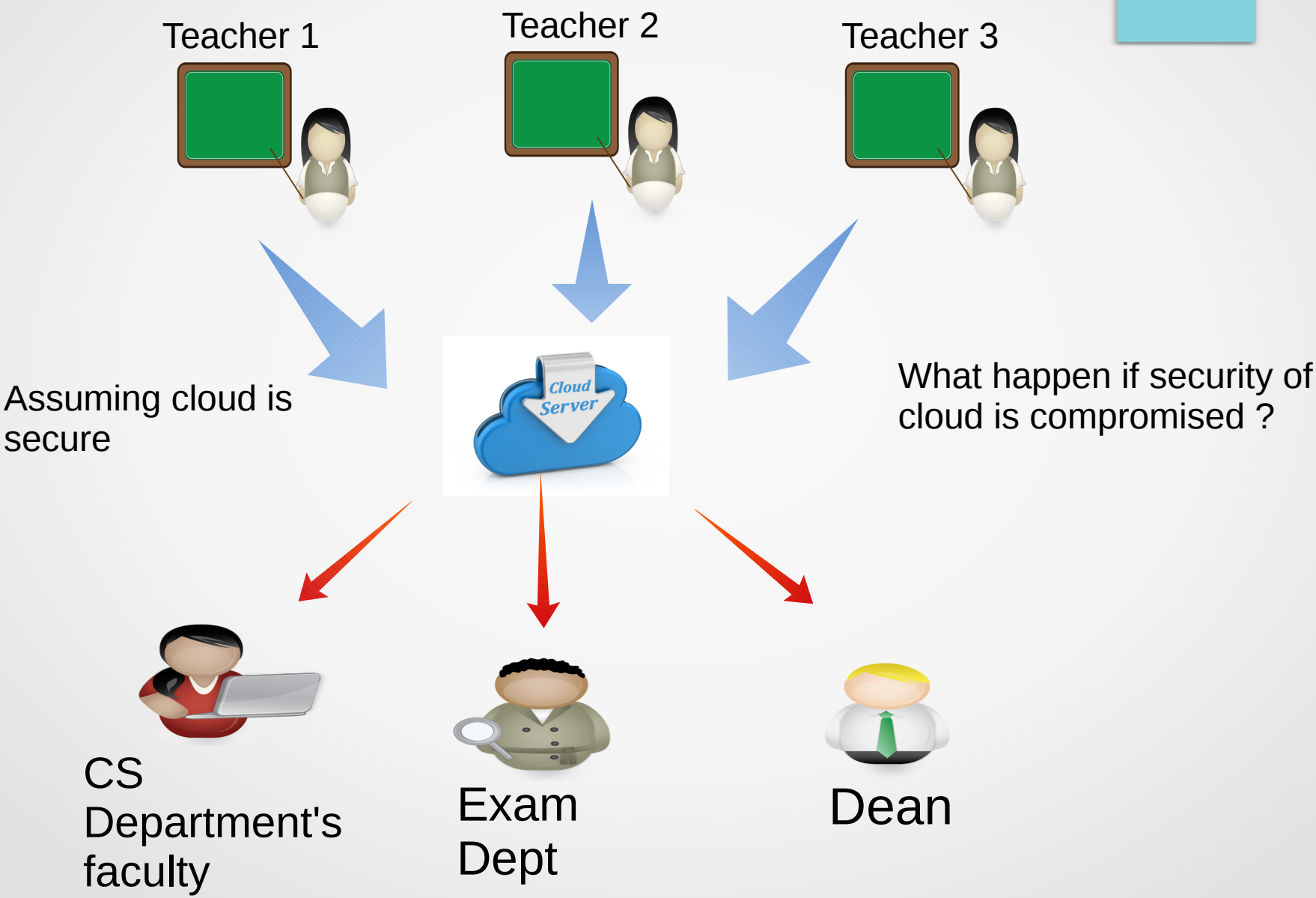
Temporal Access Control on Cloud Data

By

Ayan Das
[Roll No: CS-1414]

Under the guidance of
Dr. Sushmita Ruj

Motivation


Teacher 1
Teacher 2
Teacher 3
Assuming cloud is secure
Cloud Server
What happen if security of cloud is compromised ?
CS Department's faculty
Exam Dept
Dean

Abstract

Cloud storage is a model of data storage in which the digital data is stored in remote server. The physical storage spans multiple servers (and often locations), and the physical environment is typically owned and managed by a hosting company. These cloud storage providers are responsible for keeping the data available and accessible.

Generally data is used to store in cloud without any encryption. But The two big concerns about cloud storage are reliability and security. Clients are not likely to entrust their data to another company without a guarantee that they will be able to access their information whenever they want and no one else will be able to get at it. One solution of these problem is temporal access control which is based on attribute based encryption.

