A Ciphertext-Policy Attribute-Based Encryption Based on Multi-valued Decision Diagram

Shaowei Zhang, Long Li, Liang Chang, Tianlong Gu, Huadong Liu

A Ciphertext-policy Attribute-based Encryption Based on Multi-valued Decision Diagram

Shaowei Zhang, Long Li, Liang Chang, Tianlong Gu, and Huadong Liu

Guangxi Key Laboratory of Trusted Software,
Guilin University of Electronic Technology, Guilin 541004, China
lilong@ncepu.edu.cn

Abstract. Ciphertext-policy attribute-based encryption (CP-ABE) is a kind of asymmetric encryption which is widely used in cyber-physical system and Internet of Things. In CP-ABE, access structure is an important component affecting the efficiency and performance greatly in several stages, such as encryption stage, key generation stage, decryption stage. However, the existing CP-ABE schemes have low efficiency because of the application of traditional access structures. In order to alleviate the aforementioned problems, this paper proposes a brand-new access structure based on multi-valued decision diagram (MDD). According to this access structure, we design a new CP-ABE scheme which performs better than many current schemes. First, our scheme supports multi-valued attributes directly. Second, the size of secret key is constant because it bears no relationship to the number of attributes. Third, the time complexity of decryption stage is O(1).

Keywords: Ciphertext-policy Attribute-based Encryption; Multi-valued Decision Diagram; Access Structure.

1 Introduction

With the development of Internet and cloud computing technology, the datas in distributed and open computing environment are more and more frequently shared and processed by people. Therefore, the datas in cloud are suffering unprecedented security problems. These datas will be completely exposed to many unkind people for a lack of efficient security mechanism. At the same time, with the implementation of large-scale distributed applications, it requires resource owners to develop a security scheme supporting one-to-many situation. A practical method is to provide a flexible and reliable access control policy for resource owner and user. It can not only apply to complicated network environment and reality scene, but also guarantee data security in communication process.

The traditional public key encryption mechanism is based on encryption technology of public key infrastructure. Although it has enhanced the security of data, many defects still exist. For example, the encryption process cannot be implemented if the user can not obtain real public key certificate; the resource owner has a high computation overhead because it needs to accept every user's message, and sends the ciphertext to the corresponding user.

In order to improve these defects, Sahai and Waters[1] proposed the concept of attribute-based encryption (ABE) for the first time at 2005 European cryptography annual conference. ABE derived from identity-based encryption (IBE) mechanism based on bilinear pairings technology, and it had many advantages. First, ABE provided a one-to-many encryption mechanism. It only needed to encrypt messages according to the set of attributes, and resulted in reducing computing cost of data confidentiality. Second, ABE supported changing access structures based on attribute set, which made this scheme more realistic. Finally, the ciphertext can be decrypted successfully only if the attribute set conformed with the access structure. Overall, the flexibility, practicability, efficiency of encryption strategy and fine-grained access policy make ABE obtain a wally application prospects in distributed file management, third party data management, group key management, privacy protection and other fields [2].

Although the scheme of ABE has solved plenty of flaws of traditional encryption mechanism, several aspects should be improved, especially for the access structure. This paper puts forward a high-efficiency scheme of CP-ABE, by improving the access structure adoptting MDD.

MDD can not only realize the representation of Boolean functions but also accomplish the expression of multiple-valued attributes. Compared with the structure of AND gate, threshold structure, OBDD, et al., MDD can improve the efficiency of encryption and decryption of CP-ABE. Based on MDD, this paper proposes an efficient and flexible access structure, which supports not only positive attributes and negative attributes, but also attributes with multiple values directly. In addition, the scheme of CP-ABE this paper propose, provides a better efficiency in many stages, such as encryption stage, key generation stage and decryption stage.

