支持类型验证的多维数据选择性聚合方案

牛坤[1,2]，石淼[1,2]，彭长根[1,2]，许德权[3]，蔡斐[4]

（1.贵州大学计算机科学与技术学院，贵州 贵阳 550025；2.省部共建公共大数据国家重点实验室，贵州 贵阳 550025；
3.贵阳学院计算机科学学院，贵州 贵阳 550005；4.贵州轻工职业大学信息中心，贵州 贵阳 550025）

摘　要：随着物联网的普及，密态数据聚合已成为提升传输效率与保障隐私的重要技术。现有方案大多基于同态加密与聚合签名，能够实现加密状态下的数据汇总，但普遍仅支持单一或固定维度的聚合，且在边缘计算场景下计算与通信成本较大。针对上述问题，提出一种支持类型验证的多维密态数据选择性聚合方案。该方案基于改进的Paillier加密方案实现高效加密，结合双线性对、中国剩余定理与Shamir秘密共享，构建安全传输与分类聚合机制。实验与安全性分析结果表明，所提方案在数据隐私保护、聚合灵活性方面均优于现有方案，计算成本至少降低50%。

关键词：数据聚合；数据安全传输；聚合签名；隐私保护

中图分类号：TP309

文献标志码：A

DOI：10.11959/j.issn.1000–436x.2025179

Selective aggregation scheme for multi-dimensional data with type-based verification

NIU Kun[1,2], SHI Miao[1,2], PENG Changgen[1,2], XU Dequan[3], CAI Fei[4]

1. School of Computer Science and Technology, Guizhou University, Guiyang 550025, China
2. State Key Laboratory of Public Big Data, Ministry of Education, Guiyang 550025, China
3. College of Computer Science, Guiyang University, Guiyang 550005, China
4. Information Center of Guizhou Light Industry Polytechnic University, Guiyang 550025, China

Abstract: With the rapid proliferation of the Internet of things (IoT), ciphertext data aggregation has emerged as a fundamental technique to enhance transmission efficiency while preserving data privacy. Most existing schemes relied on homomorphic encryption and aggregate signatures to enable data aggregation in the encrypted domain, but they typically supported only single or fixed-dimensional aggregation and incurred high computation and communication overhead in edge computing scenarios. To address these issues, a selective ciphertext data aggregation scheme that supported type verification and multi-dimensional data was proposed. The scheme employed an improved Paillier encryption algorithm for efficient encryption, and integrated bilinear pairing, the Chinese Remainder Theorem, and Shamir's secret sharing to construct a secure transmission and classified aggregation mechanism. Experimental and security analysis results demonstrate that the proposed scheme outperforms existing schemes in terms of data privacy preservation and aggregation flexibility, with a computational cost reduction of at least 50%.

Keywords: data aggregation, data security transmission, aggregate signature, privacy protection

收稿日期：2025–08–19；**修回日期：**2025–10–11

通信作者：彭长根，cgpeng@gzu.edu.cn

基金项目：贵州省科技计划基金资助项目（No.[2023]434, No.[2023]371）；国家自然科学基金资助项目（No.62272124）；贵州大学引进人才科研基金资助项目（No.[2022]21）；贵阳学院博士科研启动基金资助项目（No.GYU-KY-[2025]-02）

Foundation Items: The Science and Technology Project of Guizhou Province (No.[2023]434, No.[2023]371), The National Natural Science Foundation of China (No.62272124), Research Projects for Talent Introduction at Guizhou University (No.[2022]21), The Research Initiation Funding Project of Guiyang University (No.GYU-KY-[2025]-02)

0 引言

随着物联网、云计算、大数据技术的飞速发展，各行各业产生的数据量呈指数级增长，如何有效地收集、处理、分析并挖掘这些数据背后的价值，成为学术界和工业界共同面临的重大挑战与机遇。在此背景下，数据聚合[1]技术应运而生，它不仅是一种数据处理手段，更是连接数据孤岛、实现数据价值最大化的桥梁。