Abstract continued

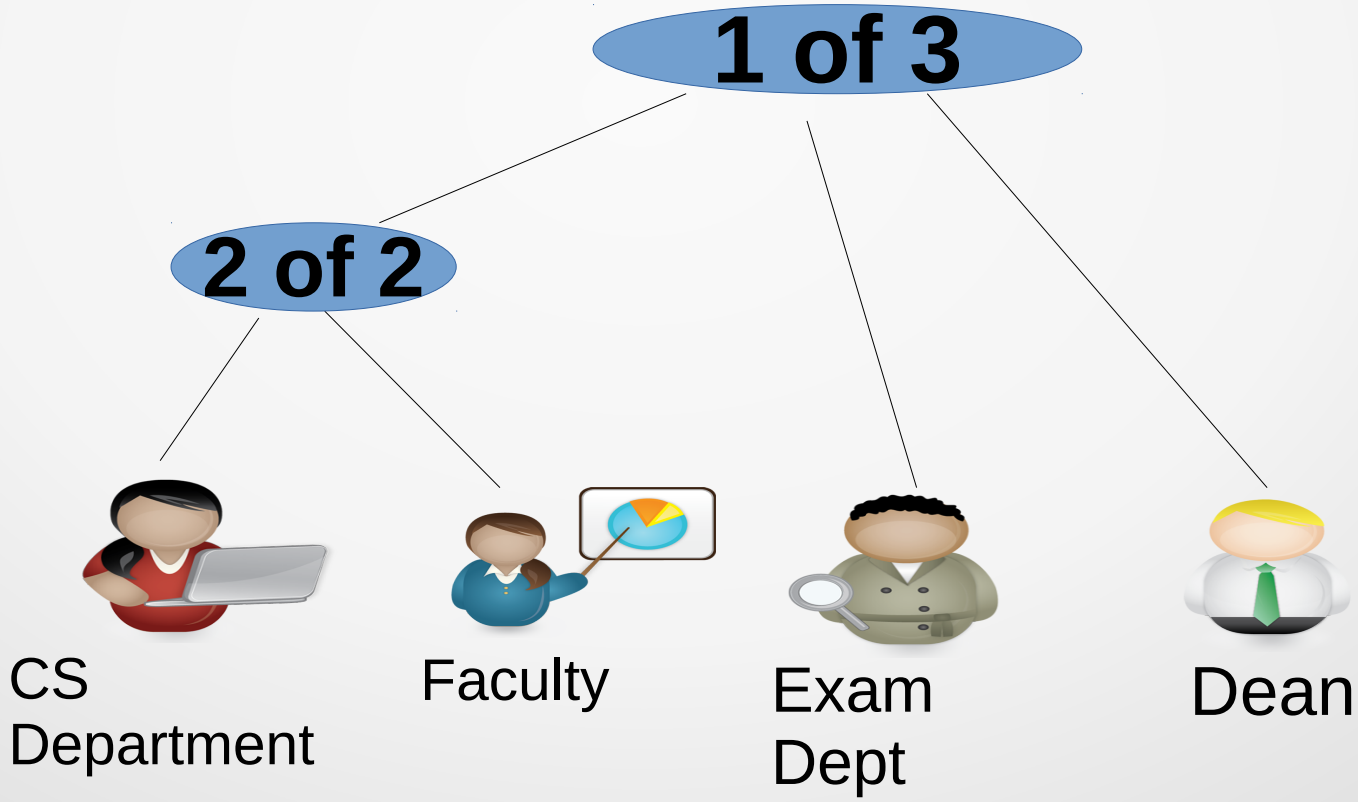
Attribute-based access control is one of the most important security mechanisms for data storage, especially in cloud computing. Attribute-based encryption is an attribute-based access control mechanism which requires data to be kept encrypted at servers. This data is open to access to all, but can be decrypted only by those users whose attributes satisfy a given access policy. Also the data owner can revoke any authorized user from decrypting the data in any point of time. An issue in attribute-based encryption is huge time complexities for generating the keys and encrypting the content. The problem becomes critical when the number of attributes is large, however little work has been done to develop schemes that support efficient and reliable storage of data in cloud with temporal access control. Here, we review some of the important work that has been done in this field. We then present a protocol which improves the efficiency, scalibilty and makes it feasible for real time implementation. We also analyze it's time and communication complexity to demonstrate the efficiency of our methodology. Another merit of our scheme is that the computationally intense task is outsourced to the cloud without compromising on the security of the scheme. In this way, we propose a comprehensive scheme which promises encompass all the major issues in attribute-based encryption.

Access Control

- refers to a method of selectively granting access to a resource
- Example : social networks like Facebook, statuses, photos, videos, and posts have to visible only to a fixed set of Friends. And once a user is removed from friend list, he will not be able to access the content further.

Attribute Based Encyption

- Consider result of CS department before publishing
- What is access structure
- (CS Dept AND Faculty) OR (Exam Dept) OR (Dean)

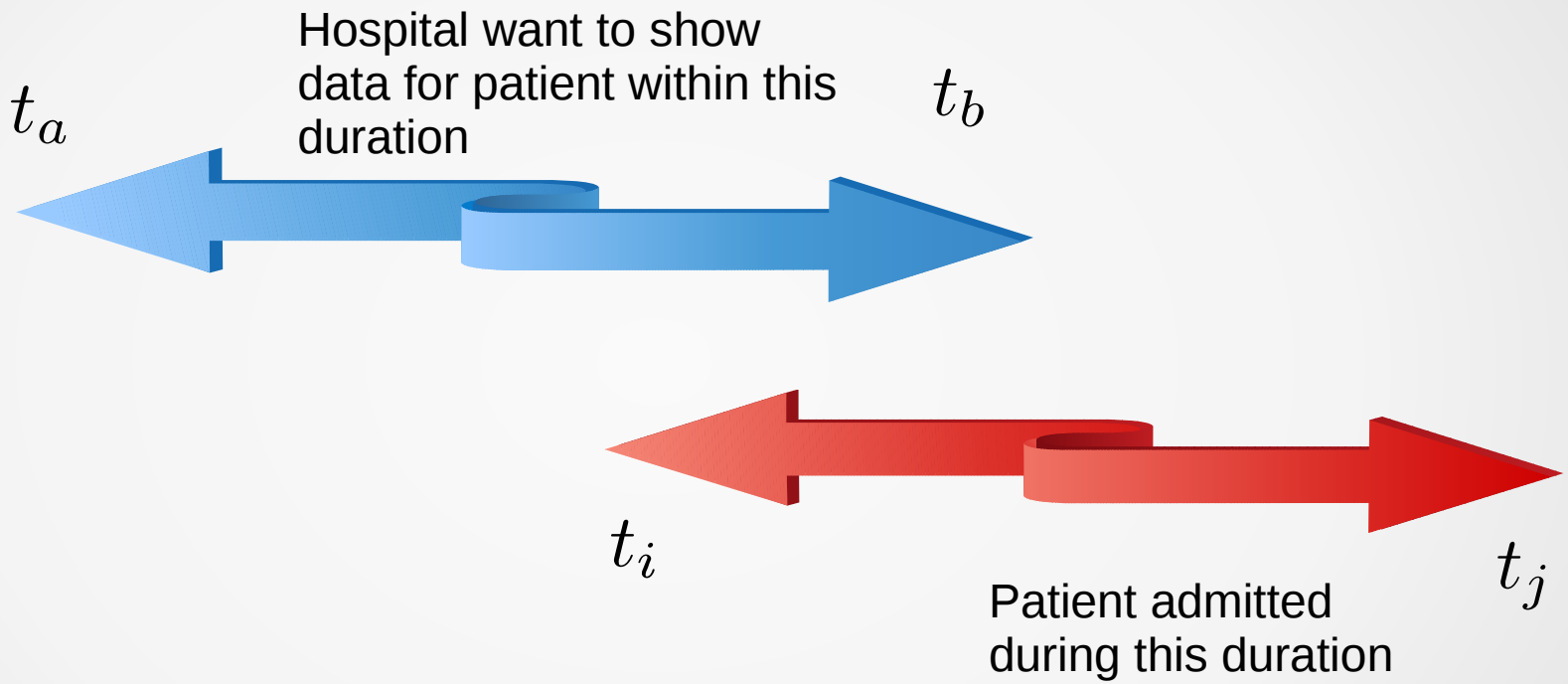


Extra features for Attribute Based Encryption on cloud data

- User revocation
- Two phase encryption
- Distributed Key generation
- Decryption outsouring
- Temporal Constraints

Our cipher policy attribute based encryption have all these features.

