09

Система синхронизации для устройств квантового распределения ключей

© Н.В. Рудавин,[1,3] В.Ю. Ящук,[1] А.А. Феимов,[1,2] Р.В. Ожегов,[2,3] Р.А. Шаховой[1,2]

[1]QRate,
143026 Сколково, Россия
[2]Центр компетенций НТИ „Квантовые коммуникации“, Национальный исследовательский технологический университет МИСИС,
119049 Москва, Россия
[3]Национальный исследовательский университет „Высшая школа экономики“,
101000 Москва, Россия
e-mail: n.rudavin@goqrate.com

Поступило в Редакцию 17 марта 2025 г.
В окончательной редакции 30 апреля 2025 г.
Принято к публикации 1 мая 2025 г.

В коммерческих устройствах квантового распределения ключей (КРК) высокая точность синхронизации между генераторами опорных частот передатчика и приемника играет ключевую роль для обеспечения их функционирования. Предложена реализация системы коррекции разницы частот генераторов для устройства КРК. Подробно описаны оптическая схема системы синхронизации, двухступенчатый метод коррекции частот и помехоустойчивый метод автоматического определения момента старта приема и передачи квантовых состояний на приемнике и передатчике. Для подтверждения работоспособности предложенных технических решений был проведен ряд экспериментов с использованием реального устройства КРК, реализующего протокол BB84. В результате было продемонстрировано, что все компоненты предложенной системы коррекции разницы частот работают стабильно. Точность стабилизации гарантирует надежное распределение секретных ключей между удаленными узлами.

Ключевые слова: стабильность генератора опорной частоты, синтезатор частот, временное и спектральное мультиплексирование, метастабильность, фазовая ошибка, М-последовательность, синхронизация, квантовое распределение ключей.

DOI: 10.61011/JTF.2026.02.62295.39-25

Введение

Квантовое распределение ключей (КРК) представляет собой перспективную технологию, обеспечивающую возможность безопасного обмена криптографическими ключами [1,2]. В большинстве предложенных протоколов КРК две удаленные стороны — передатчик (Алиса) и приемник (Боб) — генерируют общий секретный ключ, обмениваясь квантовыми состояниями через оптический канал. При этом безопасность ключа гарантируется принципами квантовой механики. В частности, благодаря вероятностной природе квантовых измерений попытка перехвата передаваемых квантовых состояний третьей стороной (Евой) внесет в них шумы, которые смогут обнаружить Алиса и Боб [3,4]. Полученный секретный ключ может быть затем использован в классических схемах шифрования [5].

Современные устройства КРК демонстрируют скорость и дальность генерации секретных ключей, достаточные для их практического применения [6–8]. Однако технические трудности, связанные с их реализацией, заметно ограничивают возможности широкого внедрения данных устройств в существующие телекоммуникационные сети. Одной из подобных трудностей является задача обеспечения стабильной синхронизации рабочих частот узлов, участвующих в процессе распределения ключей [9–11]. Синхронизация рабочих частот необходима, поскольку для приготовления и регистрации квантовых состояний приемник и передатчик, как правило, используют независимые генераторы опорной частоты (ГОЧ), необходимые для формирования базовой частоты синтезатора частот. На основе базовой частоты синтезаторы генерируют набор выходных сигналов, представляющих собой рабочие частоты устройства. Различие базовых частот, очевидно, приведет к невозможности генерации секретных ключей [12]. Современный уровень развития технологии производства ГОЧ не позволяет получать генераторы с идентичными выходными частотами. Кроме того, генераторы подвержены температурным и механическим воздействиям, а также постепенному старению. В результате даже лучшие из доступных ГОЧ не обладают достаточной стабильностью для их использования без периодической компенсации разности частот [13–15].

По причине отсутствия универсального решения, большинство существующих на рынке высокочастотных устройств КРК реализуют собственные уникальные системы синхронизации, удовлетворяющие требованиям

конкретного устройства. Чаще всего в них используются оптические сигналы для передачи информации о текущей частоте ведущего узла, при этом в качестве ведущего обычно выбирается ГОЧ Алисы [16–18]. Далее Боб использует полученную информацию для расчета разницы частот и подстройки своего ГОЧ. В качестве оптического канала для передачи сигналов синхронизации может использоваться дополнительное оптическое волокно, атмосферный канал или то же оптическое волокно, что и для передачи квантовых состояний (квантовый канал). В последнем случае для изоляции квантовых состояний от мощного излучения синхронизации могут быть использованы методы временного (TDM) или спектрального (WDM) мультиплексирования [19–21].

Распространенным подходом является использование последовательности мощных оптических импульсов в качестве синхронизирующего сигнала (синхронизирующей последовательности) [17,22,23]. Путем анализа данной последовательности Боб может извлечь из нее информацию о частоте передатчика и использовать ее для определения разности частот. Для корректной регистрации квантовых состояний необходимо не только компенсировать разность рабочих частот приемника и передатчика, но и синхронизировать их фазы. Соответственно в качестве частоты повторения импульсов в синхронизирующей последовательности может использоваться либо частота приготовления квантовых состояний, либо частоты, полученные умножением или делением данной частоты на целочисленные коэффициенты, поскольку такие частоты сохраняют жесткую фазовую связь с исходной.

Другим подходом является использование корреляции между отправленными и принятыми последовательностями информационных квантовых состояний для вычисления текущей разницы частот генераторов Алисы и Боба [11,24,25]. Например, в [25] передатчик периодически отправлял заранее известную приемнику синхронизирующую последовательность кубитов. Далее путем вычисления автокорреляционной функции (АКФ) между своей копией и принятой синхронизирующей последовательностью приемник определял временную задержку между отправленными и принятыми квантовыми состояниями. При этом данная последовательность не используется при формировании секретного ключа, благодаря чему безопасность устройства не нарушается. Помимо специальных последовательностей кубитов, в подобных системах может использоваться публичная информация, раскрываемая Алисой и Бобом на этапе просеивания сырого ключа, например базисы и типы кубитов [11].

В настоящей работе предложена система синхронизации для устройств КРК, реализующих протоколы с дискретными переменными. Данная система синхронизации может быть представлена в виде аппартно-программного комплекса, состоящего из трех основных компонентов:

1) оптической схемы синхронизации;

2) набора методов коррекции разности рабочих частот приемника и передатчика;

3) метода выравнивания моментов старта приема и передачи оптических импульсов на каждом узле.

Предложенные в настоящей работе реализации компонентов 2 и 3 не обсуждались в литературе достаточно подробно в контексте использования в системах синхронизации для устройств КРК. В настоящей работе разработанная система синхронизации рассмотрена на примере реализации для коммерческого устройства КРК на основе протокола BB84 [16]. В разд. 1 проводится краткий анализ исследуемого устройства КРК с целью определения требований к системе синхронизации. Также в разд. 1 содержится описание использованной нами оптической схемы синхронизации. В разд. 2 представлен анализ параметров, используемых в устройстве ГОЧ, а также сравнительный анализ методов перестройки рабочих частот устройства. Далее представлен двухступенчатый алгоритм компенсации разницы рабочих частот, основанный на синхронизации базовых частот синтезаторов приемника и передатчика. В разд. 2.1 подробно описан метод быстрой компенсации разницы частот в устройствах КРК при помощи цифровых асинхронных буферов переменной длины. В разд. 2.2, детально рассмотрен предложенный нами метод использования явления метастабильности цифровых триггеров и джиттера анализируемых сигналов для поддержания постоянной разницы фаз между рабочими частотами Алисы и Боба. В разд. 3 для реализации возможности помехоустойчивого выравнивания моментов старта приема и передачи оптических импульсов на приемнике и передатчике был предложен и протестирован метод на основе вычисления автокорреляционной функции М-последовательности. Комплексное исследование параметров реализованной системы синхронизации, включая точность и стабильность, было проведено на различных длинах квантового канала в составе устройства КРК, реализующего протокол BB84. Все полученные результаты тестирования приведены в разд. 4.

1. Оптическая схема синхронизации

Как было сказано ранее, конкретная реализация системы синхронизации выбирается в соответствии с параметрами устройства КРК, для которой она разрабатывается. При этом необходимо учитывать реализуемый протокол КРК, используемые в устройстве аппаратные и программные компоненты, а также оптическую схему устройства. На рис. 1, *a* приведена оптическая схема исследуемого устройства КРК, реализующего протокол BB84 с поляризационным кодированием [22].

Управление аппаратными компонентами устройства осуществляется платой на основе ПЛИС Xilinx Virtex-7. Частота формирования информационных оптических импульсов $f_{prep} = 312.5\,\mathrm{MHz}$. Эта и другие используемые в устройстве частоты формируются при помощи

