УДК 621.39, 535.14
https://doi.org/10.31854/3034-2201-2026-4-3-C01
EDN: VYMOMI

Влияние параметров однофотонных источников и детекторов на скорость и дальность квантового распределения ключей по протоколу BB84

Былина М. С., Кобяков Д. Е. ✉

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича,
Санкт-Петербург, 193232, Российская Федерация

Постановка задачи. *Классические методы криптографической защиты уязвимы к атакам с использованием квантовых компьютеров и алгоритмов. Одним из решений данной проблемы является внедрение систем квантового распределения ключей, в которых секретность ключа гарантируется фундаментальными законами квантовой физики. Однако несовершенство технической реализации таких систем может приводить к компрометации ключа.* ***Целью работы*** *является анализ влияния параметров реальных источников и детекторов одиночных фотонов на скорость и дальность распределения ключей в системе, работающей по протоколу BB84.* ***Результаты.*** *Проанализированы влияние потерь в квантовом канале, квантовой эффективности и частоты темнового счета однофотонных детекторов на скорость и дальность формирования ключа. Показано, что использование лазерного диода в качестве источника открывает возможность атаки с разделением многофотонных импульсов, снижая скорость и дальность формирования ключа. Представлены методики расчета скорости и дальности распределения ключей с учетом реальных параметров детекторов, вероятности генерации многофотонных импульсов при использовании лазерного диода, возможности осуществления атаки с разделением многофотонных импульсов.* ***Практическая значимость.*** *Представленные методики расчета скорости и дальности распределения ключей с учетом реальных характеристик оборудования могут использоваться при проектировании систем квантового распределения ключей.*

Ключевые слова: *квантовое распределение ключей, протокол квантового распределения ключей BB84, квантовый канал, лавинный фотодиод, сверхпроводящий детектор, частота темнового счета, одномодовый лазерный диод, атака с разделением многофотонных импульсов*

Введение

Квантовое распределение ключей (КРК) является одним из наиболее перспективных направлений квантовых коммуникаций, поскольку позволяет распределить между двумя легитимными участниками (Алисой и Бобом) симметричный ключ, безопасность которого гарантируется фундаментальными законами квантовой физики. Возможности злоумышленника по перехвату ключа ограничены тем, что в системах КРК для его формирования используются квантовые состояния фотонов, которые невозможно клонировать или незаметно измерить, так как измерение необратимо изменяет исходное квантовое состояние. Кроме того, все известные протоколы распределения ключей основаны на использовании неортогональных базисов, что не позволяет измерить и различить квантовые состояния без внесения

Библиографическая ссылка на статью:
Былина М. С., Кобяков Д. Е. Влияние параметров однофотонных источников и детекторов на скорость и дальность квантового распределения ключей по протоколу BB84 // Вестник СПбГУТ. 2026. Т. 4. № 3. С. 1. DOI: 10.31854/3034-2201-2026-4-3-C01. EDN: VYMOMI

Reference for citation:
Bylina M., Kobyakov D. Influence of the Parameters of Single-Photon Sources and Detectors on the Rate and Range of Quantum Key Distribution Using the BB84 Protocol // Herald of SPbSUT. 2026. Vol. 4. Iss. 3. P. 1. DOI: 10.31854/3034-2201-2026-4-3-C01. EDN: VYMOMI

© Былина М. С., Кобяков Д. Е., 2026

ошибок, поэтому в системах КРК злоумышленник не может незаметно осуществить атаку на секретный ключ [1, 2]. Однако безопасность в системе КРК обеспечивается не только природой квантовых объектов и используемым протоколом, но и качеством ее технической реализации. В работе проанализировано влияние параметров однофотонных детекторов Боба на дальность и скорость формирования секретного ключа в системе КРК, работающей по протоколу BB84.

Протокол BB84 и принцип формирования ключа

На рисунке 1 представлена структурная схема системы КРК, работающей по протоколу BB84 и использующей поляризационные состояния фотонов [1–3]. Протокол начинается сеансом квантовой связи. Алиса генерирует случайную битовую строку и кодирует каждый бит поляризационным состоянием фотона, случайным образом выбирая для этого один из двух неортогональных базисов – вертикально-горизонтальный (0° и 90°) или диагональный (135° и 45°) и посылает их Бобу по квантовому каналу. Боб проводит измерения поляризации каждого принимаемого фотона, тоже случайно выбирая базисы, интерпретирует полученные результаты как бит «0» при получении поляризации 0° или 135° и как бит «1» при получении 90° или 45° и получает сырой ключ.

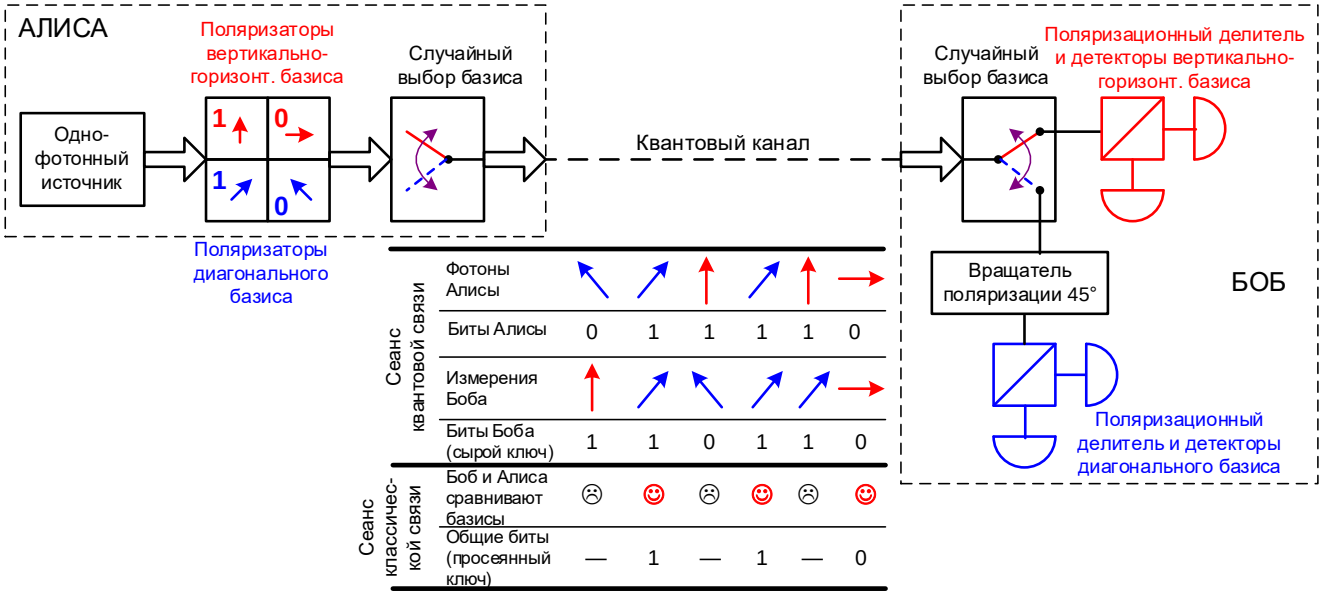


Рис. 1. Структурная схема системы КРК, работающей по протоколу BB84

После завершения сеанса квантовой связи Алиса и Боб по открытому классическому каналу сравнивают использованные ими базисы и оставляют только те биты, которые были получены при их совпадении, получая просеянный ключ. Далее оценивается количество ошибок в просеянном ключе. Если уровень ошибок превышает 11 %, ключ считается скомпрометированным, протокол прерывается, и весь процесс начинается сначала. Если ключ не скомпрометирован, выполняются процедуры исправления ошибок и усиления секретности, в результате которых формируется симметричный секретный ключ.

