А. С. Герасимов, Д. М. Голубчиков, А. В. Горбунов, А. В. Мамаев, И. В. Рябченко

ЭКСПЕРИМЕНТАЛЬНЫЕ ИССЛЕДОВАНИЯ РЕЖИМА СКАНИРОВАНИЯ ДЛИНЫ ЛИНИИ СВЯЗИ В СИСТЕМЕ КВАНТОВОГО РАСПРЕДЕЛЕНИЯ КЛЮЧЕЙ ID 3100 CLAVIS2

В настоящее время широкое распространение получили RSA-криптосистемы, которые применяются для решения различных задач защиты информации: в режиме шифрования для обеспечения секретности и целостности информации, в режиме электронной цифровой подписи для обеспечения аутентификации информации и подтверждения подлинности авторства [1]. В основе защищенности RSA-криптосистем лежит предположение о невозможности факторизации больших чисел за приемлемое время с использованием классических компьютеров. В 1994 г. П. Шор (P. Shor) создал квантовый алгоритм факторизации числа, позволяющий разложить число $N \sim 2^n$ на множители за время $O(n^2 \log n \log\log n)$ [2]. Текущие достижения в сфере разработки квантовых компьютеров (вычислительных устройств, использующих квантово-механические эффекты) говорят о том, что стойкость подобных криптосистем в перспективе будет поставлена под сомнение.

Эффекты квантовой механики могут быть использованы не только при создании квантового компьютера, но и при разработке квантовых методов связи. Примером квантового метода связи может служить передача информации, закодированной в поляризации фотонов, по волоконно-оптическим линиям связи [3]. Такие методы связи позволяют, основываясь на принципе неопределенности Гейзенберга (Heisenberg) или на парадоксе Эйнштейна — Подольского — Розена (Einstein — Podolsky — Rosen, EPR), обнаружить наличие факта перехвата при передаче информации.

Разработанные на данный момент протоколы квантового распределения ключей (Quantum Key Distribution, QKD), такие как протокол Беннета — Брассара (Bennett — Brassard) BB84, протокол Беннета B92, протокол Экерта (Ekert) E91, протокол SARG (Scarani — Acin — Ribordy — Gisin), позволяют решить задачи обеспечения секретности и целостности передаваемой информации.

Эффективная работа систем квантового распределения ключей (СКРК) возможна только при условии обеспечения синхронизации моментов прихода фотонов и подачи стробирующих импульсов на однофотонные детекторы.

Для обеспечения синхронизации необходимо с высокой точностью определить общую длину оптического пути распространения фотонов, включающую как линию связи между двумя узлами СКРК, так и длины всех оптических компонентов внутри блоков СКРК, в том числе линий задержки.

Система квантового распределения ключей id3100 Clavis2 является двухпроходной системой. Импульс лазера, сгенерированный станцией QKDS-B, посылается на станцию QKDS-A, где отражается при помощи зеркала Фарадея и ослабляется аттенюатором до заданного уровня (как правило, до уровня, соответствующего в среднем 0,1 фотона на импульс). Измерение длины линии связи в данной системе осуществляется путем измерения времени прохождения импульса от станции QKDS-B до станции QKDS-A и обратно.

В процессе измерения длины линии связи станция QKDS-B излучает одиночные лазерные импульсы и формирует стробирующие импульсы для однофотонных детекторов, последовательно увеличивая время их задержки относительно момента излучения лазерного импульса. При этом определяется время грубой задержки Coarse Delay, которой соответствует интервал с наибольшим количеством срабатываний детекторов. Затем аналогичным образом происходит определение точной задержки Fine Delay (рис. 1).

