Hindawi
Wireless Communications and Mobile Computing
Volume 2020, Article ID 8877405, 10 pages
https://doi.org/10.1155/2020/8877405

Research Article

Privacy-Protection Scheme Based on Sanitizable Signature for Smart Mobile Medical Scenarios

Zhiyan Xu,[1] **Min Luo**,[2] **Neeraj Kumar**,[3] **Pandi Vijayakumar**,[4] **and Li Li**[2]

[1]*College of Computer, Hubei University of Education, Wuhan, China*
[2]*School of Cyber Science and Engineering, Wuhan University, Wuhan, China*
[3]*Department of Computer Science and Engineering, Thapar Institute of Engineering and Technology, Patiala, India*
[4]*Department of Computer Science and Engineering, University College of Engineering Tindivanam, Tindivanam, India*

Correspondence should be addressed to Min Luo; mluo@whu.edu.cn

Received 25 June 2020; Revised 25 September 2020; Accepted 9 November 2020; Published 24 November 2020

Academic Editor: Ding Wang

With the popularization of wireless communication and smart devices in the medical field, mobile medicine has attracted more and more attention because it can break through the limitations of time, space, and objects and provide more efficient and quality medical services. However, the characteristics of a mobile smart medical network make it more susceptible to security threats such as data integrity damage and privacy leakage than those of traditional wired networks. In recent years, many digital signature schemes have been proposed to alleviate some of these challenges. Unfortunately, traditional digital signatures cannot meet the diversity and privacy requirements of medical data applications. In response to this problem, this paper uses the unique security attributes of sanitizable signatures to carry out research on the security and privacy protection of medical data and proposes a data security and privacy protection scheme suitable for smart mobile medical scenarios. Security analysis and performance evaluation show that our new scheme effectively guarantees data security and user privacy while greatly reducing computation and communication costs, making it especially suitable for mobile smart medical application scenarios.

1. Introduction

With the swift development of the Internet and smart devices, mobile medicine has emerged at the historic moment. It is a new type of medical model that can break through the limitations of objective factors such as time, space, and objects. In mobile medical applications, smart devices can provide remote health monitoring and medical supervision for patients using wireless sensor networks [1, 2].

Compared with the traditional medical model, the value of electronic medical records is no longer limited to the application of medical, scientific research, and teaching activities but more related to hospital management, insurance claims, judicial evidence collection, and preventive healthcare [3, 4]. The scope of application of medical information is getting wider and wider, and the utilization rate is getting higher and higher. Therefore, the authenticity and availability of the electronic medical information are critical to the correct use of medical data and to fully reflect the value of medical data sharing. A slight difference may endanger the safety of the patient's life and property, causing irreparable losses [5].

At the same time, medical data contains a lot of personal privacy, which may lead to the leakage of patient privacy in resource sharing [6, 7]. Unnecessary medical information leakage will cause patients to suffer unpredictable hazards such as loss of biological information, telephone fraud, and precise marketing and also seriously endanger the safety of people's life and property [8, 9]. The problems of medical data security and privacy protection have become the biggest obstacles to the further development and promotion of the mobile medical industry.

Digital signature is one of the important means to protect the authenticity and availability of medical data [10–12]. However, not all applications must obtain the complete electronic medical record. For example, when an electronic medical record is used for medical reimbursement, patients only need to provide the insurance company with real information about the treatment and insurance number. When the complete electronic medical record is provided, too much personal information unrelated to medical claims will be disclosed.

To protect the privacy of patients, one of the solutions is to require the signer to only sign information related to medical claims [13]. However, whenever a new subset of the electronic medical record needs to be shared, the signer is required to repeat the signing process, which will generate excessively high computation costs, and sometimes, even the documents cannot be resigned due to the departure of the signer.

Sanitizable signature [14] is a type of digital signature that supports controlled modification of signed messages. This feature makes it not only guarantee the integrity and authenticity of medical data but also effectively hide sensitive information of patients (specific sensitive information can be flexibly set according to different information sharing objects), which not only follows the "minimum necessary" disclosure standard of HIPAA privacy rules [15] but also promotes the use of value-added medical information and improves the efficiency of the scheme. Therefore, sanitizable signatures are very suitable for solving data security and privacy protection issues in smart mobile medical scenarios.

1.1. Our Research Contributions. We regard the main contributions of our scheme to be as follows:

(i) We propose a system model suitable for data security and privacy protection in smart mobile medical scenarios

(ii) We propose a privacy-protection scheme based on sanitizable signature for smart mobile medical scenarios (hereafter referred to as the PP-SS scheme).

(iii) We conduct security analysis and performance evaluation for the newly proposed PP-SS scheme

1.2. Organization of the Paper. The rest of the paper is organized as follows. Sections 2 and 3 present related work and the problem statement, respectively. The new PP-SS scheme is proposed in Section 4. In Sections 5 and 6, we describe the security analysis and the performance evaluation, respectively. Finally, we conclude the paper in the last section.

2. Related Work

The traditional digital signature does not allow any modification operation to the signed message; otherwise, the message signature is invalid [16, 17]. However, to achieve data integrity, authenticity, and availability while ensuring data privacy in smart mobile medical and many other application fields, users hope that signed messages can be modified in a controlled manner to derive new signed messages [18, 19].

The concept of a sanitizable signature was first proposed by Ateniese et al. [14] in 2005, which can break through the limitations of traditional digital signatures and support an entity (sanitizer) designated by the original signer to modify the signed message within the scope of authorization and generate a new signature without any interaction with the signer. Compared with a traditional signature, it not only ensures data integrity but also solves the hidden problem of sensitive information and provides more flexibility.

Brzuska et al. [20] gave the first formal security model for a sanitizable signature. Gong et al. [21] analyzed the formal security model proposed in [20] and pointed out that the security model is vulnerable to rights forgery attacks and then provided new definitions of attributes such as unforgeability and immutability. Subsequently, Krenn et al. [22] made further research on the above model and introduced stronger unforgeability and privacy.

With the continuous development of sanitizable signature technology, it covers more application examples. Brzuska et al. [23] introduced unlinkability, which can ensure that the sanitized signature will not leak from the original signature; even if the original signature is known, it is difficult determine whether the two signatures are related. Subsequent literature [24] introduced noninteractive public accountability, which can facilitate the implementation of the multieye principle [25]. Pöhls et al. [26] proposed the concept of hidden attributes, which means that outsiders cannot know which parts of the signed message are allowed to be modified. Then, Camenisch et al. [27] gave a formal definition of the hidden attribute, and Beck et al. [28] reinforced the attribute. Very recently, Bultel et al. [29] proposed a new sanitizable signature scheme, but it did not perform well in terms of performance.

