Квантовое хеширование для безопасной передачи информации. Реализация квантовых хеш-функций на основе состояний высокой размерности

Фарид Аблаев Алексей Калачев

ФИЦ КНЦ РАН и КФУ

Научный совет РАН «Квантовые технологии»,
Март, 2022

Хеширование

Постквантовая криптография

- Post-quantum cryptography, 2009) Daniel J. Bernstein, Johannes Buchmann, Erik Dahmen (editors)
- Протоколы цифровой подписи, основанные на хешировании. Например, схема подписи Лампорта, схема подписи Меркле.

Криптографические хеш-функции

$$h : \Sigma^n \to \Sigma^m, \quad n > m$$

Требования:

- Функция h должна быть однонаправленная:
  – Легко вычислима, но сложно обратима

$$h(w) = v \text{ — легко}, \qquad w \in h^{-1}(v) \text{ — сложно}$$

- Функция h должна быть коллизия устойчивой:
  – Сложно найти w, v такие, что $h(w) = h(v)$
- Лавинный эффект:
  – изменение одного бита аргумента меняет половину бит значения

Протоколы на основе хеширования

Большие семейства протоколов аутентификации, цифровой подписи и т.д.

- Протокол идентификации пользователя:
  - Алиса и Боб:
    – открыто выбирают хеш-функцию h
    – секретно вырабатывают пароль w
    – Пользователь Алиса публично предъявляет $h(w)$ при входе в систему Боб.
    – Боб по хранящемуся у него паролю w проверяет $h(w) = h(w)$?
- Протоколы семейства “запрос-ответ” (свой-чужой)
- Подпись Лампорта
- Хеш-функции в блокчейн технологиях

Хеш-функция: однонаправленность (one-way)

Формализация

Хеш-функция $f : \Sigma^n \to \Sigma^m$ Однонаправленная, если

1. (легко вычислима:) существует полиномиальный алгоритм $\mathcal{M}$ для вычисления f.
2. (сложно обращаемая:) Для произвольного обращающего вероятностного полиномиального алгоритма M, для произвольного полинома $p(n)$ выполняется:

$$Pr[M(f(w)) \in f^{-1}(w)] < 1/p(n)$$

Теорема

Если однонаправленная функция существует, то $P \neq NP$.

Квантовое хеширование

Квантовая функция:

исходная информация (последовательности) отображается в квантовые состояния.

Требуемые свойства квантовой функции:

- Однонаправленность One-way function.
  Квантово однонаправленная.
- Коллизия устойчивость collision (almost) free.
  Квантовые состояния — образы различных последовательностей должны быть максимально различимы.

δ-обратимость

Декодирование (decoding) квантового состояния

$$\mathcal{D} : (\mathcal{H}^2)^{\otimes s} \to \Sigma^k$$

- $w \in \Sigma^k$
- $|\psi\rangle \in (\mathcal{H}^2)^{\otimes s}$
- Событие $\mathit{Decode}(\mathcal{D}(|\psi\rangle) = w)$: "$\mathcal{D}$ декодирует $|\psi\rangle$ в слово w".

δ-обратимость

Для $\delta > 0$ квантовая функция

$$\psi : \Sigma^k \to (\mathcal{H}^2)^{\otimes s}$$

δ-обратима, если для каждого $w \in \Sigma^k$, для декодирования $\mathcal{D}$

$$Pr[\mathit{Decode}(\mathcal{D}(|\psi(w)\rangle) = w)] \leq \delta.$$

Теорема Холево 1973. Теорема Nayak 1992 (δ-обратимость)

Теорема Холево 1973

устанавливает верхнюю границу на количество информации, которую можно узнать о квантовом состоянии (доступная информация).

Теорема (Nayak) 1992

- По k битовому слову w создается s кубитное состояние $|\psi(w)\rangle$.
- Состояние $|\psi(w)\rangle$ измеряется и далее переводится в k битовое слово v.

Вероятность $Pr[v = w]$ правильно декодировать состояние $|\psi(w)\rangle$

$$Pr[v = w] \leq \frac{2^s}{2^k}.$$

Квантовая коллизия устойчивость

Квантовая коллизия ϵ-устойчивость

Для $\epsilon > 0$ функция

$$\psi : \Sigma^k \to (\mathcal{H}^2)^{\otimes s}$$

коллизия ϵ-устойчива, если для различных w, w' выполняется

$$\left|\langle \psi(w) \mid \psi(w') \rangle\right| \leq \epsilon.$$

Коллизия устойчивость (Классическая)

1. Для w, $h(w)$ сложно найти v такое, что $h(w) = h(v)$.
2. Сложно найти w, v такие, что $h(w) = h(v)$.
3. Лавинный эффект (Avalanche effect).

Закон Борна 1926

- $|\psi\rangle$ – известное состояние. (порождает Alice)
- $|\phi\rangle$ – неизвестное состояние. (получает Bob)
- Fidelity $F(|\psi\rangle, |\phi\rangle)$ мера близости состояний $|\psi\rangle$ и $|\phi\rangle$.

