中国科学: 信息科学 2023 年 第 53 卷 第 9 期: 1734–1749
SCIENTIA SINICA Informationis
论文

面向移动边缘计算的广播身份认证协议

周彦伟[1,2,3], 许渊[1], 杨波[1*], 顾纯祥[3], 夏喆[4], 张明武[5]

1. 陕西师范大学计算机科学学院, 西安 710062
2. 密码科学技术国家重点实验室, 北京 100878
3. 河南省网络密码技术重点实验室, 郑州 450040
4. 武汉理工大学计算机科学与技术学院, 武汉 430070
5. 湖北工业大学计算机学院, 武汉 430068
* 通信作者. E-mail: byang@snnu.edu.cn

收稿日期: 2022–10–26; 修回日期: 2022–12–16; 接受日期: 2023–01–10; 网络出版日期: 2023–09–13

国家自然科学基金 (批准号: 62272287, U2001205)、广西密码学与信息安全重点实验室开放课题 (批准号: GCIS202108)、河南省网络密码技术重点实验室开放课题 (批准号: LNCT2021-A04)、陕西省教育厅专项科研计划项目 (批准号: 21JK0590) 和中央高校基本科研业务费专项资金 (批准号: GK202301009) 项目资助

摘要 随着无线通信技术在各领域的普及, 基于该技术演进的移动边缘计算 (mobile edge computing, MEC) 引起了诸多研究者的关注. 在 MEC 中, 为确保边缘节点接入过程的安全性, 近年来多个身份认证协议相继被提出, 然而上述传统方案仅支持一对一的身份合法性认证, 即实现了一个边缘节点与一个边缘服务器间的相互认证. 由于需要通过重复认证操作以满足边缘节点在多个边缘服务器间的迁移需求, 导致传统协议的工作效率较低、用户的通信体验欠佳. 针对传统协议无法高效地解决 MEC 中边缘节点的移动性问题, 本文基于无证书公钥密码体制, 提出支持广播通信的身份认证机制, 实现一个边缘节点同时与多个边缘服务器完成身份合法性认证的目标, 确保边缘节点在多服务器间迁移过程的服务连贯性, 提高 MEC 环境下的身份认证效率. 此外, 在随机谕言机模型下, 基于离散对数问题和计算性 Diffie-Hellman 问题分别证明了本文协议中通信消息的不可伪造性和协商密钥的安全性; 同时使用形式化分析工具 ProVerif 对协议的安全性进行了模拟验证, 结果表明本文协议具有其所声称的安全性. 与现有传统方案的性能对比结果表明本文协议具有更优的计算效率, 更加适合在 MEC 等终端计算资源受限的网络环境下部署.

关键词 身份认证, 移动边缘计算, 无证书密码机制, 可证明安全性

1 引言

随着物联网、云计算和工业互联网等新型网络环境下通信技术的不断成熟, 5G 移动通信技术已在多个领域中得到了广泛应用. 在传统基于云的物联网环境中, 传感设备会将收集的大量数据上传到

引用格式: 周彦伟, 许渊, 杨波, 等. 面向移动边缘计算的广播身份认证协议. 中国科学: 信息科学, 2023, 53: 1734–1749, doi: 10.1360/SSI-2022-0419
Zhou Y W, Xu Y, Yang B, et al. Broadcast identity authentication scheme for mobile edge computing (in Chinese). Sci Sin Inform, 2023, 53: 1734–1749, doi: 10.1360/SSI-2022-0419

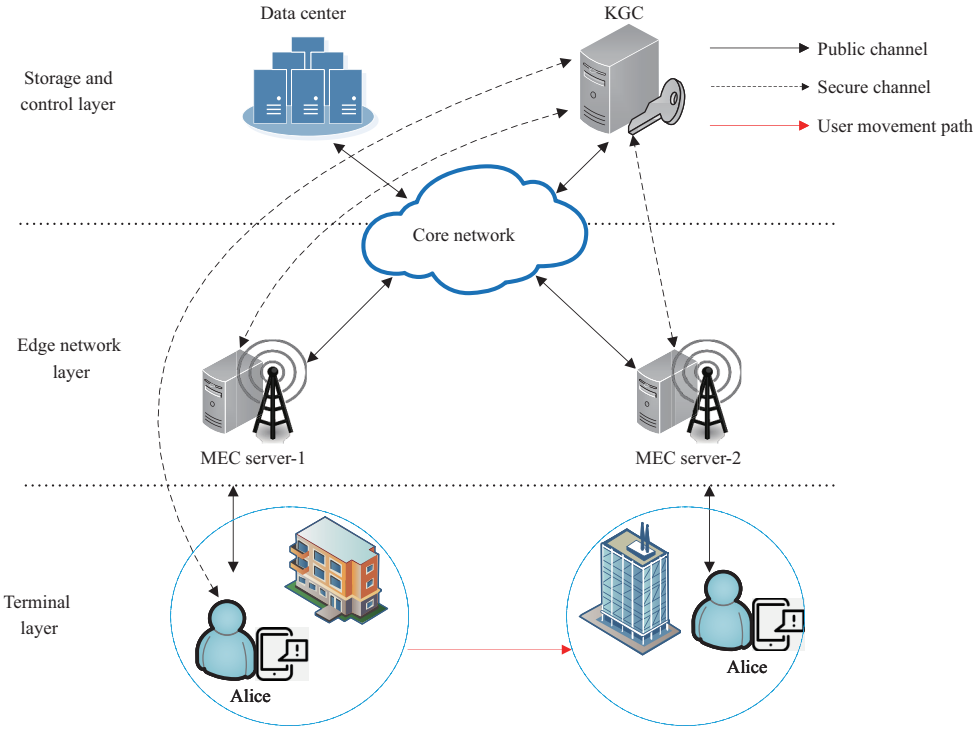

图 1 (网络版彩图) MEC 中边缘节点的移动性

Figure 1 (Color online) Mobility of edge nodes in MEC

云服务器进行集中处理和存储; 然而, 由于云服务器和传感设备所处的位置较远, 因此传统方式尚不能满足实时服务的低时延应用需求 (如车联网中的交通信息反馈、电子医疗系统中的健康监测等), 同时移动设备在处理类似业务时也受限于存储和计算能力的限制. 为了面向更多移动设备的多样化服务需求, 并满足移动终端对通信服务质量的低时延要求, 使得如何把移动网络深层融入通信业务, 提升网络带宽利用率已成为通信领域的热门研究方向 [1,2], 研究者开始探索设计能够在用户边缘提供实时服务的网络架构. 相对传统集中计算的通用模式而言, 边缘计算是将工作负载部署在用户边缘的一种新型的计算方式. 鉴于在时效性等方面的优势, 边缘计算已在云计算、物联网、工业互联网等领域得到了大规模使用 [3]. 为进一步满足移动用户对服务过程的低时延性需求, 在边缘计算的基础上, 欧洲电信标准协会提出了移动边缘计算 (mobile edge computing, MEC) 的网络架构, 将网络服务部署在移动终端周边, 用户可选择距离自己最近的边缘服务器为其提供服务, 通过减少通信过程的物理距离达到提升传输效率的目的, 同时也降低了传输过程中发生网络拥塞的可能性, 符合移动用户对网络通信服务的移动性和低时延的应用需求 [4,5]. 由于用户是在开放网络中与服务器进行通信, 增加了被攻击、窃听和假冒的风险. MEC 被广泛应用于各领域的同时对其安全性和隐私信息的保护已成为当前亟需解决的关键问题 [6]. 用户访问权限的控制和身份合法性的认证无疑是解决上述安全问题的有效途径, 因此近年来多个针对边缘计算环境的身份认证协议 [7~15] 相继被提出.

特别地, 在传统 MEC 架构中, 边缘节点的移动性问题未能得到妥善解决. 由于边缘节点需要在多个区域迁移 (例如家庭住址和工作单位之间), 当边缘节点移动到已认证边缘服务器的工作范围之外时, 需与新的边缘服务器进行重新认证, 这势必导致正在进行的服务会产生中断, 使得用户体验较差. 如图 1 所示, 边缘节点 Alice 从一个已认证的区域进入未认证的区域, 由于需要与新边缘服务器进行

身份合法性的认证, 导致 Alice 的服务发生中断. 若要维持服务的连续性就会涉及用户信息的迁移, 需与新边缘服务器建立信任关系, 多次的重复认证势必导致很难为用户提供最佳的服务质量. 针对上述问题, 本文基于广播通信方式实现边缘节点同时认证一定范围内的多台边缘服务器, 当边缘节点位置发生改变需切换服务时, 不再重复认证或转移用户的身份信息, 由于已提前完成了身份认证, 相应的边缘服务器将直接为其提供服务, 降低了重复身份认证的时间消耗, 提高了 MEC 的工作效率, 进一步优化了 MEC 的服务质量.

此外, 基于身份的密码体制虽有效避免了传统公钥基础设施中证书的复杂管理问题, 却面临着密钥托管的不足, 并且在基于身份的密码体制中可信的密钥生成中心 (key generation center, KGC) 是不可或缺的基础机构, 而 MEC 架构很难满足这样的条件, 并且在现实环境中维护完全可信的 KGC 需要花费高昂的代价, 若不对可能存在的诚实但好奇 KGC (特别地, 诚实但好奇的 KGC 是指它能够诚实地执行协议的具体操作, 但它将利用已掌握的秘密窥探其他用户的隐私信息) 做出必要的防备, 将导致诚实但好奇 KGC 假冒用户完成签名、解密等秘密操作. 针对该问题, 本文以无证书公钥密码体制为底层基础工具, 设计新的广播身份认证协议, 该机制不再要求 KGC 是完全可信的, 能有效避免诚实但好奇 KGC 所导致的安全威胁.

1.1 相关工作

下面本文从认证模式和构建方式两个方面对当前 MEC 环境下的身份认证协议进行分析.

(1) 认证模式. 文献 [6] 分析了 MEC 的研究现状以及部署 MEC 系统所要面临的安全问题, 并指出与云计算和雾计算相比, 三者基本思想接近, 但 MEC 更侧重于降低传输时延, 适合物联网、车联网和增强现实等有低时延通信需求的应用场景使用. 文献 [7] 提出基于对称加密技术的身份认证协议, 但不具备匿名性 [8]. 文献 [9,10] 提出了轻量级的身份认证协议, 虽降低了协议的计算开销, 却增加了用户与服务器间的消息交互次数. 上述协议中, 用户与服务器间进行了一对一的身份合法性认证, 当用户离开已注册边缘服务器的服务范围进入新的服务区域时, 需要与新的边缘服务器重新进行身份合法性认证, 新的身份认证过程导致其无法满足 MEC 环境下服务的持续性需求; 同时, 重复认证使得上述协议的通信时延较大, 无法适应 MEC 环境下通信服务的高效性需求. 此外, 一对一的认证方式会导致用户移动过程出现服务中断的现象, 使得用户的通信体验欠佳.

