

# An Efficient and Secure Credit Card-based Billing Scheme for Telephone Services

Chern-Tang Lin and Shiuh-Pyng Shieh

Department of Computer Science and Information Engineering,

National Chiao Tung University, Hsinchu, Taiwan

## Abstract

*MasterCard and VisaCard use credit cards to support a number of services, such as Masterphone or Visaphone, which allow cardholders to make phone calls from any telephone. However, these services take little or no security precautions. Although SET protocol has defined a secure payment method for card transactions over open networks, it cannot fit in telephone systems. In this paper, we propose a credit card-based payment scheme for public switched telephone systems. The proposed scheme can securely authenticate callers without exposing their secret information on the telecommunication networks. And the scheme also supports anonymity of callers, that is, the telephone company does not know who make these phone calls and the credit card company does not know who are callees.*

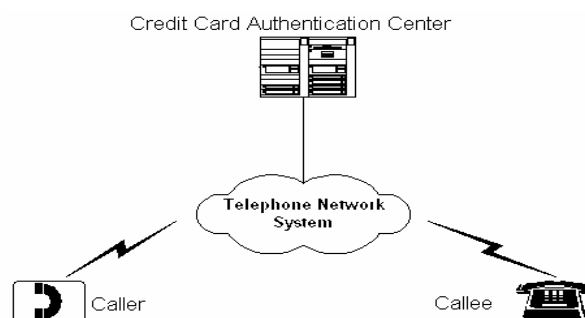
## 1 Introduction<sup>+</sup>

Masterphone and Visaphone services allow cardholders to make phone calls from any telephone [3]. These services provide a convenient means for making international long distance calls via cards for tourists. To use overseas access or to make a chargeable local call, it is common to call a toll free service number and give the operator the caller's card number, personal identification number, and the callee's phone number. The call will be connected after the verification of account details. Then the cost of calls will be automatically debited the card owner's account. This mechanism is practicable for all telephones but burdensome for callers. Another application is that the telephones with wipe readers allow people to make calls using commercial credit

cards as well as coins [5]. To make a call, the customer wipes his/her credit card through the reader of the phone, waits for authorization and then dials the callee's number. Charges for these calls appear on cardholders' monthly statements from their card company.

In today's credit card-based telecommunication services, the credit card numbers and personal identification numbers are often transmitted from cardholders to the telephone company over the telephone line without security precautions. However, this information provides the key elements needed to create counterfeit cards or fraudulent telephone calls. Thus, they should not be exposed to the telephone network system in plaintext form. The goal of this paper is to propose a method for the authentication of users without leaking users' secret information, such as the credit card numbers.

A simple credit card phone environment is shown in Figure 1. The authentication process takes place between the caller and the credit card authentication center (CCAC). CCAC is a gateway to check the authority of the caller. During the authentication process, the telephone company authenticates a

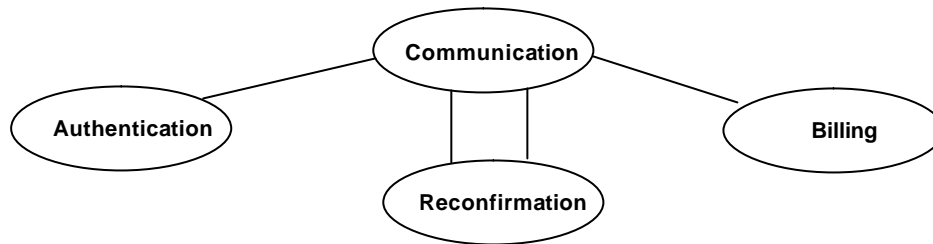


**Figure 1: Credit card Phone System**

caller only via CCAC and should not get both the credit card numbers and personal identification numbers. In addition, CCAC should not get the caller's location and the callee's phone number to

---

<sup>+</sup> This work was supported in part by the Computer and Communications Lab., Industrial Technology Research Institute, Taiwan.



**Figure 2: The state transition of the proposed protocol**

protect the privacy of the cardholder. Thus, the anonymity of customers can be guaranteed.

