Recent Advances in Technology and Engineering (RATE-2017)
6th National Conference by TJIT, Bangalore

International Journal of Science, Engineering and Technology
An Open Access Journal

A Study on Sparse Subset Sum Using Homomorphic Encryption

[1]Bokobri Lekpeli Koissy Franck Olivier, C. Umarani

Abstract

In Gentry's fully homomorphic cryptosystem a sparse sub-set sum problem is used and this big set of number are included in the public key. Reducing the size of the public key, Gentry and Halevi used a specific form of sparse subset problem using geometric progressions. The subset sum problem is major problem In complexity theory and cryptography. As the homomorphic encryption we will be used public key as well secret key for encryption and decryption of the ciphertext. Boostrappable technique will be used to squash the noise inside the polynomials degree.

Keywords: Boostrappable, homomorphic encryption

Introduction

Encryption is the conversion of electronic into another form, called ciphertext which cannot be easily understood by anyone except authorized parties. Homomorphic encryption is the one and latest encryption developed by halevi Gentry into IBM research for more security into user data and information. In this research paper we are going to understand the different parameter need and used for homomorphic encryption and showing how it re invent the security of data.in this study i will explain fully homomorphic encryption is, why implementing is interesting and worthwhile effort and give overview of the state of the art on this area.

SPAPRSE SUBSET PROBLEM

	0	1	2	3	4	5	6	7	8	9	10	11
2	T	F	T	F	F	F	F	F	F	F	F	F
3	T	F	T	T	F	T	F	F	F	F	F	F
7	T	F	T	T	F	T	F	T	F	T	T	F
8	T	F	T	T	F	T	F	T	T	T	T	F
10	T	F	T	T	F	T	F	T	T	T	T	T

ANSWER: (3,8)

FULLY HOMOMORPHIC ENCRYPTION

Our ultimate goal is to construct a fully homomorphic encryption scheme *E*. let us discuss what is *fully homomorphic*. At a high-level fully homomorphic encryption is simple: given ciphertexts that encrypt Pi1*; : : : ;* Pit, fully homomorphic encryption should allow anyone (not just the key-holder) to output a ciphertext that encrypts *f*(Pi1*; : : : ; P*it) for any desired function *f*,as long as that function can be e±ciently computed. No information about Pi1*; : : : ;* Pit or *f*(Pi1*; : : : ;* Pit), or any intermediate plaintext values, should leak; the inputs, output and intermediate values are always encrypted. Formally, there are different ways of defining what it means for the final ciphertext to encrypt" *f*(Pi1*; : : : ;* Pit). The minimal requirement is correctness. A fully homomorphic encryption scheme *E* should have an efficient algorithm Evaluate *E* that, for any valid *E* key pair (sk*;* pk), any circuit *C*, and any ciphertexts *Vi*<-Encrypt *E*(pk*;* Pi), outputs V Evaluate *E* (pk , *C, v*1*; : : : ; vt*) such that Decrypt *E*(sk*; v*) = *C*(Pi1*; : : : ;* Pit) This minimal requirement does not seem to be sufficient, however, since it permits the trivial solution, where Ã simply consists of (*C; v1; : : : ; vt*) { i.e., where the Evaluate *E* algorithm does not "process" the input ciphertexts at all.

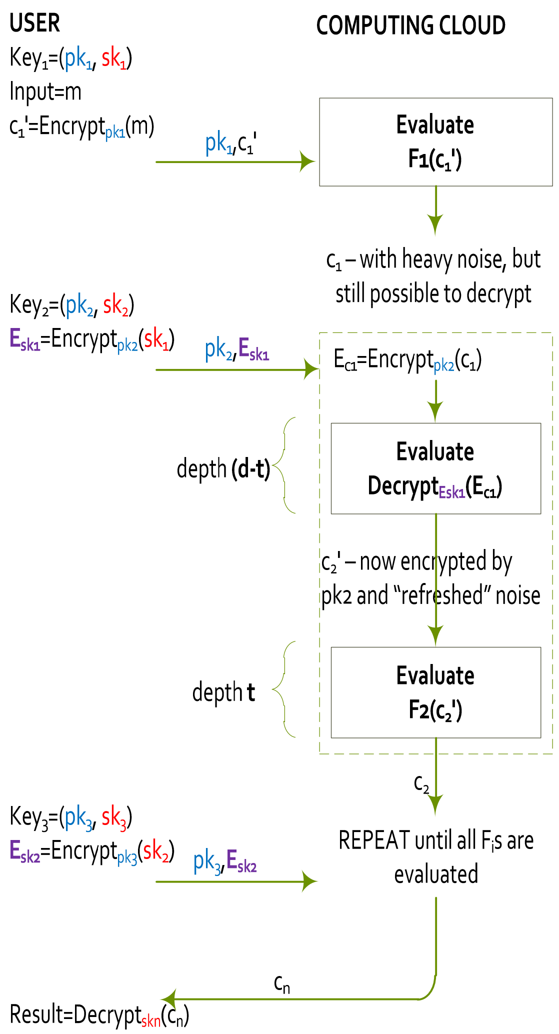
EXAMPLE OF FULLY HOMOMORPHIC ENCRYPTION OVER INTEGERS

$(180)_{10} = (10110100)_2$ Answer $(400)_{10} = (0000000110010000)_2$

$(220)_{10} = (11011100)_2$

BOOSTRAPPABLE TECHNIQUE

If E is bootstrappable, then, for any integer d, one can construct a scheme E(d) that can evaluate any circuit (consisting of NAND gates) of depth d. The decryption circuit for E(d) is the same as for E, and the complexity of encryption is alsothe same. E(d)'s public key size is O(d) times that of E's. The complexity of EvaluateE(d)is polynomial in the security parameter and linear in the circuit size. If E is semantically secure against chosen plaintext attacks, then so is EvaluateE(d).



Conclusion

In this study on sparse subset sum problem using homomorphic encryption we have been able to understand how the spasre subset sum problem is used by homomorphic encryption to choose his paramenter for secret and public key and how boostrappable technique used to evalutate homomorphic encryption with one more step. Futher work will be to include some more operations on the cipertext as for now addition and multiplication is possible.

References

1.Fully Homomorphic Encryption Using Ideal Lattices by Craig Gentry Stanford University and IBM Watson

2.A FULLY HOMOMORPHIC ENCRYPTION SCHEME A DISSERTATION SUBMITTED TO THE DEPARTMENT OF COMPUTER SCIENCE AND THE COMMITTEE ON GRADUATE STUDIES OF STANFORD UNIVERSITY IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OFDOCTOR OF PHILOSOPHY Craig Gentry September 2009

3.On the sparse subset sum problem from Gentry-Halevi's implementation of fully homomorphic encryption by Moon Sung Lee.

4.NETWORK SECURITY: PREVALENCE OF INTRUSION DETECTION SYSTEM-C.UMARANI, ISBN (13 Digits) : 978-81-910024-3-0, ISBN (10 Digits) : 81-910024-3-4

5. A Study of Symmetric key Encrpytion- C.UMARANI, OPTIMA Journal of Physical Science,ISSN 2320-4834, Volume -3.

Author's details

[1]MCA-ISMS Student, Jain University, Bangalore

[2]Professor,Jain University,Bangalore