On the Concept of Cryptographic Quantum Hashing

F. Ablayev[*]   M. Ablayev[†]

September 2015

Abstract

In the paper we define a notion of quantum resistant $((\epsilon, \delta)$-resistant) hash function which combine together a notion of pre-image (one-way) resistance (ϵ-resistance) property we define in the paper and the notion of collision resistance (δ-resistance) properties.

We show that in the quantum setting a one-way resistance property and collision resistance property are correlated: the "more" a quantum function is one-way resistant the "less" it collision resistant and vice versa. We present an explicit quantum hash function which is "balanced" one-way resistant and collision resistant and demonstrate how to build a large family quantum hash functions. Balanced quantum hash functions need a high degree of entanglement between the qubits. We use a "phase constructions" technique to express quantum hashing constructions, which is good to map hash states to coherent states in a superposition of time-bin modes. The later is ready to be implemented with current optical technology.

1   Introduction

Quantum cryptography describes the use of quantum mechanical effects (a) to break cryptographic systems and (b) to perform cryptographic tasks. Quantum factoring algorithm and quantum algorithm for finding discrete logarithm are famous results that belong for the first direction. Quantum key distribution, quantum digital signature schemes constructions belong to the second direction of quantum cryptography.

Gottesman and Chuang proposed in 2001 a quantum digital signature protocol [1] which is based on quantum one-way function. This is also the case for other protocols (see for example [2]). In [3, 4] we explicitly defined a notion of quantum hashing as a generalization of classical hashing and presented examples of quantum hash functions. It appeared that Gottesman-Chuang quantum signature schemes are based on functions

---

[*]Kazan Federal University, Kazan, Russian Federation. fablayev@gmail.com

[†]Kazan Federal University, Kazan, Russian Federation

which are actually quantum hash functions. Those functions have "unconditionally one-way" property based on Holevo Theorem [5]. More information on the role of quantum hashing for the post quantum cryptography, possible application of quantum hashing for quantum signature protocols, and technological expectations for realization of quantum signature schemes are presented in [6].

Recall that in the classical setting a cryptographic hash function h should have the following three properties [7]. (1) Pre-image resistance: Given $h(x)$, it should be difficult to find x, that is, these hash functions are one-way functions. (2) Second pre-image resistance: Given x_1, it should be difficult to find an x_2, such that $h(x_1) = h(x_2)$. (3) Collision resistance: It should be difficult to find any pair of distinct x_1, x_2, such that $h(x_1) = h(x_2)$. Note, that there are no one-way functions that are known to be provably more difficult to invert than to compute, the security of cryptographic hash functions is "computationally conditional".

Informally speaking, a quantum hash function ψ [3, 4] is a function that maps words (over an alphabet Σ) of length k to a quantum pure states of s-qubits ($\psi : \Sigma^k \to (\mathcal{H}^2)^{\otimes s}$) and has the following properties:

1. Function ψ must be one-way resistant. In quantum case this means that $k > s$.

2. Function ψ must be collision resistant. In quantum case this means that for different words w, w' states $|\psi(w)\rangle$, $|\psi(w')\rangle$ must be "almost orthogonal" (δ-orthogonal) [4].

Quantum collision resistance property cover both second pre-image resistance and collision resistance properties for the quantum setting

In papers [8, 9] we considered a quantum Branching Program as a computational model which, we believe, is adequate quantum technological model for presenting a quantum communication protocols and quantum cryptographic signature schemes based on hashing.

Our contribution. In the paper we define a notion of (ϵ, δ)-hash function where values ϵ and δ are numerical characteristics of the above two properties: (i) one-way resistance and (ii) collision resistance properties. The notion of the (ϵ, δ)-hash function is an explicit generalization of our constructions [3, 4]. We show that in the quantum setting the one-way resistance property and collision resistance property are correlated: the "more" a quantum function is one-way resistant the "less" it is collision resistant and vice versa. We present a quantum hash function which is "balanced" one-way resistant and collision resistant. In addition we present more discussion that supports the idea of quantum hashing from our papers. Note, that a realization of the balanced quantum hash function requires the high degree of entanglement between the qubits which makes such a state very difficult (or impossible) to create with current technology.

