Quantum Homomorphic Encryption

By

Joan Watiri Ngure (njoan@aims.ac.rw)
African Institute for Mathematical Sciences (AIMS), Rwanda
Supervised by: Professor Barry C Sanders
University of Calgary, Canada

June 2018

AN ESSAY PRESENTED TO AIMS RWANDA IN PARTIAL FULFILMENT OF THE REQUIREMENTS FOR THE AWARD OF MASTER OF SCIENCE IN MATHEMATICAL SCIENCES

Contents

1. Introduction

1.1 Overview

Owning a computer was the new thing in the world. Everyone wanted to have one. The first computers were very large in size but as the years passed by the size decreased. We now have portable laptops. Computers crash and we lose all our data, or the computation we want to perform, our computers cannot handle, hence a need arose to store and process our data elsewhere in addition to the local storage. This was characterized by Cloud Computing. Cloud Computing can be described as using the cloud (we can imagine is some server stored somewhere anonymous) to carry out our tasks like storage and data management over a network rather than doing it in our own computers.

We enjoyed cloud computing for a while but then the issue of security arose. We don't have control of who could access our data while in the cloud. Some people could just be curious or you may have made enemies somewhere, other times, it would be just accidental that someone gets hold of your data. Imagine a leakage of a patient's examination results or diagnoses. It started by using for example a symbol to represent a patient. Yes the patient's name maybe anonymous, but if someone has access to the hospital's data they would know how many people are suffering from a certain disease among others. This person can decide to cause unnecessary chaos or theft in case of a bank where a customers personal information is exposed. It became possible to encrypt data and send it over but performing computations on this encrypted data was not possible. Homomorphic Encryption shows that it is actually possible to perform computations on encrypted data.

1.2 Background and Motivation

In April 2011, a Play Station's network owned by Sony was hacked. There was exposure of customers information like credit card and passwords. The responsibility for this incidence was accepted by Sony. They realized they had not done enough to ensure security of their customers' data. They would have encrypted it before storage. In this same period researchers also discovered that files in Dropbox were stored unencrypted. This lead to users leaving and closing their accounts with Dropbox since they felt insecure (Ogburn et al., 2013).

According to Pfleeger and Pfleeger (2002), ensuring security would be done in different levels. Securing the hardware (this is the physical system), software (set of instructions executed in the system) and the data itself. In the hardware, locks were put to limit access to unauthorized persons. Systems to detect an intrusion and devices that verify persons identity were put into place. In the software, programs that limit access to database and protect one user from other users were developed. Also software programs were written in such a way that their weaknesses could not be easily exploited. Password checkers and virus scanners application programs were also developed. The solution to the data was encryption. Data is only useful to parties if it can be readable and interpreted. Encrypted data is only useful if one can decrypt it. All this assured

the user of security. At the instances where the user needed to use the data then a problem arose. The data needed to be decrypted before any form of computations. This raises a security issue again. We needed to develop a system that allows computations on encrypted data. This is known as Homomorphic encryption. This assured the user of total security.

Previous works have been done trying to explain how Homomorphic Encryption can be implemented on various platforms using different types of data. In 2013 (Ogburn et al., 2013) tried to explain a model which encrypts hospital data. After the computations are done the number of patients suffering from a certain disease is returned in an encrypted format. The hospital's management then decrypts it. Yokoo and Suzuki (2002) shows a system where different people are using it to perform an optimization problem among themselves. An optimization problem is a problem where you want the output to be the maximum based on certain inputs, for example maximum profit. The task is to find the inputs. These people work without revealing any information about their inputs to the server. Using a similar approach to these works, we will discuss an application of Quantum Homomorphic Encryption in the airport. This model is used to detect unauthorized personnel accessing different points of the airport.

1.3 Aim and Objectives of the Study

The aim of this essay is to show the current state of security while requiring services from an untrusted server. The objectives include explaining vividly the security concerns and showing steps taken to counter these issues.

1.4 Purpose of the Study

The purpose of this essay is to show why one would consider a Quantum Homomorphic Encryption over a Classical Homomorphic Encryption and how Quantum Homomorphic Encryption can be implemented by showing an example.

1.5 Organization of Essay

This essay has been subdivided into different chapters. In chapter 2 we will discuss about classical and cloud computing with their limitations compared to quantum computing. In chapter 3, quantum computing is vividly discussed. Different types of encryption in quantum computing and why one is chosen over the other. Chapter 4 talks about an airport example which is an application of quantum homomorphic encryption and its implementation using Python. Chapter 5 is a conclusion with recommendations.

