支持多功能的 V2G 网络隐私保护数据聚合方案

胡柏吉[1,2]，张晓娟[2]，李元诚[1]，赖荣鑫[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：针对目前隐私保护数据聚合方案的功能不够完善，不足以满足日益丰富的应用需求问题，提出了一个支持多功能的 V2G 网络隐私保护数据聚合（MFPDA）方案。基于 BGN、BLS、Shamir 密码共享等密码算法，以及雾计算和联盟链技术，将支持容错、抵抗内部攻击、批量签名验证、不需要可信第三方和多种聚合函数等多个安全功能纳入一个隐私保护数据聚合方案中。安全性分析表明，所提方案满足数据聚合的安全性、隐私性和可靠性。性能评估表明，雾计算的引入能显著减少控制中心的计算开销，减少率可达 66.6%；对联盟链的改进能有效减少系统的通信和存储开销，减少率分别可达 16.7%和 24.9%。

关键词：隐私保护；数据聚合；BGN 同态密码系统；联盟链
中图分类号：TP309.2
文献标志码：A
DOI: 10.11959/j.issn.1000−436x.2023081

Multi-function supported privacy protection data aggregation scheme for V2G network

HU Baiji[1,2], ZHANG Xiaojuan[2], LI Yuancheng[1], LAI Rongxin[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: In view of the problem that the functions of the current privacy protection data aggregation scheme were insufficient to meet the increasingly rich application requirements, a multi-function supported privacy protection data aggregation (MFPDA) scheme for V2G network was proposed. By using cryptographic algorithms such as BGN, BLS, and Shamir's secret sharing, as well as fog computing and consortium blockchain technology, multiple security functions like fault tolerance, resistance to internal attacks, batch signature verification, no need for trusted third parties, and multiple aggregation functions were integrated into one privacy protection data aggregation scheme. Security analysis shows that the proposed scheme can protect data aggregation's security, privacy and reliability. The performance evaluation shows that the introduction of fog computing can significantly reduce the computing overhead of the control center, and the reduction rate can be as high as 66.6%; the improvement of the consortium blockchain can effectively reduce the communication and storage overhead of the system, and the reduction rate can reach 16.7% and 24.9% respectively.

Keywords: privacy protection, data aggregation, BGN homomorphic cryptosystem, consortium blockchain

0 引言

随着电动汽车的大规模使用，V2G（vehicle to grid）网络逐渐成为智能电网中至关重要的一部分。得益于电池技术的发展，电动汽车不但可在用电低谷期作为分布式储能单元进行充电，也可以在用电高峰期临时充当分布式能源进行放电，从而对电网负荷起到削峰填谷的作用[1]。虽然双向电力交易引起的双向通信和电力流能够创造更多的经济效益，但同时也带来了新的隐私保护挑战。一方面，控制

收稿日期：2022−11−04；**修回日期：**2023−03−23
通信作者：李元诚，ncepua@163.com
基金项目：国家重点研发计划基金资助项目（No.2020YFB0905900）
Foundation Item: The National Key Research and Development Program of China (No.2020YFB0905900)

中心需要监测电网和分析充放电数据来控制电力的生产、调度和计费过程[2]。例如，控制中心需要对电动汽车的充放电数据进行聚合来分析用户的充放电行为，预测电网负荷并提供动态定价和灵活的电力调度策略等。另一方面，用户不愿意暴露他们的私有数据，因为数据中的位置、身份信息等可能泄露隐私，如家庭住址、工作地点、娱乐地点和常去位置，而这些信息可能被攻击者用于推断用户健康状况、个人喜好、社会关系等[3-4]，甚至可能被犯罪分子利用。

为了解决上述问题，常用的方法是使用隐私保护数据聚合技术，并引入分布式数据处理和控制策略，将一部分计算压力卸载到本地聚合器[5]。首先，由本地聚合器收集和聚合所辖区域密文数据发给控制中心；然后，控制中心收集所有聚合器的数据进一步聚合得到总聚合数据的密文；最后，控制中心对总聚合密文数据进行解密得到聚合数据。这样，控制中心和聚合器等实体要么只能获得聚合数据，要么即使获得某个用户的密文数据，也无法对其解密来侵害用户隐私。同时，控制中心只需接收和解密少量密文数据，从而大大降低通信、存储和计算开销。

按照基础架构的不同，现有的智能电网隐私保护数据聚合方案可以大致分为基于传统网络架构、基于雾计算架构和基于区块链架构三类。基于区块链架构的隐私保护数据聚合方案虽然相比其他 2 种架构具有一定的安全优势，但大部分没有考虑充分利用本地计算资源，系统性能有待提高[6]。考虑到雾计算将计算任务分散到网络边缘的特性，可以将大量异构设备整合到区块链架构中来提高系统性能和降低系统运营成本。同时区块链的分散式数据管理、数据难以篡改、冗余备份和可追溯的特性可以解决雾计算存在的安全性问题。因此本文将雾计算和区块链进行整合来设计数据聚合方案。

除了数据完整性、隐私性等基本功能特性，隐私保护数据聚合方案具备的功能特性还包括支持容错、抵抗内部攻击、支持批量签名验证、不需要可信第三方和支持多种聚合函数等，但大多数方案只具备其中部分功能特性，即使存在 Chen 等[7]、Zhang 等[8]提出的支持多功能的数据聚合方案，也不具备以上大部分安全功能特性，不适用于基于隐私保护数据聚合的机器学习[9]和数据挖掘[10]等高级应用，从而无法满足 V2G 网络日益丰富的功能需求。

为了实现支持容错、抵抗内部攻击、支持批量签名验证、不需要可信第三方和支持多种聚合函数等多功能的 V2G 网络数据聚合，本文提出支持多功能的 V2G 网络隐私保护数据聚合（MFPDA）方案，具体贡献如下。

1) 通过集成全同态加密和秘密共享技术，为 V2G 网络设计了支持容错、抵抗内部攻击和支持多种聚合函数的隐私保护数据聚合方案。

2) 引入雾计算来卸载控制中心的计算压力，极大减少 V2G 网络数据聚合过程中控制中心的计算开销，减少率高达 66.6%。

3) 引入联盟链来解决对可信第三方的依赖问题，考虑到联盟链使用的椭圆曲线数字签名算法（ECDSA）[11]无法做签名聚合，逐个验证签名会导致较大的系统开销，因此本文将原始 MFPDA 方案中联盟链使用的 ECDSA 改进为具有较短签名和可批量签名验证的 BLS（Boneh-Lynn-Shacham）[12]算法，并调整交易和区块的存储结构来减少通信和存储开销，减少率分别可达 16.7%和 24.9%。

1 相关工作

近年来，为了兼顾智能电网中用户和控制中心的利益和应对数据聚合的隐私、安全和性能挑战，已有较多隐私保护数据聚合方案被提出。考虑到 V2G 网络是智能电网的重要组成部分，其思想同样适用于 V2G 网络中的隐私保护数据聚合。按照架构不同，隐私保护数据聚合方案可以分为以下几类。

第一类是基于传统网络架构的隐私保护数据聚合方案。Liu 等[13]提出一个不依赖可信数据收集单元的实用数据聚合方案。该方案将受信任的用户链接起来形成一个虚拟的聚合区域，从而在保护用户隐私的同时提高系统的鲁棒性。Ding 等[14]提出一种基于身份的高效计量数据聚合方案，支持聚合器和服务提供商对数据进行批量验证，在保证数据私密性和完整性的同时提高系统效率。Guo 等[15]基于一种新颖的对称加密算法来设计轻量化的隐私保护数据聚合方案，并提出了一个新颖的身份认证协议用于身份验证和安全地建立会话密钥。

传统的网络架构可实现有效且安全的数据聚合，但通常采用单聚合服务器（如只由一个控制中心充当聚合器），聚合器面临巨大的计算和通信压力，存在进一步减少计算和通信开销的可能性。近

年来，随着边缘设备功能的日益强大和广泛部署，雾计算使客户能够在本地管理和分析数据，从而将计算能力和数据分析扩展到网络边缘。这种方式可克服传统网络架构的缺陷且已被证明可以显著减少计算和通信开销[16]。因此出现了第二类基于雾计算架构的隐私保护数据聚合方案。Li 等[17]设计了移动边缘计算辅助的物联网隐私保护数据聚合方案，其相比于传统模型可以节省近一半的通信成本。Merad 等[18]提出应用于雾辅助计算的智能电网多维数据聚合方案，可以解决云计算架构中的带宽和时延问题。

相比传统架构，基于雾计算的架构可以减少控制中心的计算和通信开销，但这类方案数据存储常常集中在某个雾节点或者云服务器中，仍然存在传统架构面临的中心化和单点故障问题[19]。此外，以上方案通常需要一个可信第三方和完全可信的控制中心。但实际上可信第三方容易被恶意攻击者攻破从而泄露用户私人数据。区块链技术为解决以上问题提供了新思路。区块链最早由 Nakamoto[20]提出，本质上是一个去信任的分布式账本数据库，依赖密码学算法来确保数据难以篡改、难以伪造，并使用共识机制来维持账本数据的一致性。因此第三类方案将区块链和数据聚合隐私保护进行整合。Wang 等[21]提出通过分层的区块链系统聚合智能电表数据，并通过同态加密在聚合过程中保护单个智能电表数据的隐私。Fan 等[22]提出了基于区块链的不需要可信第三方的隐私保护数据聚合方案。该方案设计了新的领导者选举算法来选择挖矿节点，并利用 Paillier 密码系统来进行隐私数据聚合。然而基于区块链的隐私保护数据聚合方案虽然增强了系统的安全性和解决了单点故障问题，但它们没有考虑通过雾/边缘计算模式充分利用本地资源来提高系统性能。因此 Chen 等[19]集成雾计算和区块链，并结合 Paillier 密码系统、批处理聚合签名和匿名身份验证开发了一个具有较低计算开销的隐私保护数据聚合方案。Wang 等[23]提出基于区块链的安全策略来保护边缘网络中的数据聚合隐私，并开发了新的块生成规则来提高交易吞吐量和时延方面的系统性能。

