EP^{2}DF: An Efficient Privacy-Preserving Data-Forwarding Scheme for Service-Oriented Vehicular Ad Hoc Networks

Xiaolei Dong, Lifei Wei, Haojin Zhu, *Member, IEEE*, Zhenfu Cao, *Senior Member, IEEE*, and Licheng Wang

***Abstract*—Service-oriented vehicular ad hoc networks (VANETs) are expected to support the diverse infrastructure-based commercial services, including Internet access, real-time traffic concerns, video streaming, and content distribution. The success of service-oriented VANETs depends on the underlying communication system to enable the user devices to connect to a large number of communicating peers and even to the Internet. This poses many new research challenges, particularly on the aspects of security and user's privacy. In this paper, we propose a novel privacy-preserving data-forwarding scheme based on our proposed novel *Lite-CA-based public key cryptography* and on-path onion encryption technique. The proposed scheme is expected to not only thwart the traffic tracing attack at the minimized computational overhead but to provide an efficient way to relieve workload and deployment complexity of certificates as well. Performance comparisons and security analysis show that the proposed schemes are very efficient and suitable for service-oriented VANETs.**

***Index Terms*—Data forwarding, Lite-CA based, privacy preservation, service-oriented vehicular ad hoc networks (VANETs).**

I. Introduction

With the advancement of wireless technology, vehicular communication networks, which are also known as vehicular ad hoc networks (VANETs), are emerging as a promising approach to increase road safety, efficiency, and convenience [1], [2]. Although the primary purpose of vehicular networks is to enable communication-based automotive safety applications, e.g., cooperative collision warning [3], VANETs also enable a wide range of promising applications and services. For example, Internet access has become a part of our daily life, and there is a growing demand to access the Internet or information centers from vehicles. Therefore, the roadside units (or RSUs) can be deployed every few miles along the highway for users to download maps, traffic data, and multimedia files. Vehicles can use RSUs to report real-time traffic information and request location-based services such as finding restaurants, gas stations, or available parking space [4]. We call these types of vehicular networks service-oriented vehicular networks [5], which are expected to provide clear customer benefits and motivate commercial operators to invest in large-scale deployments of wireless infrastructures.

Over the past several years, there have been quite a few studies on how to realize efficient data routing/forwarding in vehicular networks [6], [7]. However, vehicular networks have brought new security challenges due to their mobile and infrastructureless nature. In particular, confidentiality and location privacy are regarded as the most critical security concerns for securing service-oriented vehicular networks. Specifically, the service requester should ensure that the service contents are delivered in an appropriate way that no third parties could uncover the transmitted message and the location privacy of vehicular nodes could be preserved from external attackers. In service-oriented vehicular networks, nodes need to frequently send messages to RSUs via intermediate nodes to retrieve information from backbone Internet servers. Such a data-forwarding process may incur serious privacy leakage at the presence of external attackers, which could compromise the nodes' location privacy by monitoring the transmitted traffic.

Although there are various security proposals for securing VANETs, most of them focus on location privacy within one-hop transmission [8]–[10]. For example, when privacy-conscious nodes authenticate themselves to others, they may take advantage of the multiple pseudonym approach to avoid revealing privacy-sensitive information [11]. In the multiple pseudonym approach, every vehicular node periodically updates its public information to impede an adversary from linking old and new pseudonyms. However, this approach works well for single-hop transmission, whereas it is not suitable for service-oriented VANETs, which are characterized as multihop transmission.

To ensure security and privacy for service-oriented VANETs, in this paper, we propose an efficient privacy-preserving data-forwarding scheme (EP^{2}DF) for service-oriented VANETs. Basically, similar to the onion-routing technique [12], [13], EP^{2}DF enables the *on-path onion encryption* for each relaying hop and thus prevents any adversaries from tracing the message flows. Further, since the onion encryption is based on public

Manuscript received June 23, 2010; revised September 26, 2010; accepted October 11, 2010. Date of publication November 29, 2010; date of current version February 18, 2011. This work was supported in part by the Key Program of the National Natural Science Foundation of China under Grant 61033014, by the National Natural Science Foundation of China under Grant 60773086, Grant 60970110, Grant 60972034, Grant 60973159, and Grant 61003218, and by the National Fundamental Research Development Program of China (973) under Grant 2007CB311201. The review of this paper was coordinated by Dr. L. Cai.

X. Dong, L. Wei, H. Zhu, and Z. Cao (Corresponding author) are with the Department of Computer Science and Engineering, Shanghai Jiao Tong University, Shanghai 200240, China (e-mail: dong-xl@cs.sjtu.edu.cn; weilifei@sjtu.edu.cn; zhu-hj@cs.sjtu.edu.cn; zfcao@cs.sjtu.edu.cn).

L. Wang is with the Beijing University of Posts and Telecommunications, Beijing 100083, China (e-mail: wanglc.cn@gmail.com).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TVT.2010.2095432

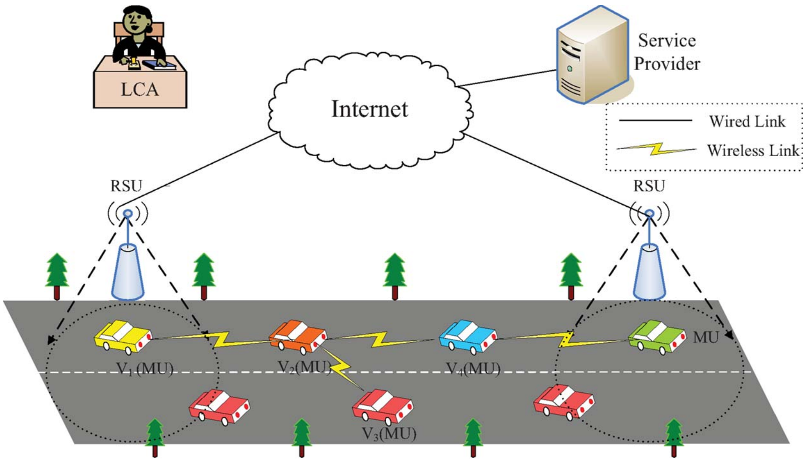


Fig. 1. System architecture.

key encryption and the conventional public key encryption schemes either incur a high computational cost or introduce a complicated public key certificate management issue [14], [15], EP^{2}DF is built on a novel encryption scheme called the *Lite-CA-based public key cryptosystem* (PKC), which originates from certificateless PKC (CL-PKC) [16]–[18] to achieve lightweight public key certificate management.

The contributions of this paper are summarized as follows.

1) First, we propose a new Lite-CA-based PKC to reduce the encryption cost and the public key certificate management complexity.
2) Second, based on the proposed Lite-CA-based PKC, we introduce a novel *on-path onion encryption* technique to achieve privacy preserving in service-oriented VANETs.
3) Finally, we evaluate the performance of EP^{2}DFs by comparing them with other schemes, discuss the advantage of our new cryptosystem, and show that it is more suitable for VANETs.

Generally, EP^{2}DF is a scheme that is extraordinarily suitable for service-oriented VANETs. Further, EP^{2}DF is also a distributed secure scheme, which does not require a centralized Certificate Authority (CA).

The rest of this paper is organized as follows: Section II presents the system architecture and the design goals. Then, the motivations of Lite-CA-based PKC are introduced in Section III. We give a formal definition of the framework and propose concrete Lite-CA-based encryption schemes based on the quadratic residues in Section IV. Our main contribution, i.e., EP^{2}DF, is designed for service-oriented vehicular network in Section V. Performance evaluation and security analysis on the proposed EP^{2}DF are given in Sections VI and VII, respectively. Further discussion on the proposed PKC is made in Section VIII. Finally, concluding remarks are made in Section IX.

II. System Architecture and Design Goals

In this section, the system model and the security requirements are presented.

A. System Architecture

Fig. 1 shows us the overall architecture of the VANET system considered in our study, which includes a *Lite Certificate Authority* (LCA), a number of fixed *Road Side Unit* (RSUs), and vehicles equipped *mobile units* (MUs) running on the road.

LCA: LCA is an organization that is responsible for key registration. In the beginning of system initialization, each vehicle or RSU has to register itself to LCA and gets back the partial public key for its key generation and system public parameters. Here, we use a novel cryptosystem to avoid certification management and key escrow problems. LCA is not required to be always online after the registration phase.

RSU: The RSUs serve as the gateway to connect service provider servers and the MUs. Usually, the RSUs are assumed that they may be compromised by attackers, whereas the service provider cannot be compromised since it is in charge of service guarantee and billing. We also assume that the RSUs could connect to service provider servers by wired links of high bandwidth capacity, low delay, and low bit error rates.

MU: In our study, the vehicles are equipped with MUs, which mainly communicate with each other for sharing local traffic information to improve safe driving conditions and with RSUs for requesting services. According to [19], the medium used for communications between neighboring MUs and between MUs and RSUs is a 5.9-GHz dedicated short-range communication identified as IEEE 802.11p. In addition, we assume that all the messages are transmitted in an encrypted form for confidential requests.

