УДК 519.17

ДЕТЕРМИНИРОВАННЫЕ МЕТОДЫ ПОСТРОЕНИЯ ГРАФОВ РАМАНУДЖАНА, ПРЕДНАЗНАЧЕННЫХ ДЛЯ ПРИМЕНЕНИЯ В КРИПТОГРАФИЧЕСКИХ АЛГОРИТМАХ, ОСНОВАННЫХ НА ОБОБЩЁННЫХ КЛЕТОЧНЫХ АВТОМАТАХ[1]

П. Г. Ключарёв

Московский государственный технический университет им. Н. Э. Баумана, г. Москва, Россия

Рассматриваются детерминированные методы построения графов Рамануджана в контексте их применения в качестве графов обобщённых клеточных автоматов, предназначенных для использования в криптографии. Изучены два семейства графов Любоцкого — Филипса — Сарнака ($X^{p,q}$ и $Y^{p,q}$), семейство графов Пайзера и семейство графов Моргенштерна. Сделан вывод, что для применения в указанном качестве подходят графы Пайзера и графы $Y^{p,q}$. Приведены значения параметров графов из этих семейств, полученные численно.

Ключевые слова: *расширяющий граф, граф Рамануджана.*

DOI 10.17223/20710410/42/6

DETERMINISTIC METHODS OF RAMANUJAN GRAPH CONSTRUCTION FOR USE IN CRYPTOGRAPHIC ALGORITHMS BASED ON GENERALIZED CELLULAR AUTOMATA

P. G. Klyucharev

Bauman Moscow State Technical University, Moscow, Russia

E-mail: pk.iu8@yandex.ru

Earlier, the author proposed a number of methods for constructing symmetric cryptographic algorithms based on generalized cellular automata. In order to make such automata to be cryptographically strong, their graphs must satisfy a number of requirements. In particular, they must be regular not bipartite graphs with a small diameter, a small degree (but not less than 4) and the amount of graphs in the family with the number of vertices from dozens to several thousand must be large enough (it would be desirable to have at least several dozens of graphs with a number of vertices more or less uniformly distributed in the given range). Some of Ramanujan graphs satisfy these requirements. There are two ways to construct relatively small Ramanujan graph: the random way and the deterministic way. In this paper, the deterministic methods for Ramanujan graphs construction in the context of their application in generalized cellular automata being a base of cryptographic algorithms are considered. Each method can be identified with the family of graphs generated by it. Among them are two families of graphs constructed by Lubotzky, Philips and Sarnak — $X^{p,q}$ and $Y^{p,q}$, the family of graphs constructed by Pizer, and the family of graphs constructed by Morgenstern. Values of parameters of graphs from these families are numerically computed. After research, we came to conclusion that Pizer

[1]Работа выполнена при финансовой поддержке РФФИ в рамках научного проекта № 16-07-00542.

graphs (based on isogenies of elliptic curves over finite fields) and the $Y^{p,q}$ Lubotzky — Philips — Sarnak graphs (based on projective transformations of a projective line over a finite field) are suitable for the purposes under consideration, because, according to literature review, they meet all the necessary requirements, in particular, they are not bipartite, and among them there are sufficiently large amount of relatively small graphs with small degrees (all Ramanujan graphs are regular and have a small diameter). At the same time, the $X^{p,q}$ Lubotzky — Philips — Sarnak graphs and Morgenstern graphs are not suitable for considered purposes, because among them there are too few not bipartite graphs with a small degree and with a number of vertices in the desired range.

Keywords: *expander graph, Ramanujan graph.*

Введение

Ранее автором в ряде работ (в том числе в [1, 2]) предложены методы построения симметричных шифров и криптографических хэш-функций, основанных на обобщённых клеточных автоматах. Криптоалгоритмы, полученные с помощью этих методов, обладают рядом ценных свойств, в частности высокой производительностью при аппаратной реализации. Для того чтобы такие алгоритмы были криптостойкими, графы обобщённых клеточных автоматов должны удовлетворять ряду требований. Данная работа посвящена детерминированным методам построения таких графов.

1. Основные понятия

Будем использовать термин «граф», допуская наличие петель и кратных рёбер.

Обобщённым клеточным автоматом называется ориентированный граф (*граф обобщённого клеточного автомата*) с множеством вершин $V = \{v_1, \ldots, v_N\}$, с каждой вершиной v_i которого ассоциированы:

— булева переменная m_i, которая называется *ячейкой*;
— булева функция $f_i(x_1, \ldots, x_{d_i})$, которая называется локальной функцией связи вершины v_i (d_i — степень вершины v_i).

При этом каждой паре (v, e), где $v \in V$ — вершина, e — входящее в неё ребро, соответствует номер аргумента локальной функции связи, вычисляемой в вершине v. Будем называть его *номером ребра e относительно вершины v*. Работа обобщённого клеточного автомата происходит следующим образом. В начальный момент времени каждая ячейка m_i, $i = 1, \ldots, N$, принимает некоторое начальное значение $m_i(0)$. Автомат работает пошагово, значения ячеек на шаге номер t вычисляются по формуле

$$m_i(t) = f_i(m_{\eta(i,1)}(t-1), m_{\eta(i,2)}(t-1), \ldots, m_{\eta(i,d_i)}(t-1)),$$

где $\eta(i, j)$ — номер вершины, из которой исходит ребро, входящее в вершину v_i и имеющее относительно этой вершины номер j.

Будем рассматривать только *неориентированные* обобщённые клеточные автоматы, т. е. такие, что для каждого ребра (u, v) в графе автомата существует и ребро (v, u). Такой граф можно рассматривать как неориентированный, для чего достаточно заменить каждую пару ориентированных рёбер (u, v) и (v, u) на неориентированное ребро $\{u, v\}$. Будем рассматривать только обобщённые клеточные автоматы, графы которых являются регулярными ($d_1 = \ldots = d_N = d$).

Обобщённый клеточный автомат представляет собой обобщение клеточного автомата [3], предложенного Дж. фон Нейманом. Подобные обобщения под разными на-

званиями использовались в различных областях (см., например, [4, 5]). Методы применения обобщённых клеточных автоматов в криптографии развиты в [1, 2].

2. Требования к графам

Как обосновано в предыдущих работах автора, для построения обобщённых клеточных автоматов, применяемых в составе криптографических алгоритмов, требуются связные неориентированные графы, обладающие следующими свойствами:

— граф должен иметь свойства, близкие к свойствам случайного графа;
— диаметр графа должен быть близок к минимально возможному;
— число петель и кратных рёбер в графе должно быть как можно меньшим;
— граф должен являться регулярным;
— степень графа должна быть как можно меньшей (для повышения эффективности аппаратной реализации обобщённого клеточного автомата);
— степень графа должна быть не меньше четырёх;
— граф не должен являться двудольным;
— количество графов с числом вершин от нескольких десятков до нескольких тысяч в семействе графов должно быть достаточно велико, чтобы в семействе существовали графы, годящиеся для построения обобщённых клеточных автоматов с различным числом ячеек (хотелось бы иметь хотя бы несколько десятков графов с числом вершин, более или менее равномерно распределённым в данном диапазоне).

Заметим, что в этом ряду требований словосочетание «как можно меньшее» следует понимать в приближённом смысле — достаточна лишь близость к минимально возможным значениям. Приведённым требованиям удовлетворяют графы Рамануджана [6–8].

3. Расширяющие графы

Графы Рамануджана изучаются в теории расширяющих графов. Это сравнительно молодая область дискретной математики, нашедшая много приложений в различных теоретических и прикладных областях математики и компьютерных наук. Ей посвящено большое количество работ, в том числе [6, 7, 9 – 12]. Приведём некоторые сведения из этой теории, необходимые для дальнейшего изложения.

Коэффициентом рёберного расширения неориентированного d-регулярного графа G с множеством вершин V называется величина

$$h(G) = \min_{\{S \subset V : 0 < |S| \leqslant |V|/2\}} \frac{|\partial S|}{|S|},$$

где $|\partial S|$ — число рёбер, каждое из которых соединяет вершину из множества S с вершиной из множества $V \setminus S$.

