面向数据出域安全的鲁棒认证密钥协商协议

张晶辉[1,2,3]，张起嘉[4]，刘海[4]，田有亮[4,5]，李凤华[1,2,3]

（1.中国科学院信息工程研究所，北京 100085；2.中国科学院大学网络空间安全学院，北京 100049；
3.网络空间安全防御全国重点实验室，北京 100085；4.贵州大学计算机科学与技术学院，贵州 贵阳 550025；
5.贵州大学大数据与信息工程学院，贵州 贵阳 550025）

摘　要：针对数据出域场景下的数据安全传输需求，给出了相应的系统模型与安全模型，并提出了一种基于TEE的鲁棒认证密钥协商协议。该协议基于收发双方的可信执行环境，实现了传输密钥的高效抗干扰合成。通过理论证明，所提协议中的通信消息具有机密性和存在性不可伪造。最后，实验结果和性能分析表明，与同类型协议相比，所提协议在安全性上具有明显优势，并且降低了通信开销与计算开销，满足基于隐私计算的多方数据安全计算模型的轻量级需求，未来可支撑在可信环境中隐私信息的按需脱敏。

关键词：数据出域安全；认证密钥协商；可信执行环境；中间人攻击；鲁棒性

中图分类号：TP309

文献标志码：A

DOI：10.11959/j.issn.1000–436x.2025015

Robust authentication key agreement protocol for cross-domain data security

ZHANG Jinghui[1,2,3], ZHANG Qijia[4], LIU Hai[4], TIAN Youliang[4,5], LI Fenghua[1,2,3]

1. Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100085, China
2. School of Cyber Security, University of Chinese Academy of Sciences, Beijing 100049, China
3. State Key Laboratory of Cyberspace Security Defense, Beijing 100085, China
4. College of Computer Science and Technology, Guizhou University, Guiyang 550025, China
5. College of Big Data and Information Engineering, Guizhou University, Guiyang 550025, China

Abstract: Towards the need for cross-domain data security, a corresponding system model and security model were presented, and a TEE-based robust authenticated key agreement protocol was proposed. This protocol achieved efficient interference-resistant key synthesis within the trusted execution environments of both sender and receiver. Theoretical proofs demonstrated that the communication messages in the proposed protocol maintain confidentiality and were unforgeability. Finally, experimental results and performance analysis indicate that compared to similar protocols, the proposed protocol offers significant advantages in terms of security, while reducing communication and computational overhead, meeting the lightweight requirements of multi-party data security computing model based on privacy computing. This paves the way for supporting on-demand data desensitization in trusted environments in the future.

Keywords: cross-domain data security, AKA, trusted execution environment, man-in-the-middle attack, robustness

---

收稿日期：2024–11–05；**修回日期：**2025–01–08

通信作者：田有亮，youliangtian@163.com

基金项目：国家重点研发计划基金资助项目（No.2021YFB3101300）；国家自然科学基金联合基金重点支持项目（No.U1836205）；国家自然科学基金资助项目（No.U23B2024, No.62272123）；贵阳市科技计划基金资助项目（No.[2022]2-4）；贵州省科技计划项目（No.[2022]065）

Foundation Items: The National Key Research and Development Program of China (No.2021YFB3101300), The Key Program of the National Natural Science Union Foundation of China (No.U1836205), The National Natural Science Foundation of China (No.U23B2024, No.62272123), The Science and Technology Program of Guiyang (No.[2022]2-4), The Science and Technology Program of Guizhou Province (No.[2022]065)

0 引言

随着互联网、大数据和人工智能等技术的快速发展和广泛应用，大模型凭借海量、多元化的数据，具备了适应多种场景和解决未见任务的能力。在此基础上，模型的应用不仅仅依赖于其通用能力，还需要与用户数据深度整合，进一步挖掘和释放数据的潜在价值。在传统数据保护中，公众和企业习惯将个人终端和企业系统视为用户私域，通过“重要数据不出域”来解决数据安全问题，然而，这种做法限制了数据在安全状态下的合法运用，形成了数据孤岛和数据壁垒，阻碍了数据价值的进一步释放。

文献[1]提出了数据出域的安全计算，并指出大模型、信用计算等场景需要原始数据出域，在数据使用方实现数据脱敏计算，从而获得高精度的计算结果，并对不可信的数据使用方保护数据提供方的数据安全和个人信息安全，指出数据从数据提供方到数据使用方的传输安全问题是数据出域安全计算中的关键问题。隐私信息在跨系统数据传输过程中极易受到恶意攻击，为了确保基于隐私计算的多方数据安全计算模型的通信安全，身份认证是各参与方进行安全通信的前提[1]。认证密钥协商（AKA, authenticated key agreement）协议能够实现通信实体之间身份的相互认证并生成会话密钥[2-3]，为通信双方提供安全的通信信道，确保通信过程中隐私信息的机密性、认证性、完整性和来源真实性。针对隐私信息接收者不可获知其他参与方提供的真实数据，不能对数据提供方的数据进行逆向还原并利用还原的数据对用户进行画像的应用需求，对数据进行的敏感操作必须由可信方执行。为通信实体采用可信执行环境（TEE, trusted execution environment）技术[4-5]，能够在传统系统运行环境之外提供一个隔离的安全系统用于加解密和脱敏操作。TEE技术通过将重要操作和数据从传统执行环境转移至独立的芯片与内存区域[6-7]，能够避免任何未经授权或位于TEE之外的代码对数据进行的读取或篡改操作。因此，搭载TEE的设备能够将私钥等重要参数存放在安全的存储区域，从而防止攻击者窃取用户密钥，造成密钥泄露等安全威胁。在用户设备执行密钥协商的过程中，TEE能够保障该参与方诚实执行协议，不会因恶意攻击而腐化，或被攻击者窃取隐私信息（如长期密钥、临时会话密钥）。

近年来，相关学者在不同领域将TEE技术引入AKA协议[8-11]，提升协议的安全性。Shepherd等[8]提出了双向信任协议（BTP, bi-directional trust protocol），基于TEE在远程传感设备之间建立安全可信的信道，实现隔离执行、安全I/O和敏感传感数据的通信。Lee等[9]针对车载信息娱乐系统相关的安全漏洞和安全问题，提出了一种基于椭圆曲线的会话密钥协商协议，由TEE提供安全端口，为敏感数据和操作提供安全存储，支持用户设备和远程信息处理控制单元之间的安全身份验证和密钥分发。Wu等[10]提出了基于软件防护扩展（SGX, software guard extension）的车联网雾辅助认证协议（SGXAP, SGX-based authentication protocol），通过将雾节点和路边单元（RSU, road side unit）的私有值存储于SGX中，抵御内部特权攻击，增强协议的安全性。随后，将SGX引入支持物联网的云计算环境，并提出了SAKAP[11]，在云服务器和控制服务器上使用SGX存储共享密钥，即使攻击者可以访问内存数据，也无法获取SGX中存储的共享密钥，从而确保数据隐私和实体之间的可持续通信。

然而，TEE仅能为设备内部提供安全保护机制，无法保障设备与外界通信过程中的安全性[12-13]，数据自TEE生成后，在从信道发送到其他设备的过程中，容易受到针对消息数据机密性与真实性的外部攻击，如中间人（MITM, man-in-the-middle）攻击[14]。在设备与外界其他设备建立会话前，中间人敌手能够干扰密钥协商过程，破坏通信的可靠性。因此，中间人攻击成了基于TEE的密钥协商协议面临的主要安全威胁。

当面对通信信道被掌控、交互信息被劫持的威胁时，多数算法[15-20]只能在协议执行的最后验证交互信息的真实性，以此实现抗中间人攻击。由于无法在协议的前期识别中间人攻击，若最后的验证失败则不得不浪费大量计算资源与通信代价。在协议执行的前期采用零知识证明是实现抗中间人攻击的有效方法。文献[21]在通信过程中引入了零知识证明确认对方发送信息的正确性，然而该方案依赖区块链完成密钥协商的通信过程，所需成本较高，不适用于大规模设备通信

环境。

在十万级以上的大规模设备通信环境中，网络情况复杂，中间人攻击所带来的物理信道干扰严重影响通信质量，给整个系统及各个设备带来巨大的损失。因此，需要密钥协商协议具备较强的鲁棒性，能够在复杂网络环境下实现高效的密钥协商。

针对以上需求，本文提出了一种面向数据出域安全的鲁棒认证密钥协商协议，采用了双重非交互式零知识证明保障信息的真实性与机密性，具体贡献如下。

1) 基于收发双方的可信执行环境，提出了一种面向数据出域安全的鲁棒认证密钥协商协议，实现了传输密钥的高效抗干扰合成，确保基于隐私计算的多方数据安全计算模型的通信安全。

2) 针对数据出域场景下的数据安全传输，定义了系统模型与形式化安全模型，并通过严格的理论安全分析，证明了本文协议在中间人攻击下的消息机密性与不可伪造性。使用协议形式化安全仿真工具 Scyther 的分析结果表明，本文协议在 Dolve-Yao 模型下满足抗中间人攻击。

3) 通过实验对比和性能分析结果表明，本文协议在面对攻击时具有更强的鲁棒性，在数据出域场景中的综合开销更低，满足基于隐私计算的多方数据安全计算模型的轻量级需求。

1　系统模型与安全模型

1.1　系统模型

本文协议的系统模型如图 1 所示，其中包含 3 个实体，分别为可信第三方 CA、密钥协商参与方 A 以及参与方 B。用户 A 与用户 B 的设备均嵌入 TEE，在协议执行过程中，方案的具体操作由外部程序调用 TEE 执行，因此考虑 CA、用户 A 与用户 B 均为诚实实体。CA 初始化系统参数，然后对用户 A 与用户 B 进行身份注册并颁发数字证书。用户私钥通过安全信道传输至设备的安全存储器内，仅由 TEE 授权调用。用户按照会话密钥生成算法进行密钥协商，实现会话密钥的生成。

