*Computer Systems Science & Engineering*
DOI:10.32604/csse.2021.015004
***Article***

Tech Science Press

# Front-end Control Mechanism of Electronic Records

**Jiang Xu[1], Ling Wang[1,2], Xinyu Liu[1,2], Xiujuan Feng[3], Yongjun Ren[1,2,*] and Jinyue Xia[4]**

[1]School of Computer and Software, Engineering Research Center of Digital Forensics, Ministry of Education, Nanjing University of Information Science & Technology, Nanjing, 210044, China
[2]Jiangsu Collaborative Innovation Center of Atmospheric Environment and Equipment Technology (CICAEET), Nanjing University of Information Science & Technology, Nanjing, 210044, China
[3]School of Mines, China University of Mining and Technology, Xuzhou, 221116, China
[4]International Business Machines Corporation (IBM), NY, USA
[*]Corresponding Author: Yongjun Ren. Email: renyj100@126.com

Received: 01 November 2020; Accepted: 22 March 2021

**Abstract:** In the digital era, how to ensure the authenticity and integrity of electronic records has become an open challenging issue. Front-end control is an important concept as well as a basic principle in electronic record management. Under the instruction of front-end control, many original management links in the record-management stage are required to move forward, and the managers enter the formation stage of the electronic records to ensure the originality. However, the front-end control technique primarily focuses on transaction management, and it lacks the strategy of providing the control of electronic records. In this paper, a novel electronic record front-end control mechanism is proposed by adopting proxy re-encryption and requiring archivists to participate in the management of electronic records before the record is created to solve the problem. Specifically, when an electronic record is generated, the proposed mechanism interacts with the producer of the electronic record to generate a corresponding encryption key. Moreover, electronic records are encrypted by the key to protect their confidentiality, which can prevent the leakage of electronic record information. In addition, when transferring the electronic record, archivists use proxy re-encryption technology to convert electronic records, allowing management by an archivist, ensuring their originality and authenticity.

**Keywords:** Electronic record; front-end control; proxy re-encryption

## 1 Introduction

It is widely acknowledged that front-end control is an important idea and basic principle of electronic records management, which is based on record life cycle theory. This concept also emphasizes that control of the electronic record starts at the beginning of its life cycle and runs through the entire archive management process [1–3]. Under the guidance of front-end control, many management links that belonged originally to the record management stage need to be advanced to the electronic record formation stage. The goal is to capture and control relevant records and information as required, as well as to meet the filing and archival preservation demands for electronic records [4–6]. This is the key to ensuring the originality and authenticity of electronic records from the source, and also aids in avoiding the distortion, loss and inadequate control of electronic records.

At present, the front-end management of electronic records mainly focuses on dividing the electronic record formation process into specific record management functions. According to the functions, the electronic record formation process can be subdivided into the following six stages: generate, capture, integrate, solidify, register, and audit trail [7–9]. However, the front-end management of electronic records focuses primarily on transaction management at present. In addition, there are few technical means available to support it. To solve this problem, this paper proposes a front-end control method of electronic records based on proxy re-encryption. In the proposed mechanism, the archivist and the producer of the electronic records interact before the electronic record is created. Moreover, when the electronic record is transferred from the producer to the archivist, proxy re-encryption technology is used to ensure its originality and authenticity [10–12].

## 2 Related Work

The front-end control of electronic records is based on the digital characteristics of these records, which are totally different from those of paper records [13–15]. According to record life cycle theory and the whole-process control principle, the objectives, requirements and rules of the entire electronic record management process are systematically analyzed. In this way, during the design phase of the electronic record system, the management functions implemented in the electronic record formation phase can be planned as uniformly as possible. Moreover, effective supervision should be conducted during the record formation and maintenance stage; this will ensure that the content, background and structure of electronic records are not changed or lost, keep it consistently, thereby providing better assurance of the authenticity, integrity, readability and availability of electronic records [16–18].

According to record life cycle theory, electronic records have a life cycle in a similar way to paper records. The management of electronic records is a systematic process that runs through the entire life cycle when records are generated. Throughout the whole life cycle, records may be changed or lost at any time for various reasons and purposes [19–21]. Accordingly, the archive scope and preservation value should be determined before records are produced, at the design phase, and corresponding protection technology should be adopted. If the archive management organization waits passively, some valuable records may be lost, or received records may be mislaid or out of date. Front-end control should focus on the overall planning of the entire record operation process. Supervision should be implemented during the record formation and maintenance phase. In other words, the value of archives should be identified during the record formation stage, with a focus on the entire record life cycle, extending the protection work forward and reflecting its foresight [22–24]. Intervening from the beginning of record formation and taking corresponding protection measures for valuable records can thus effectively prevent leakage or the destruction of records by other links. This will maximize work efficiency and realize comprehensive record management in a true sense.

The ideological root of front-end control was first developed by the French archivist C. Nogales, who stated that “Archivists need to rethink the timing of their interventions in the record life cycle, even rethink the life cycle itself” [25–27]. The Guidelines for the Management of Electronic Records (Draft) prepared by the Electronic Records Committee of the International Archives Council also dedicates significant space to the importance of rethinking the electronic record life cycle and the appropriate time to intervene in this life cycle. Eventually, this work determines that the “time to intervene” is at the design stage of the electronic record management system; it further puts many “post control” means in the original paper record management system at the front end, and advocates “taking action before record formation” [28–30].

## 3 Problem Statement

With the rapid development of the information age, the number of electronic records is increasing day by day, exhibiting an exponential growth trend. Information waste is also increasing, which is generating more interest in the use of front-end control to avoid generating electronic records without practical significance [31–33].

The quality of electronic records is variable. In the era of electronic records, due to the influence of traditional habits, along with the convenience and operability of sending records, the number of resulting records is much higher than in the traditional environment, and their quality is also uneven [34–36]. Therefore, to ensure the record's certificate, it is necessary to control the front-end.

The security of electronic records is expected to be guaranteed. Because of their unique characteristics, matters of their security are more serious than those pertaining to paper records [37–39]. It is thus urgent to strengthen the front-end control of electronic records. Electronic records exhibit a separation between information and carrier, as well as dependence on the system. Following technical innovation or improper operation, the recorded information content may be easily lost or become a “dead record”; resolving this situation also requires proper front-end control of electronic records.

The current situation in the field of electronic records management is worrying. At present, electronic record management typically adopts the “double set system” management method and multi-carrier backup. This not only demonstrates that the legal effect of electronic records has not yet been finally confirmed, but also reflects people's distrust of the security of electronic records management systems. The current situation of electronic records management and the popularization of electronic records management systems therefore needs to be addressed [40–42]. Therefore, to ensure that electronic records can be safely saved, uploaded and released, it is also necessary to control the front-end.

As electronic records are processed by means of computers and network technology, it is easy to add, delete and modify electronic records without leaving any trace. This causes a loss of originality and authenticity for electronic records. The authenticity of electronic record content is linked with the premise of its original record formation and the role of investigation [43–45]. The original voucher checking function is also an underlying principle of electronic records: without this function, there could be no electronic records. In addition, the content of electronic records can be read by any terminal device on the network, which puts the electronic record itself and its verification and security at risk.

In order to ensure the authenticity of electronic records, we can use “front-end control” technology. That is to say, in the formation stage of electronic records, the value of archives should be identified, with filing marks added as needed to prevent records from being modified or deleted. This approach fundamentally breaks the traditional management mode and the boundary between records and archives, enabling archives departments to intervene in the life cycle of records in advance [46–48]. Adopting this approach can thus effectively prevent leakage or the destruction of electronic records by other links, thereby maximizing work efficiency and enabling truly comprehensive record management to be realized. Front-end control is therefore an important method for ensuring the authenticity and originality of archived records.