Влияние потерь в квантовом канале на частоту счета фотонов у Боба

Для протокола BB84 существует доказательство невозможности перехвата ключа для идеальных условий, в частности при отсутствии потерь в квантовом канале, наличии однофотонного источника и однофотонного детектора, имеющего 100-процентную квантовую эффективность и нулевой уровень темновых отсчетов. Рассмотрим ограничения, которые накладывает наличие потерь в квантовом канале. Если все остальные компоненты системы КРК считать идеальными, то потери определяют максимальную теоретически достижимую частоту счета фотонов у Боба $F_{\max}$ в канале длиной L с коэффициентом затухания α, а также максимальную длину квантового канала $L_{\max}$, обеспечивающую частоту f счета фотонов у Боба:

$$F_{\max} = f_0 \cdot 10^{-\frac{\alpha \cdot L}{10}}, \quad (1) \qquad L_{\max} = -\frac{10}{\alpha} \cdot \lg\left(\frac{f}{f_0}\right), \quad (2)$$

где f_0 – частота генерации фотонов передатчиком Алисы.

Фундаментальный предел скорости формирования ключа. Максимальная скорость формирования секретного ключа в протоколе BB84

Фундаментальный предел скорости распределения секретного ключа в канале с потерями без квантовых повторителей с архитектурой «точка – точка» (прямая отправка квантовых состояний от Алисы к Бобу) был получен в 2017 г. группой английских ученых и получил наименование границы Пирандолы – Лауренцы – Оттавиани – Банчи (PLOB). Наличие этой границы означает, что никакой протокол не позволяет превысить скорость распределения секретного ключа T_{PLOB}, определяемую только потерями в квантовом канале [4]:

$$T_{PLOB} = -T_0 \cdot \log_2\left(1 - 10^{-\frac{\alpha \cdot L}{10}}\right), \quad (3)$$

где T_0 – скорость работы передатчика Алисы (бит/с).

Предел PLOB не достижим для протоколов на дискретных переменных (включая BB84), в которых используется классическая архитектура: Алиса отправляет фотон Бобу, Боб производит измерение. Максимальная достижимая скорость для протокола BB84 может быть рассчитана по приближенному выражению [5]:

$$T_{BB84} = 0{,}5 \cdot T_0 \cdot 10^{-\frac{\alpha \cdot L}{10}}\left(1 - 2 \cdot h(\varepsilon)\right), \quad (4)$$

где 0,5 – коэффициент, учитывающий просеивание ключа; ε – вероятность ошибок в просеянном ключе; $h(\varepsilon)$ – двоичная энтропия, вычисляемая по формуле:

$$h(\varepsilon) = -\varepsilon \cdot \log_2\varepsilon - (1-\varepsilon) \cdot \log_2(1-\varepsilon).$$

Скорость T_0 в формуле (4) численно равна частоте f_0 передатчика Алисы, так как в протоколе BB84 квантовым состоянием фотона кодируется один бит распределяемого ключа.

Величина $h(\varepsilon)$ из формулы (4) показывает, сколько бит информации может извлечь злоумышленник Ева из одного бита Алисы. Величина $1 - h(\varepsilon)$ показывает, сколько бит информации может извлечь Боб после исправления ошибок. При $\varepsilon = 0{,}11$ получаем $h(\varepsilon) = 0{,}5$; т. е. Ева и Боб имеют одинаковое количество информации о ключе. Из (4) для этого случая получаем $T_{BB84} = 0$ – распределение ключа невозможно. На рисунке 2 представлены результаты расчета максимальной скорости по выражениям (3) и (4) при использовании одномодового оптического волокна с $\alpha = 0{,}2$ дБ/км в качестве квантового канала.

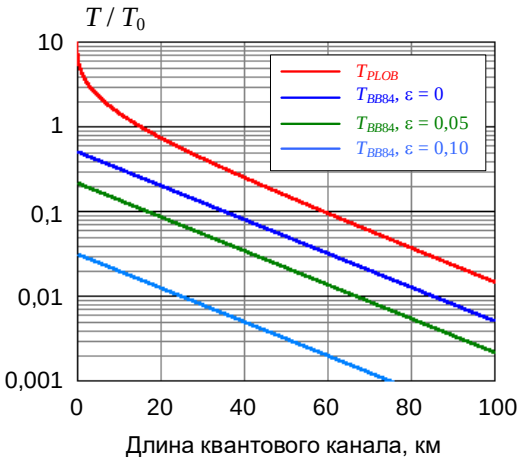


Рис. 2. Зависимости максимальной скорости распределения ключа от длины квантового канала при $\alpha = 0{,}2$ дБ/км

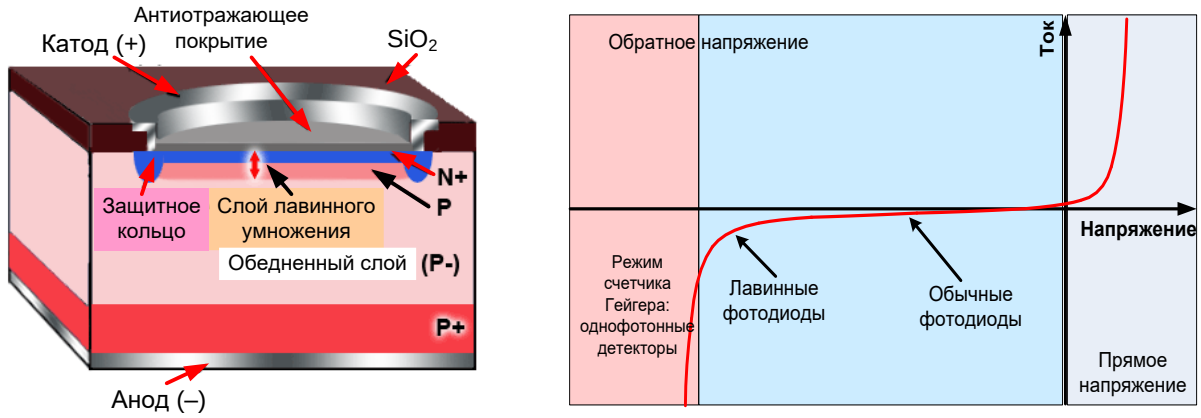
DOI: 10.31854/3034-2201-2026-4-3-C01
URL: https://vestnik-sut.ru/2026-3/C01.pdf

Из рисунка видно, что протокол BB84, даже при идеальной технической реализации, наличии канала без потерь и отсутствии Евы (при $\varepsilon = 0$), не позволяет получить скорость распределения ключа больше $0{,}5T_0$. С увеличением ε скорость быстро уменьшается.

