IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received June 21, 2019, accepted June 28, 2019, date of publication July 2, 2019, date of current version July 17, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2926404

Group Key Agreement Protocol Based on Privacy Protection and Attribute Authentication

ZHANG QIKUN[1], LI YONGJIAO[1], GAN YONG[2], ZHENG CHUANYANG[3], LUO XIANGYANG[4], AND ZHENG JUN[5]

[1]Institute of Computer and Communication Engineering, Zhengzhou University of Light Industry, Zhengzhou 450002, China
[2]Zhengzhou Institute of Technology, Zhengzhou 450044, China
[3]Department of Computer Science, Hong Kong Baptist University, Hong Kong
[4]State Key Laboratory of Mathematical Engineering and Advanced Computing, Zhengzhou 450002, China
[5]School of Computer Science and Technology, Beijing Institute of Technology, Beijing 100081, China

Corresponding author: Zheng Jun (zhengjun_bit@163.com)

This work was supported in part by the National Natural Science Foundation of China under Grant 61772477, Grant 61572445, and Grant U1804263, in part by the National Key Research and Development Program of China under Grant 2018YFB1004402, in part by the Beijing Municipal Natural Science Foundation under Grant 4172053, and in part by the Natural Science Foundation of Henan Province under Grant 162300410322.

ABSTRACT Group key agreement is a good way to ensure secure communication within a group. However, the identity authentication, privacy protection, and information sharing access control (different access rights may exist for different sensitivity of information) are key issues to be solved in group key agreement. Aiming at these problems, this paper proposes a group key agreement protocol based on privacy protection and attribute authentication (GKA-PPAA). The protocol proposes identity authentication for hidden attributes; it not only preserves the advantages of traditional identity-based key agreement protocol, but also provides hiding the identity information and privacy protection of the individual, and also proposes information sharing access control, which different secret information is shared among a set of members who have different levels of authority. It increases the flexibility of group key management. In addition, the group key factors are also calculated before the group key agreement, which eliminates most of the computation overhead due to the group key agreement. This protocol is proven secure under the discrete logarithm problem (DLP) and decisional bilinear Diffie-Hellman (DBDH) problem assumptions. The performance analysis shows that the proposed scheme is much more efficient than the existing ones.

INDEX TERMS Group key agreement, attribute authentication, information exchange, threshold authority.

I. INTRODUCTION

The recent security concerns are prevailing when multiple devices over a wireless communication interact among them leaking sensitive information to a non-participating entity [1], [2]. Group key agreement is a secure and robust approach to establish group keys for secure group oriented applications over non-private underlying networks. Therefore, the group key agreement protocol is a good way to ensure secure communication within a group. However, people are worried about privacy protection and authentication. Implementing privacy protection ensures that communication messages are not intercepted by eavesdroppers, and authentication ensures that any unauthorized user cannot fraudulently obtain the required services from the primary domain. Authenticated key agreement protocols concern the identity authentication of users, which ensures only the intended group members to establish a group session key to use encryption communication. At the same time, lightweight, small computing and communication overhead and security are important indicators in group key negotiation. With these demands in mind, Group key agreement protocol based on privacy protection and attribute authentication is proposed.

In this paper, for the sensitivity of the communication information and the permissions of terminals are different, information exchange may need different set member in the same group. Therefore, based on the different attributes of members, we propose a key agreement protocol for securely exchanging different secret information between members of different privilege groups. This protocol combines the advantages of attribute encryption and identity authentication. Attribute encryption and authentication techniques are adopted to guarantee the secure of group key agreement, and protect the personal privacy.

The associate editor coordinating the review of this manuscript and approving it for publication was Zheli Liu.

A. RELATED WORK

The first key agreement protocol based on asymmetric cryptography was proposed by Diffie and Hellman in 1976 [3]. Since then, many researches have been done in this area. Dynamic asymmetric group key agreement concerns about the scenarios such as the terminals in mobile cloud networks may join or leave at any given time [4], [5]. Authenticated key agreement protocols authenticate the identities of users to ensure that only the intended group members can establish a session in which the group members can communicate with each other [6], [7]. The affiliation-hiding protocol not only exhibits the affiliation-hiding property, but also holds the properties of detectability and perfect forward secrecy [8]–[11].

On the security of authenticated group key agreement is proposed in [12]–[14], which contributes to identify the security vulnerabilities in the existing protocols, and present a fix to the ephemeral secret key leakage attack of the protocol presented by Tan and Gupta and Biswas to make it secure. An authenticated asymmetric group key agreement based on attribute encryption is proposed [15], which combines the advantages of attribute encryption and identity authentication. Attribute encryption and authentication techniques are adopted to guarantee the secure of group key agreement, and protect the personal privacy. Its computation and communication loads moved to powerful server to reduce the workload on terminal. It is suitable to use in centralized network environment. Secure group communication is of great importance for many collaborative and distributed applications in Internet of Things [16], [17]. A secure and efficient group key agreement scheme for VANET is proposed in [18], which negotiates a dynamic session secret key using a fixed roadside unit help to provide more stable communication performance and speed up the encryption and decryption process to ensures that vehicles exchange information securely in VANET.

Multi-domain lightweight asymmetric group key agreement is proposed in [19]–[21], which adopts the bilinear mapping and blind key technology to achieve an asymmetric group key agreement protocol among mobile terminals distributed in different domains and proposes a communication and computation migration technologies to ensure that the mobile terminal lightweight computing and communication consumption and also can achieve anonymity and authentication. An authenticated group key agreement protocol with user anonymity based on Chebyshev chaotic maps is proposed in [22], it can resist reflection attack and achieve contributory group key agreement with user authentication, and it is suitable for multi-server and mobile environments. A cross-domain lightweight asymmetric group key agreement to establish a safe and efficient group communication channel between sensor nodes is proposed in [23], [24]. In this protocol, the computation and communication overhead are lightweight.

A dynamic and cross-domain authenticated asymmetric group key agreement is proposed in [25]. This protocol adopts cross-domain authentication mechanism to avoid the security risks of key escrow and the complexity of certificate management. It supports the dynamic group key update of nodes for forward secrecy and backward security of group key, and also achieves the key self-certified, the member participated group key agreement can self-certify whether the calculated group keys are correct. A Certificateless One-Way Group Key Agreement Protocol for End-to-End Email Encryption is proposed in [26], [27], which is suitable to implement E2E email encryption. The group key agreement is certificateless, so there are no key escrow problem and no public key certificate infrastructure is required, and it is one-way group key agreement and thus no back-and-forth message exchange is required. At the same time, it is a n-party group key agreement (not just 2- or 3-party).

A group key agreement mechanism based on the Chinese remainder theorem is proposed to distribute the group key for authenticated vehicles in [28]–[31]. The group key can be updated when the vehicle joins and leaves the group. It needs a third-party trusted organization with strong computing and storage capabilities to distribute group key for all vehicles, and it has security risks. A Twofold Group Key Agreement Protocol for NoC based MPSoCs is proposed in [32], [33], which proposes a twofold group key agreement protocol which addresses the need of a shared symmetric key among insider members in a group and an asymmetric key pair for any unrestricted sender. The proposed protocol offers a lightweight symmetric encryption for intra zone communication and a public key encryption for inter zone communication taking most advanced security issues into account.

A password-based conditional privacy preserving authentication and group-key generation protocol for VANETs is presented in [34]. This protocol offers group-key generation, user leaving, user joining and password change facilities. It is lightweight in terms of computation and communication since it can be designed without bilinear-pairing and elliptic curve. Concurrently Deniable Group Key Agreement and Its Application to Privacy-Preserving VANETs is proposed in [35], [36], which present a novel transformation from an unauthenticated group key agreement to a deniable (authenticated) group key agreement without increasing communication round. It designs an authenticated and privacy-preserving communication protocol for VANETs by using the proposed deniable group key agreement.

A Survey on Group Key Agreement Protocols in Cloud Environment is proposed in [37]–[39], which are group key agreement protocol, triple-party protocol and double-party protocol, according to the number of users participating in the agreement. Then we give a summary of these proposed key agreement protocols based on the classification. After performing analysis on security and performance of these key agreement protocols respectively, a comment on each category is made.

Certificateless and identity-based authenticated asymmetric group key agreement is proposed in [40], which formalizes the security model of certificateless authenticated asymmetric group key agreement and realizes a one-round

certificateless authenticated asymmetric group key agreement protocol to resist active attacks in the real world. It investigates the relation between certificateless authenticated Asymmetric group key agreement and identity-based authenticated Asymmetric group key agreement, and also proposes a concrete conversion from certificateless authenticated Asymmetric group key agreement to session key escrow-free identity-based authenticated Asymmetric group key agreement.

A secure and efficient group key agreement protocol is proposed in [41], [42], it is adaptive for cluster-based communications in mobile ad hoc networks. It describes a novel secure cluster-head selection mechanism in the proposed protocol. The protocol provides security for dynamic group operations in addition to the basic security properties. A secure key agreement protocol for dynamic group is proposed in [43]. In this work, it focuses on the confidentiality aspect of secure group communication. If a member or group of members wants to join a secure communication group, they should initially be authenticated by a separate authentication protocol. A self-authentication and deniable efficient group key agreement protocol is proposed in [44], [45]. The scheme establishes a group between road side units and vehicles by using self-authentication without certification authority, and improves certification efficiency by using group key transmission method.

Authenticated Group Key Agreement Protocol without Pairing is proposed in [46], [47], which achieved security of the proposed scheme following the most standard and recent security notion namely the EGBG model. It has proved the authenticated key exchange (AKE) security and the mutual authentication (MA) security with full forward secrecy, considering leakage of both the keys long-term and ephemeral, adopting a comparatively efficient technique, the game hopping technique. A Certificateless Group Authenticated Key Agreement Protocol for Secure Communication in Untrusted UAV Networks is proposed in [48], which propose to tackle the problem of secure communication among untrusting parties with a certificateless-group authenticated key agreement (CL-GAKA) scheme to enable confidentiality, message integrity, and authenticity in drone communications.

