CPAL: A Conditional Privacy-Preserving Authentication With Access Linkability for Roaming Service

Chengzhe Lai, *Student Member*, *IEEE*, Hui Li, *Member*, *IEEE*, Xiaohui Liang, *Member*, *IEEE*, Rongxing Lu, *Member*, *IEEE*, Kuan Zhang, *Student Member*, *IEEE*, and Xuemin Shen, *Fellow*, *IEEE*

***Abstract*—The roaming service enables mobile subscribers to access the internet service anytime and anywhere, which can fulfill the requirement of ubiquitous access for the emerging paradigm of networking, e.g., the Internet of Things (IoT). In this paper, we propose a conditional privacy-preserving authentication with access linkability (CPAL) for roaming service, to provide universal secure roaming service and multilevel privacy preservation. CPAL provides an anonymous user linking function by utilizing a novel group signature technique, which can not only efficiently hide users' identities but also enables the authorized entities to link all the access information of the same user without knowing the user's real identity. Specifically, by using the master linking key possessed by the trust linking server, the authorized foreign network operators or service providers can link the access information from the user to improve its service, while preserving user anonymity, e.g., using individual access information to analyze user preferences without revealing user's identity. Furthermore, the subscribers can also use this functionality to anonymously query their usage of service. In addition, CPAL has an efficient revocation function, which revokes a group of users at the same time. Through extensive analysis, we demonstrate that CPAL resists various security threats and provides more flexible privacy preservation compared to the existing schemes. Meanwhile, performance evaluations demonstrate its efficiency in terms of communication and computation overhead.**

***Index Terms*—Anonymous user linkability, authentication, Internet of Things (IoT), privacy preservation, roaming, security.**

I. Introduction

With the advancements in various mobile and wireless networks, e.g., long-term evolution (LTE) [1], worldwide interoperability for microwave access (WiMAX) [2], and roadside-to-vehicle communication systems [3], [4], pervasive Internet access becomes a reality, enabling mobile subscribers (MSs) to enjoy Internet service anytime and anywhere [5]–[8]. This also caters to the demand of ubiquitous access for the emerging paradigm of networking, e.g., the Internet of Things (IoT) [9]–[13], which is rapidly gaining ground in the scenario of wireless telecommunications. Due to the complementary nature of the existing networks, interworking among them is attractive [14]–[17]. However, within the heterogeneous networks, ensuring the secure and efficient roaming service is still challenging [18], [19], because different networks have different security policies and authentication protocols. Consequently, any secure roaming scheme dedicated for only one type of network technology cannot fulfill the security requirements from the heterogeneous networks.

In heterogeneous networks, user privacy preservation has become an important and challenging issue in the roaming service, and has been widely studied by researchers. In most existing secure roaming schemes, the privacy preservation only equates with anonymity, i.e., hiding users' identities. However, this may not be suitable for diverse privacy requirements in real world [4], [20]–[23]. There are a variety of personalized services associated with privacy in the real applications; therefore, according to different privacy preservation requirements, the privacy preservation should be flexibly or elaborately controlled according to a desired level. To this end, foreign network (FN) operators or service providers may need individual access information on the usage of services, while preserving anonymity. This means that FN operators or service providers can link all the access information of the same user for statistical purposes, but they cannot know who the user is, what the current membership status of the user is, and the history of the user joining and revocation. Meanwhile, a user may want to provide a specific network operator or service provider with linking capability, and remain unlinkable to others. Moreover, there may be a large number of mobile users that need to be revoked in the network anytime due to various reasons, e.g., when any illegal or exceptional events occur. However, the existing secure roaming schemes [24], [25] do not support this function. This will significantly increase the burden of the home authentication server and potentially reduce the efficiency of the whole network. Therefore, efficient user revocation for dynamic membership in the secure roaming services is important.

Manuscript received October 31, 2013; revised December 21, 2013; accepted February 04, 2014. Date of publication February 17, 2014; date of current version May 05, 2014. This work was supported in part by China Scholarship Council, in part by the National Natural Science Foundation of China under Grants 61272457, 61102056, and 61303216, in part by the China Postdoctoral Science Foundation funded project (no. 2013M542328), and in part by the research Grant from the Natural Science and Engineering Research Council (NSERC), Canada.

C. Lai and H. Li are with the State Key Laboratory of Integrated Services Networks, Xidian University, Xi'an 710071, China (e-mail: lcz.xidian@gmail.com; lihui@mail.xidian.edu.cn).

X. Liang is with the Department of Computer Science, Dartmouth College, Hanover, NH 03755 USA (e-mail: xiaohui.liang@dartmouth.edu).

R. Lu is with the Division of Communication Engineering, School of Electrical and Electronics Engineering, Nanyang Technological University, Singapore (e-mail: rxlu@ntu.edu.sg).

K. Zhang and X. Shen are with the Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, ON N2L 3G1, Canada (e-mail: k52zhang@uwaterloo.ca; sshen@uwaterloo.ca).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/JIOT.2014.2306673

In this paper, to provide universal secure roaming service and anonymous user linkability, we propose a *c*onditional *p*rivacy-preserving authentication with *a*ccess *l*inkability (CPAL) for roaming service by utilizing the novel group signature technique [26]. In the proposed CPAL, the strong anonymous authentication, session key agreement, user tracking, and anonymous user linking are provided, which make the privacy preservation more flexible. Meanwhile, CPAL has the efficient revocation function for dynamic membership, where a group of users can be revoked simultaneously. The main contributions of this paper are threefold.

1) First, we present a generic secure roaming architecture, which implements new features to achieve the corresponding security goals. Meanwhile, to fulfill different privacy preservation requirements, we introduce the multilevel privacy preservation. Especially, the privacy-preservation ability is divided into three levels, i.e., authentication, anonymity, and authorized anonymous user linking (AAUL).
2) Second, we further propose a conditional privacy-preserving authentication with access linkability for roaming service, called CPAL. The proposed CPAL scheme can not only achieve session key agreement, strong anonymous authentication, and fast user tracking (Levels 1 and 2) but also provide anonymous user linkability (Level 3). Moreover, CPAL supports efficient joining and revocation functions for dynamic membership. Particularly, it can revoke a group of users simultaneously, which makes the user revocation more efficient.
3) Third, we analyze the security strength and privacy-preservation ability of CPAL. In addition, through comparative performance analysis, we demonstrate that CPAL is efficient in terms of the communication and computation overhead.

The remainder of this paper is organized as follows. In Section II, we discuss the related work. In Section III, we introduce the network architecture and design goals. In Section IV, we recall the bilinear pairings and a hybrid linear combination encryption (HLCE). Then, we present our CPAL and discuss some applications related to CPAL in Section V, followed by its security analysis and performance evaluation in Sections VI and VII, respectively. Finally, we draw our conclusions in Section VIII.

II. Related Work

The existing secure roaming schemes can mainly be classified into three categories: symmetric-cryptosystem-based (SC-based), asymmetric-cryptosystem-based (AC-based), and hybrid schemes.

The SC-based secure roaming schemes, e.g., EAP-based authentication and key agreement protocols [5], [27]–[31], are designed based on standard protocols [32], [33]. SC-based schemes are widely accepted because they are compatible with standard protocols. However, they require the interaction between the foreign server and the home server, which may lead to the single point of failure [34], and induce large authentication transmission overhead because of the long distance between the foreign server and the home server. Moreover, recent studies [35], [36] have shown that SC-based schemes cannot provide strong user anonymity and nontraceability, and most of them cannot provide session key security and resistance to sophisticated attacks. Another weakness is that, they cannot flexibly be applied to all application scenarios because each protocol is only suitable for the corresponding network architecture, this may increase the complexity of the entire system.

Jiang and Shi [37], [38] propose several mutual authentication and key exchange schemes for roaming services. In [37] and [38], public key cryptography, e.g., digital signature and Diffie–Hellman key exchange, is adopted on the basis of SC-based schemes, which can further enhance the security of roaming service. However, they still induce large authentication transmission overhead due to the interaction between the foreign server and the home server. More importantly, their schemes cannot provide strong privacy preservation.

The limitations of SC-based schemes have greatly stimulated the research of AC-based schemes [24], [25], [39]–[42], because AC-based schemes can provide more security, stronger privacy preservation, and require fewer communication rounds. These advantages have led to the recent increasing popularity of the AC-based secure roaming schemes. One of the important security properties in the AC-based secure roaming schemes is strong user anonymity, which includes user anonymity and user untraceablility. The former means that except for the home server, the user's identity cannot be revealed to anyone else including the foreign server; the latter means that except for the home server, any past or future protocol runs of the same user cannot be linked by anyone including the foreign server [24].

AC-based secure roaming schemes have been studied by many researchers. In this section, we briefly discuss some research works closely related to CPAL. In [24], Yang *et al.* propose a universal authentication protocols for anonymous wireless communications. In their scheme, two levels of user anonymity in roaming are considered: 1) *Weak User Anonymity* that concerns about user anonymity against eavesdroppers and 2) *Strong User Anonymity* that concerns about user anonymity against both eavesdroppers and foreign servers. Accordingly, they present two protocols to achieve weak user anonymity and strong user anonymity, respectively. However, He *et al.* [25] find that scheme [24] cannot satisfy user untraceablility. Therefore, they propose a privacy-preserving universal authentication protocol for wireless communications. They point that a privacy-preserving user authentication scheme should satisfy the following requirements: *server authentication*, *subscription validation*, *provision of user revocation function*, *key establishment*, *user anonymity,* and *untraceablility*.

However, the existing privacy-preserving authentication schemes for roaming service cannot provide anonymous user linkability that makes the authorized entities, e.g., FN operators or service providers, have the ability to anonymously link the access information from the user for statistical purposes. This may not be enough for diverse applications in the roaming service.

III. Network Architecture and Design Goals

In this section, we present the generic security roaming network architecture, and identify our design goals.

