Journal of Theoretical and Applied Information Technology
15th November 2021. Vol.99. No 21

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

AN EFFICIENT NONLINEAR ACCESS POLICY BASED ON QUADRATIC RESIDUE FOR CIPHERTEXT POLICY ATTRIBUTE BASED ENCRYPTION

ANCY P R[1], ADDAPALLI V N KRISHNA[2]

[1] Research Scholar, CSE Dept, School of Engineering and Technology, CHRIST (Deemed to be University), Bangalore, India

[2] Professor, CSE Dept, School of Engineering and Technology, CHRIST (Deemed to be University), Bangalore, India

E-mail: [1]ancy.prasadam@res.christuniversity.in, [2]adapalli.krishna@christuniversity.in

ABSTRACT

Ciphertext Policy Attribute Based Encryption (CP-ABE) is an efficient encryption scheme as data owner is making decision about the attributes that can access his data and adding that attributes to access structure while encrypting that message. Most existing CP-ABE scheme are based traditional access structure such as linear secret sharing scheme which incur large ciphertext size and linearly increases according to the number of attributes. And those schemes have more computational overhead for calculating share for each attribute and when recalculating secret in data user side. In this paper, we propose a different secret sharing scheme that can be used in access policy for CP-ABE which will reduce the size of ciphertext and there by communication overhead. Furthermore, the proposed scheme reduced computational overhead of secret sharing scheme and improved overall efficiency of the scheme.

Keywords: *Ciphertext Policy Attribute Based Encryption, Access Policy, Non-linear Secret- Sharing Scheme, Encryption, Quadratic Residue*

1. INTRODUCTION

Attribute Based Encryption scheme enables a data owner to storing data in a third party server securely by the concept of data outsourcing, Which means data can be encrypted by the data owner before sending to third party server. It was first introduced by Sahai and Waters[1] in their paper called fuzzy identity-based encryption. ABE is a form of public key encryption which provide one-to-many communication. Each user is identified by a set of attributes, and secret key is generated based on this attributes. In this scheme the data owner who wants to send data will encrypt the message and append some access policy with this data and send this data to third party storage. This is called outsourcing. This access policy describes who all can decrypt and read the message. In this paper we are focusing mainly on this access policy.

Access policies are mainly divided into different classes such as threshold, tree structure and secret sharing mechanism[2]. In the case of threshold gate access policy leaf node represents attributes and non-leaf node represent threshold gate. Generally we can express as (t, n)- threshold, where $1 \leq t \leq n$ at least t child node satisfied out of n number of children. When t=1 it represent OR gate and we can make it as AND gate by t=n. For example, consider the access policy as authorized user should have P and at least two attributes from the list {Q,R,S,T}. The Boolean formula P ∧ ((Q ∧ R) ∨ (Q ∧ S) ∨ (Q ∧ T) ∨ (R ∧ S) ∨ (R ∧ T) ∨ (S ∧ T)) can be represented as access tree representation (P,(Q,R,S,T,2),2) as shown figure 1.

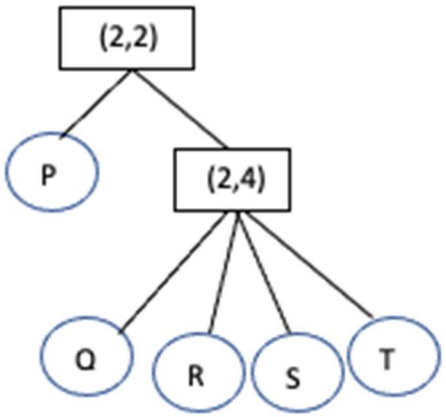

Figure 1: Access Structure Representation using Threshold Gate

In the case of access tree, the leaf node represent attributes and non-leaf node represents AND or OR gate. Access tree representation of the Boolean formula P AND (S OR (Q AND R)) is shown in figure 2.

