ИЗВЕСТИЯ РАН. СЕРИЯ ФИЗИЧЕСКАЯ, 2024, том 88, № 6, с. 967–974

УДК 535.14

ЭФФЕКТИВНОСТЬ НАЗЕМНОГО ПРИЕМНОГО ТЕРМИНАЛА ДЛЯ КВАНТОВОЙ СВЯЗИ

© 2024 г. К. А. Барбышев[1,2,*], А. В. Дуплинский[1,3], А. В. Хмелев[1], В. Л. Курочкин[1,4]

[1] *Общество с ограниченной ответственностью «КуСпэйс Технологии», Москва, Россия*

[2] *Федеральное государственное бюджетное образовательное учреждение высшего образования «Национальный исследовательский университет «МЭИ», Москва, Россия*

[3] *Федеральное государственное автономное образовательное учреждение высшего образования «Национальный исследовательский университет «Высшая школа экономики», Москва, Россия*

[4] *Федеральное государственное автономное образовательное учреждение высшего образования «Национальный исследовательский технологический университет «МИСИС», Москва, Россия*

** e-mail: k.barbyshev@goqrate.com*

Поступила в редакцию 15.12.2023
После доработки 29.01.2024
Принята к публикации 26.02.2024

Исследована возможность практической реализации квантового канала связи для распределения ключей шифрования между спутником Micius и мобильной приемной оптической станцией. С использованием теоретической оценки получены численные значения основных параметров такой линии связи: уровень потерь, скорость генерации ключа и его длина, а также коэффициент квантовых битовых ошибок.

Ключевые слова: спутниковая квантовая криптография, квантовое распределение ключей, ключ шифрования, наземная станция

DOI: 10.31857/S0367676524060193, **EDN:** PFOTOB

ВВЕДЕНИЕ

Для обеспечения безопасной передачи и хранения данных на сегодняшний день предложено использовать технологию квантового распределения ключей (КРК). Она направлена на устранение угрозы информационной безопасности, в том числе со стороны активно разрабатываемых в данный момент времени квантовых компьютеров. Технология КРК при обмене сгенерированными истинно случайными битовыми последовательностями между удаленными пользователями опирается на фундаментальные принципы квантовой механики, а не на сложность решения ряда математических задач. Поэтому такой метод обеспечения защиты информации не зависит от вычислительных мощностей злоумышленника и может обеспечить абсолютную секретность передаваемых данных [1, 2].

Главным ограничением современных квантово-криптографических систем является расстояние передачи квантового сигнала, у которого существует предел из-за поглощения фотонов в среде оптического волокна [3]. На данный момент максимальный продемонстрированный диапазон составляет несколько сотен километров [4]. В то же время использование низкоорбитальных космических аппаратов позволяет обойти главное ограничение волоконной квантовой криптографии и соединить абсолютно защищенным каналом связи любые точки планеты [5].

Работы, в которых описано применение научного спутника Micius в качестве промежуточного доверенного узла, демонстрируют возможность создания глобальной сети КРК [6—9]. Однако практическая реализация подобных спутниковых систем по-прежнему сталкивается с рядом инженерно-технических проблем, такими как большие размеры и вес наземных оптических станций, необходимых для приема квантовых сигналов. В данном исследовании мы сообщаем о результатах моделирования процедуры КРК по линии «космос–земля» на основе сеанса квантовой связи между спутником Micius и портативной приемной наземной станцией. Вес станции составляет 150 кг, что позволяет разместить ее в черте мегаполиса, например, на крыше зданий государственных органов и финансовых учреждений.

МОДЕЛЬ СПУТНИКОВОГО КВАНТОВОГО КАНАЛА СВЯЗИ

Выбор сценария сеанса распределения ключей

Для моделирования выберем из существующих вариантов [10] наиболее оптимальный сценарий КРК с нисходящей линией связи, т. е. когда передатчик, установленный на спутнике, посылает информационные сигналы на Землю. В этом случае основной причиной потерь в канале связи является дифракционная расходимость излучения, которая зависит от длины волны лазерного источника, а также размера и конструкции передающей оптической системы. Отклонение лазерного луча от первоначальной траектории, вызванное влиянием атмосферной турбулентности, происходит в самом конце пути передачи (в приземном слое атмосферы толщиной 20 км), где размер пучка из-за дифракции обычно намного больше, чем его отклонение. Следовательно, нисходящая линия характеризуется меньшим расширением луча по сравнению с восходящей и, таким образом, имеет более высокую эффективность связи.

