IDENTITY BASED ENCRYPTION WITH OUTSOURCED REVOCATION USING PSEUDONYM N CLOUD COMPUTING

Ankita Sahani

M.tech (Computer Science and engineering) from Buddha nstitute of Technology (2018-2020) University-Dr. A.P.J Abdul Kalam technical University.

ABSTRACT

This nvestigation to concentrate on dentity based encryption comprehend the open key and testament the executives at open key nfrastructure (PKI) s a significant at least one accessible prospects. We bring redistributing movement nto BE exhibit of audit and underwriting the ensured significance of re-appropriated revocable BE all of a sudden to the best of our nsight. We propose an arrangement to offload all the key age-related undertakings n the midst of key-giving and key-invigorate, leaving only a predictable number of essential exercises for PKG and qualified customers to perform locally. Along these lines, remembering the ultimate objective to keep up nterpret limit, unrevoked customers' needs to discontinuously request on key-revive for time part to an as of late ntroduced substance named Key Update Cloud Service Provider (KU-CSP). With the guide of KU-CSP, the customer needs not to contact with PKG n key-invigorate, toward the day's end, PKG s allowed to be detached n the wake of sending the denial once-over to KU-CSP. No sheltered channel or customer approval s required n the midst of key-invigorate among customer and KU-CSP.

Index Terms—Identity-based encryption, Revocation, Outsourcing, Cloud computing.

1. NTRODUCTION

1.1 Identity biased Cryptography

identity biased cryptography is a type of private key cryptography(PKC). Identity biased cryptography came as solution of traditional public key cryptography which is biased on concept PKI (public key infrastructure).In traditional public key cryptography .every party (entity) contains a pair of key, one is called public key and other is called private key. So when we join a network , we create our own public key, private key pair. We generate private key randomly but we have to create a public key as the inverse of a private key. This nvestigation to concentrate on dentity based encryption comprehend the open key and testament the executives at open key nfrastructure (PKI) s a significant at least one accessible prospects. We bring redistributing movement nto BE exhibit of audit and underwriting the ensured significance of re-appropriated revocable BE all of a sudden to the best of our nsight. We propose an arrangement to offload all the key age-related undertakings n the midst of key-giving and key-invigorate, leaving only a predictable number of essential exercises for PKG and qualified customers to perform locally. n our arrangement, we comprehend repudiation through reviving the private keys of the unrevoked customers. Along these lines, remembering the ultimate objective to keep up nterpret limit, unrevoked customers' needs to discontinuously request on key-revive for time part to an as of late ntroduced substance named Key Update Cloud Service Provider (KU-CSP). we don't have to re-issue the whole private keys, anyway essentially need to nvigorate a lightweight piece of t at a particular component KU-

CSP. With the guide of KU-CSP, the customer needs not to contact with PKG n key-invigorate, toward the day's end, PKG s allowed to be detached n the wake of sending the denial once-over to KU-CSP. No sheltered channel or customer approval s required n the midst of key-invigorate among customer and KU-CSP.

At the point when countless clients require their private keys, t mayover-trouble the quality pro.

Also, key administration system, key repudiation specifically, s vital n a protected and versatile

ABE framework

In most of existing ABE conspire, the revocation of any single private key requires key-revive at a quality expert for the remainder of the unrevoked keys which share typical ascribes with the one to be denied. trademark master.

In addition,all of these overwhelming assignments concentrated at power side would make t an effectiveness bottleneck n the entrance control framework. going at killing the most overhead estimation at both the trademark pro and the customer sides, a re-appropriated ABE plot s

endorsed that sponsorships redistributed unscrambling and furthermore empowers naming key generation.In expansion, t s seen that while encountering business distributed computing administrations, the CSPs might be childish so as to spare ts calculation or transmission capacity, which may cause results returned erroneously Keeping at the top of the priority list the ultimate objective to deal with this ssue, checkability s done on returns about originated from both KGSP and DSP.

When utilizing open key cryptography over the nternet, the primary ssue s the capacity to relate the correct open keys to the perfect people/associations. The general procedure for doing so s as per the following. n ts most straightforward structure, we accept at least one confided n Certificate-Authority (CA) focuses which at first run the mark key age calculation to process ts own open and mystery keys. Every CA holds ts mystery key under extraordinary security however generally disseminates.

Besides, we consider to acknowledging revocable BE with a semi-genuine KU-CSP. To accomplish this objective, we present a security mproved development under the as of late formalized Refereed Delegation of Computation (RDoC) model. n this way, key-update capability at PKG can be on a very basic level diminished from directly to the height of such combined tree (for example logarithmic n the amount of customers). Coincidentally, we raise that anyway the equal tree associate s competent with achieve a relative predominant, t will realize distinctive ssues Nevertheless, we call attention to that however the twofold tree acquaintance s capable with accomplish a relative elite, t will bring about other problems:1) PKG needs to create a key pair for all the hubs on the way from the character leaf hub to the root hub, which brings about multifaceted nature logarithmic n the quantity of clients n framework for giving a solitary private key. 2) The size of private key develops n logarithmic n the quantity of clients n framework, which makes t troublesome n private key stockpiling for clients. 3) As the amount of customers n structure creates, PKG needs to keep up a twofold tree with a ton of center points, which presents another bottleneck for the overall system. Pair with the mprovement of appropriated processing.

