Security

One page description

Final Year

Alexandru Sulea
D Stream
#12315152
N April 2017

Contents

List of Tables

1 Overview

The most interesting security aspect I found was the concept of homomorphic encryption within systems. This was interesting due to the fact that homomorphic encryption allows for the sending and receiving of data without ever having to encrypt and decrypt the data along the network path using the public and private keys. This can have many uses such as the storing and transmitting of data across insecure servers while maintain an increased semblance of security integrity.

A fully homomorphic encryption system can support arbitrary computation of cypher texts. The system was first theorized in 1978 after the development of RSA. It initially started as an academic search to find the most optimal encryption system, which did not have the inherent vulnerabilities or questionable development history of RSA.

Known drawbacks of homomorphic encryption are the computation time from addition and multiplication is as of yet not suitable for large-scale distributed applications. The slow computation problem arose out of solving a previous issue, which perplexed cryptographic experts for close to 30 years. The initial issue with homomorphic encryption was that the system was inherently very noisy, if a miscalculation had taken place there was no way to know and thus the encrypted information would begin to completely deteriorate over a short period of time, the initial homomorphic systems also did not encompass the ability to multiply and could only perform addition functions, thus severely limiting the system.

Gentrys 1st generation homomorphic system solves the noise problem by using lattice-based cryptography to implement multiplication functions.Drawback is that the homomorphic system is inherently noisy, and after each addition or multiplication the noise increases until the message becomes fully unrecognizable from the original.

The second improvement on this system comes from the paper ”Fully Homomorphic Encryption over the Integers”[1]. This paper theories that homomorphic encryption can be performed without the use of the ideal lattice.

The 2nd generation of systems began in 2010. The 2nd generation is based on decreasing the amount of additive noise generated during the communication process. A less noisy system, is also inversely more secure due to the message not being corrupted, either by accident or by attackers adding noise to the system to purposely corrupt it.

Fortunately the implementation of 2nd generation homomorphic systems are available in the HElib library found on github [2]. The most current implementation of the HElib supports the BGV scheme, which is the newest most optimized 2nd generation scheme available granting computations at 7 seconds.

Homomorphic encryption is attractive for a number of reasons. Firstly the encryption saw its inception in academia and has been publicly worked on and improved by academia for the last 30 years. Unlike RSA there is no suspicion among users that the encryption may already be vulnerable to intelligence agencies. The second reason is that because it was developed by academia the encryption does not belong to any one single commercial or semi-commercial agency, while Gentry was an employee at IBM when he came up with the lattice-based approach he was also studying for a PhD. at Stanford, therefore IBM did not specifically control all his findings under an NDA. Thus the most important parts of the system can be developed without the pressure of sales teams pushing for quick deployment. Lastly the project is open source on Github, anyone who is interested in contributing to the project or implementing it in their system is free to do so.

Uses of this can apply in large industries susceptible to multiple daily attacks such as health care, banking and energy systems as well as future large-scale industries such as NES or networks as a service and self-driving cars. The homomorphic system can allow these systems to perform computations without ever exposing the data to any of the other systems. A quick example of this would be that the data of a person in a self driving ambulance can travel from the persons phone to the ambulances modem to the network operator to the hospital and back without the data ever having been exposed to any of the nodes in between this network. Thus encryption keys never need to be employed and the responsibility of data integrity and security does not have to rely as heavily on all the intermittent nodes in the network.

This theoretical ease of deployment coupled with the security promised makes homomorphic encryption the perfect encryption system to supersede current standards and become the encryption standard of the future.

References

[1] M. van Dijk, C. Gentry, S. Halevi, and V. Vaikuntanathan, “Fully homomorphic encryption over the integers,” MIT and IBM, Tech. Rep., June 2010.

[2] shaih, “Helib.” [Online]. Available: https://github.com/shaih/HElib