Quantum random oracle model for quantum digital signature

(Extended Abstract for QCrypt 2017)

Tao Shang, Qi Lei, Jianwei Liu
School of Electronic and Information Engineering, Beihang University
Beijing 100191, China

Abstract

Security analysis of quantum cryptographic protocols is mostly presented with situational quantum attacks and still lacks general analysis methods. As an effective analysis tool in classical cryptography, the random oracle (RO) model has been used to design cryptographic protocols and give rigorous proofs of security over 20 years. In this work, with reference to the classical RO model, we 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. This work is presented in detail in [1].

I. Motivation

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. Over a decade, the slowpacing of experimental realization [2], [3], [4] hampered the progress of QDS and other quantum protocols. Alternatively, we consider to 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 [5], [3], [6] and quantum public-key encryption schemes [7], [8].

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 [2], [4]. In classical cryptography, similar efficient analysis model named random oracle (RO) was introduced in 1993 [9]. 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 adversarys attack power [10]. 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.

On the other hand, the rapidly evolving quantum computation equips a quantum adversary with sufficient computational power. To analyze classical cryptographic protocols against quantum adversaries, Boneh et al. [11] started pioneering work on the quantum-accessible random oracle model, in which an adversary can make quantum superposition queries, i.e., an exponential number of queries in superposition states. Till now, most of the quantum-accessible random oracle model research [12], [13], [14] has focused on classical cryptographic protocols against quantum adversaries. Furthermore, can we explore the construction of a new QRO (quantum random oracle) model to effectively analyze quantum cryptographic protocols against quantum attacks? So our work focus the construction of a QRO model to analyze the security of QDS schemes based on quantum one-way function.

II. Our contribution

(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.

(2) *A quantum digital signature scheme is proved QCMA (quantum chosen message attack)-secure in this quantum random oracle model.* To model an adversarys attacks such as eavesdropping and forgery attack, specific queries to QRO are described.

III. Main ideas

Proving security in the QRO model presents two main challenges, including the basic parts and functions of QRO and the analysis procedure in QRO model.

A. Quantum random oracle model

Considering the possible quantum collision problem, i.e., different quantum states pass the test of equality by 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 [14]. We also assume that quantum states are transmitted without interference. Therefore, we definite QRO as follows:

Definition 1: A quantum random oracle is an efficient algorithm $(\mathcal{G}, H_q, Measure)$ 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

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

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 $i \neq j$.

The definition indicates that this quantum random oracle can accurately match classical secret keys with corresponding quantum public keys.

B. Security analysis procedure in the QRO model

According to the methodology of the RO model, the QRO model for quantum cryptographic protocols can also conform to the analysis procedure of RO model. For each step of this analysis procedure, we need to further explore the following four problems.

(1) What is a feasible hard problem Π in the QRO model? For quantum cryptographic protocols, we can choose no-cloning theorem, one of the foundations of quantum cryptography, to be the hard problem Π for an absolutely secure reduction.

(2) How to redescribe a protocol for Π? Redescribing a protocol means to formally define the parameters for the protocol and the queries for modeling an adversary's capability. For QDS, we formulate Message query $q_{message}\{Alice\}$, Signing query $q_{sign}\{b\}$, Sending query $q_{send}\{b, k_b, |f_{k_b}\rangle\, , Bob\}$, Verifying query

$q_{verify}\{k_b, |f_{k_b}\rangle\}$ and Accepting query $q_{acc}\{Bob\}$ to present the execution of the QDS scheme [5]. Through these queries, we can model an adversarys possible attack such as eavesdropping, forgery attack, and intercept-resend attack.

(3) What is the specific security for quantum cryptographic protocols? For security definition of signature scheme, existential forgery under chosen message attack is always considered [14], [15]. Chosen message attack means that an adversary cannot produce $q+1$ valid message-signature pairs with q chosen message queries. We define existentially unforgeable under quantum chosen message attacks (QCMA-secure) for QDS schemes based on the quantum one-way function.