At present, sanitizable signature schemes have been tried to be implemented on different devices, from desktops [28], to smart cards [30], and then to applications in XML signatures [20]. Before deploying the sanitizable signature scheme in practical applications, users must be aware of the possible legal consequences. Some researchers have proposed emergency properties to avoid some legal challenges [31, 32], because qualified digital signatures are equivalent to handwritten digital signatures in court. The value of concern is that a sanitizable signature scheme can be used to help a redactable signature [33] achieve accountability [34].

3. Problem Statement

The definitions of the equivalence class signature and system model of our proposed PP-SS scheme are presented in this section. System components and security requirements of the privacy-protection scheme based on a sanitizable signature for smart mobile medical scenarios are then described.

3.1. Equivalence Class Signature. We give the definition of equivalence class signature (EQS). For more details, please refer to Reference [35].

Definition 1. (EQS). An EQS signature scheme consists of the following five polynomial algorithms, where $\mathcal{G}$ is the bilinear group and l is the length of a message.

(i) $\mathrm{KGen}(1^l, \mathcal{G}) \rightarrow (pk, sk)$ is a key generation algorithm; it inputs parameters $(1^l, \mathcal{G})$ and outputs a key pair (pk, sk)

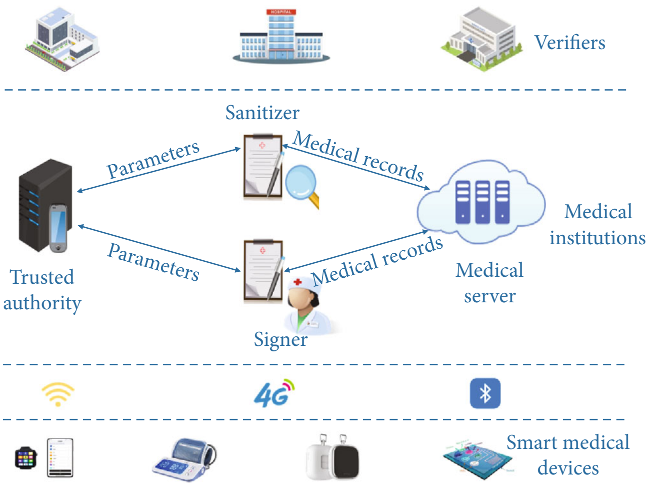

Figure 1: The architecture of our smart mobile medical scenarios.

(ii) $\mathrm{Sign}(sk, \bar{M}) \rightarrow \sigma$ is a signing algorithm; it inputs parameters $(sk, \bar{M})$ and outputs a signature σ on the equivalence class $[\bar{M}]_R$

(iii) $\mathrm{ChgRep}(pk, \bar{M}, \sigma, \rho) \rightarrow \sigma'$ is a change representation algorithm; it inputs parameters $(pk, \bar{M}, \sigma, \rho)$ and outputs a signature σ' on the equivalence class $[\bar{M}^{\rho}]_R$

(iv) $\mathrm{Vf}(\mathrm{param}, \bar{M}, \sigma) \rightarrow b$ is a signature verification algorithm; it inputs parameters $(\mathrm{param}, \bar{M}, \sigma)$ and outputs b, if $b = 1$ and σ is a valid signature; otherwise, $b = 0$ and σ is an invalid signature

(v) $\mathrm{VfKey}(pk, sk) \rightarrow b$ is a key verification algorithm; it inputs parameters (pk, sk) and outputs b, if $b = 1$ the keys are consistent; otherwise, $b = 0$ and the keys are consistent

3.2. System Model. The architecture of our smart mobile medical scenarios is shown in Figure 1, and there are six types of entities in a privacy-protection scheme based on a sanitizable signature scheme: trusted authority, smart medical device, medical server, signer, sanitizer, and verifier. Each entity is specifically defined as follows:

(i) *Trusted authority*. A trusted authority is responsible for initializing the system and generating system parameters

(ii) *Smart medical device*. A smart medical device refers to a portable or wearable medical device used to monitor the health status of patients and give timely feedback to medical experts to get better medical services

(iii) *Medical server*. A medical server is a device with strong computing power and plenty of storage space, which can handle a large amount of data received from smart medical devices

(iv) *Signer*. A signer is usually a doctor who is responsible for completing the setting of relevant parameters that allow modification of the content, the authorization of the semitrust sanitizer, and the signature of the original message

(v) *Sanitizer*. A sanitizer is usually a semitrusted third party authorized by the signer, responsible for modifying the specified content within the scope of the signer's authorization and generating a signature on the sanitized message

(vi) *Verifier*. A verifier is usually a medical data sharing entity which refers to the beneficiaries of medical data sharing, such as insurance companies, scientific research centers, and medical institutions, who can verify the validity of the message signature before and after sanitization and the legality of the identity of the signer and sanitizer

3.3. System Components. Our proposed PP-SS scheme is a collection of the following six polynomial time algorithms:

(i) $\mathrm{Setup}(1^{\lambda}) \rightarrow (\mathrm{params})$ is a probabilistic algorithm to complete system initialization, where λ is a security parameter and params is the system parameters

(ii) $\text{Extract-SKey}(\mathrm{params}) \rightarrow (SK_s, PK_s)$ is a probabilistic algorithm to generate key pairs for the signer

(iii) $\text{Extract-ZKey}(\mathrm{params}) \rightarrow (SK_z, PK_z)$ is a probabilistic algorithm to generate key pairs for the sanitizer

(iv) $\mathrm{Sign}(\mathrm{params}, m, SK_s, PK_z, \alpha,) \rightarrow \sigma$ is a randomized algorithm to generate an original signature, where $m = (m_i)$ is the message, α is a description of the admissible modifications to m, and $\sigma = (\sigma_i)$ is the signature of message m, and $i \in [1, \imath]$

(v) $\mathit{Sanitize}(\mathrm{params}, m, PK_s, SK_z, \xi) \rightarrow (m', \sigma')$ is a randomized algorithm to generate a sanitized signature, where ξ is a description of information that needs to be modified on m, m' is the sanitized message, $\sigma' = (\sigma_i')$ is the signature of sanitized message m', and $i \in [1, \iota]$

