面向物联网的轻量级可验证群组认证方案

陈书仪[1,2,3],刘亚丽[1,2,3],林昌露[2],李 涛[1,2,3],董永权[1]
(1. 江苏师范大学计算机科学与技术学院,江苏徐州 221116; 2. 福建师范大学福建省网络安全与密码技术重点实验室,
福建福州 350007;3. 河南省网络密码技术重点实验室,河南郑州 450001)

摘 要: 随着物联网应用的广泛扩展,越来越多的物联网设备出现在人们的日常生活中,包括智能电表、智能家居、智能穿戴等. 它们在带给人民生活便利的同时,由于物联网设备通过无线开放信道进行交互,造成诸多安全和隐私问题的出现. 身份认证是解决物联网安全和隐私问题的关键技术之一. 传统的点对点认证方案没有考虑到物联网海量节点和节点资源受限的情况,而群组认证是一种一次验证一组成员身份的认证技术,为物联网节点的身份认证提供了新的思路. 然而,现有适用于物联网场景的群组认证方案存在安全隐患,无法抵抗伪造、重放等恶意攻击并且无法防止群组管理者对组成员的欺骗. 本文利用可验证秘密共享技术设计了一种适用于物联网场景的轻量级可验证群组认证方案以抵抗群组管理者的欺骗行为. 另外,在物联网场景下,节点可能会动态地加入和撤出网络,针对这种情况,本文在可验证群组认证方案的基础上设计密钥更新环节以更新组成员的权限. 安全性分析表明,本文方案满足正确性、机密性,能够抵抗重放、伪造、冒充等恶意攻击. 性能分析和实验仿真表明,与现有典型的物联网群组认证方案相比,本文方案在保证安全性的同时降低了组成员的计算代价.

关键词: 群组认证; 物联网; 轻量级; 可验证秘密共享; 动态群组
中图分类号: TP309 **文献标识码:** A **文章编号:** 0372-2112(2022)04-0990-12
电子学报 URL:http://www.ejournal.org.cn **DOI:**10.12263/DZXB.20211028

Lightweight Verifiable Group Authentication Scheme for the Internet of Things

CHEN Shu-yi[1,2,3], LIU Ya-li[1,2,3], LIN Chang-lu[2], LI Tao[1,2,3], DONG Yong-quan[1]
(1. *College of Computer Science and Technology, Jiangsu Normal University, Xuzhou, Jiangsu* 221116, *China*;
2. *Fujian Provincial Key Laboratory of Network Security and Cryptology, Fujian Normal University, Fuzhou, Fujian* 350007, *China*;
3. *Henan Key Laboratory of Network Cryptography Technology, Zhengzhou, Henan* 450001, *China*)

Abstract: With the wide spread of the applications of the internet of things (IoT), more and more IoT devices appear in our lives, including smart meters, smart homes, smart wear and so on. While they bring convenience to people′s lives, many security and privacy issues arise because of the interaction of IoT devices through wireless open channels. Identity authentication is one of the key technologies to solve the security and privacy issues of IoT. The traditional point-to-point authentication schemes do not consider the massive resource-limited nodes, while group authentication is an authentication technology that can simultaneously verify a group of members, which provides a new idea for the authentication of IoT nodes. However, the existing group authentication schemes for IoT are vulnerable to some security risks, which cannot resist malicious attacks such as forgery attack, replay attack and cannot prevent the group manager from cheating group members. In this paper, a lightweight verifiable group authentication scheme for IoT based on verifiable secret sharing technology is proposed, which resists the deception of the group manager. In addition, nodes may dynamically join or leave the network in IoT scenarios. Given this situation, key updating based on the verifiable group authentication scheme is designed to

收稿日期:2021-08-01;修回日期:2022-01-05;责任编辑:崔兴华
基金项目:国家自然科学青年基金(No.61702237);国家自然科学基金面上项目(No.61872168);国家自然科学基金促进海峡两岸科技合作联合基金(No.U1705264);福建省网络安全与密码技术重点实验室(福建师范大学)开放课题(No.NSCL-KF2021-04);河南省网络密码技术重点实验室研究课题(No.LNCT2021-A07);江苏省研究生科研与实践创新计划项目(No.KYCX20_2381);江苏师范大学研究生科研与实践创新计划项目(No.2021XKT1387);江苏省自然科学青年基金(No.BK20150241);徐州市推动科技创新专项资金项目(No.KC18005);江苏省高校自然科学基金(No.14KJB520010);福建省自然科学基金(No.2019J01275);江苏政府留学奖学金

update group members′ authority. Security analysis shows that this scheme satisfies the correctness and confidentiality, and it can resist malicious attacks such as replay attack, forgery attack, impersonation attack. Performance analysis and experimental simulation show that this scheme reduces the computational cost of group members while it ensures security compared with the existing typical group authentication schemes for IoT.

Key words: group authentication; the internet of things; lightweight; verifiable secret sharing; dynamic group

1 引言

物联网(the Internet of Things,IoT)是一种新型的网络技术,它将各种信息传感设备与互联网相结合形成一个巨大的网络,实现在任何时间、任何地点,人与设备的互联互通. 物联网中的任何一个设备可以定义为一个虚拟节点或物理节点,所有节点通过网络相互连接并交换信息. 如图1所示,物联网通常具有3层架构[1,2],包括传感层、网络层和应用层. 传感层由具有各种传感能力的物联网节点组成;网络层将传感器的数据传输到服务器;应用层将传感层得到的数据进行处理,并实现具体的应用. 物联网节点之间通过开放信道实现交互,而开放的信息交互存在安全和隐私泄露问题. 目前,身份认证是解决这些问题的关键技术之一.

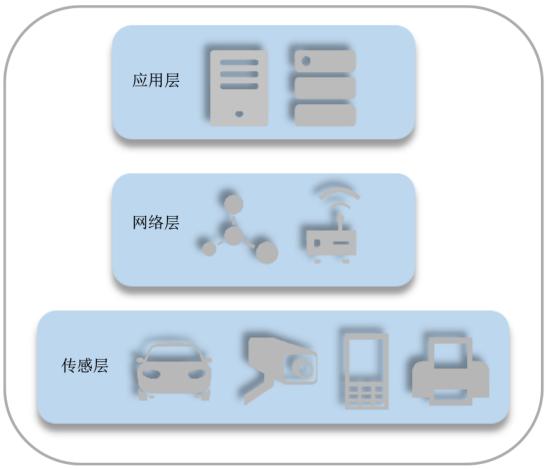

图1　物联网的3层架构

身份认证在物联网中具有广泛的应用. 张顺等人[3]提出了一种无线体域网(Wireless Body Area Network,WBAN)场景下的认证方案,该方案使用椭圆曲线技术实现了用户和医疗中心的相互认证. Fouda等人[4]提出了一种面向智能电网的认证方案,该方案使用联合会话密钥和哈希函数实现了分布式智能电表和智能设备之间的相互认证. 房卫东等人[5]在无线传感器网络(Wireless Sensor Network,WSN)场景下,使用生物特征标识技术实现了用户和传感器节点之间的双向认证. 张文芳等人[6]在车联网(Vehicular Ad Hoc Network,VANET)场景下提出一种基于无证书聚合签名的匿名认证与密钥协商方案. 李涛等人[7]提出了一种基于双物理不可克隆函数(Physical Unclonable Function,PUF)的无线射频识别(Radio Frequency Identification,RFID)认证方案,实现阅读器与标签的双向认证.

大多数物联网认证方案是节点之间一对一的认证方案,节点之间通过交互来验证身份信息. 然而这种认证方案并不适用于物联网. 一方面,物联网节点内存小、功耗低的特性无法支持较大的通信开销和复杂的计算;另一方面,物联网的节点数量越来越多,认证服务器无法同时处理大量的认证请求. 越来越多的物联网应用需要有效地对大量节点进行认证,这种应用场景需要一种新型的身份认证方案,能够同时一次验证一组节点的合法性,以节省成本和提高效率. 因此,需要设计面向物联网的轻量级群组认证方案.

群组认证[8]是单个或多个验证者对一组成员的身份进行认证. 在物联网场景下,群组认证可以实现一次对一组节点的认证,群组认证模型相较于传统认证模型,更加适用于海量认证请求的物联网场景,它可以有效地解决节点资源受限的问题. 因此研究物联网场景下的群组认证方案对于解决目前物联网中群体身份认证问题具有重要的研究意义和实践价值.