An efficient one round certificateless authenticated group key agreement protocol is proposed in [49], [50], it satisfies the security demand of mobile Ad Hoc networks. The protocol has achieved appropriate optimization to improve the performance of Ad Hoc networks in terms of frequent communication interruptions and reconnections. In addition, it has reduced executive overheads of key agreement protocol to make the protocol more suitable for mobile Ad Hoc network applications.

A flexible asymmetric group key agreement protocol that information exchange and transmission are orientable is proposed in [51]. The paper adopts bilinear mapping and two-way anonymous authentication technology to hide personal identity authentication information, and uses storage and computing migration technology to reduce the resource consumption of mobile terminal, and also proposes the secret key factor oriented extraction and combinations technology to achieve multi-level three-dimensional complex space security information exchange requirements and meet the lightweight computing. A secure chaotic maps-based group key agreement scheme is proposed in [52], [53], which provides member anonymity to ensure the privacy of the communication between the social networking platform and the members. This protocol integrates the mechanisms of message encryption and member verification into the scheme to allow the members to anonymously interact with the services of the online social network, thereby enhancing the credibility of the online social network system.

B. MOTIVATION AND CONTRIBUTION

Through the analysis of the above research status, in the current group key agreement process, exchanged information in the group is shared among all members of this group, this means that all members of the group have the same information sharing permissions, and the hierarchical group information security exchange cannot be implemented. That is, different sensitivity information can only be shared among group members with corresponding rights, and group members who do not have corresponding rights cannot share the information. The current group key negotiation study also does not implement the personal privacy protection function well, in the process of the group key agreement, the group members are easy to expose personal identity information or expose personal attribute information. To solve the above problems, the contributions of this paper are as follows:

1) An identity authentication technology based on hidden attributes is proposed, which not only hides identity information but also hides attribute information. It not only preserves the advantages of traditional identity-based key agreement protocol, but also provides protection for personal privacy.

2) A threshold-based information exchange technology is proposed, in which only the threshold of the attribute meeting the group key agreement requirement can be used for group key agreement, thereby implementing group information exchange. Different secret information is shared among a set of members who have different levels of authority. When a person has some secret information, he can exchange information with some people who have the appropriate level of security permissions rather than all the members in the group. It increases the flexibility and security of group information exchange.

3) A group key calculation correctness self-validation algorithm is proposed, in which each group key agreement participant can verify whether the calculated group key is correct according to the parameters in the calculation process. All the participants can verify the group keys correctness without any other additional communication.

C. ORGANIZATION

In section II, we describe the proposed group key agreement in this paper; In section III, we analyze and prove the

correctness and security of GKAP-PPAA protocol; In section IV, we further analyze the efficiency and performance of the protocol. Finally, we conclude the paper in Section V.

II. THE PROPOSED GROUP KEY AGREEMENT PROTOCOL

A. BILINEAR MAPS AND COMPLEXITY ASSUMPTIONS

This paper is based on the basic theory of bilinear mapping; some basic knowledge related to bilinear mapping will be described in this section.

Let G_1 be an additive group and G_2 is a multiplicative group. Both of them have the same prime order q, where $q \geq 2^{\ell}+1$, and ℓ is a security parameter. G_1 is generated by g_1, that means $G_1 = \langle g_1 \rangle$, and the discrete logarithm problems of G_1 and G_2 are difficult. We call e an admissible pairing, if $e : G_1 \times G_1 \rightarrow G_2$ satisfies the follow properties:

(1) bilinearty: For all $\mu, \nu \in G_1$, and $a, b \in \mathbb{Z}_q^*$, there is $e(a\mu, b\nu) = e(\mu, \nu)^{ab}$;

(2) Non-degeneracy: There exits $\mu, \nu \in G_1$, such that $e(\mu, \nu) \neq 1$;

(3) Computability: For all $\mu, \nu \in G_1$, there exists a efficient way to calculate $e(\mu, \nu)$.

Inference1. For all $\mu, \nu, g_1 \in G_1$, there is $e(\mu+\nu, g_1) = e(\mu, g_1)e(\nu, g_1)$.

B. LAGRANGIAN INTERPOLATION THEOREM

Generally, if known $y = f(x)$ has different function values $y_0, y_1, \cdots, y_n$ at the $n+1$ different points $x_0, x_1, \cdots, x_n$, this function passes through these $n+1$ points $(x_0, y_0), (x_1, y_1), \cdots, (x_n, y_n)$, we can consider constructing a polynomial $y = P_n(x)$ of degree at most n that passes through the $n+1$ points to satisfy: $P_n(x_k) = y_k$, $k = 0, 1, \cdots, n$

To estimate any point ε where $\varepsilon \neq x_i, i = 0, 1, 2, \cdots, n$ to use the value of $P_n(\varepsilon)$ as the approximation of the accurate value of $f(\varepsilon)$. This method is called interpolation. The formula $P_n(x_k) = y_k, k = 0, 1, \cdots, n$ is interpolation condition or criterion and the minimum interval $[a, b]$ containing $x_i (i = 0, 1, \cdots, n)$ where $a = \min\{x_0, x_1, \cdots, x_n\}$ and $b = \max\{x_0, x_1, \cdots, x_n\}$.

General Form Application Method. There are n points $(x_0, y_0), (x_1, y_1), \cdots, (x_{n-1}, y_{n-1})$ in the plane. Now a function $f(x)$ is used to make the image pass through these n points. The specific methods are as follows:

Practice. Let a set D_n be a set of subscripts about point (x, y), where $D_n = \{0, 1, \cdots, n-1\}$ and then make n polynomials $p_j(x)$ where $j \in D_n$. For any $k \in D_n$, there are p_k and $B_k = \{i \,|\, i \neq k, i \in D_n\}$, so that $p_k(x) = \prod_{i \in B_k} \frac{x - x_i}{x_k - x_i}$.

where the formula $p_k(x)$ is a polynomial of degree $n-1$ and satisfies $p_k(x_m) = 0$ and $p_k(x_k) = 1$ for all $m \in Ik$,so that $L_n(x) = \sum_{i=0}^{n-1} y_j p_j(x)$. The interpolation polynomial $L_n(x)$ of the form above is called Lagrange interpolation polynomial.

C. INITIALIZATION

In this section, we describe a group key agreement protocol based on privacy protection. The protocol consists of AA (Attribute Authority) and network terminals. AA is a key entity who generates system public parameters and master keys. The system public parameters contain some group key parameters, which can be used by network terminals to negotiate group session keys. Especially, it performs attribute authentication and permission distribution of network terminals. AA also manages users in other areas and it is fully trusted by entities in the group key agreement protocol.

In this work, it is assumed that the protocol contains an AA and n network terminals. Let $U = \{u_1, u_2, \ldots, u_n\}$ be the set of network terminals. And the corresponding identity set is $ID = \{id_{u_1}, id_{u_2}, \ldots, id_{u_n}\}$. AA defines an ordered network attribute set $Attr = \{A_1, A_2, \ldots, A_j, \ldots, A_R\}$, where $A_j < A_{j+1} (j < R)$ and $R \in N^*$ denotes the number of the network attribute. And $attr_i = \{a_{i,1}, a_{i,2}, \ldots, a_{i,r}\}$ is the ordered attribute set of network terminal u_i, where $attr_i \subseteq Attr$, $r \in N^*$, $r \leq R$ and $a_{i,r-1} < a_{i,r}$. i denotes the ith terminal and r denotes the rth attribute of u_i.

Network terminals participated in group key agreement for group security communication must have some common attributes in network.

Assuming G_1 is an additive group, and the G_2 is a multiplicative group. The discrete logarithm over G_1 and G_2 is difficult. Assuming $g_1 \in G_1$ is a generator of G_1. G_1 and G_2 have the same large prime number order q. Parameter e is a computable bilinear mapping and $e : G_1 \times G_1 \rightarrow G_2$. $H_1 : \{0,1\}^* \rightarrow \mathbb{Z}_q^*$, $H_2 : G_1 \rightarrow \mathbb{Z}_q^*$ and $H_3 : G_2 \rightarrow \mathbb{Z}_q^*$ are three hash functions.

KeyGen. $KeyGen\left(1^{\lambda}\right) \rightarrow (PK_A, SK_A)$: The $KeyGen\left(1^{\lambda}\right)$ algorithm is run by AA, It takes the security parameters λ as input, and outputs the system master key $SK_A \in \mathbb{Z}_q^*$ and public key $PK_A = g_1 SK_A$.

The AA (Attribute Authority) runs the $KeyGen(1^{\lambda})$ algorithm to obtain a public/private key pair (SK_A, PK_A), where $SK_A \in \mathbb{Z}_q^*$ and $PK_A = SK_A g_1$. The any member $u_i \in U (1 \leq i \leq n)$ chooses a random positive integer $s_{u_i} \in \mathbb{Z}_q^*$ and calculates $sk_{u_i} = H_1(id_{u_i}) s_{u_i}$ as its private key and the public key is $pk_{u_i} = g_1 sk_{u_i}$. The system parameters are $params = (PK_A, q, G_1, G_2, g_1, e, H_1, H_2, H_3)$.

D. GROUP MEMBER REGISTRATION

The group member registration of proposed protocol is depicted in Table 1, and the detailed steps are performed as follows:

(1) AA represents the attribute set $Attr = \{A_1, A_2, \ldots, A_j, \ldots, A_R\}$ as a Rth degree polynomial $f(x) = (x - A_R)(x - A_{R-1}) \ldots (x - A_1) = b_R x^R + b_{R-1} x^{R-1} + \ldots + b_0$.

(2) Each network terminal $u_i (1 \leq i \leq n)$ with the attribute set $attr_i = \{a_{i,1}, a_{i,2}, \ldots, a_{i,r}\}$ selects a random number $\lambda_i \in \mathbb{Z}_q^* (\lambda_i \neq 1, 0)$ and calculates $\{(\lambda_i g_1, a_{i,1}\lambda_i g_1, \ldots, a_{i,1}^R \lambda_i g_1), (\lambda_i g_1, a_{i,2}\lambda_i g_1, \ldots, a_{i,2}^R \lambda_i g_1), \ldots, (\lambda_i g_1, a_{i,r}\lambda_i g_1, \ldots, a_{i,r}^R \lambda_i g_1)\}$ and $\beta_i = (a_{i,1} + a_{i,2} + \ldots + a_{i,r}) sk_{u_i} \lambda_i g_1$. Then,

TABLE 1. Summary of GKAP-PPAA registration phase.