References

Stefanie Barz, Elham Kashefi, Anne Broadbent, Joseph F Fitzsimons, Anton Zeilinger, and Philip Walther. Demonstration of blind quantum computing. *Science*, 335(6066):303–308, 2012.

Michael J Bremner, Richard Jozsa, and Dan J Shepherd. Classical simulation of commuting quantum computations implies collapse of the polynomial hierarchy. In *Proceedings of the Royal Society of London A: Mathematical, Physical and Engineering Sciences*. The Royal Society, 2010.

Anne Broadbent and Stacey Jeffery. Quantum homomorphic encryption for circuits of low T-gate complexity. In *Annual Cryptology Conference*, pages 609–629. Springer, 2015.

Anne Broadbent, Joseph Fitzsimons, and Elham Kashefi. Universal blind quantum computation. In *Foundations of Computer Science, 2009. FOCS'09. 50th Annual IEEE Symposium on*, pages 517–526. IEEE, 2009.

Ran Canetti, Ben Riva, and Guy N Rothblum. Practical delegation of computation using multiple servers. In *Proceedings of the 18th ACM conference on Computer and communications security*, pages 445–454. ACM, 2011a.

Ran Canetti, Ben Riva, and Guy N Rothblum. Two 1-round protocols for delegation of computation. *IACR Cryptology ePrint Archive*, 2011, 2011b.

Joe Fitzsimons. Blind quantum computing and fully homomorphic encryption, 2012. Stackexchange.

Joseph Fitzsimons, Li Xiao, Simon C Benjamin, and Jonathan A Jones. Quantum information processing with delocalized qubits under global control. *Physical review letters*, 99(3), 2007.

Joseph F Fitzsimons. Private quantum computation: An introduction to blind quantum computing and related protocols. *npj Quantum Information*, 3(1):23, 2017.

Craig Gentry. *A fully homomorphic encryption scheme*. Stanford University, 2009.

Brian Hayes. Cloud computing. *Communications of the ACM*, 51(7):9–11, 2008.

He-Liang Huang, Qi Zhao, Xiongfeng Ma, Chang Liu, Zu-En Su, Xi-Lin Wang, Li Li, Nai-Le Liu, Barry C Sanders, Chao-Yang Lu, et al. Experimental blind quantum computing for a classical client. *Physical review letters*, 119(5), 2017.

Cescily Nicole Metzgar. *RSA Cryptosystem: An Analysis and Python Simulator*. PhD thesis, Appalachian State University, 2017.

Michael Miller. *Cloud computing: Web-based applications that change the way you work and collaborate online*. Que publishing, 2008.

Monique Ogburn, Claude Turner, and Pushkar Dahal. Homomorphic encryption. *Procedia Computer Science*, 20:502–509, 2013.

Yingkai Ouyang, Si-Hui Tan, and Joseph Fitzsimons. Quantum homomorphic encryption from quantum codes. *arXiv preprint arXiv:1508.00938*, 2015.

Charles P Pfleeger and Shari Lawrence Pfleeger. *Security in computing*. Prentice Hall Professional Technical Reference, 2002.

Andrew Steane. Quantum computing. *Reports on Progress in Physics*, 61(2):117, 1998.

Craig Stuntz. What is homomorphic encryption, and why should I care?, 2010. Blog.

Subashini Subashini and Veeraruna Kavitha. A survey on security issues in service delivery models of cloud computing. *Journal of network and computer applications*, 34(1):1–11, 2011.

Si-Hui Tan, Joshua A Kettlewell, Yingkai Ouyang, Lin Chen, and Joseph F Fitzsimons. A quantum approach to homomorphic encryption. *Scientific reports*, 6, 2016.

Max Tillmann, Si-Hui Tan, Sarah E Stoeckl, Barry C Sanders, Hubert de Guise, René Heilmann, Stefan Nolte, Alexander Szameit, and Philip Walther. Generalized multiphoton quantum interference. *Physical Review X*, 5(4), 2015.

Yang Yang et al. *Evaluation of somewhat homomorphic encryption schemes*. PhD thesis, Massachusetts Institute of Technology, 2013.

Makoto Yokoo and Koutarou Suzuki. Secure multi-agent dynamic programming based on homomorphic encryption and its application to combinatorial auctions. In *Proceedings of the first international joint conference on Autonomous agents and multiagent systems: part 1*, pages 112–119. ACM, 2002.