基于匿名凭证与区块链的V2G网络电力交易隐私保护认证方案

李元诚[1]，胡柏吉[2]，黄戎[1]
（1.华北电力大学控制与计算机工程学院，北京 102206；2.中国电力科学研究院有限公司信息通信研究所，北京 100192）

摘　要：针对传统车网互动（V2G）电力交易认证中用户隐私泄露导致的身份伪造、交易行为分析及位置追踪等问题，提出一种基于匿名凭证和区块链的V2G网络隐私保护认证方案。该方案设计了基于CL签名和零知识证明的匿名凭证，在不暴露任何隐私信息下实现身份认证。在此基础上，该方案将安全、去中心化身份认证嵌入区块链，消除对可信第三方的依赖，避免在交易认证过程中暴露EV隐私的同时，增强抵御内、外部安全威胁的能力，实现安全、可追溯的EV充放电交易。通过安全分析与性能评估证明，所提方案能够保障EV在电力交易中的隐私安全，处理计算和通信开销满足实时性需求。

关键词：区块链；隐私保护身份认证；电动汽车；零知识证明；CL签名
中图分类号：TN309.2
文献标志码：A
DOI：10.11959/j.issn.1000−436x.2025078

Privacy-preserving authentication scheme for electricity trading in V2G network using anonymous credential and blockchain

LI Yuancheng[1], HU Baiji[2], HUANG Rong[1]
1. School of Control and Computer Engineering, North China Electric Power University, Beijing 102206, China
2. Institute of Information and Communication, China Electric Power Research Institute Co., Ltd., Beijing 100192, China

Abstract: To address privacy leakage issues in traditional V2G power transaction authentication, including identity forgery, transaction behavior analysis, and location tracking, a blockchain-based privacy-preserving authentication scheme for V2G networks was proposed. The scheme designed anonymous credentials incorporating CL signatures and zero-knowledge proofs to achieve identity authentication without exposing sensitive information. Secure and decentralized authentication mechanisms were embedded into blockchain infrastructure to eliminate reliance on trusted third parties, thereby preventing EV privacy exposure during transaction authentication while enhancing resistance against internal and external security threats. Secure traceability was realized for EV charging/discharging transactions. Security analysis and performance evaluation demonstrated that the proposed scheme effectively protects EV privacy in power transactions, with computational and communication overhead shown to meet real-time requirements. The results indicate that the integration of cryptographic primitives and distributed ledger technology establishes a balanced equilibrium between privacy preservation and system accountability in V2G ecosystems.

Keywords: blockchain, privacy-preserving identity authentication, electric vehicles, zero-knowledge proof, CL signature

收稿日期：2024−12−31；**修回日期：**2025−04−15
通信作者：黄戎，huangrong@ncepu.edu.cn
基金项目：国家资助博士后研究人员计划基金资助项目（No.GZC20230791）；中央高校基本科研业务费专项资金资助项目（No.2024MS020）
Foundation Items: The Postdoctoral Fellowship Program of CPSF (No.GZC20230791), The Fundamental Research Funds for the Central Universities (No.2024MS020)

0 引言

随着车网互动（V2G, vehicle-to-grid）网络的快速发展，EV作为新型移动储能单元，能够通过充放电优化，在需求侧参与电力系统调频、调峰等能量型调节服务，以提升系统运行的经济性与灵活性[1]。EV与充电桩（CP, charging point）之间的在线电力交易频率日益增加。传统EV在线身份验证利用用户信息、支付信息等敏感数据，实现高效便捷的用户认证、交易信息检索、仲裁等。然而，由于传输信息中不可避免地包含了用户隐私数据，例如EV位置、充电状态（SOC, state of charge）、充电时间窗口、车辆及驾驶信息等，存在数据安全与隐私泄露问题。攻击者可通过分析泄露信息，推测EV使用模式与用户习惯，并将其共享给营销商、保险公司等机构，以牟取不当利益[2-3]。尤其在集中式架构的V2G能源交易系统中，单点故障、内部攻击及隐私泄露等安全问题更为严峻[4]。基于公钥基础设施（PKI, public key infrastructure）的传统身份验证方案要求EV将用户信息、车辆信息等作为凭证（如X.509证书）的公开属性对，以证明其交易身份的合法性。这暴露了EV的隐私信息，为攻击者进行身份盗用、欺骗窃电提供了客观条件。

传统V2G网络中，EV用户隐私保护依赖于匿名认证、签名及秘密共享等[5-10]。当EV用户数量激增，上述方法将不可避免地增加计算和通信开销，受到系统计算能力与计算成本的限制[5-6]。随着区块链技术的发展，由于其分布式、不可篡改和可追溯特性，可用于构建去中心化、可扩展的身份认证协议，为V2G电力交易隐私保护提供了新的解决方案[11-16]。通过结合数字签名等技术，区块链构建了具有隐私保护、可扩展的V2G能源交易系统，实现安全、高效的用户身份认证与交互。然而，大多数基于区块链的V2G身份认证依赖于PKI，仍存在传统方案的隐私安全问题[12-13]。为实现具有隐私安全的身份认证，部分方案将零知识证明（ZKP, zero-knowledge proof）与区块链结合构建匿名认证方案，在最小隐私披露情况下实现身份验证。然而，交互式ZKP要求证明者与验证者具有相应的计算能力，以生成和验证证明，但由于计算产生了大量数据，将不可避免地增加系统的通信开销。

针对上述隐私保护认证方案的缺陷，本文提出一种基于匿名凭证和联盟链的V2G网络隐私保护认证方案，通过CL（Camenisch-Lysyanskaya）签名[17]、非交互ZKP[18-19]与联盟链的有机结合，实现系统中已认证和非认证实体的隐私保护身份认证。具体贡献如下。

1) 设计了基于CL签名与非交互ZKP的匿名凭证，可以隐藏待签名的EV属性，并通过ZKP证明其所属关系。CL签名将凭证与主密钥绑定，以验证EV身份的合法性，保护电力交易过程中的隐私信息，从而在增强匿名性的同时，降低签名的计算复杂度。

2) 确保了双向认证、身份隐私保护，EV通过一次匿名凭证与ZKP参与电力交易，在不暴露隐私的情况下实现系统实体间的双向身份认证。同时，电力交易信息无法基于假名与具体用户进行关联，具有不可伪造性和不可关联性，可抵抗系统内、外部对手的恶意攻击。

3) 构建了基于联盟链的V2G网络模型，将安全、去中心化身份认证嵌入联盟链，消除对可信第三方的依赖，EV交易信息记录上链，实现具有安全性、可追溯性的EV充放电交易。安全与性能分析表明，该方案的计算和通信开销适合实际应用场景，能够满足电动汽车的实时交易需求。

1 相关工作

V2G网络实现了EV与电网之间的双向通信和电力流动，在电力负荷平衡和负荷需求响应中发挥着重要作用。随着越来越多EV通过V2G网络参与电力系统负荷侧调频、调峰，EV隐私安全问题已成为V2G网络面临的主要挑战。为保证电力交易过程中的EV身份隐私，当前研究工作基于PKI[8-10,20-24]、不可克隆函数（PUF, physical unclonable function）[25-28]、区块链[3,12-15]等提出具有隐私保护的电力交易身份认证方案。

基于PKI的V2G网络身份认证方案依赖于可信第三方，并结合匿名认证[23]、离散对数[21]、群签名[24]及秘密共享[6]等方法在交易过程中保护EV的隐私信息。EV需要从可信第三方获取证书后，才能通过V2G网络向电力系统请求充放电服务。Su等[21]基于椭圆曲线构建了适用于V2G网络的轻量级认证协议，通过结合安全多方计算保障EV的隐私安全。Zhang等[23]提出基于假名的V2G网络认证

密钥协商协议，保证了认证过程中仅有可信机构拥有EV真实身份。Xia等[24]基于雾计算和群签名提出EV充电身份认证方案，在保障EV隐私安全的同时，减少EV与云服务器交互次数。上述方案中，可信第三方的安全性制约了V2G网络的安全性，一旦被攻击者破坏，参与电力交易实体的主密钥不再可信。此外，随着EV用户的增加，此类身份认证方案将不可避免地受到计算与通信资源的制约。

基于PUF的V2G网络隐私保护认证方案依赖于设备硬件特性的唯一性。Bansal等[25]基于PUF提出了安全用户密钥交换认证协议，实现了EV与电力服务商之间的两步双向认证。Hou等[26]提出了轻量级、可扩展的充电预约认证和密钥协商协议，利用PUF响应验证参与电力交易认证。Liang等[27]将匿名认证、数据聚合与PUF结合，提出了基于数据聚合的充电认证框架，以抵御潜在信息攻击与物理攻击。由于PUF依赖于硬件特性的唯一性和不可克隆性，具有较高的环境敏感性和不稳定性，需要额外的纠错机制，增加了方案的复杂性和计算成本。此外，由于认证方案需要在EV和CP中嵌入特定硬件电路，硬件成本较高。

