На правах рукописи

АБЛАЕВ МАРАТ ФАРИДОВИЧ

КВАНТОВОЕ ХЕШИРОВАНИЕ: ОСНОВНЫЕ СВОЙСТВА, ЭФФЕКТИВНЫЕ КОНСТРУКЦИИ

01.01.09 — Дискретная математика и математическая кибернетика

Автореферат

на соискание ученой степени

кандидата физико-математических наук

Казань – 2022

Работа выполнена на кафедре теоретической кибернетики
Казанского (Приволжского) федерального университета

Научный руководитель: **Александр Валерьевич Васильев**
кандидат физико-математических наук,
доцент, КФУ

Официальные оппоненты: **Сергей Андреевич Ложкин**
доктор физико-математических наук,
профессор, Зав. Каф. Мат. кибернетики МГУ

Наркис Мусавирович Арсланов
кандидат физико-математических наук,
Зав. лаб. интегральной квантовой оптики,
Казанский квантовый центр. КНИТУ (КАИ)

Ведущая организация: Физико-технологический институт
им. К.А.Валиева РАН

Защита состоится 31 мая 2022 г. в 14.00 часов на заседании диссертационного совета КФУ.01.04 при ФГАОУ ВО «Казанский (Приволжский) федеральный университет» по адресу: 420008, г. Казань, ул. Кремлевская, д. 35, ауд. 612.

С диссертацией можно ознакомиться в Научной библиотеке им. Н.И. Лобачевского ФГАОУ ВО «Казанский (Приволжский) федеральный университет»и на официальном сайте КФУ.

Отзывы на автореферат в двух экземплярах, заверенные печатью учреждения, просьба направлять по адресу: 420008, г. Казань, ул. Кремлевская, д. 35, ученому секретарю диссертационного совета КФУ.01.04

Автореферат разослан 5 апреля 2022 года.

Ученый секретарь
диссертационного Совета КФУ.01.04
канд. физ.-мат. наук,
доцент Ильин Сергей Николаевич

Актуальность темы.

Теория и практика квантовых вычислений и квантовая передача информации – это направления квантовой информатики, активно развиваемые в последние десятилетия. Наиболее известными результатами в области квантовой криптографии на сегодняшний день являются протоколы квантовой выработки ключа (Quantum Key Distribution — QKD). В большинстве случаев сегодня под термином квантовая криптография понимаются именно QKD исследования и эти исследования составляют львиную долю работ в области квантовой криптографии. QKD работы начались в 1984 году с протокола BB84 (Bennett, Brassard) и продолжают интенсивно развиваются в наши дни. Это направление является в большей степени направлением прикладной квантовой механики — квантовой инженерии. Весомые результаты мирового уровня получены в этом направлении в России.

Серьезными достижениями алгоритмической квантовой криптографии и пожалуй наиболее известными результатами квантовой информатики являются быстрые (полиномиальные по времени) квантовый алгоритм разложения числа на простые множители и алгоритм нахождения дискретного логарифма Питера Шора 1994.

Криптографическое сообщество в ответ на подобные потенциальные угрозы выработало и весьма интенсивно развивает направление постквантовая криптография (Daniel J. Bernstein. “Introduction to post-quantum cryptography”. Springer Berlin Heidelberg, Berlin, 2009). Направление пост квантовая криптография разрабатывает криптографические системы, которые должны стать трудными для будущих квантовых компьютеров и предлагает ряд направлений противодействия квантовым компьютерам. В частности, пост квантовая криптография предлагает защищенные системы передачи информации на основе хэш-функций.

Напомним, что хеш-функция $f : \Sigma^n \to \Sigma^m$ — это сжимающая словарная функция, отображающая длинные слова (длины n) в алфавите Σ в короткие (длины m, $n > m$). Криптография предъявляет ряд специальных требований к хэш-функциям, которые обусловлены требованиями противостояния атакам на передаваемую и хранимую информацию. К таким требования относятся однонаправленность и устойчивость к коллизиям.

