

Research Paper

CONCISE AND EFFICIENT MULTI-IDENTITY FULLY HOMOMORPHIC ENCRYPTION SCHEME

ROJARAMANI ADAPA¹, KALLAM YESHASRI², GOSULA SATHWIK³,

RAPARTHI THARUN⁴

¹Assistant Professor, Dept. of CSE, Guru Nanak Institutions Technical Campus, Ibrahimpatnam, Telangana, India

^{2, 3, 4} B.Tech, Dept. of CSE, Guru Nanak Institutions Technical Campus, Ibrahimpatnam, Telangana, India

ABSTRACT— Combining multi-key fully homomorphic encryption (MKFHE) and identity-based encryption (IBE) to construct multi-identity based fully homomorphic encryption (MIBFHE) scheme can not only realize homomorphic operations and flexible access control on identity ciphertexts but also reduce the burden of public key certification management. However, MKFHE schemes used to construct MIBFHE usually have complex construction and large computational complexity, which also causes the same problem for MIBFHE schemes. To solve this problem, we construct a concise and efficient MIBFHE scheme based on the learning with errors (LWE) problem. Firstly, we construct an MKFHE scheme using a new method called “the decomposition method”. Secondly, we make a suitable deformation of

the current IBE scheme. Finally, we combine the above MKFHE scheme with IBE scheme to construct our MIBFHE scheme and prove its IND-sID-CPA security under the LWE assumption in the random oracle model. The analysis results show that our MIBFHE scheme can generate the extended ciphertext directly from the encryption algorithm, without generating fresh ciphertext in advance. In addition, the noise expansion rate is reduced from the polynomial of lattice dimension n and modulus q to the constant K of the maximum number of users. The scale of introduced auxiliary ciphertexts is reduced from $O^*(n^4L^4)$ to $O^*(n^2L^4)$ when generating the extended ciphertext.

Index Terms – Multi-identity based fully homomorphic encryption (MIBFHE), multi-

key fully homomorphic encryption (MKFHE), identity-based encryption (IBE), learning with errors (LWE), lattice-based cryptography, homomorphic encryption, access control, cloud security, post-quantum cryptography, ciphertext expansion, secure computation, random oracle model.

I. INTRODUCTION

Cloud computing can link a large number of computing, storage and software resources together to form a large scale of shared virtual IT pools, providing remote computer users with efficient, fast and diverse information services. However, cloud computing also has to face security problems, which has become an important reason restricting its development. In 1978, Rivest et al. first proposed the notion of “privacy homomorphism” which allows ciphertexts to be operated on without preliminary decryption of the operands. This property can be naturally applied to solve the security problem of cloud computing, and how to construct a fully homomorphic encryption (FHE) scheme has become an open issue in cryptography. In 2009, Gentry proposed the first FHE scheme based on ideal lattice, and made it bootstrappable by using the technique of “squash the decryption circuit”. However, such FHE schemes can

only perform homomorphic operations on ciphertexts encrypted under the same public key. In 2012, López-Alt et al. first proposed the notion of multi-key FHE (MKFHE) and constructed an MKFHE scheme based on the NTRU cryptosystem. Cryptographers have proposed a series of MKFHE schemes. As an extension of FHE, MKFHE allows homomorphic operations on ciphertexts encrypted under different public keys. However, the public key encryption (PKE) system needs to rely on public key certificates to realize identity authentication, which inevitably increases the overhead related to certificate management, especially FHE and MKFHE have a large public key size. Identity-based encryption (IBE) is another cryptographic primitive that was first proposed by Shamir in 1984. Its central idea is to generate a pair of master public key (MPK) and master secret key (MSK) from a trusted authority. User’s public key is then generated by the unique identity strings and MPK, without the need to determine and manage the public key for each user. The corresponding secret key is generated by the private key generator (PKG) from the identity strings and MSK. In 2008, Gentry et al. constructed the first IBE scheme based on the learning with errors (LWE) in the random oracle model. Compared with PKE, IBE

eliminates the calculation, distribution, storage, update, management and other operations related to public key certificates, and manages keys more effectively. According to the above analysis, combining FHE and MKFHE with IBE to construct the identity-based FHE (IBFHE) scheme and multi-identity based FHE (MIBFHE) scheme seems to be beneficial. There are also many related results. About IBFHE. In 2013, Gentry et al. (GSW scheme) described a leveled FHE scheme based on LWE problem with the approximate eigenvector method. Using this FHE scheme and the IBE scheme satisfying specific properties, they also constructed the first IBFHE scheme without breaking the non-interactivity. However, this IBFHE scheme can only perform homomorphic operations on ciphertexts encrypted under the same identity. About MIBFHE. In 2014, Clear and McGoldrick constructed an MIBFHE scheme based on the in distinguish ability obfuscation (IO). The next year, they obtained a new MIBFHE scheme based on LWE problem and demonstrated its selective security in the random oracle model. In 2017, Canetti et al. used the MIBFHE scheme to construct three FHE schemes that were secure against non-adaptive chosen ciphertext attacks (CCA1) and gave two instantiated MIBFHE schemes.