在实现群组认证的方法中,Shamir秘密共享技术[9]是一种高效、低代价的方法. Harn[8]的方案将Shamir秘密共享技术应用于群组认证上,相比于传统的认证方案,不需要每个节点之间进行一对一的认证,节约了计算和通信代价. 然而Ahmadian等人[10]指出Harn的方案是不安全的,攻击者可以通过线性子空间攻击来伪造一个有效的认证令牌,而不用恢复任何多项式,攻击者可以在不被检测到的情况下模拟一个组成员,从而通过身份认证. 随后,Chien[11]提出了一种基于双线性配对的群组认证方案,该方案的安全性基于椭圆曲线离散对数困难问题,每一轮群组认证都使用不同的本原元加密私钥,避免了群组认证过程中受到重放攻击. 然而,Xia等人[12]指出该方案无法抵抗伪造攻击,由于拉格朗日系数公开可计算,攻击者可以通过修改认证令牌中的拉格朗日系数来生成一个新的有效令牌. Aydin等人[13]在Harn和Chien的群组认证方案基础上,提出了一种轻量的群组认证方案;在群组认证时,组成员只进行简单的累加运算,具有较低的计算开销,但是该方案仍无法抵抗伪造攻击,攻击者可以修改认证令牌中的拉格朗日系数来重构一个新的有效令牌从而通过群组认证,而无须破解椭圆曲线离散对数困难问题,同

时,该方案无法抵抗重放攻击,攻击者可以重放合法组成员的认证令牌从而通过下一轮的群组认证. 随后,Xia 等人[12]提出使用匿名否决网络算法(Anonymous Veto Networks,AV-net)解决令牌被篡改的问题,然而他的方案没有考虑群组管理者欺骗的问题,群组管理者可能分发错误的私钥导致组成员无法通过群组认证,同时,该方案在群组认证阶段使用双线性配对,耗费了更多的计算代价.

综合现有的群组认证方案,现有研究工作存在以下问题.

(1)现有大多数的群组认证方案计算代价高,无法适用于资源受限的物联网场景. 物联网传感层的节点往往具有有限的内存、严格的能量限制,而且处理能力非常有限. 因此,在身份认证过程中,应该尽可能减少物联网节点上的计算开销.

(2)现有大多数的基于秘密共享技术的群组认证方案无法抵抗伪造攻击,攻击者可以通过修改认证令牌中的拉格朗日系数来伪造一个合法令牌,从而通过群组认证.

(3)现有大多数的群组认证方案无法抵抗重放攻击. 在物联网场景下,物联网节点之间通信的延时可能导致群组认证未能一次通过,如果物联网节点再次进行群组认证,攻击者可以截取上一轮的认证令牌进行重放,从而通过群组认证.

(4)现有群组认证方案均没有考虑群组管理者欺骗的问题,组成员全盘接受群组管理者分发的私钥. 在物联网场景下,群组管理者可能是网关或者其他具有高计算能力、高存储能力的物联网节点,然而,这些群组管理者可能给予部分合法组成员错误的私钥,导致这些组成员始终无法通过群组认证.

在物联网场景下,节点往往是动态变化的,新节点可以加入网络,旧节点可以离开网络. 例如:在无线体域网场景下,人体携带的医学传感器作为一组物联网节点,根据病人的需求动态变化[14];在车联网的场景下,同一区域的车作为一组物联网节点,会驶入或驶出当前区域[15]. 然而,文献[11~13]的群组认证方案尚未考虑节点加入和撤出的情况,当节点动态变化时,新节点可以使用分配的私钥通过群组认证,撤出的节点无法利用原有的私钥通过群组认证,所以群组管理者需要更新节点的私钥以实现权限的分配或撤销.

综上所述,设计一种适用于物联网场景的、轻量的、安全的、可验证的、支持组成员动态变化的群组认证方案是亟待解决的问题.

为了解决现有群组认证方案存在的以上问题,本文提出了一种面向物联网的轻量级可验证群组认证方案. 本文的主要贡献如下.

(1)本文创新性地在物联网场景下将私钥可验证思想应用于群组认证方案,对群组管理者分发的私钥进行验证,有效地防止了群组管理者的欺骗行为.

(2)本文提出了一种基于秘密共享技术的轻量级群组身份认证方案,克服了一对一身份认证存在的局限性,可以用于物联网分散式的群组身份认证场景.

(3)本文支持组成员的动态加入和撤出,群组管理者动态地更新私钥以实现组成员权限的分配或撤销,而不需要为组内所有组成员重新分配私钥.

(4)本文方案满足正确性、机密性,并且可以抵抗伪造、重放、冒充等恶意攻击,具有较好的安全性.

(5)与现有典型的群组认证方案相比,本文方案具有较低的计算开销,满足资源受限节点的轻量级群组认证的需求. 更加适用于海量认证请求的物联网场景.

2 准备工作

本节主要介绍本文方案所使用的理论基础,并且给出了本文方案的安全性定义.

2.1 理论基础

定义 1 (Shamir秘密共享方案[9])秘密共享方案包含 n 个组成员 $\{U_1,U_2,\cdots,U_n\}$ 和秘密拥有者 D. D 将秘密分发给 n 个组成员,至少 $k(k\leqslant n)$ 个组成员可以恢复秘密,其中 k 是恢复秘密的门限. 方案的具体步骤如下.

(1)**初始化阶段**. 在有限域 Z_q(q 为大素数)上,D 选择一个 $(k-1)$ 次的多项式 $f(x)=\sum_{i=0}^{k-1}a_i x^i \pmod q$,$s$ 作为秘密存储在第一个系数 a_0 中.

(2)**秘密分发阶段**. 秘密的拥有者根据组成员 U_i 的公开身份信息 x_i 计算 $s_i=f(x_i)\pmod q$ 作为组成员 U_i 的秘密份额,并把 s_i 通过秘密信道分发给组成员 U_i,其中 $1\leqslant i\leqslant n$.

(3)**秘密重构阶段**. 当组成员想要恢复秘密 s,他们只需 k 个组成员的秘密份额便可以重构出多项式 $f(x)=\sum_{i=1}^{k}f(x_i)\mu_i \pmod q$,其中 $\mu_i=\prod_{j=1,j\neq i}^{k}\frac{x-x_j}{x_i-x_j}$,进一步可以得到秘密 $s=f(0)=a_0$.

在此方案中,素数 q 需要大于秘密 s 和组成员总数 n 并且公开,而随机选择的多项式系数 $a_1,a_2,\cdots,a_{k-1}$ 是秘密信息,需要保密,在生成 n 个秘密份额后销毁.

定义 2 (双线性配对[16])双线性配对满足映射 $e(\cdot)$: $G_1\times G_2\rightarrow G_T$,其中 G_1 和 G_2 是阶为 q 的加法循环群,G_T 是阶为 q 的乘法循环群,双线性配对满足如下 3 个性质.

(1)**双线性**. 对于 $P_1,P_2\in G_1,Q\in G_2$ 且 $a,b\in Z_q$,存在.

$$e(aP_1,bQ)=e(P_1,Q)^{ab}$$

$$e(P_1+P_2,Q)=e(P_1,Q)\,e(P_2,Q)$$

(2)**非退化性**. 对于任意点 $P\in G_1,Q\in G_2$,有 $e(P,Q)\neq 1$,反之亦然.

(3)**可计算性**. 在多项式时间内,对于所有 $(P,Q)\in G_1\times G_2,e(P,Q)$ 的值是可有效计算的.

2.2 安全性定义

在文献[12]的基础上,本节给出可验证群组认证方案安全性证明的相关定义.

定义 3 (敌手模型)本文假设敌手分为内部敌手 A_I 和外部敌手 A_O,敌手的具体定义如下.

(1)**内部敌手 A_I** 假设参与群组认证的人数为 $m,k\leqslant m\leqslant n$,其中 k 是群组认证人数的门限值,n 是组成员数量,内部敌手 A_I 最多控制 $k-1$ 个组成员,A_I 可以获得这些组成员的私钥和秘密信息,它的目的是获取未被控制组成员的私钥并且伪造认证令牌通过群组认证.

(2)**外部对手 A_O** 外部敌手 A_O 不拥有任何组成员的有效私钥,它的目的是在未被检测到的情况下冒充组成员.

定义 4 (通信模型)本文假设群组管理者(Group Mananger,GM)和每个组成员之间存在一个安全的信道,以便私钥可以安全地分发而不会泄露,并且假设组成员都可以连接到一个广播频道,通过这个频道发送的任何消息都可以在某些特定的时间范围内被其他组成员听到.

