Quantum hashing and Fourier transform

Farid Ablayev¹,² and Alexander Vasiliev¹,²
¹ Kazan Federal University, 35 Kremlyovskaya street, Kazan 420008, Russian Federation
² Kazan E.K. Zavoisky Physical-Technical Institute of the Kazan Scientific Center of the Russian Academy of Sciences, 10/7 Sibirsky trakt, Kazan 420029, Russian Federation
E-mail: vav.kpfu@gmail.com

Abstract. In the paper based on the notion of small-biased sets we define the quantum transformation that describes the quantum hash function over the cyclic group. We discuss its similarity to the well-known Quantum Fourier Transform and show possible applications to constructing space-efficient algorithms in various computational scenarios, including two-party quantum communication model, simultaneous message passing model, and the model of quantum online streaming algorithms.

1. Introduction
In [1] we have proposed a cryptographic quantum hash function and later in [2] provided its generalized version for arbitrary finite abelian groups based on the notion of small-biased sets. In their seminal paper [3] Naor and Naor 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 small-biased sets are generally defined for arbitrary finite groups [4], but in this paper we focus on the case of cyclic group modulo q. We define a quantum transformation that is based on small-biased sets and lead to the quantum hash function over the cyclic group.

This transformation that can be considered as a variation of the well-known Quantum Fourier Transform (QFT), since in a special case it acts exactly like QFT (however, unlike the conventional definition of QFT we consider the case of classical input).

We show that this transformation can be used to construct space-efficient algorithms in various computational scenarios and models including quantum communication setting, simultaneous message passing model, and the model of quantum online streaming algorithms.

2. Preliminaries
We start with recalling the definition of a quantum hash function and its properties.

We define a classical-quantum (or just quantum) function ψ over the finite set X to be a function

\[ \psi : X \rightarrow (\mathbb{C}^2)^{\otimes s}. \]  (1)

In other words a quantum function ψ encodes an input \( w \in X \) into an s-qubit quantum state \( |\psi(w)\rangle \). In order to construct cryptographic applications of such a function we formulate additional requirements that it will have to satisfy. These requirements include resistance to...
inversion (known as “one-way property” or “preimage resistance”, i.e. possibility of “extraction” of encoded information out of the quantum state) and resistance to quantum collisions (which corresponds to the situation of high similarity of quantum images for different inputs). Below we describe them in more details.

One-way property. We present the following definition of a quantum $\delta$-one-way function. Let $M$ be a function $M: (H^2)^{\otimes s} \to X$. Informally speaking $M$ is an “information extracting” mechanism that makes some measurement of the state $|\psi\rangle \in (H^2)^{\otimes s}$ and decodes the result into $X$.

**Definition 1** Let $X$ be a random variable distributed over $X \{ \Pr[X = w] : w \in X \}$. Let $\psi: X \to (H^2)^{\otimes s}$ be a quantum function. Let $Y$ be a random variable over $X$ obtained by some $M$ that makes the measurement to the encoding $\psi$ of $X$ and decodes the result into $X$. Let $\delta > 0$. We call a quantum function $\psi$ a $\delta$-one-way function if for any $M$, the probability $\Pr[Y = X]$ that $M$ successfully decodes $Y$ is bounded by $\delta$.

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

(2)

For the cryptographic purposes it is natural to assume (and we do this in the rest of the paper) that the 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, the fundamental result of quantum information known as the Holevo Theorem [5] states that a quantum measurement can only give $O(s)$ bits of information about such state. We will use here the following version [6] of the Holevo Theorem.

**Property 1** Let $X$ be a random variable uniformly distributed over the finite set $X$. Let $\psi: X \to (H^2)^{\otimes s}$ be a quantum function. Let $Y$ be a random variable over $X$ obtained by some $M$ that makes some measurement of the encoding $\psi$ of $X$ and decodes the result into $X$. Then the probability of correctly decoding $Y$ is given by

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

(3)

Collision resistance. The following definition describes the property of collision resistance for a quantum function.

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

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

(4)

Note that the above inequality means near-orthogonality of quantum states $|\psi(w)\rangle$ and $|\psi(w')\rangle$. It is well-known that orthogonality of quantum states provides their distinguishability. In the context of quantum functions near-orthogonality means high collision resistance. That is, let us denote by $Pr_T[v = w]$ a probability that some test $T$ given quantum states $|\psi(v)\rangle$ and $|\psi(w)\rangle$ outputs the result “$v = w$”. For example, the well-known SWAP-test [7] gives this result with probability

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

(5)

The REVERSE-test [1], [8] gives

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

(6)
There is a known lower bound by Buhrman et al. [7] for the size of the sets of pairwise-distinguishable states: to construct a set of $|X|$ quantum states with pairwise inner products below $\varepsilon$ we will need at least $\Omega(\log(\log |X|/\varepsilon))$ qubits. This implies that a $\varepsilon$-collision-resistant quantum function requires at least $s = \Omega(\log \log X - \log \varepsilon)$ qubits. The similar lower bound of $\log \log K - \varepsilon$ was proved by a different method in [9].

