Two Forgeable and Untraceable Batch Authentication Schemes based on Pseudonym

Xiaoming Hu[a]
College of Computer and Information Engineering, Shanghai Polytechnic University, Shanghai, China

Keywords: Information Security, Batch Authentication Scheme, Certificateless Signature Scheme, Vehicle Ad Hoc Networks, Unforgeability.

Abstract: In the fields of intelligent transportation (InTrans) and vehicle ad hoc networks (VEAHT), data exchange between vehicle and vehicle or between vehicle and RSU (Road Side Unit) or between RSU and RSU or so on can cause many security problems such as sending a fake data or pretending to be a vehicle node or others. At the same time, in InTrans and VEAHT, data exchange is very frequent and also is very large. Batch authentication protocol or scheme based on pseudonym identity can improve the efficiency of message signature verification. What's more, it can protect the real identity of the vehicle node by using a pseudonym but the real identity can be traced when needed. In this paper, the security of two batch authentication schemes proposed recently is analyzed. This paper shows that the two schemes exist some security drawbacks and do not satisfy the security properties: unforgeability and traceability. In other words, a malicious vehicle (acts as an attacker) can forge a signature on a message without knowing the private key of the vehicle node and anyone cannot trace the real identity of the attacker. Finally, this paper also gives a simple improvement on the existing security drawbacks.

1 INTRODUCTION

Under the environment of intelligent transportation (Alanazi 2019, Lo 2016, Qu 2015, Zhang 2017) (InTrans) or vehicle ad hoc networks (He 2015, Li 2015, Liu 2014, Liu 2018, Shim 2012) (VEAHT), the vehicle can periodically broadcast its own data information during driving and receive data from other vehicles or the RSU (Road Side Unit) which helps to reduce the incidence of traffic accidents and helps the vehicle to plan better traffic routes. However, traffic data can involve some sensitive information such as the identity of vehicle or position which the owner of the vehicle wish only the trust organization such as RSU or TA (Trusted Authority) can get these data. On the other hand, in order to prevent illegal attacks from malicious vehicles, it needs to authenticate the realness of the identity of the vehicle and the truth of the message. Authentication technology (Cui 2018, Wang 2016, Zhong 2016) can satisfy the secure data exchange and privacy protection of the vehicle.

However, the amount of data that vehicles produce and receive every day is huge which leads to a lot of verification load. Batch authentication protocol or scheme (Bayat 2015, Gayathri 2018, Horng 2017) can effectively solve the problem. In a batch authentication scheme, the signature verifier can verify the validity of *n* signature on *n* messages with only one verification operation which improves the verification efficiency largely. Therefore, many scholars present many authentication schemes (Cui 2018, Wang 2016, Zhong 2016, Bayat 2015, Gayathri 2018, Horng 2017). However, a general authentication scheme cannot protect the privacy of the vehicles. An authentication scheme with (conditional) privacy-preserving (Horng 2015, Huang 2011, Lin 2007, Zhang 2020) can solve the problem.

In 2020, Wang et al. proposed an authentication protocol based on pseudonym in InTrans (Wang 2021). At the same time, the protocol is conditional privacy-preserving. In other words, the real identity of the vehicle can be protected normally. But when needed, the real identity of the vehicle can be traced by some method. In 2021, Zeng et al. proposed a certificateless (Ma 2020, Xie 2020, Zhao 2020, Zuo 2019, Zuo 2020) authentication scheme in VEAHT

[a] https://orcid.org/0000-0001-8046-6457

Hu, X.
Two Forgeable and Untraceable Batch Authentication Schemes based on Pseudonym.
DOI: 10.5220/0011375200003443
In *Proceedings of the 4th International Conference on Biomedical Engineering and Bioinformatics (ICBEB 2022)*, pages 985-991
ISBN: 978-989-758-595-1

(Zeng 2020). The scheme adopts the pseudonym of the vehicle to protect the real identity of the vehicle. But the real identity of the vehicle also is traced afterwards. However, in this paper, we present that in both authentication schemes, a malicious attacker can forge a signature without known the private key of the vehicle, namely do not hold the unforgeability. At the same time, the both schemes also do not hold the traceability, namely the real identity of the vehicle cannot be traced afterwards. In order to overcome these drawbacks, an improved method for the both schemes is presented.

