ISSN 2278-3091
Volume 8, No.4, July – August 2019
International Journal of Advanced Trends in Computer Science and Engineering
Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse76842019.pdf
https://doi.org/10.30534/ijatcse/2019/76842019

Revocable Identity Based Signature Scheme with Outsourced Cloud Revocation Authority

Pragya Mishra[1], Vandani Verma[2]
[1]Amity University, Noida-125,India, pragya.login@gmail.com
[2]Amity University, Noida-125, India, vandaniverma@yahoo.com

ABSTRACT

In last few years, many aspects of Identity based Cryptosystems (IBC) were studied because it has a critical feature of avoiding high overheads linked with management of public key certificate. But the one issue associated with it how to revoke defiant user remains open. Many schemes were proposed to overcome this problem. One move towards revocation in identity based settings was taken by introducing the key generation centre (KGC) which updates users' private key periodically. But with this move, computation work on KGC will increase quickly with increasing number of users. We have proposed an ID based signature scheme (IBS) with outsourced cloud revocation authority (CRA). In this scheme, the revocation functionality is outsourced to a CRA. We have described the system framework of the scheme as well as its security model with complete security analysis.

Key words : Cloud Computing, Identity based Signature (IBS), Revocation, outsourcing.

1. INTRODUCTION

In last few years, many aspects of Public key Cryptography (PKC) have been studied. The most important aspect studied among them was-Digital signatures. Digital signatures provide a user authentication, identification and non-repudiation. In ID based cryptosystems, information of user's identity is used as public key. Boneh and Franklin [2] suggested that KGC would periodically update secret keys for all non-revoked users. However, this proposal has two backdrops. One is that KGC must be online to revoke defiant users instantly which bring some threats. And the other one is huge load of overhead at KGC with increasing number of users. A speedy growth in field of cloud computing has made conscious the researchers towards outsourcing of computational tasks to some potent cloud aided server. In recent years, with this approach a revocable ID based encryption scheme was constructed [4]. In their scheme, they outsourced the task of key-updation to Key Update Cloud Service Provider (KU-CSP). The idea to offload all key-updating tasks to outsourced cloud authoirty is not very trustworthy. We have used this idea to construct an ID based signature scheme. In addition, shifting workloads to a shared infrastructure pacify the unauthorised access and disclosure of sensitive data. To have a secure data access on cloud during the data transmission, a security protocol was proposed [18] which serves the confidentiality, integrity, authencity and non-repudiation of data. However, a scheme [19] assures confidentiality of encrypted data against the new adversary. In Cloud-based systems require to be steady regarding identity management, authentication, compliance and access-related technologies, which are becoming very important day by day. In view of all, it is better to bifurcate the key-updating task in two fractions. One fraction of task to KGC and other fraction of task to CRA. The previous one is a long-term key linked with identity of users and issued by KGC. While the later one is a short-term key bounded with users identity as well as current time period.

The CRA issues and updates the time-update key periodically. In this way,the CRA can not create the true signature because it does not possess the complete signing key. In case of revocking user, KGC simply informs the cloud authority to stop issuing new time-update keys for such users.

In our paper, we have proposed a revocable ID based signature scheme with a cloud revocation authority. We have described this model frameowrk and its n identity based encryption for cloud data with analyzing its security.

1.1 Organization

Our paper is organised as- In section 2, we presents the related works done earlier in this type of IBE scheme to offload the revocation functionality . In the section 3, we have described the concept involved in the proposed scheme. The section 4, we have given the sytem framework of our propsed scheme. The section 5 gives algorithm involved in our proposed scheme. After this, we have made a security analysis of the scheme in section 6 and at end, we have given conclusion in section 7.

2. RELATED WORK

Identity based cryptosystem (IBC) was introduced by Shamir [1]. The first Identity Based Encryption (IBE) scheme practically implemented by Boneh and Franklin [2] which was founded on Weil pairing on elleptic curves. In addition, it was proven secure in random oracle model. However, first fully secure IBE without random oracle model [3] was also proposed. Since then solutions for many Identity Based Signature (IBS) schemes with bilinear pairing have been constructed. The scheme [8] was one of those which serves an efficient IBS scheme based on pairing. This scheme was extended to a general framework from which exportation of several variation (includes ElGamal variations and Schnorr version) could be done. Bellare [10] proposed a structure for security proof of Identity Based Signature (IBS) schemes. Efficient identity based encryption without random oracle was firstly proposed by Waters [13]. Further, an efficient IBS scheme with proven security in the standard oracle model was developed [7].