2. LITERATURE REVIEW

Identity-Based Encryption (IBE) which simplifies the public key and certificate management at Public Key nfrastructure (PKI) s an mportant alternative to public key encryption. However, one of the main efficiency drawbacks of BE s the overhead computation at Private Key Generator (PKG) during user revocation. Efficient revocation has been well studied n traditional PKI setting, but the cumbersome management of certificates s precisely the burden that BE strives to alleviate, DISADVANTAGS are: However, one of the main efficiency drawbacks of BE s the overhead computation at Private Key Generator (PKG) during user revocation.

Revocable BE: ntroduced by and firstly mplemented by Boneh and Franklin as well as BE has been researched ntensively n cryptographic community On the aspect of construction, these first schemes were proven secure n random oracle. Some subsequent systems achieved provable secure n standard model under selective-ID Security or adaptive-ID security. Recently, there have been multiple lattice-based constructions for BE Systems

.Nevertheless, concerning on revocable BE, there s little work Presented. As mentioned before, Boneh and Franklin's suggestion s more a viable solution but mpractical. Hanaoka et al. proposed a way for users to periodically renew their private keys without nteracting with PKG. However, the assumption required n their work s that each user needs to possess a tamper-resistant hardware device. Another solution s mediator-aided revocation

In this setting there s a special semi-trusted third party called a mediator who helps users to decrypt each cipher text. f an dentity s revoked then the mediator s nstructed to stop helping the user. Obviously, t s mpractical since all users are unable to decrypt on their own and they need to communicate with mediator for each decryption. Recently, Lin et al.proposed a space efficient revocable BE mechanism from non-monotonic Attribute- Based Encryption (ABE), but their construction requires $O(r)$ times bilinear pairing operations for a single decryption where s the number of revoked users.

Other Revocation Technique: The authors utilized proxy re-encryption to propose a revocable ABE scheme. The trusted authority only needs to update master key according to attribute revocation status n each time period and ssue proxy re-encryption key to proxy servers. The proxy servers will then re-encrypt cipher text using the re-encryption key to make sure all the unrevoked users can perform successful decryption. We specify that a third party service provider s ntroduced n both Yu et al. and this work. Differently, Yu et al. utilized the third party (work as a proxy) to realize revocation through encrypting cipher text which s only adapt to the special application that the cipher text s stored at the third party. However, n our construction the revocation s realized through updating private keys for unrevoked users at cloud service provider which has no limits on the location of cipher text.

Outsourcing Computation: The problem that how to securely outsource different kinds of expensive computations has drawn considerable attention from theoretical computer science community for a long time. Chaum and Pedersen firstly ntroduced the notion of wallets with observers, a piece of secure hardware nstalled on the client's computer to perform some expensive computations. Attalla et al. Presented a framework for secure outsourcing of scientific computations such as matrix multiplication and quadrature. Nevertheless, the solution used the disguise technique and thus leaded to leakage of private nformation. Rosenberger and Lysyanskaya proposed the first outsource-secure algorithm for modular exponentiations based on pre-computation and serveraided computation. Atallah and Li nvestigated the problem of computing the edit distance between two sequences and presented an efficient protocol to securely outsource sequence comparison with two servers. Furthermore, Benjamin and Atallah addressed the problem of secure outsourcing for widely applicable linear algebraic computations. Nevertheless, the proposed protocol required the expensive operations of homomorphism encryption. Attalla and Frikken further studied this problem and gave mproved protocols based on the so-called weak secret hiding assumption. Chen et al. made an efficiency mprovement on the work and proposed a new scheme for outsourcing single/simultaneous modular exponentiations.

3. PRELIMINARY

3.1 Cryptographic Background

Definition 1:

(i) Bilinear maps

Let G and G_T be cyclic groups of prime order q. G is an additive group and G_T multiplicative group. g is a generator of G. A bilinear pairing map $e : G \times G \to G_T$ satisfies:

- **Bilinearity:** For all $g_1,g_2 \in G$ and $a,b \in Z$, we have $e(g_1^a,g_2^b) = e(g_1,g_2)^{ab}$.
- **Non-degeneracy:** e is non-degenerate,that∈ is, $e(g_1,g_2)$ is not the identity of G_T for some g_1,g_2 G_T
- e is efficiently computable.

Definition 2:

(ii) Bilinear Diffie-Hellman(BDH) problem

Given(aP,bP,cP ∈ G) with a,b,c ∈R Z_q^*, to compute $e(P,P)^{abc}$.

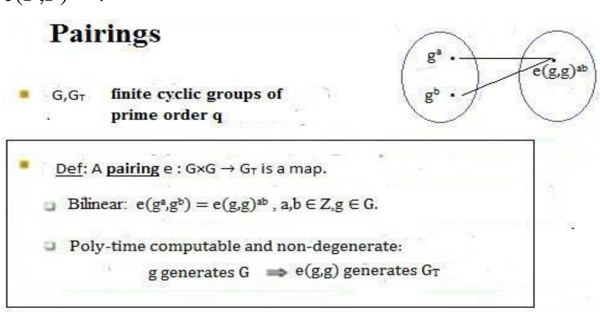


Fig.3.1

3.2 Identity Based Encryption

> Three types of Roles

1. A private key generator (PKG)
2. Sender(User)
3. Receiver(User)

Four Algorithms

1.Setup- Executed by the PKG. Setup is executed only once during the initialization phase only of the network. PKG runs setup algorithms only one time. PKG runs a setup algorithm to generate two things. One is a public parameter and the other is a master secret which we can say is the master secret of PKG.