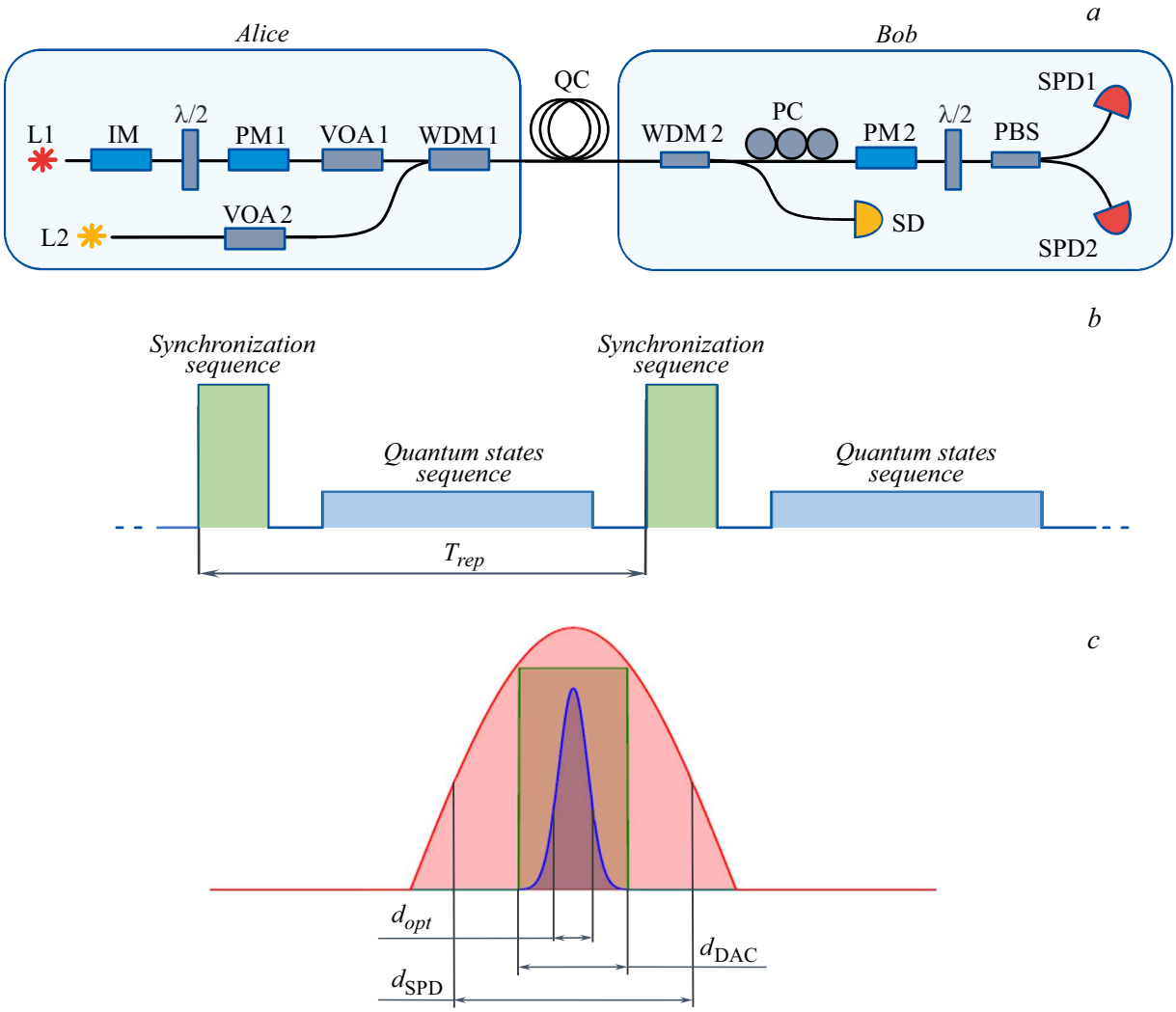

Рис. 1. *a* — оптическая схема приемника и передатчика устройства КРК с поляризационным кодированием. L1 — сигнальный лазер, IM — модулятор интенсивности, $\lambda/2$ — полуволновая пластинка, PM1 и PM2 — фазовые модуляторы, VOA1 и VOA2 — перестраиваемые оптические аттенюаторы, PC — поляризационный контроллер, PBS — поляризационный светоделитель, SPD1 и SPD2 — стробируемые детекторы одиночных фотонов, QC — квантовый канал (выделенное („темное“) одномодовое оптоволокно), L2 — синхронизирующий лазер, WDM1 и WDM2 — оптические фильтры, SD — синхронизирующий детектор. *b* — схема использования метода TDM для отправки синхронизирующей последовательности с периодом повторений T_{rep}. *c* — схема временного перекрытия импульса фазового модулятора, строба SPD и информационного лазерного импульса. d_{SPD} — ширина строба SPD, d_{opt} — ширина оптического импульса, d_{DAC} — ширина модулирующего импульса.

синтезатора частот Silicon Labs Si5340, в качестве источника опорного сигнала для которого применяется высокостабильный термостатированный ГОЧ, управляемый напряжением, с эталонной частотой 10 MHz.

В предложенной системе синхронизации для передачи информации о текущей частоте своего ГОЧ передатчик с периодом T_{rep} генерирует синхронизирующую последовательность. В качестве оптического канала для передачи данной последовательности используется квантовый канал. Однако передача мощных сигналов синхронизации по волокну сопровождается повышением уровня засветки SPD-приемника, связанным с комбинационным и рэлеевским рассеяниями в оптоволокне, а также отражениями на дефектах сварки и соединений. Для минимизации вклада засветки используется метод TDM, при котором мощная синхронизирующая последовательность и последовательность квантовых состояний посылаются в различные моменты времени, исключая влияние классического излучения на SPD. Схема использования метода TDM для отправки синхронизирующей последовательности с периодом повторений T_{rep} приведена на рис. 1, *b*. Недостатком данного подхода является снижение скорости генерации секретного ключа из-за появления временных окон синхронизации. Для обеспечения изоляции SPD от излучения синхронизирующей последовательности, шумовой засветки и многократных отражений в волокне в нашей системе синхронизации также используется метод WDM.

Оптическая схема устройства, приведенная на рис. 1, *a*, включает в себя оптическую схему приготовления и измерения квантовых состояний и оптическую схему синхронизации [22]. Последняя состоит из импульсного лазера L2, фотодетектора SD, перестраиваемого оптического аттенюатора VOA2 и фильтров WDM1 и WDM2. Лазер L2, управление которым осуществляется с помощью дополнительного трансивера на плате ПЛИС, используется для формирования синхронизирующей последовательности на передатчике. В свою очередь фотодетектор SD, установленный на стороне приемника, выполняет преобразование принятой синхронизирующей последовательности в электрический сигнал для дальнейшей обработки.

Для реализации метода WDM в приемник и передатчик установлены DWDM фильтры (WDM1 и WDM2), полоса пропускания которых соответствует длине волны информационного лазера — 1548.5 nm (36 DWDM канал). Длина волны лазера L2 была выбрана равной 1554.25 nm (28 DWDM канал).

При смене квантового канала могут измениться и оптические потери в нем, что приведет к необходимости корректировки параметров системы синхронизации, в частности, синхронизирующего лазера и синхронизирующего детектора. Выбор оптимальных параметров напрямую определяет качество синхронизации. Для того чтобы систематизировать процесс переключения между линиями с различными потерями, в оптическую схему добавлен управляемый оптический аттенюатор VOA2, позволяющий поддерживать постоянный уровень потерь между синхронизирующим лазером и синхронизирующим детектором независимо от потерь в оптоволоконной линии.

Так как отправка синхронизирующих последовательностей осуществляется с периодом T_{rep}, процедура подстройки частоты также должна выполняться через равные промежутки времени T_{corr}, причем расхождение фаз генераторов приемника и передатчика за время T_{corr} не должно превышать предельного значения $\Delta\varphi^{\max}$, при котором процесс корректного функционирования устройства КРК нарушается. В свою очередь, период между ближайшими подстройками T_{corr} ограничен снизу периодом отправки синхронизирующих последовательностей ($T_{rep} \le T_{corr}$) и определяется качеством используемых в устройстве КРК генераторов опорных частот, однако даже для наилучших доступных моделей допустимая величина T_{corr} не превосходит секунд.

В дальнейшем для удобства проведения анализа временных параметров устройства, а также расчетов с их участием, вместо величины $\Delta\varphi^{\max}$ будем использовать соответствующий ей временной сдвиг между тактами опорных частот приемника и передатчика $\Delta t^{\max}$, определяемый как:

$$\Delta t^{\max} = \frac{\Delta\varphi^{\max}}{2\pi f_{gen}},$$

где f_{gen} — номинальное значение частоты генератора. Для нахождения $\Delta t^{\max}$ рассмотрим подробнее процесс регистрации оптических импульсов приемником с учетом временных параметров устройства. Перед запуском процесса генерации секретных ключей проводится процедура первичной калибровки устройства. В частности, для корректной регистрации оптических импульсов необходимо настроить задержки стробов SPD1 и SPD2. Также необходимо выровнять задержку включения модулятора PM2 в соответствии с временем прихода оптического импульса. Отсутствие или частичная модуляция оптического импульса приведут к невозможности корректной регистрации квантовых состояний из-за роста квантовой ошибки (QBER). На рис. 1, *c* приведена схема наложения оптического импульса на управляющие импульсы приемника, получаемая в результате успешной калибровки задержек. В исследуемом устройстве КРК ширина оптического импульса $d_{\text{opt}} \approx 150$ ps, ширина строба SPD составляет $d_{\text{SPD}} \approx 800$ ps, ширина используемого модулирующего импульса составляет $d_{\text{DAC}} \approx 400$ ps. Как видно из рис. 1, *c*, расхождения тактов ГОЧ приемника и передатчика более чем на 100 ps достаточно, чтобы оптический импульс начал выходить за пределы модулирующего импульса PM2. Соответственно максимально допустимый временной сдвиг между тактами опорных частот приемника и передатчика за период подстройки должен удовлетворять условию $\Delta t^{\max} \le 100$ ps. При разработке нашей системы синхронизации в качестве целевого параметра использовалось значение $\Delta t^{\max} = 100$ ps.

2. Методы коррекции разницы частот приемника и передатчика

Как было упомянуто в разд. 1, предложенные нами методы синхронизации осуществляют коррекцию частоты приемника в соответствии с частотой передатчика с заданным периодом T_{corr}. Для определения максимально допустимого значение данной величины — $T_{corr}^{\max}$ — рассмотрим величину полного возможного отклонения частоты одного ГОЧ от эталонной (номинальной) Δf_{gen}, определяемую как совокупность аддитивных составляющих:

$$\Delta f_{gen} = \Delta f_{def} + \Delta f_{res} + \Delta f_{temp} + \Delta f_{vcc},$$

где Δf_{def} — начальная точность частоты генератора; Δf_{res} — отклонение частоты (стабильность) генератора при включении питания; Δf_{temp} — отклонение частоты (стабильность) генератора, связанное с колебаниями температуры; Δf_{vcc} — отклонение частоты (стабильность) генератора, обусловленное флуктуациями управляющего напряжения.

Типичные (средние) значения перечисленных отклонений, выраженные в ppm (миллионная доля эталонной частоты f_{gen}), приведены в технической документации используемого в устройстве ГОЧ:

- начальная точность $P_{def} = \pm 0.1$ ppm;

• стабильность частоты при включении питания $P_{res} = \pm 10 \cdot 10^{-3}$ ppm;

• стабильность частоты от температуры: $P_{temp} = \pm 0.1 \cdot 10^{-3}$ ppm;

• стабильность частоты от управляющего напряжения: $P_{\text{vcc}} = \pm 0.2 \cdot 10^{-3}$ ppm.

Заметим, что приведенные величины справедливы также для всех производных частот, сформированных из исходной частоты генератора. Напомним, что отклонение Δf от номинального значения частоты генератора f_{gen} (с периодом T_{gen}) и соответствующее ему отклонение ΔT от номинального значения периода T_{gen} определяются как:

$$\Delta f = \frac{f_{gen} \cdot P}{10^6} \tag{1}$$

и

$$\Delta T = \frac{T_{gen} \cdot P}{10^6}, \tag{2}$$

где вместо Δf и P следует подставить одно из перечисленных выше значений.

