Journal of Network Intelligence
Taiwan Ubiquitous Information
©2022 ISSN 2414-8105 (Online)
Volume **7**, Number **1**, February **2022**

Attribute-based Message Recovery Designated Verifier Proxy Signature Scheme in Telemedicine System

Yu Hu

School of Computer Science, Minnan Normal University
Zhangzhou, 363000, China
yuhucn@126.com

Yi-Fan Zhang

School of Computer Science, Minnan Normal University
Zhangzhou, 363000, China
1021784165@qq.com

Hui Huang

School of Computer Science, Minnan Normal University
Zhangzhou, 363000, China
hhui323@163.com

Yu-Ping Zhou*

School of Computer Science, Minnan Normal University
Key Laboratory of Data Science and Intelligence Application, Fujian Province University
Zhangzhou, 363000, China
Corresponding Author: yp_ zhou@mnnu.edu.cn

Received November 2021; revised January 2022

Abstract. *With the promotion of cloud medical diagnostic applications, the telemedicine system has become increasingly mature, which brings about much convenience to the people's lives. Meanwhile, the diagnostic time was greatly reduced. Due to telemedicine system usually involves the sensitive information of users, the privacy issue is urgently to be solved. In order to solve the above problem, an attribute-based designated verifier proxy signature scheme, combined with message recovery, is proposed for the telemedicine system. A proxy delegation is designed to allow the proxy signer to obtain the same signing capacity as the original signer, the attribute-based fine-grained access control is also present to enable the valid verification of the signature and recovery of data. In addition, the scheme achieves unforgeability of signature and can resist the chosen message attack in Random Oracle Model. The comparisons of performance analysis demonstrates that the scheme is efficient in signing and verification phases. Therefore, it could be well appropriate for telemedicine system.*
Keywords: Attribute-based, Designated verifier, Proxy signature, Message recovery, Telemedicine system

1. **Introduction.** In recent years, the applications of Cloud Medical Treatment (CMT) based on technologies such as Cloud Computing, 5G Communication [1], the Internet of Things (IoT) [2], has become increasingly widespread. But traditional medical diagnostic systems cannot meet patients' needs for safety and efficiency. By using telemedicine technology, patients can diagnose and treat diseases in remote areas [3]. As shown in

Figure 1, In this system, health records collected by the sensors which are attached to the body of patients, are transmitted to a hospital server. Then, the patients are provided for timely feedback, advice and suggestions after statistics and analysis of professionals.

The Telemedicine System can not only set up new contacts between doctors and patients, but also save a lot of time and money costs. However, the privacy of these health records may be maliciously attacked. There are two types of attacks: passive and active. For passive attacks, the adversary can interfere with the transmission of health records on the wireless communication link. For active attacks, the adversary can modify the health records to cause misdiagnosis.

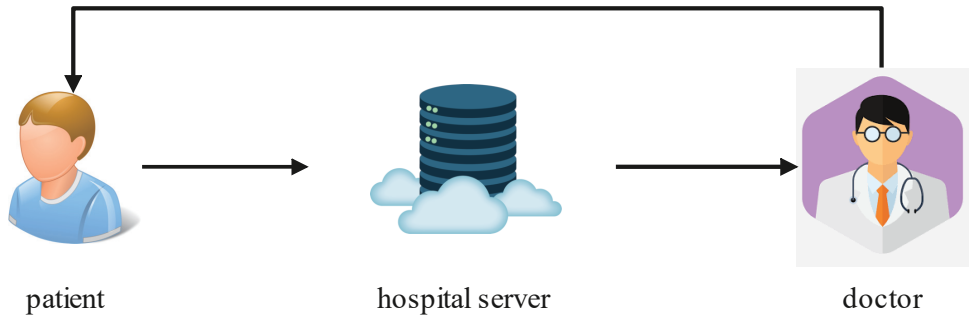

Figure 1: The main entities of telemedicine system

Unfortunately, for some of the existing schemes, there are a few issues need to be solved.

· There is no guarantee that identity information is not attacked actively or passively during the transmission of health records on the wireless communication link [4]. In other words, the identity information is easily leaked [5].

· In the proxy signatures, the original signer gives his secret key to proxy signer, the proxy signer gets the same signing capability as the original signer. For most cases, it is not practical and secure.

· Usually, the existed digital signature schemes [6-7] with message recovery have large messages in the communication process. Consequently, advanced technology for reducing the cost of transmission should be added.

To address the above problems and communicate securely, we propose a feasible scheme as following: The health records need to be signed by the sensors. As shown in Figure 2, the sensors deployed on the patient must be authenticated by the hospital server, and the server which receives medical records must be authenticated by the sensors [8]. In order to realize the trust relationship, it is necessary to adopt the method of designated verifier and proxy delegation [9]. The Deployment Agency (DA), as the original signer, delegates the signature power to the sensor, and designates a professional as the verifier. Due to the limitation of the signature storage space, the message needs to be embedded in the signature, and then when the signature is verified validly, the message is recovered by using an efficient signature scheme.

In comparison to the work, the main contributions of this paper are summarized as follows:

· In proposed schemes [10-17], we uses attribute-based fine-grained access policy for certification Authority. And attribute-based encryption enables the signature verified by the designated verifier [18].

· Besides, the delegation of original signer is designed thoughtfully and composed of a message part, time of validation of proxy signature and public key part.

