On the security of one certificateless aggregate signature scheme with dynamic revocation in vehicular ad-hoc networks

Zhengjun Cao, Lihua Liu

Abstract. We show that the certificateless signature scheme [Veh. Commun. 47: 100763 (2024)] is insecure, because an adversary can launch forgery attack for any message. The signer's certificateless public key is not tightly bound to the system public key. The inherent flaw results in that the adversary can find an efficient signing algorithm functionally equivalent to the valid signing algorithm. The findings in this note could be helpful for newcomers who are not familiar with the designing techniques for certificateless signatures.
Keywords: Certificateless signature, forgery attack, signing algorithm, verification algorithm.

1 Introduction

Certificateless public key cryptography introduced by Al-Riyami and Paterson [1], does not require the use of certificates to guarantee the authenticity of signer's public key. But the system parameters must be authentic. Chen et al. [3] investigated the structural extensions of security models for certificateless signatures. Sa et al. [10] proposed a certificateless aggregate signature from bilinear maps. Gayathri et al. [4] designed a pairing-free certificateless aggregate signature scheme for healthcare wireless medical sensor networks. Hashimoto and Ogata [7] presented a unrestricted and compact certificateless aggregate signature scheme. Wu et al. [12] discussed a certificateless aggregate signature scheme secure against fully chosen-key attacks. Gowri et al. [5] studied a certificateless aggregate signature based authentication scheme for Vehicular Ad Hoc Networks (VANET). Cahyadi et al. [2] investigated a certificateless aggregate signature scheme for security and privacy protection in VANET. Tomar et al. [11] presented a blockchain based certificateless aggregate signature scheme for fog enabled smart grid environment. Iqbal et al. [8] also proposed a certificateless aggregate signature scheme for VANET. Kabil et al. [9] designed a certificateless aggregate signature scheme with Chameleon hashing based identity authentication for VANET.

Very recently, Guo et al. [6] have proposed a certificateless aggregate signature scheme with dynamic revocation in VANET. Though the scheme is interesting, we find it is insecure. An adversary can find an efficient signing algorithm functionally equivalent to the valid signing algorithm, even though he cannot compute the private key information of any signer.

Z. Cao, Department of Mathematics, Shanghai University, Shanghai, 200444, China.
L. Liu, Department of Mathematics, Shanghai Maritime University, Shanghai, 201306, China.
Email: liulh@shmtu.edu.cn

Table 1: The Guo et al.'s certificateless signature scheme

System initialization. KGC chooses the additive group G with prime order q, and a generator P. Pick $k \in Z_q^*$ as its main private key, and compute $K_{pub} = kP$ as its main public key. Choose hash functions: $H_1 : G^2 \times \{0,1\}^* \to Z + q^*$, $H_2 : \{0,1\}^{*2} \times G^2 \to Z_q^*$, $H_3 : \{0,1\}^{*4} \times G \to Z_q^*$.
TA picks $r \in Z_q^*$ as its main private key, to compute $T_{pub} = rP$ as its main public key.
KGC publishes the parameters $params = \{q, G, P, T_{pub}, K_{pub}, H_1, H_2, H_3\}$.
Partial private key generationn. For the vehicle V_i with the real identity RID_i, TA picks $\alpha_i \in Z_q^*$ to compute $NID_{i,1} = \alpha_i P$, $L_i = \alpha_i T_{pub}$, $NID_{i,2} = RID_i \oplus H_1(rNID_{i,1}, L_i, T_i)$, where T_i is the validity period for the pseudo identity. Send $FID_i = (NID_{i,1}, NID_{i,2}, T_i)$ to KGC and V_i.
KGC checks the validity period. Then pick $n_i \in Z_q^*$ to compute $N_i = n_i P$, $h_{2i} = H_2(FID_i, K_{pub}, N_i, T_i)$, $ppk_i = n_i + kh_{2i} \bmod q$. Send (ppk_i, FID_i, N_i) to V_i via a secure channel.
Vehicle key generation. V_i computes $h_{2i} = H_2(FID_i, K_{pub}, N_i, T_i)$ and checks if $ppk_i P = N_i + h_{2i} K_{pub}$. Pick $s_i \in Z_q^*$ to compute $S_i = s_i P$, $U_i = h_{2i} S_i + N_i$, and the private key $SK_i = ppk_i + h_{2i} s_i \bmod q$. Set its certificateless public key as $PK_i = (U_i, N_i)$.
Personal signature generation. Let t_i be the current timestamp, ∇ be the current status information, m_i be the message to be signed. V_i picks $b_i \in Z_q^*$ to compute $h_{3i} = H_3(m_i, FID_i, PK_i, \nabla, t_i)$, $B_i = b_i P$, $Y_i = b_i + h_{3i} SK_i \bmod q$. Generate the signature $\delta_i = (B_i, Y_i)$. Broadcast $mt = \{FID_i, m_i, \delta_i, t_i\}$.
Personal signature verification. Check the validity of t_i and FID_i. If true, then compute $h_{2i} = H_2(FID_i, K_{pub}, N_i, T_i)$, $h_{3i} = H_3(m_i, FID_i, PK_i, \nabla, t_i)$, and check that $Y_i P = B_i + h_{3i}(U_i + h_{2i} K_{pub})$. If true, accept the signature. Otherwise, reject it.
Aggregate signature generation, Aggregate signature verification, Invalid signature tracking, and Malicious vehicle revocation. See pages 6, Ref.[6].

