

РОССИЙСКАЯ АКАДЕМИЯ НАУК

Проблемы передачи информации



том 59 вып. 4

2023

РОССИЙСКАЯ АКАДЕМИЯ НАУК

ПРОБЛЕМЫ ПЕРЕДАЧИ ИНФОРМАЦИИ

Журнал основан
в январе 1965 г.

ISSN: 0555-2923

Выходит
4 раза в год

Том 59, 2023

Вып. 4

М о с к в а

С О Д Е Р Ж А Н И Е

Теория кодирования

Угловский А.Ю., Мельников И.А., Алексеев И.А., Куреев А.А. Оценка низкого уровня ошибок с помощью выборки по значимости с равномерным распределением 3

Методы обработки сигналов

Миллер А.В. Синхронизация времени в спутниковых системах квантового распределения ключей 13

Большие системы

Петрова Е.Н., Пирогов С.А. Полураспад и соотношение неопределенностей 28

Теория сетей связи

Лихтциндер Б.Я., Привалов А.Ю. Обобщение формул для моментов очереди при неординарном пуассоновском потоке для очередей пакетов в системах телекоммуникаций 32

Авторский указатель, Т. 59, 2023 г. 38

CONTENTS

Coding Theory

Uglovskii, A.Yu., Melnikov, I.A., Alexeev, I.A., and Kureev, A.A., Effective Error Floor Estimation Based on Importance Sampling with the Uniform Distribution	3
---	---

Methods of Signal Processing

Miller, A.V., Time Synchronization in Satellite Quantum Key Distribution	13
---	----

Large Systems

Petrova, E.N. and Pirogov, S.A., Half-Life and the Uncertainty Principle	28
---	----

Communication Network Theory

Lichtzinder, B.Ya. and Privalov, A.Yu., Generalization of Formulas for Queue Length Moments under Nonordinary Poissonian Arrivals for Batch Queues in Telecommunication Systems	32
--	----

Index, V. 59, 2023	38
--------------------------	----

УДК 621.391 : 519.224.24 : 519.725.2

© 2023 г. А.Ю. Угловский, И.А. Мельников, И.А. Алексеев, А.А. Куреев

ОЦЕНКА НИЗКОГО УРОВНЯ ОШИБОК С ПОМОЩЬЮ ВЫБОРКИ ПО ЗНАЧИМОСТИ С РАВНОМЕРНЫМ РАСПРЕДЕЛЕНИЕМ¹

Основной проблемой анализа кодов с малой плотностью проверок на четность является оценка чрезвычайно низкого уровня ошибок, возникающего при высоком отношении сигнал/шум. Популярным подходом к решению этой проблемы является метод выборки по значимости. В существующих работах в качестве выборочного распределения метода выборки по значимости используется нормальное распределение со смещенным средним значением, что приводит к большой дисперсии оценки. В свою очередь, равномерное распределение имеет равновероятные выборки во всем диапазоне, что может снизить дисперсию, но приведет к смещенной оценке. Мы предлагаем модифицированный метод выборки по значимости, который позволяет рассматривать равномерное распределение в качестве выборочного, и показываем, что эта оценка лучше, чем традиционная, основанная на нормальном распределении. Также показано, что существующие критерии невозможно применить для оценки точности метода выборки по значимости с равномерным распределением во всем диапазоне отношений сигнал/шум. Для решения этой проблемы предложена новая метрика, которая использует только скорость сходимости и не зависит от истинных данных.

Ключевые слова: коды с малой плотностью проверок (МПП-коды), тупиковые множества, выборка по значимости, низкий уровень ошибок.

DOI: 10.31857/S0555292323040010, **EDN:** PFOWBX

§ 1. Введение

Коды с малой плотностью проверок (МПП-коды) широко используются в системах связи, включая волоконно-оптические линии связи (ВОЛС), сети Wi-Fi и системы 5G. Эффективность МПП-кодов во многом определяется положением низкого уровня ошибки (НУО) – области значений отношения сигнал/шум (ОСШ), в которой вероятность ошибки на блок практически не изменяется [1]. Однако оценка вероятности ошибки на блок в НУО является сложной задачей, поскольку требует длительного моделирования. В частности, для ВОЛС требуется [2] НУО порядка 10^{-12} , который можно оценить с помощью метода Монте-Карло (МК) за чрезвычайно большое время ввиду необходимости проведения большого количества испытаний.

Для уменьшения количества испытаний можно использовать метод выборки по значимости (ВЗ). ВЗ является распространенным методом оценки характеристик случайной величины с заданным распределением с помощью использования выборок из другого распределения [3, 4]. В частности, ВЗ является одним из методов

¹ Исследование выполнено в рамках Госзадания № FFNU-2022-0035 ИППИ РАН.

уменьшения дисперсии оценки, который используется для улучшения сходимости метода МК. Обычно начальное распределение величин неизвестно и может быть только оценено, в то время как плотность выборки задана. Однако в задаче оценки НУО МПП-кода исходная плотность хорошо известна, но оцениваемая функция слишком сложна и равна нулю в наиболее вероятной области определения случайной величины. Поэтому для МПП-кодов ВЗ широко используется для изучения очень редких ошибок передачи [5–8]. Как показано в [7], это существенно ускоряет применение метода МК.

В существующих исследованиях используется нормальная выборка со смещенным средним значением. Нормальное распределение сосредоточено в области среднего значения, что приводит к значительному сдвигу выборочной плотности распределения и большой дисперсии оценки. В свою очередь, равномерное распределение не концентрируется вблизи среднего значения, что гарантирует небольшую дисперсию оценки при такой же частоте появления ошибок, как и при использовании нормального распределения. Однако использование равномерного распределения в общей системе оценки ВЗ приводит к смещенной оценке. В данной статье разработан модифицированный метод ВЗ, использующий выборку по значимости с равномерным распределением (ВЗ-Р).

Точность оценки НУО можно измерить с помощью среднеквадратической ошибки (СКО), что может занять много времени, если НУО мал. В литературе [9] известен подход, использующий нормализованную дисперсию, который можно применять только в том случае, если доверительные интервалы линейно зависят от стандартного отклонения. К сожалению, данное условие не выполняется при использовании равномерного распределения. В данной статье предложена новая метрика, которая применима при использовании ВЗ-Р.

Таким образом, в данной статье, во-первых, предложен метод ВЗ-Р для оценки НУО МПП-кодов, который основан на использовании выборки по значимости из равномерного распределения, а также показано его преимущество перед существующими подходами. Во-вторых, предложена новая метрика для оценки точности метода ВЗ-Р, которая явно не зависит от вида доверительного интервала и не зависит от истинного значения математического ожидания исследуемой функции.

Статья организована следующим образом. В § 2 вводятся основные понятия, используемые в статье. В § 3 описывается разработанный метод ВЗ-Р. В § 4 представлена новая метрика для оценки точности ВЗ-Р. В § 5 приводятся численные результаты, и § 6 завершает статью.

§ 2. Оценка низкого уровня ошибок с помощью выборки по значимости

2.1. Выборка по значимости. Суть метода ВЗ заключается в замене исходной плотности новой плотностью, которая позволяет сосредоточить внимание на событиях, представляющих интерес. Пусть $X \in \mathbb{R}^n$ – наблюдаемая случайная величина с плотностью распределения $\rho(\mathbf{x})$, $\mathbf{x} \in \mathbb{R}^n$, и пусть $f(\mathbf{x}): \mathbb{R}^n \rightarrow \mathbb{R}$ – некоторая функция от $\mathbf{x}$, математическое ожидание которой $\mathbf{E}_\rho f(X) = \int_{\mathbb{R}^n} f(\mathbf{x})\rho(\mathbf{x}) d\mathbf{x}$ необходимо оценить. При применении метода ВЗ для вычисления $\mathbf{E}_\rho f(X)$ используется другая случайная величина Y с плотностью распределения $\rho^*(\mathbf{y})$, $\mathbf{y} \in \mathbb{R}^n$. Если для всех $\mathbf{y} \in \mathbb{R}^n$ плотность распределения $\rho^*(\mathbf{y}) \neq 0$, тогда

$$\mathbf{E}_\rho f(X) = \int_{\mathbb{R}^n} f(\mathbf{y}) \frac{\rho(\mathbf{y})}{\rho^*(\mathbf{y})} \rho^*(\mathbf{y}) d\mathbf{y} = \mathbf{E}_{\rho^*} [f(Y)w(Y)],$$

где $w(\mathbf{y}) = \frac{\rho(\mathbf{y})}{\rho^*(\mathbf{y})}$ – весовая функция.

Соответствующая несмещенная эмпирическая оценка принимает вид

$$\widehat{\mathbf{E}}_{\rho} f(X) = \frac{1}{N} \sum_{i=1}^N f(Y_i) w(Y_i), \quad (1)$$

где $\{Y_i\}$ является последовательностью независимых случайных величин с одинаковым распределением и плотностью $\rho^*(\mathbf{y})$. Стоит отметить, что в качестве ρ^* нельзя взять произвольную плотность распределения, поскольку оценка (1) должна обладать конечной дисперсией для построения доверительных интервалов требуемой точности. Для улучшения сходимости оценку (1) можно разделить на математическое ожидание весовой функции:

$$\widetilde{\mathbf{E}}_{\rho} f(X) = \frac{\frac{1}{N} \sum_{i=1}^N f(Y_i) w(Y_i)}{\frac{1}{N} \sum_{i=1}^N w(Y_i)} = \frac{\sum_{i=1}^N f(Y_i) w(Y_i)}{\sum_{i=1}^N w(Y_i)}. \quad (2)$$

Поскольку $\rho^*(\mathbf{y}) \neq 0$ для всех $\mathbf{y} \in \mathbb{R}^n$, то

$$\mathbf{E}_{\rho^*} w(Y) = \int_{\mathbb{R}^n} \frac{\rho(\mathbf{y})}{\rho^*(\mathbf{y})} \rho^*(\mathbf{y}) d\mathbf{y} = \int_{\mathbb{R}^n} \rho(\mathbf{y}) d\mathbf{y} = 1.$$

Таким образом, $\widetilde{\mathbf{E}}_{\rho} f(X)$ сходится почти наверное к истинному значению $\mathbf{E}_{\rho} f(X)$.

В МПП-кодах ВЗ часто используется для оценки экстремально низкой вероятности отказа от декодирования в канале с аддитивным белым гауссовским шумом (АБГШ-канале) $f(x) \equiv \mathbb{I}_{\mathbb{A}}(x)$, где x – логарифм отношения правдоподобия (ЛОП), $\mathbb{A}$ – множество значений ЛОП, которые приводят к ошибкам при декодировании, и $\mathbb{I}_{\mathbb{A}}$ – индикаторная функция множества $\mathbb{A}$. Поскольку множество $\mathbb{A}$ имеет сложную структуру, в общем случае не представляется возможным найти f аналитическими методами. Для сокращения количества испытаний необходимо найти $\rho^*(\mathbf{y})$, которое удовлетворяет двум условиям: $\Pr(Y \in \mathbb{A}) \sim 1$ и $\text{Var } w(Y) \sim 0$. Второе условие обеспечивает быструю сходимость весовой функции. Стоит отметить, что случай $\Pr(Y \in \mathbb{A}) \approx 1$ приводит к чрезвычайно высокой дисперсии w . Случай $\text{Var } w(Y) \approx 0$ является методом МК.

2.2. Тупиковые множества. МПП-коды можно представить в виде сильно разреженной проверочной матрицы $H \in \mathbb{F}_2^{m \times n}$ ($m < n$) с n столбцами и m строками. Кодовое слово представляется таким вектором-строкой $\mathbf{c}$, который удовлетворяет условию $H\mathbf{c}^T = 0$, где операции умножения и сложения выполняются в поле $\mathbb{F}_2$. Проверочную матрицу H МПП-кода можно представить в виде двудольного графа Таннера с проверочными и символьными вершинами, при этом строки матрицы соответствуют проверочным вершинам, а столбцы – символьным. Количество столбцов матрицы H равно длине кодового слова. Символьная вершина i и проверочная вершина j соединены тогда и только тогда, когда элемент h_{ij} матрицы H равен единице. Тупиковое множество (англ.: trapping set) (a, b) представляет собой набор из a символьных вершин и смежных с ними проверочных вершин в графе Таннера, b из которых имеют нечетное число вхождений в данное тупиковое множество. Известно, что тупиковые множества являются основными причинами ошибок декодирования при высоком ОСШ [10], что позволяет использовать их для нахождения $\rho^*(\mathbf{y})$. Этот факт использован в работе [11], которая описывает метод выборки по значимости со сдвигом среднего (СС-ВЗ). В ней рассматриваются тупиковые множества в проверочной матрице МПП-кода, и затем распределение ЛОП изменяется

в местах, где расположены символьные вершины выбранных тупиковых множеств. Таким образом, ошибки декодирования происходят чаще.

2.3. Метрики точности оценки. В литературе используются две основных метрики для сравнения точности различных оценок с помощью метода ВЗ. Первой метрикой является СКО для логарифмов вероятности ошибки на блок:

$$\text{СКО} = \sum_{\text{ОШ}} (\log \tilde{\mathbf{E}}_{\rho^*} \mathbb{I}_{\mathbb{A}}(X) - \log \mathbf{E}_{\rho} \mathbb{I}_{\mathbb{A}}(X))^2. \quad (3)$$

Данную метрику можно использовать только в том случае, если известны истинные значения вероятности ошибки на блок. К сожалению, для МПП-кодов с высокой корректирующей способностью истинные значения вероятности ошибки на блок можно вычислить только до некоторого порога, определяемого вычислительной мощностью устройств и временем, затраченным на получение этого истинного значения.

Известно, что каждая статистическая оценка характеризуется доверительными интервалами: чем меньше доверительный интервал, тем точнее результат оценки. Именно поэтому в качестве альтернативы в литературе предложена метрика γ , основанная на доверительных интервалах [6]:

$$\gamma(\rho^*) = \frac{1}{N} \left(\frac{\hat{\mathbf{E}}_{\rho^*} \mathbb{I}_{\mathbb{A}}^2(X)}{\hat{\mathbf{E}}_{\rho^*}^2 \mathbb{I}_{\mathbb{A}}(X)} - 1 \right).$$

Чем меньше γ , тем точнее оценка. Данную метрику можно использовать для оценки $\hat{\mathbf{E}}_{\rho^*}$, поскольку зависимость доверительных интервалов от стандартного отклонения является линейной. Для $\hat{\mathbf{E}}_{\rho^*}$ структура доверительного интервала становится неизвестной, что приводит к трудностям в получении точности оценки вероятности ошибки на блок. Тем не менее, в § 5 данная метрика также используется для оценки эффективности разработанного метода ВЗ-Р.

В свою очередь, метрика СКО является универсальной и может применяться для оценки $\tilde{\mathbf{E}}_{\rho^*}$ без изменений.

§ 3. Оценка низкого уровня ошибок

Рассмотрим распределение $Y \in \mathbb{R}^n$ с плотностью

$$\rho^*(\mathbf{y}) = \frac{1}{|T|} \sum_{t \in T} \prod_{i \in t} p_{IS}(\mathbf{y}_i) \prod_{j \notin t} p_{MC}(\mathbf{y}_j), \quad (4)$$

где $\mathbf{y} \in \mathbb{R}^n$, T – набор тупиковых множеств, i и j являются индексами символьных вершин, $p_{IS}(\cdot)$ – рассматриваемая плотность (равномерная или нормальная), и $p_{MC}(\cdot)$ – плотность ЛОП, полученная при передаче сигнала с помощью двоичной фазовой манипуляции по АБГШ-каналу, которая соответствует нормальному распределению с известной дисперсией канала:

$$p_{MC}(x) = \frac{\sigma}{2\sqrt{2\pi}} \exp \left\{ -\frac{\sigma^2}{2} (x - 2/\sigma^2)^2 \right\}, \quad x \in \mathbb{R}.$$

Иными словами, для всех ненулевых кодовых слов каждая компонента вектора ЛОП, которая не принадлежит тупиковому множеству, имеет нормальное распределение со средним $\frac{2}{\sigma^2}$ и дисперсией $\frac{4}{\sigma^2}$.

