http://bhxb.buaa.edu.cn jbuaa@buaa.edu.cn
DOI: 10.13700/j.bh.1001-5965.2021.0217

横向联邦学习环境基于身份认证及密钥协商协议

任杰[1,2]，黎妹红[1,2,*]，杜晔[1,2]，尹李纶谨[1,2]

(1. 北京交通大学 智能交通数据安全与隐私保护技术北京市重点实验室，北京 100044；
2. 北京交通大学 计算机与信息技术学院，北京 100044)

摘　　要：近年来，联邦学习受到多个领域的广泛关注，而认证及会话密钥协商是保证通信实体之间安全传输、可靠通信的关键技术和基本的安全保障。根据横向联邦学习参与方数据特征，提出一种基于身份的无证书轻量级认证及密钥协商协议；参与方在密钥生成中心（KGC）完成注册后，利用公共参数计算各自的临时密钥和长期密钥完成认证、计算会话密钥；最后，采用扩展的CK（eCK）模型对所提协议进行安全性证明。性能分析表明：所提协议在计算性能和通信开销方面可以有效地控制成本，适用于单服务器下横向联邦学习的训练环境。

关 键 词：横向联邦学习；基于身份密码体制；无证书；认证及密钥协商；eCK模型
中图分类号：V221$^+$.3; TB553
文献标志码：A　　**文章编号**：1001-5965(2023)02-0397-09

人工智能的高速发展离不开大数据的支持，但是绝大多数企业数据质量低，尤其是对数据隐私保护的要求低，无法支撑构建精准的模型。为了解决“数据孤岛”的情况，联邦学习应运而生[1]。目前已有许多横向联邦学习的商业落地应用案例，但仍处于初级阶段，尤其是数据安全方面仍存在许多技术挑战，而认证及会话密钥协商是保证通信实体之间安全传输、可靠通信的关键技术和基本的安全保障。

随着用户量的增大，基于对称密码体制和基于公钥基础设施(public key infrastructure, PKI)的密码体制认证和密钥协商协议中存在密钥管理和维护的问题。1985年Shamir[2]提出基于身份的密码体制，将用户身份与公钥绑定，省去证书的参与，大大降低了PKI存储和管理上的消耗。因此，越来越多的基于身份的认证及密钥协商协议被相继提出。Boneh和Franklin[3]利用双线性对的理论设计基于身份的认证密钥协商协议。随后Jegadeesan等[4]及Bakhtiari-chehel cheshmeh和Hosseinzadeh[5]提出适用于分布式云计算环境下的移动设备的认证及密钥协商协议，具有双向认证、用户的不可追踪和不可否认等特性。但是Wu等[6]证明文献[5]提出的协议很容易受到中间人攻击和伪造攻击，因此，文献[6]改进了该协议，提供了具有更高安全性和有效性的协议。

由于双线性对的计算开销较大，且找出满足双线性对的群很困难，因此，一些研究提出了基于非双线性对进行密钥协商[7-17]。Zhu等[7]和Cao等[8]提出非双线性对基于身份的两方认证密钥协商协议(ID-2PAKA)，该协议中采用3次信息交换实现密钥协商。随后，Cao等[9]又在此基础上做了改进，通过2轮信息交换完成密钥协商，降低了计算开销和通信轮数。但是Islam和Biswas[10]分析了文献[9]提出的协议，发现该协议易受到已知会话特定临时信息攻击(known session-specific temporary information attack, KSTIA)和密钥偏移攻击(key off-set attack, KOA)，因此，文献[10]弥补了文献[9]的安全缺陷，可以对其他参与方的会话密钥做哈希检查，避免在信息交互的过程中出现篡改和假冒攻击。但是该

收稿日期：2021-04-27；录用日期：2021-07-11；网络出版时间：2021-07-30 17:03
网络出版地址：kns.cnki.net/kcms/detail/11.2625.V.20210730.1134.003.html
基金项目：国家自然科学基金(U1736114)；国家重点研发计划(2017YFB0802805)
*通信作者. E-mail：mhli1@bjtu.edu.cn

引用格式：任杰，黎妹红，杜晔，等. 横向联邦学习环境基于身份认证及密钥协商协议[J]. 北京航空航天大学学报，2023，49(2)：397-405.
REN J，LI M H，DU Y，et al. Identity-based authentication key agreement protocol for horizontal federated learning environment[J]. Journal of Beijing University of Aeronautics and Astronautics，2023，49(2)：397-405 (in Chinese).

协议中缺少前向安全性。针对此问题，Daniel 等[11]针对文献 [10] 的协议做出了改进，并证明在扩展的 CK（extended Canetti-Krawczyk, eCK）模型[12]下是安全的。但是结合横向联邦学习环境，该协议只有在计算会话密钥后才能认证双方的身份。若协商阶段存在中间人攻击，则此次的会话密钥计算无效，给双方带来不必要的计算开销和通信开销。因此，本文结合横向联邦学习环境，提出了基于身份的椭圆曲线无证书的轻量级认证及会话密钥协商协议，在保证安全性的同时，权衡计算开销和通信开销，在实际的应用场景下具有更好的平衡性。

1 准备工作

1.1 相关困难问题及假设

本文的认证及会话密钥协商协议的安全性和证明条件依赖于以下问题：

1) 椭圆曲线离散对数问题（elliptic curve discrete logarithm problem, ECDLP）。设P_e和Q是椭圆曲线E上的2个解点，n为任意正整数，且$1<n<|E|$，其中$|E|$为椭圆曲线E的阶数。对于给定的P_e和n，计算$nP_e=Q$是容易的。但若已知P_e和Q两点，计算出n是极其困难的。

2) 计算性假设（computational diffie-hellman, CDH）。对于一个q阶环群G，其中，q为素数，P为群G的生成元，取任意整数$a,b\in Z_q^*$，其中，Z_q^*为乘法群，在给定P,aP,bP情况下无法在多项式时间内计算出abP。

3) 决定性假设（decision diffie-hellman, DDH）。对于一个q阶环群G，取任意整数$a,b,c\in Z_q^*$，在给定P，aP,bP,cP的情况下，判断是否有$\mathrm{CDH}(aP,bP)=cP$即$cP=abP$，是无法在多项式时间内完成的。

1.2 Forking 引理

给定一个安全参数为k的签名机制 (Kgen,sign, verf)，其中，Kgen为密钥生成算法，sign为签名算法，verf为验证算法。假设$\mathcal{A}$为概率多项式时间内的图灵机，其输入为公共数据，并用$q_h>0$表示$\mathcal{A}$访问随机预言机H的次数。假设在时间T内，$\mathcal{A}$以概率$\varepsilon\geqslant 7q_h/2^k$得到的有效签名$(m,r,h,s)$，其中，$m$为消息内容，$r$为承诺内容，$h$为关于$m$和$r$的哈希值，$s$为关于$h$和$r$的答案，则通过重放攻击，可以在有效时间$T'\leqslant 16Q_T/\varepsilon$内，以概率$\varepsilon'\geqslant 1/9$获得2个消息内容与承诺内容相同的有效签名$(m,r,h,s)$和$(m,r,h',s')$，且满足$h'\neq h$，其中，$h'$、$s'$为通过重放攻击后计算不同于$h$与$s$的哈希值和解密值。

