Cryptanalysis and improvement of certificateless aggregate signature with conditional privacy-preserving for vehicular sensor networks ⋆

Jiguo Li, Hong Yuan and Yichen Zhang

College of Computer and Information Engineering
Hohai University, Nanjing, China
lijiguo@hhu.edu.cn

Abstract. Secure aggregate signature schemes have attracted more concern due to their wide application in resource constrained environment. Recently, Horng et al. [S. J. Horng et al., An efficient certificateless aggregate signature with conditional privacy-preserving for vehicular sensor networks, Information Sciences 317 (2015) 48-66] proposed an efficient certificateless aggregate signature with conditional privacy-preserving for vehicular sensor networks. They claimed that their scheme was provably secure against existential forgery on adaptively chosen message attack in the random oracle model. In this paper, we show that their scheme is insecure against a malicious-but-passive KGC under existing security model. Further, we propose an improved certificateless aggregate signature.

1 Introduction

In traditional public key cryptography (PKC), each user generates a public/private key pair independently and then sends the public key to a trusted certificate authority (CA) to request a certificate. Therefore, it is facing many challenges for certificate management, including revocation, storage and distribution and the computational cost of certificate verification. Identity-based cryptography (IBC) [1] can solve certificate management problem in PKC. However, IBC suffers from inherent key escrow problem. In Asiacrypt 2003, Al-Riyami and Paterson proposed a new paradigm called certificateless public key cryptography (CL-PKC)

⋆ The authors would like to thank anonymous reviewers for their helpful comments and valuable suggestions. This research was supported by the National Natural Science Foundation of China (61272542), the Project Funded by the Priority Academic Program Development of Jiangsu Higher Education Institutions, the Fundamental Research Funds for the Central Universities (2016B10114), Jiangsu Collaborative Innovation Center on Atmospheric Environment and Equipment Technology, and the Project of Scientific Research Innovation for College Graduate Student of Jiangsu Province (KYZZ15_0151).

[2]. CL-PKC also needs a trusted third party which is called key generation center (KGC). The KGC only generates a user's partial private key, a user computes his full private key by combining his partial private key and a secret key chosen by himself, thus the key escrow problem in IBC can be overcome through this way. CL-PKC has attracted significant research attention [3-15], since it was first introduced by Al-Riyami and Paterson in 2003. As defined in [2], there exists two different types of adversaries in CL-PKC. The Type I adversary simulates an outsider attacker, who can compromise users secret value or replace user public key, but neither compromise master secret key nor get access to partial private key. At present, CL-PKC mainly suffers from two kinds of attacks, that is, public key replacement attack and malicious-but-passive-KGC attacks. For the type I adversary, Huang *et al.* [3] and Li *et al.* [4] showed the certificateless signature schemes in [2,5] were insecure against public key replacement attacks. Furthermore, they presented two improved certificateless signature schemes. The type II adversary simulates an honest-but-curious KGC who always generates the master secret key and the system parameters honestly in complete accordance with the scheme specification, but cannot compromise users secret value nor replace any public key. In the real world, a KGC may be dishonest and malicious at the very beginning of the setup stage in the system and may not follow the scheme specification for setting up the system. This means that a KGC may maliciously implant a trapdoor in the public system parameters and then attempt to forge user signature without private key of the user. For the Type II adversaries, Au *et al.* [6] presented a enhanced security model, where a malicious KGC called malicious-but-passive KGC is allowed to generate the key pair in any way. Some certificateless signature and encryption schemes [7,8,9,10] have been shown to suffer from the malicious-but-passive KGC attack.

