АЛГОРИТМ ОБНАРУЖЕНИЯ СИГНАЛА СИНХРОНИЗАЦИИ В КВАНТОВЫХ СЕТЯХ

Плёнкин А. П.[1]

DOI: 10.21681/2311-3456-2025-6-81-87

Цель исследования: *разработка и исследование алгоритма обнаружения оптического сигнала для синхронизации станций системы квантового распределения ключей с повышенной защищенностью от несанкционированного доступа.*

Методы исследования: *вероятностное распределение, статистический анализ, однофотонная регистрация.*

Результаты исследования: *обоснована важность процесса временной синхронизации, которая реализуется посредством высокоточного обнаружения оптического сигнала. Исследован алгоритм обнаружения оптического сигнала для метода синхронизации с повышенной защищенностью от несанкционированного доступа. Предложен усовершенствованный алгоритм анализа временной области распространения синхросигнала с использованием лавинных фотодетекторов. Показано, что предложенный алгоритм позволяет использовать лавинные фотодетекторы в режиме одиночного счета фотонов. Проведен анализ временных характеристик разработанного алгоритма синхронизации и представлено аналитическое выражение для расчета временной задержки детектирования, которое обеспечивает последовательный анализ временных окон с учетом перестраиваемого времени восстановления фотодетектора. Аналитическое выражение может использоваться для инженерных расчетов при проектировании системы КРК. Предложенный алгоритм значительно снижает вероятность несанкционированного доступа к процессу синхронизации и позволяет с заданной точностью определить временные параметры сигнального окна, что является критически важным для последующей работы системы квантового распределения ключей.*

Научная новизна: *предложен алгоритм обнаружения оптического сигнала в процессе синхронизации, который отличается повышенной защищенностью от несанкционированного доступа. Представлено аналитическое выражение для инженерных расчетов временной задержки детектирования в процессе синхронизации.*

Ключевые слова: *защищенность, синхронизация, квантовое распределение, однофотонность, оптический импульс.*

Введение

Квантовая криптография позволяет обеспечить безусловную защищенность данных методами квантовой физики [1–3]. Физическим воплощением квантовой криптографии являются системы квантового распределения ключей – сложные технологические устройства, в идеализированном варианте позволяющие обеспечить абсолютную криптостойкость передаваемых данных между пользователями. Целью таких систем является создание у двух устройств одинаковой последовательности случайных символов – одноразового блокнота [4, 5]. Исследования действующих систем квантового распределения ключей (СКРК) показывают наличие несовершенств в технической реализации. Такие несовершенства могут являться уязвимостями, позволяющими получить несанкционированный доступ [6]. Важным процессом в работе систем квантового распределения ключей является синхронизация разнесенной в пространстве аппаратуры. Современные квантовые коммуникации реализуются через технологию квантового распределения ключей (КРК) [7]. В базовой конфигурации «точка-точка» два абонента обмениваются квантовыми сигналами по оптическому каналу связи. Эта простая схема лежит в основе построения более сложных квантовых сетей, включая магистральные. Однако простейшая топология имеет существенные ограничения, главное из которых – максимальная дальность передачи сигнала. Ограничения обусловлены прежде всего физическими свойствами оптического волокна и особенностями работы квантовых протоколов.

Главная задача квантового распределения ключей в магистральных сетях — обеспечить безопасную передачу ключей между удалёнными узлами. Однако существующие технологии сталкиваются с рядом фундаментальных и технических ограничений. Например, ограничение дальности передачи из-за затухания в оптическом волокне. Квантовые сигналы быстро затухают в оптоволокне и уже на расстоянии 100–150 км сигнал становится слишком слабым для детектирования. При этом классические оптические усилители неприменимы, так как они разрушают квантовые состояния, а квантовые повторители невозможно использовать из-за теоремы неклонирования (No-Cloning Theorem). В современных магистральных сетях применяются доверенные промежуточные узлы (ДПУ) — защищённые аппаратные комплексы, где ключи расшифровываются и повторно шифруются. Реализация сетей на основе ДПУ сталкивается с проблемой уязвимости к физическим

1 Плёнкин Антон Павлович, кандидат технических наук, доцент, Южный федеральный университет. г. Таганрог, Россия. E-mail: pljonkin@sfedu.ru

атакам. Кроме того, каждый новый доверенный узел увеличивает общие риски сети. Активные исследования ведутся в направлении сетей с недоверенными узлами (НДУ). Такие сети работают под управлением квантовых протоколов (MDI-QKD, TF-QKD) на основе запутанных фотонов и считается, что безопасность самой сети не зависит от надежности НПУ. Одной из нерешенных задач в квантовых коммуникациях является проблема «последней мили» (last mile). Это финальный этап доставки квантовых ключей от магистральной сети к конечному пользователю. «Последняя миля» — один из ключевых технологических барьеров для массового внедрения квантовой криптографии.

