IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727
PP 51-58
www.iosrjournals.org

Authentication and Revocation Of Roaming Users

Jini Kuriakose[1], Silpa Kamalan[2], Dr Suvanam Sasidhar Babu[3]
[1.] *Department of CSE, SNGCE, Kadayiruppu, Kerala, India*
[2.] *Department of CSE, SNGCE, Kadayiruppu, Kerala, India,*
[3.] *Department of CSE, SNGCE, Kadayiruppu, Kerala, India,*

Abstract: *Roaming means a mobile device moving from home location to a foreign location. The paper mainly focuses on the authentication and revocation of roaming users. User revocation can occur in two ways such as natural revocation and premature revocation. Natural revocation occurs due to the expiration of the secret key and premature revocation is mainly due to the unauthorized activities such as hacking. The system make use of group signature for authentication and revocation is efficient.*
Keywords: *Roaming, Group Signature, Revocation, Secret key, Anonymity.*

I. Introduction

Mobile computing is getting much priority now a days since the number of portable computers is increasing and also due to the desire to have continuous network connectivity to the Internet irrespective of the physical location of the node. Mobile device users can use their network services while they are in the foreign area through roaming services. Roaming services should be secure, i.e., provide authentication to identify legal roaming users[2]. Anonymous authentication methods are used to achieve secure authentication and location privacy simultaneously. There are mainly two types of anonymous authentication: weak user anonymity authentication and strong user anonymity authentication. The weak user anonymous authentication hides the user_s identity only from third parties, whereas the strong user anonymous authentication hides the user_s identity even from foreign servers.

User revocation is of great importance to roaming protocols. Due to various reasons (e.g., the subscription period of a user has expired), the foreign server needs to find outwhether a roaming user is revoked. Any revoked user should not be allowed to enter the foreign network.

It is quite difficult to achieve efficient user revocation because of the difficulty in taking back the electronic credential. Validity check and Revocation check are the two main steps in the verification phase of authentication. Validity Check is performed to find whether the authentication token is from a valid user and Revocation Check checks whether the user has been revoked. Revocation can either be natural or premature. Natural user revocation occurs when the user's access rights has expired. Premature revocation can occur before the expiry time due to the compromise of the credential[2].

D.He et al. [3] proposed a privacy-preserving universal authentication protocol, called Priauth, which provides strong user anonymity against both eavesdroppers and foreign servers, session key establishment, and achieves efficiency. Hyo Jin Jo et al. [1] proposed a privacy preserving anonymous authentication for mobile networks where user authentication is done without involving a home server. The protocol uses a pseudo-identity-based signcryption scheme to perform efficient revocation with a short revocation list and efficient authentication. Chen et al. [4] proposed a VLR group signatures with indisputable exculability and efficient revocation. Security of scheme is based on the strong Diffie-Hellman assumption and the decisional Diffie-Hellman assumption in the random oracle model.

Similar to many existing anonymous authentication primitives (e.g., [5], [6], [7], [8], [9], [10], [11], [12]) which support revocation, either all unrevoked users need to update their credentials regularly, or the server needs to perform extra steps in verification to check each member against a revocation list. As time goes by, the list will just become larger since the authentication is anonymous. All kind of users to be revoked, including those who were authorized for a limited time period, will be added to the revocation list.

II. Authentication

The security requirements for the system are as follows:

- Subscription Validation: the foreign server is sure about the identity of the home server of the user;
- User Anonymity: besides the user and the home server, no one including the foreign server can tell the

identity of the user;

- User Untraceability: besides the user and the home server, no one including the foreign server is able to identify any previous protocol runs which have the same user involved.
- Provision of User Revocation Mechanism [3], [13]: due to various reasons the foreign server should be able to find out whether a roaming user is revoked;
- Server Authentication: the user is sure about the identity of the foreign server;
- Key Establishment: the user and the foreign server establish a random session key which is known only to them and is derived from contributions of both of them such that the home server cannot predict the value of it.

Notations used in the description is summarized in table 1.