2.Extract- Executed by the PKG in response to request by an user.The extract algorithm∈ requires master secret of PKG and user's identity {0,1}* to generate the private key corresponding to the user's identity. Any one can not generate a private key corresponding to this user's identity because a master key is also required.

3.Encrypt- Executed by sender.Encryption algorithm takes identity of receiver and message to encrypt message. This algorithm takes the identity of the receiver not sender because we are encrypting messages in his name when cipher text is generated.

4.Decrypt- Executed by receiver.Decryption algorithm takes cipher text as input parameter and private key of receiver.

4. PROBLEM STATEMENT

We present a system model for outsourced revocable IBE is shown in Fig. 1. In this model revocation for compromised users is done with the help of key update cloud service provider(KU-CSP). KU-CSP is run as a public cloud by a third party. KU-CSP provides basic computing capabilities as standardized services to PKG. KU-CSP may be hosted away for either user or PKG. KU-CSP reduces the computation and storage cost of PKG by providing an extension of infrastructure. When revocation is triggered for a compromised user,unrevoked user KU-CSP is not honest, we have to design a secure scheme. Based on the system model proposed, we are able to define the outsourced revocable IBE scheme.

International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 04 Issue: 06 | June -2020 ISSN: 2582-3930

Traditional IBE definition, The KeyGen, Encrypt and Decrypt algorithms are redefined as follows to integrate time components. Two list RL and TL are used in our definition. RL is used for storing revoked users and TL is used for storing past and current time periods.

Users Request from KU-CSP for update of lightweight component of their private keys from KU-CSP instead of re-requesting private keys from PKG.Though many details are involved in KU-CSP's deployment, In this paper KU-CSP is considered as computing service provider and considering KU-CSP is not honest we have to design secure scheme. Based on the system model proposed, we are able to define the outsourced revocable IBE scheme. Traditional IBE definition, The KeyGen, Encrypt and Decrypt algorithms are redefined as follows to integrate time components. Two list RL and TL are used in our definition. RL is used for storing revoked users and TL is used for storing past and current time periods.

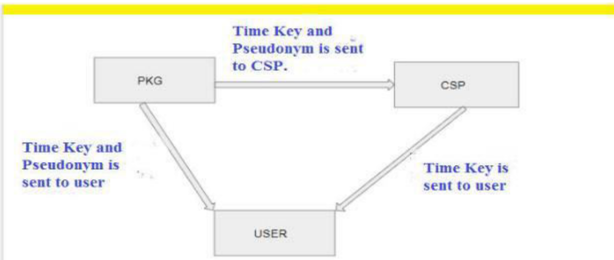


Fig.1 System Architecture

5. EFFICIENT IBE WITH OUTSOURCED REVOCATION

5.1 Intuition For efficient revocation concept of partial private key update is introduced in this paper. For this hybrid private key is used which contains two subcomponents namely the identity component and time component by using AND gate. Identity component is generated by PKG while time component is updated by KU-CSP(Key update cloud service provider).

In encryption both identity and time period is used. A user can decrypt ciphertext only if the identity and time period used in his/her private key is identical to the identity and time period used in ciphertext during encryption. Using this concept we can revoke the user's decrypt ability by updating the time component for the private key by KU-CSP. We used the idea of "partial private key update" into the proposed construction, in which identity component and time component is used. Identity component is generated by PKG while time component is generated by KU-CSP.In encryption identity component and time component is used.Using such skill, we are able to revoke the user's decryption ability through updating the time component for the private key by KU-CSP.

5.2. Proposed Construction

We present our construction as follows

Setup(k): Select two cyclic groups $(G_1,+)$ and $(G_2,.)$ of the same order q. P is the generator of G_1. $e:G_1*G_1\rightarrow \mathbf{G_2}$ is a bilinear pairing. Choose s,s_1 Z_q^* at random and compute $P_0=sP$. Select seven∈ hash functions: $H_1:\{0,1\}^*\rightarrow \mathbf{G_1}$, $H_2:\{0,1\}^*\rightarrow \mathbf{G_1}$, $H_3:\{0,1\}^*\rightarrow \mathbf{G_1}$, $H_4:\{0,1\}^l\times\{0,1\}^l\rightarrow \mathbf{Z_q^*}$, $H_5:G_2\rightarrow \mathbf{\{0,1\}^l}$, $H_6:\{0,1\}^l\rightarrow \mathbf{\{0,1\}^l}$, H_7:**{Time Periods}**$\rightarrow \mathbf{Z_q^*}$,$H_8$:**{Pseudonyms}**$\rightarrow \mathbf{Z_q^*}$. l is the message length. Time Periods(T)=$\{t ,t_2,........t_i\}$ Z_q^*

The system parameters ^{1} params ∈ are $<G_1,G_2,q,P,P_0,e,H_1,H_2,....,H_5,H_6,H_7,H_8>$. This algorithm outputs revocation list RL (initially empty) and time list TL also.The master secret key (mk) is s. Public key of PKG is P_0= sP. Master time key s_1 is sent to the cloud service provider (CSP).

