# Security Analysis on an Improved Anonymous Authentication Protocol for Wearable Health Monitoring Systems

Gayeong Eom[1]
Department of Statistics
Graduate School, Inje University
Gimhae 50834, Republic of Korea

Haewon Byeon[2]*, Younsung Choi[3]*
Department of Artificial Intelligence
Inje University, Gimhae 50834
Republic of Korea

***Abstract*—The wearable health monitoring system (WHMS) plays a significant role in medical experts collecting and using patient medical data. The WHMS is becoming more popular than in the past through mobile devices due to meaningful progress in wireless sensor networks. However, because the data about health used by the WHMS is related to privacy, it has to be protected from malicious access when wirelessly transmitted. Jiang et al. proposed a two-factor suitable for WHMSs using a fuzzy verifier. However, Jiaqing Mo et al. revealed that the protocol proposed by Jiang et al. had various security vulnerabilities and proposed an authentication protocol with improved security and guaranteed anonymity for WHMSs. In this paper, we analyse the authentication protocol proposed by Jiaqing Mo et al. and determine problems with the offline identification, password guessing attacks, operation process bit mismatch, no perfect forward secrecy, no mutual authentication and insider attacks.**

***Keywords*—Authentication protocol; health status; physiological data; security analysis; WHMS**

## I. Introduction

Electronic health system keeps Wireless communication, authentication protocol, sensors using low-power, and security solution on authentication protocol [1-8] safe. Wireless sensor networks (WSNs), which play a significant role in e-health, detect, measure, collect or record patient information on a medical server for physician diagnosis. The wearable health monitoring system (WHMS) has received considerable attention regarding its movability, adaptability and operation cost [9, 10, 11, 12]. The WHMS detects, measures, and collects patient physiological data with the WSN inserted or embed within the patient's body. In addition, after monitoring the health status, information is transmitted through wireless channels to medical-related institutions to help manage it. Remote doctors can evaluate the health status through such data as the heart rate, blood pressure and body temperature.

The WHMS is simple and efficient for medical professionals, and patients receive many benefits from the WHMS. However, the detected data are transmitted over an unsafe wireless channel; thus, concerns exist regarding security and privacy problems. Therefore, a robust certified mechanism must be designed to protect the physiological data for patients whose security is critical. If an adversary modifies the data for a patient, the doctor will misdiagnose the patient based on incorrect data. In addition, revealed data are highly likely to be used by malicious and illegal purposes. Medical personnel must authenticate that they are normal users before accessing patient's physiological data from the wearable sensor of the patient to prevent this. Even if the adversary eavesdropped on the message through the gateway of the WHMS, their identity and passwords must not be disclosed. A session key must be calculated between the sensor node and the medical personnel on the patient's body for future secure communication.

Kumar et al. [13] studied a user authentication protocol in 2012 to monitor patient physiological data in the medical WSN E-SAP and argued that the protocol was safe on the known attacks. But He et al. [14] and Khan and Kumari [15] found security vulnerabilities, such as lack of user anonymity and password guessing attack in the plans by Kumar et al. and presented improved versions. Li et al. and Wu et al., Mir et al. [16-18] individually found out that the plan by He et al. [14] has security problems, such as offline guessing attacks, denial-of-service (DoS) attacks, most attacks, and sensor node capture attacks. They proposed an enhanced version that is safer than the previous proposal to compensate for these loopholes. Das et al. [20] pointed out various security flaws such as lack of user anonymity, privileged insider attacks and sensor capture attacks in the protocol by Li et al. [21] and proposed an improved framework based on biometric recognition. Amin et al. [19] proposed a mutually authentication protocol providing user's anonymity in the WHMS and stated that the system was secure against already known various attacks. But Jiang et al. [22] revealed that the protocol has various vulnerabilities like as unsynchronised attacks, sensor key exposure and stolen mobile device attacks. Jiang et al. proposed an enhanced authentication protocol using smart card and password [22, 23]. Their protocol used square surplus, fuzzy validator [24] and timestamp mechanisms to ensure the plan by Amin et al. In addition, as a result of a security analysis, their plan achieved the desired security function.

Separately, Challa et al. [25] claimed an enhanced 3-factor (cryptography, smart card and biometric) authentication scheme for healthcare WSNs to enhance the scheme's security proposed by Liu and Chung [26]. However, this method, which requires the user to communicate directly with the remote sensor, greatly increases the sensor power consumption and

*Corresponding Author.

rapidly reduces its lifespan. Therefore, their systems cannot be applied to healthcare WSNs. Ali et al. [27] proposed a 3-factor protocol providing anonymity in the plan by Amin et al. [19] to frustrate security threats, such as user impersonation attacks, offline password guessing attacks and known session key temporary information attacks. Shen et al. [28] presented a multilayer authentication protocol using ECC in WBANs (wireless body area networks) to improve authentication's security and compute group key generation between sensors and mobile devices. Li et al. [29] proposed an efficient authentication scheme for a centralised WBAN organized two hops while maintaining anonymity and nonconnectedness in data transmission. And Shen et al. [30] proposed an ECC-based authentication protocol using public key signature scheme for WBAN. But according to [31, 32], their authentication scheme type with only two round messages is likely to fail in perfect forward secrecy.

Jiaqing Mo et al. analysed the protocol proposed by Jiang et al. [22] and discovered that Jiang et al.' protocol was not safe as their proven. Jiang et al.' scheme provides fuzzy verifiers to block offline password guessing attacks, their systems were still vulnerable to authoritative insider attacks, leading to user impersonation attacks. Unfortunately, the plan by Jiang et al. [22] is subject to KSSTI attacks; thus, their protocols are as vulnerable to sensor key disclosure as before. In addition, their protocols struggle with DoS attacks. In addition, Jiaqing Mo et al. implement an authentication scheme with improved security and guaranteed anonymity for WHMSs to solve this problem. However, in this paper, we analyse the authentication protocol proposed by Jiaqing Mo et al. and discovered problems with the offline identification, password guessing attacks, operation process bit mismatch, no perfect forward secrecy, no mutual authentication and insider attacks.

