КВАНТОВАЯ КРИПТОГРАФИЯ: КВАНТОВОЕ РАСПРЕДЕЛЕНИЕ КЛЮЧА ПОСРЕДСТВОМ КОДИРОВАНИЯ ЧЕРЕЗ ВРЕМЕННЫЕ СДВИГИ

ПУСТОХОД Д.И., ХОРОШКО Д.Б., ЧИЖЕВСКИЙ В.Н., КИЛИН С.Я.

Государственное научное учреждение "Институт физики имени Б. И. Степанова Национальной академии наук Беларуси", 220072, г. Минск, пр. Независимости, 68

Квантовое распределение ключа (КРК) — это технология, позволяющая создать у двух удаленных пользователей строку случайных бит, которая может использоваться в качестве криптографического ключа. Ключ длиной, равной длине передаваемого сообщения, является необходимым для использования в симметричных криптосистемах, которые обладают совершенной секретностью. Этим они отличаются от широко используемых в настоящее время криптосистем с открытым ключом, которые считаются секретными при условии ограниченности ресурсов противника. КРК обеспечивает безусловную секретность ключа, что означает отсутствие значимой информации о ключе у потенциального перехватчика, имеющего доступ к линии связи и неограниченные вычислительные возможности.

Для создания ключа используется свойство невозможности клонирования произвольного состояния квантового объекта. Оно заключается в том, что не существует линейного отображения пространства состояний квантовой системы $H \to H \otimes H$ такого, чтобы для любого волнового вектора $|\psi\rangle \in H$ выполнялось $|\psi\rangle \to |\psi\rangle|\psi\rangle$ [1]. Поэтому, метод перехвата информации, состоящий в копировании и последующем чтении копии, в квантовом канале связи невозможен. Любая же попытка измерить состояние самого квантового носителя информации вносит шум в передаваемый сигнал, по наличию которого легитимные стороны могут судить о наличии перехвата.

К настоящему времени предложено и теоретически обосновано достаточно много различных протоколов КРК. Основными из них являются BB84, B92 и протокол Экерта [2, 3, 4]. В качестве квантовых носителей информации в них

выступают одиночные фотоны в различных поляризационных состояниях. Следует отметить, что использование поляризованного света для передачи информации по коммерческому оптоволокну сталкивается с большими трудностями из-за значительного двулучепреломления стандартного волокна.

Нами был разработан и экспериментально реализован протокол КРК на основе кодирования через временные сдвиги, являющийся развитием протокола, предложенного в [5]. 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).

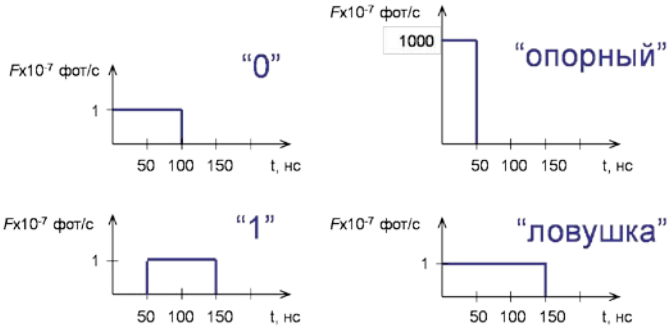

Рис. 1 — Типы световых импульсов, используемых в протоколе кодирования

Опорные импульсы используются для синхронизации генераторов передающей и принимающей сторон (далее Алисы и Боба соответственно). В качестве сигнальных применяются лазерные импульсы длительностью t_{pulse} = 100 нс. Импульсы, которыми кодируется «0» и «1», имеют разное смещение от начала такта ЛС (рис. 1). Импульсы-ловушки используются для обнаружения присутствия перехвата.

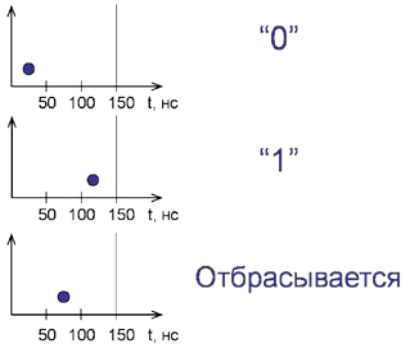

Рис. 2 — Интерпретация смещений получаемых сигналов Бобом

Принимающая сторона с помощью детектора одиночных фотонов фиксирует интервалы между принимаемыми однофотонными импульсами. Для каждого полученного фотоотсчета 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. Разность оптических длин двух плеч интерферометра составляет t_{pulse} / 2 = 50 нс. Анализ видности интерференционной кар-

тины позволяет оценить уровень информации I_E, доступной перехватчику, на основании чего стороны определяют, можно ли считать передачу данных секретной.

На этапе вторичной обработки [6] стороны, обмениваясь информацией по классическому (незащищенному) каналу, проводят коррекцию ошибок в полученных числовых последовательностях и усиление секретности для уменьшения параметра I_E до произвольно заданного малого значения.

Полученные экспериментальные результаты демонстрируют эффективную передачу ключа на расстояние до 5 км по оптическому волокну при использовании излучения на длине волны 850 нм. При переходе на длину волны 1,55 мкм это расстояние может быть увеличено на порядок.

[1] Wootters, W.K. A single quantum cannot be cloned / W.K. Wootters, W.H. Zurek // Nature. — 1982. — Vol. 299. — P 802.

[2] Bennett, C.H. Quantum cryptography: Public key distribution and coin tossing / C.H. Bennett, G. Brassard // Proceedings of IEEE International Conference on Computers and Systems and Signal Processing (Bangalore, India). — 1984. — P. 175–179.

[3] Bennett, C.H. Quantum cryptography using any two nonorthogonal states / C.H. Bennett // Phys. Rev. Lett. — 1992. — Vol. 68. — P. 3121.

[4] Ekert, A. Quantum cryptography based on Bell's theorem / A. Ekert // Phys. Rev. Lett. — 1991. — Vol. 67, No. 6. — P.661–663.

[5] Debuisschert, T. Time coding protocols for quantum key distribution / T. Debuisschert, W. Boucher // Phys. Rev. A. — 2004. — Vol. 70. — P. 042306.

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