在现有研究中，密态数据聚合技术大致经历了3个发展阶段：早期同态加密探索、边缘计算引入以及特定领域应用优化。在早期阶段，研究者主要关注基础同态加密的可行性。Gentry[2]首次提出了全同态加密（FHE）的方案。Lu等[3]使用同态Paillier密码系统对数据进行加密，在密文基础上进行数据聚合，并采用批量认证技术降低了认证成本，为后续研究奠定了基础。Lyu等[4]通过优化加密协议与减少通信成本，显著提升了聚合效率，并在一定程度上降低了计算负担。但需要指出的是，即使经过上述优化，同态加密依然属于计算密集型过程，该方法在低带宽场景下依旧面临通信受限与计算性能不足的双重挑战。

随着边缘计算的引入，研究重点转向如何在边缘侧高效完成聚合。基于边缘计算的可验证密态数据聚合方案[5]通过改进BGN（Boneh-Goh-Nissim）同态加密算法和Shamir秘密共享方案，确保数据在传输过程中的安全性和机密性，但在资源受限的边缘节点上仍存在计算与通信成本较大的问题。在工业物联网场景中，Shang等[6]进一步提出了一种健壮型隐私保护数据聚合方案，结合同态加密与高效密钥管理，使边缘节点能够直接对密文进行聚合，并通过抗攻击机制提升了系统健壮性。

随着应用场景的扩展，不同领域提出了多种轻量级聚合方法，如Gheisari等[7]提出的PPDMIT架构利用Paillier同态加密、哈希链、K-means聚类和中国剩余定理，在IoT-Cloud环境下实现了轻量级聚合，在隐私保护与效率方面均优于传统方法。Zhang等[8]设计了基于身份的聚合签名协议，虽然提升了签名验证效率，但在数据传输隐私保护方面仍存在不足。

为解决多维数据聚合的挑战，已有研究提出了多种优化方法：Shen等[9]利用霍纳法则实现多区域用户数据隐私保护聚合；Li等[10]通过超递增序列扩展了多子集数据聚合能力；Kong等[11]和Hu等[12]分别利用中国剩余定理结合Paillier加密实现多维数据聚合，有效提升了资源利用率。随着安全需求的提升，Merad-boudia等[13]和Zhang等[14]开始探索多维数据的批量验证机制，后者通过改进的BLS签名显著增强了电网数据的完整性保护。近年来，Shi等[15]提出的雾云架构方案以及Liu等[16]基于多秘密共享的创新方法都转向了更复杂的架构设计。此外，将区块链技术引入数据聚合的方案[17]，通过结合聚合签名和匿名认证实现了细粒度数据管理。Singh等[18]进一步探索系统级优化，提出了结合差分隐私、轻量级密码学与联邦学习的框架，并结合边缘计算与区块链认证实现了大规模IoT下的高效数据管理。Zhu等[19]的研究则再次凸显了中国剩余定理在同态加密场景中的优势，为数据隐私和完整性保护提供了新的思路。

以上研究尽管在数据加密、聚合计算以及验证机制等方面取得了显著进展，但普遍存在局限：一是多数方案仅关注数据聚合而缺乏对于多维度类型数据的细粒度处理；二是数据类型多样性带来的计算负担以及特定数据类型的隐私需求未被满足；三是在边缘计算场景下，终端设备与边缘节点的协同安全机制仍有优化空间。

因此，亟须一种支持类型验证与筛选的多维密态数据聚合方案。为此，本文基于改进的Paillier加密系统和类型验证密钥的新型数据聚合方案，通过设计数据类型验证机制实现了密文状态下的选择性聚合，采用边缘层聚合签名技术降低了终端负载，同时引入双线性对和秘密共享实现更高的安全性。本文的研究工作主要包括以下几个方面的贡献。

1) 基于改进的Paillier加密算法，对数据进行加密处理，同时提出数据类型密文生成和验证密钥设计方法，并基于双线性对技术设计一种多类型数据选择性验证机制。

2) 设计多维数据选择性聚合算法，引入超递增序列实现多维数据的联合聚合，并使用Shamir秘密共享方案进行聚合签名实现对聚合数据的完整性验证。

3) 安全性分析和实验验证表明，本文方案在增强数据隐私保护以及提高多维数据选择性聚合效率等方面都具有很好的表现。

1　预备知识

1.1　Paillier密码系统

Paillier加密算法是一种公钥加密方案[20],实现了加法同态和部分乘法同态操作。同态特征使用户能够对加密数据进行数学或有理运算。本文在传统Paillier加密算法的基础上进行一定改进，以支持加密数据类型的选择。具体如下。