The rest of this paper is organised as follows. Section 2 describes the terms and adversary models used in this paper. Section 3 analyses the operation process of an authentication protocol with improved security and guaranteed anonymity for the WHMS proposed by Jiaqing Mo et al. Section 4 describes the vulnerabilities found by conducting a stability analysis on the protocol proposed by Jiaqing Mo et al. Finally, in Section 5, we conclude this paper.

## II. Related Research

### A. Summary of Symbol

Symbols used in the paper's operation process are shown in Table I.

### B. Adversary Model

An adversary's capabilities are essential part of an adversary model. In this paper, it is assumed that the adversary has the following capabilities.

- An adversary can completely control open channels like as inserting, intercepting, eavesdropping, deleting, and modifying exchanged messages through open channels [33, 34].
- An adversary can find out all data (i.e. secret key and random number) stored in the mobile device when adversary acquire user's lost mobile device [35, 36].
- An adversary can estimate the ID_i and PW_i offline by listing pairs in Cartesian product D_ID×D_PW within polynomial time. Here, the D_ID represents identity space and D_PW is password space [31, 37].
- The secret key and random numbers party are suitably large so they overcome adversary from successfully guessing accurate data within polynomial time.
- The inside adversary may get a user's registration request message, and the insider may access the verification table [38, 39].

TABLE I. Summary of Symbol

| Symbol | Meaning |
|---|---|
| $U_i$ | Medical professional |
| $\mathrm{ID}_i$ | $U_i$'s identity |
| $\mathrm{PW}_i$ | $U_i$'s password |
| $S_j$ | The $j$th sensor node |
| $\mathrm{SID}_j$ | $S_j$'s identity |
| GWN | Gateway |
| $K$ | GWN's secret key |
| MD | The mobile device |
| $R_1, R_2$ and $R_3$ | Random nonce produced by $U_i$, GWN, and $S_j$, respectively |
| $\oplus$ | Bitwise XOR operation |
| $\|$ | Concatenation |
| $h()$ | One-way hash function |

## III. Operation Process of the Protocol Proposed by Jiaqing Mo et al

Jiaqing Mo et al.'s proposed protocol consists of five stages: setting, medical expert registration, patient registration, login and authentication, and password change.

### A. Setting Step

The registration center GWN selects two large primes $p$ and $q$, computes $n = pq$, and maintains the private key $(p, q)$.

### B. Medical Professional Registration Step

*1)* $U_i$ inserts own $\mathrm{ID}_i$ and $\mathrm{PW}_i$, a random-nonce $r_i$, and computes $\mathrm{HPW}_i = \mathrm{h}(r_i \oplus \mathrm{PW}_i)$; then send $\{\mathrm{ID}_i, \mathrm{HPW}_i\}$ to gateway through a secure channel.

*2)* After receiving user's registration request, GWN selects $m \in [2^4, 2^8]$, a random-nonce $R_i$, computes $\mathrm{Reg}_i = h(h(\mathrm{ID}_i \| R_i \| \mathrm{HPW}_i) \bmod m)$, $A_i = R_i \oplus \mathrm{HPW}_i$, $B_i = h(\mathrm{ID}_i \| R_i \| K)$, and $C_i = B_i \oplus h(\mathrm{ID}_i \| R_i \| \mathrm{HPW}_i)$. $\mathrm{Reg}_i$ is a fuzzy verifier. Thereafter, GWN transmits $\{\mathrm{Reg}_i, A_i, C_i, m, n, h()\}$ to $U_i$ using a secure channel.

*3)* When $U_i$ receive GWN' message, $U_i$ computes $A_i^* = A_i \oplus h(\mathrm{ID}_i \| r_i)$, $D_i = r_i \oplus h(h(\mathrm{ID}_i \| \mathrm{PW}_i) \bmod m)$ and updates MD to $\{\mathrm{Reg}_i, A_i^*, C_i, D_i, m, n, h()\}$.

### C. Patient Registration Step

This step is almost identical to Jiang's plan [22].

*1)* The patient delivers the ID to the registration center.

*2)* Select the appropriate sensor kit from the registration center and assigns a professional.

*3)* The registration center calculates $\mathrm{SK_{GW-Sj}} = h(\mathrm{SID}_j \parallel K)$ for $\mathrm{S}_j$ as a secret key between GWN and sensor node. And the registration center delivers the patient's significant information to the designated specialist.

### D. The Login and Authentication Step

Through this step, this protocol will be able to provide mutual authentication and generate session keys between $U_i$ and $\mathrm{S}_j$ for future communication.

*1)* $U_i$ chooses own $\mathrm{ID}_i$ and $\mathrm{PW}_i$, and MD calculates $r_i = D_i \oplus h(h(\mathrm{ID}_i \parallel \mathrm{PW}_i) \bmod m)$, $\mathrm{HPW}_i = \mathrm{h}(r_i \oplus \mathrm{PW}_i)$, $A_i = A_i^* \oplus h(\mathrm{ID}_i \parallel r_i)$, $R_i^* = A_i \oplus \mathrm{HPW}_i$, $\mathrm{Reg}_i^* = h(h(\mathrm{ID}_i \parallel R_i^* \parallel \mathrm{HPW}_i^*) \bmod m)$, and tests $\mathrm{Reg}_i^*$?=$\mathrm{Reg}_i$. If false, MD selects a random number $R_1$ and calculates $B_i^* = C_i \oplus h(\mathrm{ID}_i \parallel R_i \parallel \mathrm{HPW}_i)$, $\mathrm{CID}_i = (\mathrm{ID}_i \parallel R_1 \parallel R_i^* \parallel \mathrm{SID}_j)^2 \bmod n$, $M_1 = h(\mathrm{ID}_i \parallel B_i^* \parallel R_1 \parallel T_1)$, then transfers $\mathrm{msg}_1 = \{\mathrm{CID}_i, M_1, T_1\}$ to GWN. $T_1$ is the current timestamp.

