V2G 中基于 PUF 的轻量级匿名认证协议

范馨月，刘洁，何嘉辉
（重庆邮电大学通信与信息工程学院，重庆 400065）

摘　要：针对现有车辆到电网（V2G）网络认证协议中功能不够完善、通信开销大、计算开销高等问题，提出了一种基于物理不可克隆函数（PUF）的轻量级匿名认证协议，可以抵抗机器学习建模攻击。所提协议采用哈希函数和 ASCON 密码算法，实现车辆、充电桩和能源提供商之间快速的三方认证与密钥协商。通过模糊提取器结合生物特征和用户密码，实现双因素验证、密码和生物特征更新功能，并通过密码学动态累加器提供有效的用户撤销策略。ROR 模型和 Scyther 形式化验证工具证明了所提协议的安全性，非形式化安全分析表明所提协议能抵抗物理攻击、位置伪造攻击、特权内部攻击等多种安全攻击。与近几年协议的性能对比分析表明，所提协议平均减少了约 35.9% 的通信开销和 29.9% 的计算开销，高度适用于资源有限的 V2G 环境。

关键词：匿名认证；用户撤销；物理不可克隆函数；轻量级；车辆到电网
中图分类号：TN918.9
文献标志码：A
DOI: 10.11959/j.issn.1000–436x.2024175

Lightweight PUF-based anonymous authentication protocol in V2G

FAN Xinyue, LIU Jie, HE Jiahui
School of Communication and Information Engineering, Chongqing University of Posts and Telecommunications, Chongqing 400065, China

Abstract: To address the issues of incomplete functionality, high communication overhead, and high computational cost in existing vehicle-to-grid (V2G) network authentication protocols, a lightweight anonymous authentication protocol based on physical unclonable function (PUF) was proposed, which could resist machine learning modeling attacks. The proposed protocol employed Hash functions and the ASCON cryptographic algorithm to achieve rapid three-party authentication and key negotiation among vehicles, charging stations, and energy providers. By combining fuzzy extractors with biometric features and user passwords, two-factor authentication, password and biometric feature update functions were implemented. Additionally, an effective user revocation strategy was provided through a cryptographic dynamic accumulator. The ROR model and Scyther formal validation tool proved the security of the proposed protocol, and the informal security analysis showed that the proposed protocol was resistant to a variety of security attacks, such as physical attacks, location forgery attacks and privileged insider attacks. The performance comparison analysis with the protocols of recent years shows that the proposed protocol reduces the communication overhead by about 35.9% and the computational cost by 29.9% on average, which is highly suitable for resource-limited V2G environments.

Keywords: anonymous authentication, user revocation, physical unclonable function, lightweight, vehicle-to-grid

收稿日期：2024–04–26；**修回日期：**2024–08–28
通信作者：刘洁，s220131051@stu.cqupt.edu.cn
基金项目：国家自然科学基金资助项目（No.62271096）
Foundation Item：The National Natural Science Foundation of China (No.62271096)

0 引言

近年来，随着可再生低碳设备和智能交通系统（ITS, intelligent transportation system）的进步，作为强大储能设备的电动汽车（EV, electric vechile）[1]在全球范围内越来越受欢迎。电动汽车可以通过充放电设施与供电网络相连，构建新能源汽车与供电网络之间的信息流和能量流双向互动体系[2]，并为新型电力系统的高效经济运行提供重要支撑。车辆到电网（V2G, vehicle-to-grid）网络是实现电动汽车与电网之间能量双向流动[3]的关键技术，与传统电网相比，V2G框架下的新一代电网可以更有效地利用可再生能源，实现削峰填谷，解决电网的稳定性问题。

虽然V2G网络具有很多优势，但也存在诸多安全问题。例如，恶意攻击者可以冒充合法实体，窃取电动汽车的身份信息和位置信息[4]，还可以通过物理攻击窃取设备内存中的秘密参数。同时，由于电动汽车与智能电网是通过公共无线网络进行通信的，这可能会使其遭受中间人攻击、重放攻击、篡改攻击等安全攻击，从而造成安全威胁和隐私泄露。因此，在V2G网络中，身份认证和密钥协商尤其重要。通过身份认证可以防止未经授权的访问和篡改，确保信息和系统的安全性，而密钥协商能保证未来的安全通信，为相关方提供可靠的服务。V2G网络中存在部分硬件处理能力低和资源有效的终端设备[5]，这使得传统复杂的身份认证协议难以在实际中运用。当用户因各种原因需要从注册用户列表删除时，制定有效的用户撤销策略也显得尤为重要。

目前已提出了许多身份认证协议来保障V2G网络的安全传输，但有些协议不适用于资源有限的设备，且存在时延高、计算开销大、安全功能不完善等问题。因此，本文基于物理不可克隆函数（PUF, physical unclonable function）提出了一种适用于V2G网络的轻量级匿名认证协议，具体贡献如下。

1) 通过在车辆内存中配备PUF，能有效防止车辆节点遭受物理攻击，将PUF的激励响应对（CRP, challenge-response pair）通过哈希函数隐式存储在能源提供商（EP, energy provider）的数据库中，使攻击者无法直接获取CRP进行机器学习（ML, machine-learning）建模攻击。

2) 采用ASCON对称加密、Hash、异或等轻量级密码操作，实现高效快速的三方认证和密钥协商，采用不断更新的假名来保证匿名性和不可追溯性，使用随机数和时间戳来抵抗重放攻击。非形式化安全分析结果表明，本文协议可以确保机密性、完美前向安全、抗位置伪造攻击等关键安全属性。

3) 结合模糊提取器和用户密码，实现登录阶段的双因素验证、密码和生物特征更新功能，并采用密码学动态累加器提供有效的用户撤销策略，使本文协议安全功能更加完善。

4) ROR（real-or-random）模型和Scyther形式化验证工具证明了本文协议的逻辑正确性及语义安全。与近几年协议的性能对比分析表明，本文协议平均减少了约35.9%的通信开销和29.9%的计算开销，具有一定的性能优势。

1 相关工作

为解决V2G网络的安全和隐私保护问题，已提出许多认证协议。Saxena等[6]基于双因素认证，实现了车辆、注册中心和聚合器的相互认证，并通过双线性配对技术与动态累加器实现了对车辆的批量验证。Irshad等[7]结合模糊提取器技术提出了一种基于能源互联网的V2G通信架构安全模型，能够抵抗多种安全攻击。Shen等[8]提出了一种支持批量验证V2G网络能源交易的可追溯和隐私保护认证协议，采用二叉树遍历的方法快速跟踪具有非法签名的电动汽车。但上述协议都运用了双线性映射技术，额外增加了实体的运算开销，因此不适用于资源有限的V2G环境，且Reddy等[4]指出Irshad等[7]的方案不能抵御中间人攻击、特权内部攻击等安全攻击。Su等[9]为解决系统主密钥由受信任的第三方独立生成时存在主密钥泄露的问题，提出了一种基于非超奇椭圆曲线的V2G网络隐私保护认证协议，该协议采用一个密钥协议来生成系统主密钥，并为电动汽车提供假名身份来保护身份隐私，但Sureshkumar等[10]指出该协议不满足物理安全和完美前向安全。

为保障实体能抵抗物理攻击，近年来提出了一些基于PUF的V2G认证协议。Bansal等[11]设计了2个基于物理不可克隆函数的高效协议，用于电动汽车、电网服务器和聚合器之间的密钥协商。但协议中直接将激励响应对显式存储在电网服务器的数据库中，可能导致攻击者对CRP进行建模，从而造

