КВАНТОВОЕ РАСПРЕДЕЛЕНИЕ КЛЮЧЕВОЙ ИНФОРМАЦИИ В ПЕРСПЕКТИВНЫХ КРИПТОСИСТЕМАХ

В.Ф. Голиков, П.И. Махахей

В настоящее время ведутся интенсивные работы по созданию квантовых компьютеров, способных решать вычислительно трудоемкие задачи теории чисел. В перспективе окажется не защищенным основной алгоритм формирования общего ключа алгоритм Диффи–Хелманна. Квантовое распределение ключевой информации является альтернативным способом распределения ключей.

Из-за ограниченности возможностей по измерению квантовых систем, использовать квантовые способы передачи данных в целом невыгодно. Однако задействовать квантовый канал для согласования или распространения ключа между отправителем и получателем представляется разумным. Основные принципы квантовой механики, положенные в основу квантовой криптографии: невозможность различить абсолютно надежно два неортогональных квантовых состояния; запрет на клонирование; наличие перепутанных/запутанных квантовых состояний; причинность и суперпозиция.

К настоящему времени предложено и теоретически обосновано достаточно много различных протоколов квантового распределения ключа. Основными из них являются BB84, B92 и протокол Экерта.

Квантовое распределение ключа не устраняет необходимость в других криптографических примитивах, таких как аутентификация, но может быть использовано для построения систем с новыми свойствами безопасности.