Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 12 November 2018 doi:10.20944/preprints201811.0255.v1

Peer-reviewed version available at *Appl. Sci.* **2018**, *8*, 2546; doi:10.3390/app8122546

Article

A more efficient conditional private preservation scheme in Vehicular Ad Hoc Networks

Tao Wang [1,†,*], Xiaohu Tang [1,]

1 School of Information Science and Technology, Southwest Jiaotong University, Chengdu 610000, China
2 School of Information Science and Technology, Southwest Jiaotong University, Chengdu 610000, China
* Correspondence: nirro@163.com; Tel.: +86-138-8093-3379
† Current address: Affiliation 3

Version November 12, 2018 submitted to Preprints

Abstract: It is a challenging issue to provide a secure and conditional anonymous authentication scheme in vehicle ad hoc networks(VANETs) with low storage space and computational cost. In 2008, Lu et al.[8] proposed an conditional privacy preservation scheme called ECPP protocol. The ECPP protocol provides conditional privacy preservation to vehicles in VANETs, that is, on one hand vehicles can achieve anonymous authentication in the network, on the other hand allow to be traced and revoked if necessary. However, ECPP scheme suffers from large storage and high computational cost. In our scheme, an improved protocol based on the concept of ECPP protocol has been proposed, which uses minimal interaction steps, little storage space and less computation overhead to achieve more efficiency conditional privacy preservation(MECPP) scheme in VANETs.

Keywords: Vehicular Ad Hoc Networks; Conditional Privacy; Revocation;

1. Introduction

Many people are seriously injured or killed in road traffic accidents due to carelessness, traffic congestion, traffic violations, inadequate road information, increased population and lack of secure infrastructure. Therefore, reducing traffic congestion and enhancing road safety are the issues that we people are most concerned about. With the development of wireless communication technology, VANETs have aroused widespread interest. In VANET, vehicle can send other nearby vehicles about the traffic and road conditions to warn of potential emergencies and traffic jams. In addition to helping prevent accidents, VANETs also provide convenience and business services that will help improve a driver's experience[1].

However, before taking this wonderful application into practice, security and privacy issues in VANETs must be resolved. So far, the security issues of VANETs have been studied in detail, while the privacy issues still have many open questions [2]-[4]. In the absence of privacy protection, the adversary can track the location of the target vehicle by collecting their routine information. Even worse if a legitimate anonymous vehicle becomes malicious, there is no way to identify and revoke it. Thus it is necessary to limit malicious vehicles, the privacy protection must be conditional for the vehicles which are able to be tracked and revoked if need. Therefore, how to implement conditional anonymous authentication has become a basic design requirement in VANETs.

In the past few years, many secure VANET schemes have been proposed, but there are still some unsolved problems. In [5], distributing and searching of huge certificate revocation list(CRL) is inevitable, the overhead of authentication will increase linearly with the increase of CRLs. The higher overhead of identifying and revoking malicious vehicles makes GSIS [6] and hybrid method [7] unsuitable for real-time VANETs. ECPP [8], proposed by Lu et al, is a relatively practical scheme which deals with the growing revocation list while achieving conditional traceability by the authorities, but it also suffers drawbacks: 1) It needs large space to storage every vehicle's temporary information to reveal the malicious vehicles if necessary; 2) Vehicle will interact with infrastructure unit several times during short-time anonymous key generation. It's not practical to interact many times in real word.

© 2018 by the author(s). Distributed under a Creative Commons CC BY license.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 12 November 2018 doi:10.20944/preprints201811.0255.v1

Peer-reviewed version available at Appl. Sci. 2018, 8, 2546; doi:10.3390/app8122546

To resolve these problems above, we propose a more efficient conditional private preservation scheme based on ECPP. The main contributions of this paper include the following: 1)reduces the storage space. When dispute occurs, the centralized Trusted Authority can decrypt the real identity of rogue vehicle just by certification. So it don't need to storage temporary information and that will save considerable storage space; 2)lower down half of the interaction steps during anonymous key generation phase. When vehicles move in road, the speed is usually high and it needs interacting fastly. Less interaction steps help to increase the interaction speed; 3)provides more efficient computation overhead in anonymous key generation phase. The presented performance studies and comparisons with ECPP demonstrate that our scheme is effective and efficient.

The remainder of the paper is organized as follows. In Section 2, the related work will be surveyed. In Section 3, system model, desired requirements in VANETs will be describe. We will also review the bilinear pairing techniques in Section 4. Our improved MECPP will be presented in Section 5. Section 6 will give security analysis about our protocol, followed by performance analysis in Section 7. Finally, we conclude the paper in Section 8.

2. RELATED WORK

There are many research works about anonymity authentication of VANETs in the last past years. In 2006, Gamage *et al.*[21] gave a privacy protection scheme for VANET based on ID-based ring signature. However, this scheme does not achieve conditional privacy. Later, two PKI-based authentication schemes were proposed by Raya and Hubaux[2] in which a large number of anonymous public/private key pairs and corresponding public key certificates are preloaded. Each public/private key pair has a short lifetime and is changed frequently. As a result, a larger storage capacity is required. In addition, the CRL will grow with time, their revocation protocols will encounter problems with efficiency.

