applied sciences

MDPI

Article

DCAGS-IoT: Dynamic Cross-Domain Authentication Scheme Using Group Signature in IoT

Weihan Yuan [1], Xiaoya Li [1,2], Mingyue Li [1,2,*] and Liudong Zheng [1,2]

[1] School of Cyberspace Security and Computer Science, Hebei University, Baoding 071002, China
[2] Hebei Key Laboratory of Highly Trusted Information System, Hebei University, Baoding 071002, China
* Correspondence: limingyue@hbu.ecu.cn

Abstract: Cross-domain authentication requires that there is no trust gap between different trust domains that can cause cross-domain devices to exceed the security control scope of the original trust domain and further expose cross-domain authentication systems to security threats. In addition, as relying on the traditional cross-domain authentication means built by centralized institutions cannot meet the data security needs in a big data environment. Therefore, it is necessary to design a secure dynamic cross-domain authentication scheme. In this paper, we propose a dynamic cross-domain authentication scheme (DCAGS-IoT) in the Internet of Things environment using the group signature technology and the distributed system architecture of blockchain. Specifically aiming at the problem of increasing and revoking users in dynamic cross-domain authentication, a user update algorithm with the complexity of O (log$N$) was designed to manage users in the trust domain. Moreover, we used the characteristics that group signature users can sign on behalf of a group to protect the users' privacy and track suspicious users. Since the size of the signature generated by the scheme is independent of the number of group members N and only depends on the security parameters λ, the efficiency of the protocol implementation is improved, and the security and availability of the authentication scheme are guaranteed.

Keywords: Internet of Things; privacy protection; dynamic cross-domain authentication; group signature; blockchain

Citation: Yuan, W.; Li, X.; Li, M.; Zheng, L. DCAGS-IoT: Dynamic Cross-Domain Authentication Scheme Using Group Signature in IoT. *Appl. Sci.* **2023**, *13*, 5847. https://doi.org/10.3390/app13105847

Academic Editor: Fabrizio Granelli

Received: 24 March 2023
Revised: 13 April 2023
Accepted: 17 April 2023
Published: 9 May 2023

1. Introduction

To meet the application needs such as smart medical care, Internet of Vehicles (IoV) [1], smart home, industrial production, energy and power, Internet of Things (IoT) focuses on achieving communication between people, between people and things, and between things, providing Internet users with a more immersive application experience [2]. However, in recent years, as a large number of devices are continuously connected to the IoT, security problems in the IoT environment have emerged in an endless stream. Malicious attackers may use the insecure cross-domain authentication of devices, making network security problems more serious. Therefore, it is particularly important to design a secure and effective dynamic cross-domain authentication scheme in the IoT environment to protect the privacy of users.

Cross-domain authentication [3] refers to the process of user or device identity authentication between multiple trust domains. This process not only needs to establish the credibility of the relationship between each trust domain, maintain the efficiency of the authentication process and ensure the reliability of the authentication system, but also needs to ensure the security authentication and real-time management of legal devices between each trust domain. In the real-time scenario of distributed systems, we can divide cross-domain authentication into two types: static cross-domain authentication and dynamic cross-domain authentication. Static cross-domain authentication refers to the authentication performed by user to access an information service entity in the target trust domain without

leaving the trust domain to which it belongs. For example, the cross-domain authentication scenario in which devices in different factories are cooperatively produced in the Industrial IoT. The dynamic cross-domain authentication is the authentication performed by the user who moves to the target trust domain to access the information service entity. For example, in the Internet of Vehicles environment, in order to have a better travel experience, vehicles need to constantly interact with roadside units. At present, many schemes only consider static cross-domain authentication without discussing dynamic cross-domain authentication.

Motivations and benefits. Traditional cross-domain authentication frameworks rely on centralized servers [4] such as using Public Key Infrastructure (PKI) and Identity-Based Cryptograph (IBC) to design the authentication architecture. However, the centralized authentication architecture is prone to single point of failure issues and is vulnerable to denial-of-service attacks. The emergence of blockchain has promoted the development of identity authentication, thus the authentication architecture is not limited to a centralized architecture, but its openness and transparency exposes user privacy to the public. To solve some problems existing in the existing cross-domain authentication schemes in the IoT environment, this paper proposed a dynamic cross-domain authentication scheme based on the group signature technology, combined with the distributed peer-to-peer network architecture of blockchain technology. Since the size of the signature generated by the scheme is independent of the number of group members and only depends on the security parameters, the efficiency of protocol implementation is improved, and the security and availability of the authentication scheme are guaranteed.

The main contributions of this paper are as follows:

(1) Aiming at the difficulty of user joining and revocation in the dynamic cross-domain authentication environment, an effective update algorithm with complexity O(log$N$) is provided in the static Merkle tree accumulator to realize the dynamic addition and revocation of users.
(2) We used group signature technology to allow members of a group to sign messages on behalf of the entire group, thus protecting user privacy from being leaked. Moreover, users are responsible for the issued signatures as tracking agencies can be used to identify them.
(3) Blockchain distributed ledger storage is used to realize cross-domain authentication between trust domains. The analysis proves that the protocol is secure in the random oracle model, and the size of the signature generated by the scheme is independent of the number of group members N, and only depends on the security parameter λ, which effectively improves the operating efficiency of the protocol.

Organization Structure

This paper introduces the related works on cross-domain authentication in the Section 2, introduces the proposed dynamic cross-domain authentication scheme in Section 3, and presents the analysis of the proposed protocol in Section 4. The conclusions are given in Section 5.

2. Related Work

A cross-domain authentication protocol in the IoT environment has been proposed by researchers for a long time. However, most of the traditional schemes are PKI-based and IBC-based. Zhou et al. [5] proposed combining threshold secret sharing and identity-based encryption to construct a certificate authority domain that minimizes the length of the verification path and improves the authentication efficiency. Aiming at the large computational cost of the bilinear pairing operation in the elliptic curve and the certificate management in the PKI, Wang et al. [6] designed a efficient and secure authenticated key agreement protocol based on the identity-based public key cryptography algorithm and the GDH difficulty problem on the elliptic curve addition group. Ning et al. [7]

also proposed a new bilinear-free, IBC-based two-party cross-domain authenticated key agreement protocol.

Devices have higher requirements for the versatility of cross-domain authentication systems between different cryptosystems. Zhang et al. [8] proposed a complete cross-domain authentication scheme that could be used by participants in different domains with completely different settings, and the underlying design of the scheme was based on blockchain technology. Jiang et al. [9] proposed a cross-domain identity authentication scheme based on PKI and certificateless cryptography (CLC) to achieve mutual identity authentication and secure access between users of the two public key cryptosystems. Lin et al. [10] proposed a secure and effective fog computing key negotiation and user authentication scheme that could establish secure sessions between different entities, and users could achieve cross-domain access to other fog servers. Jiang et al. [11] proposed a proxy-blind signature-based approach for cross-domain identity authentication schemes based on public key infrastructures of different systems and certificateless public key cryptosystems that could not satisfy identity blindness and efficient heterogeneous cross-domain authentication. Wei et al. [12] combined blockchain technology with an identity-based cryptographic system to provide a cross-domain authentication scheme that solves the problem of devices in trust domains with different authentication mechanisms when cooperating with each other. These centralized cross-domain authentication protocols usually require a lot of computing or communication resources and have problems such as relying on trusted third parties to issue certificates and key escrow.

The core advantage of blockchain decentralization has promoted the development of the field of identity authentication. Therefore, in order to solve the above problems, there are many solutions that use blockchain technology to improve them. Bagga et al. [13] designed a new blockchain-based batch authentication scheme in IoV-based smart city deployments that enabled vehicle-to-vehicle (V2V) authentication and allowed a group of clustered vehicles to authenticate through it. Singh et al. [14] proposed a blockchain-based decentralized trust management system where the RSUs at the edge cooperatively maintain updated, reliable, and consistent vehicle trust values to reduce the workload from the master-maintained blockchain.

