Cryptanalysis of One Authentication and Key Agreement Scheme for Internet of Vehicles

Jiahua Zhu and Zhengjun Cao
(Corresponding author: Zhengjun Cao)

Department of Mathematics, Shanghai University
Shangda Raod 99, Shanghai, 200444, China
Email: caozhj@shu.edu.cn

(Received Feb. 26, 2024; Revised and Accepted Mar. 16, 2024; First Online Mar. 24, 2024)

Abstract

The security and privacy of the Internet of Vehicles has become a hot issue. Recently, Yang *et al.* [Future Gener. Comput. Syst., 145, 415-428 (2023)] have designed one authentication and key agreement scheme for the Internet of vehicles. In this note, we show that the scheme has some flaws. (1) There are some inconsistent computations, which should be corrected. (2) The planned route of a target vehicle is almost exposed. The scheme neglects the essential requirement for bit-wise XOR, and tries to encrypt the route by the simple operation. The negligence results in some trivial equalities. (3) The scheme is insecure against impersonation attacks launched by the next roadside unit in the same system.

Keywords: Authentication; Anonymity; Impersonation Attack; Internet of Vehicles; Key Agreement

1 Introduction

The term of internet of vehicles (IoV) is used to describe a network that utilizes sensors, software, and technology to connect vehicles to their relative environment (entities such as traffic management equipments, other vehicles, pedestrians, parking lots, etc) and exchange data. The internet of vehicles is an ideal solution for communication among vehicles.

It improves traffic management applications and services to guarantee safety on roads. A modern car has approximately 100 million lines of software codes. IoV enables such a smart car to access and communicate information with the ecosystem.

The connected vehicles in future will have a large number of connected end-points and a high volume of data exchanged. In the future, any vehicle will have the capability to connect anything at any time in an entirely flexible, reliable and secure way.

In 2021, Bagga *et al.* [2] designed a mutual authentication and key agreement protocol in internet of vehicles-enabled intelligent transportation system. Chattaraj *et al.* [3] put forth a blockchain-assisted certificateless key agreement protocol for internet of vehicles in smart transportation. Kamil and Ogundoyin [6] proposed a certificateless authentication scheme and group key agreement with dynamic updating mechanism for internet of vehicles in smart cities. Wu *et al.* [12] presented a lightweight authenticated key agreement protocol using fog nodes in social internet of vehicles. In 2022, Wang *et al.* [11]

discussed a multiserver authentication and key agreement protocol for internet of vehicles. Thapliyal *et al.* [10] proposed a robust authenticated key agreement protocol for internet of vehicles-envisioned intelligent transportation system. Anggriani *et al.* [1, 4, 9] studied other kinds of authentication and key agreement schemes. Hwang *et al.* [5] designed a new user authentication scheme. Lin and Hsu [7] presented a chaotic maps-based privacy-preserved three-factor authentication scheme for telemedicine systems. Xu [14] proposed a three-party authentication protocol based on Riro for mobile RFID system. Liu *et al.* [8] investigated an improved secure RFID authentication protocol using elliptic curve cryptography. Xie *et al.* [13] investigated a blockchain-based efficient privacy-preserving handover authentication protocol with key agreement for internet of vehicles.

Recently, Yang *et al.* [15] have also presented a key agreement scheme for internet of vehicles. In the considered scenario, there are three entities: OBU, RSU, and TA. OBU is a hardware equipment installed on the vehicle. RSU (roadside unit) is a communication device arranged on both sides of the road or at a specific location. TA is a credible third party, responsible for the registration and management of vehicles in the whole system.

The scheme is designed to meet many security requirements, including authentication, session-key establishment, anonymity, traceability, and resistance to impersonation attack, reply attack, etc. In this note, we show that the scheme cannot be practically implemented due to some flaws.

2 Review of the Yang *et al.*'s Scheme

Let $h() : \{0,1\}^* \rightarrow Z_q^*$ be a hash function. The authority TA picks two large primes P, q and defines an elliptic curve $E : y^2 = x^3 + ax + by \bmod q$. Pick $S \in Z_q^*$ as a private key and set the public key as $Pub_{sys} = S \cdot P$. The private key S is divided into two parts: S_1 and S_2. S_1 is stored in each vehicle's password device, and S_2 is stored in the smart card. Generate S using S_1 and S_2 when the vehicle wants to use the private key S. Select $x_i \in Z_q^*$ as RSU_i's private key and set the public key as $Pub_{RSU_i} = x_i \cdot P$. For each vehicle with the true identity RID_i and the password RPW_i, TA stores $\{RID_i, RPW_i, S_2\}$ into the smart card, and stores x_i into the device RSU_i. Publish the parameters $\{P, q, a, b, Pub_{sys}, Pub_{RSU_i}, h\}$.

