南　　華　　大　　學

資訊管理學系

碩士論文

模糊傳輸及車載隨意網路的加密系統之研究

Subscriber the cryptosystem of OT and VANETs

研 究 生：許彰原

指導教授：周志賢

中華民國 九十七年 六月

南　華　大　學

（資訊管理學系）

碩 士 學 位 論 文

模糊傳輸及車載隨意網路的加密系統之研究
Subscriber the cryptosystem of OT and VANETs

研究生：許勤原

經考試合格特此證明

口試委員：

指導教授：周志賢

系主任(所長)：

口試日期：中華民國 97 年 6 月 26 日

誌　　謝

在資管所兩年的學習過程，隨著論文的付梓，即將劃上句點，這段時間以來的點點滴滴，有回憶，有不捨；回憶之情將在我的懷中日漸晶瑩光耀，不捨之心將使我的人生成就勇氣。

本論文能順利完成，幸蒙指導教授周志賢博士指導與教誨，對於研究的方向、觀念的啟迪、架構的匡正、資料的提供與求學的態度逐一斧正與細細關懷，於此獻上最深的敬意與謝意。論文口試期間，承蒙口試委員莊振村與廖怡欽老師力鵬的鼓勵與疏漏處之指正，使得本論文更臻完備，在此謹深致謝忱。

在研究所修業期間，感謝雅玲學姐、小伍學長及同窗伙伴宗亨、啟峰兩年來的切磋討論與鼓勵，獲益良多，永難忘懷。並對於所有幫助過我、關懷過我的人，致上由衷感謝。最後，特將本文獻給我最敬愛的母親，感謝您無怨無悔的養育與無時無刻的關懷照顧，還有父親及家人在經濟上與精神上的支持，讓我能專注於課業研究中，願以此與家人共享。

模糊傳輸及車載隨意網路的加密系統之研究

學生：許彰原　　指導教授：周志賢

南　華　大　學　資訊管理學系碩士班

摘　　要

安全和效率是加密系統上關鍵的問題。許多研究致力了於這兩個問題。但是, 大多協議是不安全或不是效率。因此, 在本文裡, 我們建構了基於雙線性之高效率且班全 n 選 k 的模糊傳輸機制和在車載隨意網路上通信安全機制。我們並且分析我們的計劃安全和效率。在以後分析, 我們能推斷我們 OT 機制是不僅安全比所有這其他現有機制在帶寬消耗量還更高效率而我們在車載隨意網路上通信機制是第一個能抵抗中間人攻擊, KCI 攻擊, 平行攻擊, 和達到相互認證。

Subscriber the cryptosystem of OT and VANETs

Student：Chang-Yuan Advisors：Dr. Jue-Sam Chou

Department of Information Management
The M.I.M. Program
Nan-Hua University

ABSTRACT

Security and efficiency are crucial issues in cryptosystem. Many researches have devoted to these two issues. However, most of the protocols are insecure or not efficiency. Henceforth, in this paper, we construct an efficient secure k-out-of-n oblivious transfer scheme and a communication secure scheme on VANETS based on bilinear pairings. We also analyze the security and efficiency of our schemes. After analyze, we can conclude that our OT scheme is not only secure but also more efficient in bandwidth consumption than all of the other existing oblivious transfer schemes and our communication scheme in VANETS is the first scheme which can against man-in-middle-attack, KCI attack, parallel session attack, and achieve mutual authentication.

Table of Contents

List of Table

List of Figures

Chapter 1 Introduction

Recently, computer networks and the amount of information increased fast and large. Hence, the technology of the cryptography also broadly applied in many areas such Oblivious Transfer (OT) and Vehicular Ad Hoc Networks. So, the cryptography protocol will become very important in the application area. Security and efficiency are crucial issues in cryptosystem. Many researches have devoted to these two issues. In this paper, we study some researches in OT and VANETs and we find some protocol are insecure or not efficiency. Henceforth, we construct an efficient secure OT scheme and a secure communication scheme on VANETs based on bilinear pairings.

This paper is organized as follows. The introduction is presented OT and VANETs in Chapter 1.1 and 1.2. Preliminary is shown in Chapter 2. In Chapter 3, we review Li et al.'s scheme[9] and present their weakness. Then, we show our protocol in Section 4. In Section 5, we will analyze the security and performance of our protocol. Finally, a conclusion is given in Section 6

1.1 Oblivious Transfer

Oblivious transfer (OT) has become an important primitive for designing secure protocol. Because it has an important feature, the sender cannot know which part of the transmitted messages the receiver will receive and the receiver cannot obtain extra messages that he had not chosen in advance, that can be applied in privacy protection. The original

OT was proposed by Rabin [32] in 1981. In the scheme, Alice sends a bit to Bob and Bob only has 1/2 probability to receive the bit. Subsequently, there are many flavors for OT schemes such as 1-out-of -2 OT(OT_2^1)[1,2,17,33,35], 1-out-of-n OT(OT_n^1)[18,36,37], k-out-of-n OT(OT_n^k)[6,11,12,15,16,28], adaptive OT_n^k [14,25], interactive OT and non-interactive OT[35,38,39]. In 1985, Even et al.[34] first proposed a general OT scheme, 1-out-of-2 OT(OT_2^1), in which the sender sends two messages to the receiver, and the receiver can receive only one of them. In 1987, Crepeau [3] proved that OT_2^1 and Rabin OT are computationally equivalent. One extension of OT_2^1 is 1-out-of-n OT (OT_n^1) in which the sender sends n messages to the receiver, and the receiver can only receive one of them. The more general form is k-out-of-n OT (OT_n^k), in which the sender sends n messages to the receiver, and the receiver can receive k of them. In adaptive OT_n^k , the sender sends n messages to the receiver, and the receiver can learn k of them in an adaptive manner. Most previous OT_n^1 schemes cannot be easily used to construct OT_n^k . They need to be run k times to construct an OT_n^k scheme. Another form of OT is non-interactive. It means that the receiver doesn't need to communicate with the sender during an OT process. It is a variation of interactive OT scheme, since the receiver had chosen the wished message in advance in the setup phase.

In 2004, Wang et al.[6], presented an efficient OT_n^k scheme which

can conceal all sender's secrets and can greatly reduce the sender's communication cost. In 2005, Huang et al.[12], also proposed an efficient t-out-of-n OT. They claimed that their scheme is efficient than all existing OT schemes. However, their scheme has three rounds. This means their scheme lacks the round efficiency. In the same year, Zhang et al.s'[16], proposed two efficient t-out-of-n OT. Their schemes are based on DDH assumption and have 2k+3 times modular exponentiations operations(ME), $(k+3)\log_2 q$ bits communicational bandwidth cost for the receiver and 3n times ME, $2n\log_2 q$ bits communicational bandwidth cost for the sender. Also, in 2005, Chu, et al[5] proposed two efficient k-out-of-n oblivious transfer schemes with adaptive and non-adaptive, respectively. Their schemes are mainly based on the discrete logarithm problem. They claimed that their schemes are more efficient than all the previous ones. However, their schemes also base on DDH assumption and have O(k) ME, $k \log_2 q$ bits communicational bandwidth cost for the receiver and O(n) ME, $n \log_2 q$ bits communicational bandwidth cost for the sender. In 2006, Parakh [1] proposed an OT_2^1 scheme based on Elliptic Curve Cryptography (ECC). They use a scalar that multiplies a base point on the elliptic curve as the secret which can be deduced by the received. But indeed, the receiver cannot deduce such a scalar due to ECDLP. In the same year, Kim, et al.[35] proposed a new secure verifiable non-interactive oblivious transfer protocol using RSA. They claimed their scheme have the function to authenticate the sender and let one can not deny what he has sent to the others. But we found their protocol is unable to protect against the impersonation attack. Since if an

adversary E intercepts the messages it sent from Alice and modifies X_A to $X'_A(\equiv(X'_0,X'_1))$, then sends (X'_A,M_A,C_A) to Bob. Bob will verify him as being authentic by using his private key d_B and the sender's public key e_A to decrypt C_A, obtaining M_A. Because C_A is the signature of M_A encrypted with Bob's public key and has no relationship with X_A'. E can successfully impersonate Alice. Moreover, in their scheme, there are two modulus, n_A and n_B. If they are not properly used, for example, if $n_A>n_B$, it will incur the reblocking problem. Also, in 2006, Zhang et al.[15] proposed two efficient t-out-of-n oblivious transfer schemes. They claim that both of their schemes are efficient. However, it needs three rounds. In 2007, Ghodosi et al.[11] analyzes the security of Naor-Pinkas' distributed OT and found their scheme doesn't protect both the sender and chooser in the theoretic sense.

Although, there are so many OT schemes proposed. However, all of them lack of the efficiency consideration of communication bandwidth consumption. Henceforth, in this paper, we focus on the general form of OT scheme, OT_n^k, to propose a bilinear pairing based OT_n^k which not only is secure but also possesses the low bandwidth consumption.

1.2 Vehicular ad hoc networks

Due to the rapid development in the hardware technology, vehicular networks would be widely deployed in the coming years and become the most important application of ad hoc networks products vehicular ad hoc networks (VANETs) and many services promise superb integration of digital infrastructure into many aspects of our lives. VANETs are formed

by vehicle to, vehicle, roadside devices, base stations, and so forth. In VANETs, vehicles should provide accesses to the internet, communications among themselves, and services such as traffic information, vehicle diagnostics, cooperative driving, and entertainment services. Yet, security and efficiency are crucial issues. For example, it is essential to make sure that life-critical traffic information cannot be modified or injected by an attacker. A number of researches have investigated the safety and efficiency on VANETs [4,8,9,13,21,22,23]. In 2005, Yang et al. [8] proposed a secure and efficient authentication protocol for anonymous channel in wireless communications. However, we found that their protocol suffers form the known plaintext attack. For in their protocol, if an adversary E eavesdrops on the communication line between the two communicating parties VN and HN and knows ID_{VN} and $(ID_{VN},T_2,D,E,F)_{kh,v}$. E can guess a secret key $k_{h,v}$ to decrypt the latter. If the secret key is correct, E will find ID_{VN} in the decrypted $(ID_{VN},T_2,D,E,F)_{kh,v}$. This violates the anonymous property of their protocol. In 2007, Li et al. [9] proposed a secure and efficient communication scheme, they claimed their scheme is secure, but we found that their scheme suffers from both the parallel session attack and unsafty of each vehicle's secret key. We will describe this in Section 3 and improve it in Section 4. In the same year, Raya et al. [26] proposed a "securing vehicular ad hoc networks". However, we found that when vehicle A sends $\{B|K|T\}_{PuKB}$ and $Sig_{PrKA}[B|K|T]$ to vehicle B, we can easily use A's public key to obtain the session key from $Sig_{PrKA}[B|K|T]$. In 2008, Wang et al. [30] proposed a novel secure communication scheme in vehicular ad hoc networks. We also found the same weakness in their

scheme. Because in the scheme, when vehicle A sends $\{B|SK|T\}_{PuKB}$ and $Sig_{PrKA}[B|SK|T]$ to vehicle B, we can easily use A's public key to obtain the session key SK from $Sig_{PrKA}[B|SK|T]$. Moreover, in both Raya et al.'s and Wang et al.'s schemes when a member leaves, it does not involve an updating process for the group key. Therefore, a left member can use the old group key to decrypt group messages. In other words, their protocol doesn't have the forward and backward secrecy. Therefore, we propose a secure scheme in this area based on bilinear pairings to resolve the unsolved problems.

