ID-Based Proxy Signature with Key-Insulated Scheme for Portable Healthcare Devices in 5G-IoHT

Tzu-Wei Lin[1,2], Chien-Lung Hsu[3,4,5,6,7]*

[1] i.School, Feng Chia University, Taiwan
[2] Information Security Office, Office of Information Technology, Feng Chia University, Taiwan
[3] Graduate Institute of Business and Management, Chang Gung University, Taiwan
[4] Department of Information Management, Chang Gung University, Taiwan
[5] Healthy Aging Research Center, Chang Gung University, Taiwan
[6] Department of Visual Communication Design, Ming-Chi University of Technology, Taiwan
[7] Department of Nursing, Chang Gung Memorial Hospital, Taiwan
tweilin@fcu.edu.tw, clhsu@mail.cgu.edu.tw

Abstract

5G networks provides quality of experience and amount of devices communication. Internet of things (IoT) becomes a concept of enclosing several technologies and a network between objects and human beings, and Internet of Health Things (IoHT) combines healthcare systems with portable healthcare devices with 5G environment providing solutions of network layer to solve challenges of smart medical healthcare solutions. IoHT plays a major role in enlightening the people health level and increases the worth of life. However, security and privacy issues of IoHT are rising, and key exposure is one of the problems for devices in IoHT which may endanger not only IoHT but safety and interest of patients and medical institute. In this paper, we introduce and evaluate ID-based proxy signature with key-insulated scheme for portable healthcare devices in 5G-IoHT. Proposed scheme allows emergency secure communications between patient and medical staff and can solve problems above in an efficient way. We also provide security evaluation to prove that proposed scheme is secure enough to against potential attacks.

Keywords: 5G, IoHT, Key-insulated scheme, ID-based proxy signature

1 Introduction

5G (the fifth generation) networks is the newest standard of mobile telecommunication which is being deployed on the earth which provides high-speed network, big capacity, and scalability [1-2]. 5G networks has an efficient effect in energy consumption and provides quality of experience and amount of devices communication. 5G changes connected services and devices through higher reliability, connectivity, and cloud storage and improve quality of devices-to-devices (D2D) communication [1, 3].

To extend Internet to real objects, IoT becomes a concept of enclosing several technologies and a network between objects and human beings, which can interact and cooperate with the other devices to reach communication and sharing information. Sharing information of interconnected objects is the most important mission of IoT, which reflects manufacture, consumption, transportation, smart environments, medical care, and other details of people's life. We focus on one of the IoT applications which combines healthcare systems with portable healthcare devices called Internet of Health Things (IoHT) as Figure 1 [2, 4-7]. Patients wear portable healthcare devices, which can monitor health condition of patients and collect biodata, for self-management. Portable healthcare devices can send data to server in medical institute, and medical staff can access biodata in server to trace health condition of patients for remote healthcare monitoring [4]. No matter where patient is, portable healthcare devices can send data through wireless communication. If any abnormal or emergency situation happens to patient, portable healthcare devices can send emergency message to smart phones of medical staff directly.

Medical healthcare systems face many challenges, such as infrastructure, connections, professional requirements, data management, and real-time monitoring. IoHT with 5G environment provides solutions of network layer, including enhancing quality of service, router and jamming control, resource optimization, etc., to solve challenges of smart medical healthcare solutions [1, 8-9].

Because of rising security and privacy issues about transmitted data in device-to-device communication, development of IoHT is still slow. The primary purpose of interaction between things and objects in IoHT is to combine these objects as a group through wireless networks. In the process of communication, each side must use the same key as the basis for communication to protect transmitted message in IoHT network through wireless communications. However, wireless communications are vulnerable to many adversarial attacks.

*Corresponding Author: Tzu-Wei Lin; E-mail: tweilin@fcu.edu.tw
DOI: https://doi.org/10.70003/160792642025052603001

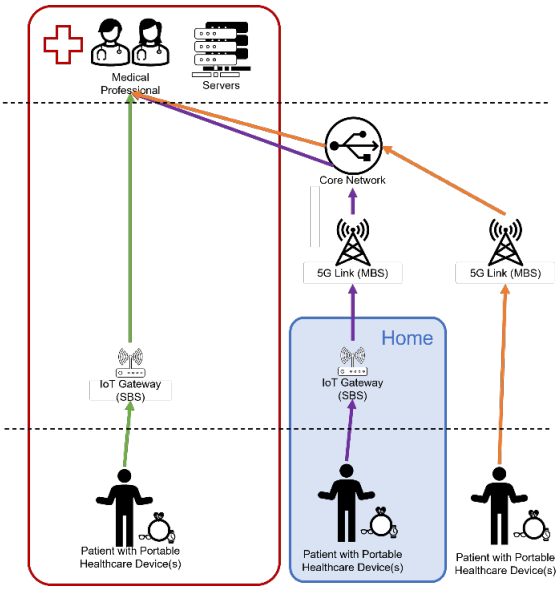

Figure 1. Concept of IoHT

In this paper, we design and evaluate ID-based proxy signature with key-insulated scheme for portable healthcare devices which can solve addressed problems and be suitable for 5G-IoHT environment. The rest of the paper is structured as below. We will introduce telemedicine systems, identity-based (ID-based) cryptosystem, key-insulated encryption, proxy signature mechanism, and Chebyshev chaotic maps (CCM) in literature reviews. Then, we will describe our proposed scheme in detail, and security and performance analysis will be performed. Finally, conclusions will be given.

2 Literature Reviews

Telemedicine systems is a technology of electronic message and telecommunication related to healthcare [10]. Patient sends healthcare related information, which is important, sensitive, and private, to healthcare services through public networks [10]. Medical staffs can know users' health condition if they are able to view information immediately [10]. Data transmission security has been discussed, such as eavesdropping, man-in-the-middle attack, data tempering attack, message modification attack, data interception attack, etc. [11]. Technical support is not enough though Health Insurance Portability and Accountability Act, General Data Protection Regulation, and Safe Harbor Laws have been made [11]. Privacy protection in telemedicine systems has caught researchers' attention [3, 12-14]. One of the keys to the questions for assuring telemedicine environments is that encryption progress should be efficient especially for end point.

The main difference between ID-based [15] and traditional public key cryptosystem is that ID-based cryptosystem derives entity's public key from public information that uniquely identifies the entity. By using such meaningful information, we do not need any certificate to prove validity of corresponding public key. Gentry *et al*. proposed hierarchical ID-based cryptography (HIDC) in 2002 which is able to reduce loading of private key generation (PKG) and risk of key escrow [16]. A key generation center exists at each level in HIDC structure, and the one at the top level is root PKG which is the third trusted center. Legal sub-level key generation centers exist where entities under the same domain. HIDC has been utilized widely including multicast systems [17], cloud computing for IoT environments [18-19], etc. Proposed scheme utilizes ID-based cryptosystem because that devices in IoHT have unique information which can be identified and public key of ID-based cryptosystem, such as series number, MAC address, etc. with mentioned features above.

Key-insulated encryption introduced by Dodis *et al*. [20] is one of the effective solutions to key exposure problems. In IoHT system, portable healthcare devices have limited resource of protecting keys. Any malicious adversary can easily obtain key information of users or devices, which leads to key exposure problems. Once private key is compromised, malicious adversary has chance to use exposed key to submit a legitimate request [21]. In public key cryptosystem with key-insulated, a receiver has two secret keys, a decryption key, and a helper key. Decryption key is a short-term key for decrypting ciphertexts and periodically updated by helper key. More specifically, lifetime of a system is divided into discrete time periods, and receiver can decrypt ciphertext, which is encrypted at some time period, by using a decryption key updated by helper key at the same time period. Decryption key is stored in a powerful but insecure device, and helper key is stored in a physically secure but computationally limited devices called a helper. Researchers have proposed several kinds of key-insulated cryptographic schemes such as symmetric-key-based key-insulated encryption [20], key-insulated signatures [22], parallel key-insulated encryption [21, 23], and so on.

