Uma versão mais forte do algoritmo RC6 contra criptanálise χ^2

Eduardo Takeo Ueda[1] Routo Terada[2]

[1]Laboratório de Arquitetura e Redes de Computadores
Departamento de Engenharia da Computação e Sistemas Digitais
Escola Politécnica da Universidade de São Paulo
edutakeo@larc.usp.br, edutakeo@gmail.com

[2]Departamento de Ciência da Computação
Instituto de Matemática e Estatística
Universidade de São Paulo
rt@ime.usp.br

VII Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais

Agenda

- Introdução
- Algoritmo RC6
- Função de Troca
- Algoritmo RC6T
- Teste χ^2
- Correlações nos Algoritmos RC6 e RC6T
- Ataque de Distinção
- Ataque de Recuperação da Chave
- Conclusão

Introdução

- Análise da técnica de criptanálise χ^2 que foi aplicada contra o algoritmo RC6 por Knudsen e Meier, mas que foi originalmente proposta por Serge Vaudenay em 1996 como um ataque sobre o DES
- Apresentação de uma versão modificada do algoritmo RC6, denotada por RC6T, obtida através da introdução de uma função de troca na sua estrutura, e constatação de que essa nova versão é mais forte contra criptanálise χ^2

Algoritmo RC6 - Cifração

$B = B + S[0]$
$D = D + S[1]$
para $i = 1$ até r faça{
$t = (B \times (2B + 1)) \lll \lg w$
$u = (D \times (2D + 1)) \lll \lg w$
$A = ((A \oplus t) \lll u) + S[2i]$
$C = ((C \oplus u) \lll t) + S[2i + 1]$
$(A, B, C, D) = (B, C, D, A)$
}
$A = A + S[2r + 2]$
$C = C + S[2r + 3]$

Função de Troca

Definição

Seja $X = (X_E, X_D)$ uma seqüência de 32 bits. Definimos a função de troca T por:

$$T(X) = \begin{cases} (X_E; X_D), & \textit{caso o número de bits 1 em } X \textit{ seja par} \\ (X_D; X_E), & \textit{caso contrário} \end{cases}$$

Propriedade

Se $X = (X_E, X_D)$ é uma seqüência de 32 bits escolhida aleatoriamente com distribuição uniforme, então:

$$P[T(X) = X] = \frac{1}{2} \quad \text{e} \quad P[T(X) \neq X] = \frac{1}{2}$$

Algoritmo RC6T - Cifração

$B = B + S[0]$
$D = D + S[1]$
para $i = 1$ até r faça{
$B = T(B)$
$D = T(D)$
$t = (B \times (2B + 1)) \lll \lg w$
$u = (D \times (2D + 1)) \lll \lg w$
$A = ((A \oplus t) \lll u) + S[2i]$
$C = ((C \oplus u) \lll t) + S[2i + 1]$
$(A, B, C, D) = (B, C, D, A)$
}
$A = A + S[2r + 2]$
$C = C + S[2r + 3]$

Algoritmo RC6T - Desempenho

Tabela: Velocidade em Kbytes/segundo dos algoritmos RC6 e RC6T

Algoritmo	r	Velocidade
RC6	20	4028
RC6T	20	3346
RC6T	18	3423
RC6T	16	3526

- RC6T-32/20/16 é 17% mais lento que RC6-32/20/16
- RC6T-32/18/16 é 15% mais lento que RC6-32/20/16
- RC6T-32/16/16 é 13% mais lento que RC6-32/20/16

Teste χ^2

Seja $X = X_0, X_1, \ldots, X_{n-1}$ variáveis aleatórias independentes tais que $X_i \in \{a_0, a_1, \ldots, a_{m-1}\}$ com distribuição de probabilidade desconhecida $\mathbf{p}$, e $N_{a_j}(X)$ o número de vezes que X assume o valor a_j. A estatística χ^2 de X que estima a distância entre a distribuição observada $\mathbf{p}$ e a distribuição uniforme esperada $\pi = (\pi_0, \pi_1, \ldots, \pi_{m-1})$ é definida como:

$$\chi^2 = \sum_{i=0}^{m-1} \frac{(N_{a_i}(X) - n\pi_i)^2}{n\pi_i}$$

Teste χ^2

Depois de calculada a estatística χ^2 é possível efetuar a decisão no seguinte teste de hipótese:

$$\begin{cases} H_0 : \mathbf{p} = \pi & (\textit{hipótese nula}) \\ H_1 : \mathbf{p} \neq \pi & (\textit{hipótese alternativa}) \end{cases}$$

No teste χ^2 o número de graus de liberdade é igual a $m - 1$

- Variáveis aleatórias de 6 bits $\Rightarrow$ 63 graus de liberdade
- Variáveis aleatórias de 8 bits $\Rightarrow$ 255 graus de liberdade
- Variáveis aleatórias de 10 bits $\Rightarrow$ 1023 graus de liberdade

