ISSN 1995-0802, Lobachevskii Journal of Mathematics, 2016, Vol. 37, No. 6, pp. 758–767. © Pleiades Publishing, Ltd., 2016.

On Quantum (δ, ϵ)-Resistant Hashing

M. Ablayev*

(Submitted by M. M. Arslanov)

Laboratory of Quantum Informatics,
Institute of Computational Mathematics and Information Technologies,
Kazan (Volga Region) Federal University, Kremlevskaya ul. 35, Kazan, 420008 Tatarstan, Russia

Received May 22, 2016

Abstract—In the paper we define a notion of quantum resistant ((δ, ϵ)-resistant) hash function which combine together a notion of pre-image (one-way) resistance (δ-resistance) property and the notion of collision resistance (ϵ-resistance) properties. We present a discussion that supports the idea of quantum hashing oriented for cryptographical purposes. We propose a quantum setting of a classical digital signature scheme do demonstrate a theoretical possibilities and restrictions of (δ, ϵ)-hashing. The assumption we use is that a set of qubits (quantum hash) we generate, send, and receive during the execution of a protocol can be stored for a certain (a large enough) amount of time; next, the scheme requires the high degree of entanglement between the qubits which makes such a quantum hash. These properties make quantum hash cryptographically efficient.

DOI: 10.1134/S1995080216060081

Keywords and phrases: *Quantum hashing, quantum hash function, δ-universal hashing, error-correcting codes, quantum signature.*

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 [12] which is based on quantum one-way function. This is also the case for other protocols (see for example [11]). In [4, 2] 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 which are actually quantum hash functions. Those functions have "unconditionally one-way" property based on Holevo Theorem [13].

A good source of information on the state of now days development in area of cryptographic hashing and quantum signatures presented the review paper [9]. Recall that in the classical setting a cryptographic hash function h should have the following three properties [9]. (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 [4, 2] 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:

*E-mail: mablayev@gmail.com

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" (ϵ-orthogonal) [2].

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

In papers [5, 18] 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 (δ, ϵ)-hash function where values δ and ϵ are numerical characteristics of the above two properties: (i) one-way resistance and (ii) collision resistance properties. The notion of the (δ, ϵ)-hash function is an explicit generalization of constructions presented in [4, 2]. 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 [6] instead of "amplitude transformation" [2].

Finally we propose a quantum double key signature scheme as a one of the possible applications of quantum hashing. The proposed scheme can be viewed as a quantum generalization of classical approach of double key digital signature schemes.

2. QUANTUM (δ, ϵ)-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 $|\sigma_1\rangle \cdots |\sigma_s\rangle = |\sigma_1\rangle \otimes \cdots \otimes |\sigma_s\rangle$.

We let $\mathbb{Z}_q$ to be finite additive group of Z/qZ, the integers modulo 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 $\mathbb{X} = \mathbb{Z}_q$. 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 δ-Resistance

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

Definition 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 $\mathbf{M}$ making measurement to the encoding ψ of X and decoding the result of measurement to $\mathbb{X}$. Let $\delta > 0$. We call a quantum function ψ a one-way δ-resistant function if*

1. *if it is easy to compute, i.e., a quantum state* $|\psi(w)\rangle$ *for a particular* $w \in \mathbb{X}$ *can be determined using a polynomial-time algorithm*

2. *for any mechanism* $\mathbf{M}$, *the probability* $Pr[Y = X]$ *that* $\mathbf{M}$ *successfully decodes* Y *is bounded by* δ

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

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 [13] states that a quantum measurement can only give s bits of information about the state. We will use here the following particular version [15] of Holevo's Theorem.

Property 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* $\mathbf{M}$ *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 ϵ*-Resistance*

The following definition was presented in [2].

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

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

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 [12].

SWAP-test. The *SWAP-test* is the known quantum test for the equality of two unknown quantum states $|\psi\rangle$ and $|\psi'\rangle$ (see [12, 4] 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 "$|\psi(v)\rangle = |\psi(w)\rangle$"). The following statement presented in [12].