(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 adversarys capability to solve the hard problem Π by controlling the RO and providing indistinguishable output. In the quantum-accessible random oracle model, the difficult point for reduction lies in the fact that the reduction algorithm must evaluate RO at all points in the superposition. Zhandry [12] 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. Combine this technique with 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. Detailed security proof is elaborated in [1].

IV. Importance

To analyze the provable security of quantum cryptographic protocols based on quantum one-way function, we provided a new QRO model and a framework of security analysis procedure. The QRO model can be used to simplify quantum cryptographic protocols based on the quantum oneway function and test its security at every step. 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. It is very meaningful to endow new meaning and explanation to the QRO model for quantum cryptosystems. Of course, queries to the QRO model still need to be standardized and extended for more quantum cryptographic protocols.

References

[1] T. Shang, Q. Lei, and J.-W. Liu, “Quantum random oracle model for quantum digital signature,” *Phys. Rev. A*, vol. 94, no. 4, p. 042314, 2016.

[2] P. J. Clarke, R. J. Collins, V. Dunjko, E. Andersson, J. Jeffers, and G. S. Buller, “Experimental demonstration of quantum digital signatures using phase-encoded coherent states of light,” *Nat. Commun.*, vol. 3, p. 1174, 2012.

[3] V. Dunjko, P. Wallden, and E. Andersson, “Quantum digital signatures without quantum memory,” *Phys. Rev. Lett.*, vol. 112, no. 4, p. 040502, 2014.

[4] R. J. Collins, R. J. Donaldson, V. Dunjko, P. Wallden, P. J. Clarke, E. Andersson, J. Jeffers, and G. S. Buller, “Realization of quantum digital signatures without the requirement of quantum memory,” *Phys. Rev. Lett.*, vol. 113, no. 4, p. 040502, 2014.

[5] D. Gottesman and I. Chuang, “Quantum digital signatures,” *arXiv:quant-ph/0105032*, 2001.

[6] H.-L. Yin, Y. Fu, and Z.-B. Chen, “Practical quantum digital signature,” *Phys. Rev. A*, vol. 93, no. 3, p. 032316, 2016.

[7] G. M. Nikolopoulos, “Applications of single-qubit rotations in quantum public-key cryptography,” *Phys. Rev. A*, vol. 77, no. 3, p. 032348, 2008.

[8] U. Seyfarth, G. Nikolopoulos, and G. Alber, “Symmetries and security of a quantum-public-key encryption based on single-qubit rotations,” *Phys. Rev. A*, vol. 85, no. 2, p. 022342, 2012.

[9] M. Bellare and P. Rogaway, “Random oracles are practical: A paradigm for designing efficient protocols,” in *Proceedings of the 1st ACM conference on Computer and communications security*. ACM, Fairfax, VA, 1993, p. 62.

[10] E. Bresson, O. Chevassut, D. Pointcheval, and J.-J. Quisquater, “Provably authenticated group diffie-hellman key exchange,” in *Proceedings of the 8th ACM conference on Computer and Communications Security*. ACM, Philadelphia, PA, 2001, p. 255.

[11] D. Boneh, Ö. Dagdelen, M. Fischlin, A. Lehmann, C. Schaffner, and M. Zhandry, “Random oracles in a quantum world,” in *Advances in Cryptology–ASIACRYPT 2011*. Springer, Kaoshiung/Taiwan, 2011, p. 41.

[12] M. Zhandry, “How to construct quantum random functions,” in *2012 IEEE 53rd Annual Symposium on Foundations of Computer Science*. IEEE, Washington, DC, 2012, p. 679.

[13] ——, “Secure identity-based encryption in the quantum random oracle model,” *Int. J. Quantum Inf.*, vol. 13, no. 04, p. 1550014, 2015.

[14] D. Boneh and M. Zhandry, “Secure signatures and chosen ciphertext security in a quantum computing world,” in *Advances in Cryptology–CRYPTO 2013*. Springer, Santa Barbara, CA, 2013, p. 361.

[15] D. Pointcheval and J. Stern, “Provably secure blind signature schemes,” in *Advances in CryptologyłASIACRYPT’96*. Springer, Kyongju/Korea, 1996, p. 252.