Большинство исследований сегодня сфокусированы на разработке новых квантовых протоколов и методах предотвращения несанкционированного доступа к системам КРК [8–11]. Лишь малая часть научных статей посвящена вопросам аутентификации, идентификации и синхронизации в квантовых сетях [12, 13]. В данной работе мы описываем важность временной синхронизации при квантовом распределении ключей. Временная синхронизация – критически важный процесс, обеспечивающий корректное детектирование квантовых сигналов и дальнейший безопасный обмен ключами. Точность синхронизации напрямую влияет на эффективность обнаружения фотонов, подавление шумов в квантовом канале, скорость генерации ключей. Синхронизация не влияет на криптографическую стойкость самого протокола, однако, в исследованиях [14–15] показано, что доступ к процессу синхронизации дает злоумышленнику несанкционированный доступ к работе системы КРК. Последнее позволяет злоумышленнику влиять[2] на работу системы, вносить управляемые помехи, оставаясь незамеченным [16].

Алгоритм обнаружения оптического импульса

До начала работы квантового протокола станции системы КРК должны провести процедуры аутентификации и идентификации [17, 18]. Роль синхронизации при квантовом распределении заключается, в том числе, в корректном сопоставление сигналов. В протоколах типа BB84 или MDI фотоны передаются в строго определённые временные интервалы и без высокоточной синхронизации приёмник не сможет отличить полезный сигнал от темновых отсчётов детектора или фонового шума. Таким образом, для минимизации ошибок алгоритмы синхронизации стараются добиться пикосекундной точности. В процессе проектирования алгоритмов синхронизации сокращение временного окна детектирования (Δt) способствует снижению вероятности ложных срабатываний фотодетектора.

2 Pljonkin A. Synchronization in quantum key distribution systems / A. Pljonkin, K. Rumyantsev, P. K. Singh // Cryptography. – 2017. – No. 1. – P. 18.

Вероятность ложных срабатываний (темновых отсчётов) лавинного фотодетектора P_{dark} определяется как вероятность регистрации сигнала при отсутствии фотонов. Для лавинных фотодетекторов она вычисляется по формуле:

$$P_{dark} = R_{dark} \cdot \Delta t, \quad (1)$$

где R_{dark} – частота темновых отсчетов.

В реальных системах КРК следует учитывать вероятность так называемого эффекта послеимпульсов $P_{afterpulse}$, который возникает из-за перезаряда детектора. При этом уточненная модель полной вероятности ложного срабатывания будет иметь вид

$$P_{false} = 1 - (1 - P_{dark}) \cdot (1 - P_{afterpulse}). \quad (2)$$

Высокий уровень P_{false} значительно увеличивает уровень квантовых ошибок (QBER) при формировании ключевой последовательности. Например, для протокола BB84 верхний предел значения QBER составляет 11 %. Наиболее эффективными способы снижения P_{false} являются температурный режим ОЛФД и снижение временного интервала детектирования Δt. Приведем пример экспоненциальной зависимости темновых отсчетов детектора от температуры:

$$R_{dark}(T) = R_0 \cdot e^{-\frac{E_g}{k_B \cdot T}}, \quad (3)$$

где E_g – ширина запрещенной зоны, R_0 – константа материала, k_B – постоянная Больцмана, T – температура.

Эмпирическая формула вероятности возникновения послеимпульсов может быть представлена в следующем виде:

$$R_{afterpulse} = n \cdot \left(1 - e^{-\frac{\tau_d}{\tau_r}}\right) \cdot e^{-\frac{v_e}{v_0}}, \quad (4)$$

где n – технологический коэффициент, v_0 – напряжение, v_e – приложенное напряжение, τ_d – мертвое время детектора, τ_r – постоянная времени восстановления.

Таким образом, оба параметра существенно влияют на скорость генерации ключевой последовательности R_{key}:

$$R_{key} = \frac{R_{pulse} \cdot n_{det} \cdot (1 - R_{false})^N}{2}, \quad (5)$$

где N – число детекторов, n_{det} – эффективность детектирования.

