中国科学: 信息科学 2022 年 第 52 卷 第 12 期: 2351–2370
SCIENTIA SINICA Informationis
论文

面向车联网的抗设备捕获认证密钥协商协议

姜奇[1,2*], 杨雪[1], 王金花[1], 程庆丰[2,3], 马鑫迪[1], 马建峰[1]

1. 西安电子科技大学网络与信息安全学院, 西安 710071
2. 河南省网络密码技术重点实验室, 郑州 450001
3. 战略支援部队信息工程大学网络空间安全学院, 郑州 450001
* 通信作者. E-mail: jiangqixdu@gmail.com

收稿日期: 2021–11–15; 修回日期: 2022–01–17; 接受日期: 2022–03–14; 网络出版日期: 2022–12–08

国家自然科学基金 (批准号: 62072352, 92167203, 62125205, 61872449, 61902290, 62072359)、陕西省教育厅科研计划项目 (批准号: 20JY016)、陕西省重点产业链项目 (批准号: 2020ZDLGY09-06) 和中央高校基本科研业务费资助项目

摘要 随着汽车保有量的持续增长和道路交通的饱和, 车联网被视为有效提高交通效率, 改善驾乘体验的有效技术之一. 认证密钥协商协议是保证车载单元 (onboard unit, OBU) 与各种信息服务器安全交互的关键手段. 通常, 认证密钥协商协议所需的密钥被存储于 OBU 中. 然而, 由于车辆常处于无人值守状态, OBU 失盗事件时有发生. 因此, 如何确保私钥的存储安全是一个具有挑战性的难题. 为了解决上述问题, 本文提出了基于不经意伪随机函数 (oblivious pseudorandom functions, OPRF) 和两方协同签名的抗捕获认证密钥协商协议. 借助于两方协同签名, 私钥被分成两个部分, 一部分使用辅助设备的公钥加密, 另一部分通过 OBU 和辅助设备运行 OPRF 协议才能恢复. 由于 OBU 中没有存储任何秘密信息, 即使 OBU 被盗取, 攻击者仍然无法获取私钥. 本文对提出的方案进行了全面的安全性分析和性能比较. 结果表明所提出的方案可以抵抗各种已知的攻击, 特别是设备被捕获导致的密钥泄露. 此外, 所提出的方案可以实现计算开销和通信开销的平衡.

关键词 车联网, Schnorr 协同签名, OPRF, 认证密钥协商, 抗设备捕获

1 引言

随着汽车保有量的持续增长和道路交通的饱和, 作为有效提高交通效率, 改善驾乘体验的关键技术之一, 车联网受到了各个国家企业和政府的广泛关注 [1]. 据调查显示, 2019 年全球车联网市场规模约为 5850 亿元, 我国车联网行业市场规模约为 1300 亿元, 并且在未来几年将会飞速增长. 然而, 随着车联网市场规模的高速发展, 车联网网络存在的漏洞和面临的攻击风险持续加剧, 车联网网络安全事件频发, 严重威胁用户的人身和财产安全 [2]. 根据 Upstream Security 发布的《2020 年汽车网络安全报

引用格式: 姜奇, 杨雪, 王金花, 等. 面向车联网的抗设备捕获认证密钥协商协议. 中国科学: 信息科学, 2022, 52: 2351–2370, doi: 10.1360/SSI-2021-0379
Jiang Q, Yang X, Wang J H, et al. Device capture resilient authentication and key agreement protocol for IoV (in Chinese). Sci Sin Inform, 2022, 52: 2351–2370, doi: 10.1360/SSI-2021-0379

© 2022《中国科学》杂志社

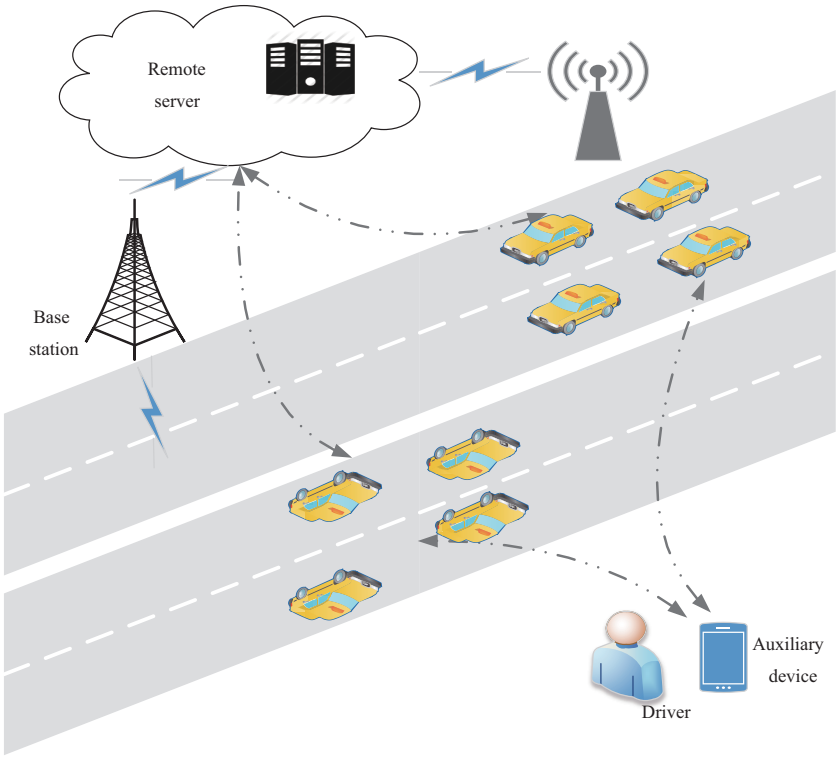

图 1　(网络版彩图) 车联网通信场景图

Figure 1　(Color online) The scenario of Internet of vehicles

告》显示, 自 2016 年以来, 每年的车联网网络安全事件数量增长了 60.5%, 仅 2019 年就增长了一倍以上 [3]. 因此, 车联网安全成为车联网发展面临的主要障碍之一, 引起了国内外的广泛关注.

典型的车联网通信场景如图 1 所示, 车联网主要通过传输实时交通信息、道路状况、预警信息等来改善交通流量, 减少交通事故 [4]. 由于信息是通过无线网络传输的, 因此车联网容易遭受各种恶意的攻击. 如果传输中的安全信息遭受到黑客的网络攻击, 驾驶员可能会做出错误的决定, 加剧道路拥堵, 甚至导致严重的交通事故. 此外, 在车辆行驶的过程中, 记录了很多的地理位置、路线等涉及个人隐私的信息, 如果被不法分子窃取, 将会导致很严重的隐私泄露问题 [5,6]. 因此, 为了确保车载单元与各种信息服务器间的交互消息是由合法实体发送的, 并且在传输过程中不会被篡改, 必须在车联网通信过程中实现身份认证, 确保消息的机密性和完整性. 国内外已经对车联网场景下的身份认证协议开展了研究, 提出了大量的认证密钥协商协议 [7~14].

私钥的安全性成为确保认证密钥协商协议安全运行的基础. 然而, 由于车辆常常放在无人看守的区域, 车载单元失盗事件时有发生 [15]. 因此攻击者可以获得存储有秘密数据的车载单元, 通过对车载单元发起边信道攻击提取存储在车辆上的秘密数据, 进而对系统的安全性造成威胁. 此外, 现有的大多数车联网场景下的认证密钥协商协议中, 未充分考虑私钥的安全存储, 大多假设密钥保存在抗篡改设备 (tamper proof device, TPD) 中, 而攻击者无法获取 TPD 中的密钥 [9,10]. 然而, 研究发现即使攻击者无法访问到 TPD 的内部, 攻击者仍可以通过发起边信道攻击来收集边信道信息, 进而计算出存储在 TPD 中的秘密数据 [16]. 因此, 确保设备捕获情形下设备中存储的秘密数据的安全性是一个具有挑战性的难题.

为了解决上述问题, 基于两方协同的密钥保护方案 [17,18] 被提出. 基于两方协同方案, Wu 等 [17] 提出了一种基于双设备的用户认证和密钥协商方案, 其中, 用户的私钥被分成两个部分, 分别存储在主设备和辅助设备中. 但是, 文献 [19] 指出该方案没有实现双因子安全, 当主设备被捕获时, 方案的安全性受到影响. 基于类似的方法, Feng 等 [18] 提出了基于两方计算的协同认证及密钥协商协议, 该方案将密钥分成两部分, 分别保存在主参与者和辅助参与者的设备中. 但是, 当主参与者的设备被捕获时, 攻击者仍可能在辅助参与者不知情的情况下与服务器实现双向认证, 即 Feng 等 [18] 的方案无法充分抵御设备捕获攻击.

不经意伪随机函数 (oblivious pseudorandom functions, OPRF) [20] 是一个两方的交互性协议, 其中发送方输入秘密值, 接收方存储 OPRF 密钥. 当协议执行完成后, 发送方可以计算 OPRF 值, 而接收方无法获取和秘密值有关的任何信息. OPRF 提供了一种检索高熵密钥的方法, 被广泛地应用于将口令和密钥相结合的场景 [21,22]. 结合 OPRF 支持 “安全的存储并恢复密钥” 的特点, 本文提出了面向车联网的基于两方协同签名和 OPRF 的认证密钥协商协议. 具体而言, 车辆的私钥被分成两个部分, 分别由车载单元和辅助设备拥有. 车载单元的密钥通过用户输入口令, 辅助设备存储 OPRF 密钥, 交互执行 OPRF 协议来恢复, 而无需存储在 TPD 中, 解决了车辆被捕获时密钥泄露的问题. 此外, 车载单元只有在辅助设备的帮助下, 才能实现车辆与服务器的认证和密钥协商. 即使车载单元和辅助设备均被盗取, 攻击者在不知道口令的情况下仍然无法计算车辆的密钥. 本文的贡献总结如下.

(1) 本文提出了一个面向车联网的基于 OPRF 和两方 Schnorr 协同签名的抗设备捕获的认证密钥协商协议. 具体来说, 在两方 Schnorr 签名中, 私钥被分为两部分, 分别由车载单元和辅助设备拥有, 只有在辅助设备的帮助下, 车载单元才可以与服务器实现双向认证和密钥协商. 任何一个设备被捕获甚至两个设备均被捕获, 都不会影响协议的安全性.

(2) 本文提出了一种基于 OPRF 的交互式密钥恢复方案. 车载单元的密钥只有在用户输入口令, 辅助设备输入 OPRF 密钥交互执行 OPRF 协议后才能恢复. 即使车载单元被攻击者捕获, 攻击者在不知道口令和 OPRF 密钥的情况下仍然无法恢复私钥.

(3) 本文对提出的方案进行了全面的安全性分析和性能比较. 结果表明所提出的方案可以抵抗各种已知的攻击, 特别是设备被捕获时的抗密钥泄露安全特性. 此外, 所提出的方案可以实现通信协议计算开销和通信开销的平衡.

本文的其余部分安排如下. 在第 2 节中回顾了面向车联网的认证协议的相关研究进展. 第 3 节简要回顾了使用到的基础知识. 第 4 节详细描述了提出的面向车联网的基于 OPRF 和两方 Schnorr 协同签名的认证密钥协商方案. 第 5 节对提出的方案进行可证明安全性分析. 第 6 节在安全性和性能方面对提出的方案和其他方案进行比较. 最后, 总结全文.

