Supervisable Anonymous Management of Digital Certificates for Blockchain PKI

Shaozhuo Li[1,2(✉)], Na Wang[1,2], Xuehui Du[1,2], and Xuan Li[3]

[1] National Digital Switching System Engineering and Technological Research Center, Zhengzhou 450000, China
494187944@qq.com
[2] Zhengzhou Science and Technology Institute, Zhengzhou 450000, China
[3] Jiuquan Satellite Launch Center, Jiuquan 732750, China

Abstract. Aiming at the requirement of anonymous supervision of digital certificates in blockchain public key infrastructure (PKI), this paper proposes a ring signature with multiple indirect verifications (RS-MIV). This mechanism can ensure multiple and indirect verification of certificate signer identity while preserving its anonymity. On this basis, a supervisable anonymous management scheme was designed based on smart contracts, which realizes the anonymity of certificate authority nodes, the anonymous issuance of digital certificates, the anonymous verification of digital certificates, and the traceability of illegal certificate issuers in the blockchain PKI. It is proved that the scheme can guarantee the anonymity and traceability of the certificate issuer's identity at an acceptable cost.

Keywords: Blockchain · Digital certificate · PKI · Ring signature

1 Introduction

Building a blockchain-based PKI and realizing open, transparent, and distributed management of digital certificates by uploading them to the blockchain can effectively solve the security problems caused by third-party CAs, which are being attacked or having weak security practices [1, 2]. These can also meet the cross-domain verification requirements of the digital certificates brought by the increasingly widespread application of distributed computing modes, such as Internet of Things, Big Data, and cloud computing [3–5].

Currently, blockchain-based PKI does not allow CA nodes (Node of CA user on blockchain) to be anonymous to ensure the credibility of the PKI. However, in some applications or scenarios where the commercial CAs are not willing to disclose their privacy, the blockchain-based PKI needs to ensure the anonymity of the CA nodes and realize anonymous management of the digital certificates. However, the anonymity of the CA nodes cannot be guaranteed without reducing the credibility of the PKI. For example, if an illegal digital certificate is detected in the blockchain, it must be accurately traced back to find the issuer of that certificate. As a result, this paper studies the supervisable anonymity management of digital certificates based on blockchain PKI.

J. Zeng et al. (Eds.): ICPCSEE 2020, CCIS 1257, pp. 130–144, 2020.
https://doi.org/10.1007/978-981-15-7981-3_10

Verifiable ring signature mechanism can prove the signer's real identity by providing some relevant data when needed. However, it cannot be directly used to achieve the supervisable anonymity management of digital certificates as this needs multiple verification without destroying the anonymity. Thus, the indirect verification of the identity of the certificate issuer can be realized when it does not cooperate.

Based on this, this paper proposes a Ring Signature with Multiple Indirect Verifications (RS-MIV), which is based on RSA (Ron Rivest, Adi Shamir, Leonard Adleman algorithm) ring signature mechanism. By introducing one-to-one verification public and private keys corresponding to the digital certificates, the signer's signature of secret information is used instead of the initial secret value. In similar, to ensure the anonymity of the signer and realize multiple and indirect verification of the signer's identity when needed, binding ring signature is utilized. As a result, this paper designs a supervisable anonymity management scheme based on smart contracts, which can realize: i) the anonymity of CA (Certificate Authority) nodes; ii) the anonymity issuance of digital certificates; iii) the anonymity verification of digital certificates, and iv) the traceability of illegal certificate issuers in the blockchain PKI, and meet the actual demand of CA node Supervisable anonymity. It is proved that the proposed scheme can guarantee the anonymity and traceability of the identity of the certificate issuer at an acceptable cost.

2 Related Work

2.1 Current Literature on Blockchain PKI

Currently, the research on blockchain PKI mainly focuses on Certcoin, IKP, SCPKI, and Permor. Certcoin [6] uses the technical characteristics of blockchain decentralization to build a fully decentralized PKI by binding the user identity and the public keys in the blockchain. It takes Namecoin [7] as its underlying platform. IKP (instant karma PKI) [8] uses the characteristics of automatic and compulsory execution of smart contracts to detect the CA nodes that behave improperly or are under attack. It uses the economic incentive mechanism of Ethereum to reward the CA nodes that issue certificates correctly, and punish the nodes that issue illegal certificates. SCPKI (Smart Contract-based PKI and Identity System) [9] uses Ethereum smart contracts to implement PGP (Pretty Good Privacy), thereby building a fully distributed PKI system. Similar to PGP, SCPKI adopts a web of trust model to measure the credibility of public keys by using the trust relationship between the users. Pemcor [10] proposes to build two blockchains to store the hash value of the generated digital certificate and the hash value of the revoked digital certificate. These blockchains should be controlled by an authority, such as a bank or government. Therefore, if the hash value of the certificate is in the generated certificate blockchain, i.e., it is not in the revoked certificate, the certificate is valid. Otherwise, it is invalid.