Для коммерческого внедрения КРК (особенно в вопросе «последней миле») критически важно улучшать методы синхронизации, делая их доступными и устойчивыми к помехам. Рассмотрим процесс синхронизации на примере коммерческого образца системы КРК. В реализованных системах квантового распределения ключей распространенным решением является многофотонный режим синхронизации,

при котором фотодетекторы работают в линейном режиме, а сам синхроимпульс представляет собой оптический сигнал высокой интенсивности. Методы обнаружения оптического сигнала могут быть реализованы по двухпроходной [19, 20] или однопроходной схеме [21, 22]. Другой метод подразумевает наличие выделенного волокна непосредственно под синхронизацию. Существуют реализации алгоритмов, основанные на мультиплексировании длин волн и временных отрезков. В классическом варианте однопроходной схемы источник излучения формирует периодическую последовательность оптических импульсов и направляет их в квантовый канал (оптическое волокно, соединяющее приемную и передающую станции системы КРК) [23–25]. На приемной стороне фотодетектор анализирует поступающий сигнал. Детектирование происходит пошаговым стробированием интервалов на всей временной оси. Максимальный период следования выбирается из расчета максимального времени, которое требуется импульсу на преодоление оптического пути. Период следования разбивается на временные интервалы, каждый из которых многократно анализируется (на предмет наличия сигнала). Итогом синхронизации должно быть выделение временного интервала длительностью не более 50 пс. Такая точность достигается путем разбиения временных интервалов с наибольшим числом зафиксированных срабатываний на более короткие по времени. При классическом методе синхронизации в системах квантовой связи не применяются алгоритмы защиты и контроля излучения, поэтому злоумышленнику не составляет труда получить доступ к квантовому каналу и использовать полученные данные для внесения управляемых помех в работу системы КРК.

Нами предложен алгоритм обнаружения оптического сигнала синхронизации в квантовых сетях, основанный на слабофотонной передаче и контролируемой мощности излучения. Число фотонов в синхроимпульсе при этом не превышает 10. В таком случае процесс синхронизации технически не отличается от работы квантового протокола. Модель оптического сигнала в предлагаемом алгоритме описывается как поток фотонов, подчиняющийся пуассоновской статистике, мощность которого в момент времени t выражается формулой

$$P(t) = N \cdot h\nu \cdot f(t), \tag{6}$$

где N – число фотонов в импульсе, $h\nu$ – энергия, $f(t)$ – форма импульса.

Так как для детектирования слабофотонного сигнала применяются лавинные фотодетекторы, то вероятностную модель обнаружения необходимо рассматривать для наличия сигнала ($P(n|H_1)$) и наличия только темнового тока ($P(n|H_0)$):

$$P(n|H_1) = \frac{(\eta N)^n \, e^{-\eta N}}{n!} \tag{7}$$

и

$$P(n|H_0) = \frac{(R_{dark} \, T)^n \, e^{-R_{dark} \, T}}{n!}. \tag{8}$$

Так как в исследуемом алгоритме синхронизации лавинные фотодетекторы функционируют в режиме Гейгера (одиночного счета фотонов), то последовательный анализ временных интервалов невозможен. Наиболее важной характеристикой в процессе обнаружения оптического сигнала при синхронизации системы квантового распределения ключей является время восстановления. Этот параметр определяет период неактивности однофотонного лавинного фотодиода после регистрации фотоэлектрона или импульса темнового тока. В современных детекторах значение времени восстановления может программно настраиваться [26]. При этом минимальное время восстановления позволяет увеличить скорость счёта, но повышает вероятность послеимпульсов. Напротив, максимальное значение снижает уровень шумов, но ограничивает частоту детектирования. Таким образом, оптимальный выбор времени восстановления критически важен для баланса между чувствительностью и уровнем шумов детектора. Этот параметр требует тщательной настройки в зависимости от конкретных условий работы СКРК (длина линии, уровень затухания, требования к скорости генерации ключей).

Как уже упоминалось, ключевая задача синхронизации заключается в точном определении момента прихода фотонных импульсов на ОЛФД. Для этого выполняется измерение общей длины квантового канала, учитывающей как протяженность волоконно-оптической линии связи, так и длину оптических трактов внутри системы КРК. Отметим, что для первичного анализа длины можно использовать рефлектометрический метод, который позволит определить ориентировочную длину квантового канала с точностью до нескольких метров. Такой точности недостаточно для синхронизации, но это позволит существенно сократить время анализа временного кадра.

