В. В. П о д к о л з и н (Краснодар, КубГУ). **Построение инъективного рюкзачного вектора для заданного множества значений на основе вариации.**

Одним из способов криптоанализа рюкзачных систем защиты информации является поиск рюкзачного вектора на основе известных шифровых значений. Очевидно, что при поиске рюкзачного вектора путем решения системы линейных уравнений количество возможных решений определяется, прежде всего, количеством различных шифротекстов и информацией о свойствах рюкзачного вектора. Статистические методы требуют большой объем элементов шифротекстов для накопления статистики и при использовании РСЗИ ДГВⁿ [2] мало применимы. В работе, представленной данным сообщением, сделана попытка определить метод поиска рюкзачного вектора с использованием свойств значений, в нем выражаемых.

Вариацией вектора $A = (a_1, a_2, \dots, a_n)$ в Z_p назовем вектор $\Delta A = (\delta_1, \delta_2, \dots, \delta_n)$, где $\delta_1 = a_1$, $\delta_i = a_i - \sum_{j=1}^{i-1} (p-1)a_j$, $i = 2, \dots, n$.

Последовательность $W_{\mu_p(A)} = (w_0, w_1, \dots, w_k)$, где $w_k = Ax_i^T$, $x_i = (\alpha_1, \alpha_2, \dots, \alpha_n)$, $i = \sum_{j=1}^n \alpha_j p^{j-1}$, $i = 0, \dots, k$, $k = p^n - 1$, будем называть *последовательностью значений вектора* A в Z_p . Последовательность $(\omega_1, \omega_2, \dots, \omega_k)$, где $\omega_i = w_i - w_{i-1}$, $i = 1, \dots, p^n - 1$, обозначим как $\delta W_{\mu_p(A)}$. Последовательность $\delta W_{\mu_p(A)}$ является симметричной относительно середины и может быть определена рекурсивно относительно размерности рюкзачного вектора A . Пусть дана возрастающая последовательность значений $W' = (w'_1, w'_2, \dots, w'_m)$. Необходимо построить такой инъективный рюкзачный вектор $A = (a_1, a_2, \dots, a_n)$, что $W' \subseteq W_{\mu_p(A)}$. Для любой последовательности W' существует хотя бы один такой вектор, в частности, сверхрастающий вектор $(1, 2, 2^2, 2^3, \dots, 2^r)$, где $r = \lceil \log_2 w'_m \rceil + 1$. В работе, представленной данным сообщением, определяется метод построения таких векторов.

Каждой подпоследовательности $\delta W_{\mu_p(A)}$ можно сопоставить сумму элементов, ее составляющих, а каждой сумме — количество вхождений в $\delta W_{\mu_p(A)}$ подпоследовательностей, ее образующих. Например, для $A = (a_1, a_2, a_3)$ последовательность $\delta W_{\mu_p(A)}$ имеет вид $(\delta_1, \delta_2, \delta_1, \delta_3, \delta_1, \delta_2, \delta_1)$. Здесь сумме $\delta_1 + \delta_2 + \delta_1 + \delta_3$ соответствуют подпоследовательности $(\delta_1, \delta_2, \delta_1, \delta_3)$, $(\delta_2, \delta_1, \delta_3, \delta_1)$, $(\delta_1, \delta_3, \delta_1, \delta_2)$, $(\delta_3, \delta_1, \delta_2, \delta_1)$. Таким образом, для каждого рюкзачного вектора можно определить последовательность $S = \{(k_i, s_i)\}$, где s_i — сумма элементов подпоследовательности $\delta W_{\mu_p(A)}$, k_i — количество вхождений последовательностей элементов, образующих s_i в $\delta W_{\mu_p(A)}$, $k_i \leq k_j$, $i < j$.

Для заданной возрастающей последовательности значений W' построим множество $\delta W' = \{\omega'_i \mid \omega'_i = w'_i - w'_{i-1}\}$, где $w'_0 = 0$. На основе $\delta W'$ определим последовательность пар $S' = \{(k'_i, s'_i)\}$ аналогично S . Последовательно сопоставляя элементы S элементам S' и, решая $|S'|$ уравнений с n неизвестными, находим, если возможно, ΔA , а, следовательно, и A .