Характеристики информационного канала также зависят от типа орбиты космического аппарата, которые делятся по орбитальной высоте на три основных класса: низкая околоземная орбита (500—2000 км), средняя околоземная (2000—36000 км) и геостационарная орбиты (> 36000 км). Для нашего случая оптимальным будет расположение спутника на низкой орбите (на высоте порядка 500 км), преимущества которой заключаются в меньших оптических потерях и меньшей стоимости достижения, а также успешной эксплуатации по сравнению с более высокими орбитами. Для снижения уровня фонового шума канал КРК работает только в ночное время. Поэтому была выбрана круговая солнечно-синхронная полуночная орбита, пересекающая экватор примерно в полночь по местному времени, тем самым оптимизируя время, проведенное в тени Земли.

Оценка длины канала

Представленный в работе метод анализа характеристик канала квантовой связи отличается от взятой за основу модели [11] тем, что учитывает реальные значения эффективности оптической системы и детекторов одиночных фотонов, которые были определены экспериментальным путем. Для того чтобы при помощи математической модели [11] определить эффективность нашего спутникового канала КРК, необходимо изначально рассчитать зависящее от времени расстояние между передатчиком и приемником, а также угол возвышения спутника над горизонтом. Рассмотрим наилучший вариант прохождения спутника — через зенитную точку над станцией наблюдения. Здесь и далее все вычисления выполнены с учетом того, что в качестве передающего узла выступает первый в мире космический аппарат для КРК — китайский спутник Micius.

Угловая скорость спутника на низкой околоземной орбите определяется выражением

$$\omega = \sqrt{\frac{g}{R}} - \omega_E \cos\beta, \qquad (1)$$

где g — ускорение свободного падения, R — расстояние от центра Земли до космического аппарата, ω_E — угловая скорость Земли, β — угол наклона орбиты космического аппарата.

Численные значения параметров орбиты спутника приведены в табл. 1.

Таблица 1. Параметры орбиты спутника Micius

h, км	R_E, км	R, км	β, °	g, м·с$^{-2}$	ω_E, рад·с$^{-1}$	ω, рад·с$^{-1}$
500	6371	6871	97.3	9.8	$7.3\cdot10^{-5}$	$120.4\cdot10^{-5}$

Зависимость угла возвышения спутника над горизонтом от времени рассчитана, исходя из простых геометрических соображений:

$$\theta_{el}(t) = \arccos\left(\sqrt{\frac{\sin^2(\omega t)}{1+\left(\frac{R_E}{R}\right)^2 - 2\left(\frac{R_E}{R}\right)\cos(\omega t)}}\right), \qquad (2)$$

где R_E — радиус Земли.

Затем была определена зависимость расстояния между спутником и наземной станцией от времени:

$$d(t) = -R_E \sin\left(\theta_{el}(t)\right) + \\ + \sqrt{{R_E}^2 \sin^2\left(\theta_{el}(t)\right) + 2R_E h + h^2}, \qquad (3)$$

где h — высота орбиты космического аппарата.

При моделировании необходимо учесть, что сеанс распределения ключей возможен не на всей траектории прохождения спутника над пунктом наблюдения, т. к. наземной станции необходимо некоторое время, чтобы навестись на объект слежки.

На рис. 1 показаны зависимости угла места спутника и расстояния до него от времени, полученные для зенитного прохода. Результаты представлены для того времени, когда спутник находился в поле зрения наземной станции, т. е. когда угол возвышения над горизонтом составлял свыше 20°.

Из графиков, представленных на рис. 1, видно, что расстояние между спутником и приемником уменьшается с увеличением угла места. Строго говоря, лишь проход спутника через зенитную точку обеспечивает максимальную продолжительность квантовой связи и наименьшую длину канала. В нашем случае длительность сеанса составила примерно 270 с, а расстояние «спутник–Земля» варьировалось

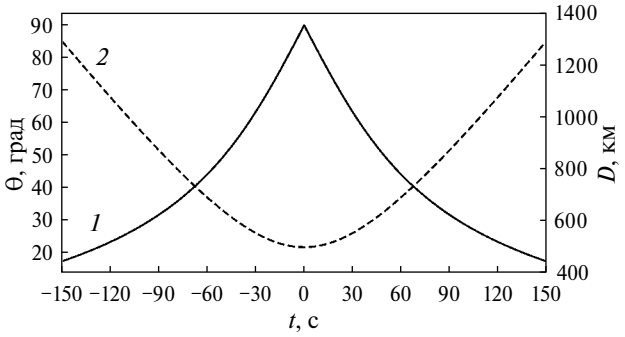

Рис. 1. Угол возвышения спутника (*1*, сплошная кривая) и расстояние до него (*2*, штриховая кривая).

от 500 до 1200 км соответственно. Для более наглядного представления полученные зависимости симметрично выровнены относительно наибольшего угла восхождения (зенитного положения), что соответствует нулевому времени.