Расширяющим графом (expander graph) называется неориентированный регулярный граф G, для которого $h(G) \geqslant c$, где c — некоторая наперёд заданная положительная константа.

Коэффициент рёберного расширения графа связан с его спектральными свойствами. Спектр неориентированного графа — это набор собственных значений его матрицы смежности, отсортированный по невозрастанию: $\lambda_1 \geqslant \lambda_2 \geqslant \cdots \geqslant \lambda_N$. Здесь и далее N — число вершин графа.

Как известно из спектральной теории графов, для d-регулярных графов $\lambda_1 = d$ и справедливо следующее *неравенство Чигера*:

$$\frac{1}{2}(d - \lambda_2) \leqslant h(G) \leqslant \sqrt{2d(d - \lambda_2)}.$$

Пусть $\lambda = \lambda(G) = \max\limits_{|\lambda_i|<d} |\lambda_i|$. *Графом Рамануджана* называется связный d-регулярный неориентированный граф G, для которого справедливо следующее неравенство:

$$\lambda(G) \leqslant 2\sqrt{d-1}. \tag{1}$$

Для диаметра $D(G)$ графов Рамануджана справедливо соотношение [13]

$$D(G) \leqslant 2\log_{d-1} N + \mathrm{O}(1).$$

Этот диаметр достаточно близок к границе Мура.

Известны следующие подходы к построению небольших графов Рамануджана:

1) построение при помощи известного детерминированного метода;
2) случайная генерация с последующей проверкой значения λ.

В данной работе мы рассмотрим известные детерминированные методы построения графов Рамануджана, чтобы выбрать подходящие для использования сгенерированных с их помощью графов в качестве графов обобщённых клеточных автоматов с расчётом на их применение в криптографии. Такой метод должен давать достаточную свободу в выборе числа вершин графа. Важным является вопрос о диаметре таких графов. Для некоторых приложений важен также обхват графа (обхватом графа называется длина наименьшего содержащегося в нём цикла).

Одним из понятий, используемых в явных конструкциях графов Рамануджана, являются графы Кэли. Пусть H — конечная группа, S — её подмножество, такое, что $1 \notin S$ и $x^{-1} \in S$ для любого $x \in S$. *Графом Кэли* $\mathfrak{G}(H, S)$ группы H по множеству S называется неориентированный граф, вершинами которого являются элементы группы H. Вершины $u \in H$ и $v \in H$ соединены ребром тогда и только тогда, когда существует такое $s \in S$, что $v = us$. Такой граф, очевидно, является $|S|$-регулярным, в нём отсутствуют петли и кратные ребра.

4. Семейство графов $X^{p,q}$ Любоцкого — Филипса — Сарнака

Пожалуй, наиболее известным семейством графов Рамануджана является так называемое семейство $X^{p,q}$ Любоцкого — Филипса — Сарнака [8, 10, 14]. Чтобы описать графы из этого семейства, напомним стандартные определения некоторых теоретико-групповых конструкций [15–19].

Пусть K — коммутативное кольцо с единицей, $\mathbb{F}$ — поле. *Полной линейной группой* $\mathrm{GL}(n, K)$ называется мультипликативная группа всех обратимых матриц размера $n \times n$ над кольцом K. Её подгруппа $\mathrm{SL}(n, K)$ матриц с определителем, равным единице, называется *специальной линейной группой*.

Проективной полной линейной группой $\mathrm{PGL}(n, \mathbb{F})$ называется фактор-группа полной линейной группы $\mathrm{GL}(n, \mathbb{F})$ по её центру — подгруппе ненулевых скалярных матриц. *Проективной специальной линейной группой* $\mathrm{PSL}(n, \mathbb{F})$ называется фактор-группа специальной линейной группы $\mathrm{SL}(n, \mathbb{F})$ по её центру. Элементами групп $\mathrm{PGL}(n, \mathbb{F})$ и $\mathrm{PSL}(n, \mathbb{F})$ являются смежные классы, которые будем обозначать их представителями.

Для удобства изложения через $\mathrm{PSL}'(2, \mathbb{F}_m)$ обозначим подгруппу группы $\mathrm{PGL}(2, \mathbb{F}_m)$, содержащую те и только те смежные классы, определители элементов которых являются квадратами. Группа $\mathrm{PSL}'(2, \mathbb{F}_m)$ изоморфна группе $\mathrm{PSL}(2, \mathbb{F}_m)$.

Перейдём к описанию метода построения рассматриваемых графов [8, 10, 14].

Пусть p и q — различные простые числа, такие, что $p \equiv 1 \pmod 4$ и $q \equiv 1 \pmod 4$. Пусть $i \in \mathbb{F}_q$ такое, что $i^2 + 1 = 0$.

Рассмотрим все наборы из четырёх элементов $(a_0, a_1, a_2, a_3) \in \mathbb{Z}^4$, для которых выполняются следующие условия:

1) a_0 — нечётное положительное число;
2) a_1, a_2, a_3 — чётные числа;
3) $a_0^2 + a_1^2 + a_2^2 + a_3^2 = p$.

Таких наборов ровно $p + 1$. Каждому такому набору $\alpha = (a_0, a_1, a_2, a_3)$ сопоставим $s_\alpha \in \mathrm{PGL}(2, \mathbb{F}_q)$:

$$s_\alpha = \begin{bmatrix} a_0 + ia_1 & a_2 + ia_3 \\ -a_2 + ia_3 & a_0 - ia_1 \end{bmatrix}.$$

Пусть множество S состоит из всех таких s_α. Его мощность равна $p + 1$.

Отметим, что если p является квадратичным вычетом по модулю q, то все s_α лежат в подгруппе $\mathrm{PSL}'(2, \mathbb{F}_q)$, изоморфной группе $\mathrm{PSL}(2, \mathbb{F}_q)$.

Семейство графов Любоцкого — Филипса — Сарнака $X^{p,q}$ определяется следующим образом:

$$X^{p,q} = \begin{cases} \mathfrak{G}(\mathrm{PGL}(2, \mathbb{F}_q), S), & \text{если } \left(\dfrac{p}{q}\right) = -1, \\ \mathfrak{G}(\mathrm{PSL}'(2, \mathbb{F}_q), S), & \text{если } \left(\dfrac{p}{q}\right) = 1, \end{cases}$$

где $\left(\dfrac{p}{q}\right)$ — символ Лежандра. Такие графы являются $(p + 1)$-регулярными. В них отсутствуют петли и кратные рёбра. Число вершин у этих графов равно

$$N = \begin{cases} q(q^2 - 1), & \text{если } \left(\dfrac{p}{q}\right) = -1, \\ \dfrac{q(q^2 - 1)}{2}, & \text{если } \left(\dfrac{p}{q}\right) = 1. \end{cases}$$

Для графов $X^{p,q}$ доказано [8], что они являются графами Рамануджана, для их диаметра выполняется неравенство

$$D(X^{p,q}) \leqslant 2(\log_p N + \log_p 2) + 1,$$

а обхват таких графов имеет следующую оценку:

$$\mathrm{girth}(X^{p,q}) \geqslant \begin{cases} 2(2\log_p q - \log_p 2), & \text{если } \left(\dfrac{p}{q}\right) = -1, \\ 2\log_p q, & \text{если } \left(\dfrac{p}{q}\right) = 1. \end{cases}$$

Если $\left(\dfrac{p}{q}\right) = -1$, то граф $X^{p,q}$ является двудольным, а если $\left(\dfrac{p}{q}\right) = 1$ — недвудольным. К сожалению, недвудольных графов небольшой степени с небольшим числом вершин из этого семейства очень мало. Так, если рассматривать только графы степени $d \leqslant 20$ с числом вершин $N \leqslant 20000$, то таких графов всего четыре (их параметры — числа p и q, степень d и число вершин N — приведены в табл. 1). Такая особенность делает эти графы непригодными для использования в рассматриваемых целях.

Таблица 1

p	q	d	N
5	29	6	12180
13	17	14	2448
13	29	14	12180
17	13	18	1092

5. Семейство графов $Y^{p,q}$ Любоцкого — Филипса — Сарнака

Рассмотрим другое семейство графов Рамануджана — семейство $Y^{p,q}$, также предложенное Любоцким, Филипсом и Сарнаком [10]. Графы, принадлежащие этому семейству, являются недвудольными. Опишем метод построения этих графов.

