American Journal of Engineering Research (AJER)
e-ISSN: 2320-0847 p-ISSN : 2320-0936
Volume-12, Issue-8, pp-165-175
www.ajer.org
Research Paper Open Access

Cryptanalysis of a Key Agreement Scheme Based on Attribute Authentication and Privacy Protection

Ahmed Tarek Elrashidy and Yasmine Abouelseoud
[1]*Faculty of Engineering, ,Alexandria, Egypt*
Corresponding Author: Ahmed Tarek Elrashidy

ABSTRACT : *In this paper, we demonstrate the weaknesses and loopholes found in GKA-PPAA (Group Key Agreement Protocol Based on Privacy Protection and Attribute Authentication) protocol. The protocol under study provides identity and attribute authentication. It claims that attributes are hidden using polynomial calculations, then the trusted authority or attribute authority cannot figure out any value of attributes during authentication. It, also divides members in the group into subsets according to the number of attributes. The more attributes the participant has, the higher authority he gets. Simply, not all information could be shared to all members with lower authority. The scheme under study claims also that it is resistant to impersonation attack. In our paper we provide a cryptanalysis to the protocol under study. We present different attack strategies and demonstrates the flaws in the scheme. Firstly, we will prove and show that AA has more than one way to figure out the values of all members attributes. AA doesn't need to try to solve (ECDLP). Secondly, we will introduce an attack strategy which enables any member to get higher fake authority. Members with lower number of attributes could pretend that they have higher number of fakes attributes. Thirdly, in our work, we will launch impersonation attack. We will show that digital signature, proposed by the scheme cannot prevent any illegal member to counterfeit that valid signature. This makes the scheme nonresistant to impersonation attack. Finally, the scheme is nonresistant to collusion attack as we will demonstrate.*

KEYWORDS *Cryptanalysis, Attribute Authentication, Threshold Authority, Impersonation Attack, Collusion Attack.*

Date of Submission: 05-08-2023 Date of acceptance: 19-08-2023

I. INTRODUCTION

Group key agreement protocols play a crucial role in achieving secure group communication over untrusted networks. These protocols enable a group of communicating parties to establish a common secret key, ensuring secure and confidential communication within the group. In recent years, significant research has been conducted to develop and improve group key agreement protocols, addressing various security requirements and challenges. The Diffie-Hellman protocol, proposed in 1976, was one of the pioneering protocols in this field. It provided a foundation for subsequent protocols and laid the groundwork for secure group communication. However, as research progressed, it became evident that the Diffie-Hellman protocol had certain limitations and vulnerabilities [1]. To address these limitations, researchers proposed successors to the Diffie-Hellman protocol. Tseng, in 2007, introduced a new group key agreement protocol specifically designed for secure group communication in a mobile environment [2]. This protocol aimed to overcome the shortcomings of previous protocols and achieve secure group communication in a mobile setting. However, Tseng's protocol was found to be non-authenticated, meaning it lacked a mechanism to ensure the validity of transmitted. To address this issue, proposed a new authenticated group key agreement protocol based on bilinear pairings. This protocol aimed to provide authentication and ensure the integrity of the transmitted messages, enhancing the overall security of the group communication. In addition to authentication, privacy protection is another important requirement in group key agreement protocols. Privacy protection ensures that sensitive information remains confidential and is only accessible to authorized parties. proposed a group key agreement protocol based on privacy protection and attribute authentication (GKA-PPAA) [3]. This protocol aimed to address the key issues of identity authentication, privacy protection, and information sharing access control in group key agreement. In our paper we introduce a cryptanalysis to (GKA-PPAA). Furthermore, the security of authenticated group key agreement protocols has been a subject of research. conducted a study to identify security vulnerabilities in existing

protocols and propose measures to avoid them in future constructions [4]. Their research aimed to enhance the security of group key agreement protocols, particularly in the context of secure multicasting in the Internet of Things. Secure group communication is important for many collaborative and distributed Internet of Things applications. [5] and [6] are two examples. [7] proposes a safe and efficient group key agreement technique for VANET, which uses a fixed roadside unit to negotiate a dynamic session secret key, allowing for more steady communication performance and faster encryption and decryption. to guarantee that cars in the VANET communicate information in a secure manner [8,10] propose a multi-domain lightweight asymmetric group key agreement protocol that uses bilinear mapping and blind key technology to achieve an asymmetric group key agreement protocol among mobile terminals distributed across domains, as well as communication and computation migration technologies. to guarantee that mobile terminals consume minimal processing and connection resources while maintaining anonymity and authentication [11] Using Chebyshev chaotic maps, presents an authenticated group key establishment protocol with user anonymity. It is multi-server compatible and mobile environments, and it can survive reflection attacks and achieve contributory group key agreement with user authentication. [12], [13] present a cross-domain light-weight asymmetric group key agreement for establishing a secure and efficient group communication channel between sensor nodes. The computation and communication overhead are both light in this protocol. [14] proposes a dynamic and cross-domain authenticated asymmetric group key agreement to circumvent the security concerns of key escrow and the complexity of certificate administration, this protocol uses a cross-domain authentication technique. It allows nodes to update their group keys dynamically for forward secrecy and backward security, The member who participated in the group key agreement can self-certify if the computed group keys are valid, as well as achieving the key self-certified. [15], [16] offer a Certificateless One Way Group Key Agreement Protocol for End-to-End Email Encryption, which is appropriate for implementing E2E email encryption. The group key agreement does not require a certificate, as a result, there is no need for key escrow and no public key certificate infrastructure, and it is a one-way group key agreement, so no back-and-forth message exchange is necessary. It is an n-party group key agreement at the same time. The distribution of the group key for authorized vehicles is proposed in [17,21] using a group key agreement method based on the Chinese remainder theorem. When a vehicle joins or leaves a group, the group key can be modified. To distribute group keys for all cars, it requires a third-party trustworthy entity with powerful computing and storage capabilities, and it poses security issues.

Due to the importance of group key agreement protocols, we provide a cryptanalysis of recent scheme [1] and summarizes our contributions as follows:

1) We will prove and show that AA has more than one way to figure out the values of all members attributes. That means, in practice, that the protocol under study cannot protect the person-al privacy of the participants.
2) We will introduce an attack strategy which enables any member to get higher fake authority. Members with lower number of attributes could pretend that they have higher number of fakes attributes. This means that information will be leaked to members with lower authority.
3) we will show that digital signature, proposed by the scheme cannot prevent any illegal member to counterfeit that valid sig-nature which makes the scheme nonresistant to impersonation attack.
4) GKA-PPAA claims that it provides threshold authority but we show easily that non honest members with low number of attributes and different attributes can collude and exchange their secret attributes to get higher authority. This means that information will be leaked to members with lower authority.

