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 (Sherman) 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 multi-level 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 enable 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—Roaming, IoT, security, authentication, privacy preservation, anonymous user linkability.

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 to enjoy Internet service anytime and anywhere [5], [6], [7], [8]. This also caters to the demand of ubiquitous access for the emerging paradigm of networking, e.g., the Internet of Things (IoT) [9], [10], [11], [12], [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], [15], [16], [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], [21], [22], [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 operators or service providers may need individual access information on the usage of services, while preserving anonymity. This means that foreign network 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.

In this paper, to provide universal secure roaming service and anonymous user linkability, we propose a conditional privacy-preserving authentication with access linkability 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 three fold.

- 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 multi-level privacy preservation. Especially, the privacy-preservation ability is divided into three levels, i.e., authentication, anonymity, and authorized anonymous user linking (AAUL).

- 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 (Level 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.

- 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. Then, we present our CPAL and discuss some applications related to CPAL in Section V, followed by its security analysis and performance evaluation in Section VI and Section 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], [28], [29], [30], [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 [24], 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 non-traceability, 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, 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], [40], [41], [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 untraceability. 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; (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 traceability. 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 untraceability.

However, the existing privacy-preserving authentication schemes for roaming service cannot provide anonymous user linkability that makes the authorized entities, e.g., foreign network 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.

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 foreign network (FN).
A mobile subscriber (MS) can access the FN through the access point (AP), e.g., E-UTRAN eNB, WiMAX BS, IEEE 802.11b AP, etc. 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 session to decrypt the authentication messages which interacted by the MS and the VAS have not been altered during the transmission, i.e., if the adversary forges access messages that interacted by the MS and the VAS have not been altered during the transmission, the malicious operations should be detected. Meanwhile, the identity of the MS cannot be revealed to adversary 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 access requests, and multiple FNs. The HAC’s responsibility is that, issuing the secret signing key for new joining MSs, and opening a session to decrypt the authentication messages which interacted by the MS and the VAS have not been altered during the transmission, i.e., if the adversary forges access messages that interacted by the MS and the VAS have not been altered during the transmission, the malicious operations should be detected. Meanwhile, the identity of the MS cannot be revealed to adversary A or the VAS.

3) Anonymous user linking: In order to provide conditional privacy-preserving authentication with access linkability, 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 Hybrid Linear Combination Encryption (HLCE), which will serve as the basis of the proposed CPAL scheme.

A. Bilinear Maps

Let $G_1$, $G_2$, and $G_T$ be multiplicative groups of prime order $p$. The bilinear map $e: G_1 \times G_2 \rightarrow G_T$ has the following properties:

1) Bilinearity: $\forall g_1 \in G_1$, $\forall g_2 \in G_2$, and $\forall a,b \in \mathbb{Z}_p^*$, $e(g_1^a, g_2^b) = e(g_1, g_2)^{ab}$;

2) Non-degenerate: $\exists g_1, g_2$ such that $e(g_1, g_2)$ has order $p$, i.e., $e(g_1, g_2)$ is a generator of $G_T$;

3) Computable: There is an efficient algorithm to compute $e(g_1, g_2)$ for any $g_1 \in G_1$ and $g_2 \in G_2$.

Definition 1. A bilinear parameter generator $Gen$ is a probabilistic algorithm that takes a security parameter $\lambda$ as input, and outputs a 5-tuple $(p, G_1, G_2, G_T, e)$ where $p$ is a 16-bit prime number, $G_1, G_2$ and $G_T$ are three groups with the same order $p$: $e: G_1 \times G_2 \rightarrow G_T$ is a nondegenerated and efficiently computable bilinear map.

B. Hybrid Linear Combination Encryption (HLCE)

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

- **KeyGen**: It chooses $u, v \in_R G_1$, $x_1, y_1, x_2, y_2 \in_R G_2$, and then computes the public key $pk = (u, v, w_1 = u x_1, w_2 = v y_1, d_1 = u x_2, d_2 = v y_2)$ and outputs its corresponding secret key $sk = (x_1, y_1, x_2, y_2)$.

- **Enc**: Given the public key $pk$ and a message $M = (M_1, M_2) \in G_1 \times G_1$, it chooses $a, b \in_R Z_p$. Then, it computes a ciphertext $c = (D_1 = u^a, D_2 = v^b, D_3 = M_1 w_1^a w_2^b, D_4 = M_2 d_1^a d_2^b)$.

