Research Article

Certificateless Network Coding Ring Signature Scheme

Huifang Yu and Weike Wang

School of Cyberspace Security, Xi'an University of Posts & Telecommunications, Xi'an 710121, China

Correspondence should be addressed to Huifang Yu; yuhuifang@qhnu.edu.cn

Received 10 May 2021; Revised 6 June 2021; Accepted 18 June 2021; Published 1 July 2021

Academic Editor: Azees M

Copyright © 2021 Huifang Yu and Weike Wang. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Traditional certificateless ring signature is not suitable for the network coding environment. In this view, a new certificateless network coding ring signature (CL-NCRS) is devised by using the techniques of multisource network coding and certificateless ring signature. Network coding is a kind of information interaction technology and can improve system robustness and save wireless network resources. CL-NCRS satisfies the unforgeability and unconditional anonymity; moreover, it has relatively higher communication and computational efficiency.

1. Introduction

Network coding is a kind of information interaction technology with the functions of routing and coding and has large information throughput and good robustness. If the nodes encode the messages in a certain mode instead of forwarding them, the network structure can obtain maximum transmission efficiency in theory [1]. In 2002, Cai and Yeung proposed the first network coding security model [2]; the source nodes must understand the internal structure of network, and the edge set may be eavesdropped. Zhou and Xu [3] proposed an antipollution network coding cipher algorithm using homomorphic digital signature which can determine the attackers' location and so can resist the pollution attacks in time. Yu and Li [4] proposed single source network coding homomorphic signature scheme by using the generation identifier and homomorphic hash function, it reduces the communication overhead and saves network resources, and it can resist the intrageneration and intergeneration pollutions. Wang et al. [5] proposed the hybrid network coding scheme that can resist data pollution attacks, label pollution attacks, and intergenerational pollution attacks. Abovementioned network coding schemes are only suitable for single source network coding. Multisource network coding is much more complex. Niu et al. [6] proposed the antipollution multisource network coding

cipher algorithm. Li and Mei [7] proposed homomorphic signature scheme using the generation identifier which can prevent the replay attacks and use the linear operation to reduce the node computing requirement. Network coding signature schemes in [8–10] can effectively prevent the forgery attacks, but the computation overhead in signature and verification phases is high. Li et al. [11] proposed new network coding signature by using homomorphism to solve the problem of identity authentication in multisource network coding.

In ring signature, there is no group administrator and all members in the ring have the same status. A user represents a group of users to sign the message with their own private key. The ring signer can sign the message on behalf of a group of users in completely anonymous way; when the verifier receives the signature, the verifier only knows that the signer comes from a ring but does not know who is the real signer; therefore, it also enhances the privacy of the signer. Ring signature overcomes the defect of excessive authority of the group administrator in group signature. Traditional certificateless ring signature is not appropriate to multisource network coding; it is worth devising an antipollution and certificateless ring signature scheme.

In this paper, on the basis of homomorphic hash function and ring signature theory [12, 13], an efficient and certificateless network coding ring signature (CL-NCRS) is

devised. In CL-NCRS, the source node generates a ring signature for each message vector by using the private key, and the intermediate node linearly combines the received messages and directly generates the ring signature of the combination message by using the homomorphic hash function. CL-NCRS has the unconditional anonymity and UF-CMA security (unforgeability against adaptive message-chosen attacks) [14, 15], and it can defense the pollution attacks.

2. Preliminaries

2.1. Multisource Network Coding Model. In multisource network coding, each source node can send multiple messages and a unified index. Assume $G = (M, E)$ is a multisource network, then M is the node set and E is the edge set. As shown in Figure 1, the source node set is denoted by $S = \{s_1, \dots, s_m\} \subset M$, and the destination node set is denoted by $T = \{t_1, \dots, t_k\} \subset M$.

Each message $\mathbf{v}_i \in (\mathbf{v}_1, \dots, \mathbf{v}_m)$ is composed of n elements in finite field F which can be regarded as a vector in n -dimensional vector space V/F , where $\mathbf{V}_i = (v_{i,1}, \dots, v_{i,n})$, $1 \leq i \leq m$. If $\mathbf{w} = (\mathbf{w}_1, \dots, \mathbf{w}_n)$ is the message sent on any side of the multicast network, the linear combination of l messages received by the intermediate node can be expressed as

$$\mathbf{w} = \sum_{j=1}^l \alpha_j \mathbf{w}_j. \quad (1)$$

The coding coefficient vector $\alpha = (\alpha_1, \dots, \alpha_l)$ is called the local coding vector; then the message $\mathbf{W}$ on one side of message transmission can also be expressed by the linear combination of original message $\mathbf{V}_i$ ($1 \leq i \leq m$):

$$\mathbf{W} = \sum_{i=1}^m \beta_i \mathbf{V}_i, \quad (2)$$

where $\beta = (\beta_1, \dots, \beta_m)$ is called the global coding vector. If the receiving node t_i receives m linearly independent

FIGURE 1: Transmission model for multisource network coding.

messages $(\mathbf{w}_1, \dots, \mathbf{w}_m)$ and the global coding vector is $(\beta_1, \dots, \beta_m)$, the original message $(\mathbf{V}_1, \dots, \mathbf{V}_m)$ can be recovered in the following way:

$$\begin{bmatrix} \mathbf{W}_1 \\ \vdots \\ \mathbf{W}_m \end{bmatrix} = \mathbf{G}_{t_i} \begin{bmatrix} \mathbf{V}_1 \\ \vdots \\ \mathbf{V}_m \end{bmatrix} \left(\mathbf{G}_{t_i} = (\beta_1, \dots, \beta_m)^{-1} \right). \quad (3)$$