Mambo *et al*. introduced proxy signature mechanisms which provides another solution for key escrow problem in ID-based cryptosystem compared to certificateless-based schemes [24-25]. Proxy signature mechanism includes two roles called original signer and proxy signer. An original signer can delegate signing warrant to proxy signers, and proxy signers can generate proxy signatures on behalf of the original signer. Researchers have already proposed proxy signature schemes for various applications including IoT and smart healthcare environments [26-28].

Chaotic system has properties, a sensitive dependence on initial conditions, pseudo-randomness, and ergodicity, which can correspond to cryptosystem's properties [29-30]. Result is unpredictable if small changes in initial values happen [31-33]. Chaotic system is a complex oscillation and has qualitative change of character of solutions [31-33]. Above features can be correspond to confusion and diffusion of cryptosystem which has been discussed for decades [29-35]. Mathematical definitions of CCM are defined as below.

(1) Chebyshev polynomial $T_n(x):\rightarrow[-1,1]$ is a polynomial in x of degree n, defined as $T_n(x)=cos(ncos^{-1}(x))$.

(2) Recurrent relation of $T_n(x)$ is defined as $T_n(x)$ =

$2xT_{n-1}(x)$-$T_{n-2}(x)$ for any $n \geq 2$, $T_0(x)=1$, and $T_1(x)=x$.

(3) Semi-group property of Chebyshev polynomials establishes $T_r(T_s(x)) = T_{rs}(x) = T_s(T_r(x))$ for any $(s, r) \in Z$ and $s \in [-1, 1]$. The interval $[-1, 1]$ is invariant under the action of the map $T_n(x):[-1, 1] \rightarrow [-1, 1]$. Therefore, Chebyshev polynomial restricted to interval $[-1, 1]$ is a well-known chaotic map for all $n > 1$ which has a unique continuous invariant measure with positive Lyapunov exponent ln n. For $n = 2$, Chebyshev maps reduces to well-known logistic maps.

(4) Zhang proposed an enhanced CCM by proving that semi-group property holds for Chebyshev polynomials defined on interval $(-\infty, +\infty)$ [36]. This paper utilizes following enhanced Chebyshev polynomials where $n \geq 2$, $x \in (-\infty, +\infty)$, and N is a large prime number.

$$T_n(x) = (2xT_{n-1}(x) - T_{n-2}(x)) \bmod N \quad (1)$$

According to Equation (1), semi-group property holds, and enhanced Chebyshev polynomials also commute.

$$T_r(T_s(x)) \bmod N = T_{rs}(x) \bmod N = T_s(T_r(x)) \bmod N \quad (2)$$

(5) Given two elements x and y, finding the integer n such that $T_n(x) \bmod N = y$ is computationally infeasible.

(6) Given three elements x, $T_r(x) \bmod N$, and $T_s(x) \bmod N$, computing $T_{rs}(x) \bmod N$ is computationally infeasible.

Proposed scheme applies extended CCM which satisfies above definitions.

3 Proposed Scheme

Patients in a medical institute or at home wear portable healthcare devices to monitor health condition, and medical staff can monitor health condition of patients from measured data in servers. If an abnormal or emergency situation happens, e.g., a patient falls over without any medical staff or caregiver by the side, an emergency signal or message should be sent to medical staff directly. We introduce ID-based proxy signature with key-insulated scheme for portable healthcare devices which allows emergency secure communications between patient and medical staff in telemedicine systems.

3.1 System Structure

The scheme includes ij patients, j medical staffs, server SV, and smart phone of patient/medical staff. Server SV is responsible for generating essential parameters and functions for the whole scheme. Smart phone is a helper to update keys in patient's portable healthcare devices and medical staff's smart phone. System structure and system syntax model of proposed scheme are illustrated as Figure 2 and Figure 3 respectively.

Proposed scheme includes four phases—preliminary, registration, key update, standard signature and verification, and proxy signature and verification phase. System parameters are generated in preliminary phase. Patient P_{ij} and medical staff D_j need to register to server SV as a legitimate party via a secure channel in registration phase. Patient's smart phone is as a helper to update key of patient P_{ij} . If Patient P_{ij} and medical staff D_j is close enough, standard signature and verification phase will be executed while patient P_{ij} sending message to medical staff D_j, otherwise patient P_{ij} and medical staff D_j have to execute proxy signature and verification phase. Patient P_{ij}, medical staff D_j, and server SV complete registration phase. Table 1 are notations used in proposed scheme.

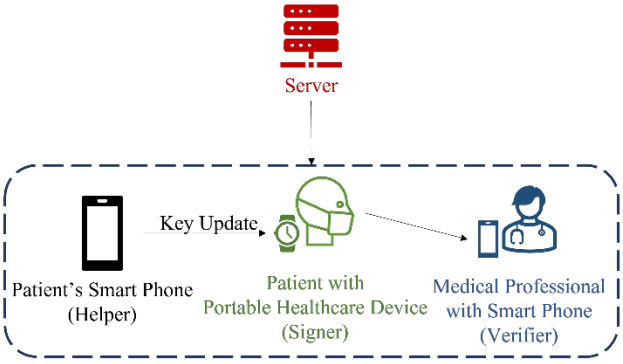

Figure 2. System structure of proposed scheme

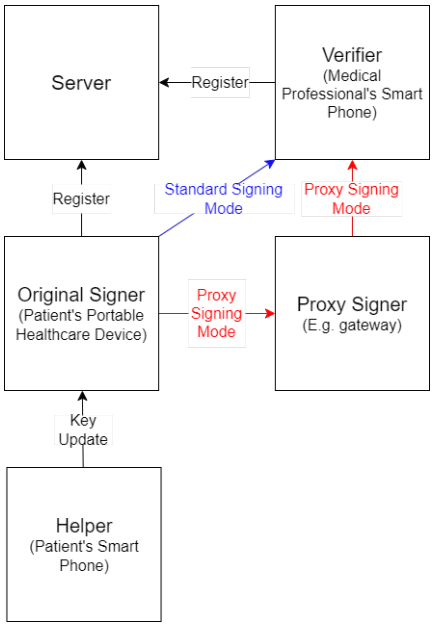

Figure 3. System syntax model of proposed scheme

3.2 Preliminary

System parameters are generated in this phase.

Step 1 Server SV generates secret values $(s_{SV}, \omega_{SV}) \in Z_p^*$, a big prime p, and a random number $x \in (-\infty, +\infty)$ and computes P_{SV} as below.

$$P_{SV} = T_{sSV}(x) \bmod p \quad (3)$$

Step 2 Server SV choses collision-resistance one-way hash functions $(H_0(.), H_1(.), H_2(.))$ where $H:\{0,1\}^* \rightarrow \{0, 1\}^n$ which takes a binary string $q \in \{0,1\}^*$ of any arbitrary length as input and produces a binary string $H_q \in \{0,1\}^n$ as an output.

