

Singapore Management University Institutional Knowledge at Singapore Management University

Research Collection School Of Information Systems

School of Information Systems

8-2018

Security analysis of a large-scale concurrent data anonymous batch verification scheme for mobile healthcare crowd sensing

Yinghui ZHANG

Xi'an Institute of Posts and Telecommunications

Jiangang SHU

City University of Hong Kong

Ximeng LIU

Singapore Management University, xmliu@smu.edu.sg

Jin LI


Guangzhou University

Dong ZHENG

Xi'an Institute of Posts and Telecommunications

DOI: <https://doi.org/10.1109/JIOT.2018.2862381>

Follow this and additional works at: https://ink.library.smu.edu.sg/sis_research

 Part of the [Information Security Commons](#), and the [Medicine and Health Sciences Commons](#)

Citation

ZHANG, Yinghui; SHU, Jiangang; LIU, Ximeng; LI, Jin; and ZHENG, Dong. Security analysis of a large-scale concurrent data anonymous batch verification scheme for mobile healthcare crowd sensing. (2018). *IEEE Internet of Things*. 1-5. Research Collection School Of Information Systems.

Available at: https://ink.library.smu.edu.sg/sis_research/4152

This Journal Article is brought to you for free and open access by the School of Information Systems at Institutional Knowledge at Singapore Management University. It has been accepted for inclusion in Research Collection School Of Information Systems by an authorized administrator of Institutional Knowledge at Singapore Management University. For more information, please email libIR@smu.edu.sg.

Security Analysis of a Large-scale Concurrent Data Anonymous Batch Verification Scheme for Mobile Healthcare Crowd Sensing

Yinghui Zhang, *Member, IEEE*, Jiangang Shu, Ximeng Liu, *Member, IEEE*, Jin Li, and Dong Zheng

Abstract—As an important application of the Internet of Things (IoT) technologies, mobile healthcare crowd sensing (MHCS) still has challenging issues, such as privacy protection and efficiency. Quite recently in IEEE Internet of Things Journal (DOI: 10.1109/JIOT.2018.2828463), Liu et al. proposed a large-scale concurrent data anonymous batch verification scheme for mobile healthcare crowd sensing, claiming to provide batch authentication, non-repudiation, and anonymity. However, after a close look at the scheme, we point out that the scheme suffers two types of signature forgery attacks and hence fails to achieve the claimed security properties. In addition, a reasonable and rigorous probability analysis indicates that the security reduction from the security of the scheme to the hardness of the Computational Diffie-Hellman (CDH) problem is invalid. We hope that similar design flaws can be avoided in future design of anonymous batch verification schemes for mobile healthcare crowd sensing.

Index Terms—Cryptanalysis, Mobile healthcare crowd sensing, Anonymity, Batch authentication.

I. INTRODUCTION

WITH the rapid advancements of the Internet of Things (IoT) technologies, mobile healthcare crowd sensing (MHCS) has emerged as a new sensing paradigm that is able to facilitate the quality improvement of healthcare [1]. A representative aspect of MHCS is that it can collect large amounts of sensitive health data pertaining to individuals. Because health data is usually sensitive and related to people’s lives, security and privacy protection measures should be enabled to eliminate erroneous data and prevent privacy violation [2]. In particular, the health data should be collected in a timely fashion to respond to latency-sensitive scenarios such as the medical emergency.

Y. Zhang is with the National Engineering Laboratory for Wireless Security, Xi’an University of Posts & Telecommunications, Xi’an 710121, China; Westone Cryptologic Research Center, Beijing 100070, China; and the School of Information Systems, Singapore Management University, Singapore 188065 (Corresponding author. e-mail: yzhzhang@163.com).

J. Shu is with the Department of Computer Science, City University of Hong Kong, Kowloon Tong, Hong Kong SAR, China (Corresponding author. e-mail: jgshu2-c@my.cityu.edu.hk).

