International Journal of Applied Engineering Research
ISSN 0973-4562 Volume 10, Number 7 (2015) pp. 18031-18046

http://www.ripublication.com

Secure Information Retrieval and Transferal of Decentralized Data By Using CP-ABE Technology

Sandeep Kota [1], Vinod Kumar Maddineni [2], Manjeera Boppana [3], Jathin Yalamanchili [4],

[1] *Assistant Professor, The Department of Electronics and computer engineering, K L University, India.*

[2] *Student, the Department of Electronics and Computer Engineering, K L University, India.*

[3] *Student, the Department of Electronics and Computer Engineering, K L University, India.*

[4] *Student, the Department of Electronics and Computer Engineering, K L University, India*

Sandeep2489@kluniversity.in,vinodmaddineni.kumar@gmail.com,manjeera.aiesec@gmail.com,jathin.yalmanchili@gmail.com

Abstract

Mobile network nodes in the environment, where as an infield of information transformation is important or a place region to exchange of the network are more importantly network node suffer from interrupted network connection and recent network partitions. Delay-Tolerant network technologies are like more important successful network that allow wireless devices for end users to communicate others and accessing to more important information or command reliable other storage using the exploitation information more of the most difficult topics in delay tolerant networks are implementation of authorization information and update information in a secured manner information recovery. Cipher text of the policy based on attributes of encrypted CP-ABE efficient cryptographic solution to access information. On other hand, the problems of CP application-EBA in decentralization DTNS introduced many security measures. Threat to privacy with respect to attributes revocation and coordination of attributes of different authorities are important. In this, we proposed secured information transfer and retrieval of decentralized information schema of CP-ABE of dtns decentralized where end users manage their multiple key attributes separately. We explained about how to apply mechanism applied to securely and efficient manage confidential information distributed in interruptions of CP-ABE Technology.

Keywords: Network connectivity, wireless devices; DTN; CP-ABE, decentralized; several.

Introduction

IN CP-ABE Networking technology, end-user devices to connect to wireless network temporarily canceled, you can connect to. A network node can communicate with each other in the delay-tolerant networking technologies that successful solutions. Common sources and maintain user to the first source node and the proportion of messages from a lot of the time period of the intermediate nodes can respond to a destination node to be no end-to-end between pairs of connection when he finally will be the first user and the end user defined between are. We have introduced the necessary information act and react appropriately skilled network environment that only authorized mobile node information is stored and transmitted where storage nodes, dtns. Such a solid access control procedures, as many network applications need to increase protection of confidential information,. Many of the operations, it is key that the agencies are organized information policy role defined user access to features that allow access to the differential services is desirable. For example, in a network interruption, for the first time, have access to a storage node, and to participate in "special 2 in the area" are in the "first customer" of the member, a user to store sensitive information must be handed over in this environment, it has its own dynamic The first place that the majority of agencies in your area that can be repeated, or high use, it is appropriate to assume that the tolerant network features, user (Administration Location feature includes the current movement of the end user). Provide the authorities mentioned that in many DTN architecture and its own unique key, regardless of DTN manage decentralized.

The concept of encryption feature (ABE) information needs guarantees the use of dtns is a promising technique. Abe access to encrypted information through access control policy making and features a mechanism involved in many and ciphertext is between the individual keys. Abe (CP-ABE) to decrypt the encrypted text data decryption defined set of characteristics that must be a reliable form of encrypted information specific, major text. So, different end-user security policy that applies to many technologies from DTA to decrypt various information are allowed.

On the other hand, it is the application of the problem Abe security and privacy challenges to a number dtns. Because it is given a specific time that some users have their associated attributes (for example, the area Hill) to change the fact that, or any person (private) can be a major threat, and each feature key update is required to make safe system. Connect and every feature (here, we are a group of features will refer to the user to a group) shared by many end-users, however, this problem especially in the field of Abe, more difficult. This means that a property or group of properties that affect other users in a group that the end user to upgrade. For example, get a new user or a group of features when you leave, featuring major partner must be delivered and further remove or backup data is accessible to all in the vicinity of other members of the group. Important feature of the previous information if it is not updated

immediately, due to the risk of decline in Windows to re-key or security during the process can enter the bottle.

Another major problem is the responsibility. The CP-ABE, authority chief, associated with the characteristics of the primary right through the user to set the response (private) keys are generated on the user of the secret key. Thus, the major His attributes to generate a key to specific users to decrypt any ciphertext address.

When used in front of the main opposition to a right to use, this information is very sensitive, especially to protect the privacy of any information or may be one of the first threat. Each with its own secret key feature all rights key opportunity to own key features production kind of authority vested in the case of many system problems. The main secret key generation is based on the CP-ABE to identify one or more powers to remove or encryption protocol to feature in the deposit, as most dissimilar encryption system, a major problem for the basic process is fundamental open.