Поскольку начальное отклонение частоты генератора от номинальной P_{def}, а также отклонение частоты при включении питания P_{res} необходимо компенсировать только один раз при запуске устройства КРК, стабильность частоты генератора во время работы устройства P_{work} определяется только стабильностью температуры и напряжения питания, так что можно записать рабочее отклонение частоты в виде:

$$P_{work} = P_{temp} + P_{vcc} = \pm 0.3 \cdot 10^{-3} \text{ ppm}.$$

Из выражений (1) и (2) следует, что в наихудшем случае полная абсолютная разница частот (или периодов) опорных сигналов двух ГОЧ во время работы устройства (с частотами f_1 и f_2 соответственно), определяется как:

$$\begin{aligned} |f_2 - f_1| =& |(f_{gen} + \Delta f_{work} + \Delta f_{\text{const}}) - (f_{gen} - \Delta f_{work})| \\ =& \frac{2 f_{gen} \cdot |P_{work}|}{10^6} + \Delta f_{\text{const}}, \end{aligned} \tag{3}$$

где Δf_{work} — типичное отклонение номинальной частоты из-за нестабильности ГОЧ в процессе работы устройства, Δf_{const} — текущая преднамеренная разность частот. Поскольку в процессе штатной работы устройства КРК величина $\Delta f_{\text{const}} = 0$, выражение (3) сводится к:

$$\begin{aligned} |f_2 - f_1| =& |(f_{gen} + \Delta f_{work}) - (f_{gen} - \Delta f_{work})| \\ =& \frac{2 f_{gen} \cdot |P_{work}|}{10^6}. \end{aligned} \tag{4}$$

Следствием отклонения частот ГОЧ на Δf_{work} в течение времени t является накопление разницы количества сгенерированных тактов:

$$\begin{aligned} |N_2 - N_1| =& |f_2 \cdot t - f_1 \cdot t| = 2|\Delta f_{work}| \cdot t \\ =& \frac{2 f_{gen} \cdot |P_{work}| \cdot t}{10^6}, \end{aligned}$$

где N_1 и N_2 — количество тактов за время t на частотах f_1 и f_2 соответственно. Временной сдвиг, соответствующий величине $|N_1 - N_2|$, определяется как:

$$\begin{aligned} \Delta t =& |N_2 - N_1| \cdot T_{gen} = \frac{2 f_{gen} \cdot |P_{work}| \cdot t \cdot T_{gen}}{10^6} \\ =& \frac{2t \cdot |P_{work}|}{10^6}. \end{aligned} \tag{5}$$

Переписав выражение (5) и подставив в него значение $\Delta t^{\max}$, получим величину максимального периода подстройки частот генераторов $T_{corr}^{\max}$:

$$T_{corr}^{\max} = \frac{\Delta t^{\max} \cdot 10^6}{2 \cdot |P_{work}|} = \frac{100 \cdot 10^{-12} \cdot 10^6}{\pm 0.6 \cdot 10^{-3}} \approx 0.167 \text{ c}.$$

Исходя из полученного значения $T_{corr}^{\max}$, были выбраны значения периода повторений синхронизирующей последовательности $T_{rep} = 3.2$ ms и периода подстройки частоты $T_{corr} = 50$ ms. Тогда в соответствии с выражением (5) получим значение максимального временного сдвига между тактами опорных частот приемника и передатчика $\Delta t_{gen}^{\max}$ с типичной нестабильностью ГОЧ P_{work} за время T_{corr} между ближайшими подстройками:

$$\begin{aligned} \Delta t_{gen}^{\max} =& \frac{2 \cdot T_{corr} \cdot |P_{work}|}{10^6} \\ =& \frac{2 \cdot 50 \cdot 10^{-3} \cdot 0.3 \cdot 10^{-3}}{10^6} = 30 \text{ ps}. \end{aligned} \tag{6}$$

Для определения требуемой точности работы алгоритма синхронизации необходимо учесть, что сигналы в реальных цифровых схемах отличаются от идеальных наличием джиттера — нежелательных фазовых или частотных отклонений, вносящих дополнительную погрешность в сопоставление временных окон на приемнике и передатчике. Величина джиттера определяется параметрами используемых аппаратных компонентов устройства и не зависит от качества синхронизации частот приемника и передатчика. Следовательно, максимально допустимый временной сдвиг между тактами генераторов $\Delta t^{\max}$ за период подстройки определяется как:

$$\Delta t^{\max} = \Delta t_{sync}^{\max} + \Delta t_{jitter}^{\max} + \Delta t_{gen}^{\max},$$

где $\Delta t_{sync}^{\max}$ — максимальный временной сдвиг между тактами ГОЧ, обусловленный точностью алгоритма синхронизации, а $\Delta t_{jitter}^{\max}$ — максимальная величина суммарного джиттера рабочих сигналов приемника и передатчика. Из выражений (6) и (7) следует, что максимальная ошибка выравнивания фаз на каждой итерации алгоритма синхронизации с учетом величины джиттера $\Delta t_{sync+jitter}^{\max} = \Delta t_{sync}^{\max} + \Delta t_{jitter}^{\max}$ составляет 70 ps ($\Delta t_{sync+jitter}^{\max} = 100 - 30 = 70$ ps).

Поскольку необходимость компенсировать разницу частот генераторов, обусловленную отклонениями Δf_{def} и Δf_{res}, возникает только при запуске устройства КРК, процедура компенсации разницы частот была

разделена на два этапа. На первом этапе (стартовой коррекции), выполняемом один раз, осуществляется компенсация Δf_{def} и Δf_{res}. Второй этап (периодическая коррекция) выполняется через каждый период подстройки T_{corr} и направлен на компенсацию P_{work} с точностью, удовлетворяющей установленному максимальному значению $\Delta t^{\max}_{sync+jitter}$.

Подстройка частот на обоих этапах производится путем перестройки базовой частоты f_{ref} синтезатора приемника. Поскольку настройки синтезаторов приемника и передатчика идентичны, синхронизация базовых частот позволит гарантировать синхронизацию синтезируемых частот. Для используемого в устройстве синтезатора Si5340 $f_{\text{ref}} = 200\,\text{MHz}$, перестройка на заданную частоту осуществляется в соответствии с документацией синтезатора Si5340 и не требует проведения дополнительных калибровок. Данный подход позволяет ограничить максимальное значение $\Delta f_{def} + \Delta f_{res}$ диапазоном перестройки базовой частоты f_{ref} синтезатора частот.

Отметим, что в случае прямого изменения частоты ГОЧ путем изменения его управляющего напряжения, необходимо проведение калибровки ЦАП генератора для его перестройки на заданную частоту. Помимо необходимости калибровки и наличия погрешности, вносимой ЦАП, большим недостатком использования ГОЧ для коррекции частот является крайне малый диапазон перестройки частоты ($\pm 3\,\text{Hz}$) относительно диапазона, доступного на синтезаторе Si5340 ($\pm 3\,$кHz). Данный недостаток является критичным, поскольку возможны ситуации, когда диапазоны частот ГОЧ приемника и передатчика не перекрываются. В этом случае работа устройства становится невозможной без проведения процедуры замены одного из ГОЧ, при этом диапазон частот нового ГОЧ должен быть подобран соответствующим образом.

2.1. Стартовая коррекция разницы частот

Рассмотрим последовательно оба этапа коррекции частот. На первом этапе расчет текущей разницы частот осуществляется путем измерения времени T_{360} между двумя соседними событиями расхождения фаз генераторов приемника $\varphi_1(t)$ и передатчика $\varphi_2(t)$ на 360°. Для этого передатчик в течение времени оценки τ осуществляет непрерывную отправку синхронизирующих импульсов на частоте $f_1^{initial}$, при этом формирование секретного ключа в течение первого этапа коррекции частот не производится (описание причин приведено в разд. 1). В свою очередь, приемник использует свою частоту $f_2^{initial}$ для измерения времени T_{360}. Разность фаз приемника и передатчика $\Delta\varphi(t)$ определяется как:

$$\Delta\varphi(t) = |\varphi_2(t) - \varphi_1(t)| = 2\pi|f_2^{initial} - f_1^{initial}|t.$$

Для $\Delta\varphi(T_{360}) = 2\pi$ из выражения (8) получим

$$T_{360} = \frac{1}{|f_2^{initial} - f_1^{initial}|}.$$

Поскольку моменту расхождения фаз на 360° соответствует появление лишнего такта на частоте опережающего ГОЧ, данные события могут быть легко зарегистрированы с использованием цифровой техники, в частности на ПЛИС, при этом время T_{360} будет выражаться в количестве тактов N_{360} частоты дискретизации f_m (с периодом T_m), на которой производится измерение:

$$T_{360} = N_{360} \cdot T_m.$$

Тогда текущая разница частот генераторов Δf_{curr} может быть выражена как:

$$\Delta f_{curr} = |f_2^{initial} - f_1^{initial}| = \frac{1}{N_{360} \cdot T_m} = \frac{f_m}{N_{360}}.$$

Заметим, что для корректного измерения величины T_{360} частота дискретизации f_m, согласно теореме Котельникова, должна удовлетворять условию $f_m > 2|f_2^{initial} - f_1^{initial}|$. В частном случае, когда в качестве частоты дискретизации f_m используется та же частота, что и для анализа расхождения фаз генераторов ($f_m = f_2^{initial}$), с учетом формулы (3), выражение (9) сводится к следующему:

$$N_{360} = \frac{1 + |P_{work}| \cdot 10^{-6} + \frac{\Delta f_{\text{const}}}{f^{initial}}}{2|P_{work}| \cdot 10^{-6} + \frac{\Delta f_{\text{const}}}{f^{initial}}},$$

где $f^{initial}$ — номинальная (эталонная) частота для частот $f_1^{initial}$ и $f_2^{initial}$. Поскольку величина P_{work}, а также значение отношения $\Delta f_{\text{const}}/f^{initial}$ являются константами для всех частот, полученных путем умножения или деления базовой частоты синтезатора f_{ref}, из выражения (10) следует, что в случае $f_m = f_2^{initial}$ величина N_{360} также является константой для данного набора частот. Соответственно, рассчитанное на частоте $f_2^{initial}$ ($f_{ref} \neq f^{initial}$) значение N_{360} может быть использовано для вычисления текущей разницы базовых частот синтезаторов приемника и передатчика путем подстановки соответствующих значений в выражение (9). Так, в нашей системе синхронизации используется $f^{initial} = f_{prep}/2 = 156.25\,\text{MHz}$. Использование данного свойства также может быть крайне целесообразным для уменьшения времени оценки τ в случае использования относительно низких значений f_{ref} ($\tau \geq T_{360}$).

В качестве реализации механизма измерения N_{360} на ПЛИС используется алгоритм анализа сигналов „empty“, генерируемых двумя буферами FIFO (First In First Out) с асинхронными доменами чтения и записи [26–28]. Буферы FIFO представляют собой аппаратно-программную реализацию структуры данных „очередь“ в ПЛИС. В общем случае, сигналы „empty“ формируются на частоте чтения из буфера, когда в буфере заканчиваются данные, доступные для чтения. При этом в реализации FIFO, используемой в наших устройствах КРК, установка данного флага происходит в начале такта, соответствующего чтению последнего доступного слова в FIFO. После записи хотя бы одного слова

в FIFO флаг „empty“ снимается, указывая на то, что данные доступны для чтения, при этом чтение возобновляется с задержкой, равной одному такту частоты чтения. В предложенном нами алгоритме входы FIFO сконфигурированы следующим образом:

• FIFO 1: чтение осуществляется на частоте приемника, запись — на частоте передатчика;

• FIFO 2: чтение осуществляется на частоте передатчика, запись — на частоте приемника.

В случае, когда частоты чтения и записи ($f_1^{initial}$ и $f_2^{initial}$) идеально совпадают, количество данных в буферах будет постоянным, так как каждому такту чтения данных будет соответствовать один такт записи, при этом сигналы „empty“ не будут формироваться ни в одном из буферов. В противном случае, в одном из используемых FIFO частота чтения будет опережать частоту записи, при этом появлению каждого лишнего такта на частоте чтения будет соответствовать уменьшение количества данных в буфере. Вне зависимости от количества слов в данном буфере в начальный момент времени, когда количество слов в буфере достигнет одного, начнут формироваться сигналы „empty“. При этом, за счет блокировки чтения из FIFO период появления сигналов „empty“, измеренный на внутренней частоте приемника $f_2^{initial}$, будет соответствовать текущему значению T_{360}. По тому, на какой частоте происходит чтение из буфера, формирующего сигналы „empty“, однозначно определяется, какая частота является опережающей и соответственно знак перестройки частоты приемника.