$\mathcal{U}_i$	User i
$\mathcal{V}$	Foreign server
$\mathcal{H}$	Home server
gpk	Public parameter of the group signature scheme
msk	Master secret key
gsk_i	User secret key of user $\mathcal{U}_i$, kept by the user
grt_i	Revocation token of user $\mathcal{U}_i$, kept by the group manager
σ	Signature generated by the user
RL	Revocation list
ID	temporary identity chosen by the user
$\mathcal{SIG}$	Signature scheme chosen by each server
$\mathcal{ENC}$	Symmetric encryption scheme chosen by each server

Table 1: Frequently Used Notations

A group signature scheme is used as a primitive for both anonymous authentication and premature revocation. Group signature, introduced by Chaum and van Heyst [14], allows a member of a group to sign messages on behalf of the group without leaking his identity. But there is a group manager who has some trapdoor information which allows him to recover the identity of the signer from any valid group signature. A normal group signature cannot achieve our goal since the signature itself does not bear with any time-related information. In the authentication phase, the foreign server gives a user U_i a challenge message m and a current time t. If U_i can generate a valid signature on m and prove that $t < \tau_I$ where τ_i is the key expiry time for user U_i , the
foreign server believes that U_i is authorized by his home server and his secret key has not expired.

A group signature[6] scheme allows users to authenticate themselves with both constant-size transcripts and full anonymity. A group signature scheme consists of a tuple of probabilistic polynomial-time algorithms (Gp.Kg, Gp.Join, Gp.Sign, Gp.Ver, Gp.Trace). During Gp.Kg, the group manager generates a master public key gpk and a master secret key msk. gpk is published while msk is kept secret. During Gp.Join, the group manager uses msk to generate a user secret key gsk_i for user U_i and a revocation token grt_i which is used to trace user U_i . During Gp.Sign, a user U_i uses his secret key gsk_i to generate a signature σ for a message m at time t. Gp.Ver takes mpk, t, m, σ and returns valid or invalid. Gp.Trace takes mpk, grt_i and a valid message-signature pair (m, σ) and returns true or false.

1) Master Key Generation Phase (Gp.Kg): The system structure is similar to the group signature scheme from Bringer and Patey construction [15]. The group manager chooses bilinear groups G_1 , G_2 of prime order p. Assume H is a hash function with range Z_p . The group manager randomly chooses

$$h, \bar{h}, \bar{g} \in \mathbb{G}_1, g_2 \in \mathbb{G}_2, Q \in \mathbb{G}_2$$

and γ_1 , γ_2 , $z \in Z^*_p$, and sets $g_1 \leftarrow \psi(g_2)$, $z_1 \leftarrow g_2^{\gamma_1}$ and $z_2 \leftarrow g_2^{\gamma_2}$. Let l be the

maximum length of the time representation. The group public key is defined as

$$gpk \leftarrow (g_1, g_2, h, \tilde{g}, \tilde{h}, z_1, z_2, H, \ell, Q, Q^z, Q^{z^2}, \cdots, Q^{z^\ell}),$$

and the master secret key is defined as msk ← (γ_1 , γ_2). The group manager publishes gpk and keeps msk secret. The group manager also maintains a revocation list RL which is initialized as an empty set.

2) User Joining Phase (Gp.Join): A new user U_i can request to join the group.
2.1 U_i randomly chooses a secret $f_i \in Z_p$. 2.2 U_i outputs $F_i \leftarrow h^{f_i}$ and proves the knowledge of f_i to the manager. This can be done by the following steps:
a) U_i computes $F\hat{} \leftarrow h^{f\hat{}}$ for some random $f\hat{}$
$\in Z_p$.
b) U_i computes $r\hat{} \leftarrow f\hat{} + H(F_i , F\hat{})f_i \bmod p$ and sends F_i , $F\hat{}$, $r\hat{}$ to the group manager. c) The group manager checks if $h^{r\hat{}} = F\hat{} \, F_i^{H}$

.
2.3 The group manager computes $\{\tau_{ij}\}_{j\varepsilon[1,l]}$
← 1-ENC(τ_i), where τ_i is the expiry time of U_i 's key.

2.4 For each $j \in \{1, 2, \ldots, l\}$, the group manager computes

$$A_{ij} \leftarrow (g_1 F_i)^{1/(\tau_{ij} + \gamma_2 + x_{ij})} * \quad \text{where } x_{ij} \in_R Z_p$$

and

$\tau_{ij}\, \gamma_1 + \gamma_2 + x_{ij} \neq 0$. Note that when τ_{ij} is null, the corresponding A_{ij} element will not be given to the user.
2.5 The group manager sends U_i (τ_i , $\{x_{ij}$, $A_{ij}\}_{j\varepsilon[1,l]}$).

