Computers, Materials & Continua CMC, vol.65, no.2, pp.1559-1570, 2020

A Trust Value Sharing Scheme in Heterogeneous Identity Federation Topologies

Ning Liu[1], Fan Yang[1, *], Xi Xiong[1, 2], Yan Chang[1] and Shibin Zhang[1]

Abstract: Recent developments in heterogeneous identity federation systems have heightened the need for the related trust management system. The trust management system evaluates, manages, and shares users' trust values. The service provider (SP) members of the federation system rely on users' trust values to determine which type and quality of service will be provided to the users. While identity federation systems have the potential to help federated users save time and energy and improve service experience, the benefits also come with significant privacy risks. So far, there has been little discussion about the privacy protection of users in heterogeneous identity federation systems. In this paper, we propose a trust value sharing scheme based on a proxy ring signature for the trust management system in heterogeneous identity federation topologies. The ring signature schemes can ensure the validity of the data and hide the original signer, thereby protecting privacy. Moreover, no group manager participating in the ring signature, which naturally matches with our decentralized heterogeneous identity federation topologies. The proxy signature can reduce the workload of the private key owner. The proposed scheme shortens the calculation time for verifying the signature and then reduces the overall time consumption in the process of trust sharing. Our studies prove that the proposed scheme is privacy-preserving, efficient, and effective.

Keywords: Heterogeneous identity federation system, proxy ring signature, trust value sharing scheme.

1 Introduction

Since traditional identity authentication systems only can manage identities for a single service provider (SP), a user may own many identities and access services that are offered by the corresponding SPs. To obtain numerous services, users have to register, remember, and manage various identities of different systems, which are repetitive and complicated tasks. Therefore, identity federation systems came into being to prevent users from getting into such kind of troubles. The users who want to obtain services from federated SPs only

[1] School of Cybersecurity, Chengdu University of Information Technology, Chengdu, China.

[2] The School of Computer Science and Engineering, Nanyang Technological University, Singapore.

[*] Corresponding Author: Yang Fan. Email: yangfan63@cuit.edu.cn.

Received: 10 March 2020; Accepted: 09 June 2020.

need to be authorized by the identity provider once [Lutz and Stiller (2013)].

The researches of identity federation systems have received a lot of attention in many areas [Perez-Mendez, Pereniguez-Garcia, Marin-Lopez et al. (2014)]. Many successful research projects have been carried out, such as deploying authorization mechanisms for federated services (DAMe), secure widespread identities for federated telecommunications (SWIFT), and secure management of information across multiple stakeholders (SEMIRAMIS).

Some studies investigated the trust management of heterogeneous identity federation systems in recent years. Yang et al. [Yang, Li, Li et al. (2019)] have proposed a unified identity information identification model for heterogeneous identity federation systems based on blockchain. Their study investigated cross-domain access. In order to obtain the users' trust values, in the first step, each SP member of the federation system needs to calculate the users' trust values individually, and then the smart contract or the third-party audit on the federation chain will collect the trust values from every SP and calculate the final comprehensive trust values. In this architecture, a trust model and a risk assessment method for cross-domain authentication based on the cloud model were proposed by Dong et al. [Dong, Chen and Li (2019)]. Their research focuses on trust evaluation and delivery. Their study assesses users' trust values according to the related certification. Users' dynamic behavior is not taken into consideration when conducting the trust evaluation.

Most studies about the trust system of the heterogeneous identity federation system mainly focus on the trust evaluation, only a few studies about the process of sharing the trust value have been carried out. Privacy-preserving is one of the primary concerns in the identity federated system [Sanchez, Almenares, Arias et al. (2012)]. These researches have not been able to establish a trust data sharing scheme that can protect users' behavior privacy in the heterogeneous identity federation systems.

It is now well known that the cryptography mechanism is effective at ensuring the validity and protecting privacy [Xiong and Shi (2018)]. In the trust management system of the heterogeneous identity federation architecture, each SP member needs to sign the newly added block during conducting trust value updates. The signature can ensure the validity of the updated trust value since only the members of the identity federation have the private key to make a valid signature. Also, the anonymous ring signature helps to hide the original signer, who modifies the user's trust value according to users' behavior, thereby protecting the behavior privacy of the user. Furthermore, our proposed scheme, based on the proxy ring signature, can decentralize the authority of signing new blocks of the trust chain to the staff of SP, which will increase the effectiveness of the trust management process.