The organization of paper is as the following: In section II, we describe the summary of registration phase of the attacked protocol; In section III we summarize the steps of establishing group key. In section IV, we analyze the loopholes of the protocol and show the mathematical proofs, needed. All notations and definitions are shown in Table 1.

Table 1

Notation	Definition
G_1	Additive group
G_2	Multiplicative group
q	prime order of G_1
g_1	Generator of G_1
e	The admissible pairing
AA	Attribute Authority
U	set of network terminals or members
u_i	ith member in the set U
ID	identity set of members
$Attr$	ordered set of attributes of AA
R	Total number of attributes
$attr_i$	Set of attributes of AA, $attr_i \subseteq Attr$
$a_{i,k}$	kth attribute of ith member
r	Number of member attribute, $r \leq R$

H_1 , H_2 , H_3	Hash functions
SK_A	Secret key of attribute authority
PK_A	Public key of attribute authority
sk_{ui}	Secret key of u_i
pk_{ui}	Public key of u_i
$\eta_{j,h}$	privilege grade
γ_i	Group public key parameter
λ_i	Random integer selected by u_i
s_{ui}	Random integer selected by u_i
PK_{g-u_j}	Group encryption key
SK_{g-u_j}, M_j	Group decryption key

II. SUMMARY OF REGISTERATION PHASE

A. *Complexity Assumption and Bilinear Maps:*

The attacked scheme is based on the theory of bilinear mapping. We describe it as the following. Assume that G_1 is an additive group and G_2 is multiplicative group. Their prime order is q, where $q \geq 2^l + 1$, and l is assumed to be the security parameter of the group. g_1 is the generator of G_1 and g_2 is the generator of G_2 , the DLP of G_1 and G_2 are very difficult. The admissible pairing $e: G_1 \times G_1 \rightarrow G_2$ has the following properties:

1. Bilinearity property: $\forall \mu, v \in G_1$, let $a, b \in Z_q^*$ then $e(a\mu, bv) = e(\mu, v)^{ab}$;
2. Non-degeneracy property: $\exists \mu, v \in G_1$, such that $e(\mu, v) \neq 1$;
3. Computability property: $\forall \mu, v \in G_1$ there is an efficient way to compute $e(\mu, v)$;

It is clear that $\forall \mu, v, g_1 \in G_1$ there is $e(\mu + v, g_1) = e(\mu, , g_1)e(v, g_1)$.

B. *Parameters Initialization*

The protocol assumes the network contains n network terminals. Let the set of network terminals or members $U = \{u_1, u_2, \dots, u_n\}$ and their corresponding identity set is $ID = \{id_{u1}, id_{u2}, \dots, id_{un}\}$.Let the ordered set of attributes by AA be $Attr = \{A_1, A_2, \dots, A_k, \dots, A_R\}$. R is the total number of attributes , set is ordered then we find $A_k < A_{k+1}$, let the terminal set of attributes $attr_i = \{a_{i,1}, a_{i,2}, \dots, a_{i,k}, \dots, a_{i,r}\}$ Any member has r attributes $r \leq R$, set is ordered then we find $a_{i,k} < a_{i,k+1}$, i denotes the ith member and r denotes the rth attribute of the terminal u_i. $r, R \in N^*, attr_i \subseteq Attr$. Assume that G_1 is an additive group and G_2 is multiplicative group. Their prime order is q, where $q \geq 2^l + 1$, and l is assumed to be the security parameter of the group. g_1 is the generator of G_1 and g_2 is the generator of G_2 , The admissible pairing $e: G_1 \times G_1 \rightarrow G_2$ is computable. There are three hash functions $H_1: \{0,1\}^* \rightarrow Z_q^*$, $H_2: G_1 \rightarrow Z_q^*$, $H_3: G_2 \rightarrow Z_q^*$, Attribute Authority selects secret key $SK_A \in Z_q^*$ then calculates public key $PK_A = SK_A g_1$. Also, terminal member u_i selects a random number $s_{ui} \in Z_q^*$ .Now u_i calculates his secret key $sk_{ui} = H_1(id_{ui})\, s_{ui}$ and his public key $pk_{ui} = sk_{ui} g_1$.and selects $\lambda_i \in Z_q^*$. It is obvious that the system parameters are in the set $parameters = \{PK_A, G_1, G_2, g_1, q, e, H_1, H_2, H_3\}$.

C. *Members Registration Phase*

The following steps summarize the registration phase:

1. AA constructs a polynomial of Rth degree and its roots are in the set $Attr = \{A_1, A_2, \dots, A_k, \dots, A_R\}$, $f(x) = (x - A_1)(x - A_2) \dots (x - A_{R-1})(x - A_R) = b_0 + b_1 x + b_2 x^2 + \cdots + b_{R-1} x^{R-1} + b_R x^R$.
2. Every terminal network u_i with attribute set $attr_i = \{a_{i,1}, a_{i,2}, \dots, a_{i,k}, \dots, a_{i,r}\}$ calculates the following:

$$\{(\lambda_i g_1, a_{i,1}\lambda_i g_1, a_{i,1}^2 \lambda_i g_1, \dots, a_{i,1}^R \lambda_i g_1),$$
$$(\lambda_i g_1, a_{i,2}\lambda_i g_1, a_{i,2}^2 \lambda_i g_1, \dots, a_{i,2}^R \lambda_i g_1),$$
$$\dots,$$
$$(\lambda_i g_1, a_{i,r}\lambda_i g_1, a_{i,r}^2 \lambda_i g_1, \dots, a_{i,r}^R \lambda_i g_1)\}$$

and $\beta_i = (a_{i,1} + a_{i,2} + \cdots + a_{i,r})\, sk_{ui} \lambda_i g_1$. then sends them to AA in addition to u_i's public key pk_{ui} .

3. AA receives the sent parameters from u_i and calculates: $\gamma_i = a_{i,1}\lambda_i g_1 + a_{i,2}\lambda_i g_1 + \cdots + a_{i,r}\lambda_i g_1$

   then makes identity verification of terminal u_i through the equation $e(\beta_i, g_1) = e(\gamma_i, pk_{ui})$. If it holds, the identity of the terminal u_i is verified successfully.