Если источник излучения и фотодетекторы расположены в одной станции (такой подход актуален для топологии «ДПУ – конечный пользователь»), то ослабление сигнала на основе анализа ВОЛС можно осуществлять как на стороне получателя, так и в начале передачи на стороне отправителя. Оптический импульс с длиной волны 1550 нм формируется источником излучения на станции отправителя. Импульс проходит через оптический канал до станции получателя. Предположим, что на обратном пути сигнал ослабляется до слабофотонного уровня и возвращается на ОЛФД станции отправителя. При каждой посылке импульса на ОЛФД подается стробирующий

сигнал, переводящий детектор в режим регистрации одиночных фотонов. Система вычисляет и фиксирует временную задержку стробирующего сигнала и детектор активируется на строго заданный временной интервал, соответствующий ожидаемому окну прихода сигнала. Режим счета одиночных фотонов в ОЛФД активируется с временными интервалами, превышающими время восстановления. Такой подход позволяет анализировать несколько временных окон в рамках одного временного кадра. Факт регистрации (или отсутствия регистрации) фотоэлектронов или темновых отсчетов в отдельных временных окнах не влияет на общую продолжительность анализа временного кадра в режиме обнаружения сигнального окна. Это позволяет сохранять стабильность работы системы независимо от характера поступающих сигналов. На рисунке 1 представлена пространственно-временная диаграмма, иллюстрирующая процедуру сканирования временного периода в ходе синхронизации.

Предположим, что длина ВОЛС между станцией системы КРК в ДПУ и станцией, расположенной у конечного пользователя, составляет 50 км. Тогда, максимальный период следования T будет рассчитываться исходя из расстояния в 100 км (двухпроходная схема распространения) и скорости распространения оптического сигнала в волокне. Для примера рассмотрим популярную модель ОЛФД InGaAs/InP ID Quantique id230. Подобные фотодетекторы применяются в системах КРК и имеют настраиваемое время восстановления в пределах от 1 до 100 мкс. Возьмем среднее значение τ_d = 50 мкс, которое является оптимальным в работе при температуре –30 °C. Зная параметр τ_d, можем установить длительность временного кадра T_k, при соблюдении условия $T_k > \tau_d$. Пусть T_k = 80 мкс. Длительность временного окна nw = 2 нс. Длительность оптического импульса τ_p = 1 нс. Вышеперечисленные параметры позволяют вычислить суммарное количество временных окон в периоде T, во временном кадре T_k и, соответственно, число временных кадров в периоде. После каждой посылки оптического импульса ОЛФД переводится в режим одиночного счета фотонов с учетом временной задержки детектирования Z_{nn}. За один период следования алгоритм анализирует одно временное окно nw в одном временном кадре T_k. После анализа всех временных кадров периода T_0 начинается последовательный просмотр временных окон периода T_1, но значение временной задержки Z_{1n} в каждом кадре теперь увеличивается на длительность временного окна. При анализе каждого nw происходит фиксация фотоэлектронов или темновых отсчетов. Таким образом производится последовательный анализ всей временной области. В результате первого этапа синхронизации алгоритм обнаруживает временные окна ns, в которых были зафиксированы срабатывания фотодетектора и выделяет интервал с максимальным значением.

