УЧЕНЫЕ ЗАПИСКИ КАЗАНСКОГО УНИВЕРСИТЕТА
Том 156, кн. 3 Физико-математические науки *2014*

УДК 519.71

УНИВЕРСАЛЬНОЕ КВАНТОВОЕ ХЕШИРОВАНИЕ

Ф.М. Аблаев, М.Ф. Аблаев, А.В. Васильев

Аннотация

Предложен метод квантового хеширования, комбинирующий известные конструкции универсальных хеш-семейств с квантовыми односторонними функциями. Определено понятие квантового хеш-генератора и предложен подход для построения большого числа различных квантовых хеш-функций. Конструкция основана на объединении классических ε-универсальных хеш-семейств и заданного семейства функций – квантового хеш-генератора. Предложенная конструкция обладает свойствами устойчивого представления информации классическими кодами с исправлением ошибок, а также возможностью высоконадежного представления информации квантовыми системами. В частности, предложена квантовая хеш-функция, основанная на коде Рида – Соломона, и доказано, что данная конструкция является оптимальной в смысле необходимого числа кубитов.

Ключевые слова: квантовые вычисления, квантовые коммуникации, квантовое хеширование.

Введение

Хеширование имеет ряд важных приложений в различных областях информатики, в частности, криптографические протоколы с открытым ключом основываются на криптографических хеш-функциях. Хеш-функции строятся так, чтобы преобразовывать входные последовательности большой длины (теоретически – любой длины) в короткие хеш-коды (на практике – фиксированной длины).

В последнее десятилетие появилось несколько подходов (в литературе известно по крайней мере два подхода) к построению понятия квантовой функции.

Первый подход предложен в работе [1], в которой определяется семейство «классически-классических» функций, аргументами и значениями которых являются классические последовательности. Такие функции предположительно являются односторонними не только для классических, но и для квантовых алгоритмов. Авторы называют их квантовыми односторонними функциями.

Другой подход к определению квантовой функции сформулирован в работе [2]. Их функции «классически-квантовые», то есть аргументами функции являются классические последовательности, значениями – квантовые состояния. Другая «классически-квантовая» функция определена в работе Бурмана и др. [3]. Данная функция построена на основе двоичных кодов, исправляющих ошибки (в [3] использованы коды Джастесена). В [2, 3] доказано, что предложенные функции являются односторонними в смысле невозможности восстановления исходного слова по его квантовому образу.

Путем использования «классически-квантовых» функций на основе двоичных кодов, исправляющих ошибки, предложены различные сценарии построения квантовых систем цифровой подписи [2, 4, 5].

В настоящей работе мы анализируем определенные в [2, 3] «классически-квантовые» функции и вводим понятие «классически-квантовой» хеш-функции,

которое является естественным обобщением понятия «классически-квантовой» односторонней функции. Мы предлагаем «классически-квантовые» хеш-функции, исследуем их криптографические свойства, рассматриваем подходы к построению универсального квантового хеширования.

1. Предварительные сведения

Квантовая односторонняя функция была определена в [2]. Классически-квантовой функцией будем называть функцию вида

$$\psi : \{0,1\}^n \to (\mathcal{H}^2)^{\otimes s}, \quad \psi : w \mapsto |\psi(w)\rangle,$$

где

$$(\mathcal{H}^2)^{\otimes s} = \mathcal{H}^2 \otimes \cdots \otimes \mathcal{H}^2 = \mathcal{H}^{2^s}$$

обозначает 2^s-мерное гильбертово пространство, описывающие состояния s кубит.

Пример 1. Слово $w \in \{0,1\}^n$ при начальном состоянии $|\psi(e)\rangle = |0\rangle = 1|0\rangle + 0|1\rangle$ кубита кодируется в следующее состояние $|\psi(w)\rangle$ кубита:

$$\psi : (w, |0\rangle) \mapsto \cos\left(\frac{2\pi w}{2^n}\right)|0\rangle + \sin\left(\frac{2\pi w}{2^n}\right)|1\rangle.$$

Здесь двоичное слово $w = w_0 \dots w_{n-1}$ также рассматривается как число $w = w_0 + w_1 2^1 + \cdots + w_{n-1} 2^{n-1}$.

Очевидно, что разные последовательности w и v могут стать «практически неотличимыми», если вектора $|\psi(w)\rangle$ и $|\psi(v)\rangle$ близки. Последнее будет нарушать требование стойкости к коллизиям.

Отметим, что в различных статьях (см., например, [4, 5]) также неявно подразумевается наличие дополнительного свойства, обеспечивающего устойчивость к квантовым коллизиям, при этом само понятие квантовой коллизии не определяется. Необходимость введения данного понятия заключается в том, что при квантовом хешировании коллизии в классическом понимании отсутствуют, так как порождаемые квантовой хеш-функцией состояния различны для различных исходных сообщений. Однако сравнение квантовых хеш-кодов подразумевает выполнение вероятностной процедуры измерения квантовых состояний, что может приводить к ошибкам, связанным с коллизиями.

Квантовой коллизией будем называть ситуацию, когда процедура, проверяющая равенство квантовых хеш-кодов, ошибочно выдает совпадение различных исходных сообщений. Такой процедурой может быть хорошо известный SWAP-тест [3] или специфический для квантовой хеш-функции алгоритм. В любом случае процедура проверки связана с понятием различимости квантовых состояний. И поскольку неортогональные состояния не могут быть достоверно различены, потребуем, чтобы они были «почти ортогональны». Для формализации данного понятия введем следующее определение.

