计算机科学
COMPUTER SCIENCE

面向工业物联网的轻量级群组密钥协商方案

王子宸, 袁程胜, 王一力, 郭萍, 付章杰

引用本文

王子宸, 袁程胜, 王一力, 郭萍, 付章杰. 面向工业物联网的轻量级群组密钥协商方案[J]. 计算机科学, 2023, 50(11A): 230700075-10.

WANG Zichen, YUAN Chengsheng, WANG Yili, GUO Ping, FU Zhangjie. Lightweight Group Key Agreement for Industrial Internet of Things [J]. Computer Science, 2023, 50(11A): 230700075-10.

计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.230700075

面向工业物联网的轻量级群组密钥协商方案

王子宸[1]　袁程胜[1]　王一力[1]　郭　萍[1]　付章杰[1,2]
1 南京信息工程大学计算机学院数字取证教育部工程研究中心　南京 210044
2 西安电子科技大学综合业务网理论及关键技术国家重点实验室　西安 710071
(princechenwzc@gmail.com)

摘　要　近年来,基于群组信息共享的工业物联网技术因具有实时、安全和信息互通等特性,被广泛应用于工业制造和金融贸易等领域。但是,该技术大多基于群组密钥协商协议,存在开销大、安全性弱、可拓展性低等缺陷。因此,如何设计安全高效的群组密钥协商协议成为当前亟需解决的科学难题,为此文中利用平衡不完全区组设计的数学结构和椭圆曲线 Qu Vanstone 认证协议,提出了一种全新的基于结构化的群组密钥协商协议。首先,为了降低协议的计算开销,使用 ECQV 认证协议,避免执行配对运算。然后,为了证明协议的安全性,借助 ECDDH 假设,对所提协议进行了安全性证明。最后,为了降低协议的通信开销,提高协议的可拓展性,利用非对称平衡不完全区组设计,对现有的群组密钥协商协议进行了拓展,将所支持的成员数从 p^2 拓展为 p^2 和 p^2+p+1。实验结果表明,所提协议能够将计算开销降低至 $O(n\sqrt{n}m)$,将通信开销降低至 $O(n\sqrt{n})$。该协议在保证抵抗选择明文攻击时安全性的同时,还能使参与群组密钥协商的人数灵活地自适应扩展,进一步提升了群组密钥协商协议的安全性和执行效率。

关键词:群组密钥协商;平衡不完全区组设计;无配对运算;工业物联网;椭圆曲线 Qu Vanstone 认证
中图法分类号　TP309

Lightweight Group Key Agreement for Industrial Internet of Things

WANG Zichen[1], YUAN Chengsheng[1], WANG Yili[1], GUO Ping[1] and FU Zhangjie[1,2]
1 School of Computer Science, Nanjing University of Information Science and Technology, Engineering Research Center of Digital Forensics Ministry of Education, Nanjing 210044, China
2 State Key Laboratory of Integrated Services Networks, Xidian University, Xi'an 710071, China

Abstract　In recent years, the industrial Internet of Things based on group information sharing has been widely used in industrial manufacturing, financial trade and other fields due to its real-time, security and information exchange characteristics. However, this technology is based on the group key agreement protocol, which has defects such as high overhead, weak security, and low scalability. Therefore, how to design a safe and efficient group key agreement protocol has become a scientific problem that needs to be solved urgently. In this paper, using the mathematical structure of balanced incomplete block design and the elliptic curve Qu Vanstone authentication protocol, a new method based on structured group key agreement protocol is proposed. First, in order to reduce the computational overhead of the protocol, the ECQV authentication protocol is used to avoid performing pairing operations. Then, the security of the proposed protocol is proved with the help of ECDDH assumption. Finally, in order to reduce the communication overhead of the protocol and improve the scalability of the protocol, the existing group key agreement protocol is extended by using the asymmetric balanced incomplete block design. And the number of supported members is changed from p^2 to p^2 and p^2+p+1. Experimental results show that the proposed protocol can reduce the computational overhead to $O(n\sqrt{n}m)$, and the communication overhead to $O(n\sqrt{n})$. While ensuring security against chosen plaintext attacks, the protocol can flexibly and adaptively expand the number of participants in group key agreement, which further improves the security and efficiency of the group key agreement protocol.

Keywords　Group key agreement, Balanced incomplete block design, Pairing-free computing, Industrial Internet of Things, Elliptic curve Qu Vanstone certificate

基金项目:国家自然科学基金(62102189);国家社会科学基金(2022GKJJGCG082);江苏省大学生创新创业训练计划支持项目(202210300107Y);南京信息工程大学大学生创新创业训练计划项目(XJDC202210300191)
This work was supported by the National Natural Science Foundation of China(62102189), National Social Sciences Foundation of China(2022GKJJGCG082), Jiangsu Province Higher Education College Student Innovation and Entrepreneurship Training Program Project(202210300107Y) and NUIST Students' Platform for Innovation and Entrepreneurship Training Program(XJDC202210300191).
通信作者:袁程胜(yuancs@nuist.edu.cn)

1 引言

近年来，基于群组密钥协商的工业物联网技术[1]被广泛应用于工业制造和金融贸易等行业。其中，工业实体在生产、运输和使用过程中会产生海量的与工业设备紧密相关的数据，因此，如何构建一个安全高效、高可拓展性的群组密钥协商协议，保障不同实体间进行安全通信，成为了当前学术界和工业界研究的热点。

自 Diffie 等[2]首次提出密钥协商这一概念后，学术界和产业界对密钥协商的研究一直方兴未艾[3-6]。作为密钥协商的一种特殊形式，群组密钥协商协议指群组成员在通信时，通过互相协商的方式产生群组会话密钥，并将其作为后续密钥，保障群组成员间进行安全高效的通信。但是，文献[2]提出的密钥协商方案仅能够为两方生成密钥，并且无法查验会话密钥持有者的身份信息，当面对中间人攻击时，无法确保协议的安全。因此，Shen 等[7]借助对称平衡不完全区组设计，利用对称平衡不完全区组设计的数学结构，提出了一种基于区组设计的群组密钥协商算法，一定程度上解决了群组密钥协商中面临的安全性弱和通信效率低的难题。为了进一步降低群组密钥协商协议的通信开销，本文引入平衡不完全区组设计的数学结构，提出了一种结构化的群组密钥协商模型，使得参与成员数量更为灵活，协议拓展性更强。

1946 年，Weil 等[8]首次提出了配对运算的概念，其通过将两个加法群中的元素映射到乘法群中，实现了乘法的同态隐藏，被广泛应用到密码学领域中。但是，当执行在线配对运算过程时需要消耗大量的算力，会一定程度地影响到用户体验。特别是当通信过程中存在大量算力较低的传感器和执行器时，基于配对运算的协议并不是最佳选择。因此，为了解决工业物联网中通信设备算力低、计算开销大的难题，本文提出了一种基于椭圆曲线 Qu Vanstone(Elliptic Curve Qu Vanstone，ECQV)的认证协议[9]，由于所提协议无需执行配对运算，因此很好地解决了工业物联网中低算力设备开销大的难题。综上，本文所提协议的创新点如下：

1)为了降低计算开销，本文使用了椭圆曲线 Qu Vanstone 认证协议，避免执行配对运算。实验结果表明，所提方案在计算开销方面优势明显，计算复杂度为 $O(n\sqrt{n}m)$，其中 n 是参与成员的数量(包括成员和志愿者)，m 代表有限域 F_{p^m} 的扩展程度。

2)为了提高协议的安全性，借助 ECDDH(Elliptic Curve Decisional Diffie Hellman) 假设，对所提协议进行了安全性证明。安全性分析表明，所有成员对群组会话密钥的贡献度均衡，保证了工业物联网中群组数据共享的安全性。

3)为了减小协议的通信开销，提高协议的可拓展性，本文利用非对称平衡不完全区组设计，对现有的群组密钥协商协议进行拓展，所支持的成员数从 p^2 拓展为 p^2 和 p^2+p+1。具体而言，本文构造了一种重构化的非对称区组设计结构，并首次将非对称区组设计应用到群组密钥协商中。通过该基于非对称区组设计的群组密钥协商协议，拓展了所支持的总成员数，从 p^2+p+1 拓展到 p^2 和 p^2+p+1，其中 p 是素数。与基于对称区组设计的协议[7]相比，基于非对称区组设计的协议的通信开销大幅降低，可拓展性得到进一步增强。