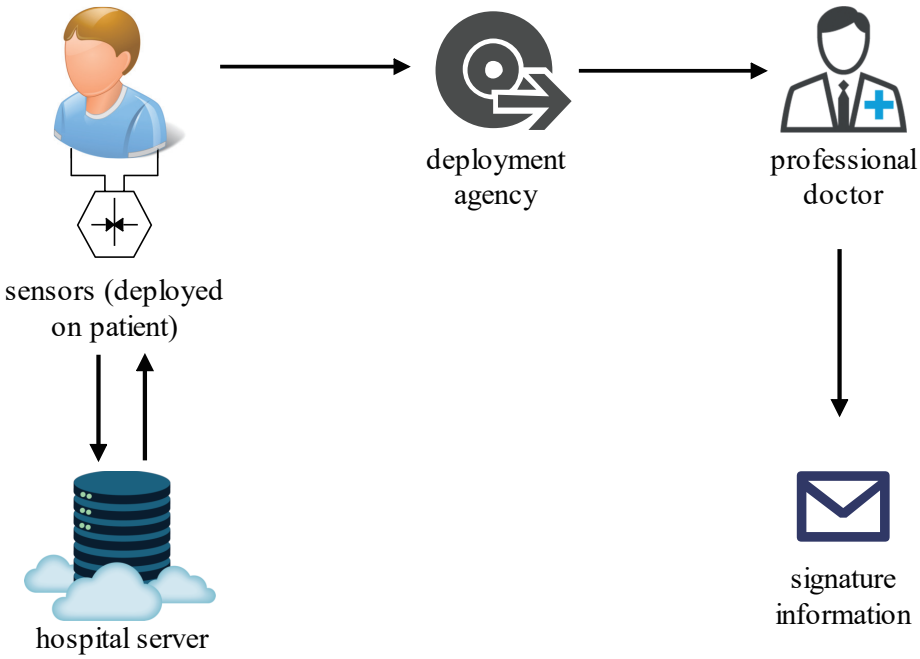

Figure 2: The architecture of telemedicine system

· In message recovery, We also utilize the method of recuing communication cost by dividing into two message blocks. Therefore, each message block contains some redundancy so that the message blocks can be correctly linked together.

· Security and performance analysis compared with others show that the proposed scheme can achieve the anonymity of identity, the unforgeability of signature and less computation and communication cost.

The rest of the paper is organized as follows. In Section 2, we first present the preliminaries related to the proposed scheme. Section 3 presents the system model definitions and syntax of the ABMR-DVPS scheme. In Section 4, we present the ABMR-DVPS scheme in detail. In Section 5, we describe a security analysis of the purposed scheme. Section 6 discusses the performance analysis. Finally, the conclusions and future work of the paper are in Section 7.

1.1. **Related work.** In recent years, many designated verifier proxy signature schemes have been proposed. In this section, we briefly review some works related to our scheme.

Dai et al. [19] proposed the designated verifier proxy signature (DVPS) firstly. In the DVPS, the verifier is specified by the original signer only, so this scheme is hence not sufficiently flexible. Later, a new DVPS scheme was proposed by Wang [20]. In this scheme, the proxy signer can specify a recipient. After that, several schemes have been presented. A pairing-based short and provably secure designated verifier proxy signature in the random oracle model was proposed by Hu et al. [21], an adapted adversary model was regarded. But the length of the signature is much longer compared to the existing scheme. In the Girraj's scheme [22], only the specified verifier can recover the information from the signature.

2. **Preliminaries.** In this section, we will review some mathematical theories and respective hard problems.

2.1. **Bilinear Pairing.** $(\mathbb{G}_1,+)$ and $(\mathbb{G}_2,\cdot)$ are cyclic groups with the same prime order p. $\mathbb{G}_1$ has the generator g. Bilinear map e: $\mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_2$. $\mathbb{G}_2$ has the three characteristics:

·Bilinearity: $e(P^a, Q^b) = e(P, Q)^{ab}$, where $P, Q \in G_1$ and $a, b \in \mathbb{Z}_p$.

·Non-degeneracy: There exists $g \in \mathbb{G}_1$ such that $e(g, g) \neq 1_{\mathbb{G}_2}$, where the $1_{\mathbb{G}_2}$ is the identity of element of the group $\mathbb{G}_2$.

·Computablility: There is an effective algorithm for computing $e(u, v)$ where $u, v \in \mathbb{G}_1$.

2.2. **Computational Diffie-Hellman (CDH) problem.** Given (g, g^a, g^b) with $a, b \in \mathbb{Z}_p^*$, it is hard to compute the g^{ab}.

2.3. **Attribute Predicate.** In this paper, we construct our scheme, which supports all predicates Υ involving threshold values k. Specially, if $\Upsilon_{k,\omega^*}(\cdot) \to 1/0$ for ω^* with k is given, then we have:

$$\Upsilon_{k,\omega^*}(\omega) = \begin{cases} 1, & |\omega \cap \omega^* \geq k \\ 0, & otherwise \end{cases}$$

2.4. **Lagrange Interpolation.** Given d points $(x_1, y_1), \ldots, (x_d, y_d)$ on a polynomial q of degree not greater than $(d-1)$, we can compute $q(i)$ for any $i \in \mathbb{Z}_p$:

$$q(i) = \sum_{j=0}^{d} q(j)\Delta_{j,S}(i)$$

Let S be a $d-element$ set, Lagrange coefficient $\Delta_{j,S}(i)$ of $q(j)$ in the computation of $q(i)$ can be defined as:

$$\Delta_{j,S}(i) = \prod_{\eta \in S, \eta \neq j} \frac{i-\eta}{j-\eta}$$

3. System Model.

3.1. **Definitions.** The system model of attribute-based message recovery designated verifier proxy signature scheme (ABMR-DVPS) is illustrated in Figure 3. In our proposed scheme, we mainly consider six entities: Attribute Authority (AA), Private Key Generator (PKG), Deploying Authority (DA), Sensor, Medical Server (MS) and Practitioner. The function descriptions of each entity are as follows:

· AA is responsible for authenticating users' attributes from their private information and distributing attributes to users.

· PKG is responsible for generating key pair and attribute private key according to the user's attributes.

· DA is a network developer, though, in certain special cases hospital, admin acts as the role of DA. It develops telemedicine Wireless Sensor Network (WSN) and has responsibility for all associated matters within WSN.

· Sensor is deployed on the patient's body to track the relevant information and send it to healthcare server via the wireless bridge. Sensor is storage and energy-limited, which sends short messages.

· MS is the mainframe with a large storage and computational power. It collects information from all connected wireless gateway. In the following analysis, the data is sent to the relevant practitioner.

· Practitioner is a trained professional who receives the analyzed data and offers more advanced treatment.