However, both MIBFHE schemes have weak compactness, that is, the size of the evaluated ciphertext depends on the size of the computing circuits, but is independent of the number of users involved in the computation. In 2018, Wang et al constructed a more compact MIBFHE scheme compared to using IO and witness pseudorandom function (WPRF) which is not a standard assumption. In 2019, Shen et al used the MKFHE scheme proposed by Mukherjee and Wichs and the IBE scheme proposed by Micciancio and Peikert to construct an efficient MIBFHE scheme. In 2020, Pal and Dutta extended IBE to a CCA1 secure MIBFHE scheme using WPRF. In 2021, Shen constructed a compressible MIBFHE scheme using a new compressible ciphertext extension technique.

II. RELATED WORK

A. Sound Lock: A novel user authentication scheme for VR devices using auditory-pupillary response

Virtual Reality (VR) has shown promising potential in many applications, such as e-business, healthcare, and social networking. Rich information regarding users' activities and online accounts is stored in VR devices. If {they are} carelessly unattended, adversarial access will cause data breaches and other critical consequences. Practical

user authentication schemes for VR devices are in dire need. Current solutions, including passwords, digital PINs, and pattern locks, mostly follow conventional approaches for general personal devices. They have been criticized for deficits in both security and usability. In this work, we propose Sound Lock, a novel user authentication scheme for VR devices using auditory-pupillary response as biometrics. During authentication, auditory stimuli are presented to the user via the VR headset. The corresponding pupillary response is captured by the integrated eye tracker. User's legitimacy is then determined by comparing the response with the template generated during the enrolment stage. To strike a balance between security and usability in the scheme design, an optimization problem is formulated. Due to its non-linearity, a two-stage heuristic algorithm is proposed to solve it efficiently. The solution provides necessary guidance for selecting effective auditory stimuli and determining their corresponding lengths. We demonstrate through extensive in-field experiments that Sound Lock outperforms state-of-the-art biometric solutions with FAR (FRR) as low as 0.76% (0.91%) and is well received among participants in the user study.

B. Efficient multi-identity full homomorphic encryption scheme on lattice

Aiming at the problem that the fully homomorphic encryption scheme based on single identity cannot satisfy the homomorphic operation of ciphertext under different identities, as well as the inefficiency of trapdoor function and the complexity of sampling algorithm, an improved lattice MIBFHE scheme was proposed.

Firstly, we combined MP12 trapdoor function with dual LWE algorithm to construct a new IBE scheme under the standard model, and prove that the scheme is IND-sID-CPA security under the selective identity. Secondly, we used the eigenvector method to eliminate the evaluation key, and transform the above efficient IBE scheme into a single identity IBFHE scheme to satisfy the homomorphic operation.

Finally, we improved the ciphertext extension method of CM15 and constructed a new Link-mask system that supports the transformation of IBFHE scheme under the standard model, and then, converted the above IBFHE scheme into MIBFHE scheme based on this system. The comparative analysis results showed that the efficiency of this scheme is improved compared with

similar schemes in the trapdoor generation and preimage sampling, and the dimension of lattice and ciphertext size are significantly shortened.

C. Secure and efficient multi-key FHE scheme supporting multi-bit messages from LWE preserving non-interactive decryption