Оценка потерь в канале связи

Потери в канале квантовой связи между космическим аппаратом и наземной приемной станцией динамически изменяются в ходе сеанса КРК, что существенно отличает этот метод от распределения ключей по оптическому волокну. При оценке уровня потерь в линии спутниковой квантовой связи необходимо учитывать следующие факторы:

1) дифракцию луча;

2) атмосферное поглощение и рассеяние;

3) эффективность оптического тракта приемного модуля;

4) квантовую эффективность детекторов одиночных фотонов.

Как правило, наибольший вклад в суммарное ослабление сигнала вносят дифракционные потери, которые зависят от изменяющейся протяженности канала. Кроме того, меняющийся со временем угол места приводит к различной эффективной толщине атмосферы, что в свою очередь отражается на коэффициенте пропускания света.

Потери из-за дифракции были рассчитаны по формуле

$$\eta_{dif}(t)=\frac{eD_t^2}{\left(\gamma d(t)\right)^2}, \qquad (4)$$

где e — коэффициент обструкции приемного телескопа, D_t — диаметр приемного телескопа, γ — угловая расходимость лазерного источника, d — длина канала связи.

Следующее немаловажное влияние на ослабление оптического сигнала оказывают потери на прохождение излучения сквозь толщу атмосферы. Для точной оценки необходимо учесть явления поглощения и рассеяния.

Рассеяние лазерного излучения на осадках различных типов таких, как дождь, снег, туман, пыль, дымка, является одной из основных причин ослабления сигнала. Присутствие таких частиц в воздухе приводит к угловому перераспределению светового потока и уменьшению дальности его распространения. Каждый тип рассеяния определяется физическим размером частиц по отношению к длине волны лазерного излучения.

Рэлеевское рассеяние — это упругое рассеяние излучения, связанное с молекулами воздуха, которые значительно меньше по размеру, чем длина волны. Коэффициент молекулярного рассеяния рассчитывается согласно формуле

$$\sigma(\lambda)=\frac{8\pi^3\left(n^2-1\right)}{3N\lambda^4}\cdot\frac{6+3\delta}{6-7\delta}, \qquad (5)$$

где n — показатель преломления среды, N — число молекул в единице объема, λ — длина волны излучения, δ — фактор деполяризации рассеянного излучения.

По формуле (5) видно, что искомый коэффициент обратно пропорционально зависит от четвертой степени длины волны. Это означает, что при использовании информационного сигнала с $\lambda = 850$ нм можно пренебречь энергетическими потерями за счет рэлеевского рассеяния.

Еще один тип рассеяния происходит на частицах аэрозоля, которые больше, чем молекулы, но достаточно малы, чтобы оставаться в воздухе на протяжении длительного периода времени — это рассеяние Ми. Размеры аэрозольных частиц в атмосфере колеблются в диапазоне от 2 нм до 100 мкм. Для оценки затухания сигнала, вызванного аэрозолями, необходимо учитывать их состав, концентрацию и распределение. Из-за значительных экспериментальных трудностей, связанных с определением всех этих параметров, были созданы модели, описывающие аэрозольные условия в зависимости от метеорологических или локальных параметров окружающей среды. Одна из таких моделей, предложенная авторами работы [12], описывает затухание сигнала в атмосфере выражением

$$\alpha(\lambda)=\frac{3.91}{V}\left(\frac{\lambda}{550}\right)^{-q}, \qquad (6)$$

где V — метеорологическая оптическая дальность, q — параметр, зависящий от метеорологической оптической дальности следующим образом:

$$q=\begin{cases}1.6 & V>50\text{ км}\\ 1.3 & 6\text{ км}<V<50\text{ км}\\ 0.16V+0.34 & 1\text{ км}<V<6\text{ км}\\ V-0.5 & 0.5\text{ км}<V<1\text{ км}\\ 0 & V<0.5\text{ км}\end{cases}. \qquad (7)$$

Чтобы учесть тот факт, что свет проходит большее расстояние через атмосферу у горизонта, чем в зените, воспользуемся соотношением Янга–Ирвина, которое авторы вывели в работе [13] для связи воздушной массы с углом места. Под воздушной массой в данном случае понимают длину пути через атмосферу. Уравнение

$$f\left(\theta_{el}\right)=\csc\left(\theta_{el}\right)\cdot\left(1-0.0012\cdot\mathrm{ctg}^2\left(\theta_{el}\right)\right) \qquad (8)$$

предполагает использование истинного зенитного угла, т. е. угла, отсчитываемого от горизонта к наблюдаемому объекту в отсутствие влияния рефракции атмосферы.

