Identity-Based Designated-Verifier Proxy Signature Scheme with Information Recovery in Telemedicine System

Yuping Zhou,1,2 Yu Hu,1 Jianneng Chen,1 Zengjie Huang,1 Hui Huang,1 and Yi Fan Zhang1

1School of Computer Science, Minnan Normal University, Zhangzhou 363000, China
2Key Laboratory of Data Science and Intelligence Application, Fujian Province University, Zhangzhou 363000, China

Correspondence should be addressed to Yuping Zhou; 2228709@163.com

Received 1 February 2022; Revised 17 February 2022; Accepted 23 February 2022; Published 18 March 2022

Abstract

With the promotion of Remote Medical Treatment, the sharing of big telemedicine data becomes more and more popular. Telemedicine based on wireless sensor networks collects blood pressure, pH value, pulse, and other medical information from the telemedicine healthcare terminal. The medical information is sent to the hospital or medical server for processing. The security protection of patient medical data, such as confidentiality and authenticity, has gradually become a critical problem to be solved in the development of cloud medical service platform. A provably secure identity-based designated-verifier proxy signature scheme with information recovery for cloud medical diagnosis network is proposed. The scheme is on the basis of computational Diffie-Hellman difficult problem and existential unforgeable against adaptive chosen message attacks in the random oracle model. The performance analysis shows that the scheme is appropriate to the remote medical diagnosis system.

1. Introduction

Cloud health care refers to that the supremacy of medical technology and equipment owned by only a few first-class hospitals or specialized hospitals has been brought into full play to perform remote diagnosis, treatment, and consultation for remote patients by relying on these technologies, such as computer technology, remote sensing, and remote-control technology [1, 2]. As the demand for telemedicine is expanding, electronic diagnosis and treatment systems based on wireless sensor networks develop rapidly [3]. In the electronic medical system, the medical data of a patient, like blood oxygen, pH value, pulse, and electrocardiogram (ECG), can be collected by the sensors embedded or worn on the remote patient and transmitted to the remote medical expert through the wireless networks. The confidentiality and authenticity of the medical data of patients often become the target of malicious attackers.

Network attackers generally utilize active attacks or passive attacks [4]. Active attack refers to the attacker interfer-
To solve these security problems, the wireless sensor network framework of cloud medical treatment based on some security technologies is proposed. Ng et al. [6] proposed a type of system framework; as shown in Figure 1, some terminal sensors are deployed on a patient. The server collects information by using a wireless internet connection, and it analyzes and transmits this information to a local or remote doctor. This framework has become a universal wireless sensor network framework of cloud medical treatment. To ensure secure communication, the collected medical data is transmitted to the hospital server after being digitally signed to ensure data integrity. In order to ensure authenticity confirmation, a method which authorizes the designated recipient is proposed. According to this scheme of things, the hospital administrator or web developer acting as Deploying Authority (DA) authorizes its signing ability to the sensor. A trained doctor is designated as the recipient. In this way, the Deploying Authority acts as the original signer, the terminal sensor acts as the proxy signer, and the healthcare professional is designated as the recipient. Because of the restrictions of storage space and energy, the medical terminal needs a digital signature scheme satisfying storage space and energy efficiency, so an efficient designated-verifier proxy signature scheme is the highly urgent request of a telemedicine system.

Mambo et al. [7] presented the proxy signature (PS); this method implements authorization of signing power. According to the idea, the proxy signer is licensed for signing an efficient proxy signature, and the verifier trusts this authorization protocol. The proxy signature scheme applying warrant is widely used in realistic communication systems. The warrant contains information about the identity of concerned people, including both principal and agent, and the validity of the agency agreement. The original signer encrypts the authorization with his private key and transmits it to the proxy signer. The proxy signer verifies the validity of the warrant with the original signer’s public key and then signs the file by using the warrant and his private key. A certificateless designated-verifier proxy signature (CLDVPS) scheme was proposed by He et al. [8]; the method can meet the requirement of certification management and key escrow and achieve high-speed operation of unmanned aerial vehicle executing commands. Only the designated verifier is able to validate the signature in the scheme. Zheng et al. [9] presented a scheme that can be deployed over the existing quantum key distribution networks without complex quantum operations. The correlated key strings are generated by the use of the scheme protecting the communication against potential eavesdroppers. A designated verifier proxy signature (DVPRS) is proposed by Wei et al. [10]; the proxy can reappoint a new verifier in DVPRS, which is applicable to deniable and/or anonymous authentication. Shi et al. [11] presented a real quantum designated verifier signature scheme on the basis of quantum deniable authentication protocol. One of the strengths of the scheme is the power of resisting impersonation attacks and entangle-measure attacks. Singh and Verma [12] utilized the advantages of information recovery signature and proxy signature to present an identity-based information recovery proxy signature scheme.

In 2020, an aggregatable certificateless designated verifier signature scheme (ACLUDVS) was presented by Thorncharoenrsi et al. to implement secure data access and sharing for cloud storage. ACLUDVS is efficient for privacy protection system of the Internet of Things or VANET, the security of the scheme relies on Computational Diffie-Hellman (CDH) assumption [13]. In 2017, an identity-based aggregate signature (IBAS) scheme with designated verifier for WSNs was presented by Shen et al., and the scheme was shown to be secure and efficient; it can keep data integrity; at the same time, the bandwidth and the storage efficiency are high for WSNs [14]. This scheme is secure in the random oracle model under the CDH assumption. In 2011, Shim [15] presented a short designated verifier proxy signature scheme which is confirmed to be safe in the enhanced attacker model. Lin et al. [16] proposed a short DVPS scheme, which is existentially unforgeable against chosen message attack in the random oracle model, but the scheme does not consider the fully attack model. In 2018, a provably secure message recovery designated verifier proxy signature (MRDVPS) scheme was proposed by Verma et al. [17], which is applicable for healthcare wireless sensor networks (HWSN). The scheme satisfies the confidentiality and authentication of data. Hu et al. [18] presented a short provably secure DVPS...
based on linear pairs in random oracle. The scheme considers an enhanced attack model including six types of attackers with different abilities. In terms of the length of a tuple consisting of information and signature, the scheme produces a signature shorter than the existing information recovery DVPS scheme.

