

МЕТОД ЭКСПЕРТНОГО КРИПТОАНАЛИЗА СИСТЕМЫ РАО-НАМА

к.т.н. А.Д. Буханцов, к.т.н. С.В. Малахов, к.т.н. Е.В. Брежнев
(представил д.т.н., проф. И. Горбенко)

На основе предложенного метода криптоанализа выводится показатель трудозатрат, позволяющий предъявить требования к криптосистеме для обеспечения ее стойкости.

Несмотря на прогресс в теории вычислительной сложности, основным принципом испытания систем безопасности данных по-прежнему остается метод, основанный на проведении экспертного криптоанализа [1]. Стойкость большинства систем защиты информации опирается на практическую сложность раскрытия, которая обычно выражается в необходимых для этих целей временных трудозатратах. При вычислении нижней границы таких трудозатрат возникает сложная задача: найти самый короткий путь криптоанализа системы защиты информации.

Криптосистема Рао-Нама основана на использовании кодов Гоппы и является модифицированным вариантом системы Мак-Элиса в качестве одноключевой криптосистемы [2]. В системе Рао-Нама секретным ключом является порождающая матрица \mathbf{G} кода Гоппы. При зашифровании сообщения \mathbf{a} случайным образом выбирается вектор ошибок \mathbf{z} и вычисляется шифртекст $\mathbf{v} = \mathbf{aG} + \mathbf{z}$. Какие-либо способы раскрытия такой криптосистемы пока не известны. Однако, она обладает тем же недостатком, что и система Мак-Элиса – большой длиной ключа, равной \mathbf{kn} символов порождающей матрицы кода (в двоичном случае \mathbf{kn} бит).

Указанный недостаток можно устранить, если в качестве ключа вместо порождающей матрицы \mathbf{G} выбирать многочлен Гоппы $\mathbf{G}(\mathbf{x})$, определяющий ее построение. При этом коэффициенты $\mathbf{G}(\mathbf{x})$ в поле Галуа $\mathbf{GF}(2^m)$ и минимальное расстояние \mathbf{d} кода Гоппы определяют длину ключа, не превышающую величины $\mathbf{m}(\mathbf{d}-1)$ бит.

Исследование рассматриваемой системы позволило определить следующие пути криптоанализа:

- анализ на основе определения кодов Гоппы в частотной области;
- анализ на основе определения кодов Гоппы во временной области;
- прямой перебор многочленов Гоппы.

Каждый из них опирается на тот факт, что зашифрованное сообщение \mathbf{v} является искаженным ошибками кодовым словом кода Гоппы. Для декодирования такого сообщения необходимо знание многочлена Гоппы $\mathbf{G}(\mathbf{x})$.

Криптоанализ, основанный на прямом переборе, является тривиальным и в статье не рассматривается. Следует лишь отметить, что необходимые при этом трудозатраты определяются количеством всевозможных многочленов заданной степени и операций, необходимых для декодирования при каждой попытке взлома системы.

Остальные пути анализа основаны на знании искаженных ошибками кодовых векторов. При попытке криптоаналитиком исправить ошибки в данных векторах он определяет искомым многочлен Гоппы, как общий делитель некоторых, поставленных в соответствие кодовым векторам, многочленов.

Рассмотрим криптоанализ на основе определения кодов Гоппы в частотной области. Согласно [3], одним из условий, определяющих код Гоппы в узком смысле, является следующее:

$$C(x) = T(x)G(x) \pmod{x^n - 1}, \quad (1)$$

где $C(x)$ – полиномиальное представление спектра кодового вектора c длины n кода Гоппы, задаваемого многочленом Гоппы $G(x)$ степени $2t$ (t – кратность исправляемых кодом ошибок); $T(x)$ – многочлен, степень которого не превышает величины $(n - 2t)$.

Без модуля выражение (1) можно переписать в виде

$$T(x)G(x) = C(x) - \beta(x^n - 1), \quad (2)$$

где β – элемент поля $GF(q)$, причем $q = n + 1$.

Согласно выражению (2), искомым многочлен Гоппы $G(x)$ содержится в разложении одного из $n + 1$ возможных многочленов вида $[C(x) - \beta(x^n - 1)]$.

Если криптоаналитику известен вес z вектора ошибок, то для успешного исправления вектора v необходимо сделать $\binom{n}{z}$ попыток декодирования.

Однако, для того, чтобы определить факт успешной попытки, необходимо выбрать хотя бы два сообщения v_1 и v_2 . В этом случае правильно восстановленным кодовым векторам c_1 и c_2 можно поставить в соответствие спектральные многочлены $[C_1(x) - \beta_1(x^n - 1)]$ и $[C_2(x) - \beta_2(x^n - 1)]$. Согласно выражению (2), пара таких многочленов будет иметь своим разложением соответственно $T_1(x)G(x)$ и $T_2(x)G(x)$. Следовательно, если многочлены $T_1(x)$ и $T_2(x)$ взаимно простые, то многочлен Гоппы $G(x)$ является наибольшим общим делителем (НОД) данной пары спектральных многочленов.

