Секция 5

ПРИКЛАДНАЯ ТЕОРИЯ КОДИРОВАНИЯ, АВТОМАТОВ И ГРАФОВ

УДК 003.26, 519.725, 519.176 DOI 10.17223/2226308X/13/28

О НОВЫХ ОЦЕНКАХ РАЗМЕРНОСТИ ПОДКОДОВ КОДОВ РИДА — МАЛЛЕРА, КВАДРАТ АДАМАРА КОТОРЫХ МАКСИМАЛЕН

В. В. Высоцкая

Наличие в коде некоторой структуры может привести к снижению стойкости всей системы, построенной на нем. Для «маскировки» кода под код «общего вида» часто используются подкоды. Однако стойкость подкодов, квадрат Адамара которых равен квадрату полного кода, сводится к стойкости этого кода. Таким образом, данное свойство необходимо учитывать как при синтезе схем на кодах, так и при их криптоанализе. В работе анализируется минимальное количество мономов степени r, которые при добавлении к коду $RM(r-1,m)$ образуют подкод, квадрат Адамара которого максимален, т. е. совпадает с кодом $RM(2r,m)$. Это число снизу оценивается аналитически, а для получения верхней оценки предлагается жадный алгоритм построения такого набора мономов.

Ключевые слова: *постквантовая криптография, кодовая криптография, коды Рида — Маллера, подкоды Рида — Маллера, произведение Адамара, криптосистема Мак-Элиса.*

В последнее время большую популярность получили кодовые криптосистемы. Этот интерес прослеживается в работах, поданных на конкурс на перспективный постквантовый алгоритм, объявленный NIST [1] в 2016 г. для дальнейшей стандартизации. Кроме того, ТК 26 выбрал схемы на кодах как одно из направлений разработки будущего российского стандарта постквантовых алгоритмов.

При синтезе новых кодовых схем одним из самых важных вопросов является выбор базового кода, от которого будут зависеть все характеристики. В целях создания асимметрии в возможностях легального пользователя и противника требуется скрывать структуру кода. Это можно сделать, например, используя подкоды. Однако в работе И. В. Чижова и М. А. Бородина [2] стойкость криптосистемы Мак-Элиса [3] на подкодах коразмерности 1 сведена к стойкости оригинальной криптосистемы. Сведение работает для подкодов, квадрат Адамара которых совпадает с квадратом базового кода. Такое свойство подкодов без наложения ограничений на коразмерность исследовано в работе [4].

Определение 1. *Кодом Рида — Маллера* $RM(r,m)$ называется множество булевых функций f от m переменных, таких, что $\deg(f) \leqslant r$.

Определение 2. *Произведением Адамара двух векторов* называется вектор, полученный в результате покомпонентного произведения координат этих векторов:

$$(a_1,\ldots,a_n)\circ(b_1,\ldots,b_n)=(a_1b_1,\ldots,a_nb_n),$$

а *произведение Адамара двух кодов* $\mathcal{A}$ *и* $\mathcal{B}$ есть линейная оболочка всех попарных произведений вида $a\circ b$, где $a\in\mathcal{A}$, $b\in\mathcal{B}$.

Отметим, что квадрат Адамара кода Рида — Маллера имеет смысл только при $m \geqslant 2r$.

Будем рассматривать подкоды вида

$$\big(RM(r-1,m) \cup \{f_1, \ldots, f_{w(m,r)}\}\big)^2 = RM(2r,m), \tag{1}$$

где $f_1, \ldots, f_{w(m,r)}$ — мономы степени r, а под возведением в квадрат понимается квадрат Адамара. Задача состоит в минимизации значения $w(m,r)$.

Перейдём к графовой интерпретации задачи. Сопоставим подкод $\mathcal{A} \subset RM(r,m)$ с гиперграфом G с m вершинами, помеченными как $x_1, \ldots, x_m$. Ребро $\{x_{i_1}, \ldots, x_{i_r}\}$ проведено тогда и только тогда, когда моном $x_{i_1} \ldots x_{i_r} \in \mathcal{A}$. В [4] показано, что для обеспечения условия (1) достаточно, чтобы гиперграф был стабильным.

Определение 3. Гиперграф называется *стабильным*, если каждое множество, состоящее из $2r$ вершин, покрыто двумя непересекающимися r-рёбрами.

Очевидно, что задача поиска стабильного гиперграфа с минимальным количеством r-рёбер эквивалентна поиску минимального числа $w(m,r)$. В работе [4] это число для $r \geqslant 2$ и $h < r/3$ оценено как

$$\mathrm{C}_m^{2r}/\mathrm{C}_{m-r}^r \leqslant w(m,r) \leqslant \mathrm{C}_m^r - T(r,m,h)\,(\mathrm{C}_{2r}^r - 2)\,, \tag{2}$$

где

$$T(r,m,h) = \max\big\{t : \exists S_1, \ldots, S_t \big(S_i \subset \{1,\ldots,m\} \;\&\; \\ \&\; |S_i| = 2r \;\&\; (i \neq j \Rightarrow |S_i \cap S_j| \leqslant h),\; i,j \in \{1,\ldots,t\}\big)\big\}.$$

Эти оценки могут быть улучшены.

