Math-Net.Ru

Общероссийский математический портал

Ф. М. Ablayev, М. Ф. Ablayev, О понятии квантового хеширования, *Матем. вопр. криптогр.*, 2016, том 7, выпуск 2, 7–20

DOI: <https://doi.org/10.4213/mvk179>

Использование Общероссийского математического портала Math-Net.Ru подразумевает, что вы прочитали и согласны с пользовательским соглашением

<http://www.mathnet.ru/rus/agreement>

Параметры загрузки:

IP: 54.157.27.8

26 апреля 2023 г., 14:28:21

On the concept of quantum hashing

F. M. Ablayev, M. F. Ablayev

Kazan Federal University, Kazan, Russia

Получено 03.III.2015

Abstract. We present the notion of quantum hashing as a natural generalization of classical hashing. We suggest the concept of a quantum hash generator and a design allowing to construct a large number of different quantum hash functions.

The construction is based on composition of a classical ε -universal hash family and a given family of functions — quantum hash generators.

Key words: hashing, quantum hashing, quantum hash function

О понятии квантового хеширования

Ф. М. Аблаев, М. Ф. Аблаев

Казанский государственный университет, Казань

Аннотация. Понятие квантового хеширования вводится как естественное обобщение классического хеширования. Предлагаются определение квантового хеширующего генератора и способ построения большого числа различных квантовых хеширующих функций.

Построение основано на композиции классического ε -универсального семейства и заданного семейства функций — квантовых хеширующих генераторов.

Ключевые слова: хеширование, квантовое хеширование, квантовая хеширующая функция

1. Introduction

Quantum cryptography describes the applications of quantum mechanical effects (in particular quantum communication and quantum computation) (a) to perform cryptographic tasks or (b) to break cryptographic systems.

Quantum key distribution is the well-known example of quantum cryptography applications of the first type. The answer of the cryptographic community to the second type of applications is the “Post-quantum cryptography”, which refers to research on problems (usually public-key cryptosystems) that cannot be efficiently broken using potential quantum computers. Currently post-quantum cryptography includes several approaches, in particular, hash-based signature schemes such as Lamport signatures and Merkle signature schemes.

Quantum versions of signature schemes were considered by several authors. Gottesman and Chuang proposed a quantum digital system [7] based on the quantum mechanics. Their results use a quantum fingerprinting technique [5] and add “quantum direction” for post-quantum cryptography. Gavinsky and Ito [6] generalized the quantum fingerprinting technique of [5] and considered quantum fingerprints as cryptographic primitives.

In [1, 2] we have explicitly defined a notion of quantum hashing as a generalization of classical hashing and presented examples of quantum hash functions. It is easy to see that quantum fingerprinting and its generalizations mentioned above are quantum hash functions. Informally speaking, we defined a quantum hash function ψ to be a function that maps words of length k to a quantum s -qubit states ($\psi : \Sigma^k \rightarrow (\mathcal{H}^2)^{\otimes s}$) and has the following properties:

- Function ψ must be designed to have maximum output difference between adjacent inputs. In quantum case this means that for different words w, w' states $\psi(w), \psi(w')$ must be “almost orthogonal” (δ -orthogonal).
- Function ψ must be physically one-way. In quantum case this means that $k \gg s$.

Our contribution. In this paper we define the concept of a quantum hash generator (Definition 3). Informally speaking, we call a family G of discrete functions a *quantum hash generator*, if G allows to construct a quantum function ψ_G which is quantum hash function. We propose a design allowing to construct quantum hash functions based on specific families G (Theorem 4).

Theorem 4 describes the method of constructing a large family of different quantum hash functions.

The results of the paper are based mainly on the arXiv paper [3]. We include here only the original proofs and omit proofs that may be found in [3].

2. Definitions and notation

We begin by recalling some definitions of classical hash families from [11].

A hash function f with a domain $\mathbb{X}$, $|\mathbb{X}| = K$, and a range $\mathbb{Y}$, $|\mathbb{Y}| = M$ (typically $K \geq M$), is a map

$$f : \mathbb{X} \rightarrow \mathbb{Y},$$

that is, the hash function maps *long* inputs to *short* outputs.

