A Novel Personal Medicine Record Scheme Based on Block Chain and Cryptographic

[1]CHENGLIAN LIU, [2]SONIA CHIEN-I CHEN
[1]Department of Science and Engineering, Shiyuan College of Nanning Normal University,
Nanning 530226, CHINA
[2]School of Economics, Qingdao University, Qingdao 266061, CHINA

Abstract: The World Health Organization (WHO) has defined “eHealth” as “the application of information and communication technology” (ICT) in the medical and health field. This includes “medical care, disease management, public health surveillance, and education and research”. E-Health can improve access to medicine and reduce medical costs. Therefore, it has a far-reaching impact on developing countries and vulnerable groups. However, whenever a medical dispute arises, there are no good handling mechanisms, such as a complaint platform that handles patient or doctor complaints to help reduce litigations in medical disputes. For this reason, the authors propose a study of this concept.

Keywords: Personal Medicine Record, Digital Signature, Anonymous, Cryptographic

Received: May 28, 2021. Revised: July 7, 2022. Accepted: August 11, 2022. Published: September 14, 2022.

1. Introduction

Security and confidentiality are major concerns when it comes to technology-oriented healthcare. Although the goals of convenience and cost-effectiveness can be met through its implementation, it is seen that personal data transmission and its secondary use remain as open issues. What e-health claims is that better health outcomes and enhanced efficiency can be facilitated with the help of technology. However, the threats of privacy preservation may overweight the benefits of convenience offered. It is relevant to propose an effective method that can enable efficiency while security and confidentiality can be ensured. We classify blockchain into one category [1]–[5], data protection into one category [6], [7], medical image into one category [8]–[10], watermarking into one category [8], [10], [11], and remainder into others category [12], [13]. Wu and Liu [14] described an anonymous delivery system using blind signature scheme. Later, Wu et al. [15] also presented a conception which used anonymity purchasing to mobile payment. Zhang et al. [16] connected RSA [17] with ElGamal [18] two algorithms in their idea on mobile purchasing without bank card. Lv et al. [19] applied to library complaint information system. Based on mathematical reasoning and model inference, we get inspiration there. In this paper the authors would like to propose a scheme using mathematical model and cryptology skill to personal medicine record system. Due to limited conditions, this study lists parts of good contributions, but is a little different then what is discussed in this article, please see Table I.

Table I
RELATED LITERATURES

Blockchain	Data Protection	Medical Image	Watermarking	Others
Yue et al. [1]	Chiang [6]	Bouslimi and Coatrieux [8]	Bouslimi and Coatrieux [8]	Fang et al. [12]
Agbo et al. [2]	Park et al. [7]	Abdmouleh et al. [9]	Anand and Singh [11]	Liu et al. [13]
Khezr et al. [3]		Zermi et al. [10]	Zermi et al. [10]	
Hasselgren et al. [4]				
Hussien et al. [5]				

2. Related Works

Our research extend the information security technology and information management, and then applied the cryptology into personal medicine record of health information system. Fang et al. [12] proposed a conception of personal health records via blockchain technology, but they just described the framework without implementation to entity. In the same year, Liu et al. [13] also presented a scheme about anonymous complaint system based on patient-doctor and hospital health information system. Neither Fang et al. [12] nor Liu et al. [13] gave formal verification way to use mathematical method to prove that schemes. The blockchain technology is applied to construct a pathway for information security in personal health records [20], [21]. By now, the authors combined two well-known public key cryptosystems RSA [17] with ElGamal algorithms [18] in this article. It addresses encryption and encryption through 10 phases authentication to achieve confidentiality: 0) System initiation; 1) Registration; 2) Account passing; 3) Doctor visiting; 4) Records filling; 5) Records updated; 6) Records checking; 7) Diagnosis; 8) Feedback and 9) Medicine taking. Taking advantage of hash function of blockchain, this method deliveries data in an anonymous manner to safeguard the privacy of personal records with mobility and transferability. After employing both theoretical and practical security analysis, this method is proven to be secured and efficient in personal health records transmission. Through applying this innovative method, stakeholders from patients, doctors, the ensured party and hospitals are authenticated to certify the accuracy of data.