2 相关工作

2.1 车联网场景中的认证协议

在 2005 年, Raya 等 [23] 使用数字签名来实现对发送方的身份验证. 此外, 为了实现条件匿名性, 每个车辆的 TPD 都会保存大量的匿名公私钥对和密钥凭证. 然而在 2007 年, Lin 等 [24] 提出文献 [23] 中的方案效率低下, 存储开销大, 对车辆撤销的维护操作复杂. 为了解决存储开销问题, Lu 等 [25] 提出了高效的条件隐私保护方案, 其中车载单元不直接存储匿名凭证, 而是在每次通话前向路边单元发起生成短时匿名密钥凭证的请求. 但是, 方案 [25] 会导致巨大的计算开销. 此外, Wasef 等 [26] 提出使用

安全高效的带密钥的哈希函数替代证书撤销过程, 缓解证书撤销过程带来的延迟, 并使用概率密钥分发思想更新密钥. 但是该方案依旧使用抗篡改模块来存储秘密信息, 并且双线性配对和哈希链的引入导致了计算开销的增加.

上述方案中的一个共同缺陷是协议的计算开销很大, 为了弥补这个缺陷, 基于对称加密的认证协议 [27~30] 被提出. Rhim 等 [27] 提出了一种有效的基于消息认证码的消息认证方案. 但是, Taeho 等 [28] 发现方案 [27] 无法抵抗重放攻击并提出了基于带密钥的消息认证码的消息认证方案, 该方案使用路边信息单元辅助车辆进行消息认证以减少车辆的开销. 在 Vighnesh 等 [29] 的方案中, 研究人员利用由身份认证中心签名的哈希链和身份认证码对车辆进行身份认证. 但是, 它容易受到拒绝服务攻击. Li 等 [30] 提出了一种轻量级安全导航方案, 车辆首先与附近的路边信息单元启动导航服务, 请求共享对称密钥, 以便与其他路边信息单元进行进一步通信. 为了提高车联网通信的效率, 研究人员提出了基于身份的认证方案 [12,13,31]. Shaikh 和 Alzahrani [12] 提出了匿名身份的信任管理方案, 它可以防止车联网传播虚假的位置和时间信息. Sun 等 [31] 提出了基于门限认证的防御方案以区分故障和恶意行为. 该方案使用假名保护车辆的隐私, 使用保护秘密信息的门限签名恢复恶意车辆的身份. 之后, Shim 等 [13] 提出了一个条件隐私保护的认证方案, 通过基于伪身份标识符的签名实现安全通信. 但是, 它很容易遭到位置跟踪攻击.

此外, 研究人员提出了基于群签名的认证方案 [32~34], 其中群的任何成员都可以使用其私钥代表群来签名消息, 而不会泄露隐私. Guo 等 [32] 提出了一种基于群签名的认证方案, 该方案实现了不可链接性. 然而, 该方案也造成了巨大的通信开销和计算开销. 之后, 为了减少计算开销, Zhu 等 [33] 提出了一个通过使用群签名和哈希消息认证码来保护隐私的有效身份认证方案. 此外, Zhang 等 [34] 利用签密、群签名和批量验证技术来实现分布式认证方案, 该方案通过路边信息单元来连接一个群进而减少通信和计算开销. 但是, 他们的方法假定路边信息单元是完全受信任的.

上述的方案有一个共同的限制是密钥管理. 为了填补这个漏洞, 许多研究人员提出了在车载单元中嵌入 TPD 的认证方案 [9,10], 将车辆的私钥或者是可信权威的主密钥保存在 TPD 中, 使得攻击者无法获取 TPD 中的秘密信息. Wang 等 [9] 使用口令和生物特征的双因子认证方案认证驾驶员的身份, 利用去中心化的 CA 抵抗拒绝服务攻击和降低数据包丢失率, 降低执行证书更新和撤销的 CA 开销, 使用生物特征加密, 使用临时 MAC 地址保护隐私. Tsaur 等 [10] 提出了使用 TPD 的安全有效的驾驶员异常通知方案. 在该方案中, 使用口令、生物特征代替车载单元对司机进行身份认证, 然后使用签密技术和基于哈希链的公钥密码技术来提高计算效率, 增强方案的可伸缩性. Kiltz 等 [16] 提出了使用乘法秘密共享技术的抗泄露的椭圆曲线加密方案, 该方案需要在 TPD 中存储可信机构的主密钥. 但是, 这种具有抗泄露特性的方案无法抵抗对 TPD 的边信道攻击. 在实际应用中, 即使攻击者不能探测到 TPD 内部, 他也可能通过边信道攻击来收集大量信息.

2.2 具有密钥保护属性的认证协议

为了实现密钥保护, 研究人员提出了基于门限秘密共享的密钥保护方案 [35,36]. 但是, 上述方案在密钥恢复阶段要求重构密钥, 且由于参与方较多, 具有较高的通信时延, 这不满足车联网对通信时延的要求. 因此, 上述方案无法应用于车联网场景下的认证密钥协商协议. 为了解决上述问题, 基于两方协同密码的密钥保护方案 [17,18] 被提出. Wu 等 [17] 提出了一种基于双设备的带密钥保护的认证密钥协商方案. 用户的私钥被分成两个部分, 分别存储在主设备和辅助设备中. 两个设备交互执行协议协同生成认证消息, 进而实现用户和服务器的双向认证与密钥协商. 但是, 当主设备被捕获时, 攻击者可以通过与辅助设备发起通信进而获取秘密值, 在之后的通信中, 攻击者可以伪装成用户实现与服务器

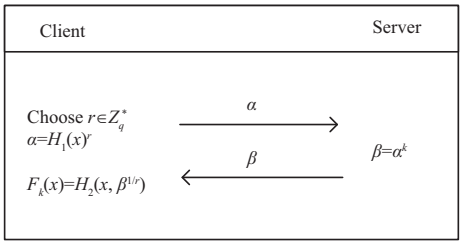

图 2 OPRF 协议实现图

Figure 2 OPRF protocol

的认证和密钥协商. 此外, 该方案采用了计算复杂的零知识证明 [37] 和 Paillier 同态密码系统 [38] 来保证交互过程中数据的完整性和保密性, 计算开销非常大, 这并不真正适用于车联网系统. 为了解决上述问题, Feng 等 [18] 提出了智能电子医疗记录系统中基于两方计算的认证密钥协商协议, 该方案将密钥分成两部分, 分别由医生和病人存储, 只有在两方的协同计算下才可以与服务器实现认证和密钥协商. 但是, 医生和病人的密钥以明文形式直接存储在设备中. 此外, 由于医生和病人的设备之间缺乏认证, 当医生的设备被捕获时, 攻击者在病人不知情的情况下与服务器实现双向认证和密钥协商, 即方案 [18] 无法抵抗设备捕获攻击.

研究人员提出了基于物理不可克隆函数 (physical unclonable function, PUF) 的认证协议 [39~41], 利用存储的挑战应答对 (challenge response pair, CRP) 实现, 具有易实现和低能耗的优点. 然而, 此类方法需特殊硬件设备支持, 增加了实现成本; 此外, 与生物特征类似, PUF 的应答存在随机噪声等问题, 影响其准确性, 对噪声的处理存在一定难度. 本文所提出的方案基于成熟的密码学算法, 可在通用设备上实现, 无需增加实现成本.

3 基础知识

本节将介绍 OPRF、传统的 Schnorr 签名等基础知识.

3.1 不经意伪随机函数

OPRF 是 Freedman 等 [20] 在 2005 年提出, 它提供了一种检索高熵密钥的独特方法. OPRF 是客户端和服务器之间的交互式协议, 其中, 服务器存储随机的 OPRF 密钥, 而客户端输入. 在协议运行结束时, 客户端将从伪随机函数函数簇中随机选择来计算并输出 OPRF 值, 而服务器无法获得和秘密值有关的信息. 具体的实现方式如图 2 所示.

3.2 Schnorr 签名

Schnorr 签名算法是由德国数学家、密码学家 Schnorr 提出 [41], 由于其在性能和可扩展性的优势, 被广泛地应用于认证和密钥协商协议中. 对消息 m 的签名算法主要包括以下 3 个步骤:

- 生成公私钥对.

(1) 选择素数 g, p 和 q, 使得 q 是 $p-1$ 的素因子且 $g^q = 1 \bmod p$, 其中 (g, p, q) 为公钥参数;

(2) 选择随机整数 x $(0 < x < q)$, 作为用户的私钥, 计算 $X = g^{-x} \bmod p$ 作为用户的公钥.

- 数字签名过程.

(1) 选择随机整数 r $(0 < r < q)$, 并计算 $R = g^r \bmod p$, 该过程和待签名消息 m 无关;

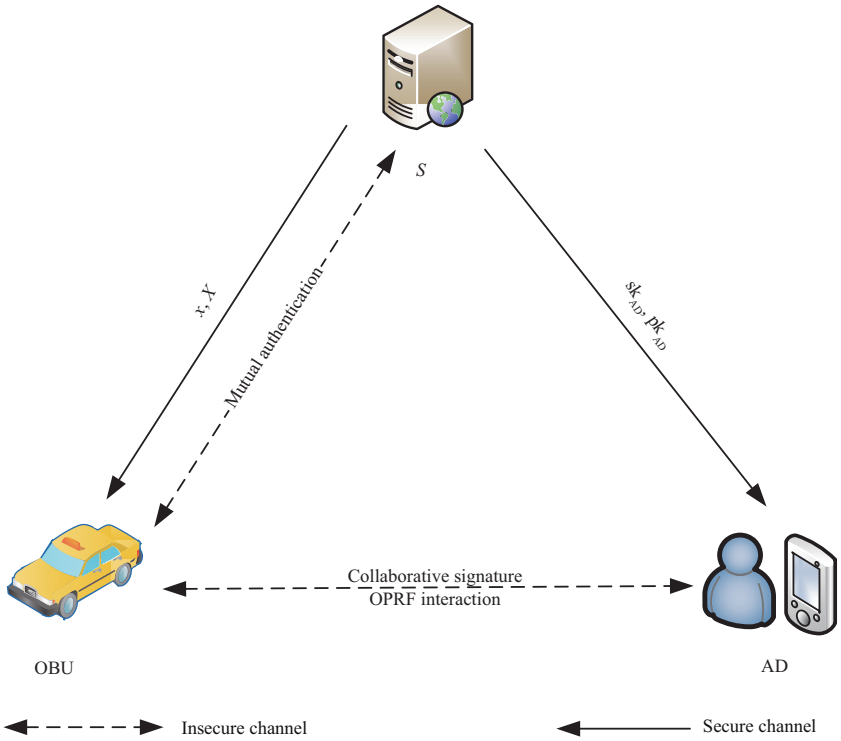

图 3 (网络版彩图) 系统模型图

Figure 3 (Color online) The system model of our proposed scheme

(2) 将 x 附在消息后面一起计算哈希值 e, $e = h(m||R)$;

(3) 计算 $s = (r + x \times e) \bmod q$, 签名包括 (R, s) 对.

- 验证签名过程.