Выберем простые числа p и q, для которых выполняются следующие условия:

$$p \equiv 1 \,(\mathrm{mod}\, 4),\ q \equiv 1 \,(\mathrm{mod}\, 4),\ p \neq q,\ \left(\frac{p}{q}\right) = 1.$$

Построим граф $Y^{p,q}$. Множеством V его вершин является проективная прямая над конечным полем $\mathbb{F}_q$, т. е. $V = \mathbb{F}_q \cup \{\infty\}$. Каждая вершина $u \in V$ соединена ребром с вершиной v, определяемой по формулам

$$v = \begin{cases} \dfrac{(a_0 + ia_1)u + (a_2 + ia_3)}{(-a_2 + ia_3)u + (a_0 - ia_1)}, & \text{если } (a_2 - ia_3)u \neq a_0 - ia_1 \text{ и } u \neq \infty, \\ \infty, & \text{если } (a_2 - ia_3)u = a_0 - ia_1 \text{ и } u \neq \infty, \\ \dfrac{ia_1 + a_0}{ia_3 - a_2}, & \text{если } ia_3 \neq a_2 \text{ и } u = \infty, \\ \infty, & \text{если } ia_3 = a_2 \text{ и } u = \infty, \end{cases}$$

для каждой четвёрки $(a_0, a_1, a_2, a_3) \in \mathbb{Z}^4$, такой, что выполняются следующие условия:

1) a_0 — нечётное положительное число;
2) a_1, a_2, a_3 — чётные числа;
3) $a_0^2 + a_1^2 + a_2^2 + a_3^2 = p$.

Здесь $i \in \mathbb{F}_q$ такое, что $i^2 + 1 = 0$. Граф имеет степень, равную количеству таких четвёрок $(p + 1)$. В построенном графе могут присутствовать кратные рёбра и петли. Для графов $Y^{p,q}$ доказано [10], что они являются графами Рамануджана.

Различных графов из семейства $Y^{p,q}$ с числом вершин от 100 до 10000 для $p = 5$ (т. е. 6-регулярных) насчитывается 298, а для $p = 13$ (т. е. 14-регулярных) — 301. При этом они достаточно равномерно распределены в указанном диапазоне.

В целях проведения вычислительных экспериментов разработано программное обеспечение на языке Python. С помощью него построено 448 таких графов степени 6 с числом вершин от 30 до 15902. Их параметры λ приведены на рис. 1, а диаметры — на рис. 2. Количество петель у каждого из построенных графов равно 6, а количество пар кратных рёбер — либо 0, либо 12. Заметим, что существенно сократить число петель и кратных рёбер позволяет описанный в п. 8 способ коррекции.

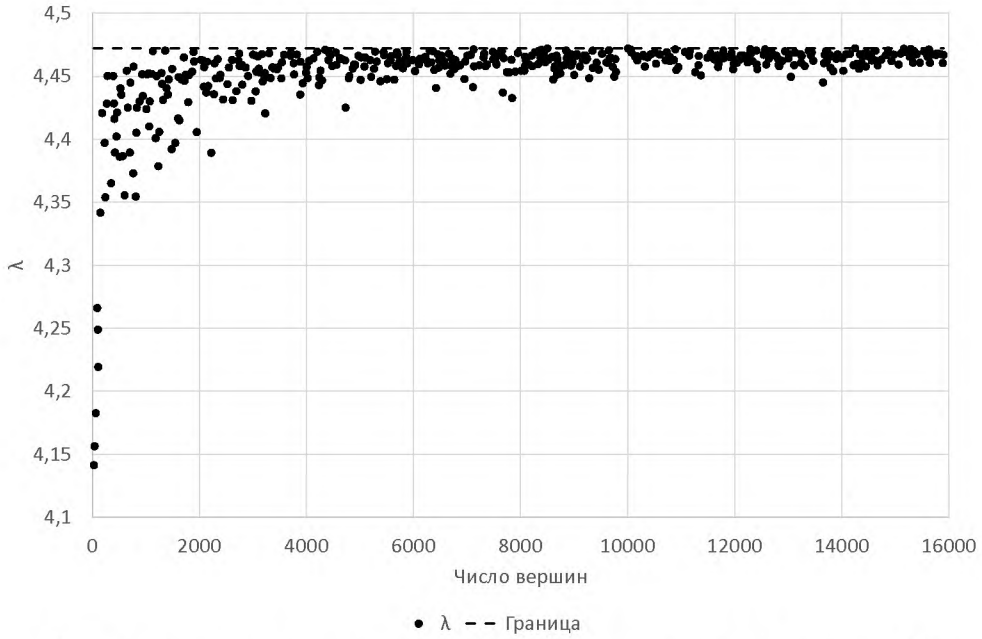

Рис. 1. Значения параметра λ графов $Y^{p,q}$ степени 6 и граница (1)

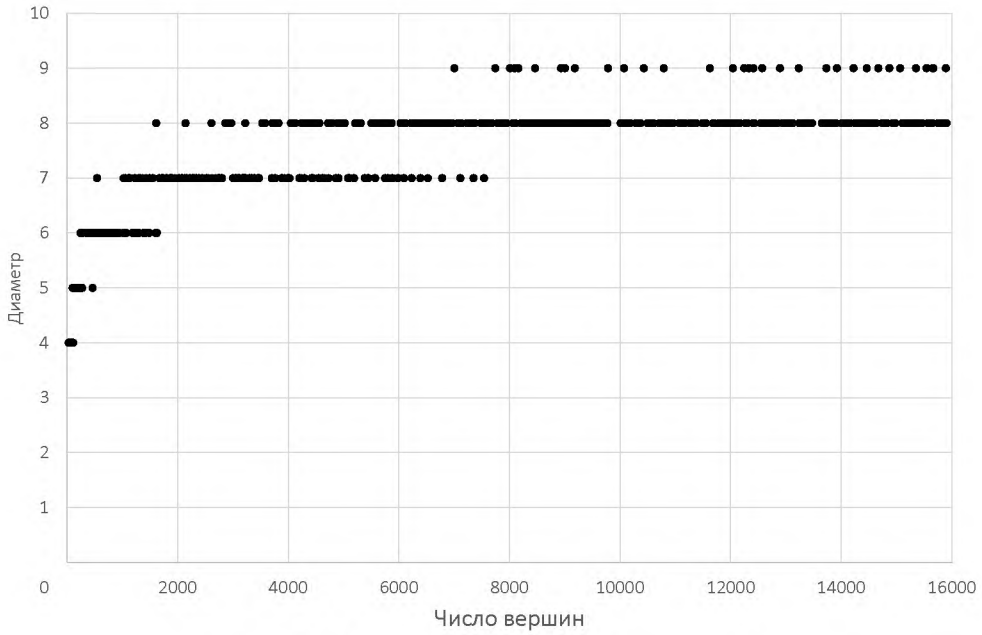

Рис. 2. Диаметры графов $Y^{p,q}$ степени 6

6. Семейство графов Моргенштерна

Другое семейство графов Рамануджана предложено Моргенштерном в работе [20]. Опишем метод построения таких графов [20 – 22].

Графы Моргенштерна представляют собой графы Кэли для группы PSL′ или PGL над полем Галуа по некоторому множеству.

Сначала рассмотрим случай поля чётной характеристики. В этом случае граф Моргенштерна недвудольный. Пусть $q = 2^\tau$ (для некоторого τ). Выберем такое $\varepsilon \in \mathbb{F}_q$, что

многочлен $f(x) = x^2 + x + \varepsilon$ неприводим над $\mathbb{F}_q$, и неприводимый многочлен $P_n(X) \in \in \mathbb{F}_q[X]$ степени n, где n — чётное. Будем использовать поле $\mathbb{F}_{q^n} = \mathbb{F}_q[X]/(P_n(X))$.

