基于区块链且可验证的智能电网多维数据聚合与分享方案

陈建伟[1,2]，王姝妤[1,2]，张美平[1,2]，张桢萍[1,2]
（1. 福建师范大学计算机与网络空间安全学院，福建 福州 350117；2. 福建省网络安全与密码技术重点实验室，福建 福州 350117）

摘 要：针对如何支持轻量级多维数据聚合，实现系统整体过程中多维数据的双端完整性验证，以及处理云服务器集中化等问题，提出了一种基于区块链且可验证的智能电网多维数据聚合与分享方案。首先，为了满足智能电网对电量数据细粒度分析的需求，利用掩蔽值和霍纳法则实现了隐私保护多维数据聚合。在此基础上，针对现有数据聚合方案在云存储数据与第三方分享方面存在的数据完整性验证问题，借用基于 RSA 的乘法同态承诺方案和同态哈希函数的同态性设计了一种新的签名算法，使云服务器不仅可以验证聚合数据的完整性，还可以验证数据分享阶段的完整性，即实现了云存储数据的双端可验证性，并且可以抵抗内部攻击。同时，提出了一种基于联盟链多链的聚合数据分享体系结构，有效地避免单机处理瓶颈和易受攻击等集中化问题。理论分析证明了所提方案的安全性。性能实验表明，所提方案比已有方案具有更低的计算和通信成本。

关键词：智能电网；可验证；云存储；数据完整性；区块链
中图分类号：TP393.1
文献标志码：A
DOI: 10.11959/j.issn.1000−436x.2024010

Blockchain-based and verifiable multidimensional data aggregation and sharing scheme for smart grid

CHEN Jianwei[1,2], WANG Shuyu[1,2], ZHANG Meiping[1,2], ZHANG Zhenping[1,2]
1. College of Computer and Cyber Security, Fujian Normal University, Fuzhou 350117, China
2. Fujian Provincial Key Laboratory of Network Security and Cryptology, Fuzhou 350117, China

Abstract: Aiming at the problem that how to support lightweight multi-dimensional data aggregation, achieve double-end integrity verification of multi-dimensional data in the overall process of the system, and deal with the centralization of cloud servers, a blockchain-based and verifiable multidimensional data aggregation and sharing scheme for smart grid was proposed. Firstly, in order to meet the demand for fine-grained analysis of power data in smart grid, privacy-preserving multidimensional data aggregation was achieved by using masked values and Horner's rule. On this basis, for the data integrity verification problem of the existing data aggregation scheme in the sharing of cloud storage data with the third party, a new signature algorithm was designed by borrowing the RSA-based multiplicative homomorphic commitment scheme and homomorphic hash function homomorphism, which enabled the cloud server to verify the integrity of aggregated data and be used for integrity verification in the data sharing phase, i.e., it achieved double-end verifiability of cloud storage data and was resistant to internal attacks. Meanwhile, an aggregated data sharing architecture based on federated chain multichain was proposed to effectively avoid centralisation problems such as single-machine processing bottleneck and vulnerability to attacks. The theoretical analysis proves the security of the scheme. Performance experiments show that the proposed scheme has lower computation and communication costs compared with existing schemes.

Keywords: smart grid, verifiable, cloud storage, data integrity, blockchain

---

收稿日期：2023−09−07；**修回日期：**2023−11−22
通信作者：王姝妤，sy_isbest@163.com
基金项目：中央引导地方科技发展资金资助项目（No.2021L3032）；福建省自然科学基金资助项目（No.2023J01296）；国家自然科学基金资助项目（No.U1905211）；福建省科技厅高校产学合作计划基金资助项目（No.2022H6025）
Foundation Items: The Central Guidance on Local Science and Technology Development Fund (No.2021L3032), The Natural Science Foundation of Fujian Province (No.2023J01296), The National Natural Science Foundation of China (No.U1905211), The University-Industry Cooperation Project of Fujian Provincial Department of Scence and Technology (No.2022H6025)

0 引言

电力系统是当今社会不可或缺的公共服务系统，社会经济的高速发展使传统电网已无法满足人们的需求，智能电网已引起世界各国的广泛关注和研究[1]。我国自 2011 年以来就将智能电网作为重大发展战略之一，至 2020 年已对智能化电网投资 3 841 亿元[2]，并预计在“十四五”期间投资约 3 750 亿元。2021 年，《中华人民共和国国民经济和社会发展第十四个五年规划和 2035 年远景目标纲要》提出，加快电网基础设施智能化改造和智能微电网建设，提高电力系统互补互济和智能调节能力。在智能电网实际应用中，住户配有的智能电表会周期性地收集电量数据，并提交到远程云服务器（CS, cloud server）。CS 对这些数据进行计算、分析和存储，并向第三方请求者提供数据分享服务[3-4]。为了防止用户的实时电量数据被窃取而泄露个人隐私，近年来研究者常用数据聚合技术来收集统计电量数据，然而，设计一个隐私保护的数据聚合与共享方案仍然面临一些亟待解决的问题。

大部分传统的数据聚合方案[5-7]研究的是单一类型的电量数据聚合。文献[8]提出一种多维的电量数据聚合方案，该方案不仅可以收集用户的总体电量数据，还可以根据不同时间和目的，提供多种类型的聚合电量数据，以满足实际应用的需求。文献[9]给出了一个采用 Paillier 同态加密算法的多维数据聚合方案，电力公司不仅能够收集所有智能电表的总体聚合数据，还能够收集指定区域的特定聚合数据，然而，基于公钥的同态加密算法大都需要较高的计算开销。为了提高计算和通信效率，文献[10]提出了一种基于椭圆曲线密码体制（ECC）的智能电网安全多维数据聚合方案，该方案不需要双线性配对和映射到点哈希操作，因此，其具有较低的计算和通信成本，适合实际应用。上述方案为了节约本地存储开销，大都将聚合数据存储在云端，然而，云端存储的数据是公开可见的，这就带来了一些数据存储安全方面的问题。为了防止云存储数据的泄露，文献[11]采用基于身份的代理加密设计了重加密策略，并结合区块链技术在数据聚合方案中实现了更加安全和低成本的访问控制。文献[12]提出了一种基于代理重加密的数据查询和共享方案，该方案不仅支持用户查询历史数据和账单，还实现了与第三方的安全数据共享。然而，这些方案能够正确执行的前提条件是存储聚合数据的 CS 是完全可信的。但在实际应用中，CS 并不是完全可信的，它为了自身利益可能隐瞒数据不完整的情况[13]，分享给第三方的存储数据可能是无效的，然而第三方无法验证该存储数据的完整性。由此，数据聚合与共享系统需要从整体上设计一种数据完整性验证方法。

为了确保云存储数据的完整性，文献[14]提出了一种基于密文策略属性基加密（CP-ABE）的轻量级可验证外包解密方案，该方案通过提供密文的可验证性来确保用户可以检查数据的完整性，但其仅支持私人验证，即只允许用户自己检查外包数据的完整性，这需要用户端承担较大的计算开销。文献[15]提出了一种新的公共验证方案，该方案采用代数签名和椭圆曲线密码学技术设计了一种完整性验证方法，可以在低计算和通信成本的情况下，有效地验证数据完整性。文献[16]提出了一种多个云数据中心的数据完整性验证协议，可以通过一次验证所有副本来提高效率。由于数据在公共网络环境中传输，极易遭受攻击，但是在上述方案[14-16]中，CS 端并没有对接收数据进行完整性验证。也就是说，既要实现用户端可验证云存储数据的完整性，又要确保 CS 端对接收数据进行完整性验证，才能进一步保证数据的完整性。为此，文献[17]提出了第一个针对雾到云的物联网安全数据存储的公共审计方案，该方案设计了一种基于双线性映射技术的标签传输策略来保护身份隐私，实现了双端可验证的安全审计，但是该方案仅支持一对一验证，并且需要大量双线性配对运算，因此计算和通信成本较高。

另一方面，当所有数据都集中在 CS 端时，会不可避免地产生单机处理瓶颈和易受攻击等集中化问题。区块链技术的出现为解决这类问题提供了新的解决方案，因为其具有去中心化和防篡改的特性，可以保证在智能电网中高效、安全地传输和分享数据。因此，文献[18]基于区块链提出了一种双端可验证的方案，该方案使用区块链技术实现了可验证和支持访问的去中心化系统，但是该方案用户端验证数据时只支持一对一验证，需要用户端承担较大的计算开销。

