Ф. К. Алиев, А. М. Бородин (Москва, ТВП). **О возможности применения квантового механизма телепортации для представления произвольной двоичной последовательности в виде суммы двух случайных равновероятных двоичных последовательностей.**

При разработке систем защиты информации часто возникает необходимость решения следующей задачи [2].

Дана двоичная последовательность $m = (m_1, m_2, \ldots, m_L)$. Требуется представить m в виде суммы двух случайных равновероятных последовательностей a и b длины L: $m = a \oplus b$, $a = (a_1, a_2, \ldots, a_L)$, $b = (b_1, b_2, \ldots, b_L)$, $m_i = a_i \oplus b_i = (a_i + b_i) \pmod 2$, $i = 1, 2, \ldots, L$.

Сформулированная задача может быть эффективно решена с привлечением квантового ресурса несепарабельных состояний квантовых систем, задействованного в виде квантового механизма телепортации [1].

Пусть значение 0 закодировано состоянием кубита $|0\rangle$, а значение 1 закодировано состоянием кубита $|1\rangle$. Пусть сгенерировано L пар кубитов A_iB_i $(i = 1, 2, \ldots, L)$ в состоянии Белла $(|00\rangle + |11\rangle)/\sqrt{2}$ [1]. Для кодирования значения каждого элемента m_i последовательности m используется отдельный кубит C_i, $i = 1, 2, \ldots, L$. Далее для вычисления элементов a_i и b_i $(i = 1, 2, \ldots, L)$ последовательностей a и b соответственно осуществляются следующие действия.

Шаг 1. Кубит C_i приготавливается в состоянии $|m_i\rangle$.

Шаг 2. Кубит C_i приводится во взаимодействие с кубитом A_i.

Шаг 3. К кубитам C_i и A_i применяется квантовый элемент CNOT [1].

Шаг 4. К кубиту C_i применяется квантовый элемент Адамара H [1].

Шаг 5. Над кубитами C_i и A_i, составляющими двухкубитную квантовую систему, выполняется измерение в базисе из векторов $|00\rangle$, $|01\rangle$, $10\rangle$ и $|11\rangle$. Результатом измерения может быть с вероятностью 0,25 одно из этих состояний.

Если в результате измерения получено $|00\rangle$ или $|10\rangle$, то полагается $a_i = 0$, в противном случае полагается $a_i = 1$.

Шаг 6. Выполняется измерение над кубитом B_i в базисе из векторов $|0\rangle$ и $|1\rangle$. Результатом измерения может быть с вероятностью 0,5 одно из этих состояний.

Если в результате измерения получено $|0\rangle$, то полагается $b_i = 0$, в противном случае полагается $b_i = 1$.

СПИСОК ЛИТЕРАТУРЫ

1. *Нильсен М., Чанг И.* Квантовые вычисления и квантовая информация. М.: Мир, 2006, 824 с.
2. *Шнайер Б.* Прикладная криптография. М.: Триумф, 2003, 816 с.