Quantum random oracle model for quantum digital signature

Tao Shang,* Qi Lei, and Jianwei Liu
School of Electronic and Information Engineering, Beihang University, Beijing 100083, China
(Received 8 April 2016; published 10 October 2016)

The goal of this work is to provide a general security analysis tool, namely, the quantum random oracle (QRO), for facilitating the security analysis of quantum cryptographic protocols, especially protocols based on quantum one-way function. QRO is used to model quantum one-way function and different queries to QRO are used to model quantum attacks. A typical application of quantum one-way function is the quantum digital signature, whose progress has been hampered by the slow pace of the experimental realization. Alternatively, we use the QRO model to analyze the provable security of a quantum digital signature scheme and elaborate the analysis procedure. The QRO model differs from the prior quantum-accessible random oracle in that it can output quantum states as public keys and give responses to different queries. This tool can be a test bed for the cryptanalysis of more quantum cryptographic protocols based on the quantum one-way function.

DOI: 10.1103/PhysRevA.94.042314

I. INTRODUCTION

Quantum digital signature (QDS) is an important direction of quantum cryptography, which can be used in message transfer to prevent impersonation, tampering, and repudiation in an information-theoretically secure way. Comparatively, classical unconditionally secure signature schemes against quantum computing attacks have been proposed [1,2], but the resource assumption of secure classical channels is practically impossible [3]. With the security verified by information-theoretical limits and quantum mechanics, QDS schemes have been applicable by just using existing mature quantum key distribution (QKD) equipment and an experimental transmission distance of more than 100 km can be achieved [4,5]. In 2001, Gottesman *et al.* [6] first proposed a QDS scheme, a quantum version of the Lamport public key based signature scheme [7], for certifying the origin and authenticity of a message. In this QDS scheme, public keys are produced through a quantum one-way function instead of the frequently used trapdoor one-way function in classical cryptography. The quantum one-way function transforms a classical bit-string into quantum states. To ensure the validity of transmitted messages, the sender transmits pairs of quantum signatures, consisting of classical secret keys and quantum public keys, to several recipients. The recipients store the signature pairs and verify the quantum signatures by nondestructive quantum state comparison, such as SWAP test. As we know, general nondestructive quantum state comparison and quantum memory are two key constraints for the development of QDS. Over 10 years later, in 2012, Clarke *et al.* [8] experimentally realized a QDS scheme based on coherent states, while the remaining challenge for QDS to be feasible in practice is quantum memory. The critical requirement of quantum memory was circumvented by Dunjko *et al.* [9,10]. They put forward a practical QDS scheme without quantum memory and later implemented it. Obviously, the slow pacing of experimental realization hampered the progress of QDS and other quantum protocols. Alternatively, we can construct a security model which can facilitate exploration of quantum one-way function to more scenarios and security analysis of related quantum cryptographic protocols, such as quantum digital signature schemes [4,6,9] and quantum public-key encryption schemes [11,12]. The desirable security model needs to provide participants with outputs of a quantum one-way function and results of quantum state comparison and, also, give the same response to an adversary to model possible quantum attacks. Then the security model can be instantiated with continuously developed techniques [8,10]. In classical cryptography, a similar efficient analysis model called random oracle (RO) was introduced in 1993 [13].

RO has been used to design effective cryptographic protocols and give rigorous proofs of security for cryptographic protocols over 20 years [13–16]. RO is virtually a theoretical black box which outputs random bits in equal length when queried by all parties including an adversary. Queries to RO are standardly designed to model an adversary's attack power [17]. The rapidly evolving quantum computation equips a quantum adversary with sufficient computational power. To analyze classical cryptographic protocols against quantum adversaries, Boneh *et al.* [18] started pioneering work on the quantum random oracle (QRO) model, more precisely, the quantum-accessible random oracle model, in which an adversary can make quantum superposition queries. Later, Zhandry [19,20] upgraded the quantum-accessible random oracle with a semiconstant distribution to make it indistinguishable with the identical uniform distribution under quantum algorithms. In 2013, Boneh and Zhandry [21] made significant progress by initiating the study of quantum-secure digital signatures and quantum chosen ciphertext security. In the quantum-accessible random oracle model, an adversary can make quantum chosen message queries and quantum chosen ciphertext queries. Till now, most of the quantum-accessible random oracle model research has focused on classical cryptographic protocols against quantum adversaries. Furthermore, can we explore the construction of a new QRO model to effectively analyze quantum cryptographic protocols against quantum attacks?

In this paper, we construct a QRO model to analyze the security of QDS schemes based on quantum one-way function. We start with the quantum random oracle modeling a collision-free quantum one-way function. Then we will ive a general security analysis procedure in the QRO model. For convenient analysis, we choose the original QDS scheme [6]. It is very

*shangtao@buaa.edu.cn

 ©2016 American Physical Society

meaningful to endow new meaning and explanation to the QRO model for quantum cryptosystems.

