УЧЕНЫЕ ЗАПИСКИ КАЗАНСКОГО УНИВЕРСИТЕТА.
СЕРИЯ ФИЗИКО-МАТЕМАТИЧЕСКИЕ НАУКИ

2020, Т. 162, кн. 3
С. 259–268

ISSN 2541-7746 (Print)
ISSN 2500-2198 (Online)

УДК 519.7

doi: 10.26907/2541-7746.2020.3.259-268

УНИВЕРСАЛЬНОЕ СЕМЕЙСТВО ХЕШ-ФУНКЦИЙ НА ОСНОВЕ КВАНТОВЫХ ПРОЦЕДУР

Ф.М. Аблаев, М.Т. Зиятдинов

Казанский физико-технический институт им. Е.К. Завойского
ФИЦ Казанский научный центр РАН, г. Казань, 420029, Россия
Казанский (Приволжский) федеральный университет, г. Казань, 420008, Россия

Аннотация

Предложены процедуры построения универсального семейства хеш-функций на основе квантового хеширующего процесса, отображающего исходную последовательность w в квантовое хеш-состояние и далее случайным преобразованием в состояние $|\psi\rangle$ и порождением последовательности u, являющимся приближенным описанием состояния $|\psi\rangle$.

Доказано, что предлагаемая процедура порождает семейство недетерминированных хеш-функций $\mathcal{F}$, которые позволяют достоверно различать различные аргументы. Семейство $\mathcal{F}$ можно считать ϵ-универсальным семейством недетерминированных хеш-функций.

Ключевые слова: квантовые хеш-функции, универсальное семейство хеш-функций, квантовое превосходство

1. Введение, результат и предварительные сведения

Возможности квантовых моделей вычислений по реализации вычислений и принципиальные трудности классических моделей вычислений по моделированию таких квантовых вычислителей были отмечены в работах основоположников теории квантовых вычислений Р. Фейнманом [1] и Ю. Маниным [2]. На сегодняшний день имеется достаточно большое число результатов, в которых доказывается теоретическая возможность получить преимущества при использовании квантовых моделей вычислений по сравнению с классическими моделями. Такие модели являются моделями с теми или иными ограничениями. Принципиальные вопросы, такие как верно ли, что $P \neq BQP$, остаются открытыми. При этом хорошо известен квантовый алгоритм факторизации [3] – алгоритм быстрого решения практически важной задачи. Напомним, что при этом вопрос построения быстрого классического алгоритма факторизации является открытой проблемой. Это задача будущих квантовых технологий.

Современные квантовые технологии являются NISQ-технологиями (Noisy Intermediate-Scale Quantum) [4]. NISQ-технологии позволяют создавать недостаточно точные квантовые вычислители с небольшой вычислительной мощностью. Но идет быстрое развитие квантовых технологий и на повестке дня стоит вопрос демонстрации «квантового превосходства» (Quantum supremacy) [5] в эпоху NISQ-технологий.

Важной является разработка задач, имеющих прикладное значение, для которых в достаточно близкой перспективе можно ожидать появления квантовых NISQ-вычислителей их решающих, но классическое моделирование которых уже

будет невозможно. С нашей точки зрения, одним из источников такого типа проблем могут стать задачи хеширования информации. Построение семейств универсальных хеш-функций является одним из таких направлений.

Понятие «универсальное хеширование» определено в работе Картера и Вегмана [6] в 1979 г. Это понятие предполагает использование семейства хеш-функций для задач экономного представления информации. Семейства хеш-функций полезны для прикладной информатики в криптографии, в системах аутентификации сообщений [7, 8] в теории кодирования, а также в теоретической информатике [9].

Говорят, что семейство $\mathcal{F}$ хеш-функций обладает свойством ϵ-универсальности для множества $\{0,1\}^n$, если для произвольных различных w, $w' \in \{0,1\}^n$ доля функций $h \in \mathcal{F}$, для которых $h(w) = h(w')$, не превосходит ϵ. Другими словами, семейство функций $\mathcal{F}$ позволяет надежно отличить различные последовательности w и w' (с вероятностью не менее $1-\epsilon$ при равновероятностном выборе h из $\mathcal{F}$).