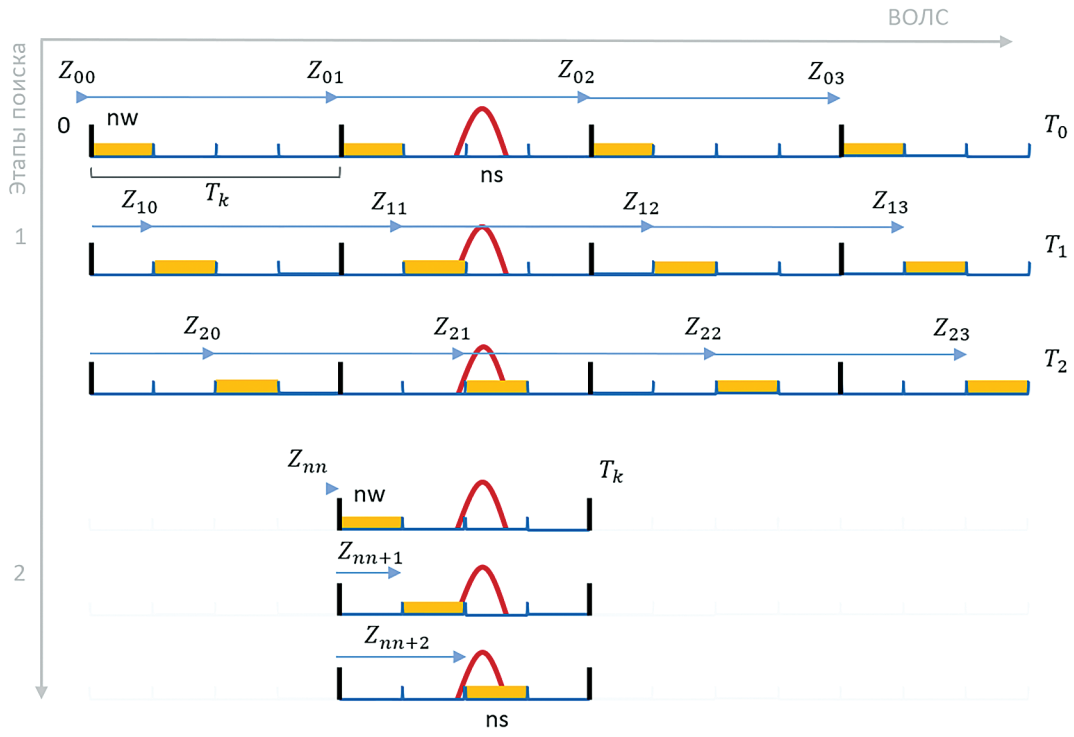

Рис. 1. Временная диаграмма поиска оптического сигнала

Отметим, что объем выборки в каждом временном окне составляет несколько сотен раз. Последнее сделано для того, чтобы минимизировать вероятность ложного срабатывания и однозначно отличить сигнал от темновых отсчетов. На втором этапе синхронизации алгоритм выделяет временной кадр T_k, в котором расположено ns с максимальным числом срабатываний. Отдельно следует выделить случай, когда ns расположены на границе двух временных кадров. В этом случае выделяется два смежных T_k. Далее происходит последовательный анализ всех временных окон в выделенных T_k. Алгоритм поиска на втором этапе аналогичен первому. В результате второго этапа синхронизации обнаруживается временное окно ns с максимальным числом зарегистрированных фотоэлектронов. На следующем этапе происходит дробление обнаруженного временного окна на временные интервалы длительностью по 10 пс. Результатом процесса синхронизации является обнаруженный временной интервал длительностью 10 пс.

Отметим, что в процессе работы квантового протокола требуется периодическая калибровка длины ВОЛС. Последнее связано с физическими изменениями в волокне из-за воздействия внешних факторов. Подстройка может реализовываться каждый раз после нескольких итераций формирования квантового ключа. В таком случае нет необходимости проводить полный анализ всего периода T_n, а достаточным будет реализация уточняющего этапа синхронизации.

Аналитическое выражение для расчета временной задержки детектирования алгоритма обнаружения сигнального временного интервала в процессе синхронизации станций СКРК при топологии «ДПУ – конечный пользователь» имеет вид (9)

$$Z_{nn} = \frac{T}{nT_n} \cdot (a_n - 1) + nw \cdot (T_n - 1), \qquad (9)$$

где nT_n – число временных кадров в периоде T; a_n – порядковый номер активации ОЛФД; T_n – порядковый номер периода.

Выводы и дискуссия

В статье поднимается вопрос синхронизации для сегмента магистральной сети квантовых коммуникаций. Обоснована важность процесса временной синхронизации, которая реализуется посредством высокоточного обнаружения оптического сигнала. Исследован алгоритм обнаружения оптического сигнала для метода синхронизации с повышенной защищенностью от несанкционированного доступа. Предложен усовершенствованный алгоритм анализа временной области распространения синхросигнала с использованием лавинных фотодетекторов. Показано, что предложенный алгоритм позволяет использовать лавинные фотодетекторы в режиме одиночного счета фотонов. Проведен анализ временных характеристик разработанного алгоритма синхронизации и представлено аналитическое выражение для расчета временной задержки детектирования, которое обеспечивает последовательный анализ временных окон с учетом перестраиваемого времени восстановления фотодетектора. Аналитическое выражение может использоваться для инженерных расчетов при проектировании системы КРК. Предложенный алгоритм значительно снижает вероятность несанкционированного доступа к процессу синхронизации и позволяет с заданной точностью определить временные параметры сигнального окна, что является критически важным для последующей работы системы квантового распределения ключей.

Исследование выполнено за счет гранта Российского научного фонда № 25-29-00007, https://rscf.ru/project/25-29-00007/

Литература

1. Subramani S., Svn S. K. Review of security methods based on classical cryptography and quantum cryptography // Cybernetics and Systems. – 2025. – Т. 56. – №. 3. – P. 302–320. DOI: https://doi.org/10.1080/01969722.2023.2166261.
2. Portmann C., Renner R. Security in quantum cryptography //Reviews of Modern Physics. – 2022. – Т. 94. – №. 2. – С. 025008. DOI: https://doi.org/10.1103/RevModPhys.94.025008.
3. Grasselli F. Quantum cryptography // Quantum science and technology. Cham: Springer. – 2021. DOI: 10.1007/978-3-030-64360-7.
4. Kumari A. B. et al. One time pad encryption technique in cryptography //International Journal of Computational Learning & Intelligence. – 2023. – Т. 2. – №. 1. – P. 1–7.
5. Al-Smadi A. M. et al. Files cryptography based on one-time pad algorithm // International Journal of Electrical and Computer Engineering (IJECE). – 2021. – Т. 11. DOI: 10.11591/ijece.v11i3.pp2335-2342.
6. Паршуткин А. В. Повышение защищенности информации от утечки через побочные электромагнитные излучения / А. В. Паршуткин, М. Р. Неаскина // Вопросы кибербезопасности. – 2022. – № 3(49). – С. 82–89. DOI 10.21681/2311-3456-2022-3-82-89.
7. Chen Y. A. An integrated space-to-ground quantum communication network over 4,600 kilometres // Nature. – 2021. – Vol. 589, No. 7841. – P. 214–219. DOI: https://doi.org/10.1038/s41586-020-03093-8.
8. Деев А. Д. Квантовые коммуникации через атмосферные (космические) каналы связи / А. Д. Деев, А. А. Калинкин, С. П. Кулик // Интернет изнутри. – 2024. – № 20. – С. 43–47.

