Раздел I. Информационные технологии и защита информации

УДК 621.396.624 DOI 10.18522/2311-3103-2016-9-415

К.Е. Румянцев, А.П. Плёнкин

ЭФФЕКТИВНОСТЬ СИНХРОНИЗАЦИИ СИСТЕМЫ КВАНТОВОГО РАСПРЕДЕЛЕНИЯ КЛЮЧА НА ОДНОФОТОННЫХ ЛАВИННЫХ ФОТОДИОДАХ

Исследована в режиме синхронизации двухпроходная система квантового распределения ключа (СКРК) с фазовым кодированием состояний фотонов на основе однофотонных лавинных фотодиодов (ОЛФД). Оценено влияние на вероятностные и временные характеристики обнаружения длительности сигнального временного окна в однофотонном режиме синхронизации. Цель исследований состоит в оценке влияния параметров ОЛФД на вероятностные и временные характеристики обнаружителя сигнального временного окна в однофотонном режиме синхронизации СКРК. Доказана возможность применения ранее полученных аналитических выражений для расчёта вероятности правильного обнаружения сигнального временного окна в процессе синхронизации СКРК при использовании в качестве фотодетекторов ОЛФД. Предложен новый алгоритм синхронизации СКРК, учитывающий в процессе обнаружения оптического импульса время для восстановления рабочего состояния ОЛФД после регистрации фотона. Приведена методика проектирования процесса обнаружения оптического импульса в процессе синхронизации с учётом особенностей применения ОЛФД в качестве регистраторов одиночных фотонов. Предложен алгоритм поиска сигнального временного окна, предполагающий деление периода следования оптических импульсов на временные окна. Особенность исследуемого алгоритма синхронизации состоит в том, что он реализуется в однофотонном режиме с регистрацией фотонов, повышая безопасность режима синхронизации СКРК. Проведен анализ параметров применяемых в системах квантового распределения ключа оптических ЛФД и их влияние на обнаружение сигнального временного окна в процессе предварительной синхронизации.

Система квантового распределение ключа; однофотонный лавинный фотодиод; синхронизация; алгоритм; время синхронизации; вероятность обнаружения сигнального временного окна.

K.Yu. Rumyantsev, A.P. Pljonkin

THE EFFECTIVENESS OF SYNCHRONIZATION OF QUANTUM KEY DISTRIBUTION SYSTEM AT THE SINGLE-PHOTON AVALANCHE PHOTODIODES

The synchronization mode of quantum key distribution system (QKDS) with phase coding states of photons on the basis of single-photon avalanche photodiodes (SPAD) is investigated. Shown is the effect of the probability of detection and temporal characteristics of the signal duration of the time window in the single-photon synchronization. The purpose of research is to evaluate the influence of SPAD parameters on probabilistic and temporal characteristics of the signal detector time window in single-photon regime QKDS synchronization. Proven is the possibility of the use of previously obtained analytical expressions for the calculation of the probability of correct detection of the signal in the time window during synchronization when used as avalanche photodetectors. A new synchronization algorithm is proposed, it takes into account in the process

of detection of the optical pulse time to restore the operating state of a photon SPAD after registration. Given is the technique of designing an optical pulse detection process during synchronization with the account of features of application SPAD as registrars of single photons. Proposed is a search algorithm signal time window, suggesting the division of the repetition period of the optical pulses in the time windows. The peculiarity of the test synchronization algorithm is that it is implemented in a single-photon regime with the registration of photons, increasing the safety synchronization mode. Given is the analysis of the parameters used in the distribution systems, quantum optical key APD and their impact on the detection signal of the time window in the sync process.

Quantum key distribution system; single-photon avalanche photodiode; the synchronization algorithm; time synchronization; the probability of detection of the signal time window.

Введение. Эффективное функционирование систем КРК возможно только при условии успешной синхронизации. Процесс синхронизации заключается в высокоточном измерении длины пути распространения оптического излучения от приемопередающей станции к кодирующей и обратно. Отметим, что общая длина пути распространения включает в себя не только ВОЛС между двумя станциями, но и длины всех волоконно-оптических компонентов внутри СКРК [1, 2].

В коммерческих СКРК процесс синхронизации базируется на регистрации момента приёма оптического импульса фотодетекторами, выполненных на базе однофотонных лавинных фотодиодов (ОЛФД) [3–6].

Наиболее подходящей формой сигнала синхронизации для СКРК является периодическая последовательность оптических импульсов [7]. Здесь временными маркерами выступают сами импульсы, а процесс измерения длины распространения заключается в разбиении временного кадра, равного периоду следования импульсов, на временные окна (подынтервалы). В каждом временном окне регистрируется преобразование фотона в первичный электрон (фотоэлектрон, ФЭ) или приём импульсов темнового тока (ИТТ). Временное окно с наибольшим числом срабатываний принимается за сигнальное, остальные окна относят к шумовым.

В [8, 9] описан стенд и результаты натурных испытаний квантово-криптографической сети на базе системы КРК Clavis2 фирмы idQuantique (Швейцария). Экспериментальными испытаниями на стенде показано, что процесс синхронизации реализуется в многофотонном режиме, где среднее число фотонов на импульс измеряется сотнями и тысячами. Это согласуется с результатами исследований в [10], где показано, что в процессе синхронизации фотодетекторы работают в линейном режиме. Реализация многофотонного режима в процессе синхронизации потенциально упрощает злоумышленнику организацию несанкционированного доступа к информации. Последнее определяет актуальность поиска алгоритмов синхронизации в однофотонном режиме, обеспечивающих повышенную защищённость процесса вхождения в связь.

