Improved Identification Protocol in the Quantum Random Oracle Model

Wen Gao, Yupu Hu, Baocang Wang, and Jia Xie
State Key Laboratory of Integrated Service Networks, Xidian University, China

Abstract: *Boneh et al. [6] proposed an identification protocol in Asiacrypt 2011 that is secure in the classical random oracle model but insecure in the quantum random oracle model. This paper finds that a constant parameter plays a significant role in the security of the protocol and the variation of this parameter changes the security greatly. Therefore, an improved identification protocol that replaces a variable with this constant parameter is introduced. This study indicates that, when the variable is chosen appropriately, the improved identification protocol is secure in both the classical and the quantum random oracle models. Finally, we find the secure lower bound for this variable.*

Keywords: *Collision-finding, quantum-accessible, identification protocol, grover's search algorithm, random oracle model.*

Received November 11, 2014; accepted February 10, 2015

1. Introduction

Several efficient quantum algorithms [10, 11, 12, 15] appear in the literatures outperform the classical algorithms. Shor [15] proposes quantum polynomial-time algorithms to factor large integers and solves the problem of discrete logarithms over cyclic groups, on which the security of most of the existing public key cryptographic systems is based. Grover's [11, 12] quantum algorithms show that searching an unsorted database can be done faster than other classical algorithms. Shor's algorithm and Grover's algorithm impose serious threats on classical cryptographic systems.

Therefore, tremendous efforts have been made on the classical schemes that remain secure against a quantum adversary, which is called post-quantum cryptosystems. Random oracle models are often used to prove the security against adversaries with classical queries. In order to allow adversaries to interact with the oracle by superposition, the quantum random oracle model has been defined recently.

Boneh *et al*. [6] propose a two-party protocol (called IS* protocol) that is secure against classical and quantum adversaries in the classical random oracle model, but insecure once quantum adversaries are allowed to make quantum queries in the quantum random oracle model.

1.1. Contributions

First, we introduce an improved identification protocol. Second, success probabilities of an adversary are derived for the improved protocol in the classical and quantum random oracle models. In the meantime, this work finds the secure lower bound on this variable, which guarantees the security in both models. Additionally, several other possible approaches are introduced.

1.2. Previous Work

Quantum random oracles have been used in several prior works. For example, Bennett *et al*. [3] prove several quantum complexity results relative to a random oracle. The quantum random oracle has also been used to construct quantum money by Aaronson [1]. Brassard and Salvail [7] and Brassard *et al*. [9] employ this model to construct quantum analogues of Merkle's Puzzles. Zhandry [17] give the first proof of security for an identity-based encryption scheme with no additional assumptions in the model.

Zhandry [16] prove that standard constructions of pseudorandom functions from pseudorandom generators or pseudorandom synthesizers are secure in the quantum oracle model, and present the poof of security for a direct construction on lattices. Boneh and Zhandry [5] construct the first existentially unforgeable message authentication codes against quantum chosen message attacks.

2. Preliminaries

2.1. Notations

Functions are denoted by capital letters (such as *F*), and sets by capital script letters (such as $\mathcal{K}$). A symbol like $\mathcal{A}\setminus\mathcal{K}$ represents a set in which elements are in $\mathcal{A}$ but not in $\mathcal{K}$. $\Pr[event]$ stands for the probability of an event. The expression $\mathrm{A}(x,y,z)\to v$ denotes an algorithm that $\mathcal{A}$ inputs (x,y,z) and outputs *v*.

$v \leftarrow \mathcal{A}(x, y, z)$ means that v is generated by the algorithm $\mathcal{A}$ with input (x, y, z).

A cryptographic scheme always incorporates a security parameter which is an integer n. When honest parties initialize the scheme (e.g., when they generate keys), they choose some value n for the security parameter; this value is assumed to be known to any adversary attacking the scheme. The running time of the adversary (and the running time of the honest parties) as well as success probability of an adversary are all viewed as functions of n. We denote any polynomial quantity of n as $poly(n)$.

A function $F(n)$ is negligible if it is non-negative and smaller than any inverse polynomial. That is, for any polynomial $poly(n)$, there exists an N such that for all integers $n>N$, it holds that $F(n)<1/poly(n)$.

A probabilistic polynomial-time (*PPT*) algorithm is a classical randomized algorithm that runs in time polynomial in the size of its input. We also call such algorithms efficient.