Property 2. *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* $|\langle\psi(v)|\psi(w)\rangle| \leq \epsilon$. *Then*

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

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

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

□

REVERSE-test. The next test for equality was first mentioned in [2]. We call this test a *REVERSE-test* [4]. *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 state (quantum hash), i.e. it "uncomputes" the quantum hash to the initial quantum 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 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 $|\langle\psi(v)|\psi(w)\rangle| \le \epsilon$. Then*

$$Pr_{reverse}[v=w] \le \epsilon^2.$$

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

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

□

2.3. Balanced Quantum (δ,ϵ)-Resistance

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

Definition 3. *Let $K=|\mathbb{X}|$ and $s \ge 1$. Let $\delta > 0$ and $\epsilon > 0$. We call a function $\psi: \mathbb{X} \to (\mathcal{H}^2)^{\otimes s}$ a quantum (δ,ϵ)-Resistant $(K;s)$-hash function (or just quantum (δ,ϵ)-Resistant hash function) iff ψ is a one-way δ-resistant and is a collision* ϵ-resistant function.

We present below the following two examples to demonstrate how one-way δ-resistance and collision ϵ-resistance are correlated. The first example was presented in [8] in terms of quantum automata.

Example 1. *Let us encode numbers v from $\{0,\dots,2^k-1\}$ 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 1) and collision $\cos\left(\pi/2^{k-1}\right)$-resistant. According to the properties 1 and 3 the function ψ has good one-way property, but has bad resistance property for a large k.

Example 2. *We consider a number $v \in \{0,\dots,2^k-1\}$ to be also a binary word $v \in \{0,1\}^k$. Let $v=\sigma_1\dots\sigma_k$. 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 $\{|0\dots0\rangle,\dots,|1\dots1\rangle\}$ gives the following result. The function ψ is one-way 1-resistant and collision 0-resistant. So, in contrary to the Example 1 the encoding ψ from the Example 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 [2] shows that quantum collision ϵ-resistant $(K;s)$ function needs at least $\log\log K - c(\epsilon)$ qubits. The following statement presented in [2].

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

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

Proof. The proof of this fact use a known combinatorial arguments and is a folklore. See [2] for technical details. □

Properties 4 and 1 provide a basis for building a "balanced" one-way δ-resistance and collision ϵ-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 $\epsilon > 0$ a collision ϵ-resistant $(K;s)$ hash function ψ with $s \approx \log\log K - c(\epsilon)$ qubits then the function f will be a one-way δ-resistant with $\delta \approx (\log K/K)$. Such a function will be balanced in respect to the Property 4.

To summarize the above consideration we can state (see also [9]) the following. A quantum (δ,ϵ)-resistant hash function is a function that satisfies all of the properties that a "classical" hash function should satisfy. Pre-image resistance follows from HolevoTs–Nayak's theorem. Second pre-image resistance and collision resistance follow, because all input states are mapped to states that are ϵ-orthogonal. Therefore, we see that quantum hash functions can satisfy the three conditions with information-theoretic security.

3. QUANTUM (δ, ϵ)-RESISTANT HASH FUNCTIONS CONSTRUCTION VIA SMALL-BIASED SETS

This section is based on the paper [19]. We present here a connection of the notion of quantum hashing and small-biased sets in terms of the paper.

We present here brief background on ϵ-biased sets and discuss their connection to quantum hashing. Note that ϵ-biased sets generally defined for arbitrary Abelian group, we restrict here ourselves to finite field $\mathbb{Z}_q$.

For an $a \in \mathbb{Z}_q$ a character χ_a of $\mathbb{Z}_q$ is a homomorphism $\chi_a : \mathbb{Z}_q \to \mu_q$, where μ_q is the (multiplicative) group of complex q-th roots of unity, $\chi_a(x) = \omega^{ax}$. Here $\omega = e^{\frac{2\pi i}{q}}$ is a primitive complex qth root of unity. A character $\chi_0 \equiv 1$ is called a trivial character.

- A set $S \subseteq \mathbb{Z}_q$ is called ϵ-biased, if for any nontrivial character $\chi \in \{\chi_a : a \in \mathbb{Z}_q\}$

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

These sets are interesting when $|S| \ll |\mathbb{Z}_q|$ (as $S = \mathbb{Z}_q$ is 0-biased). The seminal paper of Naor and Naor [14] defined these small-biased sets, gave the first explicit constructions of such sets, and demonstrated the power of small-biased sets for several applications.

- Note that a set S of $O(\log q/\epsilon^2)$ elements selected uniformly at random from $\mathbb{Z}_q$ is ϵ-biased with a positive probability >0 [7].

Many other constructions of small-biased sets followed during the last decades.

Vasiliev [19] showed that ϵ-biased sets generate collision ϵ-resistant hash functions. We present the result of [19] in terms of the paper in the following form.

