LETTER

Cryptographic quantum hashing

IOP Publishing | Astro Ltd Laser Physics Letters

Laser Phys. Lett. **11** (2014) 025202 (4pp) doi:10.1088/1612-2011/11/2/025202

Letter

Cryptographic quantum hashing

F M Ablayev and A V Vasiliev

Kazan Federal University, Kazan, Russian Federation
Institute for Informatics of Tatarstan Academy of Sciences, Kazan, Russian Federation

E-mail: Alexander.KSU@gmail.com

Received 5 December 2013
Accepted for publication 7 December 2013
Published 24 December 2013

Abstract

We present a version of quantum hash functions based on non-binary discrete functions. The proposed quantum procedure is 'classical-quantum', that is, it takes a classical bit string as an input and produces a quantum state. The resulting function has the property of a one-way function (pre-image resistance); in addition it has properties analogous to classical cryptographic hash second pre-image resistance and collision resistance.

We also show that the proposed function can be naturally used in a quantum digital signature protocol.

Keywords: quantum cryptography, quantum one-way function, quantum hashing, quantum digital signature, quantum fingerprinting

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

1. Introduction

Hashing has many fruitful applications in computer science; in particular public key cryptography relies on cryptographic hash functions. Hash functions are designed to take a string of large length (theoretically any length) as an input and produce a short (in practice a fixed-length) hash value. A cryptographic hash function must additionally be able to withstand all known types of cryptanalytic attack. As a minimum, it must have the following properties [1].

- *Pre-image resistance* (or equivalently first pre-image resistance). Given a hash v it should be 'computationally difficult to invert' hash function *hash*, that is, to find any message w such that $v = hash(w)$. The pre-image resistance property together with the 'easy computation' property (given w it is easy to compute a value $v = hash(w)$) is known as the *one-way property*.
- *Second pre-image resistance.* Given an input w it should be 'computationally difficult' to find another input w' such that $w \neq w'$ and $hash(w) = hash(w')$. Functions that lack this property are vulnerable to second pre-image attacks.
- *Collision resistance.* It should be 'computationally difficult' to find two different messages w and w' such that $hash(w) = hash(w')$. Such a pair is called a cryptographic hash collision. This property is sometimes referred to as strong collision resistance.

The 'computationally difficult (hard) problem' means that for the problem considered there must be no known algorithm (oriented for realization in a realistic computational model) except the enumeration algorithm of possible instances that potentially fit the problem solution. Classical cryptographic functions rely on assumed hardness of certain mathematical problems, such as integer factorization and discrete logarithm. Besides these well-known problems several other potentially hard problems were discovered and such investigations are still in progress.

The main problem arising in this aspect is to prove, for a certain candidate, that the considered problem is really hard. However, proving for a particular function the one-way property would imply that $P \neq NP$. The latest problem is a modern mathematical challenge of the era.

In contrast to the classical approach, quantum cryptography is based on the foundations of quantum mechanics and the information properties of quantum systems. At the end of the last century and in recent decades several models of quantum one-way functions were proposed. In [2] a family of 'classical–classical' functions was considered, whose inputs and outputs are classical binary strings. These functions are candidates to be hard to invert not only classically but also quantumly. Authors call such functions quantum one-way functions.

Quantum one-way functions defined by Gottesman and Chuang [3] are 'classical-quantum' one-way functions, that is, such a function takes a classical bit string as an input

and produces a quantum state. Another type of 'classical-quantum' one-way function was invented by Buhrman *et al* [4] based on binary error-correcting code and is known as quantum fingerprinting. Based on a classical-quantum notion of a quantum one-way function, several schemes of quantum digital signature were proposed [3, 5, 6]. Also, a cryptographic primitive based on quantum fingerprinting was introduced in [7].

In this research letter we define a notion of 'classical-quantum' hashing function which is a natural extension of the notion of 'classical-quantum' one-way function. We present a non-binary variant of quantum hashing function and prove its cryptographic properties. Finally, as an application of quantum hashing we use it in a quantum digital signature scheme.

2. Quantum one-way and hashing functions

The definition of a quantum one-way function is based on [3] and explicitly presented in [5, 6]. Let

$$\psi : \{0,1\}^n \to (\mathcal{H}^2)^{\otimes s} \tag{2.1}$$

be a function (classical-quantum function), where

$$(\mathcal{H}^2)^{\otimes s} = \mathcal{H}^2 \otimes \cdots \otimes \mathcal{H}^2 = \mathcal{H}^{2^s} \tag{2.2}$$

is a 2^s-dimensional Hilbert space made up of s copies of a single qubit space $\mathcal{H}^2$.

We will also use notation

$$\psi : w \mapsto |\psi(w)\rangle \tag{2.3}$$

for ψ, which is frequently used in different papers.