Further, many efficient IBS scheme with or withou bilinear pairing were proposed. However, only few of them was with property of revocation of unauthorised users. In 2008, a new revocable IBE scheme [5] was constructed which was based on the idea of revocation funcationality as proposed in the scheme [2]. This scheme [5] deployed a binary tree data-structure to store identities of users on leaf nodes. This delivers reduction in the key-update efficiency of private key generator upto logarithmic scale in the number of system users. However, in revokation phase, scheme [5] needs an increasing time cost with the no. Of system users for key update-time at private key generator. This aspect was given a solution by introducing outsourcing of computation into identity based encryption for very first time and constructed a revocable IBE scheme [6] in the server based setting to achieve solution of identity revocation. Because of constant Key-update efficiency, the scheme is independent of number of system users. They achieved this goal by employing a hybrid private key for every user based on AND gate used to connect and bound the time component and identity component. Libert [6] proposed the improvisation of the scheme [5] to attain adaptive-ID security.

In past, based on revocable funcationality, many IBS scheme were proposed. The first revocable Identity Based Signature (RIBS) scheme [9] was proven secure in the standard oracle model. By taking consideration of this scheme [9], another RIBS scheme [12] with improved security was proposed. In addition, an efficient RIBS scheme with outsourced revocation to cloud revocation server (CRS) [11] was also constructed. The computaion task required during key-updates are delegated to the outsourced cloud revocation server. This scheme is proven secure in random oracle model. In addition, this scheme is existentially unforgeable against adaptively chosen messages. For providing fine-grained access control to the data encrypted in cloud, many schemes have been proposed. Though, this created novel security and efficiency issues, if the access rights of some or all data users is vanished by the data owner. However, the revoked user may re-joins the system at some later time with different access rights [15]-[16]. A Secure Data Sharing (SDS) framework [17] does not allow leakage of information in the situation when user and cloud gets collusion from an earlier revoked user who rejoins the system some later time. Their solution lies in the ways of distribution of encrypted data as well as authorization tokens related to each data record between two clouds. In this way, it forms a federated cloud.

3. CONCEPTS INVOLVED

3.1 Identity based Signature

Idneity based signature (IBS) involves three users; the signer, the verifier and the KGC. An IBS scheme can be executed in four steps:

Set up: In this step, KGC takes security parameter λ as input and gives the master system key s_M , P_{pub} as public key, public parameters PP for the system.

Initial-key extraction: KGC uses master secret key and identity ID of a user as input to generate private key S_{ID} for each user.

Signature: The signer uses his/her privated key, the public parameters PP and the message m as input and outputs the signature σ .

Verification: Using signature σ ,signer's identity ID, message mand public parameters PP, the verifier returns ''Accept/Reject" to express that signature is valid or not.

3.2 Bilinear maps

Let G_1 and G_2 are two cyclic groups having same prime order p. Let g is a generator of G_1. A bilinear mapping is $e : G_1 \times G_1 \rightarrow G_2$ with the following properties:

1.Bilinear: for all m, n ∈ G and m, n ∈ Z, we have $e(u^m, v^{n)}) = e(u, v)^{mn}$
2. Non-degenerate: e(g, g) = 1

Here, G_1 is a bilinear group if the group action in G_1 is computable efficiently. In addtition, there exists a group G_2 as well as a bilinear map $e : G_1 \times G_1 \rightarrow G_2$ similar to above which is also efficiently computable.

3.3 Computational Diffie-Hellman (CDH) Problem

For a given (P, aP, bP) and some unknown $a, b \in Z_q^*$, to do computation of abP is CDH problem. The CDH assumption states that CDH problem with non-negligible probability can not be solved within polynomial time.

4. SYSTEMATIC FRAMEWORK OF THE PROPOSED SCHEME

Here, we have offered system framewok of the conceived scheme. An ID based signature scheme with revocable cloud authority is constituted with three parties: Key Generation Centre, the Cloud Revocation Authority and users (signers and verifiers). At initial stage KGC generates some public parameters and publish it in open domain. KGC also sends master secret time key to CRA. In next phase, KGC sends secret identity key to each registered user by using its master secret key. Then CRA issues and updates the time- update keys for the user as per the revocation list of users given by KGC. The framework of our proposed scheme is presented in the Figure 1.

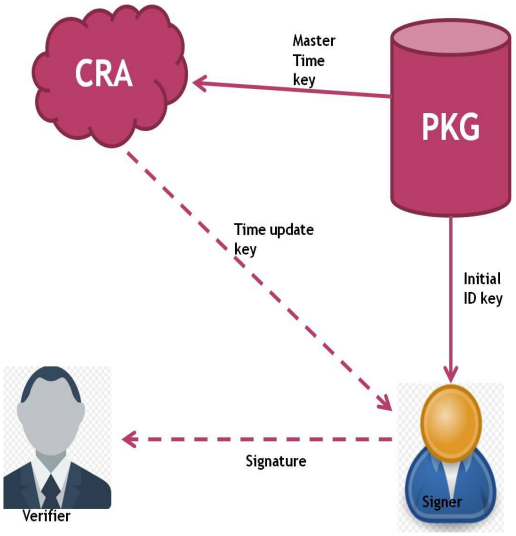

Figure 1 : IBS scheme with outsourced cloud revocation authority

5. SECURITY MODEL OF RIBS SCHEME

The security model of RIBS scheme was firstly proposed by Bellare [10]. In this model, security against existential forgery on adaptively chosen message as well as identity attacks were studied. Based upon this, we can find two type of adversaries-

