Homomorphic Encryption

Conference Paper · May 2021

DOI: 10.1007/978-3-030-76346-6_56

2 authors:

Michael Gaid
Arab Academy for Science, Technology & Maritime Transport
7 PUBLICATIONS **81** CITATIONS

SEE PROFILE

Said A. Salloum
University of Salford
235 PUBLICATIONS **8,971** CITATIONS

SEE PROFILE

Homomorphic Encryption

Michael Lahzi Gaid[1] and Said A. Salloum[2,3](✉)

[1] Faculty of Engineering and IT, The British University in Dubai, Dubai, UAE
[2] School of Science, Engineering, and Environment, University of Salford, Salford, UK
ssalloum@sharjah.ac.ae
[3] Research Institute of Sciences and Engineering, University of Sharjah, Sharjah, UAE

Abstract. Homomorphic Encryption is a class of encryption methods envisioned by Rivest, Adleman, and Dertouzos already in 1978, and first constructed by Craig Gentry in 2009. It differs from typical encryption methods in the sense that it allows computation operations to be performed directly on encrypted data without requiring access to a secret key (A Few Thoughts on Cryptographic Engineering). The result of such a computation remains in encrypted form, and can at a later point be revealed by the owner of the secret key. This form of encryption allows computation on ciphertexts, generating an encrypted result which, when decrypted, matches the result of the operations as if they had been performed on the plaintext. The purpose of Homomorphic Encryption is to allow computation on encrypted data. Usually, it is used for large-scale statistical analysis and mostly used in data encryption and decryption. Thus, it is used programs that rely mainly on information security and high-security documents in many governmental segments. The challenging aspect is performing statistical analysis on encrypted data and getting an accurate result, without putting the data through the risk of being stolen or having a backdoor copy for it.

Keywords: Homomorphic · Secret key · Cipher texts · Governmental segments

1 Introduction

Homomorphic Encryption is a form of encryption that allows computation on ciphertexts, generating an encrypted result which, when decrypted, matches the result of the operations as if they had been performed on the plaintext [1, 2]. Homomorphic Encryption schemes are widely used in many interesting applications, such as private information retrieval, electronic voting, multiparty computation, and cloud computing [3]. Abstract algebra, it is a structure-preserving map between two algebraic structures, such as groups [1]. Figure 1 shows group Homomorphism.

There are four types of Homomorphic Encryption. Homomorphic Encryption (HE), Partially Homomorphic Encryption (PHE), Somewhat Homomorphic (SWHE), and Fully Homomorphic Encryption (FHE). HE is a form of encryption that allows searching the encrypted data without the need to decrypt it first and hence leaving it vulnerable [4]. Morris argues that there are many forms PHE that allow for some specific operations to be performed (namely addition and multiplication). A cryptosystem is considered PHE

A. E. Hassanien et al. (Eds.): AICV 2021, AISC 1377, pp. 634–642, 2021.
https://doi.org/10.1007/978-3-030-76346-6_56

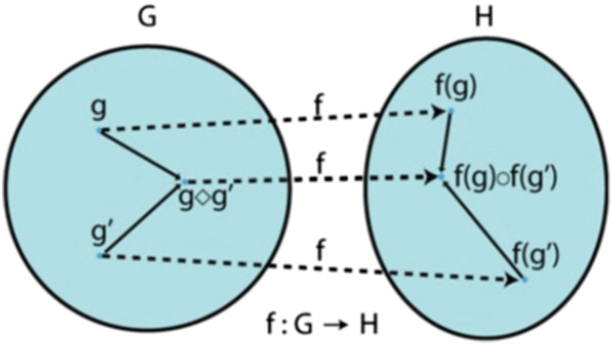

Fig. 1. Group homomorphism [1].

if it represents either addition or multiple homomorphisms, but not both [5]. It can also work with Big Integers of hundreds of bits, considering that the multiplications do not exceed the value of the module used in the encryption. Thus, it is very practical in this regard.

SWHE is considered a more generic form of Homomorphic Encryption in the sense that it can work on both addition and multiple Homomorphism. Its limitation though lies in the fact that it works with a limited number of bits [6]. Craig Gentry was the first to develop a Fully Homomorphic Cryptosystem in 2009 [7]. FHE is considered that way, since it presents both multiplicative and additive Homomorphism, with an unlimited number of bits [5]. It is the most important advantage is its enhanced privacy and retrieval of private information in the sense that it enables computing on encrypted data without first having to decrypt it, which in turn allows data to be transferred to an untrusted cloud application without fear of data leakage [3], thus, it is seen as a safe storage state. Gai used a method of blending arithmetic operations over real numbers and proposed a novel tensor-based Fully Homomorphic Encryption solution. Figure 2 shows Gai's proposed scheme [8].

