УЧЕНЫЕ ЗАПИСКИ КАЗАНСКОГО УНИВЕРСИТЕТА.
СЕРИЯ ФИЗИКО-МАТЕМАТИЧЕСКИЕ НАУКИ

2021, Т. 163, кн. 1
С. 90–94

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

ОРИГИНАЛЬНАЯ СТАТЬЯ

УДК 519.7

doi: 10.26907/2541-7746.2021.1.90-94

К ВОПРОСУ О КВАНТОВОЙ ФУНКЦИИ, УСТОЙЧИВОЙ К КОЛЛИЗИЯМ

М.Ф. Аблаев

Федеральный исследовательский центр «Казанский научный центр Российской академии наук», г. Казань, 420111, Россия

Казанский (Приволжский) федеральный университет, г. Казань, 420008, Россия

Аннотация

Коллизией в классической теории хеширования называют случай совпадения значений функции при различных аргументах. В настоящей работе формулируется квантовый аналог свойства коллизии. Предлагается вариант формализации понятия квантовой функции, устойчивой к коллизиям. В рамках такой формализации доказывается теорема (достаточное условие) о квантовой функции, устойчивой к коллизиям.

Ключевые слова: квантовая криптография, квантовое хеширование, устойчивость к коллизиям

Введение

Хеширование широко применяется в различных областях информатики. В самом общем виде под хеш-функцией понимают сжимающие словарные функции (последовательности символов произвольной длины отображаются в конечные последовательности). При этом важную роль практически во всех областях применения хеширования играет проблема устойчивости к коллизии. А именно, важным является то, что коллизия должна находиться сложно. Под коллизией в хешировании понимается ситуация, когда значения хеш-функции на двух различных аргументах совпадают. Понятно, что в случае, когда рассматриваются сжимающие хеш-функции, коллизии гарантированно существуют. Хеш-функции, для которых нахождение коллизий является сложной (в том или ином смысле) задачей, называют функциями, устойчивыми к коллизиям.

Задача определения квантового варианта хеш-функции, устойчивой к коллизиям, и свойства такой функции рассматривались нами в работе [1]. В настоящей работе предлагается вариант формализации понятия квантовой функции, устойчивой к коллизиям. В рамках такой формализации доказывается теорема (достаточное условие) о квантовой функции, устойчивой к коллизиям.

Все обозначения, которые не определены в настоящей работе, определены в [1].

1. Устойчивость к коллизиям

Напомним, что алфавитом Σ называют конечное множество символов (букв), для целого k через Σ^k обозначают последовательности (слова) длины k в алфавите Σ, Функция

$$h : \Sigma^k \to \Sigma^m, \qquad k > m$$

называется сжимающей (отображает длинные слова длины k в короткие длины m). Для сжимающих функций коллизией называется ситуация, когда для разных

элементов w, $w' \in \Sigma^k$ выполняется $h(w) = h(w')$. Поскольку $k > m$, то коллизии гарантированно существуют.

Криптографические функции,устойчивые к коллизии, должны обладать следующими свойствами:

1) хеш-функция h должна быть стойкой к коллизиям первого рода: для заданного сообщения w должно быть «вычислительно сложно» подобрать другое сообщение v, для которого $h(w) = h(v)$;

2) хеш-функция h должна быть стойкой к коллизиям второго рода: должно быть «вычислительно сложно» подобрать пару сообщений (w, v) такую, что $h(w) = h(v)$;

3) функция h должна удовлетворять лавинному эффекту (avalanche effect): изменение одного символа аргумента должно вызывать изменение в среднем половины выходных символов (лавинное изменение).

В основе перечисленных свойств лежит тот факт, что коллизии реально существуют и имеется возможность сравнения значений функции.

2. Квантовая функция

Для конечного множества $\mathbb{X}$ и множества $(\mathcal{H}^2)^{\otimes s}$ квантовых s кубитных состояний взаимно однозначную функцию

$$\psi : \mathbb{X} \to (\mathcal{H}^2)^{\otimes s} \tag{1}$$

будем называть классически-квантовой (сокращенно просто квантовой) функцией. Такое определение квантовой функции удобно для определения понятия квантовой хеш-функции и рассмотрения ее свойств.

В качестве примера приведем следующую квантовую взаимно однозначную функцию. Пусть число $v \in \{0, \ldots, 2^n - 1\}$ отображается в кубит по правилу:

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

Здесь последовательность $v = v_0 \ldots v_{n-1}$ рассматривается как число $v = \sum_{j=0}^{n-1} v_j 2^j$.

3. Квантовая функция, устойчивая к коллизии

В нашем определении квантовой функции требуется взаимная однозначность. Это, в частности, означает, что коллизий в квантовом случае в классическом смысле не существует, то есть разные элементы w, $w' \in \mathbb{X}$ порождают различные квантовые состояния (образы) $|\psi(w)\rangle$ и $|\psi(w')\rangle$.

