An Efficient Conditional Privacy-Preserving Authentication Scheme for Vehicular Sensor Networks Without Pairings

Nai-Wei Lo and Jia-Lun Tsai

***Abstract*—Constructing intelligent and efficient transportation systems for modern metropolitan areas has become a very important quest for nations possessing metropolitan cities with ever-increasing populations. A new trend is the development of smart vehicles with multiple sensors able to dynamically form a temporary vehicular ad hoc network (VANET) or a vehicular sensor network (VSN). Along with a wireless-enabled roadside unit (RSU) network, drivers in a VSN can efficiently exchange important or urgent traffic information and make driving decisions accordingly. In order to support secure communication and driver privacy for vehicles in a VSN, we develop a new identity-based (ID-based) signature based on the elliptic curve cryptosystem (ECC) and then adopt it to propose a novel conditional privacy-preserving authentication scheme based on our invented ID-based signature. This scheme provides secure authentication process for messages transmitted between vehicles and RSUs. A batch message verification mechanism is also supported by the proposed scheme to increase the message processing throughput of RSUs. To further enhance scheme efficiency, both pairing operation and MapToPoint operation are not applied in the proposed authentication scheme. In comparison with existing pseudo-ID-based authentication solutions for VSN, this paper shows that the proposed scheme has better performance in terms of time consumption.**

***Index Terms*—Conditional privacy-preserving authentication, ID-based signature, intelligent transportation system, vehicular sensor network (VSN), elliptic curve cryptosystem (ECC).**

I. Introduction

ONE of the emerging trends of the 21st century is the constant movement of people towards more metropolitan areas, where a better living environment with medical support, social security benefits and sufficient job market can be found. In anticipation of this, governments in various nations have already started, or completed, planning for their metropolitan areas to accommodate a larger population and increase economic strength on these areas. As a consequence, it has become a very important and urgent topic for metropolitan cities to manage their city traffic systems efficiently and effectively. To manage traffic caused by tens of thousands of vehicles in a metropolitan area, the introduction of intelligent transportation systems (ITS) is one of the most promising directions. Based on the developed concept of a mobile *ad hoc* network (MANET), vehicular *ad hoc* network (VANET) [1] has been introduced by researchers and vehicle manufacturers in order to construct next generation transportation systems. In a VANET environment, there are different kinds of vehicles embedded with an individual on-board unit (OBU) in which a wireless communication module is installed and supports message transmission and reception through Wi-Fi or WiMax etc. This allows vehicles to communicate with each other via mobile wireless network. For distributing emergent event messages efficiently and reliably, and supporting other useful functions, such as instant weather forecasts for drivers, roadside units (RSUs) are usually introduced in VANET-based intelligent transportation systems [2]. With wireless-enabled RSUs situated along major roadways, enabling dynamic wireless communication between vehicles and RSUs, drivers can also have access to Internet-based services. However, it is possible that a malicious vehicle (driver) might generate and spread false event messages intentionally or a vehicle with malfunctioning sensors might distribute event messages with incorrect sensor readings within a vehicular sensor network (VSN) [3]. In addition, physical and cyber securities for RSUs also need to be addressed when implementing an intelligent transportation system upon a VSN [4], [5]. Among various security threats in VSN environments, the most notable is how to securely identify legal service access rights and communication privileges of a communicating vehicle without revealing the unique identity of this vehicle. Protecting the corresponding privacy of vehicle driver (or owner) has become the basic security requirement for modern ITS. Since RSUs are usually constructed and maintained by government agencies, vehicle drivers might intend to get services and spread messages through RSUs provided that they can establish wireless connection with one of RSUs when driving on an RSU enabled road. Therefore, from an ITS design point of view, having a secure authentication scheme for vehicles to communicate with RSUs is essential for an ITS to be successfully operated in VSN environments. A well-designed authentication scheme for communication between vehicle and RSU should satisfy the following requirements: well-established security strength, privacy protection for vehicle driver (or owner), efficient authentication session processing, and scalability on authentication requests.

Manuscript received October 31, 2014; revised October 5, 2015; accepted November 15, 2015. This work was supported by the Ministry of Science and Technology, Taiwan, under Grants MOST 103-2221-E-011-091-MY2, MOST 104-2923-E-011-005-MY3, and MOST 104-2218-E-001-002. The Associate Editor for this paper was F.-Y. Wang.

The authors are with the Department of Information Management, National Taiwan University of Science and Technology, Taipei 106, Taiwan (e-mail: nwlo@cs.ntust.edu.tw; naiweilo@yahoo.com.tw; crousekimo@yahoo.com.tw).

Digital Object Identifier 10.1109/TITS.2015.2502322

A. Our Contributions

For services and applications built for VSN environments, fast user authentication with user privacy preservation is one of the key factors for vehicular drivers and passengers willing to use these services and applications. In order to develop faster authentication scheme suitable to VSN environments, we first proposes a new ID-based batch signature scheme without using bilinear pairings. The proposed signature scheme only utilizes a general one-way hash function rather than a special one-way hash function (MapToPoint), which consumes more computing time than a general one-way hash function. Since our signature scheme does not use any pairing operations during signature generation, signature verification process, and batch signature verification process, our signature scheme has better performance than other existing ID-based batch signature schemes. Security analysis is conducted to show that our ID-based signature scheme is secure against adaptive chosen message attack under random oracle. Then, we further applied the proposed ID-based signature scheme to develop a new conditional privacy-preserving authentication scheme without using bilinear pairings for communication between vehicle and RSU in VSN environments. The proposed authentication scheme supports anonymous authentication, message integrity, traceability for trusted third party, batch signature verification and driver unlinkability. In comparison with existing authentication schemes for VSN, the proposed authentication scheme has better performance in terms of total time consumption. In addition, security analysis for the proposed authentication scheme is conducted to evaluate security strength of our authentication scheme.

II. Related Work

In a general VANET environment, there are two kinds of communication patterns: vehicle-to-vehicle communication and vehicle-to-infrastructure communication. Vehicle-to-vehicle (V-to-V) communication supports multi-hop message transmission among vehicles, in which the communication pattern is directly derived from MANET. For vehicle-to-infrastructure (V-to-I) communication, the assumption is that roadside units with wireless communication capability will be built along major roadways and be connected together with wired fiber optic cables to form a network infrastructure. Under such an infrastructure, vehicles can communicate with RSUs to get extra services and information, or even indirectly exchange messages with each other through the RSU network. In VANET environments, message integrity and sender accountability are very important features for services built upon dynamic V-to-V *ad hoc* networks and for wireless V-to-I communication. Currently most available or targeting services in VANET are related with near real-time message generation, distribution, and inquiry, such as road safety alarms, real-time local weather forecasts and instant traffic predictions. Since valuable information used in these services is usually generated or obtained from distributed sensors around roadways and moving vehicles on the road, identification and authentication of message (information) sender, which could be a vehicle, a sensor, or a back-end server, has become a necessary security and accountability requirement.