Реальные детекторы для систем КРК

Для систем КРК могут использоваться различные типы детекторов одиночных фотонов (ДОФ). В данной работе анализируется применение двух детекторов – лавинного фотодиода (ЛФД) и сверхпроводящего детектора (СПД).

Полупроводниковые ЛФД (рисунок 3), работа которых основана на внутреннем фотоэффекте, получили наибольшее распространение в системах КРК [6, 7]. Для приема одиночных фотонов ЛФД работает в режиме счетчика Гейгера. Для этого на него подается обратное напряжение, превышающее напряжение лавинного пробоя. При этом ЛФД оказывается в состоянии неустойчивого равновесия – даже малейшее воздействие, которым является поглощение фотона и возникновение единственной электронно-дырочной пары, инициирует лавину.



а) б)

Рис. 3. Лавинный фотодиод: а) конструкция; б) вольтамперная характеристика

Чувствительным элементом СПД (рисунок 4) является спираль из нанопроволоки, которая при криогенной температуре становится сверхпроводящей [6, 7]. В спирали поддерживается постоянный ток. При этом напряжение на проволоке из-за отсутствия сопротивления равно нулю. При поглощении фотона происходит нагревание соответствующего участка нанопроволоки (возникновение «горячего» пятна), что приводит к локальному исчезновению сверхпроводимости, появлению ненулевого сопротивления и возникновению напряжения.

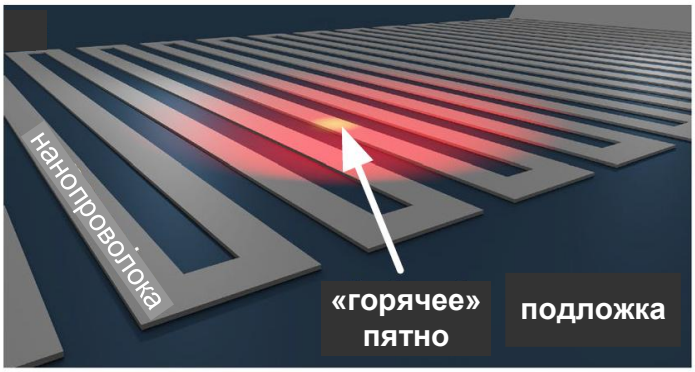


Рис. 4. Сверхпроводящий детектор

Для ДОФ можно определить:

– максимальную частоту счета фотонов $f_{\max}$, которая определяется «мертвым» временем – промежутком после срабатывания, в течение которого детектор не готов к приему следующего фотона;

– частоту темнового счета f_b или ложных срабатываний детектора, не коррелированных с моментами приема фотонов.

Параметры рассматриваемых в данной работе ДОФ приведены в таблице 1.

Таблица 1. Параметры однофотонных детекторов

Детектор	Рабочая температура, К	Квантовая эффективность на длине волны 1550 нм, %	Частота темнового счета, кГц	Максимальная частота счета фотонов, МГц
ЛФД-1 (InGaAs) [7]	240	10	16	100
ЛФД-2 (InGaAs/InP)[1]	230	20	3	100
СПД [7]	3	70	0,01	100

Влияние параметров реальных ДОФ на максимальную длину квантового канала, частоту счета фотонов у Боба и скорость распределения ключа

Отметим, что соотношения (1) и (2) показывают, что при идеальных детекторах потери в квантовом канале не накладывают ограничений на его максимальную длину. При увеличении L (росте потерь) уменьшается $F_{\max}$, т. е. увеличивается время, необходимое для накопления сырого ключа, но возможность формирования секретного ключа сохраняется. Однако при использовании реальных детекторов, характеризующихся частотой темнового счета f_b, при увеличении L возникает ситуация, когда Боб получает ложные срабатывания детекторов также часто или даже чаще, чем настоящие, что означает невозможность формирования секретного ключа.

На рисунке 5 представлены зависимости частоты счета фотонов у Боба от длины и коэффициента затухания квантового канала. На графики нанесены уровни максимальных частот счета фотонов и частот темнового счета для рассматриваемых ДОФ.

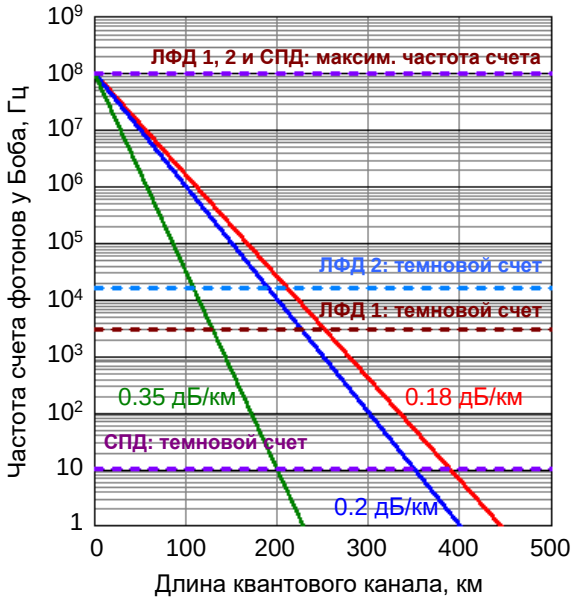


Рис. 5. Зависимости скорости счета фотонов у Боба от длины квантового канала

При уменьшении частоты счета фотонов у Боба (увеличении длины канала) вероятность ошибок в просеянном ключе ε будет возрастать. Эту величину можно оценить следующим образом [5, 8]:

[1] InGaAs SPAD detector module: technical specifications // LD-PD PTE. LTD. Singapore. URL: https://www.ld-pd.com/?a=cpinfo&id=1957 (дата обращения 27.05.2026).

$$\varepsilon = \frac{0{,}5p_b}{p_c}, \tag{5}$$

где p_c – вероятность срабатывания детектора; p_b – вероятность ложного срабатывания детектора. Коэффициент 0,5 в (5) учитывает, что схема КРК (рисунок 1) включает по два детектора для каждого базиса. Вероятность p_b определяется за один такт работы системы КРК Δt:

$$p_b = f_b \cdot \Delta t = \frac{f_b}{f_0}. \tag{6}$$

Для p_c справедливо:

$$p_c = p_b + \eta \cdot 10^{-\frac{\alpha \cdot L}{10}}(1 - p_b), \tag{7}$$

где η – квантовая эффективность детектора.