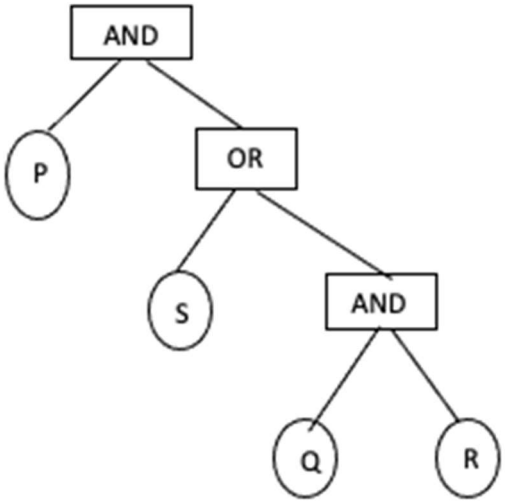

Figure 2: Access Tree Representation

Most common representation of monotone access structure is LSSS matrices [3]. An algorithm was proposed by Lewko and Waters for converting Boolean formula to LSSS matrices. Ciphertext include (M, ρ) which is nothing but LSSS matrix where M represent matrix and ρ is a function. And this function maps row of matrix to an attribute. As an example, an LSSS matrix is given in figure 3 which representing an access policy.

$$M = \begin{bmatrix} 1 & 1 & 0 \\ 0 & -1 & 0 \\ 0 & -1 & 1 \\ 0 & 0 & -1 \end{bmatrix} \quad \begin{matrix} \rho(1) = P \\ \rho(2) = S \\ \rho(3) = Q \\ \rho(4) = R \end{matrix}$$

Figure 3: An LSSS matrix example with each row represent attributes P, S, Q and R respectively.

Apart from these conventional access policies in this paper we are describing one new access policy which is based on quadratic residue [4]. In case of linear scheme if we take any secret, it is an element from finite field F. Secret is generated by doing linear mapping to secret and random field element [5]. The authorized group reconstruct secret by doing linear function to their shares. In our access policy secret sharing is done based on quadratic residue and it is explained in following sections.

1.1 Related Work

For encrypting data using a new scheme Sahai and Waters [1] introduced new scheme called attribute-based encryption in their paper called fuzzy identity-based encryption. Later Goyal et al [6] in their paper divide this scheme into two categories as KP-ABE and CP-ABE. Data owner encrypt the data using attributes and this encrypted data is decrypt using secret key associated by access policy in case of KP-ABE. And in the case of CP-ABE[3,7] data is encrypted using access policy and decrypted by secret key associated with set of attributes. Chase, M. [8] introduces the concept of multiauthority system. After that many works are came which is based on different variations in multiauthority schemes [9,10,11].

In this paper we are mainly focusing on access policy. About access policy there are mainly three categories such as threshold, access tree and secret sharing mechanism. Access structures [12] are explained in secure schemes for secret sharing and key distribution by Beimel. Sahai and Waters [1] proposed access structure based on threshold for the first time in their paper. In threshold scheme secret are divided into different parts and will fix one threshold if secret parts which are more than that threshold value only decrypt the message. The main advantage of this scheme is easy for implementation and less complexity when compare to other schemes. Now a days many works are going on threshold schemes. The tree structure [1] of access policy is based on “AND”, “OR” gates. This can be used

when the given Boolean formula are complex to express. In tree access structure leaf nodes represent attributes and non-leaf node represents "AND", "OR" gates. A new access structure was introduced to improve the security of the system which is based on Linear Secret-Sharing Schemes (LSSS) [3]. Lewko and Waters developed an algorithm that construct a LSSS matrix from any Boolean formulas [13]. According to this algorithm we can easily convert any access tree into corresponding LSSS matrix [14,15,16]. We explained this algorithm in following subsection. From the above mentioned main three access structure many different variant of access structures and in different environment [17,18,19] are introduced by many researchers and currently many researchers are working on this. One of this type is Blocked linear secret sharing scheme [20] this is a different variation of LSSS. Another one extension of LSSS is multi-linear secret sharing scheme [3] in which the we can convert any Boolean formula into LSSS matrix without converting to a minimal form.