2 REVIEW, SECURITY ANALYSIS AND IMPROVEMENT OF A CONDITIONAL PRIVACY PRESERVING OF AUTHENTICATION PROTOCOL

Here, we present a simple review, security analysis and a simple improvement on Wang et al.'s authentication protocol (Wang 2021).

2.1 Look Back on Wang et al.'s Authentication Protocol

Wang et al.'s authentication protocol (Wang 2021) consists of three stages: System Initial, Identity Authentication based on Pseudonym and Message Authentication based on Pseudonym.

2.1.1 System Initial Stage

- System parameters generation: Define six cryptography hash functions $H_0 : \{0,1\}^* \times \{0,1\}^* \rightarrow \{0,1\}^*$, $H_2 : \{0,1\}^* \rightarrow Z_q^*$, $H_1, H_3, H_4, H_5 : G \times \{0,1\}^* \rightarrow Z_q^*$ .ECA (Enrollment Certificate Authority) chooses $a \in_R Z_q^*$ as its private key SK_{ECA} and computes its public key PK_{ECA} = aP . Then, the system parameters publicly is $\{ P, G, q, PK_{ECA}, H_0, H_1, H_2, H_3, H_4, H_5 \}$. PCA (Pseudonym Certificate Authority) generates the private-public pair (SK_{PCA_i} , PK_{PCA_i}) as the above methods.
- Node registration certificate application: ECA generates registration information as follows for vehicles and RSUs (Road Side Unit) after ECA authenticates the vehicles and the RSUs. For the vehicle V_a with its real identity information RID_a , ECA chooses $\beta \in_R Z_q^*$ and computes $STicket_a$ = $H_0(\beta, RID_a)$ and $PTicket_a$ = $STicket_a P$. EVA issues the registration certificate $Ecert_a$ to V_a . For RSU R_u with its position information Loc_{R_u} , ECA computes R_u 's private and public pair (SK_{R_u} , PK_{R_u}). EVA issues the registration certificate $Ecert_u$ to R_u .

2.1.2 Identity Authentication based on Pseudonym Stage

- First, make non-interactive identity authentication based on chameleon hash, the detail process refers to the literature (Wang 2021).
- Identity authentication process based on pseudonym: when the vehicle V_a applies to PCA_i for a pseudonym, V_a chooses $\theta_1 \in_R Z_q^*$ as its temporary private key $SK_a^{'}$ and computes its temporary public key $SK_a^{'} = \theta_1 P$, and its temporary share key $K_{ai} = \theta_1 PK_{PCA_i}$. V_a chooses $k_a \in_R Z_q^*$ and computes its part pseudonym $PID_{a1} = k_a P$ and certificated value c_{ap} = $STicket_a + \theta_1 H_1 (PK_a^{'}, PID_{a1}, t)$ where t is the time stamp.
- PCA_i computes the part pseudonym PID_{a2} = H_1 (SK_{PCA_i} , PID_{a1} , $PTicket_a$, t) for V_a if $c_{ap} P$ = $PTicket_a$ + $PK_a^{'} H_1$ ($PK_a^{'}$, PID_{a1} , t). Then, the full pseudonym for V_a is PID_a = (PID_{a1} , PID_{a2}). Then, PCA_i chooses $\lambda_a \in_R Z_q^*$ and computes $PID_a^{'}$ = $H_2(PID_a)$, Λ_a = $\lambda_a P$, h_a = H_3 (Λ_a , PK_{PCA_i} , $PID_a^{'}$), d_a = $SK_{PCA_i} + \lambda_a h_a$ as its part private key.
- V_a chooses $x_a \in_R Z_q^*$ and computes $X_a = x_a P$. Then, its private key is SK_a = (x_a , d_a) and its

public key PK_a = (X_a , Λ_a), and is its pseudonym PID_a = (PID_{a1} , PID_{a2}).

- Vehicles and RSU makes two way identity authentications before data exchange (Wang 2021).