Заметим, что момент начала измерения N_{360} случайным образом соотносится с текущими фазами ГОЧ, следовательно, для однозначного определения N_{360} необходимо зафиксировать как минимум два события расхождения фаз ГОЧ на 360° за время оценки τ. С точки зрения ПЛИС данное условие удовлетворяется путем выбора максимального из полученных оценок N_{360}, а также измерением количества событий „empty“ за время τ: в случае, если количество событий „empty“ меньше 2, процедура проводится заново с увеличенным временем оценки τ.

Поскольку минимальное время, необходимое для корректной оценки T_{360}, соответствует периоду текущей разницы частот ΔT_{curr}, проведение первого этапа коррекции для текущих частот ГОЧ может потребовать больших временных затрат, при этом в предельном случае τ стремится к бесконечности. Для уменьшения времени оценки τ в предложенной системе стартовой коррекции частот мы используем метод искусственного увеличение Δf_{curr} до значений, значительно превышающих Δf_{work}, путем создания преднамеренной разности частот Δf_{const} (выражение (3)).

2.2. Периодическая коррекция разницы частот

Как было сказано ранее, алгоритм подстройки разности частот в процессе работы устройства основан на периодической подстройке базовой частоты f_{ref} синтезатора приемника в соответствии с дрейфом частоты ГОЧ передатчика. Распространенным подходом к решению данной задачи является использование системы фазовой автоподстройки частоты (ФАПЧ), работающей в периодическом режиме [29–31]. В общем случае ФАПЧ представляет собой систему автоматического управления, использующую цепь отрицательной обратной связи для синхронизации фазы и частоты ведущего и ведомого генераторов. Основным элементом данной системы является фазовый детектор, выполняющий сравнение фаз генераторов и формирование сигнала ошибки, пропорционального текущей разности фаз. В классических системах ФАПЧ полученный сигнал ошибки через фильтр низких частот подается на управляющий вход генератора, управляемого напряжением (ГУН), тем самым корректируя его частоту и поддерживая постоянную разность фаз. При этом качество автоподстройки определяется многими параметрами, в частности точностью работы фазового детектора и точностью управления генератором.

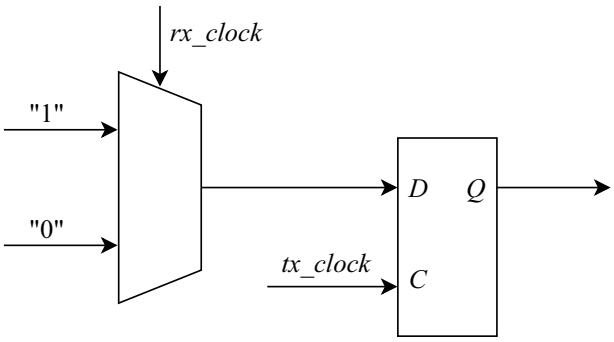

Рис. 2. RTL-схема включения *D*-триггера и мультиплексора фазового детектора.

В нашей системе синхронизации используется реализованный на ПЛИС аппаратный фазовый детектор, состоящий из мультиплексора, *D*-триггера и набора вспомогательных регистров [32]. RTL схема включения *D*-триггера и мультиплексора приведена на рис. 2: на вход синхронизации *C* *D*-триггера подается сигнал с синхронизирующего детектора (tx_clock), на вход данных *D* подается сигнал с мультиплексора. Управление мультиплексором осуществляется при помощи внутреннего сигнала приемника с частотой 156.25 MHz (rx_clock), при этом логическая единица на выходе мультиплексора формируется, когда сигнал управления также равен логической единице. Сигнал синхронизирующего детектора, несущий информацию о частоте ведущего генератора, формируется при помощи синхронизирующей последовательности заданной длины, отправляемой передатчиком с периодом $T_{rep} = 3.2$ ms.

Для каждого импульса синхронизирующей последовательности на выходе *Q* *D*-триггера формируется сигнал, представляющий собой фазовую ошибку данного им-

пульса: в случае, если положительный фронт синхронизирующего импульса придет на триггер в момент, когда сигнал внутренней частоты приемника равняется логической единице, на выходе Q также будет сформирована логическая единица, соответствующая наличию фазовой ошибки, в противном случае — логический ноль.

Далее сумма полученных сигналов для всех импульсов синхронизирующей последовательности — накопленная фазовая ошибка — используется в качестве итогового сигнала ошибки фазового детектора. Расчет величины накопленной фазовой ошибки осуществляется по положительному фронту сигнала, подаваемого на вход данных D, в течение времени, определяемого длительностью окна расчета фазовой ошибки. Благодаря использованию окна расчета удается добиться отсутствия влияния других участков синхронизирующей последовательности и шумов в квантовом канале на величину накопленной фазовой ошибки (итоговая конфигурация синхронизирующей последовательности рассмотрена в разд. 3).

Известно, что для корректной работы любого триггера необходимо обеспечить соблюдение двух временных требований: времени предустановки (setup time) и времени удержания (hold time) сигнала на входе D [33–35]. Однако в общем случае разница фаз между сигналом приемника и синхронизирующей последовательностью случайна, следовательно перечисленные временные требования будут выполняться не всегда, приводя к возникновению явления метастабильности триггера. По этой причине для предотвращения перехода уровня выхода Q в промежуточное состояние в качестве сигнала для входа D в нашей схеме используется выходной сигнал мультиплексора, а не рабочую частоту приемника напрямую. В следствие возникновения метастабильности предложенная реализация фазового детектора может принимать три различных состояния:

• момент прихода фронтов всех синхронизирующих импульсов соответствует отсутствию импульсов на частоте приемника: величина накопленной фазовой ошибки равна 0 (рис. 3, a);

• момент прихода фронтов всех синхронизирующих импульсов соответствует наличию импульсов на частоте приемника: величина накопленной фазовой ошибки максимальна (рис. 3, b);

• момент прихода фронтов синхронизирующих импульсов близок к фронтам импульсов на частоте приемника: из-за наличия джиттера сигналов и возникновения явления метастабильности величина накопленной фазовой ошибки имеет промежуточное значение, возникает плавный переход между минимальным и максимальным значением фазовой ошибки (рис. 3, c).

Помимо возникновения переходного процесса необходимо также учесть дополнительный источник неопределенности величины накопленной фазовой ошибки, возникающий из-за того, что для регистрации и формирования сигналов фазовой ошибки используются разные частоты — приемника и передатчика. Соответственно в зависимости от соотношения величин данных частот, а также текущей разности фаз между ними, возможно возникновение потерь информации о фазовых ошибках. Для ликвидации данного источника нестабильностей, в нашей схеме мы используем частоту 78.125 MHz для генерации периодической синхронизирующей последовательности. В таком случае каждому импульсу фазовой ошибки будет соответствовать два фронта на частоте 156.25 MHz, что гарантирует надежную регистрацию каждой ошибки. При этом максимальная величина накопленной фазовой ошибки будет соответствовать удвоенному числу синхронизирующих импульсов, используемых для расчета фазовой ошибки.

Поскольку промежуточное значение фазовой ошибки однозначно определяет взаимное расположение фронтов анализируемых сигналов, данное свойство может быть использовано для коррекции разницы частот данных сигналов. Для этого достаточно обеспечить удержание значения фазовой ошибки в выбранном промежуточном положении путем плавной перестройки базовой частоты f_{ref} синтезатора приемника. Для этого в нашей цепи обратной связи используется пропорционально-дифференцирующий (ПД) регулятор, выходной сигнал которого представляет собой итоговый сигнал обратной связи [36,37]. Задачей данного регулятора на каждой итерации алгоритма является поддержание постоянной разности фаз базовых частот синтезаторов приемника и передатчика путем подстройки текущей базовой частоты синтезатора приемника. Расчет нового значения $f_{ref}(n)$ выполняется следующим образом:

$$f_{ref}(n) = f_{ref}(n-1) - (P + D),$$

где P и D — пропорциональная и дифференцирующая составляющие соответственно, $f_{ref}(n-1)$ — базовая частота синтезатора на предыдущей итерации коррекции частот. Составляющие регулятора рассчитываются следующим образом:

$$P = K_p \cdot (e(n) - \Delta e_{\text{const}}),$$

$$D = K_d \cdot (e(n) - e(n-1)),$$

где K_p и K_d — коэффициенты пропорциональной и дифференцирующей составляющих соответственно, $e(n)$ и $e(n-1)$ — значения фазовой ошибки на текущей и предыдущей итерациях алгоритма соответственно, Δe_{const} — целевое значение фазовой ошибки. Из выражений (11)–(13) следует, что параметрами предложенной нами системы периодической коррекции разницы частот являются коэффициенты K_p и K_d, а также целевое значение фазовой ошибки Δe_{const}. Соответственно настройка системы сводится к определению таких значений параметров, при которых реальная точность синхронизации будет удовлетворять пороговому значению $\Delta t^{\max}_{sync+jitter} = 70\,\text{ps}$ [38].

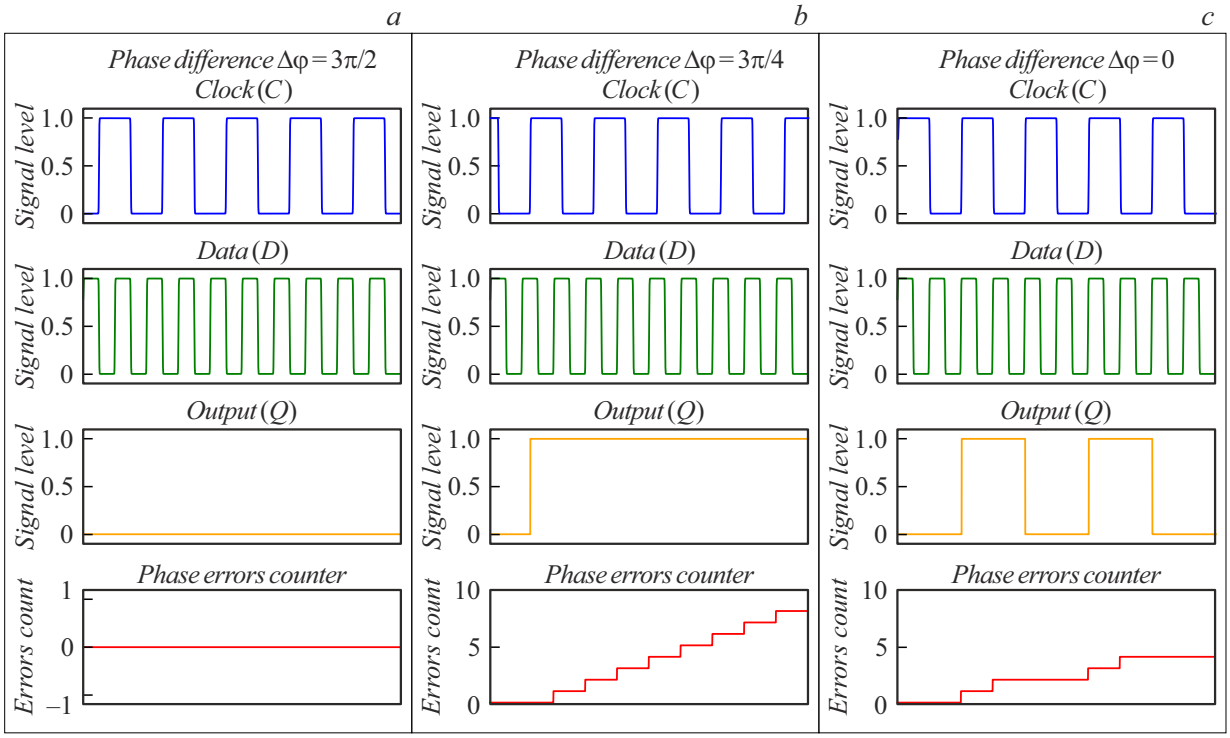

Рис. 3. Симуляция работы фазового детектора в зависимости от разницы фаз $\Delta\varphi$ между анализируемыми сигналами на входах D-триггера.

