Hindawi
Security and Communication Networks
Volume 2022, Article ID 8995704, 9 pages
https://doi.org/10.1155/2022/8995704

Research Article

Lattice-Based Self-Enhancement Authorized Accessible Privacy Authentication for Cyber-Physical Systems

Jinhui Liu,[1,2] **Yong Yu**,[3] **Houzhen Wang**,[4] **and Huanguo Zhang**[4]

[1]*School of Cyber Security, Northwestern Polytechnical University, Xi'an 710072, China*
[2]*Research & Development Institute of Northwestern Polytechnical University, Shenzhen 518057, China*
[3]*School of Cyber Security, Xi'an University of Posts and Telecommunications, Xi'an 710072, China*
[4]*School of Cyber Science and Engineering, Wuhan University, Wuhan 430072, China*

Correspondence should be addressed to Yong Yu; yuyongxy@163.com

Received 24 September 2021; Accepted 14 December 2021; Published 9 February 2022

Academic Editor: Ding Wang

Copyright © 2022 Jinhui Liu et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Healthcare cyber-physical system significantly facilitates healthcare services and patient treatment effectiveness by analyzing patients' health information data conveniently. Nevertheless, it also develops the threats to the confidentiality of health information, patients' privacy, and decidability of medical disputes. And, with the advances of quantum computing technology, most existing anonymous authentication schemes are becoming a growing threat to traditional cryptosystems. To address these problems, for healthcare cyber-physical systems, we propose a new lattice-based self-enhancement authorized accessible privacy authentication scheme by using a strong designated verifier double-authentication-preventing signature technique, called SEAPA. The SEAPA achieves three security and privacy requirements including unforgeability, anonymity for patients' information, and self-enhancement for patients themselves. A detailed security proof shows our proposal achieves those required security goals. Finally, our construction is demonstrated by parameter analysis and performance evaluation to have reasonable efficiency.

1. Introduction

Cyber-physical system is an integration of computational resources, physical processes, and communication capabilities, which is a multidimensional complex system combined by sensors, embedded devices, and wireless links. The advances in medical sensors, cloud computing, Internet of things, and wireless sensor networks (WSN) have witnessed CPS a powerful candidate for healthcare applications [1–6]. For example, COVID-19 has been causing incalculable damage to human health, economy, and life, and it is worth noting that wireless medical sensor network plays an important role in China's activity in resisting COVID-19. To provide a more convenient service and healthcare environment, a healthcare cyber-physical system (HCPS) is proposed [1]. Taking a patient at anywhere as an example, his privacy information can be collected by various sensors and then it can be sent to a third party cloud server. At the same time, doctors in a hospital can monitor the patient's physical condition and give some prescriptions or suggestions. Although each aspect of HCPS has made a great progress, security and privacy of patients' personal health information in HCPS have always been in the spotlight.

In a general HCPS system model, there occur components, including the medical sensor node of the patient, data sink which can collect patient's privacy information, and healthcare centers which have different hospitals, databases, and doctors. The system model of the healthcare cyber-physical system is shown in Figure 1. It has advantages of remote consultation system and mobile senor system. On the one hand, the privacy information of patients can be collected in data sink and uploaded to database in corresponding hospitals. On the other hand, multiple remote doctors can provide some timely and accurate medical services by analyzing patients' physiological data.

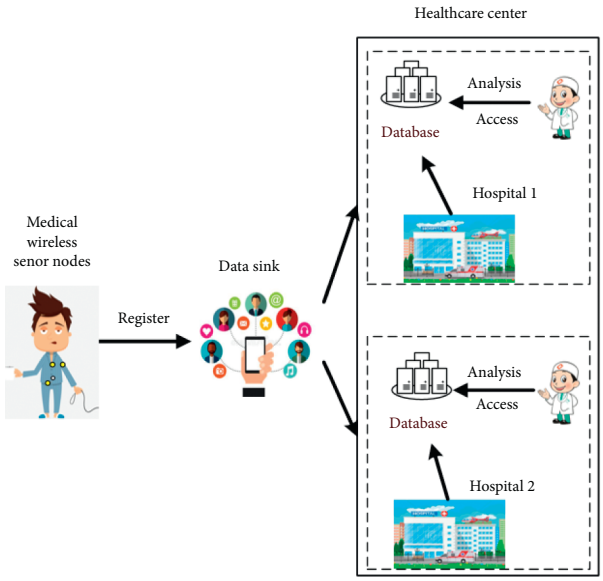

Figure 1: A system model of HCPS.

Although the HCPS system model provides convenience for the patients' treatment, it still faces some defects and potential treatments. For instance, in our daily life, there exist some misbehavior patients who want to see a doctor and do not want doctors to know her (or his) disease characteristics completely. The patient tells some ambiguous assertion to two kinds of authorized physicians, so she has to sign a pair of colliding messages with the same personal information and some different assertions. If there exist some medical disputes between them, the patient's misbehavior can be found. At present, all related digital signatures cannot provide a method to solve this problem and thus, we have to use another technique called double-authentication-preventing signature.

In addition, "Sycamore" quantum computer from the United States and the "Nine Chapter" quantum computer designed by China have been an important milestone. Since classical cryptographic protocols in HCPS will be broken by malicious adversary using quantum computers, private information of patients used to diagnose disease will be let out, which will result in loss of property and life. Lattice-based signatures have two kinds of advantages. One is that the hardness of some average-case lattice hard problems is equivalent to that of NP hard problem; the other is that lattice-based signatures have high efficiency, because it is based on operations between matrix additions and multiplications.

To realize these issues above, a novel privacy-preserving model for HCPS is established to allow patients to authorize privileges to different kinds of physicians located in the healthcare centers. Based on the model above, a self-enhancement postquantum secure privacy-preserving authentication scheme (SEAPA for short) in HCPS is proposed and it satisfies security requirements for patients. If the patient misbehaves, he (or she) will be punished by extracting his (or her) private keys. A rigorous security proof is shown that our proposed scheme is secure under the assumption of computational shortest integer solution problem in the random oracle model. Security proof and performance evaluation show that our scheme has reasonable efficiency for real applications.

2. Related Work

Digital signatures that provide message integrity, message authenticity, and nonrepudiation are publicly verifiable. However, in the HCPS model, the signed messages may infer signer's health information which reflects emotions and life of patients. In our daily life, if these signatures of messages are publicly verified, it will reveal the patients' personal health information and make some troubles for the patient. To solve these issues, Jakobsson et al. proposed an idea of designated verifier signature (DVS) that it convinces one, and only one (the designated verifier), to prove the validity of a signature [7]. Since the proposed DVS cannot resist an adversary to get the signature before it is obtained by the designated verifier, Jakobsson et al. also proposed a strong designated verifier signature (SDVS) [7]. As building blocks, DVSs are widely used in privacy-preserving security protocols such as cloud computing [8, 9], big data [10], Internet of things [11, 12], electronic voting systems [13, 14], and healthcare information systems [15, 16].