定义 5 (可验证群组认证模型)一个可验证群组认证模型包括 5 种算法:初始化算法 Init(λ)、私钥分发算法 Dist($\{x_i\}_{i\in[1,n]}$)、私钥验证算法 Veri(s_i,params)、认证令牌生成算法 Comp(params,φ,$\{x_i\}_{i\in[1,m]},s_i$)和群组认证算法 Auth(params,$\{c_i,r_iP\}_{i\in[1,m]}$).

(1)**Init**(λ) 初始化算法由 GM 运行. 以安全参数 λ 作为输入,系统参数 params 作为输出.

(2)**Dist**($\{x_i\}_{i\in[1,n]}$) 私钥分发算法由 GM 运行. 以组成员公开身份信息集合 $\{x_i\}_{i\in[1,n]}$ 作为输入,输出组成员私钥集合 $\{s_i\}_{i\in[1,n]}$,并通过安全信道发送给组成员.

(3)**Veri**(s_i,params) 私钥验证算法由每个组成员运行. 将组成员私钥 s_i 和系统参数 params 作为输入,如果私钥验证成功,则输出 1,否则输出 0.

(4)**Comp**(params,φ,$\{x_i\}_{i\in[1,m]},s_i$) 认证令牌生成算法由每个参与群组认证的组成员运行. 假设参与群组认证的组成员为 $\{U_1,U_2,\cdots,U_m\}$,将系统参数 params、会话索引 φ、参与群组认证组成员的公开身份信息集合 $\{x_i\}_{i\in[1,m]}$ 和私钥 s_i 作为输入,输出认证令牌 $\{c_i,r_iP\}$.

(5)**Auth**(params,$\{c_i,r_iP\}_{i\in[1,m]}$) 群组认证算法由每个参与群组认证的组成员运行. 将系统参数 params 和一组认证令牌 $\{c_i,r_iP\}_{i\in[1,m]}$ 作为输入,如果群组认证成功,则输出 1,否则输出 0.

针对上述所定义的可验证群组认证模型,要求其满足以下正确性和安全性要求.

(1)**正确性**. 如果参与群组认证的组成员为 $\{U_1,U_2,\cdots,U_m\}$,并且他们都是合法的组成员,则群组认证通过. 形式上,如果满足

$$\begin{aligned}&\Pr[\text{params}\leftarrow\text{Init}(\lambda);\{s_i\}_{i\in[1,n]}\leftarrow\text{Dist}(\{x_i\}_{i\in[1,n]}),\\&\text{Veri}(s_i,\text{params})=1|_{i\in[1,n]},\\&\{c_i,r_iP\}\leftarrow\text{Comp}(\text{params},\varphi,\{x_i\}_{i\in[1,m]},s_i)|_{i\in[1,m]},\\&\text{Auth}(\text{params},\{c_i,r_iP\}_{i\in[1,m]})=1]=1\end{aligned}$$

群组认证方案具有正确性. 在上述表达式中,$\Pr(X)$ 表示事件 X 发生的概率.

(2)**机密性**. 内部敌手 A_I 无法在群组认证过程中获得未被控制的组成员的任何秘密信息. 形式上,如果满足

$$\begin{aligned}&\Pr[\text{View}_{A_I}(\text{Real}_{\chi}(\lambda,\text{params}))]\\&-\Pr[\text{View}_{A_I}(\text{SIM}_S(\lambda,\text{params}))]<\varepsilon(\lambda)\end{aligned}$$

群组认证方案具有机密性. 在上述表达式中,$\text{View}_{A_I}(\text{Real}_{\chi}(\lambda,\text{params}))$ 表示在实际运行方案 χ 中内部敌手 A_I 的视图,而 $\text{View}_{A_I}(\text{SIM}_S(\lambda,\text{params}))$ 表示以公共信息为输入的模拟机 S 模拟的方案中 A_I 的视图,$\varepsilon(\lambda)$ 表示关于参数 λ 的可忽略的函数.

(3)**不可伪造性**. 内部敌手 A_I 无法伪造认证令牌通过群组认证. 形式上,如果满足

$$\begin{aligned}&\Pr[\text{params}\leftarrow\text{Init}(\lambda);\{s_i\}_{i\in[1,n]}\leftarrow\text{Dist}(\{x_i\}_{i\in[1,n]}),\\&\text{Veri}(s_i,\text{params})=1|_{i\in[1,n]},\\&C\leftarrow A_I^R(\text{params},Z,\{x_i\}_{i\in[1,m]},\{s_i\}_{i\in U_A}),\\&(\varphi\notin Z)\wedge\text{Auth}(\text{params},C)=1]<\varepsilon(\lambda)\end{aligned}$$

群组认证方案具有不可伪造性. 在上述表达式中,U_A 表示由 A_I 控制的组成员集合,满足 $U_A\subset U$ 且 $\left|U_A\right|\leqslant k-1$. R 表示用于请求群组认证服务的模拟机,Z 表示已请求会话的索引集合,$\varepsilon(\lambda)$ 表示关于参数 λ 的可忽略的函数.

(4)**不可冒充性**. 外部敌手 A_O 无法冒充一个组成员. 形式上,如果满足

$$\begin{aligned}&\Pr[\text{params}\leftarrow\text{Init}(\lambda);\{s_i\}_{i\in[1,n]}\leftarrow\text{Dist}(\{x_i\}_{i\in[1,n]}),\\&\text{Veri}(s_i,\text{params})=1|_{i\in[1,n]},\\&\{c_i,r_iP\}\leftarrow\text{Comp}(\text{params},\varphi,\{x_i\}_{i\in[1,m]}\cup\{x_\mu\},\\&s_i)|_{i\in[1,m]},\\&\{c_\mu,r_\mu P\}\leftarrow A_O(\text{params},\varphi,\{x_i\}_{i\in[1,m]}\cup\{x_\mu\},\\&\{c_i,r_iP\}_{i\in[1,m]}),\\&\text{Auth}(\text{params},\{c_i,r_iP\}_{i\in[1,m]\cup\{\mu\}})=1]<\varepsilon(\lambda)\end{aligned}$$

群组认证方案具有不可冒充性. 在上述表达式中,假定

A_O冒充组成员$U_\mu, \mu \notin [1,m]$.

定义 6 （椭圆曲线离散对数困难问题[16]）假设E是有限域Z_q上的椭圆曲线，Q,P是E上的点，满足$Q=kP, k \in Z_q$，则椭圆曲线离散对数困难问题是指：给定Q,P，求解出k是困难的.

3 本文方案

为了解决群组管理者由分发不合法私钥给组成员而导致组成员群组认证失败的问题以及满足资源受限的物联网节点的群组认证需求，本文提出一种面向物联网的轻量级可验证群组认证方案（Group Authentication Scheme with Verifiable Private Key，GASVPK）.

3.1 系统模型

群组认证系统模型如图 2 所示. 系统模型包含两种类型成员：群组管理者（Group Mananger，GM）和组成员. GM 负责设置以及更新系统参数，并通过秘密信道为组成员分发私钥. 组成员通过无线信道通信，验证其他组成员的身份. 在物联网场景下，GM 可以是服务器、网关等网络设施，组成员可以是智能电表、智能家居、智能穿戴等物联网设备.

本文提出的 GASVPK 方案假设 GM 的身份是真实的，但是 GM 可能欺骗某些组成员而分发错误的私钥，因此需要组成员在 GM 分发私钥后验证私钥的有效性. 假设参与群组认证的人数为$m, k \leqslant m \leqslant n$，$k$是群组认证人数的门限，$n$是组成员的数量. 在群组认证阶段，GASVPK 方案最多可以容忍$k-1$个内部组成员相互勾结.

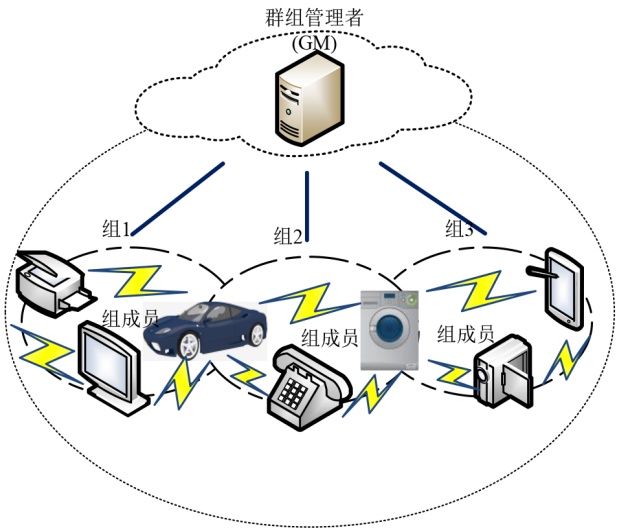

图 2 群组认证系统模型

3.2 GASVPK 方案

GASVPK 方案分为以下 6 个阶段：初始化阶段、私钥分发阶段、私钥验证阶段、认证令牌生成阶段、群组认证阶段和组成员动态变化阶段. GASVPK 方案的流程如图 3 所示.

