

A new mobile payment scheme for roaming services

Ren-Junn Hwang ^{*}, Sheng-Hua Shiau, Ding-Far Jan

Department of Computer Science and Information Engineering, Tamkang University, Tamsui, Taipei 251, Taiwan, ROC

Received 22 August 2005; received in revised form 3 May 2006; accepted 24 July 2006

Available online 11 September 2006

Abstract

Due to the advance of mobile network technologies, mobile personal devices are used to perform electronic payment. This paper proposes a new on-line payment scheme for mobile network. The proposed scheme is not only performed in the home domain, but also can be performed in visited domain. Our scheme provides consumer anonymity, authentication, non-repudiation and data integrity properties. The consumer can make transaction with shop, vendor machine and WAP site based on our scheme. Our scheme only includes symmetric encryption and one-way hash function, it takes lower computation cost and is more suitable for mobile device.

© 2006 Elsevier B.V. All rights reserved.

Keywords: Micro-payment; Mobile payment; Wireless network security; Electronic commerce; Mobile commerce

1. Introduction

Electronic payment is an important issue of electronic commerce, such as PayWord, MicoMint, PayFair, is used to describe purchasing processes itself between buyers and sellers [1–4]. Secure electronic payment will not only make purchasing activities more convenient and flexible but also create an unimaginable new era of business [1,5–10]. Due to the advance of mobile network technologies, mobile personal devices are used to perform electronic payment. Hung and Chen [11] proposed a mobile payment scheme that can deal with shop by mobile phone. Their main contribution is that merchant and bank cannot trace consumer from the electronic coins by using Brands's blind signature [12]. However, their scheme has some drawbacks: The consumers should withdraw electronic coins from bank for each consumption. The merchant of their scheme just only be the shop or vender machine. Moreover, the scheme cannot be performed in roaming environment, and takes much computation cost.

Chen et al. [13] proposed another version of mobile payment scheme. Their scheme also has some disadvantages: The merchant can impersonate a consumer to perform the payment phase, and the merchant should be a WAP site. Besides, the scheme cannot be performed in roaming environment.

This paper proposes a new on-line mobile payment scheme. We integrate electronic payment and the roaming technology to develop a novel payment scheme. The proposed scheme provides the following security requirements [4,14–16]:

1. Consumer anonymity: Merchant and VLR (the visited location register) need not to know the consumer's real identity. In a wireless network, a consumer must supply his identity to the service network for verification. This identity must be protected to against thwart fraud. In our scheme, every consumer is assigned a temporary ID to hidden the real identity.
2. Non-repudiation: From the aspect of merchant, it is very important to prevent the possibility that a consumer denies any electronic coins that he has spent. At the same time, the consumer should not be wrongly charged due to any account error or security faulty in mobile network.

^{*} Corresponding author. Tel.: +886 933 951 377; fax: +886 2 2620 9749.
E-mail addresses: junhwang@ms35.hinet.net (R.-J. Hwang),
891190067@s91.tku.edu.tw (S.-H. Shiau), 689190345@s89.tku.edu.tw (D.-F. Jan).

3. Integrity: Outside parties should not be able to modify transaction data.
4. Authentication: Malicious attackers cannot impersonate any role involved in a transaction, such as merchants, consumers, HLR (the home location register) or VLR to damage partial or whole payment scheme.
5. Double-spending: Consumers, merchants or malicious attackers cannot double spend electronic coins.
6. Roaming: Consumers still can perform this scheme in roaming environment.

The rest of this paper is organized as follows. Section 2 introduces the proposed mobile payment environment. Section 3 proposes a new mobile payment scheme for roaming services. We analyze the security of the proposed scheme in Section 4. Section 5 makes comparisons among Hung and Chen's scheme, Chen et al.'s scheme and our scheme. Finally, conclusions are given in Section 6.

2. The mobile payment environment

The mobile payment environment includes four components: consumers, HLR, VLR, and merchants.

The consumer must apply a SIM card with the mobile payment feature from HLR. Fig. 1 shows the relationship of the payment processes in home domain. The consumer withdraws electronic coins from HLR by using his SIM card. He sends the payment information to the merchant (deals with WAP site in wireless network, deals with shop or vendor machine by ultra-red ray). The merchant checks the payment information by sending them to HLR. If HLR returns the result is legal, the merchant will sell the product to the consumer.

Fig. 2 shows the relationship of the payment processes in visited domain. The VLR authenticates the consumer's identity via HLR's help when the consumer roams in the visited domain. The consumer can perform mobile payment scheme in this domain.

In addition, merchants will send the receipts to exchange money back from its HLR.