2 Review of Guo et al.'s signature scheme

In the considered scenario, there are five entities: Trusted Authority (TA) with a Tracking Authority (TRA), Transportable Roadside Unit (RSU), Key Generation Center (KGC), Application Server (AS), and Vehicles equipped with Tamper-Proof Devices (TPD). The involved notations and their descriptions are listed below (see Table 2).

Table 2: Symbols and descriptions

symbol	description
P	generator of G with prime order q
H_1, H_2, H_3	hash functions
V_i	i-th vehicle
T_{pub}, r	public/private key pair of TA
K_{pub}, k	public/private key pair of KGC
RID_i, FID_i	real/pseudo identity of V_i
PK_i, SK_i	public/private key pair of V_i
ppk_i	partial private key of V_i
VP_i, t_i	validity period and timestamp
(m_i, δ_i)	the pair of message and signature

The scheme consists of nine phases: System initialization, Partial private key generation, Vehicle key generation, Personal signature generation, Personal signature verification, Aggregate signature generation, Aggregate signature verification, Invalid signature tracking, and Malicious vehicle revocation. It can be restated as below (Table 1).

The security model considers two types of attackers. Attacker $\mathcal{A}_1$ can replace the public key of any vehicle, but cannot obtain the system master key or partial private key. Attacker $\mathcal{A}_2$ can obtain the system's master key and generate part of the user's private key, but cannot replace the public key of any vehicle.

3 Analysis of the Guo et al.'s scheme

3.1 Some typos

The definition of hash function H_2 is inconsistent (see Fig.1).

3) KGC choose three hash functions: $H_1 : G^2 \times \{0,1\}^* \to Z_q^*$, $H_2 : \{0,1\}^{*2} \times G^2 \to Z_q^*$, $H_3 : \{0,1\}^{*4} \times G \to Z_q^*$.

2) V_i selects a random number $s_i \in Z_q^*$ as the secret value and computes $S_i = s_i P$, $H_2 : \{0,1\}^* \times G \times G \times \{0,1\}^* \to Z_q^*$, $U_i = h_{2i} S_i + N_i$. Then, the private key of V_i is $SK_i = ppk_i + h_{2i} S_i$ and its corresponding public key is $PK_i = (U_i, N_i)$.

Figure 1: Some typos

The following equation

$$SK_i = ppk_i + h_{2i} S_i \tag{1}$$

should be corrected as

$$SK_i = ppk_i + h_{2i} s_i \bmod q \tag{1'}$$

because $ppk_i = n_i + kh_{2i} \in Z_q^*$, $h_{2i}S_i = h_{2i}s_iP \in G$. It has confused two different groups.

3.2 Insecure against forgery attack

Given the signer's certificateless public key $PK_i = (U_i, N_i)$ and the signature (B_i, Y_i), the verification equation is eventually expressed as

$$Y_iP = B_i + H_3(m_i, FID_i, PK_i, \nabla, t_i) \cdot (N_i + H_2(FID_i, K_{pub}, N_i, T_i)K_{pub})$$

We find the signature scheme is insecure against forgery attack. An adversary can generate valid signatures for any message.

Given a message $\hat{m}_i$ and the target signer's pseudo identity FID_i and the public key $PK_i = (U_i, N_i)$, the adversary picks $\theta \in Z_q^*$ and computes

$$\begin{aligned} Y_i = \theta, \quad B_i = & Y_iP - H_3(\hat{m}_i, FID_i, PK_i, \nabla, t_i) \\ & \cdot (N_i + H_2(FID_i, K_{pub}, N_i, T_i)K_{pub}), \end{aligned}$$

where $P \in G, K_{pub}$ are system public parameters and accessible to any adversary. Apparently, the forged signature can pass the verification equation.