Step 1. Patient applied and registered an account by hospital's health information system.
Step 2. The system center issued an account to patient who applied an ID previously.
Step 3. Patient went to hospital or clinic to meet a doctor when he felt ill.
Step 4. The doctor diagnosed patient and sent the diagnostic records to system center.
Step 5. The system center received the diagnostic records from doctor before returned the verification result.
Step 6. the doctor updated record with health bureau.
Step 7. the health bureau responded updating data to doctor.
Step 8. Doctor feeds back the result to patient.
Step 9. Patient take his medicine from pharmacy.

The diagram of conception, see Figure 1.

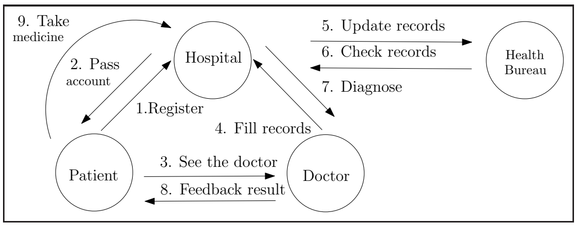

Figure 1. The Conception of Our Scheme.

3. Our Methodology

Suppose p is a large prime which its over 1024 bits length, g is a primitive root of $\mathbb{Z}_p^*$, q is a factor by $(p-1)$, namely $q|(p-1)$.

Notation and **Significant**:
p_i: large prime of RSA algorithm [17].
q_i: large prime of RSA algorithm.
n_i: modulus number of RSA algorithm.
p_1: prime number, this is deference with RSA's p_i.
g: primitive root of prime number p_1.
x_i: secret key in ElGamal-like algorithm [18].
y_i: public key in ElGamal-like algorithm.
e_i: public key in RSA algorithm.
d_i: private key in RSA algorithm.
m: digitized message.

Health Bureau: The Health Bureau (HB) means Ministry of Health and Welfare (MHL) or National Health Insurance Administration (NHI) in Taiwan. The names of medical institutions in different countries, it may be varieties.

Hospital: We usually means the hospital (or clinic) information system center. Here, we use abbreviation 'hospital' or 'system center'.

Doctor: We denote the staff who works in hospital. There are including nurse and doctor. We preferred mean to doctor who is qualified in medicine and treats people.

Patient: A common person or user who is ill.

3.1 System Initializing Phase

The Patient randomly selects a secret key x_a, where $\gcd(x_a, p-1)$, and find's the public key

$$y_a \equiv g^{x_a} \pmod{p_1} \tag{1}$$

The System center (hospital) also randomly selects a secret key x_b, and find's its public key

$$y_b \equiv g^{x_b} \pmod{p_1} \tag{2}$$

The Doctor randomly selects a secret key x_c, and find's its public key

$$y_c \equiv g^{x_c} \pmod{p_1} \tag{3}$$

The Bureau (Health Bureau) randomly selects a secret key x_d, and find's its public key

$$y_d \equiv g^{x_d} \pmod{p_1} \tag{4}$$

They did not publish their secret key but did publish their public key. Every users randomly chooses two large primes numbers p_i and q_i, and find's n_i where

$$n_i = p_i \cdot q_i \tag{5}$$

$$\phi(n_i) = (p_i - 1)(q_i - 1) \tag{6}$$

computes e_i, since $\gcd(e_i, \phi(n_i)) = 1$, to find

$$e_i \cdot d_a \equiv 1 \pmod{n_a} \tag{7}$$

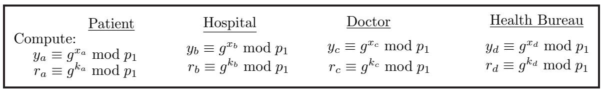
Patient
Compute:
$y_a \equiv g^{x_a} \bmod p_1$
$r_a \equiv g^{k_a} \bmod p_1$
Hospital
$y_b \equiv g^{x_b} \bmod p_1$
$r_b \equiv g^{k_b} \bmod p_1$
Doctor
$y_c \equiv g^{x_c} \bmod p_1$
$r_c \equiv g^{k_c} \bmod p_1$
Health Bureau
$y_d \equiv g^{x_d} \bmod p_1$
$r_d \equiv g^{k_d} \bmod p_1$

Figure 2. The System Initializing Phase.

