An Anonymous Roaming Payment System with Low Communication Cost by Using Group Signatures

Chih-Hung Wang, Chih-Yu Lin, and Tai-Yuan Tu

***Abstract*—Mobile devices (e.g., PDAs, smart phones and notebooks) currently have become the trend for personal use and are equipped with the capability of wireless communications. To authenticate the mobile user who transfers to the foreign area, the roaming authentication protocol is needed and usually requested for low costs to meet the requirements of lightweight communication devices. With the development of powerful functionalities on the mobile devices, the roaming payment service seems to be practical and with high commercial value. This paper proposes an efficient roaming payment protocol with low communication costs by using group signatures, inspired by the roaming authentication schemes proposed by Yang *et al.* and He *et al.* The major contribution of this paper is to integrate the PayWord-based micropayment scheme and the group signature scheme to enhance the effectiveness of the anonymous signatures and extend the fast authentication in roaming to perform lightweight payments by using hash chains.**

***Index Terms*—Mobile payment, secure wireless communication, group signature, roaming authentication.**

I. Introduction

High functionality mobile devices like PDAs and smart phones have become the mainstream in personal communication and entertainment. Some business activities have been conducted in the cell phone environments, e.g., Android market and App Store, even though they are limited to purchasing software merchandise. To build an anonymous roaming payment system, the mobile payment protocol must surmount two critical challenges. The first challenge is the user authentication with anonymity. A mobile user must present his identity to the home agent for secure communication with others and can be anonymous when roaming to the foreign area. The second one is efficiency. The mobile user can pay rapidly for the small amounts of money without frequently connecting to his home agent.

Since a mobile user moves to the foreign area and cannot directly connect to his home location register (HLR), the user usually needs an authentication by the foreign network. Many kinds of secure roaming protocols have been proposed in the previous literature [1]-[3]. In general, the visitor location register (VLR) (or called foreign server) and HLR (or called home server) have a roaming agreement and share a common session key which can be used to encrypt the further communication messages or applied to the validity checking in the fast authentication stage. The roaming scenario generally includes three parities: a mobile user MU, a foreign server VLR and a home server HLR at which the mobile user registers. Upon roaming, MU sends the request to VLR. After receiving the request messages, VLR contacts with HLR and asks it for assistance to confirm the legality of the roaming user. The genuine identity of the roaming user cannot be revealed to the foreign server for the privacy considerations. Therefore in the above general case, the communication cost between VLR and HLR will be high since there are more and more roaming requests for the mobile users and they even ask for commercial services with strict authentication such as on-line payments.

The previous approaches to the roaming authentication [2], [4], [5] may have some security and performance problems. First, these protocols may suffer from denial of service (DoS) attacks [6], since they allow the VLR unconditionally to forward the user's authentication messages to HLR without preliminary verification. Further, as mentioned above, VLR needs to on-line contact with HLR when the roaming starting that may have a high overhead in communication. In 2010, Yang *et al.* proposed a new model to achieve universal authentication in roaming by using group signatures [7]. Afterwards, He *et al.* pointed out the problem of privacy-preserving and proposed an improved one [6].

Applying the group signature scheme and revocation list to the roaming authentication to achieve both anonymity and untraceability is a subtle idea. However, it uses the time-consuming computation operations of public-keys such as pairings and elliptic curve scalar multiplications. In this paper, we propose a new model of roaming payment protocol that felicitously integrates the roaming authentication by group signatures and PayWord-based micropayments [8]. The group signature can be used to sign a commitment of a hash chains and the untraceability can be preserved in our protocol. Furthermore, we use Unbalanced One-way Binary Tree (UOBT) [9] to provide an efficient mechanism for multiple vendors architecture and a convenient paying procedure in the fast authentication phase.

The remainder of this paper is organized as follows. In Section II, we review some related works and improvements used in this paper. An efficient roaming payment protocol by using the group signatures is described in Section III. Section IV provides the security issues and performance discussions. Finally, we conclude this paper in Section V.

II. Preliminary

A. Group Signatures

The original concept of group signature is proposed by

Manuscript received November 9, 2012; revised January 23, 2013. This work was supported in part by the National Science Council under the Grant NSC 101-2219-E-415-001.