1.3 eCK 安全模型

eCK模型主要是针对两方认证及密钥协商协议的一种安全性较强的形式化分析模型，虽然证明过程较为复杂，但是其安全性优势明显。在eCK模型中每个参与者或攻击者都被模拟成一个具备概率多项式时间的预言机，其以多项式次数执行协议，预言机$\Pi_{i,\mathrm{sj}}^t$表示用户i与服务器sj的第t次密钥协商。攻击者可以控制各方交换通信，还可以利用多种方式在eCK模型下被允许进行监听、篡改、重放等基本的攻击方式。在该模型下攻击者A可以请求以下查询。

1）Send$(\Pi_{i,\mathrm{sj}}^t,M)$查询。攻击者$A$向预言机$\Pi_{i,\mathrm{sj}}^t$发送消息$M$，预言机会按照协议执行返回给攻击者消息。如果允许Send查询，则攻击者A将控制所有的通信，并可以取消或修改现有的消息，插入新的消息，如果Send查询不被允许执行，则攻击者只能被动的监听参与方之间的消息传递。

2）StaticKeyReveal(U)查询。攻击者A可以通过该查询获得参与方U的长期私钥。

3）SessionKeyReveal$(\Pi_{i,\mathrm{sj}}^t)$查询。攻击者A可以获得在会话$\Pi_{i,\mathrm{sj}}^t$中协商计算的会话密钥。

4）EphemeralKeyReveal$(\Pi_{i,\mathrm{sj}}^t)$查询。攻击者A可以通过会话$\Pi_{i,\mathrm{sj}}^t$获得用户的临时私钥。

5）Establishedparty(U)查询。攻击者A可以利用此查询获得参与方的长期私钥。因此，若攻击者有发起该请求，则参与方是诚实的。

6）Test$(\Pi_{i,\mathrm{sj}}^t)$查询。攻击者A可以在实验的任何阶段选择新鲜的随机预言机$\Pi_{i,\mathrm{sj}}^t$进行该查询，但是只能发起一次。而查询的结果取决于随机选择的比特$\mathrm{bit}\in\{0,1\}$，当$\mathrm{bit}=0$时，将返回经协商后实际的会话密钥，否则会在会话密钥空间中选择随机值。

攻击者A会根据所有发起的查询请求，猜测bit的值为bit'，若bit' = bit，则攻击者A在本次游戏中获胜，定义获胜的优势$\mathrm{Adv}_{\Pi_{i,\mathrm{sj}}^t}(A)$如下：

$$\mathrm{Adv}_{\Pi_{i,\mathrm{sj}}^t}(A)=\left|\Pr(\mathrm{bit}=\mathrm{bit}')-1/2\right| \tag{1}$$

式中：Pr为概率。

定义 1 匹配会话。若某会话$\Pi_{i,\mathrm{sj}}$发起的消息被传输到$\Pi_{\mathrm{sj},i}$，$\Pi_{\mathrm{sj},i}$的应答消息被传回到$\Pi_{i,\mathrm{sj}}$，则两会话互为匹配会话。

定义 2 新鲜会话。如果预言机$\Pi_{i,\mathrm{sj}}^t$计算后得到了一个会话密钥SK，并满足以下条件：

1）预言机$\Pi_{i,\mathrm{sj}}^t$及匹配预言机$\Pi_{\mathrm{sj},i}$没有受到SessionKeyReveal的查询；

2）预言机$\Pi_{i,\mathrm{sj}}^t$及匹配预言机$\Pi_{\mathrm{sj},i}$没有受到StaticKeyReveal和EphemeralKeyReveal的查询；

3）若$\Pi_{i,\mathrm{sj}}^t$的匹配预言机不存在，且服务器sj未受到StaticKeyReveal的查询；此时会话是新鲜的。

定义 3 安全的会话密钥协商协议。若认证

及密钥协商协议满足以下条件:

1) 2 个相互匹配的随机预言机计算出相同的会话密钥;

2) 对于任意攻击者 A,$\mathrm{Adv}_{\Pi_{i,sj}^{l}}(A)$成功的概率是可忽略的。

此时该密钥协商协议在 eCK 模型下是安全的。

1.4　攻击者模型

在实际训练环境下, 会遭到各种类型的攻击和安全威胁。本文在方案设计中, 是基于横向联邦学习环境, 主要考虑以下几个方面的安全威胁。

1) 窃听攻击。在横向联邦学习环境中, 用户更多利用无线通信传递消息, 信道处于开放的状态, 因此, 攻击者可以监听通信信道传输的信息, 进而实现窃听攻击。

2) 攻击者可以对监听的信息进行拦截、重构和重放, 实现篡改攻击、伪造攻击、重放攻击等。

3) 密钥生成中心(key generation center, KGC)的半诚实性。在密钥生成中心会产生内部攻击, 恶意的参与方会盗取用户的密钥信息并利用在后续的密钥协商中。

2　认证及会话密钥协商协议描述

结合横向联邦学习环境中要求参与方在协议中的控制权, 本文提出单服务器环境下基于身份的无证书轻量级认证及密钥协商协议。在本文方案中, 首先, KGC 生成公开系统参数集合, 参与训练的用户和服务器在 KGC 完成注册, 并计算各自的临时密钥和长期密钥。之后, 参与方可对服务器发起认证协商请求。本节详细阐述了本文方案中的初始化模块、注册模块、认证及密钥协商模块。

2.1　初始化模块

在该系统中, KGC 定义循环加群 G, G 的素数阶 q。KGC 为循环加群选择生成元 P, 并选择随机值$x\in Z_q^*$, x 为系统主私钥, 计算系统公钥 $P_{\mathrm{pub}}=xP$。KGC 还需要定义 4 个哈希函数$H_1,H_2,H_3,H_{\mathrm{MAC}}$, 其式分别为

$$H_1=\{0,1\}\times G\to Z_q^* \tag{2}$$

$$H_2=\{0,1\}\times\{0,1\}\times\{0,1\}\to Z_q^* \tag{3}$$

$$H_3=\{0,1\}\times\{0,1\}\times G^4\to\{0,1\}^l \tag{4}$$

$$H_{\mathrm{MAC}}=G\times G\times\{0,1\}^l\to Z_q^* \tag{5}$$

式中: l 为最终会话密钥的长度。

完成式(2)~式(5)的计算后, KGC 会将 x 保密存储, 并公开系统参数集合$\{G,q,P,P_{\mathrm{pub}},H_1,H_2,H_3,H_{\mathrm{MAC}}\}$。

2.2　注册模块

当存在参与方申请参与联邦学习模型训练时, 需要参与方在 KGC 注册, 其注册详细流程如图 1 所示。注册过程描述如下。

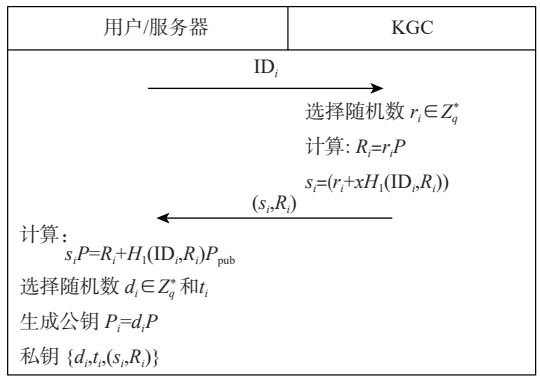

图 1　注册模块

Fig. 1　Registration module

1) 用户 i 给 KGC 发送身份标识ID_i, KGC 给用户 i 随机选择 $r_i\in Z_q^*$, 并计算 $R_i=r_iP$, $s_i=(r_i+xH_1(\mathrm{ID}_i,R_i))$, 因此, KGC 为用户生成部分私钥$(s_i,R_i)$, 并由安全信道发送给用户 i。

