Hindawi
Security and Communication Networks
Volume 2019, Article ID 6059834, 5 pages
https://doi.org/10.1155/2019/6059834

Research Article

Cryptanalysis of a Certificateless Aggregate Signature Scheme for Healthcare Wireless Sensor Network

Yu Zhan [1] **and Baocang Wang** [1,2,3]

[1] *The State Key Laboratory of Integrated Service Networks, Xidian University, Xi'an 710071, China*
[2] *The Cryptographic Research Center, Xidian University, Xi'an 710071, China*
[3] *The Key Laboratory of Cognitive Radio and Information Processing, Ministry of Education, Guilin University of Electronic Technology, Guilin 541004, China*

Correspondence should be addressed to Baocang Wang; bcwang79@aliyun.com

Received 26 February 2019; Revised 30 April 2019; Accepted 25 May 2019; Published 9 June 2019

Academic Editor: David Megias

Certificateless aggregate signatures aggregate n signatures from n different users into one signature. Therefore, a verifier can judge whether all signatures are valid by verifying once. With this advantage, certificateless aggregate signatures are widely used in the environment of limited computing resources. Recently, a novel certificateless aggregate signature scheme was proposed by Kumar et al. This scheme's security was claimed to be secure against two types of attackers under the random oracle model. In this paper, we indicate that their scheme is unable to achieve this security goal. We show an attack algorithm that the second type of attacker could forge a valid signature under an identity without the private key of the target user. Moreover, we demonstrate that the second type of attacker could forge a valid aggregate signature.

1. Introduction

Digital signature is one of the most significant concerns in the traditional public key cryptosystems. There are several types of signature schemes in the development of signature technology: public key infrastructure- (PKI-) based signature schemes, identity-based signature schemes [1, 2], and certificateless signature schemes [3, 4]. In the earliest PKI-based signature schemes, a trusted certificate authority (CA) is needed to generate a certificate that corresponds to the public key of a legitimate user. Hence, these schemes initially have to obtain and verify the certificate. This causes an amount of computational costs. Identity-based signature schemes leave out CA, but each legitimate user's private key is produced and secretly assigned by the private key generator (PKG) which is also fully trusted. Accordingly, this kind of scheme is vulnerable to the attacks launched by the PKG. Certificateless signature schemes (CLS) overcome the shortcomings of the two kinds of schemes above. In this kind of scheme, key generation center (KGC) is in charge of calculating partial private keys and assigning the keys to legitimate users secretly. Each user calculates his private key that involves the partial private key. Consequently, not only can the user's legitimacy be verified, but also the KGC is incapable of launching an attack by recovering the user's private key.

In addition, in some application scenarios, the pattern of verifying one signature one time fails to meet the requirement of fast data processing. To solve this problem, Boneh et al. first put forward the concept of aggregate signature in 2003 [5]. Aggregate signature enables multiple signatures signed by multiple users to be aggregated into a single signature. Hence, the verifier can believe that all signatures are valid by verifying only once. This pattern greatly reduces the costs of communication and computation.

It is natural to combine the certificateless signature with the aggregate signature. As a result, lots of certificateless aggregate signature (CL-AS) schemes have been presented, such as [6–9]. Recently, Kumar et al. proposed a novel certificateless signature scheme with bilinear pairing. Furthermore, they extended the CLS scheme to a CL-AS scheme [10]. They illustrated that their schemes are secure against two types of

attackers. These two types of attackers have been widely used in the security proof of CL-AS. The details of the attackers are given below:

(i) Type I: an outside attacker who can replace the public keys of users and compromise the private keys of users. However, the attacker is unable to recover the master key or the partial private key.

(ii) Type II: an "honest-but-curious" KGC with the master key. However, it cannot replace the public keys of users or compromise the private keys of users.