Цель настоящей работы – разработка подхода построения семейства универсальных хеш-функций (недетерминированных функций) на основе квантовых процедур. А именно, в работе представлена квантовая процедура, порождающая семейство недетерминированных функций. Задаваемые недетерминированные функции позволяют достоверно отличать различные последовательности $w, w' \in \in \{0,1\}^n$. Предлагаемый подход в явном виде описывается в разд. 3 и заключается в следующем.

1. На первом этапе выбирается квантовая хеш-функция

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

отображающая исходную последовательность w на основе квантового хеширующего процесса в квантовое состояние $|\psi(w)\rangle$.

2. Выбирается равновероятностно унитарное преобразование $U \in \mathcal{U}$, которое применяется к результату $|\psi(w)\rangle$ хеширования w.

3. Для выбранного U порождается (достаточное число) N копий состояния $|\psi_U(w)\rangle = U|\psi(w)\rangle$.

В результате измерения этих N копий состояний $|\psi_U(w)\rangle$ в вычислительном базисе порождается двоичная последовательность u ($|u| = 2^s \log N$), представляющая информацию о числе выпадения каждой последовательности $v \in \{0,1\}^s$ в N экспериментах (v представляет базисное состояние $|v\rangle$.

Отметим, что результаты измерений могут отличаться при повторении серии N измерений состояния $|\psi_U(w)\rangle$. Другими словами, соответствие $w \mapsto_U u$ является отношением (в программировании используют термин *недетерминированная функция*). Будем обозначать как $h_U^N(w)$.

4. Доказывается, что при подходящем выборе меры близости для небольших значений s, N выполняется следующее:

• для различных w, $w' \in \{0,1\}^n$ при равновероятностном выборе U значения $h_U^N(w)$ и $h_U^N(w')$ хорошо отличимы друг от друга (теорема 3).

Перечисленные свойства квантовой процедуры позволяют говорить о порождении универсального семейства $\mathcal{F}$ недетерминированных хеш-функций.

1.1. Обозначения и соглашения. Множество последовательностей (слов) $\{0,1\}^n$ одновременно считаем числами-элементами $\mathbb{Z}_q$ для $q = 2^n$.

Понятие «кубит», обозначения квантового состояния $|\psi\rangle$, пространства $(\mathcal{H}^2)^{\otimes s}$ s-кубитных состояний, вычислительный базис $|0\rangle, |2\rangle \ldots, |2^s - 1\rangle$, или другое обозначение $\{|v\rangle : v \in \{0,1\}^s\}$, используемые в настоящей работе, определяются, например, в работе [10].

Для матрицы A обозначим как $\|A\|_{\mathrm{tr}}$ следовую норму (trace norm) A: $\|A\|_{\mathrm{tr}} = \frac{1}{2}\operatorname{Tr}\sqrt{A^\dagger A}$ и как $\|A\|_F$ норму Фробениуса A: $\|A\|_F = \sqrt{\operatorname{Tr} A^* A}$.

Для равновероятного выбора унитарного преобразования U из множества $\mathcal{U}(n)$ всех унитарных матриц размера $n \times n$ используется мера Хаара μ [11] – единственная (с точностью до умножения на константу) мера на $\mathcal{U}(n)$, инвариантная относительно умножения на унитарные матрицы. Если случайная величина U_n равновероятно принимает значения из $\mathcal{U}(n)$, то для произвольного $H \subset \mathcal{U}(n)$ выполняется $\Pr[U_n \in H] = \mu(H)$.

2. Основные квантовые процедуры и их анализ

В этом разделе конструируется хэш-функция на основе квантовой функции, реализуемой квантовой вычислительной моделью. Вычисляется квантовый хэш-образ, а затем он преобразуется в классическую последовательность битов. Таким образом, можно считать, что *деквантизированная хэш-функция* отображает классическое входное значение в распределение вероятности на классических выходных значениях.

2.1. Квантовая хеш-функция $\psi_{q,B}$. Напомним необходимые определения квантовой однонаправленной (односторонней) и устойчивой к коллизиям функции [10].