В [1] описан процесс синхронизации и предложен алгоритм поиска фотонного импульса при использовании в качестве регистратора ФЭ и ИТТ идеального счётчика фотонов. Предполагается, что фотонный импульс не может принадлежать одновременно двум соседним временным окнам. Отметим, что последнее справедливо лишь при значительном превышении длительности временного окна над длительностью фотонного импульса. При уменьшении длительности временного окна возрастает вероятность попадания фотонного импульса на границу между двумя соседними временными окнами.

В [11] проанализирован алгоритм синхронизации СКРК с учётом случайного момента появления фотонного импульса во временном окне. Установлено, что в реализуемом алгоритме могут приниматься ошибочные решения из-за пропуска сигнального окна при равенстве накопленного числа фотонов в двух соседних временных окнах из-за распределения между ними энергии фотонных импульсов.

В [12, 13] предложен новый алгоритм, повышающий вероятность синхронизации за счёт исключения принятия ошибочного решения при равенстве числа накопленных импульсов в соседних сигнальных временных окнах. Для оценки эффективности предлагаемого алгоритма синхронизации проведено имитационное моделирование [14]. Результаты моделирования доказали эффективность предлагаемого алгоритма. Выигрыш предлагаемого алгоритма очевиден, когда вероятность принадлежности фотонного импульса двум окнам превышает 49 %. При этом достигается снижение более чем в 4 раза вероятности принятия ошибочного решения. В то же время при проведении исследований в [1, 11-14] подчеркивалось, что в качестве фотодетектора используется идеальный однофотонный прибор, который способен регистрировать все поступающие фотоэлектроны. Кроме того, такому фотоприёмнику не требуется время для восстановления работоспособности после регистрации ФЭ или ИТТ.

Характеристики применяемых в СКРК однофотонных лавинных фотодиодов (Single Photon Avalanche Photodiode – SPAD) отличны от характеристик идеального однофотонного фотодетектора (single photon detector – SPD). Во-первых, ОЛФД регистрирует только один (первый) фотон за время анализа (время работы ОЛФД в режиме счёта фотонов). Отметим, что под временем анализа в процессе синхронизации понимается длительность временного окна. Во-вторых, в случае регистрации факта приёма фотона для ОЛФД потребуется определённое время для восстановления рабочего состояния [15, 16].

Цель исследований состоит в оценке влияния параметров ОЛФД на вероятностные и временные характеристики обнаружителя сигнального временного окна в однофотонном режиме синхронизации СКРК.

Алгоритм вхождения в синхронизм станций СКРК. В процессе вхождения в синхронизм временной кадр, равный периоду следования оптических импульсов T_s, разбивается на N_w временных окон с длительностью τ_w так, что $T_s = N_w \tau_w$.

Каждое временное окно опрашивается N раз, где N – объём выборки. Последнее эквивалентно опросу j-го временного окна во временных интервалах

$$t \in \left[(i-1)T_s + (j-1)\tau_w ; (i-1)T_s + j\tau_w \right], i = \overline{1, N};\ \ j = \overline{1, N_w}.$$

Объём выборки определяется средним числом фотоэлектронов (ФЭ) в импульсе и частотой появления импульсов темнового тока (ИТТ) в однофотонном фотодетекторе.

Предполагается абсолютная стабильность периода следования ΔT_s, и длительности $\Delta\tau_s$ фотонного импульса. Отметим, что период следования T_s (длительность временного кадра) определяется протяжённостью ВОЛС и рассчитывается исходя из скорости распространения оптического импульса в волокне. При каждом опросе временного окна фиксируется число принятых ФЭ и/или ИТТ. Случай отсутствия фотонного импульса в обследуемом шумовом временном окне подразумевает регистрацию только ИТТ [17].

После опроса всех N_w временных окон формируется массив значений зарегистрированных ФЭ и/или ИТТ

$$\left\{ n_{w.N}(j),\ j = \overline{1, N_w} \right\} = \left\{ n_{w.N}(1), n_{w.N}(2), ..., n_{w.N}(j), ..., n_{w.N}(N_w) \right\}.$$

При нахождении фотонного импульса полностью в одном временном окне правильное обнаружение возможно при выполнении двух условий. Во-первых, в сигнальном временном окне за время анализа должен быть зарегистрирован хотя бы один ФЭ или ИТТ. Во-вторых, в сигнальном окне число зарегистрированных импульсов должно строго превышать число зарегистрированных импульсов во всех остальных шумовых окнах.

При распределении фотонного импульса между двумя соседними окнами правильное обнаружение возможно при выполнении уже других условий:

- регистрация хотя бы одного ФЭ или ИТТ в одном из двух окон, содержащих фотонный импульс;
- в первом сигнальном временном окне число зарегистрированных импульсов должно строго превышать число зарегистрированных импульсов во 2-м сигнальном окне и сгенерированных ИТТ во всех остальных шумовых окнах;
- во втором сигнальном окне, содержащем часть фотонного импульса, число зарегистрированных импульсов строго превышает число зарегистрированных импульсов в 1-м сигнальном окне и сгенерированных ИТТ в каждом из шумовых окон;
- при равенстве числа накопленных импульсов в двух соседних временных окнах принимается решение о приёме фотонного импульса любым из этих окон, если количество накопленных импульсов в нём превышает число зарегистрированных импульсов в остальных окнах.

Оценка влияния ограничения на число генерируемых импульсов в ОЛФД за объём выборки. Если фотонный импульс полностью располагается внутри первого временного окна, то значения $n_{w.N}(2),\ \dots,\ n_{w.N}(j),\ \dots,\ n_{w.N}(N_w)$ в $N_w - 1$ шумовых временных окнах описываются законом Пуассона с параметром $\bar{n}_{d.N} = N \cdot \xi_d \cdot \tau_w$, а в первом сигнальном временном окне число $n_{w.N}(1)$ – с параметром $\bar{n}_{w.N} = N \cdot \xi_d \cdot \tau_w + N \cdot \bar{n}_s$. Здесь ξ_d – частота появления ИТТ, $\bar{n}_s$ – среднее число ФЭ, регистрируемых за длительность фотонного импульса.

