www.revistageintec.net
ISSN: 2237-0722
revista GEINTEC Gestão, Inovação e Tecnologias

A Review on Algorithms of Homomorphic Encryption

T. Prahlad Reddy[1]; Dr.G. Mamatha[2]; Dr.M.N. Giri Prasad[3]
[1]Jawaharlal Nehru Technological University, Anantapuramu, India.
[1]prahlad001@gmail.com
[2]Jawaharlal Nehru Technological University, Anantapuramu, India.
[3]Jawaharlal Nehru Technological University, Anantapuramu, India.

Abstract
The rapid evolution of technologies like Internet of Things (IoT) and Cloud computing which handle big-scale data through the operations operate, store and manage. Besides, the technology facilitates with operations related to safety and confidentiality concerns. Moreover, the increasingly accessible cryptosystems offer the security concerns by IoT and cloud computing at several segments. In addition, the provision of third-party cloud process and analytics service contributors creates a privacy challenges to the consumer data. The current evolutions in the homomorphic encryption permits the computations on the data even when its encrypted. Therefore, a substantial research has been conducted on homomorphic encryption since few decades. However, the requirement of real-time implementation is essential for homomorphic encryption methods for achieving better improvements. Thus, the survey introduces the innumerable schemes for homomorphic encryption, advancements, and developments for decades, and its future progression for the implementation in real-time scenario.

Key-words: Homomorphic Encryption, Cloud Computing,

1. Introduction

Based on the most recent technologies of Internet of Things, data science, as well as cloud-based computing basically gather the confidential customer data to storage at the remote servers. Furthermore, the collected raw data is managed, later transformed to specific information instead of additional analytics intern to provide effective service. Nevertheless, a safety challenge exists as costumers' data to be further outsourced with the cloud-based environment for real-time practices. Therefore, such service providers' confidentiality raise concerns in the present scenario.

For instance, the third-party predictive analytics provider involvement in healthcare system raises medical data privacy concern. Instead, if the mathematical computations required in analytics can performed on an encrypted data, then the privacy issues are largely resolved.

In addition, the analysis based on the predictive and prescriptive in the health care service necessitates the data required in the analysis to be communicated to service providers. However, the security contravention for mentioned situations reached certain instances attaining the effects at greater unfavourable impacts on the privacy in data acquired by the patient. The privacy challenges can be minimized and solved with the implementation of mechanism associated to the data that is encrypted.

Besides, the important feature of the cryptosystem is implementation without the data being lost or modified. Later, the modifications based on the standard cryptosystems, both symmetric and public key are useful in implementing the Homomorphic Encryption (HE). HE is a cryptosystem where the mathematical computations are done on the ciphertext. The deciphered text is the same as result obtained by the calculations done on the plaintext.

2. Homomorphic Encryption Categories

Numerous types of algorithms for homomorphic encryption have been suggested together with differing resources for the operation of arithmetic procedures. The competences of different schemes give variable computational capabilities reliant on the implementation form and its constraints. The following listed are the practical categories of policies:

1. Partially Homomorphic Encryption (PHE)

The initial form of homomorphism is PHE that has been established in the current development. The performance of the arithmetic operations such as addition, subtraction, or multiplication has the limitation even with the range of computations allocated. Certain schemes of PHE involves the cryptosystems of ElGamal, RSA, Goldwasser-Micali, Paillier, Benaloh, Sander-Young-Yung, and Ishai-Paskin, and Boneh-Goh-Nissim.

2. Somewhat Homomorphic Encryption (SWHE)

This scheme can perform the operations involved for mutual addition and multiplication on the privacy data. However, the constraint leading to the scheme is it can implement for the limited

range of computations. Although the noise existed in combinational to the cryptosystem enhances the encrypted level of randomness. There is a trade-off between the data increase in computational count and noise domination. Thus, the necessary deciphered data is highly unfeasible towards accomplishment.

3. Fully Homomorphic Encryption (FHE)

This scheme manages with the full-fledged operations of homomorphic encryption. In order to eradicate the limitation of restricted count of operations, the SWHE scheme are integrating with a process known as bootstrapping *(RECRYPT)*. Therefore, at every stage of computation in FHE, the integration of bootstrapping is employed to maintain the noise in inspection. Nevertheless, there is drawback in combining the bootstrapping with FHE, which increase the computational burden as well as cost of the process.