The initial authentication and key agreement phase can be depicted below (see Table 1). When a vehicle behaves maliciously, TA can compute $RID_i = h(S \cdot PID_{i,1}) \oplus PID_{i,2}$, to reveal the vehicle's identity.

3 Inconsistent Computations

The scheme uses the basic operators over an elliptic curve. But we find there are some inconsistent computations. For example, it specifies that (see page 418, Ref. [15]):

> *1. TA randomly selects two large primes P, q, and finite fields Z_q^*, elliptic curve: $y^2 = x^3 + ax + by \bmod q$.*
> *2. TA randomly selects $S \in Z_q^*$ as a private key to the system and calculates the public key $Pub_{sys} = S \cdot P$.*

The specification is incorrect because it confuses the basic structure of an elliptic curve and associated elliptic curve groups. It is easy to see that P should be a point belonging to the underlying elliptic curve, *instead of a large prime*. Otherwise, any adversary can recover the master secret key S from the equation $Pub_{sys} = S \cdot P$, where both Pub_{sys} and P are public parameters. To revise, one can specify that:

Table 1: The Yang *et al.*'s scheme for the first road section

$OBU_i : \{S\}$	The first $RSU_i : \{x_i\}$
Insert the smart card.	
Enter RID_i and RPW_i.	
Check RID_i and RPW_i.	
Pick $V_i \in Z_q^*$, compute the anonymous identity $PID_i = \{PID_{i,1}, PID_{i.2}\}$, where $PID_{i,1} = V_i \cdot P$, $PID_{i,2} = RID_i \oplus h(V_i \cdot Pub_{sys})$.	
Invoke the system key S to compute $Sig_i = S \cdot h(PID_i) + V_i \cdot h(m)$ where m is the vehicle's planned route.	
Pick $\alpha_i \in Z_q^*$ to compute $R_1 = h(V_i \cdot Pub_{RSU}^i)$, $L_1 = R_1 \oplus \alpha_i$, $F_1 = h(\alpha_i) \oplus m$.	
Set the timestamp T_v^i and compute $Auth_{PID}^i = h(\alpha_I \| m \| L_1 \| F_1 \| T_V^i)$.	
Send $\{Sig_i, Auth_{PID}^i, T_V^i, PID_i, F_1, L_1\}$ to the first RSU_i.	
$\xrightarrow[\text{[open channel]}]{Sig_i,\ Auth_{PID}^i,\ T_V^i,\ PID_i,\ F_1,\ L_1}$	
	Check the timestamp T_V^i. If so, compute $R_1^* = h(x_i \cdot PID_{i,1})$, $\alpha_i^* = R_1^* \oplus L_1$, $m^* = h(\alpha_i^*) \oplus F_1$, $Auth_{PID}^{i*} = h(\alpha_i^* \| m^* \| L_1 \| F_1 \| T_V^i)$. Check $Auth_{PID}^{i*} = Auth_{PID}^i$, and $Sig_i \cdot P = Pub_{sys} \cdot h(PID_i) + PID_{i,1} \cdot h(m^*)$. If so, select the next RSU_{i+1} and pick $\beta_i \in Z_q^*$, compute $Key = x_i \cdot Pub_{RSU}^{i+1}$, $W_1 = \alpha_i^* \oplus Key$, $Z_1 = R_1^* \oplus \beta_i$, $Session_{key} = h(\alpha_i^* \| \beta_i)$. Set the timestamp T_R^i. Compute $Auth_{RSU}^i = h(W_1 \| Z_1 \| \beta_i \| Key \| T_R^i)$.
	$\xleftarrow{Auth_{RSU}^i,\ T_R^i,\ W_1,\ Z_1}$
Check the timestamp T_R^i. Compute $Key^* = W_1 \oplus \alpha_i$, $\beta_i^* = R_1 \oplus Z_1$, $Auth_{RSU}^{i*} = h(W_1 \| Z_1 \| \beta_i^* \| Key^* \| T_R^i)$. Check $Auth_{RSU}^{i*} = Auth_{RSU}^i$. If so, compute $Session_{key} = h(\alpha_i \| \beta_i^*)$.	

TA randomly selects two large primes p, q, an elliptic curve $y^2 = x^3 + ax + by \bmod p$, and a cyclic additive elliptic curve group G_q of order q, with a generator P.

