Cryptanalysis and Improvement of a Flexible and Lightweight Group Authentication Scheme

Ali Rezapour and Zahra Ahmadian

***Abstract*—Shamir's secret sharing scheme is one of the substantial threshold primitives, based on which many security protocols are constructed such as group authentication schemes. Notwithstanding the unconditional security of Shamir's secret sharing scheme, protocols that are designed based on this scheme do not necessarily inherit this property. In this work, we evaluate the security of a lightweight group authentication scheme, introduced for IoT networks in IEEE IoT Journal in 2020, and prove its weakness against the linear subspace attack, which is a recently-proposed cryptanalytical method for secret sharing-based schemes. Then, we propose an efficient and attack-resistant group authentication protocol for IoT networks.**

***Index Terms*—Group authentication, IoT Networks, Linear Subspace Attack, Secret Sharing, Lightweight.**

I. Introduction

AUTHENTICATION is a mechanism that confirms or denies the identity of an entity, whether it is what it claims or is an intruder that has impersonated the identity of a valid entity. Traditionally, the authentication operation is accomplished between two nodes, a prover (who proves its identity) and a verifier (to whom the identity is proved). The verifier approves the proof if the prover is really the one that it claims. Nevertheless, this one-to-one authentication method is unsuitable when a potentially large group of users want to authenticate each other, simultaneously. In the classic two-party solution, the number of authentication processes required to be performed grows quadratically, i.e. $O(n^2)$, with the number of users. This complexity may become a bottleneck when a massive number of users are supposed to authenticate each other.

To address this problem, some group authentication protocols have been proposed in the literature [1]–[6] whose design is tailored to group-oriented applications. In this variant of the authentication protocols, all users (members) in a pre-defined group can be simultaneously verified. If all the users are legitimate, i.e. they belong to a pre-defined group, all of them can be authenticated by a single run of the group authentication. But, if there exist at least one non-member among them, the group authentication fails.

In group authentication, the group manager (GM) is responsible for the initial enrollment of all group members. During enrollment, the GM issues private credentials to the group members. Later, all users present in the group authentication process, perform the group authentication protocol without the cooperation of the GM to authenticate one another. Each user employs her credential to calculate a token and broadcast it. Following the authentication process, users use these released values to verify whether all users belong to the identical group. Group authentication schemes are based on the satisfaction of two security requirements. One requirement is that if illegitimate members do not exist in the group (all members are legal), the authentication should ever be successful. Another is that no non-member without the required credentials can feign to be a group member without being identified.

With the growth of the Internet-of-Things, [7], [8], many new applications requiring the authentication of a group of participants have been introduced. IoT networks generally have a three-layer design, called perception, network, and application layer which are shown in Fig. 1. The data is gathered via the perception layer by sensors and then it is transmitted over the network layer to servers and the cloud in the application layer. Users bind to the system over the cloud. Indeed, the perception layer consists of IoT nodes that are connected as a thing. The network layer, which includes routers and gateways, acts as an interface connecting the application layer to the perception layer. Nodes in an IoT network communicate with other nodes and connect to the internet.

Data Confidentiality and Integrity, along with authentication of nodes are the principal security concerns in any network, including the IoT networks. If we concentrate on the communications of nodes in the IoT network, we see that authentication is a primary process in the access control mechanism following which, all the other security operations and data exchange processes are done. However, these nodes have mostly little memory and limited processing power that need to be considered [9]. Accordingly, fast and lightweight authentication suggestions are needed to authenticate multi-user at once. However, this crisis is not well responded even in 5th generation networks, in the recent 3GPP Release. [10]. Group authentication is one of the hopeful answers as an alternative to numerous one-to-one authentication approaches. A large number of nodes in an IoT network can form one group based on some specifications like their coverage area or their functionality in the system. Rather than authenticating per node separately, all nodes in the group can be authenticated at the same time.

There are multiple proposed group authentication algorithms in the literature, which primarily are based on different mathematical tools such as tree-based structures, Shamir secret sharing, Chinese remainder theorem, error correcting code,

A. Rezapour is with the Department of Electrical Engineering, Iran University of Science and Technology, Tehran, Iran (e-mail: ali_rezapour@elec.iust.ac.ir)

Z. Ahmadian is with the Department of Electrical Engineering, Shahid Beheshti University, Tehran, Iran (e-mail: z_ahmadian@sbu.ac.ir)

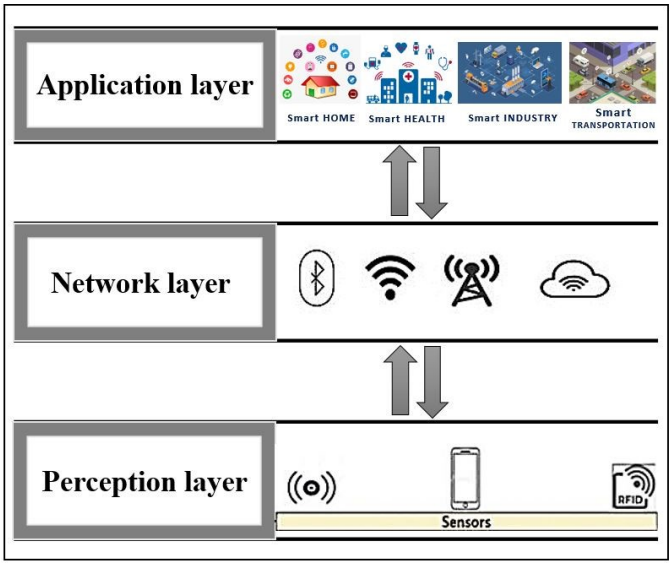

Fig. 1. The three-layered architecture of IoT.