B. Design Goals

To achieve secure service-oriented VANETs, we need to achieve the following security goals:

Confidentiality: Confidentiality is a necessary goal to ensure that sensitive information is well protected and not revealed to unauthorized third parties.

Authentication: Similar to a conventional VANET system, our scheme will provide authentication to distinguish legitimate vehicles from unauthorized vehicles, including the authentication between vehicles and the authentication between the vehicle and the RSU.

Privacy: Privacy issues for service provisioning in VANETs primarily regard preserving the anonymity of a vehicle and/or the privacy of its location. Privacy protection tries to prevent the adversaries (e.g., another vehicle or an external observer) from linking the vehicle to the driver's name, license plate, speed, position, and traveling routes along with their relationships to compromise the sender's privacy. Further, we also consider how to achieve source anonymity during VANET's multihop transmission.

Note that, in addition to the foregoing security objectives, our scheme should efficiently work without introducing much extra communication and transmission overhead. To achieve this target, we introduce a novel cryptosystem "Lite-CA-based public key cryptosystem" to realize efficient data encryption/decryption, which will be presented in the next section.

III. Lite-CA-Based Public Key Cryptosystem

According to the differences of authentication frameworks, PKCs can be divided into three categories: 1) CA-based PKC; 2) identity-based PKC (IBC); and 3) the cryptosystems evolving from them, such as self-certified PKC, certificated-based PKC, CL-PKC, etc. Up to now, CA-based PKCs with public key infrastructure (PKI) are still the most popular and prevailing authentication framework. However, high key management complexity is widely regarded as one of its major drawbacks [20].

Recently, there has been an increasing interest in adopting more advanced cryptographical results, such as IBC, in service-oriented VANETs. The main idea of IBC is to make an entity's public key directly derived from publicly known identity information such as its e-mail address and thus eliminate the requirement for public key certificate transmission and storage [20] in the CA-based PKC. However, IBC also suffers from its inherent key escrow problem. For example, the authority could use its system-wide master key to decrypt any ciphertext in the IBC. To address this key escrow problem, a new public key cryptosystem, called CL-PKCs, was introduced by Al-Riyami and Paterson [16]. In CL-PKC settings, public key is generated similar to IBC, whereas the private key is divided into two parts: One is produced by the authority, and another is produced by the user itself. Therefore, compared with IBC, the security level of CL-PKC is enhanced thanks to its special secret key generation phase [18], [21]–[25]. However, although it prevents a malicious centralized authority from decrypting unauthorized ciphertext on behalf of a legitimate user, CL-PKC still faces the impersonation attack, where a malicious authority could impersonate a user by generating fake certificates. To distinguish the various PKCs, we introduce the concept of trust level [26], which is shown as follows.

1) Level 1: The authority knows the users' private keys and therefore can impersonate any user at any time without being detected.
2) Level 2: The authority does not know the users' private keys. Nevertheless, the authority can still impersonate a user by generating a fake public key or certificate.
3) Level 3: The authority does not know the users' private keys, and the frauds of the authority are detectable. Specifically, a PKC is of trust level 3 if the authority cannot compute the users' secret keys, and it can be detected if it generates fake guarantees of users.

It is obvious that only the CA-based PKC of the aforementioned PKCs achieves trust level 3. Therefore, to guarantee the security level of a large scale of VANET, it is desirable to design a novel PKC, which is not CA based, while still achieving the highest trust level. In this paper, we answer this question by proposing a Lite-CA-based PKC. The benefits of adopting Lite-CA in service-oriented VANETs are twofold. First, by introducing an explicit authentication process, our PKC could achieve trust level 3. In other words, it could easily detect the misbehavior of malicious authority. Second, the proposed scheme is based on the large integer factorization problem, which makes them much more efficient than the CL-PKC based on bilinear pairings [16], [18]. This great property makes it very suitable in large-scale service-oriented VANETs, in which the vehicles perform a large number of encryption/decryption operations to secure their communication channels. In the next section, we will introduce the concrete Lite-CA-based encryption schemes in detail.

IV. Lite-CA-Based Encryption Schemes by Using Quadratic Residues

In this section, we first propose the definitions and the security model for the Lite-CA-based encryption schemes, and then, we design a basic Lite-CA-based encryption scheme by using quadratic residues. To proceed, we present proofs on consistency and security. Finally, our basic scheme can easily be extended to further improve the decryption efficiency.

A. Definitions and Framework of Lite-CA-Based Encryption

Definition 1: A Lite-CA-based encryption is a six-array tuple $\Pi = (\mathcal{G}_{\mathcal{LCA}}, \mathcal{G}_{\mathcal{U}}, \mathcal{E}_{\mathcal{P}}, \mathcal{S}_{\mathcal{P}}, \mathcal{E}, \mathcal{D})$ defined as follows.

1) $\texttt{Lite}-\texttt{CA}-\texttt{Setup}$ $\mathcal{G}_{\mathcal{LCA}}$ is a probabilistic polynomial time (ppt) algorithm by LCA that takes the system's security parameter k as input and outputs LCA's public/private keys pair (pk_{LCA}, sk_{LCA}).
2) $\texttt{User}-\texttt{Setup}$ $\mathcal{G}_{\mathcal{U}}$ is a ppt algorithm by the user that takes as input k and outputs the public/private key pair $(pk_U^{(1)}, sk_U)$.
3) $\texttt{Extract}-\texttt{Partial}-\texttt{Public}-\texttt{Key}$ $\mathcal{E}_{\mathcal{P}}$ is a ppt algorithm by LCA that takes k, sk_{LCA}, $pk_U^{(1)}$, and identity of user ID_U as input and outputs $pk_U^{(2)}$ as the partial public key.
4) $\texttt{Set}-\texttt{Public}-\texttt{Key}$ $\mathcal{S}_{\mathcal{P}}$ is a deterministic algorithm by the user that takes k, pk_{LCA}, ID_U, $pk_U^{(1)}$, and $pk_U^{(2)}$ as input and outputs $(pk_U^{(1)}, pk_U^{(2)})$ as the user's final public key if $pk_U^{(2)}$ is LCA's valid signature based on $pk_U^{(1)}$ and ID_U.
5) $\texttt{Encrypt}$ $\mathcal{E}$ is a ppt algorithm by anyone who wants to send ciphertext to the user, which takes a plaintext $M \in \mathcal{M}$, $pk_U^{(1)}$, $pk_U^{(2)}$, and pk_{LCA} as input and outputs a ciphertext $C \in \mathcal{C}$ or $\perp$ if $pk_U^{(1)}$ or $pk_U^{(2)}$ is invalid.

6) `Decrypt` $\mathcal{D}$ is a deterministic algorithm by the user that takes a ciphertext $C \in \mathcal{C}$ and its private key sk_U as input and outputs the corresponding plaintext $M \in \mathcal{M}$ or $\perp$, which means that C is not a valid ciphertext.

Since in the preceding scheme the partial public key $pk_U^{(2)}$ is essentially LCA's signature on the user's public key $pk_U^{(1)}$ and identity ID_U, no adversary except LCA can substitute the user's public key $pk_U^{(1)}$ of partial public key $pk_U^{(2)}$ without being detected. Therefore, we assume that the adversary can never amount the public key substitution attacks. Similar to the classic security notion for encryption [27], the design objective *ind-atk*—indistinguishability under three types of attacks (chosen plaintext attack (cpa), chosen ciphertext attack ($cca1$), and adaptive chosen ciphertext attack ($cca2$))—should be taken into consideration.

Definition 2: Let $\Pi = (\mathcal{G}_{\mathcal{LCA}}, \mathcal{G}_{\mathcal{U}}, \mathcal{E}_{\mathcal{P}}, \mathcal{S}_{\mathcal{P}}, \mathcal{E}, \mathcal{D})$ be a Lite-CA-based encryption scheme, and let $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ be a ppt adversary. For attacks $atk \in \{cpa, cca1, cca2\}$ and $1^k \in \mathbb{N}$, we say that the scheme Π is secure against atk if no such adversary $\mathcal{A}$ has a nonnegligible advantage in the following ind-atk game:

$$\begin{aligned}(pk_{LCA}, sk_{LCA}) &\leftarrow \mathcal{G}_{\mathcal{LCA}}(1^k)\\ \left(pk_U^{(1)}, sk_U\right) &\leftarrow \mathcal{G}_{\mathcal{U}}(1^k)\\ pk_U^{(2)} &\leftarrow \mathcal{E}_{\mathcal{P}}\left(1^k, sk_{LCA}, pk_U^{(1)}, ID_U\right)\\ (m_0, m_1) &\leftarrow \mathcal{A}_1^{\mathcal{O}_1}\left(pk_U^{(1)}, pk_U^{(2)}, sk_{LCA}, pk_{LCA}\right)\\ b &\leftarrow \{0,1\}\\ c^* &\leftarrow \mathcal{E}\left(m_b, pk_U^{(1)}, pk_U^{(2)}, pk_{LCA}\right)\\ b' &\leftarrow \mathcal{A}_2^{\mathcal{O}_2}(m_0, m_1, c^*)\end{aligned} \tag{1}$$

where

$$\begin{cases}\mathcal{O}_1 = \epsilon \text{ and } \mathcal{O}_2 = \epsilon, & \text{if } atk = cpa\\ \mathcal{O}_1 = \mathcal{D}_{sk_U}(\cdot) \text{ and } \mathcal{O}_2 = \epsilon, & \text{if } atk = cca1\\ \mathcal{O}_1 = \mathcal{D}_{sk_U}(\cdot) \text{ and } \mathcal{O}_2 = \mathcal{D}_{sk_U}(\cdot), & \text{if } atk = cca2.\end{cases} \tag{2}$$