3.2 Registration Phase

Patient randomly select a number k_a as their secret key to satisfy $\gcd(k_a, p-1)$, and calculate their parameters such as r_a, Reg_a as Equations (8) and (9), see Figure 3.

$$r_a \equiv g^{k_a} \pmod{p} \tag{8}$$

and

$$Reg_a \equiv (y_a \cdot r_a)^{d_a} \pmod{n_a}. \tag{9}$$

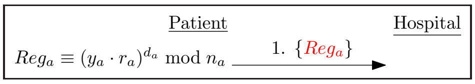

Figure 3. The Registration Phase.

3.3 Passing Account Phase

When receiving the Reg_a of the patients' registration, the system center will verify and reply $Pass_a$ by Equation (10) and Figure 4.

$$Pass_a \equiv (Reg_a)^{e_a \cdot x_b} \cdot y_c^{x_b} \pmod{n_a} \tag{10}$$

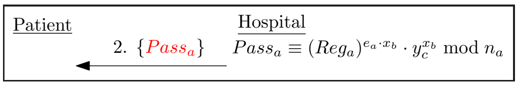
Patient
Hospital
2. $\{Pass_a\}$
$Pass_a \equiv (Reg_a)^{e_a \cdot x_b} \cdot y_c^{x_b} \bmod n_a$

Figure 4. The Passing Account Phase.

3.4 Meeting the Doctor Phase

Patient uses his account to see a doctor after went to hospital, and communicate with doctor about the situation where m_a express message, see Equation (11) and Figure 5.

$$Saw_a \equiv (Pass_a \cdot m_a)^{d_a} \pmod{n_a} \tag{11}$$

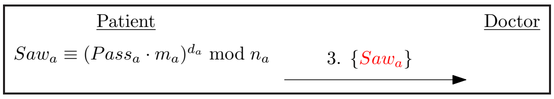

Figure 5. The Watching Doctor Phase.

3.5 Filling Records Phase

Doctor fills the record before he diagnosed patient and connected to hospital information system, see Equation (12) and Figure 6.

$$Que_a \equiv y_b^{Saw_a} \cdot Saw_a^{x_c} \cdot r_d^{k_c} \cdot r_b^{k_c} \pmod{p_1} \tag{12}$$

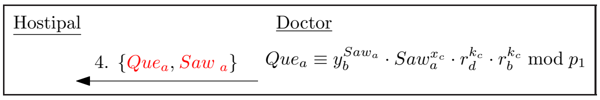
Hostipal
Doctor
4. $\{Que_a, Saw_a\}$
$Que_a \equiv y_b^{Saw_a} \cdot Saw_a^{x_c} \cdot r_d^{k_c} \cdot r_b^{k_c} \bmod p_1$

Figure 6. The Filling Records Phase.

3.6 Updating Records Phase

When system received the records from doctor, it firstly uses the public key e_a of RSA to check Equation (13), if it is hold, it then updates the records before connected to central host at Health Bureau, see Equation (14) and Figure 7.

$$Saw_a^{e_a} \overset{?}{\equiv} (Pass_a \cdot m_a) \pmod{n_a} \tag{13}$$

$$Upd_a \equiv Que_a \cdot r_d^{k_b} \cdot r_c^{-k_b} \pmod{p_1} \tag{14}$$

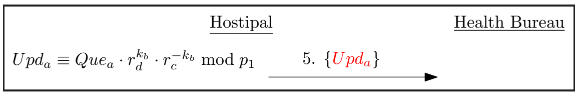
Hostipal
Health Bureau
$Upd_a \equiv Que_a \cdot r_d^{k_b} \cdot r_c^{-k_b} \bmod p_1$
5. $\{Upd_a\}$

Figure 7. The Updating Records Phase.

