УСТРАНЕНИЕ ОШИБОК В БИНАРНЫХ КЛЮЧЕВЫХ ПОСЛЕДОВАТЕЛЬНОСТЯХ ПРИ РАЗНЕСЕННОМ ФОРМИРОВАНИИ КЛЮЧА

В.Ф. Голиков, Ф. Абдольванд

Важной задачей, которую необходимо решать для обеспечения надежной работы симметричной криптосистемы, является задача формирования абонентами системы общего секретного ключа. Для ее решения уже длительное время с успехом используется алгоритм открытого распределения ключей Диффи–Хеллмана или аналогичные процедуры, базирующиеся на использовании односторонних функций. Однако развитие физики, электроники, математики и информатики сделало вполне реальным появление в ближайшем будущем квантового компьютера, одним из возможных применений которого является "взлом" традиционных односторонних функций с последующим вычислением общего ключа, формируемого по схеме Диффи–Хеллмана. в [1] рассматриваются альтернативные способы формирования общего ключа без использования классических однонаправленных функций. Суть этих методов сводится к формированию у абонентов криптосистемы бинарных последовательностей,

идентичность которых обеспечивается тем или иным способом. Независимо от способа обеспечения идентичности при этом возникает необходимость устранения различий (ошибок) последовательностей, процент которых зависит от выбранного способа формирования общего ключа. В докладе анализируются известные методы устранения ошибок с учетом потерь конфиденциальности, а также излагается новый подход эффективный для случая большого процента ошибок.

Литература

1. Голиков В.Ф., Абдольванд Ф. // 14-я Междунар. конф. "Комплексная защита информации". Могилев, 2009.