ISSN 1995-0802, Lobachevskii Journal of Mathematics, 2018, Vol. 39, No. 7, pp. 1039–1045. © Pleiades Publishing, Ltd., 2018.

Attacking Quantum Hashing. Protocols and Their Cryptanalysis

M. T. Ziatdinov*

(Submitted by F. M. Ablayev)

Kazan (Volga region) Federal University, ul. Kremlevskaya 18, Kazan, Tatarstan, 420008 Russia

Received December 6, 2017

Abstract—Quantum hash functions are similar to classical (cryptographic) hash functions and their security is guaranteed by physical laws. However, security of a primitive does not automatically mean that protocols based on this primitive are secure. We propose protocols based on quantum hash function and assess their security using Holevo entropy and recently introduced notion of quantum information cost.

DOI: 10.1134/S1995080218070211

Keywords and phrases: *Quantum hash functions, Holevo entropy, quantum information cost.*

1. INTRODUCTION

Quantum hash functions are similar to classical (cryptographic) hash functions and their security is guaranteed by physical laws. However, security of a primitive does not automatically mean that protocols that use this primitive are secure. We propose two protocols based on quantum hash functions and assess their security. We use Holevo entropy and recently introduced notion of quantum information complexity.

Quantum hash functions used in this paper are good candidates for experimental implementation. They use a small number of qubits and have an easy verifying procedure. The problem is that such quantum hash functions require maximum entanglement.

Quantum hash functions were first implicitly introduced in [1] as quantum fingerprinting. Then Gavirsky and Ito [2] noticed that quantum fingerprinting can be used as cryptoprimitive.

[3] gave a definition and construction of non-binary quantum hash functions. Ziatdinov [4] showed how to generalize quantum hashing to arbitrary finite groups. Recently, Vasiliev [5] showed how quantum hash functions are connected with ϵ-biased sets. Ziatdinov [6] introduced keyed quantum hash functions (QMAC).

Quantum hash functions map a classical message into a Hilbert space. Such space should be as small as possible, so eavesdropper can't read a lot of information about the classical message (this is guaranteed by physical laws as Holevo–Nayak's theorem states). But images of different messages should be as far apart as possible, so the recipient can check that hash differ or not with high probability. We measure this distance using an absolute value of scalar product of hashes of different messages. More detailed introduction to quantum hash functions can be found in Ablayev et al. [7].

The rest of this article is organized as follows. Next section contains necessary definitions. Section 3 contains definitions of analyzed protocols. Section 4 contains analysis of security of protocols based on quantum information cost. Section 5 is devoted to computing Holevo entropy of quantum hash.

*E-mail: gltronred@gmail.com

2. DEFINITIONS

2.1. Groups

We use standard notions from the group theory.

Definition 1 (Group). *Group $(G, +_G, 0_G, -\cdot)$ is a set of elements G equipped with binary operation $+ : G \times G \to G$ called group operation, unary operation $-\cdot : G \to G$ and fixed element 0 called identity. For any element $g \in G$: $\forall g : \ g +_G 0_G = 0_G +_G g = g$.*

For any element $g \in G$ there exists its inverse: $\forall g : \ g +_G (-g) = (-g) +_G g = 0_G$. We sometimes omit subscript G when it is clear from the context. If group operation is commutative then group is abelian:

$$\forall a, b \in G : a + b = b + a \quad \iff \quad G \text{ is abelian.}$$

Definition 2 (General linear group). *Let V be a vector space over the field $\mathbb{F}$. General linear group $\mathrm{GL}(V, \mathbb{F})$ is the group of all automorphisms of V with composition as group operation.*

Definition 3 (Group representation). *Group representation ϕ on vector space V is a group homomorphism $\phi : G \to \mathrm{GL}(V, \mathbb{F})$.*

Definition 4 (Multiplicative character). *Multiplicative character χ of a group G is a homomorphism from G to $\mathbb{C}$. There are $|G|$ different multiplicative characters of a group G and they are in bijection with elements of G. Trivial character χ_0 is* $\chi_0(g) = \begin{cases} 1, & g = 0_G, \\ 0, & g \neq 0_G. \end{cases}$

2.2. Quantum Model of Computation

We use the following model of computation.