Однонаправленность (one-way). Свойство однонаправленности означает, что значение $v = f(w)$ должно легко вычисляется по аргументу w, но по значению v аргумент w восстановить должно быть сложно. Важно отметить, что все используемые на сегодняшний день функции, для которых неизвестны быстрые алгоритмы их обращения, являются “условно однонаправленными”. Т.к. для них нет матема-

тических доказательств свойства однонаправленности. Сложность проблемы однонаправленности подчеркивает следующий факт. Известно, что доказательство свойства однонаправленности для некоей хеш-функции f будет означать доказательство свойства $P \neq NP$.

Коллизия устойчивость. Коллизией для сжимающей функции f называют ситуацию, когда выполняется $f(w) = f(v)$ для различных w и v. Понятно, что для сжимающих функций коллизии существуют. Коллизия устойчивость хеш-функции означает, что нахождение коллизий должно быть сложно.

В 2010-ые годы в исследовательской группе КФУ в области квантовых вычислений было определено понятие квантовой хэш-функции (F. Ablayev, A. Vasiliev. Cryptographic quantum hashing. Laser Physics Letters, 11(2):025202, 2014). Начаты исследования по определению области их применимости в области квантовых вычислений и в области квантовой криптографии.

Квантовая хеш-функция ψ отображает слова длины n в квантовые s-кубитные состояния. Оказалось, что если s много меньше n (например, в случае хороших квантовых хеш-функций выполняется $s = O(\log n)$), то законы квантовой механики гарантируют однонаправленность функции ψ.

Объект и предмет исследования. Объектом исследования диссертационной работы являются квантовые хеш-функции. Предметом исследования являются свойства квантовых хеш-функций и способы их генерации.

Цель работы. Разработка методов генерации оптимальных квантовых хеш-функций.

Задачи.

1. Доказательство нижней оценки числа кубит (применительно к квантовой хеш-функции) для задания коллизия устойчивой квантовой хеш-функции.

2. Разработка метода генерации квантовых хеш-функций

3. Построение различных квантовых хеш-функций

Основные положения, выносимые на защиту.

1. Дано геометрическое доказательство Теоремы о нижней оценки на число требуемых кубит для выбранного ϵ — показателя устойчивости к коллизиям.

2. Разработан метод генерации квантовых хеш-функций. Для чего:

- Введено понятие семейства функций, генерирующих квантовую хеш-функцию (генератор квантовой хеш-функции).
- Доказана теорема (Теорема о композиции) о генерировании новой квантовой хеш-функции композицией универсального хеш-семейства (классических) функций с генератором уже известной квантовой хеш-функции.

3. На основе Теоремы о композиции построены различные квантовые хеш-функции.

Теоретическая и практическая ценность. Диссертация имеет теоретический характер. Результаты могут найти применение в исследованиях по теории квантовых вычислений и квантовой криптографии, а также при разработке квантовых протоколов передачи информации.

Апробация работы. Основные результаты работы докладывались на более чем 15 международных конференциях: «CSR 2020: Computer Science in Russia 2020» (Екатиренбург, 2020), «International conference on quantum technologies PhysTech, Moscow Institute of Physics and Technology» (Москва, 2018), «The International Conference Micro-and Nanoelectronics (Москва, 2018), «International Workshop Kazan, Computation and cryptography with qu-bits» (Казань, 2017), XVIII Международная конференция "Проблемы теоретической кибернетики"(Пенза, 2017), «IV International Conference on Quantum Technologies» (Москва, 2017), «EMN Meeting on Quantum Matter. Energy Materials Nanotechnology» (Mauritius, 2016), «19th Conference on Quantum Information Processing» (Калгари, 2016), «Двенадцатый международный научный семинар Дискретная математика и ее приложения им. академика О. Б. Лупанова» (Москва, 2016), «IX Международная конференция "Дискретные модели в теории управляющих систем"(Москва, 2015), «3rd International Conference on Quantum Technologies» (Москва, 2015), International Conference on Computer Simulation in Physics and beyond, CSP 2015 (Москва, 2015), 4th International Conference on Quantum Cryptography, QCrypt 2014 (Париж, 2014).