As messages are transmitted through wireless communication channels in VSN environments, it is necessary to preserve message integrity for all VSN-based services. The IEEE Trial-Use Standard for Wireless Access in Vehicular Environments (WAVE) [6] adopted the elliptic curve digital signature algorithm (ECDSA) to maintain message integrity during a VANET authentication process. In other words, each message sent from a vehicle contains its vehicle identification, the message content and the message signature. Since ECDSA is an elliptic curve-based cryptosystem, it is more computationally efficient than the commonly used digital signature algorithm (DSA) [7]. However, IEEE Trial-Use Standard does not support identification anonymity for vehicles. Vehicle drivers may be concerned about the leakage of personal privacy related information (such as vehicle identification) when ITS services request user (or message sender) identification and authentication. To maintain accountability of the message sender and the privacy of the vehicle driver in general situations, conditional privacy-preserving authentication will be required for services in VSN environments in the near future. In order to support strong privacy protection for vehicle drivers, user anonymity and user unlinkability [8]–[12] of vehicle identification should be provided by the corresponding ITS services. Nevertheless, high speed mobility of vehicles (up to 250 km/h) and naturally large connection region of a VANET impose serious challenges on privacy-preserving authentication for VSN environment in terms of efficiency requirements. For secure VSN authentication, one should also consider insider attacks; for example, what if a legal vehicle driver intends to make some disturbances to the VSN it is connected with. Therefore, a supplemental mechanism for privacy-preserving authentication should also be provided to reveal a driver's identifier when it is necessary. Usually this kind of supplemental mechanism will introduce a trusted third party with granted authority to perform the task.

In 2006, Gamage *et al.* [13] adopted an ID-based ring signature scheme with signer ambiguity feature as a way to achieve privacy protection for VANET-based services. However, the scheme proposed by Gamage *et al.* does not support conditional privacy. Later, two PKI-based authentication schemes were proposed by Raya and Hubaux [14] and Lu *et al.* [15]. In their schemes, each vehicle is preloaded with a large number of anonymous public/private key pairs and corresponding public key certificates. Each public/private key pair has a short lifetime and a pseudo-ID adopted within each public key certificate. As a result, a larger storage capacity is required for their schemes and consequently higher verification cost occurs when a public key certificate is used and needs to be verified. In addition, a certificate revocation list (CRL), which is generated by a trusted authority, is used for their revocation protocols. Since the size of CRL will grow with time, their revocation protocols will encounter problems with efficiency. Several group-signature-based authentication schemes [16]–[20] have been proposed since 2006. In these schemes, a group manager, who has the group master key, can reveal the real identity from a group signature signed by a signer. Among these works,

GSIS [17], a secure privacy-preserving authentication scheme, adapts group signatures for V-to-V communications and ID-based signatures for V-to-I communications. In brief, pseudo-ID-based authentication schemes based on PKI technology will generate a lengthy CRL with time, and group-signature-based authentication schemes require more computation during signature verification. In order to mitigate these factors, Zhang *et al.* [21] proposed an ID-based authentication scheme with batch verification based on bilinear pairings for secure V-to-I communications. In their scheme, a pseudo-ID-based one-time signature scheme is used to minimize the transmission and verification cost of public key certificates. In addition, their scheme allows multiple signatures from multiple vehicles to be verified at the same time. However, in the scheme of Zhang *et al.*, a long-term master secret s is preloaded into the tamper-proof device of each vehicle. If an adversary learns the master secret s from one tamper-proof device by launching side-channel attacks [22], such as power analysis and laser scanning, the adversary can masquerade as any vehicle to transmit any message chosen or generated by itself. In 2011, Biswas *et al.* [23], [24] integrated an ID-based proxy signature scheme with the standard ECDSA to generate a new authentication scheme. This authentication scheme is efficient, but it does not support batch verification. Tsai [25] found that this authentication scheme is vulnerable to private key reveal attacks. Tsai then proposed an enhanced scheme to overcome those weaknesses. In 2012, Shim [26] proposed a new ID-based signature scheme and then used it to develop a new efficient conditional privacy-preserving authentication scheme for V-to-I communication. In this scheme, the long-term master secret s is not preloaded into the tamper-proof device of each vehicle. Furthermore, this scheme does not require the special one-way hash function, called MapToPoint function, in both the signature generation and verification processes. This special MapToPoint function is inefficient and probabilistic [27]; while there is a lot of discussion regarding how to construct such a hash algorithm, there is no efficient deterministic polynomial time based algorithm proposed yet. Since the computation cost of one pairing operation is three or more times that of a one point multiplication operation [12], [28], Shim's scheme requires heavy computation cost in the signature verification phase, where three multiplication point operations and three pairing operations are used.

III. Our Proposed ID-Based Signature Scheme With Batch Verification and IT Security Proof

Here we propose an identity-based (ID-based) signature scheme [29]–[31] to simplify the certificate management problem by using signers' identity information as their public keys. The private keys of the signers are generated by a trusted third party, called a private key generator (PKG). In this way, the verifier does not need to store all the public keys and the corresponding certificates of the signers. This section examines our ID-based signature scheme with batch verification, and further proves that our scheme is secure under a random oracle.

A. Our Proposed Scheme

Our identity-based signature scheme consists of five algorithms: **setup**, **extract**, **sign**, **verification**, and **batch verification** algorithms. The proposed scheme has the following advantages: (1) Our scheme does not need to use any special one-way hash function, called MapToPoint; and (2) there is no need for pairing operations. By avoiding the use of pairing operations, our proposed scheme performs better than the other ID-based batch signature schemes. Details of each algorithm are described as follows.

Setup: Let n be a large prime and F_n be the finite field over n, where n is the size of finite field. Let $(a, b) \in F_n$ be the parameters of elliptic curve E ($y^2 = x^3 + ax + b \pmod n$), where $4a^3 + 27b^2 \neq 0$) over F_n. Let O denote infinity. Let P be the generator point of E and q be the prime order of P, where $P \neq O$. The private key generator (PKG) randomly chooses a number $s \in Z_q$ as its master private key and then computes its corresponding public key $P_{pub} = sP$. After that, PKG chooses two one-way hash functions: H_1: $\{0,1\}^* \rightarrow Z_q$ and H_2: $\{0,1\}^* \rightarrow Z_q$. Next, PKG publishes P, P_{pub}, q, H_1, H_2 as its public parameters and keeps s. Note that only one string parameter is required for hash functions. In this study, when there are several data items required to be concatenated first before submitting as the parameter of a hash function, the comma symbol is used to indicate a string concatenation operation.

Extract: When a user registers on PKG, this user first sends their chosen identity ID_i to PKG via a secure channel. Upon receiving ID_i from the user, PKG computes

$$K_i = k_i P \tag{1}$$

$$S_{IDi} = k_i + H_1(ID_i, K_i) \times s \bmod q \tag{2}$$

corresponding to this identity ID_i, where k_i is a random number. After that, PKG sends (K_i, S_{IDi}) back to the user via a secure channel.

Sign: Given a message M_i, a signer with an identity ID_i computes

$$R_i = r_i P \tag{3}$$

$$V_i = H_2(K_i, R_i, ID_i, M_i) \times r_i + S_{IDi} \bmod q \tag{4}$$

where r_i is a random number. (K_i, R_i, V_i) is the signature on message M_i for identity ID_i. Notice that R_i can be precomputed before the signer signs a message M_i.