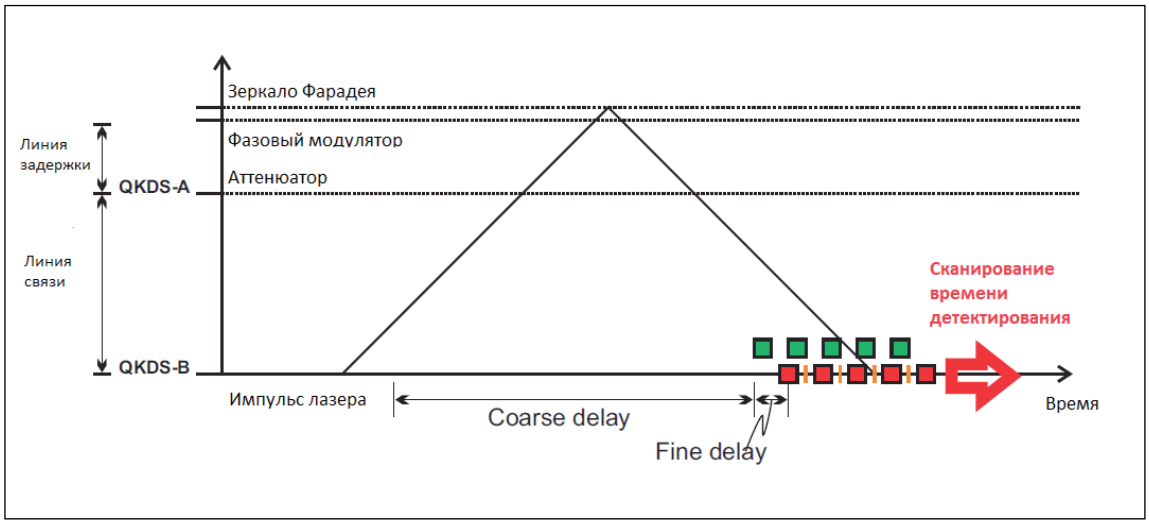

Рис. 1. Определение задержки распространения импульсов

В ряде случаев наиболее целесообразным режимом сканирования линии связи является режим RangeScan + GateScan Line Length Measurements. Однако для использования данного режима необходимо задать ориентировочное значение длины линии связи между узлами СКРК. При этом особенностью реализации режима RangeScan в СКРК Clavis2 является то, что реальная длина линии связи и длина, определяемая по результатам сканирования, могут довольно существенно различаться. Как показал ряд проведенных экспериментов, это различие достигает нескольких сотен метров и не является постоянной величиной.

Режим RangeScan + GateScan Line Length Measurements состоит из трех последовательных этапов работы оборудования: Range Scanning, Gate Scanning и Windows Scanning [4]. В режиме Range Scanning станция QKDS-B формирует одиночные лазерные импульсы длительностью около 8,4 нс с частотой следования около 800 Гц (рис. 2). Пиковая мощность импульсов на выходе станции QKDS-B составляет около минус 17,8 дБм. На данном этапе осуществляется определение диапазона значений грубой задержки Coarse Delay (как правило, определяемый диапазон составляет 3 единицы, при этом одна единица Coarse Delay соответствует 1/1,2 = 0,83 м).

В режиме Gate Scanning происходит уточнение длины линии связи путем сканирования определенного ранее диапазона Coarse Delay и предварительной оценки времени задержки Fine Delay. Форма излучаемых в линию связи импульсов аналогична режиму Range Scanning.

Рис. 2. Осциллограмма тактового импульса запуска лазера в режиме Range Scanning

На этапе Windows Scanning осуществляется точное определение времени задержки Fine Delay (одна единица которой соответствует времени задержки 10 пс). В данном режиме сканирования используются кадровая структура импульсов и алгоритмы синхронизации, аналогичные используемым в режиме формирования сырого ключа (Raw Key Exchange).

Структура кадра импульсов, излучаемых в линию связи на этапе Windows Scanning, показана на рис. 3. Один кадр состоит из преамбулы в 15 импульсов, паузы, соответствующей 2 импульсам, и 1058 импульсов в основной части кадра. Общая длительность кадра составляет около 215 мкс, период следования импульсов в кадре — около 200 нс.

Невозможность указания ориентировочного значения длины линии связи при использовании режима Range Scanning приводит к необходимости расширения границ диапазона сканирования, что, в свою очередь, существенно увеличивает время сканирования и, соответственно, время вывода системы на рабочий режим формирования ключей. Проведенные эксперименты показали, что время сканирования в режиме Range Scanning диапазона длин в 1 км составляет около 2,5 часа.