A series of designated verifier signatures with particular functions were proposed [17–25]. For example, to solve the key management problem, Huang et al. proposed an identity-based SDVS [26]. To solve the key-escrow problem of identity-based SDVS, Chen et al. proposed a certificateless SDVS with nondelegatability [22]. In recent years, He et al. proposed a certificateless designated verifier proxy signature scheme for unmanned aerial vehicle networks [27]. Zheng et al. presented a practical quantum designated verifier signature scheme for E-voting applications [28]. However, those properties may not be desirable. Consider such a scenario that a patient wants to see a doctor, while in our daily life, there exist many misbehaved patients who do not want others to know her (or his) disease characteristics completely. The patient tells some ambiguous assertion to two kinds of authorized physicians, so he/she has to sign a pair of colliding messages with the same personal information and some different assertions. If there exist some medical disputes between them, the patient's misbehavior can be found.

There are three categories in our proposed HCPS including directly authorized physicians, indirectly authorized physicians, and unauthorized physicians. By a new designated verifier signature called a designated verifier double-authentication-preventing signature (DVDAPS), which is derived from a double-authentication-preventing signature (DAPS) and a designated verifier signature (DVS), it realizes three different privacy-preserving requirements. DVDAPS can be deterrable (or punishable) by extracting the patients' secret keys of a signature on colliding messages if there exists a dispute. If patients' secret keys are extracted, their personal health information will be revealed to anyone. The DVDAPS can be considered as an attack algorithm or as a self-enhancement digital signature scheme.

2.1. Motivations. In practice, a signer may maliciously sign the messages twice to spread inappropriate contents or even sell patents more than once to gain illegal profits. Such actions must be punished as the actions impact the security, reputation, and robustness of the entire system. However, to the best of our knowledge, current digital signatures cannot provide the property of punishability. To address this issue, a double-authentication-preventing signature (DAPS for short) can be used to realize the requirement with deterrability. However, one cannot employ the existing general DAPS to solve the confidentiality and identity privacy of patients' personal health information in HCPS.

2.2. Contributions. In this paper, we give an affirmative answer to the above problem by introducing the first formal treatment for deterrability. We present a new deterrable digital signature, which is proven secure under a standard assumption on lattice, and then based on it, we realize a practical construction of DVDAPS in SEAPA. The major contributions of the paper are three-fold. Firstly, we give a formal definition of DVDAPS and propose the notions of unforgeability, anonymity, and self-enhancement in presence of attacks. Secondly, DVDAPS serves as the fundamental building blocks to offer the properties of privacy and deterrability simultaneously. To instantiate an efficient construction, we propose a secure construction under the assumption of lattice hard problems. Finally, we provide a concrete construction of SEAPA with performance evaluation.

2.3. Organization. In this paper, we propose a lattice-based self-enhancement authorized accessible privacy authentication scheme for HCPS. First, we introduce some notions, cryptographic primitives, and a security model of HCPS used in this paper. Second, we establish an authorized accessible privacy model for HCPS. Third, we present a concrete lattice-based privacy-preserving authentication scheme with properties of completeness, unforgeability, nontransferability, and extractability. Finally, we analyze our proposal from aspects of security and parameter settings.

3. Preliminaries

3.1. Notations. For a set $\mathcal{S}$, $a \leftarrow \mathcal{S}$ indicates that a is selected randomly from the set $\mathcal{S}$.

Ring is $\mathcal{R} = \mathbb{Z}[x]/(x^n + 1)$.

Column vector $\mathbf{a} = \begin{pmatrix} a_1 \\ \vdots \\ a_k \end{pmatrix}$ could be represented as $[a_1; \ldots; a_k]$.

$\|a\|_1 = \sum_{i=0}^{n-1} |a_i|$, $\|a\| = \sqrt{\sum_{i=0}^{n-1} |a_i^2|}$, and $\|a\|_\infty = \max_i |a_i|$.

For a full-rank integer lattice $\wedge$, the discrete distribution is

$$D_{\wedge,\mathbf{c},\sigma} = \frac{e^{-\|\mathbf{v}-\mathbf{c}\|^2/2\sigma^2}}{\sum_{w\in\Lambda} -\|\mathbf{v}-\mathbf{c}\|^2/2\sigma^2}. \quad (1)$$

Definition 1 (R-SIS$_{q,\beta,m}$). Given m uniform elements $a_i \in R_q$ at random and let $\mathbf{a} = (a_1, \ldots, a_m) \in R_q^m$, find out a nonzero vector $\mathbf{z} \in R^m$ with norm $\|\mathbf{z}\| \le \beta$ such that

$$\mathbf{a} \cdot \mathbf{z} = 0 \in R_q. \quad (2)$$

Note that in Ring-SIS, each $a_i \in R_q$ corresponds to n-related vectors $\mathbf{a}_i \in \mathbb{Z}_q^n$ in SIS, where n is the degree of R over $\mathbb{Z}$. Each $z_i \in R$ of a Ring-SIS solution corresponds to a block of n integers. That is to say, $\mathbf{a} \in \mathbb{Z}_q^{m\times m}$ and $\mathbf{z} \in \mathbb{Z}^{m\times m}$.

3.2. Ring-SIS Signature Scheme. Lyubashevsky's signature scheme is given as follows [29].

Secret key: $\mathbf{S} \leftarrow \{-d, \ldots, d\}^{m\times m}$

Public key: $\mathbf{A} \leftarrow Z_q^{m\times m}$, $\mathbf{T} \leftarrow \mathbf{AS}$ and H_1: $\{0,1\}^* \longrightarrow \{\mathbf{v}: \mathbf{v} \in \{-1,0,1\}^m, \|\mathbf{v}\|_1 \le \kappa\}$

Sign: given a message μ, compute the following:

(i) $\mathbf{y} \leftarrow D_\sigma^m$

(ii) $\mathbf{c} \leftarrow H_1(\mathbf{Ay}, \mu)$

(iii) $\mathbf{z} \leftarrow \mathbf{Sc} + \mathbf{y}$

(iv) Output $(\mathbf{z}, \mathbf{c})$ with probability $\min(D_\sigma^m(\mathbf{z})/\mathrm{MD}_{Sc,\sigma}^m(\mathbf{z}), 1)$, where $M = O(1)$

Verify

(i) Accept iff $\|\mathbf{z}\| \le 2\sigma\sqrt{m}$ and $\mathbf{c} = H_1(\mathbf{Az} - \mathbf{Tc}, \mu)$

We transform the signature scheme above to Ring-SIS signature scheme as follows:

Secret key: $\mathbf{s} \leftarrow R_{-d,d}^m$, where let $R_{-d,d}^m$ be $\{-d, \ldots, 0, \ldots, d\}^{m\times m}$