2) 当用户 i 收到 KGC 传来的部分私钥(s_i,R_i), 首先验证其准确性, 用户需要计算$s_iP=R_i+H_1(\mathrm{ID}_i,R_i)P_{\mathrm{pub}}$。若等式成立, 则证明用户 i 收到的为 KGC 发送的部分私钥组。

3) 用户私钥生成。用户私钥由 3 部分组成, 长期私钥、临时私钥和部分私钥。因此, 用户 i 随机选取一个随机数$d_i\in Z_q^*$和t_i, d_i 和 t_i 分别为长期私钥和临时私钥。计算公钥$P_i=d_iP$。因此, 用户 i 的私钥组为$\{d_i,t_i,(s_i,R_i)\}$, 公钥为P_i, 其中P_i可以放在公共目录中, 供其他密钥协商方使用。

服务器 sj 注册过程同用户i。

2.3　认证及会话密钥协商模块

注册完成后, 用户和服务器进行双向身份认证和会话密钥协商, 其协商流程如图 2 所示, 协商过程描述如下:

1) 用户 i 首先计算$T_i=t_iP$,利用私钥组$\{d_i,t_i,s_i\}$计算Q_i, 其式为$Q_i=t_i(s_i+d_i)^{-1}\mathrm{mod}q$, 其中 mod 为模型运算。随后参与方选择一个新鲜随机数 nonce, 利用H_2, 计算$H_i=H_2(\mathrm{ID}_i,T_i,\mathrm{nonce})$。当完成 H_i 的计算后, 用户i将消息$(\mathrm{ID}_i,R_i,Q_i,H_i,\mathrm{nonce})$发送给服务器 sj。

2) 当服务器 sj 收到来自用户 i 的认证请求后, 首先, 检查收到的新鲜随机值 nonce, 若该值在本次通信中具有新鲜性, 服务器 sj 即可将其作为后续会话密钥协商及模型训练的参数, 保证训练的安全性和训练参与方身份的有效性。然后, 服务器计算T_i', $T_i'=Q_i\left(P_i+R_i+H_i(\mathrm{ID}_i,R_i)P_{\mathrm{pub}}\right)$, 利用$T_i'$计算$H_i'=H_2\left(\mathrm{ID}_i,T_i',\mathrm{nonce}\right)$是否等于用户$i$传送过来的$H_i$, 若相等则证明服务器进入密钥协商阶段。

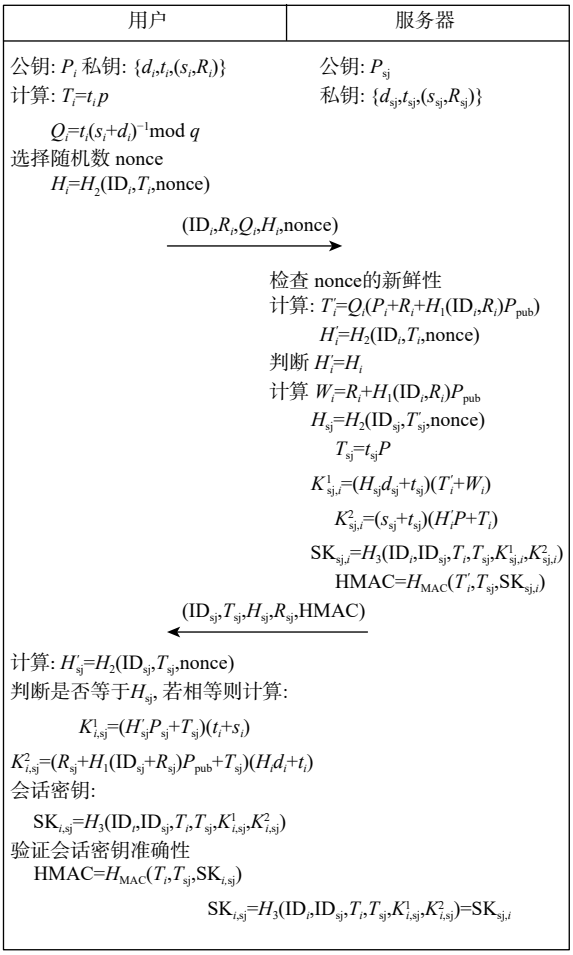

图2 认证及密钥协商模块

Fig. 2 Authentication and key agreement module

服务器利用私钥等参数,计算$W_i=R_i+H_1(\mathrm{ID}_i,R_i)P_{\mathrm{pub}}$、$H_{\mathrm{sj}}=H_2(\mathrm{ID}_{\mathrm{sj}},T_{\mathrm{sj}},\mathrm{nonce})$、$T_{\mathrm{sj}}=t_{\mathrm{sj}}P$,接下来计算会话密钥参数,$K_{\mathrm{sj},i}^1=(H_{\mathrm{sj}}d_{\mathrm{sj}}+t_{\mathrm{sj}})(T_i'+W_i)$、$K_{\mathrm{sj},i}^2=(s_{\mathrm{sj}}+t_{\mathrm{sj}})\cdot(H_i'P_i+T_i)$。即会话密钥$\mathrm{SK}_{\mathrm{sj},i}=H_3(\mathrm{ID}_i,\mathrm{ID}_{\mathrm{sj}},T_i,T_{\mathrm{sj}},K_{\mathrm{sj},i}^1,K_{\mathrm{sj},i}^2)$,服务器对SK计算哈希值,生成$\mathrm{HMAC}=H_{\mathrm{MAC}}(T_i',T_{\mathrm{sj}},\mathrm{SK}_{\mathrm{sj},i})$。完成第2步中的计算后,服务器将消息$(\mathrm{ID}_{\mathrm{sj}},T_{\mathrm{sj}},H_{\mathrm{sj}},R_{\mathrm{sj}}\mathrm{HMAC})$发送给用户$i$。

3) 当用户收到来自服务器的消息后,首先,计算$H_{\mathrm{sj}}'=H_2(\mathrm{ID}_{\mathrm{sj}},T_{\mathrm{sj}},\mathrm{nonce})$,其结果是否等于$H_{\mathrm{sj}}$,若相等,则可以判断$T_{\mathrm{sj}}$的正确性及身份的合法性。然后用户计算会话密钥参数$K_{i,\mathrm{sj}}^1$和$K_{i,\mathrm{sj}}^2$,其中:

$$K_{i,\mathrm{sj}}^1=(H_{\mathrm{sj}}'P_{\mathrm{sj}}+T_{\mathrm{sj}})(t_i+s_i) \tag{6}$$

$$K_{i,\mathrm{sj}}^2=(R_{\mathrm{sj}}+H_1(\mathrm{ID}_{\mathrm{sj}},R_{\mathrm{sj}})P_{\mathrm{pub}}+T_{\mathrm{sj}})(H_id_i+t_i) \tag{7}$$