2 Overview of ring signatures

In this paper, we propose a trust value sharing scheme for protecting the validity and privacy of trust values in the heterogeneous identity federation topologies. The identity-based proxy ring signature is utilized to achieve the aim of this study. The original ring signature schemes leak secret and keep anonymous. The ring signature was formalized by Rivest et al. [Rivest, Shamir and Tauman (2001)] to a simplified group signature. Unconditional anonymity of the ring signature provides natural privacy protection for the

actual signers. The original ring signature does not consider that the management of public key certificate verification is complicated and time-consuming. To improve the efficiency, Zhang et al. [Zhang and Kim (2002)] introduced the concept of identity-based to the ring signature. This scheme is proven to be secure in the random oracle model. The concept of proxy was introduced to the ring signatures much later than the identity-based one. Proxy signatures allow Alice to delegate her signing authority to Bob, and Bob can sign a message on behalf of Alice, lead to improved overall efficiency.

Most of the ring signatures proposed after 2007 are pairing-based cryptosystems [Awasthi and Lal (2007); Wu and Li (2009); Ajmath, Reddy, Rao et al. (2012); Sarde and Banerjee (2017); Gu, Jia and Zhang (2017); Boyen and Haines (2018)]. These schemes rely on less analyzed computational assumptions in their security analyses compared with those based on traditional assumptions [Asaar, Salmasizadeh and Susilo (2015a)]. In 2015, Asaar et al. [Asaar, Salmasizadeh and Susilo (2015a)] proposed the first provably secure identity-based proxy ring signature (PSIPRS) based on RSA. In the same year, a shorter solution, a short identity-based proxy ring signature (SIPRS) scheme from RSA, was available [Asaar, Salmasizadeh and Susilo (2015b)]. Also, the ring signature has been used to protect the privacy of the blockchain, by protecting the information of the transaction initiator [Li, Mei, Gong et al. (2020)]. However, both schemes need the identity information of the proxy signer in the process of signing. The identity of the proxy signer is displayed in the signature. In the scenario of the identity federation system, the leakage of the identity of the proxy signer could put users' privacy at risk. In addition, the timestamp is not considered in these schemes. Moreover, the time required for signature verification in both schemes is relatively long. When the signature needs to be verified by every member of the federation, the overall time consumption is relatively high.

3 Trust management system of the heterogeneous identity federation system

In order to provide users with a variety of services, the heterogeneous identity federation system brings different SPs together. Based on the users' trust value, SP decides which kind of content and quality of services can be provided. SPs usually use independent trust management system. However, in the identity federation system, each SP needs to conduct the same trust management process on users, such as trust evaluation, storage, and sharing.

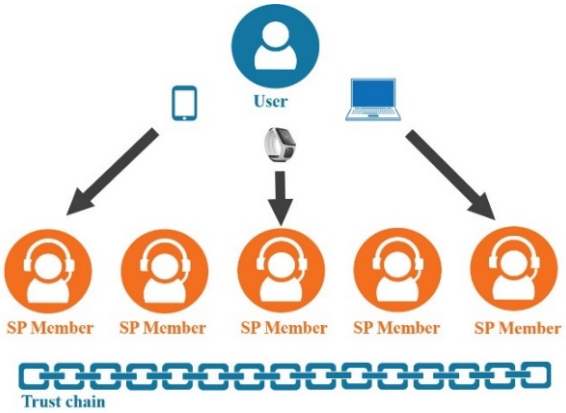

Figure 1: The construction of the heterogeneous identity federation system

The structure of the trust management system for the heterogeneous identity federation is illustrated in Fig. 1.

The heterogeneous identity federation system is mainly composed of three parts: users, SP members, and the trust chain. SP members provide services to the federated users, and they are linked by the trust chain which is a blockchain-based technology. Only SP members can add new blocks to the trust chain. Each of them has the permission and ability to verify whether any block is true. When users need to obtain services, SP members can access the federation trust management system to determine whether to provide services to them.