Since the received m messages are linearly independent and the matrix $\mathbf{G}_{t_i}$ is full rank and invertible, then the original message $(\mathbf{V}_1, \dots, \mathbf{V}_m)$ is obtained by the following method:

$$\begin{bmatrix} \mathbf{V}_1 \\ \vdots \\ \mathbf{V}_m \end{bmatrix} = \mathbf{G}_{t_i}^{-1} \begin{bmatrix} \mathbf{W}_1 \\ \vdots \\ \mathbf{W}_m \end{bmatrix}. \quad (4)$$

In order to facilitate the decoding of the destination node, the global coding vector β_i and the message can be transmitted together. The extended original message can be regarded as a vector in the $m+n$ dimension vector space V'/F :

$$\mathbf{v}_i = (v_{i,1}, \dots, v_{i,n}, 0, \dots, 0, 1, 0, \dots, 0) \in F^{m+n}, \quad 1 \leq i \leq m. \quad (5)$$

That is to say,

$$\begin{aligned} \mathbf{W} &= \sum_{i=1}^m \beta_i \mathbf{V}_i = \beta_1 \mathbf{V}_1 + \beta_2 \mathbf{V}_2 + \dots + \beta_m \mathbf{V}_m \\ &= (\beta_1 v_{1,1}, \dots, \beta_1 v_{1,n}, \beta_1, 0, \dots, 0) + (\beta_2 v_{2,1}, \dots, \beta_2 v_{2,n}, 0, \beta_2, \dots, 0) + \dots + (\beta_m v_{m,1}, \dots, \beta_m v_{m,n}, 0, 0, \dots, \beta_m) \\ &= (\beta_1 v_{1,1} + \beta_2 v_{2,1} + \dots + \beta_m v_{m,1}, \dots, \beta_1 v_{1,n} + \beta_2 v_{2,n} + \dots + \beta_m v_{m,n}, \beta_1, \beta_2, \dots, \beta_m) \\ &= \left(\sum_{i=1}^m \beta_i v_{i,1}, \dots, \sum_{i=1}^m \beta_i v_{i,n}, \beta_1, \beta_2, \dots, \beta_m \right) \\ &= \left(\sum_{i=1}^m w_{i,1}, \dots, \sum_{i=1}^m w_{i,n}, \sum_{i=1}^m \beta_{i,1}, \sum_{i=1}^m \beta_{i,2}, \dots, \sum_{i=1}^m \beta_{i,m} \right). \end{aligned} \quad (6)$$

Hence, the encoded message can be represented as $\mathbf{W}_i = (w_{i,1}, \dots, w_{i,n}, \beta_{i,1}, \beta_{i,2}, \dots, \beta_{i,m}) = (w_{i,1}, \dots, w_{i,(m+n)})$.

2.2. Homomorphic Hash Function. The trusted third party (TTP) generates a hash parameter set $G = (p, q, \vec{r})$, where p

and q are two large primes and satisfy the condition $q|p-1$. Parameter $\vec{r}$ is a row vector of $1 \times (m+n)$ which is randomly composed of all elements with order q in Z_q :

$$\begin{aligned} \vec{r} &= (1, \dots, m+n), \\ r_i^p &\equiv 1 \pmod{p}, \quad r_i \in Z_p \text{ and } 1 \leq i \leq m+n. \end{aligned} \quad (7)$$

Homomorphism verification of the hash function: for message vector $\mathbf{W}_i = (w_1, \dots, w_{(m+n)})$ received by any node in network, we have

$$H_2(\vec{w}) = \prod_{j=1}^{(m+n)} r_j^{w_j} \pmod{p}. \quad (8)$$

2.3. Bilinear Map. G_1 and G_2 are multiplicative cyclic groups with order q , where $G_1 = \langle g \rangle = \{g^k \mid k = 0, 1, \dots\}$. $e: G_1 \times G_1 \rightarrow G_2$ is a bilinear map with three properties: (1) $e(g^a, h^b) = e(g, h)^{ab}$ for any a and $b \in Z_q$ and g and $h \in G_1$; (2) $e(g, g) \neq 1$; (3) there exists an efficient algorithm to calculate $e(g, h')$ for any g and $h' \in G_1$.

2.4. DL Problem. Given a finite cyclic group $G = \langle g \rangle = \{g^k \mid k = 0, 1, \dots\}$, where g is a generator of group G , $n = |G|$. For $a \in [0, n]$ and $g \in G$, it is easy to calculate $h = g^a$. Given g and $h \in G$, the discrete logarithm (DL) problem is to find a ($0 \leq a \leq n$) such that $h = g^a$.

2.5. Flowchart of CLRS. In this section, we show the working process of a certificateless ring signature (CLRS) by Figure 2.

3. Formal Definition

3.1. Algorithm Definition. A certificateless network coding ring signature (CL-NCRS) scheme is defined as follows.

Setup: input a security parameter 1^k ; this algorithm outputs the master key x and a set ϕ of the system parameter.

Extract: input ϕ and a user's identity ID_i ; this algorithm outputs this the corresponding partial private key D_i .

KeyGen: input ϕ and a user's identity ID_i ; this algorithm outputs this user's secret value x_i and public key Y_i .

Ring signature: input ϕ , the master key x , the message $\vec{v}_j$, the partial private key D_i , the secret value x_i , and the public key Y_i ; this algorithm outputs a signature $\vec{\sigma}$.

Combine: input the coding vector $\vec{\alpha} = (\alpha_1, \dots, \alpha_l)$ and the message vector $(\vec{w}_1, \dots, \vec{w}_l)$; this algorithm outputs a combined message vector $\vec{w}$ and the corresponding signature σ .

Verification: input ϕ , $\vec{\sigma}$, the signer's identity ID_i , the public key Y_i , and the message $\vec{v}_j$. If the verification equation is true, the verifier accepts the signature and stops the game otherwise.