本文方案采用实用性最广泛的英特尔的 SGX 技术[22]作为 TEE 架构，Enclave 是基于 SGX 的 TEE 实现的基本组件，是 TEE 内部功能的具体实现，用于执行具体的安全操作。应用程序通过调用 SGX 提供的 API 来初始化 Enclave，并定义其边界。Enclave 可以提供一个隔离的可信执行环境，也可以在 BIOS、虚拟机监控器、主操作系统和驱动程序均被恶意代码攻陷的情况下，仍对 Enclave 内的代码和内存数据提供保护，防止恶意软件影响 Enclave 内的代码和内存数据，从而保障用户的关键代码和数据的机密性和完整性。

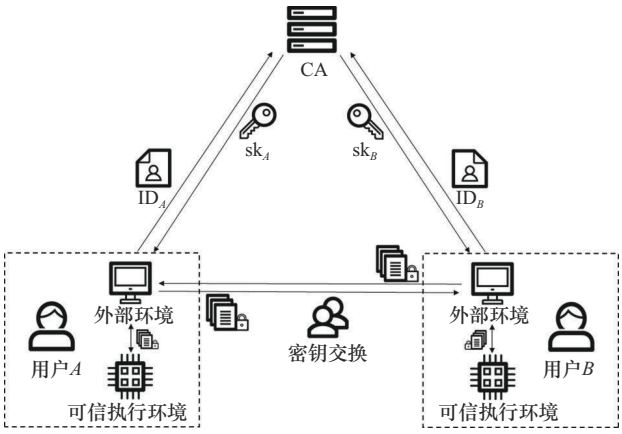

图 1　系统模型

1.2　安全假设

定义 1　离散对数（DL, discrete logarithm）困难假设。在群 G 中给定一个二元组 $(P,aP)\in G$，其中 $a\in Z_q^*$ 未知，对于任意的多项式时间算法 O 计算出 a 的优势 $\mathrm{Adv}_O^{\mathrm{DL}}(\lambda)$ 是可忽略的。

$$\mathrm{Adv}_O^{\mathrm{DL}}(\lambda)=\Pr[O(P,aP)\rightarrow a] \tag{1}$$

定义 2　计算性 CDH（computational Diffie-Hellman）困难假设。在群 G 中给定一个三元组 $(P,aP,bP)\in G^3$，其中 $a,b\in Z_q^*$ 未知，对于任意的多项式时间算法 O 计算出 abP 的优势 $\mathrm{Adv}_O^{\mathrm{CDH}}(\lambda)$ 是可忽略的。

$$\mathrm{Adv}_O^{\mathrm{CDH}}(\lambda)=\Pr[O(P,aP,bP)\rightarrow abP] \tag{2}$$

1.3　安全模型

由于 TEE 特性保证了用户设备在密钥协商过程中无法被攻击者腐化和劫持，属于强安全假设，因此本环境中不存在长期密钥泄露问题，不适用于针对密钥泄露攻击的 CK 安全模型[23]。本文方案环境中的安全威胁来源主要为通信信道，因此，本文方案的安全目标为抵抗中间人攻击，

具体来说，抵抗中间人攻击者在公开信道对通信消息进行窃听、篡改以及恶意伪造。针对抗中间人攻击的安全目标，本文提出了适用于TEE的形式化安全模型，即EUF-MITM-CMA安全以及IND-MITM-CPA安全。其中，EUF-MITM-CMA安全对应多项式时间的中间人敌手分别针对2个通信阶段发动的篡改和伪造攻击。IND-MITM-CPA安全对应多项式时间的中间人敌手对整个通信过程发动的窃听攻击。具体安全模型定义如下。

游戏1。本游戏通过挑战者C与敌手M的交互，形式化定义了中间人敌手针对通信阶段一（即用户A发送密钥生成请求）发动的篡改和伪造攻击。

初始化。C运行初始化算法，生成系统参数。

询问阶段。在该阶段，敌手M向C进行多项式有界次适应性询问，内容包含以下2项。

1) KeyGen询问。敌手M向C发送一个身份ID_i若该身份不是挑战身份，C随机选择$x_i \in Z_p$作为私钥并计算公钥，将密钥对(x_i,pub_i)返回给敌手。

2) M_{req}询问。敌手M向C发送2个身份ID_i与ID_j，C首先判断是否均为挑战身份。若不是，则生成$M_{\mathrm{req}}=(R_{Ax},R_{Ay},s_A)$并发送给$M$。

伪造。敌手M向C发送2个身份ID_i与ID_j，以及伪造的密钥生成请求消息$M_{\mathrm{req}}=(R_{Ax^*},R_{Ay^*},s_{A^*})$。$C$验证该消息是否为合法密钥生成请求，若通过验证，则敌手赢得该游戏。

游戏2。本游戏通过挑战者C与敌手M的交互，形式化定义了中间人敌手针对通信阶段二（即用户B返回密钥生成响应）的篡改和伪造攻击。

初始化。C运行初始化算法，生成系统参数。

询问阶段。在该阶段，敌手M向C进行多项式有界次适应性询问，内容包含以下2项。

1) KeyGen询问。敌手M向C发送一个身份ID_i，若该身份不是挑战身份，C随机选择$x_i \in Z_p$作为私钥并计算公钥，将密钥对$\left(x_i,\mathrm{pub}_i\right)$返回给敌手。

2) M_{rsq}询问。敌手M向C发送2个身份ID_i与ID_j，C首先判断是否均为挑战身份。若不是，则生成$M_{\mathrm{rsp}}=(T_x,T_y,s_B)$并发送给$M$。

伪造。敌手M向C发送2个身份ID_i与ID_j，以及伪造的密钥生成响应消息$M_{\mathrm{rsp}}=(T_{x^*},T_{y^*},s_{B^*})$。$C$验证该消息是否为合法密钥生成响应，若通过验证，则敌手赢得该游戏。

定义3 若不存在概率多项式时间敌手M能够以不可忽略优势赢得以上2个游戏，则本文方案满足EUF-MITM-CMA安全性。

游戏3。本游戏通过挑战者C与敌手M的交互，形式化定义了中间人敌手针对整个通信过程发动的窃听攻击。

初始化。C运行初始化算法，生成系统参数，并随机选择2个挑战身份ID_{i^*}与ID_{j^*}。

阶段1。在该阶段，敌手M向C进行多项式有界次适应性询问，内容包含以下3项。

1) KeyGen询问。敌手M向C发送一个身份ID_j，当$j=i^*$或$j=j^*$时，中止游戏。否则，C随机选择$x_j \in Z_p$作为私钥并计算公钥，然后将密钥对$\left(x_j,\mathrm{pub}_j\right)$返回给敌手。

2) M_{req}询问。M向C发送2个身份ID_i与ID_j，C首先判断是否$i=i^*$且$j=j^*$，若成立则游戏中止。否则，C生成$M_{\mathrm{req}}=(R_{Ax},R_{Ay},s_A)$并发送给$M$。

3) M_{rsq}询问。M向C发送2个身份ID_i与ID_j，C首先判断是否$i=i^*$且$j=j^*$，若成立则游戏中止。否则，C生成$M_{\mathrm{rsp}}=(T_x,T_y,s_B)$并发送给$M$。

挑战阶段。敌手M向C发送2个身份ID_i与ID_j与2个长度相等的消息(m_0,m_1)。C首先判断是否$i=i^*$且$j=j^*$，若$i\neq i^*$或$j\neq j^*$，则中止游戏。当$i=i^*$且$j=j^*$时，C使用挑战会话密钥加密m_b，其中$b\in\{0,1\}$由C随机选择，最后将M_{req}、M_{rsp}与密文一同返回给敌手M。

判断阶段。敌手M输出一个比特b'，若$b'=b$，则敌手赢得游戏。

定义4 若不存在概率多项式时间敌手M能够以不可忽略优势赢得游戏3，则本文方案满足IND-MITM-CPA安全性。

2 协议描述

基于TEE的认证密钥协商协议包含3个阶段：全局初始化阶段、注册阶段和会话密钥生成阶段，用于通信双方建立会话。表1列出了本文协议中相关符号的具体含义。

表1　　文中符号含义

符号	含义
F_q	有限域
G	SM2 曲线群中的一个生成元
q	SM2 曲线群的阶
klen	密钥长度
A,B	表示协议中不同域内的实体
CA	认证中心
ID_i	用户身份标识
sk_i	用户私钥
pub_i	用户公钥
Cert	用户数字证书
Time	时间戳
r	随机数
R_A	用户 A 发送的部分请求参数
R_{Ax}, R_{Ay}	R_A 横、纵坐标
H_{SM3}	SM3 哈希函数
s_A	用户 A 发送的部分请求参数
M_{req}	密钥生成请求消息,$M_{\mathrm{req}}=\{R_{Ax}, R_{Ay}, s_A\}$
key	会话密钥
T	用户 B 发送的部分响应参数
T_x, T_y	T 横、纵坐标
s_B	用户 B 发送的部分响应参数
M_{rsp}	密钥生成响应消息,$M_{\mathrm{rsp}}=\{T_x, T_y, s_B\}$

2.1　全局初始化阶段

在全局初始化阶段，CA 负责生成系统中所需的公开参数。首先，在有限域 F_q 上选取一条国密 SM2 算法推荐的椭圆曲线 $y^2 = x^3 + ax + b(\mathrm{mod}\,q)$，选定一个生成元 G 构成一个加法循环群，循环群的阶 q 为 256 位素数。然后，CA 选择国密 SM3 算法作为一个安全密码杂凑函数 H_{SM3}: $\{0,1\}^* \rightarrow \{0,1\}^{256}$，以及一个密钥派生函数（KDF, key derivation function），且 KDF: $\{0,1\}^* \rightarrow \{0,1\}^{\mathrm{klen}}$。

2.2　注册阶段

每个设备在发送密钥协商请求之前，需要在 CA 处进行注册。在注册阶段，CA 为通信双方 A、B 随机选取随机数 $\mathrm{sk}_A \in Z_q^*$、$\mathrm{sk}_B \in Z_q^*$ 作为用户私钥。然后，生成通信双方的公钥，$\mathrm{pub}_A = \mathrm{sk}_A \cdot G$，$\mathrm{pub}_B = \mathrm{sk}_B \cdot G$。最后，分别生成用户 A 和 B 的数字证书 Cert_A 和 Cert_B 并公开发布，完成用户注册。

