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
Морозюк Анастасія
Гетьман Дмитро

Перевірив: Курінний О.В.

Київ 2022

Мета роботи:

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

Постановка задачі:

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 : 14

Хід роботи:

Потужність побудованих базисів Грьобнера

Для $\langle f \rangle$: 1604 Polynomials in 29 Variables

Для $\langle f \oplus 1 \rangle$: 1604 Polynomials in 29 Variables

Всі знайдені функції мінімального степеня

Для $\langle f \rangle$: $x_{37}*x_9 + x_{37}$, степінь 2
Для $\langle f \oplus 1 \rangle$: $x_{37}*x_9 + x_9 + x_{37} + 1$, степінь 2

Кількість рівнянь у побудованій системі: 1000

Перші 10 рівнянь:

$x_{38}*x_{10} + x_{38}$
$x_{39}*x_{11} + x_{11} + x_{39} + 1$
$x_{40}*x_{12} + x_{12} + x_{40} + 1$
$x_{41}*x_{13} + x_{13} + x_{41} + 1$
$x_{42}*x_{14} + x_{14} + x_{42} + 1$
$x_{43}*x_{15} + x_{43}$
$x_{44}*x_{16} + x_{16} + x_{44} + 1$
$x_{45}*x_{17} + x_{45}$
$x_{46}*x_{18} + x_{18} + x_{46} + 1$
$x_{47}*x_{19} + x_{19} + x_{47} + 1$

Всі розв'язки системи:

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

x_{13}
x_{14}
$x_{15} + 1$
$x_{16} + 1$
$x_{17} + 1$
x_{18}
$x_{19} + 1$
x_{20}
x_{21}
x_{22}
$x_{23} + 1$
$x_{24} + 1$
$x_{25} + 1$
x_{26}
$x_{27} + 1$
x_{28}
$x_{29} + 1$
x_{30}
$x_{31} + 1$
$x_{32} + 1$
$x_{33} + 1$
$x_{34} + 1$
x_{35}
x_{36}
x_{37}
x_{38}
x_{39}
x_{40}
$x_{41} + 1$
$x_{42} + 1$
$x_{43} + 1$
$x_{44} + 1$
$x_{45} + 1$
$x_{46} + 1$
x_{47}
x_{48}
$x_{49} + 1$
$x_{50} + 1$
$x_{51} + 1$
x_{52}
x_{53}
x_{54}
x_{55}
x_{56}
$x_{57} + 1$
x_{58}

$x_{59} + 1$
$x_{60} + 1$
x_{61}
$x_{62} + 1$
$x_{63} + 1$

Час виконання кожної операції:

1) Час пошуку базису Грьобнера для $\langle f \rangle$: 387.0853052139282
2) Час пошуку базису Грьобнера для $\langle f \oplus 1 \rangle$: 808.2178425788879
3) Час пошуку розв'язку: 132.80726838111877

Знайдений початковий стан генератора гами

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

Програмний код можна знайти за посиланням: https://github.com/AnastasiiaMoroziuk/MC2

Висновок:

В даній роботі було практично реалізовано алгераїчну атаку на фільтрувальний генератор гами. Успішно відновлено початковий стан генератора гами. Для реалізації було локально встановлено SageMath.