We note that $\mathcal{A}_1$ outputs m_0 and m_1 with the same length. In addition, $\mathcal{A}_2$ is not permitted to make the query $\mathcal{O}_2(c^*)$. We refer to such an adversary $\mathcal{A}$ as an ind-atk adversary. We denote the adversary's advantage in attacking the scheme Π as the following function of the security parameter k:

$$Adv_{\mathcal{A},\Pi}^{ind-atk}(1^k) = \left|\Pr\left[b' = b\right] - \frac{1}{2}\right|. \tag{3}$$

Definition 3: We say that Π is *ind-atk secure* if for any ppt adversary $\mathcal{A}$ the function $Adv_{\mathcal{A},\Pi}^{ind-atk}(1^k)$ is negligible. The advantage function of this scheme is defined as

$$Adv_{\mathcal{A},\Pi}^{ind-atk}(1^k, t, q_d) = \max\left\{Adv_{\mathcal{A},\Pi}^{ind-atk}(1^k)\right\} \tag{4}$$

where the function max is taken over all adversaries that run for time t and make at most q_d queries to the decryption oracle.

B. Proposed Encryption Scheme

In this section, we present a concrete Lite-CA-based PKC for the aforementioned VANETs. The new encryption scheme, which is denoted by `BasicScheme`, consists of the following six algorithms.

1) $\texttt{Lite} - \texttt{CA} - \texttt{Setup}$: This algorithm takes the security parameter k as input and returns a secure Rivest-Shamir-Aldeman encryption scheme (RSA) [37] modulus $N = p \cdot q$ and parameters e and d, where p and q are two large secure primes, and d is the inverse of e modular $\varphi(N) = (p-1)(q-1)$. Usually, this algorithm is run by the third trusted party, which is referred as LCA in our scheme. The pair $\langle N, e\rangle$ and the tuple $\langle p, q, d\rangle$ should be looked as LCA's public key and private key, respectively. Suppose that $H : \{0,1\}^* \times \mathbb{Z}_N^* \rightarrow \mathbb{Z}_N^*$, $H_1 : \mathbb{Z}_N \rightarrow \mathbb{Z}_N$ and $H_2 : \mathbb{Z}_N^2 \rightarrow \mathbb{Z}_N$ are three cryptographic hash functions. Finally, the setup process is ended by publishing all the public parameters as $\{N, e, H, H_1, H_2\}$.
2) `Key registration`: When a user A wants to join the system, it must register to the LCA and obtain its public key. This algorithm consists of the following three subalgorithms:
   a) User Setup: This algorithm takes security parameter k and an identifier of the user A, i.e., $ID_A \in \{0,1\}^*$, as input and returns a parameter N_A such that $N_A = p_A \cdot q_A$, where p_A and q_A are two secure Blum primes. Usually, this algorithm is run by the user A with the identifier ID_A. The pair $\langle p_A, q_A\rangle$ refers to A's private key sk_A, whereas $pk_A^{(1)} = N_A$ and ID_A should be sent to LCA for registration.
   b) Extract Partial Public Key: After receiving $pk_A^{(1)}$ and ID_A from user A, LCA first validates the user's identity ID_A by checking its e-mail address, Internet Protocol address, or username; extracts A's partial public key $pk_A^{(2)} = P_A = H(ID_A, N_A)^d (\mathrm{mod}\ N)$; and sends it back to A via a public channel.
   c) Set Public Key: After receiving $pk_A^{(2)}$ from LCA, the user A validates it by checking whether $P_A^e \equiv H(ID_A, N_A)(\mathrm{mod}\ N)$ holds. If not, the user A broadcasts a "Complaint Message" against LCA; otherwise, A publishes the tuple $\langle ID_A, pk_A^{(1)}, pk_A^{(2)}\rangle$ as its public key.
3) `Encryption`: Supposing that the plaintext is m, any entity who wants to send ciphertext to user A does the following steps:
   a) Validate $pk_A^{(2)}$ by checking whether $P_A^e \equiv H(ID_A, N_A) \pmod N$ holds. If not, send to A the "Alert Message: Your public key has been juggled!" and abort.
   b) Pick a random number $r' \in \mathbb{Z}_{N_A}$ and compute $r = r'^2 - P_A^2 \pmod{N_A}$. Then, send the ciphertext $C = (c_1, c_2, c_3)$ to A via the public channel, where

$$c_1 = f_A(r), \quad c_2 = m \oplus H_1(r), \quad c_3 = H_2(m, r) \tag{5}$$

   and f_A is defined by

$$f_A(r) = \left(r + P_A^2\right)^2 - P_A^2 \pmod{N_A}. \tag{6}$$

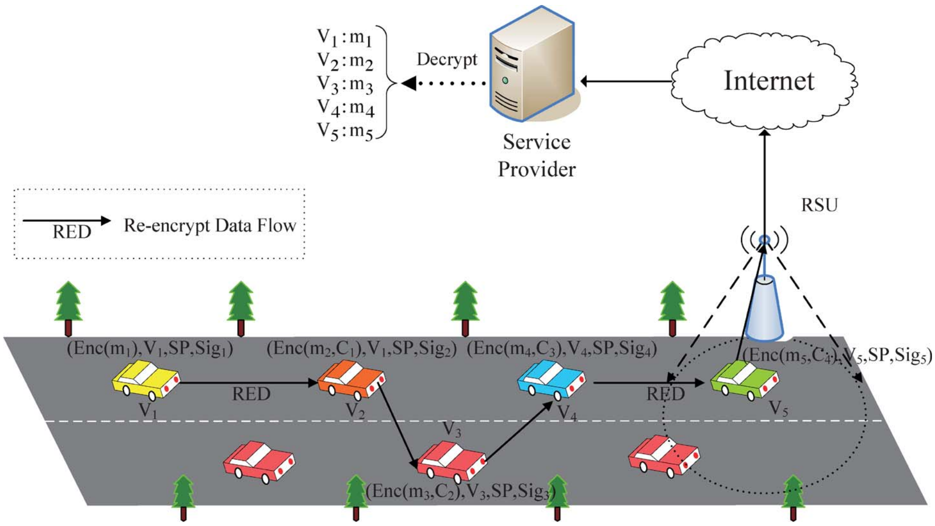


Fig. 2. Implementation in VANETs.

4) `Decryption`: Taking the ciphertext $C = (c_1, c_2, c_3)$ and the private key $\langle p_A, q_A \rangle$ as input, the user A can extract the corresponding plaintext m as follows:

a) Precomputation: Let $\lambda = (N_A - p_A - q_A + 5)/8 (\bmod\ \varphi(N_A))$. Employing the Chinese remainder theorem to the equation $x^2 \equiv 1 \ (\bmod\ N_A)$, we obtain four quadratic roots of 1, which are denoted by ± 1 and $\pm z$, respectively.

b) Let $u = c_1 + P_A^2 \ (\bmod\ N_A)$ and $v = u^\lambda \ (\bmod\ N_A)$. From four square roots

$$\begin{cases} r_1 = v - P_A^2, & \bmod N_A \\ r_2 = -v - P_A^2, & \bmod N_A \\ r_3 = zv - P_A^2, & \bmod N_A \\ r_4 = -zv - P_A^2, & \bmod N_A \end{cases} \tag{7}$$

we can derive four possible plaintexts

$$m_i = c_2 \oplus H_1(r_i), \quad i = 1, 2, 3, 4. \tag{8}$$

Then, check whether there exists some m_i such that $c_3 = H_2(m_i, r_i)$ holds. If so, then output m_i as the desired plaintext; otherwise, i.e., all possible plaintexts cannot pass these tests, output $\perp$ as a notification of an invalid ciphertext.

C. Correctness and Security

Theorem 1 (Correctness): The proposed encryption scheme in Section IV-B is correct.

Theorem 2 (IND-CCA2): The proposed encryption scheme in Section IV-B is secure against adaptive chosen ciphertext attacks in the random oracle models.

The detail proof of correctness and *IND-CCA2* security will be included in the Appendix.

D. Extended Schemes

In `BasicScheme`, the decryption algorithm is not very efficient since it has to derive four possible plaintexts and then check them one by one. With the purpose to enhance the efficiency in decryption, we describe two extended schemes as follows.