4. Levelled Fully Homomorphic Encryption (LFHE)

This technique is an enhancement to the FHE scheme. Despite of implementing the technique of bootstrapping at every stage of computation with the result of limited computations in FHE. Thus, the outcome attained will be the issues of depth constraint by distributing the bootstrapping procedure.

The following algorithm is associated to the Homomorphic encryption schemes:

1. KeyGen – The input is fed with the security parameter and results in output of secret key pair and public.
2. Encrypt – Produces the ciphertext with the utilization of plaintext and public key.
3. Decrypt – Outcome's plaintext/deciphered text with the utilization of secret key and ciphertext.
4. Evaluate – Results are obtained by providing the circuit or computation system with the ciphertext as input.
5. Bootstrapping (Recrypt) – Interprets the ciphertext following with each computation stage or with limited computations for minimizing the noise effect on the definitive result of decipher. Such case is employed in both schemes of LFHE and FHE.

Balance Equation Snippet

Assume m_1 and m_2 are assigned as the encrypted messages to be performed and *ENCRYPT(m)* signify the encryption of the variable *m* assumed.

$ENCRYPT(m_1) = c_1$ & $ENCRYPT(m_2) = c_2$

$ENCRYPT(m_1) + ENCRYPT(m_2) = c_3$

Later, the addition intended for the homomorphic encryption implemented such as follows:

$DECRYPT(c_3) = DECRYPT(c_1) + DECRYPT(c_2)$

i.e.,

$DECRYPT[ENCRYPT(m_1) + ENCRYPT(m_2)] = m_1 + m_2$

the multiplication intended for the homomorphic encryption implemented such as follows:

$DECRYPT(c_3) = DECRYPT(c_1) \times DECRYPT(c_2)$

i.e.,

$DECRYPT[ENCRYPT(m_1) \times ENCRYPT(m_2)] = m_1 \times m_2$

The scheme is demonstrated in the model of homomorphic encryption. Thus, the reflection of encrypted plaintext is computed with the performance achieved in the obtained data of the form based on decrypted system and deciphered basis.

5. Related Works

From initial stages of completely homomorphic encryption (FHE) conspire remained intended through the researchers in the year of 1978 by Adleman, Rivest, and Dertouzos [1], yet through the concerns of security in the state of homomorphisms acquired by the users. Afterward, more than 30 long lifetimes, it is defined to be the possible arrangement have been muddled however exploration has been done. According to few decades, the performance of the unsolved part of outcomes reached for the homomorphism remained presented by outcomes.

The author Craig Gentry in the year of 2009 [2] suggested current FHE scheme. Assigned plot depends for the case of ideal analysis with the cross sections that complete homomorphic state of expansion as well as duplication. Although, the procedure for the bootstrapping scheme of component remains acquainted with complete limitless quantity associated to the calculations exempting the maximum limits. However, the intricacy for the computational besides plan dwells with the grid stage in ideal scenario.

In 2010 [3] Dijik et. al., recommended for the scheme involved with the SWHE conspire through particular number-crunching as well as utilize plan for bootstrapping to transform towards the scheme of FHE. Eventually, reasonably straightforward secluded number-crunching over ideal grids is helpful for carrying out in asset compelled gadgets similar to IoT.

Brilliant et. al., [5] recommended plot for the scheme of FHE together with little important besides sizes of ciphertext contrasted with assigned case of the place Gentry's in the case of key paired with the public as well as private issues in the ciphertext in the utilization for the generic field. In comparison to the various component with the schemes of variable analysis with the SWHE against the FHE for the implementation of the evaluation in the limitations ot the boundaries in the existing system. Practically speaking plan presents the superior profundity with the unscrambling trail.

Moreover, the multi-bounce Homomorphic Encryption has been planned by Nobility et. al.,[6] in which the calculation for the HE graphs can be replaced with the execution of the own filed in the case of several iterations into the bootstrapping system for the outcome reached with the case of single input crack.

In addition, effectively executed with the integration of bootstrap with the FHE. Later, the enhancements have been planned by Nobility et. Al., [7] for minimizing the intricacy of computation. Also, primary improvement attains crucial-age strategy that doesn't need reversal of polynomial equation. Further, the clumping strategy utilized in advancing encryption system. Alongside the existence compromises are likewise accomplished.

