SN:
2181-3906
2026

International scientific journal
«MODERN SCIENCE AND RESEARCH»
VOLUME 5 / ISSUE 6 / UIF:8.2 / MODERNSCIENCE.UZ

**УДК 004.056.55:530.145**

# МАТЕМАТИЧЕСКОЕ МОДЕЛИРОВАНИЕ ПАРАМЕТРОВ ЭФФЕКТИВНОСТИ ПРОТОКОЛА BB84 В СИСТЕМЕ КВАНТОВОГО РАСПРЕДЕЛЕНИЯ КЛЮЧЕЙ

**Maksud Khamidov Maxmudovich** [1]

[1] Самаркандский государственный университет имени Шарофа Рашидова.
Самарканд, Узбекистан.

***E-mail:*** *mhamidov758@gmail.com*

ORCID: 0009-0007-1649-4008

***https://doi.org/10.5281/zenodo.20617833***

***Аннотация.*** *В статье изучается математическая модель оценки эффективности протокола BB84 в системе квантового распределения ключей. Основное внимание уделено параметрам канала, вероятности регистрации фотона, уровню ошибок и итоговой длине секретного ключа. Для описания процесса использованы выражения, связывающие длину оптического канала, коэффициент затухания, среднее число фотонов, эффективность детектора и вероятность темнового отсчёта. Такой подход позволяет заранее оценить поведение QKD-системы без проведения сложного физического эксперимента. В работе показано, что даже простая модель BB84 даёт полезную картину: рост длины канала снижает вероятность регистрации, а темновые отсчёты заметно влияют на качество ключа. Модель может использоваться в учебных и предварительных инженерных расчётах.*

***Ключевые слова:*** *BB84, QKD, вероятность регистрации, квантовая криптография, квантовое распределение ключей, квантовый канал, математическое моделирование, секретный ключ.*

# BB84 PROTOKOLI ASOSIDA KVANT KALIT TAQSIMLASH TIZIMI SAMARADORLIK PARAMETRLARINI MATEMATIK MODELLASHTIRISH

***Annotatsiya.*** *Maqolada BB84 protokoli asosida kvant kalit taqsimlash tizimining samaradorlik parametrlarini baholash uchun matematik model o‘rganiladi. Asosiy e’tibor kanal parametrlariga, fotonni qayd etish ehtimoliga, xatolik darajasiga va yakuniy maxfiy kalit uzunligiga qaratilgan. Jarayonni tavsiflash uchun optik kanal uzunligi, so‘nish koeffitsienti, fotonlarning o‘rtacha soni, detektor samaradorligi va qorong‘i sanash ehtimolini bog‘lovchi ifodalar ishlatiladi. Ushbu yondashuv murakkab fizik tajribasiz QKD tizimining xatti-harakatini oldindan baholash imkonini beradi. Ishda oddiy BB84 modeli ham foydali natija berishi ko‘rsatiladi: kanal uzunligi ortishi qayd etish ehtimolini kamaytiradi, qorong‘i sanashlar esa kalit sifatiga sezilarli ta’sir qiladi. Model o‘quv va dastlabki muhandislik hisob-kitoblarida qo‘llanishi mumkin.*

***Kalit so‘zlar:*** *BB84, kvant kalit taqsimlash, kvant kanali, kvant kriptografiyasi, matematik modellashtirish, maxfiy kalit, qayd etish ehtimoli, QKD.*

# MATHEMATICAL MODELING OF BB84 PROTOCOL EFFICIENCY PARAMETERS IN A QUANTUM KEY DISTRIBUTION SYSTEM

***Abstract.*** *The article studies a mathematical model for evaluating the efficiency parameters of the BB84 protocol in a quantum key distribution system. The main attention is paid to channel parameters, photon detection probability, error level and final secret key length. The model uses expressions that connect optical channel length, attenuation coefficient, mean photon number, detector efficiency and dark count probability.*

*This approach makes it possible to estimate the behavior of a QKD system without a complex physical experiment. The paper shows that even a simple BB84 model gives a useful picture: increasing the channel length reduces the detection probability, while dark counts noticeably affect the key quality. The model can be used for educational purposes and preliminary engineering calculations.*

***Key words:*** *BB84, detection probability, mathematical modeling, QKD, quantum channel, quantum cryptography, quantum key distribution, secret key.*

## I. ВВЕДЕНИЕ

Квантовая криптография заняла особое место в исследованиях по защите информации. Причина понятна. Классические криптографические методы опираются на вычислительную сложность отдельных математических задач. Квантовое распределение ключей, напротив, использует физические свойства квантовых состояний. На бумаге это звучит красиво. В практической системе всё сразу становится грубее: потери в канале, шумы, темновые отсчёты, неидеальные детекторы.