计算 $e' = h(m||R)$, 并验证等式 $R? = g^s \times X^{e'} \bmod p$ 是否成立. 如果等式成立, 则接收方验证签名通过, 否则终止会话.

4 基于 OPRF 和 Schnorr 协同签名的认证和密钥协商方案

本节提出了基于 OPRF 和 Schnorr 协同签名的认证密钥协商方案, 在该方案中, 车辆的私钥得到了保护. 具体而言, 车辆的私钥被拆分为两个部分, 一部分由辅助设备的公钥加密存储, 另一部分由用户口令的 OPRF 值派生计算, OPRF 值的巧妙计算使得即使敌手窃取车辆, 但在没有辅助设备的情况下也难以恢复部分密钥值, 进而实现对密钥的安全存储. 提出的方案涉及 3 个实体: 车载单元 (onboard unit, OBU)、辅助设备 (auxiliary device, AD) 和远程服务器 (remote server, S), 如图 3 所示.

提出的协议主要包括 3 个阶段: (1) 初始化阶段, (2) 注册阶段, (3) 登录和认证密钥协商阶段. 具体而言, 在初始化阶段, S 生成系统公共参数; 在注册阶段, OBU 和 AD 分别进行注册以加入车联网; 在登录和认证密钥协商阶段, 用户向 OBU 输入身份信息和口令, 在 AD 的帮助下, 进行口令验证和部分密钥的恢复进而与 S 实现相互认证和会话密钥协商. 表 1 给出了提出的协议中使用到的符号以及相应的描述.

表 1 协议符号及描述表

Table 1 Symbols and description table

Symbol	Description
OBU	Onboard unit
AD	Auxiliary device
S	Remote server
$\mathrm{ID}_i, \mathrm{pwd}$	Identity of user and password
$\mathrm{pk}_s, \mathrm{sk}_s$	The public and secret keys of remote server
$\mathrm{pk}_{\mathrm{AD}}, \mathrm{sk}_{\mathrm{AD}}$	The public and secret keys of auxiliary device
x, X	The public and secret keys of vehicle
SK	Session key established between vehicle and server
k_o	Key of OPRF
k_m	Key of MAC
a, r_1, r_2, c, d	Random number
$H_1(\cdot)$	A map-to-point function
$H_2(\cdot)$	Common one-way hash functions
$\mathrm{HMAC}_{k_m}(\cdot)$	A hash function with key

4.1 系统初始化阶段

在该阶段, S 生成所有的系统参数, 详细的细节如下:

(1) S 生成 Schnorr 签名所需要的参数. S 随机选择两个大素数 p, q 以及一个 q 阶元素 $g \in Z_p^*$, 其中 $q|p-1$, $g^q \equiv 1(\mathrm{mod}p)$, $g \neq 1$.

(2) S 生成 Elgamal 加密所需要的参数. S 选择大素数 q_1, g_1 为群 $F_{q_1}^*$ 的一个随机的乘法生成元.

(3) S 选择 3 个安全的哈希函数 $H_1(\cdot)$, $H_2(\cdot)$ 和 $\mathrm{HMAC}_{k_m}(\cdot)$, 其中, $H_1(\cdot)$ 是一个 map-to-point 函数, $H_2(\cdot)$ 是普通的单向哈希函数, $\mathrm{HMAC}_{k_m}(\cdot)$ 是一个带密钥的哈希函数.

(4) S 选择随机数 $\mathrm{sk}_S \in Z_{q_1}$ 作为 S 的私钥, 并计算相应的公钥为 $\mathrm{pk}_S = {g_1}^{\mathrm{sk}_S} \bmod q_1$, 然后 S 保存 sk_S, 并将公共参数 $\{q_1, g_1, \mathrm{pk}_S, p, q, g, H_1(\cdot), H_2(\cdot), \mathrm{HMAC}_{k_m}(\cdot)\}$ 公开给所有的用户.

4.2 注册阶段

如图 4 所示, 用户使用两个设备 (OBU 和 AD) 向 S 注册, 通过注册, 车辆的私钥被分成两个部分, 分别由 OBU 和 AD 拥有. 具体过程如下:

(1) 辅助设备注册. S 选择随机数 $\mathrm{sk}_{\mathrm{AD}} \in Z_{q_1}^*$ 为 AD 的私钥, 并计算公钥为 $\mathrm{pk}_{\mathrm{AD}} = {g_1}^{\mathrm{sk}_{\mathrm{AD}}} \bmod q_1$, $(\mathrm{sk}_{\mathrm{AD}}, \mathrm{pk}_{\mathrm{AD}})$ 用于后续的 Elgamal 加密. 之后, S 发送 $\langle \mathrm{sk}_{\mathrm{AD}} \rangle$ 给 AD, 公开 $\mathrm{pk}_{\mathrm{AD}}$ 给相应的用户.

(2) 车辆注册. (i) 用户向 OBU 输入身份标识符 ID_i 和口令 pwd, 然后发送 ID_i 给 S 用于注册. (ii) S 首先检查数据库中是否包含 ID_i, 如果有, 则拒绝注册请求; 否则继续下面的操作. S 选择随机数 $x \in Z_p^*$ 为车辆的私钥, 并计算相应的公钥为 $X = g^{-x}(\mathrm{mod}p)$. 之后 S 发送 $\langle x, \mathrm{pk}_{\mathrm{AD}} \rangle$ 给 OBU, 存储 $\langle \mathrm{ID}_i, X \rangle$ 在数据库中.

(3) 接受到消息之后, OBU 拆分车辆密钥为 x_1 和 x_2, $x_1 = H_2(\mathrm{pwd}, H_1(\mathrm{pwd}^{k_o}))$ 和 $x_2 = (x - x_1) \bmod p$, 其中 k_o 为 OBU 选择的 OPRF 密钥. 之后, OBU 计算用于后续的本地口令认证的本地验证符 $N_i = H_2((H_2(\mathrm{ID}_i) \oplus H_2(x_1)) \bmod n)$ 和票据 $\mathrm{Ticket} = E_{\mathrm{pk}_{\mathrm{AD}}}(k_m || x_2)$, 其中, k_m 为 OBU 选择的

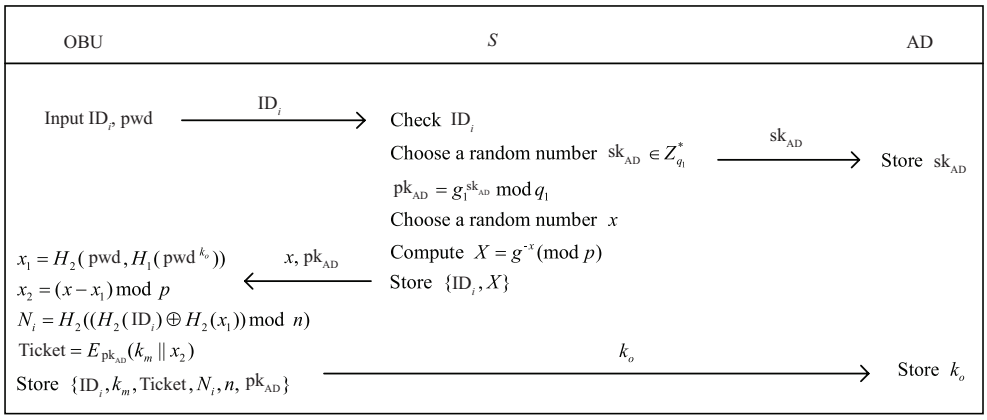

图 4　注册阶段

Figure 4　Registration phase

计算消息认证码的密钥, Ticket 用于保存 AD 的子密钥. 最后, OBU 发送 $\langle k_o \rangle$ 给 AD, 并在内存中存储参数 $\langle \mathrm{ID}_i, k_m, \mathrm{Ticket}, N_i, n, \mathrm{pk}_{\mathrm{AD}} \rangle$.

(4) AD 接收到消息之后, 存储参数 $\langle k_o, \mathrm{sk}_{\mathrm{AD}} \rangle$ 在 AD 的内存中.

4.3　登录和认证密钥协商阶段

当 OBU 想要和 S 通信时, 必须登录系统, OBU 在 AD 的帮助下恢复部分密钥, 进而实现与 S 的相互认证和密钥协商, 具体过程如图 5 所示.

(1) 司机向 OBU 输入自己的身份信息 ID_i 和相应的口令 pwd', 然后选择一个随机数 a, 计算 $A = (H_1(\mathrm{pwd}'))^a$. 之后, OBU 均匀地选择随机数 $c \in Z_{q_1}$, 然后计算 $C_1 = {g_1}^c \bmod q_1$, $C_2 = {\mathrm{pk}_S}^c \bmod q_1$ 和 $m_1 = H_2(C_1||C_2||T_1)$ 作为签名消息的一部分, 其中 T_1 为当前时间戳. 然后, OBU 计算 $R_1 = g^{r_1} \bmod p$, $m_2 = \mathrm{HMAC}_{k_m}(m_1, \mathrm{Ticket}, R_1)$ 和 $\mathrm{Ticket}' = E_{\mathrm{pk}_{\mathrm{AD}}}(\mathrm{Ticket})$, 其中 r_1 为随机数, 并将消息发送给 AD.

(2) 当 AD 接受到来自 OBU 的消息时, 它首先计算 $B = A^{k_o}$, 解密 Ticket' 得到 Ticket, 之后使用自己的私钥 $\mathrm{sk}_{\mathrm{AD}}$ 解密 Ticket 来获得参数 k_m 和 x_2, 然后通过验证等式 $m_2? = \mathrm{HMAC}_{k_m}(m_1, \mathrm{Ticket}, R_1)$ 是否成立来验证消息的完整性. 如果等式成立, 则继续下面的步骤; 否则, 会话终止.

(3) AD 使用签名私钥的一部分 x_2 计算 Schnorr 签名的一部分. 首先 AD 随机均匀选择随机数 r_2 并计算 $R_2 = g^{r_2} \bmod p$ 和 $R = R_1 R_2 \bmod p$, 之后 AD 计算 $e = H_2(R||m_1)$ 和 $s_2 = r_2 + x_2 e \bmod q$, 最后 AD 将消息 $\langle B, R, s_2 \rangle$ 返回给 OBU.

(4) OBU 接受到消息之后, 它首先进行司机身份信息的本地验证. OBU 计算 $x_1 = H_2(\mathrm{pwd}', B^{1/a})$ 和 $N_i' = H_2((H_2(\mathrm{ID}_i) \oplus H_2(x_1)) \bmod n)$, 然后 OBU 通过检查 N_i' 和 N_i 是否相等来判断司机输入口令的正确性. 如果等式成立, 则继续下一步; 否则, 请求失败, 协议运行终止. 随后, OBU 通过计算 $\mathrm{AID} = C_2 \oplus \mathrm{ID}_i$ 隐藏自己的身份信息, 然后计算 $e = H_2(R||m_1)$, $s_1 = r_1 + x_1 e \bmod q$ 和 $s = s_1 + s_2 \bmod q$ 计算签名 $\{s, R\}$. 最后, 发送 $\langle s, R, T_1, C_1, \mathrm{AID} \rangle$ 给 S.

