ISSN- 2394-5125 VOL 6, ISSUE 07, 2019

Examining expressive attribute-based encryption with lattices

[1]*Dr. J Rajaram Associate Professor,*
drrajaram81@gmail.com,
[2]*D Navya Assistant Professor,*
dubbaka.navya@gmail.com,
[3]*Bandam Naresh Assistant Professor,*
nareshbandam4@gmail.com,
[4]*Banothu Usha Assistant Professor,*
banothuusha@gmail.com,
Department of CSE Engineering,
Pallavi Engineering College,
Kuntloor(V),Hayathnagar(M),Hyderabad,R.R.Dist.-501505.

Abstract

Encryption based on attributes Using the internet to store data is known as cloud Expressiveness Control of access at the granular level Cryptography based on lattices Fine-grained access control over encrypted data may be enforced using Attribute Based Encryption (ABE). ABE schemes are presently used in cloud computing and storage systems because of their expressiveness. Quantum cryptanalysis can break down conventional ABE systems based on bilinear pairing, whereas ABE methods based on lattices are impervious to quantum assaults. Using the lattice framework, we investigate the expressiveness, complexity assumptions, efficiency, and security of a wide variety of attribute-based encryption algorithms in great detail. Also discussed are lattice-based attribute-based encryption algorithms that need additional investigation in order to outline future paths for cryptographers.

Introduction

A classic public key encryption system encrypts data before it is sent to a specified recipient who can decode it and retrieve the plaintext message, which is suitable for sensitive information transmissions and storagecapable in the event that the recipient's identity is knownwhen the data are encrypted, by the sender However, there are exceptions to this rule.situations in which the data owner may choose to disclosethe users according to a predetermined policythe qualifications of those involved.It was suggested by Sahai and Waters [1] in 2005 that Attribute Based En-Encryption (ABE) to satisfy the above-mentioned needsinitially. The private key and the public key are the same in this system.Attribute sets and private ciphertext are linked to each other.the ciphertext can only be decrypted by the key if and only if there is a matchwith respect to private key characteristics and ci-phertext. Error-tolerant encryption may be achieved using this method.May be used to implement finely grained access controls using biometricscontrol of encrypted data access as well. In spite of this, the absenceThe scheme's capacity to articulate itself restricts its use to a singlesystems. Cryptographers have devised methods to increase the expressiveness oftwo different types of attribute-based encryptionA private key or a public key is related with the access policy.key policy attribute-based encryption (KP-ABE) is the method used to encrypt this data.As well as Ciphertext Policy Attribute Based Encryption (CP-ABE)In the first case, the attribute set is linked to a ciphertext,Access policies are related with a private key's use. Notwithstanding this,the situation is inverted in the latter: It is linked to the private key.access is granted to the ciphertext with the attribute set.policy. If and only if the decryption is successful in both settings,access policy is satisfied by attribute set. The KP-ABE described aboveThe usual situation includes CP-ABE schemes and CP-ABE programmes.Because they are issued by a single body, private keys are useful fordata management inside a single trust domainor group of people. But in many cases, data is required.in accordance with an agreement that covers many companiesareas of trust and confidence. Multi-authority is required to satisfy the criterion.Multiple parties may use attribute-based encryption techniques.It is suggested that you participate in a position of authority [11–14].There are two types of attribute-based encryption schemes:An attribute-based encryption system for a tiny universe and[14–16] in the big universe attribute-based encryptionhow the attribute universe is defined In the first case, the qualities are listed.the size of the attribute space is polynomial and fixed upon setupally constrained by the specified security constraint Furthermore, the general population is aware of this.The size of a parameter is proportional to the number of characteristics.The size of the attribute universe is enormous in the second case.It is possible to use any string as an attribute, and there is no requirement to