Теорема 1.

$$w(m,r) \geqslant \sqrt{\gamma + 2\mathrm{C}_m^{2r}} + \sqrt{\gamma}, \quad \text{где} \quad \gamma = \sum_{i=\max\{1,3r-m\}}^{r-1} \mathrm{C}_r^i.$$

Для получения верхней оценки предложен алгоритм, который по параметрам кода строит соответствующий стабильный гиперграф. Его реализацию, написанную на Python, можно посмотреть в `https://github.com/VysotskayaVictory/StableGraphGreedy/`. На каждом шаге алгоритма происходит попытка добавить новое r-ребро. В случае успеха значение $w(m,r)$ увеличивается на 1, а также формируется список r-рёбер, которые пересекаются с данным. Они добавляются в список `inter`. Вместе с этим поддерживается счетчик `repeated` повторно покрытых множеств. Алгоритм останавливается, когда все C_m^{2r} множеств размера $2r$ покрыты парами непересекающихся r-рёбер. Условием останова является выполнение равенства

$$\mathrm{C}_{w(m,r)}^2 - |\texttt{inter}| - \texttt{repeated} = \mathrm{C}_m^{2r}.$$

Сравнение полученных оценок с оценками из (2) представлено на рис. 1. Его анализ позволяет говорить о том, что оценки существенно улучшены.

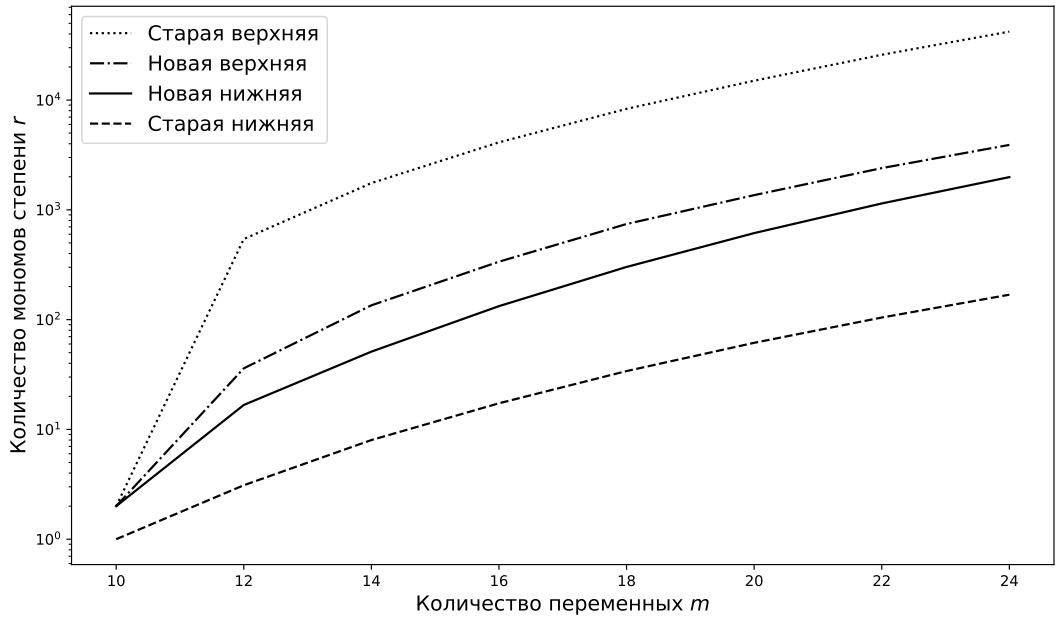

Рис. 1

ЛИТЕРАТУРА

1. `https://csrc.nist.gov/Projects/post-quantum-cryptography/Post-Quantum-Cryptography-Standardization/Call-for-Proposals`.
2. *Чижов И. В., Бородин М. А.* Классификация произведений Адамара подкодов коразмерности 1 кодов Рида — Маллера // Дискретная математика. 2020. № 32(1). С. 115–134.
3. *McEliece R. J.* A public-key cryptosystem based on algebraic coding theory // DSN Progress Report. 1978. No. 4244. P. 114–116.
4. *Vysotskaya V. V.* Characteristics of Hadamard Square of Reed — Muller Subcodes of Special Type. `https://eprint.iacr.org/2020/507`.

УДК 519.1 DOI 10.17223/2226308X/13/29

О КОЛИЧЕСТВЕ НЕДОСТИЖИМЫХ СОСТОЯНИЙ В КОНЕЧНЫХ ДИНАМИЧЕСКИХ СИСТЕМАХ ОРИЕНТАЦИЙ ПОЛНЫХ ГРАФОВ

А. В. Жаркова

Рассматриваются конечные динамические системы ориентаций полных графов. Состояниями системы являются все возможные ориентации полного графа, а эволюционная функция задаётся следующим образом: динамическим образом данного орграфа является орграф, полученный из исходного путём переориентации всех дуг, входящих в стоки, других отличий между исходным орграфом и его образом нет. Приводятся формулы для подсчёта количества недостижимых и достижимых состояний в рассматриваемых системах, представлены соответствующие таблицы для полных графов с количеством вершин от двух до десяти.

Ключевые слова: *граф, достижимое состояние, источник, конечная динамическая система, недостижимое состояние, ориентация графа, полный граф, сток, турнир, эволюционная функция.*