We consider *multi-key fully homomorphic encryption* (multi-key FHE) which is the richest variant of fully homomorphic encryption (FHE) that allows complex computation on encrypted data under different keys. Since its introduction López-Alt et al. (On-the-fly multiparty computation on the cloud via multikey fully homomorphic encryption. In: Proceedings of the forty-fourth annual ACM symposium on Theory of computing, pp 1219–1234. ACM, 2012), numerous proposals have been presented yielding various improvements in security and efficiency. However, most of these multi-key FHE schemes encrypt a single-bit message. Constructing a multi-key FHE scheme encrypting multi-bit messages have been notoriously difficult without losing efficiency for homomorphic evaluation and ciphertext extension under additional keys. In

this work, we study multi-key FHE that can encrypt multi-bit messages. Motivated by the goals of improving the efficiency, we propose a new construction with non-interactive decryption and security against chosen-plaintext attack (IND-CPA) from the standard *learning with errors* (LWE) assumption. We consider a binary matrix as plaintext instead of a single-bit. Our approach supports efficient homomorphic matrix addition and multiplication. Another interesting feature is that our technique of extending a ciphertext under additional keys yields significant reduction in the computational overhead. More interestingly, when contrasted with the previous multi-key FHE schemes for multi-bit messages, our candidates exhibit favourable results in the length of the secret key, public key and ciphertext preserving non-interactive decryption.

D. Levelled multi-hop multidentate fully homomorphic encryption

Gentry, Sahai, and Waters (CRYPTO 2013) proposed the notion of multi-identity fully homomorphic encryption (MIFHE), which allows homomorphic evaluation of data encrypted under multiple identities. Subsequently, Clear and McGoldrick (CANS 2014, CRYPTO 2015) proposed leveled MIFHE candidates. However, the proposed

MIFHE is either based on $i\mathcal{O}$, which is a nonstandard assumption or single hop; that is, an arbitrary “evaluated” ciphertext under a set of identities is difficult to further evaluate when new ciphertexts are encrypted under additional identities. To overcome these drawbacks, we propose a leveled multi-hop MIFHE scheme. In a multi-hop MIFHE scheme, one can evaluate a group of ciphertexts under a set of identities to obtain an “evaluated” ciphertext, which can be further evaluated with other ciphertexts encrypted under additional identities. We also show that the proposed MIFHE scheme is secure against selective identity and chosen-plaintext attacks (IND-sID-CPA) under the learning with errors (LWE) assumption.

III. PROPOSED METHODOLOGY

The proposed system, has introduced multi-identity based fully homomorphic encryption (MIBFHE) scheme to solve the existing problem or issues in cloud computing. Here we are Combining multi-key fully homomorphic encryption (MKFHE) and identity-based encryption (IBE) to construct multi-identity based fully homomorphic encryption (MIBFHE). Here, Identity-based encryption (IBE) is another cryptographic primitive that was first proposed by Shamir. Its central idea is to generate a pair of master

public key (MPK) and master secret key (MSK) from a trusted authority.

The analysis results show that our MIBFHE scheme can generate the extended ciphertext directly from the encryption algorithm.

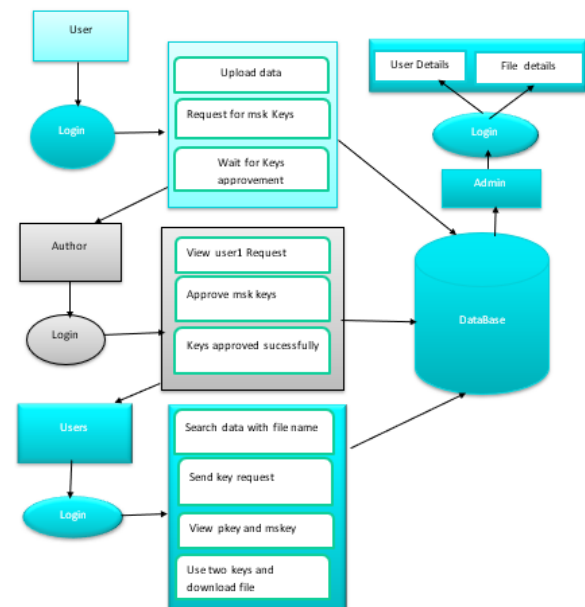
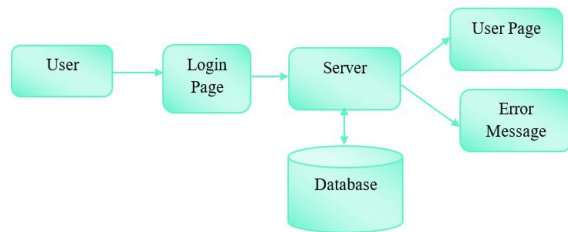


Fig. 1: System Overview

1. User Interface Design

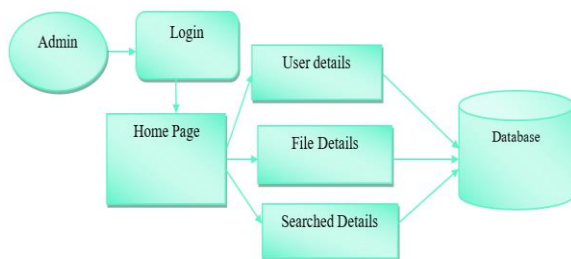
To connect with server user must give their username and password then only they can able to connect the server. If the user already exists directly can login into the server else user must register their details such as username, password, Email id, City and Country into the server. Database will create the account for the entire user to maintain upload and download rate. Name will be set as user id. Logging in is usually used to enter

a specific page. It will search the query and display the query.