The main contributions of our work are as follows.

(1) *A quantum random oracle model is redefined for the security analysis of quantum cryptographic protocols based on quantum one-way function.* QRO is used to model quantum one-way function. QRO outputs quantum states as public keys. For security reduction, the no-cloning theorem is chosen to be the hard problem.

(2) *A quantum digital signature scheme is proved QCMA (quantum chosen message attack)-secure in this quantum random oracle model.* To model an adversary's attacks such as eavesdropping and forgery attack, specific queries to QRO are described. Provable security, namely, QCMA security, is defined for the QDS. Then we prove that the original QDS scheme is QCMA-secure in this QRO model, even when an adversary has quantum access to QRO.

This paper is structured as follows. In Sec. II, we introduce the related works, including the original QDS scheme, original security model, and analysis procedure in the RO model. Section III focuses on the description of our QRO model and the definition of the QDS in the QRO model. Then we give a detailed security analysis and comparison of different security models in Sec. IV. Section V is our conclusion.

II. RELATED WORKS

A. Quantum digital signature scheme

We briefly recall the representative QDS scheme proposed by Gottesman *et al.* [6]. The scheme assumes that all participants will know how to implement the quantum one-way function, and it is based on perfect devices and channels. Notation is as follows.

b: One-bit classical message.

k_b^i: L-bit classical secret key.

$|f_{k_b^i}\rangle$: n-bit public keys of quantum states that a quantum one-way function generates.

$k_b^i \mapsto |f_{k_b^i}\rangle$: Quantum one-way function that maps a classical bit-string k_b^i to quantum states $|f_{k_b^i}\rangle$.

Initializing phase: Alice chooses a series of L-bit classical bit-strings $\{k_0^i, k_1^i\}$, $1 \leqslant i \leqslant M$, as secret keys for a single message b. k_0 is used to sign the message $b = 0$, and k_1 is used to sign the message $b = 1$. Note that k_0 and k_1 are chosen independently and randomly for each i. M is a security parameter and the scheme is exponentially secure in M when other parameters are fixed.

Signing and verifying phase:

(1) Alice chooses secret keys according to b. Then she sends public keys to at most t recipients, $t < L/n$. The signed message $(b, k_b^1, k_b^2, \ldots, k_b^M)$ are sent to recipients via the insecure classical channel.

(2) Every recipient checks each of the revealed public keys to verify $k_b^i \mapsto |f_{k_b^i}\rangle$ by quantum state comparison. Then each recipient j counts the number of incorrect keys as s_j.

(3) According to s_j, each recipient determines the message b as transferable, valid, or invalid. Then all participants discard all used and unused keys.

To prove the impossibility of forgery and repudiation, the original security model sets security parameters. In the forging scenario, an adversary wants to convince Bob that a faked message b' is valid, i.e., $b' \neq b$. Thus the secret keys k_b^i not received by recipients can be modified by the adversary. Some public keys will fail and the number of incorrect keys s_j will increase. The scheme defines the rejection parameter c_2 so that when $s_j > c_2 M$, the recipients reject the signature. In Alice's repudiation scenario, Alice wishes Bob (for instance) to accept a message and Charlie to reject it, so she may give completely different public keys to Bob and Charlie. To avoid this kind of cheating, Bob and Charlie will exchange quantum public keys to compare by SWAP test. So Alice's goal is to pass all SWAP tests and make her message to be intransferable. Analysis shows that the possibility of passing the SWAP test is exponentially small in M. In participants' reputation scenario, they can always deny the sender Alice's message. Therefore, there must be at least two honest participants.

Note that quantum states can store an arbitrary amount of data and can be different for unequal messages, but the measurement procedure may lead to collision-type errors, i.e., different classical inputs may lead to equal quantum outputs. Gottesman *et al.* assumed δ-orthogonal quantum states to limit the measurement errors of the SWAP test. Instead, to give an effective analysis of schemes based on quantum one-way function, we may reasonably use the QRO model to realize the collision-free property. So we assume that the quantum states generated by QRO are distinguishable by its measurement.

B. Security analysis procedure: From RO to QRO

Bellare and Rogaway [13] introduced the random oracle model, which made it possible to give rigorous proof of security for certain basic cryptographic protocols [22]. RO is used to model a hash function and output total random hash results. All parties, including legal communicators and an adversary, should query RO for the hash value. The security analysis procedure based on the RO model is summarized as follows:

(1) Define a hard problem Π.

(2) Redescribe a protocol for Π.

(3) Define the specific security for the protocol.

(4) Prove the security of the protocol by reduction.

According to the methodology of the RO model, the QRO model for quantum cryptographic protocols can also conform to the above analysis procedure. Proving security in the QRO model presents many challenges. For each step of this analysis procedure, we can further explore the following four problems.