3. SYSTEM MODEL AND SYSTEM SECURITY

3.1. SYSTEM MODEL

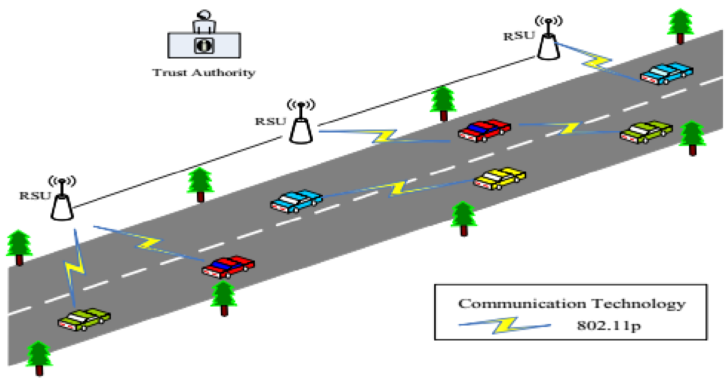

Figure 1. System Model

Figure 1 illustrate the VANET system.

System roles: VANETs generally consist of vehicles equipped with wireless communication devices which is called On Board Unit (**OBU**), infrastructure units such as Road Side Units (**RSU**s) which are located on the roadside or at a street intersection providing wireless interfaces to vehicles within their radio coverage, and a centralized Trusted Authority (**TA**) who is responsible for the RSU and OBU Registration, and what is more, recovering the vehicle's identity if it is necessary.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 12 November 2018 doi:10.20944/preprints201811.0255.v1

Peer-reviewed version available at *Appl. Sci.* **2018**, *8*, 2546; doi:10.3390/app8122546

Channels: To secure the vehicular communications which are mainly served for the civilian applications, we have following assumption about the channels:

- OBU communicates with RSU or other OBU through wireless links which is unsecured.
- RSU is assumed to connect with the TA by wired links or any other creditable links with high bandwidth, low bit error rates and low delay.

3.2. System Security

In this subsection, we present the system assumption and the desired requirements for our proposed protocol.

3.2.1. Secure VANETs Assumption

- All OBUs and RSUs are registered with the TA. The TA is infeasible to be compromised in the system and can be fully trusted by all parties.
- RSUs are usually deployed in open unattended environments which can be compromised by attackers or collude with each other. However, we assume that RSUs are monitored so that their compromise can be detected in a short time. As a result, at a given time slot, very few RSUs are compromised.
- OBUs have limited computing power and storage space while TAs have greater computational power and enough hareware.

3.2.2. Desired Requirements

- **Anonymous Vehicle Authentication.** The purpose of anonymous vehicle authentication is to verify a vehicle's authentic and legitimate while without revealing the real ID of vehicle.
- **Short-term Linkability.** In some cases, like broadcasting road condition, applications require that a recipient can link two messages sent out by the same OBU in the short-term.
- **Long-term Unlinkability.** In the long-term, messages from the same vehicle should not be able to be linked by attackers or eavesdroppers
- **Traceability and Revocation.** There must be an TA in VANETs who can trace the OBU that abuses the VANET. In addition, once the compromised OBU has been revealed, TA must revocate it immediately to prevent any further damage.
- **Non-repudiation.** Both OBUs and RSUs should not deny their behaviors and must be responsible for the decision.
- **Efficiency.** On the one hand, OBUs have resource-limited computing power to make VANETs economically viable. On the other hand, OBUs may move with the high speed. Suppose the application incorporates emergency information to be transferring to another vehicle which has more probability to meet accident, this nees a quick response from the network to pass the information. A delay less than a second may cause severe damage and result in meaningless message. Therefore, the computation overhead and communication overhead at each vehicle must be as small as possible.

4. PRELIMINARIES

4.1. Bilinear Pairing

Let G_1, G_2 be the finite additive groups and G_T be the finite multiplicative group with same order p where $|G_1| = |G_2| = |G_T| = p$, the bilinear pairing $e : G_1 \times G_2 \to G_T$ satisfies the following properties [13]:

- **Bilinearity:** The mapping $e : G_1 \times G_2 \to G_T$ is said to be bilinear if the following relation holds: $e(h_1^a, h_2^b) = e(h_1, h_2)^{ab}, \forall h_1 \in G_1, \forall h_2 \in G_2$ and $\forall a, b \in Z_p$.
- **Non-degeneracy:** There exists $h_1 \in G_1, h_2 \in G_2$ such that $e(h_1, h_2)$ is not the identity of G_T.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 12 November 2018 doi:10.20944/preprints201811.0255.v1

Peer-reviewed version available at Appl. Sci. 2018, 8, 2546; doi:10.3390/app8122546

- **Isomorphism:** ψ is an isomorphism from G_2 to G_1, with $\psi(h_2) = h_1$
- **Computability:** The bilinear map $e : G_1 \times G_2 \rightarrow G_T$ can be computed efficiently.