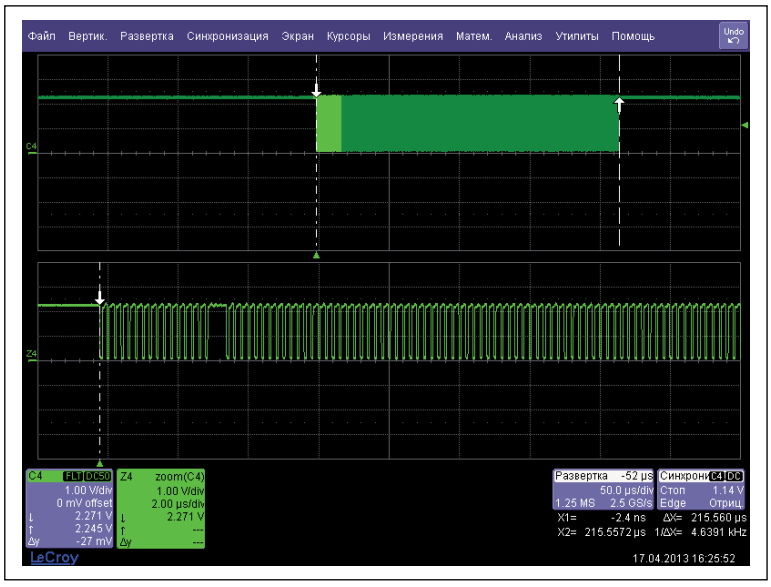

Рис. 3. Осциллограмма тактовых импульсов запуска лазера в режиме Windows Scanning

Определение ошибки в сканировании длины линии связи и особенно зависимости этой ошибки от длины линии позволит значительно сократить время сканирования и тем самым обеспечить оперативность запуска СКРК на не используемых ранее линиях связи, для которых отсутствуют результаты сканирования в виде параметров Coarse Delay / Fine Delay, используемых в СКРК id3100 Clavis2.

Для определения ошибки в сканировании проведены эксперименты, суть которых заключается в сканировании нескольких вариантов линий связи с заранее известной длиной, сопоставлении результатов сканирования с фактической длиной каждой линии связи, вычислении ошибки сканирования и определении ее зависимости от длины исследуемой линии связи.

В качестве имитации линии связи использовались соединительные шнуры длиной 2 и 20 м, нормализующие катушки с длинами 0,5, 1, 2 и 4 км и бобина волокна протяженностью около 25,2 км.

Для определения длины используемых катушек волокна проведены рефлектометрические измерения с помощью рефлектометра Yokogawa AQ7275. Для повышения точности измерения осуществлялись в обоих направлениях с последующим усреднением результатов с помощью встроенных средств рефлектометра. На рис. 4 показана рефлектограмма последовательного соединения четырех нормализующих катушек с длинами 0,5, 1, 2 и 4 км.

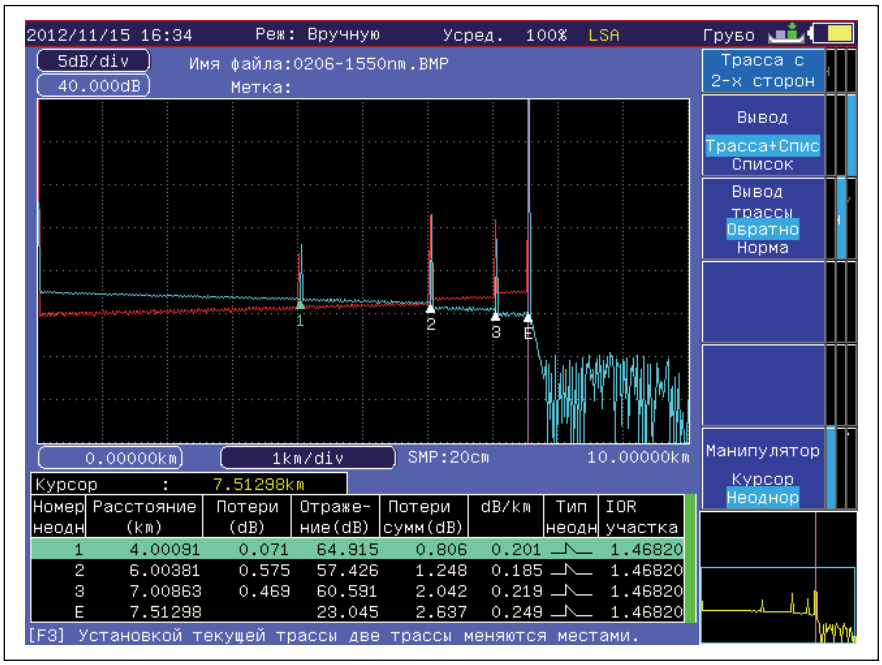

Рис. 4. Рефлектограмма последовательного соединения четырех нормализующих катушек с длинами 0,5, 1, 2 и 4 км

При проведении измерений эффективный показатель преломления волокна установлен в значение n_e = 1,4682 (паспортное значение для одномодового волокна Corning SMF-28e, используемого в нормализующих катушках).