Verification: Given a message M_i and its corresponding signature (K_i, R_i, V_i), a verifier can verify the validity of a signature (K_i, R_i, V_i) with the following equation

$$V_i P = H_2(K_i, R_i, ID_i, M_i) R_i + K_i + H_1(ID_i, K_i) P_{pub}. \tag{5}$$

If the above equation (5) holds, it means that the signature (K_i, R_i, V_i) is a valid signature; otherwise, the verifier would reject the signature (K_i, R_i, V_i).

Batch Verification: Given distinct n message-signature tuples $\{(K_1, R_1, V_1), (K_2, R_2, V_2), \ldots, (K_n, R_n, V_n)\}$ signed

by distinct n signers, the verifier can simultaneously verify the validity by checking the following equation

$$\left(\sum_{i=1}^{n} V_i\right) P = \left(\sum_{i=1}^{n} H_2(K_i, R_i, ID_i, M_i) R_i\right) + \sum_{i=1}^{n} K_i + \left(\sum_{i=1}^{n} H_1(ID_i, K_i)\right) P_{pub}. \quad (6)$$

If the above equation holds, it means that these distinct n signatures are valid. In 2014, Liu *et al.* [32] demonstrated a new attack on ID-based batch signature schemes proposed by Shim. In order overcome such attack, we can replace Eq. (6) with the following equation by adding the well-known small exponents test [32]–[35], where $a_i \in_R \{0,1\}^l$ are randomly chosen for $i = 1, \ldots, n$. Usually $l = 80$ [32] is enough for normal scenario in VANETs

$$\left(\sum_{i=1}^{n} a_i V_i\right) P = \left(\sum_{i=1}^{n} a_i H_2(K_i, R_i, ID_i, M_i) R_i\right) + \sum_{i=1}^{n} a_i K_i + \left(\sum_{i=1}^{n} a_i H_1(ID_i, K_i)\right) P_{pub}. \quad (7)$$

If equation (7) holds, it means that these distinct n signatures are valid.

B. Security Proof

Since the extract algorithm of our identity-based signature scheme is based on Schnorr's signature scheme [36], it is secure against adaptive chosen identity attacks. Thus, this subsection only shows that the proposed identity-based scheme is secure against an adaptive chosen message attack under a random oracle [37]–[40]. Before presenting the security analysis, we present the mathematical problem and forking lemma used in our security analysis, which are as follows:

Definition 1 Elliptic Curve Discrete Logarithm Problem (ECDLP): Given $x \in Z_q$ and $Y = xP \in G_1$, it is infeasible to learn a number x from $Y = xP$, where P is the generator of G_1.

Definition 2 Forking Lemma [38], [39]: Let A be a probabilistic polynomial time Turing machine whose input only consists of public data. We denote respectively by Q and R the number of queries that A can ask to the random oracle and the number of queries that A can ask to the signer. Assume that, within a time bound T, A produces, with probability $\varepsilon \geq 10(R+1)(R+Q)/2^k$, a valid signature $(m, \sigma_1, h, \sigma_2)$. If the triples (σ_1, h, σ_2) can be simulated without knowing the secret key, with an indistinguishable distribution probability, then there is another machine which has control over the machine obtained from A replacing interaction with the signer by simulation and produces two valid signatures $(m, \sigma_1, h, \sigma^2)$ and $(m, \sigma_1, h', \sigma_2')$ such that $h \neq h'$ in expected time $T' \geq 120686QT/\varepsilon$.

Let A be an adversary who performs an existential forgery under an adaptively chosen message attack against the proposed scheme within a time bound T and with a probability of ε. Details of our theorem 1 are given as follows.

Theorem 1: Let Q and R be the number of queries that an algorithm A can ask the random oracle and the number of queries that A can ask to sign the oracle, respectively. We propose that if A can break the proposed identity-based batch signature scheme, there is an algorithm B which can break ECDLP within a time period T which is expected to be less than $120686QT/\varepsilon$, if $\varepsilon \geq 10(R+1)(R+Q)/q$.

Proof: A ECDLP instance $(P, S_{IDi}P)$ is given for $S_{IDi} \in Z_q$. The algorithm B executes our identity-based signature scheme. Assume there exists an adversary A who has the capability to break the proposed identity-based signature scheme. We can claim that by serving the following queries from adversary A, the algorithm B can use the algorithm A to get the solution for ECDLP. i.e., the algorithm B breaks ECDLP by get S_{IDi} from $(P, S_{IDi}P)$. In the following, we show the process by which the algorithm B can break ECDLP by utilizing the adversary A. Notice that two hash lists, L_{H1} and L_{H2}, are maintained by the algorithm B.

Setup: This Setup algorithm takes a secure parameter k as input, and then selects a random number s its private key and computes its corresponding public key with $P_{pub} = sP$. Next, the public parameters $\{P, P_{pub}, q, H_1, H_2\}$ are sent to adversary A.

H_1 hash query: When A invokes an H_1 query with parameter (ID_i, K_i), B will then check whether the parameter (ID_i, K_i) exists in the hash list L_{H1}. If the parameter (ID_i, K_i) has already been stored in L_{H1} under the tuple (ID_i, K_i, h_1), B outputs the corresponding value h_1 in the tuple to A; otherwise, B picks a random h_1 and then inserts a new tuple (ID_i, K_i, h_1) into the hash list L_{H1}. Next, B returns the value $h_1 = H_1(ID_i, K_i)$ to A.

H_2 hash query: If A invokes an H_2 query with parameter (K_i, R_i, ID_i, M_i), then B will check whether parameter (K_i, R_i, ID_i, M_i) exists in the hash list L_{H2}. If the parameter (K_i, R_i, ID_i, M_i) has already stored in L_{H2} under the tuple $(K_i, R_i, ID_i, M_i, h_2)$, B outputs the corresponding value h_2 in the tuple to A; otherwise, B picks a random h_2 and then inserts a new tuple $(K_i, R_i, ID_i, M_i, h_2)$ into the hash list L_{H2}. Next, B returns the value $h_2 = H_2(K_i, R_i, ID_i, M_i)$ to A.

Extract query:If A makes an extract query on a user's identity ID_i, B computes $K_i = k_i P$ and then finds whether the tuple (ID_i, K_i) exists on the hash list L_{H1}, where k_i is a random number. If B cannot find the corresponding pair $(ID_i, K_i, h_1 = H_1(ID_i, K_i))$ based on (ID_i, K_i), B outputs a failure message to A and then rejects this query. Otherwise, B computes $S_{IDi} = k_i + s \times H_1(ID_i, K_i) \bmod q$ and then the value S_{IDi} is outputted to A. Notice that A cannot get S_{IDj} of the targeted victim (user) with ID_j by invoking this extract query.

Sign query: If A makes a sign query on a M_i under a user's identity ID_i, B first finds the tuple value (ID_i, K_i, h_1) from the hash list L_{H1} according to (ID_i, K_i). B then retrieves h_1 from the tuple (ID_i, K_i, h_1) and selects two random numbers r_i and h_2. Next, B selects two random numbers u_i and v_i, and tries again. Otherwise, B computes $R_i = h_2^{-1} u_i P - Y$

and $V_i = u_i$ and then returns the value (R_i, V_i) to A, where $H_2(K_i, R_i, ID_i, M_i) = h_2$.