and aggregate message authentication codes, some of which are lightweight, i.e. they achieve an effective authentication process for constrained devices in IoT networks. In [2], a lightweight group authentication along with a key distribution scheme is proposed. The proposed protocol make use of physically unclonable functions (PUF), the Chinese Remainder Theorem (CRT), and factorial tree. In [3], Ren et al. proposed a novel lightweight group authentication and transfer data scheme using PUF for NB-IoT in which the output of PUF is considered as the shared root key to achieving the mutual authentication along with a key agreement. In [4], Yang et al. proposed a group authentication protocol for RFID tags, in which a group of tags can efficiently authenticated each other, running just a single challenge/response procedure. In this study, they use bit-collision patterns where several tags belonging to a group, transmit the authentication responses simultaneously. The resulting response constructed by all the tag responses is a bit-collision pattern, which is a verifiable value and hence used for the purpose of authenticating the group of tags, at once. In [11], Xia et al. proposed a PUF-assisted lightweight group authentication and key agreement protocol in the smart home. In this scheme, the secret sharing technique and Chinese Remainder Theorem are utilized to establish the group session key between the user and smart devices.

In [10] a group authentication scheme is proposed by Aydin et al., which is claimed to be secure, flexible and lightweight. This protocol is called the FLGA protocol in this paper. The authors of [10] believed that in the previous group authentication protocols, the resource constraints imposed by the network is not well treated. So, they are not well-suited for IoT networks. Considering this demand, they proposed a group authentication protocol with the aim of providing flexibility and being lightweight. The FLGA protocol uses the secret sharing scheme and Elliptic curve cryptography (ECC) as its underlying primitives [10]. In order to perform a group authentication, the group members are required to perform only one elliptic curve point multiplication operation. Following the FLGA, several studies were proposed [6], [12]. For instance, [6] is built on the assumption that the terrestrial BS and UEs create a group and perform a group authentication using FLGA.

A. Our Contributions

In this paper, we use the linear subspace attack (LSA) approach [13] to prove the failure of the FLGA scheme proposed in [10] and demonstrates that this scheme does not have the claimed security and cannot achieve the safety features proposed by its authors in IoT networks. To be more precise, in the asynchronous communication model, the passive adversary can eavesdrop on the revealed tokens of legitimate nodes and then use released ones to forge a valid token. Following this, we employ the Anonymous Veto Networks (AV-net) to improve the FLGA scheme. Our proposed scheme does not impose any further calculations on the nodes compared to the FLGA scheme, resulting in an efficient lightweight group authentication scheme for IoT networks where its security can be reduced to some pre-defined and widely accepted basic rules with large enough complexity. Furthermore, our improved scheme does not allow an outsider with no credentials to successfully get authentication accessing a group of users; this includes impersonation attacks [5].

B. Paper Organization

The paper is organized as follows: In Section II, some preliminaries is outlined. A new representation and cryptanalysis of the FLGA scheme is brought in Section III. We introduce the improved group authentication protocol and analyze its security and efficiency in Sections IV and, respectively. Finally, Section VI concludes our work.

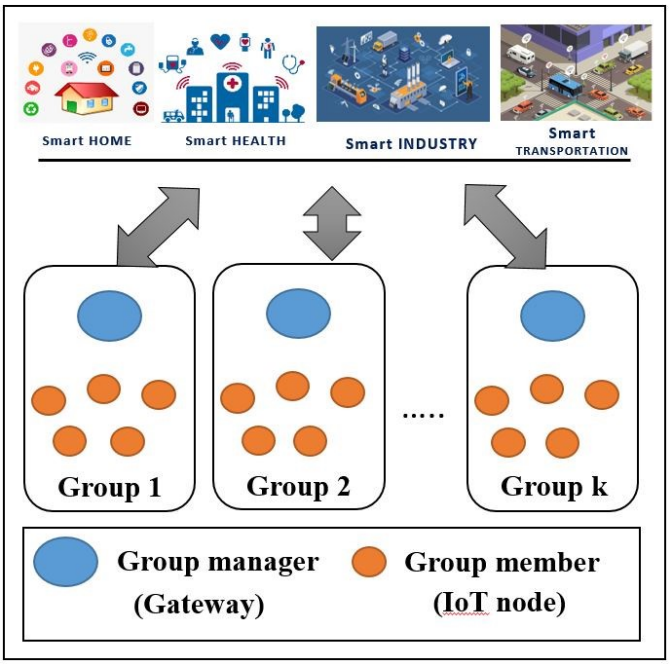

Fig. 2. FLGA's key motivation.

II. Preliminaries

Some preliminaries for the paper is presented here. Note that $|$ is used for the concatenation of two values and $|\cdot|$ denotes the set cardinality.

