ВЕРОЯТНОСТНАЯ МОДЕЛЬ ПЕРЕДАЧИ КЛЮЧЕВОЙ ИНФОРМАЦИИ В СИСТЕМЕ СО СЛУЧАЙНЫМ ПЕРЕКЛЮЧЕНИЕМ ПРИЕМО-ПЕРЕДАЮЩИХ БАЗИСОВ

В.Ф. Голиков, С.Г. Скобля

Одним из перспективных способов распределения криптографических ключей для симметричных криптосистем считается квантовая передача. Эффективность передачи криптографических ключей с помощью квантов света в настоящее время существенно зависит качества систем генерации, передачи и приема фотонов. Однако существенные резервы имеются и за счет оптимизации процедур формирования "сырого ключа" (ключа, содержащего ошибки) и устранения этих ошибок.

В докладе рассматривается гипотетическая модель передачи ключевой информации в системе со случайным переключением приемо-передающих базисов. Такая модель имитирует статистические процессы и является полезной для оценки эффективности передачи ключа. Постановка задачи следующая. Пусть имеется объект A которому необходимо передать некую двоичную последовательность K_j, где $j=\overline{1,n}$, n — длина последовательности, например, ключевую информацию, по открытому каналу связи объекту B. Злоумышленник C имеет возможность подключиться к этому каналу и перехватывать передаваемую информацию, анализировать ее и возвращать либо в неизменном виде, либо в искаженном обратно в канал связи. Будем считать, что передатчик объекта A генерирует физические сигналы, параметры которых зависят от того в каком состоянии (режиме) находится передатчик. Для управления состояниями передатчика A вырабатывается случайная последовательность чисел R_i, где i=1, 2. Пусть распределение вероятностей R_i — равномерное, т.е. каждый режим равновероятен P_i=0,5. Физический сигнал, сформированный в i-м режиме модулируется битами двоичной случайной последовательности (той последовательности, которую A должен передать B). По аналогии с квантовой технологией в i-й режим работы передатчика, в котором сформирован физический сигнал, переносящий "1" или "0", будем называть i-м базисом. Если базисы передатчика A и приемника B при передаче j-го бита совпадают, то он принимается правильно, если базисы противоположны, то независимо от передаваемого бита принимается либо "1", либо "0" с одинаковыми вероятностями. Будем считать, что злоумышленник C обладает техническими возможностями перехватывать передаваемые сигналы при этом, если базис C совпадает с базисом передатчика A, то передаваемый бит принимается C правильно, если базисы A и C противоположны, принятый бит равновероятно может оказаться равным "1" или "0". Принятый C бит (правильный или неправильный) возвращается в канал связи и достигает приемника B, который принимает его по описанному ранее алгоритму. При этом C может передавать возвращаемый бит в том же базисе, в котором он был принят им от A или в противоположном.

Для сформулированных исходных данных построен граф передачи K_j и получено выражение для вероятности правильной передачи K_j.