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.

Нидеррайтера. Их стойкость основана на вычислительной сложности задачи декодирования кода, порождающая (или проверочная) матрица которого выглядит как некая случайная матрица.

С точки зрения стойкости такой системы крайне важен выбор семейства кодов. В «оригинальной» системе Мак-Элиса используется классический двоичный код Гоппы. В работе [1] рассматривается возможность применения $[961, 771]_{31}$-кодов Гоппы, который, при одинаковой стойкости по сравнению с двоичным кодом Гоппы, дает существенно меньшую длину открытого ключа. Продолжение исследований, связанных с обоснованием преимуществ недвоичных кодов Гоппы, содержится в работе [2].

Долгое время считался удачным выбор В. М. Сидельниковым [3] двоичного кода Рида — Маллера. Однако в работе [4] предложен субэкспоненциальный алгоритм атаки на такую систему. При этом используется возможность нахождения кодового слова минимального веса кода $\mathrm{RM}(r, m)$ как произведения r слов (функций) минимального веса из $\mathrm{RM}(1, m)$. Этот алгоритм оказался эффективен для кода Рида — Маллера третьего порядка длины 2048.

Как показано в [5], к нестойкой системе приводит использование кодов Рида — Соломона в системе Нидеррайтера. На первом этапе полиномиального алгоритма вскрытия системы использована трижды транзитивность группы обобщённых автоморфизмов указанных кодов.

Ранее автором (см. [6]) найдена конструкция классов алгебро-геометрических кодов над различными конечными полями с очень хорошим соотношением скорости и относительного расстояния, в частности семейство $\{C_r : [768, 3r - 57, 768 - 3r]_{256}\}_{r=39}^{255}$ кодов на кривой над $P = \mathrm{GF}(2^8)$, заданной уравнением $y^3 = x^{60} + x^{57} + x^{54} + \ldots + x^3 + 1$.

Каждый из построенных кодов $C_r = C(D, G)$ определяется дивизорами D и G, где D — формальная сумма всех P-рациональных точек $Q_1, \ldots, Q_{768}$ кривой, а $G = r \cdot Q_\infty$. Векторами кода C являются векторы значений функций от двух переменных x и y из некоторого класса Φ_0, который, при условии $114 < \deg G = 3r < 768$, образует линейное подпространство размерности $3r - 57$ над полем P с базисом $B = \{x^i y^j : j = 0, 1, 2, i = 0, 1, \ldots, r - 20j\}$ пространства Φ всех функций от x, y над P.

Из данного кода методом, основанным на проектировании кодов, получаются семейства кодов $C'_{r,m} = C(D', G)$, где D' есть сумма m произвольных P-рациональных точек кривой при условии $114 < \deg G = 3r < m \leqslant 768$. При выполнении указанных условий размерности полученных кодов совпадают с размерностью «исходного» кода C_r. Таким образом, при фиксированном m получается до $\binom{768}{m}$ кодов длины m и размерности $3r - 57$. При этом кодовое расстояние d любого из кодов $C'_{r,m}$ равно $d = m - 3r$.

Нетрудно оценить величину числа m, обеспечивающую стойкость кодовой системы к перебору всех $\binom{768}{m}$ сочетаний вошедших в дивизор точек кривой, а также к перебору всех возможных векторов-ошибок.

С другой стороны, мы получаем возможность варьировать длину и размерность кодов для получения оптимальных параметров системы.

Таким образом были выделены семейства кодов C'_r: $[m, 3r - 57, m - 3r]_{256}$-коды при $m = \overline{150, 739}$, $r = \overline{39, 235}$.

Порождающая матрица каждого из этих кодов C' получается из порождающей матрицы кода C удалением $768 - m$ столбцов, соответствующих точкам кривой, удалённым из дивизора D при переходе к дивизору D'.

Для рассматриваемых кодов и во введённых обозначениях справедлива следующая теорема.

Теорема 1. Пусть $C_r = C(D, G)$ — код, в котором дивизор $D = Q_1 + \ldots + Q_{768}$ есть сумма всех P-рациональных точек кривой, заданной уравнением $y^3 = x^{60} + x^{57} + x^{54} + \ldots + x^3 + 1$. Тогда в порождающей матрице этого кода нет одинаковых столбцов. Для каждого фиксированного кода из рассматриваемых семейств $C'_{r,m}$ при $r \leqslant 127$ и фиксированном m получается $\dfrac{1}{18}\dbinom{768}{m}$ различных кодов.

Доказательство теоремы конструктивно и даёт возможность выбора точек дивизора D' так, чтобы все полученные коды были различны.

Код C при указанных выше значениях r изоморфен пространству Φ_0. Описание автоморфизмов алгебры Φ, оставляющих на месте Φ_0, дает следующая теорема.

Теорема 2. В указанных выше обозначениях при $39 \leqslant r \leqslant 127$ каждый автоморфизм линейной алгебры Φ, отображающий Φ_0 на себя, задается образами x, y: $\varphi(x) = ax + \delta$; $\varphi(y) = dy$, где $a, d, \delta \in P$ и $a^3 = d^3 = 1$, $\delta \in \{0, 1\}$ в поле P.

Из этой теоремы выводятся достаточные условия на выбор точек дивизора D' для получения кодов $C(D', G)$ с тривиальной группой автоморфизмов.

Обобщёнными автоморфизмами кода длины N называют композицию его автоморфизма и преобразования, заключающегося в умножении i-й координаты всех его векторов на один и тот же элемент k_i поля (зависящий от i), $i = 1, \ldots, N$. Условимся последнее преобразование называть мультипликативным сдвигом на вектор $(k_1, k_2, \ldots, k_N)$. При $k_1 = \ldots = k_N$ будем называть его тривиальным сдвигом на k_1.

Теорема 3. Код $C(D', G)$ имеет только тривиальные мультипликативные сдвиги на любые элементы из P.

ЛИТЕРАТУРА

1. *Peters Chr.* Information-set decoding for linear codes over F_q // LNCS. 2010. V. 6061. P. 81–94.
2. *Bernstein D. J., Lange T, and Peters Chr.* Wild McEliece // `http://eprint.iacr.org/2010/410`.
3. *Сидельников В. М.* Открытое шифрование на основе двоичных кодов Рида — Маллера // Дискретная математика. 1994. Т. 6. Вып. 3. С. 3–20.
4. *Minder L. and Shokrollahi A.* Cryptanalysis of the Sidelnikov cryptosystem // LNCS. 2007. V. 4515. P. 347–360.
5. *Сидельников В. М., Шестаков С. О.* О системе шифрования, построенной на основе обобщённых кодов Рида — Соломона // Дискретная математика. 1994. Т. 4. Вып. 3. С. 57–63.
6. *Глухов М. М.* О кодах Гоппы на одном семействе полей алгебраических функций // Дискретная математика. 2001. Т. 13. Вып. 2. С. 14–34.

УДК 519.7, 004.056.2, 004.056.53

УСЕЧЁННЫЕ ДИФФЕРЕНЦИАЛЬНЫЕ ХАРАКТЕРИСТИКИ С МИНИМАЛЬНЫМ КОЛИЧЕСТВОМ АКТИВНЫХ БАЙТ ДЛЯ УПРОЩЁННОЙ ХЭШ-ФУНКЦИИ WHIRLPOOL

А. А. Камаева

Хэш-функция *Whirlpool* (далее $\mathcal{W}$) разработана Винсентом Риджменом (*Vincent Rijmen*) и Пауло Баррето (*Paolo Barreto*) и опубликована в 2000 г. [1]. Претерпев ряд