X. Liu is with the School of Information Systems, Singapore Management University, Singapore 188065 (e-mail: snbnix@gmail.com).

J. Li is with the School of Computer Science, Guangzhou University, Guangzhou 510006, China. (e-mail: jinli71@gmail.com).

D. Zheng is with the National Engineering Laboratory for Wireless Security, Xi’an University of Posts & Telecommunications, Xi’an 710121, China; and Westone Cryptologic Research Center, Beijing 100070, China (Corresponding author. e-mail: zhengdong@xupt.edu.cn).

Copyright (c) 2012 IEEE. Personal use of this material is permitted. However, permission to use this material for any other purposes must be obtained from the IEEE by sending a request to pubs-permissions@ieee.org.

Quite recently, Liu et al. [3] proposed a large-scale concurrent data anonymous batch verification scheme for mobile healthcare crowd sensing, which is referred to as the MHCS scheme for convenience. In MHCS, an improved certificateless aggregate signature (CL-AS) serves as a fundamental building block. As illustrated in Figure 1, four types of entities are involved in MHCS: the management server (MS), the data center (DC), requestors, and MHCS participants. MS is responsible for the registration of each participant by issuing a half private key. DC aggregates and verifies the health sensing data collected by MHCS participants. Requestors submit healthcare sensing tasks to DC and obtain corresponding healthcare reports from DC. MHCS participants collect and submit health sensing data to DC based on various smart terminals.

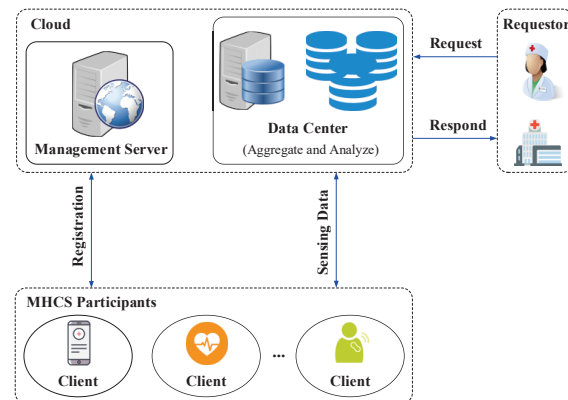


Fig. 1. The system model of MHCS.

In [3], only MS is trusted by other entities. Put another way, MHCS should be secure against possible attacks from other untrusted entities. For one thing, a malicious participant may submit erroneous data to DC and deny its malicious behaviors. For another, malicious (or compromised) DC may forge a signature on randomly chosen data to frame participants. To prove the security of the MHCS scheme, the authors gave a formal security proof (see Theorem 1 in Section III of [3]) of the improved CL-AS scheme under the Computational Diffie-Hellman (CDH) assumption. Furthermore, an informal security analysis is made on the basis of the CL-AS security to show that the MHCS scheme realizes *batch authentication*, *non-repudiation*, and *anonymity*. However, after a close look at their scheme, we find that not only any participant but also (compromised) DC can successfully forge a signature on any randomly chosen data. Thus, the MHCS scheme

cannot provide the properties of batch authentication and non-repudiation. In addition, based on a reasonable and rigorous probability analysis, we show that the security reduction from the security of the scheme to the hardness of the CDH problem is invalid.

II. REVIEW OF LIU ET AL.'S MHCS SCHEME

We first summarize the notations in Table I, and then briefly review the MHCS scheme [3] below.

TABLE I
NOTATIONS USED IN THE MHCS SCHEME.

Notation	Description
$s \in_R S$	The element s is randomly chosen from the set S .
$s_1 \parallel s_2$	The bit concatenation of two strings s_1 and s_2 .
\mathbb{G}_a (resp. \mathbb{G}_m)	A cyclic additive (resp. multiplicative) group of prime order q .
P	A generator of \mathbb{G}_a .
m_i	The health data collected by the participant with identity ID_i .
s_{MS} (resp. Q_{MS})	The private (resp. public) key of the management server.
s_{DC} (resp. Q_{DC})	The private (resp. public) key of the data center.
$s_{1,i}$	The half private key of the participant with identity ID_i .
$Q_{1,i}$	The partial public key of the participant with identity ID_i .