Terminals		AA (Attribute authority)
$u_i(1 \le i \le n)$ *Attribute set* : $attr_i = \{a_{i,1}, a_{i,2}, ..., a_{i,r}\}$		*Attribute set* : $Attr = \{A_1, A_2, ..., A_j, ..., A_R\}$ *Construct polynomial* : $f(x) = b_R x^R + b_{R-1}x^{R-1} + ... + b_0$
Selects a random number : $\lambda_i \in \mathbb{Z}_q^*(\lambda_i \ne 1, 0)$ *Calculates* : $\{(\lambda_i g_1, a_{i,1}\lambda_i g_1, ..., a_{i,1}^R \lambda_i g_1),$ $(\lambda_i g_1, a_{i,2}\lambda_i g_1, ..., a_{i,2}^R \lambda_i g_1), ...,$ $(\lambda_i g_1, a_{i,r}\lambda_i g_1, ..., a_{i,r}^R \lambda_i g_1)\}$ $\beta_i = (a_{i,1} + a_{i,2} + ... + a_{i,r})sk_{u_i}\lambda_i g_1$	$\{(\lambda_i g_1, a_{i,1}\lambda_i g_1, ..., a_{i,1}^R \lambda_i g_1),$ $(\lambda_i g_1, a_{i,2}\lambda_i g_1, ..., a_{i,2}^R \lambda_i g_1), ...,$ $(\lambda_i g_1, a_{i,r}\lambda_i g_1, ..., a_{i,r}^R \lambda_i g_1), \beta_i, pk_{u_i}\}$ →	*Calculates* : $\gamma_i = a_{i,1}\lambda_i g_1 + a_{i,2}\lambda_i g_1 + ... + a_{i,r}\lambda_i g_1$ *Verifies the equation* :$e(\beta_i, g_1) = e(\gamma_i, pk_{u_i})$ *Calculates* : $b_0\lambda_i g_1 + b_1 a_{i,1}\lambda_i g_1 + ... + b_R a_{i,1}^R \lambda_i g_1 = f(a_{i,1})\lambda_i g_1$ $b_0\lambda_i g_1 + b_1 a_{i,2}\lambda_i g_1 + ... + b_R a_{i,2}^R \lambda_i g_1 = f(a_{i,2})\lambda_i g_1, ...,$ $b_0\lambda_i g_1 + b_1 a_{i,r}\lambda_i g_1 + ... + b_R a_{i,r}^R \lambda_i g_1 = f(a_{i,r})\lambda_i g_1$ *Chooses* $t_{i,1}, t_{i,2}, ..., t_{i,r} \in \mathbb{Z}_q^*$ *Calculates* : $\{T_{i,0} = \lambda_i g_1, T_{i,1} = t_{i,1}T_{i,0}, T_{i,2} = t_{i,2}T_{i,0}, ...T_{i,r} = t_{i,r}T_{i,0}\}$ $\eta_{i,h} = SK_A(t_{i,1} + t_{i,2} + ... + t_{i,r})g_1$
Calculates : $K_{i,1} = \lambda_i^{-1}T_{i,1} = t_{i,1}g_1,$ $K_{i,2} = \lambda_i^{-1}T_{i,2} = t_{i,2}g_1, ...,$ $K_{i,r} = \lambda_i^{-1}T_{i,r} = t_{i,r}g_1$ *Obtains* : $\{K_{i,1}, K_{i,2}, ..., K_{i,r}, \eta_{i,h}, \gamma_i\}$	← $\{\gamma_i, \eta_{i,h}, T_{i,0}, T_{i,1}, T_{i,2}, ..., T_{i,r}\}$	$u_i(1 \le i \le n)$ *register successfully*

u_i sends $\{(\lambda_i g_1, a_{i,1}\lambda_i g_1, \ldots, a_{i,1}^R \lambda_i g_1), (\lambda_i g_1, a_{i,2}\lambda_i g_1, \ldots, a_{i,2}^R \lambda_i g_1), \ldots, (\lambda_i g_1, a_{i,r}\lambda_i g_1, \ldots, a_{i,r}^R \lambda_i g_1), \beta_i, pk_{u_i}\}$ to AA.

(3) After received the messages $\{(\lambda_i g_1, a_{i,1}\lambda_i g_1, \ldots, a_{i,1}^R \lambda_i g_1), (\lambda_i g_1, a_{i,2}\lambda_i g_1, \ldots, a_{i,2}^R \lambda_i g_1), \ldots, (\lambda_i g_1, a_{i,r}\lambda_i g_1, \ldots, a_{i,r}^R \lambda_i g_1), \beta_i, pk_{u_i}\}$, AA calculates $\gamma_i = a_{i,1}\lambda_i g_1 + a_{i,2}\lambda_i g_1 + \ldots + a_{i,r}\lambda_i g_1$ and verifies the identity of u_i by equation $e(\beta_i, g_1) = e(\gamma_i, pk_{u_i})$. If it holds, AA calculates $b_0\lambda_i g_1 + b_1 a_{i,1}\lambda_i g_1 + \ldots + b_R a_{i,1}^R \lambda_i g_1 = f(a_{i,1})\lambda_i g_1, b_0\lambda_i g_1 + b_1 a_{i,2}\lambda_i g_1 + \ldots + b_R a_{i,2}^R \lambda_i g_1 = f(a_{i,2})\lambda_i g_1, \ldots, b_0\lambda_i g_1 + b_1 a_{i,r}\lambda_i g_1 + \ldots + b_R a_{i,r}^R \lambda_i g_1 = f(a_{i,r})\lambda_i g_1$ respectively. If $f(a_{i,1})\lambda_i g_1 = 0, f(a_{i,2})\lambda_i g_1 = 0, \ldots, f(a_{i,r})\lambda_i g_1 = 0$, that means $f(a_{i,1}) = 0, f(a_{i,2}) = 0, \ldots, f(a_{i,r}) = 0$ and $attr_i \subseteq Attr$. Then, AA according to the number of attributes of $u_i(1 \le i \le n)$ chooses the same numbers of positive integer $t_{i,1}, t_{i,2}, \ldots, t_{i,r} \in \mathbb{Z}_q^*$. It calculates $\{T_{i,0} = \lambda_i g_1, T_{i,1} = t_{i,1}T_{i,0}, T_{i,2} = t_{i,2}T_{i,0}, \ldots T_{i,r} = t_{i,r}T_{i,0}\}$ (Note that for any two attributes $a_{i,k}$ and $a_{j,l}$ of different members of u_i and $u_j(i \ne j)$, if $k = l$, then $t_{i,k} = t_{j,l}$) . AA divides the permission level according to the number of their attributes and calculates the privilege grade $\eta_{i,h} = SK_A(t_{i,1} + t_{i,2} + \ldots + t_{i,r})g_1$. Then AA sends $\{\gamma_i, \eta_{i,h}, T_{i,0}, T_{i,1}, T_{i,2}, \ldots, T_{i,r}\}$ to the register network terminal u_i.

(4) After receiving the messages $\{\gamma_i, \eta_{i,h}, T_{i,0}, T_{i,1}, T_{i,2}, \ldots, T_{i,r}\}$ from AA, $u_i(1 \le i \le n)$ calculates $\varepsilon_i = \lambda_i^{-1}T_{i,1} + \lambda_i^{-1}T_{i,2} + \ldots + \lambda_i^{-1}T_{i,r} = (t_{i,1} + t_{i,2} + \ldots + t_{i,r})g_1$ and verifies the identity of AA by equation $e(\eta_{i,h}, g_1) = e(\varepsilon_i, PK_A)$. If it is hold, u_i computes $K_{i,1} = \lambda_i^{-1}T_{i,1} = t_{i,1}g_1, K_{i,2} = \lambda_i^{-1}T_{i,2} = t_{i,2}g_1, \ldots, K_{i,r} = \lambda_i^{-1}T_{i,r} = t_{i,r}g_1$ and obtains the attribute permission values $\{K_{i,1}, K_{i,2}, \ldots, K_{i,r}\}$ and the privilege level $\eta_{i,h}$.

With above steps, all the terminals $u_i(1 \le i \le n)$ register successfully. And AA can obtain the attribute information from all the registration terminals $u_i(1 \le i \le n)$. AA divides the permission levels of group members according to the number of attributes. Then AA can construct an information pool of registration terminals, as shown in Table 2, which can be used in different hierarchical terminals for group key agreement according to different attributes online phase.

E. GROUP KEY COMPUTING WITH DIFFERENT ATTRIBUTE PERMISSION

Members in the group may have different access authority and the information also has different security levels. Group members with the same authorization want to exchange internal information. The group information exchange sponsor may view the members with some specific attribute permission from information pool of registration terminals on the AA platform, then it can select the corresponding members with some specific attribute permission to form a group for group key agreement, thereby implementing the information exchange of the group. The detailed steps are performed as follows:

Any member $u_j(1 \le j \le n)$ with the attribute set $attr_j = \{a_{j,1}, a_{j,2}, \ldots, a_{j,r}\}$ and the privilege value $\eta_{j,h} = SK_A(t_{j,1} + t_{j,2} + \ldots + t_{j,r})g_1$ in the group wants to share the information

TABLE 2. Information pool of registration terminals.

$Terminals$	u_1	u_2	...	u_n
$Effectiveness$	yes	yes	...	yes
$Privilege\ grade$	$\eta_{1,h}$	$\eta_{2,h}$	...	$\eta_{n,h}$
$Public\ key$	pk_{u_1}	pk_{u_2}	...	pk_{u_n}
$Attribute\ privilege\ value$	$T_{i,0},...,T_{i,r}$	$T_{i,0},...,T_{i,r}$	...	$T_{i,0},...,T_{i,k}$
$Group\ public\ key\ parameter$	γ_1	γ_2	...	γ_n

with a subgroup member who has the same grade of authority or a higher grade of authority. It can select some members from the information pool on the AA platform to construct a subgroup when it wants to share secret information with them. The computational process of subgroup keys is as follows:

(1) The sponsor u_j who wants to share secret information with someone that have corresponding access authority. It searches for some attribute privilege values and corresponding privilege grade information from the information pool in Table 1. According to this information, it ensures which members can share secret information with it. For convenience, assuming it selects the members set is $\widetilde{U} = \{u_j, u_{j+1}, \ldots u_l\}(j < l)$.