В качестве выборочной плотности рассмотрим равномерное распределение $p_{IS}(x)$ в интервале $[a, b]$. Стоит отметить, что для данного распределения использование формулы (2) вместо (1) необходимо для получения несмещенной оценки.

Процедура оценки НУО с помощью ВЗ-Р разделена на три основных этапа: (i) поиск наиболее опасных тупиковых множеств, (ii) выбор параметров для каждого из распределений в выбранном диапазоне ОСШ, и (iii) сама оценка ВЗ. Рассмотрим подробнее каждый из этапов.

На первом этапе по заданному H выбираются потенциально опасные тупиковые множества, представляющие собой циклы и объединения двух циклов (см. [12]). Для нерегулярного кода также необходимо добавить к нумерованным тупиковым множествам столбцы единичного веса. Затем с помощью метода СС-ВЗ из всех тупиковых множеств исключаются менее опасные. Для этого выберем некоторый действительный параметр $\varepsilon < 1$ и порог $\theta \in (0, 1)$. Далее, для любого фиксированного тупикового множества t используется метод СС-ВЗ со следующей выборочной плотностью:

$$\rho^*(y) = \prod_{i \in t} p_{MC}\left(y_i - \frac{2\varepsilon}{\sigma^2}\right) \prod_{j \notin t} p_{MC}(y_j),$$

т.е. выборочная плотность также отвечает нормальному распределению со средним значением $\frac{2(1-\varepsilon)}{\sigma^2}$ и дисперсией $\frac{4}{\sigma^2}$. Если оценка $\Pr(Y \in A) < \theta$, то тогда тупиковое множество считается незначительным и может быть исключено из рассмотрения.

Параметр ε выбирается таким образом, чтобы более трети тупиковых множеств были незначительными. В рассматриваемом случае $\varepsilon = -5$, $\theta = 5 \cdot 10^{-2}$. Конечно, при использовании такого жадного алгоритма останется часть тупиковых множеств, которые не влияют на НУО, однако данный подход оставляет все опасные тупиковые множества и является быстрым.

На втором этапе после выбора тупиковых множеств происходит выбор параметров равномерного распределения для заданного ОСШ. Рассмотрим случайную величину $Y \in \mathbb{R}^n$ с плотностью

$$\rho^*(y) = \frac{1}{|T|} \sum_{t \in T} \prod_{i \in t} p_U(y_i) \prod_{j \notin t} p_{MC}(y_j),$$

где

$$p_U(x) = \begin{cases} \frac{\sigma^2}{4(1-k)}, & x \in \left[\frac{2k}{\sigma^2}, \frac{2(2-k)}{\sigma^2}\right], \\ 0 & \text{в противном случае,} \end{cases} \quad x \in \mathbb{R}, \quad k < 0.$$

Для заданного порога $\theta_1 \in (0, 1)$ выберем наибольшее $k < 0$, при котором выполняется условие $\Pr(Y \in A) > \theta_1$.

На третьем этапе производится метод ВЗ с использованием формул (2) и (4).

§ 4. Новая метрика точности оценки низкого уровня ошибок

Основным недостатком СКО в качестве метрики точности оценки НУО является необходимость наличия истинных значений вероятности ошибки на блок, в то время как метрика γ требует линейной зависимости доверительного интервала от стандартного отклонения. В данном параграфе предложена новая метрика, которая не обладает вышеуказанными недостатками.

Известно, что аддитивные доверительные интервалы для математического ожидания имеют следующий вид:

$$(p - CN^{-\alpha}, p + CN^{-\alpha})$$

с некоторой константой $C > 0$ и $\alpha \in \mathbb{R}$. В данном выражении p – истинное значение статистики, а N – количество испытаний.

Введем метрику точности оценки α : чем выше α , тем более точные доверительные интервалы могут быть достигнуты, начиная с N испытаний. Это приводит к следующей теореме.

Теорема. Пусть $X_1, X_2, \dots$ – независимые одинаково распределенные случайные величины, а f_N – функция N переменных. Если существуют вещественные числа α , p и абсолютно непрерывная случайная величина η , такие что

$$N^\alpha (f_N(X_1, \dots, X_N) - p) \xrightarrow[N \rightarrow \infty]{d} \eta, \quad (5)$$

то

$$\frac{\ln |f_N(X_1, \dots, X_N) - f_N(X_{N+1}, \dots, X_{2N})|}{-\ln N} \xrightarrow[N \rightarrow \infty]{d} \alpha.$$

Доказательство. Для простоты будем писать f_N, f'_N вместо $f_N(X_1, \dots, X_N)$ и $f_N(X_{N+1}, \dots, X_{2N})$ соответственно. Легко видеть, что из (5) следует, что

$$N^\alpha (f_N - p) \xrightarrow[N \rightarrow \infty]{d} \eta \quad \text{и} \quad N^\alpha (f'_N - p) \xrightarrow[N \rightarrow \infty]{d} \eta',$$

где η' – независимая копия η . Тогда

$$N^\alpha |(f_N - p) - (f'_N - p)| = N^\alpha |f_N - f'_N| \xrightarrow[N \rightarrow \infty]{d} |\eta - \eta'|,$$

и для каждого вещественного числа x

$$\Pr\left(-\frac{\ln |f_N - f'_N|}{\ln N} < x\right) = \Pr\left(N^\alpha |f_N - f'_N| > N^{\alpha-x}\right).$$

Поскольку η является абсолютно непрерывной случайной величиной, то $W = |\eta - \eta'|$ и

$$\sup_{y \in \mathbb{R}} \left| \Pr\left(N^\alpha |f_N - f'_N| > y\right) - \Pr(W > y) \right| \xrightarrow[N \rightarrow \infty]{} 0.$$

Отсюда следует, что $x < \alpha$, и значит, $\alpha - x > 0$ и

$$\begin{aligned} & \left| \Pr\left(-\frac{\ln |f_N - f'_N|}{\ln N} < x\right) \right| \leq \\ & \leq \left| \Pr\left(N^\alpha |f_N - f'_N| > N^{\alpha-x}\right) - \Pr(W > N^{\alpha-x}) \right| + \Pr(W > N^{\alpha-x}) \xrightarrow[N \rightarrow \infty]{} 0. \end{aligned}$$

Аналогично, если $x > \alpha$, то можно показать, что

$$\left| 1 - \Pr\left(-\frac{\ln |f_N - f'_N|}{\ln N} < x\right) \right| \xrightarrow[N \rightarrow \infty]{} 0. \quad \blacktriangle$$

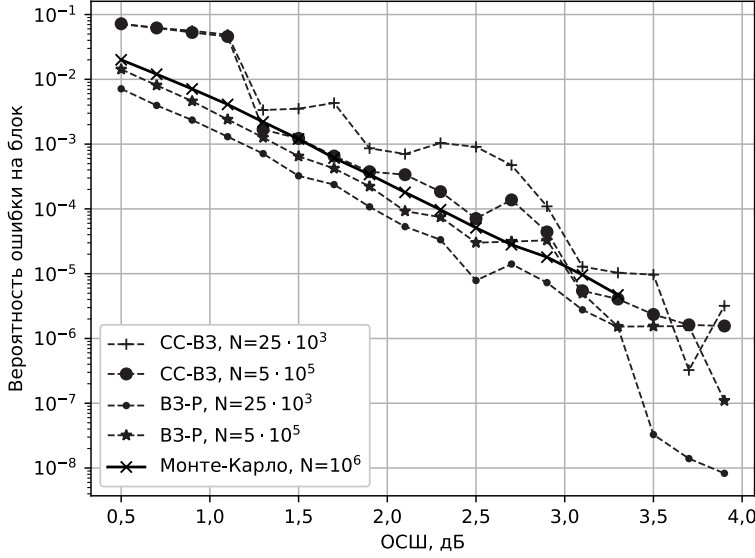


Рис. 1. Сравнение вероятности ошибки на блок для методов Монте-Карло, выборки по значимости со сдвигом среднего (СС-ВЗ) и предложенного метода выборки по значимости с равномерным распределением (ВЗ-Р)

Таким образом, α можно получить следующим образом:

$$\alpha = -\frac{1}{\ln N} \ln \left| \tilde{\mathbf{E}}_{\rho^*} \mathbb{I}_A(X) - \tilde{\mathbf{E}}'_{\rho^*} \mathbb{I}_A(X) \right|,$$

где $\tilde{\mathbf{E}}_{\rho^*} \mathbb{I}_A(X)$ и $\tilde{\mathbf{E}}'_{\rho^*} \mathbb{I}_A(X)$ – две независимые оценки вероятности ошибки на блок для метода ВЗ.

§ 5. Численные результаты

Для оценки эффективности метода ВЗ-Р, описанного в § 3, используется АБГШ-канал, в котором передается сигнал с двоичной фазовой манипуляцией, также используется Min-Sum декодер [13] и одна из наиболее широко используемых регулярных матриц МПП-кодов размера (96, 48) (см. [14]).

На рис. 1 представлены графики зависимости вероятности ошибки на блок от ОСШ для разных методов оценки НУО. Результаты показывают, что в некоторых точках СС-ВЗ немного ближе к истинным значениям, полученным с помощью метода МК, но в среднем ВЗ-Р демонстрирует более высокую точность оценки. Таким образом, область, в которой существуют значения, посчитанные с помощью метода МК (ОСШ $\in [0,5, 3,3]$), для $N = 25 \cdot 10^3$ испытаний метрика СКО равна 9,2 для СС-ВЗ и 3,8 для ВЗ-Р. В свою очередь, для $N = 5 \cdot 10^5$ испытаний метрика СКО равна 3,56 для СС-ВЗ и 0,87 для ВЗ-Р.

На рис. 2 изображена метрика γ для методов СС-ВЗ и ВЗ-Р. Стоит отметить, что оценка НУО с помощью СС-ВЗ по метрике γ лучше, чем ВЗ-Р, поскольку для СС-ВЗ величина γ ниже, чем для ВЗ-Р. Данный результат противоречит результатам, показанным на рис. 1. Причиной этого является тот факт, что метрика γ основывается на стандартном отклонении, связь которого с доверительными интервалами не является тривиальной. Поэтому $\gamma(\rho^*)$ невозможно применять к $\tilde{\mathbf{E}}_{\rho^*}$.

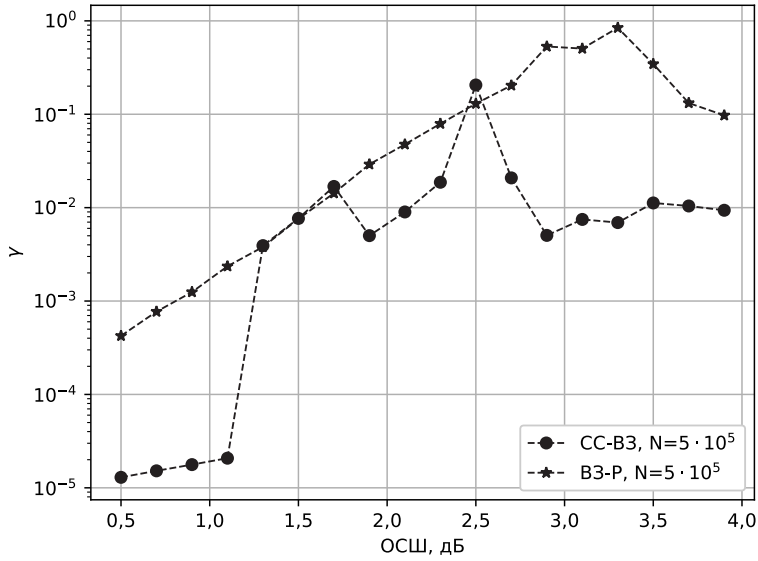


Рис. 2. Нормализованная дисперсия γ для методов CC-B3 и B3-P в зависимости от ОСШ

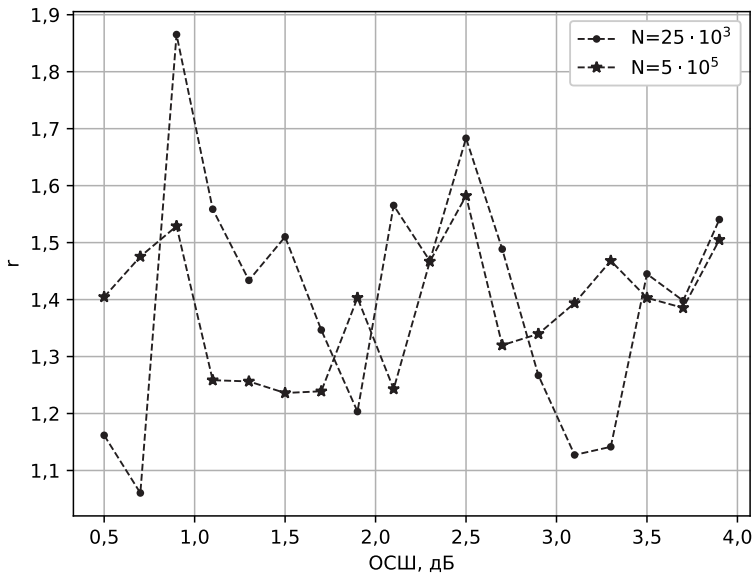


Рис. 3. Отношение $r = \alpha_{B3-P}/\alpha_{CC-B3}$ в зависимости от ОСШ

Рассмотрим применение новой метрики α к полученным результатам. На рис. 3 показано отношение r двух статистик α , т.е. $r = \alpha_{B3-P}/\alpha_{CC-B3}$, для $N = 25 \cdot 10^3$ и $N = 5 \cdot 10^5$ и для различных значений ОСШ.

Значения r превышают единицу при всех значениях ОСШ. Более того, с увеличением количества испытаний статистика r стабилизируется и стремится к своему

среднему арифметическому значению 1,4. Отсюда следует, что оценка НУО с помощью метода ВЗ-Р превосходит СС-ВЗ, что также показано с помощью СКО.

§ 6. Заключение

В данной статье разработан новый метод быстрой оценки низкого уровня ошибок МПП-кодов, который основан на выборке по значимости с равномерным распределением. Среднеквадратичная ошибка разработанного метода в три раза меньше ошибки метода на основе выборки по значимости с нормальным распределением. Для высоких значений ОСШ, при которых истинные значения вероятности ошибки на блок невозможно получить за разумное время, разработана новая метрика точности оценки, которая не требует ни истинных данных, ни явной формы доверительных интервалов.