С учетом всего вышеизложенного итоговая эффективность канала была определена с помощью выражения

$$\eta(t)=\frac{eD_t^2}{\left(\gamma d(t)\right)^2}\times$$
$$\times 10^{-0.4\alpha\cdot\csc\left(\theta_{el}(t)\right)\cdot\left(1-0.0012\mathrm{ctg}^2\left(\theta_{el}(t)\right)\right)}\eta_{opt}\eta_{det}, \qquad (9)$$

где η_{opt} — оптическая эффективность приемного модуля, η_{det} — квантовая эффективность детекторов одиночных фотонов.

В табл. 2 представлены все необходимые параметры для оценки суммарных потерь при использовании приемной оптической станции с апертурой 300 мм.

Для более наглядного представления информации выразим потери, рассчитанные по формуле (9), в дБ:

$$\eta_{link}(t)=-10\lg\left(\eta(t)\right). \qquad (10)$$

По графикам, представленным на рис. 2 можно определить, что разница потерь для положения спутника на краю траектории ($\theta_{el}=20^\circ$, $t=135$ с) и в зените ($\theta_{el}=90^\circ$, $t=0$ с) составляет 9 дБ для наилучших погодных условий и 15 дБ для наихудших.

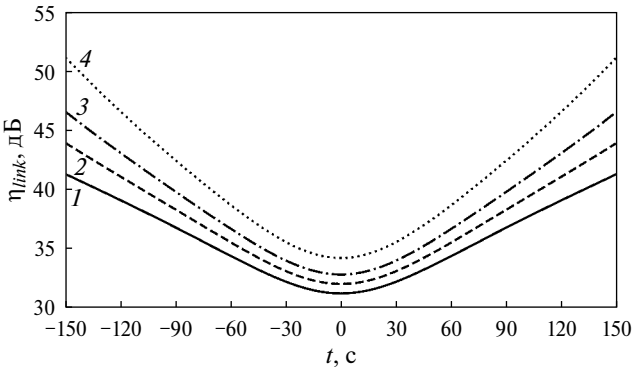

Рис. 2. Суммарные потери в линии связи в случае отличных погодных условий (*1*, сплошная кривая), хороших (*2*, штриховая кривая), средних (*3*, штрихпунктирная кривая), плохих (*4*, пунктирная кривая).

Передача однофотонного сигнала по линии связи «спутник–Земля»

Для оценки ключевых параметров сеанса КРК была использована модель, представленная в работе [14]. Согласно этой модели, передача *i*-фотонного состояния по каналу связи, описывается выражением

$$\eta_i(t)=1-\left(1-\eta(t)\right)^i, \qquad (11)$$

где $i=0, 1, 2...$

Согласно теории, число фотонов в каждом слабом когерентном импульсе лазерного источника имеет распределение Пуассона [6]. В нашем случае при реализации протокола BB84 Decoy State сигнальные импульсы имеют интенсивность сигнала $\mu=0.8$, состояния-приманки — $v=0.1$ и состояния вакуума — $\lambda=0$, которые испускаются случайным образом с вероятностями $p_s=0.5$, $p_d=0.25$ и $p_v=0.25$ соответственно.

Величина фонового шума Y_0, который представляет собой темновые срабатывания детектора, была определена экспериментальным путем при

Таблица 2. Параметры для оценки суммарных потерь в линии связи

Апертура, D_t, м	Обструкция, e	Расходимость, γ, рад	Коэф. экстинкции атмосферы, α	Эффективность оптики, η_{opt}	Эффективность детекторов, η_{det}
0.3	0.81	10^{-5}	0.1—1	0.5	0.62

Таблица 3. Параметры для моделирования сеанса распределения ключей

Тип импульса	Интенсивность, фотон·имп$^{-1}$	Вероятность отправки, p	Частота импульсов, f, МГц	Фоновый шум, Y_0, клик·с$^{-1}$	Ошибка детектирования, e_{det}
Сигнал, μ	0.8	0.50	100	250	0.01
Приманка, v	0.1	0.25			
Вакуум, λ	0	0.25			

