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

Plano de estudos
MAC5701 – Tópicos em Ciência da Computação

Aluno: Eduardo Takeo Uêda
Orientador: Prof. Dr. Routo Terada
Área de Concentração: Criptografia

Tema: "Aplicação do ataque χ^2 sobre o cifrador RC6"

São Paulo – Setembro de 2003

1. Introdução

Uma das grandes preocupações da Ciência da Computação atualmente é a garantia do sigilo de informações confidenciais que são transmitidas eletronicamente. Assim, a criptografia assume um papel de elevada importância na elaboração de sistemas.

Dentro desse contexto, em 1977 o algoritmo criptográfico conhecido como DES (Data Encryption Standard) passou a ser adotado como padrão americano de criptografia em transações comerciais.

Em 1997, o NIST (Nacional Institute of Standards and Technology) anunciou o início do desenvolvimento do AES (Advanced Encryption Standard) – uma competição internacional entre algoritmos criptográficos no qual o vencedor seria o substituto do DES.

O NIST anunciou em 2000 que o algoritmo selecionado foi o Rijndael. Porém, nosso trabalho se concentrará sobre outro algoritmo : o *RC6*, um dos cinco finalistas ao AES. Na verdade o RC6 é uma evolução melhorada do RC5, que atende as exigências do concurso AES.

2. Objetivo

Infelizmente, até o momento não se conhece um método matemático para provar que um algoritmo criptográfico é seguro. A melhor maneira que conhecemos hoje para chegar perto desse ideal é submeter determinado algoritmo às técnicas mais sofisticadas de ataque existentes e considerá-lo seguro no "estado da arte" caso ele mostre-se resistente a tais ataques.

Atualmente, os ataques sobre algoritmos simétricos mais conhecidos são os de criptanálise diferencial e linear. Entretanto, nosso objetivo consiste em analisar e constatar a segurança do algoritmo RC6 com relação a outro ataque probabilístico, conhecido como *ataque* χ^2.

O ataque χ^2 foi originalmente proposto por Knudsen e Meier como um ataque de texto escolhido sobre o RC6. Eles se concentraram sobre correlações entre bits de entrada (texto legível) e bits de saida (texto cifrado), medidas por teste χ^2.

Referências Bibliográficas

[1] Rivest, R. L.. *The RC6 Block Cipher.*

[2] Isogai, N.. *Statistical Analysis of χ^2–Attacks.*

[3] Shimoyama, T.. *Correlation Attack to the Block Cipher RC5 and the Simplified Variants of RC6.*

[4] Knudsen, L. R.. *Correlation in RC6 with a Reduced Number of Rounds.*

[5] Knudsen, L.R.. *Correlations in RC6.*