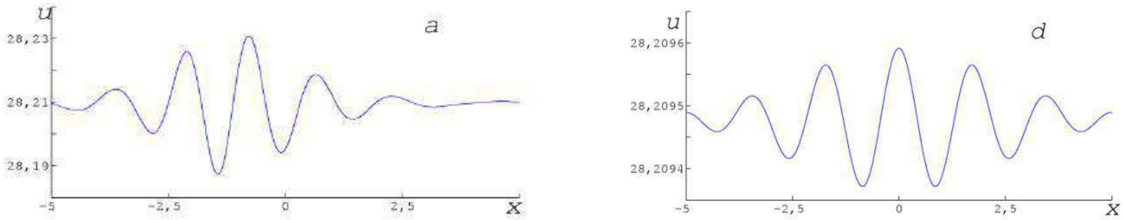

Рис. 1: График функции $u(x,t)$ в моменты времени $t = 50$ при $\alpha = 1.5$ (a), 2 (d).

На рис. 1 изображена эволюция плотности $u(x,t)$ при $a = 1$, $b_0 = 1$, $\gamma = 1$, $\chi = 0.2$, $D = 0.01$, $l = 5$, $T = 10$

Как видно из графиков, порядок производной влияет на смещение центра возмущений пространственно-временных структур. Чем ниже порядок дробной производной, тем больше смещение график и сильнее отклонение от стационарного состояния.

Список литературы

1. *Колмогоров А. Н., Петровский Н. Г., Пискунов Н. С.* // Бюл. МГУ. Сер. А. Математика и Механика. Т. 1, № 6. С. 1 (1937).
2. *Самко С. Г., Килбас А. А., Маричев О. И.* Интегралы и производные дробного порядка и некоторые их приложения. – Минск: Наука и техника, 1987. С. 38.
3. *Fisher R. A.* // Annual Eugenics. V. 7. P. 255 (1937)

ОЦЕНКА ВЫЧИСЛИТЕЛЬНОЙ СЛОЖНОСТИ КРИПТОГРАФИЧЕСКОГО АНАЛИЗА МЕГРЕЛИШВИЛИ И ДЖИНДЖИХАДЗЕ

Вьонг Х.Б.
vuonghuubao@live.com

Научный руководитель: к.ф.-м.н., доцент, Зюбин С.А., Кафедра высшей математики

В работе приводится оценка вычислительной сложности криптографического анализа протокола разделения ключа Мегрелишвили и Джинджихадзе.

Введение

Для оценки вычислительной сложности криптографического анализа системы Мегрелишвили и Джинджихадзе, рассмотрим следующий протокол разделения ключа.

Протокол разделения ключа Мегрелишвили и Джинджихадзе

Установка

Корреспонденты А и Б договариваются о выборе векторного пространства $V = F_2^n$ размерности n над полем F_2. Далее фиксируется квадратная матрица A размера $n \times n$ и вектор $v \in V$. Эти данные открыты.

Генерация ключей.

Корреспондент А выбирает случайным образом натуральное число k, вычисляет и пересылает корреспонденту Б вектор $u = vA^k$. В свою очередь корреспондент Б выбирает число l, вычисляет и пересылает А вектор $w = vA^l$.

Разделение ключа.

Затем каждый из корреспондентов вычисляет разделяемый ключ

$$K = uA^l = wA^k = vA^{k+l} \tag{1}$$

Далее приводим идею В.А. Романьков анализа системы Мегрелишвили и Джинджихадзе.

Криптографический анализ системы Мегрелишвили и Джинджихадзе.

Выпишем векторы $v = vA^0, vA, \ldots, vA^m$ до максимально возможной степени m с условием линейной независимости этого набора. Ясно, что $m \le n$, поэтому процесс эффективен. Данный набор является базисом линейного пространства $lin_{F_2}(vA^k, k \in \mathbb{N})$, порожденного всеми векторами вида $vA^k, k \in \mathbb{N}$. Для этого достаточно доказать, что любой вектор $vA^k, k \ge m+1$, линейно выражается через данный набор. Поскольку набор $v, vA, \ldots, vA^m$ является первым линейно зависимым набором, вектор vA^{m+1} допускает разложения вида