This paper found out that the node identity should be completely open to ensure the credibility of the blockchain PKI. However, in some special applications or scenarios where the commercial CAs are not willing to disclose their privacy, blockchain PKI needs to realize the manageable anonymity of the CA nodes. That is to say, the CA

nodes are allowed to issue certificates anonymously and upload the issued certificates to the blockchain. However, after discovering the illegal certificates, the identity of CA nodes that issued and uploaded the digital certificates must be confirmed for accountability to ensure the credibility of the blockchain PKI system.

2.2 Blockchain's Anonymous Mechanism

With the widespread adaptation of the blockchain in finance, the anonymity became compulsory. This mechanism can ensure the anonymity of transaction users to avoid the third parties getting the identity information of both parties from the transaction address and transaction content on the blockchain. For example, Dascoin introduces chain mixing and blinding technology to ensure user anonymity by mixing multiple users. In similar, Monroe coin hides address and ring signature. Zero Cash [11] uses zkSNARK (Zero-knowledge Succinct Non-interactive Arguments Of Knowledge) to achieve anonymity. This is by far the most secure and effective method; however, it is based on the NP (Non-deterministic Polynomial) problem, which limits its application, but makes it suitable for anonymity problems that are difficult to convert into NP problems (for example, the digital certificate Supervisable anonymity management problem solved in this paper). Furthermore, the initialization parameters of this method are complex.

Currently, the anonymity of blockchain is realized by changing the recording mode of transaction data, which hides transaction amount in the financial environment. However, these anonymous mechanisms achieve complete anonymity, and the node identity is not exposed from beginning to end, which does not meet the requirements of the CA node that can supervisable anonymity proposed in this paper.

2.3 Verifiable Ring Signature

Ring signature was first proposed by Rivest in 200112, which is mainly used in applications where the signer needs to be anonymous, such as anonymous voting and anonymous election.

A secure ring signature scheme should have the following properties:

(1) Correctness: the signature output by any member in the ring after executing the ring signature elaboration algorithm can pass the signature verification algorithm in the system;
(2) Anonymity: given a ring signature, any verifier will not identify the real signer with a probability greater than $1/n$, where n is the number of members in the ring.
(3) Unforgeability: any user who is not in the ring $U = \{U_1, U_2, \ldots U_n\}$ cannot effectively generate a message signature.

The concept of verifiable ring signature was proposed by LV [13] in 2003, which means that the real signer can prove their identity when necessary by presenting some relevant data. In 2004, Gan Zhi et al. proposed two verifiable ring signature schemes [14], based on: i) one-time identity verification; ii) zero knowledge verification. The latter adds some secret identity information to the initial parameters of the ring signature, and then confirms the identity of the signer by verifying the correctness of the secret

identity information. This scheme can only achieve one-time verification of the signer's identity. In the former, the signer sets the initial value v as a product of two large prime numbers, and then uses zero knowledge proof to validate that it knows the decomposition of the initial value to prove its identity. In 2006, Zhang et al. proposed a verifiable ring signature based on Nyberg rueppel signature [15]. This scheme only used hash function to realize ring signature, which is suitable for small computation and signature scale. In 2007, Wang et al. put forward an extension scheme based on RSA ring signature [16], which realizes verifiable ring signature based on the designated confirmer signature and the verifier verification; however, the verification process needs multiple interactions, and the calculation is relatively complex. In 2008, I. Jeong et al. proposed a linkable ring signature scheme with strong anonymity and weak linkage [17], and proved that it can be used to construct an effective verifiable ring signature scheme, which is suitable for the ring signature scenarios with linkability requirements. In 2009, Luo Dawen et al. proposed a certificateless verifiable ring signature mechanism by combining certificateless Cryptosystem with verifiable ring signature mechanism [18]. This overcame the key escrow problem of the identity-based cryptosystem and avoided the storage and management problem of public key based on certificate cryptosystem. Because it is found that the scheme does not satisfy the non-repudiation, Li Xiaolin et al. proposed the corresponding improvement scheme [19]. Because it is found that Li Xiaolin's improvement scheme does not satisfy the non forgery, Zhang Jiao et al. proposed the corresponding improvement scheme [20]. In 2012, Qin et al. extended the verifiability based on RSA ring signature [21]. The initial value of the ring signature was replaced by private information and hash value related to signature, which allowed the signer to prove itself at any time, but only once. In 2013, based on a forward secure ring signature algorithm, Yang Xudong et al. proposed an improved verifiable strong forward secure ring signature scheme [22] by using the method of double private key update that guaranteed the forward and backward security of the ring signature. In 2017, bultel x et al. proposed a verifiable ring signature mechanism based on the DDH (decision-making Diffie Hellman hypothesis) and zero knowledge proof [23]. They proved the security of the mechanism under the random oracle model, which was applicable to the ring signature scenarios with non-linkable requirements.

