Abstract

In recent years, there has been a lot of research on quantum computers. If a large-scale and error-correcting quantum computer is realized, many of the popular cryptosystems, such as RSA and elliptic curve cryptography, will be compromised. Therefore, it is important to consider quantum computers in cryptography.

In cryptography, the random oracle model is an idealized version of the cryptographic hash function, and is widely used to discuss the security of cryptographic schemes. In 2011, Boneh et al. proposed the quantum random oracle model, which is a quantum version of the random oracle model. The two differ in many points due to their quantum property. One of these is random oracle can easily record queries, whereas quantum random oracle are difficult to record queries. To address this problem, Zhandry proposed a way for quantum random oracle to record queries at CRYPTO 2019.

Zhandry introduces applications of quantum random oracle that can record queries, one of which is a proof of the optimality of Grover's algorithm. In this paper, we show that Zhandry's proof is simpler and easier to verify by transforming the oracle basis into a Fourier basis.