Выше отмечалось, что при $\varepsilon = \varepsilon_{\max} = 0{,}11$ мы получаем $h(\varepsilon) = 0{,}5$ и $T_{BB84} = 0$, т. е. распределение ключа становится невозможным. Значит максимальную длину квантового канала можно определить из условия $\varepsilon = \varepsilon_{\max}$. Из (5) и (7) получаем:

$$L_{\max} = -\frac{10}{\alpha} \cdot \lg\left(\frac{p_b \cdot (0{,}5 - \varepsilon_{\max})}{\eta \cdot \varepsilon_{\max} \cdot (1 - p_b)}\right). \tag{8}$$

В таблице 2 представлены результаты расчетов максимальной длины квантового канала по выражению (8) для рассматриваемых ДОФ. На рисунке 6 представлены зависимости максимальной длины квантового канала для рассматриваемых ДОФ от его коэффициента затухания α.

Таблица 2. Максимальные длины квантовых каналов при $f_0 = 100$ МГц

Вид детектора	p_b	Коэффициент затухания квантового канала, дБ/км		
		0,18	0,2	0,35
		Максимальная длина квантового канала, км		
ЛФД-1	$1{,}6 \times 10^{-4}$	124,8	112,3	64,2
ЛФД-2	$3{,}0 \times 10^{-5}$	181,9	163,7	93,5
СПД	$1{,}0 \times 10^{-7}$	349,7	314,8	179,9

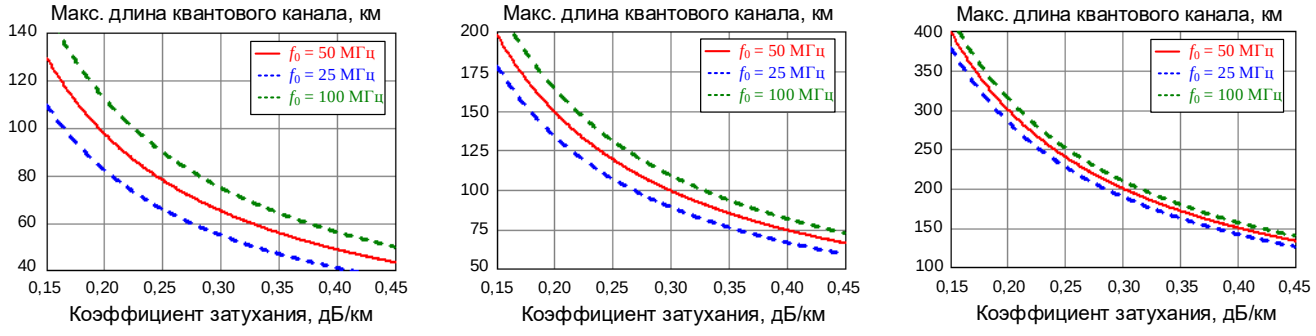


Рис. 6. Зависимости максимальной длины квантового канала от его коэффициента затухания для ЛФД-1 (а), ЛФД-2 (б), СПД (в)

Для скорости распределения ключа T_{BB84b} с учетом реальных параметров ДОФ справедливо:

$$T_{BB84b} = 0{,}5 \cdot T_0 \cdot p_c \cdot \big(1 - 2 \cdot h(\varepsilon)\big). \tag{9}$$

На рисунке 7 представлены результаты расчета относительной скорости распределения ключа T_{BB84b}/T_0 с учетом реальных параметров ДОФ по выражениям (5–9). Из таблицы 2 и рисунков 6, 7 видно, что снижение частоты темновых отсчетов позволяет увеличить длину квантового канала и скорость распределения ключа. Наибольшие скорость и дальность обеспечивает СПД.

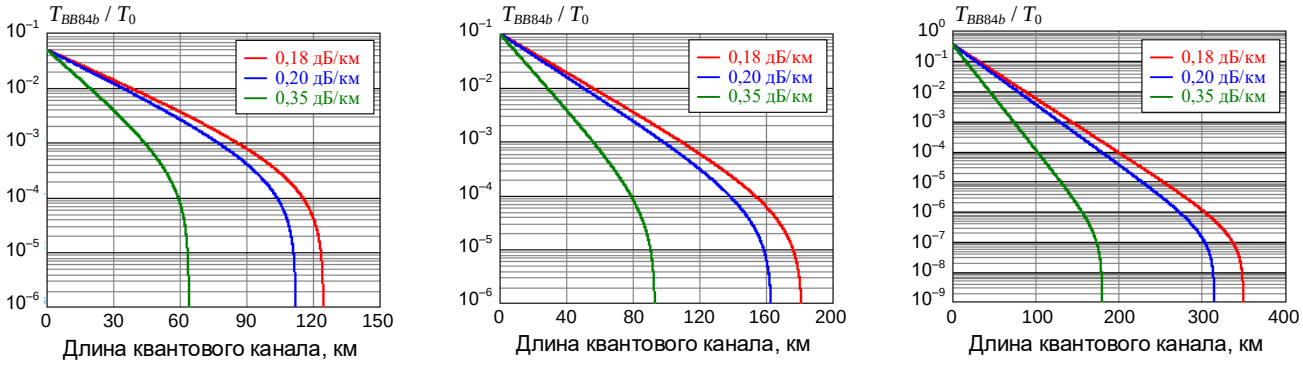


Рис. 7. Зависимости относительной скорости распределения ключа от длины квантового канала при $f_0 = 100$ МГц для ЛФД-1 (а), ЛФД-2 (б), СПД (в)

Использование лазерного диода в качестве источника одиночных фотонов

Ранее предполагалось, что Алиса использует идеальный источник одиночных фотонов (ИОФ). Однако в системах КРК в качестве ИОФ часто используется одномодовый лазерный диод (ЛД), работающий в импульсном режиме, излучение которого ослаблено аттенюатором до квазиоднофотонного состояния. Недостатком такого ИОФ является ненулевая вероятность излучения импульсов, содержащих более одного фотона, так как число фотонов в импульсе подчиняется статистике Пуассона.

Вероятность $p(n)$ того, что импульс содержит n фотонов, составляет [1, 2, 7]:

$$p(n) = \frac{\mu^n \cdot e^{-\mu}}{n!},$$

где μ – среднее число фотонов в импульсе.

На рисунке 8 представлены результаты расчетов вероятностей однофотонных, многофотонных и «пустых» (не содержащих фотонов) импульсов.