成机器学习建模攻击[12]。Gope 等[13]提出了一种基于 PUF 的可重构认证协议，以提供智能电网环境下的安全通信。PUF 的可重构特性避免了协议遭受 ML 建模攻击，但他们的协议不支持用户撤销、密码或生物特征更新等功能。Sureshkumar 等[14]为 V2G 网络设计了一种具有条件隐私保护鲁棒的认证密钥交换协议，以提供可靠的能源服务，但 Yu 等[15]指出他们的协议无法抵抗密钥泄露、冒充攻击和智能设备被盗攻击。

针对 V2G 网络设备资源有限问题，也有许多学者对此展开了研究。Abdallah 等[16]提出了一种轻量级 V2G 协议，该协议通过电动汽车私有凭证产生静态假名，适用于资源受限的车辆。但由于没有提供密码更新阶段，无法实现完美前向安全和抵抗去同步攻击。Gope 等[17]采用单向散列函数等轻量级密码原语保证车网安全通信，但协议在用户登录阶段可能会遭受去同步攻击，且敌手可以在开放信道上选取合法信息对车辆进行重放攻击与中间人攻击。Hassija 等[18]提出了一种基于区块链的轻量级 V2G 网络数据共享和能源交易框架，以安全和可扩展的方式记录 V2G 网络中越发频繁的交易，但低效的区块生成机制会导致数据处理的时延过高，海量的数据也会给区块链节点带来巨大的存储压力。Hou 等[19]使用 ASCON 对称加密算法，实现充电预约过程中 EV 与充电桩（CS, charging station）之间的安全通信，但该协议是专门为 5G-V2G 网络环境设计的，可能不适用于其他场景，且无法对恶意车辆进行追踪。

综上所述，现有许多采用双线性配对、椭圆曲线加密、哈希函数、物理不可克隆函数等密码原语的 V2G 身份认证协议，但大都无法同时满足有条件的隐私保护、轻量级认证、用户撤销、密钥更新等安全需求，因此亟须提出一种新的认证协议与密钥协商协议来克服当前 V2G 认证协议中的一些性能和安全问题。

2　理论知识

2.1　物理不可克隆函数

PUF 是一种集成电路，由 Pappu 等[20]提出，其依赖芯片制造过程中引入的固有随机物理因素产生器件独有的数字签名，具有低功耗、快速响应、鲁棒性、不可预测性、防篡改性[21]等特质，已成为一种新型的轻量级安全原语。PUF 按产生 CRP 的数量又分为强 PUF 和弱 PUF 这 2 种，强 PUF 可以生成大量的 CRP，非常适用于身份验证，但同时也容易受到建模攻击。

设激励信息 $C \in \{0,1\}^n$，响应信息 $R \in \{0,1\}^k$，PUF 利用密码学技术实现的激励−响应机制如式(1)所示。

$$R = \mathrm{PUF}(C) \tag{1}$$

PUF 具有以下特性。

1) 每个 PUF 都是唯一且不可克隆的，对同一个 PUF 输入 2 个不同的激励，会产生不同的响应。

2) 输入相同激励，不同的 PUF 会得到不同响应。

3) 任何篡改 PUF 的行为都将导致 PUF 无效。

当 PUF 用于身份验证时，首先在注册阶段由验证方向终端设备发起 PUF 激励，终端设备再根据激励生成 PUF 响应，并将 CRP 传输给验证方进行存储。在验证过程中，验证方发送相同的激励，并比对终端设备返回的响应与存储的响应是否一致，以验证终端设备的合法性和身份的真实性。

不同类型 PUF 的 CRP 提取方法并不一样，如作为强 PUF 的仲裁 PUF，电路由多个延迟链和仲裁器组成，将一个特定长度的二进制序列作为激励输入 PUF 电路中，通过比较信号在不同路径上的传输时延得出固定长度的二进制响应序列，且可通过模糊提取器内置的纠错算法解决 PUF 的噪声问题，最后生成稳定且唯一的激励响应对。

2.2　ASCON 加密算法

带关联数据的认证加密（AEAD, authenticated encryption with associated data）算法 ASCON[22]能够在不使用消息验证码的情况下同时提供数据的完整性、真实性和机密性，专为资源受限的设备设计。ASCON 算法的加密过程如式(2)所示。

$$(\mathrm{CTxt}, \mathrm{APauth}) = E_k(N, \mathrm{AD}, \mathrm{PTxt}) \tag{2}$$

其中，E 表示加密过程，该过程以密钥 k、随机数 N、关联数据 AD 以及任意长度的明文 PTxt 作为输入。以与明文 PTxt 长度相同的密文 CTxt 和认证参数 APauth 作为输出。ASCON 算法的解密过程如式(3)所示。

$$(\mathrm{PTxt}, \mathrm{APauth}') = D_k(N, \mathrm{AD}, \mathrm{CTxt}) \tag{3}$$

其中，D 表示解密过程，该过程的输入与加密过程类似，以明文 PTxt 和认证参数 APauth' 作为输出，

通过检查公式 $APauth \stackrel{?}{=} APauth'$，来验证得到的明文 PTxt 的正确性。

2.3 密码学累加器

密码学累加器是一种时间和空间高效的数据结构，可用于集合内成员关系验证，且在时间戳、成员资格撤销、区块链等[23]场景中都有着广泛的应用。累加器有不同的类型和构造，可分为静态、动态和通用累加器 3 种。一个基本的动态累加器通常包括以下算法。

1) 密钥生成算法 $\mathrm{Gen}(1^{\lambda})$。输入累加器安全参数 λ 和一组成员 X，输出初始累加器值 acc_0 和累加器参数 Para，即 $\mathrm{Gen}(1^{\lambda},X) \rightarrow (\mathrm{acc}_0, \mathrm{Para})$。

2) 成员添加算法 Add (·)。输入参数 Para、累加器值 acc_1 和成员 m_1，其中 $m_1 \notin X$，执行该算法后输出 $m_1 \in X$ 的成员证明 w_1，即 $\mathrm{Add}(\mathrm{Para}, \mathrm{acc}_1, m_1) \rightarrow w_1$。

3) 成员删除算法 Del (·)。成员 $m_2 \in X$，将 m_2 从集合 X 中删除，即 $\mathrm{Del}(\mathrm{Para}, \mathrm{acc}_2, m_2) \rightarrow \mathrm{acc}_2^*$。

4) 成员更新算法 WitUpOnDel (·)。输出成员 m_3 新的成员证明 w_3^*，即 $\mathrm{WitUpOnDel}(w_3, \mathrm{acc}_3) \rightarrow w_3^*$。

5) 成员验证算法 Ver (·)。输入累加器参数 Para、累加器值 acc_4、成员 m_4 和成员证明 w_4，可判断成员 m_4 是否属于集合 X，即 $\mathrm{Ver}(\mathrm{Para}, \mathrm{acc}_4, w_4, m_4) \rightarrow 0/1$。

3 系统模型与安全需求

3.1 系统模型

电动汽车用户通过 V2G 网络可使用充放电服务，本文协议的 V2G 系统模型如图 1 所示，主要由电动汽车、充电桩、能源提供商 3 个通信实体组成。

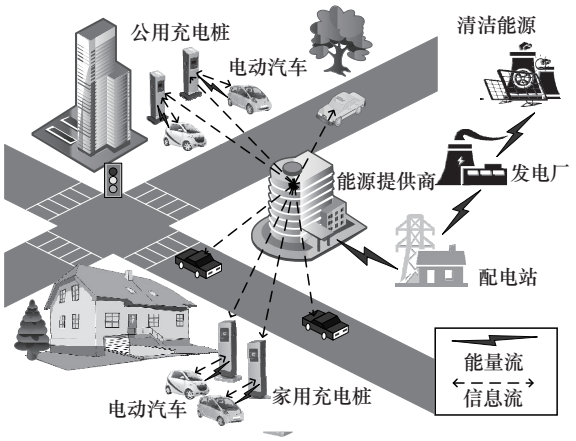


图 1 V2G 系统模型

EV 配备有双向充电器、PUF、车载单元（OBU, on broad unit）等硬件设备，可按需进行充放电服务，通过无线信道与充电桩进行数据通信。

CS 的充电速率取决于它所在的位置[24]，EV 可以在离它最近的任何一个 CS 进行充电。在相互认证阶段，EV 和 CS 都会向 EP 提供其地理位置，以便于能源提供商确定它们的位置。