- *Type I adversary AI*- AI is a revoked user with the identity ID. AI is revoked at time period T_i. AI is interested in producing valid signature after time period T_i. AI possesses the initial identity key D_{ID}. We assume that AI can collude with other legitimate users to get their time-update keys and private identity keys at arbitrary time periods. However, after revocation at time period T_i, AI would not be able to know its own time-update key.
- *Type II adversary AII*- This type of adversaery is a curious CRA who wants to creat a legitimate signature in the name of an authorized system user. Since, it holds the master time key, it can achieve the time-update key of any user at any time period. In this case, adversary AII can't know the users identity key D_{ID}. We will define the security model of our scheme via playing the two games between the challenger C_I and two types of adversaries AI & AII respectively.

Game A:

- Setup: C_1 runs the setup algorithmm using security parameters λ as input and gives master secret key S_k as output, master time key T_k and public parameters PP as per the system framework. C_1 keeps S_k and T_k secret and sends PP to AI.

- Query: AI raises a series of queries to C_1 adaptively and C_1 responds to every queries in following ways:

Initial key generation query (ID_k): To find out the initial key of any user with identity ID, AI raises this query. C_1 runs *InitKeyGen* algorithm with input (PP, S_k, ID) and returns the resultant D_{ID} to AI.

Time-Key Update query (ID_k, T_i). AI raises this query to know time update key of a user with identity ID at time period T_i. C_1 runs *TimKeyUpd* algorithm taking input (PP,T_k,ID,T_i) and sends the resulting TK_{ID,T_i} to AI.

*Signing query (m,ID,T_i).*When AI issues a signing query with message m, time period T_i and the identity ID.C_1 runs *SignGen* algorithm and result out a signature σ to AI.

- Forgery: At last AI gives a tuple (M', ID', T_i', σ') with two constraints given as under:
  1) AI does not publish any *Time Key Update query* on (ID`, $T_i$`).
  2) σ' is not the output of a *signing query* on input (M', ID', T_i') released by AI.

  AI would be said to succeed in attacking the scheme if *SignVerf* (PP, M', ID', T_1') = "Accept". AI's advantage $Adv_{A_I}(\lambda)$ is defined as-

$$Adv_{A_I}(\lambda) = \Pr[SignVerf(PP, M', ID', T_i') = "Accept"]$$

Game B: The Setup as well as Query phasesboth are same as in Game A.

- Forgery: AII outputs a tuple (M', ID', T_i', σ') with the under given two constraints:
  1) AII does not raise any *initial Key Extract query* on input ID'.
  2) σ' is not returned by a *signing query* on input (M', ID', T_i') issued by AII.

AII would be said to succeed in attacking the scheme if $SignVerf\ (PP, M', ID', T_i') =$ "Accept". AII's advantage $Adv_{A_{II}}(\lambda)$ is defined as-

$Adv_{A_{II}}(\lambda) = \Pr[SignVerf(PP, M', ID', T_i') = "Accept"]$

In view of the above two games, we can get the security definition of RIBS scheme in following ways:

"A RIBS scheme with outsourced revocation is said to be existentially unforgeable against adaptive chosen message and identity attacks if there is no probabilistic polynomial time adversary that has a non-negligible advantage in either Game A or Game B".

6 PROPOSED RIBS SCHEME WITH OUTSOURCED CRA

This scheme contains following steps:

Set up: In this step, PKG runs the algorithm in following ways;

- Choose two cyclic gorups G_1 and G_2, where G_1 is additive cyclic gorup of prime order q and with generator P. $e: G_1 X G_1 \to G_2$ is a bilinear mapping. We compute, $g = e(P, P)$.
- It randomly chooses two secret values $s, t \in z_p^*$ where t is master time key and s^t is master identity key. Then it computes $P_{pub} = s^t P, P_t = t\ P$. It keeps s^t secret and forward t to the CSP.
- The three hash functions defined $H_0 : \{0,1\}^* \to G_1,$ are- $H_1 : \{0,1\}^*\ X\ \{0,1\}^* \to G_1,$ $H_2 : \{0,1\}^*\ X G_2 \to Z_q^*$
- We publish the system parameters $PP = (G_1, G_2, p, P_{pub}, P_t, H_0, H_1, H_2)$

Intial key generation (InitKey Gen): PKG sets following for user with identity ID-

$Q_{ID} = H_1(ID), D_{ID} = s^t Q_{ID}$ and send this initial identity key D_{ID} through a secure manner to the user.