## 4 Front-end Control Mechanism of Electronic Records Based on Proxy Re-encryption

After an electronic record is generated, it is encrypted by the record producer. When the electronic record is transferred from the producer to the archivist, the archivist re-encrypts it. In this way, the front-end management of electronic records can be realized.

## 4.1 Preliminaries

### 4.1.1 Definition 4.1: Bilinear Pairings

$G_1$ is a cyclic group of prime order $p$, while $g$ is any generator element in $G_1$; $G_2$ is a multiplicative cyclic group of the same order as $G_1$. The bilinear pairing $e : G_1 \times G_2 \rightarrow G_2$ is a mapping that satisfies the following properties.

Bilinear: For any $a, b \in Z_p, g_1, g_2 \in G_1$, there is $e(g_1^a, g_2^b) = e(g_1, g_2)^{ab}$.

- Non-degradation: For any $g_1, g_2 \in G_1$, make $e(g_1, g_2) \neq I_G$, where $I_G$ is the unit element of the group $G_2$.

- Computability: For any $g_1, g_2 \in G_1$, there is an effective algorithm for calculating $e(g_1, g_2)$. A Weil pair and Tate pair can be used on an elliptic curve to construct an effective bilinear pair.

### 4.1.2 Definition 4.2: Hypothesis 3-QDBDH

$e : G_1 \times G_1 \rightarrow G_2$ is a bilinear pairing. The advantage function $Adv_{G_1,B}^{3-QDBDH}(\lambda)$ of PPT adversary B is defined as follows:

$$|\Pr[B(g, g^{x2}, g^{x2}, g^{x3}, g^z, e(g,g)^{z/x})] = 1 - \Pr[B(g, g^{x2}, g^{x2}, g^{x3}, g^z, e(g,g)^r)] = 1| \tag{1}$$

Here, $x, z, r \in Z_p$, and they are randomly selected. If, for all probabilistic polynomial time (PPT) adversaries B,$Adv_{G_1,B}^{3-QDBDH}(\lambda)$ is negligible, then the hypothesis 3-QDBDH holds.

### 4.1.3 Definition 4.3: Hypothesis Truncated q-ABDHE

$e : G_1 \times G_1 \rightarrow G_2$ is a bilinear pairing. The advantage function $Adv_{G_1,B}^{q-ABDHE}(\lambda)$ of PPT adversary B is defined as follows:

$$|\Pr[B(g, g^x, \ldots, g^{x^q}, g^z, g^{zxq+2}, e(g,g)^{zx^{q+1}})] = 1 - \Pr[B(g, g^x, \ldots, g^{x^q}, g^z, g^{zxq+2}, e(g,g)^r)] = 1| \tag{2}$$

Here, $x, z, r \in Z_p$, and they are randomly selected. The distribution above is recorded as $P_{q-ABDHE}$ and the distribution above is recorded as $R_{q-ABDHE}$. If $Adv_{G_1,B}^{q-ABDHE}(\lambda)$ is negligible for all PPT adversaries B, then the truncated q-ABDHE hypothesis holds.

## 4.2 Re-encryption Scheme for Electronic Records

The scheme is defined as follows:

- *GloSetup*$(\lambda)$: $\lambda$ is the security parameter, $(p, g, G_1, G_2, e)$ is the parameter of the bilinear pair, $u, v(u, v \in G_1)$ represent the generators of $G_1$, and $Sig = (G, S, V)$ is a signature. The message field is $G_2$, the conditional field is $Z_p{}^*$, and the public parameter is $GP = (p, g, G_1, G_2, e, u, v, Sig)$.

- *KeyGen*$(i)$: The electronic records producer $i$ chooses the random number $x_i, y_i, a_0, a_1, a_2 \in Z_p{}^*$, and calculates $X_i = g^{x_i}$,$Y_i = g^{y_i}$,$h_k = g^{a_k}$. Its public key is set to $pk_i = (X_i, Y_i, \{h_k\}_{k\in\{0,1,2\}})$ and its private key to $sk_i = (pk_i, x_i, y_i, a_0, a_1, a_2)$.

- *RKeyGen*$(sk_i, pk_j)$: Given the user $i$'s private key $sk_i = (pk_i, x_i, y_i)$ and the user $j$'s public key, a one-way partial re-encryption key $rk_{i,j} = X_j{}^{1/x_i}$ is generated.

- *CKeyGen*$(sk_i, w)$: Given the electronic records producer $i$'s private key $sk_i$ 's $x_i$ and the condition $w \in Z_p{}^*$, select three random numbers $s_k \in Z_p{}^*$, calculate $d_k = (h_k g^{-s_k})^{1/(y_i - w)}$, and set the conditional key as $ck_{i,w} = (d_k, s_k)_{k\in\{0,1,2\}}$.

- *Enc*$(pk_i, m, w)$: To encrypt the electronic records $m \in G_2$ with public key$pk_i$ and conditions $w \in Z_p{}^*$, the electronic records producer takes the following steps.

I) Select a strongly unforgivable signature, set the key pair as $(ssk, svk) \leftarrow G(\lambda)$, and set $C_1 = svk$.

II) Select $r \in Z_p{}^*$ at random and calculate $C_2 = X_i^r$, $C_3 = e(g, g)^r m$, and $C_4 = (u^{svk} v)^r$.

III) Generate a signature $\sigma = S(ssk, (C_3, C_4))$ for $(C_3, C_4)$, and the conventional cipher text is $CR_i = (C_1, C_2, C_3, C_4, \sigma)$.

IV) Select $r' \in Z_p{}^*$ at random and calculate $K = e(g, h_0)^{r'}$, $C_3{}' = C_3 K$, $G_5 = (Y_i g^{-w})^{r'}$, $G_6 = e(g, g)^{r'}$, $t = H(C_3{}', C_5, C_6), C_7 = e(g, h_1)^{r't} e(g, h_2)^{r'}$.

V) Generate another one-time signature: $\sigma' = S(ssk, (C_1, C_2, C_3{}', C_4, \sigma, C_5, C_6, C_7))$.

VI) Conditional cipher text original cipher text: $CT_i = (C_1, C_2, C_3{}', C_4, \sigma, C_5, C_6, C_7, \sigma')$.

- Re$Enc(CT_i, rk_{i,j}, ck_{i,w})$: Enter a partial re-encryption key $rk_{i,j} = X_j{}^{1/x_i}$, conditional key $ck_{i,w}$, and conditional cipher text$CT_i$. First, run $Test(CT_i, ck_{i,w})$, calculate $t = H(C_3{}', C_5, C_6)$, and test to determine whether the following formula is true: $V(C_1, \sigma'(C_1, C_2, C_3{}', C_4, \sigma, C_5, C_6, C_7)) = 1$ and $C_7 = e(C_5, d_1^t d_2) C_6^{s_1 t + s_2}$. Print "0" if the check fails or "1" otherwise; if the result is "1," calculate $K = e(C_5, d_0) C_6{}^{s_0}, C_3 = C_3{}'/K$. Accordingly, the conventional cipher text is $CR_i = (C_1, C_2, C_3, C_4, \sigma)$, and the following formula is tested to check its validity: $e(C_2, u^{C_1} v) = e(X_i, C_4)$, $V(C_1, \sigma, (C_3, C_4)) = 1$. If the preceding equation is true, $CT_i$ is re-encrypted, so that $t \in Z_p{}^*$ is selected at random and the following formulas are calculated: $C_2{}' = X_i{}^t$, $C_2{}'' = rk_{ij}{}^{1/t} = g^{(x_j/x_i)t^{-1}}, C_2{}''' = C_2{}^t = X_i^{rt}$, and the re-encryption cipher text is the following formula: $CT_j = (C_1, C_2{}', C_2{}'', C_2{}''', C_3, C_4, \sigma)$. If the equation is false, output the error symbol $\perp$.

