Комп'ютерний практикум 1

Алгебраїчна атака на фільтрувальний генератор гами

Мета роботи

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

Необхідні теоретичні відомості

Схема нелінійної фільтрації є одним зі стандартних способів побудови генераторів гами. Нагадаємо, що фільтрувальний генератор гами складається з таких компонентів (рис. 1):

1. Регістр зсуву з лінійним зворотним зв'язком довжини n, який задається певним поліномом зворотного зв'язку $p(x) = x^n \oplus c_{n-1}x_{n-1} \oplus \ldots \oplus c_1x_1 \oplus c_0$. Нагадаємо, що іншим способом задання регістра зсуву є супровідна матриця C розміру $n \times n$, яка будується таким чином:
$$C = \begin{pmatrix} 0 & 1 & 0 & \ldots & 0 \\ 0 & 0 & 1 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & 0 & \ldots & 1 \\ c_0 & c_1 & c_2 & \ldots & c_{n-1} \end{pmatrix}$$
2. Фільтрувальна нелінійна функція $f \in B_n$, $\deg f = d > 1$.

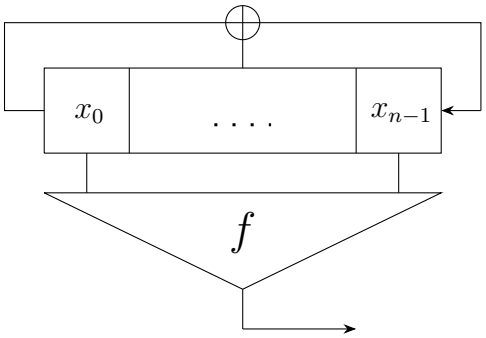

Рис. 1: Фільтрувальний генератор гами

Нехай $x = (x_0, \ldots, x_{n-1})$ є початковим станом регістру, тоді оновлення стану відбувається за формулою
$$C \cdot x^{\downarrow} = \begin{pmatrix} 0 & 1 & 0 & \ldots & 0 \\ 0 & 0 & 1 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & 0 & \ldots & 1 \\ c_0 & c_1 & c_2 & \ldots & c_{n-1} \end{pmatrix} \cdot \begin{pmatrix} x_0 \\ x_1 \\ \ldots \\ x_{n-2} \\ x_{n-1} \end{pmatrix} = \begin{pmatrix} x_1 \\ x_2 \\ \ldots \\ x_{n-1} \\ c_0x_0 \oplus \ldots \oplus c_{n-1}x_{n-1} \end{pmatrix}.$$

Відповідно, стан регістру в i-ому такті обчислюється за формулою $C^i \cdot x^{\downarrow}$, а біт гами в i-ому такті обчислюється таким чином:

$$\gamma_i = f\left(C^i \cdot x^{\downarrow}\right), \quad i = 1, 2, 3, \ldots.$$

Припустимо, що відомо N знаків гами. В такому разі можна скласти систему алгебраїчних рівнянь степеня d над полем $\mathbb{F}_2$ виду $f(C^i \cdot x^{\downarrow})$, $i = 1, \ldots, N$. З огляду на те, що задача розв'язання системи поліноміальних рівнянь над двійковим полем є $\mathcal{NP}$-повною та на практиці складність розв'язання цієї задачі збільшується з ростом степеня d, виникає необхідність у пошуку рівнянь-наслідків меншого степеня. Всі функції, що відповідають таким рівнянням-наслідкам, містяться в ідеалі, породженому функцією f. Окрім цього, потрібно ще розглядати ідеал $\langle f \oplus 1 \rangle$, оскільки він також може бути використаний для побудови рівнянь-наслідків меншого степеня.

Розглянемо дві ситуації, в яких можна побудувати рівняння-наслідки меншого степеня.

1. Припустимо, що знайшлась функція $h \in \langle f \rangle$, $\deg h < d$. Нехай також $\gamma_i = 0$, тоді з урахуванням співвідношення $\langle f \rangle = \mathrm{Ann}\,(f \oplus 1)$ маємо $h \cdot (f + 1) = 0$, відповідно, $h(C^i \cdot x^{\downarrow}) = 0$, оскільки $f(C^i \cdot x^{\downarrow}) = 0$.

2. Припустимо, що знайшлась функція $h \in \langle f \oplus 1 \rangle$, $\deg h < d$. Якщо $\gamma_i = 1$, то з урахуванням $\langle f \oplus 1 \rangle = \mathrm{Ann}\,(f)$ маємо $h \cdot f = 0$, відповідно, $h(C^i \cdot x^{\downarrow}) = 0$, оскільки $f(C^i \cdot x^{\downarrow}) = 1$.

Таким чином, побудова алгебраїчної атаки зводиться до аналізу ідеалів $\langle f \rangle$ та $\langle f \oplus 1 \rangle$, а саме пошуку функцій мінімального степеня, які містяться в кожному з цих ідеалів. Криптографічний параметр, який визначає стійкість функції f до алгебраїчних атак, називається *алгебраїчною імунністю* і визначається таким чином:

$$\mathrm{AI}\,(f) = \min\{\deg h \mid h \in \langle f \rangle \ \cup \langle f \oplus 1 \rangle\}.$$

Одним зі способів знаходження функцій мінімального степеня ідеалу є побудова *базису Грьобнера* цього ідеалу. Результат, який надає змогу застосовувати базиси Грьобнера до пошуку функцій найменшого степеня, називається теоремою Арса-Фожере.