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

Квантовая хеш-функция

Квантовая (δ, ϵ)-хеш-функция

$$\psi : \Sigma^k \to (\mathcal{H}^2)^{\otimes s}$$

- ψ "полиномиально-легко вычислима",
- ψ δ-обратима
- ψ Коллизия ϵ-устойчива:
  для произвольных $w, w' \in \Sigma^k$

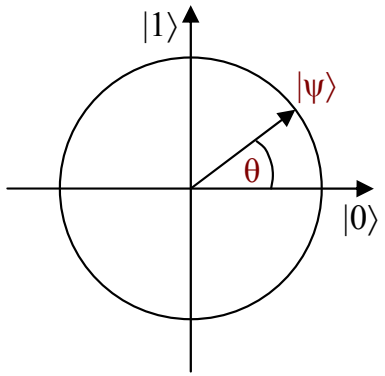
$$\left|\langle \psi(w) \mid \psi(w') \rangle\right| \leq \epsilon.$$

Пример 1: “ХОРОШАЯ” one-way и “ПЛОХАЯ” collision-free

Число $w \in \mathbb{Z}_q = \{0, \ldots, q-1\}$ отображается в кубит:

$$\psi : \mathbb{Z}_q \to \mathcal{H}^2$$

$$|\psi(w)\rangle = \cos\left(\frac{2\pi w}{q}\right)|0\rangle + \sin\left(\frac{2\pi w}{q}\right)|1\rangle,$$



Пример 2: “ПЛОХАЯ” one-way и “ХОРОШАЯ” collision-free

Число $x \in \{0, \ldots, 2^k - 1\}$ рассматриваем как слово $x \in \{0,1\}^k$.
Слово $x = x_1 \ldots x_k$ отображается в k кубит:

$$\psi : x = x_1 \ldots x_k \mapsto |\psi(x)\rangle = |x_1\rangle \otimes \cdots \otimes |x_k\rangle$$

QKD (BB84): “ПЛОХАЯ” one-way и “ХОРОШАЯ” collision-free

Alice begins with two strings of bits x and b

Binary KEY string:

$$x = x_1 \dots x_n$$

Binary RANDOM string:

$$b = b_1 \dots b_n.$$

Alice then encodes these two strings as a string of n qubits:

$$|\psi(x, b)\rangle = |\psi_{x_1 b_1}\rangle \otimes \cdots \otimes |\psi_{x_n b_n}\rangle.$$

Where

$$\text{C basis:} \quad |\psi_{00}\rangle = |0\rangle, |\psi_{10}\rangle = |1\rangle$$

$$\text{H basis:} \quad |\psi_{01}\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle, |\psi_{11}\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle.$$

Нижняя оценка на число s кубит для коллизия ϵ-устойчивой хеш-функции

Пусть

$$\psi : \Sigma^k \to (\mathcal{H}^2)^{\otimes s}$$

является коллизия ϵ-устойчивой. Тогда

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

ϵ-biased множество для конструкции квантовой хеш-функции

$\mathbb{Z}_q$ – аддитивная группа чисел по модулю q изоморфна мультипликативной группе μ_q корней из единицы. Отображение

$$\chi_a : \mathbb{Z}_q \to \mu_q, \qquad \chi_a(x) = e^{\frac{2\pi i}{q} ax} = \omega_q^{ax}$$

называют характером

Множество $S \subseteq \mathbb{Z}_q$ – ϵ-biased, если для каждого (нетривиального) характера $\chi \in \{\chi_a : a \in \mathbb{Z}_q\}$:

$$\frac{1}{|S|} \left| \sum_{x \in S} \chi(x) \right| \leq \epsilon.$$

Конструкция квантовой хеш-функции

Ben-Aroya, Ta-Shma: Constructing Small-Bias Sets from Algebraic Geometric Codes 2009:

Вероятностное множество $S \subset \mathbb{Z}_q$ мощности $t = O(\frac{\log q}{\epsilon^2})$ является ϵ-biased множеством с положительной вероятностью.

Конструкция

Для произвольного $\epsilon \in (0,1)$, для $t = O\left(\frac{\log q}{\epsilon^2}\right)$, и для $\delta = O\left(\frac{\log q}{\epsilon^2 q}\right)$ ϵ-biased множество $S = \{a_0, \ldots, a_{t-1}\} \subset \mathbb{Z}_q$, генерирует квантовую (δ, ϵ)-хеш-функцию ψ_S

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

Квантовый протокол на основе хеширования

Протокол идентификации пользователя:

- Алиса и Боб открыто выбирают хеш-функцию ψ
- Алиса и Боб секретно вырабатывают пароль w
- Алиса публично пересылает $|\psi(w)\rangle$ Бобу.
- Боб получает $|\psi\rangle$
- Боб по хранящемуся у него паролю w проверяет

$$|\psi(w)\rangle = |\psi\rangle ?$$

Реализация квантовой хеш-функции ψ_S

ϵ-biased множествО $S = \{a_0, \ldots, a_{t-1}\}$ мощности $t = O(\log q)/\epsilon^2$.