*2)* After receiving the login request $\mathrm{msg}_1$, the GWN decrypts $\mathrm{CID}_i$ with $(p, q)$ to obtain $(\mathrm{ID}_i^*, R_i^*, R_1^*, T_1)$ and confirms the freshness of the timestamp $T_1$. If the confirmation fails, GWN stops the session. Otherwise, GWN calculates $B_i' = h(\mathrm{ID}_i \parallel R_i \parallel K)$ and $M_1^* = h(\mathrm{ID}_i \parallel B_i' \parallel R_1 \parallel T_1)$ and then tests $M_1^* = M_1$. If inequality persists, GWN stops the procedure. Otherwise, GWN computes $\mathrm{SK_{GW-Sj}} = h(\mathrm{SID}_j \parallel K)$, selects a random nonce $R_2$, and computes $M_2 = h(\mathrm{ID}_i^* \parallel R_1^* \parallel R_i)$, $M_3 = h(h(M_2 \parallel \text{"1"}) \parallel \mathrm{SK_{GW-Sj}} \parallel R_2 \parallel T_2)$, $M_4 = M_2 \oplus h(\mathrm{SK_{GW-Sj}} \parallel T_2)$, and $M_5 = R_2 \oplus h(\mathrm{SK_{GW-Sj}} \parallel \mathrm{SID}_j \parallel T_2)$. Finally, GWN sends $\mathrm{msg}_2 = \{M_3, M_4, M_5, T_2\}$ to $S_j$.

*3)* When receiving $\mathrm{msg}_2$ from GWN, firstly $S_j$ checks the validity of $T_2$. If it is not fresh, $S_j$ stops next procedure. If it fresh, $S_j$ calculates $R_2' = M_5 \oplus (\mathrm{SK_{GW-Sj}} \parallel \mathrm{SID}_j \parallel T_2)$ and $M_2 = M_4 \oplus h(\mathrm{SK_{GW-Sj}} \parallel T_2)$ and tests $M_3? = h(h(M_2 \parallel \text{"1"}) \parallel \mathrm{SK_{GW-Sj}} \parallel R_2' \parallel T_2)$. If it is false, $S_j$ terminates the session. Otherwise, $S_j$ selects a random number $R_3$ and calculates $\mathrm{SK} = h(M_2' \parallel R_2' \parallel R_3)$, $M_6 = h(\mathrm{SK} \parallel R_3 \parallel \mathrm{SK_{GW-Sj}})$, and $M_7 = h(R_2' \parallel T_3) \oplus R_3$, where $T_3$ is the current timestamp. Then, $S_j$ transfers $\mathrm{msg}_3 = \{M_6, M_7, T_3\}$ to GWN.

*4)* When $\mathrm{msg}_3$ is a received from $S_j$, the GWN confirms the validity of $T_3$ firstly. If timestamp is fresh, GWN terminates next procedure. Otherwise, GWN calculates $R_3' = M_7 \oplus h(R_2' \parallel T_3)$, $\mathrm{SK}' = h(M_2 \parallel R_2 \parallel R_3')$, and $M_6' = h(\mathrm{SK}' \parallel R_3' \parallel \mathrm{SK_{GW-Sj}})$ and examines whether $M_6' = M_6$ holds. If they are same, GWN computes $M_8 = R_2 \oplus h(\mathrm{ID}_i^* \parallel R_1^*)$, $M_9 = R_3 \oplus h(\mathrm{ID}_i^* \parallel R_2^*)$, and $M_{10} = h(\mathrm{ID}_i^* \parallel \mathrm{SK}' \parallel R_3 \parallel T_4)$ and transfers $\mathrm{msg}_4 = \{M_8, M_9, M_{10}, T_4\}$ to $U_i$. Here, $T_4$ is the current timestamp.

*5)* $U_i$ receives $\mathrm{msg}_4$ from GWN and examines the timestamp $T_4$. If timestamp is not fresh, $U_i$ stops next procedure. Otherwise, $U_i$ calculates $R_2' = M_8 \oplus h(\mathrm{ID}_i \parallel R_1)$, $R_3' = M_9 \oplus h(\mathrm{ID}_i \parallel R_2')$, and $\mathrm{SK}^* = h(h(\mathrm{ID}_i \parallel R_1 \parallel R_i') \parallel R_2' \parallel R_3')$ and checks whether $M_{10}? = h(\mathrm{ID}_i \parallel \mathrm{SK}^* \parallel R_3' \parallel T_4)$ holds. If they are not same, $U_i$ terminates the current connection. If they are same, $U_i$ can believes that both GWN and $S_j$ are believable. Then $U_i$ and $S_j$ can proceed with secure communication in the future by using the session key. The login and authentication steps are summarized in Fig. 1.

## IV. Security Analysis of Jiaqing Mo Et Al's Protocol

This paper analyzed the operation process of Jiang et al.'s protocol and found various vulnerability as off-line ID, PW guessing attack, operation process bit mismatch, no perfect forward secrecy, no mutual authentication and insider attack.

### A. Off-line ID, PW Guessing Attack

According to Jiaqing Mo et al.'s proposed protocol, when an adversary acquires a MD, the adversary can extract information stored in the MD and then find out the user's ID and PW. The information of $\{\mathrm{Reg}_i, A_i, C_i, m, n, h()\}$ is sent to the MD through the GWN security channel. Thereafter, the MD calculates and updates $A_i^* = A_i \oplus h(\mathrm{ID}_i \parallel r_i)$ and $D_i = r_i \oplus h(h(\mathrm{ID}_i \parallel \mathrm{PW}_i) \bmod m)$. Finally, information of $\{\mathrm{Reg}_i, A_i^*, C_i, D_i, m, n, h()\}$ is stored in the MD. Assuming that an adversary found out this through a physical analysis method, an ID and password can be derived through the formula of $\mathrm{Reg}_i{}^* = h(h(\mathrm{ID}_i \parallel R_i^* \parallel \mathrm{HPW}_i^*) \bmod m)$.