Протокол BB84 был предложен Ч. Беннетом и Ж. Брассаром в 1984 году. В первоначальной работе была показана идея передачи ключевой информации через квантовые состояния, где попытка несанкционированного измерения меняет состояние передаваемого объекта [1]. Позже безопасность BB84 получила более строгие теоретические обоснования, в том числе в работе Шора и Прескилла [10]. Для современной криптографии это уже не экзотика, а отдельное направление, вокруг которого формируются стандарты и инженерные требования.

Актуальность темы усилилась после перехода мирового сообщества к постквантовой повестке. В 2024 году NIST опубликовал первые завершённые стандарты постквантового шифрования, рассчитанные на защиту от атак с применением квантовых компьютеров [7].

Это не делает QKD ненужной. Скорее наоборот. Постквантовые алгоритмы и квантовое распределение ключей работают по разным принципам. ETSI прямо указывает, что QKD может применяться как дополнительная квантово-безопасная техника в многоуровневых системах киберзащиты [3].

При этом у протокола BB84 есть неприятная для инженера сторона. Его эффективность нельзя оценивать только по красивой схеме «Алиса - канал - Боб». Нужны численные параметры. Длина канала влияет на затухание.

Затухание меняет вероятность регистрации фотона. Темновые отсчёты дают ложные срабатывания. После этого меняется доля ошибок, а затем и итоговая длина секретного ключа.

Цель данной статьи - построить компактную математическую модель для оценки параметров эффективности протокола BB84 в системе квантового распределения ключей.

Для достижения цели выделены следующие задачи: описать основные параметры QKD-системы, задать модель вероятности регистрации фотона, определить зависимость длины секретного ключа от параметров канала и детектора.

Объектом исследования является система квантового распределения ключей на основе протокола BB84.

Предметом исследования выступают математические зависимости между параметрами квантового канала, характеристиками детектора и итоговыми показателями формирования секретного ключа.

Практический смысл работы простой. До физического эксперимента желательно понять, где система начнёт терять эффективность. Модель не заменяет лабораторную установку. Зато она быстро показывает слабые места. В этом её скромная, но полезная сила.

**II. МАТЕРИАЛЫ И МЕТОДЫ**

Протокол BB84 относится к схемам prepare-and-measure. Алиса подготавливает квантовые состояния, Боб измеряет их в выбранных базисах. После передачи стороны сравнивают только информацию о базисах, но не раскрывают сами биты. Если базисы совпали, бит может попасть в просеянный ключ. Если не совпали, результат удаляется.

В идеальном описании всё выглядит почти безупречно. В реальной системе часть фотонов теряется. Часть событий появляется из-за шума. Детектор имеет конечную эффективность. Поэтому модель BB84 должна учитывать не только логическую схему протокола, но и параметры физического канала.

В данной работе используется упрощённая модель канала с затуханием. Коэффициент передачи канала задаётся выражением:

$$k = 10^{-\frac{\alpha L}{10}}, \quad (1)$$

где $k$ - коэффициент передачи канала, $\alpha$ - коэффициент затухания, $L$ - длина канала.

Вероятность регистрации сигнального фотона определяется через среднее число фотонов $\mu$, коэффициент передачи $k$ и эффективность детектора $\eta$:

$$P_{sig} = 1 - e^{-\mu k \eta}, \quad (2)$$

где $P_{sig}$ - вероятность регистрации полезного сигнала, $\mu$ - среднее число фотонов в импульсе, $\eta$ - эффективность детектора.

Темновой отсчёт вносится отдельно. Он связан с ложным срабатыванием детектора при отсутствии полезного фотона. В практических системах этот параметр нельзя спокойно игнорировать. При малой вероятности полезного сигнала даже слабый шум становится заметным.

Общая вероятность клика детектора задаётся так:

$$P_{click} = 1 - (1 - P_{sig})(1 - P_{dark}), \quad (3)$$

где $P_{click}$ - полная вероятность регистрации события, $P_{dark}$ - вероятность темнового отсчёта.