Chapter 2 Preliminary

This section we briefly introduce some related work that are used through the paper.

2.1 Bilinear pairings

In 2001, bilinear pairings, namely the Weil pairing and the Tate pairing, defined on elliptic curves were proved and applied to cryptography. Since then, many protocols have been designed based on the Weil pairing [7,10,24]. In the following, we briefly describe the basic definitions and properties of bilinear pairings.

Let P be a generator of G_1 that is a cyclic additive group whose order is a prime q ,and G_2 be a cyclic multiplicative group of the same order q. It is assumed that the discrete logarithm problem (DLP) in both G_1 and G_2 is difficult. A bilinear pairing has the same security level as DLP [10] and is a map e: $G_1 \times G_1 \rightarrow G_2$ with the following conditions.

(1) Bilinear: $e(aP,bQ) = e(P,Q)^{ab}$, for any $a,b \in Z_q$ and $P,Q \in G_1$.

(2) Computability: There is an efficient algorithm to compute (P, Q) for all, $P,Q \in G_1$.

(3) Non - degenerate: there exists $P \in G_1$ and $Q \in G_1$ such that $e(P,Q) \notin G_1$.

After showing what is a bilinear map, we introduce the following problems in G_1:

– **Discrete Logarithm Problem (DLP):** Given two group elements P and Q, find an integer n, such that $Q = nP$ whenever such an integer exists.

– **Decision Diffie-Hellman Problem (DDHP):** For $a, b, c \in Z_q^*$, given P, aP, bP, cP, decide whether $c \equiv ab \bmod q$.

– **Computational Diffie-Hellman Problem (CDHP):** For $a, b \in Z_q^*$, given $P, aP, bP,$ compute abP.

– **Decision Bilinear Diffie–Hellman Problem (DBDHP)**: Given P, aP, bP, cP for a, b, $c \in Z_q^*$ and $z \in$ G2, decide whether $z = e(P,P)^{abc}$.

2.2 Blind Signatures from Pairings

In 2002, Paterson [17] proposed an ID-based signature scheme from pairings on elliptic curves. In 2003, Wuu et al.'s [19] modified Paterson scheme to a blind signature protocol. In the following, we briefly describe their modification.

Assume that Alice has a message m, she wants to ask Bob to sign on the message m blindly. Let Bob's public key is $Q_B=H_1(ID_B)$ and private key is $D_B=sQ_B$.

Step 1: Alice selects a random number $t_1 \in Z_q^*$, computes $m'=t_1H_2(m)$ then sends m' to Bob.

Step 2: After receiving m', Bob selects a random number $k \in Z_q^*$. He computes $R_1=kP$, $S_1=k^{-1}m'P$ and $S_2=k^{-1}D_B$, then sends back R_1,S_1,S_2 to Alice.

Step 3: After receiving R_1,S_1,S_2, Alice selects a random number $t_2 \in Z_q^*$ and computes the signature (R,S) of m, by computing $R=t_2R_1=t_2kP$,and $S = t_2^{-1}(t_1^{-1}S_1+H_3(R)S_2) = t_2^{-1}(t_1^{-1}k^{-1}m'P+H_3(R)k^{-1}D_B)=t_2^{-1}(t_1^{-1}k^{-1}t_1H_2(m)P+H_3(R)k^{-1}D_B)$
$= t_2^{-1}(k^{-1}(H_2(m)P+H_3(R)D_B)$.

To verify the signature (R,S) on message M, the verifier computes $e(R,S)$ and compares the result to value $e(P,P)^{H2(m)} \cdot e(P_{pub},Q_B)^{H3(R)}$. If these two values in G_2 match, the signature is accepted, otherwise, it is rejected. The computation is shown as follows.

$e(R, S)=e(t_2kP, t_2^{-1}(k^{-1}(H_2(m)P+H_3(R)D_B)))= e(P, H_2(m)P+H_3(R)D_B) =$
$e(P, P)^{H2(m)} \cdot e(P, D_B)^{H3(R)} = e(P, P)^{H2(m)} \cdot e(P_{Pub}, QB)^{H3(R)}$

Chapter 3 Li et al.'s scheme

In 2007, Li et al. [9] proposed a secure and efficient scheme for vehicular ad hoc networks. But we found some flaws in their protocol. In the following, we first list the definitions of used notations then review the method. After that, we present our attack on their flaws.

3.1 Definitions of used notations

In this section, we list the definitions of used notations in Li et al.s' protocol as follows.

TTP: a trusted third party.

VID_i: the identity of vehicle i.

RID_i: the identity of roadside device i.

SID_i: the identity of service provider i.

V_i : vehicle i.

R_j : roadside device j.

S_i: service provider i.

(PK_{Si}, SK_{Si}): a public and private key pair of service provider S_i.

VK_i: V_i's secret key.

SPK_{Si}: S_i's secret key.

RK_j: R_j's secret key.

tag#: an unique tag number for a request.

hop: the number of hops a message can be transmitted.

r_l: the identity of roadway section l.

ES_i: an emergency signal issued by vehicle i.

MAC: the message authentication code defined by MAC=H(K,m), where m denotes the message and K is the protection key.

M_i: the receipt of a service access for user i to access the service that S_i provides.

AC: an authorized credential.

H(.): a collision-free and public one-way hash function.

$\oplus$: an exclusive OR operation.

H(SK): the hash value of group secret key SK shared among all nodes in the network.

t: a value whose bit length depends on the actual frequency of usage (i.e. if t's length is set according to the months in a year, then t's length would be 12)

$H_t(SK)$: an one-way hash chain represents that message m has been hashed t times.

T_i: a timestamp of vehicle or roadside device i.

$a \parallel b$: the concatenation of message a and b.

$E_{PKsi}\{x\}$: message x is encrypted with service provider S_i's public key PK_{Si}.

$D_{SKsi}\{x\}$: message x is decrypted with service provider S_i's private key SK_{Si}.

3.2 Review Li et al.s' protocol

Li et al.'s non-interactive ID-based scheme uses of members' IDs to establish a secure trust relationship between communicating vehicles, and

a blind signature-based scheme for vehicle-to-roadside device communication which allows authorized vehicles to anonymously interact with their service roadside devices. Their scheme includes a pre-deployment phase and three communication scenarios: Scenario 1: secure communications between vehicles, Scenario 2: secure communications between vehicles and roadside devices, and Scenario 3: a secure and efficient communication scheme with privacy preservation (SECSPP). We briefly describe their protocol as follow:

3.2.1 Pre-deployment Phase

Let $n=p_1*p_2*p_3*p_4$ and TTP's public/private key pair be (e,d) satisfying $ed=1 \bmod \phi(n)$. TTP first chooses four relative prime numbers p_js that $(p_j-1)/2$ is prime, for j=1 to 4. Then TTP performs some actions to deal with three cases: (a) handling new vehicles, (b) handling new roadside devices, and (c) Handling new service providers. We describe each of them as follows.

(a) Handling New Vehicles:

TTP presets V_i's identity as VID_i, the roadway section identity as r_l, the group's secret key $H^t(SK)$ and V_i's secret key $VK_i= e*log_g(VID_i^2) \bmod \phi(n)$. Then, it sends them to V_i in the network through a secret channel.

(b) Handling New Roadside Devices:

TTP presets the R_i's identity as RID_i, the roadway location identity as r_l, the initial group secret key $H^t(SK)$ and the length of t, and

RID_i's secret key $RK_i = e * log_g(RID_i^2) \bmod \phi(n)$. Then, TTP sends them to R_i in the network through a secret channel.

(c) Handling New Service Providers:

TTP issues (SID_i, $H^t(SK)$, r_l, $SPK_{Si} = e * log_g(SID_{Si}^2) \bmod \phi(n)$) and generates an asymmetric public/private key pair (PK_{Si},SK_{Si}) for service provider S_i.

3.2.2 The three Scenarios

After pre-deployment phase, Li et al.s' protocol performs the following three scenarios. Here, we only demonstrate each scenario's function. The details can be refered to [11].

Scenario 1: Secure Communications between Vehicles.

It is a secure communication mechanism with mutual authentication between vehicular nodes V_s and V_d. According to this phase, V_s can discover the path to V_d and establish the session key.

Scenario 2: Secure Communications between Vehicle and Roadside Device.

It is a secure communication mechanism with mutual authentication between vehicular nodes V_s and roadside device R_j. According to this phase, V_s can discover the path to R_j and establish the session key.

Scenario 3: A Secure and Efficient Communication Scheme with Privacy Preservation (SECSPP).

In this phase, when a vehicle wants to access

pay-services, he must first obtain the authorized credential and then use it to access services anonymously. The service provider can not link the authorized credential to the user's identity. There are two phases in this scenario: (a) access authorization phase and (b) access service phase. In the following, we only briefly depict these two phases for illustrating their protocol weakness.

(a)Access Authorization Phase:

When V_i wants to anonymously access pay-services from R_j, he must get an authorized credential AC_i from S_i by presenting the receipt M_i as shown in Figure 1, where $C=(SID_i^2)^{H(TVi)*VKi}$ and $C'=(VID_i^2)^{H(TVi)*SPKSi}$.