(1) What is a feasible hard problem Π in the QRO model? Hard problems for reduction vary among different RO models.

In the RO model, Hwang *et al.* [23] put forward a new quantum primitive called the "unbiased chosen basis" (UCB) assumption based on the no-cloning theorem and use it as a hard problem for an adversary to prove the security of three-party quantum key distribution protocol. No-cloning theorem is the foundation of quantum cryptography, which indicates that one cannot copy a qubit if he or she does not know the polarization basis of the qubit. This physical property of quantum mechanics can provide an absolutely secure reduction for the QRO model.

In the quantum-accessible random oracle model for postquantum cryptography, an adversary with quantum end-user machine is allowed to issue RO quantum queries, i.e., an exponential number of queries in superposition states. The difficult point for reduction lies in the fact that the reduction algorithm must evaluate RO at all points in the superposition. To provide an indistinguishable output under this powerful query, Boneh *et al.* [18] assumed that there exists a quantum-secure pseudorandom function (QPRF) which ensures that RO queries are answered consistently across queries. Thus, cryptographic protocols can be proven secure by means of history-free reductions related to the existence of QPRF. Their work gives an important hint about the construction of the QRO model considering quantum queries.

Furthermore, Definitions 1 and 2 give detailed descriptions of the related quantum query and quantum oracles [21].

Definition 1 (quantum chosen message query). The quantum chosen message query is the transformation

$$\sum_m \psi_m |m\rangle \rightarrow \sum_m \psi_m |m, S(k,m)\rangle,$$

where $S(k,m)$ is the signature on m using signing key k.

An attacker can sample the response to such a query and obtain one valid message-signature pair. After q such queries, it can obtain q valid message-signature pairs.

Definition 2 (quantum-accessible oracles). An oracle $O : \mathcal{X} \rightarrow \mathcal{Y}$ is implemented by a unitary transformation O, where

$$\mathrm{O}|x,y,z\rangle = |x, y + O(x), z\rangle$$

and $+ : \mathcal{X} \times \mathcal{X} \rightarrow \mathcal{X}$ is some group operation on $\mathcal{X}$. Suppose there is a quantum algorithm that makes quantum queries to oracles $O_1, \ldots, O_q$. Let $|\psi_0\rangle$ be the input state of the algorithm, and let $\mathrm{U}_0, \ldots, \mathrm{U}_q$ be the unitary transformations applied between queries. Note that the transformations U_i are themselves possibly the products of many simpler unitary transformations. The final state of the algorithm will be

$$\mathrm{U}_q \mathrm{O}_q \ldots \mathrm{U}_1 \mathrm{O}_1 \mathrm{U}_0 |\psi_0\rangle.$$

We can also have an algorithm make classical queries to O_i. In this case, the input to the oracle is measured before applying the transformation O_i. We call a quantum oracle algorithm efficient if the number of queries q is a polynomial in the size of its input, and each of the transformations U_i between queries can be written as the product of polynomially many unitary transformations from some fixed basis set.

(2) How is a protocol for Π redescribed? Redescribing a protocol means formally defining the parameters for the protocol and the queries for modeling an adversary's capability. A similar description has been given in Refs. [17] and [23]. In the RO model, an adversary interacts with players by making various queries to RO, such as the "send query" and "hash query" [23]. Modifications of these queries can be made for the security proofs in the QRO model.

(3) What is the specific security for quantum cryptographic protocols? For the security definition of signature scheme, existential forgery under chosen message attack is always considered [21,24]. Chosen message attack means that an adversary cannot produce $q + 1$ valid message-signature pairs with q chosen message queries.

(4) How can the security of quantum cryptographic protocols be proved by reduction? Reduction means that if an adversary wants to break the security of a protocol, a challenger can take advantage of the adversary's capability to solve the hard problem Π by controlling the RO and providing indistinguishable output. Considering the superposition quantum query for the reduction algorithm, Zhandry [19] provided a related definition and a lemma which allows for the efficient simulation of an exponentially large list of samples given only a polynomial number of samples.

Definition 3 (small-range distributions). Fix sets $\mathcal{X}$ and $\mathcal{Y}$ and a distribution D on $\mathcal{Y}$. Fix an integer r. Let $\mathrm{y} = (y_1, y_2, \ldots, y_r)$ be a list of r samples from D and let P be a random function from $\mathcal{X}$ to $[r]$. The distributions on y and P induce a distribution on functions $H : \mathcal{X} \rightarrow \mathcal{Y}$ defined by $H(x) = y_{\mathrm{P}(x)}$. This distribution is called a small-range distribution with r samples of D.

Lemma 1. There is a universal constant C_0 such that, for any sets $\mathcal{X}$ and $\mathcal{Y}$, distribution D on $\mathcal{Y}$, any integer ℓ, and any quantum algorithm F making q queries to an oracle $H : \mathcal{X} \rightarrow \mathcal{Y}$, the following two cases are indistinguishable,except with probability less than $C_0 q^3 / l$:

(a) $H(x) = y_x$, where y is a list of samples of D of size $|\mathcal{X}|$.