An inexpensive utilizing of FHE studying with minimum errors has been proposed in 2011 by Brakerski et. al [8]. In essence, the resistance plan depends with most pessimistic scenario issues discretionary grids. Another linearization procedure is formulated dependent on LWE which prompts provable hardness to the plan. In any case, the past plans depend on intricacy presumptions of ideal rings. An epic measurement modulus decrease procedure is acquainted with abbreviate the ciphertexts formats.

Furthermore, the FHE combined short open levers around numbers has been highlighted by the Coron et. al., [9]. Considering, plan theoretically straightforward contrasted with the Gentry's plan. In spite of the fact that Dijk et. al., utilizes a similar idea however at the expense of too huge public key size for reasonable execution. This plan decreases the public key size by scrambling with the quadratic structure. A more grounded variation of inexact GCD issue powers security. Further, basic number-crunching tasks are carried out with the productivity accomplished.

Gentry et. al., in 2013 [10] presented the integration of HIE with LWE towards accomplishment of reasonable straightforwardness. Later, plan beats costly advance including "relinearization" executed past such proposed scheme plots by carrying out a rough eigenvector technique. The plan likewise takes out the genuinely necessary assessment key to perform activities. All things being equal, barely any essential boundaries assist with developing trait personality established FHE scheme conspire.

The further works involved with the whole numbers associated to the batches of FHE proposed by Coron et. al., that has executed the plan for clump in the vector issues of plaintext morsels for the outcome of solitary ciphertext format. The plan additionally carries out self-assertive changes alongside option and duplication. The FHE assessment of such format assessed tantamount techniques earlier plans dependent at fusion approach of Ring-LWE based scheme of FHE. Assessment techniques means for the investigation of future schemes.

As in the case of real numbers the FHE scheme evaluated and is represented in [12]. The creators deliver functional requests current idea of FHE and executions because of elevated idleness. Thus. plan advance assesses dangers related security through thinking about model situations. The commotion levels are radically decreased throughout decoding employed with the mathematical tasks.

Cheon et. al., [13] estimated the excellence for the case of managing the scheme for GW in the analysis of the other senator for scaling the division of yield in the clamour for safety issues in the RLWE built for the security contravention for mentioned situations reached certain instances attaining the effects at greater unfavourable impacts on the privacy in data acquired by the patient. The privacy challenges can be minimized and solved with the implementation of mechanism associated to the data that is encrypted contribution of the novel technique in the pact feature of the execution in the model.

Wang et. al., in 2018 [14] underlined the effective dependent conspire of model of FHE schemes. This plan decreases the public key size by scrambling with the quadratic structure. A more grounded variation of inexact GCD issue powers security. Moreover, reduced case of computational expense is accomplished contrasted with up to referenced plans with a little blunder rate compromise.

6. Implementations

Developments for HE with the application of various commercial, industrial, proprietary, and opensource based operations established concerning to the area associated to the particular work in

which customer has executed in the specified practice. Not as many of the real-time analysis made as open source for the useful publicly obtainable performances for the schemes integrated to the HE is listed as follows:

Name	**Designer**	**Observations**
HElib [15]	IBM	Optimizations of the schemes involved for BGV and GHS.
PALISADE [16]	Consortium of DARPA-funded defence contractors and academics: New Jersey Institute of Technology, Duality Technologies, Raytheon BBN Technologies, MIT, University of California, San Diego and others.	General and defence purpose lattice cryptography library.
HEAAN [17]	Seoul National University	
Microsoft SEAL [18]	Microsoft	
FHEW [19]	Leo Ducas and Daniele Micciancio	
TFHE [20]	Ilaria Chillotti, Nicolas Gama, Mariya Georgieva and Malika Izabachene	
FV-NFLlib [21]	CryptoExperts	
NuFHE [22]	NuCypher	Requires a GPU operation of TFHE

7. Conclusion

The accumulation of business-related players, collaborations, and industrial assistance, the research in FHE has reached a greater height. Nevertheless, such schemes associated with certain constraints like slacken, computational burden and cost, moreover commercially not feasible in the current edge technology. However, with the implementation of FPGA and GPU stipulate the essential powered computation with more rapid operations maintain the trade-off among cost, power, and efficiency. In addition, the operations dealt with the large-scale implementations seems to be non-viable. In order to provide solution to particular challenge, the suggested combination is multiparty calculation and its variants.