Однонаправленность (*односторонность*). Пусть X является случайной переменной над множеством $\mathbb{X}$ $\{Pr[X = w] : w \in \mathbb{X}\}$. Пусть $\psi : \mathbb{X} \to (\mathcal{H}^2)^{\otimes s}$ является квантовой функцией. Пусть Y является произвольной случайной переменной над $\mathbb{X}$, полученной каким-либо способом $\mathbf{M}$ выполнения измерений состояния ψ, в котором закодировано X, и с результатом в $\mathbb{X}$. Пусть $\delta > 0$. Будем называть квантовую функцию ψ односторонней δ-устойчивой, если

1) её легко вычислить, то есть квантовое состояние $|\psi(w)\rangle$ для заданного $w \in \mathbb{X}$ может быть вычислено полиномиальным по времени алгоритмом;

2) для любого механизма $\mathbf{M}$ вероятность $Pr[Y = X]$ того, что $\mathbf{M}$ успешно декодирует Y, ограничена величиной δ

$$Pr[Y = X] \le \delta.$$

Устойчивость к коллизиям. Пусть $\epsilon > 0$. Будем называть квантовую функцию $\psi : \mathbb{X} \to (\mathcal{H}^2)^{\otimes s}$ ϵ-устойчивой к коллизиям функцией, если для любой пары w, w' различных входных значений выполняется неравенство

$$|\langle \psi(w) \,|\, \psi(w')\rangle| \le \epsilon.$$

Определение. Квантовая функция $\psi : \mathbb{X} \to (\mathcal{H}^2)^{\otimes s}$ является (δ, ϵ)-квантовой хэш-функцией (к.х.ф.), если

- ψ является δ-односторонней;
- ψ является ϵ-устойчивой к коллизиям.

Конструкции квантовых хэш-функций, описание их свойств и возможные их применения представлены в [10].

Здесь мы будем использовать функцию, взятую из [12]. Для $q = 2^n$, для множества $B = \{b_i : b_i \in \{0, \ldots, q-1\}\}$ квантовую функцию

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

где $s = \log|B| + 1$, определим следующим образом. Для $w \in \{0,1\}^n$ полагаем

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

Теорема 1. *Для произвольного $\epsilon > 0$ существует множество $B \subset \mathbb{Z}_q$ такое, что $|B| = \lceil (2/\epsilon^2)\ln(2q) \rceil = (2/\epsilon^2)(n+1)$, и функция*

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

где $s = \log|B| + 1 = \log(n+1) + \log(2/\epsilon^2)$, является (δ, ϵ)-квантовой хеш-функцией с $\delta = |B|/q$.

2.2. Функция f_ψ на основе квантовой хеш-функции ψ. Функцию

$$f_\psi : \{0,1\}^n \to \mathbb{R}^{2^s}$$

определим следующим образом. Запишем функцию ψ в виде

$$\psi(w) = \sum_{v \in \{0,1\}^s} a_v(w)|v\rangle$$

и положим $p_v(w) = |a_v(w)|^2$ для $v \in \{0,1\}^s$. Согласно постулату Бора $p_v(w)$ – это вероятность обнаружить квантовое состояние $|\psi(w)\rangle$ в базисном состоянии $|v\rangle$ при измерении $\mathcal{M}$ состояния $|\psi(w)\rangle$ в вычислительном базисе. Другими словами, $p_v(w)$ – это вероятность получить двоичную последовательность v в результате измерения $\mathcal{M}$.

Положим

$$f_\psi : w \mapsto \{p_v(w) : v \in \{0,1\}^s\}. \tag{2}$$

Значением $f_\psi(w)$ функции f_ψ является вектор распределения вероятностей последовательностей $v \in \{0,1\}^s$ – результат преобразования w квантовым хеш-отображением ψ.

2.3. Квантовая процедура приближения функции f_ψ. Мы предполагаем наличие квантовой вычислительной модели, которая может реализовать квантовую ветвящуюся программу QBB [12], реализующую функцию ψ. Для $w \in \{0,1\}^n$ такая программа QBB_ψ реализует отображение

$$QBB_\psi : w \mapsto |\psi(w)\rangle.$$

2.4. Процедура QP^N приближения значений функции f_ψ. Обозначим через QP^N квантовую процедуру, состоящую из N применений к словам $w \in \{0,1\}^n$ последовательно процедуры QBB_ψ и далее измерения $\mathcal{M}$. Результатом процедуры $QP^N(w)$ является распределение частот

$$P^N(w) = (P^N_{0\ldots0}(w), \ldots, p^N_v(w), \ldots p^N_{1\ldots1}(w)),$$

или

$$P^N(w) = \{p^N_v(w) : v \in \{0,1\}^s\}, \tag{3}$$

выпадения $v \in \{0,1\}^s$, то есть $p^N_v(w) = k(v)/N$, где $k(v)$ – число выпадений базисного состояния $|v\rangle$ при измерениях N копий квантового состояния $|\psi(w)\rangle$. На основе (3) будем использовать обозначение

$$u(w) = \left\{ k_v(w) : v \in \{0,1\}^s \right\}, \tag{4}$$

где $k_v(w)$ – число выпадений базисного состояния v при измерении N копий состояния $|\psi(w)\rangle$.