СПИСОК ЛИТЕРАТУРЫ

1. *Kruglik S.A., Potapova V.S., Frolov A.A.* A Method for Constructing Parity-Check Matrices of Quasi-Cyclic LDPC Codes over $GF(q)$ // J. Commun. Technol. Electron. 2018. V. 63. № 12. P. 1524–1529. <https://doi.org/10.1134/S1064226918120112>
2. *Smith B.P., Kschischang F.R.* Future Prospects for FEC in Fiber-Optic Communications // IEEE J. Sel. Top. Quantum Electron. 2010. V. 16. № 5. P. 1245–1257. <https://doi.org/10.1109/JSTQE.2010.2044749>
3. *Kloek T., van Dijk H.K.* Bayesian Estimates of Equation System Parameters: An Application of Integration by Monte Carlo // Econometrica. 1978. V. 46. № 1. P. 1–19. <https://doi.org/10.2307/1913641>
4. *Kloek T., van Dijk H.K.* Experiments with Some Alternatives for Simple Importance Sampling in Monte Carlo Integration // Report 8326/E, Erasmus Univ. Rotterdam, The Netherlands, 1983. <https://doi.org/10.22004/ag.econ.272281>
5. *Dolecek L., Zhang Z., Wainwright M., Anantharam V., Nikolić B.* Evaluation of the Low Frame Error Rate Performance of LDPC Codes Using Importance Sampling // Proc. 2007 IEEE Information Theory Workshop (ITW'2007). Tahoe City, CA, USA. Sept. 2–6, 2007. P. 202–207. <https://doi.org/10.1109/ITW.2007.4313074>
6. *Neshaastegaran P., Banihashemi A.H., Gohary R.H.* Error Floor Estimation of LDPC Coded Modulation Systems Using Importance Sampling // IEEE Trans. Commun. 2021. V. 69. № 5. P. 2784–2799. <https://doi.org/10.1109/TCOMM.2021.3057625>
7. *Cavus E., Haymes C.L., Daneshrad B.* Low BER Performance Estimation of LDPC Codes via Application of Importance Sampling to Trapping Sets // IEEE Trans. Commun. 2009. V. 57. № 7. P. 1886–1888. <https://doi.org/10.1109/TCOMM.2009.07.050060>
8. *Sakai T., Shibata K.* A Study on Quick Simulation for Estimation of Low FER of LDPC Codes // Proc. 2009 IEEE 9th Malaysia Int. Conf. on Communications (MICC'2009). Kuala Lumpur, Malaysia. Dec. 15–17, 2009. P. 468–473. <https://doi.org/10.1109/MICC.2009.5431553>
9. *Ferrari M., Bellini S.* Importance Sampling Simulation of Concatenated Block Codes // IEE Proc. Commun. 2000. V. 147. № 5. P. 245–251. <https://doi.org/10.1049/ip-com:20000662>
10. *Johnson S.J.* Iterative Error Correction: Turbo, Low-Density Parity-Check and Repeat Accumulate Codes. Cambridge, UK: Cambridge Univ. Press, 2010. <https://doi.org/10.1017/CB09780511809354>
11. *Cole C., Wilson S., Hall E., Giallorenzi T.* A General Method for Finding Low Error Rates of LDPC Codes. <https://doi.org/10.48550/arXiv.cs/0605051> [cs.IT], 2006.
12. *Kim K.-J., Myung S., Jeong H.* Lowering Error Floors by Removing Dominant Trapping Sets of Low-Density Parity-Check Codes for Broadcasting Systems // Proc. 2015 IEEE Int. Symp. on Broadband Multimedia Systems and Broadcasting (BMSB'2015). Ghent, Belgium. June 17–19, 2015. P. 1–3. <https://doi.org/10.1109/BMSB.2015.7177241>

13. *Chen J., Fossorier M.P.C.* Density Evolution for Two Improved BP-Based Decoding Algorithms of LDPC Codes // IEEE Commun. Lett. 2002. V. 6. № 5. P. 208–210. <https://doi.org/10.1109/4234.1001666>
14. *MacKay D.J.C.* Encyclopedia of Sparse Graph Codes (online database). <http://www.inference.org.uk/mackay/codes/EN/C/96.33.964>

Угловский Артем Юрьевич
Мельников Игнат Алексеевич
Алексеев Иван Алексеевич
Куреев Алексей Андреевич
Институт проблем передачи информации
им. А.А. Харкевича РАН, Москва
uglovski@iitp.ru
melnikov@iitp.ru
alexeev@iitp.ru
kureev@wireless.iitp.ru

Поступила в редакцию
31.01.2024
После доработки
13.02.2024
Принята к публикации
13.02.2024

УДК 621.391 : 530.145 : 512.624.95 : 629.783

© 2023 г. А. В. Миллер

СИНХРОНИЗАЦИЯ ВРЕМЕНИ В СПУТНИКОВОМ КВАНТОВОМ РАСПРЕДЕЛЕНИИ КЛЮЧЕЙ

Временная синхронизация является одной из ключевых проблем, которые должны быть решены в процессе создания системы квантового распределения ключей (КРК). Точная синхронизация времени позволяет не только правильно присвоить порядковый номер каждому событию детектирования, но также увеличивает соотношение сигнал/шум. В спутниковой связи временная синхронизация затруднена особенно, ввиду таких факторов как высокие потери, замирание сигнала и эффект Доплера. В данной статье приводится описание простого, эффективного и надежного алгоритма для синхронизации времени. Алгоритм был протестирован в ходе реальных экспериментов по КРК между *Micius*, первым в мире спутником для квантовой связи, и приемной наземной станцией, расположенной на территории России. Полученная точность синхронизации лежит в диапазоне от 467 до 497 пс. Автор сравнивает свой алгоритм с использовавшимися ранее методами. Предлагаемый подход может применяться и для наземных систем КРК.

Ключевые слова: квантовая криптография, квантовое распределение ключей, спутниковая квантовая связь, синхронизация времени.

DOI: 10.31857/S0555292323040022, EDN: RHSP7P

§ 1. Введение

В основе квантовой криптографии лежит не вычислительная сложность используемых математических алгоритмов, а законы физики. Впервые эта идея была представлена в 1984 г. Чарльзом Беннетом и Жилем Брассаром, которые предложили первый протокол квантового распределения ключей [1]. В 1989 г. была продемонстрирована первая экспериментальная реализация квантового распределения ключей (КРК) [2]. В этом эксперименте кубиты были закодированы в поляризации фотонов, которые передавались через открытое пространство на оптическом столе на расстояние 32,5 см. С тех пор технология КРК претерпела существенное развитие. Расстояние между квантовым передатчиком и приемником существенно увеличилось. Так, в 2006 г. международная коллаборация ученых провела КРК между островами Пальма и Тенерифе в Атлантическом океане на расстояние 144 км с использованием протокола BB84 с состояниями-ловушками [3]. Недавно исследователи из Китая продемонстрировали КРК через оптоволокно на дистанции 1002 км с использованием протокола *Twin-field* [4]. Хотя полученный результат и является выдающимся для наземной системы КРК, скорость генерации секретного ключа на данном расстоянии составила около 10^{-11} бит на импульс, что едва ли можно считать удовлетворительным с точки зрения практического применения. Единственным разумным способом создать по-настоящему глобальную, межконтинентальную квантовую сеть видится использование искусственных спутников Земли: например, в качестве доверенных узлов между удаленными друг от друга наземными станциями. В 2016 г.

на орбиту был выведен первый такой спутник, Micius, и вскоре после этого были проведены эксперименты по КРК со спутника на Землю [5–7], распределению квантовой сцепленности [8], КРК на основе квантовой сцепленности [9] и квантовой телепортации [10].

Синхронизация времени является одним из наиболее важных аспектов в квантовом распределении ключей. Она позволяет Алисе и Бобу присвоить каждому событию детектирования правильный порядковый номер, что дает им возможность корректно выполнить согласование базисов. Кроме того, точная синхронизация времени позволяет существенно увеличить соотношение сигнал/шум. В спутниковом КРК синхронизация затруднена особенно, ввиду таких факторов как замирание сигнала, высокие потери и эффект Доплера. В системах КРК синхронизация может осуществляться, например, с помощью электрического сигнала [11] или глобальной навигационной спутниковой системы [3]. Однако наиболее распространенным методом является синхронизация с помощью излучения, что подразумевает передачу интенсивных оптических импульсов на той же [12] или другой [5, 13–16] длине волны. Также есть элегантное решение, основанное на анализе зарегистрированного квантового сигнала, которое не требует какого-либо дополнительного оборудования [17]. Недавно этот подход был с успехом адаптирован к реальному КРК со спутника на Землю [18]. Похожий метод использовался ранее другой группой исследователей [19], хотя стоит отметить, что интенсивность оптического сигнала в этом эксперименте на несколько порядков превышала интенсивность, соответствующую однофотонному уровню. В настоящей статье предлагается альтернативный подход, который более прост в реализации и не требует каких-то сложных математических вычислений. Данный подход, при обработке данных сразу со всего сеанса связи, показывает точность по крайней мере в 1,5 раза лучше, чем любой другой из ранее использовавшихся методов.

Структура этой статьи следующая: в § 2 даны общее описание проблемы синхронизации и детальное описание предлагаемого алгоритма; в § 3 представлены экспериментальные данные, полученные в ходе КРК между Micius и приемной наземной станцией на территории Звенигородской обсерватории; наконец, в § 4 даны некоторые выводы.

§ 2. Теория

2.1. Постановка задачи. Пусть Алиса отправляет квантовые состояния с периодом T_q , так что фотон с номером i испускается в момент времени $T_q \cdot i$. Поскольку часы Алисы могут спешить или отставать, реальное время испускания фотона составляет $\frac{\nu_0}{\nu_A} \cdot T_q \cdot i$, где ν_A – частота часов Алисы, а ν_0 – частота абсолютно точных часов. В общем случае также может быть некоторая задержка t_0^A , и тогда время испускания t_i должно быть записано как

$$t_i = t_0^A + \frac{\nu_0}{\nu_A} \cdot T_q \cdot i. \quad (1)$$

Следует отметить, что в уравнении (1) подразумевается, что частота часов ν_A не зависит от времени. В общем случае ν_A может быть функцией времени: $\nu_A = \nu_A(t)$. Тогда вместо (1) следует записать

$$\frac{1}{\nu_0} \int_{t_0^A}^{t_i} \nu_A(\eta) d\eta = T_q \cdot i. \quad (2)$$

Аспекты, связанные с дрейфом частоты, обсуждаются в этой статье далее. Пока что, если не оговорено иное, будем полагать, что частоты часов Алисы и Боба меняются

настолько медленно, что этими изменениями можно пренебречь на рассматриваемых временных интервалах.

Поскольку Алиса и Боб разделены пространством, есть некоторое ненулевое время распространения сигнала t_p . Соответственно, Боб принимает фотоны в моменты времени t_i^R , определенные следующим образом:

$$t_i^R = t_0^A + \frac{\nu_0}{\nu_A} \cdot T_q \cdot i + t_p. \quad (3)$$

Боб использует свои собственные часы, которые имеют частоту ν_B и временную задержку t_0^B , поэтому он ожидает принять фотон с номером i в момент времени

$$t_i^{R,EXP} = t_0^B + \frac{\nu_0}{\nu_B} \cdot T_q \cdot i. \quad (4)$$

Очевидно, что разница между $t_i^{R,EXP}$ и t_i^R не должна превышать по крайней мере $\frac{T_q}{2}$. В противном случае Боб будет некорректно присваивать порядковые номера тем фотонам, которые он получает.

Предположим, что Алиса и Боб синхронизировали свои часы таким образом, что $t_0^B = t_0^A + t_p$, т.е. первый фотон ($i = 0$) приходит в точности в то время, когда Боб его ожидает. Тогда разница между $t_i^{R,EXP}$ и t_i^R запишется как

$$t_i^{R,EXP} - t_i^R = T_q \cdot i \cdot \nu_0 \cdot \left(\frac{1}{\nu_B} - \frac{1}{\nu_A} \right). \quad (5)$$

Принимая во внимание равенство (5) и тот факт, что $|t_i^{R,EXP} - t_i^R|$ должно быть меньше $\frac{T_q}{2}$, можно найти i_{MAX} – такой максимальный индекс i , при котором квантовое распределение ключа все еще возможно:

$$i_{MAX} \cdot \nu_0 \cdot \left| \frac{1}{\nu_B} - \frac{1}{\nu_A} \right| = \frac{1}{2}. \quad (6)$$

До сих пор мы не предполагали, что разница в частотах мала. Тем не менее в большинстве случаев относительная разница невелика. Если определить величины ε_A и ε_B следующим образом:

$$\nu_{A(B)} = \nu_0 \cdot (1 + \varepsilon_{A(B)}), \quad (7)$$

то

$$|\varepsilon_{A(B)}| \ll 1. \quad (8)$$

Величину i_{MAX} можно выразить из (6), и тогда, принимая во внимание (7) и (8), получим

$$i_{MAX} = \frac{1}{2|\varepsilon_A - \varepsilon_B|}. \quad (9)$$

Верхней оценкой для $|\varepsilon_A - \varepsilon_B|$ может служить точность часов, умноженная на 2. Таким образом можно оценить i_{MAX} . Например, точность лучших часов на основе кварцевого осциллятора составляет $\sim 10^{-7}$, и тогда соответствующий i_{MAX} равен $\sim 2,5 \times 10^6$. При частоте следования квантовых состояний 100 МГц, что имеет место на спутнике Micius [5], это соответствует отрезку времени ~ 25 мс. Это означает, что по крайней мере каждые 25 мс Алиса и Боб должны каким-то образом синхронизировать свои часы. Широко распространено использование для этой цели оптических импульсов [5, 12–16]. Так, например, Micius оснащен лазером-маяком,

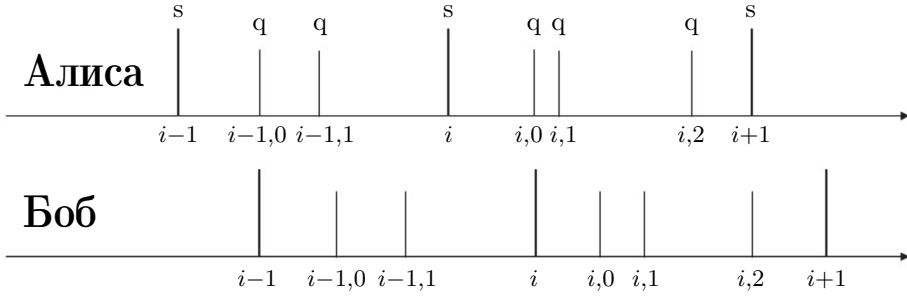


Рис. 1. Схематическое изображение синхроимпульсов (s) и квантового сигнала (q) на временной шкале

который генерирует световые импульсы длительностью 0,9 нс с частотой повторения ~ 10 кГц, которые также служат и целям синхронизации [5]. Гипотетически Алиса и Боб могли бы использовать атомные часы, которые намного более точны, и таким образом увеличить i_{MAX} на несколько порядков. Тем не менее в спутниковой связи в этом нет смысла из-за эффекта Доплера. Если спутник движется по своей орбите по скорости v_{SAT} , доплеровский сдвиг можно оценить как $\frac{v_{\text{SAT}}}{c}$, где c – скорость света в вакууме. Соответственно, нет смысла использовать часы, точность которых намного лучше, чем $\frac{v_{\text{SAT}}}{c}$, что для искусственных спутников Земли составляет $\sim 10^{-5}$. Хотя стоит отметить, что если траектория спутника известна с достаточной точностью, доплеровский сдвиг может быть скомпенсирован явным образом вычитанием рассчитанного t_p . В данной статье автор предлагает вниманию читателя альтернативный подход – простой и надежный алгоритм, который неявным образом одновременно учитывает как собственное смещение частоты, так и доплеровский сдвиг. При этом в данном подходе не требуется, чтобы траектория спутника была известна.

2.2. Предлагаемый подход.

Описание метода синхронизации. Допустим, есть последовательность из N синхроимпульсов, и пусть Алиса измеряет время каждого импульса t_{iA} , $i = 0, \dots, N-1$. Здесь и далее нижний индекс А (В) означает, что время измерено по часам Алисы (Боба). Боб принимает синхроимпульсы от Алисы и регистрирует их с помощью фотодетектора. Также Боб детектирует одиночные фотоны и присваивает каждому событию два индекса, i и j : i – это номер ближайшего предшествующего синхроимпульса, а j – порядковый номер среди всех событий, которые произошли между синхроимпульсами i и $i+1$ (см. рис. 1). Алиса отправляет Бобу значения t_{iA} по классическому открытому каналу связи. Теперь, если Бобу будут известны также значения $(t_{ij} - t_i)_A$, он сможет вычислить порядковые номера квантовых состояний n_{ij} , используя следующее выражение:

$$n_{ij} = \frac{t_{iA} + (t_{ij} - t_i)_A}{T_q}. \quad (10)$$

Таким образом, задачу синхронизации можно свести к задаче нахождения правильных значений $(t_{ij} - t_i)_A$.

