JOURNAL OF INFORMATION SCIENCE AND ENGINEERING 34, 869-884 (2018)
DOI: 10.6688/JISE.201807_34(4).0005

Novel V2V Cross-Domain Communications in Heterogeneous VANETs[*]

YAN-PING LI[1], LAI-FENG LU[1,2,+] AND KAI ZHANG[1]
[1]*School of Mathematics and Information Science*
Shaanxi Normal University
Xi'an, 710119 P.R. China
[2]*Guizhou Provincial Key Lab. of Public Big Data*
GuiZhou University
Guiyang, 550025 P.R. China
E-mail: {lyp; lulaifeng}@snnu.edu.cn; 629zhangkai@163.com

Now the vehicular ad hoc networks (VANETs) are extremely inhomogeneous because the vehicles come from different manufacturers around the world. It is difficult to realize secure communications between two heterogeneous vehicles. And confidentiality and authentication are the main security goals of secure communications. In order to achieve above two security goals simultaneously in such a heterogeneous vehicular ad hoc network, two efficient signcryption schemes are proposed in this paper. The first scheme allows a vehicle registered in a public key infrastructure (PKI) to send a message to another vehicle registered in an identity-based cryptosystem (IBC). And the second scheme allows a vehicle registered in the IBC to send a message to a vehicle registered in the PKI system. Two vehicles from different public key cryptosystems can freely communicate any authenticated and encrypted message in our proposed schemes. Finally, we prove that both schemes have indistinguishability against adaptive chosen ciphertext attacks and existential unforgeability against adaptive chosen messages attacks under the hardness assumption of decisional Diffie-Hellman problem in the random oracle model. Performance analyses demonstrate our schemes have great advantages in computation, ciphertext length, communication cost and storage.

Keywords: VANETs, PKI, IBC, signcryption, heterogeneous systems

1. INTRODUCTION

With the massive development of smart devices and wireless communication technologies, vehicular ad hoc networks (VANETs) have become a significant research area for its specific applications such as road safety and traffic management. The vehicle-to-everything communications are mainly divided into vehicle to vehicle (V2V) and vehicle to infrastructure (V2I) in VANETs. Each vehicle is equiped short-range communications (DSRC) devices, which have a range of approximately 300 meters. V2V communication technology allows neighboring vehicles to transmit or exchange information, which can improve road safety, reduce traffic congestion and provide efficient traffic

---

Received January 28, 2017; revised March 16, 2017; accepted March 26, 2017.
Communicated by Ren-Hung Hwang.

[+] Corresponding author.

[*] This work was sponsored by the NFSC China 61402275, the Shaanxi Province Natural Science Basic Research Foundation (2016JM6069), the Fundamental Research Funds for the Central Universities (GK2016 0301 2, GK201402004), the scientific research foundation for the returned overseas Chinese scholars of MOHRM, the open project fund of Guizhou Provincial Key Laboratory of Public Big Data (2017BDKFJJ 026) . An earlier version of this paper was presented at the IEEE International Conference on Networking and Network Applications (NaNA2017), Kathmandu City, Nepal, from Oct. 16-19, 2017.

management. If a traffic accident vehicle adopts the way of V2I, it will firstly send the message to roadside units (RSUs) which may be too far then RSU broadcasts the message to the other vehicles. The entire process includes RSU's message source authentication and broadcasting message. If the location of RSU is far from the accident vehicle, it may be already too late for an adjacent vehicle to take measures when it receives an accident message. If the accident vehicle transfers the message by V2V's approach, it might be much faster. What's more important, V2V communication does not depend on the location of RSUs and is more flexible and free. Hence, V2V communication is urgently worth studying.

Now the main problem existing in V2V communications is how to improve the accuracy and timeliness of the exchanged data. Since plaintext messages are easily be intercepted and altered, a vehicle cannot distinguish whether the received messages are true or not. Maybe the vehicle would rather trust the authenticated and confidential messages. Hence, authentication and tamper-resistant of the message become the foremost important requirements for V2V secure communication [1, 2].

Generally, digital signature and encryption schemes which rely on public key cryptography are commonly used to achieve authentication and confidentiality, respectively. However, we usually need to simultaneously achieve above two security goals. The traditional approach is first to sign a message and then to encrypt it, called the signature-then-encryption approach. Zheng first proposed a new cryptographic primitive which is called signcryption in 1997, which fulfills both the functions of digital signature and encryption in a logical step [3]. And its cost is significantly lower than that required by the traditional signature-then-encryption approach. An *et al.* put forward the framework of signcryption in 2002 [4]. In 2007, the formal security model for signcryption was studied by Baek *et al.* [5]. The performance advantage of signcryption makes it be studied universally.

Nowadays, vehicles come from different manufacture and the onboard devices maybe adopt different public key cryptosystem. In order to guarantee secure communications between these extremely heterogeneous vehicles, we should construct cryptographic schemes that can provide authentication and confidentiality for heterogeneous vehicles in VANETs.

1.1 Related Work

Now there are two popular public key cryptosystems: public key infrastructure (PKI) and identity-based cryptosystem (IBC). In the PKI system, the certificate authority (CA) issues a signed certificate which can provide an unforgeable and trusted link between the public key and the identity of a user. In the IBC system, the public key of a user is obtained directly from his identity information, such as telephone numbers, email, addresses and social security number. Secret keys are generated by the trusted third party called private key generator (PKG). Both of the PKI and IBC are the most widely used public key cryptosystems and have a large quantity of users.

Recently many different signcryption schemes are proposed, such as PKI-based signcryption schemes [6-8], IBC-based signcryption schemes [9-13] and certificate-less signcryption schemes [14-16]. In addition, a new type of multi-receiver signcryption schemes are proposed [17-19], which are similar to broadcast encryption technology.

Unfortunately, all these schemes are homogenous, *i.e.*, both the sender and receiver are in the same public key cryptosystem. And they cannot be used in heterogeneous communications.