1.2 Our Contribution

In this paper, we propose a new access policy for CP-ABE, which is based on quadratic residue. This is an efficient nonlinear secret-sharing scheme.

- In our paper we introduce a new access policy which is based on quadratic residue. This scheme is different from conventional LSSS matrix.
- This new access policy is an efficient nonlinear secret-sharing scheme which can be apply in CP-ABE.
- We explained how access policy based on LSSS matrix is working and how our nonlinear secret sharing scheme based on quadratic residue is working.

1.3 Organization

In section 2 we present some definitions and background. In section 3 we explained about construction and framework of CP-ABE and how we can implement quadratic residue in it. Section 4 we describe about the working of access policy based on LSSS matrix and how our new scheme with quadratic residue is working with an example. Finally, in section 5 we mention some open problem.

2. PRELIMINARIE

2.1 Bilinear Mapping

Consider two cyclic (multiplicative) groups $\mathbb{G}$ and $\mathbb{G}_T$ as of prime order p. The Bilinear mapping is represented as $e: \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$ having following three properties.

- Bilinearity: This is for any $g \in \mathbb{G}$ and any $\alpha, \beta \in \mathbb{Z}_p$, $e(g^\alpha, g^\beta) = e(g,g)^{\alpha\beta}$.
- Nondegeneracy: For a generator g of $\mathbb{G}$, $e(g,g) \neq 1_{\mathbb{G}_T}$.
- Computability: That is for any $g \in \mathbb{G}$ and any $\alpha, \beta \in \mathbb{Z}_p$, an algorithm is there to compute $e(g^\alpha, g^\beta)$ in polynomial time.

2.2 Access Structures

Let set $\{P_0, P_1, \ldots, P_{n-1}\}$ denotes parties. The collection $\mathbb{A} \subseteq 2^{P_0, P_1, \ldots, P_{n-1}}$ where access structure $\mathbb{A}$ is called monotone if it satisfies $X \in \mathbb{A}$ and $X \subseteq Y$ imply $Y \in \mathbb{A}$. Access structure is a monotone collection $\mathbb{A}$ of subsets in $\{P_0, P_1, \ldots, P_{n-1}\}$ which should be non-empty. Authorized sets are the sets in $\mathbb{A}$. The set B is called minimal set in $\mathbb{A}$ if and only if $B \in \mathbb{A}$, and for each $C \subsetneq B$ it should be $C \notin \mathbb{A}$[4].

2.3 Linear Secret Sharing Schemes(LSSS)

A secret sharing scheme Π over a set of parties $\mathcal{P}$ can be called as linear (over $\mathbb{Z}_p$) if it satisfies following two conditions such as:

- A vector over $\mathbb{Z}_p$ is formed by shares of party and
- There exists a matrix M called the share-generation matrix for Π. M contains p rows and q columns. And for every i, where i =1,2,…,p, the i^{th} row M_i of matrix M can be denoted by a party $\rho(i)$ where this ρ is a function from {1,2,…,p} to $\mathcal{P}$. Column vector $\vec{v}$ is given such that $\vec{v} = \{s, r_2, r_3, \ldots, r_q\}$, where $s \in \mathbb{Z}_p$ represent the secret which is to be shared and $r_2, r_3, \ldots, r_q \in \mathbb{Z}_p$ are chosen randomly. Vector $M\vec{v}$ is p shares of the secret s according to Π. The share $\lambda_i = (M\vec{v})_i$, ie, the inner product $M_i.\vec{v}$ which belongs to party $\rho(i)$.

As define in [12], any LSSS as we define above is reconstructed as follows. Let authorized set be $S \in \mathbb{A}$, and $I \subset \{1,2,\ldots,m\}$ is defined as $I = \{i: \rho(i) \in S\}$. There exist an constants $\{\omega_i \in \mathbb{Z}_p\}_{i \in I}$ satisfying

$\sum_{i\in I}\omega_i M_i = (1,0,\ldots,0)$, so that if $\{\lambda_i\}$ are valid shares of secret s, then $\sum_{i\in I}\omega_i\lambda_i = s$. Also, these constants $\{\omega_i\}$ can be calculated in polynomial time in the size of the share-generating matrix M. There is no such constant for unauthorized set. The LSSS is represented by (M,ρ), and the number of rows of M, that is p denotes its size.