Для начала рассчитаем время, когда Боб зарегистрирует синхроимпульс с номером i . Поскольку Алиса и Боб разделены в пространстве, есть некоторое ненулевое время распространения сигнала t_p , которое в спутниковой связи является функцией времени. Также есть некоторая случайная ошибка δt_i^{rand} , вызванная несовершен-

ством измерительного оборудования, в наибольшей степени – джиттером фотодетектора. Соответственно, время t_i^R , когда Боб регистрирует синхросигнал i , можно записать как

$$t_i^R = t_i + t_p(t_i) + \delta t_i^{\text{rand}}. \quad (11)$$

По аналогии с (11) время, когда Боб регистрирует квантовое состояние с индексами i, j , записывается как

$$t_{ij}^R = t_{ij} + t_p(t_{ij}) + \delta t_{ij}^{\text{rand}}. \quad (12)$$

Рассмотрим некоторую точку t_k , такую что все точки t_i и t_{ij} лежат в некоторой окрестности $(t_k - \delta t, t_k + \delta t)$ данной точки. Разложим функцию $t_p(t)$ в ряд Тейлора в окрестности точки t_k , удерживая квадратичные члены:

$$t_p(t_i) = t_p(t_k) + t'_p(t_k) \cdot (t_i - t_k) + \frac{1}{2} \cdot t''_p(t_k) \cdot (t_i - t_k)^2, \quad (13)$$

$$t_p(t_{ij}) = t_p(t_k) + t'_p(t_k) \cdot (t_{ij} - t_k) + \frac{1}{2} \cdot t''_p(t_k) \cdot (t_{ij} - t_k)^2. \quad (14)$$

Вычитая (11) из (12) и принимая во внимание (13) и (14), получаем

$$\begin{aligned} t_{ij}^R - t_i^R &= (t_{ij} - t_i) \cdot \left\{ 1 + t'_p(t_k) + t''_p(t_k) \cdot (t_i - t_k) + \frac{1}{2} \cdot t''_p(t_k) \cdot (t_{ij} - t_i) \right\} + \\ &+ \delta t_{ij}^{\text{rand}} - \delta t_i^{\text{rand}}. \end{aligned} \quad (15)$$

Очевидно, что если выполняется условие $t''_p \cdot \delta t \ll t'_p$, то третьим и четвертым членами в фигурных скобках можно пренебречь. Далее мы покажем, что это условие выполняется во время всего сеанса связи, за исключением короткого ($\lesssim 10$ мс) временного отрезка, внутри которого происходит изменение знака доплеровского сдвига. Стоит отметить, что вблизи точки изменения знака доплеровского смещения чрезвычайно мал и второй член в фигурных скобках t'_p . Это означает, что внутри данного интервала изменением t_p можно и вовсе пренебречь. Таким образом, квадратичные члены в (15) можно отбросить. Тогда, приняв также во внимание тот факт, что Алиса и Боб используют для измерения временных интервалов собственные часы, выражение (15) можно записать следующим образом:

$$\frac{\nu_0}{\nu_B} \cdot (t_{ij}^R - t_i^R)_B = \frac{\nu_0}{\nu_A} \cdot (t_{ij} - t_i)_A \cdot (1 + t'_p(t_k)) + \delta t_{ij}^{\text{rand}} - \delta t_i^{\text{rand}}. \quad (16)$$

Выражая $(t_{ij} - t_i)_A$ из (16), получаем

$$(t_{ij} - t_i)_A = \frac{\nu_A}{\nu_B} \cdot \frac{1}{1 + t'_p(t_k)} \cdot (t_{ij}^R - t_i^R)_B + \frac{\nu_A}{\nu_0} \cdot \frac{1}{1 + t'_p(t_k)} (\delta t_{ij}^{\text{rand}} - \delta t_i^{\text{rand}}). \quad (17)$$

Случайные ошибки δt_i^{rand} и $\delta t_{ij}^{\text{rand}}$ неизвестны, однако можно сделать разумное предположение, что математические ожидания этих величин равны 0. Тогда, если ввести обозначение

$$C_k = \frac{\nu_A}{\nu_B} \cdot \frac{1}{1 + t'_p(t_k)},$$

то (17) запишется в виде

$$(t_{ij} - t_i)_A = C_k \cdot (t_{ij}^R - t_i^R)_B. \quad (18)$$

По аналогии с (15) для двух соседних синхроимпульсов с номерами i и $i + 1$

$$t_{i+1}^R - t_i^R = \delta t_{i+1}^{\text{rand}} - \delta t_i^{\text{rand}} + (t_{i+1} - t_i) \cdot \left\{ 1 + t'_p(t_k) + t''_p(t_k) \cdot (t_i - t_k) + \frac{1}{2} \cdot t''_p(t_k) \cdot (t_{i+1} - t_i) \right\}. \quad (19)$$

Рассмотрим следующую сумму: $S_k = \sum_{i=0}^{N-2} (t_{i+1}^R - t_i^R)_B$. С одной стороны, очевидно, что

$$S_k = (t_{N-1}^R - t_0^R)_B. \quad (20)$$

С другой стороны, используя (19) и снова пренебрегая квадратичными членами, можно показать, что

$$S_k = \frac{\nu_B}{\nu_A} \cdot (t_{N-1} - t_0)_A \cdot (1 + t'_p(t_k)) + \frac{\nu_B}{\nu_0} \cdot (\delta t_{N-1}^{\text{rand}} - \delta t_0^{\text{rand}}). \quad (21)$$

Приравнявая (20) и (21), получим

$$(t_{N-1}^R - t_0^R)_B = \frac{\nu_B}{\nu_A} \cdot (1 + t'_p(t_k)) \cdot (t_{N-1} - t_0)_A + \frac{\nu_B}{\nu_0} \cdot (\delta t_{N-1}^{\text{rand}} - \delta t_0^{\text{rand}}). \quad (22)$$

Снова полагая, что математические ожидания случайных величин δt_0^{rand} и $\delta t_{N-1}^{\text{rand}}$ равны 0, ввиду того что

$$\frac{\nu_B}{\nu_A} \cdot (1 + t'_p(t_k)) \stackrel{\text{def}}{=} \frac{1}{C_k},$$

выразим C_k из (22):

$$C_k = \frac{(t_{N-1} - t_0)_A}{(t_{N-1}^R - t_0^R)_B}. \quad (23)$$

Теперь, когда C_k найдены, можно рассчитать порядковые номера квантовых состояний n_{ij} , используя выражения (10) и (18). Таким образом, предлагаемый алгоритм чрезвычайно прост в реализации. Все, что необходимо сделать, – это разбить сеанс связи на короткие отрезки времени, внутри которых изменением доплеровского сдвига можно пренебречь. Затем для каждого временного интервала необходимо, используя (23), вычислить C_k . И наконец, используя формулы (10) и (18), нужно рассчитать порядковые номера квантовых состояний.

Точность синхронизации. Минимальное N . Точность синхронизации является статистической величиной и определяется как дисперсия величины $(t_{ij} - t_i)_A$. Если бы в (22) были известны реальные значения δt_0^{rand} и $\delta t_{N-1}^{\text{rand}}$, можно было бы рассчитать истинное значение C_k :

$$C_k^r = \frac{(t_{N-1} - t_0)_A}{(t_{N-1}^R - t_0^R)_B + \frac{\nu_B}{\nu_0} \cdot (\delta t_0^{\text{rand}} - \delta t_{N-1}^{\text{rand}})}. \quad (24)$$

Аналогично, зная реальные значения случайных ошибок, из (17) можно было бы вычислить истинное значение $(t_{ij} - t_i)_A$:

$$(t_{ij} - t_i)_A^r = C_k^r \cdot (t_{ij}^R - t_i^R)_B + \frac{\nu_A}{\nu_0} \cdot \frac{1}{1 + t'_p(t_k)} \cdot (\delta t_i^{\text{rand}} - \delta t_{ij}^{\text{rand}}). \quad (25)$$

Характерная величина случайной ошибки измерения намного меньше, чем все остальные временные интервалы. Если принять это во внимание, можно показать,

что разница между величиной $(t_{ij} - t_i)_A$, рассчитанной согласно выражению (18), и истинным значением $(t_{ij} - t_i)_A^r$ будет равна

$$\begin{aligned} & \frac{\nu_A}{\nu_0} \cdot \frac{1}{1 + t'_p(t_k)} \cdot (\delta t_{ij}^{\text{rand}} - \delta t_i^{\text{rand}}) + \\ & + \frac{\nu_B}{\nu_0} \cdot \frac{(t_{N-1} - t_0)_A}{(t_{N-1}^R - t_0^R)_B} \cdot (t_{ij}^R - t_i^R)_B \cdot (\delta t_0^{\text{rand}} - \delta t_{N-1}^{\text{rand}}). \end{aligned} \quad (26)$$

Как уже было сказано, в реальности сдвиг частоты достаточно мал: $|\varepsilon_{A(B)}| \ll 1$. Величина $|t'_p|$ не может превышать $\frac{v_{\text{SAT}}}{c}$, что составляет $\sim 10^{-5}$ для искусственных спутников Земли. Следовательно, множитель $\frac{\nu_A}{\nu_0} \cdot \frac{1}{1 + t'_p(t_k)}$ в первом слагаемом примерно равен 1. Множитель во втором слагаемом может быть записан как

$$\frac{\nu_B}{\nu_0} \cdot \frac{(t_{N-1} - t_0)_A}{(t_{N-1}^R - t_0^R)_B} \times \frac{(t_{ij}^R - t_i^R)_B}{(t_{N-1}^R - t_0^R)_B}.$$

Ввиду сказанного выше первая часть множителя также примерно равна 1. Вторая часть не превышает величину, примерно равную $\frac{1}{N}$. Таким образом, если N достаточно велико, вторым слагаемым в (26) можно пренебречь. С практической точки зрения $N = 10$ является достаточным, поскольку в этом случае множитель во втором слагаемом уже на порядок меньше, чем в первом. Далее, если мы предположим, что $\delta t_{ij}^{\text{rand}}$ и δt_i^{rand} – это две независимые нормально распределенные случайные величины с математическими ожиданиями, равными 0, тогда $\delta t_{ij}^{\text{rand}} - \delta t_i^{\text{rand}}$ также является нормально распределенной случайной величиной с математическим ожиданием, равным 0, и дисперсией $\sigma^2 = \sigma_i^2 + \sigma_{ij}^2$, где σ_i определяется джиттером фотодетекторов, которые используются для регистрации синхроимпульсов на спутнике и наземной станции, в то время как σ_{ij} определяется конечной шириной лазерных импульсов и джиттером детекторов одиночных фотонов, которые используются для регистрации квантового сигнала. Таким образом, наилучшая точность синхронизации, которую можно получить при использовании нашего метода, равна

$$\sqrt{\sigma_{\text{PD,SAT}}^2 + \sigma_{\text{PD,OGS}}^2 + \sigma_{\text{SPD}}^2 + \sigma_L^2}, \quad (27)$$

где $\sigma_{\text{PD,SAT}}$ и $\sigma_{\text{PD,OGS}}$ характеризуют джиттер фотодетекторов, которые используются для регистрации синхросигнала на спутнике и на приемной наземной станции соответственно, σ_{SPD} характеризует джиттер детекторов одиночных фотонов, а σ_L – ширину оптических импульсов, формирующих квантовый сигнал.

Максимальное N и δt . Как было показано выше, область, которая содержит в себе N синхроимпульсов, должна быть достаточно малой – такой, чтобы в пределах данной области мы могли пренебречь изменением величины доплеровского сдвига:

$$\delta t \ll \frac{t'_p}{t''_p}. \quad (28)$$

Для вычисления t'_p/t''_p используется простая модель. Во-первых, предполагается, что спутник движется по окружности (эксцентриситет = 0). Вращение Земли вокруг своей оси также не учитывается: скорость движения точки на поверхности Земли даже на экваторе на порядок меньше, чем скорость движения спутника. Наконец, рассматривается только пролет через зенит. Рассчитанная согласно этой модели зависимость t'_p/t''_p от времени представлена на рис. 2, а). Если рассмотреть

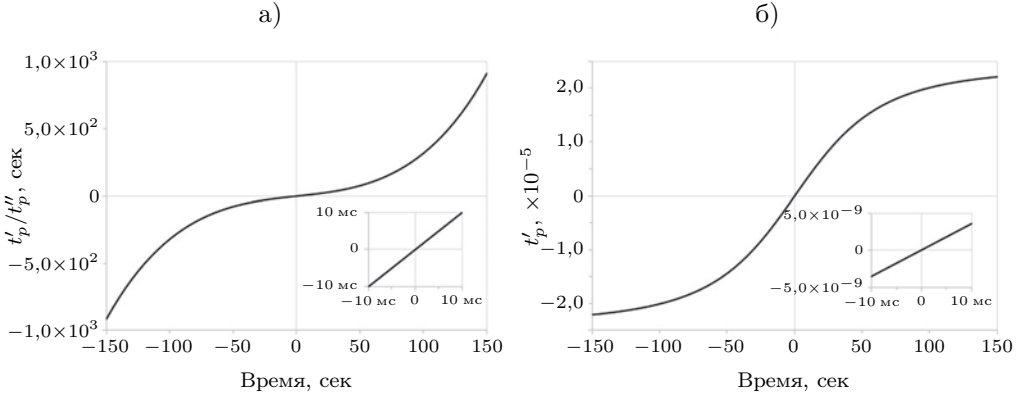


Рис. 2. Рассчитанные временные зависимости $\frac{t'_p}{t''_p}$ (а) и t'_p (б) во время пролета спутника через зенит. Здесь t'_p и t''_p – первая и вторая производные времени распространения сигнала. Высота 500 км, эксцентриситет 0. Вращение Земли вокруг своей оси не учитывается.

последовательность минимальной длины ($N = 10$), то при частоте следования синхрои́мпульсов 10 кГц это будет соответствовать $\delta t = 1$ мс. Тогда (28) выполняется для всего пролета, кроме небольшой области (± 10 мс) вблизи зенита – точки, в которой доплеровский сдвиг меняет свой знак. Однако, как можно видеть на рис. 2, б), доплеровское смещение в этой области чрезвычайно мало ($\lesssim 10^{-9}$), и поэтому его можно вовсе не принимать во внимание.

Физический смысл величины C_k . До сих пор мы не предполагали малости смещения частоты. Тем не менее в большинстве практических случаев отклонение частоты относительно мало. Модуль первой производной t'_p , которая с точностью до знака является доплеровским смещением, не превышает $\sim 10^{-5}$ для искусственных спутников Земли – т.е. это тоже малое возмущение. Таким образом, C_k можно разложить в ряд Тейлора вблизи 0. Удерживая только линейные члены, получаем

$$C_k = 1 + \varepsilon_A - \varepsilon_B - t'_p(t_k).$$

Таким образом, при малых отклонениях $C_k - 1$ характеризует то, насколько часы Алисы спешат относительно часов Боба, включая доплеровский сдвиг.

Сведение к оригинальному методу USTC. Минимальное возможное N для приведенного выше алгоритма равно 2. При $N = 2$ величина C_k определяется как $\frac{(t_1 - t_0)_A}{(t_1^R - t_0^R)_B}$. Соответственно, (18) запишется как

$$(t_{0j} - t_0)_A = \frac{(t_1 - t_0)_A}{(t_1^R - t_0^R)_B} \cdot (t_{0j}^R - t_0^R)_B,$$

что тождественно методу, который изначально применяли сотрудники Научно-технического университета Китая (USTC) [15]. Следует отметить, что при $N = 2$ множитель во втором слагаемом в (26) становится соизмерим с множителем в первом слагаемом, и поэтому второе слагаемое уже нельзя исключить из рассмотрения. Соответственно, выражение для теоретически достижимой точности синхронизации в этом случае будет отличаться от выражения, полученного для больших N .