为了解决上述问题，本文基于区块链设计了一种高效可验证的智能电网数据聚合与分享方案。

本文的主要贡献如下。

1) 针对多维数据聚合，本文设计了一种基于RSA（Rivest, Shamir, Adleman）的乘法同态承诺方案和同态哈希函数的轻量级签名算法，有效降低了完整性验证的计算和通信开销，非常适用于计算资源受限的终端设备环境。

2) 现有方案多数只支持一端数据完整性验证，对此，本文从系统整体的角度实现了双端数据完整性验证，并能够有效抵抗各种内部或外部的攻击。

3) 针对单机处理瓶颈和易受攻击等集中化问题，本文提出了一种基于联盟链多链的多维数据分享体系结构，有效地利用了区块链的去中心化和防篡改的特性。

1　预备知识

1.1　基于 RSA 的乘法同态承诺方案

本文采用了一种基于 RSA 的乘法同态承诺方案[19]。随机选择 2 个独立的大素数 p 和 q，然后计算 $N=pq$，N 是 RSA 的一个公共模数。随机选择一个公共素数 e，满足 $e>N^2$ 和 $\gcd(e,\varphi(N^2))=1$。设 g_m 为群 $Z_{N^2}^*$ 中阶最大的公共元素，并且绑定了一个秘密 $m\in Z_{N^2}^*$。发送者随机生成一个密钥 $r\in Z_{N^2}^*$，然后计算承诺 c 如下

$$c=C(m,r)=m^e g^r \bmod N^2 \tag{1}$$

该承诺的一个显著特性就是具有乘法同态性。给定 2 个承诺 $c_1=C(m_1,r_1)$ 和 $c_2=C(m_2,r_2)$，其中，$r_1,r_2\in Z_{N^2}^*$。2 个承诺的乘积等于 m_1m_2 承诺，即

$$C(m_1,r_1)(m_2,r_2)\bmod N^2=C(m_1m_2,r_1+r_2) \tag{2}$$

扩展到 V 个消息为

$$\prod_{i=1}^{V}C(m_i,r_i)=C\left(\prod_{i=1}^{V}m_i,\sum_{i=1}^{V}r_i\right)\bmod N^2 \tag{3}$$

1.2　同态哈希函数

同态哈希函数满足以下 2 个性质[20]。

1) 同态性。对任意 2 个数据 m_1、m_2 和实数 w_1、w_2，都有 $H(w_1m_1+w_2m_2)=H(m_1)^{w_1}H(m_2)^{w_2}$。

2) 免碰撞性。攻击者不存在概率多项式算法能伪造出（m_1，m_2，m_3，w_1，w_2），并满足 $m_3\neq w_1m_1+w_2m_2$，使 $H(m_3)=H(m_1)^{w_1}H(m_2)^{w_2}$。

1.3　多链交互

以太坊的创始人 Buterin 总结了三类跨链技术[21]，即公证人机制、侧链/中继、哈希锁定。中继技术通过中继链来实现各单链的交互，可很好地实现多链的跨链互联。本文多链架构中处于不同通道内的用户不能直接进行数据的访问，多链交互采用中继机制，有跨链需求的数据链可向中继链申请加入多链系统，中继链保存各数据链的信息以及与数据链的联络节点。

2　模型和设计目标

2.1　系统模型

本文系统模型如图 1 所示，主要包含 5 种实体对象：智能电表（SM）、云服务器（CS）、数据请求者（DR）、联盟链多链（MCBC）和可信权威中心（TA）。具体过程如下。

首先，TA 生成所有的公共参数和密钥，并分发给其他相应的实体对象。在终端，每个用户都配备一个 SM，SM 定期收集用户的电量数据，并将加密数据和签名分别发送给 CS（图 1 步骤 1）和挖矿节点。在每个周期，以签名最接近平均值为标准选取一个 SM 作为挖矿节点，由其负责聚合各维度数据和总体数据的签名，并将总体聚合签名发送给 CS。在云端，CS 执行签名验证和聚合解密操作，并将验证结果反馈给挖矿节点（图 1 步骤 2），同时存储解密后的聚合数据。当挖矿节点收到 CS 的正确验证结果后，将每一维电量数据的聚合签名记录到签名链中（该链为用户私有链，图 1 步骤 3）。

当 DR（可以是大功率电器销售人员、电力公司等有数据需求的请求者）需要访问 CS 存储数据时，DR 通过监管链节点（监管链节点由社会权威部门、政府能源部门等节点组成，图 1 步骤 4）向 CS 发送请求消息（图 1 步骤 5）。CS 根据请求内容执行数据聚合计算，然后将聚合数据、验证证明以及解密密钥记录到分享链中（该链为 CS 私有链，步骤 6）。监管链节点分别调用链码申请访问分享链和签名链的数据（图 1 步骤 7.1 和步骤 8.1），分享链和签名链分别返回给监管链节点所请求的数据（图 1 步骤 7.2 和步骤 8.2），监管链根据获得的数据和 DR 的请求内容来验证数据的完整性，验证通过后将正确数据返回给 DR（图 1 步骤 9）。DR 获得请求的数据后向 CS 支付费用完成交易。

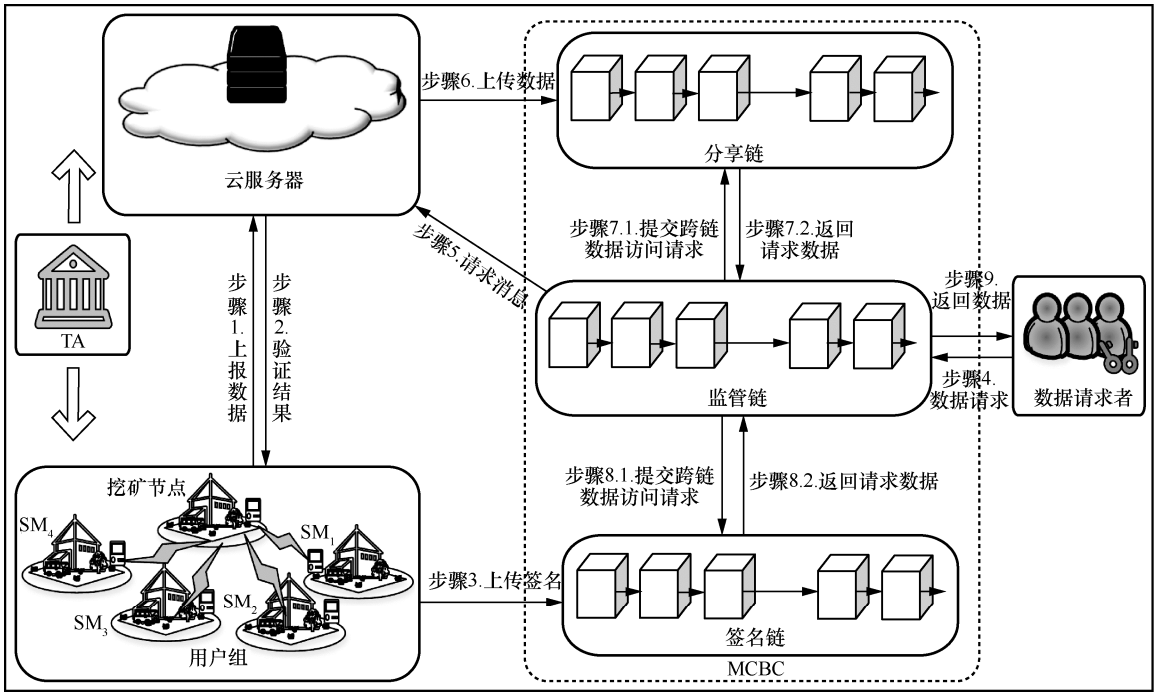

图 1 系统模型

2.2 安全模型

在本文方案的安全模型中，将可能发生的威胁分为内部攻击和外部攻击。

1) 内部攻击。第一，在用户生成区块链的过程中可能有恶意节点冒充网络中的合法节点，发动一些主动攻击（篡改攻击），损害用户私有数据的真实性和完整性。第二，CS 是不可信的，因为它可以选择隐藏数据损坏或丢失，以维护用户的信任。CS 可能发动主动攻击（伪造攻击、替换攻击）来掩盖数据的损坏或丢失。

