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

Комп’ютерний практикум 2

Статистична атака на комбінувальний генератор гами

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

Перевірив:
Курінний О.В.

Київ – 2023

Комп'ютерний практикум 2

Статистична атака на комбінувальний генератор гами

Варіант 4

Мета роботи

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

Порядок виконання роботи

1. Обчислити коефіцієнти Уолша-Адамара функції f. За допомогою цих коефіцієнтів знайти всі афінні статистичні аналоги f та ймовірності збігу цих аналогів з f.

2. Вибрати набір статистичних аналогів g1, . . . , gr, що будуть використані для відновлення початкового стану генератора. Для всіх функцій з цього набору обчислити необхідну кількість матеріалу T1, . . . , Tr відповідно, зафіксувавши $\delta = 0.01$. Побудувати низку атак на початкові стани регістрів, тим самим повністю відновивши початковий стан генератора гами.

3. Перевірити, що початковий стан генератора гами відновлено правильно, згенерувавши відрізок гами відповідної довжини й порівнявши його з вхідними даними.

Хід роботи

1. Ознайомлення з необхідним для виконання практикуму функціоналом в системі SAGE та методичними вказівками.
2. Розпочинаємо виконання практичної частини завдання, зчитуючи дані згідно з варіантом та перетворюючи їх у відповідний формат.
3. Обчислюємо коефіцієнти Уолша-Адамара та зберігаємо всі їх ненульові значення.
4. Знаходимо значення cor (f) - найбільшого числа k, для якого функція f є кореляційно-імунною порядку k.
5. Знаходимо всі афінні статистичні аналоги та ймовірності збігу з функцією f .
6. Обрали набір статистичних аналогів g1, . . . , gr, що будуть використані для відновлення початкового стану генератора. Для всіх функцій з цього набору обчислили необхідну кількість матеріалу T1, . . . , Tr відповідно, зафіксувавши $\delta = 0.01$.
7. Побудували низку атак на початкові стани регістрів, тим самим повністю відновивши початковий стан генератора гами.
8. Зробили перевірку, що початковий стан генератора гами відновлено правильно, згенерувавши відрізок гами відповідної довжини й порівнявши його з вхідними даними.

Результати

Усі афінні статистичні аналоги та ймовірності збігу з функцією f:

1) g = x3 ⊕ 1, Pr{f(x) = g(x)} = 0.75

2) g = x3 ⊕ x5 ⊕ 1, Pr{f(x) = g(x)} = 0.75

3) g = x1 ⊕ x4 , Pr{f(x) = g(x)} = 0.625

4) g = x1 ⊕ x4 ⊕ x5 ⊕ 1, Pr{f(x) = g(x)} = 0.625

5) g = x1 ⊕ x3 ⊕ x4 , Pr{f(x) = g(x)} = 0.625

6) g = x1 ⊕ x3 ⊕ x4 ⊕ x5 ⊕ 1, Pr{f(x) = g(x)} = 0.625

7) g = x0 ⊕ x2 , Pr{f(x) = g(x)} = 0.625

8) g = x0 ⊕ x2 ⊕ x5 ⊕ 1, Pr{f(x) = g(x)} = 0.625

9) g = x0 ⊕ x2 ⊕ x3 ⊕ 1, Pr{f(x) = g(x)} = 0.625

10) g = x0 ⊕ x2 ⊕ x3 ⊕ x5 , Pr{f(x) = g(x)} = 0.625

Значення cor (f): cor(f) = 0

Набір статистичних аналогів g1, . . . , gr, що будуть використані для відновлення початкового стану генератора:

1) g = x3 ⊕ 1

2) g = x3 ⊕ x5 ⊕ 1

3) g = x1 ⊕ x4

Для відновлення початкових станів x0 та x2 була використана комбінувальна функція f, яка задана у варіанті 4:

f = x0*x3*x5 ⊕ x1*x3*x5 ⊕ x1*x5 ⊕ x2*x3*x5 ⊕ x3*x4*x5 ⊕ x3*x5 ⊕ x3 ⊕ x4*x5 ⊕ x5 ⊕ 1

Необхідна кількість матеріалу T1, . . . , Tr:

T1 = 369

T2 = T3 = 590

Для відновлення початкових станів x0 та x2 брали T = 100

Мінімальні значення статистик (абсолютні й відносні) при побудові відповідних атак:

Відновлення x3

Абсолютне мінімальне значення статистики: 105

Відносне мінімальне значення статистики: min hamming distance = 0.2845528455284553

Відновлення x5

Абсолютне мінімальне значення статистики: 141

Відносне мінімальне значення статистики: min hamming distance = 0.23898305084745763

Відновлення x1 та x4

Абсолютне мінімальне значення статистики: 214

Відносне мінімальне значення статистики: min hamming distance = 0.36271186440677966

Час виконання кожної атаки

Відновлення x3: 2.3 с

Відновлення x5: 3.1 с

Відновлення x1 та x4: 28 хв 38 с

Відновлення x0 та x2: 13 хв

Знайдений початковий стан генератора гами:

[X0, X1, X2, X3, X4, X5]: [876, 764,697, 537,996,714]

Висновки

У ході виконання завдань комп'ютерного практикуму було розглянуто та реалізовано статистичну атаку на комбінувальний генератор гами. Для реалізації атаки була використана система комп'ютерної алгебри SAGE. Були обчислені коефіцієнти Уолша-Адамара, знайдені усі їх ненульові значення та на основі цих значень знайдено всі афінні статистичні аналоги та ймовірності збігу з функцією f. В якості набору статистичних аналогів g1, . . . , gr, що будуть використані для відновлення початкового стану генератора, було обрано ті афінні аналоги, для яких ймовірності збігу з функцією f були максимальними. Потім цей набір доповнився функціям таким чином, щоб серед змінних в усіх обраних аналогах були x0, x1, x2, x3, x4, x5. Далі за допомогою цих обраних аналогів g були проведені атаки та успішно відновлено початковий стан генератора.

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