2.1.3 Message Authentication based on Pseudonym Stage

- Signature stage: given a message m_a , the vehicle V_a chooses ω_a $\in_R$ Z_q^* and computes $\Omega_{a=}\omega_a P$,

$$g_a = H_4(m_a, PID_a, \Omega_a, \Lambda_a, t),$$
$$l_a = H_5(m_a, PID_a, \Omega_a, \Lambda_a, t),$$
$$\sigma_a = \omega_a + g_a x_a + l_a d_a.$$

And then ($\sigma_a, \Omega_a, \Lambda_a, t$) is the signature on m_a .

- Verification stage: after R_u gets a signature (σ_a , Ω_a , Λ_a , t), R_u verifies the freshness of the time t , and then computes g_a , l_a , and verifies if

$$\sigma_a P = \Omega_a + g_a X_a + l_a (PK_{PCA_i} + h_a \Lambda_a) \quad (1)$$

2.2 Security Analysis and Improvement of Wang et al.'s Authentication Protocol

Here, we make the analysis on the security of Wang et al.'s authentication protocol. We show that their authentication protocol does not satisfy the unforgeability. Their protocol also does not satisfy the traceability for the real identity of the vehicle.

2.2.1 The Forgeability Attack

The attacker can forge a signature without known the private key of the signature vehicle. And the attacker cannot be traced afterwards.

- The attacker chooses a message $m_a^{'}$ and generates a pseudonym $PID_a^{''}$ = ($PID_{a1}^{''}$, $PID_{a2}^{''}$) for the vehicle V_a . Then, the attacker chooses $\omega_a^{'}$ $\in_R$ Z_q^* and $x_a^{'}$ $\in_R$ Z_q^*.
- The attacker computers

$$PID_a^{'} = H_2(PID_a^{''\,'}),$$
$$\Omega_a^{'} = \omega_a^{'} P,$$
$$g_a^{'} = H_4(m_a^{'}, PID_a^{''}, \Omega_a^{'}, \Lambda_a, t^{'}),$$
$$l_a^{'} = H_5(m_a^{'}, PID_a^{''}, \Omega_a^{'}, \Lambda_a, t^{'}),$$
$$h_a = H_3(\Lambda_a, PK_{PCA_i}, PID_a^{'\,'}),$$
$$X_a^{'} = -g_a^{'-1} l_a^{'} (PK_{PCA_i} + h_a \Lambda_a) + g_a^{'-1} x_a^{'} P,$$
$$\sigma_a^{'} = \omega_a^{'} + x_a^{'}.$$

Then, ($\sigma_a^{'}, \Omega_a^{'}, \Lambda_a, t^{'}$) is the forged signature on $m_a^{'}$ where $t^{'}$ is the time stamp.

- ($\sigma_a^{'}, \Omega_a^{'}, \Lambda_a, t^{'}$) is a correct signature because

$$\Omega_a^{'} + g_a^{'} X_a^{'} + l_a^{'} (PK_{PCA_i} + h_a \Lambda_a)$$
$$= \begin{matrix} \Omega_a^{'} + g_a^{'}(-g_a^{'-1} l_a^{'} (PK_{PCA_i} + h_a \Lambda_a) \\ + g_a^{'-1} x_a^{'} P) + l_a^{'} (PK_{PCA_i} + h_a \Lambda_a) \end{matrix},$$
$$= \begin{matrix} \Omega_a^{'} - l_a^{'} (PK_{PCA_i} + h_a \Lambda_a) + x_a^{'} P \\ + l_a^{'} (PK_{PCA_i} + h_a \Lambda_a) \end{matrix},$$
$$= \Omega_a^{'} + x_a^{'} P,$$
$$= \omega_a^{'} P + x_a^{'} P$$
$$= \sigma_a^{'} P.$$

2.2.2 The Untraceability

When ECA finds to exist a malicious vehicle node or happen the dispute, ECA can trace the real identity of the malicious vehicle node or the dispute vehicle node by the pseudonym $PID_a^{''}$ = ($PID_{a1}^{''}$, $PID_{a2}^{''}$) using the method of the literature (Wang 2021). However, $PID_a^{''}$ is generated by the attacker without any real identity of the vehicle, so ECA cannot trace the real identity of the vehicle.