Public key: $\mathbf{a} \leftarrow R_q^m$, $\mathbf{t} \leftarrow \mathbf{as}$ and H: $\{0,1\}^* \longrightarrow \{\mathbf{v}: \mathbf{v} \in R_{-1,1}, \|\mathbf{v}\|_1 \le \kappa\}$

Sign: given a message μ, compute the following

(i) $\mathbf{y} \leftarrow D_\sigma^m$

(ii) $\mathbf{c} \leftarrow H(\mathbf{ay}, \mu)$

(iii) $\mathbf{z} \leftarrow \mathbf{sc} + \mathbf{y}$

(iv) Output $(\mathbf{z}, \mathbf{c})$ with probability $\min(D_\sigma^m(\mathbf{z})/\mathrm{MD}_{Sc,\sigma}^m(\mathbf{z}), 1)$, where $M = O(1)$

Verify

(i) Accept iff $\|\mathbf{z}\| \le 2\sigma\sqrt{m}$ and $\mathbf{c} = H(\mathbf{az} - \mathbf{tc}, \mu)$

3.3. System Model Description. Our system model is illustrated in Figure 2, which mainly includes three parts as follows. Healthcare providers are equipped with cloud servers, wireless transmission networks, and body area networks. The health information of a patient is transmitted to two different healthcare providers to different kinds of authorized physicians for accessing and making some medical treatments, respectively. There are two healthcare centers with healthcare providers A and B and the medical research institutions C, where Dr. Alice, Dr. Bob, and Dr. Eve are working in Hospital 1. Each of them have their cloud server. If a patient registers at Hospital 1, his (or her) health information will stored in the cloud server of the Hospital 1, while his health information will

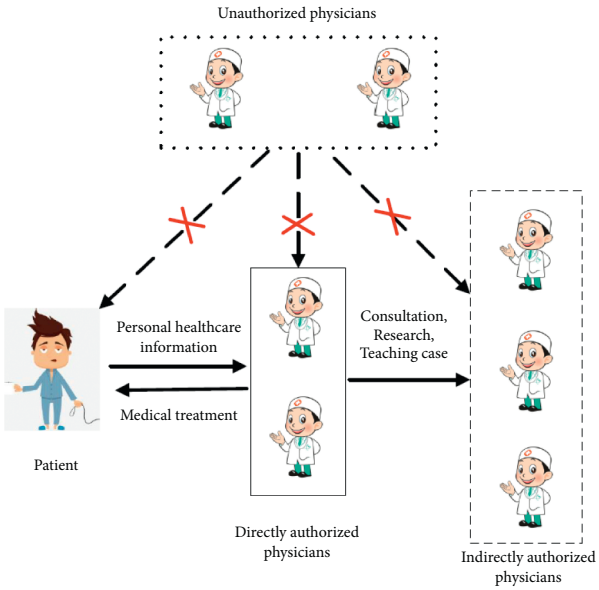

FIGURE 2: Our constructed HCPS system model.

not be seen in Hospital 2 and Dr. Alice is one of his authorized physicians. Besides, for other purposes (e.g., research and medical consultation) in cooperation with Hospital 2 and research institutions C, Dr. Alice needs to generate two indistinguishable transcript simulations to Hospital 2 and research institutions C. In some cases, the patient may register at other hospitals with ambiguous assertion about his or her healthcare information; if there exists a medical dispute, the patient can traced.

Remark 1. If the patient does not register twice, our system model is correct directly and the purpose of the twice registration is to solve some medical disputes.

4. Authorized Accessible Privacy Model

In this section, we introduce an authorized accessible privacy model for HCPS which includes a strong designated verifier double-authentication-preventing signature (SDVDAPS for short) and the corresponding security models.

4.1. Strong Designated Verifier Double-Authentication-Preventing Signatures. We provide a self-enhancement privacy-preserving authentication scheme based on a SDVDAPS to satisfy three security and privacy requirements in healthcare cyber-physical systems. Our SEAPA algorithm is described as follows:

KeyGen: on inputting public parameters Param and security parameter κ, the algorithm outputs public-private keys (PK_A, SK_A) of a patient (Alice, for example) and public-private keys (PK_B, SK_B) and (PK_C, SK_C) of two designated physicians (Bob and Eve, for example) in two different hospitals.

DVDAPSig: on inputting Alice's colliding personal healthcare information (m_0, p_1) and (m_0, p_2), Alice's secret key SK_A, Bob's public key SK_B, and Eve's public key PK_C, the algorithm generates a signature σ_1 on (m_0, p_1) by using SK_A and PK_B and a signature σ_2 on (m_0, p_2) by using SK_A and PK_C.

DVDAPVer: on inputting Alice's colliding personal healthcare information (m_0, p_1) and (m_0, p_2), (σ_1, σ_2), and PK_A, SK_B, and SK_C, the algorithm outputs 0 which means reject or outputs 1 which means accept.

Sim: the algorithm generates a signature on (m_0, p_1) by using (PK_A, SK_B, PK_B) of an authorized physician Bob in Hospital 1 and a signature on (m_0, p_2) by using (PK_A, SK_C, PK_C) of an authorized physician Bob in other hospitals which are indistinguishable from those produced by DVDAPSig $((m_0, p_1), SK_A, PK_B)$ and DVDAPSig $((m_0, p_2), SK_A, PK_C)$, respectively.

Extract: on inputting Alice's colliding personal healthcare information (m_0, p_1) and (m_0, p_2) and a valid signature pair (σ_1, σ_2), the algorithm could extract Alice's secret key SK_A.

Remark 2. If the patient does not register twice, the SDVDAPS will degenerate into a general designated verifier signature (DVS for short). Hence, we can get that our construction is correct directly:

Correctness. We need the SEAPA to be correct which means that any honestly computed signature can be verified by directly authorized physicians. That is to say, for any $\kappa > 0$, $(PK_i, SK_i) \leftarrow$ KeyGen (1^κ) for $i = A, B, C$ and $(m_0, p_i) \in \mathcal{M}$ for $i = 1, 2$, for $\delta_1 \leftarrow$ DVDAPSig $((m_0, p_1), SK_A, PK_B)$ and $\delta_2 \leftarrow$ DVDAPSig $((m_0, p_2), SK_A, PK_C)$, it holds that

$$\begin{aligned} &\Pr[\text{DVDAPVer}((m_0, p_1), \sigma_1, PK_A, SK_B) = 1] = 1, \\ &\Pr[\text{DVDAPVer}((m_0, p_2), \sigma_2, PK_A, SK_C) = 1] = 1. \end{aligned} \tag{3}$$

4.2. Security Models

4.2.1. Unforgeability. In the DVDAPS, unforgeability under chosen message attack is a basic security property, which means it is infeasible to produce a valid signature for any adversary who does not know secret keys of the signer. Then, we provide a formal description of existential unforgeability of the SEAPA.

(1) Definition 1 (Unforgeability). Our construction SEAPA shows unforgeability under chosen message attack if any adversary $\mathcal{A}$ could not win the following game.