4.2. The Strong Diffie-Hellman Assumption

In this subsection, we state the strong Diffie-Hellman hardness assumption on which our scheme are based. Let g_1 be a generator of cyclic groups G_1 and g_2 be a generator of cyclic groups G_2. G_1 and G_2 have the same prime order p.

***q*-Strong Diffie-Hellman Problem(q-SDH).** Given a $(q+2)$-tuple $(g_1, g_2, g_2^x, g_2^{x^2}, ..., g_2^{x^q})$ as input, output a pair $(c, g_1^{\frac{1}{x+c}})$ where $c \in Z_p^*$. An algorithm A is said to has advantage ε in solving $q - SDH$ problem if

$$Pr[A(g_1, g_2, g_2^x, ..., g_2^{x^q}) = (c, g_1^{\frac{1}{x+c}})] \geq \varepsilon \tag{1}$$

where the probability is over the random choice of x in Z_p^* and the random bits consumed by A.

Theorem 1. *We say that the $(q, t, \varepsilon) - SDH$ assumption holds in (G_1, G_2) if no $t - time$ algorithm has advantage at least ε in solving the $q - SDH$ problem in (G_1, G_2).*

4.3. Weak Chosen Message Attacks

In this paper, we will prove our scheme existential unforgeability under a weak chosen message attack [20], which need the adversary submit all messages in advance and then are provided the public key and signatures. This notion is defined using the following game between a challenger and adversary A:

Query: A list of q_s messages $M_1, ..., M_{q_s} \in \{0,1\}^*$ was sent to chanllenger by adversary A.

Response: The challenger runs algorithm $KeyGen$ to generate a public key PK and private key SK and then give A the public key PK and signatures $\sigma_i = Sign(SK, M_i)$ for $i = 1, ..., q_s$.

Output: Algorithm A wins the game if a pair (M, σ) is output, where:

1. M is not in $(M_1, ..., M_{q_s})$, and
2. $Verify(PK, M, \sigma) = true$

Theorem 2. *A forger $A(t, q_s, \varepsilon)$-weakly breaks a signature scheme is A runs in time at most t, A makes at most q_s signature queries, and has advantage at least ε. A signature scheme is (t, q_s, ε)-existentially unforgeable under a weak chosen message attack if no forger (t, q_s, ε)-weakly breaks it.*

5. OUR IMPROVED MORE EFFICIENT PROTOCOL

Our MECPP protocol includes four parts: system initialization, temporary anonymous key generation, safe message sending, and fast tracking algorithm.

5.1. System Initialization

First of all, The TA generates the system parameters $(p, G_1, G_2, G_T, g_1, g_2, e)$ for each RSU and vehicle using the security parameter k. Then it chooses a random number $u \in Z_p^*$ as its master key and computes $U = g_2^u \in G_2$ as its public key. In addition, it selects two secure hash functions: f and h, where $f, h : 0, 1^* \rightarrow Z_p^*$, and a secure symmetric encryption algorithm $Enc_k()$. Finally, TA publishes all public prameters $(p, G_1, G_2, G_T, g_1, g_2, e, U, f, Enc_k())$.

5.1.1. OBU Registration Protocol

When an OBU register to system with its identity ID_i, TA does the following:

1. Check the validity of the identity ID_i. If not valid, terminate the protocol;

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 12 November 2018 doi:10.20944/preprints201811.0255.v1

Peer-reviewed version available at *Appl. Sci.* **2018**, *8*, 2546; doi:10.3390/app8122546

2. Choose a fixed-length random number $rnd \in Z_p^*$, compute the pseudo-id $PID_i = Enc_u(rnd|| ID_i||h(rnd||ID_i))$;
3. Set $S_i = g_1^{\frac{1}{h(PID_i)+u}} \in G_1$.
4. Return to OBU the private key $sk_i = (PID_i, S_i)$.

5.1.2. RSU Registration Protocol

When a RSU apply for registering, TA does:

1. Get a location information $L_i \in Z_p^*$ such that $h(L_i) + u \not\equiv 0 \bmod p$, set $A_i = g_1^{\frac{1}{h(L_i)+u}} \in G_1$;
2. Return to RSU the location-awareness key A_i, where the location-awareness key means it working at location L_i;

Subsequently, RSU itself picks a random number $x_i \in Z_p^*$ as the secret key which is used to encrypt OBU's pseudo-id.

5.2. Temporary Anonymous Key Generation

This part, we will describe how to generate the OBU temporary anonymous key.

Based on ECPP, we propose an improved protocol. First of all, the temporary anonymous information of OBU do not have to be stored by RSU. After mutual authentication, a random pseudo-id of OBU has been generated by RSU which is contained in temporary certificate. When a dispute occurs, the real identity of malicious vehicle could be recovered from temporary certification by RSU and TA together. The temporary anonymous key will be changed frequently, therefore that will help to save large storage spaces. Secondly, the interaction rounds are decreased to 3 times on the premise of mutual anthentication in our scheme, while 6 times in ECPP. Because only valid RSU at location L_j can decrypt the cihpertext to get the pseudo-id PID_i, there is no risk in disclosing its pseudo-id PID_i to an attacker. It is more practical in the real world with less interactions. Finally, computation overhead is reduced because of less pairing operation and less point multiplication.