After the authentication process, the telephone company must get some evidences from CCAC and the caller. The evidence is a kind of digital signature to prove the user has made phone calls. The telephone company can charge the credit card company the cost of calls by the evidences. Then the credit card company will send the bill to its customers.

We proposed a secure credit card-based billing schemes for the public switched telephone network [17]. This scheme can authenticate callers via CCAC and guarantee the confidentiality of callers' secret information. This scheme can be also applied to mobile telecommunication systems [1, 2, 7, 8, 14], such as GSM [10]. But it has some disadvantages: 1) the caller needs a hand held authentication card to calculate the response for the authentication protocol, 2) the telephone must support encryption/decryption functions, and 3) this scheme needs 7 messages for the authentication and 4 messages for each reconfirmation to continue the conversation. The communication cost is heavy for networks which bandwidth is critical.

In this paper, we propose a new credit card-based billing scheme for the public switched telephone network. The credit card is a common IC card. The caller only needs to insert the card to the reader of telephone and dial the callee's phone number. The authentication process is automatically progressed by the card. Since the calculation of encryption/decryption is performed in the IC card, the telephone does not need any computation power except supporting an extra card-reader. In addition, our new scheme needs only 5 messages for the authentication and 2 messages for each reconfirmation to continue the conversation. This scheme is also suitable for mobile telecommunication networks.

In our scheme, we also assume that the credit card can authenticate the user directly, such as using a personal identification number (PIN) shared between the card and its owner. And the public key cryptosystem is used for the authentication between the caller and the CCAC. The authentication protocol uses the synchronized nonce scheme [16] to prevent the messages from replay attacks. Since signing documents with the private key cryptosystem is difficult, the public key cryptosystem is adopted to generate the digital signature as the evidences of calls. The public key cryptosystem also helps create a secure communication conveniently via the telephone network system.

Recently, Visa and MasterCard have jointly developed the Secure Electronic Transaction (SET) protocol as a secure payment method for card transactions [15]. In SET specifications, a cardholder is presented with an order form containing the list of items, their prices, and a total price including shipping, handling and taxes. The cardholder sends the merchant a completed order, which is digitally signed by cardholders who possess certificates. This method cannot be adapted easily to the credit card-based telephone service because a telephone charge cannot be determined until the conversation is over. After the telephone conversation, the caller may evade or refuse to sign the bill. So, the signed messages must be acquired in the telephone conversation. To resolve the problem, we design a virtual phone card scheme for our secure credit card-based billing scheme. This scheme needs two messages for each reconfirmation to continue the conversation.

In the paper, we will outline the credit card-based telecommunication system environment and propose a communication protocol in Section 2 and 3. The analysis for the proposed protocol will be presented in Section 4. Finally, we will give our conclusions in Section 5.

## 2 Secure Credit Card Phone Environment and Notations

As the credit card phone environment shown in Figure 1, we assume that the caller is Alice and the callee is Bob. The entire process can be divided into four states shown in figure 2. When Alice makes a call to Bob via the telephone network system with a credit card, the telephone company will request the CCAC whether or not she can make this call. The challenge of the user authentication is how to guarantee the confidentiality of user's secret information, such as the credit card number. If the CCAC authorizes her to make the call to Bob, the telephone network system will provide communication channel between Alice and Bob.

Since a telephone charge cannot be determined until the conversation is over, we use a periodic payment scheme, called the virtual phone card (VPC) scheme. In the scheme, CCAC must give the authorized caller a VPC for each call. Before the conversation, the caller must generate a communication evidence from the VPC and give the telephone company the evidence which will allow the conversation for a predefined interval. At the ending of the interval, the telephone company should reconfirm whether the caller would continue this conversation. If yes, the telephone company will get another evidence from the caller and continue supporting this communication channel. Otherwise, the communication line will be broken. By these communication evidences, the telephone company can get the telephone charge from Alice's credit card account later. But the challenge of the periodic payment scheme is how to reduce the overhead of reconfirmation in order to keep the smooth of communications.