$\mathcal{C}$ constructs public/private key pairs $(PK_i, SK_i) \leftarrow$ Key Gen (1^κ) for $i = A, B, C$, where κ is a security parameter and sends (PK_A, SK_B) and (PK_A, SK_C) to $\mathcal{A}$, where A is the patient and B and C are corresponding authorized physicians in different hospitals, respectively.

$\mathcal{A}$ queries the signing oracle q_{s_1} times for the message (m_0, p_{i1}) and q_{s_2} times for the message (m_0, p_{i2}), respectively.

$\mathcal{C}$ answers $\mathcal{A}$'s queries by

$$\sigma_{i1} = \mathrm{DVDAPSign}\left(\mathrm{PK}_A, \mathrm{SK}_A, \mathrm{PK}_B, (m_0, p_{i1})\right), \quad (4)$$

and

$$\sigma_{i2} = \mathrm{DVDAPSign}\left(\mathrm{PK}_A, \mathrm{SK}_A, \mathrm{PK}_C, (m_0, p_{i2})\right), \quad (5)$$

respectively.

Finally, $\mathscr{A}$ is successful if he outputs two new signatures σ_1^* and σ_2^* for message (m_0, μ^*).

For running the above games in time t, the SEAPA shows (t, ε) unforgeability (EUF-CMA secure) if there exists a negligible function $\varepsilon(\kappa) > 0$ such that the following equation holds:

$$\Pr\left[\mathrm{DVDAPVer}_{\mathrm{SEAPA},\mathscr{A}}^{\mathrm{EUF-CMA}}\left((m_0, \mu_1^*), (m_0, \mu_2^*), \sigma_1^*, \sigma_2^*\right) = 1\right] \le \varepsilon(\kappa). \quad (6)$$

4.2.2. Anonymity for the Patient. Only the authorized physicians could generate an indistinguishable signature from the one that could be produced by the signer.

(2). Definition 2 (Anonymity for the Patient). The SEAPA shows anonymity for the patient if the game is successful between a PPT adversary $\mathscr{A}$ and a distinguisher $\mathscr{D}$ as follows.

$\mathscr{C}$ constructs public/private key pairs $(\mathrm{PK}_i, \mathrm{SK}_i) \leftarrow \mathrm{Key\ Gen}(1^\kappa)$ for $i = A, B, C$, where κ is a security parameter and sends public key pairs $(\mathrm{PK}_A, \mathrm{PK}_B)$ and $(\mathrm{PK}_A, \mathrm{PK}_C)$ to $\mathscr{D}$, where A is the patient and B and C are corresponding physicians in different hospitals, respectively.

$\mathscr{D}$ queries the signing oracle q_{s_1} times for the message (m_0, p_{i1}) and q_{s_2} times for the message (m_0, p_{i2}), respectively, where $q_s = \max\{q_{s_1}, q_{s_2}\}$.

$\mathscr{C}$ answers $\mathscr{A}$'s query by

$$\sigma_{i1} = \mathrm{DVDAPSign}\left(\mathrm{PK}_A, \mathrm{SK}_A, \mathrm{PK}_B, (m_0, p_{i1})\right), \quad (7)$$

$$\sigma_{i2} = \mathrm{DVDAPSign}\left(\mathrm{PK}_A, \mathrm{SK}_A, \mathrm{PK}_C, (m_0, p_{i2})\right), \quad (8)$$

respectively.

$\mathscr{D}$ makes queries on new messages (m_0, p_1^*) and (m_0, p_2^*) to obtain corresponding challenging signatures σ_1^* and σ_2^*.

$\mathscr{C}$ tosses a coin $b \in \{0, 1\}$. If $b = 0$, $\mathscr{C}$ runs DVDAPSign algorithm and returns corresponding signatures:

$$\sigma_1^* = \mathrm{DVDAPSign}\left(\mathrm{PK}_A, \mathrm{SK}_A, \mathrm{PK}_B, (m_0, p_1^*)\right), \quad (9)$$

$$\sigma_2^* = \mathrm{DVDAPSign}\left(\mathrm{PK}_A, \mathrm{SK}_A, \mathrm{PK}_C, (m_0, p_2^*)\right), \quad (10)$$

Else, $\mathscr{C}$ runs Sim algorithm and returns

$$\sigma_1^* = \mathrm{Sim}\left(\mathrm{PK}_A, \mathrm{PK}_B, \mathrm{SK}_A, (m_0, p_1^*)\right), \quad (11)$$

$$\sigma_2^* = \mathrm{Sim}\left(\mathrm{PK}_A, \mathrm{PK}_C, \mathrm{SK}_A, (m_0, p_2^*)\right), \quad (12)$$

respectively.

$\mathscr{D}$ is able to query other new messages except for (m_0, p_1^*) and (m_0, p_2^*) after receiving challenging signatures σ_1^* and σ_2^*.

Finally, $\mathscr{D}$ is successful if he outputs $b' = b$.

For running the above games in time t, the construction SEAPA shows (t, q_s) anonymity for the patient against a chosen message distinguisher if there exists a negligible function $\varepsilon(\kappa) > 0$ such that the following equation holds:

$$\mathrm{Adv}_{\mathrm{DVDAPS},\mathscr{D}}^{\mathrm{NT-CMA}} = \left|\Pr\left[b' = b\right] - \frac{1}{2}\right| \le \varepsilon(\kappa). \quad (13)$$

The security model of anonymity for the patient means that the probability of the signature produced by the DVDAPSign algorithm and the Sim algorithm is the same.

Extractability (or punishability) could be interpreted as Alice's secret keys can be extracted if there exists a medical dispute between Bob and Eve. To some extent, extractability can be considered as a self-enhancement mechanism for the patient.

(3). Definition 3 (Self-Enhancement for the Patient). A SEAPA provides self-enhancement for the patient, if for any PPT adversary $\mathscr{A}$, there exists a negligible function $\varepsilon(\kappa)$ such that the following probability is negligible:

$$\Pr\left[\begin{array}{l}(\mathrm{SK}_i, \mathrm{PK}_i) \leftarrow \mathrm{Key\ Gen}(1^\kappa)\\ \text{for } i = A, B, C\\ ((m_0, p_1), \sigma_1) \leftarrow \mathscr{A}(\mathrm{PK}_A, \mathrm{SK}_A, \mathrm{PK}_B),\\ ((m_0, p_2), \sigma_2) \leftarrow \mathscr{A}(\mathrm{PK}_A, \mathrm{SK}_A, \mathrm{PK}_C)\\ \mathrm{SK}' \neq \mathrm{SK}\end{array}\right. \quad (14)$$

$$\left.\begin{array}{l}p_1 \neq p_2 \wedge p_1 \neq 0, p_2 \neq 0 \wedge\\ \mathrm{SK}' \leftarrow \mathrm{Extract}(m_0, p_1, p_2, \sigma_1, \sigma_2)\\ \wedge \mathrm{DVDAPVer}(m_0, p_1, \delta_1, \mathrm{PK}_A, \mathrm{SK}_B) = 1\\ \wedge \mathrm{DVDAPVer}(m_0, p_2, \delta_2, \mathrm{PK}_A, \mathrm{SK}_C) = 1\end{array}\right] \le \varepsilon(\kappa).$$

5. Our Lattice-Based SEAPA Construction

In this section, we will introduce our lattice-based SEAPA construction in detail. Our protocol consists of the following five phases.