Definition 1. *Consider the equation of the form $y^3 = x^3 + ax + b$ where $a, b \in K$ and K is a finite field. An elliptic curve over a field K, $E(K)$, is the set of all points $(x, y) \in K^2$ on the above curve along with a point O at infinity.*

Definition 2 (Elliptic Curve Discrete Logarithm assumption)**.** *Let $E(K)$ be an elliptic curve group, and $P, Q \in E(K)$ such that $Q = aP$. Given (P, Q) it is assumed to be hard to find a (the problem of finding a is called the elliptic curve discrete logarithm problem (ECDLP)).*

Definition 3 (Shamir's (t, n) secret sharing scheme (SSS) [14])**.** *Assume that s is the secret supposed to be shared among n users, in such a way that any t or more than t users can reconstruct the secret, while any less than t shares reveals no information about the secret. This procedure is performed in two phases. In the share distribution phase, the dealer first chooses a random polynomial $f(x) = s + \sum_{j=1}^{t-1} a^j x^j \bmod p$ over Z_p of degree t–1. Then, it computes the share $f(x_i)$ and sends it to user $U_i, i = 1, \ldots, n$ through the secure channel. Here, $x_i \in Z_p$ is a public parameter associated with user U_i. In the secret reconstruction phase, any subset Ω of users, conditioned that $|\Omega| \geq t$, can recover the secret s following Lagrange interpolation formula*

$$s = \sum_{j \in \Omega} f(x_i) l_i \bmod p \tag{1}$$

where $l_i = \prod_{k \in \Omega, k \neq i} \frac{x_k}{x_k - x_i} \bmod p$ is called the Lagrange coefficient.

Definition 4 (Anonymous veto networks (AV-nets) [15])**.** *Let G be a finite cyclic group of a large prime order q, in which the discrete logarithm assumption holds, and g be the generator of G. Suppose that $\{U_i\}_{i \in Z_n}$ is the set of participating users, and they all agree on (G, g). The two rounds of the protocol are as below.*

Round 1. *Each user U_i randomly chooses $x_i \in Z_q$ and broadcasts g_i^x (zero-knowledge proof for the proof of the exponent x_i). User U_i also proves that she knows x_i without revealing it, e.g., by means of the Schnorr identification technique [16]. At the end of this round, each user computes $g^{y_i} = \frac{\prod_{k=1}^{i-1} g^{x_k}}{\prod_{k=i+1}^{n} g^{x_k}}$*

Round 2. *Each user broadcasts $g^{x_i y_i}$ and proves the knowledge of x_i within $g^{x_i y_i}$ without revealing it. Then, if no one vetoed we have $\prod_{i=1}^{n} g^{y_i x_i} = 1$. By definition of $y_i = \sum_{k<i} x_k - \sum_{k>i} x_k$, the above property always holds.*

III. Specification of the Flexible and Lightweight Group Authentication Scheme

According to the system model of FLGA [10], Fig. 2, the IoT nodes are divided into k groups, where each group contains n IoT nodes and a gateway node. The gateway, whose computational capability and memory are higher than IoT nodes, is responsible for executing the authentication in the group before the data transmission, hence it is called the group manager (GM). The GM and group members communicate via the insecure wireless channel. The structure of the groups may not include GM (without a central authority).

The FLGA scheme is composed of two main stages: Group authentication and Group key agreement. The former is composed of two phases including the initialization and confirmation phases.

A. Group Authentication Stage

Initially, GM chooses a cyclic group G of prime order q, and chooses P. GM selects an Encryption scheme (E, D) and a hash function $H(\cdot)$. A univariate polynomial $f(x)$ of degree $t-1$ over Z_q is selected by GM where $f(0) = s$ and s is the secret chosen by GM. GM computes the credentials $f(x_i), i = 1, \ldots, n$, where x_i is a public information (e.g. ID) of node U_i, and transmits them to the group members via the protected channel. GM computes $Q = sP$. Finally, GM shares the system parameters **params** $= \{P, Q, (E, D), H(\cdot), H(s), x_i\}$ with all group members. The authentication process is performed after the GM shares **params**.

There are two distinct scenarios in the confirmation phase: The centralized approach, where the GM participates in the group authentication stage. In this scenario, GM is responsible for authenticating the members of the group. The other scenario is the decentralized approach where all members of the group are responsible for authenticating the other members. Each member U_i computes $f(x_i)P$, and sends $(x_i, f(x_i)P)$ to GM and other members. In the centralized scenario, GM computes $f(x_i)P$ per member and confirms whether the values are valid or not. This type of authentication is a one-time use, and each authentication session demands a new initialization and credential generation.

In the decentralized scenario, suppose that m group members, $t \leq m \leq n$, participate in the confirmation phase. Each participating member computes and broadcasts $c_i = l_i f(x_i)P$, where $l_i = \prod_{k=1, k\neq i}^{m} \frac{x_k}{x_k - x_i} \bmod q$ is the Lagrange coefficient of Shamir's secret sharing scheme. c_i is called the token or released value of user U_i.

In order to verify whether all the participating members are legitimate, Each member checks the correctness of $\sum_{i=1}^{m} c_i = Q$. This variant of FLGA scheme is one-time use.