(2) 构建方式. 文献 [11] 提出一个基于身份的匿名认证协议, 文献 [12] 发现文献 [11] 的协议无法实现前后向安全性, 并设计了改进的认证协议, 而文献 [13] 指出文献 [12] 的构造中由于增加了认证的消息交互次数导致发生安全问题的风险增加, 并且认证参数的明文传输形式无法抵抗假冒等攻击, 致使该协议未能实现安全的身份认证目标. 文献 [11~17] 都是基于身份的认证协议, 他们的密钥管理都依赖于可信的 KGC, 因此这些协议同样无法抵抗诚实但好奇 KGC 的攻击. 此外, 在现实环境中维护一个完全可信的 KGC 会耗费大量的资源. 文献 [18] 设计了两个面向无线体域网的远程匿名认证方案, 该方案基于无证书签名机制. 文献 [19] 为边缘计算设计了基于区块链的无证书身份认证协议, 并声称该方案具有去中心化和匿名性的特点. 然而上述已有协议 [18,19] 只支持单播信道传输消息, 相较于广播认证模式而言, 与多台服务器进行身份认证时单播通信的计算和通信的开销较大. 文献 [20] 表明广播消息要比多次发送单播消息的效率更高, 并且在不考虑时延控制时, 广播信道具有更精确的同步控制能力. 文献 [21,22] 都是基于广播通信的多接收者签名方案, 但是用户端的计算开销较大, 不符合 MEC 环境下将复杂计算迁移在服务器端进行处理的优化理念. 文献 [23] 提出针对隐私保护的无证书远程匿名认证协议, 但该协议不满足前向安全性. 文献 [24] 基于实时更新的时间密钥提出了可撤销的身份认证协议, 并降低了用户端的存储代价. 文献 [25] 所提出的无证书认证协议存在用户端计算成

本高的不足. 文献 [26] 在无需可信第三方的情况下设计了一个身份认证协议, 然而该协议使用了双线性映射运算导致计算效率较低. 文献 [27] 提出了基于身份的广播加密机制. 文献 [28] 提出了服务器辅助的基于属性的广播签名机制. 虽然上述方案 [27,28] 在实现广播通信的同时提供了必要的匿名性保护措施, 但是它们存在密钥托管的不足, 不适合在 MEC 环境下部署.

综上所述, 现有的身份认证协议普遍存在密钥托管, 仅支持单播通信, 计算效率偏低等不足, 导致传统身份认证协议不适合在终端资源受限的 MEC 环境下部署.

1.2 本文工作

针对现有身份认证协议所存在的不足, 面向 MEC 中边缘节点的移动性特点, 本文提出基于无证书公钥密码体制的广播身份认证协议. 该协议不再使用双线性运算实现减少计算开销的目的, 无证书密码体制的初始化过程不再依赖完全可信的 KGC, 达到避免密钥托管的目标; 通过广播认证方式解决 MEC 环境所面临的用户移动性问题, 进一步实现身份认证机制的高认证效率需求; 同时, 认证过程的匿名性有效保护了用户的通信轨迹无法被敌手追踪. 本文方案在保证身份认证过程安全可靠的同时, 降低了协议的计算开销, 具有较高的通信效率. 上述优点表明本文协议更适合在终端计算资源受限的 MEC 环境下部署.

本文的主要贡献是针对边缘节点的移动性特点, 面向 MEC 环境中通信服务的低时延性和连贯性需求, 设计了无证书广播身份认证协议, 实现一个边缘节点与多个边缘服务器间同时的身份合法性认证. 与相关身份认证协议的性能比较结果说明本文方案的计算开销更低, 并且仅需一轮信息交互即可实现一个边缘节点与多台边缘服务器间身份合法性的认证和会话密钥的协商, 提高了认证效率.

2 基础知识

2.1 困难假设

(1) 离散对数 (discrete logarithm, DL) 假设. 令 G 是阶为 q 的加法循环群, P 为 G 的生成元. 已知 $aP \in G$, 算法 $\mathcal{A}$ 在概率多项式时间内已知公开元组 (P, aP) 的前提下求解 $a \in Z_q^*$ 的优势是可忽略的. 则算法 $\mathcal{A}$ 成功解决 DL 问题的优势定义为 $\mathrm{Adv}_{\mathcal{A}}^{\mathrm{DL}}(\kappa) = \Pr[\mathcal{A}(P, aP) = a]$, 且 $\mathrm{Adv}_{\mathcal{A}}^{\mathrm{DL}}(\kappa) \leqslant \mathsf{negl}(\kappa)$, 其中 $\mathsf{negl}(\kappa)$ 表示安全参数 κ 上可忽略的值.

(2) 计算性 Diffie-Hellman (computation Diffie-Hellman, CDH) 假设. 对于 $a, b \in Z_q^*$, 已知 $aP, bP \in G$, 在概率多项式时间内已知公开元组 (P, aP, bP) 的前提下计算 abP 的优势是可忽略的. 算法 $\mathcal{A}$ 成功解决 CDH 问题的优势定义为 $\mathrm{Adv}_{\mathcal{A}}^{\mathrm{CDH}}(\kappa) = \Pr[\mathcal{A}(P, aP, bP) = abP]$, 且 $\mathrm{Adv}_{\mathcal{A}}^{\mathrm{CDH}}(\kappa) \leqslant \mathsf{negl}(\kappa)$.

2.2 分叉引理

文献 [29~31] 详细介绍了分叉引理的具体内容, 指出若存在敌手能以一定的优势伪造一个签名, 那么敌手成功伪造满足相应条件的两个合法签名的概率可表示为: 对于一个形式为 (m, δ, r, h) 的签名, 其中 m 是待签名消息, δ 是相应的签名值, r 和 h 分别为生成签名所使用的随机数和哈希值. 若存在概率多项式时间敌手 $\mathcal{A}$ 能以优势 $\varepsilon(\kappa)$ 伪造一个有效签名, 且对随机谕言机 H 进行了 q_H 次询问, 那么基于谕言机 H 的重放操作, $\mathcal{A}$ 使用相同的随机数 r^* 和不同的谕言机应答 $h^*, h'(h^* \neq h')$ 输出两个有效签名组 $(m^*, \delta^*, r^*, h^*)$ 和 (m^*, δ', r^*, h') 的概率至少为 $\left(1 - \frac{1}{\mathrm{e}}\right) \frac{\varepsilon(\kappa)}{q_H}$, 其中 e 是自然对数底数. 特别地, 上述交互中挑战者获得了两个合法签名 δ^* 和 δ'. 文献 [32,33] 详细介绍了分叉引理的使用方法.

3 系统框架和安全模型

3.1 系统框架

如图 1 所示, MEC 框架包含 3 个参与实体, 分别是移动边缘节点、边缘服务器和 KGC, 其中 KGC 只负责响应边缘节点和边缘服务器的注册请求, 并为其生成必要的部分私钥, 无需全程在线. 由上述对框架的介绍可知, 身份认证技术是 MEC 框架下确保边缘节点与边缘服务器进行安全通信的前提, 能够实现双向身份认证的同时完成会话密钥的安全协商.

3.2 安全模型

在无证书公钥密码 (certificateless public-key cryptography, CL-PKC) 体制中无需要求 KGC 是可信的, 那么诚实但好奇的 KGC 将利用掌握主私钥的便利对 CL-PKC 展开攻击; 此外恶意的用户能够通过替换合法用户公钥的方式伪装成其他用户对 CL-PKC 进行攻击. 由此可见, CL-PKC 将遭受来自恶意用户 (相当于外部敌手) 和诚实但好奇 KGC (相当于内部敌手) 两种敌手的攻击, 因此本文协议将面临外部敌手 $\mathcal{A}_1$ 和内部敌手 $\mathcal{A}_2$ 的攻击, 根据两类敌手攻击能力的不同, 分别介绍如下:

(1) $\mathcal{A}_1$ 可视为是系统的恶意用户, 可以查询和替换合法用户的公钥, 但无法掌握系统的主密钥, 也不能获知用户的私钥信息;

(2) $\mathcal{A}_2$ 可视为诚实但好奇的 KGC, 它无法替换用户的公钥, 但却已掌握系统的主密钥, 可以利用系统主密钥获取用户的部分私钥.

假设 A 和 B 为身份认证协议的两个参与者, 用 $\prod_{A,B}^{k}$ 表示参与者 A 和 B 的第 k 次会话. 通过下述游戏来定义身份认证协议的会话密钥安全性.

游戏 1. 在该游戏中, 挑战者 $\mathcal{C}$ 生成公开参数 params 和主密钥 msk, 秘密保存 msk 的同时发送公开参数 params 给 $\mathcal{A}_1$, $\mathcal{A}_1$ 可进行下述询问.

秘密值生成询问. $\mathcal{A}_1$ 询问用户 ID 的秘密值, $\mathcal{C}$ 运行秘密值生成算法生成 x_{ID} 并返回给 $\mathcal{A}_1$.

公钥生成询问. $\mathcal{A}_1$ 进行用户 ID 的公钥生成询问, 发送 ID 给 $\mathcal{C}$, 挑战者 $\mathcal{C}$ 运行秘密值生成算法和公钥生成算法产生相应的公钥 $\mathrm{pk}_{\mathrm{ID}}$ 并返回给 $\mathcal{A}_1$.

部分私钥生成询问. $\mathcal{A}_1$ 进行用户 ID 的部分私钥生成询问, 发送 ID 和 $\mathrm{pk}_{\mathrm{ID}}$ 给 $\mathcal{C}$, 挑战者 $\mathcal{C}$ 运行部分私钥生成算法产生相应的部分私钥 y_{ID} 给 $\mathcal{A}_1$.

私钥生成询问. $\mathcal{A}_1$ 进行用户 ID 的私钥生成询问, 发送 ID 给 $\mathcal{C}$, 挑战者 $\mathcal{C}$ 运行秘密值生成算法和部分私钥生成算法并返回秘密值 x_{ID} 和部分私钥 y_{ID} 作为私钥给 $\mathcal{A}_1$.

公钥替换. $\mathcal{A}_1$ 能够替换用户 ID 的公钥 $\mathrm{pk}_{\mathrm{ID}}$ 为已知的 $\mathrm{pk}'_{\mathrm{ID}}$, 并且 $\mathcal{C}$ 将记录此次替换的相关信息.

Send 询问. 模拟 $\mathcal{A}_1$ 的主动攻击能力, $\mathcal{A}_1$ 可通过发送该询问启动身份合法性认证协议.

Reveal 询问. $\mathcal{A}_1$ 获得 $\prod_{A,B}^{k}$ 产生的会话密钥 sek, 如果 $\prod_{A,B}^{k}$ 没有成功生成会话密钥, 则返回 $\perp$.

Test($\prod_{A,B}^{k}$) 询问. $\mathcal{A}_1$ 可发送针对新鲜会话 $\prod_{A,B}^{k}$ 的 Test 询问, $\mathcal{C}$ 随机选取 $b \leftarrow_R \{0,1\}$, 若 $b=1$ 则返回正确的会话密钥 sek; 否则, 返回会话密钥空间中的任意随机值.

Test 询问之后, $\mathcal{A}_1$ 输出对随机数 b 的猜测 b', 若 $b=b'$, 且下述条件都满足时, $\mathcal{A}_1$ 在游戏中获胜.

(1) $\mathcal{A}_1$ 对 A 和 B 未进行部分私钥生成和私钥生成等询问, 未对会话 $\prod_{A,B}^{k}$ 进行 Reveal 询问;

(2) 参与者 A 和 B 协商了相同的会话密钥 sek, 且 sek 不会被除 A 和 B 之外的任意第三方获得.

在上述游戏中获胜的优势可定义为关于安全参数 κ 的函数 $\mathrm{Adv}_1(\kappa) = |\Pr[b'=b] - \frac{1}{2}|$.

游戏 2. 在该游戏中, 挑战者 $\mathcal{C}$ 生成公开参数 params 和主密钥 msk, 并将它们一起发送给敌手 $\mathcal{A}_2$, 且 $\mathcal{A}_2$ 可进行下述询问.

秘密值生成询问. $\mathcal{A}_2$ 进行用户的秘密值生成询问, $\mathcal{C}$ 运行秘密值生成算法产生相应的秘密值 x_{ID} 并返回给 $\mathcal{A}_2$.