In this paper, we find that the current verifiable ring signature mechanisms cannot be directly used in the supervisable anonymous management of digital certificates. The reasons are as follows: (1) some mechanisms, such as Gan Zhi's one-time authentication mechanism [14], Zhang's verifiable ring signature mechanism based on Nyberg rueppel signature [15], Qin's verifiable extension mechanism based on RSA ring signature [21], can verify the real identity of the signer only once, and after one-time verification, the signer's identity will be completely exposed. This means that the anonymity of the signer can no longer be guaranteed. However, in the scenario where the digital certificate can be managed anonymously, it is required to verify the signer's identity many times without affecting the anonymity of the signer; (2) all mechanisms require the signer to actively expose the evidence to verify the signer's identity. However, in the case of the digital certificate's supervisable aonymous management, there is the possibility that the CA node with malicious signature will not actively expose its identity. Therefore, it is necessary to confirm the signer's identity when the digital certificate issuer does not actively expose its identity.

2.4 RSA-Based Ring Signature Mechanism

Since the PKI mainly uses RSA algorithm to sign digital certificates, this paper focuses on improving the RSA based ring signature mechanism. Below, the principles of the RSA-based ring signature mechanism is described.

By supposing that the ring size is r, ring member is $A_1, A_2, A_3 \ldots A_r$, and each member has an RSA public key $P_i = (n_i, e_i)$, the one-way threshold replacement is: $f_i(x) = x^{e_i} (\mathrm{mod} n_i), f_i \in Z_n$.

It is concluded that only A_i knows how to use the threshold information to effectively calculate inverse permutation $f_i^{-1}(x)$. E is a publicly defined symmetric encryption algorithm, so that for any length l of key k, the function E_k is a replacement on the bit string b. Define the composite function as $C_{k,v}(y_1, y_2, \ldots y_r)$, input as key k, initialization variable as v, and random number set as $\{0, 1\}^b$.

The ring signature process of the message m to be signed is as follows:

(1) The signer calculates hash for the signed message m, then symmetric key $k = h(m)$. The signer chooses a random value from $\{0, 1\}^b$ as v.
(2) The signer chooses x_i uniformly and independently from $\{0, 1\}^b$,and calculate $y_i = f_i(x_i)$.
(3) The signer solves y_s from $C_{k,v}(y_1, y_2, \ldots y_r) = v$.
(4) The signer uses its threshold knowledge to solve $x_s = f_s^{-1}(y_s)$.
(5) The output ring signature is: $(P_1, P_2, \ldots P_r; v; x_1, x_2, \ldots x_r)$.

The verifier verifies the ring signature $(P_1, P_2, \ldots P_r; v; x_1, x_2, \ldots x_r)$ as follows:

(1) The verifier calculates $y_i = f_i(x_i)$ for $i = 1, 2, \ldots, r$.
(2) The verifier calculates $k = h(m)$ for the encrypted message.
(3) The verifier calculates whether y_i satisfies $C_{k,v}(y_1, y_2, \ldots y_r) = v$. If so, the signature is legal. Otherwise, the signature is rejected.

3 Ring Signature Mechanism with Multiple Indirect Verifications

To verify the identity of the anonymous signer many times without exposing its identity, this paper improves the RSA-based ring signature mechanism and proposes a ring signature with multiple indirect verifications (RS-MIV).

In RS-MIV mechanism, before signing the digital certificate subject, the issuer synchronously generates a pair of public and private keys that are uniquely bound to the certificate. Then the issuer signs the digital certificate and the public key together. To verify the signer of a certificate many times, the signer only needs to show the signature of a message with the verification private key. To resist replay attack, the verification of certificate issuer is performed by challenge-response. To be able to confirm the identity of the issuer without revealing its identity, the RS-MIV uses the issuer's digital signature of the random number r and its own digital certificate serial number as secret information to generate parameters in the RSA ring signature

$v = h(sig(r, Cid))$, where the random number r is public. Thus, the legal certificate issuer can prove its validity to the verifier by generating its own digital signature of random number r and the certificate serial number. By excluding legal nodes, malicious nodes can be detected indirectly, i.e., the indirect verification of the identity of the digital certificate issuer can be realized.

The mechanism of the RS-MIV is detailed below:

(1) Generation of the ring signature:

1) The signer generates a pair of public and private keys for the certificate to be signed, i.e., the verification public and private keys. The public key is (n_c, e_c) and the private key is d_c. The private key is saved by the signer, which is not disclosed.
2) Generate symmetric key as $k = h(m, n_c, e_c)$ and initial value as $v = h(sig(r, Cid))$, where m is the certificate information to be signed, r is a random number, Cid is the serial number of the digital certificate of the signer, and $sig(r, Cid)$ is the digital signature of the signer to r and Cid.
3) The signer chooses x_i uniformly and independently from $\{0, 1\}^b$ and calculates $y_i = f_i(x_i)$.
4) The signer solves y_s from $C_{k,v}(y_1, y_2, \ldots y_r) = v$.
5) The signer uses its threshold knowledge to solve $x_s = f_s^{-1}(y_s)$.
6) The output ring signature is $(P_1, P_2, \ldots P_l; v; x_1, x_2, \ldots x_l; n_c, e_c, r)$.

(2) Ring signature verification:

1) For $i = 1, 2, \ldots, r$,calculate $y_i = f_i(x_i)$.
2) The verifier calculates $k = h(m, n_c, e_c)$ for the encrypted message.
3) The verifier calculates whether y_i satisfies $C_{k,v}(y_1, y_2, \ldots y_r) = v$. If so, the signature is legal. Otherwise, the signature is rejected.