Definition 2.1.

Function ψ is called quantum one-way, if it is

- *easy to compute, i.e. there is a quantum polynomial-time algorithm that on input w outputs $|\psi(w)\rangle$;*
- *impossible to invert, i.e. one cannot obtain w from $|\psi(w)\rangle$ by virtue of quantum information theory.*

Property 2.1. *If $n \gg s$ in the definition above, then given $|\psi(w)\rangle$, it is impossible to obtain w.*

Proof. This pre-image resistance property follows from the Holevo bound [8], since no more than $O(s)$ classical bits of information can be extracted from s qubits and the original message contains $n \gg s$ bits. □

Example 2.1 (*One-way function*). *A word $w \in \{0,1\}^n$ is encoded by a single qubit:*

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

Here we treat $w = w_{n-1}\ldots w_0$ also as a number $w = w_0 + w_{12}^1 + \cdots + w_{n-1}2^{n-1}$.

Clearly, we have that ψ has the one-way property of the definition 2.1 and the property 2.1 above. What we need additionally and what is implicitly assumed in various papers (see for example [5, 6]) is a collision resistance property. However, there is still no such notion as *quantum collision*. The reason why we need to define it is the observation that in quantum hashing there might be no collisions in the classical sense: since quantum hashes are quantum states they can store arbitrary amounts of data and can be different for unequal messages. However, the procedure of comparing those quantum states implies measurement, which can lead to collision-type errors.

Therefore, a *quantum collision* is a situation when a procedure that tests an equality of quantum hashes outputs true, while hashes are different. This procedure can be a well-known SWAP-test [4] or something that is adapted for a specific hashing function. Anyway, it deals with the notion of distinguishability of quantum states, and since non-orthogonal quantum states cannot be perfectly distinguished, we require them to be 'nearly orthogonal'.

To formalize the notion of 'nearly orthogonality' we will call states $|\psi_1\rangle$ and $|\psi_2\rangle$ *δ-orthogonal* if

$$|\langle\psi_1|\psi_2\rangle| < \delta. \tag{2.4}$$

Thus, for a quantum hash function it is important to have an ability to reliably compare quantum hashes of different words and those quantum states need to be distinguishable with high probability, that is, they have to pass non-equality tests.

REVERSE-test. Whenever we need to check if a quantum state $|\psi(w)\rangle$ is a hash of a classical message v, one can use the procedure that we call a *REVERSE-test* (the idea of such a test for the case of a quantum message given by $|v\rangle$ was described in [3], but it had not been given its own name).

Essentially the test applies the procedure that inverts the creation of a quantum hash, i.e. it 'uncomputes' the hash to the initial state (usually the all-zero state).

Formally, let the procedure of quantum hashing of message w consist of unitary transformation $U(w)$, applied to initial state $|0\rangle$, 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. It outputs $v = w$ iff the measurement outcome is $|0\rangle$. So, if $v = w$, then $U^{-1}(v)|\psi(w)\rangle$ would always give $|0\rangle$, and the REVERSE-test would give the correct answer. Otherwise, the resulting state would be δ-orthogonal to $|0\rangle$ since unitary operators preserve the inner product.

Overall, this test has one-sided error bounded by δ if quantum hashes of different messages are δ-orthogonal.

SWAP-test. A more general test that checks the equality of two arbitrary states is the well-known SWAP-test [4], given by the circuit in figure 1.

Applied to quantum hash codes it outputs $|\psi(w)\rangle = |\psi(v)\rangle$, if the measurement result of the first qubit is $|0\rangle$.

Property 2.2. *The probability of obtaining $|0\rangle$ in the SWAP-test is equal to $\frac{1}{2}\left(1 + |\langle\psi(w)|\psi(v)\rangle|^2\right)$.*

Proof. See [4]. □

The probability of error of the SWAP-test inherently depends on the value of the inner product of $|\psi(w)\rangle$ and

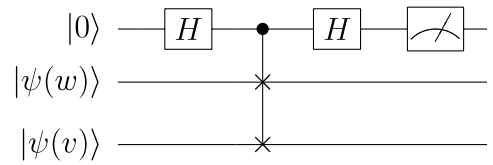

Figure 1. A quantum circuit for SWAP-test.

$|\psi(v)\rangle$ — it is minimal (close to 1/2), when these states are 'nearly orthogonal' [3].

Thus, the property of being δ-orthogonal for quantum states is crucial for quantum collision resistance [3], and at this point we come to a notion of a δ-resistance.

Definition 2.2 (δ-*resistance*). *We call a function* $\psi : w \mapsto |\psi(w)\rangle$ δ-*resistant if for any pair of inputs* w, w', $w \neq w'$ *their images are* δ-*orthogonal:*

$$\left|\langle\psi(w)|\psi(w')\rangle\right| < \delta. \tag{2.5}$$

δ-resistance of a hash function is a key property for bounding the probability of error for the SWAP-test and the REVERSE-test. Note, that the ideas of δ-resistance and REVERSE-test were used in [4].