2.6 U_i verifies that $e(A_{ij} , z_1^{\tau_{ij}} z_2 g_2^{x_{ij}}) = e(g_1 F_i , g_2)$ for all $j \in \{1, 2, \ldots, l\}$.

Finally, user U_i gets the secret key $gsk_i \leftarrow (\tau_i$, f_i , $\{x_{ij} , A_{ij}\}_{j\varepsilon[1,l]}$) and the group manager keeps the revocation token $grt_i \leftarrow (\tau_i , \{x_{ij}\}_{j\varepsilon[1,l]})$ and stores (U_i , grt_i) as a row entry in the user database. Later if user U_i is

prematurely revoked, the group manager adds grt_i into the revocation list RL.

3) Signing Phase (Gp.Sign): A user U_i signs a message m at time t by the following steps:
3.1 Compute $\{\tau_{ij}\}_{j\varepsilon[1,l]} \leftarrow$ 1-ENC(τ_i) and $\{t_j\}_{j\varepsilon[1,l]} \leftarrow$ 0-ENC(t).
3.2 Find an index $1 \le k \le l$ such that $\tau_{ik} = t_k$
.
3.3 Compute $w \leftarrow Q^{\prod_{j=1}^{l} (z+t_j)/(z+t_k)}$.
3.4 Choose a random $B \in G_1$.
3.5 Compute $J \leftarrow B^{f_i}$ and $K \leftarrow B^{x_{ik}}$.

(Element J is for exculpability as it involves user's secret f_i that is not known to anyone else. Element K allows revocation. Finally the randomization brought by element B helps to ensure the anonymity of the user.)

3.6 Compute $T \leftarrow A_{ik} \, h^{\rho_1}$ for randomly chosen $\rho_1 \in Z_p$.
3.7 Compute $W \leftarrow w \, h^{\rho_2}$ for randomly chosen $\rho_2 \in Z_p$.
3.8 Compute $V_1 \leftarrow g^{x_{ik}} h^{\rho_3}$ for randomly

chosen $\rho_3 \in Z_p$.
3.9 Compute $V_2 \leftarrow g^{tk} h^{\rho 4}$ for randomly
chosen $\rho_4 \in Z_p$.
(Elements T , W , V_1 and V_2 can be
considered as commitments of A_{ik} , w, x_{ik} and t_k respectively, which bind the signature
with these values in a hidden way.)
3.10 Let $\beta_1 \leftarrow x_{ik} \rho_1$, $\beta_2 \leftarrow \rho_1 \rho_3$, $\beta_3 \leftarrow t_k \rho_1$, $\beta_4 \leftarrow \rho_1 \rho_4$, $\beta_5 \leftarrow t_k \rho_2$, $\beta_6 \leftarrow \rho_2 \rho_4$.

3.11 Randomly pick r_x , r_f , r_t , $r_{\rho 1}$, $r_{\rho 2}$, $r_{\rho 3}$, $r_{\rho 4}$, $r_{\beta 1}$, $r_{\beta 2}$, $r_{\beta 3}$,$r_{\beta 4}$, $r_{\beta 5}$, $r_{\beta 6} \in Z_p$.

3.12 Compute helper values (for the proof-

of-knowledge system proving the well-formness of the signature to the verifier):

$$R_1 \leftarrow B^{r_f}, \quad R_2 \leftarrow B^{r_x}, \quad R_3 \leftarrow K^{r_{\rho 1}} B^{-r_{\beta 1}}$$
$$R_4 \leftarrow e(h, g_2)^{-r_f} \cdot e(T, z_1)^{r_t} \cdot e(T, g_2)^{r_x} \cdot e(\tilde{h}, z_1)^{-r_{\beta 3}} \cdot e(\tilde{h}, g_2)^{-r_{\beta 1}} \cdot e(\tilde{h}, z_2)^{-r_{\rho 1}}$$
$$R_5 \leftarrow \tilde{g}^{r_x} \tilde{h}^{r_{\rho 3}}, \quad R_6 \leftarrow \tilde{g}^{r_{tk}} \tilde{h}^{r_{\rho 4}},$$
$$R_7 \leftarrow e(W, Q)^{r_t} e(\tilde{h}, Q)^{-r_{\beta 5}} e(\tilde{h}, Q^z)^{-r_{\rho 2}}$$
$$R_8 \leftarrow \tilde{g}^{r_{\beta 1}} \tilde{h}^{r_{\beta 2}} V_1^{-r_{\rho 1}}, \quad R_9 \leftarrow \tilde{g}^{r_{\beta 3}} \tilde{h}^{r_{\beta 4}} V_2^{-r_{\rho 1}},$$
$$R_{10} \leftarrow \tilde{g}^{r_{\beta 5}} \tilde{h}^{r_{\beta 6}} V_2^{-r_{\rho 2}}$$