Table 1. Notations

Notations	Definitions
PID_{ij}	Identity of patient P_{ij} .
GID_i	Identity of proxy signer GW_i .
s_{SV}, ω_{SV}	Secret values of server SV.
p	Big prime generated by server SV.
P_{SV}, P_{HV}, α_{ij}	Public parameters generated by server SV, helper, and patient P_{ij} .
$H(.)$, $H_0(.)$, $H_1(.)$, $H_2(.)$	Collision-resistant one-way hash functions.
x	Random number generated by server SV.
r_{ij}	Random numbers generated by patient P_{ij} .
b_{ij}	Number of key update time.
w_{ij}	Warrant including delegation information generated by patient P_{ij} .
M_{ij}	Message of patient P_{ij} .

3.3 Registration Phase

Patient P_{ij} and medical staff D_j need to register to server SV as a legitimate party via a secure channel. Patient P_{ij}, medical staff D_j, and server SV complete registration phase through following steps.

Step 1 Patient P_{ij} and medical staff D_j choose a random number $r_{ij} \in Z_p^*$ and compute α_{ij} as below. After that, patient P_{ij} and medical staff D_j sends (PID_{ij}, α_{ij}) to server SV.

$$\alpha_{ij} = T_{r_{ij}}(x) \bmod p \tag{4}$$

Step 2 After receiving (PID_{ij}, α_{ij}), server SV computes elements below. Then, server SV returns ($S_{ij,0}$, σ_{ji}) to patient P_{ij} and medical staff D_j .

$$\beta_{ji} = T_{s_{SV}}(\alpha_{ij}) \bmod p \tag{5}$$

$$S_{ij,0} = H_0(PID_{ij} \| \beta_{ji}) \omega_{SV} H_0(PID_{ij} \| 0) \tag{6}$$

$$\sigma_{ji} = P_{SV} H_0(PID_{ij} \| \beta_{ji}) \tag{7}$$

3.4 Key Update Phase

Patient's/medical staff's smart phone can help patient P_{ij} and medical staff D_j to update keys through following steps.

Step 1 Smart phone computes and sends helper key $HK_{ij,\, b_{ij}}$ as below.

$$HK_{ij,b_{ij}} = \omega_{SV}[H_0(PID_{ij} \| b_{ij}) - H_0(PID_{ij} \| b_{ij} - 1)] \tag{8}$$

Step 2 After receiving $HK_{ij,\, b_{ij}}$, patient P_{ij} and medical staff D_j computes $S_{ij,\, b_{ij}}$ to update key.

$$S_{ij,b_{ij}} = S_{ij,b_{ij}} + HK_{ij,b_{ij}} \tag{9}$$

3.5 Standard Signature and Verification Phase

When patient P_{ij} has to send a message to medical staff D_j, patient P_{ij} can sign message before sending message directly. Medical staff D_j can verify message from patient P_{ij} through following steps.

Step 1 Patient P_{ij} computes (σ_{Pij1}, σ_{Pij2}) as below and sends σ_{Pij} to medical staff D_j.

$$\sigma_{P_{ij}1} = S_{PID_{ij},b_{ij}} r_i H_1(M_{ij}) \tag{10}$$

$$\sigma_{P_{ij}2} = \alpha_{ij} \tag{11}$$

$$\sigma_{P_{ij}} = (\sigma_{P_{ij}1}, \sigma_{P_{ij}2}, M_{ij}) \tag{12}$$

Step 2 After receiving σ_{Pij}, medical staff D_j verifies message as below. If it holds, medical staff D_j can confirm that message is send from patient P_{ij} .

$$v_1 = T_{\sigma_{P_{ij}1}}(x) \bmod p \tag{13}$$

$$v_2 = T_{H_0(PID_{ij} \| \sigma_{P_{ij}2})}(x) \bmod p \tag{14}$$

$$v_3 = T_{H_0(PID_{ij} \| b_{ij})}(x) \bmod p \tag{15}$$

$$v_4 = T_{H_1(M_{ij})}(x) \bmod p \tag{16}$$

$$v_1 \,?= v_2 P_{SV} v_3 P_{HA} v_4 \sigma_{P_{ij}2} \tag{17}$$

3.6 Proxy Signature and Verification Phase

If patient P_{ij} cannot send a message to medical staff D_j directly, patient P_{ij} can commissions a nearby proxy signer (e.g., gateway) to sign and send message to medical staff D_j . Medical staff D_j can verify message from patient P_{ij} through following steps.

Step 1 Patient P_i computes (σ_{Pij1}, σ_{Pij2}) as same as in Step 1 of standard signature and verification phase and sends (σ_{Pij}, w_{ij}) to proxy signer GW_i which w_{ij} is a warrant including delegation information generated by patient P_{ij}.

Step 2 After receiving (σ_{Pij}, w_{ij}), proxy signer GW_i computes (σ_{GWi1}, σ_{GWi2}, σ_{GWi3}) as below and sends (σ_{GWi}, w_{ij}) to medical staff D_j.

$$\sigma_{GW_i1} = \sigma_{P_{ij}1} S_{GID_i,\, b_i} r_i H_2(M_{ij}) r_i H_1(w) \tag{18}$$

$$\sigma_{GW_i2} = \sigma_{P_{ij}2} \alpha_i \tag{19}$$

$$\sigma_{GW_i3} = \alpha_i \tag{20}$$

$$\sigma_{GW_i} = (\sigma_{GW_i1}, \sigma_{GW_i2}, \sigma_{GW_i3}, M_{ij}) \tag{21}$$

Step 3 After receiving (σ_{GW_i}, w_{ij}), medical staff D_j verifies message as below. If it holds, medical staff D_j can confirm that message is send from patient P_{ij}.

$$v_1 = T_{\sigma_{GW_i1}}(x) \bmod p \tag{22}$$

$$v_2 = T_{H_0(PID_{ij}\|\sigma_{GW_i2})}(x) \bmod p \tag{23}$$

$$v_3 = T_{H_1(PID_{ij}\|b_{ij})}(x) \bmod p \tag{24}$$

$$v_4 = T_{H_1(M_{ij})}(x) \bmod p \tag{25}$$

$$v_5 = T_{H_0(GID_i\|\sigma_{GW_i3})}(x) \bmod p \tag{26}$$

$$v_6 = T_{H_1(GID_i\|b_s)}(x) \bmod p \tag{27}$$

$$v_7 = T_{H_2(M_{ij})}(x) \bmod p \tag{28}$$

$$v_1 ? = v_2 P_{SV} v_3 P_{HA} v_4 \sigma_{GW_i2} v_5 P_{SV} v_6 P_{HA} v_7 \sigma_{GW_i3} \tag{29}$$

4 Security Analysis

We analyzed security of proposed scheme using random oracle model [37] against A_I, A_{II}, and A_{III} adversaries if computational Diffie–Hellman (CDH) assumption holds, which defines eavesdropping attack to Diffie–Hellman key exchange scheme [38].

Theorem 1. Proposed scheme is secure against an outsider adversary A_I if CDH assumption holds.

Proof. The proof is by contradiction under the random oracle model. Suppose there exists an outsider adversary A_I that has a nonnegligible advantage ϵ in attacking proposed scheme; then we can build another algorithm B that uses A_I to solve the CDH problem. B is given a big prime p and $x \in (-\infty, +\infty)$. which is a random instance of the CDH problem. Its goal is to compute $T_{ab}(x)$ mod p. Algorithm B will simulate the challenger and interact with the forger A_I as described below.

Setup. B selects a big prime p and $x \in (-\infty, +\infty)$. Let ($T_a(x)$ mod p, $T_b(x)$ mod p) be the inputs of the CDH problem. B sets the public key $T_s(x)$ mod p, where $s \in Z_q^*$. B selects three collision-resistant hash functions H_0, H_1, H_2:$\{0, 1\}^*$. B sends (q, p, $T_s(x)$ mod p, H_0, H_1, H_2) to A_I.