2.4 Quadratic Residue

It can be explained as, an integer ω is said to be a quadratic residue modulo u if it satisfies two conditions such as $\gcd(\omega,u)=1$ and there should exist an integer b such that $\omega \equiv b^2 \bmod u$. If $\gcd(\omega,u)=1$ and there is no integer b such that $\omega \equiv b^2 \bmod u$ it is said to be quadratic non-residue. In our case the modulus is considered as odd prime p, and thus ω and b may be considered as the elements of the field $\mathbb{Z}_p$[4].

3. OUR CONSTRUCTION

3.1 Overview

We provide the construction of the CP-ABE scheme in this section. The system contains below mentioned entities.

- Attribute authority: Attribute authority is the entity which control attribute universe. Its main duty is to check validity of the user's attribute. If that is an authorized user it sends a secret key according to his attribute. It generates its own master secret key and public parameter.
- Data Owner: Data owner is the one who wants data to store in a third party storage. Based on an access policy that who are all the user that can read his message, he/she will create an access policy and message is encrypted with that access policy.
- User: Each user has set of attributes and its corresponding secret key. If secret key of a user matches the access policy of message he/she can read the message. Otherwise the permission will be denied.
- Semi trusted third party storage: This entity is in charge of storing outsourced data, ie data owner encrypts data and send to third party storage. This is the place where user store data and it can be any kind of storage service.

3.2 Framework

In our framework we have four algorithms such as: Setup, Encrypt, KeyGen, and Decrypt. We will explain each algorithm in detail.

Setup $(\lambda, \mathrm{U}) \rightarrow (PK, MSK)$ The input to this algorithm are security parameter λ and attribute universe U. Public parameters PK and a master key MSK are the outputs. This algorithm initialise the system.

Encrypt $(PK, \mathbb{A}, M) \rightarrow CT$ This algorithm is to encrypt the message for that it takes input as public parameters PK, a message M, and an access structure $\mathbb{A}$. Output is the respective ciphertext CT. It can decrypt only by an user that having attributes that satisfies the access structure.

KeyGen $(MSK, S) \rightarrow SK$ The algorithm generates private key SK by taking input as master secret key MSK, and a set of attributes S.

Decrypt $(PK, CT, SK) \rightarrow M$ The decryption algorithm decrypts ciphertext and generate back message by taking input as the public parameters PK, a ciphertext CT, which contains an access policy, and a private key SK. If set S of attributes satisfies the access structure, then the algorithm returns message M.

4. QUADRATIC RESIDUE IN CP-ABE SCHEME

4.1 Construction

In this section we have shown the construction of LSSS matrix which is commonly using and our proposed scheme based on quadratic residue. In the case of CP-ABE the data owner encrypts the data with access policy and store it in third party storage. This access policy represents who all can decrypt this data. Each user will have a set of attributes. Based on this attribute a secret key is generate. The user will use this secret key to decrypt data. If the attributes in the secret key matches the attribute in access policy, he is an authorized user and he can decrypt the data otherwise he can't access the data.

4.1.1 Linear secret sharing matrix construction

Lewko and Waters developed an algorithm that construct a LSSS matrix from any Boolean formulas [13]. Below we are explaining this algorithm briefly with an example. The input is any access tree, that is the representation of any monotone Boolean formula. Output is the corresponding LSSS matrix. First, we have to convert monotone Boolean formula to equivalent but shorter form.