Публикации по теме диссертации. По теме диссертации опубликовано 6 печатных работ. Результаты, выносимые не защиту, изложены в 5 статьях, опубликованных в рецензируемых научных изданиях, рекомендованных для защиты в диссертационном совете КФУ по специальности 01.01.09 — Дискретная математика и математическая кибернетикаи входящих в базы цитирования Scopus, Web of Science b RSCI.

Содержание работы. *Первая глава.* В первой главе представляются базовые понятия кубит, квантовый регистр и квантовое состояние регистра. Дается понятие преобразования регистра и квантового состояния. Дается понятие извлечения

информации из квантового состояния.

Вторая глава. Во второй главе определяются квантовые функции (функции, отображающие элементы конечных множеств в квантовые состояния). Определяются квантовые аналогии свойств однонаправленности (one-way) и коллизия устойчивости. В главе определяется понятие эффективной вычислимости квантовой функции на основе модели квантовой ветвящейся программы. Определяются и обсуждаются свойства однонаправленности.

Уточняется понятие ϵ-коллизия устойчивости квантовой хеш-функции и доказывается Теорема достаточное условие ϵ-коллизия устойчивости квантовой хеш-функции.

Представляется геометрическое доказательство (Теорема) нижней оценки на число требуемых кубит для выбранного ϵ — показателя устойчивости к коллизиям. Такого типа оценка в различных контекстах появлялась в литературе.

Третья глава. В третьей главе формулируется и доказывается Теорема о композиции. На основе Теоремы о композиции представляются новые конструкции квантовых хеш-функций и дается их анализ. Эти результаты являются основными результатом диссертационной работы:

Содержательно. Утверждение Теоремы о композиции предоставляет средство для конструирования различных квантовых хеш-функций на основе композиции (классических) семейств универсальных хеш-функций и известных квантовых хеш-функций.

Описание конструкций квантовых хеш-функций (утверждение Теоремы о композиции) опирается на понятие генерации квантовой хеш-функции семейством (классических) функций, определяемой в диссертационной работе.

Содержательно: семейство F функций генерирует квантовое состояние

$$|\psi\rangle = (\alpha_0 |0\rangle, \ldots, \alpha_{d-1} |d-1\rangle)^T$$

(является генератором состояния $|\psi\rangle$), если семейство F определяет амплитуды $\{\alpha_i : i \in \{0, \ldots, d-1\}\}$ состояния $|\psi\rangle$.

- Теорема о композиции утверждает, что, если F является универсальным хеш-семейством, а семейство H является генератором некоторой известной квантовой хеш функции, то их композиция $G = F \circ H$ (композиция семейств F и H) генерирует новую квантовую хеш-функцию.

Напомним, что N семейство $F = \{f_0, \ldots, f_{N-1}\}$ сжимающих функций, называется ϵ-универсальным хеш-семейством (или кратко — универсальным семейством

хеш-функций), если для двух различных аргументов w, w' функций из F существуют не более ϵN функций $f \in F$ таких, что $f(w) = f(w')$.

Более точно:

Пусть $F = \{f_0, \ldots, f_{N-1}\}$

$$f_i : \mathbb{X} \to \mathbb{Z}_q.$$

и $H = \{h_0, \ldots, h_{T-1}\}$

$$h_j : \mathbb{Z}_q \to \mathbb{Z}_q$$

являются семействами функций. Для $f \in F$ и $h \in H$, определим композицию $g = f \circ h$,

$$g : \mathbb{X} \to \mathbb{Z}_q,$$

условием

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

Определим композицию G семейств F и H следующим образом

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

Точное утверждение, сформулированное и доказанное в диссертации следующее.