- Реализация ψ_S в случае s-qubit entangled state $s = \log t$

$$\psi_S : |0\rangle \quad \xrightarrow{x} \quad |\psi_S(x)\rangle = \frac{1}{\sqrt{2^s}} \sum_{j=0}^{t-1} e^{i\frac{2\pi}{q}xa_j} |\underbrace{j}_{s}\rangle$$

- Реализация ψ_S в случае t-мерного 1-quDIT

$$\psi_S : |0\rangle \quad \xrightarrow{x} \quad |\psi_S(x)\rangle = \frac{1}{\sqrt{t}} \sum_{j=0}^{t-1} e^{i\frac{2\pi}{q}xa_j} |j\rangle$$

- Реализация ψ_S в случае s-qubit non entangled state $s = t$

$$\psi_S : |0\rangle \quad \xrightarrow{x} \quad |\psi_S(x)\rangle = |\psi_1(x)\rangle \otimes \cdots \otimes |\psi_s(x)\rangle$$

Реализация квантовой хеш-функцийна основе состояний высокой размерности.

Phys. Rev. A 104, November 2021

D. Turaykhanov, D. Akat'ev, A. Vasiliev, F. Ablayev, A. Kalachev "Quantum hashing via single-photon states with orbital angular momentum"

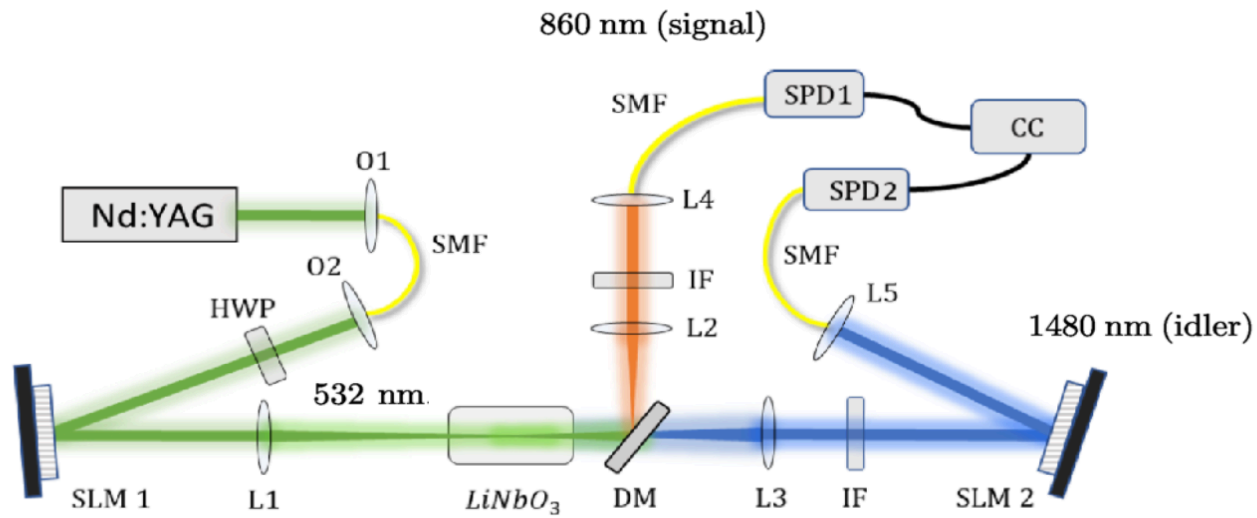
- Кванновая хеш-функция реализуется состояниями OAM.
- исходная последовательность (число) $x \in \{0, 1, \ldots, q-1\}$ отображается ("хешируется") в s фотонов

$$|\psi_S(x)\rangle = |\psi_1(x)\rangle \otimes \cdots \otimes |\psi_s(x)\rangle$$

- Хеш-функция ψ_S задает набор $S = \{a_1, \ldots, a_s\}$ параметров фаз этих s фотонов:

$$|\psi_j(x)\rangle = \frac{1}{\sqrt{2}}(|\ell\rangle + e^{i\frac{2\pi a_j x}{q}}|-\ell\rangle)$$

Реализация квантовой хеш-функций на основе состояний высокой размерности. Эксперимент.



Эффективность условного приготовления фотонов: 11%

Скорость генерации пар: 176 kHz/mW

Законы сохранения:

$$\omega_p = \omega_i + \omega_s$$

$$\vec{k}_p = \vec{k}_i + \vec{k}_s$$

$$\boxed{\ell_p = \ell_i + \ell_s}$$

Управление состоянием кубита с помощью поля накачки

Используемые состояния:

$$\boxed{|\psi\rangle = \frac{1}{\sqrt{2}}(|\ell\rangle + e^{i\varphi}|-\ell\rangle)}$$

Точность: $\delta\varphi = \pi/256$