Последовательность $u(w)$ – это двоичная последовательность длины $2^s \log N$ – результат квантовой процедуры QP^N по обработке исходной последовательности w. Отметим, что результаты измерений $\mathcal{M}$ могут отличаться при повторении серии N измерений состояния $|\psi(w)\rangle$.

2.5. Необходимое количество N копий состояний $|\psi\rangle$: анализ. Предполагаем, что в нашем распоряжении имеется квантовая процедура, которая может подготовить большое количество копий квантового хэш-состояния $|\psi(w)\rangle \in (\mathcal{H}^2)^{\otimes s}$ и измерить их в вычислительном базисе $|1\rangle, |2\rangle \ldots, |2^s\rangle$. Каково количество N копий, чтобы достоверно отличить различные состояния? Мы используем результат работы [13], в которой описывается решение задачи идентификации квантовых состояний. Задача идентификации формулируется так:

По заданному состоянию $|\psi_i\rangle$ из заранее известного ансамбля

$$\mathcal{E} = \{|\psi_1\rangle, \ldots, |\psi_m\rangle\}$$

чистых состояний в $(\mathcal{H}^2)^{\otimes s}$ определить i.

Ответ на этот вопрос даёт следующая

Теорема 2. *Пусть*

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

ϵ-устойчивая к коллизиям квантовая хэш-функция.

Пусть N является числом измерений в вычислительном базисе удовлетворяющее требованию: имея N копий состояния $|\psi(w)\rangle$, возможно идентифицировать w с вероятностью $3/4$.

Тогда

$$N \le O\Big(\frac{1}{(1-\epsilon)^2}\Big)n.$$

Доказательство. Доказательство теоремы заключается в применении и анализе алгоритма идентификации $\mathcal{A}$ [13]. В нашем случае алгоритм $\mathcal{A}$ основывается на квантовой процедуре QP^N. При этом алгоритм $\mathcal{A}$ производит измерения результата (хеш-состояния) $|\psi(w)\rangle$ в случайном базисе. Измерение будем производить в вычислительном базисе, а «случайность» выбора базиса «переносим» на «пост-преобразование» квантового хеша $|\psi(w)\rangle$ случайным унитарным преобразованием U.

Мы применяем следующее свойство, сформулированное в удобном для наших рассуждений виде.

Свойство 1. *Пусть*

$$\mathcal{E} = \{|\psi(w)\rangle : w \in \{0,1\}^n\}$$

является множеством квантовых хешей (квантовых состояний), ϵ-устойчивых к коллизиям.

Тогда достаточно $N = c(\epsilon)n$ независимых копий состояния из ансамбля $\mathcal{E}$ для идентификации состояния с вероятностью, не меньшей $3/4$, и с использованием N повторов измерений в ортонормальном базисе пространства, выбранном случайным образом в соответствии с мерой Хаара. Этот базис является базисом пространства $(\mathcal{H}^2)^{\otimes s}$, дополненного вспомогательными кубитами.

Представим описание алгоритма [13]. При этом будем следовать авторским обозначениям. Для этого положим $m = 2^n$, $S = 2^s$, а через σ будем обозначать квантовые состояния $|\psi\rangle$.

Алгоритм $\mathcal{A}$ идентификации состояния.

Показано [13], что при помощи одного POVM $\mathcal{M}$ можно получить полное вариационное расстояние не менее $c\|\sigma_i - \sigma_j\|_F$ между результатами измерения любой пары состояний σ_i, σ_j из $\mathcal{E}$, где c — константа, не зависящая от $\mathcal{E}$. На самом деле,

в качестве такого POVM можно взять случайный POVM $\mathcal{F}$ в $\mathbb{C}^S$, определённый следующим образом: добавим к состоянию вспомогательный регистр из $\mathbb{C}^k$, инициализированный нулевым состоянием, где $k = \Theta(S \log m)$, и измерим $\sigma_1 \otimes |0\rangle\langle 0|$, $\sigma_2 \otimes |0\rangle\langle 0|$ относительно случайного ортонормального базиса $\mathbb{C}^S \otimes \mathbb{C}^k$. Более того, так как максимальный ранг состояния из $\mathcal{E}$ и m не слишком велик, подходит также и случайный ортонормальный базис $\mathbb{C}^S$.