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

<table>
<thead>
<tr>
<th>Notation</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>HN</td>
<td>home network</td>
</tr>
<tr>
<td>FN</td>
<td>foreign network</td>
</tr>
<tr>
<td>HAC</td>
<td>the home authentication center</td>
</tr>
<tr>
<td>TLS</td>
<td>the trust linking server</td>
</tr>
<tr>
<td>VAS</td>
<td>the visiting authentication server</td>
</tr>
<tr>
<td>MS</td>
<td>mobile subscriber</td>
</tr>
<tr>
<td>HDPK</td>
<td>home domain public key</td>
</tr>
<tr>
<td>HDPK₀</td>
<td>the initial home domain public key</td>
</tr>
<tr>
<td>mkᵢ</td>
<td>the master issuing key</td>
</tr>
<tr>
<td>mkₒ</td>
<td>the master opening key</td>
</tr>
<tr>
<td>mk₁</td>
<td>the master linking key</td>
</tr>
<tr>
<td>IDᵢ</td>
<td>the identity of the MSᵢ</td>
</tr>
<tr>
<td>SKᵢ</td>
<td>signing key of xᵢ</td>
</tr>
<tr>
<td>VKᵦ</td>
<td>public verification key of IDᵢ</td>
</tr>
<tr>
<td>upk₁,IDᵢ</td>
<td>user public key of MS IDᵢ</td>
</tr>
<tr>
<td>usk₁,IDᵢ</td>
<td>user signing key of MS IDᵢ</td>
</tr>
<tr>
<td>sk</td>
<td>session key between the MS and the VAS</td>
</tr>
</tbody>
</table>

A. System Initialization

Given the security parameter λ, the HAC first generates the bilinear parameters (p, G₁, G₂, T, e) by running Gen(λ). Then, the HAC chooses g₁, g₂, gₙ, g, u, v ∈ R G₂, and η₁, η₂, ε₁, ε₂, η ∈ Zₚ*. Next, it computes w₁ = u⁷, w₂ = v², d₁ = u^ε₁, d₂ = v^ε₂, U = r₁^ε₁, V = r₂^ε₂ and rₚ = r₁^θ. The HAC also chooses a cryptographic hash function H, where H : {0, 1}^* → Zₚ. After that, the home domain public key HDPK will be published as:

\[ HDPK = \{ G₁, G₂, e, g, r₁, rₚ, u, v, w₁, w₂, d₁, d₂, H, g₁, g₂, gₙ \} \] (1)

where g₁, g₂ and gₙ will be updated once user revocation occurs.

Then, the HAC generates the master issuing key mkᵢ = θ, the master opening key mkₒ = (η₁, η₂, ε₁, ε₂), and the master linking key mk₁ = (U, V), respectively.

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

- Step-1. The MS with IDᵢ makes use of a standard signature technique to generate a signing key SK,IDᵢ and the corresponding public verification key VK,IDᵢ.
- Step-2. The MS with IDᵢ chooses zᵢ ∈ R Zₚ*, and then computes upk,IDᵢ = gᵢ^zᵢ = Zᵢ ∈ G₁ and σ,IDᵢ = SignSK,IDᵢ(Regist_ReqIDᵢ, upk,IDᵢ, σ,IDᵢ) to the HAC.
- Step-3. The HAC first verifies σ,IDᵢ using VK,IDᵢ. If σ,IDᵢ is valid, the HAC chooses xᵢ, yᵢ ∈ R Zₚ*, and then computes Yᵢ,IDᵢ = g¹ᵢ, X₂,IDᵢ = r⁻¹ᵢ, and S₁,IDᵢ = (g₁g₂⁵zᵢZ⁻¹₁)⁴⁻ᵐᵢ ∈ G₁.¹

¹If there is no revocation event, then S₁,IDᵢ remains unchanged.

Next, the HAC sends (S₁,IDᵢ, Y₁,IDᵢ, X₂,IDᵢ) to MS IDᵢ.

