для представления произвольных семейств преобразований вида (1) и позволяет строго описать методы исследования кратной транзитивности произвольных семейств преобразований вида (1) для любого класса $\mathcal{K}$, удовлетворяющего условию $\mathcal{Q}(\Omega) \subset \mathcal{K} \subset \mathcal{B}^*(\Omega)$;

2) все основные результаты работ [5, 7 – 9] корректным образом распространяются на случай использования нескольких бинарных операций — такой более общий подход улучшает характеристики практического использования кратно транзитивных семейств преобразований, предложенных в [7, 9], а кроме того, позволяет «аппроксимировать» некоторые известные блочные шифры, в которых S-боксы зависят от ключа, (Blowfish, Twofish и др.) семействами блочных преобразований вида (1), и, как следствие, появляется возможность оценить кратную транзитивность указанных блочных шифров.

## ЛИТЕРАТУРА


1. *Gligoroski D., Markovski S., Kocarev L., and Gusev M.* Edon80. `http://www.ecrypt.eu.org/stream/edon80p3.html` — eSTREAM, ECRYPT Stream Cipher Project.
2. *Gligoroski D., Markovski S., and Kocarev L.* Edon-R, An infinite family of cryptographic hash functions. `http://csrc.nist.gov/pki/HashWorkshop/2006/Papers/GLIGOROSKI_EdonR-ver06.pdf` — Second NIST Cryptographic Hash Workshop.
3. *Gligoroski D., Markovski S., and Knapskog S.* A public key block cipher based on multivariate quadratic quasigroups. `http://eprint.iacr.org/2008/320` — Cryptology ePrint Archive.
4. *Чередник И. В.* Об одном подходе к построению транзитивного множества блочных преобразований // Прикладная дискретная математика. Приложение. 2017. № 10. С. 27–29.
5. *Чередник И. В.* Один подход к построению транзитивного множества блочных преобразований // Прикладная дискретная математика. 2017. № 38. С. 5–34.
6. *Чередник И. В.* $k$-Транзитивность одного класса блочных преобразований // Прикладная дискретная математика. Приложение. 2018. № 11. С. 21–23.
7. *Чередник И. В.* Один подход к построению кратно транзитивного множества блочных преобразований // Прикладная дискретная математика. 2018. № 42. С. 18–47.
8. *Чередник И. В.* Об использовании бинарных операций при построении транзитивного множества блочных преобразований // Дискретная математика. 2019. № 31. Т. 3 С. 93–113.
9. *Чередник И. В.* Об использовании бинарных операций при построении кратно транзитивного множества блочных преобразований // Дискретная математика. 2020. Т. 32. № 2. С. 85–111.


УДК 519.719.1 DOI 10.17223/2226308X/13/22

# УТОЧНЕНИЕ СТРАТЕГИИ МАЙНИНГА ДЛЯ НЕБОЛЬШОЙ ГРУППЫ УЧАСТНИКОВ

А. В. Черемушкин

Ittay Eyal и Emin Gün Sirer описали стратегию проведения т. н. корыстного майнинга, показывающую уязвимость протокола формирования цепочки блоков, реализованного в биткоине, к атаке со стороны группы участников майнинга, составляющей относительно небольшую часть от общего числа майнеров, и позволяющую ей получить вознаграждение, превышающее размер доли имеющихся у них вычислительных ресурсов. В настоящей работе предложена уточнённая вероятностно-автоматная марковская модель, основанная на предположении о независимости обеих групп участников.

**Ключевые слова:** *блокчейн, майнинг, марковская модель, вероятностный автомат.*

В работе приводится уточнение вероятностной модели стратегии поведения выделенной (корыстной) группы участников майнинга, у которой суммарная вычислительная мощность принадлежащих им ресурсов не превосходит половины от общей вычислительной мощности [1–3]. Пусть доля вычислительных ресурсов корыстной группы пропорциональна $p = \alpha < 1/2$, а у второй группы, составленной из остальных участников, $q = 1 - \alpha$. Авторы [1–3] исходят из предположения, что поведение групп участников моделируется биномиальным распределением с вероятностями $p$ успешного подбора корыстной группой участников и $q$ для случая успешного подбора группой остальных участников.