Analysis: By using Forking Lemma [38], [39], once A can construct two valid signatures $(R_i, V_i = h_2 \times r_i + S_{IDi} \bmod q)$ and $(R_i, V_i' = h_2' \times r_i + S_{IDi} \bmod q)$, such that $h_2 \neq h_2'$, B can successfully derive the value S_{IDi} from these two valid signatures $(R_i, V_i = h_2 \times r_i + S_{IDi} \bmod q)$ and $(R_i, V_i' = h_2' \times r_i + S_{IDi} \bmod q)$ by computing

$$\begin{aligned} &\frac{h_2' V_i - h_2 V_i'}{h_2' - h_2} \bmod q \\ &= \frac{h_2' h_2 r_i + h_2' S_{ID_i} - h_2 h_2' r_i - h_2 S_{ID_i}}{h_2' - h_2} \bmod q \\ &= S_{IDi}. \end{aligned} \tag{8}$$

As a consequence, B can solve the ECDLP *within an expected time less than* $120686\, QT/\varepsilon$, *if* $\varepsilon \geq 10(R+1)(R+Q)/q$.

Since the proposed identity-based signature scheme also supports batch verification, we show in the following discussion that our batch verification is also secure against adaptive chosen attack.

By applying Forking Lemma, A can generate two groups of signatures $\{(ID_1, M_1, R_1, V_1), (ID_2, M_2, R_2, V_2), \ldots, (ID_m, M_m, R_m, V_m)\}$ and $\{(ID_1, M_1, R_1, V_1'), (ID_2, M_2, R_2, V_2'), \ldots, (ID_m, M_m, R_m, V_m')\}$. Take the first signatures in both groups as an example, the B first computes

$$V_1 = \sum_{i=1}^{m} V_i - \sum_{i=2}^{m} V_i \tag{9}$$

$$V_1' = \sum_{i=1}^{m} V_i' - \sum_{i=2}^{m} V_i' \tag{10}$$

, and then B eventually derives the value S_{IDi} by computing

$$\begin{aligned} &\frac{h_2' V_1 - h_2 V_1'}{h_2 - h_2'} \bmod q \\ &= \frac{h_2' h_2 r_1 + h_2' S_{ID_i} - h_2 h_2' r_1 - h_2 S_{ID_i}}{h_2' - h_2} \bmod q \\ &= S_{IDi}. \end{aligned} \tag{11}$$

As a result, B can break the ECDLP *within expected time less than* $120686\, QT/\varepsilon$, *if* $\varepsilon \geq 10(R+1)(R+Q)/q$.

IV. Our Proposed Authentication Scheme

This section first introduces our system model and security requirements for V-to-I communications. Then, we present our conditional privacy-preserving authentication scheme based on our proposed ID-based batch signature scheme.

A. System Model

A vehicular sensor network model composed of two layers is defined as follows. The lower layer consists of vehicles on roadways and RSUs along with roadsides. Each vehicle is equipped with at least an OBU and a reliable positioning system, such as global positioning system (GPS). The OBU is a data storage device with limited computing capability, and is embedded within a tamper-proof box. The OBU is wirelessly connected to the RSU through a secure channel, and is enabled with a synchronizable clock generator to effectively communicate with the RSU. Pseudo-identities and corresponding private keys of each vehicle are stored in the tamper-proof box device of OBU. The pseudo identities and its corresponding private keys of each vehicle can be renewed periodically in conjunction with regular vehicle maintenance. The upper layer of the vehicular sensor network consists of application servers (such as a traffic control and analysis center), a Private Key Generator (PKG) and a Trace Authority (TRA). The PKG and TRA are responsible for system initialization in our scheme, and we therefore assume that the PKG and the TRA are trusted and have sufficient storage space, memory modules, and computing power. Depending on the practical implementation environment, the PKG and TRA can be viewed or built together as one Trusted Authority (TA). Secure communication among TAs and RSUs is assumed since wired networks with secure protocols such as Transport Layer Security protocol are usually deployed among TAs and RSUs.

B. Security Requirements

In order to provide secure communication for the vehicle sensor network, we developed an anonymous authentication scheme based on our ID-based batch signature scheme. The proposed authentication scheme achieves the following security requirements:

(1) **Message authentication and integrity**: Each message from a vehicle is authenticated to ensure that this message cannot be modified or forged by a malicious adversary.
(2) **Identity privacy preserving**: The identity of a vehicle is not shown in any transmitted message, and all vehicles and any third party agency cannot learn the identity of a vehicle based on messages sent from a given vehicle. The only exception is that TRA is authorized to reveal the identity of a vehicle when it is necessary.
(3) **Traceability**: TRA has the capability to know the real identity of a vehicle from a transmitted message when the targeted vehicle disputes its signature associated with the corresponding message.

C. Our Authentication Scheme

The proposed authentication scheme consists of two parts: **Vehicle to RSU** and **RSU to Vehicle**. Vehicle-to-RSU communication consists of four phases: **system setup**, **pseudo-IDs generation and private key extraction**, **vehicle message signing**, and **verification of traffic information messages** phases. The system setup phase is executed by the PKG to generate the system parameters. In the private key phase, the TRA generates pseudo-IDs for each vehicle and following

TABLE I
NOTATIONS

Notation	Description	Notation	Description
V_i	ith vehicle	RID_i	A real identity for a vehicle
TRA, PKG	A Tracing Authority and a Private Key Generator	ID_R	An identity of a RSU
e	A bilinear pairing function	G_1	A cyclic additive group
s, P_{pub}	The private key and its corresponding public key of a Private Key Generator	$E_k(.)/D_k(.)$	A symmetric encryption/decryption function with a secret key k
α	The secret key of a Tracing Authority	q	The prime order of G_1
H_1, H_2	Two one-way hash functions	tt_i, tt_i^R	The current timestamp
t_i	The valid period of this pseudo-ID	PID_i=$\{PID_{i,1}, PID_{i,2}, t_i\}$	A pseudo identity for a vehicle

this the PKG generates corresponding private keys using these pseudo-IDs. Similar to the authentication scheme proposed by Shamir, we also utilize a preloading method based on our IBS scheme, in which a pool of pseudo-IDs, with short expiration time, and private keys are loaded into each vehicle by the TAs at the pseudo-ID generation and private key extraction phases. When VSN is accessible with sufficient bandwidth and the available unused pseudo-IDs are running out, the pseudo-ID pool will be replenished via a secure channel between the vehicle and TAs after proper authentication. Through these two initialization phases, each vehicle is registered with the TAs and preloaded with system parameters, its own pseudo-ID set, and private keys. In the message signing and batch verification of traffic information messages phases, each vehicle sends its traffic-related messages and its corresponding signatures to a nearby RSU, and the RSU then checks the validities of multiple signatures. Unlike the vehicle-to-RSU communication, the messages in RSU-to-Vehicle communication do not need to provide a privacy requirement, so we directly employ our ID-based signature scheme to sign the traffic-related messages. Thus, our authentication scheme for RSU-to-Vehicle communication has the same phases as that for Vehicle-to-RSU, except for removing the system setup and Pseudo-IDs generation. The notations are given in Table I.