Если же фотонный импульс одновременно располагается в двух (например, в первом и втором) временных окнах, то оба окна выступают в роли сигнальных. При этом случайные величины $n_{w.N}(3),\ \dots,\ n_{w.N}(j),\ \dots,\ n_{w.N}(N_w)$ в $N_w - 2$ шумовых окнах описываются законом Пуассона с параметром $\bar{n}_{d.N} = N \cdot \xi_d \cdot \tau_w$, а в сигнальных временных окнах числа $n_{w.N}(1)$ и $n_{w.N}(2)$ – соответственно с параметрами $\bar{n}_{w1.N} = N \cdot \xi_d \cdot \tau_w + N \cdot \bar{n}_{s1}$ и $\bar{n}_{w2.N} = N \cdot \xi_d \cdot \tau_w + N \cdot \bar{n}_{s2}$. Здесь $\bar{n}_{s1} = \bar{n}_s \cdot (1 - \tau_w/t_1)$ и $\bar{n}_{s2} = \bar{n}_s - \bar{n}_{s1}$ представляют соответственно средние числа регистрируемых фотонов в первом и втором сигнальных окнах при условии, что момент появления t_1 фотонного импульса принадлежит первому временному окну.

В [12] получено аналитическое выражение для проведения инженерных расчётов вероятности правильного обнаружения сигнального временного окна в режиме синхронизации СКРК

$$\mathrm{P_D} = \sum_{\mathrm{n_{w.N}}=1}^{\infty} \frac{(\overline{\mathrm{n_{w.N}}})^{\mathrm{n_{w.N}}}}{\mathrm{n_{w.N}!}} \cdot \exp[-\overline{\mathrm{n_{w.N}}}] \cdot \mathrm{P_{d.N}}\{\mathrm{n_{w.N}}\}. \quad (1)$$

Здесь

$$\mathrm{P_{d.N}}\{\mathrm{n_{w.N}}\} = \left(\sum_{\mathrm{n_{d.N}}=0}^{\mathrm{n_{w.N}}-1} \frac{\overline{\mathrm{n_{d.N}}}^{\mathrm{n_{d.N}}}}{\mathrm{n_{d.N}!}} \cdot \exp(-\overline{\mathrm{n_{d.N}}}) \right)^{\mathrm{N_w}-1} \quad (2)$$

представляет вероятность регистрации не более $(\mathrm{n_{w.N}} - 1)$ ИТТ во всех $(\mathrm{N_w} - 1)$ шумовых временных окнах за время анализа при условии, что в сигнальном временном окне за выборку объёмом N зарегистрировано $\mathrm{n_{w.N}}$ ФЭ и ИТТ.

Результаты моделирования показывают, что максимальное значение среднего числа ИТТ за выборку в шумовом временном окне не превышает 0,041 при разбиении временного кадра на два временных окна. При этом вероятность накопления за выборку более одного ИТТ в каждом из шумовых временных окон не превышает 0,08 %.

Напомним, что в качестве исходных данных при моделировании выступали длительность фотонного импульса τ_s=1 нс, период следования оптических импульсов T_S =1024 нс, частота появления импульсов темнового тока 400 Гц, среднее число ФЭ, принимаемых за длительность фотонного импульса $\overline{n_S}$=0,01, объём выборки отсчётов регистрируемых импульсов в каждом временном окне N=200. В процессе моделирования число временных окон N_w принимало 10 дискретных значений 1024; 512; 256; 128; 64; 32; 16; 8; 4 и 2.

При увеличении числа окон до 1024, среднее число ИТТ за выборку в шумовом временном окне опускается до 0,00008. Это позволяет производить суммирование в формуле только при 2-х значениях $n_{d.N}$, равных 0 и 1. Тогда

$$P_D = exp(-N_w \cdot \overline{n_{d.N}} + \overline{n_{d.N}}) \cdot \langle \overline{n_{w.N}} \cdot exp(-\overline{n_{w.N}}) + [1 - exp(-\overline{n_{w.N}}) - \overline{n_{w.N}} \cdot exp(-\overline{n_{w.N}})] \cdot (1 + \overline{n_{d.N}})^{N_w - 1} \rangle. \quad (3)$$

Результаты моделирования показывают, что расхождение результатов расчётов по формулам (1)−(3) не превышает 0,02 % во всём диапазоне изменений числа временных окнах.

Однако условие допустимости регистрации не выше одного ФЭ и/или ИТТ как раз и свойственно ОЛФД. Это доказывает возможность применения выражения (3) для расчёта вероятности правильного обнаружения сигнального временного окна в процессе синхронизации СКРК при использовании в качестве фотодетектора ОЛФД при условии, что $\overline{n_{w.N}} \ll 1$.

Параметры однофотонных ЛФД. Обратимся к параметрам однофотонных ЛФД, применяемых в коммерческих автокомпенсационных волоконно-оптических системах КРК с фазовым кодированием состояний фотонов. Это системы id 3000 Clavis, id 3100 Clavis2 [18] и id 5000 Vectis [19] фирмы idQuantique (Швейцария), а также системы QPN 5505, QPN 7505 [20] и QPN 8505 компании MagiQ Technologies (США).

Параметры ОЛФД имеют разное смысловое содержание в зависимости от сферы своего применения. В связи с этим проведём уточнение тех параметров ОЛФД, которые оказывают влияние на процесс синхронизации СКРК.

Квантовая эффективность (англ. detection efficiency) характеризуется производительностью лавинного фотодиода в режиме обнаружения одиночных фотонов (коэффициент полезного действия). Эта величина соответствует вероятности попадания фотона на фотодиод для обнаружения. При длине волны 1550 нм, значение эффективности обнаружения достигает 25 %, что характерно для фотодиодов на основе InGaAs/InP.

