NCRISET-2017 e-ISSN: 2456-3463
International Journal of Innovations in Engineering and Science, Vol. 2, No.6, 2017
www.ijies.net

Review Paper On Cryptoleq : Performance and Security

Miss Meenal P.Talekar [1], Mr. Ravindra Kale[2]

[1]M.Tech Student,[2] Assistant Professor,
Department of Computer Science Engineering,
G.H.Raisoni Institute of Engineering and Technology,Nagpur, India.

Abstract *– The rapid expansion and increased popularity of cloud computing comes with no shortage of privacy communication mainly depends upon digital data communication. Cryptoleq: an abstract machine based on the concept of one instruction set computer, and performing general-purpose computation on encrypted programs. The addition on the encrypted domain are protected using the Paillier partially homomorphic cryptosystem, which supports. Today our prior requirement is data security has become crucial now days in every sector. So in order to protect it, various methods and Algorithm have been implemented. Cryptography combines Science, Mathematics, Computer Engineering and Networking. The purpose of this research paper is (i) to find the best cryptographic algorithm for computations (ii) to study the Cryptoleq system which (iii) and finally the comparison of performance of algorithm with Cryptoleq and without Cryptoleq.*

Keywords- single instruction machine, heterogeneous computer, mathematical computations, encryption.

1. INTRODUCTION

The Contemporary computing paradigms used in cloud and pervasive computing, have become increasingly popular as they allow outsourcing computation it provides typically more powerful or dedicated set of machines. The owner can get the legitimate information because Cryptographic primitives such as homomorphic encryption can be leveraged to address those privacy concerns, and control of the data. From secure cloud computation and verifiable computation to multiparty computation and message authenticators.

As soon as fully homomorphic encryption (FHE) became theoretically possible the academic interest in FHE applications has increased accordingly. From secure cloud computation and verifiable computation, to multiparty computation and message authenticators. In addition, partial homomorphic encryption (PHE) has recently been leveraged for verifiable computation. Homomorphic encryptions allow complex mathematical operations to be performed on encrypted data without compromising the encryption. While preserving relationships between elements of different data sets the homomorphic describes the transformation of one data set into another data set. In addition, partial homomorphic encryption (PHE) has been used in variable computations. RSA is the most widely used public-key crypto system. Public-key cryptosystem are important because they provide data integrity and non repudiation as well as confidentiality and authentication of data. An RSA operation is a modular exponentiation, which requires repeated modular multiplications.

Cryptoleq, is a new programming language based on a single instruction computer architecture, which processes homomorphic encryption on data. One instruction set computer (OISC) is a computer architecture which supports only one instruction and is able to perform universal computation. It operates on a sequence of memory cells i.e. organized memory while processor instructions and data reside in unified memory space. Cryptoleq defines a universal computer for processing encrypted and unencrypted data together within the same program memory space. By implementing various cryptographic algorithms the execution time of mathematical computation observed. I will use RSA with Cryptoleq to reduce the execution time of computation. The Cryptoleq framework is native support for data privacy when computation is outsourced to semi-trusted parties. Thus, due to the security guarantees of that scheme, it is not generally possible to leak any plaintext information, either by examining cipher texts in memory.

II- LITERATURE SURVEY

Oleg Mazonka, Nektarios Georgios Tsoutsos, proposed a new computational model depicted in Figure 1, shows the cryptoleq abstractions layer which is based on the concept of single instruction architecture. Cryptoleq is able to execute programs whose instruction operands have been encrypted using Paillier PHE scheme.

Universal computation is achieved by introducing a software function, which adds multiplication to the abstract machine's native addition and subtraction operations. They also developed an enhanced assembly language to facilitate the development of complex programs, in addition to a compiler and an emulator.

Rivest et al (1978) Introduced for the first time the concept of Homomorphic encryption. The multiplicative property was introduced by Taher(1985) and paillier Cryptosystem was praposed by Paillier(1999) which has additive homomorphic property and these are various applications can be implemented like-voting, etc.

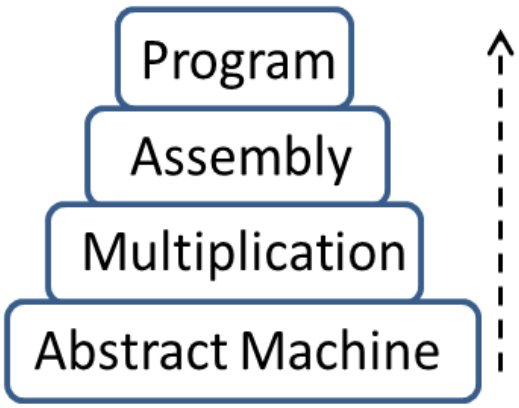

Fig. 1. Cryptoleq abstraction layers

Chan (2009) works on privacy homomorphism in which he was perform operation on encrypted data and also given two additive homomorphic schemes i.e. Iterated Hill Cipher and Modified RSA. The following table shows the various encryption schemes which perform homomorphic encryption are proposed by different researchers.

Table1: Various Homomorphic Encryption Schemes and their Properties

Researcher	Name of Algorithm	Property	Flavor
Rivest et al.(1978)	RSA	Multiplicative	Partial Homomorphic
Taher(1985)	ElGamal Cryptosystem	Multiplicative	Partial Homomorphic
Paillier(1999)	Paillier Cryptosystem	Additive	Partial Homomorphic
Chan(2009)	Iterative Hill Cipher	Additive	Partial Homomorphic
Gentry (2009)	Gentry's Fully	Both additive and fully homomorphic	Homomorphic Multiplicative Encryption.