However, due to the fact that wireless communication channels may be destroyed and taken over by malicious adversaries, and the open and transparent characteristics of blockchain, data in transit may be eavesdropped, modified, and replayed. Protecting user privacy and secure authentication are important prerequisites for ensuring secure communication as well as an important requirement for dynamic cross-domain authentication. Li et al. [15] proposed a certificate-free CPPA protocol to support privacy and security requirements in IoV systems where the vehicle and trusted authority (TA) do not need to store any certificates separately for verification and tracking. Zhang et al. [16] uploaded the hash value calculated by the certificate of the mobile device to the blockchain. During identity authentication, it is only necessary to verify whether the hash value of the certificate provided by the device is the same as the stored hash, avoiding the tedious verification process of the authentication mechanism. Li et al. [17] designed a secure cross-domain authentication and key agreement protocol for heterogeneous wireless networks with different security parameters based on blockchain. Dong et al. [18] designed a user identity credibility initialization method by using the entropy-based probability weighted subjective trust and risk evaluation method for the user's identity credibility problem in heterogeneous domain cross-domain authentication. The trustworthiness of various users in heterogeneous domains was calculated and described. Ghane et al. [19] proposed a differentially private data flow system to address privacy issues in distributed edge computing. Yang et al. [20] proposed a cross-domain identity authentication scheme for cloud service providers in different trust domains based on the group signature scheme, and used the Chinese remainder theorem to solve the problem where the traditional identity authentication model cannot be applied to cloud computing, which simplified the calculation process. Ali et al. [21] analyzed and identified some serious security flaws in the SAKA-FC

authentication key exchange scheme and made improvements. Shehzad et al. [22] proposed a secure message authentication protocol for information exchange between IoV entities based on secure symmetric lightweight hash functions and cryptographic operations.

At the same time, most cross-domain authentication schemes only consider the situation that the device accesses other trust domains in the trust domain to which it belongs, and does not discuss the scenario where the device moves to other trust domains for resource access. In addition, many solutions do not involve the addition and deletion of users, and the efficiency of the solution will also decrease as the number of users increases, affecting the user experience. Luo et al. [23] proposed a cross-domain certificateless authentication GKA protocol for 5G network slicings that supports dynamic group user management. This scheme requires only one round of communication and allows group users from different network domains with different cryptosystem parameters to jointly negotiate the group session key. Tan et al. [24] utilized homomorphic encryption to solve the VANET cross-domain authentication problem under the new RSU edge network assumption to dynamically update anonymous vehicle identities. Xu et al. [25] designed a blockchain-based authentication and key agreement protocol for the multi-TA network model, which shifted the computational load of the TA down to the RSU to improve the authentication efficiency. Zhang et al. [26] proposed a two-way anonymous traceability group authentication protocol in IoV, where the RSU in the group can anonymously trace the identity of malicious vehicles. The scheme uses the blockchain to quickly revoke their identity, and can also freely change the ID of users who reveal their true identities. Ahmed et al. [27] allowed IoV nodes in a certificateless encryption (CLC) environment to send messages to servers in a public key infrastructure (PKI) environment to secure the communication between the server and the IOV. Since there is no paired computation, the protocol has an efficient advantage over existing protocols. Trivedi et al. [28] proposed a new authentication scheme to jointly achieve effective authentication and partial trust management through scalability in a distributed IoT environment, but this scheme only considers user additions within a single trust domain.

3. Proposed Dynamic Cross-Domain Authentication Scheme

In this section, we first describe the system model, and then introduce our update algorithm, which was designed to implement user join and revoke in a dynamic cross domain authentication environment. Finally, we describe the proposed scheme in detail, which mainly includes three stages: system initialization, registration, and cross domain authentication.

3.1. System Model

The cross-domain authentication scenario mainly includes the group manager (GM), tracking manager (TM), a group of member users, and the blockchain. The specific cross-domain authentication system model is shown in Figure 1. The GM is responsible for the management of group members, establishing group resources, and generating the corresponding group public key gpk, which is open to all users in the entire system, and maintains a registration list and revocation list. It stores the identities of registered and revoked group members. Group members are all legal users in a distributed system. The blockchain exists in the system as a storage medium to ensure that the data will not be tampered with. GM acts as a full node in the system. As long as no more than half of the GM in the world is destroyed, the security of the blockchain can be guaranteed. The tracking administrator (TM) can open the signatures of group members, regulate the illegal behavior of users, acts the supervision department in the group, supervise the behavior of members in the group, and complete the behavior responsibility identification and responsibility judgment when the group members are found to have illegal behaviors.

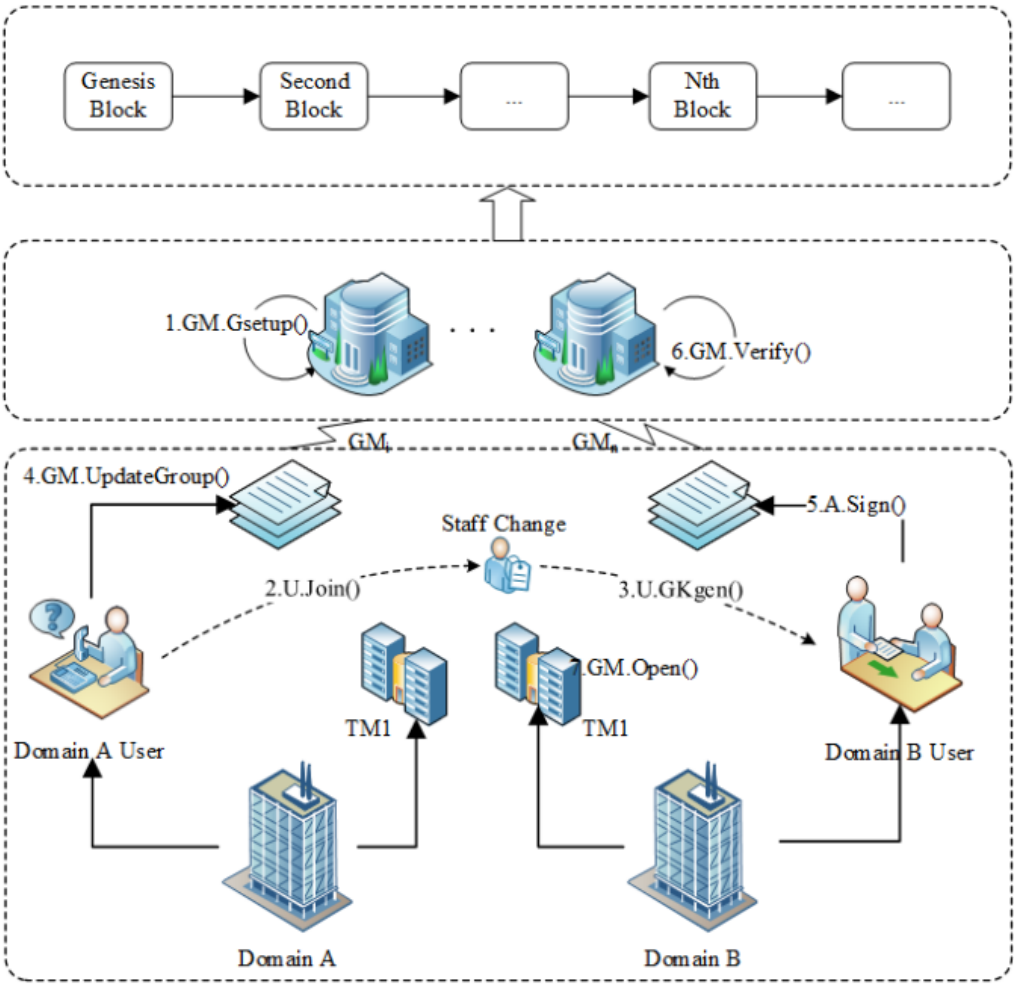

Figure 1. The system model.

3.2. User Update Algorithm

We used a simple and effective update algorithm to implement the dynamic addition and removal of users. The main idea is to make each leaf node represent a user, where the current value of the leaf node is the binary string of the public key held by the user. When the user state changes, it only needs to modify all the values in the path from the leaf to the root, without changing the entire Merkel tree. As shown in Figure 2, we provide an example of a tree with $2^3 = 8$ leaf nodes. When the status of the user u_{101} changes, we only need to change the values of the yellow nodes. It can be seen that the time complexity of the proposed algorithm is O(log$N$).