发电厂将风能、太阳能等清洁能源转化成电能输送给配电站，EP 把来自配电站的电力提供给安装在不同位置的 CS，负责对电动汽车用户和充电桩进行注册，并将所有注册的关键数据保存在自己的数据中心。

3.2 安全威胁

本文采用的威胁模型是 Dolev 等[25]提出的攻击者模型，在本文协议中的攻击者 A 具有以下能力。

1) 通过公共通道获取、窃听、修改、删除或重发通信实体间传输的消息。

2) 对设备进行物理攻击，获取秘密数据。

3) 还可能进行假冒攻击、离线密码猜测攻击、特权内部攻击等安全攻击。

3.3 安全需求

为保证 V2G 网络的通信安全，本文协议应满足以下安全需求。

1) 匿名性。当 EV 与 CS 或 EP 进行通信时，通过不断更新假名来保护车辆真实身份，减少隐私泄露的风险，实现匿名身份认证。

2) 不可追溯性。本文协议应保持车辆的不可追溯性，使攻击者无法区分两条不同的带有匿名身份的信息是来自同一车辆还是两辆不同车辆。

3) 相互认证。为防止非法实体进行冒充攻击或中间人攻击，本文协议需提供实体间的相互认证。

4) 会话密钥安全。由于车辆会多次与 CS 进行电力交互，所以生成的会话密钥必须具备前向安全性，保证当前和未来的通信安全。

5) 用户撤销。有恶意行为和不再需要 V2G 网络服务的用户都必须从注册用户列表中删除，因此本文协议需包含一个有效的用户撤销策略。

6) 密码和生物特征更新功能。用户有自由变更密码和生物特征信息的权利。

4 协议设计

本节将分 6 个部分详细介绍本文协议，包括系

统初始化阶段、注册阶段、登录阶段、认证与密钥协商阶段、密码和生物特征更新阶段、用户撤销阶段。本文协议中部分符号定义如表 1 所示。

表 1　　符号定义

符号	定义
ID_i, ID_j	EV_i 和 CS_j 的身份标识符
K_e, K_i, K_j	EP，EV_i，CS_j 的秘密参数
SK	会话密钥
n_1, n_2, n_3, r_e	随机数
PID_i, EID_i	EV_i 的假名身份和加密身份
$< C_i, R_i >$	EV_i 的激励响应对
Gen (·)	模糊提取器生成算法
Rep (·)	模糊提取器再现算法
T_i, T_{max}	时间戳，最大允许时延
L_i, L_j	EV_i 和 CS_j 的位置标识符
‖, ⊕	级联和异或
$h(\cdot)$	哈希函数
k_i	对称密钥
ACD (·), ACE (·)	ASCON 对称加密和对称解密函数

4.1　系统初始化阶段

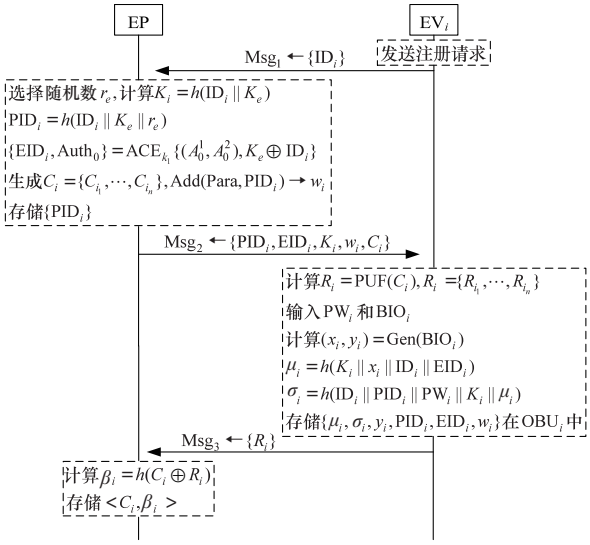
首先 EP 生成自己的长期密钥 K_e，选择单向抗碰撞哈希函数 $h(\cdot)$，存储在注册阶段的 EV_i 和 CS_j 中，其中 $h(\cdot)$ 使用 SM3。EP 调用累加器密钥生成算法生成初始累加器值 acc_0 和累加器参数 Para，即 $Gen(1^{\lambda}, V) \rightarrow (acc_0, Para)$，$V$ 为一组已注册的车辆集合，EP 保存参数 $\{acc_0, Para\}$，并将其发送给注册阶段的 CS_j 进行存储。

4.2　注册阶段

1) 车辆注册

为保证信息的安全传输，每个电动车辆用户都通过安全通道在 EP 上注册他的车辆 EV_i，EV 注册阶段步骤如图 2 所示。

首先 EV_i 使用其独特的身份标识符 ID_i 向 EP 发送注册请求。EP 在收到注册请求后，生成一个随机数 r_e 和一系列激励 C_i，并计算车辆的秘密参数 K_i。为了隐藏用户身份，EP 为车辆生成假名身份 PID_i，采用 128 bit 的 ASCON 算法生成车辆加密身份 EID_i，其中 $A_0 = h(K_e)$，将 A_0 平均分成 A_0^1 和 A_0^2 两部分，分别作为 ASCON 算法的随机数和关联数据，$k_0 = A_0^1 \oplus A_0^2$。为保证 EV_i 假名身份的有效性和合法性，EP 为 PID_i 生成一个成员见证人 w_i，其中 $PID_i \notin V$，并将消息 Msg_2 发送给 EV_i。



EV_i 收到 C_i 后通过内嵌在 OBU_i 中的 PUF 生成响应 R_i，由于 PUF 的防篡改特性，可有效防止设备遭受物理攻击。车辆用户选择一个密码 PW_i，在移动设备上输入其生物特征 BIO_i，使用模糊提取器生成秘密参数 x_i 和复制参数 y_i，并计算 $\{\mu_i, \sigma_i\}$。EV_i 将参数 $\{\mu_i, \sigma_i, y_i, PID_i, EID_i, w_i\}$ 保存在内存中，并将 R_i 发送给 EP。

EP 收到 R_i 后利用哈希函数处理 CRP 得到 β_i，并将 $\{< C_i, \beta_i >, PID_i\}$ 用 K_e 加密后保存在数据库中。

2) 充电桩注册

CS_j 在部署之前需要注册，首先 EP 为每个 CS_j 都选择一个身份标识符 ID_j，并计算其秘密参数 $K_j = h(ID_j \| K_e)$，然后将 $\{ID_j, K_j, acc_i, Para\}$ 发送给 CS_j 进行安全存储。

4.3　登录阶段

车辆用户首先输入身份标识符 ID_i，密码 PW_i 和生物特征 BIO_i'，再现秘密参数 x_i'，并计算 μ_i' 和 σ_i'。如果 $\sigma_i' = \sigma_i$，则代表在密码和生物特征双因素保护下成功登录。