The first extension of `BasicScheme`, which is denoted by `ExtScheme1`, is to add two tag bits in ciphertext, i.e., $C = (c_1, c_2, c_3; d_1, d_2)$, where $c_1 = f_A(r)$, $c_2 = m \oplus H_1(r)$, and $c_3 = H_2(m, r)$, whereas

$$d_1 = r \ (\bmod\ 2) \quad \text{and} \quad d_2 = \begin{cases} 0, & (r + P_A^2, N_A) = 1 \\ 1, & \text{otherwise} \end{cases}$$

where $(r + P_A^2, N_A)$ is the Jacobi symbol of $r + P_A^2$ with respect to (w.r.t.) the modulus N_A. Thus, among four square roots r_i, there is only one root that satisfies the foregoing condition. Therefore, we need to derive only one ciphertext from the corresponding roots. Although this makes the parity of r exposed, this exposure does not abate the security of the encryption scheme.

The second extension of `BasicScheme`, which is denoted by `ExtScheme2`, is to remain ciphertext triple unchanged, i.e., $C = (c_1, c_2, c_3)$, where $c_1 = f_A(r)$, $c_2 = m \oplus H_1(r)$, and $c_3 = H_2(m, r)$, but to add constraints to choosing random salt r' such that $r (= r'^2 - P_A^2 \ (\bmod\ N))$ is even (or odd, respectively) and $(r + P_A^2, N_A) = 1$ holds.

Apparently, both of the foregoing two extended schemes achieve IND-CCA2 secure in the random oracle models. In the following sections, we denote the proposed encryption operation as Enc.

V. EP^{2}DF: A Scheme for Service-Oriented Vehicular Ad Hoc Networks

EP^{2}DF is based on the technique of *on-path onion encryption*, which allows the message to be reencrypted during their multihop transmission from the source to the destination. We show a typical on-path onion encryption process in Fig. 2, where every intermediate node will reencrypt the received messages to provide privacy enhancement for other vehicles. On-path onion encryption is divided into three phases: 1) key registration; 2) data forwarding; and 3) data decrypting.

A. Key Registration Phase

When an MU A wants to join in the system, it must register to LCA. First, A starts the *User Setup* algorithm to choose its identifier (such as its license plate number ID_A) and obtain a pair of private keys and public key $pk_A^{(1)} = N_A$. Second, it sends $\langle ID_A, N_A \rangle$ to LCA for registration. LCA takes the *Extract Partial Public Key* algorithm by comparing ID_A with its license plate number, extracting partial public key $pk_A^{(2)} = P_A$ and returning $pk_A^{(2)}$ to MU via a public channel if ID_A is a valid license plate number. After receiving partial public key $pk_A^{(2)}$ from LCA, A can validate it by taking the *Set Public Key* algorithm and publishes its public key.

B. Privacy-Preserving Data-Forwarding Phase

For simplicity, we consider such a data-forwarding process: the source vehicle V_1 wants to send a service request message m_1 to the service provider SP. The privacy-preserving data-forwarding scheme could be described as follows: First, V_1 encrypts the message m_1 by the public key of SP and generates the packet with the ciphertext, the identity V_1 and SP, and a signature for keeping integrity. The encrypted message could be denoted as

$$C_1 = \{Enc_{SP}(m_1), V_1, SP, Sig_{V_1}\left(Enc_{SP}(m_1)\|V_1\|SP\right)\}.$$

The encrypted message will be forwarded to other intermediate nodes with any existing vehicular routing protocols. For any intermediate node V_2 receiving the forwarding data, it first verifies the signature Sig_{V_1}, then an on-path onion encryption protocol is triggered, and V_2's own service requests are included as follows:

$$\begin{aligned} C_2 = \{&Enc_{SP}(m_2\|C_1), V_2, SP, \\ &Sig_{V_2}\left(Enc_{SP}(m_2\|C_1)\|V_2\|SP\right)\} \end{aligned}$$

where m_2 refers to the service request information sent by V_2 to SP. This process is performed at any intermediate node $\{V_i | 1 \leq i \leq k\}$, where k refers to the maximum number of transmission hops from V_1 to SP. Assuming that the ciphertext sent by the previous hop is C_{i-1}, the on-path onion routing protocol for node V_i is performed as

$$\begin{aligned} C_i = \{&Enc_{SP}(m_i\|C_{i-1}), V_i, SP \\ &Sig_{V_i}\left(Enc_{SP}(m_i, C_{i-1})\|V_i\|SP\right)\}. \end{aligned}$$

Note that, by using the proposed on-path onion encryption protocol, the transmitted message and routing information sent by C_{i-1} is hidden by the encryption of the next hop C_i. The external adversaries cannot trace the forwarding message to obtain the source of request information. The privacy-preserving data-forwarding protocol will go on until it arrives at the destination, and the ciphertext obtained by the destination is referred as follows:

$$\begin{aligned} C_k = \{&Enc_{SP}(m_k, \ldots, Enc_{SP}(m_1\|C_1), V_1 \\ &SP, Sig_{V_1} \ldots), V_k, SP, Sig_{V_k}\}. \end{aligned}$$

C. Data-Decryption Phase

In the data-decryption phase, the destination service provider SP first checks the identity of V_n and then decrypts the ciphertext using its secret key. After successfully decrypting, it can obtain the decrypted message m_n provided by V_n as well as the ciphertext sent by V_{n-1}. In the next step, SP will decrypt the ciphertext again and obtain the message m_{n-1}. This process will also continue until all the encrypted messages, as well as the sender information, is decrypted. SP will then provide the vehicles with their requested services.

VI. Performance Evaluation

Comparing with the CL-PKC schemes in [16] and [18], our proposal has the following advantages:

1) Higher trust level: In our proposal, the entity A itself is totally in charge of private key generation. Therefore, just as traditional CA-based PKC, our scheme achieves trust level 3.
2) More robust: In our scheme, if the public key has been substituted by some adversaries, except authority, then it is detectable before the ciphertext has been sent. Thus, if an entity A receives a ciphertext, then it can extract the corresponding plaintext successfully. However, in CL-PKC schemes, without necessary authentication for public keys, adversaries can make trouble in A's decryption process, as aforementioned.
3) More efficient: The proposed scheme in Section IV-B is more efficient than the original CL-PKC scheme in [16] and the improved scheme in [18]. Table I shows the comparison of our proposal and the schemes in [16] and [18]. The computational costs of the following operations are measured in our comparison:

    M: the operation taking the form of $a \cdot b \pmod N$ for a, $b \in \mathbb{Z}_N^*$;

    S: the operation taking the form of $a^2 \pmod N$ for $a \in \mathbb{Z}_N^*$;

    E_1: the operation taking the form of $a^b \pmod N$ and (a/N) for $a, b \in \mathbb{Z}_N^*$;

    E_2: the operation taking the form of g^r for $g \in GF(q)$ and $r \in \mathbb{Z}_q^*$;

    P: the operation taking the form of aP for $a \in \mathbb{Z}_q^*$ and $P \in \mathbb{G}_1$;

    e: the operation taking the form of $e(P, Q)$ for P, $Q \in \mathbb{G}_1$, where $e : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$ is a bilinear pairing map;

    X_1: the operation taking the form of $a \pm b \pmod N$ or $a \oplus b$ for $a, b \in \mathbb{Z}_N^*$;

    X_2: the operation taking the form of $P + Q$ for P, $Q \in \mathbb{G}_1$.

On one hand, according to a recently announced report [28], at the 80-bit level of security comparing three quite different pairing implementations and comparing them with a standard 1024-bit RSA decryption on the same platform, i.e., a standard PC, the time consumption on the foregoing different operations is shown in Table II. Moreover, compared with elliptic operation P and pairing operation e, the time consumption of

TABLE I
EFFICIENCY COMPARISON

	CL-PKC in [16]	CL-PKC in [18]	Our Scheme
CA-Setup	$1P$	$1P$	$1M$
User-Setup	$1P$	--	$1M$
Ext-Partial-Public Key	$2e + 1P$	$2e + 1P$	$1E_1$
Set-Public-Key	$2P$	$1P$	$1E_1$
Encrypt	$3e + 1P + 1E_2 + 2X_2$	$1e + 2P + 1E_2 + 3X_2$	$1E_1 + 2S + 3X_1$
Decrypt	$1e + 2X_2$	$1e + 3X_2$	$1E_1 + 0.5M + 4.5X_1$
Total	$6e + 6P + 1E_2 + 4X_2$	$4e + 5P + 1E_2 + 6X_2$	$4E_1 + 2.5M + 2S + 7.5X_1$
Time consuming	32.57	23.97	7.68

TABLE II
TIME CONSUMPTION FOR DIFFERENT OPERATIONS

Operation	M	S	E_1	E_2	P	e	X_1	X_2
Timing (ms)	–	–	1.92	0.77	2.0	3.3	–	–

the addition operation X_2 is negligible. Similarly, compared with modular operation E_1, the time consumption of modular operations M, S, and X is also negligible. Combining the materials in Tables I and II together, we can see that the total workloads for the schemes AP03 [16], AP05 [18], and ours are about 33, 24, and 8 ms, respectively. This suggests that the workload of our scheme takes only one third and one fourth proportions w.r.t. the AP05 [18] and AP03 schemes [16], respectively.