2.2. Quantum Random Oracle Model

In the classical random oracle model, an adversary is allowed to make classical queries to a random oracle. If the random oracle is denoted by O, an adversary learns a value from $O(x)$ at the classical state x by each query, and then use the information obtained to attack the system. A suitable hash function H is included in the specification when it is implemented and thus enables a quantum adversary to evaluate this hash function on a quantum superposition of inputs.

Any hash function that can be evaluated by a quantum adversary on quantum states is a quantum-accessible hash function. As in the classical random oracle model, quantum oracles that can be accessed by a quantum adversary are introduced in the quantum world. Similarly, a quantum adversary makes quantum queries to a quantum random oracle. In order to allow a quantum adversary to interact with the quantum oracle by superposition, a new security model is required to allow a quantum adversary to make quantum queries to the quantum random oracle, and thus this new model is called the quantum random oracle model.

Note that the quantum random oracle is replaced by a quantum-accessible hash function when implemented. The classical hash function H should be transformed into a quantum-accessible hash function H_Q.

2.3. Identification Scheme

A standard identification scheme consists of three efficient algorithms, $IS = (IS.KGen, \mathcal{P}, \mathcal{V})$. The algorithm *IS.KGen* returns a key pair (sk, pk) on input 1^n. The joint execution of $\mathcal{P}(sk, pk)$ and $\mathcal{V}(pk)$ defines an interactive protocol between the prover $\mathcal{P}$ and the verifier $\mathcal{V}$. The verifier $\mathcal{V}$ finally outputs a decision bit $b \in \{0,1\}$. It is assumed that for any honest prover the verifier accepts the interaction with output $b=1$.

The security of a standard identification scheme is usually defined by an adversary $\mathcal{A}$ that first interacts with the honest prover to obtain some information about the secret key and then plays the role of the prover and makes a verifier accept the interaction.

An identification scheme is secure if the adversary convinces the verifier with a negligible probability. A identification scheme is quantum-immune if the underlying problem has so far remained immune to quantum attacks, or some evidence suggests that it may be hard for quantum computers.

2.4. Collision-Resistant Hash Function

A hash function H consists of two efficient algorithms, $H=(H.KGen, H.Eval)$. *H.KGen* is a key generation algorithm, inputs 1^n and returns a key k. *H.Eval* is a deterministic algorithm, inputs k and $M \in \{0,1\}^*$, and outputs a digest $H.Eval\ (k, M)$.

Let x be a string of length n, then the leading l bits of the string x is denoted as $x|_l$ where l is a constant integer and $1\leq l\leq n$. For any efficient algorithm $\mathcal{A}$, $k\leftarrow H.KGen(1^n)$, a hash function is near-collision-resistant if the probability we have $M\neq M'$ but $H.Eval\ (k, M)|_l= H.Eval\ (k, M')|_l$ is negligible for $(M, M')\leftarrow \mathcal{A}(k, l)$.

Classically, the upper bound on near-collision-resistance of any hash function is given by the birthday attack. This attack shows that, for any hash function with n bits outputs, an adversary can find a collision with probability of about 1/2 by examining $2^{n/2}$ distinct and random inputs. This attack is optimal for random oracles.

3. Research Methodology

This section describes the research method. Three methods are mainly used in our study, Grover’s quantum search algorithm, Chernoff bounds, and time assumptions. As Grover’s algorithm has advantages in searching an unstructured database over classical algorithms, it is applied to solve the problem of collision. We use Chernoff bounds to determine the success probability of an adversary in the security argument for the improved protocol. Additionally, time assumptions are employed to ensure a reasonable and logical security argument for our protocol.

Chernoff bounds give exponentially decreasing bounds on the tail distribution. Two theorems about Chernoff bounds are given for a sum of Poisson trials and the deviation. Refer to [13] for further information.

- *Theorem 1*. Let X_1, …, X_n be independent Poisson trials such that $\Pr(X_i)=p_i$. Let $X=\sum_{i=1}^{n} X_i$ and $\mu=E(X)$. Then the following Chernoff bounds hold:
  1. For any $\delta>0$, $\Pr(X \geq (1+\delta)\mu) < \left(\frac{e^{\delta}}{(1+\delta)^{(1+\delta)}}\right)^{\mu}$.
  2. For $0<\delta\leq 1$, $\Pr(X \geq (1+\delta)\mu) \leq e^{-\mu\delta^2/3}$.
- *Theorem 2*. Let X_1, …, X_n be independent Poisson trials such that $\Pr(X_i)= p_i$. Let $X=\sum_{i=1}^{n} X_i$ and $\mu=E(X)$. Then for $0<\delta< 1$:
  1. $\Pr(X \leq (1-\delta)\mu) \leq \left(\frac{e^{-\delta}}{(1-\delta)^{(1-\delta)}}\right)^{\mu}$.
  2. $\Pr(X \leq (1-\delta)\mu) \leq e^{-\mu\delta^2/2}$.