(b) H is drawn from the small-range distribution with ℓ samples of D.

III. QUANTUM RANDOM ORACLE MODEL

Differently from the RO model and prior QRO model (precisely, the quantum-accessible random oracle model), our objective is to construct a QRO model for quantum cryptographic protocols.

A. Definition of quantum random oracle

Considering the possible quantum collision problem resulting from quantum measurement, we assume that there exists a collision-free quantum one-way function and use QRO to model it by requiring that different quantum states produced by QRO are distinguishable by QRO measures. Since an adversary may have access to all quantum states, we assume that all parties, including sender Alice, recipient Bob, and adversary A, query QRO for classical random bits, quantum one-way function outputs, and quantum state comparison results. For a quantum adversary, this QRO can respond consistently to quantum superposition query like the quantum-accessible oracle [21]. We also assume that quantum states are transmitted without interference.

Definition 4 (quantum random oracle). A quantum random oracle is an efficient algorithm $(\mathcal{G}, H_q, \mathrm{Measure})$ where

$\mathcal{G}$: For any input of a classical bit-string m, it outputs a random bit-string $k = \{0,1\}^k$.

H_ψ: For any input of a classical bit-string $k = \{0,1\}^k$, it operates

$$\psi : \{0,1\}^k \mapsto \mathcal{H}^{\otimes s},$$

to generate distinguishable quantum states $|\psi_{k^i}\rangle$, where

$$\mathcal{H}^{\otimes s} = \mathcal{H}_1 \otimes \ldots \otimes \mathcal{H}_s$$

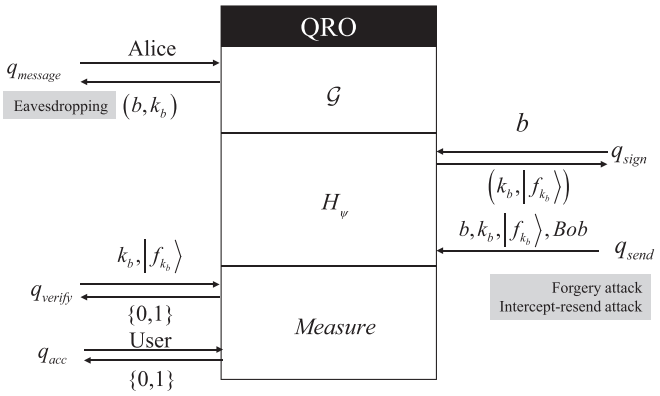

FIG. 1. QRO model.

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

Measure: Any qubits $|\psi_{k^i}\rangle$, $|\psi_{k^j}\rangle$ QRO generates are distinguishable when QRO measures, i.e.,

$$|\langle\psi_{k^i}|\psi_{k^j}\rangle|^2 = \varepsilon,$$

where ε is negligible for $i \neq j$.

We illustrate these three parts of QRO in Fig. 1.

B. Properties of quantum random oracle

Property 1. Quantum random oracle can respond consistently to quantum queries $\sum_m \psi_m|m\rangle$ by mapping $\mathcal{X} \to \mathcal{Y}$,

$$O(m,k) : \sum_m \psi_m|m\rangle \to \sum_m \psi_m|m,k\rangle,$$

where k is a random bit-string on m.

Then it samples r times from some distribution on $\mathcal{X}$ such that, for every m and k, $O(m,k)$ is uniformly distributed on $\mathcal{Y}$.

Proof. Let r be some integer to be chosen later. Replace $\mathcal{X}$ with small-range distributions of r samples on $\mathcal{Y}$. Lemma 1 shows that an adversary can distinguish $\mathcal{X}$ with $\mathcal{Y}$ with probability less than C_0q^3/r. Thus, we use r samples of a small-range $\mathcal{Y}$ to replace r samples of an exponentially large-range $\mathcal{X}$ with distinguishable probability less than C_0q^3/r, which facilitates the quantum random oracle to respond to a quantum query with suitable r.

Quantum random oracle can accurately match classical secret keys with corresponding quantum public keys.

Proof. A quantum one-way function transforms an input of classical bit-string to an output of quantum states. A forgery of signature can be made when an adversary finds out a collision error, i.e., different quantum states pass the test of equality by measurement. In the case of possible quantum collision error, we use a quantum random oracle to generate collision-free quantum states $|\psi_{k^i}\rangle$ as Definition 4,

$$|\langle\psi_{k^i}|\psi_{k^j}\rangle|^2 = \varepsilon, \tag{1}$$

where ε is negligible for $i \neq j$. Equation (1) implies that all quantum states generated by QRO vary with different classical inputs and can be measured by QRO accurately, so this quantum random oracle can accurately match classical secret keys with corresponding quantum public keys.