1) *Initialization*: Given a security parameter ℓ , the system is initialized as follows.

- MS first chooses a bilinear map $\hat{e} : \mathbb{G}_a \times \mathbb{G}_a \rightarrow \mathbb{G}_m$, where \mathbb{G}_a is a cyclic additive group and \mathbb{G}_m is a cyclic multiplicative group with the same prime order q . MS also chooses two hash functions $H_1 : \{0, 1\}^* \times \mathbb{G}_a \rightarrow \mathbb{G}_a$ and $H_2 : \{0, 1\}^* \times \mathbb{G}_a \rightarrow \mathbb{Z}_q^*$.
- Furthermore, MS picks $s_{MC} \in_R \mathbb{Z}_q^*$ as its private key and computes the corresponding public key $Q_{MS} = s_{MS}P$, where P is a generator of \mathbb{G}_a . Similarly, DC generates $\langle s_{DC}, Q_{DC} \rangle$ as its long-term key pair, where $Q_{DC} = s_{DC}P$.
- Finally, MS publishes system parameters

$$\langle \ell, q, P, \mathbb{G}_a, \mathbb{G}_m, \hat{e}, H_1, H_2, Q_{MS} \rangle.$$

2) *Registration*: As shown in Figure 2, to join the system, a participant C_i with identity id_i interacts with MS via a secure channel as follows.

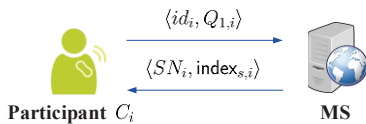


Fig. 2. The registration phase.

- C_i chooses $s_{1,i} \in_R \mathbb{Z}_q^*$ as its half private key, and sends $\langle id_i, Q_{1,i} \rangle$ to MS, where $Q_{1,i} = s_{1,i}P$.
- Upon receiving $\langle id_i, Q_{1,i} \rangle$, MS chooses $a_i \in_R \mathbb{Z}_q^*$ and computes $Q_{2,i} = H_1(id_i, Q_{1,i}), S_{2,i} = s_{MS}Q_{2,i}$ and

$$\text{index}_{s,i} = a_i S_{2,i}, \text{index}_{v,i} = a_i Q_{2,i}. \quad (1)$$

Then, MS locally stores $\langle id_i, Q_{1,i}, Q_{2,i}, \text{index}_{s,i}, \text{index}_{v,i} \rangle$, sets $SN_i = \text{index}_{v,i}$ and sends $\langle SN_i, \text{index}_{s,i} \rangle$ to C_i .

- C_i sets $\langle s_{1,i}, \text{index}_{s,i} \rangle$ as its final privacy key¹

¹In [3], $\text{index}_{s,i}$, instead of $S_{2,i}$, is used in the signature generation for identity anonymity (see Section IV of [3]).

3) *Signing*: Suppose m_i is the health data collected by C_i . C_i first chooses $k_i \in_R \mathbb{Z}_q^*$ and a timestamp t_i , which is the system time and can be used to check the freshness of corresponding messages, and then computes $V_i = k_i Q_{1,i}$, $h_i = H_2(m_i \parallel t_i, V_i)$,

$$U_i = \text{index}_{s,i} + k_i h_i s_{1,i} Q_{MS}, SN'_i = E_{Q_{DC}}(SN_i \parallel h_i \parallel t_i),$$

where E is a public key encryption algorithm. Finally, as shown in Figure 3, C_i uploads $\langle U_i, V_i, m_i, SN'_i \rangle$ to DC, which acts as a required health sensing data and can be verified based on Equation (2).

