УДК 621.391.25

Моделирование процесса идентификации бинарных последовательностей по выборкам ограниченного объема

Абдольванд Ф., Голиков В.Ф.
Белорусский национальный технический университет

При решении некоторых задач криптографической защиты информации возникает необходимость оценивать степень близости двоичных последовательностей, сохраняя при этом конфиденциальность последних. Например, при формировании общего ключа симметричной криптосистемы с использованием квантового канала передачи информации после окончания сеанса передачи одиночных поляризованных фотонов от абонента А к абоненту В и удаления из ключевой последовательности бит, принятых в несогласованных базисах, оставшаяся часть последовательности (сырой ключ) проверяется на наличие отличий. Эти отличия носят случайный характер и возникают вследствие шумовых эффектов в канале связи или в результате «прослушивания» квантового канала злоумышленником. В этом случае возникшие отличия можно считать ошибками, считая двоичную последовательность А правильной, а последовательность В искаженной. Необходимость определения уровня ошибок возникает с одной стороны для обнаружения факта «прослушивания» квантового канала, с другой для принятия решения о целесообразности дальнейшей процедуры согласования последовательностей. Действительно, при «прослушивании» канала злоумышленник узнает некоторую часть будущего криптографического ключа, но при этом вносит дополнительные ошибки в передаваемую последовательность. Поэтому при обнаружении факта прослушивания сеанс формирования общего ключа может быть отменен. Кроме того, сеанс формирования общего ключа может закончиться неудачей и при отсутствии прослушивания, если уровень ошибок по естественным причинам достаточно высок. Устранение ошибок (согласование последовательностей) сопровождается уменьшением конфиденциальности общего ключа, которое тем больше, чем больше уровень ошибок.

Предложенный способ идентификации двоичных последовательностей с использованием процедуры выборочного контроля по альтернативному признаку позволяет достаточно эффективно решать задачу при умеренных потерях конфиденциальности элементов последовательностей и может с успехом использоваться для формирования общего ключа симметричных криптосистем.