3.7 Checking Records Phase

Health Bureau obtained the data from hospital, he uses his secret key x_d to endorse this record, and send back synchronizing message, namely Equation (15), (16) and Figure 8.

$$Chk_0 \equiv Upd_a \cdot r_b^{-k_d} \pmod{p_1} \tag{15}$$

$$Chk_a \equiv Chk_0 \cdot r_c^{-k_d} \pmod{p_1} \tag{16}$$

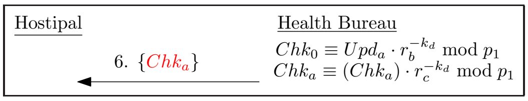
Hostipal
Health Bureau
6. $\{Chk_a\}$
$Chk_0 \equiv Upd_a \cdot r_b^{-k_d} \bmod p_1$
$Chk_a \equiv (Chk_a) \cdot r_c^{-k_d} \bmod p_1$

Figure 8. The Checking Records Phase.

3.8 Diagnosing Phase

After hospital synchronized and updated the data, it can provide to doctor upon on the diagnosis phase, see Equation (17) and Figure 9.

$$Diag_a \equiv Chk_a \cdot r_c^{k_b} \pmod{p_1} \tag{17}$$

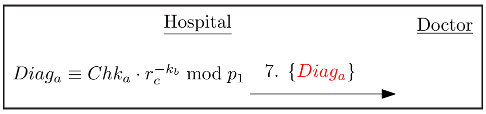

Figure 9. The Diagnosing Phase.

3.9 Feedback Result Phase

Doctor can write medical records and prescriptions for patient, see Equation (18) and Figure 10.

$$Res_a \equiv Diag_a \cdot r_b^{-k_c} \cdot Saw_a^{-x_c} \cdot m' \cdot r_a^{k_c} \pmod{p_1} \quad (18)$$

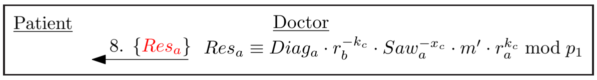
Patient
Doctor
8. $\{Res_a\}$
$Res_a \equiv Diag_a \cdot r_b^{-k_c} \cdot Saw_a^{-x_c} \cdot m' \cdot r_a^{k_c} \bmod p_1$

Figure 10. The Feedback Result Phase.

3.10 Take Medicine Phase

According from doctor's suggestions and prescriptions, patient take the drugs from hospital, see Equation (19) and Figure 11.

$$Pat_a \equiv Res_a \cdot y_b^{-Saw_a} \cdot r_c^{-k_a} \pmod{p_1} \qquad (19)$$

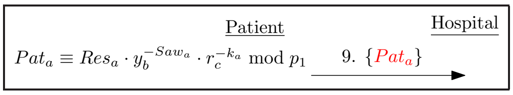
Patient
Hospital
$Pat_a \equiv Res_a \cdot y_b^{-Saw_a} \cdot r_c^{-k_a} \bmod p_1$
9. $\{Pat_a\}$

Figure 11. The Take Medicine Phase.

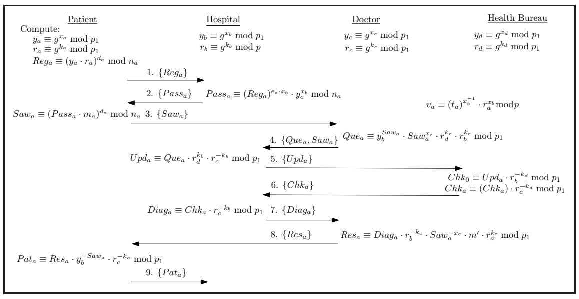
Patient
Hospital
Doctor
Health Bureau
Compute:
$y_a \equiv g^{x_a} \bmod p_1$
$r_a \equiv g^{k_a} \bmod p_1$
$Reg_a \equiv (y_a \cdot r_a)^{d_a} \bmod n_a$
$y_b \equiv g^{x_b} \bmod p_1$
$r_b \equiv g^{k_b} \bmod p$
$y_c \equiv g^{x_c} \bmod p_1$
$r_c \equiv g^{k_c} \bmod p_1$
$y_d \equiv g^{x_d} \bmod p_1$
$r_d \equiv g^{k_d} \bmod p_1$
1. $\{Reg_a\}$
2. $\{Pass_a\}$
$Pass_a \equiv (Reg_a)^{e_a \cdot x_b} \cdot y_c^{x_b} \bmod n_a$
$v_a \equiv (t_a)^{x_b^{-1}} \cdot r_a^{x_b} \mathrm{mod} p$
$Saw_a \equiv (Pass_a \cdot m_a)^{d_a} \bmod n_a$
3. $\{Saw_a\}$
4. $\{Que_a, Saw_a\}$
$Que_a \equiv y_b^{Saw_a} \cdot Saw_a^{x_c} \cdot r_d^{k_c} \cdot r_b^{k_c} \bmod p_1$
$Upd_a \equiv Que_a \cdot r_d^{k_b} \cdot r_c^{-k_b} \bmod p_1$
5. $\{Upd_a\}$
$Chk_0 \equiv Upd_a \cdot r_b^{-k_d} \bmod p_1$
$Chk_a \equiv (Chk_a) \cdot r_c^{-k_d} \bmod p_1$
6. $\{Chk_a\}$
$Diag_a \equiv Chk_a \cdot r_c^{-k_b} \bmod p_1$
7. $\{Diag_a\}$
8. $\{Res_a\}$
$Res_a \equiv Diag_a \cdot r_b^{-k_c} \cdot Saw_a^{-x_c} \cdot m' \cdot r_a^{k_c} \bmod p_1$
$Pat_a \equiv Res_a \cdot y_b^{-Saw_a} \cdot r_c^{-k_a} \bmod p_1$
9. $\{Pat_a\}$