It is not easy to design signcryption schemes for heterogeneous V2V secure communication. Sun and Li proposed two schemes for heterogeneous V2V communication between the vehicles from two popular public key cryptosystem called public key infrastructure (PKI) and identity-based cryptosystem (IBC), respectively [20]. Unfortunately, their schemes are vulnerable to internal (insider) attacks and do not provide non-repudiation. Huang *et al.* proposed a heterogeneous signcryption scheme against insider attacks [21]. However, their scheme only allows a vehicle in the IBC to send a message to a receiver vehicle in PKI system, so do the schemes proposed in [22, 23]. A vehicle in the PKI is not allowed sending a message to a receiver in the IBC. Then, Li *et al.* solved the above problem and constructed two signcryption schemes that can provide the mutual communications for heterogeneous public key cryptosystem in [24]. Since the PKI and IBC are the mainstream public key cryptosystems, this paper also supposes vehicles registered in the PKI or IBC cryptosystem and considers the scenarios that a vehicle in the PKI (or IBC) roaming to another region or country that belongs to the IBC (or PKI) system.

1.2 Our Contributions

In this paper, two new efficient bidirectional signcryption schemes (abbreviated as HVCS-I and HVCS-II) are constructed to provide heterogeneous V2V communications (see Fig. 1), in which different vehicles register in PKI or IBC. Compared with the existing schemes, our schemes have the following features:

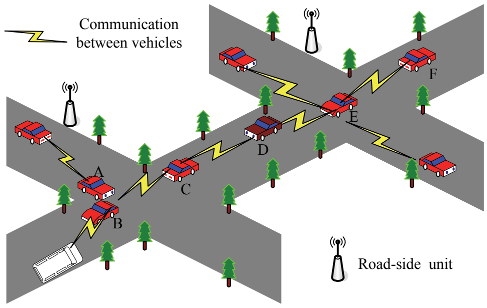

Fig. 1. The application scenarios for our schemes.

- Firstly, our proposed scheme can provide bidirectional heterogeneous V2V communications. To be specific, HVCS-I can realize a vehicle in the PKI system directly send a message to a vehicle in the IBC, and HVCS-II can realize a vehicle in the IBC system directly send a message to a vehicle in the PKI;
- Secondly, our proposed HVCS-I and HVCS-II signcryption schemes only consists of one group element and *n* bits, which have a lower storage and communication cost than other related schemes. In addition, the whole process of signcryption and unsigncryption algorithm in HVCS-I and HVCS-II only needs two pairing computations and two scalar multiplications, which is highly efficient in computation;

- Thirdly, both schemes have been proven to be indistinguishable against adaptive chosen ciphertext attacks (IND-CCA2) and existential unforgeable against adaptive chosen messages attacks (EUF-CMA) under the hardness assumption of decisional Diffie-Hellman problem (DDHP) in the random oracle model.

The rest of this paper is organized as follows. The preliminaries and the generic security models for our schemes are introduced in Section 2. Then two efficient signcryption schemes are proposed in Section 3 and their security proofs are given in Section 4. In Section 5, we discuss the security and performance of our proposed scheme. Finally, we make some conclusions in Section 6.

2. PRELIMINARIES

2.1 Bilinear Pairing

Let G/G_1 be an additive/a multiplicative group of prime order q, respectively. A map e: $G \times G \rightarrow G_1$ is called a bilinear map if it satisfies the following three properties:

Bilinear: *i.e.* $\forall P, Q \in G, a, b \in Z^*_p, (aP, bQ) = e(P, Q)^{ab}$;
Nondegenerate: There exist $P, Q \in G$, such that $e(P, Q)^{ab} \neq 1_{G_1}$;
Computable: For all $P, Q \in G$, there exists an efficient algorithm to compute $e(P, Q) \in G_1$. Please see [1, 10] for more details.

2.2 Computation Assumptions

The security of our proposed schemes is based on the decisional Diffie-Hellman problem (DDHP), that is, given $(P, aP, bP, cP) \in G$, to determine whether $ab = c \bmod q$ holds or not, where $a, b, c \in Z^*_q$ are unknown and P is a generator of cyclic group G with order q. The intractability assumption of DDHP is that, there is no algorithm solves DDHP in polynomial time with non-negligible probability.

2.3 Framework of a Heterogeneous Signcryption Scheme

Our heterogeneous signcryption schemes mainly consist of the following five algorithms.

Setup: This algorithm is performed by PKG. Input a security parameter l to the algorithm, it outputs the system master secret *msk* and master public key P_{pub} and a list of system parameters **params.**

PKI-KG: This is a key generation algorithm for PKI users. The user chooses its secret key *sk* and publish the corresponding public key *pk*.

IBC-KG: This key generation algorithm is designed for IBC users. A user submits an identity *ID* to its PKG. The PKG computes the corresponding secret key *sk* and transmits it to the user in a secure way. In this case, the user's identity *ID* is his public key, which does not need to be signed by PKG.

Signcryption: Input **params**, a message m, a sender's identity ID_s and his secret key sk_s, and a receiver's identity ID_r or his public key pk_r, the algorithm outputs a signcryption ciphertext σ of message m.

Unsigncryption: The receiver V_r with identity ID_r performs this algorithm. Input the signcrypted ciphertext σ, the sender V_s's identity ID_s and corresponding public key pk_s, and the receiver's identity ID_r and his secret key sk_r, this algorithm outputs the message m or $\perp$ which means unsigncryption fails.

2.4 Security Models of a Heterogeneous (PKI-IBC) Signcryption Scheme

A signcryption scheme should satisfy confidentiality (*i.e.* indistinguishability against adaptive chosen ciphertext attacks, or IND-CCA2, for short) and unforgeability (*i.e.* existential unforgeability against adaptive chosen messages attacks, EUF-CMA). We slightly modify the notion to adapt for heterogeneous signcryption scheme. For simplicity, PKI-IBC denotes the case that senders belong to the PKI system and receivers belong to the IBC system. And IBC-PKI denotes the case that senders belong to the IBC system and receivers belong to the PKI system.

Definition 1 (Confidentiality in PKI-IBC): A PKI-IBC signcryption scheme is said to be IND-CCA2 secure if no polynomially bounded adversary has a non-negligible advantage in the following game.

Initial: The challenger $\mathcal{C}$ runs **Setup** and **PKI-KG** algorithms with a security parameter l and sends the public parameters **params** and a sender's pk^*_s to the adversary $\mathcal{A}$.

Phase 1: The adversary $\mathcal{A}$ can perform a polynomially bounded number of the following types of queries in an adaptive way.

