DEPARTMENT OF ELECTRICAL AND INFORMATION TECHNOLOGY | LUND UNIVERSITY

**MASTER'S THESIS** XZDDF Bootstrapping in Fully Homomorphic Encryption
**STUDENT** Simon Ljungbeck
**SUPERVISOR** Qian Guo
**EXAMINER** Thomas Johansson

# Using XZDDF Bootstrapping to Speed up Fully Homomorphic Encryption

POPULAR SCIENCE ARTICLE **Simon Ljungbeck**

Fully Homomorphic Encryption (FHE) can be used when delegating computations to third parties. However, current FHE schemes tend to be slow. In this project, a new algorithm, with the potential to speed up FHE, has been investigated.

To perform computations on encrypted data, one normally needs to decrypt it first. However, a few years ago, a new type of encryption schemes was discovered, allowing computations on encrypted data directly. This kind of encryption is called Fully Homomorphic Encryption (FHE) and basically means that any function evaluation can be made without revealing the input to the function.

Fully homomorphic encryption has many interesting applications, especially when third parties are given data to do computations on. One example is when training a machine learning model in the cloud. Normally, the cloud service then gets access to the training data, violating the privacy of it. However, if using fully homomorphic encryption, one can upload the training data in an encrypted form and train the model homomorphically. The resulting model is the same, but the privacy of the training data and the model parameters is kept.

Although theoretically appealing, in practice, all existing FHE schemes are too slow. Most FHE schemes are noise-based, meaning that each ciphertext contains some noise. When performing computations homomorphically, this noise grows until a point is reached where the decryption will fail. The ciphertext needs to be refreshed before this bound is exceeded, and it is this reduction of noise that usually is the reason why fully homomorphic encryption is relatively slow.

One common way to reduce the noise, which is both simple and elegant, is the so-called bootstrapping technique. The algorithm first encrypts the ciphertext to a new ciphertext, and then exploits the homomorphic property of the encryption scheme, decrypting the first-layer ciphertext homomorphically. In this way, it is as if a new encryption, of the same message, was just computed so that the noise is reset. See Figure 1 for an illustration of this.

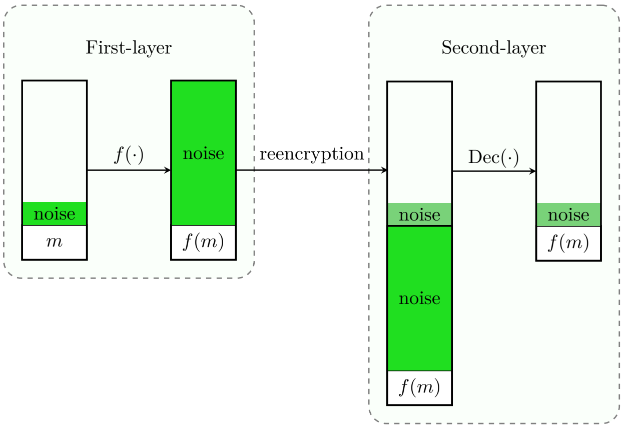

Figure 1: Illustration showing how bootstrapping works.

Since bootstrapping is the main bottleneck in FHE schemes, a lot of research is going on about the topic. In this project, a new way of doing bootstrapping was studied. The new algorithm, called XZDDF, was first analyzed and then implemented in an open-source library for fully homomorphic encryption. Theoretically, the time complexity of the algorithm is lower than for previous algorithms, but the execution time of the implementation was about the same as for conventional bootstrapping.