(5) 当接收到来自 OBU 的访问请求时, S 首先检查 T_1 的有效性, 如果超过当前阈值, 则终止协议运行, 否则继续下面的过程; 然后, S 计算 $C_2' = {C_1}^{\mathrm{sk}_S} \bmod q_1$ 和 $\mathrm{ID}_i' = C_2' \oplus \mathrm{AID}$ 获得身份信息, 根据 ID_i' 检索其对应的公钥 X, 最后, S 通过计算 $m_1' = H_2(C_1||C_2'||T_1)$, $e' = H_2(R||m_1')$ 并判断 $R? = g^s X^{e'} \bmod p$ 是否成立来验证签名的正确性. 如果等式成立, 则签名验证通过, 即服务器认证了 OBU; 否则, 身份认证失败, 会话终止.

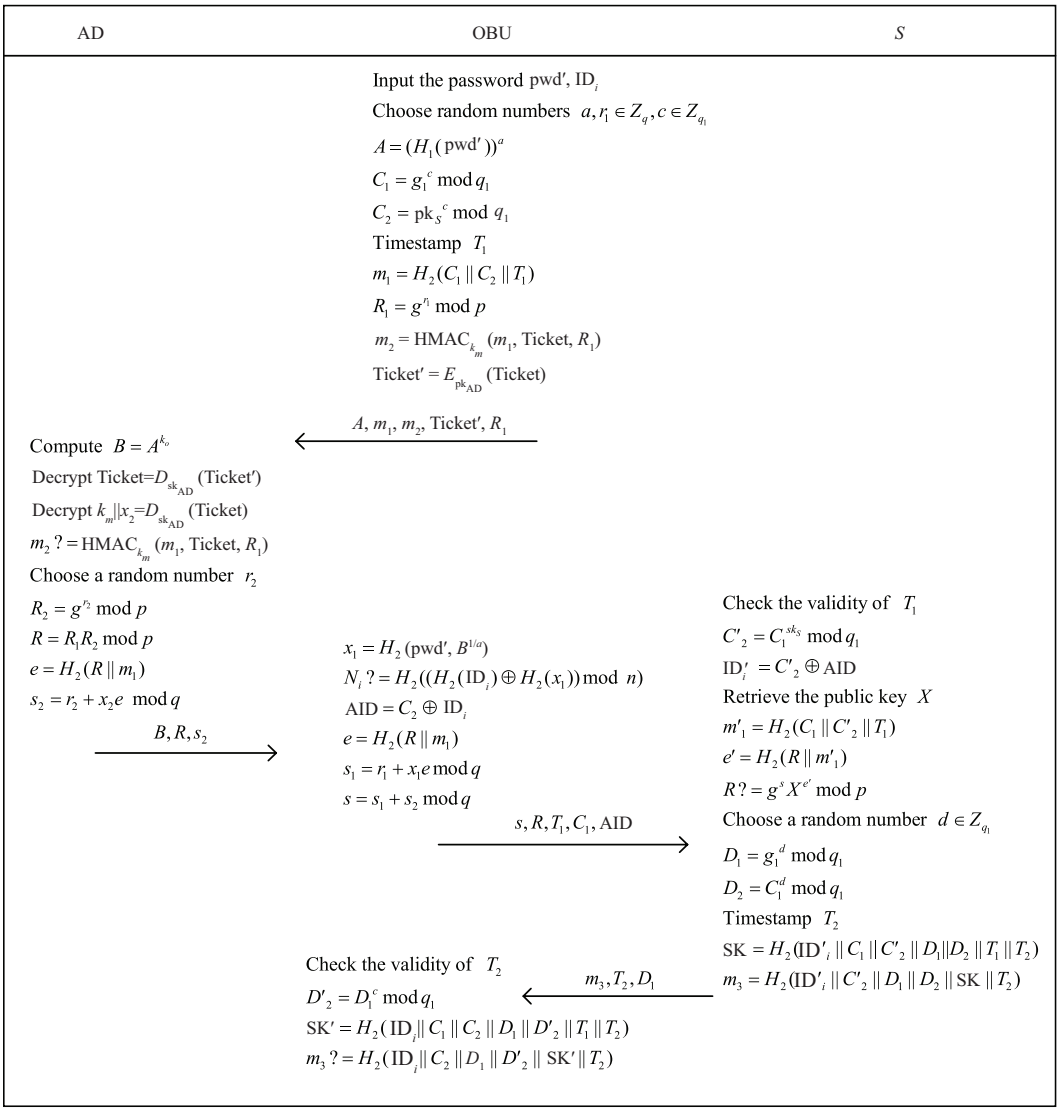

图 5 登录和认证密钥协商阶段

Figure 5 Login and authentication key agreement phase

(6) 在 S 认证 OBU 成功后, S 计算 $D_1 = {g_1}^d \bmod q_1$ 和 $D_2 = C_1^d \bmod q_1$, 其中 d 是 S 选取的随机数. 之后 S 计算会话密钥 $\mathrm{SK} = H_2(\mathrm{ID}'_i||C_1||C'_2||D_1||D_2||T_1||T_2)$ 和消息 $m_3 = H_2(\mathrm{ID}'_i||C'_2||D_1||D_2||\mathrm{SK}||T_2)$ 并发送消息 $\langle m_3, T_2, D_1\rangle$ 给 OBU.

(7) OBU 接收到消息之后首先检查 T_2 的有效性计算 $D'_2 = {D_1}^c \bmod q_1$ 和 $\mathrm{SK}' = H_2(\mathrm{ID}_i||C_1||C_2||D_1||D'_2||T_1||T_2)$, 并通过判断 $m_3? = H_2(\mathrm{ID}_i||C_2||D_1||D'_2||\mathrm{SK}'||T_2)$ 来验证消息 m_3 的正确性. 若等式成立, 则 OBU 和 S 协商会话密钥; 否则, 会话终止.

4.4 口令更新阶段

当用户想要更新口令时, 需要同时输入新旧口令, 具体过程如图 6 所示.

(1) 用户向 OBU 输入之前的口令 pwd 和想要更改的新口令 $\mathrm{pwd}_{\mathrm{new}}$, OBU 选择一个随机数 a, 计

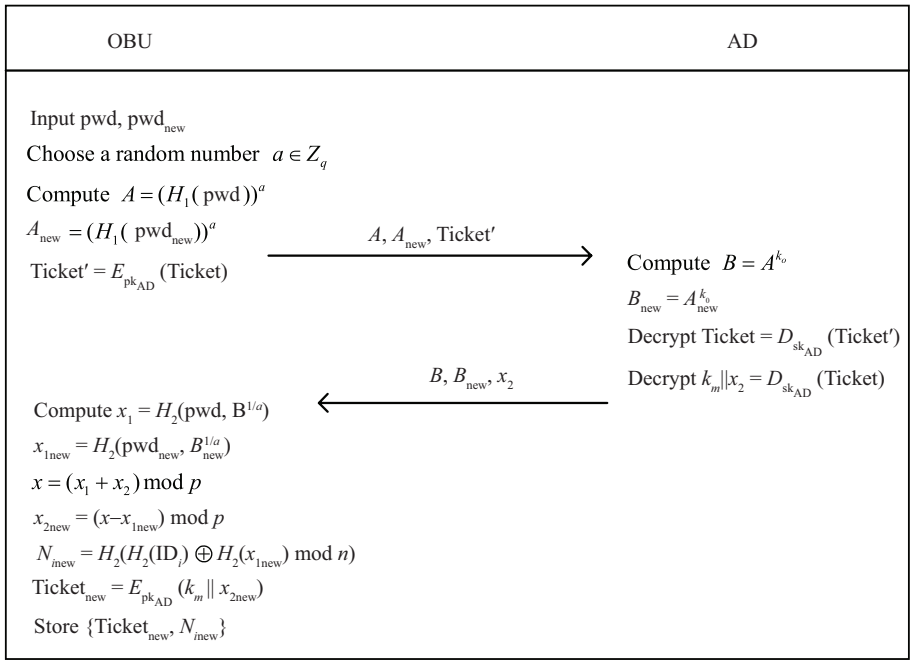

图 6　口令更新阶段

Figure 6　Password change phase

算 $A=(H_1(\text{pwd}))^a$, $A_{\text{new}}=(H_1(\text{pwd}_{\text{new}}))^a$, 并给票据加密 $\text{Ticket}'=E_{\text{pk}_{\text{AD}}}(\text{Ticket})$, 将 $\langle A, A_{\text{new}}, \text{Ticket}'\rangle$ 发送给 AD.

(2) 当 AD 接受到来自 OBU 的消息时, 首先计算 $B=A^{k_o}$ 和 $B_{\text{new}}=A_{\text{new}}^{k_0}$, 之后使用自己的私钥 sk_{AD} 解密 Ticket 来获得参数 k_m 和 x_2, 并将 $\langle B, B_{\text{new}}, x_2\rangle$ 返回给 OBU.

(3) OBU 接收到消息之后, 计算 $x_1=H_2(\text{pwd}, B^{1/a})$ 和 $x_{1\text{new}}=H_2(\text{pwd}_{\text{new}}, B_{\text{new}}^{1/a})$, 用 x_1 和 AD 发送过来的 x_2 恢复 S 的私钥 x, 并计算 $x_{2\text{new}}=(x-x_{1\text{new}}) \bmod p$, $N_{i\text{new}}=H_2(H_2(\text{ID}_i)\oplus H_2(x_{1\text{new}}) \bmod n)$, 用 $x_{2\text{new}}$ 重新计算票据 $\text{Ticket}_{\text{new}}=E_{\text{pk}_{\text{AD}}}(k_m||x_{2\text{new}})$, 存储 $\langle \text{Ticket}_{\text{new}}, N_{i\text{new}}\rangle$, 完成口令更新.

5　可证明安全分析

在这一部分, 本文根据 MacKenzie 等的形式化分析方法 [42], 对提出的方案进行安全分析, 首先给出敌手模型, 然后在随机预言模型下证明本文方案的安全性.

5.1　安全性定义

为了形式化地证明提出方案的安全性, 必须首先给出协议的安全目标以及安全性定义.

定义 $\text{Adv}(D)$ 表示成功腐化 D 中元素的敌手类型, 其中 $D\subseteq\{\text{AD}, \text{OBU}, \text{pwd}, S\}$, 如 $\text{Adv}(\{\text{AD}, \text{pwd}, S\})$ 表示拥有用户口令和辅助设备、S 的公私钥对的敌手. 本文的安全目标主要包括以下几点:

(1) 在集合 $\text{Adv}(\{\text{AD}, \text{pwd}, S\})$ 中的任意攻击者无法计算会话密钥.

(2) 在集合 $\text{Adv}(\{\text{OBU}, S\})$ 中的任意攻击者可以以最多 q/Dic 的概率计算会话密钥. 其中, q 为攻击者对服务器的访问次数, Dic 为司机选择口令的字典空间.

(3) 在集合 Adv($\{\mathrm{AD}, \mathrm{OBU}\}$) 中的任意攻击者可以计算会话密钥, 仅当车辆对司机口令进行成功的离线口令猜测后.