The deployment of cloud medical care in wireless sensor networks makes secure communication more urgent. The authenticity of the receiver and sender and the authenticity and confidentiality of patient medical data are all key issues that need to be resolved, especially different security requirements, including integrity, authenticity, confidentiality, and timeliness. To deal with these problems, Verma et al. [19] presented an information recovery proxy signature scheme applied in electronic medical wireless sensor networks, but the scheme only satisfies authenticity and timeliness. In order to meet the four security requirements, at the same time, it is necessary to study the information recovery proxy signature with more features. In the designated-verifier proxy signature, only the verifier who is designated can verify the signature. Combining a message recovery signature, the designated-verifier signature can better solve the four security challenges. In the improved DVPS scheme, the information is permitted to be retrieved only by the designated verifier, so the security features of integrity and confidentiality are achieved. In the solution design, the hospital administrator or deployment authority authorizes their signing right to the sensor, and the sensor signs information on behalf of the hospital administrator or deployment authority. Only the designated recipient, that is a professional doctor, can verify the signature. Due to constraints of energy and bandwidth in wireless sensor networks, designing an authorization method meeting more requirements on security is one of the main considerations. For the required purpose, we present an effective authentication scheme based on identity information to recover the designated-verifier proxy signature. In the scheme, it is all signature and no information which is sent to the designated verifier. The information is recovered during the verification process. The shorter length of signature and the better confidentiality are guaranteed at the same time. The scheme is existentially unforgeable against chosen message attack in the random oracle model and has better performance on computing cost and length.

2. Preliminaries

2.1. Bilinear Pairing. Let \((G, +)\) and \((G_T, \cdot)\) be cyclic groups whose order is the large prime \(q\); the Discrete Logarithm Problem (DLP) is held in \((G, +)\) and \((G_T, \cdot)\). A bilinear pairing map \(\bar{e}: G \times G \rightarrow G_T\) possesses the following properties:

1. Bilinearity: for any \(P, Q \in G\) and \(a, b \in \mathbb{Z}_q^*\), it has \(\bar{e}(aP, bQ) = \bar{e}(P, Q)^{ab}\).
2. Nondegeneracy: there exists \(P, Q \in G\) to satisfy \(\bar{e}(P, Q) \neq 1_{G_T}\).
3. Computability: for any \(P, Q \in G\), there is an efficient algorithm to compute \(\bar{e}(P, Q)\).

That is, \(\bar{e}(P, Q)\) is bilinear groups. Generally, \(G\) contains point on elliptic curve. \(e_i\) can be Tate pairing or Weil pairing.

2.2. CDH Problem. \(\forall a, \beta \in \mathbb{Z}_q^*\) and \(P, \alpha P, \beta P \in G\), compute \(\alpha \beta P \in G\).

3. System Framework

3.1. System Model. There are five entities existing in the telemedicine wireless sensor networks as shown in Figure 2: Private Key Generator (PKG), Deploying Authority (DA), Sensor, Medical Server (MS), and medical professional. The main functions of each entity are as follows:

1. Private Key Generator (PKG): the PKG creates a private key for each participant and then sends it to the user through a secure channel. It is a trusted third party.
2. Deploying Authority (DA): the DA is a network developer. It develops and maintains the system and is responsible for solving related network problems. In some special scenarios, the hospital administrator takes on the role.
3. Sensor: the sensors are embedded or wearable on patients to collect patient healthcare information and then send these data to the medical server through the wireless gateway. A short message is appropriate for the sensors with limited storage and energy.
4. Medical Server (MS): Medical Server is the core unit of the system with powerful storage and computing capabilities. Medical information is acquired from the relevant wireless gateways and sent to doctors with the help of MS.
5. Medical professional: medical professional is a trained professional. They receive medical data from the patients for diagnosis and then make clinical treatment strategies according to the medical data.

In the system model, the Deploying Authority is the original signer who can authorize the signature rights to others; the sensor acts as a proxy signer, which accepts signature right from the Deploying Authority, signs the information, and then sends the signature to the designated recipient through the medical server. Receiving the signature from any sensor, the medical server sends the signatures to the relevant doctor; finally, the doctor uses his private key to recover the patient’s medical data in the process of signature verification, performs diagnosis, and then makes clinical treatment strategies according to the medical data.

3.2. The Algorithm Framework. The paradigm of the identity-based designated-verifier proxy signature scheme (IDDVPS) scheme includes three active entities: Alice (original signer), Bob (proxy signer), and Cindy (designated signer)
The scheme is on the basis of the schemes of Singh and Verma [12] and Hu et al. [18]. The program framework contains 8 polynomial-time algorithms: Setup, Extract, DelegGen, DeleVerify, DVProxySign, DBProxySVerify, DVPSimulation, and Correctness.

1. Setup: a Probabilistic Polynomial Time (PPT) algorithm Setup enters a security parameter \( \lambda \) and outputs system parameters.

2. Extract: a PPT algorithm Extract takes input system parameters and outputs user’s key pair \((QB, SB)\), including the original signer Alice’s key pair \((QA, SA)\), the proxy signer Bob’s key pair \((QB', SB')\), and the designated verifier Cindy’s key pair \((QC, SC)\).

3. DelegGen: PPT algorithm DelegGen enters the PKG’s master key and the warrant \( w \). It outputs the delegation \( \sigma_1 \) passed to Bob by a security tunnel.