Let q be a prime and $\mathbb{F}_q$ be a finite field of order q . Let Σ^k be a set of words of length k over a finite alphabet Σ . In the paper we consider cases $\mathbb{X} = \Sigma^k$, or $\mathbb{X} = \mathbb{F}_q$, or $\mathbb{X} = (\mathbb{F}_q)^k$, and $\mathbb{Y} = \mathbb{F}_q$. A hash family is a set $F = \{f_1, f_2, \dots, f_N\}$ of hash functions $f_i : \mathbb{X} \rightarrow \mathbb{Y}$.

We recall known definition.

Definition 1 (ε -universal hash family). A family F is called an ε -universal hash family (ε - $U(N; K, M)$) if for any two distinct elements $w, w' \in \mathbb{X}$ and for the function f chosen uniformly at random from F the probability $\Pr_{f \in F}[f(w) = f(w')]$ that elements w, w' collide under f is at most ε .

The parameter ε is often referred to as the collision probability of the hash family F .

Classical-quantum function. The notion of a quantum function was considered in [9]. In this paper we use the following variant of a quantum function. First recall that mathematically a qubit $|\psi\rangle$ is described as $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, where α and β are complex numbers, satisfying $|\alpha|^2 + |\beta|^2 = 1$. So, a qubit may be represented by a unit vector in the two-dimensional Hilbert complex space $\mathcal{H}^2$. Let $s \geq 1$. Let $(\mathcal{H}^2)^{\otimes s}$ be the 2^s -dimensional Hilbert space, describing the states of s qubits, i.e. $(\mathcal{H}^2)^{\otimes s}$ is made up of s copies of a single qubit space $\mathcal{H}^2$

$$(\mathcal{H}^2)^{\otimes s} = \mathcal{H}^2 \otimes \dots \otimes \mathcal{H}^2 = \mathcal{H}^{2^s}.$$

For $K = |\mathbb{X}|$ and integer $s \geq 1$ we define a $(K; s)$ classical-quantum function to be a map of elements $w \in \mathbb{X}$ to quantum states $|\psi(w)\rangle \in (\mathcal{H}^2)^{\otimes s}$

$$\psi : \mathbb{X} \rightarrow (\mathcal{H}^2)^{\otimes s}. \quad (1)$$

We will also use the notation $\psi : w \mapsto |\psi(w)\rangle$ for ψ .

3. Quantum hashing

What we need to define for quantum hashing and what is implicitly assumed in various papers (see for example [1] for more information) is a collision resistance property. However, there is still no such notion as *quantum collision*. The reason why we need to define it is the observation that in quantum hashing there might be no collisions in the classical sense: as we will see later a quantum hash function we define is one-to-one mapping of classical words to quantum states. But the procedure of comparing those (different!) quantum states implies measurement, which may lead to collision-type errors.

So, a *quantum collision* is a situation when a procedure testing the equality of quantum hashes outputs “the hashes are the same”, while hashes are different. This procedure may be a well-known SWAP-test (see for example [1] for more information and citations) or REVERSE-test which we consider below. Anyway, it deals with the notion of distinguishability of quantum states. Since non-orthogonal quantum states cannot be perfectly distinguished, we require them to be “nearly orthogonal”.

- For $\delta \in (0, 1/2)$ we say that a function

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

is δ -resistant, if for any pair w, w' of different elements

$$|\langle \psi(w) | \psi(w') \rangle| \leq \delta.$$

Theorem 1. Let $\psi : \mathbb{X} \rightarrow (\mathcal{H}^2)^{\otimes s}$ be a δ -resistant function. Then

$$s \geq \log \log |\mathbb{X}| - \log \log \left(1 + \sqrt{2/(1 - \delta)} \right) - 1.$$

Proof. See [3] for the proof. □

The notion of δ -resistance naturally leads to the following notion of quantum hash function.

Definition 2 (Quantum hash function). Let K, s be positive integers and $K = |\mathbb{X}|$. We say that a map

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

is δ -resistant $(K; s)$ quantum hash function, if ψ is a δ -resistant function.

We use the notation δ -R $(K; s)$ as an abbreviation for δ -resistant $(K; s)$ quantum hash function.

Quantum hashing property. One of the extra justification of the quantum hash function definition is as follows. Let $\mathbb{X} = \Sigma^k$ and $\psi : w \mapsto |\psi(w)\rangle$ be δ -resistant.