2.3　会话密钥生成阶段

在这个阶段，用户 A、B 相互认证并生成会话密钥，如图 2 所示，具体步骤如下。

步骤 1　用户 A 的 Application 构建可信部分 Enclave，并调用 Ocall 函数。

步骤 2　用户 A 的 Enclave 生成密钥生成请求消息 M_{req}，并返回至 Application。步骤 2 共分为以下 4 个部分。

1) 用户 A 在 Enclave 中使用 SGX Enclave 的随机数发生器生成一个随机数 $r_A \in Z_q^*$。

2) 用户 A 在 Enclave 中计算 $R_A=(R_{Ax}, R_{Ay})$，若 R_A 为无穷远点，则返回执行 1)。

$$R_A = r_A \cdot G = (R_{Ax}, R_{Ay}) \tag{3}$$

3) 用户 A 首先输入用户 B 的身份标识，然后在 Enclave 中获取当前时间片段的时间戳 Time，并计算零知识证明参数 s_A。

$$s_A = \mathrm{sk}_A h_1 + r_A(\mathrm{mod}\,q) \tag{4}$$

其中，$h_1 = H_{\mathrm{SM3}}(R_{Ax} \| R_{Ay} \| \mathrm{ID}_A \| \mathrm{ID}_B \| \mathrm{Time})$。

4) 用户 A 的 Enclave 向 Application 返回密钥生成请求消息 $M_{\mathrm{req}}=\{R_{Ax}, R_{Ay}, s_A\}$。

步骤 3　用户 A 向用户 B 发送密钥生成请求消息 $M_{\mathrm{req}}=\{R_{Ax}, R_{Ay}, s_A\}$。

步骤 4　用户 B 接收来自用户 A 发送的密钥生成请求消息 M_{req}。

步骤 5　用户 B 从 CA 下载用户 A 的数字证书 Cert_A，并确认用户 A 的公钥 pub_A 的合法性。若验证失败，则证明请求发送方的身份非法，终止本次密钥协商；否则，继续执行步骤 6。

步骤 6　用户 B 的 Application 构建可信部分 Enclave，并调用 Ocall 函数。

步骤 7　用户 B 的 Enclave 对接收到的密钥生成请求消息 M_{req} 进行真实性验证。若验证通过，则接受协商请求，计算生成会话密钥 key 和密钥生成响应消息 M_{rsp}，并返回至用户 B 的 Application。步骤 7 共分为以下 7 个部分。

1) 用户 B 的 Enclave 接收密钥生成请求消息 M_{req}，得到 R_{Ax}, R_{Ay}, s_A。设置 $R'_A = (R_{Ax}, R_{Ay})$，并验证 R'_A 是否满足椭圆曲线方程，若不满足，则认为本次协商过程受到干扰，要求用户 A 重新发送密钥生成请求消息 M_{req}。

2) 用户 B 在 Enclave 中使用 SGX Enclave 的随

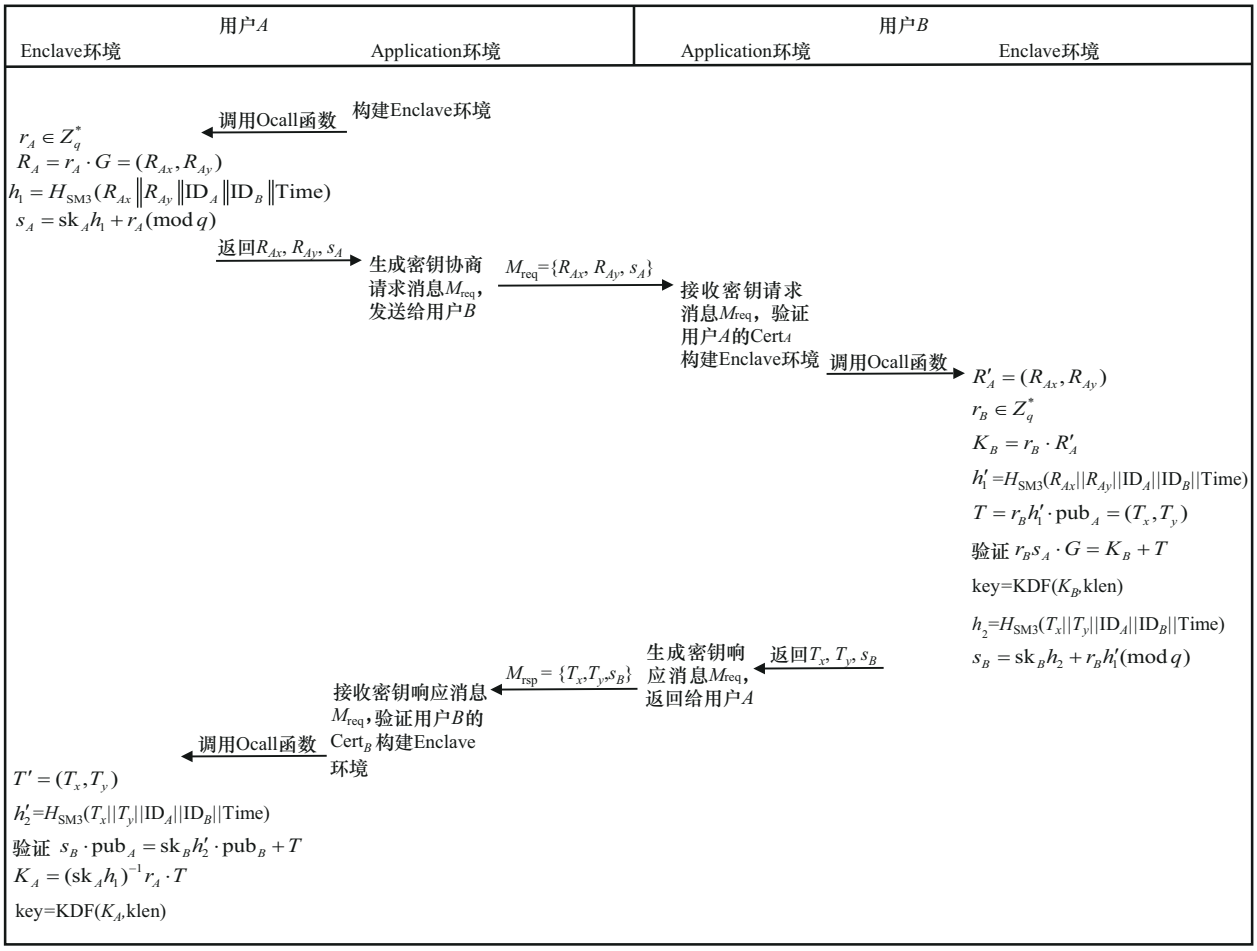

图2　基于TEE的抗中间人攻击鲁棒认证密钥协商协议

机数发生器生成一个随机数$r_B \in Z_q^*$。

3) 用户B在Enclave中计算生成临时值K_B。若K_B为椭圆曲线上的无穷远点，则返回执行2)。

$$K_B = r_B \cdot R'_A \tag{5}$$

4) 用户B在Enclave中获取当前时间片段的时间戳Time，然后计算部分响应参数T。

$$T = r_B h'_1 \cdot \mathrm{pub}_A = (T_x, T_y) \tag{6}$$

其中，$h'_1=H_{SM3}(R_{Ax}||R_{Ay}||ID_A||ID_B||Time)$。

5) 用户B在Enclave中对用户A发送的密钥协商请求进行验证。若式(7)不成立，则证明收到的协商请求非法，要求用户A重新生成并发送请求消息M_{req}；若通过验证，则接受协商请求，生成会话密钥key=KDF(K_B, klen)，并继续执行6)。

$$r_B s_A \cdot G = K_B + T \tag{7}$$

6) 用户B根据获取到的时间戳Time与4)中得到的h'_1，在Enclave中计算零知识证明参数s_B。

$$s_B = \mathrm{sk}_B h_2 + r_B h'_1 (\mathrm{mod}\, q) \tag{8}$$

其中，$h_2=H_{SM3}(T_x||T_y||ID_A||ID_B||Time)$。

7) 用户B的Enclave向Application返回密钥生成响应消息$M_{rsp}=\{T_x,T_y,s_B\}$。

步骤8　用户B向用户A发送密钥生成响应消息$M_{rsp}=\{T_x,T_y,s_B\}$。

步骤9。用户A接收来自用户B的密钥生成响应消息M_{rsp}。

步骤10　用户A从CA下载用户B的数字证书Cert$_B$，确认用户B的公钥pub$_B$的合法性。若验证失败，则证明响应返回方的身份非法，终止本次密钥协商；否则，继续执行步骤11。

步骤11　用户A的Application调用Ocall函数。

步骤12　用户A的Enclave对接收到的密钥生成响应消息M_{rsp}进行真实性验证。若验证通过，则利用M_{rsp}计算生成会话密钥key，完成密钥协商。步骤12共分为以下3个部分。

1) 用户A的Enclave接收来自用户B的密钥生成响应消息M_{rsp}，得到T_x，T_y，s_B。设置$T'=(T_x,T_y)$，

并验证T'是否满足椭圆曲线方程，若不满足，则认为用户B返回的响应消息受到篡改，要求用户B重新发送响应消息M_{rsp}。

2) 用户A在Enclave中对用户B返回的密钥协商响应进行验证，若式(9)不成立，则证明协商响应消息非法，要求用户B重新生成并发送响应消息M_{rsp}；若通过验证，则继续执行3)。

$$s_B \cdot \text{pub}_A = \text{sk}_B h_2' \cdot \text{pub}_B + T \tag{9}$$

其中，$h_2'=H_{\text{SM3}}(T_x||T_y||\text{ID}_A||\text{ID}_B||\text{Time})$。

3) 用户A在Enclave中计算生成会话密钥key，完成本次密钥协商。

$$K_A = (\text{sk}_A h_1)^{-1} r_A \cdot T \tag{10}$$

$$\text{key}=\text{KDF}(K_A, \text{klen}) \tag{11}$$

3　安全性分析

3.1　理论安全性证明

定理1　在离散对数困难假设下，本文方案中的通信消息具有EUF-MITM-CMA安全性，即中间人攻击者无法在多项式时间内成功伪造或篡改一个合法消息。

引理1　在本文方案中，用户B收到的密钥生成请求消息是真实的。若存在一个中间人攻击敌手M能够在多项式时间内以不可忽略的优势ε攻破本文方案中用户B收到的消息的EUF-MITM-CMA安全性，则能够构造一个挑战者C，利用敌手M的能力以不可忽略的优势$\text{Adv}_C^{\text{DL}}(\lambda)$求解离散对数问题。

$$\text{Adv}_C^{\text{DL}}(\lambda) \geqslant \left(1-\frac{1}{q_n}\right)^{q_{kg}}\left(1-\frac{2}{q_n}\right)^{q_m}\frac{2}{q_n}\varepsilon \tag{12}$$