3.3. Our Scheme

In this paper, the idea of a dynamic group signature was introduced into the cross-domain authentication scheme, and an on-lattice dynamic cross-domain authentication scheme with join and revocation mechanism was proposed. For the scheme parameters, this paper selected them according to the literature [29]. In this section, we describe the proposed scheme in detail. It consists of three phases: the initialization phase, registration phase, and cross-authentication phase. When the system starts up, the GM performs the initialization phase. Before users can enter the system, they must be registered in the GM through the registration phase. Table 1 describes the symbols used in the solution, and the protocol flow is shown in Figure 3. The details of the above three stages are as follows:

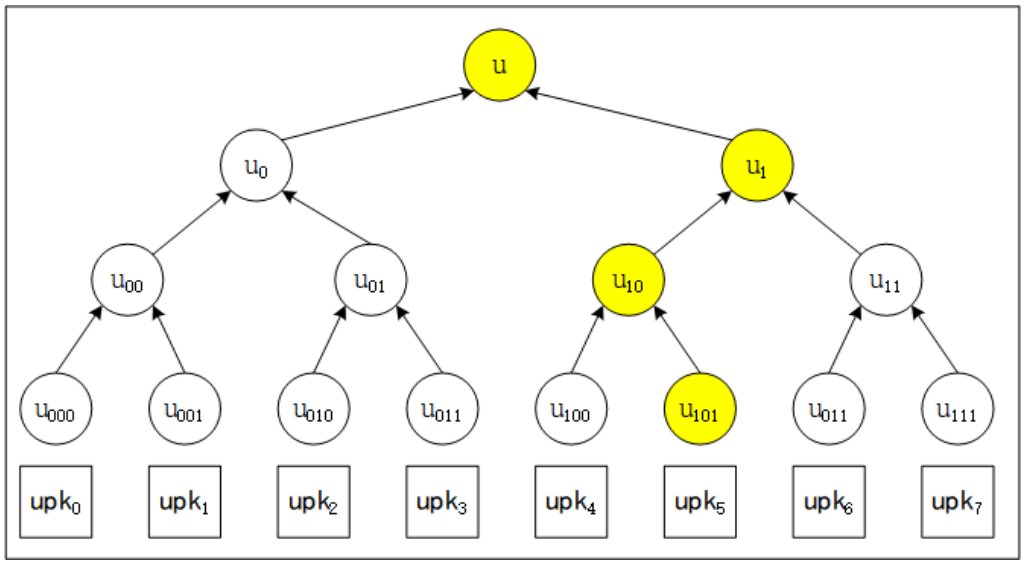

Figure 2. The user update algorithm.

Table 1. Description of the symbols.

Symbol	Meaning
GM	Group manager
TM	Track manager
U	User
gpk	Group public key
gsk	Group signing key
pp	Public parameter
λ	Safety parameters
Reg	Registration list
ik	Issue key
ok	Open key
upk	Public key
usk	Private key

3.3.1. System Initialization

System setup: Randomly select security parameters, GM runs the algorithm to generate public parameters, group public key, signature key, and tracking key, initialize internal State L and Registry Reg. Then, the public key gpk of the group is published to the blockchain, and anyone can find the public key of the group from the blockchain, and send ok to the tracking administrator TM, which will be used to regulate the daily behavior of users in the future.

The specific process is as follows:

1. Select $n = \mathcal{O}(\lambda)$, and n is a power of 2. The modulus $q = \widetilde{\mathcal{O}}(n^4)$, $R = \mathbb{Z}[X]/(X^n + 1)$, $R_q = R/qR$, where q = 3k, k is a positive integer). Then, set $\ell = \log\left\lfloor \frac{q-1}{2} \right\rfloor + 1$, $m \geq 2\lceil \log q \rceil$, $\overline{m} = m + k$.
2. Choose an integer $d \geq \log_c(\omega(\log n))$ and a strictly increasing sequence of integers, $\{c_0, c_1, \ldots, c_d\}$, where $c_0 = 0$, $c_i = \lfloor \alpha_0 c^i \rfloor$, $i \in [d]$.
3. Choose an integer $\beta = \widetilde{\mathcal{O}}(n)$, $B = \widetilde{\mathcal{O}}\left(n^{5/4}\right)$, χ for the bounded distribution of B on R.
4. $\mathcal{H}_{FS} : \{0,1\}^* \to \{1,2,3\}^{\mathcal{K}}$, where $\mathcal{K} = \omega(\log \lambda)$ is an anti-collision hash function.
5. COM is a statistical hidden and computationally bound commitment scheme.
6. Uniform random matrix $B \in R_q^{1 \times m}$.

7. Generate a verification key A, $F_0 \in R_q^{1\times \tilde{m}}$; $A_{[0]}, \ldots, A_{[d]} \in R_q^{1\times k}$; $F, F_1 \in R_q^{1\times \ell}$; $u \in R_q$, a signature key $R \in R_q^{m\times k}$.
8. Set $s_1, s_2 \leftarrow \chi$, $e_1, e_2 \leftarrow \chi^{\ell}$, $a \xleftarrow{\$} R_q^{\ell}$.
9. Calculate $b_1 = a{\cdot}s_1 + e_1 \in R_q^{\ell}$; $b_2 = a{\cdot}s_2 + e_2 \in R_q^{\ell}$.

Then, the public parameters pp, group public key gpk, ik, and ok are as follows:

$$pp = \{n, q, k, R, R_q, \ell, m, \overline{m}, \chi, d, c_0, c_1, \ldots, c_d, B, \beta, \mathcal{K}, \mathcal{H}_{FS}, COM, B\}$$

$$gpk = \left\{pp, A, \left\{A_{[j]}\right\}_{j=0}^{d}, F, F_0, F_1, u, a, b_1, b_2\right\}$$

$$ik = R$$

$$ok = (s_1, e_1)$$

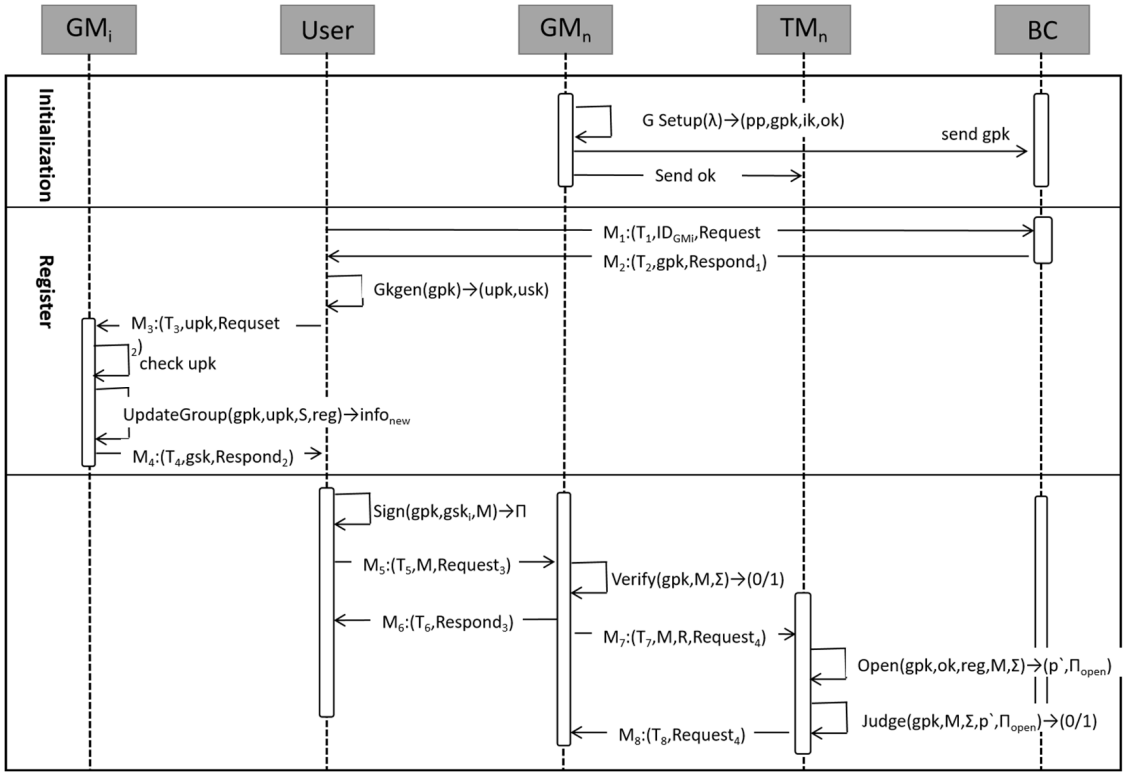

Figure 3. Scheme flowchart.