Time-key updation (TimeKeyUpd): When Cloud Revoaction Authority (CRA) receives a key-update request from user with identity ID at time period T_i, it computes

$Q_{ID}, T_i = H_2(ID, T_i), T_{ID,T_i} = t\ Q_{ID,T_i}$ and returns T_{ID,T_i} to the user.

Signature generation (Signgen): A signer with identity ID creates a signature for a given message M and time period T_i using the identity key D_{ID} and time update key $T_{ID,Ti}$ for message M as follows. Take random $r \& w \in z_p^*$ and compute in following manner:

User choose an arbitrary $\sigma \in \{0,1\}^n$ and computes-

$$\alpha = g^r, \beta = g^w$$
$$v = H_3(M, \alpha\beta^{-1})$$
$$U = rP - wP + v(D_{ID} + T_{ID,T_i})$$

The signature on message M at time period T_i is $\sigma = (U, \alpha\beta^{-1})$

Sign verification (SignVerf): For a given message M with a signature $\sigma = (U, \alpha\beta^{-1})$ at time period T_i, user computes-

$v = H_3(M, \alpha\beta^{-1})$

And verifies the signature only if

$e(U, P) = \alpha\beta^{-1} e(Q_{ID}, P_{pub})^v e(Q_{ID,T_i}, P_t)^v$ holds.The verifier accepts it otherwise rejects it.

The consistency of the scheme is as under:

$$e(U,P) = e(rP - wP + v(D_{ID} + T_{ID,T_i}), P)$$
$$= e(rP,P)e(-wP,P)e(D_{ID},P)^v e(T_{ID,T_i},P)^v$$
$$= e(P,P)^r e(P,P)^{-w} e(s^t Q_{ID},P)^v e(tQ_{ID,T_i},P)^v$$
$$= g^r g^{-w} (Q_{ID}, s^t P)^v e(Q_{ID,T_i}, tP)^v$$
$$= \alpha\beta^{-1} e(Q_{ID}, P_{pub})^v e(Q_{ID,T_i}, P_t)^v$$

7 SECURITY ANALYSIS OF PROPOSPOSED SCHEME

To perform security analysis of our scheme , we have used forking lemme technique [14].

Lemma1: If a type I adversary raises $q_{H0}, q_{H1}, q_{H2}, q_{ext}, q_{upd}, q_{sign}$ queries to the hash functions H_0 ,H_1,H_2 time key update oracle, initial key extract oracle, signing oracle and cracks the scheme with non-negligible probability $\in_1$, then there exists a probabilistic challenger who has the ability to solve the CDH problem with advantage

$$\in_1' \geq (1 - \frac{1}{q}) \frac{1}{q_{H2}} \in_1 - \frac{q_{H3}}{q}$$

Proof: Assume that AI is a Type I adversary who is the winner of attack game with advantage $\in_1$. We propose an algorithm ALG_1 which solves the CDH problem useing adversary AI as subroutine. Suppose ALG_1 is given a CDH instance

$(P, P_a = aP, P_b = bP)$, where P is generator of group G_1 of order q and a, b is unknown to AI. ALG_1 simulates a challenger to compute P_{ab}=abP for the adversary in following ways:

- Set up: ALG_1 chooses randomly $s,t \in z_p^*$ and sets $P_{pub}=s^tP$, $P_t=P_a$ and sends (P, P_{pub}, P_t) to the adversary AI. ALG_1 selects an $l = \{1, 2, ...q_{H1}\}$ and updates three empty lists L_1, L_2 and L_3 as per the queries accordingly.

- Query:

Hash query: Suppose that AI has already raised querries of concerned hash oracles before making further queries. ALG_1 responds for three kinds of hash queries as under-

H_0-query: AI issues a H_0 query on identity ID. ALG_1 firstly checks whether any entry in lsit L_1. If yes, ALG_1 returns that entry, else ALG_1 randomly chooses $x \in z_q^*$ and returns $H_0(ID) = xP$ with addition of $(ID, x, H_0(ID))$ into list L_1.

H_1-query: Suppose that ALG_1 issues i-th H_1-query against identity ID_i and time period T_j. ALG_1 firstly checkls whether list L_2 has any entry in it. If so, ALG_1 returns that entry, else it randomly chooses $y \in z_q^*$ and creates

$$H_1(ID_i, T_j) = \begin{cases} yP & i \neq l \\ yP_b & i = l \end{cases}$$

ALG_1 adds $(ID_i, T_j, y, H_1(ID_i, T_j))$ into list L_2 if $i \neq l$ otherwise ALG_1 adds $(ID_i, T_j \perp, H_1(ID_i, T_j))$ and sets $ID' = ID_i, T' = T_j$

H_2-query: When ALG_1 receives a *H_2-query* on input $(M, \alpha\beta^{-1})$, it firstly checks entry in list L_3. If there is entry in the list, ALG_1 returns the same, otherwise returns a $v \in z_q^*$ randomly chosen and adds $(M, \alpha\beta^{-1}, H_2(M, \alpha\beta^{-1}))$ into list L_3.