Hash queries. In the security proof, the hash functions (H_0, H_1, H_2) are modelled as random oracles. We regard the identity, warrant, and message queries as H_0, H_1, and H_2 queries, respectively. Assume B keeps hash tables T_0, T_1, and T_2 for these queries.

a. H_0 query. For each query on identity ID_i, if ID_i has existed in T_0, the same value $H_0(ID_i)$ is returned to A_{II}. Otherwise, B chooses a random $c_i \in Z_q$ and sets $H_0(ID_i) = T_{c_i}(x)$ mod p. B sends $T_{c_i}(x)$ mod p to A_I as well as stores (ID_i, c_i, $H_0(ID_i)$) to T_0.

b. H_1 query. Assume A_I makes q_{H_1} warrant queries; B selects a random number $\beta \in (1, q_{H_1})$, for each query on warrant w_i such that $1 \le i \ne \beta \le q_{H_1}$; if w_i has existed in T_1, the same value $H_1(w_i)$ is returned to A_I. Otherwise,
   i. If $w_i \ne w_\beta$, B chooses a random $k_i \in Zq$ and sets $H_1(w_\beta) = T_{k_i}(x)$ mod p. B sends $H_1(w_\beta)$ to A_I as well as storing (w_β, k_i, $H_1(w_\beta)$) to T_1.
   ii. If $w_i = w_\beta$, B sets $H_1(w_\beta) = T_a(x)$ mod p. B sends $H_1(w_\beta)$ to A_I .

c. H_2 query. For each query on message M_i accompanying with a warrant w_i, if $H_2(w_i, M_i)$ has existed in T_2, the same value $H_2(w_i, M_i)$ is returned to A_I. Otherwise, B chooses a random $u_i \in Z_q$ and sets $H_2(w_i, M_i) = T_{u_i}(x)$ mod p. B sends $H_2(w_i, M_i)$ to A_I as well as storing ((w_i, M_i), u_i, $H_2(w_i, M_i)$) to T_2.

Original signer's standard signing queries. A_I can query the original signer's standard signature on a warrant w_i. Assume A_I makes $q_{os's}$ queries with the original signer's identity ID_A, for each query on w_i, assume $H_0(ID_A)$ and $H_1(w_i)$ have existed in T_0 and T_1; if they are not the cases, B performs the above algorithms to assign values for $H_0(ID_A)$ and $H_1(w_i)$. Assume $H_0(ID_A) = T_{c_A}(x)$ mod p, B simulates as follows.

a. If $w_i \ne w_\beta$, assume $H_1(w_i) = T_{k_i}(x)$ mod p; then B chooses randomly $r_{A_i} \in Z_q$ and sets $\sigma_{w_i} = (\sigma_{w_i1}, \sigma_{w_i2})$ such that $\sigma_{w_i1} = sH_0(ID_A) + r_{A_i}H_1(w_i)$ and $\sigma_{w_i2} = T_{r_{A_i}}(x)$ mod p.

b. If $w_i = w_\beta$, then B chooses randomly $r_{A_\beta} \in Z_q$ and sets $\sigma\beta = (\sigma_{w\beta1}, \sigma_{w\beta2})$ such that $\sigma_{w\beta1} = sH_0(ID_A) + r_{A\beta}H_1(w_i)$ and $\sigma_{w\beta2} = T_{r_{A\beta}}(x)$ mod p.

Proxy signer's standard signing queries. Assume A_I makes $q_{ps's}$ standard signature queries under the proxy signer's identity ID_B. For each query on $\mathcal{M}_i = (w_i \| M_i)$, assume $H_0(ID_B)$ and $H_2(\mathcal{M}_i)$ have existed in T_0 and T_2; if they are not the cases, B performs the above algorithms to assign values for $H_0(ID_B)$ and $H_2(\mathcal{M}_i)$. Assume $H_0(ID_B) = T_{c_B}(x)$ mod p; B chooses a number $\delta \in (1, q_{ps's})$ and simulates as follows.

a. If $\mathcal{M}_i \ne \mathcal{M}_\delta$, assume $H_2(\mathcal{M}_2) = T_{u_i}(x)$ mod p; then B chooses randomly $r_{B_i} \in Z_q$ and sets $\sigma_{p_i} = (\sigma_{p_i1}, \sigma_{p_i2})$ such that $\sigma_{p_i1} = sH_0(ID_B) + r_{B_i}H_1(\mathcal{M}_i)$ and $\sigma_{p_i2} = T_{r_{B_i}}(x)$ mod p.

b. If $\mathcal{M}_i = \mathcal{M}_\delta$, assume $H_2(\mathcal{M}_\delta) = T_{u_\delta}(x)$ mod p; then B sets $dsk_\delta = (\sigma_{B1_\delta}, \sigma_{B2_\delta})$ such that $\sigma_{B1_\delta} = sH_0(ID_B) + bH_2(\mathcal{M}_\delta)$ and $\sigma_{B2_\delta} = T_b(x)$ mod p.

Forgery. Assume A_I outputs a valid proxy signature $\sigma^* = (\sigma^*_{\mathcal{M}_1}, \sigma^*_{\mathcal{M}_2}, \sigma^*_{\mathcal{M}_3})$ on message **M*** under a warrant **W*** with the proxy signer's identity ID_A and the proxy signer's identity ID_B. Besides,

a. (ID_A, **W***) has been queried in the original signer's standard signing queries.

b. (ID_B, **W***, **M***) has been queried in the proxy signer's standard signing queries.

If **W*** $\ne w_\beta$ or **M*** $\ne \mathcal{M}_\delta$, B will abort. Otherwise, given the forged proxy signature $\sigma^* = (\sigma^*_{\mathcal{M}_1}, \sigma^*_{\mathcal{M}_2}, \sigma^*_{\mathcal{M}_3})$. B can solve the CDH problem.

B will not abort when **W*** $= w_\beta$ and **M*** $= \mathcal{M}_\delta$. Thus, if there exists an outsider adversary A_I that has

a nonnegligible probability ϵ in breading the proposed identity-based proxy signature scheme, then there exists another probabilistic polynomial time algorithm B that has a probability as Equation (30) which is nonnegligible. Thus, we reach a contradiction.

$$succ_B^{CDH} = \frac{\epsilon}{q_{os's} \cdot q_{ps's}} \tag{30}$$

Theorem 2. Proposed scheme is secure against an outsider adversary A_{II} chosen identity and chosen warrant attacks if the CDH assumption holds.

Proof. A_{II} is a malicious proxy signer possessing the private key of the proxy signer. The simulation is as follows.

Setup. B selects a big prime p and $x \in (-\infty, +\infty)$. Let ($T_a(x)$ mod p, $T_b(x)$ mod p) be the inputs of the CDH problem. B sets the public key $T_s(x)$ mod p, where $s \in Z_q^*$. B selects three collision-resistant hash functions H_0, H_1, H_2: $\{0,1\}^*$. B sends (q, p, $T_s(x)$ mod p, H_0, H_1, H_2) to A_{II}.

