Differentials
[9]boomerang

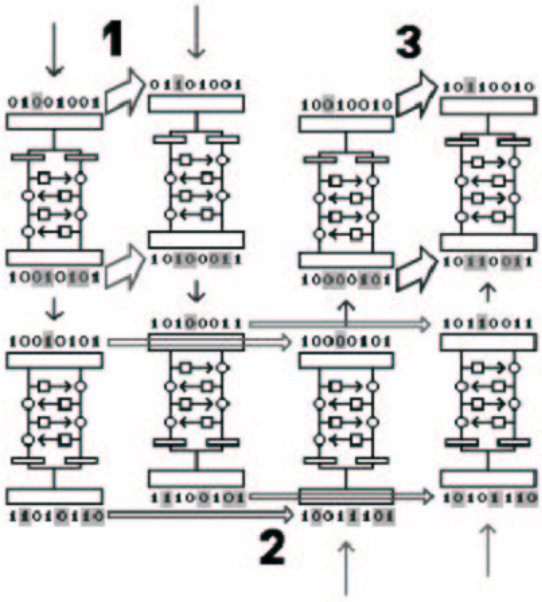

Figura 5: Ataque Bumerangue

3.4 Construção de Criptanálise Diferencial

Segundo [14], para construir as características diferenciais, são examinados as propriedades de S-Boxs de forma individual. Tais propriedades são utilizadas para determinar as características diferenciais completas, especialmente são consideradas as diferenças de entrada e saída do S-Box para determinar as pares de diferença com alta probabilidade.

Combinando as pares de diferença de S-Box, round por round, até que os bits de diferença de saída não zeros de um round, correspondam aos bits de diferença de entrada não zeros de outro round. Desta forma, é possível achar um diferencial de alta probabilidade consistindo de diferenças de textos planos e diferenças de entrada para o útlimo round.

4. Criptanálise Diferencial de Rijndael

Segundo [8], o cifrador Rijndael foi projetado de maneira que ele não apresenta características diferenciais (isto é, padrões de propagação de diferenças entre blocos de textos legíveis e blocos de textos cifrados) não triviais com probabilidade substancialmente acima de 2^{127}, que é a probabilidade de sucesso de uma tentativa isolada de quebra por inspeção.

Concretamente, a probabilidade máxima de uma característica diferencial sobre 4 passos do Rijndeal é de apenas 2^{150}, de modo que nenhuma característica diferencial individual pode ser aproveitada. Tampouco se conhece algum diferencial completo ou truncado, e não há método sistemático de busca de todas as possibilidades exceto busca exaustiva.

A seguir, serão descritos resumo de resultados de alguns ataques diferenciais para o cifrador Rijndael.

4.1 Diferencial Truncado

A seção 3.3.2 fez uma descrição do ataque Diferencial Truncado que foi introduzido por Knudsen e é uma extensão de ataque original de Criptanálise Diferencial. Apesar da possiblidade de Rijndael estar sujeito a este tipo de ataque devido a sua estrutura, os autores [2] investigaram a resistência do Rijndael contra ataque Diferencial Truncado. Para 6 rodadas ou mais, nenhum ataque tem sido encontrado que seja mais rápido do que a busca exaustiva da chave.

4.2 Diferencial Impossível de 6 rounds

Segundo [15], o ataque é baseado no ataque diferencial impossível de quatro rounds com um round adicional no início e no final de cada round, como é ilustrado na figura 6[10]. Note que o último round do Rijndael não passa pela transformação de MixColumns antes de AddRoundKey. O procedimento de ataque é o seguinte:

1. A estrutura é definida como um conjunto de textos planos com certos valores fixos. Uma estrutura consiste de 2^{32} textos planos e propõe 2^{32} x 2^{32} x $\frac{1}{2}$ = 2^{63} pares de textos planos.

2. Tem que escolher $2^{59.5}$ estruturas sendo $2^{91.5}$ textos planos e $2^{122.5}$ pares de textos planos. Escolher também pares cujos pares de textos cifrados tenham diferença de zero na linha dois e três. O número esperado de tais pares é $2^{122.5}$ x 2^{-64} = $2^{58.5}$.