公钥生成询问. $\mathcal{A}_2$ 进行用户 ID 的公钥生成询问, 发送 ID 给 $\mathcal{C}$, 挑战者 $\mathcal{C}$ 运行秘密值生成算法和公钥生成算法产生相应的公钥 $\mathrm{pk}_{\mathrm{ID}}$ 并返回给 $\mathcal{A}_2$.

Send 询问. 模拟 $\mathcal{A}_2$ 的主动攻击能力, $\mathcal{A}_2$ 可通过发送该询问启动身份认证协议.

Reveal 询问. $\mathcal{A}_2$ 获得 $\prod_{A,B}^{k}$ 产生的会话密钥 sek, 如果 $\prod_{A,B}^{k}$ 没有成功生成会话密钥, 则返回 $\perp$.

Test($\prod_{A,B}^{k}$) 询问. $\mathcal{A}_2$ 可发送针对新鲜会话 $\prod_{A,B}^{k}$ 的 Test 询问, $\mathcal{C}$ 随机选取 $b\leftarrow_R\{0,1\}$, 若 $b=1$ 则返回正确的会话密钥 sek; 否则, 返回会话密钥空间中的任意随机值.

Test 询问之后, $\mathcal{A}_2$ 输出对随机数 b 的猜测 b', 若 $b=b'$, 且下述条件都满足时, $\mathcal{A}_2$ 在游戏中获胜.

(1) $\mathcal{A}_2$ 对参与者 A 和 B 未进行秘密值生成和私钥生成等询问, 并未对 $\prod_{A,B}^{k}$ 进行 Reveal 询问;

(2) 参与者 A 和 B 协商了相同的会话密钥 sek, 且 sek 不会被除 A 和 B 之外的任意第三方获得.

在上述游戏中获胜的优势可定义为关于安全参数 κ 的函数 $\mathrm{Adv}_2(\kappa)=|\Pr[b'=b]-\frac{1}{2}|$.

定义1 (会话密钥安全性) 对于任意的概率多项式时间敌手 $\mathcal{A}_1$ 和 $\mathcal{A}_2$, 若它们在上述游戏 1 和 2 中获胜的优势都是可忽略的, 即有 $\mathrm{Adv}_1(\kappa)\leqslant \mathsf{negl}(\kappa)$ 和 $\mathrm{Adv}_2(\kappa)\leqslant \mathsf{negl}(\kappa)$, 那么相应的身份认证协议具有会话密钥安全性.

4 无证书广播身份认证协议

4.1 系统初始化

该阶段, KGC 执行初始化算法, 主要包括下述操作:

选择一个 q 阶加法循环群 G, P 为 G 的一个生成元. 选取随机数 $s\in Z_q^*$ 作为主密钥, 计算系统公开钥 $P_{\mathrm{pub}}=sP$. 令 $\mathsf{Enc}_k/\mathsf{Dec}_k$ 为语义安全的对称加解密算法, $\mathcal{K}$ 为对称密钥空间.

令 $H_1:\{0,1\}^*\times G\times G\to Z_q^*$, $H_2:\{0,1\}^*\times G\to Z_q^*$, $H_3:Z_q^*\to\{0,1\}^*$, $H_4:\{0,1\}^*\times G\times G\times\{0,1\}^*\to Z_q^*$, $H_5:\{0,1\}^*\times\{0,1\}^*\times G\times G\times\{0,1\}^*\to Z_q^*$, $H_6:G\times\{0,1\}^*\times\{0,1\}^*\times G\to\{0,1\}^*$ 和 $H_7:Z_q^*\to\mathcal{K}$ 为安全单向哈希函数.

最后, KGC 秘密保存主密钥 $\mathrm{msk}=s$ 的同时, 公开参数 $\mathrm{params}=\langle q,P,G,P_{\mathrm{pub}},H_1,H_2,H_3,H_4,H_5,H_6,H_7\rangle$.

4.2 注册阶段

边缘节点 Alice 和边缘服务器 MS 通过向 KGC 发送注册请求分别获得相应的部分私钥. 由于 MS 的注册过程与 Alice 相类似, 为避免重复, 在此本文只描述边缘节点 Alice 的注册过程.

(1) 身份为 ID_u 的边缘节点 Alice 随机选取 $x_u\in Z_q^*$, 计算 $X_u=x_uP$, 发送 (ID_u,X_u) 给 KGC.

(2) KGC 收到边缘节点 Alice 的注册请求后, 随机选取 $r_u\in Z_q^*$, 计算 $R_u=r_uP$, $H_u=H_1(\mathrm{ID}_u||R_u||X_u)$ 和 $y_u=r_u+sH_u \bmod q$, 然后返回 (R_u,y_u) 给 Alice.

(3) Alice 通过判断等式 $y_uP=R_u+P_{\mathrm{pub}}H_u$ 是否成立来验证部分私钥 (R_u,y_u) 的有效性. 最后, Alice 设置其公私钥分别为 $\mathrm{pk}_u=(X_u,R_u)$ 和 $\mathrm{sk}_u=(x_u,y_u)$.

4.3 相互身份认证

边缘节点 Alice 同时与身份为 $\{\mathrm{ID}_{\mathrm{ms}_1},\mathrm{ID}_{\mathrm{ms}_2},\ldots,\mathrm{ID}_{\mathrm{ms}_n}\}$ 的 n 个边缘服务器进行相互的身份合法性认证. 具体过程如下所述:

(1) Alice 进行如下操作. 随机选取 $a,b\in Z_q^*$, 并计算 $A=aP$, $B=bP$; 对于索引 $i\in(1,n)$, 计算 $M_i=b(X_{\mathrm{ms}_i}+R_{\mathrm{ms}_i}+H_{\mathrm{ms}_i}P_{\mathrm{pub}})$. 生成相应的身份认证参数集合 $\{\lambda_1,\lambda_2,\ldots,\lambda_n\}$, 其中 $\lambda_i=H_2\left(\mathrm{ID}_{\mathrm{ms}_i}||M_i\right)$.

选取 n 个随机数 $\{r_1,r_2,\ldots,r_n\}\in Z_q^n$ 对应每个需要认证的服务器, 通过式 (1) 计算相应会话密钥的参数集合 $W=\{w_1,w_2,\ldots,w_n\}\in Z_q^n$.

$$\begin{pmatrix} w_0\\ w_1\\ \vdots\\ w_{n-1}\end{pmatrix}=\begin{pmatrix} 1 & \lambda_1 & \cdots & \lambda_1^{n-1}\\ 1 & \lambda_2 & \cdots & \lambda_2^{n-1}\\ \vdots & \vdots & \vdots & \vdots\\ 1 & \lambda_n & \cdots & \lambda_n^{n-1}\end{pmatrix}^{-1}\begin{pmatrix} r_1\\ r_2\\ \vdots\\ r_n\end{pmatrix},\tag{1}$$

$$\begin{pmatrix} \varphi(\lambda_1)\\ \varphi(\lambda_2)\\ \vdots\\ \varphi(\lambda_n)\end{pmatrix}=\begin{pmatrix} 1 & \lambda_1 & \cdots & \lambda_1^{n-1}\\ 1 & \lambda_2 & \cdots & \lambda_2^{n-1}\\ \vdots & \vdots & \vdots & \vdots\\ 1 & \lambda_n & \cdots & \lambda_n^{n-1}\end{pmatrix}\begin{pmatrix} w_0\\ w_1\\ \vdots\\ w_{n-1}\end{pmatrix}=\begin{pmatrix} r_1\\ r_2\\ \vdots\\ r_n\end{pmatrix}.\tag{2}$$

对于 $i\in(1,n)$, 生成索引集合 $\{\pi_1,\pi_2,\ldots,\pi_n\}$, 其中 $\pi_i=H_3\left(r_i\right)$, 建立 π_i 与服务器 $\mathrm{ID}_{\mathrm{ms}_i}$ 的映射关系, π_i 作为标签帮助边缘服务器 $\mathrm{ID}_{\mathrm{ms}_i}$ 定位参数集合中隶属于自己的相关参数. 选取 $k_i\leftarrow_R\mathcal{K}$, 计算 $C=\mathsf{Enc}_{k_i}\left(\mathrm{ID}_u||A||R_u||X_u\right)$ 和 $L_i=H_7\left(r_i\right)\oplus k_i$, 令 $\tau=\{\tau_1,\tau_2,\ldots,\tau_n\}$, 其中 $\tau_i=\{L_i,\pi_i\}$; 令 $v=H_4\left(\mathrm{ID}_u||A||R_u||T_u\right)$, T_u 为 Alice 的当前时戳, 最后计算 $\sigma=v\left(a+y_u\right)+x_u$. 特别地, σ 是 Alice 为身份合法性认证消息生成的签名. 最后, Alice 将 (B,C,W,τ,σ,T_u) 以广播的形式发送给欲通信的边缘服务器集合 $\{\mathrm{ID}_{\mathrm{ms}_1},\ldots,\mathrm{ID}_{\mathrm{ms}_n}\}$.

(2) 当收到 Alice 的认证请求后, 边缘服务器 $\mathrm{MS}_j\,(j\in[1,n])$ 进行如下计算. 若 T_u 已过期, 则终止交互; 否则, MS_j 计算 $M_j'=\left(x_{\mathrm{ms}_j}+y_{\mathrm{ms}_j}\right)B$ 和 $\lambda_j=H_2\left(\mathrm{ID}_{\mathrm{ms}_j}||M'_j\right)$. 然后, 以 $W=\{w_0,w_1,\ldots,w_{n-1}\}$ 为系数构建多项式 $\varphi(x)=w_0+w_1x+\cdots+w_{n-1}x^{n-1}\bmod q$, 只有身份合法的边缘服务器才能基于身份认证参数 λ_j 根据式 (2) 计算出 $r_j=\varphi\left(\lambda_j\right)$ 和 $\pi_j=H_3\left(r_j\right)$, 并且以 π_j 为索引在集合 τ 中找出对应的参数 $\tau_j=\{L_j,\pi_j\}$. 特别地, 参数 λ_j 的合法性由等式 $M_j'=\left(x_{\mathrm{ms}_j}+y_{\mathrm{ms}_j}\right)B=b\left(X_{\mathrm{ms}_j}+R_{\mathrm{ms}_j}+H_{\mathrm{ms}_j}P_{\mathrm{pub}}\right)=M_j$ 获知.

计算 $k_j=H_7\left(r_j\right)\oplus L_j$ 和 $(\mathrm{ID}_u||A||R_u||X_u)=\mathsf{Dec}_{k_j}(C)$. 若 $\sigma P=v\left(A+R_u+H_uP_{\mathrm{pub}}\right)+X_u$ 不成立, 则边缘服务器 MS_j 终止; 否则, MS_j 选取 $d\in Z_q^*$, 计算 $D=dP$, $\eta=H_5\left(\mathrm{ID}_u||\mathrm{ID}_{\mathrm{ms}_j}||A||D||T_{\mathrm{ms}_j}\right)$ 和 $\theta'=d\left(\eta A+R_u+H_uP_{\mathrm{pub}}\right)$, T_{ms_j} 为边缘服务器 MS_j 当前的时戳信息, 并计算相应的会话密钥 $\mathrm{sek}_{\mathrm{ms}_j-u}=H_6(\theta'||\mathrm{ID}_u||\mathrm{ID}_{\mathrm{ms}_j}||x_{\mathrm{ms}_j}X_u)$. 特别地, 认证请求消息合法性验证的正确性由等式 $\sigma P=v\left(a+y_u\right)P+x_uP=v\left(A+R_u+H_uP_{\mathrm{pub}}\right)+X_u$ 获知. 最后, 边缘服务器 MS_j 将应答消息 $\left(\pi_j,\eta,D,T_{\mathrm{ms}_j}\right)$ 返回给 Alice.

