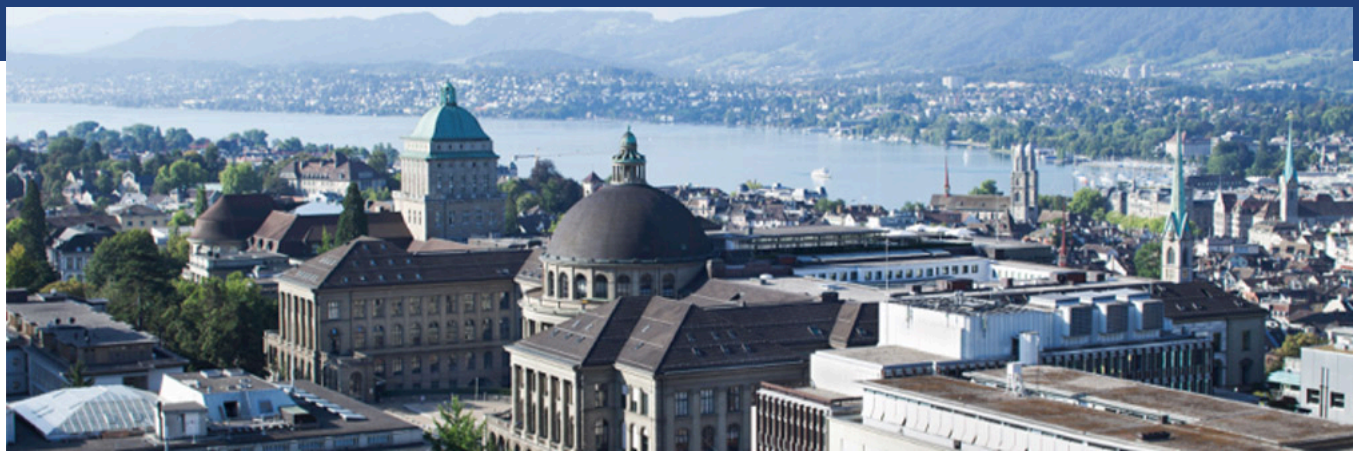
ETH zürich

RESEARCH GROUP FOR
Distributed Systems



Making Fully Homomorphic Encryption Accessible

Cloud-computing has become ubiquitous, providing the backbone for most modern consumer applications on the internet and mobile devices. However, it also exposes user data to privacy risks, including misuse by companies or third parties (e.g. data breaches). Therefore, we want to protect data by encrypting it before it leaves the device. However, traditional encryption would make most cloud-based applications impossible as the server could not perform computations on the data.

Fully Homomorphic Encryption is a powerful encryption scheme where one can perform computations on the ciphertexts that correspond to computations on the underlying plaintexts. With this, it is possible to outsource computations to the cloud without compromising user privacy. However, fully homomorphic encryption is a recent technology and still requires expert knowledge to use successfully.

As a first step towards making FHE more accessible, we developed the Marble C++ framework. This framework allows developers to quickly evaluate whether applying FHE is feasible for their application scenario. This is done by writing a (plaintext) version of the core logic against Marble's interfaces, which emulate standard C++ data types. Marble can then analyse and evaluate the code automatically, reporting on the complexity of the code and showing developers the overheads they can expect.

We want to extend Marble with more advanced features and empirically evaluate its usability with a user study. Depending on your interests, you could focus on the systems, crypto or UX aspects of this project or combine them individually.

Requirements: Students should be highly motivated, interested in working on state-of-the-art research topics, with a solid background in general computer science and have some familiarity with cryptography and security. Previous experience with FHE (or general lattice cryptography) is welcome but not required.

This project is ideally suited for a MSc thesis or master-level group (lab) project, however it can also be adapted to a BSc thesis for interested bachelor students with the required background.

github.com/MarbleHE →

Distributed Systems Group

ETH Zürich
Alexander Viand
CNB H 106
Universitätstrasse 6
8092 Zürich

Tel: +41 44 632 02 73
alexander.viand@inf.ethz.ch
people.inf.ethz.ch/vianda/ →