Despite how great this system is, yet one of its biggest drawbacks is the complexity of the system and the noise that it creates in the system. Yet, it can be applied on large scale in all segments of the governments like in the financial sector, the voting system, or even on the information of a large enterprise [5]. Polynomial is a term that consists of variables and coefficients, involved in addition, multiplication, and subtraction-based operations [9]. Polynomials increase rapidly in all arithmetic equations since each operation leads to the creation of another polynomial. Thus, an infinite number is created within a single calculation. This is why it is called noise. This noise in major cipher text operations needs to be less than 1/2 to ensure that the decryption is correct [10]. To explain this further, with any mathematical operation, the noise created by the output is mostly larger than the noise of the input. Many schemes have been studied to decrease the noise made, yet many of them were very costly, like the BFV scheme and logistic Regression tool, and both are commonly used and add great value.

The proposed study aims to examine various qualitative methods that were applied to Homomorphic Encryption. To do this, I have analyzed three qualitative methods.

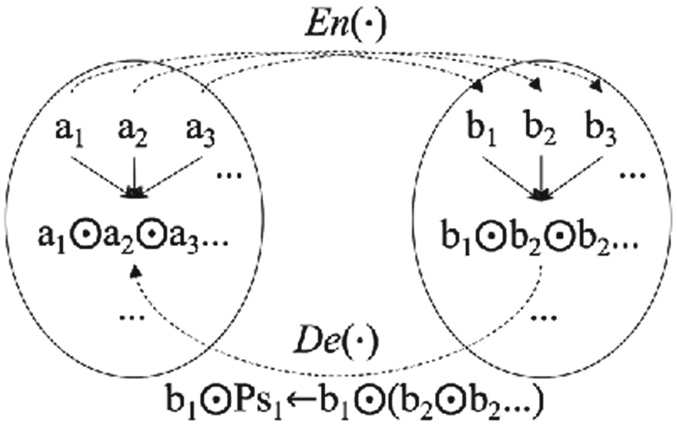

Fig. 2. Gai's proposed scheme [8]

These qualitative methods are (a) conceptual work, (b) review-based work, and (c) implementation-based work.

2 Literature Review

In this section, the summary of two research papers is provided for each qualitative methodology.

2.1 Methodology 1: Conceptual Framework

In this part, the following two latest papers of reputed journals are reviewed to identify a well-established conceptual framework in respect of Homomorphic Encryption.

Paper I

Title: "A Guide to Fully Homomorphic Encryption".
Citation: "Armknecht, F., Boyd, C., Carr, C., Gjøsteen, K., Jäschke, A., Reuter, C.A., & Strand, M. (2015). A Guide to Fully Homomorphic Encryption. *IACR Cryptology ePrint Archive, 2015*, 1192". [11].
Research Method: Conceptual framework.
The suggested methodology of encryption aims to provide unlimited numbers of addition and multiplication over the encrypted numbers, Fully Homomorphic Encryption scheme supporting addition and multiplication over the numeric numbers. Now, it is considered one of the most effective IT encryption technique to solve the data protection issue.
Description, Advantages & Disadvantages: The authors stated and summarized the different definitions in the field of homomorphic encryption. In addition, they had discussed the existing applications that need homomorphic encryption to get to the bottom of their theoretical and practical problems. On the other hand, they had systematically

reviewed Homomorphic Encryption. The Homomorphic Encryption subject is a challenging research area, and a great deal needs to be done. However, if work (especially advancing efficiency) continues at its current pace, we are optimistic that implementations in the real world may be right around the corner. There is much work to be done. Regarding the control of the noise, the time cost that is currently consumed to encrypt, operate, and decrypt. Despite, the huge amount of work that has been made in the field of Homomorphic Encryption, there is a dire need to decrease the time needed to carry out some functions using Homomorphic Encryption. Then there is the more abstract line of work. Meanwhile, a specification has been proposed for group homomorphic encryption schemes, and to some extent for FHE, there is a lack of an analogous result for complete (or at least somewhat) homomorphic encryption schemes. All protected schemes that came up with homomorphic encryption are based on adding noise, therefore the biggest challenge is; how to control the noise? Currently, this why fully homomorphic encryption schemes are considerably less efficient.