（1）初始化阶段

输入安全参数λ，GM 选择两个阶为大素数q的加法循环群G_1, G_2和一个阶为q的乘法循环群G_T，P和R分别是G_1和G_2的生成元，选择双线性配对$e(\cdot): G_1 \times G_2 \to G_T$，选择一个$k-1$次的秘密多项式$f(x)=a_0+a_1x+\cdots+a_{k-1}x^{k-1} \pmod q$，令秘密信息$s=a_0$，计算$Q=sP, v_j=e(a_jP,R), j=0,1,\cdots,k-1$，选择哈希函数$h(\cdot): \{0,1\}^* \to Z_q$，选择 GM 的公私钥对$\{\mathrm{pk_{GM}}, \mathrm{sk_{GM}}\}$，公开参数

$$\mathrm{params}=(G_1, G_2, G_T, Q, R, P, \{v_j\}_{j\in[0,k-1]}, h(\cdot), e(\cdot), \mathrm{pk_{GM}})$$

（2）私钥分发阶段

假设组U有n个组成员$\{U_1, U_2, \cdots, U_n\}$，群组管理者 GM 根据组成员的公开身份信息$x_i$计算$s_i=f(x_i)$作为组成员的私钥，并通过秘密信道将私钥分发给组成员U_i，其中$i=1,2,\cdots,n$.

（3）私钥验证阶段

组成员U_i在收到 GM 分配的私钥s_i后，验证等式$e(s_iP,R)=\prod_{j=0}^{k-1} v_j^{x_i^j}$是否成立以验证私钥$s_i$是否有效. 如果等式成立，则接受私钥$s_i$；如果等式不成立，则重新向 GM 请求私钥$s_i$.

（4）认证令牌生成阶段

①GM 向组内发送消息$\mathrm{sig}_{sk_{\mathrm{GM}}}(\mathrm{request}_U, \varphi, t)$，其中$\mathrm{request}_U$是 GM 向组$U$发起的群组认证请求，$\varphi$是当前会话序号，$t$是接收时间的阈值，$\mathrm{sig}_{sk_{\mathrm{GM}}}(\cdot)$为 GM 对消息的签名. 随后，GM 更新会话序号φ.

②组成员使用pk_{GM}验证 GM 的签名，验证成功则进行第φ次会话. 假设参与群组认证的组成员为$\{U_1, U_2, \cdots, U_m\}$，每个参与群组认证的组成员$U_i (i=1,2,\cdots,m)$在组内广播$z_i=x_i \| \varphi$作为应答消息.

③在t时间内接收到应答消息后，每个参与群组认证的组成员U_i计算当前会话标识$T=h(x_1 \| \cdots \| x_m \| \varphi)$，选择随机数$r_i \in Z_q$，计算拉格朗日系数$\mu_i=\prod_{j=1, j\neq i}^{m} \frac{x_j}{x_j-x_i}$，计算认证令牌$c_i=s_i\mu_iT+r_i$和$r_iP$，公开认证令牌$\{c_i, r_iP\}$.

（5）群组认证阶段

当组成员$U_i (i=1,2,\cdots,m)$在t时间内收到其他组成员公开的认证令牌，每个组成员验证等式$(\sum_{i=1}^{m} c_i)P=\sum_{i=1}^{m} r_iP+TQ$是否成立以验证其他组成员的身份. 如果等式成立，则群组认证通过；如果等式不成立，则群组

认证失败,重新进行下一轮群组认证.

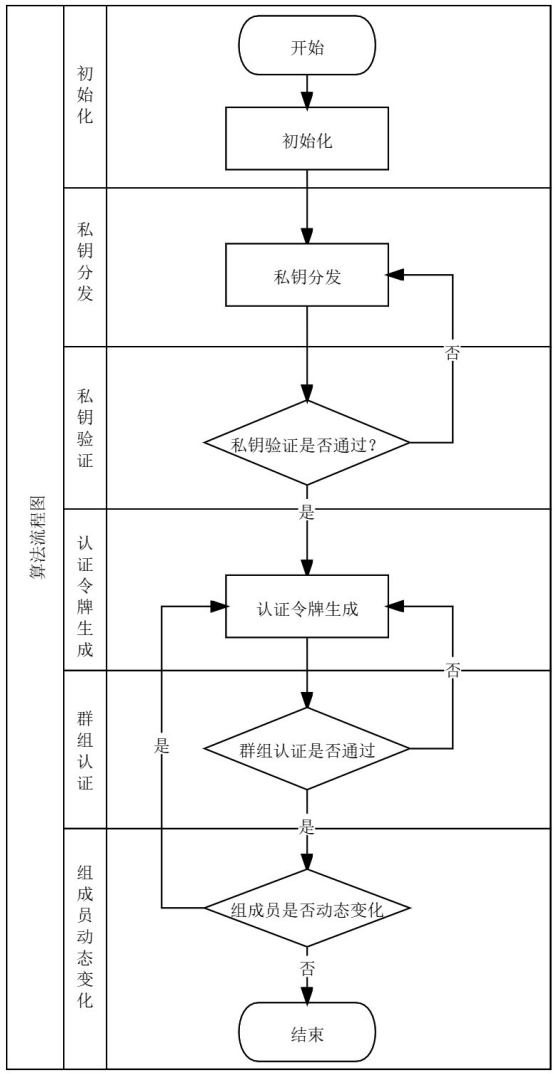

图3　GASVPK方案流程图

(6)组成员动态变化阶段

组成员动态变化阶段,组成员可以动态地加入和撤出群组,GM需要更新组成员的私钥以分配或撤销组成员的权限. 在下一轮群组认证时,新加入的组成员可以使用分配的私钥通过群组认证,撤出的组成员无法利用原有的私钥通过群组认证.

①组成员加入

(*a*)假设 U_{n+1} 想要加入组 $U=\{U_1,U_2,\cdots,U_n\}$,GM根据 U_{n+1} 的公开身份信息 x_{n+1} 计算 $s_{n+1}=f(x_{n+1})$ 作为组成员私钥,并通过秘密信道将私钥分发给 U_{n+1}.

(*b*)U_{n+1} 在收到GM分配的私钥 s_{n+1} 后,验证等式 $e(s_{n+1}P,R)=\prod_{j=0}^{k-1}v_j^{x_{n+1}{}^j}$ 是否成立以验证私钥 s_{n+1} 是否有效. 如果等式成立,则接受私钥 s_{n+1};如果等式不成立,则重新向GM请求私钥 s_{n+1}.

②组成员撤出

(*a*)假设 U_n 想要撤出组 $U=\{U_1,U_2,\cdots,U_n\}$,GM选择随机数 $h\in Z_q$,更新秘密多项式 $f(x)$ 和 v_1 为

$$f'(x)=f(x)+hx=a_0+(a_1+h)x+\cdots+a_{k-1}x^{k-1}\ (\mathrm{mod}\ q)$$

$$v_1'=v_1e(hP,R)=e((a_1+h)P,R)$$

(*b*)群组管理者GM通过秘密信道将 h 发送给组成员 $U_i,i=1,2,\cdots,n-1$,U_i 验证等式 $v_1e(hP,R)=v_1'$ 是否成立. 如果等式成立,则接受 h;如果等式不成立,则重新向GM请求 h. 然后组成员 $U_i,i=1,2,\cdots,n-1$,更新私钥 $s_i'=s_i+hx_i$.

组成员动态地加入和撤出后,可以进行群组认证,具体步骤与阶段(4)和阶段(5)相似,此处就不再赘述.

4　GASVPK方案安全性证明和分析

本节将对GASVPK方案的正确性、机密性、不可伪造性、不可冒充性做出形式化安全性证明,并且分析了方案可以抵抗重放攻击和抵抗群组管理者欺骗. GASVPK方案的安全性基于椭圆曲线离散对数困难问题[16].

4.1　安全性证明

定理1　GASVPK方案满足正确性.