2.2.3 The Simple Improvement

- From the above attack, it can find that the main reason that the attacker can forge a valid signature is that the attacker can modify arbitrarily $X_a (= x_a P)$. Therefore, the improved method is to limit X_a . The process is as follows.

Signature stage: the vehicle V_a chooses ω_a $\in_R$ Z_q^* and computes $\Omega_a = \omega_a P$,

$$g_a = H_4(m_a, PID_a, \Omega_a, \Lambda_a, X_a, t),$$

$$l_a = H_5(m_a, PID_a, \Omega_a, \Lambda_a, X_a, t),$$

$$\sigma_a = \omega_a + g_a x_a + l_a d_a,$$

and then (σ_a , Ω_a , Λ_a , t) is the signature on the message m_a .

The remaining stages are the same to the original methods of the literature (Wang 2021). Because X_a is the input of hash functions H_4 and H_5 , the attacker cannot modify the X_a . So, the attacker cannot forge the valid signature without the private key of the signer.

3 REVIEW, SECURITY ANALYSIS AND IMPROVEMENT OF CERTIFICATELESS AUTHENTICATION SCHEME

3.1 The Simple Improvement

Zeng et al.'s certificateless authentication scheme (Zeng 2020) consists of six stages: SetupSys Stage, PartKey Extract Stage, User Key Generation Stage, Pseudonym Generation Stage, Signature Stage and Verification Stage.

3.1.1 SetupSys Stage

- System initialization: KGC (Key Generation Center) chooses $s_1 \in_R Z_q^*$ as its private key and computes its public key $P_K = s_1 P$. TA (Trusted Authority) chooses $s \in_R Z_q^*$ as its main private key and computes its public key $P_T = sP$ .KGC and TA choose randomly five hash functions h : $G \rightarrow Z_q^*$, h_1 : $\{0,1\}^* \rightarrow Z_q^*$, h_3 , h_4 : $\{0,1\}^* \times G \times \{0,1\}^{*2} \rightarrow Z_q^*$, h_2 : $\{0,1\}^* \times G^2 \rightarrow Z_q^*$. KGC and TA issue the public system parameters { P , G , q , P_T , P_K , $h_1 \sim h_4$ }.
- RSU initialization: for a given RSU, TA chooses $k_r \in_R Z_q^*$ as RSU's private key and computes RSU's public key $PK_r = k_r P$. Then, choose $h \in_R Z_q^*$ and compute RSU's signature Sig$_r$ = sh($ID_r \| PK_r \| T$) where T is the time stamp.
- Vehicle initialization: for a given vehicle V_i , TA gives a real identity RID_i and a password PWD_i to V_i . Then, V_i computes $Q_i = h(RID_i)$ and AID_i = (Q_i , $RID_i \oplus h(\beta P_T)$).

3.1.2 PartiKey Extract Stage

- When a vehicle V_i requests KGC to generate the partial key, KGC chooses $d_i \in_R Z_q^*$ and computes $D_i = d_i P$, $\varphi_i = d_i + s_1 h_2(Q_i \| D_i \| P_K) \bmod q$. KGC sends (D_i , φ_i) to V_i .
- After V_i gets (D_i , φ_i), V_i accepts (D_i , φ_i) if $\varphi_i P = D_i + P_K h_2(Q_i \| D_i \| P_K)$.

3.1.3 User Key Generation Stage

The vehicle V_i chooses $x_i \in_R Z_q^*$ and computes $X_i = x_i P$. Then, its private key is SK_i = (φ_i , x_i) and its public key PK_i = (D_i , X_i).

3.1.4 Pseudonym Generation Stage

For a given vehicle V_i , RSU choose $r_i \in_R Z_q^*$ and computes its pseudonym ID_i = (T_i , ID_{i1} , ID_{i2}), where $ID_{i1} = R_t r_i P$, $ID_{i2} = RID_i \oplus h(\beta P_T) \oplus h(T_i r_i P_T)$ and T_i is the valid period.