- Step-4. Upon receipt of (S₁,IDᵢ, Y₁,IDᵢ, X₂,IDᵢ), MS IDᵢ checks if S₁,IDᵢ ∈ G₁ and e(S₁,IDᵢ, X₂,IDᵢ) = e(g₁g₂⁵zᵢ, r⁻¹ᵢ). If verification is successful, MS IDᵢ accepts the S₁,IDᵢ and generates a signature σ₂,IDᵢ = SignSK,IDᵢ(S₁,IDᵢ, Y₁,IDᵢ, X₂,IDᵢ, upk,IDᵢ) and sends σ₂,IDᵢ to the HAC.

- Step-5. The HAC verifies if σ₂,IDᵢ is valid, and then sends (xᵢ, yᵢ) to MS IDᵢ; then MS IDᵢ generates its user signing key as

\[ usk,IDᵢ = \left( S₁,IDᵢ^2 = (g₁g₂⁵zᵢg₃)^\frac{1}{4⁻ᵐᵢ} \right), xᵢ, yᵢ, zᵢ, \] (2)

where S₁,IDᵢ² corresponds to the current home domain public key HDPK and S₁,IDᵢ corresponds to the initial home domain public key HDPK₀ and will be used to update the S₁,IDᵢ when a revocation event occurs.

- Step-6. MS IDᵢ generates the signature σJudge,IDᵢ = SignSK,IDᵢ(Regist_ReqIDᵢ, upk,IDᵢ, Y₁,IDᵢ, X₂,IDᵢ, X₁,IDᵢ, σ,IDᵢ) to the registration list RegList (Fig. 2) that is built by the HAC.

B. Roaming

In this phase, when MS IDᵢ roams from the HN to an FN, the mutual authentication between MS IDᵢ 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 makes 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 SK,VAS and the corresponding public verification key VK,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 IDᵢ sends access request to the VAS; the VAS chooses a random number b ∈ R Zₚ* and computes gᵇ, and then sends gᵇ to the MS.

- Step-2. Upon receipt of gᵇ, MS IDᵢ first chooses a random number a ∈ R Zₚ* and computes gᵃ and (gᵇᵃ); then it generates its authentication message M = (Homedomain_Name||Service_Req||gᵃ||timestamp) and proceeds as follows:

\[ ² \text{If there is no update, then } S₁,IDᵢ^{cur} = S₁,IDᵢ^{init} . \]
MS ID_i chooses α, β ∈ R Z_p, and computes
X_1 = u^{α}, X_3 = S^{υ}\otimes w_{1}^{β}, X_4 = g^{2\alpha}d_{1}\otimes d_{2}, and γ = x_{1}\alpha mod p, δ = x_{1}\beta mod p.

Step-3. MS ID_i also picks r_{α}, r_{β}, r_{γ}, r_{δ}, r_{x}, r_{y}, r_{z} ∈ R Z_p, and computes

\[
Y_1 = u^{r_α}, Y_2 = v^{r_β} \\
Y_3 = e(X_3, r_1) e^{-r_α} e(w_1, r_γ) e(w_2, r_δ) e(w_1, r_β)^{-r_γ} e(w_2, r_γ)^{-r_δ}, \\
Y_4 = g^{r_γ} d_{1}^{r_α} d_{2}^{r_β} X_3 = X_1^{r_β} \gamma u^{-r_γ} Y_1 = X_2^{r_δ} \gamma v^{-r_δ}. \\
\]

Step-4. In order to generate a signature of M, MS ID_i computes
h = H(M, X_1, ..., X_4, Y_1, ..., Y_6, g^{g_1}, g^{a g_1}), and s_{α} = r_{α} + hα, s_{β} = r_{β} + hβ, s_{γ} = r_{γ} + hγ, s_{δ} = r_{δ} + hδ, s_{x} = r_{x} + h\delta X_1, s_{y} = r_{y} + hY_1, s_{z} = r_{z} + hZ. Finally, MS ID_i generates the signature