4.4　认证与密钥协商阶段

当 EV_i 想要使用 V2G 网络的服务时，车辆必须与 CS_j 和 EP 进行相互认证，此阶段在不安全的开放通道上进行，详细说明如图 3 所示，具体步骤如下。

图3 认证与密钥协商阶段步骤

步骤 1 为抵抗重放攻击，EV_i生成一个随机数n_1和当前时间戳T_1，计算参数B_1和B_2，并将消息M_1发送给CS_j。

步骤 2 CS_j收到EV_i的消息后，生成随机数n_2和时间戳T_2，检查$|T_2 - T_1| \leqslant T_{max}$是否成立，如果成立则继续，否则终止认证。$CS_j$调用成员验证算法来确定车辆是否已注册且合法，即计算$Ver(Para, acc_0, w_i, PID_i)$，若结果为1则代表假名未被撤销，则继续认证。然后$CS_j$计算参数$B_3$和$B_4$，为应对V2G设备计算资源有限的情况，降低通信开

销，利用 ASCON 算法对 PM_1 进行加密，其中 $A_1 = h(K_j)$，$k_1 = A_1^1 \oplus A_1^2$，最后 CS_j 将消息 M_2 发送给 EP。

步骤 3　EP 收到消息 M_2 后，生成 T_3 并检查 T_2 的有效性，通过对比数据库验证 ID_j 是否合法，如果合法则继续认证。EP 解密消息 CM_1 和 EID_i 得到车辆真实身份标识符 ID_i，再计算参数 K_i' 和 K_j'。EP 通过对比 2 个位置标识符 L_i 和 L_j 是否一致来防止敌手进行位置伪造攻击，若不一致则终止认证。然后计算并验证 $B_4' \stackrel{?}{=} B_4$，如果相等则继续认证。为保证车辆的匿名性和不可链接性，EP 选择一个新的随机数 r_e^* 和一对激励响应对 $< C_i^*, \beta_i^* >$，为 EV_i 计算新的假名 PID_i^* 和成员见证人 w_i^*，生成会话密钥 $SK = h(PID_i^* \| ID_j \| n_1 \| n_2 \| r_e^*)$。随后 EP 计算参数 $\{B_5, B_6, B_7, B_8, B_9\}$，并对 PM_2 进行对称加密。ASCON 算法计算时间复杂度仅为 $O(1)$，在保证数据完整性和保密性的同时，避免了采用非对称加密算法所需的大量时间和资源，满足轻量级应用需求，其中 $A_2 = h(\beta_i^*)$，$k_2 = A_2^1 \oplus A_2^2$，最后 EP 将消息 M_3 发送给 CS_j。

步骤 4　CS_j 收到消息 M_3 后，首先生成当前时间戳 T_4，并计算 $|T_4 - T_3| \leqslant T_{\max}$ 是否成立，如果成立则继续验证，计算出会话密钥 SK，并验证 $B_7' \stackrel{?}{=} B_7$ 是否成立，如果成立则将消息 M_4 发送给 EV_i。

步骤 5　EV_i 收到 M_4 后先验证其有效性，通过 PUF 得到激励 R_i^*，以此计算 β_i^* 来解密消息 CM_2，计算出会话密钥 SK 后验证 $B_9' \stackrel{?}{=} B_9$，如果相等则代表三方认证与密钥协商成功。EV_i 用 PID_i^* 和 w_i^* 更新 PID_i 和 w_i，为下次安全通信做准备。

4.5　密码和生物特征更新阶段

EV_i 用户首先执行 4.3 节的登录阶段，成功登录后，EP 通知 EV_i 输入新的密码 PW_i^* 和新的生物特征 BIO_i^*，得到 $(x_i^*, y_i^*) = Gen(BIO_i^*)$，$EV_i$ 再计算 $\mu_i^* = h(K_i \| x_i^* \| ID_i \| EID_i)$，$\sigma_i^* = h(ID_i \| PID_i \| PW_i^* \| K_i \| \mu_i')$。最后 EV_i 用 $\{y_i^*, \mu_i^*, \sigma_i^*\}$ 替换 $\{y_i, \mu_i, \sigma_i\}$ 完成密码和生物特征更新。

4.6　用户撤销阶段

当车辆存在恶意行为时，EP 可以对 EV_i 进行撤销。EP 调用成员删除算法，将用户从累加器中移除，即 $Del(Para, acc_0, PID_i) \to (acc^*)$，$EV_i$ 对应的成员见证人 w_i 也会作废，EP 将新的累加器值 acc^* 广播给所有的 CS 和车辆，CS 会更新存储的累加器值，EV 会执行成员更新算法对自己的成员证明进行更新，即 $WitUpOnDel(w_i, acc^*) \to w_i^*$。当用户不再需要 V2G 网络的服务时，用户也可以向 EP 提出撤销申请。

5　安全分析

5.1　基于 ROR 的形式化证明

由 Abdalla 等[26]提出的 ROR 是在可证明安全性分析中被广泛采用的一种安全模型，敌手 A 可以在多项式时间 t 内对协议进行攻击，在本文提出的认证模型中有 3 个实体：车辆 EV_i、充电桩 CS_j 和能源提供商 EP，每类实体都包含若干个实例，用 $\prod_{EV_i}^{s_1}$、$\prod_{CS_j}^{s_2}$ 和 $\prod_{EP}^{s_3}$ 分别表示 EV_i、CS_j 和 EP 的第 s_1、s_2 和 s_3 个实例，并且敌手 A 可以进行以下查询。在这些查询的帮助下，敌手 A 可以窃取、篡改和删除在不安全信道传输的数据。

1) Execute $(\prod_{EV_i}^{s_1}, \prod_{CS_j}^{s_2}, \prod_{EP}^{s_3})$。执行此查询时，$A$ 可模拟窃听攻击，获得实体间交换的所有信息。

2) Send $(\prod_X^s, m)$。执行此查询时，A 可以模拟主动攻击，向实体 $\prod_{EV_i}^{s}$ 发送消息 m，并获得来自实体反馈的消息。

3) CorruptEV $(\prod_{EV_i}^{s_1})$。执行此查询时，A 可以提取存储在 EV_i 内存中的所有信息。

4) CorruptCS $(\prod_{CS_j}^{s_2})$。执行此查询时，A 可以获得存储在 CS_j 内存中的秘密参数。

5) Hash (i)。在本文协议中使用的哈希函数都被建模为随机预言机，A 可以通过多个哈希查询来验证是否存在哈希冲突。

6) PUF (i)。将 PUF 也建模为随机预言机，A 可以通过 PUF 查询来访问随机预言机。

7) Test $(\prod_X^s)$。该查询是模拟实体之间会话密钥语义安全的模型，在游戏开始之前将随机生成一个比特 B，其输出结果对 A 是保密的。当 A 执行此查询后，若 B=1，则返回真实会话密钥；若 B=0，则返回一个与会话密钥等长的随机数。

定理 1　设 A 为本文协议的敌手，本文协议在多项式时间 t 内运行，若 A 不能以可忽略的优势成功攻击本文协议，则认为本文协议是安全的。假设

A破坏本文协议会话密钥安全性的优势为

$$\mathrm{Adv}_A^P \leqslant \frac{q_\mathrm{h}^2}{2^{l_\mathrm{s}}} + \frac{q_\mathrm{p}^2}{2^{l_\mathrm{p}}} + \frac{2(q_\mathrm{s}+q_\mathrm{e})^2}{N} + \frac{q_\mathrm{s}}{2^{l-1}|D|} \tag{4}$$

其中，q_h、q_s、q_e和q_p分别表示执行Hash查询、Send查询、Execute查询和Puf查询的次数，N代表随机数的空间范围，l_s表示哈希函数的输出长度，l_p表示PUF输出响应的长度，l表示生物密钥x_i的位数，$|D|$表示密码字典的空间范围。