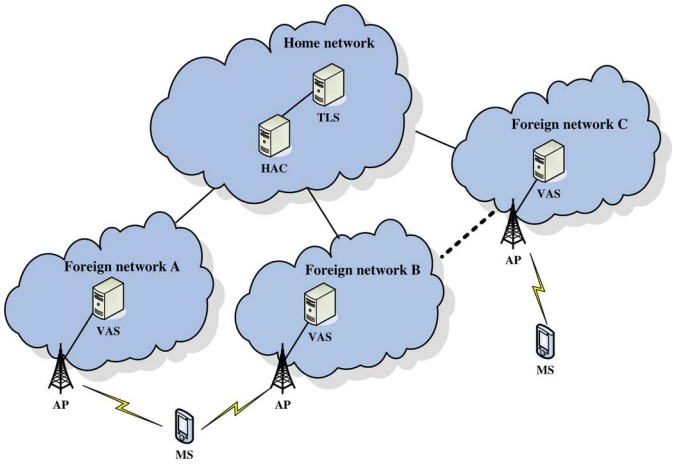

Fig. 1. Generic secure roaming network architecture.

A. Network Architecture

Fig. 1 depicts a generic secure roaming network architecture with emphasis on the interconnections among the home authentication center (HAC), the trust linking server (TLS), and the visiting authentication server (VAS). The HAC and the TLS are located in home network (HN), and the VAS is located in FN.

A MS can access the FN through the access point (AP), e.g., E-UTRAN eNB, WiMAX BS, and IEEE 802.11b AP. For an MS, there exist only one HN and multiple FNs. The HAC's responsibility is that issuing the secret signing key for new joining MSs and opening a signature and generating a proof to reveal the corresponding MS when dispute occurs. The TLS is in charge of discerning whether those signatures are from the same MS without knowing MS's identity. The VAS is responsible for performing access authentication for the MSs accessing the FN.

B. Design Goals

Our design goal in this paper is to develop a CPAL for roaming service. Especially, the following goals should be achieved:

1) Strong Anonymous Access Authentication: First, the proposed scheme should provide strong anonymous access authentication. Specifically, it requires that authentication messages, which are interacted by the MS and the VAS, have not been altered during the transmission, i.e., if the adversary $\mathcal{A}$ forges and/or modifies the authentication messages, the malicious operations should be detected. Meanwhile, the identity of the MS cannot be revealed to adversary $\mathcal{A}$ or the VAS.

2) User Tracking on a Disputed Access Request: An important and challenging issue for roaming service with efficient privacy preservation is to maintain traceability for all the access messages in the presence of the anonymous access authentication. Without the tracking function, the above anonymous access authentication can only prevent an outside attack, but cannot deal with an inside one. For instance, an inside attacker could launch a Denial of Service (DoS) attack or impersonation attack, provided with no traceability by the HAC. In a DoS attack, the adversary sends a large number of fake access messages to jam the channel or to consume the rare computation resources of the VAC; while in an impersonation attack, the adversary actively pretends to be another MS to send false access request messages.

3) Anonymous User Linking: In order to provide CPAL, i.e., anonymity can be flexibly or elaborately controlled according to the corresponding requirements, the network operators or service providers that are authorized by the HAC or MS can acquire MS's statistics on the usage of services, while MS's identity will not be revealed.

4) Efficient User Revocation for Dynamic Membership: Due to some reasons (e.g., the subscription period of a user has expired or a user's secret key has been compromised), an efficient user revocation function should be proposed, especially for dynamic membership. That means the user revocation function can revoke a group of users simultaneously, which makes the whole scheme more flexible and efficient.

Meanwhile, CPAL can provide a universal secure roaming service. That means the proposed CPAL and its signaling flows can be used in any roaming scenario regardless of the type of networks that the MS is visiting. Moreover, the proposed CPAL scheme should meet all security requirements in previous schemes.

IV. Preliminaries

In this section, we outline the bilinear pairing technique, and introduce the HLCE, which will serve as the basis of the proposed CPAL scheme.

A. Bilinear Maps

Let $\mathbb{G}_1$, $\mathbb{G}_2$, and $\mathbb{G}_T$ be multiplicative groups of prime order p. The bilinear map e: $\mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_T$ has the following properties:

1) Bilinearity: $\forall g_1 \in \mathbb{G}_1$, $\forall g_2 \in \mathbb{G}_2$, and $\forall a, b \in \mathbb{Z}_p^*$, $e({g_1}^a, {g_1}^b) = e(g_1, g_2)^{ab}$;
2) Nondegenerate: $\exists g_1, g_2$, such that $e(g_1, g_2)$ has order p, i.e., $e(g_1, g_2)$ is a generator of $\mathbb{G}_T$;
3) Computable: There is an efficient algorithm to compute $e(g_1, g_2)$,for any $g_1 \in \mathbb{G}_1$ and $g_2 \in \mathbb{G}_2$.

Definition 1: A bilinear parameter generator $\mathcal{G}en$ is a probabilistic algorithm that takes a security parameter λ as input, and outputs a 5-tuple $(p, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e)$ where p is λ-bit prime number; $\mathbb{G}_1$, $\mathbb{G}_2$, and $\mathbb{G}_T$ are three groups with the same order p; and e: $\mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_T$ is a nondegenerated and efficiently computable bilinear map.

B. Hybrid Linear Combination Encryption

In [26], Hwang *et al.* introduce an HLCE scheme that is used for constructing their novel group signature algorithm, which is described as follows:

1) **KeyGen:** It chooses $u, v \in_R \mathbb{G}_1, x_1, y_1, x_2, y_2 \in_R \mathbb{G}_2$, and then computes the public key $\mathrm{pk} = (u, v, w_1 = u^{x_1}, w_2 = v^{y_1}, d_1 = u^{x_2}, d_2 = v^{y_2})$ and outputs its corresponding secret key $\mathrm{sk} = x_1, y_1, x_2, y_2$.
2) **Enc:** Given the public key pk and a message $M = (M_1, M_2) \in \mathbb{G}_1 \times \mathbb{G}_1$, it chooses $a, b \in_R \mathbb{Z}_p^*$. Then, it computes a ciphertext $c = (D_1 = u^a,\ D_2 = v^b,\ D_3 = M_1 w_1^a w_2^b,\ D_4 = M_2 d_1^a d_2^b)$.

3) **Dec:** Given the ciphertext $c = (D_1, D_2, D_3, D_4)$, it computes the plaintext $M = (M_1, M_2)$ as follows: $M_1 = D_3(D_1^{x_1} D_2^{y_1})^{-1}$ and $M_2 = D_4(D_1^{x_2} D_2^{y_2})^{-1}$.

V. The Proposed CPAL Scheme

In this section, we describe our proposed CPAL scheme, which consists of five parts, System Initialization, Roaming, User Tracking Algorithm, Anonymous User Linking, and User Revocation. The notations used in the scheme are defined in Table I.

A. System Initialization

Given the security parameter λ, the HAC first generates the bilinear parameters $(p, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e)$ by running $\mathcal{G}en(\lambda)$. Then, the HAC chooses $g_1, g_2, g_3, g, u, v \in_R \mathbb{G}_1$, $r_1 \in_R \mathbb{G}_2$, and $\eta_1, \eta_2, \varepsilon_1, \varepsilon_1, \theta \in \mathbb{Z}_p^*$. Next, it computes $w_1 = u^{\eta_1}$, $w_2 = v^{\eta_2}$, $d_1 = u^{\varepsilon_1}$, $d_2 = v^{\varepsilon_2}$, $U = {r_1}^{\varepsilon_1}$, $V = {r_1}^{\varepsilon_2}$, and $r_\theta = {r_1}^{\theta}$. The HAC also chooses a cryptographic hash function H, where H: $\{0,1\}^* \rightarrow \mathbb{Z}_p^*$. After that, the home domain public key HDPK will be published as:

$$\mathrm{HDPK} = \left\{ \begin{matrix} \mathbb{G}_1, \mathbb{G}_2, e, g, r_1, r_\theta, u, v \\ w_1, w_2, d_1, d_2, H, g_1, g_2, g_3 \end{matrix} \right\} \tag{1}$$

where g_1, g_2, and g_3 will be updated once user revocation occurs.

Then, the HAC generates the master issuing key $\mathrm{mk}_I = \theta$, the master opening key $\mathrm{mk}_O = (\eta_1, \eta_2, \varepsilon_1, \varepsilon_1)$, and the master linking key $\mathrm{mk}_L = (U, V)$, respectively.

When an MS submits its identity ID_i for registering itself to the HN, the following procedures are performed:

Step 1) The MS with ID_i makes use of a standard signature technique to generate a signing key $\mathrm{SK}_{\mathrm{ID}_i}$ and the corresponding public verification key $\mathrm{VK}_{\mathrm{ID}_i}$.

Step 2) The MS with ID_i chooses $z_i \in_R \mathbb{Z}_p^*$, and then computes $\mathrm{upk}_{\mathrm{ID}_i} = g_3^{z_i} = Z_i \in \mathbb{G}_1$ and $\sigma_{1,i} = \mathrm{Sign}_{\mathrm{SK}_{\mathrm{ID}_i}}(\mathrm{Register\_Req}, \mathrm{ID}_i, \mathrm{upk}_{\mathrm{ID}_i})$. Next, the MS sends $(\mathrm{Register\_Req}, \mathrm{ID}_i, \mathrm{upk}_{\mathrm{ID}_i}, \sigma_{1,i})$ to the HAC.

Step 3) The HAC first verifies $\sigma_{1,i}$ using $\mathrm{VK}_{\mathrm{ID}_i}$. If $\sigma_{1,i}$ is valid, the HAC chooses $x_i, y_i \in_R \mathbb{Z}_p^*$, and then computes $Y_{1,i} = g_2^{y_i}$, $X_{2,i} = r_1^{x_i}$, and $S_i = (g_1 g_2^{-y_i} Z_i^{-1})^{\frac{1}{\theta + x_i}} \in \mathbb{G}_1$.[1] Next, the HAC sends $(S_i, Y_{1,i}, X_{2,i})$ to MS ID_i.