σ = (X_1, X_2, X_3, i, h, s_{α}, s_{β}, s_{γ}, s_{δ}, 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 sk = (g^{a})^{b} between MS ID_i and the FN, and then computes

\[
Y'_1 = u^{s_{α}} X_1^{h}, Y'_2 = v^{s_{β}} X_2^{h} \\
Y'_3 = e(X_3, r_1) e^{s_{α}} e(w_1, s_{γ}) e(w_2, s_{δ}), \\
e(g_2, r_1)^{s_{α}} e(g_3, r_1)^{s_{δ}} e(X_3, r_1)^{s_{γ}}, \\
Y'_4 = g^{s_{γ}} d_{1}^{s_{α}} d_{2}^{s_{β}} X'_3 = X_1^{s_{β}} u^{-s_{γ}} Y'_1 = X_2^{s_{δ}} v^{-s_{δ}}. \\
\]

Then, the VAS checks if

\[
h' = H(M, X_1, X_2, X_3, Y'_1, Y'_2, Y'_3, Y'_4, Y'_5, Y'_6, g^{b}, g^{a}).
\]

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

Step-6. After that, the VAS computes a signature σ_{VAS} = Sign_{SK_{V AS}}(FN_Name || g^{b} || g^{a}), and sends σ_{VAS} back to MS ID_i.

Step-7. MS ID_i verifies the σ_{VAS} by using 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_{i}} as g^{y_{i}} = X_{i}^{1} \times X_{2}^{2} \times K_{12}^{-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_{i}}) = H(g^{y_{i}}) in the RegList. If they match, the HAC retrieves corresponding upk_{ID_i}, Y_{1, i}, Y_{2, i}, X_{1, i}, and X_{2, i}.

Step-2. The HAC chooses s_1, s_2 ∈ R Z_p, and then computes

\[
K_{12} = X_{1}^{s_1} X_{2}^{s_2}, W_1 = u^{s_1}, W_2 = v^{s_2}, W_1 = X_{1}^{s_1} X_{2}^{s_2}, h_{12} = H(\sigma, u, v, K_{12}, W_1, W_2), \text{ and } s_1 = s_1 + h_{12} \text{ mod } p, s_2 = s_2 + h_{12} \text{ mod } p.
\]

After that, The HAC generates a proof \( (ID_{i}, P = K_{12}, h_{12}, s_1, s_2) \), and then sends the proof together with \( \sigma_{JUDGE_{i}, upk_{ID_{i}}, Y_{1, i}, Y_{2, i}, X_{1, i}, X_{2, i}} \) to JUDGE.

Step-3. JUDGE first verifies \( \sigma_{JUDGE_{i}} \), if it is valid, let

\[
r_{1} = \frac{g_{1}}{g_{1}^{s_1}}, \text{ where } g_{1} \text{ is an updated value of } g_{1} \text{ (if there is no upgrade, then } g_{1} = g_{1}).
\]

Step-4. JUDGE checks if the following equalities hold:

\[
\left\{ \begin{array}{l}
h_{12} = h(\sigma, u, v, K_{12}, u^{s_1} u^{-h_{12}}, v^{s_2} v^{-h_{12}}, X_{1}^{s_1} X_{2}^{s_2} K_{12}^{-1}) \\
e(X_{3}(K_{12})^{-1}, X_{2} r_{\theta}) = e(g_1 Y_{1, i}^{-1} Z_{1, i}^{-1}, r_{\theta}) \end{array} \right.
\]

where \( g_1, g_2, r_1, \text{ and } r_{\theta} \text{ are in the initial home domain public key } HDP_{K_0}. \) 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, denoted as AUTLINKER, may need user’s statistics on the usage of services.

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

\[
\begin{align*}
\Omega_1 &= e(X, r_1)(e(X, U)e(X, V))^{-1} \\
\Omega_2 &= e(X', r_1)(e(X', U)e(X', V))^{-1}
\end{align*}
\]

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, the punishment for defaulting MS, etc. In our CPAL, the user revocation is realized by implementing two key update algorithms, i.e., \( \text{HDPK}_{\text{Update}} \) and \( \text{usk}_{\text{Update}} \).