B. Group Key Agreement Stage

After the authentication has been performed, group members can communicate with each other using the secret s as the symmetric key. The group key is constructed by each group member according to the following procedure: Initially, each user U_i shares its own credential $f(x_i)$ with user U_j utilizing the symmetric key encryption scheme $E_{(f(x_i)f(x_j)P)}[f(x_i)]$. Once m decrypted values are received by U_j, it can compute $s' = \sum_{i=1}^{m} f(x_i) l_i$. Finally, if $H(s') = H(s)$, the group key is recovered. So, the participating members of the group can securely communicate with each other using the group key s.

IV. Cryptavalysis of the Flexible and Lightweight Group Authentication Scheme

Assume that m legitimate group members, $t \leq m \leq n$, are going to participate in the FLGA scheme, while an illegitimate member that here is the exact outside attacker seeks to impersonate a non-attendee legitimated member by forging its released value. we demonstrate that this attacker employs the linear subspace analysis method [13], [17] to forge a valid released value at the arbitrary point $x_{m'}$ by the information leaked from t released values, and it can pretend to be an authorized member (legitimate member for group) without being detected. In other words, any t valid tokens is enough to attain the whole information obtainable from all the m tokens in the authentication process. It is clear that these t tokens are achievable with the participation of only t-authorized members. Actually, we prove that this scheme is inefficient and insecure for the IoT network when more than t nodes participate in the confirmation phase.

In this section, we bring a new view for the FLGA scheme [10] in an algebraic framework, then we present the linear subspace attack on FLGA, accordingly.

Let us first rewrite the point $f(x_i)$ on univariate polynomial as

$$f(x_i) = \sum_{j=0}^{j=t-1} a_j x_i^j \bmod q = \mathbf{a}^T \mathbf{x}_i \tag{2}$$

where

$$\begin{aligned} \mathbf{a} &= [a_0, a_1, \ldots, a_{t-1}]^T \\ \mathbf{x}_i &= [1, x, \ldots, x^{t-1}]^T \end{aligned}$$

So each c_i can be rewritten as

$$c_i = \mathbf{a}^T \mathbf{x}_i l_i \times P \tag{3}$$

Now, we gather all $c_i, i = 1, ..., m$, into a vector $\mathbf{c}$ as follows:

$$\mathbf{c} = [c_1, c_2, \ldots, c_m] \tag{4}$$

Substituting (3) into $\mathbf{c}$ gives:

$$\begin{aligned} \mathbf{c} &= [\mathbf{a}^T \mathbf{x}_1 l_1 P, \mathbf{a}^T \mathbf{x}_2 l_2 P, \ldots, \mathbf{a}^T \mathbf{x}_m l_m P] \\ &= \mathbf{a}^T [\mathbf{x}_1 l_1 P, \mathbf{x}_2 l_2 P, \ldots, \mathbf{x}_m l_m P] \\ &= \mathbf{a}^T \mathbf{M} \end{aligned} \tag{5}$$

Where

$$\mathbf{M} = [\mathbf{x}_1 l_1 P, \mathbf{x}_2 l_2 P, \ldots, \mathbf{x}_m l_m P] \tag{6}$$

The linear system given in (5) plays an essential role in the LSA analysis of the scheme. The following theorem, which is proved in Appendix A, is the key part of the LSA method.

Theorem 1. *Let* $\mathbf{M}$ *be defined in* (6)*, then* $rank(\mathbf{M}) = t$ *for* $m \geq t$*.*

Proof. The proof is brought in Appendix A. □

This theorem is important since in LSA analysis, $rank(\mathbf{M})$ is closely related to the amount of information leaked from the tokens published by participants. Since $rank(\mathbf{M}) = t$, with more than t tokens no extra information would be obtained than that given by t tokens. So, any t tokens released by nodes provides the whole information for the attacker to mount the attack on the network. We can write the following equation:

$$\mathbf{c}_t = \mathbf{a}^T \mathbf{M}_t \tag{7}$$

where $\mathbf{c}_t$ and $\mathbf{M}_t$ are formed by the first to t^{th} column of vector $\mathbf{c}$ and matrix $\mathbf{M}$, respectively. Theorem 2, shows how the LSA attack is applied to the FLGA scheme.

Theorem 2. *If the attacker can solve the following system of equations*

$$\mathbf{M}_t \boldsymbol{\beta} = x_{m'} l_{m'} P \tag{8}$$

where $\boldsymbol{\beta} = [\beta_1, \beta_2, \ldots, \beta_t]^T \in {Z_q}^t$*, then he can forge the valid token* $c_{m'}, m' \notin \{1, ..., m\}$ *according to the following formula*

$$c_{m'} = \mathbf{c}_t \boldsymbol{\beta} \tag{9}$$

Proof. The proof is given in Appendix B. □

So, if the system given in (8) is solvable, the attacker succeeds to forge a valid token for the public parameter $x_{m'}$ associated with node $U_{m'}$. Finally, the attacker can pass the group authentication successfully since $\sum_{i=1}^{m} c_i = Q$. To examine the feasibility of the attack, we should study if system (8) is solvable.

