

На правах рукописи



Мубараков Булат Газинурович

**ПОСТРОЕНИЕ ОЦЕНОК ЭФФЕКТИВНОСТИ
ТЕСТА ПРОСТОТЫ МИЛЛЕРА–РАБИНА**

Специальность 05.13.11 — «Математическое и программное обеспечение
вычислительных машин, комплексов и компьютерных сетей»

АВТОРЕФЕРАТ
диссертации на соискание ученой степени
кандидата технических наук

Казань 2021

Работа выполнена на кафедре системного анализа и информационных технологий Института вычислительной математики и информационных технологий Казанского (Приволжского) федерального университета

Научный руководитель: доктор физико-математических наук, доцент, профессор кафедры системного анализа и информационных технологий Казанского (Приволжского) федерального университета

Ишмухаметов Шамиль Талгатович

Официальные оппоненты: доктор технических наук, профессор, зав. кафедрой "Системы информационной безопасности" Казанского национального исследовательского технического университета КАИ

Аникин Игорь Вячеславович

доктор физико-математических наук, профессор, профессор каф. Информационная безопасность Юго-Западного государственного университета (г. Курск),

Добрица Вячеслав Порфирьевич

Ведущая организация: Федеральное государственное бюджетное образовательное учреждение высшего образования Ульяновский государственный университет

Защита состоится 24 июня 2021 года в 14 часов 00 минут на заседании диссертационного совета КФУ.01.04 на базе ФГАОУ ВО «Казанский (Приволжский) федеральный университет» по адресу: 420008, Республика Татарстан, г. Казань, ул. Кремлевская, д. 35.

С диссертацией можно ознакомиться в Научной библиотеке им. Н. И. Лобачевского ФГАОУ ВО «Казанский (Приволжский) федеральный университет» по адресу 420008, Республика Татарстан, г. Казань, ул. Кремлевская, д. 35 и на официальном сайте КФУ <https://kpfu.ru>.

Сведения о защите, автореферат и диссертация размещены на официальных сайтах ВАК Министерства науки и высшего образования Российской Федерации (<https://vak.minobrnauki.gov.ru>) и ФГАОУ ВО «Казанский (Приволжский) федеральный университет» (<https://kpfu.ru>).

Автореферат разослан ____ мая 2021 года.

Ученый секретарь диссертационного совета

КФУ 01.04, канд. физ.-мат наук

Еникеев Арслан Ильясович

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы исследования. Данное исследование посвящено оценке эффективности известного в теории чисел и криптографии теста простоты Миллера–Рабина. Этот тест относится к классу полиномиально вычислимых вероятностных тестов простоты и широко используется для генерации криптографических ключей в ряде популярных протоколов криптографии таких, как RSA, DSS и других.

Актуальность данной темы обусловлена расширением класса задач, связанных с защитой информации и информационной безопасностью, усилением роли криптографии в системе комплексной защиты информации, ускорением технического прогресса в области информационных технологий и коммуникаций.

Тест Миллера–Рабина основан на малой теореме Ферма и допускает ошибки, ошибочно квалифицируя составные числа как вероятно простые. Доля таких ошибок невелика и оценена в теореме Рабина величиной $1/4^k$, где k – количество итераций в тесте Миллера–Рабина. Иначе говоря, если мы выполним k итераций для проверки простоты нечетного составного числа $n \geq 9$, то вероятность ошибочного заключения "n – простое число" будет меньше $1/4^k$ (например, при $k = 10$ такая вероятность будет меньше одной миллионной).

Вероятность ошибки уменьшается при увеличении числа раундов теста, но для того, чтобы гарантировать безошибочную проверку, необходимо выполнить не менее $2 \log^2 n$ раундов (при условии принятия гипотезы Римана), что является заведомо избыточной величиной.

С другой стороны, компьютерные вычисления и построение последовательности строго псевдопростых чисел, которая содержит наименьшие составные числа, ошибочно определяемые тестом как вероятно простые при $k = 1, 2, 3, \dots$ раундах, показывают, что реальная вероятность ошибок в те-

сте Миллера–Рабина гораздо меньшей той верхней границы $1/4^k$, которую нам гарантирует теорема Миллера. Поэтому исследование реальной вероятности ошибки этого теста позволит значительно снизить верхнюю границу ошибок в тесте и обеспечит необходимую точность решения за меньшее число раундов.