3.1.5 Signature Stage

Given a message M_i = (m_i , T_i), the vehicle V_i chooses $w_i \in_R Z_q^*$ and computes the signature (σ_i , W_i), where

$$W_i = w_i P,$$

$$h_{3i} = h_3(ID_i \| D_i \| X_i \| T_i),$$

$$h_{4i} = h_4(ID_i \| M_i \| W_i \| X_i \| T_i),$$

$$\sigma_i = h_{4i}(h_{3i} x_i + w_i) + \varphi_i \bmod q .$$

3.1.6 Verification Stage

- After RSU gets a signature (σ_i , W_i), RSU checks if the signature is fresh. If the signature is fresh, RSU verifies if

$$\sigma_i P = h_{4i}(h_{3i}X_i + W_i) + D_i + P_K h_{1i} . \qquad (2)$$

- When RSU gets n signatures on n message, RSU makes the batch verification as the literature (Zeng 2020).

3.2 Security Analysis and Improvement of Zeng et al.'s Certificateless Authenti-cation Scheme

- Here, we make the analysis on the security of Zeng et al.'s certificateless authentication scheme. We show that Zeng et al.'s certificateless authentication scheme exists the same security drawback as the above scheme (Wang 2021), namely Zeng et al.'s certificateless authentication scheme does not satisfy the unforgeability. At the same, their scheme also does not satisfy the traceability for the real identity of the vehicle.

3.2.1 The Forgeability Attack

Here, the attacker acts as a malicious KGC. The attacker can forge a signature with known the secret key of KGC but it cannot replace the public key of the vehicle V_i . Finally, the attacker cannot be traced afterwards.

- The attacker chooses $ID_i^{'}$ = ($T_i^{'}$, $ID_{i1}^{'}$, $ID_{i2}^{'}$), $Q_i^{'}$, and $m_i^{'}$. Then, the attacker chooses $w_i^{'} \in_R Z_q^*$ and $d_i^{'} \in_R Z_q^*$.
- The attacker computers

$$\begin{aligned}
&D_i^{'} = d_i^{'} P , \\
&h_{3i}^{'} = h_3(ID_i^{'} \parallel D_i^{'} \parallel X_i \parallel T_i^{'}) , \\
&h_{1i}^{'} = h_2(Q_i^{'} \parallel D_i^{'} \parallel P_K) , \\
&W_i^{'} = w_i^{'} P - h_{3i}^{'} X_i , \\
&h_{4i}^{'} = h_4(ID_i^{'} \parallel m_i^{'} \parallel W_i^{'} \parallel X_i \parallel T_i^{'}) , \\
&\sigma_i^{'} = h_{4i}^{'} w_i^{'} + d_i^{'} + s_1 h_{1i}^{'} ,
\end{aligned}$$

Then, ($\sigma_i^{'}$, $W_i^{'}$) is the forged signature on $m_i^{'}$.

- ($\sigma_i^{'}$, $W_i^{'}$) is a correct signature because

$$\begin{aligned}
&\sigma_i^{'} P \\
&= (h_{4i}^{'} w_i^{'} + d_i^{'} + s_1 h_{1i}^{'}) P , \\
&= h_{4i}^{'} w_i^{'} P + d_i^{'} P + s_1 h_{1i}^{'} P , \\
&= h_{4i}^{'} (w_i^{'} P - h_{3i}^{'} X_i + h_{3i}^{'} X_i) + d_i^{'} P + s_1 h_{1i}^{'} P , \\
&= h_{4i}^{'} (W_i^{'} + h_{3i}^{'} X_i) + d_i^{'} P + s_1 h_{1i}^{'} P , \\
&= h_{4i}^{'} (W_i^{'} + h_{3i}^{'} X_i) + D_i^{'} + h_{1i}^{'} P_K .
\end{aligned}$$

3.2.2 The Untraceability

When TA finds to exist a malicious vehicle node, according to the scheme (Zeng 2020), TA can trace the real identity of the malicious vehicle node V_i by the pseudonym $ID_i^{'}$ = ($T_i^{'}$, $ID_{i1}^{'}$, $ID_{i2}^{'}$), namely RID_i = $ID_{i2}^{'} \oplus h(\beta P_T) \oplus h(sID_{i1}^{'})$. However, $ID_i^{'}$ is chosen by the attacker without any real identity of the vehicle V_i , so TA cannot trace the real identity RID_i of the vehicle V_i by computing $ID_{i2}^{'} \oplus h(\beta P_T)$ $\oplus h(sID_{i1}^{'})$.

