Cryptoanalysis on a Cloud-Centric Internet-of-Medical-Things-Enabled Smart Healthcare System

RONGHUA XU¹ AND QIAOCHUAN REN²
¹Graduate School, Shanghai University of Finance and Economics, Shanghai 200433, China
²School of Information and Control Engineering, Xi’an University of Architecture and Technology, Xi’an, Shaanxi 710055, China

This work was supported in part by the Project of Natural Science Research in Shaanxi under Grant 2019JM118; and in part by the Project of State Key Laboratory of Information Security, Chinese Academy of Sciences, under Grant 2021MS-04.

ABSTRACT The interconnecting of the biomedical sensors (in healthcare system) with cloud for the internet-of-medical-things (IoMT) technology has great potential to ameliorate people’s living conditions. The privacy-preserving of personal health information (PHI) and the mutual authentication between the sensors and other entities are two main factors that affect the further applications of cloud-centric IoMT technology. In the recent work [IEEE IoT Journal, vol. 7(10), 10650-10659, 2020], Kumar and Chand applied identity-based aggregate signcryption scheme to the smart healthcare system (KC-system, for short), which provides privacy-preserving of PHI and the mutual authentication function, simultaneously. However, in this paper, we carefully analyze the security of KC-system and find out that the critical authentication keys of entities can be easily recovered from their communication contents. In other words, the mutual authentication function of KC-system can be easily broken. Moreover, the recovering of the keys will lead to the tedious processes, including obtaining partial private key (from network manager) and requesting for key-protection (from key-protection servers), become completely useless. Finally, we also twist their protocol into a new one, which can be proven secure against the previous attack.

INDEX TERMS Security analysis, Internet of Medical Things (IoMT), cloud computing, smart healthcare system.

I. INTRODUCTION Wireless body area network (WBAN) is an emerging paradigm in ubiquitous healthcare, whereby sensors, that are implanted or worn on human body, collect and send real-time patient’s personal health information (PHI) data such as breathing rate, heart rate and blood pressure and so on [1]. Typically, WBAN is a kind of network consisting of various tiny sensors, which have limited power, storage as well as computing ability. After collecting patient’s PHI, they transmit it to medical professional (or data consumer) via this public network [2].

From security perspective, any attack on the sensors or unauthorized access to the network may result in life-threatening risk to the patients since the transmitted data is just their sensitive PHI [3]. Obviously, the security and privacy problems are the first challenge for the further applications of WBAN [4]. The second challenge lies in that day-to-day increasing transmission of PHI data overburdens the resource-constraint cellular network [5], [6]. Many literatures find that the recent cloud-enabled internet of things (IoT) can be potentially served the data storage and computing power [7]–[10]. Another advantage of combing cloud with e-health monitoring system is that the remote diagnosing from an authorized medical entity becomes more convenient. However, some new security risks, such as a semi-trusty cloud may be curious to inappropriately access patient’s PHI [11], also appear. In addition, how to validate the integrity of the stored PHI on cloud is another critical problem for the cloud-based smart healthcare system [12].

In order to solve the above security and privacy-preserving problems, kinds of cryptographic techniques, like encryption and signature, are considered for the cloud-centric IoMT system to simultaneously ensure privacy and authenticity.
In general, encryption and signature can be composed in several ways: Sign-and-encrypt, sign-then-encrypt, and encrypt-then-sign. Each implementation mode is a simple composition of encryption and signature schemes, and thus is inefficient for the IoMT healthcare system.

It is also well-known that signcryption is an important public-key cryptographic primitive, which can achieve authentication and privacy simultaneously with a much smaller cost. Like other public-key cryptographic primitives [13], [14], signcryption scheme has also to face the problem that how to fix the relation between the public-key and its true entity. Identity-based signcryption (IBSC) scheme (see [15]–[20]) can easily bypass this issue since entity’s public-key is just its public information, such as email address, identity-card number, and so on. But the key-escrow problem (i.e. any entity’s private key is known to the key-generation center) still exists in IBSC schemes. Therefore, researchers suggested the notion of certificateless signcryption scheme and tried to use it to the cloud-centric IoMT healthcare system.