5.1. KeyGen. $s_i \leftarrow R_{-d,d}^m$ for the patient A (name Alice) and directly authorized physicians B (name Bob) and C (name Eve) in different hospitals:

(1) $\mathbf{a} \leftarrow R_q^m$, $\mathbf{t} \leftarrow \mathbf{as}$, and cryptographically collision-resistant hash functions $H: \{0,1\}^* \longrightarrow \{v: \ v \in R_{-1,1}, \|v\|_1 \le \iota\}$.

(2) Compute $\mathbf{y}_A = \mathbf{a}^T\mathbf{s}_A, \mathbf{y}_B = \mathbf{as}_B$, and $\mathbf{y}_C = \mathbf{as}_C$. Let $(\mathbf{a}, H, d, m, R, \iota)$ be public parameters.

(3) Alice's public/private pair is $(\mathbf{y}_A, \mathbf{s}_A)$, Bob's public/private pair is $(\mathbf{y}_B, \mathbf{s}_B)$, and Eve's public/private pair is $(\mathbf{y}_C, \mathbf{s}_C)$.

5.2. DVDAPSig. Given the colliding patient's personal health information (m_0, p_1) and (m_0, p_2) which can only be verified and recovered by B and C, respectively, Alice computes a signature σ_1 on (m_0, p_1) by using $\mathbf{s}_A, \mathbf{y}_B$ and a signature σ_2 on (m_0, p_2) by using $\mathbf{s}_A, \mathbf{y}_C$ in the following:

(1) $\mathbf{r} \leftarrow D_\sigma^m$

(2) if $\mathbf{r}$ is irreversible, goto step 1

(3) $\mathbf{y} \leftarrow D_\sigma^m$

(4) $c_1 \leftarrow H(m_0 \mathbf{y}_B^T \mathbf{y}, p_1)$

(5) $c_2 \leftarrow H(m_0 \mathbf{y}_C^T \mathbf{y}, p_2)$

(6) For $i = 1, 2$, compute

(7) $\mathbf{z}_i \leftarrow \mathbf{s}_A c_i + m_0 \mathbf{y} \mathbf{r}^{-1}$

(8) Output $(\mathbf{z}_i, c_i, \mathbf{r})$ with probability $\min(D_\sigma^m(\mathbf{z}_i)/\mathrm{MD}_{sc_i,\sigma}^m(\mathbf{z}_i), 1)$, where $M_i = O(1)$ and $M = \max\{M_1, M_2\}$

(9) Then, Alice sends $\sigma_1 = (\mathbf{z}_1, c_1, \mathbf{r})$ to Bob and sends $\sigma_2 = (\mathbf{z}_2, c_2, \mathbf{r})$ to Eve

5.3. DVDAPVer. After receiving signatures, physicians Bob and Eve working in the different local healthcare providers do the following things respectively:

(i) Bob accepts iff $\|\mathbf{z}_1\| \le 2\sigma\sqrt{m}$ and $c_1 = H(\mathbf{s}_B^T(\mathbf{a}\mathbf{z}_1 - \mathbf{y}_A c_1)\mathbf{r}, p_1)$

(ii) Eve accepts iff $\|\mathbf{z}_2\| \le 2\sigma\sqrt{m}$ and $c_2 = H(\mathbf{s}_C^T(\mathbf{a}\mathbf{z}_2 - \mathbf{y}_A c_2)\mathbf{r}, p_2)$

5.4. Sim

(i) Since $\mathbf{s}_B^T(\mathbf{a}\mathbf{z}_1\mathbf{r} - \mathbf{y}_A c_1 r) = \mathbf{s}_B^T(\mathbf{a}\mathbf{z}_1' - s_A c_1')$, Bob computes simulated signature $\sigma_1' = (\mathbf{z}_1', c_1', \mathbf{r})$, where $\mathbf{z}_1' = \mathbf{z}_1\mathbf{r}, c_1' = c_1\mathbf{r}$

(ii) Since $\mathbf{s}_C^T(\mathbf{a}\mathbf{z}_1\mathbf{r} - \mathbf{y}_A c_1 r) = \mathbf{s}_C^T(\mathbf{a}\mathbf{z}_2' - \mathbf{y}_A c_2')$, Eve computes simulated signature $\sigma_2' = (\mathbf{z}_2', c_2', \mathbf{r})$

5.5. Extract

(i) When there exists a medical dispute between authorized physicians and the patient, they provide their valid signature $(\mathbf{z}_1, c_1, \mathbf{r})$ and $(\mathbf{z}_2, c_2, \mathbf{r})$ to the public and anyone can compute the patient's secret key $\mathbf{s}_A = \mathbf{z}_1 - \mathbf{z}_2 / c_1 - c_2$.

6. Security Proof

In this section, we use the random oracle model to prove the security of our proposed scheme based on the security model of SEAPA.

Theorem 1. *The proposed SEAPA is correct.*

Proof. For $i = B, j = 1$ and $i = C, j = 2$, the correctness is given as follows:

$$\begin{aligned}
&\mathbf{s}_i^T\left(\mathbf{a}\mathbf{z}_j - \mathbf{y}_A c_j\right)\mathbf{r} \\
&= \mathbf{s}_i^T\left(\mathbf{a}\left(\mathbf{s}_A c_j + m_0 \mathbf{y}\mathbf{r}^{-1}\right) - \mathbf{y}_A c_j\right)\mathbf{r} \\
&= \left(\mathbf{s}_i^T \mathbf{a}\mathbf{s}_A c_j + m_0 \mathbf{s}_i^T \mathbf{a}\mathbf{y}\mathbf{r}^{-1} - \mathbf{s}_i^T \mathbf{a}\mathbf{y}_A c_j\right)\mathbf{r} \\
&= \mathbf{y}_i^T \mathbf{y} m_0.
\end{aligned} \tag{15}$$

Hence, it follows that

$$H\left(\mathbf{y}_B^T \mathbf{y} m_0, p_1\right) = c_1 = H\left(\mathbf{s}_B^T(\mathbf{a}\mathbf{z}_1 - \mathbf{y}_A c_1)\mathbf{r}, p_1\right), \tag{16}$$

$$H\left(\mathbf{y}_C^T \mathbf{y} m_0, p_2\right) = c_2 = H\left(\mathbf{s}_C^T(\mathbf{a}\mathbf{z}_2 - \mathbf{y}_A c_2)\mathbf{r}, p_2\right). \tag{17}$$

□

Theorem 2. *The proposed SEAPA is unforgeable against chosen message attack under the hardness of the Ring-SIS.*

Proof. Suppose that a PPT adversary $\mathscr{A}$ is able to produce a valid signature $\sigma^* = (\mathbf{z}_1^*, c_1^*, \mathbf{z}_2^*, c_2^*, \mathbf{r}^*)$. According to EUF-CMA game, σ^* can be correctly verified which means that $\mathscr{A}$ can compute the following equation.

