УДК 004.056.53

КВАНТОВОЕ РАСПРЕДЕЛЕНИЕ КЛЮЧЕЙ КАК ПЕРСПЕКТИВНЫЙ МЕТОД КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

В.В. Савчук
Учреждение образования «Гомельский государственный университет имени Франциска Скорины», г. Гомель, Республика Беларусь

Аннотация. В статье рассматривается квантовое распределение ключей (QKD) как перспективный метод криптографической защиты информации. Обоснована актуальность применения квантовой криптографии в условиях развития квантовых вычислений, способных снизить устойчивость классических алгоритмов. Описаны принципы работы QKD, включая использование кубитов и протокол BB84. Проанализированы основные преимущества метода, такие как независимость от вычислительных ресурсов и возможность обнаружения перехвата, а также ограничения, связанные с технической реализацией. Сделан вывод о высокой перспективности технологии для обеспечения безопасности передачи данных.
Ключевые слова: квантовая криптография; QKD; информационная безопасность; криптография; квантовые вычисления; протокол BB84; кубиты; защита информации; передача ключей; квантовые технологии

QUANTUM KEY DISTRIBUTION AS A PROMISING METHOD OF CRYPTOGRAPHIC INFORMATION SECURITY

V.V. Savchuk
Educational Institution "Francisk Skorina Gomel State University, Gomel", Republic of Belarus

Annotation. This article examines quantum key distribution (QKD) as a promising method of cryptographic information security. The relevance of applying quantum cryptography in the context of the development of quantum computing, which can reduce the stability of classical algorithms, is substantiated. The operating principles of QKD are described, including the use of qubits and the BB84 protocol. The main advantages of the method, such as independence from computing resources and the ability to detect interception, are analyzed, as well as the limitations associated with technical implementation. It is concluded that this technology has high potential for ensuring data transmission security.
Keywords: quantum cryptography; QKD; information security; cryptography; quantum computing; BB84 protocol; qubits; information security; key transfer; quantum technologies

Введение

Квантовая криптография – это наука о шифровании данных методами, основанными на законах квантовой механики. В отличие от традиционной криптографии, квантовое шифрование предполагает защиту и передачу данных при помощи физических свойств элементарных частиц [1]. Ключевым направлением квантовой криптографии является квантовое распределение ключей (QKD). Перспективность данного метода

обусловлена использованием квантового состояния частиц, изменение которых при измерении позволяет выявлять вмешательство третьей стороны при передаче информации.

Основная часть

Безопасность метода квантового распределения ключей обусловлена тем, что внешнее воздействие на квантовое состояние приводит к изменению передаваемых данных.

Передача информации осуществляется с использованием кубитов. Кубиты – квантовые аналоги классических битов. В отличие от обычного бита, принимающего значение 0 или 1, кубит может находиться в состоянии суперпозиции, при котором он может принимать значение 1 и 0 одновременно. Наглядный пример – подбрасывание монеты: после падения фиксируется один из двух состояний – «орел» или «решка», но в процессе движения невозможно однозначно определить исход, так как до момента наблюдения он не зафиксирован, можно сказать, что во время полета монета находиться в двух состояниях. Принцип суперпозиции кубита позволяет реализовать специальные способы кодирования, используемые в квантовых протоколах.

Наиболее известным протоколом квантового распределения ключей является BB84, предложенный Ч. Беннетом и Ж. Брассаром в 1984 году. В рамках данного протокола передающая сторона кодирует информацию в квантовых состояниях фотонов, используя два различных базиса. Принимающая сторона выполняет измерения, случайным образом выбирая базис измерения для каждого фотона. После передачи участники по открытому каналу обмениваются информацией о выбранных базисах и оставляют только те биты, для которых базисы совпали. Полученная последовательность используется для формирования секретного ключа. Вмешательство третьего лица в процессе передачи приводит к увеличению уровня ошибок в полученных данных. Если количество ошибок превышает допустимое значение, передача признается ненадежной, а сформированный ключ не используется. Таким образом, протокол BB84 позволяет не только передавать ключ, но и контролировать безопасность канала связи [2].

