МІНІСТЕРСТВО ОСВІТИ, НАУКИ, МОЛОДІ ТА СПОРТУ УКРАЇНИ
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ»
ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ

Комп'ютерний практикум 1

Алгебраїчна атака на фільтрувальний генератор гами

Підготували:
студенти групи ФІ-22мн
Ковальчук О.М.
Коломієць А.Ю.

Перевірив:
Курінний О.В.

Київ – 2023

Комп’ютерний практикум 1

Алгебраїчна атака на фільтрувальний генератор гами

Варіант 6

Мета роботи

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

Порядок виконання роботи

1. Знайти функції мінімального степеня ідеалів $<f>$ та $<f \oplus 1>$ за допомогою побудови базису Грьобнера. Якщо побудова базису для одного з ідеалів $<f>$ або $<f \oplus 1>$ 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 (якщо не вдається визначити аналітично, то можна підбирати кількість рівнянь емпірично). 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.

Хід роботи

1. Ознайомлення з основами роботи з системою SAGE та методичними вказівками.
2. Налаштування та підключення системи SAGE до VSCode для подальшої роботи з нею.
3. Розпочинаємо виконання практичної частини завдання, зчитуючи дані згідно з варіантом та перетворюючи їх у відповідний формат.
4. Будуємо ідеали $<f>$ та $<f \oplus 1>$ і для кожного з них обчислюємо базис Грьобнера.
5. Складаємо систему рівнянь меншого степеня. Отримали два рівняння степені котрих рівні 2. Кількість рівнянь обрано було 1000.
6. Знаходимо розв’язок побудованої системи рівнянь.
7. Знаходимо початковий стан послідовності гамми.
8. Повторно складаємо систему рівнянь зменшуючи їх кількість до 900. І намагаємося знайти розв’язки системи, і перевірняємо чи правильно було знайдено початковий стан послідовності гамма.

Результати

Потужність побудованих базисів Грьобнера:

- *для ідеалу $< f >$: Polynomial Sequence with 7423 Polynomials in 29 Variables*

- *для ідеалу $< f \oplus 1 >$: Polynomial Sequence with 8191 Polynomials in 29 Variables*

Функції мінімального степеня серед побудованих базисів *(AI = 2)*:

$$h_1(x)=x_{28}*x_6 + x_6 + x_{28} + 1, \qquad h_2(x)=x_{28}*x_6 + x_{28}.$$

Кількість рівнянь в побудованій системі: спершу зробили для *1000*, потім зменшили кількість до *900* та виявили, що цієї кількості теж достатньо.

Перші 10 рівнянь:

$$x_{29}*x_7 + x_7 + x_{29} + 1=0, \qquad x_{34}*x_{12} + x_{12} + x_{34} + 1=0,$$

$$x_{30}*x_8 + x_{30}=1, \qquad x_{35}*x_{13} + x_{35}=1,$$

$$x_{31}*x_9 + x_{31}=1, \qquad x_{36}*x_{14} + x_{14} + x_{36} + 1=0,$$

$$x_{32}*x_{10} + x_{10} + x_{32} + 1=0, \qquad x_{37}*x_{15} + x_{37}=1,$$

$$x_{33}*x_{11} + x_{33}=1, \qquad x_{38}*x_{16} + x_{16} + x_{38} + 1=0.$$

Єдиний розв'язок системи:

[0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 0, 1]

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

GB(<f>)	GB(<f⊕1>)	GB(система_1000)	GB(система_900)
16 m 6,2 s	25 m 49,8 s	4 m 1 s	7 m 38 s

Висновки

У ході виконання завдань комп'ютерного практикуму було розглянуто та реалізовано алгебраїчну атаку на фільтрувальний генератор гами з використанням базисів Грьобнера. Для побудови базисів Грьобнера та розв'язку системи рівнянь була встановлена та використана система комп'ютерної алгебри SAGE. У результаті було успішно знайдено початковий стан генератора гами із заданою фільтрувальною функцією та для заданого вихідного відрізку гами. Експериментним методом було виявлено, що для нашого варіанту завдань є достатнім побудувати систему із 900 рівнянь. Це значення теоретично можна зробити ще меншим, проте в цьому випадку доведеться «пожертвувати» часом виконання для знаходження базису Грьобнера.

https://github.com/andrew-kolomiets/METHODS-OF-CRYPTOANALYSIS-STREAM-CIPHERS.git