(Intuitively, R_1 , R_2 and R_3 are proving the well- formness of the secret components that is only known to the user, which gives exculpability and traceability; R_4 , R_5 , R_8 , R_9 are on the validity of the secret key issued to the user; finally, R_6 , R_7 , R_{10} are proving that the expiry time is later than the current time.)

3.13 Compute the value $c \leftarrow H$ (gpk, t, m,
B, J, K , T,W, V_1 , V_2 , R_1 , R_2 , R_3 , R_4 , R_5 , R_6 , R_7 , R_8 , R_9 , R_{10}).
3.14 Compute the following values in Z_p :
$s_{\rho 1} \leftarrow r_{\rho 1} + c\rho_1$, $s_{\rho 2} \leftarrow r_{\rho 2} + c\rho_2$, $s_{\rho 3} \leftarrow r_{\rho 3} +$
$c\rho_3$,
$s_{\rho 4} \leftarrow r_{\rho 4} + c\rho_4$,
$s_{\beta 1} \leftarrow r_{\beta 1} + c_{\beta 1}$, $s_{\beta 2} \leftarrow r_{\beta 2} + c_{\beta 2}$, $s_{\beta 3} \leftarrow r_{\beta 3} +$
$c_{\beta 3}$,

$s\beta 4 \leftarrow r\beta 4 + c\beta 4$, $s\beta 5 \leftarrow r\beta 5 + c\beta 5$, $s\beta 6 \leftarrow r\beta 6 +$
$c\beta 6$,
$s_x \leftarrow r_x + c_{xik}$, $s_f \leftarrow r_f + cf_i$, $s_t \leftarrow r_t + ct_k$. Finally, U_i outputs the signature for message
m and time t:
$\sigma \leftarrow$ (B, J, K , T, W, V_1 , V_2 , c, s_x , s_f , s_t ,

$s\rho 1$, $s\rho 2$, $s\rho 3$, $s\rho 4$, $s\beta 1$, $s\beta 2$, $s\beta 3$, $s\beta 4$, $s\beta 5$, $s\beta 6$
).

4) Verification Phase (Gp.Ver): Upon receiving the signature σ for message m and the signing time t, the verifier verifies the validity of the signature and ensures that it is not

generated by a revoked user. 1) Validity Check:
a) Compute $\{t_j\}_{j\varepsilon[1,l]} \leftarrow$ 0-ENC(t).

b) Compute $Y \leftarrow Q^{\prod l_{j=1}^{(z+t_j)}}$
c) Re-compute:

$$\begin{aligned}
\bar{R}_1 &\leftarrow B^{s_f} J^{-c}, \quad \bar{R}_2 \leftarrow B^{s_x} K^{-c}, \\
\bar{R}_3 &\leftarrow K^{s_{\rho_1}} B^{-s_{\beta_1}}, \\
\bar{R}_4 &\leftarrow e(h, g_2)^{-s_f} \cdot e(T, z_1)^{s_t} \cdot e(T, g_2)^{s_x} \cdot \\
&\quad e(\bar{h}, z_1)^{-s_{\beta_3}} \cdot e(\bar{h}, g_2)^{-s_{\beta_1}} \cdot \\
&\quad e(\bar{h}, z_2)^{-s_{\rho_1}} \cdot (e(T, z_2)/e(g_1, g_2))^{c} \\
\bar{R}_5 &\leftarrow \tilde{g}^{s_x} \bar{h}^{s_{\rho_3}} V_1^{-c}, \quad \bar{R}_6 \leftarrow \tilde{g}^{s_t} \bar{h}^{s_{\rho_4}} V_2^{-c}, \\
\bar{R}_7 &\leftarrow e(W, Q)^{s_t} \cdot e(\bar{h}, Q)^{-s_{\beta_5}} \cdot e(\bar{h}, Q^z)^{-s_{\rho_2}} \cdot \\
&\quad (e(W, Q^z)/e(Y, Q))^{c}, \\
\bar{R}_8 &\leftarrow \tilde{g}^{s_{\beta_1}} \bar{h}^{s_{\beta_3}} V_1^{-s_{\rho_1}}, \quad \bar{R}_9 \leftarrow \tilde{g}^{s_{\beta_3}} \bar{h}^{s_{\beta_4}} V_2^{-s_{\rho_1}}, \\
\bar{R}_{10} &\leftarrow \tilde{g}^{s_{\beta_5}} \bar{h}^{s_{\beta_6}} V_2^{-s_{\rho_2}}.
\end{aligned}$$

