DOI: 10.25586/RNU.V9187.18.11.P.83 УДК 535.14

**В.А. Минаев, А.В. Крупенин, И.Д. Королев,
Ю.В. Курочкин, А.К. Федоров**

ПОСТРОЕНИЕ КВАНТОВО-ЗАЩИЩЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ

Статья посвящена вопросам интеграции систем квантового распределения ключей и существующих сертифицированных систем шифрования. Рассматривается структурная схема системы квантовых коммуникаций, а также представлен краткий обзор полученных экспериментальных результатов по реализации квантово-защищенной передачи данных в оптоволоконных линиях связи.

Ключевые слова: *криптография, квантовое распределение ключей, квантовые вычисления, криптографическая защита информации.*

**V.A. Minaev, I.D. Korolev, A.V. Krupenin,
Yu.V. Kurochkin, A.K. Fedorov**

CREATION OF QUANTUM PROTECTED INFORMATION SYSTEMS

The article is devoted to the integration of quantum key distribution systems and existing certified encryption systems. The structural scheme of the quantum communication system is considered, and a brief review of the experimental results on the implementation of quantum-protected data transmission in fiber-optic communication lines is presented.

Keywords: *cryptography, quantum key distribution, quantum computing, cryptographic protection of information.*

Введение

Новое поколение вычислительных устройств – квантовых компьютеров [1] – ставит под угрозу возможность использования традиционных инструментов криптографической защиты информации.

С использованием квантового алгоритма Шора появилась возможность быстрого решения задач факторизации и дискретного логарифмирования, сложностью которых обеспечивается вычислительная стойкость распространенных криптографических алгоритмов для открытого распределения ключей и для электронно-цифровых подписей [2].

В свою очередь, квантовый алгоритм Гровера обеспечивает квадратичное ускорение в задачах поиска, что влияет на оценки стойкости симметричных криптографических алгоритмов с точки зрения атак полного перебора (brute-force attack) [3]. Задачей реализации квантового компьютера занимаются ведущие международные исследовательские центры.

Существует несколько подходов к построению квантово-защищенных информационных систем. Первый подход состоит в переходе на новый класс алгоритмов, не приводящих к экспоненциальному ускорению. Данная область называется постквантовой криптографией [4]. В настоящее время Национальным институтом стандартов и технологий США (NIST) проводится конкурс на новый стандарт алгоритмов для открытого распределения ключей и электронно-цифровой подписи [5].

Другим решением является использование технологии квантового распределения ключей. Данный подход основан на формировании у легитимных сторон коммуникаций – приемника и передатчика – симметричных ключей за счет обмена информацией, закодированной в квантовые состояния света (рис. 1). При этом конфиденциальность криптографических ключей гарантируется законами квантовой физики: невозможностью скопировать произвольное квантовое состояние и соотношением неопределенностей. Изучение протоколов и алгоритмов квантового распределения ключа представляет собой передовое направление в развитии систем и средств защиты информации [6].

Рис. 1. Структурная схема устройства квантовых коммуникаций

Однако применение таких систем на практике сталкивается с трудностями как технического, так и организационного плана. В частности, на сегодняшний день не разработана нормативно-правовая база для использования квантовых систем в качестве средств защиты информации.

Целью данной статьи является анализ возможности интеграции систем квантового распределения ключа в существующие российские стандартизированные криптографические средства. В ней рассматривается структурная схема системы квантовых коммуникаций, разработанной Российским квантовым центром. Представлен обзор экспериментальных результатов по реализации квантово-защищенной передачи данных в городских оптоволоконных линиях связи, в которых система квантового распределения ключей интегрирована в существующие решения для криптографической защиты информации.

Квантовое распределение ключей

Устройство, реализующее квантовое распределение ключей, условно можно разделить на две части: «квантовую» и «классическую». Структурная схема устройства представлена на рис. 1. Квантовая часть, которая в разрабатываемом устройстве называется блоком управления, отвечает за реализацию протокола квантового распределения ключа: реализует приготовление, передачу и измерение квантовых состояний света. Она использует известный протокол BB84 с обманными состояниями [7].

На рис. 2 представлена практическая реализация устройства в виде двух изделий размером 4U. Устройства соединяются выделенным оптоволоконным кабелем, по которому передатчик отправляет приемнику квантовые состояния фотонов с частотой 312,5 МГц (в перспективе планируется увеличение частоты до 1 ГГц), при этом допускается сбор линии из нескольких сегментов путем их коммутации. Для приготовления состояний фотонов используются сильно ослабленные лазерные импульсы. Протокол обменных состояний в зависимости от условий выбирает уровни сигнала, при которых вероятность нахождения фотона в импульсе составляет 0,01–0,4. Приемник производит измерение фотонов при помощи оптической схемы и детекторов одиночных фотонов, после чего состояния фотонов разрушаются. В результате работы устройства при потерях в линии 5 дБ, что соответствует 25 км, скорость генерации ключа составляет 10 кбит/с.