Для оценки квантовой битовой ошибки используется приближённое отношение:

$$Q = \frac{P_{dark}}{P_{click}}, \quad 4)$$

где $Q$ - уровень ошибок. Модель грубая, но честная для предварительного анализа. Она показывает, насколько ложные события могут исказить итоговую картину.

Число просеянных битов после сравнения базисов определяется выражением:

$$N_s = 0.5 \cdot P_{click} \cdot N_i, \quad 5)$$

где $N_s$ - число просеянных битов, $N_i$ - число отправленных импульсов. Множитель 0.5 связан с тем, что в BB84 базисы Алисы и Боба совпадают примерно в половине случаев.

После этапа оценки ошибок и коррекции часть битов исключается. В упрощённой форме это можно записать так:

$$N_e = (1 - p_e) \cdot N_s, \quad 6)$$

где $N_e$ - число битов после учёта ошибок, $p_e$ - доля ошибок или потерь на этапе обработки.

Итоговая длина секретного ключа задаётся выражением:

$$N_f = \max(N_e - t - s, 0), \quad 7)$$

где $N_f$ - итоговая длина секретного ключа, $t$ - количество битов, потерянных при проверке, $s$ - количество битов, удалённых при усилении секретности.

**Таблица 1. Основные параметры математической модели BB84**

| Обозначение | Содержание параметра | Роль в модели |
|---|---|---|
| $N_i$ | число отправленных импульсов | задаёт исходный объём передачи |
| $\mu$ | среднее число фотонов | влияет на вероятность сигнала |
| $L$ | длина канала | усиливает потери |
| $\alpha$ | коэффициент затухания | описывает ослабление сигнала |
| $\eta$ | эффективность детектора | влияет на регистрацию фотонов |
| $P_{dark}$ | вероятность темнового отсчёта | создаёт ложные события |
| $p_e$ | доля ошибок обработки | уменьшает полезный ключ |
| $t, s$ | параметры сокращения ключа | учитывают проверку и усиление секретности |

Метод исследования основан на последовательном расчёте параметров. Сначала определяется передача канала.

Затем вычисляется вероятность полезной регистрации. После этого учитывается темновой отсчёт. На последнем этапе оценивается число битов, которое может остаться в секретном ключе.

Такой порядок не выглядит сложным. Но именно он удобен для программной реализации. Пользователь меняет один параметр, а система пересчитывает всю цепочку. В учебной работе это особенно важно: формулы перестают быть отдельными строками и начинают работать как единая модель.

Для численного примера используются условные параметры, близкие к типовым оценкам в учебном моделировании:

$N_i = 2 \cdot 10^6$, $\mu = 0.1$, $\alpha = 0.2$ дБ/км, $\eta = 0.1$, $P_{dark} = 10^{-5}$, $p_e = 0.05$, $t = 1000$, $s = 2000$.

Длина канала изменяется от 10 до 100 км. Такой диапазон выбран не случайно. На малых расстояниях влияние затухания умеренное. На больших расстояниях потери становятся уже слишком заметными, особенно при слабых импульсах.

## III. РЕЗУЛЬТАТЫ И ОБСУЖДЕНИЕ

Расчёт по формулам (1) – (7) показывает ожидаемую, но всё равно неприятную картину. При росте длины канала коэффициент передачи $k$ уменьшается. Вместе с ним падает вероятность регистрации полезного сигнала $P_{sig}$. Детектор начинает чаще работать в режиме, где полезный сигнал слаб, а темновые отсчёты уже не выглядят мелкой поправкой.

**Таблица 2. Расчёт параметров BB84 при разных длинах канала**

| Длина канала, км | | | | | , бит |
|---|---|---|---|---|---|
| **10** | 0.6310 | 0.006290 | 0.006300 | 0.0016 | 2985 |
| **25** | 0.3162 | 0.003157 | 0.003167 | 0.0032 | 9 |
| **50** | 0.1000 | 0.001000 | 0.001009 | 0.0099 | 0 |
| **75** | 0.0316 | 0.000316 | 0.000326 | 0.0307 | 0 |
| **100** | 0.0100 | 0.000100 | 0.000110 | 0.0909 | 0 |

По таблице видно, что даже при достаточно большом числе отправленных импульсов итоговая длина ключа быстро уменьшается. При выбранных параметрах положительный результат сохраняется только на малой длине канала.

