ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 11, March 2016

A HYBR ID HOMOMORPHIC ENCRYPTION TO REDUCE STORAGE REQUIREMENTS

Mrs.R.SUJATHA M..E.,
Assistant Professor / IT,
M.Kumarasamy College of Engineering,
Karur –639 113
sujathar.it@mkce.ac.in

Ms.G.MONIKA
Final Year / IT,
M.Kumarasamy College of Engineering,
Karur –639 113
monikaganesan.be@gmail.com

Ms.B.DHARANI
Final Year / IT,
M.Kumarasamy College of Engineering,
Karur –639 113
bdharani694@gmail.com

ABSTRACT

We introduce a hybrid homomorphic encryption that combines public-key encryption and somewhat homomorphic encryption to reduce the storage requirements of most somewhat or fully homomorphic encryption (FHE) applications. In this model, messages are encrypted with a PKE and computations on encrypted data are carried out using SHE or FHE after homomorphic decryption. To obtain efficient homomorphic decryption, our hybrid scheme combines IND-CPA PKE without complicated message padding with SHE with a large integer message space. Furthermore, if the underlying PKE is multiplicative, the proposed scheme has the advantage that polynomials of arbitrary degree can be evaluated without bootstrapping. We construct this scheme by concatenating the ElGamal and Goldwasser–Micali schemes over a ring ZN for a composite integer N whose message space is Z × N. To accelerate the homomorphic evaluation of the PKE decryption, we introduce a method to reduce the degree of the exponentiation circuit at the cost of additional public keys. Using the same technique, we present an efficient partial solution to an open problem which is to evaluate mod q mod p arithmetic homomorphically for large p. As an independent interest, we also obtain a generic method for converting from private-key SHE to public-key SHE.Unlike the method described by Rothblum , we are free to choose the SHE message space.

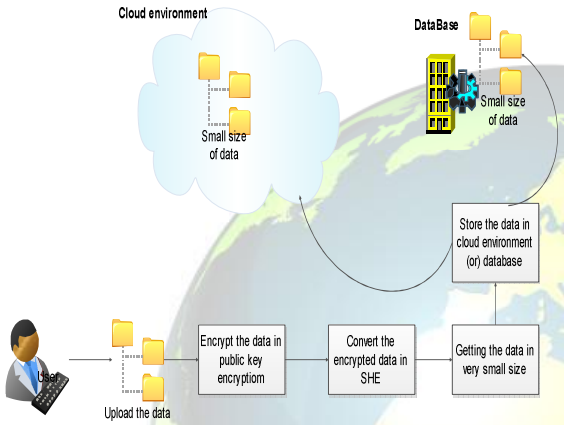
1.INTRODUCTION

The concept of computation on encrypted data without decryption was first introduced by Rivest, Adleman and Dertouzos in 1978. Thirty years later, Gentry proposed a fully homomorphic encryption (FHE) based on ideal lattices. This scheme is far from being practical because of its large computational cost and large ciphertexts. Since then, considerable efforts have been made to devise more efficient schemes. However, most FHE schemes still have very large ciphertexts (millions of bits for a single ciphertext). This presents a considerable bottleneck in practical deployments. We consider the following situation: several users upload data encrypted with a public-key FHE, a server carries outcomputations on the encrypted data and then sends them to an agency who has a decryption key for the FHE. This is common in typical FHE scenarios, such as medical and financial applications. In this situation, one approach to reduce the storage requirement is to use AES encryption to encrypt data, and then perform homomorphic computations on ciphertexts after converting to FHE-ciphertexts. This method has a great advantage in storage and communication, because only small AES-ciphertexts are transmitted from user to server, and these are homomorphically decrypted only when their homomorphic computations are required. In an asymmetric setting, we can still use this approach by adding several public-key FHE ciphertexts of a session key. However this approach is not practical when the amount of messages transmitted simultaneously is small compared with the size of on FHE ciphertext. Moreover, the conversion of AES-ciphertexts into FHE-ciphertexts requires a leveled FHE with multiplicative depth of at least forty. In this paper, we explore an alternative method that encrypts messages with a public key encryption (PKE) and converts them into SHE-ciphertexts for homomorphic computations. In this approach, the ciphertext expansion ratio is only two or three regardless of the message size. Moreover, the decryption circuit is very shallow when the SHE allows large integers as messages. For example, the decryption circuit of ElGamal over ZN has a multiplicative depth of nine

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 11, March 2016

under a SHE with the message space Z*N*. We can reduce the depth further by representing the secret exponent *e* as log*w e* binary vectors of length *w*, which is an improvement over the Gentry-Halevi technique.