We prove that Kumar et al.'s schemes cannot prevent the Type II attacker from forging a valid signature. The rest of this paper is organized as follows. We review the related work in Section 2 and describe the details of Kumar et al.'s schemes in Section 3. In Section 4, we show the attack algorithms. Finally, we concluded in Section 5.

2. Related Work

In 2003, Al-Riyami et al. [3] first introduced the notion of certificateless public key cryptosystem that is designed to solve the key escrow and certificate management issues. Besides, they proposed a CLS scheme as an instance. After that, the design and cryptanalysis of certificateless signature have become attractive research focuses. Huang et al. [11] indicated that Al-Riyami et al.'s scheme is incapable of resisting the public key replacement attack and they proposed an improvement scheme to fix the security vulnerability. Yum et al. [12] utilized the standard signature scheme and the ID-based signature scheme to propose a generic construction of CLS. Similarly, their scheme is insecure against the public key replacement attack [13]. Zhang et al. [14] presented a provably secure CLS scheme with bilinear pairing. Cao et al. [15] gave an attack algorithm for Gorantla et al.'s CLS scheme [4]. Liu et al. [16] presented a CLS scheme under the standard model. Xiong et al. [17] and Xia et al. [18] soon showed that Liu et al.'s scheme cannot achieve the security goals they claimed, respectively. Yeh et al. [19] proposed a CLS scheme which proved to be insecure by Jia et al. [20]. In addition, there are several CLS schemes that have not yet been identified as having security issues, such as [17, 21, 22].

As we mentioned above, the design and analysis of CL-AS schemes have been the concern of researchers. In 2007, Castro et al. [23] proposed an efficient CL-AS scheme. Similar with the later CL-AS schemes presented by Gong [24] and Zhang [6], the computational complexity of their schemes is too high to implement in practice. In 2010, Zhang et al. [25] introduced a novel CL-AS scheme. However, their scheme is unpractical since it needs a synchronous clock to aggregate signatures. In 2013, Xiong et al. [7] proposed a CL-AS scheme which needs constant bilinear pairing computations and is more efficient than previous works. Zhang et al. [26] and He et al. [27] indicated that the scheme [7] cannot resist the public key replacement attack. Meanwhile, Cheng et al. [8] and Tu et al. [28] presented improvement schemes based on Xiong et al.'s, respectively. Recently, researchers have gradually focused on the design of CL-AS schemes in special application environments. In 2015, Malhi et al. [29] showed a CL-AS scheme for vehicular ad hoc networks. Kumar et al. [30] found the security loophole of Malhi et al.'s scheme and gave an improvement scheme. However, Yang et al. [31] indicated that the improvement scheme is still insecure, and they proposed a new improvement scheme. Although the security of many schemes is no longer convincing, the schemes, e.g., [8, 28, 31], are still secure now.

3. Review of Kumar Et Al.'s Scheme

In this section, we first review the security model of Kumar et al.'s schemes [10].

3.1. Security Model. In their security model, the challenger $\mathscr{C}$ provides the following oracles to the adversary $\mathscr{A}$.

KeyGen(ID_i): Input an identity ID_i of user, and this oracle will output a public key pk_i under the identityID_i.

RevealSK(ID_i): Input an identity ID_i of user, and this oracle will output the private key sk_i under the identity ID_i.

RevealPK(ID_i): Input an identity ID_i of user, and this oracle will output the partial private key ppk_i under the identity ID_i.

ReplaceKey(ID_i, pk_i', sk_i'): Input an identity ID_i as well as a key pair (pk_i', sk_i'), and the original key pair will be replaced with the input one.

Sign(ID_i, m_i): If the identity ID_i has never been queried with the oracle *KeyGen*, return error symbol $\perp$. Else, the oracle runs the signing algorithm with the current key pair under ID_i and outputs the result.

The EUF-CMA (existential unforgeability against chosen message attacks) security model [32] for their CLS scheme consists of two games: Games 1 and 2.

Game 1. In this game, the adversary corresponds to the Type I attacker.