4. AA starts to check the valid attributes and counts them without knowing their values through calculating the following:

$$b_0\lambda_i g_1 + b_1 a_{i,1}\lambda_i g_1 + b_1 a_{i,1}^2\lambda_i g_1 + \cdots + b_R a_{i,1}^R\lambda_i g_1 = f(a_{i,1})\lambda_i g_1$$
$$b_0\lambda_i g_1 + b_1 a_{i,2}\lambda_i g_1 + b_1 a_{i,2}^2\lambda_i g_1 + \cdots + b_R a_{i,2}^R\lambda_i g_1 = f(a_{i,2})\lambda_i g_1$$

...

$$b_0\lambda_i g_1 + b_1 a_{i,r}\lambda_i g_1 + b_1 a_{i,r}^2\lambda_i g_1 + \cdots + b_R a_{i,r}^R\lambda_i g_1 = f(a_{i,r})\lambda_i g_1$$

If $f(a_{i,1})\lambda_i g_1 = 0, f(a_{i,2})\lambda_i g_1 = 0, \ldots, f(a_{i,r})\lambda_i g_1 = 0$,then it is obvious that $attr_i \subseteq Attr$, and the sent attributes are valid.

5. AA counts the number of attributes, which satisfied the polynomial then divides the authority or privilege level according to the number of attributes they have so AA chooses numbers of positive integers equals to number of attributes for each member. AA selects $t_{i,1}, t_{i,2}, \ldots, t_{i,r} \in Z_q^*$ and calculates $\{T_{i,1} = t_{i,1}\lambda_i g_1, T_{i,2} = t_{i,2}\lambda_i g_1, , \ldots T_{i,r} = t_{i,r}\lambda_i g_1\}$. Also calculates the privilege grade $\eta_{i,h} = SK_A(t_{i,1} + t_{i,2} + \cdots + t_{i,r})g_1$ then sends the parameter $\{\gamma_i, \eta_{i,h}, T_{i,1}, T_{i,2}, \ldots, T_{i,r}\}$ to register.
6. u_i receives the parameter $\{\gamma_i, \eta_{i,h}, T_{i,1}, T_{i,2}, \ldots, T_{i,r}\}$ from AA and calculates $\varepsilon_i = \lambda_i^{-1}T_{i,1} + \lambda_i^{-1}T_{i,2} + \cdots + \lambda_i^{-1}T_{i,r} = (t_{i,1} + t_{i,2} + \cdots + t_{i,r})g_1$. u_i starts to verify the identity of AA using the equation $e(\eta_{i,h}, g_1) = e(\varepsilon_i, PK_A)$ If it holds the identity of the AA is verified successfully.
7. u_i computes the attribute permission values $K_{i,1} = \lambda_i^{-1}T_{i,1} = t_{i,1}g_1, K_{i,2} = \lambda_i^{-1}T_{i,2} = t_{i,2}g_1, \ldots, K_{i,r} = \lambda_i^{-1}T_{i,r} = t_{i,r}g_1$ and registration is done successfully. Every member has number of attribute permission values $K_{i,r}$ equal to the number of attributes he has.
8. Finally, AA shares all public values of all members in an information pool.

I. III. Computing Group Key with Different Attribute Permissions

If member $u_j (1 \le j \le n)$ who has set of attributes $a_{ttr} = \{a_{j,1}, a_{j,2}, \ldots, a_{j,r}\}$ and the authority or privilege value $\eta_{j,h} = SK_A(t_{j,1} + t_{j,2} + \cdots + t_{j,r})g_1$ needs to establish group to share information share the information with other members who have the same grade of authority, it can select them from the information pool on the platform of AA and constructs a subgroup as follows:

1. The member or sponser u_j that needs to share secret information with members that have same grade of authority. He searches for some attribute privilege values and corresponding privilege grade information from the information pool, and selects the members set $\tilde{U} = \{u_j, u_{j+1}, \ldots u_l\}(j < l)$.
2. The sponsor u_j gets the public information $T_{k,1}, \ldots, T_{k,r}$ of every $u_k (j \le k \le l)$ from the information pool and computes the following $T_{pub} = \sum_{k=j}^{l} T_{k,0} = \sum_{k=j}^{l} \lambda_k g_1$ and $T_{pri} = \sum_{\tau=1}^{r}\sum_{k=j}^{l} T_{k,\tau} = \sum_{\tau=1}^{r} t_{k,\tau}(\lambda_j + \cdots + \lambda_l)g_1 = (t_{k,1} + \cdots + t_{k,r})(\lambda_j + \cdots + \lambda_l)g_1$.
3. u_j selects random integer $m_j \in \mathbb{Z}_p^*$, and calculates:
   $p_{u_j} = m_j T_{pub}, M_j = m_j T_{pri}, w_{j,1} = H_2(K_{j,1}), w_{j,2} = H_2(K_{j,2}), \ldots, w_{j,r} = H_2(K_{j,r})$ then constructs a (r − 1)-th degree polynomial $f(x) = m_j K_{j,r-1}x^{r-1} + \cdots + m_j K_{j,1}x + M_j$ corresponding to the attribute permission values $\{K_{j,1}, K_{j,2}, \ldots, K_{j,r}\}$ that it were calculated before and $f(0) = M_j$, then it computes $f(w_{j,1}) = y_{j,1}, f(w_{j,2}) = y_{j,1}, f(w_{j,2}) = y_{j,2}, \ldots, f(w_{j,r}) = y_{j,r}$
4. u_j calculates $\varphi_j = sk_{u_j}(y_{j,1} + y_{j,2} + \cdots + y_{j,r})$ and uses $PK_{g-u_j} = (p_{u_j}, \eta_{j,h})$ as encryption key of group and $SK_{g-u_j} = M_j$ as decryption key of group ,
5. u_j broadcasts the authentication parameters $\{(y_{j,1}, y_{j,2}, \ldots, y_{j,r}), (p_{u_j}, \eta_{j,h}), \varphi_j\}$ to all terminals $\tilde{U} = \{u_j, u_{j+1}, \ldots u_l\}(j < l)$
6. Every single member $u_k (j \le k \le l, k \ne j)$ in the group who got the broadcasted authentication data $\{(y_{j,1}, y_{j,2}, \ldots, y_{j,r}), (p_{u_j}, \eta_{j,h}), \varphi_j\}$ from u_j , calculates $\phi_k = y_{j,1} + y_{j,2} + \cdots + y_{j,r}$ and verifies the signature and identity of u_j through the pairing equation $e(\varphi_j, g_1) = e(\phi_k, pk_{u_j})$. If it holds, u_k compares its authority or privilege value $\eta_{k,h}$ with the received privilege value $\eta_{j,h}$ of the sponsor u_j. If it has the same level of privilege or higher grade of privilege than $\eta_{j,h}$, it can check that the attribute permission value of him is identical to the permission values of the sponsor. (that means $\{K_{k,1} = K_{j,1}, K_{k,2} = K_{j,2}, \ldots, K_{k,r} = K_{j,r}\}$) .