We present quantum "balanced" hashing constructions based on "phase transformation" presentation [10] instead of "amplitude transformation" [4]. The phase transformation is required to map quantum hash states into a sequence of coherent states.

Note, that quantum signature protocols using coherent states can be practically implemented by now day technology that use only a sequence of coherent states, linear optics operations, and measurements with single-photon threshold detectors. See [11, 12, 7] for more information and citations.

2 Quantum (ϵ, δ)-Resistant Hash Function

Recall that mathematically a qubit is described as 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. For an integer $j \in \{0, \ldots, 2^s - 1\}$ let $\sigma = \sigma_1 \ldots \sigma_s$ be a binary presentation of j. We use (as usual) notations $|j\rangle$ and $|\sigma\rangle$ to denote quantum state $|\sigma_1\rangle \cdots |\sigma_s\rangle = |\sigma_1\rangle \otimes \ldots \otimes |\sigma_s\rangle$.

We let q to be a prime power 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. Let $\mathbb{X}$ be a finite set. In the paper we let $\mathbb{X} = \Sigma^k$, or $\mathbb{X} = \mathbb{F}_q$. For $K = |\mathbb{X}|$ and integer $s \geq 1$ we define a $(K; s)$ classical-quantum function (or just quantum function) to be a unitary transformation (determined by an element $w \in \mathbb{X}$) of the initial state $|\psi_0\rangle \in (\mathcal{H}^2)^{\otimes s}$ to a quantum state $|\psi(w)\rangle \in (\mathcal{H}^2)^{\otimes s}$

$$\psi : \{|\psi_0\rangle\} \times \mathbb{X} \to (\mathcal{H}^2)^{\otimes s} \qquad |\psi(w)\rangle = U(w)|\psi_0\rangle \tag{1}$$

where $U(w)$ is a unitary matrix. We let $|\psi_0\rangle = |0\rangle$ in the paper and use (for short) the following notation (instead the above)

$$\psi : \mathbb{X} \to (\mathcal{H}^2)^{\otimes s} \quad \text{or} \quad \psi : w \mapsto |\psi(w)\rangle$$

2.1 One-way Resistant Function.

We present the following definition of quantum ϵ-resistant one-way function. Let "information extracting" mechanism $\mathcal{M}$ be a function $\mathcal{M} : (\mathcal{H}^2)^{\otimes s} \to \mathbb{X}$. Informally speaking mechanism $\mathcal{M}$ makes some measurement to state $|\psi\rangle \in (\mathcal{H}^2)^{\otimes s}$ and decode the result of measurement to $\mathbb{X}$.

Definition 2.1 *Let X be random variable distributed over $\mathbb{X}$ $\{Pr[X = w] : w \in \mathbb{X}\}$. Let $\psi : \mathbb{X} \to (\mathcal{H}^2)^{\otimes s}$ be a quantum function. Let Y is any random variable over $\mathbb{X}$ obtained by some mechanism $\mathcal{M}$ making measurement to the encoding ψ of X and decoding the result of measurement to $\mathbb{X}$. Let $\epsilon > 0$. We call a quantum function ψ a one-way ϵ-resistant function if for any mechanism $\mathcal{M}$, the probability $Pr[Y = X]$ that $\mathcal{M}$ successfully decodes Y is bounded by ϵ*

$$Pr[Y = X] \leq \epsilon.$$

For the cryptographic purposes it is natural to expect (and we do this in the rest of the paper) that random variable X is uniformly distributed.

A quantum state of $s \geq 1$ qubits can "carry" an infinite amount of information. On the other hand, fundamental result of quantum informatics known as Holevo's Theorem [5] states that a quantum measurement can only give s bits of information about the state. We will use here the following particular version [13] of Holevo's Theorem.