证明 下面定义了6个游戏$\mathrm{GM}_i(i\in[0,5])$来证明本文协议的安全性，$\Pr[\mathrm{Succ}_i]$表示敌手A在游戏GM_i中获胜的概率。

1) GM_0。这个游戏模拟了对本文协议P的实际攻击，A成功猜测出B的概率为

$$\mathrm{Adv}_A^P \leqslant |2\Pr[\mathrm{Succ}_0]-1| \tag{5}$$

2) GM_1。在GM_1中，A执行Execute查询在一个开放信道上进行窃听攻击，拦截登录和认证过程中的所有交换信息，再执行Test查询以确认输出的是一个真实的会话密钥还是一个随机数。在本文协议中A不能得到参数$\{\mathrm{PID}_i^*,n_1,n_2,r_e^*\}$，所有$A$在$\mathrm{GM}_1$中获胜的概率没有增加，即

$$\Pr[\mathrm{Succ}_1]=\Pr[\mathrm{Succ}_0] \tag{6}$$

3) GM_2。A增加Hash查询和Send查询次数，模拟在认证阶段的哈希碰撞和随机数碰撞，本文协议的会话密钥采用了哈希函数和随机数，所以根据生日悖论，哈希碰撞的概率为$\frac{q_\mathrm{h}^2}{2^{l_\mathrm{s}+1}}$，随机数碰撞的概率为$\frac{(q_\mathrm{s}+q_\mathrm{e})^2}{2N}$，可得

$$|\Pr[\mathrm{Succ}_1]-\Pr[\mathrm{Succ}_2]| \leqslant \frac{q_\mathrm{h}^2}{2^{l_\mathrm{s}+1}} + \frac{(q_\mathrm{s}+q_\mathrm{e})^2}{2N} \tag{7}$$

4) GM_3。这个游戏是GM_2的扩展，其中包括PUF查询，基于GM_2引入类似论证，可知本游戏结果为

$$|\Pr[\mathrm{Succ}_2]-\Pr[\mathrm{Succ}_3]| \leqslant \frac{q_\mathrm{h}^2}{2^{l_\mathrm{p}+1}} \tag{8}$$

5) GM_4。在这个游戏中，A通过CorruptEV查询来模拟电动汽车丢失或被盗攻击，A可得到参数$\{\mu_i,\sigma_i,y_i,\mathrm{PID}_i,\mathrm{EID}_i,w_i\}$。$A$可以根据得到的参数来猜测用户设置的密码$\mathrm{PW}_i$以及生物密钥$x_i$。其中$\mu_i=h(K_i\|x_i\|\mathrm{ID}_i\|\mathrm{EID}_i)$，本文协议通过模糊提取器来提取生物密钥$x_i$，$x_i\in\{0,1\}^l$，所以$A$猜中生物密钥$x_i$的概率为$\frac{1}{2^l}$。假设$A$可以使用最优猜测密码策略，对于猜测的每个密码，必须用$\sigma_i=h(\mathrm{ID}_i\|\mathrm{PID}_i\|\mathrm{PW}_i\|K_i\|\mu_i)$来验证其正确性，其中由于$\sigma_i$包含许多秘密参数，所以$A$无法执行密码验证，可得

$$|\Pr[\mathrm{Succ}_3]-\Pr[\mathrm{Succ}_4]| \leqslant \frac{q^s}{2^l|D|} \tag{9}$$

6) GM_5。A通过CorruptCS查询可以提取存储在CS_j中的$\{\mathrm{ID}_j,K_j\}$，假设A窃听了交换过程中的所有消息，基于这些消息A也不能计算出会话密钥SK，A在这个游戏中没有增加任何优势，由此可得

$$\Pr[\mathrm{Succ}_5]=\Pr[\mathrm{Succ}_4] \tag{10}$$

在提交所有查询后，A需要进行猜测比特B来赢得$\mathrm{Test}(\prod_{\mathrm{EV}_i}^{s_1},\prod_{\mathrm{CS}_j}^{s_2})$游戏，可得

$$\Pr[\mathrm{Succ}_5]=\frac{1}{2} \tag{11}$$

根据式(4)~式(11)可得

$$\begin{aligned}&\frac{1}{2}\mathrm{Adv}_A^P=\left|\Pr[\mathrm{Succ}_0]-\frac{1}{2}\right|=\\&\left|\Pr[\mathrm{Succ}_1]-\Pr[\mathrm{Succ}_5]\right|\leqslant\\&\frac{q_\mathrm{h}^2}{2^{l_\mathrm{s}+1}}+\frac{(q_\mathrm{s}+q_\mathrm{e})^2}{2N}+\frac{q_\mathrm{p}^2}{2^{l_\mathrm{p}+1}}+\frac{q_\mathrm{s}}{2^l|D|}\end{aligned} \tag{12}$$

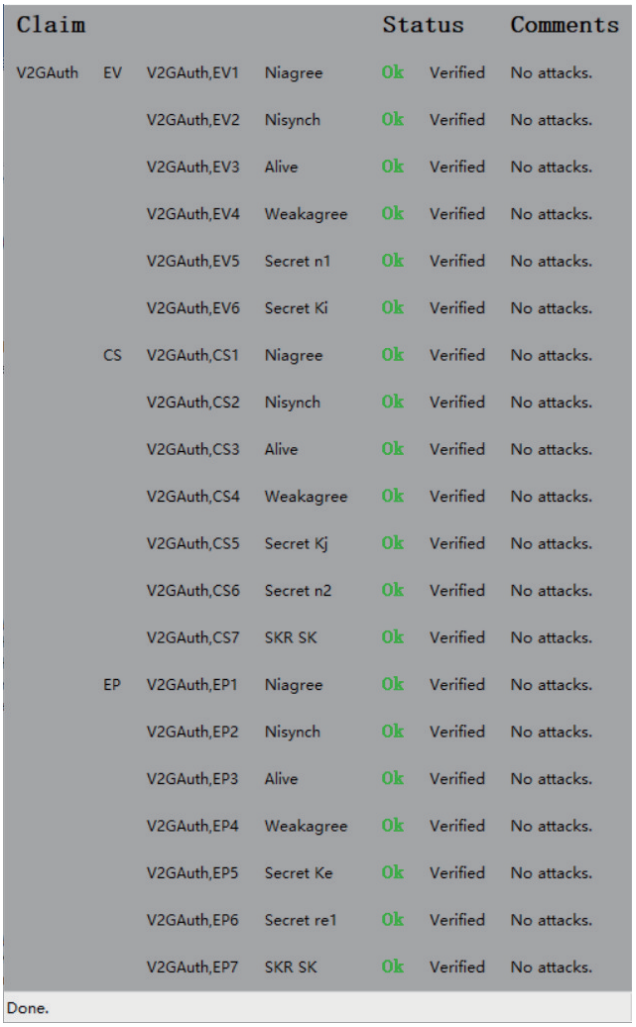
进一步推导可知，敌手A获胜的优势为

$$\mathrm{Adv}_A^P \leqslant \frac{q_\mathrm{h}^2}{2^{l_\mathrm{s}}} + \frac{(q_\mathrm{s}+q_\mathrm{e})^2}{N} + \frac{q_\mathrm{p}^2}{2^{l_\mathrm{p}}} + \frac{q_\mathrm{s}}{2^{l-1}|D|} \tag{13}$$