Как видно из результатов измерений, приведенных в нижней части рис. 4, длины катушек (при округлении до метров) определены как 504, 1004, 2003 и 4001 м.

Рефлектограмма нормализующей катушки 1 км и бобины волокна Corning SMF-28e+ показана на рис. 5. Как видно из результатов измерений, длина бобины волокна Corning SMF-28e+ (при округлении до метров) определена как 26237 – 1004 = 25233 м.

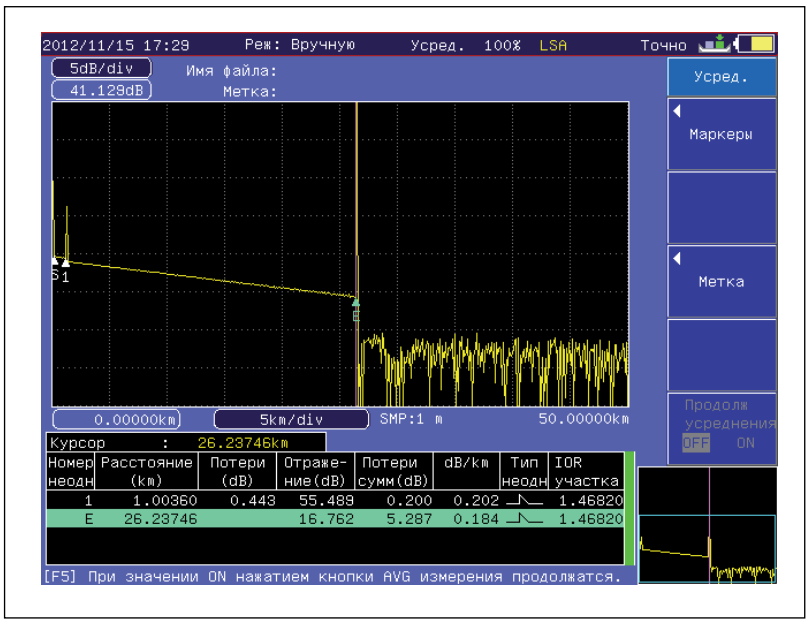

Рис. 5. Рефлектограмма последовательного соединения нормализующей катушки 1 км и бобины волокна Corning SMF-28e+ с длиной около 25,2 км

Далее в ходе экспериментальных исследований проведено сканирование указанных ранее соединительных шнуров, нормализующих катушек и бобины волокна в режиме Range Scanning для определения значений длин линий связи, фиксируемых СКРК id3100 Clavis2. Полученные результаты представлены в таблице 1.

Таблица 1. Результаты сканирования длин линии связи в режиме Range Scanning СКРК Clavis2

Паспортная длина, м	Измеренная длина в режиме Range Scanning СКРК id3100 Clavis2, м
2	987
20	1004
500	1480
1000	1969
2000	2947
4000	4904
25244	25710

Сопоставляя значения, полученные при рефлектометрических измерениях, и значения, полученные при сканировании в режиме Range Scanning (таблица 2), можно заключить, что в результатах сканирования присутствует некоторая ошибка, причем значение этой ошибки зависит от длины линии связи.

Таблица 2. Сопоставление результатов рефлектометрических измерений и результатов сканирования в режиме Range Scanning

Паспортная длина, м	Измеренная рефлектометром длина при эффективном показателе преломления волокна $n_e = 1{,}4682$, м	Измеренная СКРК id3100 Clavis2 длина в режиме Range Scanning, м	Ошибка сканирования, м (графа 3 — графа 2 (1))
2	—	987	985
20	—	1004	984
500	504	1480	976
1000	1004	1969	965
2000	2003	2947	944
4000	4001	4904	903
25244	25233	25710	477

По полученным результатам ошибки сканирования построен график (рис. 6), из которого можно заключить, что зависимость ошибки сканирования от длины линии связи близка к линейной.