Определение 1. Состояния $|\psi_1\rangle$ и $|\psi_2\rangle$ называются *δ-ортогональными*, если

$$|\langle \psi_1 | \psi_2 \rangle| < \delta. \tag{1}$$

Таким образом, для квантовой хеш-функции важна δ-ортогональность квантовых хеш-кодов различных слов, то есть они должны успешно проходить тесты на неравенство. Рассмотрим подробнее возможные процедуры проверки равенства.

REVERSE-тест. В тех случаях, когда необходимо проверить, является ли квантовое состояние $|\psi(w)\rangle$ хеш-кодом некоторого классического слова v, можно применить процедуру, которую мы называем *REVERSE-тест* (идея такого теста для случая, когда v задается квантовым состоянием $|v\rangle$, была описана в [2], однако эта процедура не получила собственного названия). Суть теста заключается в применении инвертированной процедуры создания квантового хеша, то есть его «раскручивание до начального» состояния.

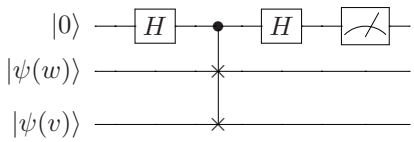
Формально, пусть процедура создания хеш-кода слова w состоит в применении унитарного преобразования $U(w)$ к начальному состоянию $|0\rangle$, то есть $|\psi(w)\rangle = U(w)|0\rangle$. Тогда REVERSE-тест заключается в применении $U^{-1}(v)$ к квантовому хешу $|\psi(w)\rangle$ и проверке полученного состояния. Если $v = w$, то результатом преобразования $U^{-1}(v)|\psi(w)\rangle$ всегда будет $|0\rangle$, и REVERSE-тест выдаст равенство; в противном случае результирующее состояние будет δ-ортогонально к $|0\rangle$, поскольку унитарные преобразования сохраняют скалярное произведение:

$$(|0\rangle, U^{-1}(v)|\psi(w)\rangle) = (U^{-1}(v)|\psi(v)\rangle, U^{-1}(v)|\psi(w)\rangle) = (|\psi(v)\rangle, |\psi(w)\rangle) < \delta. \qquad (2)$$

Таким образом, при $v \neq w$ REVERSE-тест может ошибаться с вероятностью δ. При этом предлагаемый вариант квантового хеширования позволяет применять REVERSE-тест со сколь угодно малой вероятностью ошибки δ.

Отметим, что здесь мы не учитываем погрешности реализации операторов $U(w)$ и $U^{-1}(w)$.

SWAP-тест. Для сравнения двух квантовых состояний (в частности, хеш-кодов) часто используется SWAP-тест [3], задаваемый следующей схемой:



Данный тест выдает результат $|\psi(w)\rangle = |\psi(v)\rangle$, если при измерении первый кубит оказывается в состоянии $|0\rangle$. В работе [3] показано, что SWAP-тест обладает следующим свойством.

Свойство 1. *Вероятность получения состояния* $|0\rangle$ *в результате SWAP-теста равна*

$$\frac{1}{2}\left(1 + |\langle\psi(w)\,|\,\psi(v)\rangle|^2\right).$$

Таким образом, при $|\psi(w)\rangle = |\psi(v)\rangle$ данный тест не ошибается, а в случае $|\psi(w)\rangle \neq |\psi(v)\rangle$ вероятность ошибки зависит от скалярного произведения $|\psi(w)\rangle$ и $|\psi(v)\rangle$ – она минимальна (близка к $1/2$), если эти состояния будут ортогональны или «почти ортогональны» [2].

Таким образом, свойство δ-ортогональности квантовых состояний является важным качеством для обеспечения устойчивости к квантовым коллизиям, в связи с эти введем понятие δ-устойчивости.

Определение 2. Назовем квантовую функцию $\psi : w \mapsto |\psi(w)\rangle$ δ-устойчивой (кратко δ-R), если для любой пары сообщений w, w', $w \neq w'$ выполняется:

$$|\langle\psi(w)\,|\,\psi(w')\rangle| < \delta,$$

то есть их образы δ-ортогональны.

Объединением понятия квантовой односторонней функции и определения 2 является следующее определение классически-квантовой хеш-функции.

Определение 3. Назовем функцию

$$\psi : \{0,1\}^n \to (\mathcal{H}^2)^{\otimes s}$$

δ-R $(n;s)$-квантовой хеш-функцией, если она является квантовой односторонней и δ-устойчивой функцией.

Положим $\mathbb{X} = \{0,1\}^n$, $K = |\mathbb{X}| = 2^n$. Следующая теорема, дающая нижнюю оценку на число требуемых кубит для выбранной степени устойчивости δ, верна также для конечных алфавитов Σ, отличных от $\{0,1\}$.