3. Метод выравнивания моментов старта приема и передачи оптических импульсов на каждом узле

Как было описано в разд. 1, для отправки синхронизирующих последовательностей через квантовый канал мы применяем метод временного мультиплексирования. При этом длительности временных окон отправки обеих последовательностей, а также задержки между ними, выраженные в количестве тактов частоты 156.25 MHz, задаются одинаковыми на приемнике и передатчике. Таким образом определяется полная длительность одной итерации цикла обмена данными между узлами. Соответственно помимо компенсации разницы частот ГОЧ необходимо регулярно выполнять процедуру определения момента старта очередной итерации цикла обмена данными на приемнике относительно старта на передатчике. В противном случае становятся возможны ситуации, когда приемник не будет регистрировать информационные кубиты, так как они будут приходить в момент времени, соответствующий окну приема синхронизирующей последовательности. Заметим, что подобный эффект возникнет и в случае, если длительности или расстановки временных окон на узлах отличаются.

В предложенном нами методе передача информации о начале новой итерации цикла на передатчике осуществляется путем включения в конец синхронизирующей последовательности одного периода M-последовательности длиной 127 bit, закодированной в виде оптических импульсов. M-последовательность представляет собой псевдослучайную двоичную последовательность, получаемую при помощи линейного регистра сдвига с обратной связью (LFSR) [39]. Для генерации последовательности нами использовался примитивный полином $P(x) = 1 + c_3x^3 + c_7x^7$. Ключевым свойством M-последовательности s является ее корреляционное свойство [40,41], согласно которому значения ненормированной АКФ R для сдвига n вычисляется как:

$$R(n) = \sum_{m=1}^{N} s[m] \cdot s[m+n] = \begin{cases} N & \text{если } n = 0 \\ -1 & \text{если } 0 < n < N. \end{cases} \tag{14}$$

Выражение (14) справедливо для M-последовательности, в которой все биты, равные 0, преобразованы в биты со значением -1. Как видно из (14), при достаточной длине M-последовательности значение $R(0)$ значительно превышает остальные значения АКФ, благодаря чему значительно возрастает помехоустойчивость и обнаружительная способность M-последовательностей [42].

Для определения момента старта приема квантовых состояний приемник выполняет непрерывное вычисление ненормированной АКФ своей копии M-последовательности передатчика и принимаемой синхронизирующей последовательности в соответствую-

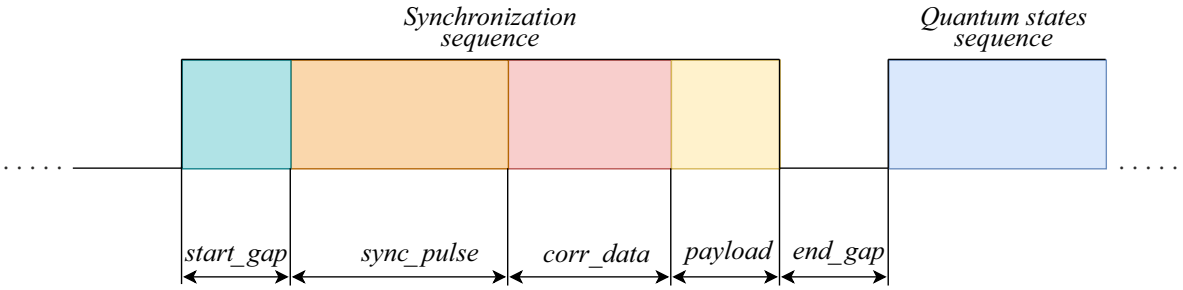

Рис. 4. Принципиальная схема используемой конфигурации синхронизирующей последовательности.

щем временном окне. В момент наложения анализируемых последовательностей приемник получит пик АКФ с высоким отношением сигнал-шум. Номер такта, соответствующий полученному пику АКФ, будет соответствовать моменту окончания формирования M-последовательности на передатчике. Соответственно, используя такое же, как передатчик, количество тактов в качестве задержки после окончания M-последовательности, приемник получит номер такта, соответствующий приходу на него первого квантового состояния с учетом задержки в квантовом канале.

Вычисление АКФ осуществляется коррелятором на ПЛИС методом побитового умножения двух последовательностей с последующим суммированием всех битов итоговой последовательности. Полученное значение АКФ сравнивается с установленным пороговым значением R_{th}, служащим критерием обнаружения пика АКФ. Поскольку элементы используемой нами M-последовательности могут принимать значения 0 и 1, при этом единиц на одну больше, максимальное значение АКФ $R(0)_{\max}$ определяется как:

$$R(0)_{\max} = \lceil L_s/2 \rceil = \lceil 127/2 \rceil = 64.$$

Используя $R_{\text{th}} < R(0)_{\max}$, мы можем компенсировать влияние искажений в регистрируемой M-последовательности. Источниками искажений в данном случае могут служить неидеальности настройки и функционирования синхронизирующего лазера и детектора, описанные в разд. 1. Заметим, что оптическое волокно обладает постоянным уровнем потерь и не является источником шумов в M-последовательности.

Принципиальная схема итоговой конфигурации синхронизирующей последовательности, формируемой передатчиком после окончания первого этапа оценки разности частот, приведена на рис. 4. Участок „sync_pulse“ соответствует периодической последовательности импульсов с частотой 78.125 MHz, используемой в процедуре коррекции частот, описанной в разд. 2.2. При этом приемник знает количество импульсов, формируемых передатчиком на участке „sync_pulse“, и использует данную информацию для определения момента окончания расчета фазовой ошибки. Далее на участке „corr_data“ на частоте 156.25 MHz передается M-последовательность, служащая для расчета фазовой ошибки. Выбор разных частот для различных участков необходим, поскольку при побитовом умножении периодической последовательности импульсов частотой 156.25 MHz на копию M-последовательности с частотой 156.25 MHz, результирующая последовательность будет равняться использованной M-последовательности. Соответственно будет получено значение АКФ $R = R(0)_{\max}$, превышающее пороговое R_{th}. В результате произойдет ошибочная регистрация M-последовательности и последующее рассогласование моментов старта окон приема и передачи.

Задержка, соответствующая участку „start_gap“, необходима, поскольку первые лазерные импульсы в синхронизирующей последовательности нестабильны и могут негативно сказаться на процедуре оценки фазовой ошибки. Нестабильность данных импульсов связана с возникновением переходных процессов в процессе розжига синхронизирующего лазера. Участок „payload“ используется для передачи полезных данных, в данном случае — номера текущей итерации цикла распределения ключей. Участок „end_gap“ используется в качестве задержки до старта окна приема информационных квантовых состояний и необходим для минимизации влияния остаточных переотражений синхронизирующей последовательности в квантовом канале на детекторы одиночных фотонов.

4. Экспериментальная часть

Для проведения экспериментальной апробации предложенной системы синхронизации, все ее компоненты, включая оптическую схему и алгоритмы управления, были интегрированы в наше устройство BB84 КРК. В результате точной настройки модулей синхронизирующего лазера, синхронизирующего детектора, а также перестраиваемого оптического аттенюатора VOA2 (рис. 1), удалось добиться стабильной регистрации оптических импульсов в диапазоне длин от 0 до 125 km оптического волокна SMF-28e между приемником и передатчиком, при этом подстройка системы синхронизации под различные длины производилась только с помощью аттенюатора VOA2. Так, на рис. 5, *a* приведена осциллограмма синхронизирующей последовательности, зарегистрированной на 100 km оптического волокна SMF-28e.

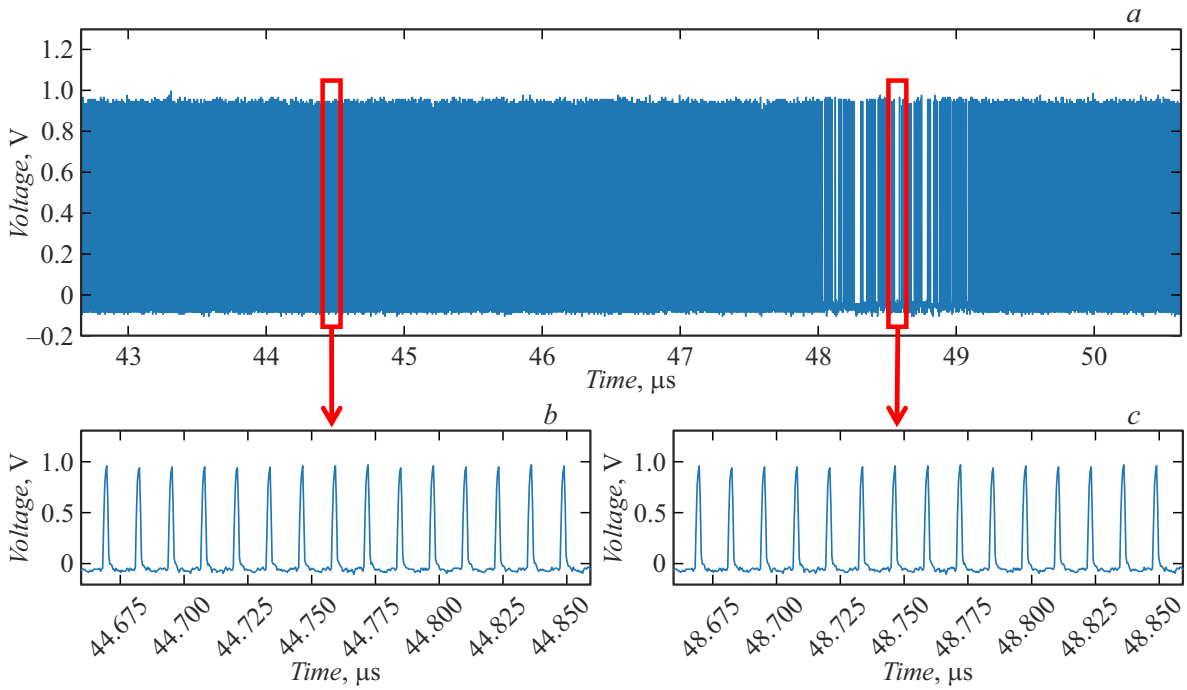

Рис. 5. Осциллограмма используемой конфигурации синхронизирующей последовательности.