For user authentication, we use a modified challenge-response protocol. In general challenge-response protocol [12], the system gives the user a nonce (a challenge) and the user must return a response based on this nonce and some secret shared between the system and user. Then the system can authenticate the user by checking if the response is correct or not. The advantage of the scheme is that the protocol does not use timestamps to prevent messages from replay attacks. Thus, the clock synchronization between the system and user is unnecessary. This feature is useful for mobile IC cards because it is difficult to synchronize both clocks in CCAC and the IC card. But the disadvantage

is that the whole protocol needs more messages than the protocols based on the timestamp scheme.

In our authentication protocol, we adopt the synchronized nonce scheme to reduce the number of messages needed in the challenge-response mode. The IC card must previously share a synchronized nonce (named as an authentication token) with CCAC. While the authentication is needed, the IC card directly generates the response with the token and gives CCAC the response. If the response is correct, CCAC gives the caller a VPC for this call. And a new authentication token is also sent to the IC card for the next authentication. In this way, the number of messages for the whole protocol will be reduced. (The authentication protocol presented in [17] needs 7 messages; the new scheme in this paper needs only 5 messages.)

Since users' credit card numbers are sensitive data, they should not be revealed as well as sent in plaintext form to the telephone company. For this reason, we also use the token to identify the caller (IC card). Since each token is different, the telephone company will not know who makes this phone call. In addition, we assume that caller's IC card has the public cryptosystem that support secure communication channels with CCAC and sign the evidences for the conversation. In this way, the telephone company can use evidences to charge users such that the user cannot deny the calls he/she made.

The following notations are used in the description of our proposed protocol:

- $C$ : The credit card authentication center (CCAC) which has a pairs of key  $(P_C, S_C)$ , where  $P_C$  is the public key;  $S_C$  is the secret key. Although CCAC is just a part of the credit card company, for simplification, we also use  $C$  to denote the whole company.
- $T_1$ : The caller's (Alice's) telephone which must store the identity of its telephone company within the machine. Besides, this telephone must also support a card reader to access users' IC cards. Note that  $T_1$  is also used as the identity of the caller's telephone in the message.
- $T_2$ : The callee's (Bob's) telephone which is a common telephone.  $T_2$  also denotes the callee's telephone number.
- $N$ : The telephone network system. Note that  $T_1$

should belong to the telephone company  $N$ , but  $T_2$  can belong to any company. As the usage of  $T_1$ ,  $N$  is also used as the identity of the telephone company.

-  $A$ : Alice's credit card (IC card) which must support a public key cryptosystem and have a pair of keys  $(P_A, S_A)$ , where  $P_A$  is the public key;  $S_A$  is the

$VC_0 = VPC$  and  $t_i$  is the expiration time of  $VC_i$ .  $N$  collects these virtual coins as conversation evidences to get the telephone charge from Alice's credit card account.

-  $\{message\}K$ : An encrypted message which uses  $K$  as the key.