上述方案在不同程度上解决了数据聚合的相应问题，但仍然存在一些不足。本文基于以上考虑，从安全性、效率、功能性和可靠性的角度出发，设计更符合 V2G 网络实际应用需求的隐私保护数据聚合方案。

2　预备知识

2.1　双线性对

合数阶双线性对。令 $\mathcal{G}$ 表示一个合数阶双线性群生成算法，以安全参数 $\tau\in\mathbb{Z}^+$ 为输入，输出 $(p,q,\mathbb{G},\mathbb{G}_T,e)$。$p$和$q$ 是 2 个大小由 τ 决定的大质数，$|p|=|q|=\tau$。$\mathbb{G}$和$\mathbb{G}_T$ 是 2 个阶为 $N=pq\in\mathbb{Z}$ 的循环群。$e:\mathbb{G}\times\mathbb{G}\to\mathbb{G}_T$ 是满足以下属性的双线性对。

1) 双线性：$\forall\, u,v\in\mathbb{G},a,b\in\mathbb{Z}_N$，$e(u^a,v^b)=e\cdot(u,v)^{ab}$。

2) 非退化性：$\exists\, g\in\mathbb{G}$，使 $e(g,g)\neq 1_{\mathbb{G}_T}$。

3) 可计算性：$\forall u,v\in\mathbb{G}$，存在一个多项式时间算法可以有效地计算 $e(u,v)$。

令 $\mathbb{G}_p$ 和 $\mathbb{G}_q$ 分别表示 $\mathbb{G}$ 中阶数为 p 和 q 的子群，可证明这 2 个子群是互相正交的：任意选择 $\mathbb{G}$ 上的一个生成元 g，则 g^q和g^p 分别是 $\mathbb{G}_p$ 和 $\mathbb{G}_q$ 的生成元。$\forall u\in\mathbb{G}_p,v\in\mathbb{G}_q$，$\exists\alpha_1,\alpha_2$ 满足 $u=(g^q)^{\alpha_1}$，$v=(g^p)^{\alpha_2}$。则 $e(u,v)=e((g^q)^{\alpha_1},(g^p)^{\alpha_2})=e(g^{\alpha_1},g^{\alpha_2})^{pq}=1$。

质数阶双线性对。令 $\mathcal{G}'$ 表示一个质数阶双线性群生成算法，选择安全参数 $\delta\in\mathbb{Z}^+$，输出 $(p',\mathbb{G}_1,\mathbb{G}_2,e')$。$p'$ 为一个大小为 δ bit 的质数，即 $|p'|=\delta$。$\mathbb{G}_1,\mathbb{G}_2$ 和 $\mathbb{G}'_T$ 是阶为 p' 的循环群。$e':\mathbb{G}_1\times\mathbb{G}_2\to\mathbb{G}'_T$ 是满足以下属性的双线性对。

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

2) 非退化性：存在 $u\in\mathbb{G}_1,v\in\mathbb{G}_2$，使 $e'(u,v)\neq 1_{\mathbb{G}_T}$。换句话说，$e'$ 不会将 $\mathbb{G}_1\times\mathbb{G}_2$ 中的所有对映射到 $\mathbb{G}'_T$ 中的单位元。

3) 可计算性：$\forall u\in\mathbb{G}_1,v\in\mathbb{G}_2$，$e'(u,v)$ 可在多项式时间内有效计算。

特别地，当 $\mathbb{G}_1=\mathbb{G}_2$ 时，e' 称为对称质数阶双线性对，否则称为非对称质数阶双线性对。

2.2　BGN 同态密码系统

BGN（Boneh-Goh-Nissim）密码系统是由 Boneh 等[24]在 2005 年提出的一个具有全同态性质的公钥密码系统，包含以下算法和性质。

密钥生成。给定安全参数 $\tau\in\mathbb{Z}^+$，运行合数阶双线性对的群生成算法 $\mathcal{G}(\tau)$ 得到 $(p,q,\mathbb{G},\mathbb{G}_T,e)$。随机选择 2 个生成元 $g,x\in\mathbb{G}$，并令 $h=x^q$，$x=g^\alpha$，α 是 x 以 g 为底的指数，则 h 为 $\mathbb{G}$ 的 p 阶子群的一个随

机生成元。$\mathrm{PK_B}=(N,\mathbb{G},\mathbb{G}_T,e,g,h)$ 和 $\mathrm{SK_B}=p$ 分别为 BGN 系统的公钥和私钥。

加密。对给定的消息 $m\in\{0,1,\cdots,M\}$，其中 $M\ll q$ 是消息空间的上界。选择随机数 $r\in\mathbb{Z}_N$ 并计算密文 $c=E(m,r)=g^m h^r\in\mathbb{G}$。

解密。给定私钥 $\mathrm{SK_B}$ 和密文 c，计算 $c^p=(g^m\ h^r)^p=(g^p)^m(h^p)^r=(g^p)^m$。令 $g_p=g^p$，则 $c^p={g_p}^m$，消息 m 可以通过求以 g_p 为底的 c^p 的离散对数得到。BGN 同态密码系统对明文空间有一定的限制，即 M 不能过大。因为解密的时候需要计算群上的离散对数，这在指数较大时是计算困难的。但当 M 较小时，利用 Pollard 的 λ 方法[25]可以在时间 $O(\sqrt{M})$ 计算得到明文 m。

加法同态性。$\forall m_1,m_2,r_1,r_2$，有 $E(m_1,r_1)\ E(m_2,r_2)=E(m_1+m_2,r_1+r_2)$，利用以上解密算法可解密得到 m_1+m_2。

一次性乘法同态性。令 $e(g,g)=g_1$，$e(g,h)=h_1$。$\forall m_1,m_2,r_1,r_2$，有

$$\begin{aligned}&e(E(m_1,r_1),E(m_2,r_2))=\\&e(g,g)^{m_1m_2}e(g,h)^R=\\&{g_1}^{m_1m_2}{h_1}^R\in\mathbb{G}_T\end{aligned}\tag{1}$$

其中，$R=m_1r_2+m_2r_1+\alpha qr_1r_2$，$\alpha$ 虽然未知但是不影响解密。由合数阶双线性群的性质可知，g_1 的阶为 N，h_1 的阶为 p，则 ${h_1}^p=1$。首先，计算

$$\begin{aligned}&({g_1}^{m_1m_2}{h_1}^R)^p=({g_1}^{m_1m_2})^p({h_1}^p)^R=\\&({g_1}^{m_1m_2})^p=({g_1}^p)^{m_1m_2}\end{aligned}\tag{2}$$

然后，令 $\hat{g}_p={g_1}^p$，于是 m_1m_2 可以通过计算以 $\hat{g}_p$ 为底的 ${\hat{g}_p}^{m_1m_2}$ 的离散对数获得。

2.3 BLS 算法

BLS 算法[12]是基于非对称质数阶双线性对构建的短签名，具体如下。

密钥生成。首先，选择阶为质数 p' 的循环群 $\mathbb{G}_1,\mathbb{G}_2,\mathbb{G}'_T$ 和双线性对 $e':\mathbb{G}_1\times\mathbb{G}_2\to\mathbb{G}'_T$。然后，选择随机点 g' 作为群 $\mathbb{G}_2$ 的生成元。最后，选择哈希函数 $H:\{0,1\}^*\to\mathbb{G}_1$ 和私钥 $\mathrm{sk}\in\mathbb{Z}^*_{p'}$，并计算得到对应的公钥 $\mathrm{pk}=g'^{\mathrm{sk}}\in\mathbb{G}_2$。

签名。假设 $m\in\mathcal{M}$ 是待签名的消息。签名者计算 $\mathcal{H}=H(m)\in\mathbb{G}_1$ 和签名 $v=\mathcal{H}^{\mathrm{sk}}\in\mathbb{G}_1$。

验证签名。验证者接收 m 和 v 后计算 $\mathcal{H}=H(m)$，并检查等式 $e'(v,g')=e'(\mathcal{H},\mathrm{pk})$ 是否成立。

2.4 Shamir 秘密共享

Shamir 秘密共享[26]是一种 (k,n) 门限秘密共享方案，假设一个秘密数据 D 要分享给 n 个人，要求至少 k 个人就能恢复 D，且任意少于或等于 k–1 个人都不能恢复秘密，具体包括秘密分发阶段和秘密重构阶段。

秘密分发阶段。秘密分发者首先选择一个大质数 p'，其中 $p'>n\geqslant k$ 且 $p'>D$。其次，从有限域 $\mathrm{GF}(p')$ 随机选择 $k-1$ 个元素构造次多项式 $f(x)=a_0+a_1x+\cdots+a_{k-1}x^{k-1}(\mathrm{mod}\ p')$，其中，$a_0=D$，$a_i\in\mathbb{Z}_{p'},i=1,2,\cdots,k-1$ 为选择的随机值；再次，计算 n 个秘密碎片 $(x_i,f(x_i)),i=1,2,\cdots,n$ 分配给 n 个秘密保管者；最后，公开 p'，销毁 $f(x)$。

秘密重构阶段。假设有 k 个秘密保管者愿意帮助秘密恢复者恢复密钥。在恢复 D 时，首先需要每个秘密碎片 $(x_j,f(x_j)),j=1,2,\cdots,k$ 的保管人将自己的秘密碎片发送给秘密恢复者。然后，秘密恢复者可通过拉格朗日插值法，计算 $f(x)=\sum_{j=1}^{k}f(x_j)\prod_{l=1,l\neq j}^{k}\frac{x_l-x}{x_l-x_j}(\mathrm{mod}\ p')$，并令 $x=0$ 来恢复得到秘密数据 $D=f(0)$。