The authors are with the Department of Computer Science and Information Engineering, National Chiayi University, Chiayi City 60004, Taiwan (e-mail: wangch@mail.ncyu.edu.tw, hgnc@hotmail.com, tlhctuty@gmail.com).

Chaum and van Heyst [10]. It has a nice property for anonymity that any one of the group member can sign the messages on behalf of the group without revealing his real identity. Therefore, this property can be used in this paper to authenticate the signer (i.e., the mobile user in roaming) having registered at HLR. He *et al.* [6] have proposed a roaming authentication by the group signature with verifier-local revocation. The group signature scheme is originated from Nakanishi and Funabiki's paper [11]. We briefly review it in the following.

1) VerLR-GSKeygen(*N*,*T*): The algorithm takes the two integers *N*, $T \in \mathbb{N}$ as the input, where *N* denotes the number of subscribers and *T* denotes the number of time intervals. The algorithm randomly chooses a generator $g \in G$ and $\tilde{g} \in_R G$. Moreover, it also chooses $h_j \in_R G$ for all $j \in [1,T]$. Then the algorithm chooses $\gamma \in_R \mathbb{Z}_P^*$ and calculates $\omega = g^{\gamma}$. It also chooses $x_i \in_R \mathbb{Z}_p^*$ and calculates $A_i = g^{1/(\gamma + x_i)}$ for all $i \in [1,N]$. Finally it calculates $B_{ij} = h_j^{x_i}$ for all *i* and *j*. The master public key *gpk* is $(g, \tilde{g}, h_1,...,h_T, \omega)$. Each subscriber's secret key *gsk*[*i*] is (A_i, x_i). The revocation token at interval *j* of subscriber U_i with secret key (A_i, x_i) is $grt[i][j] = B_{ij}$. The algorithm outputs a master public key $gpk = (g, \tilde{g}, h_1,...,h_T, \omega)$, the subscribers' secret keys $gsk = (gsk[i] = (A_i, x_i) \mid i \in [1,N])$, and revocation tokens $grt = (grt[i][j] = B_{ij} \mid i \in [1,N] \& j \in [1,T])$.

2) VerLR-GSSign(*gpk*, g*sk*[*i*], *j*, *M*): The algorithm takes the public key *gpk*, secret key *gsk*[*i*], the present time interval *j* and the message $M \in \{0,1\}^*$ as the input. The signed message $M \in \{0,1\}^*$ is assumed including time interval *j* in order to bind the signature to the interval. The followings are executing steps.
   a) The algorithm chooses random numbers $\alpha, \beta, \delta \in_R \mathbb{Z}_p^*$.
   b) The algorithm calculates
   $$T_1 = A_i \tilde{g}^{\alpha},\ T_2 = g^{\alpha} \tilde{g}^{\beta},\ T_3 = e(g^{x_i}, h_j)^{\delta} \text{ and } T_4 = g^{\delta}.$$
   c) The algorithm calculates
   $$V = SPK\{(\alpha, \beta, \delta, x_i, A_i) : T_1 = A_i \tilde{g}^{\alpha} \wedge T_2 = g^{\alpha} \tilde{g}^{\beta} \wedge T_3 = e(g^{x_i}, h_j)^{\delta} \wedge T_4 = g^{\delta} \wedge e(A_i, \omega g^{x_i}) = e(g,g)\}(M).$$

Notably, the readers can refer Nakanishi and Funabiki's paper [11] for the details of SPK (signatures converted by Fiat-Shamir heuristic from zero-knowledge proofs of knowledge).
   a) The algorithm outputs the group signature $\sigma = (T_1, T_2, T_3, T_4, V)$.

3) VerLR-GSVerify(*gpk*, *j*, RL_j, σ, *M*): The algorithm takes public key *gpk*, the current time interval *j*, the revocation list RL_j, the signature σ, and the message *M*. The algorithm performs (1) Signature check: checking *SPK V* to determine the validity of σ; (2) Revocation check: if $T_3 \neq e(T_4, B_{ij})$ for all $B_{ij} \in RL_j$, the signer was not revoked at the interval *j*.