2) 外部攻击。外部攻击者可以窃听通信通道，试图通过监听信道流量和信息来推断用户的私人数据，或进行伪造攻击，即伪造和修改用户的私人数据。

2.3 设计目标

本文旨在为智能电网设计一种高效、安全的数据聚合与分享方案，在保证数据完整性和隐私性的同时，提高系统的效率。具体来说，本文方案应满足如下设计目标。

1) 多维数据聚合。支持终端设备提交多维度数据，能够对任一维度的数据进行聚合统计，满足智能电网的细粒度数据分析需求，以便提供更加智能化的决策。

2) 隐私保护。授权的实体仅能获得聚合后的电量数据，不能获得单个用户的电量数据，并且未授权的实体不能获得任何有关用户隐私的数据。

3) 完整性验证。在用户向 CS 上报数据的过程中，或者 CS 向 DR 分享数据的过程中，内部或者外部攻击者可能会发起篡改等攻击，因此，作为接收方的 CS 或者 DR 必须能够对数据进行完整性验证。

4) 可公开验证。允许监管链作为代理验证 CS 分享数据的完整性。

5) 高效性。在数据收集和分享的整个过程中，需要传输和处理大量的电量数据，这就要求方案具有较高的计算和通信效率，能够满足智能电网的实际需求。

3 提出方案

本文方案各主要阶段的流程如图 2 所示。

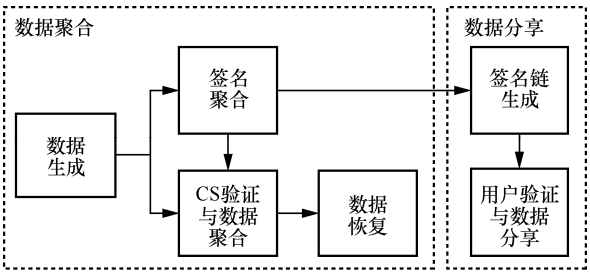

图 2 本文方案各主要阶段的流程

3.1　系统初始化阶段

假设 n 为系统中 SM 的数量，w 为电量数据的维度数，每种维度签名都小于常数 F。智能电表需要在不同时间区间 t_f 周期性（如每 1 h 或 2 h）地发送电量数据。

步骤 1 首先，TA 随机选择 2 个独立的大素数 p 和 q，计算 $N=pq$。然后，随机选择一个公共素数 e，满足 $e>N^2$ 和 $\gcd(e,\varphi(N^2))=1$，其中，$\varphi(N^2)$ 表示欧拉函数。接着，设 g_m 为群 $Z_{N^2}^*$ 中阶最大的公共元素，并绑定一个秘密 $m\in Z_{N^2}^*$。对于每个时间区间 t_f，TA 随机选择 $r_i\in Z_{N^2}^*$ 作为用户的私钥，并计算 $g_m^{r_i}$ 作为公钥。最后，选择安全的同态哈希函数 $H(\cdot)Z_{N^2}^*\to Z_{N^2}^*$。

步骤 2 对于每个时间区间 t_f，TA 使用伪随机数生成器生成一组 n 个不相关随机整数 $\{k_1,k_2,\cdots,k_n\}$ 该生成器充分利用均匀分布的范围 $\{0,\cdots,S-1\}$，k_i 分别为相应 SM_i 的加密密钥。同时计算 CS 的加密密钥 k_0 如下

$$k_0+\sum_{i=1}^{n}k_i=0 \bmod S \tag{4}$$

这里，为了保证安全性，取 $S>n\{m_i\}_{\max}$。

步骤 3 为了提供身份匿名性，TA 根据私钥 r_i 为 SM_i 生成一个假名 $\mathrm{pseu}_i=g_m^{r_i} \bmod N^2$。

步骤 4 TA 根据 SM_i 的假名，创建一个布隆过滤器。具体来说，TA 首先设置一个 v 位的数组，然后使用 u 个哈希函数来计算所有假名的哈希值，最后将数组中索引值为 $h_i(\mathrm{pseu}_i) \bmod v$ 的位置设置为 1。

步骤 5 TA 随机选择一个 R，满足 $R>wF$。

步骤 6 TA 公开系统参数 $\{e,g_m,N,S,R,H\}$。然后，将 $(k_i,\mathrm{pseu}_i,r_i)$ 和 k_0 通过安全信道分别发送给相应的 SM_i 和 CS。最后，TA 将布隆过滤器发送给 CS 和所有 SM。

3.2　数据生成阶段

智能电表 SM_i 周期性地测量并生成 w 种电量数据 $(m_{i1},m_{i2},\cdots,m_{iw})$，并将其加密发送给 CS。智能电表进行如下操作。

步骤 1 首先，SM_i 对 w 维电量数据 m_{ij} 根据密钥 k_i 进行加密

$$d_{ij}=m_{ij}+k_i \bmod S \tag{5}$$

然后，聚合得到 $d_i=\sum_{j=1}^{w}a_jd_{ij}$，其中 $a_j=R^j$。

步骤 2 SM_i 根据 d_i，生成签名如下

$$\sigma_i=C\left[\left(\sum_{j=1}^{w}a_jH(d_{ij})\right)H(\mathrm{pseu}_i\,\|\,T_S),r_i\right] \tag{6}$$

其中，T_S 为当前时间戳。然后，将私钥 r_i 加密为

$$r_i^*=r_i+k_i \bmod S \tag{7}$$

步骤 3 SM_i 将密文和签名打包成数据报告 $\{d_i,r_i^*,\mathrm{pseu}_i,T_S\}$ 和 $\{\sigma_i,\mathrm{pseu}_i,T_S\}$ 分别发送给 CS 和其他用户。

3.3　签名聚合阶段

步骤 1 首先，每个用户接收到 $n-1$ 份数据报告 $\{\sigma_i,\mathrm{pseu}_i,T_S\}$ 后，用 u 个哈希函数来计算假名 pseu_i 的映射值，如果所有映射值都为 1，则证明该假名是合法的；否则，该假名是非法的。然后，检查时间戳以确认这些报告的有效性。

步骤 2 如果步骤 1 的验证通过，所有用户根据接收到的 σ_i 计算平均值。然后，选择 σ_i 最接近平均值的 SM 作为挖矿节点。

步骤 3 挖矿节点基于霍纳法则对签名 σ_i 进行解析，挖矿节点可以获得所有 SM 每个用户各个维度电量数据的签名 $\sigma_{i1},\sigma_{i2},\cdots,\sigma_{iw}$。然后，聚合相同维度电量数据的签名得到 σ_j，即

$$\sigma_j=\prod_{i=1}^{n}\sigma_{ij}=\prod_{i=1}^{n}C(H(d_{ij})H(\mathrm{pseu}_i\,\|\,T_S),r_i) \tag{8}$$

并计算总体聚合签名 σ 如下

$$\begin{aligned}\sigma&=\prod_{j=l_1}^{l_{S_c}}\sigma_j \bmod N^2=\prod_{j=l_1}^{l_{S_c}}\prod_{i=1}^{n}\sigma_{ij} \bmod N^2=\\&C\left(\prod_{j=l_1}^{l_{S_c}}\prod_{i=1}^{n}H(d_{ij})H(\mathrm{pseu}_i\,\|\,T_S),S_c\sum_{i=1}^{n}r_i\right)=\\&C\left(H\left(\sum_{j=l_1}^{l_{S_c}}D_j\right)(T')^{S_c},S_cr_0\right)\end{aligned} \tag{9}$$

步骤 4 挖矿节点将总体聚合签名 σ 发送给 CS。

3.4　CS 端验证与数据聚合阶段

CS 接收到 n 个用户的报告 $\{d_i,r_i^*,\mathrm{pseu}_i,T_S\}$ 和挖矿节点发送总体聚合签名的 σ 后，对所有细粒度数据进行聚合，具体过程如下。

步骤 1 CS 接收到 n 份数据报告后，首先检查

时间戳 T_s。然后对接收到的每个假名使用 u 个哈希函数来计算该假名的索引值，如果所有映射值都为1，则证明该假名是合法的；否则，该假名是非法的。

步骤 2 CS 首先聚合 n 个密文，表示为

$$D^* = \sum_{i=1}^{n} a_1 d_{i1} + \sum_{i=1}^{n} a_2 d_{i2} + \cdots + \sum_{i=1}^{n} a_w d_{iw} \tag{10}$$