证明　给定C一个DL问题的实例$(G,a \cdot G)$，其中$a \in Z_q$未知，C通过与敌手M进行下面的EUF-MITM-CMA游戏，最后输出DL问题的解a。

初始化。C运行初始化算法，随机选择2个身份ID_{i^*}与ID_{j^*}。ID_{i^*}作为挑战身份隐式地将其私钥设置为a，并令$a \cdot G$为其公钥；ID_{j^*}作为用户B的身份。

哈希询问。敌手M在该阶段对随机预言机进行至多q_{H_1}次的询问，C维护一个初始为空的列表L_1，用来记录M的每次询问。

H_1询问。敌手M向C发送一个四元组$(Rx_i,Rx_j,\text{ID}_i,\text{ID}_j)$，其中$i$表示$M$向$H_1$预言机进行的第$i$次询问。$C$首先检查$L_1$中是否存在$(Rx_i,Rx_j,\text{ID}_i,\text{ID}_j,\theta_i)$的记录，若存在，则按照$L_1$中对应的内容答复敌手；否则，$C$随机选择一个$\theta_i \in Z_p$，设置$H_1(Rx_i,Rx_j,\text{ID}_i,\text{ID}_j)=\theta_i$。然后将$\theta_i$作为随机预言机$H_1$的答复返回给敌手，并将五元组$(Rx_i,Rx_j,\text{ID}_i,\text{ID}_j,\theta_i)$作为新元素添加到列表$L_1$中。

阶段1。在该阶段，敌手M向C进行多项式有界次适应性询问，内容包含以下2项。

1) KeyGen询问。敌手M向C发送一个身份ID_i，当$i=i^*$时，游戏中止；否则，C随机选择$x_i \in Z_p$作为私钥，计算公钥

$$\text{pub}_i = x_i \cdot G \tag{13}$$

并将密钥对(x_i,pub_i)返回给敌手。

2) M_{req}询问。M向C发送2个身份ID_i与ID_j，C首先判断$i=i^*$且$j=j^*$是否成立，若成立，则游戏中止；否则，C考虑以下2种情况。

① 当$i \neq i^*$时，C首先随机选择一个$r_i \in Z_q$，并计算$R_i = r_i \cdot G$。然后执行H_1询问，得到关于$(Rx_i,Rx_j,\text{ID}_i,\text{ID}_j)$的哈希值$\theta_i$，计算密钥生成请求消息如式(14)所示。

$$\begin{aligned} R_{Ax} &= Rx_i \\ R_{Ay} &= Ry_i \\ s_A &= x_i\theta_i + r_i \bmod q \end{aligned} \tag{14}$$

然后将$M_{\text{req}}=(R_{Ax},R_{Ay},s_A)$发送给$M$。容易验证$C$模拟的密钥生成请求消息是一个$\text{ID}_i$向$\text{ID}_j$发送的合法消息。

② 当$i=i^*$且$j \neq j^*$时，C首先选择2个随机数$\rho,\theta_{i*} \in Z_q$，隐式设置$r_{i*}=\rho - a\theta_{i*}$并令$R_{i*}=\rho \cdot G - \theta_{i*} a \cdot G$，其中$a \cdot G$为DL问题的实例。令关于$(Rx_{i*},Ry_{i*},\text{ID}_{i*},\text{ID}_j)$的哈希值为$\theta_{i*}$，计算密钥生成请求消息如式(15)所示。

$$\begin{aligned} R_{Ax} &= Rx_{i*} \\ R_{Ay} &= Ry_{i*} \\ s_A &= \rho \end{aligned} \tag{15}$$

该模拟密钥生成请求消息在敌手M的视角中与真实密钥生成请求消息不可区分，因为有

$$\begin{aligned} &s_A = aH_1(Rx_{i*},Ry_{i*},\text{ID}_{i*},\text{ID}_j) + r_{i*} = \\ &a\theta_{i*} + r_{i*} = a\theta_{i*} + \rho - a\theta_{i*} = \rho \end{aligned} \tag{16}$$

且该消息能够通过验证，验证如下。

生成临时值$K_B = r_B \cdot R_A$，然后计算$T = r_j H_1(R_{x_{i*}},R_{y_{i*}},\text{ID}_{i*},\text{ID}_j) \cdot \text{pub}_{i*}$，容易验证式(17)成立。

$$s_A r_B \cdot G = \rho r_B \cdot G = (\rho + a\theta_{i^*} - a\theta_{i^*}) r_B \cdot G = (\rho - a\theta_{i^*}) r_B \cdot G + a\theta_{i^*} r_B \cdot G = r_B r_{i^*} \cdot G + \theta_{i^*} r_B \cdot (a \cdot G) = r_B \cdot R_A + H_1(R_{Ax}, R_{Ay}, \mathrm{ID}_{i^*}, \mathrm{ID}_j) r_B \cdot \mathrm{pub}_{i^*} = \mathrm{key} + T \tag{17}$$

伪造。敌手M向C发送2个身份ID_i与ID_j，以及伪造的密钥生成请求消息$M_{\mathrm{req}} = (R_{Ax*}, R_{Ay*}, s_{A*})$。$C$首先判断$i = i^*$且$j = j^*$是否成立，若$i \neq i^*$或$j \neq j^*$，则游戏中止；当$i = i^*$且$j = j^*$时，$C$检查列表$L_1$，获取$(R_{Ax*}, R_{Ay*}, \mathrm{ID}_{i*}, \mathrm{ID}_{j*})$对应的哈希值$\theta'$。根据分叉引理，$C$向预言机输入相同的内容$(R_{Ax*}, R_{Ay*}, \mathrm{ID}_{i*}, \mathrm{ID}_{j*})$，在多项式时间内有概率得到不同的输出结果$\theta''(\theta'' \neq \theta')$，因此存在如式(18)的所示2个等式。

$$\begin{aligned} s_{A*} &= a\theta' + r^* \\ s'_{A*} &= a\theta'' + r^* \end{aligned} \tag{18}$$

然后使用θ'与θ''计算DL问题实例的结果如式(19)所示。

$$\frac{s_{A*} - s'_{A*}}{\theta' - \theta''} = \frac{a\theta' - r^* - a\theta'' + r^*}{\theta' - \theta''} = \frac{a\theta' - a\theta''}{\theta' - \theta''} = a \tag{19}$$

若C在以上模拟游戏中不退出，则需要同时满足以下3个条件。

1) 敌手M没有在KeyGen询问阶段向C发送过身份ID_{i^*}。

2) 敌手M没有在M_{req}询问阶段向C同时发送过身份ID_{i^*}与ID_{j^*}。

3) 敌手M在伪造阶段必须发送的是关于身份ID_{i^*}与ID_{j^*}的密钥生成请求消息。

则C在以上条件下利用敌手M伪造的密钥生成请求消息成功解决DL问题的概率为

$$\mathrm{Adv}_C^{\mathrm{DL}}(\lambda) \geqslant \Pr[\mathrm{Event}_1] \Pr[\mathrm{Event}_2] \cdot \Pr[\mathrm{Event}_3] \varepsilon \geqslant \left(1 - \frac{1}{q_n}\right)^{q_{kg}} \left(1 - \frac{2}{q_n}\right)^{q_m} \frac{2}{q_n} \varepsilon \tag{20}$$

由于现实中不存在算法能够在多项式时间内以不可忽略的优势破解离散对数困难问题，因此不存在敌手M能够以不可忽略的优势伪造或篡改用户B收到的密钥生成请求消息。证毕。

引理2 在本文方案中，用户A收到的密钥生成响应消息是真实的。若存在一个中间人攻击敌手M能够在多项式时间内以不可忽略的优势ε攻破本文方案中用户A收到的消息的EUF-MITM-CMA安全性，则能够构造一个挑战者C，利用敌手M的能力以不可忽略的优势$\mathrm{Adv}_C^{\mathrm{DL}}(\lambda)$求解离散对数问题。

$$\mathrm{Adv}_C^{\mathrm{DL}}(\lambda) \geqslant \left(1 - \frac{1}{q_n}\right)^{q_{kg}} \left(1 - \frac{2}{q_n}\right)^{q_m} \frac{2}{q_n} \varepsilon \tag{21}$$

证明 给定C一个DL问题的实例$(G, a \cdot G)$，其中$a \in Z_q$未知，C通过与敌手M进行下面的EUF-MITM-CMA游戏，最后输出DL问题的解a。

初始化。C运行初始化算法，随机选择2个身份ID_{i^*}与ID_{j^*}。ID_{j^*}作为挑战身份，隐式地将其私钥设置为a，并令$a \cdot G$为其公钥；ID_{i^*}作为用户A的身份。