Тем не менее ситуация коллизии возникает, если по элементу $w \in \mathbb{X}$ порождено квантовое состояние $|\psi(w)\rangle$, а при извлечении информации из состояния (при измерении состояния) $|\psi(w)\rangle$ оно воспринимается наблюдателем как квантовое состояние $|\psi(w')\rangle$, порожденное другим элементом w'. Этот факт можно интерпретировать как появление коллизии. А именно, для элемента $w \in \mathbb{X}$ найден элемент $w' \in \mathbb{X}$ со свойством "$|\psi(w)\rangle = |\psi(w')\rangle$". В рамках сказанного предлагается следующая формализация.

• Определим событие $Collision_\psi(w, w')$ как событие, описанное выше: по элементу $w \in \mathbb{X}$ функцией ψ порождено квантовое состояние $|\psi(w)\rangle$, а при анализе состояния $|\psi(w)\rangle$ оно воспринимается как состояние $|\psi(w')\rangle$, порожденное элементом $w' \in \mathbb{X}$.

• Обозначим через $Pr(Collision_\psi(w, w'))$ вероятность события $Collision_\psi(w, w')$.

Определение 1. Для $\epsilon \in [0,1]$ будем говорить, что квантовая функция ψ ϵ-устойчива к коллизиям, если для двух произвольных элементов w, $w' \in \mathbb{X}$ выполняется

$$Pr(Collision_{\psi}(w,w')) \leq \epsilon.$$

• Далее будем говорить, что квантовая функция ψ ϵ-ортогональна (порождает ϵ-ортогональные состояния), если для двух произвольных элементов w, $w' \in \mathbb{X}$ выполняется

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

то есть абсолютная величина скалярного произведения двух квантовых состояний $|\psi(w)\rangle$ и $|\psi(w')\rangle$ ограничена сверху величиной ϵ.

В рамках такой формализации справедлива следующая теорема.

Теорема 1. *Если квантовая функция*

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

является ϵ-ортогональной квантовой функцией для $0 \leq \epsilon \leq 1$, то квантовая функция ψ является квантовой функцией, ϵ^2-устойчивой к коллизиям.

Доказательство. Вероятность $Pr(Collision_{\psi}(w,w'))$ такой коллизии определяем на основе закона Борна (см., например, книгу [2]). Закон Борна – один из ключевых принципов квантовой механики – позволяет вычислить вероятность того, что измерение квантовой системы позволит получить какой-либо результат. Закон Борна в формулировке книги [2] (разд. 9.2) гласит, что вероятность обнаружить систему в состоянии $|\phi\rangle$ при условии, что она была приготовлена в состоянии $|\psi\rangle$, задается квадратом модуля скалярного произведения этих состояний. Эту величину называют (в квантовой механике) фиделити (Fidelity)

$$F(|\phi\rangle,|\psi\rangle) = |\langle\phi|\psi\rangle|^2.$$

Величина F является вероятностью совпадения (степенью согласованности в терминах квантовой механики) неизвестного квантового состояния с известным. Такое событие совпадения может реализоваться при измерении квантового состояния.

М. Уайлдер [2] интерпретирует закон Борна в терминах квантовой передачи информации следующим образом.

• *Предположим, что нами приготовлено квантовое состояние $|\psi\rangle$, которое передается по квантовому каналу связи. В идеале мы хотели бы получить на выходе то же самое состояние, но предположим, что на выходе получено другое состояние $|\phi\rangle$. Фиделити $F(|\phi\rangle,|\psi\rangle)$ является мерой близости полученного состояния $|\phi\rangle$ к исходному состоянию $|\psi\rangle$.*

• *Фиделити $F(|\phi\rangle,|\psi\rangle)$ интерпретируется как вероятность события «состояние $|\phi\rangle$ будет принято за исходное состояние $|\psi\rangle$».*

Понятно, что аргументы функции F «перестановочны» $F(|\phi\rangle,|\psi\rangle) = F(|\psi\rangle,|\phi\rangle)$. В силу определения фиделити имеем

$$0 \leq F(|\phi\rangle,|\psi\rangle) \leq 1.$$

Понятно, что $F(|\phi\rangle,|\psi\rangle) = 0$, если неизвестное состояние $|\phi\rangle$ ортогонально заданному $|\psi\rangle$, и $F(|\phi\rangle,|\psi\rangle) = 1$, если состояния совпадают, то есть согласно закону Борна ортогональные квантовые состояния «идеально отличимы».