$$
\begin{aligned}
\mathrm{Reg}_i{}^* &= h(h(\mathrm{ID}_i \parallel R_i^* \parallel \mathrm{HPW}_i^*) \bmod m) \\
&= h(h(\mathrm{ID}_i \parallel A_i \oplus \mathrm{HPW}_i{}^* \parallel h(r_i \oplus \mathrm{PW}_i)) \bmod m) \\
&= h(h(\mathrm{ID}_i \parallel A_i^* \oplus h(\mathrm{ID}_i \parallel r_i), \oplus \mathrm{HPW}_i{}^* \\
&\qquad \parallel h(r_i \oplus \mathrm{PW}_i)) \bmod m) \\
&= h(h(\mathrm{ID}_i \parallel A_i^* \oplus h(\mathrm{ID}_i \parallel D_i \oplus h(h(\mathrm{ID}_i \\
&\qquad \parallel \mathrm{PW}_i) \bmod m)) \oplus h(r_i \oplus \mathrm{PW}_i) \\
&\qquad \parallel h(r_i \oplus \mathrm{PW}_i)) \bmod m) \\
&= h(h(\mathrm{ID}_i \parallel A_i^* \oplus h(\mathrm{ID}_i \parallel D_i \oplus h(h(\mathrm{ID}_i \\
&\qquad \parallel \mathrm{PW}_i) \bmod m)) \oplus h(D_i \oplus h(h(\mathrm{ID}_i \\
&\qquad \parallel \mathrm{PW}_i) \bmod m) \oplus \mathrm{PW}_i) \parallel h(D_i \oplus h(h(\mathrm{ID}_i \\
&\qquad \parallel \mathrm{PW}_i) \bmod m) \oplus \mathrm{PW}_i)) \bmod m)
\end{aligned}
$$

Summarizing the above formula, the adversary will be aware of the information $\{A_i^*, D_i, m, h()\}$ except for the ID and PW. The adversary repeatedly performs verification while continuing to change until the user's ID and PW are found. Ultimately, the user's exact ID and PW can be found. The process of ID, PW guessing attack is summarized in Fig. 2.

### B. Operation Process Bit Mismatch

In Jiaqing Mo et al.'s protocol, XOR operations are widely used, and XOR operations must have the same number of bits. However, in Jiaqing Mo et al.'s protocol, there may be a problem with the XOR operation because the number of bits does not match during the XOR operation. A hash function is a function that receives a message having an arbitrary length and outputs a hash value of a fixed length. Keys are used for cryptographic algorithms, but hash functions do not use keys, so the same output is always produced for the same input. The purpose of using these hash functions is to provide integrity to detect errors or alterations in messages.

$$HPW_i = h(r_i \oplus PW_i)$$

| $U_i$/mobile device | GWN | $S_j$ |
|---|---|---|
| Input <$ID_i$, $PW_i$>;<br>$r_i = D_i \oplus h(h(ID_i \| PW_i) \bmod m)$;<br>$HPW_i = h(r_i \oplus PWi)$;<br>$A_i = A_i^* \oplus h(ID_i \| r_i)$;<br>$R_i^* = A_i \oplus HPW_i$;<br>$Reg_i^* = h(h(ID_i \| R_i^* \| HPW_i^*) \bmod m)$;<br>If $Reg_i^* \neq Reg_i^*$, abort;<br>Choose $R_1$;<br>$B_i^* = C_i \oplus h(ID_i \| R_i \| HPW_i)$;<br>$CID_i = (ID_i \| R_1 \| R_i^* \| SID_j)^2 \bmod n$;<br>$M_1 = h(ID_i \| B_i^* \| R_1 \| T_1)$;<br>$msg_1 = \{CID_i, M_1, T_1\}$ → | | |
| | Decrypt $CID_i$ with $(p, q)$ to obtain $(ID_i^*, R_i^*, R_i^*, T_1)$;<br>If $T_1$ is not fresh, abort;<br>$B_i' = h(ID_i \| R_i \| K)$;<br>$M_1^* = h(ID_i \| B_i' \| R_1 \| T_1)$;<br>If $M_1^* \neq M_1$, abort;<br>$SK_{GW\text{-}Sj} = h(SID_j \| K)$;<br>Generate $R2$;<br>$M_2 = h(ID_i^* \| R_1^* \| R_i)$;<br>$M_3 = h(h(M_2 \| "1") \| SK_{GW\text{-}Sj} \| R_2 \| T_2)$;<br>$M_4 = M_2 \oplus h(SK_{GW\text{-}Sj} \| T_2)$;<br>$M_5 = R_2 \oplus (SK_{GW\text{-}Sj} \| SID_j \| T_2)$;<br>$msg_2 = \{M_3, M_4, M_5, T_2\}$ → | |
| | | If $T_2$ is not fresh, abort;<br>$R_2' = M_5 \oplus (SK_{GW\text{-}Sj} \| SID_j \| T_2)$;<br>$M_2 = M_4 \oplus h(SK_{GW\text{-}Sj} \| T_2)$;<br>If $M_3 \neq h(h(M_2 \| "1") \| SK_{GW\text{-}Sj} \| R_2' \| T_2)$, abort;<br>Choose $R_3$;<br>$SK = h(M_2' \| R_2' \| R_3)$;<br>$M_6 = h(SK \| R_3 \| SK_{GW\text{-}Sj})$;<br>$M_7 = h(R_2' \| T_3) \oplus R_3$;<br>$msg_3 = \{M_6, M_7, T_3\}$ ← |
| | If $T_3$ is not fresh, abort;<br>$R_3' = M_7 \oplus h(R_2' \| T_3)$;<br>$SK' = h(M_2 \| R_2 \| R_3')$;<br>$M_6' = h(SK' \| R_3' \| SK_{GW\text{-}Sj})$;<br>If $M_6' \neq M_6$, abort;<br>$M_8 = R_2 \oplus h(ID_i^* \| R_i^*)$;<br>$M_9 = R_3 \oplus h(ID_i^* \| R_i^*)$;<br>$M_{10} = h(ID_i^* \| SK' \| R_3 \| T_4)$;<br>$msg_4 = \{M_8, M_9, M_{10}, T_4\}$ ← | |
| If $T_4$ is not fresh, abort;<br>$R_2' = M_8 \oplus h(ID_i \| R_1)$;<br>$R_3' = M_9 \oplus h(ID_i \| R_2')$;<br>$SK^* = h(h(ID_i \| R_1 \| R_i') \| R_2' \| R_3')$;<br>If $M_{10} = h(ID_i \| SK^* \| R_3' \| T_4)$, accept $SK^*$. | | |

Fig. 1. The Login and Authentication Phase of Jiaqing Mo Et Al.'s Protocol.