В отличие от [3], будем предполагать, что обе группы участников действуют независимо, поэтому переходы между состояниями определяются не одной случайной величиной, а двумя независимыми случайными величинами $\xi_1$ и $\xi_2$ с вероятностями успеха $\mathsf{P}[\xi_1 = 1] = p$ (для первой группы) и $\mathsf{P}[\xi_2 = 1] = q$ (для второй группы) соответственно. При этом возможны не только ситуации, когда успех имеется у одной из сторон, но и ситуации, когда обе стороны одновременно добиваются успеха, а также когда успеха не добивается ни она из сторон.

Общая идея стратегии корыстного майнинга состоит в том, что в случае успешного подбора цепочки из $s$ блоков корыстная группа не обнародует результат, а держит его в тайне от остальных до тех пор, пока остальные участники сами не подберут очередной блок. В этом случае они поступают одним из следующих вариантов:

— если $s = 1$, то они обнародуют свой блок, создавая разветвление длины 1 и откладывая вопрос о том, какая из групп получит вознаграждение;
— если $s = 2$, то корыстная группа раскрывает оба своих блока, тем самым получая вознаграждение за два блока и лишая вознаграждения группу остальных участников;
— если $s \geqslant 3$, то они обнародуют блок, стоящий в начале своей сохраняемой в тайне цепочки, создавая разветвление из двух цепочек, либо увеличивая на 1 длину цепочки в существующем разветвлении, тем самым лишая группу остальных участников выигрыша.

Такая стратегия моделируется с помощью автономного вероятностного автомата, множество состояний которого состоит из трёх групп. Первую группу составляют состояния $s_i$, $i = 0, 1, 2, \ldots$, в которых у корыстной группы участников имеется преимущество в числе подобранных хеш-значений для блоков, равное номеру состояния. Отрицательные значения не рассматриваются, так как они соответствуют нулевому состоянию. Вторую группу составляют состояния $s_{i,0}$, $i \geqslant 2$, в которых блокчейн допускает разветвление с двумя продолжениями, у которых длина цепочки, сформированной корыстной группой, содержит на $i$ блоков больше, чем цепочка, сформированная группой остальных участников майнинга. Случай $i = 1$ также не рассматривается, так как в этом случае первая группа раскрывает свою цепочку и система переходит в нулевое состояние. Третью группу образуют состояния $s_{i,i}$ при $i \geqslant 1$, которые соответствуют случаю разветвлений с двумя одинаковыми длинами продолжений исходной цепочки.

Авторы [1] рассмотрели также случай, когда при наличии разветвления среди остальных участников найдётся подгруппа, составляющая (по мощности вычислительных ресурсов) долю, равную $\gamma$, $0 \leqslant \gamma \leqslant 1$, которая будет пытаться продолжить ветку, созданную выделенной группой, тем самым повышая вероятность получения возна-

граждения корыстной группой за блоки, подобранные ею ранее. Модель [1] позволяет успешно рассчитать вероятность получения вознаграждения, превышающего долю имеющихся у группы вычислительных ресурсов — корыстная группа получает преимущество при выполнении неравенства

$$\frac{1-\gamma}{3-2\gamma} < \alpha < \frac{1}{2}.$$

Для анализа этой ситуации будем, как и раньше, рассматривать вероятностную модель, включающую две группы участников, осуществляющих майнинг с вероятностями успеха $p$ и $q$. В тех случаях, когда для группы остальных участников имеется выбор того, для какой из цепочек строить продолжение, будем предполагать, что вероятность успешного подбора продолжения для цепочки, содержащей блоки, найденные группой корыстных участников, равна $\gamma q$, а для второй цепочки в разветвлении блокчейна она равна $(1-\gamma)q$. Поэтому для тех состояний, которые соответствуют разветвлению блокчейна, должно быть не четыре, а шесть вариантов перехода в другие состояния: (два варианта для корыстной группы) $\times$ (три варианта для группы остальных участников). Это моделируется случайной величиной, принимающей три значения 0, 1, 2 с вероятностями $p$, $q\gamma$, $q(1-\gamma)$ соответственно.