Теорема 1. *Пусть функция $\psi : \mathbb{X} \to (\mathcal{H}^2)^{\otimes s}$ является δ-устойчивой. Тогда*

$$s \geq \log\log|\mathbb{X}| - \log\log\left(1 + \sqrt{2/(1-\delta)}\right) - 1.$$

Доказательство. Из определения нормы $\||\psi\rangle\| = \sqrt{\langle\psi\,|\,\psi\rangle}$ следует, что

$$\||\psi\rangle - |\psi'\rangle\|^2 = \||\psi\rangle\|^2 + \||\psi'\rangle\|^2 - 2\langle\psi\,|\,\psi'\rangle.$$

Следовательно, для произвольной пары w, w' различных слов из $\mathbb{X}$ имеем

$$\||\psi(w)\rangle - |\psi(w')\rangle\| \geq \sqrt{2(1-\delta)}.$$

Положим $\Delta = \sqrt{2(1-\delta)}$.

Рассмотрим множество $\Phi = \{|\psi(w)\rangle : w \in \mathbb{X}\}$ точек в пространстве $(\mathcal{H}^2)^{\otimes s}$. Если описать сферы радиуса $\Delta/2$ с центрами в точках $|\psi\rangle \in \Phi$, тогда все такие сферы могут пересекаться только по окружности. Все эти K сфер располагаются в сфере радиуса $1 + \Delta/2$. Объем сферы радиуса r в комплексном пространстве $(\mathcal{H}^2)^{\otimes s}$ равен $cr^{2^{s+1}}$. Константа c определяется метрикой пространства $(\mathcal{H}^2)^{\otimes s}$.

Таким образом, имеем, что число K ограничено сверху числом «малых сфер» в «большой сфере»:

$$K \leq \frac{c(1+\Delta/2)^{2^{s+1}}}{c(\Delta/2)^{2^{s+1}}}.$$

Следовательно,

$$s \geq \log\log K - \log\log\left(1 + \sqrt{2/(1-\delta)}\right) - 1.$$

□

Следующее свойство непосредственно следуют из определения 3 и свойства 1.

Свойство 2. *Если функция $\psi : w \mapsto |\psi(w)\rangle$ является δ-R $(n;s)$-квантовой хеш-функцией, тогда SWAP-тест различает квантовые хеш-коды двух слов $w \neq w'$ с вероятностью $\frac{1}{2}(1-\delta^2)$.*

Доказательство. Согласно свойству 1 вероятность ошибки SWAP-теста для различных исходных состояний описывается выражением $\frac{1}{2}\left(1 + |\langle\psi(w)\,|\,\psi(w')\rangle|^2\right)$. Таким образом, поскольку для δ-устойчивой функции $|\langle\psi(w)\,|\,\psi(w')\rangle| < \delta$, SWAP-тест различает квантовые хеш-коды двух слов $w \neq w'$ с вероятностью $\frac{1}{2}(1-\delta^2)$. □

Отметим, что вероятность ошибки SWAP-теста можно уменьшить до любого наперед заданного $\varepsilon > 0$ с помощью стандартной процедуры повтора, то есть применяя SWAP-тест на $k = O(\log 1/\varepsilon)$ независимых копиях сравниваемых состояний. Другими словами, для надежного сравнения в качестве квантового хеша для $u \in \{0,1\}^n$ можно использовать функцию

$$\psi' : u \mapsto |\psi'(u)\rangle,$$

представляемую формулой

$$|\psi'(u)\rangle = |\psi(u)\rangle^{\otimes k} = |\psi(u)\rangle \otimes \cdots \otimes |\psi(u)\rangle.$$

В этом случае общее число кубит для хеширования слов увеличивается в $k = O(\log(1/\varepsilon))$ раз.

Кроме того, заметим, что δ-устойчивость также обеспечивает стойкость к коллизиям второго рода, так как невозможно подобрать два различных сообщения, которые бы SWAP-тест ошибочно принимал за равные с вероятностью, близкой к 1.

В завершение данного раздела представим первые две квантовые хеш-функции, основанные на известных конструкциях квантовых методов отпечатков, предложенных в работах [3] и [6].

1.1. Квантовая функция отпечатков («булева (двоичная) конструкция»). В работе [3] Бурман и др. определили квантовую одностороннюю функцию

$$f_E : u \mapsto |f_E(u)\rangle$$

на двоичных словах $u \in \{0,1\}^n$, основанную на двоичных кодах, исправляющих ошибки (конкретно на коде Джастесена) $E : \{0,1\}^n \mapsto \{0,1\}^m$. Такую функцию авторы назвали квантовым отпечатком (quantum fingerprint) u и определили следующим образом:

$$|f_E(u)\rangle = \frac{1}{\sqrt{m}} \sum_{i=0}^{m-1} |i\rangle |E_i(u)\rangle,$$

где $m = cn$, $E_i(u)$ обозначает i-й бит $E(u)$. Квантовая функция f_E представима также в следующем виде:

$$|f_E(u)\rangle = \frac{1}{\sqrt{m}} \sum_{i=0}^{m-1} |i\rangle \left(\cos \frac{\pi E_i(u)}{2} |0\rangle + \sin \frac{\pi E_i(u)}{2} |1\rangle \right).$$

Свойство 3. *Для $\delta \approx 9/10 + 1/(15c)$ квантовая функция отпечатков f_E является δ-R $(n; O(\log n))$-квантовой хеш-функцией.*

Доказательство. В [3] доказано, что функция f_E является квантовой односторонней функцией и δ-устойчивой к коллизиям при $\delta \approx 9/10 + 1/(15c)$. □

1.2. Обобщенная квантовая функция отпечатков («q-я конструкция»). Рассматриваемая ниже конструкция квантовой хеш-функции является (в определенном смысле) обобщением конструкции булева варианта квантовой функции отпечатков на случай $q > 2$ и может быть названа q-й квантовой функцией отпечатков.