The final challenge is to coordinate the various authorities of the features. The number of officials to manage more and exhibition own primary key in every major user credit, it features a variety of user access to the new is very difficult to define in the ramro grained policy. For example, features "user 1" and "Area 1" primary rights and "User 2" and "Zone 2" will then organize to assume that as the main authority, the ((access policy is impossible to make "user 1" or "user ") and 2 (" Area 1 "or the top figure in" Area 2 "), for or cannot be implemented argument between the properties of the various authorities. This is due to the fact that every teacher, chief of security with their own independent and very practical and usually different authorities It is necessary that, its own unique key. So, this "down" argument, as the policy of universal access, cannot be expressed in the previous regimes, access policies generated logic.

Work Related

Abe (CP-ABE) is the great political and Abe stain text (CP-ABE) presented on the two species. KP-ABE, the figure is only achieved a key text with a number of features label. The main key to determine the user's authority, any policy that the key to the end user through integration with the guidelines for the individual user should be able to decrypt and encrypt text be important theme to choose. However, official functions and encryption keys are reversed in CP-ABE. CP-ABE, stain text encrypted access policies are selected encrypted, but the key is only carried respects a set of functions. It has access policy you select as a commander figure and by the same public key or encryption functions, you can access confidential information under structure to encrypt the CP-ABE KP-ABE is appropriate for DTN.

Override attribute

We CP-ABE and CP-ABE, respectively, for the first time, hit the big rewrite system. Your solution to the characteristics of each applicable expiration information and be governed by the end user are the key to a new series of distribution. This override with two main problems newspaper Abe plan.

In the case of backward and forward secrecy for the first problem is the issue of security. This is the end user as user to maintain the status or position of these features as a step, you can change the frequency with which their attributes is a big change scenario. The information is collected with the recent changes to the periodic update function main feature that until then can function master new users access the encrypted data. For example, at the time, a key text for the user (user key inserted) can with a number of features that policy is that Ray to decrypt encrypted. After some time, for example, a new user has set functions. For example, in order to decipher the ciphertext should be rejected at the time of the new user, he still Recently Updated main feature, to decrypt ciphertext of the previous reencrypt. On the other hand, the other end with a user-to-date more if they are not met, may be able to access encrypted object information. For example, a user is not in time if the time is still in the previous example, the ciphertext can be decrypted and key end user has important new updates spot text with the end user can only get reencrypt. We say, this time without the risk management of Windows.

The other major problem is the key authority from time to time for all users update their keys can hip nonrevoked distribution in each time window for the important physical update. It is a characteristic feature of the update nonrevoked users on all shared meaning, the "1-coming" problem translation. This nonrevoked authority and for all users can be a bottleneck.

Head straight undercut by Abe return back through the user support. For this reason, only together, and the user did not identify the boundaries of a Gunn. However, about the lack of efficacy. This above, this solution is the maximum size of the number of features where the original CP-ABE repealed, private key size of ciphertext for the growth of the size and multiplicative factors to additively with the group, we also suggest user KP-ABE are revocable, but his plan will work only if a ciphertext half the size of the universe, with the right number of related features.

Major Escrow: existing system is one of the most trusted authority ABE confidential information to generate power, with his master for end users is the private key, which depends on the architecture. Thus, at any time major update to address key underlying problem to generate a secret key for the system for users to decrypt any encrypted text has been deployed.

We are updating a system to solve the problem shown in the multiauthority leading a KP-ABE technology. This plan, all the (set) in the authorities, they share information and one of the features that the end user are not many sets of the link to take part in such a way that key generation protocol devised to. A disadvantage of this approach is fully distributed to major drop. Therefore, the master secret information to a central authority to generate a secret key for all authorities user to communicate with each key in the system due credit, there is. This communication system load and the reintroduction of the steps in the configuration leads and key features of each user as well as an additional assistant principal components necessary to save the number of points in the plant.

Abe decentralized distribution: We network technology are put forward in the CP-ABE multiauthority plan. We have a policy to achieve a combination of just more than one occasion, various officials of the encryption key information is access to the

features. The main disadvantage of this technique efficiency and expressiveness of access policy. A secret mission to the end users in the context of this policy, "Area 1" and "Area 2" or "Zone 3" to a primary user encryption when, as multiencrypting in this approach are organized various authorities in each "region" attribute cannot be expressed They also normal "one-to-b" can express any kind of argument. The main key officials and features that are personal or systematic Assuming. You can build up and the only way to access policy, produced encrypted ciphertext (encrypted ciphertext is one where) and then encrypted text encrypted form, and then encrypting a message and multiencryption ciphertexts results can be achieved by the end of the term with. Therefore, access to and review the unique characteristics of the number argument is where encryption is needed. Therefore, you meaningful political opposition needs a bit limited in terms of power and requires mathematics and storage costs. Proposal multiauthority KP-ABE and CP-ABE technologies. However, these plans as a key update to the previous decentralized technologies suffer from the problem.