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

**Definition 3** Let $s \geq 1$, $\delta \in (0, 1]$ and $\varepsilon \in [0, 1)$. We call a function $\psi : X \rightarrow (H^2)^{\otimes s}$ a quantum $(\delta, \varepsilon)$-hash function if $\psi$ is $\delta$-one-way and $\varepsilon$-collision-resistant function.

The trade-off between one-way property and collision resistance We have shown earlier [10] that one-way property and collision resistance lead to the contradictory requirements on the size of the quantum hash and the “more” a quantum function is one-way the “less” it is collision resistant and vice versa.

**Example 1** We encode a word $w \in \{0, 1\}^k$ into one qubit:

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

This function has good one-way property with $\delta = \frac{2}{2^k}$, but also has poor collision resistance of $\varepsilon = \cos\left(\frac{\pi}{2^k}\right)$.

**Example 2** We encode a word $w \in \{0, 1\}^k$ into $k$ qubits:

$$|\psi(w)\rangle = |w\rangle.$$  

This function has $\delta = 1$ (no preimage resistance) and collision resistance with $\varepsilon = 0$ (perfect resistance).

We have also provided an explicit construction of a family of “balanced” quantum hash functions that use the least possible number of qubits (that asymptotically match the aforementioned lower bound) to stay collision resistant, but also show very good one-way property [2]. This approach is given via so-called small-biased sets.

**Quantum hash function construction via small-biased sets.** In [11] we have given a general construction of a quantum hash function for arbitrary finite abelian group but here we restrict ourselves to $\mathbb{Z}_q$. In this case a set $S \subseteq \mathbb{Z}_q$ is called $\varepsilon$-biased, if for any $a \neq 0$

$$\frac{1}{|S|} \left| \sum_{x \in S} e^{2\pi ax/q} \right| \leq \varepsilon. \quad (7)$$

These sets are especially interesting when $|S| \ll |\mathbb{Z}_q|$ (as $S = \mathbb{Z}_q$ is obviously 0-biased), and it is known [12] that there exist $\varepsilon$-biased sets of size $O(\log q/\varepsilon^2)$.

We present the result of [11] in the following form.

**Property 2** Let $S = \{a_0, a_1, \ldots, a_{d-1}\} \subseteq \mathbb{Z}_q$ be an $\varepsilon$-biased set. Then $\psi_S : \mathbb{Z}_q \rightarrow (H^2)^{\otimes \log |S|}$

$$|\psi_S(x)\rangle = \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} e^{2\pi a_j x/q} |a\rangle$$  

is a quantum $(\delta, \varepsilon)$-hash function, where $\delta \leq |S|/q$. 


3. Quantum hashing and Fourier transform

Here we define a quantum transformation that is based on small-biased sets. Let \( S = \{a_0, a_1, \ldots, a_{d-1}\} \subset \mathbb{Z}_q \). For an \( x \in \mathbb{Z}_q \) we denote by \( \text{QFT}_S(x) \) the following transformation of a \( d \)-dimensional quantum state \( |y\rangle \):

\[
\text{QFT}_S(x)|y\rangle = \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} (-1)^{y \cdot j} e^{2\pi a_j x/q} |j\rangle,
\]

(9)

where \( (y \cdot j) \) is a bitwise inner product modulo 2 of binary decomposition of \( y \) and \( j \).

However, below we will restrict ourselves to the basic case of \( y = 0 \):

\[
\text{QFT}_S(x)|0\rangle = \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} e^{2\pi a_j x/q} |j\rangle.
\]

(10)

The formula above gives the transformation that can be considered as a variation of the well-known Quantum Fourier Transform (QFT). Indeed, in case of the 0-biased set \( S = \mathbb{Z}_q \) this is exactly QFT. Note however, that conventional definition of QFT implies that input is quantum (see, e.g. [13]), but here we consider this transformation to be classically-controlled, i.e. input is classical.

In terms of quantum hashing from [10] \( \text{QFT}_{\mathbb{Z}_q} \) corresponds to the unbalanced (0,1)-resistant quantum hash function (the one, that is perfectly collision resistant, but doesn’t hide any information).