Пусть $q = 2^n$, $B = \{b_i : b_i \in \{0, \ldots, q-1\}\}$. Классически-квантовая функция

$$\psi_{q,B} : \{0,1\}^n \to (\mathcal{H}^2)^{\otimes(\log|B|+1)}$$

определяется следующим образом. Для сообщения $M \in \{0,1\}^n$ полагаем

$$|\psi_{q,B}(M)\rangle = \frac{1}{\sqrt{|B|}} \sum_{i=1}^{|B|} |i\rangle \left(\cos \frac{2\pi b_i M}{q} |0\rangle + \sin \frac{2\pi b_i M}{q} |1\rangle \right). \tag{3}$$

Теорема 2. *Для произвольного $\delta > 0$ существует множество $B \subset \mathbb{Z}_q$ такое, что $|B| = \lceil (2/\delta^2) \ln(2q) \rceil$, и функция $\psi_{q,B}$ является δ-R $(n; O(\log n + \log 1/\delta))$-квантовой хеш-функцией.*

Доказательство. Для доказательства теоремы достаточно доказать, что функция $\psi_{q,B}$ является односторонней и δ-устойчивой.

Для доказательства δ-устойчивости $\psi_{q,B}$ понадобятся следующие вспомогательные сведения.

Определение 4. Дискретным преобразованием характеристической функции множества $B \subset \mathbb{Z}_q$ называется функция

$$f_B(l) = \sum_{b \in B} \exp\left(i \frac{2\pi b l}{q} \right).$$

Пусть $\lambda(B) = \max\limits_{l \neq 0} \dfrac{|f_B(l)|}{|B|}$ и $\delta(B) = \max\limits_{l \neq 0} \dfrac{|\mathrm{Re}(f_B(l))|}{|B|}$. Как было отмечено в работе [7], $\lambda(B)$ дает некоторую меру «хаотичности» множества B: чем меньше $\lambda(B)$, тем более «случайно» устроено множество B. Мы определили $\delta(B)$ подобным образом, но оно использует лишь вещественную часть $f_B(l)$. Очевидно, $\delta(B) \leq \lambda(B)$.

Для построения нашей техники нам понадобится B с наименьшим возможным $\delta(B)$. В [7] была предложена конструкция, позволяющая для $\varepsilon = \dfrac{1}{(\log q)^{O(1)}}$ получить множество B, для которого $|B| = (\log q)^{O(1)}$ и $\lambda(B) \leq \varepsilon$.

Кроме того, в работе [8] была доказана следующая лемма.

Лемма 1. *Для любого $\varepsilon \in (0,1)$ существует множество B, для которого $|B| = \left\lceil \dfrac{2}{\varepsilon} \ln(2q) \right\rceil$ и $\delta(B) < \varepsilon$.*

Заметим, что в [8] не применялось обозначение $\delta(B)$, вместо этого использовалась запись $\dfrac{1}{|B|} \sum\limits_{b \in B} \cos \dfrac{2\pi b l}{q}$.

Зафиксируем $\delta \in (0,1)$ и выберем множество B, удовлетворяющее условиям леммы 1 при $\varepsilon = \delta^2$. В этом случае функция $\psi_{q,B}$ является δ-устойчивой, так как для любых $w_1 \neq w_2$

$$|\langle \psi_{q,B}(w_1) \,|\, \psi_{q,B}(w_2) \rangle| =$$

$$= \left| \frac{1}{|B|} \sum_{i=1}^{|B|} \left(\cos \frac{2\pi b_i w_1}{q} \cos \frac{2\pi b_i w_2}{q} + \sin \frac{2\pi b_i w_1}{q} \sin \frac{2\pi b_i w_2}{q} \right) \right| =$$

$$= \left| \frac{1}{|B|} \sum_{i=1}^{|B|} \cos \frac{2\pi b_i (w_1 - w_2)}{q} \right| \leq \delta(B) < \delta. \tag{4}$$

Таким образом, функция $\psi_{q,B}$ хеширует n-битные сообщения в квантовые состояния из $O(\log n + \log 1/\delta)$ кубит и обеспечивает δ-ортогональность квантовых хеш-кодов.

□

2. Универсальное квантовое хеширование

Рассмотренные выше конструкции квантовых хеш-функций f_E и $\psi_{\delta,B}$ объединяет следующее. Обе конструкции определяют «квантово-параллельно-равноамплитудно-контролируемое» преобразование одного кубита. Каждое такое преобразование генерируется (задается) функциями из соответствующих специальных семейств.

Пусть $G = \{g_1, \ldots, g_D\}$ – семейство функций вида $g_j : \mathbb{X} \to \mathbb{F}_q$.

Обобщением рассмотренных выше конструкций является следующее.