There are so many practical applications which requires signatures for many distinct messages generated by many distinct users. For example, in the Vehicular Ad hoc networks (VANETs) [16,17,18], the large scale and number of nodes in VANETs need to authenticate each other. Each node in VANETs needs to verify vast messages in a high-density traffic scenario, which leads to a high computation burden to the receivers. In order to solve above problem, Boneh *et al.* [19] first proposed the concept for aggregate signature in Eurocrypt 2003. The aggregate signature can combine n signatures with respect to n messages from n users into a single short signature. The validity for aggregate signature is guaranteed by verifying that each signature involved in the aggregation is valid. By this means, aggregate signature greatly reduces the computation and communication overhead. This feature makes aggregate signature very helpful especially in environments with limited bandwidth and power-constrained devices, such as wireless sensor network. Due to advantage in CL-PKC, Castro and Dahab [20] introduced the concept for certificateless aggregate signature (CLAS). In 2009, Zhang and Zhang [16] refined the notion and security model for CLAS. Further,they presented an efficient CLAS scheme, which is secure against adaptive chosen-message attacks under the computational Diffie-Hellman assumption. Since then, CLAS schemes [16-27] have attracted much attention.

The researchers in [21,22,23,25] showed that two CLAS schemes [26,27] were insecure against the malicious-but-passive KGC attack. Recently, Horng *et al.* [18] provided a new certificateless signature scheme and an efficient CLAS scheme with conditional privacy-preserving for vehicular sensor networks. They claimed that their scheme was provably secure against existential forgery on adaptively chosen message attack in the random oracle model. In this article, we show that their CLAS scheme [18] is also vulnerable to malicious-but-passive KGC attack.

2 Review of Horng et al.s certificateless aggregate signature scheme

In order to facilitate analysis, we follow the notations from [18]. CLAS scheme for Horng *et al.* includes the following algorithms:

Setup: Given a security parameter l, the algorithm works as follows:

- Let $\mathbb{G}_1$ be an additive cyclic group and $\mathbb{G}_2$ be a multiplicative cyclic group with prime order q. $P, Q \in \mathbb{G}_1$ are two different generators. $e : \mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_2$ is a bilinear map.
- The KGC randomly selects $\alpha \in \mathbb{Z}_q^*$ as a master secret key and computes $P_{Pub} = \alpha P$ as a master public key.
- The TRA randomly selects $\beta \in \mathbb{Z}_q^*$ as a master secret key for traceability and computes $T_{Pub} = \beta P$ as a master public key.
- They choose two cryptographic hash functions $H_1 : \{0,1\}^* \to \mathbb{G}_1$, $H_2 : \{0,1\}^* \to \mathbb{Z}_q^*$.

The system parameters are $Params =< q, \mathbb{G}_1, \mathbb{G}_2, e, P, Q, P_{Pub}, T_{Pub}, H_1, H_2 >$, which are preloaded in the tamper-proof devices for all vehicles. α and β are the master secret keys.

Pseudo Identity Generation/Partial Private Key Extraction:

- The vehicle V_i randomly selects $k_i \in \mathbb{Z}_q^*$, computes $ID_{i,1} = k_i P$ and sends $(RID_i, ID_{i,1})$ to the TRA by a secure way, where the RID_i uniquely recognizes the vehicle V_i.
- After RID_i is verified, the TRA computes$ID_{i,2} = RID_i \oplus H(\beta \cdot ID_{i,1}, T_i)$, where β is the master secret for the TRA, T_i is the valid period of the pseudo identity. TRA sends pseudo identity $ID_i = (ID_{i,1}, ID_{i,2}, T_i)$ to the KGC by a secure channel.
- Given pseudo identity ID_i, the KGC computes $Q_{ID_i} = H(ID_i)$ and the partial private key $psk_{ID_i} = \alpha \cdot Q_{ID_i}$, where α is the master secret for the KGC. The KGC sends (ID_i, psk_{ID_i}) to the vehicle via a secure channel.

Vehicle Key Generation: The vehicle V_i randomly selects $x_{ID_i} \in \mathbb{Z}_q^*$ as secret key vsk_{ID_i}, and computes $vpk_{ID_i} = x_{ID_i} P$ as public key.

Sign: Given pseudo identity ID_i, message M_i, the signature key (vsk_{ID_i}, psk_{ID_i}), the algorithm works as follows:

- The vehicle V_i randomly selects $r_i \in \mathbb{Z}_q^*$, and computes $R_i = r_i P$.
- V_i computes $h_i = H_2(M_i, ID_i, vpk_{ID_i}, R_i, t_i)$ and $S_i = psk_{ID_i} + (vsk_{ID_i} + h_i \cdot r_i)Q$, where t_i is current timestamp. Then $\sigma_i = (R_i, S_i)$ is a certificateless signature.

