Ameliorated Approach to Search over Cipher Data in Cloud Computing

Prof. GOWRISHANKAR[1], POOJA G[2]

[1]Dept of CSE, BMS College of Engineering, Bangalore.
[2]M.Tech Student, Dept of CSE, BMS College of Engineering, Bangalore.

***

ABSTARCT: *With the prevalence of the Internet and the widespread application of cloud computing technology, personal privacy information often undergoes massive transmission via channels such as computer networks and public communication devices. Public key encryption with keyword search (PEKS) allows a cloud server to retrieve particular ciphertexts without leaking the contents of the searched ciphertexts. This kind of cryptographic primitive gives users a special way to retrieve the encrypted documents they need while preserving privacy. Nevertheless, most existing PEKS schemes only offer single-keyword search or conjunctive-keyword search. The poorly expressive ability and constantly inaccurate search results make them hard to meet users' requirements. Although several expressive PEKS (EPEKS) schemes were proposed, they entail high computation and communication costs. we propose an expressive public-key searchable encryption scheme in the prime-order groups, which allows keyword search policies (i.e., predicates, access structures) to be expressed in conjunctive, disjunctive or any monotonic Boolean formulas and achieves significant performance improvement over existing schemes. We formally define its security, and prove that it is selectively secure in the standard model. Also, we implement the proposed scheme using a rapid prototyping tool called Charm [37], and conduct several experiments to evaluate it performance. The results demonstrate that our scheme is much more efficient than the ones built over the composite-order groups*

INTRODUCTION

With the prevalence of the Internet and the widespread application of cloud computing technology, personal privacy information often undergoes massive transmission via channels such as computer networks and public communication devices. These information transmission media are unsafe yet hardly replaceable. Asymmetric cryptosystem was developed to allow people to share secret information without transmitting decryption keys. But in some cases, people need to process the encrypted information. Imagining such a situation, a user uploads a large quantity of encrypted data files to an un trusted server. Later, the user wants to fetch back some certain files from the server. How could the server pick out the target documents from a large amount of ciphertexts? In another case, to protect personal privacy, a user sends encrypted mails to the email sever. How could the receiver of the mails tell which mails contain important contents that need urgent processing and which ones could be directly ignored? One primitive way is to download and decrypt all received emails, before being able to get the wanted information. But this will result in large communication and computation cost, hence very inefficient. To address the problem, the paradigm of public key encryption with keyword search (PEKS) [1] was invented. PEKS allows a message sender to create a searchable cipher text by attaching a keyword cipher text to the encrypted file. To execute ciphertext search, the recipient makes use of his/her private key to produce a trapdoor of the search keyword (or keywords) and then sends it to the server. The server can search the ciphertexts using the trapdoor and returns all matching files. In this process, no information (neither the contents of the searched ciphertexts nor the search keyword(s)) would be disclosed to the server. As is known to all, attribute-based encryption (ABE) has a very strong access control capability [5]. In ABE, attributes are usually administered by a single central trusted authority that awards private keys to users. Each user's private key contains information on user attributes. There are two types of ABE schemes: one is the key-policy ABE (KP-ABE), and the other is ciphertext-policy ABE (CP-ABE). In a KP-ABE, an access structure (AS) is implanted in the private key and the ciphertext has a bearing on a set of attributes. Opposite to that in KP-ABE, an access structure in a CP-ABE is implanted in the ciphertext and the private key has a bearing on a set of attributes. FIGURE 2 shows the framework of KP-ABE. In a KP-ABE scheme, the trusted center uses a logical expression of attributes (which, in FIGURE 2, is shown as a logic tree) to generate an access structure. One sound way to construct an access structure is using a linear secret-sharing scheme (LSSS). The ciphertext gets decrypted only when the access structure is met by the attribute set. An access structure built via LSSS could enable the KP-ABE scheme to realize access control in cases that the logical expressions of attributes contain "AND" and "OR". This paper proposes a generic construction of EPEKS from KP-ABE and gives an efficient EPEKS scheme over the prime-order groups.