3 问题形式化描述

本节形式化地描述系统架构、敌手模型和设计目标。

3.1 系统架构

如图 1 所示，本文提出的雾和联盟链辅助的 V2G 网络主要由用户层、雾计算层和控制中心层组成，层与层之间通过公共互联网相互通信。

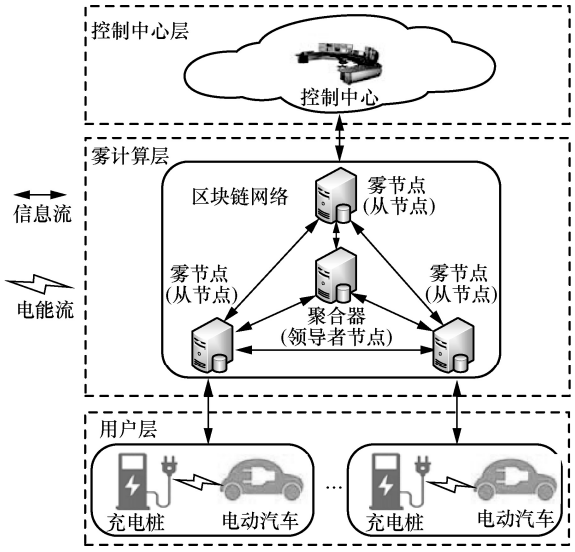

图 1 系统架构

用户层。用户层包含 ω 台电动汽车 $\mathbb{E}=\{\mathrm{EV}_1,\mathrm{EV}_2,\cdots,\mathrm{EV}_\omega\}$ 和 ω 个用于实施充放电的充电桩 $\mathbb{P}=\{\mathrm{CP}_1,\mathrm{CP}_2,\cdots,\mathrm{CP}_\omega\}$。充电桩 CP_i 内置智能电表周期性地测量电动汽车 EV_i 的充/放电量数据 d_i 和记录相应的认证信息，并对其加密和签名后发送到相应的雾节点。

雾计算层。雾计算层包含 σ 个雾节点 $\mathbb{F}=\{\mathrm{Fog}_1,\mathrm{Fog}_2,\cdots,\mathrm{Fog}_\sigma\}$，每个雾节点同时充当区块链节点，负责数据收集、存储和聚合，共同搭建一个区块链网络。本文采用 Hyperledger Fabric 搭建联盟链，其使用的 Raft 共识算法具有成熟、高效和高可靠性的领导者节点选择机制。考虑到单个节点可能被攻击者入侵从而导致单点故障，所以本文由领导者节点这个动态选择的可靠雾节点来临时充当聚合器。此外，领导者节点还参与分发系统公共参数和为节点提供注册服务。其他雾节点相应地被称作从节点。

首先，雾节点将初步验证通过的密文数据发送给聚合器（领导者节点），由聚合器使用批量签名验证来检查密文数据的完整性和认证其来源。然后，聚合器对所有密文充/放电数据进行多种类型的数据聚合。最后，聚合器将聚合的密文数据发送给 k+1 个正常工作的雾节点，由它们进行秘密共享处理后发送到控制中心层进行存储、解读与分析。

控制中心层。控制中心是 V2G 网络数据分析和网络控制的核心角色，具备云服务器的存储能力以及计算分析能力。控制中心接收来自所有雾节点的聚合密文数据和签名，对它们批量签名验证后存储在数据库中，并在需要时进行各种统计数据分析，如求和、均值、方差，对聚合密文数据进行多种类型的解读。

3.2　敌手模型

本文方案从可能面临的外部攻击者和内部攻击者角度来考虑敌手模型。

外部攻击者可能窃听任何 2 个相邻实体之间的通信信道，拦截和篡改通信数据，还可能发起重放攻击。外部攻击者甚至可能入侵内置智能电表的充电桩，通过直接访问或者篡改其数据来侵犯电动汽车用户的经济利益或者隐私。

内部攻击者可能出于商业或者经济目的等，通过攻破雾节点和控制中心来直接访问或篡改其存储的用户数据。内部攻击者还可能试图获取 BGN 同态密码系统的私钥来恢复单个电动汽车的充/放电数据，从而侵害用户隐私性。

3.3　设计目标

为了在上述敌手模型下实现安全、可靠、高效的多功能 V2G 网络隐私保护数据聚合，MFPDA 需要满足以下目标。

认证和数据完整性。所有系统实体都需要被授权为合法的参与者，在处理数据之前需要认证数据来源，保证数据由合法的实体生成。此外，系统应该能够验证数据的完整性，从而抵抗攻击者对数据的未授权篡改。

数据机密性和隐私性。在数据聚合过程中，应该保障端到端数据通信和数据存储的机密性，这样，即使攻击者窃听通信信道或者入侵数据库获得数据，它们也不能理解该加密的数据来提取用户的私密信息。此外，攻击者应该既不能直接解密单个电动汽车的密文充/放电数据，也不能解密聚合的密文数据来获取电动汽车用户的隐私数据。

支持容错。即使部分雾节点异常，其他正常雾节点也能聚合密文数据和协助控制中心解读聚合数据；即使部分电动汽车数据不能正常上报，控制中心也能聚合其他正常上报的数据。

抵抗内部攻击。即使内部攻击者通过攻击雾节点和控制中心来获取单个电动汽车用户的加密数据，也无法对其进行解密得到有效信息。

批量签名验证。批量签名验证可以在一次计算中完成多个数字签名的验证，从而减少系统计算开销，提高数据聚合效率。

不需要可信第三方。不依赖可信第三方来保障数据聚合的安全性和可靠性，从而避免可信第三方失效或被攻击导致的单点故障或隐私泄露等问题。

支持多种聚合函数。在保护用户隐私的前提下，支持除求和之外的多种聚合值计算，如平均值、方差等，提高方案的灵活性和适用性。

4　MFPDA 方案

本节详细介绍 MFPDA 方案的运行机制，包括系统设置、数据报告生成、报告验证和区块生成、隐私数据聚合、聚合数据解读这 5 个过程。MFPDA 方案中主要使用的符号及其描述如表 1 所示。

4.1　系统设置

首先，领导者节点选择适当安全参数 τ 和 δ，运行合数阶双线性对的群生成算法 $\mathcal{G}(\tau)$ 得到 BGN 同态密码系统的参数 $(N,p,q,\mathbb{G},\mathbb{G}_T,e,g,h)$，其中，$g,x$ 是 $\mathbb{G}$ 上的生成元，$x=g^{\alpha}$，α 未知，$h=x^{q}$ 是 $\mathbb{G}$

的 p 阶子群的一个生成元。其次，运行非对称质数阶双线性对的群生成算法 $\mathcal{G}'(\delta)$ 得到 BLS 签名系统参数 $(p',\mathbb{G}_1,\mathbb{G}_2,\mathbb{G}'_T,e',g')$，其中 g' 为群 $\mathbb{G}_2$ 的一个随机选择的生成元。再次，领导者节点需要选择安全的单向哈希函数 $H:\{0,1\}^*\to\mathbb{G}_1$。最后，领导者节点发布系统公共参数 $\mathrm{SP}_{\mathrm{pub}}=\{N,p',\mathbb{G},\mathbb{G}_T,\mathbb{G}_1,\mathbb{G}_2,\mathbb{G}'_T,e,e',g,g',H,h\}$，将 $\hat{g}=g^p$ 和 $\hat{g}_1=g_1^p$ 通过秘密信道发送给控制中心。

表 1　　符号及其描述

符号	描述
$N,\mathbb{G},\mathbb{G}_T,e,g,h$	BGN 公钥
p	BGN 私钥
ω	用户层的电动汽车/充电桩总数
σ	雾计算层的雾节点总数
$k+1$	$(k+1,\sigma)$ 门限秘密共享的阈值
EV_i	第 i 个电动汽车
CP_i	第 i 个充电桩
d_i	EV_i 的充/放电数据
C_i	第 i 个 BGN 密文充/放电数据
$\mathrm{id}_{\mathrm{EV}_i}$	EV_i 的身份标识
$\mathrm{id}_{\mathrm{CP}_i}$	CP_i 的身份标识
$\mathcal{S}_i$	CP_i 对第 i 个 BGN 密文数据的 BLS 签名
$\mathcal{P}_i$	EV_i 向雾节点上报的数据报告
T_i	第 i 个数据报告被打包成的一个交易
A_1	聚合器对所有密文进行均值聚合的结果
$A_2 \Vert A_3$	聚合器对所有密文进行方差聚合的结果
$A_4 \Vert A_5 \Vert A_6$	聚合器对所有密文进行单向方差分析聚合的结果
Fog_j	聚合器随机挑选的 $k+1$ 个正常工作的第 j 个雾节点
$\mathrm{id}_{\mathrm{Fog}_j}$	Fog_j 的身份标识
B_m^j	Fog_j 对 $A_m, m=1,\cdots,6$ 进行秘密共享计算得到的中间值
C^j	Fog_j 计算得到的聚合密文数据
$\mathcal{S}_{\mathrm{Fog}_j}$	Fog_j 对聚合密文数据 C^j 的 BLS 签名
M	每个充/放电数据大小的上限

