Національний технічний університет України
«Київський політехнічний інститут»

Фізико технічний інститут

Кафедра математичних методів захисту інформації

МЕТОДИ КРИПТОАНАЛІЗУ 2
КОМП'ЮТЕРНИЙ ПРАКТИКУМ №1

"Алгебраїчна атака на фільтрувальний генератор гами"

Виконали:
студенти групи ФІ-12м
Корж Нікіта
Тафтай Анастасія

Перевірив:
Курінний О.В.

Київ 2022

Мета роботи:

Практична реалізація алгебраїчної атаки на фільтрувальний генератор гами; набуття навичок роботи з системами комп'ютерної алгебри.

Завдання

1) Знайти функції мінімального степеня ідеалів $\langle f \oplus 1 \rangle$ та $\langle f \rangle$ за допомогою побудови базису Грьобнера. Якщо побудова базису для одного з ідеалів $\langle f \oplus 1 \rangle$ або $\langle f \rangle$ є занадто трудомісткою з точки зору обчислювальних ресурсів, то дозволяється будувати лише один базис – за умови, що цього буде достатньо для проведення атаки.

2) Визначити кількість рівнянь, необхідних для відновлення початкового стану. Побудувати систему рівнянь меншого степеня відносно початкового стану генератора.

3) Знайти розв'язки отриманої системи рівнянь. Зауважимо, що початковий стан за умовою комп'ютерного практикуму є ненульовим вектором.

4) Перевірити, що початковий стан відновлено правильно, згенерувавши відрізок гами відповідної довжини й порівнявши його з вхідними даними. Для побудови базису Грьобнера та розв'язання системи рівнянь можна користуватись будь-якими системами комп'ютерної алгебри, а також наявними імплементаціями.

Варіант завдання: 5

GitHub: https://github.com/NKorzhik/MC2Lab1

Хід роботи

Потужність побудованих базисів Грьобнера, всі знайдені функції мінімального степеня:

Потужності базисів:
Для $\langle f \rangle$: 7423
Для $\langle f \oplus 1 \rangle$: 8191
Мінімальні поліноми:
Для $\langle f \rangle$: $h_1 = x_{28} * x_6 + x_6 + x_{28} + 1$, $deg(h_1) = 2$;
Для $\langle f \oplus 1 \rangle$: $h_2 = x_{28} * x_6 + x_{28}$, $deg(h_2) = 2$;

Кількість рівнянь в побудованій системі, перші 10 рівнянь, всі розв'язки системи:

Кількість рівнянь в побудованій системі: 1000
Перші 10 рівнянь:
$x_{29} * x_7 + x_{29}$,
$x_{30} * x_8 + x_8 + x_{30} + 1$,
$x_{31} * x_9 + x_{31}$,
$x_{32} * x_{10} + x_{32}$,
$x_{33} * x_{11} + x_{33}$,
$x_{34} * x_{12} + x_{34}$,
$x_{35} * x_{13} + x_{35}$,
$x_{36} * x_{14} + x_{36}$,
$x_{37} * x_{15} + x_{15} + x_{37} + 1$,
$x_{38} * x_{16} + x_{16} + x_{38} + 1$.
Розв'зки системи рівнянь:
x0
x1 + 1
x2
x3
x4 + 1
x5 + 1
x6
x7
x8
x9
x10 + 1
x11 + 1
x12 + 1
x13 + 1
x14 + 1
x15
x16
x17
x18 + 1

x19 + 1
x20 + 1
x21
x22 + 1
x23
x24 + 1
x25 + 1
x26 + 1
x27 + 1
x28 + 1
x29
x30 + 1
x31
x32
x33
x34
x35
x36
x37 + 1
x38 + 1
x39 + 1
x40
x41 + 1
x42
x43 + 1
x44 + 1
x45
x46 + 1
x47 + 1
x48 + 1
x49 + 1
x50 + 1
x51 + 1
x52
x53
x54 + 1
x55 + 1
x56
x57 + 1
x58 + 1
x59
x60 + 1
x61
x62
x63

Час виконання кожної операції (побудова базису Грьбонера та системи рівнянь):

The time of GB1 : 205.79683256149292
The time of GB2 : 296.49295020103455
time for solving the system of equations : 69.99663662910461

Знайдений початковий стан генератора гами

State = [0, 1, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0]

Висновки

В даній роботі ми познайомились з алгебраїчною атакою на фільтрувальний генератор гами, реалізували атаку та успішно її провели на тестувальних данних. Для реалізації атаки було встановлено SageMath на локальний комп'ютер, який має наступні системні параметри: процессор: Intel core i5-6200U та ОЗУ: 8 гб.