Hash queries. Regard the identity, warrant, and message queries as H_0, H_1, and H_2 queries, respectively. B keeps hash tables T_0, T_1, and T_2 for these queries.

a. H_0 query. If assume A_{II} makes q_{H_0} identity queries, choose $\alpha \in (1, q_{H_0})$, for each query on identity ID_i such that $1 \le i \ne \alpha \le q_{H_0}$, if ID_i has existed in T_0, the same value $H_0(ID_i)$ is returned to A_{II}. Otherwise,
   i. If $i \ne \alpha$, B chooses a random $c_i \in Z_q$ and sets $H_0(ID_i) = T_{c_i}(x)$ mod p. B sends $T_{c_i}(x)$ mod p to A_{II} as well as storing (ID_i, c_i, $H_0(ID_i)$) to T_0.
   ii. If $i = \alpha$, B sets $H_0(ID_\alpha) = T_{bc_\alpha}(x)$ mod p, where $c_\alpha \in Z_q$ and returns $H_0(ID_i)$ to A_{II}. B adds (ID_α, c_α, $H_0(ID_\alpha)$) to T_0.

b. H_1 query. Assume A_{II} makes q_{H_1} warrant queries; B selects a random number $\beta \in (1, q_{H_1})$, for each query on warrant w_i such that $1 \le i \ne \beta \le q_{H_1}$; if w_i has existed in T_1, the same value $H_1(w_i)$ is returned to A_{II}. Otherwise,
   i. If $w_i \ne w_{\beta|ID_\alpha \to o}$, which means ID_α is included in w_i and the user with identity ID_α plays the role of original signer in the system. B chooses a random $k_i \in Z_q$ and sets $H_1(w_i) = T_{k_i}(x)$ mod p/ $T_b(x)$ mod p. B sends $H_1(w_i)$ to A_{II} as well as storing (w_i, b_i, $H_1(w_i)$) to T_1.
   ii. If $w_i \ne w_{\beta|ID_\alpha \to p}$, which means ID_α is included in w_i and the user with identity ID_α plays the role of proxy signer in the system. B chooses a random $k_i \in Z_q$ and sets $H_1(w_i) = T_{k_i}(x)$ mod p. B sends $H_1(w_i)$ to A_{II} as well as stores (w_i, k_i, $H_1(w_i)$) to T_1.
   iii. If $w_i = w_\beta$, B chooses a random $k_i \in Z_q$ and sets $H_1(w_\beta) = T_{k_i}(x)$ mod p. B sends $H_1(w_\beta)$ to A_{II} as well as storing (w_β, k_i, $H_1(w_\beta)$) to T_1.

c. H_2 query. Assume A_{II} makes q_{H_2} message queries, B selects a random number $\delta \in (1, q_{H_1})$, for each query on message M_i accompanying with a warrant w_i such that $1 \le i \ne \delta \le q_{H_2}$; if $H_2(w_i, M_i)$ has existed in T_2, the same value $H_2(w_i, M_i)$ is returned to A_{II}. Otherwise,
   i. If $w_i \ne w_\beta$, B chooses a random $u_i \in Z_q$ and sets $H_2(w_i, M_i) = T_{u_i a}(x)$ mod p. B sends $H_2(w_i, M_i)$ to A_{II} as well as storing ((w_i, M_i), u_i, $H_2(w_i, M_i)$) to T_2.
   ii. If $w_i = w_\beta$, $M_i \ne M_\delta$, the same as the case when $w_i \ne w_\beta$, $M_i \ne M_\delta$.
   iii. If $w_i \ne w_\beta$, $M_i = M_\delta$, the same as the case when $w_i \ne w_\beta$, $M_i \ne M_\delta$.
   iv. If $w_i = w_\beta$, $M_i = M_\delta$, B chooses a random $u_i \in Z_q$ and sets $H_2(w_\beta, M_\delta) = T_{u_i}(x)$ mod p. B sends $H_2(w_\beta, M_\delta)$ to A_{II} as well as storing ((w_β, M_δ), u_i, $H_2(w_\beta, M_\delta)$) to T_2.

Key extraction queries. A_{II} can make key extraction queries on any identity $ID \in \mathbf{ID}$ such that $ID \ne ID_\alpha$. If A_{II} makes key extraction query on identity ID_α, B just terminates the simulation and reports a failure. Assume A_{II} makes q_k key extractions queries, for each query on identity ID_i for $1 \le i \le q_k$.

a. If ID_i has existed in table T_0, assume $H_0(ID_i) = T_{c_i}(x)$ mod p; then B returns $sk_{ID_i} = aH_0(ID_i)$ to A_{II}.
b. Otherwise, B chooses a random $c_i \in Z_q$ and sets $H_0(ID_i) = T_{c_i}(x)$ mod p. B returns $sk_{ID_i} = T_{c_i a}(x)$ mod p to A_{II} and adds (ID_i, c_i, $H_0(ID_i)$) to T_0.

Original signer's standard signing queries. A_{II} can query original signer's standard signature on a warrant $w_i \in \mathbf{W}$ under an identity $ID_i \in \mathbf{ID}$. Assume A_{II} makes $q_{os's}$ original signer's standard signing queries. For each query, assume ID_i and w_i have been submitted to the H_0 and H_1 queries, respectively. If they are not the cases, B performs the above algorithms to set values for $H_0(ID_i)$ and $H_1(w_i)$; then B simulates σ_{w_i} as follows.

a. If $ID_i \ne ID_\alpha$ and $w_i \ne w_{\beta|ID_\alpha \to o}$, assume $H_1(ID_i) = T_{c_i}(x)$ mod p and $H_1(w_i) = T_{k_i}(x)$mod $p/T_b(x)$mod p, respectively; then B chooses a random $r_i \in Z_q$ and returns the original signer's standard signature $\sigma_{w_i} = (\sigma_{w_i 1}, \sigma_{w_i 2})$ such that $\sigma_{w_i 1} = sk_{ID_i} + r_i H_1(w_i)$ and $\sigma_{w_i 2} = T_{r_i}(x)$ mod p and to A_{II}.
b. If $ID_i \ne ID_\alpha$ and $w_i \ne w_{\beta|ID_\alpha \to p}$, assume $H_1(ID_i) = T_{c_i}(x)$ mod p and $H_1(w_i) = T_{k_i}(x)$ mod p, respectively; then B chooses a random $r_i \in Z_q$ and returns original signer's standard signature $\sigma_{w_i} = (\sigma_{w_i 1}, \sigma_{w_i 2})$ such that $\sigma_{w_i 1} = sk_{ID_i} + r_i H_1(w_i)$ and $\sigma_{w_i 2} = T_{r_i}(x)$ mod p to A_{II}.
c. If $ID_i = ID_\alpha$ and $w_i \ne w_{\beta|ID_\alpha \to o}$, assume $H_0(ID_i) = T_{bc_i}(x)$ mod p and $H_1(w_i) = T_{k_i}(x)$ mod $p/T_b(x)$ mod p, respectively; then B simulates the original signer's standard signature $\sigma_{w_i} = (\sigma_{w_i 1}, \sigma_{w_i 2})$.
d. If $ID_i = ID_\alpha$ and $w_i \ne w_{\beta|ID_\alpha \to p}$, since we do not consider self-delegation in our scheme, then B just terminates the simulation and reports failure.
e. If $ID_i = ID_\alpha$ and $w_i = w_\beta$, B terminates the simulation and reports failure.