***Vehicle to RSU**:*

***System setup**:* Let F_n be the finite field over a prime order n. Let $(a, b) \in F_n$ be the parameters of elliptic curve E ($y^2 = x^3 + ax + b \pmod n$, where $4a^3 + 27b^2 \neq 0$) over F_n. Let O denote infinity. Let P be the generator point of E with a prime order q, where $P \neq O$. The PKG computes its corresponding public key $P_{pub} = sP$, where s is a master private key for private key extraction. The TRA also selects a random number α as its master secret key for users' pseudo ID generation and for computing its public key $T_{pub} = \alpha P$. Next, the PKG and the TRA choose three one-way hash functions: H: $\{0,1\}^* \rightarrow Z_q$, H_1: $\{0,1\}^* \rightarrow Z_q$ and H_2: $\{0,1\}^* \rightarrow Z_q$, and then they publish $\{P, P_{pub}, T_{pub}, q, H, H_1, H_2\}$ as the system public parameters. Notice that the system public parameters are preloaded into the tamper-proof device of all vehicles.

Pseudo-IDs generation and private key extraction: In this phase, each vehicle needs to send its identity (RID_i) to the TRA for registration. The TRA is then responsible for generating pseudo-IDs and the PKG is responsible for generating the private keys based on the generated pseudo-IDs. Details of this phase are described as follows.

Step1. A vehicle V_i with the real identity RID_i computes $PID_{i,1} = d_i P$ and then sends $(RID_i, PID_{i,1})$ to the TRA via a secure channel, where d_i is a random number.

Step2. Upon receiving RID_i from the vehicle V_i, the TRA first checks RID_i, and then computes

$$PID_{i,2} = RID_i \oplus H(\alpha PID_{i,1}, PID_{i,1}, t_i, T_{pub}) \tag{12}$$

where t_i is the valid period of this pseudo-ID PID_i. Following this, the TRA sends this pseudo identity $PID_i = (PID_{i,1}, PID_{i,2}, t_i)$ to the PKG via a secure channel for pseudo private key generation.

Step3. Upon receiving a pseudo identity PID_i, the PKG computes

$$K_i = k_i P \tag{13}$$

$$S_i = r_i + H_1(PID_i, K_{i,k}) \times s \bmod q \tag{14}$$

corresponding to the user's pseudo identity PID_i, where k_i is a random number. After that, the PKG sends pseudo-IDs PID_i and its corresponding private keys (K_i, S_i) back to the user via a secure channel.

***Vehicle message signing**:* In this phase, all the traffic-related messages should be signed by vehicles before sending these traffic-related messages to the RSU. Upon receiving the traffic-related messages and its corresponding signatures, a RSU needs to ensure that no adversary masquerades as a legal vehicle in an attempt to cheat it. Details of this phase are described as follows.

Step 1. Vehicle V_i randomly select a pseudo ID PID_i and its corresponding private key S_i from its pseudo IDs and its corresponding private keys and then computes

$$R_i = r_i P \tag{15}$$

$$V_i = H_2(K_i, R_i, PID_i, M_i, tt_i) \times r_i + S_i \bmod q \tag{16}$$

where r_i is a random number and tt_i is the current timestamp. Notice that R_i can be pre-computed by a vehicle before the vehicle generates a signature on a traffic-related message. $\sigma = \{K_i, R_i, V_i\}$ is a signature on the traffic-related message M_i and the current timestamp tt_i for $PID_{i,k}$.

Step 2. Vehicle V_i sends $\{PID_{i,k}, M_i, tt_i, \sigma\}$ to a nearby RSU.

Verification of traffic information messages: Upon receiving n distinct traffic-related message-signature tuples $\{PID_i, M_i, tt_i, \sigma\}$ $(i = 1, \ldots, n)$, the RSU first checks whether the timestamps tt_i $(i = 1, \ldots, n)$ are in a valid time interval and that t_i in PID_i is valid. If they hold, the RSU computes $h_{i,1} = H_1(PID_i, K_i)$ and $h_{i,2} = H_2(K_i, R_i, PID_i, M_i, tt_i)$ for $i = 1, \ldots, n$ and then checks whether the following equation holds

$$\left(\sum_{i=1}^{n} V_i\right) P = \left(\sum_{i=1}^{n} h_{i,2} R_i\right) + \sum_{i=1}^{n} K_i + \left(\sum_{i=1}^{n} h_{i,1}\right) P_{pub}. \tag{17}$$

If the Eq. (17) holds, the RSU accepts these received traffic-related message-signature tuples $\{PID_i, M_i, tt_i, \sigma\}$ $(i = 1, \ldots, n)$. Notice that the receiving traffic-related signatures are generated by n distinct vehicles. In order to overcome the attack proposed by Liu *et al.* [32], we can replace Eq. (17) with the following equation, where $a_i \in_R \{0, 1\}^l$ are randomly chosen for $i = 1, \ldots, n$. Usually $l = 80$ [32] is enough for normal scenarios in VANETs

$$\left(\sum_{i=1}^{n} a_i V_i\right) P = \left(\sum_{i=1}^{n} a_i h_{i,2} R_i\right) + \sum_{i=1}^{n} a_i K_i + \left(\sum_{i=1}^{n} a_i h_{i,1}\right) P_{pub}. \tag{18}$$

If the Eq. (18) holds, it means that these distinct n signatures are valid.

RSU to Vehicle:

Private key extraction: Given an RSU's identity ID_R, the PKG computes

$$T_R = kP \tag{19}$$

$$h_R = H_1(ID_R, T_R) \tag{20}$$

$$S_R = k + h_R \times s \bmod q \tag{21}$$

where k is a random number. The PKG submits the private key (T_R, S_R) to the RSU via a secure channel. Upon receiving the private key (T_R, S_R), the RSU stores it into its secure memory.

RSU message signing: When a RSU wants to broadcast a traffic-related message $M_i \| tt_i^R$, the RSU computes

$$U_i^R = rP \tag{22}$$

$$h_i' = H_2\left(ID_R, M_i, T_R, tt_i^R, U_i^R\right) \tag{23}$$

$$V_i^R = h_i' \times r_i + S_R \bmod q \tag{24}$$

where r is a random number and tt_i is the current timestamp. Next, the RSU sends the traffic-related message $M_i \| tt_i^R$ and its corresponding signature (T_R, U_i^R, V_i^R) to the vehicles. Notice that $U_i^R = rP$ can be pre-computed before RSU wants to broadcast a traffic-related message $M_i \| tt_i^R$.

Verification of traffic information messages: Upon receiving the traffic message $M_i \| tt_i$ and its corresponding signature (T_R, U_i^R, V_i^R) from the RSU, the vehicle checks whether the identity information exists in the received message. If the received identity information does not exist in it, the message is ignored. Next, a vehicle verifies the validity of the received signature (T_R, U_i^R, V_i^R) by checking the following equation

$$V_i^R P = h_i' U_i^R + T_R + h_R P_{pub} \tag{25}$$

where $h_R' = H_2(ID_R, M_i, T_R, tt_i, U_i^R)$ and $h_R = H_1(ID_R, T_R)$. If it holds, the vehicle accepts the received signature (T_R, U_i^R, V_i^R). Otherwise, the received signature (T_R, U_i^R, V_i^R) is rejected. If m distinct signed messages $(M_1 \| tt_1, M_2 \| tt_2, \ldots, M_m \| tt_m)$ and signatures $((T_R, U_1^R, V_1^R), (T_R, U_2^R, V_2^R), \ldots, (T_R, U_m^R, V_m^R))$ from the same RSU are given, the vehicle can verify them by checking the following equation:

$$\left(\sum_{i=1}^{m} V_i^R\right) P = \left(\sum_{i=1}^{m} h_i' U_i^R\right) + \sum_{i=1}^{m} T_R + \left(\sum_{i=1}^{m} h_R\right) P_{pub}. \tag{26}$$

If it holds, the vehicle accepts the received signatures. In the batch verification process, m distinct signatures can be verified.

