Fully Homomorphic Encryption

M.L. de Groot
6103677

October 20, 2014

Introduction

A homomorphic encryption scheme allows specific types of computations to be carried out on ciphertext and generate an encrypted result which, when decrypted, matches the result of operations performed on the plaintext. In other words, the scheme encrypts data in such a way that computations can be performed on the encrypted data without knowing the secret key. This way you can delegate the processing of your data, without giving away access to it.

To illustrate the idea, two operations - addition and multiplication - are shown by the following equations when the messages consist of bits:

$$Enc(b_1) + Enc(b_2) = Enc(b_1 + b_2 \mod 2)$$

$$Enc(b_1) \cdot Enc(b_2) = Enc(b_1 \cdot b_2 \mod 2)$$

Ideally all operations are possible to apply, rendering a large and varied set of possible computations on encrypted data. As it turns out, 'only' addition and multiplication are needed to support all operations. When the scheme allows for homomorphism under both of these operations, the scheme is said to be **fully homomorphic**. Unfortunately this is very hard to achieve, usually schemes allow either addition or multiplication, but not both.

Applications

By allowing to perform arithmetic operations over encrypted bits, you can do computations on the ciphertext without decrypting it. This enhances security measures and, among many other applications, can be used for:

- Cloud computing
- Searching through encrypted data
- Private queries in a search engine
- Secure multi-party computation

The Catch

A great drawback of homomorphic schemes is the security: knowing of this property might expose structural information. For example, for an attack, the multiplication of two signatures yields a valid signature of the product of the two corresponding messages.

Furthermore, these schemes are very hard to design. Eventhough the concept was introduced in 1978 by Rivest, it was not until 2009 that the first fully homomorphic encryption (FHE) was designed by Craig Gentry.

References

- Craig Gentry, *Fully homomorphic encryption using ideal lattices*, Symposium on the Theory of Computing (STOC), 2009, pp. 169-178. `http://crypto.stanford.edu/craig/`
- Marten van Dijk, Craig Gentry, Shai Halevi and Vinod Vaikuntanathan, *Fully Homomorphic Encryption over the Integers*, Cryptology ePrint Archive, Report 2009/616. `http://eprint.iacr.org/2009/616.pdf`
- Jaydip Sen, *Homomorphic Encryption: Theory & Application* `http://arxiv.org/pdf/1305.5886.pdf`
- Shai Halevi, *Tutorial on Homomorphic Encryption by Shai Halevi*, Introductionairy lecture on YouTube.