(3) Ring signer authentication based on challenge-response:

1) The verifier generates a random number a and the digital certificate number to be verified, then it sends both to the signer.
2) The signer obtains the corresponding verification private key of the certificate according to the number of the digital certificate to be verified. Then it signs the random number with the verification private key of the certificate to be verified. Finally, it outputs $sig_c(a)$.
3) The verifier decrypts $sig_c(a)$ with the verification public key (n_c, e_c) in the certificate ring signature. If $sig_c^{e_c} = h(a) \bmod n_c$, the verification succeeds, and the signer's identity is confirmed. Otherwise, the verification fails.

(4) Indirect verification of the signer identity:

1) The contract send a message to all members in the ring, requiring all members to send $(Cid_i, sig_i(r, Cid_i))$, where r is the random number in the signature of the ring to be verified, Cid_i is the certificate number of the member sending the message, and $sig_i(r, Cid_i)$ is the signature of the member sending the message. The members who do not send $(Cid_i, sig_i(r, Cid_i))$ are recorded as malicious.
2) The verifier finds the public key (n_i, e_i) of the member according to Cid_i, and then uses it to verify the authenticity of signature S. If the verification succeedstrue, it

means that the information sent by the member is true. If the verification is false, the member is listed as a malicious member.

3) Verify whether $v = h(sig_i(r, Cid_i))$ is valid. If true, the member is the issuer. Otherwise, the member is not the issuer, which results in member's exlusion.

The RSA-based ring signature mechanism has been proved to be secure under random oracle model in [12]. The RS-MIV mechanism proposed in this paper only replaces the initial value of the RSA-based ring signature, and does not improve its structure. Thus, it still has all the characteristics of the RSA-based ring signature mechanism. At the same time, when generating the symmetric key k, the RS-MIV added the verification public key to it. If the verification public key is tampered with, in the process of ring signature verification, when k is used to calculate $C_{k,v}(y_1, y_2, \ldots y_r) = v$, the correct result cannot be obtained, and the illegal signature result is obtained. Thus, the authenticity of the verification public key is guaranteed.

4 Supervisable Anonymous Management Scheme of Digital Certificates Based on Smart Contracts

This article uses smart contracts to implement the supervisable and anonymous management of digital certificates, including the anonymity issuance, the anonymity verification, and the traceability of the illegal digital certificate issuer in the blockchain PKI. Smart contracts can ensure the automatic execution and security of the three functions.

4.1 Anonymity Issuance of the Digital Certificate

The anonymity issuance of digital certificates means that the CA node issues the digital certificate with the RS-MIV mechanism after receiving a service request and then uploads the digital certificate to the blockchain.

In our scheme, the digital certificate adopts the standard format of X.509 (see Fig. 1); however, the following modifications need to be made: (1) the digital signature part of the certificate is the ring signature by CA using RS-MIV mechanism; (2) due to the characteristics of open consensus of the blockchain, hash algorithm is used to calculate the user's private information to be protected. The hash value of the user's private information is stored in the certificate. The method of obtaining the user's private information off-blockchain and comparing it with the hash value of the private information in the certificate are for ensuring the correctness of the obtained user's private information. (3) To ensure the anonymity of the CA node, the issuer's identity information is not kept in the certificate.

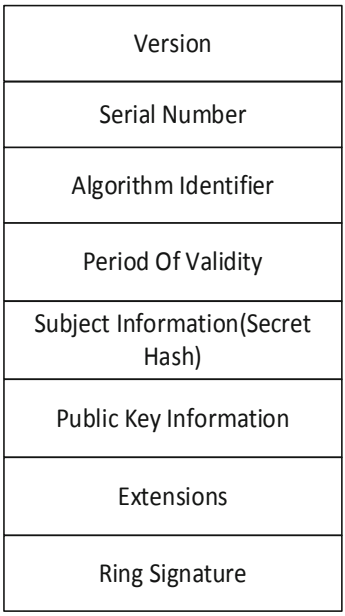

Fig. 1. Digital certificate format in our scheme.

4.2 Anonymity Verification of the Digital Certificate

When users get a digital certificate from the blockchain, they need to check the validity of the ring signature of that certificate first. In the verification process, the ring signature verification method in the RS-MIV mechanism is used. It should be noted that the current methods need to build a certificate chain from the root CA to the certificate issuing Ca, and realize one-to-one verification of the digital certificates in the certificate chain. However, in our scheme, due to the anonymity of the certificate issuing CA nodes, the certificate chain cannot be built. In this regard, the blockchain PKI adopts a node trust enhancement technology by default [2]. Under the premise that there are several root CAs with initial trust based on blockchain PKI, when a CA node wants to join the blockchain, the technology establishes the trust of CA node in the chain by verifying the certificate chain from the root CA to the CA node. Therefore, even if the scheme cannot verify the digital certificate, the node trust enhancement technology can guarantee the credibility of the CA node that issues the digital certificate anonymously.