В силу закона Борна, его интерпретации в квантовой теории информации [2] и введенного обозначения $Pr(Collision_{\psi}(w,w'))$ справедливо неравенство

$$Pr(Collision_{\psi}(w,w')) = F(|\psi(w)\rangle,|\psi(w')\rangle) = |\langle\psi(w)|\psi(w')\rangle|^2 \leq \epsilon^2,$$

которое доказывает теорему. □

В качеств примера рассмотрим квантовую взаимно однозначную функцию, задаваемую двоичным кодом, исправляющим ошибки.

Код, исправляющий ошибки, задается отображением

$$E : \Sigma^k \to \Sigma^n$$

таким, что для всех (различных) слов w, $w' \in \Sigma^k$, их образов $E(w)$ и $E(w')$ выполняется следующее: хеммингово расстояние $d(E(w), E(w'))$ между $E(w)$ и $E(w')$ не менее d. Такой код E называют (n, k, d) кодом. Код называют двоичным, если $\Sigma = \{0, 1\}$.

В работе [1] рассматривается функция

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

задаваемая условием

$$|\psi_E(w)\rangle = \frac{1}{\sqrt{n}} \sum_{i=1}^{n} |i\rangle |E_i(w)\rangle,$$

где $E_i(w)$ – i-й бит кодового слова $E(w)$. Для функции ψ_E справедливо следующее [1].

Пусть $\epsilon < 1$. Пусть k, n – целые числа, а также пусть

$$E : \{0,1\}^k \to \{0,1\}^n$$

является (n, k, d)-двоичным кодом с $d \geq (1-\epsilon)n$. Тогда для функции ψ_E и произвольной пары различных слов w, $w' \in \{0,1\}^k$ выполняется

$$|\langle \psi_E(w) | \psi_E(w') \rangle| \leq \epsilon.$$

В силу теоремы 1 функция ψ_E является ϵ^2-устойчивой к коллизиям.

Благодарности. Работа выполнена в рамках государственного задания Министерства науки и высшего образования Российской Федерации (тема № АААА-А19-119011790156-3).

Литература

1. *Аблаев Ф.М., Аблаев М.Ф., Васильев А.В.* Универсальное квантовое хеширование // Учен. зап. Казан. ун-та. Сер. Физ.-матем. науки. – 2014. – Т. 156, кн. 3. – С. 7–18.
2. *Wilde M.M.* Quantum Information Theory. – Cambridge: Cambridge Univ. Press, 2017. – 776 p.

Поступила в редакцию
25.01.2021

Аблаев Марат Фаридович, научный сотрудник лаборатории квантовой оптики и информационных технологий; научный сотрудник лаборатории «Квантовые методы обработки информации»

Федеральный исследовательский центр «Казанский научный центр Российской академии наук»

ул. Лобачевского, д. 2/31, г. Казань, 420111, Россия

Казанский (Приволжский) федеральный университет

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

E-mail: *mablayev@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)**

2021, vol. 163, no. 1, pp. 90–94

ORIGINAL ARTICLE

doi: 10.26907/2541-7746.2021.1.90-94

On Quantum Collision Resistant Function

M.F. Ablayev

*Federal Research Center "Kazan Scientific Center
of the Russian Academy of Sciences", Kazan, 420111 Russia
Kazan Federal University, Kazan, 420008 Russia*
E-mail: *mablayev@gmail.com*

Received January 25, 2021

Abstract

In the classical hashing theory, collision is a coincidence of the values of a function with different arguments. This paper formulates a quantum analogue of the collision property. A variant of formalization of the concept of quantum function resistant to collisions was proposed. Within the framework of this formalization, the theorem (sufficient condition) on the quantum function that is resistant to collisions was proved.

Keywords: quantum cryptography, quantum hashing, resistance to collisions

Acknowledgments. This study was performed as part of the state assignment no. AAAA-A19-119011790156-3 of the Ministry of Science and Higher Education of the Russian Federation.

References

1. Ablayev F.M., Ablayev M.F., Vasilev A.V. Universal quantum hashing. *Uchenye Zapiski Kazanskogo Universiteta. Seriya Fiziko-Matematicheskie Nauki*, 2014, vol. 156, no. 3, pp. 7–18. (In Russian)
2. Wilde M.M. *Quantum Information Theory*. Cambridge, Cambridge Univ. Press, 2017. 776 p.

⟨ ***Для цитирования*:** *Аблаев М.Ф.* К вопросу о квантовой функции, устойчивой к коллизиям // Учен. зап. Казан. ун-та. Сер. Физ.-матем. науки. – 2021. – Т. 163, кн. 1. – С. 90–94. – doi: 10.26907/2541-7746.2021.1.90-94. ⟩

⟨ ***For citation*:** Ablayev M.F. On quantum collision resistant function. *Uchenye Zapiski Kazanskogo Universiteta. Seriya Fiziko-Matematicheskie Nauki*, 2021, vol. 163, no. 1, pp. 90–94. doi: 10.26907/2541-7746.2021.1.90-94. (In Russian) ⟩