Consider that a client would like to a server to do some computations for him but he does not want to give information meaningful information to the server. The client therefore sends encrypted messages $c_1 = \text{Enc}(pk, m_1)$ and $c_2 = \text{Enc}(pk, m_2)$ to the server and the client would like to obtain some function $f$ of the two plaintexts $f(m_1, m_2)$. It suffices for the client to get $\text{Enc}(pk, f(m_1, m_2))$ because the client owns the secret key $sk$. He is able to use the decryption function $\text{Dec}$ on the ciphertext and gets $\text{Dec}(sk, \text{Enc}(pk, f(m_1, m_2))) = f(m_1, m_2)$.

The goal of this internship is to analyze schemes that achieve this property based on code-based cryptography.

**Prerequisites**

- linear algebra
- coding theory
- basic understanding of cryptography

**Advisors**

Georg Maringer