Показатель трудозатрат для такой атаки может быть вычислен следующим образом. Общее число попыток до успешного декодирования не превышает величины $\binom{n}{z}^2$. После каждой попытки исправления векторов v_1 и v_2

над ними производится дискретное преобразование Фурье (ПФ) в поле Галуа, составляющее не менее $n \log n$ операций. Общее число пар спектральных многочленов $[C_1(x) - \beta_1(x^n - 1)]$ и $[C_2(x) - \beta_2(x^n - 1)]$ составляет величину

$(n + 1)^2$. Нахождение НОД для каждой такой пары требует не менее $n \log^2 n$ операций. Следовательно, ожидаемый общий показатель трудозатрат в случае выбора двух векторов для криптоанализа равен

$$w_2 = \left(\frac{n}{z}\right)^2 [2n \log n + (n + 1)^2 n \log^2 n]. \quad (3)$$

Для кодов большой длины ($n \geq 128$):

$$w_2 \approx \left(\frac{n}{z}\right)^2 n^3 \log^2 n. \quad (4)$$

Необходимо отметить, что для увеличения шансов однозначного определения многочлена $G(x)$ целесообразно выбирать большее число исходных векторов, так как в общем случае многочлены $T_1(x)$ и $T_2(x)$ могут не оказаться взаимно простыми. Рассуждая аналогичным образом, можно записать выражение для общего показателя трудозатрат w_i в случае выбора i векторов для криптоанализа:

$$w_i \approx \left(\frac{n}{z}\right)^i n^{(i+1)} \log^2 n. \quad (5)$$

Таким образом, выражение (5) позволяет определить необходимые трудозатраты при криптоанализе, основанном на определении кодов Гоппы в частотной области.

Рассмотрим криптоанализ на основе определения кодов Гоппы во временной области, который опирается на тот факт, что согласно [4] любой вектор $c = (c_1, c_2, \dots, c_n)$ двоичного кода Гоппы удовлетворяет условию

$$\sum_{i=1}^n \frac{c_i}{x - \alpha_i} = \frac{f'(x)}{f(x)} \equiv 0 \pmod{G(x)}, \quad (6)$$

где $f'(x)$ – формальная производная от $f(x)$ в поле $GF(2^m)$; $\{\alpha_1, \alpha_2, \dots, \alpha_n\}$ – подмножество различных элементов поля $GF(2^m)$ таких, что $G(\alpha_i) \neq 0$.

Для сепарабельных кодов Гоппы условие (6) выполняется и для $G^2(x)$. Следовательно, для любого вектора c можно вычислить соответствующий ему многочлен $f'(x)$, каноническое разложение которого содержит $G^2(x)$, т.е. справедливо выражение

$$f'(x) = [A(x)G(x)]^2, \quad (7)$$

где $A(x)$ – некоторый многочлен с коэффициентами из поля $GF(2^m)$.

Легко показать, что для кодовых векторов минимального веса d и веса $d + 1$ выражение (7) будет иметь более простой вид:

$$f'(x) = \gamma G^2(x), \quad (8)$$

где γ – некоторый ненулевой элемент поля $GF(2^m)$.

Таким образом, выражения (7) и (8) определяют возможные пути поиска $G(x)$ как общего делителя многочленов $f'(x)$.

Наиболее благоприятной ситуацией для криптоаналитика является знание искаженных кодовых векторов, вес которых при отсутствии ошибок ра-

вен \mathbf{d} или $\mathbf{d} + 1$. С учетом вектора ошибок однозначным признаком появления такого события является наличие вектора (шифртекста) весом не более $\mathbf{d} - \mathbf{z} + 1$. Трудозатраты для такой атаки определяются числом всевозможных пар комбинаций ошибок веса \mathbf{z} на $\mathbf{n} - \mathbf{d} + \mathbf{z} - 1$ нулевых позициях вектора \mathbf{v} .

Общее число таких пар составляет величину $\binom{\mathbf{n}+\mathbf{d}+\mathbf{z}-1}{\mathbf{n}}$. Основное число вычислений после каждого исправления ошибок приходится на представление многочлена $\mathbf{f}(\mathbf{x}) = (\mathbf{x} + \alpha_1)(\mathbf{x} + \alpha_2) \cdots (\mathbf{x} + \alpha_d)$ в виде суммы одночленов, то есть $\mathbf{f}(\mathbf{x}) = \mathbf{x}^d + \mathbf{a}_{d-1}\mathbf{x}^{d-1} + \cdots + \mathbf{a}_0$. Данная процедура занимает порядка \mathbf{d}^2 операций умножения и сложения. Таким образом, ожидаемый общий показатель трудозатрат для такой атаки равен

$$\mathbf{Q} = \binom{\mathbf{n}+\mathbf{d}+\mathbf{z}-1}{\mathbf{n}}^2 \mathbf{d}^2. \quad (9)$$