7. u_k uses the values $\{K_{k,1}, K_{k,2}, \dots, K_{k,r}\}$ and computes $w_{k,1} = H_2(K_{k,1}), w_{k,2} = H_2(K_{k,2}), \dots, w_{k,r} = H_2(K_{k,r})$ then reconstructs a polynomial $f(x)$, where polynomial
$f(x) = \sum_{\chi=1}^{r} \left(\prod_{1 \le \varpi \le r, \varpi \ne \chi} \frac{x - w_{k,\varpi}}{w_{k,\chi} - w_{k,\varpi}} \right) y_{j,\chi}$ substituting the values $\{(w_{k,1}, y_{j,1}), (w_{k,2}, y_{j,2}), \dots, (w_{k,r}, y_{j,r})\}$ using Lagrange Interpolation and computes the key $M_k = f(0)$,
$f(0) = \sum_{\chi=1}^{r} \left(\prod_{1 \le \varpi \le r, \varpi \ne \chi} \frac{-w_{k,\varpi}}{w_{k,\chi} - w_{k,\varpi}} \right) y_{j,\chi} = M_j$ where M_j is decryption key.
8. u_k obtains the encryption key group $PK_{g-u_k} = (p_{u_k}, \eta_{k,h}) = \left(p_{u_j}, \eta_{j,h}\right)$ from the transmitted messages $\left\{(y_{j,1}, y_{j,2}, \dots, y_{j,r}), \left(p_{u_j}, \eta_{j,h}\right)\right\}$ by u_j.
9. All members of group $u_k (j \le k \le l)$ do not need to exchange hash values of the of the computed key to make sure of key correctness. They need only to check this equation $(p_{u_k}, \eta_{k,h}) = e(M_k, PK_A)$, if it holds , the computed keys are correct and the same.

II. IV. Cryptanalysis Of the Studied Protocol

A. *First Loophole*

AA can figure out any value of the attributes sent to him without solving ECDLP which means that the scheme under study cannot conserve or protect the personal privacy as it claims.

Attack 1. Let AA has set $Atrr = \{a_1, a_2, a_3, a_4, a_5, \dots, a_R\}$ and u_1 has $attr_1 = \{a_2, a_3, a_5\}$, u_1 selects $\lambda_1 \in Z_q^*$

and calculates the following then sends it to AA:

$$\{old\ R_1: (\lambda_1 g_1, a_2\lambda_1 g_1, a_2^2\lambda_1 g_1, \dots, a_2^R\lambda_1 g_1),$$
$$old\ R_2: (\lambda_1 g_1, a_3\lambda_1 g_1, a_3^2\lambda_1 g_1, \dots, a_3^R\lambda_1 g_1),$$
$$old\ R_3: (\lambda_1 g_1, a_5\lambda_1 g_1, a_5^2\lambda_1 g_1, \dots, a_5^R\lambda_1 g_1)\}$$

, $\beta_1 = (a_2 + a_3 + a_5)\, sk_{u1}\lambda_1 g_1$ and pk_{u1}. After that AA calculates the product of $old\ R_1$ with all attributes set

$Atrr = \{a_1, a_2, a_3, a_4, a_5, \dots, a_R\}$ respectively.

$$new\ R_1: \ (a_1\lambda_1 g_1, \ a_2 a_2\lambda_1 g_1, \ a_3\, a_2^2\lambda_1 g_1, \ a_4 a_2^3\lambda_1 g_1, \dots$$
$$, a_2^R\lambda_1 g_1 \ )$$

Third term of $old\ R_1: a_2^2\lambda_1 g_1$ matches the *second* term in the $new\ R_1$, we refer the word *second* to the attribute a_2 so first attribute of u_1 is: a_2 . AA repeats the previous process again and calculates the product of $old\ R_2$ with all attributes set $Atrr = \{a_1, a_2, a_3, a_4, a_5, \dots, a_R\}$ respectively then $new\ R_2: (a_1\lambda_1 g_1, a_2 a_3\lambda_1 g_1, a_3 a_3^2\lambda_1 g_1, a_3^3\lambda_1 g_1, \dots, a_3^R\lambda_1 g_1)$
Fourth term of $old\ R_2$ matches the term number third term in $new\ R_2$ then attribute of u_1 is: a_3. Generally, we can deduce this rule: *If the* $(r+1)th$ *term of the old row matches the* rth *term in the new row then attribute of* u_i *is* a_r.

We introduce another attack for the first loophole.

Attack 2. Let AA has $Atrr = \{a_1, a_2, a_3, a_4, a_5, \dots, a_R\}$, and $u_1, attr_1 = \{a_2, a_3, a_5\}$

AA is trying to figure out common attributes which puts the privacy of u_1 at risk.

u_1 Calculates the following and sends it to AA:

$$R_1: (\lambda_1 g_1, \ a_2\lambda_1 g_1, a_2^2\lambda_1 g_1, a_2^3\lambda_1 g_1, \dots, a_2^{R-1}\lambda_1 g_1 \ , a_2^R\lambda_1 g_1 \ )$$
$$R_2: (\lambda_1 g_1, \ a_3\lambda_1 g_1, a_3^2\lambda_1 g_1, a_3^3\lambda_1 g_1, \dots, a_3^{R-1}\lambda_1 g_1, a_3^R\lambda_1 g_1 \ )$$
$$R_3: (\lambda_1 g_1, \ a_5\lambda_1 g_1, a_5^2\lambda_1 g_1, a_5^3\lambda_1 g_1, \dots, a_5^{R-1}\lambda_1 g_1, a_5^R\lambda_1 g_1 \ )$$