Пусть $i \in \mathbb{F}_{q^n}$ — корень многочлена $f(x)$ и $S_{\text{Morg}} = \{s_0, s_1, \ldots, s_q\}$, где

$$s_j = \begin{bmatrix} 1 & a_j + b_j i \\ (a_j + b_j i + b_j)X & 1 \end{bmatrix}.$$

Здесь a_j, b_j — все лежащие в поле $\mathbb{F}_q$ решения уравнения

$$a_j^2 + a_j b_j + b_j^2 \varepsilon = 1.$$

В случае поля чётной характеристики граф Моргенштерна представляет собой граф Кэли

$$G^{q,n}_{\text{Morg}} = \mathfrak{G}(\mathrm{PSL}'(2, \mathbb{F}_{q^n}), S_{\text{Morg}}).$$

Рассмотрим теперь случай поля нечетной характеристики. Пусть p — нечётное простое, $q = p^\tau$ (для некоторого τ). Выберем $\varepsilon \in \mathbb{F}_q$, такое, что оно не является квадратом в поле $\mathbb{F}_q$; неприводимый многочлен $P_n(X) \in \mathbb{F}_q[X]$ степени n, где n — чётное; $i \in \mathbb{F}_{q^n}$, такое, что $i^2 = \varepsilon$. Будем использовать поле $\mathbb{F}_{q^n} = \mathbb{F}_q[X]/(P_n(X))$. Определим множество $S'_{\text{Morg}} = \{s'_0, s'_1, \ldots, s'_q\}$, где

$$s'_j = \begin{bmatrix} 1 & a_j - b_j i \\ (a_j + b_j i)(X - 1) & 1 \end{bmatrix}.$$

Здесь a_j, b_j — все лежащие в поле $\mathbb{F}_q$ решения уравнения

$$b_j^2 \varepsilon - a_j^2 = 1.$$

В случае поля нечётной характеристики граф Моргенштерна представляет собой граф Кэли

$$G^{q,n}_{\text{Morg}} = \begin{cases} \mathfrak{G}(\mathrm{PSL}'(2, \mathbb{F}_{q^n}), S'_{\text{Morg}}), & \text{если } \left(\dfrac{X}{P_n(X)}\right) = 1, \\ \mathfrak{G}(\mathrm{PGL}(2, \mathbb{F}_{q^n}), S'_{\text{Morg}}), & \text{если } \left(\dfrac{X}{P_n(X)}\right) = -1, \end{cases}$$

где $\left(\dfrac{a}{P_n(X)}\right)$ — символ Лежандра в поле $\mathbb{F}_{q^n}$.

Графы Моргенштерна являются $(q+1)$-регулярными графами Рамануджана без петель и кратных рёбер с числом вершин

$$N = \begin{cases} q^n(q^{2n} - 1) & \text{для группы } \mathrm{PGL}(2, \mathbb{F}_{q^n}), \\ q^n(q^{2n} - 1)/2 & \text{для группы } \mathrm{PSL}'(2, \mathbb{F}_{q^n}). \end{cases}$$

Такой граф является недвудольным при использовании группы $\mathrm{PSL}'(2, \mathbb{F}_{q^n})$ и двудольным при использовании группы $\mathrm{PGL}(2, \mathbb{F}_{q^n})$. Для таких графов доказано [20], что они имеют малый диаметр и большой обхват:

$$D(G^{q,n}_{\text{Morg}}) \leqslant 2\log_q(N) + 2,$$

$$\mathrm{girth}(G^{q,n}_{\text{Morg}}) \geqslant \begin{cases} \dfrac{4}{3}\log_q(N) & \text{для группы } \mathrm{PGL}(2, \mathbb{F}_{q^n}), \\ \dfrac{2}{3}\log_q(N) + 1 & \text{для группы } \mathrm{PSL}'(2, \mathbb{F}_{q^n}). \end{cases}$$

К сожалению, недвудольных графов Моргенштерна малых степеней с небольшим числом вершин очень мало. Параметры таких графов приведены в табл. 2, из которой видно, что для обсуждаемых целей это семейство графов не подходит.

Таблица 2

Параметры недвудольных графов Моргенштерна малых степеней (для небольших значений параметра n)

Параметры				Число вершин N графа Моргенштерна $G^{q,n}_{\mathrm{Morg}}$				
d	p	τ	q	$n=2$	$n=4$	$n=6$	$n=8$	$n=10$
4	3	1	3	360	265680	$1{,}94\cdot10^{8}$	$1{,}41\cdot10^{11}$	$1{,}03\cdot10^{14}$
5	2	2	4	2040	8388480	$3{,}44\cdot10^{10}$	$1{,}41\cdot10^{14}$	$5{,}76\cdot10^{17}$
6	5	1	5	7800	122070000	$1{,}91\cdot10^{12}$	$2{,}98\cdot10^{16}$	$4{,}66\cdot10^{20}$
8	7	1	7	58800	6920642400	$8{,}14\cdot10^{14}$	$9{,}58\cdot10^{19}$	$1{,}13\cdot10^{25}$
9	2	3	8	131040	34359736320	$9{,}01\cdot10^{15}$	$2{,}36\cdot10^{21}$	$6{,}19\cdot10^{26}$
10	3	2	9	265680	$1{,}41\cdot10^{11}$	$7{,}5\cdot10^{16}$	$3{,}99\cdot10^{22}$	$2{,}12\cdot10^{28}$

7. Семейство графов Пайзера

Опишем ещё одно семейство графов Рамануджана — графы Пайзера [21, 23, 24]. Они основаны на эллиптических кривых. Эллиптическим кривым и их применению в криптографии посвящено большое количество работ, например [25 – 28].

Напомним, что эллиптической кривой над полем $\mathbb{F}$ называется гладкая (т. е. не имеющая особых точек) алгебраическая кривая над этим полем, задаваемая уравнением

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \tag{2}$$

вместе с точкой в бесконечности O. Если эллиптическая кривая определена над полем, характеристика которого отлична от 2 и 3, то линейным преобразованием координат её уравнение сводится к форме Вейерштрасса

$$y^2 = x^3 + ax + b. \tag{3}$$

Пусть p и l — простые числа, причём $p \equiv 1 \pmod{12}$, а l является квадратичным вычетом по модулю p. Множеством вершин графа Пайзера является множество классов изоморфизма суперсингулярных эллиптических кривых над полем $\mathbb{F}_{p^2}$. Вершины такого графа удобно задавать с помощью j-инвариантов соответствующих эллиптических кривых. Будем писать «вершина j», имея в виду вершину, соответствующую классу изоморфизма эллиптических кривых с j-инвариантом j. Представителя такого класса будем обозначать E_j. Для $j \notin \{0, 1728\}$ эллиптическую кривую E_j над полем характеристики, отличной от 2 и 3, можно задать, например, уравнением вида

$$y^2 = x^3 - \frac{3j}{j-1728}x + \frac{2j}{j-1728}.$$

Вершины j_1 и j_2 являются смежными, если существует l-изогения между E_{j_1} и E_{j_2}. Более подробно построение рёбер графа описано далее. Напомним, что если E' и E'' — эллиптические кривые, то изогенией из E' в E'' называется морфизм $\varphi : E' \to E''$, для которого $\varphi(O) = O$. Изогения является гомоморфизмом групп точек эллиптических кривых. Степенью изогении называется мощность её ядра. Изогению степени l часто называют l-изогенией.

Полученный граф Пайзера, который будем обозначать $\Pi_{l,p}$, имеет $N = \lfloor p/12 \rfloor$ вершин. Он является недвудольным $(l+1)$-регулярным неориентированным графом и графом Рамануджана. Для его диаметра справедливо неравенство

$$D(\Pi_{l,p}) \leqslant 2\log_l N + 2,$$

а для обхвата — неравенство

$$\operatorname{girth}(\Pi_{l,p}) \geqslant \lceil \log_l p - \log_l 4 \rceil.$$

Важным является понятие группы l-кручения эллиптической кривой. Группа l-кручения $E[l]$ эллиптической кривой E, определённой над полем $\mathbb{F}$, представляет собой множество точек, которое задается следующим образом:

$$E[l] = \{Q \in E(\overline{\mathbb{F}}) : lQ = O\}, \tag{4}$$

где $E(\overline{\mathbb{F}})$ — группа точек эллиптической кривой E с координатами из алгебраического замыкания поля $\mathbb{F}$. Известно, что если характеристика поля $\mathbb{F}$ не делит l, то имеет место изоморфизм $E[l] \cong \mathbb{Z}_l \oplus \mathbb{Z}_l$. В этом случае $|E[l]| = l^2$.