$$\hat{e}(U_i, P) = \hat{e}(\text{index}_{v,i} + h_i V_i, Q_{MS}). \quad (2)$$

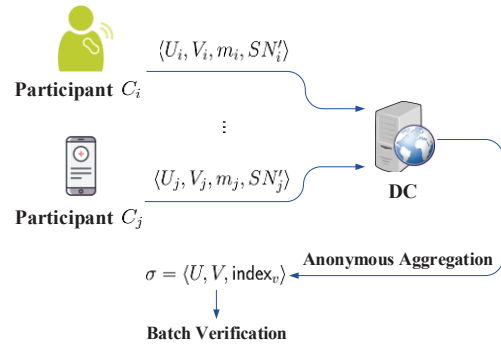


Fig. 3. The signing, anonymous aggregation and batch verification phases.

4) *Anonymous Aggregation*: As shown in Figure 3, DC acts as the aggregator of the system. For $1 \leq i \leq n$, upon receiving the health sensing data (i.e., authentication message) $\langle U_i, V_i, m_i, SN'_i \rangle$ from C_i before a given time T , DC performs the following procedures to aggregate them into a single authentication message.

- DC computes $D_{s_{DC}}(SN'_i) = SN_i \parallel h_i \parallel t_i$, where D is the decryption algorithm corresponding to E .
- DC generates $\sigma = \langle U, V, \text{index}_v \rangle$ as the aggregate authentication message on the health sensing data set $\langle m_1, m_2, \dots, m_n \rangle$, where

$$U = \sum_{1 \leq i \leq n} U_i, V = \sum_{1 \leq i \leq n} h_i V_i, \text{index}_v = \sum_{1 \leq i \leq n} \text{index}_{v,i}.$$

5) *Batch Verification*: DC thinks that σ is a valid aggregate authentication message if and only if Equation (3) holds.

$$\hat{e}(U, P) = \hat{e}(\text{index}_v + V, Q_{MS}). \quad (3)$$

If σ is valid, DC approves the health sensing data m_i uploaded by C_i within the time slot T for $1 \leq i \leq n$. Otherwise, DC aborts the health sensing data.

III. SECURITY ANALYSIS OF LIU ET AL.'S MHCS SCHEME

In this section, we first give an overview of attacks to the MHCS scheme, and then clearly illustrate the attack details. Finally, we show the security proof in [3] is invalid based on a rigorous probability analysis.

A. Overview of Attacks

In order to protect participants' identity privacy, the improved CL-AS scheme (see Section III of [3]), which fails to realize anonymity, cannot be directly exploited in the MHCS scheme (see Section IV of [3]). In MHCS, as shown in Equation (1), the partial private key and the corresponding public key are blinded by MS and then sent to the participant. In order to realize anonymity, in the signing phase, the participant encrypts the blinded public key and sends the ciphertext to DC. Finally, DC decrypts the ciphertext to obtain the blinded public key which is used in the subsequent verification, anonymous aggregation, and batch verification. Take the participant with identity ID_i as an example. It follows from Equation (2) that the decrypted blinded public key $\text{index}_{v,i} = SN_i$ is used in the verification. In other words, the relationship between the public key $Q_{1,i}$ and the partial private key $S_{2,i}$ is not required for generating a valid signature in that $\text{index}_{v,i}$ is not computed based on $Q_{1,i}$ in the verification. Particularly, the process of blindness in Equation (1) is based on a random parameter and the master secret key is not involved. Therefore, any participant can further blind its partial secret key $\text{index}_{s,i}$ and public key $\text{index}_{v,i}$ to forge a signature on any message, which corresponds to the scenario of **Attack I** in Section III-B. Additionally, if DC is malicious or the private key of DC is leaked, then the adversary can forge a signature on any message based on a previous valid health sensing data from any participant, which corresponds to the scenario of **Attack II** in Section III-C.

