УДК 621.396

05.00.00 Технические науки

СИСТЕМЫ КВАНТОВОГО РАСПРЕДЕЛЕНИЯ КЛЮЧА И ПРОБЛЕМЫ ИХ ПРАКТИЧЕСКОЙ РЕАЛИЗАЦИИ

Лойко Валерий Иванович
Заслуженный деятель науки РФ, доктор технических наук, профессор
Кубанский государственный аграрный университет, Краснодар, Россия

Хисамов Франгиз Гильфанетдинович
Доктор технических наук, профессор

Бобылев Михаил Владимирович
Оператор научной роты
Краснодарское высшее военное училище, Краснодар, Россия

Целью данной работы является анализ разработанных систем квантового распределения ключей, возможности применения этих систем, а так же анализ проблем их практического применения

Ключевые слова: КРИПТОГРАФИЯ, КВАНТОВОЕ РАСПРЕДЕЛЕНИЕ КЛЮЧА

UDC 621.396

Technical sciences

QUANTUM DISTRIBUTION SYSTEMS AND PROBLEMS OF THEIR PRACTICAL IMPLEMENTATION

Loyko Valeriy Ivanovich
Dr.Sci.Tesch., Honoured science worker of the Russian Federation, professor
Kuban state agrarian university, Krasnodar, Russia

Khisamov Frangiz Gilfanetdinovich
Dr.Sci.Tech., professor

Bobilev Mihail Vladimirovich
Operator of the Scientific devision
Krasnodar high military academy, Krasnodar, Russia

The goal of the study is to analyze the existing quantum distribution systems, their probable applications, as well as the issues with their practical implementation

Keywords: CRYPTOGRAPHY, QUANTUM KEY DISTRIBUTION

Введение

В современном мире передача конфиденциальных данных между несколькими абонентами в различных сетях связи может привести как к потере передаваемой информации, так и к ее компрометации. Компрометация означает превращение секретных данных в несекретные, т. е. разглашение информации, ставшей известной какому-либо лицу, не имеющему права доступа к ней.

Передача по каналу зашифрованных файлов позволяет решить проблему с перехватом информации в открытом виде. Предварительно зашифровав файлы, пользователь системы может обеспечить их защищённость. Однако, при этом возникает ряд проблем, связанных с распространением файлов, основные из которых связаны с распространением ключей.

Проблема распределения секретных ключей является одной из важнейших проблем, связанных с защитой информации, передаваемой по телекоммуникационным каналам. Как только пользователи получают общий секретный ключ, криптограммы можно пересылать по любому незащищенному от прослушивания каналу, возможно даже по каналу, подверженному полному пассивному прослушиванию (например, публичные объявления через средства массовой информации). Однако, чтобы получить общий секретный ключ, два пользователя, у которых изначально нет никакой общей секретной информации, должны использовать какой-то очень надежный и секретный канал. Поскольку перехват представляет собой серию измерений, проведенных подслушивающим агентом, какими бы сложными они не были с технической точки зрения, то любой канал можно в принципе прослушать. Это создает серьезную угрозу безопасности, чем и обусловлена важность обнаружения подслушивающего агента.

Таким образом, секретность передаваемой криптограммы может быть гарантирована только при условии, что ключ (или даже некоторая его часть) не попали к подслушивающему агенту. Следует подчеркнуть, что не существует никакого классического криптографического механизма, который давал бы полную гарантию, что ключ не был перехвачен при передаче по обычному (не квантовому) коммуникационному каналу.

Квантовые протоколы распределения секретных ключей предлагают другой подход к решению этой проблемы. Теоретически, квантовая криптография может обеспечить защищенное от перехвата распределения ключа, поскольку, в отличие от классической криптографии, она основана на законах физики, а не на том факте, что для успешного перехвата потребовались бы огромные вычислительные мощности. Вследствие вышеупомянутых свойств квантовых систем, злоумышленник вносит в передаваемую отдельными фотонами информацию некоторое количество

ошибок, которые могут быть обнаружены легитимными пользователями [1, с. 35-50].

Отметим, что законы квантовой механики позволяют не только обнаружить возмущения состояний, но и связать уровень ошибок при измерениях у легитимных пользователей с количеством информации, которую мог получить злоумышленник. Это приводит к усилению секретности передаваемого ключа за счет того, что выборка переданного ключа будет зависеть от уровня фоновых ошибок при передаче. В результате количество информации о ключе, зависящее от шума в канале связи, будет ограничено сверху сколь угодно малой величиной, с вероятностью близкой к единице. Таким образом, протоколы квантового распределения ключей, в отличие от большинства классических схем, имеют теоретико-информационную стойкость, не зависящую от вычислительных и других технических возможностей злоумышленника.

В идеальных системах квантовой коммуникации перехват данных невозможен, так как он моментально обнаруживается участниками обмена по возникающим ошибкам в передаче. Однако реальные системы отличаются от идеальных.