In order to overcome the attack proposed by Liu *et al.* [32], we can replace Eq. (26) with the following equation, where $a_i \in_R \{0, 1\}^l$ are randomly chosen for $i = 1, \ldots, m$. Usually $l = 80$ [32] is enough for normal scenarios in VANETs

$$\left(\sum_{i=1}^{m} a_i V_i^R\right) P = \left(\sum_{i=1}^{m} a_i h_i' U_i^R\right) + \sum_{i=1}^{m} a_i T_R + \left(\sum_{i=1}^{m} a_i h_R\right) P_{pub}. \tag{27}$$

If the Eq. (27) holds, it means that these distinct m signatures are valid.

V. Security Analysis

In this section, we show that the proposed scheme can achieve the following security requirements.

Provision to Source Authentication and Message Integrity: We have shown that the proposed identity-based batch signature scheme is secure against adaptive chosen ID attack and adaptive chosen message attack under random oracle. The proposed pseudo-ID authentication scheme is based on the proposed identity-based signature scheme. Thus, the proposed authentication scheme also supports pseudo-ID authentication, message integrity and non-repudiation.

Provision to Identity Privacy Preserving: In our authentication scheme, each pseudo identity PID_i contains the TRA's master secret key α and the user's chosen secret d_i. The values of the TRA's master secret key α and the user's chosen secret d_i are only known by the TRA and the user, respectively. Without knowing d_i or α, it is impossible for any malicious adversary to compute $\alpha PID_{i,1}$ due to CDH problems. Thus, even if an

TABLE II
EXECUTION TIME ON CRYPTOGRAPHIC OPERATIONS

	T_M	T_{MP}	T_P
Execution Time (ms)	0.03	1.50	8.12

adversary can identify a pseudo identity PID_i, they will not be able to retrieve that user's information.

Provision to Traceability: In the proposed scheme, the TRA with its master secret key α can reveal the real identity RID_i from a pseudo-ID $PID_i = (PID_{i,1}, PID_{i,2}, t_i)$ by computing $RID_i = PID_{i,2} \oplus H(\alpha PID_{i,1}, PID_{i,1}, t_i, T_{pub})$. Hence, if a signature is disputed, the TRA can trace the vehicle from the disputed signature.

Provision to User Unlinkability: User unlinkability means that no adversary can link messages sent from the same vehicle. The proposed scheme adapts the pseudo ID to achieve user unlinkability. Assume that an adversary wants to know whether two message M and M' are sent from the same vehicle. The adversary cannot do it successfully, since they will encounter the CDH problem. The unlinkability is maintained because these two messages are signed by different pseudo IDs and their corresponding private keys, and these pseudo IDs do not have any link. Hence, the proposed scheme provides complete user unlinkability.

Provision to Role Separation: There are two trusted authorities (TAs) in our scheme: TRA and PKG. TRA is responsible for generating each vehicle's pseudo-IDs and tracing the real identities from signed messages. PKG is responsible for generating each vehicle's private keys corresponding to their pseudo-IDs. Therefore, in our scheme, the PKG cannot trace the real identity of a vehicle from a pseudo ID. Only the TRA has the ability to do this, since the secret key α is only stored with the TRA. Like the private key of a certification authority (CA) in the PKI, the master secret key s of the PKG and the master secret key α of the TRA must be strongly protected. In order to protect the master secret key s (or α), we can use techniques of threshold cryptography [41], [42] to distribute the master secret key s (or α) by storing them among different PKGs (TRAs). The benefits of threshold technologies are that the compromised authorities (the number being less than the threshold) cannot trace vehicle users and compromise their private keys.

VI. COMPARISONS

Computation Overhead: In order to evaluate computation overhead of the proposed scheme, experiments were conducted to compare computation time among our scheme and other related works [21], [26], [30], [31], [40]. Let T_P be the time for performing a pairing operation, T_M be the time for performing a scalar multiplication operation, T_{MP} be the time for performing a scalar multiplication point operation. Table II shows required execution time for different cryptographic operations running on an Intel Pentium 4 3.0 GHz machine with 1GB RAM. Crypto library MIRACL is used to measure time consumption of these three cryptographic operations. Let n be the number of signatures for a batch verification process and T_H be the time for performing a MapToPoint operation. We evaluate the computation cost of our identity-based signature scheme as follows. Since the $a_i \in_R \{0,1\}^l$ $(i = 1, \ldots, n)$ are small random numbers, we omit the computation cost. In our scheme, the signer with an identity ID_i only needs one multiplication point operation, and one scalar multiplication operation to construct a signature (K_i, R_i, V_i) on the message M_i, where the one multiplication point operation can be pre-computed. In the verification process, the verifier only needs three point multiplication operations to verify the validity of the signature (K_i, R_i, V_i). In order to simultaneously verify n distinct signatures signed by n distinct signers, our scheme also developed a batch verification process. The batch verification process only needs $n + 2$ point multiplication operations. The computation cost among our scheme and existing schemes are given in Table III. From Table III, one can observe the following facts: (1) Yoon *et al.*'s scheme, EIBS, KIBS(CAPS), and our proposed scheme can pre-compute the value $R_i = r_i P$ before constructing one signature on a message. Thus, in terms of signature generation, the proposed scheme has better performance than other existing schemes if we pre-compute $R_i = r_i P$; (2) The proposed scheme does not require any pairing operation on signature verification and batch signature verification; (3) Only the proposed scheme and KIBS(CAPS) do not require any MapToPoint operation.

TABLE III
COMPUTATION COST OF IBS BATCH SCHEMES

	Signature generation	Signature Verification	n Signature Batch Verification
Yoon et al. [30]	$2T_{MP}$+T_H (pre-computed)	T_{MP}+T_H+$2T_P$	nT_{MP}+nT_H+(n+1)T_P
EIBS [31, 40]	$2T_{MP}$ (pre-computed)	T_{MP}+$2T_P$+T_H	nT_{MP}+$2T_P$+nT_H
ZLLHS [21]	T_{MP}	T_{MP}+T_H+$3T_P$	nT_{MP}+nT_H+$3T_P$
KIBS (CAPS) [26]	$2T_{MP}$ (pre-computed)	$2T_{MP}$+$3T_P$	(n+1)T_{MP}+$3T_P$
Present Study	T_M (pre-computed)	$3T_{MP}$	(n+2)T_{MP}

Since KIBS(CAPS) has the best efficiency compared with other existing schemes and does not require any MapToPoint operation, we only compare between computational costs of our proposed scheme and KIBS(CAPS). In terms of signature generation, the proposed scheme reduces $2T_{MP} - T_M$ computation time in comparison with KIBS(CAPS). There is a time reduction of approximately 2.97, based on Table II. Hence, the time for generating a signature in signature generation phase is reduced by $2.97/4.5 = 66\%$ in our scheme when compared with KIBS. In terms of signature verification phase and n signature batch verification phase, the proposed scheme reduces $3T_P - T_{MP}$ computation time compared with KIBS(CAPS).