Private-Key-Extract(params,mk,ID): The PKG computes $Q_{ID}=H_1(ID)$ and then calculates $SK_{ID}=sQ_{ID}$

as the private key of user ID.PKG also computes pseudonym (psd) $=H_3(ID)$. Let $H_2(ID,t)=H_8(psd) + P^{ti}$. Pseudonym is sent to CSP and users. Private key of the user is sent to the user.

Time-Key-Update(params,ID,t): The CSP computes $Q_{PSD,t} = H_8(psd) + P^{ti}$ and then calculates $TK_{ID,t}=s_1Q_{PSD,t}$ as the time key of the user ID at time t. Public key of CSP $P_c=s_1P$.

Encrypt(params,M,ID,t): The data owner does the following to∈encrypt a message M.

–Choose $\boldsymbol{\sigma}$ $\{0,1\}^l$,

–compute $r=H_4(\boldsymbol{\sigma},M)$;

–compute U=rP;

–compute V= $\boldsymbol{\sigma}$ $H_5(e(Q_{ID},P_0)^r)$ $H_5(Q_{ID,t},P_c)^r)$;

– Compute W=M⊕ $H_5(\boldsymbol{\sigma})$ ⊕

-Output the ciphertext C=(U,V,W)

Decrypt(params,C=(U,V,W),SK_{ID},$TK_{ID,t}$): The data user computes

Then

$\boldsymbol{\sigma}=V$ $H_5(e(SK_{ID},U))$ $H_5(TK_{ID,t},U))$

it can recover the message by calculating $M=W + H_5(\boldsymbol{\sigma})$

If the equation $U = H_3(\boldsymbol{\sigma},M)P$ holds, the message M is correct

Revoke(psd,t) If the user id with identity needs to be revoked at the time t , the CSP stops generating the time key $TK_{ID,t}$ for the users.

Correctness. To recover the plaintext from ciphertext C=(U,V,W),the key point is to computer.So, we first verify the correctness of $\boldsymbol{\sigma}$

$\boldsymbol{\sigma}=V$ $H_4(e(SK_{ID},U))$ $H_4(e(TK_{ID},U))$

$=\boldsymbol{\sigma}$ $H_5(e(Q_{ID},P_0)^r)$ $H_5(e(Q_{ID,t},P_c)^r)$ $H_5(e(sQ_{ID},rP))$ ⊕ $H(e(sQ_{PSD,t},rP))$

⊕) $H(e(sQ_{PSD,t},rP))$ ⊕

⊕ $H(e(sQ_{ID},rP))$ $H(e(sQ_{PSD,t},rP))$

⊕ ⊕

Then ⊕ ⊕ ⊕

$M=W$ $H_6(\boldsymbol{\sigma})=M$ $H_6(\boldsymbol{\sigma})$ $H_6(\boldsymbol{\sigma}) = M$.

So, if the equation $U = H_4(\boldsymbol{\sigma},M)P$ holds, the message M is correct.

- **Revoke(RL,TL,{$ID_{i1},ID_{i2},...,ID_{ik}$}):** If users with identities in the set$\{ID_{i1},ID_{i2},...,ID_{ik}\}$are to be revoked at time period T_i, PKG updates the revocation list of pseudonyms∪ corresponding to these identities as RL = RL $\{psd_{i1},psd_{i2},...,psd_{ik}\}$as well as the time list through linking the newly created time period T_{i+1} onto original list TL Revocation list and new time period T_{i+1} are sent to KU-CSP.
- **KeyUpdate(RL,ID,T_{i+1},OK_{ID}):** Upon receiving a key update request on PSD, KU-CSP firstly checks whether psd exists in the revocation list RL, if so ⊥ KU-CSP returnsand key-update is aborted.

Otherwise, KU-CSP fetches the corresponding entry (psd) in the user list UL. Finally, give the output time updated key and send it to the user.

6. EXPERIMENTAL RESULT 6.1 THEOREM

Theorem 2. If an outside adversary A_o has advantage ϵ against the IND-CCA security of our scheme when he makes q_1 times H_1 hash queries and q_4 times H_4 hash queries, then an algorithm B exits that can solve the BDH problem with probability $\boldsymbol{\epsilon' \geq \epsilon}/(q_1 \cdot q_4)$.

Proof. Suppose B wants to solve the BDH problem with random instances < aP,bp,cP >, so its ultimate goal is to compute $e(P,P)^{abc}$. So B will act as a challenger that will interact with adversary A_o. Initially B setups public parameters as < $G_1,G_2,q,P,P_0 = aP,H_i(1 \leq i \leq 8)$ ∈>. Before making any hash query adversary selects I [1,q_1].

Hash queries: All hash queries are answered by choosing the proper element randomly. The detailed query-answers are < $(ID_i,x_i$ R $Z_{*q},x_iP)$ > for H_1, <

$(ID_i,,t_i,y_i$ (E,h) > for H^5, < (σ, **(σ,M,r)** > for H_4, < h) > for H^6. Especially, when i = I,B responds with $H_1(ID_i) = bP$.

Private key queries: When B receives private key query from adversary on (ID_i), it will search H_1 list for < (ID_i,x_i,x_iP) > and computes $SK_{IDi} = x_iaP$ as the answer. Note that if i = I, B aborts the game.