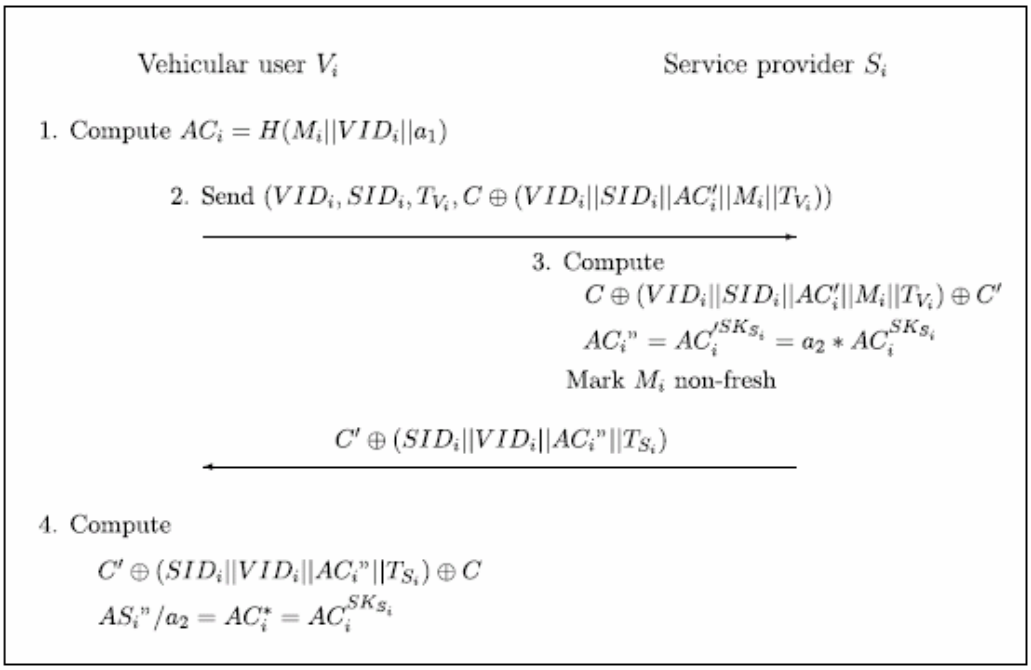

Figure 1.access authorization phase

(b)Access service Phase

After phase (a), V_i uses the authorized credential to

access the pay-services without disclosing any information about his identity VID_i as shown in Figure 2, where $C=(SID_i^2)^{H(TRj)*RKj}$ and $C'=(RID_j^2)^{H(TVi)*SPKSi}$.

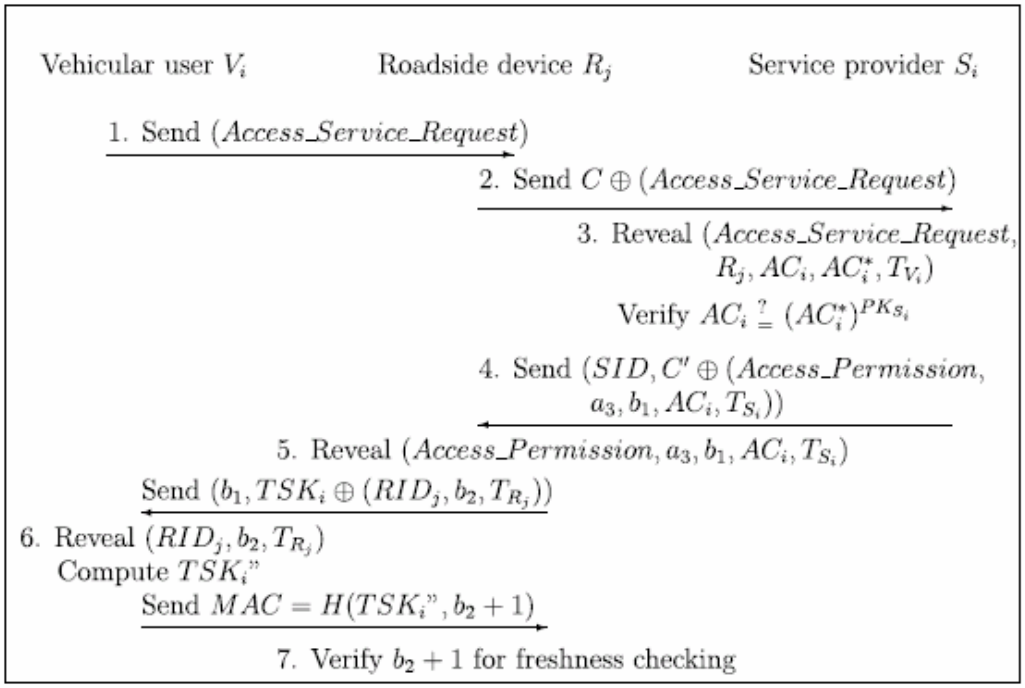

Figure 2.access service phase

3.3 **Security Analysis of Li et al.'s protocol**

Although, Li et al. claimed that their protocol can achieve secure communication between any parties. However, we found some flaws in their scheme. We describe them as follows.

(a) Violation of anonymous property insecure secret keys:

For handling new vehicle V_i in the pre-deployment phase, TTP sets V_i's secret key as $VK_i=e*log_g(VID_i^2) \bmod \phi(n)$. A malicious group member can obtain VID_i by using the hashed group secret key $H^t(SK)$ to XOR the message $H^t(SK) \oplus$

($tag\#, VID_s, VID_d, hop, T_{Vs}, r_l, C \oplus (tag\# \| VID_s \| VID_d \| T_{Vs} \| a)$ broadcast by V_i in Scenario 1 or the message $H^t(SK) \oplus (ES_i, VID_i, RID_j, T_{Vi}, r_l, C \oplus (ES_i \| VID_i \| RID_j \| T_{Vi} \| a)$ broadcast by V_i in Scenario 2. This violates the anonymous property. Moreover, if two malicious group members, V_a and V_b, collude and share their secret keys, VK_i and VID_i, for $i \in \{a,b\}$. For $VK_a = e * log_g(VID_a^2) + k_1 \phi(n)$ and $VK_b = e * log_g(VID_b^2) + k_2 \phi(n)$, they can compute $(VK_a - VK_b) = (e * log_g(VID_a^2) - e * log_g(VID_b^2)) + (k_1 - k_2) \phi(n)$, where k_1 and k_2 are two integers. Since $(VK_a - VK_b)$ and $(e * log_g(VID_a^2) - e * log_g(VID_b^2))$ are two fixed values. Let $k_3 = (k_1 - k_2)$, they can figure out $\phi(n)$ by setting k_3 from 1 to a proper value which $\phi(n)$ can be figured out. This makes the secret keys in the system insecure. Thus, the system is broken.

(b) parallel session attacking:

An adversary *E* can concurrently pretend both the user and server respectively in the communication line by operating two "windows" as shown in figure 3. In the figure, V_i sends access pay-service message (VID_i, SID_i, T_{Vi}, $C \oplus (VID_i \| SID_i \| AC_i' \| M_i \| T_{Vi})$) to S_i^* (E pretends S as S_i*). After receiving the access pay-service message, *E* impersonates V_i as V_i* and forwards the message to S_i immediately. Due to above communication, S_i will verify the receipt M_i and AC_i' as valid and send $C' \oplus (SID_i \| VID_i$

$\| AC_i'' \| T_{Si}$) back to V_i^* which E pretends. After receiving $\{C' \oplus (SID_i \| VID_i \| AC_i'' \| T_{Si})\}$ from S_i, *E* forwards $\{ C' \oplus (SID_i \| VID_i \| AC_i'' \| T_{Si})\}$ to V_i immediately. V_i will verify $\{ C' \oplus (SID_i \| VID_i \| AC_i'' \| T_{Si})\}$ as valid. E can therefore success with a non-negible probability so long as the message is transmitted in time. E can then publish certain unreal message about *S* on his site to influence V_i making unproper decision. To solve this problem, we append each communicating party's IP address to the transmitted message. For example, the source node can sign on his IP into the application layer of the transmitted packet. We will describe this in the following section.

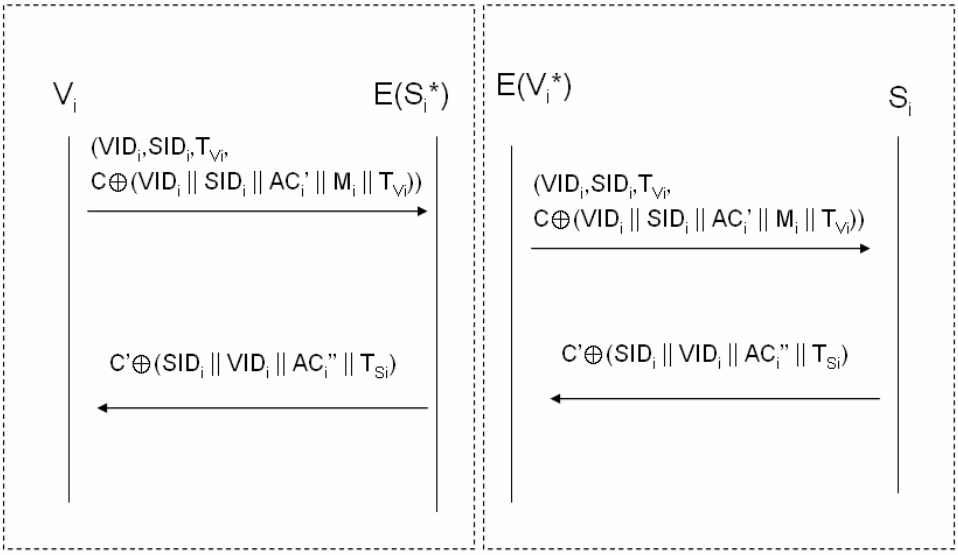

Figure 3.parallel session attack

Chapter 4 Proposed schemes

In this section, we present our OT scheme in section 4.1 and communication scheme in section 4.2.

4.1 Proposed k-out-of-n OT scheme

In this session, we present a k-out-of n OT scheme based on bilinear pairing. Our scheme consists of two phases: (1) setup phase, (2) data transfer phase. The details of our protocol are executed as follows and also illustrated in Figure 4.

(1) Setup phase

Initially, there is a public system parameter set, $\{G_1,G_2,q,P,e,H\}$, where G_1 be a cyclic additive group generated by P whose order is a prime q , G_2 be a cyclic multiplicative group of the same order q, e is a bilinear pairing mapping e: $G_1 \times G_1 \rightarrow G_2$,and H be a one-way hash function $H:\{0,1\}^* \rightarrow G_1$. R is the receiver and S is the sender.

(2) Data transfer phase.

(a). R randomly chooses n integers s_i (for i=1,2,…,n), t and w. He then computes $A_i = ws_iP$, $B_j = ts_{\sigma j}P$ (for j=1,2,…,k) and V=tP, where σ_j is the index of n random the integers s_s chosen by R. Then R sends $A_1,A_2,\ldots,A_n,B_1,B_2,\ldots,B_k$ and V to S.