Property 2.1 (Holevo-Nayak) *Let X be random variable uniformly distributed over a k bit binary words $\{0,1\}^k$. Let $\psi : \{0,1\}^k \to (\mathcal{H}^2)^{\otimes s}$ be an $(2^k; s)$ quantum function. Let Y be a random variable over $\mathbb{X}$ obtained by some mechanism $\mathcal{M}$ making some measurement of the encoding ψ of X and decoding the result of measurement to $\{0,1\}^k$. Then our probability of correct decoding is given by*

$$Pr[Y = X] \leq \frac{2^s}{2^k}.$$

2.2 Collision Resistant Function

The following definition was presented in [4].

Definition 2.2 *Let $\delta > 0$. We call a quantum function $\psi : \mathbb{X} \to (\mathcal{H}^2)^{\otimes s}$ a collision δ-resistant function if for any pair w, w' of different elements,*

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

Testing Equality. What one needs for quantum digital signature schemes realization is an equality testing procedure for quantum hashes $|\psi(v)\rangle$ and $|\psi(w)\rangle$ in order to compare classical messages v and w; see for example [1]. The *SWAP-test* is the known quantum test for the equality of two unknown quantum states $|\psi\rangle$ and $|\psi'\rangle$ (see [1, 3] for more information).

We denote $Pr_{swap}[v = w]$ a probability that the *SWAP-test* having quantum hashes $|\psi(v)\rangle$ and $|\psi(w)\rangle$ outputs the result "$v = w$" (outputs the result "$|\psi(v)\rangle = |\psi(w)\rangle$").

Property 2.2 ([1]) *Let function $\psi : w \mapsto |\psi(w)\rangle$ satisfy the following condition. For any two different elements $v, w \in \mathbb{X}$ it is true that $|\langle \psi(v) | \psi(w) \rangle| \leq \delta$. Then*

$$Pr_{swap}[v = w] \leq \frac{1}{2}(1 + \delta^2).$$

Proof. From the description of *SWAP*-test it follows that

$$Pr_{swap}[v = w] = \frac{1}{2}\left(1 + |\langle \psi(v) | \psi(w) \rangle|^2\right).$$

$\square$

The next test for equality was first mentioned in [1]. We call this test a *REVERSE-test* [3]. *REVERSE-test* was proposed to check if a quantum state $|\psi\rangle$ is a hash of

an element 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.

Formally, let for element w the procedure of quantum hashing be given by unitary transformation $U(w)$, applied to initial state $|\phi_0\rangle$. Usually we let $|\phi_0\rangle = |0\rangle$, 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 with respect to initial state $|0\rangle$. It outputs $v = w$ iff the measurement outcome is $|0\rangle$. Denote by $Pr_{reverse}[v = w]$ the probability that the *REVERSE-test* having quantum state $|\psi(w)\rangle$ and an element v outputs the result $v = w$.

Property 2.3 *Let hash function $\psi : w \mapsto |\psi(w)\rangle$ satisfy the following condition. For any two different elements $v, w \in \mathbb{X}$ it is true that $|\langle\psi(v)|\psi(w)\rangle| \leq \delta$. Then*

$$Pr_{reverse}[v = w] \leq \delta^2.$$

Proof. Using the property that unitary transformation keeps scalar product we have that

$$Pr_{reverse}[v = w] = |\langle 0|U^{-1}(v)\psi(w)\rangle|^2 = |\langle U^{-1}(v)\psi(v)|U^{-1}(v)\psi(w)\rangle|^2 = |\langle\psi(v)|\psi(w)\rangle|^2 \leq \delta^2.$$

$\square$

2.3 One-way Resistance and Collision Resistance

The above two definitions and considerations lead to the following formalization of the quantum cryptographic (one-way and collision resistant) function

Definition 2.3 *Let $K = |\mathbb{X}|$ and $s \geq 1$. Let $\epsilon > 0$ and $\delta > 0$. We call a function $\psi : \mathbb{X} \rightarrow (\mathcal{H}^2)^{\otimes s}$ a quantum (ϵ, δ)-Resistant $(K; s)$-hash function iff ψ is a one-way ϵ-resistant and is a collision δ-resistant function.*

We present below the following two examples to demonstrate how one-way ϵ-resistance and collision δ-resistance are correlated. The first example was presented in [14] in terms of quantum automata.