Let us consider the procedure that we call a *REVERSE-test* [2] and that permits to check whether a quantum state $|\psi(w)\rangle$ is a hash of a classical string v .

Essentially the test applies the procedure that inverts the creation of a quantum hash, i.e. it “uncomputes” the hash to the initial state (usually the all-zero state).

Formally, let the procedure of quantum hashing of the string w be given by unitary transformation $U(w)$ applied to the initial state $|0\rangle$, i.e. $|\psi(w)\rangle = U(w)|0\rangle$. Then the REVERSE-test, given v and $|\psi(w)\rangle$, applies $U^{-1}(v)$ to the state $|\psi(w)\rangle$ and measures the resulting state. It outputs « $v = w$ » iff the measurement outcome is $|0\rangle$. Denote by $Pr_{reverse}[\langle v = w \rangle]$ the probability that the REVERSE-test having quantum state $|\psi(w)\rangle$ and a word v outputs the result « $v = w$ ».

The following property was presented implicitly in [4].

Property 1. *If ψ is δ -resistant, then for any two different words $w, v \in \Sigma^k$*

$$Pr_{reverse}[\langle v = w \rangle] < \delta^2.$$

Proof. Let $v \neq w$. By the δ -resistance property $\langle 0 | U^{-1}(v)\psi(w) \rangle < \delta$, this bounds the probability $Pr_{reverse}[\langle v = w \rangle] = |\langle 0 | U^{-1}(v)\psi(w) \rangle|^2$ by δ^2 . $\square$

Following Definition 1 one can call δ^2 a collision probability of the δ -reversible quantum hash function ψ .

3.1. Quantum fingerprinting function is a quantum hash function

One of the first explicit quantum hash functions was defined in [5]. Originally the authors invented a construction called “quantum fingerprinting” for testing the equality of two words for a quantum communication model. The cryptographic aspects of quantum fingerprinting are presented in [6]. The quantum fingerprinting technique is based on binary error-correcting codes. Later this construction was adopted for cryptographic purposes. Here we present the quantum fingerprinting construction from the quantum hashing point of view.

An (n, k, d) error-correcting code is a map $C : \Sigma^k \rightarrow \Sigma^n$ such that for any two distinct words $w, w' \in \Sigma^k$ the Hamming distance $d(C(w), C(w'))$ between codewords $C(w)$ and $C(w')$ is at least d . The code is binary if $\Sigma = \{0, 1\}$.

The construction of a quantum hash function based on quantum fingerprinting is as follows. Let k be a positive integer and $n > k$. Let $E : \{0, 1\}^k \rightarrow \{0, 1\}^n$ be an (n, k, d) binary error-correcting code. Let $s = \log n$.

Define the value of the classical-quantum function $\psi : \{0, 1\}^k \rightarrow (\mathcal{H}^2)^{\otimes s}$ on a word w as

$$\psi(w) = \frac{1}{\sqrt{n}} \sum_{i=1}^n (-1)^{E_i(w)} |i\rangle. \quad (2)$$

The next property is the reformulation of the “quantum fingerprinting” property [5] in terms of quantum hashing.

Property 2. *For an (n, k, d) binary error-correcting code E , for $s = \log n$, for $\delta = (1 - d/n)$ the function ψ defined in (2) is an δ -R $(2^k; s)$ quantum hash function.*

Proof. For two different words w, w' , for $i \in \{1, 2, \dots, n\}$, $a_i(w, w') = E_i(w) + E_i(w') \pmod{2}$ we have

$$|\langle \psi(w) | \psi(w') \rangle| = \frac{1}{n} \sum_{i=1}^n (-1)^{a_i(w, w')} = \frac{n - d(E(w), E(w'))}{n} \leq 1 - \frac{d}{n} = \delta.$$

□

Note that the above construction of a quantum hash function needs $s = \log n$ qubits for $\delta = 1 - d/n$. Such number of qubits is good enough in the sense of the lower bound of Theorem 1 for s when $n = ck$:

$$s \geq \log(n/c) - \log \log \left(1 + \sqrt{2n/d}\right) - 1.$$

4. Quantum hash generator

In this section we define a notion of a quantum hash function which allows to construct quantum hash functions.