随着区块链技术的发展，其去中心化、不可篡改、可追溯等特点使其天然适用于分布式储能，能够为V2G网络提供可扩展的隐私保护身份认证方案[11-15,29-30]。Aggarwal等[12]基于区块链提出适用于EV、CP和公共事业中心的匿名能量交易方案，通过数字签名实现双向认证。Yue等[15]提出具有隐私保护与匿名支付的轻量级认证框架，通过同态签名和共识机制实现匿名认证和支付。上述基于区块链的认证方案仍采用集中式架构，安全性受到可信第三方的约束。针对该问题，Gabay等[3]将ZKP与智能合约结合提出V2G网络匿名认证方案，该方案将区块链作为可信第三方，通过ZKP验证EV的智能合约并发放代币，用以生成伪名参与电力交易，从而在不透漏用户隐私下完成身份认证与电力交易；然而，该方案计算较为复杂，参与ZKP的验证者和证明者都需要一定的计算和通信资源，导致为EV调度充电时间段的响应较慢。

上述方案在不同程度上实现了V2G网络中具有隐私保护的用户身份认证，但仍然存在部分问题需要进一步完善。为了实现安全、高效、可靠的电力交易，需提出新的、更有效的EV隐私保护身份认证方案，以适应资源有限、实体不完全可信的V2G交易场景。

2　预备知识

2.1　质数阶双线性映射

令Ψ为质数阶双线性群生成算法，给定安全参数$\delta \in \mathbb{Z}^+$，输出参数$(p,\mathbb{G}_1,\mathbb{G}_2,\mathbb{G}_T,e)$。其中，$p$表示大小为$\delta$比特的质数，$\mathbb{G}_1$、$\mathbb{G}_2$、$\mathbb{G}_T$表示阶为$p$的循环群，函数$e$:$\mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$为满足以下属性的双线性对。

双线性：$\forall u \in \mathbb{G}_1$，$v \in \mathbb{G}_2$，$a,b \in \mathbb{Z}_p^*$，$e(u^a,v^b)=e(u,v)^{ab}$。

非退化性：$\exists u \in \mathbb{G}_1$，$v \in \mathbb{G}_2$，$e(u,v) \neq 1_{\mathbb{G}_T}$，即函数$e$并未将$\mathbb{G}_1 \times \mathbb{G}_2$中所有对映射到$\mathbb{G}_T$。

可计算性：$\forall u \in \mathbb{G}_1$，$v \in \mathbb{G}_2$，存在与安全参数$\delta$相关的多项式时间算法，使$e(u,v)$可被高效计算。特别地，当$\mathbb{G}_1=\mathbb{G}_2$时，函数$e$称为对称质数阶双线性映射，否则为非对称质数阶双线性映射。

2.2　CL签名

CL签名是一种适用于ZKP的公钥签名方案，能够对一组数据进行签名，并保留数据之间的逻辑关系，由密钥生成、签名和签名认证3个算法构成。

密钥生成：给定安全参数δ，运行双线性映射的群生成算法$\mathrm{Setup}(1^k)$，生成元组$(q,\mathbb{G}_1,\mathbb{G}_T,g_1,g_t,e)$，其中$\mathbb{G}_1$和$\mathbb{G}_T$均为相同质数阶$q$的群。若$g_1$是$\mathbb{G}_1$的生成元，则$g_t=e(g_1,g_1)$是$\mathbb{G}_T$的生成元。选择$x,y \in \mathbb{Z}_q$和$z_i \in \mathbb{Z}_q, 1 \leqslant i \leqslant l$，设置私钥为$\mathrm{sk}=(x,y,\{z_i\})$，公钥为$\mathrm{pk}=(q,\mathbb{G}_1,\mathbb{G}_T,g_1,g_t,e,X,Y,\{Z_i\})$，其中$X=g_1^x$，$Y=g_1^y$，$Z_i=g_1^{z_i}$。

签名：对于待签名消息$M=\{m_0,\cdots,m_l\}$、私钥sk和公钥pk，随机选择$\alpha \in \mathbb{Z}_q$并计算$a={g_1}^{\alpha} \in \mathbb{G}_1$。计算$A_i=a^{z_i} \in \mathbb{G}_1$、$b=a^y \in \mathbb{G}_1$和$B_i={A_i}^y \in \mathbb{G}_1$，$1 \leqslant i \leqslant l$。最后计算

$$c=a^{x+xym_0}\prod_{i=1}^{l}{A_i}^{xym_i} \tag{1}$$

输出签名$\sigma=(a,\{A_i\},b,\{B_i\},c)$。

签名验证：对于输入公钥sk、消息M和签名σ，验证以下等式是否成立，即

$$e\left(a,Z_i\right)=e\left(g_1,A_i\right) \tag{2a}$$

$$e\left(a,Y\right)=e\left(g_1,b\right) \tag{2b}$$

$$e\left(A_i,Y\right)=e\left(g_1,B_i\right) \tag{2c}$$

$$e\left(X,a\right)e\left(X,b\right)^{m_0}\prod_{i=1}^{I}e\left(X,B_i\right)^{m_i}=e\left(g_1,c\right) \tag{2d}$$

其中，式(2a)用于验证A_i是否正确，式(2b)和式(2c)用于验证b和B_i是否正确，式(2d)验证c是否正确。

2.3 ZKP

考虑区块链的去中心特性，本文基于Schnorr签名的非交互式零知识证明（NIZKP, non-interactive zero-knowledge proof）[18]提出身份认证方案，在无须透漏任何信息的情况下，证明EV已知离散对数的解，在单一消息中完成具有隐私保护的身份认证。令$\mathrm{PK}\left(\alpha,\beta,\delta\right):y=g^{\alpha}h^{\beta}\wedge\tilde{y}=\tilde{g}^{\alpha}\tilde{h}^{\delta}$表示对整数$\alpha$、$\beta$和$\delta$的ZKP，其中$y$、$g$、$h$、$\tilde{y}$、$\tilde{g}$、$\tilde{h}$分别为群$\mathbb{G}=\langle g\rangle=\langle h\rangle$和$\tilde{\mathbb{G}}=\langle\tilde{g}\rangle=\langle\tilde{h}\rangle$的元素，除$\alpha$、$\beta$和$\delta$对验证者保密外，其他参数均向验证者公开。

令$\mathbb{G}_1=\langle g_1\rangle$表示阶为大质数$q$的循环群，Schnorr NIZKP过程如下。

初始化：证明者为Alice，验证者为Bob。Alice选择私钥$a\in\mathbb{Z}_q$，计算公钥$A=g_1{}^a\in\mathbb{G}_1$。

证明生成：首先，Alice选择$r\in\mathbb{Z}_q$，并计算生成元$R=g_1{}^r$。然后，Alice计算挑战$c=H\left(g_1\|R\|A\|\mathrm{UserID}\|\mathrm{OtherInfo}\right)$，其中UserID为证明者标识，OtherInfo为其他可选数据，$H(\cdot)$为安全哈希函数。最后，Alice计算响应$s=r-ca\bmod q$，并将$\{c\|s\|A\|\mathrm{UserID}\|\mathrm{OtherInfo}\}$发送给Bob。

证明验证：Bob计算生成元$R'=g^sA^c$和挑战$c'=H\left(g\|R'\|A\|\mathrm{UserID}\|\mathrm{OtherInfo}\right)$，并验证$c$是否等于$c'$。

3 问题描述

在V2G网络电力交易过程中，用户隐私信息面临内、外部攻击者的威胁，其系统安全性难以保障。本节详细描述了系统网络模型、对手模型及认证方案设计目标。

3.1 系统模型

基于区块链的V2G电力交易系统模型由EV，CP和区块链节点等实体构成，如图1所示。在电力交易中，EV首先向系统请求充放电，将身份信息、SOC、可用时间段、目标CP等发送给区块链节点（BC节点），进行身份验证。身份验证中，EV仅向BC节点提供身份信息的匿名凭证与ZKP，对应图中①和②。BC节点完成EV身份信息验证后，计算并返回优化调度结果，为EV颁发由CL签名的交易凭证，保留充放电时间段，对应图中③和④。最后，EV连接到CP，进行充放电交易认证，将BC颁发的交易凭证与对应的ZKP发送给CP，对应图中⑤和⑥。CP验证EV身份后，根据优化调度结果执行充放电，对应图中⑦。EV完成充放电后，根据区块链上交易数据进行支付并记录上链。

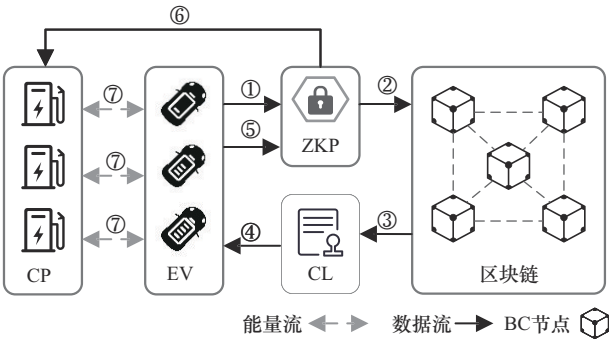

图1 V2G电力交易系统模型

BC节点：组成区块链网络的一组节点。BC节点通过协同合作，维护区块链网络，保障交易生成、节点共识及区块打包上链等功能的正常执行。在此基础上，BC节点在V2G网络中作为证书颁发机构，为EV的一组或多组属性颁发数字证书，作为凭证供EV参与电力交易。

CP：作为验证者，CP验证EV是否获得充电许可，并以分布式方式为EV提供充放电服务。CP内置的智能电表实时记录EV的充放电数据。

EV：通过匿名凭证与ZKP，EV从区块链节点（BC节点）获取交易凭证，并向CP证明拥有交易凭证对应的秘密属性，从而在不泄露隐私信息情况下，从签发者（BC节点）和验证者（CP）处获得充放电交易许可，并完成电力交易。