In the recent work [21], Kumar and Chand pointed out that, compared with IBSC, certificateless signcryption cannot achieve the identity-based nature. Therefore, they proposed an escrow-free identity-based aggregated signcryption (EF-IBASC) scheme and constructed a device-to-device aggregated-data communication protocol (see [22]) for cloud-centric smart healthcare system (KC-system, for short), whose security is based on the underlying EF-IBASC scheme. As Kumar et al. claimed, their healthcare system has many merits including PHI’s privacy-preserving, mutual authenticity of the entities, because the underlying signcryption scheme can simultaneously provide encryption and signature functions.

Unfortunately, in this paper, we will prove that the critical authentication function of the KC-system cannot be guaranteed because the authentication key(s) can be easily recovered from the communication contents transmitted in the network. In other words, one of the two guarantees (i.e. authentication and privacy) for Kumar et al.’s signcryption scheme is completely broken.

Next, we briefly introduce the underlying idea of our attack and then discuss its consequences.

Recall that, in KC-system, each entity $E$ needs to register and obtain its authentication key $d_E$ from the network manager (NM). In order to avoid the key-escrow problem, the NM only returns a partial private key for $E$. Moreover, for key’s security, $E$ also requests for key protection from many key-protection servers (KPSs), who return the corresponding shares. The key $d_E$ is computed by combining the partial private key (from NM) with the shares (from KPSs).

In the process of data transmission, the $j$th biomedical sensor (BMS) computes the encryption of the PHI data and signature (under the authentication key $d^j_{BMS}$). Then send the aggregated message $CT_j$ to personal-assisted device (PAD).

Note that, $CT_j$ contains the two items:

$$C_{aggr,j} \in \mathbb{Z}_q^n, \text{ and } E_j = C_{aggr,j}d^j_{BMS} \in \mathbb{G}_1,$$

where $\mathbb{G}_1$ is an additional group with large prime-order $q$. According to the basic number theory [23], we know that the authentication key $d^j_{BMS}$ can be easily recovered from $E_j$ if $C_{aggr,j}$ is public. Hence, the authentication key $d^j_{BMS}$ (of this BMS) is no longer secure. Similarly, other entities’ authentication keys can also be recovered.

The consequences of this attack contain the following two aspects:

1) The exposure of the authentication key leads to the tedious generation of $d_E$ be completely useless.

2) The mutual authentication function of the KC-system does not work. As a result, malicious adversary may pretend to be legal entity to join in the system and try to break the smart healthcare system.

3) The “public verifiability” algorithm cannot achieve the expected function.

A. RELATED WORKS

In [24], Akinyele et al. proposed an electronic medical record (EMR) with self-protecting by invoking attribute-based encryption technique. Similarly, Hu et al. also discussed the secure communication between a body area network and its data consumer, which still is attribute-based [25]. In [26], Li et al. gave the suggestions on using identity-based signcryption for low-power devices, such as sensors in an online/offline setting that simultaneously satisfies the authentication and confidentiality without authenticating a recipient’s public key additionally. However, this scheme suffers from the famous key-escrow attack. Hence, in [12], Omala et al. presented a certificateless signcryption scheme with the property of lightweight with the help of certificateless cryptographic technique. Later, Zhang et al. extended Omala et al.’s technique and also discussed the data communication scheme for e-health system using a generalized signcryption scheme [27]. Unfortunately, in [28], Zhou pointed out that Zhang et al.’s protocol is susceptible to insider’s attack, which means that it is insecure and vulnerable for data confidentiality.

In the previous literatures, kinds of cryptographic primitives based on bilinear map have been discussed for healthcare system. Compared with identity-based ones, certificateless-based schemes focused on the key-escrow-free problem but could not achieve the identity-based property. This is also the motivation of escrow-free identity-based aggregated signcryption scheme for the smart healthcare system.

B. ORGANIZATIONS

The following parts are organized as follows. In Section II, we introduce the system model of IoMT-enabled smart healthcare system. Next, in Section III, we present our attack...
on the KC-system and discuss the consequences of this attack. Then present our proposed solution in Section IV. Finally, conclusions are given in Section V.