9. Зякин Е. В. Перспективные протоколы КРК для оптической связи в свободном пространстве / Е. В. Зякин, А. В. Молоканов, К. М. Чуриков // Новые технологии. Наука, техника, педагогика. – 2024. – С. 141–148.
10. Петренко, А. С. Метод построения постквантовых алгоритмов ЭЦП с двумя скрытыми группами / А. С. Петренко // Вопросы кибербезопасности. – 2025. – № 2(66). – С. 52–63. DOI 10.21681/2311-3456-2025-2-52-63.
11. Nadlinger D. P. et al. Experimental quantum key distribution certified by Bell's theorem //Nature. – 2022. – Т. 607. – №. 7920. – С. 682–686. DOI: https://doi.org/10.1038/s41586-022-04941-5.
12. Lin D. High performance frame synchronization for continuous variable quantum key distribution systems // Optics Express. – 2015. – Vol. 23, No. 17. – P. 22190–22198. DOI: https://doi.org/10.1364/OE.23.022190.
13. Calderaro L. et al. Fast and simple qubit-based synchronization for quantum key distribution //Physical Review Applied. – 2020. – Т. 13. – №. 5. – С. 054041. DOI: https://doi.org/10.1103/PhysRevApplied.13.054041.
14. Williams J. et al. Implementation of quantum key distribution and quantum clock synchronization via time bin encoding //Quantum Computing, Communication, and Simulation. – SPIE, 2021. – Т. 11699. – P. 16–25. DOI: https://doi.org/10.1117/12.2581862.
15. Cochran R. D., Gauthier D. J. Qubit-based clock synchronization for QKD systems using a Bayesian approach // Entropy. – 2021. – Т. 23. – №. 8. – P. 988. DOI: https://doi.org/10.3390/e23080988.
16. Nonclassical attack on a quantum keydistribution system / A. Pljonkin, D. Petrov, L. Sabantina, K. Dakhkilgova // Entropy. – 2021. – Vol. 23, No. 5.
17. Сабанов А. Г. Идентификация и аутентификация в цифровом мире / А. Г. Сабанов, А. А. Шелупанов. – М.: Горячая Линия – Телеком. – 2022.
18. Civelli S. et al. Optical identification for user authentication in quantum key distribution systems //IET Conference Proceedings CP839. – Stevenage, UK : The Institution of Engineering and Technology, 2023. – Т. 2023. – №. 34. – P. 815–818. DOI: https://doi.org/10.1049/icp.2023.2346.
19. Krawec W. O. Security of a High Dimensional Two–Way Quantum Key Distribution Protocol //Advanced Quantum Technologies. – 2022. – Т. 5. – №. 10. – С. 2200024. DOI: https://doi.org/10.1002/qute.202200024.
20. Zheng X., Zhao Z. Quantum key distribution with two-way authentication // Optical and Quantum Electronics. – 2021. – Т. 53. – №. 6. – P. 304. DOI: https://doi.org/10.1007/s11082-021-02845-8.
21. Патент 2667755 РФ, МПК H04L9/08. Система релятивистской квантовой криптографии / Кравцов К.С. и др. (РФ). – № 2017117184; заявл. 05.17.2017; опубл. 24.09.2024.
22. Lavie E., Lim C. C. W. Improved coherent one-way quantum key distribution for high-loss channels // Physical Review Applied. – 2022. – Т. 18. – №. 6. – С. 064053. DOI: https://doi.org/10.1103/PhysRevApplied.18.064053.
23. Pljonkin A. et al. The Study of Synchronization in Quantum Key Distribution System //Futuristic Trends in Network and Communication Technologies: Third International Conference. – Springer Singapore, 2021. – P. 68–80. DOI: https://doi.org/10.1007/978-981-16-1483-5_7.
24. Румянцев К. Е. Вероятностные характеристики алгоритма обнаружения синхросигналов на основе выбора смежной пары сегментов с максимальным суммарным отсчётом / К. Е. Румянцев, П. Д. Миронова // Известия ЮФУ. Технические науки. – 2023. – № 3 (233). – С. 96–107.
25. Миронова П. Д. Алгоритм обнаружения синхросигналов на основе выбора смежной пары сегментов с максимальным суммарным отсчётом // Фундаментальные и прикладные аспекты компьютерных технологий и информационной безопасности: Сборник статей Всерос. науч.-техн. конф. – Таганрог: ЮФУ, 2023. – P. 52–53.
26. Signorelli F. et al. InGaAs/InP SPAD detecting single photons at 1550 nm with up to 50 % efficiency and low noise // 2021 IEEE International Electron Devices Meeting (IEDM). – IEEE, 2021. – P. 20.3. 1–20.3. 4. DOI: 10.1109/IEDM19574.2021.9720559.