2 相关工作

1)传统结构化的群组密钥协商。在工业物联网环境中，随着线上合作需求的增加以及共享平台的扩建，传统两、三方的密钥协商方案已无法满足实际需求，迫切需要提出一种全新的群组密钥协商方案。为此，Ingemarsson 等[10]首次设计了一个支持密钥协商的环形交互模型，并将协商人数拓展至多方。但是该协议仅能抵抗被动攻击。为了满足群组用户的动态变化，Kim 等[11]提出了一种基于二叉树的群组密钥协商协议，并且给出了一个启发性的安全性证明。紧接着，Barua 等[12]设计了一种基于三叉树的群组密钥协商协议，虽然对基于二叉树的群组密钥协商协议方案进行了拓展，但是仍然无法验证参与成员的身份信息。Burmester 等[13]提出了一种非认证的群组密钥协商协议，仅需两轮通信便可完成群组间的信息共享，并且还能够抵抗外部节点发起的假冒攻击。其缺就是无法抵抗来自内部发起的恶意攻击。为此，Bression 等[14]提出了一种基于口令的群组密钥协商协议。该协议虽然能够验证用户的身份，但是随着参与通信成员数量的增加，通信轮数会呈线性增加。2023 年，Zhang 等[15]提出了一种全新的单轮群组密钥协商协议，利用该协议，用户无法否认发送的信息，但是当用户数为 n 时，通信开销就达到了 $O(n^2)$。

2)基于组合结构的群组密钥协商。为了进一步确保群组数据的共享安全，研究人员又设计了一种高安全性的群组密钥协商协议。Shen 等[16]借用拉丁方的组合结构，构建了一种基于拉丁方的群组密钥协商协议。该方案将组合结构引入到群组密钥协商中，一定程度上减小了通信开销。但是由于通信轮数过高，导致通信效率较低。为此，Shen 等[17]又提出了一种基于身份的密钥协商协议，通过引入区组设计的数学结构，实现了支持实体认证的群组密钥协商。但该协议最多支持 7 名成员间的通信，缺乏一定的灵活性。在这之后，Shen 等[7]通过对区组设计的数据结构进行优化，又提出了一种基于区组设计的群组密钥协商协议，在填充志愿者的情况下，能够最多支持 n 个成员间的通信，并且可以将通信开销压缩至 $O(n\sqrt{n})$。但是由于该协议引入了 Weil 配对运算，导致计算开销过大。

3)基于无配对运算技术的群组密钥协商。为了解决车联网环境中无线实时数据的传输问题，Zhang 等[18]设计了一种车辆认证与密钥协商方案。另外，针对短期密钥泄露问题，该方案能够在长期密钥不泄露的前提下，保证会话密钥的安全性。但是，当车辆和云服务器的数量分别为 n 和 m 时，其通信开销达到了 $O(nm)$。2022 年，Braeken 等[19]提出了一种无需配对运算的公钥群组密钥协商协议，其能够显著降低因配对运算而产生的计算开销。由于该协议采用广播通信的方式，因此同样会增加通信开销。

综上所述，现有的群组密钥协商技术主要有如下不足：

1)传统结构化的群组密钥协商虽然能够将协议由两、三方拓展至多方，但是其存在安全性较低、通信轮数高的难题；

2)基于组合结构的群组密钥协商虽然能够有效降低通信轮数，但是在计算、通信方面开销较高，且可拓展性较低；

3)基于无配对运算技术的群组密钥协商虽然具有较低的计算开销，但是通信开销较大。

3 预备知识

本章首先介绍安全假设和所涉及的密码运算；然后给出ECQV认证方案；最后，对区组设计相关知识进行详细介绍。关于本文涉及到的参数及对应的具体含义，如表1所列。

表1 记号

Table 1 Notations

参数	含义
v	集合 V 的元素总数
b	区组总数
r	含某一元素的区组数
k	每个区组所含元素数
λ	包含某一元素对的区组数
$MOD(a,m)$	a 除以 m 的余数
$m\|n$	m 整除 n
$\|A\|$	集合 A 的元素个数
$a\neq b(\mathrm{mod}\ p)$	a 和 b 模 p 不同余
a^{-1}	a 的数论倒数

3.1 安全假设和密码运算

在公钥密码学体制中，协议的安全性是首要考虑的问题。攻击者和攻击目标可用安全模型进行详细介绍，而具体的安全性证明则依据ECDDH假设，其定义如下。

定义1 令E_p为有限域F_p上的椭圆曲线，G是E_p上阶数为n的点。X，Y和Z分别为E_p上的3个点，且满足$X=xG$，$Y=yG$，其中x，y是从F_p上随机挑选的两个整数，Z是在E_p上随机选择的椭圆曲线点。给定G，X，Y，ECDDH假设需要通过求算法$Algo$来判断Z是否等于xyG。若相等则输出1，否则输出0。

对于算法Algo，有关ECDDH假设的优势ε的定义如下：

$$\left|Pr[Algo(G,X,Y,Z)=1]-Pr[Algo(G,X,Y,xyG)=1]\right|\geqslant\varepsilon \tag{1}$$

若算法Algo能够以不可忽略的优势ε解决ECDDH问题，则违反ECDDH假设。

3.2 密码运算

接下来，为了提高协议的安全性，本文选择抗强碰撞的单向哈希函数H和对称加密解密函数对(Enc,Dec)，使用对称密钥K分别将明文M加密成密文C和将密文C解密为明文M，表达式为$C=Enc_K(M)$和$M=Dec_K(C)$。

3.3 椭圆曲线Qu Vanstone(ECQV)认证

ECQV是一种基于椭圆曲线密码学的认证方案，具有计算开销低和安全性高的特点，因此适用于物联网群组通信[20]。在该方案中，窃听者无法通过传输信道获取群组会话密钥。关于ECQV的实现步骤如算法1所示。

算法1 ECQV认证

输入：成员i身份ID_i，时间戳t_i

输出：成员i是否认证成功

1. 成员i随机选择r_i，计算$R_i=r_iG$；
2. 成员i发送(ID_i,R_i)给认证中心；
3. 认证中心随机选择d_c，r_c，计算$Q_c=d_cG$，$R_c=r_cG$；
4. 认证中心计算 $\gamma_i=R_i+R_c$，$Cert_i=Encode(\gamma_i,ID_i,*)$，$a_i=H(Cert_i,t_i)r_c+d_c$；
5. 认证中心发送$(Q_c,a_i,Cert_i,t_i)$给成员i；
6. 成员i计算$Q_i=H(Cert_i,t_i)\gamma_i+Q_c$，$d_i=H(Cert_i,t_i)r_i+a_i$；
7. If $Q_i==d_iG$ then
8. 成员i认证成功；
9. Else
10. 成员i认证失败

3.4 区组设计

在组合设计中，区组设计由集合及其子集簇构成，该子集簇中的子集称为区组。区组中的元素满足整体结构平衡，区组设计的定义如下。

定义2 令V为由v个元素构成的集合，即$V=\{1,2,\cdots,v\}$；$B=\{B_1,B_2,\cdots,B_b\}$是一个包含b个区组的集合，其中B_i是V的子集，且满足$|B_i|=k$，$i=1,2,\cdots,b$。若$\sigma=(V,B)$满足以下条件，则称其为一个(v,b,r,k,λ)-设计。

1)每个元素恰好出现r次。

2)每对元素恰好同时出现λ次。如果满足条件1和条件2，则称σ为平衡不完全区组设计。

3)σ的参数k和v必须满足$k<v$，即没有区组可以包含所有元素。

4)σ的参数b和v必须满足$b\geqslant v$。若$b=v$，则称σ为一个对称区组设计；否则称σ为一个非对称区组设计。

对于(v,b,r,k,λ)-设计，必须满足$vk=br$和$\lambda(v-1)=r(k-1)$。若$b=v$且$k=r$成立，则称其为对称平衡不完全区组设计；否则为非对称平衡不完全区组设计。

本文通过构造$(v_1,p,1)$和$(v_2,p+1,1)$-设计来构建一个群组信息共享模型，其中p是素数且满足$\lambda=1$。由于$vk=br$和$\lambda(v-1)=r(k-1)$，因此5个区组设计的参数完全取决于其中的3个。这里选择(v,k,λ)作为3个主要参数。

在本文所提的协议中，根据$(v_1,p,1)$或$(v_2,p+1,1)$-区组设计的结构，每个成员都能够确定预期消息的发送者。

4 系统模型和敌手模型

为了更好地解释本文所提协议，本节将首先介绍协议的系统模型，然后介绍敌手模型，最后总结主动攻击者的能力。系统模型如图1所示，敌手模型进一步又可分为两类：主动攻击和被动攻击。