Example 2.1 *Let us encode numbers v from $\{0, \ldots, 2^k - 1\}$ by a single qubit as follows:*

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

Extracting information from $|\psi\rangle$ by measuring $|\psi\rangle$ with respect to the basis $\{|0\rangle, |1\rangle\}$ gives the following result. The function ψ is one-way $\frac{1}{2^k}$-resistant (see Property 2.1) and collision $\cos\left(\pi/2^{k-1}\right)$-resistant. According to the properties 2.1 and 2.3 the function ψ has good one-way property, but has bad resistance property for a large k.

5

Example 2.2 *We consider a number $v \in \{0, \ldots, 2^k - 1\}$ to be also a binary word $v \in \{0, 1\}^k$. Let $v = \sigma_1 \ldots \sigma_k$. We encode v by k qubits: $\psi : v \mapsto |v\rangle = |\sigma_1\rangle \cdots |\sigma_k\rangle$.*

Extracting information from $|\psi\rangle$ by measuring $|\psi\rangle$ with respect to the basis $\{|0 \ldots 0\rangle, \ldots, |1 \ldots 1\rangle\}$ gives the following result. The function ψ is one-way 1-resistant and collision 0-resistant. So, in contrary to the Example 2.1 the encoding ψ from the Example 2.2 is collision free, that is, for different words v and w quantum states $|\psi(v)\rangle$ and $|\psi(v)\rangle$ are orthogonal and therefore reliably distinguished; but we loose the one-way property: ψ is easily invertible.

The following result [4] shows that quantum collision δ-resistant $(K; s)$ function needs at least $\log \log K - c(\delta)$ qubits.

Property 2.4 ([4]) *Let $s \geq 1$ and $K = |\mathbb{X}| \geq 4$. Let $\psi : \mathbb{X} \to (\mathcal{H}^2)^{\otimes s}$ be a δ-resistant $(K; s)$ hash function. Then*

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

Properties 2.4 and 2.1 provide a basis for building a "balanced" one-way ϵ-resistance and collision δ-resistance properties. That is, roughly speaking, if we need to hash elements w from a domain $\mathbb{X}$ with $|\mathbb{X}| = K$ and if one can build for a $\delta > 0$ a collision δ-resistant $(K; s)$ hash function ψ with $s \approx \log \log K - c(\delta)$ qubits then the function f will be a one-way ϵ-resistant with $\epsilon \approx (\log K/K)$.

3 "Balanced" Quantum Hash Functions Constructions

We start by recalling some definitions, notations, and facts from [15]. For a field $\mathbb{F}_q$, the discrete Fourier transform of a set $B \subseteq \mathbb{F}_q$ is the function

$$f_B(w) = \sum_{b \in B} \exp\left[i\frac{2\pi wb}{q}\right]$$

defined for every $w \in \mathbb{F}_q$. let $\lambda(B) = \max_{w \neq 0} |f_B(w)|/|B|$. 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 $w \in \mathbb{F}_q$, define a function $h_b : \mathbb{F}_q \to \mathbb{F}_q$ and a family H_B by the rule

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

We denote by $H_{\delta,q}$ the above set of functions and call $H_{\delta,q}$ δ-good if $B = B_{\delta,q}$ is δ-good.

Theorem 3.1 *Let $\delta > 0$ and q be a prime power. Let $H_{\delta,q} = \{h_1, \ldots, h_T\}$ be δ-good. Then for $s = \log T$ a function*

$$\left|\psi_{H_{\delta,q}}(w)\right\rangle = \frac{1}{\sqrt{T}} \sum_{j=1}^{T} \exp\left[i\frac{2\pi h_j(w)}{q}\right]|j\rangle. \tag{2}$$

is a collision δ-resistant (q; s) quantum hash function.

Proof. Note, that the proof of this theorem in terms of amplitude transformation was presented in [3]. The proof presented below is in terms of phase transformation [10].