Определение 5 (Генератор квантовых хеш-функций). Пусть $G = \{g_1, \ldots, g_D\}$ – семейство функций вида $g_j : \mathbb{X} \to \mathbb{F}_q$, $\ell \geq 1$. Для $g \in G$ пусть ψ_g – классически-квантовая функция $\psi_g : \mathbb{X} \to (\mathcal{H}^2)^{\otimes \ell}$, определяемая по правилу

$$\psi_g : w \mapsto |\psi_g(w)\rangle = \sum_{i=0}^{2^\ell - 1} \alpha_i(g(w))|i\rangle, \tag{5}$$

где коэффициенты $\alpha_i(g(w))$, $i \in \{0, \ldots, 2^\ell - 1\}$, состояния формируются (задаются) функцией g_i в процессе считывания w. Пусть, далее, $d = \log D$. Определим классически-квантовую функцию $\psi_G : \mathbb{X} \to (\mathcal{H}^2)^{\otimes(d+\ell)}$ по правилу

$$\psi_G : w \mapsto |\psi_G(w)\rangle = \frac{1}{\sqrt{D}} \sum_{j=0}^{D-1} |j\rangle \big|\psi_{g_j}(w)\big\rangle. \tag{6}$$

Будем говорить, что семейство G генерирует δ-R $(K; d + \ell)$-квантовую хеш-функцию ψ_G, и будем называть G δ-R $(K; d + \ell)$-квантовым генератором, если функция ψ_G является δ-R $(K; d + \ell)$-квантовой хеш-функцией.

В терминах определения 5 и описанных выше квантовых хеш-функций на основе квантовой функции отпечатков и обобщенной квантовой функции отпечатков имеем, что семейство $F_E = \{E_0, \ldots, E_{m-1}\}$, где $E_i : \{0,1\}^n \to \{0,1\}$, $E_i(u)$ – это i-й бит $E(u)$, и семейство $H_{q,B} = \{h_1, \ldots h_{|B|}\}$, где $h_i(w) = b_i w \pmod q$, являются генераторами квантовых хеш-функций f_E и $\psi_{q,B}$ соответственно.

2.1. ε-универсальное квантовое хеширование. Выше приведены две конструкции (булева и q-я) генераторов квантовых хеш-функций на основе методов отпечатков. Ниже предлагается подход построения квантовых хеш-функций, основанный на применении композиции классических семейств ε-универсальных хеш-функций и некоторого заданного генератора квантовых хеш-функций. Известно, что конструкции классических семейств ε-универсальных хеш-функций связаны с кодами, исправляющими ошибки (см., например, [9]). Данный подход открывает возможности построения новых квантовых хеш-функций на основе уже имеющихся. В частности, ниже показывается, что конструкция кодов Рида – Соломона эффективна для построения квантовых хеш-функций.

Терминология и система обозначений в теории кодов, исправляющих ошибки, сформировались более пятидесяти лет назад. Поэтому ниже мы будем следовать принятым стандартам. Параметры k, n будут обозначать длину исходного слова и длину его кода соответственно.

Мы используем определения из работы [9].

• Пусть $\mathbb{X}$, $|\mathbb{X}| = K$, – область определения, а $\mathbb{Y}$, $|\mathbb{Y}| = M$, – область значений, где $K \geq M$. Хеш-функция f – это отображение $f : \mathbb{X} \to \mathbb{Y}$, хеширующее *длинные* исходные слова в *короткие* слова-образы.

• Пусть q – степень простого числа, $\mathbb{F}_q$ – поле, Σ^k – множество слов длины k над алфавитом Σ. В дальнейшем будем полагать $\mathbb{X} = \Sigma^k$ или $\mathbb{X} = \mathbb{F}_q$ и $\mathbb{Y} = \mathbb{F}_q$.

N хеш-семейство – это множество $F = \{f_1, \dots f_N\}$ N хеш-функций $f_i : \mathbb{X} \to \mathbb{Y}$.

Дополнительно полагаем, что функции f семейства F эффективно вычислимы – имеется полиномиальный по времени алгоритм вычисления $f(w)$ по w (полиномиальный по времени от длины w).

• **ε-универсальное хеш-семейство.** N хеш-семейство F называется ε-универсальным, если для двух различных элементов $w, w' \in \mathbb{X}$ существуют не более εn функций $f \in F$ таких, что $f(w) = f(w')$. В работе [9] используется обозначение ε-U $(N; K, M)$ для обозначения ε-универсальных хеш-семейств.

Случай $\varepsilon = 1/N$ известен как универсальное хеширование.

Пусть $K = |\mathbb{X}|$, $M = |\mathbb{Y}|$, $F = \{f_1, \dots, f_N\}$ является семейством функций $f_i : \mathbb{X} \to \mathbb{Y}$.

Пусть $H = \{h_1, \dots, h_T\}$ является семейством функций $h_j : \mathbb{Y} \to \mathbb{F}_q$. Для $f \in F$ и $h \in H$ определим суперпозицию $g = f \circ h$,

$$g : \mathbb{X} \to \mathbb{F}_q$$

как

$$g(w) = (f \circ h)(w) = h(f(w)).$$

Определим композицию G семейств F и H следующим образом:

$$G = F \circ H = \{g = f \circ h : f \in F, h \in H\}.$$

Теорема 3. *Пусть $F = \{f_1, \dots, f_N\}$ является эффективным ε-универсальным $(N; K, M)$ хеш-семейством. Пусть $\ell \geq 1$, $H = \{h_1, \dots h_T\}$ является δ-R $(M; \log T + \ell)$-квантовым хеш-генератором, $\log K > \log N + \log T + \ell$.*

Тогда композиция $G = F \circ H$ является Δ-R $(K; s)$ квантовым хеш-генератором, причем

$$s = \log N + \log T + \ell \tag{7}$$

и

$$\Delta \leq \varepsilon + \delta. \tag{8}$$

Доказательство. Введем следующую запись для композиции $G = F \circ H$:

$$G = \{g_{ij} = f_i \circ h_j : i \in I, j \in J\},$$

где $I = \{1, \dots, N\}$, $J = \{1, \dots, T\}$.

