UNIVERSIDADE DE SÃO PAULO
INSTITUTO DE MATEMÁTICA E ESTATÍSTICA
Departamento de Ciência da Computação

Plano de trabalho para a disciplina de Tópicos em Ciência da Computação - MAC5701

Aluno : Mehran Misaghi
Orientador : Prof. Dr. Routo Terada
Área de Concentração : Criptografia

Título : " Criptanálise Diferencial de Cifrador Rijndael "

São Paulo – Setembro de 2003

1. Introdução

Este documento objetiva propor um plano de estudos para a disciplina de **Tópicos em Ciência da Computação**, do segundo semestre de 2003, baseado em referências bibliográficas relacionados com o tema do trabalho.

2. Objetivo

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 e permite duas soluções extremas: Busca exaustiva de chave e tabela de pré-computação. Em busca exaustiva de 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].

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*, tais como SAFER[5], Lucifer e funções de *hash*.

Em janeiro de 1997, NIST[1] anunciou o desenvolvimento de um novo padrão de criptografia: *AES,* para substituir o velho padrão *DES*[2]. Em 2 de outubro de 2000, NIST oficialmente anunciou o Rijndael, como vencedor entre os cinco finalistas, que se tornou o novo padrão AES a partir de 2001[2].

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.

Os autores de [7] afirmam que a busca exaustiva de chave não é um ataque que explora bem a estrutura interna do cifrador Rijndael. Os autores mostraram em [8] que o cifrador Rijndael tem uma segurança bastante elevada contra ataques de criptanálise linear e diferencial.

Este trabalha pretende abordar as técnicas de criptanálise diferencial e trabalhos relacionados com o cifrador Rijndael.

3. Tópicos selecionados

Inicialmente será abordada uma revisão bibliográfica dos conceitos, padrões e mecanismos de criptanálise diferencial. Outras técnicas de criptanálise diferencial, algumas tentativas que já foram feitas, bem como relacionamento entre diversas técnicas de criptanálise diferencial serão abordadas.

[1] National Institute of Standards and Technology
[2] Data Encryption Standard

Referências Bibliográficas

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

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

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