Цели и задачи, решаемые в диссертации. В нашей работе мы ставим задачу получить более точные асимптотические оценки вероятности ошибок теста Миллера–Рабина и проверить их экспериментально.

Для получения таких оценок мы ввели понятие нетривиального свидетеля простоты, вывели формулы подсчета числа нетривиальных свидетелей простоты для составных чисел произвольного вида и оценили распределение функции вероятности ошибок на различных числовых интервалах. Это позволило количественно оценить вероятность ошибочной классификации составных чисел как вероятно простых в зависимости от длины числа и количества простых факторов, входящих в разложение этих чисел. Для проверки полученных оценок нами был разработан алгоритм вычисления числа нетривиальных свидетелей составных натуральных чисел, основанный на представлении натуральных чисел в виде двух массивов: массива простых делителей рассматриваемого числа и массива степеней, с которыми простые делители входят в разложения этого числа. В приложении к диссертации мы приводим реализацию этого алгоритма на высокоуровневом языке программирования Python.

В каждом раунде теста Миллера–Рабина выбирается некоторый параметр a , взаимно простой с тестируемым нечетным числом n , и проверяется условие

$$a^t \equiv 1, \text{ или } a^{t2^i} \equiv -1 \pmod{n}, \quad (1)$$

где t – наибольшее нечетное число, делящее $n - 1$, 2^i – делитель $n - 1$.

Если (1) выполняется, то параметр a называется свидетелем простоты числа n . Согласно теореме Миллера, если нечетное n является простым

числом, то все a из интервала $[2; n - 1]$, взаимно-простые с n , являются свидетелями простоты n . Если же n – составное, то число свидетелей простоты n не превышает величины $\varphi(n)/4$. Таким образом, доля свидетелей простоты числа n в интервале $[2; n - 1]$ определяет вероятность вывода ” n – составное число” или ” n – вероятно простое число”.

Для построения количественных оценок вероятности ошибки нами была введена вспомогательная функция частоты

$$Fr(n) = \frac{N_w(n)}{\varphi(n)},$$

где $N_w(n)$ – число свидетелей простоты n , а $\varphi(n)$ – функция Эйлера.

Значение этой функции равно 1 на простых n и не превышает верхней границы 0,25 для составных. Значение функции $Fr(n)$ увеличивается при уменьшении числа факторов, входящих в разложение этого числа, и принимает максимальное значение на полупростых числах, представляющих собой произведение двух полупростых чисел.

Таким образом, исследование вероятности ошибки в тесте Миллера–Рабина сводится к эквивалентной задаче исследования распределения функции $Fr(n)$ на классах нечетных составных чисел и получения асимптотических верхних границ для вероятности средней ошибки в зависимости от размера и количества простых делителей исследуемого числа.

Научная новизна диссертации. В диссертации приведены новые и актуальные результаты, связанные с характеристикой вероятности ошибок в полиномиальном тесте простоты Миллера–Рабина. Введены и исследованы понятия нетривиального свидетеля простоты, функция частоты свидетелей, выведены формулы для подсчета числа нетривиальных свидетелей, разработан алгоритм вычисления средней частоты на различных числовых интервалах, выведены асимптотические верхние оценки средней частоты, проведены числовые компьютерные эксперименты по проверке асимптотических формул.

Теоретическая и практическая значимость диссертации. Результаты, приведенные в диссертации, имеют как теоретическое, так и практическое значение. Теоретическое значение диссертации состоит в разработке концепций нетривиального свидетеля и функции частоты свидетелей, которые дают возможность количественной оценки вероятности ошибки теста Миллера–Рабина в зависимости от длины тестируемых чисел.