ALGORITHM FOR DETECTING SYNCHRONIZATION SIGNAL IN QUANTUM NETWORKS

Pljenkin A. P.[3]

Keywords: *security, synchronization, quantum distribution, single-photon, optical pulse.*

Purpose of the study: *development and research of an algorithm for detecting an optical signal for synchronizing stations of a quantum key distribution system with increased protection against unauthorized access.*

Methods of research: *probability distribution, statistical analysis, single-photon detection.*

Results: *the importance of the time synchronization process, which is implemented through high-precision detection of an optical signal, is substantiated. An optical signal detection algorithm for a synchronization method with increased protection against unauthorized access is investigated. An improved algorithm for analyzing the time domain of synchronization signal propagation using avalanche photodetectors is proposed. It is shown that the proposed algorithm allows using avalanche photodetectors in the single photon counting mode. An analysis of the time characteristics of the developed synchronization algorithm is carried out and an analytical expression for calculating the time delay of detection is presented, which provides a sequential analysis of time windows taking into account the tunable recovery time of the photodetector. The analytical expression can be used for engineering calculations when designing a QKD system. The proposed algorithm significantly reduces the likelihood of unauthorized access to the synchronization process and allows determining the time parameters of the signal window with a given accuracy, which is critical for the subsequent operation of the quantum key distribution system.*

3 Anton P. Pljenkin, Ph.D. of Technical Sciences, Associate Professor, Southern Federal University. Taganrog, Russia. E-mail: pljonkin@sfedu.ru

Scientific novelty: *an algorithm for detecting an optical signal during synchronization is proposed, which is characterized by increased protection against unauthorized access. An analytical expression for engineering calculations of the delay of detection during synchronization is presented.*