The optimal traditional algorithm for searching an unstructured database with N elements requires $O(N)$ steps. A more efficient algorithm is a quantum search algorithm proposed by Grover [11], which is called Grover's algorithm. Grover's algorithm operates such a search in a period of time $O(\sqrt{N})$ by using superposition to probe all entries "simultaneously" [11, 15]. Subsequently, Brassard *et al*. [8] show that, after only $O(\sqrt[3]{N/r})$ expected evaluations of the function, a quantum algorithm can find collisions in arbitrary r-to-one functions, where N is the cardinality of the domain of the function.

Supposing the function is given by a black box, the quantum algorithm is more efficient than traditional methods. We assume a hash function is H:$\{0, 1\}^{*}\rightarrow\{0, 1\}^{n}$, Grover's algorithm can be applied to solve the problem of collision. One first picks a subset $\mathcal{K}$ from the domain $\{0, 1\}^{*}$ and then applies Grover's algorithm on an indicator function. The indicator examines if there exists an $\mathcal{M}'\in\mathcal{K}$ such that $H(\mathcal{M})=H(\mathcal{M}')$ holds for $\mathcal{M}\in\{0,1\}^{*}\backslash\mathcal{K}$. The algorithm finds a collision with a probability of at least 1/2 after $O(\sqrt[3]{2^n})$ evaluations of H, where $|\mathcal{K}|=\sqrt[3]{2^n}$.

For logical presentations about the security argument of our protocol, we formalize assumptions about the computational power of the adversary and the time it takes on quantum and classical computers. Similar to the situation in the real world, a concrete and finite amount of equipments can be used to make a progress in performance. Hence, the speed-up of a computer can be acquired by employing a parallel one with many processors. We apply three assumptions in [6].

First, let $T(C)$ denotes the required time to solve a problem C on a classical computer, and $T_P(C)$ is the required time that elapses on a parallel system. Then there exists a constant $\alpha\geq 1$, for any problem C it holds that $T_P(C)\geq T(C)/\alpha$. Second, for any hash function H and input message M, the evaluation of $H(M)$ requires a constant time $T(H(M))=T_P(H(M))=T_Q(H(M_Q))$, where T_Q denotes the time that elapses on a quantum computer, M_Q represents quantum state inputs. Third, we assume it does not take any extra time to send and receive messages or to any computation except for evaluating a hash function.

The third assumption implicitly states that, compared to the costs of a hash evaluation, the computation that quantum algorithms may create to obtain a speed-up is negligible. This might be too optimistic in the near future, just as Bernstein [4] shows that the total costs of a quantum computation can be higher than that of massive parallel computation. Nevertheless, we study conceptual issues that arise when efficient quantum computers exist, this assumption is still available in our protocol. Refer the reader to [6] for more details.

4. Description of the Improved Protocol

Figure 1 describes the improved identification protocol between a prover (denote as $\mathcal{P}$*) and a verifier (denote as $\mathcal{V}$*). This protocol adds a collision-finding stage to a standard quantum-immune identification scheme. In this stage, $\mathcal{V}$* checks whether $\mathcal{P}$* finds enough collisions for a hash function during a specific time period. Then two parties run the standard quantum-immune identification scheme. $\mathcal{V}$* accepts if $\mathcal{P}$* finds enough collisions in the collision-finding stage or identifies correctly in the identification stage.

