ИЗВЕСТИЯ РАН. СЕРИЯ ФИЗИЧЕСКАЯ, 2024, том 88, № 6, с. 981–985

УДК 004.056.55

УЛУЧШЕНИЕ ОЦЕНКИ ДЛИНЫ СЕКРЕТНОГО КЛЮЧА В КАНАЛЕ СПУТНИК–ЗЕМЛЯ

© 2024 г. Е. И. Ивченко[1, 2, 3, 4]*, А. В. Хмелев[1, 2, 3], В. Л. Курочкин[1, 2, 3, 4]

[1] Федеральное государственное автономное образовательное учреждение высшего образования «Московский физико-технический институт (национальный исследовательский университет)», Долгопрудный, Россия

[2] Общество с ограниченной ответственностью «Международный центр квантовой оптики и квантовых технологий», Москва, Россия

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

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

** e-mail: ivchenko.ei@phystech.edu*

Поступила в редакцию 15.12.2023
После доработки 29.01.2024
Принята к публикации 26.02.2024

Исследована и оптимизирована длина секретной последовательности в зависимости от интервалов разбиения сеанса связи в ходе квантового распределения ключей между спутником и наземной станцией. В силу динамически изменяющихся параметров канала предложенная методика позволяет значительно увеличить скорость генерации ключа.

Ключевые слова: квантовая криптография, спутниковые коммуникации, пост-обработка данных

DOI: 10.31857/S0367676524060214, **EDN:** PFFVHM

ВВЕДЕНИЕ

Сегодня в области защиты информации бурно развивается направление квантового распределения ключей (КРК) [1—3], которое гарантирует создание абсолютно секретного ключа для передачи данных, на основании физических законов [4]. На сегодняшний день наиболее развита область оптоволоконной криптографии [5—7], но расстояние для генерации ключа таким способом довольно ограничено из-за экспоненциального затухания. По этой причине возникла идея передачи квантовых состояний в открытом пространстве по каналу спутник-земля [8, 9].

В этой работе мы рассматриваем квантовое распределение ключей между спутником и наземной станцией [9], где биты информации кодируются в состояниях поляризации посылаемых фотонов. Процедура КРК выполняется по протоколу BB84 с пассивным выбором поляризационного базиса и с использованием состояний ловушек. В представленной работе решается задача разбиения отрезка пролета на временные интервалы для оптимальной постобработки данных.

Спутниковое квантовое распределение ключей характеризуется непостоянством параметров канала в процессе сеанса связи. Следовательно, применение алгоритмов оценки финального ключа для оптоволоконных линий в нашем случае возможно только с некоторыми допущениями. Для подходов с неизменным каналом связи мы оцениваем среднюю статистику и уровень ошибок за весь интервал, а далее работаем с этими значениями. Однако при таком способе обработки и при наличии «плохих» интервалов времени сильно занижается ключ, а также могут возникнуть проблемы с секретностью ключа. Таким образом, возникает необходимость выполнять разбиение сеанса связи на интервалы с длиной, достаточной для накопления статистики, но не слишком большой, чтобы изменение параметров не превосходило теоретические оценки в процессе постобработки.

МОДЕЛИРОВАНИЕ КАНАЛА

Для моделирования спутникового КРК понадобятся следующие параметры экспериментальной установки: среднее число фотонов на импульс (μ, ν, λ) и вероятность испускания (p_s, p_d, p_v) для разных типов состояний (сигнальных, состояний ловушек и вакуумных, соответственно), вероятность ошибки при детектировании бита информации (e_{det}), вероятность регистрации вакуумного клика на один испущенный импульс (Y_0), вероятность ошибки в вакуумных состояниях ($e_0 = 0.5$) и частота испускания квантовых состояний (f). Эти параметры указаны в табл. 1. Воспользуемся результатами статьи [10]

Таблица 1. Параметры экспериментальной установки КРК

Среднее число фотонов	μ	ν	λ
	0.8	0.1	10^{-6}
Вероятность испускания состояния	p_s	p_d	p_v
	0.5	0.25	0.25
Частота генерации квантовых импульсов f, Гц	10^8		
Вероятность ошибки в принятии бита e_{det},%	0.5		
Вероятность вакуумных срабатываний на испущенный импульс Y_0	$5\cdot10^{-6}$		

и представленными параметрами для расчета пропускания $\eta(t)$ канала спутник–земля от времени.