- Finally, V_i sends $(ID_i, vpk_{ID_i}, M_i, t_i, \sigma_i)$ to a nearby RSU.

Individual Verify: Once the RSU receives a certificateless signature $\sigma_i = (R_i, S_i)$ from V_i, the RSU computes $Q_{ID_i} = H(ID_i)$, $h_i = H_2(M_i, ID_i, vpk_{ID_i}, R_i, t_i)$ and checks whether the following verification equation $e(S_i, P) = e(Q_{ID_i}, P_{Pub})$ $e(vpk_{ID_i} + h_i \cdot R_i, Q)$ holds. If not, then rejects the signature else accepts it.

Aggregate: When receiving message-signature pairs $(M_1, t_1, \sigma_1 = (R_1, S_1), \cdots, M_n, t_n, \sigma_n = (R_n, S_n))$ from $V_i, i = 1, \cdots, n$ respectively, the RSU computes $S = \sum_{i=1}^{n} S_i$ and outputs $\sigma = (R_1, R_2, \cdots, R_n, S)$ as a CLAS.

Aggregate Verify: Once the application server receives a CLAS $\sigma = (R_1, R_2, \cdots, R_n, S)$, computes $Q_{ID_i} = H(ID_i)$, $h_i = H_2(M_i, ID_i, vpk_{ID_i}, R_i, t_i)$ for $i = 1, \cdots, n$ and checks whether the following verification equation $e(S, P) = e(\sum_{i=1}^{n} Q_{ID_i}, P_{Pub})$ $e(\sum_{i=1}^{n}(vpk_{ID_i} + h_i \cdot R_i), Q)$ holds. If not, then rejects the CLAS, else accepts it.

3 Cryptanalysis for Horng et al.s CLAS scheme

We suppose that the adversary A is malicious-but-passive KGC. A performs the malicious-but-passive KGC attack by the following 3 steps:

Step1: A implants a trapdoor in the setup algorithm, that is, A randomly selects $u \in \mathbb{Z}_q^*$ and computes $Q = u \cdot P$ as a malicious parameter. The other system parameters are generated normally. $Params =< q, \mathbb{G}_1, \mathbb{G}_2, e, P, Q, P_{Pub}, T_{Pub}, H_1, H_2 >$ are published as the system parameters.

Step2: A forges basic signature for any vehicle V_i without using its secret key. The adversary A works as follows.

- Since A is malicious-but-passive KGC, A knows the master secret key α. A can compute $Q_{ID_i} = H(ID_i)$ and the partial private key $psk_{ID_i} = \alpha \cdot Q_{ID_i}$.
- A randomly selects $r_i \in \mathbb{Z}_q^*$, and computes $R_i^* = r_i P$.
- A computes $h_i = H_2(M_i, ID_i, vpk_{ID_i}, R_i^*, t_i)$ and $S_i^* = psk_{ID_i} + u \cdot vpk_{ID_i} + u \cdot h_i \cdot R_i^*$, where u is trapdoor for A.

$\sigma_i^* = (R_i^*, S_i^*)$ is a valid certificateless signature because it satisfies verification equation.

$$
\begin{aligned}
e(S_i^*, P) &= e(psk_{ID_i} + u \cdot vpk_{ID_i} + u \cdot h_i \cdot R_i^*, P) \\
&= e(psk_{ID_i} + vsk_{ID_i} \cdot uP + h_i \cdot r_i \cdot uP, P) \\
&= e(psk_{ID_i} + (vsk_{ID_i} + h_i \cdot r_i)Q, P) \\
&= e(Q_{ID_i}, P_{Pub})\ e(vpk_{ID_i} + h_i \cdot R_i^*, Q)
\end{aligned}
$$