2.SYSTEM ARCHITECTURE



In a cloud environment, each client encrypts their messages using limited computing power and storage and a server manages the encrypted data with its large computing power and storage. However, the current FHE's may not be suited to this environment, because their large ciphertext size entails a large communication cost.

3.ALGORITHM

In constructing a hybrid scheme, candidate encryptions for an additive homomorphic IND-CPA PKE include Goldwasser–Micali, encryptions. The decryption circuit of each system requires additional circuits besides exponentiation, the Chinese remainder algorithm for the Goldwasser–Micali and Naccache–Stern encryptions, and integer division for the Paillier and Okamoto–Uchiyama encryptions. Because it is difficult to evaluate the integer division part efficiently, the latter encryptions are unsuitable for the construction of our hybrid scheme. Thus we only consider the Goldwasser–Micali, Joye–Libert, and Naccache–Stern encryptions for PKE in the hybrid scheme.

4.EXISTING SYSTEM

Several users upload data encrypted with a public-key FHE, a server carries out computations on the encrypted data and then sends them to an agency who has a decryption key for the FHE. This is common in typical FHE scenarios, such as medical and financial applications. In this situation, one approach to reduce the storage requirement is to use AES encryption to encrypt data, and then perform homomorphic computations on ciphertexts after converting to FHE-ciphertexts. This method has a great advantage in storage and communication, because only small AES-ciphertexts are transmitted from user to server, and these are homomorphically decrypted only when their homomorphic computations are required. In an asymmetric setting, we can still use this approach by adding several public-key FHE ciphertexts of a session key. However this approach is not practical when the amount of messages transmitted simultaneously is small compared with the size of on FHE ciphertext. Moreover, the conversion of AES-ciphertexts into FHE-ciphertexts requires a leveled FHE with multiplicative depth of at least forty.

5.PROPOSED SYSTEM

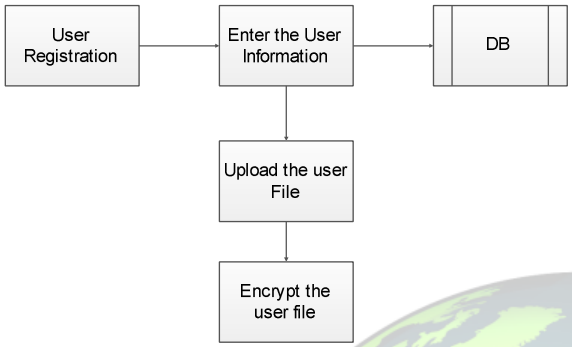
In this work explore an alternative method that encrypts messages with a public key encryption (PKE) and converts them into SHE-ciphertexts for homomorphic computations. In this approach, the ciphertext expansion ratio is only two or three regardless of the message size. Moreover, the decryption circuit is very shallow when the SHE allows large integers as messages. For example, the decryption circuit of ElGamal over Z*N* has a multiplicative depth of nine under a SHE with the message space Z*N*.2 We can reduce the depth further by representing the secret exponent *e* as log*w e* binary vectors of length *w*, which is an improvement over the Gentry-Halevi technique. When using additive (resp. multiplicative) homomorphic encryption as the underlying PKEs, we obtain the additional advantage that additions (resp. multiplications) can be computed without converting to SHE.

6.MODULES

6.1 USER LOGIN AND DATA UPLOAD

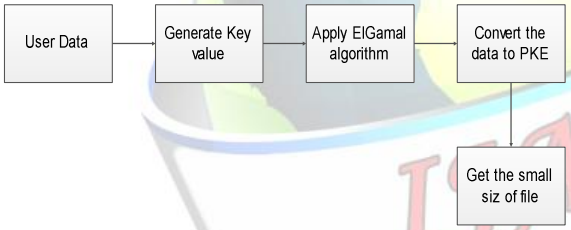
ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 11, March 2016

In this module each registers their information and login to the process. User uploads their file and file size to the encryption process.To reduce the storage requirements.