在下面证明过程中, 假设用户永远在口令输入设备上输入口令 pwd. 然而, 在现实生活中, 错误输入的现象会发生. 错误输入操作不会影响对 Adv($\{\mathrm{AD}, \mathrm{pwd}\}$) 情况的分析, 但会对其他两种情况的分析造成影响. Adv($\{\mathrm{OBU}\}$) 集合中的攻击者可以通过观察失败的 OPRF 值来尝试获得关于口令错误输入频率的信息, 这可能会给敌手提供关于口令的信息. Adv($\{\mathrm{AD}, \mathrm{OBU}\}$) 集合中的攻击者可以获得出频率之外的更多信息, 比如, 两次错误的输入是否相等.

协议的安全性. 伪造者的目标是使用相应的公钥 X 来伪造一个 Schnorr 签名, 进而计算出会话密钥. 整个分析过程中存在一个 AD 预言机、一个 OBU 预言机、一个 svr 预言机, 以及随机预言机 h, H_1 和 H_2. 随机预言机可以被询问任意多次, 它输入一个值并返回定义范围内的随机值. AD 预言机会被 partsign 质询. 在质询 partsign 中, 它代表一个部分签名请求, AD 预言机要么拒绝请求终止会话, 要么返回部分消息.

OBU 预言机可能会被 start, seskey 和 finish 质询. 假设存在一个隐式的会话概念, 使得 OBU 预言机可以确定 finish 质询的会话和 start 的一致. 在一个 start(m) 质询中, 代表请求开始执行协议, OBU 会返回消息 $\langle A, m_1, m_2, \mathrm{Ticket}', R_1\rangle$. 在相应的 seskey 质询中, 它表示来自辅助设备的响应, 输出的是前一个 start(m) 质询的结果. 在相应的 finish 质询中, 它表示来自服务器对于质询 seskey 的响应, 它要么是终止会话, 要么是返回对前一个质询的结果.

Adv($\{\mathrm{AD}, \mathrm{pwd}, S\}$), Adv($\{\mathrm{OBU}, S\}$) 和 Adv($\{\mathrm{AD}, \mathrm{OBU}\}$) 类型的伪造者成功, 当且仅当伪造者可以输出计算出会话密钥 $\mathrm{SK} = H_2(\mathrm{ID}_i||C_1||C_2||D_1||D_2||T_1||T_2)$, 且没有 start($m$) 质询.

在下面的证明过程中, 使用 q_{part} 来表示对辅助设备的 partsign 质询的次数. 使用 q_{start} 和 q_{finish} 来表示对车辆车载单元的 start 和 finish 质询的次数. 我们把 h, H_1 和 H_2 模式化为随机预言机, q_h, q_{H_1} 和 q_{H_2} 来分别表示质询的次数. 让 q_o 表示对不包括在上述预言机中的其他预言机的质询次数. 让 $\bar{q} = (q_{\mathrm{part}}, q_{\mathrm{start}}, q_{\mathrm{finish}}, q_h, q_{H_1}, q_{H_2}, q_0)$. 如果攻击者进行了 $\bar{q}$ 次质询并且以不小于 ε 的概率成功计算出会话密钥, 则认为伪造者 $(\bar{q}, \varepsilon)$ 攻破该协议.

5.2 定理及证明

定理1 如果 Adv($\{\mathrm{AD}, \mathrm{pwd}, S\}$) 的敌手攻破协议, 即存在一个敌手 $(\bar{q}, \varepsilon')$ 以 $\varepsilon' \approx \varepsilon$ 攻破仿真的协议.

证明 对于给定的敌手 $A \in$ Adv($\{\mathrm{AD}, \mathrm{pwd}, S\}$) 以 $(\bar{q}, \varepsilon')$ 攻破提出的方案. 我们为仿真的方案构建一个敌手 A^*. 已知 Schnorr 签名方案的公钥 X 并为 A 仿真提出的方案, 以至于由 A 构造的伪造者将会是仿真的协议的构造者.

仿真 A^* 给予 X 给 A 作为车辆车载单元的签名密钥; A^* 生成辅助设备的密钥对 $(\mathrm{sk}_{\mathrm{AD}}, \mathrm{pk}_{\mathrm{AD}})$ 和远程服务器的密钥对 $(\mathrm{sk}_S, \mathrm{pk}_S)$ 并将密钥对给 A. 然后, A^* 生成司机的口令 pwd $\in$ Dic, 并交给 A. 最后, A^* 使用随机值 a, r_1 和 c 正常运行协议生成 $\langle A, m_1, m_2, \mathrm{Ticket}', R_1\rangle$.

A^* 按照真实的协议响应预言机. A^* 通过查询随机预言机来获得 $B = A^{k_o}$, A^* 检查 $m_2? = \mathrm{HMAC}_{k_m}(m_1, \mathrm{Ticket}, R_1)$, 如果等式不成立, A^* 终止会话, 否则计算 $\langle B, R, s_2\rangle$ 响应相应的 start(m) 质询; A^* 通过计算相应的签名 $R = R_1R_2 \bmod p$, $s_1 = r_1 + x_1e \bmod q$ 和 $s = s_1 + s_2 \bmod q$ 来响应 seskey 质询; A^* 通过计算 $\mathrm{SK}' = H_2(\mathrm{ID}_i||C_1||C_2||D_1||D_2'||T_1||T_2)$ 和 $D_2' = {D_1}^c \bmod q_1$ 并验证 $m_3? = H_2(\mathrm{ID}_i||C_2||D_1||D_2'||\mathrm{SK}'||T_2)$ 来响应质询. 如果不相等, A^* 终止会话, 否则 A^* 返回 SK.

分析 让 S-schnorr$'$ 成为 S-schnorr 协议使用完美随机函数代替 h 的协议, 让 ε'' 表示 A 运行破

坏 S-schnorr′ 协议伪造的方案. 由于 H_2 的伪随机性, $\varepsilon'' \approx \varepsilon$. 现在让 ε' 表示 A 在仿真情况下的概率, 也就是 A^* 计算会话密钥的概率. 可以发现上面的仿真对 S-schnorr′ 对 A 是统计不可区分的, 因此 $\varepsilon'' \approx \varepsilon' \approx \varepsilon$.

定理2 让 H_1 和 H_2 表示伪随机函数. 如果 $\mathrm{Adv}(\{\mathrm{OBU}, \mathrm{AD}\})$ 的敌手攻破提出的协议, 即存在一个 $(\bar{q}, \varepsilon')$ 敌手以 $\varepsilon' \approx \varepsilon - \frac{q_{H1}+q_{H2}}{|D|}$ 的概率攻破仿真协议.

证明 对于给定的敌手 $\mathrm{Adv}(\{\mathrm{OBU}, \mathrm{AD}\})$ 以 $(\bar{q}, \varepsilon')$ 攻破提出的方案, 本文为仿真的方案构建一个敌手 A^*. A^* 已知 Schnorr 签名方案的公钥 X 并为 A 仿真提出的方案, 因此由 A 构造的无需猜测口令的敌手将会是仿真的协议的敌手.

仿真 A^* 给予 X 给 A 作为车辆车载单元的签名密钥; A^* 生成辅助设备的密钥对 $(\mathrm{sk}_{\mathrm{AD}}, \mathrm{pk}_{\mathrm{AD}})$ 和远程服务器的公钥 pk_S 并将其给 A. 然后, A^* 生成司机的口令 $\mathrm{pwd}' \in D$, 并交给 A; A^* 使用随机值 a, r_1 和 c 正常运行协议生成 $\langle A, m_1, m_2, \mathrm{Ticket}', R_1\rangle$, 其中 x_2 是随机选取的数. 最后, A^* 把 $\langle \mathrm{ID}_i, k_m, \mathrm{Ticket}, N_i, n\rangle$ 告知 A.

除去 $\mathrm{pwd} = \mathrm{pwd}'$ (H_1 和 H_2 质询) 的情况, 其余 A^* 均按照正常的随机预言机响应 H_1 和 H_2 质询. A^* 响应 veh 预言机和 AD 预言机与上述定理 1 的证明相同.

分析 除非 A 对进行 H_1 和 H_2 质询, 质询发生的概率为 $\frac{q_{H1}+q_{H2}}{|D|}$, 否则上面的仿真对真实协议是统计不可区分的, 因此如果 A 在真实协议运行下计算会话密钥的概率为 ε, 在仿真方案运行中 A^* 将会以 $\varepsilon' \approx \varepsilon - \frac{q_{H1}+q_{H2}}{|D|}$ 的概率计算会话密钥.

定理3 假设 H_1 和 H_2 在口令空间 Dic 上发生碰撞的概率是可忽略的. 如果 $\mathrm{Adv}(\{\mathrm{OBU}, \mathrm{svr}\})$ 的敌手 $(\bar{q}, \varepsilon)$ 攻破提出的协议, 其中 $\varepsilon = \frac{q_{\mathrm{part}}}{|D|} + \frac{\varphi}{2}$, 即存在一个 $(2q_{\mathrm{part}}, \varepsilon')$ 敌手以 $\varepsilon' \approx \frac{\varphi}{2(1+q_{\mathrm{part}})}$ 的概率攻破辅助服务器的加密方案或在一个 $(q_{\mathrm{start}}, \varepsilon'')$ 敌手以 $\varepsilon'' \approx \frac{\varphi}{2}$ 的概率攻破仿真协议.

证明 对于给定的敌手 $\mathrm{Adv}(\{\mathrm{OBU}, \mathrm{svr}\})$ 以 $(\bar{q}, \varepsilon')$ 攻破提出的方案, 我们为仿真的方案构建一个敌手 A^* 攻破加密方案或一个可以攻破提出协议的敌手. 如果敌手 A 攻破特定仿真的概率为 $\frac{q_{\mathrm{part}}}{|D|} + \frac{\varphi}{2}$, 我们可以构建一个敌手 $A^*(q_{\mathrm{start}}, \varepsilon'')$ 攻破仿真协议的概率为 $\varepsilon'' \approx \frac{\varphi}{2}$; 如果敌手没有以上述的概率获得胜利, 则可以构建一个 $(2q_{\mathrm{part}}, \varepsilon')$ 敌手攻破辅助服务器的加密方案的概率为 $\varepsilon' \approx \frac{\varphi}{2(1+q_{\mathrm{part}})}$.

仿真 A^* 给予 X 给 A 作为车辆车载单元的签名密钥; A^* 生成远程服务器的密钥对 $(\mathrm{sk}_S, \mathrm{pk}_S)$ 并将 pk_S 给 A. 然后, A^* 生成司机的口令 $\mathrm{pwd}' \in D$, 并交给 A; A^* 使用随机值 a, r_1 和 c 正常运行协议生成 $\langle A, m_1, m_2, \mathrm{Ticket}', R_1\rangle$, 其中 x_2 是随机选取的随机数. 最后, A^* 把 $\langle A, m_1, m_2, \mathrm{Ticket}', R_1\rangle$ 告知 A.

A^* 响应 OBU 预言机按照真实的协议. A^* 响应 $\mathrm{seskey}(s, R, T_1, C_1, \mathrm{AID})$ 质询的情况有以下两种.

(1) $\mathrm{seskey}(s, R, T_1, C_1, \mathrm{AID})$ 是来自于 $\mathrm{start}(m)$: 计算并返回 $\langle B, R, s_2\rangle$, 其中 $B = A^{k_o}$, $R = R_1R_2 \bmod p$ 且 $s_2 = r_2 + x_2 e \bmod q$, 其中 g^{r_1} 和 e 来自 $\mathrm{start}(m)$.