Граф переходов вероятностного автомата, моделирующего поведение двух групп участников, приведён на рис. 1. Вершины графа переходов помечены индексами соответствующих состояний, а переходы — парами $ab$, соответствующими значениям случайных величин $\xi_1 = a$ и $\xi_2 = b$ $(a, b \in \{0, 1, 2\})$. Из состояний первой группы имеются только четыре возможных перехода (табл. 1), а для состояний второй и третьей групп — шесть (табл. 2). Для изображения рёбер используются линии трёх типов: жирной линией нарисованы рёбра, соответствующие событиям, в которых корыстная группа гарантирует для себя вознаграждение, пунктиром — в которых вознаграждение получает группа остальных участников, а тонкие линии указывают, что ни одна из групп ничего не получает.

Таблица 1

**Переходы из состояний первой группы**

| Метка | Вероятность перехода | Событие |
|---|---|---|
| 00 | $qp$ | Ни одна группа не нашла продолжения |
| 01 | $q^2$ | Вторая группа нашла продолжение второй цепочки |
| 10 | $p^2$ | Корыстная группа нашла продолжение своей цепочки |
| 11 | $pq$ | Обе группы нашли продолжение для своих цепочек |

Таблица 2

**Переходы из состояний второй и третьей групп**

| Метка | Вероятность перехода | Событие |
|---|---|---|
| 00 | $qp$ | Ни одна группа не нашла продолжения |
| 01 | $q^2\gamma$ | Вторая группа нашла продолжение первой цепочки |
| 02 | $q^2(1-\gamma)$ | Вторая группа нашла продолжение второй цепочки |
| 10 | $p^2$ | Корыстная группа нашла продолжение своей цепочки |
| 11 | $pq\gamma$ | Обе группы нашли продолжение первой цепочки |
| 12 | $pq(1-\gamma)$ | Обе группы нашли продолжение для своих цепочек |