证毕。

5.2 基于Scyther的安全分析

Cremers[27]提出的Scyther软件是一种形式化的安全协议分析工具，采用安全协议描述语言（SPDL, secure protocol description language）来实现本文协议，其安全属性包括同步性、一致性、弱一致性和有效性。利用Scyther工具在Dolev-Yao攻击者模型下对本文协议进行分析，指定EV、CS和EP作为协议安全验证的角色，将Scyther工具设置为高级选项运行本文协议100次，以便为每个请求查找潜在攻击的多种模式。Scyther形式化分析结果如图4所示。从图4中可知，没有检测到任何潜在攻击。本文协议满足安全要求，且密钥参数和生成的会话密钥SK是保密的。



Claim				Status		Comments
V2GAuth	EV	V2GAuth,EV1	Niagree	Ok	Verified	No attacks.
		V2GAuth,EV2	Nisynch	Ok	Verified	No attacks.
		V2GAuth,EV3	Alive	Ok	Verified	No attacks.
		V2GAuth,EV4	Weakagree	Ok	Verified	No attacks.
		V2GAuth,EV5	Secret n1	Ok	Verified	No attacks.
		V2GAuth,EV6	Secret Ki	Ok	Verified	No attacks.
	CS	V2GAuth,CS1	Niagree	Ok	Verified	No attacks.
		V2GAuth,CS2	Nisynch	Ok	Verified	No attacks.
		V2GAuth,CS3	Alive	Ok	Verified	No attacks.
		V2GAuth,CS4	Weakagree	Ok	Verified	No attacks.
		V2GAuth,CS5	Secret Kj	Ok	Verified	No attacks.
		V2GAuth,CS6	Secret n2	Ok	Verified	No attacks.
		V2GAuth,CS7	SKR SK	Ok	Verified	No attacks.
	EP	V2GAuth,EP1	Niagree	Ok	Verified	No attacks.
		V2GAuth,EP2	Nisynch	Ok	Verified	No attacks.
		V2GAuth,EP3	Alive	Ok	Verified	No attacks.
		V2GAuth,EP4	Weakagree	Ok	Verified	No attacks.
		V2GAuth,EP5	Secret Ke	Ok	Verified	No attacks.
		V2GAuth,EP6	Secret re1	Ok	Verified	No attacks.
		V2GAuth,EP7	SKR SK	Ok	Verified	No attacks.

Done.

图4　Scyther形式化分析结果

5.3　非形式化安全分析

1) 抗物理攻击。假设攻击者A物理捕获了EV_i的OBU_i，并试图通过存储在其内存中的$\mu_i = h(K_i||x_i||ID_i||EID_i)$来猜测其身份标识符$ID_i$、秘密参数$K_i$和$x_i$，由于哈希函数的保护，$A$没有猜测优势，且由于$EV_i$的每个$OBU_i$都配备了PUF，$A$对$OBU_i$进行的任何篡改都会影响PUF输出响应的正确性，使会话密钥协商失败，所以本文协议可以抵抗OBU_i物理攻击。

2) 相互认证。在本文协议中，CS_j首先通过累加器对EV_i进行合法性验证，EP再通过计算B_4对CS_j进行认证。当CS_j收到EP的消息M_3时，通过计算B_7对EP进行认证。当EV_i收到CS_j的消息M_4时，通过验证B_9对CS_j进行认证，由于这些验证参数中都包含各实体的秘密参数，所以A不能通过这些验证，可见本文协议能实现实体之间的相互认证。

3) 抗模拟攻击。若A伪造消息M_2: $\{CM_1, ID_j, T_2\}$，则A可通过EP的验证，但由于A无法获得生成消息M_2所需的秘密参数n_2和K_j，所以A无法模拟合法的CS_j，即本文协议可以抵抗CS_j模拟攻击。同理，本文协议可以抵抗EV_i模拟攻击和EP模拟攻击。

4) 匿名性。当A截获公共信道的消息后，想从这些消息中推断出EV_i的真实身份ID_i，但在这些消息中ID_i都在哈希函数中隐式存在。在消息M_1中$B_1 = h(PID_i||ID_e) \oplus (EID_i||n_1)$，$EID_i$是$ID_i$由EP的密钥$K_e$进行加密的，所以只有EP可以知道$EV_i$的真实身份，且并未对$ID_i$进行存储。所以本文协议满足$EV_i$匿名性。

5) 抗离线密码猜测攻击。A可以捕获存储在车辆OBU_i中的信息$\{\mu_i, \sigma_i, y_i, PID_i, EID_i, w_i\}$，其中$\sigma_i = h(ID_i||PID_i||PW_i||K_i||\mu_i)$。$A$通过验证$\sigma_i$来猜测用户密码$PW_i$，但由于不知道秘密参数$K_i$和车辆身份$ID_i$，所以无法进行抗离线密码猜测攻击。

6) 完美前向安全。在本文协议中，假设敌手A得到一个会话密钥$SK = h(PID_i^*||ID_j||n_1||n_2||r_e^*)$，且$EV_i$的长期秘密参数$\{ID_i, K_i, x_i\}$之一被泄露，但由于$\{n_1, n_2, r_e, PID_i\}$在每轮认证中都不相同，所以$A$无法通过SK获得以前的会话密钥，保证完美前向安全。

7) 抗位置伪造攻击。充电站的电价随所处位置而有所不同，不诚实的用户或充电站可能会向EP提供虚假位置进行破坏，本文协议中当EP收到消息M_2时，会对EV_i和CS_j的位置L_i和L_j进行比较，若二者一致则继续认证，否则终止认证。因此，本文协议可以抵抗位置伪造攻击。

8) 抗重放攻击。A可能会捕获在不同实体之间传输的消息，并重放该消息以获得身份认证。在本文协议中所有消息含有时间戳T_i、随机数n_i和r_e，每个实体在认证之前会检查$|T_i - T_{i-1}| \leqslant T_{max}$，且在每次会话密钥协商结束之后还会更新$PID_i$和$w_i$，使得敌手$A$无法重放消息，所以该协议可以抵抗重放攻击。

9) 抗特权内部攻击。即使有特权的内部攻击者A窃取了用户在注册阶段的消息$\{ID_i, R_i\}$，并从车辆OBU_i中提取到信息$\{\mu_i, \sigma_i, y_i, PID_i, EID_i, w_i\}$，但因为$A$不知道车辆秘密参数$K_i$、密码$PW_i$和生物密

钥x_i，所以A也不能计算出μ_i和σ_i，因此本文协议对特权内部攻击是安全的。

10) 抗ML建模攻击。若A收集EV_i的大量激励响应对$<C_i,R_i>$，采用机器学习对PUF进行建模，预测新激励的响应，则可造成ML建模攻击。在本文协议中，车辆EV_i并不存储CRP，CRP只以$<C_i,h(C_i\oplus R_i)>$的形式存储在EP中，由于哈希函数的单向性，攻击者很难根据$h(C_i\oplus R_i)$猜测出R_i，若R_i的位数足够长[28]（如128 bit），则A猜测的优势可忽略不计，所以本文协议可以抵抗ML建模攻击。

11) 抗中间人攻击。在本文协议中，假设A拦截了消息$M_1\sim M_4$，A要执行中间人攻击，必须修改被窃听的消息使其合法。若敌手要修改消息M_3: $\{B_5,B_6,B_7,\mathrm{CM}_2,C_i^*,T_3\}$，其中，$A$可以生成一个激励$C_i^*$和时间戳$T_3$，但由于不知道$K_j$和$L_j$，其中$B_7=h(\mathrm{ID}_j\|K_j\|L_j\|\mathrm{CM}_2\|C_i^*\|T_3)$，所以无法生成合法的消息$M_3$，$A$不能作为合法$\mathrm{CS}_j$去欺骗EV，同理也不能正确修改其他消息。因此，本文协议对中间人攻击是安全的。