1) 密钥生成：选择2个大素数p'和q'，计算$p = 2p' + 1$，$q = 2q' + 1$，$N = pq$，$g = -a^{2N} \bmod N^2$，$a \in Z_{N^2}^*$，g是阶为$\dfrac{(p-1)(q-1)}{2}$的一个生成元。选择$\mathrm{sk} = \rho$作为系统私钥，且满足$\rho \in \left[1, \dfrac{N}{4}\right]$。计算$h = g^{\rho} \bmod N^2$，定义$\mathrm{pk} = (N,g,h)$作为系统公钥。

2) 加密：对于明文$m \in Z_N$，任意选择一个随机数$r \in \left[1, \dfrac{N}{4}\right]$，使用系统公钥pk将其加密为密文$C = [m]_{\mathrm{pk}} = \{D_{i1}, D_{i2}\}$，该密文由两部分组成，其中

$$D_{i1} = g^r \bmod N^2 \tag{1}$$

$$D_{i2} = h^r(1 + mN) \bmod N^2 \tag{2}$$

3) 解密：解密算法$D_{\mathrm{sk}}(\cdot)$可以通过输入私钥$\mathrm{sk} = \rho$，从而恢复明文$m = L\left(\dfrac{D_{i2}}{D_{i1}^{\rho}} \bmod N^2\right)$。其中，函数$L(x)$表示为

$$L(x) = \frac{x - 1 \bmod N^2}{N} \tag{3}$$

4) 同态性质：在纯化的同态密码系统中，输入2个加密的整数$[n_1]_{\mathrm{pk}}$和$[n_2]_{\mathrm{pk}}$，使用相同公钥pk对其加密，具有以下同态属性，即

$$D_{\mathrm{sk}}\left([n_1]_{\mathrm{pk}} \cdot [n_2]_{\mathrm{pk}}\right) \equiv n_1 + n_2 \bmod N \tag{4}$$

$$D_{\mathrm{sk}}\left([n_1]_{\mathrm{pk}}^{Y}\right) \equiv Yn_1 \bmod N \tag{5}$$

1.2　双线性对技术

设$\mathbb{G}$、$\mathbb{G}_{\mathbb{T}}$是具有相同素数阶p和生成元g的2个群。本文将$\mathbb{G}$、$\mathbb{G}_{\mathbb{T}}$视为循环群。假设离散对数问题（DLP, discrete logarithm problem）在$\mathbb{G}$和$\mathbb{G}_{\mathbb{T}}$中都是困难的。映射$e:\mathbb{G} \times \mathbb{G} \to \mathbb{G}_{\mathbb{T}}$满足以下性质时被称为双线性映射[21]。

1) 双线性：$\forall g_1,g_2 \in \mathbb{G}, a,b \in \mathbb{Z}_q^*$，有$e(g_1^a, g_2^b) = e(g_1,g_2)^{ab}$；$\forall a,b,y \in \mathbb{G}$，有$e(a \cdot b, y) = e(a,y) \cdot e(b,y)$；$\forall a,b,y \in \mathbb{G}$，有$e(y, a \cdot b) = e(y,a) \cdot e(y,b)$。

2) 非退化性：$\exists g_1,g_2$，满足$e(g_1,g_2) \neq 1$。

3) 可计算性：对于$\forall g_1,g_2 \in \mathbb{G}$，都存在一个有效的算法$e(g_1,g_2)$。

1.3　CDH困难假设

CDH困难假设[22]（computational Diffie-Hellman hardness assumption）是指对于任意元素$g, g^a, g^b \in \mathbb{G}$和一个素数阶为$p$的循环群$\mathbb{G}$，如果$g$是群$\mathbb{G}$的生成元，且$a,b \in \{0,\cdots,q-1\}$，则任何算法以不可忽略的优势计算$g^{ab}$的值被认为是计算不可行的。