Shahzadi et al.(2012) has done the detailed study of three homomorphic encryption algorithm, i.e. RSA, ElGamal and Paillier. Also they evaluated all three algorithms and shown the comparative study between these algorithm. The result shown that RSA performs better than El Gamal and Paillier. Whereas ElGamal Performs better than paillier.

Naser and Bin (2013) surveyed on specific security issues and use of cryptography in cloud computing. Carlos et al.(2013 have done survey on recent advances in homomorphic encryption techniques advances in Some What Homomorphic Encryption (SWHE) and Fully Homomorphic Encryption (FHE) algorithm.

Ramgovind et al. (2010) highlighted key security considerations currently faced by industry. Aderemi and Oluwaseyi(2011) proposed an encryption layer which is on top of the encrypted data on the cloud and also discussed about the security issues in cloud computing and the potentials of homomorphic encryption. Liu (2012) has introduced some cloud computing system to analyze cloud computing security problems. He suggested that to provide the total security in cloud single security technique cannot be used he also suggest that to solve the cloud security problem many traditional and some new strategies are required to use together.

The cryptographic program obfuscation first implemented by D.Apon,Y. Hung, J Katz, and A.J. Malozemoff (2014). They discuss both challenges encountered and optimizations made over the course of our development, and present a detailed evaluation of the performance of such obfuscators and also show that obfuscation is still far from practical. Without changing the input/output behavior of the program, the process of obfuscation making a program "unintelligible". Although there is a long line of work on heuristic techniques for obfuscation, which do not provide any cryptographic guarantee on their effectiveness.

A recent result by Garg et al. (FOCS 2013), however, shows that cryptographic program obfuscation is indeed possible based on a new primitive called a graded encoding scheme. K.M. Chung, Y. Kalai, and S. Vadhan(2010), used fully homomorphic encryption to design improved schemes for delegating computation. In this scheme, a delegator outsources the computations of a function F on many, dynamically chosen inputs.

Niyatee Bhatt, Shafika, Payal V. Parmer(2010) introduce a basic concept of the homomorphic encryption and the various encryption algorithm as per the properties of the homomorphic encryption. They introduce how various cryptographic algorithm are being used for applying homomorphic encryption for privacy preservation.

III. RESEARCH PROPOSED

The previous work on Cryptoleq describes that Cryptoleq is a single instruction set abstract machine. In the previous work the Paillier algorithm implemented with Cryptoleq for performing different types of computations. It has been observed that with Paillier algorithm the computation time

required for multiplication operation is more as compared to addition and subtraction. And according to my observation RSA performs better than Paillier. And also the computation time for multiplication operation of RSA is much better than Paillier. So I am implemented RSA in a Cryptoleq to improve the performance of multiplication computation. The main purpose of this step is to reduce the execution time of multiplication operation.

To find conclusion, I will compare the computations of Paillier and RSA algorithm with Cryptoleq system and observe the execution time of both algorithm with Cryptoleq system.

IV- CONCLUSION

Cryptoleq system introduce a new computational model based on the concept of single instruction architecture, able to execute programs whose instruction operands have been encrypted using RSA scheme. Universal computation is achieved by introducing a software function, which adds multiplication to the abstract machine's native addition and subtraction operations. This function is expressed using the only available instruction. We have also developed an enhanced assembly language to facilitate the development of complex programs, in addition to a compiler and an emulator. Cryptoleq allows for several future improvements with regards to performance and security i.e. reduces the execution time and complexity of algorithms.

ACKNOWLEDGEMENT

I would like to express my thanks to the people who have helped me most throughout my research. I am grateful to college principal, HOD, and my guide for their motivation and nonstop support.

REFERENCES

[1] *Oleg Mazonka, Nektarios Georgios Tsoutsos, "Cryptoleq: A Heterogeneous Abstract Machine for Encrypted and Unencrypted Computation" in (2016).*

[2] S. Halevi and V. Shoup, "Bootstrapping for HElib," in Advances in Cryptology. Heidelberg, Germany: Springer,, 641–670,2015.

[3] J. Zimmerman, "How to obfuscate programs directly," in Advances in Cryptology. Heidelberg, Germany: Springer, 2015, pp. 439–467.

[4] S. Halevi and V. Shoup. HElib: Design and Implementation of a Homomorphic-Encryption Library, accessed on Nov. 13, 2015.

[5] D. Apon, Y. Huang, J. Katz, and A. J. Malozemoff, "Implementing cryptographic program obfuscation," in Proc. IACR Cryptol. ePrint Arch., 2014, p. 779.

[6] S. Garg, C. Gentry, S. Halevi, and M. Zhandry, "Fully secure functional encryption without obfuscation," in Proc. IACR Cryptol. ePrint Arch.,2014, p. 666.

[7] P. T. Breuer and J. P. Bowen, "A fully homomorphic crypto-processor design," in Engineering Secure Software and Systems. Heidelberg, Germany: Springer, 2013, pp. 123–138.

[8] Naser A W S and Bin Md Fadli (2013), " Use of Cryptography in Cloud Computing", pp. 179-184, proceedings of IEEE International Conference on Control System Malaysia.

[9] Shahzadi Farah et al."An Experimental Study on Performance Evaluation of Asymmetric Encryption Algorithms", Recent Advances in information Science, Proceeding of the 3rd European Conf. of Computer Science, (EECS-12) 2012.

[10] Ramgovind S, Eloff M and smith E " The management of security in Cloud Computing", Proceedings of IEEE Conference 2010.