3.2 对手模型

电力交易过程中，V2G网络面临BC节点攻击、CP攻击、中间人攻击等，EV用户隐私安全性难以保障。因此，该隐私保护认证方案在多项式时间内考虑以下威胁。

BC 节点攻击：假设区块链节点中存在半可信实体，该实体不拒绝执行既定协议，且试图从接收的信息中挖掘隐私信息。该实体通过观察交易数据集 $D=\{d_1,d_2,\cdots,d_n\}$，其中 d_i 表示在时间 t_i 观察到的 EV 交易记录，分析计算出 EV 的隐私属性集 $A=\{m_1,m_2,\cdots,m_m\}$，其中 m_i 表示攻击者试图推断的用户隐私属性。该类节点存在恶意传播 EV 隐私信息或将其用于不当目的风险。

CP 攻击：与 BC 节点攻击类似，CP 中可能存在半可信实体或受攻击者控制的恶意节点。该类节点通过分析 EV 的充放电请求和身份凭证，以获取时间、交易信息等隐私信息。

联盟链账本攻击：在联盟链中，经过认证的用户有权查看其他用户的交易数据，存在恶意节点，根据可访问数据分析 EV 交易信息，进行数据篡改或伪造。

中间人攻击：对手试图在 EV 与 CP 或 BC 节点通信时截获传输数据，并通过分析 EV 认证消息、电力交易请求等获取隐私信息，为篡改和伪造数据做准备。

重放攻击：对手截获并重复提交之前 EV 生成或 CP 验证过的证明，以获取合法授权或重复执行交易。

3.3　认证方案设计目标

为实现具有隐私保护的 V2G 电力交易身份认证，本文认证方案保护 EV 隐私信息的同时，还需要防止对手欺诈行为，实现用户信息的有效隔离。此外，方案需要具有可扩展性，以满足不断增长的用户充放电服务需求。因此，本认证方案的设计目标如下。

隐私保护：在电动汽车充放电交易过程中，系统应确保 EV 的身份和交易数据得到有效保护，防止隐私泄露、用户信息被追踪或分析。

安全性：系统能够抵御多种潜在攻击，例如中间人攻击、重放攻击、拒绝服务攻击等，确保电动汽车交易过程中的安全性和可靠性。

不可伪造性、匿名性和不可关联性：凭证应具备不可伪造性、匿名性和不可链接性。即使 CP 与 BC 节点或其他 CP 合作，CP 和 BC 节点也不能从凭证中获取任何用户隐私信息。同时，同一 EV 的凭证不能被 CP 和 BC 节点链接。

一次性使用凭证：EV 需从 BC 节点获得匿名交易凭证，允许其进行电力交易。该凭证只能使用一次，且只能由该电动汽车使用。

可扩展性和高性能：随着电动汽车数量的快速增长，系统应具备高效处理大量 EV 并发交易的能力，保持较高性能，并具有可扩展性。

4　V2G 电力交易隐私保护认证方案设计

本节详细描述了本文 V2G 网络隐私保护认证方案。方案包括系统设置、匿名属性认证、凭证颁发及 EV 充放电认证 4 个阶段。系统设置进行系统交易环境初始化，生成交易实体所需密钥对。在匿名属性认证阶段，EV 提供匿名凭证，通过 ZKP 向 BC 节点验证其身份合法性。在凭证颁发阶段，BC 节点验证并接受 EV 身份后，基于 CL 签名为其提供的匿名凭证签名作为交易凭证颁发给 EV。在 EV 充放电认证阶段，EV 提供 BC 颁发的交易凭证，通过 ZKP 向 CP 证明其交易身份的合法性。CP 验证交易凭证并提供充放电服务。在上述认证过程中，EV 并未提供任何身份信息，通过匿名凭证与对应 ZKP 证明身份的合法性和拥有交易授权，从而避免了隐私泄露导致的身份伪造、交易行为分析及位置追踪等问题。

4.1　系统设置

系统设置阶段执行系统初始化，为 EV_j 和 BC_k 节点生成密钥对，并提供 BC_k 节点公钥的 ZKP，如图 2 所示。

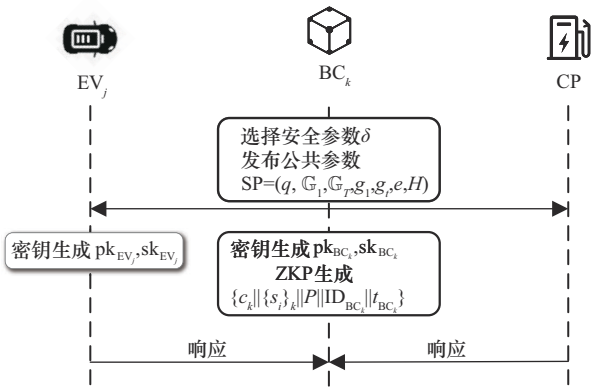

图 2　系统设置阶段

系统初始化：系统选择合适的安全参数 δ，并执行对称质数阶双线性映射群生成算法 $\mathrm{Setup}(1^k)$，生成公共参数 $(q,\mathbb{G}_1,\mathbb{G}_T,g_1,g_t,e)$。领导者节点选择抗碰撞哈希函数 $H:\{0,1\}\rightarrow\mathbb{Z}_q$，并发布公共参数

$\mathrm{SP}=\left(q,\mathbb{G}_1,\mathbb{G}_T,g_1,g_t,e,H\right)$，初始化交易认证环境。

密钥生成：根据系统公共参数，电动汽车$\mathrm{EV}_j,j\in\{1,\cdots,n\}$从$\mathbb{Z}_q$中选择满足均匀分布的私钥$\mathrm{sk}_{\mathrm{EV}_j}$和公钥$\mathrm{pk}_{\mathrm{EV}_j}=g_1^{\mathrm{sk}_{\mathrm{EV}_j}}$，以在认证中证明自己的身份。联盟链节点$\mathrm{BC}_k,k\in\{1,\cdots,\tau\}$根据CL签名生成私钥$\mathrm{sk}_{\mathrm{BC}_k}=\left(x_k,y_k,\left\{z_{k_i}\right\}\right)$和公钥$\mathrm{pk}_{\mathrm{BC}_k}=\left(q,\mathbb{G}_1,\mathbb{G}_T,g_1,g_t,e,X_k,Y_k,\left\{Z_{k_i}\right\}\right)$。认证中，$\mathrm{BC}_k$的密钥对用于对$\mathrm{EV}_j$的一组属性签名，以生成交易凭证。

ZKP生成：BC_k应提供ZKP，证明其持有的密钥在给定的凭证范式下是正确的。该ZKP为

$$\mathrm{PK}\left\{\left(x_k,y_k,\{z_{k_i}\}_{i=1}^{l}\right):P=X_kY_k\prod_{i=1}^{l}Z_{k_i}\right\}\tag{3}$$

根据ZKP，BC_k生成证明的详细过程如下。

1)选择随机数$r_i\in\mathbb{Z}_p,0\leqslant i\leqslant l+1$，计算生成元$R_k=g_1^{r_0}g_1^{r_1}\prod_{i=2}^{l+1}g_1^{r_i}$，用于隐藏$\left(x_k,y_k,\{z_{k_i}\}_{i=1}^{l}\right)$。

2)通过哈希函数生成挑战$c_k=H\left(X_k\|Y_k\|\left\{Z_{k_i}\right\}\|R_k\|P\|\mathrm{ID}_{\mathrm{BC}_k}\|t_{\mathrm{BC}_k}\right)$，$t_{\mathrm{BC}_k}$为ZKP的有效期。

3)根据挑战c_k与随机数$\{r_i\}_{i=0}^{l+1}$，生成响应$\left\{s_i\right\}_k$，其中$s_0=r_0-c_kx_k$，$s_1=r_1-c_ky_k$，$s_i=r_i-c_kz_{k_i}\bmod p,i=2,\cdots,l+1$，保留$\left\{c_k\|\left\{s_i\right\}_k\|P\|\mathrm{ID}_{\mathrm{BC}_k}\|t_{\mathrm{BC}_k}\right\}$作为$\mathrm{BC}_k$公钥$\mathrm{pk}_{\mathrm{BC}_k}$的证明。

系统设置完成后，EV_j即可向系统验证身份并申请充放电交易。BC_k根据EV_j提供的凭证信息验证其身份信息并颁发交易凭证。CP则根据EV_j提供的交易凭证验证其交易身份并提供充放电服务。

4.2 匿名属性认证

电动汽车EV_j在进行电力交易前，需要向BC_k请求交易凭证，将身份秘密属性作为凭证发送给BC_k。BC_k根据该凭证进行身份验证与签名，并作为交易凭证颁发。为了避免秘密属性（主密钥、身份信息等）的泄露，EV_j希望BC_k对该秘密属性的承诺进行签名，而非原始属性信息。不失一般性，假设EV_j凭证中所含属性都属于秘密属性$A_j=\left(m_{j_0},\cdots,m_{j_l}\right)$，并指定$m_{j_0}=\mathrm{sk}_{\mathrm{EV}_j}$，使主密钥作为特殊属性包含在凭证中充当身份信息，将不同的凭证绑定到同一身份。从而，EV_j可基于秘密属性的承诺与对应的ZKP向BC_k请求交易凭证，其中ZKP用于证明自己拥有该承诺对应的秘密属性A_j。该匿名属性验证过程如图3所示，EV_j首先向BC_k请求公钥$\mathrm{pk}_{\mathrm{BC}_k}$，验证节点身份。然后，$\mathrm{EV}_j$生成其身份秘密属性的承诺与ZKP，发送给$\mathrm{BC}_k$进行充放电交易请求。最后，$\mathrm{BC}_k$根据接收的信息验证$\mathrm{EV}_j$的身份。