- $Dec1(CT_i, sk_i)$: Enter private key $sk_i$, conditional cipher text $CT_i$, and break cipher text $CT_i = (C_1, C_2, C_3{}', C_4, \sigma, C_5, C_6, C_7, \sigma')$. If $V(C_1, \sigma'(C_1, C_2, C_3{}', C_4, \sigma, C_5, C_6, C_7)) = 1$, calculate $t = H(C_3{}', C_5, C_6)$, and then verify whether $C_7 = C_6{}^{a_1 t + a_2}$. If not, output $\perp$; if so, calculate $C_3 = C_3{}'/(C_6^{a_0})$. Therefore, the conventional cipher text is $CR_i = (C_1, C_2, C_3, C_4, \sigma)$. If the cipher text satisfies $e(C_2, u^{C_1} v) = e(X_i, C_4)$ and $V(C_1, \sigma, (C_3, C_4)) = 1$, $i$ can obtain $m = C_3 / e(C_2, g)^{1/x_i}$; otherwise, the algorithm outputs $\perp$.

- $Dec2(CT_j, sk_j)$: After entering the private key $sk_j$ and the re-encryption cipher text $CT_j = \left(C_1, C_2, C_2^{'}, C_2^{''}, C_3, C_4, \sigma\right)$, the validity of the re-encryption cipher text is checked by the following test: $e\left(C_2^{'}, C_2^{''}\right) = e\left(X_j, g\right)$, $e\left(C_2{}''', u^{C_1} v\right) = e(C_2{}', C_4)$, and $V(C_1, \sigma, (C_3, C_4)) = 1$. If both equations are true, output plaintext $m = C_3 / e(C_2{}'', C_2{}''')^{1/x_j}$; otherwise, the algorithm outputs the error sign $\perp$.

**Correctness**: Properly generated original re-encryption cipher text can be correctly decrypted. As shown below, re-encryption cipher text encrypted by a proxy without the correct encryption key or conditional key cannot be decrypted by the entrusting party. Given the original conditional cipher text $CT_i = (C_1, C_2, C_3{}', C_4, \sigma, C_5, C_6, C_7, \sigma')$ encrypted with the keyword $w$ and public key $pk_i$, two cases exist.

**Case 1** (incorrect conditional key): Assume that the proxy has a partial re-encryption key $rk_{i,j} = X_j{}^{1/x_i}$ and conditional keys $ck_{i,w'} = (d_k, s_k)_{k \in \{0,1,2\}}$, $d_k = (h_k g^{-s_k})^{1-(y_i - w')}$, and $w \neq w'$. Run Re$Enc(CT_i, rk_{i,j}, ck_{i,w'})$ to convert the cipher text $CT_i$ to the user $j$'s cipher text: obviously, $CT_i$ cannot pass the legality check.

Order $C_5 = (Y_i g^{-w})^{r'}$, $C_6 = e(g, g)^{r'}$, $t = H(C_3{}', C_5, C_6)$ and $C_7 = e(g, h_1)^{r't} e(g, h_2)^{r'}$. Then,

$$e(C_5, (d_1{}')^t (d_1{}')) C_6{}^{s_1{}' + s_2{}'} \neq e(g, h_1)^{r't} e(g, h_2)^{r'} = C_7 \quad (3)$$

$$\begin{aligned}
&\Leftrightarrow e(g^{(y_i-w)r'},(g^{(a_1-s_1{}')/(y_i-w')}))^t e(g^{(y_i-w)r'},g^{(a_2-s_2{}')/(y_i-w')})e(g,g)^{r'(s_1{}'t+s_2{}')}\neq C_7\\
&\Leftrightarrow e(g,g)^{r'(y_i-w)/(y_i-w')((a_1-s_1{}')t+(a_2-s_2{}'))}e(g,g)^{r'(s_1{}'t+s_2{}')}\neq e(g,g)^{(a_1t+a_2)r'}\\
&\Leftrightarrow ((a_1t+a_2)r'((y_i-w)/(y_i-w')-1))-((s_1{}'t+s_2{}')r'((y_i-w)/(y_i-w')-1))\neq 0\\
&\Leftrightarrow (a_1t+a_2-s_1{}'t-s_2{}')((w'-w)/(y_i-w'))\neq 0
\end{aligned}\tag{4}$$

Because $s_1{}'$ and $s_2{}'$ are randomly selected, $a_1,a_2,y_i$ comprise the private key. Therefore, $(a_1t+a_2-s_1{}'t-s_2{}')\neq 0$, $(w'-w)\neq 0$, and $(y_i-w')\neq 0$.

Even if it passes the validation test, it is still evident that $K'=e(C_5,d_0{}')C_6{}^{s_0{}'}\neq e(g,h_0)^{r'}=K$, because

$$K'=e(C_5,d_0{}')C_6{}^{s_0{}'}\neq e(g,h_0)^{r'}=K\tag{5}$$

$$\begin{aligned}
&\Leftrightarrow K'=e(g^{(y_i-w)r'},g^{(a_0-s_0{}')/(y_i-w')})e(g,g)^{r's_0{}'}\neq e(g,g)^{a_0r'}\\
&\Leftrightarrow e(g,g)^{r'(y_i-w)/(y_i-w')(a_0-s_0{}')}e(g,g)^{r's_0{}'}\neq e(g,g)^{a_0r'}\\
&\Leftrightarrow (a_0-s_0{}')r'((y_i-w)/(y_i-w')-1))\neq 0\\
&\Leftrightarrow (a_0-s_0{}')r'(w'-w)/(y_i-w')\neq 0
\end{aligned}\tag{6}$$

**Case 2** (incorrect re-encryption key): Assume that the proxy has a partial re-encryption key $rk_{i,j'}=X_{j'}{}^{1/x_i}$ and conditional keys $ck_{i,w}=(d_k,s_k)_{k\in\{0,1,2\}}$, $d_k=(h_kg^{-s_k})^{1-(y_i-w')}$, and $j\neq j'$. Run Re$Enc(CT_i,rk_{i,j},ck_{i,w'})$ to convert the cipher text $CT_i$ to the user $j$'s cipher text. Decompose $CT_j$ and set $C_2{}'=X_i^t,C_2{}''=rk_{ij'}{}^{1/t}=g^{(x_{j'}/x_i)t^{-1}}$ and $C_2{}'''=C_2{}^t=X_i^{rt}$. When decryption is conducted, $CT_j$ evidently cannot pass the legality check, because $e(C_2{}',C_2{}'')\neq e(X_j,g)$.

### *4.3 Safety Certificate*

**Theorem 1**: Assuming that the 3-QDBDH problem and q-ABDHE problem are difficult to solve, the above scheme for the re-encryption of electronic records is secure under the standard model.

**Lemma 1**: If an IND-CCA attacker exists that can attack the scheme in this paper, there is an algorithm 'B' that can solve the 3-QDBDH problem. To prove lemma 1, we first prove an assertion.

**Assertion 1**: The difficulty assumption of 3-QDBDH is equivalent to whether a given $(g,g^{1/a},g^a,g^{a_s},g^b)$ decides that $T$ is equal to $e(g,g)^{b/a^2}$ or a random value.