4. DeleVerify: PPT algorithm DeleVerify takes input \((w, \sigma_1)\) and the PKG’s master key; it outputs \( b \in \{0, 1\} \). If \( b = 1 \), it accepts the validity of \((w, \sigma_1)\); otherwise, it refuses the validity of \((w, \sigma_1)\). If \( b = 1 \), the proxy signer computes \( S_p = <\sigma_1, S_B> \) as the proxy signature key.

5. DVProxySign: PPT algorithm DVProxySign takes input the proxy signer’s key \( S_p \), the warrant \( w \), the designated verifier’s public key \( Q_C \), and the message \( m \in \{0, 1\}^{L_2} \); it outputs proxy signature \( \sigma \).

6. DVProxySVerify: PPT algorithm DVProxySVerify enters verifier Cindy’s private key \( S_C \), Bob’s public key \( QB \), and the proxy signature \( \sigma \); it outputs \( m \in \{0, 1\}^{L_2} \) and \( b \in \{0, 1\} \). If \( b = 1 \), the message \( m \) and the proxy signature \( \sigma \) are accepted; otherwise, the message \( m \) and the proxy signature \( \sigma \) are refused.

7. DVPSimulation: by using PPT algorithm DVPSimulation, verifier Cindy can imitate a proxy signature which someone is unable to tell from the original signature.

8. Correctness: PPT algorithm Correctness outputs the correctness proof of information recovery and validation process.

3.3. Security Model. Implementation of security in the IDDVPS scheme is mainly considered from several aspects, including unforgeability, nontransferability, and nonauthorization. A Universal Designated Verifier Signature (UDVS) scheme is derived on the basis of the Designated Verifier Signature (DVS) scheme proposed by Parvin et al. [20], and the signature holder can transform it into DVS. The UDVS is said to be the first nondelegatable UDVS scheme.

In 2012, Singh and Verma [12] presented the first information recovery proxy signature scheme with a shorter signature length, and the unforgeability of the scheme is mainly considered. Hu et al. [18] put forward the security model with six types of the strongest adversaries. According to these previous studies, we take into account five types of adversaries and design a play-based method to check that the IDDVPS scheme is unforgeable, nontransferable, and identifiable under the random oracle model. The attackers are divided into five types of adversaries according to their attack ability:

1. Type 1 adversary \( (A_1) \): \( A_1 \) knows the public keys of Alice, Bob, and Cindy \((QA, QB, QC)\).

2. Type 2 adversary \( (A_2) \): \( A_2 \) knows the public keys of Alice, Bob, and Cindy \((QA, QB, QC)\) and the private key of Bob \( SB \).

3. Type 3 adversary \( (A_3) \): \( A_3 \) knows the public keys of Alice, Bob, and Cindy \((QA, QB, QC)\) and the private key of Alice \( SA \).
(4) Type 4 adversary \(A_4\): \(A_4\) knows the public keys of Alice, Bob, and Cindy \((Q_A, Q_B, Q_C)\) and the private key of Cindy \(S_C\).

(5) Type 5 adversary \(A_5\): \(A_5\) knows the public keys of Alice, Bob, and Cindy \((Q_A, Q_B, Q_C)\) and the private keys of Bob and Cindy \((S_B, S_C)\).

It can be clearly seen from the above classification that if the security model can resist type 5 adversary \(A_5\), it will be sure to resist type 1 \((A_1)\), type 2 \((A_2)\), type 3 \((A_3)\), and type 4 \((A_4)\). The scheme can be proved to be provably secure against adaptive-chosen-plaintext attack in random oracle model by analyzing the type 5 adversary.

3.3.1. Game 1 (Aimed at the Unforgeability of the Type 5 Adversary \((A_5)\))

Aimed at the type 5 adversary, the model is existentially unforgeable against adaptive chosen plaintext attacks in the random oracle model. The type 5 adversary gets the public keys of signer and verifier \((Q_A, Q_B, Q_C)\), the private key of the proxy signer, and designated verifier \((S_B, S_C)\), so the proxy signature key can be obtained. To analyze EUF-ACMA, the general model of type 5 \((A_5)\) and challenger \((CH)\) is as follows:

1. Setup(.)\(): the challenger runs algorithm Setup(.), \(\text{Params} \leftarrow \text{Setup}(1^k)\), where superscript \(k\) is security param; it outputs system params.

2. Extract(.)\(): the challenger runs algorithm Extract(.); it enters system params and generates the key pair \((Q_u, S_u)\) for all user \(u\) including the original signer Alice’s key pair \((Q_A, S_A)\), the proxy signer Bob’s key pair \((Q_B, S_B)\), and the designated verifier Cindy’s key pair \((Q_C, S_C)\). And then CH provides the public keys of the original signer Alice, proxy signer Bob, designated signer Cindy \((Q_A, Q_B, Q_C)\), and the private keys of proxy signer Bob, designated signer Cindy \((S_B, S_C)\) to the adversary \(A_5\).

3. DeleGen(.)\(): adversary \(A_5\) queries the DeleGen(.) oracle, adaptively chooses input warrant \(w\), and obtains delegation \(\sigma_i\) from CH.

4. DVproxySign(.)\(): adversary \(A_5\) queries the DVproxySign(.) oracle and adaptively chooses to input message, warrant, and delegation \((m, w, \sigma_i)\); the CH returns proxy signature \(\sigma\).

5. DVproxySVerify(.)\(): \(\sigma(w^*, \sigma_i^*)A_5(w^*, \sigma_i^*)\) Output(.)\(): adversary \(A_5\) queries the DVproxySVerify(.) oracle and adaptively inputs signature; if the output is valid, the return value of CH is the corresponding message strings; otherwise, the return value of CH is invalid.