Практическое значение диссертации состоит в разработке компьютерных алгоритмов вычисления средней вероятности ошибок в тесте Миллера–Рабина для различных классов составных чисел и в числовых результатах, характеризующих убывание средней ошибки при увеличении длины тестируемых чисел. Разработан пакет программ на высокоуровневом языке программирования Python, с использованием которого была вычислена средняя ошибка теста Миллера–Рабина для различных классов составных чисел, представленных массивами простых делителей исследуемых чисел и их степеней. Выполнены числовые эксперименты по расчету средней частоты и выполнено сравнение полученных значений с теоретическими верхними оценками, что позволило интерполировать полученные оценки на числах произвольной длины, в том числе и для контроля максимальной вероятности ошибки при генерации криптографических ключей.

Методология и методы исследования. В работе над диссертацией использовались общеизвестные методы теории чисел, теории алгоритмов, алгебры и теории языков программирования.

Положения, выносимые на защиту. В качестве основных достижений нашей диссертации мы формулируем следующие положения:

1. Вывод основных формул вычисления числа свидетелей для различных классов составных чисел в зависимости от числа простых факторов, входящих в разложение этих чисел.

2. Определение и исследование функции частоты свидетелей, количе-

ственно характеризующей вероятность ошибки теста Миллера–Рабина.

3. Разработка вычислительных алгоритмов и их реализация на языке Python нахождения средней частоты свидетелей для различных классов составных чисел.

4. Построение асимптотических верхних оценок для средней вероятности ошибки на классах составных чисел, имеющих фиксированное число простых делителей, и на классе всех составных чисел.

Степень достоверности и апробация результатов.

Основные результаты работы прошли апробацию и были доложены автором на следующих научных конференциях и семинарах:

1. IV Всероссийская научно-практическая конференция "Информационные технологии в системе экономической безопасности России и ее регионов", 23-25 апреля 2012 года, Казань.

2. II Всероссийский конгресс молодых ученых, 2013, Санкт-Петербург.

3. I Международная научно-практическая конференция "Информационная безопасность в свете Стратегии Казахстан-2050" , 2013, Астана.

4. Всероссийская конференция с международным участием "Функциональный анализ и математическое образование(FAMO-2020) посвящённая 100-летию А.В. Штрауса, 2020, Ульяновск.

5. XIX Всероссийская молодежная научная школа-конференция "Лобачевские чтения 2020, Казань.

6. Ежегодные итоговые научно-практические конференции сотрудников и аспирантов Казанского федерального университета, 2012-2020 гг., Казань.

ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

Диссертация состоит из введения, четырех глав, каждая из которых разбита на параграфы, заключения и списка литературы, содержащего 56 наименований. Общий объём диссертации составляет 126 страниц.

Во введении обоснованы актуальность темы и выбор объектов исследования, кратко сформулированы цели и задачи исследования, а также основные положения, составляющие научную новизну и практическую значимость диссертации.

Первая глава содержит необходимые определения и обозначения, сведения из алгебры и теории чисел, используемые в работе, а также обзор и анализ основных результатов в области построения различных алгоритмов проверки натуральных чисел на простоту, разбор их достоинств и недостатков. Здесь рассмотрены и проанализированы основные алгоритмы поиска простых чисел. Приведенные здесь алгоритмы были поделены на две основные группы: алгоритмы просеивания и алгоритмы проверки заданного натурального числа на простоту.

В качестве примеров алгоритмов просеивания приведены классическое решето Эратосфена и решето Аткина–Берштейна, основанное на свойствах модулярных форм.

Ко второй группе относится тест, основанный на малой теореме Ферма. Эта теорема утверждает, что для простых p и $1 \leq a < p$ выполняется эквивалентность

$$a^{p-1} \equiv 1 \pmod{p}. \quad (2)$$

Хотя обратное утверждение выполнено не всегда, можно выполнять первичное отделение простых чисел от составных на основе эквивалентности (2). Такая проверка получила название теста Ферма.

Составные числа, для которых тождество (2) выполнено для всех значений a , называются числами Кармайкла. Тест Ферма ошибочно квалифицирует числа Кармайкла как вероятно простые (псевдопростые по Ферма).

Первым тестом, который успешно отвергал числа Кармайкла, был тест Лемера, основанный на свойствах символов Якоби и Лежандра. Этот тест получил другую формулировку и стал более известен, как тест Соловея–Штрассена.