3.3.2. Registration Stage

When a new group member joins the trust domain, it first registers with the GM. The specific steps for the user are as follows:

1. $M_{1(U\to BC)} : (T_1, ID_{GM_i}, Request_1)$: Before sending the registration request to the user, the user requests the BC to query the gpk at the time T1, which is convenient for generating the user's own public and private key pair.
2. $M_{2(BC\to U)} : (T_2, gpk, Respond_1)$: The blockchain returns gpk to user U at T_2.
3. $GKgen_U(gpk) \to (upk, usk)$: After the user receives the group public key gpk of the domain and the $Respond_1$, enter the gpk, and perform the following operations: the user randomly selects $x \in R^m$ and calculates $p = B{\cdot}x \in R_q$. Then, the user's own key pair is $(upk = p, usk = x)$.

4. $M_{3(U\to GM_i)}$: $(T_3, upk, Request_2)$: After the key pair is generated, the user sends a join request at T_3 to GM_i.
5. $Join(gpk, upk, pp) \to gsk$: When a user with public key upk = p sends a request to join the trust domain, GM_i first checks whether the user with upk = p has been registered before, if not, register the user in the trust domain to which they belongs, and the user becomes a group member. Finally, output the user's group signature key gsk.
   (1) Set label $t = \left(t_0, t_1 \ldots, t_{c_d-1}\right)^\top \in \mathcal{T}_d$, calculate $A_t = [A \mid A_{[0]} + \sum_{i=1}^{d} t_{[i]} A_{[i]}] \in R_q^{1\times(\overline{m}+k)}$;
   (2) Using the signing key R, generate a signature (t, r, v), where $r \in R^{\overline{m}}$, $v \in R^{\overline{m}+k}$, and
   $$\begin{cases} A_t \cdot v = F \cdot rdec(F_0 \cdot r + F_1 \cdot rdec(p)) + u \\ \| r \|_\infty \leq \beta, \ \| v \|_\infty \leq \beta \end{cases}$$
   The GM_i then sets the user's group signing key to $gsk = (t, r, v, x)$, and forwards it to the user, records it, and then updates S to $S + 1$.
6. $UpdateGroup(gpk\,, upk, S, reg) \to (info_{new})$: If a new user joins or leaves, GM_i runs the algorithm to update the group information, the algorithm returns the new public group information and updates the GM's info.
7. $M_{4(GM_i\to U)}$: $(T_4, gsk, Respond_2)$: GM_i feedbacks the user's registration $Respond_2$ to the user, where 0 means failure, and 1 means success.

3.3.3. Cross-Domain Authentication

1. $Sign(gpk, gsk_i, M) \to \Pi$: When the local user U wants to access the services of other trust domains, the algorithm is first executed, and the output group signature Π is generated using the gsk_i, gpk, and message M of the given user. Specific steps are as follows:
   (1) For $i \in \{1, 2\}$, instantiate $g_i \hookleftarrow \chi, e_{i,1} \hookleftarrow \chi^\ell$ and $e_{i,2} \hookleftarrow \chi^\ell$;
   (2) Calculate
   $$\begin{aligned} c_i &= (c_{i,1}, c_{i,2}) \\ &= (a \cdot g_i + e_{i,1},\ b_i \cdot g_i + e_{i,2} + \lfloor q/4 \rfloor \cdot rdec(p)) \in R_q^\ell \times R_q^\ell, \end{aligned}$$
   (3) Calculate $\Pi_{gs} = (\{CMT_i\}_{i=1}^{\kappa}, CH, \{RSP_i\}_{i=1}^{\kappa})$, where
   $$CH = \mathcal{H}_{FS}(M, \{CMT_i\}_{i=1}^{\kappa}, \xi)$$
   $$\xi = \left(A, A_{[0]}, \ldots, A_{[d]}, F, F_0, F_1, u, B, a, b_1, b_2, c_1, c_2\right);$$
   (4) Output $\Pi = \left(\Pi_{gs}, c_1, c_2\right)$.
2. $M_{5(U\to GM_n)}$: $\left(T_5, M, Request_3\right)$: The user makes an authentication $Request_3$ at T_5.
3. $Verify(gpk, M, \Sigma) \to (1/0)$: The algorithm checks whether it is a valid group signature on M for the group information information, and outputs a bit: 1 means accept, 0 means reject. Specific steps are as follows:
   (1) Calculate $\Sigma = (\{CMT_i\}_{i=1}^{\kappa}, (Ch_1, \ldots, Ch_\kappa), \{RSP\}_{i=1}^{\kappa}, c_1, c_2)$;
   (2) IF $(Ch_1, \ldots, Ch_\kappa) \neq \mathcal{H}_{FS}(M, \{CMT_i\}_{i=1}^{\kappa}, \xi)$, Return 0;
   (3) For each $i \in [\kappa]$, run the verification phase of the protocol and return 0 if any of the conditions are not true, return 0;
   (4) Otherwise, return 1.
4. $M_{6(GM_n\to U)}$: $\left(T_6, Respond_3\right)$: Return the authentication result to the user at T_6.
5. $M_{7(GM_n\to TM_n)}$: $(T_7, M, Requset_4)$: If abnormal behavior is found, GM_n sends a request to verify M at T_7.

6. $\mathrm{Open}(\mathrm{gpk}, \mathrm{ok}, \mathrm{reg}, \mathrm{M}, \Sigma) \rightarrow (\mathrm{p}\prime, \Pi_{\mathrm{open}})$: After the tracking administrator receives the request, execute the Open algorithm, which takes the group public key gpk, ok, Reg, message M, and signature as input, and returns the proof of the user. If the algorithm cannot attribute the signature to a specific group member, it will return $(\perp,)$, indicating that the signature is the signature of an illegal user, and set the attribute. Specific steps are as follows:
   (1) Set $\mathrm{ok} = (\mathrm{s}_1, \mathrm{e}_1)$, $\Sigma = (\Pi_{\mathrm{gs}}, \mathrm{c}_1, \mathrm{c}_2)$;
   (2) Use s_1 to decrypt $\mathrm{c}_1 = (\mathrm{c}_{1,1}, \mathrm{c}_{1,2})$ according to the following steps;
      a. Calculate $\mathrm{p}'' = \frac{\mathrm{c}_{1,2} - \mathrm{c}_{1,1} \cdot \mathrm{s}_1}{\lfloor \mathrm{q}/4 \rfloor}$,
      b. For each coefficient of p'', Returns 0 if it is closer to 0 than -1 and 1; Returns -1 if it is closer to -1 than to 0 and 1; Returns 1 if it is closer to 1 than -1 and 0,
      c. p'' is the coefficient of $\mathrm{p}' \in \mathrm{R}_{\mathrm{q}}^{\ell}$,
      d. Set $\mathrm{p}' \in \mathrm{R}_{\mathrm{q}}$ and make $\tau(\mathrm{p}') = \mathrm{H} \cdot \tau(\mathrm{p}')$.
   (3) If Reg does not include p', return $(\perp, \perp)$.
   (4) Otherwise, generate Π_{open} for proving possession $(\mathrm{s}_1, \mathrm{e}_1, \mathrm{y}) \in \mathrm{R}_{\mathrm{q}} \times \mathrm{R}_{\mathrm{q}}^{\ell} \times \mathrm{R}_{\mathrm{q}}^{\ell}$.