6. Output(.)\(): it queries the oracle; it inputs to obtain a target message string \(m^* \in \{0, 1\}^{t_2}\) and the corresponding proxy signature \(\sigma^*\), where

- (i) \((w^*, \sigma_i^*)\) is not in the output list of DeleGen(.) oracle
- (ii) \((w^*, \sigma_i^*)\) is not in the output list of DVproxySign(.) oracle
- (iii) \((w^*, \sigma_i^*)\) and \(\sigma^*\) are the valid delegation and proxy signature

The success rate of an attack of Adversary \(A_5\) is

\[
\text{Succ}^\text{EUF-ACMA}_{A_5, \text{IDEMR-DVPS}}
\]

which equals to the winning probability of Adversary \(A_5\) in game 1.

**Definition 1.** When a forger \(A_5(t, q_{del}, q_H, q_{ps}, q_{psv}, \epsilon)\) requests no more than \(q_{del}\) queries, no more than \(q_H\) hash queries, no more than \(q_{ps}\) DVProxySign(.) queries, and no more than \(q_{psv}\) DVProxySVerify(.) queries, an attack is successfully achieved with probability

\[
\text{Succ}^\text{EUF-ACMA}_{A_5, \text{IDEMR-DVPS}} > \epsilon q_{ps}
\]

within at most \(t\) time. If the probability of success of a in-game forger \(A_5(t, q_{del}, q_H, q_{ps}, q_{psv}, \epsilon)\) is negligible, then the IDEMR-DVPS scheme is robust against \(A_5(t, q_{del}, q_H, q_{ps}, q_{psv}, \epsilon)\) under adaptive-chosen-plaintext attack. In other words, the IDEMR-DVPS scheme is \(A_5(t, q_{del}, q_H, q_{ps}, q_{psv}, \epsilon)\)-existential unforgeability.
4. Identity-Based Designated-Verifier Proxy Signature Scheme with Information Recovery in Telemedicine System

The medical data of telemedicine system is required to meet some security characteristics: integrity, authenticity, confidentiality, and freshness. The application of the Message Recovery Proxy Signature (MR-PS) scheme applied in telemedicine system can only satisfy authenticity and freshness.

To meet more security characteristics, new features need to be added to the existing MR-PS scheme. In identity-based Message Recovery-Designated Verifiers Proxy Signature (IDMR-DVPS) scheme, the signature can only check the validity by the designated verifier and the message is recovered during the verification process, and thus, the confidentiality and integrity are provided; data flow of telemedicine system is shown in Figure 3.

There are eight steps in the scheme defined as follows:

(1) Setup: a probabilistic polynomial time algorithm \( (\text{Setup}) \) inputs \( 1^k \) as security parameters. The PKG selects the main key \( S \in \mathbb{Z}_q^* \), calculates

\[
P_{pub} = SP,
\]

keeps the main key \( G_T \) and outputs system public parameters \( \text{Params} = (G, G_T, H, H_0, H_1, H_2, H_3, e_r, P, P_{pub}, q, L_1, L_2) \), where \( G \) is a cyclic group, \( q \) is a multiplicative cyclic group, \( e_r : G \times G \rightarrow G_T \) is a bilinear map, \( H_1, H_2 : \{0, 1\}^{L_2} \rightarrow \{0, 1\}^{L_1} \), \( H_3 : \{0, 1\} \rightarrow \mathbb{Z}_q^* \), and \( L_1 + L_2 = |g| \).

(2) Extract: the user \( \text{ID}_U \) calculates user’s public key

\[
Q_{\text{ID}_U} = H_0(\text{ID}_U).
\]

The PKG calculates private key

\[
S_{\text{ID}_U} = sH_0(\text{ID}_U),
\]

to send to user. User verified whether the equation

\[
e_r(Q_{\text{ID}_U}, P_{pub}) = e_r(S_{\text{ID}_U}, P)
\]

holds after receiving the private key. If it holds, the user will accept the private key. Thus, the initial signer Alice has a pair of keys \( (Q_A, S_A) \), the proxy signer Bob has a pair of keys \( (Q_B, S_B) \), and the designated signer Cindy has a pair of keys \( (Q_C, S_C) \).

(3) DeleGen: the initial signer Alice calculates

\[
w' = H_3(S_A \cdot H_0(w)),
\]

according to the authorization information \( w \) (authorization information includes the identity information of the initial signer and proxy signer, authentication validity period, the type of signature information string \( m \), and other related information), and sends WCMC_1580444 to PKG; the PKG verified whether the equation

\[
w' = H_3(S_A \cdot H_0(w))
\]

holds. If it holds, the PKG computes

\[
\sigma_1 = S \cdot H_0(w)
\]

and then sends \( (w, \sigma_1) \) to the proxy signer Bob secretly by secure channel.

(4) DeleVerify: the proxy signer can validate the effect of warrant according to whether the equation

\[
e_r(\sigma_1, P) = e_r(H_0(w), P_{pub})
\]

holds. If the equation holds, the proxy signer calculates the proxy signature key

\[
S_p = \sigma_1 + S_B.
\]

(5) DVProxySign: the proxy signer performs the following Calculations according to the input information string \( m \in \{0, 1\}^{L_2} \): the proxy signer calculates

\[
u = H_2(H_1(m)) \oplus m
\]

chooses \( r \in \mathbb{Z}_q^* \) randomly, calculates

\[
h = H(w, e_r(S_p, rQ_C)),
\]

\[v = h \oplus u,
\]

\[T = (r - v)S_p,
\]

\[\sigma = (e_r(T, Q_C)),
\]

and returns proxy signature \( \sigma, w, v \). The schematic diagram in which the patient signs the information is shown in Figure 4.