If attacker acquire MD

MD has $\{\mathrm{Reg}_i,\ A_i^*,\ C_i,\ D_i,\ m,\ n,\ h()\}$ information

$$\mathrm{Reg}_i{}^* = h\big(h(\mathrm{ID}_i \parallel R_i^* \parallel \mathrm{HPW}_i^*) \bmod m\big)$$
$$= h(h(\mathrm{ID}_i \parallel A_i \oplus \mathrm{HPW}_i{}^* \parallel h(r_i \oplus \mathrm{PW}_i)) \bmod m)$$
$$= h(h(\mathrm{ID}_i \parallel A_i^* \oplus h(\mathrm{ID}_i \parallel r_i), \oplus \mathrm{HPW}_i{}^* \parallel h(r_i \oplus \mathrm{PW}_i)) \bmod m)$$
$$= h(h(\mathrm{ID}_i \parallel A_i^* \oplus h(\mathrm{ID}_i \parallel D_i \oplus h(h(\mathrm{ID}_i \parallel \mathrm{PW}_i) \bmod m)) \oplus h(r_i \oplus \mathrm{PW}_i) \parallel h(r_i \oplus \mathrm{PW}_i)) \bmod m)$$
$$= h(h(\mathrm{ID}_i \parallel A_i^* \oplus h(\mathrm{ID}_i \parallel D_i \oplus h(h(\mathrm{ID}_i \parallel \mathrm{PW}_i) \bmod m)) \oplus h(D_i \oplus h(h(\mathrm{ID}_i \parallel \mathrm{PW}_i) \bmod m) \oplus \mathrm{PW}_i) \parallel h(D_i \oplus h(h(\mathrm{ID}_i \parallel \mathrm{PW}_i) \bmod m) \oplus \mathrm{PW}_i)) \bmod m)$$

The attacker knows $\{A_i^*,\ D_i,\ m,\ h()\}$ in the formula

**That is, it is possible to find the user's ID and PW**

Fig. 2. Process of ID, PW Guessing Attack.

Random nonce values used in the formula usually use large random numbers of 128 bits or more, but the length of the password is very short compared to Random nonce. That is, the length of the random nonce and the length of the password cannot be the same. Therefore, there may be a problem with the XOR operation due to inconsistency in the number of bits in Jiaqing Mo et al.'s protocol.

### C. No Perfect Forward Secrecy

The fact that the Perfect Forward Secrecy is met means that even if one of the important master keys in the protocol is exposed, the previous session key cannot be determined. However, in this protocol, the exposure of the $(p, q)$ value, one of the unchanged long-term keys, does not meet the Perfect Forward Secrecy because it can identify not only future session keys but also previously used session keys. That is, assuming that the adversary has found out $(p, q)$, it is possible to calculate the previous session key used between the mobile device and $S_j$.

*1)* The adversary has exposed $(p, q)$ values and previous communication contents ($\mathrm{CID}_i$ of $\mathrm{msg}_1$, $M_8$ and $M_9$ of $\mathrm{msg}_4$) between the user and GWN and $S_j$. The adversary may decrypt the $\mathrm{CID}_i$ of the login request $\mathrm{msg}_1$ as $(p, q)$, and the adversary may find out $\mathrm{ID}_i^*, R_i^*, R_1^*$ and $T_1$.

*2)* In addition, the adversary may calculate $R_2{}'$ using $M_8$, $\mathrm{ID}_i$ and $R_1$.

$$R_2{}' = M_8 \oplus h(\mathrm{ID}_i \parallel R_1).$$

*3)* In addition, $R_3{}'$ may be calculated using $M_9$, $\mathrm{ID}_i$ and $R_2{}'$.

$$R_3{}' = M_9 \oplus h(\mathrm{ID}_i \parallel R_2{}').$$

*4)* Finally, the adversary may calculate the session key $\mathrm{SK}^*$ by using the $\mathrm{ID}_i$, $R_i$, $R_1$, $R_2{}'$ and $R_3{}'$ obtained so far.

$$\mathrm{SK}^* = h(h(\mathrm{ID}_i \parallel R_1 \parallel R_i{}') \parallel R_2{}' \parallel R_3{}').$$

Since long-term key $(p, q)$ is a key that does not change after it is generated, it is a serious problem that the previous session key is exposed because it does not satisfy the Perfect Forward Secrecy when $(p, q)$ is exposed.

### D. No Mutual Authentication

Mutual authentication means that all components of the authentication protocol authenticate with each other. In the present protocol, $U_i$, GWN, $S_j$ authenticates using $M_1$, $M_3$, $M_6$, $M_{10}$. Through four messages, mutual authentication between $U_i$ and GWN and mutual authentication between GWN and $S_j$ are provided, but there is a problem of not providing mutual authentication between $U_i$ and $S_j$. The mutual authentication process is as follows.

*1)* GWN verifies the authentication of $U_i$ using $\mathrm{ID}_i$ and $M_1 = h(\mathrm{ID}_i \parallel B_i^* \parallel R_1 \parallel T_1)$ having the secret key $K$ of GWN. When $M_1$ that $U_i$ has is transmitted to GWN, GWN calculates $B_i' = h(\mathrm{ID}_i \parallel R_i \parallel K)$ and $M_1^* = h(\mathrm{ID}_i \parallel B_i' \parallel R_1 \parallel T_1)$. When $M_1$ and $M_1^*$ match, GWN authenticates that $U_i$ is a normal user.