For example, if the Boolean formula is: $T\wedge((P\wedge Q)\vee(P\wedge R)\vee(P\wedge S)\vee(Q\wedge R)\vee(Q\wedge S)\vee(R\wedge S))$
The equivalent but compressed Boolean formula is $T\wedge(((P\wedge Q)\vee(R\wedge S))\vee((P\vee Q)\wedge(R\vee S)))$

Journal of Theoretical and Applied Information Technology
15th November 2021. Vol.99. No 21

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

The algorithm first initializes root node vector, v as (1), is a vector and its length is 1. Then initialize counter variable, c as 1. As next step it goes down each level and labels each node as follows:

- Parent node: OR gate with vector v
  label both children as v
  c is unchanged;
- Parent node: AND gate with vector v,
  Append v with 0's at end and make it same as the length of c
  label left child with vector v||1 (|| represent concatenation)
  right child with vector (0,….,0)||-1 ((0,…,0) is of length c) increment c by 1.

As an example, consider the Boolean formula P AND (S OR (Q AND R)). The access tree representation of the given formula is shown below in figure 4 with the labels for each node we got after applying Lewko and Waters algorithm.

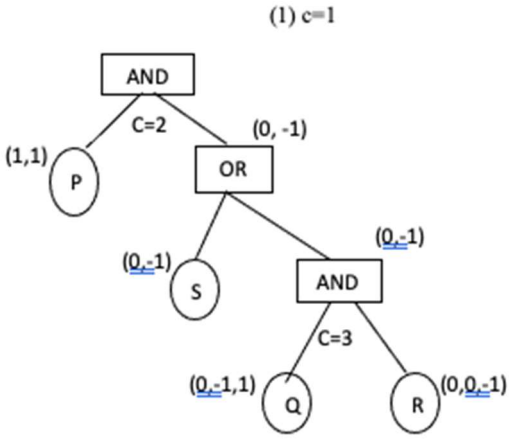

Figure 4: Access tree representation of the Boolean formula P AND (S OR (Q AND R)).

The rows of LSSS matrix are corresponding labelling of leaf node. We append shorter length vector with 0's to form same length vectors. LSSS matrix is:

$$\begin{bmatrix} 1 & 1 & 0 \\ 0 & -1 & 0 \\ 0 & -1 & 1 \\ 0 & 0 & -1 \end{bmatrix} \begin{matrix} \rho(1) = P \\ \rho(2) = S \\ \rho(3) = Q \\ \rho(4) = R \end{matrix}$$

A secret sharing scheme $\prod$ over a set of parties $\mathcal{P}$ (attributes) is called linear if:

Given a column vector $v = (s, r_2, \ldots, r_n)$

$$v = \begin{bmatrix} 2 \\ 4 \\ 5 \end{bmatrix}$$

The secret is 2 and the share $\lambda_i = (M\, v)_i$, belongs to party $\rho(i)$

$$\lambda_1 = [1 \quad 1 \quad 0] \begin{bmatrix} 2 \\ 4 \\ 5 \end{bmatrix}$$

λ_1 =6
λ_2 =-4
λ_3 =1
λ_4 =-5
I={i : ρ(i) ϵS}
I={{1,2}{1,3,4}}, Which means the authorized ser are {{P,S},{P,Q,R}}.
There exist constants $\{\omega_i \epsilon Z_p\}_{i \epsilon I}$ satisfying $\sum_{i \in I} \omega_i M_i = (1,0, \ldots\ldots,0)$
So that if $\{\lambda_i\}$ are valid shares of any secret s according to $\prod$, then $\sum_{i \in I} \omega_i \lambda_i = s$
Consider {1,2}

$$\sum_{i \in I} \omega_i M_i = (1,0, \ldots\ldots,0)$$

$\omega_1[1 \quad 1 \quad 0] + \omega_2[0 \quad -1 \quad 0] = (1,0,0)$
$[\omega_1 \quad \omega_1 \quad 0] + [0 \quad -\omega_2 \quad 0] = (1,0,0)$
ω_1=1, ω_2=1

$$\sum_{i \in I} \omega_i \lambda_i$$

=1*6+1*-4
=2, which is the secret.ie, {P, S} is an authorized set.