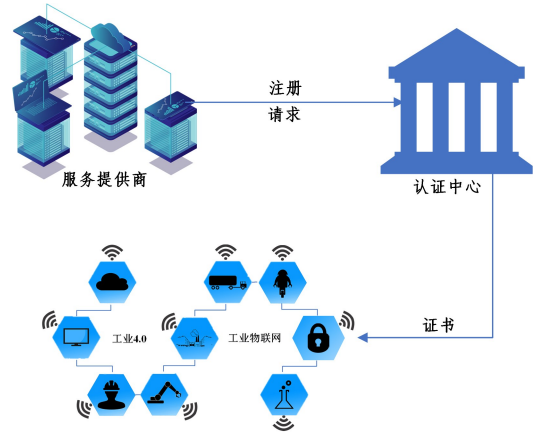


图1 系统模型

Fig. 1 System model

4.1 系统模型

本文的系统模型由3部分组成，分别为用户、服务提供商和认证中心。用户通过互相通信来获得群组会话密钥；服务提供商负责完成用户和认证中心的注册，以确保协议中的实体都是合法的；认证中心为用户初始化密钥材料，并授予用户证书以验证用户的身份。接下来，将分别对其进行详细阐述：

1)用户。在本协议中,考虑到存在不遵守群组通信规则的恶意用户,这类用户的目的是使不同成员的群组会话密钥不同,从而破坏群组通信的安全性与可靠性。根据本协议,在群组密钥协商阶段,群组成员通过检查成员的身份,来防止不合法情况的出现。

2)服务提供商。服务提供商是诚实但好奇的实体。根据本协议,由于服务提供商既不能获得其他成员的私钥,也不能获得群组的私钥,因此服务提供商无法访问群组通信的内容。

3)认证中心。认证中心是完全可信的实体,负责构建每个成员的密钥材料,并为其颁发数字证书以验证用户身份的合法性。虽然无法计算出任何成员的私钥,认证中心可以计算出群组会话密钥。此外,认证中心不能冒充任何成员,以保证协议的安全性和可靠性。在工业物联网中,认证中心能够由具有分发证书资质的大型机构承担。由于认证中心是完全可信的实体,因此与其相关的信道也是安全的。信道一旦被建立,中间人就无法攻击。在安全信道被构建的同时,由于引入了时间戳,一旦中间人发动攻击,所需时间就会超过实际通信时延,因此能够检测出中间人是否发动攻击。

4.2 敌手模型

通信信道是开放的,信息在通信过程中面临着被动攻击和主动攻击两个问题。被动攻击指攻击者通过窃听通信信道来了解群组的会话密钥;主动攻击指攻击者试图通过打断会话、冒充成员等方式破坏群组通信。

敌手模型定义了主动攻击者的能力,包括:

1)敌手能够获得成员的长期私钥,并冒充该成员与其他参会者进行交流,以获取群组会话密钥。

2)敌手能够获得先前的会话密钥,并获取新成员的密钥信息。因此,它能够冒充新成员和其他人进行交流。

3)敌手能够获得成员的私钥。之后,试图计算出之前的群组会话密钥,以获取先前的通信内容。

5 组信息交互模型

假设有 N 个成员,记 p_n 代表素数序列,如 $p_1=2$, $p_2=3$。考虑到 N 的有限性,必存在一个正整数 i_0 使得 $p_{i_0-1}^2+p_{i_0-1}+1<N\leqslant p_{i_0}^2$ 或 $p_{i_0-1}^2<N\leqslant p_{i_0}^2+p_{i_0}+1$。对于前者,本文采用 $(v_1,p,1)$-设计,并展示构建和重构阶段。对于后者,本文应用 $(v_2,p+1,1)$-设计,该构建和重构阶段由文献[7]展示。

5.1 构建 $(v_1,p,1)$-区组设计

算法 2 生成 $(v_1,p,1)$-设计

输入:素数 p

输出:$(v_1,p,1)$-区组设计 B

```
1. for i=1;i≤p;i++ do
2.     for j=1;j≤p;j++ do
3.         B_{i,j}=(i-1)p+j;
4.     end for
5.  end for
6.  for i=p+1;i≤2p;i++do
7.     for j=1;j≤p;j++do
8.         B_{i,j}=(j-1)p+i-p;
9.     end for
10. end for
11. for l=1;l≤p-1;l++do
12.  for i=(l+1)p+1;i≤(l+2)p;i++do
13.     for j=1;j≤p;j++do
14.         B_{i,j}=pMOD((j-i)l,p)+j
15.     end for
16.  end for
17. end for
```

受文献[21]启发,算法 2 构建了 $(v_1,p,1)$-区组设计。具体实现流程如下:首先,根据成员的数量确定一个质数 p。然后,计算本协议中的参数 $v_1=p^2$, $b_1=p^2+p$, $r_1=p+1$, $k_1=p$, $\lambda_1=1$。根据定义 2, $V=1,2,\cdots,v$ 表示 v 个成员。同时, $B=\{B_1,B_2,\cdots,B_b\}$ 表示 b 个区组,每个区组由 k 个成员组成, $B_{i,j}$ 表示第 i 个区块 B_i 中的第 j 个成员。所有的区组组成一个尺寸为 $b\times k$ 的矩阵 $\boldsymbol{B}$,其中第 i 行由 $B_{i,j}$ 组成, $j=1,2,\cdots,k$。而第 j 列是由 $B_{i,j}$ 组成, $i=1,2,\cdots,b$。综上所述,算法 2 给出了 $(v_1,p,1)$-区组设计的构造方式。

以质数 $p=3$ 并选择目标第 9 行第 2 列为例,对于 $(v_1,p,1)$-设计,计算 $B_{9,2}$。

$$B_{9,2}=p\cdot MOD((j-i)l,p)+j$$
$$=3\cdot MOD(-1,3)+2=3\times 2+2=8 \tag{2}$$

能够得到第 9 区块 B_9 的第 2 个成员是成员 8。

定义 3 在 $(v_1,p,1)$-区组设计模型中,定义 S_x 为连续的包含所有元素的区组集合,其计算式为 $S_x=\{B_{p(x-1)+1},B_{p(x-1)+2},\cdots,B_{px}\}$, $x=1,2,\cdots,p+1$。

5.2 重构 $(v_1,p,1)$-区组设计

在构建了原始的 $(v_1,p,1)$-区组设计之后,为了生成群组会话密钥,区组设计结构必须满足区组 B_i 包含成员 i, $i=1,2,\cdots,p^2$ 的性质。为此,本文重构 $(v_1,p,1)$-区组设计。

定义 4 令 $I_x=\{i:x\in B_i\}$ 为包含成员 x 的区组的索引集合。例如, $I_1=\{1,p+1,2p+1,\cdots,p^2-p+1\}$。显然,元素 1 出现在 $I_1,I_2,\cdots,I_p$ 中。记重构的 $(v_1,p,1)$-区组设计区组为 E_i, $1\leqslant i\leqslant p^2+p$。

引理 1 I_x 的通项公式如下。 $I_{(i_0-1)p+j_0}=\{i_0,p+j_0,(l+1)p+1+MOD(-l^{-1}(i_0-1)+j_0-1,p),l=1,2,\cdots,p-2\}$, $1\leqslant i_0,j_0\leqslant p$。

证明:根据算法 2,注意在 S_1 中, $B_{i,j}=(i-1)p+j$, $1\leqslant i,j\leqslant p$。求解方程 $B_{i,j}=x=(i_0-1)p+j_0$,可以得到对于元素 x,它的行索引是 i_0。

在 S_2 中,求解方程 $B_{i,j}=(j-1)p+i-p=x=(i_0-1)p+j_0$, $p+1\leqslant i\leqslant 2p$, $1\leqslant j\leqslant p$,解为 $p+j_0$。

对于 $S_k(k\geqslant 3)$,其求解方程 $pMOD((j-i)l,p)+j=x=(i_0-1)p+j_0$, $(l+1)p+1\leqslant i\leqslant(l+2)p$, $1\leqslant j\leqslant p$,解是 $(l+1)p+1+MOD(-l^{-1}(i_0-1)+j_0-1,p)$, $l=1,2,\cdots,p-2$。综上所述,引理 1 得到了证明。

引理 2 $q_{(i_0-1)p+j_0}=I_{(i_0-1)p+j_0,1+MOD(i_0+j_0-2,p)}$,且对于 $1\leqslant i_0,j_0\leqslant p$, $q_{(i_0-1)p+j_0}$ 互不相同,是 $1,2,\cdots,p^2$ 的一个置换。

