Laser Phys. Lett. **00** (2015) 000000 (5pp)

On the concept of cryptographic quantum hashing

F Ablayev and M Ablayev

Kazan Federal University, Russian Federation, Kazan 420000, Russia

E-mail: fablayev@gmail.com

Received 13 September 2015, revised 15 September 2015
Accepted for publication 15 September 2015
Published

Abstract

In the letter we define the notion of a quantum resistant ((ϵ, δ)-resistant) hash function which consists of a combination of pre-image (one-way) resistance (ε-resistance) and collision resistance (δ-resistance) properties.

We present examples and discussion that supports the idea of quantum hashing. We present an explicit quantum hash function which is 'balanced', one-way resistant and collision resistant and demonstrate how to build a large family of quantum hash functions. Balanced quantum hash functions need a high degree of entanglement between the qubits. We use a phase transformation technique to express quantum hashing constructions, which is an effective way of mapping hash states to coherent states in a superposition of time-bin modes. The phase transformation technique is ready to be implemented with current optical technology.

Keywords: quantum hashing, quantum one-way function, quantum signature

(Some figures may appear in colour only in the online journal)

1. Introduction

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

Gottesman and Chuang proposed in 2001 a quantum digital signature system [1] which is based on a quantum one-way function. This is also an issue for other protocols (see for example [2]). In [3, 4] we explicitly defined the notion of quantum hashing as a generalisation of classical hashing and presented examples of quantum hash functions. It appears that the Gottesman–Chuang quantum signature schemes are based on functions which are actually quantum hash functions. Those functions have an 'unconditionally one-way' property which is based on the Holevo theorem [5]. More information on the role of quantum hashing for post-quantum cryptography, the possible application of quantum hashing for quantum signature protocols, and the technological expectations for the realisation of quantum signature schemes are presented in [6].

Let us recall that in a 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 distinct pair 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 the 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 quantum pure states of s-qubits ($\psi : \Sigma^k \to (\mathcal{H}^2)^{\otimes s}$); it also has the following properties:

(i) The function ψ must be one-way resistant. In the quantum case this means that $k > s$.
(ii) The function ψ must be collision resistant. In the quantum case this means that for different word w, w' states $|\psi(w)\rangle$ and $|\psi(w')\rangle$ must be 'almost orthogonal' (δ-orthogonal) [4].

JNL:LPL PIPS: AA0394 TYPE: LET TS: NEWGEN DATE:17/10/15 EDITOR: IOP SPELLING: US

A quantum collision resistant property covers 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 an adequate quantum technological model for presenting quantum communication protocols and quantum cryptographic signature schemes based on hashing.

In this letter we define the notion of a (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 generalisation of our constructions [3, 4]. We present examples and further discussion that supports the idea of quantum hashing as outlined in our papers. We present a quantum hash function which is 'balanced', one-way resistant and collision resistant.

We present quantum 'balanced' hashing constructions based on a phase transformation presentation [10] instead of an 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 today using technology that uses only a sequence of coherent states, linear optics operations, and measurements with single-photon threshold detectors. See [7, 11, 12] for more information and citations.

2. Quantum (ϵ, δ)-resistant hash function

Let us recall that mathematically a qubit is described as a unit vector in the two-dimensional Hilbert complex space $\mathcal{H}^2$. Let $s \geqslant 1$. Let $(\mathcal{H}^2)^{\otimes s}$ be the 2^s-dimensional Hilbert space, describing the states of s qubits. For the 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 the quantum state $|\sigma_1\rangle \cdots |\sigma_s\rangle = |\sigma_1\rangle \otimes \cdots \otimes |\sigma_s\rangle$.