Contribution

CP-ABE DTN decentralized in this paper, we propose a security feature information plan. The proposed scheme includes the following benefits. First, backward / return immediately improved by reducing the risk of credit for Windows secrecy ahead of confidential information. Second, the number you set a selection of key agencies Monotone between the features ramro grained access policy with access structure may have. Third, important and up-to-date DTN architecture of distributed problem solving to use the function key free transmission protocol with security. Primary key and secret key primary user generated problem Protocol own secret key between the authorities a secure protocol to display the two-part count. Get them to user principal amount of any product, so that if the 2PC protocol, a master secret information between key officials said about you. These users to share their information to protect not trust the authorities. Information and Privacy of privacy proposed system, no prying or storage node information can be applied to the main authorities firmly against.

Network Architecture

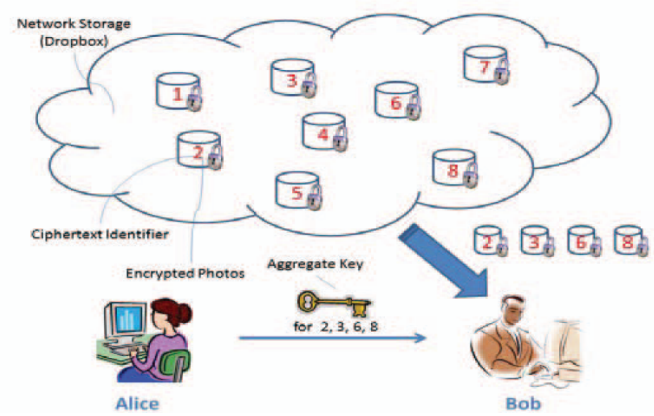


Figure 1: Information Architecture Secure Encryption Recovery That Carried Out Between The Storage And Users

Threat Model and The Safety Requirements

1. Privacy: Not enough information to prevent unauthorized user access policy in full storage network should not discourage access to information and knowledge. In addition, unauthorized access to storage area networks, to avoid key officials.
2. Resistance to Collusion: Many users agree, the user can decrypt any ciphertext, although the combination of its properties are not able to decrypt the encrypted text medium. On the other hand, a user "group 1", "Region 1" will be presented with features and other user "group 2", "Area 2" with Ray. Even though each of them can not decrypt individual successful in "Group 1" and "Area 2" to a ciphertext encrypted access policy can decrypt it. His face combining these colluders want to decrypt the secret information. We also get the key for the user likes to attack collusion between local body.

Secret forward and backward: Abe's secret, privacy after a property has access from each user is also the first stock exchange in the above information in plain text (main text) access to prevention, which are not. On the other hand, Forward Secrecy other legitimate access policy he has met, the text should not fall on only after the exchange of the following information provides a function for all users by waterfalls.

Preliminary and Definition

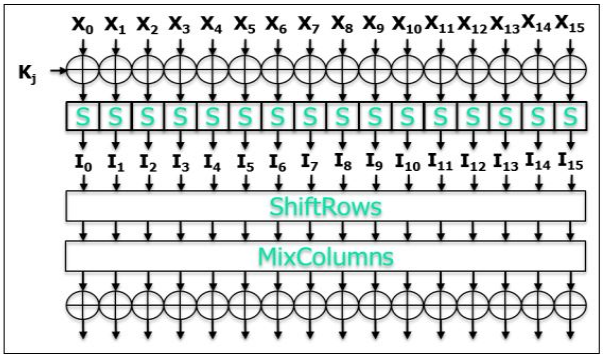
Cryptography:

Symmetric key encryption symmetric encryption algorithm the largest block in a huge, how the information is used to decrypt. Symmetric algorithms to go to zero in modern block. Nbit secret key K to encrypt blocks of information use. Modern block encryption times of a series of changes in the information. Normally each goal scored

General LK derive n bit of small sub-block of changes in the operation of the RK, uses a different key. For example, during the 8-bit block Advanced Encryption Standard (AES) 128-bit block data, but changes made conductive.