(3) 收到 $\mathrm{MS}_j\,(j\in[1,n])$ 的应答消息后, Alice 进行如下操作. 若时间 T_{ms_j} 已过期, 则 Alice 终止认证; 否则, 根据 π_j 找到对应的 $\mathrm{ID}_{\mathrm{ms}_j}$, 并确定相应的公开信息 $\left(R_{\mathrm{ms}_j},X_{\mathrm{ms}_j}\right)$. 若等式 $\eta=H_5(\mathrm{ID}_u||\mathrm{ID}_{\mathrm{ms}_j}||A||D||T_{\mathrm{ms}_j})$ 不成立, 则 MS_j 终止交互; 否则, 计算 $\theta=\left(\eta a+y_u\right)D$ 和 $\mathrm{sek}_{u-\mathrm{ms}_j}=H_6(\theta||\mathrm{ID}_u||\mathrm{ID}_{\mathrm{ms}_j}||x_uX_{\mathrm{ms}_j})$. 特别地, 由 $\theta=\left(\eta a+y_u\right)D=d\left(\eta aP+y_uP\right)=d\left(\eta A+R_u+H_uP_{\mathrm{pub}}\right)=\theta'$ 和 $x_uX_{\mathrm{ms}_j}=x_ux_{\mathrm{ms}_j}P=x_{\mathrm{ms}_j}X_u$ 可知 $\mathrm{sek}_{\mathrm{ms}_j-u}=\mathrm{sek}_{u-\mathrm{ms}_j}$. 特别地, 本文协议中对称加解密算法的语义安全性确保通信消息具有机密性.

4.4 安全性证明

本小节将对上述协议中认证及应答消息的不可伪造性和协商密钥的安全性分别进行证明, 且根据敌手能力的不同分两类情况分别进行证明.

定理1 若存在概率多项式时间敌手 $\mathcal{A}_1$ 能够以不可忽略的优势 ε_1 假冒边缘节点并伪造有效的身份认证请求消息, 那么存在敌手 $\mathcal{C}$ 能以显而易见的优势 $\varepsilon_1' \geqslant (1-\frac{1}{\mathrm{e}})\frac{\varepsilon_1}{q_h \mathrm{e}(q_1+q_2+q_3+1)}$ 解决 DL 问题, 其中 $\mathcal{A}_1$ 最多进行 q_1 次部分私钥生成询问, q_2 次私钥生成询问, q_3 次 Send 询问和 q_h 次 H_1 谕言机询问. 此外, e 为自然对数底数.

证明 敌手 $\mathcal{C}$ 从 DL 困难问题的挑战者处获得相应的公开参数 (q,P,G) 和挑战元组 $(P,\omega P)$, 令 $P_{\mathrm{pub}}=\omega P$ (隐含地设置主私钥 $s=\omega$), 并发送公开参数 $\mathrm{params}=\langle q,P,G,P_{\mathrm{pub}},H_1,H_2,H_3,H_4,H_5,H_6,H_7\rangle$ 给 $\mathcal{A}_1$, 其中 H_2,H_3,H_4,H_5,H_6 和 H_7 分别为安全的单向哈希函数, H_1 是随机谕言机. 此外, $\mathcal{C}$ 维持初始为空的列表 $L_{H_1},L_{\mathrm{pk}},L_{\mathrm{sk}},L_d$ 分别用于跟踪 $\mathcal{A}_1$ 所提交的 H_1 谕言机、公钥生成、私钥生成和部分私钥生成等询问; 并用列表 L_s 记录 $\mathcal{A}_1$ 所提交的身份认证请求信息. 特别地, $\mathcal{C}$ 随机选取询问身份 ID_{i^*} 作为挑战身份.

(1) 部分私钥生成询问. 该询问的输入是 (ID_i,X_i). 若 $\mathrm{ID}_i=\mathrm{ID}_{i^*}$, 则 $\mathcal{C}$ 终止游戏; 否则 $\mathcal{C}$ 执行下述操作: 若 $(\mathrm{ID}_i,R_i,y_i)\in L_d$, 那么 $\mathcal{C}$ 返回相应的 (R_i,y_i) 给 $\mathcal{A}_1$; 否则, $\mathcal{C}$ 随机选取 $y_i,H_i\in Z_q^*$ 满足 $(*,*,*,H_{u_i})\notin L_{H_1}$(避免哈希函数产生碰撞), 计算 $R_i=y_iP-H_iP_{\mathrm{pub}}$, 返回 (R_i,y_i) 给 $\mathcal{A}_1$, 将元组 (ID_i,R_i,y_i) 和 $(\mathrm{ID}_i,X_i,R_i,H_i)$ 分别添加到列表 L_d 和 L_{H_1}.

(2) H_1 询问. 该询问的输入是 (ID_i,X_i,R_i). 若有 $(\mathrm{ID}_i,X_i,R_i,H_i)\in L_{H_1}$, 则 $\mathcal{C}$ 返回相应的 H_i 给 $\mathcal{A}_1$; 否则, 随机选取 $x_i\in Z_q^*$, 计算 $X_i=x_iP$, 通过提交元组 (ID_i,X_i) 给 $\mathcal{C}$ 对 ID_i 进行部分私钥生成询问, 获得相关应答后返回列表 L_{H_1} 中相应元组 $(\mathrm{ID}_i,X_i,R_i,H_i)$ 的 H_i 给 $\mathcal{A}_1$.

(3) 私钥生成询问. 该询问的输入是 ID_i. 若 $\mathrm{ID}_i=\mathrm{ID}_{i^*}$, 则 $\mathcal{C}$ 终止游戏; 否则 $\mathcal{C}$ 执行下述操作: 若 $(\mathrm{ID}_i,x_i,y_i)\in L_{\mathrm{sk}}$, $\mathcal{C}$ 返回 (x_i,y_i) 给 $\mathcal{A}_1$; 否则 $\mathcal{C}$ 随机选取 $x_i\in Z_q^*$, 计算 $X_i=x_iP$, 对 (ID_i,X_i) 进行部分私钥生成询问, 获得相应的应答 (R_i,y_i) 后, $\mathcal{C}$ 返回 (x_i,y_i) 给 $\mathcal{A}_1$, 并将元组 (ID_i,x_i,y_i) 和 (ID_i,X_i,R_i) 分别添加到列表 L_{sk} 和 L_{pk}.

(4) 公钥生成询问. 该询问的输入是 ID_i. 若 $(\mathrm{ID}_{u_i},X_{u_i},R_{u_i})\in L_{\mathrm{pk}}$, 则 $\mathcal{C}$ 返回给 $\mathcal{A}_1$; 否则 $\mathcal{C}$ 进行下述操作: 若 $\mathrm{ID}_i=\mathrm{ID}_{i^*}$, 随机选取 $x_{i^*},r_{i^*}\in Z_q^*$, 计算 $X_{i^*}=x_{i^*}P$ 和 $R_{i^*}=r_{i^*}P$, 返回 (X_{i^*},R_{i^*}) 给 $\mathcal{A}_1$, 并将 $(\mathrm{ID}_{i^*},X_{i^*},R_{i^*})$ 加入 L_{pk}; 否则, 随机选取 $x_i\in Z_q^*$, 计算 $X_i=x_iP$, 通过提交元组 (ID_i,X_i) 给 $\mathcal{C}$ 对 ID_i 进行部分私钥生成询问, 获得应答 (R_i,y_i) 后, 返回 (X_i,R_i) 给 $\mathcal{A}_1$, 并将元组 (ID_i,x_i,y_i) 和 (ID_i,X_i,R_i) 分别添加到列表 L_{sk} 和 L_{pk}.

(5) 公钥替换询问. 该询问的输入是 ID_i. $\mathcal{A}_1$ 可用其已知的 pk' 代替 ID_i 的原始公钥 pk_i, 并且 $\mathcal{C}$ 将修改 L_{pk} 中的相关记录.

(6) Send 询问. 在该游戏中, $\mathcal{A}_1$ 可发送下述 3 种类型的 Send 询问.

(i) $\mathrm{Send}(\prod_{i,j}^k,\mathrm{start})$. 如果 $\mathrm{ID}_i=\mathrm{ID}_{i^*}$, 则游戏终止; 否则执行以下操作: 如果 $\mathrm{ID}_i\notin L_{\mathrm{sk}}$, $\mathcal{C}$ 通过私钥生成询问获取 ID_i 的私钥 (x_i,y_i); 否则, $\mathcal{C}$ 从相应的列表 L_{sk} 中获得 ID_i 的私钥 (x_i,y_i). 然后根据协议执行过程计算 (B,C,W,τ,σ,T_u), 并将其返回给 $\mathcal{A}_1$, 同时更新 L_s. 特别地, $\prod_{i,j}^k$ 表示身份认证协议的发起者, 即边缘节点.

(ii) $\mathrm{Send}(\prod_{j,i}^k,(B,C,W,\tau,\sigma,T_u))$. 如果 $\mathrm{ID}_j\in L_{\mathrm{sk}}$, $\mathcal{C}$ 提取相关私钥; 否则以 ID_j 为输入进行私钥生成询问. 然后计算 $M_j=(x_j+y_j)\,B$ 和 $\lambda_j=H_2\,(\mathrm{ID}_j||M_j)$, 构建多项式 $\varphi(x)=w_0+w_1x+\cdots+w_{n-1}x^{n-1}\bmod q$, 并计算 $r_j=\varphi\,(\lambda_j)$, $\pi_j=H_3\,(r_j)$ 和 $k_j=H_7\,(r_j)\oplus L_j$, 通过运行对称的解密算法

$\mathcal{D}_{k_j}(C)$ 获知相应的交互信息 $(\mathrm{ID}_i||A||R_i||X_i)$. 若等式 $\sigma P = v\left(A + R_i + H_i P_{\mathrm{pub}}\right) + X_i$ 不成立 (其中 $v = H_4\left(\mathrm{ID}_u||A||R_u||T_u\right)$), 则拒绝响应该询问, 并终止游戏; 否则执行下述操作: 若 $\mathrm{ID}_i \neq \mathrm{ID}_{i^*}$, $\mathcal{C}$ 按照协议描述计算 $(\pi_j, \eta, D, T_{\mathrm{ms}_j})$ 返回给 $\mathcal{A}_1$; 若 $\mathrm{ID}_i = \mathrm{ID}_{i^*}$, 那么 $\mathcal{A}_1$ 伪造了合法的身份认证请求消息 $(B, C, W, \tau, \sigma, T_u)$. 特别地, $\prod_{j,i}^{k}$ 表示身份认证协议的应答者, 即边缘服务器.

(iii) Send$(\prod_{i,j}^{k}, (\pi_j, \eta, D, T_{\mathrm{ms}_j}))$. 如果 ID_i 的信息可以在 L_s 中检索到, 则以 π_j 为索引找到对应的 ID_j, 若 $\eta = H_5(\mathrm{ID}_u||\mathrm{ID}_{\mathrm{ms}_j}||A||D||T_{\mathrm{ms}_j})$, 则认证成功; 否则认证失败, 并终止会话.