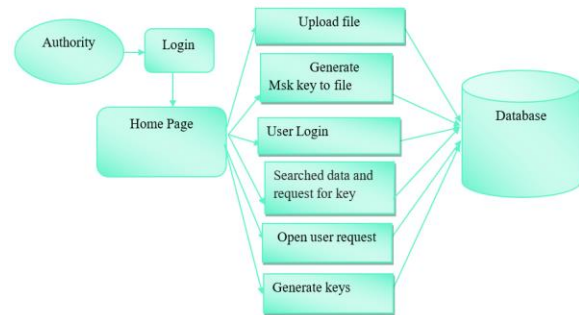
2. Admin

This is the third module in our project where Admin Controls all the of the project role. Administration managers ensure an organization's activities run smoothly and efficiently. The primary goals of an administration manager are to direct, control and supervise the support services of the organization to facilitate its success.



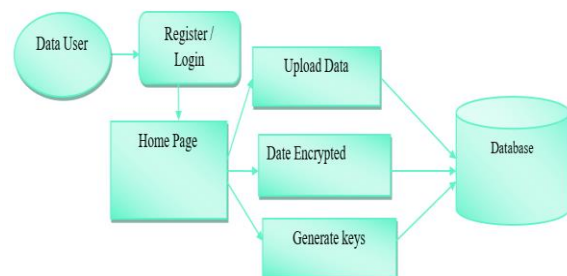
3. Authority

Hospital is the third module in our project, Authority first login with Username and password then view User request for key and generate master secrete key (MSK). When user uploads a file the for that file should generate msk key, that is done by trusted authority.



4. Data User

This is the fourth module in our project where data user plays the main part of the project role. User register and then login in to the application, the registration details are stored inside database. After User Login he will directly navigate user home page and Upload data. When data user upload data the data will be encrypted the encrypted keys will be stored inside database.



5. Search

This is the fourth module in our project where data user plays will search data with keyword. User register and then login in to the application, the registration details are stored inside database. After user Login he

will directly navigate user home page and search for with file name.



IV. EXPERIMENTAL RESULTS AND ANALYSIS

The experimental results show that the proposed MIBFHE scheme achieves lower computational complexity and improved efficiency compared to existing multi-identity homomorphic encryption methods. The scheme reduces the noise expansion rate from a polynomial function to a constant factor and decreases the size of auxiliary ciphertexts from $\tilde{O}(n^4L^4)$ to $\tilde{O}(n^2L^4)$. It also generates extended ciphertexts directly during encryption, eliminating the need for fresh ciphertext generation.