(2) u_j gets the information $T_{k,1}, \ldots, T_{k,r}$ of each $u_k(j \leq k \leq l)$ from the information pool in Table 1 and computes $T_{pub} = \sum_{k=j}^{l} T_{k,0} = \sum_{k=j}^{l} \lambda_k g_1$ and $T_{pri} = \sum_{\tau=1}^{r}\sum_{k=j}^{l} T_{k,\tau} = \sum_{\tau=1}^{r} t_{k,\tau}(\lambda_j + \ldots + \lambda_l)g_1 = (t_{k,1}+\ldots+t_{k,r})(\lambda_j+\ldots+\lambda_l)g_1$.

(3) u_j selects $m_j \in \mathbb{Z}_p^*$ randomly, computes $p_{u_j} = m_j T_{pub}$, $M_j = m_j T_{pri}$, $w_{j,1} = H_2(K_{j,1})$, $w_{j,2} = H_2(K_{j,2}), \ldots, w_{j,r} = H_2(K_{j,r})$ and constructs a (r−1)-th degree polynomial $f(x) = m_j K_{j,r-1} x^{r-1} + \ldots + m_j K_{j,1} x + M_j$ according to the attribute permission values $\{K_{j,1}, K_{j,2}, ..., K_{j,r}\}$ that it kept before and $f(0) = M_j$, then it computes $f(w_{j,1}) = y_{j,1}, f(w_{j,2}) == y_{j,1}, f(w_{j,2}) = y_{j,2}, \ldots, f(w_{j,r}) = y_{j,r}$ and $\varphi_j = sk_{u_j}(y_{j,1} + y_{j,2} + \ldots + y_{j,r})$. u_j uses $PK_{g-u_j} = (p_{u_j}, \eta_{j,h})$ as group encryption key and $SK_{g-u_j} = M_j$ as group decryption key, where $\eta_{j,h}$ can be found in Table 2 . u_j broadcasts the messages $\{(y_{j,1}, y_{j,2}, ..., y_{j,r}), (p_{u_j}, \eta_{j,h}), \varphi_j\}$ to all members $\widetilde{U} = \{u_j, u_{j+1}, ...u_l\}(j < l)$ in the group.

(4) Each member u_k $(j \leq k \leq l, k \neq j)$ in the group who received the message $\{(y_{j,1}, y_{j,2}, \ldots, y_{j,r}), (p_{u_j}, \eta_{j,h}), \varphi_j\}$ from u_j, it computes $\phi_k = y_{j,1} + y_{j,2} + \ldots + y_{j,r}$ and verifies the identity of u_j by equation $e(\varphi_j, g_1) = e(\phi_k, pk_{u_j})$. If it holds, u_k compares its privilege value $\eta_{k,h}$ with the privilege value $\eta_{j,h}$. If it has the same grade of authority or higher grade of authority than $\eta_{j,h}$, it can find the correspond attribute permission values $\{K_{k,1}, K_{k,2}, \ldots, K_{k,r}\}$ (that means $\{K_{k,1} = K_{j,1}, K_{k,2} = K_{j,2}, ..., K_{k,r} = K_{j,r}\}$) and compute $w_{k,1} = H_2(K_{k,1})$, $w_{k,2} = H_2(K_{k,2})$, ..., $w_{k,r} = H_2(K_{k,r})$. u_k constructs a polynomial $f(x) = \sum_{\chi=1}^{r}\left(\prod_{1\leq\varpi\leq r,\varpi\neq\chi}\frac{x-w_{k,\varpi}}{w_{k,\chi}-w_{k,\varpi}}\right) y_{j,\chi}$ according to the information $\{(w_{k,1}, y_{j,1}), (w_{k,2}, y_{j,2}), \ldots, (w_{k,r}, y_{j,r})\}$ and Lagrange theorem and computes the constant term $M_k = f(0) = \sum_{\chi=1}^{r}\left(\prod_{1\leq\varpi\leq r,\varpi\neq\chi}\frac{-w_{k,\varpi}}{w_{k,\chi}-w_{k,\varpi}}\right) y_{j,\chi} = M_j$ as its group decryption key. u_k can also obtain the group encryption key $PK_{g-u_k} = (p_{u_k}, \eta_{k,h}) = (p_{u_j}, \eta_{j,h})$ from the broadcasted messages $\{(y_{j,1}, y_{j,2}, \ldots, y_{j,r}), (p_{u_j}, \eta_{j,h})\}$ by u_j.

All the members $u_k(j \leq k \leq l)$ in the group can compute the same group decryption key M_k and the group encryption key $(p_{u_k}, \eta_{k,h})$ if they have the same grade of authority or higher grade of authority than $\eta_{j,h}$ of the group key agreement sponsor.

F. GROUP KEYS CORRECTNESS SELF-CERTIFIED

All the group members $u_k(j \leq k \leq l)$ calculated group keys, they needn't broadcast the hash values of the group keys to other group members and compare with hash values of the group the other members broadcast to verify whether the correctness of the group keys it computed. They can verify whether the equation $e(p_{u_k}, \eta_{k,h}) = e(M_k, PK_A)$ holds to check whether the correctness of the computed group keys.

G. GROUP SECURITY INFORMATION EXCHANGE

Instance: For any plaintext message $m \in \mathcal{M}^*$ ($\mathcal{M}^*$: plaintext space), each u_j with the group encryption key $PK_{g-u_j} = (p_{u_j}, \eta_{j,h})$ and group decryption key M_j operates as the follows:

Encryption: u_j chooses a random number $\varsigma \in \mathbb{Z}_p^*$, and calculates $H_3(e(p_{u_j}, \eta_{j,h}))^{\varsigma}, \upsilon = \varsigma PK_A, \overline{V} = m \oplus H_3((e(p_{u_j}, \eta_{j,h})^{\varsigma})$, Then it broadcasts ciphertext $c = (\upsilon, \overline{V})$.

Decryption: After receiving a ciphertext $c = (\upsilon, \overline{V})$, anyone $u_k(j \leq k \leq l)$ in the same group can calculate $m = \overline{V} \oplus H_3(e(\upsilon, M_k))$ with a valid M_k.

III. CORRECTNESS AND SECURITY ANALYSIS

In this section, some performances of the proposed GKAP-PPAA protocol are discussed. Firstly, the correctness of our proposed protocol is shown. Secondly, the security analysis of GKAP-PPAA protocol is given. Finally, the efficiency analysis of GKAP-PPAA protocol is testified. In order to validate performances claim of proposed protocol, the following theorems are proven.

Theorem 1 (Contributiveness) : By running the proposed GKAP-PPAA protocol, contributory group keys can be established by all participators of GKAP-PPAA protocol . Each participator may confirm that its contribution was included in the group encryption key and group decryption key.

Proof: Since each participator $u_k(j \le k \le l)$ in the group computed the group encryption key is $PK_{g-u_k} = (p_{u_k}, \eta_{k,h})$ and the parameter $p_{u_k} = m_j T_{pub}$, $T_{pub} = \sum_{k=j}^{l} T_{k,0} = \sum_{k=j}^{l} \lambda_k g_1$, so the $PK_{g-u_k} = (p_{u_k}, \eta_{k,h}) = (m_j \sum_{k=j}^{l} \lambda_k g_1, \eta_{k,h}) = \{m_j(\lambda_j + \lambda_{j+1} + \ldots + \lambda_l)g_1, \eta_{k,h}\}$, which means each parameter λ_k of u_k is included in the group encryption key PK_{g-u_k}. So the contribution of each participator u_k is included in the group encryption key.

In the same way, the group decryption key is $SK_{g-u_k} = m_j T_{pri}$ and the parameter is $T_{pri} = \sum_{\tau=1}^{r} \sum_{k=j}^{l} T_{k,\tau} = (t_{k,1} + \ldots + t_{k,r})(\lambda_j + \ldots + \lambda_l)g_1$, so M_k includes each participator u_k's parameter λ_k. Therefore, the contribution of each participator u_k also was included in the group decryption key M_k.

For above, the contribution of each participator u_k in GKAP-PPAA was included in the group encryption key and group decryption key.

A. CORRECTNESS

The proof of the correctness of the GKAP-PPAA is shown in the following theorems.

Theorem 2: If they have the same grade of authority or higher grade of authority than sponsor u_j demanded, each $u_k(j \le k \le l)$ can calculate an identical group decryption key SK_{g-u_k} and group encryption key PK_{g-u_k} in this protocol.

Proof: We assume that the attribute set of u_j is set $attr_j = \{a_{j,1}, a_{j,2}, \ldots, a_{j,r}\}$ and the correspond attribute permission value set of u_j is $V_{u_j} = \{K_{j,1}, K_{j,2}, ..., K_{j,r}\}$. The attribute set of $u_k(j \le k \le l)$ in the group is $attr_k = \{a_{k,1}, a_{k,2}, ..., a_{k,\omega}\}$ and the correspond attribute permission value set of $u_k(j \le k \le l)$ is $V_{u_k} = \{K_{k,1}, K_{k,2}, ..., K_{i,\omega}\}$.