(vi) Verify$(\text{params}, PK_s, PK_z, m, \sigma) \rightarrow \{0, 1\}$ is a deterministic algorithm to verify the validity of the signature σ, with 1 or 0 as outputs to indicate whether the message m keeps intergrity

3.4. Security Requirements. A privacy-protection scheme based on a sanitizable signature needs to satisfy the following functions and security requirements:

(i) *Integrity*. To ensure that a verifier can check the message integrity by verifying the validity of the signature

(ii) *Unforgeability*. To ensure that the signature can be proven whether it is generated by the signer or sanitizer, and no one can forge the signature generated by the signer or sanitizer

(iii) *Privacy*. On the premise of maintaining the validity of the original signature, the sanitizer can be allowed to sanitize the sensitive information in the signed message, and no one can distinguish whether the message has been sanitized

4. Our Proposed PP-SS Scheme

Our proposed PP-SS scheme includes six phases, namely, Setup phase, Extract-SKey phase, Extract-ZKey phase, Sign phase, Sanitize phase, and Verify phase.

4.1. Setup. The trusted authority generates system parameters after obtaining the security parameter λ by executing the following operations:

(1) Generate two cyclic addition groups G_1, G_2 and one multiplication group G_T with the same order q, where q is a prime. P is a generator of G_1. $e : G_1 \times G_2 \rightarrow G_T$ is a bilinear pairing

(2) Select one hash function: $H : \{0, 1\}^* \rightarrow G_2$

(3) Publish system parameter list params $= (\lambda, G_1, G_2, G_T, P, e, q, H)$

4.2. Extract-SKey. The signer produces his public-private key by executing the following operations:

(1) Select random values $x_1, x_2, y_1, y_2 \in Z_q^*$

(2) Compute $X_1 = P^{x_1}$, $X_2 = P^{x_2}$ and set $X = (X_1, X_2)$

(3) Compute $Y_1 = {X_1}^{y_1}$, $Y_2 = {X_1}^{y_2}$ and set $Y = (Y_1, Y_2)$

(4) Set $PK_s = (X, Y)$ as signer's public key and $SK_s = (x_1, x_2, y_1, y_2)$ as signer's private key

4.3. Extract-ZKey. The sanitizer produces his public-private key by executing the following operations:

(1) Select random value $x \in Z_q^*$ and set $SK_z = x$ as the sanitizer's private key

(2) Compute $PK_z = x \cdot P$ as the sanitizer's public key

4.4. Sign. The signer produces the signature σ on the message $m = \{m_1 \| m_2 \| \cdots \| m_\iota\}$ by executing the following operations:

(1) Input system parameters params, signer's private key SK_s, sanitizer's public key PK_z, message m, and a description α of the admissible modifications to m

(2) Compute $\vartheta = \text{EQS} \cdot \text{Sign}_{SK_s}(X)$ and $\omega = \text{EQS} \cdot \text{Sign}_{SK_s}(Y)$

(3) Compute $\sigma_i = H(i \| m_i)^{\varsigma_i}$ for $i = (1, 2, \cdots, \iota)$, where

$$\varsigma_i = \begin{cases} y_1, & \text{if } i \in \alpha, \\ 0, & \text{Otherwise,} \end{cases} \tag{1}$$

and set $\sigma = \{\sigma_1, \sigma_2, \cdots, \sigma_\iota\}$ as the signature of message m

(4) Choose a random number $r \in Z_q^*$ and compute $R = rP$, $Q = rPK_z$

(5) Set $R = (x_R, y_R), Q = (x_Q, y_Q)$

(6) Compute $c = (x_Q \| y_Q) \oplus (\alpha \| y_1)$

(7) Return $(\vartheta, \omega, X, Y, R, \sigma = \{\sigma_i\}_1^\iota, c)$

4.5. Sanitization. The sanitizer completes the modification of the message m and produces the signature σ' for the sanitized message m' by executing the following operations:

(1) Input system parameters params, signer's public key PK_s, sanitizer's private key SK_z, message m, signature σ, and a description ξ of the admissible modifications to m

(2) Compute $\theta = SK_z \cdot R$ and set $\theta = (x_\theta, y_\theta)$

(3) Compute $(x_\theta \| y_\theta) \oplus c$ to get $\alpha \| y_1$

(4) If $\xi \in \alpha$, then excute $m' = \xi(m)$; otherwise, return $\perp$

(5) Select random values u, $v \in Z_q^*$ as randomization factors

(6) Compute $X' = (X_1', X_2') = (X_1^u, X_2^u)$ and $Y' = (Y_1', Y_2') = (Y_1^{u.v}, Y_2^{u.v})$ and set $PK_s' = (X', Y')$

(7) Compute $\vartheta' = \text{EQS} \cdot \text{ChgRep}_{PK_s}(X_1, X_2), \vartheta, u)$ and $\omega' = \text{EQS} \cdot \text{ChgRep}_{PK_s}(Y_1, Y_2), \omega, u \cdot v)$

(8) Compute $y_1' = v \cdot y_1$

(9) For $i = (1, 2, \cdots, \iota)$, compute

$$\sigma_i' = \begin{cases} H\left(i\|m_i'\right)^{\varsigma_i{}'}, & \text{if } i \in \alpha, \\ \sigma_i^{\nu}, & \text{Otherwise,} \end{cases} \tag{2}$$

where $\varsigma_i' = y_1'$

(10) Return $(\vartheta', \omega', X', Y', \sigma' = \{\sigma_i'\}_1^{\iota})$

4.6. Verification. The verifier verifies the signature σ' of message m' by executing the following operations:

(1) Input system parameters params, signer's public key PK_s', sanitizer's public key PK_z, message m', signature σ', and a description ξ of the admissible modifications to m

(2) For $i = (1, 2, \cdots, \iota)$, compute

$$b_i = \left(e\left(X_i', \sigma_i'\right) = e\left(Y_i', H\left(i\|m_i'\right)\right)\right), \tag{3}$$

where

$$X_i' = \begin{cases} X_1', & \text{if } i \in \xi, \\ X_2', & \text{Otherwise,} \end{cases}$$
$$Y_i' = \begin{cases} Y_1', & \text{if } i \in \xi, \\ Y_2', & \text{Otherwise} \end{cases} \tag{4}$$

(3) Compute

$$b = \prod_{i=1}^{\iota} b_i \tag{5}$$

(4) If $b = 1$, accept σ'; otherwise, reject σ'

5. Security Analysis

5.1. Correctness. Our proposed sanitizable signature scheme is correct if and only if the sanitized signature generated from our scheme can satisfy Equation (3), where the correctness of the scheme is elaborated as follows, where $i \in \{1, 2, \cdots \iota\}$:

$$\begin{aligned} e\left(X_i', \sigma_i'\right) &= e\left(X_i', H\left(i\|m_i'\right)^{y_i{}'}\right) = e\left(\left(X_i'\right)^{y_i{}'}, H\left(i\|m_i'\right)\right) \\ &= e\left(Y_i', H\left(i\|m_i'\right)\right). \end{aligned} \tag{6}$$

5.2. Provable Security. In this section, we demonstrate that our presented PP-SS scheme has perfect strong transparency against adversaries as defined in [29].