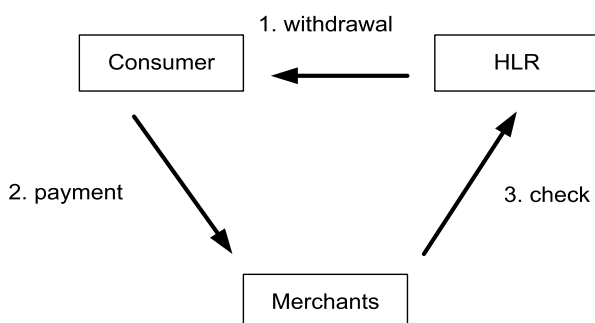


Fig. 1. Payment in home domain.

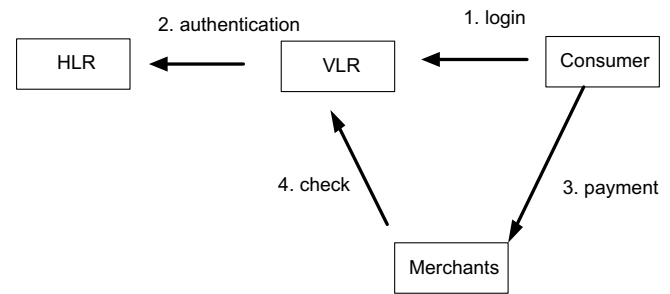


Fig. 2. Payment in visited domain.

3. The proposed mobile payment scheme

Before interpret the proposed scheme, we give the definition of the notations in this paper. Then the proposed scheme will show in Section 3.2.

3.1. Definition of notations

We use the following notations to describe the proposed scheme.

C	consumer
H	the home location register (HLR)
V	the visited location register (VLR)
M	merchant
n	the value of electronic coins.
ID_C, ID_H, ID_V, ID_M	the identities of consumer, HLR, VLR and merchant, respectively.
TID, VID	temporary identities of the consumer which are used at home domain and visited domain, respectively
K_{AB}	the shared key between two entities A and B
$S_{K_H}()$	the signature of HLR by signing with his private key K_H
$E_{K_{CH}}()$	the symmetric encrypt function using shared key K_{CH}
$h^n()$	perform n times one-way hash function, and $h^n() = h(h^{n-1}())$
T	timestamp

3.2. The proposed schemes

The proposed mobile payment scheme consists of eight phases as following:

1. Register: consumer registers in HLR and obtains SIM card securely.
2. Withdrawing electronic coins in HLR: the consumer should withdraw electronic coins in the home domain before performing mobile payment.
3. Payment in home domain: consumer pays the electronic coins to the merchant in his home domain.
4. Login VLR: the consumer roams in visited domain, he must login VLR first.

5. Payment in the visited domain: consumer roams in a visited domain, he pays the electronic coins to the merchant of the visited domain.
6. Consumer withdraws electronic coins in the visited domain: If the consumer runs out of his electronic coins in visited domain, he can withdraw electronic coins via VLR by performing this phase.
7. Logout VLR by the consumer himself: consumer logout VLR.
8. The consumer logout from the old VLR by his HLR: the consumer does not logout when he leaves a VLR but he wants to login another new VLR. HLR should perform this phase to cancel the authority of the consumer in the old visited domain.

3.2.1. Register

In this phase, consumers register in HLR and obtain SIM cards. The SIM card includes a shared key K_{CH} , a temporary identity TID and HLR's identity ID_H . The consumer should perform the following steps to register in HLR. Fig. 3 shows the transmitted messages between HLR and consumer.

- Step 1: The consumer sends a service request to the HLR.
 Step 2: HLR generates a shared key and a temporary identity as the following sub-steps.
- 2-1: Generate a shared key K_{CH} and a temporary identity TID for the consumer.
 - 2-2: Save TID , K_{CH} and ID_H in SIM card and his own database respectively.
 - 2-3: Return the SIM card to the consumer.

3.2.2. Withdrawing electronic coins in HLR

The consumer withdraws electronic coins via this phase before paying. We assume that the consumer wants to withdraw n units of electronic coins, he should perform the following steps. The transmitted messages between the consumer and HLR are shown in Fig. 4.

- Step 1: The consumer generates electronic coins and informs HLR as the following sub-steps.
- 1-1: Pick a non-repeat number $C_{\text{chainroot}}$ and compute $R_n = h^n(C_{\text{chainroot}})$.
 - 1-2: Use the shared key K_{CH} to encrypt R_n , n and timestamp T .

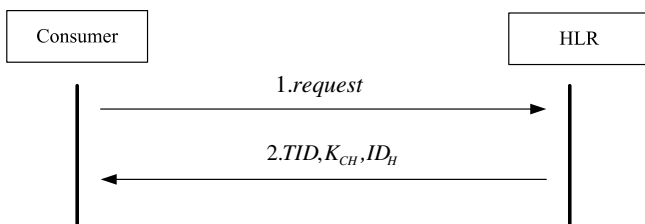


Fig. 3. Register.