**Proof**: Given $(g,g^{1/a},g^a,g^{a_2},g^b)$, set up a 3-QDBDH instance by setting $\left(y=g^{1/a},y^x=g,y^{x^2}=g,y^{x^3}=g^{a^2},y^2=b\right)$; this implies $x=a,z=ab$. One then has $\mathrm{e}(g,g)^{z/x}=e\left(g^{1/a},g^{1/a}\right)^{(ab)/a}=e(g,g)^{b/a^2}$, which means that these two problems are equivalent, thereby completing the proof of Assertion 1.

**Proof of Lemma 1**: If there is a PPT attacker that can attack the scheme proposed in this paper, a simulator B exists that can solve the 3-QDBDH problem. The simulation proceeds as follows.

First, the challenger sets the groups $G_1$ and $G_2$, the bilinear pair $e$, and generator $g$ of group $G_1$. The simulator enters an instance of a q-ABDHE problem $(A_{-1}=g^{1/a},A_1=g^a,A_2=g^{a^2},B=g^b,T)$: the purpose of the simulator B is to distinguish $T=e(g,g)^{b/a^2}$, $T$ or a random number of group $G_2$.

$CT^*=(C_1{}^*,C_2{}^*,C_3{}'^*,C_4{}^*,\sigma^*,C_5{}^*,C_6{}^*,C_7{}^*,\sigma'^*)$ represents the challenge cipher text sent to A in the game. The event $F_{OTS}$ indicates that A performs A's decryption query and A's re-encryption query on the cipher text $CT^* = (C_1{}^*, C_2, C_3{}', C_4, \sigma, C_5, C_6, C_7, \sigma')$, but $V(C_1{}^*, \sigma', (C_1, C_2, C_3{}', C_4, \sigma, C_5, C_6, C_7, \sigma')) = 1$, or $V(C_1{}^*, \sigma(C_3, C_4)) = 1$.

In phase 1, $A$ has no information on the event $svk^*$, meaning that the probability of the previous event $F_{OTS}$ is no more than $q_k\theta$. $q_k$ denotes the total number of times the query was tested, while $\theta$ represents the maximum probability (no more than $1/p$) of a signature's verification key $svk^*$. In phase 2, $F_{OTS}$ presents an algorithm to break a signature. Therefore, $\Pr[F_{OTS}] \leq q_k/p + Adv^{OTS}$; the second part represents the probability of a signature being destroyed, which is also negligible. A detailed description of the $B$ simulation is now provided: when $F_{OTS}$ occurs, $B$ simply stops and output a random bit. During the preparation phase, $B$ generates a signature pair $(ssk^*, svk^*) \leftarrow G(\lambda)$ and provides public parameters to $A$, including $u = A_1{}^{\alpha_1}$ and $v = A_1{}^{-\alpha_1 svk^*} A_2{}^{\alpha_2}$, where $\alpha_1$ and $\alpha_2$ are random and $\alpha_1, \alpha_1 \in Z_p{}^*$. The set of honest participants is represented by $HU$, including the user $i^*$ specifying the public key $pk_{i^*}$, while $CU$ is the set of corrupted participants. The environment simulation of $A$ proceeds as follows.

(a) System setup: $\lambda$ is the security parameter, $(p, g, G_1, G_2, e)$ is the bilinear pair parameter, $u = A_1{}^{\alpha_1}$, and $v = A_1{}^{-\alpha_1 svk^*} A_2{}^{\alpha_2}$, where $\alpha_1$ and $\alpha_2$ are random, and $\alpha_1, \alpha_1 \in Z_p{}^*$. Generate a signature $Sig = (G, S, V)$. The public parameter is $GP = (p, q, G_1, G_2, e, u, v, Sig)$.

(b) Query phase 1: The attacker $A$ makes the following queries.

- Uncorrupted-key-generation query $\langle i \rangle$: The public key of the honest user $i \in HU \backslash \{i^*\}$ is defined as $X_i = (g^a)^{x_i} = g^{ax_i}$, while $x_i \in Z_p{}^*$ is random. Select $y_i, a_0, a_1, a_2 \in Z_p{}^*$ at random and calculate $Y_i = g^{y_i}, h_k = g^{a_k}$ . Then, set the public key to $pk_{i^*} = (x_{i^*}, y_{i^*}, \{h_{k^*}\}_{k \in \{0,1,2\}})$ and send to $A$.

- Corrupt-key-generation query $\langle j \rangle$: Considering the corrupt user $j \in CU$, select random numbers $\mathrm{x}_i, y_j, a_0, a_1, \mathrm{a}_2 \in Z_p^*$ and calculate $X_j = g^{x_j}, Y_j = g^{y_j}, h_k = g^{a_k}$. Set its public key $pk_j = (X_j, Y_j, \{h_k\}_{k \in \{0,1,2\}})$ and private key $sk_j = (pk_j, x_j, y_j, a_0, a_1, a_2)$, and send $(pk_j, sk_j)$ to $A$.

- Partial-re-encryption-key query $\langle pk_i, pk_j \rangle$: The following cases involving $B$ must be distinguished.

- If $i \in CU$, $B$ knows that $sk_i = (pk_i, x_i, y_i, a_0, a_1, a_2)$ and $X_j$ is given, such that it is easy to output the one-way re-encryption key $rk_{i,j} = X_j{}^{1/x_i}$.

- If $i \in HU \backslash \{i^*\}$ and $j = i^*$, $B$ returns a valid re-encryption key $rk_{i,i^*} = (g^{1/a})^{x_i/x_{i^*}} = g^{(ax_i)/(a^2 x_{i^*})}$.

- If $i = i^*, j \in HU \backslash \{i^*\}$, $B$ returns the correct distribution $rk_{i^*,i} = (g^{1/a})^{x_i/x_{i^*}} = g^{(ax_i)/(a^2 x_{i^*})}$.

- If $i, j \in HU \backslash \{i^*\}$, $B$ returns $rk_{i,j} = g^{x_j/x_i} = g^{(ax_j)/(ax_i)}$.

- Conditional key query $\langle pk_i, w \rangle$: $B$ selects $s_k \in Z_p{}^*$ at random and calculates $d_k = (h_k g^{-s_k})^{1/(y_i - w)}$.

- Re-encryption key query $\langle pk_i, pk_j, (w, CT_i) \rangle$: For the re-encryption key query of the conditional cipher text $CT_i = (C_1, C_2, C_3{}', C_4, \sigma, C_5, C_6, C_7, \sigma')$ from user $i$ to $j$, the conditional key is $ck_{i,w} = \{d_{w,k}, s_{w,k}\}_{k \in \{0,1,2\}}$ . Calculate $t = H(C_3{}', C_5, C_6)$, and then verify whether the following formula is true: $V(C_1, \sigma'(C_1, C_2, C_3{}', C_4, \sigma, C_5, C_6, C_7)) = 1$ and $C_7 = e(C_5, d_1^t d_2) C_6^{s_1 t + s_2}$. If the verification fails, output $\perp$; otherwise, calculate $K = e(C_5, d_0) C_6^{s_0}, C_3 = C_3{}'/K$, obtain the conventional cipher text $CR_i = (C_1, C_2, \mathrm{C}_3, C_4, \sigma)$ and check its validity by testing the following expressions:

$$e(C_2, u^{C_1} v) = e(X_i, C_4),$$
$$V(C_1, \sigma, (C_3, C_4)) = 1. \quad (7)$$

If the equation is not true, then $B$ returns $\perp$.

- If $i = i^*$ or $i = i^*, j \in HU \backslash \{i^*\}$, in both cases $B$ is encrypted with the re-encryption key $rk_{i,j}$.