Consider {1,3}

$$\sum_{i \in I} \omega_i M_i = (1,0, \ldots\ldots,0)$$

$\omega_1[1 \quad 1 \quad 0] + \omega_3[0 \quad -1 \quad 1] = (1,0,0)$
ω_1=1, ω_3=1

$$\sum_{i \in I} \omega_i \lambda_i$$

=1*6+1*1
=7, which is not the secret, ie {P, R} is an unauthorized set.

In general,

p_2	1	1	0	1	s	$s+r_2+r_4$
p_2	0	1	1	0	r_2	r_2+r_3
p_1	0	1	1	0	r_3	r_2+r_3
p_3	1	1	0	0	r_4	$s+r_2$
p_4	0	0	1	1		r_3+r_4

4.1.2 Access policy with quadratic residue

Consider Z_p be the ring of integers modulo u, and its elements are denoted with the integers {0, 1, . . . , p−1}. Any integer ω is said to be a *quadratic residue* modulo u if it should satisfy two conditions such as gcd (ω, p)=1 and there should exists an integer b such that $\omega \equiv b^2 \bmod p$. Otherwise, it is called *quadratic non-residue*. In this paper we are

considering n-party access structure. Where, n=2m. Parties are denoted by p_i^b, where $0 \leq i < m$ and $b \in \{0,1\}$. The dealer chooses random $m-1$ elements $z_0, z_1, \ldots, z_{m-2} \in z_p$ and an additional random element $r \in z_p$. Define $z_{m-1} = -\Sigma_{i=0}^{m-2} z_i$[4]. Each parties have shares and it specified in the table 1.

Table 1. Secret Sharing Scheme based on Quadratic Residue.

	$s=0$	$s=1$
P_0^b	$r^2 + z_0$	$br^2 + z_0$
$P_i^b 1 \leq i < m$	z_i	$2^i br^2 + z_i$

Correctness and privacy are the main feature of the above-mentioned scheme is based on the following.
$SUM_\omega = \omega^s r^2$.
Let SUM_ω means the sum of the m shares of parties in B_w. B_w is a set of size m and it is defined by $B_w = \{P_i^{\omega_i} : 0 \leq i < m\}$.
Here we are considering two conditions which is based on the secret such as *s=0 and s=1.*

If s=0 then
$SUM_\omega = r^2$.
If s=1 then
$SUM_\omega = r^2\omega$.

We consider two types of minimal authorized sets B:

- $B=\{p_i^0, p_i^1\}$
  s=0, iff shares of p_i^0 and p_i^1 are equal
- $B=B_\omega$, ω is not a quadratic residue modulo p. (ie either 0 or or quadratic non-residue)
  s=0, iff SUM_ω is a quadratic residue.

Access policy with quadratic residue can replace regular access policy. Some of the access policy that are commonly using are Boolean formula, access tree and LSSS matrix. It can only realize access structures in NC. So, in this paper we have introduce a new access policy which is based on quadratic residue. We can represent any access structure by using quadratic residue that cannot represent using convectional access policy.

4.2 Example of Access Policy with Quadratic Residue.

In this section we are explaining our proposed access policy which is based on quadratic residue with an example.

As an example, consider p=7. We can write set Z_7 as:
Z_7= {1,2,3,4,5,6}
To find the quadratic residue:

$1^2 \bmod 7 = 1$	gcd (1,7) =1
$2^2 \bmod 7 = 4$	gcd (2,7) =1
$3^2 \bmod 7 = 2$	gcd (3,7) =1
$4^2 \bmod 7 = 2$	gcd (4,7) =1
$5^2 \bmod 7 = 4$	gcd (5,7) =1
$6^2 \bmod 7 = 1$	gcd (6,7) =1