$$\begin{cases} \|\mathrm{s}_1\|_\infty \leq \mathrm{B}; \|\mathrm{e}_1\|_\infty \leq \mathrm{B}; \| \mathrm{y} \|_\infty \leq \lceil \mathrm{q}/10 \rceil \\ \mathrm{a} \cdot \mathrm{s}_1 + \mathrm{e}_1 = \mathrm{b}_1 \\ \mathrm{c}_{1,2} - \mathrm{c}_{1,1} \cdot \mathrm{s}_1 = \mathrm{y} + \lfloor \mathrm{q}/4 \rfloor \cdot \mathrm{rdec}(\mathrm{p}') \end{cases} \quad (1)$$

   $\Pi_{\mathrm{Open}} = (\{\mathrm{CMT}_i\}_{i=1}^{\kappa}, \mathrm{CH}, \{\mathrm{RSP}\}_{i=1}^{\kappa})$, where $\mathrm{CH} = \mathcal{H}_{\mathrm{FS}}(\{\mathrm{CMT}_i\}_{i=1}^{\kappa}, \mathrm{a}, \mathrm{b}_1, \mathrm{M}, \Sigma, \mathrm{p}') \in \{1,2,3\}^{\kappa}$.
   (5) Output $(\mathrm{p}', \Pi_{\mathrm{Open}})$.
7. $\mathrm{Judge}(\mathrm{gpk}, \mathrm{M}, \Sigma, \mathrm{p}', \Pi_{\mathrm{Open}}) \rightarrow 1/0$: This algorithm is used by the TM to check the validity of the signature Π_{Open} . The output is 1 for valid and 0 for invalid.
8. $\mathrm{M}_{8(\mathrm{TM_n} \rightarrow \mathrm{GM_n})}$: $(\mathrm{T}_8, \mathrm{Respond}_4)$: After executing the algorithm, $\mathrm{TM_n}$ will feedback the result of whether it is a suspicious user at T_8.
9. Revoke: This algorithm is executed by the group administrator $\mathrm{GM_n}$. When the user actively or passively leaves the trusted domain, the user will be revoked from the registration list, and a new registration list will be updated and published. If the algorithm output is 1, the revocation is successful, otherwise the output is 0.

4. Analysis of Proposed Protocol

4.1. Security Attribute Analysis

(1) Anonymity

The scheme is based on the group signature scheme. Any group member in a trust domain can sign a message on behalf of the entire group in an anonymous manner, and the receiver does not know that the signature is signed by the group member in the group. Like other digital signatures, group signatures are publicly verifiable and can be verified using only a single group public key. Given a group signature, it is impossible for anyone other than the group administrator to know the identity of the actual signer.

(2) Resist replay attack

The validity of the interactive message is guaranteed by the timestamp. After the message receiver receives the interactive message, it first checks whether it is valid, and then performs subsequent operations. Since the timestamp cannot be tampered with, if the attacker reuses the intercepted message, the verification will fail due to the invalid timestamp, so replay attacks can be effectively prevented.

(3) Traceability

In the event of an argument, a group manager can open a signature to determine the identity of the actual signer, and the signer cannot prevent the opening of the signature, so it is traceable.

(4) Privacy protection

The scheme uses a group signature scheme to hide user identity information, and does not use their real identity when interacting with other devices, and the privacy of the participants will be protected in the subsequent process. In the process of data sharing, no entity will disclose the identity information of the participants. The verifier only knows the trust domain to which the message sender belongs instead of the original identity information. The group administrator can trace the disputed membership, but the blockchain keeps information consistent, so it can effectively protect privacy.

(5) Avoid single point of failure

The heterogeneous inter-domain scheme adopts a decentralized storage architecture. The blockchain structure composed of GM in each trust domain replaces the location of a trusted third party, ensures the consistency of information storage, builds inter-domain trust, and completes cross-domain authentication, thus effectively solving the single point of failure problem.

In addition, the dynamic cross-domain authentication scheme based on group signature proposed in this paper and other existing cross-domain authentication schemes can avoid single point of failure, efficiency, privacy protection, anonymity, traceability, and other aspects. Comparisons were made, as shown in Table 2. The authentication scheme based on the group signature proposed by Yang et al. [20] could effectively solve the security problem of user identity authentication in a heterogeneous cloud environment. Zhang et al. [26] proposed a two-way anonymous traceability group authentication protocol in IoV. The RSU in the group can anonymously trace the identity of malicious vehicles and use the blockchain to quickly revoke their identity. However, the efficiency of the schemes in [20,26] was restricted by the number of group members. Zhang et al. [8] proposed a complete cross-domain authentication scheme based on blockchain. Participants from different trust domains can directly access the chain code in the blockchain, reducing the computational burden of the verification server. Wei et al. [14] proposed a cross-domain identity authentication scheme based on the identity cryptosystem on the consortium chain based on the IBC identity cryptosystem, aiming at the problem of cross-domain identity authentication when users access network services in different trust domains. However, the schemes in [8,14] are easy to leak user privacy. Tan et al. [24] proposed a pairless authentication and key management scheme for dynamic cross-domain authentication that achieved low latency and high reliability of vehicle-to-RSU transmission and ensured that vehicle privacy was not leaked, but did not achieve the traceability function.

Table 2. A comparison of the security attribute analysis with other schemes.

Reference	Privacy Protection	Efficiency is Independent of the Number of Members	Anonymity	Traceable	Dynamic User Addition
Ref [8]	×	√	×	√	×
Ref [14]	√	√	×	×	×
Ref [20]	√	×	√	×	√
Ref [24]	√	×	√	√	×
Ref [26]	√	×	√	√	√
Ours	√	√	√	√	√

4.2. Efficiency Analysis

We first analyzed the efficiency of the scheme described in Section 4 in terms of the security parameters. The time complexity of the group public key gpk was $\mathcal{O}(\lambda \cdot log^2\lambda) = \widetilde{\mathcal{O}}(\lambda)$, the time complexity of the signature key gsk was $\mathcal{O}(\lambda \cdot log^2\lambda) = \widetilde{\mathcal{O}}(\lambda)$, and the size of the signature was $\mathcal{O}(\lambda \cdot log^3\lambda) \cdot \omega(log\lambda) = \widetilde{\mathcal{O}}(\lambda)$. Table 3 shows the efficiency comparison between this scheme and other group signature schemes.

Table 3. A comparative analysis with the other group signature schemes.

Reference	Signature Size	Group Public Key Size	Signer's Private Key Size	Functional
[30]	$\widetilde{\mathcal{O}}(\lambda \cdot \ell)$	$\widetilde{\mathcal{O}}(\lambda^2 + \lambda \cdot \ell)$	$\widetilde{\mathcal{O}}(\lambda \cdot \ell)$	Static
[31]	$\widetilde{\mathcal{O}}(\lambda \cdot \ell)$	$\widetilde{\mathcal{O}}(\lambda^2 \cdot \ell)$	$\widetilde{\mathcal{O}}(\lambda)$	Partial dynamics
[32]	$\widetilde{\mathcal{O}}(\lambda \cdot \ell)$	$\widetilde{\mathcal{O}}(\lambda^2 \cdot \ell)$	$\widetilde{\mathcal{O}}(\lambda)$	Dynamics
[33]	$\widetilde{\mathcal{O}}(\lambda \cdot \ell)$	$\widetilde{\mathcal{O}}(\lambda^2 + \lambda \cdot \ell)$	$\widetilde{\mathcal{O}}(\lambda) + \ell$	—
Ours	$\widetilde{\mathcal{O}}(\lambda)$	$\widetilde{\mathcal{O}}(\lambda)$	$\widetilde{\mathcal{O}}(\lambda)$	Dynamics