Теперь зафиксируем $1 \le i < j \le m$. При условии, что неизвестное состояние либо σ_i, либо σ_j, применим $\mathcal{M}$ к каждой из N копий неизвестного состояния, а затем используем процедуру оценки максимального правдоподобия для идентификации состояния с вероятностью успеха не меньше $1 - 1/4m$ (в соответствии со стандартной оценкой Чернова). Пусть F_{ij} является этой процедурой оценки максимального правдоподобия.

Алгоритм $\mathcal{A}$ идентификации состояния применяет $\mathcal{M}$ к каждой из N копий неизвестного состояния, которое априори может быть любым состоянием $\sigma_i \in \mathcal{E}$. После этого $\mathcal{A}$ выполняет $m - 1$ итерацию классической пост-обработки для нахождения минимального расстояния, сравнивая по два возможных состояния σ_i, σ_j на итерации, используя классические процедуры F_{ij} на N полученных исходах. Заметим, что в каждой из процедур F_{ij} «переиспользуются» те же самые N исходов, новых измерений не производится. Вероятность успеха пост-обработки и, соответственно, алгоритма $\mathcal{A}$, составляет не менее $1 - (m-1)/4m \ge 3/4$.

Обозначим через $\mathcal{E} = \{|\psi_1\rangle, \ldots, |\psi_m\rangle\}$ множество значений квантовой хэш-функции с минимальным попарным следовым расстоянием δ.

Пусть $\mathcal{U} = \{U\}$ – множество всех унитарных преобразований ($2^s \times 2^s$ унитарные матрицы). Матрицы $U \in \mathcal{U}$ выбираются равновероятностно в соответствии с мерой Хаара.

Пусть U является случайным преобразованием, выбранным случайным образом в соответствии с мерой Хаара. Положим

$$\mathcal{E}_U = \{U|\psi(w)\rangle : w \in \{0,1\}^n\} = \{|\psi'_1\rangle, \ldots |\psi'_{2^n}\rangle\}.$$

Наша задача заключается в следующем. Имея N копий состояния $|\psi'_i\rangle$ из неизвестного (случайного) множества $\mathcal{E}_U$, идентифицировать i, используя измерения в вычислительном базисе.

В нашем случае измерения выполняются в фиксированном (вычислительном) базисе, но случайное преобразование применяется к ансамблю. Легко видеть, что эта задача дуальна задаче из свойства 1, поэтому нам необходимо $N = O\big(\log m/\delta^2\big) = c(\epsilon)n$ копий для решения этой задачи. □

3. Классическое ϵ-универсальное хеш-семейство на основе квантовых процедур

В данном заключительном разделе интегрируются результаты предыдущего раздела и формулируется понятие ϵ-универсальное хеш-семейство на основе квантовых процедур.

Квантовая процедура $QBB_\psi - QP_U^N - \mathcal{A}$.

1. Последовательность $w \in \{0,1\}^n$ хешируется квантовой процедурой QBB_ψ Результатом является состояние $|\psi(w)\rangle$.

2. Равновероятностно (в соответствии с мерой Хаара) выбирается унитарное преобразование U.

Реализуется процедура PQ_U^N по обработке и измерении N копий состояния $|\psi_U(w)\rangle = |U\psi(w)\rangle$.

Результатом являются N последовательностей – результатов измерений $|\psi_U(w)\rangle$, которые объединяются в описание (двоичные последовательности u длины $|u| = 2^s \log N = O(n \log n)$) следующего вида:

$$u: \ u = (k_1, \ldots, k_{2^s}),$$

где k_i – число выпадений базисного состояния $|i\rangle$ в N экспериментах. Понятно, что в общем случае все N последовательностей различны.

3. Применяется алгоритм $\mathcal{A}$ – процедура идентификации. Эта процедура принимает на вход описание u результатов N измерений и возвращает номер i, $i \in \{1, \ldots, 2^n\}$, квантового состояния $|\psi_i\rangle$ такого, что $|\psi_i\rangle = |\psi_U(w)\rangle$.

