УДК 512.624

МЕТОД ВОССТАНОВЛЕНИЯ НАЧАЛЬНОГО СОСТОЯНИЯ ЛИНЕЙНОГО ГЕНЕРАТОРА НАД КОНЕЧНЫМ ПОЛЕМ, УСЛОЖНЁННОГО НАЛОЖЕНИЕМ МАСКИ

А. В. Волгин, А. В. Иванов

Рассматривается линейный генератор [1], который определяется как последовательность $\{u_n\}_{n=0}^{\infty}$ над полем $P = (\mathrm{GF}(q), +, \cdot)$, $q = p^s$, удовлетворяющая линейному соотношению

$$u_{n+1} = au_n + b,\ a, b \in GF(q),\ a \neq 0,\ n = 0, 1, \ldots$$

Пусть $\alpha = (\alpha_1, \ldots, \alpha_s)$ — фиксированный базис поля P, $\varepsilon_0, \ldots, \varepsilon_s$ — некоторые элементы поля P, которые имеют представление в базисе α:

$$\varepsilon_i = \varepsilon_i^{(1)}\alpha_1 + \ldots + \varepsilon_i^{(s)}\alpha_s,\ \varepsilon_i^{(j)} \in \mathrm{GF}(p),\ i = 0, \ldots, s,\ j = 1, \ldots, s.$$

Зафиксируем $k \in \mathbb{N}$, $k < s$. Будем считать, что $\varepsilon_i^{(j)} = 0$ для всех $i = 0, \ldots, s$, $j = k + 1, \ldots, s$.

Пусть задано некоторое натуральное число t, $k+1 \geqslant t > 2$, известны параметры a, b и элементы $w_0, \ldots, w_{t-1}$ поля P вида

$$w_i = u_i - \varepsilon_i,\ i = 0, \ldots, t-1. \tag{1}$$

Пусть также известно, что $a \notin \mathcal{F}$, где $\mathcal{F}$ — фиксированное подмножество P, $|\mathcal{F}| < 2p^{\delta_t} + \binom{k}{t-2} p^{2k-t+2}$, где δ_t — наибольший из делителей s, которые меньше t. В [1] предложен метод, позволяющий при данных условиях восстанавливать значение u_0 с полиномиальной сложностью. В докладе предлагается метод, позволяющий восстанавливать u_0 при условии, когда параметр b неизвестен.

Теорема 1. Пусть известны $w_0, \ldots, w_{t-1}$ из соотношения (1), известен мультипликативный множитель a, $a \notin \mathcal{F} \subset P$, $\mathcal{F}$ — фиксированное множество, $|\mathcal{F}| < 2p^{\delta_t} + \binom{k}{t-2} p^{2k-t+2}$, $k + 1 \geqslant t > 2$, δ_t — наибольший из делителей s, которые меньше t, и неизвестна аддитивная константа b. Тогда существует алгоритм, который при определённых условиях с полиномиальной сложностью находит начальное значение u_0.

ЛИТЕРАТУРА

1. *Gutierrez J., Ibeas A., Gomez-Perez D., and Shparlinski I. E.* Predicting masked linear pseudorandom number generators over finite fields. Berlin: Springer, 2012.

УДК 003.26.09

О СИСТЕМЕ МАК-ЭЛИСА НА НЕКОТОРЫХ АЛГЕБРО-ГЕОМЕТРИЧЕСКИХ КОДАХ[1]

М. М. Глухов-мл.

В последние годы внимание многих специалистов в области криптографии с открытым ключом уделено развитию кодовых криптосистем, в частности схем Мак-Элиса и

[1]Работа поддержана грантом РФФИ, проект № 6260.2012.10.