Note also, that this δ-resistance property also corresponds to the classical *Second pre-image resistance*, since we cannot find two different messages for which the SWAP-test would erroneously output true with probability close to 1.

Finally, we naturally come to the following definition of a quantum hash function.

Definition 2.3 ((n, s, δ)-*quantum hash function*). *We call a function*

$$\psi : \{0,1\}^n \to (\mathcal{H}^2)^{\otimes s} \tag{2.6}$$

(n, s, δ)-*quantum hash function, if it is a quantum one-way and* δ-*resistant.*

The following property is an immediate implication of definition 2.3 and property 2.2.

Property 2.3. *If a function* $\psi : w \mapsto |\psi(w)\rangle$ *is a* (n, s, δ)-*quantum hash function, then the SWAP-test distinguishes the hashes of two messages* $w \neq w'$ *with probability* $\frac{1}{2}(1 - \delta^2)$.

Proof. By the property 2.2 the probability of error for the SWAP-test is $\frac{1}{2}\left(1 + |\langle\psi(w)|\psi(w')\rangle|^2\right)$, since for a δ-resistant function $\left|\langle\psi(w)|\psi(w')\rangle\right| < \delta$, this test distinguishes quantum hashes of the pair of messages $w \neq w'$ with probability $\frac{1}{2}(1 - \delta^2)$. □

Remark 2.1. *The error probability of the SWAP-test can be reduced to any* $\epsilon > 0$ *by standard repetition technique, that is by performing this test upon* $k = O(\log 1/\epsilon)$ *copies of compared states. In other words, we could have used a function*

$$\psi' : \{0,1\}^n \mapsto |\psi'(u)\rangle, \tag{2.7}$$

given by

$$|\psi'(u)\rangle = |\psi(u)\rangle^{\otimes k} = |\psi(u)\rangle \otimes \cdots \otimes |\psi(u)\rangle. \tag{2.8}$$

In this case, the total number of qubits to encode a word of length n *is* $O(\log n \log(1/\epsilon))$.

In the next two sections we show that the known quantum fingerprinting function is a quantum hashing function and we present our construction of a quantum hash function with slightly different characteristics.

3. Quantum fingerprinting

In [4] Buhrman *et al* defined a quantum one-way function

$$f_E : u \mapsto |f_E(u)\rangle \tag{3.1}$$

of a bit string $u \in \{0,1\}^n$, which they have called *quantum fingerprinting*. Based on the existence of the binary error-correcting code $E : \{0,1\}^n \mapsto \{0,1\}^m$ with $m = cn$ and Hamming distance $(1 - \delta)m$ (for $c > 2$ and $\delta < 9/10 + 1/(15c)$) they have defined a quantum fingerprint of u as follows:

$$|f_E(u)\rangle = \frac{1}{\sqrt{m}} \sum_{i=1}^{m} |i\rangle |E_i(u)\rangle \tag{3.2}$$

where $E_i(u)$ denotes the ith bit of $E(u)$.

Property 3.1. *For a* $\delta \approx 9/10 + 1/(15c)$ *the quantum fingerprinting function* f_E *is an* $(n, O(\log n), \delta)$-*quantum hashing function.*

Proof. The function f_E is quantum one-way and is δ-resistant for $\delta \approx 9/10 + 1/(15c)$ [4]. □

4. Quantum hashing

In this section we propose a quantum hashing function based on construction from [9].

Let $N = 2^n$. Let $K = \{k_i : k_i \in \{0, \ldots, N-1\}\}$ and $d = |K|$. We define a classical-quantum function

$$h_K : \{0,1\}^n \to (\mathcal{H}^2)^{\otimes(\log d + 1)} \tag{4.1}$$

as follows. For a message $M \in \{0,1\}^n$ we let

$$|h_K(M)\rangle = \frac{1}{\sqrt{d}} \sum_{i=1}^{d} |i\rangle \otimes \left(\cos\frac{2\pi k_i M}{N}|0\rangle + \sin\frac{2\pi k_i M}{N}|1\rangle\right). \tag{4.2}$$

Theorem 4.1. *For arbitrary* $\delta > 0$ *there exists a set* K *with* $|K| = \lceil (2/\delta^2)\ln(2N)\rceil$ *such that quantum function* h_K *is an* $(n, O(\log n + \log 1/\delta), \delta)$-*quantum hashing function.*

The full proof can be found in [10].

5. Quantum digital signature based on quantum hashing

The proposed quantum hashing is a suitable one-way function for the quantum digital signature protocol from [3] and

below we describe its basic structure modified for the specific hashing function.