*2)* When the consistency is confirmed, $S_j$ confirms the authentication of GWN using $M_2 = h(\mathrm{ID}_i^* \parallel R_1^* \parallel R_i)$ and $\mathrm{SK}_{\mathrm{GW-S}j} = h(\mathrm{SID}_j \parallel K)$. The authentication is confirmed by comparing $M_3 = h(h(M_2 \parallel \text{"1"}) \parallel \mathrm{SK}_{\mathrm{GW-S}j} \parallel R_2 \parallel T_2)$ and $h(h(M_2 \parallel \text{"1"}) \parallel \mathrm{SK}_{\mathrm{GW-S}j} \parallel R_2{}' \parallel T_2)$ having session key $\mathrm{SK}_{\mathrm{GW-S}j}$ of GWN and $S_j$.

*3)* When authentication is confirmed, GWN checks the consistency between $M_6 = h(\mathrm{SK} \parallel R_3 \parallel \mathrm{SK}_{\mathrm{GW-S}j})$ and $M_6{}' = h(\mathrm{SK}' \parallel R_3{}' \parallel \mathrm{SK}_{\mathrm{GW-S}j})$ to confirm the authentication of $S_j$.

*4)* Finally, if $M_{10} = h(\mathrm{ID}_i{}^* \parallel \mathrm{SK}' \parallel R_3 \parallel T_4)$ matches $h(\mathrm{ID}_i \parallel \mathrm{SK}^* \parallel R_3{}' \parallel T_4)$, $U_i$ authenticates GWN.

GWN authenticates Ui through $M_1$, and $S_j$ authenticates GWN through $M_3$. Through $M_6$, GWN authenticates $S_j$, and $U_i$ authenticates GWN through M10. That is, $U_i$ and GWN, GWN and $S_j$ are mutually authenticated, but in this protocol, mutual authentication between $U_i$ and $S_j$ is not provided. In order to create an authentication protocol with improved security, the authentication protocol will be safer only when $U_i$ and $S_j$ are also mutually authenticated. Fig. 3 describes in detail how the mutual authentication process is performed.

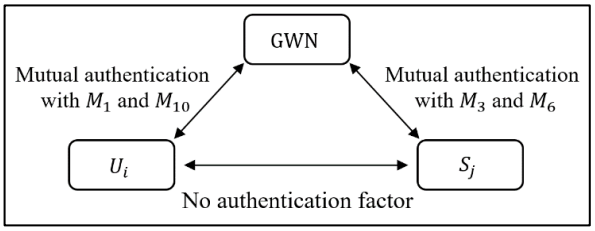


Fig. 3. Mutual Authentication Process.

### E. Insider Attack

Even an insider of GWN should not be able to pretend to be a normal user by utilizing the information obtained in the process of verifying the user's authentication information in the MD authentication step. However, in the protocol proposed by Jiaqing Mo et al., there is a problem that insiders can disguise themselves as normal users using only $\{\mathrm{ID}_i^*, R_i^*\}$. In this protocol, in the process of calculating the user's authentication information, an internal adversary can find out the user's $\{\mathrm{ID}_i^*, R_i^*\}$ information that authenticates with the GWN's secret key $K$. Based on this information, an internal adversary can

succeed in authentication under the guise of a normal user, and a session key can also be calculated. Fig. 4 shows the protocol authentication process and the adversary calculating the session key.

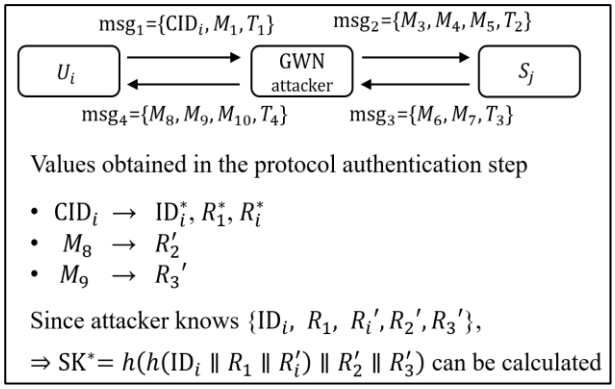


Fig. 4. The Adversary's Session Key Calculation Process.

Among $\text{msg}_1 = \{\text{CID}_i, M_1, T_1\}$ transmitted to GWN by an insider, $\text{CID}_i = (\text{ID}_i \parallel R_1 \parallel R_i^* \parallel \text{SID}_j)^2 \bmod n$ may calculate using the unchanged values $\text{ID}_i^*$ and $R_i^*$ obtained by an insider adversary. In the case of $M_1$, $B_i^*$ of $M_1 = h(\text{ID}_i \parallel B_i^* \parallel R_1 \parallel T_1)$ may be found using information of $B_i' = h(\text{ID}_i \parallel R_i \parallel K)$ known by an internal adversary. Since the $T_1$ value can also be generated by the internal adversary at the current time, $M_1$ can be calculated. This allows an internal adversary to succeed in authentication under the guise of a user with only the information received from GWN. An insider adversary who succeeds in logging in receives $\{M_8, M_9, M_{10}, T_4\}$ information through $\text{msg}_1, \text{msg}_2, \text{msg}_3, \text{msg}_4$. The insider adversary must calculate information of $R_2'$ and $R_3'$ to compute the session key. Since the insider adversary has all the information in $R_2' = M_8 \oplus h(\text{ID}_i \parallel R_1)$, $R_2'$ may be calculated, and $R_3' = M_9 \oplus h(\text{ID}_i \parallel R_2')$ may be calculated using $R_2'$. An insider adversary may calculate $\text{SK}^* = h(h(\text{ID}_i \parallel R_1 \parallel R_i') \parallel R_2' \parallel R_3')$ because it has all the information of $\{\text{ID}_i, R_1, R_i', R_2', R_3'\}$ necessary for calculating the session key. As a result, authentication can be successful under the guise of a normal user only with the information possessed by the insider adversary.