From above we found {1,2,4} is quadratic residue and {3,5,6} is quadratic non residue.
{1,2,4} is quadratic residue and its binary representation is (0001,0010,0100).
{3,5,6} is quadratic non residue and its binary representation is (0011,0101,0110).
Consider our attributes are $\{p_0^0, p_0^1, p_1^0, p_1^1\}$.
And the possible combination of attributes is given below:
$\{\{p_0^0\},\{p_0^1\},\{p_1^0\},\{p_1^1\},\{p_0^0,p_0^1\},\{p_0^0, p_1^0\},\{p_0^0,p_1^1\}, \{p_0^1,p_1^0\},\{p_0^1, p_1^1\},\{p_1^0,p_1^1\},\{p_0^0,p_0^1,p_1^0\},\{p_0^0,p_1^0,p_1^1\}, \{p_0^1,p_1^0,p_1^1\},\{p_0^0,p_0^1,p_1^0,p_1^1\}\}$
Here we are having 4 attributes so n=4. All other values are obtained from above mentioned definition.
n=4
m=2
z_0=4
r=2
z_1=-4
From these values and above table we calculate secret-sharing table. The values for this example are given below.

	S=0	S=1
p_0^0	8	4
p_0^1	8	8
p_1^0	-4	-4
p_1^1	-4	4

Let us consider we have two authorized set such as $\{\{p_0^0, p_1^1\}, \{p_0^0, p_0^1, p_1^0\}\}$.

From the definition we can identify minimal authorized sets B:

B = $\{p_i^0, p_i^1\}$

$\{\{p_0^0, p_0^1\}, \{p_1^0, p_1^1\}\}$
B= B_ω
$\{\{p_0^0\}, \{p_1^0\}, \{p_0^0, p_1^0\}, \{p_0^1, p_1^1\}, \{p_0^0, p_1^1\}, \{p_0^0, p_0^1, p_1^0, p_1^1\}\}$
First let consider two attributes $\{p_0^0, p_1^1\}$ and secret s=0.
So, if we calculate SUM_ω and $\omega^s r^2$ we can find that both are same and the values are given below. Which means this is an authorized set.
SUM_ω=4 and $\omega^s r^2$=4
Consider another set $\{p_0^0, p_0^1, p_1^0\}$ and secret s=1.
So, if we calculate SUM_ω and $\omega^s r^2$ we can find that both are same and the values are given below. Which means this is an authorized set.
SUM_ω=8 and $\omega^s r^2$=4*2=8
Now consider another set $\{p_0^0, p_0^1\}$ and secret s=0.
If we calculate SUM_ω and $\omega^s r^2$ we can find that both are different values and the values are given below. Which means this is an unauthorized set.
SUM_ω=16 and $\omega^s r^2$=4
Like this we can identify authorized and un authorized set.

5. DISCUSSION

A new access policy which is based on quadratic residue is proposed in this paper. Which is based on nonlinear secret-sharing scheme apart from conventional access policy. This scheme thus improves efficiency and security of the system. We can also find that this scheme is easy to implement. We explained both schemes that is LSSS matrix and access policy using quadratic residue with an example. We identified that this new scheme is more powerful than linear schemes because in case of linear secret sharing matrix scheme they cannot efficiently realize access structures outside NC[4].

6. CONCLUSION

Attribute based encryption is a prominent area in cryptography where many researches are going on. Many works are going on different aspect of attribute-based encryption. In this paper we introduce a new access policy which is based on quadratic residue. It is an efficient nonlinear secret sharing scheme. This can be implemented in any CP-ABE to improve the security of the system. Based on the study that we conducted on literature we identified that non-linear secret sharing scheme can implement in any access policy. It can improve access structure without converting into matrix. In this paper we explained conventional LSSS matrix and our proposed access policy using quadratic residue with an example. Most of the work in access policy of attribute-based encryption are done on access tree and LSSS matrix so our paper introduces a new concept.