Teste χ^2

Tabela: Distribuição χ^2 com diferentes graus de liberdade

Nível	0.5	0.60	0.70	0.80	0.90	0.95	0.99
63 graus de liberdade	62	65	68	72	77	82	92
255 graus de liberdade	254	260	266	273	284	293	310
1023 graus de liberdade	1022	1033	1046	1060	1081	1098	1131

Por exemplo, (nível, χ^2) = (0.95, 82) na Tabela significa que o valor da estatística χ^2 excederá 82 somente 5% das vezes se a distribuição da observação X for realmente uniforme

Teste χ^2

Teorema 1

Quando H_0 é verdadeira, a estatística χ^2 definida anteriormente segue a distribuição χ^2 cujo grau de liberdade é aproximadamente $m-1$. Em adição, a média ou variância esperada é calculada por $E_{H_0}(\chi^2) = m-1$ ou $V_{H_0}(\chi^2) = 2(m-1)$, respectivamente.

Teorema 2

Quando H_1 é verdadeira, a estatística χ^2 definida anteriormente segue a distribuição χ^2 não-central cujo grau de liberdade é aproximadamente $m-1$. Em adição, a média ou variância esperada é calculada por $E_{H_1}(\chi^2) = m-1+n\theta$ ou $V_{H_1}(\chi^2) = 2(m-1)+4n\theta$, respectivamente, onde $n\theta$ é chamado de parâmetro não-central e temos que $n\theta = n\sum_{i=0}^{m-1} \frac{(\pi_i - P(a_i))^2}{\pi_i}$, onde $P(a_i)$ é a probabilidade de ocorrência de a_i.

Correlações nos Algoritmos RC6 e RC6T

- **Teste 1:** Estatística χ^2 de $lsb_3(A_{r+1})||lsb_3(C_{r+1})$ no caso de $lsb_5(A_0) = lsb_5(C_0) = 0$
- **Teste 2:** Estatística χ^2 de $lsb_3(A_{r+1})||lsb_3(C_{r+1})$ no caso de $lsb_5(B_0) = lsb_5(D_0) = 0$

Tabela: Teste 1 no RC6-32/r/16 com $r = 2, 4$ iterações

r	$\log_2(\#$ textos$)$	χ^2	$\#$ testes
2	14	72	20
2	15	96	20
4	30	59	10
4	31	134	10

Tabela: Teste 1 no RC6T-32/r/16 com $r = 2, 4$ iterações

r	$\log_2(\#$ textos$)$	χ^2	$\#$ testes
2	18	79	20
2	19	123	20
4	36	79	1
4	37	137	1

Tabela: Teste 2 no RC6-32/r/16 com $r = 3, 5$ iterações

r	$\log_2(\#$ textos$)$	χ^2	$\#$ testes
3	15	72	20
3	16	90	20
5	32	74	10
5	33	115	10

Tabela: Teste 2 no RC6T-32/r/16 com $r = 3, 5$ iterações

r	$\log_2(\#$ textos$)$	χ^2	$\#$ testes
3	22	73	20
3	23	112	20
5	39	54	1
5	40	128	1

Ataque de Distinção

Entrada: Algoritmo RC6(RC6T) ou permutação aleatória,
Número n de textos;

Saída: Responde se a entrada é RC6(RC6T) ou não;

1. considere n textos (A, B, C, D) cifrados com RC6(RC6T) ou não;
2. para $i = 1$ até n faça:
   $j = lsb_3(A_i)||lsb_3(C_i)$;
   incremente $array[j]$;
3. calcule χ^2 de $array$;
4. se (χ^2 calculado) ≥ 82
   então retorna *"A entrada é RC6(RC6T)"*;
   senão retorna *"A entrada é uma permutação aleatória"*.

Tabela: Complexidade para distinguir o RC6-32/r/16 usando o Teste 2

r	$\log_2(\#$ textos$)$	χ^2	Comentário
3	15	72	Implementado, média de 20 testes
3	16	91	Implementado, média de 20 testes
5	31	53	Implementado, média de 10 testes
5	32	95	Implementado, média de 10 testes

Considerando um fator igual a 2^{16} textos adicionais para se medir valores χ^2 equivalentes a cada 2 iterações, estimamos que para o RC6 com r iterações resultados semelhantes serão alcançados com:

$$2^{16}(2^{16})^{\frac{r-3}{2}} = 2^{8r-8} textos \Rightarrow \log_2(\#textos) = 8r - 8$$

Ataque de Distinção

Tabela: Complexidade para distinguir o RC6-32/r/16 usando o Teste 2

r	$\log_2(\#$ textos$)$	χ^2	Comentário
7	48		Estimado
9	64		Estimado
11	80		Estimado
13	96		Estimado
15	112		Estimado
17	128		> 118