TABLE IV
FORMAT OF THE SIGNED MESSAGE IN CURRENT IEEE TRIAL-USE STANDARD FOR VANET SECURITY

Protocol Version	Type	Message	Certificate	Signature
1 byte	1 byte	67 bytes	125 bytes	56 bytes

TABLE V
FORMAT OF THE SIGNED MESSAGE FOR OBU AND RSU IN THE PROPOSED SCHEME

Type ID	Message ID	Payload(message)	Timestamp	Signature	Pseudo ID (OBU)/RSU ID
1 byte	1 byte	67 bytes	4 bytes	60 bytes	41 bytes /10 bytes

In other words, no matter how many signatures are simultaneously verified, based on Table II the proposed scheme will reduce about 22.86 ms computation time in comparison with KIBS(CAPS), the next most efficient scheme available. As a result, our proposed scheme has better performance than KIBS(CAPS) in terms of computation cost.

Communication Overhead: The communication overhead of the proposed scheme is discussed as follows. Based on the current IEEE Trial-Use standard [6] for VANET security as shown in Table IV, a 67 bytes message generated from an OBU or a RSU should be first encapsulated into a signed message of 250 bytes. This signed message contains one byte for protocol version, one byte for type, 67 bytes for the original message, 125 bytes for certificate, and 56 bytes for ECDSA signature. In order to reduce signature size, Shim [26] developed a method to reduce the size of a point $Q = (x, y)$ if an OBU or a RSU can send this point to a well-designed destination, i.e., another RSU or OBU. The signature size reduction method is that an OBU or a RSU only sends the x-coordinate of Q and the designed destination can learn the y-coordinate by computing the square root. Since the size of the signature is reduced by applying Shim's method, the total communication cost of KIBS(CAPS) is reduced. Table V shows the format of the signed message adopted in our scheme. Based on the same signature size reduction method, the total size of one signed message is $159 + 159 + 159 + 3 = 480$ bits $= 60$ bytes, provided that a 159-bit subgroup of the MNT curve with an embedding degree of 6 is used in our scheme. Then, the total size of pseudo ID is $159 + 159 + 2 + 4 = 324$ bits $= 40.5$ bytes, where the timestamp field is set as 4 bytes. The proposed authentication scheme for RSU to vehicle communication uses a real RSU identity, therefore, 10 bytes is assumed for a real RSU identity. Hence, the total message size from vehicle (OBU) to RSU (RSU to vehicle) in the proposed authentication scheme is only 174 (143) bytes based on the signed message format shown in Table V. If the size reduction method proposed by Shim [26] is adopted, our proposed scheme has the same signature size as KIBS(CAPS). In summary, the proposed scheme and KIBS(CAPS) require less communication bandwidth to transmit signed messages by applying the signature size reduction method and corresponding message format when comparing with signed messages using current IEEE Trial-Use standard format for VANET security.

VII. CONCLUSION

In this study, a new efficient identity-based batch signature scheme is first introduced and then a new conditional privacy-preserving authentication scheme is developed based on the invented signature scheme for vehicular sensor network. Security analysis is conducted to show that the proposed identity-based batch signature scheme is secure against an adaptive chosen ID attack as well as an adaptive chosen message attack under random oracle. The proposed identity-based batch signature scheme does not utilize any MapToPoint operation and pairing operation. Therefore, the proposed signature scheme is more efficient in terms of time consumption. In comparison with KIBS(CAPS), the proposed authentication scheme is approximately 1.52 times faster at the signature generation stage. In terms of signature verification or batch signature verification with n signatures, the proposed authentication scheme always reduces $3T_P - T_{MP}$ computing time when comparing with KIBS(CAPS). The proposed authentication scheme supports anonymous authentication, message integrity, traceability for trusted third party, batch signature verification and driver unlinkability. In Table III, we have shown that our proposed authentication scheme is faster than other existing schemes in terms of total time consumption.

For future research directions, privacy-aware lightweight authentication schemes will have great demand in a near future when Internet of Things environments associated with drivers' hand held devices or vehicles are emerging and deployed massively. Another research direction is to design secure lightweight schemes for new VANET applications such as advertisement dissemination services [43].

REFERENCES

[1] R. Azimi, G. Bhatia, R. Rajkumar, and P. Mudalige, "Vehicular networks for collision avoidance at intersections," *Proc. SAE World Congr.*, Detroit, MI, USA, Apr. 2011, pp. 1–11.
[2] J. A. Misener, "Vehicle-infrastructure integration (VII) and safety: Rubber and radio meets the road in California," *Intellimotion*, vol. 11, no. 2, pp. 1–3, 2005.
[3] U. Lee *et al.*, "Mobeyes: Smart mobs for urban monitoring with a vehicular sensor network," *IEEE Wireless Commun.*, vol. 13, no. 5, pp. 52–57, Oct. 2006.
[4] F. Wang, D. Zeng, and L. Yang, "Smart cars on smart roads: An IEEE intelligent transportation systems society update," *IEEE Pervasive Comput.*, vol. 5, no. 4, pp. 68–69, Oct.–Dec. 2006.

[5] J. M. De Fuentes, A. I. Gonz´lez-Tablas, and A. Ribagorda, *Overview of Security Issues in Vehicular Ad-hoc Networks, Handbook of Research on Mobility and Computing: Evolving Technologies and Ubiquitous Impacts*. Hershey, PA, USA: IGI Global, 2011, pp. 894–911.

[6] *IEEE Trial-Use Standard for Wireless Access in Vehicular Environments (WAVE)—Security Services for Applications and Management Messages*, IEEE Std. 1609.2, Jul. 2006.

[7] *Digital Signature Standard (DSS)*, Nat. Inst. Stand. Technol., Washington, DC, USA, Fed. Inf. Process. Std. 1862, 2000. [Online]. Available: http://csrc.nist.gov/publications/fips/

[8] J. P. Hubaux, S. Capkun, and J. Luo, "The security and privacy of smart vehicles," *IEEE Security Privacy Mag.*, vol. 2, no. 3, pp. 49–55, May/Jun. 2004.

[9] L. Y. Yeh and Y. C. Lin, "A proxy-based authentication and billing scheme with incentive-aware multihop forwarding for vehicular networks," *IEEE Trans. Intell. Transp. Syst.*, vol. 15, no. 4, pp. 1607–1621, Aug. 2014.

[10] G. Yan, D. Wen, S. Olariu, and M. C. Weigle, "Security challenges in vehicular cloud computing," *IEEE Trans. Intell. Transp. Syst.*, vol. 14, no. 1, pp. 284–294, Mar. 2013.

[11] J. L. Tsai, N. W. Lo, and T. C. Wu, "Novel anonymous authentication scheme using smart cards," *IEEE Trans. Ind. Informat.*, vol. 9, no. 4, pp. 2004–2013, Nov. 2013.

[12] J. L. Tsai and N. W. Lo, "A privacy-aware authentication scheme for distributed mobile cloud computing services," *IEEE Syst. J.*, vol. 9, no. 3, pp. 805–815, Sep. 2015.