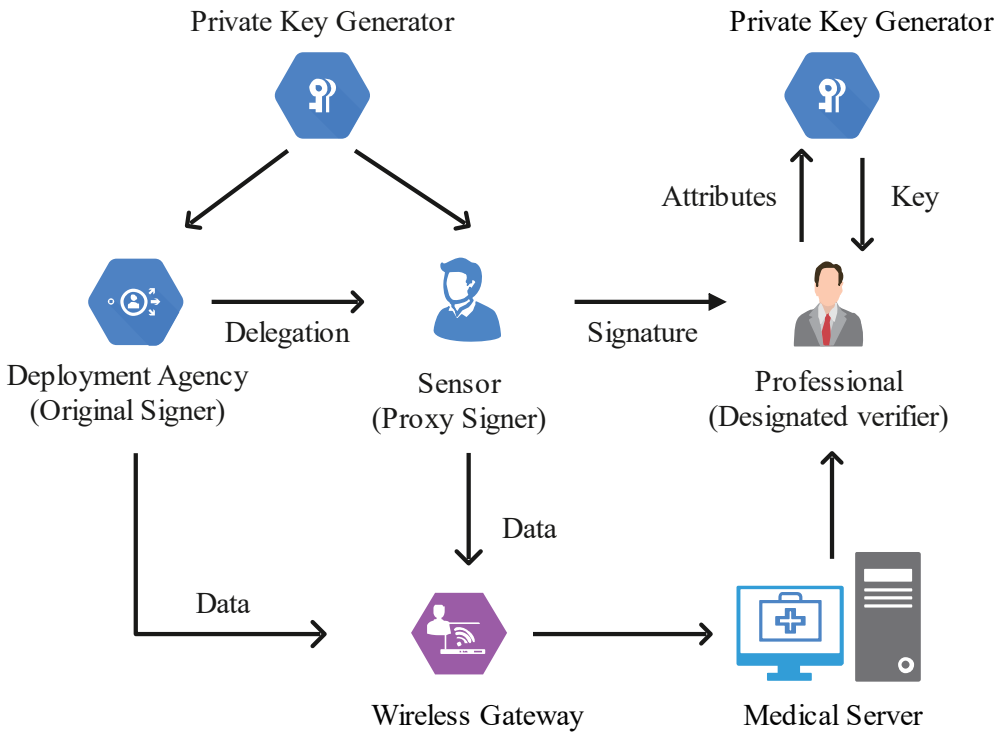

Figure 3: The system model of ABMR-DVPS

3.2. **A Syntax for ABMR-DVPS.** The scheme consists of eight algorithms, which are defined as follows:

Setup$(1^\lambda) \rightarrow (mk,params)$: The algorithm inputs 1^λ as the security parameter, it outputs the makter key mk of PKG and system public parameter $params$.

KeyGen$(params) \rightarrow (pk_i,sk_i), i \in \{a,b\}$: The algorithm inputs the system public parameters params and outputs original signer's key pair (pk_a, sk_a), proxy signer's key pair (pk_b, sk_b).

AttrKeyGen$(\omega, mk, params) \rightarrow pk_{c_i}$: The algorithm inputs the designated verifier attribute set $\omega \in \mathbb{A}$, where $\mathbb{A}$ is the universal set of possible attributes, and then outputs attribute public key $pk_{c_i} = (pk_{i_0}, pki_1)$.

DeleGen$(sk_a, \omega) \rightarrow \delta$: The algorithm inputs the original private key sk_a, a warrant ω specified by the original signer, and then algorithm outputs delegation δ.

DVProxySign$(sk_b, \delta, pk_{c_i}, m) \rightarrow \sigma_p$: The proxy signing algorithm. The algorithm inputs the proxy signer's private key sk_b, a delegation δ, the designated verifier attribute public key pk_{c_i}, and the message m, and then outputs the proxy signature σ_p.

DVProxyVerify$(sk_{c_i}, \delta, \sigma_p, \Upsilon, pk_a, pk_b) \rightarrow 1/0$: The algorithm inputs the private key sk_{c_i} of designated verifier, a delegation δ, the proxy signature σ_p, a predicate Υ, the public key pk_a of original signer, the public key pk_a of original signer, the public key pk_b of proxy signer. σ_p can be verified if $\Upsilon = 1$, and then algorithm recovers the original message m.

3.3. **Adversary Model.** In our adversary model, we assume that AA and PKG cannot be compromised, and the private information stored in AA cannot be leaked. Besides, PKG distributes the user's secret key via secure channels. The DA and MS are honest but curious, which means that they exactly perform the presented algorithms and protocols, however, they try to infer both user's private information from the data what they have known.

4. **ABMR-DVPS Scheme.**

Setup: First, we define a universal set of possible attributes $\mathbb{A}$ with attribute sets in $\mathbb{Z}_p^*$. A dumb attribute set from $\mathbb{Z}_p^*$, which does not intersect with the universal set $\mathbb{A}$, is given as $\Omega = \{\Omega_1, \Omega_2, \ldots, \Omega_{d-1}\}$, an n-element attribute set $\omega^* \in \mathbb{A}$. We set a generator randomly $g \in \mathbb{G}_1$, a random element $\alpha \in \mathbb{Z}_p^*$ and compute $g_1 = g^\alpha$. The algorithm selects a random element $g_2 \in \mathbb{G}_1$ and set $g_3 = g_2^\alpha$, computes $E = e(g_1, g_2)$. The collision resistant hash functions are constructed such that $H_1 : \{0,1\}^* \to \mathbb{G}_1, H_2 : \{0,1\}^* \to \mathbb{Z}_p^*, F_1 : \{0,1\}^{l_2} \to \{0,1\}^{l_1}, F_2 : \{0,1\}^{l_1} \to \{0,1\}^{l_2}$ where l_1, l_2 are positive integers such that $l_1 + l_2 = p$ where p is prime.The system $params = (g, g_1, g_2, g_3, d, E, H_1, H_2, F_1, F_2)$. The master key $mk = \alpha$.

KeyGen: The user selects a random element $x_a, x_b \in \mathbb{Z}_p^*$ and generates the original signer's key pair $(sk_a, pk_a) = (x_a, g^{x_a})$, proxy signer's key pair $(sk_b, pk_b) = (x_b, g^{x_b})$.

AttrKeyGen: In order to generate the designated verifier's attribute public key pk_{c_i} for the attribute set ω, the public key is built according to the steps following:

·Chooses a random polynomial q of degree $(d-1)$ with $q(0) = \alpha$

·Generates a new set of attributes $\hat{\omega}$, where $\hat{\omega} = \omega \cup \Omega$. For each attribute $attr_i \in \hat{\omega}$, the algorithm selects $r_i \in \mathbb{Z}_p$ randomly as the private key and computes $pk_{i_0} = g_2^{q(i)} \cdot H_1(attr_i)^{r_i}, pk_{i_1} = g^{r_i}$

·Finally, it outputs $pk_{c_i} = (pk_{i_0}, pk_{i_1})$ as the attribute public key for $i \in \hat{\omega}$

DeleGen: To delegate the ability original signatory to the proxy signatory, the original signatory first generates a warrant w for the proxy signer. The original signer's delegation [8] is generated as:

$$\delta = H_1(w)^{x_a}$$

and then the original signer sends the delegation (w, δ) to the proxy signer.

