An Implementation of McEliece Public Key Cryptosystems for Post-Quantum Cryptography Using AG Codes and Analysis

Andres Arroyo, University ofPuerto Rico-Rio Piedras

Current public key cryptography standards recommended by the National Institute of Standards and Technology (NIST) and heavily used in commerce, such as: RSA and several Elliptic Curve Cryptosystems rely on the fact that the problem of factorizing and finding discrete logarithm are hard. However, in 1994, an algorithm was developed that can factor numbers using a quantum computer fast, rendering these cryptosystems non-viable. One of the cryptosystems that is highly promising in the Post-Quantum world, is the McEliece public-key cryptosystem, based on the theory of error-correcting codes. The system uses the generator matrix of an error correcting code with good rate, error correction capability, and a fast decoding algorithm to encrypt and decrypt data. The original system uses a class of codes known as Goppa Codes, with a large number of inequivalent systems, and a good decoding algorithm with complexity O(n log n). Becuase the problem of decoding a general linear code is known to be NP-Complete, and brute force attacks have been show to have a large work factor, these public key cryptosystems are so far regarded as safe, even from attack by quantum computers. In this project, we implement the McEliece Cryptosystem using different families of Algebraic Geometry (AG) codes, and we compare and analyze the resulting encryption/decryption methods, their running times and their parameters.