公钥正确性验证：EV_j在发送交易申请前，需

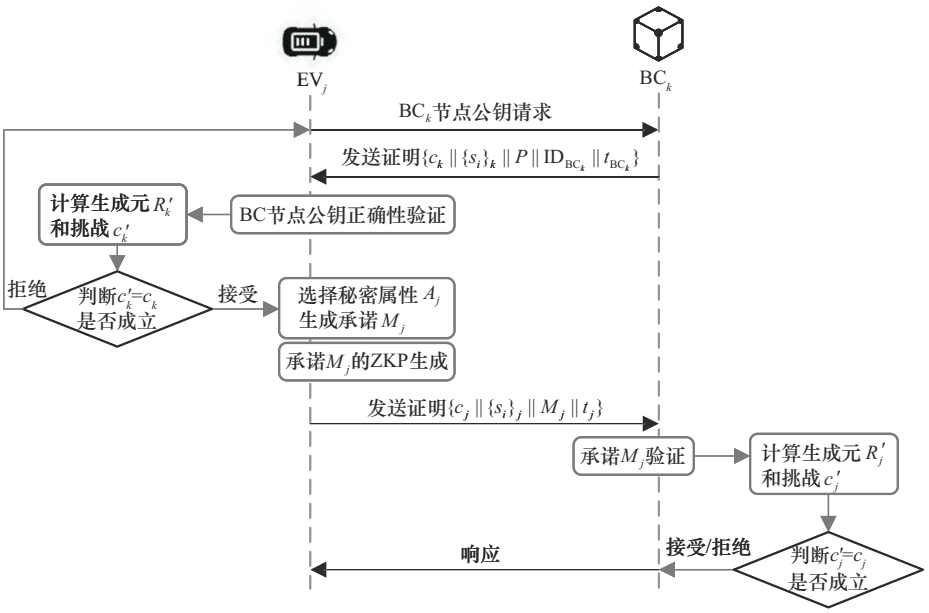

图3 匿名属性验证过程

验证BC_k公钥pk_{BC_k}的正确性，保证BC_k为合法BC节点。

1)根据BC_k提供的公钥pk_{BC_k}，EV_j计算生成元$R_k'=\left(g_1{}^{s_0}g_1{}^{s_1}\prod_{i=2}^{l+1}g_1{}^{s_i}\right)(P)^{c_k}$和挑战$c_k'=H\left(X_k\|Y_k\|\left\{Z_{k_i}\right\}\|R_k'\|P\|\mathrm{ID}_{BC_k}\|t_{BC_k}\right)$。

2)判断等式$c_k'=c_k$是否成立，成立则接受公钥pk_{BC_k}，否则拒绝。等式$c_k'=c_k$的正确性来自$R_k'=R_k$。

$$R_k'=\left(g_1{}^{s_0}g_1{}^{s_1}\prod_{i=2}^{l+1}g_1{}^{s_i}\right)(P)^{c_k}=$$
$$g_1{}^{s_0}g_1{}^{s_1}\prod_{i=2}^{l+1}g_1{}^{s_i}\left(X_kY_k\prod_{i=2}^{l+1}Z_{k_i}\right)^{c_k}=$$
$$g_1{}^{s_0}g_1{}^{s_1}\prod_{i=2}^{l+1}g_1{}^{s_i}\left(g_1{}^{x_k}g_1{}^{y_k}\prod_{i=2}^{l+1}g_1{}^{z_{k_i}}\right)^{c_k}=$$
$$g_1{}^{s_0+c_kx_k}g_1{}^{s_1+c_ky_k}\prod_{i=2}^{l+1}g_1{}^{s_i+c_kz_{k_i}}=$$
$$g_1{}^{r_0}g_1{}^{r_1}\prod_{i=2}^{l+1}g_1{}^{r_i}=R_k \tag{4}$$

生成秘密属性承诺：为了隐藏秘密属性，EV_j采用Pedersen承诺方案，使用BC_k的公钥pk_{BC_k}对秘密属性A_j生成承诺$M_j=g_1{}^{m_{j_0}}\prod_{i=1}^{l}Z_{k_i}{}^{m_{j_i}}$。该承诺具有不可篡改和不可关联性，允许$EV_j$在不泄露秘密属性情况下将身份信息提交给$BC_k$。

承诺证明生成：EV_j需证明所生成的承诺是正确的，其对应的ZKP为

$$\mathrm{PK}\left\{\left(m_{j_0},m_{j_1},\cdots,m_{j_l}\right):M_j=g_1{}^{m_{j_0}}\prod_{i=0}^{l}Z_{k_i}{}^{m_{j_i}}\right\} \tag{5}$$

该承诺证明的生成过程如下。

1)EV_j选择随机数$r_i\in\mathbb{Z}_q,0\leqslant i\leqslant l$，计算生成元$R_j=g_1{}^{r_0}\prod_{i=1}^{l}Z_{k_i}^{r_i}$。

2)生成挑战$c_j=H\left(g_1\|\left\{Z_{k_i}\right\}\|R\|M_j\|t_j\right)$，$t_j$是当前的时间戳。

3)计算响应$\left\{s_i\right\}_j$，其中$s_j=r_j-c_jm_{j_i}\bmod p$，$0\leqslant i\leqslant l$。

4)将$\left\{c_j\|\left\{s_i\right\}_j\|M_j\|t_j\right\}$发送给$BC_k$。

承诺证明验证：BC_k接收承诺与ZKP并进行正确性验证，以证明EV_j拥有承诺对应的秘密属性。

1)根据收到的承诺M_j，BC_k计算生成元$R_j'=\left(g_1{}^{s_0}\prod_{i=1}^{l}Z_{k_i}{}^{s_i}\right)\left(M_j\right)^{c_j}$，及挑战$c_j'=H\left(g_1\|\left\{Z_{k_i}\right\}\|R_j'\|M_j\|t_j\right)$。

2)判断等式$c_j'=c_j$是否成立，成立则接受承诺M_j，否则拒绝。等式$c_j'=c_j$的正确性来自$R_j'=R_j$。

$$R_k'=\left(g_1{}^{s_0}\prod_{i=1}^{l}Z_{k_i}{}^{s_i}\right)\left(M_j\right)^{c_j}=$$
$$g_1{}^{s_0}\prod_{i=1}^{l}Z_{k_i}{}^{s_i}\left(g_1{}^{m_{j_0}}\prod_{i=1}^{l}Z_{k_i}{}^{m_{j_i}}\right)^{c_j}=$$
$$g_1{}^{s_0}g_1{}^{s_1}\prod_{i=2}^{l+1}g_1{}^{s_i}\left(g_1{}^{x_k}g_1{}^{y_k}\prod_{i=2}^{l+1}g_1{}^{z_{k_i}}\right)^{c_k}=$$
$$g_1{}^{s_0+c_jm_{j0}}\prod_{i=1}^{l}Z_{k_i}{}^{s_i+c_jm_{j_i}}=g_1{}^{r_0}\prod_{i=1}^{l}Z_{k_i}{}^{r_i}=R_j \tag{6}$$

4.3　凭证颁发

BC_k验证并接受承诺M_j后，使用CL签名算法对M_j进行签名，并将其作为交易凭证颁发给EV_j，如图4所示。

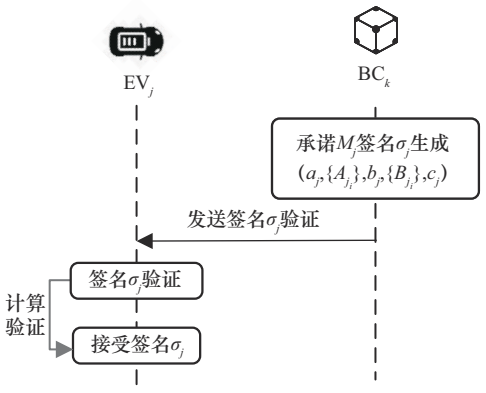

图4　凭证颁发

凭证签名生成：根据CL签名，BC_k随机生成$\alpha_j\in\mathbb{Z}_q$并计算$a_j=g_1{}^{\alpha_j}$。随后BC_k对承诺M_j签名，计算$A_{j_i}=a_j{}^{z_{k_i}}$，$b_j=a_j{}^{y_k}$，$B_{j_i}=A_{j_i}{}^{y_k}$和$c_j=a_j{}^{x_k}\left(M_j\right)^{\alpha_jx_ky_k}$，$1\leqslant i\leqslant l$，生成签名$\sigma_j=\left(a_j,\left\{A_{j_i}\right\},b_j,\left\{B_{j_i}\right\},c_j\right)$，将其作为交易凭证发送给$EV_j$。由于$c_j=a_j{}^{x_k+x_ky_km_{j_0}}\prod_{i=1}^{l}A_{j_i}{}^{x_ky_km_{j_i}}$，$A_{j_i}=a_j{}^{z_{k_i}}=g_1{}^{\alpha_jz_{k_i}}=Z_{k_i}{}^{\alpha_j}$，该