B. Attack I: Forgery Attacks from Participants

Suppose participant C_i has a final private key $\langle s_{1,i}, \text{index}_{s,i} \rangle$. We know $\text{index}_{s,i} = a_i S_{2,i}$, $S_{2,i} = s_{MS} Q_{2,i}$, $Q_{2,i} = H_1(id_i, Q_{1,i})$, and $Q_{1,i} = s_{1,i} P$. Then, as shown in Figure 4, for any randomly chosen health sensing data $m_j^* \in_R \{0, 1\}^*$ with $j \neq i$, C_i can forge a signature message $\langle U_j^*, V_j^*, m_j^*, SN_j^{*'} \rangle$ below:

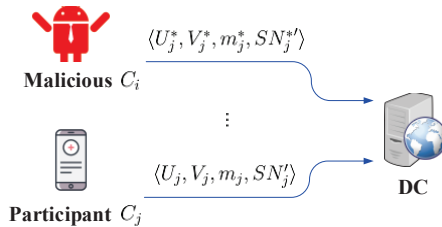


Fig. 4. The scenario of attack I.

Forgery Attack: C_i performs the following procedures.

- 1) Choose $s_{1,j}^*, k_j^* \in_R \mathbb{Z}_q^*$, and set $Q_{1,j}^* = s_{1,j}^* P$, $V_j^* = k_j^* Q_{1,j}^*$.
- 2) Compute $h_j^* = H_2(m_j^* \| t_j^*, V_j^*)$, where t_j^* is the current system time and is used as a timestamp.
- 3) Choose $a_j^* \in_R \mathbb{Z}_q^*$ and set

$$\text{index}_{s,j}^* = a_j^* \text{index}_{s,i}, SN_j^{*'} = a_j^* SN_i \text{ (i.e., } a_j^* \text{index}_{v,i}).$$

- 4) Compute $U_j^* = \text{index}_{s,j}^* + k_j^* h_j^* s_{1,j}^* Q_{MS}$.
- 5) Compute $SN_j^{*'} = E_{Q_{DC}}(SN_j^{*'} \| h_j^* \| t_j^*)$.
- 6) Send $\langle U_j^*, V_j^*, m_j^*, SN_j^{*'} \rangle$ to DC.

Verification: The forged signature message $\langle U_j^*, V_j^*, m_j^*, SN_j^{*'} \rangle$ can be verified by DC as follows.

- 1) Compute $D_{s_{DC}}(SN_j^{*'}) = SN_j^* \| h_j^* \| t_j^*$.
- 2) Ensure $h_j^* = H_2(m_j^* \| t_j^*, V_j^*)$, and set $\text{index}_{v,j}^* = SN_j^*$.
- 3) Think that $\langle U_j^*, V_j^*, m_j^*, SN_j^{*'} \rangle$ is valid if and only if

$$\hat{e}(U_j^*, P) = \hat{e}(\text{index}_{v,j}^* + h_j^* V_j^*, Q_{MS}). \quad (4)$$

Anonymous Aggregation: For $1 \leq j \leq n$, upon receiving the forged signature message $\langle U_j^*, V_j^*, m_j^*, SN_j^{*'} \rangle$, DC performs the procedure 1) and procedure 2) in the above verification phase. Then, DC aggregates the messages into a single authentication message $\sigma^* = \langle U^*, V^*, \text{index}_{v,i}^* \rangle$, where

$$U^* = \sum_{1 \leq j \leq n} U_j^*, V^* = \sum_{1 \leq j \leq n} h_j^* V_j^*, \text{index}_{v,i}^* = \sum_{1 \leq j \leq n} \text{index}_{v,j}^*. \quad (5)$$