算法 3 重构 $(v_1,p,1)$-设计

输入:素数 p, $(v_1,p,1)$-区组设计 B

输出:重构化的 $(v_1,p,1)$-区组设计 E

```
1. for i=1;1≤i≤p;i++ do
2.    for j=1;1≤j≤p;j++ do
3.        E_{(i-1)p+j}=B_{I_{(i-1)p+j,1+MOD(i+j-2,p)}}
4.    end for
5. end for
```

证明:为便于理解,记矩阵 $\boldsymbol{I}$ 为所有 I_x, $1\leqslant x\leqslant p^2$ 按列聚

合。值得注意的是$(k-1)p+1\leqslant I_{x,k}\leqslant kp$，故所有元素都在1到$p^2$之间。通过固定$i_0$，考虑$p$个数$(i_0-1)p+1,(i_0-1)p+2,\cdots,i_0p$，一般情况下具有相同的$i_0$但不同的$j_0$。根据算法3，它们在$\boldsymbol{I}$的不同列中。因此$q_{(i_0-1)p+j_0}$，$1\leqslant j_0\leqslant p$彼此不同。故只需证明在$1+MOD(i_0+j_0-2,p)$列的$q_x$，$x=(i_0-1)p+j_0$各不相同。对于$t=1+MOD(i_0+j_0-2,p)$，本文将分3种情况进行讨论。值得注意的是，对于每个t，$1\leqslant t\leqslant p$，恰有p对的(i_0,j_0)满足$t=1+MOD(i_0+j_0-2,p)$。

情况1　当$t=1$时，i_0从1遍历到p，$q_{(i_0-1)p+j_0}=i_0$互不相同。

情况2　当$t=2$时，j_0从1遍历到p时，$q_{(i_0-1)p+j_0}=p+j_0$互不相同。

情况3　当$t\geqslant 3$时，i_0从1遍历到p时，需要证明$(t-1)p+1+MOD(-(t-2)^{-1}(i_0-1)+j_0-1,p)$互不相同。考虑到$t=1+MOD(i_0+j_0-2,p)$固定，仅需证明$-(t-2)^{-1}(i_0-1)+t-i_0$，$1\leqslant i_0\leqslant p$互不相同，等价于$(1+(t-2)^{-1})i_0$，$1\leqslant i_0\leqslant p$互不相同。依据数论知识，命题等价于$1+(t-2)^{-1}\neq 0(\mathrm{mod}\ p)$。求解不等式，得到$t\neq 1(\mathrm{mod}\ p)$。由于$t\geqslant 3$，故情况3得证。

综上所述，引理2得到了证明。

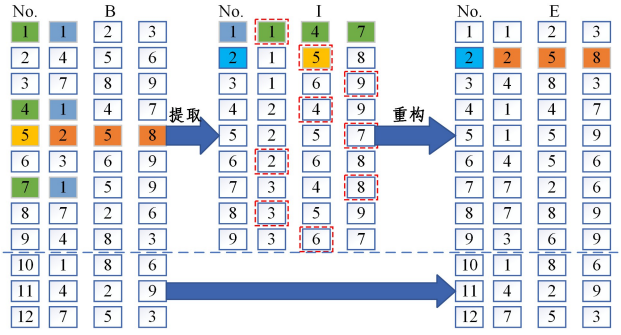


图2　非对称平衡不完全区组设计示意图

Fig. 2　Asymmetric balanced incomplete block design model

引理2保证了算法3的正确性。基于算法3，本文完成了对$(v_1,p,1)$-区组设计的重构。例如，当$p=3$时，$E_2=B_5=\{2,5,8\}$。

6　群组密钥协商协议

在本协议中，群组密钥协商过程采用无需执行配对运算的公钥群组密钥协商协议[19]，包括6个主要阶段：在注册阶段，服务提供商向认证中心请求分配所需的密钥材料；在密钥初始化阶段，认证中心选择系统参数并准备成员的密钥材料；在群组密钥协商阶段，成员通过两轮通信，接收来自其他成员的消息。每个成员使用密钥初始化阶段获得的密钥材料生成群组会话密钥；在加密阶段，群内用户可使用群组公钥加密明文；在解密阶段，每个用户能够解密发送方发送的密文；在群组更新阶段，本文将介绍服务提供商如何应对新成员的加入或旧成员的离开。

6.1　注册阶段

本协议使用带有生成元G的椭圆曲线和哈希函数H。认证中心选择密钥d_c并计算相应的公钥$Q_c=d_cG$。这些系统参数和公钥Q_c是公开的。

服务提供商持有参与群组通信的成员的身份和公钥(ID_i,Q_i)，可以通过ECQV计算公钥Q_i以保证公钥的证书认证。每个成员的私钥为d_i，满足$d_iG=Q_i$。

服务提供商向认证中心发送一个包含群组员(ID_i,Q_i)的请求，以开始密钥初始化阶段。

6.2　密钥初始化阶段

从服务提供商得到请求后，认证中心选择3个系统参数r_c,β_1,β_2和对应的椭圆曲线点$R_c=r_cG,G_1=\beta_1G,G_2=\beta_2G$。然后，认证中心开始为成员$i$进行ECQV过程，其中$Q_i$代替$R_i$，$R_{c,i}=r_{c,i}G$代替认证中心选择的椭圆曲线随机点，认证中心计算$\gamma_i=R_{c,i}+Q_i$。在此基础上，$ID_i$的证书定义为$Cert_i=Encode(\gamma_i,ID_i,*)$。然后认证中心记录时间戳$t_i$，并计算$a_i=H(Cert_i,t_i)r_{c,i}+d_c$。此外，认证中心准备了一组椭圆曲线ELGamal参数用于加密中间密钥。详细来说，认证中心为成员i选择两个随机值y_i,k_i，并对所有组成员公开$Y_i=y_iG$和k_i。

接下来，认证中心为群组通信的成员计算密钥对$(sk_{i,1},sk_{i,2})$。第一个参数$sk_{i,1}$等于d_c-u_i，其中u_i是一个随机选定的整数。$sk_{i,2}$是一个元素对$(r_{i,1},r_{i,2})$，满足式(3)：

$$u_i=r_{i,1}\beta_1+r_{i,2}\beta_2-r_c \tag{3}$$

密钥对必须用它的新私钥$Q_{i,n}$加密，以与成员秘密共享。详细来说，通过对称私钥$nsk_i=H(r_cQ_{i,n})$加密，产生密文$C_i=Enc_{nsk_i}(sk_{i,1},sk_{i,2})$。

然后，消息$(ID_i,a_i,R_{c,i},C_i,R_c,G_1,G_2,t_i)$被单独发送给每个选定的成员。收到消息后，成员记录当前时间戳t_i'，通过将当前时间与发送时间做差，来检查消息是否在时间限Δt内发送，并能够生成其证书$Cert_i=Encode(R_{c,i}+Q_i,ID_i,*)$，私钥$d_{i,n}=H(Cert_i,t_i)d_i+a_i$和对应的公钥$Q_{i,n}=d_{i,n}G$。注意到$r_cQ_{i,n}=r_cd_{i,n}G=R_cd_{i,n}$。因此，如果成员$i$可以使用对称密钥$nsk_i=H(R_cd_{i,n})$恢复密钥对$(sk_{i,1},sk_{i,2})$，则其能够通过检查等式(4)来确认密钥材料和公钥的合法性。

$$Q_c+R_c=sk_{i,1}G+r_{i,1}G_1+r_{i,2}G_2 \tag{4}$$

参数$R_c,G_1,G_2,R_{c,i},t_i,i=1,2,\cdots,v$也被服务提供商获得。因此，服务提供商能够生成$Q_{i,n}=H(Encode(R_{c,i}+Q_i,ID_i,*),t_i)(R_{c,i}+Q_i)+Q_c$。但是由于没有$d_i$，服务提供商无法获得私钥$d_{i,n}$。此外，群组身份唯一地由椭圆曲线点$R_c$定义。

6.3　群组密钥协商

在群组密钥共享阶段，用户需要通过两轮通信来生成群组会话密钥，具体采用基于重构化的$(v_1,p,1)$和$(v_2,p+1,1)$设计。

首先，对于每个成员，挑选两个随机整数w_i,l_i，其中w_i用来增加系统的随机性，l_i代表成员为产生群组密钥而做出的贡献，并构建以下6个参数$C_{i,1},C_{i,2},C_{i,3},C_{i,4},C_{i,5},C_{i,6}$，具体求解公式分别为：

$$\begin{aligned}
C_{i,1}&=H(w_iQ_c)+l_i\\
C_{i,2}&=w_iG\\
C_{i,3}&=w_iG_1=w_i\beta_1G\\
C_{i,4}&=w_iG_2=w_i\beta_2G\\
C_{i,5}&=w_iR_c=w_ir_cG\\
C_{i,6}&=l_iG
\end{aligned} \tag{5}$$