然后，CS 基于霍纳法则对聚合密文 D^* 进行解析，可以获得每个用户各维度电量数据的聚合密文 $D_1, D_2, \cdots, D_w$。在该算法中，系数表示每个用户各维度电量数据的聚合密文 $D_j = \sum_{i=1}^{n} d_{ij}$。最后，计算一维聚合密文为

$$D = \sum_{i=1}^{n} D_j \tag{11}$$

步骤 3 CS 首先聚合解密承诺，表示为

$$r_0 = \sum_{i=1}^{n} r_i^* + k_0 \bmod S \tag{12}$$

然后，CS 采用批量验证对签名进行验证，确保收到数据报告中的电量数据未被篡改和伪造，即验证式(13)是否成立。

$$\sigma \bmod N^2 = C\left(H(D)\prod_{i=1}^{n} H(\mathrm{pseu}_i \,\|\, T_S)^w, wr_0 \right) \tag{13}$$

如果式(13)成立，则验证成功，否则验证失败。最后，将验证结果发送给挖矿节点。

为实现CS端批量验证接收数据的完整性，式(13)的正确性验证如下

$$\sigma \bmod N^2 = \prod_{i=1}^{w} \sigma_j \bmod N^2 =$$

$$\prod_{j=1}^{w}\prod_{i=1}^{n} \sigma_{ij} \bmod N^2 =$$

$$\prod_{j=1}^{w}\prod_{i=1}^{n} C(H(d_{ij})H(\mathrm{pseu}_i \,\|\, T_S), r_i) \bmod N^2 =$$

$$C\left(\prod_{j=1}^{w}\prod_{i=1}^{n} H(d_{ij})H(\mathrm{pseu}_i \,\|\, T_S), w\sum_{i=1}^{n} r_i \right) =$$

$$C\left(H\left(\sum_{j=1}^{w}\sum_{i=1}^{n} d_{ij} \right)\prod_{i=1}^{n} H(\mathrm{pseu}_i \,\|\, T_S)^w, w\sum_{i=1}^{n} r_{ij} \right) =$$

$$C\left(H(D)\prod_{i=1}^{n} H(\mathrm{pseu}_i \,\|\, T_S)^w, wr_0 \right) \tag{14}$$

3.5 数据恢复阶段

如果批量验证通过，则 CS 执行密文恢复操作得到多维聚合数据。具体过程如下。

步骤 1 CS 利用私钥 k_0 进行解密得到总体聚合数据 M。

$$M = D^* + wk_0 \bmod S \tag{15}$$

步骤 2 CS 基于霍纳法则对总体聚合数据 M 进行解析，可以恢复多维聚合数据 $M_1, M_2, \cdots, M_w$，在该算法中，系数表示每个维度的聚合电量数据 $M_j = \sum_{i=1}^{n} m_{ij}$。

步骤 3 CS 将多维聚合数据($M_1, M_2, \cdots, M_w$)和当前时间戳 T_S 存储在一起。

3.6 签名链生成阶段

挖矿节点收到 CS 验证成功的结果后，将签名记录到签名链中。

步骤 1 挖矿节点将各维度聚合签名打包成交易的形式 $\mathrm{Tran}_j = (\sigma_j, \mathrm{pseu}_i)$。

步骤 2 挖矿节点对签名进行哈希处理，生成当前哈希 H_c=SHA256(bNum||H_p||timestamp||H_r||average)。其中，bNum 是块号，H_p 是前一个块头的哈希值，timestamp 是时间戳，H_r 是根哈希，average 是平均值。

步骤 3 块头记录根哈希、时间戳、前一个块头的哈希值、块的哈希值和平均值，挖矿节点生成一个新的块。然后，将新块发布给其他用户进行检查。

步骤 4 在接收到新块的时候，用户需要检查时间戳、哈希值、平均值以及与自身相关的信息。如果检查结果一致，则验证成功，然后接收其他用户的检查结果反馈。如果接收到超过 $\frac{2n}{3}+1$ 个用户发送的检查成功的反馈消息，则该新块被添加到签名链上。

3.7 用户端验证与数据分享阶段

当 DR 想要访问数据时，向监管链节点发出数据请求信息，监管链返回正确的数据。具体实现过程如下。

3.7.1 挑战生成

DR 根据需要的电量数据的维度，生成一个含有 S_c 个元素的子集 $I=\{l_1, l_2, \cdots, l_{S_c}\}$作为数据请求信息，随后将其发送给监管链节点。监管链节点接收请求后，需要根据请求内容对每个 $j \in I$ 生成挑战信息 chal=$\{j\}_{j\in I}$，并将其发送给 CS。

3.7.2 证明生成

首先，CS 接收到挑战信息 chal=$\{j\}_{j\in I}$ 后，选择相应维度的聚合数据 $\{D_j\}_{j\in I}$、时间戳 T_S 以及 r_0。其次，计算二次聚合数据 $D^{'}=\sum_{k=1}^{k=S_c}a_kD_{lk}$ 和 $T^{'}=\prod_{i=1}^{n}H(\text{pseu}_i\,\|\,T_S)$。最后，CS 生成分享事务 $T_{\text{Share}}=(D^{'},r_0,T^{'})$，如果前一个块的哈希值被填满，就按照规则生成分享链的一个新块，并向监管链发送一个已生成新块的提醒。

3.7.3 数据验证

监管链节点在接收到提醒后，首先调用链码分别向分享链和签名链申请验证证明 (D',r_0,T') 和相应维度电量数据的聚合签名 $D_j=\sum_{i=1}^{n}d_{ij}$ 等信息。然后，监管链节点根据霍纳法则解析二次聚合数据 D' 获得相应维度的加密数据 D_j。最后，监管链节点根据获得的数据验证 CS 存储加密数据的完整性，即验证式(16)是否成立，如果成立则验证成功，否则验证失败。

$$\prod_{j=l_1}^{l_{S_c}}\sigma_j \bmod N^2=C\left(H\left(\sum_{j=l_1}^{l_{S_c}}D_j\right)(T^{'})^{S_c},S_cr_0\right)\quad(16)$$

为实现用户端批量验证 CS 存储数据的完整性，式(16)的正确性验证如下

$$\prod_{j=l_1}^{l_{S_c}}\sigma_j \bmod N^2=\prod_{j=l_1}^{l_{S_c}}\prod_{i=1}^{n}\sigma_{ij} \bmod N^2=$$

$$\prod_{j=l_1}^{l_{S_c}}\prod_{i=1}^{n}C(H(d_{ij})H(\text{pseu}_i\,\|\,T_S),r)_i \bmod N^2=$$

$$C\left(\prod_{j=l_1}^{l_{S_c}}\prod_{i=1}^{n}H(d_{ij})H(\text{pseu}_i\,\|\,T_S),S_C\sum_{i=1}^{n}r_i\right)=$$

$$C\left[H\left(\sum_{j=l_1}^{l_{S_c}}\sum_{i=1}^{n}d_{ij}\right)\prod_{i=1}^{n}(H(\text{pseu}_i\,\|\,T_S))^{S_c},S_c\sum_{i=1}^{n}r_i\right]=$$

$$C\left(H\left(\sum_{j=l_1}^{l_{S_c}}D_j\right)(T^{'})^{S_c},S_cr_0\right)\quad(17)$$

3.7.4 数据分享

如果数据验证成功，监管链节点将相应维度的聚合数据 $\{D_j\}_{j\in\text{I}}$ 发送给 DR，CS 通过安全通道将密钥 k_0 发送给 DR，DR 根据密钥 k_0 解密，获得所需要的电量数据。否则，监管链节点将返回给 DR 数据损坏的通知并终止交易。

4 安全分析

4.1 完整性

定理 1 用户只有发送给 CS 正确的数据报告才能通过 CS 端的完整性验证。

证明 给定 n 个来自用户的数据报告 $\{d_i,r_i^*,\text{pseu}_i,T_S\}$，其中 $r_i^*=r_i+k_i \bmod S$，CS 计算 $D_j=\sum_{i=1}^{n}d_{ij}$，$D=\sum_{j=1}^{w}D_j$，$r_0=\sum_{i=1}^{n}r_i^*+k_0 \bmod S$。然后，根据挖矿节点发送的 σ，CS 计算得到

$$\sigma \bmod N^2=C\left(H(D)\prod_{i=1}^{n}H(\text{pseu}_i\,\|\,T_S)^w,wr_0\right)(18)$$