При длине канала 10 км итоговая длина секретного ключа составляет 2985 бит. При увеличении расстояния до 25 км значение $N_f$ уменьшается до 9 бит, что уже почти не имеет практического смысла. Начиная с 50 км, при выбранных параметрах модель даёт нулевую итоговую длину ключа.

Особенно важен параметр $Q$. Его рост связан не только с увеличением шума. Он связан с тем, что полезный сигнал становится малым. Один и тот же уровень темновых отсчётов при коротком канале выглядит почти незаметно. При длинном канале он уже портит общую статистику.

SN:
2181-3906
2026

International scientific journal
«MODERN SCIENCE AND RESEARCH»
VOLUME 5 / ISSUE 6 / UIF:8.2 / MODERNSCIENCE.UZ

Это одна из причин, почему практические QKD-системы требуют тщательного выбора детекторов. В обзоре Хэдфилда отдельно подчёркивается значение однофотонных детекторов для квантовых оптических приложений [4]. В работах по практической безопасности QKD также показано, что реальные устройства нельзя заменять идеальными элементами без потери смысла анализа [9].

Для улучшения дальности и скорости генерации ключа в литературе часто применяются decoy-state методы. В работе Lo, Ma и Chen предложена схема decoy-state QKD, направленная на повышение защищённости практических систем при использовании слабых когерентных импульсов [6]. В дальнейшем Ma, Qi, Zhao и Lo представили практическую схему с двумя decoy-состояниями и одним сигнальным состоянием [5]. Для данной статьи эти методы не включаются в расчётную модель. Но их наличие важно.

Простая модель BB84 показывает проблему, а decoy-state подходи уже пытаются её смягчить.

Если представить результаты графически, то зависимость $N_f(L)$ имеет резкий спад.

На первом участке система ещё формирует ключ. Затем наступает область, где итоговая длина ключа становится нулевой. Такая форма зависимости удобна для предварительной настройки параметров. Можно быстро понять, при какой длине канала выбранная конфигурация теряет практический смысл.

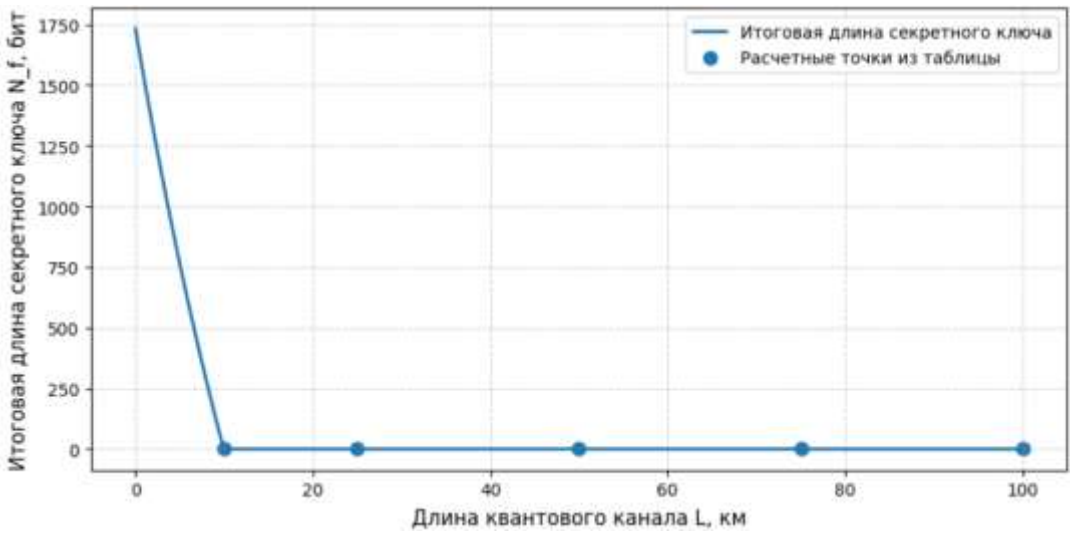


**РИСУНОК 1. Качественная зависимость итоговой длины секретного ключа от длины квантового канала**

На РИСУНКЕ 1 показана убывающая кривая: по горизонтальной оси откладывается длина канала $L$, по вертикальной - итоговая длина секретного ключа $N_f$. В начальной области значение $N_f$ положительно. Далее кривая опускается к нулю.