B. Unbalanced One-Way Binary Tree

To support the multiple-vendors functionality in roaming payment, our protocol adopts the unbalanced one-way binary tree (UOBT) propoded by Yen *et al.* [9] in 1999 to construct the generalized PayWord chains. The UOBT can establish a two-dimensional matrix by deriving from a root value. Assume that the UOBT consists of the hash chains $P_1,...,P_a$ and $P_{a,b}$ is a hash chain root value. $P_{a,b}$ is extended by using hash function h_1 to generate $a-1$ subroots. Each subroot can derive an individual hash chain by applying another hash function h_2. The UBOT structure is shown in Fig. 1.

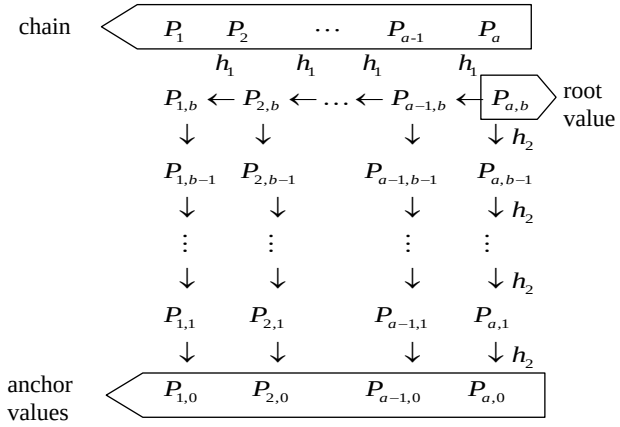

Fig. 1. Unbalanced one-way binary tree.

III. Proposed Protocol

The proposed protocol employs the group signature to eliminate the communications between VLR and HLR in roaming. When a mobile user reaches the circumscription controlled by the foreign server, he signs a UOBT matrix on behalf of HLR as a commitment for paying later on. VLR and the valid mobile user can share a common session key at the end of authentication stage. The session key can be used in fast payment to confirm the validity of the requesting user and protect the payment information. The details of the proposed protocol are shown below (also see Fig. 2).

Step 1: The mobile user MU chooses a random number R_u and a temporary identity *tid*. MU computes $\sigma_U = VerLR\text{-}GSSign$

$$(gpk_{HLR}, gsk[i], j, (ID_H \| ID_V \| tid \| g^{R_u} \| ts \| \Omega \| P_{\ell,0} \| b \| P_{\ell,start}))$$

where $P_{\ell,0}$ denotes the chain anchor value of UOBT for VLR_ℓ, $P_{\ell,start}$ denotes the chain starting in this payment event, *ts* denotes a timestamp and Ω denotes a root value of the hash chain used in the fast roaming payment (see below). MU sends σ_U, ID_H, *tid*, g^{R_u}, *ts*, Ω, $P_{\ell,0}$, *b*, $P_{\ell,start}$ to VLR_ℓ.

Step 2: Upon receiving the messages from MU, VLR_ℓ verifies whether the group signature is valid or not. If the verification passes, VLR_ℓ chooses a random number R_V and computes an elliptic curve digital signature algorithm:

$\sigma_V = ECDSASign(sk_V, (ID_H \| ID_V \| tid \| g^{R_u} \| g^{R_V}))$ with his private key sk_V, and computes the session key $CK = (g^{R_u})^{R_V}$. Otherwise VLR_ℓ rejects this request. Notably, VLR_ℓ sends $(\sigma_V, g^{R_V}, ID_V)$ to MU if all verifications are successful and MU was not revoked at interval j.