## V. Conclusion

In this paper, a security analysis was conducted after explaining the operation process of an authentication protocol with improved security and guaranteed anonymity for the WHMS proposed by Jiaqing Mo et al. The protocols proposed by Jiaqing Mo et al. have vulnerabilities in offline identification, password guessing attacks, operation process bit mismatch, no perfect forward secrecy, no mutual authentication and insider attack problems.

## Acknowledgment

This research was funded by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education, grant number "2018R1D1A1B07041091, 2021S1A5A8062526", and "2022 Development of Open-Lab based on 4P in the Southeast Zone".

## References

[1] R. Amin and G. P. Biswas, A secure three-factor user authentication and key agreement protocol for TMIS with user anonymity, J. Med. Syst, vol. 39, no. 8, pp. 1-19, 2015. https://doi.org/10.1007/s10916-015-0258-7.

[2] S. A. Chaudhry, H. Naqvi, and M. K. Khan, An enhanced lightweight anonymous biometric based authentication scheme for TMIS, Multimed. Tools Appl. vol. 77, no. 5, pp. 5503–5524, 2018. https://doi.org/10.1007/s11042-017-4464-9.

[3] F. Wei, P. Vijayakumar, J. Shen, R. Zhang, and L. Li, A provably secure password-based anonymous authentication scheme for wireless body area networks, Comput. Electr. Eng. vol. 65, pp. 322–331, 2018. https://doi.org/10.1016/j.compeleceng.2017.04.017.

[4] X. Liu, C. Jin, and F. Li, An improved two-layer authentication scheme for wireless body area networks, J. Med. Syst. vol. 42, no. 8, pp. 1-14, 2018. https://doi.org/10.1007/s10916-018-0990-x.

[5] L. Zhang, Y. Zhang, S. Tang, and H. Luo, Privacy protection for e-health systems by means of dynamic authentication and three-factor key agreement, IEEE Trans. Ind. Electron. vol. 65, no. 3, pp. 2795-2805, 2018. doi: 10.1109/TIE.2017.2739683.

[6] O. Mir and M. Nikooghadam, A secure biometrics based authentication with key agreement scheme in telemedicine networks for e-health services, Wirel. Pers. Commun. vol. 83, no. 4, pp. 2439–2461, 2015. https://doi.org/10.1007/s11277-015-2538-4.

[7] Q. Jiang, M. K. Khan, X. Lu, J. Ma, and D. He, A privacy preserving three-factor authentication protocol for e-health clouds, J. Supercomput. vol. 72, no. 10, pp. 3826–3849, 2016. https://doi.org/10.1007/s11227-015-1610-x.

[8] Y. K. Ever, Secure-anonymous user authentication scheme for e-healthcare application using wireless medical sensor networks, IEEE Syst J, vol. 13, no. 1, pp. 456-467, 2019. doi: 10.1109/JSYST.2018.2866067.

[9] M. M. Baig, H. Gholamhosseini, and M. J. Connolly, A comprehensive survey of wearable and wireless ECG monitoring systems for older adults, Med. Biol. Eng. Comput. vol. 52, no. 5, pp. 485-495, 2013. https://doi.org/10.1007/s11517-012-1021-6.

[10] Z. Yang, Q. Zhou, L. Lei, K. Zheng, and W. Xiang, An IoTcloud based wearable ECG monitoring system for smart healthcare, J. Med. Syst. vol. 40, no. 12, pp. 1-11, 2016. https://doi.org/10.1007/s10916-016-0644-9.

[11] Y. Yin, H. Jiang, S. Feng et al., Bowel sound recognition using SVM classification in a wearable health monitoring system, Sci. China Inf. Sci. vol. 61, no. 8, pp. 1-3, 2018. https://doi.org/10.1007/s11432-018-9395-5.

[12] V. Trovato, C. Colleoni, A. Castellano, and M. R. Plutino, The key role of 3-glycidoxypropyltrimethoxysilane sol–gel precursor in the development of wearable sensors for health monitoring, J. Sol-Gel Sci. Technol. vol. 87, no. 1, pp. 27-40, 2018. https://doi.org/10.1007/s10971-018-4695-x.

[13] P. Kumar, S. G. Lee, and H. J. Lee, E-sap: efficient-strong authentication protocol for healthcare applications using wirelessmedical sensor networks, Sensors, vol. 12, no. 2, pp. 1625–1647, 2012. https://doi.org/10.3390/s120201625.

[14] D. He, N. Kumar, J. Chen, C.-C. Lee, N. Chilamkurti, and S.-S. Yeo, Robust anonymous authentication protocol for health-care applications using wireless medical sensor networks, Multimed. Syst. vol. 21, no. 1, pp. 49-60, 2015. https://doi.org/10.1007/s00530-013-0346-9.

[15] [15] M. K. Khan and S. Kumari, An improved user authentication protocol for healthcare services via wireless medical sensor networks, Int. J. Distrib. Sens. Netw. vol. 10, no. 4, pp. 347169, 2014. https://doi.org/10.1155/2014/347169.

[16] F. Wu, L. Xu, S. Kumari, and X. Li, An improved and anonymous two-factor authentication protocol for health-care applications with wireless medical sensor networks, Multimed. Syst. vol. 23, no. 2, pp. 195-205, 2015. https://doi.org/10.1007/s00530-015-0476-3.

[17] O. Mir, J. Munilla, and S. Kumari, Efficient anonymous authentication with key agreement protocol for wireless medical sensor networks, Peer Peer Netw Appl . vol. 10, no. 1, pp. 79-91, 2015. https://doi.org/10.1007/s12083-015-0408-1.

[18] C. T. Li, C. C. Lee, and C. Y. Weng, A secure cloud-assisted wireless body area network in mobile emergency medical care system, J. Med. Syst. vol. 40, no. 5, pp. 1-15, 2016. https://doi.org/10.1007/s10916-016-0474-9.