3.2. Security Model. In this section, the UF-CMA security model of CL-NCRS is in terms of the game G_l (G_2) between the challenger B and adversary A1 (A_2) is discussed [16].

Public key queries: A_1 (A_2) queries a public key for the identity ID_i ; B returns a public key.

Partial private key queries: A_1 (A_2) queries a partial private key for the identity ID_i ; B returns a partial private key.

Secret value queries: A_1 (A_2) queries a secret value for the identity ID_i ; B returns a secret value.

Public key replacement: A_1 replaces the previous Y_i with a new public key Y'_i chosen in a suitable range.

Ring signature queries: A_1 (A_2) submits a signature query for a message. B returns a signature σ by calling the signature algorithm.

Combination queries: A_1 (A_2) submits a combination query. B returns a combination signature.

Verification queries: A_1 (A_2) submit a verification query. If the verification equation holds, B outputs a plaintext and otherwise stops the game.

Finally, A_1 (A_2) outputs a forged signature. In queries, A_1 should not request the full private key of identity ID_i ; A_2 cannot query the private key of identity ID_i . In addition, the forged signature should not be returned by any signcryption oracle. A_1 (A_2) wins the G_l (G_2) if the result of unsigncryption is not the symbol $\perp$. We define the advantage of A_1 (A_2) as the probability which it wins the game G_l (G_2).

Definition 1 (unforgeability). A CL-NCRS is UF-CMA secure if no probabilistic polynomial time adversary A_1 (A_2) wins in the G_l (G_2) with nonnegligent advantage.

4. Concrete Instance of CL-NCRS

4.1. Setup. In the setup algorithm, G_1 and G_2 are two multiplicative cyclic groups with order q ; g is a generator of group G_1 ; $e: G_1 \times G_1 \rightarrow G_2$ is a bilinear map, as shown in Section 2.3; $H_1: \{0, 1\}^* \rightarrow G_1$ and $H_2: \{0, 1\}^* \rightarrow Z_q^*$ are one-way hash functions. KGC (Key Generator Center) chooses a master key x from Z_q^* and calculates the system public key $Y = g^x$. Finally, KGC keeps the master key x secret but publishes a set $\phi = \{G_1, G_2, Y, g, q, e, H_1, H_2\}$ of system parameter.

4.2. Extract. In the extraction algorithm, KGC calculates a user's partial private key $D_i = Q_i^x$, where $Q_i = H_1(ID_i)$ and ID_i is the identity of user. Then, KGC sends D_i to the user.

4.3. KeyGen. In the key generation algorithm, a user with ID_i chooses x_i from Z_q^* as a secret value and calculates the corresponding public key $Y_i = g^{x_i}$. The full private key of this user is (x_i, D_i) .

4.4. Ring Signature. In this algorithm, ID_s is the identity of ring signer $ID_s \in \{ID_1, \dots, ID_c\}$, the full private key of the ring signer is (x_s, D_s) , the public key of the ring signer is Y_s , and $\vec{v} \in \{0, 1\}^*$ is a message. Relevant operation steps are carried out as follows:

- (1) For $j = 1, 2, \dots, c$ ($j \neq s$), ring signer randomly selects $a_j \in Z_q^*$ and calculates $\sigma_j = Y_i Y^{a_j}$

FIGURE 2: Flowchart of working process of CLRS.

- (2) Ring signer calculates $\eta = H_2(\vec{v})$
- (3) Ring signer calculates $\sigma_s = (D_s^\eta Q_s^{x_s} / \prod_{j=1, j \neq s}^c \sigma_j)$
- (4) Ring signer outputs a ring signature of message $\vec{v}$: $\vec{\sigma}(u_s) = (\sigma_1(u_s), \dots, \sigma_c(u_s))$ which is recorded as $\vec{\sigma} = (\sigma_1, \dots, \sigma_c)$ for convenience

4.5. Combine. Given the local coding vector $\vec{\alpha} = (\alpha_1, \dots, \alpha_l)$, the message vector received by intermediate nodes $(\vec{w}_1, \dots, \vec{w}_l)$, and its corresponding ring signature $(\vec{\sigma}_1, \dots, \vec{\sigma}_l)$. If the combined message vector is $\vec{w} = \sum_{j=1}^l \alpha_j \vec{w}_j$, then the generation process of signature $\vec{\sigma} = (\sigma_1, \dots, \sigma_c)$ relevant to $\vec{w}$ is $\sigma_j = \prod_{i=1}^l \sigma_{i,j}^{\alpha_i}$, where $\sigma_{i,j}$ ($1 \leq i \leq m$ and $1 \leq j \leq c$) represents the j -th element of $\vec{\sigma}_i$. Then, the combined signature can be expressed as follows:

$$\sigma = \prod_{i=1}^l \sigma_i^{\alpha_i}. \quad (9)$$

4.6. Verification. Given the public keys $Y_1, \dots, Y_c \in G_1$, message $\vec{v}$, and ring signature $\vec{\sigma} = (\sigma_1, \dots, \sigma_c)$, the destination codes calculate $\eta = H_2(\vec{v})$ firstly. If the verification equality $e(Q_s, Y^\eta Y_s) = \prod_{j=1}^c e(\sigma_j, g)$ holds, this means that $\vec{\sigma} = (\sigma_1, \dots, \sigma_c)$ is valid and invalid otherwise.