对于消息$(C_{i,1},C_{i,2},C_{i,3},C_{i,4},C_{i,5},C_{i,6})$，成员$i$使用$s_i=w_i-h_id_{i,n}$进行哈希运算生成签名$s_i$，其中$h_i=H(C_{i,1},C_{i,2},$

$C_{i,3}$,$C_{i,4}$,$C_{i,5}$,$C_{i,6}$,t_i),t_i为时间戳,用来进行身份验证。采用本文的群组数据共享模型,实际成员数 N 分别对应于(v_1,p,1)与(v_2,$p+1$,1)-设计两种情况,接下来将分别详细分析上述两种情况。

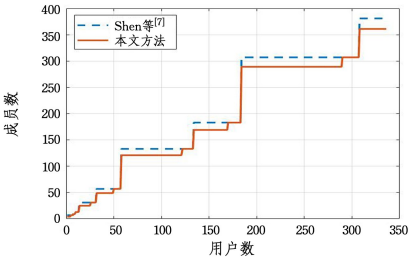


图 3 改进后成员数与用户数的比较

Fig. 3 Comparison between original and refined number of members

情况 1 若存在i_0,使 N 满足$p_{i_0-1}^2+p_{i_0-1}+1<N\leqslant p_{i_0}^2$,本文采用($v_1$,$p_{i_0}$,1)-区组设计。因此本文需要 N 名成员和$p_{i_0}^2-N$ 个志愿者共同参与群组通信,其中 $v=p_{i_0}^2$ 表示所有成员的数量。

第一轮 如果 $j\in E_i$,$1\leqslant i,j\leqslant p_{i_0}^2$ 或成员 i 和成员 j 在同一个区组E_x,$p_{i_0}^2+1\leqslant x\leqslant p_{i_0}(p_{i_0}+1)$中,成员 j 将消息$D_j=(ID_j,Cert_j,C_{j,1},C_{j,2},C_{j,3},C_{j,4},C_{j,5},C_{j,6},s_j,t_j)$发送给成员 i。因为重构化的(v_1,p,1)-区组设计具有区组E_i包含成员 i 的性质,所以成员 i 自身不能进行通信。因此,若 $j\in E_i(j\neq i)$或 $i,j\in E_x$,$p_{i_0}^2+1\leqslant x\leqslant p_{i_0}(p_{i_0}+1)$,成员 i 收到来自成员 j 的消息后,检查消息是否是在时间限 Δt 内发送的。成员收到来自 $p_{i_0}-1$ 名成员的消息。成员 i 通过密钥材料($sk_{i,1}$,$sk_{i,2}$)计算等式(6)。

$$\begin{aligned}&sk_{i,1}C_{j,2}+r_{i,1}C_{j,3}+r_{i,2}C_{j,4}-C_{j,5}\\&=(sk_{i,1}+r_{i,1}\beta_1+r_{i,2}\beta_2-r_c)\times w_jG\\&=d_cw_jG\\&=w_jQ_c\end{aligned}\tag{6}$$

其中:

$$\begin{aligned}sk_{i,1}&=d_c-u_i\\&=d_c-r_{i,1}\beta_1-r_{i,2}\beta_2+r_c\end{aligned}\tag{7}$$

成员 i 随即通过等式(8)计算出l_j并由等式(9)验证l_j。

$$l_j=C_{j,1}-H(w_jQ_c)\tag{8}$$

$$C_{j,6}=l_jG\tag{9}$$

此外,成员 i 通过椭圆曲线 ELGamal 方案[22],即通过式(10)计算($S_{i,j,1}$,$S_{i,j,2}$,$D'_{i,j}$),在第二轮通信中,用户 j 将通过($S_{i,j,1}$,$S_{i,j,2}$,$D'_{j,i}$)生成群组会话密钥。

$$\begin{aligned}&\mathscr{M}_{i,j}=\sum_{\substack{x\in E_i\setminus\{j\}\\1\leqslant i,j\leqslant p_{i_0}^2}}l_x\\&D'_{i,j}=\bigcup_{\substack{x\in E_i\setminus\{j\}\\1\leqslant i,j\leqslant p_{i_0}^2}}D_x\\&S_{i,j,1}=k_jG\\&S_{i,j,2}=\mathscr{M}_{i,j}+k_jY_j\end{aligned}\tag{10}$$

第二轮 如果 $i\in E_j$,$1\leqslant i,j\leqslant p_{i_0}^2$,用户 i 收到用户 j 的消息($S_{j,i,1}$,$S_{j,i,2}$,$D'_{j,i}$),通过等式(11)解密,检查消息是否是在时间限 Δt 内发送,以抵抗重放攻击。

$$S_{j,i,2}-y_iS_{j,i,1}=\mathscr{M}_{j,i}\tag{11}$$

实际上每个($S_{j,i,1}$,$S_{j,i,2}$)都为生成群组会话密钥贡献$p_{i_0}-1$条消息。对于S_x,$1\leqslant x\leqslant p_{i_0}$,用户 i 收到$p_{i_0}(p_{i_0}-1)$条消息。对于$S_{p_{i_0}+1}$,用户 i 收到$p_{i_0}-1$条消息。借助消息$D'_{j,i}$,解密(γ_j,ID_j,$*$)$=Decode(Cert_j)$后,成员 i 通过式(12)完成用户身份的验证。

$$(\sum_{j,j\neq i}s_j)G=\sum_{j,j\neq i}(C_{j,2}-h_jH(Cert_j,t_j)\gamma_j)-(\sum_{j,j\neq i}h_j)Q_c\tag{12}$$

其中,$h_i=H(C_{i,1},C_{i,2},C_{i,3},C_{i,4},C_{i,5},C_{i,6},t_i)$,协议的完整性通过聚合所有成员的贡献验证,具体计算式见等式(13):

$$\begin{aligned}\mathscr{M}&=l_i+\sum_{\substack{i\in E_j\\1\leqslant i,j\leqslant p_{i_0}^2}}\mathscr{M}_{j,i}+\sum_{\substack{i,j\in E_k,j\neq i\\p_{i_0}^2+1\leqslant k\leqslant p_{i_0}^2+p_{i_0}}}l_j\\&=l_i+\sum_{\substack{i\in E_j\\1\leqslant i,j\leqslant p_{i_0}^2}}\sum_{x\in E_j\setminus\{i\}}l_x+\sum_{\substack{i,j\in E_k,j\neq i\\p_{i_0}^2+1\leqslant k\leqslant p_{i_0}^2+p_{i_0}}}l_j\\&=\sum_{i=1}^{p_{i_0}^2}l_i\end{aligned}\tag{13}$$

合法成员通过式(5)和式(6),使用密钥材料($sk_{i,1}$,$sk_{i,2}$),可以从D_i恢复出l_i。因此,群组会话公钥是(Q_c,G_1,G_2,R_c+MG),私钥是元素对($sk'_{i,1}$,$sk_{i,2}$),其中 $sk'_{i,1}$更新为 $sk_{i,1}+\mathscr{M}$。

情况 2 若存在i_0,使 N 满足$p_{i_0-1}^2<N\leqslant p_{i_0}^2+p_{i_0}+1$,采用($v_2$,$p_{i_0}+1$,1)-区组设计,需要 N 个成员和$p_{i_0}^2+p_{i_0}+1-N$ 个志愿者,其中 v 为所有成员的数量,计算式为 $v=p_{i_0}^2+p_{i_0}+1$。与情况 1 类似,生成群组会话密钥需要两轮通信。

第一轮 如果 $j\in E_i$,$1\leqslant i,j\leqslant p_{i_0}^2+p_{i_0}+1$,成员 j 发送消息$D_j=(ID_j,Cert_j,C_{j,1},C_{j,2},C_{j,3},C_{j,4},C_{j,5},C_{j,6},s_j,t_j)$给成员 i。尽管重构后的(v_2,$p+1$,1)-区组具有区组E_i中成员 i 的性质,但是其自身内部无法通信。若 $j\in E_i(j\neq i)$,则成员 i 收到来自成员 j 的消息。当成员 i 从p_{i_0}个成员处收到消息后,成员 i 将验证该消息是否是在时间限 Δt 内发送的。类似地,通过使用自己的密钥材料($sk_{i,1}$,$sk_{i,2}$)并计算式(6),成员 i 从$C_{j,1}$中恢复出整数l_j并由$C_{i,6}$验证。此外,成员 i 根据等式(11)计算($S_{i,j,1}$,$S_{i,j,2}$,$D'_{i,j}$),为第二轮成员 j 生成群组会话密钥。

$$\begin{aligned}&\boldsymbol{M}_{i,j}=\sum_{\substack{x\in E_i\setminus\{j\}\\1\leqslant i,j\leqslant p_{i_0}^2+p_{i_0}+1}}l_x\\&D'_{i,j}=\bigcup_{\substack{x\in E_i\setminus\{j\}\\1\leqslant i,j\leqslant p_{i_0}^2+p_{i_0}+1}}D_x\\&S_{i,j,1}=k_jG\\&S_{i,j,2}=M_{i,j}+k_jY_j\end{aligned}\tag{14}$$