根据式(6)和式(7)的结果,计算得到会话密钥为$\mathrm{SK}_{i,\mathrm{sj}}=H_3(\mathrm{ID}_i,\mathrm{ID}_{\mathrm{sj}},T_i,T_{\mathrm{sj}},K_{i,\mathrm{sj}}^1,K_{i,\mathrm{sj}}^2)$,并计算$\mathrm{HMAC}'=H_{\mathrm{MAC}}(T_i,T_{\mathrm{sj}},\mathrm{SK}_{i,\mathrm{sj}})$验证生成密钥的准确性,若经过哈希计算后得到的值与接收到的HMAC相同,则此次会话密钥协商完成。

3 安全性分析与证明

定理1 假设CDH是困难问题,哈希函数H_1、H_2、H_3是随机预言机,则提出的模型在eCK模型下是安全的[11]。

证明 在1.3节提出的认证及密钥协商协议的正确性要求相匹配的会话要返回相同的会话密钥,因此,根据协议安全性要求,只需要证明攻击者无法在概率多项式的时间内有不可忽略的概率赢得游戏来证明协议的安全性。

3.1 随机预言机安全模型

会话密钥SK的计算需要利用元组$(\mathrm{ID}_i,\mathrm{ID}_{\mathrm{sj}},T_i,T_{\mathrm{sj}},K_{i,\mathrm{sj}}^1,K_{i,\mathrm{sj}}^2)$,发起$H_3$请求,挑战者$C$会维护3个独立列表来模拟$H_1$、$H_2$、$H_3$,挑战者$C$会将每一条输入输出记录在列表中。如果攻击者$A$发起了哈希请求,并在列表中可以找到相匹配的某个参与方的值,则挑战者C会将匹配的值输出给攻击者A,否则挑战者C会随机生成一个值输出,并将其记录在列表中。

H_1预言机。挑战者C为H_1预言机初始化一个空列表H_1^{List},在列表中每一个实体组成是$(\mathrm{ID}_i,R_i,H_1)\in\{0,1\}^{\mathrm{len}(\mathrm{ID}_i)}\times G\times Z_q^*$,$\mathrm{len}(\cdot)$为计算消息bit长度的函数,当挑战者$C$计算参与方的部分私钥后,将该元组插入列表中。在游戏过程中,若攻击者发起H_1请求,挑战者C会在列表中查找是否有匹配的信息,将查找元组输出给攻击者A,否则挑战者C随机选择一个随机数$N_{\mathrm{rad}}\ (N_{\mathrm{rad}}\in Z_q^*)$,返回给攻击者$A$,同时将该值记录在$H_1^{\mathrm{List}}$中。

H_2预言机。挑战者C为H_2预言机初始化一个空列表H_2^{List},在列表中每一个实体组成是$(\mathrm{ID}_i,T_i,\mathrm{nonce},H_2)\in\{0,1\}^{\mathrm{len}(\mathrm{ID}_i)}\times\{0,1\}^{\mathrm{len}(T_i)}\times\{0,1\}^{\mathrm{len}(\mathrm{nonce}_i)}\times Z_q^*$。在游戏过程中,攻击者如果发起了$H_2$请求,挑战者$C$会在列表中查找是否有匹配的信息,如果有则直接将查找元组输出给攻击者A,否则挑战者C要随机选择一个随机数$N_{\mathrm{rad}}\ (N_{\mathrm{rad}}\in Z_q^*)$,返回给攻击者$A$,同时将该值记录在$H_2^{\mathrm{List}}$中。

H_3预言机。挑战者C为H_3预言机初始化一个空列表H_3^{List},在列表中每一个实体组成是$(\mathrm{ID}_i,\mathrm{ID}_{\mathrm{sj}},T_i,T_{\mathrm{sj}},K_{i,\mathrm{sj}}^1,K_{i,\mathrm{sj}}^2,\mathrm{SK})\in\{0,1\}\times\{0,1\}\times G^4\times\{0,1\}^l$,挑战者$C$需要确保SessionSecretReveal请求与H_3预言机一致,才能成功模拟H_3预言机。但是在某些情况下,挑战者C可能无法得到所有元素以计算有效的会话密钥存储在H_3^{List}中,因此,挑战者C会维护另一张表l^{list},其中列表元素组成为$(\mathrm{ID}_i,\mathrm{ID}_{\mathrm{sj}},T_i,T_{\mathrm{sj}},\mathrm{SK}')$。当有SessionSecretReveal请求时,会首先检查l^{list},若列表中存在匹配的元素,则返回对应的SK'给攻击者A,并将其添加到H_3^{List}。否则检查H_3^{List},并利用

DDH oracle 模型检查共享密钥$K_{i,\mathrm{sj}}^1$、$K_{i,\mathrm{sj}}^2$的正确性, 正确则返回 SK, 并添加在l^{list}中, 否则挑战者 C 生成随机数$N_{\mathrm{rad}}, N_{\mathrm{rad}} \in \{0,1\}^l$, 并记录在$l^{\mathrm{list}}$列表中。

3.2　安全游戏模型设计

在会话$\Pi_{i,\mathrm{sj}}^{\mathrm{T}}$中, 攻击者可能模拟$\mathrm{ID}_i$, 因此, 挑战者 C 只知道另一方服务器 sj 的临时私钥t_{sj}, 并不知道ID_i的部分私钥已经被攻击者 A 获取, 此时挑战者 C 会向被攻击者 A 控制的诚实参与方中嵌入一个 CDH 假设问题, 挑战者 C 无法计算$K_{i,\mathrm{sj}}^1$、$K_{i,\mathrm{sj}}^2$的正确性, 但是仍然需要回答H_3请求和 SessionSecretReveal 请求, 因此, 当攻击者 A 请求H_3时, 会输入$\left(\mathrm{ID}_i, \mathrm{ID}_{\mathrm{sj}}, T_i, T_{\mathrm{sj}}, K_{i,\mathrm{sj}}^1, K_{i,\mathrm{sj}}^2\right)$。挑战者 C 首先会检查l^{list}中是否存在会话$\left(\mathrm{ID}_i, \mathrm{ID}_{\mathrm{sj}}, T_i, T_{\mathrm{sj}}\right)$或匹配会话$(\mathrm{ID}_{\mathrm{sj}}, \mathrm{ID}_i, T_{\mathrm{sj}}, T_i)$, 若找到匹配元组, 则验证$K_{i,\mathrm{sj}}^1, K_{i,\mathrm{sj}}^2$是否符合 DDH 条件, 即

$$\mathrm{DDH}\left(H_{\mathrm{sj}}P_{\mathrm{sj}} + T_{\mathrm{sj}}, T_i' + W_i, K_{i,\mathrm{sj}}^1\right) = 1 \tag{8}$$

$$\mathrm{DDH}\left(H_{\mathrm{sj}}P_{\mathrm{sj}} + T_{\mathrm{sj}}, W_i + T_i, K_{i,\mathrm{sj}}^2\right) = 1 \tag{9}$$

如果验证成功, 则返回H_3中的值 SK 作为答案, 因此, 攻击者可以获得此次会话协商的密钥。

假设$\mathrm{Adv}_A(\lambda)$代表给定条件下, 攻击者赢得游戏的优势, λ为安全参数, $\mathrm{ns}(\lambda)$为攻击者可以发起的最多会话次数, $\mathrm{ne}(\lambda)$为攻击者可以查询的最多参与者的数量, $\mathrm{nas}(\lambda)$为攻击者可激活的最多会话次数, $\mathrm{nq}(\lambda)$为攻击者可激活的与预言机H_3不同的哈希请求。由于H_3是随机预言机模型, 攻击者 A 可以有 2 种方法, 从测试会话中区分随机字符串。

