Національний Технічний Університет України
“Київський Політехнічний Інститут”
Фізико-Технічний Інститут

СИМЕТРИЧНА КРИПТОГРАФІЯ

КОМП'ЮТЕРНИЙ ПРАКТИКУМ №4:
Побудова генератора псевдовипадкових послідовностей на лінійних регістрах зсуву (генератора Джиффі) та його кореляційний криптоаналіз

Виконав студент 3-го курсу
групи ФІ-14
Геращенко Володимир

Київ 2024

1 Мета роботи

Ознайомлення з деякими принципами побудови криптосистем на лінійних регістрах зсуву; практичне освоєння програмної реалізації лінійних регістрів зсуву (ЛРЗ); ознайомлення з методом кореляційного аналізу криптосистем на прикладі генератора Джиффі.

2 Хід роботи

2.1 Реалізація ЛРЗ і генератору Джиффі

Саме тут проблем не було - ЛРЗ містить маску і стан у вигляді цілих невід'ємних чисел, а генератор Джиффі просто містить L1, L2, L3.

2.2 Оптимізація аналізу генератора Джиффі

Так як хотілося зробити звичайний варіант, а не для "дурників то прийшлось якось оптимізовувати сам аналіз ЛРЗ. Ми скористались тим, що поліноми для L1, L2 і L3 - незвідні, тому можна було згенерувати одразу m-послідовність для кожного з них, і зберігали їх в пам'яті. Також для максимально ефективних перевірок для L3 ми спочатку перевіряли перші 64 біта - якщо не співпадають, то переходили до наступного.

2.3 Знаходження параметрів C, β і N^*

Маємо, що:

$$C = Np_1 + t_{1-\alpha}\sqrt{Np_1(1-p_1)} = \frac{N}{4} + t_{0.99}\sqrt{N\frac{3}{16}}$$

і

$$t_{1-\beta} = \frac{Np_2 - C}{\sqrt{Np_2(1-p_2)}} = \frac{\frac{N}{2} - C}{\sqrt{\frac{N}{4}}} \Rightarrow C = \frac{N}{2} - t_{1-\beta}\frac{\sqrt{N}}{2}$$

де t_γ - γ-квантиль нормального розподілу.

$$\begin{cases} C = \frac{N}{4} + t_{0.99}\sqrt{N\frac{3}{16}} \\ C = \frac{N}{2} - t_{1-\beta}\frac{\sqrt{N}}{2} \end{cases}$$

Віднімаємо:

$$0 = -\frac{N}{4} + \sqrt{N}(t_{0.99}\frac{\sqrt{3}}{4} + \frac{t_{1-\beta}}{2})$$

$$\sqrt{N}(-\frac{1}{4}\sqrt{N} + (t_{0.99}\frac{\sqrt{3}}{4} + \frac{t_{1-\beta}}{2}) = 0$$

Так як $N = 0$ не підходить, то

$$\sqrt{N} = 4(t_{0.99}\frac{\sqrt{3}}{4} + \frac{t_{1-\beta}}{2})$$

$$N = 16(t_{0.99}\frac{\sqrt{3}}{4} + \frac{t_{1-\beta}}{2})^2$$

Тепер, можемо знайти β за допомогою нерівності:

$$\beta < \frac{1}{M}$$

де $M = 2^n$, n - степінь генеруючого полінома ЛРЗ. Так як нам потрібна приблизна оцінка, то ми можемо брати $\beta = \frac{1}{2^M}$. Також відомо знаємо $t_{0.99} = 2.3263$ Тепер просто підставимо значення для різних ЛРЗ:

1. Для дурників:
   - L1: $n = 25, \beta < \frac{1}{2^{25}}, t_{1-\beta} = 5.420 : N \approx 221.095 \Rightarrow N = 222, C \approx 70.508 \Rightarrow C = 71$
   - L2: $n = 26, \beta < \frac{1}{2^{26}}, t_{1-\beta} = 5.543 : N \approx 228.447 \Rightarrow N = 229, C \approx 72.337 \Rightarrow C = 73$
2. Звичайний варіант:
   - L1: $n = 30, \beta < \frac{1}{2^{30}}, t_{1-\beta} = 6.009 : N \approx 257.538 \Rightarrow N = 258, C \approx 80.55 \Rightarrow C = 81$
   - L2: $n = 31, \beta < \frac{1}{2^{31}}, t_{1-\beta} = 6.121 : N \approx 264.738 \Rightarrow N = 265, C \approx 82.574 \Rightarrow C = 83$

3 Результати роботи

Був взятий як завжди 1-ший варіант. Результати роботи буду вставляти скріншотами, так як вставляти бітові послідовністі у латех та ще морока...

3.1 Варіант для дурників

Рис. 1: Варіант для дурників

Наші кандидати перевіряються одразу і підставляються у генератор Джиффі, що дає нам ту саму послідовність:
L1 = 6050500 = 0010111000101001011000100;
L2 = 65635703 = 11111010011000010101110111;
L3 = 42841770 = 010100011011011011010101010;

3.2 Звичайний варіант

Рис. 2: Звичайний варіант

Так само і для звичайного варіанту:
L1 = 960529051 = 111001010000000100000101001101l;
L2 = 849466889 = 0110010101000011101011000001001;
L3 = 2204291428 = 10000011011000101101000101100100;

4 Висновок

За результатами цієї лабораторної можемо побачити, що генератор Джиффі не дуже криптостійкий та з його вихідної послідовності можна знайти початкові заповнення для L1, L2 і

L3 просто використовуючи перебір та математичну статистику. Але так як складність такого перебору все одно $2^{n_1} + 2^{n_2} + 2^{n_3}$ це все одно може бути довго :).