ISSN- 2394-5125 VOL 6, ISSUE 07, 2019

list them.Added properties to the system when it was first installed. Waters, Rouselakis, anda large-world attribute-based encryption systemThe typical model uses a prime order bilinear map. Notwithstanding this,Their encryption method, decryption time, and ciphertext size all increase linearly.access structure is more complicated. The issues may be resolved by:Access to the large-universe attribute set was suggested by Fu and colleagues [16].Control in the cloud storage system with efficient decryption. BothAmong the many attributes of a huge cosmos, schemes [15,16] have the exclusive authority.based methods of data encrypting The proposal by Rouselakis and Waters [14]A multi-authority attribute-based encryption technique for a broad area of spaceAs a result of the lack of security provided by the random oracle,This includes all of the above-mentioned attribute-based encryption methodson the elliptic curve bilinear pairing, whichcomputers can withstand traditional computer assaults, but cannot withstand newer threats.Attacks by a quantum computer. Once upon a time, Shor [17] noted,The tum computer is constructed, using number theoretic security as its foundation.assumption that discrete logarithm probabilities are intractablesolving and factoring huge integers might be a challenge for lembreakage in polynomial time with probability. Cryptography based on latticesraphy can withstand both conventional and quantum computer assaults.assaults on computers

ι	KeyGen	Encrypt	$Eval_{PK} + Eval_{CT}$	Decrypt
2	153.2	21.2	98 + 86.4 = 184.4	1.31
4	163	32.2	282.4 + 263.8 = 546.2	1.444
8	168.6	43.8	637 + 588.4 = 1225.4	1.6154

(ι, b)	KeyGen	Encrypt	Decrypt
(6, 2)	214.4	65.4	1.8
(6, 1024)	50	10.2	0.2
(8, 2)	259.6	87.4	2.4
(8, 1024)	60.4	16.8	0.3
(16, 2)	454.8	171.6	5.4
(16, 1024)	95	32.2	0.6
(20, 2)	588.4	227	5.6
(20, 1024)	116.6	40.6	1.8
(32, 2)	902.6	345.4	9
(32, 1024)	178.6	67.8	2

Table 9

Execution times (ms) of ciphertext policy attribute basedencryption for different bases from lattices

Our Contributions.

The degree to which they represent information and the assumptions made about their complexity and efficiency are only a few of the elements we examine while investigating attribute-based encryption algorithms based on lattices. They're already here. ice and ci encryption schemes Multi-authority attribute-based encryption systems based on lattices for encrypting a substantial chunk of the cosmos with encrypted pheromones Tracing a traitor utilising lattices and a tribute system in addition to completely homomorphic encryption chemes. Consider, for example, the following: comparative assessments of the many aspects, designs, and implementations of these plans and the future research paths that should be explored;

Organizations

According to the following structure, the rest of this paper is arranged: Section 2 covers the preliminaries. An attribute-based encryption taxonomy from lattices is shown here. Section 3 In Section 4, we compare the features of attribute-based encryption techniques based on lattices. We discuss typical constructions of attribute-based encryption algorithms based on latticesin. Section 5: Section 6 presents results from simulations of attribute-based encryption algorithms based on lattices. Section 7 outlines future research directions. Section 8 is where we come to our findings.

2. Preliminaries

Lattices, complexity assumptions, learning with errors (LWE), and ring-learning with mistakes are covered in this section (R-LWE). Lattice-based attribute-based encryption methods use them.

2.1. Basics of lattices

Lattice is a set of points with a periodic structure. The latticegenerated by n-linearly independent vectors b1,

