УДК 535.14

КВАНТОВОЕ РАСПРЕДЕЛЕНИЕ КЛЮЧЕЙ

Марчук А.А., студентка гр. 914302

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Пухир Г.А. – ст. преподаватель

Аннотация. Рассматриваются причины возникновения квантовой криптографии, технология квантовой криптографии. Приводится обоснование применения алгоритмов шифрования на основе квантового распределения ключей. Выделяются проблемы квантовой криптографии.

Ключевые слова. Ключ шифрования, квантовая криптография.

История квантовой криптографии началась не с технологий связи, а с попытки решить совершенно другую задачу – создать деньги, которые невозможно подделать. Стивен Визнер из Колумбийского университета в 1983 году предложил создать квантовые банкноты государственного образца, которые нельзя скопировать даже в том случае, если у желающего сделать это есть типографское оборудование и бумага, при помощи которых изготавливался оригинал. Вероятность изготовления точной копии оригинала, защищенного квантовыми технологиями, стремится к нулю.

В криптографии, шифрование является процессом преобразования информации в шифротекст с помощью ключей. Этот процесс преобразует исходное представление информации, известное как открытый текст, в альтернативную форму, известную как зашифрованный текст. В идеале только авторизованные стороны могут расшифровать зашифрованный текст обратно в открытый и получить доступ к исходной информации. Шифрование само по себе не предотвращает возможность перехвата информации, но не позволяет потенциальному перехватчику получить доступное содержимое. Среди этапов практически любого алгоритма шифрования наиболее уязвимым считается этап распределения ключей. В большинстве стандартных подходов проблема решается с помощью инфраструктуры открытых ключей, однако это усложняет сам процесс шифрования и предъявляет повышенные требования к условиям его реализации.

Технология квантового распределения криптографических ключей решает одну из основных задач криптографии – гарантированное на уровне фундаментальных законов природы распределение ключей между удаленными пользователями по открытым каналам связи. Криптографический ключ – это числовая последовательность определенной длины, созданная для шифрования информации. Квантовая криптография позволяет обеспечить постоянную и автоматическую смену ключей при передаче каждого сообщения в режиме одноразового «шифроблокнота»: на сегодняшний день это единственный вид шифрования со строго доказанной криптографической стойкостью.

Чтобы скопировать банкноту, фальшивомонетчик должен измерить поляризации фотонов, но он не знает, в каком базисе поляризован каждый из них (эту информацию, как и параметры поляризации, банк держит в секрете, и только он знает, какие поляризации соответствуют номеру банкноты). Преступник может выбирать базисы случайным образом, и тогда у него есть некоторые шансы на успех, правда, очень небольшие. Но они становятся ничтожными, если создать фотонные ловушки: например, увеличить число фотонов на каждой банкноте (вероятность угадать снижается как обратная степенная функция от числа фотонов). Если каждый денежный знак снабдить десятком ловушек, вероятность успешной подделки падает почти до нуля.

Ограничениями первых реализаций квантовых систем шифрования были небольшая дальность передачи и очень низкая скорость. Еще одна проблема квантовой криптографии – это необходимость создания прямого соединения между абонентами, ведь только такой способ взаимодействия позволяет организовать защищенное распределение ключей шифрования. Стоимость квантовых систем на сегодняшний день составляет десятки и сотни тысяч долларов, так что разработчики коммерческих решений предлагают технологию квантового распределения ключей в виде сервиса, ведь большую часть времени оптические каналы простаивают.

UDC 535.14

QUANTUM KEY DISTRIBUTION

Marchuk A.A, Student of the group 914302

Belarusian State University of Informatics and Radioelectronics
Minsk, Republic of Belarus

Puhir G.A. – Senior Lecturer

Annotation. The reasons for the emergence of quantum cryptography, the technology of quantum cryptography are considered. The substantiation of the application of encryption algorithms based on quantum key distribution is given. The problems of quantum cryptography are highlighted.

Keywords. Encryption key, quantum cryptography.