On the other hand, according to a technique report from the ECRYPT project [30], 1) at present, without precomputation, the fastest known algorithms for scalar multiplication are the Montgomery Ladder version of Lopez and Dahab (known as the LD algorithm) for $GF(2^m)$, and the relevant amount of operations required by the $GF(2^m)$ algorithm is $6mM + 5mS + (I + 10M)$, where M stands for modular multiplication, S stands for modular squaring, and I stands for modular inversion. 2) As for modular multiplication M and modular squaring S, most of the current researches use either an optimal normal basis (ONB) [31] multiplier or a polynomial basis [32] (PB) multiplier. With the use of ONB, the squaring operation is only a bit rotate shift. Nevertheless, multiplication is about twice as complex as PB multiplication. While a squaring in PB is not as cheap as in ONB, the use of trinomial and pentanomial irreducible polynomials could drastically reduce the complexity. These kinds of polynomials are recommended by the National Institute of Standards and Technology [33] and the SEC [34] and lead to efficient bit parallel implementations. For example, modular squaring with a trinomial requires at most $\lfloor m + k - 1/2 \rfloor$ bit additions. With respect to large multipliers, the area of a dedicated bit parallel squarer is negligible. This operation could therefore be performed in one clock cycle, as does the addition. 3) As for modular inversion I, it is a compound operation. Using the extended Euclidean algorithm, inversion takes on average 35 times longer than multiplication in $GF(2^m)$. 4) Although currently the Elliptic Curve Cryptography (ECC) processor is small enough to fit radio-frequency ID tags, the power consumption of ECC operations is still a serious problem on passively-powered tags.

For the detailed protocol, we can evaluate the encryption cost with an increasing number of hops from 1 to 50. Fig. 3(a) shows that in our protocol the encryption cost is much less than all of the other two schemes, which leads to efficient encryption in every hop for each vehicular. Fig. 3(b) plots the total computational cost with increasing hops from 1 to 50. Our protocol is also the best for its high efficiency. Compared with identity-based cryptography [20], [29], our protocol is also efficient in computational cost. The encryption cost in [29] is almost $2P + e$, and its decryption cost is e. Fig. 3(c) shows the comparison of the encryption computational cost between the protocol using our scheme and the identity-based cryptography.

VII. SECURITY ANALYSIS

In this section, a detailed security analysis is given in terms of our predefined security objectives.

Confidentiality: In this paper, the user's sensitive information such as service information could be protected and not revealed to unauthorized third parties. Our encryption scheme prevents this information from exposing to anyone who does not have the corresponding private key. The successor vehicle cannot decrypt the ciphertext from the predecessor and cannot even find any effective information from the ciphertext since our encryption scheme has been proved to achieve the IND-CCA2 security.

Authentication: Our scheme provides a novel authentication technique to distinguish the legitimate vehicle from the unauthorized vehicle. In our scheme, the signature is an important part for the successor to authenticate its predecessor, which makes the information undeniable and could successfully thwart the man-in-the-middle attack.

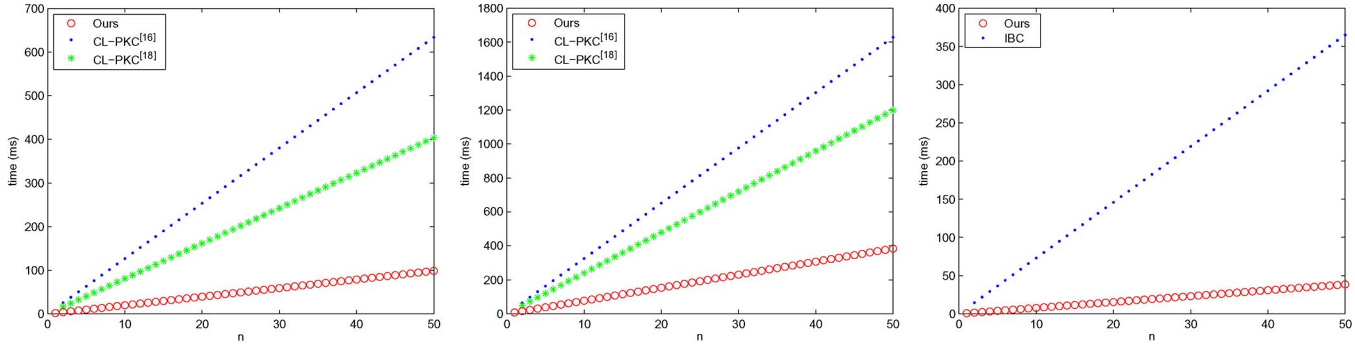
Privacy: Our scheme takes advantage of on-path onion encryption to achieve the unlinkability between the source and the destination and prevents adversaries from tracking the service delivery routes. Because the message sent by the source vehicle could be encrypted at each intermediate node, the adversary cannot find out the identity of the source node.

From the foregoing discussion, we could conclude that the proposed scheme can successfully achieve confidentiality, authentication, and service privacy, which are critical for secure service-oriented vehicular networks.

VIII. FURTHER DISCUSSIONS

In this section, we will further discuss more issues (see Table III) related to the benefits of our proposed Lite-CA-based PKC by comparing our proposal and the well-known PKCs from the following seven perspectives:

1) `who_gen_sk`: Who is in charge of private key generation?
2) `who_gen_pk`: Who is in charge of public key generation?



(a) (b) (c)

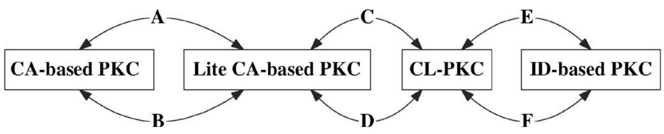
Fig. 3. Cryptographic cost comparison. (a) Encryption cost comparison. (b) Total computational cost comparison. (c) Encryption cost comparing with IBC [29].

TABLE III
COMPARISON OF VARIOUS PKCs

	CA based PKC	identity based PKC	Certificateless PKC	Our Scheme
who_gen_sk	user	authority	user and authority	user
who_gen_pk	user	user	user	user and authority
who_man_pk	authority	indifferent, such as users themselves		
where_pub_pk	directory	indifferent, such as bulletin board, etc.		
pk_man_mode	centralized	decentralized		
pk_auth_mode	explicit	implicit		explicit
ttp_tl	3	1	2	3

3) `who_man_pk`: Who is in charge of public key maintenance?
4) `where_pub_pk`: Where does public key publish to?
5) `pk_man_mode`: Which is the public key maintaining mode, centralized or decentralized?
6) `pk_auth_mode`: Which is the public key authentication mode, explicit or implicit?
7) `ttp_tl`: Which trust level can the trusted third party (TTP) achieve?

Apparently, we can see that the proposed scheme has elaborate differences from CA-based PKC, IBC, and CL-PKC. If CL-PKC can be looked as an intermediate solution between CA-based PKC and IBC, then our proposal can also be regarded as an intermediate solution between CA-based PKC and CL-PKC. Although our scheme still needs explicit public key authentication, just as that of in CA-based schemes, there is an obvious difference between them: In traditional CA-based PKC, the CA's signature on public keys, i.e., certificate, is not the public key itself, whereas in our scheme, the partial public key P_A is a part of the public key. For clarity, we illustrate the relationship of our proposal, which is denoted by Lite-CA-based PKC, and CA-based PKC, CL-PKC, and IBC in the following figure.



In the figure, the similar ties are denoted by A, C, and E, whereas the different ties are denoted by B, D, and F. In detail, their semantics are the following:

1) A: Both of them have certificate authority.
2) B: Lite-CA-based PKC has no centralized certificate management center.
3) C: Both of them have no explicit certificates.
4) D: Lite-CA-based PKC has explicit verification process, whereas CL-PKC has no such process. Thus, Lite-CA-based PKC is much more robust than CL-PKC, since the invalid public key can be detected at the beginning of the encryption process.
5) E: Both of them remove the certificate authority.
6) F: IBC has inherent private key escrow problem, whereas CL-PKC has no such problem.

More specifically, we would like to illustrate the flowcharts of CA-based PKC, Lite-CA-based PKC, and CL-PKC in Fig. 4. In this figure, *thin boxes* represent general process, whereas *thick boxes* represent communication between entities; *green* and *red boxes* represent public and private channels, respectively; *blue terms* can be published publicly, whereas *red terms* should be kept secret. We can see that the proposed Lite-CA-based PKC indeed possesses the following new features.