此外，充电桩以及雾节点通过以下方式注册到系统。领导者节点选择随机数 $\mathrm{sk}_{\mathrm{CP}_i}\in\mathbb{Z}_{p'}^*$ 和计算 $\mathrm{pk}_{\mathrm{CP}_i}=g'^{\mathrm{sk}_{\mathrm{CP}_i}}$，并将它们分别作为私钥和公钥通过秘密信道分配给 CP_i。类似地，领导者节点随机生成一个 k 次多项式 $f(x)=p+a_1x+\cdots+a_kx^k \bmod p'$，其中，$p$ 为 BGN 私钥，$a_l\in\mathbb{Z}_{p'}$，$l=1,2,\cdots,k$，并计算 $\mathrm{sk}_{\mathrm{Fog}_j}=f(j)$，$\mathrm{pk}_{\mathrm{Fog}_j}=g'^{\mathrm{sk}_{\mathrm{Fog}_j}}$。$\mathrm{sk}_{\mathrm{Fog}_j}$ 和 $\mathrm{pk}_{\mathrm{Fog}_j}$ 分别作为私钥和公钥通过秘密信道分配给雾节点 Fog_j。这样，BGN 私钥 p 通过 Shamir 秘密共享的方式分配给多个雾节点，控制中心不能获取该私钥。

4.2　数据报告生成

如图 2 所示，电动汽车 EV_i 在其充放电过程中，充电桩 CP_i 每隔一定的时间段（如 15 min）采集一次数据 $d_i\in\{0,1,\cdots,M\}, i\in\{1,\cdots,\omega\}$。

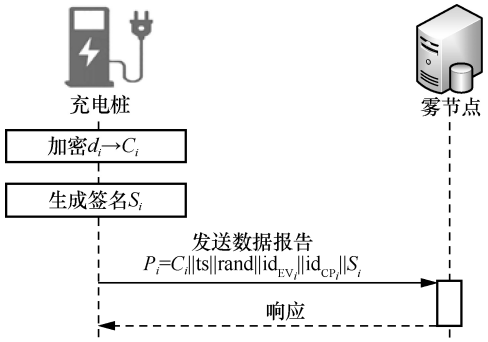

图 2　数据报告生成过程

数据加密。CP_i 使用 BGN 公钥对数据 d_i 进行加密得到密文 $C_i=g^{d_i}h^{r_i}\in\mathbb{G}$。

数据签名。为保证数据的完整性和数据来源的可靠性，CP_i 使用 BLS 算法对 C_i 进行签名得到 $\mathcal{S}_i=\mathcal{H}_i^{\mathrm{sk}_{\mathrm{CP}_i}}\in\mathbb{G}_1$，$\mathcal{H}_i=H(C_i\Vert\mathrm{ts}\Vert\mathrm{rand}\Vert\mathrm{id}_{\mathrm{EV}_i}\Vert\mathrm{id}_{\mathrm{CP}_i})$。其中，ts 表示当前时间戳，rand 表示一个随机数，它们结合 $\mathcal{S}_i$ 可抵抗重放攻击。

数据报告生成。CP_i 将数据报告 P_i 发送到所附属的雾节点，其中，$P_i=C_i\Vert\mathrm{ts}\Vert\mathrm{rand}\Vert\mathrm{id}_{\mathrm{EV}_i}\Vert\mathrm{id}_{\mathrm{CP}_i}\Vert\mathcal{S}_i$。

4.3　报告验证和区块生成

初步验证。如图 3 所示，收到来自 CP_i 的报告 P_i 后，从节点首先检查报告的时间戳 ts、rand、$\mathrm{id}_{\mathrm{EV}_i}$、$\mathrm{id}_{\mathrm{CP}_i}$ 来初步验证 P_i 的有效性。然后，验证合法的 P_i 被雾节点打包成交易 T_i 后发送到领导者节点。

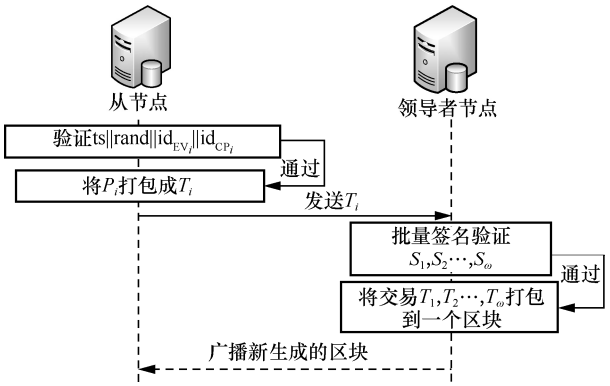

图 3　数据报告验证和区块生成过程

批量签名验证。领导者节点利用 BLS 算法对所有新增交易中的签名进行批量验证：$e'\left(\prod_{i=1}^{\omega}\mathcal{S}_i,g'\right)=\prod_{i=1}^{\omega}e'(\mathcal{H}_i,pk_{\mathrm{CP}_i})$，正确性证明如下。

$$e'\left(\prod_{i=1}^{\omega}\mathcal{S}_i,g'\right)=e'\left(\prod_{i=1}^{\omega}\mathcal{H}_i^{\mathrm{sk}_{\mathrm{CP}_i}},g'\right)=\prod_{i=1}^{\omega}e'(\mathcal{H}_i,g'^{\mathrm{sk}_{\mathrm{CP}_i}})=\prod_{i=1}^{\omega}e'(\mathcal{H}_i,\mathrm{pk}_{\mathrm{CP}_i}) \tag{3}$$

区块生成。所有验证通过的交易被领导者节点打包成区块后广播到雾计算层的所有其他从节点。最终每个区块链节点都将新的区块链接到本地区块链账本，从而维护区块链的一致性。需要说明的是，在将交易打包到区块时不需要保留每个交易的签名字段。只需在区块头保存一个签名聚合$\prod_{i=1}^{\omega}\mathcal{S}_i$以证明该区块中交易的合法性，不需要为每个交易单独保存签名，这样可以轻量化区块链的数据存储开销。因为一旦新生成的区块被链接到区块链，区块链的难以篡改、难以删除和可追溯的特性可保证所有交易的完整性和认证性。

4.4　隐私数据聚合

如图 4 所示，通过 Raft 共识算法推选出的领导者节点具有较高的可信性和可靠性。所以由领导者节点充当聚合器，在不需要解密的情况下对区块中密文数据$C_1,C_2,\cdots,C_\omega$进行多种类型的数据聚合。

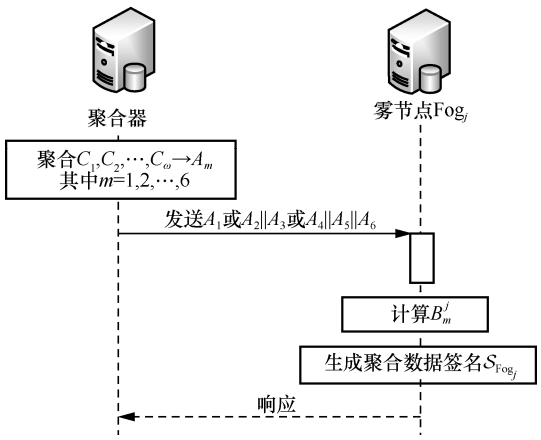

图 4　隐私数据聚合过程

均值聚合。所有电动汽车充放电量的均值$N_{\mathrm{mean}}=\frac{1}{\omega}\sum_{i=1}^{\omega}d_i$有助于控制中心进行实时负荷预测和动态电价制定。聚合器对密文数据进行如下均值聚合得到A_1。

$$A_1=\prod_{i=1}^{\omega}C_i=\prod_{i=1}^{\omega}(g^{d_i}h^{r_i})=g^{\sum_{i=1}^{\omega}d_i}h^{R_1} \tag{4}$$

其中，$R_1=\sum_{i=1}^{\omega}r_i \bmod p$。

方差聚合。令$N_{\mathrm{var}}=\sum_{i=1}^{\omega}(d_i-\bar{d})^2$，其中，$\bar{d}=\frac{\sum_{i=1}^{\omega}d_i}{\omega}$表示电动汽车充/放电量总体方差，可用于控制中心检测电动汽车充放电的异常波动情况。聚合器对密文数据进行如下方差聚合得到A_2和A_3。

$$A_2=e(\prod_{i=1}^{\omega}C_i,\prod_{i=1}^{\omega}C_i)=e(\prod_{i=1}^{\omega}g^{d_i}h^{r_i},\prod_{i=1}^{\omega}g^{d_i}h^{r_i})=e(g^{\sum_{i=1}^{\omega}d_i\sum_{i=1}^{\omega}r_i}h^{\sum_{i=1}^{\omega}d_i\sum_{i=1}^{\omega}r_i},g^{(\sum_{i=1}^{\omega}d_i)^2}h_1^{R_2}) \tag{5}$$

其中，$R_2=2\sum_{i=1}^{\omega}d_i\sum_{i=1}^{\omega}r_i+\alpha q\left(\sum_{i=1}^{\omega}r_i\right)^2 \bmod p$。

类似地，$A_3=\prod_{i=1}^{\omega}e(C_i,C_i)=g_1^{\sum_{i=1}^{\omega}d_i^2}h_1^{R_3}$，其中$R_3=\sum_{i=1}^{\omega}(2d_ir_i+\alpha qr_i^2) \bmod p$。