Recall that a qubit $|\Psi\rangle$ is a superposition of basis states $|0\rangle$ and $|1\rangle$, i.e., $|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle$, where $\alpha, \beta \in \mathbb{C}$ and $|\alpha|^2 + |\beta|^2 = 1$. So, qubit $|\Psi\rangle \in \mathcal{H}^2$, where $\mathcal{H}^2$ is a two-dimensional Hilbert complex space.

Let $s \geq 1$. We denote 2^s-dimensional Hilbert complex space by $(\mathcal{H}^2)^{\otimes s}$: $(\mathcal{H}^2)^{\otimes s} = \mathcal{H}^2 \otimes \mathcal{H}^2 \otimes \ldots \otimes \mathcal{H}^2 = \mathcal{H}^{2^s}$. We denote a state $|a_1\rangle|a_2\rangle \ldots |a_n\rangle$, each $a_i \in \{0, 1\}$, by $|i\rangle$, where i is $\overline{a_1 a_2 \ldots a_n}$ in binary. For example, we denote $|1\rangle|1\rangle|0\rangle$ by $|6\rangle$. Usually it is clear, which space this state belongs to. Computation is done by multiplying a state by a unitary matrix: $|\Psi_1\rangle = U|\Psi_0\rangle$, where U is a unitary matrix: $U^\dagger U = I$, $U^\dagger$ is the conjugate matrix and I is the identity matrix.

The density matrix of a mixed state $\{p_i, |\psi_i\rangle\}$ is a matrix $\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|$. A density matrix belongs to $\mathrm{Hom}((\mathcal{H}^2)^{\otimes s}, (\mathcal{H}^2)^{\otimes s})$, the set of linear transformations from $(\mathcal{H}^2)^{\otimes s}$ to $(\mathcal{H}^2)^{\otimes s}$.

At the end of computation state is measured by POVM (Positive Operator Valued Measure). A POVM on a $(\mathcal{H}^2)^{\otimes s}$ is a collection $\{E_i\}$ of positive semi-definite operators $E_i : \mathrm{Hom}((\mathcal{H}^2)^{\otimes m}, (\mathcal{H}^2)^{\otimes m}) \to \mathrm{Hom}((\mathcal{H}^2)^{\otimes m}, (\mathcal{H}^2)^{\otimes m})$ that sums up to the identity transformation, i.e., $E_i \succeq 0$ and $\sum_i E_i = I$. Applying a POVM $\{E_i\}$ on a density matrix ρ results in answer i with probability $\mathrm{Tr}(E_i \rho)$.

2.3. Information Complexity

Definition 5 (Trace distance, [8]). *For two states ρ_1, ρ_2 trace distance is defined as $||\rho_1 - \rho_2||_A = \mathrm{Tr}(|\rho_1 - \rho_2|)$.*

Definition 6 (Shannon entropy). *For any random variable X with discrete probability distribution $\{p_i\}$ Shannon entropy is defined as $H(X) = \sum_i p_i \log p_i$. We denote by $H(p)$ entropy of random variable with probability distribution $p_i = p$.*

Definition 7 (Von Neumann entropy, [8]). *For any state ρ von Neumann entropy is defined as $S(A)_\rho = \mathrm{Tr}(\rho \log \rho)$. By convention we take that $0 \log 0 = 0$. For a state ρ^{AB} conditional entropy is defined as $S(A|B)_{\rho^{AB}} = S(AB)_{\rho^{AB}} - S(B)_{\rho^B}$.*

Definition 8 (Mutual information, [8]). *For a states ρ^{AB} and ρ^{ABC} mutual information is defined as $I(A;B)_{\rho^{AB}} = S(A)_{\rho^A} - S(A|B)_{\rho^{AB}}$, and conditional mutual information as $I(A;B|C)_{\rho^{ABC}} = S(A|C)_{\rho^{AC}} - S(A|BC)_{\rho^{ABC}}$.*