Setup: the challenger $\mathscr{C}$ runs the setup algorithm. Then, $\mathscr{C}$ keeps the master key secretly and returns the corresponding public key to $\mathscr{A}$.

Queries: the adversary $\mathscr{A}$ could query the above five oracles in polynomial bound.

Output: After querying, the adversary outputs a message m, the identity of target user ID^*, and a signature of message σ^*.

The adversary $\mathscr{A}$ will win this game if σ^* is a valid signature of m while Sign(ID^*, m) and RevealPK(ID^*) have never been queried.

Game 2. In this game, the adversary corresponds to the Type II attacker.

Setup: the challenger $\mathscr{C}$ runs the setup algorithm. Then, $\mathscr{C}$ returns the master key and the corresponding public key to $\mathscr{A}$.

Queries: the adversary $\mathscr{A}$ can query the above oracles expect ReplaceKey in polynomial bound. It is unnecessary to provide the RevealPK oracle since the adversary could calculate the partial private key under an identity with the master key by itself.

Output: after querying, the adversary outputs a message m, the identity of target user ID^*, and a signature of message σ^*.

The adversary $\mathcal{A}$ will win this game if σ^* is a valid signature of m while Sign(ID^*, m) and RevealSK(ID^*) have never been queried.

The CLS scheme is EUF-CMA secure only if the probability polynomial adversary cannot win in both games with nonnegligible advantages. The security model for the CL-AS scheme consists of two games too. The details are given below.

Game 3. In this game, the adversary corresponds to the Type I attacker.

The Setup and Queries stages are the same with Game 1.

Output: After querying, the adversary outputs a tuple $(\{m_i\}, \{ID_i^*\}, \sigma^*)$, where $\{m_i\}$ is a set of messages, $\{ID_I^*\}$ is a set of the identities of target users, and σ^* is an aggregate signature of $\{m_i\}$.

If σ^* is a valid aggregate signature of $\{m_i\}$ while there is at least one identity ID_j that has never been queried for Sign(ID_j^*, m_j) and RevealPK(ID_j^*), the adversary $\mathcal{A}$ wins this game.

Game 4. In this game, the adversary corresponds to the Type II attacker.

The Setup and Queries stages are the same as Game 2.

Output: After querying, the adversary outputs a tuple $(\{m_i\}, \{ID_i^*\}, \sigma^*)$, where $\{m_i\}$ is a set of messages, $\{ID_i^*\}$ is a set of the identities of target users, and σ^* is an aggregate signature of $\{m_i\}$.

If σ^* is a valid aggregate signature of $\{m_i\}$ while there is at least one identity ID_j that has never been queried for Sign(ID_j^*, m_j) and RevealSK(ID_j^*), the adversary $\mathcal{A}$ wins this game.

The CL-AS scheme is EUF-CMA secure only if the probability polynomial adversary cannot win in both games with nonnegligible advantages.

Next, we review the Kumar et al.'s scheme that includes seven algorithms. The details are given below.

3.2. Setup Algorithm. Given the security parameter λ, the setup algorithm that was performed by KGC generates a system parameter *param* and a master key *msk* as follows.

(1) Randomly select a prime p according to the security parameter λ.

(2) Select an additive cyclic group G_1 and a multiplicative cyclic group G_2 of prime order p. Particularly, g is a random generator of G_1.

(3) Select a bilinear map $\tilde{e} : G_1 \times G_1 \longrightarrow G_2$ which is effective to compute.

(4) Randomly select a master key $msk = s \longleftarrow \mathbb{Z}_p^*$, and compute the corresponding public key as $mpk = sg$.

(5) Define three secure hash functions: $H_0 : \{0,1\}^* \longrightarrow G_1$, $H_1 : \{0,1\}^* \longrightarrow G_1$, and $H_2 : \{0,1\}^* \longrightarrow \mathbb{Z}_p^*$.

(6) Disclose the system parameter $param = (H_0, H_1, H_2, g, G_1, G_2, \tilde{e}, mpk)$ and keep *msk* secretly.