(6) DVProxySVerify: the designated verifier Cindy executes the following calculation during the verification process and calculates

\[
u = v \oplus H(w, \sigma \cdot e_r(v(Q_B + H_0(w)), S_C)),
\]

\[m_0 = H_2(u \mid u) \oplus |u|_{L_2},
\]

where \( u \mid u \) means the first bits of \( u \) from the left side.\( |u|_{L_2} \)
means the first \( L_2 \) bits of \( u \) from the right side \( L_1 \). Cindy verified whether the equation

\[
L_1 | u | = H_1 (m_0)
\]

holds. If it holds, the signature and message are accepted. If it does not hold, the signature and message are rejected.

(7) DVPSimulation: receiving a string \( m \in \{0, 1\}^{L_2} \), the designated verifier Cindy randomly selects \( r' \in \mathbb{Z}_q^* \) and then calculates

\[
h' = H \left( w, e_1 \left( r' \cdot H_0 (w) + Q_B \right), S_C \right),
\]

\[
u' = r' \oplus u,
\]

\[
T' = \left( r' - v' \right) S_C,
\]

\[
\sigma' = e_1 \left( T', H_0 (w) + Q_B \right)
\]

and simulates proxy signature \( (\sigma', w, v') \). The distribution of the simulated proxy signature and the original proxy signature verification is consistent and indistinguishable.

(8) Correctness: the process of DVProxySVerify is correct. For \( \sigma = (e_1 T, Q_C) \), \( \sigma = (e_1 T, Q_C) = e_1 \left( (r - v) S_p, Q_C \right) \), thus,

\[
h = H \left( w, \sigma \cdot e_1 (v(Q_B + H_0 (w)), S_C) \right)
\]

\[
= H \left( w, e_1 \left( (r - v) S_p + Q_C \right) \cdot e_1 (v(Q_B + H_0 (w)), S_C) \right)
\]

\[
= H \left( we_1 (r - v) S_p + Q_C \right) = H \left( we_1 (r - v) S_p + Q_C \right)
\]

\[
= H \left( w, e_1 (r \cdot (H_0 (w) + Q_B), S_C) \right)
\]

\[
= H \left( w, e_1 (r \cdot (H_0 (w) + Q_B), S_C) \right)
\]

\[
u = v \oplus h,
\]

For \( u = H_1 (m) \oplus m \), thus,

\[
L_1 | u | = H_1 (m),
\]

\[
| u | L_2 = H_2 (H_1 (m)) \oplus m
\]

Figure 4: Schematic diagram of the patient’s signature information.
verified whether the equation
\[ H_1(m_0) = \langle L_1 | u \rangle \]  
(27)
is tenable. If it is tenable, the designated verifier Cindy recognizes the valid of \((\sigma, w, v)\) for the information \(m\).

### 5. Security Analysis

The scheme has security characteristics of EUF-ACMA, nondelegation, nontransferability, and strong-identifiability.

#### 5.1. Unforgeability

For example, in game 1, the scheme is EUF-ACMA against type 5 adversary.

**Theorem 1.** Let a adversary \(A_5\) be a PPT Adversary who plays \(\text{Exp}_{\lambda}^\text{DELMR-DVPS}\) by using \(\text{DelegGen}(\cdot), H_0(\cdot), H(\cdot), H_1(\cdot), H_2(\cdot), \) and \(\text{DVProxySign}(\cdot)\) oracles to produce recovery designated verifier’s signature \(\sigma\) based on the identity within \(t\) times, and the signature \(\sigma\) can be verified by \(\text{DVProxySVerify}(\cdot)\) with a nonnegligible probability \(\varepsilon > 0\).

\(A_5\) requests \(q_{d_1}, q_{H_1}, q_{H_2}, q_{H_1}, q_{\text{dvps}}\) and \(q_{\text{dvps}}\) time queries for \(\text{DelegGen}(\cdot), H_0(\cdot), H(\cdot), H_1(\cdot), H_2(\cdot), \) \(\text{DVProxySign}(\cdot), \) and \(\text{DVProxySVerify}(\cdot)\) oracle, respectively. Then, the polynomial time algorithm \(B\) can be designed as a solution to the BDH problem with successful probability
\[ \text{Succ}^{(\text{CDHP})} \geq \frac{1}{\varepsilon^2} \left( \frac{1}{q + 1} \right)^q \varepsilon, \]  
(28)
where \(q\) is the max value of \(\{q_{d_1}, q_{H_1}, q_{H_2}, q_{H_1}, q_{\text{dvps}}\}, \varepsilon\) is the base of a natural logarithm, and \(B\) simulates a challenger as the following proof.

**Proof.** \(B\) chooses \(c_1 \in \mathbb{Z}_q^*\) randomly and sets the public key of the PKG \(P_{\text{pub}} = \alpha P\), the public key of original signer Alice \(Q_A = c_1 P\), the public key of proxy signer Bob \(Q_B = \beta P\), and the public key of designated verifier Cindy \(Q_C = c_P P\). The PKG sends \((Q_A, Q_B, Q_C, c_1)\) to \(A_5\). The goal of \(B\) is to compute \(e(P, P)^{abc}\) according to \((P, \alpha P, \beta P, c_P P)\), and then the BDH problem is solved. Assume \(B\) controls \(\text{DelegGen}(\cdot), H_0(\cdot), H(\cdot), H_1(\cdot), H_2(\cdot), H_3(\cdot), \) \(\text{DVProxySign}(\cdot), \) and \(\text{Extract}(\cdot)\) oracles and holds all answer lists such as \(\text{list}_{D_0}, \text{list}_{D_1}, \text{list}_{H_0}, \text{list}_{H_1}, \text{list}_{H_2}, \text{list}_{H_3}, \text{list}_{\text{DVPS}}, \) and \(\text{list}_{\text{C}}\); all lists are empty initially. \(H_0(\cdot)\) query: \(B\)'s response outputs to all asked \(w_i (1 \leq i \leq q_{\text{dvps}})\) are saved as the records of \(\text{list}_{H_0}\). \(B\) first inquires \(\text{list}_{H_0}\) oracle according to the enquired warrant \(w_i\). If there is a corresponding record in the list, the record is output to the adversary \(A_5\). Otherwise, \(B\) chooses \(h_0 \in \mathbb{Z}_q^*\) randomly, sets \(K_i = h_0^i P \leftarrow H_0(w_i)\), and then updates \(\text{list}_{H_0} \leftarrow \text{list}_{H_0} \cup \{(K_i, w_i, h_0^i)\}\).