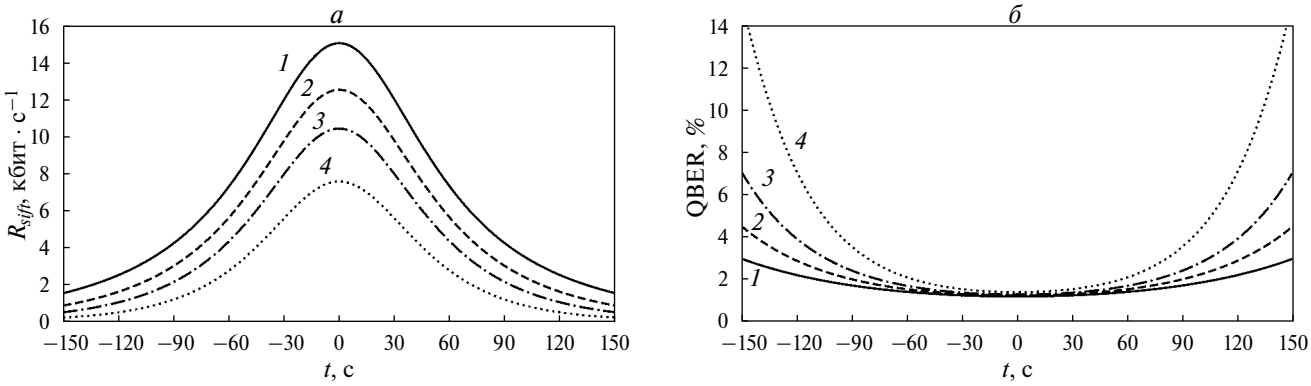

Рис. 3. Скорость генерации просеянного ключа (а) и коэффициент квантовых битовых ошибок (б) в случае отличных погодных условий (*1*, сплошная кривая), хороших (*2*, штриховая кривая), средних (*3*, штрихпунктирная кривая), плохих (*4*, пунктирная кривая).

сопровождении спутника с выключенным передатчиком КРК. Уровень шума был постоянным на протяжении всего сеанса связи и составил 250 кликов/с для наземной станции с апертурой 300 мм.

Кроме того, ошибка детектирования (вероятность попадания фотона в ошибочный детектор) e_{det}, вызванная точностью измерений приемника, не зависела от расстояния и составила порядка 1 %. Значения, использованные для моделирования сеанса КРК, перечислены в табл. 3.

Скорость генерации просеянного ключа R_{sift} и коэффициент квантовых битовых ошибок QBER были рассчитаны с учетом параметров оптической линии связи, а также технических характеристик устройств Алисы и Боба по оценочным выражениям, предложенным в работе [14]:

$$R_{sift}(t) = \frac{1}{2} f p_s \left(Y_0 + 1 - e^{-\mu\eta_1(t)} \right), \qquad (12)$$

$$\mathrm{QBER}(t) = \frac{1}{2} \frac{f p_s \left(e_0 Y_0 + e_{det} \left(1 - e^{-\mu\eta_1(t)} \right) \right)}{R_{sift}(t)}, \qquad (13)$$

где f — частота следования импульсов, e_0 — ошибка, равная 0.5 для протокола BB84 Decoy State, $\eta_1(t)$ — эффективность передачи однофотонного состояния.

На рис. 3 представлены расчетные значения R_{sift} и QBER для зенитного пролета спутника в зависимости от погодных условий. Видно, что скорость распределения просеянного ключа и коэффициент ошибок имеют сильную зависимость от угла места и изменяются неравномерно по ходу проведения сеанса КРК.

Оценка длины ключа

Длину просеянного ключа l_{sift} после процедуры сверки базисов можно определить, исходя из информации о скорости его распределения между абонентами, а также длительности сеанса связи:

$$l_{sift} = \int_{t_1}^{t_2} R_{sift} dt, \qquad (14)$$

где t_1 и t_2 — время начала и окончания сеанса КРК, соответственно.

Финальный же ключ пользователи получают из просеянного после выполнения ряда процедур и математических операций по коррекции ошибок и усилению секретности. Нижний предел длины секретного ключа l_{sec} оценивается выражением

$$l_{sec} \geq N p_s q \left(Q_1 \left(1 - H_2(e_1) \right) - \varepsilon Q_\mu H_2(E_\mu) \right), \qquad (15)$$

где N — общее количество импульсов, излучаемых источником, p_s — вероятность испускания сигнального импульса, q — ошибка выбора базиса (для протокола BB84 Decoy State $q = 0.5$), Q_1 — усиление однофотонных состояний, Q_μ — усиление состояний сигнала с интенсивностью μ, $H_2(p)$ — функция бинарной энтропии Шеннона, e_1 — коэффициент ошибок однофотонных состояний, E_μ — среднее значение квантовых битовых ошибок за сеанс, ε — коэффициент эффективности коррекции ошибок, равный 1.44 [15].

Для того, чтобы определить длину ключа, необходимо знать, от чего зависят и как рассчитываются величины, входящие в состав выражения (15). Например, под бинарной энтропией Шеннона понимают меру неопределенности случайной величины, принимающей значения 0 и 1. Она показывает количество информации, содержащейся в сообщении, и определяется выражением

$$H_2(p) = -p \log_2(p) - (1-p) \log_2(1-p), \qquad (16)$$

где p — вероятность того, что случайная бинарная величина равна 1.