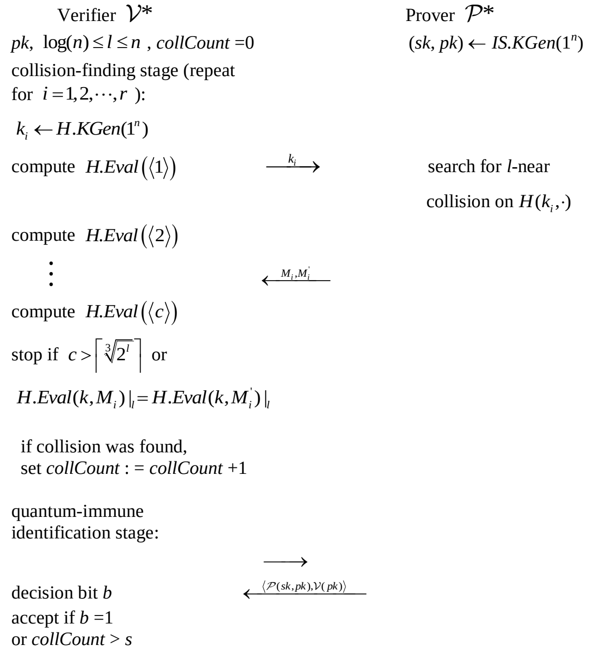
Verifier $\mathcal{V}$*
Prover $\mathcal{P}$*
pk, $\log(n)\leq l\leq n$, $collCount$ =0
$(sk, pk)\leftarrow IS.KGen(1^n)$
collision-finding stage (repeat for $i=1,2,\cdots,r$):
$k_i\leftarrow H.KGen(1^n)$
compute $H.Eval(\langle 1\rangle)$
$\xrightarrow{k_i}$
search for l-near collision on $H(k_i,\cdot)$
compute $H.Eval(\langle 2\rangle)$
$\vdots$
$\xleftarrow{M_i,M_i^{'}}$
compute $H.Eval(\langle c\rangle)$
stop if $c>\lceil\sqrt[3]{2^l}\rceil$ or
$H.Eval(k,M_i)|_l=H.Eval(k,M_i^{'})|_l$
if collision was found,
set $collCount := collCount+1$
quantum-immune identification stage:
$\longrightarrow$
decision bit b
$\xleftarrow{\langle\mathcal{P}(sk,pk),\mathcal{V}(pk)\rangle}$
accept if b =1
or $collCount > s$

Figure 1. The improved IS* protocol.

Assume that IS= ($IS.KGen$, $\mathcal{P}$, $\mathcal{V}$) is a standard quantum-immune identification scheme, and H=($H.KGen$, $H.Eval$) is a hash function. The IS* protocol is denoted by $IS^{*}=(IS.KGen^{*}(1^{n}), \mathcal{P}^{*}, \mathcal{V}^{*})$. $IS.KGen^{*}(1^{n})$ is the key generation algorithm that, for some constant l and $\log(n)\leq l\leq n$, runs $IS.KGen^{*}(1^{n})\rightarrow(sk, pk)$ and returns sk and (pk, l).

Boneh *et al.* [6] show the security of this protocol for $s = r/4$. They prove that it is secure in the classical random oracle model, but is insecure in the quantum random oracle model.

We propose that this protocol can be modified to be secure in the quantum random oracle model. In the next section, we analyze the choice of the variable s. As different choices of the variable lead to different security, we find the expression of the success probability of an adversary for different choices and the secure lower bound on the variable in the classical and quantum settings.

5. Security Argument

An identification protocol is secure if an adversary $\mathcal{A}$ can not impersonate an honest prover $\mathcal{P}^{*}$ to convince $\mathcal{V}^{*}$. The security of the above protocol in the classical random oracle model and in the quantum random oracle model is researched in this section. First, we study its security in the classical random oracle model.

Assume that $\mathcal{V}^{*}$ accepts an adversary $\mathcal{A}$ with outputting a decision bit $b^{*}=1$ after interacting with the adversary $\mathcal{A}$, two parties are both given (pk, l) as input. According to the above protocol, $\mathcal{V}^{*}$ accepts with $b=1$ or $\mathcal{P}^{*}$ finds at least s near-collisions. In view of the independence of two stages in the protocol, Pr[$\mathcal{A}$"*breaks*"*IS**]≤Pr[*collCount*>*s*]+ Pr[$\mathcal{A}$ "*breaks*"*IS*]. Supposing the underlying *IS* is secure, the success probability Pr[$\mathcal{A}$ "*breaks*"*IS*] is negligible.