DVProxySign: Given the delegation δ, designated verifier's attribute public key pk_{c_i}, proxy signer's private key sk_b. In order to sign a message m of length k_2, the proxy signature is constructed as:

To demonstrate possessing at least k attributes among the n-element attribute set ω^*, the algorithm selects a k-element subset $\omega' \subseteq \omega \cap \omega^*$

·Set a dumb attribute set Ω' as the subset of Ω where $|\Omega'| = d - k$, selects $n + d - k$ elements $r_i' \in \mathbb{Z}_p$ randomly, where $i \in \omega^* \cup \Omega'$

·Computes $f = F_1(m)||(F_2(F_1(m)) \oplus m)$

·Computes $M = H_2(E) + f$

The proxy signature is constructed as:

$$\sigma_p = (M, \sigma_1, \sigma_2)$$

we have:

$$\sigma_1 = \prod_{i \in \omega' \cup \Omega'} pk_{i_0}^{\Delta_{i,s}(0)} \cdot \prod_{i \in \omega^* \cup \Omega'} H_1(attr_i)^{r_i'} \cdot \delta \cdot H_1(M)^{sk_b}$$

$$\sigma_i = \begin{cases} pk_{i_1}^{\Delta_{i,s}(0)} \cdot g^{r_i'}, & i \in \omega' \cup \Omega' \\ g^{r_i'}, & i \in \omega^* / \omega' \end{cases}, \sigma_2 = \sigma_{i i \in \omega * \cup \Omega'}$$

DVProxyVerify: Given the proxy signature σ_p, a delegation δ, designated verifier's attribute private key and predicate $\Upsilon_{k,\omega^*}(\omega)$. We set $\epsilon = \sum_{i \in \hat{\omega}} sk_{c_i}$, a designated-verifier

accepts σ_p is valid if $\Upsilon_{k,\omega^*}(\omega) = 1$ and the following equation holds:

$$E^{\epsilon} = e(g_1, g_2)^{\epsilon} = \frac{e(g, \sigma_1) \cdot e(g^{\epsilon-1}, g_2^{\alpha})}{\prod\limits_{i \in \omega^* \cup \Omega'} e(H_1(attr_i), \sigma_2) \cdot e(pk_a, H_1(w)) \cdot e(pk_b, H_1(M))}$$

$$M - H_2(E) = f$$

and then the message m will be recovered [9] from f:

$$\begin{aligned} F_2(|f|^{l_1}) \oplus |f|_{l_2} &= F_2(|F_1(m)||F_2(F_1(m)) \oplus m|)^{l_1} \oplus (F_2(F_1(m)) \oplus m)_{l_2} \\ &= F_2(F_1(m)) \oplus m \oplus F_2(F_1(m)) \\ &= m. \end{aligned}$$

The accuracy of this scheme may be substantiated as follows:

$$\begin{aligned} &\frac{e(g, \sigma_1) \cdot e(g^{\epsilon-1}, g_2^{\alpha})}{\prod\limits_{i \in \omega^* \cup \Omega'} e(H_1(attr_i), \sigma_2) \cdot e(pk_a, H_1(w)) \cdot e(pk_b, H_1(M))} \\ &= \frac{e(g, \prod\limits_{i \in \omega' \cup \Omega'} pk_{i_0}^{\Delta_{i,s}(0)} \cdot H_1(attr_i)^{r'_i} \cdot \delta \cdot H_1(M)^{sk_b}) \cdot e(g^{\epsilon-1}, g_2^{\alpha})}{\prod\limits_{i \in \omega^* \cup \Omega'} e(H_1(attr_i), \sigma_2) \cdot e(pk_a, H_1(w)) \cdot e(pk_b, H_1(M))} \\ &= \frac{e(g, \prod\limits_{i \in \omega' \cup \Omega'} pk_{i_0}^{\Delta_{i,s}(0)} \cdot H_1(attr_i)^{r'_i} \cdot H_1(w)^{x_a} \cdot H_1(M)^{sk_b}) \cdot e(g^{\epsilon-1}, g_2^{\alpha})}{\prod\limits_{i \in \omega^* \cup \Omega'} e(H_1(attr_i), \sigma_i) \cdot e(g^{x_a}, H_1(w)) \cdot e(g^{x_b}, H_1(M))} \\ &= \frac{e(g, \prod\limits_{i \in \omega' \cup \Omega'} pk_{i_0}^{\Delta_{i,s}(0)} \cdot \prod\limits_{i \in \omega^* \cup \Omega'} H_1(attr_i)^{r'_i} \cdot e(g^{\epsilon-1}, g_2^{\alpha})}{\prod\limits_{i \in \omega^* \cup \Omega'} e(H_1(attr_i), \sigma_i)} \\ &= \frac{e(g, \prod\limits_{i \in \omega' \cup \Omega'} pk_{i_0}^{\Delta_{i,s}(0)} \cdot \prod\limits_{i \in \omega^* \cup \Omega'} H_1(attr_i)^{r'_i} \cdot e(g^{\epsilon-1}, g_2^{\alpha})}{\prod\limits_{i \in \omega^* \cup \Omega'} e(H_1(attr_i), pk_{i_1}^{\Delta_{i,s}(0)} \cdot g^{r'_i}) \cdot \prod\limits_{i \in \omega^* / \omega'} e(H_1(attr_i), g^{r'_i})} \\ &= \frac{e(g, \prod\limits_{i \in \omega' \cup \Omega'} g_2^{q(i) \cdot \Delta_{i,s}(0)} \cdot \prod\limits_{i \in \omega^* \cup \Omega'} H_1(attr_i)^{r_i \cdot \Delta_{i,s}(0) + r'_i} \cdot e(g, \prod\limits_{i \in \omega^* / \omega'} H_1(attr_i)) \cdot e(g^{\epsilon-1}, g_2^{\alpha})}{\prod\limits_{i \in \omega^* \cup \Omega'} e(H_1(attr_i), g^{r_i \cdot \Delta_{i,s}(0) + r'_i} \cdot g^{r'_i}) \cdot \prod\limits_{i \in \omega^* / \omega'} e(H_1(attr_i), g^{r'_i})} \\ &= e(g, \prod_{i \in \omega' \cup \Omega'} g_2^{q(i) \cdot \Delta_{i,s}(0)} \cdot e(g^{\epsilon-1}, g_2^{\alpha}) \\ &= e(g, g_2^{q(0)}) \cdot e(g^{\epsilon-1}, g_2^{\alpha}) \\ &= e(g, g_2^{\alpha}) \cdot e(g^{\epsilon-1}, g_2^{\alpha}) \\ &= e(g_{\alpha}, g_2^{\epsilon}) \\ &= e(g_1, g_2^{\epsilon}) \\ &= E^{\epsilon} \end{aligned}$$

5. **Security Analysis.**

According the above ABMR-DVPS scheme, there are three kinds of adversaries are considered:

Type 1($\mathcal{A}_1$): This adversary only has the original signer's public key pk_a, the proxy signer's public key pk_b, the designated verifier's attribute public key pk_{c_i}, and attempts to get a forgery of proxy signature σ_p.