4.3. Security Analysis

(1) Correctness analysis

Specifically, for an honest user, when they sign a message on behalf of the group, they are required to be able to prove possession of a valid tuple $\boldsymbol{\xi}$. The verify algorithm accepts **Πgs** with probability 1. Regarding the correctness of the open algorithm, please note

$$\begin{aligned} \mathbf{c_{1,1}} - \mathbf{c_{1,2}} \cdot \mathbf{s_1} &= \mathbf{b_1} \cdot \mathbf{g_1} + \mathbf{e_{1,2}} + \lfloor \mathbf{q/4} \rfloor \cdot \mathbf{rdec(p)} - (\mathbf{a} \cdot \mathbf{g_1} + \mathbf{e_{1,1}}) \cdot \mathbf{s_1} \\ &= (\mathbf{a} \cdot \mathbf{s_1} + \mathbf{e_1}) \cdot \mathbf{g_1} + \mathbf{e_{1,2}} + \lfloor \mathbf{q/4} \rfloor \cdot \mathbf{rdec(p)} - (\mathbf{a} \cdot \mathbf{g_1} + \mathbf{e_{1,1}}) \cdot \mathbf{s_1} \\ &= \mathbf{e_1} \cdot \mathbf{g_1} + \mathbf{e_{1,2}} - \mathbf{e_{1,1}} \cdot \mathbf{s_1} + \lfloor \mathbf{q/4} \rfloor \cdot \mathbf{rdec(p)} \end{aligned}$$

Among them $\|\mathbf{e_1}\|_\infty \leq \mathbf{B}, \|\mathbf{s_1}\|_\infty \leq \mathbf{B}, \|\mathbf{g_1}\|_\infty \leq \mathbf{B}, \|\mathbf{e_{1,1}}\|_\infty \leq \mathbf{B}, \|\mathbf{e_{1,2}}\|_\infty \leq \mathbf{B}$. For $\mathbf{B} = \widetilde{\mathcal{O}}\left(\mathbf{n^{5/4}}\right)$ and $\mathbf{q} = \widetilde{\mathcal{O}}(\mathbf{n^4})$,

Therefore,

$$\|\mathbf{e_1} \cdot \mathbf{g_1} + \mathbf{e_{1,2}} - \mathbf{e_{1,1}} \cdot \mathbf{s_1}\|_\infty \leq \mathbf{2n} \cdot \mathbf{B^2} + \mathbf{B} = \widetilde{\mathcal{O}}\left(\mathbf{n^{3.5}}\right) \leq \left\lceil \frac{\mathbf{q}}{\mathbf{10}} \right\rceil = \widetilde{\mathcal{O}}\left(\mathbf{n^4}\right)$$

In the case of probability 1, the open algorithm recovers rdec(p) and outputs the actual signer p. Therefore, the GM can identify the signer of the signature, thus guaranteeing the correctness of the open algorithm.

When the TM correctly restores rdec(p) and p, it also has a valid tuple (s1, e1, y) that satisfies the condition in (1). Then, ΠOpen is generated according to the perfect completeness of the demonstration system, and the TM will accept the open result output by the GM, so the correctness of the judge algorithm is established.

(2) Security analysis

Theorem 1. *Under the random oracle model, under the assumptions of RLWE and RSIS, it is proven that the proposed dynamic cross-domain authentication scheme based on group signature satisfies traceability.*

In the random oracle model, the proof of the theorem relies on the following facts:

1. *The zero-knowledge parameters used are simulation-sound.*
2. *For a correctly generated user key pair* $(\boldsymbol{x}, \boldsymbol{p})$*, it is impossible to find* $\boldsymbol{x'} \in \boldsymbol{R_q^m}$ *so that* $\|\boldsymbol{x'}\|_\infty \leq \mathbf{1}, \boldsymbol{x'} \neq \boldsymbol{x}$ *and* $\boldsymbol{B} \cdot \boldsymbol{x'} = \boldsymbol{p}$*.*

Proof of Theorem 1. The proof of the theorem is proved by the lemma given below. □

Lemma 1. *Assumptions* $\boldsymbol{RSIS^{\infty}_{n,\overline{m},q,\widetilde{\mathcal{O}}(n^2)}}$ *problems are hard to solve. Then, it is proved that the given group signature scheme is traceable in the random oracle model.*

Proof of Lemma 1. We prove traceability by contradiction. Assuming that the adversary $\mathcal{A}$ succeeds with a non-negligible advantage ϵ, we then construct a PPT algorithm $\mathcal{B}$, based on the complexity of the problem $\mathbf{RSIS^{\infty}_{n,\overline{m},q,\widetilde{\mathcal{O}}(n^2)}}$, which breaks the unforgeability of the signature scheme with a non-negligible probability. Then, we prove that our construction is traceable. □

When a verification key for a signature scheme is given, the simulator faithfully runs the experiments when given the verification key for the signature scheme. $\mathcal{B}$ can answer $\mathcal{A}$ all oracle queries. However, it is possible to resort to the query on the signature scheme. In both cases, the corresponding user is registered to the group. When $\mathcal{A}$ is stopped, it outputs $\left(\mathbf{M}^*, \mathbf{\Pi^*_{gs}}, \mathbf{c_1^*}, \mathbf{c_2^*}\right)$. $\mathcal{A}$ wins the experiment with a non-negligible probability. Parse $\left(\{\mathbf{CMT_i^*}\}^{\kappa}_{\mathbf{i=1}}, \mathbf{CH}^*, \{\mathbf{RSP_i^*}\}^{\kappa}_{\mathbf{i=1}}\right)$. Let $\xi^* = \left(\mathbf{A}, \mathbf{A_{[0]}}, \ldots, \mathbf{A_{[d]}}, \mathbf{F}, \mathbf{F_0}, \mathbf{F_1}, \mathbf{u}, \mathbf{B}, \mathbf{a}, \mathbf{b_1}, \mathbf{b_2}, \mathbf{c_1^*}, \mathbf{c_2^*}\right)$.

Then, $\mathbf{CH}^* = \mathcal{H}_{\mathbf{FS}}\left(\mathbf{M}^*, \{\mathbf{CMT_i^*}\}^{\kappa}_{\mathbf{i=1}}, \xi^*\right)$ and $\mathbf{RSP_i^*}$ is a valid response w.r.t. $\mathbf{CMT_i^*}$ and for each $\mathbf{i} \in [\kappa]$, $\mathbf{CH_i^*}$ the fact that $\mathcal{A}$ wins and $\left(\mathbf{\Pi^*_{gs}}, \mathbf{c_1^*}, \mathbf{c_2^*}\right)$ is therefore a valid signature on $\mathbf{M}^*$.

We think $\mathcal{A}$ made a query $\left(\mathbf{M}^*, \{\mathbf{CMT_i^*}\}^{\kappa}_{\mathbf{i=1}}, \xi^*\right)$ to the hash oracle $\mathcal{H}_{\mathbf{FS}}$ with overwhelming probability. Otherwise, the probability of guessing the correct value of $\mathcal{H}_{\mathbf{FS}}\left(\mathbf{M}^*, \{\mathbf{CMT_i^*}\}^{\kappa}_{\mathbf{i=1}}, \xi^*\right)$ is at most $\mathbf{3^{-\kappa}}$, which is negligible. Therefore, there is a probability of $\epsilon' = \epsilon - \mathbf{3^{-\kappa}}$ querying $\mathcal{H}_{\mathbf{FS}}$. $\theta^* \in \{\mathbf{1}, \mathbf{2}, \ldots, \mathbf{Q_H}\}$ is the index for a particular query, where $\mathbf{Q_H}$ is the total number of hash queries $\mathcal{A}$ made.

The algorithm $\mathcal{B}$ is then run at most $\mathbf{32} \cdot \mathbf{Q_H} / \epsilon'$ times. For each new run, it is exactly the same as the original run until the θ^*th query of $\mathcal{H}_{\mathbf{FS}}$. From this point of view, for each new run, the returned hash query has uniformly random and independent values. This guarantees that the input to the θ^*th query is a tuple $\left(\mathbf{M}^*, \{\mathbf{CMT_i^*}\}^{\kappa}_{\mathbf{i=1}}, \xi^*\right)$ for each new run, while the output of this hash query is consistently random and independent for each new run. Thus, the same tuple with pairwise distinct hash values $\mathbf{CH^{(1)}_{\theta^*}}, \mathbf{CH^{(2)}_{\theta^*}}, \mathbf{CH^{(3)}_{\theta^*}} \in \{\mathbf{1}, \mathbf{2}, \mathbf{3}\}^{\kappa}$ and corresponding valid responses $\mathbf{RSP^{(1)}_{\theta^*,j}}, \mathbf{RSP^{(2)}_{\theta^*,j}}, \mathbf{RSP^{(3)}_{\theta^*,j}}$ are obtained with greater than or equal to probability $\mathbf{1/2}$. A simple calculation shows that there is a probability $\mathbf{1} - \left(\frac{7}{9}\right)^{\kappa}$, proof that for each $\mathbf{j} \in \{\mathbf{1}, \mathbf{2}, \ldots, \kappa\}$, there is $\left\{\mathbf{CH^{(1)}_{\theta^*,j}}, \mathbf{CH^{(2)}_{\theta^*,j}}, \mathbf{CH^{(3)}_{\theta^*,j}}\right\} = \{\mathbf{1}, \mathbf{2}, \mathbf{3}\}$.