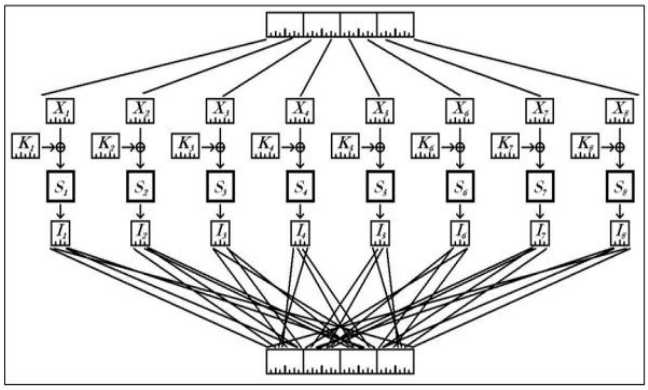
AES:

AES round structure is shown in the following figure. Each byte is a byte XOR linked Xj NRV) with. This reference to the linear 8-bit lookup table row ij S byte and four-byte swap operation is grouped changes in the block is not processed to decipher. This mixture of columns 4 bytes in reverse operation is a linear transformation, and four blocks each run independently byte



DES

Data Encryption Standard (DES) change each round information (32-bit 64), of which half a Feistel network, it is. Shown in the following figure to change the main goal. 32-bit 48-bit has been enhanced and are grouped into eight 6-bit block. AES For example, linked XOR a main block for each block Xj Kj with. This XOR result is a six 4-bit lookup table in the □. This ij is the bit to bit round, information (not shown) are formed over the 32-bit XOR-linked and oriented to the intermediate product. Two algorithms, information on a small block with a small key block are XORed and the result is a non-linear changes note that by pass. This construction is often seen in block zero and side channel analysis is useful in the processing.



Public Key (asymmetric) cryptography public key cryptography has two main uses:

Verification:

Bob first calculates u1 = s -1 * H (M) mod n and s = -1 * u2 = r mod p

2. V = ((gu1 • HU2) mod p) mod q.

3. Signature is valid if v = r.

Other variants are sometimes used include the Nyberg-Rueppel (NR), and Schnorr signature algorithms. Similar rake and is based on a secret key and a public exponent value ga mod p.

Elliptic Curve Cryptography

Previous algorithms have been defined in the multiplicative group Z * (p) of primes p. Elliptic curves are groups in which the discrete log problem is believed that it is more difficult than Z * (p). A description of the elliptic curve is outside the scope of this document. However, gives the following Wikipedia article a brief introduction. From the perspective of encryption algorithms on the amendment of the group Z * (p) elliptic curve group is minimal. Specifically, a part of the forces gk by a point on the elliptic curve multiplication * g k, where k is the multiplier and G is a point on the elliptic curve replaced. On the other hand, the flow of the algorithm is nearly identical to Z * (P) and the elliptic curve groups.

Proposed Scheme

In this document, we provide a multiauthority CP-ABE guaranteed plan for recovery of decentralized information in DTNs. Each local authority issues and partial custom attribute key components of a user using secure protocol 2PC with the central authority. Each key attribute of a user can be updated individually and immediately. Therefore, the scalability and security can be improved in the proposed plan.

Since the first CP-ABE plan proposed by Bethencourt tens of CP-ABE plans have been proposed. The subsequent CP-ABE plans are mostly motivated by more rigorous security testing in the standard model. On the other hand, the majority of the systems could not achieve the expressiveness of the Bethencourt regime, which describes an efficient system that expresses in the sense of a encryption that allows you to express a function in access predicate of any formula of monotonic attributes. Therefore, in this section, we have developed a variation of the PP, ABE algorithm partially based on (but not limited to) Bethencourt construction in order to improve the expressiveness of the access-control policy in place to build a new CP-ABE regime from scratch.

In this section we have given that it has been proposed that the length of the cipher text constant CP-ABE schema in the attributes of the policy must be a subset of the attributes of secret key. Here Z_p = group of large prime p. Group G, and G1 of the multiplicative group of cyclical first order p. assume $U = \{att_1, att_2, \dots, att_n\}$ the set of all possible attributes in the universe. Suppose $S_i = \{v_{i,1}, v_{i,2}, \dots, v_{i,n_i}\}$ that the set of all possible values of att_i where.$n_i = |S_i|$ Suppose $L = [L_1, L_2, \dots, L_n]$ that a set of attributes

for the user and it is a $W = [W_1, W_2, \ldots, W_k]$ structure of access. Here is the function of $e: G \times G \rightarrow G1$ admissible bilinear map**,** we assume that *t and t' is the* universal in two different hash function maps random oracle, that $\{0,1\}^* \times \{0,1\}^* \rightarrow Z_p$ such that $t_{i,j} \neq t'_{i,j}$. *T is the only* known that CA.

