УДК 004.41.42

В. Б. Кимсо, магистрант; Н. В. Пацей, доц., канд. тех. наук
(БГТУ, г. Минск)

КВАНТОВОЕ КРИПТОГРАФИЧЕСКОЕ ХЭШИРОВАНИЕ ИНФОРМАЦИИ

В квантовой криптографии можно выделить два базовых направления. Первое - базируется на кодировании квантового состояния одиночной частицы и основано на невозможности различить абсолютно надежно два неортогональных квантовых состояния. Произвольное состояние любой двухуровневой квантово-механической системы представляется в виде линейной суперпозиции $|\Psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$, с состояниями $|0\rangle$и $|1\rangle$ и комплексными коэффициентами α и β, причем должно выполняться соотношение $|\alpha|^2 + |\beta|^2 = 1$. Защищенность данного метода основывается на теореме о запрете клонирования неизвестного квантового состояния. Благодаря унитарности и линейности квантовой механики, невозможно создать точную копию неизвестного квантового состояния без воздействия на исходное состояние.

Второе направление развития основано на эффекте квантового перепутывания (запутывания). Две квантово-механические системы(в том числе разделенные в пространстве) могут находиться в состоянии корреляции, так что измерение выбранной величины, осуществляемое над одной из систем, определит результат измерения этой величины на другой. Таким образом, ни одна из запутанных систем не может находиться в определенном состоянии. А следовательно, запутанное состояние не может быть записано как прямое произведение состояний систем. Состояние двух частиц со спином 1/2 может служить примером запутанного состояния:

$$|\Psi_0\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}}.$$

Измерение дает с равной вероятностью состояния $|0\rangle$ или $|1\rangle$. Состояние другой подсистемы должно быть противоположным.

Базовым протоколом квантового распределения на основе эффекта квантового запутывания является протокол EPR (Einstein-Podolsky-Rosen). Существует множество других протоколов квантовой криптографии основанных на передаче информации посредством кодирования в состояниях одиночных фотонов: BB84, B92, BB84(4+2), Гольденберга- Вайдмана, Коаши-Имотои их модификации.