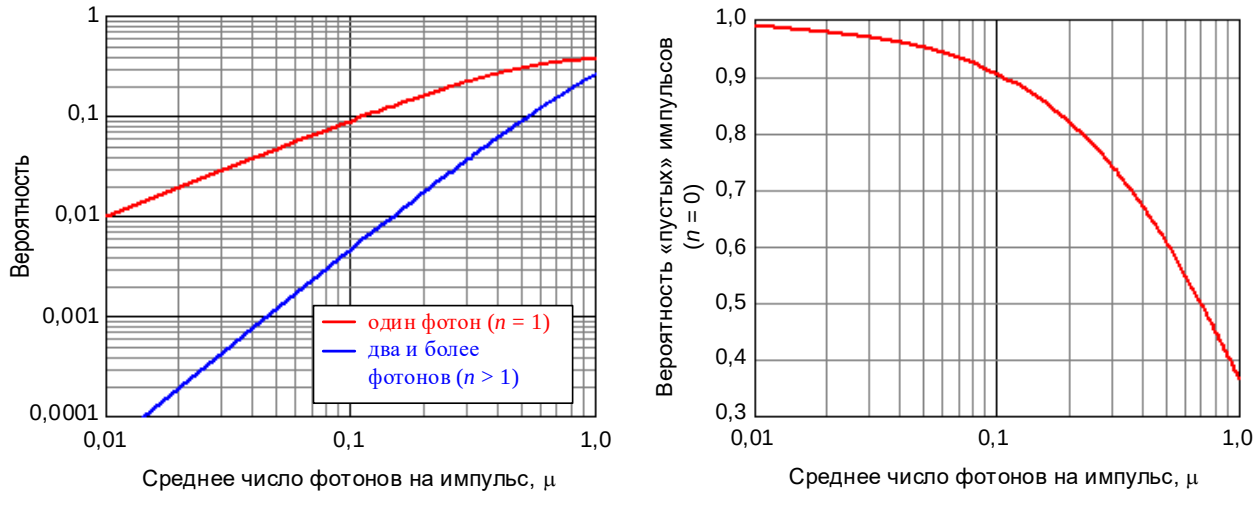


Рис. 8. Зависимости вероятностей появления однофотонных и многофотонных импульсов (а) и «пустых» импульсов (б) от среднего числа фотонов в импульсе

DOI: 10.31854/3034-2201-2026-4-3-C01
URL: https://vestnik-sut.ru/2026-3/C01.pdf

Из рисунка видно, что для повышения вероятности появления однофотонных импульсов и одновременного снижения вероятности многофотонных необходимо выбирать $\mu < 1$. Например, при $\mu = 0{,}2$ вероятность однофотонного импульса в 10 раз выше, чем многофотонного, а при $\mu = 0{,}02$ – в 100 раз. Вероятность «пустых» импульсов при этом составляет 82 % и 98 % соответственно.

Большая вероятность «пустых» импульсов означает, что реальная частота $f_{0\mu}$ генерации фотонов будет существенно меньше f_0:

$$f_{0\mu} = f_0\big(1 - p(0)\big).$$

На рисунке 9 проиллюстрировано снижение скорости счета фотонов у Боба при уменьшении μ.

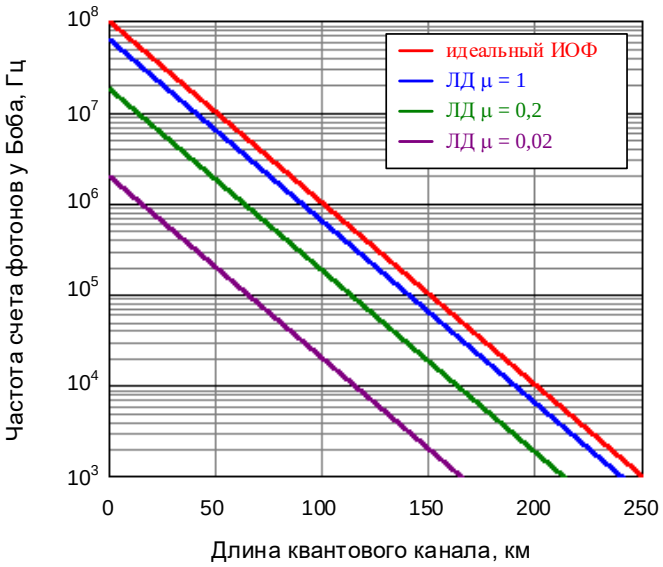


Рис. 9. Зависимости частоты счета фотонов у Боба от длины квантового канала для $f_0 = 100$ МГц и $\alpha = 0{,}2$ дБ/км при использовании идеального ДОФ

Скорость и дальность распределения секретного ключа в системе КРК, работающей по протоколу BB84, без учета атаки PNS

Скорость распределения секретного ключа с ЛД в качестве ИОФ для системы КРК, работающей по протоколу BB84, без учета возможной атаки с разделением многофотонных импульсов (PNS, *аббр. от англ.* Photon Number Splitting) может быть определена по выражению, аналогичному (9):

$$T_{BB84\mu} = \frac{1}{2} \cdot T_0 \cdot p_\mu \cdot \Big(1 - 2 \cdot h\big(\varepsilon_\mu\big)\Big), \tag{10}$$

где p_μ – вероятность срабатывания детектора у Боба; ε_μ – вероятность ошибок в просеянном ключе.

Для p_μ и ε_μ справедливы выражения:

$$p_\mu = \sum_{n=0}^{\infty} p(n) \cdot \left[1 - (1 - p_b) \cdot \left(1 - \eta \cdot 10^{-\frac{\alpha \cdot L}{10}}\right)^n\right], \tag{11}$$

$$\varepsilon_\mu = \frac{0{,}5 p_b}{p_\mu}. \tag{12}$$

На рисунке 10 показаны результаты расчета относительной скорости распределения ключа $T_{BB84\mu}/T_0$ по выражениям (10–12), в таблице 3 – результаты расчетов скорости распределения

секретного ключа $T_{BB84\mu}/T_0$ для систем КРК при частоте импульсов передатчика Алисы 100 МГц для двух длин квантового канала – 25 и 50 км.

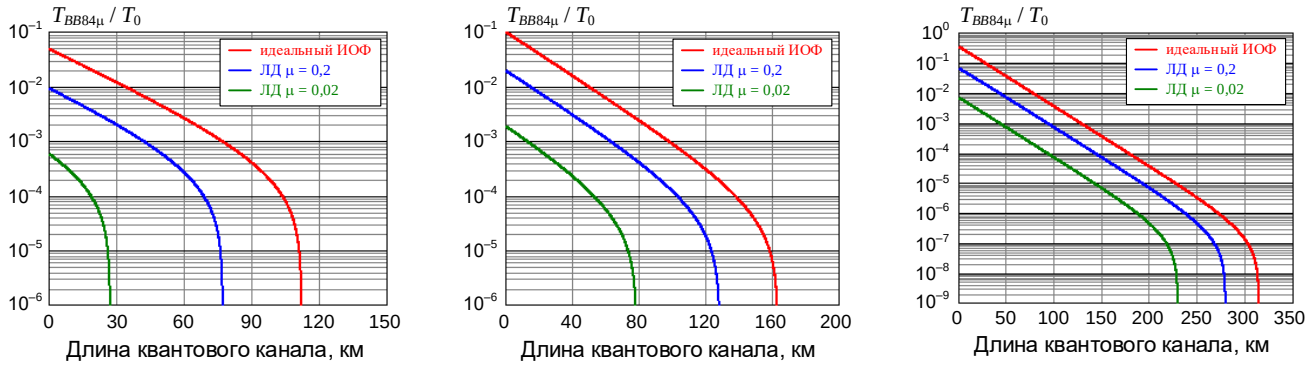


Рис. 10. Зависимости относительной скорости распределения ключа $T_{BB84\mu}/T_0$ от длины квантового канала при $f_0 = 100$ МГц и $\alpha = 0{,}2$ дБ/км для ЛФД-1 (а), ЛФД-2 (б), СПД (в)