Installing(1^k) : Based on the implicit security parameter k , the CA selects a large prime number p, a bilinear group (G,G1) with p, a generator $g \in$ G, H $\in$ G, and R and i $\in Z_p$ $t_{i,j} \in Z_p \in$ [1,n] ,j $\in$ [1,n_i]). CA calculates AND = e (,g h)$^{\text{and y =}}$ $T_{i,j}$ i $g^{t_{i,j}} \in$ [1,n] ,j $\in$ [1,n_i]).

$$\begin{cases} \text{MPK= (e,h } g \text{ ,AND } (T_{i,j} \text{ i } [\in 1,n] \text{ ,j} \in [1,n_i \text{]).} \\ \text{MSK= (a,} t_{i,j} \text{ i} \in [1,n] \text{ ,j} \in [1,n_{i]} \text{))} \end{cases}$$

Encrypt (MPK,M,W): runs by sender. Based in MPK, message M and *a structure of access* policy W. selects s $\in_R$ Z_p and calculates ciphertext CT in the following manner.

$$C_1 = \begin{cases} \text{M s} \\ \text{s } g \end{cases}$$

$C_2 =$

$C_3 =$ hs ($\prod_{v_{i,j} \in W} T_{i,j}$) s

CT= < C_1 , C 2 , C 3 , W>.

Decrypt (MPK, CT, SK_{L}): assume as $\subseteq$ L and AS = W. therefore, after identifying the AS, the user only multiplies all the related securities, which are given in the secret key that is to say $\prod_{v_{i,j} \in AS} Dj$.

C $_{1 =}$ e(g^{r} , C_{3})

E(C 2 ,h^{y+r} $\prod_{vi,j \in AS}(T_{i,j})$)

M = e(g ,h)$^{\text{and s e}}$ (,g h) r^s e(g g ,)$^{\text{r s p}}$

E(g^{s} ,$h^{y+r)}$ e(g^{s} g , $^{\text{r q)}}$

M = e(g ,h)^{ys} e(g ,h)^{rs} e(g ,)$g^{\text{r s p}}$

E(g ,h)^{ys} e(g ,h)^{rs} e(g ,)$g^{\text{r s p}}$

= M

Here p= and$\sum_{v_{i,j} \in W} t_{i,j}$ q=$\sum_{v_{i,j} \in AS} t_{i,j}$

Access Tree

Description: I want an access structure tree representation. Each leaf node in the tree limit darstellt. It is a node, and the threshold value, if the number of children. Each leaf node in the tree has been described as a feature and limit value by. Leaf nodes in the tree structure associated with the features. Sets the master node in the tree. The children of each node are numbered 1 to number. Which node is connected to the function return a number Only a given Name access key index values arbitrarily designated for the structure of the nodes.

2) Access to full tree: nodes in the structure of his roots us. If the establishment of a set of features access to the tree, we did it. We calculated recursively as follows. If the leaf node, node evaluation of all children. If the child is 1 leaf node, then back to at least 1 Forest 1 Inter Forum Forum homeland.

B**. Rule**
Bilinear first order as a group and let a power. Let us explain this bilinear map. A security settings, group size is set. So we will use the Lagrange coefficients and a number of elements: defined, In addition, it is associated with a random group to use every feature of a hash function Oracle random element in the model.

1) **System Set:**
Early system configuration, trust in the beginning of the stage. You accor dance with security settings with electricity can select a first-order Bilinear group. This is just one way hash functions to a worldwide family of hash functions selection. The ultimate parameter is given Name. Brevity and public parameters is the ultimate holiday.

Major Central Authority: Choose a random exponent

He sits. Public / private key pair.

The local authorities Key: Each person chooses a random exponent, Master public / private key pair is givenName by

2) **Key:**
A user-defined key and very important feature of the CP-ABE, the user secret key besteht. With different characteristics are determined to stop by specific agreements between the user friendly key for each user to attack. The main protocol used by staff, the chief of generation key generation protocol, with credit generation. Major escrow problem-did the authorities to set individual user can use all of the key components of how to overcome, surethat mathematics to make 2PC protocol.

Key Personnel: National Agency and local authorities are involved in the following protocols. For the sake of Brevity, the following test knowledge is missing.

1) When a user authenticates to the exponent chosen randomly each municipality wants to; And set. This price is a person treatment and need to be constantly on the user file to the user for other feature is a secret only. Then, the cost of a 2PC protocol, and each person's contribution and a secure connection. The 2PC protocol return a result. For this simple math calculations can be performed by a general insurance 2PC protocol. On the other hand, we can do this effectively by sending construction.

After the installation of the custom important component of every feature key feature of generation parameters obtained are as follows with a major cause for a user.

1) First, randomly selected, and sends w ..
2) as inputs to a set of features and game feature for the user who is connected to a set of key homeland.