For $i = B, j = 1$ and $i = C, j = 2$,

$$\begin{aligned}
&\mathbf{s}_i^T\left(\mathbf{a}\mathbf{z}_j^* - \mathbf{y}_A c_j^*\right)\mathbf{r}^* \mathbf{r}^{-*} - \mathbf{y}_i^T \mathbf{z}_j^* \\
&= -\mathbf{s}_i^T \mathbf{y}_A c_j^* \bmod q \\
&= -\mathbf{y}_i^T \mathbf{s}_A c_j^* \bmod q.
\end{aligned} \tag{18}$$

Let $\mathbf{X} = -\mathbf{y}_i^T \mathbf{s}_A c_j^* \bmod q$. If $\|\mathbf{s}_A c_j^*\| \le \beta$, $\mathscr{A}$ obtains a solution for Ring-SIS problem.

If an adversary $\mathscr{A}$ could obtain a valid SEAPA signature by EUF-CMA game in time t, he can solve the Ring-SIS problem in polynomial time. Hence, we have

$$\begin{aligned}
&\Pr\left[\mathrm{DVDAPVer}_{\mathrm{SEAPA},\mathscr{A}}^{\mathrm{EUF-CMA}}((m_0, \mu_1^*), (m_0, \mu_2^*), \sigma_1^*, \sigma_2^*) = 1\right] \\
&= \Pr\left[\mathbf{X} = -\mathbf{y}_i^T \mathbf{s}_A c_j^* : \left\|\mathbf{s}_A c_j^*\right\| \le \beta\right] \le \varepsilon(\kappa).
\end{aligned} \tag{19}$$

□

Theorem 3. *The proposed SEAPA shows anonymity for the patient.*

Proof. According to the proposed scheme, anonymity for the patient means that any valid signature on a message produced by the Sim algorithm in SEAPA is indistinguishable from the signature produced by the DVDAPSign algorithm. That is to say, the probability of the signature produced by the two algorithms are the same.

Let $\overline{\sigma} = (\overline{\mathbf{z}}_1, \overline{c}_1, \overline{\mathbf{z}}_2, \overline{c}_2, \overline{\mathbf{r}})$ be a valid signature, and some signatures are chosen randomly from the set of DVDAPS. The probability of the signature $\sigma = (\mathbf{z}_1, c_1, \mathbf{r})$ produced by the DVDAPSign is given by

$$\Pr\left[\begin{array}{c}\mathbf{r}\leftarrow D_\sigma^m,\\ \mathbf{y}\leftarrow D_\sigma^m,\\ \overline{\sigma}=\sigma:\quad c_1\leftarrow H\left(m_0\mathbf{y}_B^T\mathbf{y},p_1\right)\\ \mathbf{z}_1\leftarrow\mathbf{s}_A c_1+m_0\mathbf{y}\mathbf{r}^{-1}\end{array}\right]=\frac{1}{\gamma^m\left(\gamma^m-1\right)}. \tag{20}$$

For randomly selected $y'\leftarrow D_\sigma^m$, the signature $\sigma'=(\mathbf{z}_1',\nu,c_1',\mathbf{r})$ produced by the Sim is given by

$$\Pr\left[\begin{array}{c}\mathbf{z}_1',c_1'\leftarrow D_\sigma^m,\\ \overline{\sigma}=\sigma'\ :c_1\leftarrow H\left(\mathbf{s}_B^T\left(\mathbf{a}\mathbf{z}_1'-\mathbf{y}_A c_1'\right),p_1\right)\\ \mathbf{z}_1=\mathbf{z}_1'\mathbf{r}^{-1}\end{array}\right]=\frac{1}{\gamma^m\left(\gamma^m-1\right)}. \tag{21}$$

In a similar way,

$$\Pr\left[\begin{array}{c}\mathbf{r}\leftarrow D_\sigma^m,\\ \mathbf{y}\leftarrow D_\sigma^m,\\ \overline{\sigma}=\sigma:\quad c_2\leftarrow H\left(m_0\mathbf{y}_C^T\mathbf{y},p_2\right)\\ \mathbf{z}_2\leftarrow\mathbf{s}_A c_2+m_0\mathbf{y}\mathbf{r}^{-1}\end{array}\right], \tag{22}$$

$$\Pr\left[\begin{array}{c}\mathbf{z}_2',c_2'\leftarrow D_\sigma^m,\\ \overline{\sigma}=\sigma':\quad c_2\leftarrow H\left(\mathbf{s}_C^T\left(\mathbf{a}\mathbf{z}_2'-\mathbf{y}_A c_2'\right),p_2\right)\\ \mathbf{z}_2=\mathbf{z}_2'\mathbf{r}^{-1}\end{array}\right].$$

Therefore,

$$\mathrm{Adv}_{\mathrm{SEAPA},\mathscr{D}}=\left|\Pr\left[b'=b\right]-\frac{1}{2}\right|\le\varepsilon(\kappa). \tag{23}$$

That is, the proposed SEAPA scheme shows anonymity for the patient. □

Theorem 4. *The proposed SEAPA scheme shows self-enhancement for the patient.*

Proof. It is easy to verify the extractability from the algorithm Extract based on Theorem 1. So, if the signature private keys are important for her, she will not make some ambiguous assertions which means that there does not exist colliding personal health information (m_0, p_1) and (m_0, p_2); that is to say, $p_1 = p_2$. To some extent, there will not occur some medical disputes. Hence, our proposed scheme shows self-enhancement for the patient.

By going through the criteria of Wang et al., Hussain et al., and Bonneau et al. [30–32], we propose some major categories that our scheme satisfies as shown in Table 1, where "Must Have" category is related to providing robust security, "May or May Not Have" category is dealing with user experience, and "Nice to Have" category has one criterion related to user experience which is sound repairability while the other is related to security. Besides these criteria, our scheme also satisfies postquantum security. □

Table 1: Criterion categorization.