При этом δ-R $(M; \log T + \ell)$-квантовый хеш-генератор H генерирует δ-R $(M; \log T + \ell)$-квантовую хеш-функцию

$$\psi_H : v \mapsto \frac{1}{\sqrt{T}} \sum_{j \in J} |j\rangle |\psi_{h_j}(v)\rangle. \tag{9}$$

Для $s = \log N + \log T + \ell$, используя семейство G, определим отображение

$$\psi_G : \mathbb{X} \to (\mathcal{H}^2)^{\otimes s}$$

как

$$|\psi_G(w)\rangle = \frac{1}{\sqrt{N}} \sum_{i \in I} |i\rangle \otimes |\psi_H(f_i(w))\rangle. \tag{10}$$

Докажем Δ-устойчивость функции ψ_G. Рассмотрим пару w, w' различных элементов $\mathbb{X}$ и скалярное произведение $\langle\psi_G(w)\,|\,\psi_G(w')\rangle$. Используя линейность скалярного произведения, получаем

$$\langle\psi_G(w)\,|\,\psi_G(w')\rangle = \frac{1}{N}\sum_{i\in I}\langle\psi_H(f_i(w))\,|\,\psi_H(f_i(w'))\rangle. \tag{11}$$

Для пары w, w' определим два множества индексов I_{bad} и I_{good}:

$$I_{\text{bad}} = \{i\in I : f_i(w) = f_i(w')\}, \quad I_{\text{good}} = \{i\in I : f_i(w) \neq f_i(w')\}.$$

Тогда получаем

$$|\langle\psi_G(w)\,|\,\psi_G(w')\rangle| \le \frac{1}{N}\sum_{i\in I_{\text{bad}}}|\langle\psi_H(f_i(w))\,|\,\psi_H(f_i(w'))\rangle| + \\ + \frac{1}{N}\sum_{i\in I_{\text{good}}}|\langle\psi_H(f_i(w))\,|\,\psi_H(f_i(w'))\rangle|. \tag{12}$$

Хеш-семейство F является ε-универсальным, так как

$$|I_{\text{bad}}| \le \varepsilon N.$$

Квантовая функция $\psi_H : \mathbb{Y} \to (\mathcal{H}^2)^{\log T+\ell}$ является δ-устойчивой, поскольку для произвольной пары v, v' различных элементов $\mathbb{Y}$ скалярное произведение их образов принимает значение

$$|\langle\psi_H(v)\,|\,\psi_H(v')\rangle| \le \delta. \tag{13}$$

Наконец, из (12) и двух предыдущих неравенств получаем, что

$$|\langle\psi_G(w)\,|\,\psi_G(w')\rangle| \le \varepsilon + \frac{|I_{\text{good}}|}{N}\delta \le \varepsilon + \delta. \tag{14}$$

Последнее неравенство (14) доказывает Δ-устойчивость $\psi_G(w)$ (например, для $\Delta = \varepsilon + \delta$), что завершает доказательство неравенства (8).

Чтобы завершить доказательство теоремы, нам осталось показать, что функция ψ_G может быть представлена в виде (6). Из (9) и (10) мы получаем, что

$$|\psi_G(w)\rangle = \frac{1}{\sqrt{N}}\sum_{i\in I}|i\rangle\otimes\left(\frac{1}{\sqrt{T}}\sum_{j\in J}|j\rangle\big|\psi_{h_j}(f_i(w))\big\rangle\right). \tag{15}$$

Используя запись (5), представим (15) в следующем виде (6):

$$|\psi_G(w)\rangle = \frac{1}{\sqrt{NT}}\sum_{i\in I,\,j\in J}|ij\rangle\big|\psi_{g_{ij}}(w)\big\rangle. \tag{16}$$

□

2.2. Конструкции квантового хеширования, основанные на классическом универсальном хешировании. Следующее утверждение является следствием теоремы 3 и является основой для дальнейшего построения квантовых хеш-функций в явном виде. Пусть q является степенью простого числа и $\mathbb{F}_q$ является полем, $\delta \in (0,1)$. Пусть $H_{\delta,q} = \{h_1,\dots h_{|B|}\}$, где $h_i(w) = b_i w \pmod q$, является генератором квантовой хеш-функции (3). Обозначим $|\mathbb{X}| = K$.