单向方差分析聚合。单向方差分析可用于找出有显著影响的因素。当运营商提出新的充放电电价策略时，可以通过单向方差分析判断哪种电价策略对电动车用户有显著影响，从而帮助运营商挑选最能激励用户的电价策略。本文假设分析的策略个数为ρ，每组样本数为ω。单向方差分析需要计算组内平方和$N_{\mathrm{ssw}}=\sum_{s=1}^{\rho}\sum_{i=1}^{\omega}(d_{si}-\bar{d}_{s\cdot})^2$和组间平方和$N_{\mathrm{ssb}}=\sum_{s=1}^{\rho}\omega(\bar{d}_{s\cdot}-\bar{d})^2$，其中，$\bar{d}_{s\cdot}=\frac{\sum_{i=1}^{\omega}d_{si}}{\omega}$，$\bar{d}=\frac{\sum_{s=1}^{\rho}\sum_{i=1}^{\omega}d_{si}}{\rho\omega}$，$d_{si}$表示电动汽车$\mathrm{EV}_i$在第$s$种电价策略下充/放电数据。令$C_{si}=g^{d_{si}}h^{r_{si}}$表示$d_{si}$的密文，聚合器对密文数据进行如下单向方差分析聚合得到A_4、A_5和A_6。

$$A_4=\prod_{s=1}^{\rho}\prod_{i=1}^{\omega}e(C_{si},C_{si})=\prod_{s=1}^{\rho}\prod_{i=1}^{\omega}e(g^{d_{si}}h^{r_{si}},g^{d_{si}}h^{r_{si}})=\prod_{s=1}^{\rho}\prod_{i=1}^{\omega}g_1^{d_{si}^2}\prod_{s=1}^{\rho}\prod_{i=1}^{\omega}h_1^{2d_{si}r_{si}+\alpha qr_{si}^2}=g_1^{\sum_{s=1}^{\rho}\sum_{i=1}^{\omega}d_{si}^2}h_1^{R_4} \tag{6}$$

其中，$R_4=\sum_{s=1}^{\rho}\sum_{i=1}^{\omega}(2d_{si}r_{si}+\alpha q r_{si}^{\ 2}) \bmod p$。类似地，$A_5=\prod_{s=1}^{\rho}e\left(\prod_{i=1}^{\omega}C_{si},\prod_{i=1}^{\omega}C_{si}\right)=g_1^{\sum_{s=1}^{\rho}\left(\sum_{i=1}^{\omega}d_{si}\right)^2}h_1^{R_5}$，其中，$R_5=\prod_{s=1}^{\rho}\left(2\sum_{i=1}^{\omega}d_{si}\sum_{i=1}^{\omega}r_{si}+\alpha q\left(\sum_{i=1}^{\omega}r_{si}\right)^2\right) \bmod p$；$A_6=e\left(\prod_{s=1}^{\rho}\prod_{i=1}^{\omega}C_{si},\prod_{s=1}^{\rho}\prod_{i=1}^{\omega}C_{si}\right)=h_1^{R_6}g_1^{\left(\sum_{s=1}^{\rho}\sum_{i=1}^{\omega}d_{si}\right)^2}$，其中 $R_6=2\sum_{s=1}^{\rho}\sum_{i=1}^{\omega}d_{si}\sum_{s=1}^{\rho}\sum_{i=1}^{\omega}r_{si}+\alpha q\left(\sum_{s=1}^{\rho}\sum_{i=1}^{\omega}r_{si}\right)^2 \bmod p$。

多方秘密共享。聚合器将 A_m（m=1,2,⋯,6）发送给随机挑选的 k+1 个正常工作的雾节点 $\left\{\text{Fog}_j \mid j=1,\cdots,k+1\right\}$。雾节点 Fog_j 收到数据及请求后使用自己的私钥 sk_{Fog_j} 计算得到用于秘密共享的数据 $B_m^j=A_m^{f(j)\left(\prod_{l=1,l\neq j}^{k+1}\frac{l}{l-j}\right)}$，其中 $f(j)=\text{sk}_{\text{Fog}_j}$。

聚合数据签名。每个 Fog_j 使用私钥 sk_{Fog_j} 对聚合密文数据 C^j 签名后得到 $\mathcal{S}_{\text{Fog}_j}=H(C^j\|\text{ts}\|\text{rand}\|\text{id}_{\text{Fog}_j})^{\text{sk}_{\text{Fog}_j}}$，其中 $C^j=B_1^j$ 或 $C^j=B_2^j\|B_3^j$ 或 $C^j=B_4^j\|B_5^j\|B_6^j$，并将 $C^j\|\text{ts}\|\text{rand}\|\text{id}_{\text{Fog}_j}\|\mathcal{S}_{\text{Fog}_j}$ 发送到控制中心进行聚合数据解读。

4.5 聚合数据解读

如图 5 所示，在收到所有雾节点提交的数据后，控制中心首先检查 ts、rand 和 id_{Fog_j} 来初步验证数据的有效性并对其进行签名验证。然后，控制中心对聚合密文数据 $C^j, j=1,\cdots,k+1$ 进行多种类型的解读，最终在不侵害电动汽车充/放电数据隐私的前提下得到所需要的统计值。

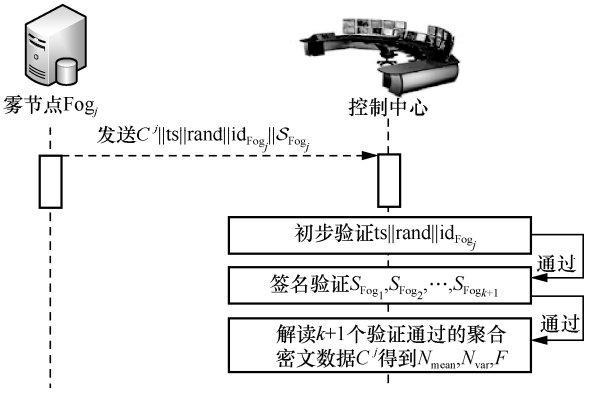

图 5 聚合数据解读过程

批量签名验证。控制中心验证签名 $\mathcal{S}_{\text{Fog}_j}$，$j=1,\cdots,k+1$，$e'(\mathcal{S}_{\text{Fog}_j},g')=e'(\text{H}(C^j\|\text{ts}\|\text{rand}\|\text{id}_{\text{Fog}_j}),\text{pk}_{\text{Fog}_j})$。

均值解读。当 $C^j=B_1^j$ 时，控制中心计算

$$\prod_{j=1}^{k+1}B_1^j=\prod_{j=1}^{k+1}A_1^{f(j)\prod_{l=1,l\neq j}^{k+1}\frac{l}{l-j}}=A_1^{\sum_{j=1}^{k+1}f(j)\prod_{l=1,l\neq j}^{k+1}\frac{l}{l-j}} \tag{7}$$

根据拉格朗日插值公式 $f(x)=\sum_{j=1}^{k+1}f(x_j)\prod_{l=1,l\neq j}^{k+1}\frac{x_l-x}{x_l-x_j}$，不失一般性，取 $x_l=l$、$x_j=j$、$x=0$，可恢复 BGN 私钥 $p=f(0)=\sum_{j=1}^{k+1}f(j)\prod_{l=1,l\neq j}^{k+1}\frac{l}{l-j}$。因此，式 (7) 可进一步等价为 $A_1^{\sum_{j=1}^{k+1}f(j)\prod_{l=1,l\neq j}^{k+1}\frac{l}{l-j}}=A_1^{p}=\left(g^{\sum_{i=1}^{\omega}d_i}h^{R_1}\right)^p=(g^p)^{\sum_{i=1}^{\omega}d_i}(h^p)^{R_1}=\hat{g}^{\sum_{i=1}^{\omega}d_i}$。由 $d_i\leqslant M$ 可知 $\sum_{i=1}^{\omega}d_i\leqslant\omega M$，通过计算以 $\hat{g}$ 为底的 $\hat{g}^{\sum_{i=1}^{\omega}d_i}$ 的离散对数，控制中心可在时间 $O(\sqrt{\omega M})$ 计算得到 $N_{\text{sum}}=\sum_{i=1}^{\omega}d_i$，从而最终计算得到均值 $N_{\text{mean}}=\frac{1}{\omega}N_{\text{sum}}$。

方差解读。类似地，当 $C^j=B_2^j\|B_3^j$ 时，控制中心首先计算 $\prod_{j=1}^{k+1}B_2^j=\hat{g}_1^{\left(\sum_{i=1}^{\omega}d_i\right)^2}$、$\prod_{j=1}^{k+1}B_3^j=\hat{g}_1^{\sum_{i=1}^{\omega}d_i^2}$。然后，分别通过计算以 $\hat{g}_1$ 为底的 $\hat{g}_1^{\left(\sum_{i=1}^{\omega}d_i\right)^2}$ 和 $\hat{g}_1^{\sum_{i=1}^{\omega}d_i^2}$ 的离散对数，控制中心可分别在时间 $O(\omega M)$ 和 $O(\sqrt{\omega}M)$ 计算得到 $N_{\text{sqrsum}}=\left(\sum_{i=1}^{\omega}d_i\right)^2$ 和 $N_{\text{sumsqr}}=\sum_{i=1}^{\omega}d_i^2$。最终可计算 $N_{\text{var}}=\sum_{i=1}^{\omega}(d_i-\overline{d})^2=\sum_{i=1}^{\omega}d_i^{\,2}-\omega\overline{d}^{\,2}=\sum_{i=1}^{\omega}d_i^{\,2}-\frac{1}{\omega}\left(\sum_{i=1}^{\omega}d_i\right)^2=N_{\text{sumsqr}}-\frac{1}{\omega}N_{\text{sqrsum}}$。

单向方差分析解读。当 $C^j=B_4^j\|B_5^j\|B_6^j$ 时，首先，控制中心可计算得到 $\prod_{j=1}^{k+1}B_4^j=\hat{g}_1^{\sum_{s=1}^{\rho}\sum_{i=1}^{\omega}d_{si}^2}$、