Fig. 2 shows an example of a process in which a user requests service from an SP member of a heterogeneous federation system.

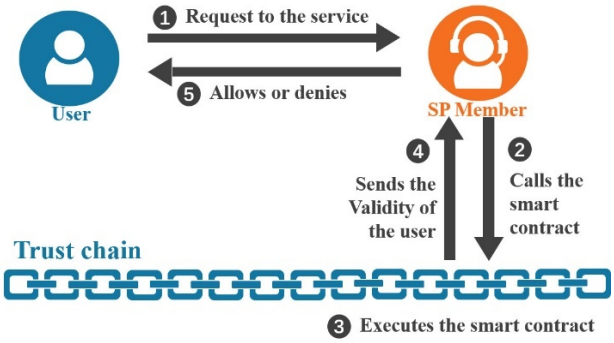

Figure 2: The flowchart of the request process

First, the user should submit the service request to the SP member. The SP member formulates the received request to a transaction. Then, the SP member broadcasts this transaction to the federation of members, those members later act as the distributed policy decision point (PDP), and they accept or reject the transaction. The PDP evaluates the request and then executes a smart contract which is already deployed in the trust chain. The execution of the smart contract leads to decide whether the request should be permitted or denied. Finally, SP members will allow or deny the request based on the executed result. When updating the trust value of a user, a new block is created and added at the end of the trust chain by the corresponding SP member.

An example of the trust chain is shown in Fig. 3.

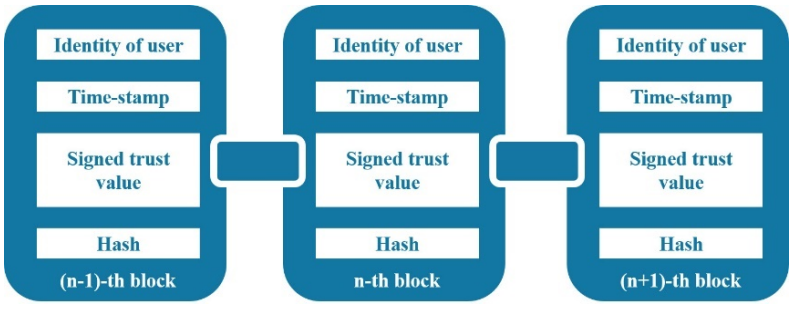

Figure 3: The blocks of the trust chain

The trust chain is made up of concatenation of blocks.

The n-th block is composed of four parts.

1. **Identity of the user:** It indicates the user whose trust value will be modified.
2. **T:** It is the timestamp when the block is added.
3. **Signed trust value:** The SP member calculates the trust value and makes a signature for proving the validity.
4. **Hash value:** It is a classic part of the blockchain, which ensures the block unforgeable.

Our scheme focusses on the third part of the block. Our scheme can ensure that the user's trust value will only be adjusted by the SP member of this federation, and avoid malicious modification. Only SPs of the federation, which have the specific key, can add a new block to the trust chain, and verify that the signer is indeed the member in the federation. In our proposed method, identity-based ring signatures are used instead of ordinary signatures, which can provide users with anonymity, so that the sources of changes in trust values will not be exposed.

Finally, due to the use of a blockchain-like structure and smart contract, the trust management system achieves a decentralized structure, which further improves the security of trust value management. Based on the proxy ring signature method, the proxy staff of SP members can generate the signature for the modified trust values, which will increase the efficiency of trust management.

4 Preliminaries

4.1 Strong RSA assumption

Let N be a k-bit RSA modulus, namely $N = pq$, where p and q are strong primes.

Given an element $x \in Z_n$, it happens with probability $neg(k)$ for a computationally bounded adversary A to find $y > 1$ and such that $a^y = x \bmod N$.

4.2 Forking lemma for ring signature schemes

Herranz et al. [Herranz and Sáez (2003)] introduce the forking lemmas to the ring signature. The processes of the forking lemmas are as follows.