Temporal Attribute



$$t_i < t_b \text{ and } t_a < t_j$$

My Contribution

- Our first TA scheme support user revocation and decryption outsourcing with temporal attribute.(scheme-3)
- We have shown two basic scheme derived from previous scheme:-

  1. Scheme without decryption Outsourcing and revocation (scheme 1)

  2. Scheme without decryption Outsourcing with revocation (scheme-2)
- Divide encryption into two phases . First offline encryption then online encryption(scheme-4)
- On scheme-4 I divided key generation to different authorities. (scheme-5)
- We have shown analytically and graphically that key generation and encryption cost reduced compared to other existing CPABE scheme.
- proved the security of our scheme from differnt aspects.

Forward and backward derivation function

All the temporal attribute have two values v_{t_i} and v_{t_j}

- Definition :Given a function f : V → V , it is called a forward derivation function if it satisfies the conditions:

  1. Easy to compute: the function f can be computed in polynomial-time, if

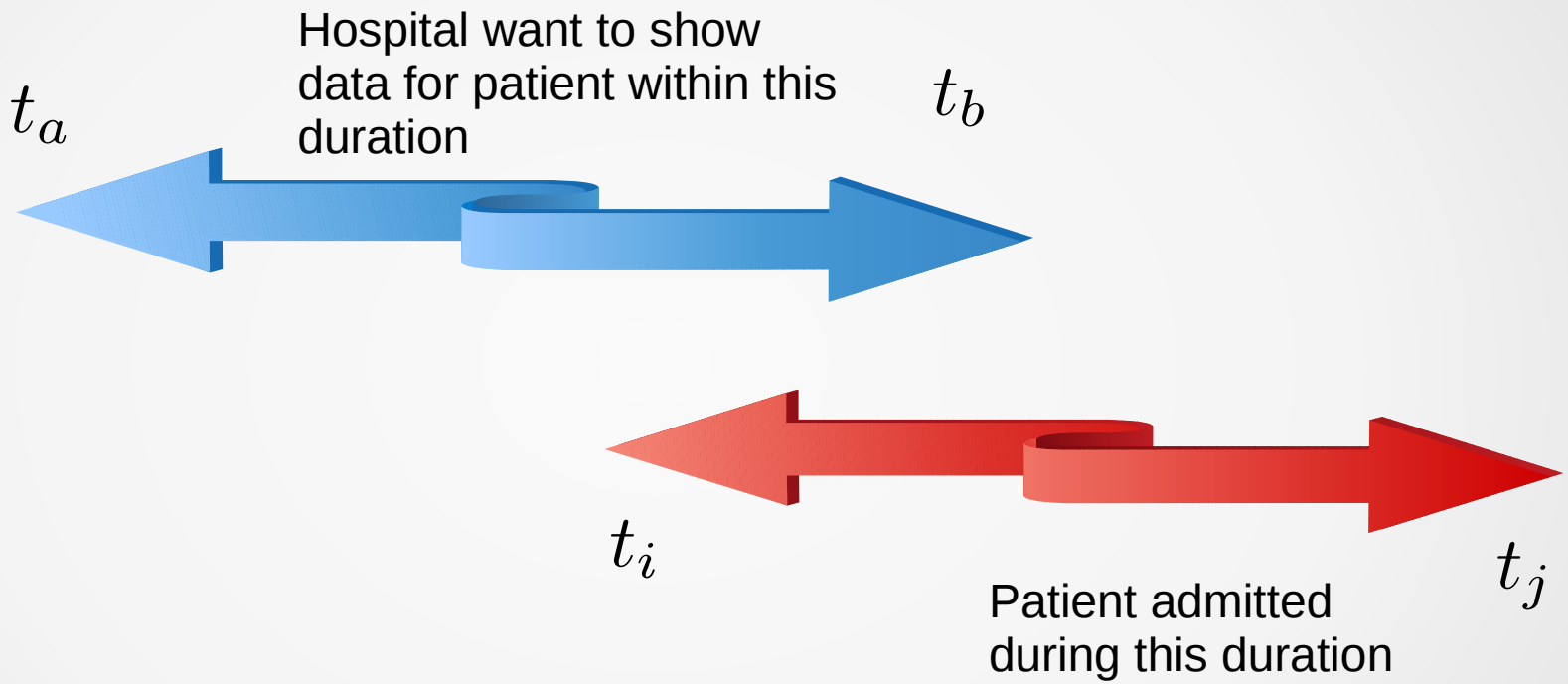
  $$\mathrm{t}_i \leq t_j, \text{ i.e., } v_{t_j} \leftarrow f_{t_i \leq t_j}(v_{t_i})$$