Proxy signing queries. A_{II} can query a proxy signature on a message $M_i \in \mathbf{M}$ under a warrant $w_i \in \mathbf{W}$ with the proxy signer's identity ID_{1i} and the original signer's identity ID_{2i} such that ID_{1i}, $ID_{2i} \in \mathbf{ID}$. Assume ID_{1i}, ID_{2i} have been submitted to the H_0 query and w_i and ($w_i \| M_i$)

have been submitted to the H_1 and H_2 queries, respectively. If they are not the cases, the above algorithms will be performed to assign new values $H_0(ID_{1i})$, $H_0(ID_{2i})$, $H_1(w_i)$, and $H_2(w_i, M_i)$. Assume A_{II} makes q_{ps} proxy signing queries. For each query on a message M_i with warrant w_i such that $1 \le i \le q_{ps}$, B simulates the corresponding proxy signature as follows.

a. If $ID_{1i} \neq ID_\alpha$, $ID_{2i} \neq ID_\alpha$ assume $H_0(ID_{1i})=T_{c_{1i}}(x) \bmod p$, $H_0(ID_{2i})=T_{c_{2i}}(x) \bmod p$; then B chooses two random numbers r_{1i}, $r_{2i} \in Z_q$ and returns the proxy signature $\sigma_i=(\sigma_{M_i1}, \sigma_{M_i2}, \sigma_{M_i3})$ to A_{II}.

b. If $ID_{1i} \neq ID_\alpha$, $ID_{2i} = ID_\alpha$, assume $H_0(ID_{1i})=T_{c_{1i}}(x) \bmod p$, $H_0(ID_{2i})= T_{c_\alpha b}(x) \bmod p$; then
   i. If $w_i \neq w_{\beta|ID_\alpha \to o}$, $M_i \neq M_\delta$ or $w_i \neq w_{\beta|ID_\alpha \to o}$, $M_i = M_\delta$, B terminates the simulation and reports failure.
   ii. If $w_i \neq w_{\beta|1D_\alpha \to p}$ and $M_i \neq M_\delta$, assume $H_1(w_i)=T_{k_i}(x) \bmod p$ and $H_2(w_i, M_i) = T_{u_ia}(x) \bmod p$; B simulates the proxy signature $\sigma_i=(\sigma_{M_i1}, \sigma_{M_i2}, \sigma_{M_i3})$.
   iii. If $w_i \neq w_{\beta|ID_\alpha \to p}$, $M_i = M_\delta$ or $w_i = w_\beta$, $M_i \neq M_\delta$, B performs the same as that in case ii.
   iv. If $w_i = w_\beta$ and $M_i = M_\delta$, B terminates the simulation and reports failure.

c. If $ID_{1i} = ID_\alpha$, $ID_{2i} \neq ID_\alpha$, assume $H_0(ID_{1i})=T_{c_\alpha b}(x) \bmod p$, $H_0(ID_{2i})=T_{c_{2i}}(x) \bmod p$, then
   i. If $w_i \neq w_{\beta|ID_\alpha \to o}$ and $M_i \neq M_\delta$, assume $H_1(w_i) = T_{k_i}(x) \bmod p / T_b(x) \bmod p$ and $H_2(w_i, M_i) = T_{u_ia}(x) \bmod p$. B simulates the proxy signature $\sigma_i=(\sigma_{M_i1}, \sigma_{M_i2}, \sigma_{M_i3})$.
   ii. If $w_i \neq w_{\beta|ID_\alpha \to p}$, $M_i \neq M_\delta$ or $w_i \neq w_{\beta|ID_\alpha \to p}$, $M_i = M_\delta$, B terminates the simulation and reports failure.
   iii. If $w_i \neq w_{\beta|ID_\alpha \to o}$ and $M_i = M_\delta$, assume $H_1(w_i) = T_{k_i}(x) \bmod p / T_b(x) \bmod p$ and $H_2(w_i, M_i) = T_{u_ia}(x) \bmod p$; B performs the same as that in case i.
   iv. If $w_i = w_\beta$ and $M_i \neq M_\delta$, assume $H_1(w_\beta) = T_{k_i}(x) \bmod p$ and $H_2(w_\beta, M_i) = T_{u_ia}(x) \bmod p$; B simulates the proxy signature $\sigma_i=(\sigma_{M_i1}, \sigma_{M_i2}, \sigma_{M_i3})$.
   v. If $w_i = w_\beta$ and $M_i = M_\delta$, B terminates the simulation and reports failure.

d. If $ID_{1i} = ID_\alpha$, $ID_{2i} = ID_\alpha$, B terminates the simulation and reports failure.

Forgery: assume A_{II} outputs a valid proxy signature $\sigma^*=(\sigma^*_{\mathcal{M}_1}, \sigma^*_{\mathcal{M}_2}, \sigma^*_{\mathcal{M}_3})$ on message **M*** under a warrant **W*** with the proxy signer's identity ID_A and the proxy signer's identity ID_B. Besides,

a. ID_A has not been queried in the key extraction queries.
b. (ID_A, **W***) has not been queried in the delegation queries.
c. (ID_A, ID_B, **W***, **M***) has not been queried in the proxy signing queries, If $H_0(ID_A) \neq T_{c_\alpha b}(x) \bmod p$ or $H_1(\mathbf{W}^*) \neq T_{k_\beta}(x) \bmod p$ or $H_2(\mathbf{W}^*, \mathbf{M}^*) \neq T_{u_\delta}(x) \bmod p$, B will abort. Otherwise, given the forged proxy signature $\sigma^*=(\sigma^*_{\mathcal{M}_1}, \sigma^*_{\mathcal{M}_2}, \sigma^*_{\mathcal{M}_3})$. B can solve the CDH problem when $H_0(ID_A)=T_{c_\alpha b}(x) \bmod p$, $H_1(ID_B)=T_{k_\beta}(x) \bmod p$, and $H_2(\mathbf{W}^*, \mathbf{M}^*)=T_{u_\delta}(x) \bmod p$.

Next, we analysed the success probability of B; B will not abort if the following conditions hold.

a. $ID_A = ID_\alpha$.
b. $\mathbf{W}^* = w_\beta$.
c. $\mathbf{M}^* = M_\delta$.

Therefore, if A_{II} has a nonnegligible probability ϵ in breaking the proposed IDPS-KI scheme, then the success probability of B in solving CDH problem is as Equation (31) which is nonnegligible. Thus, we reach a contradiction.

$$succ_B^{CDH} \ge \frac{\epsilon}{(q_{H_0} + q_k + q_{os's} + 2q_{ps})(q_{H_1} + q_{os's} + q_{p_s})(q_{H_2} + q_{ps})} \quad \textbf{(31)}$$

Theorem 3. Proposed scheme is secure against A_{III} chosen message and identity attack if the CDH assumption holds.

Proof. The security is similar to that in Theorem 2. Thus, we describe it briefly.

Setup, **hash queries**, and **key extract queries** are the same as those in the security proof against a malicious proxy signer.

Proxy signer's standard signing queries and **proxy signing queries** are similar to the **original signer's standard signing queries** and **proxy signing queries** in the security for Theorem 2.

Through simulation, it can be reduced that if there exists a malicious original signer that can break the proposed scheme with a nonnegligible probability ϵ, then we can build another probabilistic polynomial time algorithm B that can solve the CDH problem with a nonnegligible probability as Equation (32) where $q_{ps's}$ refers to the number of proxy signer's standard signing queries. Thus, we reach a contradiction.

$$succ_B^{CDH} \ge \frac{\epsilon}{(q_{H_0} + q_k + q_{ps's} + 2q_{ps})(q_{H_1} + q_{ps's} + q_{p_s})(q_{H_2} + q_{ps})} \quad \textbf{(32)}$$

In summary, proposed scheme is secure enough to against A_I, A_{II}, and A_{III} adversaries if CDH assumption holds after proving through random oracle models [37].

5 Performance Analysis

According to previous research, times of performing a one-way hash function operation (T_h) is about 0.006 milliseconds (ms), and time for performing a CCM operation (T_{ch}) is about 0.252ms [39-42], and using CCM can be more efficient than using elliptic-curve cryptography. We present results of computational complexity and performing time of proposed scheme in Table 2. Performing standard signature and verification phase will spend at least 0.786ms. Performing proxy signature and verification phase will spend at least 1.572ms.