[13] C. Gamage, B. Gras, B. Crispo, and A. S. Tanenbaum, "An identity-based ring signature scheme with enhanced privacy," in *Proc. SecureComm*, 2006, pp. 1–5.

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

[15] R. Lu, X. Lin, H. Zhu, P. H. Ho, and X. Shen, "ECPP: Efficient conditional privacy-preservation protocol for secure vehicular communications," in *Proc. IEEE Conf. Comput. Commun.*, Apr. 2008, pp. 1229–1237.

[16] X. Lin *et al.*, "Security in vehicular ad hoc networks," *IEEE Commun. Mag.*, vol. 46, no. 4, pp. 88–95, Apr. 2008.

[17] X. Lin, X. Sun, P. H. 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.

[18] K. Sampigethaya *et al.*, "Caravan, providing location privacy for VANET," in *Proc. ESCAR*, 2005, pp. 1–15.

[19] A. Studer, E. Shi, F. Bai, and A. Perrig, "TACKing together efficient authentication, revocation, and privacy in VANETs," in *Proc. IEEE SECON Conf.*, 2009, pp. 1–9.

[20] J. Sun, C. Zhang, Y. Zhang, and Y. Fang, "An identity-based security system for user privacy in vehicular ad hoc networks," *IEEE Trans. Parallel Distrib. Syst.*, vol. 21, no. 9, pp. 1227–1239, Sep. 2010.

[21] C. Zhang, R. Lu, X. Lin, P. H. Ho, and X. Shen, "An efficient identity-based batch verification scheme for vehicular sensor networks," in *Proc. IEEE INFOCOM*, 2008, pp. 246–250.

[22] S. Ravi, A. Raghunathan, and S. Chakradhar, "Tamper resistance mechanisms for secure embedded systems," in *Proc. IEEE Int. Conf. VLSID*, 2006, pp. 605–611.

[23] S. Biswas, J. Misic, and V. Misic, "ID-based safety message authentication for security and trust in vehicular networks," in *Proc. 31st ICDCSW*, 2011, pp. 323–331.

[24] S. Biswas and J. Misic, "A cross-layer approach to privacy-preserving authentication in WAVE-enabled VANETs," *IEEE Trans. Veh. Technol.*, vol. 62, no. 5, pp. 2182–2192, Jun. 2013.

[25] J. L. Tsai, "An improved cross-layer privacy-preserving authentication in WAVE-enabled VANETs," *IEEE Commun. Lett.*, vol. 18, no. 11, pp. 1931–1934, Nov. 2014.

[26] K. A. Shim, "CPAS: An efficient conditional privacy-preserving authentication scheme for vehicular sensor networks," *IEEE Trans. Veh. Technol.*, vol. 61, no. 4, pp. 1874–1883, May 2012.

[27] F. Zhang, S. N. Reihaneh, and W. Susilo, "An efficient signature scheme from bilinear pairings and its applications," in *Proc. PKC*, 2004, pp. 277–290.

[28] P. S. L. M. Barreto, H. Y. Kim, B. Lynn, and M. Scott, "Efficient algorithms for pairing-based cryptosystems," in *Proc. Crypto*, 2002, pp. 354–368.

[29] A. Shamir, "Identity-based cryptosystems and signature schemes," in *Advances in Cryptology*. New York, NY, USA: Springer-Verlag, 1984, pp. 47–53.

[30] H. Yoon, J. H. Cheon, and Y. Kim, "Batch verifications with ID-based signatures," in *Proc. ICISC*, 2005, pp. 233–248.

[31] K. A. Shim, "An ID-based aggregate signature scheme with constant pairing computations," *J. Syst. Softw.*, vol. 83, no. 10, pp. 1873–1880, Oct. 2010.

[32] J. K. Liu, T. H. Yuen, M. H. Au, and W. Susilo, "Improvements on an authentication scheme for vehicular sensor networks," *Expert Syst. Appl.*, vol. 41, no. 5, pp. 2559–2564, Apr. 2014.

[33] J. H. Cheon and D. H. Lee, "Use of sparse and/or complex exponents in batch verification of exponentiations," *IEEE Trans. Comput.*, vol. 55, no. 12, pp. 1536–1542, Dec. 2006.

[34] A. L. Ferrara, M. Green, S. Hohenberger, and M. Ø. Pedersen, "Practical short signature batch verification," in *Proc. CT-RSA*, 2009, pp. 309–324.

[35] J. Camenisch, S. Hohenberger, M. Ø. Pedersen, "Batch verification of short signatures," *J. Cryptology*, vol. 25, no. 4, pp. 723–747, 2012.

[36] C. P. Schnorr, "Efficient identification and signatures for smart cards," in *Proc. CRYPTO*, 1990, pp. 339–351.

[37] S. Goldwasser, S. Micali, and R. L. Rivest, "Digital signature scheme secure against adaptive chosen-message attacks," *SIAM J. Comput.*, vol. 17, no. 2, pp. 281–308, Apr. 1988.

[38] D. Pointcheval and J. Stern, "Security arguments for digital signatures and blind signatures," *J. Cryptology*, vol. 13, no. 3, pp. 361–396, Jun. 2000.

[39] D. Pointcheval and J. Stern, "Security arguments for digital signatures and blind signatures," in *Proc. Eurocrypt*, 1996, vol. 1070, pp. 387–398.

[40] K. A. Shim, "Reconstruction of a secure authentication scheme for vehicular ad hoc networks using a binary authentication tree," *IEEE Trans. Wireless Commun.*, vol. 12, no. 11, pp. 5386–5393, Nov. 2013.

[41] P. Gemmell, "An introduction to threshold cryptography," *CryptoBytes, A Techn. Newsl. RSA Lab.*, vol. 2, no. 3, pp. 7–12, 1997.

[42] R. Gennaro, S. Jarecki, H. Krawczyk, and T. Rabin, "Secure distributed key generation for discrete-log based cryptosystems," in *Proc. Eurocrypt*, 1999, pp. 295–310.

[43] Z. Li, C. Liu, and C. Chigan, "On Secure VANET-based ad dissemination with pragmatic cost and effect control," *IEEE Trans. Intell. Transp. Syst.*, vol. 14, no. 1, pp. 124. 135, Mar. 2013.

Nai-Wei Lo received the B.S. degree in engineering science from National Cheng Kung University, Tainan, Taiwan, in 1988 and the M.S. and Ph.D. degrees in computer science and electrical engineering from the State University of New York at Stony Brook, Stony Brook, NY, USA, in 1992 and 1998, respectively.

He is currently a Professor with the Department of Information Management, National Taiwan University of Science and Technology, Taipei, Taiwan, and the Director of Taiwan Information Security Center, National Taiwan University of Science and Technology (TWISC@NTUST). His research interests include smart grid security, IoT/IoV security, web technology, and cloud security. He is a member of the IEEE Communications Society.

Jia-Lun Tsai received the Ph.D. degree from National Taiwan University of Science and Technology (NTUST), Taipei, Taiwan, in 2013.

He is currently an Adjunct Assistant Professor with the Department of Information Management, NTUST. He has published in more than 25 papers on journals and conferences. His research interests include cryptography, wireless security, and network security. He is the member of the Phi Tau Phi Scholastic Honor Society of the R.O.C. He currently serves as one of the editorial board members for the *Information Technology and Control* journal.