3. Assumir um valor de 64 bits na linha 0 e 1 da chave do último round, K_6.

4. Para cada par de texto cifrado (C, C^*), calcular $C_5 = BS^{-1} \circ SR^{-1}(C + K_6)$ e $C_5^* = BS^{-1} \circ SR^{-1}(C^* + K_6)$ e escolher pares cuja diferença de $MC^{-1}(C_5 + C_5^*)$ seja zero nos quatro bytes (1,6,11,16), (2,7,12,13), (3,8,9,14) ou (4,5,10,15) depois da inversão da transformação MixColumns. O número esperado dos pares remanescentes é de $2^{58.5}$ x 2^{-30} = $2^{28.5}$.

[10] Esta figura consta em [15]

5. para um par (P, P^*) com tais pares de textos cifrados e valor de 32 bits para quatro bytes (1,8,11,14) da chave inicial K_0 deve-se calcular:

$$MC \circ SR(BS(P + K_0) + BS(P^* + K_0))$$

e então escolher pares cuja diferença é zero exceto somente um byte depois da transformação de MixColumns.

6. Desde que tal diferença é impossível, qualquer chave que propõe tal diferença é uma chave errada.

7. O passo quatro requer aproximadamente $2^{123.5}$ operações de um round. O passo 5 requer aproximadamente 2^{119} operações de um round. Consequentemente, desde que este procedimento seja repetido duas vezes, este ataque requer aproximadamente $2^{91.5}$ de textos planos escolhidos e 2^{122} cifragens de Rijndael reduzido para 6 rounds.

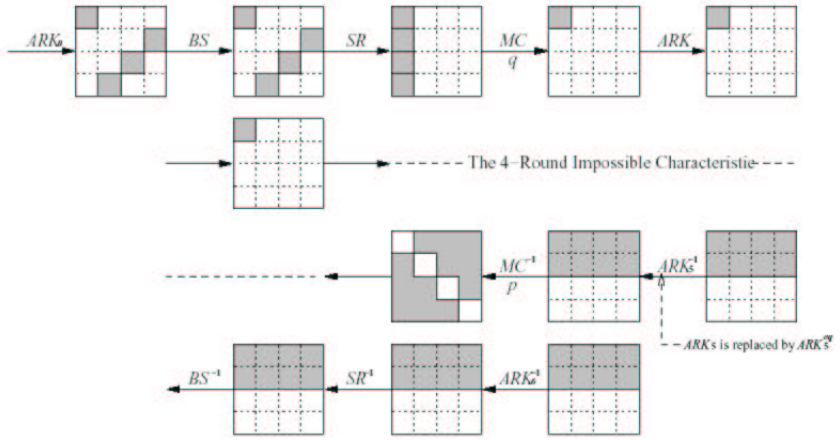

Figura 6: Ataque Diferencial Impossível com 6 rounds. A função de MixColumns é representada por MC, ByteSub por BS, ShiftRows por SR e AddRoundKey por ARK.

4.3 Saturação

Ataque de Saturação é um ataque de texto plano escolhido nos cifradores que tem a estrutura de round semelhante ao de Rijndael. Este ataque pode ser implementado independentemente da escolha da S-Box no passo não-linear e escalonamento da chave. Ataque de Saturação aplicado ao cifrador Rijndael, segundo [2], é mais rápido do que uma busca exaustiva da chave para rounds reduzidos até 6 rounds. Este ataque, segundo [8], é o ataque de criptanálise mais poderoso que pode ser aplicado ao cifrador Rijndael.

4.4 Probabilidade de sucesso em Criptanálise Linear e Diferencial

segundo [16], se um ataque sobre uma chave de m bits adquirir o valor correto da r-ésima candidata entre 2^m possibilidades, pode-se dizer que o ataque obteve uma vantagem de $m - \lg r$ bits sobre a busca exaustiva. A definição mais estrita do sucesso, onde o atacante descobre a chave correta como a primeira candidata, corresponde a obtenção de m bits de vantagens sobre uma chave de m bits.