Let k be the security parameter, H be a hash function that outputs k-bit long elements. Given a ring U of n members $(U = \{ID_1, \cdots, ID_n\})$ and a message M, a generic ring signature scheme produces a tuple $\Theta = (U, M, R_1, \cdots, R_n, h_1, \cdots, h_n, \sigma)$. The values of $R_1, \cdots, R_n$ are randomly chosen in such a way that R_i s are distinct and no R_i can emerge with probability greater than $\frac{2}{2^k}$. Signer computes $h_i = H(U, M, ID_i, R_i)$. The value σ is fully determined by $R_1, \cdots, R_n$, $h_1, \cdots, h_n$ and the message M.

Theorem 1 (The Ring Forking Lemma) Let a generic ring signature scheme using the security parameter k. The member number of the corresponding ring is n. Consider A being a probabilistic polynomial-time Turing machine which takes as public data that can

ask for at most Q queries to the random oracle, with $Q \geq n$.

Assume that A produces a valid ring signature $\Theta = (U, M, R_1, \cdots, R_n, h_1, \cdots, h_n, \sigma)$. For some ring $U \subset U^*$ of n users within time-bound T and with a non-negligible probability of success $\varepsilon \geq \frac{C_n^Q}{2^k}$. For integers Q and n such that $Q \geq n \geq 1$, we denote C_n^Q as the number of n-permutations of Q elements, that is, $C_n^Q = Q(Q-1)\cdots(Q-n+1)$. By replaying the Turing machine, we can get two valid ring signatures $(U, M, R_1, \cdots, R_n, h_1, \cdots, h_n, \sigma)$ and $(U, M, R_1, \cdots, R_n, h_1', \cdots, h_n', \sigma')$ such that $h_j \neq h_j'$, for some $j \in \{1, \cdots, n\}$ and $h_i = h_i'$ for all $i \neq j$ and $i \in \{1, \cdots, n\}$ in time $T' \leq 2T$ and with probability $\varepsilon' \geq \frac{\varepsilon^2}{66 C_n^Q}$.

In our ring scheme, the hash function such that h_i is the hash value of (U, M, ID_i, R_i) is called H_2.

5 Our scheme

Our signature scheme implements an identity-based proxy ring signature from RSA. Staffs of SPs act as proxies to sign the block (including the changed trust value). The signature can be validated by other SPs.

Tab. 1 describes the symbolic parameters used in the scheme process.

Table 1: Parameter table

Notation	Description
SP	Server provider
ID_i	Identity of i-th SP member
BID	The block name
t	The valid timestamp
U	The set of identities
SK_i	The secret key of i-th SP member
φ	The delegation

Our scheme comprises six phases: System Setup, Key Generation, Proxy Setup, Delegation Generation, Proxy Ring Sign, and Verify algorithms as described below.

1. **System Setup:** Let k be the security parameter. Let positive integer N be the product of two k-bit, distinct odd primes (p and q). Chosen a fixed value l, let e be a randomly chosen positive integer, that $2^l < e < 2^{l+1}$, less than and relatively prime

to $\varphi(N)=(p-1)(q-1)$. Compute $d=e^{-1}mod(\varphi(N))$, define a cryptographic hash function $H_1:\{0,1\}^*\to Z_N^*$ and $H_2:\{0,1\}^*\to\{0,1\}^l$.

Then, we got our system parameters: $\{k,l,N,e,H_1,H_2\}$ and the system secret key: $\{p,g,d\}$.

2. **Key Generation:** In this step, we choose the secret/public pair of keys $(SK_i,H_1(ID_i))$ which is $SK_i=(H_1(ID_i))^d$ for the SP member with ID_i.

3. **Proxy Setup:** Let $U=\{ID_1,\cdots,ID_n\}$ be the set of all identities of *n* SP members. The practice staff of the corresponding SP member carries out the following steps to give an ID-based signature on behalf of the ring U. ID_p is the identity of the practice staff. Choose random numbers $A_i\in Z_N^*$ for $i\in\{1,\cdots,n\}$, where $i\neq p$, and compute $R_i=A_i^e mod\ N$. For a block of trust chain which is named *BID* and the valid timestamp t, compute $h_i=H_2(U,t,BID,ID_i,R_i)$. Choose $A_p\in Z_N^*$ for the SP member with ID_p and compute $R_p=A_p{}^e\cdot BID^{-H_1(t,BID)}\cdot\prod_{i\neq p}H_1(ID_i)^{-h_i}$. If $R_p\equiv 1 \bmod N$ or $R_p=R_i(i\neq p)$ back to choose a new $A_p\in Z_N^*$.