  2. Hard to invert: it is infeasible for any probabilistic polynomial (PPT) algorithm to compute

  $$\mathrm{v}_{t_i} \text{ from } v_{t_j} \text{ if } t_i < t_j$$

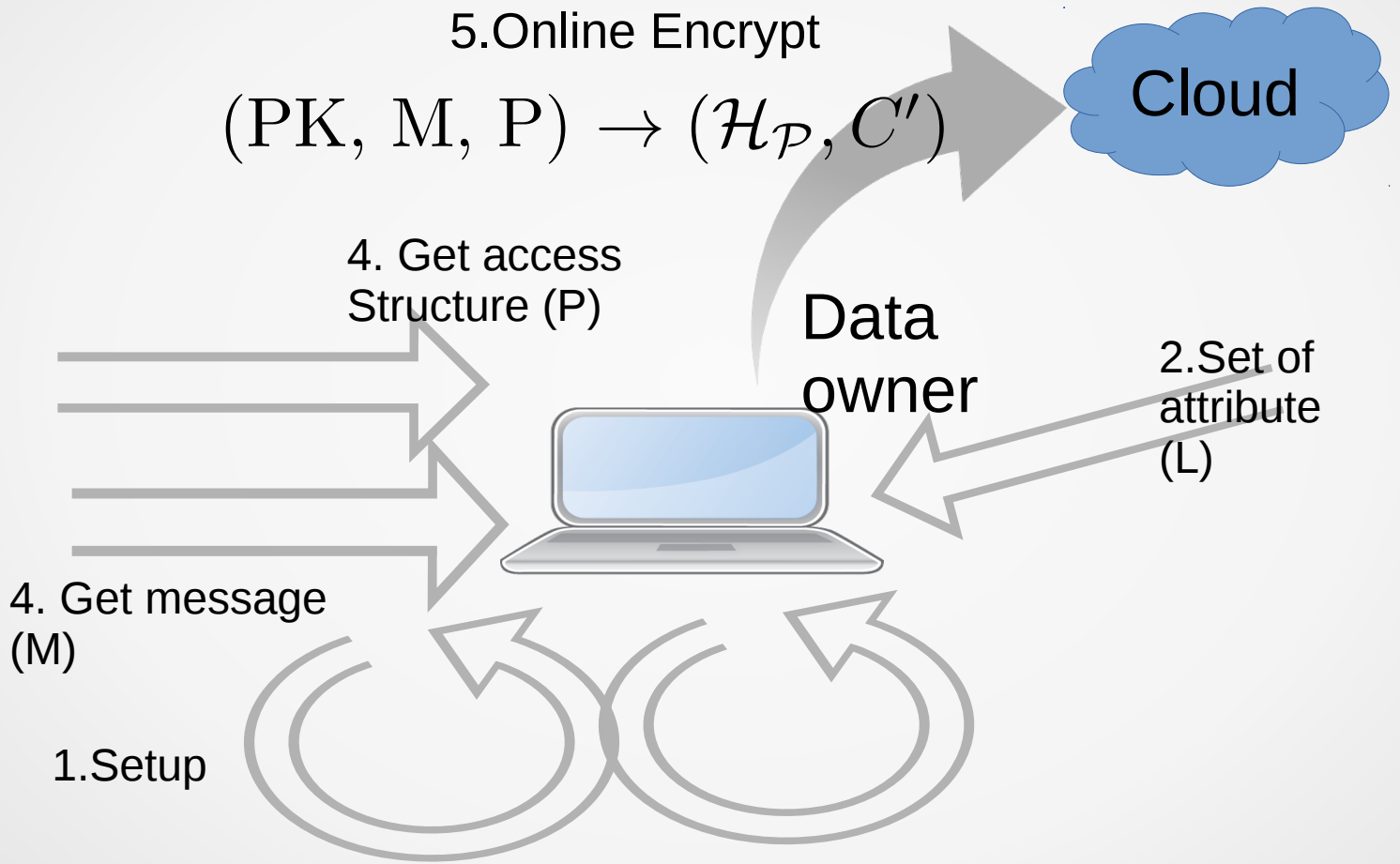
- How it help in satisfying temporal attribute?

Temporal Attribute



$$t_i < t_b \text{ and } t_a < t_j$$

TA Scheme with two phase encryption



Decryption process

7.Get data

$(\widetilde{SK}_{\mathcal{L}'}, \mathcal{H}_{\mathcal{P}}) \rightarrow \widetilde{\mathcal{H}_{\mathcal{P}}}$

8.Decrypt proxy

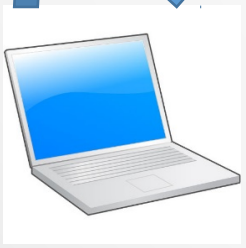
9. Return Content

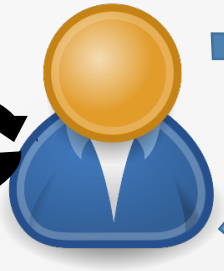
6. Request proxy

$(\mathrm{MK}, \mathrm{u}_k, \mathcal{L}) \rightarrow SK_{\mathcal{L}}$

2.Generate Key

3.Send Key





5.Delegate

$(\mathrm{SK}_{\mathcal{L}}, \mathcal{L}') \rightarrow \widetilde{SK}_{\mathcal{L}'}$

1.Request Key

4.ProxyReKey

$(\mathrm{PK},\mathrm{MK},\mathrm{RL}) \rightarrow PXK$

10.Decrypt User

$(\mathrm{SK}_{\mathcal{L}}, \widetilde{\mathcal{H}_{\mathcal{P}}}, C') \rightarrow M$

Problems with the previous schemes

Suppose I can encrypt a message such that if anyone have any 2 of the 3 valid document can decrypt.

- Driving licence
- University pass certificate
- Voter id

I need a key generation authority that can validate all the 3 document.

Can a single authority validate all these three in practical senario?

TA Scheme with decentralized key Gen

$(\mathrm{PK}, \tau_{k_0}) \rightarrow SK_{\mathcal{L}}$

Generate central Key

Send Key

Request Key

Decryptor

Keygen

$(\mathrm{MK}, \mathrm{u}_k, \mathcal{L}_m) \rightarrow SK_{\mathcal{L}_m}$

Authority for voter id

For university certificate

For driving licence

Performance Comparision platform

- Intel Core i3-5010U CPU @ 2.10GHz*4 with 4 GB of RAM and Ubuntu 14.04 using JPBC library We used two type of bilinear map. 1st one is type-A(prime order with q = 512 and r = 160 bits) for CPABE and KPABE and other is type-A1 (composite order pairing with 2 prime and size of each prime is 512 bits)
- Assumption:-

I. Three authorities in case of Multi-authority TA Scheme

II. Experiment done for 8 different set of access tree. I put them here :- https://github.com/ayanDas-isi/TemporalAccess/blob/master/StructureVsTimeTaken.txt

III. as there is no non-temporal attribute in comparision based ABE so we are assuming that there is no non-temporal attribute in temporal access control ABE, online-offline ABE and multi-authority ABE as well for better understanding.