根据式(16)，CS 可以计算得出

$$\sigma \bmod N^2=\prod_{j=1}^{w}\sigma_j \bmod N^2=$$

$$C\left(H(D)\prod_{i=1}^{n}H(\text{pseu}_i\,\|\,T_S),wr_0\right)\quad(19)$$

因此，当且仅当用户发送给 CS 正确的数据报告时，式(19)成立，才能通过 CS 端的完整性验证。证毕。

定理 2 CS 只有正确地存储数据才能通过用户端的完整性验证。

证明 给定一个来自分享链生成的新块数据 $(\{D_j\}_{j\in\text{I}},r_0,T^{'})$，其中 $T^{'}=\prod_{i=1}^{n}H(\text{pseu}_i\,\|\,T_S)$。监管链节点调用链码向分享链和签名链申请数据，得到返回数据后监管链节点验证签名，如式(20)所示。

$$\prod_{j=l_1}^{l_{S_c}}\sigma_j \bmod N^2=$$

$$C(H\left(\sum_{j=l_1}^{l_{S_c}}D_j\right)(T^{'})^{S_c},S_cr_0)\quad(20)$$

根据式(17)，监管链节点计算得到

$$\prod_{j=l_1}^{l_{S_c}}\sigma_j \bmod N^2=\prod_{j=l_1}^{l_{S_c}}\prod_{i=1}^{n}\sigma_{ij} \bmod N^2=$$

$$C\left(\prod_{j=l_1}^{l_{S_c}}\prod_{i=1}^{n}H(d_{ij})H(\text{pseu}_i\,\|\,T_S),S_c\sum_{i=1}^{n}r_i\right)=$$

$$C\left(H(\sum_{j=l_1}^{l_{S_c}}D_j)(T^{'})^{S_c},S_cr_0\right)\quad(21)$$

因此，当且仅当 CS 正确的存储数据时，式(21)成立，才能通过用户端的完整性验证。证毕。

4.2 隐私性

许多研究者提出了基于掩蔽的智能电网隐私保护的数据聚合方案[22-25]。

定理 3 CS 无法根据 d_i、D^*和 D 推断出单个 SM 的电量数据。

证明 在本文方案中，SM_i 将电量数据传输给 CS，CS 将数据聚合解密后通过算法 3 恢复各维度电量数据的总和。在这个过程中单一电量数据从未作为普通值释放，CS 只能得到加密后的数据 $d_i=\sum_{j=1}^{w}a_jd_{ij}=\sum_{j=1}^{w}a_jm_{ij}+k_i \bmod S$。但是 k_i 是不可区分的随机值，k_i 完全由 TA 产生，SM_i 保留 k_i。因此，在没有任何目标 SM_i 的加密密钥 k_i 的情况下，CS 无法根据 d_i、D^*和 D 推断出单个 SM 的电量数据。证毕。

定理 4 外部攻击者无法提取任何关于目标 SM 的数据。

证明 在数据聚合的整个过程中，外部攻击者没有关于 k_i 的任何信息。因此，在没有任何可用的加密密钥 k_i 的情况下，外部攻击者无法获取任何关于目标 SM 的数据。证毕。

4.3 抵抗攻击

4.3.1 抗伪造攻击

定理 5 CS 伪造的数据无法通过用户端的完整性验证。

证明 如果数据被损坏或丢失，CS 可能会伪造数据以通过验证。因此，将安全游戏根据文献[26]定义如下。

通过分析挑战信息 chal=$\{j\}_{j\in I}$，CS 可以生成一个伪造的证明($\{D_j^{'}\}_{j\in I}, r_0^{'}, T^{''}$)。如果根据该证明不能通过验证，CS 就会输掉游戏；否则，监管链节点可以成功验证 CS 存储数据的完整性，如式(22)所示。

$$\prod_{j=l_1}^{l_{S_c}}\sigma_j \bmod N^2=C\left(H\left(\sum_{j=l_1}^{l_{S_c}}D_j^{'}\right)(T^{''})^{S_c},S_cr_0^{'}\right) \tag{22}$$

根据式(17)分析可知

$$C\left(H\left(\sum_{j=l_1}^{l_{S_c}}D_j\right)(T^{'})^{S_c},S_cr_0\right)=C\left(H\left(\sum_{j=l_1}^{l_{S_c}}D_j^{'}\right)(T^{''})^{S_c},S_cr_0^{'}\right) \tag{23}$$

即

$$\left(H\left(\sum_{j=l_1}^{l_{S_c}}D_j\right)(T^{'})^{S_c}\right)^e g_m^{S_cr_0}=\left(H\left(\sum_{j=l_1}^{l_{S_c}}D_j^{'}\right)(T^{''})^{S_c}\right)^e g_m^{S_cr_0^{'}} \bmod N^2 \tag{24}$$

由此可以得出

$$g_m^{S_c(r_0-r_0^{'})}=\left[\frac{\left(H\left(\sum_{j=l_1}^{l_{S_c}}D_j\right)(T^{'})^{S_c}\right)}{\left(H\left(\sum_{j=l_1}^{l_{S_c}}D_j^{'}\right)(T^{''})^{S_c}\right)}\right]^e \tag{25}$$

由于 $r_0, r_0^{'}\in Z_{N^2}^*$，且 e 是一个比 N 大的素数，可以得出 $S_c(r_0-r_0^{'})<e$ 并且 $\gcd(S_c(r_0-r_0^{'}),e)=1$。因此，根据 Bèzout 等式，存在整数 A 和 B，使 $AS_c(r_0-r_0^{'})+Be=\gcd(S_c(r_0-r_0^{'}),e)=1$ 成立。由此可得

$$g_m^1=g_m^{AS_c(r_0-r_0^{'})+Be}=(g_m^{S_c(r_0-r_0^{'})})^A g_m^B \bmod N^2=\left[\left(\frac{H\left(\sum_{j=l_1}^{l_{S_c}}D_j\right)(T^{'})}{H\left(\sum_{j=l_1}^{l_{S_c}}D_j^{'}\right)(T^{''})^{S_c}}\right)^A g_m^B\right]^e \tag{26}$$

因此，最终可以得出

$$g_m^{1/e}=\left(\frac{H\left(\sum_{j=l_1}^{l_{S_c}}D_j\right)(T^{'})}{H\left(\sum_{j=l_1}^{l_{S_c}}D_j^{'}\right)(T^{''})^{S_c}}\right)^A g_m^B \tag{27}$$

根据式(27)可以计算出 g_m 模 N^2 的 e 根，但是，这与 RSA 对足够大的复合 N^2 的困难性假设相矛盾。因此，可以得出结论，CS 伪造的数据无法通过用户端的完整性验证。证毕。

定理 6 外部攻击者伪造的数据无法通过完整性验证。

证明 在所提方案中，没有参与者可以在没有私钥 r_i 和 k_i 的情况下生成正确的数据$\{d_i, r_i^*, \text{pseu}_i, T_S\}$，其中 $r_i^*=r_i+k_i \bmod S$。并且定理 5 表明攻击者无法生成有效的签名。因此，外部攻击者伪造的数据无法通过完整性验证。证毕。

4.3.2 抗替换攻击

定理 7 CS 用其他维度的数据替换指定维度的数据是无效的。

证明　CS 发起替换游戏时，在收到挑战信息 chal= $\{j\}_{j\in \mathrm{I}}$ 后，将返回到($\{D_j^{'}\}_{j\in \mathrm{I}}, r_0, T^{'}$)中进行验证，其中第 l_i 维数据被替换为第 l_k 维数据（$k\neq i$）。如果该证明无法得到证实，CS 将会输掉游戏，结果如式(28)所示

$$\sigma' \bmod N^2 = \prod_{j\in I \& j\neq l_i} \sigma_j \sigma_{l_k} \bmod N^2 = C\left(H\left(\sum_{j\in I \& j\neq l_i} D_j \right) (T^{'})^{S_c-1}, (S_c-1) r_0 \right) C(H(D_{l_k})T^{'}, r_0) \tag{28}$$

根据承诺的性质，将式(28)化简可得

$$\sigma_{l_i} \bmod N^2 = C(H(D_{l_i})T^{'}, r_0) = C(H(D_{l_k})T^{'}, r_0) \tag{29}$$