哈希询问。敌手M在该阶段对2个随机预言机分别进行至多q_{H_1}次与q_{H_2}次的询问，C维护2个初始为空的列表L_1, L_2，用来记录M的每次询问。

H_1询问。敌手M向C发送一个四元组$(Rx_i, Ry_i, \mathrm{ID}_i, \mathrm{ID}_j)$，其中$i$表示$M$向$H_1$预言机进行的第$i$次询问。$C$首先检查$L_1$中是否存在$(Rx_i, Ry_i, \mathrm{ID}_i, \mathrm{ID}_j, \theta_i)$的记录，若存在，则按照$L_1$中对应的内容答复敌手；否则，$C$随机选择一个$\theta_i \in Z_p$，设置$H_1(Rx_i, Ry_i, \mathrm{ID}_i, \mathrm{ID}_j) = \theta_i$。然后将$\theta_i$作为随机预言机$H_1$的答复返回给敌手，并将五元组$(Rx_i, Ry_i, \mathrm{ID}_i, \mathrm{ID}_j, \theta_i)$作为新元素添加到列表$L_1$中。

H_2询问。敌手M向C发送一个四元组$(Tx_i, Ty_i, \mathrm{ID}_j, \mathrm{ID}_i)$，其中$i$表示$M$向$H_2$预言机进行的第$i$次询问。$C$首先检查$L_2$中是否存在$(Tx_i, Ty_i, \mathrm{ID}_j, \mathrm{ID}_i, \tau_i)$的记录，若存在，则按照$L_2$中对应的内容答复敌手；否则，$C$随机选择一个$\tau_i \in Z_p$，设置$H_2(Tx_i, Ty_i, \mathrm{ID}_j, \mathrm{ID}_i) = \tau_i$。然后将$\tau_i$作为随机预言机$H_2$的答复返回给敌手，并将五元组$(Tx_i, Ty_i, \mathrm{ID}_j, \mathrm{ID}_i, \tau_i)$作为新元素添加到列表$L_2$中。

阶段1。在该阶段，敌手M向C进行多项式有界次适应性询问，内容包含以下2项。

1) KeyGen询问。敌手M向C发送一个身份ID_j，当$j = j^*$时，游戏中止；否则，C随机选择$x_j \in Z_p$作为私钥，计算公钥

$$\mathrm{pub}_j = x_j \cdot G \tag{22}$$

并将密钥对$\left(x_j, \mathrm{pub}_j\right)$返回给敌手。

2) M_{rsp}询问。M向C发送2个身份ID_i与ID_j，C首先判断$i = i^*$且$j = j^*$是否成立，若成立，则游戏中止；否则，C考虑以下2种情况。

① 当$j \neq j^*$时，C首先随机选取一个点R_{Aj}，然

后执行 H_1 询问得到关于 $(R_{Ax_j},R_{Ay_j},\mathrm{ID}_i,\mathrm{ID}_j)$ 的哈希值 θ_j，然后随机选取整数 $r_j \in Z_q$，计算 $T_j = \theta_j r_j \cdot \mathrm{pub}_A$，接着执行 H_2 询问得到哈希值 τ_j，并计算密钥生成响应消息如式(23)所示。

$$\begin{aligned} T_x &= Tx_j \\ T_y &= Ty_j \\ s_B &= x_j\tau_j + r_j\theta_j \bmod q \end{aligned} \tag{23}$$

然后将 $M_{\mathrm{rsp}} = (T_x,T_y,s_B)$ 发送给 M。容易验证 C 模拟的密钥生成请求消息是一个 ID_j 向 ID_i 发送的合法消息。

② 当 $i \neq i^*$ 且 $j = j^*$ 时，C 首先选择 2 个随机数 $\rho,\tau_{j^*} \in Z_q$，然后随机选取一个点 $R_{Aj} = r_a \cdot G(r_a \in Z_q)$，并执行 H_1 询问得到关于 $(R_{Ax_j},R_{Ay_j},\mathrm{ID}_i,\mathrm{ID}_{j^*})$ 的哈希值 θ_{j^*}，再隐式设置 $r_{j^*} = \dfrac{\rho - a\tau_{j^*}}{\theta_{j^*}}$，计算

$$K_{Bj^*} = r_{j^*} \cdot R_{Aj} = \frac{\rho}{\theta_{j^*}} \cdot R_{Aj} - \frac{\tau_{j^*}}{\theta_{j^*}}(a \cdot G) \tag{24}$$

$$T_j = \theta_j r_j \cdot \mathrm{pub}_A = \rho \cdot \mathrm{pub}_A - \tau_{j^*}(a \cdot G) \tag{25}$$

其中，$(a \cdot G)$ 为 DL 问题的实例。令 $\tau_{j^*} = H_2(Tx_{j^*},Ty_{j^*},\mathrm{ID}_i,\mathrm{ID}_{j^*})$，计算密钥生成响应消息如式(26)所示。

$$\begin{aligned} T_x &= T_{xj^*} \\ T_y &= T_{yj^*} \\ s_B &= \rho \end{aligned} \tag{26}$$

该模拟密钥生成响应消息在敌手 M 的视角中与真实密钥生成响应消息不可区分，因为有

$$\begin{aligned} & s_B = aH_2(Tx_{j^*},Ty_{j^*},\mathrm{ID}_i,\mathrm{ID}_{j^*}) + \\ & r_{j^*}H_1(Rx_i,Ry_i,\mathrm{ID}_i,\mathrm{ID}_{j^*}) = \\ & a\tau_{j^*} + r_{j^*}\theta_{j^*} = a\tau_{j^*} + \\ & \frac{\rho - a\tau_{j^*}}{\theta_{j^*}}\theta_{j^*} = a\tau_{j^*} + \rho - a\tau_{j^*} = \rho \end{aligned} \tag{27}$$

且该消息能够通过式(28)所示的验证。

$$\begin{aligned} & s_B \cdot \mathrm{pub}_A = \rho \cdot \mathrm{pub}_A = \\ & (\rho + a\tau_{j^*} - a\tau_{j^*}) \cdot \mathrm{pub}_A = \\ & a\tau_{j^*} \cdot \mathrm{pub}_A + \left(\frac{\rho - a\tau_{j^*}}{\theta_{j^*}}\right)\theta_{j^*} \cdot \mathrm{pub}_A = \\ & H_1(R_{Ax},R_{Ay},\mathrm{ID}_A,\mathrm{ID}_j)r_{j^*} \cdot \mathrm{pub}_A + \\ & x_A\tau_{j^*}(a \cdot G) = \\ & x_A H_2(Tx_{j^*},Ty_{j^*},\mathrm{ID}_A,\mathrm{ID}_{j^*})(a \cdot G) + T \end{aligned} \tag{28}$$

伪造。敌手 M 向 C 发送 2 个身份 ID_i 与 ID_j，以及伪造的密钥生成响应消息 $M_{\mathrm{rsp}} = (T_{x*},T_{y*},s_{B*})$。$C$ 首先判断 $i = i^*$ 且 $j = j^*$ 是否成立，若 $i \neq i^*$ 或 $j \neq j^*$，则游戏中止；当 $i = i^*$ 且 $j = j^*$ 时，C 检查列表 L_1，获取 $(R_{Ax*},R_{Ay*},\mathrm{ID}_{i*},\mathrm{ID}_{j*})$ 对应的哈希值 θ'。再由 x_A,r_A 计算会话密钥 key。检查列表 L_2，获取 $H_2(Tx_{j^*},Ty_{j^*},\mathrm{ID}_{i^*},\mathrm{ID}_{j^*})$ 对应的哈希值 τ'，根据分叉引理，C 向预言机输入相同的内容 $(Tx_{j^*},Ty_{j^*},\mathrm{ID}_{i^*},\mathrm{ID}_{j^*})$，在多项式时间内有概率得到不同的输出结果 $\tau''(\tau'' \neq \tau')$，因此存在如式(29)所示的 2 个等式。

$$\begin{aligned} s_{B*} &= a\tau' + r^*\theta' \\ s'_{B*} &= a\tau'' + r^*\theta' \end{aligned} \tag{29}$$

然后计算 DL 问题实例的结果，如式(30)所示。

$$\begin{aligned} a &= \frac{s_{B*} - s'_{B*}}{\tau' - \tau''} = \\ & \frac{a\tau' + r^*\theta' - a\tau'' - r^*\theta'}{\tau' - \tau''} = \\ & \frac{a\tau' - a\tau''}{\tau' - \tau''} = a \end{aligned} \tag{30}$$

若 C 在以上模拟游戏中不退出，则需要同时满足以下 3 个条件。

1) 敌手 M 没有在 KeyGen 询问阶段向 C 发送过身份 ID_{i^*}。

2) 敌手 M 没有在 M_{rsp} 询问阶段向 C 同时发送过身份 ID_{i^*} 与 ID_{j^*}。

3) 敌手 M 在伪造阶段必须发送的是关于身份 ID_{i^*} 与 ID_{j^*} 的密钥生成响应消息。

则挑战者 C 在以上条件下利用敌手 M 伪造的密钥生成请求消息成功解决 DL 问题的概率为

$$\begin{aligned} & \mathrm{Adv}_C^{\mathrm{DL}}(\lambda) \geqslant \Pr[\mathrm{Event}_1]\Pr[\mathrm{Event}_2] \cdot \\ & \Pr[\mathrm{Event}_3]\varepsilon \geqslant \\ & \left(1 - \frac{1}{q_n}\right)^{q_{kg}}\left(1 - \frac{2}{q_n}\right)^{q_m}\frac{2}{q_n}\varepsilon \end{aligned} \tag{31}$$

由于现实中不存在算法能够在多项式时间内以不可忽略的优势破解离散对数困难问题，因此不存在敌手 M 能够以不可忽略的优势伪造或篡改用户 A 收到的密钥生成响应消息。证毕。

定理 2　在 CDH 困难假设下，本文方案中的通信消息具有机密性，即中间人攻击者无法在多项式时间内得到关于会话密钥的信息。若存在一个中间人攻击敌手 M 能够在多项式时间内以不可忽略的优

势ε攻破本文方案中消息的IND-MITM-CPA安全性，则能够构造一个攻击者C，利用敌手M的能力以不可忽略的优势$\mathrm{Adv}_C^{\mathrm{CDH}}(\lambda)$求解CDH困难问题。

$$\mathrm{Adv}_C^{\mathrm{CDH}}(\lambda) \geqslant \frac{1+2\varepsilon}{q_{H_2}q_n}\left(1-\frac{2}{q_n}\right)^{q_{kg}+q_{M_{\mathrm{rsp}}}+q_{M_{\mathrm{req}}}} \tag{32}$$