Реальный ОЛФД имеет конечное время восстановления, которое должно пройти до регистрации последующих фотонов. Суммарная временная задержка между моментом образования лавины, её гашения и последующего восстановления определяет мёртвое время регистрации фотона однофотонным фотодетектором τ_{dead}. Отметим, что чем меньше устанавливается время восстановления рабочего режима, тем больше вероятность регистрации импульсов темнового тока.

Временное разрешение τ_{FWHM} или «джиттер» (англ. «jitter») однофотонного фотодетектора определяется длительностью отклика на приём фотона (однофотонного импульса – ОФИ) на уровне половины амплитуды (англ. Full Width at Half Maximum – FWHM). Термин «джиттер» или IRF Shift (англ. Instrument Response Function Shift) использован для неопределенности временной задержки между приходом фотона и генерацией выходного импульса в ОЛФД.

Эффективная ширина ворот τ_{EGWR} (англ. effective gate width range) характеризует временной интервал, в течение которого ОЛФД может находиться в режиме счета одиночных фотонов (режим Гейгера).

В таблице 1 приведены сравнительные характеристики параметров приёмных оптических модулей на основе ОЛФД, применяемых в коммерческих системах КРК [21, 22]. Модули включают активную цепь гашения лавины, конструктивно объединённую с ОЛФД на кремниевом чипе. Чип установлен на термоэлектрическом холодильнике и упакован в стандартной головной части TO5 с прозрачным окном в крышке. Для контроля температуры используется термистор. Высокое напряжение питания, используемое для смещения ОЛФД выше напряжения пробоя (для работы в однофотонном режиме), снабжено преобразователем DC/DC. Выходной импульс модуля при приёме фотона формируется цепью временного удержания (захвата) на 50-омной нагрузке. Внутренние регулировки обеспечивают работу ОЛФД в оптимальном режиме при комнатной температуре.

Таблица 1

Параметры приёмных оптических модулей на основе ОЛФД

Наименование ОЛФД	Рабочая длина волны оптического излучения, нм	Частота появления ИТТ, не более, Гц	Мёртвое время. Типовое (макс.) значение, нс	Временное разрешение (FWHM). Типовое (макс.) значение, пс
ID100-SMF20. Обычное исполнение	350 – 900	200 (60) (5)	45 (50)	40 (60)
ID100-MMF50. ID100-MMF100. Обычное исполнение	350 – 900	200 (80) (20)	45 (50)	40 (60)
id101-20	350 – 900	15 (50)	35 (40)	40 (60)
id101-50	350 – 900	100 (300)	45 (50)	40 (60)
id110	350 – 900	250	70 – 100000	200
id110-MMF-105	350 – 900	0.1 – 0.25	70	200
id110-MMF-105	350 – 900	100 –250	1000	200
id150 (1×8)	350 – 900	15 000	50	40 (60)
id150 (1×10)	350 – 900	200 (300)	70 (100)	40 (60)
id120-500-650nm	350 – 1000	500	1 000	400 (1 000)
id120-500-800nm	350 – 1000	3 000	1 000	400 (1 000)
id201	900 – 1700	100	0,1	0,3
id210	900 – 1700	40	100 000	10
id220	900 – 1700	6 000	25 000	400
id230	900 – 1700	50	100 000	200
id280	600 – 1700	100	67	70
id400	1064	150	0,1	300
SPAD-8	350 – 900	1000	50	70
PDM	375 – 1000	5…500	77	35
InGaAs SPAD	900 – 1700	10 000	1 000-3 000 000	100

Оценка влияния временных параметров ОЛФД на эффективность синхронизации СКРК. Пусть известен показатель преломления оптического излучения в сердечнике оптического волокна (n_{fiber}=1,49). Тогда скорость распространения оптических сигналов в ВОЛС равна

$$v_{fiber} = \mathrm{c}_{opt}/\mathrm{n}_{fiber} = 300000/1{,}49 = 201000 \text{ км/с},$$

где c_{opt} – скорость оптического излучения в вакууме.

Предельная протяжённость ВОЛС между двумя станциями СКРК L_{FOL} уже превышает 100 км. С учётом обратного распространения излучения в двухпроходной автокомпенсационной волоконно-оптической системе с фазовым кодированием состояний фотонов для исключения наложения встречных импульсов при L_{FOL} =100 км значение периода следования оптических импульсов должно превышать $T_{s.min} = 2 \cdot L_{FOL}/v_{fiber}$≈1 мс. Следовательно, максимальная частота следования оптических импульсов при протяжённости ВОЛС в 100 км не должна превышать $f_{s.max} = 1/T_{s.min}$ ≈1 кГц.

Длительность оптического импульса принимается равной $\tau_s = 1$ нс и выбирается исходя из параметров, применяемых в системах КРК лазерных источников излучения.

Установлено, что в процессе начального процесса синхронизации длительность временного окна следует выбирать исходя из условия

$$\tau_w = (2 \dots 4) \cdot \tau_s. \quad (4)$$

Аналитические выражения и результаты моделирования показывают незначительные изменения вероятности правильного обнаружения сигнального временного окна (изменения в примере, в пределах от 69,89 до 67,03 %), причём с плавным падением с уменьшением длительности временного окна. При этом можно говорить об уменьшении первоначальной временной неопределённости в отношении момента приёма фотонного импульса в 2 раза при переходе от $\tau_w = 3\tau_s$ к $\tau_w = 4\tau_s$.

При анализе процесса синхронизации обычно исходят из идеальности однофотонных фотодетекторов. В первую очередь предполагается, что однофотонный фотодетектор регистрирует все приходящие фотоны (фотоэлектроны), мгновенно восстанавливая свою работоспособность. Это позволяет допустить последовательный опрос временных окон внутри временного кадра. Однако, применяемые в СКРК однофотонные лавинные фотодиоды требуют времени для восстановления работоспособности после образования лавины (формирования однофотонного импульса (ОФИ)). Последнее исключает последовательный опрос временных окон.