5. Correctness Analysis

5.1. Signature Verification. After receiving a ring signature $\vec{\sigma} = (\sigma_1, \dots, \sigma_c)$, the receiver calculates $\eta = H_2(\vec{v})$ and then verifies the following equality:

$$e(Q_s, Y^\eta Y_s) = \prod_{j=1}^c e(\sigma_j, g). \quad (10)$$

The verification process of above equality is as follows:

$$\begin{aligned}
 \prod_{j=1}^c e(\sigma_j, g) &= \prod_{j=1, j \neq s}^c e(\sigma_j, g) \cdot e(\sigma_s, g) \\
 &= \prod_{j=1, j \neq s}^c e(Y_i Y^{a_j}, g) \cdot \frac{e(D_s^\eta Q_s^{x_s}, g)}{e(\prod_{j=1, j \neq s}^c Y_i Y^{a_j}, g)} \\
 &= e\left(\prod_{j=1, j \neq s}^c Y_i Y^{a_j}, g\right) \cdot \frac{e(D_s^\eta Q_s^{x_s}, g)}{e(\prod_{j=1, j \neq s}^c Y_i Y^{a_j}, g)} \\
 &= e(Q_s, Y^\eta Y_s).
 \end{aligned} \quad (11)$$

5.2. Combination Verification. Given the message $(\vec{v}_1, \dots, \vec{v}_m)$ and global coding vector $\vec{\beta} = (\beta_1, \dots, \beta_m)$, the message vector $\vec{w} = \sum_{j=1}^m \beta_j \vec{v}_j$ ($1 \leq j \leq m$) is received by the intermediate nodes and the signature corresponds to the message vector $\vec{w}$ is $\vec{\sigma} = (\sigma_1, \dots, \sigma_c)$. In the verification phase, $e(Q_s, Y^\eta Y_s) = \prod_{i=1}^c e(\sigma_i, g)$ holds, where $\eta_j = H_2(\vec{v}_j)$.

In the multisource network coding environment, the intermediate nodes combine the messages from different source nodes and form a combination signature. Each source node s_i has a unique identifier $u_i \in \{u_1, \dots, u_c\}$, the global coding vector of each source node user is expressed as $\beta_j(u_1), \dots, \beta_j(u_c)$, respectively. In order to distinguish the possible combination of the same message vector, the message vector is expressed as $\vec{w} = \sum_{j=1}^m \sum_{k=1}^d \beta_j(u_k) \vec{v}_j$ ($1 \leq j \leq m$).

Ring signature of message vector $\vec{w}$ can be expressed as $\vec{\sigma} = \prod_{j=1}^m \prod_{k=1}^d (\sigma_j(u_k))^{\beta_j(u_k)}$, and then, the i -th component in ring signature can be expressed as $\vec{\sigma}_i = \prod_{j=1}^m \prod_{k=1}^d (\sigma_j(u_k))^{\beta_j(u_k)}$, $1 \leq i \leq c$, where $\sigma_{j,i}(u_k)$

denotes the i -th component of ring signature $\vec{\sigma}_j(u_k)$. Then, the verification process of the equality $e(Q_s, Y^{\eta_j} Y_s) = \prod_{i=1}^c e(\sigma_i, g)$ is as follows:

$$\begin{aligned} \prod_{i=1}^c e(\sigma_i, g) &= \prod_{i=1}^c e\left(\prod_{j=1}^m \prod_{k=1}^d (\sigma_{j,i}(u_k)^{\beta_j(u_k)}), g\right) \\ &= \prod_{j=1}^m \prod_{k=1}^d e\left(\prod_{i=1}^c \sigma_{j,i}(u_k), g\right)^{\beta_j(u_k)} \\ &= \prod_{j=1}^m \prod_{k=1}^d \left(\prod_{i=1}^c e(\sigma_{j,i}(u_k), g)^{\beta_j(u_k)}\right). \end{aligned} \quad (12)$$

Then, the verification equality $e(Q_s, Y^{\eta_j} Y_s) = \prod_{j=1}^m e(\sigma_j(u_s), g)$ holds and the verification of message $\vec{v}_j$ can be denoted as $e(Q_s, Y^{\eta_j} Y_s) = \prod_{i=1}^c e(\sigma_{j,i}(u_s), g)$, and the verification process of this equality is shown as follows:

$$\begin{aligned} &\prod_{j=1}^m \prod_{k=1}^c \left(\prod_{i=1}^c e(\sigma_{j,i}(u_k), g)^{\beta_j(u_k)}\right) \\ &= \prod_{j=1}^m \prod_{k=1}^c e(Q_s, Y^{\eta_j} Y_s)^{\beta_j(u_k)} \\ &= \prod_{j=1}^m e\left(Q_s, Y^{\sum_{k=1}^c \beta_j(u_k)} Y_s\right) \\ &= \prod_{j=1}^m e(Q_s, Y^{\eta_j^{\beta_j}} Y_s) \\ &= e\left(\prod_{j=1}^m Q_s, Y^{\eta_j^{\beta_j}} Y_s\right) \\ &= e(Q_s, Y^{\eta_j} Y_s). \end{aligned} \quad (13)$$

6. Security Analysis

In CL-NCRS, no external attacker can obtain any message signature without the members' private key. CL-NCRS is vulnerable to two types of adversaries: A_1 and A_2 . Here, A_1 is a malicious user who can change the public key of any user but cannot know the master key of the system; A_2 is a malicious KGC who knows the master key of the system but cannot change any user's public key and provide the security proof of existential unforgeability, unconditional anonymity, and antipollution attacks under adaptive chosen-plaintext attacks.

Theorem 1. *In the random oracle model, if a probabilistic polynomial time adversary A_1 can break the UF-CMA-I security of CL-NCRS with probability ϵ , then there must exist an algorithm B to solve the discrete logarithm (DL) problem with*

probability ϵ' (q_p , q_s , and q_r are the query times of partial private key, secret value, and public key replacement, respectively), where $\epsilon' \geq (\epsilon/e(q_s + q_p + q_r))$.