Symbols and description

Table 1: Notations

Symbol	Description
$(\mathbb{E}_T/\mathbb{E}_1)$	time taken for exponentiation in the group $\mathbb{G}_T/\mathbb{G}_1$
$(\mathbb{M}_T/\mathbb{M}_1)$	time taken for exponentiation in $\mathbb{G}_T/\mathbb{G}_1$
$\mathbb{D}_T$	time taken Division in $\mathbb{G}_\mathbb{T}$
$\mathbb{S}_{\mathbb{Z}_ı}$	time taken for sum in $\mathbb{Z}_ı$
$\mathbb{M}_{\mathbb{Z}_ı}$	time taken for multiplication in $\mathbb{Z}_ı$
S_A	number of leaf nodes in the access tree
S_{A_t}	number of temporal attributes among the leaf nodes in the access tree
S_{A_n}	number of nontemporal attributes among the leaf nodes in the access tree
S_D	set of all attributes by which decryptor is going to decrypt
S_{D_t}	set of temporal attributes by which decryptor is going to decrypt
S_{D_n}	set of non-temporal attributes by which decryptor is going to decrypt
$\mathbb{P}$	Time required for pairing operation
$\mathbb{H}$	Time required for hash using H
$\mathbb{P}_{enc}$	complexity of internal node required for encryption
$\|m\|$	size of the message
$\|\mathbb{G}_T\|/\|\mathbb{G}_1\|/\|\mathbb{Z}_p\|$	Size of the group $\mathbb{G}_T/\mathbb{G}_1/\mathbb{Z}_p$
$\|\tau\|$	size of the access structure
$\|\gamma\|$	size of the attribute set
au	Number of authorities in case of Multi-authority attribute based encryption

Schemes with whom I have compared

- CPABE : The scheme of Cipher Policy Attribute Based Encryption [1]
- CBABE : The scheme of comparision Based access control [2]
- TAABE : The scheme of Temporal Access Control [3]
- OOABE : Our scheme Scheme-4: Temporal Access Control with added two phase encryption
- MAABE : Our scheme Scheme-5: distributed Access Control Scheme (added Multi-Authority key generation)

References

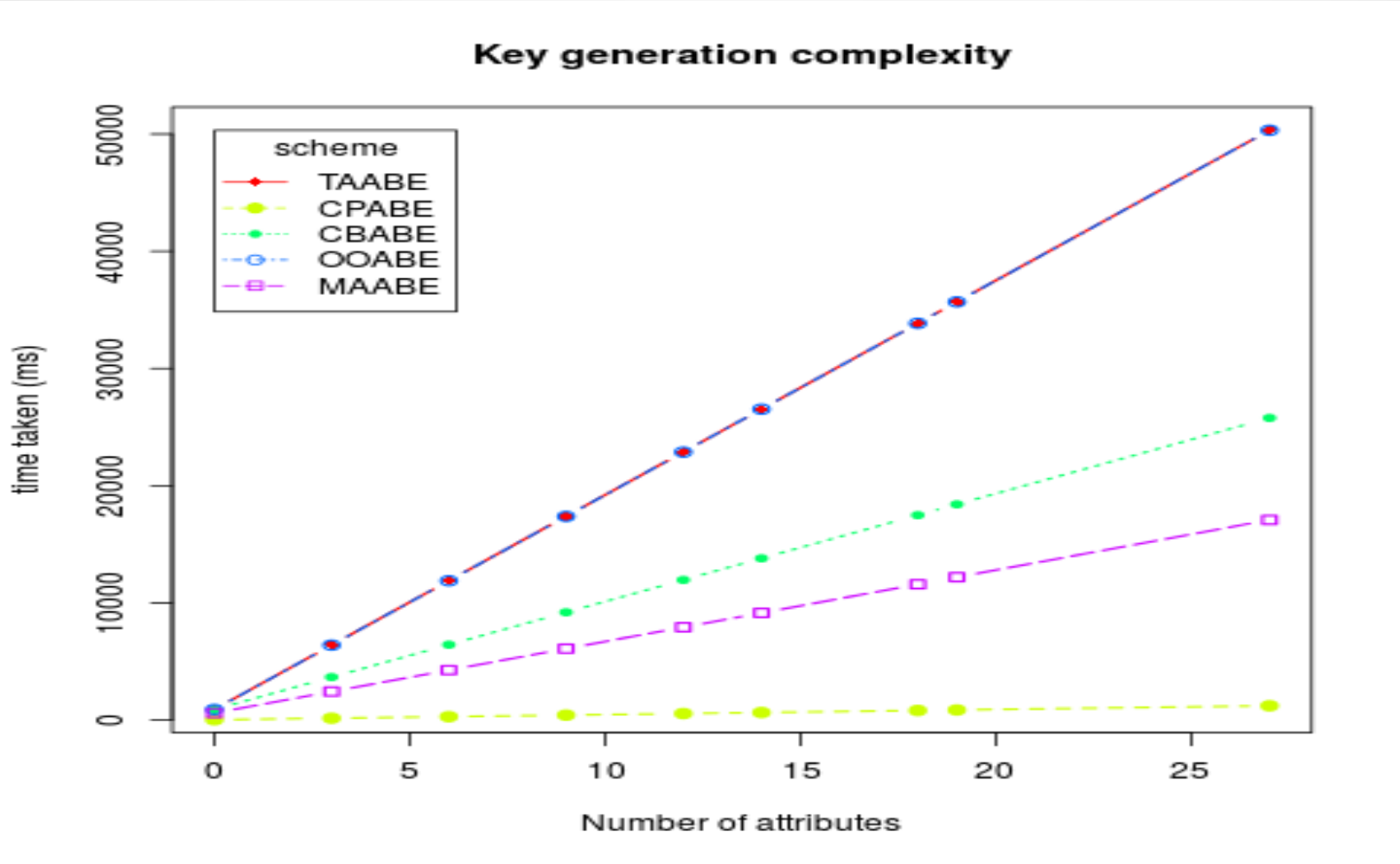
- [1] J. Bethencourt, A. Sahai, and B. Waters. Ciphertext-policy attribute-based encryption. In IEEE Symposium on Security and Privacy, pages 321-334, 2007.
- [2]Y. Zhu, H. Hu, G. Ahn, M. Yu, H. Zhao. Comparison-Based Encryption for Finegrained Access Control in Clouds. Proceedings of the second ACM conference onData and Application Security and Privacy,page 105–116, 2012.
- [3]N. Balani and S. Ruj. Temporal access control with user revocation for cloud data, IEEE 13th International Conference on Trust, Security and Privacy in Computing and Communications.pages 336–343, year 2014.