证明 给定C一个CDH问题的实例$(G,a\cdot G,b\cdot G)$，其中$a,b\in Z_q$未知，C通过与敌手M进行下面的IND-MITM-CPA游戏，最后输出CDH问题的解$ab\cdot G$。

初始化。C运行初始化算法，随机选择2个挑战身份ID_{i^*}与ID_{j^*}，随机选择4个整数$\rho,\rho',\theta^*,\tau^*\in Z_q$，分别隐式地将其私钥设置为$\mathrm{sk}_A=-\dfrac{a+\rho}{\theta^*}$和$\mathrm{sk}_B=-\dfrac{b\theta^*+\rho'}{\tau^*}$，设置用户$A$的公钥$\mathrm{pub}_A=-\dfrac{1}{\theta^*}(a\cdot G)-\dfrac{\rho}{\theta^*}\cdot G$与用户$B$的公钥$\mathrm{pub}_B=-\dfrac{\theta^*}{\tau^*}(b\cdot G)-\dfrac{\rho'}{\tau^*}\cdot G$，其中，$a\cdot G$和$b\cdot G$均为CDH问题实例中的元素。

哈希询问。敌手M在该阶段对2个随机预言机分别进行至多q_{H_1}次与q_{H_2}次的询问，C维护2个初始为空的列表L_1,L_2，用来记录M的每次询问。

H_1询问。敌手M向C发送一个四元组$(Rx_i,Ry_i,\mathrm{ID}_i,\mathrm{ID}_j)$，其中$i$表示$M$向$H_1$预言机进行的第$i$次询问。$C$首先检查$L_1$中是否存在$(Rx_i,Ry_i,\mathrm{ID}_i,\mathrm{ID}_j,\theta_i)$的记录，若存在，则按照$L_1$中对应的内容答复敌手；否则，$C$随机选择一个$\theta_i\in Z_p$，设置$H_1(Rx_i,Ry_i,\mathrm{ID}_i,\mathrm{ID}_j)=\theta_i$。然后将$\theta_i$作为随机预言机$H_1$的答复返回给敌手，并将五元组$(Rx_i,Ry_i,\mathrm{ID}_i,\mathrm{ID}_j,\theta_i)$作为新元素添加到列表$L_1$中。

H_2询问。敌手M向C发送一个四元组$(Tx_i,Ty_i,\mathrm{ID}_j,\mathrm{ID}_i)$，其中$i$表示$M$向$H_2$预言机进行的第$i$次询问。$C$首先检查$L_2$中是否存在$(Tx_i,Ty_i,\mathrm{ID}_j,\mathrm{ID}_i,\tau_i)$的记录，若存在，则按照$L_2$中对应的内容答复敌手；否则，$C$随机选择一个$\tau_i\in Z_p$，设置$H_2(Tx_i,Ty_i,\mathrm{ID}_j,\mathrm{ID}_i)=\tau_i$。然后将$\tau_i$作为随机预言机$H_2$的答复返回给敌手，并将五元组$(Tx_i,Ty_i,\mathrm{ID}_j,\mathrm{ID}_i,\tau_i)$作为新元素添加到列表$L_2$中。

阶段1。敌手M向C进行多项式有界次适应性询问，内容包含以下3项。

1) KeyGen询问。敌手M向C发送一个身份ID_j，当$j=i^*$或$j=j^*$时，游戏中止；否则，C随机选择$x_j\in Z_p$作为私钥，计算公钥

$$\mathrm{pub}_j=x_j\cdot G \tag{33}$$

并将密钥对$\left(x_j,\mathrm{pub}_j\right)$返回给敌手。

2) M_{req}询问。M向C发送2个身份ID_i与ID_j，C首先判断$i=i^*$且$j=j^*$是否成立，若成立，则游戏中止；否则，C考虑以下2种情况。

① 当$i\neq i^*$时，C首先随机选择一个$r_i\in Z_q$，并计算$R_i=r_i\cdot G$。然后执行H_1询问，得到关于$(Rx_i,Ry_i,\mathrm{ID}_i,\mathrm{ID}_j)$的哈希值$\theta_j$，计算密钥生成请求消息如式(34)所示。

$$\begin{aligned}&R_{Ax}=Rx_i\\&R_{Ay}=Ry_i\\&s_A=x_i\theta_j+r_i \bmod q\end{aligned} \tag{34}$$

最后将$M_{\mathrm{req}}=(R_{Ax},R_{Ay},s_A)$发送给敌手$M$。容易验证$C$模拟的密钥生成请求消息是一个$\mathrm{ID}_i$向$\mathrm{ID}_j$发送的合法消息。

② 当$i=i^*$且$j\neq j^*$时，C首先选择随机数$k\in Z_q$，隐式设置$r_i=ka$并令$R_i=ka\cdot G$。然后令$(Rx_i,Ry_i,\mathrm{ID}_i,\mathrm{ID}_j)$的哈希值为$\theta_i=k\theta^*$，计算密钥生成请求消息如式(35)所示。

$$\begin{aligned}&R_{Ax}=Rx_{i^*}\\&R_{Ay}=Ry_{i^*}\\&s_A=-k\rho\end{aligned} \tag{35}$$

该模拟密钥生成请求消息在敌手M的视角中与真实密钥生成请求消息不可区分，因为有

$$\begin{aligned}s_A&=\mathrm{sk}_A H_1(Rx_i,Ry_i,\mathrm{ID}_i,\mathrm{ID}_j)+r_i=\\&-\frac{a+\rho}{\theta^*}H_1(Rx_i,Ry_i,\mathrm{ID}_i,\mathrm{ID}_j)+ka=\\&-\frac{a+\rho}{\theta^*}k\theta^*+ka=-k\rho\end{aligned} \tag{36}$$

3) M_{rsp}询问。M向C发送2个身份ID_i与ID_j，C首先判断$i=i^*$且$j=j^*$是否成立，若成立，则游戏中止；否则，C考虑以下2种情况。

① 当$j\neq j^*$时，C首先随机选取一个点R_{Aj}，执行H_1询问得到关于$(R_{Ax_j},R_{Ay_j},\mathrm{ID}_i,\mathrm{ID}_j)$的哈希值$\theta_j$。然后随机选取整数$r_j\in Z_q$，计算$\mathrm{key}_j=r_j\cdot R_{Aj}$以及$T_j=\theta_j r_j\cdot\mathrm{pub}_i$，执行$H_2$询问得到哈希值$\tau_j$，并计算密钥生成响应消息如式(37)所示。

$$\begin{aligned}&T_x=Tx_j\\&T_y=Ty_j\\&s_B=x_j\tau_j+r_j\theta_j \bmod q\end{aligned} \tag{37}$$

最后将$M_{\mathrm{rsp}}=(T_x,T_y,s_B)$发送给敌手$M$。容易验

证C模拟的密钥生成请求消息是一个ID_j向ID_i发送的合法消息。

② 当$i \neq i^*$且$j = j^*$时，C首先选择2个随机数$k,\tau_{j^*} \in Z_q$，然后随机选取一个点$R_{Aj} = r_a \cdot G(r_a \in Z_q)$，并执行$H_1$询问得到关于$(R_{Ax_j},R_{Ay_j},\mathrm{ID}_i,\mathrm{ID}_{j^*})$的哈希值$\theta_{j^*}$，再隐式设置$r_{j^*} = \dfrac{kb\theta^*}{\theta_{j^*}}$，计算

$$\mathrm{key}_{j^*} = r_{j^*} \cdot R_{Aj} = \frac{kb\theta^*}{\theta_{j^*}} \cdot R_{Aj} = \frac{kr_a\theta^*}{\theta_{j^*}}(b \cdot G)$$

$$T_j = \theta_{j^*} r_{j^*} \cdot \mathrm{pub}_i = \theta^* x_i k(b \cdot G) \tag{38}$$

令$H_2(Tx_{i^*},Ty_{i^*},\mathrm{ID}_i,\mathrm{ID}_{j^*}) = k\tau^*$，计算密钥生成响应消息如式(39)所示。

$$\begin{aligned} T_x &= T_{xj^*} \\ T_y &= T_{xj^*} \\ s_B &= -k\rho' \end{aligned} \tag{39}$$

该模拟密钥生成请求消息在敌手M的视角中与真实密钥生成响应消息不可区分，因为有

$$\begin{aligned} & s_B = \mathrm{sk}_B H_2(Tx_{i^*},Ty_{i^*},\mathrm{ID}_i,\mathrm{ID}_{j^*}) + \\ & r_{j^*} H_1(Rx_i,Ry_i,\mathrm{ID}_i,\mathrm{ID}_{j^*}) = \\ & \mathrm{sk}_B k\tau^* + r_{j^*}\theta_{j^*} = \\ & -\frac{b\theta^* + \rho'}{\tau^*}k\tau^* + \frac{kb\theta^*}{\theta_{j^*}}\theta_{j^*} = \\ & -b\theta^* k - \rho' k + \frac{kb\theta^*}{\theta_{j^*}}\theta_{j^*} = -k\rho' \end{aligned} \tag{40}$$

挑战阶段。敌手M向C发送2个身份ID_i与ID_j和2个长度相等的消息(m_0,m_1)。C首先判断$i = i^*$且$j = j^*$是否成立，若$i \neq i^*$或$j \neq j^*$，则游戏中止；若$i = i^*$且$j = j^*$，设置$r_A = a$，$r_B = b$，$H_1(R_{Ax},R_{Ay},\mathrm{ID}_A,\mathrm{ID}_{j^*}) = \theta^*$，$H_1(Tx,Ty,\mathrm{ID}_{i^*},\mathrm{ID}_{j^*}) = \tau^*$，计算$M_{\mathrm{req}}$

$$\begin{aligned} R_A &= a \cdot G \\ R_{Ax} &= Rx_i \\ R_{Ay} &= Ry_i \\ s_A &= -\rho \end{aligned} \tag{41}$$

随机选择点T，计算M_{rsp}

$$\begin{aligned} T_x &= Tx_j \\ T_y &= Ty_j \\ s_B &= -\rho' \end{aligned} \tag{42}$$