Property 5. *Let $S \subseteq \mathbb{Z}_q$ be an ϵ-biased set. Let $H_S = \{h_a(x) = ax \pmod q, \quad a \in S\}$ be a set of functions $(h_a : \mathbb{Z}_q \to \mathbb{Z}_q)$ determined be S. Then a quantum function $\psi_S : \mathbb{Z}_q \to (\mathcal{H}^2)^{\otimes \log |S|}$*

$$|\psi_S(x)\rangle = \frac{1}{\sqrt{|S|}} \sum_{a \in S} \omega^{h_a(x)} |a\rangle$$

is an an (δ, ϵ)-resistant quantum hash function, where $\delta \leq |S|/(q \log q)$.

Proof. One-way δ-resistance property of ψ_S follows from Property 1: a probability of correct decoding an x from a quantum state $|\psi_S(x)\rangle$ (in the meaning of Definition 1) is bounded by $|S|/(q \log q)$.

Collision ϵ-resistance property of ψ_S follows directly from the corresponding property of [19]. Note that

$$|\psi_S(x)\rangle = \frac{1}{\sqrt{|S|}} \sum_{a \in S} \omega^{h_a(x)} |a\rangle = \frac{1}{\sqrt{|S|}} \sum_{a \in S} \chi_x(a) |a\rangle.$$

Further proof coincides with the proof of the paper [19]. □

- It is natural to call the set H_S of functions a *uniform ϵ-biased quantum hash generator* in the contest of the definition of quantum hash generator [1] and the above consideration.

As a corollary from Property 5 and the above consideration we can state the following.

Property 6. *For a small size ϵ-biased set $S = \{a_1, \ldots, a_T\} \subset \mathbb{Z}_q$ with $T = O(\log q/\epsilon^2)$, for $\delta = O(1/(q\epsilon^2))$ a quantum hash generator H_S generates balanced (δ, ϵ)-resistant quantum hash function ψ_S*

$$|\psi_S(x)\rangle = \frac{1}{\sqrt{T}} \sum_{j=0}^{T-1} \omega^{a_j x} |j\rangle. \tag{2}$$

3.1. Computing A Quantum Hash $|\psi_S(x)\rangle$

In this section we let $S \subset \mathbb{Z}_q$ to be a small size ϵ-biased set corresponding Property 6, that is, $S = \{a_1, \ldots, a_T\}$ with $T = O(\log q/\epsilon^2)$.

Computing $|\psi_S(x)\rangle$ by ϵ-biased Fourier transform. Let F_S be an $T \times q$ matrix. The rows of F_S are indexed by $a \in S = \{a_0, \ldots, a_{T-1}\}$ and the columns indexed by $x \in \{0, \ldots q-1\}$. An (a, x)-entry of the matrix F_S is $\frac{1}{\sqrt{T}}\omega^{ax}$. Then the quantum hash state $|\psi_S(x)\rangle$ (2) can be viewed as the result of the action of linear operator F_S (ϵ-biased Fourier transform) on the basis state $|x\rangle$ for $x \in \{0, \ldots q-1\}$

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

Following the construction from the section "The quantum Fourier transform" [16] it is not hard work to derive an efficient quantum circuit for the ϵ-biased Fourier transform F_S.

Computing $|\psi_S(x)\rangle$ by Quantum Branching Program Curcuit. Consider a Quantum Read-once Branching Program circuit [3] modified for computing a states $|\psi_S(x)\rangle : x \in \mathbb{Z}_q$. We represent an integer $x \in \{0, \ldots, q-1\}$ as the bit-string $x = x_0 \ldots x_{\log q - 1}$ that is the binary representation of $x = x_0 + 2^1 x_1 + \cdots + 2^{\log q - 1} x_{\log q - 1}$.

For a binary string $x = x_0 \ldots x_{\log q - 1}$ a Quantum Branching Program Q over the space $(\mathcal{H}^2)^{\otimes s}$ for computing $|\psi_S(x)\rangle$ (composed of $s = \log T$ qubits) is defined as $Q = \langle \mathbb{T}, |\psi_0\rangle\rangle$, where the state

$$|\psi_0\rangle = \frac{1}{\sqrt{T}} \sum_{j=0}^{T-1} |j\rangle$$

is the initial state of Q. $\mathbb{T}$ is a sequence of $\log q$ instructions:

$$\mathbb{T}_j = (x_j, U_j(0), U_j(1))$$

is determined by the variable x_j tested on the step j, and $U_j(0)$, $U_j(1)$ are unitary transformations in $(\mathcal{H}^2)^{\otimes s}$. More precise $U_j(0)$ is $T \times T$ identity matrix. $U_j(1)$ is the $T \times T$ diagonal matrix whose diagonal entries are $\omega^{a_0 2^j}, \omega^{a_1 2^j}, \ldots, \omega^{a_{T-1} 2^j}$ and the off-diagonal elements are all zero. That is,

$$U_j(1) = \begin{bmatrix} \omega^{a_0 2^j} & & & \\ & \omega^{a_1 2^j} & & \\ & & \ddots & \\ & & & \omega^{a_{T-1} 2^j} \end{bmatrix}.$$