ISSN- 2394-5125 VOL 6, ISSUE 07, 2019

bn ∈ Rm is2

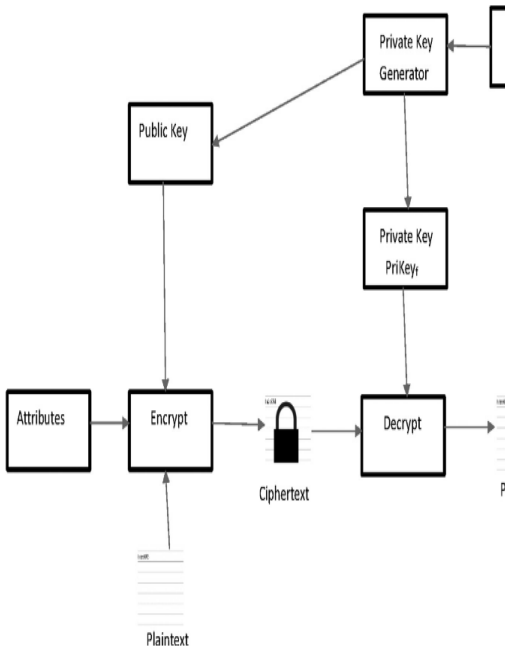

Fig. 1.Key Policy Attribute Based Encryption from Lattices.

On the premise of learning with errors and quasi-polynomial approximation factors, it is safe. Gorbunov et al. [26] demonstrated an effective key policy attribute-based encryption for branching programmes. Using polynomial approximation factors, this system's security is built on the idea that learning errors may be utilised to shrink private keys. First, Dai et al. created and analysed encryption using key policy attribute lattices for the first time [27]. More efficient than the previous one, which relied on learning from errors [25], this team of researchers came up with a novel attribute-based encryption method [27]. Because of the homomorphism between their scheme's public key and encrypted data, they are able to protect their data. Lattice-based ciphertext encryption with policy attribute synchronisation Figure 2's lattices employ a private key to tie characteristics to access policy, which is shown in the figure. When data is encrypted by the data owner, ciphertext policy attribute-based encryption enables for fine-grained access control in the cloud storage systems that utilise this kind of encryption. Lattice-based ciphertext policy attribute encryption was initially proposed by Zhang et al. [28]. Assuming that learning happens via errors, their method supports flexible threshold access limits on literal (or boolean) features. Gür and colleagues [29] built and analysed ciphertext policy attribute based encryption fromlattices based on the ring learning with errors assumption. A Gaussian sampling method may be used to reduce both execution time and storage space requirements for non-binary bases of the gadget matrix. Tsabary proposed an adaptively secure ciphertext strategy based on attributes for t-CNF from LWE. As a result, the three systems [28–30] lack expressiveness. Agrawal and Yamada first the idea of attribute-based encryption in [31]. Unlike the previous scheme, the foundation of this one is laid forth in one single tenet. Circuits may be encrypted using the CP-ABE approach developed by Vaikuntanathan [32] for ciphertext size to be determined by the depth of the underlying policy circuits. On the other hand, their strategy isn't foolproof. In the case of symmetric keys, Agrawal and Yamada proposed CP-ABE, or ciphertext-policy attribute-based encryption. Some downsides exist, such as the absence of a stable framework. Datta et al. [34] hypothesised that the first secure CP-ABE system based on the LWE assumption might allow rules of access in NC. Despite the fact that it is less efficient than existing models, however, KeyGen, Encrypt, EvalPK + EvalCT, and Decrypt all scale with the amount of characteristics that may be generated. Using the PALISADE Library [46] on an Intel Corei7-9750H@CPU2.60 GHz running Ubuntu 18.04 TLS, we were able to measure the execution times (in milliseconds) of ciphertext policy attribute-based en-cryption [29]. Table 9 shows that the execution times (ms) of KeyGen, Encrypt, and Decrypt scale with the amount of characteristics, while the base decreases.

Future research directions

We analyze different attribute based encryption schemes fromlattices in terms of expressiveness, complexity assumptions, effi-ciency, security and so on. Attribute based encryption schemesfrom lattices deserving further research can be carried out asfollows:

Future research directions

For example, we look at the expressiveness, scalability, efficiency, and security of a variety of attribute-based encryption algorithms. Research on attribute-based encryption systems using lattices may be carried out in the following ways. Efficiency of