Также в главе 1 приведены формулировка и доказательство теста Миллера–Рабина, являющегося основным изучаемым тестом в нашей работе. Определим понятие свидетеля простоты.

Определение 1. Пусть n – произвольное натуральное число, $n = 2^s \cdot u$, где u – нечетно. Введем обозначения $\text{bin}(n) = s$ и $\text{odd}(n) = u$. Для нечетного n и целого a из интервала $1 \leq a < n$, взаимно-простого с n , назовем a свидетелем простоты n , если выполняется одно из следующих двух условий:

$$\begin{aligned} 1. & \quad b = a^{\text{odd}(n-1)} \equiv 1 \pmod{n}, \\ 2. & \quad (\exists i) \quad 0 \leq i < \text{bin}(n-1) \quad b^{2^i} \equiv -1 \pmod{n}. \end{aligned} \tag{3}$$

Теорема Рабина, на которой основан тест Миллера–Рабина, утверждает следующее:

Теорема 1. Если нечетное число $n \geq 9$ является составным, то количество свидетелей простоты числа n ограничено значением

$$|W(n)| \leq \frac{\varphi(n)}{4}.$$

Этот тест подробно анализируется в оставшихся главах диссертации. Мы приводим альтернативное доказательство теоремы Рабина, найденное С.Б. Гашковым.

Также в главе 1 мы даем формулировку единственного известного на сегодняшний день детерминированного полиномиального теста простоты AKS. Существование детерминированного полиномиального теста простоты являлось известной проблемой, за решение которой брались многие известные математики, включая Ферма, Эйлера и Гаусса, однако решение получили только в начале 21 столетия три индийских математика Агравела, Каял и Саксена, по начальным буквам фамилий которых и был назван этот тест. Решая крупную теоретическую проблему, тем не менее этот тест является бесполезным для практики, так как его реализация является

сложной, а полином, ограничивающий сложность алгоритма AKS, имеет слишком высокую (двенадцатую) степень.

Вторая глава содержит формулировку и вывод основных теоретических результатов, на которых строятся асимптотические оценки средней вероятности ошибок теста Миллера–Рабина, выводимые в третьей и четвертой главах. Сформулируем основные результаты этой главы.

Теорема 2.1 Пусть n – нечетное число, и a является свидетелем простоты n , тогда $n - a$ также является свидетелем простоты n .

Непосредственно из этой теоремы вытекает важное следствие: если при выборе набора баз a для теста Миллера–Рабина не брать одновременно числа a и $n - a$, то после k успешных раундов вероятность ошибки уменьшается до величины $1/4^{2k}$, что значительно меньше оценки теорем Рабина $1/4^k$.

Следующие результаты этой главы связаны с выводом формул числа свидетелей различных типов составных чисел. В частности, для полупростого числа $n = pq$, p, q – простые числа, число свидетелей простоты определяется следующей величиной:

Теорема 2.3. (Ишмухаметов, Мубараков, Рубцова [5]). Число свидетелей простоты полупростого числа $n = pq$ равно

$$|W(pq)| = (\text{odd}(d))^2 \cdot (4^{\text{bin}(d)} + 2)/3, \quad (4)$$

где $d = \text{GCD}(p - 1, q - 1)$.

Доказательство этой теоремы использует элементарные теоретико-числовые свойства целых чисел. Следующие несколько теорем связаны с нахождением числа свидетелей простоты для различных видов составных чисел. Завершается эта серия формулировкой и доказательством общей теоремы, касающейся числа свидетелей простоты произвольного нечетного составного числа.

Теорема 2.8 (Основная теорема о числе свидетелей). Пусть $n =$

$q_1^{r_1} q_2^{r_2} \dots q_k^{r_k}$ – произвольное составное нечетное натуральное число. Общее число свидетелей числа n равно

$$|W(n)| = e_1 \cdot e_2 \cdot \dots \cdot e_k \cdot \left(1 + \sum_{i=0}^{s-1} 2^{ki} \right),$$

где $e_i = \text{odd}(d_i)$, $d_i = \text{GCD}(q_i - 1, n/q_i^{r_i} - 1)$, $s_i = \text{bin}(d_i)$, $s = \min\{s_i \mid 1 \leq i \leq k\}$.