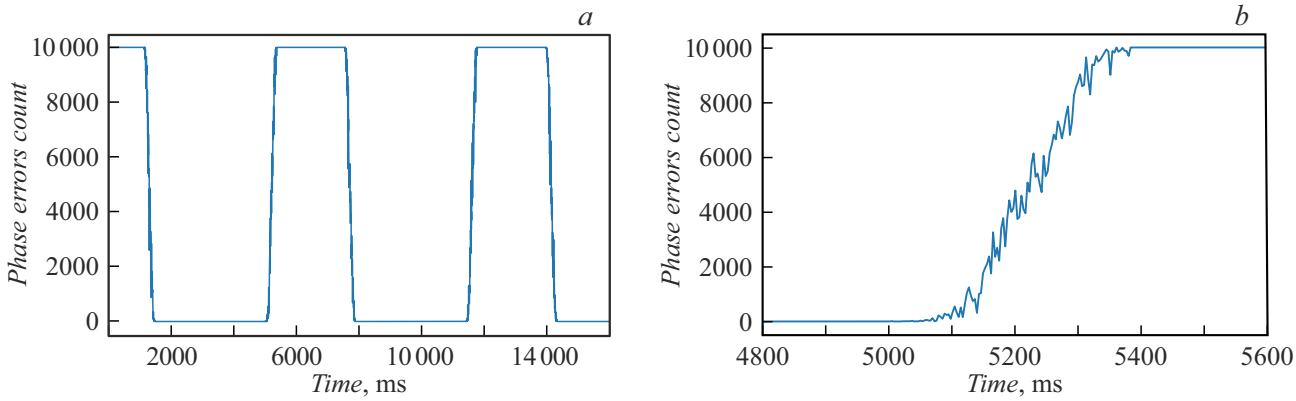

Рис. 6. Результаты экспериментальных измерений накопленной фазовой ошибки на выходе фазового детектора.

В частности, на рис. 5, *b* и *c* приведены участки, соответствующие синхронизирующей последовательности для расчета фазовой ошибки и *M*-последовательности соответственно. Видно, что в первом случае используемая частота повторения лазерных импульсов вдвое меньше, при этом форма импульсов на рис. 5, *b* не отличается от формы на рис. 5, *c*, что свидетельствует о корректной работе синхронизирующего детектора на заданной длине оптической линии.

Далее мы провели тестирование предложенной нами реализации фазового детектора. Как было показано в разд. 2.2, работа алгоритма периодической коррекции частот основана на использовании переходного процесса в величине фазовой ошибки для поддержания постоянной разности фаз между ГОЧ приемника и передатчика. Для подтверждения возникновения данного процесса мы провели измерения величины накопленной фазовой ошибки в зависимости от разности фаз между синхронизирующей последовательностью, длиной 5 000 импульсов, и сигналом приемника с частотой 78.125 MHz. В ходе эксперимента коррекция разности частот не производилась. Результаты измерений приведены на рис. 6. Видно, что полученная зависимость совпадает с результатами симуляций, показанными на рис. 3. Так, из рис. 6, *a* следует, что накопленная фазовая ошибка является периодической функцией, при этом максимальное значение фазовой ошибки составляет 10 000, что соответствует удвоенной длине использованной синхронизирующей последовательности. Рис. 6, *b* демонстрирует наличие переходного процесса, параметры которого зависят от

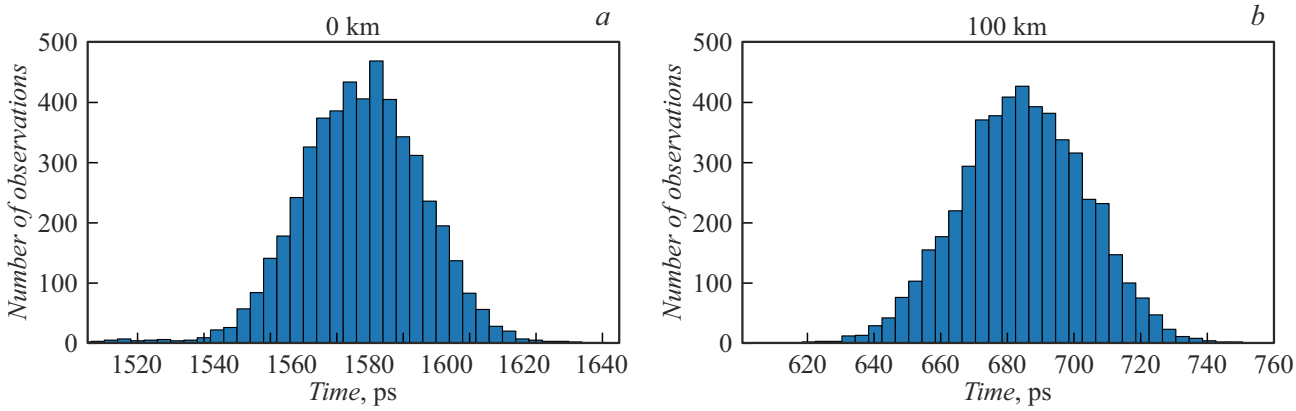

Рис. 7. Распределение величины задержки между фронтами рабочих частот приемника и передатчика на 0 и 100 km оптического волокна.

Несмещенные оценки суммарного СКО задержки на различных длинах оптической линии

Длина оптической линии, km	$\sigma_{\text{sum}}^{\text{meas}}$, ps	σ_{sum}, ps	$\sigma_{\text{sync+jitter}}$, ps
0	≈ 18.5	≈ 18.07	≈ 15.05
100	≈ 18.88	≈ 18.45	≈ 15.5

разности частот измеряемых сигналов в момент проведения измерений.

Поскольку предложенная система стартовой коррекции разницы частот не требует дополнительной настройки (разд. 2.1), финальным шагом настройки системы является определение значений параметров ПД-регулятора, используемого при периодической подстройке (разд. 2.2). Для этого мы использовали метод эмпирической настройки, в ходе которой были экспериментально протестированы различные комбинации параметров [38]. Отметим, что все последующие измерения проводились с одними параметрами ПД-регулятора.

После завершения настройки для количественной оценки предложенной системы синхронизации мы провели ряд экспериментов, в ходе которых исследовалась величина задержки между сигналами Алисы и Боба с частотой 156.25 MHz на различных длинах оптической линии в периодическом режиме работы системы коррекции частот. Данные сигналы подавались на измерительное оборудование напрямую с тестировочных SMA выходов на плате ПЛИС. В первых экспериментах мы использовали осциллограф Teledyne LeCroy WaveRunner 8404m с частотой дискретизации 40 Gs/s для точной оценки величины задержки. Гистограммы результатов измерений для 0 и 100 km оптической линии приведены на рис. 7, несмещенные оценки среднеквадратического отклонения σ_{sum}^{meas} (СКО) для данных распределений приведены в табл. 1. Форма полученных распределений свидетельствует, что предложенная система синхронизации работает корректно, поддерживая постоянную разность фаз базовых частот синтезаторов. Полученное из данных распределений значение СКО позволяет оценить суммарную точность совпадения временных отсчетов приемника и передатчика, поскольку содержит вклад сразу нескольких компонент:

$$\sigma_{sum}^{meas} = \sqrt{\sigma_{sync}^2 + \sigma_{gen}^2 + 2\sigma_{jitter}^2 + \sigma_{osc}^2},$$

где σ_{sync} — СКО, определяемое точностью коррекции частот, σ_{gen} — СКО, вызванное расхождением частот ГОЧ за период подстройки, σ_{jitter} — СКО джиттера измеряемых сигналов, σ_{osc} — СКО временного джиттера осциллографа, на котором проводились измерения. Согласно документации для использованного осциллографа $\sigma_{osc} = 4$ ps. Как было сказано ранее джиттер управляющих сигналов оказывает влияние не только на результаты проведенных измерений, но и на возможность корректной синхронизации временных отсчетов в целом, при этом σ_{jitter} необходимо учитывать дважды, поскольку джиттеры приемника и передатчика независимы друг от друга.

Поскольку форма полученного распределения близка к нормальному, воспользуемся правилом трех сигм для оценки достигнутой точности синхронизации. Для этого рассмотрим выбранные ранее значения отклонений $\Delta t^{\max} = 100$ ps, $\Delta t_{gen}^{\max} = 30$ ps и $\Delta t_{sync+jitter}^{\max} = 70$ ps в качестве границ соответствующих диапазонов $(\mu - 3\sigma; \mu + 3\sigma)$. Величина μ представляет собой средний временной сдвиг между тактами базовых частот приемника и передатчика и в дальнейших рассуждениях ей можно пренебречь ($\mu = 0$). Тогда, воспользовавшись равенством $\Delta t^{\max} = 3\sigma^{\max}$, получим следующее соотношение для СКО задержки без учета джиттера осциллографа σ_{sum}:

$$3\sigma_{sum} \in (-\Delta t^{\max}; \Delta t^{\max}). \qquad (16)$$

Аналогично, для СКО задержки без учета джиттера осциллографа и дрейфа частот ГОЧ прием-

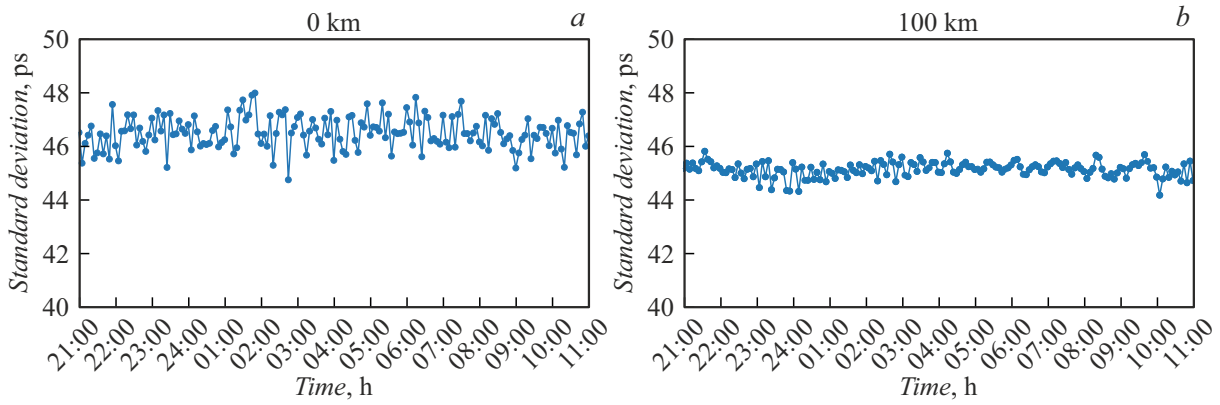

Рис. 8. Зависимость несмещенной оценки СКО задержки между сигналами приемника и передатчика с частотой 156.25 MHz от времени для оптических линий длиной 0 и 100 km.