Type 2($\mathcal{A}_2$): This adversary has the proxy signer's private key sk_a, and attempts to get a forgery of proxy signature σ_p.

Type 3($\mathcal{A}_3$): This adversary has the original signer's private key sk_b, and attempts to get a forgery of proxy signature σ_p.

It is obvious that if the ABMR-DVPS scheme can against $\mathcal{A}_2$ or $\mathcal{A}_3$, it also against $\mathcal{A}_1$. In the following, we will only focus on $\mathcal{A}_2$ and $\mathcal{A}_3$ types of adversaries. Before presenting each adversary model in detail, we first list five kinds of oracle queries with the adversary $\mathcal{A}$ and challenger $\mathcal{C}$:

·Attribute Oracle: For the attribute query about attribute $attr_i \subseteq \omega$, $\mathcal{C}$ returns a hash value $H_1(attr_i) \in \mathbb{G}_1$ to $\mathcal{A}$.

·Delegation Oracle: For the warrant query about a warrant $w \in \{0,1\}^*$, $\mathcal{C}$ returns a hash value $H_1(w) \in \mathbb{G}_1$ to $\mathcal{A}$.

·Message Oracle: For the message query about a message $M \in \{0,1\}^*$, $\mathcal{C}$ returns a hash value $H_1(M) \in \mathbb{G}_1$ to $\mathcal{A}$.

·Extract Oracle: For extract oracle about an attribute set ω of designated verifier, $\mathcal{C}$ returns designated verifier's attribute public key $pk_{c_i} = (pk_{i_0}, pk_{i_1})$ to $\mathcal{A}$ where each $i \in \omega$.

·Proxy Signing Oracle: For the proxy signing oracle on designated verifier's attribute set ω where $\omega \subseteq \mathbb{A}$ and message $M \in \{0,1\}^*$, the Challenger $\mathcal{C}$ returns a valid proxy signature σ_p to the adversary $\mathcal{A}$.

Theorem 5.1. *The ABMR-DVPS scheme is existential unforgeable under selected messaging attacks in the random oracle model, in other words, there is no such probability polynomial time adversary $\mathcal{A}_2$ who can forge a valid proxy signature.*

Proof: Since adversary $\mathcal{A}_2$ has the public key $\{pk_a, pk_b, pk_{c_i}\}$ of both the signers and verifier. Also, it has the original signer private key sk_a. So, $\mathcal{A}_2$ cannot obtain proxy signature. the game between the challenger $\mathcal{C}$ and adversary $\mathcal{A}_2$ as follows:

Setup: Given $\Omega = \{\Omega_1, \Omega_2, \cdots, \Omega_{d-1}\}$ as the dumb attribute set. $\mathcal{C}$ selects $g_1 = g^\alpha$, $g_2 = g^\beta$, computes $E = e(g_1, g_2)$ and sends public parameters $params = (g, g_1, g_2, d, E, H_1, H_2, F_1, F_2)$ to $\mathcal{A}_2$.

KeyGen: $\mathcal{C}$ chooses random elements $x_a \in \mathbb{Z}_p^*$ and sets the key pair $(sk_a, pk_a) = (x_a, g^{x_a})$ of proxy signer.

Hash Queries: $\mathcal{C}$ keeps hash tables L_1, L_2 and L_3 for the attribute queries, delegation queries and message queries, respectively. The hash queries are as follows:

Attribute Query: Assume $\mathcal{A}_2$ make q_a times attribute queries, where each query on attribute $attr_i$, the simulations of $\mathcal{C}$ are as following:

Upon receiving the attribute query with respect to an attribute $attr_i$, if the $attr_i$ is already in the table L_1, $\mathcal{C}$ returns $H_1(attr_i)$ to $\mathcal{A}_2$, otherwise:

·if the $attr_i$ is not included in the L_1 and $attr_i \in \omega^* \cup \Omega'$, $\mathcal{C}$ selects $a_i \in \mathbb{Z}_p^*$ randomly and returns $H_1(attr_i) = g^{a_i}$ to $\mathcal{A}_2$. $\mathcal{C}$ records $(attr_i, g^{a_i})$ in the table L_1.

·if the $attr_i$ is not included in the L_1 and $attr_i \notin \omega^* \cup \Omega'$, $\mathcal{C}$ selects a_i, $b_i \in \mathbb{Z}_p^*$ randomly and returns $H_1(attr_i) = g^{-a_i} g^{b_i}$ to $\mathcal{A}_2$. $\mathcal{C}$ records $(attr_i, g^{-a_i} g^{b_i})$ in the table L_1.

Delegation Query: Assume $\mathcal{A}_2$ makes q_d delegation queries, $\mathcal{C}$ selects $\mu \in (0, q_d)$ randomly, for each query on warrant w_i, the simulations of $\mathcal{C}$ are as following:

Upon receiving the delegation query with respect to a warrant w_i, if the w_i is already in the table L_2, $\mathcal{C}$ returns $H_1(w_i)$ to $\mathcal{A}_2$, otherwise:

·if $i = \mu$, $\mathcal{C}$ selects $a_i^{'} \in \mathbb{Z}_p^*$ randomly and returns $H_1(w_i) = g^{a_i^{'}}$ to $\mathcal{A}_2$. $\mathcal{C}$ records $(w_i, g^{b_i^{'}})$ in the table L_2.

·if $i \neq \mu$, $\mathcal{C}$ selects $a_i^{'}, b_i^{'} \in \mathbb{Z}_p^*$ randomly and returns $H_1(w_i) = g_1^{b_i^{'}} g^{a_i^{'}}$ to $\mathcal{A}_2$. $\mathcal{C}$ records $(w_i, g_1^{b_i^{'}} g^{a_i^{'}})$ in the table L_2.