Theorem 3. *The system of equations defined in* (8) *is always solvable.*

Proof. The proof is given in Appendix C. □

To conclude, according to our security analysis the group authentication scheme of [10] can be broken. In fact, an illegal node in the IoT networks can always wait until t legitimate nodes have revealed their tokens $(x_i, f(x_i)P)$ and then forge the token $c_{m'}$ of member $U_{m'}$ based on the revealed tokens without being detected. This is in contrary to one of the two fundamental security requirements for group authentication schemes.

V. An Improvement Of The FLGA Scheme

In this part of the paper, by considering the LSA attack, we will propose an improvement of FLGA scheme that not only resolves the weaknesses of FLGA [10], but also inspired from the method given in [18], provides some desirable aspects in practical usage. Users do not require new credentials in different authentication sessions and can reuse their credentials for multiple authentication sessions. This possibility of multiple use of credentials bypasses the bulky initialization processes for generating and broadcasting credentials prior to each authentication session. This is particularly useful in the distributed environments such as the IoT networks, especially considering the inherent constraints on nodes in these networks.

The system model of our scheme is based on the FLGA scheme though with some modifications. Our system model is introduced in two asynchronous applications. The security of the proposed scheme can be reduced to some widely-accepted computational hardness assumptions.

A. Asynchronous One-Time Group Authentication Scheme

Assume that there are n nodes and one GM in a group. Comparing to group members, GM has less resource limitations. The scheme has two phases: initialization and authentication phases.

1) Initialization Phase: GM selects a cyclic group G of prime order q and generator P. GM selects $s \in Z_q$ and computes $Q = sP$. GM assigns distinct x_i to the legal users U_i, where $i = 1, \ldots, n$ (group member registration). A univariate polynomial $f(x)$ of degree $t-1$ is randomly chosen over Z_q by GM where $f(0)$ is equal to secret s. GM computes the credential $f(x_i)$, $i = 1, \ldots, n$ and sends it to group member U_i securely trought a protected channel. Finally, GM outputs the public parameters $\textbf{params} = \{P, Q, q, \{x_i\}_{i=1,\ldots,n}\}$

2) Authentication phase: Suppose that Ω, with $|\Omega| \geq t$, is the subset of group members which are going to participate in the authentication phase. Every participating member U_i in Ω first selects $u_i \in Z_q$ randomly and broadcasts $u_i P$ (ECDLP). Then, it computes

$$v_i P = \sum_{j<i} u_j P - \sum_{j>i} u_j P \tag{10}$$

(AV-nets). Also, it computes and broadcasts its token as follows

$$c_i = l_i f(x_i) P + u_i v_i P \tag{11}$$

where l_i is the Lagrange coefficient. Once all the members released their tokens, each member computes $\sum_{i\in\Omega} c_i$ and verifies whether the equation $\sum_{i\in\Omega} c_i = Q$ holds. If yest, all members of the group authenticate each other, otherwise the group authentication fails.

B. Asynchronous Multiple-Time Group Authentication Scheme

In this approach, the same credentials can be reused in different group authentication sessions, which is reasonable for the asynchronous communication model. We know that the establishment of an asynchronous model is more convenient than a synchronous one in a distributed environment such as IoT.

1) Initialization Phase: GM picks a secure hash function $H(\cdot)$, a cyclic group G of large prime order q, and also k generators $\{R_i\}_{i=1,..,k}$ for group G. GM assigns distinct x_i to the legal users U_i, where $i = 1, \ldots, n$. GM then randomly chooses secret $s \in Z_q$, obtains $H(R_i s)$ for $i = 1, \ldots, k$, and randomly selects polynomial $f(x)$ of degree $t-1$ over Z_q, where $f(0) = s$. GM computes the credentials $f(x_i), i = 1, \ldots, n$. Then, it transmits each of these credentials to the corresponding group members via the secure channel. Finally, GM broadcasts public parameters:

$$\textbf{params} = \{H, G, q, \{R_i\}_{1,\ldots,k}, \{H(R_i s)\}_{1,\ldots,k}, \{x_i\}_{1,\ldots,n}\}$$

2) Authentication Phase: In the σ-th session ($\sigma \in Z_k$), each user $U_i \in \Omega$ attending the authentication phase, randomly chooses $u_i \in Z_q$ and broadcasts $u_i R_\sigma$. Then, it computes $v_i R_\sigma = \sum_{j<i} u_j R_\sigma - \sum_{j>i} u_j R_\sigma$. Then, each participating user computes and releases its token as follows.

$$c_i = l_i f(x_i) R_\sigma + u_i v_i R_\sigma \tag{12}$$

where l_i is the Lagrange coefficient. Finally, each user can verify the nonattendance of any illegitimate member by verifying the $H(\sum_{i\in\Omega} c_i) = H(R_\sigma s)$

VI. Security Analysis Of The Proposed Scheme

There are two main properties that the proposed scheme should meet, which are correctness and security.

A. Correctness

The group authentication scheme proposed in Sec. V provides the correctness property. If the set of participating nodes in the authentication phase is denoted by Φ, where $|\Phi| \geq t$:

$$\begin{aligned}\sum_{i\in\Phi} c_i &= \sum_{i\in\Phi} l_i f(x_i) R_\sigma + \sum_{i\in\Phi} u_i v_i R_\sigma \\ &= \sum_{i\in\Phi} l_i f(x_i) R_\sigma = R_\sigma s\end{aligned}$$

Concluding that the equation $H(\sum_{i\in\Phi} c_i) = H(R_\sigma s)$ holds, and the authentication will be successful.