- If $i = i^*$ and $j \in CU$:

i) If $C_1 = svk^*$, then $(C_1, C_2, C_3{}', C_4, \sigma, C_5, C_6, C_7, \sigma') \neq \left(C_1^*, C_2^*, C_3^*, C_4^*, \sigma^*, C_5^*, C_6^*, C_7^*, \sigma'^*\right)$, and $B$ is faced with the $F_{OTS}$ event and stops the game.

ii) Another possible situation is the following: $C_1 \neq svk^*$, $i = i^*, j \in CU$. At this time, ${C_2}^{1/x_{i^*}}$ is given from $C_4 = (u^{svk}v)^r = ((g^a)^{\alpha_1(svk-svk^*)}(g^{a^2})^{\alpha_2})^r$. $B$ calculates $(A_1)^r = (g^a)^r = (C_4/(C_2^{\alpha_2/x_{i^*}}))^{1/(\alpha_1(svk-svk^*))}$

and knows $(A_1)^r$ and user $j$'s private key. $B$ randomly selects $t \in {Z_p}^*$, calculates $C_2' = (A_1)^t = g^{at}$,$C_2'' = (A_{-1})^{x_j/t} = \left(g^{1/a}\right)^{x_j/t}$, $C_2''' = (A_1)^{rt} = X_i^{rt}$, and returns the correct cipher text $\mathrm{C}_j = \left(C_1, C_2', C_2'', C_2''', \mathrm{C}_3, \mathrm{C}_4, \sigma\right)$.

- Decryption query $\langle pk_i, CT_i\rangle$ or $\left\langle pk_j, CT_j\right\rangle$: If $\langle pk_i, CT_i\rangle$ represents a decryption query on the original conditional re-encryption cipher text $CT_j = (C_1, C_2, C_2', C_2'', C_3, C_4, \sigma)$, use the following formulae to check the validity of the re-encryption cipher text: $\mathrm{e}\left(C_2', C_2''\right) = e\left(X_j, g\right), e\left(C_2''', u^{c_1}v\right) = \mathrm{e}\left(\mathrm{C}_2', C_4\right)$, and $V(C_1, \sigma, (C_3, C_4)) = 1$. If the equation is not true, return$\perp$. Supposing that $j \in HU$, because $B$ otherwise knows the private key, it does not need to perform a decryption query.

First, if $C_1 = {C_1}^* = svk^*$: if $(C_3, C_4, \sigma) \neq ({C_3}'^*, {C_4}^*, \sigma^*)$, $B$ faces the occurrence of the $F_{OTS}$ event and stops the game; if $(C_3, C_4, \sigma) = ({C_3}'^*, {C_4}^*, \sigma^*)$, $B$ outputs $\perp$, indicating that $\left\langle pk_j, CT_j\right\rangle$ is derived from $\langle pk_{i^*}, CT^*\rangle$. As in stage 2 for the same hidden index $r$, the following must be the case that, assuming $C_1 \neq {C_1}^*$:

- For $X_j = g^{ax_j}$, if $j \in HU\backslash\{i^*\}$, the legitimacy of the cipher text ensures that, for $r \in {Z_p}^*$, the following formulas are satisfied: $e({C_2}'', {C_2}''') = e(g, X_j)^r = e(g, g)^{arx_j}$ and $C_4 = (u^{svk}v)^r = ((g^a)^{\alpha_1(svk-svk^*)}(g^{a^2})^{\alpha_2})^r$.

Therefore,

$$e(C_4, A_{-1}) = e(C_4, g^{1/a}) = e(g, g)^{a_1r(svk-svk^*)}e(g, g)^{a\alpha_2r} \tag{8}$$

$$e(g, g)^r = ((e(C_4, A_{-1}))/(e({C_2}'', {C_2}'''))^{\alpha_2/x_j})^{1/(\alpha_1(svk-svk^*))} \tag{9}$$

It is thus easy to calculate the plaintext $m$.

- If $j = i^*$, for the index, it is known that $x_{i^*} \in {Z_p}^*$ and one has $X_j = g^{a^2x_{i^*}}$. Because

$$e({C_2}'', {C_2}''') = e(g, X_{i^*})^r = e(g, g)^{a^2rx_{i^*}} \tag{10}$$

and

$$e(C_4, g) = e(g, g)^{a\alpha_1r(svk-svk^*)}e(g, g)^{a^2\alpha_2r}, \tag{11}$$

$B$ first obtains $\gamma = e(g, g)^{ar} = ((e(C_4, g))/(e({C_2}'', {C_2}'''))^{\alpha_2/x_{i^*}})^{1/(\alpha_1(svk-svk^*))}$.

As relationship $e(C_4, A_{-1}) = e(C_4, g^{1/a}) = e(g, g)^{a_1r(svk-svk^*)}e(g, g)^{a\alpha_2r}$, $\gamma$ reveals that

$$e(g, g)^r = ((e(C_4, A_{-1}))/(\gamma)^{a^2/x_{i^*}}))^{1/(\alpha_1(svk-svk^*))}. \tag{12}$$

It is thus easy to calculate the plaintext $m = C_3/e(g, g)^r$.

In phase 2, $B$ must check that $m$ is different from the challenge message to $m_0$, $m_1$. According to the security model's restriction rules, if $m \in \{m_0, m_1\}$, $B$ returns $\perp$.

(c) Challenge: Once $A$ decides that the query 1 phase is over, it outputs the challenge condition $w^*$ and two plaintexts of the same length ($m_0$, $m_1$). Challenge $B$ randomly selects $b \in \{0, 1\}$, and sets the challenge cipher text by taking the following steps: set ${C_1}^* = svk^*$ and calculate $C_2^* = B^{x_i^*}$, $C_3^* = T \cdot m_b$and$C_3^* = B^{x_2}$; for $({C_3}^*, {C_4}^*)$ generating a strong and unforgettable $\sigma^* = S(ssk, (C_3^*, C_4^*))$, so that the conventional cipher text is $CR_{i^*} = \left(C_1^*, C_2^*, C_3^*, C_4^*, \sigma^*\right)$; choose $r' \in Z_p{}^*$ randomly, calculate $K = e(g, h_0)^{r'}$,$C_3{}'{*} = C_3{}^*K$, $G_5{}^* = (Y_{i^*}g^{-w})^{r'}$, $G_6{}^* = e(g, g)^{r'}$, $t^* = H\left(C_3'^*, C_5^*, C_6^*\right)$,$C_7^* = e(g, h_1)^{r' t^*} e(g, h_2)^{r'}$; generate another strong and unforgettable $\sigma'^* = S(ssk, \left(C_1^*, C_2^*, C_3'^*, C_4^*, \sigma^*, C_5^*, C_6^*, C_7^*\right))$; therefore, the conditional cipher text is $CT^* = \left(C_1^*, C_2^*, C_3'^*, C_4^*, \sigma^*, C_5^*, C_6^*, C_7^*, \sigma'^*\right)$. Return $CT^*$to $A$.

(d) Query phase 2: A executes the same query as in phase 1.

(e) Guess: The attacker outputs his guess $b'$. If $b$=$b'$, it outputs 1, $T = e(g, g)^{b/a^2}$; otherwise, it outputs 0, $T = e(g, g)^r$.

**Probabilistic Analysis:** Suppose there is a PPT attacker A in game 1 capable of attacking the scheme proposed in this paper with a non-negligible advantage $\varepsilon$ under the standard model. The probability of the simulator is now given, supposing $F_{OTS}$ does not happen.