随机选择一点key，使用对称加密算法加密m_b，其中$b \in \{0,1\}$由C随机选择，最后将M_{req}、M_{rsp}与密文一同返回给敌手M。

判断阶段。敌手M输出一个比特b'，若$b' = b$，则敌手赢得游戏。C则在列表L_2中寻找一个五元组$(Tx_i,Ty_i,\mathrm{ID}_j,\mathrm{ID}_i,\tau_i)$，并计算$K_B = -\rho(b \cdot G) - T$，然后将$K_B$作为CDH问题的解，输出$K_B$。

当敌手M能够以不可忽略的优势赢得该游戏时，敌手M一定能够根据M_{req}和M_{rsp}计算出正确的$K_B = r_A r_B \cdot G = ab \cdot G$，并发动$H_2$询问获取哈希值$\tau_i$。此时的$K_B$为CDH困难的问题的正确解。

若C在以上模拟游戏中不退出，则需要同时满足以下4个条件。

1) 敌手M没有在KeyGen询问阶段向C发送过身份ID_{i^*}与ID_{j^*}。

2) 敌手M没有在M_{req}询问阶段向C同时发送过身份ID_{i^*}与ID_{j^*}。

3) 敌手M没有在M_{rsp}询问阶段向C同时发送过身份ID_{i^*}与ID_{j^*}。

4) 敌手M在挑战阶段必须发送的是身份ID_{i^*}与ID_{j^*}。

那么C在以上条件下利用敌手M的能力成功解决CDH困难问题的概率为

$$\begin{aligned} & \mathrm{Adv}_C^{\mathrm{CDH}}(\lambda) \geqslant \Pr[\mathrm{Event}_1]\Pr[\mathrm{Event}_2]\Pr[\mathrm{Event}_3] \cdot \\ & \Pr[\mathrm{Event}_4]\frac{1}{q_{H_2}}\left(\frac{1}{2}+\varepsilon\right) \geqslant \\ & \left(1-\frac{2}{q_n}\right)^{q_{kg}}\left(1-\frac{2}{q_n}\right)^{q_{M\mathrm{rsp}}}\left(1-\frac{2}{q_n}\right)^{q_{M\mathrm{req}}}\frac{2}{q_{H_2}q_n}\left(\frac{1}{2}+\varepsilon\right) \geqslant \\ & \frac{2}{q_{H_2}q_n}\left(1-\frac{2}{q_n}\right)^{q_{kg}+q_{M\mathrm{rsp}}+q_{M\mathrm{req}}}\left(\frac{1+2\varepsilon}{2}\right) \geqslant \\ & \frac{1+2\varepsilon}{q_{H_2}q_n}\left(1-\frac{2}{q_n}\right)^{q_{kg}+q_{M\mathrm{rsp}}+q_{M\mathrm{req}}} \end{aligned} \tag{43}$$

由于现实中不存在算法能够在多项式时间内以不可忽略的优势破解CDH困难问题，因此不存在敌手M能够以不可忽略的优势攻破本文方案并获取会话密钥的信息。证毕。

3.2　形式化安全性分析

本文方案使用形式化仿真工具Scyther来仿真和辅助分析协议的安全性。Scyther是在完美密码学假设（即除非攻击者知道加密密钥，否则无法获取消息内容）的前提下，进行协议形式化分析的仿真工具。Scyther基于Dolev-Yao强安全模型，不存在状态空间爆炸，适用于分析使用第三方加密算法且参与角色较少的协议。Scyther使用SPDL标准协议描述语言描述协议，按照参与角色模拟消息传递

过程，从基本的协议形式化模型的安全属性角度，验证认证协议中消息是否可达且被接受，能否保证消息同步，能否在一定程度上抵御消息篡改和伪造、身份假冒、中间人攻击等安全攻击。其结果只存在安全或攻击2种可能，如果存在攻击，则以攻击图的形式呈现在界面上。

Scyther仿真输出结果中的“verified”表示对安全属性的验证，“ok”表示安全属性可满足。本文方案使用SPDL标准协议描述语言描述，实现形式如图3所示。Scyther验证结果如图4所示。

```
role Alice
{
        fresh rA: Nonce;
        var rB: Nonce;

        macro RA={rA}G;
        macro SA = h2(hash{RAAlcel}sk(Alice),rA,q);
        macro key = {rB}RA;
        macro T = {{hash(RA.Bob)}rB}pk(Bob);
        macro SB = h1({hash(T.key}sk(Bob),[{hash(RA.Bob}rB,q);

        send_1 (Alice, Bob,{RA,SA}pk(Bob));
        recv_2 (Bob,Aice, {T,SB}pk(Alicel));
        send_ 3 (Alice,Bob,{hash(SB)}pk(Bobl));

        claim .4(Alice, Secret key);
        claim_5 (Alice, Alive);
        claim_6 (Alice,Weakagree);
        claim_7 (Alice, Niagree );
        claim_8 (Alice, Nisynch);
}       macro SA = h2(hash{RAAlcel}sk(Alice),rA,q);

role Bob
{
        var rA: Nonce;
        fresh rB: Nonce;

        macro RA=[{rA}G;
        macro SA =h2({hash(RA.Alice)}sk(Alice),IA,q);
        macro key ={rB}RA;
        macro T ={{hash(RA.Bob)}rB}pk(Bob);
        macro SB = h1({hash(T,key)}sk(Bob),{hash(RA,Bob)}rB,q);

        recv_1(Alice, Bob,{RA,SA}pk(Bob));
        send_2(Bob,Alice,{T,SB}pk(Alice));
        recv_ 3(Alice,Bob,{hash(SB)}pk(Bob));

        claim_9 (Bob,Secret,key);
        claim_10(Bob,Alive);
        claim_11(Bob,Weakagree);
        claim_12(Bob,Niagree);
        claim_13(Bob,Nisynch);

}
```

图3　本文方案在形式化分析工具中的实现形式

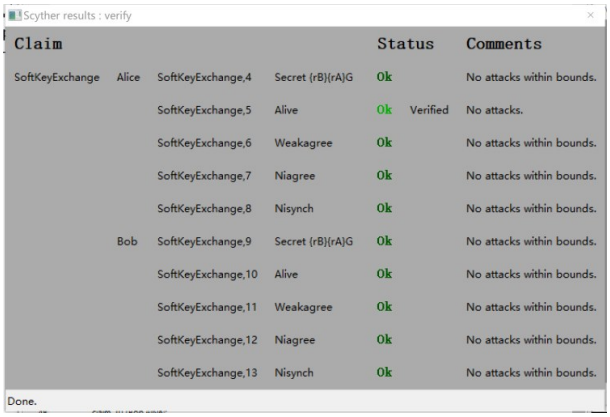

图4　Scyther验证结果

Scyther验证结果表明，本文协议能够抵御中间人发动的消息篡改和伪造、身份假冒以及窃听等安全攻击，满足抗中间人攻击的安全性。

3.3　非形式化安全性分析

1) 抗重放攻击

本文方案在两方生成的零知识证明中均引入了时间戳作为输入，时间戳能保证发送的数据包仅在指定的时间范围内有效，若零知识证明中的时间戳与对方验证的当前时间不符，则验证无法通过，导致协商失败。因此，中间人敌手无法通过转发早期信道中已截获的数据包发起重放攻击。并且，在本文协议中，时间戳嵌入在零知识证明的s参数中，只有拥有合法私钥的用户才能生成合法的证明参数，并替换新的时间戳。而中间人敌手由于无法篡改证明参数，因此无法通过更新时间戳的方式发起重放攻击。因此，本文方案可以抵抗中间人敌手发起的重放攻击。

2) 抗前向/后向安全威胁

本文方案中的会话密钥包含协商双方的TEE各自临时生成的随机数，并且会根据每次调用Enclave环境而动态改变。中间人敌手无法了解双方的TEE内部情况，所以不能了解随机数产生和更新的逻辑规律。因此，本文方案产生的会话密钥是由TEE保障的动态密钥，中间人敌手不能通过已经掌握的会话密钥来推断密钥双方在前期和后期协商生成的其他会话密钥，即本文方案能抵抗中间人敌手的前向/后向安全威胁。

4　性能分析

为了展示本文方案在效率方面的优势，以及抗中间人攻击的高鲁棒性，本节对本文方案进行了性

能分析，选取的4个对比方案分别为近期提出的认证密钥协商协议[15,20-21]以及国密SM2认证密钥协商协议[18]。通过将本文方案与4个对比方案进行实验对比，验证了本文方案在抗中间人攻击方面的有效性与鲁棒性。

本文协议的计算开销涉及异或运算、级联运算、算数运算、模逆运算、单向哈希运算T_h和椭圆曲线点乘T_{ecm}，其中，异或、级联、算数和模逆运算需要的计算时间较短，因此在计算开销中可忽略。本文实验中选用的椭圆曲线参数为国密SM2推荐的椭圆曲线参数，其中一个点的尺寸为$|G|$=64 B，整数群元素的大小与国密SM3哈希值的尺寸相同，均为$|Z_q|$=32 B。

本文实验的配置环境为支持SGX的HPE服务器，操作系统版本为CentOS Linux release 7.9.2009 (Core)，CPU版本为Intel(R) Xeon(R) Silver 4410Y，内存大小为256 GB，内核版本为3.10.0-1160.el7.x86_64。本文协议中密码学运算在机密计算环境中的平均执行时间如表2所示。各协议的通信开销与计算开销对比如表3所示。

表2　　密码学运算的平均执行时间

密码运算	执行环境	计算时间/ms
T_h	Enclave	0.009 776 7
T_{ecm}	Enclave	1.418 4

表3　　各协议性能开销对比

方案	用户通信次数/次	通信开销/B	计算开销/ms
文献[15]	2	$6\|G\|+2\|Z_q\|$	$16T_{\text{ecm}}+2T_h$
文献[21]	2	$6\|G\|+6\|Z_q\|$	$10T_{\text{ecm}}+2T_h$
文献[20]	2	$2\|G\|+\|Z_q\|$	$8T_{\text{ecm}}+6T_h$
文献[18]	2	$2\|G\|+\|Z_q\|$	$6T_{\text{ecm}}+4T_h$
本文方案	2	$2\|G\|+2\|Z_q\|$	$7T_{\text{ecm}}+4T_h$