Step 4) Upon receipt of $(S_i, Y_{1,i}, X_{2,i})$, MS ID_i checks if $S_i \in \mathbb{G}_1$ and $e(S_i, X_{2,i} r_\theta) = e(g_1 Y_{1,i}^{-1} g_3^{-z_i}, r_1)$. If verification is successful, MS ID_i accepts the S_i and generates a signature $\sigma_{2,i} = \mathrm{Sign}_{\mathrm{SK}_{\mathrm{ID}_i}}(S_i, Y_{1,i}, X_{2,i}, \mathrm{upk}_{\mathrm{ID}_i})$ and sends $\sigma_{2,i}$ to the HAC.

Step 5) The HAC verifies if $\sigma_{2,i}$ is valid, and then sends (x_i, y_i) to MS ID_i; then MS ID_i generates its user signing key as

$$\begin{aligned} \mathrm{usk}_{\mathrm{ID}_i} = (S_i^{\mathrm{cur}} = (g_1' g_2'^{-y_i} g_3'^{-z_i})^{\frac{1}{\theta + x_i}}, x_i, y_i, z_i, \\ S_i^{\mathrm{ini}} = (g_1 g_2^{-y_i} g_3^{-z_i})^{\frac{1}{\theta + x_i}}) \end{aligned} \tag{2}$$

where S_i^{cur}[2] corresponds to the current home domain public key HDPK, and S_i^{ini} corresponds to the initial home domain public key HDPK_0 and will be used to update the S_i^{cur} when a revocation event occurs.

Step 6) MS ID_i generates the signature $\sigma_{\mathrm{Judge},i} = \mathrm{Sign}_{\mathrm{SK}_{\mathrm{ID}_i}}(\mathrm{upk}_{\mathrm{ID}_i}, Y_{1,i} = g_2^{y_i}, Y_{2,i} = r_1^{y_i}, X_{1,i} = g^{x_i}, X_{2,i} = r_1^{x_i})$, and sends $\sigma_{\mathrm{Judge},i}$ and $(\mathrm{upk}_i, Y_{2,i}, X_{1,i})$ to the HAC.

Step 7) After receiving the message from MS ID_i, the HAC verifies if $e(X_{1,i}, r_1) = e(g, X_{2,i})$, $e(Y_{1,i}, r_1) = e(g_2, Y_{2,i})$. If verification passes, the HAC appends $(H(g^{y_i}), ID_i, y_i, S_i, \mathrm{upk}_{\mathrm{ID}_i}, Y_{1,i}, Y_{2,i}, X_{1,i}, X_{2,i}, \sigma_{\mathrm{Judge},i})$ to the registration list *RegList* (Fig. 2) that is built by the HAC.

TABLE I
Definition of Notations in the Scheme

Notation	Definition
HN	home network
FN	foreign network
HAC	the home authentication center
TLS	the trust linking server
VAS	the visiting authentication server
MS	mobile subscriber
HDPK	home domain public key
HDPK_0	the initial home domain public key
mk_I	the master issuing key
mk_O	the master opening key
mk_L	the master linking key
ID_i	the identity of the MS i
SK_x	signing key of x
VK_x	public verification key of x
$\mathrm{upk}_{\mathrm{ID}_i}$	user public key of MS ID_i
$\mathrm{usk}_{\mathrm{ID}_i}$	user signing key of MS ID_i
sk	session key between the MS and the VAS

B. Roaming

In this phase, when MS ID_i roams from the HN to an FN, the mutual authentication between MS ID_i and the VAS should be accomplished before the MS accesses the FN. Note that the HN and the FNs have established cooperative relations through the roaming agreements, which make the MSs registered in the HN access the FN and obtain the service provided by the FN during roaming. Therefore, the HDPK and related information of HN have been transmitted to the FN in advance. Meanwhile, the VAS makes use of a standard signature technique to generate a signing key $\mathrm{SK}_{\mathrm{VAS}}$ and the corresponding public verification key $\mathrm{VK}_{\mathrm{VAS}}$. Fig. 3 shows the access authentication between the MS and the VAS during roaming, and the detailed steps are described as follows.

Step 1) MS ID_i sends access request to the VAS; the VAS chooses a random number $b \in_R \mathbb{Z}_p^*$ and computes g^b, and then sends g^b to the MS.

Step 2) Upon receipt of g^b, MS ID_i first chooses a random number $a \in_R \mathbb{Z}_p^*$, and computes g^a and $(g^b)^a$; then it generates its authentication message $M = (\mathrm{HomedomainName} \| \mathrm{ServiceReq} \| g^a \| \mathrm{timestamp})$ and proceeds as follows: MS ID_i chooses $\alpha, \beta \in_R \mathbb{Z}_p^*$, and computes $X_1 = u^\alpha$, $X_1 = v^\beta$, $X_3 = S_i^{\mathrm{cur}} w_1^\alpha w_2^\beta$, $X_4 = g^{y_i} d_1^\alpha d_2^\beta$, and $\gamma = x_i \alpha \bmod p$, $\delta = x_i \beta \bmod p$.

[1] If there is no revocation event, then S_i remains unchanged.

[2] If there is no update, then $S_i^{cur} = S_i^{ini}$.

Index number	User authentication information
i	$(H(g^{y_i}), ID_i, y_i, S_i, upk_{ID_i}, Y_{1,i}, Y_{2,i}, X_{1,i}, X_{2,i}, \sigma_{Jugde,i})$

Fig. 2. Registration list of MS ID_i.

Step 3) MS ID_i also picks $r_\alpha, r_\beta, r_\gamma, r_\delta, r_x, r_y, r_z \in_R \mathbb{Z}_p^*$, and computes

$$\begin{cases} Y_1 = u^{r_\alpha}, Y_2 = v^{r_\beta} \\ Y_3 = e(X_3, r_1)^{r_x} e(w_1, r_\theta)^{-r_\alpha} e(w_2, r_\theta)^{-r_\beta} e(w_1, r_1)^{-r_\gamma} \\ \quad e(w_2, r_1)^{-r_\delta} e(g_2, r_1)^{r_y} e(g_3, r_1)^{r_z} \\ Y_4 = g^{r_y} d_1^{r_\alpha} d_2^{r_\beta}, Y_5 = X_1^{r_x} u^{-r_\gamma}, Y_6 = X_2^{r_x} v^{-r_\delta}. \end{cases} \tag{3}$$

Step 4) In order to generate a signature of M, MS ID_i computes $h = H(M, X_1, \ldots, X_4, Y_1, \ldots, Y_6, g^b, g^{ab})$, and $s_\alpha = r_\alpha + h\alpha$, $s_\beta = r_\beta + h\beta$, $s_\gamma = r_\gamma + h\gamma$, $s_\delta = r_\delta + h\delta$, $s_x = r_x + hx_i$, $s_y = r_y + hy_i$, $s_z = r_z + hz_i \mod p$. Finally, MS ID_i generates the signature $\sigma = (X_1, X_2, X_3, X_4, h, s_\alpha, s_\beta, s_\gamma, s_\delta, s_x, s_y, s_z)$, and then sends M together with σ to the VAS.

Step 5) Upon receiving the M and σ from MS ID_i, the VAS first generates session key $\mathrm{sk} = (g^a)^b$ between MS ID_i and the FN, and then computes

$$\begin{cases} Y_1' = u^{s_\alpha} X_1^{-h}, Y_2' = v^{s_\beta} X_2^{-h} \\ Y_3' = e(X_3, r_1)^{s_x} e(w_1{}^{-s_\alpha} w_2{}^{-s_\beta}, r_\theta) e(w_1{}^{-s_\gamma} w_2{}^{-s_\delta}, r_1) \\ e(g_2, r_1)^{s_y} e(g_3, r_1)^{s_z} (e(X_3, r_\theta)/e(g_1, r_1))^h \\ Y_4' = g^{s_y} d_1^{s_\alpha} d_2^{s_\beta} X_4^{-h}, Y_5' = X_1^{s_x} u^{-s_\gamma}, Y_6' = X_2^{s_x} v^{-s_\delta}. \end{cases} \tag{4}$$

Then, the VAS checks if

$$h \stackrel{?}{=} H(M, X_1, X_2, X_3, X_4, Y_1', Y_2', Y_3', Y_4', Y_5', Y_6', g^b, g^{ab}). \tag{5}$$

If verification is successful, the VAS accepts session key $\mathrm{sk} = (g^a)^b$ between MS ID_i and the FN for subsequent communication.

Step 6) After that, the VAS computes a signature $\sigma_{\mathrm{VAS}} = \mathrm{Sign}_{\mathrm{SK_{VAS}}}(\mathrm{FN\_Name} \| g^a \| g^b \| g^{ab})$, and sends σ_{VAS} back to MS ID_i.

Step 7) MS ID_i verifies the σ_{VAS} by using $\mathrm{VK_{VAS}}$. If verification is successful, it accepts the sk, and can access the FN successfully.

C. User Tracking Algorithm

Once a dispute occurs on an access request during roaming, the CPAL is equipped with an algorithm for tracking the corresponding user of the disputed access request message. If a grievant (e.g., an FN), denoted as JUDGE, raises doubts about one access request, it will ask the HAC to track the MS's identity related to the disputed access request message. The detailed steps are as follows.

Step 1) The HAC first recovers $g^{y'}$ as $g^{y'} = X_4 (X_1^{\varepsilon_1} X_2^{\varepsilon_2})^{-1}$ from the signature of the disputed access request message. By using a binary search on the *RegList*, the HAC finds the y_i corresponding to ID_i such that $H(g^{y'}) = H(g^{y_i})$ in the *RegList*. If they match, the HAC retrieves corresponding $\mathrm{upk_{ID_i}}$, $Y_{1,i}$, $Y_{2,i}$, $X_{1,i}$, and $X_{2,i}$.