Em um ataque de criptanálise diferencial, o atacante primeiramente acha uma característica do cifrador atacado. Uma característica é uma seqüência de diferenças entre as entradas do round na cifragem de dois blocos de textos planos com uma diferença inicial dada. Para que uma característica seja útil em um ataque, um par de texto plano com uma diferença inicial dada tem que possuir uma probabilidade não trivial para seguir a seqüência de diferenças dada durante o processo da cifragem.

Uma medida importante para sucesso do ataque de criptanálise diferencial é a proporção entre a probabilidade de que a chave correta sendo sugerida por um par correto, e a probabilidade de uma chave aleatória sendo sugerida por um par aleatório com uma diferença inicial dada. Esta proporção é S/N que foi explicado na seção 3.2.1.

4.5 Padrões Diferenciais Consistentes de Rijndael

Os autores de [7] introduziram o conceito de padrões diferenciais consistentes de Rijndael que será útil para ataque de criptanálise deste cifrador. O que se entende por padrões diferenciais consistentes é:

- Se dois textos planos do cifrador diferem somente por um byte, então existem quatro pares de bytes na diferença de saída do segundo round, com cada par tendo o mesmo valor;
- Se dois textos planos do cifrador diferem por mais de 4 bytes em certas posições, então o padrão acima aparece na diferença de saída do segundo roundo também.
- Para qualquer 2^{8n} textos planos, que variam em n bytes e que outros bytes são todos o mesmo, se fazermos pares de um destes textos planos com qualquer um dos outros textos planos, então qualquer diferença de saída é igual ao XOR de outra diferença de saída depois do terceiro round.
- Para qualquer 2^{32} textos planos, que vairam em certos quatro bytes e que outros bytes todos são o mesmo, se fazermos pares de um destes textos planos com qualquer

um dos outros textos planos, então qualquer diferença de saída é igual ao XOR de outra diferença de saída depois do quarto round.

Os autores de [7] fizeram diversas observações de padrões diferenciais consistentes para o cifrador de Rijndael até seis rounds. A figura 7 ilustra o processo de padrões diferenciais consistentes no primeiro round.

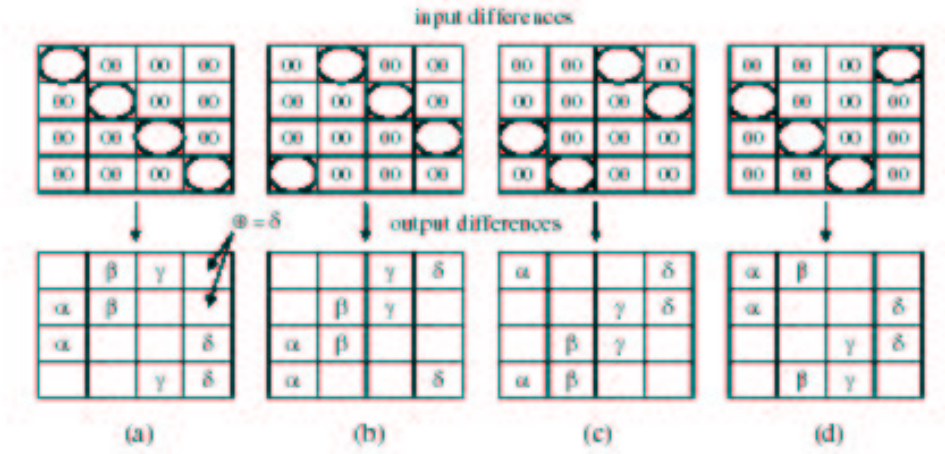

Figura 7: Padrões diferenciais consistentes no primeiro round

5. Considerações Finais

Este trabalho abordou os conceitos de criptanálise diferencial do cifrador Rijndael através de diversos tipos de ataques que foram descritos. Em um ataque de criptanálise diferencial, o criptanalista necessita conhecer um padrão de diferença de entrada que propaga-se para um padrão de diferença de saída, com uma alta probabilidade [2].