- Hash queries: $\mathcal{A}$ can request any hash value, $\mathcal{C}$ returns the corresponding value.
- Key generation queries: $\mathcal{A}$ chooses an identity ID, $\mathcal{C}$ runs **IBC-KG** algorithm and sends the corresponding secret key sk_{ID} to $\mathcal{A}$.
- Unsigncrypt queries: $\mathcal{A}$ produces a receiver's identity ID_r and a signcrypted ciphertext σ. $\mathcal{C}$ first runs **IBC-KG** algorithm to generate the receiver's secret key sk_{ID_r}. Then $\mathcal{C}$ runs **Unsigncrypt**(σ, pk^*_s, sk_{ID_r}) algorithm and sends the result to $\mathcal{A}$ (the result can be the $\perp$ symbol if σ is an invalid ciphertext).

Challenge: $\mathcal{A}$ decides when to end Phase 1. $\mathcal{A}$ generates two equal length plaintexts (m_0, m_1), a receiver's identity ID^*_r which he wants to challenge and sends them to $\mathcal{C}$. The secret key corresponding to ID^*_r should never been asked during **Phase 1**. $\mathcal{C}$ takes a random bit $\beta \in \{0, 1\}$ to compute $\sigma^* = \text{Signcrypt}(m_\beta, sk^*_s, ID^*_r)$ and returns σ^* to $\mathcal{A}$.

Phase 2: $\mathcal{A}$ can adaptively make a polynomially bounded number of queries again as in the Phase 1. This time, $\mathcal{A}$ cannot make a key extraction query on ID^*_r and cannot make an Unsigncrypt query on (σ, pk^*_s, sk_{ID_r}) to obtain the corresponding plaintext.

Guess: $\mathcal{A}$ produces a bit β' and wins the game if $\beta'=\beta$. The advantage of $\mathcal{A}$ is defined as Adv($\mathcal{A}$) = $|2\Pr[\beta'=\beta]-1|$, where $\Pr[\beta'=\beta]$ denotes the probability that $\beta'=\beta$.

Definition 2 (Unforgeability in PKI-IBC): A PKI-IBC signcryption scheme is said to be EUF-CMA secure if no polynomially bounded adversary has a non-negligible advantage in the following game.

Setup: The challenger $\mathcal{C}$ runs **Setup** and **PKI-KG** algorithms with a security parameter l and sends the public params and a sender's public key pk^*_s to a forger $\mathcal{F}$.

Attack: The forger $\mathcal{F}$ can perform a polynomially bounded number of the following types of queries in an adaptive way.

- Hash queries: $\mathcal{F}$ can ask the hash value of any string, $\mathcal{C}$ returns the corresponding value.
- Signcrypt queries: $\mathcal{F}$ submits a message m, a sender's identity ID_s and a receiver's identity ID_r to $\mathcal{C}$. Then $\mathcal{C}$ runs **Signcrypt**(m, sk_s, ID_r) algorithm and sends ciphertext σ to $\mathcal{F}$.

Forgery: After the above queries, $\mathcal{F}$ produces a receiver's identity ID^*_r and a new signcryption ciphertext σ^*. $\mathcal{F}$ wins the game if the outputs of **Unsigncrypt**(σ^*, pk^*_s, $sk^*_{ID_r}$) is not $\perp$.The advantage of the forger $\mathcal{F}$ is defined as the probability that it wins.

Definition 3 (Confidentiality in IBC-PKI): A IBC-PKI signcryption scheme is said to satisfy IND-CCA2 security if no polynomially bounded adversary has a non-negligible advantage in the following game.

Initial: The challenger $\mathcal{C}$ runs **Setup** and **PKI-KG** algorithms with a security parameter l and sends the system parameters params and a receiver's public key pk^*_r to $\mathcal{A}$.

The remaining phases (**Phase 1, Challenge, Phase 2** and **Guess**) are very similar to the game in **Definition 1**. Due to the limited space, we will not repeat them again.

Definition 4 (Unforgeability in IBC-PKI): A IBC-PKI signcryption scheme is said to satisfy EUF-CMA security if no polynomially bounded adversary has a non-negligible advantage in the following game.

Setup: The challenger $\mathcal{C}$ runs **Setup** and **PKI-KG** algorithm with a security parameter l and sends the params and a receiver's public key pk^*_r to the forger $\mathcal{F}$.

The remaining phases (**Attack** and **Forgery**) are very similar to the game in **Definition 2**. We will omit them here due to the limited space.

3. OUR PROPOSED HVCS-I AND HVCS-II SCHEMES

In this section, two novel and efficient signcryption schemes that provide heterogeneous V2V communications are stated as follows.

3.1 PKI-IBC Scheme (HVCS-I)

The first scheme is adapted to a scenario that a vehicle V_r who has public/secret key of IBC receives the signcryption ciphers of m from a vehicles V_s who registered in a PKI system.

Setup: Given a security parameter l, the PKG chooses a cyclic additive group G on elliptic curve which is generated by P with prime order $q \geq 2^l$, chooses a cyclic multiplicative group G_1 with the same order and a bilinear map e: $G \times G \to G_1$.The PKG also chooses cryptographic hash functions H_1: $\{0, 1\}^* \to G$, H_2: $G_1 \to \{0, 1\}^n$, n is the number of bits of a message m to be signcrypted. The PKG chooses a random $s \in Z_q^*$ as the master secret key and sets master public key $P_{pub} = sP$. PKG makes the system parameters **params** = $\{q, G, G_1, e, P, P_{pub}, H_1, H_2\}$ public and keeps $\boldsymbol{s}$ secret.

PKI-KG: A vehicle V in a PKI system chooses a random x_V from Z_q^* as its secret key $sk_V = x_V$ and computes $pk_V = x_V P$ as its public key. Below we use ($sk_s = x_s$, $pk_s = x_s P$) to denote the public/secret key pair of vehicle V_s that sends the message.

IBC-KG: A vehicle in the IBC system submits its identity ID (such as vehicle identification code, license number, *etc.*) to the PKG. The PKG computes the corresponding secret key $sk_{ID} = sH_1(ID) = sQ_{ID}$, and sends it to the vehicle in a secure way. We denote the identity of vehicle V_s which will receive the messages is ID_r and its corresponding key pair is ($pk_r = ID_r$, $sk_r = sQ_r$).