1) 密钥重放攻击。攻击者 A 强制不匹配的会话计算与测试会话相同的会话密钥, 攻击者 A 可以通过查询不匹配会话的密钥获取测试会话的会话密钥。在安全游戏中, 根据假设前提, H_3是随机预言机, 猜测输出的会话密钥的概率是$O\left(1/2^l\right)$, 该值是可忽略的。由于 2 次会话是不相匹配的会话, 参与方是不同的, 退一步讲, 当攻击者选中的会话是重放密钥的协商双方, 但是由于不同的会话其使用的临时密钥是不同的, 因此, 攻击者想要通过密钥重放攻击猜测出本次会话密钥等同于找到H_3碰撞。而每一个攻击者最多可以请求$\mathrm{nas}(\lambda)$次会话, 因此发生碰撞的概率为$O\left(\mathrm{nas}/2^l\right)$, 该值是可忽略的, 因此通过情景 1, 攻击者是无法赢得游戏的。

2) 假冒攻击。假设$\Pi_{i,\mathrm{sj}}^{\mathrm{T}}$为测试会话, 当执行到某一步骤时, 攻击者 A 会在ID_i和$\mathrm{ID}_{\mathrm{sj}}$之间的测试会话中, 利用元组$\left(\mathrm{ID}_i, \mathrm{ID}_{\mathrm{sj}}, T_i, T_{\mathrm{sj}}, K_{i,\mathrm{sj}}^1, K_{i,\mathrm{sj}}^2\right)$发起$H_3$预言机的请求, 在这种情况下, 攻击者会自行计算$K_{i,\mathrm{sj}}^1$、$K_{i,\mathrm{sj}}^2$。在安全游戏中, 挑战者 C 利用攻击者 A 的优势从测试会话中区分随机字符串, 挑战者 C 自身有解决 CDH 问题的优势, 会模拟攻击者 A 的安全游戏, 并回答攻击者 A 的所有请求。在游戏开始前, 挑战者 C 猜测测试会话和攻击者可能采取的方法。为了达到这个目的, 挑战者从 ne 个参与者中选中 2 个, 从可激活的会话中 nas 中确定测试会话, 在此用$\Pi_{i,\mathrm{sj}}^{\mathrm{T}}$表示选择的测试会话, 挑战者 C 选择正确的参与实体及会话的概率为$1/\left[\mathrm{nas}(\lambda)\mathrm{ne}(\lambda)^2\right]$, 挑战者会根据可能出现的结果来模拟, 当挑战者 C 猜测错误时游戏终止, 否则游戏程序正常进行。

由于协议双方协商的机制, 需要存在与测试会话相匹配的会话, 基于该要求, 提出以下 2 个情景。

情景 1。所有的诚实参与者均没有与测试会话相匹配的会话。

情景 2。存在与测试会话相匹配的会话, 而且该会话由某个参与者所有。

假设测试会话为$\Pi_{i,\mathrm{sj}}^{\mathrm{T}}$, 与之相匹配的会话为$\Pi_{\mathrm{sj},i}^{\mathrm{S}}$。从该会话中可知, 会话密钥协商双方为$\mathrm{ID}_i$、$\mathrm{ID}_{\mathrm{sj}}$, 接下来就本节 2 个情景在 eCK 模型下进行安全证明。

3.3　安全性证明

3.3.1　情景 1 分析

攻击者 A 需要在测试会话中计算出协商的会话密钥, 当攻击者 A 发起测试会话的请求时, 实际上并不存在与之匹配的会话, 因此, 这种情景下攻击者并不知道参与方ID_i、$\mathrm{ID}_{\mathrm{sj}}$的临时私钥和长期私钥。假设挑战者 C 随机选择一个用户 i, 在该情境下, 挑战者 C 并不知道用户 i 的部分私钥及长期密钥, 攻击者 A 模拟服务器$\mathrm{ID}_{\mathrm{sj}}$, 但是并不知道服务器 sj 的部分私钥。因此, 初始化阶段, 挑战者 C 会模拟 KGC 为每一个协议参与方生成部分私钥组(s,R)。挑战者 C 会首先选择系统主公钥 X 并选择随机数, 计算$R_i = s_iP - h_iX$, 对于每一个参与者, 挑战者 C 都会发送部分密钥组(s_i,R_i)给攻击者 A, 并将元组$\{s_i,R_i,h_i\}$添加到H_1^{List}中, 令$h_i = H_1(\mathrm{ID}_i,R_i)$, 挑战者 C 会给攻击者提供用户 i 的临时私钥Y, 以及长期公钥Z。如果挑战者 C 选择了$\Pi_{i,\mathrm{sj}}^{\mathrm{T}}$作为测试会话, 则该游戏模拟不会失败。攻击者 A 会模拟服务器$\mathrm{ID}_{\mathrm{sj}}$按照协议的要求计算相应的应答元组中的元素, 在测试会话$\Pi_{i,\mathrm{sj}}^{\mathrm{T}}$中, 用户$\mathrm{ID}_i$从攻击者 A 处收到消息$\left(\mathrm{ID}_{\mathrm{sj}}, T_{\mathrm{sj}}, H_{\mathrm{sj}}, R_{\mathrm{sj}}, \mathrm{HMAC}\right)$, 其中$R_{\mathrm{sj}}$是由攻击者 A 随机生成, 对于$\mathrm{ID}_{\mathrm{sj}}$来说是不正确的, 挑战者 C 设置$H_1(\mathrm{ID}_i,R_i) = \overline{h_i} \in Z_q^*$。如果攻击者 A 以不可忽略的优势赢得游戏, 则需要利用元组$(\mathrm{ID}_i, \mathrm{ID}_{\mathrm{sj}}, Y, T_{\mathrm{sj}}, K_{i,\mathrm{sj}}^1, K_{i,\mathrm{sj}}^2)$发起对$H_3$请求, 其中:

$$K_{i,\mathrm{sj}}^1 = \left(H_{\mathrm{sj}}'Z + T_{\mathrm{sj}}\right)\left(D\log_y Y + s_i\right) \tag{10}$$

$$K_{i,\mathrm{sj}}^2 = \left(W_{\mathrm{sj},E} + T_{\mathrm{sj}}\right)\left(H_i D\log_y Z + D\log_y Y\right) \tag{11}$$

$$W_{\mathrm{sj}\to A} = R_{\mathrm{sj}} + H_1\left(\mathrm{ID}_{\mathrm{sj}}, R_{\mathrm{sj}}\right)X = R_{\mathrm{sj}} + \overline{h}_{\mathrm{sj}}X \tag{12}$$

式中: D 为解密。

因此基于式 (10)～式 (12) 的计算, 挑战者 C 仅

能获取部分私钥s_i，临时密钥$t_i=Y$和长期密钥$d_i=Z$，t_{sj}和d_{sj}及计算部分私钥的r_{sj}是由攻击者A选择的。攻击者A要获取临时密钥和长期密钥，需要发起LongKeyReveal和EphemeralKeyReveal请求。因此，为了解决CDH问题，挑战者C会检查攻击者A是否利用元组$(\mathrm{ID}_i,\mathrm{ID}_{\mathrm{sj}},Y,T_{\mathrm{sj}},K_{i,\mathrm{sj}}^1,K_{i,\mathrm{sj}}^2)$发起$H_3$预言机的请求，其中要求：

$$\mathrm{DDH}\left(H_{\mathrm{sj}}'Z+T_{\mathrm{sj}},Y+W_i,K_{i,\mathrm{sj}}^1\right)=1 \tag{13}$$

$$\mathrm{DDH}\left(W_{\mathrm{sj}\to E}+T_{\mathrm{sj}},H_iZ+Y,K_{i,\mathrm{sj}}^2\right)=1 \tag{14}$$