RELATED WORKS

In [6], Song came up with the concept of searchable encryption and exhibited a specific scheme under symmetric key system. Boneh et al. [1] gave the first PEKS scheme in 2004 and proposed a generic construction of PEKS from identity-based encryption (IBE). Since then, many scholars have proposed lots of improved PEKS schemes to enhance the scheme performance or security [7-20]. To improve search accuracy when using search engines, users are more likely to search several keywords rather than a single keyword. Multi-keyword search is also needed for retrieving ciphertext.

Golle et al. [21] constructed a searchable symmetric encryption scheme with conjunctivekeyword search. In the scheme, every document has several keyword domains and each keyword domain has a keyword to represent a feature. The communication cost changes linearly with the number of keyword domains and the feature representation is not flexible enough due to constraints by keyword domains. Park et al. [2] gave the first PEKS scheme supporting conjunctive-keyword search. Based on Park et al.'s works, further efforts were made to reduce computation cost and trapdoor size [22-25].

EPEKS has attracted widespread concern in the domain of searchable encryption because of its strong search function. Lai et al. [3] put forward the first EPEKS scheme on the basis of a completely secure KP-ABE scheme [26]. Lai et al.'s scheme is established over the composite-order groups. Hence, its computation cost is high and the length of the ciphertext and that of the trapdoor are both linear to the keyword number. Lv et al. [4] proposed the first expressive PEKS scheme supporting "AND", "OR" and "NOT". This scheme is also over the composite-order groups and hence inefficient. In 2016, Cui et al. [27] embedded the LSSS structure into keyword search and, for the first time, implemented an EPEKS scheme over the prime-order groups.

In this paper, we propose a public-key based expressive SE scheme in prime-order groups, which is especially suitable for keyword search over encrypted data in scenarios of multiple data owners and multiple data users such as the cloud-based healthcare information system that hosts outsourced PHRs from various healthcare providers.

PROPOSED APPROACH

The basic idea of our scheme is to modify a key-policy attributed-based encryption (KP-ABE) scheme constructed from bilinear pairing over prime-order groups. Without loss of generality, we will use the large universe KP-ABE scheme selectively secure in the standard model proposed by Rouselakis and Waters in [18] to illustrate our construction during the rest of the paper. In KP-ABE, a ciphertext is computed with respect to a set of attributes and an access policy is encoded into a user's private key. A ciphertext can be decrypted by a private key only if the set of attributes associated with the ciphertext satisfies the access policy associated with the private key. Access policies in [18] can be very expressive, supporting any monotonic Boolean formulas. At first sight, a KP-ABE scheme can be transformed to an expressive SE scheme by treating attributes as keywords to be searched, by directly transforming the key generation algorithm on attribute access structures to a trapdoor generation algorithm on keyword search predicates, and by using the decryption algorithm to test whether keywords in a ciphertext satisfy the predicate in a trapdoor. However, KPABE schemes (e.g., [18], [19]) are not designed to preserve privacy of attributes (keywords) associated with ciphertexts. Specifically, given the public parameter and a ciphertext, the attributes (keywords) in the ciphertext can be discerned by anyone. In the following, to keep our description compact and consistent, we will use access structure, policy and predicate interchangeably.

In order to hide keywords in a ciphertext, inspired by the "linear splitting" technique in [20], we firstly split ciphertext components corresponding to every keyword into two randomized complementary components. Thus, even though the ciphertext still contains information about the keywords, this information is computationally infeasible to obtain from the public parameter and the ciphertext. We secondly re-randomize trapdoor components corresponding to every keyword associated with an access structure to match the splitted components in the ciphertext.

MOTIVATION AND CONTRIBUTIONS

This paper focuses on the efficient construction of EPEKS from KP-ABE. KP-ABE has strong access control capacity and efficient operation performance. In a KP-ABE scheme, every user is marked by an attribute set and only users with specific attributes are authorized to decrypt a specific ciphertext. Clearly, KP-ABE makes user screening possible. Implementing such a screening process on a cloud storage sever, users can only retrieve specific files, which is exactly what EPEKS could do. This inspires us to devise a generic transformation from KP-ABE to EPEKS.

In a KP-ABE scheme, a trusted center authority generates users' private keys according to the user attributes. If the user attributes are regarded as the search keywords, then the private key generation algorithm in the KP-ABE scheme could be used to generate the trapdoors of search keywords in the EPEKS scheme. Correspondingly, the keyword ciphertexts in EPEKS could be generated by using the KPABE encryption algorithm to encrypt a random message.