II. PRELIMINARIES

A. HARDNESS ASSUMPTION

First, we would like to introduce the hardness assumption based on Okamoto’s conference-key sharing scheme (CONF) [29]. Concretely, for a cyclic group $G$ with prime-order $q$ and generator $P$. For randomly chosen $x, y \in \mathbb{Z}_q$, given the tuple $(g, xg, (xy)g) \in G^3$, an algorithm $A$ intends to compute and output $g^y \in G$. If for any probabilistic polynomial time adversary $A$, the probability that it can successfully output $g^y$ is negligible, then we call that the CONF assumption holds.

B. SYSTEM MODEL OF IoMT-ENABLED SMART HEALTHCARE SYSTEM

In this section, we introduce the system model of IoMT-enabled smart healthcare system. As depicted in Fig. 1, it consists of the following six entities.

- **Network Manager (NM).** This entity initializes the whole system, and generates the system parameters as well as its own master secret key. In order to avoid the key-escrow problem of the previous identity-based authentication scheme, the NM is viewed as a semi-trusted entity. Therefore, given the identity $ID_1$, it only returns a partial private key.
- **Key-Protection Servers (KPSs).** These entities provide the key-protection services for user’s private key. More precisely, they generate their public-secret key pairs, and then compute independent shares to user’s protected private key.
- **Biomedical Sensor (BMS).** The whole system includes many BMSs. Each BMS is a tiny sensor and has very limited storage space, battery life as well as computing power. All the BMSs are installed on/oustrside the patient’s body (i.e. some wearable sensors), or deployed in the patient’s tissues (i.e. some implanted sensors).
- **Personal-Assisted Device (PAD).** This entity is a data sink, which has sufficient computing power and storage space. In the system, the PAD collects real-time PHI data transmitted from several BMSs and transfers patient’s PHI to cloud server for storing (after signing it based on its private key). In fact, it is viewed as not trustworthy entity in Kumar et al.’s model because they think that, for an adversary, it is effortless to physically steal or statistically attack it.
- **Medical Cloud Server (MCS).** This entity provides storing services for the PHI transferred from PAD. In addition, it also provides the accessability of the stored PHI to SD. It is viewed as a semi-trusted entity.
- **Service Device (SD).** This device is on the medical institution’s side, which is allowed to access the PHI stored on MCS, and diagnoses the patient’s diseases (based on PHI). Finally, send the prescription to the corresponding BMS in the reverse direction.

III. SECURITY ANALYSIS ON THE KC-SYSTEM

In this section, we analyze the security of the KC-system. In particular, we will first prove that the authentication keys for BMS and PAD can be easily recovered, and then analyze its consequences.

A. INSECURITY OF ENTITIES’ AUTHENTICATION KEYS

Note that, in the final phase of algorithm “Entity’s Authentication and Registration”, each entity $E \in \{\text{BMS, PAD, SD}\}$ obtains the authentication key

$$d_E = s_0(s_1 + s_2 + \cdots + s_n)H_1(ID_E) \in G_1,$$

which should be secret to anyone else. However, we will analyze that these authentication keys can be recovered by anyone who eavesdrops the transmitted contents among the entities.

Concretely, recall that, in the algorithm “PHI Aggregate Signcryption”, the $j$th BMS signs and encrypts the original PHI messages $M_{1,j}, M_{2,j}, \cdots, M_{m,j}$ into

$$(C_{1,j}, D_{1,j}), (C_{2,j}, D_{2,j}), \cdots, (C_{m,j}, D_{m,j}),$$
R. Xu, Q. Ren: Cryptoanalysis on Cloud-Centric Internet-of-Medical-Things-Enabled Smart Healthcare System

and then aggregates them into

\[ C_{agg} = H_t(C_{1,j}, C_{2,j}, \ldots, C_{m,j}) \in \mathbb{Z}_q^*, \]

\[ E_j = C_{agg,j}^d_{BMS}. \]

Finally, send CT\(_j\) = \{A\(_j\), B\(_j\), C\(_{agg,j}\), \(\sum_i D_{i,j}\), E\(_j\)\} to PAD.