KeyGen and enc complexity comparision

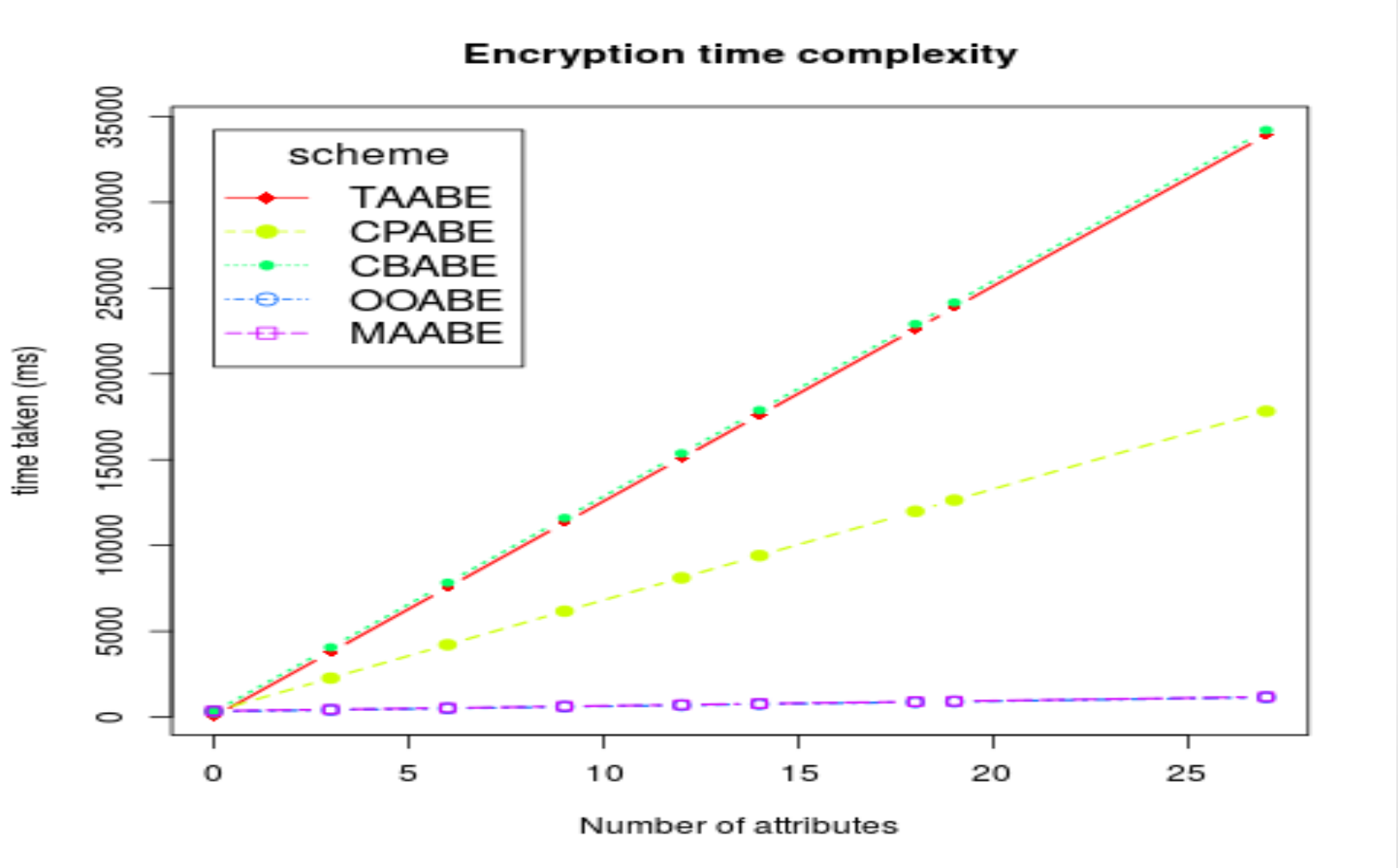
Scheme	Key generation cost
CPABE	$S_{A_t}(2\mathbb{E}_1 + \mathbb{M}_1 + H) + 2\mathbb{E}_1 + \mathbb{S}_{z_1} + \mathbb{D}_{z_1}$
CBABE	$3\mathbb{E}_1 + \mathbb{S}_{z_1} + \mathbb{D}_{z_1} + S_{A_t}(3\mathbb{E}_1 + \mathbb{M}_1 + H + 2\mathbb{M}_{z_1})$
TAABE	$3\mathbb{E}_1 + \mathbb{M}_t + S_{A_t}(6\mathbb{E}_1 + \mathbb{M}_1 + H) + S_{A_n}(2\mathbb{E}_1 + \mathbb{M}_1 + H)$
OOABE	Same as TAABE
MAABE	$((complexityofOOABE)/au) + S_{z_1}(au + 1) + \mathbb{E}_1$

Scheme	Offline Encryption Complexity of encryption	Online Encryption Complexity of encryption
CPABE		$\mathbb{E}_T + \mathbb{M}_T + \mathbb{E}_1 + S_A(2\mathbb{E}_1 + H) + \mathbb{P}_e nc + S_A$
CBABE		$\mathbb{E}_1 + S_{A_t}(4\mathbb{E}_1 + H + 2\mathbb{M}_1) + \mathbb{P}_e nc + S_A + S_{A_t}\mathbb{S}_z$
TAABE		$\mathbb{E}_T + \mathbb{M}_T + S_{A_t}(4\mathbb{E}_1 + H + 2\mathbb{M}_1 + \mathbb{S}_z) + \mathbb{P}_e nc + S_{A_n}(H + 2\mathbb{E}_1)$
OOABE	$S_{A_t}(2R + 4\mathbb{E}_1 + H + 2\mathbb{M}_1 + \mathbb{S}_z) + S_{A_n}(H + 2\mathbb{E}_1)$	$\mathbb{P}_{enc} + \mathbb{S}_z S_A + \mathbb{E}_1 + \mathbb{M}_T + \mathbb{E}_T$
MAABE	complexity of OOABE	complexity of OOABE $+\mathbb{E}_T$