假设 $\mathcal{A}_1$ 伪造了合法的身份认证请求消息 $(B, C, W, \tau, \sigma, T_u)$, 则有等式 $\sigma P = v(A + R_i + H_i P_{\mathrm{pub}}) + X_i$ 成立. 那么得到合法伪造验证信息中的签名值 σ 后, 对于 $\mathcal{C}$ 而言它将面临两个未知的随机数, 其中一个是 DL 困难问题的解 ω, 另一个是敌手 $\mathcal{A}_1$ 生成签名 σ 时选取的随机数 a. 由于 $\mathcal{C}$ 基于 σ 仅能得到关系 $\sigma = v\left(a + r_{i^*} + H_{i^*}\omega\right) + x_{i^*}$, 无法确定上述两个未知随机数 ω 和 a 的具体值, 因此 $\mathcal{C}$ 无法利用一条成功伪造的身份验证请求消息解决 DL 困难问题. 根据分叉引理, $\mathcal{C}$ 基于重放的方式, 通过更改谕言机 H_1 的应答结果, 使得 $\mathcal{A}_1$ 基于相同的随机数 a 和不同的谕言机应答结果 H_{i^*} 再次生成合法的身份认证请求消息 $(B, C, W, \tau, \tilde{\sigma}, T'_u)$, 那么 $\mathcal{C}$ 可以得到另一个关于未知随机数 ω 和 a 的关系 $\tilde{\sigma} = v\left(a + r_{i^*} + h'_{i^*}\omega\right) + x_{i^*}$. 上述两式相减得到 $\sigma - \tilde{\sigma} = v\left(H_{i^*} - h'_{i^*}\right)\omega$, 那么 $\mathcal{C}$ 输出 DL 问题的解 $\omega = \frac{\sigma - \tilde{\sigma}}{v(H_{i^*} - h'_{i^*})}$.

为评估 $\mathcal{C}$ 解决 DL 问题的优势, 定义事件 E_1 表示上述模拟游戏未终止; E_2 表示伪造了关于挑战身份的身份认证请求消息; E_3 表示敌手 $\mathcal{A}_1$ 生成了两个合法的身份认证请求消息 $(B, C, W, \tau, \sigma, T_u)$ 和 $(B, C, W, \tau, \tilde{\sigma}, T'_u)$. 由于在部分私钥生成、私钥生成和 Send 等询问中, 当 $\mathrm{ID}_i = \mathrm{ID}_{i^*}$ 时会导致上述模拟游戏终止, 因此有 $\Pr(E_1) = (1 - \frac{1}{q_1+q_2+q_3+1})^{q_1+q_2+q_3}$ 和 $\Pr\left(E_2\right) = \frac{1}{q_1+q_2+q_3+1}$; 此外, 根据分叉引理可知 $\Pr(E_3) \geqslant (1 - \frac{1}{\mathrm{e}})\frac{\varepsilon_1}{q_h}$. 因此, 有 $\varepsilon'_1 = \Pr(E_1 \wedge E_2 \wedge E_3) \geqslant (1 - \frac{1}{\mathrm{e}})\frac{\varepsilon_1}{q_h \mathrm{e}(q_1+q_2+q_3+1)}$.

综上所述, 若存在概率多项式时间敌手能够以不可忽略优势假冒边缘节点生成合法的身份认证消息, 那么可构造敌手能以显而易见的优势 $\varepsilon'_1 \geqslant \left(1 - \frac{1}{\mathrm{e}}\right)\frac{\varepsilon_1}{q_h \mathrm{e}(q_1+q_2+q_3+1)}$ 解决 DL 问题.

定理2 若存在概率多项式时间敌手 $\mathcal{A}_1$ 能够以不可忽略的优势 ε_2 伪造边缘服务器的合法应答消息, 那么存在敌手 $\mathcal{C}$ 能够以显而易见的优势 $\varepsilon'_2 \geqslant \frac{\varepsilon_2}{\mathrm{e}(q_1+q_2+q_3+1)}$ 解决 CDH 问题, 其中 $\mathcal{A}_1$ 最多进行 q_1 次部分私钥生成询问, q_2 次私钥生成询问, q_3 次 Send 询问.

证明 敌手从 CDH 困难问题的挑战者处获得相应的公开参数 (q, P, G) 和挑战元组 $(P, \alpha P, \beta P)$, 运行初始化算法后发送公开参数 $\mathrm{params} = \langle q, P, G, P_{\mathrm{pub}}, H_1, H_2, H_3, H_4, H_5, H_6, H_7\rangle$ 给 $\mathcal{A}_1$, 并秘密保存主私钥, 其中 H_2, H_3, H_4, H_5, H_6 和 H_7 分别为安全的单向哈希函数, H_1 是随机谕言机. 此外, $\mathcal{C}$ 维护初始化为空的 3 个列表 $L_{\mathrm{pk}}, L_{\mathrm{sk}}, L_d$ 分别用于跟踪 $\mathcal{A}_1$ 所提交的公钥生成、私钥生成和部分私钥生成等询问, 并用列表 L_s 记录 $\mathcal{A}_1$ 所提交的身份认证请求信息. 特别地, $\mathcal{C}$ 随机选取 ID_{j^*} 作为挑战身份.

(1) 部分私钥生成、私钥生成和公钥替换操作与定理 1 类似, 为避免重复此处不再赘述.

(2) 公钥生成询问. 该询问的输入是 ID_j. 当 $(\mathrm{ID}_j, X_j, R_j) \in L_{\mathrm{pk}}$, 则 $\mathcal{C}$ 返回 (X_j, R_j) 给 $\mathcal{A}_1$; 否则 $\mathcal{C}$ 进行下述操作: 若 $\mathrm{ID}_j = \mathrm{ID}_{j^*}$, 则令 $X_{j^*} = \beta P$ (隐含地设置对应的秘密值为 $x_{j^*} = \beta$, $\mathcal{C}$ 随机选取 $y_{j^*}, H_{j^*} \in Z_q^*$ 满足 $(*, *, *, h_{j^*}) \notin L_{H_1}$, 计算 $R_{j^*} = y_{j^*}P - H_{j^*}P_{\mathrm{pub}}$, 将元组 $(\mathrm{ID}_{j^*}, \perp, y_{j^*})$, $(\mathrm{ID}_{j^*}, X_{j^*}, R_{j^*})$ 和 $(\mathrm{ID}_{j^*}, X_{j^*}, R_{j^*}, H_{j^*})$ 分别添加到列表 L_{sk}, L_{pk} 和 L_{H_1}, 最后返回 (X_{j^*}, R_{j^*}) 给 $\mathcal{A}_1$; 否则, $\mathcal{C}$ 随机选取 $x_j \in Z_q^*$, 计算 $X_j = x_j P$, 对 (ID_j, X_j) 进行部分私钥生成询问获得 (R_j, y_j) 后, 返回 (X_j, R_j) 给 $\mathcal{A}_1$, 最后将 $(\mathrm{ID}_j, x_j, y_j)$ 和 $(\mathrm{ID}_j, X_j, R_j)$ 加入 L_{sk} 和 L_{pk}.

(3) Send 询问. 在这场游戏中, $\mathcal{A}_1$ 可发送下述 3 种类型的 Send 询问.

(i) Send$(\prod_{i,j}^{k}, \mathrm{start})$. 若 $\mathrm{ID}_j = \mathrm{ID}_{j^*}$ 且 $\mathrm{ID}_i \in L_{\mathrm{sk}}$, 令 $B = \alpha P$, 根据协议计算 $(C, W, \tau, \sigma, T_u)$, 返回

给 $\mathcal{A}_1$; 否则 $\mathcal{C}$ 通过私钥生成询问获得 ID_i 的私钥 (x_i, y_i) 并生成身份认证请求消息, 同时更新 L_s.

(ii) Send($\prod_{j,i}^{k}, (B, C, W, \tau, \sigma, T_u)$). 若 $\mathrm{ID}_j = \mathrm{ID}_{j^*}$, 则游戏终止; 否则, $\mathcal{C}$ 对 ID_j 进行私钥生成询问得到 ID_j 的相应私钥, 然后验证 σ 的合法性. 若 σ 的合法性验证通过, 则根据协议描述计算应答消息 $(\pi_j, \eta, D, T_{\mathrm{ms}_j})$ 并返回给 $\mathcal{A}_1$; 否则拒绝响应该询问.

(iii) Send($\prod_{i,j}^{k}, (\pi_j, \eta, D, T_{\mathrm{ms}_j})$). 如果 ID_i 的信息能够在列表 L_s 中检索到, 则根据索引 π_j 找到对应的 ID_j, 然后验证 $\eta = H_5\left(\mathrm{ID}_i||\mathrm{ID}_j||A||D||T_{\mathrm{ms}_j}\right)$, 若上述等式成立, 则 $\mathcal{A}_1$ 成功假冒边缘服务器并伪造了合法的身份认证应答消息 $(\pi_j, \eta, D, T_{\mathrm{ms}_j})$; 否则, 游戏终止.

若敌手 $\mathcal{A}_1$ 能够伪造合法的身份认证应答消息, 那么意味着 $\mathcal{C}$ 为敌手 $\mathcal{A}_1$ 提供了正确的参数 M'_{j^*}, 其中 $M'_{j^*} = (x_{j^*} + y_{j^*})\,B$, 那么 $\mathcal{C}$ 输出 $\alpha\beta P = M'_{j^*} - y_{j^*}B$ 作为 CDH 问题的解 (y_{j^*} 是已掌握的随机数).

为评估敌手 $\mathcal{C}$ 在上述游戏中获胜的优势, 定义事件 E_1 表示游戏在模拟过程中未终止; E_2 表示敌手 $\mathcal{A}_1$ 伪造了关于挑战身份的身份认证应答; E_3 表示 $(\pi_j, \eta, D, T_{\mathrm{ms}_j})$ 为合法的身份认证应答消息. 因此有 $\Pr(E_1) = (1 - \frac{1}{q_1+q_2+q_3+1})^{q_1+q_2+q_3}$, $\Pr(E_2) = \frac{1}{q_1+q_2+q_3+1}$ 和 $\Pr(E_3) \geqslant \varepsilon_2$. 那么有 $\varepsilon'_2 = \Pr(E_1 \wedge E_2 \wedge E_3) \geqslant \frac{\varepsilon_2}{\mathrm{e}(q_1+q_2+q_3+1)}$.

综上所述, 若存在概率多项式时间敌手 $\mathcal{A}_1$ 能以不可忽略优势 ε_2 假冒边缘服务器生成合法的身份认证应答消息, 那么能够构造一个敌手 $\mathcal{C}$ 能以显而易见的优势 $\varepsilon'_2 \geqslant \frac{\varepsilon_2}{\mathrm{e}(q_1+q_2+q_3+1)}$ 解决 CDH 问题.

定理3 若敌手 $\mathcal{A}_1$ 能够以不可忽略的优势 ε_3 在会话密钥安全性游戏中获胜, 那么存在敌手 $\mathcal{C}$ 能以不可忽略的优势 $\varepsilon'_3 \geqslant \frac{\varepsilon_3}{\mathrm{e}q_3(q_3-1)}$ 解决 CDH 问题, 其中 $\mathcal{A}_1$ 最多进行 q_1 次部分私钥生成询问, q_2 次私钥生成询问, q_3 次 Send 询问.

证明 敌手 $\mathcal{C}$ 从 CDH 困难问题的挑战者处获得相应的公开参数 (q, P, G) 和挑战元组 $(P, \alpha P, \beta P)$, 运行初始化算法后发送公开参数 $\mathrm{params} = \langle q, P, G, P_{\mathrm{pub}}, H_1, H_2, H_3, H_4, H_5, H_6, H_7\rangle$ 给 $\mathcal{A}_1$, 并秘密保存主私钥, 其中 H_2, H_3, H_4, H_5, H_6 和 H_7 分别为安全的单向哈希函数, H_1 是随机谕言机. 此外, $\mathcal{C}$ 维护初始化为空的列表 $L_{\mathrm{pk}}, L_{\mathrm{sk}}, L_d$ 分别用于跟踪 $\mathcal{A}_1$ 所提交的公钥生成、私钥生成和部分私钥生成等询问, 并用列表 L_s 记录 $\mathcal{A}_1$ 所提交的身份认证请求信息. $\mathcal{C}$ 随机选取 ID_{i^*} 和 ID_{j^*} 作为挑战身份.