Here, we know that any eavesdropper can see the transmitted CT\(_j\), which includes C\(_{agg,j}\) and E\(_j\). From the two items, the eavesdropper can recover the authentication key d\(_{BMS}\) of this BMS as follows.

From C\(_{agg} \in \mathbb{Z}_q^*\) and the prime q, one can easily know that there exist integer \(\mu\) such that

\[ \mu C_{agg} \equiv 1 \ mod \ q, \]

which can be obtained by Extended-Euclidean algorithm. Hence, it holds that

\[ \mu E_j = \mu C_{agg,j}^d_{BMS} = (\mu C_{agg,j})^d_{BMS} = 1d_{BMS} = d_{BMS}. \]

As a result, anyone seeing the content CT\(_j\) can easily compute and recover the authentication key d\(_{BMS}\) of the jth BMS.

In addition, from the description of the algorithm “PHI Re-Aggregation”, we know that the PAD will send CT\(_{PAD}\) = \{A\(_j\), B\(_j\), C\(_{PAD}\), C\(_{agg,j}\), \(\sum_i D_{i,j}\), E\(_j\), F\} \in \mathbb{Z}_q^*\) and F = C\(_{PAD}\)D\(_{PAD}\), to the MCS. Similarly, any eavesdropper can easily compute and recover the authentication key d\(_{PAD}\) of the PAD from F.

As Kumar and Chand suggested, after obtaining the patient PHI, SD diagnoses it and returns the signedcrypted prescription P by using a similar algorithm as “PHI Aggregate Signcryption”. In this case, anyone can also recover SD’s authentication key by performing a similar analysis as recovering d\(_{BMS}\).

In all, the authentication keys can be recovered by any eavesdropper who only needs to observe the communication contents among the entities.

**B. THE CONSEQUENCE I**

Now, we discuss the first consequence (denoted by Consequence I) of the above attack.

Recall that, in the system-setup step of the KC-system, the NM initializes the system, authenticates the entity with identity ID, and issues partial private key, which is further protected by multiple KPSs, to it. Meanwhile, the KPSs forward the protected private key shares to the entity, who finally combines the shares and extracts its authentication key d\(_E\). We remark that the ultimate goal of these processes is to guarantee that the entity can correctly extract the key d\(_E\).

Since, in our attack, any eavesdropper can easily recover the authentication key d\(_E\), the tedious processes, such as requesting partial private key (from NM) and asking for key-protection (from multiple KPSs), are of no use. Therefore, the first consequence under our attack is that many steps in the algorithms “System Setup” and “Entity’s Authentication and Registration” (especially for the latter one) become useless and thus can be “cut” from the KC-system.

**C. THE CONSEQUENCE II**

Here, we discuss the second consequence (denoted by Consequence II) of our attack. In particular, the exposure of d\(_E\) (for \(E \in \{BMS, PAD, SD\}\)) will result in loss of the authentication function of the whole KC-system. In other words, malicious adversary may pretend to be legal entity to join in the system and thus break the smart healthcare system.

Next, we take “malicious BMS” (denoted by BMS\(^*\)) for example to show it. According to the description of our attack, BMS\(^*\) can easily recover the authentication key d\(_{BMS}\) of the jth BMS, who is a legal entity in the system. Then it can pretend to BMS\(_j\) and interact with other entities as follows.

Randomly choose a\(^*\) \in \mathbb{Z}_q^*\) and compute

\[ A^* = a^*H_1(ID_{BMS}), B^* = a^*P. \]

Then set \(K^* = e(a^*d_{BMS}, H_1(ID_{SD}))\) and compute

\[ S^k = H_2(ID_{SD}, A^*, K^*, S^{k-1}). \]

Aggregate the PHI as

\[ C_{agg} = H_4(C^*_1, C^*_2, \ldots, C^*_m), \text{ and } E^* = C_{agg}d_{BMS}. \]

Finally, send CT\(_*\) = \{A\(_*\), B\(_*\), C\(_{agg}\), \(\sum_i D_{i,*}\), E\(_*\)\} to PAD.

