Известия вузов. Математика *http://kpfu.ru/science/nauchnye-izdaniya/ivrm/*
2016, № 9, с. 68–73 *e-mail: izvuz.matem@kpfu.ru*

Краткое сообщение, представленное Н.К. Замовым

А.В. ВАСИЛЬЕВ

ДВОИЧНОЕ КВАНТОВОЕ ХЕШИРОВАНИЕ

Аннотация. Предлагается метод двоичного квантового хеширования, позволяющий представлять двоичные наборы в виде квантового состояния. Показаны криптографические свойства данного метода, включая устойчивость к коллизиям и устойчивость к восстановлению прообраза. Кроме того, предложен эффективный квантовый алгоритм построения квантовых хеш-кодов, что означает односторонность предлагаемой квантовой хеш-функции. Предлагаемая конструкция является асимптотически оптимальной по числу используемых квантовых бит.

Ключевые слова: квантовые вычисления, квантовая криптография, квантовое хеширование, линейные двоичные коды, квантовые ветвящиеся программы.

УДК: 519.7

Введение

Хеширование является чрезвычайно полезным приемом в информатике и используется в самых разнообразных приложениях, включая криптографические протоколы, алгоритмы быстрого поиска и проверку целостности данных. Недавно был предложен квантовый аналог данной техники [1], который может служить основой эффективных квантовых алгоритмов и защищенных квантовых коммуникационных протоколов. Так, рассмотрены применения квантового хеширования для эффективного вычисления некоторого класса булевых функций в модели квантовых ветвящихся программ [2] и приложение данной техники для вычисления булевых функций в квантовой коммуникационной модели [3]. Кроме того, известный протокол однобитовой квантовой цифровой подписи [4] основывается на использовании квантовой односторонней функции, в качестве которой можно использовать предложенную квантовую хеш-функцию [1].

В работе [5] рассмотрено обобщение предложенной ранее функции, позволяющее строить новые квантовые хеш-функции на основе комбинации произвольных классических универсальных хеш-семейств и некоторого специального семейства функций, называемого квантовым хеш-генератором. Известно, что классические универсальные хеш-семейства тесно связаны с кодами с исправлением ошибок – одно можно получить из другого [6]. Это дает возможность использования произвольных кодов с исправлением ошибок для получения новых квантовых хеш-функций.

Поступила 22.12.2015

Благодарности. Работа выполнена при финансовой поддержке Российского фонда фундаментальных исследований, гранты №№ 14-07-00878, 15-37-21160.

Как было показано ранее [1], основными свойствами квантовой хеш-функции являются эффективная вычислимость, устойчивость к восстановлению прообраза и устойчивость к коллизиям, причем все эти свойства тесно связаны.

В частности, свойства эффективной вычислимости и устойчивости к восстановлению прообраза часто объединяют в свойство односторонности — как и в классическом случае односторонняя функция должна быть эффективно вычислима, но сложна при вычислении прообраза.

В квантовом случае чаще всего прообраз и вовсе невозможно достоверно получить благодаря фундаментальному результату из области квантовой информации, известному как теорема Холево [7]. Из данной теоремы следует, что из s-кубитного состояния невозможно извлечь более $O(s)$ бит классической информации. Поэтому при построении квантовой хеш-функции требуется, чтобы размер получаемого квантового состояния был намного меньше (чаще всего экспоненциально меньше) исходного сообщения.

Кроме того, в работе [8] была проанализирована взаимосвязь описанных выше свойств квантовой хеш-функции. Показано, что свойства односторонности и устойчивости к коллизиям коррелируют: чем более устойчива квантовая хеш-функция к восстановлению прообраза, тем менее она устойчива к коллизиям и наоборот.

В данной работе предлагается новая квантовая хеш-функция, основанная на так называемых множествах с ε-отклонением [9]. Данный комбинаторный объект имеет ряд важных приложений в различных областях, таких как дерандомизация, теория графов, теория чисел и т. д. Для построения таких множеств используется их тесная связь с кодами, исправляющими ошибки, и соответствующие явные конструкции таких кодов [9]–[11]. Учитывая необходимость обеспечения криптографических свойств квантового хеширования, предлагаемая функция оказывается асимптотически оптимальной по размеру получаемых квантовых хеш-кодов.

1. Предварительные сведения

Данная работа основывается на определении квантовой хеш-функции и ее свойств из статьи [1]. При этом предлагаемая квантовая хеш-функция подразумевает преобразование классической информации в квантовые состояния, поэтому может быть эффективно реализована в вычислительных моделях с классическим управлением, например, в модели квантовых ветвящихся программ [12]. Для полноты изложения в данном разделе приведем необходимые определения.