Key Generation Complexity



Encryption Complexity

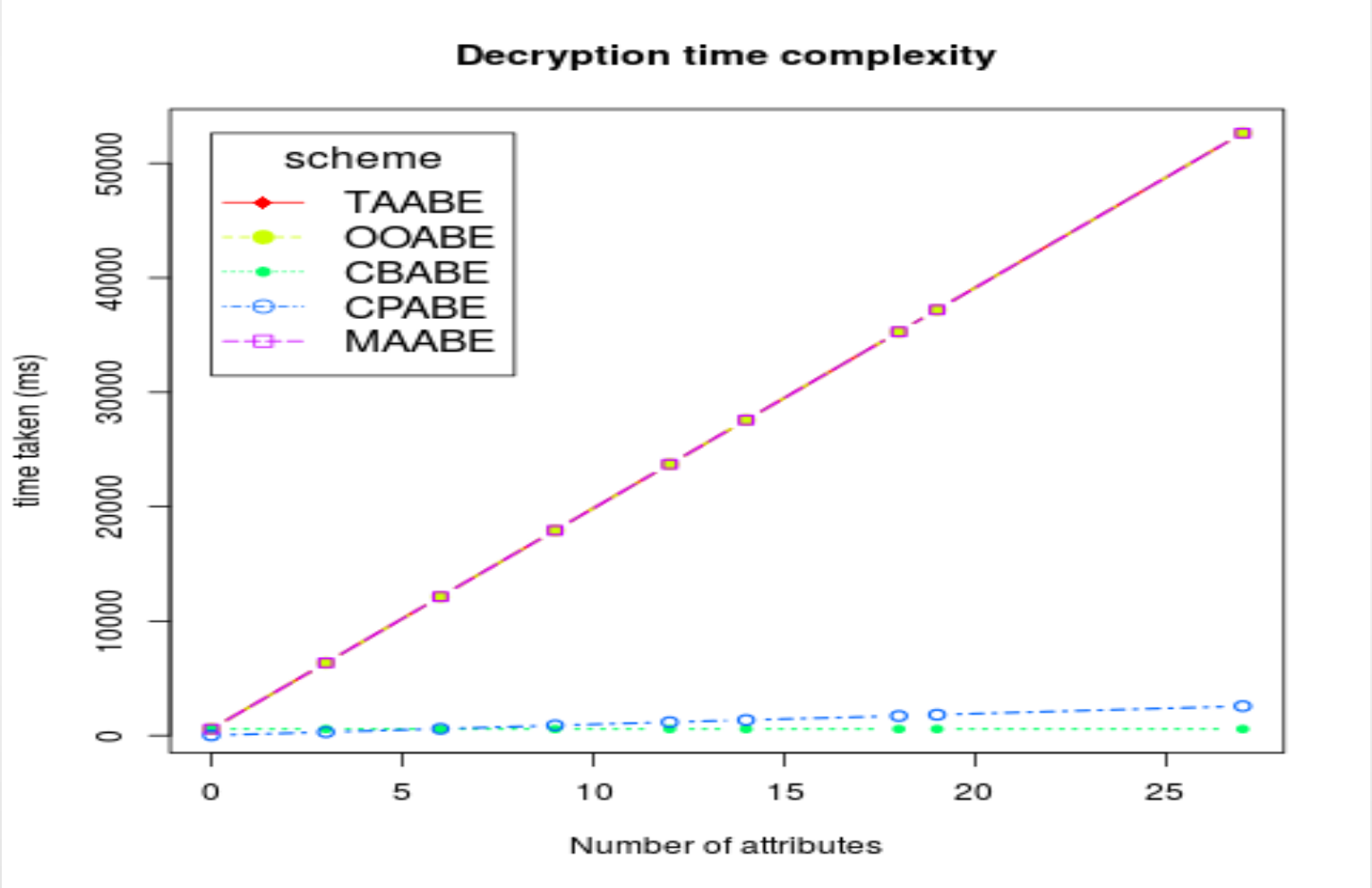


Dec complexity and ciphertext size

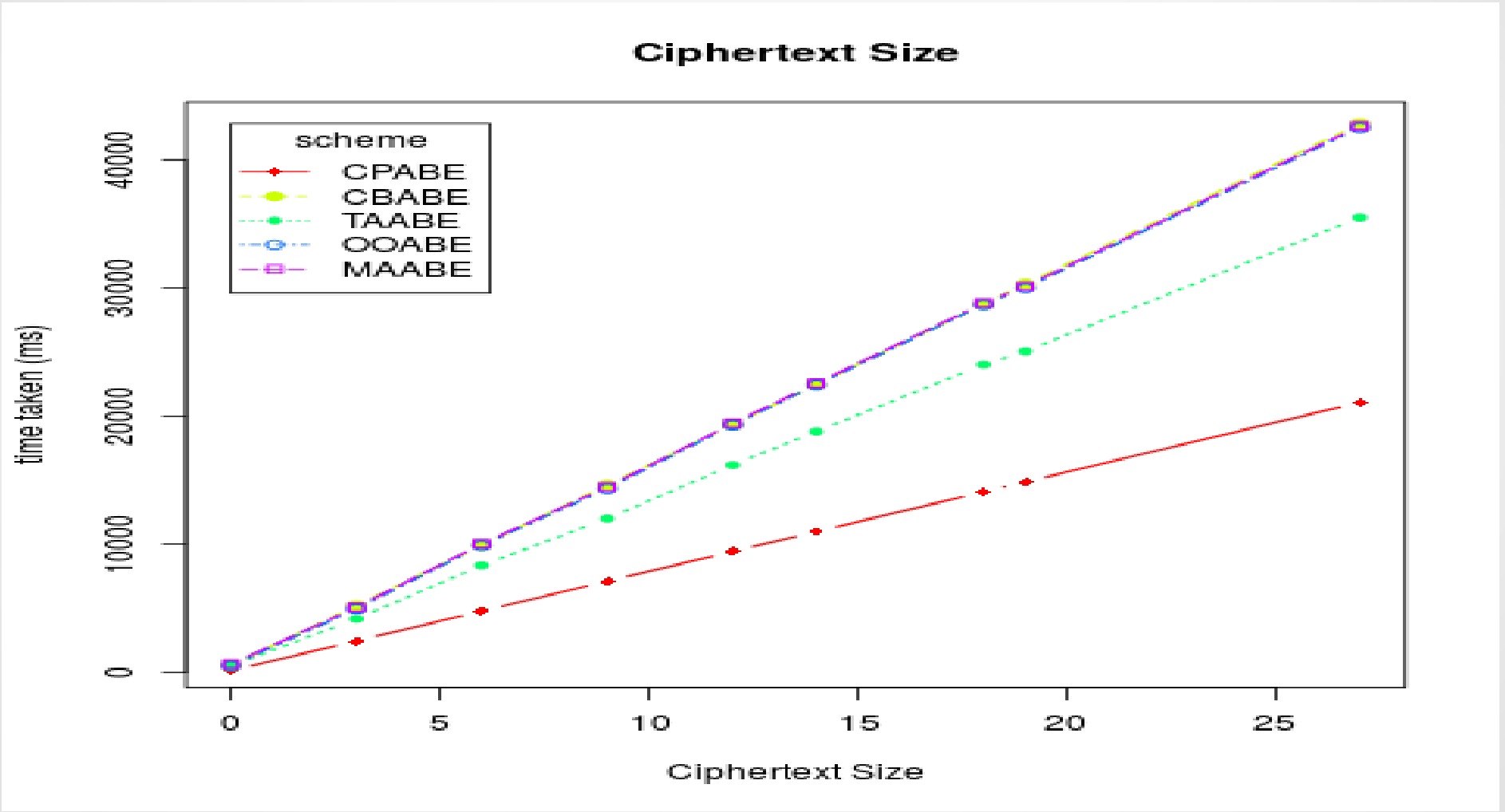
Scheme	Delegete	DecryptProxy	DecryptUser
CPABE			$\mathbb{PS}_D + \mathbb{E}_T\mathbb{P}_{enc} + 2\mathbb{D}_T + \mathbb{P}$
CBABE		$\mathbb{E}_T\mathbb{P}_{enc} + 2\mathbb{PS}_D$	$\mathbb{D}_T + \mathbb{P} + \mathbb{E}_1 + \mathbb{M}_1$
TAABE	$\mathbb{S}_{D_t}(7\mathbb{E}_1 + 10\mathbb{M}_1 + H + 4P + 2\mathbb{E}_T) +$ $\mathbb{S}_{D_n}(2\mathbb{M}_1 + \mathbb{E}_1 + H + \mathbb{E}_T + 2P) + \mathbb{E}_1 + \mathbb{M}_1$	$\mathbb{S}_{D_t}(3\mathbb{M}_T + 4P + 2\mathbb{D}_T) +$ $\mathbb{S}_{D_n}(\mathbb{M}_T + \mathbb{D}_T + 2P) + \mathbb{P}_{enc}$	$2\mathbb{D}_T + \mathbb{P} + \mathbb{E}_1 + \mathbb{M}_1$
OOABE	Time comlexity of Temporal access scheme	Time comlexity of Temporal access scheme + $2P + \mathbb{D}_T + \mathbb{M}_T + \mathbb{S}_{\mathbb{Z}}\mathbb{S}_{D_t} + O(\mathbb{S}_{D_T})\mathbb{M}_T$	Time comlexity of Temporal access scheme
MAABE	Time comlexity of Temporal access scheme	Time comlexity of OOABE + $P + \mathbb{M}_T(au + 1)$	Time comlexity of OOABE $+\mathbb{M}_{z_1}$

Scheme	Ciphertext size
CPABE	$\lvert\mathbb{G}_T\rvert + \lvert 2\mathbb{G}_1\rvert\mathbb{S}_A + \lvert\tau\rvert$
CBABE	$\lvert\mathbb{G}_T\rvert + \lvert\mathbb{G}_1\rvert + 4\lvert\mathbb{G}_1\rvert\mathbb{S}_A + \lvert\tau\rvert$
TAABE	$\lvert\mathbb{G}_T\rvert + \lvert\mathbb{G}_1\rvert + 4\lvert\mathbb{G}_1\rvert\mathbb{S}_{A_t} + 2\lvert\mathbb{G}_1\rvert\mathbb{S}_{A_n} + \lvert\tau\rvert$
OOABE	size of temporal access scheme ciphertext $+2\lvert\mathbb{Z}_p\rvert\mathbb{S}_A$
MAABE	size of OOABE ciphertext $+\lvert\mathbb{G}_1\rvert$