Note that this CT\(_*\) can pass the public verifiability since it holds that

\[ e(E^*, B^*) = e(C^*_{agg}d_{BMS}, a^*P) = e(C^*_{agg}, s_0 + s_2 + \ldots + s_n)H_1(ID_{BMS}, a^*P) = e(a^*H_1(ID_{BMS}, s_0 + s_2 + \ldots + s_n)P)C^*_{agg} = e(A^*, Y)C^*_{agg}. \]

Obviously, the legal entity BMS\(_j\) is successfully replaced by a malicious adversary BMS\(^*\), but the KC-system cannot detect and avoid it. Therefore, the mutual authentication function as Kumar et al. claimed is broken.

**D. INVALID PUBLIC VERIFIABILITY ALGORITHM**

An adversarial cloud server can pass the algorithms “Public Verifiability” auditing, even if it does not well maintain the outsourced data. In other words, the “Public Verifiability” algorithm cannot achieve the expected function.

Specifically, \(\sum_i D_{i,j}\) in the data packet

\[ CT_{PAD} = \{A_j, B_j, C_{PAD}, C_{agg,j}, \sum_i D_{i,j}, E_j, F\} \]
sent to the cloud by user U can be arbitrarily deleted or modified by the cloud, while \( \sum_j D_{ij} \) is the most important in the entire data package, because the user’s personal health information \( M_{ij} \) and \( T_{ij} \) are XORed with \( S_j^k \) and then stored in \( D_{ij} \).

For example, we assume that the encrypted data \( CT_{PAD} = \{ A_j, B_j, C_{PAD}, C_{aggr,j}, \sum_i D_{ij}, E_j, F \} \) on the MCS has been modified to

\[
CT_{PAD}^* = \{ A_j, B_j, C_{PAD}, C_{aggr,j}, \sum_i D_{ij}, E_j, F \},
\]

and the verifier runs the algorithm “Public Verifiability”. At this time, \( CT_{PAD}^* \) can still be passed by two equations of “Public Verifiability”:

\[
e(F, P) = e( Q_{PAD}, Y) \]

and

\[
e(E_j, B_j) = e(A_j, Y)^{C_{aggr,j}}.
\]

Therefore, the MCS passes the verifier’s auditing, even if \( CT_{PAD} \) is modified to \( CT_{PAD}^* \). The expected public verifiability function is invalid.

### IV. OUR PROPOSED SCHEME

First, we present the twisted KC-scheme, which is based on the original KC-scheme and consists of the following algorithms:

- **System Setup.** For the security parameter \( \lambda \), the NM generates a bilinear map \( e : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2 \), where \( \mathbb{G}_1 \) and \( \mathbb{G}_2 \) are additive and multiplicative groups, respectively, with the same prime-order \( q \). Let \( P \) be \( \mathbb{G}_1 \)'s generator and denote by \( m, \ell, t \) the sizes of message, identity and timestamp (in bits). Then five hash functions are chosen as follows. \( H_1 : \{0, 1\}^t \rightarrow \mathbb{G}_1 \), \( H_2 : \{0, 1\}^* \rightarrow \{0, 1\}^{m+|e| \times \ell} \times \mathbb{G}_1 \), \( H_3 : \mathbb{G}_2 \times \{0, 1\}^n \rightarrow \mathbb{Z}_q^* \), \( H_4 : \mathbb{G}_1^m \rightarrow \mathbb{Z}_q^* \), and \( H_5 : \mathbb{Z}_q^* \times \mathbb{G}_1 \rightarrow \mathbb{Z}_q^* \). Next, the NM randomly chooses \( s_0 \) from \( \mathbb{Z}_q^* \) and defines the public key as \( P_0 = s_0 P \). Broadcast \( P_0 \) to each KPS, who also randomly chooses \( s_j \in \mathbb{Z}_q^* \), defines \( P_j = s_j P_0 \), and returns \( P_j \) to the NM. Finally, the NM generates the system public key as

\[
Y = \sum_{i=1}^n P_i = s_0(s_1 + s_2 + \cdots + s_n)P.
\]