C. QDS in the QRO model

In order to prove whether a QDS scheme is resistant to a chosen message attack, even when an adversary submits quantum superpositions of messages, we need a suitable definition of the QDS scheme in the QRO model.

Definition 5. A quantum digital signature scheme is a tuple of $(\mathcal{G},\text{Sign},\text{Verify})$ algorithm called the generator, signing algorithm, and verifying algorithm, respectively.

Generator $\mathcal{G}$: On inputting a bit-string 1^k, the generator randomly produces a classical secret key k.

Signing algorithm $\text{Sign}(m,k)$: To sign a message m, QRO operates $|f_k\rangle \leftarrow \text{H}_\psi(m,k)$ to generate a public key of quantum state $|f_k\rangle$.

Verifying algorithm $\text{Verify}(k,|f_k\rangle)$: To verify a signature pair $(k,|f_k\rangle)$, QRO takes quantum measurement $\text{Verify}(k,|f_k\rangle) \in \{0,1\}$. This must be the case for all $|f_k\rangle \in \text{H}_\psi(m,k)$, $\text{Verify}(k,|f_k\rangle) = 1$.

In contrast to core algorithms of classical digital signature schemes the QDS scheme generates a public key of quantum states in the signing algorithm, and the verifying algorithm is measurement rather than computation.

IV. SECURITY ANALYSIS OF A QDS SCHEME IN THE QRO MODEL

As mentioned in Sec. II, the security analysis of quantum cryptographic protocols in QRO follows the following procedure: (1) Define a hard problem Π, (2) redescribe the quantum protocol for Π, (3) define the specific security for the quantum protocol, (4) prove the security of the quantum protocol by reduction. Phases (1) and (3) are related to specific quantum protocols. For example, the three-party quantum key distribution protocol [23] chooses UCB assumption as a hard problem for the authenticated quantum key distribution security. Here we use the no-cloning theorem as a hard problem for the provable security of a QDS scheme. Phases (2) and (4) are common for all quantum cryptographic protocols, just as in classical cryptography [13,17,21]. Formal queries need to be defined in phase (2) to model an adversary's capability and proving security. Here we take the QDS scheme [6] described in related works as an example for security analysis.

A. Hard problem in the QRO model

For quantum cryptographic protocols, we choose the no-cloning theorem, one of the foundations of quantum cryptography, to be the hard problem Π for reduction. The no-cloning theorem indicates that it is impossible to create an identical copy of an arbitrary unknown quantum state. Note that we carry out security reduction relative to a quantum physical property instead of the existence of the collision-free quantum one-way function. For example, consider a QDS scheme; we prove it to be unforgeable for quantum adversaries by a reduction to no-cloning theorem. We can claim that the QDS scheme is unforgeable as long as violating the no-cloning theorem is infeasible, even when an adversary has quantum access to random oracle. This technique works well whenever we can assure the success of the adversary A.

B. Description of the QDS scheme

Since an adversary interacts with players by making various queries to QRO, we formulate specific queries to describe the QDS scheme [6]. According to Property 2, QRO can correctly match secret keys and public keys. So the number of incorrect keys s_j is equal to 0. Then we do not need the acceptable or transferable boundaries. Here we present the QDS scheme with a single key pair.

(1) Message query $q_{\text{message}}\{\text{Alice}\}$: All parties are allowed to know whether or not Alice has sent a message b to QRO. If Alice sends the message, QRO sends (b,k_b) back. Otherwise it outputs $(l+1)$-bit zeros (1-bit message and l-bit secret key). Since a classical channel cannot guarantee that the message will not be tapped, we use this query to model the process that A eavesdrops message and secret keys via a classical channel. The worst case is that A fully accesses the message and secret key, i.e., QRO directly returns b and k_b.

(2) Signing query $q_{\text{sign}}\{b\}$: Anyone can ask QRO for the quantum digital signature for b. QRO operates quantum one-way function to output key pairs $(k_b,|f_{k_b}\rangle)$. This query models the process that a signer (Alice) generates secret keys of classical bits and public keys of quantum states for every message bit b.

(3) Sending query $q_{\text{send}}\{b,k_b,|f_{k_b}\rangle,\text{Bob}\}$: To transfer a signature to Bob, Alice sends $q_{\text{send}}\{b,k_b,|f_{k_b}\rangle,\text{Bob}\}$ to QRO. QRO sends a secret key k_b and a public key $|f_{k_b}\rangle$ to Bob. In this query, a signer can choose a secret key and a public key to a recipient, which models an adversary's forgery attack. Besides, A might practically intercept the key pair, measure it, and resend the tampered keys to Bob. This scenario also changes the key pair and can be modeled by sending a query.