The test algorithm in the EPEKS scheme could be executed by decrypting the random-message ciphertext and checking whether the decrypted message is the same as that in the original ciphertext. In so doing, the strong access control ability of KP-ABE on user screening could be inherited by the derived EPEKS scheme to screen files. However, such transformation is unsuitable to most existing KP-ABE schemes, because these schemes should attach an attribute set behind the generated ciphertext and thus don't provide any protection to the user attributes. Privacy protection of the keywords is a very important issue in the construction of EPEKS. Therefore, these KP-ABE schemes cannot be directly exploited to construct the EPEKS schemes. To protect the privacy of attributes, some anonymous ABE schemes were proposed, e.g. [34, 35]. This kind of schemes can be transformed to EPEKS directly, but they are quite inefficient. After a close examination of existing KP-ABE schemes, we find that most KP-ABE schemes could turn anonymous if the attribute sets get removed from the ciphertexts. But such removal makes the ciphertext decryption a challenging task, which also makes the test algorithm in the post-transformation EPEKS scheme ineffective. In [27], Cui et al. provided a solution to this problem, which exposes the keyword attribute names while hiding the keyword values. For example, during the production of a ciphertext with a keyword set {"job = teacher", "gender = male"}, the attribute names ("job", "gender") are attached to the ciphertext without displaying the keyword values. In this way, the privacy of keywords is preserved. Actually, in many practical retrieval systems, the search keywords are input in certain orders according to the attributes of the generic names. After inputting the search keywords, users could search for their expected documents accurately. In such context, the number and order of keywords are both pre-defined. Therefore, if the attributes (including the number and the order) of the keywords encrypted in ciphertexts are pre-defined, the keyword attribute names need not be attached to the ciphertexts.

EXPERIMENTAL RESULTS

We test two schemes on a Lenovo L440 Laptop equipped with Intel Core i7 CPU (2.3GHz) and 8GB RAM. Our operate system is Win 7 (64 bit). The PBC (Pairing-Based Cryptography)-0.5.14 library [44] is installed for cryptographic operation. The bilinear map is established on Type A pairing over the elliptic curve with 512-bit group size. FIGURE 1, 2, 3 and 4 show the experimental results. We randomly choose 2-10 keywords to generate a predicate P and get trapdoor from the P. Actually, the number of keywords in a searching query is no more than 10 in practical application. As shown in FIGURE 1, Trapdoor generation for 2, 4, 6, 8, 10 keywords in our scheme costs about 32.485ms, 59.693ms, 83.046ms, 125.338ms and 178.189ms, respectively, while that in scheme [27] is about 93.265ms, 179.731ms, 258.124ms, 349.251ms and 452.572ms, respectively. To check the time cost of the encryption algorithm, we generate different random keyword sets containing 10-50 keywords to generate the ciphertexts. As shown in FIGURE 2, our scheme costs about half of the time required by Cui et al.'s scheme [27]. The computation cost of Test algorithm is related to predicate P and the keywords used to generate SEWS. The computation time will increase as the number of keywords. in both the trapdoor and the ciphertext increases. The experimental results of two compared schemes are respectively given in FIGURE 3 and 4.