REFERENCES:

[1] A. Sahai, B. Waters, "Fuzzy identity-based encryption", in: *Theory and Applications of Cryptographic Techniques, Springer Berlin Heidelberg,* 2005, pp. 457-473.
[2] Sun, Pan Jun. "Privacy protection and datasecurity in cloud computing: a survey, challenges, and solutions." *IEEE Access* 7, 2019, 147420-147452.
[3] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," *Proc. - IEEE Symp. Secur. Priv.*, 2007, pp. 321–334.
[4] Beimel, Amos, and Yuval Ishai. "On the power of nonlinear secret-sharing." *Proceedings 16th Annual IEEE Conference on Computational Complexity*. IEEE, 2001.
[5] T. M. Laing, K. M. Martin, M. B. Paterson, and D. R. Stinson, "Localised multisecret sharing," *Cryptogr. Commun.*, 2017, vol. 9, no. 5, pp. 581–597.
[6] Ali, Mohammad, et al. "A fully distributed hierarchical attribute-based encryption scheme." *Theoretical Computer Science* 815, 2020, 25-46.
[7] S. V. Gadge, "Analysis and Security based on Attribute based Encryption for data Sharing," *Int. J. Emerg. Res. Manag. &Technolog*, 2014, vol. 3, no. 3, pp. 74–78.
[8] Melissa Chase, "Multi-authority attribute-based encryption," *In Theory of cryptography conference,* 2007, pp. 515-534.
[9] R. Guo, X. Li, D. Zheng, and Y. Zhang, "An attribute-based encryption scheme with multiple authorities on hierarchical personal health record in cloud," *J. Supercomput.*, 2018.
[10] V. K. Arthur Sandor, Y. Lin, X. Li, F. Lin, and S. Zhang, "Efficient decentralized multi-authority attribute-based encryption for

mobile cloud data storage," *J. Netw. Comput. Appl.*, 2019, vol. 129, pp. 25–36.

[11] Wei, J., Liu, W., & Hu, X. "Secure and efficient attribute-based access control for multiauthority cloud storage". *IEEE Syst. J*, 2018, pp. 1731-1742.

[12] A. Beimel, "Secure schemes for secret sharing and key distribution," Ph.D. dissertation, Faculty Comput. Sci., Technion–Israel Inst. Technol., Haifa, Israel, 1996.

[13] Lewko, A., & Waters, B. "Decentralizing attribute-based encryption". In*Annual international conference on the theory and applications of cryptographic techniques,* 2011, pp. 568-588, Springer, Berlin, Heidelberg.

[14] H. Wang, Z. Zheng, L. Wu, and P. Li, "New directly revocable attribute-based encryption scheme and its application in cloud storage environment," *Cluster Comput.*, 2017, vol. 20, no. 3, pp. 2385–2392.

[15] Y. S. Rao, "A secure and efficient Ciphertext-Policy Attribute-Based Signcryption for Personal Health Records sharing in cloud computing," *Futur. Gener. Comput. Syst.*, 2017, vol. 67, pp. 133–151.

[16] J. Li, Y. Zhang, X. Chen, and Y. Xiang, "Secure attribute-based data sharing for resource-limited users in cloud computing," *Comput. Secur.*, 2018, vol. 72, pp. 1–12.

[17] J. Fu and N. Wang, "A Practical Attribute-Based Document Collection Hierarchical Encryption Scheme in Cloud Computing," *IEEE Access*, 2019, vol. 7, no. c, pp. 36218–36232.

[18] Q. He, N. Zhang, Y. Wei, and Y. Zhang, "Lightweight attribute-based encryption scheme for mobile cloud assisted cyber-physical systems," *Comput. Networks*, 2018, vol. 140, pp. 163–173.

[19] L. Zhang, Y. Cui, and Y. Mu, "Improving Security and Privacy Attribute Based Data Sharing in Cloud Computing," *IEEE Syst. J.*, 2019, pp. 1–11.

[20] J. Wang, C. Huang, N. N. Xiong, and J. Wang, "Blocked linear secret sharing scheme for scalable attribute-based encryption in manageable cloud storage system," *Inf. Sci. (Ny).*, 2018, vol. 424, pp. 1–26.

[21] Amos Beimel, Aner Ben-Efraim. "Multi-linear Secret-Sharing Schemes". *International Association for Cryptologic Research*., 2014, LNCS 8349, pp. 394–418.