Таблица 3. Скорости распределения ключа при $f_0 = 100$ МГц без учета возможной атаки PNS

Длина квантового канала, км		25			50		
Коэффициент затухания, дБ/км		0,18	0,2	0,35	0,18	0,2	0,35
Идеальный ДОФ: $p_b = 0$; $\eta = 100$ %							
Скорость распределения ключа, кбит/с	μ = 0,2	3425	3064	1316	1243	990,1	177,5
	μ = 0,02	353,5	315,2	133,2	125,7	99,9	17,8
ЛФД-1: $p_b = 1{,}6 \cdot 10^{-4}$; $\eta = 10$ %							
Скорость распределения ключа, кбит/с	μ = 0,2	298,0	261,0	88,6	81,8	58,5	–
	μ = 0,02	4,94	2,21	–	–	–	–
ЛФД-2: $p_b = 3{,}0 \cdot 10^{-5}$; $\eta = 20$ %							
Скорость распределения ключа, кбит/с	μ = 0,2	689,1	613,2	252,6	237,9	186,8	26,5
	μ = 0,02	60,4	52,9	18,2	16,8	12,1	–
СПД: $p_b = 10^{-7}$; $\eta = 70$ %							
Скорость распределения ключа, кбит/с	μ = 0,2	2423	2165	924,7	873,4	695,0	124,2
	μ = 0,02	247,7	220,8	93,2	88,0	69,9	12,4

Из таблицы 3 и рисунка 10 видно, что скорость распределения ключа быстро падает с увеличением длины квантового канала и уменьшением μ. В таблице 4 представлены результаты расчета максимальной длины квантового канала. При использовании ЛД в качестве ИОФ и среднем числе фотонов на импульс $\mu << 1$ максимальная длина квантового канала уменьшается по сравнению с идеальным ИОФ (таблица 2).

Таблица 4. Максимальные длины квантовых каналов при $f_0 = 100$ МГц без учета возможной атаки PNS

Вид детектора	Среднее число фотонов в импульсе, μ	Коэффициент затухания, дБ/км		
		0,18	0,2	0,35
		Максимальная длина квантового канала, км		
ЛФД-1	0,2	85,9	77,3	44,2
	0,02	30,4	27,3	15,6
ЛФД-2	0,2	143,1	128,8	73,6
	0,02	87,5	78,8	45,0
СПД	0,2	310,9	279,8	159,9
	0,02	255,4	229,8	131,3

DOI: 10.31854/3034-2201-2026-4-3-C01
URL: https://vestnik-sut.ru/2026-3/C01.pdf

Скорость и дальность распределения секретного ключа в системе КРК, работающей по протоколу BB84, с учетом атаки PNS

В системе КРК с ЛД в качестве ИОФ Ева может осуществлять атаку PNS – отделять фотон от каждого многофотонного импульса и сохранять в квантовой памяти до публичного объявления базисов. Для получения более полной информации о ключе Ева может уничтожать все однофотонные импульсы. Однако Боб, зная величину затухания квантового канала, может заметить, что получает меньше ожидаемого числа импульсов, поэтому Ева маскирует атаку, подменяя квантовый канал на канал с меньшими потерями.

В условиях данной атаки формирование ключа все еще возможно, но скорость его распределения и максимальная длина квантового канала существенно уменьшатся. Для скорости распределения ключа с учетом PNS справедливо выражение [9]:

$$T_{BB84p} = \frac{1}{2} \cdot T_0 \cdot \left[p_1\left(1 - h(\varepsilon_1)\right) - p_\mu \cdot h(\varepsilon_\mu)\right], \tag{13}$$

где p_μ – вероятность срабатывания детектора Боба; ε_μ – вероятность ошибок в просеянном ключе; p_1 – вероятность регистрации Бобом однофотонного импульса; ε_1 – вероятность ошибок, оцениваемая по однофотонным импульсам.

Величины p_1 и ε_1 можно приближенно оценить по выражениям:

$$p_1 = p_b + p(1) \cdot (1 - p_b) \cdot \left(1 - \eta \cdot 10^{-\frac{\alpha \cdot L}{10}}\right), \tag{14}$$

$$\varepsilon_1 = \frac{0{,}5 p_b}{p_1}. \tag{15}$$

В формуле (14) учитываются только ошибки, обусловленные ложными срабатываниями детекторов.

На рисунке 11 показаны результаты расчета относительной скорости распределения ключа T_{BB84p}/T_0 по выражениям (13–15). В таблице 5 представлены результаты расчетов скорости распределения секретного ключа для систем КРК, работающих по протоколу BB84, при частоте импульсов передатчика Алисы 100 МГц с учетом возможной атаки PNS; в таблице 6 – результаты расчета максимальной длины квантового канала, полученные при тех же условиях.

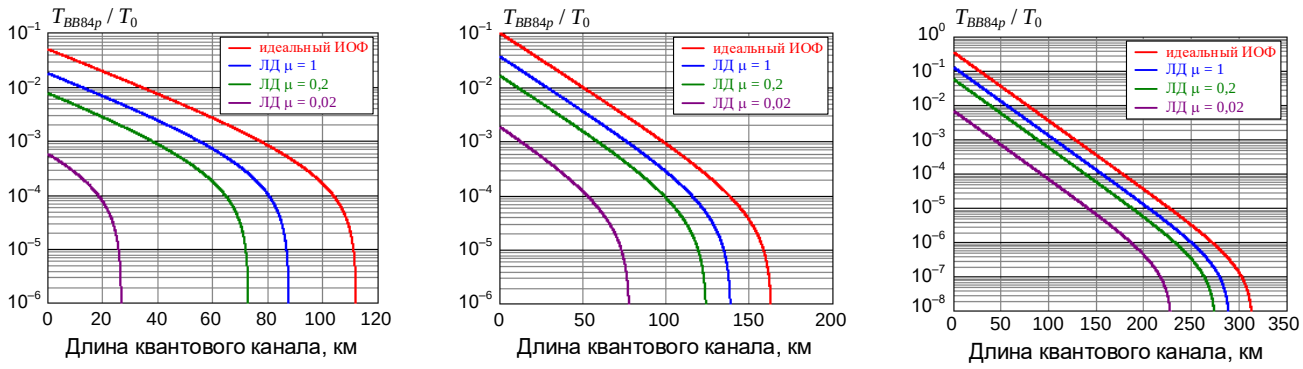


Рис. 11. Зависимости относительной скорости распределения ключа T_{BB84p}/T_0 от длины квантового канала при $f_0 = 100$ МГц и $\alpha = 0{,}2$ дБ/км для ЛФД-1 (а), ЛФД-2 (б), СПД (в)