All of the algorithms below need the system parameter *param* to calculate. We omit it in the following descriptions.

3.3. Partial Private Key Generation Algorithm. With a user's identity ID_i, this algorithm generates a partial private key. The KGC performs as follows.

(1) Calculate $P_i = H_0(ID_i)$.

(2) Calculate the partial private key as $ppk_i = sP_i$.

(3) Transmit ppk_i through a secure communication channel to the user U_i.

3.4. Key Generation Algorithm. This algorithm outputs a public/private key pair for a user U_i under ID_i. The user performs as follows.

(1) Randomly select $x_i \longleftarrow \mathbb{Z}_p^*$ as the private key, i.e., $sk_i = x_i$.

(2) Compute the public key as $pk_i = x_i g$.

3.5. Signing Algorithm. Given a partial private key ppk_i, a private key sk_i under an identity ID_i, the state information α (randomly selected from the public parameter), and a message m_i as inputs, the user U_i generates a signature σ_i of m_i as follows.

(1) Randomly select $r_i \longleftarrow \mathbb{Z}_p^*$ and compute $T_i = r_i g$.

(2) Calculate $h_i = H_2(m_i, ID_i, pk_i, T_i)$ and $Q = H_1(\alpha)$.

(3) Calculate $V_i = ppk_i + r_i Q + h_i x_i mpk$.

(4) Set the signature as $\sigma_i = (T_i, V_i)$.

3.6. Verification Algorithm. This algorithm takes a public key pk_i under an identity ID_i, the state information α, a signature σ_i, and a message m_i as inputs. The verifier performs as follows.

(1) Compute $P_i = H_0(ID_i)$, $h_i = H_2(ID_i, m_i, pk_i, T_i)$, and $Q = H_1(\alpha)$.

(2) Verify whether the equation $\tilde{e}(V_i, g) = \tilde{e}(P_i + h_i pk_i, mpk)\tilde{e}(Q, T_i)$ holds. If yes, accept the signature σ_i.

3.7. Aggregation Algorithm. This algorithm takes n signatures $\{\sigma_1, \sigma_2, \ldots, \sigma_n\}$ of n messages $\{m_1, m_2, \cdots, m_n\}$ as inputs. These signatures are generated by n users under identities $\{ID_1, ID_2, \ldots, ID_n\}$, respectively. Then, the aggregator sets the aggregate signature as $\sigma = (T_1, T_2, \ldots, T_n, V)$ after calculating $V = \sum_{i=1}^{n} V_i$.

3.8. Aggregate Verification Algorithm. Given an aggregate signature σ, n public keys $\{pk_1, pk_2, \ldots, pk_n\}$ under identities $\{ID_1, ID_2, \ldots, ID_n\}$, n messages $\{m_1, m_2, \cdots m_n\}$, and the state information α as inputs, this algorithm performs as follows.

(1) Compute $P_i = H_0(ID_i)$, $h_i = H_2(ID_i, m_i, pk_i, T_i)$ for $i = 1, \ldots, n$.

(2) Compute $Q = H_1(\alpha)$.

(3) Verify whether the equation $\tilde{e}(V, g) = \tilde{e}(\sum_{i=1}^{n}(P_i + h_i pk_i), mpk)\tilde{e}(Q, \sum_{i=1}^{n} T_i)$ holds. If yes, accept σ.

We clearly show the loophole of their schemes in the next section.

4. Cryptanalysis of the Kumar Et Al.'s Schemes

We indicate that the KGC who owns the master key msk is capable of forging a valid signature under an identity ID_i without the corresponding private key sk_i. Furthermore, the KGC can forge a valid aggregate signature. The details of the attacks are given below.

4.1. Attack on the Certificateless Signature Scheme. Given a message m_i, a public key pk_i under an identity ID_i, and the state information α, the KGC forges a signature σ of m_i as follows.

