A Security Proof of FO-PKC in the Quantum Random Oracle Model

2310126 Naoki Hasegawa

In recent years, expectations for the realization of quantum computers have increased, and the research on post-quantum cryptography (PQC) has become active. Accordingly, the National Institute of Standards and Technology (NIST) has been working on a standardization project for post-quantum cryptography. Cryptographic schemes utilizing hash functions have traditionally been studied and developed with a focus on their security in the Random Oracle Model (ROM), which considers only classical algorithms. However, in the post-quantum cryptography, it is common to use the Quantum Random Oracle Model (QROM), which accounts for quantum algorithms that allow superposition queries to the random oracle. The security evaluation of cryptographic schemes in the QROM is an important topic, as the understanding of security in this model remains incomplete.

The Fujisaki-Okamoto (FO) transformation is a generic method for converting any weak public-key encryption scheme into an IND-CCA secure public-key encryption scheme in the random oracle model. There are two versions of the FO transformation: the PKC version and the CRYPTO version. While the FO transformation has been extensively studied in the classical Random Oracle Model, it is not yet fully understood whether similar results hold in the QROM. In the QROM, the security of the FO transformation has been established through security proofs in the CRYPTO version and its improved version. However, the security proof for the PKC version has not yet been completed.

The reserch in the QROM, properties that could be applied in ROM cannot be used without proof in QROM. Therefore, a key challenge is to prove whether the same theorems and properties as in ROM can be applied or to devise alternative approaches. In the QROM, the challenge was to record queries to the random oracle, which can be done trivially in the classical model. However, Zhandry developed in the compressed oracle technique, which can record queries on the oracle side in the QROM.

Subsequently, Don et al. showed that an upper bound on the computational error when exchanging the order of a unitary operator and a measurement operator within the compressed oracle. This bound, known as the commutator bound, showed that in the QROM, the order of computations in algorithms can be interchanged within a statistical error margin.

From these results, Don et al. constructed a simulator capable of extracting the content of an adversary's queries to the QROM without the adversary being aware of it and before all queries are completed. Applying this simulator, they provided a security proof for the CRYPTO version of the FO

transformation, which converts a PKE with one-way security against CPA attacks (OW-CPA) into a KEM with indistinguishability security against CCA attacks (IND-CCA).

However, to the best of our knowledge, there is no existing security proof for the FO transformation in the PKC version, which converts a PKE with indistinguishability security against CPA attacks (IND-CPA) into a PKE with IND-CCA security.

In this paper, we provide a security proof for the FO-PKC version in the Quantum Random Oracle Model, referencing the proof techniques used by Don et al.

The key point of this proof lies in the differences between proofs in the ROM and QROM. In the QROM proof, the order of the steps differs from that in the ROM proof.

In the ROM, where inputs and outputs are classical bits, it is straightforward to record the access to the random oracle and extract its contents. As a result, after providing the adversary with the challenge ciphertext c^*, the decryption oracle can be replaced with one that extracts results by referencing the random oracle access. This operation allows the implementation of a decryption oracle that does not require the secret key. Subsequently, the proof is completed by bounding the differences introduced by this replacement using the OW-Game.

On the other hand, in the QROM, where superposition inputs are allowed, recording and extracting query contents requires the use of a compressed oracle. This necessitates a method for replacing the compressed oracle.

In both classical and quantum proofs, the challenge ciphertext c^* is generated during the initial setup of the game. At this point, the random oracle H is accessed, and its output is used to encrypt c^*. In the classical proof, the simulation of the decryption oracle is performed first. To follow the same order in the quantum proof, H must be replaced with a compressed oracle. However, the compressed oracle must be implemented independently of the challenge ciphertext c^*. Therefore, it is not possible to conduct the quantum proof in the same order as the classical proof.

To resolve this issue, the quantum proof replaces H with a different random oracle H'. The differences introduced by this replacement can be bounded using the O2H lemma. Subsequently, this replaced H is further replaced with a compressed oracle, enabling the challenge ciphertext c^* and the compressed oracle to be treated independently. This replacement allows query recording and extraction, eliminating the need for the secret key, thereby completing the proof.Abstract of this paper

Future work in this study includes improvements to One Way to Hiding Lemma (O2H) and to the commutator bound. In the current proof method,

the application of O2H bounds the probability using a square root of the probability. In the classical model, the probability is bounded by the probability without the square root, so if the probability can be bounded by the probability without or close to the square root in the quantum case using some method, better security evaluation results can be obtained.

Additionally, in this proof, the order of the algorithms in the simulator is interchanged, and the error term is generated by the number of such swaps and the commutator bound. Therefore, if the commutator bound can be bounded to a smaller upper bound or the number of exchanging can be reduced to a smaller number, the error term will be smaller, and leading to improved results.