§ 3. Эксперимент и результаты

3.1. Эксперимент. Представленный в данной статье алгоритм применяли в ходе экспериментов по КРК между спутником *Micius* и приемной наземной станцией, расположенной на территории Звенигородской обсерватории ($55^{\circ}41'56''$ с.ш., $36^{\circ}45'32''$ в.д., 180 м над уровнем моря). *Micius* был запущен в 2016 г., после чего были проведены эксперименты по КРК со спутника на Землю [5–7], распределению квантовой сцепленности [8], КРК на основе квантовой сцепленности [9], квантовой телепортации [10] и некоторые другие [20]. Спутник оснащен лазером-маяком, работающим на длине волны 530 нм, который генерирует оптические импульсы длительностью 0,9 нс с частотой повторения ~ 10 кГц, которые также служат целям синхронизации. Наземная станция представляет собой телескоп с апертурой 0,6 м, который сопряжен с остальной оптикой: в основном это телескоп-гид и камера с широким полем зрения, которые нужны для грубого контура наведения, пьезозеркало и камера с узким полем зрения для тонкого контура наведения, дихроичное зеркало, спектральный фильтр и собственно квантовый приемник с пассивным выбором базиса. Для детектирования четырех возможных состояний поляризации используются четыре детектора одиночных фотонов, характеризующиеся джиттером 350 пс FWHM. Более подробное описание оптической наземной станции можно найти в предшествующих публикациях [21–24].

3.2. Полученные результаты. На рис. 3 приведена типичная зависимость $C_k - 1$ от времени в ходе пролета спутника (нижняя серая кривая). Полученные коэффициенты C_k используются для вычисления $(t_{ij} - t_i)_A$ (18). Соответствующее распределение срабатываний детектора по времени приведено на рис. 4. В экспериментах по КРК точность синхронизации варьируется от 536 пс 1 марта 2022 г. до 593 пс 10 марта 2022 г. Как было показано выше (27), наилучшая точность синхронизации, которую можно получить при использовании нашего алгоритма, равна $\sqrt{\sigma_{PD,SAT}^2 + \sigma_{PD,OGS}^2 + \sigma_{SPD}^2 + \sigma_L^2}$. Поскольку в нашем случае квантовый и синхросигнал регистрировали на Земле детекторами одиночных фотонов, причем одного и того же типа, это выражение можно записать как

$$\sqrt{\sigma_{PD,SAT}^2 + 2\sigma_{SPD}^2 + \sigma_L^2}. \quad (29)$$

Джиттер детекторов одиночных фотонов, которые использовались в данной статье, составляет 350 пс FWHM. Ширина лазерных импульсов, формирующих квантовый сигнал, составляет 200 пс [5]. Если пренебречь джиттером фотодетектора на спутнике, то из (29) получается, что наилучшая точность синхронизации, которую можно достичь, – около 230 пс. Как можно заметить, точность, полученная в реальном эксперименте, существенно хуже. По всей видимости, это расхождение вызвано конечной шириной синхроимпульсов (0,9 нс) и ограниченной мощностью синхросигнала: как результат, детектор не всегда срабатывает в точности по переднему фронту синхроимпульса – есть значительная вероятность срабатывания позже. Действительно, ранее было показано, что при определенных условиях флуктуации интенсивности оптического сигнала в атмосфере могут приводить к значительной ошибке синхронизации [25]. Второй возможной причиной ухудшения точности синхронизации может быть временная различимость квантовых состояний: на *Micius* поляризационные состояния формируются различными лазерными диодами, и гипотетически, если не проводить точную подстройку, между временами срабатывания лазерных диодов могут быть ненулевые задержки, что может приводить к кажущемуся ухудшению точности синхронизации. Детальное исследование флуктуаций интенсивности из-за мерцания в атмосфере и временной различимости квантовых состояний выходит за рамки данной статьи – это может быть темой отдельного исследования.

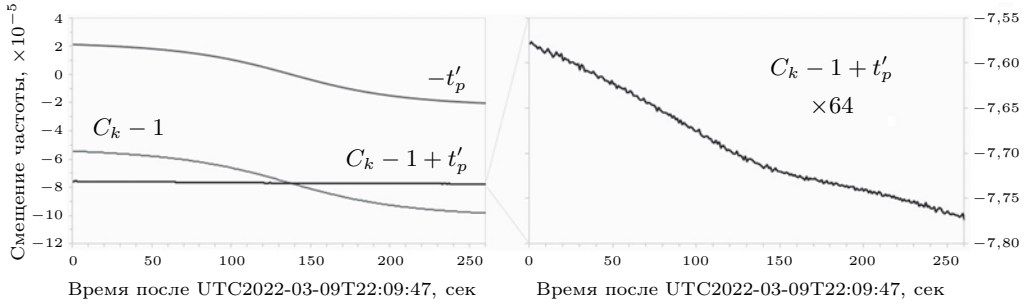


Рис. 3. Сеанс КРК 9 марта 2022 г. Разница (относительная) между частотами часов передатчика и приемника: верхняя серая кривая – доплеровский сдвиг из траектории спутника, рассчитанной с помощью модели SGP4; нижняя серая кривая – это $C_k - 1$ из анализа синхросигнала; черная кривая получена вычитанием доплеровского смещения из $C_k - 1$.

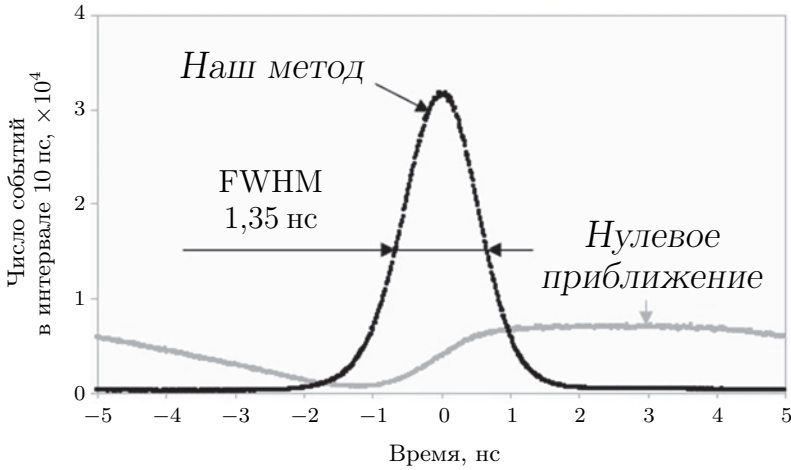


Рис. 4. Сеанс КРК 9 марта 2022 г. Распределение событий по времени, $\text{gem}\left(t_{iA} + (t_{ij} - t_i)_A + \frac{T_q}{2}, T_q\right) - \frac{T_q}{2}$. Серые точки – нулевое приближение: $(t_{ij} - t_i)_A = (t_{ij}^R - t_i^R)_B$. Черные точки – рассматриваемый метод синхронизации. Учитываются все события детектирования между UTC2022-03-09T22.09.47 и UTC2022-03-09T22.14.08 (261 сек).

Спутник и наземная станция были оснащены приемниками GPS, которые могли выдавать точные метки времени – сигнал “Pulse-per-second”, или сокращенно “PPS”. Это давало возможность отслеживать смещение частоты часов напрямую, путем анализа временного сдвига меток PPS. Максимальные скорости дрейфа часов Алисы и Боба ε'_A и ε'_B , обнаруженные во время сеансов квантовой связи, приведены в табл. 1. Как можно видеть, частота часов Алисы меняется как минимум на порядок быстрее, чем частота часов Боба. Кроме того, часы Алисы всегда дрейфуют в одном направлении – их частота уменьшается. По всей видимости, генератор опорной частоты на спутнике не термостабилизирован и начинает нагреваться после включения электроники. Тем не менее даже для часов на спутнике максимальная скорость ухода частоты, которую обнаружили в экспериментах, все еще как минимум на порядок ниже, чем скорость изменения доплеровского смещения,

Обзор экспериментов по КРК между спутником *Micius* и наземной станцией в Звенигородской обсерватории

Дата	Время начала сеанса квантовой связи, UTC+0	Время КРК, сек	Угол восхождения ^a , °	Макс. $ \varepsilon'_A $, сек ⁻¹	Макс. $ \varepsilon'_B $, сек ⁻¹	Точность синхронизации, пс
1 марта 2022 г.	UTC2022-03-01T22.12.28	222	28,5 / 23,0	$7,3 \times 10^{-9}$	$2,0 \times 10^{-10}$	536
9 марта 2022 г.^b	UTC2022-03-09T22.09.47	261	20,8 / 23,2	$7,4 \times 10^{-9}$	$7,7 \times 10^{-11}$	571
10 марта 2022 г.	UTC2022-03-10T21.46.26	249	25,6 / 23,6	$7,3 \times 10^{-9}$	$4,6 \times 10^{-10}$	593

^a Угол восхождения, при котором начинался/прекращался прием квантового сигнала.

^b Вместо истинно-случайной последовательности квантовые состояния фотонов модулировались заранее известной последовательностью длиной в 42 949 672 960 состояний.

которая составляет $\sim 10^{-7}$ сек⁻¹. Как было показано выше, первая производная доплеровского сдвига, равная второй производной времени распространения сигнала t''_p , достаточно мала, и соответственно, квадратичными членами в (15) и (19) можно пренебречь. Следовательно, ввиду того что скорость дрейфа часов составляет $\lesssim 10^{-8}$ сек⁻¹, в данном случае мы тем более можем не рассматривать соответствующие квадратичные поправки.

Помимо описанного выше способа определения смещения частоты мы также используем другой подход, основанный на анализе синхросигнала. Как было показано выше, для малых возмущений

$$C_k = 1 + \varepsilon_A - \varepsilon_B - t'_p(t_k).$$

Таким образом, $\varepsilon_A - \varepsilon_B$ можно вычислить как $C_k - 1 + t'_p(t_k)$. Коэффициенты C_k находятся из анализа синхросигнала описанным выше способом. Доплеровское смещение $-t'_p$ можно рассчитать из известной траектории спутника. В данной статье траекторию *Micius* рассчитывали с помощью модели SGP4 на основе данных TLE, взятых из открытых источников. В качестве примера на рис. 3 приведены временные зависимости $C_k - 1$ (нижняя серая кривая) и $-t'_p$ (верхняя серая кривая), полученные 9 марта 2022 г. После вычитания $-t'_p$ из $C_k - 1$ получается черная кривая, которая отображает совокупный дрейф часов Алисы и Боба относительно друг друга. В наших экспериментах максимальное расхождение между найденной таким образом величиной $\varepsilon_A - \varepsilon_B$ и той же величиной, найденной путем анализа сигнала PPS, не превышает 5% в течение всего сеанса связи.

Следует отметить, что рассматриваемый в данной статье алгоритм синхронизации не предполагает того, что траектория спутника известна. Использование приемников GPS также не является обязательным. Единственной целью представленных выше рассуждений является доказательство справедливости предположения, сделанного в начале статьи, – о том, что частоты часов Алисы и Боба можно рассматривать как константы, не зависящие от времени.

3.3. Сравнение с другими методами. В более ранних экспериментах со спутником *Micius* при использовании первоначального метода USTC точность синхронизации лежала в диапазоне 854–1041 пс, а при использовании метода “Qbit4Sync” – 711–988 пс [18]. Поскольку в тех экспериментах использовали детекторы одиночных фотонов того же самого типа, результаты можно сравнивать напрямую. В среднем по всем пролетам спутника наш алгоритм показывает точность синхронизации

Таблица 2

Прямое сравнение предлагаемого метода (МЦКТ) с методом “Qubit4Sync” (USTC) на интервалах 1 сек.

Дата	Время начала интервала 1 сек, UTC+0	Точность синхронизации, пс		Скорость просеянного ключа, кбит/с		
		МЦКТ	USTC	МЦКТ ^a	USTC ^{a,b}	Максимум ^b
1 марта 2022 г.	UTC2022-03-01T22.14.40	467	373	13,4	14,1	15,7
9 марта 2022 г.^c	UTC2022-03-09T22.12.36	480	369	8,58	9,08	10,1
10 марта 2022 г.	UTC2022-03-10T21.48.55	497	380	17,2	18,3	20,4

^a Применяется временная фильтрация с окном 2 нс.

^b Рассчитано в предположении нормального распределения ошибки по времени.

^c Вместо истинно-случайной последовательности квантовые состояния фотонов модулировались заранее известной последовательностью длиной в 42 949 672 960 состояний.

лучше в 1,7 и 1,5 раза, чем оригинальный метод USTC и метод “Qbit4Sync” соответственно.

Кроме того, было проведено прямое сравнение нашего алгоритма с методом “Qbit4Sync” на временных интервалах длительностью 1 сек. Реализация алгоритма “Qbit4Sync” была выполнена на стороне USTC. Обзор полученных результатов сравнения приведен в табл. 2. Как можно заметить, во-первых, точность синхронизации на интервале 1 сек значительно лучше, чем при обработке данных всего сеанса связи. Для нашего метода синхронизации она в среднем лучше на 15%. В случае метода USTC относительное изменение намного более существенное – на порядок больше. Во-вторых, если сравнивать два метода между собой на интервале 1 сек, “Qbit4Sync” показывает точность в 1,3 раза лучше, чем наш алгоритм.

Мы провели оценку, в какой степени разница в точности между двумя методами синхронизации влияет на скорость генерации секретного ключа. Для данной оценки мы делаем два предположения. Первое предположение – случайная ошибка измерения подчиняется нормальному распределению по времени. Второе – применяемое во временной фильтрации окно не меняется и составляет 2 нс. Согласно расчетам, при использовании в наших экспериментах с Micius алгоритма USTC скорость генерации просеянного ключа увеличилась бы не более чем на 6%: точные значения приведены в табл. 2. Помимо скорости генерации просеянного ключа необходимо принять во внимание и изменение уровня квантовых ошибок – “quantum bit error rate”, или “QBER”: на скорость генерации секретного ключа влияют оба параметра. Например, QBER, полученный 9 марта 2022 г. на интервале 1 сек с UTC2022-03-09T22.12.36, составляет 1,18%. Из них только 0,54% вызваны шумовыми срабатываниями детектора. Остальные ошибки, 0,64%, возникают вследствие конечного коэффициента поляризационной экстинкции из-за несовершенства оптических компонентов. Поэтому соотношение сигнал/шум, а следовательно, и точность синхронизации, на эти ошибки не оказывают никакого влияния.

Принимая во внимание два предположения, сделанных выше, можно показать, что при использовании в эксперименте метода USTC уровень квантовых ошибок из-за шумовых срабатываний понизился бы с 0,54 до 0,51%. Соответственно, суммарный QBER снизился бы с 1,18 до 1,15%. Таким образом, изменение QBER было бы пренебрежимо малым и, следовательно, не оказало бы какого-либо существенного эффекта на скорость генерации секретного ключа. Как итог, улучшение точности в 1,3 раза в условиях данного эксперимента приводит к выигрышу в скорости генерации квантового ключа только в 6%.

§ 4. Заключение

В данной статье вниманию читателя предлагается к рассмотрению простой, эффективный и надежный алгоритм для синхронизации времени в спутниковом квантовом распределении ключей. Предлагаемый подход не предполагает того, что траектория спутника известна, и не требует сложных математических вычислений. Алгоритм был протестирован во время реальных экспериментов по квантовому распределению ключа между спутником *Micius* и приемной наземной станцией, расположенной на территории Звенигородской обсерватории. Во время этих экспериментов максимальное смещение частоты между передатчиком и приемником, включая доплеровский сдвиг, составляло около 10^{-4} . При этом полученная точность синхронизации не превышала 0,5 нс.

Результаты сравнения с другими методами синхронизации неоднозначны. На коротких (1 сек) временных отрезках метод “Qubit4Sync”, разработанный в USTC, показывает точность в 1,3 раза лучше, чем наш алгоритм. Однако при этом выигрыш в скорости генерации квантового ключа относительно небольшой – не более 6%. Если применять наш метод для обработки данных со всего сеанса связи, который длится несколько сотен секунд, то он показывает точность синхронизации по крайней мере в 1,5 раза лучше, чем любой другой из применявшихся ранее методов.