证明　如果 n 个组成员中参与群组认证的组成员为 $\{U_1,U_2,\cdots,U_m\},k\le m\le n$,$k$ 是群组认证人数的门限. 根据拉格朗日插值定理,秘密值 $s=f(0)=\sum_{i=1}^{m}f(x_i)\mu_i=\sum_{i=1}^{m}s_i\mu_i$,其中 $\mu_i=\prod_{j=1,j\ne i}^{m}\frac{x_j}{x_j-x_i}$ 是拉格朗日系数,组成员的令牌 $c_i=s_i\mu_iT+r_i$,可以得到

$$\sum_{i=1}^{m}c_i=T\sum_{i=1}^{m}s_i\mu_i+\sum_{i=1}^{m}r_i=sT+\sum_{i=1}^{m}r_i,$$

$$(\sum_{i=1}^{m}c_i)P=(sT+\sum_{i=1}^{m}r_i)P=\sum_{i=1}^{m}r_iP+TsP=\sum_{i=1}^{m}r_iP+TQ$$

因此,验证公式 $(\sum_{i=1}^{m}c_i)P=\sum_{i=1}^{m}r_iP+TQ$ 成立,群组认证成功.

假设 U_{n+1} 加入组 $U=\{U_1,U_2,\cdots,U_n\}$,如果参与群组认证的组成员为 $\{U_1,U_2,\cdots,U_m,U_{n+1}\},k-1\le m\le n$. 根据拉格朗日插值定理,秘密值 $s=f(0)=\sum_{i=1}^{m}s_i\mu_i+s_{n+1}\mu_{n+1}$,其中 $\mu_i=\prod_{j=1,j\ne i}^{m}\frac{x_j}{x_j-x_i}\frac{x_{n+1}}{x_{n+1}-x_i},i=1,\cdots,m,\mu_{n+1}=\prod_{j=1}^{m}\frac{x_j}{x_j-x_{n+1}}$ 是拉格朗日系数,组成员的令牌 $c_i=s_i\mu_iT+$

r_i,同理可以验证公式$(\sum_{i=1}^{m}c_i+c_{n+1})P=\sum_{i=1}^{m}r_iP+r_{n+1}P+TQ$成立.

假设U_n撤出组$U=\{U_1,U_2,\cdots,U_n\}$,如果参与群组认证的组成员为$\{U_1,U_2,\cdots,U_m\},k\leqslant m\leqslant n-1$. 组成员$U_i(i=1,2,\cdots,m)$的私钥$s_i'=f'(x_i)=f(x_i)+hx_i$,根据拉格朗日插值定理,秘密值$s=f'(0)=\sum_{i=1}^{m}s_i'\mu_i$,其中$\mu_i=\prod_{j=1,j\neq i}^{m}\frac{x_j}{x_j-x_i}$是拉格朗日系数,组成员的令牌$c_i'=s_i'\mu_iT+r_i$,同理可以验证公式$(\sum_{i=1}^{m}c_i')P=\sum_{i=1}^{m}r_iP+TQ$成立.

证毕.

定理2 GASVPK方案满足机密性.

证明 设$\mathrm{Real}_{\chi}(\lambda,\mathrm{params})$为实际运行的方案$\chi$,$\mathrm{SIM}_S(\lambda,\mathrm{params})$为一个把公开信息作为输入的模拟机$S$模拟的方案,定理2的证明由引理1推出,两种运行方案如下.

(1)$\mathrm{Real}_{\chi}(\lambda,\mathrm{params})$

①初始化阶段

GM生成并输出公开参数:

$$\mathrm{params}=(G_1,G_2,G_T,Q,R,P,\{v_j\}_{j\in[0,k-1]},h(\cdot),e(\cdot),\mathrm{pk}_{\mathrm{GM}})$$

②私钥分发阶段

GM计算私钥$s_i=f(x_i)$并且通过秘密信道发送给组成员. 假定内部敌手A_I至多知道$k-1$个组成员的私钥$\{s_1,s_2,\cdots,s_{k-1}\}$.

③私钥验证阶段

每个组成员验证等式$e(s_iP,R)=\prod_{j=0}^{k-1}v_j^{x_i^j}$是否成立.

④认证令牌生成阶段

假设n个组成员中参与群组认证的组成员为$\{U_1,U_2,\cdots,U_m\},k\leqslant m\leqslant n$. 在第$\varphi$次会话中,每个参与群组认证的组成员$U_i$选择随机数$r_i\in Z_q$,计算会话标识$T=h(x_1\|\cdots\|x_m\|\varphi)$和拉格朗日系数$\mu_i=\prod_{j=1,j\neq i}^{m}\frac{x_j}{x_j-x_i}$,计算并公开认证令牌$c_i=s_i\mu_iT+r_i$和$r_iP$. 在这个阶段,内部敌手$A_I$知道$k-1$个组成员的私钥$\{s_1,s_2,\cdots,s_{k-1}\}$、随机数和所有公开的信息.

⑤群组认证阶段

每个组成员验证等式$(\sum_{i=1}^{m}c_i)P=\sum_{i=1}^{m}r_iP+TQ$是否成立.

(2)$\mathrm{SIM}_S(\lambda,\mathrm{params})$

①初始化阶段

模拟机S输出公开参数:

$$\mathrm{params}=(G_1,G_2,G_T,Q,R,P,\{v_j\}_{j\in[0,k-1]},h(\cdot),e(\cdot),\mathrm{pk}_{\mathrm{GM}}).$$

②私钥分发阶段

S发送$k-1$个组成员的私钥$\{s_1,s_2,\cdots,s_{k-1}\}$给内部敌手$A_I$.

③私钥验证阶段

每个组成员验证等式$e(s_iP,R)=\prod_{j=0}^{k-1}v_j^{x_i^j}$是否成立.

④认证令牌生成阶段

假设n个组成员中参与群组认证的组成员为$\{U_1,U_2,\cdots,U_m\},k\leqslant m\leqslant n$. 在第$\varphi$次会话中,$S$发送$\{r_1,r_2,\cdots,r_{k-1}\}$给$A_I$,然后$S$从$Z_q$上随机选择选择$m-k$个值$\{c_k',c_{k+1}',\cdots,c_{m-1}'\}$,计算$c_m'$满足公式$c_m'=\sum_{i=k}^{m}c_i-\sum_{i=k}^{m-1}c_i'$. S公开认证令牌$\{c_1,\cdots,c_{k-1},c_k',\cdots,c_m'\}$和$\{r_iP\}_{i\in[1,m]}$.

⑤群组认证阶段

每个组成员验证等式$(\sum_{i=1}^{k-1}c_i+\sum_{i=k}^{m}c_i')P=\sum_{i=1}^{m}r_iP+TQ$是否成立.

证毕.

引理1 如果存在内部敌手A_I,他能够至多进行Q次尝试,并且能以不可忽略的概率ε区分出两种运行方案,则存在一种算法能够以$\varepsilon'\geqslant\varepsilon\frac{q}{Q}$的优势解决椭圆曲线上离散对数困难问题.

证明 如果存在内部敌手A_I,他能够区分出两种运行方案,则他能够区分出$\{c_k,\cdots,c_m\}$和$\{c_k',\cdots,c_m'\}$,由于$c_i=s_i\mu_iT+r_i$,则他能够区分出两种运行方案的概率等同于A_I可以获得s_i和r_i的值的概率,其中$i=k,\cdots,m$. 下面来计算A_I可以获得s_i和r_i的概率.

根据拉格朗日插值定理,只有私钥的个数不小于门限值k才可以重构多项式,进而获得其他组成员的私钥. A_I至多知道$k-1$个私钥$\{s_1,s_2,\cdots,s_{k-1}\}$,则他至少需要猜出多项式上一个点值,由于点值在$Z_q$上是随机分布的,所以$A_I$猜出一个点值的概率约为$1/q$,所以,$A_I$获得$s_i$的值的概率至多为$1/q$. 假设$A_I$能以$\varepsilon'$的概率解决椭圆曲线上离散对数困难问题,给定$(P,r_iP)$为群$G_1$上离散对数困难问题的一个实例,$A_I$能以$\varepsilon'$的概率求出$r_i$的值,则$A_I$获得$r_i$的值的概率为$\varepsilon'$.