2 Related Work

The initial access structure in ABE was implemented by access control tree, which can satisfy the linear access structure, such as AND gate, OR gate, and threshold structure. Later, in [3], Rafail Ostrovsky proposed an ABE scheme supporting access structure of nonlinear properties by using linear secret sharing scheme, which further improved the efficiency. Liu X [4] designed a hierarchical access control structure by using threshold secret sharing mechanism. Balu A [5] put forward an ABE scheme by taking advantage of integer linear secret sharing system instead of linear secret sharing scheme on finite field. It made the scheme more efficient.

Literature [6] proposed an ABE scheme which supported multi-value attributes by breaking previous situation. In the scheme, each attribute corresponded to two types of status value (0, 1). It made access structure more flexible. Literature [7] fused multiple access structures into a large access control tree which reduced ciphertext storage and encryption costs. Literature [8] proposed a fine-grained ciphertext access control scheme supporting user attribute revocation mechanism.

Literature [9] proposed a new access structure based on OBDD. It reduced the nodes of the access control tree compared with the threshold structure. Moreover, the time complexity and size of generated ciphertext both had a good performance. Literature [10] provided a privacy-preserving multi-keyword text search scheme with similarity-based ranking, and it alleviated the problem of over encrypted data. In literature [11], the authors designed a scheme in which access structures were AND gates on positive and negative attributes. It observably reduced the ciphertext size and encryption/decryption time .

3 Background Knowledge

3.1 Bilinear Map and Bilinear Group

Theorem 1. Bilinear Map: Let G and G_T be two multiplicative cycle groups of prime order p, with g is one of generators of G and 1_T is a unit element of G_T. If the map $e : G \times G \to G_T$ satisfies the following conditions, e is called a bilinear map:

(1) Bilinearity: $\forall v, w \in G$ and $\forall m, n \in Z_p$, $e(v^m, w^n) = e(v, w)^{mn}$;

(2) Non-degeneracy: $e(g, g) \neq 1_T$.

Theorem 2. Bilinear Group: We say that (G, G) are a bilinear group if the group operation in G and the bilinear map $e : G \times G \to G_T$ can both be computed efficiently.

3.2 CP-ABE

Setup: Attribute authority executes the Setup algorithm with inputting security parameters. It returns system public key PK and master key MK, which are distributed to the data owner and data user at later stages.

Encrypt: Encryption algorithm is executed by the data owner in order to encrypt plaintext M. It needs to input the system public key PK and an access policy T which data owner provides. It generates and outputs a ciphertext CT.

KeyGen: KeyGen algorithm is executed by data authority with inputting the system public key PK, master key MK, and an attribute set L. It generates a secret key SK which is corresponding to the attribute set L.

Decrypt: At this stage, data user inputs public key PK, ciphertext CT and a secret key SK. It outputs the message M if user's attribute set satisfies the access structure.

3.3 Access Structure

Access structure is an access control policy for accessing ciphertext, and it is mainly formed by attribute set in CP-ABE. Given an attribute set L and an access structure F, $L \vDash F$ represents L satisfies F, and $L \nvDash F$ means L does not match F. If $L \vDash F$, it can decrypt successfully, otherwise, the decryption fails.

3.4 MDD

MDD is a directed acyclic graph, in which each node has k children, and k is the number of values of the node. Usually, MDD consists of terminal nodes (leaf nodes), non-terminal nodes and edges, and terminal nodes normally represent the results of MDD.

In general, a MDD is described as a graph consisting of circles, boxes, and one-way arrows. Each circle means a non-terminal node, which can be a variable of function or a component of system. The boxes mean the terminal nodes corresponding to the results of system. The number of possible states of the system corresponds to the number of terminal nodes, and usually we mark the system status as either normal or error. The outgoing branches of non-terminal nodes are represented by one-way arrows, and the number of states or values corresponds to the number of outgoing branches. Therefore, a MDD contains a number of non-terminal nodes and two terminal nodes generally.

4 A CP-ABE scheme based on MDD

4.1 Access Structure Based on MDD

The access structure based on MDD conforms with the realistic world more than the existing access structure such as [8] and [9], because it can represent the cases of multiple attribute values directly.