We let q 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 this letter we let $\mathbb{X} = \Sigma^k$, or $\mathbb{X} = \{0, \ldots, q-1\}$—the support of $\mathbb{F}_q$. For $K = |\mathbb{X}|$ and the integer $s \geqslant 1$ we define a $(K; s)$ quantum function as 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 $|\psi(w)\rangle \in (\mathcal{H}^2)^{\otimes s}$

$$\psi : \{|\psi_0\rangle\} \times \mathbb{X} \to (\mathcal{H}^2)^{\otimes s} \qquad |\psi(w)\rangle = U(w)|\psi_0\rangle \qquad (2.1)$$

where $U(w)$ is a unitary matrix. We let $|\psi_0\rangle = |0\rangle$ in the letter and use (for short) the following notation (instead of the equation defined 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 a quantum ε-resistant one-way function. Let 'information extracting mechanism' $\mathcal{M}$ be a function $\mathcal{M} : (\mathcal{H}^2)^{\otimes s} \to \mathbb{X}$ measuring the state $|\psi\rangle \in (\mathcal{H}^2)^{\otimes s}$ and decoding the results of the measurements to $\mathbb{X}$.

Definition 2.1. Let X be a 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 be any random variable over $\mathbb{X}$ obtained by some mechanism $\mathcal{M}$ measuring the encoding ψ of X and decoding the result of the 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

$$Pr[\, Y = X] \leqslant \epsilon.$$

For cryptographic purposes it is natural to expect that the random variable X is uniformly distributed; we apply this expectation to the rest of the letter.

A quantum state of $s \geqslant 1$ qubits can 'carry' an infinite amount of information. On the other hand, the fundamental result of quantum informatics which is 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 a random variable uniformly distributed over k bit binary words $\{0, 1\}^k$. Let $\psi : \{0, 1\}^k \to (\mathcal{H}^2)^{\otimes s}$ be a $(2^k; s)$ 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 the measurement to $\{0, 1\}^k$. Then our probability of correct decoding is given by

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

2.2. Collision resistant function

The following definition is 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,

$$\left|\langle \psi(w) | \psi(w') \rangle\right| \leqslant \delta.$$

What one needs for the realisation of quantum digital signature schemes 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 recognised quantum test for the equality of two unknown quantum states $|\psi\rangle$ and $|\psi'\rangle$. This test, which can be implemented efficiently, takes two states $|\psi\rangle$ and $|\psi'\rangle$ as input, and returns 'same' with probability $\frac{1}{2}(1 + |\langle\psi|\psi'\rangle|^2)$ otherwise returning 'different' (see [1, 3] for more information).

The next test for equality was first mentioned in [1]. We call this test the *REVERSE-test* [3]. The *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, in the procedure of quantum hashing let the element w be given by unitary transformation $U(w)$, applied to the 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 in respect to the initial state $|0\rangle$. It outputs $v = w$ if the measurement outcome is $|0\rangle$. Denote by $Pr_{\text{reverse}}[v = w]$ the probability that the *REVERSE-test* having a quantum state $|\psi(w)\rangle$ and an element v outputs the result that $v = w$.

Property 2.2. 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 $\left|\langle\psi(v)|\psi(w)\rangle\right| \leqslant \delta$. Then

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

Proof. Using the property that unitary transformation keeps the scalar product we have that $Pr_{\text{reverse}}[v = w] = |\langle 0|U^{-1}\rangle(v)\psi(w)\rangle|^2 = |\langle U^{-1}(v)(w)\rangle|^2 = |\langle\psi(v)|\psi(w)\rangle|^2 \leqslant \delta^2$. □

2.3. One-way resistance and collision resistance

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

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

We present below the following two simple examples to demonstrate the above definitions. 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 $|\psi\rangle$ in 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 $\cos(\pi/2^{k-1})$-resistant. In accordance with the properties 2.1 and 2.2 the function ψ has a good one-way property, but it has a bad resistance property for a large k.

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 $|\psi\rangle$ in 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 contrast to 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, though we lost the one-way property ψ which is easily invertible.

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

Property 2.3 [4]. Let $s \geqslant 1$ and $K = |\mathbb{X}| \geqslant 4$. Let $\psi : \mathbb{X} \to (\mathcal{H}^2)^{\otimes s}$ be a δ-resistant $(K; s)$ hash function. Then

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

Properties 2.3 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 $\mathbb{X}$ of cardinality 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 approximately one-way $(\log K/K)$-resistant.

