Journal of Physics: Conference Series

PAPER • **OPEN ACCESS**

On the balanced quantum hashing

To cite this article: F Ablayev *et al* 2016 *J. Phys.: Conf. Ser.* **681** 012019

On the balanced quantum hashing

F Ablayev, M Ablayev and A Vasiliev

Kazan Federal University, Kazan, Russian Federation

E-mail: Alexander.KSU@gmail.com

Abstract. In the paper we define a notion of a resistant quantum hash function which combines a notion of pre-image (one-way) resistance and the notion of collision resistance. In the quantum setting 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 an explicit quantum hash function which is "balanced" one-way resistant and collision resistant and demonstrate how to build a large family of balanced quantum hash functions.

1. Introduction

Peter Shor's quantum factoring algorithm and quantum algorithm for finding discrete logarithm are results that use quantum mechanical effects to break cryptographic systems. The response from a cryptographic community is a "Post-quantum cryptography", which refers to research on problems (usually public-key cryptosystems) that are not efficiently solvable by quantum computers. Currently post-quantum cryptography includes different approaches, in particular, hash-based digital signature schemes such as Lamport signature and Merkle signature scheme.

Quantum key distribution and quantum digital signature are also part of Post-quantum cryptography. Gottesman and Chuang introduced a notion of a quantum one-way function and proposed a quantum digital signature protocol [1], which is based on such a function. This is also the case for other protocols (see for example [2] and [3]).

Recall that in the classical setting a cryptographic hash function h should have at least the following three properties (see, for example, [3]): (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 hard to invert, the security of cryptographic hash functions is "computationally conditional".

In [4], [5] we defined a notion of quantum hashing as a quantum counterpart of classical hashing and presented approach for constructing quantum hash functions. It appeared that the quantum digital signature by Gottesman and Chuang is based on quantum functions which are actually quantum hash functions. Those quantum functions have "unconditionally one-way" property based on Holevo Theorem [6]. We have also shown that quantum hashing can be useful for constructing efficient quantum algorithms [7] and quantum communication protocols [8].

For a quantum hash function, which is a mapping that creates a quantum state from classical information, we require the following properties:

- It can be effectively computed given classical input;
- It is impossible to extract this input from the quantum hash;
- Hashes of different inputs can be distinguished with high probability, which also implies a reliable equality test.

In this paper we investigate the connection between the last two properties. We show that there is a trade-off between them and introduce a notion of the balanced quantum hash function that has both in a good combination.

2. Quantum Hashing

In this section we briefly recall the notion of the quantum hash function, formalize its properties and give several examples.

In the paper [9] we defined a notion of (ϵ, δ)-hash function where values ϵ and δ are numerical characteristics of the above two properties: (i) one-way resistance and (ii) collision resistance properties. The notion of the (ϵ, δ)-hash function is a generalization of the quantum hash function defined in [4], [5].

We present formal definitions now. For $s \geq 1$ let $(\mathcal{H}^2)^{\otimes s}$ be the 2^s-dimensional Hilbert space, describing the states of s qubits. Let $\mathbb{X}$ be a finite set of size $K = |\mathbb{X}|$. We define a $(K; s)$ quantum function ψ to be a unitary transformation (determined by an element $w \in \mathbb{X}$) of the initial state $|\psi_0\rangle^{\otimes s} \in (\mathcal{H}^2)^{\otimes s}$ to a quantum state $|\psi(w)\rangle \in (\mathcal{H}^2)^{\otimes s}$:

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

where $U(w)$ is a unitary matrix. We will also use a shorter notation $\psi : \mathbb{X} \to (\mathcal{H}^2)^{\otimes s}$.

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

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

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

We will use here the following fact [10]. 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 a $(2^k; s)$ quantum function. Let Y be a random variable over $\{0,1\}^k$ obtained by some decoding $\mathcal{M}$ of $|\psi(X)\rangle$ to $\{0,1\}^k$. Then the probability of correct decoding is bounded by

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

That is, we should pick s as small as possible to make a quantum hash function one-way resistant.

Collision Resistant Function. As we have noted in [4] there might be no collisions in the classical sense: since quantum hashes are quantum states they can store arbitrary amount of data and can be different for unequal messages. But the procedure of comparing those quantum states implies measurement, which can lead to collision-type errors.

That is, in order to make a quantum hash function resistant to quantum collisions, we must guarantee the distinguishability of quantum hashes for different inputs. Therefore, the pairwise inner product of the quantum hash function values should be bounded. This is formalized by the following definition.

Definition 2.2 *Let $\delta > 0$. Following [9] 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,*

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

There is a known lower bound by Buhrman et al. [11] for the size of the sets of pairwise-distinguishable states: to construct a set of 2^k quantum states with pairwise inner products below δ we will need at least $\Omega(\log(k/\delta))$ qubits. Using the notation above this implies the bound $s = \Omega(\log\log K - \log\delta))$. The similar lower bound of $\log\log K - c(\delta)$ was proved by a different method in [5].

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

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

The trade-off between one-way resistance and collision resistance The following examples show that one-way resistance and collision resistance lead to the contradictory requirements on the size of the quantum hash and the “more” a quantum function is one-way resistant the “less” it is collision resistant and vice versa.

Example 2.1 *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 $\epsilon = \frac{2}{2^k}$, but also has poor collision resistance of $\delta = \cos\left(\pi/2^k\right)$.

Example 2.2 *We encode a word $w \in \{0,1\}^k$ into k qubits:*

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

This function has one-way resistance $\epsilon = 1$ (no resistance) and collision resistance with $\delta = 0$ (perfect resistance).