O cifrador Rijndael foi projetado da forma que não apresente características diferenciais. Por isto, são utilizadas variações de ataque diferencial que são aplicados em uma versão de rounds reduzidas do cifrador Rijndael. Dentre estes, foram abordados ataques diferencial truncado, diferencial impossível para 6 rounds, e saturação. Como a probabilidade de sucesso também é um assunto de suma importância para criptanálise linear e diferencial, a seção 4.4 descreveu como seria a probabilidade de sucesso em criptanálise diferencial aplicado ao cifrador de Rijndael. Para finalizar, a seção 4.5 comentou como os padrões diferenciais consistentes podem ser úteis para criptanálise diferencial.

O campo de criptanálise diferencial é um assunto em franca expansão que apesar de ter algumas literaturas a respeito, não existem implementações, simulações e dados estatítiscos que ajudem a assimilar e aplicar os conceitos desta área nos sistemas cripotográficos. O cifrador Rijndael, pelas exigências expostas na sua fase de implementação e já no seu projeto, possui mecanismos que dificultam qua tais ataques sejam bem sucedidos.

Por razões acima citadas, trabalhos futuros podem focar na implementação, prototipação e simulação de métodos de criptanálise diferencial para fins didáticos. Tais contribuições certamente ajudarão o público que estuda e aprecia a análise dos sistemas criptográficos.

Referências

[1] Rouvroy, Gael. *Implementation of cryptographic standards and cryptanalysis using FPGAs*. Prix de la SRBE, setember 2002.

[2] Daemon, Joan; Rijmen, Vincent. **The Design of Rijndael**. Springer-Verlag, 2002.

[3] Biham, E.; Shamir, A. *Differential Cryptanalysis of DES-like Cryptosystems.*. Journal of Cryptology, 4(1):3-72, 1991.

[4] Biham, E.;Shamir, A. *Differential Cryptanalysis of Full 16-Round DES*. Advances in Cryptology, Crypto'92, LNCS 740: 487-496, Springer-Verlag, 1993.

[5] Knudsen L. R.; Berson, T. A. *Truncated Differantials of SAFER*. 3rd Fast Software Encryption Workshop, LNCS 1039: 15-26. Springer-Verlag, 1996.

[6] Terada, Routo. **Segurança de Dados - Criptografia em Redes de Computador**, Editora Edgard Blücher Ltda, SP, 2000.

[7] Song, Beomsik; Seberry, Jennifer. *Consistent Differntial Patterns of Rijndael*, LNCS 2587: 149-163, Springer-Verlag, 2003.

[8] Daemon, Joan; Rijmen, Vincent; Barreto, Paulo S.L.M. *Rijndael: beyond the AES*, Mikulasska Kryptobesidka, 2002.

[9] Miers, Chalres C.*Modelo Simplificado do AES*. Dissertação de Mestrado, 2002.

[10] Daemon, Joan; Rijmen, Vincent. *Fast Sofware Encryption'02*, LNCS 2365, Springer-Verlag, 2002.

[11] Lenstra, Arjen K.; Verheul, Eric R.*Selecting Cryptography Key Sizes*, 1999.

[12] Nakahara, Jorge J. *Cryptanalysis and Design of Block Ciphers*. Tese de Doutorado, 2003.

[13] Nakahara, Jorge J. *Criptanálise Diferencial-Linear aplicada às Cifras FEAL-N e FEAL-NX*. Dissertação de Mestrado, 1996.

[14] Heys, Howard M. *A Tutorial on Linear and Differential Cryptanalysis*, 2001.

[15] Lee, Jung-Yeun *Cryptanalysis of Rijndael*, 2001.

[16] Selçuk, Ali A.; Biçak, Ali. *On Probability of Success in Linear and Differential Cryptanalysis*, LNCS 2576: 174-185, Springer-Verlag, 2003.