In this case, the difficulty of retrieving secret key S from equation $Pub_{sys} = S \cdot P$ directly relies on that of elliptic curve discrete logarithm problem (ECDLP), which is a famous intractable problem in cryptography.

4 The Exposure of Planned Route

The Boolean logic operation XOR, denoted by $\oplus$, is widely used in cryptography which compares two input bits and generates one output bit. If the bits are the same, the result is 0. If the bits are different, the result is 1. When the operator is performed on two strings, they must be of a same bit-length. Otherwise, the shorter string should be stretched by padding some 0s to its left side. In this case, the partial string corresponding to the padding bits is directly copied into the final string.

In the Yang *et al.*'s scheme, a target vehicle's planned route is expressed as m. To protect the route, the scheme adopts the below mechanism

$$R_1 = h(V_i \cdot Pub^i_{RSU}), \quad L_1 = R_1 \oplus \alpha_i, \quad \text{[Encryption]} \quad F_1 = h(\alpha_i) \oplus m,$$
$$R^*_1 = h(x_i \cdot PID_{i,1}), \quad \alpha^*_i = R^*_1 \oplus L_1, \quad \text{[Decryption]} \quad m^* = h(\alpha^*_i) \oplus F_1$$

due to that

$$V_i \cdot Pub^i_{RSU} = V_i(x_i \cdot P) = x_i(V_i \cdot P) = x_i \cdot PID_{i,1}$$

But we find the simple operation bit-wise XOR is insufficient to encrypt the route m, because the hash value $h(\alpha_i)$, practically 256 bits or 512 bits, is too short to mask the other operand m. Generally, the bit-length of route m is far greater than 512, i.e., BitLength(m)$>$ 512 (the route information contains more than 64 ASCII symbols). Hence, we have

$$F_1 = (00\cdots0 \| \underbrace{h(\alpha_i)}_{512-\text{bits}}) \oplus m$$

which means the route m is almost exposed, once the adversary captures the transferred parameter F_1 via the open channel. The scheme has neglected the basic requirement for bit-wise XOR operator and presented a trivial encryption. To revise, one should adopt other encryption mechanism such as block cipher, stream cipher, etc.

5 Insecure Against Impersonation Attack

As we see, the agreed key is set as $Session_{key} = h(\alpha_i \| \beta_i)$, where α_i, β_i are picked by the OBU_i and the first RSU_i, respectively. To carry forward the planned route, the RSU_i should choose the next roadside unite RSU_{i+1} and invoke its public key Pub^{i+1}_{RSU}. But we find it adopts a very simple secret-key invoking mechanism, i.e.,

$$Key = x_i \cdot Pub^{i+1}_{RSU} = x_i(x_{i+1} \cdot P) = x_{i+1}(x_i \cdot P) = x_{i+1}Pub^i_{RSU}$$

which means the corrupted roadside unit RSU_{i+1} who knows the secret key x_{i+1}, can obtain the parameter Key by invoking the public key Pub^i_{RSU}. The corrupted unit then uses the captured data

$$\{Sig_i, Auth^i_{PID}, T^i_V, PID_i, F_1, L_1; Auth^i_{RSU}, \ T^i_R, \ W_1, \ Z_1\}$$

via open channels, to compute

$$\alpha_i = W_1 \oplus Key, \quad R_1 = \alpha_i \oplus L_1, \quad \beta_i = R_1 \oplus Z_1$$

With the retrieved nonce α_i and β_i, the corrupted roadside unit can compute the session key $Session_{key} = h(\alpha_i \| \beta_i)$. Using this key, the corrupted unit can impersonate the target unit in the upcoming session. Thus, the scheme is insecure against impersonation attack launched by the next roadside unit.

6 Conclusion

We show that the Yang *et al.*'s authentication and key agreement scheme is flawed. It seems difficult to revise the scheme because of its misused encryption and simple secret-key invoking mechanism. The findings in this note will be helpful for the future work on designing such authentication and key agreement schemes.

Acknowledgements

We are grateful to the reviewers for their valuable suggestions.

References

[1] K. Anggriani, N. Wu, and M. S. Hwang, "Research on data hiding schemes for AMBTC compressed images," *International Journal of Network Security*, vol. 24, no. 6, pp. 1114–1123, 2022.

[2] P. Bagga, A. K. Das, M. Wazid, J. J. P. C. Rodrigues, K. K. R. Choo, and Y. H. Park, "On the design of mutual authentication and key agreement protocol in internet of vehicles-enabled intelligent transportation system," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 2, pp. 1736–1751, 2021.