We define a computation of Q on an input $x = x_1 \ldots x_{\log q} \in \{0,1\}^{\log q}$ as follows:

1. a computation of Q starts from the initial state $|\psi_0\rangle$;
2. the j-th instruction of Q reads the input symbol x_j (the value of x) and applies the transition matrix $U_j(x_j)$ to the current state $|\psi\rangle$ to obtain the state $|\psi'\rangle = U_j(x_j)|\psi\rangle$;
3. the final state is

$$|\psi_S(x)\rangle = \left(\prod_{j=0}^{\log q - 1} U_j(x_j) \right) |\psi_0\rangle.$$

To summarize the above construction of the Read-once Quantum Branching Program Q we formulate the following property.

Property 7. *For $x \in \mathbb{Z}_q$, for ϵ-biased set $S \subset \mathbb{Z}_q$, $|S| = T$, quantum state (quantum hash state) $|\psi_S(x)\rangle$ (2) can be computed by the quantum read-once branching program Q composed from $s = \log T$ qubits in $\log q$ steps.*

There is a homomorphism between $\mathbb{Z}_q$ and the set of unitary operators, which define quantum states $\{|\psi_S(x)\rangle : x \in \mathbb{Z}_q\}$. That is for $x, b \in \mathbb{Z}_q$

$$|\psi_S(x+b)\rangle = U_S(b)|\psi_S(x)\rangle,$$

where $U_S(b)$ is $T \times T$ diagonal matrix whose diagonal entries are $\omega^{a_0 b}, \omega^{a_1 b}, \ldots, \omega^{a_{T-1} b}$.

4. DIGITAL SIGNATURE SCHEME: QUANTUM SETTING

Many kinds of quantum signature schemes presented during the last decades oriented to current and nearest coming quantum technology. We refer to the review [9] for different quantum schemes descriptions and more information on the subject. In this section we propose a quantum setting of a classical digital scheme do demonstrate a theoretical possibilities and restictions of (δ, ϵ)-hashing. For example, such a classical one is a known Diffie–Hellman signature scheme. Roughly speaking in a quantum setting a classical one-way function (the discrete logarithm function for Diffie–Helmann scheme) is replaces by quantum hash function.

Such a quantum setting of a classical signature scheme is "a very theoretical" for the now days quantum technology: the assumption we use is that a set of qubits (quantum hash) we generate, send, and receive during the execution of a protocol can be stored for a certain (a large enogh) amount of time. The last is a great problem for a quantum technology.

Classical Digital Signature Scheme. Recall that a digital signature is a mathematical scheme for demonstrating the authenticity of a digital message. A valid digital signature gives a recipient reason to believe that the message was created by a known sender, that the sender cannot deny having sent the message (authentication and non-repudiation), and that the message was not altered in transit (integrity).

A digital signature scheme typically consists of three algorithms (G, S, V):

1. G (key-generator) a key generation algorithm that selects a private (secret) key sk uniformly at random from a set of possible private keys. The algorithm outputs the private key sk and a corresponding public key pk;

2. S (signing) a signing algorithm that, given a message m and a private key sk, produces a signature (tag) t;

3. V (verifying) outputs *"accept"* or *"reject"* on the inputs: the public key, pk, a message, m, and a tag, t. That is, V given the message, public key and signature, either accepts or rejects the message's claim to authenticity.

Two main properties are required. First, the authenticity of a signature generated from a fixed message and fixed private key can be verified by using the corresponding public key. Secondly, it should be computationally infeasible to generate a valid signature for a party without knowing that party's private key. A digital signature is an authentication mechanism that enables the creator of the message to attach a code that acts as a signature.

Below we present quantum signature scheme—a quantum generalization of classical double-key digital signature schemes.