第二轮 若 $i\in E_j$,$1\leqslant i,j\leqslant p_{i_0}^2+p_{i_0}+1$,则成员 i 从成员 j 处收到($S_{j,i,1}$,$S_{j,i,2}$,$D'_{j,i}$),用等式(11)解密并验证该消息是否是在时间限 Δt 内发送。

上述群组会话密钥生成的过程中,每个$\boldsymbol{M}_{j,i}$均贡献了p_{i_0}个消息。对于S_x,$1\leqslant x\leqslant p_{i_0}+1$,成员 i 收到$p_{i_0}(p_{i_0}+1)$条消息,接下来通过聚合所有消息,并借助式(12)进行身份验证。协议的正确性通过式(15)保障,所有成员分别获得所有l_j。

$$\begin{aligned}\boldsymbol{M}&=l_i+\sum_{\substack{i\in E_j\\1\leqslant i,j\leqslant p_{i_0}^2+p_{i_0}+1}}\boldsymbol{M}_{j,i}\\&=\sum_{\substack{i\in E_j\\1\leqslant i,j\leqslant p_{i_0}^2+p_{i,0}+1}}\sum_{x\in E_j\setminus\{i\}}l_x+l_i\\&=\sum_{i=1}^{p_{i_0}^2+p_{i_0}+1}l_i\end{aligned}\tag{15}$$

因此,群组会话公钥为(Q_c,G_1,G_2,$R_c+\boldsymbol{M}G$),私钥为元素对($sk'_{i,1}$,$sk_{i,2}$),其中 $sk'_{i,1}$更新为 $sk_{i,1}+\boldsymbol{M}$。

6.4 加密阶段

首先,成员 i 随机选择一个 w_i 并对明文 m 计算 5 个消息 (C_1,C_2,C_3,C_4,C_5)。

$$\begin{aligned}C_1&=H(w_iQ_c)+m\\C_2&=w_iG\\C_3&=w_iG_1=w_i\beta_1G\\C_4&=w_iG_2=w_i\beta_2G\\C_5&=w_i(R_c+\boldsymbol{M}G)=w_i(r_c+\boldsymbol{M})G\end{aligned}\tag{16}$$

然后,成员 i 广播消息 $CT=(C_1,C_2,C_3,C_4,C_5)$。

6.5 解密阶段

拥有群组会话私钥的成员,借助式(17)便能够从 CT 中解密密文。

$$sk'_{j,1}C_2+r_{j,1}C_3+r_{j,2}C_4-C_5=w_iQ_c\tag{17}$$

由于 $sk'_{j,1}=sk_{j,1}+\mathcal{M}=d_c-u_j+\mathcal{M}$,因此等式(17)是正确的。

6.6 群组更新阶段

在群组成员更新阶段,服务提供商负责组建群组并激活认证中心,以保证完美的后向/前向安全性。

为了确保后向安全,当新成员 i 进入该群组,其无法获悉前群组的私钥。同时,为了使更改最小化,认证中心将会修改系统参数 $\beta_{1,n}$,$\beta_{2,n}$ 和所有由 $\beta_{1,n}$ 和 $\beta_{2,n}$ 产生的参数,并将新生成的参数秘密地发送给成员,通过密钥初始化获取公私密钥对,接收密钥材料 $(sk_{i,1},sk_{i,2})$。然后,它可以按照群组密钥协商阶段获得群组会话密钥。

若旧成员离开了该群组,便无法再获得后来的群组密钥。认证中心同样需要修改 $\beta_{1,n}$,$\beta_{2,n}$ 和所有由 $\beta_{1,n}$ 和 $\beta_{2,n}$ 产生的参数。此后,小组进行群组密钥协商并彼此通信。

7 安全性证明

本文所提协议的安全性主要依据 ECDDH 假设。接下来,重点介绍本文所设计的协议如何抵抗被动攻击和主动攻击。

7.1 抵抗被动攻击的安全性

首先对于选择明文攻击下的语义安全性问题,认证中心是完全可信的,攻击者在服务提供商处注册,却不参与通信,因此被动攻击者仅能通过窃听信道来试图了解群组会话密钥。

定理 1 在选择明文攻击下,若无法提供安全通信,则存在一个多项式时间内的算法能够解决 ECDDH 问题。

证明:假定挑战者 $\mathscr{C}$ 和敌手 $\mathscr{A}$ 之间进行博弈,$\mathscr{C}$ 负责操作协议并响应 $\mathscr{A}$ 的问询。首先,$\mathscr{A}$ 给 $\mathscr{C}$ 发送两条长度相等的消息 M_0 和 M_1;然后 $\boldsymbol{C}$ 随机选择 c∈{0,1}并将加密后的密文传递给 $\mathscr{A}$。若 $\mathscr{A}$ 能以不可忽略的优势区分消息 M_c 是由哪一条消息加密的,则 $\mathscr{A}$ 赢得博弈。关于 ECDDH 问题的详细分析如下。

首先,$\mathscr{C}$ 在 F_q 中选择一条合适的椭圆曲线,其生成元为 G。随后,$\mathscr{A}$ 选取两个随机整数 $a,b\in F_q$ 并随机生成 $\mu\in\{0,1\}$,根据 μ 的值,$\mathscr{C}$ 计算 $Z_\mu=\begin{cases}abG, & \mu=0\\ r, & \mu=1\end{cases}$,其中 r 是 F_q 中随机选取的整数。$\mathscr{C}$ 将 ECDDH 问题参数 G,aG,bG,Z_μ 发送给模拟器 $\mathscr{S}$。在下面的博弈中,$\mathscr{S}$ 将代替 $\mathscr{C}$ 作为 $\mathscr{A}$ 的挑战者。

模拟器 $\mathscr{S}$ 选择两个随机值 b_1 和 b_2,并分别计算 $G_1=b_1G$ 和 $G_2=b_2G$,将公钥设置为 aG,群组身份设置为 $R_c=r_cG$,其中 r_c 是一个随机整数。

问询阶段:敌手 $\mathscr{A}$ 向模拟器 $\mathscr{S}$ 发送与 R_c 群组相关的问询。根据敌手模型,敌手 $\mathscr{A}$ 无法请求属于挑战群组 R_c' 的成员密钥。模拟器 $\mathscr{S}$ 利用等式(18),可获得该挑战组的身份 R_c'。

$$R_c'=R_c-aG=(r_c-a)G\tag{18}$$

若成员属于 R_c',那么 $\mathscr{S}$ 将会计算密钥材料 $(sk_{i,1},sk_{i,2})$,其中 $sk_{i,1}=h_i$,$sk_{i,2}=(r_{i,1},r_{i,2})$,满足 $r_c-h_i=r_{i,1}b_1+r_{i,2}b_2$。若攻击者 $\mathscr{A}$ 多次问询,则模拟器 $\mathscr{S}$ 重复问询阶段。

在问询阶段结束后,敌手 $\mathscr{A}$ 向模拟器 $\mathscr{S}$ 发送两个长度相同的消息给 M_0,M_1。从 0,1 中随机选择 c 后,模拟器 $\mathscr{S}$ 返回加密后的 M_c。具体来说,$\mathscr{S}$ 计算 $C_1=H(Z_\mu)+M_c$,$C_2=bG$,$C_3=b_1bG$,$C_4=b_2bG$,$C_5=r_cbG$,$C_6=M_cG$,并将所得密文 $(C_1,C_2,C_3,C_4,C_5,C_6)$ 发送给 $\mathscr{A}$。接下来 $\mathscr{A}$ 选择出正确的 c',$\mathscr{S}$ 选择出正确的 μ'。当且仅当 $\mathscr{A}$ 选择出正确的 c 时,$\mathscr{S}$ 才能选择出正确的 μ,即 $Pr[\mu'=\mu]=Pr[c'=c]$。假设 $\mathscr{A}$ 具有不可忽略的优势 ε 选择出正确的 c,即破解本协议,考虑 μ 为 0 或 1 的两种情况,由贝叶斯公式产生如下结果:

$$\begin{aligned}Pr[\mu'=\mu]&=Pr[c'=c]\\&=\frac{1}{2}Pr[c'=c|\mu=0]+\frac{1}{2}Pr[c'=c|\mu=1]\\&=\frac{1}{2}\cdot\left(\frac{1}{2}+\varepsilon\right)+\frac{1}{2}\cdot\frac{1}{2}\\&=\frac{1}{2}+\frac{\varepsilon}{2}\end{aligned}\tag{19}$$