1) Lite-CA-based PKC versus CA-based PKC: In CA-based schemes, CA has to maintain the certificate directory, which is a heavy burden for implementing CA-based PKI, whereas in Lite-CA-based schemes, the users maintain the partial public keys by themselves. Meanwhile, any party can check the validity of the partial public keys since CA's public key is available for any entity in the domain.
2) Lite-CA-based PKC versus CL-PKC: In CL-PKC, the authority generates partial private keys for the users, and as a consequence, private channels for transferring these secrets are required. However, in Lite-CA-based PKC, CA generates partial public keys for the users and can send them via public channels. Moreover, Lite-CA-based PKC is much more robust than CL-PKC since the

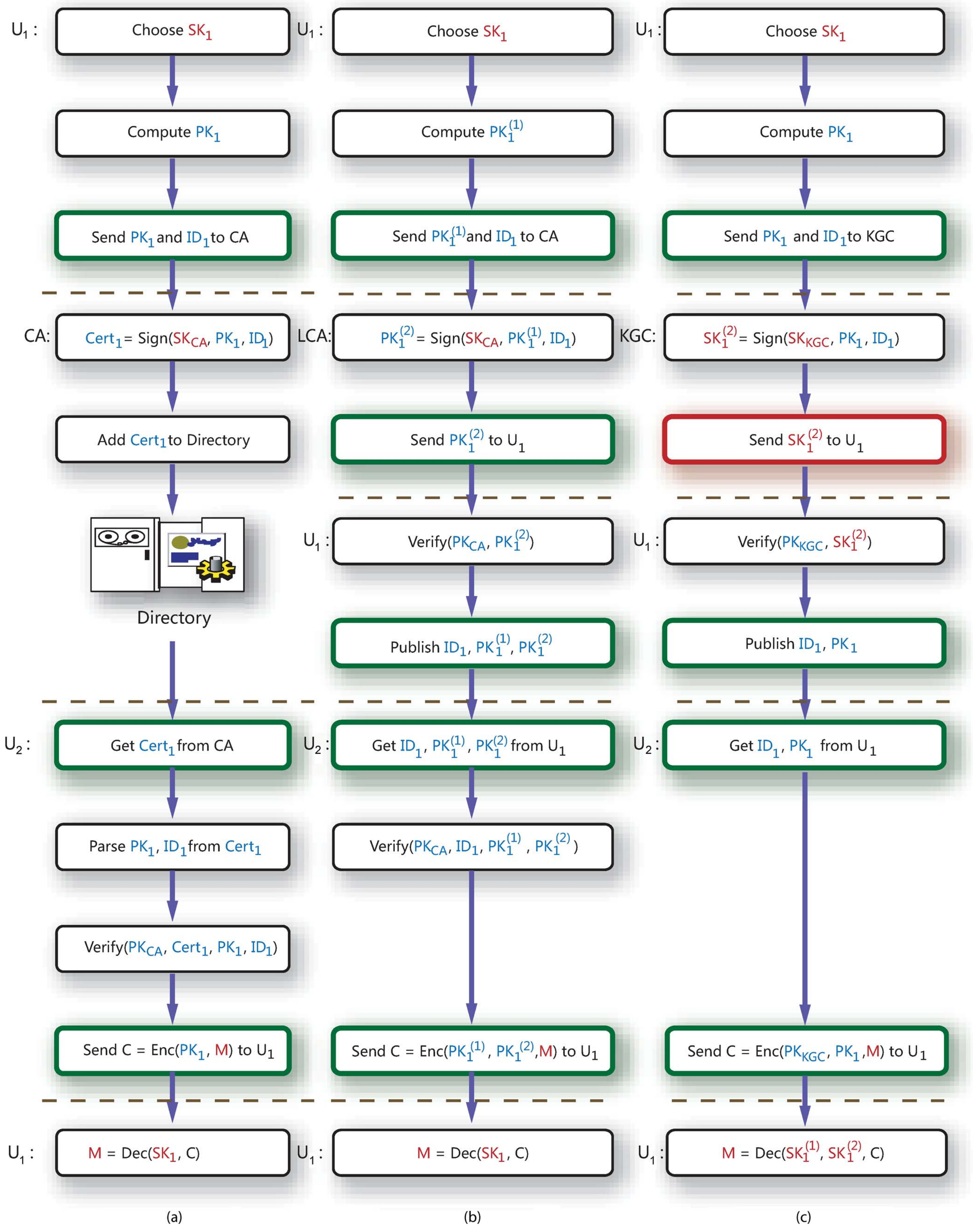

U_1 :
Choose SK_1
Compute PK_1
Send PK_1 and ID_1 to CA
CA:
$Cert_1 = Sign(SK_{CA}, PK_1, ID_1)$
Add $Cert_1$ to Directory
Directory
U_2 :
Get $Cert_1$ from CA
Parse PK_1, ID_1 from $Cert_1$
$Verify(PK_{CA}, Cert_1, PK_1, ID_1)$
Send $C = Enc(PK_1, M)$ to U_1
U_1 :
$M = Dec(SK_1, C)$
(a)
U_1 :
Choose SK_1
Compute $PK_1^{(1)}$
Send $PK_1^{(1)}$ and ID_1 to CA
LCA:
$PK_1^{(2)} = Sign(SK_{CA}, PK_1^{(1)}, ID_1)$
Send $PK_1^{(2)}$ to U_1
U_1 :
$Verify(PK_{CA}, PK_1^{(2)})$
Publish ID_1, $PK_1^{(1)}$, $PK_1^{(2)}$
U_2 :
Get ID_1, $PK_1^{(1)}$, $PK_1^{(2)}$ from U_1
$Verify(PK_{CA}, ID_1, PK_1^{(1)}, PK_1^{(2)})$
Send $C = Enc(PK_1^{(1)}, PK_1^{(2)}, M)$ to U_1
U_1 :
$M = Dec(SK_1, C)$
(b)
U_1 :
Choose SK_1
Compute PK_1
Send PK_1 and ID_1 to KGC
KGC:
$SK_1^{(2)} = Sign(SK_{KGC}, PK_1, ID_1)$
Send $SK_1^{(2)}$ to U_1
U_1 :
$Verify(PK_{KGC}, SK_1^{(2)})$
Publish ID_1, PK_1
U_2 :
Get ID_1, PK_1 from U_1
Send $C = Enc(PK_{KGC}, PK_1, M)$ to U_1
U_1 :
$M = Dec(SK_1^{(1)}, SK_1^{(2)}, C)$
(c)

Fig. 4. Relationship among CA-based PKC, Lite-CA-based PKC, and CL-PKC. (a) CA-based PKC. (b) Lite-CA-based PKC. (c) CL-PKC.

invalid public key can be detected at the beginning of the encryption process. This analysis justifies our motivation of insisting on explicit authentication for U_i's public key during encryption.

3) Lite-CA-based PKC versus IBC: On one hand, Lite-CA-based PKC achieves trust level 3, whereas IBC merely reaches trust level 1. On the other hand, IBC has the so-called inherent escrow drawback, whereas Lite-CA-based PKC has no such problem.

From the foregoing discussion, it is obvious that, compared with the conventional PKCs, Lite-CA-based PKC has the advantages of enhanced security, efficiency, and higher trust level, which makes it more suitable in service-oriented VANETs.

IX. Conclusion

How to ensure security and privacy in service-oriented VANETs still represents a challenging issue. In this paper, we answer this question with our proposed privacy-preserving data-forwarding scheme by introducing a novel and provable secure Lite-CA-based cryptosystem and the on-path onion encryption technique. Our cryptosystem brings new ideas and implementations compared with traditional CA based PKC and IBCs in VANETs. To enhance the efficiency and robustness of the existing certificateless encryption schemes, we designed efficient and distributed encryption schemes based on quadratic residues. Performance comparisons and security analysis show that the proposed schemes are very efficient and suitable for service-oriented VANETs.

Appendix A
Proof of Theorem 1

Proof: Since

$$\left(r+P_A^2\right)^2 \equiv f_A(r)+P_A^2 \equiv c_1+P_A^2 \equiv u \pmod{N_A} \tag{9}$$

$$v^2 \equiv u^{\frac{N_A-p_A-q_A+5}{4}} \equiv u^{\frac{\varphi(N_A)}{4}} \cdot u \equiv u \pmod{N_A} \tag{10}$$

the proposed scheme is consistent. ■

Appendix B
Proof of Theorem 2

Proof: The proof is very straightforward. In 1993, Bellare and Rogaway [35] proposed a general framework for the construction of the IND-CCA2 secure encryption. The framework can be described as

$$E(x) = f(r) \,\|G(r) \oplus x\|\, H(rx)$$

where f is an arbitrary one-way trapdoor permutation, whereas G and H are modeled as random oracles. In our `BasicScheme`, G and H are instantiated with the hash function H_1 and H_2, respectively. Thus, the left thing is to prove that f_A in `BasicScheme` is a one-way trapdoor permutation. This is concluded in the following lemma. ■

Lemma 1: Let N be the product of two large primes p and q with $p \equiv q \equiv 3 \pmod 4$. Then, for arbitrary $P \in \mathbb{Z}_N$, the restriction of the following function on its range is a one-way trapdoor permutation:

$$f : \mathbb{Z}_N \to \mathbb{Z}_N, \quad x \mapsto (x+P^2)^2 - P^2 \pmod N. \tag{11}$$

Proof: In the case of $P = 0$, we define a new function

$$\hat{f}(x) \triangleq f|_{P=0}(x) = x^2 \pmod N. \tag{12}$$

Clearly, $\hat{f}$'s range is

$$R_{\hat{f}} = \widehat{QR_N} \triangleq \left\{x^2 \ (\mathrm{mod}\ N) : x \in \mathbb{Z}_N\right\} \tag{13}$$

i.e., the extended quadratic residue set w.r.t. the modulus N. Note that the standard quadratic residue set w.r.t. N is defined as

$$QR_N \triangleq \left\{x^2 \ (\mathrm{mod}\ N) : x \in \mathbb{Z}_N, (x,N) = 1\right\} \tag{14}$$

which is a subset of $\widehat{QR_N}$.