Signcrypt: Input **params**, a message m, a vehicle V_s's secret key sk_s, and a vehicle V_s's identity ID_r, this algorithm works as follows.

1. Choose a random $r \in Z_q^*$ and compute $R = rpk_s$;
2. Compute $k = e(sk_s P_{pub}, Q_r)^r$, $c = m \oplus H_2(k)$;
   The signcryption ciphertext is $\sigma = (R, c)$.

Unsigncrypt: The receiver V_r takes the signcryption σ and its private key sk_r as inputs, performs as follows:

1. Compute $k = e(R, sk_r)$; (1)
2. Compute $m = c \oplus H_2(k)$, and output the message m.

3.2 IBC-PKI Scheme (HVCS-II)

The second scheme is designed to the scenario that a vehicle V_r who has public/secret key of PKI system will receive the signcryption ciphertext of m from a vehicle V_s who registered in IBC. The detailed scheme is described as follows.

The **Setup**, **PKI-KG** and **IBC-KG** algorithms are the same as the above HVCS-I algorithm. Here we denote the sender V_s's key pair by ($pk_s = ID_s$, $sk_s = sQ_s$) and the receiver V_r's key pair by ($pk_r = x_r P$, $sk_r = x_r$).

Signcrypt: Input **params**, a message m, a sender V_s's secret key sk_s, and a receiver V_r's public key pk_r, this algorithm works as follows.

1. Choose a random $r \in Z_q^*$ and compute $R = rP_{pub}$;
2. Compute $k = e(pk_r, sk_s)^r$, $c = m \oplus H_2(k)$;
   The signcryption ciphertext is $\sigma = (R, c)$.

Unsigncrypt: The receiver V_r takes signcryption σ and its private key sk_r as inputs and performs as follows:

1. Compute $k = e(Q_s, R)^{sk_r}$; (2)
2. Compute $m = c \oplus H_2(k)$ and output the message m.

4. SECURITY PROOF OF TWO HVCS SCHEMES

In this section, the correctness and security of the proposed schemes are proved. The HVCS-I is proved to satisfy confidentiality and unforgeability by **Theorems 1** and **2**, respectively, and the HVCS-II is proved to satisfy confidentiality and unforgeability by **Theorems 3** and **4**, respectively.

4.1 Correctness

HVCS-I (PKI-IBC) scheme. We firstly prove the correctness of Eq. (1).

$$e(x_sP_{pub}, Q_r)^r = e(rx_sP, Q_r) = e(R, sk_r). \tag{3}$$

HVCS-II (IBC-PKI) scheme. The correctness of Eq. (2) is given below.

$$e(sk_s, pk_r)^r = e(sQ_sP, rx_rP) = e(Q_s, rP_{pub})^{x_r}. \tag{4}$$

Both of above equations indicate that our schemes satisfy the correctness.

4.2 Security Proof

We will prove HVCS-I and HVCS-II schemes satisfy the confidentiality and unforgeability by following Theorems 1-4, respectively. tm denotes the time to compute a scalar multiplication and tp represents the time to compute a pairing in G.

Theorem 1: In the random oracle model, if an adversary $\mathcal{A}$ has a non-negligible advantage (probability) ε against the IND-CCA2 security of HVCS-I scheme within a time span t, after asking at most q_{H_i} times H_i queries $(i = 1, 2)$, q_k times key generation queries, q_u times unsigncrypt queries, then there exists an algorithm $\mathcal{C}$ that can solve a DDHP instance in time $t' \leq t + O(q_u + 1)t_p + O(2q_{H_1} + 2q_k + 1)t_m$ with the probability $\varepsilon' \geq (1 - \frac{1}{q_k})^{q_k}(1 - \frac{1}{q_u})^{q_u}\delta\varepsilon$.

Proof: We will describe how $\mathcal{C}$ can use $\mathcal{A}$ as a subroutine to solve a given DDHP instance (P, aP, bP, cP), which is obtained by $\mathcal{C}$ in advance.

Initial: The challenger $\mathcal{C}$ runs **Setup** algorithm with a security parameter l, sets $P_{pub}=aP$ and sends the system parameters to the adversary $\mathcal{A}$. $\mathcal{C}$ also runs **PKI-KG** algorithm to get a V_s's (pk_s^*, sk_s^*) and sends pk_s^* to $\mathcal{A}$.

Phase 1: The adversary $\mathcal{A}$ can perform a polynomially bounded number of the following types of queries in an adaptive way. $\mathcal{C}$ maintains two lists L_{H_1} and L_{H_2} to simulate hash oracles H_1 and H_2. Assume that H_1 queries are distinct, and $\mathcal{A}$ will ask for $H_1(ID_r)$ before ID_r is used in any other queries and the target identity ID_r^* is submitted to H_1 at some point.

***H*₁ queries:** $\mathcal{C}$ maintains a list L_{H_1} of tuples $\{ID_{ri}, \alpha_i, Q_{ri}, D_{ri}, c_i\}$. $\mathcal{A}$ submits a query on ID_{ri}, if the request has been asked before, $\mathcal{C}$ returns the same answer from the list L_{H_1}. Otherwise, $\mathcal{C}$ then flips a coin $c_i \in \{0,1\}$ that yields 0 with probability δ and 1 with probability $1-\delta$ and performs as follows:

1. If $c_i=1$, $\mathcal{C}$ sets $Q_{ri} = bP$, $\alpha_i = \perp$, $D_{ri} = \perp$, Otherwise;
2. $\mathcal{C}$ randomly picks $\alpha_i \in Z_p^*$, computes $Q_{ri} = \alpha_i P$, $D_{ri} = \alpha_i aP$, adds $\{ID_{ri}, \alpha_i, Q_{ri}, D_{ri}, c_i\}$ to L_{H_1} list and returns Q_i.

***H*₂ queries:** $\mathcal{C}$ maintains a list L_{H_2} of tuples $\{k_i, \rho_i\}$. When $\mathcal{A}$ submits a $k_i \in G_2$ and issues an H_2 queries, $\mathcal{C}$ returns the same answer from the list L_{H_2} if the request has been asked before. Otherwise, $\mathcal{C}$ randomly chooses a string $\rho_i \in \{0, 1\}^n$ and adds $\{k_i, \rho_i\}$ to L_{H_2} list and returns ρ_i.