12) 不可追溯性。当A捕获消息M_1: $\{B_1,B_2,\mathrm{PID}_i,w_i,T_1\}$后，只能知道EP为$\mathrm{EV}_i$生成的假名身份$\mathrm{PID}_i$，且在每次会话后$\mathrm{PID}_i$会被更新，所以$A$无法将某次会话与特定$\mathrm{EV}_i$关联起来，即本文协议具有不可追溯性。

综上所述，本文协议在ROR模型的证明和Scyther形式化分析工具的验证下均满足安全性。此外，通过非形式化的安全分析可以得出，本文协议具备相互认证、匿名性、完美前向安全以及抗重放攻击等属性。

6 性能分析

本节将从安全功能、计算开销和通信开销3个方面对本文协议进行分析，并与文献[7]、文献[9]、文献[14]、文献[15]和文献[29]的协议进行对比，最终得出，本文协议在综合性能上具有较大优势，适用于资源受限的V2G网络环境。

6.1 安全功能对比

将本文协议与其他协议的安全功能进行对比，结果如表2所示。由表2可知，对比文献中所有协议满足抗密码猜测攻击和抗重放攻击。文献[7]、文献[9]、文献[14]和文献[29]都将关键信息存储在设备内存中，攻击者可以通过物理攻击来获取设备内存中的信息，但没有PUF的保护，容易遭受物理攻击。本文协议在PUF不可篡改特性的保护下可以抵抗物理攻击，且将激励响应对隐式存储，可抵抗ML建模攻击。文献[9]仅提供两方身份认证，不支持三方身份验证，且无法抵抗模拟攻击、特权内部攻击等重要安全攻击。由于文献[9]、文献[14]、文献[15]和文献[29]中的协议均未对车辆和充电桩的位置信息进行比对，容易遭受位置伪造攻击。因此，本文协议对各种安全攻击具有鲁棒性，能提供更好的安全功能。

6.2 计算开销

本节评估了本文协议的计算开销，并与其他协议的计算开销进行了比较。本文使用一台配置为Intel(R) Core(TM) i7-8850U CPU，8.0G RAM的电脑对各种加密原语进行运算，使用四核1.2 GHz和1 GB RAM的Raspberry Pi-3来评估PUF的计算开销[28]。表3给出了各种密码原语的执行时间。

表2 安全功能对比

协议	抗物理攻击	相互认证	抗模拟攻击	匿名性	抗离线密码猜测攻击	完美前向安全	抗位置伪造攻击	抗重放攻击	抗特权内部攻击	抗ML建模攻击	抗中间人攻击	不可追溯性
文献[7]	×	√	×	×	√	×	√	√	×	×	×	×
文献[9]	×	×	×	√	√	×	×	√	×	×	×	√
文献[14]	×	√	×	√	√	√	×	√	√	×	√	√
文献[15]	√	√	√	√	√	√	×	√	√	√	√	√
文献[29]	×	√	√	√	√	√	×	√	√	×	√	√
本文协议	√	√	√	√	√	√	√	√	√	√	√	√

表 3　　单个相关操作执行时间

运算操作	定义	执行时间/ms
T_H	单向哈希运算	0.000 1
T_{PUF}	PUF 运算	0.000 5
T_{AC}	ASCON 加/解密	0.301 0
T_{ECM}	椭圆曲线点乘运算	0.599 8
T_{ECA}	椭圆曲线点加运算	0.002 3
T_S	对称加/解密	0.349 0

本文协议车辆端使用了 7 次 Hash 操作、一次 PUF 操作和一次 ASCON 解密操作，执行时间为 $7T_H+T_{PUF}+T_{AC}\approx0.302\ 2$ ms，在充电桩和服务器端使用了 14 次 Hash 操作和 3 次 ASCON 加/解密操作，执行时间为 $14T_H+3T_{AC}\approx0.904\ 4$ ms，本文协议的计算开销共计为 $21T_H+T_{PUF}+4T_{AC}\approx1.206\ 6$ ms。由表 4 计算开销对比结果可知，文献[9]协议的总计算开销最高，因为该协议采用了大量椭圆曲线点乘和点加运算操作。文献[7]和文献[14]协议认证过程中仅采用哈希操作，计算开销最低，但由表 2 可知，二者不满足一些重要的安全属性，且由图 5 可知，通信开销也远高于本文协议。本文协议采用 Hash、ASCON、PUF 等轻量级密码操作，平均减少了约 29.9% 的计算开销。

6.3　通信开销

在通信开销比较中，仅考虑身份认证与密钥协商阶段的消息传输，设置 Hash 函数的输出和位置标识符为 256 bit，PUF 的激励响应对和累加器见证人 w_i 为 64 bit，ID、随机数、对称加/解密块和密码 PW 为 128 bit，时间戳为 32 bit，椭圆曲线点乘为 320 bit。

本文协议在身份认证与密钥协商过程中交换了 4 条消息，M_1: $\{B_1,B_2,\mathrm{PID}_i,w_i,T_1\}$，$M_2$: $\{\mathrm{CM}_1,\mathrm{PID}_i,\mathrm{ID}_j,T_2\}$，$M_4$: $\{\mathrm{CM}_2,C_i^*,T_4\}$，$M_3$: $\{B_5,B_6,B_7,\mathrm{CM}_2,C_i^*,T_3\}$ 通信开销分别为：B_{M_1}=256 + 256 + 256 + 64 +32= 864 bit，B_{M_2}=128+128+32=288 bit，B_{M_3}=256+256+256+128+64+32=992 bit，B_{M_4}=128+64+32=224 bit，总的通信开销为 B_{total}=864+288+992+224=2 368 bit。其他协议的通信开销计算同理，本文协议和其他文献协议的通信开销对比结果如图 5 所示。由图 5 可知，本文协议通信开销是最低的，本文协议采用轻量级 ASCON 对称加密算法对消息进行了压缩加密传输，平均降低了约 35.9% 的通信开销。

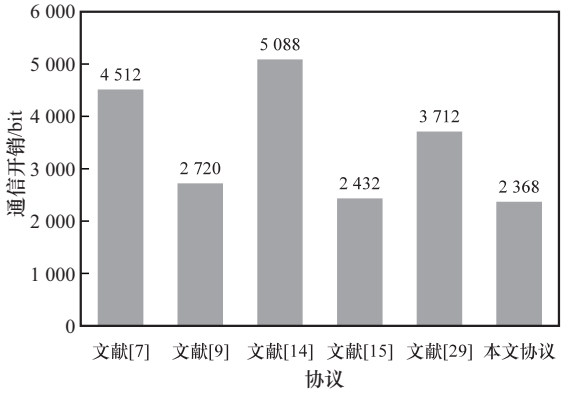


图 5　通信开销对比

7　结束语

面对电动汽车和智能电网频繁的能源与信息交互给资源受限的终端设备带来的隐私和安全问题，本文基于 PUF 为 V2G 网络提出了一种高效的轻量级匿名身份认证与密钥协商协议。本文协议

表 4　　计算开销对比

协议	EV 端	EP 端	合计	总计算开销/ms
文献[7]	$5T_H$	$12T_H$	$17T_H$	0.001 7
文献[9]	$2T_H + 5T_{ECM} + 3T_{ECA}$	$2T_H + 4T_{ECM} + 2T_{ECA}$	$4T_H + 9T_{ECM} + 5T_{ECA}$	5.410 1
文献[14]	$23T_H$	$14T_H$	$37T_H$	0.003 7
文献[15]	$9T_H$	$15T_H + 4T_S$	$24T_H + 4T_S$	1.398 4
文献[29]	$4T_H + T_{ECM}$	$10T_H + 2T_{ECM}$	$14T_H + 3T_{ECM}$	1.800 8
本文协议	$7T_H + T_{PUF} + T_{AC}$	$14T_H + 3T_{AC}$	$21T_H + T_{PUF} + 4T_{AC}$	1.206 6

结合PUF、ASCON、Hash等轻量级密码学原语，有效实现了三方认证、用户撤销和密码或生物特征更新功能，ROR模型和Scyther形式化验证工具表明，该协议满足匿名性、抗物理攻击、抗位置伪造攻击、抗建模攻击等多种安全属性。通过与现有相关协议进行性能比较得出本文协议在安全功能、通信开销和计算开销方面具有一定的优越性。

参考文献：

[1] TONG L, ZHAO S, JIANG H, et al. Multi-scenario and multi-objective collaborative optimization of distribution network considering electric vehicles and mobile energy storage systems[J]. IEEE Access, 2021, 9: 55690-55697.