Batch Verification: $\langle U^*, V^*, \text{index}_{v,i}^* \rangle$ is a valid aggregate authentication message on the health sensing data set $\langle m_1^*, m_2^*, \dots, m_n^* \rangle$ if and only if

$$\hat{e}(U^*, P) = \hat{e}(\text{index}_{v,i}^* + V^*, Q_{MS}). \quad (6)$$

Correctness: Equation (4) is correct because

$$\begin{aligned} \hat{e}(U_j^*, P) &= \hat{e}(\text{index}_{s,j}^* + k_j^* h_j^* s_{1,j}^* Q_{MS}, P) \\ &= \hat{e}(a_j^* \text{index}_{s,i} + k_j^* h_j^* s_{1,j}^* Q_{MS}, P) \\ &= \hat{e}(a_j^* a_i S_{2,i} + k_j^* h_j^* s_{1,j}^* Q_{MS}, P) \\ &= \hat{e}(a_j^* a_i Q_{2,i} + k_j^* h_j^* s_{1,j}^* P, Q_{MS}) \\ &= \hat{e}(\text{index}_{v,j}^* + h_j^* V_j^*, Q_{MS}). \end{aligned} \quad (7)$$

It easily follows from Equation (5) and Equation (7) that Equation (6) holds. Therefore, the above attack I is correct.

C. Attack II: Forgery Attacks from (Compromised) DC

In this case, the adversary is either the malicious DC, which wants to frame other participants by forging signatures, or any participant that gets the private key of (compromised) DC. As shown in Figure 5, given a valid health sensing data $\langle U_j, V_j, m_j, SN_j' \rangle$ from C_j , the adversary can forge a signature message $\langle U_j^*, V_j^*, m_j^*, SN_j^{*'} \rangle$ below for any randomly chosen health sensing data $m_j^* \in_R \{0, 1\}^*$.

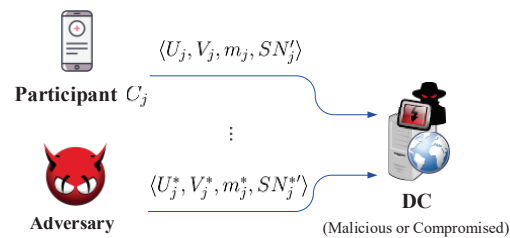


Fig. 5. The scenario of attack II.

Forgery Attack: DC performs the following procedures.

- 1) Compute $D_{s_{DC}}(SN_j') = SN_j \| h_j \| t_j$.
- 2) Set $V_j^* = V_j$ and compute $h_j^* = H_2(m_j^* \| t_j^*, V_j^*)$, where t_j^* is the current system time and is used as a timestamp.
- 3) Set $U_j^* = h_j^* h_j^{-1} U_j$.
- 4) Set $SN_j^* = h_j^* h_j^{-1} SN_j$ and $SN_j^{*'} = E_{Q_{DC}}(SN_j^* \| h_j^* \| t_j^*)$.

5) Use $\langle U_j^*, V_j^*, m_j^*, SN_j^* \rangle$ as a signature message.

Verification, Anonymous Aggregation, and Batch Verification are the same as those in **Attack I**.

Correctness: The above attack II is correct because

$$\begin{aligned}
 \hat{e}(U_j^*, P) &= \hat{e}(h_j^* h_j^{-1} U_j, P) \\
 &= \hat{e}(h_j^* h_j^{-1} (\text{index}_{s,j}^* + k_j h_j s_{1,j} Q_{MS}), P) \\
 &= \hat{e}(h_j^* h_j^{-1} (a_j S_{2,j} + k_j h_j^* s_{1,j} Q_{MS}), P) \\
 &= \hat{e}(h_j^* h_j^{-1} (a_j Q_{2,j} + h_j^* V_j), Q_{MS}) \\
 &= \hat{e}(h_j^* h_j^{-1} S N_j + h_j^* V_j^*, Q_{MS}) \\
 &= \hat{e}(\text{index}_{v,j}^* + h_j^* V_j^*, Q_{MS}),
 \end{aligned}$$

where $\text{index}_{v,j}^* = S N_j^*$ and h_j^* are specified in the procedure 2) of **Verification**.