Proof. Given a discrete logarithm random instance $(g, g^a) \in G_1$, the aim of the challenger B is to use the adversary A_1 as a subroutine to obtain the value of a . B selects a challenge identity ID^* and maintains the initially empty lists L_1, L_2, L_3, L_4 , and L_5 which represent the H_1 query list, the H_2 query list, the public key query list, the signature query list, and the combination query list, respectively. At first, B runs the setup algorithm to obtain the system parameter $\phi = \{G_1, G_2, Y = g^a, g, q, e, H_1, H_2\}$ and then sends ϕ to A_1 , where a acts as the master key of system and is unknown to B . Then, A_1 adaptively carries out a series of polynomial bounded queries as follows.

Public key queries: A_1 queries a public key for the identity ID_i . B returns Y_i to A_1 and adds $(U, ID_i, Y_i, x_i, -)$ into the list L_3 .

H_1 queries: A_1 queries the H_1 oracle for the identity ID_i . If the relevant content already exists in the list L_1 , B returns h_i as answer; otherwise, B returns $Q_i \leftarrow g^{\lambda_i}$ and adds $(U, ID_i, -, Q_i, \lambda_i)$ into the list L_1 , where λ_i is a random from Z_q^* .

H_2 queries: A_1 queries the H_2 oracle for the identity ID_i . If the corresponding query result already exists in the list L_2 , B returns h_2 as the answer; otherwise, B returns a random number h_2 from Z_q^* and adds $(U, ID_i, \vec{v}, h_2)$ into the list L_2 .

Partial private key queries: A_1 queries a partial private key for the identity ID_i . B responds as follows: (1) if $ID_i = ID^*$, B fails and terminates the game; (2) if $ID_i \neq ID^*$, B returns $D_i \leftarrow Y_i^{\lambda_i}$ to A_1 and updates the list L_3 with (U, ID_i, Y_i, x_i, D_i) .

Secret value queries: A_1 queries a secret value for the identity ID_i . If $ID_i \neq ID^*$, B outputs the secret value x_i from the list L_3 ; otherwise, B fails and terminates the game.

Public key replacement: A_1 chooses Y'_i to replace the public key of the identity ID_i . If $ID_i = ID^*$, B fails and terminates the game; otherwise, B updates list L_3 with $(U, ID_i, Y'_i, -)$.

Ring signature queries: A_1 submits a ring signature query. If $ID_s \neq ID^*$ and the public key of identity ID_i is not replaced, B returns a signature by running ring signature algorithm. If $ID_s = ID^*$ and the public key of identity ID_i has been replaced, B responds as follows:

- (1) B randomly selects $a_j \in Z_q^*$ to calculate $\sigma_j = Y_i Y^{a_j}$ ($1 \leq j \leq c$ and $j \neq s$) and $\eta = H_2(\vec{v})$
- (2) B calculates $\sigma_s = (Y^{\eta \lambda_s} Y_s^{\lambda_s} / \prod_{j=1, j \neq s}^c \sigma_j)$ and adds $(\vec{v}, U, ID_i, a_j, \eta, \sigma_j, \sigma_s)$ into the list L_4
- (3) B returns $\vec{\sigma}(u_s) = (\sigma_1(u_s), \dots, \sigma_c(u_s))$

Combination queries: A_1 submits a combination query. B calculates the combination message vectors $\vec{w} = \sum_{j=1}^l \alpha_j \vec{w}_j$, and the signature of $\vec{w}$ is $\sigma_j = \prod_{i=1}^l \sigma_{i,j}^{\alpha_i}$, where $\sigma_{i,j}$ ($1 \leq i \leq m$ and $1 \leq j \leq c$) represents the j -th element

of $\vec{\sigma}_i$. Finally, B returns the combination signature $\sigma = \prod_{i=1}^l \sigma_i^{\alpha_i}$ to A_1 and stores $(\vec{\alpha}, \vec{w}, \sigma)$ in the list L_5 . Note that $\vec{\alpha} = (\alpha_1, \dots, \alpha_l)$ is the local coding vector; $(\vec{w}_1, \dots, \vec{w}_l)$ are the message vectors, and $(\vec{\sigma}_1, \dots, \vec{\sigma}_l)$ are the ring signatures.

Verification queries: A_1 submits a verification query. If $e(Q_s, Y^\eta Y_s) = \prod_{j=1}^c e(\sigma_j(u_s), g)$ holds, B outputs a valid ring signature and terminates the game otherwise.

After a series of adaptive queries, A_1 outputs a forgery $(\vec{v}^*, U, ID^*, a_j^*, \eta^*, \sigma_j^*, \sigma_s^*)$ to B . A_1 does not know the private key of any member in the ring. In the probabilistic polynomial time, two valid signatures are generated as follows:

$$\begin{aligned} \sigma_s &= \left(\frac{D_s^\eta Q_s^{x_s}}{\prod_{j=1, j \neq s}^c Y_i Y^{a_j}} \right), \\ \sigma_s &= \left(\frac{D_s^{*\eta^*} Q_s^{x_s^*}}{\prod_{j=1, j \neq s}^c Y_i^* Y^{a_j^*}} \right). \end{aligned} \quad (14)$$

Then, the solution a of DL problem instance can be obtained via the above equalities:

$$a = \frac{\left(\sum_{j=1, j \neq s}^c \log(Y_i Y_i^{*-1}) \right) + \lambda_s^* x_s^* - \lambda_s x_s}{\lambda_s \eta - \lambda_s^* \eta^* - \sum_{j=1, j \neq s}^c (a_j - a_j^*)}. \quad (15)$$

Referring to the probability analysis in [16], we obtain that the probability $\epsilon' \geq (\epsilon/e(q_s + q_p + q_r))$ of B in solving the discrete logarithm problem in polynomial time is negligible. Hence, A_1 cannot break the UF-CMA-I security of CL-NCRS. $\square$

Theorem 2. *In the random oracle model, if a probabilistic polynomial time adversary A_2 can break the UF-CMA-II security of CL-NCRS with probability ϵ then, there must exist an algorithm B to solve the discrete logarithm (DL) problem with probability ϵ' (q_s is the query time relevant to the secret value oracle), where $\epsilon' \geq (\epsilon/e q_s)$.*

Proof. Given a discrete logarithm random instance $(g, g^a) \in G_1$, the purpose of B is to use the adversary A_1 as a subroutine to obtain the value of a . L_1, L_2, L_3, L_4 , and L_5 store the values of the query and answer of various random oracles. At first, B runs the initialization algorithm to obtain $\phi = \{G_1, G_2, Y = g^x, g, q, e, H_1, H_2\}$ and then sends ϕ and x to A_2 . Then, A_2 carries out a series of queries in an adaptive way. Note that the H_1 and H_2 oracle queries and answers are as those in Theorem 1.