Если значение p близко к 0 или 1, то энтропия Шеннона будет близка к 0. Это означает, что сообщение содержит мало информации и практически

известно. Если же вероятность p равна 0.5, то энтропия будет максимальна и равна 1.

Важным параметром является вероятность обнаружения на стороне Боба i-фотонного состояния, посланного Алисой, Y_i (здесь и далее $i = 1$). Эта величина зависит от уровней фонового шума Y_0 и полезного квантового сигнала η_i:

$$Y_i = Y_0 + \eta_i - Y_0\eta_i \approx Y_0 + \eta_i. \qquad (17)$$

Усиление i-фотонного состояния Q_i представляет собой произведение вероятности того, что Алиса отправит i-состояние в соответствии с распределением Пуассона и вероятности события обнаружения этого состояния Бобом:

$$Q_i = Y_i \frac{\mu^i}{i!} e^{-\mu}. \qquad (18)$$

Частота ошибок i-фотонного состояния e_i определяется выражением

$$e_i = \frac{e_0 Y_0 + e_{det}\eta_i}{Y_i}, \qquad (19)$$

где e_0 — частота ошибок фона, равная 0.5, т. к. фон случаен.

Усиление состояний сигнала Q_μ с интенсивностью μ вычисляется по формуле

$$Q_\mu = \sum_{i=0}^{\infty} Y_i \frac{\mu^i}{i!} e^{-\mu} = Y_0 + 1 - e^{-\eta_i\mu}. \qquad (20)$$

Среднее значение квантовых битовых ошибок за сеанс E_μ:

$$E_\mu = \sum_{i=0}^{\infty} e_i Y_i \frac{\mu^i}{i!} e^{-\mu} = e_0 Y_0 + e_{det}\left(1 - e^{-\eta_i\mu}\right). \qquad (21)$$

В табл. 4 представлены итоговые результаты моделирования сеанса КРК для случая пролета спутника над наземной станцией через зенит (сеанс начинается, когда спутник достигает угловой высоты, равной 20°). Значения R_{sift} и QBER из данной таблицы согласовываются с графиками на рис. 3 для временного промежутка от −135 с до 135 с, что соответствует длительности сеанса КРК 270 с.

Описание оптического приемного модуля системы КРК

Оптическая схема наземного приемного модуля для регистрации однофотонных сигналов со спутника показана на рис. 4а. Данный модуль объединяет в себе следующие функциональные узлы:

1) телескоп Шмидта–Кассегрена (SCT) с фокусным расстоянием 3 м и апертурой 0.3 м для наведения и слежения за космическими аппаратами;

2) модуль анализа и обработки оптических сигналов (APS), где разделяются квантовый и опорный сигналы от спутника;

3) поляризационный анализатор (PA), представляющий собой блок декодера по протоколу BB84;

4) блок электроники с детекторами одиночных фотонов (SPD) для регистрации сигнального излучения;

5) телескоп-гид (GT) для первичного грубого наведения на спутник;

6) блок приема опорного сигнала (SCM) для синхронизации времени отправки и приема квантовых состояний.

Принцип работы приемного модуля заключается в следующем. Когда спутник выходит из тени Земли, в систему автоматического наведения и сопровождения наземной станции передаются TLE-координаты космического аппарата для начала процедуры отслеживания целевого объекта. TLE (Two-Line Element set) — это формат описания орбитальных параметров и прогнозирования положений и скоростей искусственных спутников Земли в режиме реального времени. Опорно-поворотное устройство станции осуществляет поворот оптико-механического блока по заданному TLE-координатами направлению. Начинается процедура грубого слежения за спутником, в ходе которой происходит удержание целевой точки в поле зрения камеры телескопа-гида за счет лишь прецизионной механики, позволяющей добиться плавного и равномерного ведения трубы телескопа. Далее включается наземный лазерный маяк с длиной волны 671 нм, работающий в непрерывном режиме. После обнаружения этого сигнала

Таблица 4. Результаты моделирования сеанса распределения ключей для случая пролета спутника над наземной станцией через зенит

Параметр	Погодные условия			
	Отличные	Хорошие	Средние	Плохие
Коэффициент экстинкции атмосферы, α	0.1—0.3	0.31—0.50	0.51—0.70	0.71—1.00
Потери в канале, η_{link}, дБ	31—40	32—43	33—45	34—49
Скорость генерации ключа, R_{sift}, кбит·с$^{-1}$	1.9—15.0	1.2—12.6	0.7—10.4	0.3—7.6
Длина просеянного ключа, l_{sift}, кбит	2000	1582	1245	830
Длина секретного ключа, l_{sec}, кбит	456	310	192	36
QBER,%	1.20—2.60	1.24—3.64	1.29—5.34	1.4—10.7