Because $x_{i^*} = (g^{a^2})^{x_{i^*}} = g^{a^2 x_{i^*}}$ and $B = g^b$, if $T = e(g, g)^{b/a^2}$, then $CT^*$ is the legal cipher text with index $r = b/a^2 m_b$. Conversely, if $T$ is a random number in $G_2$, $CT^*$ hides $m_b$ perfectly. $A$ guesses that the probability of $b$ does not exceed 1/2. Obviously,

$|\Pr[B(g, g^{1/a}, g^a, g^{a_2}, g^b, e(g, g)^{b/a^2}) = 1] - \Pr[B(g, g^{1/a}, g^a, g^{a_2}, g^b, e(g, g)^r| \geq |(1/2 \pm \varepsilon) - 1/2| =$ $\varepsilon(13)$ is not negligible. This completes the proof of Lemma 1.

**Lemma 2**: Assuming that an IND-CCA can attack KP-CPRE, an algorithm $B$ exists that can solve the q-ABDHE problem for all $q \geq q_k + 1$, where $q_k$ denotes the total number of conditional key queries for challenge users.

**Proof**: Supposing there is a polynomial time attacker $A$ in the game that can attack the KP-CPRE scheme in the standard model. Let $q_k$ be the total number of trap door queries, setting up a simulator A that can solve the q-ABDHE problem for all $q \geq q_k + 1$. $HU$ represents honest participation in the square set, including user $i^*$ with the specified public key $pk_{i^*}$, while $CU$ is corrupt participation in the square set.

This is simulated as follows.

First, the challenger sets up the group $G_1$,$G_2$, the effective bilinear pair $e$, and the generator $g$ of group $G_1$. The simulator enters an instance of the q-ABDHE problem $\left(g, g^x, g^{x^2}, \ldots, g^{x^q}, g^{zx^{q+2}}, T\right)$. The purpose of the simulator $B$ is to distinguish $T = e(g, g)^{zx^{q+2}}$ or $T$ is a random number in the group $G_2$.

A. System setup: $\lambda$ is a security parameter, while $(p, g, G_1, G_2, e)$ is a parameter of bilinear pairing, producing $u, v \in G_1$ and a strong and unforgettable $Sig = (G, S, V)$. The public parameter is $GP = (p, g, G_1, G_2, e, u, v, Sig)$.

B. Query phase 1: The attacker $A$ makes the following queries.

- Non-corrupted-key-generation query $\langle i \rangle$: The public key of challenge user $i = i^*$ is defined as follows: $B$ randomly chooses three $q$-order polynomials $f_k(X)$ where $k \in \{0, 1, 2\}$. Defining $\left\{h_{k^*} = f_k(x)^{f_k(x)}\right\}_{k \in \{0,1,2\}}$ and $Y_{i^*} = g^x$, then the private key of the system is $\{a_{k^*} = f_k(x)\}_{k \in \{0,1,2\}}$. Randomly select $X_{i^*} \in Z_p{}^*$ and calculate $X_{i^*} = g^{x_{i^*}}$. Set the public key of the challenge user to $pk_{i^*} = \left(x_{i^*}, y_{i^*}, \{h_{k^*}\}_{k \in \{0,1,2\}}\right)$ and send the public key to $A$. The honest user $i \in HU \backslash \{i^*\}$ is consistent with the key algorithm; this means that the simulator $B$ knows the public and private keys of $i \in HU \backslash \{i^*\}$ and sends them to $A$.

- Corrupted-key-generation query $\langle i \rangle$: The corrupt user $i \in CU$ is consistent with the key-generation algorithm. Simulator $B$ knows the public and private keys of $i \in CU$ and sends them to $A$.

- Partial-re-encryption-key query $\langle pk_i, pk_j \rangle$: $B$ generates a one-way re-encryption key $rk_{i,j} = X_j{}^{1/x_i}$; because $B$ knows the $X_i$ part of all user private keys, $B$'s calculations are correct.

- Conditional key query $\langle pk_i, w\rangle$: For challenge users $i = i^*$, $B$ calculates $\{s_{w,k} = f_k(w)\}_{k\in\{0,1,2\}}$, $d_{w,k} = \mathrm{g}^{(f_k(x)-f_k(w))/(x-w)}$ and sends the condition key $ck_{i,w} = \{d_{w,k}, s_{w,k}\}_{k\in\{0,1,2\}}$ to $A$. When $q \geq q_k + 1$, $\left\{s_{w,k} = f_k(w)\right\}_{k\in\{0,1,2\}}$ is random from $A$'s perspective, as $f_k(X)$ is a random polynomial of order $q$.

For user $i \neq i^*$, $B$ randomly chooses $s_k \in Z_p{}^*$, calculates $d_k = (h_k g^{-s_k})^{1/(y_i-w)}$, and sets $ck_{i,w} = \left\{d_{w,k}, \mathrm{s}_{w,k}\right\}_{k\in\{0,1,2\}}$.

- Re-encryption query: Because, for all users $i$ and $j$, $B$ can calculate a one-way re-encryption key $rk_{i,j}$, and a condition key $ck_{i,w} = \{d_{w,k}, s_{w,k}\}_{k\in\{0,1,2\}}$, for $\left\langle pk_i, pk_j, (w, CT_i)\right\rangle$, $B$ can calculate it correctly.

- Decryption query $\left\langle pk_j, CT_j\right\rangle$: If $\left\langle pk_j, CT_j\right\rangle$ indicates a query for re-encryption cipher text $C_j = (C_1, C_2{}', C_2{}'', C_2{}''', C_3, C_4, \sigma)$, the legality of the re-encryption cipher text $C_j$ is checked as follows: $e(C_2{}', C_2{}'') = e(X_j, g)$,$e(C_2{}''', u^{C_1}v) = e(C_2{}', C_4)$, and $V(C_1, \sigma, (C_3, C_4)) = 1$. If the equation is true, $B$ returns plaintext $m = C_3/e(C_2{}'', C_2{}''')^{1/x_j}$; otherwise, it returns $\perp$.

- Decryption query $\left\langle pk_j, (w, CT_j)\right\rangle$: If $\langle pk_i, CT_i\rangle$ represents a query that re-encrypts the original condition, $B$ performs a re-encryption query on $\left\langle pk_i, pk_j, (w, CT_i)\right\rangle$ to obtain the re-encryption cipher text $CT_j$, then performs a decryption query on $\left\langle pk_j, CT_j\right\rangle$ and returns the result to $A$.

C. Challenge: Once $A$ has decided to end query 1 and output the challenge condition to $(w_0, w_1)$ and two plaintexts $(m_0, m_1)$ of the same length, Challenge $B$ randomly chooses $b \in \{0, 1\}$ and sets $\left\{S_{w_b,k} = f_k(w_b)\right\}_{k\in\{0,1,2\}}$. $B$ then calculates $d_{w_b,k} = g^{(f_k(x)-f_k(w_b))/(x-w_b)}$, selects a key-pair with a strong unforgettable signature as $(ssk^*, svk^*) \leftarrow G(\lambda)$, and sets $C_1{}^* = svk^*$; $B$ randomly chooses $r \in Z_p{}^*$ and calculates $\mathrm{C}_2^* = X_{i^*}^r, C_3^* = e(g,g)^r m, C_4^* = (u^{swk^*}v)^r$. It then produces a strong unforgettable $\sigma^* = \mathrm{S}\left(ssk^*, \left(C_3^*, \mathrm{C}_4^*\right)\right)$ and cipher $CR_{i^*} = (C_1^*, C_2^*, C_3^*, C_4^*, \sigma^*)$, and then defines a polynomial of order $q+1$:

$$F^*(X) = (X^{q+2} - (w^*)^{q+2})/(X - w^*) = \sum_{i=0}^{q+1} (F_i{}^* X^i). \tag{14}$$