Step3: A forges CLAS scheme. The adversary A first forges message-signature pairs $(M_1, t_1, \sigma_1^* = (R_1^*, S_1^*), \cdots, M_n, t_n, \sigma_n^* = (R_n^*, S_n^*))$ for $V_i, i = 1, \cdots, n$. Then, A computes $S^* = \sum_{i=1}^{n} S_i^*$. $\sigma^* = (R_1^*, R_2^*, \cdots, R_n^*, S^*)$ is a valid CLAS scheme, because it satisfies the following verification equation.

$$e(S^*, P) = e(\sum_{i=1}^{n} Q_{ID_i}, P_{Pub})\ e(\sum_{i=1}^{n}(vpk_{ID_i} + h_i \cdot R_i^*), Q)$$

4 Improvement for Horng et al.s CLAS scheme

In our attack, malicious-but-passive KGC can modify the relation between the generators $P, Q \in \mathbb{G}_1$ at the very beginning of the setup stage in the system.

Thus, KGC may maliciously implant a trapdoor in the public system parameters and attempt to forge basic certificateless signature and certificateless aggregate signature without private key of the user. In order to withstand this attack, we destroy this relation between the generators $P, Q \in \mathbb{G}_1$, which can be utilized by KGC by deleting generator $Q \in \mathbb{G}_1$ in the setup stage of improved scheme. In the sign stage of improved scheme, the vehicle V_i computes hash value to replace the generator $Q \in \mathbb{G}_1$ for original scheme. Based on CLAS scheme for Horng *et al.*, we present an improved scheme as follows.

Setup: Given a security parameter l, the algorithm works as follows:

- Let $\mathbb{G}_1$ be an additive cyclic group and $\mathbb{G}_2$ be a multiplicative cyclic group with prime order q. P is generator for group $\mathbb{G}_1$. $e : \mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_2$ is a bilinear map.

- The KGC randomly selects $\alpha \in \mathbb{Z}_q^*$ as a master secret key and computes $P_{Pub} = \alpha P$ as a master public key.

- The TRA randomly selects $\beta \in \mathbb{Z}_q^*$ as a master secret key for traceability and computes $T_{Pub} = \beta P$ as a master public key.

-They choose two cryptographic hash functions $H_1 : \{0,1\}^* \to \mathbb{G}_1$, $H_2 : \{0,1\}^* \to \mathbb{Z}_q^*$.

The system parameters are $Params =< q, \mathbb{G}_1, \mathbb{G}_2, e, P, P_{Pub}, T_{Pub}, H_1, H_2 >$, which are preloaded in the tamper-proof devices for all vehicles. α and β are the master secret keys.

Pseudo Identity Generation/Partial Private Key Extraction:

- The vehicle V_i randomly selects $k_i \in \mathbb{Z}_q^*$, computes $ID_{i,1} = k_i P$ and sends $(RID_i, ID_{i,1})$ to the TRA by a secure way, where the RID_i uniquely recognizes the vehicle V_i.

- After RID_i is verified, the TRA computes $ID_{i,2} = RID_i \oplus H_2(\beta \cdot ID_{i,1}, T_i)$, where β is the master secret for the TRA, T_i is the valid period of the pseudo identity. TRA sends pseudo identity $ID_i = (ID_{i,1}, ID_{i,2}, T_i)$ to the KGC by a secure channel.

- Given pseudo identity ID_i, the KGC computes $Q_{ID_i} = H_1(ID_i)$ and the partial private key $psk_{ID_i} = \alpha \cdot Q_{ID_i}$, where α is the master secret for the KGC. The KGC sends (ID_i, psk_{ID_i}) to the vehicle via a secure channel.

Vehicle Key Generation: The vehicle V_i randomly selects $x_{ID_i} \in \mathbb{Z}_q^*$ as secret key vsk_{ID_i}, and computes $vpk_{ID_i} = x_{ID_i} P$ as public key.

Sign: Given pseudo identity ID_i, message M_i, the signature key (vsk_{ID_i}, psk_{ID_i}), the algorithm works as follows:

- The vehicle V_i randomly selects $r_i \in \mathbb{Z}_q^*$, and computes $R_i = r_i P$.