Definition 2. (transparency). Transparency is also indistinguishability, which means that the sanitized signature looks like it has not been sanitized. It requires that one cannot decide whether the signature is sanitized or nonsanitized without the help of the oracle [22].

Theorem 3. *A sanitizable signature scheme is perfectly strongly transparent if for all probability polynomial time adversaries A, Asanitize*

$$\Pr\left[ExpTrans_A^0(\lambda) = 1\right] = \Pr\left[ExpTrans_A^1(\lambda) = 1\right], \tag{7}$$

where $ExpTrans_A^b$ is the security experiments of transparency for sanitizable signatures.

Proof. We prove that the scheme has perfectly strong transparency through the hybrid argument. Now, let q denote the maximum number of times that adversary A can query the Sign/SanO$_b$ oracle, and define the hybrid variables Hb_0, Hb_1,..., Hb_q as follows.

Hb_0 is identical to $\mathrm{ExpTrans}_A^0(\lambda)$. For $j \in \{1, 2, \cdots, q\}$, Hb_j is almost the same as the value of Hb_{j-1}, except for the answer of the j-th query to Sign/SanO$_b$ is $\mathrm{ExpTrans}_A^1(\lambda)$. That is to say, the answer of the first j-th query to Sign/SanO$_b$ is the sanitized signature, and the remaining q-j signatures are unsanitized (original) signatures. It should be noted that $Hb_q = \mathrm{ExpTrans}_A^1(\lambda)$. Obviously, if Pr $[Hb_{j-1} = 1]$ = Pr $[Hb_j = 1]$ for $j \in \{1, 2, \cdots, q\}$, then $\mathrm{ExpTrans}_A^1(\lambda) = \mathrm{ExpTrans}_A^0(\lambda)$ holds.

For $j \in \{1, 2, \cdots, q\}$, we demonstrate that Pr $[Hb_{j-1} = 1]$ = Pr $[Hb_j = 1]$ as below. Let the tuple (m, ξ, α) be the j-th query of adversary A to Sign/SanO$_b$ oracle, if $\xi \notin \alpha$, then oracle returns $\perp$ and the equality holds trivially. Otherwise, let $m' \coloneqq \xi(m)$ and σ' be the answer. The signature σ' comes from the mathematical distribution $\mathbf{D}$, where

$$\mathbf{D} \coloneqq \left\{ \begin{array}{c} x_i, y_i \in Z_q^*, X_i \coloneqq P^{x_i}, Y_i \coloneqq X_i^{y_i}, i \in [\iota] \\ \vartheta = \mathrm{EQS} \cdot \mathrm{Sign}_{SK_s}(X_1, X_2) \\ \omega = \mathrm{EQS} \cdot \mathrm{Sign}_{SK_s}(Y_1, Y_2) \\ \sigma_i = H\left(i\|m_i'\right)^{\varsigma_i}, i \in [\iota] \\ \varsigma_i = \begin{cases} y_1, & \text{if } i \in \alpha \\ 0, & \text{Otherwise} \end{cases} \\ R = rP, Q = rPK_z. \\ c = \left(x_Q\|y_Q\right) \oplus (\alpha\|y_1). \\ \sigma = \left(u, v, \{\sigma_i, X_i, Y_i\}_{i=1}^{\iota}, c\right) \end{array} \right\}. \tag{8}$$

Replacing x_i and y_i with $u \cdot x_i$ and $v \cdot y_i$, respectively, for some $u, v \in Z_q^*$, we can obtain a mathematical distribution $\mathbf{D}' = \mathbf{D}$, where

$$\mathbf{D}' := \left\{ \begin{array}{c} u, v \in Z_q^* \\ x_i, y_i \in Z_q^*, X_i := P^{x_i}, Y_i := X_i^{y_i}, i \in [\iota] \\ \vartheta = \text{EQS} \cdot \text{Sign}_{SK_s}(X_1, X_2)^u \\ \omega = \text{EQS} \cdot \text{Sign}_{SK_s}(Y_1, Y_2)^{u \cdot v} \\ \sigma_i = H\left(i \| m_i'\right)^{\varsigma_i'}, i \in [\iota] \\ \varsigma_i' = \begin{cases} v \cdot y_1, & \text{if } i \in \alpha \\ 0, & \text{Otherwise} \end{cases} \\ R = rP, Q = rPK_z. \\ c = \left(x_Q \| y_Q\right) \oplus (\alpha \| y_1). \\ \sigma = \left(u, v, \{\sigma_i, X_i^u, Y_i^{u \cdot v}\}_{i=1}^{\iota}, c\right) \end{array} \right\}. \tag{9}$$