Message Query: Assume $\mathcal{A}_2$ makes q_m message queries, for each query on message M_i, the simulations of $\mathcal{C}$ are as following:

·if M_i is already in the table L_3, $\mathcal{C}$ returns the corresponding $H_1(M_i)$ in the L_3 to $\mathcal{A}_2$.

·otherwise, $\mathcal{C}$ selcets $r_i \in \mathbb{Z}_p^*$ randomly and returns $H_1(M_i) = g^{r_i}$ to $\mathcal{A}_2$. $\mathcal{C}$ records (M_i, g^{r_i}) in the L_3.

Extract Query: Assume $\mathcal{A}_2$ issues an attribute key extraction query on attribute set ω such that $|\omega^* \cap \omega| < k$. We define three sets Γ, $\Gamma^{'}$, S satisfy: $\Gamma = (\omega \cup \omega^*) \cap \Omega^{'}$ and $\Gamma \subseteq \Gamma^{'} \subseteq S$ with $|\Gamma^{'}| = d-1, S = \Gamma^{'} \cap \{0\}$. $\mathcal{C}$ generates the attribute key pk_{c_i} as follows:

·for $i \in \Gamma^{'}$, $\mathcal{C}$ selects two elements $\tau_i, r_i \in \mathbb{Z}_p^*$ randomly. In this case, $\mathcal{C}$ selects $(d-1)$ degree polynomial $q(i) = \tau_i$. $\mathcal{C}$ can compute pk_{c_i} for $i \in \Gamma^{'}$ as follows: $pk_{c_i} = (g_2^{q(i)} \cdot H_1(attr_i)^{r_i}, g^{r_i}) = (g_2^{\tau_i} \cdot H_1(attr_i)^{r_i}, g^{r_i})$.

·for $i \notin \Gamma^{'}$, $\mathcal{C}$ looks up the table L_1 to find the record about attribute $attr_i$ and get the corresponding a_i. $\mathcal{C}$ selects an element $r_i^{'} \in \mathbb{Z}_p^*$ randomly, and let $r_i = \frac{\Delta_{0,S}(i)q(j)}{a_i}\beta + r_i^{'}$. $\mathcal{C}$ can compute the value $q(i)$ corresponding to $i \notin \Gamma^{'}$ of the $(d-1)$ degree polynomial $q(i)$ by using Lagrange interpolation as

$$q(i) = \sum_{j \in \Gamma'} \Delta_{j,S}(i) \cdot q(j) + \Delta_{0,S}(i) \cdot q(0)$$

$\mathcal{C}$ can computes pk_{c_i} for $i \notin \Gamma^{'}$ as follows

$$pk_{(i_0)} = g_2^{q(i)} \cdot H_1(attr_i)^{r_i} = g_2^{\frac{\Delta_{0,S^{(i)}b_i}}{a_i} + \sum_{j \in \Gamma'} \Delta_{j,S}(i) \cdot q(j)}$$

$$pk_{(i_1)} = g_2^{\frac{\Delta_{0,S^{(i)}}}{a_i}}$$

$\mathcal{C}$ returns $pk_{c_i} = (pk_{i_0}, pk_{i_1})$ for each $i \in (\omega \cap \Omega)$ as the public key of ω.

Proxy Signing Queries: In this phrase, we will show how $\mathcal{C}$ simulate the proxy signature. Assume $\mathcal{A}_2$ makes q_{ps} proxy signing queries, for each query on message M_i, C simulates as follows:

·computes $E = e(g_1, g_2)$.

·computes $f_i = F_1(m_i)||(F_2(F_1(m_i)) \oplus m_i)$.

·computes $M_i = H_2(E) + f_i$.

·computes $\sigma_1^* = g_2^{\alpha} \prod_{i \in \omega^* \cap \Omega'} H_1(attr_i)^{r_i} H_1(w_i)^{sk_a} H_1(M_i)^{sk_b}$, $\sigma_i^* = g^{r_i}$, for $i \in \omega^* \cap \Omega^{'}$.

·outputs the proxy signature $\sigma_p = M_i, \sigma_1^*, \sigma_i^*$.

Thus, $\mathcal{C}$ can compute

$$g^{\alpha\beta} = \frac{\sigma_1^*}{\prod_{i \in \omega^* \cap \Omega'} (\sigma_i^*)^{a_i} \cdot pk_a^{a_i^{'}} \cdot pk_b^{r_i}}$$

where $H_1(attr_i) = g^{a_i}$, $H_1(w_i) = g^{a_i^{'}}$.

If there is not a time polynomial adversary capable of forging a valid proxy signature, we say that the ABMR-DVPS scheme can against $\mathcal{A}_2$ existential forgery under selected message attacks.

Theorem 5.2. *The ABMR-DVPS scheme is existential unforgeable under selected message attacks in the random oracle model, in other words, there is no such probability polynomial time adversary $\mathcal{A}_3$ who can forge a valid proxy signature.*

Proof: Since adversary $\mathcal{A}_3$ has the public key $\{pk_a, pk_b, pk_{c_i}\}$ of both signers and verifiers. Also, it has the private key sk_b of the proxy signer. Therefore, $\mathcal{A}_3$ can get proxy signature. The following is a game between the challenger $\mathcal{C}$ and adversary $\mathbb{A}_3$.

Setup: $\mathcal{C}$ selects a generator $g \in \mathbb{G}_1$ randomly and choosed a $(d-1)$ degree polynomial q with $q(0) = x$. $\mathcal{C}$ sets $sk_b = \alpha, pk_b = g_1 = g^\alpha, g_2 = g^\beta$, computes $E = e(g_1, g_2)$ and sends public parameters $params = (g, g_1, g_2, d, E, H_1, H_2, F_1, F_2)$ to $\mathcal{A}_3$.

KeyGen: $\mathcal{C}$ chooses random elements $x_a \in \mathbb{Z}_p^*$ and sets the key pair $(sk_a, pk_a) = (x_a, g^{x_a})$.

Hash Queries: Assume $\mathcal{C}$ keeps hash lists L_1, L_2 and L_3 for the attribute, delegation, message queries. The hash queries for the attribute and delegation are similarly in Theorem 2. Assume $\mathcal{A}_\ni$ makes q_m message queries. $\mathcal{C}$ simulates as follows:

·If $M_i \neq M_v$, $\mathcal{C}$ returns $H_1(M_i) = g^{r_i}$ and records $(M_i, H_1(M_i))$ in the table L_3.

