Secure and Efficient Solutions for Post-Quantum Cryptography from Codes with Compact Representations

Challenge:

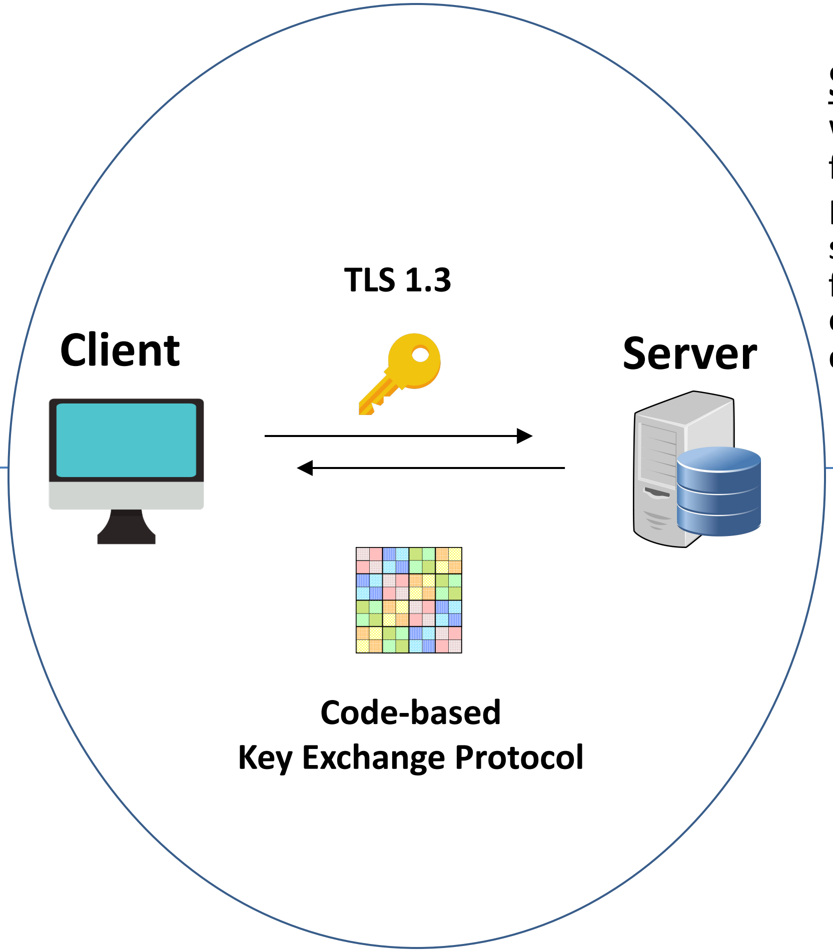
Code-based cryptography is one of the main candidates for security in the quantum era.

Our goal is to create efficient, long-term secure primitives from code-based cryptography, in the context of encryption and key establishment.

Solution:

We will use *reproducible codes* to obtain compact key sizes. To achieve misuse resistance, we will design a Key Encapsulation Mechanism with only *negligible decoding failure rate*.

Our scheme will be implemented in *constant time* to defeat side-channel attacks.



TLS 1.3

Client

Server

Code-based
Key Exchange Protocol

Scientific Impact:

We obtain highest security level for public-key crypto (IND-CCA).

Implementation resistant to side-channel attacks. Candidate for public-key encryption/key exchange standard for years to come.

Broader Impact:

Our project supports NIST's Post-Quantum Standardization effort, augmenting the U.S. and Israeli footprint in the process, and laying the foundation for the cryptographic solutions of the future.

Disseminate knowledge about post-quantum cryptography to a wide and diverse audience worldwide via meetings and seminars.