УДК 519.217.2 519.857.3 336.717

Старобогатов Р. О. к. ф.-м. н., доц., СПбГИЭУ; e-mail: rstarobogatov@gmail.com

Квантовый криптографический протокол платежей.

Квантовый протокол базируется на суперпозиции диаграмм, кодирующих последовательности полиномов. Создание квантовых денег начинается со стохастической суперпозиции:

$$|initial\rangle = \frac{1}{\sqrt{|B|}} \sum_{e \in B} |e\rangle|0\rangle \qquad (1)$$

Здесь B – ряд случайных чисел. Затем, функцией f→f(e) получают состояние:

$$\frac{1}{\sqrt{|B|}} \sum_{e \in B} |e\rangle|(\mathrm{f(e)}\rangle \qquad (2)$$

В итоге, монетный двор создает квантовую денежную меру стоимости f. Если результатом измерения является v, то результирующее состояние равно

$$|\$_v\rangle|v\rangle = \frac{1}{\sqrt{N_v}} \sum_{e \in B} |e\rangle|v\rangle \qquad (3)$$

Квантовые деньги представляют собой классический номер v и квантовое состояние \$. Квантовый алгоритм их верификации использует классические цепи Маркова. Измеряемая производителем квантовых денег функция f является полиномом Александера ориентированной цепи, представленной решеточной диаграммой. Процедура проверки основана на преобразованиях Редемейстера, не изменяющих значение полинома. Полином Александера вычисляется по ориентированной цепи и будет инвариантен относительно преобразований Редемейстера. Полином Александера определяется списком коэффициентов, а не значением. При создании квантовых денег сначала выбирают параметр безопасности D и определяют

соответствующее распределение[1-2,4]. Затем производитель использует алгоритм подготовки состояния

$$\sum_{d=2}^{2\overline{D}} d!\sqrt{q(d)}\left|d\right\rangle \tag{4}$$

Используя прямую единичную трансформацию, воздействуя на это состояние и на дополнительную запись, производитель получает

$$\sum_{d=2}^{2\overline{D}} d!\sqrt{q(d)}\left|d\right\rangle\left(\frac{1}{d!}\sum_{\pi_X,\pi_0\in S_d}\left|\pi_X,\pi_0\right\rangle\right) \tag{5}$$

и затем проверяет, являются ли 2 перестановки π_X,π_O несовместными (они являются несовместными с вероятностью, близкой к *1/e*). Если производитель получает несовместный результат измерения, он пересчитывает измерение *d* в первой записи для получения исходного состояния $\left|initial\right\rangle$ в последних двух записях, где

$$\left|initial\right\rangle=\frac{1}{\sqrt{N}}\sum_{\substack{grid\\diagrams\\G}}\sqrt{q(d(G))}\left|G\right\rangle \tag{6}$$

а *N* – нормализующая константа. Если результат измерения не может быть определен, нужно начинать вычисления заново. Распределение *q(d)* выбирают таким образом, что если нужно измерить *d(G)* на $\left|initial\right\rangle$, то тогда распределение результатов будет очень сильно приближенным к распределению Гаусса, что означает, что *D* ограничено границами интервала $\left[2,2\overline{D}\right]$. При увеличении *D*, недостающий вес в отклонении стремится к нулю. Из состояния $\left|initial\right\rangle$, производитель вычисляет полином Александера *A(G)* для другой записи, и затем измеряет эту запись, получая полиномиальное *p*. Результирующее состояние $\left|\$_p\right\rangle$, суперпозиция всех решеточных диаграмм (включая *2D* размерности) с полиномом Александера *p*

$$\left|\$_p\right\rangle=\frac{1}{\sqrt{N}}\sum_{G:A(G)=p}\sqrt{q(d(G))}\left|G\right\rangle \tag{7}$$

где N отвечает за нормализацию. Квантовые деньги состоят из состояния $|\$_p\rangle$, и серийного номера, которым является полиномиальное p, представленное списком коэффициентов. Если полиномиальное p равно 0, то производитель должен начать создавать состояние заново[3-5]. Проверка квантовых платежей возможна различными способами. Если вам передают квантовое состояние $|\phi\rangle$ и серийный номер, который соответствует полиномиальному числу p, и уверяют вас, что это подлинный квантовый платеж. Чтобы удостовериться в подлинности в этом случае, можно использовать описанный [5,9] алгоритм проверки. Такая процедура будет определять подлинные квантовые состояния с высокой вероятностью, а другие состояния, которые могут пройти проверку, крайне трудно создать. Состояния же для квантовых денег можно создать, и они проходят проверку подлинности с высокой вероятностью. Квантовые деньги практически невозможно подделать.

Литература

1. Нильсен М., Чанг М. Квантовые вычисления и квантовая информация. М.: Мир, 2006.
2. Балонишников А. М., Старобогатов Р.О. Квантовые модели безопасных протоколов // Вестник ИНЖЭКОНА, серия: технические науки, 2011, Вып.8(51), с.17-26.
3. Старобогатов Р.О. Квантовые протоколы платежей // Вестник ИНЖЭКОНА, серия: экономические науки,2011, в.3(46), с.138-143.
4. Aaronson S., Christiano P. Quantum Money from Hidden Subspaces. *http://arxiv.org/pdf/1203.4740.pdf* (дата обращения 01.8.12)
5. Molina A., Vidick T., Watrous J. Optimal counterfeiting attacks and generalizations for Wiesner's quantum money http://arxiv.org/pdf/1202.4010v1.pdf (дата обращения 02.8.12)

6. Farhi E. et al.// Quantum money from knots. http://arxiv.org/pdf/1004.5127v1.pdf (дата обращения 02.8.12)

http://www.nlr.ru/index.html (дата обращения: 20.02.2007)

Логинова Л. Г. Сущность результата дополнительного образования детей // Образование: исследовано в мире: междунар. науч. пед. интернет-журн. 21.10.03. URL: http://www.oim.ru/reader.asp?nomer=366 (дата обращения: 17.04.07).