1.4　中国剩余定理

中国剩余定理[23]（CRT, Chinese remainder theorem）是一个关于同余方程组的定理，可以唯一地求解任何一对具有相对素数模的同余。若一组整数两两互质，则对任意的整数$a_1,a_2,\cdots,a_n$，同余方程组$x \equiv a_i \bmod m_i$具有模$M = m_1 \times m_2 \times \cdots \times m_n$的唯一解，即

$$x \equiv \sum_{i=1}^{n} a_i M_i t_i \bmod M \tag{6}$$

其中，$M_i = \dfrac{M}{m_i}$，且$M_i t_i \equiv 1 \bmod m_i$。

1.5　Shamir秘密共享方案

Shamir秘密共享方案[24]利用拉格朗日插值法将一个秘密S分为多个碎片即秘密份额，并将其分发给N个不同的用户，只有满足阈值才能成功解密出秘密值。Shamir秘密共享主要包括秘密共享和秘密恢复2个算法。

1) 秘密共享：假设现有秘密值S与n个用户进行分享,首先确定一个$T-1$次多项式为

$$E(x) = S + b_1 x + b_2 x^2 + \cdots + b_{T-1} x^{T-1} \tag{7}$$

其中，多项式系数$b_1,b_2,\cdots,b_{T-1} \in Z_q$，$T < n$。计算$S_j = E(x_j)$并将其分发给第$j$个用户。

2) 秘密恢复:在恢复秘密S时,至少需要T个成员参与并用各自的子秘密一起构建拉格朗日插值公式才可以恢复秘密。假设T个成员的子秘密分别为$(x_1,S_1),(x_2,S_2),\cdots,(x_T,S_T)$,按照重构公式恢复秘密值。当$x = 0$时，秘密值被恢复。

2　系统模型

2.1　系统架构

本文方案是一种面向物联网应用场景的数据可选择性聚合传输方案，包括4类相关实体：可信权威（TA, trust authority,）中心、底层物联网设备、网络边缘服务器及中心服务器。系统架构如图1所示，相关实体的具体工作职责如下。

1) 可信权威中心负责系统初始化、参数生成以及系统公钥和私钥分发，并为每个数据类型生成唯一的验证密钥。TA与所有其他实体通过安全信道通信。

2) 底层物联网设备是数据采集器，首要职责是采集原始传感数据，并利用TA分发的密钥对数据进行加密和签名，生成标准的传输报文，并将其发送至其连接的边缘服务器。

3) 网络边缘服务器承担核心的数据筛选与聚合任务，接收来自大量物联网设备传输的数据，并根据中心服务器的需求使用特定的验证密钥对报文进行筛选，只聚合特定类型的密文和签名。筛选、聚合均在密文状态下完成，边缘服务器无法解密任何原始数据。最终将聚合密文和签名发送至中心服务器进行解密、验证。

4) 中心服务器是最终的数据处理端，接收来自边缘服务器的聚合结果，执行最终的解密操作以获取明文聚合结果，并验证聚合签名的合法性，以确保数据在传输与聚合过程中的完整性。

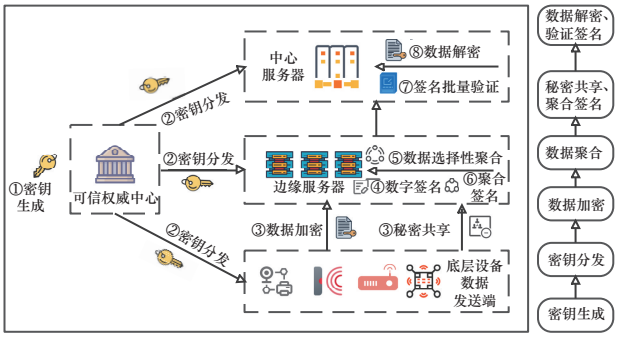

图1　系统架构

2.2　设计目标

1) 数据隐私保护：数据传输过程中必须保证数据隐私性和安全性，因此原始数据需加密处理。

2) 数据选择性聚合：密文数据需按类型过滤聚合，且保证在此过程中不存在任何安全漏洞。

3) 数据聚合签名：加密数据的同时需各物联网设备通过秘密共享方案恢复公共私钥，对数据签名并聚合。

4) 数据解密及验证：中心服务器接收到聚合数据后，验证数据完整性并使用私钥解密，验证数据的正确性。

5) 安全性方面：能够有效抵抗常见攻击。具体而言，终端侧通过改进的Paillier加密系统确保数据在传输过程中不泄露，从而抵抗窃听攻击；边缘层结合类型验证密钥与聚合签名机制，能够防止非法数据混入并避免伪造或篡改攻击；中心服务器在解密与验证阶段进一步保证聚合结果的完整性与可靠性。

