ЭЛЕМЕНТЫ АЛГЕБРАИЧЕСКОГО КРИПТОАНАЛИЗА В УЧЕБНЫХ ДИСЦИПЛИНАХ ПО КРИПТОГРАФИЧЕСКИМ МЕТОДАМ ЗАЩИТЫ ИНФОРМАЦИИ

Благовисная А.Н., Михляева А.В.
Оренбургский государственный университет

В процессе преподавания дисциплин, посвященных криптографическим методам защиты информации, довольно часто вместе с изучением методов создания криптоалгоритмов рассматриваются и примеры раскрытия шифров. Как правило, это задачи, использующие методы раскрытия традиционных (исторических) шифров, основаные на идеях перебора, частотного анализа. Практика преподавания дисциплин, связанных с математическими методами защиты информации, показывает, что данные методы криптоанализа доступны для понимания и реализации студентами практически любого уровня подготовки. Следует отметить, что решение задач на раскрытие исторических шифров вызывает интерес у студентов не только к учебной дисциплине, но и к криптографии как науке. В связи с этим возникает вопрос: а возможно ли на доступном для студентов уровне знакомство с методами криптоанализа, позволяющими раскрывать современные криптографические конструкции? На наш взгляд, такое знакомство возможно на уровне изучения основных идей современных разделов криптоанализа на примерах решения учебных задач, подразумевающих раскрытие упрощенных моделей криптографических конструкций.

Рассмотрим данный подход на примере решения задач, демонстрирующих основные идеи алгебраического криптоанализа.

Алгебраический криптоанализ является сравнительно новым методом раскрытия шифров. В 2003 году появилась атака на фильтрующие генераторы [9], которая получила название алгебраической. Позднее было показано применение алгебраической атаки на комбинирующие генераторы и блочные шифры. В настоящее время методы алгебраического криптоанализа активно применяются для исследования поточных [7, 8], блочных [2, 3] алгоритмов шифрования. Развиваются и методы решения систем булевых уравнений [1], составляющих основу алгоритмов алгебраического криптоанализа.

В некоторых учебных изданий [5, 6], предназначенных для студентов вузов, встречаются разделы, посвященные криптографическим свойствам, которыми должны обладать булевы функции для обеспечении стойкости шифров к алгебраическим криптоатакам. В этих же книгах можно найти и формулировки заданий на раскрытие шифров методами алгебраического криптоанализа.

Основная идея алгебраического криптоанализа заключается в составлении системы булевых уравнений, которые описывают преобразование шифра. Такая система строится на основе полностью известного алгоритма шифрования. Особенностью системы булевых уравнений, которая возникает при

криптоанализе, является её непротиворечивость, то есть система имеет как минимум одно решение. Рассмотрим, как получаются такие системы булевых уравнения с позиции формулировок и решения учебных задач.

Покажем алгебраическую атаку на генератор с регистром длины 4, уравнение рекурсии которого $u(i+4)=u(i+1)\oplus u(i)$, фильтрующая функция $f(x_1,x_2,x_3,x_4)=x_1x_2x_3\oplus x_1x_2\oplus x_1x_4\oplus x_3x_4\oplus x_3,$ если известен начальный отрезок гаммы $\gamma=(1,0,0,1)$.

Нам необходимо найти начальное состояние генератора. Пусть u_0, u_1, u_2, u_3 – элементы искомой последовательности, задающей начальное состояние генератора. Составим систему уравнений на основе фильтрующей функции:

$$\begin{cases} f(u_0,u_1,u_2,u_3)=u_0u_1u_2\oplus u_0u_1\oplus u_0u_3\oplus u_2u_3\oplus u_2=1,\\ f(u_1,u_2,u_3,u_4)=u_1u_2u_3\oplus u_1u_2\oplus u_1u_4\oplus u_3u_4\oplus u_3=0,\\ f(u_2,u_3,u_4,u_5)=u_2u_3u_4\oplus u_2u_3\oplus u_2u_5\oplus u_4u_5\oplus u_4=0,\\ f(u_3,u_4,u_5,u_6)=u_3u_4u_5\oplus u_3u_4\oplus u_3u_5\oplus u_5u_6\oplus u_5=1. \end{cases} \quad (1)$$

