Post-Quantum Code-Based Cryptography Simulator

Lior Ovadia*

March 2025

Code-based cryptography is the area of research that focuses on the study of cryptosystems based on error-correcting codes.

This idea of code-based cryptography was introduced by Robert McEliece in 1978. He began with a specific error-correcting code, the binary Goppa code, and used an invertible linear transformation to jumble it. On a very fundamental level, McEliece's approach equates to a secret factorization, which is somewhat similar to the Rivest Shamir and Adleman public key cryptosystem, known as RSA. Only the owner is aware of the factorization of the public key, which is the result of the Goppa code and the linear transformation.

In code-based cryptography, the public key is a randomly generating matrix of an arbitrarily permuted version of the private key. The sender purposefully introduces errors to the ciphertext (i.e., the codeword) to make decoding (and subsequently decryption) challenging. The recipient of the ciphertext, who is the owner of the private key, can correct the errors, but an attacker without access to the secret knowledge cannot.

In contrast to RSA and other well-known public key systems, McEliece's method appears to be quantum-resistant, which has rekindled interest in it. We shall also examine a variation of McEliece's method, invented by Niederreiter, that is based on scrambling the parity-check matrix rather than the generator matrix. In this case the ciphertext is a syndrome rather than a codeword. The McEliece technique was relegated to the back of the line for designers. Due to the fact that McEliece's approach required significantly larger public keys than other methods, like RSA, it did not generate much interest at the time. However, as the era of quantum computers approaches, it is being given another look because it appears to be impervious to attacks utilizing Shor's method.

In this project we intend to build and run a simulator for new methods for code-base cryptography, selecting different codes (either block or convolutional) with different code parameters, and testing their performance in terms of both resistance to cryptanalysis and computational complexity.

*MSc project under the supervision of Prof. Meir Ariel