B. Security.

The security of the suggested scheme is twofold: security against the inside adversary and security against the outside adversary.

Security against the inside adversary. The inside adversary is a malicious group member who authorized and owns a valid token and attempts to collude with other group members to recover the secret or generate a fresh valid token. Security against the inside adversary means that no information of the group member's credentials is leaked to the inside adversary due to the multiple execution of the protocol.

Security against the outside adversary. The outside adversary is a non-member external entity that does not have a valid credential or any other knowledge from the secret. It eavesdrops on the public parameters of the scheme (**params** vector) and released tokens of the previous sessions. Security against the outside adversary means that the outside adversary can not attain any information from the secret or forge a valid token of a non-attendee group member.
The outside adversary can benefit from the LSA method to forge valid tokens or retrieve the secret value. So, it is necessary to prove the resistance of our scheme against LSA.

1) The resistance against outside attacks (the no forgery property): Let us first provide an algebraic representation of our scheme. U_i's token, c_i in (12), can be rewritten as

$$c_i = \mathbf{a}^T \mathbf{x}_i l_i R_\sigma + u_i v_i R_\sigma \tag{13}$$

Without loss of generality, we assume that $u_1 < u_2 < \cdots < u_n$, therefore we have the following simple representation for $v_i R_\sigma = \sum_{j<i} u_j R_\sigma - \sum_{j>i} u_j R_\sigma$.

$$v_i R_\sigma = \mathbf{u}^T \mathbf{h}_i R_\sigma \tag{14}$$

Where

$$\begin{aligned}\mathbf{u} &= [u_1, u_2, \ldots, u_n]^T_{1\times n} \\ \mathbf{h}_i &= [1, \ldots, 1 \underbrace{0}_{i^{th}} -1, \ldots, -1]^T_{1\times n}\end{aligned}$$

So, c_i can be presented as follows.

$$c_i = \mathbf{a}^T \mathbf{x}_i l_i R_\sigma + u_i \mathbf{u}^T \mathbf{h}_i R_\sigma \tag{15}$$

We know that $u_i R_\sigma$ is a scalar value that is multiplied by the vector $\mathbf{h}_i$. So, the above relation is rewritten as follows:

$$c_i = \mathbf{a}^T \mathbf{x}_i l_i R_\sigma + \mathbf{u}^T \mathbf{h}_{u_i R_\sigma} \tag{16}$$

where $\mathbf{h}_{u_i R_\sigma} = u_i R_\sigma \mathbf{h}_i$. Now, the token vector $\mathbf{c}$ will be as follows.

$$\begin{aligned}\mathbf{c} &= [c_1, c_2, \ldots, c_n] \\ &= [\mathbf{a}^T \mathbf{x}_1 l_1 R_\sigma + \mathbf{u}^T \mathbf{h}_{u_1 R_\sigma} \ldots \mathbf{a}^T \mathbf{x}_n l_n R_\sigma + \mathbf{u}^T \mathbf{h}_{u_n R_\sigma}] \\ &= \mathbf{a}^T [\mathbf{x}_1 l_1 R_\sigma \ldots \mathbf{x}_n l_n R_\sigma] + \mathbf{u}^T [\mathbf{h}_{u_1 R_\sigma} \ldots \mathbf{h}_{u_n R_\sigma}]\end{aligned}$$

We define matrices $\mathbf{M} = [\mathbf{x}_1 l_1 R_\sigma, \ldots, \mathbf{x}_n l_n R_\sigma]$ and $\mathbf{H} = [\mathbf{h}_{u_1 R_\sigma}, \ldots, \mathbf{h}_{u_n R_\sigma}]$. So, the tokens vector $\mathbf{c}$ can be rewritten as follows

$$\begin{aligned}\mathbf{c} &= \mathbf{a}^T \mathbf{M} + \mathbf{u}^T \mathbf{H} \\ &= \mathbf{b}^T \mathbf{S}\end{aligned} \tag{17}$$

where $\mathbf{b} = \begin{bmatrix} \mathbf{a} \\ \mathbf{u} \end{bmatrix}$ and $\mathbf{S} = \begin{bmatrix} \mathbf{M} \\ \mathbf{H} \end{bmatrix}$.

Note that equation (17) is a system of linear equations in unknown vector $\mathbf{b}$. The coefficient matrix $\mathbf{S}$ is public while the right-hand constant vector $\mathbf{c}$ is the known tokens vector.