An adversary $\mathcal{A}$, with access to a random oracle H, has a negligible probability in finding s near-collisions on $H(k_i, \cdot)$ for given k_i in time $O(\sqrt[3]{2^{l}})$. The birthday attack states that at least one collision can be found with probability ≥1/2 after $\sqrt{2^{l}}$ random input evaluations. If we take the parallel power of the adversary into account, $\mathcal{A}$ is allowed to make at most $\alpha\sqrt[3]{2^{l}}$ queries for some constant $\alpha\geq 1$. Since $l>6\log(\alpha)$, we can get $\alpha\sqrt[3]{2^{l}}<\sqrt{2^{l}}$. Bellare *et al.* [2] show that the upper bound on the birthday attack for q queries is $q(q-1)/(2N)$, where N is the range size of a function. Therefore, the success probability of an adversary with at most $q=\alpha\sqrt[3]{2^{l}}$ queries to a random oracle with a range $\{0,1\}^{l}$ is denoted as *Pr*[*Coll*], that is, $\Pr[Coll]\leq\alpha^{2}/(2\sqrt[3]{2^{l}})\leq\alpha^{2}/(2\sqrt[3]{n})$, $\log(n)\leq l\leq n$. The verifier $\mathcal{V}^{*}$ transmits a new "k_i" in each round, the adversary can not use the previously obtained information and has to resume the search for a new key in each round. Hence, the success probability of an adversary for finding one collision is at most *Pr*[*Coll*] in each round.

- *Theorem 3*. Let $r=polly(n)$, and $\Pr[Coll]=p$ is the success probability of an adversary for finding one collision in the collision-finding stage. The success probability of an adversary of the IS* protocol in the random oracle model is:

$$Pr[collCount>s]\leq exp\left(-\frac{(s-pr)^{2}}{3pr}\right) \tag{1}$$

Where $pr< s\leq 2pr$. If the success probability of the adversary in each round is $\Pr[Coll]\leq\alpha^{2}/(2\sqrt[3]{n})$, then:

$$Pr[collCount>s]\leq exp[-\left(\frac{2s^{2}\sqrt[3]{n}}{3\alpha^{2}r}+\frac{\alpha^{2}r}{6\sqrt[3]{n}}-\frac{2s}{3}\right)] \tag{2}$$

Where $\alpha^{2}r/(2\sqrt[3]{n})<s\leq\alpha^{2}r/(\sqrt[3]{n})$, and thus the total success probability of an adversary $\mathcal{A}$ is negligible in the classical random oracle when $s\geq\alpha^{2}r/(2\sqrt[3]{n})$ in secure parameter n for a constant α.

- *Proof*. Chernoff-bounds are employed to find the success probability of a classical adversary in finding at least s collisions in r independent rounds.

As $\delta>0$ and $s=(1+\delta)\mu=(1+\delta)pr$ in the first entry of Theorem 1, $\delta=s/pr-1$. Hence, the success probability of the adversary can be obtained:

$$Pr[collCount>s]\leq e^{s-pr}(pr)^{s}/(s^{s}),\ s>pr \tag{3}$$

As $0<\delta\leq 1$ and $s=(1+\delta)\mu=(1+\delta)pr$ in the second entry of Theorem 1, $\mu< s\leq 2\mu$. That is, $pr< s\leq 2pr$. The success probability of the classical adversary can be obtained:

$$Pr[collCount>s]\leq exp\left(-\frac{(s-pr)^{2}}{3pr}\right),\ pr< s\leq 2pr \tag{4}$$

A classical adversary, making at most $q=\alpha\sqrt[3]{2^{l}}$ queries to a random oracle with a range $\{0, 1\}^{l}$, has a success probability of $p\leq\alpha^{2}/(2\sqrt[3]{2^{l}})\leq\alpha^{2}/(2\sqrt[3]{n})$. We just consider the case when $\Pr(X_i)=p_i=\alpha^{2}/(2\sqrt[3]{n})$, and thus $\alpha^{2}r/(2\sqrt[3]{n})<s\leq\alpha^{2}r/(\sqrt[3]{n})$. The success probability of the classical adversary for finding at least s collisions in r independent rounds can be obtained:

$$\Pr[collCount>s]\leq\exp[-\left(\frac{2s^{2}\sqrt[3]{n}}{3\alpha^{2}r}+\frac{\alpha^{2}r}{6\sqrt[3]{n}}-\frac{2s}{3}\right)] \tag{5}$$

Where $\alpha^{2}r/(2\sqrt[3]{n})<s\leq\alpha^{2}r/(\sqrt[3]{n})$. It is negligible when $s\geq\alpha^{2}r/\sqrt[3]{n}$ in secure parameter n for a constant α due to its decrease with s. Therefore, the total success probability of a classical adversary $\mathcal{A}$ is negligible in the random oracle model. As a result, in classical

settings, the classical adversary's probability of success is negligible.

Next, we discuss the security of the protocol against quantum adversaries in the classical random oracle model. By applying the Grover's search algorithm, we obtain a speed-up by evaluating the indicator function on superposition of inputs. The indicator function is based on the random oracle *H*. As only classical queries can be made to the oracle in the classical random oracle model, the power of the quantum computer can not be employed. Hence, the success probability of a quantum adversary with classical queries, the same as the probability in the random oracle model, is bounded by the classical attack on collision-search.