Time key queries: When B receives decryption key query from adversary on (ID_i,t_i), it will search H_2 list for < (ID_i,t_i,y_i,y_iP) > and computes $TK_{IDi},t_i = y_iaP$ as the answer.

Decryption queries When adversary requests a decryption query from B on (C=(U,V,W),ID,t), B executes Decrypt(params,C,SK_{ID},$TK_{ID,t}$) and output the resulting plaintext M. After that,Adversary outputs two equal-length plaintexts M_0,M_1, T_* and

ID_* that it wants to challenge. If $ID_* \neq ID_I$, B aborts the game; Challenger picks a random bit b_I {0,1}

Adversary

and sets CT = Encrypt(M_{bI},ID ,T ,PK). adaptively issues more queries as before with the restriction that (ID_*,T $_*$) cannot be queried in the time key query on (ID_*,t_*) At the ∈end of the game, the adversary outputs a guess b_I' { 0,1} and wins the game if $b_I' = b_I$.

Analysis. If B does not abort the game and A_o can break the IND-CCA security of the scheme with advantage ϵ, B can solve the BDH problem with probability ϵ' ≥ ϵ/q_4. So, ϵ' ≥ ϵ/($q_1 \cdot q_4$).

Theorem 3. If an inside adversary A_i who makes q_2 times H_2 hash queries and q_4 times H_5 hash queries, then an algorithm B exits that can solve the BDH problem with probability ϵ' ≥ ϵ/($q_2 \cdot q_4$).

Proof. Suppose B wants to solve the BDH problem with random instances < aP,bP,cP >, so its ultimate goal is to compute $e(P,P)^{abc}$. So B will act as a challenger that will interact with adversary A_i.

Initially B setups public parameters as < $G_1,G_2,q,P,P_0 = aP,H_i(1 \leq i \leq 8)$ >. Adversary selects I [1,q_2] before making any hash query and the I_{th} query to the H_2 oracle is on (ID_*,t_*).

Hash queries: All hash queries are answered by choosing the proper element randomly. The detailed query-answers are < $(ID_i,x_i$ R $Z_{*q},x_iP)$ > for H_1, <

$(ID_i,,t_i,y_i$ (E,h) > for H^5, < (σ, **(σ,M,r)** > for H_4, < h) > for H^6. Especially, when i = I,B responds with $H_1(ID_i) = bP$.

Private key queries: When B receives private key query from adversary on (ID_i), it will search H_1 list for < (ID_i,x_i,x_iP) > and computes $SK_{IDi} = x_iaP$ as the answer. Note that if i = I, B aborts the game.

Time key queries: When B receives decryption key query from adversary on (ID_i,t_i), it will search H_2 list for < (ID_i,t_i,y_i,y_iP) > and computes $TK_{IDi},t_i = y_iaP$ as the answer.

Decryption queries When adversary requests a decryption query from B on (C=(U,V,W),ID,t), B executes Decrypt(params,C,SK_{ID},$TK_{ID,t}$) and outputs the resulting plaintext M. After that, the adversary outputs two equal-length plaintexts M ,M , T_* and

ID that it wants to challenge. If ID ID_I, B aborts the game; Challenger picks a random bit b_I {0,1}

Adversary

and sets CT = Encrypt(M_{bI},ID ,T ,PK). adaptively issues more queries as before with the restriction that (ID_*,T $_*$) cannot be queried in the time key query on (ID_*,t_*) At the ∈end of the game, the adversary outputs a guess b_I' { 0,1} and wins the game if $b_I' = b_I$.

Analysis. If B does not abort the game and A_i can break the IND-CCA security of the scheme with advantage ϵ, B can solve the BDH problem with probability ϵ' ≥ ϵ/q_4. Since the probability that the game does not abort is 1/q_2,so, ϵ' ≥ ϵ/($q_1 \cdot q_4$).

International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 04 Issue: 06 | June -2020 ISSN: 2582-3930

6.2 REFEREED DELEGATION OF COMPUTATION MODEL

In this chapter, we produce a construction under the under the recently formalized RDoC model.

In the RDoC model, the client interacts with multiple servers and it has a right output as long as any server having the proposed protocol exists. In order to use RDoC in our setting, we use another **k−1** independent KU-CSPs. For simplicity, we use only 2 KU-CSP as shown in figure 7.1.

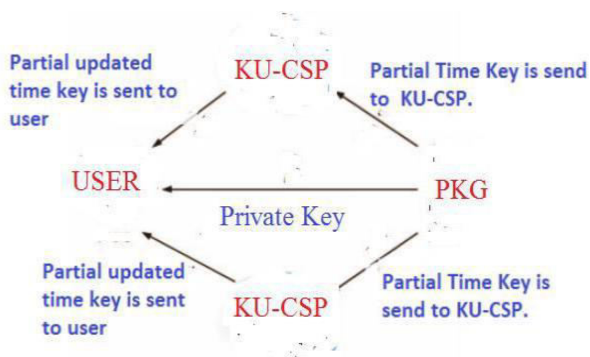


Fig.6.1 System model with two KU-CSPs

In this model we have the following three requirements: **1)** One of KU-CSP among multiple KU-CSP is honest. **2)** Computational complexity of the honest KU-CSP to perform revocation is not much more than the other KU-CSP. **3)** PKG's running time will be less in comparison to running time required to directly perform revocation. To avoid that time key should not leak with private key at the same time such type of advanced construction is needed.To get this , we break the time key (timekey = s1) into timekey(1) = s21 and timekey(2) = s22 and send it to the two KU-CSPs to produce partial time component timekey(1) and timekey(2) .