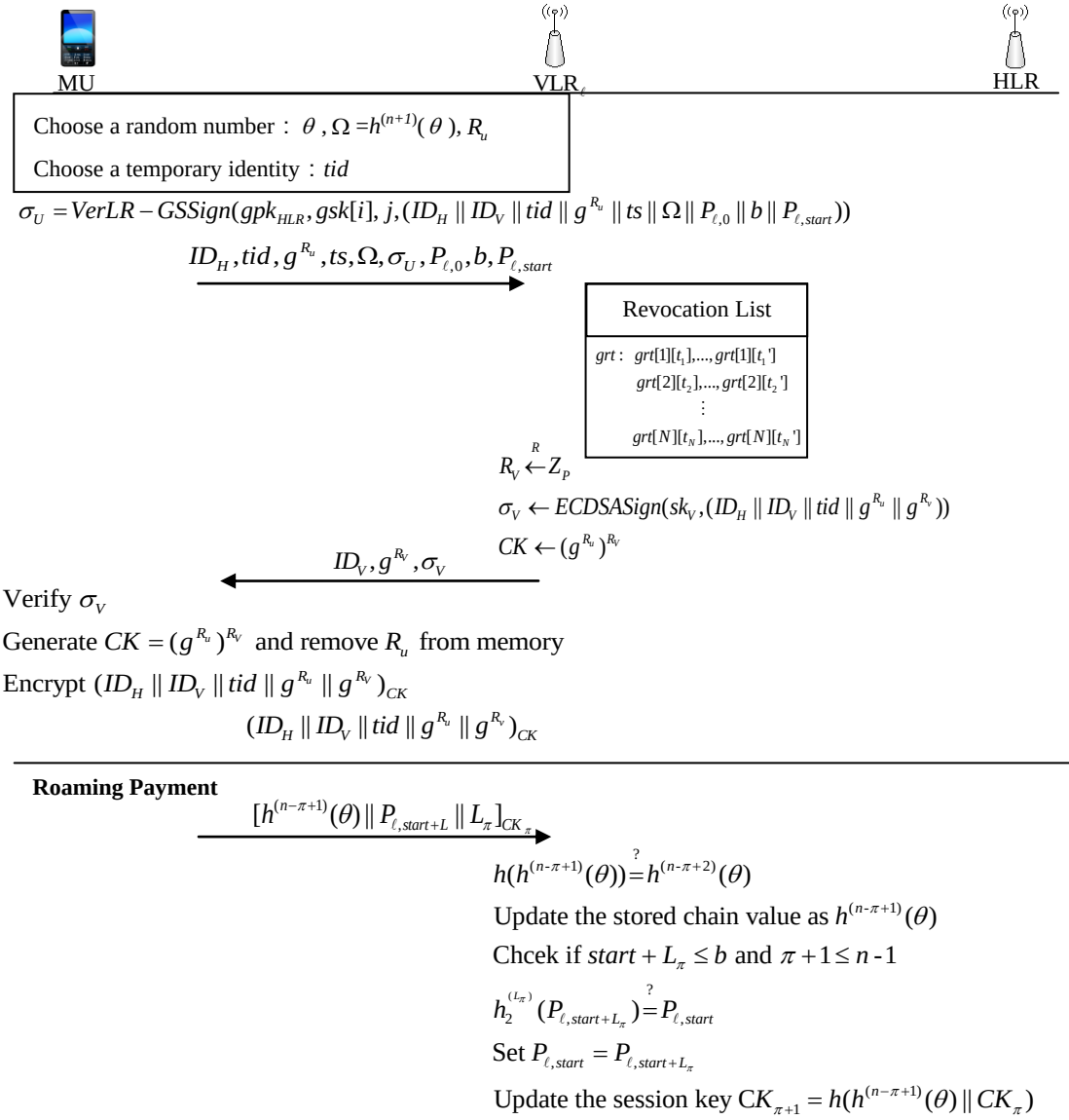

Fig. 2. A roaming payment protocol by using group signatures.

Step 3: Upon receiving the messages from VLR_ℓ, MU verifies σ_V by $ECDSAVer(pk_V, (ID_H \| ID_V \| tid \| g^{R_u} \| g^{R_V}), \sigma_V)$. If the verification passes, MU computes the session key $CK = (g^{R_u})^{R_V}$ and removes R_u from its memory. Then MU encrypts ID_H, ID_V, tid, g^{R_u}, g^{R_V} by the session key CK and sends the encrypted message to VLR_ℓ. Afterwards, VLR_ℓ decrypts the message and verifies it. If the verification passes, the session key CK can be established between VLR_ℓ and MU.