Отдельного внимания заслуживает параметр $\mu$. Если среднее число фотонов слишком мало, полезных регистраций будет недостаточно. Если оно слишком велико, возрастает риск, связанный с многофотонными импульсами. Именно здесь простая модель BB84 начинает скрипеть.

Она удобна для первичной оценки, но не закрывает всю задачу безопасности. В серьёзной инженерной работе потребуется более полный анализ, включая тип источника, статистику фотонов и метод усиления секретности.

Результаты можно обобщить в виде нескольких рабочих наблюдений.

Первое. Длина канала является одним из главных факторов снижения эффективности. Это связано с экспоненциальным характером затухания в формуле (1).

Второе. Вероятность клика детектора зависит не только от полезного сигнала.

Темновые отсчёты могут казаться малыми, но при длинном канале их вклад становится грубым.

Третье. Итоговая длина секретного ключа чувствительна к параметрам постобработки. Даже если просеянный ключ существует, проверка и усиление секретности могут полностью его обнулить.

Эти наблюдения выглядят немного сурово. Но в этом и есть польза моделирования.

Оно не обещает красивый результат заранее. Оно показывает, где система перестаёт быть удобной.

С точки зрения области применения данная модель может использоваться в трёх направлениях. Во-первых, в учебных курсах по квантовой криптографии. Во-вторых, при предварительном выборе параметров QKD-системы. В-третьих, как основа для программного модуля, где пользователь меняет входные параметры и сразу получает расчёт ключевых показателей.

В сравнении с обзорными работами по QKD данная статья имеет более узкую цель.

Обзоры Gisin и соавторов, Scarani и соавторов, Pirandola и соавторов дают широкую картину развития квантовой криптографии [2], [8], [9]. Здесь задача скромнее. Нужно показать, как небольшая система формул помогает оценить эффективность BB84 на уровне базового моделирования.

## IV. ВЫВОДЫ

В статье построена математическая модель оценки параметров эффективности протокола BB84 в системе квантового распределения ключей. Модель включает коэффициент передачи канала, вероятность регистрации полезного сигнала, вероятность клика детектора, уровень ошибок и итоговую длину секретного ключа.

Полученные расчёты показывают, что рост длины квантового канала быстро уменьшает вероятность регистрации фотона. При этом темновые отсчёты начинают сильнее влиять на уровень ошибок. В результате итоговая длина секретного ключа может стать нулевой даже при большом числе отправленных импульсов.

Практическая ценность модели связана с её простотой. Она подходит для учебного анализа и предварительной оценки QKD-системы. Конечно, для промышленной реализации одной такой модели мало. Нужны более точные данные о детекторах, источниках фотонов и процедурах постобработки. Но как первый расчётный слой она вполне рабочая. И, пожалуй, честная.

**Литература**

1. Bennett C. H., Brassard G. Quantum cryptography: Public key distribution and coin tossing // Proceedings of IEEE International Conference on Computers, Systems and Signal Processing. Bangalore, India, 1984. P. 175–179.
2. Gisin N., Ribordy G., Tittel W., Zbinden H. Quantum cryptography // Reviews of Modern Physics. 2002. Vol. 74. P. 145–195.
3. ETSI. Quantum Key Distribution (QKD); Vocabulary. ETSI GR QKD 007 V1.2.1. 2026.
4. Hadfield R. H. Single-photon detectors for optical quantum information applications // Nature Photonics. 2009. Vol. 3, No. 12. P. 696–705.
5. Ma X., Qi B., Zhao Y., Lo H.-K. Practical decoy state for quantum key distribution // Physical Review A. 2005. Vol. 72. 012326.
6. Lo H.-K., Ma X., Chen K. Decoy state quantum key distribution // Physical Review Letters. 2005. Vol. 94. 230504.
7. NIST. NIST releases first 3 finalized post-quantum encryption standards. 2024.
8. Pirandola S., Andersen U. L., Banchi L. et al. Advances in quantum cryptography // Advances in Optics and Photonics. 2020. Vol. 12, No. 4. P. 1012–1236.
9. Scarani V., Bechmann-Pasquinucci H., Cerf N. J., Dušek M., Lütkenhaus N., Peev M. The security of practical quantum key distribution // Reviews of Modern Physics. 2009. Vol. 81. P. 1301–1350.
10. Shor P. W., Preskill J. Simple proof of security of the BB84 quantum key distribution protocol // Physical Review Letters. 2000. Vol. 85. P. 441–444.