References

1. Subramani S., Svn S. K. Review of security methods based on classical cryptography and quantum cryptography // Cybernetics and Systems. – 2025. – T. 56. – №. 3. – P. 302-320. DOI: https://doi.org/10.1080/01969722.2023.2166261.
2. Portmann C., Renner R. Security in quantum cryptography //Reviews of Modern Physics. – 2022. – T. 94. – №. 2. – C. 025008. DOI: https://doi.org/10.1103/RevModPhys.94.025008.
3. Grasselli F. Quantum cryptography // Quantum science and technology. Cham: Springer. – 2021. DOI: 10.1007/978-3-030-64360-7.
4. Kumari A. B. et al. One time pad encryption technique in cryptography //International Journal of Computational Learning & Intelligence. – 2023. – T. 2. – №. 1. – P. 1–7.
5. Al-Smadi A. M. et al. Files cryptography based on one-time pad algorithm //International Journal of Electrical and Computer Engineering (IJECE). – 2021. – T. 11. DOI: 10.11591/ijece.v11i3.pp2335-2342.
6. Parshutkin A., Neaskina M. Increasing the security of information from leakage through side electromagnetic emissions / Voprosy kiberbezopasnosti. – 2022. – № 3(49). – P. 82–89. DOI 10.21681/2311-3456-2022-3-82-89.
7. Chen Y. A. An integrated space-to-ground quantum communication network over 4,600 kilometres // Nature. – 2021. – Vol. 589, No. 7841. – P. 214–219. DOI: https://doi.org/10.1038/s41586-020-03093-8.
8. A. D. Deev, A. A. Kalinkin, S. P. Kulik. Kvantovye kommunikacii cherez atmosfernye (kosmicheskie) kanaly svyazi // Internet iznutri. – 2024. – № 20. – Pp. 43–47.
9. E. V. Zyakin, A. V. Molokanov, K. M. Churikov. Promising QKD protocols for optical communications in free space // New Technologies. Science, Engineering, Pedagogics: Proceedings of the All-Russian Scientific-Practical Conference, Moscow, 2024, pp. 141–148.
10. Petrenko A. S. Method for constructing post-quantum algorithms of eds with two hidden groups / Voprosy kiberbezopasnosti. – 2025. – № 2(66). – P. 52–63. DOI 10.21681/2311-3456-2025-2-52-63.
11. Nadlinger D. P. et al. Experimental quantum key distribution certified by Bell's theorem // Nature. – 2022. – T. 607. – №. 7920. – P. 682–686. DOI: https://doi.org/10.1038/s41586-022-04941-5.
12. Lin D. High performance frame synchronization for continuous variable quantum key distribution systems // Optics Express. – 2015. – Vol. 23, No. 17. – P. 22190–22198. DOI: https://doi.org/10.1364/OE.23.022190.
13. Calderaro L. et al. Fast and simple qubit-based synchronization for quantum key distribution //Physical Review Applied. – 2020. – T. 13. – №. 5. – P. 054041. DOI: https://doi.org/10.1103/PhysRevApplied.13.054041.
14. Williams J. et al. Implementation of quantum key distribution and quantum clock synchronization via time bin encoding //Quantum Computing, Communication, and Simulation. – SPIE, 2021. – T. 11699. – P. 16–25. DOI: https://doi.org/10.1117/12.2581862.
15. Cochran R. D., Gauthier D. J. Qubit-based clock synchronization for QKD systems using a Bayesian approach // Entropy. – 2021. – T. 23. – №. 8. – P. 988. DOI: https://doi.org/10.3390/e23080988.
16. Nonclassical attack on a quantum keydistribution system / A. Pljonkin, D. Petrov, L. Sabantina, K. Dakhkilgova // Entropy. – 2021. – Vol. 23, No. 5.
17. Sabanov A. G., Shelupanov A. A. Identification and authentication in the digital world. Moscow, Hot Line-Telecom, 2022.
18. Civelli S. et al. Optical identification for user authentication in quantum key distribution systems //IET Conference Proceedings CP839. – Stevenage, UK : The Institution of Engineering and Technology, 2023. – T. 2023. – №. 34. – P. 815–818. DOI: https://doi.org/10.1049/icp.2023.2346.
19. Krawec W. O. Security of a High Dimensional Two–Way Quantum Key Distribution Protocol //Advanced Quantum Technologies. – 2022. – T. 5. – №. 10. – C. 2200024. DOI: https://doi.org/10.1002/qute.202200024.
20. Zheng X., Zhao Z. Quantum key distribution with two-way authentication // Optical and Quantum Electronics. – 2021. – T. 53. – №. 6. – P. 304. DOI: https://doi.org/10.1007/s11082-021-02845-8.
21. Pat. 2667755 RF, MPK H04L9/08. Sistema relyativistskoj kvantovoj kriptografii / Kravcov K. S. i dr. (RF). – № 2017117184; zayavl. 05.17.2017; opubl. 24.09.2024.
22. Lavie E., Lim C. C. W. Improved coherent one-way quantum key distribution for high-loss channels // Physical Review Applied. – 2022. – T. 18. – №. 6. – C. 064053. DOI: https://doi.org/10.1103/PhysRevApplied.18.064053.
23. Pljonkin A. et al. The Study of Synchronization in Quantum Key Distribution System //Futuristic Trends in Network and Communication Technologies: Third International Conference. – Springer Singapore, 2021. – 3. 68–80. DOI: https://doi.org/10.1007/978-981-16-1483-5_7.
24. Rumyancev K. E. Veroyatnostnye xarakteristiki algoritma obnaruzheniya sinxrosignalov na osnove vybora smezhnoj pary segmentov s maksimal'nym summarnym otschyotom / K. E. Rumyancev, P. D. Mironova // Izvestiya YuFU. Texnicheskie nauki. – 2023. – № 3 (233). – P. 96–107.
25. Mironova P. D. Algoritm obnaruzheniya sinxrosignalov na osnove vybora smezhnoj pary segmentov s maksimal'nym summarnym otschyotom // Fundamental'nye i prikladnye aspekty komp'yuternyx texnologij i informacionnoj bezopasnosti: Sbornik statej Vseros. nauch.-texn. konf. – Taganrog: YuFU, 2023. – P. 52–53.
26. Signorelli F. et al. InGaAs/InP SPAD detecting single photons at 1550 nm with up to 50 % efficiency and low noise // 2021 IEEE International Electron Devices Meeting (IEDM). – IEEE, 2021. – P. 20.3. 1–20.3. 4. DOI: 10.1109/IEDM19574.2021.9720559.