Step 2) The HAC chooses $\varsigma_1, \varsigma_2 \in_R \mathbb{Z}_p^*$, and then computes $K_{12} = X_1^{\eta_1} X_2^{\eta_2}$, $W_1 = u^{\varsigma_1}$, $W_2 = v^{\varsigma_2}$, $W_{12} = X_1^{\varsigma_1} X_2^{\varsigma_2}$, $h_{12} = H(\sigma, u, v, K_{12}, W_1, W_2, W_{12})$, and $s_1 = \varsigma_1 + h_{12}\eta_1 \mod p$, $s_1 = \varsigma_2 + h_{12}\eta_2 \mod p$. After that, the HAC generates a *proof* $(\mathrm{ID}_i, (\mathrm{P} = K_{12}, h_{12}, s_1, s_2))$, and then sends the *proof* together with $\sigma_{\mathrm{Judge},i}$, $\mathrm{upk_{ID_i}}$, $Y_{1,i}$, $Y_{2,i}$, $X_{1,i}$, and $X_{2,i}$ to JUDGE.

Step 3) JUDGE first verifies $\sigma_{\mathrm{Judge},i}$, if it is valid, let $r_1' = r_1^{\log_{g_1}^{g_1'}}$, where g_1' is an updated value of g_1 (if there is no upgrade, then $g_1' = g_1$).

Step 4) JUDGE checks if the following equalities hold:

$$\begin{cases} h_{12} \stackrel{?}{=} h(\sigma, u, v, K_{12}, u^{s_1} w_1^{-h_{12}}, v^{s_2} w_2^{-h_{12}}, X_1^{s_1} X_2^{s_2} K_{12}^{-h_{12}}) \\ e(X_3 (K_{12})^{-1}, X_{2,i} r_\theta) \stackrel{?}{=} e(g_1 Y_{1,i}^{-1} Z_i^{-1}, r') \end{cases} \tag{6}$$

where g, g_2, r_1, and r_θ are in the initial home domain public key $\mathrm{HDPK_0}$. If these two equalities hold, it proves that MS ID_i has ever accessed the FN and requested the corresponding services, and it cannot repudiate that.

D. Anonymous User Linking

The network operators or service providers that are authorized by the HAC or MS ID_i, denoted as AUTLINKER, may need user's statistics on the usage of services.

First, the HAC sends the master linking key $\mathrm{mk}_L = (U, V)$ to the appointed AUTLINKER. Assume that the AUTLINKER has collected some of signatures and the corresponding messages in the previous access of MS ID_i, e.g., two pairs of signatures and messages, (σ', M) and (σ', M'). The AUTLINKER first checks if the signatures are valid. If so, using mk_L, it computes

$$\begin{cases} \Omega_1 = e(X_4, r_1)(e(X_1, U) e(X_2, V))^{-1} \\ \Omega_2 = e(X_4', r_1)(e(X_1', U) e(X_2', V))^{-1}. \end{cases} \tag{7}$$

If $\Omega_1 = \Omega_2$, it manifests that these signatures and the corresponding messages generated by the same MS registered in the HN, while MS's identity will not be revealed.

E. User Revocation

User revocation can be executed when any illegal or exceptional events occur, e.g., MS's secret key has been compromised, and the punishment for defaulting MS. In our CPAL, the user revocation is realized by implementing two key update algorithms, i.e., `HDPK_Update` and `usk_Update`.

First of all, a revocation event counter C is defined, which is increased by 1 when a new revocation event occurs. If a set of keys need to be revoked for one revocation event, let the initial home domain public key be

$$\mathrm{HDPK_0} = \left\{ \begin{matrix} \mathbb{G}_1,\ \mathbb{G}_2,\ e,\ g,\ r_1,\ r_\theta,\ u,\ v \\ w_1,\ w_2,\ d_1,\ d_2,\ H,\ g_1,\ g_2,\ g_3 \end{matrix} \right\}.$$

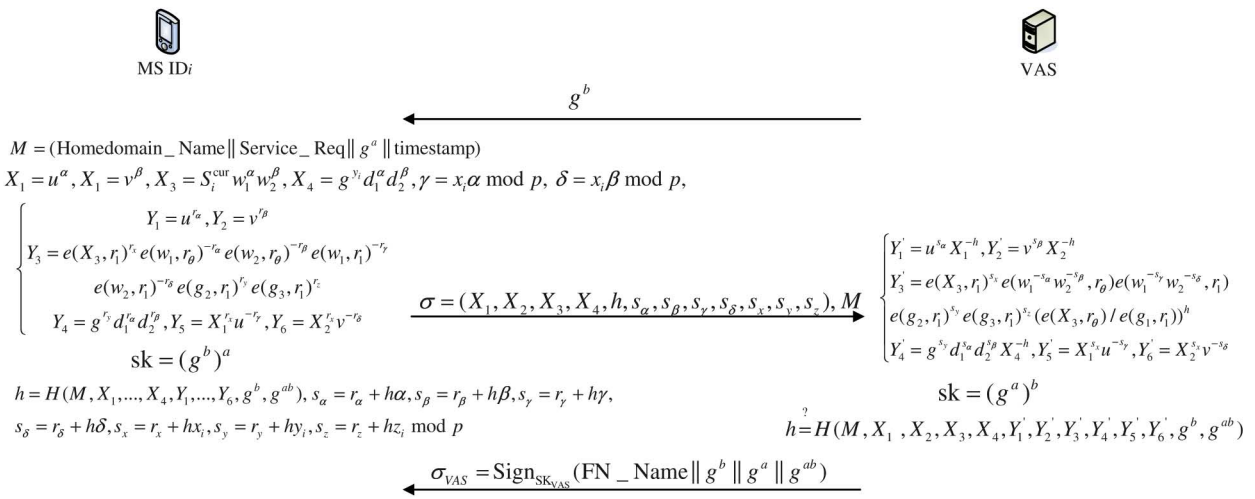

Fig. 3. Access authentication between the MS and the VAS during roaming.

The HDPK_0 can be further expressed as

$$\text{HDPK}_0 = (\Delta,\ g_1,\ g_2,\ g_3)$$

where $\Delta = (\mathbb{G}_1,\ \mathbb{G}_2,\ e,\ g,\ r_1,\ r_\theta,\ u,\ v,\ w_1,\ w_2,\ d_1,\ d_2,\ H)$, and Δ does not change regardless of revocation.

Let the current home domain public key be

$$\text{HDPK}_{C-1} = (\Delta,\ g_1',\ g_2',\ g_3').$$

Meanwhile, assume that there are κ MSs, which correspond to κ keys to be revoked, and then the user revocation list *user revocation list (URL)* is formed as

$$\text{URL} = \Big\{P_{1,n} = g_1^{\frac{1}{\theta + x_{C,n}}},\ P_{2,n} = g_2^{\frac{1}{\theta + x_{C,n}}},\ P_{3,n} = g_3^{\frac{1}{\theta + x_{C,n}}},\ x_{C,n} | n = 1, \ldots, \kappa_C\Big\}$$

Then, `HDPK_Update` and `usk_Update` are executed as follows:

1) `HDPK_Update` is used to update an HDPK. To update the current HDPK_{C-1} to the latest HDPK_C, `HDPK_Update` works as follows:

   As mentioned before, in order to update HDPK, we only need to update g_1, g_2, g_3. Therefore, the HAC computes

$$\begin{cases} g_1'' = g_1' \prod_{n=1}^{\kappa} P_{1,n} = g_1^{1+\phi} \\ g_2'' = g_2' \prod_{n=1}^{\kappa} P_{2,n} = g_2^{1+\phi} \\ g_3'' = g_3' \prod_{n=1}^{\kappa} P_{3,n} = g_3^{1+\phi} \end{cases} \tag{8}$$

   where $\phi = \sum_{j=1}^{C} \sum_{n=1}^{\kappa_j} \frac{1}{\theta + x_{j,n}}$.

   The latest $\text{HDPK}_C = (\Delta,\ g_1'',\ g_2'',\ g_3'')$.

2) `usk_Update` is used to update a user's signing key. To update a user signing key from $\text{usk}_{\text{ID}_i}^{C-1} = (S_i',\ x_i\ , y_i,\ z_i,\ S_i^{\text{ini}})$ to the latest $\text{usk}_{\text{ID}_i}^{C} = (S_i^{\text{sur}},\ x_i\ , y_i,\ z_i,\ S_i^{\text{ini}})$, `usk_Update` works as follows:

   By using *URL* and HDPK_C, it computes

$$\text{K}_{C,n} = \left[\left(P_{1,n} P_{2,n}^{-y_i} P_{3,n}^{-z_i}\right)(S_i^{\text{ini}})^{-1}\right]^{\frac{1}{x_i - x_{C,n}}} \tag{9}$$

   ($x_i \neq x_{C,n}$ for any $n = 1, \ldots, \kappa$).

$$S_i^{\text{cur}} = S_i' \prod_{n=1}^{\kappa} K_{C,n} = \left(g_1''(g_2'')^{-y_i}(g_3'')^{-z_i}\right)^{\frac{1}{\theta + x_i}}. \tag{10}$$

F. Discussion

So far we have introduced the CPAL in detail, which can provide anonymous user linking function. In this section, we further discuss some applications related to CPAL.

1) User Service Query in the FN: When a user wants to check its own service usage in an FN, first, the user can acquire the master linking key $\text{mk}_L = (U, V)$ from the TLS. Assume that the FN has built a service usage list, and an example is shown in Table II. The first column is collected signatures and the corresponding messages in the previous access of MSs. The second and third columns are date and service type, respectively. The fourth and fifth columns are service time and billing. After the user accesses the FN, it can check its own service usage by searching this list. The user gets some signatures according to the corresponding conditions, e.g., service type is *type 1* and access dates are *2013/12/16* and *2013/12/02*, thus the user can get (σ_1, M_1) and (σ_4, M_4). Then, the user can execute the algorithm in Section V-D by using mk_L. If (σ_1, M_1) and (σ_4, M_4) all belong to this user, the user can look up its own total service time and billing of service type 1, while its identity would not be revealed. Besides, more specific applications with the anonymous user linking function can be further developed according to the needs of users or service providers.