·Otherwise, $\mathcal{C}$ selects $r_v \in \mathbb{Z}_p^*$ randomly and returns $H_1(M_v) = (g^\beta)^{r_v}$ to A_3. $\mathcal{C}$ records $(M_v, (g^\beta)^{r_v})$ in the table L_3.

Proxy Signing Queries: Assume that the adversary $\mathcal{A}_3$ makes a proxy signature query on message $M \in \{0,1\}^*$. The Challenger $\mathcal{C}$ first generates the attribute public key pk_{c_i} using the same extration query as in Theorem 2. After, the Challenger $\mathcal{C}$ generates the delegation $\delta = H_1(w)^{r_a^*}$ using the same delagation query as in Theorem 2. Finally, the Challenger $\mathcal{C}$ makes the simulation of the proxy signature query:

If M is already in the L_3, assume $H_1(M) = g^{r_M}$, $\mathcal{C}$ simulates the proxy signature $\sigma_p = (M, \sigma_1, \sigma_2)$.

where

$$M = H_2(E) + f$$

$$\sigma_1 = g_2^\alpha \prod_{i \in \omega^* \cap \Omega'} H_1(attr_i)^{r_i} H_1(w)^{r_a^*} pk_b^{r_M}$$

$$\sigma_2 = \{\sigma_i^*\}_{i \in \omega^* \cap \Omega'} = \{g^{r_i}\}_{i \in \omega^* \cap \Omega'}$$

Otherwise, $\mathcal{C}$ chooses $r^* \in \mathcal{Z}_p^*$ and simulates the proxy signature $\sigma_p^* = (M, \sigma_1^*, \sigma_2^*)$

$$\sigma_1^* = g_2^\alpha \prod_{i \in \omega^* \cap \Omega'} H_1(attr_i)^{r_i} H_1(w)^{r_a^*} \cdot pk_b^{r^*}$$

$$\sigma_2^* = \{\sigma_i^*\}_{i \in \omega^* \cap \Omega'} = \{g^{r_i}\}_{i \in \omega^* \cap \Omega'}$$

and records $(M, H_1(M))$ in table L_3.

$\mathcal{C}$ can compute

$$g^{\alpha\beta} = \left(\frac{\sigma_1^*}{g_2^\alpha \prod_{i \in \omega \cap \Omega'} (\sigma_2^*)^{a_i} \cdot pk_a^{a_i'} \cdot pk_b^{r^*}}\right)^{\frac{1}{r_v}}$$

If there is not a time polynomial adversary capable of forging a valid existential forgery proxy signature under the selected message attacks, it turns out that the ABMR-DVPS scheme can against $\mathcal{A}_3$.

6. **Performance Analysis.**

In this section, we compare the ABMR-DVPS scheme with previous schemes to show our scheme is better suited to the telemedicine system. A certificate-based proxy signature scheme was proposed by Mahmoodi et al. [23], which has the ownership of the delegation, but this system cannot achieve fine grain access control and allow for flexible privacy control. A stronger concept of proxy signature security by allowing opponents to behave more adaptively in oracle access. was proposed by Singh et al. [24]. An attribute-based signature scheme, the scheme can achieve the anonymity of signer and provide precise access control was proposed by Wang et al. [25]. But this scheme does not have the

delegation property which is not adequate to preserve the integrity of data. Our scheme can achieve anonymity for the user to control confidentiality in a flexible way. The signing ability also can be delegated to proxy signer. The ABMR-DVPS scheme turns out to be existential unforgeability in the random oracle model.

Table 1: The comparison between our scheme and the previous schemes

Scheme	Mahmoodi [23]	Singh [24]	Wang [25]	Ours
User's anonymity	No	No	Yes	Yes
Fine-grained access	No	No	Yes	Yes
Delegation property	Yes	Yes	No	Yes
Provable secure	Yes	Yes	Yes	Yes
Data integrity	Yes	Yes	Yes	Yes
Pairing based	No	Yes	Yes	Yes
Existential unforgeability	Yes	Yes	Yes	Yes

In telemedicine system, the medical data are collected by the sensors deployed in the body of patients. Then, the sensor communicates the data to medical server. Thus, the performance analysis should be conducted based on the length of signature and computation overhead on the sensors. In ABMR-DVPS scheme, different phases are done by different entities. some phases are done by sensors (such as DeleVerify and DVProxySign) and some by deploying authority or by medical server and therefore, we consider the length of communicated signature (in bits) and total consumes in different phases. The notations used in the proposed scheme: S_m denotes a scalar multiplication (0.39ms), e_t denotes a pairing computation(3.21ms), H denotes map to point hashing (0.09ms). We do not consider the operations such as elliptic point addition, X-OR addition $\oplus$, hashes H_1, H_2 and modular addition. To achieve 3072 bits RSA level, length of the elements from $\mathbb{G}$, $\mathbb{G}_T$ and $\mathbb{Z}_q$ are 256 ($|\mathbb{G}|$), 3072($|\mathbb{G}_T|$), 256($|\mathbb{Z}_q|$) bits respectively. The warrant length and message length are denoted by $|w|$ and $|\mathbb{G}|$ respectively. Due to message recovery feature, the length of the scheme is $|w| + 512$ bits.

The computing costs of our scheme is smaller than scheme [24], equal to scheme [23] and is 0.3ms more than our scheme [25], but the signature lengths among are bigger than our scheme (differences are $|m| + 256$, $|m| + 2560$ and $|m|$ bits respectively). Thus, the performance of our ADMR-DVPS scheme is better with respect to consumes and bandwidth. DeleGen and DVProxySign phases are executed by the sensors. However, DVProxySign is not executed in every cycle of signing. Compared with DVProxySign, executed more frequently, and consuming $S_m + 2e_t$ (6.81ms). This cost is bearable to a sensor.

Summarily, our scheme consumes 17.97ms overall which has high efficiency and due to designed receiver and message recovery attributes, it also satisfies all four security requirements along with shortest bandwidth. While, other schemes provide an inefficient bandwidth or satisfy part of the security requirements only. Therefore, our ADMR-DVPS scheme is suitable for telemedicine system.