В заключительном параграфе главы 2 вводится важное понятие функции частоты свидетелей $Fr(n)$, характеризующей вероятность того, что случайно выбранное a , $2 \leq a < n$, окажется свидетелем простоты для натурального числа n :

$$Fr(n) = \frac{|W(n)|}{\varphi(n)}$$

(в знаменателе дроби стоит функция Эйлера (Totient Euler's Function)).

Функция $Fr(n)$ принимает значение 1 на простых числах, а на составных числах ее значение не превышает величины 0, 25. Наибольшие значения эта функция принимает на полупростых числах (числах, являющихся произведением двух разных простых чисел). Поэтому изучение распределения функции $Fr(n)$ на полупростых числах является важной задачей.

Здесь же приведены интервальные границы для значений этой функции для разных типов полупростых чисел, включая числа общего вида $n = pq$, $p = k_1 u + 1$, $q = k_2 u + 1$, $\text{GCD}(k_1, k_2) = 1$:

$$\frac{1}{3k_1 k_2} < Fr(n) \leq \frac{1}{2k_1 k_2}$$

Особый интерес к полупростым числам вызван также тем, что верхние оценки средней вероятности ошибок для таких чисел оказываются оценками для всего класса составных чисел в целом.

Завершается глава 2 выводами по сформулированным здесь новым понятиям и утверждениям.

В главе 3 мы вводим понятие средней частоты, количественно характеризующую вероятность ошибки в тесте Миллера–Рабина, взятой по

множеству составных чисел, и выводим теоретические оценки для среднего значения этой функции по разным числовым множествам. Среднее значение вычисляется по обычному алгоритму, при котором суммируются средние частоты $Fr(n)$ по всем составным числам из рассматриваемого класса чисел, и полученная сумма делится на количество элементов рассматриваемого класса.

Изучаемая здесь проблема напрямую связана с проблемой оценки вероятности ошибок в тесте Миллера–Рабина на заданном числовом интервале. Общая проблема, которую мы решаем, состоит в поиске хороших асимптотических верхних оценок средней частоты для класса всех составных чисел, ограниченных некоторой границей. Однако, полная проблема является на текущий момент слишком сложной, поэтому мы решаем ее для частного случая полупростых чисел. Этот класс составных чисел выделен особо в силу того, что они наиболее близки к простым числам по метрике, задаваемой функцией частоты. Верхние оценки, полученные для этого класса, мажорируют верхние оценки для других классов составных чисел, поэтому изучение именно этого класса составных чисел представляет собой важную задачу.

Отметим, что алгоритм вычисления средней частоты имеет экспоненциальную верхнюю оценку, поэтому уже при границе $X = 10^6$ вычисление занимает около часа компьютерного времени. При распараллеливании этой процедуры возможно ускорение в некоторое фиксированное раз. Поэтому построение верхних оценок и их экстраполяция за границы построенных значений имеет важное значение для практической оценки вероятности ошибок теста Миллера–Рабина.

Используя различные теоретико-числовые свойства простых чисел, оценки их распределения, даваемые теоремой Чебышева, мы строим асимптотическую верхнюю границу для полупростых чисел с фиксированным первым делителем, проверяем ее экспериментально, используя компьютер-

ные вычисления. Основные результаты этой главы состоят в следующем.

Теорема 3.1. Пусть число p – простое и $X > p^2$. Тогда среднее значение функции частоты свидетелей в классе всех полупростых чисел $n = pq < X$, $p < q$, в предположении равномерного распределения простых чисел q в интервале $[1; X/p]$, имеет асимптотическую верхнюю оценку

$$Est(X, p) = \frac{p^2 \ln X}{2X}.$$

Таким образом, средняя ошибка по классу полупростых чисел с фиксированным меньшим аргументом p , ограничена сверху величиной, убывающей со скоростью $\ln X/X$, где X – граница интервала. Доказательство использует формулу Эйлера о частичной сумме гармонического ряда.