Definition 9 (Protocol, [8]). *A protocol Π for implementing N on input $\rho^{A_{in}B_{in}}$ is defined by a sequence of unitaries $U_1, \ldots, U_{M+1}$ along with a pure state ψ shared between Alice and Bob, for arbitrary finite dimensional registers T_A, T_B. For appropriate finite dimensional memory registers $A_1, A_3, \ldots, A_{M-1}, A'$ held by Alice, $B_2, B_4, \ldots, B_{M-2}, B'$ held by Bob, and communication registers $C_1, C_2, C_3, \ldots .C_M$ exchanged by Alice and Bob, we have $U_1 \in \mathcal{U}(A_{in} \otimes T_A, A_1 \otimes C_1), U_2 \in \mathcal{U}(B_{in} \otimes T_B \otimes C_1, B_2 \otimes C_2), U_3 \in U(A_1 \otimes C_2, A_3 \otimes C_3), U_4 \in \mathcal{U}(B_2 \otimes C_3,\ B_4 \otimes C_4), \ldots, U_M \in \mathcal{U}(B_{M-2} \otimes C_{M-1}, B_{out} \otimes B \otimes C_M), U_{M+1} \in \mathcal{U}(A_{M-1} \otimes C_M, A_{out} \otimes A')$. We also write Π to denote the channel implemented by the protocol, i.e.,*

$$\Pi(\rho) = \mathrm{Tr}_{A'B'}(U_{M+1}U_M \cdots U_2U_1(\rho \otimes \psi)).$$

Then we say that a protocol Π for implementing channel $\mathcal{N}$ on input $\rho^{A_{in}B_{in}}$, with purification $\rho^{A_{in}B_{in}R}$ for a reference system R, has error $\epsilon \in [0, 2]$ if $||\Pi(\rho) - \mathcal{N}(\rho)||_{A_{out}B_{out}} \leq \epsilon$.

Definition 10 (Quantum information cost, [8]). *For a protocol Π and an input state ρ, the quantum information cost of Π on input ρ is*

$$\mathrm{QIC}(\Pi, \rho) = \sum_{i>0,\mathrm{odd}} \frac{1}{2} I(C_i; R|B_{i-1}) + \sum_{i>0,\mathrm{even}} \frac{1}{2} I(C_i; R|A_{i-1}),$$

in which we have labelled $B_0 = B_{in} \times T_B$.

2.4. Quantum Hash Functions

Informally, quantum hash function is a function that maps *large* classical input to a *small* quantum (hash) state such that two requirements are satisfied: (1) it is hard to restore input given the hash state and (2) it is easy to check with high probability that inputs for two quantum hash states are equal or different.

It is easy to meet the first requirement for a constant hash size. One can simply take a qubit $|\Psi(w)\rangle = \alpha(w)|0\rangle + \beta|1\rangle$ and encode the input in a fractional part of α. But then the second requirement is not satisfied.

It is easy to meet the second requirement for a hash size that is logarithmic in input size. One can simply map the input to the corresponding base state: $|\Psi(i)\rangle = |i\rangle$. However, then the first requirement is not satisfied.

Let us give the formal

Definition 11 (Quantum hash function [7]). *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 $\boldsymbol{M}$ making measurement to the encoding ψ of X and decoding the result of the measurement to $\mathbb{X}$. Let $\delta > 0$ and $\epsilon > 0$. Quantum function ψ is a (δ, ϵ)-quantum hash function, iff*

- *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,*
- *for any mechanism $\boldsymbol{M}$, the probability $Pr[Y = X]$* that $\mathbf{M}$ *successfully decodes Y is bounded by δ: $Pr[Y = X] \leq \delta$,*
- *for any pair w, w' of different inputs, $|\langle\psi(w)|\psi(w')\rangle| \leq \epsilon$.*

Quantum hash function maps inputs of length $K = \log \mathbb{X}$ to (quantum) outputs of length s. If $K \gg s$ any attacker can't get a lot of information by Holevo–Nayak theorem [9]. The equality of two hashes can be checked using, for example, well-known SWAP-test [10] or REVERSE-test [7]. All hash functions we use also require additional structure, namely, they map elements of some group G to quantum state.

For example, the group G can be thought of as $\{0, 1\}_{2^n}$ with group operation $+$, then elements of G can be encoded as binary strings $\{0, 1\}^n$ of length n.