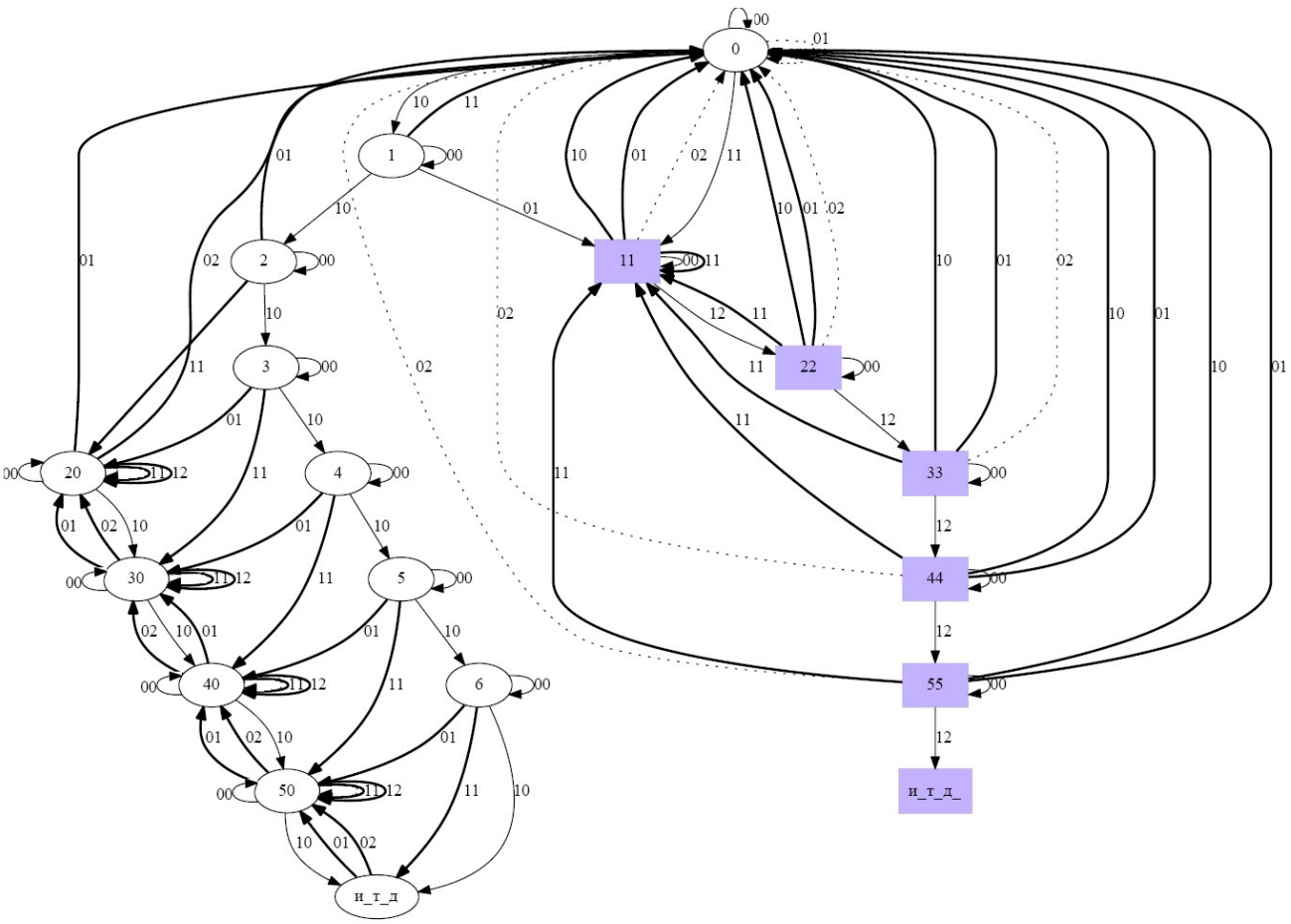


Рис. 1. Граф переходов состояний при $0 \leqslant \gamma \leqslant 1$

Для удобства соберём в одну таблицу возможные переходы автомата (табл. 3).

Для оценки вероятностей выигрыша каждой из групп необходимо сначала вычислить вероятности $p_i$ $(i = 0, 1, \ldots)$, $p_{i,0}$ $(i = 2, 3, \ldots)$ и $p_{i,i}$ $(i = 1, 2, \ldots)$ нахождения системы в каждом из состояний. Будем исходить из предположения, что соответствующая цепь Маркова является стационарной, т. е. эти вероятности не зависят от момента времени. Поэтому вероятности нахождения системы в каждом из состояний должны удовлетворять следующей системе уравнений:

$$
\begin{gathered}
p_0 = (p^2 + q^2) \sum_{i \geqslant 1} p_{i,i} + qp_0 + pqp_1 + q^2 \left(p_2 + p_{2,0}\right), \\
p_i = pq\, p_i + p^2 p_{i-1}, \quad i \geqslant 1, \\
p_{1,1} = qp\, p_{1,1} + pq\, p_0 + q^2 p_1 + pq\gamma \sum_{j \geqslant 1} p_{j,j}, \\
p_{i,i} = pq\, p_{i,i} + pq(1-\gamma)\, p_{i-1,i-1}, \quad i \geqslant 2, \\
p_{2,0} = qp\, p_{2,0} + q^2 p_{3,0} + pq\, p_{2,0} + pq\, p_2 + q^2 p_3, \\
p_{i,0} = qp\, p_{i,0} + p^2 p_{i-1,0} + q^2 p_{i+1,0} + pq\, p_{i,0} + pq\, p_i + q^2 p_{i+1}, \quad i \geqslant 3, \\
\sum_{i \geqslant 0} p_i + \sum_{i \geqslant 1} p_{i,i} + \sum_{i \geqslant 2} p_{i,0} = 1.
\end{gathered}
\tag{1}
$$