Paper 2

Title: "Core Concept: Homomorphic Encryption".
Citation: "Robert Frederick, Proceedings of the National Academy of Sciences Jul 2015, 112 (28) 8515–8516; https://doi.org/10.1073/pnas.1507452112". [12].
Research Method: Conceptual architecture.
This paper presented the core concept of Homomorphic Encryption, then discussed the different degrees of Homomorphic Encryption; the difference between "Fully" and "Partly." Homomorphic, stating that, Partly Homomorphic does not work for multiplication. Multiplying 2 by 3 would be encrypted as 20*30, and decrypting the answer, 600, gets you 60, not 6, as desired. Creating a Fully Homomorphic encryption scheme is intuitively straightforward; as doing so in the aforementioned example means defining "encrypted multiplication" to include a division by 10. Then, the paper discussed the hard part that has been motivating and creating the Fully Homomorphic Encryption scheme efficient; the new algorithm that has been presented by Gentry, 2009.
Description, Advantages & Disadvantages: This paper had introduced a precise stating and a concise roadmap for the progress of Homomorphic encryption. Moreover, the new term of Homomorphic Encryption; which is "Practical Homomorphic Encryption" was discussed. In addition to that, the main functions of Homomorphic Encryption were presented sided by time consumption for each different degree of Homomorphic Encryption. This paper tried to analyze the progress that has been done in the cryptography field mainly the Homomorphic Encryption schemes, meaning the advantages and disadvantages of each algorithm, specifying the most reputation cryptography homomorphically team, and the current world challenge, despite that, the paper lacked to deeply view the technical part of each algorithm and it didn't even wave to the technical part of any of the aforementioned discussed papers. Missing the part of the conclusion and/or recapitulate, what should be concluded with?

2.2 Methodology 2: Review Based Work

In this part, the following latest paper of reputed journals is reviewed to identify a well-established review work in respect of Homomorphic Encryption.

Title: "Somewhat Practical Fully Homomorphic Encryption".
Citation: "Fan J, Vercauteren F. Somewhat Practical Fully Homomorphic Encryption. IACR Cryptology ePrint Archive. 2012 Mar;2012:144." [6].
Research Method: Review based work.
The purpose of this study is to come up with the requirements for a somewhat homomorphic scheme to be circularly secure, namely that; the scheme can be used to securely encrypt its own. The secret key is obstacles in moving from "somewhat" to complete homomorphism. This requirement was not known to be feasible under any cryptographic assumption for all known rather homomorphic encryption schemes and had to be specifically assumed.
Description, Advantages & Disadvantages: This paper ported Brakerski's FHE scheme from the LWE to the RLWE setting and presenting a detailed analysis of all involved subroutines such as multiplication, relinearization, and bootstrapping. This study results in strong worst-case constraints on the noise generated by homomorphic operations, which can be used to extract very specific parameters for which the scheme can be made completely homomorphous. The study found two optimized variants of relinearization resulting in a smaller re-linearization key as well as faster computations than existing solutions. Additionally, the study condensed the analysis of the bootstrapping step by a modulus switching trick. This paper's findings provided a solid theoretical basis for practical implementations. However, they noted that the derived boundaries are the worst-case boundaries and not the average case boundaries that can easily be extracted from the central limit theorem. The paper mentioned that they will consider very practical aspects of the scheme in a follow-up paper, including the average case boundaries, and report on an implementation in the Magma computer algebra system and a highly optimized dedicated multiplier hardware implementation.
Two more major improvements are feasible and are in progress, namely, the bootstrapping stage can be greatly improved by using a much better SIMD approach than the current state of the art; and the actual homomorphic method itself should be replaced by our approach to FHE, which minimizes the size of the ciphertext to the size of the noise found therein.

2.3 Methodology 3: Implementation Based Work

In this part, the following two latest papers of reputed journals are reviewed to identify a well-established implementation-based work in respect of Homomorphic Encryption.

Paper 1

Title: "CryptoNets: Applying Neural Networks to Encrypted Data with High Throughput and Accuracy".

Citation: “Nathan Dowlin Ran Gilad-Bachrach Kim Laine Kristin Lauter Michael Naehrig John Wernsing, MSR-TR-2016–3 | February 2016” [13].
Research Method: Implementation based work.
The author’s design is a technique that was proposed that transfers learned artificial feed-forward neural networks into CryptoNets. This allows the user to upload his data on any cloud service while still encrypted, thus, the cloud service cannot get any data without the decryption key, in other words, it relies on an End-to-End system. This method has proven accuracy, speed, and private predictions [13]. In this study, CryptoNets were demonstrated on MINIST (Modified National Institute of Standards and Technology database) optical character recognition task. Table 1 shows the breakdown time to apply CryptoNets on MINIST network and Table 2 shows its performance for MINIST.