First of all, a revocation event counter \( C \) is defined, which is increased by one 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

\[
\text{HDPK}_0 = \left\{ \mathcal{G}_1, \mathcal{G}_2, e, g, r_1, r_0, u, v, w_1, w_2, d_1, d_2, H, g_1, g_2, g_3 \right\}.
\]

The \( \text{HDPK}_0 \) can be further expressed as

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

where \( \Delta = (\mathcal{G}_1, \mathcal{G}_2, e, g, r_1, r_0, u, v, w_1, w_2, d_1, d_2, H) \), and \( \Delta \) 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 \( \kappa \) MSs which correspond to \( \kappa \) keys to be revoked, and then the user revocation list \( URL \) is formed as

\[
URL = \{ P_{i,n} = g_{1+n}^{\frac{r_0}{n+C,n}}, P_{2,n} = g_{2+n}^{\frac{r_0}{n+C,n}}, P_{3,n} = g_{3+n}^{\frac{r_0}{n+C,n}}, x_{C,n}|n = 1, ..., \kappa_C \}.
\]

Then, \( \text{HDPK}_{\text{Update}} \) and \( \text{usk}_{\text{Update}} \) are executed as follows:

- \( \text{HDPK}_{\text{Update}} \) is used to update an HDPK. To update the current \( \text{HDPK}_{C-1} \) to the latest \( \text{HDPK}_C \), \( \text{HDPK}_{\text{Update}} \) 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

\[
\begin{align*}
 g_1'' &= g_1 \prod_{n=1}^{\kappa} P_{1,n} = g_1^{1+\phi} \\
 g_2'' &= g_2 \prod_{n=1}^{\kappa} P_{2,n} = g_2^{1+\phi} \\
 g_3'' &= g_3 \prod_{n=1}^{\kappa} P_{3,n} = g_3^{1+\phi}
\end{align*}
\]

where \( \phi = \sum_{j=1}^{C} \sum_{n=1}^{\kappa_j} \frac{1}{n+x_j^2} \).

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

- \( \text{usk}_{\text{Update}} \) that is used to update a user’s signing key. To update a user signing key from \( \text{usk}^{D_{C-1}}_i = (S_i, x_i, y_i, z_i, S_{i}^{\text{sur}}) \) to the latest \( \text{usk}^{D_C}_i = (S_i^{\text{sur}}, x_i, y_i, z_i, S_{i}^{\text{sur}}) \), \( \text{usk}_{\text{Update}} \) works as follows:

By using \( URL \) and \( \text{HDPK}_C \), it computes

\[
K_{C,n} = \left[ (P_{1,n}P_2^{-z_i}P_3^{-\gamma_i})(S_i^{\text{sur}})^{-1} \right] x_{C,n}^{\frac{1}{\theta_i}}
\]

(9)

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

\[
S_{i}^{\text{sur}} = S_i^{\text{sur}} \prod_{n=1}^{\kappa} K_{C,n} = \left( g_1'' g_2'' g_3'' \right)^{\frac{1}{n+C,n}}
\]

(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.

<table>
<thead>
<tr>
<th>YYYY/MM/DD</th>
<th>Service</th>
<th>Length (Min)</th>
<th>Billing ($)</th>
</tr>
</thead>
<tbody>
<tr>
<td>2013/12/16</td>
<td>Type 1</td>
<td>10</td>
<td>10</td>
</tr>
<tr>
<td>2013/08</td>
<td>Type 2</td>
<td>20</td>
<td>4</td>
</tr>
<tr>
<td>2013/12/02</td>
<td>Type 3</td>
<td>30</td>
<td>15</td>
</tr>
<tr>
<td>2013/11/15</td>
<td>Type 4</td>
<td>60</td>
<td>30</td>
</tr>
<tr>
<td>2013/11/15</td>
<td>Type 4</td>
<td>120</td>
<td>20</td>
</tr>
</tbody>
</table>

1) User Service Query in the Foreign Network: When a user wants to check its own service usage in a foreign network, firstly, the user can acquire the master linking key \( mk_L = (U, V) \) from the TLS. Assume that the foreign network 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 column and third column are date and service type, respectively. The fourth column and fifth column 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 date are 2013/12/16 and 2013/12/02, thus the user can get (\( \sigma_1, M_1 \)) and (\( \sigma_4, M_4 \)). Then, the user can execute the algorithm in section V-D by using \( mk_L \). If \( (\sigma_1, M_1) \) and (\( \sigma_4, M_4 \) all belong to this user, the user can look up its own total service time and billing of service type 1, while its identity won’t be revealed. Besides, more specific applications with the anonymous user linking...
This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2014.2306673, IEEE Internet of Things Journal

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 home network, 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., Internet of Things (IoT), VANET, e-Health, etc. When these users want to access a foreign network which is different from the home network where the service was registered, CPAL can be applied to the access process to provide security and privacy preservation. 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.