Public key queries: A_2 queries a public key for the identity ID_i . B returns $Y_i \leftarrow g^{x_i}$ to A_2 as the answer and adds $(U, ID_i, Y_i, x_i, -)$ to the list L_3 if $ID_i \neq ID^*$; otherwise, B returns $Y_i \leftarrow g^a$ to A_2 as the answer and adds $(U, ID_i, Y_i, -, -)$ to the list L_3 .

Partial private key queries: A_2 queries a partial private key for the identity ID_i . B responds as follows: (1) if $ID_i = ID^*$, B fails and terminates the game; (2) if $ID_i \neq ID^*$ and there is a query value, B returns $D_i \leftarrow g^{x_{\lambda_i}}$ to A_2 .

Secret value queries: A_2 queries a secret value for the identity ID_i . B calls the public key oracle and returns a secret value x_i if $ID_i \neq ID^*$ and terminates the game otherwise.

Ring signature queries: for a ring signature query, B returns a signature to A_2 by calling the ring signature algorithm if $ID_s \neq ID^*$; otherwise, B responds as follows:

- (1) B randomly selects $a_j \in \mathbb{Z}_q^*$ to calculate $\sigma_j = Y_i Y^{a_j}$ ($1 \leq j \leq c$ and $j \neq s$) and $\eta = H_2(\vec{v})$
- (2) B calculates $\sigma_s = (g^{\eta x_{\lambda_s}} Y_i^{\lambda_s} / \prod_{j=1, j \neq s}^c \sigma_j)$ and adds $(\vec{v}, U, ID_i, a_j, \eta, \sigma_j, \sigma_s)$ into the list L_4
- (3) B returns $\vec{\sigma}(u_s) = (\sigma_1(u_s), \dots, \sigma_c(u_s))$

Combination queries: A_2 issues a combination query. Note that $(\vec{\sigma}_1, \dots, \vec{\sigma}_l)$ are the ring signatures. B calculates the combination message vector $\vec{w} = \sum_{j=1}^l \alpha_j \vec{w}_j$, where $\vec{\alpha} = (\alpha_1, \dots, \alpha_l)$ is the local coding vector and $(\vec{w}_1, \dots, \vec{w}_l)$ are the message vectors. $\sigma_j = \prod_{i=1}^l \sigma_{i,j}^{\alpha_i}$ is the signature of $\vec{w}$, where $\sigma_{i,j}$ ($1 \leq i \leq m$ and $1 \leq j \leq c$) represents the j -th element of $\vec{\sigma}_i$. Finally, B returns a combination signature $\sigma = \prod_{i=1}^l \sigma_i^{\alpha_i}$ to A_2 and stores $(\vec{\alpha}, \vec{w}, \sigma)$ in the list L_5 .

Verification queries: A_2 submits a verification query. B outputs a valid ring signature if $e(Q_s, Y^\eta Y_s) = \prod_{j=1}^c e(\sigma_j, g)$ and terminates the game otherwise.

After a sequence of adaptive queries, A_2 outputs a forgery $(\vec{v}^*, U, ID^*, a_j^*, \eta^*, \sigma_j^*, \sigma_s^*)$ to B . A_2 does not know the private key of any member in the ring. In the probabilistic polynomial time, two valid signatures are obtained as follows:

$$\begin{aligned} \sigma_s &= \left(\frac{D_s^\eta Q_s^{x_s}}{\prod_{j=1, j \neq s}^c Y_i Y^{a_j}} \right), \\ \sigma_s &= \left(\frac{D_s^{*\eta^*} Q_s^{x_s^*}}{\prod_{j=1, j \neq s}^c Y_i^* Y^{a_j^*}} \right). \end{aligned} \quad (16)$$

Then, the solution a of the discrete logarithm problem can be obtained by the above two signatures:

$$a = \frac{\left(\sum_{j=1, j \neq s}^c \log(Y_i Y_i^{*-1}) \right) + x(\lambda_s^* \eta^* - \lambda_s \eta \sum_{j=1, j \neq s}^c (a_j - a_j^*))}{\lambda_s - \lambda_s^*}. \quad (17)$$

Referring to the probability analysis in [16], the probability of B in solving the discrete logarithm problem in the probabilistic polynomial time is negligible. Hence, A_2 cannot break the UF-CMA-II security of CL-NCRS. $\square$

Theorem 3. *CL-NCRS can resist the pollution attacks in the multisource network coding environment.*

Proof. In CL-NCRS, if the adversary attempts to forge a ring signature, it must obtain a ring signer's private key by solving the discrete logarithm problem. As we know, it is computationally infeasible to solve the discrete logarithm problem. If the adversary wants to forge a valid signature, the forger has to perform the following operations:

TABLE 1: Feature comparison of several schemes.

Reference	Unforgeability	Unconditional anonymity	Public key cryptosystem	Is it suitable for network coding?
Chen's scheme	✓	✓	Identity-based	No
Zhao's scheme	✓	✓	Identity-based	No
Yu's scheme	×	×	Identity-based	Yes
CL-NCRS scheme	✓	✓	Certificateless	Yes

TABLE 2: The time complexity of cryptographic operations.