Initial key extraction query: For such type of query against identity ID, ALG_1 explores list L_1 to find the entry $(ID, x, H_0(ID))$ and responds with $D_{ID} = xP_{pub}$.

Time key updating query: If AI issues a query on ID_i and T_j, ALG_1 first checks if $(ID_i, T_j) = (ID', T')$. If not, ALG_1 explores the list L_2 to find out the entry $(ID_i, T_j, y, H_2(ID))$ and returns $T_{ID_i,T_j} = yP_t$ else it sets $T_{ID_i,T_j} = \perp$.

Signing query: On receiving the signing query from AI against identity ID_i,T_j and message M, ALG_1 explores the list L_1,L_2 to search the corresponding $H_0(ID)$ and $H_1(ID, T_i)$. ALG_1 chooses $U \in G, v \in z_q^*$ randomly and computes

$$\alpha\beta^{-1} = e(U, P)e(P_{pub}, H_0(ID_i))^{-v} e(P_t, H_1(ID_i, T_j))^{-v}$$

Now ALG_1 explores the list L_3, if there is any entry $(M, \alpha\beta^{-1}, H_2(M, \alpha\beta^{-1}))$ and $H_2(M, \alpha\beta^{-1}) \neq v$, then ALG_1 returns the signature $\sigma = (U, \alpha\beta^{-1})$ to AI. Here, σ is a valid signature.

- Forgery: At last, adversary AI outputs a signature $\sigma' = (U', \alpha'(\beta^{-1})')$ on $ID"T"$ and message M'. If $(ID'', T'') = (ID', T')$ and $Ver(PP, M', ID', T') = "Accept"$ then output will be $\sigma' = (U', \alpha'(\beta^{-1})')$ otherwise it returns $"Fail"$. ALG_1 runs the simulated game twice with the same random coins but it replies the hash queries raised by adversary AI with altered random values. As per the General Forking Lemma, AI will output a different forgery $\sigma" = (U", \alpha"(\beta^{-1})")$ on the same identity ID‘, message M‘ and time period T‘ with non-negligible probability. We have, $\alpha' = \alpha" = g^r, \beta' = \beta" = g^w$ from some $r, w \in z_q^*$ while the hash values are different corresponding to the two forged signatures. We consider that for the signature $\sigma' = (U', \alpha'(\beta^{-1})')$, $H_0(ID') = x'P$, $H_1(ID', T') = y'P_b, H_2(M', \alpha'(\beta^{-1})') = v'$

While in signature $\sigma" = (U", \alpha"(\beta^{-1})")$ $H_0(ID") = x"P$, $H_1(ID", T") = y"P_b, H_2(M", \alpha"(\beta^{-1})") = v"$. Since the selection of hash values are random so, $x' \neq x", y' \neq y", v' \neq v"$ with elevated probability.

Since both $\sigma' = (U', \alpha'(\beta^{-1})')$ and $\sigma" = (U", \alpha"(\beta^{-1})")$ are valid signatures, we have,

$$e(U', P) = \alpha'(\beta^{-1})' e(P_{pub}, x'P)^{v'} e(P_t, y'P_b)^{v'}$$

$$e(U", P) = \alpha"(\beta^{-1})" e(P_{pub}, x"P)^{v"} e(P_t, y"P_b)^{v'}$$

By dividing both the abov e equations with condition $\alpha' = \alpha"$, we get

$$e(U'-U'',P)=e(P_{pub},P)^{x'v'-x''v''}e(P_t,P_b)^{y'v''-y''v''}$$
$$=e(sP,P)^{x'v'-x''v''}e(P_a,P_b)^{y'v'-y''v''} \quad \text{then}$$
$$=e(P,sP)^{x'v'-x''v''}e(P,P_{ab})^{y'v'-y''v''}$$
$$e(P,P_{ab})^{y'v'-y''v''}=e(P,U'-U'')e(P,sP)^{x''v''-x'v'}$$
$$=e(P,U'-U'')e(P,(x'v'-x''v''),sP)$$
$$=e(P,U'-U'')+(x''v''-x'v')sP)$$

So

$$e(P,P_{ab})=e(P,U'-U'')+$$
$$(x''v''-x'v')sP)^{(y'v'-y''v'')^{-1}}$$
$$=e(P,(y'v'-y''v'')^{-1}(U'-U'')+$$
$$(x''v''-x'v')sP))$$

From the above equation, we may obtain $P_{ab}=(y'v'-y''v'')^{-1}(U'-U''+(x''v''-x'v')sP)$ and thus we get the solution of challenging CDH instance.

Now we would analyze the probability of success of ALG_1. During the setup and query phases, the simulation performs well except happening of two events. One is - ALG_1 issues a query (ID',T') to H_2 oracle which has a probability of q_{H2}/q.