Quantum Signature Scheme. Key generation Phase. Both parties *Alice* and *Bob* publicly select $\mathbb{Z}_q$, and a (small size) ϵ-biased set $S \subset \mathbb{Z}_q$. Say an ϵ-biased set $S = \{a_1, \ldots, a_T\}$ with $T = O(\log q/\epsilon^2)$.

As a result *Alice* and *Bob* publicly fix a corresponding quantum hash generator H_S that generates balanced (δ, ϵ)-resistant quantum hash function

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

with $\delta \leq O(1/(\epsilon^2 q))$ in according to Property 5:

$$|\psi_S(x)\rangle = \frac{1}{\sqrt{|S|}} \sum_{a \in S} \omega^{h_a(x)} |a\rangle.$$

- *Alice* generates her private (secret) key sk—an element $b \in \mathbb{Z}_q$ uniformly at random from $\mathbb{Z}_q$, $(sk = b)$;
- *Alice* computes a public key pk (quantum state) $pk = |\psi_S(b)\rangle$;

$$|\psi_S(b)\rangle = \frac{1}{\sqrt{|S|}} \sum_{a \in S} \omega^{h_a(b)} |a\rangle;$$

- *Alice* sends public key $|\psi_S(b)\rangle$ to *Bob*.

Quantum Signature Scheme. Signing Phase

- *Alice* has a message $m \in \mathbb{Z}_n$ to sign;
- Signature equation is $y + m = b$;
- *Alice* given a message m, private key b, and a solution $y \in \mathbb{Z}_q$ of a signature equation produces a signature (a tag)

$$|\psi_S(y)\rangle = \frac{1}{\sqrt{|S|}} \sum_{a \in S} \omega^{h_a(y)} |a\rangle.$$

  That is, based on a second private key y according to the signature equation *Alice* generates a signature $|\psi_S(y)\rangle$;
- *Alice* sends to *Bob* a pair (message,signature) $(m, |\psi_S(y)\rangle)$.

Quantum Signature Scheme. Verifying Phase

- Using m computes state

$$|\psi(y + m)\rangle = \frac{1}{\sqrt{|S|}} \sum_{a \in S} \omega^{h_a(y+m)} |a\rangle;$$

- Verify (using the SWAP-test) whether $|\psi(b)\rangle = |\psi(y + m)\rangle$.

  If many copies of the two states are available, performing the SWAP-test many times determines whether the states are equal or not with a probability that can be made arbitrarily close to one (see for example [9]).

Quantum Signature Scheme. Security. Clearly the proposed quantum signature scheme is non-repudiation, that is, the sender cannot deny having sent the message.

In the case when *Eve* (adversary) can create only "passive attacks", that is, *Eve* can only "read an information without it modification" (classical and quantum) exchanged between *Alice* and *Bob* but do not have possibility to modify these information, then clearly the proposed scheme is secure. That is, the proposed signature scheme gives a recipient reason to believe that the message was created by a known sender, that the sender cannot deny having sent the message (authentication and non-repudiation), and that the message was not altered in transit (integrity).

In the case of "intercept and resend" attack an *Eve* selects her own key $b' \in \mathbb{Z}_q$, replace the *Alice's* public key $pk = |\psi_S(b)\rangle$ by $|\psi_S(b')\rangle$, and further replace message m by m' and the tag $|\psi_S(y)\rangle$ by $|\psi_S(y')\rangle$, where $y' + m' = b'$.

Another "intercept and resend" attack is based on the property that quantum function $\psi_S : \mathbb{Z}_q \to (\mathcal{H}^2)^{\otimes s}$ is a homomorphism between $\mathbb{Z}_q$ and the set of unitary operators, which define quantum hash values, see Property 7. So, a simple forgery scheme is the following. *Eve* do not modify the public key $pk = |\psi_S(b)\rangle$ but modify a message m to $m' = m + a'$, modify a tag $|\psi_S(y)\rangle$ to $|\psi_S(y')\rangle = |\psi_S(y - a')\rangle$, and replace *Alice's* pair (message,signature) $(m, |\psi_S(y)\rangle)$ by $(m', |\psi_S(y')\rangle)$.

Note, that last years quantum cryptography technology suggests a scheme known as a "relativistic quantum protocols". Relativistic quantum protocols are based on time-spread coherent quantum states, which, due to their distributed nature inevitably cause delays, if successful "intercept and resend" attack is performed. Roughly speaking relativistic quantum protocols technology does not allow to organize the "intercept and resend" attack undetected. See [17] for more details.