Table 1. OBU temporary anonymous key generation

OBU(ID_i, PID_i)		**RSU**(ID_j) **at location** L_j
$R_1 = (g_2^{h(L_j)} \cdot U)^{(r_1)}$ $R_2 = e(g_1, g_2)^{r_1}$ $Y = g_1^x$ $Sig_{OBU} = S_i^{(r_1+f(R_2\|\|T_i\|\|Y))}$ $C = Enc_{R_2}(Y, T_i, Sig_{OBU}, PID_i)$		
	$\xrightarrow{(R_1,\, C)}$	
		$R_2' = e(A_j, R_1)$ decrypt C as $Dec_{R_2'}(C)$, Judge T_i and PID_i check $R_2' \cdot e(g_1, g_2)^{f(R_2'\|\|T_i\|\|Y)} \stackrel{?}{=} e(Sig_{OBU}, g_2^{h(PID_i)} \cdot U)$ issue the cetificate $Cert_i = (L_j, T_i, Y, PID_i', Sig_{RSU})$, where $PID_i' = Enc_{x_j}(T_i, PID_i)$, $Sig_{RSU} = A_j^{f(R_2'\|\|T_i\|\|Y\|\|PID_i')}$
	$\xleftarrow{(Cert_i)}$	
Judge T_i and check $e(g_2^{h(L_j)} \cdot U, Sig_{RSU}) \stackrel{?}{=} e(g_1, g_2)^{f(R_2\|\|T_i\|\|Y\|\|PID_i')}$		

- Setp 1. When an OBU go into the location L_j, it firstly compute $R_1 = (g_2^{h(L_j)} \cdot U)^{(r_1)} \in G_2$ and $R_2 = e(g_1, g_2)^{r_1}$ where $r_1 \in Z_p^*$ is a random number. Then the OBU chooses another random number $x \in Z_p^*$ as its temporary short-time anonymous private key, computes the corresponding temporary public key $Y = g_1^x \in G_1$. At last, the OBU uses its private key S_i

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 12 November 2018 doi:10.20944/preprints201811.0255.v1

Peer-reviewed version available at Appl. Sci. 2018, 8, 2546; doi:10.3390/app8122546

to make a signature $Sig_{OBU} = S_i^{(r_1+f(R_2||T_i||Y))}$ where T_i is the current time-stamp, encrypts the signature as $C = Enc_{R_2}(Y, T_i, Sig_{OBU}, PID_i)$, and sends request information (R_1, C) to the $RSU(ID_j)$.

- Step 2. After receiving the request, $RSU(ID_j)$ computes $R_2' = e(A_j, R_1)$, and decrypts the ciphertext C with R_2'. Then $RSU(ID_j)$ will check the validity of T_i and PID_i. Either of them are invalid, the protocol aborts. Otherwise, $RSU(ID_j)$ checks the equation $R_2' \cdot e(g_1, g_2)^{f(R_2'||T_i||Y)} \stackrel{?}{=} e(Sig_{OBU}, g_2^{h(PID_i)} \cdot U)$. If it holds, i.e., the OBU is authenticated, then $RSU(ID_j)$ issues the certificate $Cert_i = (L_j, T_i, Y, PID_i', Sig_{RSU})$, where $PID_i' = Enc_{x_j}(T_i, PID_i)$ and $Sig_{RSU} = f(R_2'||T_i||Y||PID_i')A_j$, the lifecycle of certification is based on time-stamp T_i; otherwise, the OBU fails the authentication since

$$\begin{aligned} e(Sig_{OBU}, g_2^{h(PID_i)} \cdot U) & \\ &= e(S_i^{(r_1+f(R_2||T_i||Y))}, g_2^{h(PID_i)} \cdot g_2^u) \\ &= e(g_1^{\frac{(r_1+f(R_2||T_i||Y))}{h(PID_i)+u}}, g_2^{(h(PID_i)+u)}) \\ &= R_2' \cdot e(g_1, g_2)^{f(R_2'||T_i||Y)} \end{aligned} \tag{2}$$

- Setp 3. To verify $RSU(ID_j)$ and the validity of certificate $Cert_i$, the OBU checks $e(g_2^{h(L_j)} \cdot U, Sig_{RSU}) \stackrel{?}{=} e(g_1, g_2)^{f(R_2||T_i||Y||PID_i')}$. If it holds, $Cert_i$ is valid and the RSU is also authenticated, because the adversary has no ability to recover the secret key R_2; Otherwise, the protocol aborts and the RSU cannot pass the authentication since

$$\begin{aligned} e(g_2^{h(L_j)} \cdot U, Sig_{RSU}) & \\ &= e(g_2^{h(L_j)} \cdot g_2^u, A_j^{f(R_2'||T_i||Y||PID_i')}) \\ &= e(g_2^{(h(L_j)+u)}, g_1^{\frac{f(R_2'||T_i||Y||PID_i')}{h(L_j)+u}}) \\ &= e(g_1, g_2)^{f(R_2'||T_i||Y||PID_i')} \\ &= e(g_1, g_2)^{f(R_2||T_i||Y||PID_i')} \end{aligned} \tag{3}$$