Нас будет интересовать случай, когда число l — простое. Тогда группа l-кручения имеет $l + 1$ подгруппу порядка l, а x-координаты точек, входящих в неё, являются корнями некоторого специального полинома ψ_l. Для эллиптических кривых в форме Вейерштрасса (над полями характеристики, отличной от 2 и 3) этот полином вычисляется в соответствии с рекуррентными формулами

$$\psi_{2m+1} = \psi_{m+2}\psi_m^3 - \psi_{m-1}\psi_{m+1}^3 \quad \text{для } m \geqslant 2; \tag{5}$$

$$\psi_{2m} = \frac{\psi_m}{2y}(\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2) \quad \text{для } m \geqslant 3, \tag{6}$$

при этом $\psi_1 = 1$; $\psi_2 = 2y$; $\psi_3 = 3x^4 + 6ax^2 + 12bx - a^2$; $\psi_4 = 4y(x^6 + 5ax^4 + 20bx^3 - 5a^2x^2 - 4abx - 8b^2 - a^3)$.

Рёбра графа Пайзера соответствуют изогениям. Для построения всех рёбер, инцидентных вершине z, следует найти j-инварианты образов всех l-изогений из эллиптической кривой E_z. Для построения изогении нужно найти её ядро. Ядро l-изогении является подгруппой порядка l группы l-кручения эллиптической кривой. Таким образом, каждой подгруппе порядка l группы $E_z[l]$ соответствует инцидентное вершине z ребро.

Пусть для эллиптической кривой вида (2) изогения задана ядром C. Образ изогении может быть найден с помощью формул Велу, предложенных в [29]. Приведём их (формулы приводятся на основе работы [30]).

Для точки $P = (x_P, y_P) \in C$, не являющейся точкой в бесконечности, определим следующие параметры:

$$g_P^x = 3x_P^2 + 2a_2x_P - a_1y_P + a_4,$$
$$g_P^y = -2y_P - a_3 - a_1x_P,$$

$$r_P = \begin{cases} g_P^x, & \text{если } 2P = O, \\ 2g_P^x - a_1g_P^y, & \text{если } 2P \neq O, \end{cases}$$
$$u_P = (g_P^y)^2.$$

Пусть $C_2 \subseteq C$ — множество точек порядка 2, содержащихся в множестве C. Выберем такое множество $R \subset C$, что C является объединением четырёх попарно непересекающихся множеств:

$$C = \{O\} \cup C_2 \cup R \cup (-R),$$

где $(-R) = \{-Q : Q \in R\}$. Вычислим параметры r и w следующим образом:

$$r = \sum_{Q \in R \cup C_2} r_Q; \quad w = \sum_{Q \in R \cup C_2} (x_Q r_Q + u_Q).$$

Тогда образом изогении будет являться эллиптическая кривая

$$y^2 + a'_1 xy + a'_3 y = x^3 + a'_2 x^2 + a'_4 x + a'_6,$$

где $a'_1 = a_1$; $a'_2 = a_2$; $a'_3 = a_3$; $a'_4 = a_4 - 5r$; $a'_6 = a_6 - (a_1^2 + 4a_2)r - 7w$. Сама изогения задаётся формулами

$$x' = x + \sum_{Q \in R \cup C_2} \left(\frac{r_Q}{x - x_Q} + \frac{u_Q}{(x - x_Q)^2} \right),$$

$$y' = y - \sum_{Q \in R \cup C_2} \left(u_Q \frac{2y + a_1 x + a_3}{(x - x_Q)^3} + r_Q \frac{y - y_Q + a_1(x - x_Q)}{(x - x_Q)^2} + \frac{a_1 u_Q - g_Q^x g_Q^y}{(x - x_Q)^2} \right).$$

Чтобы узнать, какой вершине графа Пайзера соответствует образ изогении (ребро, соответствующее изогении, инцидентно этой вершине), остаётся вычислить его j-инвариант.

Для эллиптических кривых в форме Вейерштрасса (3) вышеприведенные формулы Велу упрощаются:

$$g_P^x = 3x_P^2 + a,$$

$$g_P^y = -2y_P,$$

$$r_P = \begin{cases} g_P^x, & \text{если } 2P = O, \\ 2g_P^x, & \text{если } 2P \neq O, \end{cases}$$

$$u_P = (g_P^y)^2,$$

$$r = \sum_{Q \in R \cup C_2} r_Q, \quad w = \sum_{Q \in R \cup C_2} (x_Q r_Q + u_Q).$$

Образом изогении в этом случае является эллиптическая кривая, заданная уравнением

$$y^2 = x^3 + (a - 5r)x + (b - 7w).$$

Для построения всех образов изогений для данной эллиптической кривой можно предложить следующую методику:

1) Найти полином ψ_l по формулам (5), (6).
2) Найти корни полинома ψ_l. Множество точек, соответствующих этим корням, вместе с точкой в бесконечности составляет группу l-кручения эллиптической кривой.
3) Найти все подгруппы порядка l группы l-кручения. Их число равно $l + 1$.
4) Каждая подгруппа порядка l группы l-кручения образует ядро одной из l-изогений. Найти образы всех l-изогений с помощью формул Велу.

Итак, построение графа Пайзера $\Pi_{l,p}$ происходит следующим образом:

1) выбирается j-инвариант, соответствующий суперсингулярной эллиптической кривой над полем $\mathbb{F}_{p^2}$;
2) производится обход графа в ширину с построением образов l-изогений и вычислением их j-инвариантов. Получившийся граф является графом Пайзера $\Pi_{l,p}$.

Графов Пайзера существует достаточно много. Так, число графов Пайзера степени 6 с числом вершин от 100 до 10000 составляет 1360. Данные по количеству графов Пайзера различных степеней с числом вершин в этом диапазоне приведены в табл. 3.

Таблица 3

Степень	Параметр l	Число графов Пайзера
4	3	2749
6	5	1360
8	7	1361
12	11	1377
14	13	1352
18	17	1360
20	19	1351

Некоторые графы Пайзера (степеней 4, 6, 8) были явно построены с целью проведения вычислительных экспериментов. Всего построено 56 графов степени 6, 57 графов степени 4 и 21 граф степени 8. Программа построения графов разработана автором для системы компьютерной алгебры Magma [31, 32]. Параметры λ построенных графов приведены на рис. 3–5, а значения их диаметров — на рис. 6.

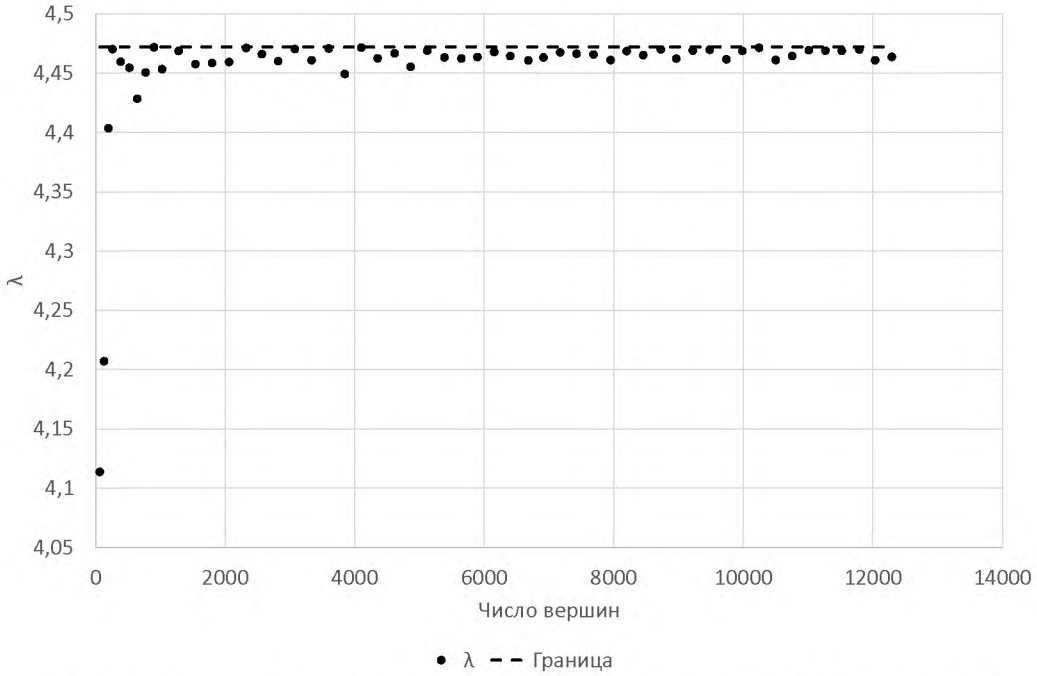

Рис. 3. Значения параметра λ графов Пайзера степени 6 и граница (1)