4. **Delegation Generation:** The practice staff sends $\tau=(h_p,U,t,BID,R_p)$ to the SP member, to require for the delegation. The SP member checks if $h_p=H_2(U,t,BID,ID_p,R_p)$, otherwise, it stops. Then, he computes the delegation $\varphi=SK_p{}^{h_p}$ and sends it to the practice staff.

5. **Proxy Ring Sign:** The practice staff computes $\sigma=\varphi\cdot A_p\cdot\prod_{i\neq p}A_i \bmod N$.

   The signature on *BID* and the valid timestamp *t* for the ring $U=\{ID_1,\cdots,ID_n\}$ is $\Theta=(U,t,BID,R_1,\cdots,R_n,\sigma)$. Then, the staff or the SP member can now write the signed trust value into the block and add the block to the trust chain and broadcast it to other SP members of the identity federation.

6. **Verify:** When SP members received the new block of the trust chain, they need to check the validity of a signature $\Theta=(U,t,BID,R_1,\cdots,R_n,\sigma)$ and a ring of identities U as follows:

   Compute $h_i=H_2(U,BID,ID_i,R_i)$ for $\forall i\in\{1,\cdots,n\}$;

   Accept the signature if $\sigma^e=BID^{H_1(t,BID)}\cdot\prod_{1\le i\le n}R_i\cdot H_1(ID_i)^{h_i} \bmod N$, and add the block into the trust chain of their service, and update the trust value of the corresponding user. Otherwise, reject the signature.

6 Analysis of the scheme

In this section, we will prove the security of our scheme. The first is correctness, which indicates our scheme can produce a valid signature. Then anonymity, which indicates the signature cannot reveal the identity of the actual signer. The actual signer must be one of the SP members, but the probability of each member to be the actual signer is equal. The last is unforgeability, which indicates only SP members or someone who has the delegation of SP members can produce a valid signature.

6.1 Correctness

Every SP member of the identity federation has received the new block with the signature after the block has been correctly generated.

First, they can compute $h_i = H_2\left(U, BID, ID_i, R_i\right)$ for $\forall i \in \{1, \cdots, n\}$;

Then, they have

$$\sigma^e = \left(SK_p{}^{h_p} \cdot A_p \cdot \prod_{i \neq p} A_i \right)^e \ mod\ N \tag{1}$$

$$\sigma^e = \left(SK_p{}^{h_p \cdot e} \cdot A_p{}^e \cdot \prod_{i \neq p} A_i^e \right) mod\ N \tag{2}$$

$$\sigma^e = BID^{H_1(t, BID)} \cdot \prod_{1 \le i \le n} R_i \cdot H_1\left(ID_i\right)^{h_i}\ mod\ N \tag{3}$$

Finally, the correctness of the proposed scheme is proved.

6.2 Anonymity

We can see that only SP members of the federation can produce a valid signature. The actual signer must be one of those SP members. Due to the scheme is completely symmetrical, the probability of each member being the actual signer is equal. Even if all private keys of SP members were leaked, no one could able to find the actual signer. Therefore, the scheme can realize unconditional anonymity for the SP members.

6.3 Unforgeability

We assume that P is an SP member or a staff of SP members. If someone wants to forge a signature of P, the most direct method is to get the private key of P from the data owner. However, that is impracticable.

In the case of the verified message of P ($\sigma^e = \prod_{1 \le i \le n} \left(R_i \cdot H_1\left(ID_i\right)^{h_i} \right) \bmod N$), the message is clearly identifiable and configurable, but it is difficult to obtain the e-th root of the constructed value.

In addition, we assume F is a non-deterministic polynomial-time Turing machine, who gives public data as input. Modeling the hash function as a random oracle, and F can make Q queries to the random oracle.

The forking lemma of the ring signature shows that if A can forge a legal signature in a non-negligible probability within the polynomial time TA, then B can forge two legal signatures. B has got $\Theta_1 = (U, BID, t, R_1, \cdots, R_n, \sigma)$ and $\Theta_2 = (U, BID, t, R_1, \cdots, R_n, \sigma')$ in a non-negligible probability $\varepsilon_b \geq \frac{{\varepsilon_a}^2}{65Q(Q-1)\cdots(Q-n+1)}$ within the polynomial time $2TA$.