2.3　形式化定义

在本节给出本文方案包含算法的形式化定义。本文方案由6个多项式时间算法组成：系统密钥生成（CryptoSysKeyGen）、密钥分发（KeyDist）、秘密共享（SecretSplitter）、数据加密（DataEnc）、数据选择性聚合（SelectiveDataAggr）和数据解密（DataEncryptor）。

1) $\mathrm{CryptoSysKeyGen}(p)\rightarrow(\mathrm{ParamSet})$: 由可信权威中心执行。算法要求输入一个安全参数$\lambda$，可信权威中心输出一组系统公共参数：$\mathrm{ParamSet}=\{g,\mathbb{G},\mathbb{G}_{\mathbb{T}},\xi,e,\varepsilon,\varepsilon_1,\varepsilon_2,N,S,H(\cdot),f(m)\}$。

2) $\mathrm{KeyDist}\left(S,\{T_1,\cdots,T_i\}\right)\rightarrow(\mathrm{PK}_R,\mathrm{SK}_{R/\mathrm{IoT}_i},\mathrm{TV}_i,S^i)$：由可信权威中心算法要求输入大素数$S$作为中心服务器的第$i$个数据类型，可信权威中心输出中心服务器的公钥$\mathrm{PK}_R$，私钥$\mathrm{SK}_R$，物联网设备的私钥$\mathrm{SK}_{\mathrm{IoT}_i}$以及第$i$个加密数据类型的验证密钥$\mathrm{TV}_i$，可信权威中心将以上数据安全发送给相应实体。

3) $\mathrm{SecretSplitter}\left(\{b_1,\cdots,b_{T-1}\},\{x_1,\cdots,x_j\}\right)\rightarrow\left(\mathrm{SK}_{\mathrm{IoT}}\right)$：由可信权威中心执行。算法要求输入随机生成的多项式系数$\{b_1,\cdots,b_{T-1}\}$，其中T是参与秘密恢复的数据发送端设备的门限值，然后由可信权威中心为参与秘密共享的设备生成秘密值$\{x_1,\cdots,x_j\}$并将其分发给设备。参与秘密共享的设备收到秘密值后进行秘密恢复，得出数据发送端设备的共享私钥$\left(\mathrm{SK}_S\right)$。

4) $\mathrm{DataEnc}\left(\mathrm{SK}_{\mathrm{IoT}_i},\mathrm{PK}_R,T_i,m_i\right)\rightarrow\left(c_i,\sigma_i,\mathrm{TS}_i\right)$：由

底层物联网设备执行。算法要求输入物联网设备的私钥$\mathrm{SK}_{\mathrm{IoT}_i}$，中心服务器的公钥$\mathrm{PK}_R$，所需数据类型$T_i$以及明文消息$m_i$。底层物联网设备输出密文$c_i$，签名$\sigma_i$以及加密数据类型的选择密钥$\mathrm{TS}_i$。

5) $\mathrm{SelectiveDataAggr}\left(T_i, \mathrm{TV}_i\right) \rightarrow \left(c_{\mathrm{aggr}}, \sigma_{\mathrm{aggr}}\right)$：由边缘服务器执行，算法要求输入所需的数据类型$T_i$和不同数据类型的验证密钥$\mathrm{TV}_i$。

6) $\mathrm{DataEncryptor}\left(\mathrm{SK}_R\right) \rightarrow (m)$：由中心服务器执行。算法要求输入私钥$\mathrm{SK}_R$，输出为各数据类型聚合结果$m = \sum m_i$。

