An efficient anonymous authentication scheme based on a signature with deterable function for mobile healthcare crowd sensing

Jinhui Liu[1], Yong Yu[1*], Yannan Li[2], Yanqi Zhao[1], and Xiaojiang Du[3]

[1] School of Computer Science, Shaanxi Normal University, Xi'an 710119, China
[2] School of Computing and Information Technology, University of Wollongong, Wollongong, NSW2522, Australia
[3] Dept. of Computer and Information Sciences, Temple University, Philadelphia PA 19122, USA
{yuyong}@snnu.edu.cn

Abstract. With the widespread growth of cloud computing and mobile healthcare crowd sensing (MHCS), an increasing number of individuals are outsourcing their masses of bio-information in the cloud server to achieve convenient and efficient. In this environment, Cloud Data Center (CDC) needs to authenticate masses of information without revealing owners' sensitive information. However, tremendous communication cost, storage space cost and checking time cost lead to CDC that give rise to all kinds of privacy concerns as well. To mitigate these issues, To mitigate these issues, we propose a data anonymous batch verification scheme for MHCS based on a certificateless double authentication preventing aggregate signature. The proposed scheme can authenticate all sensing bio-information in a privacy preserving way. We then present that the proposed CL-DAPAS scheme is existentially unforgeable in the Random Oracle Model (ROM) assuming that Computational Diffie-Hellman problem is difficult to solve. Furthermore, we provide an implementation and evaluate performance of the proposed scheme and demonstrate that it achieves less efficient computational cost compared with some related schemes.

Keywords: Mobile healthcare crowd sensing · Security · Privacy · Double authentication preventing signature · Elliptic curve discrete logarithm problem.

1 Introduction

An increasing interest is growing around Cloud Data Centers (CDC) that allows the delivery of various kinds of agile services and applications over telecommunication networks and the Internet. Mobile crowd sensing (MCS) in the IOT assembles scenario, environmental, and individual data within a specific range via the intelligent sensing equipment carried by mobile users, thus providing social decision-making services [1]. As an important application branch of MCS,

MHCS furnishes a more convenient healthcare medical services for institutions and individuals [2, 3]. In MHCS, participants accept a sensing assignment for specific purpose from cloud sever and they make a collection of relevant health data and upload these data to the cloud sever. At the same time, the cloud sever transmits requested information to a range of special healthcare institutes for further analysis. CDC in MHCS needs to authenticate masses of bio-information without revealing sensitive information of these participants. There exists numerous research findings from data integrity checking protocols and data deletion protocols that were proposed to different requirements of authentication which can be applied to MHCS [4–10].

A representative structure of the MHCS is listed in Fig.1 [3, 11]. Communication process in MHCS can be falled into two aspects. For one thing, participants put up health data which are assembled by mobile intelligent terminals to a CS (Cloud Server). For anthother, by studying personal health data, anytime anywhere medical service and health information can be offered by remote healthcare system and vital signs of patients which are refered to long distance health applications can be mounted in mobile intelligent endpoints or other monitoring equipment.

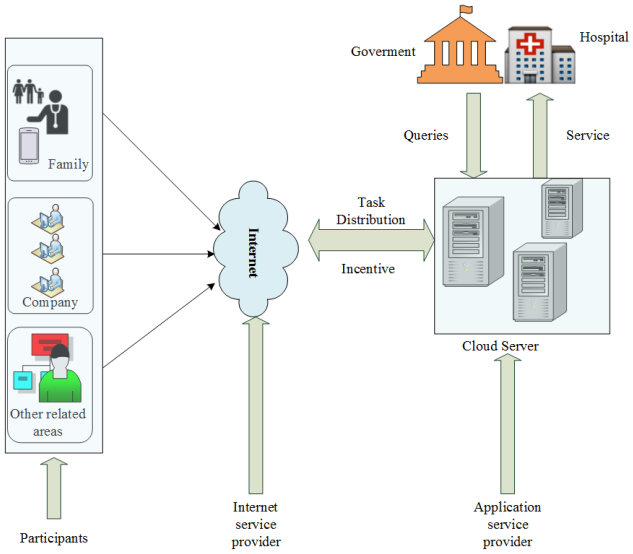

Fig. 1. A typical MHCS framework

By wireless communication model, adversaries against MHCS is easy to manage fairly communication channels, that is to say, adversaries could hold up, alter, replay and erase messages that transmitted in MHCS system. Hence MHCS are susceptible to numberous types of attacks. In practice, sensitive information of participates, such as identity, individual social activities and health status, may

be leakaged by the collected health data. These collected health data ought to be managed safely in a actual time mode, else it will reduce health service quality. If health data is eavesdropped or tampered by an adversary, it will cause damage to personal health and estates, so far as to personal lives. Therefore, security and privacy protection of collected health data in MHCS is an indispensable part of many practical applications [12–14].