• The proposed CPAL scheme can provide strong anonymous mutual authentication and key agreement.

(1) When MS $ID_1$ roams from the HN to an FN, it sends access request to the VAS. The VAS chooses a random number $b \in \mathbb{Z}_p^*$, computes $g^b$, and sends $g^b$ to the MS. MS $ID_1$ first chooses a random number $a \in \mathbb{Z}_p^*$ and computes $g^a$; then it generates authentication message $M = (Homedomain_Name||Service_Req||g^a||\text{timestamp})$. Next, MS $ID_1$ uses its $\text{usk}_{1_{ID_1}}$ to generate the signature $\sigma = (X_1, X_2, X_3, h, a, s_1, s_2, s_3, s_4, s_5, s_6, s_7, s_8)$, and then sends $M$ together with $\sigma$ to the VAS. When the VAS receives $M$ and the corresponding $\sigma$, it first computes

$$
Y_1' = u^{s_1}X_1^{-h}, Y_2' = v^{s_1}X_2^{-h},
Y_3' = e(X_3, r_1)^s_1e(w_1^{-s_2}w_2^{-s_3}, r_9)e(w_1^{-s_2}w_2^{-s_3}, r_1),
Y_4' = g^s_{1,1}d_1^s_1d_2X_4^{-h}, Y_5' = X_1^{s_1}w^{-s_2}, Y_6' = X_2^{s_1}w^{-s_3}.
$$

Then, the VAS checks

$$
h_12 = \frac{h(\sigma, u, v, K_{12}, u^{s_1}w^{-h_{12}}, v^{s_1}w^{-h_{12}}, X_1X_2K_{12}^{-h_{12}})}{e(X_3, K_{12})^{-1}, X_2, r_\theta} = e(g_1Y_1^{-1}Z_1^{-1}, r')
$$

(13)

where $g_1, g_2, r_1$, and $r_\theta$ are in the initial home domain public key $HDPK_0$. If these two equalities hold, it proves that MS $ID_1$ 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.

• 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, the punishment for defaulting MS, etc. In our CPAL, the user revocation is realized by implementing two key update algorithms, i.e., $HDPK_{\text{Update}}$ and $\text{usk}_{\text{Update}}$. By executing algorithms $HDPK_{\text{Update}}$ and $\text{usk}_{\text{Update}}$, 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.
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 satisfy all security requirements in roaming services, have the level 3 ability of privacy preservation, which cannot be reached by other secure roaming schemes.

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 \( e(w_1, r_3)^{-r_2}, e(w_2, r_3)^{-r_3}, e(w_1, r_1)^{-r_2}, e(w_2, r_1)^{-r_3}, e(g_2, r_1)^{r_3}, e(g_3, r_1)^{r_2} \) can be precomputed and stored by MSs. During roaming, the VAS first computes \( g^a \) to require the access request message of MS, it requires 1 exponentiation operation in \( G_1 \). Then, the MS generates an access request message \( M \), it requires 2 exponentiation operations in \( G_1 \) 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 \( G_1 \) and 10 multi-exponentiations (1 multi-exponentiation \( \approx 1.25 \) 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 \( e(S_{\text{cur}}, r_1) e(w_1, r_1)^{a} e(w_2, r_1)^{b} \), therefore, this step requires no pairing computation. In order to verify the signature of the MS, it requires 7 multi-exponentiations and 1 pairing computation, since the VAS can derive \( Y_3^8 \) by merging \( e(X_3, r_1)^{x} \) and \( e(X_3, r_1)^{y} \) 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 \( sk = g^{ab} \) which requires 1 exponentiation operation in \( G_1 \). Denote the computation costs of an exponentiation operation in \( G_1 \) and multi-exponentiation, and a pairing operation in \( G_T \) by \( C_e, C_{me} \) and \( C_p \), respectively. According to [24], [25], we present the computation cost comparison of CPAL, scheme [24] and Priauth [25] during roaming in Table V.