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

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

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 $\lambda(B) \leqslant \delta$. 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 prime powers. Let $H_{\delta,q} = \{h_1, \ldots, h_T\}$ be δ-good. Then for $s = \log T$ a function*

$$|\psi_{H_{\delta,q}}(w)\rangle = \frac{1}{\sqrt{T}}\sum_{j=1}^{T}\exp\left[\mathrm{i}\frac{2\pi h_j(w)}{q}\right]|j\rangle. \qquad (3.1)$$

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

Proof. For the proof see the ArXiv version [16]. □

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

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 $\psi_{H_{\delta,q}}$.

3.1. 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 the 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 summarises theorem 3.1 and the above considerations.

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*

(i) *$\psi_{H_{\delta,q}}$ is the 'balanced' quantum $(\epsilon(q), \delta(q))$-resistant quantum $(T(q); s)$-hash function.*

(ii) *The number s of qubits is good in the sense of the lower bound of property 2.3 which gives the following lower bound*

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

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

3.2. Balanced quantum hash function families

In [4] we offered a design, which allows a large amount of different balanced quantum hash functions to be built. The construction is based on the composition of a classical ε-universal hash family [17] and a given family $H_{\delta,q}$ of 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 the Reed–Solomon code.

Let q be a prime power, let $k \leqslant n \leqslant q$, let $\mathbb{F}_q$ be a finite field. A *Reed–Solomon* (RS) code is a linear code $C_{\mathrm{RS}} : (\mathbb{F}_q)^k \to (\mathbb{F}_q)^n$ defined as follows. Each word $w \in (\mathbb{F}_q)^k$, $w = w_0 w_1 \dots w_{k-1}$ is associated with the polynomial $P_w(x) = \sum_{i=0}^{k-1} w_i x^i$. Pick n distinct elements (evaluation points) $A = \{a_1, \dots, a_n\}$ of $\mathbb{F}_q$. A common special case is $n = q - 1$ with the set of evaluating points being $A = \mathbb{F}_q \setminus \{0\}$. To encode word w we evaluate $P_w(x)$ at all n elements $a \in A$ $C_{\mathrm{RS}}(w) = (P_w(a_1) \dots P_w(a_n))$.

We define family $F_{\mathrm{RS}} = \{f_a : a \in A\}$ based on the 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 $H_{\delta,q} = \{h_1, \dots, h_T\}$ be a δ-good set of functions, satisfying corollary 3.1. Composition

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

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

$$|\psi_{G_{\mathrm{RS}}}(w)\rangle = \frac{1}{\sqrt{nT}} \sum_{l=1,j=1}^{n,T} \exp\left[\mathrm{i}\frac{2\pi g_{jl}(w)}{q}\right] |lj\rangle \qquad (3.2)$$

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 $2 \leqslant k < n \leqslant q$. Then for arbitrary $\delta \in (0, 1)$ the function $\psi_{G_{\mathrm{RS}}}$ is an (ϵ, Δ)-resistant $(q^k; s)$ quantum hash function, where $\epsilon \leqslant (q \log q)/q^k$, $\Delta \leqslant \frac{k-1}{n} + \delta$, and $s \leqslant \log(q \log q) + 2\log 1/\delta + 4$.

Let $c > 1$. If we select $n = ck$, then $\Delta < 1/c + \delta$ and in accordance to property 2.3 there exist the constants $c_1(\Delta)$ and $c_2(\Delta)$ such that $\log(q \log q) - c_1(\Delta) \leqslant s \leqslant \log(q \log q) + c_2(\Delta)$. Thus, RS codes provide balanced parameters for resistance values ε and Δ and for a number s of qubits for the hash function ψ_{RS}.

4. Presenting quantum hash states via coherent states

Written in the form given in (3.1) and (3.2), the hash states $|\psi_{H_{\delta,q}}(w)\rangle \in (\mathcal{H}^2)^{\otimes s}$, $w \in \mathbb{F}_q$, and $|\psi_{\mathrm{RS}}(w)\rangle \in (\mathcal{H}^2)^{\otimes s}$, $w \in (\mathbb{F}_q)^k$, need a high degree of entanglement between the s qubits. A number of papers [7, 11, 12] consider the idea of presenting quantum fingerprinting states via coherent states and developed signature constructions based on such coherent states.