\(H(\cdot)\) query: the adversary \(A_5\) inquires \(H(\cdot)\) oracle about Hash value by inputting \((w_i, \text{ID}_A, \text{ID}_B, \text{ID}_C)\). \(B\)'s response outputs for all Hash requests are saved as the records of \(\text{list}_{H}\). \(B\) first inquires \(\text{list}_{H}\), if there exists a corresponding record in the list; the record is output to the adversary \(A_5\). Otherwise, \(B\) selects \(r_i \in \{0, 1\}^{q_{\text{dvps}}}, h_i \leftarrow H(w_i, e(r_i \cdot a \cdot (H_0(w_i) + H_0(\text{ID}_B)), c_P)\) randomly, sends \(h_i\) to the adversary \(A_5\), and then updates \(\text{list}_{H} \leftarrow \text{list}_{H} \cup \{(h_i, w_i, r_i, \text{ID}_A, \text{ID}_B, \text{ID}_C)\}\).

\(H_1(\cdot)\) query: if the adversary \(A_5\) queries \(m_i \in \{0, 1\}^{q_{\text{dvps}}}\) from \(H_1(\cdot)\) oracle, when \(m_i\) does not exist in the output list of \(\text{DVProxySign}(\cdot)\), \(B\) saves the list of records \(\text{list}_{H}\) responded from \(H_1(\cdot)\) query to adversary \(A_5\). \(B\) searches \(\text{list}_{H}\) first, if there exists a corresponding record in the list, \(B\) sends it to \(A_5\). Otherwise, \(B\) chooses \(s_{i_1} \in \{0, 1\}^{q_{\text{dvps}}}\) randomly, sets
\[ F_1(m_i) = s_{i_1}, \]  
(29)
sends record to \(A_5\), and updates \(\text{list}_{H} \leftarrow \text{list}_{H} \cup \{(m_i, s_{i_1}, s_{i_1})\}\).

\(H_2(\cdot)\) query: \(B\) saves the list of records \(\text{list}_{D_0}\) responded from \(\text{DelegGen}(\cdot)\) query. \(B\) searches target in \(\text{list}_{H}\) according to \((k_i, w_i, h_0^i, b_i)\). If there exists a corresponding record in the list, \(B\) sends it to \(A_5\). Otherwise, \(B\) requests \(H_0(\cdot)\) to get the output and chooses \(b_i \in \{0, 1\}\) randomly to make
\[ \text{Pr}[b_i = 0] = \frac{1}{\delta}. \]  
(31)
If \(b_i = 0\), \(B\) quits and output fails. If \(b_i = 1\), \(B\) outputs
\[ \sigma_1^i = h_0^i P_{\text{pub}} = a \cdot h_1^i \cdot P, \]  
(32)
then \(A_5\) as delegation updates \(\text{list}_{D_0} \leftarrow \text{list}_{D_0} \cup \{(w_i, \sigma_1^i, b_i)\}\).

\(H_3(\cdot)\) query: supposing the adversary \(A_5\) inquires \(\text{DVProxySign}(\cdot)\) according to \(m_i \in \{0, 1\}^{q_{\text{dvps}}}, w_i (1 \leq i \leq q_{\text{dvps}})\), \(B\) saves the list of records \(\text{list}_{\text{DVPS}}\) responded from \(\text{DVProxySign}(\cdot)\). \(B\) inquires \(\text{list}_{\text{DVPS}}\) according to input. If the corresponding item can be found, the output is sent to the adversary \(A_5\). Otherwise, \(B\) runs \(H_0(\cdot), \text{DelegGen}(\cdot), F_1(\cdot), F_2(\cdot), \) and \(H(\cdot)\) to acquire \((w_i, k_i, h_0^i), (\sigma_1^i, b_i, w_i), (m_i, s_{i_1}, s_{i_2}), \) and \((r_i, h_i, w_i)\), and calculates
\[ v_i = h_i \oplus (s_{i_1} \| s_{i_2} \oplus m_i), \]  
(33)
If \( b_1 = 0 \), \( B \) stops running and quits. If \( b_1 = 1 \), \( B \) calculates
\[
\sigma_i = e((r_i - v_i)(H_Q(w) + bP), cP)
\]
and sends \((\sigma_i, v_i)\) to \( A_5 \). If \( e((r_i - v_i)(H_Q(w) + H_Q(ID_b)), S_c) = e((r_i - v_i)S_p, Q_c) \) holds, \((\sigma_i, v_i)\) is a valid signature.

Output(\( \cdot \)): the adversary \( A_5 \) generates a forged signature as follows:
Adversary \( A_5 \) generates \((\sigma^*, w^*, v^*)\) as a valid proxy signature of \( m^* \) and \((v^*, w^*, v^*) \notin \text{list}_{DVPS} \).