Therefore, for all challenges $\mathbf{1}, \mathbf{2}, \mathbf{3}$ w.r.t. the same $\mathbf{CMT_j^*}$, there are three valid responses $\mathbf{RSP^{(1)}_{\theta^*,j}}, \mathbf{RSP^{(2)}_{\theta^*,j}}, \mathbf{RSP^{(3)}_{\theta^*,j}}$. $\mathcal{B}$ is able to extract witnesses due to **COM** being computationally binding

$$\mathbf{t}^* \in \mathcal{T}_{\mathbf{d}}; \mathbf{r}^* \in \mathbf{R}_{\mathbf{q}}^{\overline{\mathbf{m}}}; \mathbf{v}^* \in \mathbf{R}_{\mathbf{q}}^{\overline{\mathbf{m}}+\mathbf{k}}; \mathbf{p}^* \in \mathbf{R}_{\mathbf{q}}^{\ell},$$

make $\|\mathbf{r}^*\|_{\infty} \leq \beta$, $\|\mathbf{v}^*\|_{\infty} \leq \beta$, $\|\mathbf{p}^*\|_{\infty} \leq \mathbf{1}$ and

$$\mathbf{A_{t^*}} \cdot \mathbf{v}^* = \mathbf{F} \cdot \mathbf{rdec}(\mathbf{F_0} \cdot \mathbf{r}^* + \mathbf{F_1} \cdot \mathbf{p}^*) + \mathbf{u},$$

$\mathbf{c_1^*}, \mathbf{c_2^*}$ are the correct encryption of $\mathbf{p}^*$.

As a result of $\mathcal{A}$ winning the competition, we either have (i) the open algorithm output $(\perp, \perp)$, or (ii) the open algorithm output $\left(\mathbf{p}', \mathbf{\Pi^*_{open}}\right)$, $\mathbf{p}' \neq \perp$, but the judge algorithm rejects the open result.

Case (i), if $\mathbf{c_1^*}$ is decrypted as $\mathbf{p}'$ and $\mathbf{p}' \in \mathbf{R_q}$ so that $\boldsymbol{\tau}(\mathbf{p}') = \mathbf{H} \cdot \boldsymbol{\tau}(\mathbf{p}') \in \mathbb{Z}_{\mathbf{q}}^{\mathbf{n}}$, $\mathbf{p}'$ is not in the registry. From the decryption, we know that $\mathbf{p}^*$ will be decrypted by the correctness of our encryption scheme. Therefore, the middle open result is $\mathbf{p}' = \mathbf{p}^*$. On the other hand, the fact that $\mathbf{p}'$ is not in the registry means that the group is not joined. All in all, $\mathcal{B}$ without querying the signature on $\mathbf{p}'$ and extracting the signature $(\mathbf{t}^*, \mathbf{r}^*, \mathbf{v}^*)$ on $\mathbf{p}'$, making $\boldsymbol{\tau}(\mathbf{p}') = \mathbf{H} \cdot \boldsymbol{\tau}(\mathbf{p}')$. Hence $(\mathbf{p}^*, \mathbf{t}^*, \mathbf{r}^*, \mathbf{v}^*)$ is a valid forgery of the signature scheme.

Case (ii), if $\mathbf{c_1^*}$ is decrypted as $\mathbf{p}'$ and $\mathbf{p}' \in \mathbf{R_q}$ makes $\boldsymbol{\tau}(\mathbf{p}') = \mathbf{H} \cdot \boldsymbol{\tau}(\mathbf{p}') \in \mathbb{Z}_{\mathbf{q}}^{\mathbf{n}}$, $\mathbf{p}'$ is in the registry and $\boldsymbol{\Pi}_{\text{open}}^*$ is not accepted by the judge algorithm. From decryption, we know that $\mathbf{p}^*$ will be decrypted by the correctness of our encryption scheme. Hence, the middle open result is $\mathbf{p}' = \mathbf{p}^*$. On the other hand, we think $\mathbf{rdec}(\mathbf{p}') \neq \mathbf{p}' = \mathbf{p}^*$. Otherwise, $\mathbf{dec}(\mathbf{p}') = \mathbf{p}' = \mathbf{p}^*$, $\mathcal{B}$ has a valid proof to generate $\boldsymbol{\Pi}_{\mathbf{open}}^*$. Due to the perfect completeness generated by the underlying argument system, it will be accepted by the judge algorithm with probability 1. This is contradictory, so we obtain $\mathbf{rdec}(\mathbf{p}') \neq \mathbf{p}' = \mathbf{p}^*$. Recall that in the join algorithm, the issuer only generates signatures on $\mathbf{rdec}(\mathbf{p}')$. Therefore, only the signatures on $\mathbf{rdec}(\mathbf{p}')$ are queried, so $(\mathbf{p}^*, \mathbf{t}^*, \mathbf{r}^*, \mathbf{v}^*)$ is a valid forgery of the signature scheme.

Therefore, the unforgeability $\frac{1}{2} \cdot (\epsilon - 3^{-\kappa})\left(1 - \left(\frac{7}{9}\right)^{\kappa}\right)$ of the signature scheme is broken at least with a non-negligible probability, and the proof is complete.

Discussion and limitation. This paper used blockchain distributed ledger storage to achieve cross domain authentication between trust domains and can be applied to the distributed power grid management scenarios for production consumers mentioned in [34] such as mutual authentication between different communities. However, traditional blockchain technology requires miners' nodes to have strong computing power and sufficient storage space to ensure the consensus and tamper resistance of transaction ledgers across the entire network, which limits resource constrained devices (such as power grid nodes) from joining the blockchain. Therefore, our future work is to utilize lightweight blockchain technology to achieve cross domain authentication.

5. Conclusions

Aiming at the privacy protection of cross-domain authentication between different authentication mechanisms in the IoT environment, this paper proposed a dynamic cross-domain authentication scheme by using group signature technology and the distributed peer-to-peer network architecture of blockchain technology, and proved the security of the protocol under the random oracle model. The analysis shows that the protocol was proven to be secure in the random oracle model, and the size of the signature generated by the scheme was independent of the number of group members N and only depended on the security parameters λ. It effectively improved the operation efficiency of the protocol and proved that the scheme has good security and effectiveness. In the future, we will focus on using lightweight blockchain for dynamic cross-domain authentication in IoT.