- V_i computes $h_i = H_2(M_i, ID_i, vpk_{ID_i}, R_i, t_i)$, $Q = H_1(q, P, P_{Pub}, T_{Pub})$ and $S_i = psk_{ID_i} + (vsk_{ID_i} + h_i \cdot r_i)Q$, where t_i is current timestamp. Then $\sigma_i = (R_i, S_i)$ is a certificateless signature.

- Finally, V_i sends $(ID_i, vpk_{ID_i}, M_i, t_i, \sigma_i)$ to a nearby RSU.

Individual Verify: Once the RSU receives a certificateless signature $\sigma_i = (R_i, S_i)$ from V_i, the RSU computes $Q_{ID_i} = H_1(ID_i)$, $h_i = H_2(M_i, ID_i, vpk_{ID_i}, R_i, t_i)$, $Q = H_1(q, P, P_{Pub}, T_{Pub})$ and checks whether the following verification

equation $e(S_i, P) = e(Q_{ID_i}, P_{Pub})\ e(vpk_{ID_i} + h_i \cdot R_i, Q)$ holds. If not, then rejects the signature else accepts it.
Aggregate: When receiving message-signature pairs $(M_1, t_1, \sigma_1 = (R_1, S_1), \cdots, M_n, t_n, \sigma_n = (R_n, S_n))$ from $V_i, i = 1, \cdots, n$ respectively, the RSU computes $S = \sum_{i=1}^{n} S_i$ and outputs $\sigma = (R_1, R_2, \cdots, R_n, S)$ as a CLAS.
Aggregate Verify: Once the application server receives a CLAS $\sigma = (R_1, R_2, \cdots, R_n, S)$, computes $Q_{ID_i} = H(ID_i)$, $h_i = H_2(M_i, ID_i, vpk_{ID_i}, R_i, t_i)$ for $i = 1, \cdots, n$, $Q = H_1(q, P, P_{Pub}, T_{Pub})$ and checks whether the verification equation $e(S, P) = e(\sum_{i=1}^{n} Q_{ID_i}, P_{Pub})\ e(\sum_{i=1}^{n}(vpk_{ID_i} + h_i \cdot R_i), Q)$ holds. If not, then rejects the CLAS, else accepts it.

5 Conclusion

In this paper, we first analyze the security for the certificateless aggregate signature presented by Horng *et al.*[18] which was claimed secure against two attack games of certificateless signature scheme. Unfortunately, we point out that the scheme does not resist malicious-but-passive KGC attack, which KGC may maliciously implant a trapdoor in the public system parameters and attempt to forge certificateless aggregate signature without private key of the user. Furthermore, an improved scheme is proposed.

References

1. Shamir, A.: Identity-based cryptosystems and signature schemes. In: Blakely G.R., Chaum D. (Eds.) CRYPTO 1984, LNCS vol. 196, pp. 47-53, 1985.
2. S.S. Al-Riyami, K.G. Paterson, Certificateless public key cryptography, in: Proceedings of the Asiacrypt 2003, LNCS 2894, Springer-Verlag, Taipei, Taiwan, 2003, pp. 452-473.
3. X. Huang, W. Susilo, Y. Mu, F. Zhang, On the security of certificateless signature schemes from Asiacrypt 2003, in: Proceedings of CANS, LNCS 3810, Springer-Verlag, 2005, pp. 13-25.
4. J. Li, X. Huang, Y. Mu, W. Wu, Cryptanalysis and improvement of an efficient certificateless signature scheme, J. Commun. Netw. 10 (1) (2008) 10-17.
5. W.S. Yap, S.H. Heng, B.M. Goi, An efficient certificateless signature scheme, emerging directions in embedded and ubiquitous computing, in: Proceedings of EUC Workshops 2006, LNCS 4097, Springer-Verlag, Seoul, Korea, 2006, pp. 322-331.
6. M. Au, Y. Mu, J. Chen, D. Wong, J. Liu, G. Yang, Malicious KGC attacks in certificateless cryptography, in: Proceedings of the 2nd ACM Symposium on Information, Computer and Communications Security, ACM, 2007, pp. 302-311.
7. A. Dent, B. Libert, K. Paterson, Certificateless encryption schemes strongly secure in the standard model, in: Proceedings of the Practice and Theory in Public Key Cryptography, 11th International Conference on Public Key Cryptography, Springer-Verlag, 2008, pp. 344-359.
8. X. Li, K. Chen, L. Sun, Certificateless signature and proxy signature schemes from bilinear pairings, Lithuanian Math. J. 45 (1) (2005) 76-83.