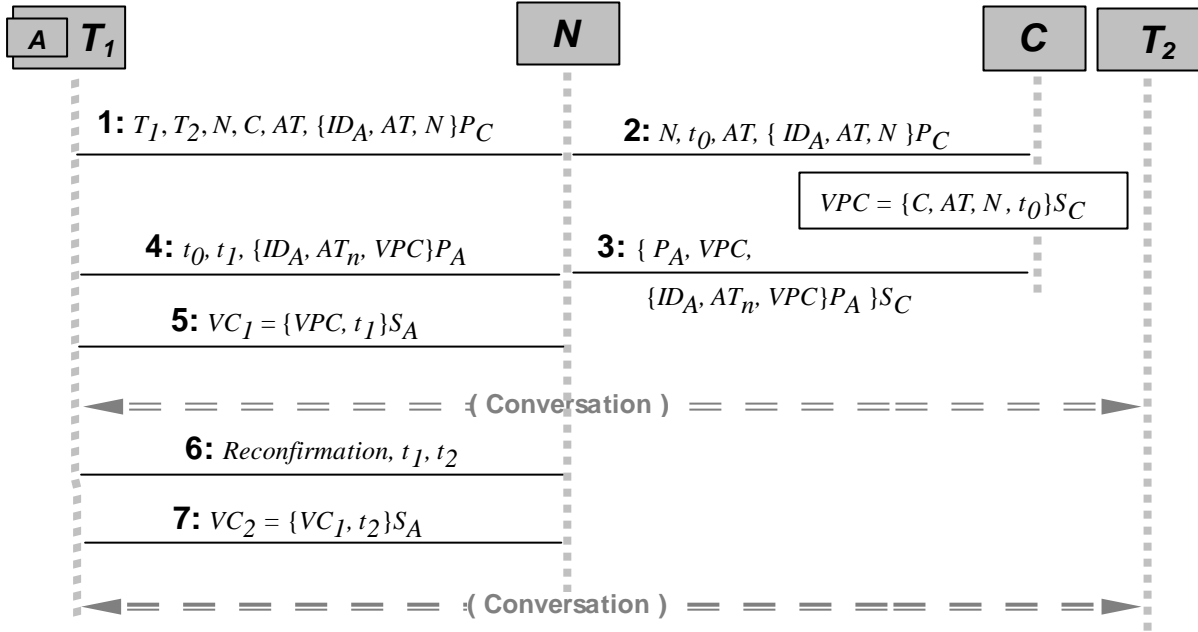


Figure 3: The efficient and secure credit card-based billing scheme

secret key.

-  $ID_A$ : Alice's credit card number. To guarantee Alice's privacy,  $ID_A$  should be known only by  $A$  and  $C$ .

-  $AT$ : The authentication token of  $A$ . In the paper,  $AT$  denotes the token which is stored in  $A$  or is being used in the current call and  $AT_n$  denotes the new token used for the next call.

-  $VPC$ : The virtual phone card issued by  $C$  for this phone call. This message is signed by  $C$  and denotes that  $C$  authorizes  $A$  to make the credit card phone.  $C$  uses  $VPC$  to prove for  $N$  that  $A$  is a legal credit card user, and to inform  $A$  that she is allowed to make this call.

-  $t_i$ : Timestamps issued by  $N$ .

-  $VC_i$ : The virtual coin issued by  $A$ , and  $i = 1, 2, \dots, j$ . The coin is based on the value  $VC_{i-1}$  and  $t_i$ , where

### 3 The Secure Credit Card-based Billing Scheme

The credit card-based billing scheme is shown as Figure 3.

**Step 1:** Alice inserts her credit card  $A$  to the card reader of  $T_1$ . First, Alice dials her personal identification number (PIN) to enable the card. If PIN is correct,  $A$  will get the identity of the telephone company  $N$  from  $T_1$  and generate the message  $X_{11} = \{ID_A, AT, N\}P_C$ . Then  $A$  will give  $T_1$  the following data: the identity of CCAC  $C$ , its authentication token  $AT$ , and the message  $X_{11}$ . Finally, Alice dials the callee's telephone number  $T_2$ , and  $T_1$  sends the message  $(T_1, T_2, N, C, AT, X_{11})$  to  $N$ .

**Step 2:** When the telephone network system  $N$  receives the message, it will verify if  $C$  is a legal and contracted credit card company that supports the service of credit card phone. If

yes, it will keep the data  $T_1, T_2, C$ , and  $AT$  in the database itself. Then  $N$  generates a timestamp  $t_0$  that denotes the startup time for billing. And the message  $X_{21} = (N, t_0, AT, X_{11})$ , where  $X_{11}$  was received from  $T_1$ , is sent to  $C$ .

**Step 3:** The credit card authentication center  $C$  uses its secret key  $S_C$  to decrypt the message  $X_{11}$ . Then  $C$  knows the caller's credit card number  $ID_A$ , the authentication token  $AT$ , and the telephone company  $N$ . Since only  $C$  and  $A$  know the credit card number  $ID_A$  and the current token  $AT$ ,  $C$  can distinguish whether the message is new and generated for a phone call by  $A$ . If the verification is successful, the message  $X_{11}$  is not masqueraded.  $N$  hence is the telephone company which is chosen by the caller to deliver the call.