Предлагаемый подход не предполагает ни использования приемников GNSS, ни даже того, что синхроимпульсы и квантовый сигнал формируются на основе сигнала с одного генератора опорной частоты. Автор полагает, что предложенный метод может применяться не только в спутниковой квантовой связи, но также и в наземных системах КРК.

Автор благодарит Научно-технический университет Китая (USTC) и компанию “QSpace Technologies” за разрешение использовать данные, полученные в ходе совместных экспериментов. Автор выражает особенную благодарность д-ру Чао-Цзэ Вану из USTC за помощь, оказанную при обработке экспериментальных данных.

СПИСОК ЛИТЕРАТУРЫ

1. *Bennett C.H., Brassard G.* Quantum Cryptography: Public Key Distribution and Coin Tossing // Proc. Int. Conf. of Computers, Systems & Signal Processing. Bangalore, India. Dec. 9–12, 1984. V. 1. P. 175–179.
2. *Bennett C.H., Bessette F., Brassard G., Salvail L., Smolin J.* Experimental Quantum Cryptography // J. Cryptol. 1992. V. 5. № 1. P. 3–28. <https://doi.org/10.1007/BF00191318>
3. *Schmitt-Manderbach T., Weier H., Furst M., Ursin R., Tiefenbacher F., Scheidl T., Perdigues J., Sodnik Z., Kurtsiefer C., Rarity J.G., Zeilinger A., Weinfurter H.* Experimental Demonstration of Free-Space Decoy-State Quantum Key Distribution over 144 km // Phys. Rev. Lett. 2007. V. 98. № 1. P. 010504 (4 pp.). <https://doi.org/10.1103/PhysRevLett.98.010504>
4. *Liu Y., Zhang W.-J., Jiang C., Chen J.-P., Zhang C., Pan W.-X., Ma D., Dong H., Xiong J.-M., Zhang C.-J., Li H., Wang R.-C., Wu J., Chen T.-Y., You L., Wang X.-B., Zhang Q., Pan, J.-W.* Experimental Twin-Field Quantum Key Distribution over 1000 km Fiber Distance // Phys. Rev. Lett. 2023. V. 130. № 21. P. 210801 (6 pp.). <https://doi.org/10.1103/PhysRevLett.130.210801>
5. *Liao S.-K., Cai W.-Q., Liu W.-Y., Zhang L., Li Y., Ren J.-G., Yin J., Shen Q., Cao Y., Li Z.-P., Li F.-Z., Chen X.-W., Sun L.-H., Jia J.-J., Wu J.-C., Jiang X.-J., Wang J.-F., Huang Y.-M., Wang Q., Zhou Y.-L., Deng L., Xi T., Ma L., Hu T., Zhang Q., Chen Y.-A., Liu N.-L., Wang X.-B., Zhu Z.-C., Lu C.-Y., Shu R., Peng C.-Z., Wang J.-Y., Pan J.-W.* Satellite-to-Ground Quantum Key Distribution // Nature. 2017. V. 549. № 7670. P. 43–47. <https://doi.org/10.1038/nature23655>
6. *Liao S.-K., Cai W.-Q., Handsteiner J., Liu B., Yin J., Zhang L., Rauch D., Fink M., Ren J.-G., Liu W.-Y., Li Y., Shen Q., Cao Y., Li F.-Z., Wang J.-F., Huang Y.-M., Deng L.,*

- Xi T., Ma L., Hu T., Li L., Liu N.-L., Koidl F., Wang P., Chen Y.-A., Wang X.-B., Steindorfer M., Kirchner G., Lu C.-Y., Shu R., Ursin R., Scheidl T., Peng C.-Z., Wang J.-Y., Zeilinger A., Pan J.-W. Satellite-Relayed Intercontinental Quantum Network // *Phys. Rev. Lett.* 2018. V. 120. № 3. P. 030501 (4 pp.). <https://doi.org/10.1103/PhysRevLett.120.030501>
7. Chen Y.-A., Zhang Q., Chen T.-Y., Cai W.-Q., Liao S.-K., Zhang J., Chen K., Yin J., Ren J.-G., Chen Z., Han S.-L., Yu Q., Liang K., Zhou F., Yuan X., Zhao M.-S., Wang T.-Y., Jiang X., Zhang L., Liu W.-Y., Li Y., Shen Q., Cao Y., Lu C.-Y., Shu R., Wang J.-Y., Li L., Liu N.-L., Xu F., Wang X.-B., Peng C.-Z., Pan J.-W. An Integrated Space-to-Ground Quantum Communication Network over 4,600 Kilometres // *Nature*. 2021. V. 589. № 7841. P. 214–219. <https://doi.org/10.1038/s41586-020-03093-8>
8. Yin J., Cao Y., Li Y.-H., Liao S.-K., Zhang L., Ren J.-G., Cai W.-Q., Liu W.-Y., Li B., Dai H., Li G.-B., Lu Q.-M., Gong Y.-H., Xu Y., Li S.-L., Li F.-Z., Yin Y.-Y., Jiang Z.-Q., Li M., Jia J.-J., Ren G., He D., Zhou Y.-L., Zhang X.-X., Wang N., Chang X., Zhu Z.-C., Liu N.-L., Chen Y.-A., Lu C.-Y., Shu R., Peng C.-Z., Wang J.-Y., Pan J.-W. Satellite-Based Entanglement Distribution over 1200 Kilometers // *Science*. 2017. V. 356. № 6343. P. 1140–1144. <https://doi.org/10.1126/science.aan3211>
9. Yin J., Li Y.-H., Liao S.-K., Yang M., Cao Y., Zhang L., Ren J.-G., Cai W.-Q., Liu W.-Y., Li S.-L., Shu R., Huang Y.-M., Deng L., Li L., Zhang Q., Liu N.-L., Chen Y.-A., Lu C.-Y., Wang X.-B., Xu F., Wang J.-Y., Peng C.-Z., Ekert A.K., Pan J.-W. Entanglement-Based Secure Quantum Cryptography over 1,120 Kilometres // *Nature*. 2020. V. 582. № 7813. P. 501–505. <https://doi.org/10.1038/s41586-020-2401-y>
10. Ren J.-G., Xu P., Yong H.-L., Zhang L., Liao S.-K., Yin J., Liu W.-Y., Cai W.-Q., Yang M., Li L., Yang K.-X., Han X., Yao Y.-Q., Li J., Wu H.-Y., Wan S., Liu L., Liu D.-Q., Kuang Y.-W., He Z.-P., Shang P., Guo C., Zheng R.-H., Tian K., Zhu Z.-C., Liu N.-L., Lu C.-Y., Shu R., Chen Y.-A., Peng C.-Z., Wang J.-Y., Pan J.-W. Ground-to-Satellite Quantum Teleportation // *Nature*. 2017. V. 549. № 7670. P. 70–73. <https://doi.org/10.1038/nature23675>
11. Beveratos A., Brower R., Gacoin T., Villing A., Poizat J.-P., Grangier P. Single Photon Quantum Cryptography // *Phys. Rev. Lett.* 2002. V. 89. № 18. P. 187901 (4 pp.). <https://doi.org/10.1103/PhysRevLett.89.187901>
12. Stucki D., Gisin N., Guinnard O., Ribordy G., Zbinden H. Quantum Key Distribution over 67 km with a Plug&Play System // *New J. Phys.* 2002. V. 4. P. 41 (8 pp.). <https://doi.org/10.1088/1367-2630/4/1/341>
13. Sasaki M., Fujiwara M., Ishizuka H., Klaus W., Wakui K., Takeoka M., Miki S., Yamashita T., Wang Z., Tanaka A., Yoshino K., Nambu Y., Takahashi S., Tajima A., Tomita A., Domeki T., Hasegawa T., Sakai Y., Kobayashi H., Asai T., Shimizu K., Tokura T., Tsurumaru T., Matsui M., Honjo T., Tamaki K., Takesue H., Tokura Y., Dynes J.F., Dixon A.R., Sharpe A.W., Yuan Z.L., Shields A.J., Uchikoga S., Legre M., Robyr S., Trinkler P., Monat L., Page J.-B., Ribordy G., Poppe A., Allacher A., Maurhart O., Langer T., Peev M., Zeilinger A. Field Test of Quantum Key Distribution in the Tokyo QKD Network // *Opt. Express*. 2011. V. 19. № 11. P. 10387–10409. <https://doi.org/10.1364/OE.19.010387>
14. Wang S., Chen W., Yin Z.-Q., Li H.-W., He D.-Y., Li Y.-H., Zhou Z., Song X.-T., Li F.-Y., Wang D., Chen H., Han Y.-G., Huang J.-Z., Guo J.-F., Hao P.-L., Li M., Zhang C.-M., Liu D., Liang W.-Y., Miao C.-H., Wu P., Guo G.-C., Han Z.-F. Field and Long-Term Demonstration of a Wide Area Quantum Key Distribution Network // *Opt. Express*. 2014. V. 22. № 18. P. 21739–21756. <https://doi.org/10.1364/OE.22.021739>
15. Wang C., Li Y., Cai W., Yang M., Liu W., Liao S., Peng C. Robust Aperiodic Synchronous Scheme for Satellite-to-Ground Quantum Key Distribution // *Appl. Opt.* 2021. V. 60. № 16. P. 4787–4792. <https://doi.org/10.1364/AO.425085>
16. Shakhovoy R., Puplauskis M., Sharoglazova V., Maksimova E., Hydyrova S., Kurochkin V., Duplinskiy A. Wavelength- and Time-Division Multiplexing via Pump Current Variation of a Pulsed Semiconductor Laser—A Method of Synchronization for Quantum Key Distribution // *IEEE J. Quantum Electron.* 2023. V. 59. № 1. Article No. 8000110 (10 pp.). <https://doi.org/10.1109/JQE.2023.3237265>

17. *Calderaro L., Stanco A., Agnesi C., Avesani M., Dequal D., Villoresi P., Vallone G.* Fast and Simple Qubit-Based Synchronization for Quantum Key Distribution // *Phys. Rev. Appl.* 2020. V. 13. № 5. P. 054041 (9 pp.). <https://doi.org/10.1103/PhysRevApplied.13.054041>
18. *Wang C.-Z., Li Y., Cai W.-Q., Liu W.-Y., Liao S.-K., Peng C.-Z.* Synchronization Using Quantum Photons for Satellite-to-Ground Quantum Key Distribution // *Opt. Express.* 2021. V. 29. № 19. P. 29595–29603. <https://doi.org/10.1364/OE.433631>
19. *Takenaka H., Carrasco-Casado A., Fujiwara M., Kitamura M., Sasaki M., Toyoshima M.* Satellite-to-Ground Quantum-Limited Communication Using a 50-kg-Class Microsatellite // *Nat. Photon.* 2017. V. 11. P. 502–508. <https://doi.org/10.1038/nphoton.2017.107>
20. *Lu C.-Y., Cao Y., Peng C.-Z., Pan J.-W.* Micius Quantum Experiments in Space // *Rev. Mod. Phys.* 2022. V. 94. № 3. P. 035001 (46 pp.). <https://doi.org/10.1103/RevModPhys.94.035001>
21. *Хмелев А.В., Дуплинский А.В., Майборода В.Ф., Бахшалиев Р.М., Баланов М.Ю., Курочкин В.Л., Курочкин Ю.В.* Регистрация однофотонного сигнала от низколетящих спутников для целей спутникового квантового распределения ключей // *Письма в ЖТФ.* 2021. Т. 47. № 17. С. 46–49. <https://doi.org/10.21883/PJTF.2021.17.51387.18817>
22. *Khmelev A.V., Duplinsky A.V., Kurochkin V.L., Kurochkin Y.V.* Stellar Calibration of the Single-Photon Receiver for Satellite-to-Ground Quantum Key Distribution // *J. Phys.: Conf. Ser.* 2021. V. 2086. № 1. P. 012137 (5 pp.). <https://doi.org/10.1088/1742-6596/2086/1/012137>
23. *Khmelev A.V., Ivchenko E.I., Miller A.V., Duplinsky A.V., Kurochkin V.L., Kurochkin Yu.V.* Semi-Empirical Satellite-to-Ground Quantum Key Distribution Model for Realistic Receivers // *Entropy.* 2023. V. 25. № 4. P. 670 (14 pp.). <https://doi.org/10.3390/e25040670>
24. *Miller A.V., Pismeniuk L.V., Duplinsky A.V., Merzlinkin V.E., Plukchi A.A., Tikhonova K.A., Nesterov I.S., Sevryukov D.O., Levashov S.D., Fetisov V.V., Krasnopejev S.V., Bakhshaliev R.M.* Vector—Towards Quantum Key Distribution with Small Satellites // *EPJ Quantum Technol.* 2023. V. 10. Article No. 52 (20 pp.). <https://doi.org/10.1140/epjqt/s40507-023-00208-8>
25. *Wu Q.-L., Han Z.-F., Miao E.-L., Liu Y., Dai Y.-M., Guo G.-C.* Synchronization of Free-Space Quantum Key Distribution // *Opt. Commun.* 2007. V. 275. № 2. P. 486–490. <https://doi.org/10.1016/j.optcom.2007.03.068>

Миллер Александр Витальевич
 ООО “Московский центр квантовых технологий”
 avm@mcqt.ru

Поступила в редакцию
 15.11.2023
 После доработки
 08.02.2024
 Принята к публикации
 18.02.2024

УДК 621.391:530.145.1

© 2023 г. Е.Н. Петрова, С.А. Пирогов

ПОЛУРАСПАД И СООТНОШЕНИЕ НЕОПРЕДЕЛЕННОСТЕЙ

Сделана попытка дать точную математическую интерпретацию соотношения неопределенностей “энергия-время”.

Ключевые слова: квантовая механика, соотношение неопределенностей, время полураспада.

DOI: 10.31857/S0555292323040034, **EDN:** VRNUVG

§ 1. Введение

Со времени создания квантовой механики известны два соотношения неопределенностей [1]:

$$\Delta p \cdot \Delta q \sim \hbar, \quad (1)$$

$$\Delta E \cdot \Delta t \sim \hbar. \quad (2)$$

Здесь Δp и Δq – неопределенности импульса и координаты вдоль выбранного направления, а ΔE и Δt – неопределенности энергии и времени.

Первому из них, (1), точный математический смысл придали Э. Кеннард [2] и независимо Г. Вейль [3] в 1927–28 гг. А именно, если под Δp и Δq понимать среднеквадратические отклонения измеряемых величин p и q в каком-либо квантовом состоянии, то

$$\Delta p \cdot \Delta q \geq \frac{1}{2} \hbar.$$

Однако подобная интерпретация соотношения (2) невозможна, потому что квантовая механика не приписывает времени t никакого распределения вероятностей.

Физическая интерпретация соотношения (2) была дана Н. Бором [4]. Однако для нее нелегко найти точную математическую формулировку. Л.Д. Ландау возразил против буквального понимания соотношения (2) фразой: “Кто же мне помешает точно измерить энергию и тут же посмотреть на часы?” [5]. В курсе [6] соотношение (2) интерпретируется через характеристическое время эволюции физической системы, определение которого громоздко и неявно (т. 1, гл. VIII).

Мы хотим связать неопределенность энергии ΔE с такой характеристикой состояния физической системы как время полураспада. Близкая к нашей оценка правой части (2) получена в работе Л.И. Мандельштама и И.Е. Тамма [7] более сложным путем. Для краткости положим $\hbar = 1$.