2) Application Scenario: The term "roaming" originates from the Global System for Mobile Communications (GSM), referring to the extension of connectivity service in a location that is different from the home location where the service was registered. In particular, roaming is the ability for a cellular user to automatically make and receive voice calls, send and receive data, or access other services, including home data services, when traveling outside the geographical coverage area of the HN, by means of using a visited network. With the development of wireless communications, the concept of roaming can be extended to the emerging paradigm of networking, e.g., IoT, VANET, and e-Health. When these

TABLE II
USER SERVICE USAGE LIST

	YYYY/MM/DD	Service	Length (min)	Billing ($)	.....
σ_1, M_1	2013/12/16	Type 1	10	10	
σ_2, M_2	2013/12/08	Type 2	20	4	
σ_3, M_3	2013/12/08	Type 3	30	15	
σ_4, M_4	2013/12/02	Type 1	5	5	
σ_5, M_5	2013/11/30	Type 3	60	30	
σ_6, M_6	2013/11/15	Type 4	120	20	
$\vdots$					

users want to access an FN, which is different from the HN where the service was registered, CPAL can be applied to the access process to provide security and privacy preservations. In this sense, CPAL has universality and is suitable for a variety of application scenarios.

VI. SECURITY ANALYSIS

In this section, we analyze the security properties of the proposed CPAL scheme. In particular, following the security and the privacy preservation goals discussed earlier, our analysis will focus on how the proposed CPAL scheme can provide strong anonymous mutual authentication and key agreement, efficient user tracking, user revocation, and anonymous user linking functions.

A. The Proposed CPAL Scheme can Provide Strong Anonymous Mutual Authentication and Key Agreement

1) When MS ID_i roams from the HN to an FN, it sends access request to the VAS. The VAS chooses a random number $b \in_R \mathbb{Z}_p^*$, computes g^b, and sends g^b to the MS. MS ID_i first chooses a random number $a \in_R \mathbb{Z}_p^*$ and computes g^a; then it generates authentication message $M = (\mathrm{Homedomain\_Name} \| \mathrm{Service\_Req} \| g^a \| \mathrm{timestamp})$. Next, MS ID_i uses its $\mathrm{usk}_{\mathrm{ID}_i}$ to generate the signature $\sigma = (X_1, X_2, X_3, X_4, h, s_\alpha, s_\beta, s_\gamma, s_\delta, s_x, s_y, s_z)$, and then sends M together with σ to the VAS. When the VAS receives M and the corresponding σ, it first computes

$$\begin{cases} {Y_1}' = u^{s_\alpha} X_1^{-h}, {Y_2}' = v^{s_\beta} X_2^{-h} \\ {Y_3}' = e(X_3, r_1)^{s_x} e({w_1}^{-s_\alpha} {w_2}^{-s_\beta}, r_\theta) e({w_1}^{-s_\gamma} {w_2}^{-s_\delta}, r_1) \\ e(g_2, r_1)^{s_y} e(g_3, r_1)^{s_z} (e(X_3, r_\theta)/e(g_1, r_1))^h \\ {Y_4}' = g^{s_y} d_1^{s_\alpha} d_2^{s_\beta} X_4^{-h}, {Y_5}' = X_1^{s_x} u^{-s_\gamma}, {Y_6}' = X_2^{s_x} v^{-s_\delta}. \end{cases} \tag{11}$$

Then, the VAS checks

$$h \stackrel{?}{=} H(M, X_1, X_2, X_3, X_4, {Y_1}', {Y_2}', {Y_3}', {Y_4}', {Y_5}', {Y_6}', g^b, g^{ab}). \tag{12}$$

If it holds, the VAS is able to authenticate MS ID_i, but the VAS just knows that the MS belongs to the HN without revealing the identity of the MS. Then, the VAS computes a signature $\sigma_{\mathrm{VAS}} = \mathrm{Sign}_{\mathrm{SK_{VAS}}}(\mathrm{FN\_Name} \| g^a \| g^b \| g^{ab})$, and sends σ_{VAS} to MS ID_i. MS ID_i verifies the σ_{VAS} by using $\mathrm{VK_{VAS}}$. If the verification is successful, it accepts the VAS, and can access the FN successfully.

2) The VAS chooses a random number $b \in_R \mathbb{Z}_p^*$ and computes g^b, then it sends g^b to MS ID_i. MS ID_i first chooses a random number $a \in_R \mathbb{Z}_p^*$ and computes g^a an $(g^b)^a$; then it generates authentication message $M = (\mathrm{Homedomain\_Name} \| \mathrm{Service\_Req} \| g^a \| \mathrm{timestamp})$ and generates the signature σ; then the VAS generates session key $\mathrm{sk} = (g^a)^b$ between MS ID_i and the FN for subsequent communication. After that, the VAS computes a signature $\sigma_{\mathrm{VAS}} = \mathrm{Sign}_{\mathrm{SK_{VAS}}}(\mathrm{FN\_Name} \| g^a \| g^b \| g^{ab})$, and sends σ_{VAS} to MS ID_i. MS ID_i verifies the σ_{VAS} by using $\mathrm{VK_{VAS}}$. If verification is successful, it accepts the sk, and can access the FN successfully.

B. The Proposed CPAL Scheme can Provide an Efficient User Tracking Function

Once a dispute occurs on an access request during roaming, the CPAL is equipped with an algorithm for tracking the corresponding user of the disputed access request message. If a grievant (e.g., an FN), denoted as JUDGE, raises doubts about one access request, it will ask the HAC to track the MS's identity related to the disputed access request message. According to Section V-C, JUDGE can track the corresponding MS ID_i by checking if the following equalities hold:

$$\begin{cases} h_{12} \stackrel{?}{=} h(\sigma, u, v, K_{12}, u^{s_1} w_1^{-h_{12}}, v^{s_2} w_2^{-h_{12}}, X_1^{s_1} X_2^{s_2} K_{12}^{-h_{12}}) \\ e(X_3 (K_{12})^{-1}, \ X_{2,i} r_\theta) \stackrel{?}{=} e(g_1 Y_{1,i}^{-1} Z_i^{-1}, \ r') \end{cases} \tag{13}$$

where g, g_2, r_1, and r_θ are in the initial home domain public key HDPK_0. If these two equalities hold, it proves that MS ID_i has ever accessed the FN and requested the corresponding services, and it cannot repudiate that.

This function can overcome the drawback existed in the previous schemes based on the pseudonym system or conventional group signature technique, i.e., it is necessary to trust the HAC, and the grievant cannot validate whether the identity revealed by the HAC is real. However, with CPAL, the grievant does not need to trust the HAC and can validate the real identity of the corresponding user of the disputed access request message itself.

C. The Proposed CPAL Scheme Can Provide an Efficient User Revocation Function

User revocation can be executed when any illegal or exceptional events occur, e.g., MS's secret key has been compromised, and the punishment for defaulting MS. In our CPAL, the user revocation is realized by implementing two key update algorithms, i.e., `HDPK_Update` and `usk_Update`. By executing algorithms `HDPK_Update` and `usk_Update`, the user revocation can be executed efficiently. Particularly, the user revocation can revoke a group of users simultaneously.

Correctness: The correction of algorithms in Section V-E can hold based on the following two equations.

$$K_{C,n} = \left[(P_{1,n}P_{2,n}^{-y_i}P_{3,n}^{-z_i})(S_i^{\text{ini}})^{-1}\right]^{\frac{1}{x_i-x_{C,n}}}$$
$$= \left[\left(g_1^{\frac{1}{\theta+x_{C,n}}}g_2^{\frac{-y_i}{\theta+x_{C,n}}}g_3^{\frac{-z_i}{\theta+x_{C,n}}}\right)\cdot\left(g_1^{\frac{1}{\theta+x_{C,n}}}g_2^{\frac{-y_i}{\theta+x_{C,n}}}g_3^{\frac{-z_i}{\theta+x_{C,n}}}\right)^{-1}\right]^{\frac{1}{x_i-x_{C,n}}}$$
$$= \left(g_1^{\frac{1}{\theta+x_{C,n}}}g_2^{\frac{-y_i}{\theta+x_{C,n}}}g_3^{\frac{-z_i}{\theta+x_{C,n}}}\right)^{\frac{1}{\theta+x_i}}. \quad (14)$$

$$S_i^{\text{cur}} = \left[S_i'\prod_{n=1}^{\kappa}K_{C,n} = (g_1g_2^{-y_i}g_3^{-z_i})^{\frac{1}{\theta+x_i}}\cdot\right.$$
$$\left.\prod_{j=1}^{C-1}\left(\prod_{n=1}^{\kappa_j}\left(g_1^{\frac{1}{\theta+x_{j,n}}}g_1^{\frac{-y_i}{\theta+x_{j,n}}}g_3^{\frac{-z_i}{\theta+x_{j,n}}}\right)^{\frac{1}{\theta+x_i}}\right)\right]\cdot$$
$$\left(\prod_{n=1}^{\kappa_j}\left(\left(g_1^{\frac{1}{\theta+x_{j,n}}}g_1^{\frac{-y_i}{\theta+x_{j,n}}}g_3^{\frac{-z_i}{\theta+x_{j,n}}}\right)^{\frac{1}{\theta+x_i}}\right)\right)$$
$$= \left[(g_1^{1+\phi})(g_2^{1+\phi})^{-y_i}(g_3^{1+\phi})^{-z_i}\right]^{\frac{1}{\theta+x_i}}$$
$$= \left((g_1'')(g_2'')^{-y_i}(g_3'')^{-z_i}\right)^{\frac{1}{\theta+x_i}}. \quad (15)$$

In addition, the exposure problem of user status history can be resolved in the proposed CPAL, because the MS's secret key to be revoked and published is independent of its linkage information.