Let $B_{\delta,q} = \{b_1, \ldots, b_T\}$ determines δ-good family $H_{\delta,q}$. We let $H = H_{\delta,q}$ in the proof. We consider the following quantum function $\psi_H : \mathbb{F}_q \to (\mathcal{H}^2)^{\otimes s}$ of function ψ_H

$$|\psi_H(w)\rangle = \frac{1}{\sqrt{T}} \sum_{j=1}^{T} \exp\left[i\frac{2\pi h_j(w)}{q}\right]|j\rangle = \frac{1}{\sqrt{T}} \sum_{j=1}^{T} \exp\left[i\frac{2\pi w b_j}{q}\right]|j\rangle.$$

The quantum state $|\psi_H(w)\rangle$ composed from s qubits. To show that ψ_H is collision δ-resistant $(q; s)$ quantum hash function we prove the collision δ-resistance of ψ_H. Consider a pair w, w' of different elements from $\mathbb{F}_q$ and their inner product $\langle\psi_H(w)|\psi_H(w')\rangle$. Recall that the inner product of two complex vectors $|\alpha\rangle = (\alpha_1, \ldots, \alpha_T)$ and $|\beta\rangle = (\beta_1, \ldots, \beta_T)$ 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. Using the fact that the conjugate of $e^{i\phi}$ is $e^{-i\phi}$, and the fact that $B_{\delta,q}$ is δ-good we have that

$$\langle\psi_H(w)|\psi_H(w')\rangle = \frac{1}{T}\sum_{b\in B_{\delta,q}} \exp\left[i\frac{2\pi(w-w')b}{q}\right] \leq \lambda(B_{\delta,q}) \leq \delta.$$

□

- In [4] we defined a set of discrete functions a *quantum hash generator* if it allow to built a quantum hash function.

In the context of Theorem 3.1 the set $H_{\delta,q}$ is a collision δ-resistant hash generator: it generates the quantum hash function $\psi_{H_{\delta,q}}$.

Optimality of the hashing scheme. The following facts were presented in [15]. 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 $|B_{\delta,q}| = (\log q/\delta(q))^{O(1)}$. Several optimal (in the sense of the above lower bound) explicit constructions of δ-good sets $B_{\delta,q}$ were presented by different authors. For those constructions

$$\delta(q) = \frac{1}{(\log q)^{O(1)}} \quad \text{and} \quad |B_{\delta,q}| = (\log q)^{O(1)}.$$

The following statement summarize Theorem 3.1 and the above consideration.

Corollary 3.1 *Let q be a prime power, $T(q) = (\log q)^{O(1)}$, and $s = \log T(q)$. Let $\epsilon(q) = T(q)/q$ and $\delta(q) = 1/T(q)$. Let $H_{\delta,q}$ be $\delta(q)$-good set of functions with $|H_{\delta,q}| = T(q)$. Then*

1. $\psi_{H_{\delta,q}}$ *is "balanced" quantum $(\epsilon(q), \delta(q))$-resistant quantum $(T(q); s)$-hash function.*

2. *The number s of qubits is good in the sense of the lower bound of Property 2.4 which gives the following lower bound $s \geq \log \log q - \log \log \left(1 + \sqrt{2/\delta}\right) - 1$.*

We refer to the paper [3] for more information on practical construction of the set $H_{\delta,q}$ and the Numerical results from genetic algorithm for $H_{\delta,q}$ construction.

Balanced Quantum Hash Function Families. In [4] we offered design, which allows to build a large amount of different quantum hash functions. The construction is based on composition of classical ϵ-universal hash family [16] and a given family $H_{\delta,q}$ a quantum hash generator. A resulting family of functions is a new quantum hash generator. In particular, we present a quantum hash generator G_{RS} based on Reed-Solomon code.

Let q be a prime power, 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 $C_{RS} : (\mathbb{F}_q)^k \to (\mathbb{F}_q)^n$ defined as follows. Each word $w \in (\mathbb{F}_q)^k$, $w = w_0 w_1 \ldots w_{k-1}$ associated with the polynomial $P_w(x) = \sum_{i=0}^{k-1} w_i x^i$. Pick n distinct elements (evaluation points) $A = \{a_1, \ldots, a_n\}$ of $\mathbb{F}_q$. A common special case is $n = q - 1$ with the set of evaluating points being $A = \mathbb{F}_q \backslash \{0\}$. To encode word w we evaluate $P_w(x)$ on over all n elements $a \in A$ $C_{RS}(w) = (P_w(a_1) \ldots P_w(a_n))$.