如果式(29)成立，则有 $H(D_{l_i}) = H(D_{l_k})$ 成立，即 $D_{l_i} = D_{l_k}$。然而，根据定义可知 $D_{l_i} \neq D_{l_k}$。此外，同态哈希函数是抗碰撞的。因此，$H(D_{l_i})$ 和 $H(D_{l_k})$ 并不相同。由此可得，CS 输掉了游戏，CS 用其他维度的数据替换指定维度的数据是无效的。证毕。

4.3.3　抗重放攻击

定理 8　本文方案中，外部攻击者不能使用之前的数据通过验证。

证明　外部攻击者只有通过验证，才能赢得游戏。但是，由于当前的时间戳与旧的时间戳不同，外部攻击者无法使用之前的数据通过验证。证毕。

4.4　安全特性比较

本文方案与文献[11,16-18]方案的安全特性比较如表 1 所示。从表 1 可以看出，本文方案可以满足表 1 中的所有安全特性，而其余方案只能满足部分安全特性。对于轻量级验证的安全特性，已知在文献[11]方案中验证数据完整性，仅需要控制中心进行少量的轻量级运算，如指数运算、乘法运算和对数运算等；在文献[16]方案中，为了实现在多个云数据中心的多数据副本的完整性验证，需要进行大量的签名验证算法；在文献[17]方案中，为了实现双端可验证，使用了大量的双线性配对运算；在文献[18]方案中，需要用户端验证结果正确性，并进行大量的签名验证算法。

5　性能分析

本节将具体评价本文方案的性能，包括完整性验证有效性、计算成本和通信成本。所提方案将与 2 个具有代表性的方案，即 Mouris 等[19]提出的方案和 Tian 等[17]提出的方案进行比较。仿真实验在一台配置 Intel Core i5-1135G7 的 CPU、16 GB 内存、安装 Windows10 系统的笔记本电脑上进行，实验代码采用 Java 语言编写。公平起见，实验中本文方案的模 S 和 RSA 的模数 N 分别定义为 512 bit 和 1 024 bit，并采用 160 bit 的椭圆曲线以及组阶为 160 bit 的 MNT d159 曲线。实验测量数据均取 1 000 次运行的平均值。

5.1　完整性验证有效性

假设云存储的数据是 w 维，其中 z 维是错误的（如被损坏或被篡改），每次随机抽样 μ 维来进行验证。本文验证算法基于概率模型，设随机变量 X 表示检测到的数据被损坏的维数，因此可以得出 $P\{X\geqslant 1\} \in \left[1-\left(\frac{w-z}{w}\right)^{\mu}, 1-\left(\frac{w-z-\mu+1}{w-\mu}\right)^{\mu} \right]$，则验证一次检测到错误的概率至少为 $1-\left(\frac{w-z}{w}\right)^{\mu}$。当验证 a 次时，随机挑战的维数则为 $a\mu$，因此验证 a 次检测到错误的概率 $P\geqslant 1-\left(\frac{w-z}{w}\right)^{a\mu}$，即至少有 $1-\left(\frac{w-z}{w}\right)^{a\mu}$ 的概率检测到数据被损坏。图 3 说明了完整性验证算法的有效性，例如，当 z=0.02w 时，如果监管链节点随机检测的维数为 $a\mu$=200，则检测到错误的概率大于 0.982 4。

表 1　本文方案与相关方案的安全特性比较

方案	用户端可验证性	云端可验证性	隐私性	一对多验证性	区块链技术	可公共验证	抗攻击性	轻量级验证
文献[11]方案	否	是	是	是	是	否	否	是
文献[16]方案	是	否	否	否	否	是	是	否
文献[17]方案	是	是	是	是	否	是	是	否
文献[18]方案	是	否	是	是	是	是	是	否
本文方案	是	是	是	是	是	是	是	是

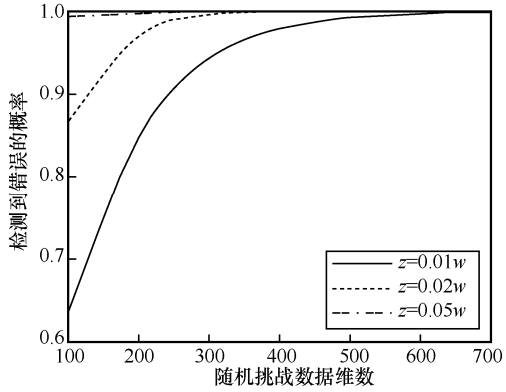

图 3 完整性验证算法的有效性

5.2 计算成本

实验中，主要操作的运行时间如表 2 所示，忽略了一些轻量级操作，如加法、减法等。

表 2 主要操作的运行时间

符号	操作	运行时间/ms
T_{M}	G_1 中的乘法运算操作	0.08
T_{ECC}	ECC 中的放缩乘法操作	0.07
T_{p}	双线性配对操作	1.90
T_{H_1}	单向哈希操作	0.02
T_{H_2}	映射到点的哈希操作	0.65
T_{N^2}	Z_{N^2} 中的求幂操作	0.37
$T_{\exp}$	p 中的求幂操作	0.03
T_m	双线性配对中的比例乘法操作	0.26

首先，计算不同方案下 SM 生成签名的计算成本。在 Mouris 等方案中，每个 SM 生成签名需要在 G_1 中进行 w 次乘法运算操作，在 ECC 中进行 w 次缩放乘法操作和 w 次单向哈希操作。因此，SM 生成签名的计算成本为 $w(T_{\mathrm{M}}+T_{\mathrm{ECC}}+T_{H_1})$= 0.17$w$ ms。在 Tian 等方案中，每个 SM 生成签名需要在 G_1 中进行 3w 次幂运算操作，3w 次单向哈希操作。

因此，SM 生成签名的计算成本为 $3w(T_{\exp}+T_{H_1})$ = 0.15w ms。在本文方案中，每个 SM 生成签名需要 w+1 次单项哈希操作、2 次在 Z_{N^2} 中的求幂操作和 2 次在 G_1 中的乘法运算操作。因此，SM 生成签名的计算成本为 $(w+1)T_{H_1}+2T_{N^2}+2T_{\mathrm{M}}$ = (0.02w+0.92) ms。

其次，计算不同方案下 CS 端完整性验证的计算成本。Mouris 等方案缺少这一验证阶段，因此在这个阶段只与 Tian 等方案进行比较。在 Tian 等方案中，FN 验证签名需要 2w 次双线性配对操作、w 次双线性配对中的比例乘法操作、w 次单向哈希操作和 2w 次在 G_1 中的幂运算操作。因此，FN 验证签名的计算成本为 $w(2T_{\mathrm{p}}+T_m+T_{H_1}+2T_{\exp})$= 4.14$w$ ms。在 Tian 等方案中，CSP 验证签名需要 2w+2 次双线性配对操作、w 次映射到点的哈希操作、一次双线性配对中的比例乘法操作，一次单向哈希操作和 2 次在 G_1 中的幂运算操作。因此，CSP 验证签名的计算成本为 $w(2T_{\mathrm{p}}+T_{H_1})+2T_{\mathrm{p}}+T_m+T_{H_1}+2T_{\exp}$ = (4.45w + 4.14) ms。在本文方案中，CS 验证签名需要 2 次单项哈希操作，3 次在 Z_{N^2} 中的求幂操作和 2 次在 G 中的乘法运算操作。因此，CS 验证签名的计算成本为 $2T_{H_1}+3T_{N^2}+2T_{\mathrm{M}}$ = 1.31 ms。

最后，计算不同方案下用户端完整性验证的计算成本。在 Mouris 等方案中，TPA 验证签名需要 μ 次单项哈希操作、一次在 G_1 上的乘法运算操作和 2 次在 ECC 中的缩放乘法操作。因此，TPA 验证签名的计算成本为 $\mu T_{H_1}+T_{\mathrm{M}}+2T_{\mathrm{ECC}}=(0.02\mu+0.22)$ ms。在 Tian 等方案中，TPA 验证签名需要 μ+1 次单项哈希操作、一次在 G_1 中的幂运算操作和一次双线性配对操作。因此，TPA 验证签名的计算成本为 $(\mu+1)T_{H_1}+T_{\exp}+T_{\mathrm{p}}=(0.03\mu$+1.96) ms。在本文方案中，监管链节点验证签名需要 μ+2 次在 G_1 中的乘法运算操作、3 次在 Z_{N^2} 中的求幂操作和一次单向哈希操作。因此，监管链节点验证签名的计算成本为 $(\mu+2)T_{\mathrm{M}}+3T_{N^2}+T_{H_1}=(0.08\mu$+1.29) ms。