Criterion	Category
C1-No verifier table	Must have
C2-Password friendly	Must Have
C3-No password exposure	Must Have
C4-No smart card loss attack	Must Have
C5-Resistance to known attacks	Must Have
C7-Provision of key agreement	Must Have
C10-Mutual authentication	Must Have
C11-User anonymity	Must Have
C6-Sound repairability	Nice to Have
C12-Forward secrecy	Nice to Have
C8-No clock synchronization	Nice to Have
C9-Timely typo detection	May or May Not Have

Table 2: Parameter size in the SEAPA scheme.

n	512	512	1024
m	1024	1024	2048
q	2^{24}	2^{33}	8380417
d	1	31	1
k	1024	1024	2048
κ s.t. $2^\kappa\binom{n}{\kappa}\ge 2^{100}$	14	14	14
$\sigma\approx 12\cdot d\cdot\kappa\cdot\sqrt{m}$	5376	166656	5376
$M\approx\ \exp(12\ d\kappa\sqrt{m}/\sigma+(d\kappa\sqrt{m}/2\sigma)^2)$	2.72	2.72	2.72
Size of signature $\approx 2m\log(12\sigma)$ bits	33000	41100	82200
Size of secret key $\approx 2m^2\log(2\ d+1)$ bits	$2^{20.5}$	$2^{22.5}$	$2^{23.7}$
Size of public key $\approx 1/2m^2\log(q)$ bits	$2^{21.5}$	2^{22}	$2^{25.5}$

7. Concrete Parameters Analysis

7.1. Communication Cost. In our SEAPA scheme, we set up some parameters $q, n, m, \eta, \Phi, d, \beta$, and γ for postquantum computational security [33]. The security of our scheme is based on the hardness of the Ring-SIS$_{q,n,d,m,\beta}$ problem. In the scheme, we set $m = 2n$ and $4\ d\beta\ \le q$, and the Ring-SIS$_{q,n,d,m}$ problem can reduce to ℓ_2–Ring-SIS$_{q,n,d,m,\beta}$. The definition of its parameters are listed in Table 2.

From Table 2, we can see that the signature size of the SEAPA scheme is about 4 KB, 5 KB, and 10 KB for different parameters, respectively.

7.2. Computational Cost. We execute our algorithms on Intel Core i7-4710 processor with 12 GB memory and Ubuntu Linux operating system. Some important cryptographic operations are implemented with NFLlib, which is a NTT-based fast lattice library. By statistics, these important algorithm operations mainly consist of one polynomial addition, one polynomial multiplication, and one polynomial Gaussian. Since the implementation of any hash function is not included in NFLlib, we test the running time of the hash function by a HMAC based on SM3 algorithm. The execution time of each cryptographic operation is shown in Table 3.

We use KG, Sig, Ver, Sim, and Ext to represent the five algorithms KeyGen, DVDAPSig, DVDAPVer, Sim, and Extract, respectively. The degree of polynomial we choose is 8, 128, 1024, 8192, and 32768, and the corresponding size of

Table 3: The cryptographic operation time in the SEAPA scheme (microseconds).

n	q	m	Poly addition	Poly subtraction	Poly multiplication	Poly Gaussian	Hash function
8	60	16	0.00456	0.00250	0.00333	0.00243	0.105
128	14	216	0.00335	0.00230	0.00243	0.00262	0.1100
1024	60	2048	0.00248	0.00369	0.00227	0.00256	0.175
8192	124	16384	0.00454	0.00475	0.00652	0.00474	0.177
32768	124	65536	0.0120	0.0120	0.02678	0.0375	0.287

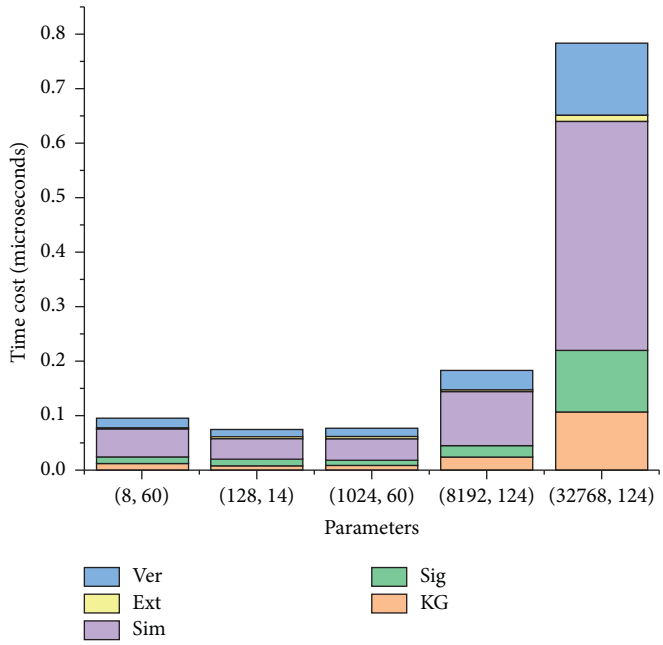

Figure 3: Time cost of each algorithm in SEAPA.

integer ring is 14 bits, 60 bits, 124 bits, and 124 bits. So the total running time of our algorithm for different parameters is about 0.096711 ms in keygen phase, 0.076315 ms in signature phase, 0.078821 ms in simulation phase, 0.184251 ms in extraction phase, and 0.784562 ms in verification phase. The execution result is depicted in Figure 3.

8. Conclusion and Future Work

In this paper, we presented an authorized accessible privacy model and provided a concept of the patient self-enhancement privacy-preserving authentication scheme. Our construction is derived from strong designated verifier signatures and double-authentication-preventing signatures based on lattice. Security proof shows that our construction satisfies different levels of security requirements in the HCPS system model. Concrete parameters analysis and performance evaluation demonstrated that our construction has reasonable efficiency for real applications. In future work, on the basis of lattice-based strong designated verifier signatures, we will provide some comparisons on the concrete parameters and the communication cost.

Data Availability

No data were used to support this study.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work was supported by the National Natural Science Foundation of China (61872229, 61802239, 62062019, and 62074131), Key Research and Development Program of Shaanxi Province (2020ZDLGY09-06, 2021ZDLGY06-04, and 2021ZDLGY05-01), Natural Science Basic Research Plan in Shaanxi Province of China (2019JQ-667 and 2020JQ-422), and Shenzhen Fundamental Research Program (20210317191843003).

References

[1] Y. Zhang, M. Qiu, C. W. Tsai, M. M. Hassan, and A. Alamri, "Health-CPS: healthcare cyber-physical system assisted by cloud and big data," *IEEE Systems Journal*, vol. 11, no. 1, pp. 88–95, 2015.

[2] J. Xu, L. Wei, W. Wu, A. Wang, Y. Zhang, and F. Zhou, "Privacy-preserving data integrity verification by using lightweight streaming authenticated data structures for healthcare cyber-physical system," *Future Generation Computer Systems*, vol. 108, pp. 1287–1296, 2020.

[3] S. Wang, H. Wang, J. Li et al., "A fast cp-abe system for cyber-physical security and privacy in mobile healthcare network," *IEEE Transactions on Industry Applications*, vol. 56, no. 4, pp. 4467–4477, 2020.