Используя уравнение рекурсии, выразим u_4, u_5, u_6:

$$u_4=u_0+u_1,\ u_5=u_1+u_2,\ u_6=u_2+u_3. \quad (2)$$

Найденные выражения (2) подставим в систему (1). После преобразований уравнений системы, заключающихся в раскрытии скобок и приведении подобных, получим следующую систему:

$$\begin{cases} u_0u_1u_2\oplus u_0u_1\oplus u_0u_3\oplus u_2u_3\oplus u_2=1,\\ u_1u_2u_3\oplus u_0u_1\oplus u_0u_3\oplus u_1u_2\oplus u_1u_3\oplus u_1\oplus u_3=0,\\ u_0u_2u_3\oplus u_1u_2u_3\oplus u_0u_1\oplus u_0u_2\oplus u_2u_3\oplus u_0\oplus u_2=0,\\ u_0u_1u_3\oplus u_0u_2u_3\oplus u_1u_2u_3\oplus u_0u_3\oplus u_1u_2\oplus u_1=1. \end{cases} \quad (3)$$

Количество уравнений и переменых в получившейся системе (3) не так велико, поэтому решение системы можно найти, перебирая все возможные наборы значений переменных. Перебор различных вариантов решений удобно офомить в таблице (таблица 1).

В результате подбора решений системы (3) удалось установить, что непротиворечивыми все уравнения системы являются лишь в одном случае, когда $u_0=1, u_1=1, u_2=0, u_3=0$. Это решение является единственным решением системы (3), то есть искомое начальное состояние генератора представляется в виде (1,1,0,0).

Таблица 1 – Подбор решений системы (3)

u_0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1
u_1	0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1
u_2	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1
u_3	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1
u_0u_1	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1
u_0u_2	0	0	0	0	0	0	0	0	0	0	1	1	0	0	1	1
u_0u_3	0	0	0	0	0	0	0	0	0	1	0	1	0	1	0	1
u_1u_2	0	0	0	0	0	0	1	1	0	0	0	0	0	0	1	1
u_1u_3	0	0	0	0	0	1	0	1	0	0	0	0	0	1	0	1
u_2u_3	0	0	0	1	0	0	0	1	0	0	0	1	0	0	0	1
$u_0u_1u_2$	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1
$u_0u_1u_3$	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1
$u_0u_2u_3$	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	1
$u_1u_2u_3$	0	0	0	0	0	0	0	1	0	0	0	0	0	0	1	1
1 ур-ие	0≠1	0≠1		0≠1	0≠1	0≠1		0≠1	0≠1					0≠1		
2 ур-ие		1≠0		1≠0	1≠0	1≠0		1≠0						1≠0		1≠0
3 ур-ие			1≠0				1≠0	1≠0	1≠0	1≠0	1≠0	1≠0			1≠0	1≠0
4 ур-ие	0≠1		0≠1				0≠1		0≠1	0≠1	0≠1					0≠1
Вывод	–	–	–	–	–	–	–	–	–	–	–	–	+	–	–	–

Перебор всех возможных вариантов решений получающейся при алгебраической криптоатаке системы булевых уравнений не является рациональным методом поиска решений систем. На практике используются другие подходы к поиску неизвестных, удовлетворяющих уравнениям системы. Один из таких подходов основан на понятии аннигиляторов булевой функции.

Определение. Булева функция g, не равная тождественно нулю, минимальной степени, такая, что $fg = 0$ или $(f+1)g = 0$, называется аннигилятором булевой функции f.

В качестве примера рассмотрим алгебраическую атаку на генератор с регистром длины 3, с уравнением рекурсии $u(i+3) = u(i+1) \oplus u(i)$ и фильтрующей

функцией $f(x_1, x_2, x_3) = x_1x_2x_3 \oplus x_2x_3 \oplus x_2 \oplus x_3$. Пусть известен отрезок гаммы $\gamma = (1,1,0)$.

Система уравнений для поиска начального состояния генератора имеет вид:

$$\begin{cases} f(u_0, u_1, u_2) = u_0u_1u_2 \oplus u_1u_2 \oplus u_1 \oplus u_2 = 1, \\ f(u_1, u_2, u_3) = u_1u_2u_3 \oplus u_2u_3 \oplus u_2 \oplus u_3 = 1, \\ f(u_2, u_3, u_4) = u_2u_3u_4 \oplus u_3u_4 \oplus u_3 \oplus u_4 = 0. \end{cases} \quad (4)$$

С учетом того, что $u_3 = u_0 + u_1$, $u_4 = u_1 + u_2$, система (4) примет следующий вид:

$$\begin{cases} u_0u_1u_2 \oplus u_1u_2 \oplus u_1 \oplus u_2 = 1, \\ u_1u_2(u_0 \oplus u_1) \oplus u_2(u_0 \oplus u_1) \oplus u_2 \oplus (u_0 \oplus u_1) = 1, \\ u_2(u_0 \oplus u_1)(u_1 \oplus u_2) \oplus (u_0 \oplus u_1)(u_1 \oplus u_2) \oplus (u_0 \oplus u_1) \oplus (u_1 \oplus u_2) = 0. \end{cases} \quad (5)$$

