A Improvement of Classical Homomorphic Encryption for Quantum Circuits

2210052 Kousei Kawano

Fully Homomorphic Encryption (FHE) is a cryptographic scheme that allows arbitrary computations to be performed directly on encrypted data without decryption. The concept of FHE was first proposed by Rivest, Adleman, and Dertouzos in 1978; however, achieving fully homomorphic encryption that supports both multiplication and addition remained an open problem for many years. This problem was first solved in 2009 when Gentry introduced the concept of bootstrapping. However, bootstrapping is computationally expensive, and various improvements have been proposed to enhance its efficiency, such as the GSW scheme and the TFHE scheme, which enables even faster homomorphic computations. Moreover, research has been conducted to extend the framework of FHE to quantum computing, leading to the development of Quantum Fully Homomorphic Encryption (QFHE). Quantum computers are not only expensive but also require advanced expertise for operation and maintenance. As quantum computing technology advances, it is expected that enterprises and individuals will increasingly outsource quantum computations to external quantum computing services. However, outsourcing quantum computations poses a significant privacy risk, as users' confidential data may be exposed to the service provider. As a solution to this issue, QFHE is a promising technology that enables secure quantum computation while preserving data confidentiality, making it highly valuable from the perspective of security and privacy in quantum computing services. A major limitation of conventional QFHE schemes is that the evaluation key is a quantum state, requiring the client to have access to quantum computing resources. To address this limitation, Mahadev (FOCS 2018) proposed a protocol that allows a classical client to delegate encrypted quantum computations to a quantum server via a classical communication channel. This protocol achieves secure delegated quantum computation by utilizing classical fully homomorphic encryption (FHE) to handle Clifford gates and the non-Clifford Toffoli gate. Since Clifford and Toffoli gates together form a universal gate set, this protocol allows a classical client to securely delegate arbitrary quantum computations to a quantum server. However, Mahadev's protocol has certain limitations. Specifically, in the homomorphic evaluation of non-Clifford gates, it requires the encryption and homomorphic computation of classical FHE to be performed on a quantum computer, making it inefficient. Additionally, the protocol remains within the framework of quantum leveled FHE, imposing restrictions on the number of computations. In this study,

we aim to enhance the efficiency of Mahadev's protocol by introducing two key modifications. First, we demonstrate that the Toffoli gate used in Mahadev's protocol can be replaced with the simpler non-Clifford gate, the T gate. This modification reduces the number of homomorphic computations required for the non-Clifford gate evaluation from three to one. Second, we propose replacing the classical FHE scheme used in Mahadev's protocol with an alternative scheme to improve computational efficiency. These modifications enable the extension of quantum leveled FHE to QFHE, eliminating the need for cryptographic transformations that were previously essential in existing approaches.