1.1. **Квантовые ветвящиеся программы.**

Определение 1. Квантовая ветвящаяся программа Q над d-мерным гильбертовым пространством $\mathcal{H}^d$ – это тройка $Q = \big(|\psi_0\rangle, T, \mathrm{Accept}\big)$, где

- $|\psi\rangle \in \mathcal{H}^d$ — состояния (нормированные вектора из $\mathcal{H}^d$), $|\psi_0\rangle \in \mathcal{H}^d$ — начальное состояние;
- $T = (T_1, \ldots, T_\ell)$ — последовательность инструкций;
- каждая инструкция $T_j = \langle x_{i_j}, U_j(0), U_j(1)\rangle$ определяется переменной x_{i_j}, а $U_j(0)$ и $U_j(1)$ — унитарные преобразования в $\mathcal{H}^d$;
- j-й шаг: тестируется переменная x_{i_j} и выполняется переход в состояние $|\psi'\rangle = U_j(\sigma_{i_j})|\psi\rangle$;
- $\mathrm{Accept} \subset \{1, \ldots, d\}$ задает принимающее множество. После выполнения всех инструкций итоговое состояние измеряется, и входной набор принимается $\Longleftrightarrow$ результат измерения принадлежит Accept:

$$|\psi_0\rangle \xrightarrow{U_1(\sigma_{i_1})} \cdots |\psi\rangle \xrightarrow{U_j(\sigma_{i_j})} |\psi'\rangle \cdots \xrightarrow{U_\ell(\sigma_{i_\ell})} |\psi(\sigma)\rangle \longrightarrow \begin{cases}\text{Accept}\\ \text{Reject.}\end{cases}$$

Мерами сложности квантовой ветвящейся программы являются ее длина (количество инструкций) и ширина (размерность пространства состояний). Однако в данной работе будет применяться другая мера сложности — память, требуемая для хранения состояния квантовой ветвящейся программы, однозначным образом определяемая ее шириной. Длина же рассматриваться не будет, поскольку предлагаемые алгоритмы будут описаны в модели один раз читающих квантовых ветвящихся программ.

Определение 2. Квантовая ветвящаяся программа Q называется QOBDD или один раз читающей квантовой ветвящейся программой, если каждая переменная $x \in \{x_1, \ldots, x_n\}$ появляется в последовательности инструкций T программы Q не более одного раза.

Таким образом, длина один раз читающих квантовых ветвящихся программ не превышает длины входного набора и не может быть меньше числа существенных переменных вычисляемой функции.

Замечание 1. Отметим, что последовательные инструкции, считывающие одну и ту же переменную, можно склеить в одну, операторы которой будут произведениями соответствующих последовательностей унитарных операторов. Однако для наглядности не будем этого делать, при этом в оценках сложности такую последовательность инструкций будем учитывать как одну операцию.

1.2. **Квантовые хеш-функции.**

Определение 3. Классически-квантовой функцией будем называть функцию вида

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

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, описывающее состояния s кубит.

Согласно [4] классически-квантовая функция ψ называется квантовой односторонней функцией, если

- ее легко вычислять, т. е. существует алгоритм полиномиальной сложности, который на входном наборе w выдает значение $|\psi(w)\rangle$;
- тяжело обратить: имея лишь $|\psi(w)\rangle$, невозможно достоверно получить w.

Свойство 1. *Если $n \gg s$, то, имея лишь $|\psi(w)\rangle$, невозможно достоверно получить w.*

Схема доказательства. Необратимость функции квантового хеширования следует из теоремы Холево [7]. Так как из s кубит можно извлечь не более $O(s)$ бит классической информации, а $n \gg s$, то полностью восстановить w из $|\psi(w)\rangle$ невозможно. □

В определении квантовых односторонних функций явно не требуется наличие еще одного важного свойства, которое требуется для их практически значимых применений. Речь идет о возможности с высокой вероятностью различать образы квантовой односторонней функции. Как было показано в [1], это свойство можно определить следующим образом.

Определение 4. Назовем классически-квантовую функцию $\psi : \{0,1\}^n \to (\mathcal{H}^2)^{\otimes s}$ δ-устойчивой, если $|\langle \psi(w_1) \mid \psi(w_2)\rangle| < \delta$ для любой пары входных наборов w_1, w_2, $w_1 \neq w_2$.

Объединением приведенных выше определений стало понятие квантовой хеш-функции.

Определение 5. Назовем классически-квантовую функцию $\psi : \{0,1\}^n \to (\mathcal{H}^2)^{\otimes s}$ квантовой хеш-функцией, если она является квантовой односторонней и δ-устойчивой функцией.