If the participator $u_k(j \le k \le l)$ in the group has the same grade of authority or higher grade of authority than sponsor u_j, it means u_k has the same number of attribute permission values or more attribute permission values than u_j, that is $V_{u_j} \subseteq V_{u_k}$.

u_j computes $w_{j,1} = H_2(K_{j,1}), w_{j,2} = H_2(K_{j,2}), \ldots, w_{j,r} = H_2(K_{j,r})$ and constructs a r-th degree polynomial $f(x) = m_j K_{j,r-1} g_1 x^{r-1} + ... + m_j K_{j,1} g_1 x + M_j$ according to the attribute permission values $\{K_{j,1}, K_{j,2}, ..., K_{j,r}\}$. Since $V_{u_j} \subseteq V_{u_k}$ and $V_{u_k} = \{K_{k,1}, K_{k,2}, ..., K_{i,\omega}\}$ is ordered, u_k can also computes the $w_{k,1} = H_2(K_{k,1}), w_{k,2} = H_2(K_{k,2}), ..., w_{k,r} = H_2(K_{k,r})$ and there is $w_{k,1} = w_{j,1}, w_{k,2} = w_{j,2}, ..., w_{k,r} = w_{j,r}$.

u_k received the values $\{f(w_{j,1}) = y_{j,1}, f(w_{j,2}) = y_{j,2}, \ldots, f(w_{j,r}) = y_{j,r}\}$ from u_j, it can construct number pairs $\{(y_{j,1}, w_{k,1}), (y_{j,2}, w_{k,2}), \ldots, (y_{j,r}, w_{k,r})\}$ and restore r-th degree polynomial $f(x) = m_j K_{j,r-1} g_1 x^{r-1} + \ldots + m_j K_{j,1} g_1 x + M_j$ according to the Lagrangian interpolation formula.

Similarly, all the participator $u_k(j \le k \le l)$ in the group can receive an identical group encryption key $(p_{u_j}, \eta_{j,h})$ from u_j.

Theorem 3: any group members $u_k(j \le k \le l)$ can decrypt the ciphertext information that encrypted by member $u_\tau(1 \le \tau \le n)$ using the group encryption key $(p_{u_k}, \eta_{k,h})$ with its group decryption key SK_{g-u_k}.

Proof: Since $T_{pub} = \sum_{k=j}^{l} T_{k,0} = \sum_{k=j}^{l} \lambda_k g_1$, $T_{pri} = \sum_{\tau=1}^{r} \sum_{k=j}^{l} T_{k,\tau} = (t_{k,1} + \ldots + t_{k,r})(\lambda_j + ... + \lambda_l)g_1$, $\eta_{k,h} = SK_A(t_{k,1} + t_{k,2} + ... + t_{k,r})g_1$, $p_{u_k} = m_j T_{pub}$ and $SK_{g-u_k} = m_j T_{pri}$, there are $p_{u_k} = m_j T_{pub} = m_j(\lambda_j + ... + \lambda_l)g_1$ and $SK_{g-u_k} = m_j(t_{k,1} + ... + t_{k,r})(\lambda_j + ... + \lambda_l)g_1$.

For the above calculation, and the properties of the bilinear pairings, any ciphertext information $\overline{V} = m \oplus H_3((e(p_{u_k}, \eta_{k,h})^{\varsigma})$ encrypted by member u_τ using the group encryption key $(p_{u_k}, \eta_{k,h})$, where $\varsigma \in \mathbb{Z}_p^*$, $\upsilon = \varsigma PK_A$. The corresponding plaintext information m can be obtained by $m = \overline{V} \oplus H_3(e(\upsilon, SK_{g-u_k}))$ using its group decryption key SK_{g-u_k}.

B. SECURITY ANALYSIS

Theorem 4: The proposed GKAP-PPAA protocol is secure against passive adversary: A group key agreement protocol is secure against a passive adversary if a passive attacker is unable to obtain information about the established session key by eavesdropping on messages transmitted over the broadcast channel. To prove that is so, we need a well-known security assumption. Here we adopt the DLP problem and DBDH problem assumption to prove that the new protocol is secure against a passive adversary. Several works have already demonstrated the security and the variants of the decision bilinear Diffie-Hellman problem.

Assumption 1 (DLP Problem and DBDH Problem): Let G_1 be an additive group and G_2 be a multiplicative cyclic group, Both of the two groups have the same large prime order q, where $q \ge 2^{\ell} + 1$, and ℓ is a security parameter, the discrete logarithm over G_1 and G_2 is difficult, $G_1 = \langle g_1 \rangle$ is generated by g_1, G_1 and G_2 are a pair of bilinear group, $e : G_1 \times G_1 \to G_2$ is a calculable bilinear mapping.

Discrete Logarithm problem (DLP). For given $\psi = ag_1$, $\zeta = bg_1$, and $\sigma = abg_1$, where $b, a \in \mathbb{Z}_q^*$ and $\psi, \zeta, \sigma \in G_1$, $a < q$. If a and ζ are given, it is easy to calculate σ. But if ζ and σ are given, it will be difficult to calculate a.

Decisional Bilinear Diffe-Hellman (DBDH) Problem: Suppose the following two triples $(g_1, g_2, ag_1, bg_1, cg_1, e(g_1, g_1)^{abc})$ and $(g_1, g_2, ag_1, bg_1, cg_1, \pi)$, for any $a, b, c \in \mathbb{Z}_q^*$, $g_1 \in G_1$, $g_2 \in G_2$ and $\pi \in G_2$, are computationally indistinguishable. In other words, there is no efficient algorithm $\mathcal{A}$

that satisfies

$$|\Pr[\mathcal{A}(abg_1, ag_1, bg_1, e) = 1] - \Pr[\mathcal{A}(abg_1, ag_1, \pi, e) = 1]| \geq \frac{1}{Q(|2^k|)}.$$

for any polynomial Q, where the probability is over the random choice of a, b, c and π.

Lemma 1: Under the random oracle model, if computing the DLP is hard, any malicious adversary $\mathcal{C}$ without the same grade of authority or higher grade of authority than the group key agreement sponsor demanded will be unable to obtain the group decryption key SK_{g-u_j}.

Proof: $\mathcal{C}$ only has two ways to solve the group decryption key SK_{g-u_j}.

The first method is to solve the polynomial: if $\mathcal{C}$ without the same grade of authority or higher grade of authority than that of group key agreement sponsor u_j demanded, that means $\mathcal{C}$ does not have enough attributes and the corresponding attribute permission values $\{K_{j,1}, K_{j,2}, \ldots, K_{j,r}\}$. Although $\mathcal{C}$ can get the messages $\{(y_{j,1}, y_{j,2}, ..., y_{j,r}), (p_{u_j}, \eta_{j,h}), \varphi_j\}$ broadcast by u_j over the open network, it does not have the corresponding attribute permission values $\{K_{j,1}, K_{j,2}, ..., K_{j,r}\}$ and cannot calculate the corresponding polynomial parameters $w_{j,1} = H_2(K_{j,1}), w_{j,2} = H_2(K_{j,2}), ..., w_{j,r} = H_2(K_{j,r})$, and it can't construct the construct the corresponding pairs $\{(w_{j,1}, y_{j,1}), (w_{j,2}, y_{j,2}), \ldots, (w_{j,r}, y_{j,r})\}$. According to Lagrange interpolation formula, $\mathcal{C}$ cannot recover polynomial $f(x) = \sum_{\chi=1}^{r} \left(\prod_{1 \leq \varpi \leq r, \varpi \neq \chi} \frac{x - w_{j,\varpi}}{w_{j,\chi} - w_{j,\varpi}} \right) y_{j,\chi}$ and cannot calculate the group decryption key $SK_{g-u_j} = f(0) = \sum_{\chi=1}^{r} \left(\prod_{1 \leq \varpi \leq r, \varpi \neq \chi} \frac{-w_{j,\varpi}}{w_{j,\chi} - w_{j,\varpi}} \right) y_{j,\chi} = M_j$.

The second way is to compute the SK_{g-u_j} with public information : $\mathcal{C}$ can get the messages $\{(y_{j,1}, y_{j,2}, \ldots, y_{j,r}), (p_{u_j}, \eta_{j,h}), \varphi_j\}$ broadcast by u_j over the open network. The parameters of group encryption key $p_{u_j} = m_j T_{pub} = m_j \sum_{k=j}^{l} \lambda_k g_1$ and $\eta_{j,h} = SK_A(t_{j,1} + t_{j,2} + ... + t_{j,r})g_1 = (t_{j,1} + t_{j,2} + ... + t_{j,r})PK_A$. Since $SK_{g-u_j} = m_j T_{pri} = (t_{j,1} + ... + t_{j,r}) m_j \sum_{k=j}^{l} \lambda_k g_1$, if $\mathcal{C}$ wants to calculate the group decryption key SK_{g-u_j}, it must compute $(t_{j,1} + t_{j,2} + ... + t_{j,r})$ from $\eta_{j,h}$ and compute $(t_{j,1} + t_{j,2} + ... + t_{j,r}).p_{u_j} = (t_{k,1} + ... + (t_{k,1} + ... + t_{k,r}) m_j \sum_{k=j}^{l} \lambda_k g_1$ to get SK_{g-u_j}. We assume that $\mathcal{C}$ can compute the value $(t_{j,1} + t_{j,2} + ... + t_{j,r})$ from $\eta_{j,h}$ by an efficient algorithm $\mathcal{A}$. Then, $\mathcal{C}$ can construct an efficient algorithm $\mathcal{A}'$ to uses $\sigma = abg_1 = \eta_{j,h}$ and $\zeta = bg_1 = SK_A g_1$ as input, and output $a = (t_{j,1} + t_{j,2} + ... + t_{j,r})$. So it can use $\mathcal{A}$ to construct an efficient algorithm $\mathcal{A}'$ to solve the DLP problem, which is a contradiction for the hard of DLP problem.

Lemma 2: Under the decision bilinear Diffie-Hellman assumption: for any $a, b, c \in \mathbb{Z}_q^*$, $g_1 \in G_1$, $g_2 \in G_2$ and $\pi \in G_2$, the two triples $(g_1, g_2, ag_1, bg_1, cg_1, e(g_1, g_1)^{abc})$ and $(g_1, g_2, ag_1, bg_1, cg_1, \pi)$ are computationally indistinguishable. Even if adversary $\mathcal{C}$ obtains relevant information $PK_{g-u_j} = (p_{u_j}, \eta_{j,h})$ and $c = (\upsilon, \overline{V})$ through the open network, it cannot obtain the plaintext information $m = \overline{V} \oplus H_3(e(\upsilon, M_j))$ without the group key $SK_{g-u_j} = M_j$.