The security of the protocol against quantum adversaries in the quantum random oracle model is discussed as follows.

The classical hash function *H* should be transformed into a quantum-accessible function (denoted as H_Q) at first. The security is studied when we instantiate the quantum random oracle by the function H_Q. The function H_Q allows quantum queries, which is called a quantum-accessible function. Here, we obey the fact [14] that all the classical computations running on a classical computer can also be operated on a quantum machine. Due to the quantum-accessible function H_Q is allowed to be queried, the evaluation of this function can be applied to Grover's algorithm directly. For each k_i, the attacker $\mathcal{A}_Q$ operates Grover's algorithm on an indicator function to check whether the equation $H_Q.Eval(k_i, x')|_l = H_Q.Eval(k_i, x')|_l$ holds for distinct $x \neq x'$. An algorithm proposed by Brassard et al. [8] tells us that it outputs a collision (M_i, M'_i) with a probability of at least 1/2 after $\sqrt[3]{2^l}$ evaluations of H_Q.

The time assumptions in section 3 show that a quantum evaluation of H_Q approximately elapses the same time as an evaluation of its corresponding classical function *H* does, and any other computation that does not require the evaluation costs zero time. As Grover's algorithm only requires quantum-accessible black-box access to the hash function, the method described above applies directly to the quantum-accessible random oracle model.

- *Theorem 4*. Let *r*=*poly*(*n*), p_Q denotes the success probability of a quantum adversary for finding one collision in the collision-finding stage. The success probability of a quantum adversary in the quantum random oracle model of the IS* protocol is ($p_Q \geq$ 1/2):

$$Pr[collCount > s] < exp(-r/4 - s^2/r + s),\ 0 < s < p_Q r \tag{6}$$

$$Pr[collCount > s] \leq exp[-(s - p_Q r)^2/(3\, p_Q r)]\ ,\ p_Q r < s \leq r \tag{7}$$

- *Proof*. In each round of the collision-finding stage, the adversary $\mathcal{A}_Q$ finds a collision with a probability $p_Q \geq 1/2$, and thus the expectation for finding collisions in *r* independent rounds is $E(X_i) = \mu = p_Q r$.

For $0 < s < p_Q r = \mu$ and $s = (1-\delta)\mu$, then $0 < \delta < 1$. By applying the second entry of Theorem 2, the probability of a quantum adversary for finding collisions that are less than *s* collisions is obtained as:

$$Pr[collCount < s] < \exp(s - r/4 - s^2/r),\ 0 < s < p_Q r \tag{8}$$

For $p_Q r \leq s \leq r$, since $\mu < (1+\delta)\mu \leq 2\mu$ where $0 < \delta \leq 1$, we can get $p_Q r < s \leq 2\ p_Q r$. Only the case $p_Q r < s \leq r$ is studied due to $p_Q \geq 1/2$. According to the second entry of Theorem 1, the following success probability of a quantum adversary can be obtained:

$$Pr[collCount > s] \leq exp[-(s - p_Q r)^2/(3\, p_Q r)] \tag{9}$$

6. Research Data

The research data is outlined in this section. According to the proof of Theorem 1, a classical adversary has the same probability of success with a quantum adversary in the classical random oracle model. Table 1 shows success probabilities of an adversary in the classical random oracle model; Table 2 provides success probabilities of a quantum adversary in the quantum random oracle model.

Table 1. Security in the random oracle model (*r*=*poly*(*n*)).

s	**r/4**	**2r/5**	**r/8**	**3r/5**	**3r/4**
Success probability	$\leq \exp\left(-\frac{r\sqrt[3]{n}}{32\alpha^2}\right)$	$\leq \exp\left(-\frac{r\sqrt[3]{n}}{25\alpha^2}\right)$	$\leq \exp\left(-\frac{r\sqrt[3]{n}}{128\alpha^2}\right)$	$\leq \exp\left(-\frac{18r\sqrt[3]{n}}{75\alpha^2}\right)$	$\leq \exp\left(-\frac{9r\sqrt[3]{n}}{32\alpha^2}\right)$
security	secure	secure	secure	secure	secure

Table 2. Security in the quantum random oracle model (*r*=*poly*(*n*)).

s	**r/4**	**2r/5**	**r/8**	**3r/5**	**3r/4**
Success probability	$> 1 - \exp(-\frac{r}{16})$	$> 1 - \exp(-\frac{r}{100})$	$> 1 - \exp(-\frac{9r}{64})$	$< \exp\left(-\frac{(3-5p_Q)^2 \cdot r}{75p_Q}\right)$	$< \exp\left(-\frac{(3-4p_Q)^2 \cdot r}{48p_Q}\right)$
security	insecure	insecure	insecure	secure	secure

From the research data in Table 1, we can get the conclusion that, in the classical random oracle model, the success probabilities of an adversary are negligible. It is difficult to find collisions for a classical or quantum adversary.