Several papers have studied related security and privacy of wireless issues [15–18]. Aggregate signature (AS), as one of the most efficient privacy and integrity, resolving the issues of limited resources, privacy, message integrity and authenticity, is applicable to addressing the some issues in MHCS [19–22]. At present, there are many AS schemes which have been put forward for all kinds of practical applications. In 2003, Boneh et al. put forward the first AS (aggregate signature) which enables a signer to construct a valid signatures on their messages to be signed and have a batch verification [19]. After that, most of AS schemes were incured a complicated certificate management [23, 37]. In 2007, Castro et al. [24] provided a general notion of certificateless (CL) AS that made a combination of properties of AS and CLPKC (Certificateless Public Key Cryptography). The same year, Gong et al. standardized a security model for CL-AS [25]. After that many CLAS schemes were designed [3, 26–29]. Although previously proposed AS could mitigate privacy preserving authentication for MHCS, there exists many double signatue problems and the performance of these schemes is unsatisfactory.

Consider such a scenario, if some special field doctor in a hospital sign twice about a patient of same identity and kinds of diseases, we can consider that the doctor have done some misconducts. To prevent fraud by discouraging users from submitting (signing) duplicates, we use double authentication preventing signatures (DAPS) instead of conventional signatures, where the address a (or its associated space respectively) can be given some application dependent semantics. Unlike group signature and linkable-ring signature[30, 31], DAPS are stronger signatures in the sense that signers secret keys can be revealed [32, 33]. Revealing the secret key as discouragement to behave fraudulent is related to PKI-assured non-transferability approach in anonymous credential systems. Many instances are shown that a double signer is not enough of a penalty but is enough of a deterable function. There are some research about post-quantum DAPS system [34–36]. Based on these, we provide a new and more higher efficient conditional privacy protection signature scheme for MHCS.

Our main contributions are summarized in the following.

1. We provide a certificateless double authentication preventing aggregate signature scheme (CL-DAPAS) with deterable function for MHCS.

2. We make a security analysis to show that CL-DAPAS fulfil some security needs in MHCS.

3. We propose a high efficient authentication scheme to verify batch messages received from MHCS participants.

4. We present a computation cost analysis to show that our CL-DAPAS scheme has higher efficiency than some related schemes.

2 Preliminaries and system model

2.1 Hard problem assumption

Definition 1 (ECDLP (Elliptic Curve Discrete Logarithm Problem)). *Given two points $P, Q \in G$ on E, it is difficult to calculate an integer $x \in Z_q^*$ to get the equation $P = xQ$.*

Definition 2 (CDHP (Computational Diffie Hellman Problem) [?]). *Given two random points $xP, yP \in G_1$, where x, y are two unknown information in Z_q, it is difficult to obtain xyP in polynomial time.*

2.2 System model

We define system model of MHCS scenario, which consists of requestors, a Cloud Data Center (CDC), a Management Server (MS), and a MHCS participants.

1. For some specific purposes, requestors refer healthcare sensing tasks to CDC. Then they can study memoir from CDC and then forecast certain health and medical problems in some regions.

2. According to the demands of the requestors, CDC release and manage healthcare sensing tasks. And it can aggregate and verify healthcare data for participants.

3. MS can administer registration for participants, where MS is a trusted third party. MS assignments indexes for participants to substitute for their actual identities and is reponsible for issuing a half private keys of legitimate participants. MS is able to verify health data uploaded by participants by using an index.