After receiving the two partial time components, user perform a computation to obtain the **final** updated key. Since the setup, encryption and decryption phases operate exactly as before, we will introduce the KeyCombine algorithm and only provide the key generation and revocation for the advanced construction as follows.

- **KeyGen(MK,ID,RL,TL,PK):** The KeyGen algorithm used in this model is similar to our proposed construction as in chapter 5. The difference is that PKG sends time keys to two KU-CSP instead of one KU-CSP as in our proposed construction in chapter 5. PKG breaks randomly time key s2 in s21 and s22 with s2 = s21 + s22 Finally, PKG sends timekey(1) = s2l to l-th KU-CSP for l =1 ,2.
- **KeyUpdate(RL,psd,T_{i+1},timekey):** When KU-CSP get the key-update request on psd corresponding to an ID, the l-th KU-CSP checks whether psd exists in the revocation list RL, if psd exists in RL then the key update is aborted. If psd does not exist in RL, the KeyUpdate algorithm fetches the corresponding entry timekey(1) = s2l in the user list UL and computes the partial time component as shown in Fig. 7.2.

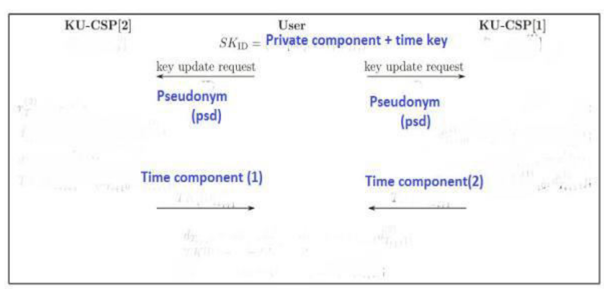


Fig.6.2 KeyUpdate and KeyCombine in Advanced Construction

Finally send the updated partial time component back to the user.

- **KeyCombine(timekey(1) + timekey(2)):** After getting timekey(1) and timekey(2), the user performs a key combination by computing timekey(1) and timekey(2) as shown in figure to obtain a full time component. Finally the private key is updated. Since the setup, encryption and decryption phases operate exactly as in chapter 5, we will give the KeyCombine algorithm and only show the key generation and revocation for the advanced construction as given

6.3 PERFORMANCE EVALUATION

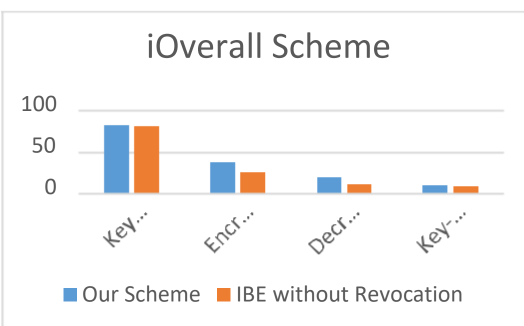
Here **experimental evaluation** of proposed construction as shown chapter 6 is shown.

A. Performance Evaluation for Overall Scheme Here we are presenting time taken by each stage in our outsourced revocable scheme and original IBE where revocation is not considered in table I.

	Our Scheme	BEiwithout Revocation
Setup	81.421 ms	80.233 ms
Key-Issuing.	39.243 ms	20.121 ms
Encryption.	37.612 ms	24.595 ms
Decryption.	19.143 ms	10.285 ms
Key-Update.	9. 792 msi	—

This time cost is evaluated at KU-CSP.

TABLE 6.1



EFFICIENCY COMPARISON FOR STAGES IN REVOCABLE IBE

64-bit M2 high-memory quadruple extra large Linux servers in Amazon EC2 platform as KU-CSP, and a Linux machine with Intel(R) Core(TM)2 Duo CPU clocked at 2.40 GHz and 2 GB of system memory as the user and PKG are used respectively.The groups G and GT are selected in 160-bit and 512-bit length.

EFFICIENCY COMPARISON FOR STAGES IN REVOCABLE IBE

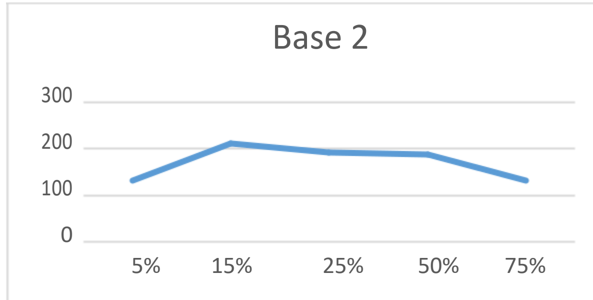
Our scheme takes more time because our scheme handles revocation issues.Our key issuing stage takes more time because a time component is taken in our scheme which is added to the private key.

Due to time component encryption and decryption algorithms also take more time.