Suppose that the outside attacker aims to forge the n^{th} user's token i.e. c_n, using the LSA method while it has gathered the other remaining $n-1$ tokens. The following system of equation is constructed

$$c_n = \mathbf{c}_{n-1} \boldsymbol{\beta} \tag{18}$$

where $\mathbf{c}_{n-1}$ is the vector made by the first $n-1$ element of $\mathbf{c}$ and $\boldsymbol{\beta} = [\beta_1, \ldots, \beta_{n-1}]^T$. Similar to the LSA cryptanalysis of FLGA protocol, the system given in (18) is solvable if the following equation holds:

$$\mathbf{S}_{n-1} \boldsymbol{\beta} = \begin{bmatrix} \mathbf{x}_n l_n R_\sigma \\ \mathbf{h}_{u_n R_\sigma} \end{bmatrix} \tag{19}$$

According to the Rouch'e-Capelli Theorem [19], this system has a unique solution if

$$rank(\mathbf{S}_{n-1}) = rank(\left(\begin{array}{c|c} \mathbf{S}_{n-1} & \begin{matrix} \mathbf{x}_n l_n R_\sigma \\ \mathbf{h}_{u_n R_\sigma} \end{matrix} \end{array} \right)) \tag{20}$$

Since the right side of (19) is exactly the last column of $\mathbf{S}$, condition (20) is simplified to $rank(\mathbf{S}_{n-1}) = rank(\mathbf{S})$. However, our simulations shows that $\mathbf{S}$ is a full-rank matrix, i.e. $rank(\mathbf{S}) = n$. Therefore, the condition given in (20) does not hold which means that the forgery attack on the proposed scheme, using the LSA method is not possible.

2) Resistance against the inside attack (the no colluding property): This scheme can withstand the collusion of $t-1$ nodes,even if insiders have information from previous authentication sessions. Since, after collecting all the participating nodes $\Omega = \{U_1, U_2, \ldots, U_{t-1}\}$, they can compute $\sum_{i\in\Omega} u_i v_i R_\sigma = 0$ and the AV-nets protocol is satisfied. But since the secret values $(f(x_i), i = 1, .., n)$ are generated using a secret $t-1$ degree polynomial, the reconstruction phase of Shamir's (t, n) secret sharing scheme is never correctly performed with the participation of less than t nodes and the scheme can resist the collusion of up to $t-1$ insiders.

C. Discussion.

An important challenge in IoT networks is that after the authentication process a secure communication can be realized between the nodes. A solution for this purpose is to use different keys for different nodes. As the number of nodes grows, key distribution and key management would become a bottleneck in time, energy consumption, computations, and memory usage. Therefore, instead of using different keys for each node, the group key that was selected by the GM in the group authentication stage can be used as the group key. The issue is how the nodes recover the group key. To overcome this issue, FLGA proposes a key agreement protocol run by each node to share a key with others. In our scheme, due to the use of AV-nets protocol, an outside attacker can not obtain $f(x_i)P$, so despite the FLGA scheme [10], ours does not require a separate key agreement stage. In more details, instead of using different keys for each node, the secret chosen by the GM can be utilized as the group key. At the end of the group authentication stage, if $H(\sum_{i\in\Omega} c_i) = H(R_\sigma s)$ each node considers the secret $R_\sigma s$ as the group key for further communications. Our proposed scheme is a lightweight algorithm in IoT networks because resource-constrained nodes are not forced to heavy computations. Compared to the previous insecure scheme [10], group members must compute only one point of the AV-net protocol.

VII. Conclusion

By the use of the linear subspace attack as the cryptanalysis tool, we challenged the security claim in the FLGA scheme and presented a token forgery attack for this group authentication protocol. To fix this security flaw of FLGA, We made use of the AV-net to solve this issue and we have demonstrated that our modification also provides additional appropriate security features. Consequently, our suggested scheme can be safely used as an appropriate group authentication protocol for IoT networks. Because our scheme has no additional assumptions compared to the previous designs, it is compatible to IoT resource-constrained devices. Compared with other group authentication schemes based on Shamir's secret sharing method, the security of our scheme is proved by some well-studied complexity theoretic assumptions.

Additionally, As mentioned in [17], the linear subspace attack can be potentially employed to evaluate the security of the SSS-based schemes. In this method, first the attacker collects all the information published during the execution of the protocol from the released values in the scheme then creates a linear subspace spanned by these values with the highest possible dimension. Next, the dependency (belonging) of the secret parameters to this subspace is examined. There is a plenty of SSS-based cryptographic schemes that can be regarded as future targets for security evaluation using linear subspace attack.

Appendix A
Proof of Theorem 1

We perform a column operation to simplify matrix $\mathbf{M} = [\mathbf{x}_1 l_1 P, \mathbf{x}_2 l_2 P, \ldots, \mathbf{x}_m l_m P]$. Multiply the i^{th} column of $\mathbf{M}$, $i = 1, \ldots, m$, by ${l_i}^{-1} \bmod q$. The resulting matrix is $\mathbf{M}^{(1)} = [\mathbf{x}_1, \ldots, \mathbf{x}_m]P$. The matrix $\mathbf{M}^{(1)}$ is a $t \times m$ Vandermonde matrix. So $rank(\mathbf{M}) = rank(\mathbf{M}^{(1)}) = min\{t, m\} = t$.