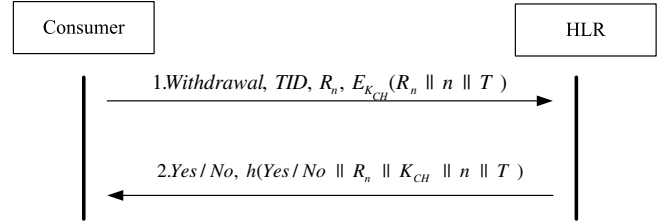


Fig. 4. Withdrawing electronic coins in HLR.

- 1-3: Send the message: *Withdrawal*, TID , R_n , $E_{K_{CH}}(R_n || n || T)$ to HLR.
- Step 2: HLR receives the message and performs the following sub-steps to verify the consumer.
- 2-1: Recover the consumer's real identity from TID .
 - 2-2: Use the shared key K_{CH} to get R_n , n and T , and verify R_n . If the verification is correct, then HLR performs Sub-step 2-3a, otherwise he performs Sub-step 2-3b.
 - 2-3a: Deduct n units of electronic coins from consumer's account and send the message: *Yes*, $h(Yes || R_n || K_{CH} || n || T)$ to the consumer.
 - 2-3b: Set $n = 0$ and send the message: *No*, $h(No || R_n || K_{CH} || n || T)$ to the consumer.

After Step 2, the consumer verifies $h(Yes/No || R_n || K_{CH} || n || T)$. R_n is the started point of the n units of electronic coins. We use a symmetric encryption function to protect confidentiality of n and timestamp T .

3.2.3. Payment in home domain

We assume that the consumer buys some products that cost x units of electronic coins in a merchant of home domain network. The consumer pays x units of electronic coins to merchant via the following steps. Without losing of the generality, we assume that the consumer has spent i units of electronic coins before consuming in this merchant. The based point of the electronic coins is R_i . The transmitted messages of this phase are showed in Fig. 5.

- Step 1: The consumer generates the payment information as the following sub-steps.
- 1-1: Compute $R_{i-x} = h^{i-x}(C_{\text{chainroot}})$ such that $h^x(R_{i-x}) = R_i$.
 - 1-2: Send the message: *PurchaseInformation*, TID , ID_H , (R_i, R_{i-x}, x) , $h(K_{CH} || ID_M || R_{i-x} || x)$ to the merchant.
- Step 2: The merchant verifies the value of the electronic coins by performing the following sub-steps.
- 2-1: Verify $R_i = h^x(R_{i-x})$.
 - 2-2: Send the message: ID_M , T , TID , (R_i, R_{i-x}, x) , $h(K_{CH} || ID_M || R_{i-x} || x)$ to HLR.
- Step 3: HLR performs the following sub-steps to verify the payment information.

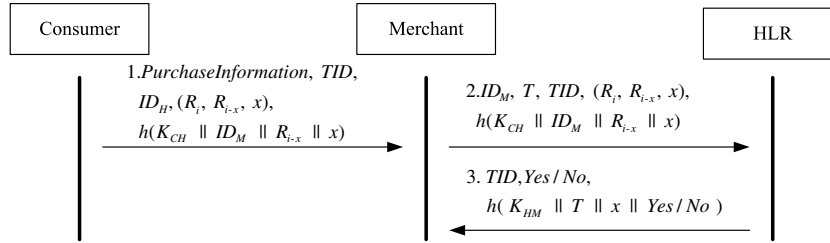


Fig. 5. Payment in home domain.

- 3-1: Verify that whether the request exceeds consumer's balance and the based point R_i . If both the verifications are correct, then HLR performs Sub-step 3-2a, otherwise he performs Sub-step 3-2b.
- 3-2a: Update consumer's based point to R_{i-x} and send the message: $TID, Yes, h(K_{HM} || T || x || Yes)$ to the merchant.
- 3-2b: Set $x = 0$ and send the message: $TID, No, h(K_{HM} || T || x || No)$ to the merchant.

After Step 3, the merchant verifies $h(K_{HM} || T || x || Yes/No)$ to make sure (R_i, R_{i-x}, x) is valid. The merchant delivers the products to the consumer. The *PurchaseInformation* of Step 1 lists the products that the consumer ordered. (R_i, R_{i-x}, x) is the payment which costs x units of electronic coins.

3.2.4. Login VLR

When the consumer roams in the visited domain, he should perform the following steps to login the VLR. We assume that the consumer has spent j units of electronic coins before login this VLR. The based point of the electronic coins is R_j . Fig. 6 shows the transmitted messages among the consumer, VLR and HLR in this phase.

- Step 1: The consumer computes the quota, *total_coin*, of his electronic coins by performing the following sub-steps.
- 1-1: Compute *total_coin* = j .
- 1-2: Send the message: *CheckIn*, $TID, ID_H, R_j, h(R_j || total_coin || K_{CH})$ to VLR.