Figure 12. The Flow of Our Scheme Protocol.

this is .....

4. Security Analysis

Definition 1. *(Discrete Logarithm Problem, DLP) Discrete Logarithm Problem [22] $DLP(p, g, y_i)$ is a problem that on input a prime p and integers g, $y_i \in Z_p^*$, outputs $x_i \in Z_{p-1}$ satisfying $g^{x_i} \equiv y_i \pmod{p}$ if such an x_i exists. Otherwise, it outputs Ω.*

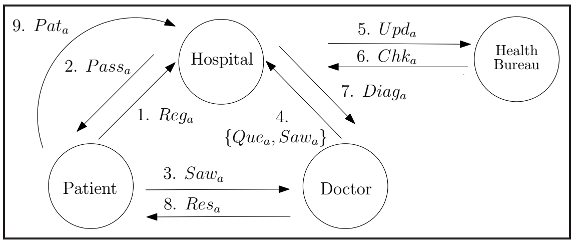

Figure 13. Concept of Personal Medical Records Based on Cryptographic Protocol.

Definition 2. *(Computational Square-Root Exponent, CSRE) $CSRE(p, g, y_i)$ is a problem that on inputting a prime p and integers $g, y_i \in Z_p^*$, outputs $g^{x_i} \pmod{p}$ for $x_i \in Z_{p-1}^*$ satisfying $y_i \equiv g^{x_i^2} \pmod{p}$ if such an x_i exists. Otherwise, it outputs $\perp$.*

The function above will output if there is no solution for a query. This should be expressed as CSRE*, as the CSRE notation is used when a weaker function has no solution to the query [23]. This study, however, will evaluate stronger functions only and will omit the asterisk for the remainder of the paper. Many cryptosystems are designed on the basis of the DLP [22], but most of them have the security equivalent of a weaker variant of DLP rather than DLP itself. The two most important weaker variants are as follows.

Definition 3. *(The Computation Diffie-Hellman Problem, CDHP) [24], [25] Given (g, g^x, g^y), compute g^{xy}.*

Definition 4. *(The Decisional Diffie-Hellman Problem, DDHP) [26] Given (g, g^x, g^y, g^z), decide whether $z = xy$ in $\mathbb{Z}_p$.*

4.1 Theoretical Security

Lemma 1. *If the patient is honest, the Equation (13) holds.*

Proof. $(Saw_a)^{e_a} \overset{?}{\equiv} (Pass_a \cdot m_a) \pmod{n_a}$.
Since $Saw_a \equiv (Pass_a \cdot m_a)^{d_a} \pmod{n_a}$ by Equation (11), we get $(Saw_a)^{e_a} \equiv (Pass_a \cdot m_a) \pmod{n_a}$ through RSA algorithm theorem, and $Reg_a \equiv (y_a \cdot r_a)^{d_a} \pmod{n_a}$ by Equation (9), where $r_a \equiv g^{k_a} \pmod{p_1}$ from Equation (8).
Checks $(Reg_a)^{e_a} \equiv (y_a \cdot r_a) \pmod{n_a}$.