(b). S randomly chooses an integer r, computes $C_i=m_i \oplus H(e(A_i,V)^r)$ and $D_j=rB_j$. Then he sends $C_i,C_2,\ldots,C_n,D_1,D_2,\ldots,D_k$ to R.

(c). After receiving $C_1,C_2,\ldots,C_n,D_1,D_2,\ldots,D_k$, R computes $m_{\sigma j}=c_{\sigma j}\oplus H(e(D_j,P)^w)$ to obtain $m_{\sigma j}$.

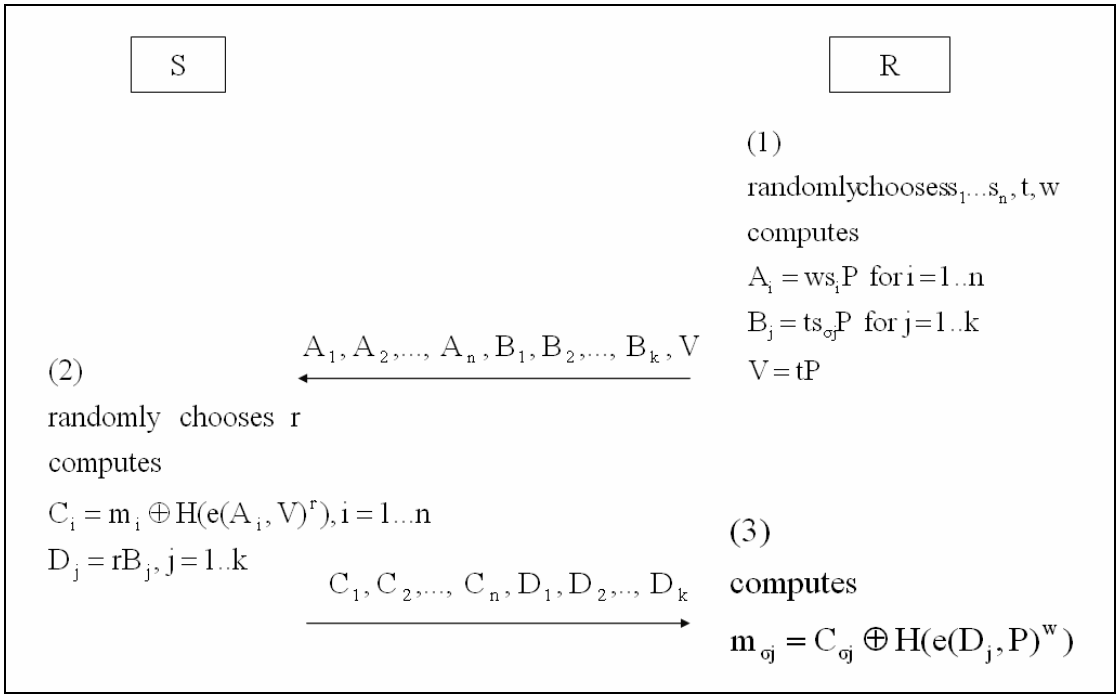

Figure 4. Our k-out-of OT

4.2 proposed communication scheme

For there still lacks a secure scheme in VANETs, in this section, we propose a novel secure protocol based on bilinear pairings. We first list the definitions of used notations in Section 4.2.1, and present our scheme in Section 4.2.2.

4.2.1 Definitions of used notations

In the following, we only list the definitions of used notations in our protocol which are not listed in Section 4.2.1.

G_1: a cyclic additive group with order q

G_2: a cyclic multiplicative group with order q

P: a generator of G_1

e: $G_1 \times G_1 \rightarrow G_2$ be a bilinear pairing

f : a public one-way hash function with arbitrary input length and fixed output length

$H_1 : G_1 \rightarrow \{0,1\}^*$

$H : G_2 \rightarrow \{0,1\}^*$

s: the private key of TTP

$P_{pub}(=sP)$: the public key of the TTP

$Q_{Vi}(=H(VID_i))$: the public key of V_i

$S_{Vi}(=sQ_{Vi})$: the private key of V_i

$Q_{Si}(=H(SID_i))$: the public key of S_i

$S_{Si}(=sQ_{Si})$: the private key of S_i

$Q_{Ri}(=H(RID_i))$: the public key of R_i

$S_{Ri}(=sQ_{Ri})$: the private key of R_i

$h_{ij}(=H(S_i,Q_j)=H(Q_i,S_j))$: a common secret shared between node i and node j.

4.2.2 Our proposed communication protocol

As in Li et al.s' protocol, our scheme also contains a pre-deployment phase and three communication scenarios.

(1). Pre-deployment Phase

TTP selects P as a generator of G_1, s as his secret key and computes $P_{pub}=sP$ as his public key. When a new vehicle V_i or new service provider S_i joins, TTP computes their public/private key pairs as

$Q_{Vi}(=H(VID_i))/S_{Vi}(=sQ_{Vi})$ and $Q_{Si}(=H(SID_i))/S_{Si}(=sQ_{Si})$, correspondingly.

(2). Scenario 1: Secure Communications between Vehicles

For this scenario, we show our protocol as follows and also depict it in figure 5.

Step 1: For initiating a route discovery process to establish a route, V_s generates a unique *tag#* and a random number *a*. He computes $C=H(e(S_{Vs},aQ_{Vd}))$ and $C_s=\oplus(tag\#||VID_s||VID_d||T_{Vs})$, where T_{Vs} is V_s system timestamp. Then, V_s broadcasts the route discovery message $(tag\#, VID_s, VID_d, hop, T_{Vs}, r_l, h_{VsVd}\oplus(tag\# \| VID_s \| VID_d \| T_{Vs} \| C_s \| aQ_{Vs}))$, where $h_{VsVd} = H(e(S_{Vs}, Q_{Vd}))$ is the pre-computed secrecy shared between V_s and V_d.

Step 2: When a vehicle receives the message, it checks to see if $(hop\text{--})\leqq 0$, if so the system drops the message; otherwise, it checks to see if itself is the destination VID_d. If this is not the case, the vehicle forwards the message $(VID_s, VID_d, hop\text{--}, T_{Vs}, r_l, h_{VsVd}\oplus(tag\# \| VID_s \| VID_d \| T_{Vs} \| C_s \| aQ_{Vs}))$ to its neighboring nodes; otherwise, it(V_d) uses his h_{VSVd} and XORs the received message to

obtain ($tag\# \| VID_s \| VID_d \| T_{Vs} \| C_s \| aQ_{Vs}$). Then he decrypts C_s by computing $C' = H(e(aQ_{Vs}, S_{Vd}))$ and $Cs \oplus C'$ to obtain ($tag\# \| VID_s \| VID_d \| T_{Vs}$). V_d then selects a random number b and computes $\delta = H(e(aQ_{Vs}, bS_{Vd}))$, $\delta_d = \delta \oplus (tag\# \| VID_s \| VID_d \| T_{Vd})$ and the session key $sk = f(\delta \| 0)$. He then sends ($tag\#$, VID_d, VID_s, hop, T_{Vd}, r_l, $h_{VsVd} \oplus (tag\# \| VID_d \| VID_s \| T_{Vd} \| r_l \| \delta_d \| bQ_{Vd})$ to V_s along the backward path.

Step 3: V_s uses h_{VsVd} to decrypt the message, obtaining ($tag\# \| VID_d \| VID_s \| T_{Vd} \| r_l \| \delta_d \| bQ_{Vd}$). He then computes $\delta' = H(e(aS_{Vs}, bQ_{Vd}))$ to decrypt δ_d, obtaining ($tag\# \| VID_d \| VID_s \| T_{Vd}$). Finally, he computes the session key $sk = f(\delta' \| 0)$. V_s and V_d can then use this session key to communicate with each other.

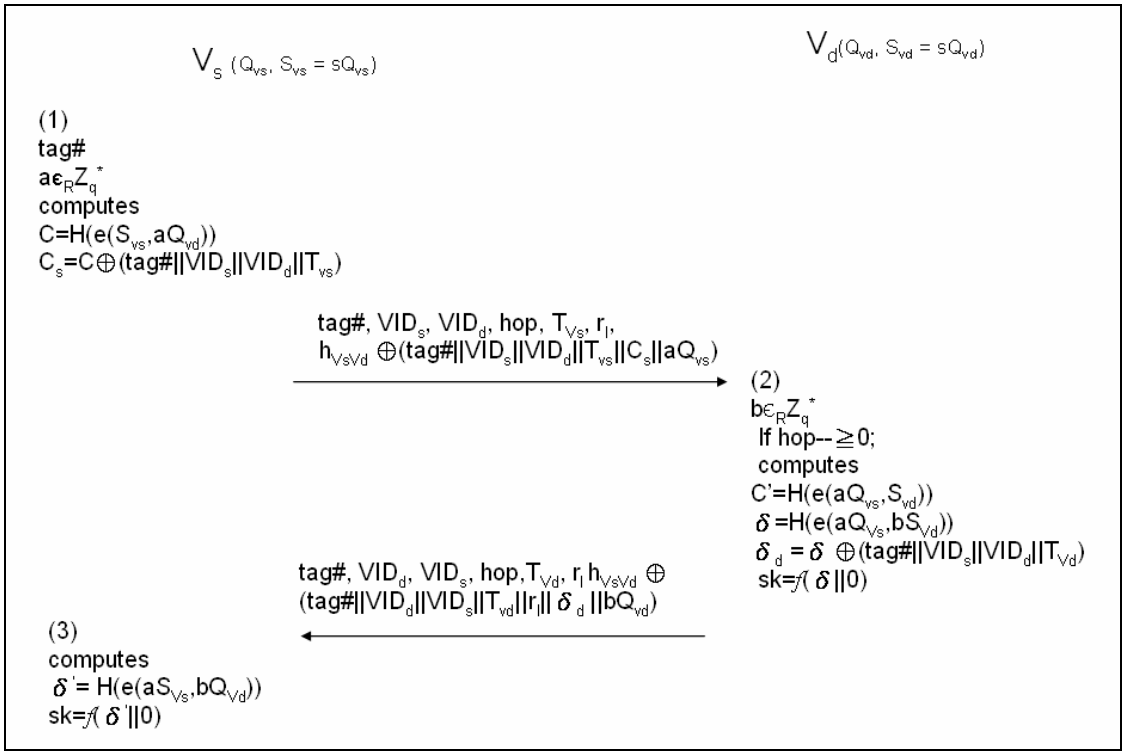

Figure 5. secure communications between vehicles

(3). Scenario 2: Secure Communications between Vehicle and Roadside Device

For this scenario, we show our protocol as follows and also depict it in figure 6.