Appendix B
Proof of Theorem 2

In order to proof this theorem, two sides of equation (7) are first multiplied by the solution vector $\boldsymbol{\beta}$ from right. Then, using equations (8) and (3), we obtain

$$\begin{aligned} \mathbf{c}_t &= \mathbf{a}^T \mathbf{M}_t \\ \mathbf{c}_t\boldsymbol{\beta} &= \mathbf{a}^T \mathbf{M}_t \boldsymbol{\beta} \\ &= \mathbf{a}^T \mathbf{x}_{m'} l_{m'} P \\ &= c_{m'} \end{aligned} \tag{21}$$

Appendix C
Proof of Theorem 3

The system $\mathbf{M}_t\boldsymbol{\beta} = \mathbf{x}_{m'} l_{m'} P$ is consistent (has solution) if and only if $rank(\mathbf{M}) = rank([\mathbf{M} \mid \mathbf{x}_{m'} l_{m'} P])$[12]. Based on the proof of Theorem 1, $rank(\mathbf{M}) = t$. On the other hand, new matrix $[\mathbf{M} \mid \mathbf{x}_{m'} l_{m'} P]$ is a $t \times (t+1)$ Vandermonde matrix, having the same structure of $\mathbf{M}$. So $rank(\mathbf{M}) = min\{t, t+1\} = t$. To be specific, vector $\mathbf{x}_{m'} l_{m'} P$ belongs to the column space of $\mathbf{M}$. Hence, the linear system of equations given by (8) is always solvable.

References

[1] L. Harn, "Group authentication," *IEEE Transactions on computers*, vol. 62, no. 9, pp. 1893–1898, 2012.

[2] H. Yıldız, M. Cenk, and E. Onur, "Plgakd: A puf-based lightweight group authentication and key distribution protocol," *IEEE Internet of Things Journal*, vol. 8, no. 7, pp. 5682–5696, 2020.

[3] X. Ren, J. Cao, M. Ma, H. Li, and Y. Zhang, "A novel puf-based group authentication and data transmission scheme for nb-iot in 3gpp 5g networks," *IEEE Internet of Things Journal*, 2021.

[4] A. Yang, D. Boshoff, Q. Hu, G. P. Hancke, X. Luo, J. Weng, K. Mayes, and K. Markantonakis, "Privacy-preserving group authentication for rfid tags using bit-collision patterns," *IEEE Internet of Things Journal*, vol. 8, no. 14, pp. 11 607–11 620, 2021.

[5] R. Xu, X. Wang, and K. Morozov, "Group authentication for cloud-to-things computing: Review and improvement," *Computer Networks*, vol. 198, p. 108374, 2021.

[6] Y. Aydin, G. K. Kurt, E. Ozdemir, and H. Yanikomeroglu, "Group handover for drone base stations," *IEEE Internet of Things Journal*, vol. 8, no. 18, pp. 13 876–13 887, 2021.

[7] S. Kim, J. Y. Choi, and J. Jeong, "On authentication signaling costs in hierarchical lte networks," in *2014 7th International Conference on Ubi-Media Computing and Workshops*. IEEE, 2014, pp. 11–16.

[8] J. Li, M. Wen, and T. Zhang, "Group-based authentication and key agreement with dynamic policy updating for mtc in lte-a networks," *IEEE Internet of Things Journal*, vol. 3, no. 3, pp. 408–417, 2015.

[9] H. Suo, J. Wan, C. Zou, and J. Liu, "Security in the internet of things: a review," in *2012 international conference on computer science and electronics engineering*, vol. 3. IEEE, 2012, pp. 648–651.

[10] Y. Aydin, G. K. Kurt, E. Ozdemir, and H. Yanikomeroglu, "A flexible and lightweight group authentication scheme," *IEEE Internet of Things Journal*, vol. 7, no. 10, pp. 10 277–10 287, 2020.

[11] Y. Xia, R. Qi, S. Ji, J. Shen, T. Miao, and H. Wang, "Puf-assisted lightweight group authentication and key agreement protocol in smart home," *Wireless Communications and Mobile Computing*, vol. 2022, pp. 1–15, 2022.

[12] X. Wu, F. Ren, Y. Li, Z. Chen, and X. Tao, "Efficient authentication for internet of things devices in information management systems," *Wireless Communications and Mobile Computing*, vol. 2021, pp. 1–14, 2021.

[13] Z. Ahmadian and S. Jamshidpour, "Linear subspace cryptanalysis of harn's secret sharing-based group authentication scheme," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 2, pp. 502–510, 2017.
[14] A. Shamir, "How to share a secret," *Communications of the ACM*, vol. 22, no. 11, pp. 612–613, 1979.
[15] F. Hao and P. Zieliński, "A 2-round anonymous veto protocol," in *International Workshop on Security Protocols*. Springer, 2006, pp. 202–211.
[16] C.-P. Schnorr, "Efficient signature generation by smart cards," *Journal of cryptology*, vol. 4, no. 3, pp. 161–174, 1991.
[17] S. Jamshidpour and Z. Ahmadian, "Security analysis of a dynamic threshold secret sharing scheme using linear subspace method," *Information Processing Letters*, vol. 163, p. 105994, 2020.
[18] Z. Xia, Y. Liu, C.-F. Hsu, and C.-C. Chang, "Cryptanalysis and improvement of a group authentication scheme with multiple trials and multiple authentications," *Security and Communication Networks*, vol. 2020, 2020.
[19] S. Banerjee and A. Roy, *Linear algebra and matrix analysis for statistics*. Crc Press Boca Raton, FL, USA:, 2014, vol. 181.