However, in the quantum random oracle model, let *s*=*wr*, where $p_Q \leq w \leq 1$. Hence, if (w-p_Q) is positive and non-negligible, thus $(w\text{-}p_Q)^2 r/(3p_Q)$ is very large due to

$r=poly(n)$. Hence, $exp[-(w-p_Q)^2 r/(3p_Q)]$ is exponentially small. As Table 2 shows, if $(p_Q-3/5)$ is non-negligible and the parameter $s>3r/5$, this protocol is secure in the quantum random oracle model.

7. Results Analysis

We analyze our results in this section, and find the lower bound on this parameter. Additionally, some other optional approaches are given to make the identification protocol secure in the quantum random oracle model.

7.1. Lower Bound

The lower bounds of the variable s are explored to guarantee the security of the IS* protocol in the classical and quantum random oracle models.

- *Theorem 5*. Assuming that the security parameter is n, p (p_Q, respectively) denotes the success probability of collision-finding in each round of the protocol in the classical (quantum, respectively) random oracle model. Then, the lower bound of the variable s against a quantum adversary have the same expression with a classical adversary as: $s_l = pr + \sqrt{-3npr \ln 2}$.

- *Proof*. In the random oracle model, according to Theorem 3, the success probability of an adversary with classical queries is:

$$Pr[collCount> s]\leq e^{s-pr} (pr)^s/(s^s),\ s>pr \tag{10}$$

Detailed, $Pr[collCount> s]\leq exp[-(s-pr)^2/(3pr)]$ where $pr< s\leq 2pr$, and $\Pr[collCount\geq s]\leq 2^{-s}$, $s\geq 6pr$. It is apparent that the probability decreases with s, and thus the lower bound of s is $pr< s_l\leq 2pr$ since the success probability is negligible when $[s/(pr)-1]$ is non-negligible. Since the security parameter is n, we can get $s_l = pr + \sqrt{-3npr \ln 2}$.

In the quantum random oracle model, the success probability of a quantum adversary of the protocol is:

$$Pr[collCount< s]\leq exp[-(p_Q r)^2/(2p_Q r)] \tag{11}$$

Where $0< s< p_Q r$, and

$$Pr[collCount> s]\leq exp[-(p_Q r-s)^2/(3p_Q r)] \tag{12}$$

Where $p_Q r< s\leq r$. We can also get the secure lower bound of the parameter $s_l = p_Q r + \sqrt{-3np_Q r\, ln 2}$.

7.2. Other Approaches

Assume that the prover fails to pass the identification stage and the decision bit b=0, the identification of IS* protocol totally depends on the collision-finding stage. We present several approaches that can be considered to modify the protocol to be secure even in the quantum random oracle model.

- Let the parameter $s > p_Q r + \sqrt{-3np_Q r\, ln 2}$, the protocol will be secure in the quantum random oracle model.
- Reducing the number of evaluations to $<<\left\lceil \sqrt[3]{2^l} \right\rceil$, the probability of finding a collision in each round is negligible as the case in the random oracle model.
- The collision-search stage of the protocol is encouraged to transform into other quantum-secure primitives.

8. Conclusions

An improved protocol is introduced to modify the security of the IS* protocol proposed by Boneh *et al.* [6]. The improved protocol is not only secure in the classical random oracle model, but is also secure in the quantum random oracle model. Success probabilities of an adversary are studied in all cases instead of just in the setting where $s = r/4$ in the original protocol. Our results give the lower bound on the quantum research of the near-collision-resistant hash function, and thus it can be used even if the conclusion of the problem of collision is changed. Furthermore, the secure lower bound is given on the variable s in the IS* protocol.

Although some other approaches are introduced, further study is needed. Quantum algorithms that accelerating the classical methods significantly, like Grover's and Shor's algorithms, and other quantum secure primitives in the quantum random oracle model need to be explored.