Definition 3 (Quantum hash generator). Let $K = |\mathbb{X}|$ and $G = \{g_1, g_2, \dots, g_D\}$ be a family of functions $g_j : \mathbb{X} \rightarrow \mathbb{F}_q$. Let $\ell \geq 1$ be an integer. For $g \in G$ let ψ_g be a classical-quantum function $\psi_g : \mathbb{X} \rightarrow (\mathcal{H}^2)^{\otimes \ell}$ determined by the rule

$$\psi_g : w \mapsto |\psi_g(w)\rangle = \sum_{i=1}^{2^\ell} \alpha_i(g(w)) |i\rangle, \quad (3)$$

where the amplitudes $\alpha_i(g(w))$, $i \in \{1, 2, \dots, 2^\ell\}$, of the state $|\psi_g(w)\rangle$ are determined by $g(w)$.

Let $d = \log D$, $s = d + \ell$. We define a classical-quantum function $\psi_G : \mathbb{X} \rightarrow (\mathcal{H}^2)^{\otimes s}$ by the rule

$$\psi_G : w \mapsto |\psi_G(w)\rangle = \frac{1}{\sqrt{D}} \sum_{j=1}^D |j\rangle |\psi_{g_j}(w)\rangle. \quad (4)$$

We say that the family G generates the δ - R ($K; s$) quantum hash function ψ_G . We call G a δ - R ($K; s$) quantum hash generator, if ψ_G is a δ - R ($K; s$) quantum hash function. We call G a quantum hash generator if ψ_G generates a δ - R ($K; s$) quantum hash function for some δ , K , s .

Below we present two examples of quantum hash generators: the binary and non binary constructions.

4.1. Binary quantum hash generator

First we present the construction of quantum fingerprinting function from the Section 3.1 in terms of Definition 3.

Theorem 2. *Let for (n, k, d) binary error-correcting code $E : \{0, 1\}^k \rightarrow \{0, 1\}^n$ a family of functions $F_E = \{E_1, E_2, \dots, E_n\}$ be defined by the rule: $E_i : \{0, 1\}^k \rightarrow \mathbb{F}_2$ is the i -th bit of the codeword $E(w)$. The family F_E is an δ - R ($2^k; s$) quantum hash generator for $\delta = 1 - d/n$ and $s = \log n$.*

Proof. For $E_j \in F_E$ we define $\psi_{E_j} : \{0, 1\}^k \rightarrow \mathcal{H}^2$ as $|\psi_{E_j}(w)\rangle = (-1)^{E_j(w)} |1\rangle$ and let

$$|\psi_{F_E}(w)\rangle = \frac{1}{\sqrt{n}} \sum_{j=1}^n |j\rangle |\psi_{E_j}(w)\rangle = \frac{1}{\sqrt{n}} \sum_{j=1}^n (-1)^{E_j(w)} |j\rangle |1\rangle.$$

We can omit the $|1\rangle$ from the last equation and finally we obtain

$$|\psi_{F_E}(w)\rangle = \frac{1}{\sqrt{n}} \sum_{j=1}^n (-1)^{E_j(w)} |j\rangle.$$

The last equality together with (2) and Property 2 proves the statement. $\square$

4.2. Non-binary quantum hash generator

We start with recalling some definitions, notations, and facts from [10]. For a field $\mathbb{F}_q$ the discrete Fourier transform of a set $B \subseteq \mathbb{F}_q$ is the function

$$f_B(a) = \sum_{b \in B} e^{\frac{2\pi i}{q} ab}$$

defined for every $a \in \mathbb{F}_q$. Let $\lambda(B) = \max_{a \neq 0} |f_B(a)|/|B|$.

For $\delta > 0$ we define $B \subseteq \mathbb{F}_q$ to be δ -good if $\lambda(B) \leq \delta$. By $B_{\delta, q}$ we denote δ -good subset of $\mathbb{F}_q$.

For a field $\mathbb{F}_q$ let $B \subseteq \mathbb{F}_q$. For every $b \in B$ and $w \in \mathbb{F}_q$ we define a function $h_b : \mathbb{F}_q \rightarrow \mathbb{F}_q$ and a family H_B by the rule

$$h_b(w) = bw \pmod{q}, \quad H_B = \{h_b : b \in B\}.$$

We denote a family H_B of functions by $H_{\delta,q}$ and say that $H_{\delta,q}$ is δ -good if B is δ -good ($B = B_{\delta,q}$).

