Quantum resistant Reed Muller codes on McEliece cryptosystem

Jasmine Elder

Preprint no. 2020-01

Abstract

Cryptography is the science of converting a plaintext, or message into a ciphertext, or scrambled message in order to provide secrecy. With the development of quantum computers on the horizon, it poses a threat to the security of the current cryptosystems that are in place. Quantum computers are able to process complex algorithms and perform advance calculations like integer factorization and discrete logarithm problem that are expected to break all the current cryptosystems. Recently, Dr. Wang presented a new post quantum encryption scheme, Random Linear Code-Based Encryption scheme, RLCE, which is a variant to the McEliece encryption scheme. It is already well-known that the McEliece Encryption scheme with Reed Muller codes is not considered as a secure system for both classical and quantum computers. In this dissertation, we introduce and study the Reed-Muller code-based RLCE scheme. These successful attacks on the Reed Muller code based McEliece encryption scheme, namely, the Minder-Shokrollahis attack, the Chizhov-Borodins attack, and the Square Code attack, are proven to unsuccessful for the proposed Reed Muller code-based RLCE scheme. We determine the optimal method in preventing these known attacks against the new encryption scheme. We suggest parameters needed for the 128, 192, and 256 bits security level.

Department of Mathematics, UNC Charlotte, Charlotte, NC 28223