签名σ_j等价于直接对秘密属性A_j的签名，证明计算式为

$$\begin{aligned}&c_j = {a_j}^{x_k}\left(M_j\right)^{\alpha_j x_k y_k} = \\ &{a_j}^{x_k}\left({g_1}^{m_{j_0}}\prod_{i=1}^{l}{Z_{k_i}}^{m_{j_i}}\right)^{\alpha_j x_k y_k} = \\ &{a_j}^{x_k}\left({g_1}^{\alpha_j m_{j_0}}\prod_{i=1}^{l}{Z_{k_i}}^{\alpha_j m_{j_i}}\right)^{x_k y_k} = \\ &{a_j}^{x_k}\left({a_j}^{m_{j_0}}\prod_{i=1}^{l}{A_{j_i}}^{m_{j_i}}\right)^{x_k y_k} = \\ &{a_j}^{x_k + x_k y_k m_{j_0}}\prod_{i=1}^{l}{A_{j_i}}^{x_k y_k m_{j_i}}\end{aligned} \tag{7}$$

对于BC_k，由于EV_j已经通过ZKP证明承诺M_j对应属性的有效性，因此其对承诺M_j的签名具有等同于直接对其秘密属性A_j签名的安全性。而对于EV_j，虽然BC_k拥有秘密属性A_j的承诺M_j，但由于Pedersen承诺的特性，M_j独立于A_j，BC_k无法从M_j中推理出A_j的相关信息。

凭证签名验证：EV_j收到交易凭证σ_j后，验证其有效性。验证过程如下。

1)判断等式$e\left(a_j,Z_{k_i}\right)=e\left(g_1,A_{j_i}\right)$是否成立，以验证$A_{j_i}$是否正确，表示为

$$\begin{aligned}&e\left(a_j,Z_{k_i}\right)=e\left({g_1}^{\alpha_j},{g_1}^{z_{k_i}}\right)=e\left(g_1,{g_1}^{\alpha_j z_{k_i}}\right)= \\ &e\left(g_1,{a_j}^{z_{k_i}}\right)=e\left(g_1,A_{j_i}\right)\end{aligned} \tag{8}$$

2)判断等式$e\left(a_j,Y_k\right)=e\left(g_1,b_j\right)$是否成立，以验证$b_j$是否正确，表示为

$$\begin{aligned}&e\left(a_j,Y_k\right)=e\left({g_1}^{\alpha_j},{g_1}^{y_k}\right)=e\left(g_1,{g_1}^{\alpha_j y_k}\right)= \\ &e\left(g_1,{\alpha_j}^{y_k}\right)=e\left(g_1,b_j\right)\end{aligned} \tag{9}$$

3)判断等式$e\left(A_{j_i},Y_k\right)=e\left(g_1,B_{j_i}\right)$是否成立，以验证$B_{j_i}$是否正确，表示为

$$\begin{aligned}&e\left(A_{j_i},Y_k\right)=e\left({g_1}^{\alpha_j z_{k_i}},{g_1}^{y_k}\right)=e\left(g_1,{g_1}^{\alpha_j z_{k_i} y_k}\right)= \\ &e\left(g_1,{a_j}^{z_{k_i} y_k}\right)=e\left(g_1,{A_{j_i}}^{y_k}\right)=e\left(g_1,B_{j_i}\right)\end{aligned} \tag{10}$$

4)判断$e\left(X_k,a_j\right)e\left(X_k,b_j\right)^{m_{j_0}}\prod_{i=1}^{l}e\left(X_k,B_{j_i}\right)^{m_{j_i}}=e\left(g_1,c_j\right)$是否成立，以验证$c_j$是否正确，表示为

$$\begin{aligned}&e\left(X_k,a_j\right)e\left(X_k,b_j\right)^{m_{j_0}}\prod_{i=1}^{l}e\left(X_k,B_{j_i}\right)^{m_{j_i}}= \\ &e\left({g_1}^{x_k},a_j\right)e\left({g_1}^{x_k},{a_j}^{y_k}\right)^{m_{j_0}}\prod_{i=1}^{l}e\left({g_1}^{x_k},{a_j}^{z_{k_i}y_k}\right)^{m_{j_i}}= \\ &e\left(g_1,a_j\right)^{x_k}e\left(g_1,a_j\right)^{x_k y_k m_{j_0}}\prod_{i=1}^{l}e\left(g_1,a_j\right)^{z_{k_i}x_k y_k m_{j_i}}= \\ &e\left(g_1,a_j\right)^{x_k + x_k y_k m_{j_0} + \sum_{i=1}^{l} z_{k_i} x_k y_k m_{j_i}}= \\ &e\left(g_1,a_j^{\,x_k + x_k y_k m_{j_0}\prod_{i=1}^{l}{A_{j_i}}^{x_k y_k m_{j_i}}}\right)=e\left(g,c_j\right)\end{aligned} \tag{11}$$

其中，${A_{j_i}}={a_j}^{z_{k_i}}$。

4.4　电动汽车充放电认证

EV_j获得充放电交易授权后，在指定的时间段到达目标CP，进行交易验证与充放电操作。在充放电认证中，EV_j计算盲化的交易凭证，生成交易假名以进行电力交易。EV_j将盲化交易凭证与对应的ZKP发送给CP，在泄露假名对应的秘密属性情况下，向CP证明拥有该假名。CP验证EV_j交易身份的合法性，并提供充放电服务。EV_j充放电认证如图5所示。

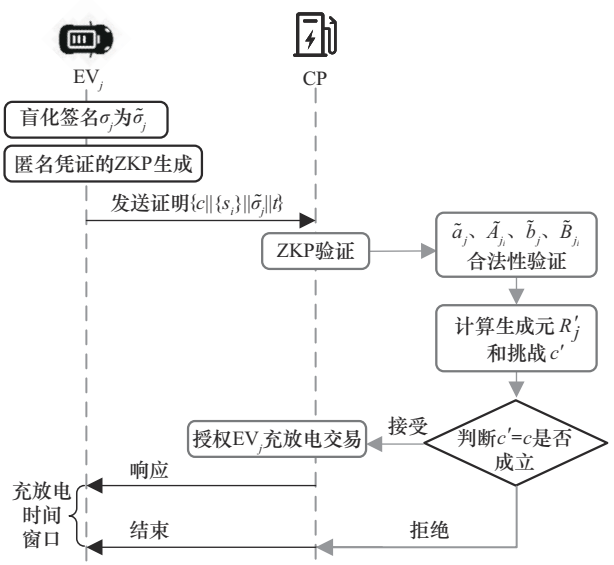

图5　EV_j充放电认证

盲化凭证生成：EV_j选择随机数$r,r'\in\mathbb{Z}_q$，计算盲化凭证为

$$\begin{aligned}&\tilde{\sigma}_j=\left(a_j^r,\{A_{j_i}^r\},b_j^r,\{B_{j_i}^r\},c_j^{rr'}\right)= \\ &(\tilde{a}_j,\{\tilde{A}_{j_i}\},\tilde{b}_j,\{\tilde{B}_{j_i}\},\tilde{c}_j^{r'})= \\ &(\tilde{a}_j,\{\tilde{A}_{j_i}\},\tilde{b}_j,\{\tilde{B}_{j_i}\},\hat{c}_j)\end{aligned} \tag{12}$$

其中，$\hat{c}_j$为$\tilde{c}_j$的进一步盲化，$\hat{c}_j$源自EV_j秘密属性的承诺M_j，满足均匀分布且独立于其他参数，可作为假名参与电力交易。充放电交易完成后，EV_j的假名及其对应交易信息将记录上链，用于交易查询与仲裁。

凭证证明生成：充放电认证中，EV_j需要向CP证明其拥有交易凭证对应的秘密属性A_j，对应的ZKP为

$$\mathrm{PK}\left\{m_{j_0},m_{j_1},\cdots,m_{j_l},r':(v_s)^{-r'}=v_x(v_{xy})^{m_{j_0}}\prod_{i=1}^{l}(v_{xy}^i)^{m_{j_i}}\right\} \tag{13a}$$

$$v_x=e(X_k,\tilde{a}_j) \tag{13b}$$

$$v_{xy}=e(X_k,\tilde{b}_j) \tag{13c}$$

$$v_{xy}^i=e(X_k,\tilde{B}_{j_i}) \tag{13d}$$

$$v_s=e(g_1,\hat{c}_j) \tag{13e}$$

交易凭证证明生成过程如下。

1)EV_j计算v_x、v_{xy}、$\left\{v_{xy}^i\right\}$和v_s。

2)选择随机数$r_i\in\mathbb{Z}_q,0\leqslant i\leqslant l+1$，计算生成元$R=\left(v_{xy}\right)^{r_0}\prod_{i=1}^{l}\left(v_{xy}^i\right)^{r_i}\left(v_s\right)^{r_{l+1}}$。

3)计算挑战$c=H\left(v_x\|v_{xy}\|\left\{v_{xy}^i\right\}\|v_s\|R\|\tilde{\sigma}_j\|t\right)$，$t$是当前的时间戳。

4)计算响应$\left\{s_i\right\}$，其中$s_i=r_i-c_im_{j_i}\bmod p$，$0\leqslant i\leqslant l$，$s_{l+1}=r_{r+1}-cr'$，生成$\left\{c\|\left\{s_i\right\}\|\tilde{\sigma}_j\|t\right\}$并发送给对应CP。