Second is, ALG_1 returns a signature (U,α) on (M,IDi,T_j) and $H_2(M,\alpha\beta^{-1})$ exists already in list L_3, where, $H_2(M,\alpha\beta^{-1})\neq v$ and v is randomly chosen by . Probability of happeninig of this event is q_{H3}/q. If the simulation takes place smoothly, then during the forgery phase, AI will produce a valid forgery (ID'',T'',M',σ') with an advantage of $\in_1$. Since H_1 is random oracle, probability that (ID'',T'',M',σ') is valid without any query of $H_1(ID'',T'')$ is 1/q. So, in the query phase , (ID'',T'') has been queried to H_1 oracle with a probability of $1-\frac{1}{q}$. Also, l is chosen randomly from $\{1,2,...q_{H1}\}$. Thus, $(ID'',T'')=(ID',T')$ holds with aprobability of $(1-\frac{1}{q})\frac{1}{q_{H1}}$ .Therefore, probability that $Ver(ID'',T'',M',\sigma')=Accept$ and $(ID'',T'')=(ID',T')is$ $(1-\frac{1}{q})\frac{1}{q_{H1}}\in_1-\frac{q_{H2}}{q}$. This is the probability of solving the CDH problem by ALG_1.

Lemma 2. If there is a type II adversary who raises $q_{H0},q_{H1},q_{H2},q_{ext},q_{upd},q_{sign}$ queries to the hash functions H_0,H_1,H_2, time-update key oracle, initial key extract oracle, signing oracle and cracks the scheme with non-negligible probability $\in_1$, then there exists a probabilistic challenger who would be able to solve the CDH problem with advantage

$$\in_2^{'}\geq(1-\frac{1}{q})\frac{1}{q_{H0}}\in_2-\frac{q_{H2}}{q}$$

Proof: Assume that AII is a Type II adversary who wins the attack game with advantage $\in_2$. We construct an algorithm ALG_{II} which solves the CDH problem useing adversary AII as subroutine. Suppose ALG_{II} is given a CDH instance $(P,P_a=aP,P_b=bP)$, where P is generator of cyclic group G_1 with prime order q and a, b is unknown to ALG_{II}. It simulates a challenger to compute P_{ab}=abP for the adversary in following ways:

- Set up: ALG_{II} chooses randomly $t\in z_p^*$ and sets $P_{pub}=P_a$, $P_t=tP$ and sends (P, P_{pub}, P_t) to the adversary AII. ALG_{II} selects an $l=\{1,2,...q_{H1}\}$ and updates three empty lists L_1, L_2 and L_3 as per the queries accordingly.

- Query:

Hash query. Suppose that AII has already raised the concerned hash oracles before making additional queries. ALG_{II} responds for three kinds of hash queries as given under-

H_0-query: Suppose that ALG_{II} issues i-th H_1-query against identity ID_i. ALG_{II} firstly checks whether list L_1 has any entry in it. If so, ALG_{II} returns the same entry, else it chooses randomly $x\in z_q^*$ and creates

$$H_0(ID_i)=\begin{cases}xP & i\neq l\\ xP_b & i=l\end{cases}$$

ALG_{II} returns $H_0(ID_i)$ to AII and adds $(ID_i,x,H_0(ID_i))$ into list L_1 if $i\neq l$ otherwise ALG_{II} adds $(ID_i,\perp,H_0(ID_i))$ into list L_1 and sets $ID^{'}=ID_i$

H_1-query: AII issues a H_2 query on identity ID_i and T_j , ALG_{II} firstly checks whether any entry in lsit L_2. If yes, ALG_{II} returns the entry, else ALG_{II} chooses randomly

$y \in z_q^*$ and returns $H_0(ID_i, T_j) = yP$ with further addition of $(ID_i, T_j, y, H_1(ID_i, T_j))$ into list L_2.

H_2-query: When ALG_{II} receives a *H_3-query* on input $(M, \alpha\beta^{-1})$, it firstly checks entry in list L_3. If there is, ALG_{II}, it returns that entry, else returns a $v \in z_q^*$ which is randomly chosen and adds $(M, \alpha\beta^{-1}, H_2(M, \alpha\beta^{-1}))$ into list L_3.

Initial key extraction query: For such type of query against identity ID, ALG_{II} explores if ID=ID*. If not, it explores list L_1 to find the entry $(ID, x, H_0(ID))$ and responds with $D_{ID} = xP_{pub}$ else ALG_{II} returns $\perp$.

Time key updating query: If AII issues a query on ID_i and T_j, ALG_{II} explores the list L_2 to find out the entry $(ID_i, T_j, y, H_1(ID_i, T_j))$ and responds with $T_{ID_i,T_j} = yP_t$.