[19] R. Amin, S. H. Islam, G. P. Biswas, M. K. Khan, and N. Kumar, A robust and anonymous patient monitoring system using wireless medical sensor networks, Future Gener. Comput. Syst. vol. 80, pp. 483-495, 2016. https://doi.org/10.1016/j.future.2016.05.032.

[20] A. K. Das, A. K. Sutrala, V. Odelu, and A. Goswami, A secure smartcard-based anonymous user authentication scheme for healthcare applications using wireless medical sensor networks, Wirel. Pers. Commun. vol. 94, no. 3, pp. 1899-1933, 2017. https://doi.org/10.1007/s11277-016-3718-6.

[21] X. Li, J. Niu, S. Kumari, J. Liao, W. Liang, and M. K. Khan, A new authentication protocol for healthcare applications using wireless medical sensor networks with user anonymity, Secur. Commun. Netw. vol. 9, no. 15, pp. 2643–2655, 2016. https://doi.org/10.1002/sec.1214.

[22] Q. Jiang, J. Ma, C. Yang, X. Ma, J. Shen, and S. A. Chaudhry, Efficient end-to-end authentication protocol for wearable health monitoring systems, Comput. Electr. Eng. vol. 63, pp. 182–195, 2017. https://doi.org/10.1016/j.compeleceng.2017.03.016.

[23] K. H. Rosen, Elementary Number Theory and Its Applications, Addison-Wesley, Reading, MA, USA, 1988.

[24] C.-G. Ma, D. Wang, and S. D. Zhao, Security flaws in two improved remote user authentication schemes using smart cards, Int. J. Commun. Syst. vol. 27, no. 10, pp. 2215-2227, 2015. https://doi.org/10.1002/dac.2468.

[25] S. Challa, A. K. Das, V. Odelu et al., An efficient ECC-based provably secure three-factor user authentication and key agreement protocol for wireless healthcare sensor networks, Comput. Electr. Eng. vol. 69, pp. 534-554, 2018. https://doi.org/10.1016/j.compeleceng.2017.08.003.

[26] C. H. Liu and Y. F. Chung, Secure user authentication scheme for wireless healthcare sensor networks, Comput. Electr. Eng. vol. 59, pp. 250–261, 2017. https://doi.org/10.1016/j.compeleceng.2016.01.002.

[27] R. Ali, A. K. Pal, S. Kumari, A. K. Sangaiah, X. Li, and F. Wu, An enhanced three factor based authentication protocol using wireless medical sensor networks for healthcare monitoring, J. Ambient Intell. Humaniz. Comput. pp. 1-22, 2018. https://doi.org/10.1007/s12652-018-1015-9.

[28] J. Shen, S. Chang, J. Shen, Q. Liu, and X. Sun, A lightweight multi-layer authentication protocol for wireless body area networks, Future Gener. Comput. Syst. vol. 78, pp. 956–963, 2016. https://doi.org/10.1016/j.future.2016.11.033.

[29] X. Li, M. H. Ibrahim, S. Kumari, A. K. Sangaiah, V. Gupta, and K. K. R. Choo, Anonymous mutual authentication and key agreement scheme for wearable sensors in wireless body area networks, Comput. Netw. vol. 129, pp. 429–443, 2017. https://doi.org/10.1016/j.comnet.2017.03.013.

[30] J. Shen, Z. Gui, S. Ji, J. Shen, H. Tan, and Y. Tang, Cloud-aided lightweight certificateless authentication protocol with anonymity for wireless body area networks, J. Netw. Comput. Appl. vol. 106, pp. 117–123, 2018. https://doi.org/10.1016/j.jnca.2018.01.003.

[31] D. Wang and P. Wang, Two birds with one stone: two-factor authentication with security beyond conventional bound, IEEE Trans. Dependable Secure Comput. vol. 15, no. 4, pp. 708-722, 2016. doi: 10.1109/TDSC.2016.2605087.

[32] H. Krawczyk, HMQV: a high-performance secure Diffie-Hellman protocol, in Advances in Cryptology – CRYPTO 2005, V. Shoup, Ed., vol. 3621 of Lecture Notes in Computer Science, Berlin, Heidelberg, pp. 546-566, 2005. https://doi.org/10.1007/11535218_33.

[33] C. Wang, G. Xu, and J. Sun, An enhanced three-factor user authentication scheme using elliptic curve cryptosystem for wireless sensor networks, Sensors, vol. 17, no. 12, pp. 2946, 2017. https://doi.org/10.3390/s17122946.

[34] R. Amin, S. H. Islam, G. P. Biswas, M. K. Khan, L. Leng, and N. Kumar, Design of an anonymity-preserving three-factor authenticated key exchange protocol for wireless sensor networks, Comput. Netw. vol. 101, pp. 42–62, 2016. https://doi.org/10.1016/j.comnet.2016.01.006.

[35] S. Mangard, E. Oswald, and T. Popp, Power Analysis Attacks: Revealing the Secrets of Smart Cards, Springer Science & Business Media, 2010.

[36] T. H. Kim, C. K. Kim, and I. H. Park, Side channel analysis attacks using AM demodulation on commercial smart cards with SEED, J. Syst. Softw. vol. 85, no. 12, pp. 2899–2908, 2012. https://doi.org/10.1016/j.jss.2012.06.063.

[37] Q. Jiang, S. Zeadally, J. Ma, and D. He, Lightweight threefactor authentication and key agreement protocol for internet-integrated wireless sensor networks, IEEE Access, vol. 5, pp. 3376–3392, 2017. doi: 10.1109/ACCESS.2017.2673239.

[38] Y. Choi, Y. Lee, J. Moon, and D. Won, Security enhanced multi-factor biometric authentication scheme using bio-hash function, PLoS One, vol. 12, no. 5, pp. e0176250, 2017. https://doi.org/10.1371/journal.pone.0176250.

[39] W. Li, Y. Shen, and P. Wang, Breaking Three Remote User Authentication Systems for Mobile Devices, J. Signal Process. Syst. vol. 90, no. 8, pp. 1179–1190, 2018. https://doi.org/10.1007/s11265-017-1305-z.