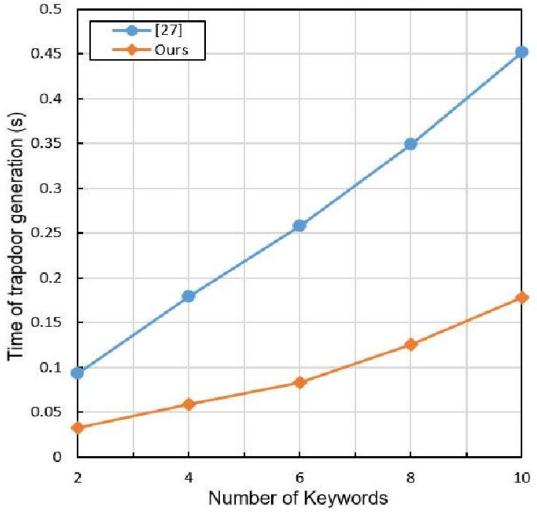


Figure 1: Computational cost of the Trapdoor algorithm

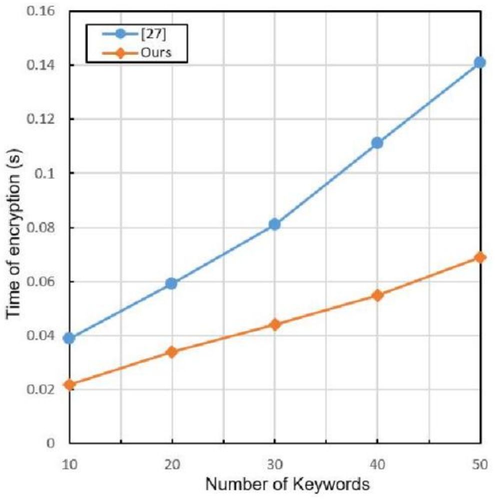
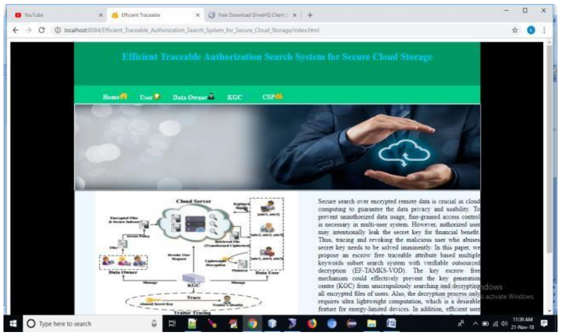


Figure 2: Computational cost of the Encryption algorithm


localhost:8084/Efficient_Traceable_Authorization_Search_System_for_Secure_Cloud_Storage/index.html

Efficient Traceable Authorization Search System for Secure Cloud Storage

Secure search over encrypted remote data is crucial in cloud computing to guarantee the data privacy and usability. To prevent unauthorized data usage, fine-grained access control is necessary in multi-user system. However, authorized user may intentionally leak the secret key for financial benefit. Thus, tracing and revoking the malicious user who abuses secret key needs to be solved imminently. In this paper, we propose an escrow free traceable attribute based multiple keywords subset search system with verifiable outsourced decryption (EF-TAMKS-VOD). The key escrow free mechanism could effectively prevent the key generation centre (KGC) from unscrupulously searching and decrypting all encrypted files of users. Also, the decryption process only requires ultra lightweight computation, which is a desirable feature for energy-limited devices. In addition, efficient user

Figure 4: User registration

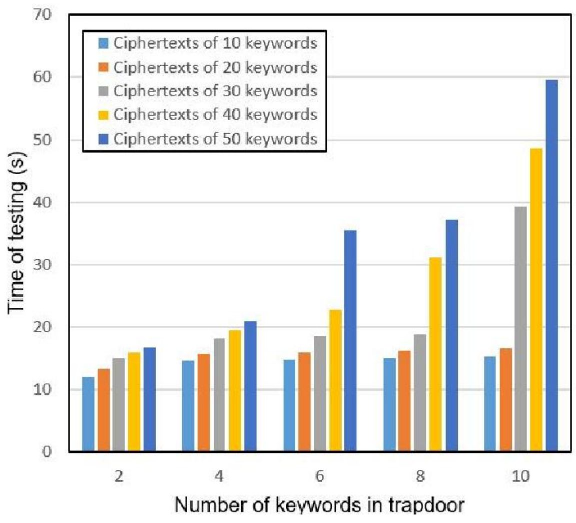
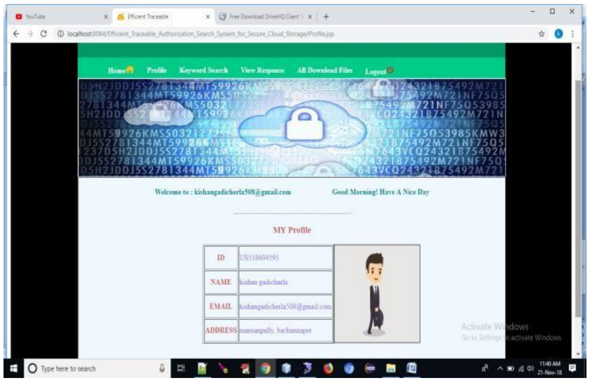


Figure 3. Computational cost of the Test algorithm in [27].