d) Check whether c = H (gpk, t, m, B, J, K ,
T, W, V_1 , V_2 , R_1 , R_2 , R_3 , R_4 , R_5 , R_6 , R_7 , R_8 , R_9 , R_{10}).

e) Output invalid if it is not equal, otherwise continue for revocation check.

2) Revocation Check: For each grt_i in the list RL,
a) Parse $(\tau_i , \{x_{ij}\}) \leftarrow grt_i$.
b) Compute $\{\tau_{ij}\}_{j\varepsilon[1,l]} \leftarrow 1\text{-ENC}(\tau_i)$ and $\{t_j\}_{j\varepsilon[1,l]} \leftarrow 0\text{-ENC}(t)$.

c) Find the single index $1 \leq k \leq l$ such that $\tau_{ik} = t_k$. If there exists k such that $K = B^{x_{ik}}$

holds, then we conclude this user has been revoked.

If the validity check is passed and the user is not revoked, it outputs valid. Otherwise, it outputs invalid.

5) Tracing Phase (Gp.Trace): The group manager can open a signature σ (on message m signed at time t) to trace the signer. For each grt_i (corresponding to user U_i) in the user

database, it does the following:
1) Parse $(\tau_i , \{x_{ij}\}) \leftarrow grt_i$.

2) Compute $\{\tau_{ij}\}_{j\varepsilon[1,l]} \leftarrow 1\text{-ENC}(\tau_i)$ and $\{t_j\}_{j\varepsilon[1,l]} \leftarrow 0\text{-ENC}(t)$.
3) Find the single index $1 \leq k \leq l$ such that
$\tau_{ik} = t_k$. If there exists k such that $K = B^{x_{ik}}$
holds, then we conclude this user U_i is the signer of the signature σ .

III. Roaming Protocol

The complete roaming protocol consists of our underlying group signature scheme and an adopted key exchange mechanism [7]. The protocol requires the following setup:

1) Each server is an independent group manager and generates its own master secret key msk and public parameter gpk from Gp.Kg. In addition, each server chooses a symmetric encryption scheme EN C = (Enc, Dec) andhas a signing/verification key pair (sk, pk) of a conventional digital signature scheme SIG = (Sig, Ver).

2) Assume that the public parameter of each server is publicly known to all other servers. We also assume that the description of the symmetric encryption EN C and the verification key pk (together with the verification mechanism Ver) of each server are publicly known to

all users within the network controlled by the server.

3) Let g be a generator in a cyclic group G with group order p. (g, G, p) is known to every entity.

4) Each server runs Gp.Join to issue user secret key gsk_i to its subscribed user U_i and keeps the revocation token grt_i secret.

5) At the beginning of each day, each server sends its revocation list RL to other servers.

Below the protocol of the connection between a single user with the foreign server is described. Many users can connect to the foreign server at the same time independently.