Найдём выражения для всех вероятностей через вероятность $p_1$ и значения параметров $p, q$ и $\gamma$.

Таблица 3

**Переходы модифицированного графа**

| Исходное состояние | Метка ребра | Верояность перехода | Следующее состояние | Выигрыш обеих групп |
|---|---|---|---|---|
| $s_i$ $(i \geqslant 0)$ | 00 | $qp$ | $s_i$ | $(0,0)$ |
| $s_0$ | 01 | $q^2$ | $s_0$ | $(0,1)$ |
| $s_1$ | 01 | $q^2$ | $s_{1,1}$ | $(0,0)$ |
| $s_2$ | 01 | $q^2$ | $s_0$ | $(2,0)$ |
| $s_i$ $(i \geqslant 3)$ | 01 | $q^2$ | $s_{i-1,0}$ | $(1,0)$ |
| $s_i$ $(i \geqslant 0)$ | 10 | $p^2$ | $s_{i+1}$ | $(0,0)$ |
| $s_0$ | 11 | $pq$ | $s_{1,1}$ | $(0,0)$ |
| $s_1$ | 11 | $pq$ | $s_0$ | $(2,0)$ |
| $s_i$ $(i \geqslant 2)$ | 11 | $pq$ | $s_{i,0}$ | $(1,0)$ |
| $s_{i,i}$ | 00 | $pq$ | $s_{i,i}$ | $(0,0)$ |
| $s_{i,i}$ | 01 | $q^2\gamma$ | $s_0$ | $(i,1)$ |
| $s_{i,i}$ | 02 | $q^2(1-\gamma)$ | $s_0$ | $(0,i+1)$ |
| $s_{i,i}$ | 10 | $p^2$ | $s_0$ | $(i+1,0)$ |
| $s_{i,i}$ | 11 | $pq\gamma$ | $s_{1,1}$ | $(i,0)$ |
| $s_{i,i}$ | 12 | $pq(1-\gamma)$ | $s_{i+1,i+1}$ | $(0,0)$ |
| $s_{i,0}$ | 00 | $qp$ | $s_{i,0}$ | $(0,0)$ |
| $s_{2,0}$ | 01 | $q^2\gamma$ | $s_0$ | $(2,0)$ |
| $s_{i,0}$ $(i>2)$ | 01 | $q^2\gamma$ | $s_{i-1,0}$ | $(1,0)$ |
| $s_{2,0}$ | 02 | $q^2(1-\gamma)$ | $s_0$ | $(2,0)$ |
| $s_{i,0}$ $(i>2)$ | 02 | $q^2(1-\gamma)$ | $s_{i-1,0}$ | $(1,0)$ |
| $s_{i,0}$ | 10 | $p^2$ | $s_{i+1,0}$ | $(0,0)$ |
| $s_{i,0}$ | 11 | $pq\gamma$ | $s_{i,0}$ | $(1,0)$ |
| $s_{i,0}$ | 12 | $pq(1-\gamma)$ | $s_{i,0}$ | $(1,0)$ |

**Утверждение 1.**

1) Вероятности $p_i$ при $i \geqslant 0$ удовлетворяют соотношению

$$p_{i+1} = \frac{p^2}{1-pq} p_i.$$

2) Вероятности $p_{i,i}$ при $i \geqslant 1$ удовлетворяют соотношениям

$$p_{1,1} = p_1 \frac{q(1-pq(2-\gamma))}{p(1-pq)(1-2pq)}, \qquad p_{i+1,i+1} = \frac{pq(1-\gamma)}{1-pq} p_{i,i}.$$