Calculate $C_5^* = g^{zx^{q+2}}(g^z)^{-(w^*)^{q+2}}, C_6^* = T^{F_{q+1}^*} e(g^Z, \prod_{i=0}^{q} (g^{x_i})^{F_2^*}), C_3' * = C_3^* \cdot e(C_5^*, d_{w_b,0})(C_6^*)^{S_{w_b,0}}$, $t^* = H(C_3{}'^*, C_5{}^*, C_6{}^*)$, and $C_7^* = e((C_5^*, d_{w_b,1})^{t^*} d_{w_b,2}) \cdot (C_6^*)^{S_{w_b,1}t^* + S_{w_b,2}}$. Set $r^* = zF^*(x)$,if $T = e(g,g)^{zx^{q+1}}$, and then $C_5^* = g^{(x-w_b)r'^*} = (Y_{i^*}g^{-w_b})^{r'^*}$, $C_6{}^* = e(g,g)^{r'^*}$,$C_3{}'^* = C_3{}^* e(g, h_0{}^*)^{r'^*}$, and $C_7^* = e(g, h_1^*)^{t^*r^*} e(g, h_2^*)^{r'^*}$; generate another signature $\sigma'^* = S(ssk^*, (C_1^*, C_2^*, C_3^*, C_4^*, C_5^*, C_6^*, C_7^*))$; the conditional cipher text is $CT^* = \left(C_1^*, C_2^*, C_3'^*, \sigma^*, C_4^*, C_5^*, C_6^*, C_7^*\right)$; return $CT^*$ to $A$.

D. Query phase 2: $A$ runs the same query as in phase 1.

E. Guess: The attacker outputs his guess $b'$. If $b$=$b'$, output 1, $T = e(g,g)^{zx^{q+1}}$; otherwise, output 0, $T = e(g,g)^r$.

**Probability analysis:** If $T = e(g,g)^{zx^{q+1}}$, the simulation is perfect: $A$ correctly guesses that the probability of $b$ is 1/2 + ε. Otherwise, $T$ is a random number, and $(C_5{}^*, C_6{}^*)$ are random and independent of each other. In this case, the probability that the inequality $C_6{}^* \neq e(C_5{}^*, g)^{1/(x-W_b)}$ is established is $1-1/p$. When the inequality is true, $K^* = e(C_5^*, d_{w_b,0})(C_6^*)^{S_{w_b,0}} = e(C_5^*, (h_0)^{1/(x-w_b)})((C_6^*)/e(C_5^*, g)^{1/(x-w_b)})^{S_{w_b,0}}$ is random, and from the perspective of $A$ is independent of each other (apart from $C_3{}'^*$). $s_{w_b,0}$ (when $q \geq q_k + 1$, $\{s_{w,k} = f_k(w)\}_{k\in\{0,1,2\}}$ is random from $A$'s perspective) is random, and from the perspective of $A$, all elements are independent of each other (apart from $C_3{}'^*$). Thus, $C_3{}'^*$ is random and independent.

Moreover, $(C_5{}^*, C_6{}^*, C_3{}'^*)$ does not disclose any information in $b$. This completes the proof of Lemma 2. Therefore, Theorem 1 is proved.

## 5 Conclusion

The present paper investigates and applies proxy re-encryption. In our approach, before the electronic record is generated, its producer interacts with the record manager. When an electronic record is generated, the record producer encrypts it. When the electronic record needs to be verified, it is decrypted to verify authenticity. When the producer hands the electronic record over to the record manager, the record manager re-encrypts it. When verifying, our approach can use the record manager's secret key to decrypt again so that the authenticity of the electronic record is guaranteed.

**Funding Statement:**Y. J. Ren gratefully acknowledges the financial support of the NSFC (61772280, 62072249), http://www.nsfc.gov.cn.

**Conflicts of Interest:**The authors declare that they have no conflicts of interest to report regarding the present study. Xiujuan Feng and Yongjun Ren are the co-corresponding authors.

## References

[1] Y. Bi and H. Xie, “Web archiving and preservation from the archival science perspective,” *Archives Science Study*, vol. 26, no. 4, pp. 74–78, 2015.

[2] Y. J. Ren, Y. Leng, F. J. Zhu, J. Wang and H.J. Kim, “Data storage mechanism based on blockchain with privacy protection in wireless body area network,” *Sensors*, vol. 19, no. 10, pp. 2395.1–2395. 16, 2019.

[3] Y. N. Liu and J. Y. Li, “Conceptual comparison and linkage between electronic data in law field and electronic records in archival field,” *Archives Science Study*, vol. 28, no. 4, pp. 92–99, 2017.

[4] Y. J. Ren, J. Shen, D. Z. Liu, J. Wang and J. Kim, “Evidential quality preserving of electronic record in cloud storage,” *Journal of Internet Technology*, vol. 17, no. 6, pp. 1125–1132, 2016.

[5] Y. Fu, S. Wen, L. Ma and J. Shu, “Survey on single disk failure recovery methods for erasure coded storage systems,” *Journal of Computer Research and Development*, vol. 55, no. 1, pp. 1–13, 2018.

[6] J. Wang, Y. Gao, W. Liu, W. Wu and S. Lim, “An asynchronous clustering and mobile data gathering schema based on timer mechanism in wireless sensor networks,” *Computers, Materials & Continua*, vol. 58, no. 3, pp. 711–725, 2019.

[7] Y. Huang, “Research on the connotation and management of trusted electronic records,” *Zhejiang Archives*, vol. 31, no. 5, pp. 12–15, 2014.

[8] S. Zhang, Y. Chang, L. Yan, Z. Sheng, F. Yang *et al.,* “Yang etal, Quantum communication networks and trust management: a survey,” *Computers, Materials & Continua*, vol. 61, no. 3, pp. 1145–1174, 2019.

[9] K. Gu, Y. Wang and S. Wen, “Traceable threshold proxy signature,” *Journal of Information Science and Engineering*, vol. 33, no. 1, pp. 63–79, 2017.

[10] C. Ge, Z. Liu, J. Xia and L. Fang, “Revocable identity-based broadcast proxy re-encryption for data sharing in clouds,” *IEEE Trans. on Dependable and Secure Computing*, vol. 19, no. 6, pp. 1–1, 2019.

[11] Y. Chen, J. Wang, R. Xia, Q. Zhang, Z. Cao *et al.,* “The visual object tracking algorithm research based on adaptive combination kernel,” *Journal of Ambient Intelligence and Humanized Computing*, vol. 10, no. 12, pp. 4855–4867, 2019, 2019.

[12] Y. J. Ren, F. J. Zhu, J. Qi, J. Wang and A. K. Sangaiah, “Identity management and access control based on blockchain under edge computing for the Industrial Internet of Things,” *Applied Sciences*, vol. 19, no. 9, pp. 2058.1–2058.12058, 2019.

[13] Q. Xiao and L. Wu, “Research on digital continuity plan of Australian National Archives,” *Journal of Information Resources Management*, vol. 5, no. 4, pp. 19–23, 2015.

[14] Y. J. Ren, Y. Leng, J. Qi, K. S. Pradip, J. Wang *et al.,* "Multiple cloud storage mechanism based on blockchain in smart homes," *Future Generation Computer Systems*, vol. 115, no. 2, pp. 304–313, 2021.

[15] J. Zhang, X. Jin, J. Sun, J. Wang and A. K. Sangaiah, "Spatial and semantic convolutional features for robust visual object tracking," *Multimedia Tools and Applications*, vol. 79, no. 21-22, pp. 15095–15115, 2020.

[16] N. Zhang, C. Wang, Z. Liu and W. Wang, "Study on the evaluation strategy of electronic document authenticity based on digital continuity thought," *Archives Research*, vol. 6, pp. 69–72, 2015.