由此可得,存在一种算法 Algo 解决 ECDDH 问题的优势为 $\frac{\varepsilon}{2}$,即:

$$Adv(Algo)=\left|Pr[\mu'=\mu]-\frac{1}{2}\right|=\frac{\varepsilon}{2}\tag{20}$$

也就是说,如果敌手 $\mathscr{A}$ 有能力以不可忽略的优势 ε 赢得提出的博弈,$\mathscr{C}$ 能够找到算法 $Algo$ 以优势 $\frac{\varepsilon}{2}$ 解决 ECDDH 问题,结论与 ECDDH 假设矛盾,证明本文提出的定理 1 是正确的。

7.2 抵抗主动攻击的安全性

为了提高协议的安全性,除了能够抵御被动攻击者通过窃听获取群组密钥外,本文还证明了所提协议在以下 6 个方面具有主动攻击安全性。

1)抗密钥泄露伪装。在抗密钥泄露伪装方面,攻击者通过窃取成员 i 的长期密钥,试图冒充合法成员与成员 i 进行通信[23]。在本文提出的群组密钥协商协议中,长期密钥会因为成员的身份的不同而不同。由于每个成员参与协商的密钥都不相同,即使泄露一个密钥,也不会影响其他成员的密钥安全。此外,认证中心会在证书和成员签名中绑定时间戳 t_i,防止攻击者通过重放攻击窃取认证。

2)已知会话密钥。如果协议能够防止主动攻击者获得新成员的密钥,则它满足已知密钥安全的要求。在最坏的情况下,攻击者可能会了解一些以前的会话密钥。在本协议中,每个成员随机选择短期密钥 w_i 和 l_i。由于 ECDLP 的困难性,敌手无法区分随机值与新成员的会话密钥。

3)密钥控制安全。密钥控制安全要求每一个成员都能够贡献群组会话密钥,同时没有任何成员能够影响其他成员的

输入。由于签名是随机选择的，并且每个签名是相互独立的，冒充其他成员的签名意味着攻击者必须破解 ECDLP。因此，不存在合法的成员可以被冒充。

4)已知密钥安全。如果某个群组会话密钥被泄露，敌手仍然无法访问其他群组会话密钥。在密钥初始化阶段，认证中心为每个会话准备唯一的密钥材料R_c，$\beta_{1,n}$，$\beta_{2,n}$。这些密钥材料代表会话的唯一性，而且群组会话密钥是通过这些密钥材料计算得到的。因此，即使某个群组会话密钥被泄露，敌手仍然无法访问其他群组会话密钥，从而保证了已知密钥的安全。

5)抗未知密钥共享。在抗未知密钥共享安全下，每个成员都相信其他成员的真实性。由于认证中心进行的 ECQV 认证过程中，每个成员的密钥与其身份相关联，这将不会引起混淆。因此，所有成员都确信群组成员的身份和密钥的真实性，从而保证了抗未知密钥共享的安全性。

6)完美前向安全。如果长期密钥$(sk'_{i,1}, sk_{i,2})$被泄露，攻击者不应推导出之前的群组会话密钥[24]。在本协议中，注意到$sk_{i,1}=d_c+r_c-r_{i,1}\beta_1-r_{i,2}\beta_2$。根据本方案，$\beta_1$和$\beta_2$随会话更改并随机选择。由于 ECDLP 和 ECDDH 问题的困难性，攻击者不可能计算出之前的群组会话密钥，因此本协议具有完美前向安全性。

8 性能分析与评价

本章通过与 Shen 等[7]提出的方案对比可知，本文所提协议在通信和计算开销两个方面均取得最佳[7]。具体实验分析如下。

8.1 性能分析

一般来说，群组密钥协商协议的性能评价主要包含通信和计算开销，本文的通信开销包括数据共享的开销，计算开销主要由椭圆曲线点乘运算组成。本文将详细讨论每个成员的计算开销，同时还将讨论两种情况，即$(v_1, p, 1)$-区组设计和$(v_2, p+1, 1)$-区组设计。

表 2 比较结果

Table 2 Comparison results

	Braeken 2022	Shen 2017	SMAKA 2020	Zhang 2023	本协议
消息通信的形式	广播	多播	多播	广播	多播
通信模型	去中心化	去中心化	中心化	去中心化	去中心化
成员数量	n	n	n	n	n
每个成员的 Weil 配对运算数	0	$O(1)$	0	$O(1)$	0
每个成员的椭圆曲线点乘运算数	$O(n)$	$O(1)$	$O(1)$	$O(n)$	$O(n)$
通信开销	$O(n^2)$	$O(n\sqrt{n})$	$O(n^2)$	$O(n^2)$	$O(n\sqrt{n})$
计算开销	$O(n^2m)$	$O(nm^2)$	$O(n^2m)$	$O(nm(m+n))$	$O(n\sqrt{n}m)$

在群组密钥协商阶段，成员 i 需要进行 6 个椭圆曲线点乘计算$C_{i,1}, C_{i,2}, \cdots, C_{i,6}$，这对于两种情况均相同。具体分析如下。

针对情况 1，第一轮中，统计计算开销如下：对于 $2(p-1)$ 个成员，成员 i 需要通过三次椭圆曲线点乘运算计算w_jQ_c；同时对于 $p-1$ 个成员，成员 i 需要通过两次椭圆曲线点乘运算计算$(S_{j,i,1}, S_{j,i,2})$。此外，统计通信开销如下：成员 i 需要进行 $2(p-1)$次信息交换。第二轮中，统计计算开销如下：成员 i 需要进行 $2(p-1)$次椭圆曲线点乘运算解密$(S_{j,i,1}, S_{j,i,2})$，同时生成群组会话公钥需要一次椭圆曲线点乘运算。此外，统计通信开销如下：成员 i 需要进行 $p-1$ 次消息交换。综上所述，每个成员 i 需要进行 $10p-3$ 次椭圆曲线点乘运算和 3 $(p-1)$次消息交换。

情况 2，第一轮中，统计计算开销如下：对于 p 个成员，成员 i 需要通过三次椭圆曲线乘运算计算w_jQ_c，需要通过两次椭圆曲线乘运算计算出$(S_{j,i,1}, S_{j,i,2})$。此外，统计通信开销如下：成员 i 需要进行 p 次消息交换。第二轮中，统计计算开销如下：为了解密$(S_{j,i,1}, S_{j,i,2})$，需要进行 $2p$ 次椭圆曲线点乘运算。同样，生成群组会话公钥需要一次椭圆曲线点乘运算。统计通信开销如下：成员 i 需要进行 p 次消息交换。总的来说，成员 i 进行了 $7p+7$ 次椭圆曲线点乘运算和 $2p$ 次消息交换。

综上，通信复杂度为$O(vp)\approx O(v\sqrt{v})$，而计算复杂度为$O(vpm)\approx O(v\sqrt{v}m)$，如表 2 所列。这里，$m$ 表示有限域F_{p^m}的扩展次数。值得一提的是，对于基于平衡不完全区组设计的群组密钥协商协议，通信复杂度不优于$O(v\sqrt{v})$。

定理 2 基于平衡不完全区组设计的群组密钥协商协议的通信复杂度至少是$O(v\sqrt{v})$。

证明：请注意，基于(v,b,k,r,λ)-设计的群组密钥协商协议的通信复杂性是$O(bk)=O(vr)$。然而，有$\lambda(v-1)=r(k-1)$和$b\geqslant v$。因此有以下不等式：

$$\begin{aligned} vr &= bk \\ &\geqslant \sqrt{b^2k(k-1)} \\ &= \sqrt{bvrk(k-1)} \\ &= \sqrt{\lambda bv(v-1)} \\ &\geqslant \sqrt{v^2(v-1)} \\ &\approx O(v\sqrt{v}) \end{aligned} \tag{21}$$

故，本文证明了定理 2 的正确性。

8.2 性能评价

为了评价本协议的性能，针对提出的协议进行实验，相关测试的实现采用 C 语言编写，使用 PBC-0.5.14 和 GMP-6.2.1 环境，在 VMware Workstation 上运行。详细实验环境配置如表 3 所列。