(1) Randomly select $r_i^* \longleftarrow \mathbb{Z}_p^*$ and calculate $T_i^* = r_i^* g$.

(2) Calculate $h_i^* = H_2(ID_i, m_i, pk_i, T_i^*)$, $Q = H_1(\alpha)$, and $P_i = H_0(ID_i)$.

(3) Calculate $V_i^* = s \cdot P_i + r_i^* Q + h_i^* \cdot s \cdot pk_i$.

(4) Set the signature as $\sigma = (T_i^*, V_i^*)$

Correctness

$$\begin{aligned}\widetilde{e}(V_i^*, g) &= \widetilde{e}(s \cdot P_i + r_i^* Q + h_i^* \cdot s \cdot pk_i, g)\\ &= \widetilde{e}(s \cdot P_i + h_i^* \cdot s \cdot pk_i, g)\,\widetilde{e}(r_i^* Q, g)\\ &= \widetilde{e}(P_i + h_i^* pk_i, sg)\,\widetilde{e}(Q, r_i^* g)\\ &= \widetilde{e}(P_i + h_i^* pk_i, mpk)\,\widetilde{e}(Q, T_i^*)\end{aligned} \tag{1}$$

Hence, $\sigma = (T_i^*, V_i^*)$ is a valid signature of m_i under ID_i. This CLS scheme is insecure against the attack launched by the "honest-but-curious" KGC.

4.2. Attack on the Certificateless Aggregate Signature Scheme. The CL-AS scheme presented by Kumar et al. is also insecure against the attack launched by the "honest-but-curious" KGC. Given n messages $\{m_1, m_2, \ldots, m_n\}$ and n users under $\{ID_1, ID_2, \ldots, ID_n\}$, the KGC performs as follows.

(1) Generate n signatures with the algorithm given in Section 3.5: $(m_1, \sigma_1), (m_2, \sigma_2), \cdots, (m_n, \sigma_n)$.

(2) Calculate $V^* = \sum_{i=1}^{n} V_i^*$.

(3) Set the aggregate signature as $\sigma = (T_1^*, T_2^*, \ldots, T_n^*, V^*)$.

Correctness

$$\begin{aligned}\widetilde{e}(V^*, g) &= \widetilde{e}\left(\sum_{i=1}^{n} V_i^*, g\right)\\ &= \widetilde{e}(s \cdot P_1 + r_1^* Q + h_1^* \cdot s \cdot pk_1, g)\\ &\cdots \widetilde{e}(s \cdot P_n + r_n^* Q + h_n^* \cdot s \cdot pk_n, g)\\ &= \widetilde{e}(P_1 + h_1^* pk_1, mpk)\,\widetilde{e}(Q, T_1^*)\\ &\cdots \widetilde{e}(P_n + h_n^* pk_n, mpk)\,\widetilde{e}(Q, T_n^*)\\ &= \widetilde{e}\left(\sum_{i=1}^{n}(P_i + h_i^* pk_i), mpk\right)\widetilde{e}\left(Q, \sum_{i=1}^{n} T_i^*\right)\end{aligned} \tag{2}$$

The forged aggregate signature $sigma = (T_1^*, T_2^*, \ldots, T_n^*, V^*)$ is a valid aggregate signature according to Section 3.7. Hence, this CL-AS scheme is insecure either.

5. Conclusions

Kumar et al. [10] proposed a CLS scheme and a CL-AS scheme. They claimed that these two schemes are both secure against two types of attackers. In this paper, we present attack algorithms for the two schemes, respectively. Details of our attacks show that the KGC can forge a valid signature of a message under a target identity without the corresponding private key. Similarly, the KGC can forge a valid aggregate signature. Hence, their schemes are insecure to implement in practical.