The following facts were presented in [10].

- Let $\delta = \delta(q)$ be any function tending to zero as q grows to infinity. Then there exists δ -good set $B_{\delta,q}$ with $|B_{\delta,q}| = (\log q / \delta(q))^{O(1)}$.
- Different authors have presented several optimal (in the sense of the above lower bound) explicit constructions of δ -good sets $B_{\delta,q}$ such that for $\delta(q) = \frac{1}{(\log q)^{O(1)}}$ the estimate $|B_{\delta,q}| = (\log q)^{O(1)}$ is true.

Theorem 3. *Let $\delta > 0$ and q be a prime. Let $H_{\delta,q}$ be δ -good. Then for $s = \log |H_{\delta,q}|$ a family $H_{\delta,q}$ is an δ -R ($q; s$) quantum hash generator.*

Proof is given in the appendix. $\square$

5. Quantum hashing via classical ε -universal hashing constructions

In this section we present a construction of a quantum hash generator based on the composition of an ε -universal hash family with a given quantum hash generator. We begin with the definitions and notation that will be used in the following.

Let $K = |\mathbb{X}|$, $M = |\mathbb{Y}|$. Let $F = \{f_1, f_2, \dots, f_N\}$ be a family of functions,

$$f_i : \mathbb{X} \rightarrow \mathbb{Y}, \quad i = 1, 2, \dots, N.$$

Let q be a prime and $\mathbb{F}_q$ be a field. Let $H = \{h_1, h_2, \dots, h_T\}$ be a family of functions, where

$$h_j : \mathbb{Y} \rightarrow \mathbb{F}_q.$$

For $f \in F$ and $h \in H$, define composition $g = f \circ h$,

$$g : \mathbb{X} \rightarrow \mathbb{F}_q,$$

by the rule

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

Define the composition $G = F \circ H$ of two families F and H as follows:

$$G = \{g_{ij} = f_i \circ h_j : i \in I, j \in J\},$$

where $I = \{1, 2, \dots, N\}$, $J = \{1, 2, \dots, T\}$.

Theorem 4. Let $F = \{f_1, f_2, \dots, f_N\}$ be an ε - $U(N; K, M)$ hash family. Let $H = \{h_1, h_2, \dots, h_T\}$ be a δ - $R(M; \ell)$ quantum hash generator.

Then the composition $G = F \circ H$ is a Δ - $R(K; s)$ quantum hash generator, where

$$s = \log N + \ell \quad (5)$$

and

$$\Delta \leq \varepsilon + \delta. \quad (6)$$

Proof. See the paper [3] for the proof. $\square$

In [3] and in the Appendix B different explicit constructions of quantum hash functions based on the above Theorem are presented.

References

- [1] Ablayev F., Vasiliev A., “Quantum hashing” (2013), arXiv: 1310.4922 [quant-ph].
- [2] F. Ablayev, A. Vasiliev, “Cryptographic quantum hashing”, *Laser Physics Letters*, **11**:2 (2014), 025202.
- [3] Ablayev F., Ablayev M., “Quantum hashing via classical ε -universal hashing constructions” (2014), arXiv: 1404.1503 [quant-ph].
- [4] Ablayev F., Vasiliev A., “Computing Boolean functions via quantum hashing”. In: “*Computing with New Resources*”, Lect. Notes Comput. Sci., **8808**, 2014, 149–160.
- [5] Buhrman H., Cleve R., Watrous J., de Wolf R., “Quantum fingerprinting”, *Phys. Rev. Lett.*, **87** (2001), 167902.
- [6] Gavinsky D., Ito T., “Quantum fingerprints that keep secrets”, *Quantum Inf. and Comput.*, **13**:7–8 (2013), 583–606.
- [7] Gottesman D., Chuang I., “Quantum digital signatures” (2001), <http://arxiv.org/abs/quant-ph/0105032>.
- [8] Freivalds R., “Probabilistic machines can use less running time”. In: “*Proc. IFIP Congress 77, Toronto, Canada, 1977*”, Amsterdam: North-Holland, 1977, 839–842.
- [9] Montanaro A., Osborne T., “Quantum Boolean functions”, *Chicago J. Theor. Comput. Sci.*, **2010**:1 (2010), arXiv: 0810.2435.
- [10] Razborov A., Szemerédi E., Wigderson A., “Constructing small sets that are uniform in arithmetic progressions”, *Comb., Probab. and Comput.*, **2**:4 (1993), 513–518.
- [11] Stinson D. R., “On the connections between universal ε -hashing, combinatorial designs and error-correcting codes”, *Congr. Numer.*, **114** (1996), 7–27.

