В. В. Подколзин (Краснодар, КубГУ)**. Модель системы защиты информации с открытым ключом на основе динамической генерации рюкзачного вектора.**

Обозначим $\Delta A = (\delta_1, \delta_2, \ldots, \delta_n)$ вектор изменений вектора $A = (a_1, a_2, \ldots, a_n)$, где $\delta_1 = a_1$, $\delta_i = a_i - \sum_{j=1}^{i-1} a_j$, $i = 2, \ldots, n$.

Определение. Произвольную всюду определенную функцию F: $N^k \to N^n$ будем называть *генератором положительных векторов размерности* n.

Вектор $A = (a_1, a_2, \ldots, a_n)$ определяется генератором векторов F, если существует $\alpha \in N^k$, для которого $F(\alpha) = A$. В качестве генератора положительных векторов размерности n (ГПВ^n) могут выступать алгоритм, аналитическая функция или их совокупность, важным здесь является то, что $F(\alpha)$ может быть найдено за приемлемое (в том или ином смысле) время.

Вектор $F(\alpha) = A$ можно рассматривать как рюкзачный вектор размерности n, но в общем случае необходимость существования и единственности решения задачи о рюкзаке [1] может потребовать наложения ряда ограничений на ГПВ^n. С другой стороны, если рассматривать $F(\alpha)$ как ΔA, то A — сверхрастущий рюкзачный вектор.

Определим модель защиты информации с использованием ГПВ^n. Пусть $S = N^c$ и $P = N^d$ таковы, что $S \times P = N^k$. 1) Секретным ключом является ГПВ^n F: $S \times P \to N^n$ и вектор $s \in S$; 2) открытым ключом является случайное значение $p \in P$; 3) отправитель вычисляет криптотекст $w = (A, v)$ для входа v, где $F(s, p) = \Delta A$; 4) получатель, на основе секретного ключа (F, s) для сообщения (p, w), определяет A и вычисляет v.

Очевидно, что задача криптоанализа для вышеопределенной модели является NP-полной. Более того, в случае большого размера исходных данных, они могут быть разделены на блоки с собственным открытым ключом.

Преимущество предложенной модели СЗИ с открытым ключом заключается в том, что даже при большой размерности рюкзачного вектора, определяемого ГПВ^n, сам генератор может быть достаточно прост. Проиллюстрируем данное утверждение на примере.

Пример. ГПВ^n F: $N^4 \to N^n$ определим следующим образом: для заданного вектора $(t_0, x_0, y_0, z_0) \in N^4$ решим уравнение

$$\sin(t + z)^{xy} = 0 \tag{1}$$

среди всех решений (1) выберем такие $t_1, t_2, \ldots, t_n, \ldots$, что

$$t_0 \leqslant t_j < t_{j+1}, j = 1, \ldots, n-1, \tag{2}$$

и на отрезке $[t_1, t_n]$ нет других решений (1). Вектор $([t_1], [t_2], \ldots, [t_n])$ определим как значение F. Открытым ключом является пара $p = (t_0, y_0)$. Закрытым ключом — $(F, (t_0, x_0))$.

Для рассмотренной в примере модели СЗИ с открытым ключом, несмотря на (2), задача криптоанализа остается NP-полной, хотя процессы шифрования и дешифрования достаточно просты.

СПИСОК ЛИТЕРАТУРЫ

1. *Саломаа А.* Криптография с открытым ключом. М.: Мир, 1995.