4. Participants can upload healthcare data for CDC by intelligent terminals.

2.3 Security requirements

The aim objective of the proposed scheme for MHCS is to provide an efficient privacy preserving to satisfy the following security requirements:

1. **Batch authentication**: The signed health data is able to be aggregated and verified by CDC.
2. **Nonrepudiation**: Participants have sent related health data to CDC that they cannot deny.
3. **Anonymity**: Even if CDC can obtain and check these aggregated messages, CDC is not able to get data provider's real identity.
4. **Deterable-iff-double signature by one signer**: If an participant signs on colliding message (a, p_1) and (a, p_2), he can be linked and his signature keys can be extracted by anyone.

3 The proposed data batch verification scheme based on CL-DAPAS for MHCS

Consider such a scenario in MHCS, if some special field doctor in a hospital sign twice about a patient of same identity and kinds of diseases, we can consider that the doctor have done some misconduct.

3.1 The proposed scheme

Initialization In this phase, MS sets up an enrollment system in the following.

1. G is an q order additive group. P is a generator of G. Choose a key s_{MS} and calculate coresponding public key $P_{MSpub} = s_{MS}P$. Elect hash functions $h_1 : \{0,1\}^* \times G \to G$ and $h_2 : \{0,1\}^* \times G \to Z_q^*$.
2. Publish parameters $(P, E, G, p, q, P_{MSpub}, h_1, h_2)$ and maintain the master private key s_{MS}. CDC regards (Q_{CDC}, s_{CDC}) as its key pair, where $Q_{CDC} = s_{CDC}P$.

Registration In this phase, a participant C_i computes partial key and MS is to access a CDC.

1. C_i chooses randomly a number $s_{i1} \in Z_q^*$ as partial private key and computes $Q_{i1} = s_{i1}P$. C_i obtains psk_{i1} from MS who computes $psk_{i1} = s_{MS}h_1(Id_i, Q_{i1})$ as the other part of private key. C_i puts (s_{i1}, psk_{i1}) as private key and (Id_i, Q_{i1}) as public key.
2. MS chooses randomly a number $w_i \in Z_q^*$ and computes $Q_{i2} = h_1(Id_i, Q_{i1})$, $psk_{i2} = s_{MS}h_1(Id_i, Q_{i1})$, $index_{is} = w_iQ_{i2}$ and $index_{iv} = w_ipsk_{i2}$. Thus, MS stores serial number $sn_i = (Id_i, Q_{i1}, Q_{i2}, index_{is}, index_{iv})$. Then it sends $SN_i = index_{iv}$ and $index_{is}$ to the C_i with Id_i via a secure channel.

Sign C_i chooses randomly $r_i \in Z_q^*$ and t_i, where t_i is a time stamp which is able to keep freshness of $m_i = (a, p_i)$. C_i performs the following steps:

1. Compute $R_i = r_iP$; $K_i = h_2(p_i\|t_i, R_i)$; $S_i = s_{i1} + a \cdot K_ir_i \bmod q$; $U_i = psk_{i1} + r_iP_{MSpub}$; $Enc_{Q_{CDC}}(SN_i\|K_i\|t_i) = SN_i'$
2. C_i uploads $(R_i, K_i, S_i, U_i, M_i, SN_i')$ to CDC who announces the sensing task, where $M_i = (a, p_i)$.

Verify To ensure the validity of each required sensing data signed by a C_i, the following steps are executed by CDC.

1. Calculate $SN_i\|K_i\|t_i = Dec_{s_{CDC}}(SN_i')$. Verify $K_i = h_2(p_i\|t_i, R_i)$.
2. Check whether the equation

$$S_iP = Q_{i1} + a \cdot k_iR_i \text{ and } e(U_i, P) = e(P_{MSpub}, R_i + h_1(Id_i, Q_{i1})) \text{ holds.}$$

If the above equations are true, then the verifier affirms the signature is a valid signature; otherwise, the signature is invalid.

Aggregation Upon receiving $(R_i, K_i, S_i, U_i, M_i, SN_i')$, CDC computes $SN_i \| K_i \| t_i = Dec_{s_{CDC}}(SN_i')$.