Acknowledgements

This work is supported by the National Natural Science Foundations of China (No. 61472309, 61572390, 61672412), and the 111 Project (No. B08038).

References

[1] Aaronson S., "Quantum Copy-Protection and Quantum Money," *in Proceeding of 24th Annual IEEE Conference on Computational Complexity*, Washington DC, pp. 229-242, 2009.

[2] Bellare M., Kilian J., and Rogaway P., "The Security of Cipher Block Chaining Message Authentication Code," *Journal of Computer and System Sciences*, vol. 61, no. 3, pp. 362-399, 1994.

[3] Bennett C., Bernstein E., Brassard G., and Vazirani U., "Strengths and Weaknesses of Quantum Computing," *SIAM Journal in Computing*, vol. 26, no. 5, pp. 1510-1523, 1997.

[4] Bernstein D., "Cost Analysis of Hash Collisions: Will Quantum Computers Make SHARCS Obsolete?," *in Proceeding of 4th Workshop on Special-purpose Hardware for Attacking Cryptograhic Systems*, Lausanne, pp. 105-116, 2009.

[5] Boneh D. and Zhandry M., "Quantum-secure Message Authentication Codes," *in Proceeding*

of 32nd International Conference on the Theory and Applications of Cryptographic Techniques, Athens, pp. 592-608, 2013.

[6] Boneh D., Dagdelen Ö., Fischlin M., Lehmann A., Schaffner C., and Zhandry M., "Random Oracles in a Quantum World," *in Proceeding of 17th International Conference on the Theory and Application of Cryptology and Information Security*, Seoul, pp. 41-69, 2011.

[7] Brassard G., and Salvail L., "Quantum Merkle Puzzles," *in Proceeding of 2nd International Conference on Quantum, Nano and Micro Technologies*, Washington, pp. 76-79, 2008.

[8] Brassard G., Høyer P., and Tapp A., *Theoretical Informatics*, Springer, 1998.

[9] Brassard G., Høyer P., Kalach K., Kaplan M., Laplante S., and Salvail L., *Advances in Cryptology-CRYPTO*, Springer, 2011.

[10] Daoud E., "Quantum Computing for Solving a System of Nonlinear Equations over GF(q)," *the International Arab Journal of Information and Technolgy*, vol. 4, no. 3, pp. 201-205, 2007.

[11] Grover L., "A Fast Quantum Mechanical Algorithm for Database Search," *in Proceeding of 28th Annual Symposium on the Theory of Computing*, New York, pp. 212-219, 1996.

[12] Grover L., "Quantum Search on Structured Problems," *in Proceeding of Quantum Computing and Quantum Communications*, vol. 1509, London, pp. 126-139, 1998.

[13] Mitzenmacher M. and Upfal E., *Probability and Computing Randomized Algorithms and Probabilistic Analysis*, Cambridge University Press, 2005.

[14] Nielsen M. and Chuang I., *Quantum Computation and Quantum Information*, Cambridge University Press, 2000.

[15] Shor P., "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer," *SIAM Journal on Computing*, vol. 26, no. 5, pp. 1484-1509, 1997.

[16] Zhandry M., "How to Construct Quantum Random Functions," *in Proceeding of FOCS'12*, New Brunswick, pp. 679-687, 2012.

[17] Zhandry M., "Secure Identity-based Encryption in the Quantum Random Oracle Model," *International Journal of Quantum Information*, vol. 13, no. 4, pp. 758-775, 2012.

Wen Gao is a PhD student in Xidian University. She received her BS in Electronic Information Engineering from Henan University of Technology, China in 2011 and she takes a successive postgraduate and doctoral program. Her research interests include lattice-based cryptography and quantum computation and quantum attack.

Yupu Hu is a professor and PhD supervisor of the School of Telecommunications Engineering, Xidian University, China. He received his PhD in cryptography from Xidian University, China in 1999, and received his MS and BS in mathematics from Xidian University, China in 1987 and 1982, respectively. His main research interests include public key cryptography based on lattices and the analysis and application of fully homomorphic encryption schemes.

Baocang Wang is a professor and PhD supervisor of the School of Tele-communications Engineering, Xidian University, China. He received his PhD in cryptography from Xidian University, China in 2006, and received his MS and BS in mathematics from Xidian University in 2004 and 2001, respectively. His main research interests include public-key cryptography and wireless network security.

Jia Xie is a PhD student in Xidian University. She received her BS in Electronic Information Engineering from Henan University of Technology, China in June, 2011. Her research interests include lattice-based cryptography and quantum computation and quantum information.