Table 2. Computational complexity and performing time of proposed scheme

Role \ Phase	Standard signature and verification	Proxy signature and verification
Patient	T_h=0.006ms	T_h=0.006ms
Medical staff	$4T_{ch}+3T_h$ =(0.024+0.756)ms =0.78ms	$7T_{ch}+6T_h$ =(0.042+1.512)ms =1.554ms
Gateway	N/A	$2T_h$=(0.012)ms

6 Conclusion

5G provides amount of devices communication, and IoT arranges objects in distributed network, which can interact and cooperate with other devices. We focus on IoHT which combines healthcare systems with portable healthcare devices, and 5G provides solutions of network layer to solve challenges of smart medical healthcare solutions. Key exposure is one of the security and privacy issues of IoHT which may endanger not only IoHT but safety and interest of patients and medical institutes. We introduce and evaluate ID-based proxy signature with key-insulated scheme for portable healthcare devices in 5G-IoHT, which can solve problems above in an efficient way, and we also provide security analysis to prove that proposed scheme is secure enough to against potential attacks.

Acknowledgement

This research was funded by Nation Science & Technology Council NSTC-111-2410-H-182-007-MY2 and 112-2634-F-004-001-MBK and Chang Gung Memorial Hospital Research Project (CMRP) CARPD3P0011.

References

[1] A. Ahad, M. Tahir, K. L. A. Yau, 5g-Based Smart Healthcare Network: Architecture, Taxonomy, Challenges and Future Research Directions, *IEEE Access*, Vol. 7, No. pp. 100747-100762, July, 2019. https://doi.org/10.1109/ACCESS.2019.2930628

[2] L. Chettri, R. Bera, A Comprehensive Survey on Internet of Things (Iot) toward 5g Wireless Systems, *IEEE Internet of Things Journal*, Vol. 7, No. 1, pp. 16-32, January, 2020. https://doi.org/10.1109/JIOT.2019.2948888

[3] S. Anwar, R. Prasad, Framework for Future Telemedicine Planning and Infrastructure Using 5g Technology, *Wireless Personal Communications*, Vol. 100, No. 1, pp. 193-208, May, 2018. https://doi.org/10.1007/s11277-018-5622-8

[4] S. J. Bhasha, P. Sunita, An Iot-Based Body Area Network in Medical Care System: Related Challenges and Issues, *International Journal of Innovative Technology and Exploring Engineering*, Vol. 9, No. 1 pp. 541-546, November, 2019. http://doi.org/10.35940/ijitee.L2545.119119

[5] S. A. Chaudhry, A. Irshad, M. A. Khan, S. A. Khan, S. Nosheen, A. A. AlZubi, Y. B. Zikria, A Lightweight Authentication Scheme for 6g-Iot Enabled Maritime Transport System, *IEEE Transactions on Intelligent Transportation Systems*, Vol. 24, No. 2, pp. 2401-2410, February 2023. https://doi.org/10.1109/TITS.2021.3134643

[6] S. A. Chaudhry, A. Irshad, J. Nebhen, A. K. Bashir, N. Moustafa, Y. D. Al-Otaibi, Y. B. Zikria, An Anonymous Device to Device Access Control Based on Secure Certificate for Internet of Medical Things Systems, *Sustainable Cities and Society*, Vol. 75, Article No. 103322, December, 2021. https://doi.org/10.1016/j.scs.2021.103322

[7] H. D. Jude, V. E. Balas, *Telemedicine Technologies: Big Data, Deep Learning, Robotics, Mobile and Remote Applications for Global Healthcare*, Elsevier Science, 2019.

[8] M. Chen, J. Yang, J. Zhou, Y. Hao, J. Zhang, C.-H. Youn, 5g-Smart Diabetes: Toward Personalized Diabetes Diagnosis with Healthcare Big Data Clouds, *IEEE Communications Magazine, Communications Magazine*, *IEEE Communications Magazine*, Vol. 56, No. 4, pp. 16-23, April, 2018. https://doi.org/10.1109/MCOM.2018.1700788

[9] J. Lloret, L. Parra, M. Taha, J. Tomás, An Architecture and Protocol for Smart Continuous Ehealth Monitoring Using 5g, *Computer Networks*, Vol. 129, pp. 340-351, December, 2017. https://doi.org/10.1016/j.comnet.2017.05.018

[10] Á. Garai, I. Péntek, A. Adamkó, Revolutionizing Healthcare with Iot and Cognitive, Cloud-Based Telemedicine, *Acta Polytechnica Hungarica*, Vol. 16, No. 2, pp. 163-181, 2019.

[11] I. A. Zriqat, A. Altamimi, Security and Privacy Issues in Ehealthcare Systems: Towards Trusted Services, *International Journal of Advanced Computer Science and Applications*, Vol. 7, No. 9, pp. 229-236, 2016. https://dx.doi.org/10.14569/IJACSA.2016.070933

[12] D. Dharminder, D. Mishra, X. Li, Construction of Rsa-Based Authentication Scheme in Authorized Access to Healthcare Services, *Journal of Medical Systems*, Vol. 44, No. 1, Article No. 6, January, 2020. https://doi.org/10.1007/s10916-019-1471-6

[13] K. Renuka, S. Kumari, X. Li, Design of a Secure Three-Factor Authentication Scheme for Smart Healthcare, *Journal of Medical Systems*, Vol. 43, No. 5, Article No. 133, May, 2019. https://doi.org/10.1007/s10916-019-1251-3

[14] V. Sureshkumar, R. Amin, M. S. Obaidat, I. Karthikeyan, An Enhanced Mutual Authentication and Key Establishment Protocol for Tmis Using Chaotic Map, *Journal of Information Security and Applications*, Vol. 53, Article No. 102539, August, 2020. https://doi.org/10.1016/j.jisa.2020.102539

[15] A. Shamir, Identity-Based Cryptosystems and Signature Schemes, in: G. R. Blakley, D. Chaum (Eds.), *Advances in Cryptology*, Berlin, Heidelberg, 1985, pp. 47-53. https://doi.org/10.1007/3-540-39568-7_5

[16] C. Gentry, A. Silverberg, Hierarchical Id-Based Cryptography, in: Y. Zheng (Eds.), *Advances in Cryptology — ASIACRYPT 2002*, Berlin, Heidelberg, 2002, pp. 548-566.

[17] V. R. L. Shen, W.-C. Huang, A Time-Bound and Hierarchical Key Management Scheme for Secure Multicast Systems, *Wireless Personal Communications*, Vol. 85, No. 4, pp. 1741-1764, December, 2015. https://doi.org/10.1007/s11277-015-2865-5

[18] P. Fremantle, B. Aziz, Cloud-Based Federated Identity for the Internet of Things, *Annals of Telecommunications*, Vol.