AA calculates:

$$S = \lambda_1 g_1 + \ a_i\lambda_1 g_1 + \ a_i^2\lambda_1 g_1 + \dots + a_i^{R-1}\lambda_1 g_1$$
$$\therefore \ S = (1 + \ a_i + \ a_i^2 + \dots + a_i^{R-1})\lambda_1 g_1$$

From geometric series summation rule:

$$S = (a_i - 1)^{-1}(a_i^R - 1)\lambda_i g_1$$
$$(a_i - 1)S = (a_i^R - 1)\lambda_i g_1$$
$$(a_i - 1)S = (a_i^R \lambda_i g_1 - \lambda_i g_1)$$
$$(x - 1)S = (a_i^R \lambda_i g_1 - \lambda_i g_1)$$

For R_1, AA substitutes for the value of x with his first attribute a_1 in $(x-1)S = (a_2^R \lambda_1 g_1 - \lambda_1 g_1)$ which does not satisfy the equation then try for a_2. Now it satisfies the equation and a_2 is known. AA repeats the process for the second row substituting in the equation $(x-1)S = (a_5^R \lambda_1 g_1 - \lambda_1 g_1)$ starting from a_1 till reaching a_5 which satifies the equation and so on.

B. Second Loophole

Any non honest member u_i can pretend that he has more than his actual number of attributes which gives him a higher authority.

Attack 3. Let AA has: $Atrr = \{a_1, a_2, a_3, a_4, a_5, \dots, a_R\}$ and u_1 who is non honest member has $attr_1 = \{a_1, a_2, a_3\}$. u_1 calculates the following :

$$R_1 : (\lambda_1 g_1, a_1\lambda_1 g_1, a_1^2\lambda_1 g_1, a_1^3\lambda_1 g_1, \dots, a_1^R\lambda_1 g_1)$$
$$R_2 : (\lambda_1 g_1, a_2\lambda_1 g_1, a_2^2\lambda_1 g_1, a_2^3\lambda_1 g_1, \dots, a_2^R\lambda_1 g_1)$$
$$R_3 : (\lambda_1 g_1, a_3\lambda_1 g_1, a_3^2\lambda_1 g_1, a_3^3\lambda_1 g_1, \dots, a_3^R\lambda_1 g_1)$$

, then u_1 calculates $2R_1$, $2R_2$, $2R_3$, $(R_1 + R_2)$, $(R_1 + R_3)$ and $(R_2 + R_3)$. u_1 starts to calculate these combinations

$$\{2R_1: (2\lambda_1 g_1, 2a_1\lambda_1 g_1, 2a_1^2\lambda_1 g_1, 2a_1^3\lambda_1 g_1, \dots, 2a_1^R\lambda_1 g_1)$$
$$, 2R_2: (2\lambda_1 g_1, 2a_2\lambda_1 g_1, 2a_2^2\lambda_1 g_1, 2a_2^3\lambda_1 g_1, \dots, 2a_2^R\lambda_1 g_1)$$
$$, 2R_3: (2\lambda_1 g_1, 2a_3\lambda_1 g_1, 2a_3^2\lambda_1 g_1, 2a_3^3\lambda_1 g_1, \dots, 2a_3^R\lambda_1 g_1)$$
$$, R_1 + R_2: (2\lambda_1 g_1, (a_1 + a_2)\lambda_1 g_1, (a_1^2 + a_2^2)\lambda_1 g_1, (a_1^3 + a_2^3)\lambda_1 g_1, \dots, (a_1^R + a_2^R)\lambda_1 g_1)$$
$$, R_2 + R_3: (2\lambda_1 g_1, (a_2 + a_3)\lambda_1 g_1, (a_2^2 + a_3^2)\lambda_1 g_1, (a_2^3 + a_3^3)\lambda_1 g_1, \dots, (a_2^R + a_3^R)\lambda_1 g_1)$$
$$, R_1 + R_3: (2\lambda_1 g_1, (a_1 + a_3)\lambda_1 g_1, (a_1^2 + a_3^2)\lambda_1 g_1, (a_1^3 + a_3^3)\lambda_1 g_1, \dots, (a_1^R + a_3^R)\lambda_1 g_1)$$
$$\beta = (2a_1 + 2a_2 + 2a_3 + (a_1 + a_2) + (a_2 + a_3) + (a_1 + a_3))\lambda_1 sk_{u_1} g_1$$
$$pk_{u_1} = sk_{u_1} g_1$$

u_1 sends the previous combinations, β and pk_{u_1} to AA. AA calculates $\gamma = (2a_1\lambda_1 g_1 + 2a_2\lambda_1 g_1 + 2a_3\lambda_1 g_1 + (a_1 + a_2)\lambda_1 g_1 + (a_2 + a_3)\lambda_1 g_1 + (a_1 + a_3)\lambda_1 g_1$ then verifies the equation $e(\beta, g_1) = e(\gamma, pk_{u_1})$. Let us check it mathematically.

$$LHS = e(\beta, g_1) =$$
$$e\big((2a_1 + 2a_2 + 2a_3 + (a_1 + a_2) + (a_2 + a_3) + (a_1 + a_3))\lambda_1 sk_{u_1} g_1, g_1\big) =$$
$$e\big((4a_1 + 4a_2 + 4a_3)\lambda_1 sk_{u_1} g_1, g_1\big) = e(g_1, g_1)^{(4a_1 + 4a_2 + 4a_3)\lambda_1 sk_{u_1}}$$
$$RHS = e\big(\gamma, pk_{u_1}\big)$$
$$e\big((2a_1 + 2a_2 + 2a_3 + (a_1 + a_2) + (a_2 + a_3) + (a_1 + a_3))\lambda_1 g_1, sk_{u_1} g_1\big) =$$
$$e\big((4a_1 + 4a_2 + 4a_3)\lambda_1 g_1, sk_{u_1} g_1\big) = e(g_1, g_1)^{(4a_1 + 4a_2 + 4a_3)\lambda_1 sk_{u_1}}$$

$$e(\gamma, pk_{u_1}) = e(g_1, g_1)^{(4a_1+4a_2+4a_3)\lambda_1 sk_{u_1}}$$

$$LHS = RHS$$

Identity verification is successful. AA uses his polynomial for attributes authentication:

$f(x) = b_o + b_1 x + b_2 x^2 + b_3 x^3 + b_4 x^4 + \cdots + b_R x^R$

First attribute authentication:

$$b_o 2\lambda_1 g_1 + b_1\, 2\, a_1 \lambda_1 g_1 + b_2\, 2a_1^2 \lambda_1 g_1 + \cdots + b_R 2a_1^R \lambda_1 g_1$$
$$= (b_o + b_1\ a_1 + b_2\, a_1^2 + b_3 a_1^3 + \cdots + b_R a_1^R) 2\lambda_1 g_1\ = f(\,a_1) 2\lambda_1 g_1$$
$$= (0,0)$$

Second attribute authentication:

$$b_o 2\lambda_1 g_1 + b_1\, 2\, a_2 \lambda_1 g_1 + b_2\, 2a_2^2 \lambda_1 g_1 + \cdots + b_R 2a_2^R \lambda_1 g_1$$
$$= (b_o + b_1\ a_2 + b_2\, a_2^2 + b_3 a_2^3 + \cdots + b_R a_2^R) 2\lambda_1 g_1\ = f(\,a_2) 2\lambda_1 g_1 = (0,0)$$

Third attribute authentication:

$$b_o 2\lambda_1 g_1 + b_1\, 2\, a_3 \lambda_1 g_1 + b_2\, 2a_3^2 \lambda_1 g_1 + \cdots + b_R 2a_3^R \lambda_1 g_1$$
$$= (b_o + b_1\ a_3 + b_2\, a_3^2 + b_3 a_3^3 + \cdots + b_R a_3^R) 2\lambda_1 g_1\ = f(\,a_3) 2\lambda_1 g_1 = (0,0)$$

Fourth attribute authentication:

$$(b_o 2\lambda_1 g_1 + b_1\,(\,a_1 + a_2)\lambda_1 g_1 + b_2\,(a_1^2 + a_2^2)\lambda_1 g_1$$
$$+ b_3(a_1^3 + a_2^3)\lambda_1 g_1 + \cdots + b_R(a_1^R + a_2^R)\lambda_1 g_1\ )$$
$$= (b_o \lambda_1 g_1 + b_1\, a_1 \lambda_1 g_1 + b_2\, a_1^2 \lambda_1 g_1 + \cdots + b_R a_1^R \lambda_1 g_1)$$
$$+ (b_o \lambda_1 g_1 + b_1\ a_2 \lambda_1 g_1 + b_2\, a_2^2 \lambda_1 g_1 + \cdots + b_R a_2^R \lambda_1 g_1)$$
$$= (b_o + b_1\ a_1 + b_2\, a_1^2 + b_3 a_1^3 + \cdots + b_R a_1^R)\lambda_1 g_1 +$$
$$(b_o + b_1\ a_2 + b_2\, a_2^2 + b_3 a_2^3 + \cdots + b_R a_2^R)\lambda_1 g_1$$
$$= f(\,a_1)\lambda_1 g_1 + f(\,a_2)\lambda_1 g_1$$
$$= (0,0)$$

Fifth attribute authentication:

$$(b_o 2\lambda_1 g_1 + b_1\,(\,a_3 + a_2)\lambda_1 g_1 + b_2\,(a_3^2 + a_2^2)\lambda_1 g_1$$
$$+ b_3(a_3^3 + a_2^3)\lambda_1 g_1 + \cdots + b_R(a_3^R + a_2^R)\lambda_1 g_1\ )$$
$$= (b_o \lambda_1 g_1 + b_1\, a_3 \lambda_1 g_1 + b_2\, a_3^2 \lambda_1 g_1 + \cdots + b_R a_3^R \lambda_1 g_1)$$
$$+ (b_o \lambda_1 g_1 + b_1\ a_2 \lambda_1 g_1 + b_2\, a_2^2 \lambda_1 g_1 + \cdots + b_R a_2^R \lambda_1 g_1)$$
$$= (b_o + b_1\ a_3 + b_2\, a_3^2 + b_3 a_3^3 + \cdots + b_R a_3^R)\lambda_1 g_1 +$$
$$(b_o + b_1\ a_2 + b_2\, a_2^2 + b_3 a_2^3 + \cdots + b_R a_2^R)\lambda_1 g_1$$
$$= f(\,a_3)\lambda_1 g_1 + f(\,a_2)\lambda_1 g_1$$
$$= (0,0)$$

Sixth attribute authentication:

$$(b_o 2\lambda_1 g_1 + b_1\,(\,a_1 + a_3)\lambda_1 g_1 + b_2\,(a_1^2 + a_3^2)\lambda_1 g_1$$
$$+ b_3(a_1^3 + a_3^3)\lambda_1 g_1 + \cdots + b_R(a_1^R + a_3^R)\lambda_1 g_1\ )$$
$$= (b_o \lambda_1 g_1 + b_1\, a_1 \lambda_1 g_1 + b_2\, a_1^2 \lambda_1 g_1 + \cdots + b_R a_1^R \lambda_1 g_1)$$
$$+ (b_o \lambda_1 g_1 + b_1\ a_3 \lambda_1 g_1 + b_2\, a_3^2 \lambda_1 g_1 + \cdots + b_R a_3^R \lambda_1 g_1)$$
$$= (b_o + b_1\ a_1 + b_2\, a_1^2 + b_3 a_1^3 + \cdots + b_R a_1^R)\lambda_1 g_1 +$$

$$(b_o + b_1\ a_3 + b_2\ a_3^2 + b_3 a_3^3 + \cdots + b_R a_3^R)\lambda_1 g_1$$
$$= f(\ a_1)\lambda_1 g_1 + f(\ a_3)\lambda_1 g_1$$
$$= (0,0)$$

It is obvious now that u_i can make any linear combination of rows to pretend that he has more than his actual attributes .If he has 3 rows then he can generate valid fake 6 rows. He can repeat the same steps for the 6 fake rows and gets 21 valid fake rows and so on. We can deuce that *if u_i has n valid rows then he can generate number of attributes equals:*

$$n_{fake} = \binom{n}{2} + n\ .$$

$$n'_{fake} = \binom{n_{fake}}{2} + n_{fake}$$

C. *Third Loophole*

The protocol under study is not secure against an impersonator's attack. Any non honest or illegal member u_i can pretend to be the sponsor u_j of key establishment to initiate an invalid group key establishment session and counterfeit the valid signature φ_j although the impersonator u_i doesnot know the private key sk_{u_j} of u_j .

Attack 4. Assume that u_i is nonhonest member who intends to launch impersonation attack and pretend to be u_j.