It is obvious that different variable orderings can generate different MDD, although the multi-valued function is same. Therefore, it is necessary to determine the variable ordering before constructing the MDD in order to obtain a unique access structure.

Assuming that, in the system, n is the number of attributes. The attributes can be represented as a set $V = \{v_1, v_2, \ldots\ldots, v_n\}$. Each attribute contains multiple values. The values of each attribute can be described as a set $v_i = \{v_{i,0}, v_{i,1}, \ldots\ldots, v_{i,n_i}\}$, $1 \leq i \leq n$. n_i is the number of the value of attribute v_i. In addition, $v_{i,0}$ is specified as "Non" which means the attribute set does not have this attribute. The MDD is expressed as $MDD = \{id, i, v_{i,k_i}, next_{i,k_i}\}$, $id \in ID, i \in I, 1 \leq i \leq n, 0 \leq k_i \leq n_i$. ID represents the set of the node serial numbers and I is a set of the attribute variable serial numbers. id is the serial number of the current node, and i is the serial number of the attribute of the current node. The attribute value of the current node is represented as v_{i,k_i}, and $next_{i,k_i}$ is the serial number of the next child node where the value of the current node is v_{i,k_i}. The parameter v_{i,k_i} and $next_{i,k_i}$ are used to maintain the relationship between the parent nodes and child nodes. In addition, let $\underline{W_i}$ represent the concrete value of the attribute W_i, $N = \{1, 2, \ldots\ldots, n\}$. It should be pointed out that the leaf nodes whose node serial numbers respectively are 0 and 1 only mean the fail or success of the decryption, so delete the domain of i, v_{i,k_i} and n_{i,k_i}.

Supposing that encryption attribute set is $W = \{W_1, W_2, \ldots\ldots, W_n\}$, and $W_i = \{W_{i,1}, W_{i,2}, \ldots\ldots, W_{i,n_i}\}$. Decryption attribute set is $L = \{L_1, L_2, \ldots\ldots,$

$L_n\}$, and $L_i = \{L_{i,0}, L_{i,1}, \ldots\ldots, L_{i,n_i}\}$. We use encryption attribute set W build an access structure F. If $W \subseteq L$ and $W_i \subseteq L_i$, we say the set L satisfies the set W, or say the set L satisfies the access structure$F$. If L satisfies F, the ciphertext can be decrypted by the user successfully; otherwise, the decryption fails.

For example, in order to access the file, the attributes of data visitors need to satisfy one of the following three conditions. Category 1: graduate students (Gra) of computer school (CS); Category 2: graduate students of law school (LS); Category 3: undergraduates (Und) of business school (BS). According to the above description, the following access structure based on MDD can be constructed.

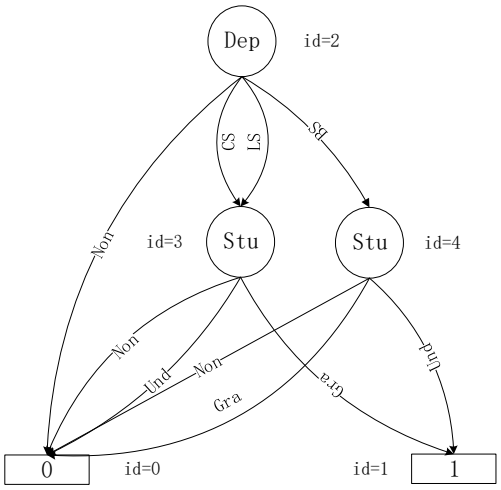

Fig. 1. Access Structure Based on MDD

Theorem 3. Valid Path: In MDD, if a path derives from root node and ends at terminal node 1, it is called a valid path. For example, in Fig.1, $Dep \xrightarrow{CS} Stu \xrightarrow{Gra} 1$, $Dep \xrightarrow{LS} Stu \xrightarrow{Gra} 1$ and $Dep \xrightarrow{BS} Stu \xrightarrow{Und} 1$ are valid paths, but others are not valid paths, such as $Dep \xrightarrow{CS} Stu \xrightarrow{Und} 1$.