D. Invalid Security Reduction in the Security Proof

The MHCS scheme [3] is based on an improved CL-AS scheme. The formal security proof (see Theorem 1 in Section III of [3]) shows a reduction from the security of the improved CL-AS scheme to the hardness of the CDH problem. However, we find that the security reduction in the security proof is invalid. In the proof, the challenger C , who plays the role of a solver of the CDH problem, is given a random CDH instance (P, aP, bP) , where $a, b \in_R \mathbb{Z}_q^*$. C sets $Q_{KGC} = aP$ (i.e., $Q_{MS} = aP$). In the new queries to H_1 , C flips a coin $c_i \in \{0, 1\}$ such that $c_i = 0$ with probability λ and $c_i = 1$ with probability $1 - \lambda$. Then, C chooses $\alpha_i \in_R \mathbb{Z}_q^*$. If $c_i = 0$, C sets $Q_{2,i} = \alpha_i(bP)$. Otherwise, $c_i = 1$, it sets $Q_{2,i} = \alpha_i P$. In the extraction queries, C returns failure if $c_i = 0$, and otherwise returns corresponding partial private key. In the signing queries, if $c_i = 1$, C returns failure and otherwise returns a signature.

In the analysis of the success probability of C , three events E_1, E_2, E_3 are defined. E_1 : C does not return failure in any extraction queries from the adversary; E_2 : The adversary generates (i.e., forges) a valid signature that can be verified; and E_3 : The adversary outputs a valid forgery and C does not return failure. It easily follows that $\Pr[E_1] \geq (1 - \lambda)^{q_k}$ and $\Pr[E_2|E_1] \geq \epsilon$, where q_k represents the number of extraction queries, and ϵ is the advantage of the adversary in attacking the CL-AS scheme.

New Probability Analysis: As for $\Pr[E_3|E_1 \wedge E_2]$, it is claimed in [3] that $\Pr[E_3|E_1 \wedge E_2] \geq \lambda$. However, that's not true and in fact $\Pr[E_3|E_1 \wedge E_2] \geq \lambda^{q_{sig}}$ in that there are q_{sig} signing queries. In this case, the probability for C to succeed in solving the CDH problem is

$$\begin{aligned}
 \text{Adv}_{\text{CDH}}^C &= \Pr[E_1 \wedge E_2 \wedge E_3] \\
 &= \Pr[E_1] \cdot \Pr[E_2|E_1] \cdot \Pr[E_3|E_1 \wedge E_2] \\
 &\geq (1 - \lambda)^{q_k} \cdot \epsilon \cdot \lambda^{q_{sig}}.
 \end{aligned}$$

Define $q_{min} = \min\{q_{min}, q_{sig}\}$. Note that

$$\begin{aligned}
 (1 - \lambda)^{q_k} \cdot \epsilon \cdot \lambda^{q_{sig}} &\leq (1 - \lambda)^{q_{min}} \cdot \epsilon \cdot \lambda^{q_{min}} \\
 &= (\lambda - \lambda^2)^{q_{min}} \cdot \epsilon \leq \frac{\epsilon}{4^{q_{min}}}.
 \end{aligned}$$

Obviously, $\frac{1}{4^{q_{min}}}$ is negligible when q_{min} is large enough. Thus, it cannot be concluded from $\text{Adv}_{\text{CDH}}^C \geq \frac{\epsilon}{4^{q_{min}}}$ that $\text{Adv}_{\text{CDH}}^C$

is non-negligible, which means the security reduction in the formal security proof [3] is invalid.

IV. CONCLUSION

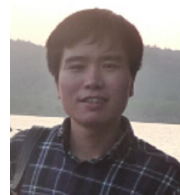
We analyzed the security of a large-scale concurrent data anonymous batch verification scheme [3], and showed that two types of signature forgery attacks exist and hence the scheme fails to achieve the claimed properties of batch authentication and non-repudiation. In addition, we showed that the security reduction in the formal security proof is invalid. We remark that it is still an open problem to design an efficient anonymous batch verification scheme for mobile healthcare crowd sensing.