Key generation queries: When $\mathcal{A}$ issues a key generation query on ID_i, $\mathcal{C}$ first makes an H_1 query on ID_i and finds the tuples $\{ID_i, \alpha_i, Q_i, D_i, c_i\}$ in L_{H1} list. Then $\mathcal{C}$ returns D_i. If $ID_r = ID_r^*$, returns $\perp$.

Unsigncrypt queries: Finally $\mathcal{A}$ produces a V_r's identity ID_r and a ciphertext σ. If $ID_r = ID_r^*$, $\mathcal{C}$ returns $\perp$. Otherwise, $\mathcal{C}$ executes **Unsigncrypt**$(\sigma, pk_s^*, sk_{ID_r})$ in the normal way and returns what the **Unsigncrypt** algorithm returns.

Challenge: After queries, $\mathcal{A}$ generates two equal length plaintexts (m_0, m_1) and a V_r's identity ID_r^* on which it wants to be challenged. If $ID_r \neq ID_r^*$, $\mathcal{C}$ returns $\perp$. Otherwise, $\mathcal{C}$ takes a random bit $\beta \in \{0, 1\}$ and $r^* \in Z_q^*$, computes $c^* = H_2(e(r^* pk_s^*, cP)) \oplus m_\beta$, $r^* pk_s^* = R^*$. Then $\mathcal{C}$ returns $\sigma^* = (R^*, c^*)$ to $\mathcal{A}$. ❑

Phase 2: $\mathcal{A}$ can ask a polynomially bounded number of queries adaptively again as in the Phase 1. It is not allowed to make a key extraction query on ID_r^* and the **Unsigncrypt** query on $(\sigma^*, pk_s^*, ID_r^*)$ to obtain the corresponding plaintexts.

Guess: After $\mathcal{A}$ has made a sufficient number of queries, $\mathcal{A}$ returns its guess a bit β'. If $\beta' = \beta$, $\mathcal{C}$ outputs 1 as the answer to the DDHP instance. Otherwise, it outputs 0. The advantage of $\mathcal{A}$ is defined as $\varepsilon = |2\Pr[\beta' = \beta] - 1|$.

If $\mathcal{A}$'s guess is right, $\mathcal{A}$ should have queried the H_2 oracle with $e(r^* pk_s^*, abP)$ and saved $\{e(r^* pk_s^*, abP), \rho^*\}$ to L_{H2} list. By our setting, abP should be equal to cP.

To complete the proof, it remains to analyze $\mathcal{C}$'s advantage. Define the events E_1, E_2, E_3 and E_4 as follows.

E_1: $\mathcal{A}$ does not make a key generation query on the identity ID_r^*.
E_2: $\mathcal{C}$ does not abort an unsigncryption query.
E_3: $\mathcal{A}$ chooses ID_r^* as the V_r's identity in the challenge phase.
E_4: $\mathcal{A}$ has a ε probability to guess $\beta' = \beta$.

If all the above events happen, $\mathcal{C}$ succeeds and his advantage is $\varepsilon' = \Pr[E_1 \wedge E_2 \wedge E_3 \wedge E_4]$. We know $\Pr[E_2|E_1] = (1-\frac{1}{q_k})^{q_k}$, $\Pr[E_2|E_1] = (1-\frac{1}{q_u})^{q_u}$, $\Pr[E_3|E_1E_2] \geq \delta$, and $\Pr[E_4|E_1 E_2E_3] \geq \varepsilon$, therefore $\Pr[E_1 \wedge E_2 \wedge E_3 \wedge E_4] \geq (1-\frac{1}{q_k})^{q_k}(1-\frac{1}{q_u})^{q_u}\delta\varepsilon \cdot$

The running time for $\mathcal{C}$ is the sum of $\mathcal{A}$'s running time, the time that $\mathcal{C}$ answers queries and $\mathcal{C}$ computes the DDHP instance. During each H_1 query, key generation query, unsigncrypt queries, it needs 2,2 scalar multiplications and 1 pairing computation, respectively. There are 1 scalar multiplications and 1 pairing computation in **Challenge** phase. So $t' \leq t + O(q_u + 1)t_p + O(2q_{H_1} + 2q_k + 1)t_m$.

Remark 1: In above four games, the responses from the random oracle to $\mathcal{A}$ is uniformly random and independently distributed in G. From the $\mathcal{A}$'s view, all responses is valid and random, which are indistinguishable from the real life.

Theorem 2: In the random oracle model, if there exists a forger $\mathcal{F}$ who has an advantage ε in forging a valid signcryption ciphertext of the HVCS-I scheme within a time span t, after asking at most q_{H_i} times $H_i(i=1, 2)$ queries, q_k times key generation queries, q_s times Signcrypt queries, then a DDHP instance can be solved in $t' \leq t + O(q_u + 1)t_p + O(2q_{H_1} + 2q_k + 1)t_m$ with the probability $\varepsilon' \geq (1-\frac{1}{q_k})^{q_k}(1-\frac{1}{q_u})^{q_u}\delta\varepsilon$.

The proof of **Theorem 2** is very similar to **Theorem 1**. Due to the limited space, we omit it here.

Theorem 3: In the random oracle model, if an adversary $\mathcal{A}$ has a non-negligible advantage ε against the IND-CCA2 security of the HVCS-II scheme within a time span t, after asking at most q_{H_i} times $H_i(i=1, 2)$ queries, q_k times key generation queries, q_u times unsigncrypt queries, then there exists an algorithm $\mathcal{C}$ that can solve the DDHP within time $t' \leq t + O(q_{H_1} + q_k + 1)t_m + O(q_u + 1)t_p$ with the probability $\varepsilon' \geq \varepsilon\delta(1-\delta)^{q_k+q_{H_1}}(1-\frac{1}{q_u})^{q_u}$.

Proof: We describe how $\mathcal{C}$ can use $\mathcal{A}$ as a subroutine to solve a given instance (P, aP, bP, cP) of the DDHP.

Setup: The challenger $\mathcal{C}$ runs **Setup** algorithm with a security parameter l and sets $P_{pub} = aP$.

