Разработка и исследование алгоритмов алгебраического криптоанализа

Маро Е.А.
Руководитель: д.т.н., профессор Бабенко Л.К.

Факультет Информационной Безопасности
Таганрогский Технологический Институт
Южного Федерального Университета

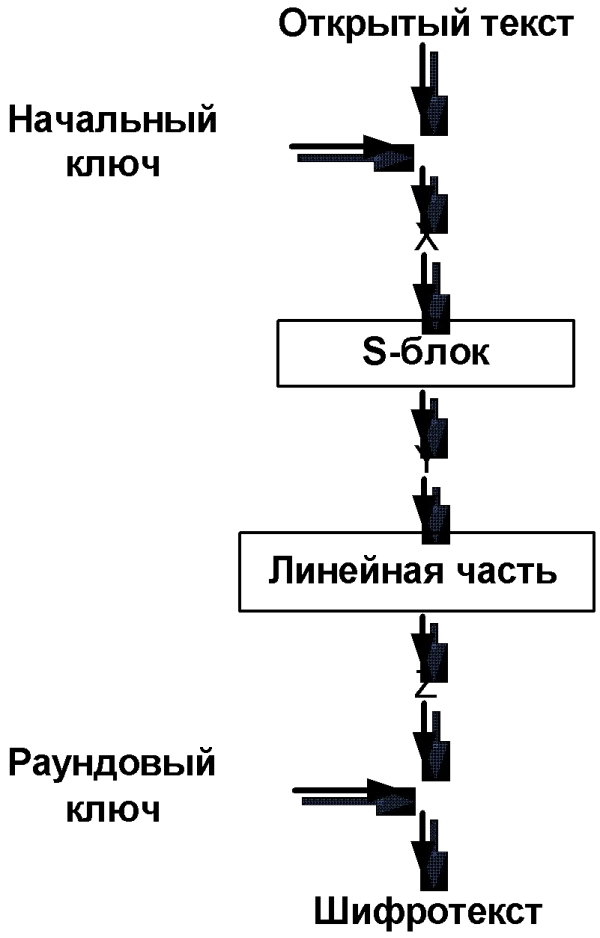
Задача алгебраического криптоанализа

- Алгебраические атаки используют внутреннюю структуру шифра, то есть для получения ключа шифрования необходимо представить преобразования шифрования в виде системы многомерных многочленных уравнений и впоследствии решить данную систему.
- Несмотря на то, что данный метод может быть применим к некоторому числу алгоритмов шифрования, в данной работе анализ алгебраический методов сфокусирован на применении их к алгоритму шифрования Rijndael, а точнее его упрощенному варианту - BabyRijndael.

Значимость задачи

- Большинство современных шифров было создано с учетом традиционных методов криптоанализа, таких как дифференциальный и линейный , поэтому такого рода атаки зачастую не оказывают влияния на их безопасность. Для большинства подобных атак сложность возрастает экспоненциально с ростом числа раундов, при этом данные методы становятся неэффективными.
- В отличие от них, алгебраический криптоанализ затрагивает внутреннюю структуру шифров и оказывается более эффективным. Следует отметить возможность улучшения производительности алгебраических алгоритмов криптоанализа путем распараллеливания вычислительных процессов.

Алгоритм одного раунда упрощенного варианта шифра Rijndael



- Размер блоков и ключей составляет 16 бит.
- Число раундов равно 4.
- Замена в S-блоках имеет вид:

x	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
$s(x)$	a	4	3	b	8	e	2	c	5	7	6	f	0	1	9	d

получаем следующим образом:

$$\omega_0 = \begin{pmatrix} k_0 \\ k_1 \end{pmatrix} \qquad \omega_1 = \begin{pmatrix} k_2 \\ k_3 \end{pmatrix}$$

где

$$\omega_{2i} = \omega_{2i-2} \oplus S(\mathrm{reverse}(\omega_{2i-1})) \oplus y_i$$

$$\omega_{2i+1} = \omega_{2i-1} \oplus \omega_{2i} \qquad y_i = \begin{pmatrix} 2^{i-1} \\ 0 \end{pmatrix}$$

Алгоритм шифрования для упрощенной модели Rijndael

Система уравнений S-блоков

- Уравнения, описывающие работу S-блоков, имеют вид:

$$\sum \alpha_{ij} x_i x_j + \sum \beta_{ij} y_i y_j + \sum \gamma_{ij} x_i y_j + \sum \delta_i x_i + \sum_{2*n} \varepsilon_i y_i + \eta = 0$$

- Максимальное число одночленов равно t=( )+2n+1
- Для составления уравнений необходимо получить таблицу истинности вида:

η	x_1	...	x_n	y_1	...	y_n	x_1x_2	...	$x_{n-1}x_n$	y_1y_2	...	$y_{n-1}y_n$	x_1y_1	...	x_ny_n
1	0	...	0												
...															
1	1	...	1												

Получение системы уравнений

Можно выделить три этапа:

1. Получение уравнений для S-блоков
2. Получение дополнительных уравнений, учитывающих алгоритм работы S-блоков
3. Уменьшение числа переменных

Разработка алгоритма получения уравнений для S-блоков

- Рассматриваем 2^t вариантов уравнений и отбираем уравнения, удовлетворяющие таблице истинности.
- Из полученных уравнений выбираем уравнения, содержащие только один квадратный элемент (то есть элемент вида $x_i y_j$, $x_i x_j$ или $y_i y_j$)
- Определяем, какие из квадратных элементов не встречаются в данных уравнениях
- Находим уравнение, в котором присутствует недостающий квадратный элемент
- Производим сложение по модулю 2 данного уравнения с другим уравнением, таким чтобы при сложении произошло обнуление уже встречавшихся квадратных элементов.
- Отбрасываем уравнения содержащие два и более квадратных элемента.