Proof: Since $p_{u_j} = m_j T_{pub} = m_j \sum_{k=j}^{l} \lambda_k g_1$, $\upsilon = \varsigma PK_A$, $\eta_{j,h} = (t_{j,1} + t_{j,2} + \ldots + t_{j,r})PK_A$, without loss of generality, let $\mathcal{R} = PK_A = SK_A g_1$. Then, $\mathcal{C}$ constructs an algorithm $\mathcal{A}'$, it randomly selects $(\rho_1, \rho_2, \cdots, \rho_r)$ from $\mathbb{Z}_q^*$ and calculates values are as follows:

$$f_1 = \rho_1 p_{u_j} = \rho_1 m_j \sum_{k=j}^{l} \lambda_k g_1;$$

$$f_2 = \rho_2 p_{u_j} = \rho_2 m_j \sum_{k=j}^{l} \lambda_k g_1;$$

$$\vdots$$

$$f_r = \rho_r p_{u_j} = \rho_r m_j \sum_{k=j}^{l} \lambda_k g_1.$$

Therefore, the algorithm $\mathcal{A}'$ constructs all message pair (υ, f_i), for $1 \leq j \leq r$ and computes $\mathcal{F} = f_1 + f_2 + \ldots + f_r$ and $\pi = e(\upsilon, \mathcal{F})$. If $\mathcal{A}'$ can compute $m = \overline{V} \oplus H_3(\pi)$ and get the plaintext message m. It is obvious that $SK_{g-u_j} = \mathcal{F}$ based on property of bilinear map $\pi = e(\upsilon, \mathcal{F}) = e(\upsilon, SK_{g-u_j})$ holds. That is, we can construct another algorithm $\mathcal{A}$ called $\mathcal{A}'$ to efficiently distinguish $(g_1, g_2, ag_1, bg_1, cg_1, e(g_1, g_1)^{abc})$ and $(g_1, g_2, ag_1, bg_1, cg_1, \pi)$, where $\upsilon = \varsigma PK_A = ag_1$, $\eta_{j,h} = (t_{j,1} + t_{j,2} + \ldots + t_{j,r})PK_A = bg_1$, $p_{u_j} = m_j T_{pub} = m_j \sum_{k=j}^{l} \lambda_k g_1 = cg_1$, $e(g_1, g_1)^{abc} = e(g_1, g_1)^{\varsigma SK_A \cdot (t_{j,1} + t_{j,2} + ... + t_{j,r}) \cdot SK_A \cdot m_j \sum_{k=j}^{l} \lambda_k}$ and $\pi = e(\upsilon, \mathcal{F}) = e(\upsilon, \mathcal{F})^{\varsigma SK_A \cdot (\rho_1 + \rho_2 + ... + \rho_r) \cdot m_j \sum_{k=j}^{l} \lambda_k}$, which is a contradiction for the DBDH problem assumption. Thus, the proposed protocol is secure against passive attacks under the DBDH problem assumption.

Theorem 5: Under the random oracle model, the proposed protocol is secure against an impersonator's attack. Any illegal member u_i cannot pretend to be a key agreement sponsor u_j to initiate an invalid group key agreement.

Proof: we know that only one legal participant u_j with secret key sk_{u_j} can generate a valid signature $\varphi_j = sk_{u_j}(y_{j,1} + y_{j,2} + \ldots + y_{j,r})$. Since impersonator u_i does not know u_j's secret key sk_{u_j}, it cannot counterfeit the valid signature φ_j. If the impersonator u_i attempts to disrupt the establishment of a group key among honest participants, he will be detected by verifying the equation $e(\varphi_j, g_1) = e(\phi_i, pk_{u_j})$. Therefore, the proposed protocol is secure against impersonator attack.

IV. EFFICIENCY ANALYSIS

During the process of designing protocol, except security, the computational time, the computational complexity and communication costs are important performance measures of the group key agreement. In this paper, we compared and analyzed the literature that can be quantified in recent years. We compare the proposed protocol with the related works [26], [37], [54] in communication costs, computation costs and time cost. Below are the few notations and data that are going to be used in comparison [34].

- T_{inv}: Execution time for calculating the modular inverse operation, $T_{inv} \approx 0.174ms$.
- T_{mul}: Execution time for the multiplication of two numbers, $T_{mul} \approx 0.015ms$.
- T_{exp}: Execution time for Exponentiation, $T_{exp} \approx 3.886ms$.
- T_{pa-ecc}: Execution time for calculating the elliptic curve point addition, $T_{pa-ecc} \approx 0.0018ms$.
- T_{sm-ecc}: Execution time for calculating the elliptic curve point multiplication, $T_{sm-ecc} \approx 0.442ms$.
- T_h: Execution time for the general hash operation, $T_h \approx 0.0001ms$.
- T_{bp}: Execution time for the bilinear pairing operation, $T_{bp} \approx 4.211ms$.
- T_{mtp}: Execution time of the map-to-point hash operation, $T_{mtp} \approx 4.406ms$.
- T_{pa-bp}: Execution time of the point addition related to bilinear pairing, $T_{pa-bp} \approx 0.071ms$.
- T_{sm-bp}: Execution time of the multiplication of scalar with the point based on bilinear pairing, $T_{sm-bp} \approx 1.709ms$.

Table 3 lists the comparison and analysis between the GKAP-PPAA protocol and other three group-key agreement protocols in the calculation of complexity, communication load and time cost of group key agreement initiator. We assume that there are n members to participate group key agreement and the group key agreement initiator requires members with at least r attributes to participate in the group key negotiation in the GKAP-PPAA, where r is very small relative to n.

In reference [26] scheme, the Parameter calculation phase, there needs $(n+2)T_{mul} + nT_h$, the computing of group encryption key phase, there needs $(n-1)T_{bp} + nT_{sm-bp} + nT_{pa-bp}$, the computing of group decryption key phase, there needs nT_{pa-ecc}, the total computation cost is $(n-1)T_{bp}+(n+2)T_{mul}+nT_{sm-bp}+nT_{pa-bp}+nT_{pa-ecc}+nT_h$. Communication cost: message of sent is $(n+3)|G|$, message of received is $(n+3)|G|$.

In reference [46] scheme, the Parameter calculation phase there needs $nT_{exp}+nT_{mul}$. The computing of group encryption key phase there needs $3nT_{bp}+2nT_{sm-bp}+nT_{sm-ecc}$. The computing of group decryption key phase, there needs nT_{sm-ecc}, the total computation cost is $3nT_{bp}+nT_{exp} + 2nT_{sm-bp} + 2nT_{sm-ecc} + nT_{mul}$. Communication cost: message of sent is $(n+3)|G|$, message of received is $(n+3)|G|$.

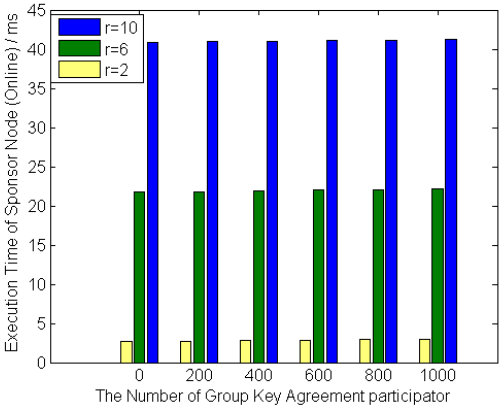


FIGURE 1. Online execution time of sponsor node in GKAP-PPAA.

GKAP-PPAA scheme, the Parameter calculation phase, there needs $(2n+r)T_{pa-ecc} + T_{sm-ecc}$. The computing of group encryption key phase, there needs $1T_{sm-ecc}$. Polynomial construction phase, there needs $(r-2)T_{exp} + 2(r-1)T_{sm-ecc} + (r-1)T_{pa-ecc} + rT_h$. The computing of group decryption key phase, there needs $1T_{sm-ecc}$. The Signature phase, there needs $1T_{sm-ecc}+rT_{pa-ecc}$. The total computation cost is $(r-2)T_{exp}+2(r+1)T_{sm-ecc}+(2n+3r-1)T_{pa-ecc}+rT_h$. Communication cost: message of sent is $(r+3)|G|$, message of received is $(r+3)|G|$.

From Table 3, GKAP-PPAA has the lowest computational complexity, Lv et al.'s protocol [37] have the high computational complexity, Zhang et al.'s protocol [26] and Wei et al.'protocol [46] have the highest computational complexity. In communication, Wei et al.'protocol [46] has the highest communication complexity. Zhang et al.'s protocol [26] and, Lv et al.'s protocol [37] with the similar of communication complexity, have lower communication complexity. GKAP-PPAA has the lowest communication complexity.

For convenience and without loss of generality, we do time cost analysis involves the ordinary node of group key agreement. Based on the data provided by Table 3, we analyzed the time consumption of sponsor as the size of the group key agreement changes when $r = 2, r = 6, r = 10$ respectively and compared the GKAP-PPAA with other three protocols in time cost of ordinary node when $r = 10$. The results are show as Fig. 2 and Fig. 3 respectively.

From Fig.1, when the size of the group key agreement member changes in the GKAP-PPAA, the calculation time of the group key initiator changes little.

From figure 2, for the ordinary nodes, GKAP-PPAA has the lowest time cost of ordinary nodes when the number of group key agreement members is less than 20, followed by Lv et al.'s protocol [37] and Zhang et al.'s protocol [26]. Wei et al.'protocol [46] has the highest time cost.

When these protocols are used in a wireless network environment, the communication consumption of the protocol should be taken into account. In this section, we perform the total energy consumption cost analysis of performing GKA using the data provided in Wei et al. [46]. As for

TABLE 3. Complexity analysis of the four protocols.