为了更直观地展示对比结果，图5以直方图的形式列出了表3各协议的计算开销情况，图6以直方图的形式列出了表3各协议的通信开销情况。从图5和图6中可以看出，本文方案的性能与文献[20]和文献[18]接近，优于文献[15]和文献[21]。其中，文献[20]和文献[18]均为基于国密SM2算法的密钥协商协议，本文方案采用的双重非交互式零知识证明方法仅需用户A多执行一次点乘运算，用户B的计算开销则与SM2密钥协商算法的用户一致；文献[15]设计中要求用户生成大量椭圆曲线群中元素导致计算开销与通信开销较大；文献[21]则由于需要通过区块链来帮助完成通信过程，且在协议执行过程中引入了基于离散对数的零知识证明算法，因此带来了较大的计算压力与通信负担。

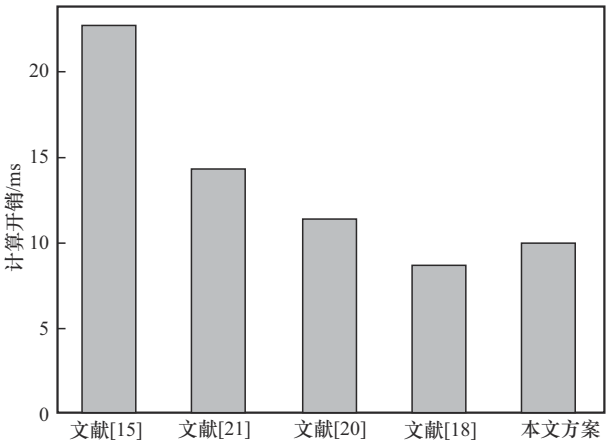

图5　计算开销比较

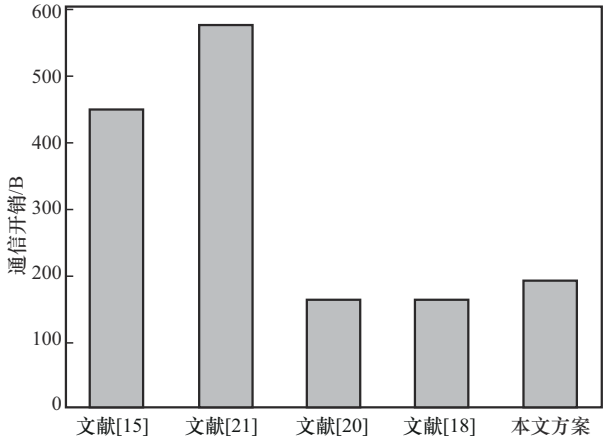

图6　通信开销比较

5　结束语

本文对数据出域场景中大规模设备通信需求下的认证密钥协商协议进行了研究，基于TEE提出了一种面向数据出域安全的鲁棒认证密钥协商协议。本文在可信执行环境中结合双重非交互式零知识证明，实现了鲁棒抗中间人攻击。并且针对TEE设备抗中间人攻击的安全目标，提出了2个相应的安全模型，并对本文协议进行了形式化安全性证明。最后，实验结果和性能分析表明，本文协议与同类型的协议相比在安全性与效率方面均有优势，满足数据出域场景下的数据安全传输需求。

参考文献：

[1] 李凤华, 李晖, 牛犇, 等. 数据要素流通与安全的研究范畴与未来发展趋势[J]. 通信学报, 2024, 45(5): 1-11.
LI F H, LI H, NIU B, et al. Research category and future development trend of data elements circulation and security[J]. Journal on Communications, 2024, 45(5): 1-11.

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

[3] BELLARE M, ROGAWAY P. Entity authentication and key distribution[C]// Advances in Cryptology-CRYPTO' 93. Berlin: Springer, 1994: 232-249.

[4] SHEPHERD C, MARKANTONAKIS K. Trusted execution environments[M]. Berlin: Springer, 2024.

[5] ASOKAN N. Hardware-assisted trusted execution environments: look back, look ahead[C]//Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security. New York: ACM Press, 2019: 1687.

[6] SABT M, ACHEMLAL M, BOUABDALLAH A. Trusted execution environment: what it is, and what it is not[C]//Proceedings of the 2015 IEEE Trustcom/BigDataSE/ISPA. Piscataway: IEEE Press, 2015: 57-64.

[7] EKBERG J K, KOSTIAINEN K, ASOKAN N. Trusted execution environments on mobile devices[C]//Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security. New York: ACM Press, 2013: 1497-1498.

[8] SHEPHERD C, AKRAM R N, MARKANTONAKIS K. Establishing mutually trusted channels for remote sensing devices with trusted execution environments[C]//Proceedings of the 12th International Conference on Availability, Reliability and Security. New York: ACM Press, 2017: 1-10.

[9] LEE S, LEE J H. TEE based session key establishment protocol for secure infotainment systems[J]. Design Automation for Embedded Systems, 2018, 22(3): 215-224.

[10] WU T Y, GUO X L, CHEN Y C, et al. SGXAP: SGX-based authentication protocol in IoV-enabled fog computing[J]. Symmetry, 2022, 14(7): 1393.

[11] WU T Y, WANG L Y, GUO X L, et al. SAKAP: SGX-based authentication key agreement protocol in IoT-enabled cloud computing[J]. Sustainability, 2022, 14(17): 11054.

[12] 冯登国, 秦宇, 汪丹, 等. 可信计算技术研究[J]. 计算机研究与发展, 2011, 48(8): 1332-1349.
FENG D G, QIN Y, WANG D, et al. Research on trusted computing technology[J]. Journal of Computer Research and Development, 2011, 48(8): 1332-1349.

[13] 杨波, 冯伟, 秦宇, 等. 基于TEE和SE的移动平台双离线匿名支付方案[J]. 软件学报, 2024, 35(8): 3553-3576.
YANG B, FENG W, QIN Y, et al. Dual offline anonymous E-payment scheme for mobile devices based on TEE and SE[J]. Journal of Software, 2024, 35(8): 3553-3576.

[14] AL-ANI A, ANBAR M, HASBULLAH I H, et al. Authentication and privacy approach for DHCPv6[J]. IEEE Access, 2019, 7: 73144-73156.

[15] 曾润智, 王立斌. 一种高效的无证书认证密钥交换协议[J]. 密码学报, 2020, 7(4): 421-429.
ZENG R Z, WANG L B. An efficient certificateless authenticated key exchange protocol[J]. Journal of Cryptologic Research, 2020, 7(4): 421-429.

[16] 冉津豪, 蔡栋梁. 基于区块链和可信执行环境的属性签名身份认证方案[J]. 计算机研究与发展, 2023, 60(11): 2555-2566.
RAN J H, CAI D L. Attribute signature identity authentication scheme based on blockchain and trusted execution environment[J]. Journal of Computer Research and Development, 2023, 60(11): 2555-2566.

[17] 姚志强, 竺智荣, 叶帼华. 基于密钥协商的防范DHCP中间人攻击方案[J]. 通信学报, 2021, 42(8): 103-110.
YAO Z Q, ZHU Z R, YE G H. Achieving resist against DHCP man-in-the-middle attack scheme based on key agreement[J]. Journal on Communications, 2021, 42(8): 103-110.

[18] 汪朝晖, 张振峰. SM2椭圆曲线公钥密码算法综述[J]. 信息安全研究, 2016, 2(11): 972-982.
WANG Z H, ZHANG Z F. Overview on public key cryptographic algorithm SM2 based on elliptic curves[J]. Journal of Information Security Research, 2016, 2(11): 972-982.

[19] 王新明, 曹瑀晗, 杜科. 基于SM2的车联网身份认证密钥协商协议[J]. 物联网技术, 2024, 14(3): 62-65, 71.
WANG X M, CAO Y H, DU K. SM2-based key agreement protocol for identity authentication of vehicle networking[J]. Internet of Things Technologies, 2024, 14(3): 62-65, 71.

[20] 王晓虎, 林超, 伍玮. 基于SM2的标识认证密钥交换协议[J]. 信息安全学报, 2024, 9(2): 84-95.
WANG X H, LIN C, WU W. SM2-based identity-based authentication key exchange protocol[J]. Journal of Cyber Security, 2024, 9(2): 84-95.

[21] 黄佩达, 林超, 伍玮, 等. 基于SM2数字签名的区块链匿名密钥交换协议[J]. 信息安全学报, 2024, 9(3): 19-28.
HUANG P D, LIN C, WU W, et al. Blockchain anonymous key exchange based on SM2 digital signature protocol[J]. Journal of Cyber Security, 2024, 9(3): 19-28.

[22] MCKEEN F, ALEXANDROVICH I, BERENZON A, et al. Innovative instructions and software model for isolated execution[C]//Proceedings of the 2nd International Workshop on Hardware and Architectural Support for Security and Privacy. New York: ACM Press, 2013: 1-8.

[23] CANETTI R, KRAWCZYK H. Analysis of key-exchange protocols and their use for building secure channels[C]//International Conference on the Theory and Applications of Cryptographic Techniques. Berlin: Springer, 2001: 453-474.

[作者简介]

张晶辉（1988– ），女，天津人，中国科学院信息工程研究所博士生，主要研究方向为数据安全。

张起嘉（1995– ），男，河北深州人，贵州大学博士生，主要研究方向为公钥密码学。

田有亮（1982– ），男，贵州盘州人，博士，贵州大学教授、博士生导师，主要研究方向为算法博弈论、密码学与安全协议、大数据安全与隐私保护等。

刘海（1989– ），男，贵州遵义人，博士，贵州大学副教授、硕士生导师，主要研究方向为安全与隐私风险评估、应用密码与可证安全、数据安全与隐私保护等。

李凤华（1966– ），男，湖北浠水人，博士，中国科学院信息工程研究所研究员、博士生导师，主要研究方向为网络与系统安全、信息保护、隐私计算。