[4] R. Agarwal and M. Hussain, "Generic framework for privacy preservation in cyber-physical systems," in *Proceedings of the Progress in Advanced Computing and Intelligent Engineering*, pp. 257–266, Springer, Odisha, India, October 2021.

[5] H. Sedjelmaci, F. Guenab, S.-M. Senouci, H. Moustafa, J. Liu, and S. Han, "Cyber security based on artificial intelligence for cyber-physical systems," *IEEE Network*, vol. 34, no. 3, pp. 6-7, 2020.

[6] C. Kannan, M. Dakshinamoorthy, M. Ramachandran, R. Patan, H. Kalyanaraman, and A. Kumar, "Cryptography-based deep artificial structure for secure communication using IoT-enabled cyber-physical system," *IET Communications*, vol. 15, no. 6, pp. 771–779, 2021.

[7] M. Jakobsson, K. Sako, and R. Impagliazzo, "Designated verifier proofs and their applications," in *Proceedings of the Theory and Applications of Cryptographic Techniques*, vol. 143–154Berlin, Heidelberg, Springer, May 1996.

[8] L. Wei, H. Zhu, Z. Cao et al., "Security and privacy for storage and computation in cloud computing," *Information Sciences*, vol. 258, pp. 371–386, 2014.

[9] Y. Zhang, Q. Liu, C. Tang, and H. Tian, "A lattice-based designated verifier signature for cloud computing," *International Journal of High Performance Computing and Networking*, vol. 8, no. 2, pp. 135–143, 2015.

[10] S. Hou, X. Huang, J. K. Liu, J. Li, and L. Xu, "Universal designated verifier transitive signatures for graph-based big data," *Information Sciences*, vol. 318, pp. 144–156, 2015.

[11] X. D. Yang, L. K. Xiao, C. L. Chen, and C. F. Wang, "A strong designated verifier proxy re-signature scheme for IoT environments," *Symmetry*, vol. 10, no. 11, pp. 1486–1491, 2018.

[12] Y. Yu, Y. Ding, Y. Zhao et al., "LRCoin: leakage-resilient cryptocurrency based on bitcoin for data trading in IoT," *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 4702–4710, 2019.

[13] L. Zuo, N. Kumar, H. Tu, A. Singh, N. Chilamkurti, and S. Rho, "Detection and analysis of secure intelligent universal designated verifier signature scheme for electronic voting system," *The Journal of Supercomputing*, vol. 70, no. 1, pp. 177–199, 2014.

[14] P. Grontas, A. Pagourtzis, A. Zacharakis, and B. Zhang, "Towards everlasting privacy and efficient coercion resistance in remote electronic voting," in *Proceedings of the Financial Cryptography and Data Security*, pp. 210–231, Springer, Nieuwpoort, Curaçao, March 2018.

[15] J. Zhou, X. Lin, X. Dong, and Z. Cao, "PSMPA: patient self-controllable and multi-level privacy-preserving cooperative authentication in distributedm-healthcare cloud computing system," *IEEE Transactions on Parallel and Distributed Systems*, vol. 26, no. 6, pp. 1693–1703, 2014.

[16] Z. Jun, C. Zhenfu, D. Xiaolei, L. Xiaodong, and A. V. Vasilakos, "Securing m-healthcare social networks: challenges, countermeasures and future directions," *IEEE Wireless Communications*, vol. 20, no. 4, pp. 12–21, 2013.

[17] S. Saeednia, S. Kremer, and O. Markowitch, "An efficient strong designated verifier signature scheme," in *Proceedings of the ISC2003*, pp. 40–54, Springer, Seoul, Korea, November 2003.

[18] L. Deng, Y. Yang, and R. Gao, "Certificateless designated verifier anonymous aggregate signature scheme for healthcare wireless sensor networks," *IEEE Internet of Things Journal*, vol. 8, no. 11, pp. 8897–8909, 2021.

[19] Y. Li, W. Susilo, Y. Mu, and D. Pei, "Designated verifier signature: definition, framework and new constructions," in *Proceedings of the Ubiquitous Intelligence and Computing*, pp. 1191–1200, Springer, Hong Kong, China, July 2007.

[20] Q. Huang, G. Yang, D. S. Wong, and W. Susilo, "Efficient strong designated verifier signature schemes without random oracle or with non-delegatability," *International Journal of Information Security*, vol. 10, no. 6, p. 373, 2006.

[21] J.-G. Li, N. Qian, X.-Y. Huang, and Y.-C. Zhang, "Certificate-based strong designated verifier signature scheme," *Chinese Journal of Computers*, vol. 35, no. 8, pp. 1579–1587, 2012.

[22] Y. Chen, Y. Zhao, H. Xiong, and F. Yue, "A certificateless strong designated verifier signature scheme with non-delegatability," *International Journal on Network Security*, vol. 19, no. 4, pp. 573–582, 2017.

[23] Y. Shi, H. Fan, and Q. Liu, "An obfuscatable designated verifier signature scheme," *IEEE Transactions on Emerging Topics in Computing*, vol. 5, no. 2, pp. 271–285, 2017.

[24] J. Cai, H. Jiang, P. Zhang, Z. Zheng, G. Lyu, and Q. Xu, "An efficient strong designated verifier signature based on $\mathcal{R}-$ SIS assumption," *IEEE Access*, vol. 7, pp. 3938–3947, 2019.

[25] J. Cai, H. Jiang, P. Zhang et al., "ID-based strong designated verifier signature over R-SIS assumption," *Security and Communication Networks*, vol. 2019, Article ID 9678095, 8 pages, 2019.

[26] X. Huang, W. Susilo, Y. Mu, and F. Zhang, "Short (Identity-Based) strong designated verifier signature schemes," in *Proceedings of the Information Security Practice and Experience (ISPE)*, pp. 214–225, Springer, Hangzhou, China, April 2006.

[27] 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, pp. 1–15, 2021.

[28] 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.

[29] V. Lyubashevsky, "Lattice signatures without trapdoors," in *Proceedings of the Advances in Cryptology - EUROCRYPT 2012 TACT*, pp. 738–755, Springer, Cambridge, UK, April 2012.

[30] J. Bonneau, C. Herley, P. Oorschot, and F. Stajano, "The quest to replace passwords: a framework for comparative evaluation of web authentication schemes," *IEEE Symposium on Security and Privacy*, pp. 1–15, 2012.

[31] K. Hussain, N. Jhanjhi, H. M. ur-Rahman, J. Hussain, and M. Hasan Islam, "Using a systematic framework to critically analyze proposed smart card based two factor Authentication schemes," *Journal of King Saud University - Computer and Information Sciences*, vol. 33, no. 4, pp. 417–425, 2021.

[32] D. Wang and P. Wang, "two birds with one stone: two-factor Authentication with security beyond conventional bound," *IEEE Transactions on Dependable and Secure Computing*, vol. 15, no. 4, pp. 708–722, 2016.

[33] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," *SIAM Review*, vol. 41, no. 2, pp. 303–332, 1999.