$$\begin{aligned} (Reg_a)^{e_a} &\overset{?}{\equiv} [(y_a \cdot r_a)^{d_a}]^{e_a} \pmod{n_a} \\ &\equiv (y_a \cdot r_a) \pmod{n_a} \qquad (20) \end{aligned}$$

As mentioned above, the Equations (1), (8), (9), (10) and (11) hold, indicating that the patient's identity is correct and valid. □

Lemma 2. *If the system center is honest, the Equations (2), (10), (14), and (17) hold.*

Proof. 1) Honesty to patients. 2) Be honest with the authority. 3) Honesty with doctors.

1) If system center deceived, the Equation (13) cannot be established. Unless the patient and the hospital conspire, however, this link at least needs the doctor to become a tripartite conspiracy, otherwise it cannot be established. Lemma 1 proves that the patient and the hospital are honest with each other, otherwise Lemma 1 is contradictory, so the system center is also honest with the patient.
2) The integrity of the system center to the health bureau. As known from Equation (12), the doctor generates parameter Que_a and then sent to system center before the center signed its Upd_a. The center transmitted to Health bureau, while Health bureau return the Chk_a to center health. The system center found

$$Chk_a \overset{?}{\equiv} y_b^{Saw_a} \cdot Saw^{x_c} \pmod{p_1}. \tag{21}$$

Since the Equation (21) be generated by doctors, doctor has to calculates Equation (12) before both system center and health bureau signed its parameters. Doctor then obtained Equation (21). In other words, the Equation (21) must be signed by both system center and health bureau before calculation. Therefore, when health bureau sends back Equation (16) to system center, it indicates that both the system center and the health bureau have completed the authentication each others. On the other hand, when the system center passes Equation (17) to the doctor, the doctor can verify

$$y_b^{Saw_a} \cdot Saw_a^{x_c} \overset{?}{\equiv} Diag_a \cdot r_b^{-k_c} \pmod{p_1}. \tag{22}$$

If holds, it indicates that the system center and the doctor have completed the authentication each others. Therefore, from Equation (12) to Equation (17), it means that the system center, the doctor and the health bureau jointly complete the tripartite authentication.
3) If system center is honest with doctors, the Equation (12) and (17) holds. As known from Equation (17)

$$Diag_a \overset{?}{\equiv} Chk_a \cdot r_c^{-k_b} \pmod{p_1}. \tag{23}$$

If Equation (22) does not equal to (23), then there must be a cheat between of the system center and the doctor. However, this is inconsistent with point (II) of Lemma 2, so the system center and the doctor are honest with each other and cannot deny each other's signing behavior.

□

Lemma 3. *If the doctor is honest, the Equations (12), (18) and (19) hold.*

Proof. As known the doctors, the system center and the health bureau do not deny each other, it means that the tripartite: doctor, system center and health bureau are honest with each other, which is proved by points (II) and (III) of Lemma 2. But it doesn't mean the doctors are honest with patients. If the doctor carries out forwarding attack; for example, to Equations (11) and (12), it is simply forwarded to the system center, and the system center only verifies whether Equation (13) is effective, which does not guarantee the honesty of the doctor to the patient, but it shows the blind spot of the system here. However, the Equation (18) can rewrites as

$$Res_a \overset{?}{\equiv} y_b^{Saw_a} \cdot m' \cdot r_c^{k_c} \pmod{p_1}. \tag{24}$$

Its factors $r_a^{k_c}$ have bound and authenticated with patients and doctors. If doctors cheat, patients cannot be calculated m' by Equation (19), this is a contradictory to Equation (18). Reviewing Lemma 1, Lemma 2 and Lemma 3, the authors proved the quartet patients, system center, doctors and health bureau are independent of each other, but they should be honest and do not deny each other. Otherwise, from Equation (9) to Equation (19), if one of the steps is wrong, all the stages will be wrong. It has the effect of fail to stop [27]. □

4.2 Practical Security

Scenario 1: If attacker want to find the private key such as x_a, (x_b, x_c, x_d) and nonce value k_a by public key y_a (y_b, y_c, y_d), he would challenge the discrect logarithm problem.