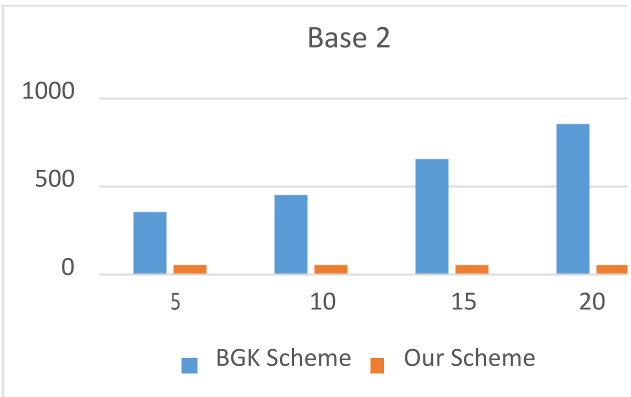
Our scheme acts as revocable identity based encryption without adding more computing overhead in original IBE.

B. Performance Evaluation for Revocation Secondly, In this we are showing comparison between our outsourced revocable IBE and and other outsourced revocable schemes in the scenario of multi-user revocation– BGKscheme. In this experiment we are using 32 bit integers to identify each node in a binary tree. In BGK system 32 bit integer is used to manage user.We are comparing Key Issuing stage and key updation stage.

1) Key-Issuing Stage: In BGK scheme a binary tree is used to manage all users.Users are assigned to leaf nodes of binary trees In key issuing stage PKG has to perform computation on each nodes in the parh from the corresponding leaf node to root node.For a single key generation request BGK responding time is in proportion to $O(\log_2(N))$ where N is the maximum number of users. But our scheme achieves constant efficiency in comparison to the BGK scheme. Since PKG has to perform computation on each node in the parh from the corresponding leaf node to root node the BGK scheme has an increasing private key size whereas in our schemes constant key size is achieved. Our scheme supports a dynamic number of users whereas in BGK scheme users are fixed initially to build binary trees.



Private Key Size



Comparisons n Key Update (Case: 215 System Users)

Revocation Ratio	2^5	2^{10}	2^{15}	2^{20}
5%	131.321 ms	3.56 s	1.721 min	0.970 h
15%	211.291 ms	6.323 s	3.123 min	1.728 h
25%	192.683 ms	7.012 s	3.651 min	2.10 h
50%	187.552 ms	8.890 s	3.512 min	1.80 h
75%	131.851 ms	3.876 s	2.299 min	1.199 h

7. CONCLUSION

Outsourcing computation has been introduced in revocable identity based encryption. Revocation operation is done by CSP. During key-update PKG is not required. Key-updition is handled by KU-CSP. No secure channel is required between KU-CSP and users in updated key transmission. PKG is allowed to be offline after transmitting revocation list and time list to KU-CSP. Since KU-CSP is untrusted pseudonyms for each user for each user so that adversary is not able to get the real identity of the user.

REFERENCES

[1] W. Aiello, S. Lodha, and R. Ostrovsky, "Fast digital identity revocation," in Advances in Cryptology – CRYPTO'98. Springer, 1998.
*[2] V. Goyal, "**Certificate** revocation using **fine** grained **certificate** space partitioning," in Financial Cryptography and Data Security, ser. Lecture Notes in Computer Science, S. Dietrich and R. Dhamija, Eds. Springer Berlin / Heidelberg, 2007, vol. 4886, pp. 247–259.*

*[3] F. Elwailly, C. Gentry, and Z. Ramzan, "Quasimodo: **Efficient certificate** validation and revocation," in Public Key Cryptography PKC 2004, ser. Lecture Notes in Computer Science, F. Bao, R. Deng, and J. Zhou, Eds. Springer Berlin / Heidelberg, 2004, vol. 2947, pp. 375–388.*
[4] D. Boneh and M. Franklin, "Identity-based encryption from the weil pairing," in Advances in Cryptology – CRYPTO 2001, ser. Lecture Notes in Computer Science, J. Kilian, Ed. .Springer Berlin / Heidelberg, 2001, vol. 2139, pp. 213–229.
*[5] A. Boldyreva, V. Goyal, and V. Kumar, "Identity-based encryption with **efficient** revocation," in Proceedings of the 15th ACM conference on Computer and communications security, ser. CCS '08. New York, NY, USA: ACM, 2008, pp. 417–426.*
[6] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in Advances in Cryptology EUROCRYPT 2005, ser. Lecture Notes in Computer Science, R. Cramer, Ed. Springer Berlin / Heidelberg, 2005, vol. 3494, pp. 557–557. [7] R. Canetti, B. Riva, and G. N. Rothblum, "Two 1-round protocols for delegation of