(1) 部分私钥生成询问、私钥生成询问、公钥生成询问和公钥替换操作与定理 1 类似, 为避免重复此处不再赘述.

(2) Send 询问. 在这场游戏中, $\mathcal{A}_1$ 可发送下述 3 种类型的 Send 询问.

(i) Send($\prod_{i,j}^{k}$, start). 若 $\mathrm{ID}_i = \mathrm{ID}_{i^*}$, 令 $A = \alpha P$; 否则随机选取 $a' \leftarrow Z_q^*$, 并计算 $A = a'P$; 然后 $\mathcal{C}$ 通过私钥生成询问获取 ID_i 的私钥 (x_i, y_i), 再根据协议描述计算 $(B, C, W, \tau, \sigma, T_u)$ 后返回给 $\mathcal{A}_1$, 并更新 L_s.

(ii) Send($\prod_{j,i}^{k}, (B, C, W, \tau, \sigma, T_u)$). 若 $\mathrm{ID}_j = \mathrm{ID}_{j^*}$, 令 $D = \beta P$; 否则随机选取 $d \in Z_q^*$, 并计算 $D = dP$. 如果 $\mathrm{ID}_i \neq \mathrm{ID}_{i^*}$ 且 $\mathrm{ID}_j \in L_{\mathrm{sk}}$, $\mathcal{C}$ 从相应的列表中获得相应的私钥; 否则以 ID_j 为输入通过私钥生成询问获取私钥. 然后计算 $M'_j = (x_j + y_j)\,B$ 和 $\lambda_j = H_2(\mathrm{ID}_j||M_j)$, 构建多项式 $\varphi(x) = w_0 + w_1 x + \cdots + w_{n-1}x^{n-1} \bmod q$, 并计算 $r_j = \varphi(\lambda_j)$, $\pi_j = H_3(r_j)$ 和 $k_j = H_7(r_j) \oplus L_j$, 运行对称的解密算法 $\mathcal{D}_{k_j}(C)$ 得到信息 $(\mathrm{ID}_i||A||R_i||X_i)$. 验证等式 $\sigma P = v\,(A + R_i + H_i P_{\mathrm{pub}}) + X_i$ 是否成立 (其中 $v = H_4(\mathrm{ID}_u||A||R_u||T_u)$), 若不成立, 则终止此次会话; 否则 $\mathcal{C}$ 按照协议描述计算 $(\pi_j, \eta, D, T_{\mathrm{ms}_j})$ 返回给 $\mathcal{A}_1$, 并更新 L_s.

(iii) Send($\prod_{i,j}^{k}, (\pi_j, \eta, D, T_{\mathrm{ms}_j})$). 如果 ID_i 的信息可以在列表 L_s 中检索到, 则以 π_j 为索引找到对应的 ID_j, 若等式 $\eta = H_5(\mathrm{ID}_i||\mathrm{ID}_j||A||D||T_{\mathrm{ms}_j})$ 成立, 则认证成功; 否则认证失败, 并终止会话.

(3) Reveal($\prod_{i,j}^{k}$). 若 L_s 中存在 $\prod_{i,j}^{k}$ 对应的元组, 则接受会话, 并返回 sek, 否则返回 $\perp$.

(4) Test($\prod_{i,j}^{t}$). 若 $\mathrm{ID}_i = \mathrm{ID}_{i^*}$ 且 $\mathrm{ID}_j = \mathrm{ID}_{j^*}$, 且 $\mathcal{A}_1$ 输出的猜测 b' 满足 $b' = b$, 那么 $\mathcal{C}$ 输出 $\alpha\beta P = (\theta - y_{i^*}D)\,\eta^{-1}$ (其中 $\theta = (\eta a + y_{i^*})\,\beta P$) 作为 CDH 问题的解; 否则游戏终止.

定义事件 E_1 表示上述游戏中敌手 $\mathcal{A}_1$ 进行部分私钥生成和私钥生成等询问时游戏未终止; E_2 表示进行 Send 询问时游戏未终止; E_3 表示 $\mathcal{A}_1$ 进行 Test 询问时游戏未终止. 因此有 $\Pr(E_1) = (1 - \frac{1}{q_1+q_2+1})^{q_1+q_2}$, $\Pr(E_2) \geqslant \varepsilon_3$ 和 $\Pr(E_3) = \frac{1}{q_3(q_3-1)}$. 那么有 $\varepsilon_3' = \Pr(E_1 \wedge E_2 \wedge E_3) \geqslant \frac{\varepsilon_3}{\mathrm{e}q_3(q_3-1)}$.

综上所述, 若存在概率多项式时间敌手 $\mathcal{A}_1$ 能以不可忽略的优势 ε_3 在会话密钥安全性游戏中获胜, 则可构建敌手 $\mathcal{C}$ 能以显而易见的优势 $\varepsilon_3' \geqslant \frac{\varepsilon_3}{\mathrm{e}q_3(q_3-1)}$ 解决 CDH 问题.

定理4 若存在概率多项式时间敌手 $\mathcal{A}_2$ 能以不可忽略的优势假冒边缘节点并伪造合法的身份请求消息, 那么存在敌手能够以显而易见的优势解决 DL 问题, 其中 $\mathcal{A}_2$ 最多进行 q_1 次部分私钥生成询问, q_2 次私钥生成询问, q_3 次 Send 询问和 q_h' 次 H_4 谕言机询问.

证明 敌手 $\mathcal{C}$ 从 DL 困难问题的挑战者处获得相应的公开参数 (q, P, G) 和挑战元组 $(P, \omega P)$, 运行初始化算法生成相应的公开参数和主私钥, 并发送公开参数 $\mathrm{params} = \langle q, P, G, P_{\mathrm{pub}}, H_1, H_2, H_3, H_4, H_5, H_6, H_7\rangle$ 和主密钥给 $\mathcal{A}_2$, 其中 H_1, H_2, H_3, H_5, H_6 和 H_7 分别为安全的单向哈希函数, H_4 是随机谕言机. 此外, $\mathcal{C}$ 维持 4 个初始为空的列表 $L_{H_4}, L_{\mathrm{pk}}, L_{\mathrm{sk}}$ 分别用于跟踪所提交的 H_4 谕言机、公钥生成、私钥生成和部分私钥生成等询问; 并用列表 L_s 记录 $\mathcal{A}_2$ 所提交的身份认证请求信息. $\mathcal{C}$ 随机选取询问身份 ID_{i^*} 作为挑战身份.

(1) H_4 询问. 该询问的输入是 $(\mathrm{ID}_i, A, R_i, T_i)$. 若 $(\mathrm{ID}_i, A, R_i, T_i, H_i') \in L_{H_4}$, 则 $\mathcal{C}$ 返回 H_i' 给 $\mathcal{A}_2$; 否则, $\mathcal{C}$ 在 H_4 的值域中随机选取 H_i', 并返回 H_i', 然后将元组 $(\mathrm{ID}_i, A, R_i, T_i, H_i')$ 添加到列表 L_{H_4}.

(2) 私钥生成询问. 该询问的输入是 ID_i. 若 $(\mathrm{ID}_i, x_i, y_i) \in L_{\mathrm{sk}}$, $\mathcal{C}$ 返回 (x_i, y_i) 给 $\mathcal{A}_2$; 否则, $\mathcal{C}$ 进行下述操作: 若 $\mathrm{ID}_i = \mathrm{ID}_{i^*}$, 则 $\mathcal{C}$ 终止游戏; 否则, $\mathcal{C}$ 随机选取 $x_i, r_i \in Z_q^*$, 并计算 $X_i = x_i P$, $R_i = r_i P$ 和 $y_i = r_i + sH_1(\mathrm{ID}_i||R_i||X_i)$, 返回 (x_i, y_i), 并将元组 $(\mathrm{ID}_i, x_i, y_i)$ 和 $(\mathrm{ID}_i, X_i, R_i)$ 分别添加到列表 L_{sk} 和 L_{pk}.

(3) 公钥生成询问. 该询问的输入是 ID_i. 若 $(\mathrm{ID}_i, X_i, R_i) \in L_{\mathrm{pk}}$, 则 $\mathcal{C}$ 返回 (X_i, R_i) 给 $\mathcal{A}_2$; 否则, $\mathcal{C}$ 进行下述操作: 若 $\mathrm{ID}_i = \mathrm{ID}_{i^*}$, $\mathcal{C}$ 随机选取 $x_{i^*} \in Z_q^*$, 计算 $X_{i^*} = x_{i^*}P$, 令 $R_{i^*} = Q$ (隐含地设置相应的秘密值为 $r_{i^*} = \omega$), 返回 (X_i, R_i) 给 $\mathcal{A}_2$, 并将 $(\mathrm{ID}_{i^*}, X_{i^*}, R_{i^*})$ 和 $(\mathrm{ID}_{i^*}, x_{i^*}, \perp)$ 分别添加到 L_{pk} 和 L_{sk}; 否则, $\mathcal{C}$ 随机选取 $x_i, r_i \in Z_q^*$, 并计算 $X_i = x_i P$, $R_i = r_i P$ 和 $y_i = r_i + sH_1(\mathrm{ID}_i||R_i||X_i)$, 返回 (X_i, R_i) 给 $\mathcal{A}_2$, 并将 $(\mathrm{ID}_i, x_i, y_i)$ 和 $(\mathrm{ID}_i, X_i, R_i)$ 分别添加到 L_{sk} 和 L_{pk}.

(4) Send 询问. 在这场游戏中, $\mathcal{A}_2$ 可发送下述 3 种类型的 Send 询问.

(i) Send($\prod_{i,j}^{k}$, start). 如果 $\mathrm{ID}_i = \mathrm{ID}_{i^*}$, 则游戏终止; 否则执行以下操作: 如果 $\mathrm{ID}_i \notin L_{\mathrm{sk}}$, $\mathcal{C}$ 通过私钥生成询问获取 ID_i 的私钥 (x_i, y_i); 否则, $\mathcal{C}$ 从相应的列表 L_{sk} 中获得 ID_i 的私钥 (x_i, y_i). 然后根据协议执行过程计算 $(B, C, W, \tau, \sigma, T_u)$, 并将其返回给 $\mathcal{A}_2$, 同时更新 L_s.

(ii) Send($\prod_{j,i}^{k}$, $(B, C, W, \tau, \sigma, T_u)$). 如果 $\mathrm{ID}_j \in L_{\mathrm{sk}}$, $\mathcal{C}$ 相应的列表中获知 ID_j 的私钥; 否则以 ID_j 为输入进行私钥生成询问. 然后计算 $M_j = (x_j + y_j)\,B$ 和 $\lambda_j = H_2(\mathrm{ID}_j||M_j)$, 构建多项式 $\varphi(x) = w_0 + w_1 x + \cdots + w_{n-1}x^{n-1} \bmod q$, 并计算 $r_j = \varphi(\lambda_j)$, $\pi_j = H_3(r_j)$ 和 $k_j = H_7(r_j) \oplus L_j$, 通过运行对称的解密算法 $\mathcal{D}_{k_j}(C)$ 获知相应的交互信息 $(\mathrm{ID}_i||A||R_i||X_i)$. 若等式 $\sigma P = v(A + R_i + H_i P_{\mathrm{pub}}) + X_i$ 不成立, 则游戏终止; 否则, 当 $\mathrm{ID}_i \neq \mathrm{ID}_{i^*}$ 时, $\mathcal{C}$ 按照协议描述计算 $\left(\pi_j, \eta, D, T_{\mathrm{ms}_j}\right)$ 返回给 $\mathcal{A}_2$; 若 $\mathrm{ID}_i = \mathrm{ID}_{i^*}$, 那么 $\mathcal{A}_2$ 伪造了合法的身份认证请求消息 $(B, C, W, \tau, \sigma, T_u)$.