Получение дополнительных уравнений, учитывающих алгоритм работы S-блоков

Учитывая, что в S-блоках сначала находится обратный входному значению элемент и лишь потом применяется аффинное преобразование, обозначим его через h, можем получить дополнительные уравнения из выражения: $h(Y) = X^{-1}$ или X*h(Y)=(0,0,0,1).

Таким образом, путем приравнивания каждого бита с левой стороны к биту с правой стороны, получим 4 дополнительных уравнения.

Алгоритм уменьшения числа переменных

Исходя из схемы алгоритма шифрования BabyRijndael и алгоритма выработки ключей, возможно произвести следующие замены:

1. Входное значение S-блока равно открытый текст XOR начальный ключ.
2. Выходное значение S-блока равно шифротекст XOR раундовый ключ.
3. Второй столбец раундового ключа представляет собой сумму по модулю 2 второго столбца начального ключа и первого столбца раундового ключа.

XL атака

XL (eXtended Linearization) метод предложили Николя Куртуа, Александр Климов и Ади Шамир в 2000 году.

Обозначим через D параметр алгоритма XL, причем , где n- число переменных, а m- количество уравнений. $D \approx \frac{n}{\sqrt{m}}$

Данный алгоритм базируется на перемножении каждого возможного уравнения 1…m на все возможные значения переменных в степени D-2.

Алгоритм реализации XL метода

- **Multiply:** составление всех произведений вида $(\Pi_{ij}^{k} x_{ij}) \boxtimes_i \in I_D$, где k≤D-2;
- **Linearize:** рассмотрение каждого одночлена x_i в степени ≤ D как новой переменной и применение Гауссовского исключения к уравнениям, полученным в пункте 1.
- **Solve:** повторение пункта 2 до тех пор, пока в результате не будет получено по крайней мере одно уравнение с единственной переменной.
- **Repeat:** упростить уравнения и повторить процесс для нахождения значений других переменных.

XSL атака

В 2002 году вместо техники XL был создан алгоритм, использующий преимущества особой структуры уравнений и их разреженность. Эта атака была названа XSL-атака, что расшифровывается как «eXtended Sparse Linearization» или «multiply(X) by Selected monomials and Linearize».

Алгоритм XSL предложен для работы только со специальными типами шифров, для который выполняются условия:

- S-блоки должны быть такими, чтобы их можно было описать с помощью сверхопределенной системы квадратных уравнений.
- Алгоритм получения ключей должен иметь схожую структуру с алгоритмом зашифрования.

Алгоритм реализации XSL метода

- Обработка имеющейся системы уравнений путем выбора конкретного набора одночленов и уравнений, которые будут использоваться в дальнейших этапах алгоритма
- Выбор значения параметра P и умножение выбранных на предыдущем этапе уравнений на результаты произведений (P-1) выбранных одночленов
- При недостаточном числе уравнений применение T’ метода, в котором некоторые выбранные уравнения умножаются на одиночные переменные. Цель данного метода – создание новых уравнений без получения каких-либо новых одночленов.
- Применение линеаризации, путем представления каждого одночлена в виде новой переменной и выполнения Гауссовского исключения.

Оценка сложности атаки для алгоритма шифрования BabyRijndael

Для метода XL сложность Гауссовского преобразования T^{ω} составляет:

$T^{\omega} \approx (\binom{n}{D})^{\omega} \approx (\binom{n}{n/\sqrt{m}})^{\omega} = 2^{63}$, где n - число переменных, m - количество уравнений, ω≤3 - показатель Гауссовского преобразования.

Для XSL атаки сложность составляет

$T^{\omega} = t^{P\omega} * (\binom{S}{P})^{\omega} = 2^{55}$, где t – число одночленов, P – параметр алгоритма XSL атаки, S - число S-блоков, ω - показатель Гауссовского преобразования.

Заключение

В данной работе были рассмотрены основные алгебраические методы криптоанализа, а именно XL (eXtended Linearization) и XSL (eXtended Sparse Linearization) атаки, рассчитана сложность их реализации для алгоритма шифрования BabyRijndael. Также был разработан алгоритм получения системы уравнений, описывающей процесс шифрования.

В заключении можно отметить, что для алгоритма шифрования BabyRijndael система будет содержать 792 уравнения с 96 переменными. Число различных одночленов, встречающихся в данных уравнениях, составляет 2332. На практике последующее применение к данной системе алгебраических методов криптоанализа приводит к получению ключа шифрования.