Таблица 5. Скорости распределения ключа при $f_0 = 100$ МГц с учетом возможной атаки PNS

Длина квантового канала, км		25			50		
Коэффициент затухания, дБ/км		0,18	0,2	0,35	0,18	0,2	0,35
ЛФД-1: $p_b = 1{,}6 \cdot 10^{-4}$; $\eta = 10\ \%$							
Скорость распределения ключа, кбит/с	μ = 0,2	237,4	207,1	67,0	61,5	42,8	–
	μ = 0,02	4,48	1,82	–	–	–	–
ЛФД-2: $p_b = 3{,}0 \cdot 10^{-5}$; $\eta = 20\ \%$							
Скорость распределения ключа, кбит/с	μ = 0,2	565,9	503,0	205,4	193,3	151,4	20,5
	μ = 0,02	59,1	51,7	17,7	16,4	11,8	–
СПД: $p_b = 10^{-7}$; $\eta = 70\ \%$							
Скорость распределения ключа, кбит/с	μ = 0,2	2033	1812	764,2	721,4	573,0	101,8
	μ = 0,02	243,4	216,9	91,4	86,3	68,5	12,1

Таблица 6. Максимальные длины квантовых каналов при $f_0 = 100$ МГц с учетом возможной атаки PNS

Вид детектора	Среднее число фотонов в импульсе, μ	Коэффициент затухания, дБ/км		
		0,18	0,2	0,35
		Максимальная длина квантового канала, км		
ЛФД-1	0,2	81,3	73,2	41,8
	0,02	30,0	27,0	15,4
ЛФД-2	0,2	138,4	124,6	71,2
	0,02	87,1	78,4	44,8
СПД	0,2	306,3	275,6	157,5
	0,02	254,9	229,4	131,1

Из таблиц 3–6 видно, что атака PNS снижает скорость и дальность распределения ключа. На рисунках 12 и 13 сопоставлены зависимости скорости распределения ключа и максимальной длины квантового канала от параметра μ при наличии и отсутствии атаки PNS. При $\mu << 1$ влияние атаки на возможность распределения ключа пренебрежимо мало, однако ее роль быстро возрастает при увеличении μ, т. е. с повышением вероятности генерации многофотонных импульсов.

Увеличить скорость и дальность распределения ключа можно, используя протокол BB84 совместно с применением состояний-ловушек (Decoy State), что позволяет снизить эффективность атаки PNS [10].

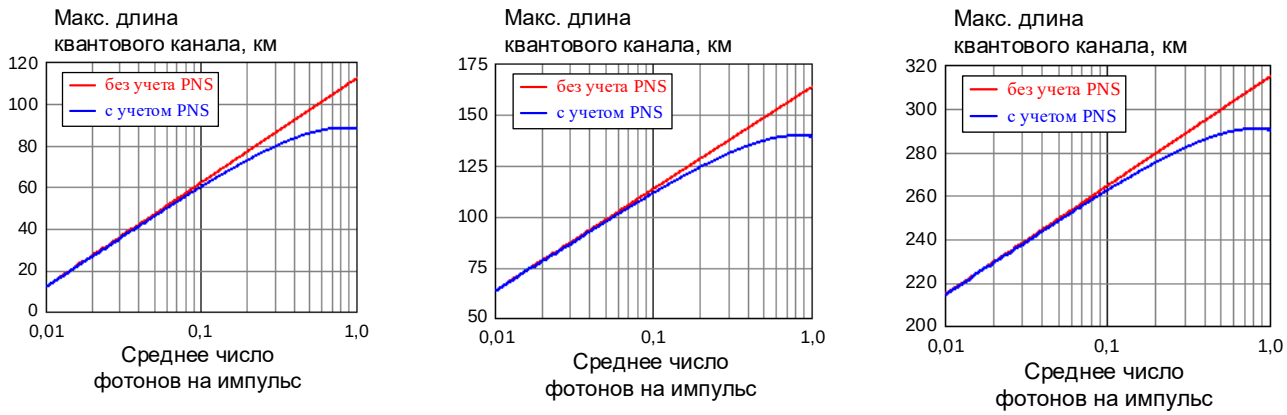
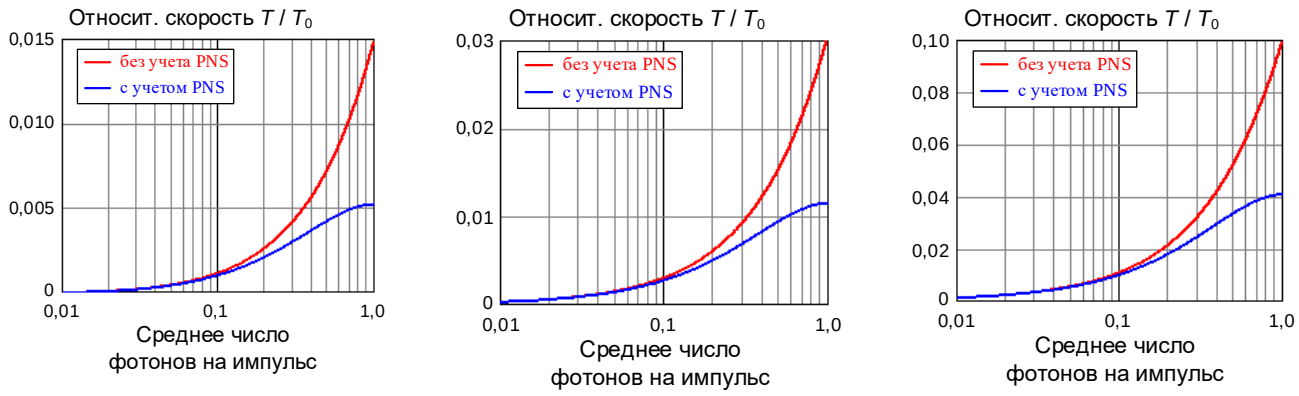


Рис. 12. Максимальная длина квантового канала при $f_0 = 100$ МГц и $\alpha = 0{,}2$ дБ/км для ЛФД-1 (а), ЛФД-2 (б), СПД (в)



а) б) в)

Рис. 13. Относительная скорость распределения ключа при длине квантового канала 25 км, $f_0 = 100$ МГц и $\alpha = 0{,}2$ дБ/км для ЛФД-1 (а), ЛФД-2 (б), СПД (в)

Заключение

Проведенные в работе исследования показали, что:

– параметры реальных источников и детекторов, а также потери в квантовом канале оказывают существенное влияние на работу систем КРК, ограничивая скорость и дальность распределения ключа;

– потери в квантовом канале при идеальных ИОФ и ДОФ не ограничивают его длину, но снижают максимально достижимую скорость распределения ключа;

– наличие у реального ДОФ вероятности ложного срабатывания (ненулевой частоты темновых отсчетов) повышает вероятность ошибок в ключе;

– вероятность ошибок возрастает при увеличении длины квантового канала и снижении квантовой эффективности ДОФ;

– установив допустимый уровень ошибок (11 % для протокола BB84), можно получить максимальную длину, на которой распределение ключа еще возможно;

– использование ЛД в качестве ИОФ со средним числом фотонов на импульс $\mu < 1$ не только снижает реальную частоту работы передатчика Алисы, но и делает возможной для Евы атаку PNS, эффективность которой возрастает с увеличением μ;

– использование СПД, имеющего самую низкую частоту темновых отсчетов и самую высокую квантовую эффективность среди всех рассмотренных ДОФ, позволяет получить наибольшие длину квантового канала и скорость распределения ключа; однако эти ДОФ требуют глубокого охлаждения, что усложняет техническую реализацию системы КРК и увеличивает ее габариты и стоимость;

– ЛФД не требуют сложной системы охлаждения и обладают удовлетворительными характеристиками, поэтому их использование в коммерческих системах КРК целесообразно.