B can obtain that

$$\sigma^e = BID^{H_1(t,BID)} \cdot \prod_{1 \leq i \leq n} R_i \cdot H_1(ID_i)^{h_i} \ mod\ N \tag{4}$$

$$(\sigma')^e = BID^{H_1(t,BID)} \cdot \prod_{1 \leq i \leq n} R_i \cdot H_1(ID_i)^{h_i'} \ mod\ N \tag{5}$$

Since h_i' is randomly picked, it can be $h_i = h_i'$ of all $i \neq j$, which is obtained by dividing the two equations, the function will be $\left(\frac{\sigma}{\sigma'}\right)^e = \left(H_1(ID_j)^{h_j - h_j'}\right) \bmod N$.

Since σ' is forged after making h_j', $\omega^e = u \bmod N$ can be found, where $\omega = \left(\frac{\sigma}{\sigma'}\right) mod\ N$ and $u = \left(H_1(ID_j)^{h_j - h_j'}\right) mod\ N$. Thus, he successfully solves the RSA problem. Therefore, the proposed ring signature scheme is unforgeable.

7 Comparison

Table 2: Comparison between our proposed and previously proven secure schemes

Scheme	PSIPRS	SIPRS	Ours
Proxy Setup Cost	0	0	$(2n-1)$exp
Delegation Generation Cost	2exp	2exp	exp
Delegation Verify Cost	2exp	2exp	0
Proxy Ring Sign Cost	$(2n+1)$exp	$(n+2)$exp	0
Total Consumption	$(2n+5)$exp	$(n+6)$exp	$(2n)$exp
Verify Cost	$(n+2)$exp	$(2n+1)$exp	$(n+1)$exp
Signature Size	$(n+2)Z_N^*$	$(n+1)Z_N^* + l_1$	$(n+1)Z_N^* + n + S_{BID}$

Tab. 2 summarizes the comparison of the proposed scheme with other similar identity-based proxy ring signature schemes. All three schemes are based on RSA and are provably secure [Asaar, Salmasizadeh and Susilo (2015a); Asaar, Salmasizadeh and

Susilo (2015b)]. We compare the computational costs of proxy setup, delegation generation, proxy ring sign, and verify. The exp denotes exponentiation in Z_N^* in Tab. 2. For the sake of comparison, it is assumed that other operations take zero time and the numbers of ring members are set to n. Since l_1 represents the size of the hash function in the SIPRS scheme, $l_1 \ll Z_N^*$ (for example, l_1 is about 160 bits, while $Z_N^* = 1024$) [Asaar, Salmasizadeh and Susilo (2015a)]. S_{BID} refers to the size of the BID in our scheme. In general, S_{BID} is much smaller than l_1.

Regarding the total time cost of producing a ring signature, if the number of members in the ring is less than 6, our solution will consume the least time. But if there are more than 6 ring members, SIPRS only needs almost half the computational complexity of PSIPRS or our scheme.

In our scheme, the main time-consuming part of the signature work is conducted by the staff. Only one step, Delegation Generation, requires the participation of the SP members. At this step, our scheme is the least time-consuming one among the three schemes. In addition, in terms of signature verification, our scheme has the lowest time complexity. This is very important for reducing overall time consumption of the trust management system, since each SP member of the federation needs to verify the signature, which means that this step will be replayed $(n-1)$ times.

In terms of the size of the signature of three schemes, there is no significant difference among the three schemes.

8 Conclusion

In this work, we propose a trust value sharing scheme based on a proxy ring signature. The aim is to provide an efficient trust value sharing method for better privacy-preserving in heterogeneous identity federation topologies. The unconditional anonymity, which is provided by the identity-based ring signature algorithm, prevents the source signer from being exposed, thereby protecting users' privacy. We also prove that our scheme is verifiable, signer anonymous, unforgeable, and effective.