5.3. Safe Message Sending

1. Signing: When vehicle i wants to send message M to other surrounding vehicles, it signs on message M with the short-time anonymous public key certificate $Cert_i$ and the private key x before sending it out.
   - *Step 1*. Compute $R = g_1^r \in G_1$ where $r \in Z_p^*$ is a random number, and sign the message $s_r \equiv r + x \cdot h(M, R) (\text{mod } p)$.
   - *Step 2*. Set signature $Sig_M = (R, s_r, Cert_i)$.
2. Verification: Once receiving the message, the receiver is firstly checking the validity of T_i and $Cert_i$ like Step 3 in subsection 5.2. If invalid, the verification process aborts. Otherwise, the receiver verify the signature Sig_M by checking the equotation $g_1^{s_r} = R \cdot Y^{h(M,R)}$. If it holds, the message is ture and can be accepted, otherwise neglected.

5.4. Fast Tracking

Tracing operation is a essential issue for anonymous communication system. If a malicious vehicle makes a violation, the real identity of the signature should be revoked and transfered to the judiciary for punishment. When the TA receives the report:

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 12 November 2018 doi:10.20944/preprints201811.0255.v1

Peer-reviewed version available at Appl. Sci. 2018, 8, 2546; doi:10.3390/app8122546

- *step 1*. The TA sends the tracing demand (M, Sig_M) to the specified RSU according to the location information L_j in $Cert_i$.
- *step 2*. The RSU return the pseudo-id PID_i to TA by decrypting $PID_i = Dec_{x_j}(PID_i')$ with security key x_j.
- *step 3*. The TA recovers the real identity ID_i by decrypting $rnd||ID_i||h(rnd||ID_i) = Dec_u(PID_i)$ with master key u and then calculate $h'(rnd||ID_i)$. If $h'(rnd||ID_i) = h(rnd||ID_i)$, the ID_i and PID_i are valid and then broadcasts the pseudo-id PID_i to all RSUs. Then the malicious vehicle can not get temporary short-time anonymous key from the RSUs any more.

6. SECURITY ANALYSIS

6.1. PROVABLE SECURITY

1. Private Key Security. The TA use master key to allocate initial private keys to OBUs or RSUs during the registration stage. The security of private key is based on the *q-SDH*[18] hardness assumption. Even through several OBUs and RSUs are compromised, deducing the private keys of other OBUS and RSUs from the compromised private key is still computationally infeasible.it is still computationally infeasible to deduce other OBUs and RSUs' private keys from the compromised private keys.

Lemma 1. *If the q-SDH assumption holds in (G_1, G_2), then our scheme is secure against existential forgery under a chosen message attack.*

Proof of Lemma 1. Assume A is a forger that (t, q_S, ε)-breaks our scheme and B is an attacker which solves the $q - SDH$ problem in time t' with advantage ε by interacting with A. $(g_1, g_2, A_1, ..., A_q)$ is a instance of the $q - SDH$ problem, where $A_i = g_2^{(x^i)} \in G_2$ for $i = 1, ..., q$ and for some unknown $x \in Z_p^*$. For convenience we set $A_0 = g_2$. Algorithm B's goal is to produce a pair $(c, g_1^{\frac{1}{x+c}})$ for some $c \in Z_p^*$. It does so as follows:

Query: Algorithm A chooses a list of random pseudo-id $PID_1, PID_2, ..., PID_{q_s} \in Z_p^*$, and requests for private key of PID_i, where $q_s < q$. We may assume that $q_s = q - 1$.

Response: B must response with TA's public key and PID_i's private keys. Let $f(y)$ be the polynomial $f(y) = \prod_{i=1}^{q-1}(y + h(PID_i))$. Expand $f(y)$ and write $f(y) = \sum_{i=0}^{q-1} \alpha_i y^i$ where $\alpha_0, ..., \alpha_{q-1} \in Z_p$. Compute:

$$P_2' \leftarrow \prod_{i=0}^{q-1}(A_i)^{\alpha_i} = g_2^{f(x)} \quad and \quad K_{TA} \leftarrow \prod_{i=1}^{q}(A_i)^{\alpha_{i-1}} = g_2^{xf(x)} = (g_2')^x \tag{4}$$

Also, let $P_1' = \psi(P_2')$. The public key given to A is (P_1', P_2', K_{TA}). Next, algorithm B will generate private keys k_i for each PID_i where $i = 1, 2, ..., q - 1$. To do so, let $f_i(y)$ be the polynomial $f_i(y) = f(y)/(y + h(PID_i)) = \prod_{j=1, j\neq i}^{q-1}(y + h(PID_j))$. We expand and write $f_i(y) = \sum_{j=0}^{q-2} \beta_j y^j$. Compute

$$S_i \leftarrow \prod_{j=0}^{q-2} A_j^{\beta_j} = g_2^{f_i(x)} = (g_2')^{\frac{1}{x+h(PID_i)}} \in G_2 \tag{5}$$

Observe that $k_i = \psi(S_i) \in G_1$ is a valid private key of PID_i under the public key (P_1', P_2', K_{TA}). Algorithm B gives the $q - 1$ private keys $k_1, ..., k_{q-1}$ to A.