Например, необходимо найти рюкзачный вектор $A = (a_1, a_2, \dots, a_n)$ минимальной размерности n , для которого выполняется $W' = (5, 6, 8, 10, 12, 15, 21, 23) \subseteq W_{\mu_p(A)}$. Так как $|W'| = 8$, то $n \geq 4$. Построим последовательность пар $S' = \{(5, 2), (4, 5), (3, 3), (3, 6), (3, 7), (3, 8), (3, 10), (3, 13), (3, 15), (2, 1), (2, 4), (2, 9), (2, 11), (1, 8), (1, 12), (1, 16), (1, 17), (1, 18), (1, 21), (1, 23)\}$. Начальные элементы S_4 имеют вид: $(8, \delta_1)$, $(8, \delta_1 + \delta_2)$, $(8, \delta_1 + \delta_2 + \delta_1 + \delta_3)$, $(8, \delta_1 + \delta_2 + \delta_1 + \delta_3 + \delta_1 + \delta_2 + \delta_1 + \delta_4)$, $(4, \delta_2)$, $(4, \delta_1 + \delta_3)$, $(4, \delta_1 + \delta_2 + \delta_1)$, $(4, \delta_1 + \delta_2 + \delta_3)$, $(4, \delta_1 + \delta_2 + \delta_1 + \delta_3 + \delta_1)$, $(4, \delta_1 + \delta_2 + \delta_1 + \delta_3 + \delta_1 + \delta_2)$, $(4, \delta_1 + \delta_2 + \delta_1 + \delta_4), \dots$. Последовательно приравнивая вторые компоненты каждой пары S' к соответствующим значениям S_4 , получим следующее.

1. Для $(5, 2) \in S'$ возможно соответствие первых четырех элементов S_4 . Полагаем соответствие $\delta_1 = 2$ (если данное предположение окажется ложным, то будем последовательно приравнивать δ_1 значениям вторых компонент пар S').

2. Из $\delta_1 + \delta_2 = 2$ следует $\delta_2 = 0$, что противоречит возрастанию строимого

вектора, приравниваем $\delta_1 + \delta_2 = 5$. Получим $\delta_2 = 3$.

3. $\delta_1 + \delta_2 + \delta_1 + \delta_3 = 3 \Rightarrow \delta_3 = -4$, что невозможно. Проверяем следующий элемент S' : $\delta_1 + \delta_2 + \delta_1 + \delta_3 = 6$. Тогда $\delta_3 = -1$.

4. Для элемента $(8, \delta_1 + \delta_2 + \delta_1 + \delta_3 + \delta_1 + \delta_2 + \delta_1 + \delta_4) \in S_4$, последовательно проверяя элементы S' и выбирая удовлетворяющие условию инъективности и возрастания рюкзачного вектора, получим $\delta_1 + \delta_2 + \delta_1 + \delta_3 + \delta_1 + \delta_2 + \delta_1 + \delta_4 = 10 \Rightarrow \delta_4 = -3$.

Проверкой убеждаемся, что вектор $A = (2, 5, 6, 10)$ является искомым.

Следует отметить, что количество вариантов, которые необходимо перебрать при поиске решений, зависит от мощности множества W' , и существенным здесь является только количество различных значений, а не их частотные характеристики. Более того, предложенный метод также применим для поиска рюкзачного вектора заданной размерности.

На основе анализа предложенного метода можно сделать вывод о том, что чем больше известно значений из подпоследовательности W , принадлежащих отрезку $[a_n, \sum_{j=1}^n (p-1)a_j]$, тем проще будет процесс нахождения решения, так как в данном отрезке находятся значения, использующие в своем выражении все элементы рюкзачного вектора.

СПИСОК ЛИТЕРАТУРЫ

1. Саломаа А. Криптография с открытым ключом. М.: Мир, 1995.
2. Подколзин В. В. Модель системы защиты информации с открытым ключом на основе динамической генерации рюкзачного вектора. — Обозрение прикл. и промышл. матем., 2009, т. 16, в. 5, с. 913.