D. The Proposed CPAL Scheme Can Provide Anonymous User Linking

The network operators or service providers that are authorized by the HAC or MS ID_i, denoted as AUTLINKER, may need user's statistics on the CPAL of services. First, the HAC sends the master linking key $\text{mk}_L = (U, V)$ to the appointed AUTLINKER. Assume that the AUTLINKER has collected some of signatures and the corresponding messages in the previous access of MS ID_i, e.g., two pairs of signatures and messages, (σ', M) and (σ', M'). The AUTLINKER first checks if the signatures are valid. If so, using mk_L, If $\Omega_1 = \Omega_2$, it manifests that these signatures and the corresponding messages are generated by the same MS registered in the HN, while MS's identity will not be revealed.

In order to evaluate the ability of privacy preservation for user access authentication during roaming, we define three levels of user privacy, which are required for achieving authentication, anonymity, and AAUL, respectively, as shown in Table III. As discussed before, the AAUL function makes the privacy preservation of user more flexible. Any authorized entities including the MS itself can use this function to develop personalized applications, while guaranteeing the identity of the user will not be leaked.

Furthermore, the comprehensive comparisons of properties among the existing secure roaming schemes are shown in Table IV. From Table IV, we can see that our CPAL satisfies all security requirements in roaming services and has the level 3 ability of privacy preservation, which cannot be reached by other secure roaming schemes.

TABLE III
DEFINITIONS OF THE ABILITY OF PRIVACY PRESERVATION

	Authentication	Anonymity	AAUL
Level 1	✓	✗	✗
Level 2	✓	✓	✗
Level 3	✓	✓	✓

VII. PERFORMANCE EVALUATION

In this section, we evaluate the performance of the proposed CPAL scheme in terms of communication overhead and computation cost.

A. Computation Cost

In this section, we mainly compare our CPAL scheme with the existing two strong anonymous schemes [24], [25], rather than all secure roaming schemes, because other schemes do not have strong user anonymity. We first evaluate the computation cost during roaming, since this part might impact on the performance of the whole roaming service.

In the proposed CPAL scheme, the pairings $e(w_1, r_\theta)^{-r_\alpha}$, $e(w_2, r_\theta)^{-r_\beta}$, $e(w_1, r_1)^{-r_\gamma}$, $e(w_2, r_1)^{-r_\delta}$, $e(g_2, r_1)^{r_y}$, $e(g_3, r_1)^{r_z}$ can be precomputed and stored by MSs. During roaming, the VAS first computes g^b to require the access request message of MS, it requires 1 exponentiation operation in $\mathbb{G}_1$. Then, the MS generates an access request message M, it requires 2 exponentiation operations in $\mathbb{G}_1$ to compute g^a and g^{ab}. Next, in order to compute $X_1, X_2, X_3, X_4, \gamma, \delta, Y_1, Y_2, Y_3, Y_4, Y_5, Y_6$, and generate the signature, 2 exponentiations in $\mathbb{G}_1$ and 10 multiexponentiations ($1\ \text{multiexponentiation} \approx 1.25$ exponentiation [43]) are required. The MS can cache $e(S^{\text{cur}}, r_1)$. Instead of evaluating a pairing for each generation of a signature, $e(X_3, r_1)$ can be computed by $e(S^{\text{cur}}, r_1)e(w_1, r_1)^{\alpha}e(w_2, r_1)^{\beta}$; therefore, this step requires no pairing computation. In order to verify the signature of the MS, it requires 7 multiexponentiations and 1 pairing computation, since the VAS can derive Y_3' by merging $e(X_3, r_1)^{s_x}$, $e(X_3, r_\theta)^h$, and $e(X_3, r_1{}^{s_x}r_\theta{}^h)$ and evaluating one pairing. The hash computation and the multiplication are considered negligible compared to exponentiation and pairing operations. Finally, the VAS also needs to compute the $\text{sk} = g^{ab}$, which requires 1 exponentiation operation in $\mathbb{G}_1$. Denote the computation costs of an exponentiation operation in $\mathbb{G}_1$ and multiexponentiation, and a pairing operation in $\mathbb{G}_T$ by C_e, C_{me}, and C_p, respectively. According to [24] and [25], we present the computation cost comparison of CPAL, scheme [24] and Priauth [25] during roaming in Table V.

From Table V, the computation costs of an MS and the VAS are $3C_e + 10C_{\text{me}}$ and $C_e + 7C_{\text{me}} + C_p$ in the proposed CPAL scheme; in [24], totally for the MS and the VAS, the computation costs are $2C_e + 2C_{\text{me}} + 2C_p$ and $2C_e + C_{\text{me}} + C_p$, respectively; for Priauth [25], the computation costs of an MS and the VAS are $5C_e + 4C_{\text{me}} + 2C_p$ and $5C_e + 3C_{\text{me}} + 2C_p$, respectively.

Once a dispute occurs on an access request during roaming, the user tracking algorithm requires only 1 multiexponentiation in $\mathbb{G}_1$ and a binary search. If a key-update by revocation is considered, since g^{y_i} does not change regardless of revocation, the user tracking algorithm can directly determine the corresponding MS and thus minimize the computation. Judging a proof output by

TABLE IV
COMPARISONS OF PROPERTIES AMONG THE EXISTING SECURE ROAMING SCHEMES

Scheme	TOC	SRR	UNI	NOP	NOR	SUA	URF	APP	JRD
CPAL	Public	Yes	Yes	2	3	Yes	Yes	Level 3	Yes
EAP-based	Symmetric	Partially	No	3	6	No	No	Level 1	No
SFRIC [41]	Public	Partially	No	2	3	No	No	Level 1	No
Scheme [37]	Hybrid	Partially	Yes	3	5	No	No	Level 1	No
Scheme [38]	Hybrid	Partially	Yes	3	6	No	No	Level 1	No
Scheme [24]	Public	Partially	Yes	3	3	Yes	Yes	Level 2	No
Priauth [25]	Public	Yes	Yes	2	3	Yes	Yes	Level 2	No

TOC, type of cryptosystem; SRR, security requirements of roaming service; UNI, universality; NOP, the number of parties; NOR, the number of rounds; SUA, strong user anonymity; URF, user revocation function; APP, the abilities of privacy preservation; JRD, efficient joining and revocation function for dynamic membership.

TABLE V
COMPARISON OF COMPUTATION COST DURING ROAMING

ms	CPAL	Scheme [24]	Priauth [25]
MS	$3C_e + 10C_{me}$	$2C_e + 2C_{me} + 2C_p$	$5C_e + 4C_{me} + 2C_p$
VAS	$C_e + 7C_{me} + C_p$	$2C_e + C_{me} + C_p$	$5C_e + 3C_{me} + 2C_p$
Total	$25.25C_e + C_p$	$8.75C_e$+$3C_p$	$15.75C_e$+$4C_p$

TABLE VI
COMPARISON OF COMPUTATION COST EXCLUDING THE ROAMING

ms	CPAL	Scheme [24]	Priauth [25]
User tracking	$4C_{me}$+$2C_p$	N/A	N/A
Anonymous user linking	$6C_p$	N/A	N/A

our user tracking algorithm requires 3 multiexponentiations and 2 pairing computations. There is no user tracking function in scheme [24] and Priauth [25].

Once anonymous user linking is required, the linking algorithm computes 6 pairing operation for two given signatures σ and σ'. If the linking test needs to be executed for a fixed link index $e(X_4, r_1)$, then only two pairing computations for $e(X_1', U)e(X_2', V)$ are required for each new signature. In the proposed CPAL scheme, all revoked MSs must update their secret signing keys. Let n be the number of revoked MSs. This updating requires $3n$ multiexponentiations in $\mathbb{G}_1$ in our scheme. There are no anonymous user linking function in scheme [24] and Priauth [25]. Therefore, we present the computation cost comparison of CPAL, scheme [24] and Priauth [25] excluding the roaming in Table VI.

From Table VI, we can see that there are no values in scheme [24] and Priauth [25], because there are no the corresponding functions in scheme [24] and Priauth [25].

According to [44], in order to study the computation costs, the experiments are conducted with pairing-based cryptography (PBC) [45] and multiprecision integer and rational arithmetic C/C++ library (MIRACL) [46] libraries running on a 3.0-GHz processor 512 MB-memory computing machine. The experimental results indicate that a single exponentiation operation almost costs 12.4 ms, and the corresponding pairing operation costs 20 ms. With the exact computation costs, we can conclude that the total computation costs of CPAL, scheme [24], and Priauth [25] are 313.1, 168.5, and 275.3 ms, respectively. The computation costs of the user tracking and anonymous user linking algorithm are 102 and 120 ms, respectively. We can find that the computation costs of our CPAL scheme with access linkability is only larger 37.8 ms than that of Priauth [25], but can provide user tracking, anonymous user linking, joining, and revocation function for dynamic membership that other schemes do not have.

B. Communication Overhead

We focus on the communication overhead during roaming, since this part might impact on the performance of the whole roaming service.

In order to evaluate the transmission cost, assume that the transmission cost between the MS and the HAC is 1 unit. Let the transmission cost of an authentication message between the MS and the VAS be α unit, and between the VAS and the HAC be β unit, respectively. Since the VAS locates the FN, which is far away from the HAC, $\beta \gg \alpha$. We compare the transmission cost of CPAL with that of the existing schemes as shown in Table VII.

Table VII shows the transmission overheads of the reference schemes. From Table VII, our CPAL, scheme [24], Priauth [25], and SFRIC [41] need to transfer authentication 3 messages between the MS and the VAS without any communication between the VAS and the HAC. Jiang's scheme [37] need to transfer 3 authentication messages between the MS and the VAS, and 2 authentication messages between the VAS and the HAC. Scheme [38] and EAP-based schemes need to transfer 4 authentication messages between the MS and the VAS, and 2 authentication messages between the VAS and the HAC.

In addition, we compare our proposed CPAL scheme with the conventional EAP-based schemes. We consider the following two cases in the EAP-based schemes

1) The VAS must fetch the fresh authentication vectors from the HAC;
2) The VAS has the fresh authentication vectors already.