4.2 Main Process of the CP-ABE Based on MDD

Setup: Let G and G_T be two bilinear group of prime order p, with g is a generator of G and $e : G \times G \to G_T$ is a bilinear map. Choose several random exponents $y, t_{i,k_i} \in Z_p (i \in I)$. Define $Y = e(g,g)^y$, $T_{i,k_i} = g^{t_{i,k_i}}$, $\underline{T_{i,k_i}} \in \{T_{i,k_i} | i \in I\}$, the paintext $M \in G$, and then generate the public key $\overline{PK} =<$

$e, g, Y, \{T_{i,k_i|(i\in N)}\} >$, the master key $MK =< y, \{t_{i,k_i|(i\in N)}\} >$. In addition, this algorithm makes T_{i,k_i} (t_{i,k_i}) correspond to the attribute value v_{i,k_i}.

Encrypt: The data owner executes encrypt algorithm in order to encrypt the plaintext M. The valid paths in the access structure are $R = \{R_0, R_1, \ldots\ldots, R_{m-1}\}$, m is the number of valid paths. The operations of encrypt algorithm follow:

(1) Choose $s \in Z_p$ randomly;

(2) Compute $C_1 = g^s, C_2 = M \cdot Y^s$;

(3) If $\underline{W_i} = W_{i,k_i}$, then $\underline{T_{i,k_i}} = T_{i,k_i}$;

(4)Compute $C_{R_t} = (\prod_{i\in I} \underline{T_{i,k_i}})^s = g^{(\sum_{i\in I} t_{i,k_i} \cdot s)}, i \in I, 0 \le k_i \le n_i$;

(5) The corresponding ciphertext is $CT =< MDD, C_1, C_2, \{C_{R_t} | R_t \in R\} >$.

KeyGen: This algorithm is implemented by the trusted authorization center and generates a private key SK corresponding to the attribute set L provided by the data user.

(1) Select $r \in Z_p$ randomly;

(2) Compute $D_1 = g^{y-r}, D_2 = g^{(r/\sum_{i\in I} t_{i,k_i})}$;

(3) The private key is $SK =< D_1, D_2 >$.

Decrypt: Suppose the private key is $SK =< D_1, D_2 >$, ciphertext is $CT =< MDD, C_1, C_2, \{C_{R_t} | R_t \in R\} >$, the process of decrypt algorithm follows:

(1) take the root node as current node which is being operated;

(2) Get the information of current node such as v_{i,k_i}. Then, take the node whose node number is $next_{i,k_i}$ as current node. Repeat the step (2) until it reachs the leaf node;

(3) If reach the leaf node 0 finally, the decryption fails;

(4) If reach the leaf node 1 finally, execute the step (5);

(5) Stores the current decryption path. In sequence, compute $e(C_1, D_1) \cdot e(C_{R_t}, D_2) = e(g, g)^{s\cdot(y-r)} e(g, g)^{s\cdot y} = Y^s$ and $M = C_2/Y^s = C_2/e(g, g)^{s\cdot y}$.

4.3 Analysis of Capacities and Efficiency

Our scheme supports multi-valued system directly because of the implementation of access structure based on MDD, which performs well in supporting multiple values. Besides, lots of advantages can be found in many aspects. In Encrypt algorithm, the computation complexity and the size of the ciphertext are only affiliated to the valid paths, instead of the attributes of the system. Thus, it performs better than several other CP-ABE schemes such as [10] and [11]; In KeyGen algorithm, the computation complexity is O(1), because it only needs two exponential operations in G; In Decrypt algorithm, it supports fast decryption, because it only needs two exponentiations in G and two bilinear pairings computation, and the size of the secret key is constant. Furthermore, the CP-ABE scheme based on MDD in this paper can resist collusion attacks effectively in which attackers have multiple private keys.