Because of the perfect adaption of EQS [35], the distribution of $\vartheta = \text{EQS} \cdot \text{Sign}_{SK_s}(X_1, X_2)^u$ and $\omega = \text{EQS} \cdot \text{Sign}_{SK_s}(Y_1, Y_2)^{u \cdot v}$ is the same as that of $\text{ChgRep}_{PK_s}(X_1, X_2), \vartheta', u)$ and $\text{ChgRep}_{PK_s}(Y_1, Y_2), \omega', u \cdot v)$, where $\vartheta' = \text{EQS} \cdot \text{Sign}_{SK_s}(X_1, X_2)$, $\omega' = \text{EQS} \cdot \text{Sign}_{SK_s}(Y_1, Y_2)$. Then, we can obtain a distribution $\mathbf{D}' = \mathbf{D}''$, and we have

$$\mathbf{D}'' := \left\{ \begin{array}{c} u, v \in Z_q^* \\ x_i, y_i \in Z_q^*, X_i := P^{x_i}, Y_i := X_i^{y_i}, i \in [\iota] \\ \vartheta' = \text{EQS} \cdot \text{Sign}_{SK_s}(X_1, X_2) \\ \omega' = \text{EQS} \cdot \text{Sign}_{SK_s}(Y_1, Y_2) \\ \vartheta = \text{ChgRep}_{PK_s}(X_1, X_2), \vartheta', u\big) \\ \omega = \text{ChgRep}_{PK_s}(Y_1, Y_2), \omega', u \cdot v\big) \\ \sigma_i = H\left(i \| m_i'\right)^{\varsigma_i'}, i \in [\iota] \\ \varsigma_i' = \begin{cases} v \cdot y_1, & \text{if } i \in \alpha \\ 0, & \text{Otherwise} \end{cases} \\ R = rP, Q = rPK_z. \\ c = \left(x_Q \| y_Q\right) \oplus (\alpha \| y_1). \\ \sigma = \left(u, v, \{\sigma_i, X_i^u, Y_i^{u \cdot v}\}_{i=1}^{\iota}, c\right) \end{array} \right\}. \tag{10}$$

From the above derivation process, it is easy to find that in Hb_j, the signature σ' completely came from $\mathbf{D}''$. Therefore, we can conclude that Hb_{j-1} and Hb_j are equivalent in function.

5.3. Comparative Summary: Security Properties. We show that our PP-SS scheme can meet all the security requirements presented in Section 3.

(i) *Integrity*. The PP-SS scheme proposed in this paper has the characteristics of a traditional digital signature. Before sharing medical data, first sign it, and then the verifier can determine the integrity of the medical data by verifying the signature of the message

(ii) *Unforgeability*. The PP-SS scheme proposed in this paper introduces Fuchsbauer et al.'s EQS scheme, which has been proven to be unforgeable under chosen message attacks [35], which can ensure no one can forge the signature generated by the signer or sanitizer

(iii) *Sanitization*. The sanitizer in our proposed PP-SS scheme in this paper can be allowed to sanitize the information in the signed message, which can effectively hide the patient's sensitive information

(iv) *Privacy*. The PP-SS scheme proposed in this paper can effectively hide the patient's sensitive information, and the unsanitized signature and the sanitized signature generated from our PP-SS scheme are indistinguishable as proven in Section 5.2, which effectively protects the privacy of the patient

5.4. Comparative Summary: Security Comparison. As can be seen from Table 1, we observe that Jiang et al.'s scheme [16], Wu et al.'s scheme [17], Bultel et al.'s scheme [29], and our proposed PP-SS scheme can all meet the integrity and unforgeability. Only our PP-SS scheme can satisfy the sanitization and privacy. Suppose a patient agrees to share his electronic medical record with other medical research institutions through a third-party platform (hospital) but does not want to expose the privacy information such as the identity in the message. If users try to solve the above problems using the schemes of Jiang et al. or Wu et al., they will find that both of them can only obscure the identity of the information publisher, but cannot effectively hide user privacy information contained in the message.

In Bultel et al.'s scheme [29] and our PP-SS scheme, patients can entrust a third-party platform as a sanitizer to modify the privacy information specified by the original signer in the message. In addition, both of them can meet the indistinguishability and the attacker cannot obtain the user's private information, which can effectively protect the privacy of the user's sensitive information. Comparatively speaking, Bultel et al.'s scheme and our PP-SS scheme satisfy all four security requirements in Table 1 and outperform the two other schemes in terms of data security and privacy protection.

6. Comparative Summary: Performance

In this section, we analyze the performance of our proposed PP-SS scheme by evaluating the computation and communication costs.

6.1. Computation Costs. We evaluate the performance of our new proposal and Bultel et al.'s scheme [29]. In the specific implementation, we choose a nonsingular elliptic curve E

Table 1: Comparative summary: security properties.

	Jiang et al.'s scheme [16]	Wu et al.'s scheme [17]	Bultel et al.'s scheme [29]	Our scheme
Integrity	✓	✓	✓	✓
Unforgeability	✓	✓	✓	✓
Sanitization	×	×	✓	✓
Privacy	×	×	✓	✓

: $y^2 = x^3 + ax + b \bmod q$, and a, $b \in Z_q^*$, G is the additive group with the order q on E, security parameter $|\lambda| = 80$ bits, and p and q are both prime numbers with a length of 160 bits. We run the simulation experiment using the MIRACL library [36] on a personal computer (Intel core with I7-4770@3.4 GHz CPU, 4 GB random memory, and Windows 7 operating system). The running time of different operations is shown in Table 2.

Because Setup, Extract-SKey, and Extract-ZKey phases are a one-off operation, we only consider the computation costs in the Sign phase, Sanitize phase, and Verify phase. AnEQS $\cdot$ Signalgorithm includes$(2n-2)$point addition operations and$(2n+2)$point multiplication operations, an EQS $\cdot$ ChgRep algorithm requires $(n+4)$ point multiplication operations, and an EQS $\cdot$ Verify algorithm requires $(n+5)$ bilinear pair operations, where n is the number of messages involved in the operation [35].

In the Sign phase, the signer in Bultel et al.'s scheme needs to perform 3ι exponentiation operations, $(4\iota-4)$ point addition operations, $(4\iota+6)$ point multiplication operations, and ι hash to point operations; therefore, the computation cost of the Sign phase in Bultel et al.'s scheme is $3\iota T_{\mathrm{exp}} + (4\iota-4)T_{\mathrm{pa}} + (4\iota+6)T_{\mathrm{pm}} + \iota T_{\mathrm{mtp}}$. The signer in our PP-SS scheme needs to perform ι exponentiation operations, four point addition operations, fourteen point multiplication operations, and ι hash to point operations; therefore, the computation cost of Sign phase in our PP-SS scheme is $\iota T_{\mathrm{exp}} + 4T_{\mathrm{pa}} + 14T_{\mathrm{pm}} + \iota T_{\mathrm{mtp}}$.