[3] D. Chattaraj, B. Bera, A. K. Das, S. Saha, P. Lorenz, and Y. H. Park, "Block-clap: Blockchain-assisted certificateless key agreement protocol for internet of vehicles in smart transportation," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 8, pp. 8092–8107, 2021.

[4] M. S. Hwang, S. T. Hsu, and C. Y. Yang, "A new secure channel free public key encryption with keyword search scheme based on ElGamal cryptosystems," *International Journal of Network Security*, vol. 25, no. 6, pp. 1070–1076, 2023.

[5] M. S. Hwang, H. W. Li, and C. Y. Yang, "An improved of enhancements of a user authentication scheme," *International Journal of Network Security*, vol. 25, no. 3, pp. 508–514, 2023.

[6] I. A. Kamil and S. O. Ogundoyin, "A lightweight certificateless authentication scheme and group key agreement with dynamic updating mechanism for lte-v-based internet of vehicles in smart cities," *Journal of Information Security and Applications*, vol. 63, p. 102994, 2021.

[7] T. W. Lin and C. L. Hsu, "Chaotic maps-based privacy-preserved three-factor authentication scheme for telemedicine systems," *International Journal of Network Security*, vol. 25, no. 2, pp. 194–200, 2023.

[8] W. R. Liu, Z. Y. Ji, and C. C. Chu, "An improved secure RFID authentication protocol using elliptic curve cryptography," *International Journal of Network Security*, vol. 26, no. 1, pp. 106–115, 2024.

[9] Y. C. Lu and M. S. Hwang, "A cryptographic key generation scheme without a trusted third party for access control in multilevel wireless sensor networks," *International Journal of Network Security*, vol. 24, no. 5, pp. 959–964, 2022.

[10] S. Thapliyal, M. Wazid, D. P. Singh, A. K. Das, and S. H. Islam, "Robust authenticated key agreement protocol for internet of vehicles-envisioned intelligent transportation system," *Journal of Systems Architecture*, vol. 142, p. 102937, 2023.
[11] J. Wang, L. Wu, H. Wang, K. K. R. Choo, L. Wang, and D. He, "A secure and efficient multiserver authentication and key agreement protocol for internet of vehicles," *IEEE Internet of Things Journal*, vol. 9, no. 23, pp. 24398–24416, 2022.
[12] T. Y. Wu, X. Guo, L. Yang, Q. Meng, and C. M. Chen, "A lightweight authenticated key agreement protocol using fog nodes in social internet of vehicles," *Mobile Information Systems*, vol. 2021, pp. 3277113:1–3277113:14, 2021.
[13] X. Xie, B. Wu, and B. Hou, "BEPHAP: A blockchain-based efficient privacy-preserving handover authentication protocol with key agreement for internet of vehicles," *Journal of Systems Architecture*, vol. 138, p. 102869, 2023.
[14] S. H. Xu, "Three-party authentication protocol based on Riro for mobile RFID system," *International Journal of Network Security*, vol. 26, no. 1, pp. 1–9, 2024.
[15] Q. Yang, X. Zhu, X. Wang, J. Fu, J. Zheng, and Y. Liu, "A novel authentication and key agreement scheme for internet of vehicles," *Future Generation Computer Systems*, vol. 145, pp. 415–428, 2023.

Biography

Jiahua Zhu is currently pursuing his master degree from Department of Mathematics, Shanghai University. His research interests include information theory and cryptography.

Zhengjun Cao is an associate professor with Department of Mathematics, Shanghai University, Shanghai, China. He received his PhD degree from Academy of Mathematics and Systems Science, Chinese Academy of Sciences, Beijing, China. He had been serving as a post-doctor with Computer Sciences Department, Universite Libre de Bruxelles, Belgium. His research interests include information security, cryptography, and computational complexity. He has published over 80 papers in different journals and conference proceedings, including: Information & Computation, IEEE Transactions on Parallel & Distributed System, IEEE Transactions on Cloud Computing, IEEE Transactions on Big Data, IEEE Transactions on Dependable & Secure Computing, IEEE Systems Journal, Quantum Information Processing, International Journal of Quantum Information, International Journal of Computer Mathematics, International Journal of Bifurcation & Chaos, International Journal of Information & Computer Security, International Journal of Network Security, Sciences in China, Wireless Personal Communications, Telecommunication Systems, Journal of Approximation Theory.