7. **Conclusions.**

In this paper, we propose the ABMR-DVPS scheme in the telemedicine system. The scheme can let a proxy signer to sign the message on behalf of an original owner and a designated verifier to verify the proxy signature. We prove the ABMR-DVPS scheme is existential unforgeable against $\mathcal{A}_2$ and $\mathcal{A}_3$ adversary. Comparison analysis demonstrates

Table 2: Computations cost comparison

Scheme	Computing costs	Signature lengths
Mahmoodi [23]	$4H + 4S_m + 5e_t$ (17.97ms)	$\|w\| + \|m\| + 768$ (bits)
Singh [24]	$4H + 4S_m + 5e_t$ (18.63ms)	$\|w\| + \|m\| + 3072$ (bits)
Wang [25]	$5H + 3S_m + 5e_t$ (17.67ms)	$\|w\| + \|m\| + 512$ (bits)
ADMR-DVPS	$4H + 4S_m + 5e_t$ (17.97ms)	$\|w\| + 512$ (bits)

our scheme is suitable for the telemedicine system. Future work will focus on the deployment of the scheme on Blockchain.

Acknowledgment. This work was supported by the National Social Science Fund of China (No.21XTQ015), the Natural Science Foundation of Fujian Province of China (No.2020J01814) and the Natural Science Foundation of Fujian Province of China under Grant (No.2019J01752). The authors also gratefully acknowledge the helpful comments and suggestions of the reviewers, which have improved the presentation.

REFERENCES

[1] Y. Lei, Y.C. Chen, T.Y. Wu, Provably secure client-server key management scheme in 5G networks, *Wireless Communications and Mobile Computing*, vol. 2021, 4083199, 2021.

[2] S. Hussain, I. Ullah, H. Khattak, M.A. Khan, C.M. Chen, S.Kumari, A lightweight and provable secure identity-based generalized proxy signcryption (IBGPS) scheme for Industrial Internet of Things (IIoT), *Journal of Information Security and Applications*, vol. 58, 102625, 2021.

[3] T.Y. Wu, Y. Lei, J.N. Luo, J. Ming-Tai Wu, A provably secure authentication and key agreement protocol in cloud-based smart healthcare environments, *Security and Communication Networks*, vol. 2021, 2299632, 2021.

[4] H. Xiong, Y.Z. Hou, X. Huang, Y.N. Zhao, C.M. Chen, Heterogeneous Signcryption Scheme From IBC to PKI With Equality Test for WBANs, *IEEE Systems Journal*, pp. 1-10, 2021.

[5] A. Shamir, Identity-based cryptosystems and signature schemes, *Workshop on the theory and application of cryptographic techniques*, Springer, Berlin, Heidelberg, pp. 47-53, 1984.

[6] N. Kaisa, Rueppel. RA, A new signature scheme based on the DSA giving message recovery, *Proceedings of the 1st ACM Conference on Computer and Communications Security*, pp. 58-61, 1993.

[7] F.G. Zhang, S. Willy, Y. Mu, Identity-based partial message recovery signatures (or how to shorten ID-based signatures), *International Conference on Financial Cryptography and Data Security*, Springer, Berlin, Heidelberg, pp. 45-56, 2005.

[8] K. Dalia, Authenticating with Attributes, *IACR Cryptol. ePrint Arch*, vol. 2008, 31, 2008.

[9] W.W. Liu, Y. Mu, M.Y. Guo, Attribute-based signing right delegation, *International Conference on Network and System Security*, Springer, Cham, pp. 323-334, 2015.

[10] K. Dalia, Attribute Based Group Signatures, *IACR Cryptol. ePrint Arch*, vol. 2007, 159, 2007.

[11] K. Dalia, Attribute Based Group Signature with Revocation, *IACR Cryptol. ePrint Arch*, vol. 2007, 241, 2007.

[12] P.Y. Yang, Z.F. Cao, X.L. Dong, Fuzzy Identity Based Signature, *IACR Cryptol. ePrint Arch*, vol. 2008, 2, 2008.

[13] H.K. Maji, P. Manoj, R. Mike, Attribute-based signatures: Achieving attribute-privacy and collusion-resistance, *Cryptology ePrint Archive*, 2008, https://ia.cr/2008/328.

[14] S.Q. Guo, Y.P. Zeng, Attribute-based signature scheme, *2008 International Conference on Information Security and Assurance (ISA 2008)*, IEEE, pp. 509-511, 2008.

[15] L. Jin, K. Kwangjo, Attribute-Based Ring Signatures, *IACR Cryptol. ePrint Arch*, vol. 2008, 394, 2008.

[16] S.F. Shahandashti, S.N. Reihaneh, Threshold attribute-based signatures and their application to anonymous credential systems, *International conference on cryptology in Africa*, Springer, Berlin, Heidelberg, pp. 198-216, 2009.

[17] L. Jin, H.A. Man, S. Willy, D.Q. Xie, R, Kui, Attribute-based signature and its applications, *Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security*, pp. 60-69, 2010.

[18] H.K. Maji, P. Manoj, R. Mike, Attribute-based signatures, *Cryptographers' track at the RSA conference*, Springer, Berlin, Heidelberg, pp. 376-392, 2011.

[19] J.Z. Dai, X.H. Yang, J.X. Dong, Designated-receiver proxy signature scheme for electronic commerce, *SMC'03 Conference Proceedings. 2003 IEEE International Conference on Systems, Man and Cybernetics. Conference Theme-System Security and Assurance (Cat. No. 03CH37483)*, pp.384-389, 2003.

[20] G.L. Wang, Designated-verifier proxy signatures for e-commerce, *2004 IEEE International Conference on Multimedia and Expo (ICME)(IEEE Cat. No. 04TH8763)*, pp. 1731-1734, 2004.

[21] X.M. Hu, W.A. Tan, H.J. Xu, J. Wang, Short and provably secure designated verifier proxy signature scheme, *IET Information Security*, vol. 10, no. 2, pp. 69-79, 2016.

[22] G.K. Verma, B.B. Singh, H. Singh, Bandwidth efficient designated verifier proxy signature scheme for healthcare wireless sensor networks, *Ad Hoc Networks*, vol. 81, pp. 100-108, 2018.

[23] A. Mahmoodi, J. Mohajery, M. Salmasizadeh, A certificate-based proxy signature with message recovery without bilinear pairing, *Security and Communication Networks*, vol. 9, no. 18, pp. 4983-4991, 2016.

[24] H. Singh, G.K. Verma, ID-based proxy signature scheme with message recovery, *Journal of Systems and Software*, vol. 85, no. 1, pp. 209-214, 2012.

[25] K.F. Wang, Y. Mu, W. Susilo, F.C. Guo, Attribute-based signature with message recovery, *International Conference on Information Security Practice and Experience*, Springer, Cham, pp. 433-447, 2014.