凭证证明验证：CP收到EV_j发送的信息后，判断时间戳t是否有效，进而验证盲化凭证$\tilde{\sigma}_j$的合法性，判断下列等式是否成立，即

$$e\left(\tilde{a}_j,Z_{j_i}\right)=e\left(g_1,\tilde{A}_{j_i}\right) \tag{14a}$$

$$e\left(\tilde{a}_j,Y_k\right)=e\left(g_1,\tilde{b}_j\right) \tag{14b}$$

$$e\left(\tilde{A}_{j_i},Y_k\right)=e\left(g_1,\tilde{B}_{j_i}\right) \tag{14c}$$

该ZKP过程如下。

1)CP首先计算v_x、v_{xy}、$\left\{v_{xy}^i\right\}$和v_s，进而计算$R_j'=\left(\left(v_{xy}\right)^{s_0}\prod_{i=1}^{l}\left(v_{xy}^i\right)^{s_i}v_s^{s_{l+1}}\right)\left(v_x^{-1}\right)^c$，生成$c'=H\left(v_x\|v_{xy}\|\left\{v_{xy}^i\right\}\|v_s\|R_j'\|\tilde{\sigma}_j\|t\right)$。

2)判断等式$c'=c$是否成立，成立则接受凭证，否则拒绝。等式$c'=c$的正确性来自$R_j'=R_j$，计算式为

$$\begin{aligned}R_j'&=((v_{xy})^{s_0}\prod_{i=1}^{l}(v_{xy}^i)^{s_i}v_s^{s_{l+1}})(v_x^{-1})^c=\\&((v_{xy})^{s_0}\prod_{i=1}^{l}(v_{xy}^i)^{s_i}v_s^{s_{l+1}})((v_{xy})^{m_{j_0}}\prod_{i=1}^{l}(v_{xy}^i)^{m_{j_i}}v_s^{r'})^c=\\&(v_{xy})^{s_0+cm_{j_0}}\prod_{i=1}^{l}(v_{xy}^i)^{s_j+cm_{j_i}}(v_s)^{s_{l+1}+cr'}=\\&\left(v_{xy}\right)^{r_0}\prod_{i=1}^{l}(v_{xy}^i)^{r_i}\left(v_s\right)^{r_{l+1}}=R_j\end{aligned} \tag{15}$$

完成上述验证后，CP为EV_j提供充放电服务。根据认证过程可知，EV_j在交易中生成的假名具有唯一性，能够保障任何实体无法将不同的假名关联到同一主密钥。从而对手无法通过关联EV_j的多次电力交易提取用户的交易习惯等隐私信息。此外，由于对手无法得知假名对应的主密钥及其他属性，不能通过假名验证自己的身份，故无法通过伪造和冒用假名进行交易攻击。

5　安全性与隐私分析

本文隐私保护认证方案旨在V2G网络电力交易身份认证中保障EV的隐私信息，具有匿名、不可关联及不可伪造等特性，能有效抵御V2G电力交易过程中潜在的攻击威胁。针对3.2节所述常见的电力交易系统威胁，方案的安全性分析如下。

BC节点攻击：本文方案中，EV_j通过ZKP向BC节点证明拥有承诺对应的匿名秘密属性，以获取电力交易许可。EV_j无须透露任何真实身份信息，BC节点仅知道经过认证的用户通过匿名请求充放电交易。由于不同交易采用的假名$\hat{c}_j$不同，半可信、不可信BC节点无法通过观察交易数据集关联用户交易信息，从而无法推断EV_j的充放电习惯、位置等隐私信息。

CP攻击：在EV_j与CP的交互中，本文方案通过CL签名生成其假名$\hat{c}_j$，并获得ZKP的认证。CP无法将$\hat{c}_j$关联到EV_j的真实身份，仅知道经过认证并获得交易授权的用户在分配的时间段内进行了充放电。因此，恶意CP无法通过分析EV_j的交易请求和身份凭证，获取交易信息等敏感数据。

联盟链账本攻击：根据本文方案，BC节点所保存的交易信息以假名$\hat{c}_j$作为标识。因此，即使联盟链中授权用户有权查看交易数据，但仍无法通过假名将EV_j的交易信息进行关联，从而无法根据可

访问数据分析EV用户身份、充电习惯、位置等隐私信息。

中间人攻击：在EV_j与BC节点的交互过程中，根据本文方案，消息可采用BC节点的公钥pk_{BC_k}进行加密。由于没有对应的私钥sk_{BC_k}，攻击者无法从截获的交互信息中获取其明文。由于采用了匿名凭证与ZKP，即使攻击者通过恶意控制BC节点等方式获得了明文信息，只能获得EV_j的充放电时间段及与其绑定的假名，无法将其与EV_j的真实身份关联，从认证过程中获取用户隐私信息。

重放攻击：本文方案加入了时间戳，标识凭证的有效时间范围。验证者可根据时间戳判断凭证是否处于有效时间，从而抵御重放攻击。

根据安全性分析可知，即使系统中存在半可信或恶意节点，本文方案能够保障交易过程不泄露任何EV隐私信息。在任意认证过程中，验证方通过ZKP为证明方颁发凭证，从而无法接触证明方的隐私信息。因此，EV的身份凭证具有匿名和不可关联性，BC节点和CP难以将同一凭证的不同证明进行关联，从而任何内、外部攻击者无法从信道截获的消息或区块链账本提取EV的隐私信息。故本文方案能够在电力交易过程中保障EV的隐私安全。

6 性能分析

在本节中，从计算开销和通信开销对本文隐私保护认证方案进行评估。方案采用的CL签名算法和Schnorr NIZKP协议基于JPBC（java pairing-based cryptography）库[19]的Type A双线性映射算法编程实现。仿真系统运行环境为CentOS 7.4，配置为Intel(R) 4核CPU@2.80 GHz，8 GB内存。联盟链电力交易系统基于Hyperledger Fabric v2.3.2构建，客服端程序基于fabric-sdk-java开发，智能合约基于fabric-chaincode-java开发。方案所采用的双线性映射在域$\mathbb{F}_p(|p|=512\ \text{bit})$上构造，$\mathbb{G}_1$为在椭圆曲线$E(\mathbb{F}_p)$上的点构成的群，最大质数阶为$q$（$|q|=160\ \text{bit}$）。方案涉及的实验数据均由仿真系统运行产生，其中EV用于认证身份的秘密属性包含主密钥、CP编号、充电时间、车辆信息等。由于认证方案为EV每个秘密属性$a_1 \in A$生成固定长度的承诺M（$|M|=L_{\mathbb{G}_1}$），因此方案的计算开销与通信开销仅与秘密属性的个数相关，与具体属性内容无关。

6.1 计算开销评估

针对本文方案中匿名属性认证、凭证颁发及EV充放电认证过程，评估不同参与实体的在参与签名与签名认证、ZKP生成与验证时的计算成本。在仿真实验中，群$\mathbb{G}_1$和$\mathbb{G}_T$中指数运算成本实测为$T_{_1}=9.9\ \text{ms}$和$T_{\mathbb{G}_T}=0.7\ \text{ms}$，双线性映射对计算开销实测为$T_{\text{bp}}=5.6\ \text{ms}$。方案涉及的随机数生成、哈希等其他计算开销此处忽略不计。

在匿名属性验证中，EV验证BC节点公钥pk_{BC}时，需要在群$\mathbb{G}_1$上进行$l+3$次指数运算；生成秘密属性对应承诺M_j需要在群$\mathbb{G}_1$上进行$l+1$次指数运算；生成承诺证明需要在群$\mathbb{G}_1$上进行$l+1$次指数运算。因此，EV在匿名属性验证中的总计算开销为$(3l+5)T_{\mathbb{G}_1}$。对于BC节点，其验证EV承诺M_j需要在群$\mathbb{G}_1$上进行$l+2$次指数运算。

在凭证颁发中，EV验证BC对承诺M_j的签名σ_j需要验证A_{j_i}、b_j和B_{j_i}、c_j是否正确，分别需要$2l$、$2(l+1)$、$l+3$次对计算，此外验证c_j还需在群$\mathbb{G}_T$上进行$l+1$次指数运算，因此EV在凭证颁发中的总计算开销为$(l+1)T_{\mathbb{G}_T}+(5l+5)T_{\text{bp}}$。对于BC节点，其生成凭证签名需要在群$\mathbb{G}_1$上进行$2l+4$次指数运算。

在EV充放电认证过程中，EV生成盲化凭证和ZKP，需要$l+3$次对计算及$l+2$次$\mathbb{G}_1$上的指数运算，计算开销为$(l+2)T_{\mathbb{G}_T}+(l+3)T_{\text{bp}}$。对于CP，验证EV的凭证需要判断$\tilde{a}_j$、$\left\{\tilde{A}_{j_i}\right\}$、$\tilde{b}_j$、$\left\{\tilde{B}_{j_i}\right\}$的合法性，共需要$4l+2$次对运算；验证EV交易请求的ZKP大约需要$l+3$次对计算和$l+3$次$\mathbb{G}_T$上的指数运算，计算开销为$(l+3)T_{\mathbb{G}_T}+(l+3)T_{\text{bp}}$。

从而，EV进行一次电力交易产生的开销为$(3l+5)T_{G_1}+(2l+3)T_{G_T}+(6l+8)T_{\text{bp}}$。令BC节点服务的EV最大数量为$N$，则BC节点为$N$个EV提供充放电服务所需开销为$N(3l+6)T_{_1}$。对于CP，其为一个EV提供充放电服务所需开销为$(l+3)T_{\mathbb{G}_T}+(5l+5)T_{\text{bp}}$。