- **Entity’s Authentication and Registration.** Let \( E \in \{ \text{BMS}, \text{PAD}, \text{SD} \} \) and \( ID_E \) be its identity. First, \( E \) randomly chooses \( x_E \in \mathbb{Z}_q^* \), computes

\[
X_E = x_E P, \quad D_E = x_E H_1(ID_E),
\]

and sends \( (ID_E, X_E, D_E) \) to NM, who computes and returns the partial private key

\[
(X_{E0}, D_{E0}) = (s_0X_E, s_0D_E).
\]

Then \( E \) requests to KPS\(^i\) for key protection, who computes and returns \( D_{EI} = s_iD_{E0} \) to \( E \). Finally, \( E \) recovers the (full) private key

\[
d_E = x_E^{-1} \sum_{i=1}^n D_{EI} = s_0(s_1 + s_2 + \cdots + s_n)H_1(ID_E).
\]

- **PHI Aggregate Signcryption.** The \( j \)th BMS first randomly chooses \( a_j \in \mathbb{Z}_q^* \) and computes

\[
A_j = a_j H_1(ID_{BMS}^j), \quad B_j = a_j P.
\]

Then set \( K_j = e(a_jd_{BMS}^j, H_1(ID_{SD})) \), and compute

\[
S_j^k = H_2(ID_{SD}, A_j, K_j, S_j^{k-1}), \quad \text{where } S_j^{k-1} \text{ is the previous key.}
\]

For the timestamp \( T_{ij} \in \{0, 1\}^l \) and PHI \( M_{ij} \in \{0, 1\}^m \), the \( j \)th BMS computes \( h_{i,j} = H_3(M_{ij}, A_j, T_{ij}) \) and

\[
C_{i,j} = (a_j + h_{i,j})d_{BMS}^j, \quad D_{i,j} = \left(M_{ij}||C_{i,j}||ID_{BMS}^j||T_{ij}\right) \oplus S_j^k,
\]

where \( 1 \leq i \leq m, 1 \leq j \leq n \). Aggregate the PHI as \( C_{aggr,j} = H_4(C_{1,j}, C_{2,j}, \cdots, C_{m,j}) \in \mathbb{Z}_q^* \) and then compute

\[
X_j = C_{aggr,j} Y, \quad E_j = C_{aggr,j} d_{BMS}^j.
\]

Finally, transmit \( CT_j = \{ A_j, B_j, X_j, \sum_i D_{ij}, E_j \} \) to PAD.

- **PHI Re-Aggregation.** After receiving the signcrypted data \( CT_1, CT_2, \cdots, CT_n \), the PAD re-aggregates them as

\[
C_{PAD} = H_5(x_{PAD}, X_1, X_2, \cdots, X_n) \in \mathbb{Z}_q^*,
\]

and

\[
Z_{PAD} = C_{PAD} Y, \quad F = C_{PAD} d_{PAD}.
\]

Then store \( CT_{PAD} = \{ A_j, B_j, Z_{PAD}, X_j, \sum_i D_{ij}, E_j, F \} \) on the MCS.

- **Public Verifiability.** On stored encrypted data

\[
CT_{PAD} = \{ A_j, B_j, Z_{PAD}, X_j, \sum_i D_{ij}, E_j, F \}
\]

on the MCS, anyone in the network can verify the integrity of data as follows. Check the equality

\[
e(F, P) = e(H_1(ID_{PAD}), Z_{PAD})
\]

and

\[
e(E_j, B_j) = e(A_j, X_j).
\]

If it is true, the data is complete and correct; otherwise, it is incorrect or missing.

The correctness of the twisted KC-system can be obtained in the similar way as that of Kumar and Chand in [21]. As for
its security against our previous attack, we have the following result.

**Theorem 1:** If Okamoto’s CONF assumption holds, then our twisted KC-scheme is secure against the attack presented in Section III in the random oracle.