Теорема 4. *Пусть* $F = \{f_1, \ldots, f_N\}$ *является эффективным* ε*-универсальным* $(N; K, q)$ *хеш-семейством, где* $f_i : \mathbb{X} \to \mathbb{F}_q$. *Тогда для произвольного* $\delta > 0$ *семейство* $G = F \circ H_{\delta,q}$ *является* Δ*-R* $(K; s)$*-квантовым хеш-генератором, где*

$$s \le \log N + \log\log q + 2\log 1/\delta + 3 \tag{17}$$

и

$$\Delta \le \varepsilon + \delta. \tag{18}$$

Доказательство. Семейство $H_{\delta,q} = \{h_1, \ldots, h_T\}$, где $h_i : \mathbb{F}_q \to \mathbb{F}_q$, $T = \lceil (2/\delta^2)\ln(2q)\rceil$, $\ell = 1$, является δ-R $(q; s)$-квантовым хеш-генератором при $s = \log T + 1 \le \log n + \log\log q + 2\log 1/\delta + 3$. □

В оставшейся части раздела мы приводим примеры квантовых хеш-функций, основанных на универсальных линейных семействах хеш-функций и кодах, исправляющих ошибки.

2.3. Квантовое хеширование и коды, исправляющие ошибки. Пусть q является степенью простого числа и $\mathbb{F}_q$ является полем. $(n, k, d,)$-код, исправляющий ошибки, называется *линейным* с $\Sigma = \mathbb{F}_q$, и $\mathcal{C} = \{C(w) : w \in \Sigma^k\}$ – подпространство пространства $\mathbb{F}_q^n$. Мы будем обозначать такой линейный код как $[n, k, d]_q$-код.

Теорема 5. *Пусть* $\mathcal{C}$ *является* $[n, k, d]_q$*-кодом. Тогда для произвольного* $\delta \in (0, 1)$ *существует* Δ*-R* $(q^k; s)$*-квантовый хеш-генератор* G*, где* $\Delta = (1-d/n)+\delta$ *и* $s \le \log n + \log\log q + 2\log 1/\delta + 4$.

Доказательство. В [10] было доказано следующее свойство. Имея $[n, k, d]_q$-код $\mathcal{C}$, мы можем в явном виде построить $(1 - d/n)$-U $(n; q^k; q)$ хеш-семейство $F_{\mathcal{C}}$.

По теореме 4 композиция $G = F_{\mathcal{C}} \circ H_{\delta,q}$ является Δ-R $(q^k; s)$ квантовым хеш-генератором, где $\Delta = (1 - d/n) + \delta$ и $s \le \log n + \log\log q + 2\log 1/\delta + 4$. □

2.4. Квантовые хеш-функции на основе конструкции кода Рида – Соломона. В качестве примера приведем конструкцию квантовой хеш-функции, используя код Рида – Соломона.

Пусть q является степенью простого числа. *Расширенный код Рида – Соломона* – это линейный код

$$C_{\mathrm{RS}} : (\mathbb{F}_q)^k \to (\mathbb{F}_q)^n \tag{19}$$

с параметрами $[n, k, n - (k - 1)]_q$, где $k \le n = q$, который задается следующим образом. Каждому слову $w \in (\mathbb{F}_q)^k$, $w = w_0 w_1 \ldots w_{k-1}$, ставится в соответствие полином

$$P_w(x) = \sum_{i=0}^{k-1} w_i x^i. \tag{20}$$

Для кодирования слова w вычисляем $P_w(x)$ во всех q элементах $a \in \mathbb{F}_q$:

$$C_{\mathrm{RS}}(w) = (P_w(0)P_w(1)\ldots P_w(q-1)). \tag{21}$$

Используя коды Рида – Соломона, мы получаем следующее утверждение.

Теорема 6. *Пусть* q *является степенью простого числа,* $1 \le k \le q$. *Тогда для произвольного* $\delta \in (0, 1)$ *существует* Δ*-R* $(q^k; s)$*-квантовый хеш-генератор* G_{RS}*, где* $\Delta \le \dfrac{k-1}{q} + \delta$ *и* $s \le \log(q\log q) + 2\log 1/\delta + 4$.

Доказательство. Код Рида – Соломона C_{RS} является $[q, k, q-(k-1)]_q$-кодом, где $k \leq q$. Тогда согласно теореме 5 семейство G_{RS} является Δ-R $(q^k; s)$-квантовым хеш-генератором с требуемыми параметрами. □

В частности, выбрав $q \in [ck, c'k]$ для постоянной $c < c'$, получаем, что $\delta \leq 1/c + \delta$ для $\delta \in (0, 1)$, и в соответствии с теоремой 1

$$\log(q \log q) - \log\log\left(1 + \sqrt{2/(1-\delta)}\right) - \log c'/2 \leq s \leq \log(q \log q) + 2\log 1/\delta + 4. \quad (22)$$

Таким образом, коды Рида – Соломона имеют достаточно хорошие параметры устойчивости δ, и нам нужно построить квантовую хеш-функцию ψ_{RS} для s кубитов.