综上所述,A_I可以获得s_i和r_i的概率$\varepsilon\leqslant\varepsilon'Q/q$,其中$Q$是$A_I$尝试的次数. 所以,$A_I$可以区分出两种运行方案的概率$\varepsilon\leqslant\varepsilon'Q/q$. 可以推出,$A_I$解决椭圆曲线上离散对数困难问题的概率$\varepsilon'\geqslant\varepsilon Q/q$,其中$\varepsilon$为一个不可忽略的概率.

A_I能以一个不可忽略的概率解决椭圆曲线上离散对数困难问题,这与定义6中的椭圆曲线上的离散对数

困难性假设矛盾,所以A_I无法区分出$\mathrm{Real}_\chi(\lambda,\mathrm{params})$和$\mathrm{SIM}_S(\lambda,\mathrm{params})$,可以得到

$$\Pr[\mathrm{View}_{A_I}(\mathrm{Real}_\chi(\lambda,\mathrm{params}))]$$
$$-\Pr[\mathrm{View}_{A_I}(\mathrm{SIM}_S(\lambda,\mathrm{params}))]<\varepsilon(\lambda)$$

其中,$\varepsilon(\lambda)$表示关于参数λ的可忽略的函数. 因此,由定义5的安全性要求可知,GASVPK方案满足机密性.

定理3　GASVPK方案满足不可伪造性.

证明　假定X事件是指A_I能够从公开参数中预测出s,Y事件是指A_I能够通过询问模拟机得知一些秘密信息,F事件是指成功伪造出未被控制组成员的认证令牌,可以得到

$$\begin{aligned}\Pr[F]&=\Pr[F|X\vee Y]\cdot\Pr[X\vee Y]\\&\quad+\Pr[F|\bar{X}\wedge\bar{Y}]\cdot\Pr[\bar{X}\wedge\bar{Y}]\\&\leqslant\Pr[X\vee Y]+\Pr[F|\bar{X}\wedge\bar{Y}]\\&\leqslant\Pr[X]+\Pr[Y]+\Pr[F|\bar{X}\wedge\bar{Y}]\end{aligned}$$

首先,基于离散对数困难问题假设,可以得到$\Pr[X]<\varepsilon_1(\lambda)$,其中,$\varepsilon_1(\lambda)$表示关于参数$\lambda$的可忽略的函数. 其次,定理2证明了协议满足机密性,不会泄露任何秘密信息给A_I,且即使A_I查询模拟机多项式次数,他也不会知道任何秘密信息. 因此,可以得到,$\Pr[Y]<\varepsilon_2(\lambda)$,$\varepsilon_2(\lambda)$表示关于参数$\lambda$的可忽略的函数. 最后,分析$\Pr[F|\bar{X}\wedge\bar{Y}]$,在这种情况,为了伪造出未被控制组成员的认证令牌,A_I需要猜出s,因为s在Z_q上是随机分布的,所以A_I猜出s的可能性为$1/q$,且A_I可以尝试多项式次数,可以得到$\Pr[F|\bar{X}\wedge\bar{Y}]=Q/q$,其中$Q$是$A_I$尝试的次数. 综合以上分析,可以得到

$$\begin{aligned}\Pr[F]&=\Pr[X]+\Pr[Y]+\Pr[F|\bar{X}\wedge\bar{Y}]\\&<\varepsilon_1(\lambda)+\varepsilon_2(\lambda)+\frac{Q}{q}\\&<\varepsilon(\lambda)\end{aligned}$$

其中,$\varepsilon(\lambda)$表示关于参数λ的可忽略的函数. 因此,由定义5的安全性要求可知,GASVPK方案满足不可伪造性.

定理4　GASVPK方案满足不可冒充性.

证明　假定X事件是指A_O能够从公开参数中预测出s和$r_i,i=1,\cdots,m$,F事件是指A_O成功冒充组成员$U_\mu,\mu\notin[1,m]$且不被发现,可以得到

$$\begin{aligned}\Pr[F]&=\Pr[F|X]\cdot\Pr[X]+\Pr[F|\bar{X}]\cdot\Pr[\bar{X}]\\&\leqslant\Pr[X]+\Pr[F|\bar{X}]\end{aligned}$$

首先,基于离散对数困难问题假设,可以得到$\Pr[X]<\varepsilon_1(\lambda)$,其中,$\varepsilon_1(\lambda)$表示关于参数$\lambda$的可忽略的函数. 然后,分析$\Pr[F|\bar{X}]$的概率. 在这种情况下,$A_O$需要输出一个令牌$c_\mu$满足$(\sum_{i=1}^{m}c_i+c_\mu)=(sT+\sum_{i=1}^{m}r_i+r_\mu)$,$\{c_i\}_{i\in[1,m]}$是$A_O$已知的其他参与者的认证令牌集合,因为$s,r_i$在$Z_q$上是随机分布的,所以$A_O$猜出$(sT+\sum_{i=1}^{m}r_i+r_\mu)$的可能性为$1/q$,且$A_O$可以尝试多项式次数,可以得到$\Pr[F|\bar{X}]=Q/q$,其中$Q$是$A_O$尝试的次数. 综合以上分析,可以得到$\Pr[F]<\varepsilon_1(\lambda)+Q/q<\varepsilon(\lambda)$,其中,$\varepsilon(\lambda)$表示关于参数$\lambda$的可忽略的函数. 因此,由定义5的安全性要求可知,GASVPK方案满足不可冒充性.

4.2　安全性分析

(1)抗重放攻击

在GASVPK方案中,GM向组U发起群组认证请求,其中包含会话序号φ,由于GM每一轮都会更新φ,所以每一轮的φ是不同的,每一轮产生的会话标识$T=h(x_1\|\cdots\|x_m\|\varphi)$也是不同的. 即使两轮参与群组认证的组成员相同,敌手重放上一轮的消息也无法通过下一轮的群组认证. 假设上一轮的会话序号为φ_1,参与群组认证的组成员为$\{U_1,U_2,\cdots,U_m\}$,会话标识$T_1=h(x_1\|\cdots\|x_m\|\varphi_1)$,组成员$U_i$的会话令牌为$c_i=s_i\mu_iT_1+r_i$和$r_iP$,假设下一轮的会话序号为$\varphi_2,\varphi_2\neq\varphi_1$,参与群组认证的组成员同样为$\{U_1,U_2,\cdots,U_m\}$,会话标识$T_2=h(x_1\|\cdots\|x_m\|\varphi_2)$,组成员$U_i$的会话令牌为$c_i'=s_i\mu_iT_2+r_i'$和$r_i'P$. 由于$T_1\neq T_2$,敌手无法通过重放组成员$U_i$上一轮的会话令牌通过下一轮的群组认证. 因此,GASVPK方案可以抵抗重放攻击,提高了群组认证的安全性.

(2)抗群组管理者欺骗

在GASVPK方案中,组成员验证了私钥的有效性,防止了群组管理者欺骗. 组成员$U_i(i=1,\cdots,m)$利用公开参数$v_j=e(a_jP,R)(j=0,1,\cdots,k-1)$验证等式$e(s_iP,R)=\prod_{j=0}^{k-1}v_j^{x_i^j}$. 当组成员动态变化时,假设$U_{n+1}$加入组$U=\{U_1,U_2,\cdots,U_n\}$,$U_{n+1}$验证等式$e(s_{n+1}P,R)=\prod_{j=0}^{k-1}v_j^{x_{n+1}^j}$;假设$U_n$撤出组$U=\{U_1,U_2,\cdots,U_n\}$,组成员$U_i,i=1,\cdots,n-1$验证等式$v_1e(hP,R)=v_1'$. 如果等式不成立,代表私钥无效,群组管理者可能存在欺骗行为,组成员重新向群组管理者请求私钥. 因此,GASVPK方案较好地防止了群组管理者的欺骗行为.

5　性能分析与仿真分析

本节将从安全性和计算开销两个方面对GASVPK方案进行性能分析,并与文献[11~13,17,18]的群组认证方案进行对比分析. 同时,通过仿真实验实现GASVPK方案、文献[11~13,17,18]方案,并根据实验结果进行计算开销的对比分析.

5.1 性能分析

对于群组认证方案，计算开销是性能测量的重要指标之一. 表1给出了各种密码运算的名称、对应的英文以及运算时间的符号表示. T_{EM} 为一次椭圆曲线点乘运算的时间，T_{EA} 为一次椭圆曲线点加运算的时间，$T_{mul,\,q}$ 为 Z_q 上一次乘法运算的时间，$T_{inv,\,q}$ 为 Z_q 上一次逆运算的时间，T_{pair} 为一次双线性配对运算的时间，T_{htp} 为一次哈希映射到点运算的时间. 在性能评估中忽略哈希函数、加减法等运算的时间，因为这些运算与点乘等运算相比，时间可以忽略不计，根据文献[11]中的计算代价，$T_{EM}\cong 1189T_{mul,\,q}$，$T_{EA}\cong 4.92T_{mul,\,q}$，$T_{pair}\cong 5356T_{mul,\,q}$，$T_{inv,\,q}\cong 240T_{mul,\,q}$.