ISSN- 2394-5125 VOL 6, ISSUE 07, 2019

lattice-based attribute-based cryptography Currently, most lattice-based attribute encryption is inefficient since it relies on LWE, making it difficult to put into reality. A lattice-based attribute-based encryption technique may be made more efficient: RLWE. a Except for two attribute-based encryption techniques [27,29], the security of all standard lattice-based encryption relies on ring learning with errors assumption. Due to the inherent quadratic cost in the usage of LWE, attribute-based encryption from lattices is relatively inefficient. Attribute-based encryption from lattices based on ring learning with mistakes assumption is more efficient and may be used to create fine-grained access control over encrypted data in reality. b. Lattice-based attribute-based offline-online encryption methods A lattice-based attribute-based encryption system may be a barrier for particular applications, such as mobile cloud computing, since the computation costs for private key generation and encryption rise with the complexity of circuits or the number of attributes. Two distinct models may be used: an offline phase that does the bulk of calculation before any data is available, and an online phase that performs the data-gathering process quickly. [46] [29] [46] [27,29] Data are assembled into an ABE ciphertext by X. Fu, Y. Ding, H. Li and others in Computer Science Review 43 (2022) 100438. An outstanding topic, however, is the design and implementation of offline–online attribute-based encryption algorithms from lattices. the use of lattices for decryption of attribute-based encryption systems the decryption time scales with circuit complexity in attribute-based encryption methods from lattices. When attribute-based encryption systems are decrypted using lattices, the burden on the user is reduced. It remains an open question, however, how to develop and deploy outsourced decryption systems based on attribute encryption from lattices the constant ciphertext from lattices in attribute-based encryption methods For lattice attribute-based encryption, the size and number of attributes influences the performance of encryption and decryption as a function of circuit complexity and key size. Nevertheless, how to create attribute-based encryption methods from lattices with constant ciphertext and constant private key is still an issue to be solved. 7.2. Lattice-based revocation in attribute-based encryption schemes In practise, it is necessary to have both user revocation and attribute revocation, since the latter allows for more precise revocation. There are two main security needs that must be met: security for forward and security for backward. Revocation of the private key does not allow the revoked user to view the later released ciphertext. It is possible for a new user to read the previously released ciphertext if its characteristics meet the access structure. Backward security assures this. There are three ways to re-energise yourself: A revocation is predicated on the re-encryption of the proxy's encryption. 2. a broadcast encryption-based revocation. third-party algorithm for revoking privileges How to create lattice-based attribute encryption schemes with effective revocation remains an unresolved question. From lat-tices, attribute-based encryption methods may be updated with circuit changes Alterations to the lattice's circuit may occur over time in attribute-based encryption methods So the circuit has to be reworked or replaced. The cloud storage server should be used to execute circuit updates in order to increase efficiency and assure security. Attribute-based encryption techniques from lattices with efficient circuit updates are still an open question. Lattice key escrow in attribute-based encryption systems There must be total faith in the attributes authority in order for attribute-based encryption techniques from lattices such as these to work. A key escrow issue in attribute-based encryption systems from lattices is yet unsolved, but For circuits, 7.5. Ciphertext policy attribute-based encryption The only ciphertext policy attribute-based encryp-tion techniques now available are for Boolean formulae and rely on lattice-based encryption. It remains an open question, however, how to build attribute-based encryption schemes for all polynomial time predicates without universal circuit transformation from key policy attribute-based encryption schemes from lattices. 3.3. Lattice-based multi-authority attribute encryption In the lattice-based multi-authority attribute encryption shown in Figure 3, the sender may wish to offer an access policy that covers several trust domains. As an example, a partnership between Huawei and Alibaba might lead to the release of characteristics. This means that one organisation will have to give up power to another if a single authority system is utilised. Zhang, Qin, and Qazi [35] proposed multi-authority attribute-based encryption based on lattices. Nevertheless, the central authority of their scheme needs the establishment of a trustworthy single point of failure. Based on the idea that individuals learn from their failures, they also use an ineffective strategy that is not very effective. Rahman, Basu, and Kiyomoto [36] devised decentralised ciphertext policy attribute-based encryption to overcome these problems. Their system, which is based on ring-learning and errors accepted for efficiency, has no

ISSN- 2394-5125 VOL 6, ISSUE 07, 2019

central authority. Datta et al. [34] originally proposed a multi-authority CP-ABE system that supports access restrictions given by DNF equations under the LWE assumption. The predicate0073 of polynomial time is not supported by [34–36] since they employ a secret sharing access method.