Отметим, что рассмотренный в работе протокол BB84 не является наилучшим с точки зрения достижения максимальных скорости и дальности распределения ключа. Даже при идеальной технической реализации системы КРК этот протокол не позволяет достичь предела PLOB – максимальной скорости, достижимой для систем с прямой отправкой квантовых состояний от Алисы к Бобу без промежуточных узлов. К этому пределу можно приблизиться, только используя протоколы на непрерывных переменных [11].

Литература

1. Gisin N., Ribordy G., Tittel W., Zbinden H. Quantum Cryptography // Reviews of Modern Physics. Vol. 74. Iss. 1. 2002. PP. 145–195. DOI: 10.1103/RevModPhys.74.145. EDN: LXJNVR

2. Гайдаш А. А., Егоров В. И., Иванова А. Е., Козубов А. В., Кынев С. М. и др. Квантовые технологии: учебно-методическое пособие. СПб.: Университет ИТМО, 2023. 136 с.

3. Bennett Ch. H., Brassard G. Quantum Cryptography: Public Key Distribution and Coin Tossing // Proceedings of International Conference on Computers, Systems & Signal Processing (9–12 December 1984, Bangalore, India). 1984. PP. 175–179.

4. Pirandola S., Laurenza R., Ottaviani C., Banchi L. Fundamental Limits of Repeaterless Quantum Communications // Nature Communications. 2017. Vol. 8. Iss. 1. P. 15043. DOI: 10.1038/ncomms15043. EDN: YDVJUL

5. Lütkenhaus N. Security against individual attacks for realistic quantum key distribution // Physical Review A. 2000. Vol. 61. Iss. 5. P. 052304. DOI: 10.1103/PhysRevA.61.052304

6. Eisaman M. D., Fan J., Migdall A., Polyakov S. V. Invited Review Article: Single-photon Sources and Detectors // Review of Scientific Instruments. 2011. Vol. 82. Iss. 7. P. 071101. DOI: 10.1063/1.3610677. EDN: OLHAON

7. Килин С. Я., Хорошко Д. Б., Низовцев А. П., Шатохин В. Н., Букач А. А. и др. Квантовая криптография: идеи и практика. Минск: ИД «Белорусская наука», 2007. 392 с. EDN: PMYTRM

8. Zhu C.-H., Quan D.-X., Zhang F., Pei C.-X. Improving Key Rate of Optical Fiber Quantum Key Distribution System Based on Channel Tomography // International Journal of Theoretical Physics. 2013. Vol. 52. PP. 596–603. DOI: 10.1007/s10773-012-1365-6

9. Ma X. Unconditional Security at a Low Cost // Physical Review A. 2006. Vol. 74. P. 052325. DOI: 10.1103/PhysRevA.74.052325

10. Трушечкин А. С., Киктенко Е. О., Кронберг Д. А., Федоров А. К. Стойкость метода обманных состояний в квантовой криптографии // Успехи физических наук. 2021. Т. 191. № 1. С. 93–109. DOI: 10.3367/UFNr.2020.11.038882. EDN: RGYQJF

11. Ghalaii M., Kumar R., Ottaviani C., Pirandola S., Razavi M. Continuous-Variable Quantum Key Distribution Enhanced by Quantum Scissors // Proceedings of the 7th International Conference on Quantum Cryptography (QCrypt 2017, 18–22 September 2017, Cambridge, UK). 2017. URL: http://2017.qcrypt.net/wp-content/uploads/2017/09/We480.pdf (дата обращения 24.05.2026)

Статья поступила 27 мая 2026 г.
Одобрена после рецензирования 29 июня 2026 г.
Принята к публикации 08 октября 2026 г.

Информация об авторах

Былина Мария Сергеевна – кандидат технических наук, доцент, заведующий кафедрой оптических и квантовых систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича. Email: Bylina.Maria@sut.ru

Кобяков Демьян Евгеньевич – студент группы ИКТО-38 Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича. Email: kobiakov.de@sut.ru

https://doi.org/10.31854/3034-2201-2026-4-3-C01
EDN: VYMOMI

Influence of the Parameters of Single-Photon Sources and Detectors on the Rate and Range of Quantum Key Distribution Using the BB84 Protocol

M. Bylina, D. Kobyakov ✉

The Bonch-Bruevich Saint Petersburg State University of Telecommunications,
St. Petersburg, 193232, Russian Federation

Problem statement. *Classical methods of cryptographic protection are vulnerable to attacks using quantum computers and algorithms. One solution to this problem is the deployment of quantum key distribution systems, in which key secrecy is guaranteed by the fundamental laws of quantum physics. However, imperfections in the technical implementation of such systems can lead to key compromise.* ***The aim*** *of this work is to analyze the influence of the parameters of real single-photon sources and detectors on the rate and range of key distribution in a system operating under the BB84 protocol.* ***Results.*** *The influence of losses in the quantum channel, quantum efficiency, and dark count rate of single-photon detectors on the key generation rate and range is analyzed. It is shown that the use of a laser diode as a source opens up the possibility of a photon-number-splitting attack, reducing the key generation rate and range. Methods are presented for calculating the key distribution rate and range taking into account the real parameters of detectors, the probability of multi-photon pulse generation when using a laser diode, and the feasibility of a photon-number-splitting attack.* ***Practical significance.*** *The presented methods for calculating the key distribution rate and range with allowance for the real characteristics of the equipment can be used in the design of quantum key distribution systems.*

Key words: *quantum key distribution, BB84 quantum key distribution protocol, quantum channel, avalanche photodiode, superconducting detector, dark count rate, single-mode laser diode, photon-number-splitting attack*

Information about Authors

Bylina Maria – Ph. D. of Engineering Sciences, Associate Professor, Head of the Department of Optical and Quantum Communication Systems (The Bonch-Bruevich Saint Petersburg State University of Telecommunications). E-mail: Bylina.Maria@sut.ru

Kobyakov Demian – Student of the IKTO-38 group (The Bonch-Bruevich Saint Petersburg State University of Telecommunications). Email: kobiakov.de@sut.ru