3. PROTOCOLS

One application of classical cryptographic hash functions is modification detection codes. Alice sends message to Bob using authenticated channel and sends him hash of this message. If hash computed by Bob is equal to sent hash, he says that message was not modified.

We use similar protocol, but Alice sends quantum hash of classical message:

- Alice and Bob have group elements g_1 and g_2 correspondingly. They do not know each other's input.
- Alice computes $h = |\Psi(g_1)\rangle$ and sends to Bob.
- Bob compares h and $|\Psi(g_2)\rangle$ using some mechanism M and accepts if M answers that h and $|\Psi(g_2)\rangle$ is equal.

Eavesdropper Eve wants to interfere with this protocol and either learn something about g_1 or change h to some h' such that Bob will accept it.

We use the following hash functions.

Theorem 1 (Ziatdinov [4]). *Let the function $\Psi_{\mathrm{GR}} : G \to (\mathcal{H}^2)^{\otimes \log t+d}$ be defined as*

$$|\Psi_{\mathrm{GR}}(g)\rangle = \frac{1}{\sqrt{t}} \sum_{i=1}^{t} |i\rangle \otimes \phi(k_i(g))|0\rangle,$$

where g is an element of a group G, $\phi : G \to \mathrm{Hom}((\mathcal{H}^2)^{\otimes d}, (\mathcal{H}^2)^{\otimes d})$ is a linear representation of G on $(\mathcal{H}^2)^{\otimes d}$ and $K = \{k_i\}, i = 1, \ldots, t$ is a random set of automorphisms of G with property

$$\forall g \in G, g \neq e : \frac{1}{|K|} \left| \sum_{k \in K} \langle 0|\phi(k(g))|0\rangle \right| < \epsilon. \tag{1}$$

Then $|\Psi_{\mathrm{GR}}(g)\rangle$ is a $(\frac{\log t+d}{|G|}, \epsilon)$-quantum hash function w.h.p. Chen et al. [11] gives an explicit construction of such representations.

If we change representations of a group to multiplicative characters (i.e., one-dimensional representations), we get the following hash function.

Theorem 2. (Vasiliev [5]). *Let the function $\Psi_{\mathrm{EBS}} : G \to (\mathcal{H}^2)^{\otimes \log t}$ be defined as*

$$|\Psi_{\mathrm{EBS}}(g)\rangle = \frac{1}{\sqrt{t}} \sum_{i=1}^{t} \chi_{S_i}(g)|i\rangle,$$

where $g \in G$ is an element of a group G, χ_h is a multiplicative character of a group G corresponding to an $h \in G$, $S \subset G$ is an ϵ-biased subset of G. Then $|\Psi_{\mathrm{EBS}}(g)\rangle$ is a $(\log t/|G|, \epsilon)$-quantum hash function.

Alon and Roichman [12] proved that a set of $O(\log |G|/\epsilon^2)$ elements selected uniformly at random is ϵ-biased w.h.p. Chen et al. [11] gives explicit construction of such sets.

These two quantum hash functions have many similarities. Therefore, we sometimes denote both of them as $|\Psi_{\mathrm{Hash}}(g)\rangle$. We denote protocol based on quantum hash function $|\Psi_{\mathrm{EBS}}(g)\rangle$ as Π_{EBS} and protocol based on $|\Psi_{\mathrm{GR}}(g)\rangle$ as Π_{GR}.

3.1. Classical Attacks on Protocols

Classical attacks on modification detection codes are collision attack and preimage attack. To perform the collision attack Eve finds two different words w, w' such that $h(w) = h(w')$. In quantum setting Eve looks for $w \neq w'$ such that verifying procedure considers their hashes equal with high probability. Ablayev et al. [7] show that resistance to this attack is equivalent to the following condition: $\langle \Psi(w)|\Psi(w')\rangle < \epsilon$ for every pair of different words.

To perform the preimage attack Eve finds w such that $h(w)$ is equal to given h_0. To perform this attack against quantum hash Eve has to find w such that verifying procedure considers $\Psi(w)$ equal to Ψ_0. Ablayev et al. [7] use Holevo–Nayak theorem to bound this probability.

The second preimage attack, where Eve has to find $w \neq w_0$ such that $h(w)$ is equal to hash $h(w_0)$ of given word w_0, is the same as preimage attack in the quantum setting, because quantum hash functions are injective.