图 4 展示了 3 种方案的计算成本对比。图 4(a)给出了 3 种方案的 SM 生成签名的计算成本随数据维数 w 增大的变化情况。显然，与其他方案相比，本文方案 SM 的计算成本最小。图 4(b)给出了本文方案 CS 端和 Tian 等方案 CSP 和 FN 验证签名的计算成本随数据维数 w 增大的变化情况。从图 4(b)可以看出，随着数据维数 w 的增长，本文方案 CS 端验证签名的计算成本基本保持不变，并且远小于 Tian 等方案的计算成本。其原因是本文方案采用霍纳法则将多维数据构造成一个数据，只需要对该数据进行一次验证即可。图 4(c)给出了 3 种方案的用户端验证签名的计算成本随数据维数 w 增大的变化情况。由于实现了一个签名算法双端可验证，因此本文方案用户端验证的计算成本要稍大于其他方案，但是差距并不是特别大。总体来说，本文方案有效地降低了计算成本。

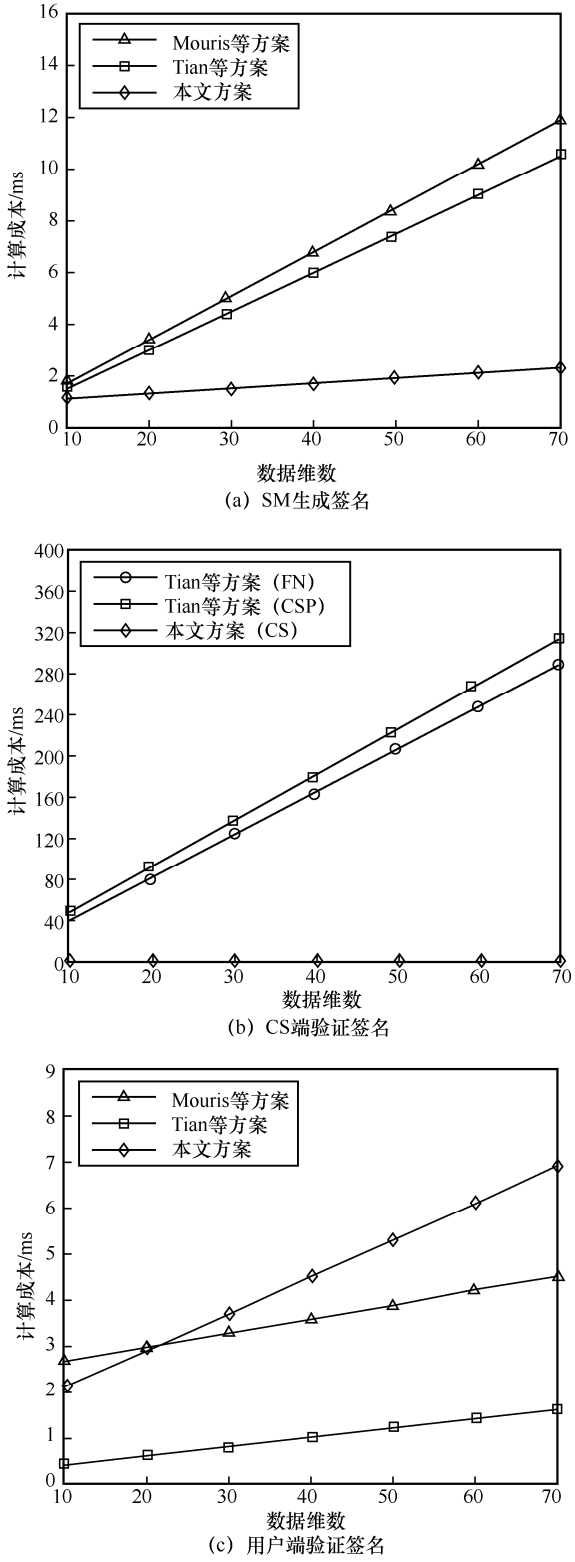

图 4　3 种方案的计算成本对比

5.3　通信成本

本节将 3 种方案在数据传输阶段、数据验证与分享阶段的通信成本进行对比，其中，哈希函数的长度为 160 bit，时间戳的长度为 32 bit。

图 5 展示了 3 种方案在数据传输阶段的通信成本对比。在本文方案中，SM_i 向 CS 发送 $\{d_i, r_i^*, \text{pseu}_i, T_S\}$，挖矿节点向 CS 发送 σ，因此，这一阶段本文方案的通信成本为 n(512+2 048+2 048 +32) + 2 048 = (4 640n+2 048) bit。图 5(a)给出了在用户数量 n=1 000 时，3 种方案通信成本随数据维数 w 增加的变化情况。图 5(b)给出了在数据维数 w=70 时，3 种方案通信成本随用户数量 n 增加的变化情况。从图 5 可以看出，本文方案的通信成本低于其他 2 种方案。

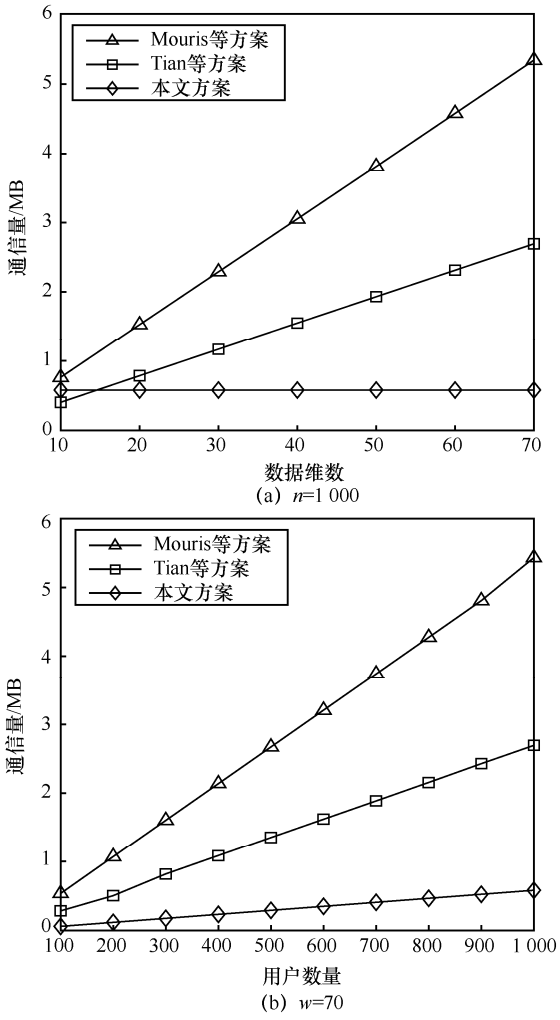

图 5　数据传输阶段的通信成本对比

图 6 展示了 3 种方案在数据验证与分享阶段的通信成本对比。在本文方案中，监管链节点获得返回数据 $(D', r_0, T', \{\sigma_j\}_{j\in I})$，因此，这一阶段本文方案的通信成本为 512+2 048+160+ 2 048μ = (2 720+ 2 048μ) bit。图 6(a)给出了在用户数量 n=1 000 时，3 种方案通信成本随抽样数

据维数 μ 增加的变化情况。显然，与 Mouris 等方案相比，本文方案的通信成本几乎可以忽略不计，而更接近 Tian 等方案。图 6(b)给出了在 μ=70 时，3 种方案通信成本随用户数量 n 增加的变化情况。从图 6(b)可以看出，在抽样数据维数固定的条件下，随着用户数量 n 的增长，本文方案的通信成本基本保持不变。