If the adversary succeeds in forging, \((\sigma^*, w^*, v^*)\) is the valid proxy signature.
If \( b_1^* = 1 \), \( B \) quits and output fails.
If \( b_1^* = 0 \), then, \( H_Q(w^*) = h_0^*PT^* = (r^* - v^*)(h_0^*P + bP) \)
\( a, B \) calculates
\[
\sigma^* = e_1(T, Q_c) = e_1((r^* - v^*)(h_0^*P + bP), a, cP)
= e_1(h_0^*P_{pub} Q_c)^{r^* - v^*} e_1(P, P)^{abc(r^* - v^*)}.
\]

Then,
\[
\frac{\sigma^*- (r^* - v^*)}{e_1(h_0^*P_{pub} Q_c)^{r^* - v^*}} = e_1(P, P)^{abc}
\]
is the solution of BDH problem.
Consider the probability of \( B \) successfully solving the CDH problem in the following two situations.
\( (E_1) \): \( b_1^* = 0 \) in request.
\( (E_2) \): the adversary \( A_5 \) forges a valid signature.
Then,
\[
\text{Succ}_{B,G_0}^{\text{CDHP}} = \text{Pr}[E_1 \cap E_2] = \text{Pr}[E_1] \text{ Pr}[E_2 | E_1] \geq \left(1 - \frac{1}{7}\right)^{q_{G_0}} \left(1 - \frac{1}{7}\right)^{d_j} \epsilon.
\]
\[
(37)
\]
To achieve the optimal probability of success, set \( l = q + 1 \), where \( q = \{q_{G_0}, q_{H_1}, q_{H_2}, q_{H_3}, q_{G_0}, q_{G_1}, q_{G_2}\} \), then
\[
\text{Succ}_{B,G_1}^{\text{BDHP}} = \text{Pr}[E_1 \cap E_2] = \text{Pr}[E_1] \text{ Pr}[E_2 | E_1] \geq \frac{1}{e^l} \epsilon.
\]
\[
(38)
\]
5.2. Nontransferability. The designated verifier Cindy cannot confirm to a third party whether the signature was signed by the proxy signer Bob or himself. In short, the proxy signature and the simulated signature have the same distribution. Through simulation, the distribution of probability \( \text{Pr}[(\sigma, v) = (\sigma_1, v_1)] \) and probability \( \text{Pr}[(\sigma', v') = (\sigma_1, v_1)] \) are the same, and the scheme is nontransferable.

5.3. Strong Identifiability. The program provides a warrant, and the proxy signer Bob can be identified by verifying the warrant \( w \), so the scheme has strong identifiability.
In the anti-misuse attack, the warrant contains the signed information string, so that the proxy signer Bob cannot sign proxy signature by using illegal information string, which can effectively prevent misuse attacks. At the same
time, apart from the designated verifier, no third party can validate the proxy signature, which makes the scheme robust.

6. Performance Analysis
In the wireless medical sensor networks, the collection of remote medical data is completed by the sensor embedded in or worn on the patient, and then the sensor transmits the medical data to the medical server, so the signature length and the computational cost of sensor become the main performance indicator of design scheme. Different steps of the scheme are completed by different entities. For example, proxy verification and proxy signature are performed on the sensor while some steps are performed on the authority or the medical server. Therefore, it is necessary to consider the signature length and overall consumption of transmission in different stages. Related notations are denoted in Table 1.

Here, elliptic curve point addition, XOR, \( H_1, H_2 \), modular addition, and other effective operations are ignored. In order to achieve the 3072-bit RSA security level, the element lengths of \( G, G_T, Z_q \) are considered to be 256 bits \((|G|)\), 3072 bits \((|G_T|)\), and 256 bits separately, and the length of the information string is \(|m|\). Because the message is recovered during the signature verification process and no message string is attached to the signature, the signature length of the scheme is \(|w| + 512\).

We evaluate the costs of the basic operations on a client machine with Intel i7-4600U 2.70GHz CPU and 4GB RAM. The operating system of the host is Ubuntu 14.04 for 64 bit. As shown in Table 2, the computing cost of IDEMR-DVPS is smaller than that of literature [15] and equal to that of the literature [21]. The computing cost of literature [18] is 0.3 ms less than that of IDEMR-DVPS scheme, but their signature length is \(|m| + 256|, |m| + 2560, and \(|m| \) bits larger than that of IDEMR-DVPS, respectively. As far as computation cost and bandwidth are concerned, the performance of IDEMR-DVPS scheme is better. In the telemedicine wireless sensor networks, Deleverify(\( . \)) and DVProxySign(\( . \)) are executed on the sensor, but Deleverify(\( . \)) is not executed in

| Symbol | Definition | Time |
|--------|------------|------|
| \( S_m \) | Multiplication | 0.39 ms |
| \( c_t \) | Pair operation | 3.21 ms |
| \( H \) | Point hash operation | 0.09 ms |

**Table 2:** Comparison of efficiency of different schemes.

| Scheme | Computing cost | Signature length |
|--------|----------------|------------------|
| Literature [21] | \( 4H + 4S_m + 5c_t \) (17.97 ms) | \(|m| + |w| + 768\) |
| Literature [15] | \( 7H + 5S_m + 5c_t \) (18.63 ms) | \(|w| + |m| + 3072\) |
| Literature [18] | \( 5H + 3S_m + 5c_t \) (17.67 ms) | \(|m| + |w| + 512\) |
| IDEMR-DVPS | \( 4H + 4S_m + 5c_t \) (17.97 ms) | \(|w| + 512\) |
every session of signing, which is executed more frequently than DVProxySign(·). And its computing cost is \( S_m + 2e \), (6.81 ms) affordable for the sensor.

In summary, the IDEMR-DVPS scheme consumes 17.97 ms overall and is highly efficient. Meanwhile, the scheme with several attributes such as the designated verifier and message recovery satisfies the four security requirements and short bandwidth, while other schemes have low bandwidth efficiency or can only meet part of the security requirements. The IDEMR-DVPS scheme is suitable for telemedicine wireless sensor networks.