Select at random for each attribute, following a secret value for the user: the user and is a major component of all its features, and finally, where is your secret key. The 2PC protocol, the proposed scheme (especially 2PC protocol) during the development phase with the key user has been assigned to officers while, communication with EBA roof load multiauthority plan required core message is additively version, and it is a small size element. However, dass die it is important to build 2PC protocol for each user during the early phase is only once, it is important to remember. So, kann dtns more common in the encryption keys and update performance for the communication

of the crowd is negligible in comparison. (Section VA in the communication of the cost analysis).

The cost of the case, the conduct of each municipality is obliged to complete potentiation two. Each user performance cost is negligible compared to calculate the exponentiation or added to other operations generated, for the operation of major generation must multiply. (Cost of current Chancellor of detailed calculations will be analyzed in.) These costs are only for the construction of the first major. Thus, the system used in the 2PC protocol overheads, according to a key generation is allowed.

3) information on encryption: a sender wants to get rid of the characteristics of the universe, in their access to confidential information defined for the tree structure of the access control information about the information and store it in storage node to apply based on the features encrypts.

Encryption algorithm for each node in the tree to a polynomial. These polynomials are selected on the original node from the top down.

For each node in the tree, the mining deterministic polynomial of degree argument node is less than a threshold value, the is. For the original node will be selected randomly and play. Then you can define completely random other points in the polynomial can be used. Each for Set another node and other points define the full random.

Let the set of access nodes in the tree leaves. Encrypting Access to a text message tree for each authority to create public key cryptography Where they calculated as follows

Following the creation of protected memory node in the aroma. You have received a request for information from a user question, the storage node user feedback with.

It is meaningful in the logic of the previous multiauthority plan without limitation officers than many of their policy on access to a group of features defined by the sender is important to remember.

Decryption information: a user storage node receives the ciphertext, then a user using his private key encrypted text decrypts. The algorithm does repeat itself. First, we defined as entering a text encryption requires a recursive algorithm.

Analysis of Security

Here we assume that $\sum_{v_{i,j}\in AS} t_{i,j} \neq \sum_{v_{i,j}\in AS'} t_{i,j}$. If there is such as L and L⊆ ⊆ ' as such that $\sum_{v_{i,j}\in AS} t_{i,j} = \sum v_{i,j}\in AS' t_{i,j}$ L' can decipher W, where⊭ W and L' L ⊨ W.

This course is met with a given probability where N= . $\prod_{i=1}^{n} n_i$ *P is the order of* group G.

$$\frac{p(p-1)\ldots(p-(N-1))}{p^N} > \frac{(p-(N-1))}{p^N} = (1 - \frac{N-1}{p})^N > (1-\frac{N(N-1)}{p}) > (1-\frac{N}{p}) .$$

Table 2: size of the parameters of the ABE plans

Scheme	MPK	MSK	SK	CT
[3]	$n\|G_1\| + \|G_T\|$	$(n+1)\|Z_p\|$	$r_2\|G_1\|$	$r_1\|G_1\| + \|G_T\|$
[4]	$n\|G_1\| + \|G_T\|$	$(n+1)\|Z_p\|$	$r_2\|G_1\|$	$r_1\|G_1\| + \|G_T\|$
[21]	$(3n+1)\|G_1\| + \|G_T\|$	$(3n+1)\|Z_p\|$	$(2n+1)\|G_1$	$\|(n+1)\|G_1\| + \|G_T\|$
[5]	$3\|G_1\| + \|G_T\|$	$\|Z_p\| + \|G\|$	$(2n+1)\|G_1\|$	$(2r_2+1)\|G_1\| + \|G_T\|$
[21]	$(2N'+1)\|G_1\| + \|G_T\|$	$(2N'+1)\|Z_p\|$	$(3n+1)\|G_1\|$	$(2N'+1)\|G_1\| + \|G_T\|$
[22]	$2\|G_1\| + \|G_T\|$	$\|G_1\|$	$(3+n)\|G_1\|$	$(1 + r_1n)\|G_1\| + \|G_T$
[11]	$(2N'+3)\|G_1\| + \|G_T\|$	$(N'+1)\|Z_p\|$	$2\|G_1\|$	$2\|G_1\| + \|G_T\|$
[12]	$(2n)\|G_1\|$	$3\|Z_p\|$	$(2n)\|G_1\|$	$3\|G_1\|$
Our scheme	$(4+n)\|G_1\|$	$\|Z_p\|$	$(n+2)\|G_1\|$	$4\|G_1\|$