Далее, предполагая, что число фотонов в импульсном лазерном излучении подчиняется пуассоновскому распределению с заданным средним значением, основываясь на результатах исследований [11], получим теоретический вид вероятности принятия квантовых состояний со средним числом фотонов в импульсе $\delta_\varphi \in \{\mu, \nu, \lambda\}$ и квантовых битовых ошибок (QBER_φ) в них:

$$Q_\varphi = 1-(1-Y_0)\cdot e^{-\eta_\varphi(t)\delta_\varphi}, \quad (1)$$

$$\mathrm{QBER}_\varphi = \frac{e_\varphi}{Q_\varphi} = \frac{e_0 Y_0 + e_{det}\left(1-e^{-\eta_\varphi(t)\delta_\varphi}\right)}{Q_\varphi}, \quad (2)$$

где $\varphi \in \{s,d,v\}$ обозначает тип состояний (сигнальные, состояния ловушки, вакуумные соответственно).

Чтобы получить количество кликов из вероятности их принятия, нужно умножить вероятность на число испущенных импульсов соответствующего типа.

После получения средних значений принятого сигнала и ошибок в нем необходимо сгенерировать помехи. Чаще всего в реальных экспериментах встречаются два вида помех. Первый — статистические флуктуации вокруг среднего значения и второй — значительное ослабление пропускания канала. Первый вид помех имеет полностью вероятностную природу, поэтому эти шумы присутствуют всегда, и их величина пропорциональна корню из среднего значения числа кликов или ошибок. Источник второго вида помех связан с нестабильностью работы экспериментального оборудования, плохими погодными условиями и другими подобными причинами. Величина данных флуктуаций пропорциональна $N\dfrac{T-\tau}{\tau}$, где N — среднее значение числа кликов, τ — промежуток времени, на котором возникли шумы, T — полное время связи со спутником.

Результаты моделирования статистических флуктуаций представлены на рис. 1, а случай присутствия второго типа помех проиллюстрирован на рис. 2.

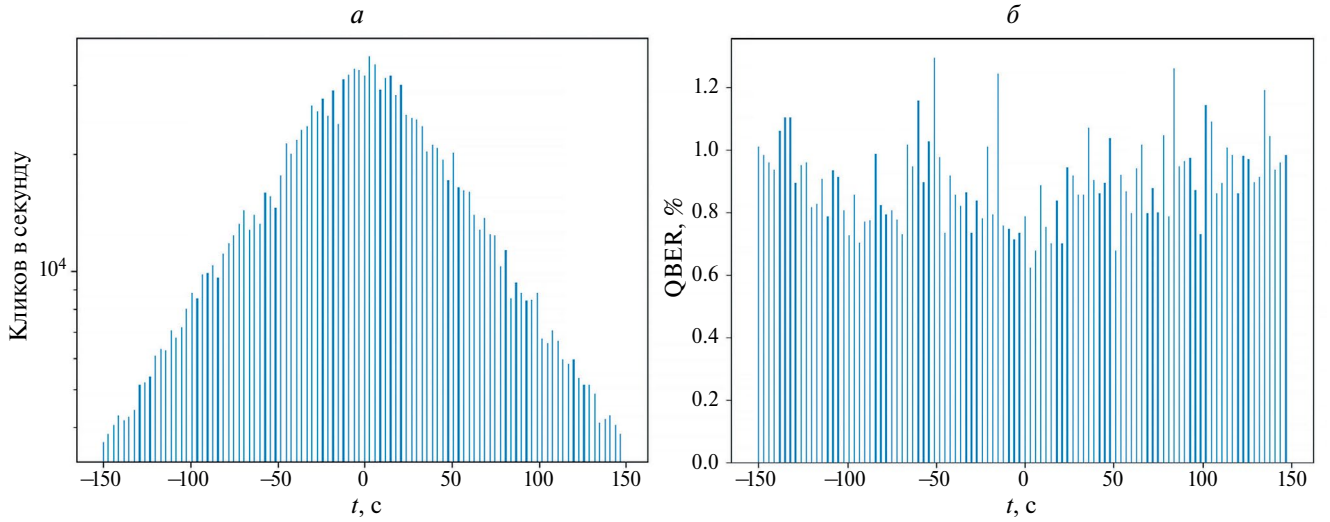

Рис. 1. Гистограммы зависимости количества полученных кликов (а) и процента квантовых битовых ошибок (QBER) в них (б) для случая небольших флуктуаций в районе модельных средних значений.