ника и передатчика $\sigma_{sync+jitter}$, используя равенство $\Delta t^{\max}_{sync+jitter} = 3\sigma^{\max}_{sync+jitter}$ получим:

$$3\sigma_{sync+jitter} \in (-\Delta t^{\max}_{sync+jitter}; \Delta t^{\max}_{sync+jitter}), \qquad (17)$$

В табл. 1 приведены оценки точности синхронизации, полученные с помощью выражения (15), на основании которых можно сделать вывод, что на обеих оптических линиях достигнутая точность синхронизации удовлетворяет сформулированным в условиях (16) и (17) требованиям к системе синхронизации ($3\sigma_{sum} < 100$ и $3\sigma_{sync+jitter} < 70$ ps). Напомним, что в разд. 2 было показано, что выполнение данных требований гарантирует достаточную для нашего устройства КРК точность синхронизации на протяжении одного периода подстройки частот ($T_{corr} = 50$ ms).

Далее для подтверждения корректности работы системы на больших временных промежутках мы провели исследование стабильности синхронизации на больших временных промежутках. Для этого мы с заданным промежутком времени проводили измерение распределения задержки между сигналами Алисы и Боба, аналогичные измерениям из предыдущего эксперимента. Для автоматизации эксперимента вместо осциллографа был использован потоковый время-цифровой преобразователь Swabian Time Tagger 20 с заявленной величиной СКО временного джиттера 34 ps. В ходе эксперимента система коррекции частот работала в периодическом режиме, измерения проводились каждые 5 min с использованием ширины временного окна преобразователя 10 ps, набор статистики осуществлялся в течение 10 s.

На рис. 8 приведены результаты двух экспериментов, полученные с использованием двух независимых устройств КРК и оптических линий длиной 0 и 100 km соответственно. Как видно из графиков, величины СКО задержки в процессе всего эксперимента оставались постоянными, испытывая незначительные флуктуации, не сказывающиеся на работе устройства КРК. Наблюдаемая разница амплитуд флуктуаций СКО для двух устройств КРК обусловлена индивидуальными особенностями элементов оптической схемы синхронизации, в частности, параметрами и стабильностью синхронизирующих лазеров и синхронизирующих детекторов (параметры ПД-регулятора в обоих устройствах были одинаковыми). Полученные результаты позволяют заключить, что предложенная система коррекции разности частот обладает высокой временной стабильностью на оптических линиях различной длины. Отметим, что отличие величин СКО, приведенных на рис. 8, от величин в табл. 1, является следствием большой погрешности измерений при помощи Swabian Time Tagger 20.

На следующем этапе мы провели исследование, направленное на подтверждение корректности работы предложенной системы выравнивания моментов старта приема и передачи оптических импульсов. На рис. 9 приведены осциллограммы, демонстрирующие взаимное расположение окон приема и отправки квантовых состояний на Алисе и Бобе для различных оптических линий. В качестве осциллограмм синхронизирующей последовательности использованы результаты ее детектирования на приемнике. Видно, что ее расположение совпадает с промежутками между окнами приема квантовых состояний, подтверждая корректность работы системы временного мультиплексирования сигналов в оптическом канале. Как показано на нижнем графике на рис. 9, величина временного сдвига окна приема относительно окна передачи соответствует задержке, возникающей при прохождении оптическим сигналом 100 km оптического волокна. Следовательно, можно сделать вывод, что взаимное расположение окон, приведенное на верхнем и среднем графике на рис. 9, позволяет приемнику осуществлять корректную регистрацию квантовых состояний с учетом задержки в квантовом канале.

В качестве итогового тестирования разработанной системы синхронизации был проведен сеанс распределения квантовых ключей с использованием стандартного оптоволоконного квантового канала длиной 25 km. На протяжении всего средняя скорость генерации просеян-

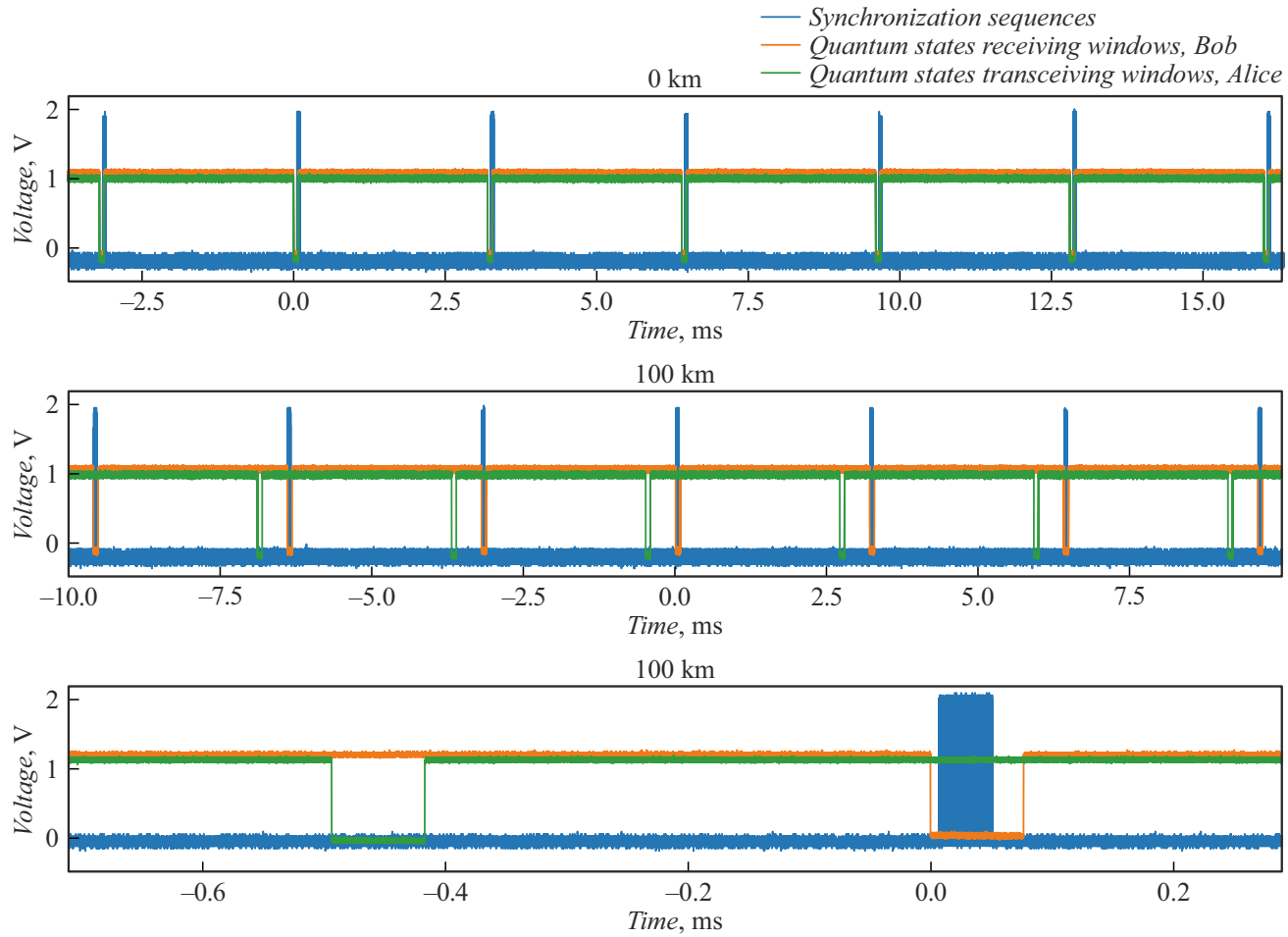

Рис. 9. Осциллограмма окон приема и передачи квантовых состояний и синхронизирующих последовательностей между ними.

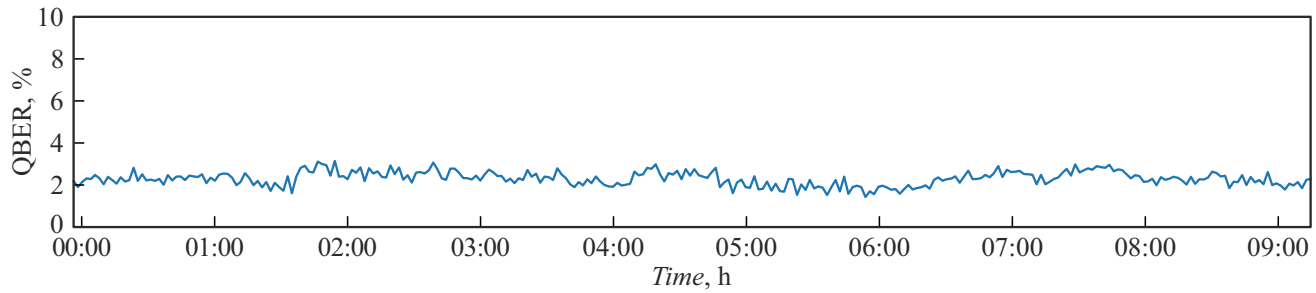

Рис. 10. Зависимость величины QBER от времени в режиме генерации квантовых ключей с использованием квантового канала длиной 25 km.

ных и секретных ключей составила ≈ 60 и ≈ 20 Kbit/s соответственно [22]. Генерация ключей ни разу не прерывалась, что подтверждает результаты предыдущих экспериментов и говорит о высокой стабильности как системы синхронизации, так и устройства КРК в целом. Средний уровень QBER в ходе эксперимента составил $\leq 4\%$. Результаты мониторинга QBER приведены на рис. 10 и свидетельствуют, что предложенная система обладает достаточной точностью синхронизации.

Заключение

В работе детально рассмотрена реализация системы коррекции разницы частот опорных генераторов для устройств КРК. Была предложена оптическая схема синхронизации, использующей методы временного и частотного мультиплексирования сигналов, а также алгоритм ее настройки, позволяющий быстро адаптироваться к оптическим линиям различной длины. Кроме того,

для формирования требований к точности коррекции были проанализированы параметры стабильности ГОЧ, используемых в устройстве. На основе полученных результатов был разработан двухступенчатый метод, обеспечивающий эффективную коррекцию разницы частот в процессе работы устройства, при этом степень влияния системы синхронизации на выработку секретных ключей была минимизирована. Также разработан помехоустойчивый метод автоматического определения момента старта приема и передачи квантовых состояний на приемнике и передатчике соответственно.

Для подтверждения работоспособности предложенных аппаратных и программных решений был проведен ряд экспериментов с использованием коммерческого устройства КРК, реализующего протокол BB84. В результате было продемонстрировано, что все компоненты предложенной системы коррекции разницы частот работают стабильно с точностью, удовлетворяющей установленным требованиям.