4. QUANTUM INFORMATION COST OF QUANTUM HASH

Quantum information cost is what the two parties learn about each other's inputs from the execution of the protocol. Therefore, it also measures the amount of information that attacker can obtain from quantum hash. In our case there is only one message transmitted between Alice and Bob, so definition of quantum information cost is simplified to the following:

$$\begin{aligned}\mathrm{QIC}(\Pi_{Hash}, \rho_{AB}) &= \frac{1}{2} I(C; R|B) = \frac{1}{2}(S(C|B) - S(C|RB)) \\ &= \frac{1}{2}(S(CB) + S(RB) - S(B) - S(RCB)),\end{aligned}$$

where C is a message register, B is Bob's input and R is a purifying register, and Π_{Hash} is the protocol described in Section 3.

Theorem 3. *Let $\delta > 0$ and $\epsilon > 0$. Let Ψ_{EBS} be a (δ, ϵ)-quantum hash function defined as*

$$|\Psi_{\mathrm{EBS}}(g)\rangle = \frac{1}{\sqrt{t}} \sum_{i=1}^{t} \chi_{S_i}(g)|i\rangle,$$

where $g \in G$ is an element of a group G, χ_h is a multiplicative character of a group G corresponding to an $h \in G$, $S \subset G$ is an ϵ-biased subset of G. Let Ψ_{GR} be defined as

$$|\Psi_{\mathrm{GR}}(g)\rangle = \frac{1}{\sqrt{t}} \sum_{i=1}^{t} |i\rangle \otimes \phi(k_i(g))|0\rangle,$$

where g is an element of a group G, $\phi : G \to \mathrm{Hom}((\mathcal{H}^2)^{\otimes d}, (\mathcal{H}^2)^{\otimes d})$ is a linear representation of G on $(\mathcal{H}^2)^{\otimes d}$ and $K = \{k_i\}, i = 1, \ldots, t$ is a set of automorphisms of G such that Ψ_{GR} is a (δ, ϵ)-quantum hash function. Then

$$\mathrm{QIC}(\Pi_{EBS}, \rho_{AB}) \leq (\log t - 1) \log |G|, \quad \mathrm{QIC}(\Pi_{GR}, \rho_{AB}) \leq (\log t + \log d - 1) \log |G|.$$

Proof. (Sketch) Input state in our case is mixed state $\rho_{AB} = \frac{1}{|G|^2} \sum_{g_1 \in G} \sum_{g_2 \in G} |g_1^A\rangle\langle g_1^A| \otimes |g_2^B\rangle\langle g_2^B|$. Here we define $|g\rangle$ as quantum state which encodes classical input $g \in G$. Therefore, by [13, § 2.5], state of purifying register and input register is

$$|RAB\rangle = \frac{1}{|G|} \sum_{g_1, g_2 \in G} |g_1^{RA}\rangle |g_2^{RB}\rangle |g_1^A\rangle |g_2^B\rangle,$$

$$\rho_{RAB} = \frac{1}{|G|^2} \sum_{g_1, g_2, g_3, g_4 \in G} |g_1^{RA}\rangle\langle g_3^{RA}| \otimes |g_2^{RB}\rangle\langle g_4^{RB}| \otimes |g_1^A\rangle\langle g_3^A| \otimes |g_2^B\rangle\langle g_4^B|,$$

where $|g^A\rangle, |g^B\rangle, |g^{RA}\rangle|g^{RB}\rangle$ are basis states of system A, system B and system R, correspondingly. The state of the whole system RACB is

$$\rho_{RABC} = \frac{1}{|G|^2} \sum_{g_1,g_2,g_3,g_4 \in G} |g_1^{RA}\rangle\langle g_3^{RA}| \otimes |g_2^{RB}\rangle\langle g_4^{RB}| \otimes |g_1^{A}\rangle\langle g_3^{A}| \otimes |g_2^{B}\rangle\langle g_4^{B}| \otimes |\Psi_{\text{Hash}}(g_1)\rangle\langle\Psi_{\text{Hash}}(g_3)|,$$

where $|\Psi_{\text{Hash}}(g)\rangle$ is an image of a quantum hash function. It can be proved that for any of our quantum hash functions

$$\frac{1}{|G|}\sum_{g\in G} \text{Tr}(|\Psi_{Hash}\rangle(g)\langle\Psi_{Hash}(g)|) = 1$$

and quantum information cost reduces to

$$I(C;R|B) = \left(S\left(\frac{1}{|G|}\sum_{g\in G} |\Psi_{\text{Hash}}(g)\rangle\langle\Psi_{\text{Hash}}(g)|\right) - 1\right)\log|G|. \tag{2}$$