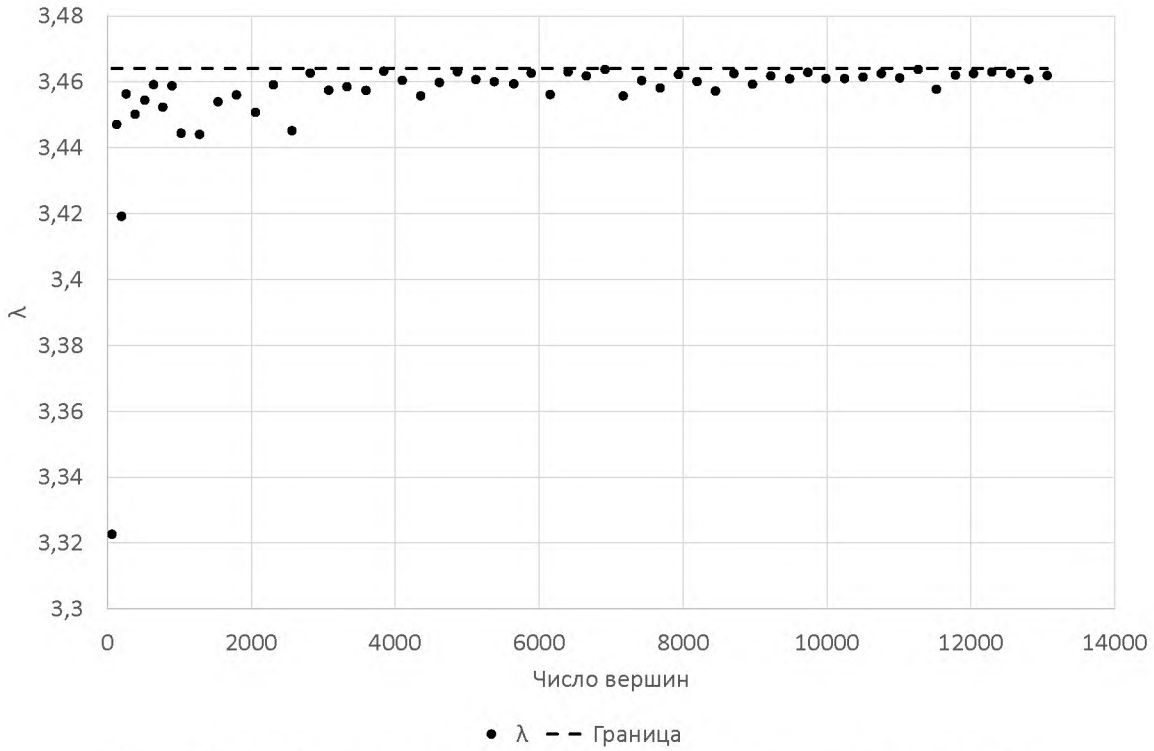

Рис. 4. Значения параметра λ графов Пайзера степени 4 и граница (1)

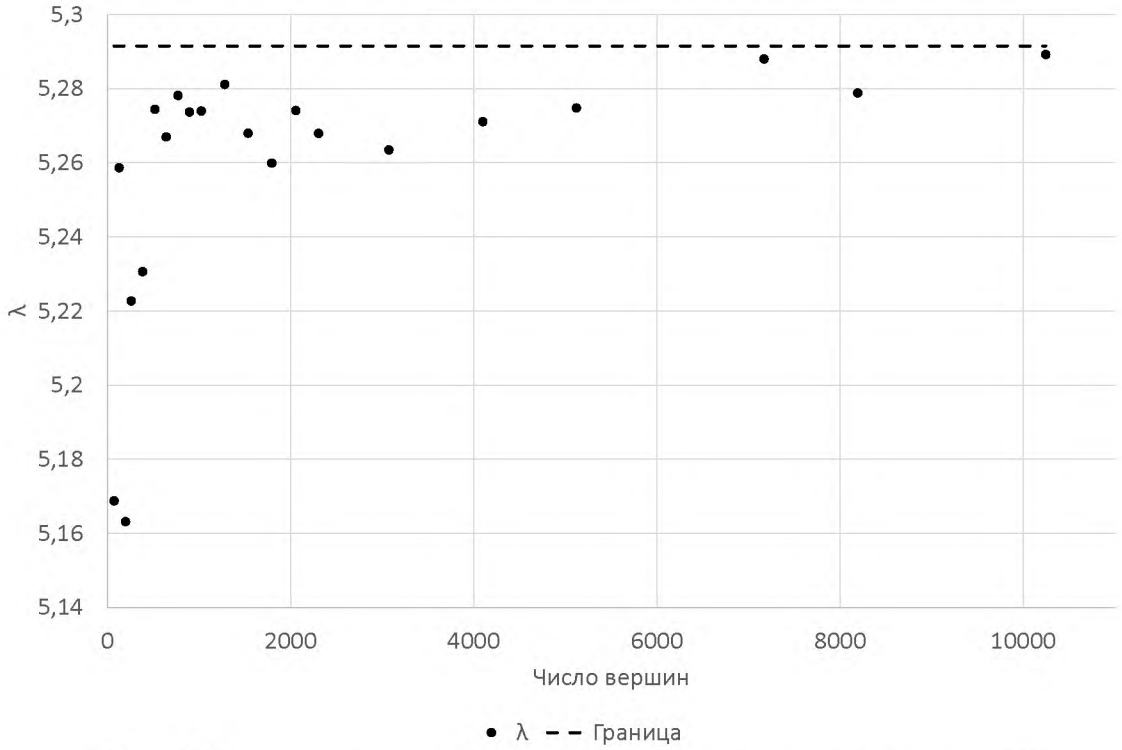

Рис. 5. Значения параметра λ графов Пайзера степени 8 и граница (1)