2.4　敌手模型

可信权威中心始终是一个完全可信的实体，它与其他实体之间的通信在安全信道中进行。

物联网设备被视为半诚实实体，它会遵循数据采集和上报协议，但可能被敌手腐蚀以获取其内部状态，进而试图推测其他设备的隐私信息。

边缘服务器被视为半诚实实体，它会严格遵循筛选与聚合协议，但可能被敌手腐蚀，即敌手可通过窥探流经的密文与签名，试图推测原始数据。

中心服务器假设为诚实可信的实体。

在本文方案中引入了一个半诚实敌手$\mathcal{A}$。$\mathcal{A}$的目标是通过以下方式试图推断物联网设备的原始数据和边缘服务器的聚合结果。

1) 敌手$\mathcal{A}$可能会窃听数据发送过程的所有通信以获取加密数据。

2) 敌手$\mathcal{A}$可能会腐蚀一个或多个物联网设备（不包括被挑战的物联网设备），以获取其内部状态。

3) 敌手$\mathcal{A}$可能会腐蚀被挑战的边缘服务器，以获取其接收到的聚合密文，推断所有聚合密文的原始值。

4) 敌手$\mathcal{A}$可能会同时腐蚀物联网设备和边缘服务器，以获取其内部状态进行关联分析。

本文方案的核心安全假设是：敌手无法通过物理手段攻破物联网设备并获取$\mathrm{SK}_{\mathrm{IoT}}$。本文方案的安全目标均建立在$\mathrm{SK}_{\mathrm{IoT}}$未被泄露的基础之上。

3　详细设计

本节详细介绍了数据传输分类的过程，主要分为系统密钥生成、密钥分发、数据加密、秘密共享、边缘层数据选择性聚合以及中心服务器解密6个部分。系统参数如表1所示。

表1　　系统参数

参数	含义
p,q	大素数
$p',q',\mu,m_1,m_2,m_3,m_4$	$\mathbb{Z}_N^*$中的素数
a	$\mathbb{Z}_{N^2}^*$中的随机数
S	超递增序列
g,ε	循环群的生成元
k_1,k_2	$\mathbb{Z}_N^*$中的随机数
$\mathbb{G},\mathbb{G}_{\mathbb{T}}$	循环群
e	双线性映射
$H(\cdot)$	哈希函数
ε_i	循环群$\mathbb{G}$中的元素
M	m_i的乘积
$f(m)$	中国剩余定理的系数
SK_R	中心服务器私钥
PK_R	中心服务器公钥
T_i	第i类数据类型
ω_i,r_1,r_2	$\mathbb{Z}_\mu$中的随机数
TV_i	第i类数据类型的验证密钥
$\mathrm{TV}_{i1/2/3/4/5/6}$	第i类数据类型的验证子密钥
$\mathrm{SK}_{\mathrm{IoT}}$	物联网设备的公共私钥
TS_i	第i类数据类型的选择密钥
$\mathrm{TS}_{i1/2/3/4/5/6}$	第i类数据类型的选择子密钥
c_i	第i个类型数据的密文
σ_i	第i个类型数据的聚合签名
c_{aggr}	第i个类型数据的聚合密文
σ_{aggr}	第i个类型数据的签名
IoT_i	第i个物联网设备
edge_i	第i个边缘服务器
m_i	第i个类型的数据明文
TS_p	当前时段时间戳
$r_i',\hat{r}_i$	$\left[1,\frac{N}{4}\right]$中的随机数

3.1　系统密钥生成

1) 以安全参数λ作为输入，可信权威中心首先随机选择2个大素数$p',q' \in \mathbb{Z}_N^*$，计算$p = 2p' + 1$，$q = 2q' + 1$，$N = pq$。同时，可信权威中心选择随机

数$a \in \mathbb{Z}_{N^2}^*$，计算$g = -a^{2N} \bmod N^2$。最后，可信权威中心选择1个大素数$S \in \left[1, \frac{N}{4}\right]$构造1个超递增序列$\left(1, S, S^2, \cdots, S^i\right)$。

2) 可信权威中心随机选择素数$m_1, m_2, m_3, m_4 \in \mathbb{Z}_N^*$作为中国剩余定理的模数，并计算它们的乘积$M = \prod m_i$以及对应的系数$f\left(m_i\right) = \frac{M}{m_i}$。