To sign a single message bit b Alice picks from $\{1, \ldots, L\}$ uniformly at random a pair of keys (K_0, K_1). This pair constitutes her *private* key.

Using her private key pair Alice creates a sufficient number of public key pairs

$$(|h_{K_0}\rangle, |h_{K_1}\rangle) \tag{5.1}$$

and sends them to potential recipients. It can be easily verified that quantum states in each pair are nearly orthogonal and thus distinguishable with high probability.

Now, given a message bit b, Alice sends it to Bob together with a part of her private key K_b, which constitutes her signature.

Finally, Bob, the recipient of a signed message, validates the signature by 'uncomputing' $|h_{K_b}\rangle$ the same way it was created, i.e. by a sequence of controlled rotations by the negative angles and the Hadamard transform. If the signature is correct Bob will always obtain the all-zero state out of it. Otherwise, the probability of error will be bounded by δ due to δ-collision resistance of the hashing function.

This protocol uses $O(\log \log L)$ qubits for public keys, where L is a security level parameter and it should be chosen to deal with the $1/L$ probability of guessing what the private key is by the possible forger.

6. Numerical results

The aforementioned methods for computing the set K of hashing parameters make sense for comparatively large n. For smaller n the influence of δ results in quite large sizes of the set K. This problem is especially important for the quantum digital signature protocol, where the value of n is not very large.

To deal with this problem we have developed a genetic algorithm that gives good results in acceptable time. Table 1 contains several examples of its work. We recall the notation used in the definition of the hash function h_K:

- n is the length of the message,
- $q_{\text{Numerical}}$ is the size of the quantum hash (number of qubits) obtained by numerical optimization,
- $q_{\text{Theoretical}} = 1 + \lceil \log(2 \ln(2^{n+1})/\delta^2) \rceil$ is the theoretical size of the quantum hash,
- δ is the resulting resistance of h_K (the threshold of the algorithm was set to 0.01).

Table 1. Numerical results from genetic algorithm.

n	$q_{\text{Numerical}}$	δ	$q_{\text{Theoretical}}$
5	5	0.0625	13
6	6	0.0924	12
7	7	0.0995	12
8	8	0.0930	12
9	8	0.0969	12
10	8	0.0998	12
11	9	0.0832	13
12	9	0.0957	12
13	9	0.0965	13
14	9	0.0997	13
15	10	0.0824	13
16	10	0.0880	13
17	10	0.0917	13
18	10	0.0933	13
19	10	0.0969	13
20	10	0.0994	13

7. Conclusion

Quantum cryptography is an emerging field of computer science and new results in this area are of great importance, since they might have applications in the near future. Quantum communications are already here and we need to make them secure. Since hashing has been extensively used for secure classical communications, we expect the same for quantum hashing. In this letter we show how hashing can be used for the single-bit quantum digital signature protocol, and we hope more hashing-based security protocols for quantum communications will appear.

Acknowledgments

Research was partially supported by the Russian Fund for Basic Research (under the grants 11-07-00465, 12-01-31216). We also thank our colleagues from the Academy of Cryptography of the Russian Federation for valuable discussions. Part of this work was done during a visit of the first author to the Department of Information Technology and Education ETH Zurich in the framework of the project 'Computation Power of Randomization and Nondeterminism'.

References

[1] Rogaway P and Shrimpton T 2004 Cryptographic hash-function basics: definitions, implications, and separations for preimage resistance, second-preimage resistance, and collision resistance *Fast Software Encryption* (*Lecture Notes in Computer Science* vol 3017) ed B Roy and W Meier (Berlin: Springer) pp 371–88

[2] Kashefi E and Kerenidis I 2007 Statistical zero knowledge and quantum one-way functions *Theor. Comput. Sci.* **378** 101–16

[3] Gottesman D and Chuang I 2001 Quantum digital signatures *Technical Report* Cornell University Library arXiv:quant-ph/0105032

[4] Buhrman H, Cleve R, Watrous J and de Wolf R 2001 Quantum fingerprinting *Phys. Rev. Lett.* **87** 167902

[5] Lu X and Feng D 2005 Quantum digital signature based on quantum one-way functions *ICACT 2005: 7th Int. Conf. on Advanced Communication Technology* vol 1 pp 514–7

[6] Zhou J, Zhou Y, Niu X and Yang Y 2011 Quantum proxy signature scheme with public verifiability *Sci. China Phys. Mech. Astron.* **54** 1828–32

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

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

[9] Ablayev F and Vasiliev A 2009 Algorithms for quantum branching programs based on fingerprinting *Electron. Proc. Theor. Comput. Sci.* **9** 1–11

[10] Ablayev F and Vasiliev A 2013 Quantum hashing *Technical Report* Cornell University Library arXiv:1310.4922[quant-ph]