3.2.3 The Simple Improvement

From the above attack, it can find that the main reason that the attacker acts as a malicious KGC can forge a valid signature is that the attacker can modify arbitrarily W_i (= $w_i P$). Therefore, the improved method is to limit W_i . The process is as follows.

- Given a message M_i = (m_i , T_i), the vehicle V_i chooses $w_i \in_R Z_q^*$ and computes the signature (σ_i , W_i), where

$$\begin{aligned}
&W_i = w_i P , \\
&h_{3i} = h_3(ID_i \parallel D_i \parallel X_i \parallel W_i \parallel T_i) , \\
&h_{4i} = h_4(ID_i \parallel M_i \parallel W_i \parallel X_i \parallel T_i) , \\
&\sigma_i = h_{4i}(h_{3i} x_i + w_i) + \varphi_i \mod q ,
\end{aligned}$$

and then (σ_i , W_i) is the signature on the message m_i .

The remaining stages are the same to the original methods of the literature (Zeng 2020). Because W_i is the input of the hash function h_3 , the attacker cannot modify the W_i . So, the attacker cannot forge the valid signature even who knows the private key of KGC.

4 CONCLUSIONS

In this paper, two batch authentication schemes based on pseudonym is reviewed. Then, this paper gives an analysis on the security of the two batch authentication schemes. The analysis shows that both of the batch authentication schemes do not satisfy the unforgeability, a malicious vehicle node or a malicious KGC (Key Generation Center) can forge a signature on any choose message which leads to be untraceable of the real identity of the vehicle. In other words, the two batch authentication schemes also hold the traceability. This paper also presents an improvement method on the security problems of the two batch authentication schemes. However, this paper does not give the detailed formal security analysis for both batch improved authentication schemes which will be as the future research work.

ACKNOWLEDGEMENTS

This work was supported by the Key Disciplines of Computer Science and Technology of Shanghai Polytechnic University, the Innovation Program of Shanghai Municipal Education Commission (No.14ZZ167), the Cultivation of Innovative talents-Construction of Curriculum System-Electronic Information (No. A30DB212103-0350), the Collaborative Innovation Platform of Electronic Information Master of Shanghai Polytechnic University, the First Class Undergraduate Specialty “Network Engineering” Construction in Shanghai (No.A30DB212103-0305), the Network Engineering Teaching Funds (No. A01GY21G013-0202).

REFERENCES

Alanazi, F., Shareeda, A., Ozguner, F. (2019). An Efficient Cppa Scheme for Intelligent Transportation Networks. Pervasive and Mobile Computing, 59(8): 1-16.

Bayat, M., Barmshoory, M., Rahimi, M., et al. (2015). A secure authentication scheme for VANETs with batch verification. Wireless Networks, 21(5): 1733–1743.

Cui, J., Tao, X., Zhang, J., et al. (2018). HCPA-GKA: A hash function-based conditional privacy-preserving authentication and group-key agreement scheme for VANETs. Vehicular Communications, 14: 15–25.

Gayathri, N.B., Thumbur, G., Reddy, P., et al. (2018). Efficient pairing-free certificateless authentication scheme with batch verification for vehicular ad-hoc networks. IEEE Access, 6: 31808–31819.

He, D., Zeadally, S., Xu, B., et al. (2015). An efficient identity-based conditional privacy-preserving authentication scheme for vehicular ad hoc networks. IEEE Transactions on Information Forensics and Security, 10(12): 2681–2691.

Horng, S., Tzeng, S., Li, T., et al. (2017). Enhancing security and privacy for identity-based batch verification scheme in VANETs. Vehicular Technology, IEEE Transactions, 66(4): 3235-3248.