Data Availability

No data were used to support this study.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work is supported by the National Key R&D Program of China under Grant No. 2017YFB0802000, the National Natural Science Foundation of China under Grant Nos. 61572390 and U1736111, the National Cryptography Development Fund under Grant No. MMJJ20180111, the Plan For Scientific Innovation Talent of Henan Province under Grant No. 184100510012, the Program for Science & Technology Innovation Talents in the Universities of Henan Province under Grant No. 18HASTIT022, the Science & Technology Plan Projects of Henan Province 182102210124, the Innovation Scientists and Technicians Troop Construction Projects of Henan Province, the Fundamental Research Funds for the Central Universities, and the Innovation Fund of Xidian University No. 10221150004.

References

[1] J. C. Choon and J. H. Cheon, "An identity-based signature from gap diffie-hellman groups," in *Proceedings of the International Workshop on Theory and Practice in Public Key Cryptography: Public Key Cryptography*, vol. 2567, pp. 18–30, 2003.

[2] . Xun Yi, "An identity-based signature scheme from the Weil pairing," *IEEE Communications Letters*, vol. 7, no. 2, pp. 76–78, 2003.

[3] S. S. Al-Riyami and K. G. Paterson, "Certificateless public key cryptography," in *Advances in Cryptology-ASIACRYPT*, vol. 2894 of *Lecture Notes in Computer Science*, pp. 452–473, Springer, 2003.

[4] M. C. Gorantla and A. Saxena, "An efficient certificateless signature scheme," in *Proceeings of the International Conference on Computational Intelligence and Security*, vol. 3802, pp. 110–116, 2005.

[5] D. Boneh, C. Gentry, B. Lynn, and H. Shacham, "Aggregate and verifiably encrypted signatures from bilinear maps," in *Proceedings of the International Conference on the Theory and Applications of Cryptographic Techniques*, pp. 416–432, Springer, 2003.

[6] L. Zhang and F. Zhang, "A new certificateless aggregate signature scheme," *Computer Communications*, vol. 32, no. 6, pp. 1079–1085, 2009.

[7] H. Xiong, Z. Guan, Z. Chen, and F. Li, "An efficient certificateless aggregate signature with constant pairing computations," *Information Sciences*, vol. 219, pp. 225–235, 2013.

[8] L. Cheng, Q. Wen, Z. Jin, H. Zhang, and L. Zhou, "Cryptanalysis and improvement of a certificateless aggregate signature scheme," *Information Sciences*, vol. 295, pp. 337–346, 2015.

[9] S. Horng, S. Tzeng, P. Huang, X. Wang, T. Li, and M. K. Khan, "An efficient certificateless aggregate signature with conditional privacy-preserving for vehicular sensor networks," *Information Sciences*, vol. 317, pp. 48–66, 2015.

[10] P. Kumar, S. Kumari, V. Sharma, A. K. Sangaiah, J. Wei, and X. Li, "A certificateless aggregate signature scheme for healthcare wireless sensor network," *Sustainable Computing Informatics & Systems*, vol. 18, pp. 80–89, 2018.

[11] X. Huang, W. Susilo, Y. Mu, and F. Zhang, "On the security of certificateless signature schemes from asiacrypt 2003," in *Proceedings of the International Conference on Cryptology and Network Security*, pp. 13–25, Springer, 2005.

[12] D. H. Yum and P. J. Lee, "Generic construction of certificateless signature," in *Proceedings of the Australasian Conference on Information Security and Privacy*, pp. 200–211, Springer, 2004.

[13] B. C. Hu, D. S. Wong, Z. Zhang, and X. Deng, "Key replacement attack against a generic construction of certificateless signature," in *Proceedings of the Australasian Conference on Information Security and Privacy*, pp. 235–246, Springer, 2006.

[14] Z. Zhang, D. S. Wong, J. Xu, and D. Feng, "Certificateless public-key signature: security model and efficient construction," in *Proceedings of the International Conference on Applied Cryptography and Network Security*, pp. 293–308, Springer, 2006.

[15] X. Cao, K. G. Paterson, and W. Kou, "An attack on a certificateless signature scheme," *Cryptology ePrint archive*, https://eprint.iacr.org/2006/441.