After the authentication,  $C$  makes sure whether  $t_0$  is within the valid interval or not. If  $t_0$  is much larger or smaller than the local clock in  $C$ , the message may be modified by a hostile or masqueraded by  $N$  itself.  $C$  thus discards the message and denies the request for the phone call. Otherwise,  $C$  generates a virtual phone card  $VPC = \{C, AT, N, t_0\}S_C$  for this phone call, and randomly selects a new authentication token  $AT_n$  for  $A$ . To secretly transmit  $AT_n$  to  $A$ ,  $C$  uses  $A$ 's public key to generate the message  $X_{31} = \{ID_A, AT_n, VPC\}P_A$ . Then  $C$  sends  $N$  the message  $X_{32} = \{P_A, VPC, X_{31}\}S_C$ . Note that  $A$ 's public key  $P_A$  is encapsulated in  $X_{32}$ . That is because  $N$  does not know  $A$ 's credit card number and its public key.

**Step 4:** After receiving  $X_{32}$ ,  $N$  uses  $C$ 's public key to verify the message:  $P_C$  is used to decrypt  $X_{32}$  to get  $P_A, VPC$ , and  $X_{31}$ .  $P_C$  is used again to decrypt  $VPC$  to get four numbers:  $C', AT', N'$ , and  $t'$ . If 1)  $C'$  and  $N'$  is respectively equal to  $C$  and  $N$ , 2)  $AT'$  is equal to  $AT$  received from  $A$  in Step 2, and 3)  $t'$  is equal to the timestamp  $t_0$  that  $N$  itself sent to  $C$  in Step 2,  $VPC$  is a legal virtual phone card. That is,  $C$  has authenticated the caller as a legal credit card user and permitted her to make the credit card phone. Since  $VPC$  is trusted,  $P_A$  is also trustworthy. Then  $N$  generates a new timestamp  $t_1$  that indicates the expiration time of the first

conversation interval. And  $N$  sends  $T_1$  the message  $X_{41}$  that contains the startup time  $t_0$ , the expiration time  $t_1$ , and the message  $X_{31}$ .

**Step 5:** When  $T_1$  receives  $X_{41}$ , it forwards the message to the IC card  $A$ .  $A$  uses its secret key to decrypt the ciphertext  $X_{31}$  and adopts the same process mentioned in Step 4 to verify whether  $VPC$  is legal. If  $VPC$  is legal,  $A$  generates a virtual coin  $VC_1$  as the first evidence of the following conversation interval, where  $VC_1 = \{VPC, t_1\}S_A$ .

While  $N$  receives  $VC_1$ , it should use  $A$ 's public key  $P_A, VPC$ , and  $t_1$  to verify whether the evidence is legal. If yes, it establishes the communication channel between  $T_1$  and  $T_2$ . The virtual coin should be collected to charge the credit card company the cost of calls in the future.

**Step 6:** In advance, the telephone network system  $N$  needs to negotiate a reconfirmation interval with the credit card authentication center  $C$  by a contract. If the conversation between  $T_1$  and  $T_2$  is longer than the interval time,  $N$  should issues a reconfirmation signal to  $T_1$  periodically. The reconfirmation message should contain the expiration time of the next interval ( $t_2$  in Figure 4).

**Step 7:** When  $T_1$  receives the reconfirmation message, it forwards the message to  $A$ . Then  $A$  will generate a new virtual coin  $VC_2 = \{VC_1, t_2\}S_A$  and send it to  $N$  as the next conversation evidence.

$N$  also needs to verify whether the evidence is legal with  $A$ 's public key  $P_A, t_2$ , and the old evidence  $VC_1$ . If yes, the channel between  $T_1$  and  $T_2$  is kept for another time interval. And the evidence  $VC_2$  is saved.