TABLE V
COMPARISON OF COMPUTATION COST DURING ROAMING

<table>
<thead>
<tr>
<th>( ms )</th>
<th>( CPAL ) scheme [24]</th>
<th>Priauth [25]</th>
</tr>
</thead>
<tbody>
<tr>
<td>MS</td>
<td>( 3C_e + 10C_{me} + 2C_p )</td>
<td>( 2C_e + 2C_{me} + 2C_p )</td>
</tr>
<tr>
<td>VAS</td>
<td>( C_e + 7C_{me} + C_p )</td>
<td>( 2C_e + C_{me} + C_p )</td>
</tr>
<tr>
<td>Total</td>
<td>( 25.25C_e + 3C_{me} + 2C_p )</td>
<td>( 8.75C_e + 3C_{me} + 3C_p )</td>
</tr>
</tbody>
</table>

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

Once a dispute occurs on an access request during roaming, the user tracking algorithm requires only 1 multi-exponentiation in $G_1$ and a binary search. If a key-update by revocation is considered, since $g^{\varphi}$ 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 our user tracking algorithm requires 3 multi-exponentiations and 2 pairing computations. There is no the 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 $\sigma$ and $\sigma'$. 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 $3n$ multi-exponentiations in $G_1$ in our scheme. There are no the 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 PBC [45] and 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 ms, 168.5 ms, 275.3 ms, respectively. The computation costs of the user tracking and anonymous user linking algorithm are 102 ms 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.

### Table IV

Comparisons of Properties Among the Existing Secure Roaming Schemes

<table>
<thead>
<tr>
<th>Scheme</th>
<th>TOC</th>
<th>SRR</th>
<th>UNI</th>
<th>NOP</th>
<th>NOR</th>
<th>SUA</th>
<th>URF</th>
<th>APP</th>
<th>JRD</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPAL</td>
<td>Public</td>
<td>Yes</td>
<td>Yes</td>
<td>2</td>
<td>3</td>
<td>Yes</td>
<td>Yes</td>
<td>Level 3</td>
<td>Yes</td>
</tr>
<tr>
<td>EAP-based</td>
<td>Symmetric</td>
<td>Partially</td>
<td>No</td>
<td>3</td>
<td>6</td>
<td>No</td>
<td>No</td>
<td>Level 1</td>
<td>No</td>
</tr>
<tr>
<td>SFRIC [41]</td>
<td>Public</td>
<td>Partially</td>
<td>No</td>
<td>2</td>
<td>3</td>
<td>No</td>
<td>No</td>
<td>Level 1</td>
<td>No</td>
</tr>
<tr>
<td>Scheme [37]</td>
<td>Hybrid</td>
<td>Partially</td>
<td>Yes</td>
<td>3</td>
<td>5</td>
<td>No</td>
<td>No</td>
<td>Level 1</td>
<td>No</td>
</tr>
<tr>
<td>Scheme [38]</td>
<td>Hybrid</td>
<td>Partially</td>
<td>Yes</td>
<td>3</td>
<td>6</td>
<td>No</td>
<td>No</td>
<td>Level 1</td>
<td>No</td>
</tr>
<tr>
<td>Scheme [24]</td>
<td>Hybrid</td>
<td>Partially</td>
<td>Yes</td>
<td>3</td>
<td>3</td>
<td>Yes</td>
<td>Yes</td>
<td>Level 2</td>
<td>No</td>
</tr>
<tr>
<td>Priauth [25]</td>
<td>Public</td>
<td>Yes</td>
<td>Yes</td>
<td>2</td>
<td>3</td>
<td>Yes</td>
<td>Yes</td>
<td>Level 2</td>
<td>No</td>
</tr>
</tbody>
</table>

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 VI

Comparison of Computation Cost Excluding the Roaming

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>User tracking</td>
<td>$4C_{m} + 2C_{p}$</td>
<td>N/A</td>
</tr>
<tr>
<td>Anonymous user linking</td>
<td>$6C_{p}$</td>
<td>N/A</td>
</tr>
</tbody>
</table>

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 $\alpha$ unit, and between the VAS and the HAC be $\beta$ 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