	Zhang et al.'s protocol [26]	Lv et al.'s protocol [37]	Wei et al.'protocol [46]	GKAP-PPAA
Computational complexity of each ordinary node (online)	$(2n+3)T_{bp}+3nT_{mul}+2nT_h$	$(n-1)T_{bp}+nT_{sm-bp}+nT_{pa-bp}+nT_{pa-ecc}$	$3(n+1)T_{bp}+(2n+1)T_{sm-bp}+2nT_{sm-ecc}$	$2T_{bp}+(r^2-1)T_{pa-ecc}+r(r+1)T_{sm-ecc}+rT_h$
Computational complexity required by the sponsor node	$(2n+3)T_{bp}+(n+1)T_{exp}+4nT_{mul}+3nT_h$	$(n-1)T_{bp}+(n+2)T_{mul}+nT_{sm-bp}+nT_{pa-bp}+nT_{pa-ecc}+nT_h$	$3nT_{bp}+nT_{exp}+2nT_{sm-bp}+2nT_{sm-ecc}+nT_{mul}$	$(r-2)T_{exp}+2(r+1)T_{sm-ecc}+(2n+3r-1)T_{pa-ecc}+rT_h$
The number of message sent	$(n+2)\,\|G\|$	$(n+3)\,\|G\|$	$(n+3)\,\|G\|$	$(r+3)\,\|G\|$
The number of message received	$(3n-1)\,\|G\|$	$(n+3)\,\|G\|$	$5(n-1)\,\|G\|$	$(r+3)\,\|G\|$

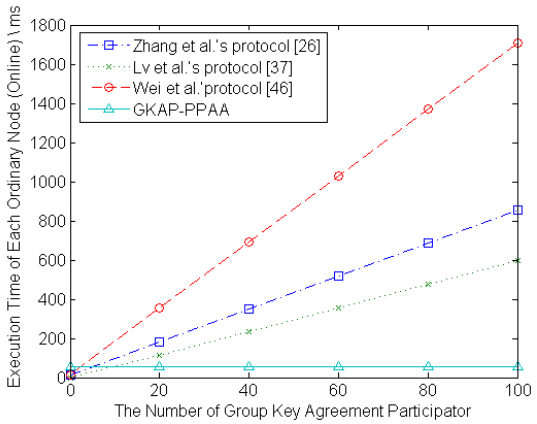


FIGURE 2. Online execution time of ordinary node in the four protocols.

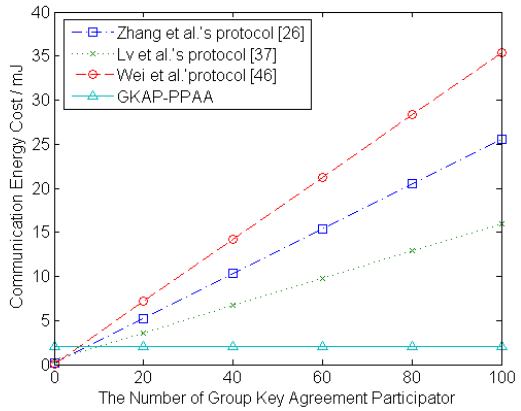


FIGURE 3. Communication energy cost of the four protocols.

the communication energy cost, an IEEE 802.11 Spectrum24 WLAN card consumes 0.00066 mJ for the transmission of 1 bit and 0.00031 mJ for the reception of 1 bit. The abovementioned energy costs will be used for the communication energy analysis of the four GKA protocols. To compute the communication cost, we need to know the size of the information exchange. We assume that the secure key length is 160b of the elliptic curve cryptography. All these four protocols adopt the elliptic curve cryptography, so their key length is 160b. Let the length of the information exchange be 160b, and the communication consumption is shown in Fig. 3.

The communication consumption of the examined Protocols are depicted in Fig.3. Lv et al.'s protocol [37] has the worst performance, followed by Zhang et al.'s protocol [26] and Lv et al.'s protocol [37]. GKAP-PPAA is very efficient in terms of communication When the number of group key agreement members exceeds 20.

V. CONCLUSION

Group key agreement is one of the key technologies to ensure the secure exchange of information among groups. This paper proposes an asymmetric group key agreement protocol based on attribute authentication and personal privacy protection. The protocol adopts attribute-based identity authentication technology. In the process of attribute authentication, the attribute is hidden by polynomial calculation to achieve the purpose of attribute-based hidden identity authentication, which ensures that personally identifiable information is not leaked, and that personal attribute information is protected from disclosure. The protocol also uses threshold function technology to implement hierarchical group information security exchange, that is, group information with different sensitivities can only be shared among group members with corresponding rights. The protocol ensures that the computing and communication as simple and small as possible. The security of this protocol is based on the hardness of BDLP and DBDH problems. The GKAP-PPAA is also analyzed to be secure, efficient, which is suitable in multilevel and stereoscopic space security information exchange in complex network environment.

REFERENCES

[1] K. Sharma and B. B. Gupta, "Attack in smartphone Wi-Fi access channel: State of the art, current issues, and challenges," in *Next-Generation Networks* (Advances in Intelligent Systems and Computing), vol. 638. Singapore: Springer, 2018, pp. 555–561.

[2] K. Sharma and B. B. Gupta, "Taxonomy of distributed denial of service (DDoS) attacks and defense mechanisms in present era of smartphone devices," *Int. J. E-Services Mobile Appl.*, vol. 10, no. 2, pp. 58–74, 2018.

[3] W. Diffie and M. E. Hellman, "New directions in cryptography," *IEEE Trans. Inf. Theory*, vol. IT-22, no. 6, pp. 644–654, Nov. 1976.

[4] I. Ingemarsson, D. Tang, and C. Wong, "A conference key distribution system," *IEEE Trans. Inf. Theory*, vol. IT-28, no. 5, pp. 714–720, Sep. 1982.

[5] Q. K. Zhang, Y. Li, D. Song, and Y. Tan, "Alliance-authentication protocol in clouds computing environment," *China Commun.*, vol. 9, no. 7, pp. 42–54, 2012.

[6] X. Zhang, C. Liang, Q. Zhang, Y. Li, J. Zheng, and Y.-A. Tan, "Building covert timing channels by packet rearrangement over mobile networks," *Inf. Sci.*, vols. 445–446, pp. 66–78, Jun. 2018.

[7] Y.-A. Tan, Y. Xue, C. Ling, J. Zheng, Q. Zhang, J. Zheng, and Y. Li, "A root privilege management scheme with revocable authorization for Android devices," *J. Netw. Comput. Appl.*, vol. 107, pp. 69–82, Apr. 2018.

[8] X. Zhang, Y.-A. Tan, C. Liang, Y. Li, and J. Li, "A covert channel over VoLTE via adjusting silence periods," *IEEE Access*, vol. 6, pp. 9292–9302, 2018.

[9] Q. Zhang, Y. Li, Q. Zhang, J. Yuan, R. Wang, Y. Gan, and Y. Tan, "A self-certified cross-cluster asymmetric group key agreement for wireless sensor networks," *Chin. J. Electron.*, vol. 28, no. 2, pp. 280–287, 2019.

[10] C. Liang, X. Wang, X. Zhang, Y. Zhang, K. Sharif, and Y.-A. Tan, "A payload-dependent packet rearranging covert channel for mobile VoIP traffic," *Inf. Sci.*, vol. 465, pp. 162–173, Oct. 2018.

[11] Z. Guan, Y. Zhang, L. Zhu, L. Wu, and S. Yu, "EFFECT: An efficient flexible privacy-preserving data aggregation scheme with authentication in smart grid," *Sci. China Inf. Sci.*, vol. 62, no. 3, pp. 1–14, Mar. 2019.

[12] S. Bala, G. Sharma, H. Bansal, and T. Bhatia, "On the security of authenticated group key agreement protocols," *Scalable Comput., Pract. Exper.*, vol. 20, no. 1, pp. 93–99, 2019.

[13] X. Gao, Y.-A. Tan, H. Jiang, Q. Zhang, and X. Kuang, "Boosting targeted black-box attacks via ensemble substitute training and linear augmentation," *Appl. Sci.*, vol. 9, no. 11, p. 2286, 2019.

[14] X. Du, Y. Xiao, M. Guizani, and H.-H. Chen, "An effective key management scheme for heterogeneous sensor networks," *Ad Hoc Netw.*, vol. 5, no. 1, pp. 24–34, 2007.

[15] Q. Zhang, Y. Gan, L. Liu, X. Wang, X. Luo, and Y. Li, "An authenticated asymmetric group key agreement based on attribute encryption," *J. Netw. Comput. Appl.*, vol. 123, pp. 1–10, Dec. 2018.

[16] Y.-A. Tan, X. Zhang, K. Sharif, C. Liang, Q. Zhang, and Y. Li, "Covert timing channels for IoT over mobile networks," *IEEE Wireless Commun.*, vol. 25, no. 6, pp. 38–44, Dec. 2018.

[17] Q. Zhang, H. Gong, X. Zhang, C. Liang, and Y.-A. Tan, "A sensitive network jitter measurement for covert timing channels over interactive traffic," *Multimedia Tools Appl.*, vol. 78, no. 3, pp. 3493–3509, 2019.

[18] L. Liu, Y. Wang, J. Zhang, and Q. Yang, "A secure and efficient group key agreement scheme for VANET," *Sensors*, vol. 19, no. 3, pp. 1–14, 2019.

[19] J. Zheng, Y. Tan, X. Zhang, Q. Zhang, Q. Zhang, and C. Zhang, "Multi-domain lightweight asymmetric group key agreement," *Chin. J. Electron.*, vol. 27, no. 5, pp. 1085–1091, Sep. 2018.

[20] Q. Zhang, J. Yuan, G. Guo, Y. Gan, and J. Zhang, "An authentication key establish protocol for WSNs based on combined key," *Wireless Pers. Commun.*, vol. 99, no. 1, pp. 95–110, 2017.

[21] Y. Li, S. Yao, K. Yang, Y.-A. Tan, and Q. Zhang, "A high-imperceptibility and histogram-shifting data hiding scheme for JPEG images," *IEEE Access*, vol. 7, pp. 73573–73582, 2019.

[22] T.-W. Lin and C.-L. Hsu, "Anonymous group key agreement protocol for multi-server and mobile environments based on Chebyshev chaotic maps," *J. Supercomputing*, vol. 74, no. 9, pp. 4521–4541, 2018.