$$vA^{m+1} = \sum_{i=0}^{m} \alpha_i vA^i, \alpha_i \in F_2. \tag{2}$$

Пусть уже доказано, что вектор $vA^k, K \ge m+1$, представим в виде

$$vA^k = \sum_{i=0}^{m} \beta_i vA^i, \beta_i \in F_2. \tag{3}$$

Умножим обе части (3) справа на матрицу А и проведем преобразование с использованием равенства (3):

$$vA^{k+1} = \sum_{i=0}^{m} \beta_i vA^{i+1} = \sum_{i=0}^{m-1} \beta_i vA^{i+1} + \beta_m \cdot \sum_{i=0}^{m} \beta_i vA^i = \beta_m \cdot \beta_0 v + \sum_{i=0}^{m} (\beta_{i-1} + \beta_m \cdot \beta_i) vA^i. \tag{4}$$

Утверждение о базисе $v, vA, \ldots, vA^k$ пространства $lin_{F_2}(vA^k, k \in \mathbb{N})$ следует по индукции.

Теперь можно получить разложение

$$u = vA^k = \alpha_0 v + \alpha_1 vA + \ldots + \alpha_m vA^m, \alpha_i \in F_2 \tag{5}$$

Заметим, что для получения разложения (5) не нужно знать k, а только u.

После этого подставим в правую часть полученного выражения (5), где все компоненты известны, вектор w вместо v и получим

$$\alpha_0 w + \alpha_1 wA + \ldots + \alpha_m wA^m = (\alpha_0 v + \alpha_1 vA + \ldots + \alpha_m vA^m) A^l = vA^{l+k} = K. \tag{6}$$

Оценка вычислительной сложности

Оценим вычислительную сложность нахождения ключа при атаке Романькова на систему Мегрелишвили и Джинджихадзе [1]. Нахождение ключа состоит из нескольких вычислительных этапов: вычисление векторов vA^i, проверка на линейную зависимость системы vA^i, нахождение разложения $u = \alpha_0 v + \ldots + \alpha_n vA^n$ и нахождение ключа $k = vA^{k+l}$.

Оценим сложность этапов:

Вычисление вектора vA, где:

$$v = \begin{pmatrix} v_1 & v_2 & \cdots & v_n \end{pmatrix}$$

$$A = \begin{pmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \ldots & a_{nn} \end{pmatrix}$$

Пусть наибольшее среди чисел v_i, a_{ij} имеет k разрядов двоичных цифр.

Умножения $[v_i]_{1\times n}\times[a_{i1}]_{n\times 1}$ содержит n операций умножения k разрядных двоичных чисел и $n-1$ операций сложения:

Time (умножение $[v_i]_{1\times n}\times[a_{i1}]_{n\times 1}$) < $k^2n+k(n-1)$ для $i=\overline{1,n}$. Следовательно,

$$\text{Time}\,(vA)<[k^2n+k(n-1)]n\ .$$

Вычисление векторов $vA^2=(vA)\cdot A; vA^3=(vA^2)\cdot A$; ...; $vA^n=(vA^{n-1})\cdot A$ аналогично вычислению vA. Поэтому

$$\text{Time}\,(vA^j)<[k^2n+k(n-1)]n\ .$$

Т.е для вычисления набора $vA; vA^2; vA^3; ...; vA^n$:

Time (Вычисление набора, $vA, vA^2, ..., vA^n$)< $[k^2n+k(n-1)]n\cdot n=[k^2n+k(n-1)]n^2$

Проверка на линейную независимость для набора векторов

$$v=\begin{pmatrix} v_1 & v_2 & \cdots & v_n \end{pmatrix},$$
$$vA=\begin{pmatrix} b_{11} & b_{12} & \cdots & b_{1n} \end{pmatrix},$$
$$....$$
$$vA^m=\begin{pmatrix} b_{m1} & b_{m2} & \cdots & b_{mn} \end{pmatrix}.$$

Используя метод Гаусса найдем ранг матрицы

$$B=\begin{pmatrix} v_1 & v_2 & \dots & v_n \\ b_{11} & b_{12} & \dots & b_{1n} \\ b_{21} & b_{22} & \dots & b_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ b_{m1} & b_{m2} & \dots & b_{mn} \\ u_1 & u_2 & \dots & u_n \end{pmatrix}.$$

Число разрядов двоичных чисел $max[b_{ij}]\le 2k+1$

Для вычисления ранга необходимо будет выполнить умножения $v_1\cdot b_{11}; v_1\cdot b_{21}; \cdots; v_i\, b_{mi}$

Умножение $v_1\cdot b_{11}\cdot b_{21}\cdots b_{n1}$:

$$\text{Time}\,(v_1b_{11}...b_{n1})\le(2k+1)^2\cdot m.$$

Это операция повторяется $(m+1)\cdot n$ раз для $m+1$ строк и n столбцов.