Appendix A. Proof of Theorem 3

Let $B_{\delta,q} = \{b_1, b_2, \dots, b_T\}$ determines δ -good family $H_{\delta,q}$. We denote $H = H_{\delta,q}$ in the proof. For function $h_b \in H$ we define $\psi_{h_b} : \mathbb{F}_q \rightarrow \mathcal{H}^2$ as

$$|\psi_{h_b}(a)\rangle = e^{\frac{2\pi i}{q}h_b(a)}|1\rangle = e^{\frac{2\pi i}{q}ab}|1\rangle$$

and define function $\psi_H : \mathbb{F}_q \rightarrow (\mathcal{H}^2)^{\otimes(s+1)}$ by the rule

$$|\psi_H(a)\rangle = \frac{1}{\sqrt{T}} \sum_{j=1}^T |j\rangle |\psi_{h_{b_j}}(a)\rangle = \frac{1}{\sqrt{T}} \sum_{j=1}^T e^{\frac{2\pi i}{q}ab_j} |j\rangle |1\rangle.$$

We consider the following projection $\psi_H : \mathbb{F}_q \rightarrow (\mathcal{H}^2)^{\otimes s}$ of function ψ_H (speaking informally we omit the $|1\rangle$ from the above definition of ψ_H):

$$|\psi_H(a)\rangle = \frac{1}{\sqrt{T}} \sum_{j=1}^T e^{\frac{2\pi i}{q}ab_j} |j\rangle.$$

The quantum state $|\psi_H(a)\rangle$ is composed from s qubits. To show that ψ_H is δ - $R(q; s)$ quantum hash function we prove the δ -resistance of ψ_H . Consider a pair a, a' of different elements from $\mathbb{F}_q$ and their inner product $\langle \psi_H(a) | \psi_H(a') \rangle$. Recall that the inner product of two complex vectors $|\alpha\rangle = (\alpha_1, \alpha_2, \dots, \alpha_T)$ and $|\beta\rangle = (\beta_1, \beta_2, \dots, \beta_T)$ is the sum $\langle \alpha | \beta \rangle = \sum_j \alpha_j \bar{\beta}_j$ where $\bar{\beta}_j$ is the complex conjugate of β_j . Taking into account that the conjugate of $e^{i\phi}$ is $e^{-i\phi}$ and that $B_{\delta,q}$ is δ -good we obtain

$$\langle \psi_H(a) | \psi_H(a') \rangle = \frac{1}{|B|} \sum_{b \in B} e^{\frac{2\pi i}{q}(a-a')b} \leq \lambda(B_{\delta,q}) \leq \delta.$$

□

Notice that the construction of quantum hash function ψ , generated by quantum hash generator $H_{\delta,q}$, presented in [2] terms of real valid amplitudes.

Appendix B. Explicit constructions of quantum hash functions based on classical universal hash

The following statement is a corollary of Theorem 4 and is a basis for explicit constructions of quantum hash functions in this section. Let q be a prime and $\mathbb{F}_q$ be a field.

Theorem 5. *Let $F = \{f_1, f_2, \dots, f_N\}$ be an ε - $U(N; K, q)$ hash family, where $f_i : \mathbb{X} \rightarrow \mathbb{F}_q$. Let $H_{\delta, q}$ be an optimal δ - $R(q, O(\log \log q))$ quantum hash generator. Then the family $G = F \circ H_{\delta, q}$ is a Δ - $R(K; s)$ quantum hash generator, where*

$$s \leq \log N + O(\log \log q) \quad \text{and} \quad \Delta \leq \varepsilon + \delta.$$

Proof. Family $H_{\delta, q} = \{h_1, h_2, \dots, h_T\}$, where $h_i : \mathbb{F}_q \rightarrow \mathbb{F}_q$, $T = \lceil (2/\delta^2) \ln(2q) \rceil$, $\ell = 1$, and $s = \log T + 1 \leq \log n + \log \log q + 2 \log 1/\delta + 3$ is δ - $R(q; s)$ quantum hash generator. $\square$

Quantum hashing based on Freivalds' fingerprinting

For a fixed positive constant k let $\mathbb{X} = \{0, 1\}^k$. Let $c > 1$ be a positive integer and let $M = ck \ln k$. Let $\mathbb{Y} = \{0, 1, \dots, M-1\}$.