Квантовое распределение ключей обладает рядом принципиальных преимуществ по сравнению с классическими методами криптографической защиты информации.

Во-первых, безопасность QKD не зависит от сложности математических задач, следовательно и от вычислительных возможностей нарушителя. В классической криптографии устойчивость алгоритмов может снижаться с ростом вычислительной мощности, тогда как

в квантовых системах защита основана на физических свойствах квантовых состояний, которые невозможно измерить без их изменения.

Во-вторых, QKD обеспечивает встроенный механизм обнаружения перехвата. Любое вмешательство в процесс передачи приводит к появлению ошибок в ключе, что позволяет сторонам обмена выявить факт атаки до использования ключевой информации.

В-третьих, квантовое распределение ключей позволяет формировать секретные ключи с высокой степенью доверия, потому что их безопасность может быть проверена в процессе передачи. Это особенно важно для систем, в которых критична защита каналов связи, включая государственные, финансовые и корпоративные сети.

Основной из проблем является высокая стоимость оборудования, включающего источники фотонов, детекторы и специализированные каналы связи. Существенным ограничением также является дальность передачи, поскольку потери сигнала в каналах связи снижают эффективность системы и усложняют ее интеграцию в существующую инфраструктуру. Дополнительные сложности связаны с требованиями к условиям функционирования квантовых систем: для сохранения стабильности квантовых состояний необходимо поддерживать строго контролируемые параметры среды, включая сверхнизкие температуры и защиту от внешних воздействий, так как любые помехи могут приводить к декогеренции. Кроме того, QKD используется совместно с классическими криптографическими алгоритмами и требует адаптации существующих систем информационной безопасности.

Заключение

Несмотря на существующие технические ограничения, технология имеет высокий потенциал практического применения. В перспективе развитие квантовых технологий и снижение стоимости оборудования будут способствовать более широкому внедрению QKD в системы защиты информации.

Квантовое распределение ключей – перспективное направление развития криптографической защиты информации, обеспечивающее высокий уровень безопасности за счет законов квантовой механики. В отличие от классических методов, QKD позволяет обнаруживать попытки перехвата и не зависит от вычислительных возможностей нарушителя, что делает его устойчивым к угрозам, связанным с развитием квантовых вычислений.

Список использованных источников

1. Что такое квантовая криптография. [Электронный ресурс] // Kaspersky Encyclopedia: Глоссарий. – URL: https://encyclopedia.kaspersky.ru/glossary/quantum-cryptography/. – Дата доступа: 15.03.2026.

2. Принципы работы некоторых квантовых протоколов шифрования. [Электронный ресурс] // Habr: Песочница. – URL: https://habr.com/ru/sandbox/163613/. – Дата доступа: 15.03.2026.

References

1. What is quantum cryptography [Electronic resource] // Kaspersky Encyclopedia: Glossary. – URL: https://encyclopedia.kaspersky.ru/glossary/quantum-cryptography/. – Access date: 03/15/2026.

2. Principles of operation of some quantum encryption protocols. [Electronic resource] // Habr: Sandbox. – URL: https://habr.com/ru/sandbox/163613 /. – Access date: 15.03.2026.

Сведения об авторах

Савчук В.В., студентка факультета физики и информационных технологий, специальности «Кибербезопасность», учреждение образования «Гомельский государственный университет имени Франциска Скорины», barbarasavchuk007@gmail.com.

Васькевич В.В., старший преподаватель кафедры радиофизики и электроники, учреждение образования «Гомельский государственный университет имени Франциска Скорины», vaskevich@gsu.by

Information about the authors

Savchuk V., student of the Faculty of Physics and Information Technology, specialty "Cybersecurity", Educational Institution "Francisk Skorina Gomel State University, Gomel", barbarasavchuk007@gmail.com

Vaskevich V., Senior Lecturer at the Department of Radiophysics and Electronics, Educational Institution "Francisk Skorina Gomel State University, Gomel", vaskevich@gsu.by