In case of the small-sized and small-biased set \( S \subset \mathbb{Z}_q \) we obtain the transformation that defines a balanced quantum hash function \( \psi_S \), given by (8):

\[
|\psi_S(x)\rangle = \text{QFT}_S(x)|0\rangle.
\]

(11)

4. Computing Boolean functions via \( \text{QFT}_S \)

In this section we exploit the definition of the characteristic polynomial for a Boolean function proposed in [14].

**Definition 4** We call a polynomial \( g(x_1, \ldots, x_n) \) over the ring \( \mathbb{Z}_q \) a characteristic polynomial of a Boolean function \( f(x_1, \ldots, x_n) \) and denote it \( g_f \) when for all \( \sigma \in \{0,1\}^n \) \( g_f(\sigma) = 0 \) iff \( f(\sigma) = 1 \).

Note, that such a polynomial always exists.

**Lemma 1 ([14])** For any Boolean function \( f \) of \( n \) variables there exists a characteristic polynomial \( g_f \) over \( \mathbb{Z}_{2^n} \).

Generally, there are many polynomials for the same function. For example, the function \( EQ_n \), which tests the equality of two \( n \)-bit binary strings, has the following polynomial over \( \mathbb{Z}_{2^n} \):

\[
\sum_{i=1}^{n} (x_i(1 - y_i) + (1 - x_i)y_i) = \sum_{i=1}^{n} (x_i + y_i - 2x_i y_i).
\]

(12)

On the other hand, the same function can be represented by the polynomial

\[
\sum_{i=1}^{n} x_i 2^{i-1} - \sum_{i=1}^{n} y_i 2^{i-1}.
\]

(13)

Let \( \sigma = \sigma_1 \ldots \sigma_n \) be an input string and \( g_f \) be a characteristic polynomial of a Boolean function \( f \) we are about to compute.

To compute the function \( f \) via \( \text{QFT}_S \) we perform the following steps:
• Initialize the quantum register in the $d$-dimensional ($d = |S|$) state $|0\rangle$.
• Based on the input $\sigma$ we hash its value into the state:

$$|\psi_S(g_f(\sigma))\rangle = \text{QFT}_S(g_f(\sigma))|0\rangle.$$  \hfill (14)

Such a presentation can be used in various computational scenarios depending on the problem we need to solve and depending on the computational model we use.

For instance, let’s consider the quantum communication setting [15], where the input $\sigma$ is split between communicating parties – Alice has $(\sigma_1, \ldots, \sigma_k)$ and Bob has $(\sigma_{k+1}, \ldots, \sigma_n)$. Let $g_f$ be a characteristic polynomial that is a sum of polynomials over independent subsets of variables:

$$g_f(\sigma_1, \ldots, \sigma_n) = g_1(\sigma_1, \ldots, \sigma_k) + g_2(\sigma_{k+1}, \ldots, \sigma_n).$$ \hfill (15)

Then we can perform an efficient distributed computation of $f$ by sending a single $d$-dimensional state:

• Alice creates and sends $|\psi_S(g_1(\sigma))\rangle$ to Bob;
• Bob creates $|\psi_S(-g_2(\sigma))\rangle$ and compares it to $|\psi_S(g_1(\sigma))\rangle$ via the SWAP-test.

If $g_f(\sigma) = 0 \bmod q$ then $g_1(\sigma) = -g_2(\sigma) \bmod q$, and the probability of success would be 1, otherwise the probability of error would be bounded by $\frac{1}{2}(1 + \varepsilon^2)$ due to the construction of the SWAP-test and the properties of an $\varepsilon$-biased set $S$.

This technique works as well for the simultaneous message passing model (SMP) with no shared resources (see, for example [7] for details), where Alice and Bob do not interact but can send messages to the referee, who makes the final decision. In this case it is the referee who performs the SWAP-test of $|\psi_S(g_1(\sigma))\rangle$ and $|\psi_S(-g_2(\sigma))\rangle$.

If we consider the model of quantum online streaming algorithms [16, 17] and $g_f$ is linear (or quasi-linear), then the state $|\psi_S(g_f(\sigma))\rangle$ can be created within $O(d)$-dimensional space while streaming the input $\sigma$. Afterwards this state is compared (via projective measurement) to the quantum hash of 0:

$$|\psi_S(0)\rangle = \text{QFT}_S(0)|0\rangle = \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} |j\rangle.$$ \hfill (16)

The probability of their coincidence can be expressed as follows:

$$|\langle \psi_S(g_f(\sigma)) | \psi_S(0) \rangle|^2 = \left| \frac{1}{d} \sum_{j=0}^{d-1} e^{2\pi i a_j g_f(\sigma)/q} \right|^2.$$

If $g_f(\sigma) = 0 \bmod q$ then this is exactly 1, otherwise this probability is bounded by $\varepsilon^2$ whenever the set $S = \{a_1, \ldots, a_d\}$ is $\varepsilon$-biased.