In the Sanitize phase, the sanitizer in Bultel et al.'s scheme needs to perform 3ι exponentiation operations, $(2\iota+9)$ point multiplication operations, and α hash to point operations; therefore, the computation cost of the Sanitize phase in Bultel et al.'s scheme is $3\iota T_{\mathrm{exp}} + (2\iota+9)T_{\mathrm{pm}} + \alpha T_{\mathrm{mtp}}$. The sanitizer in our PP-SS scheme needs to perform $(4+\iota)$ exponentiation operations, thirteen point multiplication operations, and α hash to point operations; therefore, the computation cost of Sanitize phase in our PP-SS scheme is $(4+\iota)T_{\mathrm{exp}} + 13T_{\mathrm{pm}} + \alpha T_{\mathrm{mtp}}$.

In the Verify phase, the verifier in Bultel et al.'s scheme needs to perform $(4\iota+10)$ bilinear pair operations and ι hash to point operations; therefore, the computation cost of the Verify phase in Bultel et al.'s scheme is $(4\iota+10)T_{\mathrm{bp}} + \iota T_{\mathrm{mtp}}$. The verifier in our PP-SS scheme needs to perform $(2\iota+20)$ bilinear pair operations and ι hash to point operations; therefore, the computation cost of Verify phase in Bultel et al.'s scheme is $(2\iota+20)T_{\mathrm{bp}} + \iota T_{\mathrm{mtp}}$.

Table 2: Running time of different operations (ms).

Notations	Operations	Time
T_{exp}	A modular exponentiation operation	3.8636
T_{pa}	A point addition operation	0.0018
T_{pm}	A point multiplication operation	0.4421
T_{bp}	A bilinear pair operation	4.2110
T_{mtp}	A hash to point operation	4.4060

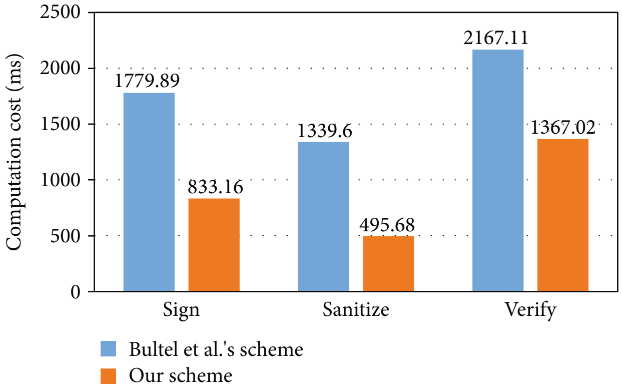

Figure 2: Comparative summary: computation costs.

As shown in Figure 2 and Table 3, if $\iota = 100$ and $\alpha = 20$, we can observe that the computation cost of the Sign phase in our PP-SS scheme is 833.16 ms, which is reduced by 53.19% compared with Bultel et al.'s scheme (the computation cost is 1779.89 ms); the computation cost of the Sanitize phase in our PP-SS scheme is 495.68 ms, which is reduced by 62.99% compared with Bultel et al.'s scheme (the computation cost is 1339.60 ms); and the computation cost of the Verify phase in our PP-SS scheme is 1367.02 ms, which is reduced by 36.92% compared with Bultel et al.'s scheme (the computation cost is 2167.11 ms) in terms of computation cost percentage. Obviously, our new scheme greatly reduces the computation cost at different phases.

6.2. Communication Costs. In the Setup, Extract-SKey, Extract-ZKey, and Verify phases, there is no additional communication cost in Bultel et al.'s scheme [29] and our proposed PP-SS scheme. Hence, we only consider the communication costs of the Sign phase and the Sanitize phase. For simplicity, we assume the length of the user's electronic medical record F is ℓ in accordance with the above implementation. The communication cost is analyzed as follows.

In the Sign phase, the signer in Bultel et al.'s scheme needs to send $\sigma = (\mu, \eta, \{\sigma_i, X_i, Y_i\}_{i=1}^{\iota}, c)$, R, and the electronic medical record F to the sanitizer. Since $|\mu| = 8|q|$, $|\eta| = 8|q|$, $|c| = (\iota+1)|q|$, and R, σ_i, X_i, Y_i are all the elements in G_2, the communication cost of Bultel et al.'s scheme is $|\mu| + |\eta| + |c| + \iota(|\sigma_i| + |X_i| + |Y_i|) + |R| + |F| = 8|q| + 8|q| + (\iota+1)|q| + \iota(2|q| + 2|q| + 2|q|) + 2|q| + \ell$ bits. The signer in our PP-SS scheme needs to send $(\vartheta, \omega, X, Y, R, \sigma = \{\sigma_i\}_1^{\iota}, c)$

Table 3: Computation cost comparison (ms).

Scheme	Sign	Sanitize	Verify
Bultel et al.'s [29]	$300T_{\text{exp}} + 396T_{\text{pa}} + 406T_{\text{pm}} + 100T_{\text{mtp}} \approx 1779.89$	$300T_{\text{exp}} + 209T_{\text{pm}} + 20T_{\text{mtp}} \approx 1339.60$	$410T_{\text{bp}} + 100T_{\text{mtp}} \approx 2167.11$
Our scheme	$100T_{\text{exp}} + 4T_{\text{pa}} + 14T_{\text{pm}} + 100T_{\text{mtp}} \approx 833.16$	$104T_{\text{exp}} + 13T_{\text{pm}} + 20T_{\text{mtp}} \approx 495.68$	$220T_{\text{bp}} + 100T_{\text{mtp}} \approx 1367.02$

Table 4: Comparative summary: communication cost (bit).

	Bultel et al.'s scheme [29]	Our scheme
Sign	$8\mid q\mid +8\lvert q\rvert + 51\lvert q\rvert + 50(2\mid q\rvert+2\mid q\rvert+2\mid q\mid) + 2\lvert q\rvert + \ell \approx 60064$	$8\mid q\mid +8\lvert q\rvert + 2\lvert q\rvert + 100\lvert q\rvert + 2\lvert q\rvert + 2\lvert q\rvert + 2\lvert q\rvert + 2\lvert q\rvert + 2\lvert q\rvert + \ell \approx 21504$
Sanitize	$8\mid q\mid +8\lvert q\rvert + 50(2\mid q\rvert+2\mid q\rvert+2\mid q\mid) + \ell \approx 51584$	$8\mid q\mid +8\lvert q\rvert + 100\lvert q\rvert + 2\lvert q\rvert + 2\lvert q\rvert + 2\lvert q\rvert + 2\lvert q\rvert + \ell \approx 20864$