Квантовая процедура $QBB_\psi - QP_U^N - \mathcal{A}$ порождает недетерминированную функцию

$$h_U^N: \ w \mapsto \{u : u = (k_1, \ldots, k_{2^s}), \mathcal{A}(u) = w\}.$$

На основе теорем 1 и 2 имеем следующее утверждение.

Теорема 3. *Для произвольной пары слов* $w \neq w'$

$$\Pr_U \left[u(w) \in h_U^N(w')\right] < \frac{1}{4}.$$

Теорема 3 дает основание следующему свойству. Зададим семейство $\mathcal{F}$ условием

$$\mathcal{F} = \{h_U^N : U \in \mathcal{U}\}.$$

Множество $\mathcal{F}$ является $1/4$-универсальным семейством недетерминированных хеш-функций в следующем смысле.

Пусть для произвольной последовательности $w \in \{0,1\}^n$ на основе квантовой процедуры порождения квантового хеша $|\psi(w)\rangle$ и применения процедуры $QBB_\psi - QP_U^N - \mathcal{A}$ получена последовательность u. Тогда вероятность Pr_{error} того, что u окажется последовательностью из области значений $h_U^N(w')$, для некоторого $w' \neq w$ не превосходит $1/4$:

$$Pr_{\text{error}} \leq 1/4.$$

Заключение

В последние годы несколько групп заявило, что они близки к достижению квантового превосходства [14–16]. Однако разрабатываемые ими квантовые компьютеры не связаны с квантовыми коммуникациями, и квантовые хэш-функции, предложенные в работах групп [10, 17, 18], не могут быть на них реализованы.

Подход к построению универсального семейства хеш-функций на основе квантовых процедур, изложенный в настоящей статье, с нашей точки зрения, позволит использовать квантовые процессы в криптографии и других прикладных областях.

Благодарности. Исследование выполнено за счет гранта Российского научного фонда (проект № 19-19-00656).

Литература

1. *Feynman R.P.* Quantum mechanical computers // Opt. News. – 1985. – V. 11, No 2. – P. 11–20. – doi: 10.1364/ON.11.2.000011.

2. *Манин Ю.И.* Вычислимое и невычислимое. – М.: Сов. радио, 1980. – 128 с.

3. *Shor P.W.* Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer // SIAM Rev. – 1999. – V. 41, No 2. – P. 303–332. – doi: 10.1137/S0036144598347011.

4. *Preskill J.* Quantum computing in the NISQ era and beyond // Quantum. – 2018. – V. 2. – P. 79. – doi: 10.22331/q-2018-08-06-79.

5. *Harrow A.W., Montanaro A.* Quantum computational supremacy // Nature. – 2017. – V. 549, No 7671. – P. 203–209. – doi: 10.1038/nature23458.

6. *Carter J.L, Wegman M.N.* Universal classes of hash functions // J. Comput. Syst. Sci. – 1979. – V. 18, No 2. – P. 143–154.

7. *Thorup M.* High speed hashing for integers and strings. – 2015. – arXiv:1504.06804.

8. *Stinson D.R., Paterson M.* Cryptography: Theory and Practice. – Chapman and Hall/CRC, 2018. – 598 p.

9. *Luby M., Wigderson A.* Pairwise independence and derandomization // Found. Trends Theor. Comput. Sci. – 2005. – V. 1, No 4. – P. 237–301. – doi: 10.1561/0400000009.

10. *Ablayev F., Ablayev M., Vasiliev A., Ziatdinov M.* Quantum fingerprinting and quantum hashing. Computational and cryptographical aspects // Balt. J. Mod. Comput. – 2016. – V. 4, No 4. – P. 860–875. – doi: 10.22364/bjmc.2016.4.4.17.

11. *Diestel J., Spalsbury A.* The Joys of Haar Measure. – Providence, RI: Am. Math. Soc., 2014. – xiv+320 p.

12. *Аблаев Ф.М., Васильев А.В.* Квантовое хеширование для квантовых коммуникаций. – Saarbrucken: LAMBERT Acad. Publ., 2015. – 84 с.

13. *Radhakrishnan J., Rötteler M., Sen P.* Random measurement bases, quantum state distinction and applications to the hidden subgroup problem // Algorithmica. – 2009. – V. 55, No 3. – P. 490–516. – doi: 10.1007/s00453-008-9231-x.

14. *Mohseni M., Read P., Neven H., Boixo S., Denchev V., Babbush R., Fowler A., Smelyanskiy V., Martinis J.* Commercialize quantum technologies in five years // Nature. – 2017. – V. 543, No 7644. – P. 171–174.