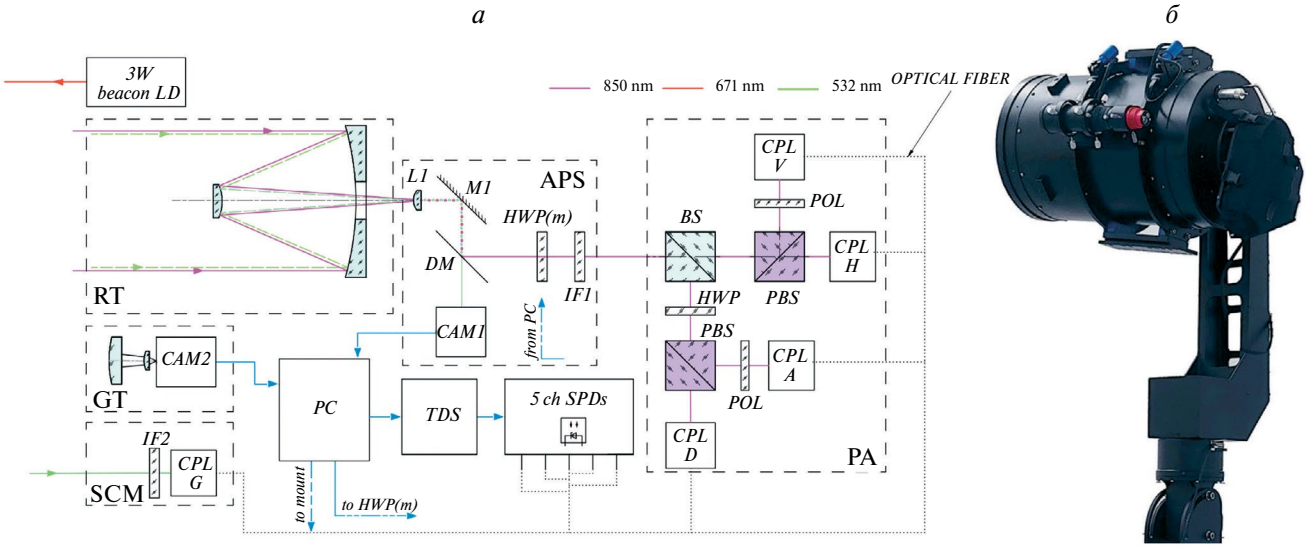

Рис. 4. Наземная оптическая станция [11]: оптическая схема (а) и внешний вид (б).

системой наведения спутника, космический аппарат активирует свой лазер-маяк с длиной волны 532 нм и частотой следования импульсов 10.7 кГц. Это излучение также используется приемным терминалом для синхронизации отправленных и принятых квантовых состояний. Передача квантового сигнала на длине волны 850 нм начинается не ранее, чем спутник поднимется на 20° над горизонтом. Собранное телескопом Шмидта–Кассегрена (SCT) излучение разделяется по спектру дихроичным зеркалом (DM). Сигнал маяка проходит сквозь данное зеркало без отражения и попадает на матрицу камеры (CAM1), обеспечивающей обратную связь для контура точного наведения. В данном случае специальный алгоритм вычисляет положение центра лазерного пятна относительно центра матрицы и на основе полученных значений отклонений корректирует скорость поворота оптико-механического блока. Квантовый же сигнал, отражаясь от дихроичного зеркала, проходит через набор моторизованных волновых пластин (CP(m)), предназначенных для компенсации поворота плоскости поляризации фотонов, узкополосный интерференционный фильтр (IF1) и попадает в блок дешифратора по протоколу BB84 (PA). Там фотоны случайным образом проходят в одно из плеч светоделительного куба (BS), который делит падающий на него поток излучения в соотношении 50:50, реализуя тем самым пассивный выбор измерительного базиса. В каждом из базисов расположен поляризационный светоделительный куб (PBS), который разделяет ортогональные поляризационные состояния на два канала. Для увеличения коэффициента экстинкции поляризации и, соответственно, уменьшения уровня квантовых битовых ошибок, в отражающем плече такого куба дополнительно установлен поляризатор (POL). Таким образом, попадая в один из четырех каналов, сигнал при помощи коллиматора заводится в оптическое волокно и по нему направляется на приемную площадку детектора одиночных фотонов (SPD). При регистрации фотона детектор посылает электрический импульс на время-цифровой преобразователь (TDC), который фиксирует время срабатывания детектора.

ЗАКЛЮЧЕНИЕ

Описана мобильная наземная оптическая станция для приема квантовых сигналов со спутника, разработанная с учетом требований к миниатюризации. Вес станции составляет 150 кг, что позволяет разместить ее и протестировать на крышах зданий в черте мегаполиса.