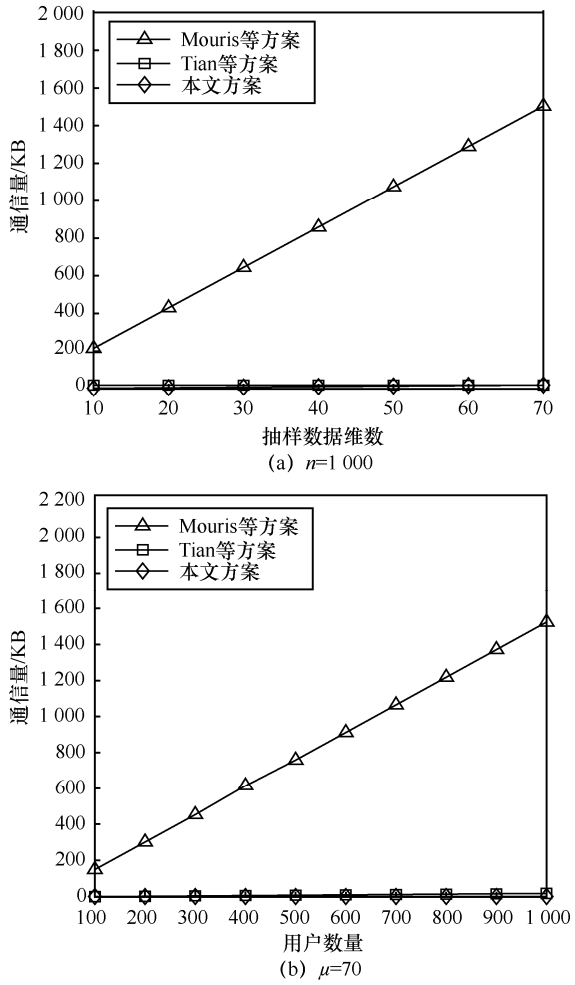

图 6 数据验证与分享阶段的通信成本对比

6 结束语

针对现有方案在支持轻量级多维数据的收集，实现整体上对多维数据的完整性有效验证，以及处理云服务器集中化问题等方面存在的不足，本文提出了一种基于区块链且可验证的数据聚合与分享方案。本文方案从整体上设计了支持多维数据的完整性验证算法，利用掩蔽值和霍纳法则实现了隐私保护多维数据聚合；结合基于 RSA 的乘法同态性承诺方案和同态哈希函数设计了一种新的签名算法，不仅实现了云存储数据的双端可验证性，还可以抵抗内部恶意攻击。进一步地，提出了一种基于联盟链多链的聚合数据分享体系结构，有效地避免了单机处理瓶颈和易受攻击等集中化问题。理论分析和性能实验表明，本文方案能够很好地满足设计目标。

参考文献：

[1] VASILJEVSKA J. Smart grids and beyond - an EU research and innovation perspective: EUR 30786[S]. 2021.

[2] 贺琰旻. 电力周界安防的应用及发展变化[J]. 中国安防, 2015(12): 35-38.
HE Y M. Application and development of power perimeter security[J]. China Security & Protection, 2015(12): 35-38.

[3] GHIASI M, NIKNAM T, WANG Z, et al. A comprehensive review of cyber-attacks and defense mechanisms for improving security in smart grid energy systems: past, present and future[J]. Electric Power Systems Research, 2023, 215: 108975.

[4] KIM Y, HAKAK S, GHORBANI A. Smart grid security: attacks and defence techniques[J]. IET Smart Grid, 2023, 6(2): 103-123.

[5] SULTAN S. Privacy-preserving metering in smart grid for billing, operational metering, and incentive-based schemes: a survey[J]. Computers & Security, 2019, 84: 148-165.

[6] FAN M C, ZHANG X H. Consortium blockchain based data aggregation and regulation mechanism for smart grid[J]. IEEE Access, 2019, 7: 35929-35940.

[7] ZHAO S, LI F H, LI H W, et al. Smart and practical privacy-preserving data aggregation for fog-based smart grids[J]. IEEE Transactions on Information Forensics and Security, 2021, 16: 521-536.

[8] LU R X, LIANG X H, LI X, et al. EPPA: an efficient and privacy-preserving aggregation scheme for secure smart grid communications[J]. IEEE Transactions on Parallel and Distributed Systems, 2012, 23(9): 1621-1631.

[9] CHEN Y W, MARTÍNEZ-ORTEGA J F, CASTILLEJO P, et al. A homomorphic-based multiple data aggregation scheme for smart grid[J]. IEEE Sensors Journal, 2019, 19(10): 3921-3929.

[10] MING Y, ZHANG X Y, SHEN X Q. Efficient privacy-preserving multi-dimensional data aggregation scheme in smart grid[J]. IEEE Access, 2019, 7: 32907-32921.

[11] LI K, YANG Y, WANG S, et al. A lightweight privacy-preserving and sharing scheme with dual-blockchain for intelligent pricing system of smart grid[J]. Computers & Security, 2021, 103: 102189.

[12] LI K, SHI R, WU M, et al. A novel privacy-preserving multi-level aggregate signcryption and query scheme for smart grid via mobile fog computing[J]. Journal of Information Security and Applications, 2022, 67: 103214.

[13] YANG C, CHEN X, XIANG Y. Blockchain-based publicly verifiable data deletion scheme for cloud storage[J]. Journal of Network and

Computer Applications, 2018, 103: 185-193.

[14] GUO R, ZHUANG C Y, SHI H X, et al. A lightweight verifiable outsourced decryption of attribute-based encryption scheme for blockchain-enabled wireless body area network in fog computing[J]. International Journal of Distributed Sensor Networks, 2020, doi: org/oi.org/10.1177/1550147720906796.

[15] PING Y, ZHAN Y, LU K, et al. Public data integrity verification scheme for secure cloud storage[J]. Information, 2020, 11(9): 409.

[16] LI J G, YAN H, ZHANG Y C. Efficient identity-based provable multi-copy data possession in multi-cloud storage[J]. IEEE Transactions on Cloud Computing, 2022, 10(1): 356-365.

[17] TIAN H, NAN F L, CHANG C C, et al. Privacy-preserving public auditing for secure data storage in fog-to-cloud computing[J]. Journal of Network and Computer Applications, 2019, 127: 59-69.

[18] TAN T L, SALAM I, SINGH M. Blockchain-based healthcare management system with two-side verifiability[J]. PLoS One, 2022, 17(4): e0266916.

[19] MOURIS D, TSOUTSOS N G. Masquerade: verifiable multi-party aggregation with secure multiplicative commitments[J]. IACR Cryptology ePrint Archive, 2021: eprint.iacr.org/2021/1370.

[20] YAO H L, WANG C F, HAI B, et al. Homomorphic hash and blockchain based authentication key exchange protocol for strangers[C]// Proceedings of 2018 Sixth International Conference on Advanced Cloud and Big Data (CBD). Piscataway: IEEE Press, 2018: 243-248.

[21] OU W, HUANG S, ZHENG J, et al. An overview on cross-chain: echanism, platforms, challenges and advances[J]. Computer Networks, 2022, 218: 109378.

[22] GOPE P A, SIKDAR B. Lightweight and privacy-friendly spatial data aggregation for secure power supply and demand management in smart grids[J]. IEEE Transactions on Information Forensics and Security, 2018, 14(6): 1554-1566.

[23] SONG J, LIU Y, SHAO J, et al. A dynamic membership data aggregation (DMDA) protocol for smart grid[J]. IEEE Systems Journal, 2019, 14(1): 900-908.

[24] XUE K P, ZHU B, YANG Q Y, et al. An efficient and robust data aggregation scheme without a trusted authority for smart grid[J]. IEEE Internet of Things Journal, 2019, 7(3): 1949-1959.

[25] SU Y, LI Y P, LI J L. LCEDA: lightweight and communication-efficient data aggregation scheme for smart grid[J]. IEEE Internet of Things Journal, 2021, 8(20): 15639-15648.

[26] LI J, WU J, JIANG G, et al. Blockchain-based public auditing for big data in cloud storage[J]. Information Processing & Management, 2020, 57(6): 102382.

[作者简介]

陈建伟（1980− ），男，福建诏安人，博士，福建师范大学副教授、硕士生导师，主要研究方向为物联网、移动群感知计算、网络安全与隐私保护等。

王姝妤（1996− ），女，山东德州人，福建师范大学硕士生，主要研究方向为物联网、隐私保护。

张美平（1979− ），男，福建宁化人，福建师范大学副教授，主要研究方向为嵌入式系统、数据安全等。

张桢萍（1979− ），女，福建连城人，福建师范大学讲师，主要研究方向为网络安全与隐私保护等。