Following ideas presented in [11, 12], we map the hash state $|\psi_{H_{\delta,q}}(w)\rangle \in (\mathcal{H}^2)^{\otimes s}$ 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

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

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

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

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

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

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

5. Conclusion

The definition 2.3 of a quantum (ϵ, δ)-resistant hash function combines together the notions of quantum one-way ε-resistant and quantum collision δ-resistant functions. Examples 2.1 and 2.2 demonstrate that in the quantum setting the one-way resistance property and the 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 a balanced quantum hash function. In [4] we offered a design, which allows a large amount of different balanced quantum hash functions to be built. Note that a realisation of such quantum functions—as the balanced quantum hash function requires a high degree of entanglement between the qubits—makes such a state difficult to create with current technology.

Applying the 'phase transformation' presentation of quantum hash states [10] and using the mapping balanced quantum hash states to coherent states we can use quantum optic technology to develop quantum signature schemes based on balanced quantum hash functions.

Acknowledgments

The work is performed according to the Russian Government Program of Competitive Growth of Kazan Federal University, partially supported by Russian Foundation for Basic Research, Grants 14-07-00878, 14-07-00557, 15-37-21160.

References

[1] Gottesman D and Chuang I 2001 Quantum digital signatures *Technical Report* Cornell University Library arXiv:quantph/0105032

[2] Gavinsky D and Ito T 2010 Quantum fingerprints that keep secrets *Technical Report* Cornell University Library arXiv:1010.5342

[3] Ablayev F and Vasiliev A 2013 Cryptographic quantum hashing *Laser Phys. Lett.* **11** 025202

[4] Ablayev F and Ablayev M 2015 Quantum hashing via classical ε-universal hashing constructions *Technical Report* Cornell University Library arXiv:1404.1503v2 [quant-ph]

[5] Holevo A S 1973 Some estimates of the information transmitted by quantum communication channel (in Russian) *Probl. Pereda. Inf.* **9** 311

[6] Korol'kov A 2015 About some applied aspects of quantum cryptography in the context of development of quantum computations and emergence of quantum computations and emergence of quantum computers (in Russian) *Vopr. kiberbezopasnosty* **1** 6–13

[7] Amiri R and Andersson E 2015 Unconditionally secure quantum signature *Entropy* **17** 5635–59

[8] Ablayev F and Vasiliev A 2014 *Computing Boolean Functions via Quantum Hashing and Computing with New Resources* (*Lecture Notes in Computer Science* vol 8808) (Berlin: Springer)

[9] Vasiliev A 2015 Quantum communications based on quantum hashing *Int. J. Appl. Eng. Res.* **10** 31415–26

[10] Ablayev M 2015 On constructing quantum hash functions (in Russian) *9th Int. Conf. 'Diskretnye Modely V Teorii Upravlyauschih System' (Moscow State University)* pp 8–9

[11] Arrazola J and Lütkenhaus N 2014 Quantum fingerprinting with coherent states and a constant mean number of photons *Phys. Rev.* A **89** 062305

[12] Arrazola J and Lütkenhaus N 2014 Quantum communication with coherent states and linear optics *Phys. Rev.* A **90** 042335

[13] Nayak A 1999 Optimal lower bounds for quantum automata, random access codes *Technical Report* Cornell University Library arXiv:quant-ph/9904093v3

[14] Ambainis A and Freivalds R 1998 1-way quantum finite automata: strengths, weaknesses, generalizations *Technical Report* Cornell University Library arXiv:quant-ph/9802062v3

[15] Razborov A, Szemeredi E and Wigderson A 1993 Constructing small sets that are uniform in arithmetic progressions *Comb. Probab. Comput.* **2** 513–8

[16] Ablayev F and Ablayev M 2015 On the conception of cryptographical quantum hashing *Technical Report* Cornell University Library arXiv:1509.01268 [quant-ph]

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