Далее вычитания 2-я; 3-я; ... строка минус первая строка и сравнения с нулем, операция повторяется m раз для m строк:

$$\text{Time}<[(2k+1)n+(2k+1)n]\cdot m$$

Для проверки линейной независимости строк измененной матрицы при $m=\overline{1,n}$

$$\text{Time}<\sum_{m=2}^{n}\ \sum_{i=1\ j=n-m+1}^{i=m\ j=n}(2k+1)^2(i-1)ij+2(2k+1)\,j(i-1)$$

Таким образом для вычисления набора вектор $v; vA; ...; vA^n$ и проверка его линейная независимость:

$$\text{Time}<[k^2n+k(n-1)]n^2+\sum_{m=2}^{n}\ \sum_{i=1\ j=n-m+1}^{i=m\ j=n}k^2(i-1)ij+2kj(i-1)<5k^2n^5;$$

Далее необходимо найти разложение:

$$u=vA^k=\alpha_0v+\alpha_1vA^1+...+\alpha_nvA^n,\alpha_i\in F_2$$

Для этого надо решить систему $XB = U$ или $XC = U$, где С-матрица полеченная из В после применение метод Гаусса для нахождения ранга. Матрица С является треугольной поэтому нужно решить систему:

$X \times B = U$, где:

$$B = \begin{pmatrix} v_1 & v_2 & \dots & v_n \\ b_{11} & b_{12} & \dots & b_{1n} \\ b_{21} & b_{22} & \dots & b_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ b_{m1} & b_{m2} & \dots & b_{mn} \end{pmatrix}$$

$$X = \begin{pmatrix} \alpha_0 & \alpha_1 & \cdots & \alpha_n \end{pmatrix}$$

$$U = \begin{pmatrix} u_0 & u_1 & \cdots & u_n \end{pmatrix}$$

Для того чтобы найти $\alpha_i, i = \overline{1, n}$, необходимо выполнить умножения $n - i$ раз, и вычитания $n - i$ раз.

$$k^2(n-i) + k(n-1)$$

Нахождения $\alpha_0; \alpha_1; ...; \alpha_n$.

$$\text{Time} < \sum_{i=0}^{n} k^2(n-i) + k(n-i) = \frac{k^2 n(n+1)}{2} + \frac{kn(n+1)}{2} < k^2(n+1)^2$$

После этого найдем вектор vA^{k+l} следующим образом:

1. Умножения $\alpha_0 v; \alpha_1 vA; ...; \alpha_n vA^n$

$$Time < n^2 k^2$$

2. Нахождение сумму $\alpha_0 v + \alpha_1 vA + ... + \alpha_n A^n$

$$Time < kn(n-1)$$

3. Умножение $(\alpha_0 v + \alpha_1 vA + ... + \alpha_n A^n) \cdot A^l = K$

$$Time < [k^2 n + k(n-1)]n$$

Следовательно, общее время атаки Романькова:

$$\sum Time < 5k^2 n^5 + k^2(n+1)^2 + n^2 k^2 + kn(n-1) + [k^2 n + k(n-1)]n = O(n^5 k^2).$$

Заключение

Итак, в работе оценена вычислительная сложность криптографического анализа протокола разделения ключа Мегрелишвили и Джинджихадзе. Результат показывает, что по идее В.А. Романькова алгоритм нахождения ключа протокола Мегрелишвили и Джинджихадзе занимает время порядка $O(k^2 n^5)$ и задача анализа системы Мегрелишвили и Джинджихадзе решена эффективно.

Литература

1. Романьков В.А. Криптографический анализ некоторых схем шифрования, использующих автоморфизмы. // Прикладная дискретная математика, № 3 (21), с. 35-51, (2013).