Cryptographic operations	Time (ms)
Time to perform an exponential operation: C_{me}	0.83
Time to perform a scalar multiplication: C_{mul}	0.75
Time to perform a hash operation: C_{mtp}	1.18
Time to perform a bilinear operation: C_{par}	2.75

TABLE 3: Computational efficiency comparison of several schemes.

Reference	Signature length	Signature time (ms)	Verification time (ms)	Total time (ms)
Chen's scheme	$O(l2^{n-1}n \text{ lb } n)$	$(2n+1) C_{mul} + 2nC_{mtp}$	$2C_{par} + 4nC_{mul} + nC_{mtp}$	$3C_{par} + (6n+1) C_{mul} + (3n+1) C_{mtp} + C_{me}$
Zhao's scheme	$O(l2^{n-1}n^2 \text{ lb } n)$	$(4n+2) C_{me}$	$2nC_{par} + (2n+3) C_{me}$	$(2n+1) C_{par} + (6n+5) C_{me} + 2C_{mtp} + nC_{mul}$
Yu's scheme	$O(l2^n n^2 \text{ lb } n)$	$2nC_{me} + 2nC_{mul} + C_{mtp}$	$(2n+1) C_{me} + C_{mtp} + (n+2) C_{par}$	$(5n+2) C_{me} + 2nC_{mul} + 5C_{mtp} + (n+2) C_{par}$
CL-NCRS scheme	$O(2^{n-1}n \text{ lb } n)$	$(n+2) C_{me} + 2C_{mtp} + nC_{mul}$	$2C_{par} + (n+4) C_{me} + 3C_{mtp} + nC_{mul}$	$3C_{par} + (2n+7) C_{me} + 7C_{mtp} + 2nC_{mul}$

- (1) The forger attempts to sign a forged message directly. In the ring signature algorithm of CL-NCRS, it is needful to use the signer's private key and $a_j \in Z_q^*$ ($1 \leq j \leq c$ and $j \neq s$) to sign the message. Obtaining the private key from the ring signer's public key is equivalent to solving the discrete logarithm problem; and it is also equivalent to solving the discrete logarithm problem to obtain a_j from a signature.
- (2) The forger tried to obtain a valid signature by exhaustive search. Assume that the length of an element in ring signature is n and the number of ring members is m , then the size of ring signature is $n \times m$. For example, if n is 256 bit on the elliptic curve, the size of ring signature is $256 \times m$, and it is difficult to solve the discrete logarithm of 1589 bit [17]. Obviously, it is impossible to obtain a valid ring signature. $\square$

Theorem 4. CL-NCRS can satisfy the unconditional anonymity of ring signers.

A CL-NCRS can meet the unconditional anonymity [18–20]: no attacker can obtain the private key of all possible signers in illegal ways.

Proof. Given a signature set $\vec{\sigma} = (\sigma_1, \dots, \sigma_c)$ of identity set $L = (ID_1, \dots, ID_n)$ and the corresponding public key set $PK = (PK_1, \dots, PK_n)$, ID_s of the real signer in the ring and ξ is the probability of ring signature $\vec{\sigma} = (\sigma_1, \dots, \sigma_c)$.

For the adversary, since a_j ($j \neq s$ and $a_j \neq 1$) is randomly chosen from Z_q^* , then the probability of selecting $a_1, a_2, \dots, a_{s-1}, a_{s+1}, \dots, a_c$ in turn is

$$\frac{1}{q-1} \times \frac{1}{q-2} \times \dots \times \frac{1}{q-c+1}. \quad (18)$$

For $\sigma_s = (D_s^q Q_s^{x_s} / \prod_{j=1, j \neq s}^c Y_i Y^{a_j})$, the probability of selecting all $a_1, a_2, \dots, a_c$ in turn is

$$\xi = \frac{1}{q} \times \frac{1}{q-2} \times \dots \times \frac{1}{q-c+1} \times \frac{1}{q-c}. \quad (19)$$

Here, ξ has nothing to do with the identity of the ring signer. If the adversary obtains the private keys of all users in the ring and even if the verifier can verify the ring signature, the probability of inferring the identity of the real ring signer from valid signature is less than $1/c$. It is obvious that CL-NCRS satisfies the unconditional anonymity of the real signer. $\square$

7. Performance Analysis

In this section, we provide the performance comparison between CL-NCRS and relevant schemes [15, 21, 22]. Table 1 shows the comparison of the relevant features of several schemes. According to the analysis, it is found that Chen's scheme and Zhao's scheme are not suitable for the network coding environment. Table 2 shows the time complexity of main cryptography operations [4]. Table 3 shows the comparison case of several schemes, where l is the output

FIGURE 3: Comparison of signature time.

FIGURE 4: Comparison of verification time.

FIGURE 5: Total time comparison of several schemes.

length of bilinear pairing. From the comparison of signature length in Table 3, it can be seen that the computational complexity of CL-NCRS is relatively lower.

Simulation curves of time-consuming signature of several schemes are shown in Figure 3. Simulation curves of time-consuming verification of several schemes are shown in Figure 4. The simulation curve of total algorithm time of several schemes is shown in Figure 5. Because two comparison schemes are not suitable for the network coding environment, for the convenience, we omit the network coding combination phase. The number of ring members n is 10, 20, 30, 40, and 50. Experiment results show that the running time of different schemes increases linearly with the increase of the number of ring members. As shown in Figure 3, in the signature phase, the growth rate of CL-NCRS is relatively slower than that of other schemes. As seen from Figure 4, the computational efficiency of CL-NCRS is the highest. In terms of total time in Figure 5, CL-NCRS takes the least time. In addition, the computational cost of other schemes is relatively high. Hence, CL-NCRS is the good cryptography scheme with short communication length and high computation efficiency.