- Step 2: VLR generates a shared key, a temporary virtual identity (*VID*) and send those parameters to HLR as the following sub-steps.

- 2-1: Select a non-repeat *VID* and a shared key K_{CV} .
- 2-2: Send the message: *CheckIn*, $ID_V, h(R_j || total_coin || K_{CH}), E_{K_{HV}}(TID || VID || R_j || K_{CV})$ to HLR.

- Step 3: HLR performs the following sub-steps to verify the authority of the consumer and returns some parameters to VLR.

- 3-1: Decrypt the ciphertext and know who wants to login VLR.
- 3-2: Check whether the consumer has logout from old VLR. If the consumer does not logout from the old VLR, HLR must perform "The consumer logout from the old VLR by his HLR" (Section 3.2.8).
- 3-3: Verify $h(R_j || total_coin || K_{CH})$ and save VLR's identity, ID_V .
- 3-4: Use the shared key K_{CH} to encrypt those parameters that VLR wants to give to the consumer as $E_{K_{CH}}(ID_V || VID || K_{CV} || Yes/No || T)$, where the message contains *Yes* when the verification in Sub-step 3-3 is correct, otherwise it contains *No*.
- 3-5: Send the message: $ID_H, E_{K_{HV}}(TID || total_coin || Yes/No || E_{K_{CH}}(ID_V || VID || K_{CV} || Yes/No || T))$ to VLR.

- Step 4: VLR records the quota of the consumer as follows:

- 4-1: Decrypt the message to get and record the consumer's quota *total_coin*.
- 4-2: Send the message: $ID_V, E_{K_{CH}}(ID_V || VID || K_{CV} || Yes/No || T)$ to the consumer.

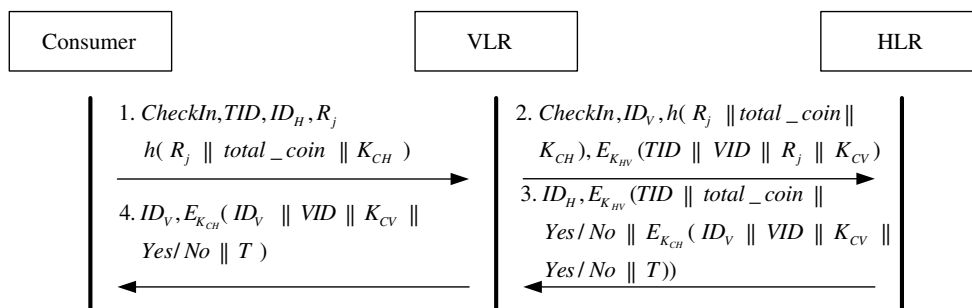


Fig. 6. Login VLR.

After Step 4, the consumer knows that he login VLR successful by the message *Yes*, and saves his temporary virtual identity *VID* and the shared key K_{CV} . All of the confidential messages are encrypted by the shared key K_{VH} , when the VLR wants to send them to HLR at Step 2. The confidential messages are secure.

3.2.5. Payment in the visited domain

Assume the consumer buys some products that cost x units of electronic coins in a merchant of visited domain network. The consumer pays x units of electronic coins to the merchant by the following steps. For generality, we assume that the consumer has spent j units of electronic coins before shopping in this merchant. The based point of electronic coins is R_j . The messages transmitted among the consumer, the merchant and VLR are shown in Fig. 7.

- Step 1: The consumer generates the payment information by performing the following sub-steps.
- 1-1: Compute $R_{j-x} = h^{j-x}(C_{\text{chainroot}})$ such that $R_j = h^x(R_{j-x})$.
 - 1-2: Send the message: *PurchaseInformation*, *VID*, ID_V , (R_j, R_{j-x}, x) , $h(K_{CV} \| ID_M \| R_{j-x} \| x)$ to the merchant.
- Step 2: Merchant verifies the value of electronic coins as follows:
- 2-1: Verify $R_j = h^x(R_{j-x})$.
 - 2-2: Send the message: ID_M , T , *VID*, (R_j, R_{j-x}, x) , $h(K_{CV} \| ID_M \| R_{j-x} \| x)$ to VLR.
- Step 3: VLR verifies the payment information via performing the sub-steps.
- 3-1: Verify the request does not exceed his quota and the based point R_j . If both the verifications are correct, then VLR performs Sub-step 3-2a, otherwise he performs Sub-step 3-2b.
 - 3-2a: Update consumer's based point to R_{j-x} and send the message: *VID*, *Yes*, $h(K_{VM} \| T \| x \| \text{Yes})$ to the merchant.
 - 3-2b: Set $x = 0$ and send the message: *VID*, *No*, $h(K_{VM} \| T \| x \| \text{No})$ to the merchant.

After Step 3, the merchant verifies $h(K_{VM} \| T \| x \| \text{Yes/No})$ to make sure the (R_j, R_{j-x}, x) is valid. The *PurchaseInformation* of Step 1 lists the products that the consumer ordered.

