КВАНТОВАЯ СИСТЕМА ФОРМИРОВАНИЯ КЛЮЧЕВЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ В УСЛОВИЯХ ПРОСЛУШИВАНИЯ

Н.В. ПЕНКРАТ, В.Ф. ГОЛИКОВ

Информация сегодня — самый ценный товар, поэтому обеспечение ее конфиденциальности, целостности и доступности чрезвычайно актуально. Для достижения вышеуказанной цели применяются методы криптографии. В отличие от традиционной криптографии, квантовая криптография использует явления квантовой физики. Квантовая физика угрожает раскрытием классических шифров, переведя экспоненциальные задачи в разряд задач, решаемых за полиномиальное время. Однако она позволяет создавать принципиально новые криптографические системы.

Известные протоколы формирования криптографического ключа с помощью квантового канала отменяют сеансы формирования при прослушивании квантового канала криптоаналитиком из-за большого процента ошибок, а также того, что криптоаналитик сможет сформировать свою последовательность, в которой 62% бит совпадет с формируемым ключом. В докладе предлагается протокол использования квантового канала, позволяющий формировать ключ в условиях прослушивания. Протокол основан на комбинировании числа оглашаемых и не оглашаемых базисов в сеансе формирования. Показано, что при определенной пропорции оглашаемых и не оглашаемых базисов удается добиться некритичного в смысле потерь конфиденциальности ключа при приемлемом уровне ошибок. Ошибки в дальнейшем устраняются по методу согласования слабосовпадающих бинарных последовательностей [1], а уровень конфиденциальности восстанавливается путем известной процедуры повышения секретности [2].

Дальнейшие исследования, проведенные с помощью имитационной модели согласования ключевой информации в условиях прослушивания, показали, что процент оглашаемых базисов не оказывает решающее влияние на количество известных злоумышленнику бит. Минимальный процент известных злоумышленнику бит во многом определяется характером расположения скомпрометированных бит в переданном ключе. Однако использование процедуры усиления секретности обеспечивает случайность местоположения скомпрометированных бит, поэтому ключи, передаваемые с помощью разработанного алгоритма, целесообразно использовать при блочном шифровании.

Литература

1. *Голиков В.Ф., Абдольванд Ф.* // Докл. БГУИР. 2010. № 6.
2. *Экерт А. и др.* Физика квантовой информации. М, 2002.