表1 密码运算时间的符号表示

密码运算名称	英文	运算时间的符号表示
椭圆曲线点乘运算	Elliptic curve point multiplication operation	T_{EM}
椭圆曲线点加运算	Elliptic curve point addition operation	T_{EA}
Z_q 上乘法运算	Multiplication operation in field q	$T_{mul,\,q}$
Z_q 上逆运算	Inverse operation in field q	$T_{inv,\,q}$
双线性配对运算	Bilinear pairing operation	T_{pair}
哈希映射到点运算	Hash to point operation	T_{htp}

设参与群组认证的组成员个数为 m，GASVPK方案与文献[11~13,17,18]方案中组成员的计算开销如下.

在方案[11]中，Chien计算了每个组成员在一次群组认证中的计算开销，但经过分析并与作者沟通确认，其算法中每个组成员需要 $(7m+12134)T_{mul,\,q}$ 生成认证令牌和验证组成员身份，另外在群组认证开始，组成员之间需要协商一个点 R，作者没有给出具体的算法，设时间为 T_a，所以每个组成员单次群组认证实际耗费 $(7m+12134)T_{mul,\,q}+T_a$.

在方案[12]中，每个组成员需要 $(2m-2)T_{mul,\,q}+T_{inv,\,q}+3T_{EM}+(m-1)T_{EA}$ 生成认证令牌、$(m-1)T_{EA}+2T_{pair}$ 验证组成员身份，所以每个组成员耗费 $(2m-2)(T_{mul,\,q}+T_{EA})+T_{inv,\,q}+3T_{EM}+2T_{pair}$. 进一步评估方案[12]的计算开销，每个组成员单次群组认证耗费 $(12m+14507)T_{mul,\,q}$.

在方案[13]中，每个组成员需要 $(2m-3)T_{mul,\,q}+T_{inv,\,q}+2T_{EM}$ 生成认证令牌、$(m-1)T_{EA}$ 验证组成员身份，所以每个组成员耗费 $(2m-3)T_{mul,\,q}+T_{inv,\,q}+2T_{EM}+(m-1)T_{EA}$. 进一步评估方案[13]的计算开销，每个组成员单次群组认证耗费 $(7m+2610)T_{mul,\,q}$.

在方案[17]中，每个组成员需要 $2T_{EM}+T_{EA}+T_{htp}$ 生成认证令牌、$3(m-1)T_{EA}+3T_{pair}+T_{mul,\,q}+(m-1)T_{htp}$ 验证组成员身份，所以每个组成员耗费 $(3m-2)T_{EA}+2T_{EM}+3T_{pair}+T_{mul,\,q}+mT_{htp}$. 进一步评估方案[17]的计算开销，每个组成员单次群组认证耗费 $(15m+18437)T_{mul,\,q}+mT_{htp}$.

在方案[18]中，每个组成员需要 $T_{EM}+T_{mul,\,q}$ 生成认证令牌、$3T_{EM}+2T_{EA}$ 验证组成员身份，由于该方案中组成员之间是一对一的认证，每个组成员与剩余 $m-1$ 个组成员相互认证，所以每个组成员耗费 $(m-1)(4T_{EM}+2T_{EA}+T_{mul,\,q})$. 进一步评估方案[18]的计算开销，每个组成员单次群组认证耗费 $(4767(m-1))T_{mul,\,q}$.

在GASVPK方案中，每个组成员需要 $(2m-1)T_{mul,\,q}+T_{inv,\,q}+T_{EM}$ 生成认证令牌 $c_i=s_i\mu_iT+r_i$ 和 r_iP、$2T_{EM}+mT_{EA}$ 验证组成员身份，所以每个组成员耗费 $(2m-1)T_{mul,\,q}+T_{inv,\,q}+3T_{EM}+mT_{EA}$. 进一步评估GASVPK方案的计算开销，每个组成员单次群组认证耗费 $(7m+3806)T_{mul,\,q}$.

GASVPK方案与文献[11~13,17,18]方案的组成员计算开销和安全性对比如表2所示. 从表2可以看出，与其他方案相比，GASVPK方案支持私钥的验证和组成员的动态加入和撤出，抵抗伪造攻击和重放攻击，并且在群组认证阶段具有较低的计算开销.

5.2 仿真分析

本节通过仿真实验比较文献[11~13,17,18]方案

表2 6种方案的组成员计算开销和安全性对比

	GASVPK方案	文献[11]方案	文献[12]方案	文献[13]方案	文献[17]方案	文献[18]方案
是否支持私钥验证	Y	N	N	N	N	N
是否支持组成员的动态加入和撤出	Y	N	N	N	Y	N
是否抵抗伪造攻击	Y	N	Y	N	Y	Y
是否抵抗重放攻击	Y	Y	Y	N	Y	Y
单次群组认证每个组成员的计算开销	$(7m+3806)T_{mul,\,q}$	$(7m+12134)T_{mul,\,q}+T_a$	$(12m+14507)T_{mul,\,q}$	$(7m+2610)T_{mul,\,q}$	$(15m+18437)T_{mul,\,q}+mT_{htp}$	$4767(m-1)\,T_{mul,\,q}$

和GASVPK方案的计算开销. 在个人电脑(Win10操作系统、主频1.80GHz的i5-8250的处理器、内存为8GB)利用MIRACL库实现了各个方案. 本文利用了椭圆曲线加密技术,而文献[11,12,17]方案另外采用了双线性配对技术. 为了达到相同的测试环境,几种方案都基于同一种支持双线性配对的椭圆曲线,具体设置如下:由生成元P生成阶为q的加法群,其中P为度为2的超奇异椭圆曲线$E: y^2 = x^3 - 3x (\mathrm{mod}\, p)$上的点,$p$为1536比特的素数,$q$为256比特的素数.

图4描述了GASVPK方案在不同群组认证人数和不同阶段情况下所有组成员耗费的总时间. 图5描述了GASVPK方案两轮群组认证所有组成员耗费的总时间. 图6描述了GASVPK方案在组成员动态变化阶段,不同变化人数情况下GM更新组成员权限耗费的时间. 如果在群组认证阶段节点发生重放、篡改等攻击导致一轮群组认证未通过,无须重新运行整个方案,组成员重新生成认证令牌并进行二轮群组认证.

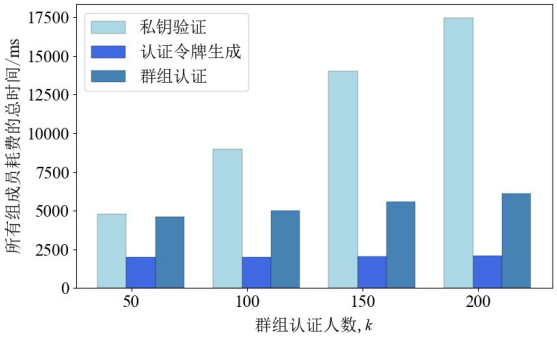

图4　GASVPK方案所有组成员耗费的总时间

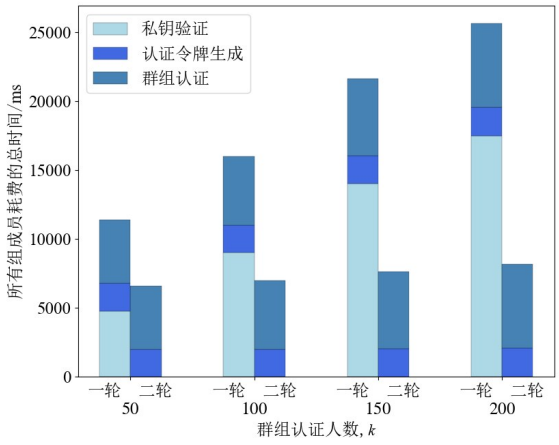

图5　GASVPK方案两轮群组认证所有组成员耗费的总时间

GASVPK方案与文献[11~13,17,18]方案单次群组认证每个组成员耗费时间的对比如图7所示. 横坐标代表群组认证的人数,纵坐标表示每个组成员耗费的时间. 由于方案[11]没有给出协商共同秘密值的具体算法,因此默认转换当前时间为共同秘密值,实际运行时间会比图7中运行时间更多. 文献[13]方案与GASVPK计算时间相近,然而文献[13]方案无法抵抗伪造和重放攻击,不具备安全性.