Кроме того, следует остановиться и ещё на одном условии, которое значительно упрощает реализацию цифровой аппаратуры. События, требующие подсчёта в процессе синхронизации, должны быть кратны 2.

Необходимость учёта отмеченных условий покажем на конкретном примере.

Пример проектирования подсистемы синхронизации в СКРК. Пусть протяжённость ВОЛС между двумя станциями СКРК L_{FOL} = 100 км. Для одномодового оптического волокна Corning®SMF-28e$^+$ на рабочей длине волны 1550 нм эффективный показатель преломления оптического излучения в сердечнике n_{fiber}=1,4670. Следовательно, скорость распространения излучения в сердечнике одномодового оптического волокна составит $v_{fiber} = \mathrm{c}_{opt}/\mathrm{n}_{fiber} \approx 205000$ км/с. С учётом обратного распространения излучения в двухпроходной автокомпенсационной волоконно-оптической системе с фазовым кодированием состояний фотонов для исключения наложения встречных импульсов значение периода следования оптических импульсов должно превышать $T_{s.min} = 2L_{FOL}/v_{fiber}$≈978 мкс. Следовательно, максимальная частота следования оптических импульсов не должна превышать 1 кГц.

Пусть передающий оптический модуль (ПОМ) генерирует оптические синхроимпульсы длительностью $\tau_s = 1$ нс с периодом следования $\mathrm{T}_s = 1$ мс ($f_s = 1/T_s \approx$ 1 кГц).

Исходя из требований (4) выбираем длительность временного окна $\tau_w = 2\tau_s$=2 нс. Требуемое для опроса количество временных окон составляет $N_w = T_s/\tau_w = 5 \cdot 10^5$ = 500 000. Следовательно, обнаружение сигнального временного окна позволит в 500 000 раз уменьшить первоначальную временную неопределённость в отношении момента приёма синхроимпульса.

Число временных окон не кратно двум. Ближайшее число, удовлетворяющее этому условию при T_s≥1 мс, будет 524 288=2^{19}. Это позволяет уточнить требования к ПОМ: период следования генерируемых оптических синхроимпульсов $T_s = N_w\tau_w = 524\,288 \cdot 2 = 1\,048\,576$ нс≈1,05 мс ($f_s = 1/T_s$ ≈954 Гц). Увеличение временного кадра не превышает 5 %.

Если объём выборки взят равным N = 256 = 2^8, то общее время анализа 256 временных кадров при использовании идеального однофотонного фотодетектора составит 256·1,05=268,8 мс.

В случае применения в ПОМ однофотонного ЛФД id100-SMF20 с частотой появления ИТТ не более 5 Гц (малошумное исполнение) среднее число регистрируемых ИТТ за объём выборки в шумовом временном окне составит всего лишь $\bar{n}_{d.N} = N \cdot \xi_d \cdot \tau_w = 256 \cdot 5 \cdot 2 \cdot 10^{-9} = 2{,}56 \cdot 10^{-6}$.

Согласно используемого алгоритма синхронизации, среднее число ФЭ в фотонном импульсе, излучаемое станцией Алиса не может превышать значения 0,1. При протяжённости ВОЛС в 100 км потери в оптическом волокне составят 20 дБ, т.е. сигнал ослабится в 100 раз. Поэтому среднее число ФЭ в фотонном импульсе, принимаемое станцией Боб составит $\bar{n}_s$ = 0,001. Следовательно, среднее число ФЭ и ИТТ, принимаемое за время действия всех фотонных импульсов за выборку в сигнальном временном окне, составит

$$\bar{n}_{w.N} = \bar{n}_{d.N} + N \cdot \bar{n}_s = 2{,}56 \cdot 10^{-6} + 256 \cdot 0{,}001 \cong 0{,}256.$$

Расчёт вероятности правильного обнаружения сигнального временного окна в режиме синхронизации СКРК при использовании в качестве регистратора идеального счётчика фотонов по приближённой формуле (3) даёт $P_{\mathrm{D}} = 7{,}95$ %.

Отметим, что расчёты по точным формулам (1) и (2) отличаются от расчетов по упрощённому выражению (3) не больше чем на 0,002 %.

С учетом предельного ослабления оптического сигнала при обратном распространении до уровня 0,001, увеличим объём выборки до 1024. С учетом этого, получим вероятность обнаружения по выражению (3) $P_{\mathrm{D}} = 27{,}5$ %. В тоже время при частоте импульсов темнового тока 25 Гц, среднем уровне сигнала 0,01, объёме выборки 1024 получим вероятность правильного обнаружения по формуле (3) $P_{\mathrm{D}} = 99{,}89$ %.

Однако при проведении расчётов не учитывалось мёртвое время регистрации фотона однофотонным ЛФД τ_{dead}, типовое значение которого для образца id100-SMF20 составляет 45 нс. Это указывает, что после осмотра временного окна потребуется время $\tau_w - \tau_{dead}$ на восстановление работоспособности однофотонного ЛФД. В нашем случае время от момента начала осмотра временного окна до момента завершения процесса восстановления ЛФД эквивалентно времени на осмотр τ_{dead}/τ_w не менее 22 окон.

Последнее требует введения понятия длительности модуля τ_m, которое не может быть меньше мёртвого времени регистрации фотона τ_{dead}. В нашем случае выбор длительности модуля целесообразно остановить на τ_m=64 нс. Тогда за 1-й цикл будет проанализировано каждое 32-е (2^6) временное окно, т.е. осмотр 1-го,

33-го, 65-го и т.д. временных окон (рис. 1). После осмотра последнего 2^{19}: 2^6=2^{13}-го (2^{19} : 2^6) временного окна система должна перейти ко второму циклу и анализу уже 2-го, 34-го, 66-го и т.д. временных окон. По завершению последнего 32-го цикла будет завершён осмотр всех временных окон в кадре по одному разу. Заметим, что число циклов равно $N_c = \tau_m/\tau_w$.