单个BC节点的计算开销由秘密属性的数量l和EV的数量N决定，如图6所示。当BC节点服务50个EV，每个EV仅保密其私钥sk_{EV}，节点的

计算开销获得最小值210 ms。当BC节点服务500个EV，且每个EV的秘密属性增加10个，节点的计算开销获得最大值12 600 ms。因此，在本文方案中，BC节点能够及时处理多个EV的并发服务请求，在可接受时间内完成验证与签名。对于单个EV请求充放电交易服务时，EV、BC节点和CP的计算开销仅由l决定，如图7所示。当EV仅保密私钥$\mathrm{sk}_{\mathrm{EV}}$时，EV、BC节点和CP的计算开销分别为96.4 ms、4.2 ms和30.1 ms；当EV保密的秘密属性增加10个时，EV、BC节点和CP的计算开销分别为743.4 ms、25.2 ms和317.1 ms。因此，本文方案 单个EV的身份认证响应时间能够满足用户需求。

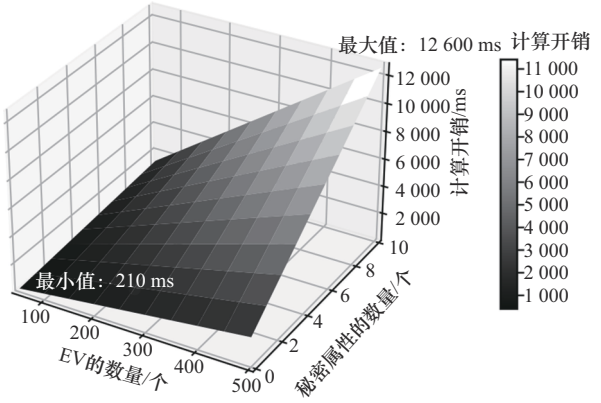

图6　单个BC节点的计算开销

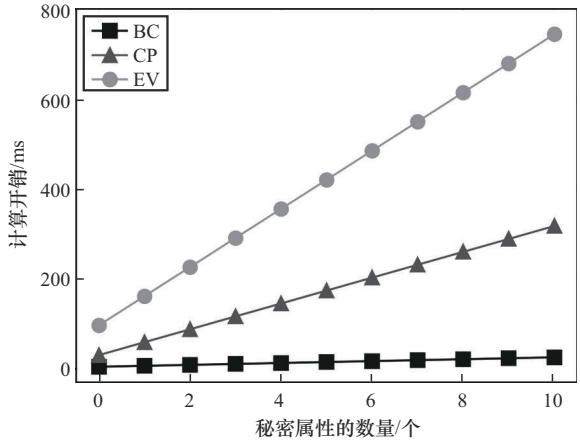

图7　单个EV电力交易中各实体计算开销

6.2　通信开销评估

在本文方案中，Schnorr NIZKP协议使用的安全哈希函数为SHA-256，哈希值长度$L_H = 256$ bit。根据仿真系统设置，$\mathbb{Z}_q$中的元素长度为$L_{\mathbb{Z}_q} = 160$ bit，群$\mathbb{G}_1$中的元素长度为$L_{\mathbb{G}_1} = 512$ bit。

对于EV与BC节点之间的通信开销，在匿名属性验证中，EV发送给BC节点的证明$\{c\|\{s_i\}\|M\|t\}$中，c的大小为L_H，$\{s_i\}$的总大小为$(l+1)L_{\mathbb{Z}_q}$，M的大小为$L_{\mathbb{G}_1}$，t忽略不计。在凭证颁发过程中，BC节点发送给EV的签名σ中，a、b、c的大小均为$L_{\mathbb{G}_1}$，$\{A_i\}$和$\{B_i\}$的大小均为$lL_{\mathbb{G}_1}$。因此，N个EV与BC节点之间的总通信开销为$N\left[L_H + (l+1)L_{\mathbb{Z}_q} + (2l+4)L_{\mathbb{G}_1}\right]$，如图8所示。当BC节点服务50个EV，且每个EV仅保密其私钥$\mathrm{sk}_{\mathrm{EV}}$，节点的通信开销获得最小值123 200 bit ≈ 15 KB。当服务500个EV，每个EV增加10个秘密属性，节点的通信开销获得最大值7 152 000 bit ≈ 873 KB。

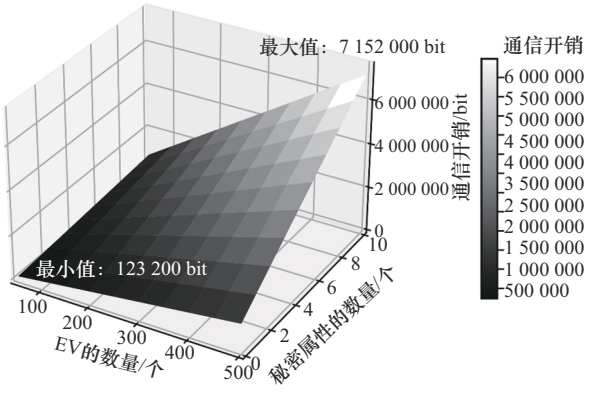

图8　EV与BC节点之间的通信开销

对于EV与CP之间的通信开销，在充放电认证中，EV发送给CP的凭证$\{c\|\{s_i\}\|\tilde{\sigma}\|t\}$中，$c$的大小为$L_H$，$\{s_i\}$的总大小为$(l+2)L_{\mathbb{Z}_q}$，$\tilde{\sigma}$的大小为$(2l+3)L_{\mathbb{G}_1}$，$t$忽略不计。因此，EV与CP之间的总通信开销为$L_H + (l+2)L_{\mathbb{Z}_q} + (2l+3)L_{\mathbb{G}_1}$。

当EV秘密属性只有$\mathrm{sk}_{\mathrm{EV}}$时，其与BC节点和CP的通信开销分别为2 112 bit和2 464 bit，当EV保密的秘密属性增加10个时，其与BC节点和CP的通信开销分别为14 304 bit和13 952 bit。因此，本文方案所设计的匿名凭证签发及充放电认证过程占用的通信资源均较少，适用于基于区块链的电力交易系统。

6.3　方案安全性与性能对比

本节从安全功能和算法开销2个方面，将本文提出的认证方案与最新基于区块链的隐私保护认证

方案[12,15,29-30]进行了对比。

不同方案安全功能对比如表 1 所示。文献[12]中交易实体的伪身份采用哈希算法生成，函数输入为公钥、身份标识和时间戳。由于只有时间戳变化，攻击者可能通过哈希碰撞攻击实现身份关联和伪造。文献[15]采用可信第三方进行用户注册和管理，存在权限滥用与未授权访问风险，导致令牌伪造、中间人攻击等。文献[29]中 CA 在注册阶段将 EV 公钥等信息记录上链，面临 BC 节点攻击的威胁。文献[30]借助可信第三方验证和维护区块链中电力交易记录，存在权力滥用和内部攻击问题。总之，即使中心化认证方案利用区块链辅助认证，仍因权力集中，难以抵抗内部攻击。本文方案依赖区块链的认证方案，除 EV 外，参与电力交易的任意实体无法获得 EV 的秘密属性，能够提供更好的安全功能，具体见安全性分析。

不同方案运行成本对比如表 2 所示，其中，哈希函数、群 $\mathbb{G}_2$ 中指数运算及椭圆曲线乘法运算成本分别为 $T_h \approx 0.006$ ms、$T_{\mathbb{G}_2} \approx 21.8$ ms、$T_{\text{ecm}} \approx 3.2$ ms，N_l 为文献[15]中会员管理树的深度。文献[12]的计算开销仅由 T_h 决定，计算开销最小，约为 0.078 ms。文献[29]与文献[30]的计算开销几乎由 T_{ecm} 决定，因此文献[29]计算开销约为 16.4 ms，小于文献[30]的 25.6 ms。但上述方案未考虑用户秘密属性对数量对于计算开销的影响，具有局限性。文献[15]和本文方案均采用双线性映射，考虑了秘密属性对的数量对计算开销的影响。在相同设置下，对于单个 EV 用户，当秘密属性仅有身份 ID 时，本文方案计算开销 185.9 ms 小于文献[15]的 567.13 ms。不同认证方案 EV 进行一次电力交易时的通信开销如图 9 所示。文献[12]传输的认证消息仅包含身份信息、公钥、时间戳等，获得最小通信开销；然而，该方案在计算通信开销时并未计入公钥、时间戳。在其他认证方案中，本文方案获得最小通信开销。

综上所述，在安全功能比较中，本文方案具有匿名、双向认证、不可关联、可追溯等特性，对内外部攻击具有鲁棒性。在性能对比中，本文方案获得较好表现，在同类型认证方案中，单个 EV 的计算开销减低了 67.2%，通信开销降低了 56.4%。在保障 EV 用户隐私安全的同时，需要的 EV 计算资源更少。

表 1 不同方案安全功能对比

方案	匿名性	双向认证	不可关联性	不可伪造性	可追溯性	抗内部攻击	抗中间人攻击	抗重放攻击
文献[12]	√	√	×	×	√	√	√	√
文献[15]	√	√	√	×	√	×	×	×
文献[29]	√	√	√	√	√	×	√	√
文献[30]	√	√	√	√	√	×	√	√
本文方案	√	√	√	√	√	√	√	√