Предположение о равномерном распределении простых чисел является существенным. Поскольку простые числа встречаются реже ближе к концу интервала, оценка, приведенная в теореме 3.1, является неточной. Компьютерные вычисления показывают, что точные значения при увеличении границы дают расхождение с верхней оценкой.

Для получения более точных оценок на основе теоремы Пуссина о распределении простых чисел в арифметических прогрессиях была вычислена средняя длина интервала между простыми числами в зависимости от длины числа и с использованием интегрального исчисления получена следующая оценка.

Теорема 3.2. Пусть p – произвольное простое число, а X – некоторая граница. Тогда средняя частота в последовательности A полупростых чисел $n = pq \leq X$ на интервале $[1; X]$ имеет асимптотическую оценку

$$Est(X, p) = C_p \cdot \frac{\ln X \cdot \ln \ln X}{X},$$

где множитель C_p удовлетворяет неравенству $2 < C_p \leq 2p$, причем верхняя оценка $C_p = 2p$ достигается на числах $p = 2r + 1$, где r – также простое число.

Оценка теоремы 3.2 более точно по сравнению с теоремой 3.1 характеризует величину убывания средней частоты при увеличении длины рассматриваемого интервала. Компьютерные вычисления, выполненные до границы $X = 10^6$, подтверждают этот вывод.

X	$E(X)$	$Est(X)$	Est/E
10^3	0.00575854	0.00674035	1.1705
10^4	0.00125442	0.00164338	1.3101
10^5	0.00021904	0.00027702	1.2647
10^6	0.00003307	0.00004032	1.2193

В этой таблице приведены расчеты средней частоты для множества чисел вида $n = pq \leq X = 10^k$ для $p = 13$, $k = 3, 4, 5, 6$. Первый столбец содержит значения k , второй – экспериментальные значения средней частоты при коэффициенте $C_p = 2$, третий – теоретическую оценку теоремы 3.2, а последний – отношение оценки к точному значению. Можно видеть, что оценочное значение теоремы 3.2 несколько превышает точные значения, и наблюдается сходимость точных и оценочных значений при увеличении границы X .

Значение коэффициента C_p зависит от числа простых делителей числа $p - 1$. Действительно, наибольший вклад в среднюю частоту вносят слагаемые по подсерии чисел $n = pq$, $q = k(p - 1) + 1$. Вклад остальных чисел в подсчитываемое выражение зависит от количества делителей $p - 1$. Чем больше делителей имеет $p - 1$, тем большим является вклад остальных подсерий, что увеличивает среднюю частоту по всей серии.

Анализ представленной таблицы показывает, что при $X = 10^3$ полученная оценка немного выпадает из общей закономерности убывания значений последнего столбца. Это объясняется тем, что число составных чисел вида $n = pq \leq X$, входящее в знаменатель средней частоты, оценивалось по теореме Пуссина, которая дает значительную погрешность на небольших интервалах.

В заключительной главе 4 приводится описание алгоритма вычисления средней частоты для различных классов составных чисел, вводится понятие нетривиального свидетеля простоты, более точно связанного с практической оценкой вероятности ошибок теста Миллера–Рабина, выводятся основные формулы числа нетривиальных свидетелей для различных классов составных чисел. Понятие нетривиального свидетеля дается следующим определением.

Определение 2. Пусть $n > 1$ – нечетное натуральное число, и число a является свидетелем простоты n согласно определению (3). Число a называется нетривиальным свидетелем простоты n , если оно принадлежит интервалу $[2, (n - 1)/2]$.

Главным преимуществом этого определения является то, что вероятность ошибки теста Миллера–Рабина при единичной проверке уменьшается согласно теореме 2.1 с величины 0,25 до величины 1/16. Соответствующие оценки средней частоты будут также уменьшены.