В качестве возможных направлений для дальнейшего развития системы предлагается реализация алгоритма автоматической настройки параметров ПД-регулятора для упрощения процесса калибровки и повышения устойчивости синхронизации в условиях изменяющихся характеристик канала [38]. Также предлагается провести значительную доработку компонентной базы, используемой в оптической схеме. Так, использование фотодиода с широким динамическим диапазоном и механизма автоматической регулировкой усиления (АРУ) в составе синхронизирующего детектора позволит значительно улучшить качество приема сигналов и повысить общую надежность системы в сложных эксплуатационных условиях [43]. Кроме того, это позволит значительно облегчить процедуру настройки предложенной оптической схемы.

Благодарности

Работа выполнена при поддержке Программы фундаментальных исследований НИУ ВШЭ в 2025 году.

Конфликт интересов

Авторы заявляют, что у них нет конфликта интересов.

Список литературы

[1] Ch.H. Bennett, G. Brassard. Theoret. Comput. Sci., **560**, 7 (2014). DOI: 10.1016/j.tcs.2014.05.025
[2] C.E. Shannon. Bell System Tech. J., **27** (3), 379 (1948). DOI: 10.1002/j.1538-7305.1948.tb01338.x
[3] N. Gisin, G. Ribordy, W. Tittel, H. Zbinden. Rev. Mod. Phys., **74** (1), 145 (2002), DOI: 10.1103/RevModPhys.74.145
[4] V. Scarani, H. Bechmann-Pasquinucci, N.J. Cerf, M. Dušek, N. Lütkenhaus, M. Peev, Rev. Mod. Phys., **81** (3), 1301 (2009). DOI: 10.1103/RevModPhys.81.1301
[5] D. Boneh и др. Notices of the AMS, **46** (2), 203 (1999).
[6] M. Sasaki, M. Fujiwara, H. Ishizuka, W. Klaus, K. Wakui, M. Takeoka, S. Miki, T. Yamashita, Z. Wang, A. Tanaka, K. Yoshino, Y. Nambu, S. Takahashi, A. Tajima, A. Tomita, T. Domeki, T. Hasegawa, Y. Sakai, H. Kobayashi, T. Asai, K. Shimizu, T. Tokura, T. Tsurumaru, M. Matsui, T. Honjo, K. Tamaki, H. Takesue, Y. Tokura, J.F. Dynes, A.R. Dixon, A.W. Sharpe, Z.L. Yuan, A.J. Shields, S. Uchikoga, M. Legré, S. Robyr, P. Trinkler, L. Monat, J.-B. Page, G. Ribordy, A. Poppe, A. Allacher, O. Maurhart, T. Länger, M. Peev, A. Zeilinger. Opt. Express, **19** (11), 10387 (2011). DOI: 10.1364/OE.19.010387
[7] B. Korzh, Ch. Ci Wen Lim, R. Houlmann, N. Gisin, M. Jun Li, D. Nolan, B. Sanguinetti, R. Thew, H. Zbinden. Nat. Photonics, **9**, 163 (2015). DOI: 10.1038/nphoton.2014.327
[8] H.-L. Yin, T.-Y. Chen, Z.-W. Yu, H. Liu, L.-X. You, Y.-H. Zhou, S.-J. Chen, Y. Mao, M.-Q. Huang, W.-J. Zhang, H. Chen, M.J. Li, D. Nolan, F. Zhou, X. Jiang, Z. Wang, Q. Zhang, X.-B. Wang, J.-W. Pan. Phys. Rev. Lett., **117** (19), 190501 (2016). DOI: 10.1103/PhysRevLett.117.190501
[9] A. Tanaka, M. Fujiwara, S.W. Nam, Y. Nambu, S. Takahashi, W. Maeda, K.-I. Yoshino, Sh. Miki, Bu. Baek, Zh. Wang, A. Tajima, M. Sasaki, A. Tomita. Opt. Express, **16** (15), 11354 (2008). DOI: 10.1364/OE.16.011354
[10] O.L. Guerreau, J.-M. Merolla, A. Soujaeff, F. Patois, J.-P. Goedgebuer, F.J. Malassenet. IEEE J. Sel. Top. Quantum Electron., **9** (6), 1533 (2004). DOI: 10.1109/JSTQE.2003.820929
[11] R.D. Cochran, D.J. Gauthier. *Qubit-based clock synchronization for QKD systems using a Bayesian approach*. arXiv (2021). DOI: 10. 3390/e23080988.eprint:2107.01304
[12] J.C. Bienfang, A.J. Gross, A. Mink, B.J. Hershman, A. Nakassis, X. Tang, R. Lu, D.H. Su, Ch.W. Clark, C.J. Williams, E.W. Hagley, J. Wen. Opt. Express, **12** (9), 2011 (2004). DOI: 10.1364/OPEX.12.002011.
[13] Р.М. Гальярди, Ш. Карп. *Оптическая связь.* (Астрель Связь, 1976).
[14] J.R. Vig. NASA STI/Recon Technical Report, **95**, 19519 (1994).
[15] M. Frerking. *Crystal oscillator design and temperature compensation.* (Springer Science & Business Media, 2012).
[16] A. Duplinskiy, V. Ustimchik, A. Kanapin, V. Kurochkin, Y. Kurochkin. Opt. Express, **25** (23), 28886 (2017). DOI: 10.1364/OE.25.028886.
[17] K.A. Patel, J.F. Dynes, I. Choi, A.W. Sharpe, A.R. Dixon, Z.L. Yuan, R.V. Penty, A.J. Shields. Phys. Rev. X, **2** (4), 041010 (2012). DOI: 10.1103/PhysRevX.2.041010.
[18] J.F. Dynes, W. WS Tam, A. Plews, B. Fröhlich, A.W. Sharpe, M. Lucamarini, Zh. Yuan, Ch. Radig, A. Straw, T. Edwards et al. Scientific reports, **6** (1), 35149 (2016).
[19] R. Kumar, H. Qin и R. Alléaume. New J. Phys., **17** (4), 043027 (2015). DOI: 10.1088/1367-2630/17/4/043027
[20] P. Eraerds, N. Walenta, M. Legré, N. Gisin, H. Zbinden. New J. Phys., **12** (6), 063027 (2010). DOI: 10.1088/1367-2630/12/6/063027
[21] Y. Mao, B.-X. Wang, Ch. Zhao, G. Wang, R. Wang, H. Wang, F. Zhou, J. Nie, Q. Chen, Y. Zhao, Q. Zhang, J. Zhang, T.-Y. Chen, J.-W. Pan. Opt. Express, **26** (5), 6010 (2018). DOI: 10.1364/OE.26.006010

[22] A.V. Duplinskiy, E.O. Kiktenko, N.O. Pozhar, M.N. Anufriev, R.P. Ermakov, A.I. Kotov, A.V. Brodskiy, R.R. Yunusov, V.L. Kurochkin, A.K. Fedorov, Y.V. Kurochkin. *Quantum-secured data transmission in urban fibre-optic communication lines*. arXiv (2017). DOI: 10.1007/s10946-018-9697-1
[23] N. Walenta, A. Burg, D. Caselunghe, J. Constantin, N. Gisin, O. Guinnard, R. Houlmann, P. Junod, B. Korzh, N. Kulesza, M. Legré, C.W. Lim, T. Lunghi, L. Monat, C. Portmann, M. Soucarros, R.T. Thew, P. Trinkler, G. Trolliet, F. Vannel, H. Zbinden. New J. Phys., **16** (1), 013047 (2014). DOI: 10.1088/1367-2630/16/1/013047
[24] C. Ho, A. Lamas-Linares, Ch. Kurtsiefer. New J. Phys., **11** (4), 045011 (2009). DOI: 10.1088/1367-2630/11/4/045011.
[25] L. Calderaro, A. Stanco, C. Agnesi, M. Avesani, D. Dequal, P. Villoresi, G. Vallone. Phys. Rev. Appl., **13** (5), 054041 (2020). DOI: 10.1103/PhysRevApplied.13.054041
[26] E. Mendes, S. Baron, C. Soos, J. Troska, P. Novellini. IEEE Trans. Nucl. Sci., **67** (3), 473 (2020). DOI: 10.1109/TNS.2020.2968112.
[27] Bing Qi Liu, Ming Zhe Liu, Gang Yang, Xiao Bo Mao, Huai Liang Li. App. Mechan. Mater., **650**, 3440 (2014). DOI: 10.4028/www.scientific.net/AMM.644-650.3440
[28] S. Das, U. Basu, R. Das, Sh. Saha, A. Basu. *FPGA Implementation of Asynchronous FIFO. Proceedings of International Conference on Industrial Instrumentation and Control* (Springer, Singapore: 2022), c. 399–407. DOI: 10.1007/978-981-16-7011-4_39
[29] A. Grebene, H. Camenzind. *Phase locking as a new approach for tuned integrated circuits. 1969 IEEE International Solid-State Circuits Conference.Digest of Technical Papers*. (IEEE, 1969) DOI: 10.1109/ISSCC.1969.1154749
[30] L.N. Arruda, S.M. Silva, B.J.C. Filho. *PLL structures for utility connected systems. Conference Record of the 2001 IEEE Industry Applications Conference. 36th IAS Annual Meeting (Cat. No. 01CH37248)* (IEEE, 2001), c. 2001–04. DOI: 10.1109/IAS.2001.955993
[31] G.A. Leonov, N.V. Kuznetsov, M.V. Yuldashev, R.V. Yuldashev. IEEE Trans. Circ. Syst. I, **62** (10), 2454 (2017). DOI: 10.1109/TCSI.2015.2476295.27
[32] J.P. Eckert. Proc. IRE, **41** (10), 1393 (2007). DOI: 10.1109/JRPROC.1953.274316
[33] L. Kleeman, A. Cantoni. IEEE Des. Test Comput., **4** (6), 4 (2007). DOI: 10.1109/MDT.1987.295189.
[34] L.-S. Kim, R.W. Dutton. IEEE J. Solid-State Circuits, **25** (4), 942 (1990). DOI: 10.1109/4.58286
[35] J.U. Horstmann, H.W. Eichel, R.L. Coates. IEEE J. Solid-State Circuits, **24** (1), 146 (1989). DOI: 10.1109/4.16314
[36] K.H. Ang, G. Chong, Y. Li. IEEE Trans. Control Syst. Technol., **13** (4), 559 (2005). DOI: 10.1109/TCST.2005.847331
[37] C. Knospe. IEEE Control Syst. Mag., **26** (1), 30 (2006). DOI: 10.1109/MCS.2006.1580151
[38] H.O. Bansal, R. Sharma, P.R. Shreeraman. J. Control Eng. Technol. **2** (4), (2012).
[39] Л.Е. Варакин. *Системы связи с шумоподобными сигналами* (1985)
[40] D.V. Sarwate, M.B. Pursley. Proc. IEEE, **68** (5), 593 (2005). DOI: 10.1109/PROC.1980.11697
[41] R.J. McEliece. *Finite fields for computer scientists and engineers* (Springer Science & Business Media, 2012)
[42] Я.Д. Ширман. *Теория и техника обработки радиолокационной информации на фоне помех* (Рипол Классик, 1981)
[43] D. Whitlow. Microwave J., **46** (5), 254 (2003).