5 Conclusion and Further Work

In this paper, we provide a new CP-ABE scheme based on MDD, which improves the efficiency and capability in many stages. Our scheme supports multi-valued attributes directly because of the access structure based on MDD. At the same time, the scheme allows for the collusion attacks in which the attacker has multiple private keys. At last, compared with several other CP-ABE schemes, our scheme performs better in terms of the main computation of KeyGen algorithm, Decrypt algorithm and the size of secret key.

In the future, it will be an exciting work to explore the approaches of improving the efficiency and capability of CP-ABE scheme, especially for the improvement of access structure. We can explore that whether the access structure based on Zero Suppressed Binary Decision Diagrams and Algebraic Decision Diagrams can help to enhance the effectiveness of CP-ABE scheme.

Acknowledgments

This work is supported by the Natural Science Foundation of China (Nos. U1501252, 61572146, U1711263, 61561016); the Natural Science Foundation of Guangxi Province (Nos. 2016GXNSFDA380006, 2017GXNSFAA198283); the Key Research and Development Program of Guangxi (Nos. AC16380014, AA172-02048); Innovation Project of Guangxi Graduate Education (No. YCSW2018139); and the High Level of Innovation Team of Colleges and Universities in Guangxi and Outstanding Scholars Program.

References

1. Bethencourt, J., Sahai, A., Waters, B.: A Ciphertext-Policy Attribute-Based Encryption Based on an Ordered Binary Decision Diagram. In: 2007 IEEE Symposium on Security and Privacy, pp. 321-334 (2007)
2. Li, L., Gu, T., Chang, L., Li, J., Qian, J.: CP-ABE based Access Control with Policy Updating and Fast Decryption for Intelligent Manufacturing. J. Journal of Internet Technology, 19(3), 825-836 (2018)
3. Boneh, D., Crescenzo, G.D., Ostrovsky, R., Persiano, G.: Public Key Encryption with Keyword Search. J. Eurocrypt, 3027, 506-522 (2004)
4. Liu, X., Ma, J., Xiong, J., Liu, G.: Ciphertext-policy Hierarchical Attribute-based Encryption for Fine-grained Access Control of Encryption Data. J. International Journal of Network Security, 16, 437-443 (2014)
5. Balu, A., Kuppusamy, K., Ciphertext-Policy Attribute-Based Encryption with User Revocation Support. In: International Conference on Heterogeneous Networking for Quality, Reliability, Security and Robustness, pp. 696-705. Springer, Heidelberg (2013)
6. Fan, C.I., Huang, S.M., Ruan, H.M.: Arbitrary-State Attribute-Based Encryption with Dynamic Membership, J.: IEEE Transactions on Computers, 63(8), 1951-1961 (2014)

7. Wang, S., Zhou, J., Liu, J.K., Yu, J., Chen, J.: An Efficient File Hierarchy Attribute-Based Encryption Scheme in Cloud Computing. J. IEEE Transactions on Information Forensics and Security, 1265-1277 (2017)
8. Hur, J., Dong, K.N.: Attribute-Based Access Control with Efficient Revocation in Data Outsourcing Systems. J. IEEE Transactions on Parallel and Distributed Systems, 22, 1214-1221 (2011)
9. Li, L., Gu, T., Chang, L., Xu, Z., Liu, Y., Qian, J.: A Ciphertext-Policy Attribute-Based Encryption Based on an Ordered Binary Decision Diagram. J. IEEE Access, 5, 1137-1145 (2017)
10. Sun, W,. Wang, B., Cao, Li, M., Lou, W.: Privacy-preserving multi-keyword text search in the cloud supporting similarity-based ranking. J. IEEE Transactions on Parallel and Distributed Systems. 25(11), 3025-3035 (2014)
11. Ling, C., Newport, C.: Provably Secure Ciphertext Policy ABE. In: 2007 ACM Conference on Computer and Communications Security, pp. 456-465 (2007)