Attack: The adversary $\mathcal{A}$ can perform a polynomially bounded number of the following type of queries in an adaptive way. $\mathcal{C}$ maintains two lists L_{H_1} and L_{H_2} to simulate hash oracles H_i, $i = 1, 2$. And $\mathcal{C}$ also runs **PKI-KG** algorithm to get a V_r's public/secret keys and send pk_r^* to $\mathcal{A}$.

H_1 queries: $\mathcal{C}$ maintains a list L_{H_1} of tuples $\{ID_{si}, \alpha_i, Q_{si}, D_{si}, d_i\}$. $\mathcal{A}$ submits a query on ID_{si}, $\mathcal{C}$ flips a coin $d_i \in \{0, 1\}$ that yields 0 with probability δ and 1 with probability $1 - \delta$. If $d_i = 1$, $\mathcal{C}$ sets $Q_{si} = bP$, $\alpha_i = \perp$, adds $\{ID_{si}, \perp, Q_{si}, \perp, d_i\}$ to L_{H1}. Otherwise, $\mathcal{C}$ randomly picks $\alpha_i \in Z_q^*$, sets $Q_{si} = \alpha_i P$, $D_{si} = \alpha_i bP$, adds $\{ID_{si}, \alpha_i, Q_{si}, D_{si}, d_i\}$ to L_{H1} and returns Q_{si}.

H_2 queries: $\mathcal{C}$ maintains a list L_{H_2} of tuples $\{k_i, \rho_i\}$. When $\mathcal{A}$ submits a $k_i \in G_1$ and issues an H_2 queries, if the request has been asked before, $\mathcal{C}$ returns the same answer ρ_i from the list L_{H2}. Otherwise, $\mathcal{C}$ randomly chooses a string $\rho_i \in \{0, 1\}^n$ and adds $\{k_i, \rho_i\}$ to L_{H2} list and returns ρ_i.

Key generation queries: This process is similar to the challenge-response of H_1 queries. If $d_i = 1$, $\mathcal{C}$ outputs $\perp$.

Unsigncrypt queries: $\mathcal{A}$ produces a V_s's identity ID_s and a signcryption ciphertext σ. If $ID_s = ID_s^*$, $\mathcal{C}$ returns $\perp$. Otherwise, $\mathcal{C}$ executes **Unsigncrypt(**σ, sk_s, pk_r^***)** algorithm in the normal way and returns what the **Unsigncrypt** algorithm returns.

Challenge: After queries, $\mathcal{A}$ generates two equal length plaintexts (m_0, m_1) and a V_s's identity ID_s^* on which it wants to be challenged. If $ID_s \neq ID_s^*$, $\mathcal{C}$ returns $\perp$. Otherwise, $\mathcal{C}$ takes a random bit $\beta \in \{0, 1\}$ and $r^* \in Z_q^*$, computes $R^* = r^* P_{pub}$, $c^* = m_\beta \oplus H_2(e(r^* pk_r^*, cP))$, then $\mathcal{C}$ returns $\sigma^* = (R^*, c^*)$ to $\mathcal{A}$.

Phase 2: $\mathcal{A}$ can ask a polynomially bounded number of queries adaptively again as in the Phase 1. This time $\mathcal{A}$ is not allowed to make an **Unsigncrypt** query on $(\sigma^*, pk_s^*, sk_r^*)$ to obtain the corresponding plaintext.

Guess: After $\mathcal{A}$ has made a sufficient number of queries, $\mathcal{A}$ returns its guess a bit β'. If $\beta' = \beta$, then $\mathcal{C}$ outputs 1 as the answer to the DDHP. Otherwise, it outputs 0. Since the adversary is denied access to the **Unsigncrypt** oracle with the challenge signcryption, if $\mathcal{A}$'s guess is right, $\mathcal{A}$ should have queried the H_2 oracle with $e(r^* pk_r^*, abP)$ and saved $\{e(r^* pk_s^*, abP), \rho^*\}$ to L_{H2} list. By our setting, abP should be equal to cP. In this proof, the probability of $\mathcal{C}$ solving the given instance of DDHP is $\varepsilon' \geq \varepsilon\delta(1-\delta)^{q_k + q_{H_1}} \left(1 - \frac{1}{q_u}\right)^{q_u}$, and the running time of $\mathcal{C}$ is $t' \leq t + O(q_{H_1} + q_k + 1)t_m + O(q_u + 1)t_p$.

Theorem 4: In the random oracle model, if there exists an adversary $\mathcal{F}$ who has an advantage ε in forging a valid signature of the HVCS-II scheme with in a times pan t, after $\mathcal{F}$ asking at most q_{H_i} times $H_i (i = 1, 2)$ queries, q_s times Signcrypt queries, then the DDHP instance can be solved in time $t' \leq t + O(q_{H_1} + q_k + 1)t_m + O(q_u + 1)t_p$ with the probability $\varepsilon' \geq \varepsilon\delta(1-\delta)^{q_k + q_{H_1}} \left(1 - \frac{1}{q_u}\right)^{q_u}$.

5. APPLICATION AND PERFORMANCE EVALUATION

Here, we give an example of the potential application of our schemes. Suppose the vehicle A collided with the vehicle B in Fig. 1. In order to avoid traffic jams, the vehicle A and B would signcrypt the collision message to surrounding vehicles by V2V (for example, the propagation of B→C→D→E→F approximately needs 30 seconds) and the other vehicles can go round early. Hence, it can prevent more vehicles from joining the traffic jams. The reason for signcrypting the message is to ensure the message authentication and the source's reliability. Nobody can decrypt the signcrypted message except the designated vehicle. If any vehicle sends distorted news, it will be blacklisted by other vehicles, and unable to share message with others. Based this risk, most vehicle should send true information honestly.

Many existing signcryption schemes [3-19] all need the sender and the receiver registered on the same public key cryptosystem. And these schemes are not suitable for heterogeneous scenarios. Although schemes proposed in [20-23] can provide heterogeneous communications, the schemes in [20] do not resist the insider attack and the schemes in [21-23] only support one-way communication (*i.e.* IBC-PKI). Only the schemes in [24] and our schemes can realize heterogeneous secure mutual communications. The performance and security comparisons of our schemes with the schemes in [22-24] are given. The results are illustrated in Tables 1 and 2.