3.2.6. Consumer withdraws electronic coins in the visited domain

If the consumer runs out of his electronic coins in visited domain, he can withdraw electronic coins by performing the following steps. We assume that the consumer wants to withdraw n' units of electronic coins. Fig. 8 shows the messages transmitted among the consumer, VLR and HLR in this phase.

- Step 1: The consumer generates n' units of electronic coins as follows:
- 1-1: Pick a non-repeat number $C'_{\text{chainroot}}$.
 - 1-2: Compute $R'_{n'} = h^{n'}(C'_{\text{chainroot}})$.
 - 1-3: Send the message: *Withdrawal*, *VID*, $R'_{n'}$, $E_{K_{CH}}(R'_{n'} \| n' \| ID_V \| TID \| T)$ to VLR.
- Step 2: VLR changes and forwards this message to HLR as Sub-steps 2-1 and 2-2.
- 2-1: Change *VID* to *TID*.
 - 2-2: Send the message: *Withdrawal*, *TID*, $R'_{n'}$, ID_V , $E_{K_{CH}}(R'_{n'} \| n' \| ID_V \| TID \| T)$ to HLR.
- Step 3: HLR verifies the authority of the consumer as follows:
- 3-1: Decrypt the ciphertext to get that the consumer wants to withdraw n' units of electronic coins that starts with the based point $R'_{n'}$ and verify $R'_{n'}$. If the verification is correct, then HLR performs Sub-step 3-2a, otherwise he performs Sub-step 3-2b.
 - 3-2a: Deduct n' units of electronic coins from the consumer's account and send the message: ID_H , $E_{K_{HV}}(h(\text{Yes} \| R'_{n'} \| n' \| K_{CH}) \| TID \| R'_{n'} \| n' \| \text{Yes})$ to VLR.
 - 3-2b: Set $n' = 0$ and send the message: ID_H , $E_{K_{HV}}(h(\text{No} \| R'_{n'} \| n' \| K_{CH}) \| TID \| R'_{n'} \| n' \| \text{No})$ to VLR.
- Step 4: VLR gets the new quota and based point of the consumer by the following sub-steps.
- 4-1: Use shared key K_{HV} to get n' and $R'_{n'}$.
 - 4-2: Record the new quota and based point of the consumer.
 - 4-3: Send the message: *Yes/No*, $R'_{n'}$, *VID*, $h(\text{Yes/No} \| R'_{n'} \| n' \| K_{CH})$ to the consumer.

After Step 4, the consumer verifies $h(\text{Yes/No} \| R'_{n'} \| n' \| K_{CH})$ to make sure that he has got n' units of electronic coins.

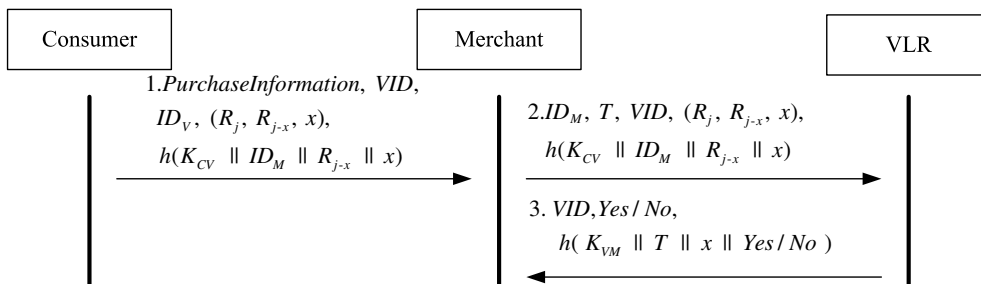


Fig. 7. Payment in visited domain.

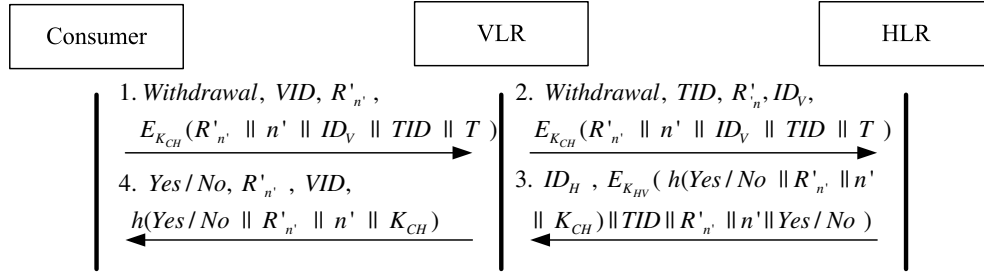


Fig. 8. Consumer withdraws electronic coins in the visited domain.