(2) T_1, C_1, AID 是来自于 $\mathrm{start}(m)$, 而 s, R 不是: 返回终止会话.

A^* 响应 veh $\mathrm{start}(m)$ 质询与上述定理 1 的证明相同.

分析 由于口令是随机均匀选取的, 且实用的随机函数在口令空间内发生碰撞的概率是可忽略的, A^* 进行成功的在线口令猜测的的概率为 $\frac{q_{\mathrm{oprf}}}{|D|}$, 上面的仿真对真实协议是统计不可区分的. 因此如果 A 在仿真协议运行下计算会话密钥的概率至少为 $\varepsilon = \frac{q_{\mathrm{oprf}}}{|D|} + \frac{\varphi}{2}$, 在真实方案运行中 A^* 将最少以 $\frac{\varphi}{2}$ 的概率计算会话密钥.

6 安全性分析与性能评估

6.1 非形式化安全性分析

在这一部分, 我们对提出的方案进行了非形式化安全分析, 分析结果表明, 本文方案可以抵抗很多已知的攻击并提供想要的安全属性. 特别地, 提出的方案可以抵抗离线口令猜测攻击和提供抗设备捕获的安全特性.

(1) 抗离线口令猜测攻击. 当 OBU 丢失或被窃取的时候, 敌手 A 可以通过边信道攻击获取存储在 OBU 上的安全参数 $\langle \mathrm{ID}_i, k_m, \mathrm{Ticket}, N_i, n\rangle$. 然而, 由于敌手不知道 pwd 的值, 无法直接计算出 x_1 的值. 即使敌手可以从口令字典中猜测到正确的候选口令, 在不知道 k_o 的情况下, 敌手也无法计算 $x_1 = H_2(\mathrm{pwd}, H_1((\mathrm{pwd})^{k_o}))$. 此外, 由于 $N_i = H_2((H_2(\mathrm{ID}_i) \oplus H_2(x_1)) \bmod n)$ 采用了模糊因子 (模操作), 即使敌手选择了一个错误的口令, 上述等式也有可能是成立的. 因此, 敌手在获得存储在 OBU 上的参数后也无法猜测出用户的口令, 即提出的方案可以抵抗离线口令猜测攻击.

(2) 抗设备捕获. 因为 OBU 常常被放在无人看管的环境中, 则攻击者可以通过探测 OBU 来获得大量的有用信息. 假定攻击者在捕获 OBU 后可以获得 OBU 上存储的全部参数 $\langle \mathrm{ID}_i, k_m, \mathrm{Ticket}, N_i, n\rangle$. 然而, 即使 OBU 丢失或被偷且敌手获得了全部参数, 在没有 AD 帮助的情况下, 敌手也无法计算 $x_1 = H_2(\mathrm{pwd}, H_1((\mathrm{pwd})^{k_o}))$, 即敌手无法恢复 OBU 端的密钥. 当 AD 被捕获时, 即使敌手可以获得存储在 AD 上的秘密值 $\langle k_o, \mathrm{sk}_{\mathrm{AD}}\rangle$, 也无法计算出正确的 x_1, 进而通过 S 的认证. 即使在敌手同时获得 OBU 和 AD 的情况下, 由于不知道口令, 敌手也无法计算出正确的 OBU 端的密钥. 此外, 由于方案中的口令是通过本地验证符 $N_i = H_2((H_2(\mathrm{ID}_i) \oplus H_2(x_1)) \bmod n)$ 在本地模糊验证的, 因此会出现敌手输入错误的口令却通过本地认证的情形, 进而得到一个错误的密钥值 x_1. 因此, 即使 OBU 和 AD 均被捕获, 认证密钥协商协议的密钥仍然是安全的. 也就是说, 提出的方案提供了抗设备捕获的安全特性.

(3) 匿名性和不可追踪性. OBU 匿名性表明, 除了 OBU 和 S, 任何第三方都无法了解到用户的身份. 在我们的方案中, OBU 和 AD 的通信没有涉及到身份信息的传递; 在 OBU 和 S 的传输过程中, 传递的消息包括 $\langle s, R, T_1, C_1, \mathrm{AID}\rangle$ 和 $\langle m_3, T_2, D_1\rangle$, 只有 AID 涉及到身份信息. OBU 身份以密文 $\mathrm{AID} = C_2 \oplus \mathrm{ID}_i$ 的形式被发送给 S, S 在接受到之后可以解密 $\mathrm{ID}_i' = C_2' \oplus \mathrm{AID}$ 获得相应的身份, 而攻击者无法从协议运行中识别用户身份. 因此, 提出的方案实现了 OBU 身份的匿名性.

用户不可追踪性确保攻击者无法识别同一用户发起的任何两次过去的协议运行. 本文提议的协议在登录和认证过程中, 消息 $\langle A, m_1, m_2, \mathrm{Ticket}', R_1\rangle$, $\langle B, R, s_2\rangle$, $\langle s, R, T_1, C_1, \mathrm{AID}\rangle$ 和 $\langle m_3, T_2, D_1\rangle$ 在 OBU, AD 和 S 之间传递. 因为每个消息的计算都包含了随机数或时间戳, 因此每个会话中的消息都是动态更新的, 而非固定不变的. 因此攻击者无法根据在不同的会话中捕获到的消息来追踪车辆, 即提出的方案实现了 OBU 的不可追踪性.

(4) 双向认证. 在 OBU 和 AD 的交互过程中, OBU 发送消息 $\langle A, m_1, m_2, \mathrm{Ticket}', R_1\rangle$ 给 AD, 只有相应的 OBU 才存储正确的 k_m, 通过验证 $m_2 ?= \mathrm{HMAC}_{k_m}(m_1, \mathrm{Ticket}, R_1)$ 是否成立实现对 OBU 的认证; AD 发送消息 $\langle B, R, s_2\rangle$ 给 OBU, 只有相应的 AD 才可以使用正确的 k_o 计算出 x_1, OBU 通过验证等式 $N_i' = H_2((H_2(\mathrm{ID}_i) \oplus H_2(x_1)) \bmod n)$ 是否成立实现对 AD 的认证. 因此, 提出的方案实现了 OBU 和 AD 的双向认证.

在提出的方案中, OBU 发送消息 $\langle s, R, T_1, C_1, \mathrm{AID}\rangle$ 给 S, 只有相对应的 S 才可以计算出 $C_2' = {C_1}^{\mathrm{sk}_S} \bmod q_1$ 以解密 $\mathrm{ID}_i' = C_2' \oplus \mathrm{AID}$ 获得相应的身份 ID_i, 并查找对应的公钥验证签名的正确性. S 通过验证签名的有效性实现对 OBU 的认证. S 发送消息 $\langle m_3, T_2, D_1\rangle$ 给 OBU, OBU 通过验证等式

$m_3? = H_2(\mathrm{ID}_i||C_2||D_1||D_2'||\mathrm{SK}'||T_2)$ 是否成立来实现对 S 的认证. 因为只有具有私钥的 S 才可以对 C_1 解密来获得相对应的身份 ID_i, 进而计算会话密钥和 m_3. 因此, 提出的方案实现了 OBU 和 S 的双向认证.

因此, 提出的方案实现了 OBU 和 S, OBU 和 AD 的双向认证.

(5) 抗中间人攻击. 假定攻击者可以获得 OBU, AD 和 S 在登录和认证阶段传输的所有消息, 并且使用自己计算的消息去替换部分或全部的消息. 具体地, 如果攻击者想要修改消息 $\langle A, m_1, m_2, \mathrm{Ticket}', R_1\rangle$, 需要生成随机数 r_1. 如果攻击者要计算 $m_2 = \mathrm{HMAC}_{k_m}(m_1, \mathrm{Ticket}, R_1)$, 则需知道 k_m, 但是因为 $\mathrm{Ticket} = E_{\mathrm{pk_{AD}}}(k_m||x_2)$ 对 k_m 的保护, 攻击者无法获得相应的值. 因此, 敌手无法计算 m_2. 同样地, 攻击者无法计算 $\langle s, R, T_1, C_1, \mathrm{AID}\rangle$, 因为由于攻击者不知道签名私钥 x, 无法计算 $\langle s, e\rangle$. 攻击者无法计算 $\langle m_3, T_2, D_1\rangle$, 因为攻击者在不知道服务器私钥的情况下无法获得身份标识, 则攻击者无法计算 $m_3 = H_2(\mathrm{ID}_i'||C_2'||D_1||D_2||\mathrm{SK}||T_2)$. 因此, 提出的方案可以抵抗中间人攻击.

(6) 抗伪装攻击. OBU 伪装攻击: 敌手想要在提出的方案中伪装成 OBU 访问 S, OBU 需要构造消息 $\langle s', R', T_1', C_1', \mathrm{AID}'\rangle$ 来通过认证. 敌手可以选择在 AD 的帮助下和不在 AD 的帮助下构造消息来请求访问 S. 如果敌手在不通过 AD 的帮助下直接构造消息, 则敌手首先选择随机数 $c \in Z_{q_1}$, 然后计算 $C_1' = g_1^c \bmod q_1$, $C_2' = \mathrm{pk}_S^c \bmod q_1$ 和 $\mathrm{AID}' = C_2 \oplus \mathrm{ID}_i$. 之后敌手计算 $R' = g^{r'} \bmod p$ 和 $e' = h(R'||m_1)$, 由于不知道 OBU 的私钥, 敌手无法计算正确的 s'. 如果敌手选择在 AD 的帮助下构造消息, 则敌手首先要通过 AD 的认证. 然而由于敌手不知道用户的口令, 无法计算出正确的 x_1, 即攻击者无法恢复 OBU 的部分私钥. 攻击者就无法构造可以通过认证的消息. 因此, 提出的方案可以抵抗车辆伪装攻击.

AD 伪装攻击. 敌手想要在提出的认证密钥协商协议中伪装成 AD 欺骗 OBU, 则攻击者必须构造正确的消息 $\langle B', R', s_2'\rangle$ 来响应请求, 即攻击者要计算 $B' = A^{k_o}$ 并发送给 OBU. 然而, 攻击者在不知道 k_o 的情况下无法计算正确的 B'. 如果攻击者选用错误的 k_o' 来计算, 则 AD 无法通过 OBU 的认证. 因此, 提出的方案可以免于辅助设备伪装攻击的威胁.

S 伪装攻击. 敌手想要在提出的方案中伪装成 S, S 需要构造消息 $\langle m_1', C_3', T_2'\rangle$ 来通过认证并和 OBU 协商会话秘钥. 然而, $C_3' = g^{r'_4} \bmod q_1$, $m_1' = h(\mathrm{ID}_i||C_4'||\mathrm{SK}')$, $C_4' = C_1^{r'_4} \bmod q_1$ 且 $\mathrm{SK}' = h(\mathrm{ID}_i||C_1||C_3'||C_4'||T_1||T_2')$. 因此, 敌手必须知道请求访问的车辆的 ID_i, 但是, 通过前面的分析可以得知, 在不知道 S 私钥的情况下, 敌手无法解密获得车辆的 ID_i, 也就是说, 敌手无法构造消息 $\langle m_1', C_3', T_2'\rangle$. 因此, 提出的方案可以抵抗服务器伪装攻击.