Signing query: On receiving the signing query from AII against identity $ID_i T_i$ and message M, ALG_{II} first explores the list L_1, L_2, L_3 to find out the corresponding $H_0(ID)$ and $H_1(ID, T_i)$. ALG_{II} chooses $U \in G, v \in z_q^*$ randomly and calculates-

$$\alpha\beta^{-1} = e(U, P)e(P_{pub}, H_0(ID))^{-v} e(P_t, H_1(ID, T_i))^{-v}$$

Now ALG_{II} explores the list L_3, if there is any entry $(M, \alpha\beta^{-1}, H_2(M, \alpha\beta^{-1}))$ and $H_2(M, \alpha\beta^{-1}) \neq v$, then ALG_{II} returns the signature $\sigma = (U, \alpha\beta^{-1})$ to AII. Here, σ is a valid signature.

- Forgery: At last, adversary AII outputs a signature $\sigma' = (U', \alpha'(\beta^{-1}))'$ on ID'', T'' and message M‘.

If $(ID', T') = (ID', T')$ and $Ver(PP, M', ID'', T'') = "Accept"$ then output $\sigma' = (U', \alpha'(\beta^{-1}))'$ as the forgery otherwise output comes $"Fail"$. ALG_{II} runs the simulated game two times with the same random coins but it returns the hash queries rasied by adversary AII with altered random values. Using the General Forking Lemma, AII will give a different forgery $\sigma'' = (U'', \alpha''(\beta^{-1}))''$ on the same identity ID', message M' and time period T' with non-negligible probability. We have, $\alpha' = \alpha'' = g^r, \beta' = \beta'' = g^w$ from some $r, w \in z_q^*$ and assume that for the signature $\sigma' = (U', \alpha'(\beta^{-1}))'$, $H_0(ID') = x'P_b$, $H_1(ID', T_i') = y'P_t, H_2(M', \alpha'(\beta^{-1})') = v'$

While in signature $\sigma'' = (U'', \alpha''(\beta^{-1}))''$, $H_0(ID') = x'P_b$, $H_1(ID', T_i') = y''P_t, H_2(M', \alpha'(\beta^{-1})') = v''$. Since the selection of hash values are random so, $x' \neq x'', y' \neq y'', v' \neq v''$ with elevated probability.

On the other side, since both $\sigma' = (U', \alpha'(\beta^{-1}))'$ and $\sigma'' = (U'', \alpha''(\beta^{-1}))''$ are valid signatures, we have,

$$e(U', P) = \alpha'(\beta^{-1})' e(P_{pub}, x'P_b)^{v'} e(P_t, y'P)^{v'}$$

$$e(U'', P) = \alpha''(\beta^{-1})'' e(P_{pub}, x''P_b)^{v''} e(P_t, y''P)^{v''}$$

By dividing both the abov e equations with condition $\alpha' = \alpha''$, we get

$$e(U'-U'', P) = e(P_{pub}, P_b)^{x'v'-x''v''} e(P_t, P)^{y'v'-y''v''}$$

$$= e(aP, bP)^{x'-x''v''} e(tP, P)^{y'v'-y''v''}$$ then

$$= e(P, P_{ab})^{x'v'-x''v''} e(P, tP)^{y'v'-y''v''}$$

$$e(P, P_{ab})^{y'v'-y''v''} = e(P, U'-U'')e(P, tP)^{y''v''-y'v'}$$

$$= e(P, U'-U'')e(P, (y'v'-y''v''), tP)$$

$$= e(P, (U'-U'') + (y''v''-y'v')tP)$$

So

$$e(P, P_{ab}) = e(P, (U'-U'') + (y''v''-y'v')tP)^{(x'v'-x''v'')^{-1}}$$

$$= e(P, (x'v'-x''v'')^{-1}((U'-U'') + (y''v''-y'v')tP))$$

From the above equation, we get-

$P_{ab} = (x'v'-x''v'')^{-1}(U'-U'' + (y''v''-y'v')tP)$ and thus we get the solution of challenging CDH instance.

Here, analysis of advantage of ALG_{II} is similar to ALG_I in simulated Game I. AII will output a valid signature on identity ID ID' in the end with the probability $(1-\frac{1}{q})\frac{1}{q_{H0}} \in_2 -\frac{q_{H2}}{q}$. This is the real advantage gained by ALG_{II} in the game II. By merging lemma 1 and lemma 2 together, following theorem may be obtained:

Theorem: The proposed RIBS scheme is existence unforgeable against adaptive chosen identity as well as message attack under the CDH assumption.

8 CONCLUSIONS AND FUTURE WORK

We studied previously proposed revocable identity based signature schemes which were contributed for shifting of revocation task of defiant users.We have aslo constructed a revocable IBS scheme in which during the key-updates process, most of the computational tasks are offloaded to the CRA. Security analysis of the proposed revocable identity based signature scheme shows that scheme is existence unforgeable against adaptive chosen identity as well as message attack under the Computational Diffie Hellman assumption.