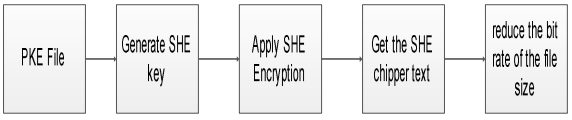
6.2 USER DATA CONVERT TO PUBLIC KEY ENCRYPTION

In this module user data's are converted to the Public Key Encryption. Data owners upload their file to PKE. In the Encryption process ElGamal Encryption is used for reduce the chipertext file size. Using public key encryption algorithm reduces the storage space.



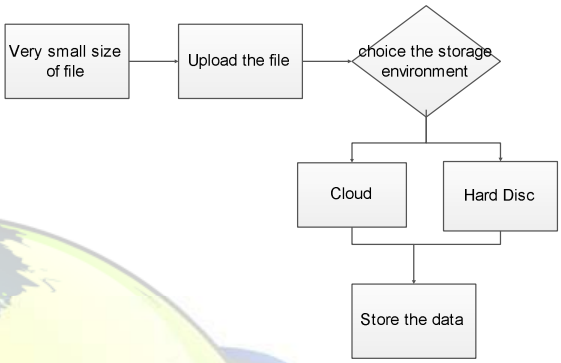
6.3 PKE DATA CONVERT TO SOMEWHAT HOMOMORPHIC ENCRYPTION

In this module PKE data convert to the SomeWhatHomomorphic Encryption. User generates the Key value for the user data. Put the key value and convert the PKE file to SomeWhatHomomorphic Encryption process. Get the very small size of Cipher text file.



6.4 UPLOAD THE FILE TO STORAGE ENVIRONMENT

In this module user upload their chipper text file to the storage environment. User has the very small size of chipper text file and which environment their want to store the data. If their retrieve the data to see the original plaintext. Enter the correct key to decrypt the data.



7.RELATED WORK

7.1SCALE-INVARIANT FULLY HOMOMORPHIC ENCRYPTION OVER THE INTEGERS

A scale-invariant fully homomorphic encryption scheme based on the LWE problem, in which the same modulus is used throughout the evaluation process, instead of a ladder of moduli when doing \modulus switching". In this paper we describe a variant of the van Dijk et al. FHE scheme over the integers with the same scale-invariant property. Ourscheme has a single secret modulus whose size is linear in the multiplicative depth of the circuit to be homomorphically evaluated, instead of exponential; we therefore construct a leveled fully homomorphic encryption scheme. This scheme can be transformed into a pure fully homomorphic encryption scheme using bootstrapping, and its security is still based on the Approximate-GCD problem. We also describe an implementation of the homomorphic evaluation of the full AES encryption circuit, and obtain signi_cantly improved performance compared to previous implementations: about 23 seconds per AES block at the 72-bit (resp. 80-bit) security level on a mid-range workstation. Finally, we prove the equivalence between the (error-free) decisional Approximate-GCD problem introduced by Cheon et al. (Eurocrypt 2013) and the classical computational Approximate-GCD problem. This equivalence allows

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 11, March 2016

to get rid of the additional noise in all the integer-based FHE schemes described so far, and therefore to simplify their security proof. Christo Ananth et al. [4] proposed a system in which the complex parallelism technique is used to involve the processing of Substitution Byte, Shift Row, Mix Column and Add Round Key. Using S- Box complex parallelism, the original text is converted into cipher text. From that, we have achieved a 96% energy efficiency in Complex Parallelism Encryption technique and recovering the delay 232 ns. The complex parallelism that merge with parallel mix column and the one task one processor techniques are used. In future, Complex Parallelism single loop technique is used for recovering the original message. Constructed the _rst fully homomorphic encryption scheme (FHE), i.e. a scheme allowing a worker to evaluate any circuit on plaintext values while manipulating only ciphertexts.