When user U_i (whose home server is H) is roaming at a foreign server V (who has a signing/verification key pair (sk_V , pk_V)), the following steps are carried out to authenticate each other and establish a session key:
1) U_i selects a random number $r_u \in Z_p$ and a

temporary pseudonym P D, and sends (H, P D, g^{ru}) to V.
2) V selects a random number $r_v \in Z_p$ and

computes $\sigma_V \leftarrow Sig_{skV}(m_V)$ where $m_V = V||H||P\ D||g^r{}_v\ ||g^r{}_u$. V sends (V, $g^{r}{}_v$, σ_V) to

U_i . V also computes $\kappa \leftarrow (g^{r}{}_u)^r{}_v$ and erases r_v from its memory.
3) When U_i receives (V, $g^{r}{}_v$, σ_V), he runs
$Ver_{pkV}(m_V , \sigma_V)$ to verify σ_V . If it returns invalid, U_i rejects the connection. Otherwise,
U_i generates a group signature

$\sigma_U \leftarrow Gp.Sign_{gski}(m_U)$ where $m_U = H||P\ D||V||g^{r}{}_u\ ||g^{r}{}_v$. U_i computes $\kappa' \leftarrow (g^{r}{}_v)^r{}_u$

and uses κ' as session key to encrypt σ_U as $\alpha \leftarrow Enc_{\kappa'}(\sigma_U)$. U_i sends α to V.
4) Upon receiving α, V uses κ to decrypt
and gets $\sigma_U \leftarrow Dec_{\kappa}(\alpha)$. It runs $Gp.Ver_{gpkU}$

(m_U , σ_U) to verify σ_U (which includes the revocation check implicitly). If it returns invalid, V rejects the connection. Otherwise, it uses κ as the session key and accepts the connection.

The interactive protocol is illustrated in Figure 1.The user expiry time information is embedded into gsk_i which is then used to generate σ_U . Thus σ_U also contains the information of the expiry time, yet to keep the size of σ_U as a constant. This is achieved by using a cryptographic technique called accumulator . By doing so, the expiry time is not needed to be sent to the Foreign Server V, and thus the size can be kept to O(1).

User revocation is trivial in our protocol, as it is already implicitly embedded in our underlying group signature scheme.

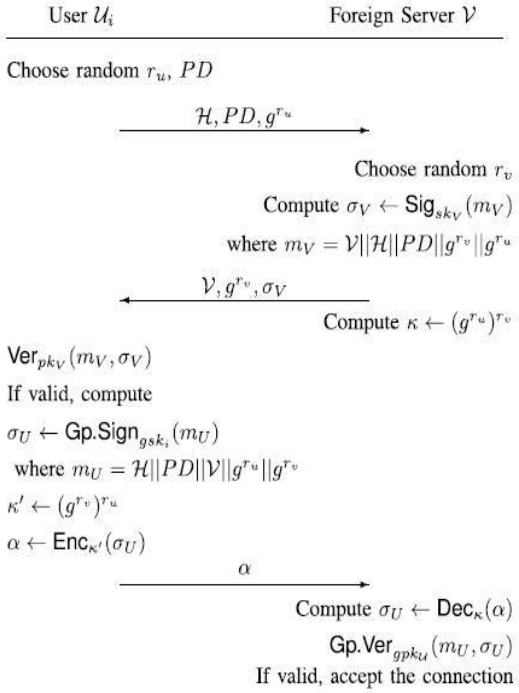

Figure 1: Complete Roaming Protocol

If user U_i is revoked by his home server, his revocation token grt_i is put into the revocation list RL which is uploaded to other servers each day. If U_i is roaming at a foreign network V, the group signature signed by U_i will not pass V‘s revocation check. secret key to sign (that is, the user is revoked naturally, or the subscription has been expired), although the user is not included in the revocation list, the validity check of the group signature verification will not pass.

Premature revocation of the user occurs when the user tries to access the websites in an unauthorized manner. The user will be notified by the foreign server about the unauthorized access and will be revoked. So a user cannot perform unauthorized actions while they are in the foreign domain.

IV. Analysis

Analysis of the proposed system is performed based on the computational time required for performing the revocation operation. The revocation of the user is performed base on the time stamp expiration. The time stamp is already embedded to the secret key once the user is registered. For each user , the time will be different. This is because the revocation procedure makes use of randomization for evaluation and for each user the time will be different. Some security requirements are also analyzed. The protocol ensures selfless anonymity, untraceability, subscription validation etc.. Digital signature is being produced through the group signature scheme where a member of a group can generate a valid signature. The identity of the user is kept anonymous so that the foreign server won't be able to trace them. Selfless-anonymity allows the signer of a signature to tell if the signature is signed by him/her. A group signature scheme is traceable if no polynomial-time adversary can forge a valid signature that can be improperly opened. A group signature scheme is exculpable if no polynomial-time adversary can forge a signature that is attributed to an honest member such that the member cannot dispute.