Проблемы практического применения систем квантового распределения ключей

Результатом различия реальных и идеальных систем квантового распределения ключа являются следующие проблемы их практического применения.

Во-первых, аппаратура участников информационного обмена несовершенна, что приводит к появлению ошибок приема-передачи. В этих обстоятельствах наличие определенного уровня ошибок не должно восприниматься системой как попытка подслушивания. А наличие

собственного фона ошибок позволяет противнику осуществлять перехват, маскируя неизбежно возникающие при этом искажения под собственные ошибки системы [2, с. 353 - 356].

Во-вторых, из невозможности клонирования состояний фотонов следует, что использование усилителя в системах квантовой криптографии оказывает такое же разрушающее воздействие при передаче по оптическому квантовому каналу, как и попытка перехвата сообщения. Поэтому требованием к квантово-криптографическим системам является малость потерь в передающем оптическом волокне, а также использование для регистрации фотонов фотодетекторов, работающих в режиме счета единичных фотонов. Следовательно, из-за потерь при передаче, волоконно-оптическая квантово-криптографическая система может оперировать только на ограниченных расстояниях. Для всех существующих систем, основанных на инфракрасных фотонах и кварцевых световодах, минимальный уровень потерь оптического излучения составляет порядка 0,2 дБ/км.

Основная трудность в применении волоконно-оптической квантово-криптографической системы с фазовым кодированием состоит в необходимости добиться полной идентичности всех компонентов двух интерферометров системы, что само по себе довольно трудно реализуется на практике. Рассмотрим зависимость видности интерференции от рассогласования оптических путей в интерферометре. Для оптических монохроматических волн видность интерференционной картины всегда равна 1. Свет от реального физического источника никогда не бывает строго монохроматическим, так как даже самая узкая спектральная линия обладает конечной шириной. Кроме того, физический оптический источник имеет конечные размеры и состоит из огромного числа элементарных излучателей. Поэтому для адекватного описания интерференции рассматривают квазимонохроматический свет. То есть

свет, состоящий из спектральных компонент, которые занимают частотный интервал, малый по сравнению со средней частотой [2, с. 363 – 356].

В волоконно-оптических интерферометрах на четкость интерференции негативно влияет также дрейф фазы оптического излучения. Поэтому для нормальной работы оптической установки необходима активная система компенсации дрейфа фазы и подстройка фазы каждый раз перед циклом передачи ключа. Для того, чтобы количество ошибок в сыром ключе не превышало 11% (максимально допустимое количество), ошибка в установке фазы должна быть менее 10 %.

Одной из основных проблем квантовой криптографии является то, что до сих пор невозможно создавать чистые однофотонные оптические импульсы. Обычно источником света для квантовой криптографии является просто ослабленный аттенюатором луч лазера. Для такого типа света число фотонов в оптическом импульсе есть случайная величина с пуассоновским распределением. Это значит, что некоторые импульсы могут вообще не содержать фотонов, а в других может быть несколько фотонов. Из оптических импульсов с более чем одним фотоном информация может быть подслушана, а для очень слабых импульсов мало отношение сигнала к шуму.

При повышении скорости передачи данных в волоконно-оптических квантово-криптографических системах, появляются проблемы, связанные с детектированием единичных фотонов. На сегодняшний день многие квантово-криптографические системы работают на низкой частоте, так как повышение частоты ведет к повышению процента ошибок при детектировании [3, с. 3229 – 3239].

На рисунке 1 показана система фазового кодирования на одном интерферометре с отражателями.

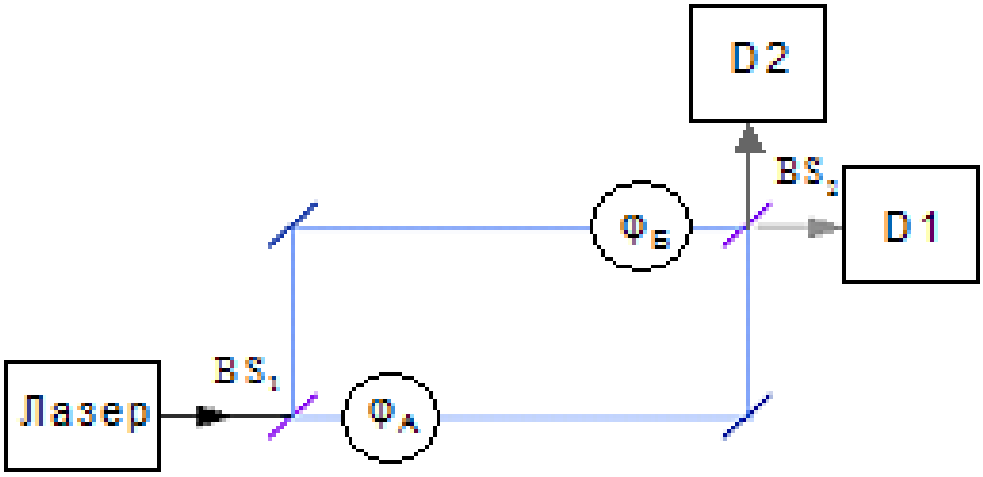

Рис. 1 Система фазового кодирования на одном интерферометре с отражателями.