Рис. 2. Реализация устройства квантового распределения ключей

Классическая часть реализует набор алгоритмов для обработки квантовых ключей и их передачи потребителю. Обработка квантовых ключей состоит из нескольких этапов. На первом этапе происходит процедура согласования способов приготовления и измерения квантовых состояний, так называемая процедура просеивания. Затем происходит исправление ошибок, в результате которых корректируются возможные искажения, возникшие в процессе передачи битов ключа по квантовому каналу. В устройстве РКЦ исправление ошибок происходит с помощью процедуры, называемой слепым симметричным исправлением ошибок [8]. Данная процедура является наиболее эффективным способом исправления ошибок. Затем происходит определение параметров канала, дающее возможность оценить объем информации, который может получить потенциальный перехватчик. На этом этапе принимается решение о реальной конфиденциальности ключей.

На последнем этапе наблюдается усиление секретности: происходит сокращение размеров ключа так, чтобы потенциальная информация перехватчика о сокращенном ключе была исчезающе мала [9]. Важнейшим элементом обработки является обеспечение аутентификации коммуникации по классическому каналу.

В результате работы системы квантового распределения ключей легитимные стороны коммуникаций получают закрытые ключи для шифрования. У систем квантового распределения ключей существуют по крайней мере два технических ограничения.

Во-первых, эти системы требуют прямого соединения и выделенного оптического волокна без усилителей и повторителей.

Во-вторых, режимы с необходимой скоростью генерации ключей (10–100 кбит/с) достигаются на расстояниях, не превышающих 50–100 км.

Для передачи ключей потребителям реализован специальный API-протокол, основанный на технологии Thrift-API. Взаимодействие потребителя с квантовым устройством осуществляется посредством сети Ethernet. Для аутентификации пользователей и защиты канала связи применяется протокол SSL (TLSv1.2). Для предоставления квантовых ключей используется RPC-фреймворк Apache Thrift.

Интеграция квантового распределения ключей в средства криптографической защиты информации

На сегодняшний день наиболее эффективным техническим решением является работа квантовых устройств распределения ключей в составе существующих средств криптографической защиты информации (СКЗИ) (рис. 3).

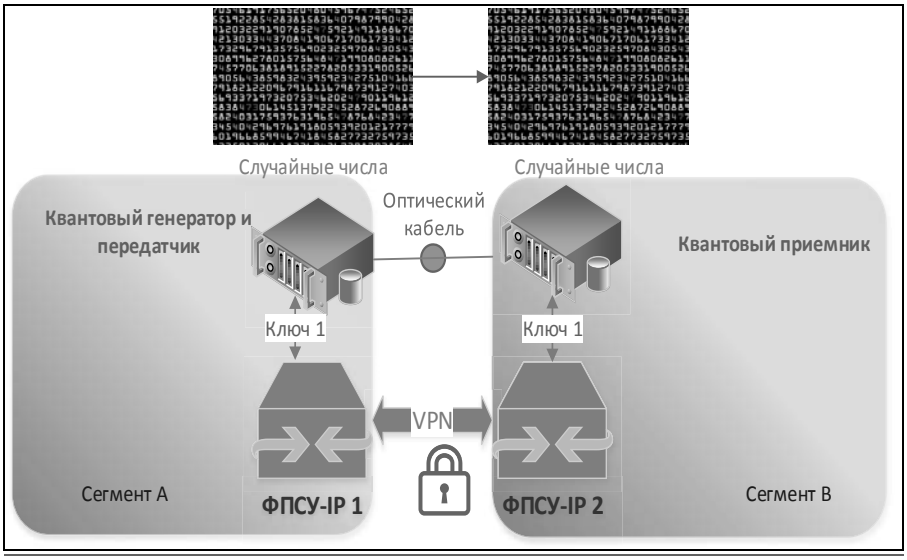

Рис. 3. Структурная схема квантово-защищенной передачи данных

Устройства РКЦ для квантового распределения ключей протестированы вместе с устройствами ФСПУ-IP «Амикон». Устройства ФСПУ-IP представляют собой функционально законченное решение, предназначенное для обеспечения приема и передачи любого вида информации (данных, речевой и др.) от абонентов защищаемой сети одного узла к абонентам защищаемой сети другого узла. В результате испытаний получены значения технических параметров и характеристик, представленных в таблице.

Результаты испытаний

Параметр/характеристика	Значение
Частота следования импульсов, МГц	3 125
Частота следования трейнов, кГц	0,8
Количество сигнальных импульсов, шт.	98 200
Количество синхроимпульсов, шт.	75 000
Мертвое время детекторов, мкс	5
Диапазон значений QBER, %	4,8–5,5 (при потерях 14 дБ)
Период запроса ключа, с	400
Объем запрашиваемого ключа, бит	256
Скорость генерации ключа, кбит/с	0,1

При передаче информации комплексы ФПСУ-IP обеспечивают шифрование, имитозащиту и фильтрацию передаваемых данных. При штатной работе ФПСУ-IP используют устройства квантового распределения ключей для получения от них сеансовых ключей шифрования (рис. 3). Эти устройства обеспечивают выработку симметричных последовательностей на двух сторонах с использованием оптической среды передачи данных.