7.2 SOMEWHAT PRACTICAL FULLY HOMOMORPHIC ENCRYPTION

Fully homomorphic encryption allows evaluation of arbitrary functions on encrypted data, and as such has a myriad of potential applications such as private cloud computing. Gentry were the _rst to show that FHE is theoretically possible. His construction consisted of three parts: _rst, construct an encryption scheme that is somewhat homomorphic, i.e. that can evaluate functions of limited complexity (think low degree), secondly, simplify the decryption function of this scheme as much as possible (so called squashing), thirdly, evaluate this simpli_ed decryption function homomorphically to obtain ciphertexts with a _xedinherent noise size (so called bootstrapping). The _rst variants of Gentry's scheme all followed the same struc- ture and as such had to make additional security assumptions to enable the squashing step. More recent schemes avoid squashing all together and can bootstrap by evaluating the real decryption circuit. Another advantage of the more recent schemes is that their security is based on the Learning with Errors (LWE) problem or its ring variant RLWE, the hardness of which can be related to classical problems on (ideal) lattices.

7.3 A QUASI-POLYNOMIAL ALGORITHM FOR DISCRETE LOGARITHM IN FINITE FIELDS OF SMALL CHARACTERISTICS

The discrete logarithm problem (DLP) was first proposed as a hard problem in cryptography in the seminal article of Diffie and Hellman. Since then, together with factorization, it has become one of the two major pillars of public key cryptography. As a consequence, the problem of computing discrete logarithms has attracted a lot of attention. Recently, practical and theoretical advances have been made with an emphasis on small to medium characteristic finite fields and composite degree extensions. The most general and efficient algorithm a complexity of L(1=4 + o(1)) when the characteristic is smaller than the square root of the extension degree. Among the ingredients of this approach, we find the use of a very particular representation of the finite field; the use of the so-called systematic equation1; and the use of algebraic resolution of bilinear polynomial systems in the individual logarithm phase. In this work, we present a new discrete logarithm algorithm, in the same vein as in that uses an asymptotically more efficient descent approach. The main result gives a quasi-polynomial heuristic complexity for the DLP in finite fields of small characteristic. By quasi-polynomial, we mean a complexity of type n O(log n) where n is the bit-size of the cardinality of the finite field. Such a complexity is smaller than any L(_) for _ > 0. It remains super-polynomial in the size of the input, but offers a major asymptotic improvement compared to L(1=4 + o(1)).

7.4 ON DATA BANKS AND PRIVACY HOMOMORPHISMS

Encryption is a well—known technique for preserving the privacy of sensitive information. One of the basic, apparently inherent, limitations of this technique is that an information system working with encrypted data can at most store or retrieve the data for the user; any more complicated operations seem to require that the data be decrypted before being operated on. This limitation follows from the choice of encryption functions used, however, and although there are some truly inherent limitations on what can be accomplished, we shall see that it appears likely that there exist encryption functions which permit encrypted data to be operated on without preliminary decryption of the operands, for many sets of interesting operations. These special encryption functions we call “privacy homomorphisms”; they form an interesting subset of arbitrary encryption schemes

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 11, March 2016

(called "privacy transformations"). As a sample application, consider a small loan company which uses a commercial time—sharing service to store its records. The loan company's "data bank" obviously contains sensitive information which should be kept private. On the other hand, suppose that the information protection techniques employed by the time sharing service are not considered adequate by the loan company. In particular, the systems programmers would presumably have access to the sensitive information. The loan company therefore decides to encrypt all of its data kept in the data bank and to maintain a policy of only decrypting data at the home office —— data will never be decrypted by the time—shared computer. The situation is thus that of Figure 1, where the wavy line encircles the physically secure premises of the loan company.