Далее упростим систему (5). Для этого потребуется найти аннигиляторы для функций f и $f \oplus 1$ (для нашего примера $f(x_1, x_2, x_3) = x_1x_2x_3 \oplus x_2x_3 \oplus x_2 \oplus x_3$). Для поиска аннигиляторов булевых функций нами в среде Visual Studio на языке объектно-ориентированного программирования C++ написано программное средство. В программе реализованы возможности выбора количества переменных булевой функции, ввода булевой функции, предусмотрена обработка исключительных ситуаций. Программа нахождения аннигиляторов булевой функции реализована в соответствии с алгоритмом, рассмотренным в работе [4] и предназначена для работы с учебными задачами.

Аннигиляторами для функций f и $f \oplus 1$ являются функции $g_1 = x_2x_3 \oplus x_2 \oplus x_3 \oplus 1$ и $g_2 = x_2 \oplus x_3$соответственно. Далее, в соответствии со схемой алгебраической атаки, первые два уравнения системы следует заменить на уравнения $g_1(u_0, u_1, u_2) = 0$ и $g_1(u_1, u_2, u_3) = 0$, а третье – на $g_2(u_2, u_3, u_4) = 0$. В результате получаем систему

$$\begin{cases} u_1u_2 \oplus u_1 \oplus u_2 \oplus 1 = 0, \\ u_2(u_0 \oplus u_1) \oplus u_2 \oplus (u_0 \oplus u_1) \oplus 1 = 0, \\ u_0 \oplus u_2 = 0. \end{cases} \quad (6)$$

Будем искать решения системы, рассуждая следующим образом. Из последнего уравнения системы видно, что либо $u_0 = u_2 = 0$, либо $u_0 = u_2 = 1$. По-

этому нам не нужно рассматривать все возможные варианты решений, как это было сделано в предыдущем примере, а достаточно рассмотреть лишь варианты, при которых последнее уравнение имеет смысл. При $u_0 = 1, u_1 = 0, u_2 = 1$ противоречивых уравнений в системе (5) не будет, и мы получим единственное решение системы, которое дает начальное состояние генератора (1,0,1).

Таким образом, рассмотренные примеры раскрытия упрощенных криптографических конструкций можно использовать в качестве учебных задач, демонстрирующих идеи алгебраического криптоанализа.

Список использованных источников

1. Агибалов, Г.П. Методы решения систем полиномиальных уравнений над конечным полем / Г.П. Агибалов // Вестник Томского государственного университета. – 2006. – № 17. – С. 4-9.

2. Бабенко, Л.К. Анализ стойкости блочных алгоритмов шифрования к алгебраическим атакам / Л.К. Бабенко, Е.А. Маро // Известия ЮФУ. Технические науки. – 2011. – №12. – С.110-119.

3. Маро, Е. А. Алгебраический криптоанализ упрощённого алгоритма шифрования Rijndael / Е.А. Маро // Известия ЮФУ. Технические науки. – 2009. – № 11 (110). – С.187-199.

4. Отрыванкина, Т. М. Криптографические свойства булевых функций: методические указания / Т. М. Отрыванкина, А. Н. Благовисная; Оренбургский гос. ун-т. – Оренбург: ОГУ, 2014. – 55 с.

5. Панкратова, И.А. Булевы функции в криптографии: учебное пособие / И. А. Панкратова. – Томск: Издательский Дом Томского государственного университета, 2014. – 88 с.

6. Токарева, Н. Н. Симметричная криптография. Краткий курс: учебное пособие / Н. Н. Токарева. – Н: Новосибирский государственный университет, 2012. – 232 с.

7. Хузина, Э.И. Модель связи в криптографии и алгебраические атаки на поточные шифры / Э.И. Хузина // Молодёжный научно-технический вестник. – 2013. – № 12. – С. 1-4.

8. Чиликов, А. А. Анализ поточных шифров с помощью решения системы алгебраических уравнений / А. А. Чиликов, Э. И. Хузина // Научное издание МГТУ им. Н. Э. Баумана. Наукаиобразование. – 2013. – № 3. – С. 257-268.

9. Courtois, N. Algebraic attack on stream ciphers with linear feedback / N. Courtois, W. Meier // LNCS. – 2003. – V. 2656. – P. 345–359.