(iii) Send($\prod_{i,j}^{k}$, $(\pi_j, \eta, D, T_{\mathrm{ms}_j})$). 如果 ID_i 的信息可以在 L_s 中检索到, 则以 π_j 为索引找到对应的

ID_j, 若等式 $\sigma' P = v'\left(A + R_j + H_j P_{\mathrm{pub}}\right) + X_j$, 则认证成功; 若不成立, 终止会话.

假设敌手 $\mathcal{A}_2$ 成功伪造了合法的验证请求消息 $(B, C, W, \tau, \sigma, T_i)$, 由于 $\mathcal{C}$ 无法利用一条成功伪造的合法性验证请求消息解决 DL 困难问题. 基于分叉引理, $\mathcal{C}$ 基于重放的方式, 通过更改谕言机 H_4 的应答结果, 使得 $\mathcal{A}_2$ 基于相同的随机数 a 和不同谕言机 H_4 应答结果 H_4' 再次生成合法的身份认证请求消息 $(B, C, W, \tau, \tilde{\sigma}, T'_i)$, 那么 $\mathcal{C}$ 可以得到 $\sigma = H_4\left(a + \omega + H_{i^*} s\right) + x_{i^*}$ 和 $\tilde{\sigma} = H_4'\left(a + \omega + H_{i^*} s\right) + x_{i^*}$, 两式相减得到 $\sigma - \tilde{\sigma} = \left(a + \omega + H_{i^*} s\right)\left(H_4 - H_4'\right)$, 那么输出 DL 问题的解 $\omega = \frac{\sigma - \tilde{\sigma}}{H_4 - H_4'} - a - H_{i^*} s$.

为评估 $\mathcal{C}$ 在上述游戏中获胜的优势, 定义事件 E_1 表示上述模拟游戏未终止; E_2 表示伪造了关于挑战身份的认证请求消息; E_3 表示敌手生成了两个合法的身份认证请求消息 $(B, C, W, \tau, \sigma, T_i)$ 和 $(B, C, W, \tau, \tilde{\sigma}, T_i')$. 因此有 $\Pr\left(E_1\right) \geqslant \left(1 - \frac{1}{q_2 + q_3 + 1}\right)^{q_2 + q_3}$ 和 $\Pr\left(E_2\right) = \frac{1}{q_2 + q_3 + 1}$; 此外, 根据分叉引理可知 $\Pr\left(E_3\right) \geqslant \left(1 - \frac{1}{\mathrm{e}}\right)\frac{\varepsilon_4}{q_h'}$. 那么有 $\varepsilon_4' = \Pr\left(E_1 \wedge E_2 \wedge E_3\right) \geqslant \left(1 - \frac{1}{\mathrm{e}}\right)\frac{\varepsilon_4}{q_h' \mathrm{e}(q_2 + q_3 + 1)}$.

综上所述, 若存在概率多项式时间敌手 $\mathcal{A}_2$ 能以不可忽略优势假冒边缘节点生成有效的身份合法性验证请求消息, 那么存在敌手 $\mathcal{C}$ 能以显而易见的优势 $\varepsilon_4 \geqslant \left(1 - \frac{1}{\mathrm{e}}\right)\frac{\varepsilon_4}{q_h' \mathrm{e}(q_2 + q_3 + 1)}$ 解决 DL 问题.

定理5 若存在概率多项式时间敌手 $\mathcal{A}_2$ 能够以不可忽略的优势假冒边缘服务器并伪造合法的身份认证应答消息, 那么存在敌手 $\mathcal{C}$ 能以显而易见的优势解决 CDH 问题.

定理6 若存在概率多项式时间敌手 $\mathcal{A}_2$ 能以不可忽略的优势在会话密钥安全性游戏中获胜, 那么存在敌手 $\mathcal{C}$ 能以显而易见的优势解决 CDH 问题.

定理 2 和 3 的证明中敌手 $\mathcal{C}$ 具备为敌手提供完整主私钥的能力, 因此可以使用与定理 2 和 3 相类似的方法证明定理 5 和 6, 为避免重复本文不再赘述.

4.5 形式化分析

本文除对认证消息的不可伪造性和会话密钥的安全性进行形式化证明之外, 还利用安全性模拟工具 ProVerif 对本文协议的安全性进行了模拟仿真, 验证了协议所具有的安全属性. 为了便于理解, 本文模拟了边缘节点与两个边缘服务器的认证场景. 如图 2 所示, ProVerif 的模拟仿真结果表明本文协议可顺利执行, 协议参与者获得了相同的会话密钥, 且在协议交互过程中会话密钥不被攻击者获得, 模拟结果进一步表明本文协议具有相应的安全性. 本文已将仿真源代码上传至 github[1)].

4.6 性能分析

本小节对本文协议性能进行仿真分析. 实验电脑的配置为: Ubuntu 20.04 (64 bits) 操作系统, Intel Core i5-6300U-2.30 GHz, 8 GB 内存. 此外, 相应的参数选择为: p, q 均为 256 bit, G, Z_q 分别为 512 和 256 bit. 为了方便对比相应协议的计算成本, 本文定义 T_{bp} 为双线性映射的运算时间; T_m 为群上的乘法运算的时间; T_a 为群上加法运算的时间; T_h 为计算哈希函数的时间; T_e 为模指数运算的时间; T_{mm} 为模乘运算的时间. 上述操作的具体运算时间如表 1 所示.

表 2 给出了本文协议与现有相关身份认证协议 [11,12,16,17] 具体计算开销的对比结果, n 代表同时认证的边缘服务器数量. 服务器端的总计算开销等于单台服务器开销的倍, 因此表 2 只需考虑单台服务器的计算开销即可. 对于服务器端的计算开销, 文献 [17] 的计算成本最大, 是 27.84 ms; 文献 [11, 12, 16] 的计算成本分别为 22.8, 19.84 和 20.94 ms; 本文协议在服务器端的计算成本最低, 为 17.66 ms. 而用户端的计算开销会受到参与身份认证的服务器数量 n 的影响. 当 n 分别为 1, 2, 5, 10 和 20 时, 文献 [11,12,16,17] 和本文协议用户端和服务器端计算开销的变化情况如图 3(a) 和 (b) 所示, 其中当 $n = 1$ 时本文协议的用户端计算开销并不是最优的, 但随着同时认证服务器数量的增加, 本文

1) https://github.com/XuYuan615/Formal-Security-Validation-2.

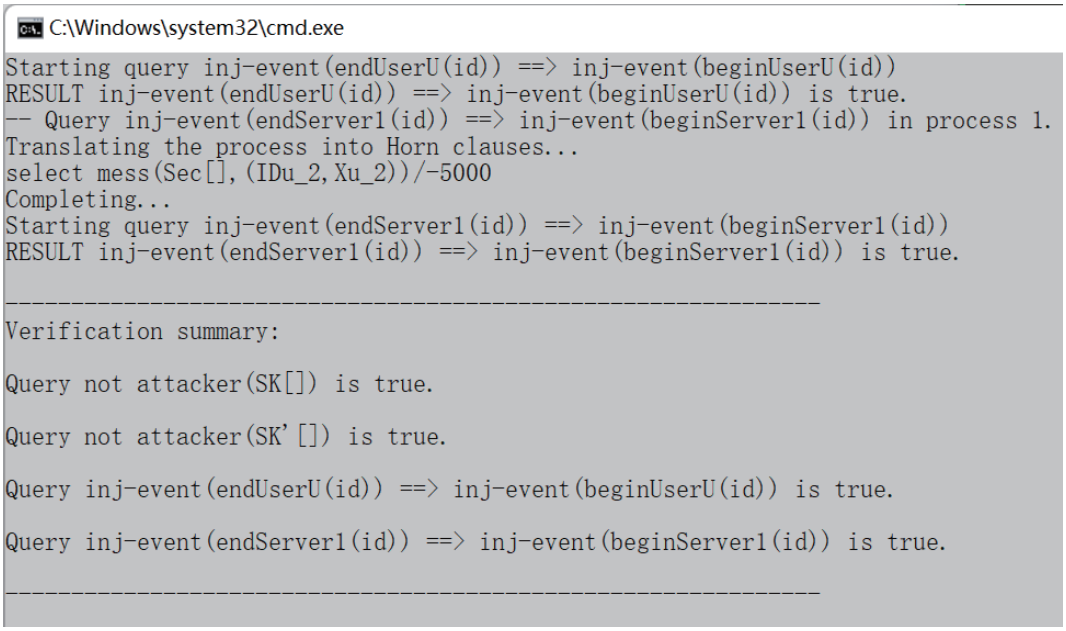

图 2　ProVerif 的模拟仿真结果

Figure 2　Simulation results of ProVerif

表 1　协议中基本操作的运算时间 (ms)

Table 1　Running time of basic opeartions (ms)

Operation	Running time	Operation	Running time	Operation	Running time
T_{bp}	8.08	T_a	0.017	T_e	0.534
T_m	2.92	T_h	0.014	T_{mm}	0.01

表 2　计算成本比较 (ms)

Table 2　Comparison of computational cost (ms)

Scheme	User's computational cost	Server's computational cost
[11]	$4nT_m + nT_e + nT_a + 5nT_h$	$1T_{\mathrm{bp}} + 5T_m + 3T_a + 5T_h$
[12]	$6nT_m + 4nT_a + 5nT_h$	$1T_{\mathrm{bp}} + 4T_m + 3T_a + 2T_h$
[16]	$nT_{\mathrm{bp}} + 2nT_m + 2nT_e + 8nT_h$	$1T_{\mathrm{bp}} + 2T_m + 2T_e + 8T_h$
[17]	$nT_{\mathrm{bp}} + 3nT_m$	$2T_{\mathrm{bp}} + 4T_m$
Our scheme	$(3n+2)\,T_m + 1T_e + 2nT_a + \frac{5n^2-n}{2}T_{\mathrm{mm}} + (6n+1)\,T_h$	$6T_m + 3T_a + 7T_h$

协议用户端和服务器端计算开销的增长速率最慢, 由此可见本文协议更适合部署在边缘节点与众多边缘服务器同时进行认证的环境. 因此, 相较于现有构造 [11,12,16,17], 本文协议具有更优的计算效率, 更适合在移动边缘计算等终端计算资源受限的网络环境下使用.

