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-12мн
Мазур Анастасія
Мітрофанова Еліна

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 : 1

Хід роботи

Потужність побудованих базисів Грьобнера:

Для$\langle f \rangle$: 2239 Polynomials in 32 Variables
Для$\langle f \oplus 1 \rangle$: 2239 Polynomials in 32 Variables

Всі знайдені функції мінімального степеня:

Для$\langle f \rangle$: $h_1 = x_{53}x_0 + x_0 + x_{53} + 1$
Для$\langle f \oplus 1 \rangle$: $h_2 = x_{53}x_0 + x_{53}$

Перші 10 рівнянь:

$x_{54}x_1 + x_{54}$
$x_{55}x_2 + x_2 + x_{55} + 1$
$x_{56}x_3 + x_{56}$
$x_{57}x_4 + x_4 + x_{57} + 1$
$x_{58}x_5 + x_5 + x_{58} + 1$
$x_{59}x_6 + x_6 + x_{59} + 1$
$x_{60}x_7 + x_{60}$
$x_{61}x_8 + x_8 + x_{61} + 1$
$x_{62}x_9 + x_{62}$
$x_{63}x_{10} + x_{63}$
Кількість рівнянь у побудованій системі: 1000

Всі розв'язки системи:

x_0
$x_1 + 1$
x_2
x_3
$x_4 + 1$
$x_5 + 1$
$x_6 + 1$
x_7
x_8
$x_9 + 1$
$x_{10} + 1$
$x_{11} + 1$
$x_{12} + 1$
x_{13}
$x_{14} + 1$
x_{15}

x_{16}
x_{17}
$\mathrm{x}_{18} + 1$
$\mathrm{x}_{19} + 1$
x_{20}
$\mathrm{x}_{21} + 1$
x_{22}
x_{23}
$\mathrm{x}_{24} + 1$
$\mathrm{x}_{25} + 1$
x_{26}
$\mathrm{x}_{27} + 1$
$\mathrm{x}_{28} + 1$
x_{29}
$\mathrm{x}_{30} + 1$
$\mathrm{x}_{31} + 1$
$\mathrm{x}_{32} + 1$
$\mathrm{x}_{33} + 1$
$\mathrm{x}_{34} + 1$
$\mathrm{x}_{35} + 1$
$\mathrm{x}_{36} + 1$
$\mathrm{x}_{37} + 1$
x_{38}
$\mathrm{x}_{39} + 1$
x_{40}
x_{41}
$\mathrm{x}_{42} + 1$
$\mathrm{x}_{43} + 1$
x_{44}
$\mathrm{x}_{45} + 1$
$\mathrm{x}_{46} + 1$
$\mathrm{x}_{47} + 1$
x_{48}
$\mathrm{x}_{49} + 1$
$\mathrm{x}_{50} + 1$
x_{51}
$x_{52} + 1$
$x_{53} + 1$
x_{54}
$x_{55} + 1$
x_{56}
$x_{57} + 1$
$x_{58} + 1$
$x_{59} + 1$
x_{60}
$x_{61} + 1$
x_{62}
$x_{63} + 1$

Час виконання кожної операції:

Побудова базису Грьобнера GB1 : 588.1085448265076
Побудова базису Грьобнера GB2 : 7.107132196426392
Час вирішення системи рівнянь : 54.502185583114624

Знайдений початковий стан генератора гами

(0, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1)

Програмний код для знаходження початкового стану:

Побудова системи рівнянь

92]:
```
equations = []
for i in range(1000):
    current_state = C * current_state
    if gamma[i] == '0':
        equations.append(h1(*(current_state)))
    else:
        equations.append(h2(*(current_state)))

for i in range(10):
    print(equations[i])
```

```
x54*x1 + x54
x55*x2 + x2 + x55 + 1
x56*x3 + x56
x57*x4 + x4 + x57 + 1
x58*x5 + x5 + x58 + 1
x59*x6 + x6 + x59 + 1
x60*x7 + x60
x61*x8 + x8 + x61 + 1
x62*x9 + x62
x63*x10 + x63
```

83]:
```
start = time.time()
I = Ideal(equations)
GB = I.groebner_basis()
end = time.time()
print("Solution time : ", end-start)
```

```
Solution time :  54.502185583114624
```

Висновки

У даній роботі побудовано алгебраїчну атаку на фільтрувальний генератор гами. Успішно відновленно початковий стан генератора. Кількість рівнянь для відновлення початкового стану становить 1000. Побудова базису Грьобнера ідеалу $\langle f \rangle$ зайняла майже 10 хвилин, а $\langle f \oplus 1 \rangle$ – близько 8 секунд. Початковий стан був відновленний приблизно за 55 секунд.