8. Conclusion

Based on the certificateless ring signature and homomorphic hash function, a new certificateless network coding ring signature (CL-NCRS) is proposed. CL-NCRS satisfies the unforgeability against adaptive chosen-message attacks and unconditional anonymity of the real ring signer. CL-NCRS can resist the pollution attacks in the network coding environment and has the characteristics of low computation complexity and strong robustness. The limitation of this scheme is that it requires to send the message in undistorted ways.

Data Availability

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

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work was supported by the Key Program of Natural Science Foundation of Shanxi Province under Grant no. 2020JZ-54.

References

- [1] R. Ahlswede, N. Ning Cai, S.-Y. R. Li, and R. W. Yeung, "Network information flow," *IEEE Transactions on Information Theory*, vol. 46, no. 4, pp. 1204–1216, 2000.
- [2] N. Cai and R. W. Yeung, "Secure network coding," in *Proceedings of the IEEE International Symposium on Information Theory*, p. 323, Ulm, Germany, August 2002.
- [3] Z. B. Zhou and L. Xu, "Pollution-resistant network coding scheme based on digital signature," *Computer Systems Applications*, vol. 25, no. 6, pp. 185–190, 2016.
- [4] H. F. Yu and W. Li, "Homomorphic signature schemes for single-source and multi-source network coding," *Journal on Communications*, vol. 40, no. 11, pp. 112–121, 2019.
- [5] Y. X. Wang, X. J. Lin, and H. P. Qu, "An effective hybrid network coding scheme against pollution attacks," *Netinfo Security*, vol. 2019, no. 5, pp. 69–76, 2019.
- [6] S. F. Niu, C. F. Wang, Y. L. Zhang, and S. Z. Cao, "Data integrity verification scheme for multi-source network coding," *Computer Engineering*, vol. 41, no. 3, pp. 21–25, 2015.
- [7] S. H. Li and Z. H. Mei, "Homomorphic signature scheme for network coding against inter-generation pollution attacks," *Computer Technology and Development*, vol. 26, no. 10, pp. 73–76, 2016.
- [8] D. Boneh, D. Freeman, J. Katz, and B. Waters, "Signing a linear subspace: signature schemes for network coding," in *Proceedings of the The International Workshop on Public Key Cryptography*, pp. 68–87, Springer, Irvine, CA, USA, March 2009.
- [9] G. J. Liu and B. Wang, "Secure network coding against intra/inter-generation pollution attacks," *China Communications*, vol. 10, no. 8, pp. 100–110, 2013.
- [10] C. Cheng, T. Jiang, Y. Liu, and M. W. Zhang, "Security analysis of a homomorphic signature scheme for network coding," *Security and Communication Networks*, vol. 8, no. 18, pp. 4053–4060, 2016.
- [11] T. Li, W. Chen, Y. Tang, and H. Yan, "A homomorphic network coding signature scheme for multiple sources and its application in IoT," *Security and Communication Networks*, vol. 2018, Article ID 9641273, 6 pages, 2018.
- [12] H. S. Qin, L. Zhang, Y. Q. Feng, C. B. He, and W. J. Wu, "Certificateless ring signcryption scheme without paring design," *Computer Engineering and Design*, vol. 34, no. 3, pp. 841–844, 2013.
- [13] C. L. Liu and L. You, "Linkable certificateless ring signature scheme," *Communications Technology*, vol. 52, no. 8, pp. 1967–1970, 2019.
- [14] H. J. Yang, *Analysis and Improvement of Ring Signature*, Kunming University of Science and Technology, Kunming, China, 2015.
- [15] H. F. Yu and X. Z. Gao, "Homomorphic ring signature scheme technology for multi-source network coding," *Netinfo Security*, vol. 19, no. 2, pp. 36–42, 2019.
- [16] H.-F. Yu and B. Yang, "Low-computation certificateless hybrid signcryption scheme," *Frontiers of Information Technology & Electronic Engineering*, vol. 18, no. 7, pp. 928–940, 2017.
- [17] D. Boneh, B. Lynn, and H. Shacham, "Short signatures from the weil pairing," in *Proceedings of the International Conference on the Theory and Application of Cryptology and Information Security*, pp. 514–532, Berlin Springer, Gold Coast, Australia, December 2001.
- [18] J. Subramani, D. Muneeswaran, A. Maria, M. Arunachalam, R. Neelagandan, and B. Eppas, "Energy-efficient privacy-preserving and physically secure mutual authentication scheme for secure communication in smart grid systems,"

- International Journal of Communication Systems*, vol. 34, no. 8, 2021.
- [19] J. Subramani, A. Maria, R. B. Neelakandan, and A. S. Rajasekaran, "Efficient anonymous authentication scheme for automatic dependent surveillance-broadcast system with batch verification," *IET Communications*, vol. 15, no. 9, pp. 1187–1197, 2021.
 - [20] J. Subramani, A. Maria, R. B. Neelagandan, U. Subramaniam, J. Almakhlles, and J. D. Epaw, "Efficient privacy preserving anonymous mutual authentication scheme for wireless body area networks (WBANs)," *IEEE Access*, vol. 8, pp. 48576–48586, 2020.
 - [21] S. J. Chen, S. P. Zhai, and Y. J. Wang, "Blockchain privacy protection algorithm based on ring signature," *Journal of Xidian University*, vol. 47, no. 5, pp. 86–93, 2020.
 - [22] Y. Q. Zhao, Q. Q. Lai, Y. Yu, B. Yang, and Y. Zhao, "ID-based ring signature in the standard model," *Acta Electronica Sinica*, vol. 46, no. 4, pp. 1019–1024, 2018.