computation," Cryptology ePrint Archive, Report 2011/518, 2011.
[8] U. Feige and J. Kilian, "Making games short (extended abstract)," in Proceedings of the twenty-ninth annual ACM symposium on Theory of computing, ser. STOC '97. New York, NY, USA: ACM, 1997, pp. 506–516.
[7] R. Canetti, B. Riva, and G. N. Rothblum, "Two 1-round protocols for delegation of computation," Cryptology ePrint Archive, Report 2011/518, 2011.
[8] U. Feige and J. Kilian, "Making games short (extended abstract)," in Proceedings of the twenty-ninth annual ACM symposium on Theory of computing, ser. STOC '97. New York, NY, USA: ACM, 1997, pp. 506–516
[9] S. Hohenberger and A. Lysyanskaya, "How to securely outsource cryptographic computations," in Proceedings of the Second international conference on Theory of Cryptography, ser. TCC'05. Berlin, Heidelberg: Springer-Verlag, 2005, pp. 264–282.
[10] R. Canetti, B. Riva, and G. Rothblum, "Two protocols for delegation of computation," in Information Theoretic Security, ser. Lecture Notes in Computer Science, A. Smith, Ed. Springer Berlin / Heidelberg, 2012, vol. 7412, pp. 37–61.
[11] X. Chen, J. Li, J. Ma, Q. Tang, and W. Lou, "New and secure outsourcing algorithms of modular exponentiations," in 17th European Symposium on Research in Computer Security (ESORICS), 2012. [12] M. J. Atallah and K. B. Frikken, "Securely outsourcing linear algebra computations,"in Proceedings of the 5th ACM Symposium on Information,ComputerandCommunicationsSecurity,ser.ASIACCS '10. New York, NY, USA: ACM, 2010, pp. 48–59.
[13] A. Shamir, "Identity-based cryptosystems and signature schemes," in Advances in Cryptology – CRYPTO, ser. Lecture Notes in Computer Science, G. Blakley and D. Chaum, Eds. Springer Berlin / Heidelberg, 1985, vol. 196, pp. 47–53.
[14] C. Cocks, "An identity based encryption scheme based on quadratic residues," in Cryptography and Coding, ser. Lecture Notes in Computer Science, B. Honary, Ed. Springer Berlin / Heidelberg, 2001, vol. 2260, pp. 360–363.
[15] R. Canetti, S. Halevi, and J. Katz, "A forward-secure public-key encryption scheme," in Advances in Cryptology EUROCRYPT 2003, ser. Lecture Notes in Computer Science, E. Biham, Ed. Springer Berlin / Heidelberg, 2003, vol. 2656, pp. 646–646.
*[16] D. Boneh and X. Boyen, "**Efficient** selective-id secure identity-based encryption without random oracles," in Advances in Cryptology - EUROCRYPT 2004, ser. Lecture Notes in Computer Science, C. Cachin and J. Camenisch, Eds. Springer Berlin / Heidelberg, 2004, vol. 3027, pp. 223–238.*
[17] ——, "Secure identity based encryption without random oracles," in Advances in Cryptology – CRYPTO 2004, ser. Lecture Notes in Computer Science, M. Franklin, Ed. Springer Berlin / Heidelberg, 2004, vol. 3152, pp. 197–206.
*[18] B. Waters, "**Efficient** identity-based encryption without random oracles," in Advances in Cryptology EUROCRYPT 2005, ser. Lecture Notes in Computer Science, R. Cramer, Ed. Springer Berlin / Heidelberg, 2005, vol. 3494, pp. 114–127.*
[19] C. Gentry, "Practical identity-based encryption without random oracles," in Advances in Cryptology - EUROCRYPT 2006, ser. Lecture Notes in Computer Science, S. Vaudenay, Ed. Springer Berlin / Heidelberg, 2006, vol. 4004, pp. 445–464.
[20] C. Gentry, C. Peikert, and V. Vaikuntanathan, "Trapdoors for hard lattices and new cryptographic constructions," in Proceedings of the 40th annual ACM symposium on Theory of computing, ser. STOC '08. New York, NY, USA: ACM, 2008, pp. 197–206.
*[21] S. Agrawal, D. Boneh, and X. Boyen, "**Efficient** lattice (h)ibe in the standard model," in Advances in Cryptology EUROCRYPT 2010, ser. Lecture Notes in Computer Science, H. Gilbert, Ed. Springer Berlin / Heidelberg, 2010, vol. 6110, pp. 553–572.*
[22] D. Cash, D. Hofheinz, E. Kiltz, and C. Peikert, "Bonsai trees, or how to delegate a lattice basis," in Advances in Cryptology EUROCRYPT 2010, ser. Lecture Notes in Computer Science, H. Gilbert, Ed. Springer Berlin / Heidelberg, 2010, vol. 6110, pp. 523–552.
[23] Y. Hanaoka, G. Hanaoka, J. Shikata, and H. Imai, "Identity-based hierarchical strongly key-insulated encryption and its application," in Advances in Cryptology - ASIACRYPT 2005, ser. Lecture Notes in Computer Science, B. Roy, Ed. Springer Berlin / Heidelberg, 2005, vol. 3788, pp. 495–514.
*[24] D. Boneh, X. Ding, G. Tsudik, and C. Wong, "A method for fast **revocationofpublickeycertificatesandsecuritycapabilities,"**in 10th USENIX Security Symposium, 2001, pp. 297–308.*
*[25] B. Libert and J.-J. Quisquater, "**Efficient** revocation and threshold pairing based cryptosystems," pp. 163–171, 2003.*
*[26] H. Lin, Z. Cao, Y. Fang, M. Zhou, and H. Zhu, "How to design space **efficient** revocable ibe from non-monotonic abe," in Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security, ser. ASIACCS '11. New York, NY, USA: ACM, 2011, pp. 381–385.*

Curriculum Vitae

Name : Ankita Sahani

Address:-Ilahibagh Near S. B. Gorakhpur Pin code - 273001

Academic Details –

1) Pursuing M.tech (Computer Science and engineering) from Buddha nstitute of Technology (2018-2020) University-Dr. A.P.J Abdul Kalam technical University.
2) B.tech (IT) n 2017 from Buddha nstitute of Technology Gida gorakhpur