Horng, S.J., Tzeng, S.F., Huang, P.H., et al. (2015). An efficient certificateless aggregate signature with conditional privacy-preserving for vehicular sensor networks, Inf. Sci., 317:48-66.

Huang, D., Misra, S., Verma, M. (2011). PACP: An Efficient Pseudonymous Authentication-based Conditional Privacy Protocol for VANETs. IEEE Transactions on Intelligent Transportation Systems, 12(3): 736-746.

Li, J., Lu, F., Guizani, M. (2015). ACPN: A novel authentication framework with conditional privacypreservation and non-repudiation for VANETs. IEEE Transactions on Parallel and Distributed Systems, 26(4): 938–948.

Lin, X., Sun,X., Ho,P., et al. (2007). GSIS: A Secure and Privacy Preserving Protocol for Vehicular Communications. IEEE Trans, 56(6): 3442-3456.

Liu, J., Yuen, T., Au,M., et al.(2014). Improvements on an authentication scheme for vehicular sensor networks. Expert Systems with Applications, 41(5): 2559-2564.

Liu, Z., Xiong, L., Peng, T., et al.(2018). A realistic distributed conditional privacy- preserving authentication scheme for vehicular ad hoc networks. IEEE Access, 6: 26307–26317.

Lo, N.W., Tsai, J.L. (2016). An efficient conditional privacypreserving authentication scheme for vehicular sensor networks without pairings. IEEE Transactions on Intelligent Transportation Systems, 17(5): 1319–1328.

Ma,L., Yang,Q., Lai,J.(2020). A certificateless-based aggregated signature scheme with designated verifier property, Henan Science and Technology, 717(17): 10-12.

Qu, F., Wu,Z., Wang,F., et al.(2015). A security and privacy review of VANETs. IEEE Transactions on Intelligent Transportation Systems, 16(6):2985-2996.

Shim, K.A.(2012). CPAS: An efficient conditional privacy preserving authentication scheme for vehicular sensor networks. IEEE Transactions on Vehicular Technology, 61(4): 1874–1883.

Wang, F., Xu, Y., Zhang, H., et al. (2016). 2FLIP: A two-factor lightweight privacy-preserving authentication scheme for VANET. IEEE Transactions on Vehicular Technology, 65(2): 896–911.

Wang, J., Zhao, M., Chen, Z., et al. (2021). An authentication scheme for conditional privacy preserving based on pseudonym in intelligent transportation. Netinfo Security, 4:49-61.

Xie, Y., Li, X., Zhang, S., et al. (2020). An improved provable secure certificateless aggregation signature scheme for vehicular ad hoc NETworks. Journal of Electronics & Information Technology, 42(5): 1125–1131.

Zeng, P., Guo,R., Ma,Y., et al. (2020). Provable security certificateless authentication scheme for vehicular ad hoc network. Journal of Electronics & Information Technology, 42(12):2873-2881.

Zhang, L., Wang, J., Mu, Y. (2020). Secure and privacy-preserving attribute-based sharing framework in vehicles ad hoc networks. IEEE Access, 8:116781-116795.

Zhang, L., Wu, Q., Dominggo, F., et al. (2017). Distributed aggregate privacy-preserving authentication in VANETs. IEEE Transactions on Intelligent Transportation Systems, 18(3): 516-526.

Zhao, N., Zhang, G., Gu, X. (2020). Certificateless aggregate signature scheme for privacy protection in VANET, Computer Engineering, 46(1): 114-128.

Zhong, H., Wen, J., Cui, J., et al. (2016). Efficient conditional privacy-preserving and authentication scheme for secure service provision in VANET. Tsinghua Science and Technology, 21(6): 620–629.

Zuo, L., Chen, Z., Xia, P., et al.(2019). Improved efficient certificateless short signature scheme, Journal: Computer Science, 46(4):172-176.

Zuo, L., Zhang, M., Hu, K., et al.(2020). Certificateless short signature scheme with double KGC, Application Research of Computers, 137(5): 1482-1487.