3) Вероятности $p_{i,0}$ при $i \geqslant 2$ вычисляются по формулам

$$p_{2,0} = p_1 \frac{p^3}{q^2(1-pq)}, \qquad p_{i+1,0} = p_1 \left(\frac{p^2}{q^2}\right)^i \left(\frac{p+q^2}{1-pq} - \left(\frac{q^2}{1-pq}\right)^i\right).$$

Оценим величину $R = r_0/(r_0+r_1)$ доли корыстной группы в общей сумме вознаграждения, полученной при применении описанной стратегии майнинга. Вознаграждение первой группы в этом случае определяется как

$$r_0 = p_1(2pq + q^2 \frac{p^2}{1-pq} + q^2 p_{2,0}) + q \sum_{i \geqslant 2} p_i + q \sum_{i \geqslant 2} p_{i,0} + p^2 \sum_{i \geqslant 1} (i+1) p_{ii} + q\gamma \sum_{i \geqslant 1} i p_{i,i}.$$

Для второй группы вознаграждение равно

$$r_1 = q^2(p_0 + (1-\gamma)p_1\Sigma_1 + \gamma \sum_{i \geqslant 1} p_{i,i}) = q^2 \left(p_1 \frac{1-pq}{p^2} + (1-\gamma) \sum_{i \geqslant 1} (i+1) p_{ii} + \gamma \sum_{i \geqslant 1} p_{i,i}\right).$$

**Утверждение 2.** Суммы вероятностей вычисляются по следующим формулам:

$$\sum_{i\geqslant 2} p_i = p_1\frac{p^2}{q},$$

$$\sum_{i\geqslant 1} p_{i,i} = p_1\frac{q}{p(1-2pq)},$$

$$\sum_{i\geqslant 1}(i+1)p_{i,i} = p_1\frac{q(2-pq(3-\gamma))}{p(1-2pq)(1-pq(2-\gamma))},$$

$$\sum_{i\geqslant 1} ip_{i,i} = p_1\frac{q(1-pq)}{p(1-2pq)(1-pq(2-\gamma))},$$

$$\sum_{i\geqslant 2} p_{i,0} = p_1\frac{p^3}{q(q-p)}.$$

Заметим, что выражение для $R$ не зависит от $p_1$. Само значение вероятности $p_1$ находится из последнего равенства системы (1) с использованием соотношения

$$p_1\left(\frac{(1-pq)^2}{p^2q} + \frac{q}{p(p^2+q^2)} + \frac{p^3}{q(q-p)}\right) = 1.$$

Приведённые формулы позволяют вычислить значение доли $R$ при произвольных значениях параметров $0 \leqslant p < 1/2$ и $0 \leqslant \gamma \leqslant 1$. Результаты вычислений приведены на рис. 2–4.

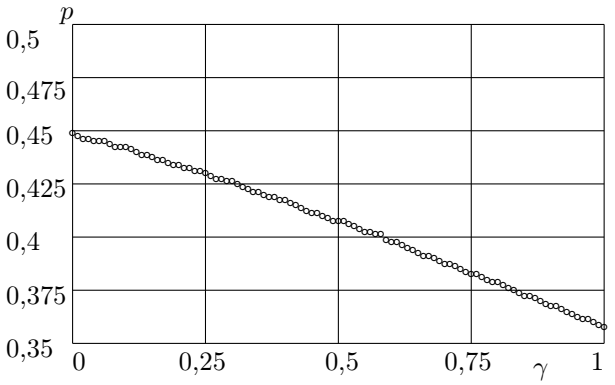


Рис. 2

На рис. 2 показан график зависимости от параметра $\gamma$ минимального значения вероятности $p$, при котором впервые выполняется условие $R > 1/2$. Вычисления показывают, что выигрыш корыстной группы превышает при соответствующем значении $\gamma$ выигрыш остальной группы при значениях вероятности $p$ в пределах

$$0{,}358 \leqslant p \leqslant 0{,}449.$$

Наибольшее значение достигается при $\gamma = 0$, а наименьшее при $\gamma = 1$.