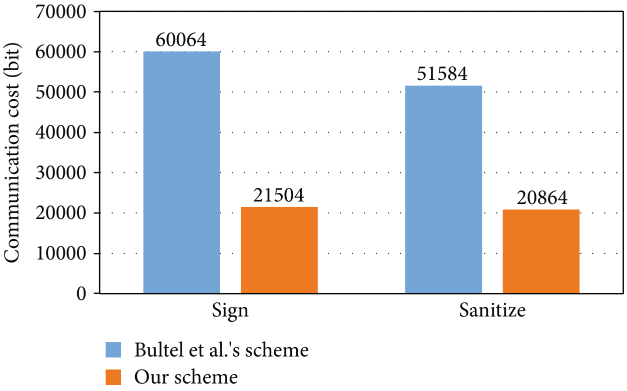

Figure 3: Comparative summary: communication costs.

and electronic medical record F to the sanitizer. Since $|\vartheta| = 8|q|$, $|\omega| = 8|q|$, $|c| = 2|q|$, and R, σ_i, X_1, X_2, Y_1, Y_2 are all the elements in G_2, the communication cost of Bultel et al.'s scheme is $|\vartheta| + |\omega| + |c| + \iota|\sigma_i| + |X_1| + |X_2| + |Y_1| + |Y_2| + |R| + |F| = 8\mid q\mid +8|q| + 2|q| + 2\iota|q| + 2|q| + 2|q| + 2|q| + 2|q| + 2|q| + \ell$ bits.

In the Sanitize phase, the sanitizer in Bultel et al.'s scheme needs to send $\sigma' = (\mu', \eta', \{\sigma_i', X_i', Y_i'\}_{i=1}^{\iota})$ to the sanitizer. Since $|\mu'| = 8|q|$, $|\eta'| = 8|q|$, and σ_i', X_i', Y_i' are all the elements in G_2, the communication cost of Bultel et al.'s scheme is $|\mu'| + |\eta'| + \iota(|\sigma_i'| + |X_i'| + |Y_i'|) + |F'| = 8\mid q\mid +8|q| + \iota(2\mid q\mid+2\mid q|+|Y_i\mid) + \ell$ bits. The signer in our PP-SS scheme needs to send $(\vartheta', \omega', X', Y', \sigma' = \{\sigma_i'\}_1^{\iota})$ and electronic medical record F' to the sanitizer. Since $|\vartheta'| = 8|q|$, $|\omega'| = 8|q|$, and σ_i', X_1', X_2', Y_1', Y_2' are all the elements in G_2, the communication cost of Bultel et al.'s scheme is $|\vartheta'| + |\omega'| + \iota|\sigma_i'| + |X_1'| + |X_2'| + |Y_1'| + |Y_2'| + |F'| = 8\mid q\mid +8|q| + \iota(2\mid q\mid) + 2|q| + 2|q| + 2|q| + 2|q| + \ell$ bits.

If we choose $\iota = 50$ and $|F| = \ell = 1024$ bits, the comparative summary of the communication costs is demonstrate in Table 4 and Figure 3. We can observe that the communication cost of the Sign phase in our PP-SS scheme is 21504 bits, which is reduced by 64.20% compared with Bultel et al.'s scheme (the communication cost is 60064 bits), and the communication cost of the Sanitize phase in our PP-SS scheme is 20864 bits, which is reduced by 59.55% compared with Bultel et al.'s scheme (the communication cost is 51584 bits) in terms of communication cost percentage. Obviously, our new scheme greatly reduces the communication cost at different phases.

7. Conclusion

Smart mobile medical is a trend that is unlikely to disappear in the foreseeable future, and as the amount of user data continues to increase, it is essential to ensure the availability of medical data and the privacy of user information. Many digital signature schemes have been proposed recently, but most schemes have certain limitations and cannot be well adapted to the needs of smart medical applications.

To overcome this security problem, we propose a new data security and privacy protection scheme based on a sanitizable signature for smart mobile medical scenarios. Security analysis and detailed performance evaluation demonstrate that our PP-SS scheme can not only ensure the integrity of medical data and support the privacy protection of patient but also achieve a higher level of security assurance when communication and computation costs are greatly reduced. Therefore, our proposed PP-SS scheme is more suitable for actual deployment in smart mobile medical scenarios.

Data Availability

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

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 (Nos. 61902115, 61972294, and 61932016) and the Opening Project of Guangdong Provincial Key Laboratory of Data Security and Privacy Protection (No. 2017B030301004-11).

References

[1] P. Kakria, N. K. Tripathi, and P. Kitipawang, "A real-time health monitoring system for remote cardiac patients using smartphone and wearable sensors," *International Journal of*

Telemedicine and Applications, vol. 2015, Article ID 373474, 11 pages, 2015.

[2] M. S. Hossain, G. Muhammad, and A. Alamri, "Smart healthcare monitoring: a voice pathology detection paradigm for smart cities," *Multimedia Systems*, vol. 25, no. 5, pp. 565–575, 2019.

[3] H.-R. Lim, H. S. Kim, R. Qazi, Y.-T. Kwon, J.-W. Jeong, and W.-H. Yeo, "Advanced soft materials, sensor integrations, and applications of wearable flexible hybrid electronics in healthcare, energy, and environment," *Advanced Materials*, vol. 32, no. 15, article 1901924, 2020.

[4] K. Kroenke, D. P. Alford, C. Argoff et al., "Challenges with implementing the centers for disease control and prevention opioid guideline: a consensus panel report," *Pain Medicine*, vol. 20, no. 4, pp. 724–735, 2019.

[5] C. Peng, P. Goswami, and G. Bai, "A literature review of current technologies on health data integration for patient-centered health management," *Health Informatics Journal*, vol. 26, no. 3, pp. 1926–1951, 2020.

[6] M. Al Ameen, J. Liu, and K. Kwak, "Security and privacy issues in wireless sensor networks for healthcare applications," *Journal of Medical Systems*, vol. 36, no. 1, pp. 93–101, 2012.

[7] T. Gong, H. Huang, P. Li, K. Zhang, and H. Jiang, "A medical healthcare system for privacy protection based on IoT," in *2015 Seventh International Symposium on Parallel Architectures, Algorithms and Programming (PAAP)*, pp. 217–222, Nanjing, China, December 2015.

[8] R. F. Greaves, S. Bernardini, M. Ferrari et al., "Key questions about the future of laboratory medicine in the next decade of the 21st century: a report from the IFCC-emerging technologies division," *Clinica Chimica Acta*, vol. 495, pp. 570–589, 2019.