From Table 1, the ciphertext size of our schemes is shortest in all related schemes, regardless of the size of m and G. The specific bytes are based on the common assumption that $|G|$=160bits, $|m|$ =160bits and |ID|=80bits. Therefore, the communication cost and storage of our schemes also decrease with the shorter ciphertext length.

In Table 2, t_m, t_p, t_{inv} and t_e denote the times to perform one scalar multiplication, a pairing evaluation in G, an inverse operation in Z_q^* and an exponent operation in G_1, respectively. Here the time of hash t_h and XOR is negligible because t_h and XOR are very lightweight compared with t_p, t_m. n is the number of user set.

Table 1. Comparisons of security features and ciphertext length.

Scheme	PKI-IBC	IBC-PKI	Hardness assumption	Provable security	Ciphertext length
Scheme in [22]	×	√	q-BDHIP	Yes	(IBC-PKI) $\|m\|+3\|G\|$ (80bytes)
Scheme in [23]	×	√	DDHP	Yes	(IBC-PKI) $\|m\|+(n+1)\|G\|+n\|ID\|$ $(40+30n)$ bytes
Schemes in [24]	√	√	q-BDHIP	Yes	(IBC-PKI) $\|m\|+2\|G\|$(60bytes) (PKI-IBC) $\|m\|+2\|G\|$(60bytes)
Our Schemes	√	√	DDHP	Yes	(IBC-PKI) $\|m\|+\|G\|$(40bytes) (PKI-IBC) $\|m\|+\|G\|$(40bytes)

Table 2. The comparison of computation overhead of related schemes.

Schemes	PKI-setup	IBC-setup	Signcryption *assumption*	Unsigncryption Whole computation *length*	Energy Consumption
Scheme in [22]	t_m+t_{inv}	t_m+t_{inv}	(IBC-PKI)$t_e+3t_m+t_{inv}$	$t_p+t_e+2t_m+t_{inv}$	170.88+5.68mJ
Scheme in [23]	t_m	t_m	(IBC-PKI)$(n+3)t_m$	$2t_p+n\ t_m$	149.52+38.88n+2.84+2.13mJn
Schemes in [24]	t_m+t_{inv}	t_m+t_{inv}	(PKI-IBC)t_e+3t_m	$2t_p+t_e+t_{inv}$	
			(IBC-PKI)t_e+2t_m	$2t_p+t_e+t_m+t_{inv}$	214.32+4.26 mJ
Our Schemes	t_m	t_m	(PKI-IBC)t_p+2t_m	t_p	
			(IBC-PKI)t_p+2t_m	t_p	130.08+2.84 mJ

From Table 2, we can see the computational complexity of our schemes is significantly smaller than those of the other three protocols, whether in the setup phase or in the signcryption/unsigncryption phases. The average execution time of the operation t_p is about 1.9s, a t_e operation in G_1 takes 0.9s using the supersingular elliptic curve $y^2 + y = x^3 + x$ and a t_m operation takes 0.81s [23] (the experiment data from tests on the widely used MICAz platform that is equipped with an ATmega128L 8-bit processor clocked at 7.3728MHz, 4KB RAM and 128KB ROM). We give a quantitative analysis of schemes in [22, 24] and our scheme just for IBC-to-PKI communications that is provided by all the above schemes. Note that the scheme in [23] is omitted in Figs. 2 and 3 because its computation grows linearly with the number of group members (n) and is more time-consuming. A t_{inv} operation in G_1 also be taken as 0.9s although a t_{inv} operation is more time-consuming than a t_e operation in theory. The whole computation time includes the computation time in signcryption and unsigncryption phases.

The total energy consumption in Fig. 3 includes the computational energy and the communication energy consumption. As in [25], a pairing operation consumes 3V×8mA ×1.9s=45.6mJ, a scalar multiplication consumes 3V×8mA×0.81s=19.44mJ, an exponent operation consumes 3V×8mA×0.9s=21.6mJ, here we suppose $t_{inv} \approx t_e$. In addition to computation energy consumption, the energy consumption on receiving a message of x bytes $W_r = V \times I_r \times x \times 8/d_r$,where I_r is the current draw in receiving mode and d_r is the data rate. In MICAz, I_r = 8mA/10mA/27mA when the current draw is in active/receiving/ transmitting mode and d_r = 12.4kbps. A sensor consumes 3V×10mA×8/12400=0.019mJ and 3V×27mA×8/12400=0.052mJ to receive and transmit one byte message. Combined with the ciphertext length in Table 1, we give the energy consumption in Table 2 and the comparisons of the relevant schemes are given in Fig. 3 (just for IBC-PKI that the above schemes all can provide). From Table 2, we know a vehicle only need 132.92mJ energy to receive and unsigncrypt a message, then signcrypt and transmit a new message. A vehicle only needs 5.42s to unsigncrypt and signcrypt a message. The computational time and energy consumption are viable and sound for practical VANETs applications.

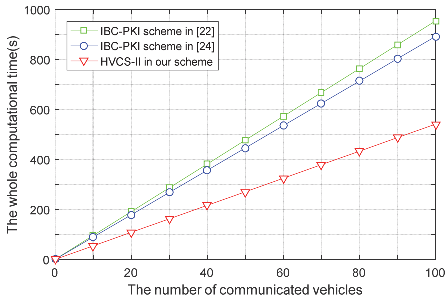

Fig. 2. Comparisons of the computational overhead.

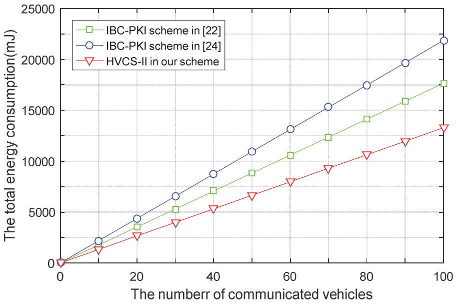

Fig. 3. The total energy consumption versus vehicle number.