[17] L. Fang, C. Yin, L. Zhou, Y. Li, C. Su *et al.,* "A physiological and behavioral feature authentication scheme for medical cloud based on fuzzy-rough core vector machine," *Information Sciences*, vol. 507, no. 1, pp. 143–160, 2020.

[18] W. Li, H. Liu, J. Wang, L. Xiang and Y. Yang, "An improved linear kernel for complementary maximal strip recovery: simpler and smaller," *Theoretical Computer Science*, vol. 786, no. 1, pp. 55–66, 2019.

[19] L. Johnston, "ERA 2.0: the national archives new framework for electronic records preservation," in *Proc. of the Association for Information Science and Technology*, New York, NY, USA, pp. 197–202, 2017.

[20] Y. J. Ren, F. J. Zhu, S. P. Kumar, T. Wang, J. Wang *et al.,* "Data query mechanism based on hash computing power of blockchain in Internet of Things," *Sensors*, vol. 20, no. 7, pp. 2071–207. 22, 2020.

[21] K. Gu, L. Yang and B. Yin, "Location data record privacy protection based on differential privacy mechanism," *Information Technology and Control*, vol. 47, no. 4, pp. 639–654, 2018.

[22] Y. Qian, "Millennial-scale phase relationship between North Atlantic deep-level temperature and Qinghai-Tibet Plateau temperature and its evolution since the Last Interglaciation," *Chinese Science Bulletin*, vol. 59, no. 3, pp. 75–81, 2014, 2014.

[23] Y. Mao, J. Zhang, H. Qi and L. Wang, "DNN-MVL: DNN-multi-view-learning-based recover block missing data in a dam safety monitoring system," *Sensors*, vol. 19, no. 13, pp. 2895.1–2895.19, 2019.

[24] Y. Lu and T. Feng, "Research on trusted DNP3-BAE protocol based on hash chain," *EURASIP Journal on Wireless Communications and Networking*, vol. 2018, no. 5, pp. 108.1–108.10, 2018, 2018.

[25] Z. Yi, "Research on the formation process of electronic records based on the thought of front-end control," *Archives Science Study*, vol. 23, no. 3, pp. 16–23, 2012.

[26] Y. J. Ren, J. Qi, Y. P. Cheng, J. Wang and O. Alfarraj, "Digital continuity guarantee approach of electronic record based on data quality theory," *Computers, Materials & Continua*, vol. 63, no. 3, pp. 1471–1483, 2020.

[27] J. Wang, X. Gu, W. Liu, A. K. Sangaiah and H. Kim, "An empower Hamilton loop based data collection algorithm with mobile agent for WSNs," *Human-Centric Computing and Information Sciences*, vol. 18, no. 9, pp. 1794–1808, 2019.

[28] F. Upword, B. Reed, G. Oliver and J. Evans, "Record keeping informatics: Re-figuring a discipline in crisis with a single-minded approach," *Records Management Journal*, vol. 23, no. 1, pp. 47–54, 2013.

[29] J. M. Zhang, W. Wang, Ch Q. Lu, J. Wang and A. K. Sangaiah, "Lightweight deep network for traffic sign classification," *Annals of Telecommunications*, vol. 75, no. 7-8, pp. 369–379, 2020.

[30] Y. J. Ren, Y. Leng, Y. P. Cheng and J. Wang, "Secure data storage based on blockchain and coding in edge computing," *Mathematical Biosciences and Engineering*, vol. 16, no. 4, pp. 1874–1892, 2019.

[31] Y. Chen, H. Hou, H. Su and Q. Yang, "Records management in e-government system: issues and reflections," *Archives Science Study*, vol. 26, no. 2, pp. 28–37, 2015.

[32] W. Zhang, F. Y. Shih, S. Hu and M. Jian, "A visual secret sharing scheme based on improved local binary pattern," *International Journal of Pattern Recognition and Artificial Intelligence*, vol. 32, no. 6, pp. 185–195, 2018.

[33] Y. J. Ren, Y. P. Liu, S. Ji, K. Arun and J. Wang, "Incentive mechanism of data storage based on blockchain for wireless sensor networks," *Mobile Information Systems*, vol. 2018, no. 8, pp. 1–10, 2018.

[34] S. B. Dewdney and L. Jason, "Electronic records, registries, and the development of 'big data': crowd-sourcing quality toward knowledge," *Frontiers in Oncology*, vol. 268, no. 1, pp. 20–27, 2017.

[35] W. Wan, J. Chen and S. Zhang, "A cluster correlation power analysis against double blinding exponentiation," *Journal of Information Security and Applications*, vol. 48, no. 10, pp. 102357, 2019.

[36] D. Zeng, Y. Dai, J. Wang, F. Li and A. K. Sangaiah, "Aspect based sentiment analysis by a linguistically regularized CNN with gated mechanism," *Journal of Intelligent & Fuzzy Systems*, vol. 36, no. 5, pp. 3971–3980, 2019.

[37] X. Jia, “Analysis and implications of the New Zealand digital continuity action plan,” *Library and Information Work*, vol. 2016, no. 1, pp. 45–51, 2016, 2016.

[38] L. Xie, J. Wang and L. Ma, “Trusting records: findings of team asia InterPARES,” *Archives Science Study*, vol. 28, no. S1, pp. 8–13, 2017.

[39] T. Li, Y. Ren and J. Xia, “Blockchain queuing model with non-preemptive limited-priority,” *Intelligent Automation & Soft Computing*, vol. 26, no. 5, pp. 1111–1122, 2020.

[40] L. Xie, J. Wang and L. Ma, “The project of InterPARES: Where it has been and where it is going,” *Archives Science Study*, vol. 28, no. S1, pp. 14–20, 2017.

[41] Y. T. Chen, J. J. Tao, L. W. Liu, J. Xiong, R. L. Xia *et al.,* “Research of improving semantic image segmentation based on a feature fusion model,” *Journal of Ambient Intelligence and Humanized Computing*, vol. 20, no. 5, pp. 1–13, 2020.

[42] J. Wang, Y. Gao, W. Liu, A. K. Sangaiah and H. Kim, “An intelligent data gathering schema with data fusion supported for mobile sink in WSNs,” *Int. Journal of Distributed Sensor Networks*, vol. 2019, no. 3, pp. 1550–1561, 2019, 2019.

[43] L. Chao and H. Qu, “Electronic records management systems: from digital continuity to data continuity,” *Archives Science Bulletin*, vol. 64, no. 1, pp. 20–25, 2019.

[44] C. P. Ge, W. Susilo, Z. Liu, J. Y. Xia, P. Szalachowski *et al.,* “Secure keyword search and data sharing mechanism for cloud computing,” *IEEE Trans. on Dependable and Secure Computing*, vol. 20, no. 3, pp. 1–1, 2020.

[45] Y. Ren, J. Qi, Y. Liu, J. Wang and G. Kim, “Integrity verification mechanism of sensor data based on bilinear map accumulator,” *ACM Trans. on Internet Technology*, vol. 21, no. 1, pp. 1–19, 2021.

[46] J. Seymour, “The modern records management program: An overview of electronic records management standards,” *Bulletin of the Association for Information Science and Technology*, vol. 43, no. 2, pp. 35–39, 2017.

[47] J. Wang, C. W. Ju, Y. Gao, A. K. Sangaiah and G.-J. Kim, “A PSO based energy efficient coverage control algorithm for wireless sensor networks,” *Computers Materials & Continua*, vol. 56, no. 3, pp. 433–466, 2018.

[48] A. A. Aziz, Z. M. Yusof, U. A. Mokhtar and D. I. Jambari, “Establishing policy for the implementation of electronic document and records management system in public sector in Malaysia: the influencing factors,” *Advanced Science Letters*, vol. 23, no. 11, pp. 10732–10736, 2017.