We prove that

$$S\left(\frac{1}{|G|}\sum_{g\in G} |\Psi_{EBS}(g)\rangle\langle\Psi_{EBS}(g)|\right) \le \log t. \tag{3}$$

We also prove that if ϕ is irreducible representation and its dimension is d, then

$$S\left(\frac{1}{|G|}\sum_{g\in G} |\Psi_{GR}(g)\rangle\langle\Psi_{GR}(g)|\right) \le \log t + \log d. \tag{4}$$

Substituting (3) and (4) into (2), we complete the proof. □

5. HOLEVO ENTROPY OF QUANTUM HASH

Gavinsky and Ito [2] proved that accessible information in $|\Psi_{\text{ECC}}\rangle$ is constant. However, they used Shannon entropy of measurement result. Using the same technique, Vasiliev et al. [14] proved that accessible information for $|\Psi_{\text{EBS}}\rangle$ is constant.

We prove similar result but use von Neumann entropy, i.e., we compute Holevo entropy $\Xi(\rho) = S(\rho) - \sum_x p_x\rho_x$. This result is more natural in the following sense. Suppose that Alice prepares quantum state $\rho = \sum_x p_x\rho_x$ that depends on classical (random) variable x, i.e., she prepares one of states ρ_x with probability p_x. Eve measure state ρ and get result y. She tries to decode this result into x. The probability of incorrect decoding p_e is bounded by Holevo inequality

$$H(p_e) + p_e(\log|X| - 1) \ge H(X|Y) \ge H(X) - \Xi(\rho).$$

So, if $\Xi(\rho)$ is small, then it is hard for Eve to decode the state.

Theorem 4. *Holevo entropy of quantum hash function* $|\Psi_{EBS}(g)\rangle$ is $\Xi(\rho^{EBS}) = \frac{t-1}{t}\log t$.

Proof. Let us compute $\Xi(\rho^{EBS})$:

$$\rho_g = \frac{1}{t^2}\sum_{i=1}^{t}\sum_{j=1}^{t}\chi_g(k_i)\chi_g^*(k_j)|i\rangle\langle j|,$$

$$\rho = \frac{1}{|G|}\sum_{g\in G}\rho_g = \frac{1}{|G|t^2}\sum_{g\in G}\sum_{i=1}^{t}\sum_{j=1}^{t}\chi_g(k_i)\chi_g^*(k_j)|i\rangle\langle j| = \frac{1}{t^2}\sum_{i=1}^{t}\sum_{j=1}^{t}\left(\frac{1}{|G|}\sum_{g\in G}\chi_g(k_i-k_j)\right)|i\rangle\langle j|.$$

For $i \ne j$, $k_i - k_j \ne 0_G$. It is known [15, Theorem 5.4] that for any nontrivial multiplicative character χ $\sum_{g\in G}\chi(g) = 0$, and, by definition, $\chi_g(0_G) = 1$. Therefore, $\rho = I/t$, and $S(\rho) = \text{Tr}(\rho\log\rho) = \sum_i \lambda_i\log\lambda_i = \log t$.

Let us compute eigenvalues of ρ_g. Define vector $a = 1/t(\chi_g(k_1)\chi_g(k_2)\dots\chi_g(k_t))$. Then $\rho_g = aa^T$. It is easy to see that matrix aa^T has eigenvalues $(||a||^2 00\dots0)$. Firstly, let u be

$$(aa^T)u = \lambda u, \quad a(a^T u) = \lambda u, \quad (a^T u)a = \lambda u.$$

Therefore, a is an eigenvector of aa^T with eigenvalue $||a||^2$. Secondly, let v be any vector orthogonal to a^T: $(aa^T)v = \lambda v, \quad a(a^T v) = \lambda v$. So, v is an eigenvector of aa^T with eigenvalue 0. There are $t-1$ linear independent vectors, orthogonal to a^T. So we have found all eigenvalues of $aa^T = \rho_g$.