因为攻击者采用假冒攻击的方式请求本次测试会话，因此挑战者C利用Forking定理，采用与攻击者A相同的输入进行接下来的游戏分析。

挑战者C重新设置$H_1(\mathrm{ID}_i,R_i)=\widetilde{h}_i\in Z_q^*$，其中要求$\overline{h}_i\neq\widetilde{h}_i$，且攻击者还会利用元组$(\mathrm{ID}_i,\mathrm{ID}_{\mathrm{sj}},Y,T_{\mathrm{sj}},\tilde{K}_{i,\mathrm{sj}}^1,\tilde{K}_{i,\mathrm{sj}}^2)$发起对$H_3$预言机的请求，以实现概率多项式时间内赢得游戏，其中：

$$\widetilde{K}_{i,\mathrm{sj}}^1=\left(\widetilde{H}_{\mathrm{sj}}'Z+T_{\mathrm{sj}}\right)\left(D\log_yY+s_i\right) \tag{15}$$

$$\widetilde{K}_{i,\mathrm{sj}}^2=\left(\widetilde{W}_{\mathrm{sj}\to E}+T_{\mathrm{sj}}\right)\left(H_iD\log_xZ+D\log_yY\right) \tag{16}$$

$$\widetilde{W}_{\mathrm{sj}\to E}=R_{\mathrm{sj}}+H_1\left(\mathrm{ID}_{\mathrm{sj}},R_{\mathrm{sj}}\right)X=R_{\mathrm{sj}}+\widetilde{h}_{\mathrm{sj}}X \tag{17}$$

因此，当挑战者C检查到攻击者A发起了H_3预言机的请求时，会检查请求元组中是否满足条件：

$$\mathrm{DDH}\left(\widetilde{H}_{\mathrm{sj}}'Z+T_{\mathrm{sj}},Y+W_i,K_{i,\mathrm{sj}}^1\right)=1 \tag{18}$$

$$\mathrm{DDH}\left(\widetilde{W}_{\mathrm{sj}\to E}+T_{\mathrm{sj}},H_iZ+Y,K_{i,\mathrm{sj}}^2\right)=1 \tag{19}$$

并计算困难问题如下：

$$\begin{aligned}K_{i,\mathrm{sj}}^1-\widetilde{K}_{i,\mathrm{sj}}^1=&\left(H_{\mathrm{sj}}'Z+T_{\mathrm{sj}}\right)\left(D\log_yY+s_i\right)-\left(\widetilde{H}_{\mathrm{sj}}'Z+T_{\mathrm{sj}}\right)\cdot\\&\left(D\log_yY+s_i\right)=\left(H_{\mathrm{sj}}'Z-\widetilde{H}_{\mathrm{sj}}'Z\right)\left(D\log_yY+s_i\right)=\\&\left(H_{\mathrm{sj}}'-\widetilde{H}_{\mathrm{sj}}'\right)Z\left(D\log_yY+s_i\right)\end{aligned} \tag{20}$$

对于$K_{i,\mathrm{sj}}^1\sim\widetilde{K}_{i,\mathrm{sj}}^1$结果，挑战者$C$将解决如下CDH问题：

$$(Y,Z)=\left(H_{\mathrm{sj}}'-\widetilde{H}_{\mathrm{sj}}'\right)^{-1}\left(K_{i,\mathrm{sj}}^1-\widetilde{K}_{i,\mathrm{sj}}^1\right)-s_iZ=\left(D\log_yY\right)Z \tag{21}$$

而对于$K_{i,\mathrm{sj}}^2$、$\widetilde{K}_{i,\mathrm{sj}}^2$，计算如下：

$$\begin{aligned}K_{i,\mathrm{sj}}^2-\widetilde{K}_{i,\mathrm{sj}}^2=&\left(W_{\mathrm{sj}\to E}+T_{\mathrm{sj}}\right)\left(H_iD\log_yZ+D\log_yY\right)-\\&\left(\widetilde{W}_{\mathrm{sj}\to E}+T_{\mathrm{sj}}\right)\left(H_iD\log_yZ+D\log_yY\right)=\\&\left(W_{\mathrm{sj}\to E}-\widetilde{W}_{\mathrm{sj}\to E}\right)\left(H_iD\log_yZ+D\log_yY\right)=\\&\left(\left(R_{\mathrm{sj}}+\overline{h}_{\mathrm{sj}}X\right)-\left(R_{\mathrm{sj}}+\widetilde{h}_{\mathrm{sj}}X\right)\right)\cdot\\&\left(H_iD\log_yZ+D\log_yY\right)=\\&X\left(H_iD\log_yZ+D\log_yY\right)\left(\overline{h}_{\mathrm{sj}}-\widetilde{h}_{\mathrm{sj}}\right)\end{aligned} \tag{22}$$

对于$K_{i,\mathrm{sj}}^2-\widetilde{K}_{i,\mathrm{sj}}^2$的结果，挑战者$C$将解决CDH问题如下：

$$(X,Z)=H_i^{-1}\left(\left(\overline{h}_{\mathrm{sj}}-\widetilde{h}_{\mathrm{sj}}\right)^{-1}\left(K_{i,\mathrm{sj}}^2-\widetilde{K}_{i,\mathrm{sj}}^2\right)-\left(D\log_yY\right)X\right)=\left(D\log_yZ\right)X \tag{23}$$

因此，基于Forking引理，挑战者C与攻击者A的优势关系如下：

$$\mathrm{Adv}_{\Pi}(C)\geqslant\frac{\delta}{\mathrm{nas}(\lambda)\mathrm{ne}(\lambda)^2}\mathrm{Adv}_{\Pi}(A) \tag{24}$$

式中：δ为有效签名的概率。在情景1中，挑战者C随机选择测试会话的匹配会话来模拟该协议中，基于eCK模型下的分析，由于CDH问题求解的困难性，所以攻击者在该情境下赢得游戏的概率是可忽略的。

3.3.2 情景2分析

与情景1证明方法类似，当存在与测试会话$\Pi_{i,\mathrm{sj}}^{\mathrm{T}}$相匹配的会话$\Pi_{\mathrm{sj},i}^{\mathrm{M}}$后，攻击者处于被动的状态，只能观察参与方之间交互的信息。挑战者C会随机选择2个参与者i、sj所参与的会话。攻击者会伪造其中一方进行会话密钥协商，利用测试会话和其匹配会话计算出会话密钥SK，因此，首先需要计算出其中的$K_{i,\mathrm{sj}}^1$和$K_{i,\mathrm{sj}}^2$，并且通过其中的H_3预言机的请求获取会话密钥SK。由于攻击者发起的测试会话存在与其相匹配的会话，且在会话密钥协商过程中需要协商双方的长期私钥(d_i,d_{sj})、临时私钥(t_i,t_{sj})及部分私钥组(s_i,R_i)、$(s_{\mathrm{sj}},R_{\mathrm{sj}})$。由于存在测试会话，当选中了某个测试会话后，攻击者A会有正确的部分私钥信息，但是系统的主私钥可能泄露，因此，在初始阶段，挑战者C会模拟KGC生成每一个用户部分私钥，将$\{\mathrm{ID}_i,R_i\}$发送给攻击者，将$\{\mathrm{ID}_i,R_i,h_i\}$元组添加到$H_1^{\mathrm{list}}$列表中。