6. CONCLUSIONS

In this paper, we proposed two signcryption schemes for heterogeneous V2V communication in VANETs. They can setup a secure channel between vehicles that support end-to-end confidentiality and authentication services. And our schemes can provide a solution when a vehicle in the PKI (IBC) system roaming to another region/domain that belongs to the IBC (PKI) system. Both schemes have been proven to be indistinguishable against adaptive chosen ciphertext attacks and existential unforgeability against adaptive chosen messages attacks under the decisional Diffie-Hellman problem in the random oracle model. As compared with recently existing schemes, the schemes proposed in this paper have great advantages in terms of computation, storage, ciphertext size and communication cost as showed in Tables 1 and 2, Figs. 2 and 3. The ongoing work is to design V2I signcryption schemes by making full use of the strong computational ability of roadside facilities.

REFERENCES

1. X. Li, J. Niu, S. Kumari, *et al.*, "A robust biometrics based three-factor authentication scheme for global nobility networks in smart city," *Future Generation Computer Systems*, https://doi.org/10.1016/j.future.2017.04.012.
2. X. Li, J. Niu, S. Kumari, *et al.*, "A three-factor anonymous authentication scheme for wireless sensor networks in IoT environments," *Journal of Network and Computer Applications*, https://doi.org/10.1016/j.jnca.2017.07.001.
3. Y. Zheng, "Digital signcryption or how to achieve cost (signature and encryption) $\ll$cost(signature)+cost(encryption)," in *Proceedings of Advances in Cryptology*, 1997, pp. 165-179.
4. J. H. An, Y. Dodis, and T. Rabin, "On the security of joint signature and encryption," in *Proceedings of International Conference on the Theory and Applications of Cryptographic*, 2002, pp. 83-107.
5. J. Baek, R. Steinfeld, and Y. Zheng, "Formal proofs for the security of signcryption," *Journal of Cryptology*, Vol. 20, 2007, pp. 203-235.
6. J. Malone-Lee and W. Mao, "Two birds one stone: signcryption using RSA," in *Proceedings of Topics in Cryptology*, 2003, pp. 211-225.
7. C. Li, G. Yang, D. Wong, *et al.*, "An efficient signcryption scheme with key privacy and its extension to ring signcryption," *Journal of Computer Security*, Vol. 18, 2010, pp. 451-473.
8. C. Zhou, "An improved multi-receiver generalized signcryption scheme," *International Journal of Network of Security*, Vol. 17, 2015, pp. 340-350.
9. S. S. M Chow, S. M. Yiu, L. C. K Hui, *et al.*, "Efficient forward and provably secure ID-based signcryption scheme with public verifiability and public ciphertext authenticity," in *Proceedings of International Conference on Information Security and Cryptology*, 2004, pp. 352-369.
10. L. Chen and J. Malone-Lee, "Improved identity-based signcryption," in *Proceedings of International Conference on Public Key Cryptography*, 2005, pp. 362-379.
11. G. Enos and Y. Zheng, "An ID-based signcryption scheme with compartmented secret sharing for unsigncryption," *Information Processing Letters*, Vol. 115, 2015, pp. 128-133.
12. Y. Sun and H. Li, "ID-based signcryption KEM to multiple recipients," *Chinese Journal of Electronics*, Vol. 20, 2011, pp. 317-322.

13. Y. Zhang, X. Chen, and H. Li. "Key-evolving hierarchical ID-based signcryption," *The Computer Journal*, Vol. 56, 2013, pp. 1228-1248.
14. Z. Liu, Y. Hu, X. Zhang, *et al.*, "Certificateless signcryption scheme in the standard model," *Information Sciences*, Vol. 180, 2010, pp. 452-464.
15. W. Shi, N. Kumar, P. Gong, *et al.*, "Cryptanalysis and improvement of a certificateless signcryption scheme without bilinear pairing," *Frontiers of Computer Science*, Vol. 8, 2014, pp. 656-666.
16. H. Yu and B. Yang, "Provably secure certificateless hybird signcryption," *Chinese Journal of Computers*, Vol. 38, 2015, pp. 804-813.
17. S. Lal and P. Kushwah, "Anonymous ID-based signcryption scheme for multiple receivers," *IACR Cryptology ePrint Archive*, 2012, 2009.
18. L. Pang, H. Li, J. Cui, *et al.*, "Design and analysis of a fair ID-based multi receiver anonymous signcryption," *Journal of Software*, Vol. 25, 2014, pp. 2409-2420.
19. Y. S. Rao and R. Dutta, "Efficient attribute-based signature and signcryption realizing expressive access structures," *International Journal of Information Security*, Vol. 15, 2016, pp. 1-29.
20. Y. Sun and H. Li, "Efficient signcryption between TPKC and IDPKC and its multi-receiver construction," *Science China Information Sciences*, Vol. 53, 2010, pp. 557-566.
21. Q. Huang, D. S. Wong, and G. Yang, "Heterogeneous signcryption with key privacy," *The Computer Journal*, Vol. 54, 2011, pp. 525-536.
22. F. Li and P. Xiong, "Practical secure communication for integrating wireless sensor networks into the internet of things," *IEEE Sensors Journal*, Vol. 13, 2013, pp. 3677-3684.
23. F. Li, Z. Zheng, and C. Jin, "Secure and efficient data transmission in the internet of things," *Telecommunication Systems*, Vol. 62, 2016, pp. 111-122.
24. F. Li, H. Zhang, and T. Takagi, "Efficient signcryption for heterogeneous systems," *IEEE Systems Journal*, Vol. 7, 2013, pp. 420-429.
25. K. A. Shim, "S^2DRP: Secure implementations of distributed reprogramming protocol for wireless sensor networks," *Ad Hoc Networks*, Vol. 19, 2014, pp. 1-8.

Yan-Ping Li (李艳平) received her M.S. degree from Shaanxi Normal University in 2004 and Ph.D. degree from Xidian University in 2009, Xian, China. She now is an Associate Professor with the School of Mathematics and Information Science, Shaanxi Normal University. Her research interests include public key cryptography and its applications.

Lai-Feng Lu (鲁来凤) received M.S. and Ph.D. degrees in Computer System Architecture from Xidian University, Shaanxi, China, in 2005 and 2012, respectively. Now she is an Associate Professor in Shaanxi Normal University. Her research interests include privacy protection and ad hoc network security.

Kai Zhang (张凯) received the M.S. degree in Applied Mathematics from Shaanxi Normal University in 2013 and Ph.D. degree in from Xidian University in 2017, Shaanxi, China. Now he is a Lecture in Shaanxi Normal University. His research interests include information security and privacy, and applied cryptography.