For the i -th prime $p_i \in \mathbb{Y}$ define a function (fingerprint) $f_i : \mathbb{X} \rightarrow \mathbb{Y}$ by the rule $f_i(w) = w \pmod{p_i}$. Here we treat a word $w = w_0 w_1 \dots w_{k-1}$ also as an integer $w = w_0 + w_1 2 + \dots + w_{k-1} 2^{k-1}$. Consider the set

$$F_M = \{f_1, f_2, \dots, f_{\pi(M)}\}$$

of fingerprints. Here $\pi(M)$ denotes the number of primes less than or equal to M . Note that then $\pi(M) \sim M/\ln M$ as $M \rightarrow \infty$. Moreover,

$$\frac{M}{\ln M} \leq \pi(M) \leq 1.26 \frac{M}{\ln M} \quad \text{for } M \geq 17.$$

The following fact is based on a construction of “Freivalds' fingerprinting method” due to Freivalds [8].

Property 3. *The set F_M of fingerprints is a $(1/c)$ - $U(\pi(M); 2^k, M)$ hash family.*

Proof (sketch). For any pair w, w' of distinct words from $\{0, 1\}^k$ the number $N(w, w') = |\{f_i \in F_M : f_i(w) = f_i(w')\}|$ is bounded from above by k . Thus, if we pick a prime p_i (uniformly at random) from $\mathbb{Y}$ then

$$\Pr[f_i(w) = f_i(w')] \leq \frac{k}{\pi(M)} \leq \frac{k \ln M}{M}.$$

Picking $M = ck \ln k$ with a constant c gives

$$\Pr[f_i(w) = f_i(w')] \leq \frac{1}{c} + o(1). \quad \square$$

Theorem 5 and Property 3 provide the following statement.

Theorem 6. *Let $c > 1$ be a positive integer and let $M = ck \ln k$. Let $q \in \{M, M+1, \dots, 2M\}$ be a prime. Let $\delta = 1/(\log q)^{O(1)}$ and let $H_{\delta, q}$ be an optimal δ - $R(q, O(\log \log q))$ quantum hash generator. Then family $G = F_M \circ H_{\delta, q}$ is a Δ - $R(2^k; s)$ quantum hash generator, where*

$$s \leq \log ck + O(\log \log k) \quad \text{and} \quad \Delta \leq \frac{1}{c} + \delta.$$

Proof. It follows from Theorem 5 and the choice of c above that $M = ck \ln k$. Thus

$$s = \log |F_M| + O(\log \log q) \leq \log \pi(M) + \log \log M \leq \log ck + O(\log \log k). \quad \square$$

Construction of ψ_G . For a word $w \in \{0, 1\}^k$ we define ψ_G by the rule

$$|\psi_G(w)\rangle = \frac{1}{\sqrt{|F_M|T}} \sum_{l=1, j=1}^{|F_M|, T} e^{\frac{2\pi i}{q} h_j(f_l(w))} |lj\rangle.$$

Remark. Note that from Theorem 1 it follows that

$$s \geq \log k + \log \log (ck \ln k) - \log \log \left(1 + \sqrt{\frac{2}{1-\delta}} \right) - 1.$$

This lower bound shows that the quantum hash function ψ_G is good enough in the sense of the number of qubits used for the construction.

Quantum hashing and error-correcting codes

Let q be a prime and let $\mathbb{F}_q$ be a field. An (n, k, d) error-correcting code is called *linear* if $\Sigma = \mathbb{F}_q$, and $\mathcal{C} = \{C(w) : w \in \mathbb{F}_q^k\}$ is a subspace of $(\mathbb{F}_q)^n$. We will denote such linear code by an $[n, k, d]_q$ code.

