Иванов Павел Александрович,
ЧГУ им. Ульянова 2 курс магистратуры,
г.Чебоксары, Чувашская Республика

КВАНТОВАЯ КРИПТОГРАФИЯ

Квантовая криптография – метод защиты коммуникаций, основанный на принципах квантовой физики. В отличие от традиционной криптографии, которая использует математические методы, чтобы обеспечить секретность информации, квантовая криптография сосредоточена на физике, рассматривая случаи, когда информация переносится с помощью объектов квантовой механики. Процесс отправки и приёма информации всегда выполняется физическими средствами, например, при помощи электронов в электрическом токе, или фотонов в линиях волоконно-оптической связи. Подслушивание может рассматриваться как изменение определённых параметров физических объектов - в данном случае, переносчиков информации.

Схема практической реализации квантовой криптографии показана на рисунке 1. Передающая сторона находится слева, а принимающая - справа. Ячейки Покеля необходимы для импульсной вариации поляризации потока квантов передатчиком и для анализа импульсов поляризации приемником. Передатчик может формировать одно из четырех состояний поляризации. Передаваемые данные поступают в виде управляющих сигналов на эти ячейки. В качестве канала передачи данных может быть использовано оптоволокно. В качестве первичного источника света можно использовать и лазер.

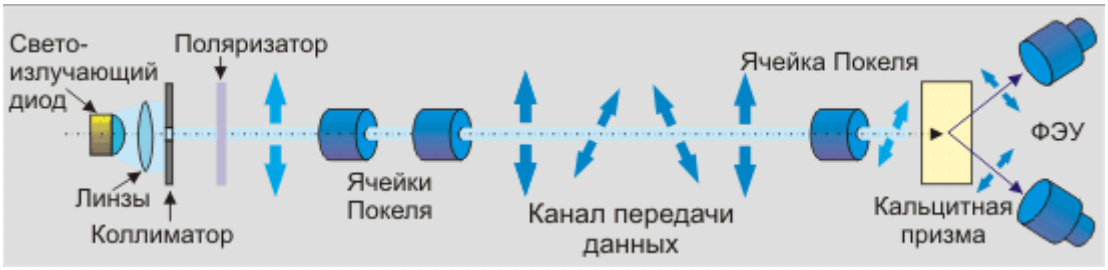

Рис. 1. **Схема практической реализации квантовой криптографии**

На принимающей стороне после ячейки Покеля установлена кальцитовая призма, которая расщепляет пучок на два фотодетектора (ФЭУ), измеряющие две ортогональные составляющие поляризации. При формировании передаваемых импульсов квантов возникает проблема их интенсивности, которую необходимо решать. Если квантов в импульсе 1000, есть вероятность, что 100 квантов по пути будет отведено злоумышленником на свой приемник. В последующем, анализируя открытые переговоры между передающей и принимающей стороной, он может получить нужную ему информацию. Поэтому в идеале число квантов в импульсе должно быть около одного. В этом случае любая попытка отвода части квантов злоумышленником приведет к существенному изменению всей системы в целом и, как следствие, росту числа ошибок у принимающей стороны. В подобной ситуации принятые данные должны быть отброшены, а попытка передачи повторена. Но, делая канал более устойчивым к перехвату, специалисты сталкиваются с проблемой "темнового" шума (получение сигнала, который не был отправлен передающей стороной, принимающей стороной) приемника, чувствительность которого повышена до максимума. Для того, чтобы обеспечить надежную передачу данных, логическому нулю и единице могут соответствовать определенные последовательности состояний, допускающие коррекцию одинарных и даже кратных ошибок.

В МИРЕ ИССЛЕДОВАНИЙ

За последние 20 лет были достигнуты следующие результаты в области развития квантовой криптографии:

Один из первых лабораторных вариантов квантовой криптосистемы с использованием оптоволоконной линии связи длиной в 30 км был реализован в исследовательской лаборатории фирмы British Telecom (Великобритания) в 1995 г.

Результатом разработки швейцарских ученых в Женевском университете совместно с компанией SwissCom стала практическая реализация квантовой криптосистемы с длиной 23 км волоконно-оптического кабеля по дну Женевского озера между городами Нион и Женева.

В Лос-Аламосской национальной лаборатории (США) завершена разработка опытной линии связи общей длиной 48 км.

В 2004 году была создана первая локальная сеть с квантовой криптографической системой распределения ключей длиной в 10 км в Бостоне, использующей принцип фазового кодирования. Это совместный проект BBN Technologies, MIT, Harvard University, финансируемый правительственным агентством DARPA (Defense Advanced Research Projects Agency).

В Японии успешно реализовано объединение различных систем квантового распределения ключей, разработанных Mitsubishi Electric Corporation и NEC.

Продемонстрирована принципиальная возможность передачи однофотонных сигналов между наземной станцией и спутником, находящимся на околоземной орбите (1600 км).

Европейская программа в области квантовой криптографии SECOQC (Secure Communications based on Quantum Cryptography) стартовала в 2004 г. В результате была продемонстрирована квантовая

сеть, отдельные ветви которой работали по нескольким популярным протоколам квантового распределения ключей. В Европейском союзе достигнуто лидерство в системах квантовой криптографии при передаче ключей через открытое пространство. Рекорд составляет 144 км по дальности, что превышает рекорд для оптоволоконных систем квантовой криптографии в 120 км. Конечной целью работы является создание квантовой криптографической системы передачи ключей через низкоорбитальные спутники.

Таким образом, исследования в области квантовой криптографии за последние годы перешли от чисто фундаментальных работ к практическим реализациям и первым коммерческим прототипам. Можно назвать такие компании как HYPERLINK "http://www.idquantique.com/)" \\t "_blank" Id Quantique, HYPERLINK "http://www.magiqtech.com/" \\t "_blank" MagiQ, HYPERLINK "http://smartquantum.co.uk/" \\t "_blank" Smart Quantum, которые предлагают либо готовые криптосистемы, либо сопутствующие компоненты, такие как генераторы случайных чисел, источники пар фотонов, однофотонные детекторы и др. К сожалению, фирмы не раскрывают рынок сбыта своей продукции, однако известно, что коммерческими системами квантового распределения ключей интересуются в первую очередь банки. Несомненно, что технологии квантовой коммуникации будут определять облик информационных технологий и систем защищенной передачи информации уже в ближайшем будущем.

Квантовая криптография еще не вышла на уровень практического использования, но приблизилась к нему. В мире существует несколько организаций, где ведутся активные исследования в области квантовой криптографии. Среди них IBM, GAP-Optique, Mitsubishi, Toshiba, Нацио-

нальная лаборатория в Лос-Аламосе, Калифорнийский технологический институт (Caltech), а также молодая компания MagiQ и холдинг QinetiQ, поддерживаемый британским министерством обороны. Диапазон участников охватывает как крупнейшие мировые институты, так и небольшие начинающие компании, что позволяет говорить о начальном периоде в формировании рыночного сегмента, когда в нем на равных могут участвовать и те, и другие.

Конечно же, квантовое направление криптографическоӣ защиты информации очень перспективно, так как квантовые законы позволяют вывести методы защиты информации на качественно новый уровень. На сегодняшний день уже существует опыт по созданию и апробированию компьютернoӣ сети, защищенноӣ квантово-криптографичекими методами – единственноӣ в мире сети, которую невозможно взломать.Квантово-криптографические исследования развиваются быстрыми темпами. В ближайшем будущем методы защиты информации на основе квантовоӣ информации будут использоваться в первую очередь в сверхсекретных военных и коммерческих приложениях.