1. The attacker u_i searches for some attribute privilege values and corresponding privilege grade $\eta_{i,h}$ information from the information pool, and selects the members set $u_k(i < k \le l, k \ne j)$.
2. The attacker u_i claculates $w_{i,1} = H_2(K_{i,1}), w_{i,2} = H_2(K_{i,2}), \dots, w_{i,r} = H_2(K_{i,r})$ and selects integer $m'_i \in \mathbb{Z}_q^*$, where $m'_i = -r^{-1}(w_{i,1} + w_{i,2} + \cdots w_{i,\mathrm{r}}) mod\ q$, assume that $M'_i = m'_i \eta_{,h}$ is the group key decryption.
3. u_i constructs a (r − 1)-th degree fake polynomial $f(x) = g_1 x^{r-1} + g_1 x^{r-2} + \cdots + g_1 x^2 + \eta_{,h} x + M'_i$ and $f(0) = M'_i$, then he computes $f(w_{i,1}) = y_{i,1}, f(w_{i,2}) = y_{i,1}, f(w_{i,2}) = y_{i,2}, \dots, f(w_{i,r}) = y_{i,r}$
4. u_i uses $PK_{g-u_i} = (p_{u_i}, \eta_{i,h})$ as encryption key of group where p_{u_i}=$m'_i\ PK_A$ and $SK_{g-u_i} = M'_i$ as decryption key of group.
5. The hardest part of this attack is counterfeiting the valid signature φ_j using the public key pk_{u_j} of the real sponsor u_j , the attacker u_i computes

$$z_{i,1} = (w_{i,1} - 1)^{-1}({w_{i,1}}^r - {w_{i,1}}^2) pk_{u_j}$$
$$z_{i,2} = (w_{i,2} - 1)^{-1}({w_{i,2}}^r - {w_{i,2}}^2) pk_{u_j}$$
$$\dots,$$
$$z_{i,r} = (w_{i,r} - 1)^{-1}({w_{i,r}}^r - {w_{i,r}}^2) pk_{u_j}$$

For simplicity let $B_{i,r} = (w_{i,r} - 1)^{-1}({w_{i,r}}^r - {w_{i,r}}^2)$

Then we find

$$z_{i,1} = B_{i,1} pk_{u_j}$$
$$z_{i,2} = B_{i,2} pk_{u_j}$$
$$\dots,$$
$$z_{i,r} = B_{i,r} pk_{u_j}$$

Simply, the fake signature is:

$$\varphi'_j = z_{i,1} + z_{i,2} + \cdots + z_{i,r}$$
$$\varphi'_j = (B_{i,1} + B_{i,2} + \cdots + B_{i,r}) pk_{u_j}$$

6. u_i broadcasts the authentication parameters $\{(y_{i,1}, y_{i,2}, \dots, y_{i,r}), (p_{u_i}, \eta_{i,h}), \varphi'_j\}$ to all terminals $u_k(i < k \le l, k \ne j)$. Every single member $u_k(i < k \le l, k \ne j)$ in the group who got the broadcasted authentication data $\{(y_{i,1}, y_{i,2}, \dots, y_{i,r}), (p_{u_i}, \eta_{i,h}), \varphi'_j\}$ from u_i, calculates $\phi_k = y_{i,1} + y_{i,2} + \cdots + y_{i,r}$ and verifies the signature and identity of u_i through the pairing equation $e(\varphi'_j, g_1) = e(\phi_k, pk_{u_j})$. We can prove that the previous equation holds as follows:

$\phi_k = y_{i,1} + y_{i,2} + \cdots + y_{i,r}$, where $y_{i,1} = f(w_{i,1}) =$

$$g_1 {w_{i,1}}^{r-1} + g_1 {w_{i,1}}^{r-2} + \cdots + g_1 {w_{i,1}}^2 + \eta_{,h} w_{i,1} + M_i'$$

From the summation of geometric series we consider:

$$y_{i,1} = (w_{i,1} - 1)^{-1}\left({w_{i,1}}^r - {w_{i,1}}^2\right)g_1 + \eta_{,h} w_{i,1} + M_i'$$
$$y_{i,2} = (w_{i,2} - 1)^{-1}\left({w_{i,2}}^r - {w_{i,1}}^2\right)g_1 + \eta_{,h} w_{i,2} + M_i'$$
$$\ldots,$$
$$y_{i,\mathrm{r}} = (w_{i,r} - 1)^{-1}\left({w_{i,r}}^r - {w_{i,1}}^2\right)g_1 + \eta_{,h} w_{i,\mathrm{r}} + M_i'$$

But $B_{i,r} = (w_{i,r} - 1)^{-1}\left({w_{i,r}}^r - {w_{i,r}}^2\right)$ and $M_i' = m_i'\eta_{,h}$ then we can write the previous equations in the following form:

$$y_{i,1} = B_{i,1} g_1 + \eta_{,h} w_{i,1} + m_i'\eta_{,h}$$
$$y_{i,2} = B_{i,2} g_1 + \eta_{,h} w_{i,2} + m_i'\eta_{,h}$$
$$\ldots,$$
$$y_{i,\mathrm{r}} = B_{i,r} g_1 + \eta_{,h} w_{i,\mathrm{r}} + m_i'\eta_{,h}$$

Finally, $\phi_k = y_{i,1} + y_{i,2} + \cdots + y_{i,r}$

$$= (B_{i,1} + B_{i,2} + \cdots + B_{i,r})g_1$$
$$+(w_{i,1} + w_{i,2} + \cdots w_{i,\mathrm{r}})\eta_{,h} + r\, m_i'\eta_{,h}$$

Then $\phi_k = (B_{i,1} + B_{i,2} + \cdots + B_{i,r})g_1$

$$+(w_{i,1} + w_{i,2} + \cdots w_{i,\mathrm{r}} + r\, m_i')\eta_{,h}$$

We can prove, simply that:

$(w_{i,1} + w_{i,2} + \cdots w_{i,\mathrm{r}} + r\, m_i')\eta_{,h} = (0,0)$ as

$$m_i' = -r^{-1}(w_{i,1} + w_{i,2} + \cdots w_{i,\mathrm{r}})$$

u_k finds the final value of

$\phi_k = (B_{i,1} + B_{i,2} + \cdots + B_{i,r})g_1$, let's check the pairing equation

$$e(\varphi_j', g_1) = e\left(\phi_k, pk_{u_j}\right)$$
$$RHS = e\left(\phi_k, pk_{u_j}\right)$$
$$= e\left((B_{i,1} + B_{i,2} + \cdots + B_{i,r})g_1, sk_{u_j} g_1\right)$$
$$= e(g_1, g_1)^{(B_{i,1} + B_{i,2} + \cdots + B_{i,r})sk_{u_j}}$$
$$LHS = e(\varphi_j', g_1)$$
$$= e\left((B_{i,1} + B_{i,2} + \cdots + B_{i,r})sk_{u_j} g_1, g_1\right)$$
$$= e(g_1, g_1)^{(B_{i,1} + B_{i,2} + \cdots + B_{i,r})sk_{u_j}}$$

$$LHS = RHS$$

It is clear the signature forgery is successful as the pairing equation holds.

