ПОВЫШЕНИЕ ЭФФЕКТИВНОСТИ КВАНТОВОГО РАСПРЕДЕЛЕНИЯ КЛЮЧЕЙ

С.Г. Скобля, В.Ф. Голиков

Существенными недостатками современных симметричных и асимметричных криптографических систем являются: 1) возможность ретроспективного взлома; 2) отличная от нуля вероятность обнаружения алгоритмов быстрого вычисления односторонних функций, используемых в асимметричных системах; 3) незащищенность

перед алгоритмами взлома, разработанными для квантовых компьютеров. И если алгоритмы Гровера (для взлома DES) и Шора (для факторизации), разработанные для несуществующих пока квантовых компьютеров, никак не сказываются на степени взломостойкости информации, защищенной с помощью упомянутых систем, то два первых недостатка заставляют работать над поиском альтернативных решений уже сегодня.

Одной из перспективных альтернатив является квантовая криптография, а более конкретно — квантовое распределение ключей. В этом направлении сейчас ведутся интенсивные исследования, уже получены практические результаты, разработаны первые промышленные установки. Однако, имея очевидные преимущества перед конкурентами, системы квантового распределения ключей на современном этапе развития имеют и существенные недостатки, важнейший из которых — низкая эффективность распределения ключевой информации, которая выражается, главным образом, в низкой скорости генерации ключа и относительно небольших максимальных расстояниях передачи.

Изучение существующих протоколов квантового распределения ключей и принципов функционирования установок, в которых они реализованы, анализ причин, ограничивающих эффективность передачи ключевой информации, позволяет сделать вывод о том, что повышение эффективности подобных систем возможно. Основными перспективными направлениями исследований в этой области видятся: 1) улучшение аппаратной части, включающее усовершенствование оборудования и материалов, используемых в установках, в особенности — источников и приемников фотонов, оптоволокна; 2) разработка новых более эффективных протоколов передачи и совершенствование существующих протоколов (и, в частности, методов формирования окончательного ключа из "сырого"). В докладе рассматриваются возможности второго направления.