ACKNOWLEDGMENT

We are grateful to the editors and anonymous referees for their invaluable suggestions. This work was supported in part by the National Key R&D Program of China under Grant 2017YFB0802000, in part by the National Natural Science Foundation of China under Grant 61772418, Grant 61472472, Grant 61472091, and Grant 61402366, and in part by Natural Science Basic Research Plan in Shaanxi Province of China under Grant 2018JZ6001, and Grant 2015JQ6236. The work of J. Li was supported by the National Natural Science Foundation for Outstanding Youth Foundation under Grant 61722203 and the Natural Science Foundation of Guangdong Province for Distinguished Young Scholars under Grant 2014A030306020. The work of Y. Zhang was supported by the New Star Team of Xi'an University of Posts and Telecommunications under Grant 2016-02.

REFERENCES

- [1] N. D. Lane, E. Miluzzo, H. Lu, D. Peebles, T. Choudhury, and A. T. Campbell, "A survey of mobile phone sensing," *IEEE Communications magazine*, vol. 48, no. 9, 2010.
- [2] Y. Zhang, D. Zheng, and R. H. Deng, "Security and privacy in smart health: efficient policy-hiding attribute-based access control," *IEEE Internet of Things Journal*, vol. 5, no. 3, pp. 2130–2145, 2018.
- [3] J. Liu, H. Cao, Q. Li, F. Cai, X. Du, and M. Guizani, "A large-scale concurrent data anonymous batch verification scheme for mobile healthcare crowd sensing," *IEEE Internet of Things Journal*, 2018. [Online]. Available: <https://ieeexplore.ieee.org/abstract/document/8341503/>



Yinghui Zhang received his Ph.D degree in Cryptography from Xidian University, China, in 2013. He is an associate professor at National Engineering Laboratory for Wireless Security (NELWS), Xi'an University of Posts & Telecommunications. Currently, he is also a research fellow at Singapore Management University. He has published over 60 research articles including ASIACCS, IEEE Transactions on Services Computing, Computer Networks, IEEE Internet of Things Journal, Computers & Security. His research interests include cloud security, network security, security and privacy in IoT, and public key cryptography.



Jiangan Shu received the BE degree and the MS degree from Nanjing University of Information Science and Technology, Nanjing, China, in 2012 and in 2015, respectively. Since 2015, he has been working toward the PhD degree in computer science at the Department of Computer Science, City University of Hong Kong, Hong Kong. His research interests include cloud computing security, security and privacy in crowdsourcing, and network security.



Ximeng Liu received his Ph.D. degrees in Cryptography from Xidian University, China, in 2015. Now, he is a research fellow at School of Information System, Singapore Management University, Singapore. He has published over 80 research articles including IEEE Transactions on Information Forensics and Security, IEEE Transactions on Dependable and Secure Computing, IEEE Transactions on Services Computing, etc. His research interests include cloud security and big data security.



Jin Li is currently a professor of School of Computer Science, Guangzhou University. He got his Ph.D degree in information security from Sun Yat-sen University at 2007. He served as a senior research associate at Korea Advanced Institute of Technology (Korea) and Illinois Institute of Technology (U.S.A.) from 2008 to 2010, respectively. His research interests include secure cloud storage and outsourcing computation. He has published more than 100 papers. His work has been cited more than 10000 times at Google Scholar.



Dong Zheng received his Ph.D. degree in communication engineering from Xidian University, China, in 1999. He is currently a Professor at National Engineering Laboratory for Wireless Security (NELWS), Xi'an University of Posts & Telecommunications. He has published over 100 research articles including CT-RSA, IEEE Transactions on Services Computing, IEEE Communications Magazine, IEEE Transactions on Industrial Electronics, etc. His research interests include cloud security, wireless network security and code-based cryptography.