We define family $F_{RS} = \{f_a : a \in A\}$ based on RS-code C_{RS} as follows. For $a \in A$ define $f_a : (\mathbb{F}_q)^k \to \mathbb{F}_q$ by the rule $f_a(w) = P_w(a)$. Let $H_{\delta,q} = \{h_1, \ldots, h_T\}$ be a δ-good set of functions, satisfying Corollary 3.1. Composition

$$G_{RS} = F_{RS} \circ H_{\delta,q} = \{g_{jl} : g = h_j(f_{a_l}), h_j \in H_{\delta,q}, f_{a_l} \in F_{RS}\}$$

is a quantum hash generator. Let $s = \log n + \log T$. G_{RS} generates function $\psi_{G_{RS}} : (\mathbb{F}_q)^k \to (\mathcal{H}^2)^{\otimes s}$ for a word $w \in (\mathbb{F}_q)^k$ by the rule

$$|\psi_{G_{RS}}(w)\rangle = \frac{1}{\sqrt{nT}} \sum_{l=1,j=1}^{n,T} \exp\left[i\frac{2\pi g_{jl}(w))}{q}\right]|lj\rangle \tag{3}$$

here $|lj\rangle$ denotes a basis quantum state, where lj is treated as a concatenation of the binary representations of l and j.

Property 3.1 *Let q be a prime power and let $2 \leq k < n \leq q$. Then for arbitrary $\delta \in (0,1)$ the function $\psi_{G_{RS}}$ is an (ϵ, Δ)-resistant $(q^k; s)$ quantum hash function, where $\epsilon \leq (q \log q)/q^k$, $\Delta \leq \frac{k-1}{n} + \delta$, and $s \leq \log(q \log q) + 2 \log 1/\delta + 4$.*

Let $c > 1$. If we select $n = ck$, then $\Delta < 1/c + \delta$ and according to Theorem 2.4 there exist constants $c_1(\Delta)$, $c_2(\Delta)$ such that $\log(q \log q) - c_1(\Delta) \leq s \leq \log(q \log q) + c_2(\Delta)$. Thus, Reed Solomon codes provide balanced parameters for resistance values ϵ, Δ and for a number s of qubits for hash function ψ_{RS}.

4 Presenting Quantum Hash States via Coherent States

Written in the form given in (2) and (3), the hash states $\left|\psi_{H_{\delta,q}}(w)\right\rangle \in (\mathcal{H}^2)^{\otimes s}$, $w \in \mathbb{F}_q$, and $|\psi_{RS}(w)\rangle \in (\mathcal{H}^2)^{\otimes s}$, $w \in (\mathbb{F}_q)^k$, need high degree of entanglement between s qubits which is hard for the current technology. Papers [11, 12, 7] consider the idea of presenting quantum fingerprinting states via coherent states and developed signature constructions based on such coherent states.

Following idea from [11, 12], we map the hash state $\left|\psi_{H_{\delta,q}}(w)\right\rangle \in (\mathcal{H}^2)^{\otimes s}$ for $w \in \mathbb{F}_q$ to a coherent state as follows. For short we let $H_{\delta,q} = H$ in the rest of the section. Let $T = 2^s$. First, we define *hash mode* (H-hash mode) $a_{H,w}$ as

$$a_{H,w} = \frac{1}{\sqrt{T}} \sum_{j=1}^{T} \exp\left[i\frac{2\pi h_j(w)}{q}\right] b_j,$$

where $b_j \in \{b_1, \ldots, b_T\}$ is the annihilation operator of the jth optical mode. Hash state is a single-photon state in the hash mode: $|\psi_H(w)\rangle = a_{H,w}|0\rangle$.