**Proof:** Let $A$ be an adversary who launches the attack given in Section III. Now, we construct another adversary $B$ attacking on Okamoto’s CONF assumption by invoking $A$ as the subroutine. More concretely, given the tuple $(g, xg, (xy)g) \in G^3$, $B$ intends to compute and output the element $g^y \in G$. Simulate the environment for $A$ as follows.

- **Simulating System Setup.** $B$ generates a bilinear map $e : G_1 \times G_1 \to G_2$. Choose five hash functions $H_1, \ldots, H_5$ as in the step of System Setup. Randomly choose $s_0, s_1, \ldots, s_n \in \mathbb{Z}_q^*$, and define
  \[ Y = g, \quad P_0 = (s_1 + \cdots + s_n)^{-1}Y, \quad \text{and} \quad P = (s_0)^{-1}P. \]

- **Simulating Entity’s Authentication and Registration.** For an entity $E \in \{BMS, PAD, SD\}$ but not $BMS$, the algorithm $B$ computes $X_E, D_E$ by randomly choosing $x_E \mathbb{Z}_q^*$. Then the partial private key $(X_{E0}, D_{E0})$ can be calculated as follows.
  \[ X_{E0} = x_EP_0, \quad D_{E0} = x_EH_1(ID_E). \]

Finally, the (full) private key $d_E$ is generated by computing
\[ d_E = (s_1 + s_2 + \cdots + s_n)H_1(ID_E). \]

- **Simulating PHI Aggregate Signcryption.** The $j$th BMS computes $A_j$ and $B_j$ by randomly choosing $a_j \in \mathbb{Z}_q^*$, and then sets $K_j = e(a_j^{d^j_{BMS}}, H_1(ID_{SD}))$. Then normally compute $C_{i,j}$ and $D_{i,j}$ for $1 \leq i \leq m, 1 \leq j \leq n$ and set
  \[ X_j = xg, \quad E_j = (xy)g. \]

Finally, transmit $CT_j = \{A_j, B_j, X_j, \sum_i D_{i,j}, E_j\}$ to PAD.

- **Simulating PHI Re-Aggregation.** Given the sign-crypted data $CT_1, CT_2, \ldots, CT_n$, the algorithm $B$ computes $C_{PAD}, Z_{PAD}$ and $F$. Then store
  \[ CT_{PAD} = \{A_j, B_j, Z_{PAD}, X_j, \sum_i D_{i,j}, E_j, F\} \]
on the MCS.

- **Public Verifiability.** Since the process of verifiability does not relies on any private key, $B$ can correctly simulate it for $A$.

In the last phase, if the adversary $A$ can correctly compute and output $d^j_{BMS}$, then the algorithm $B$ also outputs it as its solution of $(xy)g$. Then the proof of Theorem 1 is obtained since Okamoto’s CONF assumption holds. This ends the proof of Theorem 1.

**V. CONCLUSION**

In this paper, we analyze the security of the KC-system, which is proposed for smart healthcare system. Although Kumar et al. claimed that their system can achieve both the privacy-preserving of patient’s health information and identity, and the mutual authentication of the entities included in the system, we proved that their authentication key can be easily recovered from their communication contents. Hence, the complicated processes of the KC-system become completely useless. Moreover, potential attacks may also occur in their smart healthcare system. In addition, we also proved that the KC-system did not achieve the expected public verifiability function. Finally, we proposed a twisted KC-scheme to defend against the previous attack and proved its security.

**REFERENCES**

[1] C. Zhou, “An improved lightweight certificateless generalized signcryption scheme for mobile-health system,” *Int. J. Distrib. Sensor Netw.*, vol. 15, no. 1, pp. 1–16, 2019.

[2] M. Kumar and S. Chand, “A lightweight cloud-assisted identity-based anonymous authentication and key agreement protocol for secure wireless body area network,” *IEEE Syst. J.*, vol. 15, no. 2, pp. 2779–2786, Jun. 2021, doi: 10.1109/JSYST.2020.2990749.

[3] Y. Zhang, D. Zheng, and R. H. Deng, “Security and privacy in smart health: Efficient policy-hiding attribute-based access control,” *IEEE Internet Things J.*, vol. 5, no. 3, pp. 2130–2145, Jun. 2018.