7. u_k compares its authority or privilege value $\eta_{k,h}$ with the recieved privilege value $\eta_{i,h}$ of the attacker u_i. And finds it the same. He can check that the attribute permission value of him is identical to the permission values of the sponsor. (that means $\{K_{k,1} = K_{i,1}, K_{k,2} = K_{i,2}, \ldots, K_{k,r} = K_{i,r}\}$) .
8. u_k uses the values $\{K_{k,1}, K_{k,2}, \ldots, K_{k,r}\}$ and computes $w_{k,1} = H_2(K_{k,1}), w_{k,2} = H_2(K_{k,2}), \ldots, w_{k,r} = H_2(K_{k,r})$ then reconstructs a polynomial $f(x) = \sum_{\chi=1}^{r}\left(\prod_{1\le\varpi\le r,\varpi\neq\chi}\frac{x - w_{k,\varpi}}{w_{k,\chi} - w_{k,\varpi}}\right)y_{i,\chi}$ substituting the values $\{(w_{k,1}, y_{i,1}), (w_{k,2}, y_{i,2}), \ldots, (w_{k,r}, y_{i,r})\}$ using Lagrange Interpolation and computes the key $M_k = f(0) = \sum_{\chi=1}^{r}\left(\prod_{1\le\varpi\le r,\varpi\neq\chi}\frac{-w_{k,\varpi}}{w_{k,\chi} - w_{k,\varpi}}\right)y_{i,\chi} = M_i$ where M_i is decryption key.
9. u_k obtains the encryption key og group $PK_{g-u_k} = (p_{u_k}, \eta_{k,h}) = (p_{u_i}, \eta_{i,h})$ from the transmitted messages $\{(y_{i,1}, y_{i,2}, \ldots, y_{i,r}), (p_{u_i}, \eta_{i,h})\}$ by u_i.
10. All members of group $u_k (i < k \le l)$ could make sure of key correctness by checking this equation

$$e(p_{u_k}, \eta_{k,h}) = e(M_k, PK_A)$$

$$LHS = e(p_{u_k}, \eta_{k,h})$$
$$= e(m_i' SK_A g_1,\ SK_A(t_{k,1} + t_{k,2} + \cdots + t_{k,r})g_1)$$
$$= e(g_1, g_1)^{m_i' SK_A . SK_A(t_{k,1} + t_{k,2} + \cdots + t_{k,r})}$$
$$RHS = e(M_k, PK_A)$$
$$= e(m_i' \eta_{k,h},\ SK_A g_1)$$
$$= e(m_i' SK_A(t_{k,1} + t_{k,2} + \cdots + t_{k,r})g_1,\ SK_A g_1)$$
$$= e(g_1, g_1)^{m_i' SK_A . SK_A(t_{k,1} + t_{k,2} + \cdots + t_{k,r})}$$
$$LHS = RHS$$

Every member in group has ensured that his computed key is correct which means that our impersonation attack is successful.

D. *Fourth Loophole*

Non honest members with low number of attributes and different attributes can collude and exchange their secret attributes to get higher authority.

Attack 5. Let two non honest members u_1 and u_2 have sets of attributes $attr_1 = \{a_2,\ a_3,\ a_5, a_6\}$ and $attr_2 = \{a_1,\ a_4,\ a_6, a_7\}$ respectively. Every member have 3 attributes which are not subet of the other member attributes. If they shared their attributes between them $attr_1' = attr_2' = \{a_1, a_2,\ a_3, a_4,\ a_5,\ a_6\ , a_7\}$, now they got higher authority and became able to access non allowable information.

V. CONCLUSION

One of the most important methods for ensuring the secure transmission of information across groups is group key agreement. This study examined the flaws and loopholes in the proposed protocol, AA was able to figure out the value of any attributes sent to him without solving DLP and he did not need to perform any polynomial calculations which seemed to be useless so that the purpose of protocol could not be achieved and information was leaked. Any member u_i could pretend that he has more than his actual number of attributes which gives him a higher authority. We showed and proved that any non honest or illegal member u_i can pretend that he has higher number of fake attributes more than the actual number he has.

REFERENCES

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

[2] Lee, T. Lin, C. Tsai, "A New Authenticated Group Key Agreement In a Mobile Environment", Ann. Telecommun., vol. 64, no. 11-12, p. 735-744, 2009.

[3] Z. Qikun, L. Yongjiao, G. Yong, Z. Chuanyang, L. Xiangyang, and Z. Jun, "Group key agreement protocol based on privacy protection and attribute authentication," IEEE Access, vol. 7, pp. 87085–87096, 2019.

[4] S. Bala, G. Sharma, H. Bansal, T. Bhatia, "On the Security Of Authenticated Group Key Agreement Protocols", SCPE, vol. 20, no. 1, p. 93-99, 2019.

[5] 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.

[6] 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.

[7] 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.

[8] 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.

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

[10] 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.

[11] 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.

[12] 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.

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

[14] 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.

[15] 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.

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

[17] 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 fogenhanced IoT," J. Netw. Comput. Appl., vol. 125, pp. 82–92, Jan. 2019.

[18] J. Cui, X. Tao, J. Zhang, Y. Xu, and H. Zhong, "HCPA-GKA: A hash function-based conditional privacy-preserving authentication and groupkey agreement scheme for VANETs," Veh. Commun., vol. 14, pp. 15–25, Oct. 2018.
[19] 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.
[20] 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.
[21] X. Du and H. H. Chen, "Security in wireless sensor networks," IEEE Wireless Commun. Mag., vol. 15, no. 4, pp. 60–66, Aug. 2008.