Output: Algorithm A returns a forgery (PID_*, k_*) such that $k_* \in G_1$ is a valid private key for PID_* and $PID_* \notin PID_1, ..., PID_{q-1}$. In other words, $e(k_*, K_{TA} \cdot (g_2')^{h(PID_*)}) = e(g_1', g_2')$. Since $K_{TA} = (g_2')^x$, we have that $e(k_*, (g_2')^{(x+h(PID_*))}) = e(g_1', g_2')$ and therefore

$$k_* = (g_1')^{\frac{1}{x+h(PID_*)}} = g_1^{\frac{f(x)}{x+h(PID_*)}} \tag{6}$$

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 12 November 2018 doi:10.20944/preprints201811.0255.v1

Peer-reviewed version available at Appl. Sci. 2018, 8, 2546; doi:10.3390/app8122546

Using long division we expand the polynomial f as $f(y) = \gamma(y)(y + h(PID_*)) + \gamma_{-1}$ for some polynimal $\gamma(y) = \sum_{i=0}^{q-2} \gamma_i y^i$ and some $\gamma_{-1} \in Z_p$. Then computing as

$$f(y)/(y + h(PID_*)) = \frac{\gamma_{-1}}{y + h(PID_*)} + \sum_{i=0}^{q-2} \gamma_i y^i \tag{7}$$

Note that $\gamma_{-1} \neq 0$, since $f(y) = \prod_{i=1}^{q-1}(y + h(PID_i))$ and $PID_* \notin PID_1, ..., PID_{q-1}$, as thus $(y + h(PID_*))$ does not divide $f(y)$. Then algorithm B computes

$$\omega \leftarrow (k_* \cdot \prod_{i=0}^{q-2} \psi(A_i)^{-\gamma_i})^{1/\gamma_{-1}} = g_1^{\frac{1}{x+h(PID_*)}} \tag{8}$$

and returns $(h(PID_*), \omega)$ as the solution to the $q - SDH$ instance.

2. Signautre Security. The security of OBU's signature Sig_M is based on the discrete logarithm assumption. It's is infeasible to output a forgery in polynomial time which makes our scheme resisitve to the impersonation attack and the bogus message spoofing attack.

Lemma 2. *If the discrete logarithm assumption holds, then the signature is secure against existential forgery under an adaptively chosen message attack.*

Proof of Lemma 2. We suppose that A who is an adversary taking message M and public key Y as input has a non-negligible probability to output an existential forgery in polynomial time. Then A can get two forgeries for the same message according to the forking lemma [19]. Let $Sig_M = (R, s_1)$ and $Sig'_M = (R, s_2)$ are the two signature forgeries respectively, where $R = g_1^r, s_1 = r + x \cdot h(M, R)$ mod p and $s_2 = r + x \cdot h'(M, R)$ mod p. Then we have the following equation.

$$s_1 - s_2 = x(h(M, R) - h'(M, R)) \quad mod \quad p \tag{9}$$

Hence

$$x = (s_1 - s_2)(h(M, R) - h'(M, R))^{-1} \quad mod \quad p \tag{10}$$

As can be seen from the above, x can be computed successfully. But it contradicts with the discrete logrithm assumption. Therefore, Sig_M is unforgeable.

6.2. FURTHER SECURITY ANALYSIS OF THE PROPOSED SCHEME

1. Mutual Authentication. Our scheme realizes mutual authentication between the RSU and the OBU by the request-response protocol.

- *The RSU can quickly authenticate the OBU.* In Step 2 of Subsection 5.2, if the verification equation $R'_2 \cdot e(g_1, g_2)^{f(R'_2||T_i||Y)} = e(Sig_{OBU}, g_2^{h(PID_i)} \cdot U)$ holds, the OBU can authenticated with pseudo-id PID_i. Since the private key is secure according to **Lemma 1**, therefore Sig_{OBU} is unforgeable, and no adversary can launch an impersonations attack on the RSU.
- *The OBU can also efficiently authenticate the RSU at location L_j.* In Step 3 of Subsection 5.2, if the equation $e(h(L_j)P_2 + U, Sig_{RSU}) = e(g_1, g_2)^{f(R_2||T_i||Y||PID'_i)}$ holds, the RSU is authenticated. Because the adversary is infeasible to recover the correct R_2 without knowing the RSU's private key $A_j = g_1^{\frac{1}{h(L_j)+u}}$.

2. Anonymous Vehicle Authentication. The OBU's identity can be kept perfectly anonymous in this protocol, since the real ID of OBU is not known to the RSU and other vehicles except the TA.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 12 November 2018 doi:10.20944/preprints201811.0255.v1

Peer-reviewed version available at Appl. Sci. 2018, 8, 2546; doi:10.3390/app8122546

- When the OBU requests for a short-time anonymous key, it sends to RSU the pseudo-id $PID_i = Enc_u(rnd||ID_i)$ which is a random identity mark, and RSU does not know who it is.
- When OBUs communicate each other, OBU uses a random pseudo-id $PID_i' = Enc_{x_j}(T_i, PID_i)$ to denote the identity, it is different with time going by and it has no means to other OBUs.