Step 1: V_i selects a random number a, computes $C=H(e(S_{Vi},aQ_{Rj}))$ and $C_i=C \oplus (ES_i||VID_i||RID_j||T_{Vi})$. He then sends ($ES_i$, VID_i, RID_j, T_{Vi}, r_l, $h_{ViRj} \oplus (ES_i \,||\, VID_i \,||\, RID_j \,||\, T_{Vi} \,||\, r_l \,||\, C_i \,||aQ_{Vs})$ to R_j, where $h_{ViRj} = H(e(S_{Vi}, Q_{Rj}))$ is a pre-shared secrecy shared between V_i and R_j.

Step 2: On receiving the message from V_i, R_j first checks the validity of T_{Vi} to see if it is in time. If

it is, R_j decrypts the message by using h_{ViRj}, obtaining ($ES_i \| VID_i \| RID_j \| T_{Vi} \| r_l \| C_i \| aQ_{Vi}$). He then checks the validity of VID_i. If it is valid, R_j selects a random number b, computes $\delta=H(e(aQ_{Vi},bS_{Rj})),\delta_j = \delta \oplus (ES_i \| RID_j \| VID_i \| T_{Rj})$ and the session key $sk=f(\delta\|0)$. Then, R_j sends (ES_i, RID_j, VID_i, T_{Rj}, r_l, $h_{RjVi} \oplus (ES_i \| RID_j \| VID_i \| T_{Rj} \| r_l \| \delta_j \| bQ_{Rj})$ to V_i,where $h_{RjVi}= H(e(Q_{Vi}, S_{Rj}))= h_{ViRj}$.

Step 3: On receiving the message from R_j, V_i first checks the validity of T_{Rj} to see if it is in time. If it is, V_i uses h_{ViRj} to decrypt the message, obtaining ($ES_i \| RID_j \| VID_i \| T_{Rj} \| r_l \| \delta_j \| bQ_{Rj}$). He then computes $\delta'=H(e(aS_{Vi},bQ_{Rj}))$ and the common session key as $sk= f(\delta'\|0)$.

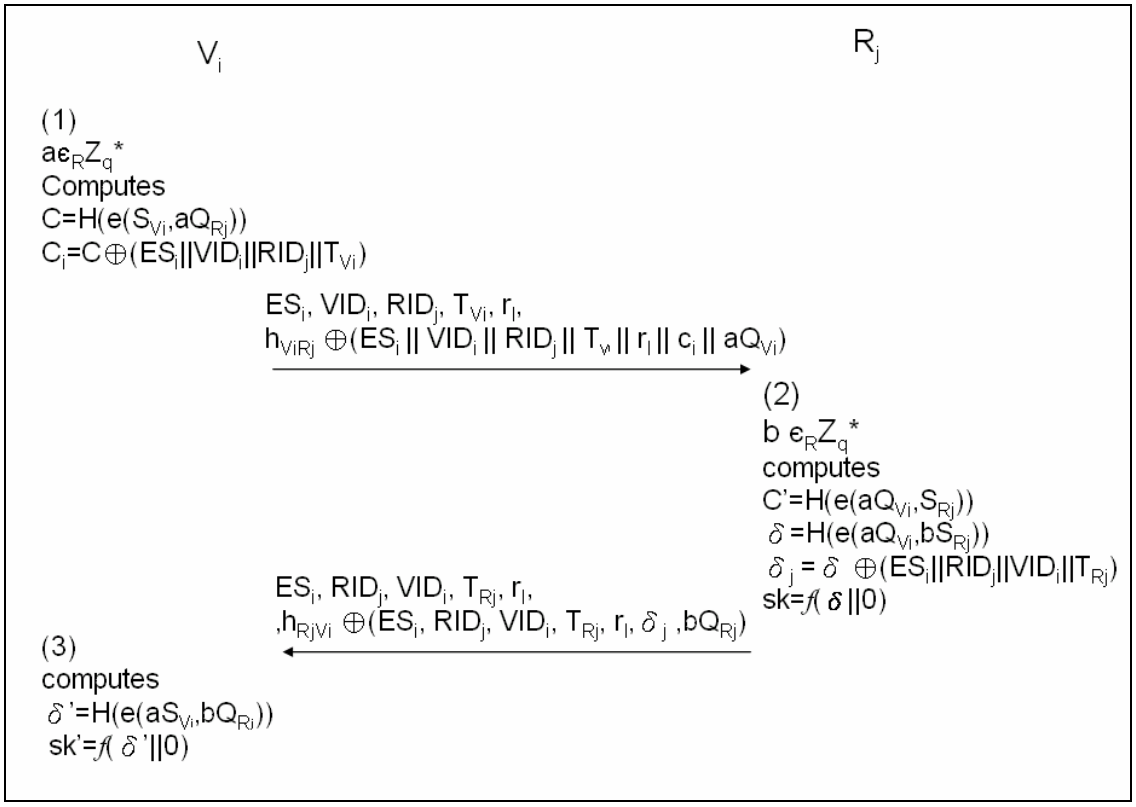

Figure 6. secure communications between vehicles and roadside devices

(4). Scenario 3: A Secure and Efficient Communication Scheme with Privacy Preservation

This scenario consists of two phases: (a) access authorization phase, and (b) access service phase. We describe them as follows and also depict them in figure 7 and figure 8 respectively.

(a) Access Authorization Phase:

For this phase, V_i and S_i perform the following steps.

Step 1: V_i selects a random number α and computes the authorized credential AC_i as $AC_i = f(M_i \,||\, VID_i)$. Then, he computes $AC_i^* = \alpha * AC_i$, $\sigma_{Vi}=H(e(f(IP_{Vi})S_{Vi}, Q_{Si}))$ and sends ($f(IP_{Vi})$, σ_{Vi},

AC_i^*) to S_i.

Step 2: On receiving the message form V_i, S_i check to see whether $\sigma_{Vi}=H(e(f(IP_{Vi})Q_{Vi},S_{Si}))$. If it holds, S_i selects a random number k, computes $R_1=kP$, $S_1=k^{-1}AC_i^*P$, $S_2=k^{-1}S_{Si}$ and $\sigma_{Si}=H(e(f(IP_{Si})Q_{Vi},S_{Si}))$. S_i then sends R_1,S_1,S_2, $f(IP_{Si})$ and σ_{Si} to V_i.

Step 3: After receiving the message from S_i, V_i checks to see whether$\sigma_{Si}=H(e(f(IP_{Si})S_{Vi},Q_{Si})$. If it holds, he computes (R,S), the signature of AC_i, as $R=\alpha R_1$ and $S=\alpha^{-1}(\alpha^{-1}S_1+H_1(R)S_2)$

After step 3, any one can verify (R,S) by computing whether the equation $e(R,S)=e(P,P)^{ACi}e(P_{Pub},Q_{Si})^{H_1(R)}$ holds.

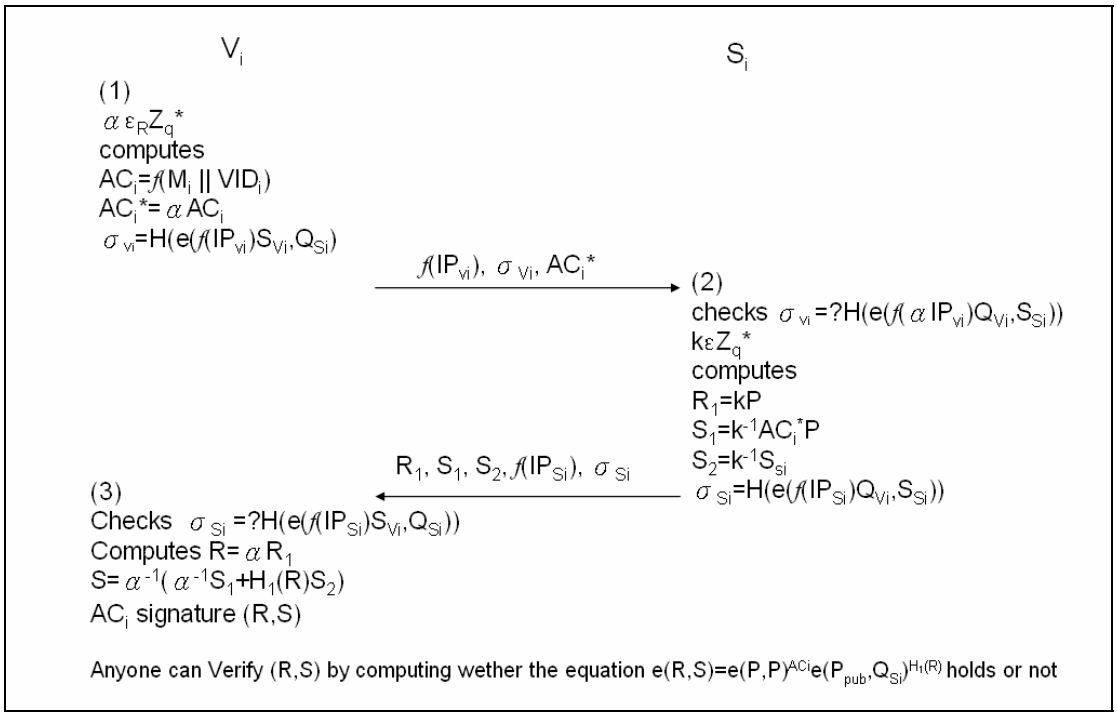

Figure 7. access authorization phase

(b) Access service Phase

For this phase, V_i uses the authorized credential to access service anonymously and S_i doesn't need to provide the service to V_i anonymously. It performs the following steps.

Step 1: When V_i wants to access the pay-service from the roadside device R_j, he selects a random number *a*, computes $h_{ViSi}'=H(e(aS_{Vi},Q_{Si}))$ and $\sigma_{Vi}=H(e(f(aIP_{Vi})S_{Vi},Q_{Si}))$. He then sends the request message $h_{ViSi}'\oplus(Request,\ RID_j,\ AC_i,\ AC_i^*,\ T_{Vi},\ f(aIP_{Vi}),\ \sigma_{Vi}),\ aQ_{Vi}$ to R_j

Step 2: After receiving the message form V_i, R_j selects a random number *b* and forwards RID_j ,T_{Rj} ,$h_{RjSi}\oplus(\ h_{ViSi}'\oplus(\ Request,\ RID_j,\ AC_i,\ R,\ S,\ T_{Vi},\ f(aIP_{Vi}),\ \sigma_{Vi}),\ aQ_{Vi},\ bQ_{Rj})$ to S_i, where $h_{RjSi}=H(e(S_{Rj},Q_{Si}))$ is a pre-shared secrecy between R_j and S_i.