Conclusions

An attribute-based encryption system from lattices is examined in terms of expressiveness, complexity assumptions and efficiency and security. Attribute-based encryption algorithms from lattices are compared, and their constructions are given, as well as their performance assessments and research goals.

References

[1] A. Sahai, B. Waters, Fuzzy identity based encryption, in: Cramer, Ronald(Eds.), Eurocrypt 2005, Springer, Denmark, 2005, pp. 457–473.

[2] V. Goyal, O. Pandey, A. Sahai, B. Waters, Attribute-based encryption forfine-grained access control of encrypted data, in: Ari Juels (Ed.), CCS 2006,ACM, USA, 2006, pp. 89–100.

[3] R. Ostrovsky, A. Sahai, B. Waters, Attribute-based encryption with non-monotonic access structures, in: Peng Ning (Ed.), ACM Conference onComputer and Communications Security, ACM, Alexandria, Virginia, USA,,2007, pp. 195–203.

[4] J. Bethencourt, A. Sahai, B. Waters, Ciphertext-policy attribute-based en-cryption, in: Tsudik, Gene (Eds.), IEEE Symposium on Security and Privacy,IEEE, USA, 2007, pp. 321–334.[5] A. Lewko, B. Waters, Decentralizing attribute-based encryption, in: Pa-terson, Kenneth G. (Eds.), EUROCRYPT 2011, Springer, Estonia, 2011, pp.568–588.

[6] S. Müller, S. Katzenbeisser, C. Eckert, Distributed attribute-based encryp-tion, in: Lee, PilJoong, Cheon, Jung Hee (Eds.), ICISC 2008, Springer, Korea,2008, pp. 20–36.

[7] L. Cheung, C.C. Newport, Provably secure ciphertext policy abe, in: PengNing (Ed.), CCS 2007, ACM, USA, 2007, pp. 456–465.[8] R. Ostrovsky, A. Sahai, B. Waters, Attribute-based encryption with non-monotonic access structures, in: Peng Ning (Ed.), CCS 2007, ACM, USA,2007, pp. 195–203.

[9] V. Goyal, A. Jain, O. Pandey, A. Sahai, Bounded ciphertext policy attribute-based encryption, in: Luca Aceto (Ed.), ICALP, Springer, Iceland, 2008, pp.579–591.

[10] B. Waters, Ciphertext-policy attribute-based encryption: An expressive,efficient, and provably secure realization, in: Dario Catalano (Ed.), PKC2011, Springer, Italy, 2011, pp. 53–70.

[11] M. Chase, Multi-authority attribute based encryption, in: KNAWTrippenhuis (Ed.), TCC, Amsterdam, The Netherlands, 2007, pp. 515–534.

[12] M. Chase, S.S.M. Chow, Improving privacy and security in multi-authority attribute-based encryption, in: ACM Conference on Computerand Communications Security, ACM, 2009, pp. 121–130.

[13] A.B. Lewko, B. Waters, Decentralizing attribute-based encryption, in:EUROCRYPT, Springer, 2011, pp. 568–588.[14] Y. Rouselakis, B. Waters, Efficient statically-secure large-universe multi-authority attribute-based encryption, in: Financial Cryptography, 2015, pp.315–332.

[15] Y. Rouselakis, B. Waters, Practical constructions and new proof methodsfor large universe attribute-based encryption, in: ACM Conference onComputer and Communications Security, ACM, 2013, pp. 463–474.

[16] X. Fu, X. Nie, T. Wu, F. Li, Large universe attribute based access controlwith efficient decryption in cloud storage system, J. Syst. Softw. 135 (2018)157–164.