In the case 1), there are 4 messages between the MS and the VAS, and there are 2 messages between the VAS and HAC during one authentication procedure. The transmission cost of EAP-based schemes is

$$T_{\mathrm{EAP}-1} = 4\alpha + 2\beta. \tag{16}$$

In the case 2), since the VAS has the fresh authentication vectors already, it does not need to communicate with the HAC any more. Thus, the transmission cost of EAP-based schemes is

$$T_{\mathrm{EAP}-2} = 4\alpha. \tag{17}$$

However, in the proposed CPAL scheme, there are only 3 messages between the MS and the VAS during one authentication procedure. Therefore, the transmission cost of the proposed CPAL scheme is

$$T_{\mathrm{CPAL}} = 3\alpha. \tag{18}$$

TABLE VII
COMPARISON OF COMMUNICATION OVERHEAD

Scheme	$T_{\mathrm{MS-VAS}}{}^{a}$	$T_{\mathrm{VAS-HAC}}{}^{b}$
CPAL	3α	0
EAP-based	4α	2β
SFRIC [41]	3α	0
Scheme [37]	3α	2β
Scheme [38]	4α	2β
Scheme [24]	3α	0
Priauth [25]	3α	0

[a]The authentication transmission cost between MS and VAS.
[b]The authentication transmission cost between VAS and HAC.

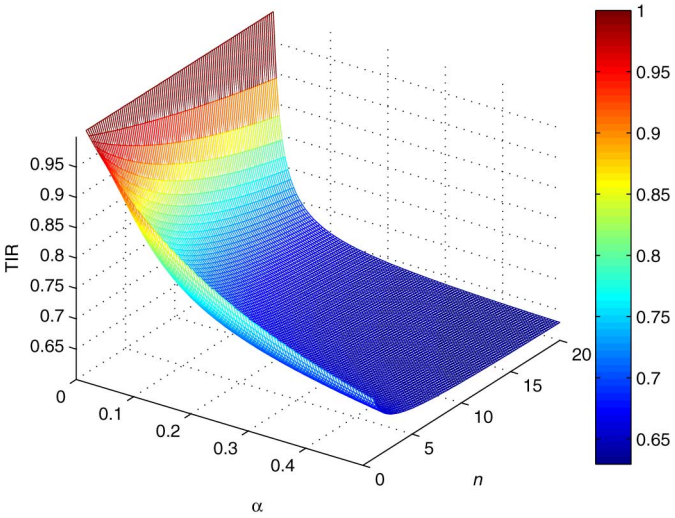

Fig. 4. Transmission improvement rate TIR.

Suppose that the VAS fetches n authentication vectors during the authentication procedure. The average transmission cost of the EAP-based schemes is

$$\begin{aligned} T_{\mathrm{EAP}} &= \tfrac{1}{n} T_{\mathrm{EAP}-1} + \tfrac{n-1}{n} T_{\mathrm{EAP}-2} \\ &= \tfrac{8\alpha n + 2\beta}{n}. \end{aligned} \tag{19}$$

We define a transmission improvement rate TIR to evaluate the improvement of the proposed CPAL compared to the EAP-based scheme.

The definition of transmission improvement rate TIR is as follows:

$$\mathrm{TIR} = \frac{T_{\mathrm{EAP}} - T_{\mathrm{CPAL}}}{T_{\mathrm{EAP}}} = \frac{5\alpha n + 2\beta}{8\alpha n + 2\beta}. \tag{20}$$

From the definition of TIR, we know that the bigger the TIR is, the smaller the transmission cost of our proposed scheme.

Fig. 4 plots the transmission improvement rate TIR varying with the number of authentication vectors n, and the value α that stands for the message transmission cost between the MS and the VAS. As can be seen from Fig. 4, at the beginning, the TIR is maximum (approximate to 1); when the size n of authentication vectors increases, the TIR decreases, then reaches 0.65 and tends to be stable. This is because in the initial stage, the VAS must communicate more frequently with the HAC to obtain fresh authentication vectors in the EAP-based schemes. Moreover, when the authentication message transmission cost α between the MS and the VAS increases, similarly, TIR will decrease and then attains to stability. The TIR is always greater than 0.65, which manifests that the communication cost of CPAL is less than that of EAP-based schemes. The reason is that the proposed CPAL scheme does not need the message exchanging for getting authentication vectors between the VAS and the HAC, thus it avoids the additional communication overhead of obtaining authentication vectors.

VIII. CONCLUSION AND FUTURE WORK

In this paper, we have proposed a CPAL for roaming service, which can provide multilevel privacy preservation for the emerging paradigm of networking, such as the IoT. Particularly, the proposed CPAL can make authorized network operators or service providers link all the access information of the same user for statistical purposes, but they cannot know who the user is, what the current membership status of the user is, and the history of the user joining and revocation. Through extensive analysis, we demonstrate that CPAL resists various security threats and provides more flexible and elaborate privacy preservation including user tracking, anonymous user linking, joining, and revocation function for dynamic membership. In addition, performance evaluations demonstrate its efficiency in terms of communication and computation overhead. For the future work, we will study the possible behavior by internal attackers and extend the CPAL scheme to effectively resist such attacks. In addition, we will design the lightweight secure and privacy-preserving scheme supporting very large group of IoT devices.

REFERENCES

[1] S. Sesia, I. Toufik, and M. Baker, *LTE–The UMTS Long Term Evolution: From Theory to Practice.* Hoboken, USA: vol. 66, Wiley Online Library, 2009.
[2] IEEE-SA Standards Board, *Air Interface for Fixed Broadband Wireless Access Systems, Part 16, Amendment 2 and Corrigendum 1*, IEEE Standard 802.16e-2005 and IEEE Standard 802.16-2004/Cor1-2005.
[3] X. Lin, X. Sun, P. Ho, and X. Shen, "GSIS: A secure and privacy-preserving protocol for vehicular communications," *IEEE Trans. Veh. Technol.*, vol. 56, no. 6, pp. 3442–3456, Nov. 2007.
[4] R. Lu, X. Lin, H. Zhu, P. Ho, and X. Shen, "ECPP: Efficient conditional privacy preservation protocol for secure vehicular communications," in *Proc. IEEE INFOCOM,* 2008, pp. 1229–1237.
[5] A. Al Shidhani and V. Leung, "Fast and secure reauthentications for 3GPP subscribers during WiMAX-WLAN handovers," *IEEE Trans. Dependable Secure Comput.*, vol. 8, no. 5, pp. 699–713, Sep./Oct. 2011.
[6] W. Song, J. Chung, D. Lee, C. Lim, S. Choi, and T. Yeoum, "Improvements to seamless vertical handover between mobile WiMAX and 3GPP UTRAN through the evolved packet core," *IEEE Commun. Mag.*, vol. 47, no. 4, pp. 66–73, Apr. 2009.
[7] F. Xu, L. Zhang, and Z. Zhou, "Interworking of WiMAX and 3GPP networks based on IMS [IP multimedia systems (IMS) infrastructure and services]," *IEEE Commun. Mag.*, vol. 45, no. 3, pp. 144–150, Mar. 2007.
[8] P. Taaghol, A. Salkintzis, and J. Iyer, "Seamless integration of mobile WiMAX in 3GPP networks," *IEEE Commun. Mag.*, vol. 46, no. 10, pp. 74–85, Oct. 2008.
[9] L. Atzori, A. Iera, and G. Morabito, "The internet of things: A survey," *Comput. Netw.*, vol. 54, no. 15, pp. 2787–2805, 2010.
[10] L. Tan and N. Wang, "Future internet: The internet of things," in *Proc. 3rd Int. Conf. Adv. Comput. Theory Eng.,* 2010, vol. 5, pp. 376–380.
[11] M. Zorzi, A. Gluhak, S. Lange, and A. Bassi, "From today's INTRAnet of things to a future INTERnet of things: A wireless-and mobility-related view," *IEEE Wireless Commun.*, vol. 17, no. 6, pp. 44–51, Dec. 2010.
[12] G. Broll, E. Rukzio, M. Paolucci, M. Wagner, A. Schmidt, and H. Hussmann, "Perci: Pervasive service interaction with the internet of things," *IEEE Internet Comput.*, vol. 13, no. 6, pp. 74–81, Nov./Dec. 2009.