Step 3: After receiving the message form R_j, S_i obtains bQ_{Rj} then uses h_{RjSi} to decrypt and computes $h_{ViSi}''=H(e(aQ_{Vi},S_{Si}))=h_{ViSi}'$ to decrypt the result, obtaining $(Request,RID_j,\ AC_i,\ R,\ S,\ T_{Vi},\ f(aIP_{Vi}),\ \sigma_{Vi})$. Then he checks to see whether $\sigma_{Vi}=H(e(f(aIP_{Vi})Q_{Vi},S_{Si})$. If it holds,

he verifies the validity of authorized credential by checking whether $e(R,S) = e(P,P)^{ACi} e(P_{pub}, Q_{Si})^{H_i(R)}$ holds or not. If it holds, S_i selects a random c and computes the temporary service $Tsk_i = H(e(aQ_{Vi}, bQ_{Rj})^{cs} || AC_i || 0)$ and $\sigma_{Si} = H(e(aQ_{Vi}, f(IP_{Si}) S_{Si}))$. Then, S_i sends $(f(IP_{Si}), \sigma_{Si}, SID_i, T_{Si}, h_{RjSi} \oplus (permision, acQ_{Vi}, AC_i, T_{Si}), h_{SjVi}' \oplus bcQ_{Rj})$ to R_j.

Step 4: After receiving the message form S_i, R_j uses h_{RjSi} to decrypt $h_{RjSi} \oplus (permision, acQ_{Vi}, AC_i, T_{Si})$. He then can obtain the temporary service key by computing $Tsk_i' = f(H(e(acQ_{Vi}, bS_{Rj})) || AC_i || 0)$. After that, he selects a random number b_2 and sends $(f(IP_{Si}), \sigma_{Si}, h_{SjVi}' \oplus bcQ_{Rj}, Tsk_i' \oplus (RID_j, b_2, T_{Rj}))$ to V_i.

Step 5: After receiving the message form R_j, V_i checks to see whether $\sigma_{Si} = H(e(aS_{Vi}, f(IP_{Si}) Q_{Si}))$. If it holds, he uses h_{SiVi}' to decrypt $h_{SiVi}' \oplus bcQ_{Rj}$, obtaining bcQ_{Rj}. He then computes $Tsk_i'' = f(H(e(aS_{Vi}, bcQ_{Rj})) || AC_i || 0)$ to decrypt $(Tsk_i' \oplus (RID_j, b_2, T_{Rj}))$, obtaining (RID_j, b_2, T_{Rj}). Then, he computes $MAC = f(Tsk_i'', b2+1)$ and sends MAC to R_j.

Step 6: After receiving the message form V_i, Rj

checks to see whether $MAC=f(Tsk_i', b_2+1)$. If it hold, finally, V_i and R_j can use $TSK_i=f(H(e(aS_{Vi}, bcQ_{Rj}))||AC_i||0)$ for securing the subsequent data traffic in the access service phase.

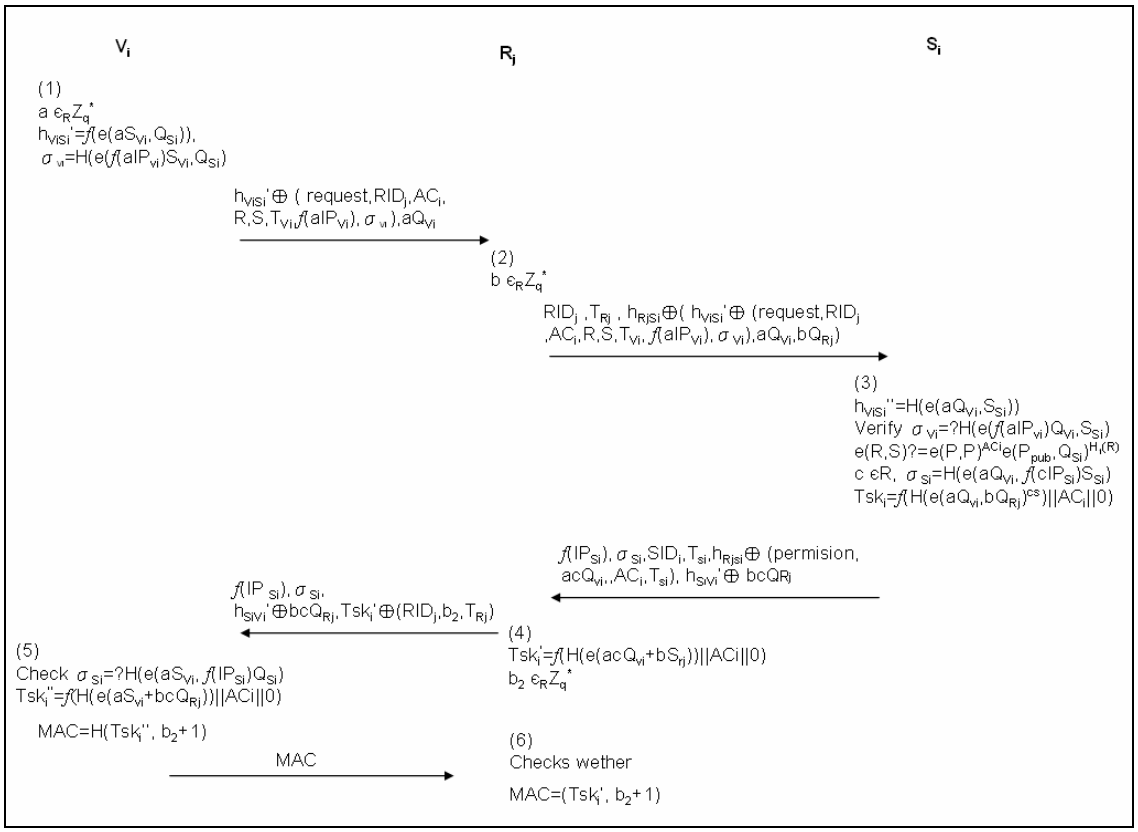

Figure 8.access service phase

Chapter 5 Security and Performance analysis

In this session, we analyze the security and performance of our OT scheme in section 5.1, analyze security and performance of our communication scheme in section 5.2.

5.1 Security analysis

In this session, we analyze the security of our scheme in Section 5.1.1 and we also compare its communicational cost with the other related work in Section 5.1.2.

5.1.1 Security Analysis of OT protocol

In this section, we examine the security of our scheme by using the following dimensions.

(1). **Correctness:**

When receiving messages, $C_i,C_2,\ldots,C_n,D_1,D_2,\ldots,D_k$, R can correctly decrypt $C_{\sigma 1}$, $C_{\sigma 2},\ldots,C_{\sigma k}$ to obtain the messages $m_{\sigma 1},m_{\sigma 2},\ldots,m_{\sigma k}$, which he had chosen by computing $m_{\sigma j}=C_{\sigma j}\oplus H(e(D_j,P)^w) = C_{\sigma j}\oplus H(e(rB_j,P)^w) = C_{\sigma j}\oplus H(e(rts_{\sigma j}P,P)^w) = C_{\sigma j}\oplus H(e(ws_{\sigma j}P,tP)^r) = C_{\sigma j}\oplus H(e(A_j,V)^r)$.

(2). Assurance of the sender's privacy:

The sender sends message m_i which is protected by XORing $H(e(A_i,tP)^r)$. If R wants to obtain extra messages which he didn't choose, he need to know the number r. However, solving the random

number r from V is computationally infeasible due to the ECDLP assumption.

(3). Assurance of the receiver privacy:

The receiver's k choices in the n random numbers s_s, $s_{\sigma 1}$, $s_{\sigma 2}$,…, $s_{\sigma k}$, are enciphered in A_i (= ws_iP) and B_j (=$ts_{\sigma j}P$). After receiving $A_1,A_2,\ldots,A_n,B_1,B_2,\ldots,B_k$ and V(= tP) from R, S can not compute $s_{\sigma 1}$, $s_{\sigma 2}$,…, $s_{\sigma j}$ in polynomial time due to the ECDLP assumption. Therefore, the sender can not know which k messages, $m_{\sigma j}$, for j=1 to k, the receiver chose.

(a). Against dishonest receiver: In our k-out-of-n OT scheme, if R is dishonest in computing B_j(=$ts_{\sigma j}P$, for i=1,…,k) or V=(tP), R can not obtain the correct $m_{\sigma j}$ by computing $m_{\sigma j} = C_{\sigma j} \oplus H(e(D_j,P)^w) = C_{\sigma j} \oplus H(e(rB_j,P)^w) \neq C_{\sigma j} \oplus H(e(A_j,V)^r) = C_{\sigma j} \oplus H(e(ws_{\sigma j}P,tP)^r) = C_{\sigma j} \oplus H(e(rts_{\sigma j}P,P)^w)$.

5.1.2 Security Analyze of Communication protocol

In this session, we discuss the security of our protocol. We argue that our scheme can satisfy the following security requirements: (1) mutual authentication and preventing replay attack (2) against KCI attack (3) against man-in-middle attack.(4) against parallel session attack (5) anonymity. We describe them as follows.

(1) Mutual authentication and preventing replay attack

Our protocol can achieve mutual authentication in each case of (a) secure communications between vehicles, (b) secure

communications between vehicle and roadside device, and (c) a secure and efficient communication scheme with privacy preservation.

(a). secure communications between vehicles

When V_s wants to communicate with V_d. V_s broadcasts the route discovery message ($tag\#, VID_s, VID_d, hop, T_{Vs}, r_l, h_{VsVd} \oplus (tag\# \| VID_s \| VID_d \| T_{Vs} \| C_s \| aQ_{Vs})$), where $h_{VsVd} = H(e(S_{Vs}, Q_{Vd}))$ is a pre-shared secrecy shared between V_s and V_d, $C_s = C \oplus (tag\# \| VID_s \| VID_d \| T_{Vs})$ and $C = H(e(S_{Vs}, aQ_{Vd}))$. If V_d can decrypt the message by using h_{VsVd}, it represents V_s has the same pre-shared secrecy as his own. Similarly, after receiving the message form V_s, V_d sends ($tag\#, VID_d, VID_s, hop, T_{Vd}, r_l, h_{VdVs} \oplus (tag\# \| VID_d \| VID_s \| T_{Vd} \| r_l \| \delta_d \| bQ_{Vd})$ back to V_s. If V_s can decrypt the message using h_{VsVd}, he can verify that V_d has the same pre-shared secrecy as his own. Moreover, a is a random number selected by V_s and b is a random number chosen by V_d, both are used to assure every session key being fresh, and preventing from replay attack. V_d and V_s can compute the session key sk as $f(H(e(aQ_{Vs}, bS_{Vd}))\|0))$ and $f(H(e(aS_{Vs}, bQ_{Vd}))\|0))$, respectively. If V_s and V_d use sk to communicate, then they can implicitly authenticate each other.