15. *Gambetta J.M., Chow J.M., Steffen M.* Building logical qubits in a superconducting quantum computing system // npj Quantum Inf. – 2017. – V. 3. – Art. 2, P. 1–7. – doi: 10.1038/s41534-016-0004-0.

16. *Svore K., Geller A., Troyer M., Azariah J., Granade C., Heim B., Kliuchnikov V., Mykhailova M., Paz A., Roetteler M.* Q#: Enabling scalable quantum computing and development with a high-level DSL // RWDSL2018: Proc. Real World Domain Specific Languages Workshop 2018. – Vienna, 2018. – Art. 7, P. 1–10. – doi: 10.1145/3183895.3183901.

17. *Gottesman D., Chuang I.L.* Quantum digital signatures. – 2001. – arXiv:quant-ph/0105032.

18. *Gavinsky D., Ito T.* Quantum fingerprints that keep secrets // Electronic Colloquium on Computational Complexity. – 2010. – Report No. 165. – URL: https://eccc.weizmann.ac.il/report/2010/165/.

Поступила в редакцию
14.07.2020

Аблаев Фарид Мансурович, доктор физико-математических наук, главный научный сотрудник лаборатории нелинейной оптики; заведующий кафедрой теоретической кибернетики

Казанский физико-технический институт им. Е.К. Завойского ФИЦ Казанский научный центр РАН

ул. Сибирский тракт, д. 10/7, г. Казань, 420029, Россия

Казанский (Приволжский) федеральный университет

ул. Кремлевская, д. 18, г. Казань, 420008, Россия

E-mail: *fablayev@gmail.com*

Зиятдинов Мансур Тагирович, научный сотрудник лаборатории нелинейной оптики; научный сотрудник лаборатории «Квантовые методы обработки информации»
Казанский физико-технический институт им. Е.К. Завойского ФИЦ Казанский научный центр РАН
ул. Сибирский тракт, д. 10/7, г. Казань, 420029, Россия
Казанский (Приволжский) федеральный университет
ул. Кремлевская, д. 18, г. Казань, 420008, Россия
E-mail: *gltronred@gmail.com*

ISSN 2541-7746 (Print)
ISSN 2500-2198 (Online)

**UCHENYE ZAPISKI KAZANSKOGO UNIVERSITETA.
SERIYA FIZIKO-MATEMATICHESKIE NAUKI
(Proceedings of Kazan University. Physics and Mathematics Series)**

2020, vol. 162, no. 3, pp. 259–268

doi: 10.26907/2541-7746.2020.3.259-268

Universal Hash Functions from Quantum Procedures

F.M. Ablayev , M.T. Ziatdinov***

Zavoisky Physical-Technical Institute, FRC Kazan Scientific Center, Russian Academy of Sciences, Kazan, 420029 Russia
Kazan Federal University, Kazan, 420008 Russia
E-mail: **fablayev@gmail.com*, ***gltronred@gmail.com*

Received July 14, 2020

Abstract

Modern quantum technologies are NISQ (Noisy Intermediate-Scale Quantum) devices, which are used to create insufficiently accurate quantum computers with low computing power. However, quantum technologies have advanced considerably during the past years. Thus, the issue of demonstrating "quantum supremacy" in the era of NISQ technologies is on the agenda. This study demonstrates that "quantum supremacy" is forthcoming. We propose procedures for constructing a universal family of hash functions based on a quantum hashing process that maps the original sequence w to a quantum hash state and then by random transformation to the state $|\psi\rangle$ and generating the sequence u, which is an approximate description of the state $|\psi\rangle$. We proved that the proposed procedure generates a family of nondeterministic hash functions $\mathcal{F}$, which allow us to reliably distinguish between different arguments. The $\mathcal{F}$ family can be considered an ϵ-universal family of nondeterministic hash functions. We assume that the development of this research area will cast light on the effect of "quantum supremacy" and will also have a certain impact on the advance of post-quantum cryptography.

Keywords: quantum hash functions, universal hash family, quantum supremacy

Acknowledgments. The study was supported by the Russian Science Foundation (project no. 19-19-00656).