Далее дается описание алгоритмической и компьютерной реализации алгоритма вычисления средней частоты. Этот алгоритм основан на представлении составных чисел в виде двух массивов, первый из которых содержит список простых делителей рассматриваемого числа, а второй – набор показателей этого числа. Алгоритм генерирует всевозможные кортежи простых чисел и их степеней, выполняется вычисление числа свидетелей $|W(n)|$ для каждого сгенерированного числа n , вычисляет функцию Эйлера и рассчитывает частоту $Fr(n) = |W(n)|/\varphi(n)$. Далее алгоритм в цикле суммирует полученные частоты и рассчитывает значение средней частоты по всему рассматриваемому интервалу $[1; X]$. Представление составных чисел в виде двух массивов позволяет организовать эффективный перебор всех составных чисел и легкий переход от одного числа к другому.

Мы изучаем изменение значения средней частоты для полупростых чисел при увеличении меньшего делителя, анализируем ее поведение при

объединении нескольких классов с фиксированным младшим делителем, выполняем переход к классам составных чисел произвольного вида и проверку и уточнение асимптотических оценок, полученных в главе 3.

Основным достижением этой главы является построение экспериментальных верхних оценок средней частоты для классов составных чисел с фиксированным числом простых делителей. Эта задача была решена и экспериментально получена верхняя оценка для таких классов. Она совпадает с верхней границей средней частоты для всех составных чисел, ограниченных аргументом X и равна $X^{-1/2}$. Эта оценка проверена для чисел $X \leq 10^8$, что не достаточно для использования в криптографических протоколах, однако, приведенные нами аргументы дают серьезные основания полагать, что эта оценка будет выполнена и для этих чисел.

Предполагая истинной нашу гипотезу об общей верхней оценке средней частоты, мы предложили методику расчета минимального числа итераций (раундов) теста Миллера–Рабина для получения необходимой степени точности (верхней границы для вероятности ошибки) для определения простых чисел заданной длины.

ЗАКЛЮЧЕНИЕ

Представленное нами исследование содержит последовательное исследование эффективности теста простоты Миллера–Рабина, направленное на решение проблемы нахождения вероятности средней ошибки теста для чисел заданной длины. Известная оценка, даваемая теоремой Миллера, состоит в том, что при однократном тестировании вероятность ошибки определения составного числа как простого, не превышает значения 0,25. Эта оценка слишком велика и не зависит от длины рассматриваемого числа. В своей работе мы усилили результат Миллера и доказали, что такая вероятность уменьшается с ростом размера тестируемых чисел.

Перечислим в завершение основные результаты, приведенные в диссертационной работе.

Снижена оценка вероятности ошибки при однократном тестировании теста Миллера–Рабина с 0,25 до $1/16$ и получены формулы для общего числа свидетелей простоты произвольных составных чисел.

Эти формулы послужили тем фундаментом, на котором были построены последующие результаты диссертации. Были введена и изучена концепция средней частоты как инструмент количественной оценки вероятности ошибки однократного тестирования теста Миллера–Рабина, получены верхние асимптотические оценки для средней частоты для классов полупростых чисел с фиксированным делителем, разработаны алгоритмы и программное обеспечение для проверки полученных асимптотических формул.

Была выполнена разработка понятий нетривиальных свидетелей простоты и функции модифицированной частоты, как более точно отражающих реальные ошибки в тесте Миллера–Рабина. Для исследования средней частоты был разработан алгоритм поиска числа нетривиальных свидетелей и частоты на основе специального представления составных чисел, получены и обоснованы экспериментальные верхние оценки средней частоты для классов составных чисел с фиксированным числом простых делителей и для класса всех составных чисел. Важным выводом из этих оценок является доказательство обратной зависимости вероятности ошибки от размера тестируемых чисел.

Наконец, на основе полученных зависимостей и верхних оценок была разработана методика количественного вычисления числа необходимых раундов теста Миллера–Рабина при заданной степени точности (вероятности ошибки) и заданной длине тестируемых чисел.

ПУБЛИКАЦИИ АВТОРА

Основные результаты диссертации представлены в 13 публикациях, из которых публикации [1] – [5] представлены журналами, входящими в списки ВАК, Scopus и Web of Science.