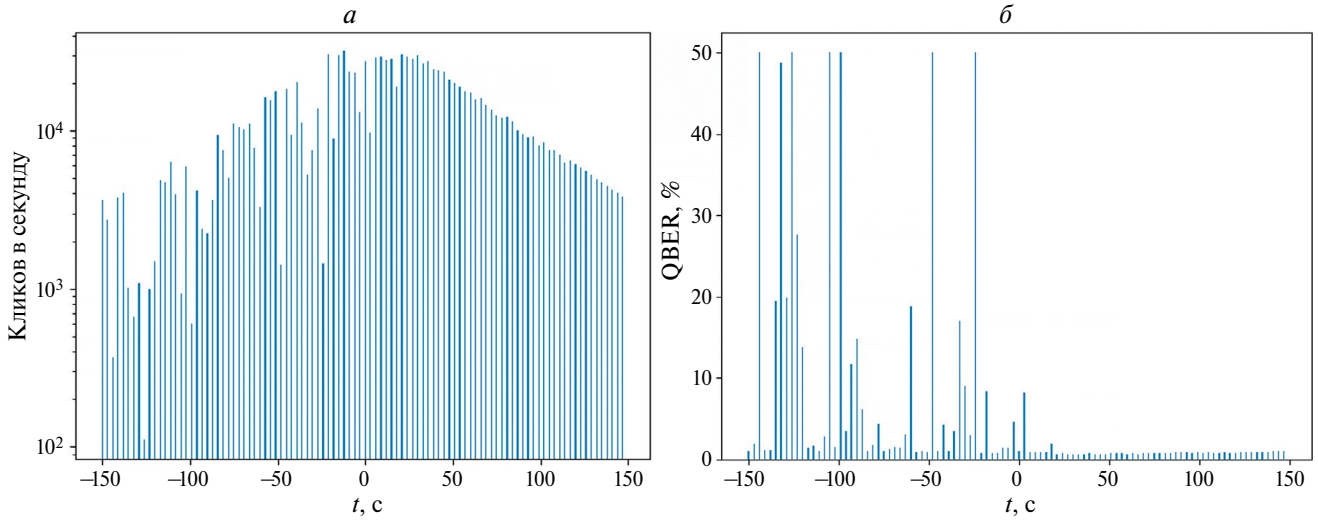

Рис. 2. Гистограммы зависимости количества полученных кликов (а) и процента квантовых битовых ошибок (QBER) в них (б) для случая значительных флуктуаций, которые могут быть связаны с нестабильностью работы экспериментального оборудования и плохими погодными условиями.

ВЫДЕЛЕНИЕ ОПТИМАЛЬНОГО РАЗБИЕНИЯ

Длина финального ключа зависит от двух параметров: количества зарегистрированных импульсов и процента квантовых битовых ошибок (QBER). Уровень квантовых битовых ошибок отвечает за секретность последовательности и влияет на длину ключа сильнее чем величина зарегистрированных кликов, которая линейно масштабирует секретную последовательность. Это можно видеть из следующего выражения для скорости генерации ключа [11]:

$$R_{sec} \geq p_s q\left(Q_1\left(1-H_2\left(e_1\right)\right)-f_{ec}Q_{\mathrm{s}}H_2\left(E_{\mathrm{s}}\right)\right), \quad (3)$$

где $f_{ec} = 1.41-$ эффективность процедуры коррекции ошибок, $q = 0.5$ — коэффициент просеивания ключа, $H_2(x) = x\log_2(x) - (1-x)\log_2(1-x) -$ бинарная энтропия, Q_1 — вероятность принятия квантовых состояний, содержащих ровно один фотон и e_1 — вероятность ошибки в них.