[16] J. K. Liu, M. H. Au, and 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 (ASIACCS '07)*, pp. 273–283, March 2007.

[17] H. Xiong, Z. Qin, and F. Li, "An improved certificateless signature scheme secure in the standard model," *Fundamenta Informaticae*, vol. 88, no. 1-2, pp. 193–206, 2008.

[18] Q. Xia, C. Xu, and Y. Yu, "Key replacement attack on two certificateless signature schemes without random oracles," *Key Engineering Materials*, vol. 439-440, pp. 1606–1611, 2010.

[19] K. Yeh, C. Su, K. R. Choo, and W. Chiu, "A Novel Certificateless Signature Scheme for Smart Objects in the Internet-of-Things," *Sensors*, vol. 17, no. 5, p. 1001, 2017.

[20] X. Jia, D. He, Q. Liu, and K. R. Choo, "An efficient provably-secure certificateless signature scheme for Internet-of-Things deployment," *Ad Hoc Networks*, vol. 71, pp. 78–87, 2018.

[21] X. Huang, Y. Mu, W. Susilo, D. S. Wong, and W. Wu, "Certificateless signatures: new schemes and security models," *The Computer Journal*, vol. 55, no. 4, pp. 457–474, 2012.

[22] D. He, B. Huang, and J. Chen, "New certificateless short signature scheme," *IET Information Security*, vol. 7, no. 2, pp. 113–117, 2013.

[23] R. Castro and R. Dahab, "Efficient certificateless signatures suitable for aggregation," *IACR Cryptology ePrint Archive*, https://pdfs.semanticscholar.org/f580/b66051a832c4f9e39e5d533276f3afa3297b.pdf.

[24] Z. Gong, Y. Long, X. Hong, and K. Chen, "Two certificateless aggregate signatures from bilinear maps," in *Proceedings of the Eighth ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing (SNPD 2007)*, vol. 3, pp. 188–193, IEEE, Qingdao, China, July 2007.

[25] L. Zhang, B. Qin, Q. Wu, and F. Zhang, "Efficient many-to-one authentication with certificateless aggregate signatures," *Computer Networks*, vol. 54, no. 14, pp. 2482–2491, 2010.

[26] F. Zhang, L. Shen, and G. Wu, "Notes on the security of certificateless aggregate signature schemes," *Information Sciences*, vol. 287, pp. 32–37, 2014.

[27] D. He, M. Tian, and J. Chen, "Insecurity of an efficient certificateless aggregate signature with constant pairing computations," *Information Sciences*, vol. 268, pp. 458–462, 2014.

[28] H. Tu, D. He, and B. Huang, "Reattack of a certificateless aggregate signature scheme with constant pairing computations," *The Scientific World Journal*, vol. 2014, Article ID 343715, 10 pages, 2014.

[29] A. K. Malhi and S. Batra, "An efficient certificateless aggregate signature scheme for vehicular ad-hoc networks," *Discrete Mathematics & Theoretical Computer Science*, vol. 17, no. 1, pp. 317–338, 2015.

[30] P. Kumar and V. Sharma, "On the security of certificateless aggregate signature scheme in vehicular ad hoc networks," in *Soft Computing: Theories and Applications*, vol. 583, pp. 715–722, 2018.

[31] X. Yang, C. Chen, T. Ma, Y. Li, and C. Wang, "An improved certificateless aggregate signature scheme for vehicular ad-hoc networks," in *Proceedings of the 2018 IEEE 3rd Advanced Information Technology, Electronic and Automation Control Conference (IAEAC)*, pp. 2334–2338, Chongqing, China, October 2018.

[32] X. Huang, Y. Mu, W. Susilo, D. S. Wong, and W. Wu, "Certificateless signature revisited," in *Proceedings of the Australasian Conference on Information Security and Privacy*, pp. 308–322, Springer, 2007.