The pseudo code of the smart contract used for anonymous authentication of digital certificate is as follows:

Algorithm 1: Anonymous certificate verification contract

Input: Verified certificate serial number :Serial number;Verified certificate ring signature: Ring Signature;

Output: judgment result: flag;

```
1.  Certification cert=null;int flag=null;
2.  for i=0 to addcert.length do
3.    if(addcert[i].Serial number=Serial number)then
4.        {cert=addcert[i];
5.        End for;}
6.  if(date<cert.Period Of Validity)then{
7.    if(revokelistquery(cert.Serial number)=1&&RS-MIVverification(cert.
Serial number,ce rt.Ring Signature)=1)then{
8.        flag=1;
9.    }else flag=0;
10. }else flag=0;
11. return flag;
```

4.3 Traceability of the Issuer of Illegal Digital Certificates

After finding the illegal digital certificates in the blockchain, it is necessary to trace the issuer of these certificates.

Under normal circumstances, the first thing to do is checking the ring signature of the certificate and finding the ring signed for it. Then, the serial number of the certificate is sent to the ring group member, and the CA node that issues the certificate claims it through the ring signature authentication method based on challenge-response in the RS-MIV mechanism. When the verification is successful, the CA node that issued the illegal certificate needs to revoke the certificate. To encourage CA nodes to actively report illegal certificates, the economic incentive feature of the blockchain can be used as a reward mechanism.

In the case that CA node does not report illegal certificates, the ring signature function must be suspended. This is followed by asking all nodes in the ring to show proof $sig(Cid, r)$ and Cid. Then, the indirect verification method in the RS-MIV mechanism is used to confirm the identity of the node presenting the proof, excluding the legal CA node. The CA nodes that fail to pass identity verification are considered as

malicious nodes. For malicious nodes, economic punishment measures based on blockchain can be taken. If the node is no longer trusted, all certificates issued by the node will be revoked, and the node will be removed from the blockchain PKI. By following, a new ring will be formed with the remaining nodes in the ring.

The smart contract pseudo code is as follows:

Algorithm 2: Anonymous certificate traceability contract

Input: illegal certificate serial number: Serial number;

Output: illegal certificate issuer:cert ; malicious node:illegalnode;

```
1. Certification cert=null;Certification[] illegalnode=null;
2. if(RS-MIVactivelytraceability( Serial numbert )=null)then{
3.    illegalnode=RS-MIVtraceability(Serial number);
4.    return illegalnode;
5. }else{
6.    cert=RS-MIVactivelytraceability( Serial number);
7.    return cert;
8. }
```

5 Security Analysis

5.1 Anonymity

Conclusion 1: If the hash function and the RSA algorithm are secure and the RS-MIV mechanism satisfies anonymity, the certificate issuer satisfies anonymity.

Prove: $A_{IBAnony}$ is defined as the adversary to attack the anonymity in the simulation attack game, A_{Hash} is the adversary to attack the hash function, A_{RRS} is the adversary to attack the anonymity of the RS-MIV mechanism, and A_{RSA} is the adversary to attack the RSA algorithm. A polynomial time algorithm $A \in (A_{Hash}, A_{RRS}, A_{RSA})$, which contains the ability of all the above attackers, is defined and A through the interaction of $A_{IBAnony}$ and A in anonymous simulation attack game is constructed. Thus, it can perform the above-explained attacks. If $A_{IBAnony}$ successfully attacks the anonymity of this scheme, then A can successfully attack the other parts, including the hash function, the RS-MIV mechanism, and the RSA algorithm, under a certain probability.

(1) Initialization: Algorithm A initializes the system, runs the anonymous certificate issuance and verification process, gives the certificate public key PK to the attacker $A_{IBAnony}$, and keeps the certificate private key SK and Ca for the certificate signature S.

(2) Query: Opponent $A_{IBAnony}$ queries algorithm A with polynomial bounded degree:

1) Ask for the private key SK of the corresponding anonymous certificate. The algorithm A attacks the ring signature scheme and the RSA algorithm by running A_{Hash}, A_{RRS}, A_{RSA}. Then it hands the private key SK to the attacker $A_{IBAnony}$.
2) Ask for the secret information $sig(Cid, r)$ of the issuing CA corresponding to the anonymous certificate. Algorithm A attacks by running A_{Hash}, A_{RRS}, A_{RSA}, and returns the secret information to $A_{IBAnony}$.

(3) Challenge: When the attacker $A_{IBAnony}$ finishes asking, A selects two nodes i_0, i_1, and generates corresponding private keys SK_{i_0}, SK_{i_1} according to the RSA algorithm. Then, it randomly selects a bit $\mu \in \{0, 1\}$, executes the above parts, and obtains the certificate $Cert$ and secret information $sig(Cid, r)$, Finally, it extracts the challenge certificate and returns $clCert = CLCert(SK_{i_b}, PK, Cert, sig(Cid, r))$ to A.

(4) Guess: The attacker $A_{IBAnony}$ conducts polynomial bounded query on A as before, but it is not allowed to query the private key of i_0 and i_1 and the secret information of the issuing CA.