$\prod_{j=1}^{k+1} B_5^j = \hat{g}_1^{\sum_{s=1}^{\rho}\left(\sum_{i=1}^{\omega} d_{si}\right)^2}$ 和 $\prod_{j=1}^{k+1} B_6^j = \hat{g}_1^{\left(\sum_{s=1}^{\rho}\sum_{i=1}^{\omega} d_{si}\right)^2}$。然后，通过分别计算以 $\hat{g}_1$ 为底，$\hat{g}_1^{\sum_{s=1}^{\rho}\sum_{i=1}^{\omega} d_{si}^2}$、$\hat{g}_1^{\sum_{s=1}^{\rho}\left(\sum_{i=1}^{\omega} d_{si}\right)^2}$ 和 $\hat{g}_1^{\left(\sum_{s=1}^{\rho}\sum_{i=1}^{\omega} d_{si}\right)^2}$ 的离散对数，控制中心可分别在时间 $O(\sqrt{\rho}\omega M)$、$O(\sqrt{\rho}\omega M)$ 和 $O(\rho\omega M)$ 计算得到 $N_4 = \sum_{s=1}^{\rho}\sum_{i=1}^{\omega} d_{si}^2$、$N_5 = \sum_{s=1}^{\rho}\left(\sum_{i=1}^{\omega} d_{si}\right)^2$ 和 $N_6 = \left(\sum_{s=1}^{\rho}\sum_{i=1}^{\omega} d_{si}\right)^2$。根据定义，可计算 $N_{\mathrm{ssw}} = \sum_{s=1}^{\rho}\sum_{i=1}^{\omega}(d_{si} - \bar{d}_{s\cdot})^2 = \sum_{s=1}^{\rho}\sum_{i=1}^{\omega} d_{si}{}^2 - \frac{1}{\omega}\sum_{s=1}^{\rho}\left(\sum_{i=1}^{\omega} d_{si}\right)^2 = N_4 - \frac{1}{\omega}N_5$。类似地，可计算 $N_{\mathrm{ssb}} = \sum_{s=1}^{\rho}\omega(\bar{d}_{s\cdot} - \bar{d})^2 = \frac{1}{\omega}N_5 - \frac{1}{\rho\omega}N_6$。从而最终控制中心可以得到服从 F 分布的随机变量值 $F = \frac{N_{\mathrm{ssb}}}{\rho - 1}\frac{\omega - \rho}{N_{\mathrm{ssw}}}$，并查表得到组内自由度为 $\omega - \rho$ 和组间自由度为 $\rho - 1$ 的 F 临界 F_{cri}。如果 $F > F_{\mathrm{cri}}$，控制中心拒绝零假设，即至少有一个电价策略对电动汽车充/放电量有显著影响；否则控制中心接受零假设，即在不同的电价策略下电动汽车充/放电量变化不大。

5　安全分析

5.1　身份认证和数据完整性

MFPDA 可以认证雾计算层和控制中心层接收的数据来源。充电桩和雾节点的公钥都通过高可信的领导者节点颁发，且在批量签名验证中，验证方根据 id 对应的公钥来进行签名验证，从而可保证数据由合法的实体生成。

MFPDA 中不管是充电桩提供的报告数据还是雾节点发送的聚合密文数据都通过 BLS 算法签名。考虑到 BLS 的安全性基于计算 Diffie- Hellman 假设，在随机预言机模型中的自适应选择明文攻击下是验证难以伪造的[12]。这样，即使攻击者能篡改消息，签名验证程序也不能通过，从而可以保证数据完整性。此外数据一旦存储到区块链上，区块链的特性可以保证其完整性和难以伪造性。

5.2　数据机密性和隐私保护

充电桩提供的充/放电密文数据 C_i 和聚合器聚合的密文数据 $A_1, A_2, \cdots, A_6$ 都是标准的 BGN 密文形式。因为 BGN 同态密码系统被证明在子群决策假设下是语义安全的[24]，所以电动汽车充/放电数据 d_i 和统计数据 N_{sum}、N_{sumsqr}、N_{sqrsum}、N_4、N_5、N_6 的机密性可以得到保证。因此，即使外部攻击者能攻破用户层和雾计算层之间、雾节点之间、雾计算层与控制中心层之间的通信，它们也不能从密文数据中获取关于用户的私密信息。

此外，某个雾节点只拥有 BGN 私钥 p 的秘密碎片 $(j, f(j) = \mathrm{sk}_{\mathrm{Fog}_j})$，在恶意雾节点不超过 k 个的情况下，它们无法通过共谋攻击获取 p。控制中心也无法直接获得每个雾节点的私钥 $f(j) = \mathrm{sk}_{\mathrm{Fog}_j}$ 或者通过其他方式来恢复 BGN 系统私钥 p。因此，即使雾节点和控制中心受到内部攻击，单个电动汽车用户数据的机密性和隐私性都可以得到保证。

5.3　安全功能分析

如表 2 所示，将 MFPDA 与近年来提出的几个基于同态加密的具有类似安全功能的数据聚合方案进行对比。表 2 中，√表示方案具有此功能特性；×表示方案不具备此功能特性。从表 2 可以看出，只有 MFPDA 同时支持数据机密性、数据完整性和认证、容错、抵抗内部攻击、批量签名验证、不需要可信第三方和多种聚合函数。

支持容错方面，文献[27]、文献[13]、文献[28]、文献[8]和文献[7]方案均采用单个聚合服务器，因此它们不支持容错。相比之下，文献[18]方案支持容错，即使部分智能电表发送数据失败也不影响最终聚合结果。MFPDA 由 σ 个雾节点充当区块链节点搭建了一个区块链网络，由高可靠性的领导节点充当聚合器，以分布式、协同的方式给控制中心提供数据聚合服务，因此也支持容错，具体分析如下。

抵抗内部攻击方面，文献[27]方案通过在用户和控制中心注入盲因子（秘密因子）来抵抗内部攻击者泄露用户隐私，但也会因为部分数据丢失导致这些盲因子不能在最终的聚合结果中相互抵消，导致方案不支持容错性。文献[8]方案中，即使单个用户密文数据的解密密钥泄露给内部攻击者，其也无法恢复明文。MFPDA 中控制中心不拥有密文数据的解密密钥，某个雾节点也只拥有解密密钥的秘密碎片，通过秘密共享的方式将解密密钥分享给控制中心来解密聚合密文，避免内部攻击者攻击雾节点

表 2 类似方案的安全功能比较

方案	功能特性						
	数据机密性	数据完整性和认证	容错	抵抗内部攻击	批量签名验证	不需要可信第三方	多种聚合函数
文献[27]	√	√	×	√	√	×	×
文献[13]	√	√	×	×	√	√	×
文献[28]	√	√	×	×	√	×	×
文献[8]	√	√	×	√	×	×	√
文献[7]	√	×	×	×	×	×	√
文献[18]	√	√	√	×	√	×	×
MFPDA	√	√	√	√	√	√	√

或者控制中心获取解密密钥而泄露单个电动汽车用户的隐私。

批量签名验证方面，文献[13,18,27-28]方案和 MFPDA 均利用双线性对的性质来支持批量签名验证。

不需要可信第三方方面，文献[13]方案不需要可信第三方，而是依赖奖惩机制保证聚合结果的可信。MFPDA 则依赖区块链而不是可信第三方，借助动态选出的高可靠性领导者节点保证聚合结果可信。

支持多种聚合函数方面，文献[7-8]方案都支持除了求和之外的均值、方差等的多种隐私保护聚合函数。考虑到数据聚合计算是数据聚合方案的核心功能，也是主要计算开销来源，因此以下计算开销分析中主要与这几个使用同态加密算法来支持多种聚合函数的方案进行比较，以体现本文方案在性能上的优势。

此外，容忍部分雾节点异常。事实上，攻击者想攻破一个雾节点是困难的。因此可以假设攻击者只能攻破不超过 $k=\left\lceil\frac{\sigma}{2}\right\rceil-1$ 个雾节点并获取它们的私钥。一方面，攻击者不能获取 BGN 私钥 p 来解密充/放电密文数据，因为根据 Shamir 秘密共享的“all or nothing”特性，至少需要 $k+1$ 个雾节点合作才能恢复密钥 p。另一方面，这时仍然有 $\sigma-k\geqslant k+1$ 个雾节点正常工作，可以聚合密文数据和协助控制中心解读聚合数据，从而保障系统的正常运行。

容忍部分用户层数据上报异常。以均值聚合为例，如果部分电动汽车或充电桩故障，导致部分充电桩 $\widehat{\mathrm{CP}}\subset\mathbb{P}$ 不能正常上报数据，聚合器节点仍然生成聚合密文数据 $\widehat{A_1}=\prod_{\mathrm{CP}_i\in\left(\mathbb{P}-\widehat{\mathrm{CP}}\right)}C_i=\prod_{\mathrm{CP}_i\in\left(\mathbb{P}-\widehat{\mathrm{CP}}\right)}(g^{d_i}h^{r_i})=g^{\sum_{\mathrm{CP}_i\in\left(\mathbb{P}-\widehat{\mathrm{CP}}\right)}d_i}h^{R_1}$，其中 $R_1=\sum_{\mathrm{CP}_i\in\left(\mathbb{P}-\widehat{\mathrm{CP}}\right)}r_i \bmod p$。如前所述，控制中心通过挑选的 $k+1$ 个验证通过的聚合密文数据仍然可以求得聚合数据 $\sum_{\mathrm{CP}_i\in\left(\mathbb{P}-\widehat{\mathrm{CP}}\right)}d_i$。同理，即使只有 $\mathbb{P}-\widehat{\mathrm{CP}}$ 个充电桩能正常上报数据，方差和单向方差分析聚合也可以成功进行。

6 性能评估

本节评估 MFPDA 的性能，分别从计算、通信和存储开销几个方面进行讨论。部分系统设置如下。区块链部分采用 Hyperledger Fabric v2.3.1[29]来实施；充电桩节点、雾节点和控制中心分别在运行 CentOS 7.4 的 2.20 GHz 4vCPU 8 GB 内存虚拟机上部署；fabric-sdk-java 和 fabric-chaincode-java 分别用于开发 Fabric 客户端和智能合约（Fabric 中称为 chaincode）。此外使用 JPBC（Java pairing-based cryptography）库来实施 BGN、ECDSA 和 BLS 算法，并设定它们的安全参数大小都为 256 bit，即 $|p|=|q|=|p'|=|q'|=256$。所有的密码学运算时间是 10 000 次重复实验的平均值。