Roaming Payment: This phase provides fast authentications and payments. The session key would be updated in each round by using hash chain technique from [12]. MU prepares a hash chain $\{h^{(i)}(\theta) \mid i \in [1, n+1], h^{(i+1)}(\theta) = h(h^{(i)}(\theta)) \text{ and } h^{(n+1)}(\theta) = \Omega\}$ in advance by selecting a random θ. Assume that CK_π denotes πth session for MU to connect to VLR_ℓ during the roaming service, and MU spends L_π dollars in πth session. Furthermore, we assume that VLR_ℓ have stored $h^{(n-\pi+2)}(\theta)$ before running πth session payment. The details of payment at πth session are shown in the following.

Step 1: MU sends $[h^{(n-\pi+1)}(\theta) \| P_{\ell,start+L} \| L_\pi]_{CK_\pi}$ to VLR_ℓ.

Step 2: VLR_ℓ uses session key CK_π to decrypt the received messages, and then checks if the equation $h(h^{(n-\pi+1)}(\theta)) = h^{(n-\pi+2)}(\theta)$ holds. If the verification passes, VLR_ℓ updates the stored chain value to be $h^{(n-\pi+1)}(\theta)$, and then VLR_ℓ checks if $h_2^{(L_\pi)}(P_{\ell,start+L_\pi}) = P_{\ell,start}$, $\pi + 1 \le n - 1$ and $start + L_\pi \le b$. If the above verifications pass, VLR_ℓ sets $P_{\ell,start} = P_{\ell,start+L_\pi}$ and updates the session key $CK_{\pi+1} = h(h^{(n-\pi+1)}(\theta) \| CK_\pi)$.

IV. Analysis and Discussion

In this paper, the session key can be established by using

variant Diffie-Hellman protocol and the challenge-response technique. Therefore the robustness of the session key can be guaranteed. Moreover, by using the group signature scheme, the property of existential unforgeability can be achieved that means only a legitimate mobile user who has registered at HLR can generate a valid group signature on behalf of HLR.

The proposed payment protocol, similar to He *et al.*'s scheme [6], also can achieve anonymity and untraceability. We especially explain the case that the mobile user MU's revocation token $grt[i][j]$ appears in RL_j (jth interval of the revocation list). Although VLR can make sure that the connecting mobile user has been revoked at interval j, but it cannot link the real identity of the mobile user and cannot connect $grt[i][j]$ to other revocation tokens for different time intervals.

The performance of the proposed protocol is analyzed as follows. First, the user public key operations in group signature, ECDSA and session key calculations, according to the estimations by He *et al.* [6], are about four pairings plus 15.75 elliptic curve scalar multiplications. Second, our payment procedure cannot increase the costs of the authentication. We only add one symmetric encryption for MU and $L_\pi + 2$ hash operations for VLR_ℓ in the roaming payment procedure. It would be valuable to combine the payment into signature-based roaming authentication protocol, since the overhead is low and the practicality is high for some commercial applications.

TABLE I: THE COMPARISON AMONG THE PROPOSED PROTOCOL AND THE PREVIOUS SCHEMES

	HLR Off-line	DoS Attack Resistance	BF	User Untraceablility	Session Key Establishment	Fast Authentication	Used Techniques	Payment
Hwang-Chang [1]	No	No	No	Yes	Yes	Yes	Self-encryption	No
He-Ma-Zhang-Chen-Bu [4]	No	No	No	Yes	No	No	Smart Card	No
Yang-Huang- Wong-Deng [7]	No	No	No	No	Yes	No	Group Signature	No
He-Chan [5]	No	No	No	Yes	No	No	Hash Function	No
Yang-Wong-Deng [2]	No	No	No	Yes	Yes	No	AAKE-R	No
D. He-Bu-Chan-Chen-Yin [6]	Yes	Yes	Yes	Yes	Yes	No	VerLR Group Signature	No
Youn-Lim [12]	No	No	No	Yes	Yes	Yes	Delegation-based Signature	No
Ours	Yes	Yes	Yes	Yes	Yes	Yes	VerLR Group Signature, UOBT, hash chains	Yes

BF: Provision of User Revocation with Backward and Forward Unlinkabilities AAKE-R: Anonymous and Authenticated Key Exchange for Roaming

Table I shows the comparison in functionalities among the proposed protocol and other previous schemes.