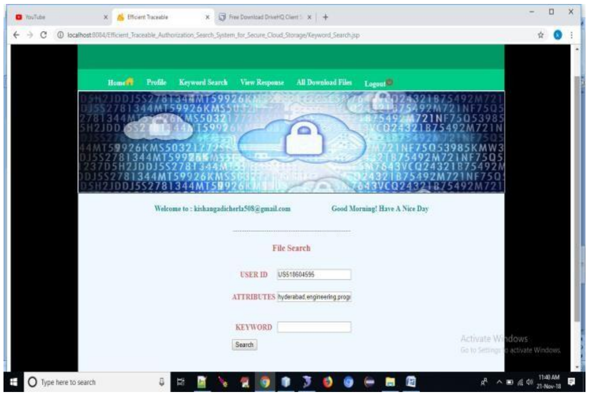

localhost:8084/Efficient_Traceable_Authorization_Search_System_for_Secure_Cloud_Storage/Profile.jsp

Welcome to : kishangadicherla508@gmail.com Good Morning! Have A Nice Day

MY Profile

ID	US518604595
NAME	kishan gadicharla
EMAIL	kishangadicherla508@gmail.com
ADDRESS	mansampally, bachannapet

Figure 5: Keyword Search


localhost:8084/Efficient_Traceable_Authorization_Search_System_for_Secure_Cloud_Storage/Keyword_Search.jsp

Welcome to : kishangadicherla508@gmail.com Good Morning! Have A Nice Day

File Search

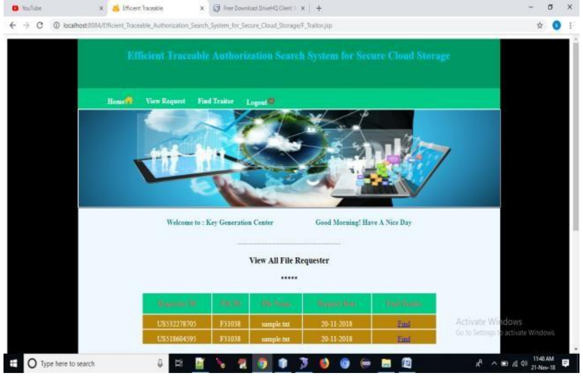
USER ID US518604595

ATTRIBUTES hyderabad,engineering,progr

KEYWORD

Search

Figure 5: Illegal request send to KGC page


localhost:8084/Efficient_Traceable_Authorization_Search_System_for_Secure_Cloud_Storage/F_Traitor.jsp

Efficient Traceable Authorization Search System for Secure Cloud Storage

Welcome to : Key Generation Center Good Morning! Have A Nice Day

View All File Requester

*****

[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
US532278705	F31038	sample.txt	20-11-2018	Find
US518604595	F31038	sample.txt	20-11-2018	Find

Figure 6: Traitor find page

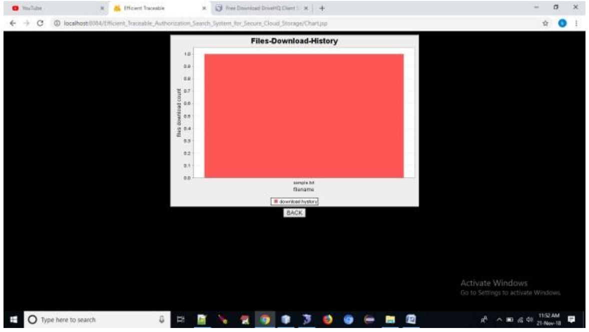


Figure 7: Chart page

CONCLUSION

An efficient concrete EPEKS scheme over the prime-order groups is given and its performance is analyzed. Yet, the EPEKS proposed in this paper only supports the logical expression of "AND" and "OR", excluding "NOT". And existing schemes that support the logical expression of "AND", "OR" and "NOT" are all based on composite-order groups, hence not quite efficient. There exist only a few public-key searchable encryption systems that support expressive keyword search policies, and they are all built from the inefficient composite-order groups [17]. In this paper, we focused on the design and analysis of public-key searchable encryption systems in the prime-order groups that can be used to search multiple keywords in expressive searching formulas. Based on a large universe key-policy attribute-based encryption scheme given in [18], we presented an expressive searchable encryption system in the primeorder group which supports expressive access structures expressed in any monotonic Boolean formulas. Also, we proved its security in the standard model, and analyzed its efficiency using computer simulations.