Ataque de Distinção

Tabela: Complexidade para distinguir o RC6T-32/r/16 usando o Teste 2

r	$\log_2(\#$ textos$)$	χ^2	Comentário
3	22	78	Implementado, média de 20 testes
3	22.6	92	Implementado, média de 20 testes
5	39	66	Implementado, apenas 1 teste
5	39.4	84	Implementado, apenas 1 teste

Considerando um fator igual a $2^{16.8}$ textos adicionais para se medir valores χ^2 equivalentes a cada 2 iterações, estimamos que para o RC6 com r iterações resultados semelhantes serão alcançados com:

$$2^{22.6}(2^{16.8})^{\frac{r-3}{2}} = 2^{8.4r-2.6} textos \Rightarrow \log_2(\#textos) = 8.4r - 2.6$$

Ataque de Distinção

Tabela: Complexidade para distinguir o RC6T-32/r/16 usando o Teste 2

r	$\log_2(\#$ textos$)$	χ^2	Comentário
7	56.2		Estimado
9	73		Estimado
11	89.8		Estimado
13	106.6		Estimado
15	123.4		> 118
17	140.2		

Ataque contra o algoritmo RC6(RC6T) sem "post-whitening"

Tabela: Notações adotadas no algoritmo de ataque

Notação
$F(X) = [X(2X+1) \pmod{2^w}] \lll \lg w$
$(y_b, y_d) = (lsb_3(B_{r+1}), lsb_3(D_{r+1}))$
$(x_a, x_c) = (lsb_5(F(C_{r+1})), lsb_5(F(A_{r+1})))$
$(s_a, s_c) = (lsb_2(S[2r]), lsb_2(S[2r+1]))$
$s = s_a \|\| s_c$

Observação: x_a (respectivamente x_c) é a quantidade de rotação sobre A_r (respectivamente C_r) na *r-ésima* iteração.

Ataque contra o algoritmo RC6(RC6T) sem "post-whitening"

1. Escolha um texto legível (A_0, B_0, C_0, D_0) tal que $lsb_5(B_0) = lsb_5(D_0) = 0$ e o cifre por r iterações.
2. Para cada (s_a, s_c), decifre $y_b||y_d$ com a chave $0||s_a, 0||s_c$ por 1 iteração para $z_a||z_c$, sendo $z = z_a||z_c$ um inteiro de 6 bits.
3. Para cada s, x_a, x_c e z, atualize cada vetor incrementando $count[s][x_a][x_c][z]$.
4. Para cada s, x_a e x_c, calcule $\chi^2[s][x_a][x_c]$.
5. Calcule a média $med[s]$ de $\{\chi^2[s][x_a][x_c]\}_{x_a,x_c}$ para cada s e retorne o valor s com maior $med[s]$ como $lsb_2(S[2r])||lsb_2(S[2r+1])$.

Ataque contra o algoritmo RC6 sem "post-whitening"

- Complexidade do ataque de recuperação da chave sobre o algoritmo RC6 sem *"post-whitening"*:

$$2^{-8}2^{21.8}(2^{16})^{\frac{r-3}{2}} = 2^{8r-10.2} \ \textit{textos}$$

- Complexidade de tempo do ataque de recuperação da chave sobre o algoritmo RC6 sem *"post-whitening"*:

$$(\#\textit{de textos}) \times 2^4 = 2^{8r-10.2} \times 2^4 = 2^{8r-6.2} \text{ u.t.}$$

Ataque contra o algoritmo RC6T sem "post-whitening"

- Complexidade do ataque de recuperação da chave sobre o algoritmo RC6T sem *"post-whitening"*:

$$2^{-8.5}2^{27.2}(2^{17})^{\frac{r-3}{2}} = 2^{8.5r-6.8} \textit{ textos}$$

- Complexidade de tempo do ataque de recuperação da chave sobre o algoritmo RC6T sem *"post-whitening"*:

$$(\#\textit{de textos}) \times 2^4 = 2^{8.5r-6.8} \times 2^4 = 2^{8.5r-2.8} \text{ u.t.}$$

Conclusão

- Um ataque de distinção pode ser aplicado ao RC6 com 15 iterações, sendo necessário 2^{112} textos; já para o RC6T foi estimado que 13 iterações podem ser atacadas utilizando-se $2^{106.6}$ textos
- O algoritmo de ataque de recuperação da chave apresentado pode quebrar 16 iterações do RC6 sem *"post-whitening"* usando $2^{117.8}$ textos e com probabilidade de sucesso de 95%; mas no caso do RC6T sem *"post-whitening"* pode quebrar 14 iterações usando $2^{112.2}$ textos

Perguntas?