Выводы

1. Являясь передовым решением в области защиты информации, системы квантового распределения ключа позволяют создавать абсолютную защиту от необнаруженного перехвата передаваемой информации, основанную на фундаментальных физических законах [10; 11].

2. Квантовое распределение ключа позволяет использовать абсолютно стойкие криптографические системы, стойкость которых не зависит от вычислительных ресурсов злоумышленника (включая квантовые компьютеры).

3. Перспективы широкого практического применения квантовых компьютеров требуют заблаговременного перехода всех критически важных систем защиты информации на системы с квантовым распределением ключа.

Литература

1. *Бауместер Д., Экерт А., Цайлингер А.* Физика квантовой информации. М.: Постмаркет, 2002. 376 с.

2. *Shor P.W.* Polynomial-time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer // SIAM Journal on Computing. 1997. Vol. 26. P. 1484–1509.

3. *Grover L.K.* A Fast Quantum Mechanical Algorithm for Database Search / Proceedings of 28th Annual ACM Symposium on the Theory of Computing. NY.: ACM Press, 1996. P. 212–219.

4. *Daniel J., Bernstein D., Lange T.* Post-quantum Cryptography – Dealing with the Fallout of Physics Success // Nature. 2017. Vol. 549. P. 188–194.

5. Information Technology Laboratory. URL: http://www.nist.gov. 24 мая 2018 г.

6. *Gisin N., Ribordy G., Tittel W., Zbinden H.* Quantum Cryptography // Review of Modern Physics. 2002. No 1. Vol. 74. P. 145–175.

7. *Bennett C.H., Brassard G.* Quantum Cryptography: Public Key Distribution and Coin Tossing // IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India (IEEE, New York, 1984). P. 175–179.

8. *Kiktenko E.O., Trushechkin A.S., Kurochkin Y.V., Fedorov A.K.* Post-processing procedure for industrial quantum key distribution systems // Journal of Physics: Conference Series. 2016. No 1. Vol. 741. 6 p.

9. *Kiktenko E.O., Trushechkin A.S., Lim C.C.W., Kurochkin Y.V., Fedorov A.K.* Symmetric Blind Information Reconciliation for Quantum Key Distribution // Physical Review Applied. 2017. Vol. 8. 12 p.

10. *Фисун А.П., Касилов А.Г., Фисенко В.Е., Минаев В.А., Афанасьев В.В., Митяев В.В., Фисун Р.А., Джевага К.А., Кожухов С.А.* Развитие методологических основ информатики и информационной безопасности систем. Депонированная рукопись. Орловский государственный университет. Номер 1165-В2004. ВИНИТИ. Дата депонирования 07.07.2004. 253 с.

11. *Минаев В.А.* Простые числа: новый взгляд на закономерности формирования: монография. М.: Издат. дом «Логос Пресс», 2011. 80 с.

References

1. *Baumester D., Ekert A., Tsaylinger A.* Fizika kvantovoy informatsii. M.: Postmarket, 2002. 376 s.

2. *Shor P.W.* Polynomial-time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer // SIAM Journal on Computing. 1997. Vol. 26. P. 1484–1509.

3. *Grover L.K.* A Fast Quantum Mechanical Algorithm for Database Search / Proceedings of 28th Annual ACM Symposium on the Theory of Computing. NY.: ACM Press, 1996. P. 212–219.

4. *Daniel J., Bernstein D., Lange T.* Post-quantum Cryptography – Dealing with the Fallout of Physics Success // Nature. 2017. Vol. 549. P. 188–194.

5. Information Technology Laboratory. URL: http://www.nist.gov. 24 maya 2018 g.

6. *Gisin N., Ribordy G., Tittel W., Zbinden H.* Quantum Cryptography // Review of Modern Physics. 2002. No 1. Vol. 74. P. 145–175.

7. *Bennett C.H., Brassard G.* Quantum Cryptography: Public Key Distribution and Coin Tossing // IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India (IEEE, New York, 1984). P. 175–179.

8. *Kiktenko E.O., Trushechkin A.S., Kurochkin Y.V., Fedorov A.K.* Post-processing procedure for industrial quantum key distribution systems // Journal of Physics: Conference Series. 2016. No 1. Vol. 741. 6 p.

9. *Kiktenko E.O., Trushechkin A.S., Lim C.C.W., Kurochkin Y.V., Fedorov A.K.* Symmetric Blind Information Reconciliation for Quantum Key Distribution // Physical Review Applied. 2017. Vol. 8. 12 p.

10. *Fisun A.P., Kasilov A.G., Fisenko V.E., Minaev V.A., Afanas'ev V.V., Mityaev V.V., Fisun R.A., Dzhevaga K.A., Kozhukhov S.A.* Razvitie metodologicheskikh osnov informatiki i informatsionnoy bezopasnosti sistem. Deponirovannaya rukopis'. Orlovskiy gosudarstvennyy universitet. Nomer 1165-B2004. VINITI. Data deponirovaniya 07.07.2004. 253 s.

11. *Minaev V.A.* Prostye chisla: novyy vzglyad na zakonomernosti formirovaniya: monografiya. M.: Izdat. dom "Logos Press", 2011. 80 s.