7.5 FULLY HOMOMORPHIC ENCRYPTION USING IDEAL LATTICES

We propose a fullyhomomorphic encryption scheme i.e., a scheme that allows one to evaluate circuits over encrypted data without being able to decrypt. Our solution comes in three steps. First, we provide a general result – that, to construct an encryption scheme that permits evaluation of arbitrary circuits, it suffices to construct an encryption scheme that can evaluate (slightly augmented versions of) its own decryption circuit; we call a scheme that can evaluate its (augmented) decryption circuit bootstrappable. Next, we describe a public key encryption scheme using ideal lattices that is almost bootstrappable. Lattice-based cryptosystems typically have decryption algorithms with low circuit complexity, often dominated by an inner product computation that is in NC1. Also, ideal lattices provide both additive and multiplicative homomorphisms (modulo a public-key ideal in a polynomial ring that is represented as a lattice), as needed to evaluate general circuits. Unfortunately, our initial scheme is not quite bootstrap- pable – i.e., the depth that the scheme can correctly evalu- ate can be logarithmic in the lattice dimension, just like the depth of the decryption circuit, but the latter is greater than the former. In the final step, we show how to modify the scheme to reduce the depth of the decryption circuit, and thereby obtain a bootstrappable encryption scheme, with- out reducing the depth that the scheme can evaluate. Ab- stractly, we accomplish this by enabling the encrypter to start the decryption process, leaving less work for the de- crypter, much like the server leaves less work for the de- crypter in a server-aided cryptosystem.

8.CONCLUSION

We proposed a hybrid scheme that combines public key encryption and somewhat homomorphic encryption. The proposed scheme is suitable for cloud computing environments since it has small bandwidth, low storage requirement, and supports efficient computing on encrypted data. Our solution provides a trade-off between the size of the transmitted ciphertexts and the conversion costs. While the ciphertext expansion of PKE is larger than that of AES, it can be homomorphically evaluated with a SHE of much smaller multiplicative depth. The parameters of our hybrid scheme are very large when the message space of the underlying FHE is Z_N. For an efficient implementation, we need a method to evaluate mod N arithmetic using an FHE whose message space is Z_M for small $M > 2$.

REFERENCES

[1] R. Barbulescu, P. Gaudry, A. Joux, and E. Thomé.(2013). "A quasipolynomial algorithm for discrete logarithm in finite fields of small characteristic."[Online].
[2] J. H. Cheon*et al.*, "Batch fully homomorphic encryption over the integers," in *Advances in Cryptology* (Lecture Notes in Computer Science), vol. 7881, T. Johansson and P. Nguyen, Eds. Berlin, Germany: Springer-Verlag, 2013, pp. 315–335.
[3] K.-M. Chung, Y. Kalai, and S. Vadhan, "Improved delegation of computation using fully homomorphic encryption," in *Advances in Cryptology* (Lecture Notes in Computer Science), vol. 6223, T. Rabin, Ed. Berlin, Germany: Springer-Verlag, 2010, pp. 483–501.
[4] Christo Ananth, H.Anusuya Baby, "Encryption and Decryption in Complex Parallelism", International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), Volume 3, Issue 3, March 2014,pp 790-795
[5] T. ElGamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," in *Advances in Cryptology* (Lecture Notes in Computer Science), vol. 196, G. R. Blakley and D. Chaum, Eds. Berlin, Germany: Springer-Verlag, 1984, pp. 10–18.
[6] J. Fan and F. Vercauteren, "Somewhat practical fully homomorphic encryption," in *Proc. IACR*

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 11, March 2016

Cryptol., 2012, p. 144.

[7] C. Gentry and S. Halevi, "Fully homomorphic encryption without squashing using depth-3 arithmetic circuits," in *Proc. IEEE 52nd Annu.Symp. Found. Comput. Sci. (FOCS)*, Oct. 2011, pp. 107–109.

[8] C. Gentry, S. Halevi, and N. P. Smart, "Homomorphic evaluation of the AES circuit," in *Advances in Cryptology* (Lecture Notes in Computer Science), vol. 7417, R. Safavi-Naini and R. Canetti, Eds. Berlin, Germany: Springer-Verlag, 2012, pp. 850–867.

[9] S. Goldwasser and S. Micali, "Probabilistic encryption," *J. Comput.Syst.Sci.*, vol. 28, no. 2, pp. 270–299, 1984.

[10] M. Naehrig, K. Lauter, and V. Vaikuntanathan, "Can homomorphic encryption be practical?" in *Proc. 3rd ACM Cloud Comput. SecurityWorkshop (CCSW)*, 2011, pp. 113–124.