[9] L. Fang, C. Yin, J. Zhu et al., "Privacy protection for medical data sharing in smart healthcare," *ACM Transactions on Multimedia Computing Communications and Applications*, vol. 1, no. 1, pp. 1–18, 2020.

[10] D. He, Y. Zhang, D. Wang, and K. K. R. Choo, "Secure and efficient two-party signing protocol for the identity-based signature scheme in the IEEE P1363 standard for public key cryptography," *IEEE Transactions on Dependable and Secure Computing*, vol. 17, no. 5, pp. 1124–1132, 2018.

[11] Y. Zhang, D. He, X. Huang, D. Wang, K. K. R. Choo, and J. Wang, "White-box implementation of the identity-based signature scheme in the IEEE P1363 standard for public key cryptography," *IEICE Transactions on Information and Systems*, vol. E103.D, no. 2, pp. 188–195, 2020.

[12] Q. Feng, D. He, Z. Liu, D. Wang, and K. K. R. Choo, "Distributed signing protocol for IEEE p1363-compliant identity-based signature scheme," *IET Information Security*, vol. 14, no. 4, pp. 443–451, 2020.

[13] H. Jin, Y. Luo, P. Li, and J. Mathew, "A review of secure and privacy-preserving medical data sharing," *IEEE Access*, vol. 7, pp. 61656–61669, 2019.

[14] G. Ateniese, D. H. Chou, B. De Medeiros, and G. Tsudik, "Sanitizable signatures," in *European Symposium on Research in Computer Security*, pp. 159–177, Springer, 2005.

[15] Centers for Disease Control and Prevention, "HIPAA privacy rule and public health. Guidance from CDC and the US Department of Health and Human Services," *MMWR: Morbidity and Mortality Weekly Report*, vol. 52, Supplement 1, pp. 1–17, 2003.

[16] Y. Jiang, Y. Ji, and T. Liu, *An anonymous communication scheme based on ring signature in VANETs*, Computer Science, 2014.

[17] L. Wu, Z. Xu, D. He, and X. Wang, "New certificateless aggregate signature scheme for healthcare multimedia social network on cloud environment," *Security and Communication Networks*, vol. 2018, Article ID 2595273, 13 pages, 2018.

[18] D. S. Tug, C. H. Tug, D. D. Tug et al., *Overview of functional and malleable signature schemes*, 2015.

[19] A. Bilzhause, H. C. Pöhls, and K. Samelin, "Position paper: the past, present, and future of sanitizable and redactable signatures," in *Proceedings of the 12th International Conference on Availability, Reliability and Security*, pp. 1–9, Reggio Calabria, Italy, August 2017.

[20] C. Brzuska, M. Fischlin, T. Freudenreich et al., "Security of sanitizable signatures revisited," in *International Workshop on Public Key Cryptography*, pp. 317–336, Springer, 2009.

[21] J. Gong, H. Qian, and Y. Zhou, "Fully-secure and practical sanitizable signatures," in *International Conference on Information Security and Cryptology*, pp. 300–317, Springer, 2010.

[22] S. Krenn, K. Samelin, and D. Sommer, "Stronger security for sanitizable signatures," in *Data Privacy Management, and Security Assurance*, pp. 100–117, Springer, 2015.

[23] C. Brzuska, M. Fischlin, A. Lehmann, and D. Schröder, "Unlinkability of sanitizable signatures," in *International Workshop on Public Key Cryptography*, pp. 444–461, Springer, 2010.

[24] C. Brzuska, H. C. Pöhls, and K. Samelin, "Non-interactive public accountability for sanitizable signatures," in *European Public Key Infrastructure Workshop*, pp. 178–193, Springer, 2012.

[25] A. Bilzhause, M. Huber, H. C. Pöhls, and K. Samelin, "Cryptographically enforced four-eyes principle," in *2016 11th International Conference on Availability, Reliability and Security (ARES)*, pp. 760–767, Salzburg, Austria, August 2016.

[26] H. C. Pöhls, K. Samelin, and J. Posegga, "Sanitizable signatures in xml signature performance, mixing properties, and revisiting the property of transparency," in *International Conference on Applied Cryptography and Network Security*, pp. 166–182, Springer, 2011.

[27] J. Camenisch, D. Derler, S. Krenn, H. C. Pöhls, K. Samelin, and D. Slamanig, "Chameleon-hashes with ephemeral trapdoors," in *IACR International Workshop on Public Key Cryptography*, pp. 152–182, Springer, 2017.

[28] M. T. Beck, J. Camenisch, D. Derler et al., "Practical strongly invisible and strongly accountable sanitizable signatures," in *Australasian Conference on Information Security and Privacy*, pp. 437–452, Springer, 2017.

[29] X. Bultel, P. Lafourcade, R. W. Lai, G. Malavolta, D. Schröder, and S. A. K. Thyagarajan, "Efficient invisible and unlinkable sanitizable signatures," in *IACR International Workshop on Public Key Cryptography*, pp. 159–189, Springer, 2019.

[30] H. C. Pöhls, S. Peters, K. Samelin, J. Posegga, and H. de Meer, "Malleable signatures for resource constrained platforms," in *IFIP International Workshop on Information Security Theory and Practices*, pp. 18–33, Springer, 2013.

[31] M. Rost and A. Pfitzmann, "Datenschutz-Schutzziele — revisited," *Datenschutz und Datensicherheit - DuD*, vol. 33, no. 6, pp. 353–358, 2009.

[32] H. C. Pöhls, *Increasing the legal probative value of cryptographically private malleable signatures*, 2018.

[33] S. Lim, E. Lee, and C. M. Park, “A short redactable signature scheme using pairing,” *Security and Communication Networks*, vol. 5, no. 5, 534 pages, 2012.

[34] H. C. Pöhls and K. Samelin, “Accountable redactable signatures,” in *2015 10th International Conference on Availability, Reliability and Security*, pp. 60–69, Toulouse, France, August 2015.

[35] C. Hanser and D. Slamanig, “Structure-preserving signatures on equivalence classes and their application to anonymous credentials,” in *International Conference on the Theory and Application of Cryptology and Information Security*, pp. 491–511, Springer, 2014.

[36] M. Scott, *Miracl–Multiprecision Integer and Rational Arithmetic c/c++ Library*, Shamus Software Ltd, Dublin, Ireland, 2003.