[23] J. Zheng, Y.-A. Tan, Q. Zhang, X. Zhang, L. Zhu, and Q. Zhang, "Cross-cluster asymmetric group key agreement for wireless sensor networks," *Sci. China-Inf. Sci.*, vol. 61, no. 4, 2018, Art. no. 048103.

[24] Q. Zhang, X. Wang, J. Yuan, L. Liu, R. Wang, H. Huang, and Y. Li, "A hierarchical group key agreement protocol using orientable attributes for cloud computing," *Inf. Sci.*, vol. 480, pp. 55–69, Apr. 2019.

[25] Z. Qikun, G. Yong, Z. Quanxin, W. Ruifang, and T. Yu-An, "A dynamic and cross-domain authentication asymmetric group key agreement in telemedicine application," *IEEE Access*, vol. 6, pp. 24064–24074, 2018.

[26] L. Zhang, Q. Wu, B. Qin, and J. Domingo-Ferrer, "Provably secure one-round identity-based authenticated asymmetric group key agreement protocol," *Inf. Sci.*, vol. 181, pp. 4318–4329, Oct. 2011.

[27] Z. Guan, Y. Zhang, L. Wu, J. Wu, J. Li, Y. Ma, and J. Hud, "APPA: An anonymous and privacy preserving data aggregation scheme for fog-enhanced IoT," *J. Netw. Comput. Appl.*, vol. 125, pp. 82–92, Jan. 2019.

[28] J. Cui, X. Tao, J. Zhang, Y. Xu, and H. Zhong, "HCPA-GKA: A hash function-based conditional privacy-preserving authentication and group-key agreement scheme for VANETs," *Veh. Commun.*, vol. 14, pp. 15–25, Oct. 2018.

[29] X. Du, M. Guizani, Y. Xiao, and H.-H. Chen, "Transactions papers a routing-driven elliptic curve cryptography based key management scheme for heterogeneous sensor networks," *IEEE Trans. Wireless Commun.*, vol. 8, no. 3, pp. 1223–1229, Mar. 2009.

[30] Y. Xue and K. Nahrstedt, "Providing fault-tolerant ad hoc routing service in adversarial environments," *Wireless Pers. Commun.*, vol. 29, nos. 3–4, pp. 367–388, 2004.

[31] X. Du and H. H. Chen, "Security in wireless sensor networks," *IEEE Wireless Commun. Mag.*, vol. 15, no. 4, pp. 60–66, Aug. 2008.

[32] G. Sharma, V. Kuchta, R. A. Sahu, S. Ellinidou, O. Markowitch, and J.-M. Dricot, "A twofold group key agreement protocol for NoC based MPSoCs," in *Proc. 16th Annu. Conf. Privacy, Secur. Trust (PST)*, Aug. 2018, pp. 1–2.

[33] Q. Zhang, Z. Ma, and Y. Tan, "An authenticated asymmetric group key agreement for imbalanced mobile networks," *Chin. J. Electron.*, vol. 23, no. 4, pp. 827–835, 2014.

[34] S. H. Islam, M. S. Obaidat, P. Vijayakumar, E. Abdulhay, F. Li, and M. K. C. Reddy "A robust and efficient password-based conditional privacy preserving authentication and group-key agreement protocol for VANETs," *Future Gener. Comput. Syst.*, vol. 84, pp. 216–227, Jul. 2018.

[35] S. Zeng and Y. Chen, "Concurrently deniable group key agreement and its application to privacy-preserving VANETs," *Wireless Commun. Mobile Comput.*, vol. 2018, Apr. 2018, Art. no. 6870742.

[36] Z. Guan, G. Si, X. Zhang, L. Wu, N. Guizani, X. Du, and Y. Ma, "Privacy-preserving and efficient aggregation based on blockchain for power grid communications in smart communities," *IEEE Commun. Mag.*, vol. 56, no. 7, pp. 82–88, Jul. 2018.

[37] X. Lv, H. Li, and B. Wang, "Authenticated asymmetric group key agreement based on certificateless cryptosystem," *Int. J. Comput. Math.*, vol. 91, no. 3, pp. 447–460, 2014.

[38] Y Li, J. Hu, Z. Wu, C. Liu, F. Peng, and Y. Zhang, "Research on QoS service composition based on coevolutionary genetic algorithm," *Soft Comput.*, vol. 22, no. 23, pp. 7865–7874, 2018.

[39] Y. Zhang, D. Zheng, and R. H. Deng, "Security and privacy in smart health: Efficient policy-hiding attribute-based access control," *IEEE Internet Things J.*, vol. 5, no. 3, pp. 2130–2145, Jun. 2018.

[40] L. Zhang, Q. Wu, B. Qin, H. Deng, J. Li, J. Liu, and W. Shi, "Certificateless and identity-based authenticated asymmetric group key agreement," *Int. J. Inf. Secur.*, vol. 16, no. 3, pp. 559–576, 2017.

[41] O. Ermi , S. Bahtiyar, E. Anarim, and M. U. Çaglayan, "A secure and efficient group key agreement approach for mobile ad hoc networks," *Ad Hoc Netw.*, vol. 67, pp. 24–39, Dec. 2017.

[42] Y. Xiao, X. Du, J. Zhang, and S. Guizani, "Internet protocol television (IPTV): The killer application for the next generation Internet," *IEEE Commun. Mag.*, vol. 45, no. 11, pp. 126–134, Nov. 2007.

[43] M. Bilal and S.-G. Kang, "A secure key agreement protocol for dynamic group," *Cluster Comput.*, vol. 20, no. 3, pp. 2779–2792, 2017.

[44] M. Han, L. Hua, and S. Ma, "A self-authentication and deniable efficient group key agreement protocol for VANET," *Kill Trans. Internet Inf. Syst.*, vol. 11, no. 7, pp. 3678–3698, Jul. 2017.

[45] C. Liang, Y.-A. Tan, X. Zhang, X. Wang, J. Zheng, and Q. Zhang, "Building packet length covert channel over mobile VoIP traffics," *J. Netw. Comput. Appl.*, vol. 118, pp. 144–153, Sep. 2018.

[46] G. Wei, X. Yang, and J. Shao, "Efficient certificateless authenticated asymmetric group key agreement protocol," *KSII Trans. Internet Inf. Syst.*, vol. 6, no. 12, pp. 3352–3364, 2012.

[47] Y. Xiao, V. K. Rayi, B. Sun, X. Du, F. Hu, and M. Galloway, "A survey of key management schemes in wireless sensor networks," *J. Comput. Commun.*, vol. 30, nos. 11–12, pp. 2314–2341, 2007.

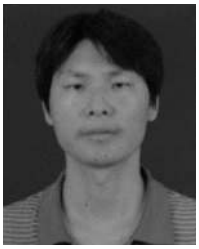
[48] B. Semal, K. Markantonakis, and R. N. Akram, "A certificateless group authenticated key agreement protocol for secure communication in untrusted UAV networks," in *Proc. IEEE/AIAA 37th Digit. Avionics Syst. Conf. (DASC)*, Sep. 2018, pp. 1–8.

[49] D. Cheng, J. Liu, Z. Guan, and T. Shang, "A one-round certificateless authenticated group key agreement protocol for mobile ad hoc networks," *IEICE Trans. Inf. Syst.*, vol. E99.D, no. 11, pp. 2716–2722, 2016.

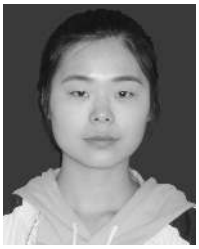
[50] Y.-A. Tan, X. Xu, and C. Liang, "An end-to-end covert channel via packet dropout for mobile networks," *Int. J. Distrib. Sensor Netw.*, vol. 14, no. 5, 2018, Art. no. 1550147718779568.

[51] Y. Tan, J. Zheng, Q. Zhang, X. Zhang, Y. Li, and Q. Zhang, "A specific-targeting asymmetric group key agreement for cloud computing," *Chin. J. Electron.*, vol. 27, no. 3, pp. 866–872, Jul. 2018.

[52] C.-T. Li, T.-Y. Wu, and C.-M. Chen, "A provably secure group key agreement scheme with privacy preservation for online social networks using extended chaotic maps," *IEEE Access*, vol. 6, pp. 66742–66753, 2018.
[53] Y. Xue, Y.-A. Tan, C. Liang, Y. Li, J. Zheng, and Q. Zhang, "RootAgency: A digital signature-based root privilege management agency for cloud terminal devices," *Inf. Sci.*, vol. 444, pp. 36–50, May 2018.
[54] R. S. Ranjani, D. L. Bhaskari, and P. S. Avadhani, "An extended identity based authenticated asymmetric group key agreement protocol," *Int. J. Netw. Secur.*, vol. 17, no. 5, pp. 510–516, 2015.



ZHANG QIKUN was born in 1980. He received the B.S. degree from Xidian University, in 2004, the M.S. degree from the Lanzhou University of Technology, in 2008, and the Ph.D. degree from the Beijing Institute of Technology, in 2013. He is currently an Associate Professor with the Department of Computer and Communication Engineering, Zhengzhou University of Light Industry. His research interests include information security and cryptography.



LI YONGJIAO was born in 1994. She received the B.S. degree from the Henan University of Chinese Medicine, in 2018. She is currently pursuing the master's degree with the Department of Computer and Communication Engineering, Zhengzhou University of Light Industry. Her research interests include information security and cryptography.

GAN YONG was born in 1965. He was a Ph.D. Professor. He is currently with the Zhengzhou Institute of Technology. His research interests include multimedia communications, image processing, coding, and network engineering.

ZHENG CHUANYANG was born in Henan, China, in 1999. He is currently pursuing the bachelor's degree with the Department of Computer Science, Hong Kong Baptist University. His research interests include information security and cryptography.

LUO XIANGYANG was born in Henan, China, in 1978. He is currently a Professor with the State Key Laboratory of Mathematical Engineering and Advanced Computing. His research interests include network and information security.

ZHENG JUN was born in Beijing, China, in 1969. She is currently a Ph.D. Professor with the Beijing Institute of Technology. Her research interests include information security and cloud computing.