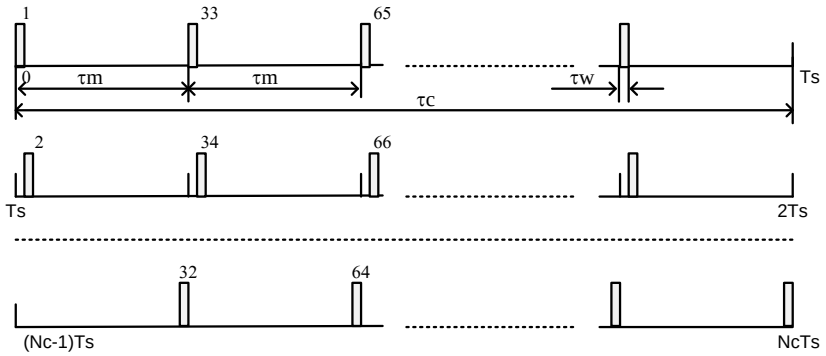

Рис. 1. Поиск сигнального временного окна с учётом мёртвого времени регистрации фотона однофотонным ЛФД

Общее время анализа при требуемом объёме выборки 256 с учётом мёртвого времени регистрации фотона однофотонным ЛФД возрастает в N_c раз (количество циклов), составляя уже 8,6 с.

Ситуация ещё более ухудшается в случае применения приёмного модуля id230, у которого мёртвое время составляет 1000 мс. В этом случае за один цикл может быть осмотрено только одно временное окно, а число циклов станет равным числу всех временных окон в кадре, т.е. $N_c = N_w = 2^{19}$. При этом общее время анализа при том же объёме выборки 256 достигает 39 часов.

Отметим, что исследована оценка влияния временных параметров ОЛФД на эффективность синхронизации в системах КРК с фазовым кодированием состояний фотонов. В системах КРК с другими способами кодирования, например, поляризационным, временным и др., указанные требования будут отличны.

Выводы. Описан принцип работы предварительного этапа вхождения в синхронизм двухпроходной автокомпенсационной СКРК с фазовым кодированием состояний фотонов. Предложен алгоритм поиска сигнального временного окна, предполагающий деление периода следования оптических импульсов на временные окна. Особенность исследуемого алгоритма синхронизации состоит в том, что он реализуется в однофотонном режиме с регистрацией фотонов, повышая безопасность режима синхронизации СКРК. Предложено аналитическое выражение для инженерных расчётов вероятности правильного обнаружения сигнального временного окна, снижающее требования к вычислительным ресурсам. Проведен анализ параметров применяемых в системах квантового распределения ключей оптических ЛФД и их влияние на обнаружения сигнального временного окна в процессе предварительной синхронизации. Исследована временная модель предварительного этапа вхождения в синхронизм системы КРК. Показано, что предлагаемый алгоритм позволяет сократить время вхождения в связь за счет анализа нескольких временных окон за период следования оптического импульса.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Плёнкин А.П., Румянцев К.Е.* Синхронизация системы квантового распределения ключа при использовании фотонных импульсов для повышения защищённости // Известия ЮФУ. Технические науки. – 2014. – № 8 (157). – С. 81-96.
2. *Румянцев К.Е.* Системы квантового распределения ключа: монография. − Таганрог: Изд-во ТТИ ЮФУ, 2011. – 264 с.
3. *Gisin N., Ribordy G., Tittel W., Zbinden H.* Quantum cryptography // Reviews of Modern Physics. – 2002. – Vol. 74, No. 1. – P. 145-195.
4. *Gisin N. et al.* Quantum cryptography // Rev. Mod. Phys. − 2002. − Vol. 74, No. 1. − P. 145-195.
5. *Bennet C.H. et al.* Experimental quantum cryptography // J. Cryptol. − 1992. − Vol. 5. − P. 3-28.
6. *Muller A. et al*. «Plug and play» systems for quantum cryptography // Appl. Phys. Lett. − 1996. − Vol. 70, No. 7. − P. 793-795.
7. *Гальярди Р.М., Карп Ш.* Оптическая связь: пер. с англ. / под ред. А.Г. Шереметьева. − М.: Связь, 1978. – 424 с.
8. *Плёнкин А.П.* Исследование режима вхождения в синхронизм при использовании фотонных импульсов системы квантового распределения ключа // ES-ФМ-2014-011. Физико-математические методы и информационные технологии в естествознании, технике и гуманитарных науках: сборник материалов международного научного е-симпозиума. Россия, г. Москва, 27–28 декабря 2014 г. – Киров: МЦНИП, 2015. – С. 101-113.
9. *Румянцев К.Е., Плёнкин А.П.* Экспериментальные испытания телекоммуникационной сети с интегрированной системой квантового распределения ключей // Телекоммуникации. – 2014. – № 10. – С. 11-16.
10. *Курочкин В.Л., Курочкин Ю.В., Зверев А.В., Рябцев И.И., Неизвестный И.Г.* Экспериментальные исследования в области квантовой криптографии // Фотоника. – 2012. – № 5. – С. 54-66.
11. *Румянцев К.Е., Плёнкин А.П.* Безопасность режима синхронизации системы квантового распределения ключей // Известия ЮФУ. Технические науки. – 2015. – № 5 (156). – С. 152-160.
12. *Румянцев К.Е., Плёнкин А.П.* Повышение эффективности алгоритма вхождения в синхронизм системы квантового распределения ключей // Известия ЮФУ. Технические науки. – 2015. − № 8 (169). – С. 6-19.
13. *Rumyantsev K.E., Pljonkin A.P.* Preliminary Stage Synchronization Algorithm of Autocompensation Quantum Key Distribution System with an Unauthorized Access Security. International Conference on Electronics, Information, and Communications (ICEIC). 2016. Vietnam, Danang. – P. 1-4. DOI: 10.1109/ELINFOCOM.2016.7562955.
14. *Румянцев К.Е., Плёнкин А.П.* Моделирование процесса вхождения в синхронизм системы квантового распределения ключа при использовании для регистрации фотонных импульсов однофотонного лавинного фотодетектора для повышения защищённости: Свидетельство №2015610876. − Ростов-на-Дону, 2015. − 11 с.
15. *Румянцев К.Е., Плёнкин А.П.* Синхронизация системы квантового распределения ключа в режиме однофотонной регистрации импульсов для повышения защищенности // Радиотехника. – 2015. – № 2. – С. 125-134.
16. *Задорин А.С., Максимов А.В., Махорин Д.А.* Режимы работы фотоприемного устройства системы квантовой криптографии // Доклады ТУСУРа. – 2012. − № 2 (26). – С. 63-66.
17. *Pljonkin A., Rumyantsev K.* Single-photon synchronization mode of quantum key distribution system // International Conference on Computational Techniques in Information and Communication Technologies (ICCTICT). − India, New Delhi, 2016. − P. 531-534. DOI: 10.1109/ICCTICT.2016.7514637.
18. Clavis. Plug & play quantum cryptography // id 3000. Specifications. id Quantique SA. – Ver. 2.1. – January 2005. – 2 p.
19. Vectis. id 5000. Specifications // id Quantique SA. – Ver. 1.2. – April 2005. – 2 p.
20. QPN 5505. User's manual // MagiQ Technologies, Inc. – November 2004. – 62 p. − URL: www.magiqtech.com.
21. *Kang Y. et al.* InGaAs-on-Si single photon avalanche photodetectors // Appl. Phys. Lett. − 2004. − Vol. 85, No. 10. − P. 1668-1670.
22. Single photon detection modules with high timing resolution and low dark count rate. Visible single-photon counters. 2016. Specifications as of January 2016. − URL: www.idquantique.com.