[13] H. Li, H. Chen, J. Li, and F. Qi, "Study on the influence of IOT (Internet of Things) on mobile network," in *Proc. IET Int. Conf. Commun. Technol. Appl.,* 2011, pp. 619–621.
[14] Y. Soh, T. Quek, M. Kountouris, and H. Shin, "Energy efficient heterogeneous cellular networks," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 5, pp. 840–850, May 2013.
[15] R. Karri, H. Wang, K. I. Pedersen, and C. Rosa, "Multicell cooperation for LTE-advanced heterogeneous network scenarios," *IEEE Wireless Commun.*, vol. 20, no. 1, pp. 27–34, Feb. 2013.
[16] J. Jailton, T. Carvalho, V. Warley, N. Carlos, and R. Francês, "A quality of experience handover architecture for heterogeneous mobile wireless multimedia networks," *IEEE Commun. Mag.*, vol. 51, no. 6, pp. 152–159, Jun. 2013.
[17] M. Peng, Y. Liu, D. Wei, W. Wang, and H. Chen, "Hierarchical cooperative relay based heterogeneous networks," *IEEE Wireless Commun.*, vol. 18, no. 3, pp. 48–56, Jun. 2011.
[18] A. Bikos and N. Sklavos, "LTE/SAE security issues on 4G wireless networks," *IEEE Secur. Privacy*, vol. 11, no. 2, pp. 55–62, Mar./Apr. 2013.
[19] D. He, C. Chen, J. Bu, S. Chan, and Y. Zhang, "Security and efficiency in roaming services for wireless networks: Challenges, approaches, and prospects," *IEEE Commun. Mag.*, vol. 51, no. 2, pp. 142–150, Feb. 2013.
[20] R. Lu, X. Lin, and X. Shen, "SPOC: A secure and privacy-preserving opportunistic computing framework for mobile-healthcare emergency," *IEEE Trans. Parallel Distrib. Syst.*, vol. 24, no. 3, pp. 614–624, Mar. 2013.
[21] B. Wang, B. Li, and H. Li, "Public auditing for shared data with efficient user revocation in the cloud," in *Proc. IEEE INFOCOM,* 2013, pp. 1–9.
[22] R. Lu, X. Li, H. Luan, X. Liang, and X. Shen, "Pseudonym changing at social spots: An effective strategy for location privacy in VANETs," *IEEE Trans. Veh. Technol.*, vol. 61, no. 1, pp. 86–96, Jan. 2012.
[23] X. Liang, X. Li, H. Luan, R. Lu, X. Lin, and X. Shen, "Morality-driven data forwarding with privacy preservation in mobile social networks," *IEEE Trans. Veh. Technol.*, vol. 61, no. 7, pp. 3209–3221, Sep. 2012.
[24] G. Yang, Q. Huang, D. Wong, and X. Deng, "Universal authentication protocols for anonymous wireless communications," *IEEE Trans. Wireless Commun.*, vol. 9, no. 1, pp. 168–174, Jan. 2010.
[25] 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.
[26] J. Hwang, S. Lee, B. Chung, H. S. Cho, and D. Nyang, "Group signatures with controllable linkability for dynamic membership," *Inf. Sci.*, vol. 222, pp. 761–778, 2012.
[27] C. Fan, Y. Lin, and R. Hsu, "Complete EAP method: User efficient and forward secure authentication protocol for IEEE 802.11 wireless LANs," *IEEE Trans. Parallel Distrib. Syst.*, vol. 24, no. 4, pp. 672–680, Apr. 2013.
[28] C. Lai, H. Li, X. Li, and J. Cao, "A novel group access authentication and key agreement protocol for machine-type communication," *Trans. Emerging Telecommun. Technol.,* Apr. 2013.
[29] H. Mun, K. Han, and K. Kim, "3G-WLAN interworking: Security analysis and new authentication and key agreement based on EAP-AKA," in *Proc. Wireless Telecommun. Symp.,* 2009, pp. 1–8.
[30] C. Ntantogian and C. Xenakis, "Reducing authentication traffic in 3G-WLAN integrated networks," in *Proc. 18th IEEE Int. Symp. Pers., Indoor Mobile Radio Commun.,* 2007, pp. 1–5.
[31] M. Zhang and Y. Fang, "Security analysis and enhancements of 3GPP authentication and key agreement protocol," *IEEE Trans. Wireless Commun.*, vol. 4, no. 2, pp. 734–742, Mar. 2005.
[32] D. Zhang, "3GPP TS 33.401 V12.5.0, 3GPP System Architecture Evolution (SAE); Security Architecture," Sep. 2012.
[33] J. Arkko and H. Haverinen, "Extensible Authentication Protocol Method for Third Generation Authentication and Key Agreement (EAP-AKA), IETF RFC 4187," Jan. 2006.
[34] K. Dooley, *Designing Large Scale LANs.* Sebastopol, CA, USA: Reilly Media, 2009.
[35] K. Hoeper and L. Chen, "Where EAP security claims fail," in *Proc. 4th Int. Conf. Heterog. Netw. Quality, Reliab., Secur. Robustness Workshops,* 2007, pp. 1–7.
[36] G. Yang, D. S. Wong, and X. Deng, "Deposit-case attack against secure roaming," in *Proc. Inf. Secur. Privacy,* 2005, pp. 417–428.
[37] Y. Jiang, C. Lin, X. Shen, and M. Shi, "Mutual authentication and key exchange protocols for roaming services in wireless mobile networks," *IEEE Trans. Wireless Commun.*, vol. 5, no. 9, pp. 2569–2577, Sep. 2006.
[38] M. Shi, H. Rutagemwa, X. Shen, J. Mark, and A. Saleh, "A service-agent-based roaming architecture for WLAN/Cellular integrated networks," *IEEE Trans. Veh. Technol.*, vol. 56, no. 5, pp. 3168–3181, Sep. 2007.
[39] M. Chuang, J. Lee, and M. Chen, "SPAM: A secure password authentication mechanism for seamless handover in proxy mobile IPv6 networks," *IEEE Syst. J.*, vol. 7, no. 1, pp. 102–113, Mar. 2013.
[40] Z. Wan, K. Ren, and B. Preneel, "A secure privacy-preserving roaming protocol based on hierarchical identity-based encryption for mobile networks," in *Proc. 1st ACM Conf. Wireless Netw. Secur.,* 2008, pp. 62–67.
[41] Y. Kim, W. Ren, J. Jo, Y. Jiang, and J. Zheng, "SFRIC: A secure fast roaming scheme in wireless LAN using ID-based cryptography," in *Proc. IEEE ICC,* 2007, pp. 1570–1575.
[42] J. Ren and L. Harn, "An efficient threshold anonymous authentication scheme for privacy-preserving communications," *IEEE Trans. Wireless Commun.*, vol. 12, no. 3, pp. 1018–1025, Mar. 2013.
[43] A. Menezes, P. V. Oorschot, and S. Vanstone, *Handbook of Applied Cryptography.* Boca Raton, FL, USA: CRC press, 2010.
[44] R. Lu, X. Liang, X. Li, X. Lin, and X. Shen, "EPPA: An efficient and privacy-preserving aggregation scheme for secure smart grid communications," *IEEE Trans. Parallel Distrib. Syst.*, vol. 23, no. 9, pp. 1621–1631, Sep. 2012.
[45] B. Lynn. (2012). *PBC Library* [Online]. Available: http://crypto.stanford.edu/pbc/
[46] Shamus Software Ltd, (2012). *Multiprecision Integer and Rational Arithmetic C/C++ Library* [Online]. Available: http://www.shamus.ie/

Chengzhe Lai (S'13) received the B.S. degree from Xi'an University of Posts and Telecommunications, Xi'an, China, in 2008. He is working toward a Ph.D. degree in cryptography at Xidian University, China. He is currently a visiting Ph.D. student with the Broadband Communications Research (BBCR) Group, the University of Waterloo, ON, Canada.

His research interests include wireless network security, privacy preservation, and M2M communications security.

Hui Li received the B.Sc. degree from Fudan University, Shanghai, China, in 1990, M.A.Sc. and Ph.D. degrees from Xidian University, Xi'an, China, in 1993 and 1998, respectively.

He was as a Visiting Scholar with the Department of Electrical and Computer Engineering, University of Waterloo, Ontario, Canada, in 2009. He is a Professor with the School of Telecommunications Engineering, Xidian University. His research interests are in the areas of cryptography, security of cloud computing, wireless network security, information theory, and network coding.

Dr. Li is the co-author of two books. He served as TPC co-chair of ISPEC 2009 and IAS 2009, general co-chair of e-forensic 2010, ProvSec 2011, and ISC 2011.

Xiaohui Liang (S'10–M'13) received the M.Sc. and B.Sc. degrees from the Department of Computer Science, Shanghai Jiao Tong University, Shanghai, China, in 2009 and 2006, respectively. He obtained the Ph.D. degree in electrical and computer engineering from the University of Waterloo, Ontario, Canada, in 2013. He is a Postdoctoral Fellow with the Department of Computer Science, Dartmouth College, Hanover, NH, USA.

His research focuses on security, privacy, and trustworthiness of information and communication for mobile healthcare, mobile social networks, and cloud computing.

Rongxing Lu (S'09–M'11) received the Ph.D. degree in computer science from Shanghai Jiao Tong University, Shanghai, China, in 2006 and the Ph.D. degree in electrical and computer engineering from the University of Waterloo, Ontario, Canada, in 2012.

He is currently an Assistant Professor with the Division of Communication Engineering, School of Electrical and Electronics Engineering, Nanyang Technological University, Singapore. His research interests include wireless network security, applied cryptography, and trusted computing.

Kuan Zhang (S'13) received the B.Sc. degree in electrical and computer engineering and the M.Sc. degree in computer science from Northeastern University, Shenyang, China, in 2009 and 2011, respectively. He is currently working toward a Ph.D. degree at the Broadband Communications Research (BBCR) Group, Department of Electrical and Computer Engineering, University of Waterloo, Ontario, Canada.

His research interests include security and privacy for mobile social networks.

Xuemin (Sherman) Shen (M'97–SM'02–F'09) received the B.Sc. degree from Dalian Maritime University, Dalian, China, in 1982, and M.Sc. and Ph.D. degrees from Rutgers University, New Jersey, USA, in 1987 and 1990, all in electrical engineering.

He is a Professor and University Research Chair in the Department of Electrical and Computer Engineering, University of Waterloo, Ontario, Canada. His research focuses on resource management in interconnected wireless/wired networks, UWB wireless communications networks, wireless network security, wireless body area networks, and vehicular ad hoc and sensor networks.

Dr. Shen is a co-author of three books, and has published more than 400 papers and book chapters in wireless communications and networks, control, and filtering. He is the Editor-in-Chief of IEEE Network, and will serve as a Technical Program Committee Co-Chair for IEEE INFOCOM 2014. He is the Chair of the IEEE ComSoc Technical Committee on Wireless Communications, and P2P Communications and Networking, and a voting member of GITC. He was a Founding Area Editor for IEEE Transactions on Wireless Communications, and a Guest Editor for IEEE Journal of Selected Areas in Communications, IEEE Wireless Communications, and *IEEE Communications Magazine*. He also served as the Technical Program Committee Chair for GLOBECOM'07, Tutorial Chair for ICC'08, and Symposia Chair for ICC'10. He received the Excellent Graduate Supervision Award in 2006 and the Outstanding Performance Award in 2004, 2007, and 2010 from the University of Waterloo, and the Premier's Research Excellence Award in 2003 from the Province of Ontario, Canada. He is a registered Professional Engineer of Ontario, Canada, a Fellow of the Engineering Institute of Canada, a Fellow of Canadian Academy of Engineering, and was a ComSoc Distinguished Lecturer.