Associate Professorship of Coding and Cryptography
TUM Department of Electrical and Computer Engineering
Technical University of Munich

Forschungspraxis, Master's Thesis

Homomorphic encryption

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 c1 = Enc(pk, m1) and c2 = Enc(pk, m2) to the server and the client would like to obtain some function f of the two plaintexts f(m1,m2). It suffices for the client to get Enc(pk, f(m1,m2)) because the client owns the secret key sk. He is able to use the decryption function Dec on the ciphertext and gets Dec(sk, Enc(pk,f(m1,m2=))) = f(m1,m2).

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