For a set of n participants $C_1, \cdots, C_n$ and the corresponding signatures $(R_i, K_i, S_i, U_i, M_i)$, CDC aggregates all signatures as follows once time T is up:

1. $KR = \sum_{i=1}^{n} a \cdot K_i R_i$; $Q = \sum_{i=1}^{n} Q_{i1}$; $R = \sum_{i=1}^{n} R_i$; $S = \sum_{i=1}^{n} S_i \bmod q$; $H = \sum_{i=1}^{n} h_1(Id_i, Q_{i1})$; $index_v = \sum_{i=1}^{n} index_{iv} \bmod q$.
2. $\sigma = (KR, Q, S, R, H, index_v)$ is the aggregated signature.

Batch Verification CDC verifies the validity of the equation above in the following. Check whether the equations

$$SP = Q + KR \text{ and } e(U, P) = e(P_{MSpub}, H + R) \text{ hold.}$$

Extract$_{sk}$ iff double signature by one signer C_i: If C_j sign twice, CDC receives two signatures from colliding messages $M_{i1} = (a, p_{i1})$ and $M_{i2} = (a, p_{i2})$ from one signer.

According to signatures $\sigma_{i1} = (R_i, K_{i1}, S_{i1}, U_i)$ and $\sigma_{i2} = (R_i, K_{i2}, S_{i2}, U_i)$, Anyone can compute the private key s_{i1}, psk_{i1} of C_j as follows.

1. According to $R_i = r_i P$, $K_{i1} = h_2(ID_i \| R_i \| p_{i1})$, $K_{i2} = h_2(ID_i \| p_i, R_i)$,
$$\begin{cases} S_{i1} = s_{i1} + a \cdot K_{i1} r_i \text{mod} q \ ; \\ S_{i2} = s_{i1} + a \cdot K_{i2} r_i \text{mod} q \ . \end{cases}$$
2. Compute
$$s_{i1} = \frac{(K_{i1} S_{i2} - K_{i2} S_{i1})}{(K_{i1} - K_{i2})} \ , r_i = \frac{(S_{i2} - S_{i1})}{a(K_{i2} - K_{i1})} \text{ and } psk_{i1} = U_i - \frac{(S_{i2} - S_{i1})}{a(K_{i2} - K_{i1})} P_{pub}.$$

3.2 Security analysis

Theorem 1. *If the adversary $\mathcal{A}_1$ who has the ability of substituting for participants' public keys with MS' private keys can break CLDAPAS, CDH problem could be solved in a non-negligible probability.*

Theorem 2. *Assuming that CDH problem is hard, our CL-DAPAS is existentially unforgeable in ROM against $\mathcal{A}_2$.*

The proof process of the two theorem above can be found in the full paper. By security analysis, we can show that our scheme satisfy the following property.

Batch authentication and message integrity authentication: According to the security analysis, there is no adversary that could generate a legal signature σ_i. So CDC could authenticate identities of participants by their signatures. Futhermore, CDC is able to find any variation of received signatures by checking whether the equation $SP = Q + KR$ holds.

Non-repudiation: MHCS participants can not deny that they have transmitted their health data. CDC can verify their signatures via corresponding

public keys. Then, according to their public keys, MS can find serial number sn_i and MS can obtain real identity for every participant C_i.

No inefficiency problem of the double secret key: Due to the phases of the proposed scheme, CDC just needs to save the master key secretly. Therefore, the proposed scheme for MHCS is able to provide no inefficiency problem of the double secret key.

Deterable-iff-double signature by one signer: By the proposed scheme, we can see that our scheme is able to discourage signers from misbehaving.

4 Performance analysis

To give practical performance analysis, we get the execution time of different cryptographic processes by Pairing-Based Cryptography library [38], which is a famous and free java library for implementing of pairing-based cryptosystems. For schemes based on bilinear pairings for MHCS, to achieve 80 bits security level, we choose a bilinear pairing $e : G_a \times G_a \rightarrow G_m$, where G_a is generated by a q order point P on $E : y = x^3 + x \bmod \overline{p}$. For the proposed scheme, we use Type-I elliptic curve $E : y^2 = x^3 - x + 1$ over a ternary extension field F_{3^m}. G_1 is a group of points $E(F_{3^m})$. The experiment is executed on a personal calculater, which is equipped with an windows 7 64 OS, intel(R) Core(TM) i7-4710MQ CPU 2.50GHz,12GB RAM With JPBC library for 1000 times. Execution time and related cryptographic operations are shown in Table 1.

Table 1. The definition and execution time of related operations.