6.1 计算开销分析

本节以均值聚合为例，考虑控制中心的计算开销，将 MFPDA 与文献[7]的 MuDA 方案和文献[8]的 KLR-EDA 方案进行对比。由于 MuDA 没有考虑认证和数据完整性功能，因此以下计算开销分析不涉及签名和验签。令 $T_{\exp}$ 表示群 $\mathbb{G}$ 中的模指数运算时间，T_{mul} 表示群 $\mathbb{G}$ 中的模乘法运算时间，

T_{pl}表示使用 Pollard 的λ方法计算群$\mathbb{G}$中的离散对数的时间。其他密码学运算用时极少，可忽略不计。

在 MFPDA 的聚合数据解读过程，控制中心选择$k+1$个验证通过的数据进行均值解读，需要k个$\mathbb{G}$中的模乘法运算和计算一次$\mathbb{G}$中的离散对数，计算开销为$kT_{\mathrm{mul}}+T_{\mathrm{pl}}$。在 MuDA 的安全报告读取过程中，控制中心需要计算$g_{\gamma}{}^{p}$、$(A_{1,r})^{p}$以及一次$\mathbb{G}$中的离散对数，计算开销为$2T_{\mathrm{exp}}+T_{\mathrm{pl}}$。在 KLR-EDA 的验证和解密过程，控制中心需要计算 3 次$\mathbb{G}$中的离散对数，计算开销为$3T_{\mathrm{pl}}$。

假设每个雾节点能给 2 500 个 EV 提供服务，即$k=\left\lceil \dfrac{\omega}{2500\times 2} \right\rceil$。系统每 15min 采集一次充/放电数据$d_i \leqslant 100$ kWh （即 M=100）。实验测试得到$T_{\mathrm{exp}}=32\,879.0\,\mu\mathrm{s}$、$T_{\mathrm{mul}}=57.2\,\mu\mathrm{s}$。$T_{\mathrm{pl}}$ 随 ω 变化的实验结果（M=100）如表 3 所示。从表 3 可以看出，T_{pl}与$\sqrt{\omega M}$成比例，这与本文在聚合数据解读过程中分析的控制中心可在时间$O(\sqrt{\omega M})$计算得到N_{sum}的结论相符。

表 3　T_{pl} 随 ω 变化的实验结果（M=100）

ω	k	T_{pl}/μs	$\dfrac{T_{\mathrm{pl}}}{\sqrt{\omega M}}$/μs
10 000	2	37 360.0	37.36
20 000	4	52 976.4	37.46
30 000	6	64 640.1	37.32
40 000	8	74 660.0	37.33
50 000	10	83 405.3	37.3
60 000	12	91 635.4	37.41
70 000	14	98 474.9	37.22
80 000	16	105 952.9	37.46
90 000	18	111 930.0	37.31
100 000	20	118 205.9	37.38

图 6 显示了 MFPDA 和 MuDA 方案中的控制中心计算开销对比，从图 6 可以看出，MFPDA 中控制中心的计算开销远小于 MuDA 和 KLR-EDA，当电动汽车数量为 10^4 台时，减少率可达 66.6%。从而可以得出结论，在雾节点的帮助下 MFPDA 可以显著减少控制中心的计算开销。

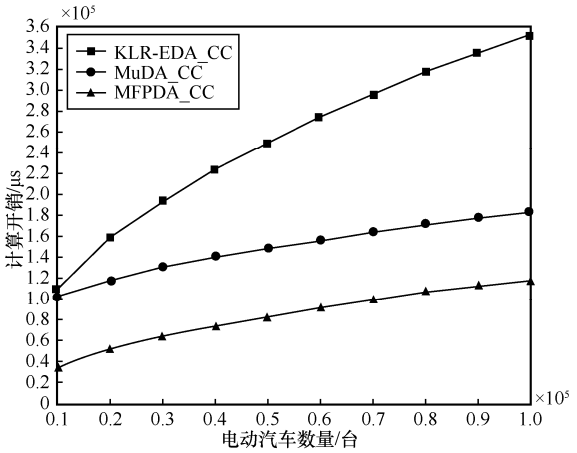

图 6　MFPDA 和 MuDA 方案中的控制中心计算开销对比

6.2　通信开销分析

本节分析 MFPDA 的通信开销，以均值聚合为例。原始方案交易中的关键参数如表 4 所示。原始方案和改进方案采用分别采用 ECDSA 和 BLS 作为其签名算法，其交易大小分别为$L_{\mathrm{T}}=(L_{\mathrm{ecd}}+108\,\mathrm{B}+\phi L_{\mathrm{A}})$和$L'_{\mathrm{T}}=(L_{\mathrm{blg}}+108\,\mathrm{B}+\phi L_{\mathrm{A}})$。$L_{\mathrm{ecd}}=64\,\mathrm{B}$ 和 $L_{\mathrm{blg}}=32\,\mathrm{B}$ 分别表示 ECDSA 和 BLS 签名大小。ϕ为一个交易包含的动作个数，L_{A}为一个动作的大小。动作中的关键参数如表 5 所示。方案中的动作大小均为$L_{\mathrm{A}}=80\,\mathrm{B}+4\psi\,\mathrm{B}$，其中$\psi$为交易读写集对应的键值对的个数。MFPDA 的交易中只包含一个充/放电数据，可设$\phi=\psi=1$。

表 4　原始方案交易中的关键参数

参数	签名	交易数据头		动作数组
		通道数据头	签名数据头	
长度/B	L_{ecd}	72	36	ϕL_{A}

表 5　动作中的关键参数

参数	数据头	链码提案载荷	动作	
			背书 ID	提案响应载荷
长度/B	36	36	8	4ψ

综上可得，原始方案和改进方案中交易大小分别为$L_{\mathrm{T}}=256$ B 和$L'_{\mathrm{T}}=224$ B。BGN 密文大小为$L_{\mathrm{bgn}}=64\,\mathrm{B}$，其他通信负载如 ID、随机数和时间戳可忽略不计。1) 数据报告生成过程。每个充电桩需要传输一个密文C_i和一个签名$\mathcal{S}_i$给雾节点。原始方案和改进方案中充电桩总通信开销分别为$\omega(L_{\mathrm{bgn}}+L_{\mathrm{ecd}})$和$\omega(L_{\mathrm{bgn}}+L_{\mathrm{blg}})$。2) 区块生成过程。从节点总共需要向

领导者节点传输 ω 个交易，因此原始方案和改进方案中从节点总通信开销分别为 ωL_T 和 $\omega L_T'$。3) 隐私数据聚合过程。聚合器节点将 A_{I} 发给 $k+1$ 个雾节点，其中 A_{I} 为 BGN 密文形式。因此原始方案和改进方案中聚合器节点通信开销都为 $(k+1)L_{\mathrm{bgn}}$。4) 聚合数据解读过程。$k+1$ 个雾节点中每个都需要传输一个密文 $C^j=B_{\mathrm{I}}^j$ 和一个签名 $\mathcal{S}_{\mathrm{Fog}_j}$ 给控制中心。因此原始方案和改进方案中控制中心总通信开销为分别为 $(k+1)(L_{\mathrm{bgn}}+L_{\mathrm{ecd}})$ 和 $(k+1)(L_{\mathrm{bgn}}+L_{\mathrm{blg}})$。综上，原始方案和改进方案的系统总通信开销分别为 $(\omega+2k+2)L_{\mathrm{bgn}}+(\omega+k+1)\ L_{\mathrm{ecd}}+\omega L_{\mathrm{T}}$ 和 $(\omega+2k+2)L_{\mathrm{bgn}}+(\omega+k+1)L_{\mathrm{blg}}+\omega L_T'$。图 7 描述了原始方案和改进方案的充电桩和系统的通信开销对比。从图 7 可知，改进方案在充电桩通信开销和系统总通信开销上都有明显降低，分别能减少 25.0%和 16.7%。因为所有充电桩定期上报数据，大量数据同时上报会对雾节点的造成较大的通信压力。本文的改进方案可以大大降低系统的通信负载，这对系统的实时性至关重要，特别是当 ω 很大时。

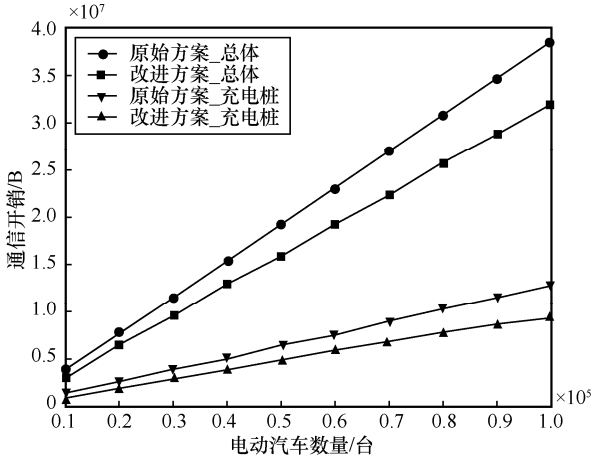

图 7 原始方案和改进方案的充电桩和系统的通信开销对比

6.3 存储开销分析

假设所有充电桩上报的 ω 个交易都通过验证并被打包成一个区块。原始方案中区块的关键参数如表 6 所示。正如前文所述，原始方案交易中的签名采用 ECDSA 作为签名算法，而改进方案将签名算法改成了 BLS 短签名算法。一方面，利用 BLS 的签名聚合功能，交易中可以删除签名字段，只在区块中存储一个所有交易的签名聚合。本文可以只关心区块中所有的签名是否正确。因为区块一旦添加到区块链，其难以篡改的特性可以保障区块中的所有交易都是合法的。另一方面，在相同的安全级别下，BLS 的数字签名大小只有 ECDSA 的一半，可以减少区块的存储开销。综上，原始方案和改进方案区块大小分别为 $116\,\mathrm{B}+\omega L_{\mathrm{T}}$ 和 $116\,\mathrm{B}+\omega(L_{\mathrm{T}}'-L_{\mathrm{blg}})+L_{\mathrm{blg}}$。图 8 描述了原始方案和改进方案的区块存储开销对比。从图 8 可以看出，改进方案具有更小的区块存储开销，且 EV 的数量越多其优势更明显，当 ω=10^5 时，可以减少高达 24.9%的区块存储开销。