Figure 2: Computational time for revocation

V. Conclusion

An anonymous authentication roaming protocol that supports efficient revocation of naturally expired credentials is proposed. It relies on the group signature scheme which can bind the expiry time to the secret key of every user. With this new feature, expired keys are no longer needed to be included in the revocation list. This results in a significant efficiency improvement for revocation checking, due to the elimination of the expired keys in the revocation list.

References

[1]. Hyo Jin Jo,Jung Ha Paik, Dong Hoon Lee, ―Efficient Privacy-Preserving Authentication in Wireless Mobile Networks‖, IEEE Trans. Mobile Coputing,vol.13,no.7,July 2014.
[2]. Joseph K. Liu, Cheng-kang Chu, Sherman S. M. Chow, Xinyi Huang, Man Ho Au, Jianying Zhou ―Time-Bound Anonymous Authentication for Roaming Networks,‖ IEEE Trans. Information Forensics and Security,vol.10,no.1,January 2015.
[3]. D. He, J. Bu, S. Chan, C. Chen, and M. Yin, ―Privacy-preserving universal authentication protocol for wireless communications,‖ IEEE Trans. Wireless Commun., vol. 10, no. 2, pp. 431–436, Feb. 2011.
[4]. L. Chen and J. Li, ―VLR group signatures with indisputable exculpability and efficient revocation,‖ in Proc. IEEE 2nd Int. Conf. SocialCom, Aug. 2010, pp. 727–734.
[5]. M. H. Au, J. K. Liu, W. Susilo, and T. H. Yuen, ―Secure ID-based linkable and revocable-iff-linked ring signature with constant-size construction,‖ Theoretical Comput. Sci., vol. 469, pp. 1–14, Jan. 2013.
[6]. D. Boneh and H. Shacham, ―Group signatures with verifier-local revocation,‖ in Proc. 11th ACM Conf. CCS, 2004, pp. 168–177.
[7]. L. Chen, S.-L. Ng, and G. Wang, ―Threshold anonymous announcement in VANETs,‖ IEEE J. Sel. Areas Commun., vol. 29, no. 3, pp. 605–615, Mar. 2011.
[8]. S. S. M. Chow, W. Susilo, and T. H. Yuen, ―Escrowed linkability of ring signatures and its applications,‖ in Progress in Cryptology (Lecture Notes in Computer Science), vol. 4341. Berlin, Germany: Springer-Verlag, 2006, pp. 175–192.
[9]. B. Libert and D. Vergnaud, ―Group signatures with verifier-local revocation and backward unlinkability in the standard model,‖ in Cryptology and Network Security (Lecture Notes in Computer Science), vol. 5888. Berlin, Germany: Springer-Verlag, 2009, pp. 498–517.
[10]. D. Johnson, A. Menezes, and S. Vanstone, ―The elliptic curve digital signature algorithm (ECDSA),‖ Int. J. Inform. Security, vol. 1,no. 1, pp. 36–63, 2001.
[11]. T. Nakanishi and N. Funabiki, ―Verifier-local revocation group signature schemes with backward unlinkability from bilinear maps,‖ in Advances in Cryptology (Lecture Notes in Computer Science), vol. 3788. Berlin, Germany: Springer-Verlag, 2005, pp. 533–548.
[12]. K. Y. Yu, T. H. Yuen, S. S. M. Chow, . M. Yiu, and L. C. K. Hui, ―PE(AR) 2 : Privacy-enhanced anonymous authentication with reputation and revocation,‖ in Computer Security (Lecture Notes in Computer Science), vol. 7459. Berlin, Germany: Springer-Verlag, 2012 pp. 679–696.
[13]. D. Boneh and H. Shacham, ―Group signatures with verifier-local revocation,‖ in Proc. 11th ACM Conf. CCS, 2004, pp. 168– 177.
[14]. D.Chaum and E. van Heyst,‖Group Signatures‖, in Advances in Cryptology(Lecture Notes in Computer Science),vol.547.Berlin,Germany:Springer-Verlag,1991.pp. 215-220.
[15]. J. Bringer and A. Patey, ―VLR group signatures—How to achieve both backward unlinkability and efficient revocation checks,‖ in Proc. SECRYPT, 2012, pp. 215–220.