(4) Verifying query $q_{\text{verify}}\{k_b,|f_{k_b}\rangle\}$: Bob sends QRO the key pair $(k_b,|f_{k_b}\rangle)$ he received to verify the signature. If the pair is validated by quantum state measurement, QRO returns 1. Otherwise it returns 0. QRO records the verifier's identity and verification result. This query models the verifying phase that recipients compare the quantum states they received with the quantum states generated according to the secret key.

(5) Accepting query $q_{\text{acc}}\{\text{Bob}\}$: If the record value in verifying query is 1, i.e., the signature is valid, then QRO returns 1. Otherwise it returns 0. Through this query, Alice can make sure whether her signature is accepted and adversary A can figure out whether his attack is successful.

Different queries related to corresponding parts of QRO are shown in Fig. 1. Based on these specific queries, we present the execution of the QDS scheme [6].

(1) Alice sends a 1-bit message to QRO with $q_{\text{sign}}\{b\}$ query and gets the corresponding secret keys and public keys $(k_b,|f_{k_b}\rangle)$.

(2) Alice sends Bob the key pairs $(k_b,|f_{k_b}\rangle)$ by $q_{\text{send}}\{b,k_b,|f_{k_b}\rangle,\text{Bob}\}$.

(3) Bob makes a query, namely, $q_{\text{verify}}\{k_b,|f_{k_b}\rangle\}$, to verify the signature he received. Then QRO records the measurement result for the next accepting query.

C. Definition of security in the QRO model

Definition 6 (QCMA-secure). A quantum digital signature scheme $(\mathcal{G},\mathcal{S}\text{ign},\text{Verify})$ is existentially unforgeable under quantum chosen message attacks (QCMA-secure) if, for any efficient quantum algorithm F and any polynomial q (in the input of the quantum algorithm), F's probability of success in the following game is negligible:

Key generation. A challenger runs $k_b \leftarrow \mathcal{G}$, then operates $|f_{k_b}\rangle \leftarrow \mathrm{H}_\psi(m,k_b)$ to generate a public key of quantum states $|f_{k_b}\rangle$ and gives $|f_{k_b}\rangle$ to F.

Signing queries. An adversary makes a polynomial q chosen message queries. For each query, the challenger responds by signing each message in the query by mapping $\mathcal{X} \to \mathcal{Y}$,

$$O(m,k) : \sum_m \psi_m|m\rangle \to \sum_m \psi_m|m,k\rangle.$$

Forgeries. The adversary is required to produce $q+1$ message-signature pairs. The challenger then measures that all signatures are valid and all message-signature pairs are distinct. If so, the challenger reports that the adversary wins.

D. Proof of security in the QRO model

Theorem 1. Assume that an adversary A has algorithm F and queries QRO for the quantum state signature. A breaks the QCMA security if A inputs an inconsistent pair of secret key and public key that QRO cannot distinguish with non-negligible probability. Then a challenger takes advantage of A to clone quantum states. If quantum states cannot be cloned perfectly, then the signature is QCMA-secure in the quantum random oracle model.

Proof. We can use QRO to construct a signature on any given message b and output the signature $(k_b,|f_{k_b}\rangle)$. Then we prove that this QRO can respond to a classical chosen message attack when A is only given a polynomial number of signatures on random messages.

If A intends to forge a signature, A queries $q_{\text{message}}\{\text{Alice}\}$ to identify whether Alice has sent the message b to QRO. Then A gets the message and secret key (b,k_b). Through q times queries of $q_{\text{message}}\{\text{Alice}\}$, A gets q pairs of message and secret key (b^i,k_b^i), $1 < i < q$. A runs the algorithm F to produce a message b'. A queries $q_{\text{sign}}\{b'\}$ to get $q+1$ key pairs $(k_{b'},|f_{k_{b'}}\rangle)$. A sends the secret key of b and the public key of b' to Bob through the $q_{\text{send}}\{b',k_{b'},|f_{k_b}\rangle,\text{Bob}\}$ query. Then A sends the $q_{\text{verify}}\{k_{b'},|f_{k_b}\rangle\}$ query to figure out whether his attack is successful. If QRO outputs 1, A successfully makes a forgery attack with non-negligible probability ε. Therefore, a challenger could use $k_{b'}$ to clone quantum states $|f_{k_b}\rangle$ with probability ε, which violates quantum physical property.

Furthermore, if the adversary is armed with a quantum computer and issues quantum chosen message queries, each of the exponentially many messages in the query superposition are to be signed. Therefore, using the above technique directly would require an exponential number of random values for the quantum one-way function. To avoid needing exponential quantum states, we use the technique of small-range distributions and Lemma 1 to reduce the number of signed messages required to a polynomial. Let A be a quantum adversary breaking the QCMA security of the signature with non-negligible probability ε. The idea of security proof is a slight modification to Boneh's work [21] that the contradiction lies in violating a quantum physical property instead of the hash collision-resistance property. The security of the scheme is proved through a sequence of games in QRO.