(b). secure communications between vehicle and roadside device

When V_i wants to communicate with R_j, he sends ($ES_i, VID_i,$

RID_j, T_{Vi}, r_l, $h_{ViRj} \oplus (ES_i \| VID_i \| RID_j \| T_{Vi} \| r_l \| C_i \| aQ_{Vs})$ to R_j. If R_j can decrypt the sent message, he can verify that V_i has the same pre-shared secrecy as his own. Similarly, after receiving the message form V_i, R_j sends (ES_i, RID_j, VID_i, T_{Rj}, r_l, $h_{RjVi} \oplus (ES_i \| RID_j \| VID_i \| T_{Rj} \| r_l \| \delta_j \| bQ_{Rj})$ back to V_i. If V_i can decrypt the sent message, he can verify that R_j has the same pre-shared secrecy as his own. Moreover, a is a random number chosen by V_i and b is a random number chosen by R_j, both are used to assure every session key being fresh and preventing from replay attack. They each (Rj and V_i) can compute the session key $sk = f(H(e(aQ_{Vi}, bS_{Rj})\|0))$ and $sk = f(H(e(aS_{Vi}, bQ_{Rj})\|0))$, respectively. If V_i and R_j can use sk to communicate, then V_i and R_j can implicitly authenticate each other.

(c). a secure and efficient communication scheme with privacy preservation

When V_i wants to access the pay-service from the roadside device R_j, and S_i has received and successfully decrypted the request message $h_{RjSi} \oplus (h_{ViSi} \oplus (Request, RID_j, AC_i, R, S, T_{Vi}, f(aIP_{Vi}), \sigma_{Vi}), bQ_{Rj})$ from R_j, S_i can verify that both S_i and R_j have the same pre-shared secrecy as his own. Moreover, b and c are two random numbers chosen by R_j and S_i respectively to assure every session key being fresh and preventing from replay attack. After receiving ($f(IP_{Si})$, σ_{Si},

$SID_i, T_{Si}, h_{RjSi} \oplus (permission,\ acQ_{Vi},\ AC_i,\ T_{Si}),\ h_{SiVi}' \oplus bcQ_{Rj})$ from S_i, R_j can verify that S_i has the same pre-shared secrecy as his own if he can decrypt the message. Then, he randomly chooses b_2 be to computed in the replied MAC made by V_i and uses his secret key to compute $Tsk_i' = H(e(acQ_{Vi}, bS_{Rj})||AC_i||0)$. R_j then sends $f(IP_{Si}),\ \sigma_{Si},\ h_{SiVi}' \oplus bcQ_{Rj},\ Tsk_i' \oplus (RID_j, b_2, T_{Rj})$ to V_i. If V_i can successfully decrypt the message sent from R_j, he can verify that R_j has the same pre-shared secrecy as his own. He then uses his private key to compute $Tsk_i'' = H(e(aS_{Vi}, bcQ_{Rj})||AC_i||0)$. If Tsk_i'' is equal to Tsk_i', V_i can implicitly authenticate R_j. Similarly, R_j can implicitly authenticate V_i.

(2) Against KCI attack

KCI means that when a node's secret key has been compromised, an adversary can impersonate any other node to communicate with the compromised node. In the following, we describe how our protocol can resist to such a KCI attack in the following three cases.

(a). Secure Communications between Vehicles

Here, we assume that the private key S_{Vd} of V_d had been compromised to an adversary E. E can easily forge a valid route discovery message by computing $h_{VsVd} = H(e(Q_{Vs}, S_{Vd}))$, $C = H(e(Q_{Vs}, aS_{Vd}))$ and $C_s = C \oplus (tag\#||VID_s||VID_d||T_{Vs})$. But he can not compute the valid session key for he needs to compute

$e(aQ_{Vs},bS_{Vd})$. However, he only knows S_{Vd}, he can not figure out b which has been protected by the encryption form bQ_{Vd}, according to ECDLP assumption. Hence, E fails to generate a session key shared with V_d. Therefore, E can not successfully launch a KCI attack.

(b). Secure Communications between Vehicle and Roadside Device

Here, we assume that the private key S_{Rj} of R_j had been compromised to an adversary E. E can easily forge a valid route discovery message by computing $h_{ViRj} = H(e(Q_{Vi}, S_{Rj}))$, $C = H(e(Q_{Vi},aS_{Rj}))$ and $C_s = C \oplus (tag\#||VID_i||RID_j||T_{Vi})$. But he fails to compute the valid session key for he needs to compute $e(aQ_{Vi},bS_{Rj})$. However, he only knows S_{Rj}, he can not figure out b which is protected by the encryption form bQ_{Rj}, according to ECDLP assumption. Hence, E fails to generate a session key shared with R_j. Therefore, E can not launch a KCI attack.

(c). A Secure and Efficient Communication Scheme with Privacy Preservation

Here, we assume that the private key S_{Si} of S_i had been compromised to an adversary E who wants to impersonate V_i to communicate with S_i. E can easily forge a valid route discovery message by computing $h_{ViSi} = H(e(Q_{Vi}, S_{Si}))$. But he can not compute the valid session key for he needs to compute $e(aS_{Vi},bcQ_{Rj})^s$. However, he only knows S_{Rj}, he can

not know S_{Vi}. Hence, E fails to generate a session key shared with R_j. Therefore, E can not launch a KCI attack.

(3) Against man-in-middle attack (MIMA)

This attack means that an adversary E who eavesdrops on the communication line between two communicating parties can make them believe that they were talking to the intended party. But, indeed, they each is talking E. According to Section 4.2.2, the transmit message is protected by h_{VsVd}, E can not decrypt the message. Moreover, due to that a is protected by the encryption from aQ_{Vs} and E can not know the private key of V_d , E can not compute the session key $sk(=f(H(e(aQ_{Vs},bS_{Vd}))||0))$. Similarly, in the other case, E can not compute the session key $sk(=f(H(e(aQ_{Vi},bS_{Rj}))||0))$ in the other direction. Therefore, E can not launch such a MIMA attack.

(4) Against parallel session attack

To resist against the parallel session attack we mentioned in Section 3.3, we append each communicating party's IP address to the message he sends out. For example, in figure 7, V_i sends h_{ViSi}' $\oplus(Request, RID_j, AC_i, R, S, T_{Vi}, f(aIP_{Vi}), \sigma_{Vi}, aQ_{Vi}$ to R_j and R_j forwards the message to S_i. After receiving the message, S_i checks to see whether $\sigma_{Vi}=H(e(f(aIP_{Vi})Q_{Vi},S_{Si})$ holds or not. If it holds, S_i can confirm that the message is from V_i. Hence, the parallel session attack doesn't exist.

(5) Anonymity

In the access authorization phase, V_i*'s* identity and M_i are

hashed together to form the authorized credential AC_i, and AC_i is protected by a blind factor α. After V_i receiving (R_1,S_1,S_2), He computes (R,S), the signature of AC_i, as $R=\alpha R_1$, $S=\alpha^{-1}(\alpha^{-1}S_1+H(R)S_2)$. Everyone can verify (AC_i, R, S, Q_{Si}) by computing $e(R,S)=e(P,P)^{ACi}e(P_{Pub},Q_{Si})^{H(R)}$. In the access service phase, V_i sends a request message, $h_{ViSi}' \oplus (Request, RID_j, AC_i, AC_i^*, T_{Vi}, f(aIP_{Vi}), \sigma_{Vi}), aQ_{Vi}$ to R_j which is protected by $h_{ViSi}'=H(e(aS_{Vi},Q_{Si}))$ and doesn't disclose any information about his identity. Only the right service provider can compute $h_{ViSi}''=H(e(aQ_{Vi},S_{Si}))$ to decrypt the request message. Moreover, the service provider can not link the user identity from the authorized credential for $ACi=H(M_i \,||\, VID_i)$.

5.2 Performance comparisons

In this section, we first compare the efficiency in bandwidth consumption of our scheme with Chu et al.s' [5], Zhang et al.s'[16] and Mu et al.s' [38]. Then, we compare the computational cost of our scheme with theirs.

If the computation in discrete log problem needs 1024 bits, the bilinear pairings only needs 160 bits to achieve the same security. Based on this fact, first, we compare the communicational cost of our scheme with the others by considering three factors, the number of needed rounds between S and R, the number of bits transfered from R to S, and the number of bits needed for transferring messages from S to R. We show

the result in Table 1.

Table 1：comparisons of needed number of rounds and transferred bits

	Our scheme	Chu et al.s'[5]	Zhang et al.s'[16]	Mu et al.s'[38]
Needed rounds	2	2	3	2
Bits needed from R to S	(n+k+1) *160 bits	k*1024 bits	(K+3)*1024 bits	2n*1024 bits
Bits needed from S to R	(n+k)*160 bits	(n+k+1)*1024 bits	2n*1024 bits	n*1024 bits

From table 1, we can see that if we wish our scheme to be more efficient than the others such as [5], (n+k+1)*160 must be less than k*1024. That is (n+k+1)*160 $\leqq$ 1024k. In other words, when n $\leqq$ 5.4k-1, our scheme has the best performance in bandwidth consumption. Now, we compare the computational cost with the other three by using two factor: (1)the number of operations S needs to compute, and (2) the number of operations R needs to compute. We show the result in Table 2.

T_{Exp}: the time of a modular exponentiation,1 ($T_{Exp} \cong 240\ T_{Mul}$)[29]

T_{Mul}: the time of a modular multiplication

T_{XOR}: the time of a modular bit-XOR

T_{EC_Mul}: the time of a scalar multipling a paint on an elliptic curve Z_p;(1 $T_{EC\_Mul} \cong 29\ T_{Mul}$)[29]

T_{bp} : the computation time of a bilinear pairing

T_{hash}: the computation time of a hash function

T_{enc}: the computation time of an encrypted under DLP

T_{dec}: the computation time of a decrypted under DLP

T_{asym}: the time for an asymmetric encryption/decryption operation

T_{sym}: the time for an symmetric encryption/decryption operation

Table 2: comparisons of computational cost of various operations

	Our scheme	Chu et al.s'[5]	Zhang et al.s'[16]	Mu et al.s'[38]
Receiver	$(2n+2k+1)T_{EC\_Mul}+k(T_{bp}+T_{XOR})+kT_{hash}$	$2kT_{Mul}+2kT_{Exp}+kT_{XOR}+2kT_{hash}$	$2k+3\ T_{Exp}+kT_{Mul}$	$kT_{Exp}+2kT_{Mul}+kT_{dec}$ or $2kT_{Exp}+2kT_{Mul}$
Sender	$n(T_{bp}+T_{XOR})+k\ T_{EC\_Mul}+n\ T_{hash}$	$(n+k+1)T_{Exp}+nT_{XOR}+(n+k)\ T_{hash}$	$3n\ T_{Exp}+3nT_{Mul}$	$2nT_{Exp}+nT_{Mul}+nT_{enc}$ or $3nT_{Exp}+nT_{Mul}$

From Table 1 and Table 2, we can see that our scheme maybe less efficient in computation time. However, it is more efficient in bandwidth consumption than the other proposed schemes which play an important role in a busy commercial network for the end-of-day settlement.