Suppose  $VC_j = \{VC_{j-1}, t_j\}S_A$  is the last evidence. The telephone company  $N$  sends  $C$  the message  $(N, C, AT, t_0, t_j, VPC, VC_j)$  as a bill for the charge of this call. When  $C$  gets this bill, the token  $AT$  and the startup time  $t_0$  are used as indices to search the corresponding credit card number  $ID_A$  and its public key  $P_A$ . Then  $C$  verifies the virtual coin:

- 1) Decrypt  $VPC$ . Check if the content is equal to  $(C, AT, N, t_0)$  or not.
- 2) Repeatedly decrypt the virtual coin  $VC_j$  for  $j$  times to get the result  $(VPC', t_1)$ . Check if  $VPC'$  is equal to  $VPC$  or not.
- 3) Check if the time list  $(t_0, t_1, \dots, t_j)$  computed from

the above step is valid (the sequence should be monotonically increased and the interval should be equal to the predefined value).

If it is correct,  $C$  has to pay this call. The charge of this call will appear on the caller Alice's monthly credit card statements.

In addition to the public switched telephone networks, this billing scheme can be also applied to mobile telecommunication systems, such as GSM. It is essential to the convenience of calling. No matter where a caller is, he can borrow a handset nearby to make a phone call. Owner of the handset will not be responsible for the charge of this call. The expense of calls will be charged to the caller's credit card account.

## 4 Protocol Analysis

Since in telephone systems, we cannot guarantee the caller is in a secure environment. Thus, it is very important to protect callers' privacy and guarantee that the telephone company can charge the money for the phone calls it served. The proposed scheme can not only support the authentication of callers to guarantee they will pay for these calls via their credit card accounts, but also has three important features:

- 1) **Confidentiality.** In the protocol, all sensitive data is encrypted with the receiver's public key, and only the desired receiver can decrypt and share the information. Consequently, we can make sure that the credit card number  $ID_A$  is never disclosed and shared only by the credit card  $A$  and CCAC  $C$ . With this shared secret, nobody can forge  $X_{11}$ , and  $C$  can verify if the request is issued by  $A$ . Note that the new token  $AT_n$  is also kept secret in Step 3 and 4. If the token is transmitted in the plaintext form, it is possible to be hostilely modified. Both values of  $AT_n$  in  $C$  and  $A$  will be different, so the authentication for the next phone call will fail.
- 2) **Anonymity.** Since  $A$  and  $C$  do not expose the credit card number  $ID_A$  in messages, the telephone company does not know who make the phone call. In addition,  $T_1$  and  $T_2$  are known only by  $N$ , the credit card company cannot use these information to trace where its customer made the call and know who is the callee. The personal privacy is protected. Of course, if there exists an argument about the bill,  $C$  and  $N$  can cooperate

to disclose the details of the phone calls, such as  $ID_A$ ,  $T_1$ ,  $T_2$ , and  $t_0$ .

- 3) **Efficient reconfirmation.** The proposed protocol adopts a periodic payment scheme to resolve the problem that the caller may repudiate he/she made a call. A phone call consists of many conversation intervals. At the ending of an interval,  $N$  must reconfirm whether the caller will continue the conversation. If yes, the caller must give  $N$  a 'coin' to buy the next conversation interval. As the reconfirmation phase needs only two messages shown in Section 3, the time spending for the reconfirmation is very short.

The virtual coin (see Step 7 in Section 4) is based on the previous coin or the virtual phone card  $VPC$ , and signed by the caller himself.  $VPC$  is signed by the credit card company  $C$  and verified by  $N$  in Step 4 and by  $A$  in Step 5. Thus, with the virtual coins and the corresponding  $VPC$ , neither the caller nor  $C$  can repudiate that the phone call was made. Since  $N$  can drop all coins except the last one  $VC_j$  to charge the phone call, the space for recording a phone call is also very small. Therefore, the proposed payment scheme is efficient and practical for the phone service, even the period of the reconfirmation is short.

There are four kinds of assailant in the system: outsiders, the caller, the credit card company  $C$  and the telephone company. Anyone, who wants to make a toll-free call, he/she should generate a victim Alice's credit number  $ID_A$  and the authentication token  $AT$  to generate the message  $X_{11}$  and to impersonate Alice. Since our protocol guarantees the confidentiality of all sensitive data, such as  $ID_A$  and  $AT$ , impersonating a victim to make a phone call is difficult except that he/she conspires with the credit card company.