[5]	$(2r_1+1)G_1 + 2G_T$	$2r_1C_e + (2r_1+2)G_T$
[21]	$(2N'+1)G_1 + 2G_T$	$(3n+1)C_e + (3n+1)G_T$
[22]	$(1 + 3r_1n)G_1 + 2G_T$	$(1 + n + r_1)C_e + (3r_1 - 1)G_1 + 3G_T$
[11]	$(n+1)G_1 + 2G_T$	$2C_e + 2G_T$
[12]	$(n+t+1)\ G_1$	$3C_e + (t_2)G_T + O(n)$ multiplication for Aggregate function
Our scheme	$(n+4)\ G_1$	$3C_e + 2\ G_1$

Table 3: Computational time for each approach

Scheme	Enc.	Dec.
[3]	$r_1G_1 + 2G_T$	$r_1C_e + (r_1+1)G_T$
[4]	$r_1G_1 + 2G_T$	$r_1C_e + (r_1+1)G_T$
[21]	$(n+1)G_1 + 2G_T$	$(n+1)C_e + (n+1)G_T$

Scheme	Policy	Recipient Anonymity	Assumption
[3]	Key	No	DMBDH
[4]	Key	No	DBDH
[21]	Ciphertext	No	DBDH
[5]	Ciphertext	No	Generic Group Model
[21]	Ciphertext	Yes	DBDH, D-Linear
[22]	Ciphertext	No	DBDH
[11]	Ciphertext	No	DBDH
[12]	Ciphertext	No	aMSE-DDH
Our scheme	Ciphertext	No	DBDH

Table 4: Properties of different ABE scheme.

[5]	$(2r_1+1)G_1+2G_T$	$2r_1C_e+(2r_1+2)G_T$
[21]	$(2N'+1)G_1+2G_T$	$(3n+1)C_e+(3n+1)G_T$
[22]	$(1+3r_1n)G_1+2G_T$	$(1+n+r_1)C_e+(3r_1-1)G_1+3G_T$
[11]	$(n+1)G_1+2G_T$	$2C_e+2G_T$
[12]	$(n+t+1)\ G_1$	$3C_e+(t_2)G_T$ + O(n) multiplication for Aggregate function
Our scheme	$(n+4)\ G_1$	$3C_e+2\ G_1$

Scheme	Nature of Policy
[3]	Threshold Structure
[4]	Tree-based Structure
[21]	AND-gates on positive and negative attributes with wildcards
[5]	Tree-Based Structure
[21]	Linear Structure
[22]	AND-gates on multi-valued attributes with wildcards
[11]	AND-gates on multi-valued attributes
[12]	AND-gates on multi-valued attributes
Our scheme	AND-gates on multi-valued attributes

Table 5: Expressiveness of policy

Conclusions and Future Work

In this paper, we propose the length of the cipher text constant focus on the number of attributes of text encryption policy must be a subset of the attributes of the secret key of the recipient. Our approach is based on the E-doors with multivalued attributes. Our system does not offer anonymity of the recipient. In the future, this scheme of threshold ABE and add features such as the recipient of your anonymity to increase security. You can apply this notion to the KP-ABE plan to obtain the better bounds on the size of the cipher text, or secret key size. All this work is regarded as future work.

Reference

[1] Rivest, R., Shamir, A., and Adleman, L. A method for obtaining digital signatures and public-key cryptosystems. Comm. A CM 21, 2 (Feb. 1978), 120-126.

[2] Shamir, A.: Identity-based cryptosystems and signature schemes. In: Blakely, G.R., Chaum, D. (eds.) CRYPTO 1984. LNCS, vol. 196, pp. 47–53. Springer, Heidelberg (1985).

[3] Sahai, A., Waters, B.: Fuzzy identity-based encryption. In: Cramer, R. (ed.) EUROCRYPT 2005. LNCS, vol. 3494, pp. 457–473. Springer, Heidelberg (2005).

[4] Goyal, V., Pandey, O., Sahai, A., Waters, B.: Attribute-based encryption for fine-grained access control of encrypted Information. In: Proceedings of Computer and Communications Security, CCS 2006, pp. 89–98. ACM, New York (2006).

[5] Bethencourt, J., Sahai, A., Waters, B.: Ciphertext-policy attribute-based encryption. In: Proceedings of IEEE Symposium on Security and Privacy, pp. 321–334. IEEE Society Press, Los Alamitos (2007).

[6] Goyal, V., Jain, A., Pandey, O., Sahai, A.: Bounded ciphertext policy attributebased encryption. In: Aceto, L., Damg˚ard, I., Goldberg, L.A., Halld´orsson, M.M., Ing´olfsd´ottir, A., Walukiewicz, I. (eds.) ICALP 2008, Part II. LNCS, vol. 5126, pp. 579– 591. Springer, Heidelberg (2008).