Поэтому далее в работе рассуждения основываются на рассмотрении влияния процента ошибок на финальный ключ.

Определить отрезки разбиения можно из следующего соотношения:

$$\mathrm{QBER}^L \leq \overline{\mathrm{QBER}_L} \leq \overline{\mathrm{QBER}_U} \leq \mathrm{QBER}^U. \quad (4)$$

Это соотношение связывает верхние нижние значения среднего $\overline{\mathrm{QBER}}$, которое получается методами математического моделирования для некоторого временного интервала, и верхние нижние пределы экспериментального QBER, которые находятся из оценок границ Чернова на статистические флуктуации. Разделение времени пролета спутника на интервалы с соблюдением данного условия позволяет максимизировать длину финального ключа с применением теории для оптоволоконных линий связи.

Основной проблемой для спутникового КРК является динамическое изменение параметров канала в процессе генерации ключа. Из-за этого мы можем узнать только усредненные параметры нашего КРК за некоторый временной промежуток. Определение уровня ошибок требует раскрытия части полученной информации, в силу этого невозможно получить полный профиль ошибок экспериментальным путем. Следовательно, необходимо восстановить профиль ошибок в зависимости от времени по измеренной в процессе эксперимента статистике кликов. Для этого нужно определить верхнюю и нижнюю границу ошибок. Верхнюю границу оцениваем из предположения, что количество ошибок не уменьшается, а нижнюю находим при помощи умножения числа ошибок на функцию, моделирующую число квантовых кликов, для сохранения процента ошибок. После восстановления границ ошибок можно выделять отрезки разбиения исходя из условия (4).

На сегодняшний день в спутниковом КРК используется метод обработки полученной информации блоками одинаковой длины [9], для этого исходные данные делятся на части примерно равной величины. Графики зависимости длины ключа при оптимальном разбиении от размера блоков представлены на рис. 3. Анализ полученной зависимости показывает, что при использовании предложенного метода можно значительно увеличить ключ только для случая сильных помех в канале, при слабых флуктуациях эффективнее обрабатывать сразу весь промежуток.

Сравнение результатов представленного метода было проведено со случаем, когда для постобработки используются суммарные данные со всего пролета.

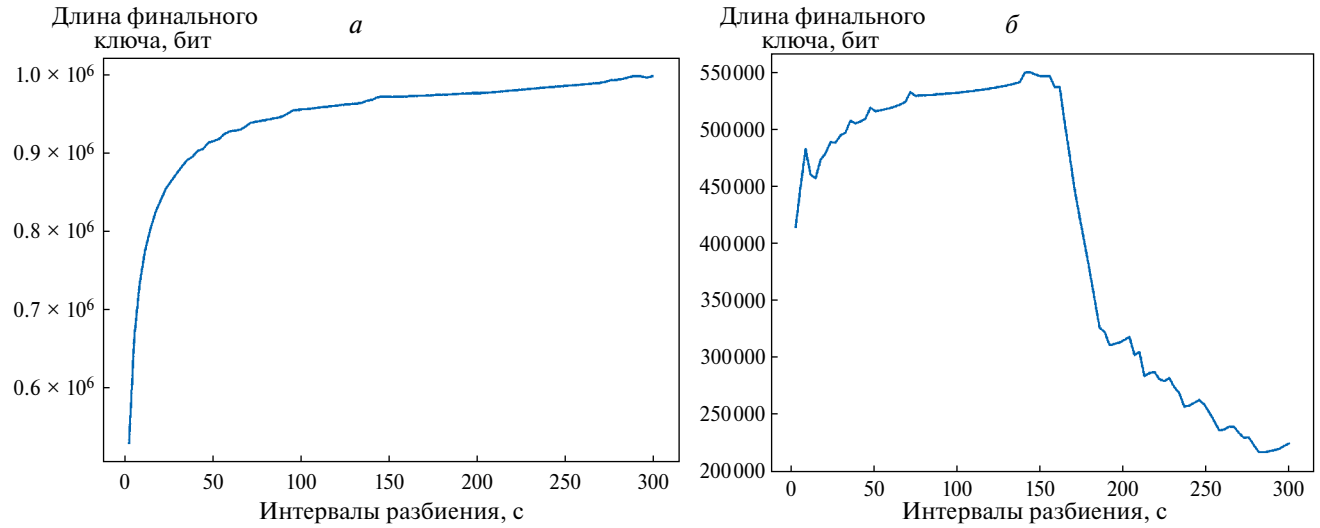

Рис. 3. Графики зависимости длины финального ключа в зависимости от размера отрезков разбиения интервала сеанса связи в случае небольших флуктуаций (а) и для больших отклонений (б) числа кликов от теоретического среднего.