§ 2. Формулировка

В комплексном линейном пространстве L состояний физической системы считается заданным скалярное произведение $(\cdot, \cdot)$, предполагается, что оно линейно по

второму аргументу и антилинейно по первому. Пространство L мы будем считать полным, т.е. гильбертовым. Будем считать, что динамику системы задает некий самосопряженный оператор, т.е. гамильтониан, H . Состояния системы описываются единичными векторами в пространстве L . При этом, если в момент времени $t = 0$ система находится в состоянии $\psi(0)$, то в момент времени t ее состоянию будет соответствовать вектор

$$\psi(t) = \exp(-itH)\psi(0).$$

Считается, что если система находится в некотором состоянии φ , то вероятность обнаружить ее (при измерении) в состоянии ψ определяется формулой

$$P = |(\varphi, \psi)|^2$$

(“постулат Борна”, см. также [8]). В частности, если в начальный момент времени система находилась в состоянии $\psi(0) = \psi$, то вероятность найти ее через время t в том же самом состоянии ψ равна

$$P(t) = |(\psi, \exp(-itH)\psi)|^2.$$

Поэтому естественно дать следующее

Определение 1. *Временем полураспада* состояния ψ физической системы называется величина

$$T_{1/2} = \inf \left\{ t > 0 : P(t) < \frac{1}{2} \right\}. \quad (3)$$

(Эта величина равна длине отрезка временной оси, начинающегося в нуле, на котором $P(t) \geq \frac{1}{2}$.)

Неопределенность энергии ΔE определяется аналогично неопределенностям Δp и Δq как среднеквадратическое отклонение энергии. Поскольку оператор энергии H (т.е. гамильтониан) является самосопряженным, то для него существует спектральное разложение

$$H = \int E \Pi(dE), \quad (4)$$

где $\Pi(dE)$ – проекторнозначная мера на вещественной оси. Спектральное разложение обобщает представление эрмитова оператора H с простым дискретным спектром в виде

$$H = \sum E_n P_n,$$

где P_n – проектор на вектор состояния с энергией E_n . При этом распределение вероятностей значений энергии в некотором состоянии ψ (которое является единичным вектором в L) задается формулой [9]

$$F(dE) = (\psi, \Pi(dE) \psi). \quad (5)$$

Результат измерения энергии в состоянии ψ является, таким образом, случайной величиной, имеющей распределение $F(dE)$. Обозначим через ξ эту случайную величину. Математическое ожидание, соответствующее распределению F , мы будем обозначать угловыми скобками $\langle \cdot \rangle$. Всегда предполагается, что математическое ожидание $\langle \xi \rangle$ существует и конечно. Обычным образом определяется дисперсия: $\text{Var } \xi = \langle \xi^2 \rangle - \langle \xi \rangle^2$.

Определение 2. *Неопределенностью энергии ΔE в состоянии ψ называется среднеквадратическое уклонение*

$$\Delta E = \sqrt{\text{Var } \xi}.$$

Теорема 1. *В любом состоянии ψ имеет место неравенство*

$$\Delta E \cdot T_{1/2} \geq \sqrt{2 - \sqrt{2}}. \quad (6)$$

§ 3. Доказательство

В силу спектральной теоремы (4) и равенства (5) имеем

$$(\psi, \psi(t)) = \int \exp(-itE) F(dE).$$

Если мы введем характеристическую функцию распределения $F(dE)$ обычным путем как

$$\varphi_F(t) = \int \exp(itE) F(dE),$$

то

$$P(t) = |\varphi_F(t)|^2,$$

и время полураспада можно будет определить формулой

$$T_{1/2} = \inf \left\{ t > 0 : |\varphi_F(t)| < \frac{1}{\sqrt{2}} \right\}.$$

Удобно ввести функцию

$$\chi(t) = \exp(-it\langle \xi \rangle) \varphi_F(t),$$

иначе говоря,

$$\chi(t) = \int \exp(it(E - \langle \xi \rangle)) F(dE).$$

Таким образом, $\chi(t)$ – это характеристическая функция centered величины $\xi - \langle \xi \rangle$. Очевидно, что

$$|\chi(t)| = |\varphi_F(t)|$$

и потому

$$P(t) = |\chi(t)|^2,$$

а значит,

$$T_{1/2} = \inf \left\{ t > 0 : |\chi(t)| < \frac{1}{\sqrt{2}} \right\}.$$

Для функции $\chi(t)$ имеем элементарные равенства

$$\chi(0) = 1, \quad \chi'(0) = 0, \quad \chi''(0) = -\text{Var } \xi,$$

и при любом t

$$\chi''(t) = - \int (E - \langle \xi \rangle)^2 \exp(it(E - \langle \xi \rangle)) F(dE),$$

а значит, при любом t

$$|\chi''(t)| \leq \text{Var } \xi.$$

Отсюда имеем

$$|\chi'(t)| \leq \text{Var } \xi \cdot t, \quad t > 0,$$

$$|1 - \chi(t)| = \left| \int_0^t \chi'(s) ds \right| \leq \text{Var } \xi \cdot \frac{t^2}{2}.$$

Следовательно,

$$\frac{\text{Var } \xi}{2} \cdot T_{1/2}^2 \geq 1 - \frac{1}{\sqrt{2}},$$

$$\Delta E \cdot T_{1/2} \geq \sqrt{2 - \sqrt{2}},$$

т.е. в обычных единицах $\sqrt{2 - \sqrt{2}}\hbar$.

СПИСОК ЛИТЕРАТУРЫ

1. *Ландау Л.Д., Лифшиц Е.М.* Квантовая механика. Нерелятивистская теория. М.: Наука, 1989.
2. *Kennard E.H.* Zur Quantenmechanik einfacher Bewegungstypen // Z. Physik. 1927. V. 44. № 4–5. P. 326–352. <https://doi.org/10.1007/BF01391200>
3. *Weyl H.* Gruppentheorie und Quantenmechanik. Leipzig: Hirzel, 1928.
4. *Bohr N.* Das Quantenpostulat und die neuere Entwicklung der Atomistik // Naturwissenschaften. 1928. V. 16. № 15. P. 245–257. <https://doi.org/10.1007/BF01504968>
5. *Пайерлс Р.* Сюрпризы в теоретической физике. М.: Наука, 1988.
6. *Мессиа А.* Квантовая механика. Т. 1. М.: Наука, 1978.
7. *Мандельштам Л.И., Тамм И.Е.* Соотношение неопределенности энергия – время в нерелятивистской квантовой механике // Изв. АН СССР. Сер. физ. 1945. Т. 9. № 1–2. С. 122–128.
8. *Landau L., Peierls R.* Erweiterung des Unbestimmtheitsprinzips für die relativistische Quantentheorie // Z. Physik. 1931. V. 69. № 1–2. P. 56–69. <https://doi.org/10.1007/BF01391513>
9. *Макки Дж.* Лекции по математическим основам квантовой механики. М.: Мир, 1965.

Петрова Елена Николаевна
Пирогов Сергей Анатольевич
 Институт проблем передачи информации
 им. А.А. Харкевича РАН, Москва
 petrova@iitp.ru
 s.a.pirogov@bk.ru

Поступила в редакцию
 21.01.2024
 После доработки
 28.02.2024
 Принята к публикации
 28.02.2024

УДК 621.391 : 519.872.6

© 2023 г. Б.Я. Лихтциндер, А.Ю. Привалов

**ОБОБЩЕНИЕ ФОРМУЛ ДЛЯ МОМЕНТОВ ОЧЕРЕДИ
ПРИ НЕОРДИНАРНОМ ПУАССОНОВСКОМ ПОТОКЕ
ДЛЯ ОЧЕРЕДЕЙ ПАКЕТОВ В СИСТЕМАХ ТЕЛЕКОММУНИКАЦИЙ**

Предлагается подход для обобщения полученных авторами ранее формул для первого и второго моментов очереди в системе массового обслуживания с неординарным пуассоновским входным потоком, одним прибором и постоянным временем обслуживания на случай переменного времени обслуживания. Время обслуживания предполагается случайной величиной с конечным множеством значений. Эта модель адекватна для широкого класса систем пакетной передачи информации, так как в реальных системах время передачи пакета может принимать только конечное число значений.

Ключевые слова: система массового обслуживания, неординарный входной поток, моменты очереди, интервальный метод анализа очередей, пакетная передача информации.

DOI: 10.31857/S0555292323040046, **EDN:** YRRRNC

§ 1. Введение

Неординарный (групповой) пуассоновский поток [1, 2] может являться простой в анализе альтернативой более сложным моделям телетрафика с долговременными зависимостями, в частности, самоподобным (см., например, [3–6]), если речь идет о приближении статистических характеристик очереди, создаваемой трафиком для передачи в узле связи.

В предлагаемой статье выводятся формулы для первого и второго моментов очереди в системе массового обслуживания (СМО) с одним прибором и неординарным пуассоновским входным потоком для случая, когда время обслуживания заявки является случайной величиной с конечным числом значений. Предлагаемые формулы являются обобщением полученных ранее авторами статьи формул для случая, когда время обслуживания постоянно. При этом использовался интервальный метод (см. [1]).

Интервальный метод основан на определении чисел заявок, поступающих в течение интервалов времени, равных времени обслуживания одной заявки. Вводится понятие мгновенного коэффициента загрузки. Вместо анализа использовавшихся ранее двух вероятностных распределений анализируется одна характеристика – распределение вероятностей мгновенных коэффициентов загрузки. При этом учитывается, что среднее число событий, поступающих за постоянный интервал времени, не зависит от вида закона распределения потока событий.

Заметим, что при моделировании систем пакетной передачи информации, использующих в имеющемся канале конечный набор сигнально-кодовых конструкций, битовая скорость принимает конечное число возможных значений. А поскольку информационный пакет состоит из целого числа байт и при этом максимальный размер

пакета ограничен, то время передачи пакета (моделируемое временем обслуживания заявки) может принимать конечный набор значений.

Обобщение интервального метода на случай такого переменного времени обслуживания нуждается в обосновании, которое и приводится ниже.

§ 2. Обоснование интервального метода для переменного времени обслуживания и пуассоновского входного потока

Уравнение эволюции очереди в системе с одним обслуживающим прибором во время периода занятости прибора может быть записано в виде

$$q_i = q_{i-1} + m(\tau_i) - \delta_i, \quad \text{где} \quad \delta_i = \begin{cases} 0, & \text{если } q_{i-1} = m(\tau_i) = 0, \\ 1 & \text{в противном случае.} \end{cases} \quad (1)$$

Здесь q_i – очередь в момент ухода из системы i -й заявки, τ_i – интервал времени обслуживания i -й заявки, $m(\tau_i)$ – количество пришедших за этот интервал заявок из входного потока. Нетрудно видеть, что в период простоя прибора это уравнение тоже справедливо, причем для любой величины τ_i , а q_{i-1} и q_i – это нулевые очереди на интервалах простоя.

Для постоянного времени обслуживания заявки τ это позволяет рассматривать всю ось времени разделенной на временные окна размера τ , и в каждом таком окне эволюция очереди описывается уравнением (1). Далее в интервальном методе обе части уравнения возводятся в нужную степень, и полученное уравнение, в предположении эргодичности соответствующих случайных процессов и существования стационарного состояния системы, усредняется по реализации для получения уравнения относительно нужных статистических характеристик.

Но для переменного времени обслуживания такой подход встречает трудности при интерпретации уравнения (1) в периоды простоя прибора. Для формулировки подхода в этом случае сделаем несколько достаточно очевидных замечаний:

1. Вероятность для очереди принять какое-то значение при усреднении по реализации – это отношение времени, в течение которого очередь имеет данное значение, к общему времени, на котором рассматривается реализация, при устремлении этого общего времени к бесконечности.
2. Поэтому, если внутри этого большого интервала взять какой-либо период занятости, окруженный с обеих сторон периодами простоя, и менять длины этих периодов простоя так, чтобы их сумма оставалась неизменной (т.е. двигать период занятости по оси времени), то распределение очереди при этом не изменится.
3. Из некоррелированности и стационарности входного пуассоновского потока нетрудно видеть, что при любом таком сдвиге будет получаться возможная для рассматриваемой СМО реализация поведения очереди.

На основании этого перед тем как проводить усреднение по какой-либо реализации, взяв большой интервал времени, определим суммарную продолжительность всех периодов простоя на нем и разделим ее на интервалы, имеющие такое же распределение, как и распределение времени обслуживания. Далее в произвольном порядке расставим эти части между периодами занятости (при необходимости и периоды занятости можно ставить друг за другом, и периоды простоя тоже). Очевидно, что в общем случае только один из получившихся промежутков времени простоя может быть не равен требуемому значению. Но поскольку он будет один и имеет конечную величину по предположению о распределении времени обслуживания, то при устремлении интервала усреднения к бесконечности это не окажет влияния на результат.

Таким образом, мы можем считать, что уравнение (1), в котором τ_i имеет распределение времени обслуживания, справедливо на всей оси времени, и вычислять статистические характеристики очереди в этом предположении.

Далее можно уже действовать аналогично случаю постоянного времени обслуживания. А именно нетрудно видеть, что для δ_i справедливы следующие свойства:

$$(\delta_i)^k = \delta_i, \quad \delta_i m(\tau_i) = m(\tau_i), \quad \delta_i q_{i-1} = q_{i-1}, \quad \overline{m(\tau_i)} = \overline{\delta_i}, \quad (2)$$

где все равенства, кроме последнего, прямо следуют из (1), а усреднение в последнем равенстве берется в стационарном состоянии системы и представляет собой глобальное уравнение статистического баланса. Заметим, что в стационарном состоянии $\overline{m(\tau_i)} = \rho$, где ρ – коэффициент загрузки прибора.

Далее мы кратко приведем некоторые этапы последующих преобразований. Для вывода формулы средней очереди возведем обе части (1) в квадрат, используя при этом свойства (2):

$$(q_i)^2 = (q_{i-1})^2 + m^2(\tau_i) + \delta_i + 2q_{i-1}m(\tau_i) - 2q_{i-1} - 2m(\tau_i).$$

Теперь усредним обе части данного равенства, предполагая стационарное состояние системы, используя последнее равенство в (2), а также то, что в стационарном состоянии $\overline{(q_i)^2} = \overline{(q_{i-1})^2}$, так что эти члены сокращаются:

$$\overline{m^2(\tau_i)} - \overline{m(\tau_i)} + 2\overline{q_{i-1}m(\tau_i)} = 2\overline{q_{i-1}}.$$

Так как при пуассоновском входном потоке $\overline{q_{i-1}m(\tau_i)} = \overline{q_{i-1}} \cdot \overline{m(\tau_i)}$ вследствие независимости текущей очереди и следующих прибытий из входного потока, то

$$2\overline{q_{i-1}}(1 - \overline{m(\tau_i)}) = \overline{m^2(\tau_i)} - \overline{m(\tau_i)}.$$

Отсюда

$$\overline{q_{i-1}} = \frac{\overline{m^2(\tau_i)} - \overline{m(\tau_i)}}{2(1 - \overline{m(\tau_i)})}.$$

Если в числителе правой части вычесть и прибавить $\overline{m^2(\tau_i)}$ и использовать стандартное обозначение для дисперсии, то формула для средней очереди примет вид

$$\overline{q} = \frac{\mathbf{D}(m(\tau))}{2(1 - \rho)} - \frac{\rho}{2}. \quad (3)$$

Для получения формулы для второго момента очереди обе части уравнения (1) надо возвести в третью степень:

$$(q_i)^3 = (q_{i-1})^3 + 3(q_{i-1})^2(m(\tau_i) - \delta_i) + 3q_{i-1}(m(\tau_i) - \delta_i)^2 + (m(\tau_i) - \delta_i)^3.$$

После раскрытия скобок, применения свойств (2) и выделения общих множителей получим

$$(q_i)^3 = (q_{i-1})^3 + 3(q_{i-1})^2(m(\tau_i) - 1) + 3q_{i-1}(m^2(\tau_i) - 2m(\tau_i) + 1) + m^3(\tau_i) - 3m^2(\tau_i) + 3m(\tau_i) - \delta_i.$$

Усредняя это равенство в стационарном состоянии, учитывая, что в этом случае $(q_i)^3 = (\overline{q_{i-1}})^3$, и применяя последнее равенство в (2), получаем

$$3\overline{(q_{i-1})^2 m(\tau_i)} - 3\overline{(q_{i-1})^2} + 3\overline{q_{i-1} m^2(\tau_i)} - 6\overline{q_{i-1} m(\tau_i)} + 3\overline{q_{i-1}} + \overline{m^3(\tau_i)} - 3\overline{m^2(\tau_i)} + 2\overline{m(\tau_i)} = 0.$$

Аналогично предыдущему случаю, пользуясь независимостью текущей очереди и будущих прибытий из входного пуассоновского потока, получаем

$$\overline{(q_{i-1})^2} (1 - \overline{m(\tau_i)}) = \overline{q_{i-1}} (\overline{m^2(\tau_i)} - 2\overline{m(\tau_i)} + 1) + \frac{\overline{m^3(\tau_i)} - 3\overline{m^2(\tau_i)} + 2\overline{m(\tau_i)}}{3}.$$

Добавляя и вычитая $\overline{m^2(\tau_i)}$ в скобках в правой части, несложно получить формулу

$$\overline{q^2} = \frac{\overline{q}}{(1 - \overline{m(\tau_i)})} (\mathbf{D}(m(\tau_i)) + (1 - \overline{m(\tau_i)})^2) + \frac{\overline{m^3(\tau_i)} - 3\overline{m^2(\tau_i)} + 2\overline{m(\tau_i)}}{3(1 - \overline{m(\tau_i)})},$$

и после подстановки выражения для $\overline{q}$ выражение для второго момента очереди примет вид

$$\overline{q^2} = \frac{\overline{m^2(\tau_i)} - \rho}{2} \left(\frac{\mathbf{D}(m(\tau_i))}{(1 - \rho)^2} + 1 \right) + \frac{\overline{m^3(\tau_i)} - 3\overline{m^2(\tau_i)} + 2\rho}{3(1 - \rho)}. \quad (4)$$

Таким образом, моменты размеров очереди зависят только от моментов чисел заявок, приходящих в систему в течение случайных интервалов времени обслуживания с заданным распределением вероятностей.