REFERENCES

[1] D. Boneh, G. Di Crescenzo, R. Ostrovsky, and G. Persiano, “Public key encryption with keyword search,” in Proc. EUROCRYPT 2004, Interlaken, Switzerland, 2004, pp. 506-522.

[2] D.J. Park, K. Kim, and P.J. Lee, “Public key encryption with conjunctive field keyword search,” in Proc. WISA 2004, Wuhan, China, 2005, pp. 73-86.

[3] J. Lai, X. Zhou, R. H. Deng, Y. Li, and K. Chen, “Expressive searchon encrypted data,” in Proc. ASIA CCS 2013, Hangzhou, China 2013, pp. 243–252.

[4] Z. Lv, C. Hong, M. Zhang, and D. Feng, “Expressive and secure searchable encryption in the public key setting,” in Proc. ISC 2014,Hong Kong, China, 2014, pp 364-376.

[5] Y. Rouselakis and B. Waters, “New constructions and proof methods for large universe attribute-based encryption,” in Proc. ACM CCS 2013, Berlin, Germany, 2013, pp. 463–474.

[6] D. Song, D. Wagner, and A. Perrig, “Practical techniques for searching on encrypted data,” in Proc. 2000 IEEE symposium on Security and Privacy, Berkeley, California, USA, 2000, pp 44-55.

[7] R. Chen, M. Yi, and G. Yang, “Dual-server public-key encryptionwith keyword search for secure cloud storage,” IEEE Transactions on Information Forensics & Security, vol. 11, no. 4, pp.789-798, April. 2016, DOI: 10.1109/TIFS.2015.2510822.

[8] F. K. Tseng, R. J. Chen, and B. S. P. Lin, “iPEKS: Fast and secure cloud data retrieval from the public-key encryption with keyword search,” in 2013 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, Melbourne, VIC, Australia, 2013, pp. 452-458

[9] Y. Lu, J. Li and Y. Zhang, “Secure channel free certificate-based searchable encryption withstanding outside and inside keyword guessing attacks,” IEEE Transactions on Services Computing, inpress, DOI: 10.1109/TSC.2019.2910113.

[10] Y. Lu, G. Wang, J. Li, “Keyword guessing attacks on a public key encryption with keyword search scheme without random oracle and its improvement,” Information Sciences, vol. 479, pp. 270-276, April. 2019, DOI: 10.1016/j.ins.2018.12.004.

[11] Y. Lu, J. Li, Y. Zhang, “SCF-PEPCKS: Secure channel free public key encryption with privacy-conserving keyword search,” IEEE Access, vol. 7, no. 1, pp. 40878-40892, March 2019, DOI:10.1109/ACCESS.2019.2905554

[12] P. Xu, Q. Wu, and W. Wang, “Generating searchable public-key ciphertexts with hidden structures for fast keyword search,” IEEE Transactions on Information Forensics and Security, vol. 10, no. 9,pp. 1993-2006, Sept. 2015, DOI: 10.1109/TIFS.2015.2442220.

[13] K. Emura, L. Phong, and Y. Watanabe, “Keyword revocable searchable encryption with trapdoor exposure resistance and regenerateability,” in Peoc. 2015 IEEE Trustcom/BigDataSE/ISPA, Helsinki, Finland, 2015, pp. 167-174.

[14] H. S. Rhee, and D. H. Lee, “Keyword Updatable PEKS,” in Proc.WISA 2015, Jeju Island, Korea, 2016, pp. 96–109.

[15] L. Wu, B. Chen, K. Choo, and D. He, “Efficient and secure searchable encryption protocol for cloud-based Internet of Things,” Journal of Parallel and Distributed Computing, vol. 111, pp. 152-161, Jan. 2018, DOI: 10.1016/j.jpdc.2017.08.007.