[17] P.W. Shor, Polynomial-time algorithms for prime factorization and discretelogarithms on a quantum computer, SIAM J.Comput. (1997) 1484–1509.

[18] C. Peikert, A Decade of Lattice Cryptography, 2015.

[19] B. A., Secure Schemes for Secret Sharing and Key Distribution, (Ph.D.thesis), Israel Institute of Technology, Israel, 1996.

[20] Z. Jafargholi, A. Scafuro, D. Wichs, Adaptively indistinguishable garbledcircuits, in: Proceedings of TCC, 2017.] W. Dai, Y. Doröz, Y. Polyakov, K. Rohloff, H. Sajjadpour, E. Savas, B. Sunar,Implementation and evaluation of a lattice-based key-policy ABE scheme,IEEE Trans. Inf. Forensics Secur. 13 (5) (2018) 1169–1184.

[21] J. Zhang, Z. Zhang, A. Ge, Ciphertext policy attribute-based encryption fromlattices, in: AsiaCCS, 2012, pp. 16–17.

[22] K.D. Gür, Y. Polyakov, K. Rohloff, G.W. Ryan, H. Sajjadpour, E. Savas,Practical applications of improved Gaussian sampling for trapdoor lattices,2017, IACR Cryptology EPrint Archive.

[23] R. Tsabary, Fully secure attribute-based encryption for t-CNF from LWE,in: CRYPTO 2019, 2019, pp. 62–85.

[25] S. Agrawal, S. Yamada, Optimal broadcast encryption from pairings andLWE, in: EUROCRYPT, 2020, pp. 13–43.

[26] Z. Brakerski, V. Vaikuntanathan, Lattice-inspired broadcast encryption andsuccinct ciphertext-policy ABE, 2020, IACR Cryptology EPrint Archive2020/191.

[27] S. Agrawal, S. Yamada, Cp-ABE for circuits (and more) in the symmetrickey setting, in: TCC, 2020, pp. 117–148.

[28] P. Datta, I. Komargodski, B. Waters, Decentralized multi-authority ABE forDNFs from LWE, in: EUROCRYPT, 2021, pp. 177–209.

[29] G. Zhang, J. Qin, S. Qazi, Multi-authority attribute-based encryption schemefrom lattices, J. Univers. Comput. Sci. 21 (3) (2013) 483–501.

[30] M.S. Rahman, A. Basu, S. Kiyomoto, Decentralized ciphertext-policy

attribute-based encryption: A post-quantum construction, J. Internet Serv.Inf. Secur. 7 (3) (2017) 1–16.

[31] S. Wang, F. Feng, Large universe attribute-based encryption scheme fromlattices, CoRR abs/1405.3394, 2014.

[32] Z. Brakerski, V. Vaikuntanathan, Circuit-ABE from LWE: Unboundedattributes and semi-adaptive security, in: CRYPTO, 2016, pp. 363–384.

[33] S. Agrawal, M. Maitra, S. Yamada, Attribute based encryption (and more)for nondeterministic finite automata from LWE, in: CRYPTO 2019, 2019pp. 765–797.

[34] C. Gentry, A. Sahai, B. Waters, Homomorphic encryption from learningwith errors: Conceptually-simpler, asymptotically-faster, attribute-based,in: CRYPTO, 2013, pp. 75–92.

[35] Z. Brakerski, D. Cash, R. Tsabary, H. Wee, Targeted homomorphic attributebased encryption, 2016, IACR Cryptology EPrint Archive 2016, 691.

[36] R. Goyal, V. Koppula, B. Waters, Collusion resistant traitor tracing fromlearning with errors, in: STOC, 2018, pp. 660–670.

[37] Y. Chen, V. Vaikuntanathan, B. Waters, H. Wee, D. Wichs, Traitor-tracingfrom LWE made simple and attribute-based, in: TCC, vol. 2, 2018, pp.341–369.