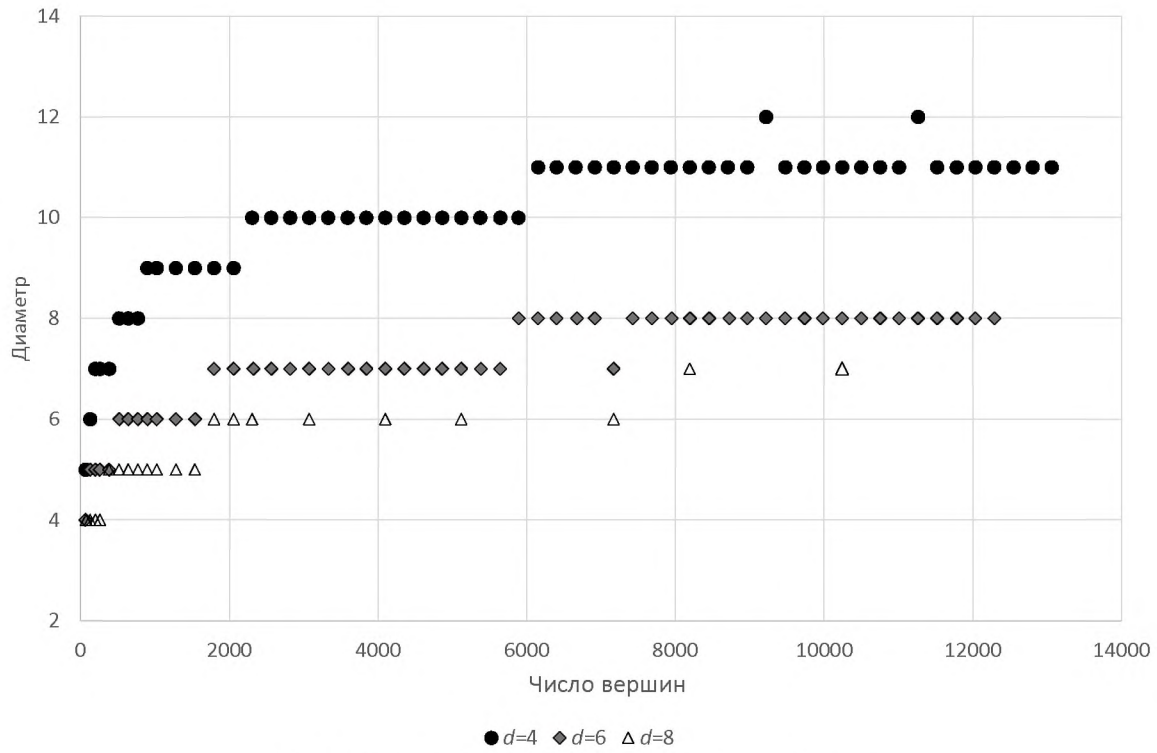

Рис. 6. Диаметры графов Пайзера степени d

8. Удаление петель и кратных рёбер

Наличие в графе петель и кратных рёбер может ухудшить криптографические свойства обобщённого клеточного автомата, поэтому необходимо уменьшить их количество. Сделать это нужно так, чтобы граф оставался регулярным. Приведём простой алгоритм, вариант которого использовался автором ранее [33].

Обработаем кратные рёбра следующим образом. Рассмотрим две пары кратных рёбер: пару ребер, соединяющих вершины u_1, v_1, и пару ребер, соединяющих вершины u_2, v_2 (здесь $u_1, v_1, u_2, v_2 \in V$ — попарно различные вершины графа, V — множество вершин графа). Удалим одно ребро $\{u_1, v_1\}$ и одно ребро $\{u_2, v_2\}$, после чего добавим рёбра $\{u_1, u_2\}$ и $\{v_1, v_2\}$. Обработаем так все пары кратных ребер в графе (если их количество нечётное, то все, кроме одной).

Петли обработаем следующим образом. Пусть в графе имеются петли $\{u_1, u_1\}$, $\{u_2, u_2\}$, $\ldots$, $\{u_t, u_t\}$, где $u_1, \ldots, u_t \in V$. Удалим эти петли из графа, после чего добавим рёбра $\{u_1, u_2\}, \{u_2, u_3\}, \ldots, \{u_{t-1}, u_t\}, \{u_t, u_1\}$ (заметим, что если при этом появятся кратные рёбра, то порядок вершин последовательности $u_1, u_2, \ldots, u_t$ следует, если возможно, изменить так, чтобы кратных рёбер не появлялось).

Если после выполнения этих процедур петли и кратные рёбра остаются, можно произвести следующие действия. Пусть для некоторых попарно различных вершин $u, v, w \in V$ имеется пара кратных рёбер, соединяющих вершины u, v, и петля $\{w, w\}$. Тогда можно удалить одно ребро из этой пары и петлю, после чего добавить рёбра $\{u, w\}$ и $\{v, w\}$.

Приведённый алгоритм позволяет существенно уменьшить количество кратных рёбер и петель, не влияя на регулярность графа и не приводя к увеличению его диаметра.

Для большинства сгенерированных в рамках настоящей работы графов его применение не привело к существенному изменению параметра λ.

Заключение

Для применения в качестве графов обобщённых клеточных автоматов графы Моргенштерна и графы $X^{p,q}$, очевидно, не подходят, поскольку таких графов небольшой степени с небольшим числом вершин существует очень мало. Вместе с тем для рассматриваемых целей подходят графы $Y^{p,q}$ и графы Пайзера, так как они удовлетворяют всем необходимым требованиям. Следует заметить, что число петель и кратных рёбер в графе может быть при необходимости сведено к минимуму способом, изложенным в п. 8.

ЛИТЕРАТУРА

1. *Ключарёв П. Г.* Блочные шифры, основанные на обобщённых клеточных автоматах // Наука и образование. МГТУ им. Н. Э. Баумана. Электрон. журн. 2012. № 12. С. 361–374.
2. *Ключарёв П. Г.* Криптографические хэш-функции, основанные на обобщённых клеточных автоматах // Наука и образование. МГТУ им. Н. Э. Баумана. Электрон. журн. 2013. № 1. С. 161–172.
3. *Тоффоли Т., Марголус Н.* Машины клеточных автоматов: пер. с англ. М.: Мир, 1991. 280 с.
4. *Kauffman S. A.* Metabolic stability and epigenesis in randomly constructed genetic net // J. Theor. Biol. 1969. No. 22. P. 437–467.
5. *Сухинин Б. М.* Разработка генераторов псевдослучайных двоичных последовательностей на основе клеточных автоматов // Наука и образование. МГТУ им. Н. Э. Баумана. Электрон. журн. 2010. № 9. `http://engineering-science.ru/doc/159714.html`
6. *Davidoff G., Sarnak P., and Valette A.* Elementary Number Theory, Group Theory and Ramanujan Graphs. Cambridge: Cambridge University Press, 2003. V. 55. 144 p.
7. *Hoory S., Linial N., and Wigderson A.* Expander graphs and their applications // Bull. Amer. Math. Soc. 2006. V. 43. No. 4. P. 439–562.
8. *Lubotzky A., Phillips R., and Sarnak P.* Ramanujan graphs // Combinatorica. 1988. V. 8. No. 3. P. 261–277.
9. *Krebs M. and Shaheen A.* Expander Families and Cayley Graphs: A Beginner's Guide. Oxford: Oxford University Press, 2011. 258 p.
10. *Sarnak P.* Some Applications of Modular Forms. Cambridge: Cambridge University Press, 1990. V. 99. 111 p.
11. *Chung F.* Spectral Graph Theory. Amer. Math. Soc., 1997. 207 p.
12. *Sarnak P.* What is ... an expander? // Notices Amer. Math. Soc. 2004. V. 51. P. 762–770.
13. *Lubotzky A.* Discrete Groups, Expanding Graphs and Invariant Measures. Springer Science & Business Media, 2010. 196 p.
14. *Lubotzky A., Phillips R., and Sarnak P.* Explicit expanders and the Ramanujan conjectures // Proc. 18th Ann. ACM Symp. on Theory of Computing. ACM, 1986. P. 240–246.
15. *Grove L.* Classical Groups and Geometric Algebra. Fields Institute Communications. Amer. Math. Soc., 2002. 169 p.
16. *Humphreys J.* A Course in Group Theory. Oxford Graduate Texts in Mathematics. Oxford: Oxford University Press, 1996. 279 p.
17. *James G. and Liebeck M.* Representations and Characters of Groups. Cambridge Mathematical Textbooks. Cambridge: Cambridge University Press, 2001. 458 p.
18. *Lanski C.* Concepts in Abstract Algebra. Amer. Math. Soc., 2005. 545 p.