References

1. Feynman R.P. Quantum mechanical computers. *Opt. News*, 1985, vol. 11, no. 2, pp. 11–20. doi: 10.1364/ON.11.2.000011.
2. Manin Yu.I. *Vychislimoe i nevychislimoe* [Computable and Noncomputable]. Moscow, Sov. Radio, 1980. 128 p. (In Russian)

3. Shor P.W. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Rev.*, 1999, vol. 41, no. 2, pp. 303–332. doi: 10.1137/S0036144598347011.

4. Preskill J. Quantum computing in the NISQ era and beyond. *Quantum*, 2018, vol. 2, p. 79. doi: 10.22331/q-2018-08-06-79.

5. Harrow A.W., Montanaro A. Quantum computational supremacy. *Nature*, 2017, vol. 549, no. 7671, pp. 203–209. doi: 10.1038/nature23458.

6. Carter J.L, Wegman M.N. Universal classes of hash functions. *J. Comput. Syst. Sci.*, 1979, vol. 18, no. 2, pp. 143–154.

7. Thorup M. High speed hashing for integers and strings. 2015. arXiv:1504.06804.

8. Stinson D.R., Paterson M. *Cryptography: Theory and Practice*. Chapman and Hall/CRC, 2018. 598 p.

9. Luby M., Wigderson A. Pairwise independence and derandomization. In: *Found. Trends Theor. Comput. Sci.*, 2005, vol. 1, no. 4, pp. 237–301. doi: 10.1561/0400000009.

10. Ablayev F., Ablayev M., Vasiliev A., Ziatdinov M. Quantum fingerprinting and quantum hashing. Computational and cryptographical aspects. *Balt. J. Mod. Comput.*, 2016, vol. 4, no. 4, pp. 860–875. doi: 10.22364/bjmc.2016.4.4.17.

11. Diestel J., Spalsbury A. *The Joys of Haar Measure*. Providence, RI, Am. Math. Soc., 2014. xiv+320 p.

12. Ablayev F.M., Vasiliev A.V. *Kvantovoe kheshirovanie dlya kvantovykh kommunikatsii* [Quantum Hashing for Quantum Communications]. Saarbrucken, LAMBERT Acad. Publ., 2015. 84 p. (In Russian)

13. Radhakrishnan J., Rötteler M., Sen P. Random measurement bases, quantum state distinction and applications to the hidden subgroup problem. *Algorithmica*, 2009, vol. 55, no. 3, pp. 490–516. doi: 10.1007/s00453-008-9231-x.

14. Mohseni M., Read P., Neven H., Boixo S., Denchev V., Babbush R., Fowler A., Smelyanskiy V., Martinis J. Commercialize quantum technologies in five years. *Nature*, 2017, vol. 543, no. 7644, pp.171–174.

15. Gambetta J.M., Chow J.M., Steffen M. Building logical qubits in a superconducting quantum computing system. *npj Quantum Inf.*, 2017, vol. 3, art. 2, pp. 1–7. doi: 10.1038/s41534-016-0004-0.

16. Svore K., Geller A., Troyer M., Azariah J., Granade C., Heim B., Kliuchnikov V., Mykhailova M., Paz A., Roetteler M. Q#: Enabling scalable quantum computing and development with a high-level DSL. *RWDSL2018: Proc. Real World Domain Specific Languages Workshop 2018*. Vienna, 2018, art. 7, pp. 1–10. doi: 10.1145/3183895.3183901.

17. Gottesman D., Chuang I.L. Quantum digital signatures. 2001. arXiv:quant-ph/0105032.

18. Gavinsky D., Ito T. Quantum fingerprints that keep secrets. *Electronic Colloquium on Computational Complexity*, 2010, report no. 165. Available at: https://eccc.weizmann.ac.il/report/2010/165/.

⟨ ***Для цитирования*:** *Аблаев Ф.М., Зиятдинов М.Т.* Универсальное семейство хеш-функций на основе квантовых процедур // Учен. зап. Казан. ун-та. Сер. Физ.-матем. науки. – 2020. – Т. 162, кн. 3. – С. 259–268. – doi: 10.26907/2541-7746.2020.3.259-268. ⟩

⟨ ***For citation*:** Ablayev F.M., Ziatdinov M.T. Universal hash functions from quantum procedures. *Uchenye Zapiski Kazanskogo Universiteta. Seriya Fiziko-Matematicheskie Nauki*, 2020, vol. 162, no. 3, pp. 259–268. doi: 10.26907/2541-7746.2020.3.259-268. (In Russian) ⟩