3. Short-term Linkability. Since the anonymous key is valid for a short time interval, any message signed by that key can be linked.

4. Long-term Unlinkability. In order to protect the privacy of the driver, we require that the information sent by the same vehicle be unlinkable in the long-term. We calculate the probability to quantify the risk that the victim OBU is tracked by some compromised RSUs. Here we give some assumptions:

- The RSUs may be compromised because of the insecure environment, but will be quickly rescued in the next period. We assume that the number of RSUs is N_{rsu}, and at most probability p_c RSUs can be compromised. Then the number of compromised RSUs is $N_c = N_{rsu} * p_c$.
- We assume that the number of anonymous keys that an OBU requests at some period is N_k.

Let $Pr\{i\}$ represent the probability that exactly i $(i \geq 2)$ among N_k anonymous keys are requested from different compromised RSUs, we have $Pr\{i\} = \frac{\binom{N_{rsu}-N_c}{N_k-i}\binom{N_c}{i}}{\binom{N_{rsu}}{N_k}}$. Then the probability is

$$\begin{aligned} Pr\{i \geq 2\} &= 1 - Pr\{i = 0\} - Pr\{i = 1\} \\ &= 1 - \frac{\binom{N_{rsu}-N_c}{N_k}\binom{N_c}{0} + \binom{N_{rsu}-N_c}{N_k-1}\binom{N_c}{1}}{\binom{N_{rsu}}{N_k}} \end{aligned} \tag{11}$$

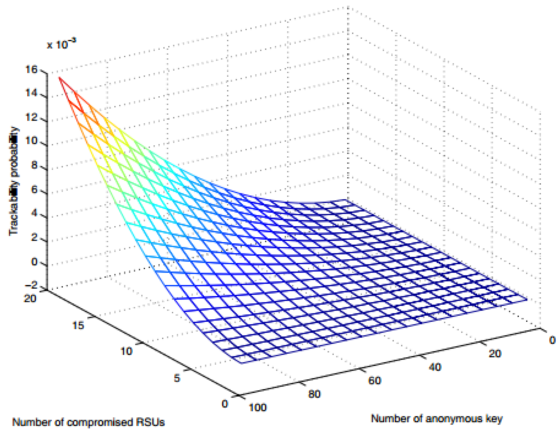

Figure 2. Tracking Probability

From Figure 2 below, it can be seen that the tracking probability increases very slowly with the increase of the number of anonymous keys and the number of compromised RSUs. So it is long-term unlinkability.

6. Traceability. Even if the message does not contain identifying information about vehicles, by using our Fast Tracking algorithm describe in Subsection 5.4, the TA can recover the real identity of the malicious vehicle if required.

7. Non-repudiation. It is obvious that signature Sig_{OBU} of OBU can provide the non-repudiation proof on the OBU's temporary anonymous key requesting, while signature Sig_{RSU} of RSU provide the non-repudiation proof on cert issue.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 12 November 2018 doi:10.20944/preprints201811.0255.v1

Peer-reviewed version available at Appl. Sci. 2018, 8, 2546; doi:10.3390/app8122546

7. PERFORMANCE ANALYSIS

In this section, we compare the performance of the proposed protocol with ECPP.

7.1. Computation Overhead on Short-time Anonymous Key Generation

As ECPP, we give the main processing time for an MNT curve of embedding degree $k = 6$ and $160 - bitq$. The result was obtained on an Intel Pentium IV 3.0 GHZ machine [17].

Table 2. The Main Processing Time for MNT Curve

	Descriptions	Execution Time
T_{pmul}	The time for one point multiplication	0.6 ms
T_{pair}	The time for one pairing operation	4.5ms

In ECPP protocol, it requires $13T_{pmul} + 6T_{pair}$ to generate the short-time anonymous key. Let T_{ECPP} be the required time cost in ECPP, then we have:

$$T_{ECPP} = 13T_{pmul} + 6T_{pair} = 13 * 0.6 + 6 * 4.5 = 34.8$$

In our scheme, there are less pairing computation and $e(P_1, P_2)$ can be calculate in advance. Let T_{MECPP} stand for the required time cost in our MECPP protocol, so that:

$$T_{MECPP} = 7T_{pmul} + 3T_{pair} = 7 * 0.6 + 3 * 4.5 = 17.7$$

From the comparison, we can notice that our require time has decreased by about 50%. Besides, our interaction steps are decreased to 3 times while ECPP is 6 times.

7.2. RSU Storage Overhead

In ECPP, every short-time anonymous key should be storaged by RSU in order to track the malicious vehicle. While in our MECPP, pseudo-id is hidden in Cert, so the real identity could be decrypted from Cert directly, when it is necessary.

Considering that the short-time anonymous key will be changed frequently to secure the identity, it helps to save a large of storage space for RSU.

In this sense, our MECPP protocol is more practial than ECPP.

8. CONCLUSION

In this paper, we proposed an optimized protocol based on ECPP for secure vehicular communications. Our protocol not only provides the security and privacy protection to vehicles but also is more efficient than ECPP in terms of computation overhead on temporary anonymous key generation and RSU storage overhead. In the next study, we will try to improve the efficiency of batch certification on the temporary anonymous key generation phase.