5. CONCLUSION

The Definition 3 of quantum (δ, ϵ)-resistant hash function combines together the notions of quantum one-way δ-resistant and quantum collision ϵ-resistant functions. Examples 1 and 2 demonstrate that in the quantum setting the one-way resistance property and collision resistance property can correlate: the "more" a quantum function is one-way resistant the "less" it is collision resistant and vice versa. Such correlation leads to the notion of balanced quantum hash function. In [2] offered design, which allows to build a large amount of different balanced quantum hash functions. Note, that a realization of such quantum functions as the balanced quantum hash function requires the high degree of entanglement between the qubits makes quantum hash cryptographically efficient simultaneously high degree of entanglement between the qubits makes such a state difficult to create with current technology.

Proposed quantum signature scheme needs a quantum memory for storing a public quantum key. The problem of creating a long living quantum memory is a hard problem for the modern quantum technology. In this content the proposed quantum double key signature scheme can be considered as a theoretical generalization of classical of double key digital signature schemes. The nearest practical implementation of quantum signature might be an authentication.

Note also that ϵ-orthogonality property of quantum states are important for constructing quantum bounded-error computational models. The property $k \gg s$ (where k is the length of encoded words and s is the number of qubits for encoding) is the basis for building quantum computational models of low complexity. Constructions of quantum computational models explored these two properties were invented by different authors: first for quantum finite automata [8] and later for quantum communication computations [10]. In [10] authors called such function a quantum fingerprinting.

ACKNOWLEDGMENTS

Kazan Federal University. Partially supported by Russian Foundation for Basic Research, Grants 14-07-00557, 15-37-21160.

REFERENCES

1. F. Ablayev and M. Ablayev, On the conception of cryptographical quantum hashing. arXiv:1509.01268 [quant-ph] (2015).
2. F. Ablayev and M. Ablayev, Quantum hashing via classical δ-universal hashing constructions. arXiv:1404.1503v2 [quant-ph] (2015).
3. F. Ablayev and A. Vasiliev, "Algorithms for quantum branching programs based on fingerprinting," Electronic Proceedings in Theoretical Computer Science **9**, 1–11 (2009).
4. F. Ablayev and A. Vasiliev, "Cryptographic quantum hashing," Laser Phys. Lett. **11** (2), 025202 (2013).
5. F. Ablayev and A. Vasiliev, "Computing Boolean functions via quantum hashing," Computing with New Resources, Lecture Notes in Computer Science **8808**, 149–160 (2014).
6. M. Ablayev, "On constructing quantum hash functions," *Discrete Models in Control Systems Theory: IX International Conference, Moscow and Moscow region, 20–22 May, 2015* (MAKS Press, Moscow, 2015), pp. 8–9 [In Russian].
7. N. Alon and Y. Roichman, "Random Cayley graphs and expanders," Random Structures & Algorithms **5** (2), 271–284 (1994).
8. A. Ambainis and R. Freivalds, 1-Way quantum finite automata: strengths, weaknesses and generalizations. arXiv:quant-ph/9802062v3 (1998).

9. R. Amiri and E. Andersson, "Unconditionally secure quantum signature," Entropy, **17** (8), 5635–5659 (2015).
10. H. Buhrman, R. Cleve, J. Watrous, and R. de Wolf, "Quantum fingerprinting," Phys. Rev. Lett. **87**, 167902 (2001).
11. D. Gavinsky and T. Ito, Quantum fingerprints that keep secrets. arXiv:1010.5342 (2010).
12. D. Gottesman and I. Chuang, Quantum digital signatures. arXiv:quantph/0105032 (2001).
13. A. Holevo, "Some estimates of the information transmitted by quantum communication channel," Probl. Inf. Transm. **9** (3), 177–183 (1973).
14. J. Naor and M. Naor, "Small-bias probability spaces: Efficient constructions and applications," *Proceedings of the Twenty-Second Annual ACM Symposium on Theory of Computing* (1990), pp. 213–223..
15. A. Nayak, Optimal lower bounds for quantum automata and random access codes. arXiv:quant-ph/9904093v3 (1999).
16. M. Nielsen and I. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, 2010).
17. I. Radchenko, K. Kravtsov, S. Kulik, and S. Molotkov, "Relativistic quantum cryptography," Laser Phys. Lett. **11** (6), 065203 (2014).
18. A. Vasiliev, "Quantum communications based on quantum hashing," International Journal of Applied Engineering Research **10** (12), 31415–31426 (2015).
19. A. Vasiliev, Quantum Hashing for Finite Abelian Groups. arXiv:1603.02209 [quant-ph] (2016).