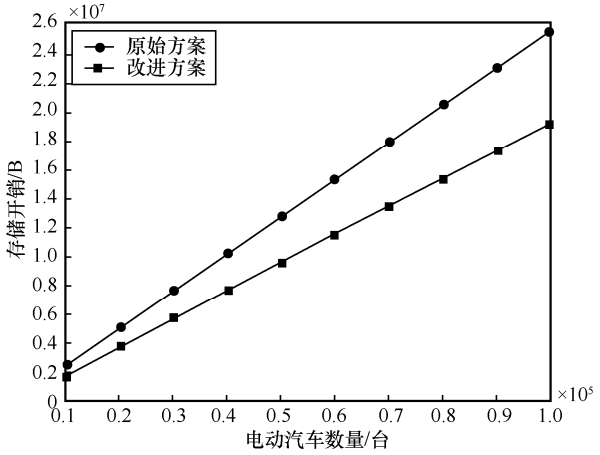

图 8 原始方案和改进方案的区块存储开销对比

7 结束语

本文方案结合密码学和区块链等技术，从隐私保护数据聚合方案的多功能、安全和高效等方面开展研究。具体来说，首先，通过结合雾计算和联盟链构建了一个可有效利用本地资源的、安全增强的三层架构。其次，基于 BGN 同态密码系统设计了支持多种统计值计算的隐私保护数据聚合函数；结合 BLS 算法确保电动汽车充放电数据的机密性、完整性和批量签名验证；采用 Shamir 秘密共享算法来

表 6 原始方案中区块的关键参数

参数	区块数据头			交易数组	元数据
	序号	前一个区块的哈希值	本区块数据哈希值		
长度/B	4	32	32	ωL_{T}	48

支持部分雾节点和用户端异常情况下的容错以及抵抗内部攻击；基于联盟链的去信任化剔除对可信第三方的依赖。此外，本文改进了联盟链的签名算法并优化了区块和交易的存储结构以轻量化数据聚合。最后，通过安全分析验证了 MFPDA 多方面的安全特性；性能对比分析验证了 MFPDA 的优势和有效性。未来工作可以考虑设计更加多样化的隐私保护聚合函数，如设计可进行密文比较的聚合函数，用于求最大值、最小值、中位数和众数。

参考文献：

[1] NIMALSIRI N I, MEDIWATHTHE C P, RATNAM E L, et al. A survey of algorithms for distributed charging control of electric vehicles in smart grid[J]. IEEE Transactions on Intelligent Transportation Systems, 2020, 21(11): 4497-4515.

[2] HAN W L, XIAO Y. IP^{2}DM: integrated privacy-preserving data management architecture for smart grid V2G networks[J]. Wireless Communications and Mobile Computing, 2016, 16(17): 2956-2974.

[3] 赵小敏, 梁学利, 蒋双双, 等. 安全的WSN数据融合隐私保护方案设计[J]. 通信学报, 2014, 35(11): 154-161.
ZHAO X M, LIANG X L, JIANG S S, et al. Design of secure privacy-preserving data aggregation scheme for wireless sensor network[J]. Journal on Communications, 2014, 35(11): 154-161.

[4] HAN W, XIAO Y. Privacy preservation for V2G networks in smart grid: a survey[J]. Computer Communications, 2016, 91/92: 17-28.

[5] 张晓莹, 彭辉, 陈红. 无线传感器网络隐私保护数据聚集技术[J]. 通信学报, 2018, 39(10): 130-142.
ZHANG X Y, PENG H, CHEN H. State-of-the-art survey of privacy-preserving data aggregation in wireless sensor networks[J]. Journal on Communications, 2018, 39(10): 130-142.

[6] LU W F, REN Z H, XU J, et al. Edge blockchain assisted lightweight privacy-preserving data aggregation for smart grid[J]. IEEE Transactions on Network and Service Management, 2021, 18(2): 1246-1259.

[7] CHEN L, LU R X, CAO Z F, et al. MuDA: multifunctional data aggregation in privacy-preserving smart grid communications[J]. Peer-to-Peer Networking and Applications, 2015, 8(5): 777-792.

[8] ZHANG X J, HUANG C, XU C X, et al. Key-leakage resilient encrypted data aggregation with lightweight verification in fog-assisted smart grids[J]. IEEE Internet of Things Journal, 2021, 8(10): 8234-8245.

[9] ZHANG Z Z, CAO T F, WANG X Y, et al. VC-PPQ: privacy-preserving Q-learning based video caching optimization in mobile edge networks[J]. IEEE Transactions on Network Science and Engineering, 2022, 9(6): 4129-4144.

[10] WANG J, WU L B, ZEADALLY S, et al. Privacy-preserving data aggregation against malicious data mining attack for IoT-enabled smart grid[J]. ACM Transactions on Sensor Networks, 2021, 17(3): 1-25.

[11] JOHNSON D, MENEZES A, VANSTONE S. The elliptic curve digital signature algorithm (ECDSA)[J]. International Journal of Information Security, 2001, 1(1): 36-63.

[12] BONEH D, LYNN B, SHACHAM H. Short signatures from the Weil pairing[C]//Advances in Cryptology - ASIACRYPT 2001. Berlin: Springer, 2001: 514-532.

[13] LIU Y N, GUO W, FAN C N, et al. A practical privacy-preserving data aggregation (3PDA) scheme for smart grid[J]. IEEE Transactions on Industrial Informatics, 2018, 15(3): 1767-1774.

[14] DING Y, WANG B Y, WANG Y J, et al. Secure metering data aggregation with batch verification in industrial smart grid[J]. IEEE Transactions on Industrial Informatics, 2020, 16(10): 6607-6616.

[15] GUO C, JIANG X, CHOO K K R, et al. Lightweight privacy preserving data aggregation with batch verification for smart grid[J]. Future Generation Computer Systems, 2020, 112: 512-523.

[16] PENT G M, DHAINI A R, HO P H. Toward integrated cloud-fog networks for efficient IoT provisioning: key challenges and solutions[J]. Future Generation Computer Systems, 2018, 88: 606-613.

[17] LI X, LIU S P, WU F, et al. Privacy preserving data aggregation scheme for mobile edge computing assisted IoT applications[J]. IEEE Internet of Things Journal, 2019, 6(3): 4755-4763.

[18] MERAD B O R, SENOUCI S M. An efficient and secure multidimensional data aggregation for fog-computing-based smart grid[J]. IEEE Internet of Things Journal, 2021, 8(8): 6143-6153.

[19] CHEN S, YANG L, ZHAO C, et al. Double-blockchain assisted secure and anonymous data aggregation for fog-enabled smart grid[J]. Engineering, 2022, 8: 159-169.

[20] NAKAMOTO S. BITCOIN: a peer-to-peer electronic cash system[R]. 2008.

[21] WANG Y X, LUO F J, DONG Z Y, et al. Distributed meter data aggregation framework based on Blockchain and homomorphic encryption[J]. IET Cyber-Physical Systems: Theory & Applications, 2019, 4(1): 30-37.

[22] FAN H B, LIU Y N, ZENG Z X. Decentralized privacy-preserving data aggregation scheme for smart grid based on blockchain[J]. Sensors, 2020, 20(18): 5282.

[23] WANG X D, GARG S, LIN H, et al. A secure data aggregation strategy in edge computing and blockchain-empowered Internet of things[J]. IEEE Internet of Things Journal, 2022, 9(16): 14237-14246.

[24] BONEH D, GOH E J, NISSIM K. Evaluating 2-DNF Formulas on Ciphertexts[C]//Theory of Cryptography Conference. Berlin: Springer, 2005: 325-341.

[25] MENEZES A J, OORSCHOT P C V, VANSTONE S A. Handbook of applied cryptography[M]. Boca Raton: CRC Press, 2018.

[26] SHAMIR A. How to share a secret[J]. Communications of the ACM, 1979, 22(11): 612-613.

[27] VAHEDI E, BAYAT M, PAKRAVAN M R, et al. A secure ECC-based privacy preserving data aggregation scheme for smart grids[J]. Computer Networks, 2017, 129: 28-36.

[28] SHEN H, ZHANG M W, SHEN J. Efficient privacy-preserving cube-data aggregation scheme for smart grids[J]. IEEE Transactions on Information Forensics and Security, 2017, 12(6): 1369-1381.

[29] ANDROULAKI E, BARGER A, BORTNIKOV V, et al. Hyperledger Fabric: a distributed operating system for permissioned blockchains[C]// Proceedings of the Thirteenth EuroSystem Conference. New York: ACM Press, 2018: 1-15.

[作者简介]

胡柏吉（1992− ），男，湖南衡阳人，华北电力大学博士生，主要研究方向为区块链、密码学、隐私保护等。

张晓娟（1988− ），女，河北张家口人，博士，中国电力科学研究院有限公司高级工程师，主要研究方向为密码学、数据安全、电力系统信息安全等。

李元诚（1970− ），男，山东烟台人，博士，华北电力大学教授、博士生导师，主要研究方向为密码学、信息安全等。

赖荣鑫（1996− ），男，海南澄迈人，华北电力大学硕士生，主要研究方向为区块链、密码学、信息安全等。