2.5. Эффективные конструкции семейства $G_{\mathbf{RS}}$ и функции $\psi_{G_{\mathbf{RS}}}$. Определим $(k-1)/q$-U $(q; \mathbb{F}_q^k; q)$-хеш-семейство $F_{\mathrm{RS}} = \{f_a : a \in \mathbb{F}_q\}$ на основе кода C_{RS} следующим образом. Для $a \in \mathbb{F}_q$ определим $f_a : (\mathbb{F}_q)^k \to \mathbb{F}_q$ как

$$f_a(w_0 \ldots w_{k-1}) = \sum_{i=0}^{k-1} w_i a^i. \quad (23)$$

Пусть $H_{\delta,q} = \{h_1, \ldots, h_T\}$, где $h_j : \mathbb{F}_q \to \mathbb{F}_q$ и $T = \lceil (2/\delta^2) \ln 2q \rceil$. Для $s = \log q + \log T + 1$ композиция $G_{\mathrm{RS}} = F_{\mathrm{RS}} \circ H_{\delta,q}$ определяет функцию

$$\psi_{G_{\mathrm{RS}}} : (\mathbb{F}_q)^k \to (\mathcal{H}^2)^{\otimes s}$$

для слова $w \in (\mathbb{F}_q)^k$ следующим образом:

$$|\psi_{G_{\mathrm{RS}}}(w)\rangle = \\ = \frac{1}{\sqrt{q}} \sum_{a \in \mathbb{F}_q} |a\rangle \otimes \left(\frac{1}{\sqrt{T}} \sum_{j=1}^{T} |j\rangle \otimes \left(\cos \frac{2\pi h_j(f_a(w))}{q} |0\rangle + \sin \frac{2\pi h_j(f_a(w))}{q} |1\rangle \right) \right). \quad (24)$$

Работа выполнена за счет средств субсидии, выделенной в рамках государственной поддержки Казанского (Приволжского) федерального университета в целях повышения его конкурентоспособности среди ведущих мировых научно-образовательных центров, а также гранта РФФИ № 14-07-00878-а.

Summary

F.M. Ablayev, M.F. Ablayev, A.V. Vasilev. Universal Quantum Hashing.

In the paper we propose a method of quantum hashing which mostly combines the existing constructions of universal hash families with quantum one-way functions. Next, we define the concept of a quantum hash generator and present an approach for building a large number of various quantum hash functions. The construction is based on the integration of a classical ε-universal hash family and a given family of functions – quantum hash generator. The proposed construction combines the properties of robust representation of information by classical error-correcting codes together with the possibility of highly reliable representation of information by quantum systems. In particular, we present a quantum hash function based on the Reed–Solomon code and prove that this construction is optimal in the sense of the number of qubits needed.

Keywords: quantum computations, quantum communications, quantum hashing.

Литература

1. *Kashefi E., Kerenidis I.* Statistical Zero Knowledge and quantum one-way functions // Theor. Comput. Sci. – 2007. – V. 378, No 1. – P. 101–116. – doi: 10.1016/j.tcs.2007.03.013.

2. *Gottesman D., Chuang I.* Quantum Digital Signatures: arXiv:quant-ph/0105032. – 2001. – URL: http://arxiv.org/abs/quant-ph/0105032.

3. *Buhrman H., Cleve R., Watrous J., de Wolf R.* Quantum Fingerprinting // Phys. Rev. Lett. – 2001. – V. 87, No 16. – P. 167902-1–167902-4. – doi: 10.1103/PhysRevLett.87.167902.

4. *Lu X., Feng D.* Quantum digital signature based on quantum one-way functions // The 7th Int. Conf. on Advanced Communication Technology (ICACT'2005). – 2005. – V. 1. – P. 514–517.

5. *Zhou J., Zhou Y., Niu X., Xian Y.* Quantum proxy signature scheme with public verifiability // Science China Physics, Mechanics and Astronomy. – 2011. – V. 54, No 10. – P. 1828–1832. – doi: 10.1007/s11433-011-4457-z.

6. *Ablayev F., Vasiliev A.* Algorithms for Quantum Branching Programs Based on Fingerprinting // Electr. Proc. in Theor. Comput. Sci. – 2009. – V. 9. – P. 1–11.

7. *Razborov A.A., Szemeredi E., Wigderson A.* Constructing Small Sets that are Uniform in Arithmetic Progressions // Combinatorics, Probability & Computing. – 1993. – V. 2. – P. 513–518.

8. *Ablayev F., Vasiliev A.* On the Computation of Boolean Functions by Quantum Branching Programs via Fingerprinting // Electronic Colloquium on Computational Complexity (ECCC). – 2008. – V. 15. – Art. 059. – URL: http://www.eccc.uni-trier.de/report/2008/059/, свободный.

9. *Stinson D.R.* On the Connections between Universal Hashing, Combinatorial Designs and Error-Correcting Codes // Proc. Congressus Numerantium 114. – 1996. – P. 7–27.

10. *Bierbrauer J., Johansson T., Kabatianskii G., Smeets B.* On Families of Hash Functions via Geometric Codes and Concatenation // Advances in Cryptology – CRYPTO'93 / By ed. D.R. Stinson. – Berlin; Heidelberg: Springer, 1994. – P. 331–342.

Поступила в редакцию
05.08.14

Аблаев Фарид Мансурович – доктор физико-математических наук, заведующий кафедрой теоретической кибернетики, Казанский (Приволжский) федеральный университет, г. Казань, Россия.

E-mail: *fablayev@gmail.com*

Аблаев Марат Фаридович – младший научный сотрудник лаборатории квантовой информатики, Казанский (Приволжский) федеральный университет, г. Казань, Россия.

E-mail: *mablayev@gmail.com*

Васильев Александр Валерьевич – кандидат физико-математических наук, доцент кафедры системного анализа и информационных технологий, Казанский (Приволжский) федеральный университет, г. Казань, Россия.

E-mail: *Alexander.Vasiliev@kpfu.ru*