Cryptographic operation	Definition	Execution time
T_{bp}	a bilinear pairing process	7.8 ms
T_{sm-bp}	a point multiplication process	14 ms
T_{pa-bp}	a point addition process	0.0005 ms
T_{Z_p-bp}	a map-to-point hash process	0.003 ms
T_{G_1-bp}	a map-to-G_1 hash process	32.8 ms
T_{sm-ecc}	a point multiplication process	2.8 ms
T_{pa-ecc}	a point addition process	0.0005 ms
T_{Z_p-ecc}	a map-to-point hash process	0.003 ms
T_{G_1-ecc}	a map-to-G_1 hash process	0.2 ms

Let P_1, P_2, P_3 and P_4 denote Signing, Verification, Aggregation and Batch Verification phase respectively. We present a comparison analysis of THH [27], Malhi-Batra [28], XGCL [29], Liu-Cao scheme [3] and our proposed scheme.

In the Signing stage P_1, we find that our scheme requires $2nT_{bp}+nT_{HZ_p-ecc}+nT_{sm-ecc} + nT_{pa-ecc} \approx 18.4035n$ ms, while schemes in THH [27], Malhi-Batra [28], XGCL [29] and Liu-Cao's scheme [3] require $2nT_{HZ_p-bp} + 2nT_{HG-bp} + 3nT_{sm-bp} \approx 107.6006n$ ms, $nT_{HZ_p-bp}+4nT_{sm-bp} \approx 56.003n$ ms and $nT_{HZ_p-bp}+3nT_{sm-bp} \approx 42.003n$ ms, $nT_{HZ_p-bp} + 2nT_{sm-bp} \approx 28.003n$ ms respectively. For the total execution time, the percentage improvement for the Signing stage P_1 of

CLDAPAS over THH et al.'s scheme is about $\frac{(107.6006n-18.4035n)}{107.6006n} \approx 83\%$. Other percentage improvements can also be computed by similar method, they are 67%, 56%, 34% respectively.

In the verification stage, our scheme needs $nT_{HZ_p-bp}+nT_{HG-bp}+5nT_{sm-ecc}+2nT_{bp} \approx 29.8003n$ ms, while schemes require $2nT_{HZ_p-bp}+3nT_{HG-bp}+4nT_{bp}+2nT_{sm-bp} \approx 157.606n$ ms in [21], $nT_{HZ_p-bp}+nT_{HG-bp}+3nT_{bp}+3nT_{sm-bp} \approx 98.203n$ ms in [22], $nT_{HZ_p-bp}+nT_{HG-bp}+3nT_{bp}+2nT_{sm-bp} \approx 84.203n$ ms in [23] and $nT_{HZ_p-bp}+nT_{HG-bp}+2nT_{bp}+nT_{sm-bp} \approx 62.403n$ ms in [3]. The percentage improvement for P_2 of CLDAPAS are 81%, 70%, 65%, 52% respectively.

In aggregation stage P_3, our scheme needs $5T_{sm-ecc} \approx 14n$ ms scalar multiplications, while the scheme in [3] requires $28n$ ms.

In aggregation verification stage P_4, our scheme needs $2nT_{sm-ecc}+2T_{bp} \approx 21.2$ ms, while schemes in [21][22][23][3] requires about $31.2+28n$ ms, $23.4+42n$ ms, $23.4+28n$ ms and 15.6 ms respectively. Although the execution time of our scheme in batch verification stage P_4 is higher than the execution time of scheme [3], other stages are much lower than execution time of these schemes.

5 Conclusion

To protect the security and privacy of online health data from the unauthorized entities in MHCS, we construct a novel and an efficient anonymous data batch authentication scheme for MHCS based on CL-DAPAS. Our proposed scheme has advantages of certificateless signature, aggregate signature and double signature that can be disincentivized. The security analysis of the scheme is conducted to ensure the data integrity, non-repudiation, no inefficiency problem of the double secret key, batch authentication and deterable function. Performance analysis results of our proposed scheme has higher efficient in time consumption which makes it suitable for deployment in the MHCS system. With rapid development of quantum computers, in the future we will study the design of post-quantum certificateless double authentication preventing aggregate signatures which are suitable for MHCS.