But, in the payment system,  $C$  must be trustful and impartial. If a caller conspires with the credit card company, the caller can impersonate a victim and cheat the telephone network system  $N$ . In this way, the telephone company will believe a forged evidence and bill the victim. Consequently,  $C$  can collect the payment from a victim's account. The fraud hurts customers' interest. Therefore, CCAC must be impartial and trustful. Furthermore, since the telephone company does not have the credit card authentication center  $C$ 's secret key  $S_C$  and the caller's secret key  $S_A$ , it cannot produce a forged evidence.

## 5 Conclusions

Since the credit card does not have the limitation of many physical mechanisms, everyone can register more than one credit card number. The use of credit card to pay the charge of services is very convenient. In this paper, we propose a secure payment scheme for public switched telephone networks with which the expense of calls will be charged from the cardholder's account. This protocol is also suitable for mobile telecommunication networks, such as GSM. The proposed protocol spends five messages to authenticate the caller. A telephone company, through these messages, can distinguish whether the caller is a legal cardholder and the credit card account is chargeable. Furthermore, we design a periodic payment scheme which requires only two messages to reconfirm the next conversation interval. Thus the protocol is very efficient and practical. Besides, the protocol also guarantees the confidentiality of sensitive data transmitted in the telecommunication networks. Finally, the protocol can guarantee the anonymity of the caller. Thus the telephone company does not know the caller's credit card number, and the credit card company does not know both where the caller is and who the callee is.

## Reference

- [1] Beller, "Privacy and Authentication on a Portable Communications System", IEEE Journal on Selected Areas in Communications, vol. 11, no. 6, August 1993.
- [2] V. Bharghavan, "Secure Wireless LANs", ACM, pp.10-17, 1994.
- [3] CitiBank, "Masterphone Service", (<http://www.citibank.com/argentina/e/gc/arcpdbaa.htm>), 1996.
- [4] Chenturvasan Duraiappan and Yuliang Zheng, "Enhancing Security in GSM", Proceedings of International Computer Symposium, pp.297-302, 1994.
- [5] Hongkong Telecom, "International Calls", (<http://hkt.net/international.htm>), 1996.
- [6] Internet Bank of DISCS, "Electronic Commerce", (<http://137.132.88.57/Ibank/chap2.htm>), 1996.
- [7] Refik Molva, Didier Sarmfat and Gene Tsudik, "Authentication of Mobile Users", IEEE Network, pp.26-34, March/April 1994.
- [8] Yi Mu and Vijay Varadharajan, "On the Design of Security Protocols for Mobile Communications", 1996.
- [9] NetPartners, "CRYPTO Card", (<http://www.netpart.com/crypto/tokens.html>), 1996.
- [10] Moe Rahnema, "Overview of the GSM System and Protocol Architecture", IEEE Communications Magazine, pp.92-100, April 1993.
- [11] Kenvin M. Savetz and Andrew Sears, "FAQ: How can I use the Internet as a telephone?", ver. 0.5, July 25 1996.
- [12] Bruce Schneier, "Applied Cryptography: protocols, algorithms, and source code in C", 2<sup>nd</sup>, pp.47-74, 1996.
- [13] M. Tatebayashi, N. Matsuzaki and D.B. Newman, "Key Distribution Protocol for Digital Mobil Communication System", Advances in Cryptology - Crypto' 89 Proceedings, pp.324-334, 1990.
- [14] Vijay Varadharajan and Yi Mu, "Design of Secure End-to-End Protocols for Mobile Systems", Wireless' 96.
- [15] Visa and MasterCard, "Secure Electronic Transaction (SET) Specification, Book 1: Business Description", June 17 1996.
- [16] C. T. Lin and S. P. Shieh, "Chain Authentication in Mobile Communication Systems," in revision, Journal of Telecommunication Systems

- [17] S. P. Shieh, C. T. Lin, M. J. Peng, W.C. Yang, and J.N. Yang, "A Secure Credit-Card Based Billing Schemes for Telephone Services," International Conference on Mobile Computing, March 1998.