The drawback is due to that the component B_i of signature is simply used for the verification, not truly bound to the target message and any entity's public key.

By the way, the security proof (see page 8, Ref.[6]) is flawed because in the signature query process it falsely specifies the dependency

$$Y_i = x, \quad B_i = (x - y - z)P.$$

It doesn't consider the above forgery attack.

3.3 Further discussions

In certificateless public key cryptogrphy, the signer's public key should be tightly bound to the system public key. One can check the dependency so as to confirm that the signer's public key is really unreplaced by any adversary. But Guo et al. [6] have forgotten the necessary requirement. It has not specified any mechanism to check the necessary dependency. Actually, in the original presentation, the explicit dependency between the signer's certificateless public key and secret key is not properly used to construct any intractable problem, such as Elliptic Curve Discrete Logarithm (ECDL), Computational Diffie-Hellman (CDH), and Decisional Diffie-Hellman (DDH).

To fix the scheme, we refer to the certificateless signature schemes [3] for techniques to clarify the mechanism for authenticating the signer's public key and the signature concurrently, especially, the technique of using hash functions to create the explicit dependency between the public key and the resulting signature.

4 Conclusion

We show that the Guo et al.'s certificateless signature scheme is insecure against forgery attack, because an adversary can find an efficient signing algorithm functionally equivalent to the valid signing algorithm. We hope the findings in this note could be helpful for the future work on designing such schemes.

References

[1] S. Al-Riyami and K. G. Paterson. Certificateless public key cryptography. In Chi-Sung Laih, editor, *Proc. ASIACRYPT'03*, volume 2894 of *Lecture Notes in Computer Science*, pages 452–473, Heidelberg, 2003. Springer.

[2] E. F. Cahyadi, T. Su, C. C. Yang, and M. S. Hwang. A certificateless aggregate signature scheme for security and privacy protection in VANET. *Int. J. Distributed Sens. Networks*, 18(5):155013292210806, 2022.

[3] Y. C. Chen, R. Tso, W. Susilo, X. Huang, and G. Horng. Certificateless signatures: Structural extensions of security models and new provably secure schemes. Cryptology ePrint Archive, Paper 2013/193, 2013.

[4] N. B. Gayathri, T. Gowri, P. R. Kumar, M. Z. U. Rahman, P. V. R., and A. Lay-Ekuakille. Efficient and secure pairing-free certificateless aggregate signature scheme for healthcare wireless medical sensor networks. *IEEE Internet Things J.*, 6(5):9064–9075, 2019.

[5] T. Gowri, G. S. Rao, P. V. Reddy, N. B. Gayathri, D. V. R. K. Reddy, and M. Padmavathamma. Efficient and secure certificateless aggregate signature-based authentication scheme for vehicular ad hoc networks. *IEEE Internet Things J.*, 8(3):1908–1920, 2021.

[6] R. Guo, R. Dong, X. Li, Y. Zhang, and D. Zheng. DRCLAS: an efficient certificateless aggregate signature scheme with dynamic revocation in vehicular ad-hoc networks. *Veh. Commun.*, 47:100763, 2024.

[7] K. Hashimoto and W. Ogata. Unrestricted and compact certificateless aggregate signature scheme. *Inf. Sci.*, 487:97–114, 2019.

[8] A. Iqbal, M. Zubair, M. Asghar Khan, I. Ullah, G. U. Rehman, A. V. Shvetsov, and F.l Noor. An efficient and secure certificateless aggregate signature scheme for vehicular ad hoc networks. *Future Internet*, 15(8):266, 2023.

[9] A. Kabil, H. Aslan, M. A. A., and M. Rasslan. CHAM-CLAS: A certificateless aggregate signature scheme with chameleon hashing-based identity authentication for vanets. *Cryptogr.*, 8(3):43, 2024.

[10] P. K. Sa, V. Sharma, G. Sharma, and T. Bhatia. An efficient and secure certificateless aggregate signature from bilinear maps. *Int. J. Inf. Secur. Priv.*, 13(4):89–108, 2019.

[11] A. Tomar, S. Tripathi, and K. Arivarasan. A blockchain-based certificateless aggregate signature scheme for fog-enabled smart grid environment. *IEEE Trans. Green Commun. Netw.*, 7(4):1892–1905, 2023.

[12] G. Wu, F. Zhang, L. Shen, F. Guo, and W. Susilo. Certificateless aggregate signature scheme secure against fully chosen-key attacks. *Inf. Sci.*, 514:288–301, 2020.