1.3. **Множества с ε-отклонением.** Предлагаемый подход основан на важном комбинаторном объекте, называемом *множества с ε-отклонением* (в англоязычной литературе — ε-biased set). Приведем его определение согласно [11].

Определение 6. Множество $B \subseteq \{0,1\}^n$ называется множеством с ε-отклонением, если для любого непустого $I \subseteq \{1,\dots,n\}$

$$\frac{1}{|B|}\left|\sum_{b\in B}(-1)^{\sum_{i\in I} b_i}\right| \le \varepsilon.$$

Данное определение можно переформулировать эквивалентным образом, заменив произвольное множество индексов его характеристическим вектором.

Определение 7. Множество $B \subseteq \{0,1\}^n$ называется множеством с ε-отклонением, если для любого $x \in \{0,1\}^n$, $x \neq 0$,

$$\frac{1}{|B|}\left|\sum_{b\in B}(-1)^{\sum_{i=1}^n b_i x_i}\right| \le \varepsilon.$$

Здесь суммирование в показателе степени ведется по модулю два.

Как было доказано в [13] существует такое множество с ε-отклонением B, что $|B| = O(n/\varepsilon^2)$, а в статье [11] приводится явная конструкция размера $O(n/(\varepsilon^2\log(1/\varepsilon)))^{5/4}$, основанная на алгебраических кодах. Данная конструкция основывается на тесной связи между множествами с ε-отклонением и так называемыми ε-сбалансированными линейными кодами с исправлением ошибок.

Определение 8. Линейный код $C : \{0,1\}^n \to \{0,1\}^m$ для сообщений длины n и блоков длины m называется ε-сбалансированным, если вес любого ненулевого кодового слова $C(x)$ находится в диапазоне $\left(\frac{1}{2}-\varepsilon\right)m$ и $\left(\frac{1}{2}+\varepsilon\right)m$.

Поскольку C является двоичным линейным кодом, его порождающая матрица A с элементами из $\mathbb{F}_2$ имеет размер $(n \times m)$, и $C(x) = x \cdot A$.

Известно [11], что мультимножество $B \subset \{0,1\}^n$ является множеством с ε-отклонением тогда и только тогда, когда ε-сбалансированным является линейный код C_B, порождающая матрица которого состоит из элементов B.

2. Двоичное квантовое хеширование

Для дальнейших построений зафиксируем $\varepsilon \in (0,1)$ и предположим, что $B = \{b_1, b_2, \dots\} \subseteq \{0,1\}^n$ является множеством с ε-отклонением.

Определение 9. Определим классически-квантовую функцию $\psi_B : \{0,1\}^n \to (\mathcal{H}^2)^{\otimes(\log|B|)}$ для входного набора $w \in \{0,1\}^n$

$$|\psi_B(w)\rangle = \frac{1}{\sqrt{|B|}}\sum_{i=1}^{|B|}(-1)^{\sum_{j=1}^n b_{ij}w_j}|i\rangle,$$

где b_{ij} — это j-й элемент двоичного набора $b_i \in B$, а суммирование в показателе степени ведется по модулю два.

Теорема. *Функция ψ_B является ε-устойчивой квантовой хеш-функцией.*

Идея доказательства заключается в демонстрации устойчивости к коллизиям и устойчивости к восстановлению прообраза у функции ψ_B на основе свойств множества с ε-отклонением B. Также предлагается эффективный квантовый алгоритм построения квантовых хеш-кодов в модели один раз читающих квантовых ветвящихся программ.

Замечание 2. Заметим, что размер образа квантовой хеш-функции ψ_B является асимптотически оптимальным ввиду известной нижней оценки из работы [14] на размер множеств попарно различимых квантовых состояний. Так, чтобы получить множество из 2^n квантовых состояний, попарное скалярное произведение которых ограничено ε, необходимо как минимум $\Omega(\log(n/\varepsilon))$ кубит. Поскольку при квантовом хешировании необходимо сопоставить различимые квантовые состояния всем 2^n двоичным наборам, эта оценка влечет нижнюю оценку $\Omega(\log n - \log \varepsilon)$ на размер образа ε-устойчивой квантовой хеш-функции. При этом существование множества B размера $O(n/\varepsilon^2)$ обеспечивает верхнюю оценку $O(\log n - \log \varepsilon)$ на размер образа предлагаемой квантовой хеш-функции.

3. Сравнение с квантовой функцией отпечатков

Авторы работы [14] определили квантовую одностороннюю функцию

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

на двоичных словах $u \in \{0,1\}^n$, основанную на двоичных кодах с исправлением ошибок (конкретно на коде Джастесена) $E : \{0,1\}^n \mapsto \{0,1\}^m$. Образы данной функции назвали квантовыми отпечатками (quantum fingerprints), которые являются квантовыми состояниями вида

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

где $m = cn$, и $E_i(u)$ обозначает i-й бит $E(u)$.