В следующем параграфе найдем необходимые моменты чисел заявок, приходящих в течение случайного интервала времени обслуживания.

§ 3. Моменты количества заявок, приходящих за интервал обслуживания

Рассмотрим пуассоновский поток с параметром λ независимых событий, i -е из которых ($i = 1, 2, \dots$) есть одновременное прибытие пачки пакетов для передачи, где размеры пачек B_i – независимые одинаково распределенные случайные величины с заданным распределением $\Pr(B_i = k) = f_k$, $k = 1, 2, \dots$. Все пакеты поступают в буфер, где образуют очередь для передачи. Времена передачи τ_i каждого пакета являются независимыми одинаково распределенными дискретными случайными величинами с заданным распределением $\Pr(\tau_i = t_k) = p_k$, $k = 1, 2, \dots, K$.

Для применения формул (3) и (4) вычислим моменты $m(\tau_i)$ с помощью производящих функций. Пусть $f(z) = \sum_{k=1}^{\infty} f_k z^k$ – производящая функция размера пачки. Тогда для производящей функции случайной величины $m(\tau_i)$ имеем

$$G_{m(\tau_i)}(z) = \sum_{k=1}^K \Pr(\tau_i = t_k) \sum_{n=0}^{\infty} \frac{(\lambda t_k)^n}{n!} e^{-\lambda t_k} (f(z))^n = \sum_{k=1}^K p_k e^{\lambda t_k (f(z) - 1)},$$

где использовалась пуассоновость потока пачек. Тогда

$$\begin{aligned} \left. \frac{\partial G_{m(\tau_i)}(z)}{\partial z} \right|_{z=1} &= \sum_{k=1}^K p_k \lambda t_k f'(z) e^{\lambda t_k (f(z) - 1)} \Big|_{z=1} = \lambda \overline{B} \sum_{k=1}^K p_k t_k = \\ &= \lambda \overline{\tau B} = \overline{m(\tau_i)}, \end{aligned} \quad (5)$$

где $\overline{B}$ и $\overline{\tau}$ – математические ожидания соответствующих случайных величин. Аналогично

$$\begin{aligned} \frac{\partial^2 G_{m(\tau_i)}(z)}{(\partial z)^2} \Big|_{z=1} &= \sum_{k=1}^K p_k (\lambda t_k f''(z) + (\lambda t_k f'(z))^2) e^{\lambda t_k (f(z)-1)} \Big|_{z=1} = \\ &= \lambda \overline{\tau} (\overline{B^2} - \overline{B}) + \overline{\tau^2} (\lambda \overline{B})^2 = \overline{m^2(\tau_i)} - \overline{m(\tau_i)}, \end{aligned}$$

откуда

$$\overline{m^2(\tau_i)} = \lambda \overline{\tau} \overline{B^2} + \overline{\tau^2} (\lambda \overline{B})^2, \quad (6)$$

$$\mathbf{D}(m(\tau_i)) = \lambda \overline{\tau} \overline{B^2} + (\lambda \overline{B})^2 (\overline{\tau^2} - (\overline{\tau})^2) = \lambda \overline{\tau} \overline{B^2} + (\lambda \overline{B})^2 \mathbf{D}(\tau). \quad (7)$$

Аналогично

$$\begin{aligned} \frac{\partial^3 G_{m(\tau_i)}(z)}{(\partial z)^3} &= \sum_{k=1}^K p_k (\lambda t_k f'''(z) + 3(\lambda t_k)^2 f'(z) f''(z) + (\lambda t_k f'(z))^3) \times \\ &\times e^{\lambda t_k (f(z)-1)} \Big|_{z=1} = \lambda \overline{\tau} (\overline{B^3} - 3\overline{B^2} + 2\overline{B}) + 3\lambda^2 \overline{\tau^2} \overline{B} (\overline{B^2} - \overline{B}) + (\lambda \overline{B})^3 \overline{\tau^3} = \\ &= \overline{m^3(\tau_i)} - 3\overline{m^2(\tau_i)} + 2\overline{m(\tau_i)}, \end{aligned}$$

откуда

$$\begin{aligned} \overline{m^3(\tau_i)} &= \lambda \overline{\tau} (\overline{B^3} - 3\overline{B^2} + 2\overline{B}) + 3\lambda^2 \overline{\tau^2} \overline{B} (\overline{B^2} - \overline{B}) + (\lambda \overline{B})^3 \overline{\tau^3} + \\ &+ 3(\lambda \overline{\tau} \overline{B^2} + \overline{\tau^2} (\lambda \overline{B})^2) - 2\lambda \overline{\tau} \overline{B} = \lambda \overline{\tau} \overline{B^3} + 3\lambda^2 \overline{\tau^2} \overline{B} \overline{B^2} + (\lambda \overline{B})^3 \overline{\tau^3}. \end{aligned} \quad (8)$$

Подставляя (5)–(8) в (3) и (4), получим

$$\overline{q} = \frac{\lambda \overline{\tau} \overline{B^2} + (\lambda \overline{B})^2 \mathbf{D}(\tau)}{2(1 - \lambda \overline{\tau} \overline{B})} - \frac{\lambda \overline{\tau} \overline{B}}{2} = \frac{\lambda \overline{\tau} \overline{B^2} + (\lambda \overline{B})^2 \mathbf{D}(\tau)}{2(1 - \rho)} - \frac{\rho}{2}, \quad (9)$$

$$\begin{aligned} \overline{q^2} &= \frac{(\lambda \overline{\tau} \overline{B^2} + (\lambda \overline{B})^2 \overline{\tau^2} - \rho)(\lambda \overline{\tau} \overline{B^2} + (\lambda \overline{B})^2 \mathbf{D}(\tau) + (1 - \rho)^2)}{2(1 - \rho)^2} + \\ &+ \frac{\lambda \overline{\tau} (\overline{B^3} - 3\overline{B^2} + 2\overline{B}) + 3\lambda^2 \overline{\tau^2} \overline{B} (\overline{B^2} - \overline{B}) + (\lambda \overline{B})^3 \overline{\tau^3}}{3(1 - \rho)} = \\ &= \frac{(\lambda \overline{\tau} \overline{B^2} + (\lambda \overline{B})^2 \mathbf{D}(\tau))^2 - (1 - \rho)(\lambda \overline{\tau} \overline{B^2} + (\lambda \overline{B})^2 \mathbf{D}(\tau) - \rho(1 - \rho)^2)}{2(1 - \rho)^2} + \\ &+ \frac{\lambda \overline{\tau} (\overline{B^3} - 3\overline{B^2} + 2\overline{B}) + 3\lambda^2 \overline{\tau^2} \overline{B} (\overline{B^2} - \overline{B}) + (\lambda \overline{B})^3 \overline{\tau^3}}{3(1 - \rho)}. \end{aligned} \quad (10)$$

Если в формулах (5)–(8) положить $\tau_i = \text{const}$, то получатся соответствующие формулы из [1], при этом (9) и (10) также превратятся в их аналоги из [1].

А если при случайном τ_i положить $B = 1$, т.е. перейти от группового пуассоновского входного потока к ординарному, то (9) и (10) превратятся в формулы Поллачека – Хинчина для первого и второго начальных моментов очереди в системе $M/G/1$.

§ 4. Заключение

В статье представлены формулы для первых двух моментов очереди в системе с одним прибором, неординарным пуассоновским потоком на входе и временем обслуживания, являющимся случайной величиной с конечным числом значений. При

переходе к постоянному времени обслуживания или к ординарному пуассоновскому потоку представленные формулы превращаются в известные формулы для этих случаев. Предложенный подход в принципе может быть использован для вывода формул моментов очереди и более высоких порядков.

СПИСОК ЛИТЕРАТУРЫ

1. *Лихтциндер Б.Я., Привалов А.Ю., Моисеев В.И.* Неординарные пуассоновские модели трафика мультисервисных сетей // Пробл. передачи информ. 2023. Т. 59. № 1. С. 71–79. <https://www.mathnet.ru/ppi2392>
2. *Лихтциндер Б.Я.* Трафик мультисервисных сетей доступа (интервальный анализ и проектирование). М.: Науч.-тех. изд-во «Горячая линия – Телеком», 2019.
3. *Yunhua R.* Evaluation and Estimation of Second-Order Self-similar Network Traffic // Comput. Commun. 2004. V. 27. № 9. P. 898–904. <https://doi.org/10.1016/j.comcom.2004.02.003>
4. *Privalov A.Yu., Tsarev A.* Analysis and Simulation of WAN Traffic by Self-similar Traffic Model with OMNET // Proc. 10th Int. Wireless Communications and Mobile Computing Conf. (IWCMC'2014). Nicosia, Cyprus. Aug. 4–8, 2014. P. 629–634. <https://doi.org/10.1109/IWCMC.2014.6906429>
5. *Millán Naveas G., San Juan Urrutia E., Vargas Guzmán M.* A Simple Multifractal Model for Self-similar Traffic Flows in High-Speed Computer Networks // Comp. y Sist. 2019. V. 23. № 4. P. 1517–1521. <https://doi.org/10.13053/cys-23-4-2831>
6. *Вишневский В.М., Дудин А.Н.* Системы массового обслуживания с коррелированными входными потоками и их применение для моделирования телекоммуникационных сетей // Автомат. и телемех. 2017. № 8. С. 3–59. <https://www.mathnet.ru/rus/at14562>

Лихтциндер Борис Яковлевич

Поволжский государственный университет
телекоммуникаций и информатики, Самара
b.lihtcinder@psuti.ru

Привалов Александр Юрьевич

Самарский национальный исследовательский университет
им. академика С.П. Королева
Поволжский государственный университет
телекоммуникаций и информатики, Самара
privalov1967@gmail.com

Поступила в редакцию

17.01.2024

После доработки

03.02.2024

Принята к публикации

08.02.2024

Алексеев И.А. см. Угловский А.Ю. и др.

Башконуш Х.М. см. Гао В. и др.

Боржес Ж., Зиновьев В.А., Зиновьев Д.В. О перечислении полностью регулярных кодов с радиусом покрытия два и дуальными антиподальными кодами 3 26

Воробьев И.В. Покрывающие коды для метрики Левенштейна фиксированной длины 2 18

Вялый М.Н. О проверке выполнимости алгебраических формул над полем из двух элементов 1 64

Гао В., Башконуш Х.М., Каттани К. Эффективность передачи данных при атаках с точки зрения варианта изолированной жесткости 2 83

Голубев Г.К. Перепараметризованные тесты максимального правдоподобия для обнаружения разреженных векторов 1 46

Дворкин Г.Д. Геометрическая интерпретация энтропии софических систем ... 2 49

Докучаев Н.Г. Почти идеальные предикторы и каузальные фильтры для дискретных сигналов 2 32

Жижина Е.А., Пирогов С.А. Инвариантные меры для процессов контактов с интенсивностями рождения и гибели, зависящими от состояния 2 63

Зиновьев В.А. см. Боржес Ж. и др.

Зиновьев Д.В. см. Боржес Ж. и др.

Илларионов А.А. Существование последовательностей, удовлетворяющих рекуррентным соотношениям билинейного типа. 2 102

Кабатянский Г.А. см. Фернандес М. и др.

Каттани К. см. Гао В. и др.

Колесников С.Г., Леонтьев В.М. Серии формул для параметров Бхаттачарьи в теории полярных кодов 1 3

Круглик С.А. см. Фернандес М. и др.

Куреев А.А. см. Угловский А.Ю. и др.

Леонтьев В.М. см. Колесников С.Г.

Лихтциндер Б.Я., Привалов А.Ю., Мойсеев В.И. Неординарные пуассоновские модели трафика мультисервисных сетей 1 71

Лихтциндер Б.Я., Привалов А.Ю. Обобщение формул для моментов очереди при неординарном пуассоновском потоке для очередей пакетов в системах телекоммуникаций 4 32

Мельников И.А. см. Угловский А.Ю. и др.

Миллер А.В. Синхронизация времени в спутниковом квантовом распределении ключей 4 13

Могильных И.Ю., Соловьева Ф.И. Конструкции и инварианты оптимальных кодов в метрике Ли	2	3
Моисеев В.И. см. Лихтциндер Б.Я. и др.		
Мяо И. см. Фернандес М. и др.		
Петрова Е.Н., Пирогов С.А. Полураспад и соотношение неопределенностей ...	4	28
Пирогов С.А. см. Жижина Е.А.		
Пирогов С.А. см. Петрова Е.Н.		
Привалов А.Ю. см. Лихтциндер Б.Я.		
Привалов А.Ю. см. Лихтциндер Б.Я. и др.		
Соловьева Ф.И. см. Могильных И.Ю.		
Станоевич И., Шенк В. Сверточные коды с оптимальным двусторонним профилем расстояний	3	3
Трифонов П.В. Построение и декодирование полярных кодов с большими ядрами: обзор	1	25
Угловский А.Ю., Мельников И.А., Алексеев И.А., Куреев А.А. Оценка низкого уровня ошибок с помощью выборки по значимости с равномерным распределением	4	3
Фернандес М., Кабатянский Г.А., Круглик С.А., Мяо И. Коды для точного нахождения носителя разреженного вектора по ошибочным линейным измерениям и их декодирование	1	17
Шенк В. см. Станоевич И.		

Р е д к о л л е г и я :

Главный редактор А.Н. СОБОЛЕВСКИЙ

**А.М. БАРГ, Л.А. БАССАЛЫГО, В.А. ЗИНОВЬЕВ, В.В. ЗЯБЛОВ,
И.А. ИБРАГИМОВ, Н.А. КУЗНЕЦОВ (зам. главного редактора),
В.А. МАЛЫШЕВ, Д.Ю. НОГИН (ответственный секретарь),
В.М. ТИХОМИРОВ, Ю.Н. ТЮРИН, Б.С. ЦЫБАКОВ**

Зав. редакцией *С.В. ЗОЛОТАЙКИНА*

Адрес редакции: 127051, Москва, Б. Каретный пер., 19, стр. 1, тел. (495) 650-47-39

Оригинал-макет подготовил *Д.Ю. Ногин*

**Москва
ФГБУ Издательство «Наука»**