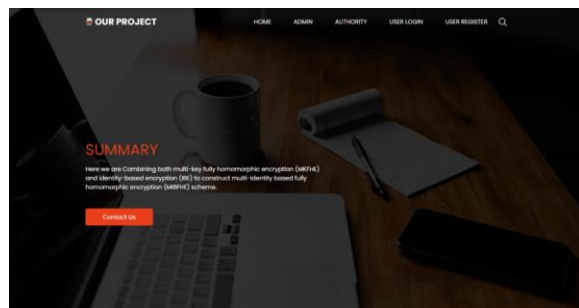


Fig. 2: Home Page



Fig. 3: Authority Login

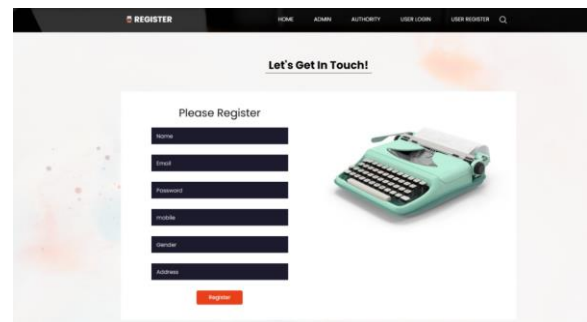


Fig. 4: Registration

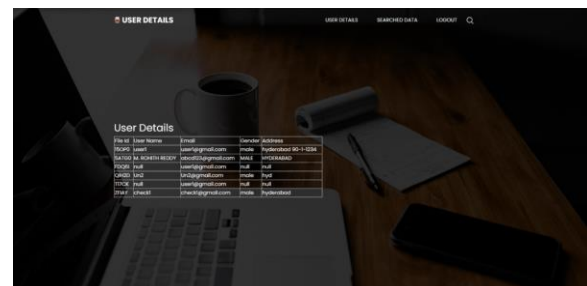


Fig. 5: User Details

V. CONCLUSION

We construct an MKFHE scheme using a new method (the decomposition method) and then construct an MIBFHE scheme, which provides a new idea and reference for cryptographers to study FHE. We tried to extend our MIBFHE scheme to multi-hop scenarios, but if the number of users is not

fixed, how to use “the decomposition method” in this paper to extend the evaluated ciphertexts still needs a better solution. Although the existing multi-hop MKFHE scheme can achieve this goal, the scheme construction is too complicated. How to construct a more concise and efficient multi-hop MIBFHE scheme still needs more research.

REFERENCES

- [1] R. L. Rivest, L. Adleman, and M. L. Dertouzos, “On data banks and privacy homomorphisms,” *Found. Secure Comput.*, vol. 4, no. 11, pp. 169–180, 1978.
- [2] C. Gentry, “Fully homomorphic encryption using ideal lattices,” in *Proc. 41st Annu. ACM Symp. Theory Comput. (STOC)*, Bethesda, MD, USA, 2009, pp. 169–178.
- [3] C. Gentry, A. Sahai, and B. Waters, “Homomorphic encryption from learning with errors: Conceptually-simpler, asymptotically-faster, attribute-based,” in *Advances in Cryptology–(CRYPTO)*. Berlin, Germany: Springer, 2013, pp. 75–92.
- [4] J. Alperin-Sheriff and C. Peikert, “Faster bootstrapping with polynomial error,” in *Advance in Cryptology–(CRYPTO)*. Santa Barbara, CA, USA: Springer, 2014, pp. 297–314.
- [5] A. López-Alt, E. Tromer, and V. Vaikuntanathan, “On-the-fly multiparty computation on the cloud via multikey fully homomorphic encryption,” in *Proc. 44th Annu. ACM Symp. Theory Comput. (STOC)*, May 2012, pp. 1219–1234.
- [6] M. Clear and C. McGoldrick, “Multi-identity and multi-key leveled FHE from learning with errors,” in *Advances in Cryptology–(CRYPTO)*, vol. 9216. Berlin, Germany: Springer, 2015, pp. 630–656.
- [7] P. Mukherjee and D. Wichs, “Two round multiparty computation via multikey FHE,” in *Advances in Cryptology–(EUROCRYPT)*, vol. 9666. Berlin, Germany: Springer, 2016, pp. 735–763.
- [8] C. Peikert and S. Shiehian, “Multi-key FHE from LWE, revisited,” in *Theory of Cryptography–(TCC)*, vol. 9986. Berlin, Germany: Springer, 2016, pp. 217–238.
- [9] Y. Huang, K. Wu, and M. Chen, “Fully dynamic multi-key FHE without Gaussian noise,” *IEEE Access*, vol. 9, pp. 50639–50645, 2021.

- [10] P. Ananth, A. Jain, Z. Jin, and G. Malavolta, “Multi-key fullyhomomorphic encryption in the plain model,” in Theory of Cryptology–(TCC), vol. 12550. Raleigh, NC, USA: Springer, 2020, pp. 28–57.

AUTHORS Profile



Mrs. ROJARAMANI ADAPA, received M.Tech (CSE) from JNTUH. She has teaching experience 20 yrs and has guided many

undergraduate and post graduate projects. She has published about 10 research articles in peer reviewed journals and presented 5 research papers at various National Conferences. At present she is working as Asst. Prof. in CSE Department at Guru Nanak Institutions Technical Campus, Ibrahimpatnam, Telangana, India.



Ms. KALLAM YESHASRI pursuing B.Tech degree in Computer Science and Engineering at Guru

Nanak Institutions Technical Campus affiliated to JNTUH in 2022-2026.



Mr. GOSULA SATHWIK pursuing B.Tech degree in Computer Science and Engineering at Guru

Nanak Institutions Technical Campus affiliated to JNTUH in 2022-2026.



Mr. RAPARTHI THARUN pursuing B.Tech degree in Computer Science and Engineering at Guru

Nanak Institutions Technical Campus affiliated to JNTUH in 2022-2026.