接下来挑战者C会随机选择2个协议参与方i和sj并选择2个其参与过的会话，利用eCK模型中定义的匹配会话要求，验证选择的2个会话是否匹配，而且每个参与方最多只能选择$\mathrm{ns}(\lambda)$次。因此，初始化结束后，攻击者已经知道参与者的部分私钥。由于在测试会话$\Pi_{i,\mathrm{sj}}^{\mathrm{T}}$中不能对同一参与者发起LongKeyReveal和EphemeralKeyReveal请求，因此假设攻击者A模拟sj，在会话密钥协商中的长期私钥是由参与方自行生成，长期公钥在初始化阶段完成计算，并存储在公共目录中。在此假设攻击者A已知sj和i的长期公钥，因此，攻击者在计算会话密钥中需要已知参与双方针对当前会话的临时私钥，结合该情景，攻击者主要面临如下问题：当测试会话$\Pi_{i,\mathrm{sj}}^{\mathrm{T}}$存在与之相匹配的会话$\Pi_{\mathrm{sj},i}^{\mathrm{M}}$，但是攻击者并不知道本次协商使用的临时私钥$t_i$和$t_{\mathrm{sj}}$。

对于该问题, 攻击者 A 发起 EphemeralKeyReveal 请求, 获取参与方 i 和 sj 的临时密钥。挑战者 C 在回答攻击者 A 的请求时会设置 i 临时密钥 X, sj 临时密钥 Y, 假如攻击者 A 选中了测试会话 $\Pi_{i,\mathrm{sj}}^{\mathrm{T}}$, 则该模拟可能不会失败。攻击者 A 若以不可忽略的概率赢得游戏, 需要利用元组 $\left(\mathrm{ID}_i, \mathrm{ID}_{\mathrm{sj}}, Y, T_{\mathrm{sj}}, K_{i,\mathrm{sj}}^1, K_{i,\mathrm{sj}}^2\right)$ 发起对 H_3 预言机的请求, 其中

$$K_{i,\mathrm{sj}}^1 = \left(H_{\mathrm{sj}}^{'} P_{\mathrm{sj}} + Y\right)\left(D\log_y X + s_i\right) \tag{25}$$

$$K_{i,\mathrm{sj}}^2 = \left(W_{\mathrm{sj}} \to A + Y\right)\left(H_i D\log_y P_i + D\log_y X\right) \tag{26}$$

为了解决 CDH 问题, 挑战者 C 会检查攻击者 A 是否发起 H_3 预言机的请求, 要求

$$\mathrm{DDH}\left(H_{\mathrm{sj}}^{'} P_{\mathrm{sj}} + Y, X + W_i, K_{i,\mathrm{sj}}^1\right) = 1 \tag{27}$$

$$\mathrm{DDH}\left(W_{\mathrm{sj}\to E} + Y, H_i P_i + X, K_{i,\mathrm{sj}}^2\right) = 1 \tag{28}$$

若满足条件, 则挑战者 C 计算如下 CDH 问题:

$$\begin{aligned}\widetilde{K}_{i,\mathrm{sj}}^1 = K_{i,\mathrm{sj}}^1 - H_{\mathrm{sj}}^{'} P_{\mathrm{sj}}\left(D\log_y X + s_i\right) - s_i Y = \left(H_{\mathrm{sj}}^{'} P_{\mathrm{sj}} + Y\right)\cdot \\ \left(D\log_y X + s_i\right) - H_{\mathrm{sj}}^{'} P_{\mathrm{sj}}\left(D\log_y X + s_i\right) - s_i Y = \\ \left(D\log_y X\right) Y\end{aligned} \tag{29}$$

$$\begin{aligned}\widetilde{K}_{i,\mathrm{sj}}^2 = K_{i,\mathrm{sj}}^2 - W_{\mathrm{sj}\to E}\left(H_i D\log_y P_i + D\log_y X\right) - H_i D\log_y P_i \cdot \\ Y = \left(W_{\mathrm{sj}\to E} + Y\right)\left(H_i D\log_y P_i + D\log_y X\right) - \\ W_{\mathrm{sj}\to E}\left(H_i D\log_y P_i + D\log_y X\right) - \left(H_i D\log_y P_i\right) Y = \\ \left(D\log_y X\right) Y\end{aligned} \tag{30}$$

攻击者 A 若在该问题成功进行伪造攻击, 则挑战者 C 一定能解决上述的 CDH 问题, 因此, 挑战者 C 与攻击者 A 的优势关系如下:

$$\mathrm{Adv}_{\Pi}(C) \geqslant \frac{1}{\mathrm{nas}(\lambda)^2 \mathrm{ne}(\lambda)^2}\mathrm{Adv}_{\Pi}(A) \tag{31}$$

综合 3.2 节中的安全问题及证明过程得出的挑战者 C 与攻击者 A 的关系, 当 $\mathrm{Adv}_{\Pi}(A)$ 是不可忽略的值时, $\mathrm{Adv}_{\Pi}(C)$ 也是不可忽略的, 攻击者若以不可忽略的概率赢得模拟游戏, 则需要挑战者 C 解决 CDH 问题, 由于 CDH 困难问题, 因此, 提出的该会话密钥协商协议在 eCK 模型下是安全的。

4　性能分析

为了更好的评价所提协议的安全性和有效性, 本节将分析 Daniel 等[13] 提出的方案、Xie 等[14] 提出的方案、Islam 和 Biawas [10] 提出的方案、郭松辉等 [15] 提出的方案与本节提出的基于身份认证及会话密钥协商方案进行比较。表 1 中对比分析了已有的 4 个协议及本节所提协议的安全属性, 5 组协议中均满足已知会话密钥安全和前向安全性, 但是 Xie 等[14] 和 Islam 和 Biawas [10] 提出的方案中无法满足双向认证及临时密钥泄露攻击, Daniel 等[13] 提出的方案可以对抗临时密钥攻击, 但是无法进行双向认证, 郭松辉等[15] 提出的方案中会话密钥协商前需要进行双向认证后再进行计算会话密钥, 但是存在临时密钥泄露的危险。

表 1　相关协议安全属性对比

Table 1　Security properties comparison among related protocols

协议	双向认证	临时私钥泄露	已知会话密钥安全	前向安全性
文献[14]	×	×	√	√
文献[13]	×	√	√	√
文献[10]	×	×	√	√
文献[15]	√	×	√	√
本文所提协议	√	√	√	√

本文所提协议中除了满足 eCK 模型下基本的安全属性, 还满足用户和服务器的双向认证后再进行会话密钥的计算, 而且在计算过程中基于 CDH 困难问题混淆临时密钥。因此, 结合横向联邦学习环境及现有的认证及密钥协商协议, 所提方案优于其他 4 个方案。