Осуществлено математическое моделирование процедуры спутникового квантового распределения ключей, выполнена оценка длины секретного ключа и уровня ошибок в ходе сеанса квантовой связи между спутником Micius и нашим наземным приемным терминалом. Полученные результаты показывают перспективу использования оптических станций малого формата для решения задач спутниковой квантовой криптографии. Применение таких портативных станций позволит в будущем развернуть глобальную квантовую сеть. Кроме того, наш оптический модуль может быть использован в качестве приемного терминала для высокоскоростной космической лазерной связи.

Работа выполнена при поддержке Министерства образования и науки Российской Федерации в рамках Программы стратегического академического лидерства «Приоритет 2030» (Стратегический проект «Квантовый Интернет»).

СПИСОК ЛИТЕРАТУРЫ

1. *Трушечкин А.С., Киктенко Е.О., Кронберг Д.А., Федоров А.К.* // УФН. 2021. Т. 191. № 1. С. 93; *Trushechkin A.S., Kiktenko E.O., Kronberg D.A., Fedorov A.K.* // Phys. Usp. 2021. V. 64. No. 1. P. 88.
2. *Балыгин К.А., Кулик С.П., Молотков С.Н.* // Письма в ЖЭТФ. 2022. Т. 116. № 2. С. 128; *Balygin K.A., Kulik S.P., Molotkov S.N.* // JETP Lett. 2022. V. 116. No. 2. P. 128.
3. *Курочкин В.Л., Неизвестный И.Г.* // Изв. РАН. Сер. физ. 2015. Т. 79. № 2. *С.* 195; *Kurochkin V.L., Neizvestnyj I.G.* // Bull. Russ. Acad. Sci. Phys. 2015. V. 79. No. 2. P. 173.
4. *Wang S., Yin Z.Q., He D.Y. et al.* // Nature Photonics. 2022. V. 16. No. 2. P. 154.
5. *Хмелев А.В., Дуплинский А.В., Майборода В.Ф. и др.* // Письма в ЖТФ. 2021. Т. 47. № 17. *С.* 46; *Khmelev A.V., Duplinsky A.V., Mayboroda V.F. et al.* // Tech. Phys. Lett. 2021. V. 47. No. 12. P. 858.
6. *Liao S.K., Cai W.Q., Liu W.Y. et al.* // Nature. 2017. V. 549. No. 7670. P. 43.
7. *Yin J., Li Y.H., Liao S.K. et al.* // Nature. 2020. V. 582. No. 7813. P. 501.
8. *Liao S.K., Cai W.Q., Handsteiner J. et al.* // Phys. Rev. Lett. 2018. V. 120. No. 3. Art. No. 030501.
9. *Liao S.K., Yong H.L., Liu C. et al.* // Nature Photonics. 2017. V. 11. No. 8. P. 509.
10. *Bedington R., Arrazola J.M., Ling A.* // NPJ Quantum Inf. 2017. V. 3. Art. No. 30.
11. *Khmelev A.V., Ivchenko E.I., Miller A.V. et al.* // Entropy. 2023. V. 25. No. 4. Art. No. 670.
12. *Kim I.I., McArthur B., Korevaar E.J.* // Proc. SPIE. 2001. V. 4214. P. 26.
13. *Young A.T., Irvine W.M.* // Astron. J. 1967. V. 72. No. 8. P. 945.
14. *Ma X., Qi B., Zhao Y., Lo H.K.* // Phys. Rev. A. 2005. V. 72. No. 1. Art. No. 012326.
15. *Kiktenko E.O., Trushechkin A.S., Lim C.C.W. et al.* // Phys. Rev. Appl. 2017. V. 8. No. 4. Art. No. 044017.

Ground station efficiency for quantum communications

K. A. Barbyshev[1,2]*, A. V. Duplinsky[1,3], A. V. Khmelev[1,3], V. L. Kurochkin[1,4]

[1] QSpace Technologies LLC, Moscow, 143026, Russia
[2] National Research University "Moscow Power Engineering Institute", Moscow, 111250, Russia
[3] HSE University, Moscow, 101000, Russia
[4] National University of Science and Technology "MISIS", Moscow, 119049, Russia
**e-mail: k.barbyshev@goqrate.com*

We investigated the possibility of practical implementation of a quantum communication link for encryption key distribution between a Micius satellite and a mobile ground optical station. Thanks to theoretical estimation numerical values of the main parameters of such a communication link are obtained: total loss, key generation rate and secret key length, as well as quantum bit error rate.

Keywords: satellite quantum cryptography, quantum key distribution, encryption key, ground station