REFERENCES

1. *Plenkin A.P., Rumyantsev K.E.* Sinkhronizatsiya sistemy kvantovogo raspredeleniya klyucha pri ispol'zovanii fotonnykh impul'sov dlya povysheniya zashchishchennosti [Synchronization of quantum key distribution system using photon pulses to improve the security], *Izvestiya YuFU. Tekhnicheskie nauki* [Izvestiya SFedU. Engineering Sciences], 2014, No. 8 (157), pp. 81-96.
2. *Rumyantsev K.E.* Sistemy kvantovogo raspredeleniya klyucha: monografiya [The system of quantum key distribution: a monograph]. Taganrog: Izd-vo TTI YuFU, 2011, 264 p.
3. *Gisin N., Ribordy G., Tittel W., Zbinden H.* Quantum cryptography, *Reviews of Modern Physics*, 2002,– Vol. 74, No. 1, pp. 145-195.
4. *Gisin N. et al.* Quantum cryptography, *Rev. Mod. Phys*., 2002, Vol. 74, No. 1, pp. 145-195.
5. *Bennet C.H. et al.* Experimental quantum cryptography, *J. Cryptol*, 1992, Vol. 5, pp. 3-28.
6. *Muller A. et al*. «Plug and play» systems for quantum cryptography, *Appl. Phys. Lett*., 1996, Vol. 70, No. 7, pp. 793-795.
7. *Gal'yardi R.M., Karp Sh.* Opticheskaya svyaz' [Optical communication]: translation from English, ed. by A.G. Sheremet'eva. Moscow: Svyaz', 1978, 424 p.
8. *Plenkin A.P.* Issledovanie rezhima vkhozhdeniya v sinkhronizm pri ispol'zovanii fotonnykh impul'sov sistemy kvantovogo raspredeleniya klyucha [Study of mode of entry into synchronism when using the photon pulses of the system of quantum key distribution], *ES-FM-2014-011. Fiziko-matematicheskie metody i informatsionnye tekhnologii v estestvoznanii, tekhnike i gumanitarnykh naukakh: sbornik materialov mezhdunarodnogo nauchnogo e-simpoziuma. Rossiya, g. Moskva, 27-28 dekabrya 2014 g*. [ES-FM-2014-011. Physico-mathematical methods and informational technologies in science, technology and the Humanities: materials of the international scientific e-conference. Russia, Moscow, 27-28 Dec 2014], [Electronic resource]. Kirov: MTsNIP, 2015, pp. 101-113.
9. *Rumyantsev K.E., Plenkin A.P.* Eksperimental'nye ispytaniya telekommunikatsionnoy seti s integrirovannoy sistemoy kvantovogo raspredeleniya klyuchey [Experimental testing of telecommunication networks with integrated quantum key distribution], *Telekommunikatsii* [Telecommunications], 2014, No. 10, pp. 11-16.
10. *Kurochkin V.L., Kurochkin Yu.V., Zverev A.V., Ryabtsev I.I., Neizvestnyy I.G.* Eksperimental'nye issledovaniya v oblasti kvantovoy kriptografii [Experimental research in the field of quantum cryptography], *Fotonika* [Photonics], 2012, No. 5, pp. 54-66.
11. *Rumyantsev K.E., Plenkin A.P.* Bezopasnost' rezhima sinkhronizatsii sistemy kvantovogo raspredeleniya klyuchey [Security of synchronization mode of quantum keys distribution system], *Izvestiya YuFU. Tekhnicheskie nauki* [Izvestiya SFedU. Engineering Sciences], 2015, No. 5 (156), pp. 152-160.
12. *Rumyantsev K.E., Plenkin A.P.* Povyshenie effektivnosti algoritma vkhozhdeniya v sinkhronizm sistemy kvantovogo raspredeleniya klyuchey [Improving efficient of synchronization algorithm of quantum key distribution system], *Izvestiya YuFU. Tekhnicheskie nauki* [Izvestiya SFedU. Engineering Sciences], 2015, No. 8 (169), pp. 6-19.
13. *Rumyantsev K.E., Pljonkin A.P.* Preliminary Stage Synchronization Algorithm of Autocompensation Quantum Key Distribution System with an Unauthorized Access Security. International Conference on Electronics, Information, and Communications (ICEIC). 2016. Vietnam, Danang, pp. 1-4. DOI: 10.1109/ELINFOCOM.2016.7562955.
14. *Rumyantsev K.E., Plenkin A.P.* Modelirovanie protsessa vkhozhdeniya v sinkhronizm sistemy kvantovogo raspredeleniya klyucha pri ispol'zovanii dlya registratsii fotonnykh impul'sov odnofotonnogo lavinnogo fotodetektora dlya povysheniya zashchishchennosti: Svidetel'stvo №2015610876 [Modeling of the process of entering into synchronism system of quantum key distribution when used for registration of photon pulses single-photon avalanche photo-detector to enhance safety and security: Certificate No. 2015610876]. Rostov-on-Don, 2015, 11 p.
15. *Rumyantsev K.E., Plenkin A.P.* Sinkhronizatsiya sistemy kvantovogo raspredeleniya klyucha v rezhime odnofotonnoy registratsii impul'sov dlya povysheniya zashchishchennosti [Synchronization system of quantum key distribution in single-photon mode of check pulses to make it more secure], *Radiotekhnika* [Radioengineering], 2015, No. 2, pp. 125-134.
16. *Zadorin A.S., Maksimov A.V., Makhorin D.A.* Rezhimy raboty fotopriemnogo ustroystva sistemy kvantovoy kriptografii [Modes of operation of the photodetector system of quantum cryptography], *Doklady TUSURa* [Proceedings of TUSUR], 2012, No. 2 (26), pp. 63-66.