Then, we compare the computational cost of our communication

protocol with the other similar vehicle work. For in authorization phase of our scheme, V_i can pre-compute $AC_i = H(M_i \| VID_i)$, $AC_i^* = \alpha * AC_i$,$\sigma_{Vi} = H(e(H(\alpha IP_{Vi})S_{Vi},Q_{Si})$ and in the access phase, he can pre-compute $h_{ViSi}' = H(e(aS_{Vi},Q_{Si}))$, $\sigma_{Vi} = H(e(H(aIP_{Vi})S_{Vi},Q_{Si})$ before the communication taking place, we omit these pre-computed computations in table 3.

Table 3: computational cost comparison of various communication schemes

scheme / phase	Our scheme	Li et al.'s scheme[9]	Yang et al.'s scheme[8]	He et al.'s scheme[31]
Authorization Phase	$3T_{hash}$ +4 T_{EC_Mul} +3T_{bp}	4 T_{XOR} +3 T_{hash} +3 T_{Exp} +2 T_{asym}	4 T_{XOR} +4 T_{sym} +13 T_{Exp}	2 T_{asym} + T_{hash}
Access Service Phase	$5T_{XOR}$ +3 T_{hash} +8T_{bp}+2 T_{EC_Mul}	5 T_{XOR} +6 T_{hash} +3 T_{Exp} +3 T_{asym} +2 T_{Mul}	4 T_{Exp} +4 T_{sym}	4 T_{asym} +4 T_{hash} +2 T_{sym}

Chapter 6 Conclusion

We propose a novel efficient and secure k-out-of-n oblivious transfer scheme and a secure communication scheme based on pairings. In our OT scheme, we reduce communicational cost for both sender and the receiver. Also, we analyze the security and efficiency of our scheme. After our analysis, we can conclusion that our scheme is not only secure but also more efficient in bandwidth consumption than all other existing oblivious transfer schemes. In our communication scheme, according to our analysis in Section 5.2, our scheme is the first scheme which can against man-in-middle attack, KCI attack, parallel session attack and achieve mutual authentication. That is, up to how, our scheme is the first robust scheme in VANETs.

References

[1] Abhishek Parakh, “Oblivious Transfer Using Elliptic Curves,” Proceedings of the 15th International Conference on Computing, Page(s):323 - 328 , IEEE , 2006.

[2] Abhishek Parakh, “Oblivious Transfer based on Key Exchange,” eprint arXiv: 0705.0178, 2007

[3] C.Crepeau, “Equivalence between two floavors of oblivious transfer,” EUROCRYPTO 87, pp.350-354, 1987.

[4] Carlos J. Bernardos, Ignacio Soto, and Maria Calderon,”VARON: Vehicular Ad hoc Route Optimisation for NEMO,” Computer Communication 30, 1765-1784,2007

[5] Cheng-Kang Chu, and Wen-Guey Tzeng, “efficient k-out-of-n oblivious transfer Schemes with adaptive and non-adptive queries,” PKC 2005, LNCS, pages 172-183, 2005

[6] Chih-Hung Wang and Chi-Shin Lin, ”A New Efficient k-out-of-n Transfer Scheme by means of Common Cipher,” Int. Computer Symposium, Dec. 15-17, 2004, Taipei, Taiwan

[7] Chih-Yin Lin, Tzong-Chen Wu, Fangguo Zhang and Jing-Jang Hwang, “New identity-based society oriented signature schemes from pairings on elliptic curves,” Mathematics and Computation, Vol 160, p.p 245-260, 2005.

[8] Chou-Chen Yang, Yuan-Liang Tang, Ren-Chiun Wang, and Hung-Wen Yang, “A secure and efficient authentication protocol for anonymous channel in wireless communications,” Mathematics and Computation,169(2):pp.1431-1439,2005

[9] CT Li, MS Hwang, and YP Chu,”A Secure and Efficient Communication Scheme with Authenticated Key Establishment and Privacy Preserving for Vehicular Ad Hoc Networks,” Computer Communications, 2007 – Elsevier

[10] D.Boneh and M.Franklin, “Identity-based encryption from the Weil pairings,” Cryptology-Crypto 2001,LNCS 2139,pp.213-229,2001.

[11] Hossein Ghodosi, “On insecurity of Naor-Pinkas’ distributed

oblivious transfer," Information Processing Letters, Vol104,2007

[12] Hui-Feng Huang, and Chin-Chen Chang, "A New Design for Efficient t-out-n Oblivious Transfer Scheme," Proceedings of Advanced Information Networking and Application, Vol 2, p.p28-30, IEEE, 2005.

[13] J Zhang, L Ma, W Su, and Y Wang," Privacy-Preserving Authentication Based on Short Group Signature in Vehicular Networks," Data, Privacy, and E-Commerce, 2007.

[14] Jan Camenish, Gregory Neven, and abhi shelat, "Simulatable adaptive oblivious transfer," Eurocrypt 2007, LNCS, page 573-590, 2007

[15] Jianhong Zhang, and Wei Zou, "Two t-out-of-n oblivious transfer schemes with designated receiver," wuhan university journal of natural sciences, Vol.11, 2006.

[16] Jianhong Zhang, and Yumin Wang, "Two provably secure k-out-of-n oblivious transfer schemes," Mathematics and Computation, Volume 169, 2005.

[17] KG Paterson," ID-based signatures from pairings on elliptic curves," Electronics Letters, 2002 - eprint.iacr.org

[18] Kun Peng, Colin Boyd and Ed Dawson, "Batch verification of validity of bids in homomorphic e-auction," Computer Communications, Volume 29, 2006.

[19] L Wuu ,and Yi-Wei Lu, " electronic payment systems by group blind signatures,". ethesys.yuntech.edu.tw,2003

[20] M. Naor, and B. PInkas, " Distributed oblivious transfer," Cryptology-Processings of ASIACRYPT'00, in: Lecture Notes in Computer Science, vol. 1976, 2000

[21] M. Raya, and J. P. Hubaux, " Security aspects of inter-vehicle communications," Proceedings of the 5th Swiss Transport Research Conference (STRC 2005), Ascona, Switzerland, 2005

[22] M.Raya, and J. P. Hubaux,"The security of vehicular ad hoc networks," Proceedings of the 3rd ACM workshop on Security of ad hoc and sensor networks, pages 11-21,Alexandria, USA, 2005.

[23] M Raya, D Jungels, P Papadimitratos, I Aad, and JP, ”Certificate Revocation in Vehicular Networks,” Laboratory for Computer Communications and Applications (LCA-Report-2006-006)

[24] Manik Lal Das, Ashutosh Saxena, Ved P. Gulati and Deepak B. Phatak, “A novel remote user authentication scheme using bilinear pairings,” Computers & Security, Volume 25, Pages 184-189, 2006

[25] Matthew Green, and Susan Hohenberger, “Blind Identity-Based Encryption and Simulatable Oblivious Transfer,” Cryptology ePrint Archive, Report 2007/235, 2007

[26] Maxim Raya, and Jean-Pierre Hubaux, “ Securing vehicular ad hoc networks,” Journal of Computer Security 15, pp.39-68,2007

[27] Minh-Dung Dang, “More Extensions of Weak Oblivious Transfer,” lnternational Conference on Volume , Issue , Feb. 12-16, pp.40-45. 2006.

[28] Moni Naor and Benny Pinkas, “Oblivious Transferwith Adaptive Queries,” Proceedings of Advances in Cryptology-CRYPTO 99, LNCS, Vol. 1666, pp. 573-590. 1999.

[29] Narn-Yih Lee, Chien-Nan Wu, and Chien-Chih Wang, “Authenticated multiple key exchange protocols based on elliptic curves and bilinear pairings,” Computers and Electrical Engineering, Vol. 34, pp.12-20. 2008.

[30] Neng-Wen Wang, Yueh-Min Huang, and Wei-Ming Chen,”A novel secure communication scheme in vehicular ad hoc networks,” Computer Communications, doi:10.1016/j.comcom.2007.12.003.

[31] Qi He, Dapeng Wu, and Pradeep Khosla, “The quest for personal control over mobile location privacy,” IEEE Communications Magazine, Vol. 42(5), pp.130-136,2004.

[32] Rabin, “Exchange secrets by oblivious transfer,” Computer Science Lab, HarvardUniversity, Cambridge, MA, TR-81,1981

[33] Shai Halevi, and Yael Tauman Kalai, “Smooth projective hashing and two-message oblivious transfer,” Cryptology ePrint Archive, 118, 2007.

[34] Shimon Even, Oded Goldreich, and Abraham Lempel, “A

randomized protocol for signing contracts," Communications of the ACM, Vol. 28(6), pp.637-647,1985

[35] Soongohn Kim, Seoksoo Kim, and Geuk Lee, "Secure verifiable non-interactive oblivious transfer protocol using RSA and Bit commitment on distributed environment," Future Generation Computer Systems, Available online 14, 2006.

[36] U Shinmyo, M Kuribayashi, M Morii, and H Tanaka, "Fingerprinting Protocol Based on Distributed provider Using," IEICE Trans. Fundamentals,Vol.E89-A, No.10, Oct. 2006.

[37] Wen-Guey Tzeng, "Efficient 1-out-n oblivious transfer schemes," Proceedings of the Public-Key Cryptography (PKC '02), pages 159–171. 2002.

[38] Yi Mu, Junqi Zhang, and Vijay Varadharajan, "m out of n Oblivious Transfer," Proceedings of the 7th Australasian Conference on Information Security and Privacy (ACISP '02),LNCS, Vol. 2384, pp.395-405. 2002

[39] Yi Mu, Junqi Zhang, Vijay Varadharajan, and Yan-Xia Lin, "Robust Non-Interactive Oblivious Transfer," IEEE Communication Letters, Vol. 7, No. 4,Apr. 2003.