На рис. 3 показан аналогичный график зависимости от параметра $\gamma$ минимального значения вероятности $p$, при котором впервые выполняется условие $R > p$. Получаем, что выигрыш корыстной группы при соответствующем значении $\gamma$ превышает выигрыш, полученный ими при честном выполнении протокола, при значениях вероятности $p$ в пределах

$$0 < p \leqslant 0{,}429.$$

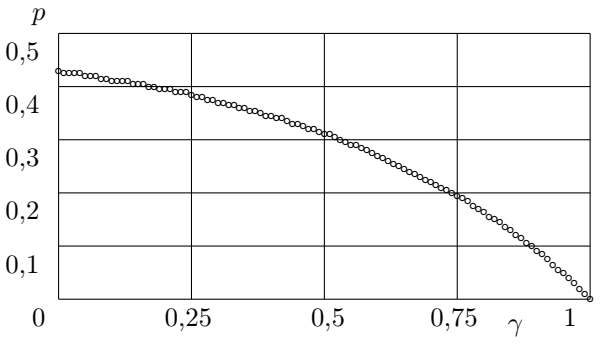


Рис. 3

В работе [1] этот интервал имеет вид $0 < p \leqslant 0{,}333$.

На графике рис. 4 приведена зависимость величины выигрыша $R$ при честном и корыстном майнинге в зависимости от величины вероятности $p$ для трёх значений параметра $\gamma$ (0, 0,5 и 1).

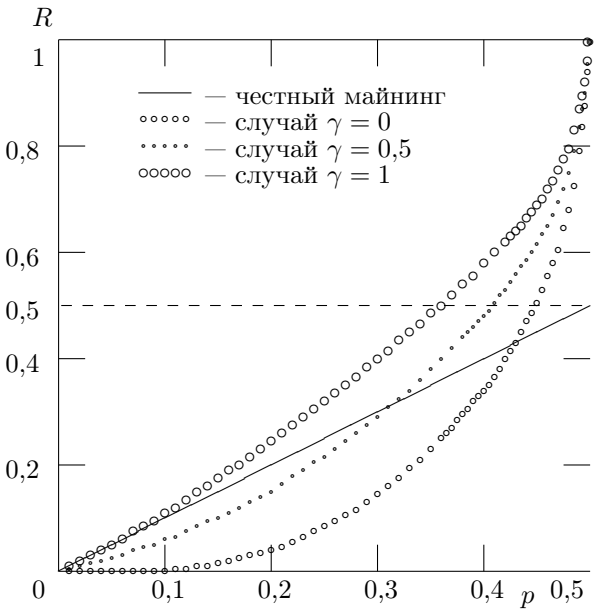


Рис. 4

Автор выражает благодарность рецензенту за внимательное прочтение рукописи и многочисленные полезные замечания.

## ЛИТЕРАТУРА

1. *Ittay E. and Emin G. S.* Majority is Not Enough: Bitcoin Mining is Vulnerable. arXiv:1311.0243. 2013. `http://arxiv.org/abs/1311.0243`.
2. *Ittay E. and Emin G. S.* Majority is not enough: bitcoin mining is vulnerable // Financial Cryptography and Data Security: 18th Intern. Conf. Christ Church, Barbados, March 3–7, 2014. P. 436–454.
3. *Ittay E. and Emin G. S.* Majority is not enough: bitcoin mining is vulnerable // Commun. ACM. 2018. V. 61. No. 7. P. 95–102. `https://doi.org/10.1145/3212998`.