REFERENCES

1. A. Shamir, "**Identity-based cryptosystems and signature schemes**," *in Advances in cryptology*, pp. 47-53, 1985. https://doi.org/10.1007/3-540-39568-7_5
2. D. Boneh and M. Franklin, "**Identity-based encryption from the Weil pairing**," *SIAM Journal on Computing*, vol. 32, pp. 586-615, 2003. https://doi.org/10.1137/S0097539701398521
3. C.Gentry, "**Practical identity-based encryption without random o**racles," *in Advances in Cryptology-EUROCRYPT 2006*, ed:Springer, pp. 445-464. https://doi.org/10.1007/11761679_27
4. J. Li, Jingwei Li, X. Chen, C. Jia and W. Lou, "**Identity based Encryption with outsourced revocation in cloud computing**", *in IEEE transactions on computers*, 2015,vol. 64(2), https://doi.org/10.1109/TC.2013.208
5. A. Boldyreva, V. Goyal and V. Kumar, "**Identity based encryption with efficient revocation**", *in Proceedings of 15th ACM conference on computer and communications security*, ser. CCS'08. New York, NY, USA: ACM, 2008, pp. 417-426, https://doi.org/10.1145/1455770.1455823
6. B. Libert and D. Verngnaud, "**Adaptive id-secure revocable identity based encryption**", *In Topics in Cryptology* CT-RSA 2009, ser. LNCS, M. Fischlin. Ed. Springer Berlin/Heidelberg, vol.5473, pp 1-15, 2009. https://doi.org/10.1007/978-3-642-00862-7_1
7. K.G. Paterson and J.C. N. Schuldt, "**Efficient identity-based signatures secures in the Standard Model**" Berlin. Germany; Springer 2006. https://doi.org/10.1007/11780656_18
8. F. Hess, "Efficient identity-based signature schemes based on pairings," Berlin. Germany; Springer 2003. https://doi.org/10.1007/3-540-36492-7_20
9. T.T.Tsai, Y.M. Tseng and T.Y.Wu, "**Provably secure revocable id-based signature in the standard model**", *Secure. Commun. Netw.*, vol.6, no. 10, pp, 1250-1260, 2013. https://doi.org/10.1002/sec.696
10. M. Bellare, C. Namprempre and G. Neven, "**Security proofs for identity based identification and signature schemes**, *J. Cryptol*., vol. 22, no. 1, pp. 1-61, 2009. https://doi.org/10.1007/s00145-008-9028-8
11. X. Jia, D. He, S. Zeadally and L. Li. "**Efficient revocable ID-based signature with cloud revocation serve**r", *IEEE Access*, vol. 5, pp. 2945-2954, 2017. https://doi.org/10.1109/ACCESS.2017.2676021
12. Y.H. Hung, T.T.Tsai, Y.M.Tseng and S.S. Huang. "**Strongly secure revocable id-based signature without random oracles**", *Inf. Technol. Control*, vol.43, no. 3, pp 264-276, 2014. https://doi.org/10.5755/j01.itc.43.3.5718
13. B. Waters. "Efficient identity based encryption without random oracles". Berlin. Germany; *Springer* 2005. https://doi.org/10.1007/11426639_7
14. D. Pointcheval and J. Stern, "**Security arguments for digital signatures and blind signatures**", *J. Crypto*l., vol. 13, no. 3, pp. 361-396, 2000. https://doi.org/10.1007/s001450010003
15. S. Yu, C. Wang, K. Ren, and W. Lou. "**Achieving secure, scalable, and fine-grained data access control in cloud computing**". In *Proceedings of IEEE INFOCOM*, pp. 1–9, 2010.
16. G. Wang, Q. Liu, and J. Wu. "**Hierarchical attribute-based encryption for fine-grained access control in cloud storage services**". In *Proceedings of the 17th ACM conference on Computer and communications security*, CCS'10, pp. 735–737, 2010. https://doi.org/10.1145/1866307.1866414
17. BK Samanthula, Y. Elmehdwi, G. Howser and S. Madria. "**A Secure Data Sharing and Query Processing Framework via Federation of Cloud Computin**g". *Information Systems* vol 48. pp 196-212, 2015. https://doi.org/10.1016/j.is.2013.08.004
18. A.E Karrar, M.F.I. Fadl. **"Security protocol for data transmission in cloud computing**". *International Journal of Advanced Trends in Computer Sciences and Engineering*, Vol 7 ,No. 1, pp. 1-5, 2018. https://doi.org/10.30534/ijatcse/2018/01712018
19. G. Amarulla, M. Mourya, R. R. Sanikommu and A.A. Afroz. **"A survey of : Securing Cloud Data under Key Exposure"**, *International Journal of Advanced Trends in Computer Sciences and Engineering*, Vol 7, No. 3, pp. 30-33, 2018. https://doi.org/10.30534/ijatcse/2018/01732018