[7] Waters, B.: Ciphertext-policy attribute-based encryption: an expressive, efficient, and provably secure realization. (2008), manuscript available at, http://eprint.iacr.org/2008/290

[8] Daza, V., Herranz, J., Morillo, P., R` afols, C.: Extended access structures and their cryptographic applications. To appear in Applicable Algebra in Engineering, Communication and Computing (2008), http://eprint.iacr.org/2008/502.

[9] Shamir, A.: How to share a secret. Communications of the ACM 22, 612–613 (1979).

[10] Lewko, A., Okamoto, T., Sahai, A., Takashima, K., Waters, B.: Fully secure functional encryption: attribute-based encryption and (hierarchical)

inner product encryption. To appear in Proceedings of Eurocrypt 2010 (2010), http://eprint.iacr.org/2010/110.

[11] Emura, K., Miyaji, A., Nomura, A., Omote, K., Soshi, M.: A ciphertext-policy attributebased encryption scheme with constant ciphertext length. In: Bao, F., Li, H., Wang, G. (eds.) ISPEC 2009. LNCS, vol. 5451, pp. 13–23. Springer, Heidelberg (2009)

[12] Javier Herranz , Fabien Laguillaumie , and Carla R`afols : Constant Size Ciphertexts in Threshold Attribute-Based Encryption. In PKC 2010, LNCS 6056, pp. 19–34, 2010.

[13] Delerabl´ ee, C., Pointcheval, D.: Dynamic threshold public-key encryption. In: Wagner,

[14] D. (ed.) CRYPTO 2008. LNCS, vol. 5157, pp. 317–334. Springer, Heidelberg (2008).

[15] Bagga, W., Molva, R.: Policy-based cryptography and applications. In: S. Patrick, A., Yung, M. (eds.) FC 2005. LNCS, vol. 3570, pp. 72–87. Springer, Heidelberg (2005).

[16] Al-Riyami, S., Malone-Lee, J., Smart, N.P.: Escrow-free encryption supporting cryptographic workflow. International Journal of Information Security 5(4), 217–229 (2006).

[17] Chai, Z., Cao, Z., Zhou, Y.: Efficient ID-based broadcast threshold decryption in ad hoc network. In: Proceedings of IMSCCS 2006, vol. 2, pp. 148–154. IEEE Computer Society, Los Alamitos (2006).

[18] Daza, V., Herranz, J., Morillo, P., R` afols, C.: CCA2-secure threshold broadcast encryption with shorter ciphertexts. In: Susilo, W., Liu, J.K., Mu, Y. (eds.) ProvSec 2007. LNCS, vol. 4784, pp. 35–50. Springer, Heidelberg (2007).

[19] Miyaji, A., Nakabayashi, M., Takano, S.: New explicit conditions of elliptic curve traces for fr-reduction. IEICE transactions on fundamentals of electronics, communications and computer sciences 84(5), 1234–1243 (2001).

[20] Abdalla, M., Dent, A.W., Malone-Lee, J., Neven, G., Phan, D.H., Smart, N.P.: Identitybased traitor tracing. In: Okamoto, T., Wang, X. (eds.) PKC 2007. LNCS,vol. 4450, pp. 361–376. Springer, Heidelberg (2007).

[21] Chase, M.: Multi-authority attribute based encryption. In: Vadhan, S.P. (ed.) TCC 2007. LNCS, vol. 4392, pp. 515–534. Springer, Heidelberg (2007).

[22] Nishide, T., Yoneyama, K., Ohta, K.: Attribute-based encryption with partially hidden encryptor-specified access structures. In: Bellovin, S.M., Gennaro, R., Keromytis, A.D., Yung, M. (eds.) ACNS 2008. LNCS, vol. 5037, pp. 111–129. Springer, Heidelberg (2008).

[23] Waters, B.: Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization. In: Cryptology ePrint report 2008/290 (September 1, 2008).

[24] Lewko, A., Waters, B.: Decentralizing attribute-based encryption. Cryptology ePrint Archive, Report 2010/351 (2010), http://eprint.iacr.org/

[25] Vladimir Bozovic and Daniel Socek and Rainer Steinwandt and Viktoria I. Villanyi.: Multi-authority attribute based encryption with honest-but-curious central authority. Cryptology ePrint Archive, Report 2009/083 (2009), http://eprint.iacr.org/

[26] Müller S, S. Katzenbeisser, and C. Eckert, *Distributed attribute-based encryption. ICISC 2008, LNCS 5461, pp. 20–36, 2009. Springer-Verlag Berlin Heidelberg 2009.*

[27] Muller, S., Katzenbeisser, S., and Eckert, C. 2009. On multi-authority ciphertext-policy attribute-based encryption. Bulletin of the Korean Mathematical Society 46, 4 (July), 803– 819.