TABLE I. Comparison among different random oracle (RO) models.

Comparison item	Model		
	RO	Quantum-accessible RO	Quantum RO
Model	Hash function	Hash function	Quantum one-way function
Assumption	PRF	QPRF	Collision-free measurement
Response to quantum query	No	Yes	Yes
Form of signature	Classical	Classical	Quantum
Reduction	PRF, etc.	Learning with errors, QPRF, etc.	No-cloning theorem

Game 0. A issues the $q_{\text{message}}\{\text{Alice}\}$ query and receives q pairs of message and secret key (b,k_b^i), $1 < i < q$. A is allowed to make a polynomial number of quantum chosen message queries. For query i, the challenger runs random generator $\mathcal{G}$ and responds to each message in the query superposition as follows:

(a) Let $k_b^i = \mathcal{G}^{(i)}(b)$.

(b) Operate the quantum one-way function $|f_{k_b^i}\rangle = H_\psi(k_b^i)$.

(c) Respond with the signature $(k_b^i,|f_{k_b^i}\rangle)$.

In the end, A must produce $q+1$ distinct pairs $(k_{b'}^i,|f_{k_b^i}\rangle)$ such that query $q_{\text{verify}}\{k_{b'}^i,|f_{k_b^i}\rangle\} = 1$ is verified. By definition, A wins with probability ε, which is non-negligible. Therefore, there is some polynomial $p = p(\lambda)$ such that $p(\lambda) > 1/\varepsilon(\lambda)$ for infinitely-many λ. Here λ is the input of $\mathcal{G}$.

Game 1. We modify the condition in which A wins by requiring that no two pairs $(k^i,|f_{k^i}\rangle)$ form a collision error for H in QRO. Then A succeeds in Game 1 with probability at least $\varepsilon - \text{negl}$.

Game 2. Let $\ell = 2C_0qp$, where C_0 is a constant from Lemma 1. At the beginning of the game, sample values $\hat{k}_j^{(i)}$ for $i = 1,\ldots,q$ and $j = 1,\ldots,\ell$, and let $|\hat{f}_{k_j^{(i)}}\rangle = H_\psi(\hat{k}_b^{(i)})$. Also pick q random functions O_i to map m to ℓ according to Property 1. Then let $k_m^{(i)} = \hat{k}_{O_i(m)}^{(i)}$ and $|f_{k_m^{(i)}}\rangle = |\hat{f}_{k_{O_i(m)}^{(i)}}\rangle$. The difference between Game 1 and Game 2 lies only in the generation of $k_m^{(i)}$ and $|f_{k_m^{(i)}}\rangle$ by q small-range distributions on ℓ samples. Each of the small-range distributions is only required once, so Lemma 1 implies that the success probability is still at least $\varepsilon - \text{negl} - 1/2p$.

If the adversary wins in Game 2, it produces two secret keys, k_b^* and $k_{b'}^*$, on the same public key $|f_{k_b^i}\rangle$. Then a challenger could produce the same quantum states with probability $\varepsilon - \text{negl} - 1/2p$. The quantum states produced by QRO are distinguishable, which implies that this quantity is negligible, thus $\varepsilon - 1/2p$ is negligible. Since $\varepsilon > 1/p$ infinitely often, and $1/2p < \text{negl}$ infinitely often, there exists a contradiction. So ε is negligible.

In this section, we formulate the message query, signing query, sending query, and verifying query, etc. These queries are used to model an adversary's possible attack such as eavesdropping, forgery attack, and intercept-resend attack. Then we give a general definition of QCMA security for the QDS scheme based on the quantum one-way function. Through a series of games, we prove that the QDS scheme is QCMA-secure even under the quantum chosen message attack by a reliable reduction to the no-cloning theorem.

E. Discussion

In the original security model [6], the QDS scheme is proved information-theoretically secure, which relies on a significantly large security parameter. An adversary may use a collision-type error to easily pass the verifying phase, while the original security model does not provide the related analysis. Apart from information-theoretically security, we can provide the provable security of quantum cryptographic protocols, especially the existential unforgeable security for a signature scheme. In the QRO model, we prove the QCMA security of a QDS scheme via a series of indistinguishability games, even if an adversary has quantum access to QRO. We use different queries to model different attack scenarios, including the collision case. The QRO model can be used to simplify quantum cryptographic protocols based on the quantum one-way function and test its security at every step. When QRO is instantiated, we can analyze special attack scenarios and define a similar security parameter to protect its security.