表 2 不同方案运行成本对比

方案	EV	BC 节点/可信第三方	CP	总开销
文献[12]	$4T_h$	$5T_h$	$4T_h$	$13T_h$
文献[15]	$(15+N_l+l)T_{\mathbb{G}_1}+(4+N_l+l)T_{\mathbb{G}_1}+8T_{\mathbb{G}_T}+(6+2N_l)T_{\text{bp}}+2T_h$	$(4+2N_l)T_{\mathbb{G}_1}+3T_{\mathbb{G}_2}+T_h$	$5T_{\mathbb{G}_1}+(1+l)T_{\mathbb{G}_2}+12T_{\mathbb{G}_T}+8T_{\text{bp}}+2T_h$	$(24+3N_l+l)T_{\mathbb{G}_1}+(8+N_l+2l)T_{\mathbb{G}_2}+20T_{\mathbb{G}_T}+(14+2N_l)T_{\text{bp}}+5T_h$
文献[29]	$23T_h+T_{\text{ecm}}$	$21T_h$	$18T_h+4T_{\text{ecm}}$	$62T_h+5T_{\text{ecm}}$
文献[30]	$3T_h+T_{\text{ecm}}$	$2T_h+3T_{\text{ecm}}$	$3T_h+4T_{\text{ecm}}$	$7T_h+8T_{\text{ecm}}$
本文方案	$(3l+5)T_{\mathbb{G}_1}+(2l+3)T_{\mathbb{G}_T}+(6l+8)T_{\text{bp}}+3T_h$	$N(3l+6)T_{\mathbb{G}_1}+2NT_h$	$(l+3)T_{\mathbb{G}_T}+(5l+5)T_{\text{bp}}+T_h$	$(3Nl+3l+6N+5)T_{\mathbb{G}_1}+(3l+6)T_{\mathbb{G}_T}+(11l+13)T_{\text{bp}}+(2N+4)T_h$

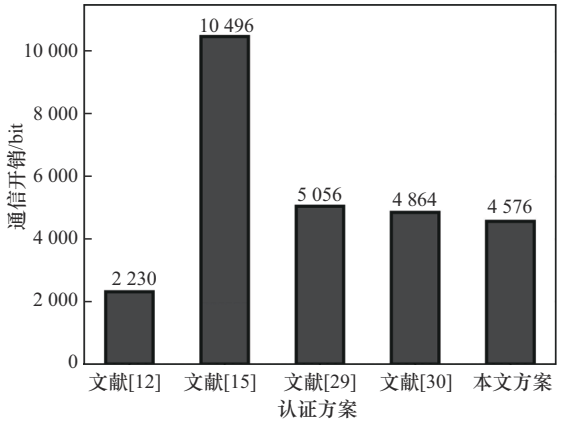

图9　不同认证方案EV进行一次电力交易时的通信开销

7　结束语

针对V2G网络电力交易中潜在的EV隐私泄露问题，本文提出了基于匿名凭证与联盟链的电力交易隐私保护认证方案。该方案将匿名凭证、CL签名、ZKP与区块链结合，实现了去中心化的身份认证。电力交易中EV不提供任何隐私信息，具有不可伪造性、匿名性和不可关联性，可抵抗内、外部半可信、不可信实体的攻击。通过安全分析与性能比较，本文认证方案具有一定的先进性。在未来的工作中，将考虑多EV电力交易请求并发场景，进一步减少EV和V2G网络开销，以在资源受限环境下高效处理大规模用户充放电请求。

参考文献：

[1] LI Y C, HU B J. A consortium blockchain-enabled secure and privacy-preserving optimized charging and discharging trading scheme for electric vehicles[J]. IEEE Transactions on Industrial Informatics, 2021, 17(3): 1968-1977.

[2] YUCEL F, AKKAYA K, BULUT E. Efficient and privacy preserving supplier matching for electric vehicle charging[J]. Ad Hoc Networks, 2019, 90: 101730.

[3] GABAY D, AKKAYA K, CEBE M. Privacy-preserving authentication scheme for connected electric vehicles using blockchain and zero knowledge proofs[J]. IEEE Transactions on Vehicular Technology, 2020, 69(6): 5760-5772.

[4] HAN W L, XIAO Y. Privacy preservation for V2G networks in smart grid: a survey[J]. Computer Communications, 2016, 91: 17-28.

[5] YANG X H, LI W J. A zero-knowledge-proof-based digital identity management scheme in blockchain[J]. Computers & Security, 2020, 99: 102050.

[6] ROTTONDI C, FONTANA S, VERTICALE G. Enabling privacy in vehicle-to-grid interactions for battery recharging[J]. Energies, 2014, 7(5): 2780-2798.

[7] 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.

[8] CHEN J, ZHANG Y Y, SU W C. An anonymous authentication scheme for plug-in electric vehicles joining to charging/discharging station in vehicle-to-Grid (V2G) networks[J]. China Communications, 2015, 12(3): 9-19.

[9] 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.

[10] SUBRAMANI J, MARIA A, SEKAR RAJASEKARAN A, et al. Mutual and batch authentication with conditional privacy-preserving scheme for V2G communication system[J]. IEEE Access, 2024, 12: 69593-69602.

[11] 胡柏吉, 张晓娟, 李元诚, 等. 支持多功能的V2G网络隐私保护数据聚合方案[J]. 通信学报, 2023, 44(4): 187-200.
HU B J, ZHANG X J, LI Y C, et al. Multi-function supported privacy protection data aggregation scheme for V2G network[J]. Journal on Communications, 2023, 44(4): 187-200.

[12] AGGARWAL S, KUMAR N, GOPE P. An efficient blockchain-based authentication scheme for energy-trading in V2G networks[J]. IEEE Transactions on Industrial Informatics, 2021, 17(10): 6971-6980.

[13] WAN Z G, ZHANG T, LIU W Z, et al. Decentralized privacy-preserving fair exchange scheme for V2G based on blockchain[J]. IEEE Transactions on Dependable and Secure Computing, 2022, 19(4): 2442-2456.

[14] WANG Y S, LI Y X, ZHAO J J, et al. A fast and secured peer-to-peer energy trading using blockchain consensus[C]//Proceedings of the 2022 IEEE Industry Applications Society Annual Meeting (IAS). Piscataway: IEEE Press, 2022: 1-8.

[15] YUE X H, BI X, YANG H B, et al. PAP: a privacy-preserving authentication scheme with anonymous payment for V2G networks[J]. IEEE Transactions on Smart Grid, 2024, 15(6): 6092-6111.

[16] BEN SASSON E, CHIESA A, GARMAN C, et al. Zerocash: decentralized anonymous payments from Bitcoin[C]//Proceedings of the 2014 IEEE Symposium on Security and Privacy. Piscataway: IEEE Press, 2014: 459-474.

[17] CAMENISCH J, LYSYANSKAYA A. Signature schemes and anonymous credentials from bilinear maps[C]// Advances in Cryptology – CRYPTO 2004. Berlin: Springer, 2004: 56-72.

[18] AGRAWAL S, GANESH C, MOHASSEL P. Non-interactive zero-knowledge proofs for composite statements[C]//Advances in Cryptology – CRYPTO 2018. Berlin: Springer, 2018: 643-673.

[19] DE CARO A, IOVINO V. jPBC: Java pairing based cryptography[C]// Proceedings of the 2011 IEEE Symposium on Computers and Communications (ISCC). Piscataway: IEEE Press, 2011: 850-855.

[20] SHEN J, ZHOU T Q, WEI F S, et al. Privacy-preserving and lightweight key agreement protocol for V2G in the social Internet of Things[J]. IEEE Internet of Things Journal, 2018, 5(4): 2526-2536.

[21] 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.

[22] 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.

[23] ZHANG Y H, ZOU J, GUO R. Efficient privacy-preserving authentication for V2G networks[J]. Peer-to-Peer Networking and Applications, 2021, 14(3): 1366-1378.

[24] XIA Z Q, FANG Z W, GU K, et al. Effective charging identity authentication scheme based on fog computing in V2G networks[J]. Journal of Information Security and Applications, 2021, 58: 102649.

[25] 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.

[26] 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.

[27] LIANG Y F, LIU Y N, ZHANG X C, et al. Physically secure and privacy-preserving charging authentication framework with data aggregation in vehicle-to-grid networks[J]. IEEE Transactions on Intelligent Transportation Systems, 2024, 25(11): 18831-18846.

[28] 范馨月, 刘洁, 何嘉辉. V2G中基于PUF的轻量级匿名认证协议[J]. 通信学报, 2024, 45(10): 129-141.
FAN X Y, LIU J, HE J H. Lightweight anonymous authentication protocol based on PUF in V2G [J]. Journal on Communications, 2024, 45(10): 129-141.

[29] KWON D, SON S, PARK K, et al. Design of blockchain-based multi-domain authentication protocol for secure EV charging services in V2G environments[J]. IEEE Transactions on Intelligent Transportation Systems, 2024, 25(12): 21783-21795.

[30] SHARMA G, JOSHI A M, MOHANTY S P. sTrade: blockchain based secure energy trading using vehicle-to-grid mutual authentication in smart transportation[J]. Sustainable Energy Technologies and Assessments, 2023, 57: 103296.

[作者简介]

李元诚（1970– ），男，山东烟台人，博士，华北电力大学教授，主要研究方向为密码学、数据隐私保护、网络空间安全，电力信息安全等。

胡柏吉（1992– ），男，湖南衡阳人，中国电力科学研究院有限公司中级工程师，主要研究方向为数据安全、无线通信安全等。

黄戎（1995– ），女，贵州黔西南州人，博士，华北电力大学讲师，主要研究方向为电力信息安全、人工智能安全等。