Scenario 2: Only patient computes Saw_a since he owns his secret key d_a where $Saw_a \equiv (Pass_a \cdot m_a)^{d_a} \pmod{n_a}$ through Equation (11). If attacker wants to guess patient's identified, he has to guess the RSA's secret key "d_a". However, it is a big challenge to break the RSA cryptosystem [28]. Thus, the attacker does not face the DLP, he also meet decomposing the product of two large primes. That's dual complexity.

Scenario 3: The doctor and hospital (system center) can not mutually deny each other. Since Que_a is produced by the doctor where he uses his secret key x_c to find Equation (12). On the other hand, the hospital uses his nonce key k_b to calculate Equation (17). It doesn't matter which side is liar. If someone cheats to another ones, this scheme will fail to stop; else it is a contradiction. The Lemma 2 and Lemma 3 gave good provable security.

Scenario 4: We did not assume while health bureau be hacked this situation. If health bureau honest, he would use his semi key k_d to compute Equation (15) and (16) before send back to hospital; if Equation (25) is hold

$$Chk_a \overset{?}{\equiv} y_a^{Saw_a} \cdot Saw_c^{x_c} \pmod{p_1}, \tag{25}$$

otherwise that is contradiction.

5. Conclusions

In summary, this study contributes to the current knowledge by offering an innovative method of secured data transmission based on the features of blockchain technology. Their adaption in encryption and decryption can enable a dynamic authentication mechanism for each receiver for better outcomes both on security and efficiency. Further application in different areas and how to scale up its employment can be considered in future work.

Acknowledgments

The authors would like to thank the anonymous reviewers for their useful comments. This work is partially supported from university project under the number NUIT2020-001. This work also partially supported by Guandong province special funds to foster the student's science and technology innovation under the number PDJH2020B0689 (Climbing program funds).

References

[1] X. Yue, H. Wang, D. Jin, M. Li, and W. Jiang, "Healthcare data gateways: Found healthcare intelligence on blockchain with novel privacy risk control," *Journal of Medical Systems*, vol. 40, no. 10, pp. 218:1–8, October 2016.

[2] C. C. Agbo, Q. H. Mahmoud, and J. M. Eklund, "Blockchain technology in healthcare: A systematic review," *Healthcare*, vol. 7, no. 2, p. 56, 2019.

[3] S. Khezr, M. Moniruzzaman, A. Yassine, and R. Benlamri, "Blockchain technology in healthcare: A comprehensive review and directions for future research," *Applied Sciences*, vol. 9, no. 9, p. 1736, 2019.

[4] A. Hasselgren, K. Kralevska, D. Gligoroski, S. A. Pedersen, and A. Faxvaag, "Blockchain in healthcare and health sciences–a scoping review," *International Journal of Medical Informatics*, vol. 134, p. 104040, 2020.

[5] H. M. Hussien, S. M. Yasin, N. I. Udzir, M. I. H. Ninggal, and S. Salman, "Blockchain technology in the healthcare industry: Trends and opportunities," *Journal of Industrial Information Integration*, vol. 22, p. 100217, June 2021.

[6] C.-M. F. Chiang, "Medical research and personal-data protection–take Japanese epidemiology research as the basis," *Technology Law Review*, vol. 10, no. 1, pp. 61–113, 2013.

[7] S. Park, G. J. Choi, and H. Ko, "Information technology-based tracing strategy in response to COVID-19 in South Korea-privacy controversies," *JAMA*, vol. 323, no. 21, pp. 2129–2130, June 2020.

[8] D. Bouslimi and G. Coatrieux, "A crypto-watermarking system for ensuring reliability control and traceability of medical images," *Signal Processing: Image Communication*, vol. 47, pp. 160–169, September 2016.

[9] M. K. Abdmouleh, A. Khalfallah, and M. S. Bouhlel, "A novel selective encryption scheme for medical images transmission based-on JPEG compression algorithm," *Procedia Computer Science*, vol. 112, pp. 369–376, 2017.

[10] N. Zermi, A. Khaldi, K. Redouane, K. Fares, and E. Salah, "A DWT-SVD based robust digital watermarking for medical image security," *Forensic Science International*, vol. 320, p. 110691, 2021.