### 7. Conclusion

Telemedicine wireless sensor networks have been gaining popularity in practice, and the authorized signature scheme of the designated verifier is adopted in most system development. A safe and bandwidth-available IDEMR-DVPS scheme applying elliptic curve bilinear pair mapping is proposed in our paper, and the message is not attached to the signature to be sent to the verifier in the scheme. During the verification process, the scheme satisfies security requirements of telemedicine wireless sensor networks such as data integrity, authenticity, and confidentiality for the verifier’s private key used. The scheme can resist replay attacks effectively due to the construction of warrant. The scheme based on random oracles is EUF-ACMA to be against a stronger adversary in the enhanced attack model. Further, the IDEMR-DVPS scheme has the advantage of being suitable for telemedicine wireless sensor networks applications.

The IDEMR-DVPS scheme ignoring pair computing will be the next step because pair operation costs much more than scalar multiplication operation. Designing an MR-DVPS scheme in the standard model is also an open issue.

### Data Availability

The simulation experiment data used to support the findings of this study are available from the corresponding author upon request.

### Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

### Acknowledgments

This work was supported in part by the National Social Science Fund of China (Grant No. 21XTQ015) and the Natural Science Foundation of Fujian Province of China (Grant No. 2020J01814).

### References

[1] S. Hussain, I. Ullah, H. Khattak, M. A. Khan, C. M. Chen, and 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, article 102625, 2021.

[2] L. Dong, W. Wu, Q. Guo, M. N. Satpute, T. Znati, and D. Z. Du, "Reliability-aware offloading and allocation in multilevel edge computing system," IEEE Transactions on Reliability, vol. 70, no. 1, pp. 200–211, 2021.

[3] W. Shu, K. Cai, and N. Xiong, "Research on strong agile response task scheduling optimization enhancement with optimal resource usage in green cloud computing," Future Generation Computer Systems, vol. 124, pp. 12–20, 2020.

[4] M. Zhang, D. Zhang, S. Fu, P. Kujala, and S. Hirdarisi, "A predictive analytics method for maritime traffic flow complexity estimation in inland waterways," Reliability Engineering and System Safety, vol. 220, article 108317, 2022.

[5] H. Rong, Z. Wang, H. Jiang, X. Zhu, and F. Zeng, "Energy-aware clustering and routing in infrastructure failure areas with D2D communication," IEEE Internet of Things Journal, vol. 6, no. 5, pp. 8645–8657, 2019.

[6] H. Ng, M. Sim, and C. Tan, "Security issues of wireless sensor networks in healthcare applications," BT Technology Journal, vol. 24, no. 2, pp. 138–144, 2006.

[7] M. Mambo, K. Usuda, and E. Okamoto, "Proxy signatures: delegation of the power to sign messages," IEICE Transactions on Fundamentals of Electronics, Communications and Computer Science, vol. 79, no. 9, pp. 1338–1354, 1996.

[8] L. He, J. Ma, L. Shen, and D. Wei, "Certificateless designated verifier proxy signature scheme for unmanned aerial vehicle networks," Science China Information Sciences, vol. 64, no. 1, 2021.

[9] M. Zheng, K. Xue, S. Li, and N. Yu, "A practical quantum designated verifier signature scheme for E-voting applications," Quantum Information Processing, vol. 20, no. 7, pp. 1–22, 2021.

[10] J. Wei, G. Yang, and Y. Mu, "Designated verifier proxy signature for deniable and anonymous wireless communications," Wireless Personal Communications, vol. 97, no. 2, pp. 3017–3030, 2017.

[11] W. M. Shi, S. Wang, Y. M. Wang, Y. H. Zhou, and Y. G. Yang, "A scheme on converting quantum deniable authentication into universal quantum designated verifier signature," Optik, vol. 190, pp. 10–20, 2019.

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

[13] P. Thorncharoensri, W. Susilo, and J. Baek, "Aggregateable certificateless designated verifier signature," IEEE Access, vol. 8, pp. 95019–95031, 2020.

[14] L. Shen, J. Ma, X. Liu, F. Wei, and M. Miao, "A secure and efficient ID-based aggregate signature scheme for wireless sensor networks," IEEE Internet of Things Journal, vol. 4, no. 2, pp. 546–554, 2017.

[15] K. A. Shim, "Short designated verifier proxy signatures," Computers and Electrical Engineering, vol. 37, no. 2, pp. 180–186, 2011.

[16] H. Y. Lin, T. S. Wu, and S. K. Huang, "An efficient strong designated verifier proxy signature scheme for electronic commerce," Journal of Information Science and Engineering, vol. 28, no. 4, pp. 771–785, 2012.

[17] I. K. Verma, B. B. Singh, and H. Singh, "Bandwidth efficient designated verifier proxy signature scheme for healthcare wireless sensor networks," Ad Hoc Networks, vol. 81, no. 12, pp. 100–108, 2018.

[18] X. Hu, W. Tan, H. Xu, and J. Wang, "Short and provably secure designated verifier proxy signature scheme," IET Information Security, vol. 10, no. 2, pp. 69–79, 2016.
[19] G. K. Verma, B. Singh, and H. Singh, "Provably secure message recovery proxy signature scheme for wireless sensor networks in e-healthcare," *Wireless Personal Communications*, vol. 99, no. 1, pp. 539–554, 2018.

[20] R. Parvin, B. Mehdi, D. Mohammad, and S. Willy, "Universal designated verifier signature scheme with non-delegatability in the standard model," *Information Sciences*, vol. 479, pp. 321–334, 2019.

[21] B. Kang, C. Boyd, and E. Dawson, "Identity-based strong designated verifier signature schemes: attacks and new construction," *Computers and Electrical Engineering*, vol. 35, no. 1, pp. 49–53, 2009.