5　结论

本文针对移动边缘计算中边缘节点的移动性特点, 面向用户对网络服务的持续性需求, 提出了一

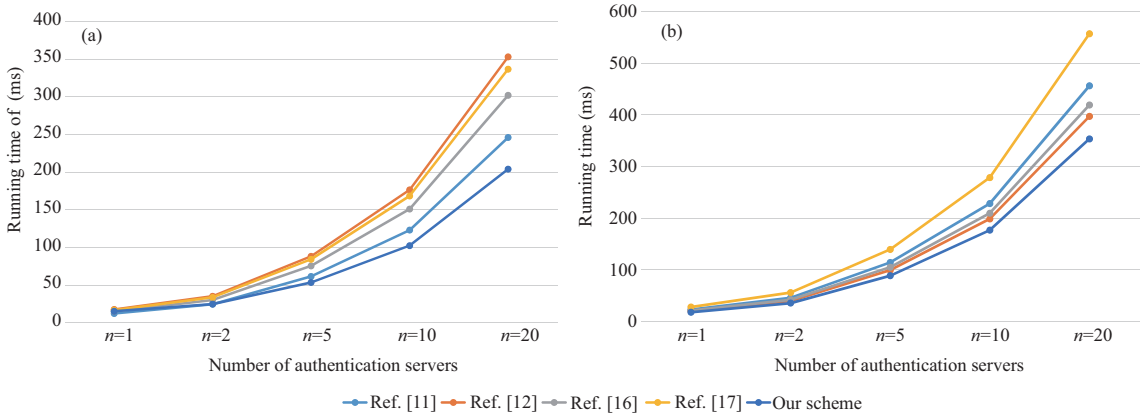

图 3　(网络版彩图) 认证协议中 (a) 用户端和 (b) 服务器端计算成本的比较

Figure 3　(Color online) Comparison of computing cost on (a) the user side and (b) the server side

个广播身份认证协议. 该协议基于无证书密码体制解决了密钥托管的不足, 同时利用广播通信的方式解决了边缘节点在不同服务器间切换时需迁移身份信息和重复认证的问题, 本文协议未使用耗时较高的双线性映射操作, 减少了计算开销. 此外, 基于 DL 问题和 CDH 问题的困难性, 证明了本文协议的安全性, 同时对协议所具有的相互认证、匿名性、前后向安全性和抗重放攻击等安全属性进行了详细分析. 同时, 仿真结果表明与现有的身份认证协议相比, 本文协议在与多个服务器进行身份合法性认证时具有更高的计算效率.

边信道、冷启动等泄露攻击方式的出现, 使得传统安全模型下被证明安全的密码机制由于泄露的存在而不再保持其所声称的安全性, 因此需在密码原语抗泄露性研究 [34, 35] 的基础上, 进一步研究身份认证协议的泄露容忍性及电子医疗 [36] 等新兴应用系统环境下身份认证协议的设计.

参考文献

1　Mao Y, You C, Zhang J, et al. A survey on mobile edge computing: the communication perspective. IEEE Commun Surv Tut, 2017, 19: 2322–2358

2　Barbarossa S, Sardellitti S, Di Lorenzo P. Communicating while computing: distributed mobile cloud computing over 5G heterogeneous networks. IEEE Signal Process Mag, 2014, 31: 45–55

3　Shi W S, Sun H, Cao J, et al. Edge computing — an emerging computing model for the internet of everything era. J Comput Res Develop, 2017, 54: 907–924 [施巍松, 孙辉, 曹杰, 等. 边缘计算: 万物互联时代新型计算模型. 计算机研究与发展, 2017, 54: 907–924]

4　Zhang K Y, Gui X L, Ren D W, et al. Survey on computation offloading and content caching in mobile edge networks. J Softw, 2019, 30: 2491–2516 [张开元, 桂小林, 任德旺, 等. 移动边缘网络中计算迁移与内容缓存研究综述. 软件学报, 2019, 30: 2491–2516]

5　Tran T X, Hajisami A, Pandey P, et al. Collaborative mobile edge computing in 5G networks: new paradigms, scenarios, and challenges. IEEE Commun Mag, 2017, 55: 54–61

6　Qu Y B, Qin Z, Ma J H, et al. Service provisioning for air-ground collaborative mobile edge computing. J Comput, 2022, 45: 781–797 [屈毓锛, 秦蓁, 马靖豪, 等. 面向空地协同移动边缘计算的服务布置策略. 计算机学报, 2022, 45: 781–797]

7　Wang D, Li W, Wang P. Measuring two-factor authentication schemes for real-time data access in industrial wireless sensor networks. IEEE Trans Ind Inf, 2018, 14: 4081–4092

8　Zhao J J, Gu D W. Provably secure two-party authenticated key exchange protocol in eCK model. Chin J Comput, 2011, 34: 47–54 [赵建杰, 谷大武. eCK 模型下可证明安全的双方认证密钥协商协议. 计算机学报, 2011, 34: 47–54]

9 Esfahani A, Mantas G, Matischek R, et al. A lightweight authentication mechanism for M2M communications in industrial IoT environment. IEEE Int Things J, 2019, 6: 288–296

10 Kaur K, Garg S, Kaddoum G, et al. A lightweight and privacy-preserving authentication protocol for mobile edge computing. In: Proceedings of IEEE Global Communications Conference (GLOBECOM), Waikoloa, 2019. 1–6

11 Jia X, He D, Kumar N, et al. A provably secure and efficient identity-based anonymous authentication scheme for mobile edge computing. IEEE Syst J, 2019, 14: 560–571

12 Li Y, Cheng Q, Liu X, et al. A secure anonymous identity-based scheme in new authentication architecture for mobile edge computing. IEEE Syst J, 2020, 15: 935–946

13 Jia X, Luo M, Choo K K R, et al. A redesigned identity-based anonymous authentication scheme for mobile-edge computing. IEEE Int Things J, 2022, 9: 10108–10120

14 Cui Z H, Xue F, Zhang S Q, et al. A hybrid blockchain-based identity authentication scheme for multi-WSN. IEEE T Serv Comput, 2020, 13: 241–251

15 Kumar M, Chand S. A lightweight cloud-assisted identity-based anonymous authentication and key agreement protocol for secure wireless body area network. IEEE Syst J, 2020, 15: 2779–2786

16 Xiong L, Peng D Y, Peng T, et al. An enhanced privacy-aware authentication scheme for distributed mobile cloud computing services. KSII Trans Int Inform Syst, 2017, 11: 6169–6187

17 Chaudhry S A, Kim I L, Rho S, et al. An improved anonymous authentication scheme for distributed mobile cloud computing services. Cluster Comput, 2019, 22: 1595–1609

18 Liu J, Zhang Z, Chen X, et al. Certificateless remote anonymous authentication schemes for wirelessbody area networks. IEEE Trans Parall Distrib Syst, 2013, 25: 332–342

19 Cheng G, Chen Y, Deng S, et al. A blockchain-based mutual authentication scheme for collaborative edge computing. IEEE Trans Comput Soc Syst, 2021, 9: 146–158

20 Peng C, Chen J, Obaidat M S, et al. Efficient and provably secure multireceiver signcryption scheme for multicast communication in edge computing. IEEE Int Things J, 2020, 7: 6056–6068

21 Zhu J, Chen L L, Zhu X, et al. A new efficient certificateless multi-receiver public key encryption scheme. Int J Comput Sci Issues, 2016, 13: 1–7

22 He D, Wang H, Wang L, et al. Efficient certificateless anonymous multi-receiver encryption scheme for mobile devices. Soft Comput, 2017, 21: 6801–6810

23 Xiong H. Cost-effective scalable and anonymous certificateless remote authentication protocol. IEEE Trans Inform Forensic Secur, 2014, 9: 2327–2339

24 Zhang S, Fan H L, Zhong H. Efficient revocable certificateless remote anonymous authentication protocol for wireless body area network. J Commun, 2018,39: 100–111 [张顺, 范鸿丽, 仲红, 等. 无线体域网中高效可撤销的无证书远程匿名认证协议. 通信学报, 2018, 39: 100–111]

25 Liu J W, Zhang Z H, Sun R, et al. An efficient certificateless remote anonymous authentication scheme for wireless body area networks. In: Proceedings of IEEE International Conference on Communications (ICC), 2012. 3404–3408

26 Mishra D, Dharminder D, Yadav P, et al. A provably secure dynamic ID-based authenticated key agreement framework for mobile edge computing without a trusted party. J Inf Security Appl, 2020, 55: 102648

27 Li J, Yu Q, Zhang Y. Identity-based broadcast encryption with continuous leakage resilience. Inf Sci, 2018, 429: 177–193

28 Li J, Chen Y, Han J, et al. Decentralized attribute-based server-aid signature in the Internet of Things. IEEE Int Things J, 2022, 9: 4573–4583

29 Qiao Z, Yang Q, Zhou Y, et al. Improved secure transaction scheme with certificateless cryptographic primitives for IoT-based mobile payments. IEEE Syst J, 2022, 16: 1842–1850

30 Pointcheval D, Stern J. Security proofs for signature schemes. Lect Notes Comput Sci, 1996, 1070: 387–398

31 Yang B. Modern Cryptography. 4th ed. Beijing: Tsinghua University Press, 2015 [杨波. 现代密码学 (第四版). 北京: 清华大学出版社, 2015]

32 Qiao Z, Zhou Y, Yang B, et al. Secure and efficient certificate-based proxy signature schemes for industrial Internet of Things. IEEE Syst J, 2022, 16: 4719–4730

33 Qiao Z, Yang Q, Zhou Y, et al. An efficient certificate-based aggregate signature scheme with provable security for industrial Internet of Things. IEEE Syst J, 2023, 17: 72–82

34 Zhou Y, Cao L, Yang B, et al. A direct construction of continuous leakage-resilient (H)IBE scheme with CCA security from dual system encryption. Comput Stand Interfaces, 2023, 83: 103668
35 Zhou Y, Xu R, Zhang W, et al. Public-key encryption scheme with optimal continuous leakage resilience. Inf Process Lett, 2023, 180: 106318
36 Zhang M, Chen Y, Susilo W. Decision tree evaluation on sensitive datasets for secure e-healthcare systems. IEEE Trans Depend Sec Comput, 2022, doi: 10.1109/TDSC.2022.3219849

Broadcast identity authentication scheme for mobile edge computing

Yanwei ZHOU[1,2,3], Yuan XU[1], Bo YANG[1*], Chunxiang GU[3], Zhe XIA[4] & Mingwu ZHANG[5]

1. *School of Computer Science, Shaanxi Normal University, Xi'an* 710062*, China*;
2. *State Key Laboratory of Cryptology, Beijing* 100878*, China*;
3. *Henan Key Laboratory of Network Cryptography Technology, Zhengzhou* 450040*, China*;
4. *School of Computer Science and Technology, Wuhan University of Technology, Wuhan* 430070*, China*;
5. *School of Computer, Hubei University of Technology, Wuhan* 430068*, China*
* Corresponding author. E-mail: byang@snnu.edu.cn

Abstract With the rapid advancement of wireless communication technology, mobile edge computing (MEC) has garnered increasing attention from researchers. To ensure the security of mobile edge nodes, several identity authentication schemes have been proposed. However, these earlier methods primarily support one-to-one identity authentication. In this scenario, users must repeatedly undergo identity authentication to fulfill the migration requirements of mobile edge nodes across multiple servers. This traditional identity authentication approach results in low service efficiency and a subpar communication experience for users. Consequently, existing identity authentication schemes within MEC fail to meet the mobility demands of edge nodes. In this study, to address the aforementioned issues comprehensively, we propose an identity authentication scheme employing broadcast communication based on certificateless cryptography. This scheme achieves seamless migration service continuity for edge nodes across multiple servers. Furthermore, our proposal enables mutual authentication between a single user and multiple servers simultaneously, significantly enhancing the efficiency of identity authentication. Moreover, we provide formal proof of the unforgeability of the message and the security of session keys within the random oracle model, relying on the discrete logarithm problem and the computational Diffie-Hellman problem, respectively. Additionally, we utilize formal analysis tools, such as ProVerif, to simulate the security aspects of our proposal. When compared to existing schemes, our proposal exhibits superior computational efficiency, making it better suited for deployment in the context of MEC.

Keywords identity authentication, mobile edge computing, certificateless cryptography, provably security