Оптическое излучение лазера делится на два луча пластиной BS1, оба луча, пройдя через фазовые модуляторы $\varphi_А$ и $\varphi_Б$, интерферируют с помощью пластины BS2. В результате интерференции оптическое излучение поступает на детекторы D1 или D2 в зависимости от внесенной фазовыми модуляторами разности фаз.

Таким образом, практическая реализация схемы с фазовым кодированием на двух разбалансированных волоконно-оптических интерферометрах Маха-Цендера сталкивается с рядом серьезных проблем. Как показывают расчеты, для получения четкой интерференции на выходе системы, оба интерферометра должны быть идентичны с точностью до единиц микрометров. В такой системе будет возникать так же дрейф фазы, который необходимо свести к минимуму путем применения систем температурной стабилизации и компенсации набега фазы. Для приемлемой видности интерференции, расщепители излучения на входах и выходах интерферометра должны разделять интенсивность волны пополам. Из-за потерь при передаче информации и невозможности клонирования фотонов, волоконно-оптическая квантово-криптографическая система может оперировать только на ограниченных расстояниях.

В-третьих, у противника есть лучшая стратегия перехвата, чем простое угадывание базиса. Дело в том, что законы квантовой механики запрещают лишь идеальное клонирование квантовой системы, неидеальное клонирование при этом остается возможным. В настоящее время доказана теоретическая возможность успешного однократного копирования состояния квантовой системы с вероятностью успеха 5/6, а с ростом числа копий эта вероятность снижается до 2/3. Эксперименты по клонированию фотонов показывают результат, близкий к предсказанному теорией. Это дает противнику возможность копировать фотон и затем анализировать его поляризацию в двух различных базисах. Конечно, при этом будут возникать ошибки, но их уровень будет ниже, чем при простом угадывании базиса. И если базис окажется сопоставим с собственным фоном ошибок системы, прослушивание становится возможным. Поэтому в распоряжении противника всегда есть возможность перехватить какую-то часть передаваемых битов, замаскировав неизбежно сопровождающие такой перехват ошибки под собственные ошибки системы.

Для отсеивания собственных ошибок в реальных системах квантовой криптографии необходимо применять различные протоколы коррекции, а для снижения значимости перехваченных противником битов нужно использовать процедуру усиления секретности. Для этого проще всего вырабатывать несколько «слепков» ключа, а итоговый рабочий ключ получать простым побитовым суммированием по модулю 2 этих «слепков». Тогда, чтобы наверняка определить хотя бы один бит ключа, злоумышленнику нужно знать соответствующие биты во всех «слепках». Другой возможный способ заключается в том, чтобы вырабатывать ключи из сформированного битового вектора с помощью хэш-функций.

Заключение

Таким образом, в отличие от идеальных реальные системы квантовой коммуникации не способны обеспечить абсолютную секретность передаваемых данных. Это обусловлено наличием у них фона собственных ошибок, под которые можно замаскировать попытки перехвата, а также затуханием в каналах связи из-за необходимости использования многофотонных импульсов. Последнее делает возможным неразрушающий перехват данных и является практически неустранимым фактором, так как качество каналов не всегда поддается контролю, например в радиоканале между наземным центром управления и низкоорбитальным спутником.

Список литературы

1. Бауместер Д., Экерт А., Цайлингер А. Физика квантовой информации. – М.: Постмаркет, 2003. – 253 с.
2. Bennett C.,Bessette F., Brassard G., Salvail L., Smolin J. Experimental Quantum Cryptography // J. of Cryptology, 1992. – № 5 – P. 356-353.
3. Tittel W., Brendel J., Gisin B., Herzog T., Zbinden H., Gisin N. Experimental demonstration of quantum correlations over more than 10 km // Phys. Rev. A., 1998.– V.57 – P. 3229-3232.

References

1. Baumester D., Jekert A., Cajlinger A. Fizika kvantovoj informacii. – M.: Postmarket, 2003. – 253 s.
2. Bennett C.,Bessette F., Brassard G., Salvail L., Smolin J. Experimental Quantum Cryptography // J. of Cryptology, 1992. – № 5 – P. 356-353.
3. Tittel W., Brendel J., Gisin B., Herzog T., Zbinden H., Gisin N. Experimental demonstration of quantum correlations over more than 10 km // Phys. Rev. A., 1998.– V.57 – P. 3229-3232.