From $N = p \cdot q$, we know that the congruent equation

$$x^2 \equiv y \pmod N \tag{15}$$

can be rephrased by the following two equations:

$$x^2 \equiv y \pmod p \tag{16}$$

$$x^2 \equiv y \pmod q. \tag{17}$$

Now, let us consider the following four subcases:

1) When $(y, N) = 1$, i.e., $p \nmid y$ and $q \nmid y$, (16) has exactly two roots, which are denoted by x_{11} and x_{12}. Moreover, we know that only one of them, for example, x_{11} without loss of generality, satisfies $(x_{11}, p) = 1$ since $p \equiv 3 \pmod 4$. Similarly, suppose that x_{21} and x_{22} are two roots of (17) and that $(x_{21}, q) = 1$ holds. For $i, j = 1, 2$, suppose that r_{ij} are the roots of

$$\begin{cases} x \equiv x_{1i} \pmod p \\ x \equiv x_{2j} \pmod q. \end{cases} \tag{18}$$

We know that r_{ij} $(i, j = 1, 2)$ are four roots $\mathrm{mod}\ N$ of (15). Among them, only one of them, more precisely r_{11}, lies in the set $\widehat{QR_N}$.

2) When $p|y$ and $q \nmid y$, then $x_{11} = x_{12} = 0$. Suppose that r_j is the root $\mathrm{mod}\ N$ of

$$\begin{cases} x \equiv 0 \pmod p \\ x \equiv x_{2j} \pmod q \end{cases} \tag{19}$$

for $j = 1, 2$. We know that r_j $(j = 1, 2)$ are two roots $\mathrm{mod}\ N$ of (15). Among them, only one of them, more precisely r_1, lies in the set $\widehat{QR_N}$.

3) Similarly, we can prove the uniqueness of the root of (15) that lies in $\widehat{QR_N}$ in the case of $p \nmid y$ and $q|y$.

4) When $p|y$ and $q|y$, (15) has a unique root 0, which, of course, lies in $\widehat{QR_N}$.

The preceding reductions suggest that $\hat{f}|_{R_{\hat{f}}}$ is a permutation.

In the case of $0 < P < N - 1$, we introduce a shift mapping

$$\tau : \widehat{QR_N} \to R_f, \quad x \mapsto x - P^2 \pmod N. \tag{20}$$

Apparently, τ is a 1–1 correspondence between $\widehat{QR_N}$ and f's range that is specified by

$$R_f \overset{\Delta}{=} f(\mathbb{Z}_N) = \{y \in \mathbb{Z}_N : \exists x \in \mathbb{Z}_N \ s.t. \ y \equiv f(x) \pmod N\}. \tag{21}$$

Then, we have

$$\begin{aligned} f|_{R_f}(x) &= (x + P^2)^2 - P^2 \pmod N \\ &= y^2 - P^2 = y^2 - P^2 \hat{f}(y) - P^2 \pmod N \\ &= \tau\left(\hat{f}(y)\right) = \tau\left(\hat{f}\left(\tau^{-1}(x)\right)\right). \end{aligned} \tag{22}$$

In other words, we obtain the following commutative diagram:

$$\begin{tikzcd} R_f \arrow[r, "f|_{R_f}"] \arrow[d, "\tau^{-1}"'] & R_f \\ \widehat{QR_N} \arrow[r, "\hat{f}"] & \widehat{QR_N}. \arrow[u, "\tau"'] \end{tikzcd} \tag{23}$$

Since $\hat{f}$, τ, and τ^{-1} are bijections, we can immediately conclude that f is also a bijection. Note that R_f is finite; therefore, $f|_{R_f}$ is a permutation.

Moreover, one can convert $f(x)$ if and only if he knows the factorization of the modulus N whenever $P = 0$ or $0 < P < N - 1$. This suggests that $f|_{R_f}$ is a one-way trapdoor permutation. ■

Remark 1: In the encrypting process `BasicScheme`, the purpose of picking random $r' \in \mathbb{Z}_{N_A}$ and then calculating $r = r'^2 - P_A^2 \pmod{N_A}$ is to choose a proper random salt r such that r lies in $R_{f_A} = \widehat{QR_{N_A}} - P_A^2$, i.e., the domain of One-Way Trapdoor Permutation (OWTP) $f_A|_{R_{f_A}}$.

Remark 2: Based on the newly developed OWTP $f_A|_{R_{f_A}}$, one can also construct an efficient IND-CCA2 secure encryption scheme by employing the so-called optimal asymmetric encryption padding technology proposed in [36], provided that one can find an efficient way to map arbitrary binary strings that take the forms of

$$m0^{k_1} \oplus G(r) \| r \oplus H\left(m0^{k_1} \oplus G(r)\right)$$

into R_{f_A}, where k_1 is the length of the padding, m is the plaintext required to be encrypted, and r is the random salt, whereas both G and H are modeled as random oracle models.

References

[1] M. Raya and J. Hubaux, "The security of vehicular ad hoc networks," in *Proc. 3rd ACM Workshop Security Ad Hoc Sensor Networks*, Alexandria, VA, 2005, pp. 11–21.

[2] R. Lu, X. Lin, H. Zhu, P. Ho, and X. Shen, "ECPP: Efficient conditional privacy preservation protocol for secure vehicular communications," in *Proc. IEEE INFOCOM*, Phoenix, AZ, 2008, pp. 1229–1237.

[3] X. Yang, J. Liu, F. Zhao, and N. Vaidya, "A vehicle-to-vehicle communication protocol for cooperative collision warning," in *Proc. 1st Annu. Int. Conf. MobiQuitous*, Boston, MA, 2004, pp. 114–123.

[4] X. Lin, X. Sun, P. Ho, and X. Shen, "GSIS: A secure and privacy-preserving protocol for vehicular communications," *IEEE Trans. Veh. Technol.*, vol. 56, no. 6, pp. 3442–3456, Nov. 2007.

[5] H. Zhu, R. Lu, X. Shen, and X. Lin, "Security in service-oriented vehicular networks," *IEEE Wireless Commun.*, vol. 16, no. 4, pp. 16–22, Aug. 2009.

[6] F. Li and Y. Wang, "Routing in vehicular ad hoc networks: A survey," *IEEE Veh. Technol. Mag.*, vol. 2, no. 2, pp. 12–22, Jun. 2007.

[7] J. Nzouonta, N. Rajgure, G. Wang, and C. Borcea, "VANET routing on city roads using real-time vehicular traffic information," *IEEE Trans. Veh. Technol.*, vol. 58, no. 7, pp. 3609–3626, Sep. 2009.

[8] H. Zhu, X. Lin, R. Lu, P. Ho, and X. Shen, "SLAB: A secure localized authentication and billing scheme for wireless mesh networks," *IEEE Trans. Wireless Commun.*, vol. 7, no. 10, pp. 3858–3868, Oct. 2008.

[9] H. Zhu, X. Lin, M. Shi, P. Ho, and X. Shen, "PPAB: A privacy-preserving authentication and billing architecture for metropolitan area sharing networks," *IEEE Trans. Veh. Technol.*, vol. 58, no. 5, pp. 2529–2543, Jun. 2009.

[10] H. Zhu, X. Lin, R. Lu, Y. Fan, and X. Shen, "SMART: A secure multilayer credit-based incentive scheme for delay-tolerant networks," *IEEE Trans. Veh. Technol.*, vol. 58, no. 8, pp. 4628–4639, Oct. 2009.

[11] J. Freudiger, M. Manshaei, J. Hubaux, and D. Parkes, "On noncooperative location privacy: A game-theoretic analysis," in *Proc. 16th ACM Conf. CCS*, Chicago, IL, 2009, pp. 324–337.

[12] D. Goldschlag, M. Reed, and P. Syverson, "Onion routing," *Commun. ACM*, vol. 42, no. 2, pp. 39–41, Feb. 1999.