Decryption Complexity on user side



Ciphertext Size



Proof of Security

1) Security for collusion privilage attack.
2) Security against the online offline encryption scheme using shamir's secret sharing.
3) Security against revoked user.
4) Security against attack by the user with non overlapping time duration of attributes.
5) Security against derivation key attack by collusion.
6) Security against derivation key attack by 2 revoked user's collusion.
7) Security against derivation key attack by one revoked user and one non-revoked user collusion.
8) Security against derivation key attack by the previous derivation key.

Theorems related to proof

Theorem1 (against collusion attack): Given a TA(temporal access) cryptosystem over the RSA type elliptic curve system S_N, It is impossible to extract the values g^{τ_a} or $H(A_t)^{rP(0)}$ from the user's key SK_L if computational Co-Diffie-Hellman assumption holds.
This theorem shows that the colluders cannot forge a new key by exchanging g^{τ_a} and $H(A_t)^{rP(0)}$ from some known private keys.Hence our scheme can resist the CPA-1 type attack.

Theorem 2 (against collusion attack): Given a multi-tuple $(N, \varphi, \lambda, t_i, (\varphi^r)^{\lambda^{t_i}})$ over the RSA-type elliptic curve system S_N , where $r \in R_z$. It is intractable to compute $(t_j, (\varphi^r)^{\lambda^{t_j}})$ with $t_j < t_i$ for all PPT algorithms under the RSA assumption.

Scope of improvement

a) Implementation cannot be done due to some problem in composite order pairing

b) Is is possible to remove central authority for key generation for the scheme-5 (All key generation will be done only by distributed authorities)

Thank you