Теорема 0.1 (Теорема о композиции)**.** *Пусть семейство*

$$F = \{f_0, \ldots, f_{N-1}\}$$

является ϵ_1-универсальным хеш–семейством, пусть $s_1 = \log N$. Пусть семейство

$$H = \{h_0, \ldots, h_{T-1}\}$$

генерирует квантовую коллизия ϵ_2-устойчивую хеш-функцию

$$\psi_H : \mathbb{Z}_q \to (\mathcal{H}^2)^{\otimes s_2}$$

для $s_2 = \log T + 1$ условием

$$\psi_H : v \mapsto |\psi_H(v)\rangle = \frac{1}{\sqrt{T}} \sum_{j=0}^{T-1} |j\rangle \left|\psi_{h_j}(v)\right\rangle.$$

Тогда композиция $G = F \circ H$ семейств F и H генерирует для $s = s_1 + s_2$ квантовую хеш-функцию

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

которая имеет вид

$$\psi_G : w \mapsto |\psi_G(w)\rangle = \frac{1}{\sqrt{NT}} \sum_{i=0}^{N-1} \sum_{j=0}^{T-1} |ij\rangle \left|\psi_{g_{ij}}(w)\right\rangle .$$

При этом квантовая функция ψ_G является квантовой (δ, ϵ)-хеш функцией с

$$\delta \leq 2^s/|\mathbb{X}| \quad \text{и} \quad \epsilon = \epsilon_1 + \epsilon_2.$$

В качестве следствия из Теоремы о композиции в последующей части главы 3 приводятся различные конструкции квантовых хеш-функций. В качестве исходного семейства H (семейства генератор квантовой хеш-функции) берется семейство $H_S = \{h_a(x) = ax : a \in S\}$, определяемое ϵ-biased подмножеством $S \subset \mathbb{Z}_q$ группы $\mathbb{Z}_q$. Конструкция квантовой хеш-функции (сокращенно квантовая хеш-функция Васильева) на основе ϵ-biased подмножеств предложена и исследована А. Васильевым (A. Vasiliev. Quantum hashing for finite abelian groups. *Lobachevskii Journal of Mathematics*, 37(6):751–754, 2016). В частности, доказано, что квантовые хеш-функции, порождаемые семейством H_S, являются *оптимальными* (в свете нижней оценки (оценки второй главы) на число кубит.

Далее новые генераторы квантовых хеш-функций — семейства G строятся как композиции $G = F \circ H_S$. В диссертации в качестве семейств F универсальных хеш-функций рассматриваются следующий три разных семейства функций.

1. Первое семейство F_M универсальных хеш-функций определяется основе семейства функций, применяемого в “технике отпечатков” Фрейвалда

   $$F_M = \{f_0, \ldots, f_{N-1}\}, \quad \text{где} \quad f_l(w) = w \mod p_l,$$

   $N = \pi(M)$ — число простых чисел не превосходящих M.

   Доказываются теоремы (Теорема для амплитудной формы хеш-функции и Теорема для фазовой формы хеш-функции), которые описывают конструкции квантовых хеш-функций, генерируемых семейством $G = F_M \circ H_S$.

   Утверждение Теоремы в фазовой форме в тектсе диссертации следующее:

   Теорема 0.2 (Фазовая форма)**.** *Пусть $c > 1$ произвольное положительное целое, положим $\epsilon_1 = 1/c$. Пусть $M = ck \ln k$, положим $N = \pi(M)$. Пусть число $q \in \{M, \ldots, 2M\}$ является простым. Пусть выбрано ϵ_1-универсальное семейство F_M.*

   $$F_M = \{f_0, \ldots, f_{N-1}\}, \quad \text{где} \quad f_l(w) = w \mod p_l,$$

N линейных функций.

