УДК 004.056.55

МОДЕЛИРОВАНИЕ АТАК НА ПРОТОКОЛЫ КВАНТОВОГО РАСПРЕДЕЛЕНИЯ КЛЮЧЕЙ

Коблов А.Ю. (Университет ИТМО, Санкт-Петербург)
Научный руководитель – к.т.н. Бибиков С.В.
(Университет ИТМО, Санкт-Петербург)

В работе представлено моделирование актуальных атак на различные протоколы квантового распределения ключей.

Введение. Взаимная информация при атаках на протоколы квантового распределения ключей является одним из показателей защищённости протоколов. Уровень взаимной информации можно использовать для оперативного контроля секретности сеанса передачи ключей. Это возможно за счёт вычисления статистики и определения количества информации, которую мог перехватить злоумышленник, для минимизации доли этой информации в финальном ключе.

Основная часть. Взаимная информация – мера, описывающая количество информации, содержащееся в одной случайной величине относительно другой. В теории связи взаимная информация используется для оценки потерь при передаче в канале с шумом. Так как в квантовой криптографии подслушивание вносит ошибки в процесс передачи, то можно говорить о том, сколько информации получил злоумышленник, внеся долю ошибок D. Данный метод определения защищённости достаточно прост и наиболее описан для различных протоколов КРК.

Ошибки в канале могут появляться как из-за прослушивания канала, так и из-за помех и затухания в канале. Технически невозможно определить, чем они были вызваны, поэтому все ошибки считаются последствиями прослушивания канала. Для протокола основными уязвимостями являются невозможность активного защиты от прослушивания, вследствие которого Ева может проводить измерения над кубитами, и невозможность создания строго однофотонных импульсов. Для генерации импульсов используют ослабленное лазерное излучение. Поэтому возможно появление многофотонных импульсов. Знание доли таких импульсов необходимо для определения вклада разных стратегий атакующего в общую взаимную информацию между Алисой и Евой.

Взаимная информация является одним из наиболее часто встречающихся критериев при описании атак на протоколы. Однако, протоколы BB84 и B92 сравнимы так как они имеют примерно одинаковую структуру, в то время как COW отличается по природе подготовки состояний и имеет отличные критерии, от которых зависит определение взаимной информации.

Выводы. В работе продемонстрированы актуальные атаки на протоколы квантового распределения ключей и составлена целевая функция для моделирования атак на однофотонные и многофотонные импульсы.

Коблов А.Ю.

Бибиков С.В.