17. *Pljonkin A., Rumyantsev K.* Single-photon synchronization mode of quantum key distribution system, *International Conference on Computational Techniques in Information and Communication Technologies (ICCTICT)*. India, New Delhi, 2016, pp. 531-534. DOI: 10.1109/ICCTICT.2016.7514637.
18. Clavis. Plug & play quantum cryptography, *id 3000. Specifications. id Quantique SA*, Ver. 2.1. January 2005, 2 p.
19. Vectis. id 5000. Specifications, *id Quantique SA*, Ver. 1.2, April 2005, 2 p.
20. QPN 5505. User's manual, *MagiQ Technologies, Inc*., November 2004, 62 p. Available at: www.magiqtech.com.
21. *Kang Y. et al.* InGaAs-on-Si single photon avalanche photodetectors, *Appl. Phys. Lett*., 2004, Vol. 85, No. 10, pp. 1668-1670.
22. Single photon detection modules with high timing resolution and low dark count rate. Visible single-photon counters. 2016. Specifications as of January 2016. Available at: www.idquantique.com.

Статью рекомендовал к опубликованию к.т.н., доцент Е.А. Ищукова.

Румянцев Константин Евгеньевич − Южный федеральный университет; e-mail: rke2004@mail.ru; 347928, г. Таганрог, ул. Чехова, 2; тел.: 89281827209; кафедра информационной безопасности телекоммуникационных систем; зав. кафедрой; д.т.н.; профессор.

Плёнкин Антон Павлович – e-mail: pljonkin@mail.ru; тел.: 89054592158; кафедра информационной безопасности телекоммуникационных систем; к.т.н.; ассистент.

Rumyantsev Konstantin Evgen'evich – Southern Federal University; e-mail: rke2004@mail.ru; 2, Chekhov street, Taganrog, 347928, Russia; phone: +79281827209; the department of information security of telecommunication systems; head of department; dr. of eng. sc.; professor.

Pljonkin Anton Pavlovich – e-mail: pljonkin@mail.ru; phone: +79054592158; the department of information security of telecommunication systems; cand. of eng. sc.; assistant.

УДК 621.39 DOI 10.18522/2311-3103-2016-9-1526

В.В. Котенко

ЭФФЕКТИВНОСТЬ ВИРТУАЛЬНОГО ПОМЕХОУСТОЙЧИВОГО КОДИРОВАНИЯ

Проведен анализ стратегических моделей передачи и защиты информации с позиций теории виртуализации. Проведенный анализ показал возможность усовершенствования известных решений путём обеспечения криптографической эффективности кодирования на основе виртуализации информационных потоков. Отличительной особенностью виртуализации помехоустойчивого кодирования является реализованная возможность комплексного решения задач помехоустойчивости, криптографической защиты и имитостойкости. Это при сравнительно низких экономических затратах позволит существенно расширить возможности телекоммуникационных систем в части защиты информации. Виртуализация реализуется включением на выходе преобразования кодирования и на входе преобразования декодирования модуля виртуализации информационного потока, осуществляющего декодирование кодограмм исходного и виртуального информационных потоков, кодирование результатов декодирования и задержки во времени кодограмм и сообщений. Это обеспечивает оптимизацию исходных преобразований кодирования и декодирования. В работе экспериментально обоснована эффективность комплексного решения задач защиты информации с позиций виртуализации процессов помехоустойчивого кодирования. Экспериментально исследовались эффективность криптографической защиты, обеспечиваемая виртуальными помехоустойчивыми кодами и влияние виртуализации на эффективность исходного помехоустойчивого кода. Оценка эффективности криптографической защиты осуществлялось путем применения апробированного комплекса тестов NIST STS в ходе экспериментальной проверки компьютерной модели комплекса виртуального кодирования и базового криптографического алгоритма aes256-cbc. Полученные результаты показывают, что виртуальное помехоустойчивое кодирование обеспечивает эф-