Comparison of Communication Overhead

<table>
<thead>
<tr>
<th>Scheme</th>
<th>$T_{MS-VAS}$</th>
<th>$T_{VAS-HAC}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPAL</td>
<td>$3\alpha$</td>
<td>0</td>
</tr>
<tr>
<td>EAP-based</td>
<td>$4\alpha$</td>
<td>$2\beta$</td>
</tr>
<tr>
<td>SFRIC [41]</td>
<td>$3\alpha$</td>
<td>0</td>
</tr>
<tr>
<td>Scheme [37]</td>
<td>$3\alpha$</td>
<td>$2\beta$</td>
</tr>
<tr>
<td>Scheme [38]</td>
<td>$4\alpha$</td>
<td>$2\beta$</td>
</tr>
<tr>
<td>Scheme [24]</td>
<td>$3\alpha$</td>
<td>0</td>
</tr>
<tr>
<td>Priauth [25]</td>
<td>$3\alpha$</td>
<td>0</td>
</tr>
</tbody>
</table>

1. The authentication transmission cost between MS and VAS
2. The authentication transmission cost between VAS and HAC

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.
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:

(i) The VAS must fetch the fresh authentication vectors from the HAC;
(ii) The VAS has the fresh authentication vectors already.

In the case (i), 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

\[ T_{EAP-1} = 4\alpha + 2\beta. \]  

(16)

In the case (ii), 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

\[ T_{EAP-2} = 4\alpha. \]  

(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

\[ T_{CPAL} = 3\alpha. \]  

(18)

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

\[
T_{EAP} = \frac{1}{n} T_{EAP-1} + \frac{n-1}{n} T_{EAP-2} = \frac{8\alpha n + 2\beta}{n}. \]  

(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

\[
TIR = \frac{T_{EAP} - T_{CPAL}}{T_{EAP}} = \frac{5\alpha n + 2\beta}{8\alpha n + 2\beta}. \]  

(20)

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

Fig. 4 plots the transmission improvement rate \( TIR \) varying with the number of authentication vectors \( n \), and the value \( \alpha \) 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 \( \alpha \) between the MS and the VAS increases, similarly, \( TIR \) will decreases and then attains to stability. The \( TIR \) is always greater than 0.65, which manifest 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 conditional privacy-preserving authentication with access linkability for roaming service, named CPAL, which can provide multi-level 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.

ACKNOWLEDGMENTS

Our research is supported by China Scholarship Council, the National Natural Science Foundation of China Grant 61272457, 61102056, 61303216, and the China Postdoctoral Science Foundation funded project (No.2013M542328). This work is also supported by a research grant from the Natural Science and Engineering Research Council (NSERC), Canada.

REFERENCES

Chengzhe Lai (S’13) received the B.S. degree from Xi’an University of Posts and Telecommunications in 2008. He is working toward a Ph.D. degree in Cryptography, Xidian University, China. He is currently a visiting Ph.D. student with the Broadband Communications Research (BBCR) Group, University of Waterloo. His research interests include wireless network security, privacy preservation, and M2M communications security.

Hui Li received the B.Sc. degree from Fudan University in 1990, M.A.Sc. and Ph.D. degrees from Xidian University in 1993 and 1998. He is a Professor with School of Telecommunications Engineering, Xidian University, Xi’an, China. In 2009, he was with Department of ECE, University of Waterloo as a visiting scholar. His research interests are in the areas of cryptography, security of cloud computing, wireless network security, information theory and network coding. He 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 an MSc (’09) degree and a BSc (’06) degree, both from the Department of Computer Science at Shanghai Jiao Tong University, China. He obtained his Ph.D. degree (’13) in Electrical and Computer Engineering at the University of Waterloo, Canada. He is a Postdoctoral Fellow, in the Department of Computer Science, at Dartmouth College. His research focuses on security, privacy, and trustworthiness of information and communication for mobile healthcare, mobile social networks, and cloud computing.

Xuemin (Sherman) Shen (M’97-SM’02-F’09) received his B.Sc. degree from Dalian Maritime University, China, in 1982, and M.Sc. and Ph.D. degrees from Rutgers University, New Jersey, 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. 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. He 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 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 JSAC, 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, an IEEE Fellow, a Fellow of the Engineering Institute of Canada, a Fellow of Canadian Academy of Engineering, and was a ComSoc Distinguished Lecturer.

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, Waterloo, ON, Canada, in 2012. He is currently an Assistant Professor with 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, 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, Canada. His research interests include security and privacy for mobile social networks.