This approach results into space-efficient quantum algorithms with a small one-sided error for a family of Boolean functions that have linear or quasi-linear polynomial presentations [14, 18, 19].

5. Conclusion
Quantum Fourier Transform (QFT) is extremely important technique in the area of quantum information processing for it allows constructing efficient quantum algorithms that outperform best known classical counterparts. In this paper we show that quantum hashing may be considered as an extension of the QFT, and though having certain intrinsic differences, it can also allow constructing efficient quantum algorithms for a certain class of computational tasks.
Acknowledgments
The research is supported by the Russian Science Foundation, project No. 19-19-00656.

References
[1] Ablayev F and Vasiliev A 2014 Laser Physics Letters 11 025202 URL http://stacks.iop.org/1612-202X/11/i=2/a=025202
[2] Vasiliev A 2016 Lobachevskii Journal of Mathematics 37 751–754 ISSN 1995-0802 URL http://arxiv.org/abs/1603.02209
[3] Naor J and Naor M 1990 Proceedings of the Twenty-second Annual ACM Symposium on Theory of Computing STOC ’90 (New York, NY, USA: ACM) pp 213–223 ISBN 0-89791-361-2 URL http://doi.acm.org/10.1145/100216.100244
[4] Chen S, Moore C and Russell A 2013 Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques (Lecture Notes in Computer Science vol 8096) ed Raghavendra P, Raskhodnikova S, Jansen K and Rolim J D (Springer Berlin Heidelberg) pp 436–451 ISBN 978-3-642-40327-9 URL http://dx.doi.org/10.1007/978-3-642-40328-6_31
[5] Holevo A S 1973 Probl. Pered. Inform. [Probl. Inf. Transm.] 9 3–11
[6] Nayak A 1999 Foundations of Computer Science, 1999. 40th Annual Symposium on pp 369–376 ISSN 0272-5428
[7] Buhrman H, Cleve R, Watrous J and de Wolf R 2001 Phys. Rev. Lett. 87 167902 URL www.arxiv.org/quant-ph/0102011v1
[8] Gottesman D and Chuang I 2001 Quantum digital signatures Tech. Rep. arXiv:quant-ph/0105032 Cornell University Library URL http://arxiv.org/abs/quant-ph/0105032
[9] Ablayev F and Ablayev M 2015 Lobachevskii Journal of Mathematics 36 89–96 ISSN 1995-0802 URL http://link.springer.com/10.1134/S199508021502002X
[10] Ablayev F, Ablayev M and Vasiliev A 2016 Journal of Physics: Conference Series 681 012019 URL http://stacks.iop.org/1742-6596/681/i=1/a=012019
[11] Vasiliev A 2016 Lobachevskii Journal of Mathematics 37 751–754 ISSN 1995-0802 URL http://arxiv.org/abs/1603.02209
[12] Alon N and Roichman Y 1994 Random Structures & Algorithms 5 271–284 ISSN 1098-2418 URL http://dx.doi.org/10.1002/rsa.3240050203
[13] Nielsen M A and Chuang I L 2000 Quantum Computation and Quantum Information 1st ed (Cambridge University Press) ISBN 0521635039 URL http://www.worldcat.org/isbn/521635039
[14] Ablayev F and Vasiliev A 2009 Electronic Proceedings in Theoretical Computer Science 9 1–11 URL http://arxiv.org/abs/0901.2317
[15] Klauke H 2000 In Proc. Intl. Colloquium on Automata, Languages, and Programming (ICALP) pp 241–252
[16] Khadiev K, Khadieva A and Mannapov I 2018 Lobachevskii Journal of Mathematics 39 1377–1387
[17] Ablayev F, Ablayev M, Khadiev K and Vasiliev A 2018 Classical and Quantum Computations with Restricted Memory (Springer International Publishing) pp 129–155 ISBN 978-3-319-98355-4
[18] Ablayev F and Vasiliev A 2011 Electronic Proceedings in Theoretical Computer Science 52 1–12 ISSN 2075-2180 URL http://dx.doi.org/10.4204/EPTCS.52.1
[19] Ablayev F and Vasiliev A 2011 11th International Conference PaCT 2011 Proceedings (Lecture Notes in Computer Science vol 6873) ed Malyskhin V (Springer) pp 1–13