(5) Output: Finally, the attacker $A_{IBAnony}$ outputs a guess $\mu' \in \{0, 1\}$. If $\mu' = \mu$, it means that the attacker $A_{IBAnony}$ wins the game. The probability of the opponent $A_{IBAnony}$ success is:

$$
\begin{aligned}
Adv_{A_{IBAnony}}(k) &= \Pr\left[Exp_{A_{IBAnony}}(k) = 1\right] \\
&= \Pr\left[A_{IBAnony}(guess) = 1 | \mu = 1\right] \cdot \Pr[\mu = 1] + \Pr\left[A_{IBAnony}(guess) = 0 | \mu = 0\right] \cdot \Pr[\mu = 0] \\
&= \frac{1}{2}\left(\Pr\begin{bmatrix} A_{Hash}(guess) = 1 \\ A_{RRS}(guess) = 1 \\ A_{RSA}(guess) = 1 \end{bmatrix} \mu = 1 + \Pr\begin{bmatrix} A_{Hash}(guess) = 0 \\ A_{RRS}(guess) = 0 \\ A_{RSA}(guess) = 0 \end{bmatrix} \mu = 0\right) \\
&< \frac{1}{2}(\Pr[A_{Hash}(guess) = 1 | \mu = 1] \cdot \Pr[\mu = 1] + \Pr[A_{Hash}(guess) = 0 | \mu = 0] \cdot \Pr[\mu = 0]) + \\
&\frac{1}{2}(\Pr[A_{RRS}(guess) = 1 | \mu = 1] \cdot \Pr[\mu = 1] + \Pr[A_{RRS}(guess) = 0 | \mu = 0] \cdot \Pr[\mu = 0]) + \\
&\frac{1}{2}(\Pr[A_{RSA}(guess) = 1 | \mu = 1] \cdot \Pr[\mu = 1] + \Pr[A_{RSA}(guess) = 0 | \mu = 0] \cdot \Pr[\mu = 0]) \\
&= \Pr[Exp_{A_{Hash}}(k) = 1] + \Pr[Exp_{A_{RRS}}(k) = 1] + \Pr[Exp_{A_{RSA}}(k) = 1] \\
&= Adv_{A_{Hash}}(k) + Adv_{A_{RRS}}(k) + Adv_{A_{RSA}}(k)
\end{aligned}
$$

As a result, if the attacker A_{Hash} successfully attacks the hash function, A_{RRS} successfully attacks the anonymity of the RS-MIV mechanism, and A_{RSA} successfully attacks the RSA algorithm. Thus, $A_{IBAnony}$ will win the anonymity simulation attack game of this scheme. However, thanks to the above-given algorithm and the security of the RS-MIV scheme, the probability of successful attack of the opponent $A_{IBAnony}$ can be ignored, so the scheme satisfies anonymity.

5.2 Traceability

Conclusion 2: When the CA node is trusted and if the blockchain meets the requirement of non-tamperability, the RS-MIV mechanism meets the requirements of non-forgery and verifiability. This means that the RSA algorithm is secure, and the identity of certificate issuer can be traced when necessary.

Prove: $A_{IBAnony}$ is defined as the adversary who attacks the anonymity simulation attack of the scheme,A_{Blc} as the adversary against the non-tamperable blockchain,A_{RRS} as the adversary against the unforgeability and verifiability of the RS-MIV case, and A_{RSA} as the opponent against RSA. A polynomial time algorithm $A \in (A_{Blc}, A_{RRS}, A_{RSA})$, which comprises the abilities of all the above-defined attackers, and constructs A through the interaction of $A_{IBAnony}$ and A in the anonymous simulation attack game to perform the attacks. If $A_{IBAnony}$ successfully attacks the traceability, A can successfully attack other parts with a certain probability, including the blockchain non-tamperability, the RS-MIV scheme, and the RSA algorithm.

(1) Initialization: Algorithm A initializes the system, runs the anonymous certificate issuance and verification process in the scheme, hands the certificate public key PK to the attacker $A_{IBAnony}$, and keeps the certificate private key SK and the CA's ring signature S for the certificate.

(2) Query: Opponent $A_{IBAnony}$ queries algorithm A with polynomial bounded degree:

1) The adversary $A_{IBAnony}$ requests the private key SK corresponding to the certificate owned by node i, and algorithm A sends the obtained private key SK to $A_{IBAnony}$ by running the simulated attack games of A_{Blc}, A_{RRS}, and A_{RSA}, respectively.
2) The adversary $A_{IBAnony}$ requests the ring signature threshold knowledge Knl corresponding to the certificate owned by node I, And algorithm A sends the acquired threshold knowledge to $A_{IBAnony}$ by running the simulated attack games of A_{Blc}, A_{RRS}, and A_{RSA}, respectively.
3) The adversary $A_{IBAnony}$ requests the secret information of the CA that issued the certificate to node I, and algorithm A sends the obtained secret information to $A_{IBAnony}$ by running the simulated attack games of A_{Blc}, A_{RRS}, and A_{RSA}, respectively.

(3) Challenge: The adversary $A_{IBAnony}$ outputs the certificate $clCert = CLCert(SK, PK, Cert, Knl)$ and CA's secret message $sig(Cid, r)$ based on the information obtained.