Acknowledgments The author would like to thank the anonymous reviewers for their constructive comments and suggestions. This work was supported by National Key R&D Program of China (2017YFB0802000), National Natural Science Foundation of China (61772326, 61572303, 61872229, 61802239), NSFC Research Fund for International Young Scientists (61750110528), National Cryptography Development Fund during the 13th Five-year Plan Period (MMJJ20170216, MMJJ201701304), Foundation of State Key Laboratory of Information Security (2017-MS-03), Fundamental Research Funds for the Central Universities(GK201702004, GK201803061, 2018CBLY006) and China Postdoctoral Science Foundation (2018M631121).

References

1. Ganti R K, Ye F, Lei H. Mobile crowdsensing: current state and future challenges. IEEE Communications Magazine, 49(11), 2011; 32-37.

2. Pryss R, Reichert M, Herrmann J, Langguth B, Schlee W. Mobile Crowd Sensing in Clinical and Psychological Trials – A Case Study. IEEE International Symposium on Computer-Based Medical Systems. 2015; 23-24.
3. Liu J, Cao H, Li Q, Cai F, Du X, Gui M. A Large-scale Concurrent Data Anonymous Batch Verification Scheme for Mobile Healthcare Crowd Sensing. IEEE Internet of Things Journal, 2018; 1-10.
4. Zhang H, Zhang Q, Du X, Toward Vehicle-Assisted Cloud Computing for Smartphones, IEEE Transactions on Vehicular Technology, 12(64), 2015; 5610-5618.
5. Li J, Chen X, Chow S S M , Huang Q, Wong D S, Liu Z. Multi-authority fine-grained access control with accountability and its application in cloud. Journal of Network and Computer Applications. DOI: 10.1016/j.jnca.2018.03.006.
6. Li T, Li J, Liu Z, Li P, Jia C. Differentially Private Naive Bayes Learning over Multiple Data Sources. Information Sciences, 444: 89-104, 2018.
7. Yu Y, Au M H, Ateniese G, Huang X, Susilo W, Dai Y, Min G. Identity-Based Remote Data Integrity Checking With Perfect Data Privacy Preserving for Cloud Storage. IEEE Trans. Information Forensics and Security 12(4): 767-778, 2017.
8. Li Y, Yu Y, Susilo W, Min G, Ni J, Choo R. Fuzzy Identity-Based Data Integrity Auditing for Reliable Cloud Storage Systems. IEEE Trans. on Dependable and Secure Computing, DOI: 10.1109/TDSC.2017.2662216, 2016.
9. Yu Y, Li Y, Yang B, Susilo W, Yang G, Bai J, Attribute-based cloud data integrity auditing for secure outsourced storage, IEEE Trans. on Emerging Topics in Computing. doi:10.1109/TETC.2017.2759329.
10. Xue L,Yu Y, Li Y, Au M H, Du X, Yang B. Efficient Attribute-based Encryption with Attribute Revocation for Assured Data Deletion, Information Science, DOI: 10.1016/j.ins.2018.02.015.
11. He D, Chan S, Guizani M. User privacy and data trustworthiness in mobile crowd sensing. IEEE Wireless Communications, 22(1), 2015; 28-34.
12. Gisdakis S, Giannetsos T, Papadimitratos P. Security, privacy, and incentive provision for mobile crowd sensing systems. IEEE Internet of Things Journal, 3(5), 2016; 839-853.
13. Zhang K, Ni J, Yang K, Liang X, Ren J, Shen X S. Security and privacy in smart city applications: Challenges and solutions. IEEE Communications Magazine, 55(1), 2017;122-129.
14. Ni J, Zhang K, Yu Y, Lin X, Shen X S. Providing Task Allocation and Secure Deduplication for Mobile Crowdsensing via Fog Computing. IEEE Transactions on Dependable and Secure Computing. 2018; 1-12.
15. Xiao Y, Rayi V, Sun B , Du X, Hu F, Galloway M, A Survey of Key Management Schemes in Wireless Sensor Networks, Journal of Computer Communications, 30(11-12), 2007; 2314-2341.
16. Du X, Xiao Y, Guizani M, Chen H H, An Effective Key Management Scheme for Heterogeneous Sensor Networks, Ad Hoc Networks, Elsevier, 5(1), 2007; 24C34
17. Du X, Chen H H, Security in Wireless Sensor Networks, IEEE Wireless Communications Magazine, 15(4), 2008; 60-66.
18. Du X, Guizani M, Xiao Y, Chen H H, Transactions papers, A Routing-Driven Elliptic Curve Cryptography based Key Management Scheme for Heterogeneous Sensor Networks, IEEE Transactions on Wireless Communications, 8(3), 2009; 1223 - 1229.
19. Boneh D, Gentry C, Lynn B, Shacham H. Aggregate and verifiably encrypted signatures from bilinear maps. In International Conference on the Theory and Applications of Cryptographic Techniques . Springer, Berlin, Heidelberg. 2003, 416-432.

