Dissertação de Mestrado em Engenharia Informática (2017/2018)

Title : Homomorphic Encryption

Supervisor: Prof. Paul Crocker

Co-Supervisor Prof. Dr. Celino Miguel (Dep. Matemática)

Email: crocker@di.ubi.pt

Description

In the paper Fully Homomorphic Encryption over the Integers by Dijk et al. a somewhat homomorphic scheme is detailed and explained how the scheme may be turned into a fully homomorphic scheme. The scheme is a simple scheme based only on the integers and its security property on the hardness of the approximate GCD problem, see [1]. An interesting question is to how use the same ideas but over different algebraic structures, such as polynomials rings as in [2]. Other possibility exists and the main focus of this dissertation will be to explore the use of other structures, in particular which structures can and cannot be used and what are the computational implications.

Work Plan

1 Literature and State of the Art Review
2 Study of the characteristics, algorithms and architectures to be used.
3 Implementation, Testing and Evaluation of the proposed solution
4 Publication of the results
5 Writing of the Dissertation.

References

[1]. van Dijk, C. Gentry, S. Halevi, V. Vaikuntanathan Fully homomorphic encryption over the integers Advances in Cryptology-EUROCRYPT 2010, Springer (2010), pp. 24-43 https://eprint.iacr.org/2009/616.pdf

[2] Design of a polynomial ring based symmetric homomorphic encryption scheme Smaranika Dasgupta and .S.K.Pal Perspectives in ScienceVolume 8, September 2016, Pages 692-695 http://www.sciencedirect.com/science/article/pii/S2213020916302002