Next, we define *coherent hash state* as $|\alpha, \psi_H(w)\rangle = D_{H,w}(\alpha)|0\rangle$, with parameter α, where $D_{H,w}(\alpha) = \exp\left[\alpha a_{H,w}^\dagger - \alpha^* a_{H,w}\right]$ is the displacement operator. According to [12] we have that the state $|\psi_H(w)\rangle$ is mapped to $|\alpha, \psi_H(w)\rangle$:

$$|\psi_H(w)\rangle \quad \rightarrow \quad |\alpha, \psi_H(w)\rangle = \bigotimes_{j=1}^{T} \left|\exp\left[i\frac{2\pi h_j(w)}{q}\right]\frac{\alpha}{\sqrt{T}}\right\rangle_j,$$

where $\left|\exp\left[i\frac{2\pi h_j(w)}{q}\right]\frac{\alpha}{\sqrt{T}}\right\rangle_j$ is a coherent state with amplitude $\frac{\alpha}{\sqrt{T}}$ in the jth mode.

Similarly one can map the hash state $|\psi_{RS}(w)\rangle \in (\mathcal{H}^2)^{\otimes s}$ with $w \in (\mathbb{F}_q)^k$ to a coherent state.

In the next paper we will present a variants of quantum signature schemes based on quantum hash functions different from quantum fingerprinting function.

References

[1] Daniel Gottesman and Isaac Chuang. Quantum digital signatures. Technical Report arXiv:quantph/0105032, Cornell University Library, Nov 2001.

[2] Dmitry Gavinsky and Tsuyoshi Ito. Quantum fingerprints that keep secrets. Technical Report arXiv:1010.5342, Cornell University Library, Oct 2010.

[3] Farid Ablayev and Alexander Vasiliev. Cryptographic quantum hashing. *Laser Phys. Lett.* **11**(2):025202, Dec 2013.

[4] Farid Ablayev and Marat Ablayev. Quantum Hashing via Classical ϵ-universal Hashing Constructions. Technical Report arXiv:1404.1503v2 [quant-ph], Cornell University Library, Jan 2015.

[5] Alexander S. Holevo. Some estimates of the information transmitted by quantum communication channel (russian). *Probl. Pered. Inform. [Probl. Inf. Transm.]*, 9(3):311, 1973.

[6] A. Korol'kov. About some applied aspects of quantum cryptography in the context of development of quantum computations and emergense of quantum computations and emergence of quantum computers (russian). *Voprosy kiberbezopasnosty*, 1(9), 2015.

[7] Ryan Amiri and Erika Andersson. Unconditionally Secure Quantum Signature. *Entropy*, 17:5635–5659, 2015.

[8] Farid Ablayev and Alexander Vasiliev. Computing Boolean Functions via Quantum Hashing, Computing with New Resources. *Lecture Notes in Computer Science. - Springer Berlin / Heidelberg*, 8808:149–160, 2014.

[9] Alexander Vasiliev. Quantum Communications Based on Quantum Hashing. *International Journal of Applied Engineering Research*, 10(12):31415–31426, 2015.

[10] Marat Ablayev. On Constructing Quantum Hash Functions (russian). *9th International Conference "Diskretnye modely v teorii upravlyauschih system", Moscow State University*, 8–9, 2015.

[11] Juan Arrazola, and Norbert Lütkenhaus. Quantum Fingerprinting with Coherent States and a Constant Mean Number of Photons. 2014 *Phys. Rev.* A **89**, 062305.

[12] Juan Arrazola, and Norbert Lütkenhaus. Quantum Communication with Coherent States and Linear Optics. 2014 *Phys. Rev.* A **90**, 042335.

[13] Ashwin Nayak. Optimal Lower Bounds for Quantum Automata and Random Access Codes. Technical Report arXiv:quant-ph/9904093v3, Cornell University Library, Sep 1999.

[14] Andris Ambainis and Rusin Freivalds. 1-Way Quantum Finite Automata: Strengths, Weaknesses and Generalizations. Technical Report ArXiv:quant-ph/9802062v3, Cornell University Library, Sep 1998.

[15] Alexander Razborov, Endre Szemeredi, and Avi Wigderson. Constructing small sets that are uniform in arithmetic progressions. Combinatorics, *Probability & Computing*, 2:513–518, 1993.

[16] Douglas Stinson. On the connections between universal ϵ-hashing, combinatorial designs and error-correcting codes. *Congressus Numerantium* 114:7–27, 1996.