V. CONCLUSION

It can be predicted that the roaming applications for business such as payments will be popular in the near future. Although the proposed authentication mechanism applied Diffie-Hellman-like protocol to construct the sharing key *CK* between MU and VLR, it can resist against the man-in-the-middle attack since the signatures *VerLR-GSSign* and *ECDSASign* are used to protect the exchanged parameters. This paper proposed an efficient roaming payment protocol with session key update and UOBT chains to rapidly pay for small amounts of money. The user authentication uses a group signature to make HLR off-line in the protocol, which can eliminate DoS attacks and reduce the communication costs.

REFERENCES

[1] K. F. Hwang and C. C. Chang, "A self-encryption mechanism for authentication of roaming and teleconference services," *IEEE Trans. on Wireless Communications*, vol. 2, pp. 400-407, Mar. 2003.

[2] G. Yang, D. S. Wong, and X. Deng, "Anonymous and authenticated key exchange for roaming networks," *IEEE Trans. on Wireless Communications*, vol. 6, pp. 3461-3472, Sep. 2007.

[3] G. Yang, D. S. Wong, and X. Deng, "Formal security definition and efficient construction for roaming with a privacy-preserving extension," *Journal of Universal Computer Science, Special Issue on Cryptography in Computer System Security*, vol. 14, pp. 441-462, Feb. 2008.

[4] D. He, M. Ma, Y. Zhang, C. Chen, and J. Bu, "A strong user authentication scheme with smart cards for wireless communications," *Journal Computer Communications*, vol. 34, pp. 367-374, Mar. 2011.

[5] D. He, S. Chan, C. Chen, J. Bu, and R. Fan, "Design and validation of an efficient authentication scheme with anonymity for roaming service in global mobility networks," *Wireless Personal Communications: An International Journal*, vol. 61, pp. 465-476, Nov. 2011.

[6] D. He, J. Bu, S. Chan, C. Chen, and M. Yin, "Privacy-preserving universal authentication protocol for wireless communications," *IEEE Trans. on Wireless Communications*, vol. 10, pp. 431-436, Feb. 2011.

[7] G. Yang, Q. Huang, D. S. Wong, and X. Deng, "Universal authentication protocols for anonymous wireless communications," *IEEE Trans. on Wireless Communications*, vol. 9, pp. 168-174, Jan. 2010.

[8] R. L. Rivest and A. Shamir, "Payword and micromint: two simple micropayment schemes," in *Proc. the International Workshop on Security Protocols*, *Lecture Notes in Computer Science*, vol. 1189, 1996, pp. 69-87.

[9] S. Yen, L. Ho, and C. Huang, "Internet micropayment based on unbalanced one-way binary tree," in *Proc. International Workshop on Cryptographic Techniques and E-Commerce*, July 1999, pp.155-162.

[10] D. Chaum and E. van Heyst, "Group signatures," in *Proc. the 10th annual international conference on Theory and Application of Cryptographic Ttechniques*, *EUROCRYPT'91*, 1991, pp. 257-265.

[11] T. Nakanishi and N. Funabiki, "Verifer-local revocation group signature schemes with backward unlinkability from bilinear maps," in *Proc. the 11th international conference on Theory and Application of Cryptology and Information Security*, *ASIACRYPT'05*, vol. 3788, 2005, pp. 533-548.

[12] T. Youn and J. Lim, "Improved delegation-based authentication protocol for secure roaming service with unlinkability," *IEEE Communications Letters*, vol. 14, pp. 791-793, Sep. 2010.

Chih-Hung Wang was born in Kaohsiung, Taiwan in 1968. He received the BS degree in Information Science from Tunghi University and MS degree in Information Engineering from National Chung Cheng University, Taiwan in 1991 and 1993, respectively. He received the Ph.D. degree in Information Engineering from National Cheng Kung University, Taiwan in 1998. He is presently an associate professor of Department of Computer Science and Information Engineering, National Chiayi University, Taiwan. His research interests include cryptography,

information security and data compression.

Chih-Yu Lin is a master student of Department of Computer Science and Information Engineering, National Chiayi University, Taiwan. Her research interests include cryptographic protocols and information security.

Tai-Yuan Tu is a Ph.D. student of Department of Computer Science and Information Engineering, National Chiayi University, Taiwan. His research interests include multimedia security, data hiding and watermarking technology.