(7) 已知会话密钥安全. 假定攻击者获得了之前 OBU 和 S 之间协商的会话密钥 $\mathrm{SK} = h(ID_i'||C_1||C_2'||D_1||D_2||T_1||T_2)$. 然而, 会话密钥的计算需要使用随机数 c 和 d, 因此每个会话会使用不同的随机数来确保每个会话的会话密钥不同. 因此, 提出的方案可以实现已知会话密钥安全性.

(8) 抗重放攻击. 在提出的抗捕获认证密钥协商协议中, 随机数、时间戳和挑战 – 应答机制被用来抵抗重放攻击. 具体来说, 消息 $\langle A, m_1, m_2, \mathrm{Ticket}', R_1\rangle$ 的值是使用 OBU 选择的随机数 r_1, c 和当前时间戳 T_1 来计算的. 如果敌手直接重放消息, 则该消息不会通过 AD 的核查. 因此, AD 将终止会话. 特别地, 值 Ticket' 的计算不涉及随机数或时间戳, 但是直接重放 Ticket' 不会影响协议的正确运行. 另外, 消息 $\langle B, R, s_2\rangle$ 的计算需要 AD 选择的随机数 r_2 的参与. OBU 可以通过验证 R 的新鲜度来检测重放的消息. 此外, 发送给 S 的消息 $\langle s, R, T_1, C_1, \mathrm{AID}\rangle$ 包含随机数 r_1, r_2 和 c 以及时间戳 T_1 用于抵抗重放攻击. 消息 $\langle m_3, T_2, D_1, \rangle$ 也包含随机数 d 和时间戳 T_2, 并且和消息 $\langle s, R, T_1, C_1, \mathrm{AID}\rangle$ 是属于挑战应答. 因此, 提出的方案可以免受重放攻击的影响.

表 2 安全特征的比较 a)

Table 2 Comparison of security features[a)]

Security features	Feng et al.'s scheme [18]	Wu et al.'s scheme [17]	The proposed scheme
Offline password guessing attack resistance	–	–	√
Device capture resilient	√	×	√
Anonymity	√	√	√
Untraceability	√	√	√
Mutual authentication	×	√	√
Man-in-the-middle attack resistance	√	√	√
Impersonation attack resistance	√	√	√
Two-factor security	–	×	√
Known session key security	√	√	√
Replay attack resistance	√	√	√
Key security	×	×	√

a) "√"means that the security feature is satisfied; "×"means that the security feature is not satisfied; "–"means that it is not comparable.

6.2 安全特征比较

本文对提出的方案和其他的基于两方计算的认证密钥协商协议进行比较, 如表 2 所示. 与本文提出的协议相比, Feng 等 [18] 的方案中辅助设备与设备之间缺乏双向认证, Wu 等 [17] 的方案容易遭受设备捕获攻击且没有实现真正的双因子安全. 此外, 方案 [17,18] 中签名两方的部分私钥以明文的形式存储在相应的设备中, 不满足密钥安全性. 因此, 本文提出的方案具有更强的安全性.

6.3 计算开销分析

本文在个人计算机 (联想, Intel Core$^{\text{TM}}$ i5-8250U 1.60 GHz 处理器和 Windows 10 操作系统) 和移动设备 (HUAWEI Kirin 810 处理器的 HLK-AL, 8 G 运行内存和 Android 10.0.0 操作系统) 上使用 Java 编程语言基于 jpbc 库运行如下的运算操作.

T_h: SHA-256 哈希函数的运行时间; T_{exp}: 在循环群运行指数操作的时间; T_{mtp}: 在循环群上运行 Map-to-point 哈希操作时间; T_f: 函数 f 的运行时间; T_{enc}: ElGamal 加密操作的执行时间; T_{dec}: ElGamal 解密操作的执行时间; T_{mac}: 计算消息认证码的时间; T_{mul}: 计算标量乘法的执行时间; $T_{p\text{-mul}}$: 循环群上计算标量乘法的执行时间; T_{pen}: Paillier 同态加密的执行时间; T_{pde}: Paillier 同态解密的执行时间.

在实验执行过程中, 移动设备和笔记本电脑分别代表车载单元、辅助设备/远程服务器. 为了和其他方案进行比较, 本文在相同的开发环境下运行了如下的密码原语, 运算操作的运行时间为 1000 次测试的平均值, 所需的时间如表 3 所示. 并且在此基础上, 对比了现有的两方协同认证并实现密钥协商的相似协议 [17,18] 的计算开销, 结果如表 4 所示, 计算开销对比如图 7 所示. 提出的总方案计算开销 255.418 ms, 方案 [17,18] 的总计算时间分别为 313.821 和 369.789 ms. 虽然方案 [18] 在主设备端具有一定的优势, 方案 [17] 在服务器端具有一定的计算优势, 但考虑到方案的总体运行以及密钥的安全存储, 提出的方案具有更强的优势.

表 3 给定运算操作的运行时间 (单位: ms)

Table 3 Running time of given operation (ms)

Operations	Vehicle/auxiliary device	Server
T_h	0.054	0.009
T_{exp}	20.325	7.591
T_{mtp}	73.684	13.417
T_f	0.063	0.014
T_{enc}	3.825	1.570
T_{dec}	1.858	0.715
T_{mac}	0.071	0.017
T_{mul}	0.127	0.020
$T_{p\text{-mul}}$	18.933	6.270
T_{pen}	9.846	7.540
T_{pde}	12.944	10.043

表 4 计算开销对比 (单位: ms)

Table 4 Calculation of cost comparison (ms)

	Feng et al.'s scheme [18]	Wu et al.'s scheme [17]	The proposed scheme
OBU/device	$4T_{\text{exp}}+3T_h+T_{\text{mtp}}$ $=155.146$	$8T_{p\text{-mul}}+6T_h+2T_{\text{mul}}+T_{\text{pde}}$ $+2T_{\text{pen}}=184.678$	$T_{\text{mtp}}+6T_h+5T_{\text{exp}}+T_{\text{mac}}$ $+T_{\text{enc}}+2T_{\text{mul}}+T_f=179.846$
Auxiliary device	$T_{\text{mtp}}+T_{\text{exp}}+T_h+T_{\text{mul}}$ $=94.190$	$4T_{p\text{-mul}}+2T_h+3T_{\text{mul}}+3T_{\text{exp}}$ $+T_{\text{pde}}+T_{\text{pen}}=159.986$	$2T_{\text{exp}}+T_h+2T_{\text{dec}}+T_{\text{mac}}$ $+2T_{\text{mul}}=44.745$
Server	$5T_{\text{exp}}+4T_h+2T_{\text{mtp}}+T_{\text{mul}}$ $=64.485$	$4T_{p\text{-mul}}+5T_h=25.125$	$T_{\text{dec}}+4T_{\text{exp}}+4T_h$ $=30.827$
Overall computation cost	$155.146+94.190+64.485$ $=313.821$	$184.678+159.986+25.125$ $=369.789$	$179.846+44.745+30.827$ $=255.418$

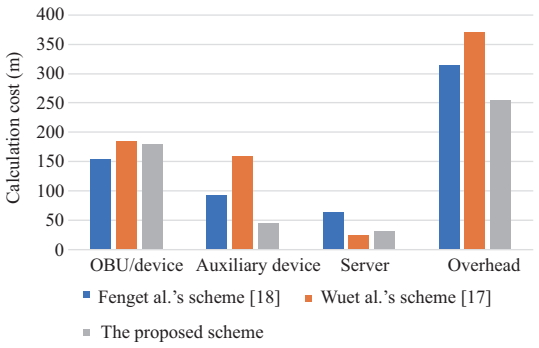

图 7 (网络版彩图) 计算开销对比图

Figure 7 (Color online) Comparison of computing costs

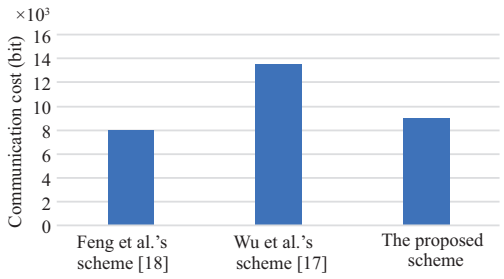

图 8 (网络版彩图) 通信开销对比图

Figure 8 (Color online) Comparison of communication overhead

6.4 通信开销分析

本方案与方案 [17,18] 的通信开销对比如图 8 所示. 此处依据文献 [24], 假设哈希函数输出的长度为 256 比特, 认证加密的密钥长度均为 128 比特, p, q 和 q_1 的长度为 512 比特, 则 n 的长度为 1024 比特, 群 G 中元素的长度为 1024 比特, 假设用户的身份和时间戳均为 32 比特.

在 Feng 等 [18] 的方案中, 医生和病人之间传递的消息为 $\langle C\rangle$ 和 $\langle R, r'\rangle$, 其中, C 为哈希函数的输出, $R \in Z_n$, r' 为两个数的乘积 (不小于 $256+1024=1280$ 比特), 医生和医疗服务器之间传输的消息为 $\langle \mathrm{AID}_i, R, R_3, \alpha, T_1\rangle$ 和 $\langle R_4, \beta, T_2\rangle$, 其中, $\mathrm{AID}, X_d, S, \beta, Y_S \in Z_n$. 因此, Feng 等 [18] 的方案的通信开销为 $256+1024+1280+1024\times 5+256+32\times 2=8000$ 比特.

在 Wu 等 [17] 的方案中, 主设备和辅助设备之间传递的消息为 $\langle R_1, C_1, \pi_1\rangle$ 和 $\langle R_2, C_2, \pi_2\rangle$, 其中, C_1, C_2 为 Paillier 同态加密的密文, 密文输出结果为 2048 比特, π_1, π_2 为两个不同零知识证明的输出 ($\pi_1=\{z_1, C_1, e_1\}$, $\pi_2=\{z_2, e_2\}$), $R_1, R_2 \in G$; 主设备和服务器之间传输的消息为 $\mathrm{Auth}_1=\{\mathrm{AID}_i, R, R_3, a, T_1\}$ 和 $\mathrm{Auth}_2=\{\beta, R_4, T_2\}$, 其中, $R, R_3, R_4 \in G$. 因此, Wu 等 [17] 的方案通信开销为 $1024\times 5+2048\times 3+256\times 5+32\times 2+512\times 2=13568$ 比特.

在本方案中, OBU 和 AD 之间发送消息为 $\langle A, m_1, m_2, \mathrm{Tickte}', R_1\rangle$ 和 $\langle B, R, s_2\rangle$, OBU 和 S 之间发送消息 $\langle \mathrm{s}, R, T_1, C_1, \mathrm{AID}\rangle$ 和 $\langle m_3, T_2, D_1\rangle$, 因此, 提出的方案的通信开销可以计算为 $1024\times 2+512\times 11+256\times 3+128\times 4+32\times 3=9056$ 比特.

因此, 在通信开销方面, 本方案较之文献 [17] 具有明显优势. 较之文献 [18], 本方案的通信开销略有增加, 但本方案可保证在设备被捕获时依然能提供安全防护.