Author Contributions: T.W. conceived the ideas and wrote the paper. X.H.T. revised the manuscript.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. F. Qu, Z. Wu, F.-Y. Wang, and W. Cho, "A security and privacy review of VANETs", IEEE Trans. Intell. Transp. Syst., vol. 16, no. 6, pp. 2985-2996, Dec. 2015.
2. Author2, L. The title of the cited contribution. In *The Book Title*; Editor1, F., Editor2, A., Eds.; Publishing House: City, Country, 2007; pp. 32-58, ISBN.
3. C. Zhang, R. Lu, X. Lin, P. Ho, and X. Shen, "An efficient identity-based batch verification scheme for vehicular sensor networks," in Proc. IEEE INFOCOM, Apr. 2008, pp. 246-250.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 12 November 2018 doi:10.20944/preprints201811.0255.v1

Peer-reviewed version available at Appl. Sci. 2018, 8, 2546; doi:10.3390/app8122546

4. H. Zhu, X. Lin, R. Lu, P. Ho, and X. Shen, "AEMA: An aggregated emergency message authentication scheme for enhancing the security of vehicular ad hoc networks," in Proc. IEEE ICC, May 2008, pp. 1436-1440.
5. M. Raya and J-P. Hubaux. "Securing Vehicular Ad Hoc Networks", Journal of Computer Security, Special Issue on Security of Ad Hoc and Sensor Networks, 15(1):39-68, 2007.
6. X. Lin, X. Sun, P.-H. Ho and X. Shen. "GSIS: A Secure and Privacy-Preserving Protocol for Vehicular Communications", IEEE Transac. on Vehicular Technology, vol. 56, no. 6, pp. 3442-3456, 2007.
7. G. Calandriello et al., "Efficient and Robust Pseudonymous Authentication in VANET", Proceedings of the fourth ACM international workshop on vehicular ad hoc networks 2007, Montreal, Quebec, Canada, Sep. 10 2007.
8. R. Lu, X. Lin, H. Zhu, P. -H. Ho and X. Shen, "ECPP: Efficient Conditional Privacy Preservation Protocol for Secure Vehicular Communications", proceedings of the IEEE INFOCOM, Phoenix, AZ, pp. 1229-1237, 2008.
9. U.S. Department of Transportation, National Highway Traffic Safety Administration, Vehicle Safety Communications Project—Final Rep. Apr. 2006. [online]. Available: http://www.nhtsa.gov/DOT/NHTSA/NRD/Multimedia/PDFs/Crash
10. M.Raya and J.-P. Hubaux, "The security of vehicular ad hoc networks", in proc. 3rd ACM Workshop Security AD Hoc Sens. Netw., 2005,pp. 11-21.
11. D. Boneh, X. Boyen, and H. Shacham, "Short group signatures", in Advance in cryptology – CRYPTO 2004, LNCS 3152, pp. 41-55, Springer-Verlag, 2004.
12. X. Lin, X. Sun, P. H. Ho, and X. Shen, "GSIS: a secure and privacy preserving protocol for vehicular communications", IEEE Transaction on Vehicular Technology, Vol. 56, No. 6, pp. 3442-3456, 2007.
13. Camenisch, J., Lysyanskaya, A.: Signature Schemes and Anonymous Credentials from Bilinear Maps. In: Franklin, M. (ed.) CRYPTO 2004. LNCS, vol. 3152, pp. 56-72. Springer, Heidelberg (2004)
14. Nan Xiang-hao, Chen Zhong, Summary of Network Security Technology, National Defence Industry Press , 2003.
15. Nan Xiang-hao, CPK Cryptography and Internet Security, National Defence Industry Press, 2008.12
16. A. Miyaji, M. Nakabayashi, and S. Takano, "New explicit conditions of elliptic curve traces for FR-reduction", IEICE Transactions on Fundamentals, Vol. E84-A, No. 5, pp. 1234-123, 2001.
17. M. Scott, "Efficient implementation of crytographic pairings," [Online]. Available: http://ecrypt-ss07.rhul.ac.uk/ Slides/Thursday/mscottsamos07.pdf
18. D. Boneh, X. Boyen, and H. Shacham. Short group signatures. In Proc. CRYPTO 2004, pages 41–55. Springer-Verlag, 2004. Lecture Notes in Computer Science No. 3152
19. D. Pointcheval and J. Stern, "Security arguments for digital signatures and blind signatures", Journal of Cryptology, Vol. 13, No. 3, pp. 361-396, 2000.
20. D. Boneh and X. Boyen. Short signatures without random oracles. In Advances in Cryptology- EUROCRYPT 2004, volume 3027 of Lecture Notes in Computer Science, pages 56-73. Berlin:Springer- Verlag, 2004.
21. C. Gamage, B. Gras, B. Crispo, and A. S. Tanenbaum, "An identity-based ring signature scheme with enhanced privacy," in Proc. SecureComm,2006, pp. 1–5.

Sample Availability: Samples of the compounds ...... are available from the authors.