References

R.L. Rivest, L. Adleman, and M.L. Dertouzos, "On data banks and privacy homomorphisms," *Foundations of Secure Computation*, 169–180, 1978.

C. Gentry, *"A fully homomorphic encryption scheme,"* Ph.D. dissertation, Stanford University, 2009.

M. van Dijk, C. Gentry, S. Halevi, and V. Vaikuntanathan, “Fully homomorphic encryption over the integers,” *in EUROCRYPT,* 2010, 24–43.

O. Regev, “On lattices, learning with errors, random linear codes, and cryptography,” *in STOC,* 2005, 84–93.

N.P. Smart and F. Vercauteren, “Fully homomorphic encryption with relatively small key and ciphertext sizes,” *in Public Key Cryptography*, 2010, 420–443.

C. Gentry, S. Halevi, V. Vaikuntanathan, “i-Hop Homomorphic Encryption and Rerandomizable Yao Circuits”, *in CRYPTO* 2010, 2010.

C. Gentry and S. Halevi, “Implementing Gentry’s fully-homomorphic encryption scheme,” *in EUROCRYPT,* 2011, 129–148.

Z. Brakerski and V. Vaikuntanathan, “Efficient fully homomorphic encryption from (standard) LWE,” *in FOCS,* 2011, pp. 97–106.

J.S. Coron, A. Mandal, D. Naccache, and M. Tibouchi, “Fully homomorphic encryption over the integers with shorter public keys,” *in CRYPTO,* 2011, 487–504.

Gentry C., Sahai A., Waters B., “Homomorphic Encryption from Learning with Errors: Conceptually-Simpler, Asymptotically-Faster, Attribute-Based, CRYPTO 2013. *Lecture Notes in Computer Science,* 8042. Springer, Berlin, Heidelberg.

JS. Coron, T. Lepoint, and M. Tibouchi, “Batch fully homomorphic encryption over the integers,” *IACR Cryptology ePrint Archive,* vol. 2013, p. 36, 2013.

K. Gai, M. Qiu, Y. Li and X. Liu, “Advanced Fully Homomorphic Encryption Scheme Over Real Numbers”, 2017 *IEEE 4th International Conference on Cyber Security and Cloud Computing (CSCloud),* New York, NY, 2017, pp. 64-69.

Cheon J.H., Kim A., Kim M., Song Y. “Homomorphic Encryption for Arithmetic of Approximate Numbers”, *ASIACRYPT 2017, Lecture Notes in Computer Science,* 10624. Springer, Cham.

X. Wang, T. Luo, J. Li, “A More Efficient Fully Homomorphic Encryption Scheme Based on GSW and DM Schemes”, Security and Communication Networks, 2018, Article ID 8706940, 14, 2018.

Shai Halevi, Victor Shoup. “HElib: An Implementation of homomorphic encryption”, February 2021. *https://github.com/homenc/HElib*

“PALISADE Lattice Cryptography Library”. February 2021. *http://palisade-crypto.org/*

Jung Hee Cheon; Kyoohyung Han; Andrey Kim; Miran Kim; Yongsoo Song. *“Homomorphic Encryption for Arithmetic of Approximate Numbers”*. February 2021. *https://github.com/snucrypto/HEAAN*

Microsoft Research. “Microsoft SEAL”. February 2021. *https://www.microsoft.com/en-us/research/project/microsoft-seal*

Leo Ducas; Daniele Micciancio. “FHEW: A Fully Homomorphic Encryption library”. February 2021. *https://github.com/lducas/FHEW*

Ilaria Chillotti; Nicolas Gama; Mariya Georgieva; Malika Izabachene. “Faster Fully Homomorphic Encryption: Bootstrapping in less than 0.1 Seconds”. February 2021. *https://tfhe.github.io/tfhe*

Crypto Experts. “FV-NFLlib”. November 2019. *https://github.com/CryptoExperts/FV-NFLlib*

NuCypher. “A GPU implementation of fully homomorphic encryption on torus”. February 2021. *https://github.com/nucypher/nufhe*