Example 2.3 *This example is based on the quantum fingerprinting by Buhrman et al. [11].*

Let $E : \{0,1\}^k \to \{0,1\}^n$ be an error-correcting code with Hamming distance $d \geq n - \delta n$ and $E_i(w)$ is the i-th bit of the codeword $E(w)$.

Quantum hash function $\psi_E : \{0,1\}^k \to (\mathcal{H}^{2n})$ *is defined as following:*

$$|\psi_E(w)\rangle = \frac{1}{\sqrt{n}}\sum_{i=1}^{n}|i\rangle|E_i(w)\rangle = \frac{1}{\sqrt{n}}\sum_{i=1}^{n}|i\rangle\left(\cos\frac{\pi E_i(w)}{2}|0\rangle + \sin\frac{\pi E_i(w)}{2}|1\rangle\right).$$

The properties of this function depend on the underlying error-correcting code. For instance, the original work [11] used Justesen code $E : \{0,1\}^k \mapsto \{0,1\}^n$ *with* $n = ck$ *and Hamming distance* $(1-\delta)n$ *(for* $c > 2$ *and* $\delta < 9/10 + 1/(15c)$*). For that code the corresponding function has one-way resistance* $\epsilon = 2ck/2^k$ *and collision resistance* $\delta < 9/10 + 1/(15c)$.

Example 2.4 *This example is based on the quantum fingerprinting by Ablayev and Vasiliev [12].*

Let $B = \{b_j : b_j \in \{0,\ldots,2^k-1\}\}$, $\delta \in (0,1)$.

Quantum function $\psi_H : \{0,1\}^k \to (\mathcal{H}^{2|B|})$ *is defined as following*

$$|\psi_B(w)\rangle = \frac{1}{\sqrt{|B|}}\sum_{j=1}^{|B|}|j\rangle\left(\cos\frac{2\pi b_j w}{2^k}|0\rangle + \sin\frac{2\pi b_j w}{2^k}|1\rangle\right).$$

The properties of this function depend on the set of numeric parameters B*. We have proved the existence of such a set* B *with* $|B| = \lceil(2/\delta^2)\ln(2^{k+1})\rceil = O(k/\delta^2)$*, that the corresponding function has one-way resistance* $\epsilon = 2|B|/2^k$ *and collision resistance equal to the* δ *above (for proof see [12]).*

3. "Balanced" Quantum Hash Functions

The above considerations lead to the notion of a "balanced" quantum hash function. Informally, if we need to hash elements w from a domain $\mathbb{X}$, $|\mathbb{X}| = K$ and if one can build for $\delta > 0$ a collision δ-resistant $(K; s)$ hash function ψ with $s = O(\log\log K - \log\delta))$ qubits then the function f will be one-way ϵ-resistant with $\epsilon = O(\log K/(\delta * K))$.

The functions from Examples 2.3 and 2.4 are exactly such functions.

In [9], we have defined the concept of a quantum hash generator and offered design, which allows to build different quantum hash functions based on the composition of function from Example 2.4 and an arbitrary classical ϵ-universal hash family [13]. This construction allows to build a large family of balanced quantum hash functions [9]. In particular the following construction explicitly presented:

- Using the relationship between ϵ-universal hash families and Freivalds fingerprinting schemas we present explicit balanced quantum hash function and prove that this construction is optimal with respect to of number of qubits needed for construction.
- Using the relationship between ϵ-universal hash families and error correcting codes (see for example [13]) we present explicit balanced hash function based on Reed-Solomon codes and prove that this construction is optimal with respect to the number of qubits needed for construction.

Acknowledgments

The work is performed according to the Russian Government Program of Competitive Growth of Kazan Federal University. Work was in part supported by the Russian Foundation for Basic Research (under the grants 14-07-00878, 14-07-00557, 15-37-21160).

References

[1] 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

[2] Gavinsky D and Ito T 2013 *Quantum Information & Computation* **13** 583–606 ISSN 1533-7146 URL http://dl.acm.org/citation.cfm?id=2535649.2535652

[3] Amiri R and Andersson E 2015 *Entropy* **17** 5635–5659 ISSN 1099-4300 (*Preprint* 1508.01893) URL http://arxiv.org/abs/1508.01893

[4] Ablayev F M and Vasiliev A V 2014 *Laser Physics Letters* **11** 025202 URL http://stacks.iop.org/1612-202X/11/i=2/a=025202

[5] Ablayev F and Ablayev M 2015 *Lobachevskii Journal of Mathematics* **36** 89–96 ISSN 1995-0802 URL http://link.springer.com/10.1134/S199508021502002X

[6] Holevo A S 1973 *Probl. Pered. Inform. [Probl. Inf. Transm.]* **9** 311

[7] Ablayev F and Vasiliev A 2014 *Computing with New Resources* Lecture Notes in Computer Science ed Calude C S, Freivalds R and Kazuo I (Springer International Publishing) pp 149–160 ISBN 978-3-319-13349-2 URL http://dx.doi.org/10.1007/978-3-319-13350-8_11

[8] Vasiliev A 2015 *International Journal of Applied Engineering Research* **10** 31415–31426

[9] Ablayev F and Ablayev M 2015 (*Preprint* 1509.01268) URL http://arxiv.org/abs/1509.01268

[10] Nayak A 1999 *Foundations of Computer Science, 1999. 40th Annual Symposium on* pp 369–376 ISSN 0272-5428

[11] Buhrman H, Cleve R, Watrous J and de Wolf R 2001 *Phys. Rev. Lett.* **87** 167902 URL www.arXiv.org/quant-ph/0102001v1

[12] Ablayev F and Vasiliev A 2009 *Electronic Proceedings in Theoretical Computer Science* **9** 1–11 URL http://arxiv.org/abs/0911.2317

[13] Stinson D R 1996 *In Proc. Congressus Numerantium 114* pp 7–27