[13] D. Catalano, D. Fiore, and R. Gennaro, "Certificateless onion routing," in *Proc. 16th ACM Conf. CCS*, Chicago, IL, 2009, pp. 151–160.

[14] C. Gentry, "Certificate-based encryption and the certificate revocation problem," in *Proc. Int. Conf. Theory Appl. Cryptographic Techn.*, Warsaw, Poland, 2003, pp. 272–293.

[15] P. Papadimitratos, G. Mezzour, and J. Hubaux, "Certificate revocation list distribution in vehicular communication systems," in *Proc. 5th ACM Int. Workshop VANET*, San Francisco, CA, 2008, pp. 86–87.

[16] S. Al-Riyami and K. Paterson, "Certificateless public key cryptography," in *Proc. 9th Int. Conf. Theory Appl. Cryptology Inf. Security*, Taiwan, 2003, pp. 452–473.

[17] D. Yum and P. Lee, "Generic construction of certificateless encryption," in *Proc. ICCSA*, Assisi, Italy, 2004, pp. 802–811.

[18] S. Al-Riyami and K. Paterson, "CBE from CL-PKE: A generic construction and efficient schemes," in *Proc. 8th Int. Workshop Theory Practice PKC*, Les Diablerets, Switzerland, 2005, pp. 398–415.

[19] M. Raya and J. Hubaux, "Securing vehicular ad hoc networks," *J. Comput. Security*, vol. 15, no. 1, pp. 39–68, 2007.

[20] A. Shamir, "Identity-based cryptosystems and signature schemes," in *Proc. 4th Int. Cryptology Conf.*, Santa Barbara, CA, 1984, pp. 47–53.

[21] B. Libert and J. Quisquater, "On constructing certificateless cryptosystems from identity based encryption," in *Proc. 9th Int. Workshop Theory Practice PKC*, New York, 2006, pp. 474–490.

[22] M. Au, Y. Mu, J. Chen, D. Wong, J. Liu, and G. Yang, "Malicious KGC attacks in certificateless cryptography," in *Proc. 2nd ASIACCS*, Singapore, 2007, pp. 302–311.

[23] B. Hu, D. Wong, Z. Zhang, and X. Deng, "Certificateless signature: A new security model and an improved generic construction," *Des., Codes Cryptography*, vol. 42, no. 2, pp. 109–126, Feb. 2007.

[24] L. Wang, Z. Cao, X. Li, and H. Qian, "Simulatability and security of certificateless threshold signatures," *Inf. Sci.*, vol. 177, no. 6, pp. 1382–1394, Mar. 2007.

[25] M. Barbosa and P. Farshim, "Certificateless signcryption," in *Proc. 4th ASIACCS*, Tokyo, Japan, 2008, pp. 369–372.

[26] M. Girault, "Self-certified public keys," in *Proc. Int. Conf. Theory Appl. Cryptographic Techn.*, Brighton, U.K., 1991, pp. 490–497.

[27] S. Goldwasser and S. Micali, "Probabilistic encryption," *J. Comput. Syst. Sci.*, vol. 28, no. 2, pp. 270–299, Apr. 1984.

[28] M. Scott, "Implementing cryptographic pairings," in *Proc. 1st Int. Conf. Pairing-Based Cryptography (Pairing)*, Tokyo, Japan, 2007.

[29] D. Boneh and M. Franklin, "Identity-based encryption from the Weil pairing," *SIAM J. Comput.*, vol. 32, no. 3, pp. 586–615, 2003.

[30] "State of the art in hardware implementations of cryptographic algorithms," ECRYPT Techn. Rep., Mar. 2006.

[31] S. Gao and H. Lenstra, "Optimal normal bases," *Des., Codes Cryptography*, vol. 2, no. 4, pp. 315–323, Dec. 1992.

[32] H. Wu, "Bit-parallel polynomial basis multiplier for new classes of finite fields," *IEEE Trans. Comput.*, vol. 57, no. 8, pp. 1023–1031, Aug. 2008.

[33] NIST, *Recommended Elliptic Curves for Federal Government Use*, Jul. 1999. [Online]. Available: csrc.nist.gov/encryption

[34] D. R. L. Brown, SEC 2: Recommended Elliptic Curve Domain Parameters, Sep. 2005. [Online]. Available: www.secg.org/download/aid-776/sec2.pdf

[35] M. Bellare and P. Rogaway, "Random oracles are practical: A paradigm for designing efficient protocols," in *Proc. 1st ACM Conf. CCS*, Fairfax, VA, 1993, pp. 62–73.

[36] V. Shoup, "OAEP reconsidered," *J. Cryptology*, vol. 15, no. 4, pp. 223–249, 2008.

[37] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Commun. ACM*, vol. 21, no. 2, pp. 120–126, 1978.

Xiaolei Dong received the Ph.D. degree in mathematics from Harbin Institute of Technology, Harbin, China, in 2001.

From September 2001 to July 2003, she was a Postdoctoral Researcher with Shanghai Jiao Tong University (SJTU), Shanghai, China. Then, she was with the Department of Computer Science and Engineering, SJTU. She is currently a Professor with SJTU. She has published more than 40 academic papers. Her primary research interests include number theory, cryptography, trusted computing, etc. She is an Associate Editor of *Security and Communication Networks* (Wiley).

Dr. Dong's project entitled "Number Theory and Modern Cryptographic Algorithms" won the first prize of the Science and Technology Progress Award in Universities of China in 2002. Her project entitled "New Theory of Cryptography and Other Fundamental Problems" won the second prize at the Shanghai Natural Science Awards in 2007. Her project entitled "Formalized Security Theories on Complex Crytposystems and Their Applications" won the second prize at the Natural Science Awards of the Ministry of Education in 2008. She won the first prize of the "Outstanding Teachers on the School Award" first prize from Shanghai Jiao Tong University in 2009.

Lifei Wei received the B.Sc. and M.Sc. degrees in applied mathematics from the University of Science and Technology Beijing, Beijing, China, in 2005 and 2007, respectively. He is currently working toward the Ph.D. degree in computer science with the Trusted Digital Technology (TDT) Laboratory, Department of Computer Science and Engineering, Shanghai Jiao Tong University, Shanghai, China.

His research interests include applied cryptography, cloud computing, and wireless network security.

Haojin Zhu (M'09) received the B.Sc. degree in computer science from Wuhan University, Wuhan, China, in 2002, the M.Sc. degree in computer science from Shanghai Jiao Tong University, Shanghai, China, in 2005, and the Ph.D. degree in electrical and computer engineering from the University of Waterloo, Waterloo, ON, Canada, in 2009.

He is currently an Assistant Professor with the Department of Computer Science and Engineering, Shanghai Jiao Tong University. His research interests include wireless network security, wireless communication, and mobile computing.

Dr. Zhu was the recipient of the Best Paper Award at the 2007 IEEE International Communications Conference Computer and Communications Security Symposium and the Third International Conference on Communications and Networking in China Wireless Communication Symposium.

Zhenfu Cao (SM'10) received the B.Sc. degree in computer science and technology and the Ph.D. degree in mathematics from Harbin Institute of Technology, Harbin, China, in 1983 and 1999, respectively.

He was exceptionally promoted to Associate Professor in 1987 and became a Professor in 1991. He is currently a Distinguished Professor and the Director of the Trusted Digital Technology Laboratory, Shanghai Jiao Tong University, Shanghai, China. He also serves as a member of the expert panel of the National Nature Science Fund of China.

Prof. Cao is actively involved in the academic community, serving as Committee/Session Chair and program committee member for several international conference committees, as follows: the IEEE Global Communications Conference (since 2008), the IEEE International Conference on Communications (since 2008), the International Conference on Communications and Networking in China (since 2007), etc. He is the Associate Editor of *Computers and Security* (Elsevier), an Editorial Board member of *Fundamenta Informaticae (IOS)* and *Peer-to-Peer Networking and Applications (Springer-Verlag)*, and Guest Editor of the Special Issue on *Wireless Network Security, Wireless Communications and Mobile Computing* (Wiley), etc. He has received a number of awards, including the Youth Research Fund Award of the Chinese Academy of Science in 1986, the Ying-Tung Fok Young Teacher Award in 1989, the National Outstanding Youth Fund of China in 2002, the Special Allowance by the State Council in 2005, and a corecipient of the 2007 IEEE International Conference on Communications—Computer and Communications Security Symposium Best Paper Award in 2007. He also received seven awards granted by the National Ministry and governments of provinces such as the first prize of the Natural Science Award from the Ministry of Education.

Licheng Wang received the B.S. degree in computer science from Northwest Normal University, Lanzhou, China, in 1995, the M.S. degree in mathematics from Nanjing University, Nanjing, China, in 2001, and the Ph.D. degree in computer science from Shanghai Jiao Tong University, Shanghai, China, in 2007.

He is currently an Assistant Professor with the Beijing University of Posts and Telecommunications, Beijing, and an Expert Researcher with the Information Security Research Center, National Institute of Information and Communications Technology. His current research interests include cryptography, information security, and trust computation.