9. J. Liu, M. Au, W. Susilo, Self-generated-certificate public key cryptography and certificateless signature/encryption scheme in the standard model, in: Proceedings of the 2nd ACM Symposium on Information, Computer and Communications Security, ACM, 2007, pp. 273-283.
10. Y.Yu, Y.Mu, G.Wang, Q.Xia, B.Yang, Improved certificateless signature scheme provably secure in the standard model, IET Inf. Secur. 6(2)(2012)102-110.
11. Y. Yuan,C. H. Wang, Certificateless signature scheme with security enhanced in the standard model, Information Processing Letters 114(2014)492-499.
12. Sun, Y.X., Zhang, F.T., Baek, J.: Strongly secure certificateless public key encryption without pairing. Bao F. et al. (Eds.): CANS 2007, LNCS vol. 4856, pp. 194-208, 2007.
13. X. Huang, Y. Mu, W. Susilo, D.S. Wong, W. Wu, Certificateless signatures: new schemes and security models, Comput. J. 55 (4) (2012) 457-474.
14. J. Li, J. Zhao, Y. Zhang, Certificateless online/offline signcryption scheme, Security and Communication Networks, 2015, 8:1979-1990.
15. J. Li, Y. Li, Y. Zhang, Provably secure forward secure certificateless proxy signature scheme. KSII Transactions on Internet and Information Systems, 2013, 7(8): 1972-1988.
16. L. Zhang, F. Zhang, A new certificateless aggregate signature scheme, Computer Communications 32 (6) (2009) 1079-1085.
17. L. Zhang, B. Qin, Q. Wu, F. Zhang, Efficient many-to-one authentication with certificateless aggregate signatures, Computer Networks 54 (14) (2010) 2482-2491.
18. S. J. Horng et al., An efficient certificateless aggregate signature with conditional privacy-preserving for vehicular sensor networks, Information Sciences 317 (2015) 48-66.
19. D. Boneh, C. Gentry, B. Lynn, H. Shacham, Aggregate and verifiably encrypted signatures from bilinear maps, in: E. Biham (Ed.), EUROCRYPT 2003, LNCS 2656, Springer-Verlag, Warsaw, Poland, 2003, pp. 416-432.
20. R. Castro, R. Dahab, Efficient certificateless signatures suitable for aggregation, Cryptology ePrint Archive, Report 2007/454.
21. L. Cheng, Q. Wen, Z. Jin, H. Zhang, L. Zhou,Cryptanalysis and improvement of a certificateless aggregate signature scheme,Information Sciences 295 (2015) 337-346.
22. F. Zhang, L. Shen, G. Wu, Notes on the security of certificateless aggregate signature schemes, Information Sciences 287 (2014) 32-37.
23. D. He, M. Tian, J. Chen, Insecurity of an efficient certificateless aggregate signature with constant pairing computations, Information Sciences 268 (2014) 458-462
24. J. Deng, C. Xu, H. Wu, L. Dong, A new certificateless signature with enhanced security and aggregation version, Concurrency Computat.: Pract. Exper. (2015),doi: 10.1002/cpe.3551
25. Yulei Zhang and Caifen Wang,Comment on new construction of efficient certificateless aggregate signatures, International Journal of Security and Its Applications, Vol.9, No.1 (2015), pp.147-154
26. H. Xiong, Z. Guan, Z. Chen, F. Li, An efficient certificateless aggregate signature with constant pairing computations, Inform. Sci. 219 (2013) 225-235.
27. H. Liu, S. Wang, M. Liang and Y. Chen, New construction of efficient certificateless aggregate signatures, International Journal of Security and Its Applications, vol. 8, no. 1, (2014), pp. 411-422.