Список литературы

- [1] Ishmukhametov S., Mubarakov B. On practical aspects of the Miller–Rabin Primality Test // Lobachevskii Journal of Mathematics. – 2013. – Vol. 34 (4). – P. 304-312. (ВАК, Scopus, WoS) (авт. вклад – 0,28 п.л.).
- [2] Mubarakov B.G., Mochalov A.S., Rubtsova R.G. Investigation of Distribution of Pseudosimple Numbers // Research Journal of Applied Sciences. – 2015. – Vol. 10 (8). – P. 358-364. (Scopus), (авт. вклад – 0,15 п.л.).
- [3] Каратаев О.Р., Мубараков Б.Г., Мочалов А.С. О повышении эффективности теста простоты Миллера–Рабина // Вестник Казанского технологического университета. – 2015. – Т. 18, №17. – С. 183-186. (ВАК) (авт. вклад – 0,1 п.л.).
- [4] Ишмухаметов Ш.Т., Мубараков Б.Г., Камаль Маад Аль-Анни Вычисление коэффициентов Безу для k-арного алгоритма нахождения НОД // Известия высших учебных заведений. Математика. – 2017. – №11. – С. 30-38. (Scopus, WoS, ВАК) (авт. вклад – 0,19 п.л.).
- [5] Ishmukhametov S.T., Mubarakov B.G., Rubtsova R.G. On the number of witnesses in the Miller–Rabin primality test // Symmetry. – 2020.– Vol. 12 (6). – Номер статьи 890. (Scopus) (авт. вклад – 0,25 п.л.).
- [6] Мубараков Б.Г. *Исследование рядов простых чисел.* // Информационные технологии в системе социально-экономической безопасности России и ее регионов: труды IV Всероссийской научной конференции, Казань, 18

23–26 апреля 2012 г. / науч. ред. Голицына И.Н. – Казань: КФУ, 2012.– С. 158-162.

- [7] Мубараков Б.Г. *Исследование строго псевдопростых чисел* / Сборник трудов II Всероссийского конгресса молодых ученых / гл. ред.: В.О. Никифоров. Вып. 2.– Санкт-Петербург: ИТМО, 2013. – С. 291-293.
- [8] Мубараков Б.Г. *О выводе частичных сумм рядов по простым числам* / Итоговая научно-образовательная конференция студентов Казанского федерального университета 2012 года: сборник статей. В Т.5. Институт математики и механики им. Н.И. Лобачевского, Институт вычислительной математики и информационных технологий, Институт управления и территориального развития, Институт физики. – Казань: Казан. ун-т, 2012.– С. 57-62.
- [9] Ишмухаметов Ш.Т., Мубараков Б.Г., Рубцова Р.Г. О проблеме нахождения строго псевдопростых чисел // Информационная безопасность в свете Стратегии Казахстан-2050: сборник трудов I Международной научно-практической конференции (12 сентября 2013 г., Астана). – Астана: Евразийский национальный университет им.Л.Н.Гумилева, 2013. – С. 349–353 (авт. вклад – 0,1 п.л.).
- [10] Ишмухаметов Ш.Т., Мубараков Б.Г. Об одном классе строго псевдопростых чисел // Эвристические алгоритмы и распределенные вычисления.– 2014. – Т. 1, №1. – С. 64-73 (авт. вклад – 0,3 п.л.).
- [11] Mubarakov B.G., Ishmukhametov Sh.T., Mochalov A.S. Euclidean algorithm for recurrent sequences // Applied Discrete Mathematics and Heuristic Algorithms. – 2015. – Vol. 1 (1). – P. 23-28 (авт. вклад – 0,13 п.л.).
- [12] Мубараков Б.Г. Эффективная оценка теста простоты Миллера–Рабина натуральных чисел / Труды Математического центра имени

Н.И.Лобачевского. Т.59 / "Лобачевские чтения – 2020" // Материалы XIX Всероссийской молодежной научной школы-конференции – Казань: Изд-во Академии наук РТ, 2020. – Т. 59. – С. 106-109.

- [13] 13. Ishmukhametov S., Rubtsova R., Mubarakov B., Arkan M. On a new algorithm for computing GCD of integer numbers // Trends in Computer Science and Information Technology. – 2020. – Vol. 5 (1). – P. 15-17 (авт. вклад – 0,05 п.л.).