(4) Output: If the certificate output or the CA's secret information is invalid, then the attack is considered as successful.

As a result, the successful attack probability of the adversary $A_{IBAnony}$ is:

$$
\begin{aligned}
Adv_{A_{IBAnony}}(k) &= \Pr\left[Exp_{A_{IBAnony}}(k) = 1\right] \\
&= \Pr[clCert = 1] \cdot \Pr[Address = 1] + \Pr[clCert = 0] \cdot \Pr[Address = 1] + \\
&\Pr[clCert = 1] \cdot \Pr[Address = 0] + \Pr[clCert = 0] \cdot \Pr[Address = 0] \\
&= (\Pr[clCert = 1] + \Pr[clCert = 0]) \cdot (\Pr[Address = 1] + \Pr[Address = 0]) \\
&= (\Pr[Exp_{A_{Blc}}(k) = 1] + \Pr[Exp_{A_{RRS}}(k) = 1]) \cdot \Pr[Exp_{A_{RSA}}(k) = 1] \\
&= (Adv_{A_{Blc}}(k) + Adv_{A_{RRS}}(k)) \cdot Adv_{A_{RSA}}(k)
\end{aligned}
$$

If the attacker A_{Blc} successfully attacks the tamperability of the blockchain, the attacker A_{RRS} successfully attacks the RS-MIV scheme, and the attacker A_{RSA} successfully attacks the RSA algorithm. Thus, $A_{IBAnony}$ can win the traceability simulation attack game of this scheme. However, according to the security of known components, the successful attack probability of $A_{IBAnony}$ is ignored, and thus the scheme meets the traceability.

6 Performance Analysis

We selected the RSA algorithm as 1024 bit, defined E as the exponential operation cost, H as the hash operation cost, the ring size as r, and ignored the cost of multiplication and addition. Table 1 illustrates the calculation cost of the RS-MIV mechanism.

Table 1. The calculation cost of the RS-MIV mechanism.

Process	Algorithm	Expenses
Anonymity issuance of the digital certificate	Hash	H
	RSA	$E+H$
	RS-MIV signature	$(3r+2)E+rH+H$
Anonymity verification of the digital certificate	RS-MIV signature	$rE+H$

From Table 1, we can see that the total calculation cost of our scheme is $(4r+3)E+(r+4)H$, where the highest cost belongs to the RS-MIV signature algorithm. The performance of RS-MIV mechanism is tested on PC with Win10 (64 bit), inter (R) core (TM) i7-7700 @ 3.6 GHz and 16 GB memory. The test results are shown in Fig. 2. When the r is close to 100, the RS-MIV signature algorithm takes 1.2 s, while the RS-MIV signature verification algorithm takes about 0.3 s. However, in practice, the signature algorithm is only used when the digital certificate is issued, which does not affect the performance of the digital certificate application. The efficiency of digital certificate application is only affected by signature verification algorithm. And in practice, the number of Ca nodes that need anonymous digital certificate management will not reach a very large number. When the number of nodes participating in the ring is limited, the time-consuming of the algorithm is acceptable. On the premise that digital certificates can be managed anonymously, this paper considers that the increased time is acceptable for users.

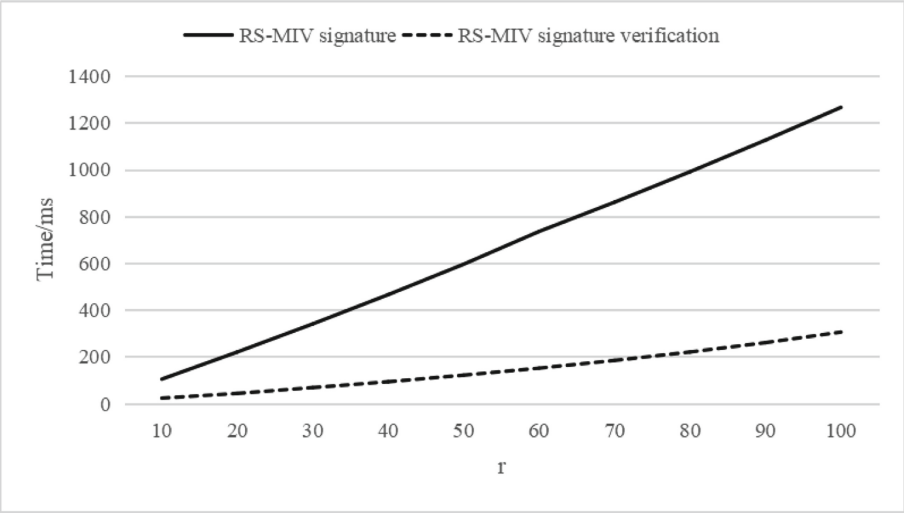

Fig. 2. The relationship between the main algorithm time cost and *r*.

7 Concluding Remarks

In this paper, we propose a ring signature mechanism that can be indirectly verified many times. We design a supervisable anonymous management scheme for digital certificate based on smart contracts, which can guarantees the anonymity of CA nodes in the blockchain PKI and realizes the supervisable anonymous management of digital certificate. However, our solution only uses hash encryption to protect the user's private information in the digital certificate, which cannot meet the on-demand disclosure requirements. Thus, this issue will be studied in future work.