Theorem 7. *Let $\mathcal{C}$ be an $[n, k, d]_q$ code. Then for arbitrary $\delta \in (0, 1)$ there exists a Δ -R $(q^k; s)$ quantum hash generator G with $\Delta = (1 - d/n) + \delta$ and $s \leq \log n + \log \log q + 2 \log 1/\delta + 4$.*

Proof. The following fact was observed in [11]. Having an $[n, k, d]_q$ code $\mathcal{C}$, we can explicitly construct a $(1 - d/n)$ -U $(n; q^k; q)$ hash family $F_{\mathcal{C}}$.

By Theorem 5 a composition $G = F_{\mathcal{C}} \circ H_{\delta, q}$ is a Δ -R $(q^k; s)$ quantum hash generator with $\Delta = (1 - d/n) + \delta$ and $s \leq \log n + \log \log q + 2 \log 1/\delta + 4$. $\square$

Quantum hash function via Reed-Solomon code

As an example we present construction of quantum hash function, using Reed–Solomon codes.

Let q be a prime, let $k \leq n \leq q$, let $\mathbb{F}_q$ be a finite field. A *Reed-Solomon code* (for short RS-code) is a linear code

$$C_{RS} : (\mathbb{F}_q)^k \rightarrow (\mathbb{F}_q)^n$$

having parameters $[n, k, n - (k - 1)]_q$:

$$C_{RS}(w) = (P_w(a_1)P_w(a_2) \cdots P_w(a_n)).$$

Using Reed–Solomon codes we obtain the following construction of quantum hash generator.

Theorem 8. *Let q be a prime and let $1 \leq k \leq n \leq q$. Then for arbitrary $\delta \in (0, 1)$ there is a Δ -R $(q^k; s)$ quantum hash generator G_{RS} , where*

$$\Delta \leq \frac{k-1}{n} + \delta \quad \text{and} \quad s \leq \log(q \log q) + 2 \log \frac{1}{\delta} + 4.$$

Proof. Reed–Solomon code C_{RS} is $[n, k, n - (k - 1)]_q$ code, where $k \leq n \leq q$. Then according to Theorem 7 there is a family G_{RS} , which is a Δ -R $(q^k; s)$ quantum hash generator with stated parameters. $\square$

In particular, if we select $n \in [ck, c'k]$ for constants $c < c'$, then $\Delta \leq 1/c + \delta$ for $\delta \in (0, 1)$ and according to Theorem 1 we find that

$$\begin{aligned} \log(q \log q) - \log \log \left(1 + \sqrt{\frac{2}{1-\Delta}} \right) - \log \frac{c'}{2} &\leq \\ &\leq s \leq \log(q \log q) + 2 \log \frac{1}{\Delta} + 4. \end{aligned}$$

Thus, Reed–Solomon codes provides good enough parameters for resistance value Δ and for a number s of qubits needed to construct quantum hash function ψ_{RS} .

Explicit constructions of G_{RS} and $\psi_{G_{RS}}$

Define $(k-1)/q$ - $U(q; \mathbb{F}_q^k; q)$ hash family $F_{RS} = \{f_a : a \in A\}$ based on C_{RS} as follows. For $a \in A$ define $f_a : (\mathbb{F}_q)^k \rightarrow \mathbb{F}_q$ by the rule

$$f_a(w_0 w_1 \cdots w_{k-1}) = \sum_{i=0}^{k-1} w_i a^i.$$

Let $H_{\delta, q} = \{h_1, h_1, \dots, h_T\}$, where $h_j : \mathbb{F}_q \rightarrow \mathbb{F}_q$ and $T = \lceil (2/\delta^2) \ln 2q \rceil$. For $s = \log n + \log T + 1$ the composition $G_{RS} = F_{RS} \circ H_{\delta, q}$ defines function

$$\psi_{G_{RS}} : (\mathbb{F}_q)^k \rightarrow (\mathcal{H}^2)^{\otimes s}$$

for a word $w \in (\mathbb{F}_q)^k$ by the rule

$$\begin{aligned} \psi_{G_{RS}}(w) &= \\ &= \frac{1}{\sqrt{n}} \sum_{i=1}^n |i\rangle \otimes \left(\frac{1}{\sqrt{T}} \sum_{j=1}^T |j\rangle \left(\cos \frac{2\pi h_j(f_{a_i}(w))}{q} |0\rangle + \sin \frac{2\pi h_j(f_{a_i}(w))}{q} |1\rangle \right) \right). \end{aligned}$$