УДК 53

Д. И. Пустоход, Д. Б. Хорошко, В. Н. Чижевский, С. Я. Килин

КВАНТОВОЕ РАСПРЕДЕЛЕНИЕ КЛЮЧА ПОСРЕДСТВОМ КОДИРОВАНИЯ ПО ВРЕМЕНИ

Институт физики им. Б.И.Степанова НАН Беларуси
пр-т Независимости, 68, 220072 Минск, Беларусь
d.pustakhod@dragon.bas-net.by

Современные системы защиты информации нуждаются в системах распределения криптографических ключей между двумя удаленными точками. В данной работе описывается протокол квантового распределения ключа посредством кодирования по времени и экспериментальные результаты, полученные при его реализации.

Передача ключа осуществляется с помощью когерентных лазерных импульсов, ослабленных до уровня одиночных фотонов. При кодировании используются четыре типа сигналов: опорные, сигнальные импульсы и импульсы-ловушки (рис. 1).

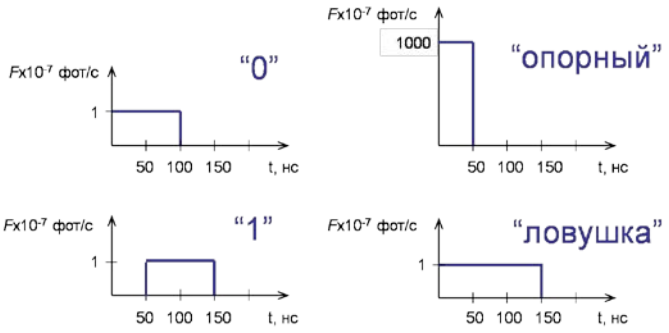


Рис. 1 — Типы световых импульсов, используемых в протоколе кодирования

Опорные импульсы используются для синхронизации задающих генераторов передающей и принимающей сторон (далее Алисы и Боба соответственно). В качестве сигнальных выступают лазерные импульсы длительностью t_{pulse} = 100 нс. При передаче «0» генерируется импульс, не смещенный относительно начала такта линии связи (ЛС), а при передаче «1» импульс смещается на половину своей длины. Импульсы-ловушки имеют длительность, равную длительности такта ЛС и используются для обнаружения присутствия перехвата.

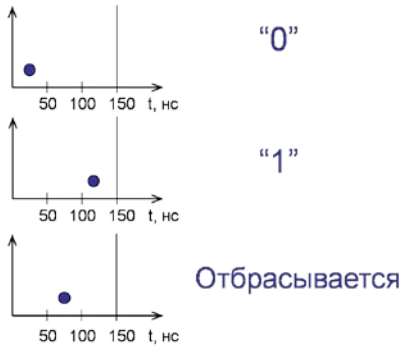
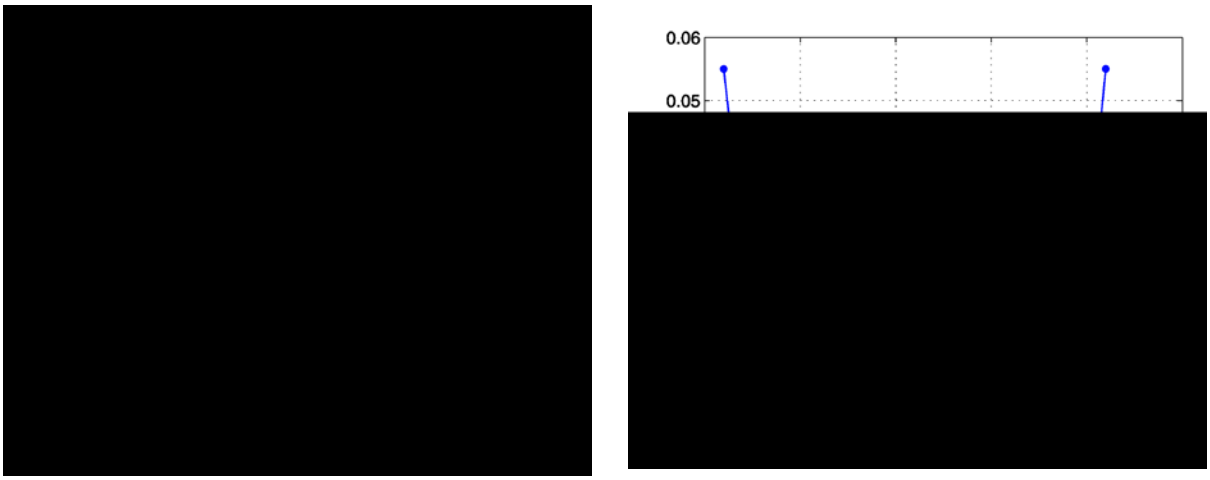


Рис. 2 — Интерпретация смещений получаемых сигналов Бобом

Принимающая сторона в процессе обмена информацией по квантовому каналу с помощью сигнального детектора фиксирует интервалы между принимаемыми однофотонными импульсами. После проведения синхронизации генераторов (на основе сильных опорных импульсов, регистрируемых по переднему фронту), для каждого полученного сигнала Боб вычисляет его смещение относительно начала такта ЛС и декодирует данные согласно рис. 2.

Часть светового потока ответвляется с помощью делителя 50/50 в контрольную ветвь с интерферометром Маха-Цандера и контрольным детектором. Разность хода в плечах интерферометра составляет половину длины сигнального импульса. Набором статистики времен регистрации для импульсов-ловушек измеряется фазовый шум $Q_P = N_P/N_A$, где N_P — число фотонов на контрольном детекторе во временном окне от 50 нс до 150 нс от начала такта ЛС за время T, а N_A — число фотонов на сигнальном детекторе за то же время. В случае отсутствия перехвата и идеальной экспериментальной установки фазовый шум Q_P=0. На основе измеренной величины фазового шума стороны делают оценку уровня информации I_E, доступной перехватчику, и определяют, можно ли считать передачу ключа секретной.

На этапе вторичной обработки [1] стороны, обмениваясь информацией по классическому (незащищенному) каналу, проводят коррекцию ошибок полученного ключа и усиление секретности для уменьшения параметра I_E до произвольно заданного малого значения.



а б

а — гистограмма смещений регистрируемых импульсов от начала такта ЛС, б — уровень ошибок в зависимости от смещения сигнала от начала такта ЛС.

Рис. 3 — Экспериментальные характеристики кодирования и декодирования данных слабыми лазерными импульсами с системе квантового распределения ключа. Длительность такта — 2,5 нс

На рис.3а приведено распределение времен регистрации фотонов Бобом. Вертикальными линиями обозначены границы интервалов, при попадании отсчета в которые Боб производит однозначное декодирование полученного импульса. Значения этих интервалов выбираются таким образом, чтобы минимизировать уровень ошибок (рис. 3б).

Полученные предварительные результаты говорят о возможности эффективной передачи ключа на расстояние до 5 км по оптическому волокну при использовании излучения на длине волны 850нм. Переход на длины волн 1,55 мкм обеспечит увеличение расстояния на порядок.

[1] Квантовая криптография: идеи и практика / Под ред. С. Я. Килина, Д. Б. Хорошко, А. П. Низовцева.— Беларуская навука, 2007.