19. *Каргаполов М. И., Мерзляков Ю. И.* Основы теории групп. М.: Наука, Физматлит, 1996. 287 с.
20. *Morgenstern M.* Existence and explicit constructions of $q + 1$ regular Ramanujan graphs for every prime power q // J. Combinatorial Theory. Ser. B. 1994. V. 62. No. 1. P. 44–62.
21. *Petit C.* On Graph-Based Cryptographic Hash Functions. PhD Thesis. Catholic University of Louvain, 2009. 286 p. `www0.cs.ucl.ac.uk/staff/c.petit/files/thesis.pdf`
22. *Nikkel T.* Ramanujan Graphs. Master's Thesis. University of Manitoba, 2007. 112 p. `http://mspace.lib.umanitoba.ca/bitstream/handle/1993/9146/thesis.pdf`
23. *Pizer A. K.* Ramanujan graphs and Hecke operators // Bull. Amer. Math. Soc. 1990. V. 23. No. 1. P. 127–137.
24. *Charles D. X., Lauter K. E., and Goren E. Z.* Cryptographic hash functions from expander graphs // J. Cryptology. 2009. V. 22. No. 1. P. 93–113.
25. *Silverman J.* Advanced Topics in the Arithmetic of Elliptic Curves. Graduate Texts in Mathematics. N.Y.: Springer, 2013. 528 p.
26. *Blake I., Seroussi G., and Smart N.* Elliptic Curves in Cryptography. Lecture Note Series. Cambridge: Cambridge University Press, 1999. 204 p.
27. *Silverman J.* The Arithmetic of Elliptic Curves. Graduate Texts in Mathematics. N.Y.: Springer, 2009. 402 p.
28. *Washington L.* Elliptic Curves: Number Theory and Cryptography. 2nd Ed. Discrete Mathematics and its Applications. Boca Raton: CRC Press, 2008. 536 p.
29. *Vélu J.* Isogénies entre courbes elliptiques // CR Acad. Sci. Paris Sér. AB. 1971. V. 273. P. A238–A241.
30. *Shumow D.* Isogenies of Elliptic Curves: A Computational Approach. Master's Thesis. University of Washington, 2009. 78 p. `https://arxiv.org/abs/0910.5370`
31. *Bosma W., Cannon J., and Playoust C.* The Magma algebra system. I. The user language // J. Symbolic Comput. 1997. V. 24. No. 3–4. P. 235–265.
32. Handbook of Magma Functions. Edition 2.20 / eds. W. Bosma, J. Cannon, C. Fieker, and A. Steel. 2014. 5583 p. `https://www.math.uzh.ch/sepp/magma-2.19.8-cr/Handbook.pdf`
33. *Ключарёв П. Г.* Построение псевдослучайных функций на основе обобщенных клеточных автоматов // Наука и образование. МГТУ им. Н. Э. Баумана. Электрон. журн. 2012. № 10. С. 263–274.

REFERENCES

1. *Klyucharev P. G.* Blochnye shifry, osnovannye na obobshchyonnyh kletochnyh avtomatah [Block ciphers based on generalized cellular automata]. Science and Education of the Bauman MSTU, 2012, no. 2, pp. 361–374. (in Russian)
2. *Klyucharev P. G.* Kriptograficheskie hesh-funkcii, osnovannye na obobshchyonnyh kletochnyh avtomatah [Cryptographic hash functions based on generalized cellular automata]. Science and Education of the Bauman MSTU, 2013, no. 1, pp. 161–172. (in Russian)
3. *Toffoli T. and Margolus N.* Cellular Automata Machines. MIT Press, 1987. 276 p.
4. *Kauffman S. A.* Metabolic stability and epigenesis in randomly constructed genetic net. J. Theor. Biol., 1969, no. 22, pp. 437–467.
5. *Suhinin B. M.* Razrabotka generatorov psevdosluchajnyh dvoichnyh posledovatelnostej na osnove kletochnyh avtomatov [Construction of pseudorandom binary sequence generators based on cellular automata]. Science and Education of the Bauman MSTU, 2010, no. 9. `http://engineering-science.ru/doc/159714.html`. (in Russian)
6. *Davidoff G., Sarnak P., and Valette A.* Elementary Number Theory, Group Theory and Ramanujan Graphs. Cambridge, Cambridge University Press, 2003, vol. 55. 144 p.

7. *Hoory S., Linial N., and Wigderson A.* Expander graphs and their applications. Bull. Amer. Math. Soc., 2006, vol. 43, no. 4. pp. 439–562.
8. *Lubotzky A., Phillips R., and Sarnak P.* Ramanujan graphs. Combinatorica, 1988, vol. 8, no. 3, pp. 261–277.
9. *Krebs M. and Shaheen A.* Expander Families and Cayley Graphs: A Beginner's Guide. Oxford, Oxford University Press, 2011. 258 p.
10. *Sarnak P.* Some Applications of Modular Forms. Cambridge, Cambridge University Press, 1990, vol. 99. 111 p.
11. *Chung F.* Spectral Graph Theory. Amer. Math. Soc., 1997, 207 p.
12. *Sarnak P.* What is ... an expander? Notices Amer. Math. Soc., 2004, vol. 51, pp. 762–770.
13. *Lubotzky A.* Discrete Groups, Expanding Graphs and Invariant Measures. Springer Science & Business Media, 2010. 196 p.
14. *Lubotzky A., Phillips R., and Sarnak P.* Explicit expanders and the Ramanujan conjectures. Proc. 18th Ann. ACM Symp. on Theory of Computing, ACM, 1986, pp. 240–246.
15. *Grove L.* Classical Groups and Geometric Algebra. Fields Institute Communications. Amer. Math. Soc., 2002. 169 p.
16. *Humphreys J.* A Course in Group Theory. Oxford Graduate Texts in Mathematics. Oxford, Oxford University Press, 1996. 279 p.
17. *James G. and Liebeck M.* Representations and Characters of Groups. Cambridge Mathematical Textbooks. Cambridge, Cambridge University Press, 2001. 458 p.
18. *Lanski C.* Concepts in Abstract Algebra. Amer. Math. Soc., 2005. 545 p.
19. *Kargapolov M. I. and Merzlyakov Yu. I.* Osnovy Teorii Grupp [Foundations of Group Theory]. Moscow, Nauka, Fizmatlit Publ., 1996. 287 p. (in Russian)
20. *Morgenstern M.* Existence and explicit constructions of $q + 1$ regular Ramanujan graphs for every prime power q. J. Combinatorial Theory, Ser. B, 1994, vol. 62, no. 1, pp. 44–62.
21. *Petit C.* On Graph-Based Cryptographic Hash Functions. PhD Thesis, Catholic University of Louvain, 2009. 286 p. `www0.cs.ucl.ac.uk/staff/c.petit/files/thesis.pdf`
22. *Nikkel T.* Ramanujan Graphs. Master's Thesis, University of Manitoba, 2007. 112 p. `http://mspace.lib.umanitoba.ca/bitstream/handle/1993/9146/thesis.pdf`
23. *Pizer A. K.* Ramanujan graphs and Hecke operators. Bull. Amer. Math. Soc., 1990, vol. 23, no. 1, pp. 127–137.
24. *Charles D. X., Lauter K. E., and Goren E. Z.* Cryptographic hash functions from expander graphs. J. Cryptology, 2009, vol. 22, no. 1, pp. 93–113.
25. *Silverman J.* Advanced Topics in the Arithmetic of Elliptic Curves. Graduate Texts in Mathematics. N.Y., Springer, 2013. 528 p.
26. *Blake I., Seroussi G., and Smart N.* Elliptic Curves in Cryptography. Lecture Note Series. Cambridge, Cambridge University Press, 1999. 204 p.
27. *Silverman J.* The Arithmetic of Elliptic Curves. Graduate Texts in Mathematics. N.Y., Springer, 2009. 402 p.
28. *Washington L.* Elliptic Curves: Number Theory and Cryptography, 2nd Edition. Discrete Mathematics and Its Applications. Boca Raton, CRC Press, 2008. 536 p.
29. *Vélu J.* Isogénies entre courbes elliptiques. CR Acad. Sci. Paris Sér. AB, 1971, vol. 273, pp. A238–A241.
30. *Shumow D.* Isogenies of Elliptic Curves: A Computational Approach. Master's Thesis, University of Washington, 2009. 78 p. `https://arxiv.org/abs/0910.5370`
31. *Bosma W., Cannon J., and Playoust C.* The Magma algebra system. I. The user language. J. Symbolic Comput., 1997, vol. 24, no. 3–4, pp. 235–265.

32. Handbook of Magma Functions. Edition 2.20 / eds. W. Bosma, J. Cannon, C. Fieker, and A. Steel. 2014. 5583 p. `https://www.math.uzh.ch/sepp/magma-2.19.8-cr/Handbook.pdf`
33. *Klyucharev P. G.* Postroenie psevdosluchajnyh funkcij na osnove obobshchennyh kletochnyh avtomatov [Construction of pseudorandom functions based on generalized cellular automata]. Science and Education of the Bauman MSTU, 2012, no. 10, pp. 263–274. (in Russian)