3.2.7. Logout VLR by the consumer himself

If the consumer wants to leave the visited domain, he can perform the following steps to logout. Without losing of the generality, we assume that the consumer has spent l units of electronic coins when he wants to logout from the visited domain. The based point of electronic coins is R_l . The messages transmitted among the consumer, VLR and HLR of this phase are shown in Fig. 9.

- Step 1: The consumer sends the message: *CheckOut*, VID , R_l , $h(K_{CH}||R_l||ID_V)$ to VLR.
- Step 2: VLR performs the following sub-steps to verify and settle the consumer's account.
- 2-1: Verify R_l .
 - 2-2: Settle the electronic coins that the consumer paid is $total_spent$.
 - 2-3: Send the message: *CheckOut*, TID , R_l , $total_spent$, $h(K_{CH}||R_l||ID_V)$, $h(K_{HV}||R_l||total_spent)$ to HLR.
- Step 3: HLR verifies $total_spent$ and generates a signature to VLR as follows:
- 3-1: Verify the consumer and VLR by K_{CH} and K_{HV} respectively.
 - 3-2: Verify $h^{total_spent}(R_l) = R_j$, where R_j is based point of electronic coins when consumer login VLR.
 - 3-3: Record R_l and $total_spent$.
 - 3-4: Update the consumption record of the consumer.
 - 3-5: Use his private key to sign a signature of $total_spent$ and send the message: TID , *Done*, $S_{K_H}(TID||ID_V||R_l||total_spent)$, $h(TID||R_l||K_{CH})$ to VLR.

Step 4: VLR verifies the signature and informs the consumer by the following sub-steps.

- 4-1: Verify the signature and save it.
- 4-2: Send the message: *Done*, $h(TID||R_l||K_{CH})$ to the consumer.

After Step 4, the consumer knows that he has logout from VLR.

3.2.8. The consumer logout from the old VLR by his HLR

If the consumer did not logout from old VLR by himself, and he wants to login a new VLR directly, HLR should perform the following steps to logout the consumer from the old VLR. For the generality, we assume that the consumer has spent l units of electronic coins before he login new VLR. The based point of electronic coins is R_l . Fig. 10 shows the messages transmitted in this phase.

- Step 1: HLR sends the message: *CheckOutByHome*, ID_H , TID , T , $h(TID||T||K_{HV})$ to the old VLR.
- Step 2: VLR settles the consumer's account as follows:
- 2-1: Verify $h(TID||T||K_{HV})$.
 - 2-2: Settle consumer's account, $total_spent = l - j$ (The consumer had spent j units of electronic coins before he login the old VLR).
 - 2-3: Send message: TID , R_l , $total_spent$, $h(TID||R_l||total_spent||K_{HV})$ to HLR.
- Step 3: HLR verifies and generates the signature in the following sub-steps.
- 3-1: Verify the equation $h^{total_spent}(R_l) = R_j$.

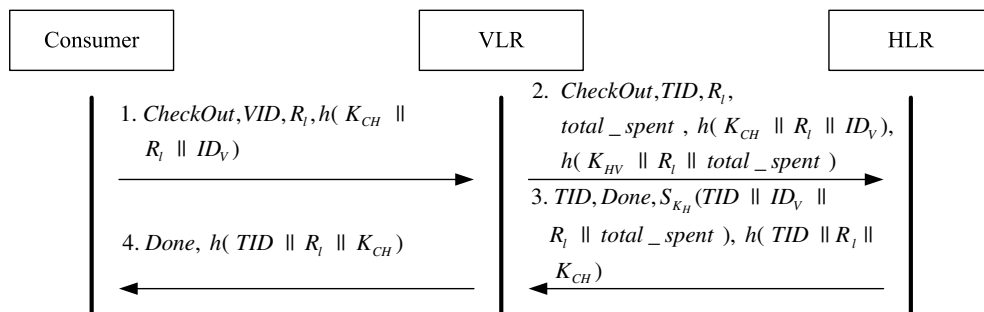


Fig. 9. Logout VLR by consumer himself.

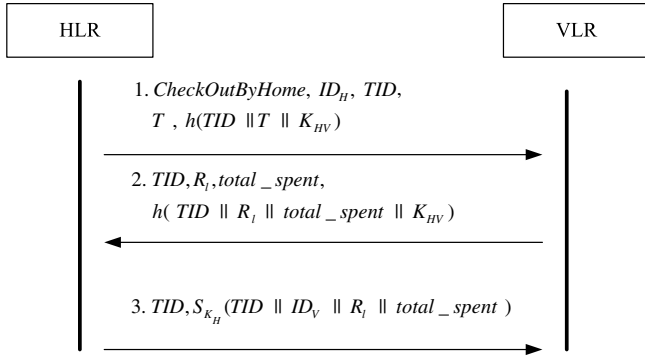


Fig. 10. The consumer logout from the old VLR by his HLR.