Table 1. CryptoNet breakdown time on MINST.

Layer	Description	Time to compute
Convolution layer	Weighted sums layer with windows of size 5 × 5, stride size of 2. From each window, 5 different maps are computed and a padding is added to the upper side and left side of each image.	30 seconds
1^{st} square layer	Squares each of the 835 outputs of the convolution layer	81 seconds
Pool layer	Weighted sum layer that generates 100 outputs from the 835 outputs of the 1^{st} square layer	127 seconds
2^{nd} square layer	Squares each of the 100 outputs of the pool layer	10 seconds
Output layer	Weighted sum that generates 10 outputs (corresponding to the 10 digits) from the 100 outputs of the 2^{nd} square layer	1.6 seconds

Table 2. MIST performance.

Stage	Latency	Additional latency per each instance in a batch	Throughput
Encoding+Encryption	44.5 seconds	0.138 seconds	24193 per hour
Network application	250 seconds	0	58982 per hour
Decryption+Decoding	3 seconds	0.012 seconds	274131 per hour

Description, Advantages & Disadvantages: Homomorphic Encryption takes away the decryption key from the server and makes the server process the information in its encrypted form and this provides major advantages from a security standpoint. However, Homographic Encryption is extremely slower than unencrypted systems, and this specific drawback makes using big data analytics useless. CreptoNet increases parallelism by matching the operation used in Homomorphic codes with neural networks to increase speed. Knowing that Homomorphic Encryption works with polynomials, Microsoft tweaked the neural network to only work with polynomials to increase speed. CryptoNet was tested on an MNIST database for handwritten digit recognition, and it achieved 99% accuracy and made ~ 59000 predictions/hour, which makes it a feasible commercial service [13]. From the limitations of this program, as argued by Adrian Colyer, CryptoNet was tested using the MNIST optical character recognition dataset

and it showed that it can only work on a small volume of data. Also, it mainly depends on leveled Homomorphic Encryption scheme that mainly depends on knowing the predictions that will be used, rather than building the neural network itself. Thus, it can be impractical and too expensive to develop and worked with.
CryptoNet paves the way to build secure cloud-based neural network prediction services without invading users' privacy by Using Homomorphic Encryption and modifications to the activation functions [13].

Paper 2

Title: "Secure Translation Using Fully Homomorphic Encryption and Sequence-to-Sequence Neural Networks".
Citation: "Gaid, M., Fakhr, m., & Selim g., (2018, November). Conference: 28th International Conference on Computer Theory and Applications At Alexandria, Egypt (pp. 171–183)" [14].
Research Method: Implementation based work.
This work presented a new principle for the secure translation, by merging sequence to sequence neural network with Fully Homomorphic Encryption, to ensure the secrecy and confidentiality of the translated text, by modifying the 7 gates of the Long Short Term Memory (LSTM) inside the encoder and the decoder which are the main two components of the sequence to sequence neural network; bypassing the public key to the encoder and decoder, then encrypt all weights of the neural networks of the encoder of the decoder using the public key, producing and new ciphertext as the output of the decoder, which will be decrypted using only the private key, to find the target language.
Description, Advantages & Disadvantages: The proposed algorithm is novel, The Sequence-to-Sequence neural network and Homomorphic encryption are rapidly advancing fields, in this research, and both Fully Homomorphic Encryption and Sequence to Sequence Neural Network are used to complement each other. Not only the known problems of the homomorphic encryption scheme in terms of producing large data were overcome by the Sequence to Sequence Neural Network; but also provided organized layers and protected against data explosion and waste when going inwards and backward in the layers. The training was carried using a limited vocabulary, where it proceeded with translating a text from English to Arabic in an encrypted format; by using a combination between sequence to sequence neural network and Fully Homomorphic Encryption. This study managed to prevent the need to decrypt the text to be able to search within it, thus, secured the safety of the data, if it needed to be sent to a third party who is outside the institution, like a cloud service. The proposed algorithm succeeded to create a secure LSTM with a 100% accuracy translational rate. It can be said that the main problem with the performance of the program is that it takes a too long time to translate. Of course, the execution time should be decreased by any means, especially that translating 3 words takes almost 8 h and this can be solved in future work.