Пусть для $q > 2$, $\epsilon_2 > 0$, $T = O((\log q)/\epsilon_2^2)$ множество $S \subseteq \mathbb{Z}_q$

$$S = \{a_0, \ldots, a_{T-1}\}$$

является множеством с ϵ_2-отклонением и определяет семейство (генератор)

$$H_S = \{h_j(x) : h_j(x) = a_j x \pmod q, \quad a_j \in S\}.$$

Тогда композиция $G = F_M \circ H_S$ генерирует для $s = \log N + \log T$ квантовую хеш-функцию

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

вида

$$|\psi_G(w)\rangle = \frac{1}{\sqrt{NT}} \sum_{l=0}^{N-1} \sum_{j=0}^{T-1} e^{i\frac{2\pi}{q} a_j f_l(x)} |lj\rangle .$$

При этом квантовая функция ψ_G является квантовой (δ, ϵ)-хеш функцией с

$$\delta \leq 2^s/|\mathbb{X}| \quad \text{и} \quad \epsilon = \epsilon_1 + \epsilon_2.$$

Доказывается, что такие квантовые хеш-функции *оптимальны* (в свете нижней оценки (оценки второй главы) на число кубит.

2. Второе семейство F_{lin} универсальных хеш-функций определяется основе семейства всех линейных функций

$$F_{lin} = \left\{ f_a : a \in (\mathbb{F}_q)^k, f_a(w) = \sum_{l=1}^{k} a_l w_l. \right\}$$

Доказываются теоремы (Теорема для амплитудной формы хеш-функции и Теорема для фазовой формы хеш-функции), которые описывают конструкции квантовых хеш-функций, генерируемых семейством $G = F_{lin} \circ H_S$.

Доказывается, что такие квантовые хеш-функции *не оптимальны* (в свете нижней оценки (оценки второй главы) на число кубит.

3. Третье большое семейство универсальных хеш-функций задается на основе линейных кодов, исправляющих ошибки. Отметим, что достаточно простой и мало известный факт связи семейств универсальных хеш-функций с линейными кодами, исправляющих ошибки был явно установлен в 1990-ые годы.

Доказываются общие теоремы (Теорема для амплитудной формы хеш-функции и Теорема для фазовой формы хеш-функции), которые описывают конструкции квантовых хеш-функций, генерируемых семейством $G = F_{\mathcal{C}} \circ H_S$. Здесь универсальное семейство $F_{\mathcal{C}}$ хеш-функций задается линейным кодом $\mathcal{C}$ исправляющим ошибки.

Общие теоремы (Теорема для амплитудной формы хеш-функции и Теорема для фазовой формы хеш-функции) конкретизируются для случая, когда в качестве линейного кода $\mathcal{C}$ исправляющего ошибки берется RS код (код Рида-Соломона).

Доказывается, что такие квантовые хеш-функции (на основе кода Рида-Соломона) *оптимальны* (в свете нижней оценки (оценки второй главы) на число кубит.

Точная формулировка утверждения теоремы в фазовой форме следующая.

Теорема 0.3 (Фазовая форма)**.** *Пусть для целого $k > 2$ (длины хешируемых слов), для целого $c > 2$ выбрано простое $q \in \{ck, \ldots, 2ck\}$.*

Пусть множество

$$F_{RS} = \{f_0, \ldots, f_{q-1}\} \quad c \quad f_a : \mathbb{F}_q^k \to \mathbb{F}_q \quad \text{вида} \quad f_a(w) = P_w(a)$$