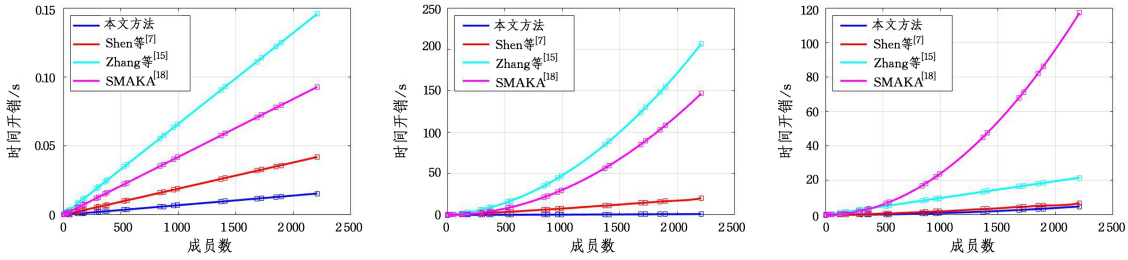
表 3 实验环境配置

Table 3 Experimental environment configuration

实验环境	配置
处理器	AMD Ryzen 7 5800H with Radeon Graphics 3.20GHz
物理内存	2GB
操作系统	Ubuntu 12.04 over VMware workstation 16.2.3

首先，与 Shen 等提出的方案[7]、Zhang 等提出的方案[15]和 SMAKA[18]进行比较，实验结果如图 4 所示，其中 X 轴表示成员的数量，Y 轴表示不同阶段下的时间开销。如图 4(a)所示，椭圆曲线点乘运算所需的时间开销较小，因此本文所提协议的性能优于其他 3 个协议。在图 4(b)中，鉴于本文所提

协议不执行配对运算，因此在群组密钥协商阶段，本协议在计算开销方面相比其他 3 个方案优势更大。对于图 4(c)，文献[7]中的协议和文献[15]中的协议应用了一定量的指数运算，而文献[18]中的协议的计算开销达到了 $O(n^2)$，使得时间开销更高。实际上，在认证阶段，本协议的计算开销是 $O(n^2)$，而 Shen[7]的计算开销是 $O(n\sqrt{n})$。当用户数量较少时，本协议的优势较为明显。此外，本协议是在收到所有消息后进行身份查验，而不是在收到消息后一一验证。



(a)密钥初始化阶段　(b)密钥协商阶段　(c)认证阶段

图 4　各阶段计算开销对比

Fig. 4　Computation cost comparison of different phases

与 Shen 等提出的协议[7]相比，本协议有额外的注册阶段，但是总开销仍然更佳。如图 5 所示，本文所提的群组密钥协商协议与其他 3 个协议相比，计算开销增长更慢，计算和通信开销更低。

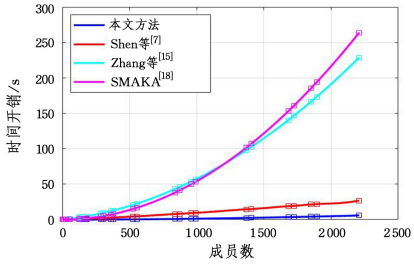


图 5　整体协议的计算开销对比

Fig. 5　Comparison of computational complexity for the whole protocol

结束语　针对现有群组密钥协商方案存在灵活性差、计算开销大的问题，提出了一种基于平衡不完全区组设计的群组密钥协商协议，该协议无需执行配对运算，从而实现一种轻量级的群组密钥协商。通过区组设计结构的数学性质和无需配对运算技术的帮助，本文还能够进一步降低群组密钥协商的计算和通信开销。在接下来的研究过程中，将会着重解决认证中心密钥托管的脆弱性问题。

参 考 文 献

[1] VINOTH R, DEBORAH L J. An efficient key agreement and authentication protocol for secure communication in industrial IoT applications[J]. Journal of Ambient Intelligence and Humanized Computing, 2023, 14(3): 1431-1443.

[2] DIFFIE W, HELLMAN M E. New directions in cryptography [J]. IEEE Transactions on Information Theory, 1976, 22(6): 644-654.

[3] BLAKE-WILSON S, JOHNSON D, MENEZES A. Key agreement protocols and their security analysis[J]. Lecture Notes in Computer Science, 1997, 1355: 30-45.

[4] YI X. Identity-based fault-tolerant conference key agreement [J]. IEEE Transactions on Dependable and Secure Computing, 2004, 1(3): 170-178.

[5] SHEN J, ZHOU T, CHEN X, et al. Anonymous and traceable group data sharing in cloud computing[J]. IEEE Transactions on Information Forensics and Security, 2017, 13(4): 912-925.

[6] ZHANG R, ZHANG L, CHOO K K R, et al. Dynamic authenticated asymmetric group key agreement with sender non-repudiation and privacy for grouporiented applications[J]. IEEE Transactions on Dependable and Secure Computing, 2021, 20(1): 492-505.

[7] SHEN J, ZHOU T, HE D, et al. Block design-based key agreement for group data sharing in cloud computing [J]. IEEE Transactions on Dependable and Secure Computing, 2017, 16(6): 996-1010.

[8] LXV W R. An illusion of size[J]. The London, Edinburgh, and Dublin Philosophical Magazine and Journal of Science, 1946, 37(272): 643-648.

[9] CAMPAGNA M. Sec 4: Elliptic curve qu-vanstone implicit certificate scheme(ecqv)[J]. Standards for Efficient Cryptography, Version, 2013, 4(1): 1-28.

[10] INGEMARSSON I, TANG D, WONG C. A conference key distribution system[J]. IEEE Transactions on Information Theory, 1982, 28(5): 714-720.

[11] KIM Y, PERRIG A, TSUDIK G. Tree-based group key agreement-[J]. ACM Transactions on Information and System Security (TISSEC), 2004, 7(1): 60-96.

[12] BARUA R, DUTTA R, SARKAR P. Extending joux's protocol to multi party key agreement(extended abstract)[J]. Lecture Notes in Computer Science, 2003, 2003: 205-217.

[13] BURMESTER M, DESMEDT Y. A secure and efficient conference key distribution system [C] // Advances in Cryptology EUROCRYPT'94: Workshop on the Theory and Application of Cryptographic Techniques Perugia. Italy, Springer, 1995: 275-286.

[14] BRESSON E, CHEVASSUT O, POINTCHEVAL D. Group diffie-hellman key exchange secure against dictionary attacks[C]// Advances in Cryptology ASIACRYPT 2002: 8th International Conference on the Theory and Application of Cryptology and Information Security Queenstown. New Zealand, Springer, 2002: 497- 514.

[15] ZHANG R, ZHANG L, CHOO K K R, et al. Dynamic Authenticated Asymmetric Group Key Agreement With Sender Non-Repudiation and Privacy for Group-Oriented Applications[J]. IEEE Transactions on Dependable and Secure Computing, 2021: 492-505.

[16] SHEN J, ZHOU T, LIU X, et al. A novel latinsquare- based secret sharing for m2m communications[J]. IEEE Transactions on Industrial Informatics, 2018, 14(8): 3659-3668.

[17] SHEN J, MOH S, CHUNG I. Identity-based key agreement protocol employing a symmetric balanced incomplete block design [J]. Journal of Communications and Networks, 2012, 14(6): 682-691.

[18] ZHANG J, ZHONG H, CUI J, et al. SMAKA: Secure Many-to-Many Authentication and Key Agreement Scheme for Vehicular Networks[J]. IEEE Transactions on Information Forensics and Security, 2020, 16: 1810-1824.

[19] BRAEKEN A. Pairing free asymmetric group key agreement protocol[J]. Computer Communications, 2022, 181: 267-273.

[20] PORAMBAGE P, KUMAR P, SCHMITT C, et al. Certificate-based pairwise key establishment protocol for wireless sensor networks[C] // 2013 IEEE 16th International Conference on Computational Science and Engineering. IEEE, 2013: 667-674.

[21] SHEN H. Combinatorial design theory[M]. Shanghai: Shanghai Jiaotong University Press, 1996: 1-63.

[22] ELGAMAL T. A public key cryptosystem and a signature scheme based on discrete logarithms[J]. IEEE Transactions on Information Theory, 1985, 31(4): 469-472.

[23] STRANGIO M A. On the resilience of key agreement protocols to key compromise impersonation [C] // EuroPKI. Springer, 2006: 233-247.

[24] XIE M, WANG L. One-round identity-based key exchange with perfect forward security [J]. Information Processing Letters, 2012, 112(14/15): 587-591.

WANG Zichen, born in 2003, postgraduate. His main research interests include information security and so on.

YUAN Chengsheng, born in 1989, Ph.D, associate professor, MA supervisor, is a member of China Computer Federation. His main interests include information security and so on.