7 结论

针对车联网场景下设备被捕获后的密钥的安全问题, 本文提出了抗捕获的认证密钥协商协议. 该协议通过结合 OPRF 技术和两方协同签名技术实现防止设备被捕获后的密钥泄露. 具体而言, OBU 的私钥被分成两个部分: 一部分使用 AD 的公钥加密, 另一部分通过拥有输入的 OBU 和拥有 OPRF 密钥的 AD 运行 OPRF 协议恢复. 即使 OBU 被攻击者盗取, 由于 OBU 中没有存储任何秘密信息, 攻击者仍然无法获取私钥. 本文对提出的方案进行了全面的安全性分析和性能比较. 结果表明所提出的方案可以抵抗各种已知的攻击, 尤其是设备被捕获时的密钥安全. 此外, 和现有的基于两方计算的认证密钥协商协议相比, 本文提出的协议具有更优的性能.

参考文献

1 China Academy of Information and Communications Technology (CAICT). Internet of Vehicles White Paper. 2021 [中国信息通信研究院. 车联网白皮书. 2021] http://www.caict.ac.cn/kxyj/qwfb/bps/202112/t20211224_394522.htm

2 National Bureau of Statistics. Statistical Bulletin on National Economic and Social Development 2019. 2020-02-28 [国家统计局. 中华人民共和国 2019 年国民经济和社会发展统计公报. 2020-02-28] http://www.gov.cn/xinwen/2020-02/28/content_5484361.htm

3 Automotive Cybersecurity Report 2020. 2020-08-23 [2020 年汽车网络安全报告. 2020-08-23] http://www.chinabgao.com/report/7308322.html

4 Zhang Y X, He W Q, Chen H, et al. Patent analysis review of automated driving vehicle safety technology. Sci Sin Inform, 2020, 50: 1732–1755 [张玉新, 何文钦, 陈虹, 等. 自动驾驶汽车安全技术专利分析综述. 中国科学: 信息科学, 2020, 50: 1732–1755]

5 Zhang W F, Lei L T, Wang X M, et al. Secure and efficient authentication and key agreement protocol using certificateless aggregate signature for cloud service oriented VANET. Acta Electron Sin, 2020, 9: 1814–1823 [张文

芳, 雷丽婷, 王小敏, 等. 面向云服务的安全高效无证书聚合签名车联网认证密钥协商协议. 电子学报, 2020, 9: 1814–1823]

6 Li C C. Research on secure mechanism in internet of vehicles for information security issues. Dissertation for Ph.D. Degree. Beijing: Beijing Jiaotong University, 2019 [李聪聪. 面向车联网信息安全问题的安全机制研究. 博士学位论文. 北京: 北京交通大学, 2019]

7 Bagga P, Das A K, Wazid M, et al. On the design of mutual authentication and key agreement protocol in Internet of vehicles-enabled intelligent transportation system. IEEE Trans Veh Technol, 2021, 70: 1736–1751

8 Amin R, Islam S H, Khan M K, et al. A two-factor RSA-based robust authentication system for multiserver environments. Secur Commun Netw, 2017, 2017: 1–15

9 Wang F, Xu Y, Zhang H, et al. 2FLIP: a two-factor lightweight privacy-preserving authentication scheme for VANET. IEEE Trans Veh Technol, 2016, 65: 896–911

10 Tsaur W J, Yeh L Y. DANS: a secure and efficient driver-abnormal notification scheme with IoT devices over IoV. IEEE Syst J, 2019, 13: 1628–1639

11 Jiang Q, Zhang X, Zhang N, et al. Three-factor authentication protocol using physical unclonable function for IoV. Comput Commun, 2021, 173: 45–55

12 Shaikh R A, Alzahrani A S. Intrusion-aware trust model for vehicular ad hoc networks. Secur Comm Netw, 2014, 7: 1652–1669

13 Shim K A. $\mathcal{CPAS}$: an efficient conditional privacy-preserving authentication scheme for vehicular sensor networks. IEEE Trans Veh Technol, 2012, 61: 1874–1883

14 Jiang Q, Zhang N, Ni J, et al. Unified biometric privacy preserving three-factor authentication and key agreement for cloud-assisted autonomous vehicles. IEEE Trans Veh Technol, 2020, 69: 9390–9401

15 Jiang Q, Zhang X, Zhang N, et al. Two-factor authentication protocol using physical unclonable function for IoV. In: Proceedings of IEEE/CIC International Conference on Communications in China (ICCC), 2019. 195–200

16 Kiltz E, Pietrzak K. Leakage resilient elgamal encryption. In: Proceedings of International Conference on the Theory and Application of Cryptology and Information Security, 2010. 595–612

17 Wu L, Wang J, Choo K K R, et al. Secure key agreement and key protection for mobile device user authentication. IEEE Trans Inform Forensic Secur, 2019, 14: 319–330

18 Feng Q, He D, Wang H, et al. Lightweight collaborative authentication with key protection for smart electronic health record system. IEEE Sens J, 2020, 20: 2181–2196

19 Han Y, Xu C, He D, et al. On the security of a key agreement and key protection scheme. IEEE Trans Inform Forensic Secur, 2020, 15: 3293–3294

20 Freedman M J, Ishai Y, Pinkas B, et al. Keyword search and oblivious pseudorandom functions. In: Proceedings of Theory of Cryptography Conference, 2005. 303–324

21 Jarecki S, Krawczyk H, Xu J Y. OPAQUE: an asymmetric PAKE protocol secure against pre-computation attacks. In: Proceedings of Annual International Conference on the Theory and Applications of Cryptographic Techniques, 2018. 456–486

22 Jarecki S, Kiayias A, Krawczyk H. Round-optimal password-protected secret sharing and T-PAKE in the password-only model. In: Proceedings of International Conference on the Theory and Application of Cryptology and Information Security, 2014. 233–253

23 Raya M, Hubaux J. The security of vehicular ad hoc networks. In: Proceedings of the 3rd ACM Workshop on Security of Ad Hoc and Sensor Networks, 2005. 11–21

24 Lin X D, Sun X T, Ho P H, et al. GSIS: a secure and privacy-preserving protocol for vehicular communications. IEEE Trans Veh Technol, 2007, 56: 3442–3456

25 Lu R, Lin X, Zhu H, et al. ECPP: efficient conditional privacy preservation protocol for secure vehicular communications. In: Proceedings of the 27th Conference on Computer Communications, 2008. 1229–1237

26 Wasef A, Shen X. EMAP: expedite message authentication protocol for vehicular ad hoc networks. IEEE Trans Mobile Comput, 2013, 12: 78–89

27 Rhim W. A study on MAC-based efficient message authentication scheme for VANET. Dissertation for Master's Degree. Seoul: Hanyang University, 2012

28 Taeho S, Jaeyoon I, Hyunsung K, et al. Enhanced MAC-based efficient message authentication scheme over VANET.

In: Proceedings of the 7th International Multi-Conference on Engineering and Technological Innovation, 2014. 110–113
29 Vighnesh N V, Kavita N, Urs S R, et al. A novel sender authentication scheme based on hash chain for vehicular ad-hoc networks. In: Proceedings of IEEE Symposium on Wireless Technology and Applications (ISWTA), 2011. 96–101
30 Li J, Lu H, Guizani M. ACPN: a novel authentication framework with conditional privacy-preservation and non-repudiation for VANETs. IEEE Trans Parallel Distrib Syst, 2015, 26: 938–948
31 Sun J Y, Zhang C, Zhang Y C, et al. An identity-based security system for user privacy in vehicular ad hoc networks. IEEE Trans Parallel Distrib Syst, 2010, 21: 1227–1239
32 Guo J H, Baugh J P, Wang S Q. A group signature based secure and privacy preserving vehicular communication framework. In: Proceedings of Mobile Networking for Vehicular Environments, 2007. 103–108
33 Zhu X, Jiang S, Wang L, et al. Efficient privacy-preserving authentication for vehicular ad hoc networks. IEEE Trans Veh Technol, 2014, 63: 907–919
34 Zhang L, Wu Q H, Solanas A, et al. A scalable robust authentication protocol for secure vehicular communications. IEEE Trans Veh Technol, 2010, 59: 1606–1617
35 Jarecki S, Kiayias A, Krawczyk H, et al. Highly-efficient and composable password-protected secret sharing. In: Proceedings of IEEE European Symposium on Security and Privacy, 2016. 276–291
36 İşler D, Küpçü A. Threshold single password authentication. In: Proceedings of European Symposium on Research in Computer Security International Workshop on Data Privacy Management Cryptocurrencies and Blockchain Technology, 2017. 143–162
37 Lindell Y. Fast secure two-party ECDSA signing. In: Proceedings of Annual International Cryptology Conference, 2017. 613–644
38 Paillier P. Public-key cryptosystems based on composite degree residuosity classes. In: Proceedings of International Conference on the Theory and Application of Cryptographic Techniques, 1999. 223–238
39 Hou W Y, Sun Y, Li D W, et al. Anonymous authentication and key agreement protocol for 5G-V2V based on PUF. J Comput Res Dev, 2021, 58: 2265 [侯琬钰, 孙钰, 李大伟, 等. 基于 PUF 的 5G 车联网 V2V 匿名认证与密钥协商协议. 计算机研究与发展, 2021, 58: 2265]
40 Guan Z, Liu H, Qin Y. Physical unclonable functions for IoT device authentication. J Commun Inform Netw, 2019, 4: 44–54
41 Schnorr C P. Efficient identification and signatures for smart cards. In: Proceedings of Advances in Cryptology-CRYPTO'89, 1990. 239–252
42 MacKenzie P, Reiter M K. Networked cryptographic devices resilient to capture. Int J Inf Secur, 2003, 2: 1–20

Device capture resilient authentication and key agreement protocol for IoV

Qi JIANG[1,2*], Xue YANG[1], Jinhua WANG[1], Qingfeng CHENG[2,3], Xindi MA[1] & Jianfeng MA[1]

1. *School of Cyber Engineering, Xidian University, Xi'an* 710071*, China*;
2. *Henan Key Laboratory of Network Cryptography Technology, Zhengzhou* 450001*, China*;
3. *School of Cyberspace Security, Strategic Support Force Information Engineering University, Zhengzhou* 450001*, China*
* Corresponding author. E-mail: jiangqixdu@gmail.com

Abstract With the steady growth of car ownership and the saturation of road traffic, the Internet of vehicle (IoV) is regarded as one of the most effective technologies to improve traffic efficiency and driving experience. Authentication and key agreement protocol (AKA) is a key means to ensure secure interaction between the onboard unit (OBU) and the various information servers. Typically, the private key of AKA protocol is stored in the OBU. However, OBU theft occurs as vehicles are often left unattended. Therefore, it is a challenge to ensure the secure storage of private keys. To address the above problem, a capture-resistant AKA protocol based on oblivious pseudorandom functions (OPRF) and collaborative signature is proposed in this paper. The private key is divided into two parts, one is encrypted using the public key of the auxiliary device and another can only be recovered by running the OPRF protocol between the OBU and the auxiliary device. Since no secret information is stored in the OBU, the adversary cannot obtain the private key even if the OBU is stolen. The comprehensive security analysis and performance comparison of the proposed scheme is provided in this paper. The result demonstrates that the proposed scheme is resistant to various known attacks, especially key leakage caused by device capture. In addition, the proposed scheme can strike a balance between computational and communication overhead.

Keywords Internet of vehicle, Schnorr collaborative signature, OPRF, authentication key agreement, capture resilient