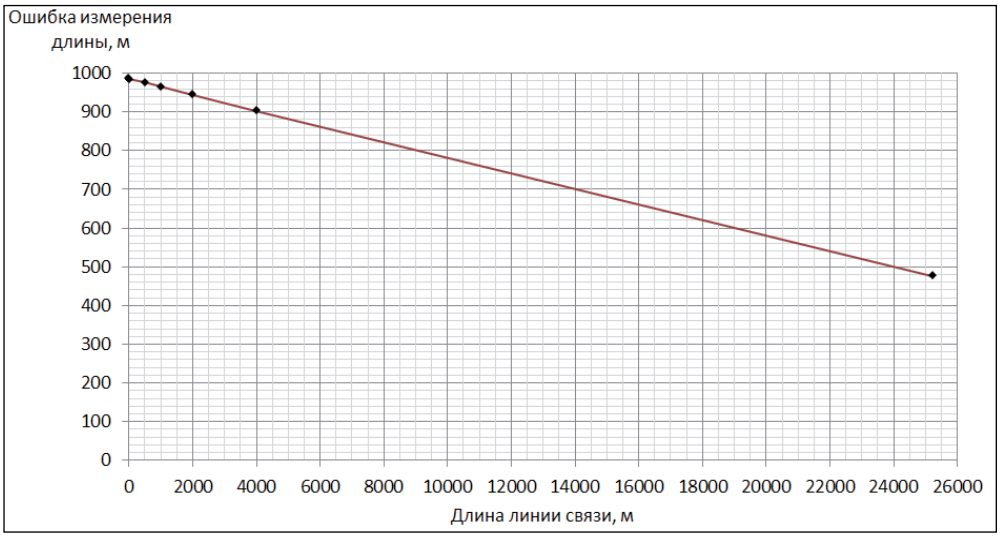

Рис. 6. Зависимость значения корректировки длины линии (в метрах) от фактической длины линии (в метрах), измеренной рефлектометрическим методом при эффективном показателе преломления волокна $n_e = 1{,}4682$

Аппроксимация полученной экспериментальной зависимости с помощью метода наименьших квадратов позволяет получить следующее выражение:

$$\Delta L[\text{м}] = -2{,}0133 \times 10^{-2} \times L_0[\text{м}] + 985, \quad (1)$$

где ΔL — расчетное значение ошибки определения длины линии связи; L_0 — фактическое значение длины линии (при эффективном показателе преломления волокна $n_e = 1{,}4682$).

Непостоянное значение ошибки говорит о влиянии двух факторов — неверный учет длины внутренней линии задержки и несовпадение показателя преломления волокна, используемого системой в расчетах, с реальным значением показателя преломления волокна, используемого в линии связи.

Например, при использовании эффективного показателя преломления волокна $n_e = 1{,}49837$ длина бобины волокна, использованной в эксперименте, будет определена рефлектометром как 24725 м. В этом случае ошибка сканирования составит 25710 – 24725 = 985 м, то есть будет равна значению ошибки сканирования при нулевой длине линии. Другими словами, при использовании в рефлектометрических измерениях длины линии связи значения эффективного показателя преломления волокна $n_e = 1{,}49837$ ошибка сканирования не будет существенно зависеть от длины линии связи и составит около 985 м.

Из выражения (1) при известных длине линии связи L_x, определенной рефлектометрическим способом, и показателе преломления n_x, используемом при рефлектометрических измерениях, можно получить формулу для расчета значения длины линии связи L_{RS}, которую необходимо указывать при сканировании линии связи в режиме Range Scanning:

$$L_{RS}[\text{м}] = L_x[\text{м}]\left(\frac{n_x}{1{,}49837}\right) + 985 \cdot \quad (2)$$

Таким образом, полученные в работе эмпирические формулы (1) и (2) позволяют по результатам рефлектометрических измерений длины имеющейся линии связи L_x рассчитать ошибку ΔL, учесть эту ошибку в качестве поправки к исходным данным и определить скорректированное значение длины L_{RS}, которое необходимо указать СКРК id3100 Clavis2 в режиме сканирования Range Scanning.

Справедливость выражений (1) и (2) проверена при сканировании длин линии связи 5, 6 и 7 км, не используемых в основной части экспериментов. При этом различия в скорректированных длинах линии связи и значениях, полученных при сканировании в режиме Range Scanning, не

превышали 3 м, что позволяет указывать диапазон сканирования около 5–10 м и тем самым уменьшать время сканирования до нескольких минут.

СПИСОК ЛИТЕРАТУРЫ:

1. *Тилборг ван Х. К. А.* Основы криптологии. Профессиональное руководство и интерактивный учебник. М.: Мир, 2006. – 471 с.
2. *Холево А. С.* Введение в квантовую теорию информации. М.: МЦНМО, 2002. – 128 с.
3. *Валиев К. А.* Квантовая информатика: компьютеры, связь и криптография // Вестник Российской Академии наук. 2000. № 8. С. 688–695.
4. Quantum Key Distribution System id3100 Clavis2. User Guide. Version 2.0. 2011.