[4] W. Sun, Z. Cai, Y. Li, F. Liu, S. Fang, and G. Wang, “Security and privacy in the medical Internet of Things: A review,” *Secure. Commun. Netw.*, vol. 2018, Mar. 2018, Art. no. 5978636.

[5] J. Chang, B. Shao, Y. Ji, M. Xu, and R. Xue, “Security and privacy in the medical Internet of Things: A review,” *Secure. Commun. Netw.*, vol. 2021, no. 12, Dec. 2021, Art. no. 229301.

[6] V. Suresh Kumar, R. Amin, V. R. Vijay Kumar, and S. R. Sekar, “Robust secure communication protocol for smart healthcare system with FPGA implementation,” *Future. Gener. Comput. Syst.*, vol. 100, pp. 938–951, Nov. 2019.

[7] Y. Li, Y. Yu, R. Chen, X. Du, and M. Guizani, “IdentityChain: Provable data possession for decentralized storage,” *IEEE J. Sel. Areas Commun.*, vol. 38, no. 6, pp. 1205–1217, Jun. 2020.

[8] H. Shucham and B. Waters, “Compact proofs of retrievability,” *J. Cryptol.*, vol. 26, no. 3, pp. 442–483, Jul. 2013.

[9] B. Wang, B. Li, H. Li, and F. Li, “Certificateless public auditing for data integrity in the cloud,” in *Proc. IEEE Conf. Comput. Commun. Netw. Secur. ( CNS)*, Oct. 2013, pp. 136–144, doi: 10.1109/CNS.2013.6682701.

[10] H. Wang, L. Feng, Y. Ji, B. Shao, and R. Xue, “Toward usable cloud storage auditing,” *IEEE J. Sel. Areas Commun.*, vol. 31, no. 1, pp. 178–179, Jan. 2013.

[11] B. Wang, Y. Ji, and R. Xue, “Towards provable security in cloud storage,” *IEEE J. Sel. Areas Commun.*, vol. 31, no. 1, pp. 178–179, Jan. 2013.

[12] A. Omalu, N. Robert, and F. Li, “A provably-secure transmission scheme for wireless body area networks,” *J. Med. Syst.*, vol. 40, no. 11, p. 247, 2016.

[13] J. Chang, Y. Ji, B. Shao, M. Xu, and R. Xue, “Certificateless homomorphic signature scheme for network coding,” *IEEE/ACM Trans. Netw.*, vol. 28, no. 6, pp. 2615–2628, Dec. 2020.

[14] X. Hiong and Z. Qin, “Revocable and scalable certificateless remote authentication protocol with anonymity for wireless body area networks,” *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 7, pp. 1442–1455, Jul. 2015.

[15] M. Kumar and S. Chand, “ESKI-BEF: Efficient and secure key issuing identity-based encryption with cloud privacy centers,” *Multimedia Tools. Appl.*, vol. 78, no. 14, pp. 19753–19786, Jul. 2019.

[16] J. Chang, H. Wang, F. Wang, A. Zhang, and Y. Ji, “RKA security for identity-based signature scheme,” *IEEE Access*, vol. 8, pp. 17833–17841, 2020.

[17] J. Li, H. Yan, and Y. Zhang, “Identity-based privacy preserving remote data integrity checking for cloud storage,” *IEEE Syst. J.*, vol. 15, no. 1, pp. 577–585, Mar. 2021, doi: 10.1109/JSYST.2020.2978146.
RONGHUA XU received the B.S. degree in biomedical engineering from Nanjing Medical University and the M.S. degree in green technology (energy) from Hong Kong Baptist University. He is an Assistant Research Fellow with the Case Center, SUFE. His interests include information technology and case study.

QIAOCHUAN REN was born in 1996. He is currently pursuing the master’s degree with the School of Information and Control Engineering, Xi’an University of Architecture and Technology (XAUAT), Xi’an, Shaanxi, China. His research interests include information security and cryptography.

23624

VOLUME 10, 2022