- 3-2: Record R_i .
- 3-3: Update the consumer's consumption record.
- 3-4: HLR uses his private key to sign $total_spent$ as receipt and sends the message: $TID, S_{K_H}(TID || ID_V || R_i || total_spent)$ to VLR.

After Step 3, VLR verifies the signature and saves it.

4. Security analysis

In this section, we analyze the security of the proposed scheme. In the home domain network, consumer uses temporary identity TID instead of real identity, so that merchants do not know consumer's real identity. In visited domain network, VLR only knows that consumer is one of valid subscribers of HLR. The consumer uses the virtual identity VID that VLR given to deal with merchants. Both of VLR and merchants do not know the consumer's real identity.

Both the withdrawals in HLR and VLR phase, the n units of electronic coins are represented by a hash chain: $R_0(=C_{\text{chainroot}}), R_1(=h(C_{\text{chainroot}})), \dots, R_{n-1}(=h^{n-1}(C_{\text{chainroot}})), R_n(=h^n(C_{\text{chainroot}}))$. The consumer should spend them by the order: $R_n, R_{n-1}, R_{n-2}, \dots, R_1, R_0$. The seed of hash chain, $C_{\text{chainroot}}$, is randomly selected by the consumer in the withdrawal phase. Nobody except the consumer knows the $C_{\text{chainroot}}$. By the properties of one-way hash function, no-

body can get $R_{i-1}(=h^{i-1}(C_{\text{chainroot}}))$ from $R_i(=h^i(C_{\text{chainroot}}))$. The consumer cannot deny that he has spent those coins. Our scheme provides the non-repudiation property.

The mobile network is an open channel and anybody can eavesdrop the transmitted message easily. In all phases of in our scheme, we use the symmetric encryption function to protect those confidential messages. The encryption key is the shared key of receiver and sender and they can authenticate each other. We also use the message authentication code (MAC) to provide the integrity of important messages. The proposed scheme provides the integrity and identity authentication.

The double-spending problem is an important issue of electronic payment. In our scheme, HLR or VLR will verify the payment information on-line. The merchant will provide those products to the consumer after he obtains the proof from the HLR or VLR. The proposed scheme prevents the double-spending problem.

5. Discussions

This section makes some comparisons among Huang and Chen's scheme, Chen et al.'s schemes and our scheme. The first item of the comparisons is the consumer's identity confidentiality aspect. Our scheme and Huang and Chen's scheme can achieve that, but Chen et al.'s scheme is fail in this point.

In interaction efficiency aspect, our scheme and Chen et al.'s scheme almost takes the same number of steps, but Huang and Chen's scheme takes extra steps to withdraw coins for each transaction. In addition, our scheme can deal with merchant, vender machine and WAP site. Huang and Chen's scheme just can deal with merchant and vender machine. Chen et al.'s scheme only can deal with WAP site.

In the withdrawal phase, our scheme takes $(n+2)T_h + 2T_{\text{sym}}$ time totally, while Huang and Chen's scheme takes $2T_h + 16T_{\text{exp}} + 10T_{\text{mul}} + T_{\text{div}} + T_{\text{add}}$ time and Chen et al.'s scheme takes $2nT_h + 4T_{\text{sym}}$ time. The consumer should take $(n+1)T_h + T_{\text{sym}}$ time to withdraw n units of electronic coins in our scheme, while he takes

Table 1
The comparisons of our, Huang and Chen's and Chen et al.'s schemes

	Our scheme	Huang and Chen	Chen et al.'s
Anonymous of the consumer	To merchant and VLR	To merchant and HLR	No
Rounds in withdrawal phase	2	6	2
Rounds in payment phase	3	1	3
The time cost of the withdrawal phase	$(n+2)T_h + 2T_{\text{sym}}$	$2T_h + 16T_{\text{exp}} + 10T_{\text{mul}} + T_{\text{div}} + T_{\text{add}}$	$2nT_h + 4T_{\text{sym}}$
The time cost of the payment phase	$(n^2/2 + n/2 + 4)T_h$	$T_h + 6T_{\text{exp}} + 3T_{\text{mul}}$	$(n^2/2 + n/2)T_h + 4T_{\text{pub}}$
The types of merchant	Merchant, vender machine and WAP site	Merchant and vender machine	WAP site
Need to withdraw for each payment	No	Yes	No
Support roaming	Yes	No	No
Merchant can counterfeit consumer	No	No	Yes

Note: T_h – the time to execute one-way hash function. T_{exp} – the time to execute modulus exponent. T_{pub} – the time to execute public key encryption or decryption. T_{mul} – the time to execute modulus multiplication. T_{div} – the time to execute modulus division. T_{add} – the time to execute modulus addition. T_{sym} – the time to execute symmetric encryption or decryption. n – the number of electronic coins that the consumer withdraws.