[2] JAVED M U, JAVAID N, MALIK M W, et al. Blockchain based secure, efficient and coordinated energy trading and data sharing between electric vehicles[J]. Cluster Computing, 2022, 25(3): 1839-1867.

[3] MWASILU F, JUSTO J J, KIM E K, et al. Electric vehicles and smart grid interaction: a review on vehicle to grid and renewable energy sources integration[J]. Renewable and Sustainable Energy Reviews, 2014, 34: 501-516.

[4] REDDY A G, BABU P R, ODELU V, et al. V2G-auth: lightweight authentication and key agreement protocol for V2G environment leveraging physically unclonable functions[J]. IEEE Transactions on Industrial Cyber-Physical Systems, 2023, 1: 66-78.

[5] BIBAK B, TEKINER-MOĞULKOÇ H. A comprehensive analysis of vehicle to grid (V2G) systems and scholarly literature on the application of such systems[J]. Renewable Energy Focus, 2021, 36: 1-20.

[6] SAXENA N, CHOI B J. Authentication scheme for flexible charging and discharging of mobile vehicles in the V2G networks[J]. IEEE Transactions on Information Forensics and Security, 2016, 11(7): 1438-1452.

[7] IRSHAD A, USMAN M, CHAUDHRY S A, et al. A provably secure and efficient authenticated key agreement scheme for energy Internet-based vehicle-to-grid technology framework[J]. IEEE Transactions on Industry Applications, 2020, 56(4): 4425-4435.

[8] SHEN G, XIA C, LI Y M, et al. Traceable and privacy-preserving authentication scheme for energy trading in V2G networks[J]. IEEE Internet of Things Journal, 2024, 11(4): 6664-6676.

[9] SU Y X, SHEN G, ZHANG M W. A novel privacy-preserving authentication scheme for V2G networks[J]. IEEE Systems Journal, 2020, 14(2): 1963-1971.

[10] SURESHKUMAR V, MUGUNTHAN S, AMIN R. An enhanced mutually authenticated security protocol with key establishment for cloud enabled smart vehicle to grid network[J]. Peer-to-Peer Networking and Applications, 2022, 15(5): 2347-2363.

[11] BANSAL G, NAREN N, CHAMOLA V, et al. Lightweight mutual authentication protocol for V2G using physical unclonable function[J]. IEEE Transactions on Vehicular Technology, 2020, 69(7): 7234-7246.

[12] QURESHI M A, MUNIR A. PUF-RAKE: a PUF-based robust and lightweight authentication and key establishment protocol[J]. IEEE Transactions on Dependable and Secure Computing, 2022, 19(4): 2457-2475.

[13] GOPE P, SIKDAR B. A privacy-aware reconfigurable authenticated key exchange scheme for secure communication in smart grids[J]. IEEE Transactions on Smart Grid, 2021, 12(6): 5335-5348.

[14] SURESHKUMAR V, CHINNARAJ P, SARAVANAN P, et al. Authenticated key agreement protocol for secure communication establishment in vehicle-to-grid environment with FPGA implementation[J]. IEEE Transactions on Vehicular Technology, 2022, 71(4): 3470-3479.

[15] YU S, PARK K. PUF-based robust and anonymous authentication and key establishment scheme for V2G networks[J]. IEEE Internet of Things Journal, 2024, 11(9): 15450-15464.

[16] ABDALLAH A, SHEN X S. Lightweight authentication and privacy-preserving scheme for V2G connections[J]. IEEE Transactions on Vehicular Technology, 2017, 66(3): 2615-2629.

[17] GOPE P, SIKDAR B. An efficient privacy-preserving authentication scheme for energy Internet-based vehicle-to-grid communication[J]. IEEE Transactions on Smart Grid, 2019, 10(6): 6607-6618.

[18] HASSIJA V, CHAMOLA V, GARG S, et al. A blockchain-based framework for lightweight data sharing and energy trading in V2G network[J]. IEEE Transactions on Vehicular Technology, 2020, 69(6): 5799-5812.

[19] HOU W Y, SUN Y, LI D W, et al. Lightweight and privacy-preserving charging reservation authentication protocol for 5G-V2G[J]. IEEE Transactions on Vehicular Technology, 2023, 72(6): 7871-7883.

[20] PAPPU R, RECHT B, TAYLOR J, et al. Physical one-way functions[J]. Science, 2002, 297(5589): 2026-2030.

[21] GAO Y S, AL-SARAWI S F, ABBOTT D. Physical unclonable functions[J]. Nature Electronics, 2020, 3(2): 81-91.

[22] DOBRAUNIG C, EICHLSEDER M, MENDEL F, et al. Ascon v1.2: lightweight authenticated encryption and hashing[J]. Journal of Cryptology, 2021, 34(3): 33.

[23] 苗美霞, 武盼汝, 王赟玲. 密码累加器研究进展及应用[J]. 西安电子科技大学学报, 2022, 49(1): 78-91.
MIAO M X, WU P R, WANG Y L. Research progress and applications

of cryptographic accumulators[J]. Journal of Xidian University, 2022, 49(1): 78-91.

[24] SHAMSHAD S, MAHMOOD K, SHAMSHAD U, et al. A provably secure and lightweight access control protocol for EI-based vehicle to grid environment[J]. IEEE Internet of Things Journal, 2023, 10(18): 16650-16657.

[25] DOLEV D, YAO A. On the security of public key protocols[J]. IEEE Transactions on Information Theory, 1983, 29(2): 198-208.

[26] ABDALLA M, FOUQUE P A, POINTCHEVAL D. Password-based authenticated key exchange in the three-party setting[J]. IEE Proceedings-Information Security, 2006, 153(1): 27-39.

[27] CREMERS C J F. The scyther tool: verification, falsification, and analysis of security protocols[C]//International Conference on Computer Aided Verification. Berlin: Springer, 2008: 414-418.

[28] TANVEER M, KHAN A U, KUMAR N, et al. A robust access control protocol for the smart grid systems[J]. IEEE Internet of Things Journal, 2022, 9(9): 6855-6865.

[29] BABU P R, AMIN R, REDDY A G, et al. Robust authentication protocol for dynamic charging system of electric vehicles[J]. IEEE Transactions on Vehicular Technology, 2021, 70(11): 11338-11351.

[作者简介]

范馨月（1979– ），女，四川犍为人，重庆邮电大学副教授、硕士生导师，主要研究方向为信息安全、通信信号处理、图像视频处理等。

刘洁（1999– ），女，重庆人，重庆邮电大学硕士生，主要研究方向为车联网安全、认证协议等。

何嘉辉（1999– ），男，四川达州人，重庆邮电大学硕士生，主要研究方向为车联网安全等。