В остальных случаях, когда вес кодового вектора превышает $\mathbf{d} + 1$, криптоаналитик может воспользоваться выражением (7). Тогда при определении трудозатрат необходимо учесть общее число комбинаций ошибок веса \mathbf{z} , а также затраты на вычисление многочленов $\mathbf{f}(\mathbf{x})$, $\mathbf{f}'(\mathbf{x})$ и НОД соответствующих формальных производных. Таким образом, по аналогии с рассуждениями при вычислении показателя (5), выражение для общего показателя трудозатрат \mathbf{W}_i при начальном выборе для анализа i искаженных кодовых векторов будет иметь вид

$$\mathbf{W}_i = \binom{\mathbf{n}}{\mathbf{z}}^i \mathbf{n} \log^2 \mathbf{n}. \quad (10)$$

Очевидно, что наименьшие трудозатраты определяются выражением (9). Однако, можно показать, что доля кодовых слов минимального веса для линейных блочных кодов очень мала. Распределение весов таких кодов хорошо аппроксимируется биномиальным распределением [4]. Если спектру весов $\mathbf{B}_1, \mathbf{B}_2, \dots, \mathbf{B}_n$ где \mathbf{B}_j – число кодовых слов веса j двоичного $(\mathbf{n}, \mathbf{k}, \mathbf{d})$ -кода, поставить в соответствие вектор $\mathbf{b} = (\mathbf{b}_0, \mathbf{b}_1, \dots, \mathbf{b}_n)$, где $\mathbf{b}_j = \mathbf{B}_j/2^k$, причем $\mathbf{b}_0 = 2^{-k}$, $\mathbf{b}_1 = \mathbf{b}_2 = \dots = \mathbf{b}_{d-1} = 0$, то для компоненты \mathbf{b}_j с индексами $j \geq \mathbf{d}$ выполняется соотношение

$$\mathbf{b}_j \approx \frac{1}{2^n} \binom{\mathbf{n}}{j}. \quad (11)$$

Следовательно, при равновероятном и независимом появлении кодовых слов \mathbf{v} , вероятность появления слова минимального веса будет равна

$$\mathbf{P}_d \approx \frac{1}{2^n} \binom{\mathbf{n}}{d}. \quad (12)$$

В табл. 1 приведены значения вероятности \mathbf{P}_d для кодов различной длины \mathbf{n} и скорости \mathbf{R} . Следует заметить, что для кодов большой длины ($\mathbf{n} \geq 128$)

появление кодовых комбинаций малого веса можно считать маловероятным событием.

Таблица 1

Вероятность появления кодового слова минимального веса для кодов Гоппы различной длины и скорости

	$n = 32$	$n = 64$	$n = 128$	$n = 256$	$n = 512$	$n = 1024$
$R = 3/4$	5×10^{-5}	3×10^{-11}	7×10^{-24}	10^{-52}	4×10^{-105}	5×10^{-218}
$R = 1/2$	8×10^{-4}	7×10^{-7}	2×10^{-15}	6×10^{-34}	10^{-74}	10^{-155}
$R = 1/3$	0,03	9×10^{-6}	10^{-10}	3×10^{-22}	3×10^{-56}	3×10^{-91}

Таким образом, при подсчете необходимых трудозатрат для рассмотренных путей криптоанализа следует использовать выражения (5) и (10). Сравнивая данные выражения, можно заметить, что при равном числе векторов $i \geq 2$ показатель W_i содержит операций в n^i раз меньше, чем показатель w_i . Поэтому выражение (10) определяет самый короткий путь криптоанализа из предложенных.

Практическая значимость выведенного в процессе криптоанализа показателя трудозатрат (10) состоит в том, что с его помощью можно определить параметры системы Рао-Нама, обеспечивающие заданную стойкость данной криптосистемы.

ЛИТЕРАТУРА

1. Брикелл Э.Ф., Одлижко Э.М. Криптоанализ: Обзор новейших результатов // ТИИЭР. – Т.76. – №5. – 1988. – С. 75 - 93.
2. Диффи У. Первые десять лет криптографии с открытым ключом // ТИИЭР. – Т.76. – №5. – 1988. – С. 54 - 74.
3. Блейхут Р. Теория и практика кодов, контролирующих ошибки: Пер. с англ. / Под ред. К.Ш. Зигангирова. – М.: Мир, 1986. – С. 263 - 279.
4. Мак-Вильямс Ф.Дж., Слоэн Н.Дж.А. Теория кодов, исправляющих ошибки: Пер. с англ. / Под ред. Л.А. Бассалыго. – М.: Связь, 1979. – 744 с.

Поступила 22.04.2002

БУХАНЦОВ Андрей Дмитриевич, канд. техн. наук, зам. нач. НИО научного центра при ХВУ. В 1986 году окончил Харьковское ВВКИУ РВ. Область научных интересов – обработка информации, помехоустойчивое кодирование.

МАЛАХОВ Сергей Витальевич, канд. техн. наук, нач. лаборатории научного центра при ХВУ. В 1990 году окончил Харьковское ВВКИУ РВ. Область научных интересов – обработка информации, системы управления.

БРЕЖНЕВ Евгений Витальевич, канд. техн. наук, старший научный сотрудник научного центра при ХВУ. В 1994 году окончил ХВУ. Область научных интересов – экспертный анализ и синтез сложных систем.