Funding Statement: This work is supported by the National Key Research and Development Project of China (No. 2017YFB0802302), the Key Research and Development Project of Sichuan Province (Nos. 20ZDYF2324, 2019ZYD027, 2018TJPT0012), the Science and Technology Support Project of Sichuan Province (Nos. 2018GZ0204, 2016FZ0112), and the Science and Technology Project of Chengdu (No. 2017-RK00-00103-ZF).

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

Ajmath, K. A.; Reddy, P. V.; Rao, B. U.; Varma, S. V. K. (2012): Identity-based directed proxy ring signature scheme. *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 15, no. 2-3, pp. 181-192.

Asaar, M. R.; Salmasizadeh, M.; Susilo, W. (2015a): A provably secure identity-based proxy ring signature based on RSA: A provably secure ID-based PRS based on RSA. *Security and Communication Networks*, vol. 8, no. 7, pp. 1223-1236.

Asaar, M. R.; Salmasizadeh, M.; Susilo, W. (2015b): A short identity-based proxy ring signature scheme from RSA. *Computer Standards & Interfaces*, vol. 38, pp. 144-151.

Awasthi, A. K.; Lal, S. (2007): ID-based ring signature and proxy ring signature schemes from bilinear pairings. *International Journal of Network Security*, pp. 187-192.

Boyen, X.; Haines, T. (2018): Forward-secure linkable ring signatures from Bilinear maps. *Cryptography*, vol. 2, no. 4, pp. 35.

Dong, G.; Chen, Y.; Li, H. (2019): Cross-domain authentication credibility based on blockchain in heterogeneous environment. *Communications Technology*, vol. 52, no. 6, pp. 1450-1460.

Gu, K.; Jia, W.; Zhang, J. (2017): Identity-based multi-proxy signature scheme in the standard model. *Fundamenta Informaticae*, vol. 150, no. 2, pp. 179-210.

Herranz, J.; Sáez, G. (2003): Forking lemmas in the ring signatures scenario. *Proceedings of Indocrypt'03, Springer LNCS*, vol. 2904, pp. 266-279.

Li, X.; Mei, Y.; Gong, J.; Xiang, F.; Sun, Z. (2020): A blockchain privacy protection scheme based on ring signature. *IEEE Access*, vol. 8, pp. 76765-76772.

Lutz, D. J.; Stiller, B. (2013): A survey of payment approaches for identity federations in focus of the SAML technology. *IEEE Communications Surveys Tutorials*, vol. 15, no. 4, pp. 1979-1999.

Perez-Mendez, A.; Pereniguez-Garcia, F.; Marin-Lopez, R.; Lopez-Millan, G.; Howlett, J. (2014): Identity federations beyond the web: a survey. *IEEE Communications Surveys & Tutorials*, vol. 16, no. 4, pp. 2125-2141.

Rivest, R. L.; Shamir, A.; Tauman, Y. (2001): How to leak a secret. *Lecture Notes in Computer Science*. *ASIACRYPT*, pp. 552-565.

Sanchez, R.; Almenares, F.; Arias, P.; Diaz-Sanchez, D.; Marin, A. (2012): Enhancing privacy and dynamic federation in IdM for consumer cloud computing. *IEEE Transactions on Consumer Electronics*, vol. 58, no. 1, pp. 95-103.

Sarde, P.; Banerjee, A. (2017): A secure ID-based blind and proxy blind signature scheme from bilinear pairings. *Journal of Applied Security Research*, vol. 12, no. 2, pp. 276-286.

Wu, L.; Li, D. (2009): An efficient ID-based proxy ring signature scheme. *WRI International Conference on Communications and Mobile Computing*, pp. 560-563.

Xiong, L.; Shi, Y. (2018): On the privacy-preserving outsourcing scheme of reversible data hiding over encrypted image data in cloud computing. *Computers, Materials & Continua*, vol. 55, no. 3, pp. 523-539.

Yang, C.; Li, J.; Li, H.; Hao, Y.; Dong, G. (2019): A research on heterogeneous identity alliance unified identity model. *Information Security and Communication Confidentiality*, no. 6, pp. 27-35.

Zhang, F.; Kim, K. (2002): ID-based blind signature and ring signature from pairings. *Lecture Notes in Computer Science*, pp. 533-547.