является универсальным хеш–семейством, задаваемым RS-кодом. Пусть для $q > 2$, $\epsilon_2 > 0$, $T = O((\log q)/\epsilon_2^2)$ множество $S \subseteq \mathbb{Z}_q$

$$S = \{a_0, \ldots, a_{T-1}\}$$

является множеством с ϵ_2-отклонением и определяет семейство (генератор)

$$H_S = \{h_j(x) : h_j(x) = a_j x \pmod q, \quad a_j \in S\}.$$

Тогда композиция $G = F_{RS} \circ H_S$ семейств F_{RS} и H_S генерирует квантовую хеш-функцию

$$\psi_G : (_q)^k \to (\mathcal{H}^2)^{\otimes s}$$

для $s = \log q + \log T = O(\log(ck))$, которая задает s-кубитные квантовые состояния $|\psi_G(w)\rangle$ вида

$$|\psi_G(w)\rangle = \frac{1}{\sqrt{qT}} \sum_{l=0}^{q-1} \sum_{j=0}^{T-1} e^{i\frac{2\pi}{q} a_j P_w(l)} |lj\rangle .$$

При этом квантовая функция ψ_G является квантовой (δ, ϵ)-хеш функцией с

$$\delta \leq \frac{1}{(ck)^{k-O(1)}} \quad \text{и} \quad \epsilon \leq \frac{2}{c}.$$

Четвертая глава. В четвертой главе рассматривается вопрос реализации квантовых хеш-функций в модели квантовых ветвящихся программ (QBP). Реализация вычисления квантовой хеш-функции и организация протоколов на основе квантовых хеш-функций рассматривается на примере квантовой хеш-функции ψ_S — квантовой хеш-функции Васильева. для подходящего множества $S = \{a_0, \ldots, a_{T-1}\} \subset \mathbb{F}_q$ функция

$$\psi_S : \mathbb{F}_q \to (\mathcal{H}^2)^{\otimes s}$$

является квантовой хеш-функцией. Для $\omega = e^{i\frac{2\pi}{q}}$, для входа $x \in \mathbb{F}_q$ функция ψ_S определяет квантовое состояние

$$|\psi_S(x)\rangle = \frac{1}{\sqrt{T}} \sum_{j=0}^{T-1} \omega^{a_j x} |j\rangle .$$

Доказывается, что функция Васильева ψ_S достаточно просто реализуется в модели QBP.

В заключение текста диссертации подводится итог исследований и представленных результатов и перечисляются области дальнейших возможных исследований и приложений техники квантового хеширования.

Список работ Аблаева Марата Фаридовича, опубликованных по теме диссертации, которые входят в международные реферативные базы данных и системы цитирования(ВАК, Scopus / Web of Science):

1. Ablayev F. Quantum hashing via e-universal hashing constructions and classical fingerprinting / F. Ablayev, M. Ablayev // Lobachevskii Journal of Mathematics. - 2015. - Т.36, №2. - С.89-96

2. Ablayev M. On quantum (§, s)-resistant hashing // Lobachevskii Journal of Mathematics. - 2016. - Т.37, №6. - С.758-767

3. Ablayev M.F. Efficient branching programs for quantum hash functions generated by small-biased sets // Lobachevskii Journal of Mathematics. - 2018. - Т.39, №7. - С.961-966

4. Аблаев М.Ф. Квантовый поиск заданной подстроки в тексте на основе техники хеширования / Аблаев М.Ф., Салихова Н.М. // Ученые записки Казанского университета. Серия Физико-математические науки / Uchenye Zapiski Kazanskogo Universiteta. Seriya FizikoMatematicheskie Nauki. - 2020. - Т.162, кн. 3. - С.241-258

5. Аблаев М.Ф. К вопросу о квантовой функции, устойчивой к коллизиям // Ученые записки Казанского университета. Серия Физико- математические науки / Uchenye Zapiski Kazanskogo Universiteta. Seriya FizikoMatematicheskie Nauki. - 2021. - Т. 163, кн. 1. - С.90-94

6. Ablayev F. Quantum hashing and fingerprinting for quantum cryptography and computations / F. Ablayev, M. Ablayev, A Vasiliev //. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics). — 2020. — Volume 12159 LNCS. — P.1-15