Author Contributions: Validation, M.L.; Data curation, L.Z.; Writing—original draft, X.L.; Writing—review & editing, W.Y. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported by the National Natural Science Foundation of China (61972073), the Key Research and Development Program of Hebei Province of China (22340701D), and the Natural Science Foundation of Hebei Province of China (F2022201005).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The data is unavailable due to privacy or ethical restrictions.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Akbar, A.; Jangsher, S.; Bhatti, F.A. NOMA and 5G emerging technologies: A survey on issues and solution techniques. *Comput. Netw.* **2021**, *190*, 107950. [CrossRef]
2. Qureshi, K.N.; Din, S.; Jeon, G.; Piccialli, F. Internet of Vehicles: Key Technologies, Network Model, Solutions and Challenges with Future Aspects. *IEEE Trans. Intell. Transp. Syst.* **2020**, *22*, 1777–1786. [CrossRef]
3. Cui, J.; Liu, N.; Zhang, Q.; He, D.; Gu, C.; Zhong, H. Efficient and Anonymous Cross-Domain Authentication for IIoT Based on Blockchain. *IEEE Trans. Netw. Sci. Eng.* **2022**, *10*, 899–910. [CrossRef]

4. Huang, C.; Xue, L.; Liu, D.; Shen, X.; Zhuang, W.; Sun, R.; Ying, B. Blockchain-Assisted Transparent Cross-Domain Authorization and Authentication for Smart City. *IEEE Internet Things J.* **2022**, *9*, 17194–17209. [CrossRef]
5. Zhou, X.; Miao, F.; Xiong, Y. A Certificate Authority Domain-based Cross-domain Authentication Scheme for Virtual Enterprise Using Identity Based Encryption. In Proceedings of the 2021 7th International Conference on Big Data Computing and Communications, Deqing, China, 13–15 August 2021; pp. 144–149. [CrossRef]
6. Wang, Z.; Ma, Z.F.; Luo, S.S. Identity-based Efficient Authentication Key Agreement Protocol for Mobile Internet. *J. Commun.* **2017**, *38*, 19–27. [CrossRef]
7. Ning, B.; Deng, L. Identity-based two-party cross-domain authentication key agreement protocol. *J. Guizhou Norm. Univ. (Nat. Sci. Ed.)* **2020**, *38*, 92–100. [CrossRef]
8. Zhang, H.; Chen, X.; Lan, X.; Jin, H.; Cao, Q. BTCAS: A Blockchain-Based Thoroughly Cross-Domain Authentication Scheme. *J. Inf. Secur. Appl.* **2020**, *55*, 102538. [CrossRef]
9. Jiang, Z.; Shi, C. Cross-domain identity authentication scheme based on heterogeneous systems in hybrid cloud envi-ronment. *Comput. Eng.* **2019**, *45*, 13–18. [CrossRef]
10. Lin, Y.; Wang, X.; Gan, Q.; Yao, M. A secure cross-domain authentication scheme with perfect forward security and complete anonymity in fog computing. *J. Inf. Secur. Appl.* **2021**, *63*, 103022. [CrossRef]
11. Jiang, Z.; Xu, J. Efficient heterogeneous cross-domain authentication scheme based on proxy blind signature in cloud environment. *Comput. Sci.* **2020**, *47*, 60–67. [CrossRef]
12. Wei, S.; Li, S.; Wang, J. Cross-domain authentication protocol based on identity cryptography system and blockchain. *Chin. J. Comput.* **2021**, *44*, 908–920. [CrossRef]
13. Bagga, P.; Sutrala, A.K.; Das, A.K.; Vijayakumar, P. Blockchain-based batch authentication protocol for Internet of Vehicles. *J. Syst. Arch.* **2020**, *113*, 101877–101883. [CrossRef]
14. Singh, P.K.; Singh, R.; Nandi, S.K.; Ghafoor, K.Z.; Rawat, D.B.; Nandi, S. Blockchain-Based Adaptive Trust Management in Internet of Vehicles Using Smart Contract. *IEEE Trans. Intell. Transp. Syst.* **2020**, *22*, 3616–3630. [CrossRef]
15. Li, J.L.; Ji, Y.; Choo, K.-K.R.; Hogrefe, D. CL-CPPA: Certificate-Less Conditional Privacy-Preserving Authentication Protocol for the Internet of Vehicles. *IEEE Internet Things J.* **2019**, *6*, 10332–10343. [CrossRef]
16. Zhang, J.; Li, X.; Zeng, X.; Zhao, Y.; Duan, R.; Yang, D. Blockchain-based cross-domain authentication and key agreement protocol in edge computing environment. *J. Inf. Secur.* **2021**, *6*, 54–61. [CrossRef]
17. Li, G.; Wang, Y.; Zhang, B.; Lu, S. Smart Contract-Based Cross-Domain Authentication and Key Agreement System for Heterogeneous Wireless Networks. *Mob. Inf. Syst.* **2020**, *2020*, 2964562. [CrossRef]
18. Dong, G.; Chen, Y.; Li, H. Research on the credibility of cross-domain authentication based on blockchain in heterogeneous environments. *Commun. Technol.* **2019**, *52*, 1450–1460.
19. Ghane, S.; Jolfaei, A.; Kulik, L.; Ramamohanarao, K.; Puthal, D. Preserving Privacy in the Internet of Connected Vehicles. *IEEE Trans. Intell. Transp. Syst.* **2020**, *22*, 5018–5027. [CrossRef]
20. Yang, Y.; Hu, M.; Kong, S.; Gong, B.; Liu, X. Scheme on Cross-Domain Identity Authentication Based on Group Signature for Cloud Computing. *Wuhan Univ. J. Nat. Sci.* **2019**, *24*, 134–140. [CrossRef]
21. Ali, Z.; Chaudhry, S.A.; Mahmood, K.; Garg, S.; Lv, Z.; Bin Zikria, Y. A clogging resistant secure authentication scheme for fog computing services. *Comput. Netw.* **2020**, *19*, 107731. [CrossRef]
22. Chaudhry, S.A. Designing an Efficient and Secure Message Exchange Protocol for Internet of Vehicles. *Secur. Commun. Netw.* **2021**, *56*, 5554318. [CrossRef]
23. Luo, M.; Wu, J.; Li, X. Cross-domain certificateless authenticated group key agreement protocol for 5G network slicings. *Telecommun. Syst.* **2020**, *45*, 456–489. [CrossRef]
24. Tan, H.; Xuan, S.; Chung, I. HCDA: Efficient Pairing-Free Homographic Key Management for Dynamic Cross-Domain Authentication in VANETs. *Symmetry* **2020**, *12*, 1003. [CrossRef]
25. Xu, Z.; Liang, W.; Li, K.-C.; Xu, J.; Jin, H. A blockchain-based Roadside Unit-assisted authentication and key agreement protocol for Internet of Vehicles. *J. Parallel Distrib. Comput.* **2020**, *65*, 589–601. [CrossRef]
26. Zhang, H.; Huang, H.; Liu, K.; He, X. A provably secure anonymous and traceable fast group authentication protocol in the Internet of Vehicles. *J. Commun.* **2021**, *42*, 213–225. [CrossRef]
27. Elkhalil, A.; Zhang, J.; Elhabob, R.; Eltayieb, N. An efficient signcryption of heterogeneous systems for Internet of Vehicles. *J. Syst. Arch.* **2021**, *113*, 101885. [CrossRef]
28. Trivedi, H.S.; Patel, S.J. Design of secure authentication protocol for dynamic user addition in distributed Internet-of-Things. *Comput. Netw.* **2020**, *178*, 107335. [CrossRef]
29. Ling, S.; Nguyen, K.; Wang, H.; Xu, Y. Constant-Size Group Signatures from Lattices. In Proceedings of the 21st International Conference on Practice and Theory of Public-Key Cryptography, Rio de Janeiro, Brazil, 25–29 March 2018; pp. 58–88. [CrossRef]
30. Shafieinejad, M.; Esfahani, N.N. A scalable post-quantum hash-based group signature. *Des. Codes Cryptogr.* **2021**, *89*, 1061–1090. [CrossRef]
31. Kong, W.; Shen, J.; Vijayakumar, P.; Cho, Y.; Chang, V. A practical group blind signature scheme for privacy protection in smart grid. *J. Parallel Distrib. Comput.* **2020**, *136*, 29–39. [CrossRef]

32. Ling, S.; Nguyen, K.; Wang, H.; Xu, Y. Lattice-Based Group Signatures: Achieving Full Dynamicity with Ease. In Proceedings of the 15th International Conference on Applied Cryptography and Network Security, Kanazawa, Japan, 10–12 July 2017; pp. 293–312. [CrossRef]
33. Kundu, N.; Debnath, S.K.; Mishra, D. A secure and efficient group signature scheme based on multivariate public key cryptography. *J. Inf. Secur. Appl.* **2021**, *58*, 102776. [CrossRef]
34. Górski, T. Reconfigurable Smart Contracts for Renewable Energy Exchange with Re-Use of Verification Rules. *Appl. Sci.* **2022**, *12*, 5339. [CrossRef]