[11] A. Anand and A. K. Singh, "An improved DWT-SVD domain watermarking for medical information security," *Computer Communications*, vol. 152, pp. 72–80, February 2020.

[12] J. Fang, C. Liu, and S. C.-I. Chen, "Toward security and confidentiality in personal health records via blockchain technology," *Basic and Clinical Pharmacology and Toxicology*, vol. 126, no. S5, p. 10, April 2020.

[13] C. Liu, J. Fang, S. C.-I. Chen, and D. Gardner, "Study of anonymous complaint system based on patient-doctor and hospital tripartite scheme," *Basic and Clinical Pharmacology and Toxicology*, vol. 126, no. S5, pp. 11–12, April 2020.

[14] J. Wu and C. Liu, "A study of anonymous delivery based on blind signature scheme," *Procedia Computer Science*, vol. 52, pp. 1065–1070, 2015.

[15] J. Wu, C. Liu, and D. Gardner, "A study of anonymous purchasing based on mobile payment system," *Procedia Computer Science*, vol. 83, pp. 685–689, 2016.

[16] C. Zhang, Y.-Z. Luo, C. Liu, and B. Zhao, "A dynamic passcode system for mobile purchasing without bank card," in *2018 9th International Symposium on Parallel Architectures, Algorithms and Programming (PAAP)*, 2018, pp. 111–113.

[17] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the ACM*, vol. 21, no. 2, pp. 120–126, Feb. 1978.

[18] T. ElGamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," *IEEE Transactions on Information Theory*, vol. 31, no. 4, pp. 469–472, 1985.

[19] Y. Lv, C. Liu, and T. Huang, "Research on the university library anonymous customer complaint system based on blockchain technology," *Design Engineering*, no. 2, pp. 681–689, 2021.

[20] D. V. Dimitrov, "Blockchain applications for healthcare data management," *Healthcare Informatics Research*, vol. 25, no. 1, pp. 51–56, 2019.

[21] D. Manset, L. Berna, M. Koscina, and O. P. Kempner, "Blockchain and GDPR compliance for the healthcare industry," *Health Management*, vol. 19, no. 1, pp. 41–44, 2019.

[22] W. Feng, Y.-G. He, H.-M. Li, and C.-L. Li, "Image encryption algorithm based on discrete logarithm and memristive chaotic system," *The European Physical Journal Special Topics*, vol. 228, no. 10, pp. 1951–1967, October 2019, 10.1140/epjst/e2019-800209-3.

[23] C. KONOMA, M. MAMBO, and H. SHIZUYA, "Complexity analysis of the cryptographic primitive problems through square-root exponent," *IEICE TRANSACTIONS on Fundamentals of Electronics, Communications and Computer Sciences*, vol. E87-A, no. 5, pp. 1083–1091, May 2004.

[24] N. Döttling and S. Garg, "Identity-based encryption from the Diffie-Hellman assumption," in *Advances in Cryptology–CRYPTO 2017*, J. Katz and H. Shacham, Eds. Cham: Springer International Publishing, 2017, pp. 537–569.

[25] Z. Hu, S. Liu, K. Chen, and J. K. Liu, "Revocable identity-based encryption and server-aided revocable IBE from the Computational Diffie-Hellman assumption," *Cryptography*, vol. 2, no. 4, 2018. [Online]. Available: https://www.mdpi.com/2410-387X/2/4/33

[26] Y. Wen, S. Liu, and S. Han, "Reusable fuzzy extractor from the decisional Diffie-Hellman assumption," *Designs, Codes and Cryptography*, vol. 86, no. 11, pp. 2495–2512, November 2018, 10.1007/s10623-018-0459-4.

[27] G. Bleumer, *Fail-Stop Signature*. Boston, MA: Springer US, 2005, pp. 213–215.

[28] F. Boudot, P. Gaudry, A. Guillevic, N. Heninger, E. Thomé, and P. Zimmermann, "Comparing the difficulty of factorization and discrete logarithm: A 240-digit experiment," in *Advances in Cryptology–CRYPTO 2020*, D. Micciancio and T. Ristenpart, Eds. Cham: Springer International Publishing, 2020, pp. 62–91.