Acknowledgements. This work was supported in part by the National Key Research and Development Program of China under Grant 2018YFB0803603 and Grant 2016YFB0501901, and in part by the National Natural Science Foundation of China under Grant 61502531, Grant 61702550, and Grant 61802436.

References

1. Liu, A., Du, X., Wang, N., Li, S.: Blockchain technology and its research progress in the field of information security. J. Softw. **7**, 2092–2115 (2018)
2. Li, S., Wang, N., Du, X., Liu, A.: Internet web trust system based on smart contract. In: Cheng, X., Jing, W., Song, X., Lu, Z. (eds.) ICPCSEE 2019. CCIS, vol. 1058, pp. 295–311. Springer, Singapore (2019). https://doi.org/10.1007/978-981-15-0118-0_23
3. Faisca, J.G., Rogado, J.Q.: Personal cloud interoperability. In: World of Wireless, Mobile and Multimedia Networks, pp. 1–3 (2016)
4. Zhu, J., Fu, Y.: Dynamic multi center collaborative authentication model of supply chain based on blockchain. J. Netw. Inf. Secur. **2**(1), 27–33 (2016)

5. Kuo, T.T., Hsu, C.N., Ohno-Machado. L.: ModelChain: decentralized privacy-preserving healthcare predictive modeling framework on private blockchain networks
6. Fromknecht, C., Velicanu, D., Yakoubov, S.A.: Decentralized public key infrastructure with identity retention. IACR Cryptology ePrint Archive, 2014: 803 (2014)
7. Wikipedia, "Namecoin," [EB/OL], 28 December 2018. https://en.wikipedia.org/wiki/Namecoin
8. Matsumoto, S., Reischuk, R.M.: IKP: Turning a PKI around with decentralized automated incentives. In: 2017 IEEE Symposium on Security and Privacy (SP), pp. 410–426. IEEE (2017)
9. Al-Bassam, M.: SCPKI: a smart contract-based PKI and identity system. In: Proceedings of the ACM Workshop on Blockchain, Cryptocurrencies and Contracts, pp. 35–40. ACM (2017)
10. Corella, F.: "Implementing a PKI on a Blockchain," Pomcor research in mobile and web technology, [EB/OL], 28 December 2018. https://pomcor.com/2016/10/25/implementing-a-pki-on-a-blockchain/
11. Ben Sasson, E., Chiesa, A., Garman, C.: Zerocash: Decentralized anonymous payments from bitcoin. In: 2014 IEEE Symposium on Security and Privacy (SP). IEEE (2014)
12. Rivest, R.L., Shamir, A., Tauman, Y.: How to leak a secret. In: Boyd, C. (ed.) ASIACRYPT 2001. LNCS, vol. 2248, pp. 552–565. Springer, Heidelberg (2001). https://doi.org/10.1007/3-540-45682-1_32
13. Lv, J., Wang, X.: Verifiable ring signature. In: Proceedings of DMS 2003-The 9th International Conference on Distribted Multimedia Systems, pp. 663–667 (2003)
14. Zhi, G., Ke-Fei, C.: A New verifiable ring signature scheme. Acta Scientiarum Naturalium Universitatis Sunyatseni, **43**(2), 132–134 (2004)
15. Zhang, C., Liu, Y., He, D.: A new verifiable ring signature scheme based on Nyberg-Rueppel scheme. In: International Conference on Signal Processing. IEEE (2006)
16. Wang, C.H., Liu, C.Y.: A new ring signature scheme with signer-admission property. Inf. Sci. **177**(3), 747–754 (2007)
17. Jeong, I., Kwon, J., Lee, D.: Ring signature with weak linkability and its applications. IEEE Trans. Knowl. Data Eng. **20**(8), 1145–1148 (2008)
18. Wen, L.D., Xing, H., Yi, L.: Certificateless verifiable ring signature scheme. Comput. Eng. **15**, 141–143
19. Xiaolin, L., Qianqian, L., Kui, L., et al.: Analysis and improvement of verifiable ring signature scheme. Comput. Appl. **32**(12), 3466–3469 (2012)
20. Zhang, J., He, Y., Li, X.: Security analysis and improvement of two verifiable ring signature schemes. Comput. Eng. Appl. **8**, 115–119 (2016)
21. Dong, Q., Li, X., Liu, Y.: Two extensions of the ring signature scheme of Rivest–Shamir–Taumann. Inf. Sci. **188**, 338–345 (2012)
22. Yang, X.: Research on the strong forward security ring signature scheme based on improved verifiability. Comput. Appl. Softw. **4**, 325–328
23. Bultel, X., Lafourcade, P.: Unlinkable and strongly accountable sanitizable signatures from verifiable ring signatures. In: Capkun, S., Chow, Sherman S.M. (eds.) CANS 2017. LNCS, vol. 11261, pp. 203–226. Springer, Cham (2018). https://doi.org/10.1007/978-3-030-02641-7_10