为了评估计算开销, 本节定义 T_{M} 为标量乘操作的计算时间, T_{A} 为点加运算[13]。分析协议计算性能比较如表 2 所示。

表 2　性能分析

Table 2　Performance analysis

协议	计算开销	通信轮数
文献[14]	$4T_{\mathrm{M}} + 4T_{\mathrm{A}}$	2
文献[13]	$10T_{\mathrm{M}} + 6T_{\mathrm{A}}$	2
文献[10]	$6T_{\mathrm{M}} + 4T_{\mathrm{A}}$	2
文献[15]	$4T_{\mathrm{M}} + 8T_{\mathrm{A}}$	2
本文所提协议	$6T_{\mathrm{M}} + 4T_{\mathrm{A}}$	2

表 2 的协议中均采用了无证书基于身份的认证及密钥协商协议, 消除了双线性对运算, 完成认证及密钥协商只需要 2 轮通信, 在通信开销上并没有频繁的信息交互, 但是在计算效率上, 虽然本文所提协议相对文献 [14] 提出的协议计算时间大于 $2T_{\mathrm{M}}$, 但是从安全性方面, 本文所提协议安全性更高, 因此, 综合安全性和计算开销, 所提方案更适合计算能力较低的终端设备作为用户完成与中央服务器的聚合, 更具备经济价值。

5　结　论

1) 本文结合横向联邦学习训练环境及现有的认证及会话密钥协商协议, 提出无证书的基于身份的轻量级认证及密钥协商协议。

2）所提协议中在双方完成双向认证后再进行会话密钥协商，避免因为攻击问题产生不必要的计算开销。

3）在安全性分析方面，除了传统的正确性分析和基本的安全属性分析，还引入eCK模型，通过模拟攻击者可能采用的攻击手段进行模拟游戏，证明所提协议的安全性能。

4）在计算性能和通信开销方面可以有效地控制成本，因此所提协议在实际应用场景中有较高的价值。

参考文献（References）

[1] MCMAHAN H B, MOORE E, RAMAGE D, et al. Communication-efficient learning of deep networks from decentralized data[C]// 20th International Conference on Artificial Intelligence and Statistics. Fort Lauderdale: PMLR, 2017: 1273-1282.

[2] SHAMIR A. Identity-based cryptosystems and signature schemes [C]//Advances in Cryptology. Berlin: Springer , 1985: 47-53.

[3] BONEH D, FRANKLIN M. Identity-based encryption from the Weil pairing[C]// Advances in Cryptology. 2001: 213-229.

[4] JEGADEESAN S, AZEES M, KUMAR P M, et al. An efficient anonymous mutual authentication technique for providing secure communication in mobile cloud computing for smart city applications[J]. Sustainable Cities and Society, 2019, 49: 101522.

[5] BAKHTIARI-CHEHELCHESHMEH S, HOSSEINZADEH M. A new certificateless and secure authentication scheme for ad hoc networks[J]. Wireless Personal Communications, 2017, 94(4): 2833-2851.

[6] WU L B, WANG J, RAYMOND CHOO K K, et al. An efficient provably-secure identity-based authentication scheme using bilinear pairings for Ad hoc network[J]. Journal of Information Security and Applications, 2017, 37: 112-121.

[7] ZHU R W, YANG G M, WONG D S. An efficient identity-based key exchange protocol with KGS forward secrecy for low-power devices[J]. Theoretical Computer Science, 2007, 378(2): 198-207.

[8] CAO X, KOU W, YU Y, et al. Identity-based authentication key agreement protocols without bilinear parings[J]. IEICE Transaction on Fundamentals, 2008, E91.A(12): 3833-3836.

[9] CAO X F, KOU W D, DU X N. A pairing-free identity-based authenticated key agreement protocol with minimal message exchanges[J]. Information Sciences, 2010, 180(15): 2895-2903.

[10] ISLAM S H, BISWAS G P. An improved pairing-free identity-based authenticated key agreement protocol based on ECC[J]. Procedia Engineering, 2012, 30: 499-507.

[11] DANIEL R M, RAJSINGH E B, SILAS S. An efficient ECK secure certificateless authenticated key agreement scheme with security against public key replacement attacks[J]. Journal of Information Security and Applications, 2019, 47: 156-172.

[12] LAMACCHIA B, LAUTER K, MITYAGIN A. Stronger security of authenticated key exchange[C]//International Conference on Provable Security. Berlin: Springer, 2007: 1-16.

[13] DANIEL R M, RAJSINGH E B, SILAS S. An efficient ECK secure identity based two party authenticated key agreement scheme with security against active adversaries[J]. Information and Computation, 2020, 275: 104630.

[14] XIE Y, WU L B, SHEN J, et al. Efficient two-party certificateless authenticated key agreement protocol under GDH assumption[J]. International Journal of Ad Hoc and Ubiquitous Computing, 2019, 30(1): 11.

[15] 郭松辉, 牛小鹏, 王玉龙. 一种基于椭圆曲线的轻量级身份认证及密钥协商方案[J]. 计算机科学, 2015, 42(1): 137-141.
GUO S H, NIU X P, WANG Y L. Elliptic curve based light-weight authentication and key agreement scheme[J]. Computer Science, 2015, 42(1): 137-141(in Chinese).

[16] 曹阳, 邓方安, 陈涛, 等. 一种基于身份可认证两方密钥协商方案[J]. 成都理工大学学报(自然科学版), 2016, 43(6): 757-761.
CAO Y, DENG F G, CHEN T, et al. A two-party key agreement scheme based on authenticated identity[J]. Journal of Chengdu University of Technology (Science & Technology Edition), 2016, 43(6): 757-761(in Chinese).

[17] 周彦伟, 杨波, 张文政. 一种改进的无证书两方认证密钥协商协议[J]. 计算机学报, 2017, 40(5): 1181-1191.
ZHOU Y W, YANG B, ZHANG W Z. An improved two-party authenticated certificateless key agreement protocol[J]. Chinese Journal of Computers, 2017, 40(5): 1181-1191(in Chinese).

Identity-based authentication key agreement protocol for horizontal federated learning environment

REN Jie[1, 2], LI Meihong[1, 2, *], DU Ye[1, 2], YIN Liguanjin[1, 2]

(1. Beijing Key Laboratory of Security and Privacy in Intelligent Transportation, Beijing Jiaotong University, Beijing 100044, China;
2. School of Computer and Information Technology, Beijing Jiaotong University, Beijing 100044, China)

Abstract: In recent years, federated learning has received extensive attention in many fields, but this technology inevitably causes data transmission security problems. However, authentication and key agreement are important to ensure secure transmission and reliable communication between communicating entities. This study suggests a lightweight certificateless authentication and key agreement protocol that is identity-based and takes into account the data properties of horizontal federated learning. The participants need to register at the key generation center (KGC) and use public parameters to calculate their temporary keys and long-term keys which is to complete authentication and calculate the session key. Subsequently, the eCK model is used to prove the security of the protocol proposed in this paper. A thorough analysis shows that this protocol is appropriate for a single-server horizontal federated learning environment since it has full security features, low processing and communication costs.

Keywords: horizontal federated learning; identity-based cryptosystem; certificateless; authentication and key agreement; eCK model

Received: 2021-04-27; **Accepted**: 2021-07-11; **Published Online**: 2021-07-30 17:03

URL: kns.cnki.net/kcms/detail/11.2625.V.20210730.1134.003.html

Foundation items: National Natural Science Foundation of China (U1736114); The National Key R & D Program of China (2017YFB0802805)

* **Corresponding author**. E-mail: mhli1@bjtu.edu.cn