3 Pros and Cons of Each Method

There are several advantages/disadvantages of each qualitative method that can be recapitulated as:

One of the popular approaches which can be used to implement a new approach in a growing area is the conceptual system or conceptual modeling. Presenting an architecture or conceptual structure is, however, a promising work and requires a profound knowledge of the topic. Review-based research one survey-based work that offers comprehensive information of the interest domain. Proposing a new research work by review-based work is not an effective way, because only comparisons with current research works are used. The implementation based approach is one of the widely used methods in which work is validated by experiments using various simulation techniques. The implementation-based approach is an effective method of research work though, but this type of work requires real-world implementation or model for simulation.

4 Selection and Justification of the Preferred Method

For research work on homomorphic encryption, the conceptual system or conceptual modeling approach was chosen. The explanation why the conceptual structure approach is chosen is because of conceptual work, it is easy to suggest and explain a new strategy. The growing part of the proposed work can be clearly described with the help of a conceptual framework. In addition, as far as the protection and confidentiality of Homomorphic Encryption are concerned, there are several specific components of the model and there is also dataflow since this is an effective way of using computational modeling.

5 Preferred Method Detailed Comparison

The suggested approach, computational modeling, is an effective way to provide the Homomorphic Encryption research model. Because of this, the review-based research is only used to evaluate current approaches, while the implementation-based methods require real-world implementing tools or simulation platforms to test and check the proposed work.

6 Conclusion

A detailed study on Homomorphic Encryption has been given in this report. I have considered three qualitative approaches for evaluating the research in the proposed area, conceptual modeling, analysis-based work, and implementation-based work. For each qualitative approach, I have given a detailed summary of one or two research papers. In terms of Homomorphic Encryption, I have preferred conceptual modeling to the proposed research model based on existing work.

Acknowledgment. This work is a part of a project submitted in fulfilment of MSc Informatics (Knowledge & Data Management) Faculty of Engineering & Information Technology.

At The British University in Dubai.

References

1. Homomorphic Encryption. https://en.wikipedia.org/wiki/Homomorphic_encryption. Accessed 20 Feb 2018
2. Yousuf, H., Lahzi, M., Salloum, S.A., Shaalan, K.: Systematic review on fully homomorphic encryption scheme and its application. In: Al-Emran, M., Shaalan, K., Hassanien, A. (eds.) Recent Advances in Intelligent Systems and Smart. Studies in Systems, Decision and Control, vol. 295, pp. 537–551. Springer, Cham (2021)
3. Cramer, R., Damgård, I., Nielsen, J.B.: Multiparty computation from threshold homomorphic encryption. In: International Conference on the Theory and Applications of Cryptographic Techniques, pp. 280–300 (2001)
4. Greenberg, A.: Hacker lexicon: what is homomorphic encryption (2017)
5. Morris, L.: Analysis of partially and fully homomorphic encryption. Rochester Inst. Technol. 1–5 (2013)
6. Fan, J., Vercauteren, F.: Somewhat practical fully homomorphic encryption. IACR Cryptol. ePrint Arch. **2012**, 144 (2012)
7. Gentry, C.: A fully homomorphic encryption scheme, vol. 20(9). Stanford University Stanford (2009)
8. Gai, K., Qiu, M.: Blend arithmetic operations on tensor-based fully homomorphic encryption over real numbers. IEEE Trans. Ind. Inform. **14**(8), 3590–3598 (2017)
9. Polynomial. https://en.wikipedia.org/wiki/Polynomial
10. Chen, H., et al.: Logistic regression over encrypted data from fully homomorphic encryption. BMC Med. Genomics **11**(4), 3–12 (2018)
11. Armknecht, F., et al.: A guide to fully homomorphic encryption. IACR Cryptol. ePrint Arch. **2015**, 1192 (2015)
12. Frederick, R.: Core concept: Homomorphic encryption. Proc. Natl. Acad. Sci. **112**(28), 8515–8516 (2015)
13. Gilad-Bachrach, R., Dowlin, N., Laine, K., Lauter, K., Naehrig, M., Wernsing, J.: Cryptonets: Applying neural networks to encrypted data with high throughput and accuracy. In: International Conference on Machine Learning, pp. 201–210 (2016)
14. Gaid, M.L.: Secure Translation Using Fully Homomorphic Encryption and Sequence-to-Sequence Neural Networks. no. October, p. 4 (2018)