Let us compute $||a||^2$: $||a||^2 = \frac{1}{t^2}\sum_{i=1}^{t}\chi_g(k_i)\chi_g^*(k_i) = \frac{1}{t^2}\sum_{i=1}^{t}\chi_g(e) = \frac{1}{t}$. Therefore, $S(\rho_g) = (1/t)\log t$. Finally, we get

$$\Xi(\rho) = S(\rho) - \frac{1}{|G|}\sum_{g\in G} S(\rho_g) = \log t - \frac{1}{t}\log t = \frac{t-1}{t}\log t.$$

□

6. SUMMARY

We proposed two protocols based on quantum hash, one based on quantum hash function $|\Psi_{GR}(g)\rangle$ based on groups, and one based on $|\Psi_{EBS}(g)\rangle$ based on ϵ-biased sets. We computed quantum information cost for these protocols:

$$\mathrm{QIC}(\Pi_{EBS}, \rho_{AB}) = (\log t - 1)\log|G|, \quad \mathrm{QIC}(\Pi_{GR}, \rho_{AB}) = (\log t + \log d - 1)\log|G|.$$

Also we were able to compute Holevo entropy for protocol based on $|\Psi_{EBS}(g)\rangle$:

$$\Xi(\rho^{EBS}) = \frac{t-1}{t}\log t.$$

Holevo entropy gives us better bounds than Holevo–Nayak theorem which was used in earlier works.

ACKNOWLEDGMENTS

The work is performed according to the Russian Government Program of Competitive Growth of Kazan Federal University. The reported study was funded by RFBR according to the research project 17-07-01606.

REFERENCES

1. H. Buhrman, R. Cleve, J. Watrous, and R. de Wolf, "Quantum fingerprinting," Phys. Rev. Lett. **87**, 167902 (2001).
2. D. Gavinsky and T. Ito, "Quantum fingerprints that keep secrets," arXiv:1010.5342 (2010), pp. 1–28.
3. F. Ablayev and A. Vasiliev, "Cryptographic quantum hashing," Laser Phys. Lett. **11**, 025202 (2014).
4. M. Ziatdinov, "Quantum hashing. Group approach," Lobachevskii J. Math. **37**, 222–226 (2016).
5. A. Vasiliev, "Quantum hashing for finite Abelian groups," Lobachevskii J. Math. **37**, 751–754 (2016).
6. M. Ziatdinov, "From graphs to keyed quantum hash functions," Lobachevskii J. Math. **37**, 705–712 (2016).
7. F. Ablayev, M. Ablayev, A. Vasiliev, and M. Ziatdinov, "Quantum fingerprinting and quantum hashing. Computational and cryptographical aspects," Baltic J. Mod. Comput. **4**, 860–875 (2016).
8. D. Touchette, "Quantum information complexity," in *Proceedings of the 47th Annual ACM Symposium on Theory of Computing, STOC'15* (2015), pp. 317–326.
9. A. V. Nayak, *Lower Bounds for Quantum Computation and Communication* (Univ. California, Berkeley, CA, 1999).
10. D. Gottesman and I. L. Chuang, "Quantum digital signatures," arXiv:quant-ph/0105032 (2001), pp. 1–8.
11. S. Chen, C. Moore, and A. Russell, "Small-bias sets for nonabelian groups,", Lect. Notes Comput. Sci. **8096**, 436–451 (2013).
12. N. Alon and Y. Roichman, "Random Cayley graphs and expanders," Random Struct. Algorithms **5**, 271–284 (1994).
13. M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge Univ. Press, Cambridge, 2004).
14. A. Vasiliev, A. Vasilov, and M. Latypov, "Analysis of properties of quantum hashing," Itogi Nauki Tekh., Ser.: Sovrem. Mat. Prilozh. **138**, 11–18 (2017).
15. R. Lidl and H. Niederreiter, *Finite Fields* (Cambridge Univ. Press, Cambridge, 1997).