20. Xiong H, Guan Z, Chen Z, Li F. An efficient certificateless aggregate signature with constant pairing computations. Information Sciences, 219, 2013; 225-235.
21. Shen L, Ma J, Liu X, Wei F, Miao M. A secure and efficient id-based aggregate signature scheme for wireless sensor networks. IEEE Internet of Things Journal, 4(2), 2017; 546-554.
22. Kumar P, Kumari S, Sharma V, Sangaiah A K, Wei J, Li X. A Certificateless aggregate signature scheme for healthcare wireless sensor network. Sustainable Computing: Informatics and Systems. 2017.
23. Zhang L, Zhang F. A new certificateless aggregate signature scheme. Computer Communications, 32(6), 2009; 1079-1085.
24. Deng J, Xu C, Wu H, Dong L. A new certificateless signature with enhanced security and aggregation version. Concurrency and Computation: Practice and Experience, 28(4), 2016; 1124-1133.
25. Gong Z, Long Y, Hong X, Chen K, Two certificateless aggregate signatures from bilinear maps,In IEEE SNPD 2007, 3, 2007;188-193.
26. Au M H, Yang G, Susilo W, Zhang Y. (Strong) multidesignated verifiers signatures secure against rogue key attack. Concurrency and Computation: Practice and Experience, 26(8), 2014;1574-1592.
27. Tu H, He D, Huang B, Reattack of a certificateless aggregate signature scheme with constant pairing computations, The Scientific World Journal, 2014, 2014; 1-9.
28. Malhi A K, Batra S, An efficient certificateless aggregate signature scheme for vehicular ad-hoc networks, Discrete Mathematics and Theoretical Computer Science,17(1), 2015; 317-320.
29. Bayat M , Barmshoory M, Rahimi M, Aref M R. A secure authentication scheme for VANETs with batch verification, Wireless Networks, 21(5), 2014; 1-11.
30. Camenisch J, Stadler M. Efficient group signature schemes for large groups, CRYPTO97, Springer, Berlin, Heidelberg, 1997; 410-424.
31. Au M H , Liu J K , Susilo W, Yuen T H. Secure id-based linkable and revocable-iff-linked ring signature with constant-size construction. Theory Computer Science, 469, 2013; 1-14.
32. Poettering B, Stebila D. Double authentication preventing signatures. In ESORICS 2014, 2014; 7-11:
33. Bellare M, Poettering B, Stebila D. Deterring certificate subversion: Efficient double authentication preventing signatures. In PKC 2017, 2017; 121-151.
34. Dan B, Kim S, Nikolaenko V. Lattice-Based DAPS and Generalizations: Self-enforcement in Signature Schemes, International Conference on Applied Cryptography and Network Security. Springer, Cham, 2017; 457-477.
35. Mao S, Zhang P, Wang H, Zhang H, Wu W. Cryptanalysis of a lattice based key exchange protocol. Science China Information Sciences, 60(2), 2017; 028101-028105.
36. Wu W, Zhang H, Wang H, Mao S, Wu S, Han H. Cryptanalysis of an MOR cryptosystem based on a finite associative algebra. Science China Information Sciences, 59(3), 2016; 32111.
37. Huang X, Mu Y, Susilo W, Wong D S , Wu W, Certificateless signatures: New schemes and security models 1,The Computer Journal, 55(4), 2011: 457-474.
38. He D, Zeadally S, Xu B, Huang X. An Efficient Identity-Based Conditional Privacy-Preserving Authentication Scheme for Vehicular Ad Hoc Networks. IEEE Transactions on Information Forensics and Security, 2015, 10(12):2681-2691.