73, No. 7-8, pp. 415-427, August, 2018. https://doi.org/10.1007/s12243-018-0641-8

[19] M. L. B. A. Santos, J. C. Carneiro, A. M. R. Franco, F. A. Teixeira, M. A. A. Henriques, L. B. Oliveira, Flat: Federated Lightweight Authentication for the Internet of Things, *Ad Hoc Networks*, Vol. 107, Article No. 102253, October, 2020. https://doi.org/10.1016/j.adhoc.2020.102253

[20] Y. Dodis, J. Katz, S. Xu, M. Yung, Key-Insulated Public Key Cryptosystems, in: L.R. Knudsen (Eds.), *Advances in Cryptology — EUROCRYPT 2002*, Berlin, Heidelberg, 2002, pp. 65-82. https://doi.org/10.1007/3-540-46035-7_5

[21] J. Cui, J. Lu, H. Zhong, Q. Zhang, C. Gu, L. Liu, Parallel Key-Insulated Multiuser Searchable Encryption for Industrial Internet of Things, *IEEE Transactions on Industrial Informatics*, Vol. 18, No. 7, pp. 4875-4883, July, 2022. https://doi.org/10.1109/TII.2021.3110193

[22] Y. Dodis, J. Katz, S. Xu, M. Yung, Strong Key-Insulated Signature Schemes, in: Y. G. Desmedt (Eds.), *Public Key Cryptography — PKC 2003*, Berlin, Heidelberg, 2003, pp. 130-144. https://doi.org/10.1007/3-540-36288-6_10

[23] B. Libert, J.-J. Quisquater, M. Yung, Parallel Key-Insulated Public Key Encryption without Random Oracles, In: T. Okamoto, X. Wang (Eds.), *Public Key Cryptography – PKC 2007*, Berlin, Heidelberg, 2007, pp. 298-314. https://doi.org/10.1007/978-3-540-71677-8_20

[24] M. Mambo, K. Usuda, E. Okamoto, Proxy Signatures: Delegation of the Power to Sign Messages, *IEICE transactions on fundamentals of electronics, communications and computer sciences*, Vol. E-79-A, No. 9, pp. 1338-1354, September, 1996.

[25] D. He, Y. Chen, J. Chen, An Efficient Certificateless Proxy Signature Scheme without Pairing, *Mathematical and Computer Modelling*, Vol. 57, No. 9-10, pp. 2510-2518, May, 2013. https://doi.org/10.1016/j.mcm.2012.12.037

[26] X. Jia, D. He, Q. Liu, K.-K. R. Choo, An Efficient Provably-Secure Certificateless Signature Scheme for Internet-of-Things Deployment, *Ad Hoc Networks*, Vol. 71, pp. 78-87, March, 2018. https://doi.org/10.1016/j.adhoc.2018.01.001

[27] I. A. Kamil, S. O. Ogundoyin, A Lightweight Clas Scheme with Complete Aggregation for Healthcare Mobile Crowdsensing, *Computer Communications*, Vol. 147, pp. 209-224, November, 2019. https://doi.org/10.1016/j.comcom.2019.08.027

[28] G. K. Verma, B. B. Singh, N. Kumar, M. S. Obaidat, D. He, H. Singh, An Efficient and Provable Certificate-Based Proxy Signature Scheme for Iiot Environment, *Information Sciences*, Vol. 518, pp. 142-156, May, 2020. https://doi.org/10.1016/j.ins.2020.01.006

[29] E.-J. Yoon, I.-S. Jeon, An Efficient and Secure Diffie–Hellman Key Agreement Protocol Based on Chebyshev Chaotic Map, *Communications in Nonlinear Science and Numerical Simulation*, Vol. 16, No. 6, pp. 2383-2389, June, 2011. https://doi.org/10.1016/j.cnsns.2010.09.021

[30] E.-J. Yoon, K.-Y. Yoo, Cryptanalysis of Group Key Agreement Protocol Based on Chaotic Hash Function, *IEICE Transactions on Information and Systems*, Vol. E94. D, No. 11, pp. 2167-2170, November, 2011.

[31] L. Kocarev, Chaos-Based Cryptography: A Brief Overview, *IEEE Circuits and Systems Magazine*, Vol. 1, No. 3, pp. 6-21, 2001. https://doi.org/10.1109/7384.963463

[32] L. Kocarev, S. Lian, *Chaos-Based Cryptography: Theory, Algorithms and Applications*, Springer Berlin, Heidelberg, 2011.

[33] D. Solev, P. Janjic, L. Kocarev, *Introduction to Chaos*, in: L. Kocarev, S. Lian (Eds.), Chaos-Based Cryptography, Springer, Berlin, Heidelberg, 2011, pp. 1-25. https://doi.org/10.1007/978-3-642-20542-2_1

[34] H.-Y. Lin, Improved Chaotic Maps-Based Password-Authenticated Key Agreement Using Smart Cards, *Communications in Nonlinear Science and Numerical Simulation*, Vol. 20, No. 2, pp. 482-488, February, 2015. https://doi.org/10.1016/j.cnsns.2014.05.027

[35] T.-F. Lee, C.-H. Hsiao, S.-H. Hwang, T.-H. Lin, Enhanced Smartcard-Based Password-Authenticated Key Agreement Using Extended Chaotic Maps, *PLOS ONE*, Vol. 12, No. 7, Article No. e0181744, July, 2017. https://doi.org/10.1371/journal.pone.0181744

[36] L. Zhang, Cryptanalysis of the Public Key Encryption Based on Multiple Chaotic Systems, *Chaos, Solitons & Fractals*, Vol. 37, No. 3, pp. 669-674, August, 2008. https://doi.org/10.1016/j.chaos.2006.09.047

[37] M. Bellare, P. Rogaway, Random Oracles Are Practical: A Paradigm for Designing Efficient Protocols, Fairfax, Virginia, USA, 1993, pp. 62-73.

[38] M. Bellar; P. Rogaway, *Introduction to Modern Cryptography*, 2005.

[39] L. Yan, C. Rong, G. Zhao, Strengthen Cloud Computing Security with Federal Identity Management Using Hierarchical Identity-Based Cryptography, in: M. G. Jaatun, G. Zhao, C. Rong (Eds.), *Cloud Computing*, Berlin, Heidelberg, 2009, pp. 167-177. https://doi.org/10.1007/978-3-642-10665-1_15

[40] C. Hu, P. Liu, S. Guo, Q. Xu, Anonymous Hierarchical Identity-Based Encryption with Bounded Leakage Resilience and Its Application, *International Journal of High Performance Computing and Networking*, Vol. 10, No. 3, pp. 226-239, 2017. https://doi.org/10.1504/IJHPCN.2017.084251

[41] B. Ying, A. Nayak, Lightweight Remote User Authentication Protocol for Multi-Server 5g Networks Using Self-Certified Public Key Cryptography, *Journal of Network and Computer Applications*, Vol. 131, No. pp. 66-74, April, 2019. https://doi.org/10.1016/j.jnca.2019.01.017

[42] I. ul haq, J. Wang, Y. Zhu, Secure Two-Factor Lightweight Authentication Protocol Using Self-Certified Public Key Cryptography for Multi-Server 5g Networks, *Journal of Network and Computer Applications*, Vol. 161, Article No. 102660, July, 2020. https://doi.org/10.1016/j.jnca.2020.102660

Biographies

Tzu-Wei Lin is an assistant professor of i.School at Feng Chia University (FCU) in Taiwan, R.O.C. He received a B.S. degree in information management, an M.S. degree in information management, and a Ph.D. degree in business and management from Chang Gung University, Taiwan in 2011, 2013, and 2021, respectively. Currently, he is director of Information Security Office, Office of Information Technology, FCU.

Chien-Lung Hsu is a professor of Information Management Department at Chang Gung University, Taiwan (R.O.C.). He received a B.S. degree in business administration, an M.S. degree in information management, and a Ph.D. degree in information management from

National Taiwan University of Science and Technology, Taiwan in 1995, 1997, and 2002, respectively. Currently, he is the director of Chinese Cryptology & Information Security Association, director of Taiwan Association for Medical Informatics, and a senior researcher of Taiwan Information Security Center, Taiwan, (R.O.C.).