Такой подход использует максимальный набор статистики, что позволяет минимизировать статистические флуктуации, и является оптимальным для случая отсутствия в канале помех.

ЗАКЛЮЧЕНИЕ

При использовании разработанного метода постобработки для случая малых флуктуаций около средних значений, скорость генерации слабо зависит от длины отрезков разбиения. Для такого подхода отличие в результатах со случаем обработки всего пролета может составлять не более двух процентов, так как по критерию разбиения можно брать почти весь интервал. Иначе дело обстоит при наличии значительных ослаблений пропускания канала (рис. 2), которые могут быть связаны с нестабильностью работы экспериментального оборудования, плохими погодными условиями и другими подобными причинами. В этих случаях обработка описанным методом приводит к увеличению скорости генерации до 60%. Также существуют случаи, когда по полному интервалу ключ не генерируется, но, правильно подобрав отрезки временного разбиения, можно получить ненулевую секретную последовательность.

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. *Gisin N., Ribordy G., Tittel W., Zbinden H.* // Rev. Mod. Phys. 2002. V. 74. No. 1. P. 145.
2. *Кронберг Д.А., Ожигов Ю.И., Чернявский А.Ю.* Квантовая информатика и квантовый компьютер: учебное пособие. М.: МАКС Пресс, 2011. 64 с.
3. *Bennett C.H., Brassard G.* // arXiv:2003.06557. 2020.
4. *Shor P.W., Preskill J.* // Phys. Rev. Lett. 2000. V. 85. No. 2. P. 441.
5. *Курочкин В.Л., Кривякин Г.К., Зверев А.В. и др.* // Изв. РАН. Сер. физ. 2016. Т. 80. № 1. С. 10; *Kurochkin V.L., Krivyakin G.K., Zverev A.V. et al.* // Bull. Russ. Acad. Sci. Phys. 2016. V. 80. No. 1. P. 5.
6. *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.
7. *Lucamarini M., Yuan Z.L., Dynes J.F., Shields A.J.* // Nature. 2018. V. 557. No. 7705. P. 400.
8. *Курочкин В.Л., Коляко А.В.* // Изв. РАН. Сер. физ. 2016. Т. 80. № 1. С. 5; *Kurochkin V.L., Kolyako A.V.* // Bull. Russ. Acad. Sci. Phys. 2016. V. 80. No. 1. P. 1.
9. *Liao S.K., Cai W.Q., Liu W.Y. et al.* // Nature. 2017. V. 549. No. 7670. P. 43.
10. *Khmelev A.V., Ivchenko E.I., Miller A.V. et al.* // Entropy. 2023. V. 25. No. 4. Art. No. 670.
11. *Ma X., Qi B., Zhao Y., Lo H.K.* // Phys. Rev. A. 2005. V. 72. No. 1. Art. No. 012326.

Improving length estimation of the secret key in satellite-to-ground quantum channel

E. I. Ivchenko[1, 2, 3, 4]*, A. V. Khmelev[1, 2, 3], V. L. Kurochkin[1, 2, 3, 4]

[1] Moscow Institute of Physics and Technology, Dolgoprudny, 141701, Russia
[2] International Center for Quantum Optics and Quantum Technologies, Moscow, 121205, Russia
[3] QSpace Technologies LLC, Moscow, 143026, Russia
[4] National University of Science and Technology "MISIS", Moscow, 119049, Russia
** e-mail: ivchenko.ei@phystech.edu*

We study and optimize the length of the secret sequence depending on the intervals of splitting the communication session between the satellite and the ground station during the quantum key distribution. Due to dynamically changing channel parameters, the proposed technique allows for significant increases in the final key rate and length.

Keywords: Quantum cryptography, satellite communication, post-processing