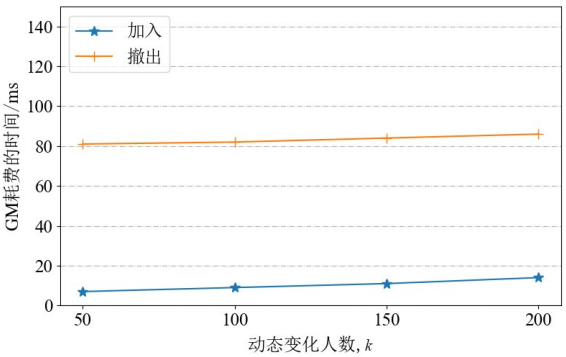

图6　GASVPK方案GM更新组成员权限耗费的时间

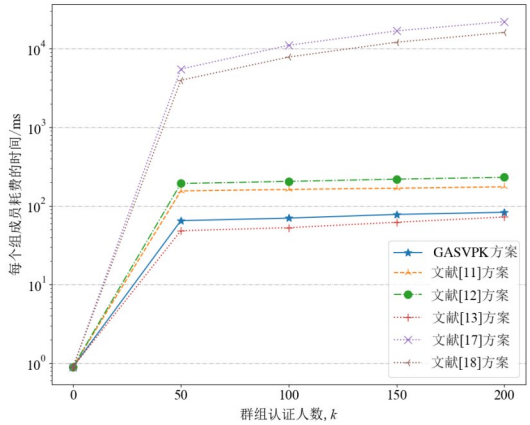

图7　六种方案单次群组认证每个组成员耗费时间的对比

综上所述,性能分析和仿真分析表明,GASVPK方案比文献[11~13,17,18]方案具有更高的安全性和更低的计算开销.

6　结束语

面向物联网的轻量级群组认证是解决物联网各种应用场景下多个设备间并行认证的有效方法. 然而,现有群组认证方案存在众多安全隐患,没有考虑群组管理者欺骗的情况,不支持组成员的动态变化,并且计算代价相对较高,无法适用于物联网节点资源受限的情况. 本文提出了一种面向物联网的轻量级群组认证方案GASVPK. 本方案创新性地在物联网场景下对群组管理者分发的私钥进行验证,防止群组管理者的欺骗行为,并且支持组成员的动态加入和撤出. 方案满足正

确性、机密性,并且可以抵抗伪造、重放、冒充等恶意攻击.与现有面向物联网的群组认证方案相比,本文方案具有更高的安全性和较低的计算开销,更加适用于海量认证请求的物联网场景,可以有效地满足物联网场景下资源受限节点的轻量级群组认证的需求.

参考文献

[1] 武传坤.物联网安全关键技术与挑战[J].密码学报,2015,2(1):40-53.
WU C K. An overview on the security techniques and challenges of the internet of things[J]. Journal of Cryptologic Research, 2015, 2(1): 40-53. (in Chinese)

[2] 陈亮,李峰,任保全,等.软件定义物联网研究综述[J].电子学报,2021,49(5):1019-1032.
CHEN L, LI F, REN B Q, et al. Software-defined internet of things: a survey[J]. Acta Electronica Sinica, 2021, 49(5): 1019-1032. (in Chinese)

[3] 张顺,范鸿丽,仲红,等.无线体域网中高效可撤销的无证书远程匿名认证协议[J].通信学报,2018,39(4):100-111.
ZHANG S, FAN H L, ZHONG H, et al. Efficient revocable certificateless remote anonymous authentication protocol for wireless body area network[J]. Journal on Communications, 2018, 39(4): 100-111. (in Chinese)

[4] FOUDA M M, FADLULLAH Z M, KATO N, et al. A lightweight message authentication scheme for smart grid communications[J]. IEEE Transactions on Smart grid, 2011, 2(4): 675-685.

[5] 房卫东,张武雄,杨旸,等.基于生物特征标识的无线传感器网络三因素用户认证协议[J].电子学报,2018,46(3):702-713.
FANG W D, ZHANG W X, YANG Y, et al. Biometric-based three-factor user authentication protocol for wireless sensor network[J]. Acta Electronica Sinica, 2018, 46(3): 702-713. (in Chinese)

[6] 张文芳,雷丽婷,王小敏,等.面向云服务的安全高效无证书聚合签名车联网认证密钥协商协议[J].电子学报,2020,48(9):1814-1823.
ZHANG W F, LEI L T, WANG X M, et al. Secure and efficient authentication and key agreement protocol using certificateless aggregate signature for cloud service oriented VANET[J]. Acta Electronica Sinica, 2020, 48(9): 1814-1823. (in Chinese)

[7] 李涛,刘亚丽.一种基于双PUF的RFID认证协议[J].计算机研究与发展,2021,58(8):1801-1810.
LI T, LIU Y L. A double PUF-based RFID authentication protocol[J]. Journal of Computer Research and Development, 2021, 58(8): 1801-1810. (in Chinese)

[8] HARN L. Group authentication[J]. IEEE Transactions on Computers, 2012, 62(9): 1893-1898.

[9] SHAMIR A. How to share a secret[J]. Communications of the ACM, 1979, 22(11): 612-613.

[10] AHMADIAN Z, JAMSHIDPOUR S. Linear subspace cryptanalysis of Harn′s secret sharing-based group authentication scheme[J]. IEEE Transactions on Information Forensics and Security, 2017, 13(2): 502-510.

[11] CHIEN H Y. Group authentication with multiple trials and multiple authentications[J]. Security and Communication Networks, 2017, 2017: 1-7.

[12] XIA Z, LIU Y N, HSU C F, et al. Cryptanalysis and improvement of a group authentication scheme with multiple trials and multiple authentications[J]. Security and Communication Networks, 2020, 2020(3): 1-8.

[13] AYDIN Y, KURT G K, OZDEMIR E, et al. A flexible and lightweight group authentication scheme[J]. IEEE Internet of Things Journal, 2020, 7(10): 10277-10287.

[14] XIONG H, QIN Z. Revocable and scalable certificateless remote authentication protocol with anonymity for wireless body area networks[J]. IEEE Transactions on Information Forensics and Security, 2015, 10(7): 1442-1455.

[15] JIANG S, ZHU X, WANG L. An efficient anonymous batch authentication scheme based on HMAC for VANETs[J]. IEEE Transactions on Intelligent Transportation Systems, 2016, 17(8): 2193-2204.

[16] ZHANG L, ZHANG F T, HUANG X Y. A secure and effcient certificateless signature scheme using bilinear pairing[J]. Chinese Journal of Electronics, 2009, 18(1): 145-148.

[17] WANG F, CHANG C C, CHOU Y C. Group authentication and group key distribution for ad hoc networks[J]. International Journal of Network Security, 2015, 17(2): 199-207.

[18] MAHMOOD K, CHAUDHRY S A, NAQVI H, et al. An elliptic curve cryptography based lightweight authentication scheme for smart grid communication[J]. Future Generation Computer Systems, 2018, 81: 557-565.

作者简介

陈书仪　女,1998年生,江苏淮安人. 江苏师范大学计算机科学与技术学院硕士研究生. 主要研究方向为群组认证技术、物联网安全和区块链.
E-mail: chenshuyi@jsnu.edu.cn

刘亚丽(通讯作者)　女,1981年生,江苏徐州人. 博士,副教授,硕士生导师,CCF会员. 主要研究方向为信息安全、物联网认证和隐私保护技术、区块链安全和隐私、车载自组织网络、密码算法和协议及其在物联网和移动通信中的应用等.
E-mail: liuyali@jsnu.edu.cn

林昌露　男,1978年生,福建大田人. 博士,副教授,博士生导师. 主要研究方向为密码学和网络安全、秘密共享、安全多方计算、公钥密码学及其应用等.
E-mail: cllin@fjnu.edu.cn

李　涛　男,1998年生,湖北黄冈人. 江苏师范大学计算机科学与技术学院硕士研究生. 主要研究方向为RFID认证技术、物联网安全和区块链.
E-mail: taoli@jsnu.edu.cn

董永权　男,1979年生,江苏宿迁人. 博士,教授,硕士生导师. 主要研究方向为Web信息管理和Web信息安全等.
E-mail: tomdyq@163.com