Из работы [14] следует, что данная функция обладает следующим свойством.

Свойство 2. *Пусть d — это кодовое расстояние для кода E, $\delta = 1 - d/m$. Тогда квантовая функция отпечатков f_E является δ-устойчивой квантовой хеш-функцией.*

Сравнивая данную функцию с предлагаемой квантовой хеш-функцией можно заметить, что при использовании одного и того же ε-сбалансированного кода квантовая функция отпечатков обладает меньшей устойчивостью к квантовым коллизиям. Как было показано выше, предложенная квантовая хеш-функция имеет оценку ε, в то время как у квантовой функции отпечатков она равна $\delta = 1/2 + \varepsilon$.

Литература

[1] Ablayev F.M. *Cryptographic quantum hashing*, Laser Physics Letters **11** (2), 025202 (2014), http://stacks.iop.org/1612-202X/11/i=2/a=025202.

[2] Ablayev F. *Computing Boolean functions via quantum hashing*, in: Computing with New Resources, Ed. by C.S. Calude, R. Freivalds, I. Kazuo. Lecture Notes in Computer Science (Springer International Publishing, 2014), 149–160, http://dx.doi.org/10.1007/978-3-319-13350-8_11.

[3] Vasiliev A. *Quantum communications based on quantum hashing*, International J. Appl. Engineering Research **10** (12), 31415–31426 (2015).

[4] Gottesman D. *Quantum digital signatures*, Tech. Rep. arXiv:quant-ph/0105032, Cornell University Library, Nov. 2001, http://arxiv.org/abs/quant-ph/0105032.

[5] Ablayev F. *Quantum hashing via ε-universal hashing constructions and classical fingerprinting*, Lobachevskii J. Math. **36** (2), 89–96 (2015), http://link.springer.com/10.1134/S199508021502002X.

[6] Stinson, D.R. *On the connections between universal hashing, combinatorial designs and error-correcting codes* in: Proc. Congressus Numerantium **114**, 7–27 (1996).
[7] Холево А.С. *Некоторые оценки для количества информации, передаваемого квантовым каналом связи*, Пробл. передачи информ. **9** (3), 3–11 (1973).
[8] Ablayev F. *On the concept of cryptographic quantum hashing*, Laser Physics Letters **12** (12), 125204 (2015), http://stacks.iop.org/1612-202X/12/i=12/a=125204.
[9] Naor J. *Small-bias probability spaces*: *Effcient constructions and applications*, Proceedings of the twenty second annual ACM Symposium on Theory of Computing STOC'90 (New York, NY, USA, ACM, 1990), 213–223, http://doi.acm.org/10.1145/100216.100244.
[10] Alon N., Goldreich O., Hastad J., Peralta R. *Simple constructions of almost k-wise independent random variables*, Random Structures & Algorithms **3** (3), 289–304 (1992), http://dx.doi.org/10.1002/rsa.3240030308.
[11] Ben-Aroya A. *Constructing small-bias sets from algebraic-geometric codes*, 50th Annual IEEE Symposium Foundations of Computer Science FOCS'09 (Oct. 2009), 191–197.
[12] Ablayev F. *On computational power of quantum branching programs*, Fundamentals of computation theory (Riga, 2001), 59–70, Lecture Notes in Comput. Sci. (Springer, Berlin, 2001), Vol. 2138.
[13] Alon N. *Random Cayley graphs and expanders*, Random Structures & Algorithms **5** (2), 271–284 (1994), http://dx.doi.org/10.1002/rsa.3240050203.
[14] Buhrman H., Cleve R., Watrous J., deWolf R. *Quantum fingerprinting*, Phys. Rev. Lett. **87** (16), 167902 (2001), www.arXiv.org/quant-ph/0102001v1.

А.В. Васильев
Казанский (Приволжский) федеральный университет,
ул. Кремлевская, д. 18, г. Казань, 420008, Россия,
e-mail: Alexander.KSU@gmail.com

A.V. Vasiliev

Binary quantum hashing

Abstract. We propose a binary quantum hashing technique that allows to present binary inputs by quantum states. We prove the cryptographic properties of the quantum hashing, including its collision resistance and preimage resistance. We also give an efficient quantum algorithm that performs quantum hashing, and altogether this means that this function is quantum one-way. The proposed construction is asymptotically optimal in the number of qubits used.

Keywords: quantum computation, quantum cryptography, quantum hashing, binary linear codes, quantum branching programs.

A.V. Vasiliev
Kazan (Volga Region) Federal University,
18 Kremlyovskaya str., Kazan, 420008 Russia,
e-mail: Alexander.KSU@gmail.com