Furthermore, in contrast to the classical RO model, QRO is used to model quantum one-way function to analyze the provable security of the QDS scheme. Considering the vaguely defined and not yet implemented quantum hash [25], we select a broader concept, namely, quantum one-way function, to be the modeling object. In the QRO model, the collision-free measurement assumption replaces the computational hardness assumption of the pseudorandom function (PRF) in the RO model. A new function is added to QRO such that it can not only respond to quantum state queries, but output signatures of quantum states. Unlike the prior quantum-accessible random oracle model [18], which relies on classical hard problems such as the learning with errors problem and the assumption of QPRF against quantum adversaries, we use the no-cloning theorem as a hard problem for reduction. In addition, we use queries to QRO to model an adversary's capability. The comparison among different RO models is summarized in Table I.

V. CONCLUSION

To analyze the provable security of quantum cryptographic protocols based on the quantum one-way function, we have

provided a QRO model and the framework of a security analysis procedure. A QDS scheme is proved QCMA-secure through a sufficiently reliable reduction to the no-cloning theorem. Of course, queries to the QRO model still need to be standardized and extended for more quantum cryptographic protocols.

ACKNOWLEDGMENTS

This project was supported by the National Natural Science Foundation of China (No. 61571024 and No. 61272501) and the National Basic Research Program of China (No. 2012CB315905).

[1] C. M. Swanson and D. R. Stinson, in *International Conference on Information Theoretic Security* (Springer, Berlin, 2011), p. 100.
[2] R. Amiri and E. Andersson, Entropy **17**, 5635 (2015).
[3] J. M. Arrazola, P. Wallden, and E. Andersson, Quantum Inf. Comput. **6**, 0435 (2016).
[4] H.-L. Yin, Y. Fu, and Z.-B. Chen, Phys. Rev. A **93**, 032316 (2016).
[5] H.-L. Yin, Y. Fu, H. Liu, Q.-J. Tang, J. Wang, L.-X. You, W.-J. Zhang, S.-J. Chen, Z. Wang, Q. Zhang *et al.*, arXiv:1608.01086.
[6] D. Gottesman and I. Chuang, arXiv:quant-ph/0105032.
[7] L. Lamport, *Constructing digital signatures from a one-way function* (Technical Report CSL-98 (SRI International, Palo Alto, CA, 1979).
[8] P. J. Clarke, R. J. Collins, V. Dunjko, E. Andersson, J. Jeffers, and G. S. Buller, Nat. Commun. **3**, 1174 (2012).
[9] V. Dunjko, P. Wallden, and E. Andersson, Phys. Rev. Lett. **112**, 040502 (2014).
[10] R. J. Collins, R. J. Donaldson, V. Dunjko, P. Wallden, P. J. Clarke, E. Andersson, J. Jeffers, and G. S. Buller, Phys. Rev. Lett. **113**, 040502 (2014).
[11] G. M. Nikolopoulos, Phys. Rev. A **77**, 032348 (2008).
[12] U. Seyfarth, G. M. Nikolopoulos, and G. Alber, Phys. Rev. A **85**, 022342 (2012).
[13] M. Bellare and P. Rogaway, in *Proceedings of the 1st ACM Conference on Computer and Communications Security* (ACM, Fairfax, VA, 1993), p. 62.
[14] M. Bellare and P. Rogaway, in *Advances in Cryptology—Eurocrypt'96* (Springer, Saragossa, Spain, 1996), p. 399.
[15] D. Pointcheval and J. Stern, in *Advances in Cryptology-EUROCRYPT'96* (Springer, Saragossa, Spain, 1996), p. 387.
[16] R. Canetti, S. Halevi, and J. Katz, in *Advances in Cryptology-Eurocrypt 2004* (Springer, Interlaken, Switzerland, 2004), p. 207.
[17] E. Bresson, O. Chevassut, D. Pointcheval, and J.-J. Quisquater, in *Proceedings of the 8th ACM Conference on Computer and Communications Security* (ACM, Philadelphia, PA, 2001), p. 255.
[18] D. Boneh, Ö. Dagdelen, M. Fischlin, A. Lehmann, C. Schaffner, and M. Zhandry, in *Advances in Cryptology—ASIACRYPT 2011* (Springer, Kaoshiung, Taiwan, 2011), p. 41.
[19] M. Zhandry, in *2012 IEEE 53rd Annual Symposium on Foundations of Computer Science* (IEEE, Washington, DC, 2012), p. 679.
[20] M. Zhandry, Int. J. Quantum. Inform. **13**, 1550014 (2015).
[21] D. Boneh and M. Zhandry, in *Advances in Cryptology—CRYPTO 2013* (Springer, Santa Barbara, CA, 2013), p. 361.
[22] N. Koblitz and A. J. Menezes, Design Code Cryptogr. **77**, 587 (2015).
[23] T. Hwang, K.-C. Lee, and C.-M. Li, IEEE T. Depend. Secure. **4**, 71 (2007).
[24] D. Pointcheval and J. Stern, in *Advances in Cryptology—ASIACRYPT'96* (Springer, Kyongju, Korea, 1996), p. 252.
[25] F. Ablayev and A. Vasiliev, Laser Phys. Lett. **11**, 025202 (2013).