Теорема. *Нехай $I \lhd B_n$, де $I \neq \{0\}$, $\preceq$ – степеневе мономіальне впорядкування на $\mathbb{N}_0^n$, G – мінімальний базис Грьобнера ідеалу I. Нехай також $g_1, \ldots, g_l$ – усі функції з G, які мають найменший степінь d, де $d \geq 1$. Тоді*

1. *всі функції мінімального степеня ідеалу I мають степінь d;*

2. *будь-яка функція $f \in I$ степеня d може бути єдиним чином представлена у вигляді*

$$f = c_1 g_1 \oplus \ldots \oplus c_l g_l,$$

де $c_i \in \{0, 1\}$ для $i \in \overline{1, l}$.

Зокрема, ідеал I містить рівно $2^l - 1$ функцій степеня d.

Отже, для пошуку функцій найменшого степеня ідеалу достатньо знайти базис Грьобнера ідеалу та вибрати серед функцій цього базису ті, які мають найменший степінь.

Вхідні дані

1. Довжина регістру 64 біти. Поліном зворотного зв'язку для всіх варіантів є однаковим:

$$p(x) = x^{64} \oplus x^{63} \oplus x^{62} \oplus x^{60} \oplus x^{59} \oplus x^{58} \oplus x^{57} \oplus x^{56} \oplus x^{53} \oplus x^{50} \oplus x^{47} \oplus x^{45} \oplus x^{44} \oplus x^{43} \oplus \\ \oplus x^{42} \oplus x^{41} \oplus x^{40} \oplus x^{39} \oplus x^{38} \oplus x^{37} \oplus x^{36} \oplus x^{34} \oplus x^{32} \oplus x^{30} \oplus x^{28} \oplus x^{24} \oplus x^{18} \oplus \\ \oplus x^{15} \oplus x^{14} \oplus x^{13} \oplus x^{11} \oplus x^{9} \oplus x^{6} \oplus x^{4} \oplus 1.$$

2. Фільтрувальні функції $f(x_0, \ldots, x_{63})$ генератора гами для всіх варіантів містяться в архіві під назвою `Variants_FilterFunction.rar`.

3. Відрізки гами $\gamma_1, \ldots, \gamma_N$ довжини 50000 бітів для всіх варіантів містяться в архіві під назвою `Variants_Gamma.rar`.

Порядок виконання роботи

1. Знайти функції мінімального степеня ідеалів $\langle f \rangle$ та $\langle f \oplus 1 \rangle$ за допомогою побудови базису Грьобнера. Якщо побудова базису для одного з ідеалів $\langle f \rangle$ або $\langle f \oplus 1 \rangle$ 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.

Оформлення протоколу

Протокол до комп'ютерного практикуму оформлюється згідно зі стандартними правилами оформлення наукових робіт. До протоколу можна не включати анотацію, перелік термінів та позначень та перелік використаних джерел. Також не обов'язково оформлювати зміст.

Протокол має містити:

– мету комп'ютерного практикуму;

– постановку задачі, варіант завдання та хід роботи;

– потужність побудованих базисів Грьобнера, всі знайдені функції мінімального степеня;

– кількість рівнянь в побудованій системі, перші 10 рівнянь, всі розв'язки системи;

– час виконання кожної операції (побудова базису Грьбонера та системи рівнянь);

– знайдений початковий стан генератора гами;

– програмний код для знаходження початкового стану генератора гами;

– висновки.

Оцінювання комп'ютерного практикуму

Оцінка за комп'ютерний практикум складається з двох складових: оцінки за презентацію отриманих студентом результатів, яка складає 9 балів, та оцінки за протокол, яка складає 6 балів.

Якщо знайдений в ході виконання комп'ютерного практикуму початковий стан є неправильним, то здача комп'ютерного практикуму не зараховується. В такому разі студенту надається можливість переробити комп'ютерний практикум.

Під час презентації отриманих результатів студент надає викладачу в усній формі звіт по виконаній роботі. В процесі цього викладач може ставити уточнювальні питання по програмному коду, а також теоретичні питання по матеріалах курсу, які стосуються цього комп'ютерного практикуму. Окрім цього, викладач може поставити питання до реалізації тих чи інших функцій у використаних студентом програмних реалізаціях (наприклад, який алгоритм знаходження базису Грьобнера використовується в обраній системі комп'ютерної алгебри, особливості його імплементації в цій системі). Якщо студент не орієнтується в програмному коді своєї роботи або не володіє відповідним теоретичним матеріалом, то відповідь не зараховується, і йому у майбутньому буде надано ще одну спробу для презентації. Дата та час повторної здачі врегульовується за домовленістю з викладачем в індивідуальному порядку.

Критерії оцінювання презентації отриманих результатів та протоколу містяться в положенні про рейтингову систему оцінювання.

Здача протоколу після назначеного терміну виконання без поважної причини приводить до зниження оцінки за нього на 1 бал за кожен тиждень запізнення (перший бал втрачається одразу після назначеного терміну виконання); при цьому оцінка не опускається нижче нуля. Тижнем в даному випадку вважається 7 календарних днів. Якщо в програмному коді та/або протоколі присутні ознаки плагіату, то студент отримує за нього нуль балів без можливості повторного виконання цього завдання.