$T_h + 13T_{\text{exp}} + 9T_{\text{mul}} + T_{\text{div}}$ in Huang and Chen's scheme and he should takes $nT_h + 2T_{\text{sym}}$ in Chen et al.'s scheme to withdraw n units of electronic coins. Our scheme is more efficient.

In payment phase, our scheme totally takes $(n^2/2 + n/2 + 4)T_h$ time and consumer should take $(n^2/2 + n/2 + 1)T_h$ among these phase. Huang and Chen's scheme takes $T_h + 6T_{\text{exp}} + 3T_{\text{mul}}$ time and extra $T_h + 13T_{\text{exp}} + 9T_{\text{mul}} + T_{\text{div}}$ time to withdraw electronic coins. Chen et al.'s scheme takes $(n^2/2 + n/2)T_h + 4T_{\text{pub}}$ time and consumer should take $(n^2/2 + n/2)T_h$ time in it. Our scheme is more efficient in the payment phase. Table 1 summarizes the comparisons.

6. Conclusion

We propose a novel on-line mobile payment scheme that supports roaming service. In our scheme, no one except HLR knows consumer's real identity. We use MAC technique to protect data integrity and identity authentication. Our scheme can deal with different type of merchants such as: shop, vendor machine and WAP site. It is more practical. Our scheme only uses one-way hash function and symmetric encryption, so we have high performance and easily apply it in mobile device that claims low computing and less memory storage. Our scheme is practical and efficient in mobile e-commerce.

Acknowledgement

This work was partially supported by the TWISC@NTUST project sponsored by the National Science Council, Taiwan.

References

- [1] A. Herzberg, Micropayments, in: W. Kou (Ed.), *Payment Technologies for E-Commerce*, Springer, New York, 2003, pp. 245–282.
- [2] A. Odlyzko, The case against micropayments, in: *Proceedings of FC 2003, Lecture Notes in Computer Science*, vol. 2742, Springer, Berlin, 2003, pp. 77–83.
- [3] R.L. Rivest, A. Shamir, PayWord and MicroMint: two simple micropayment scheme, *CryptoBytes* 2 (1996) 7–11.
- [4] S.M. Yen, PayFair: a prepaid internet ensuring customer fairness micropayment scheme, *IEEE Proceedings of Computers and Digital Techniques* 148 (2001) 207–213.
- [5] L. Michael, Micropayments: an idea whose time has passed twice? *IEEE Security and Privacy* 2 (1) (2004) 61–63.
- [6] J.F. Stach, E.K. Park, K. Makki, Performance of an enhanced GSM protocol supporting non-repudiation of service, *Computer Communications* 22 (1999) 675–680.
- [7] P. Vishwas, R.K. Shyamasundar, An efficient, secure and delegable micro-payment system, in: *Proceedings of the 2004 IEEE International Conference on e-Technology, e-Commerce and e-Service (EEE'04)*, Taiwan, 2004, pp. 394–404.
- [8] B. Yang, H. Garcia-Molina, PPay: micropayments for Peer-to-Peer Systems, in: *Proceedings of the 10th ACM Conference on Computer and Communication Security, USA*, 2003, pp. 300–310.
- [9] J. Zhu, N. Wang, J. Ma, A micro-payment scheme for multiple-vendor in M-Commerce, in: *Proceedings of the 2004 IEEE International Conference on E-Commerce Technology for Dynamic E-Business (CEC-East'04)*, 2004, pp. 202–208.
- [10] M. Jakobsson, J.-P. Hubaux, L. Buttyan, A micro-payment scheme encouraging collaboration in MultiHop cellular networks, in: *Proceedings of FC 2003, Lecture Notes in Computer Science*, vol. 2742, Springer, Berlin, 2003, pp. 15–33.
- [11] Z. Huang, K.F. Chen, Electronic payment in mobile environment, in: *Proceedings of 13th International Workshop on Database and Expert Systems Applications (DEXA 2002)*, France, 2002, pp. 345–349.
- [12] S. Brands, Untraceable off-line cash in wallet with observers, *Advances in Cryptology – CRYPTO'93* 773 (1993) 302–318.
- [13] Y.H. Chen, Y.H. Liu, Y.Y. Chen, C.H. Song, Online checking micro-payment system in the mobile environment, in: *Proceeding of the Second International Workshop for Asian Public Key Infrastructures (IWAP 2002)*, Taiwan, 2002, pp. 142–146.
- [14] N. Asokan, P.A. Janson, M. Steiner, M. Waidner, The state of the art in electronic payment systems, *Computer* 30 (1997) 28–35.
- [15] S. Kungpisdan, B. Srinivasan, P.D. Le, A secure account-based mobile payment protocol, in: *Proceedings of the International Conference on Information Technology: Coding and Computing (ITCC'04)*, vol. 1, USA, 2004, pp. 35–39.
- [16] U. Varshney, Mobile payments, *Computer* 35 (2002) 120–121.