3)可信权威中心选择2个具有相同素数阶ξ的循环群$\mathbb{G}$和$\mathbb{G}_{\mathbb{T}}$，其中ξ必须满足$M \mid \xi - 1$，选取$\mathbb{G}$的生成元$\varepsilon \in \mathbb{Z}^+$，使双线性映射成立$e: \mathbb{G} \times \mathbb{G} \to \mathbb{G}_{\mathbb{T}}$。

4) 可信权威中心选择哈希函数$H(\cdot): \{0,1\}^* \times \mathbb{G} \times \mathbb{G} \to \mathbb{Z}_N^*$作为强抗碰撞的哈希函数，随机选择2个整数$k_1, k_2 \in \mathbb{Z}_N$，并计算$\varepsilon_1 = \varepsilon^{k_1}, \varepsilon_2 = \varepsilon^{k_2}$。

5) 最后，可信权威中心公布公共参数$\left(g, \mathbb{G}, \mathbb{G}_{\mathbb{T}}, \xi, e, \varepsilon, \varepsilon_1, \varepsilon_2, N, S, H(\cdot), f(m)\right)$。

3.2 密钥分发

1) 可信权威中心计算$a_i = k_1 \bmod m_i$并选择1个e_i满足$f\left(m_i\right) \cdot e_i = 1 \bmod m_i$。

2) 可信权威中心选择$\mathrm{SK}_R = \tau \in \frac{\lambda\left(N^2\right)}{8}$作为中心服务器的私钥，并为其生成公钥$\mathrm{PK}_R = g^{\tau}$。

3) 可信权威中心在安全通道中将$\left(\mathrm{SK}_R, \mathrm{PK}_R\right)$传输到中心服务器。然后中心服务器公开公钥$\mathrm{PK}_R$。

4) 假设中心服务器可以接收i种数据类型，表示为$\left\{T_1, \cdots, T_i\right\}$。中心服务器随机选择$\omega_i \in \mathbb{Z}_\mu$，计算出第$i$个数据类型的验证密钥$\mathrm{TV}_i = \left\{\mathrm{TV}_{i1}, \mathrm{TV}_{i2}, \mathrm{TV}_{i3}, \mathrm{TV}_{i4}, \mathrm{TV}_{i5}, \mathrm{TV}_{i6}\right\}$，其中$\mathrm{TV}_{i1} = \varepsilon_2^{\omega_i}$，$\mathrm{TV}_{i2} = H\left(T_i\right)^{\omega_i}$，$\mathrm{TV}_{i3} = \varepsilon_2^{e_2 \cdot a_2 \cdot \omega_i}$，$\mathrm{TV}_{i4} = \varepsilon_2^{f\left(m_1\right) \cdot e_1 \cdot a_1 \cdot \omega_i}$，$\mathrm{TV}_{i5} = \varepsilon^{f\left(m_3\right) \cdot e_3}$，$\mathrm{TV}_{i6} = \varepsilon^{f\left(m_4\right) \cdot e_4 \cdot a_4}$。

5) 中心服务器将需要聚合的数据类型的验证密钥$\mathrm{TV}_i = \left\{\mathrm{TV}_{i1}, \mathrm{TV}_{i2}, \mathrm{TV}_{i3}, \mathrm{TV}_{i4}, \mathrm{TV}_{i5}, \mathrm{TV}_{i6}\right\}$和超递增序列$S$上传到第$i$个边缘节点$\mathrm{edge}_i$进行数据选择和过滤。

3.3 秘密共享

1) 对于每个参与的物联网设备，可信权威中心随机生成多项式系数$\left\{b_1, \cdots, b_{T-1}\right\}$，以及参与秘密共享的设备秘密值$\left\{x_1, \cdots, x_j\right\}$。其中，$T$是参与秘密恢复的数据发送端设备的门限值。TA确定$T-1$次多项式$E(x) = s + b_1 x + b_2 x^2 + \cdots + b_{T-1} x^{T-1}$后计算出$S_j = E\left(x_j\right)$，并将秘密值和$S_j$共同分发给相应数据发送端设备。

2) 物联网设备收到秘密值和S_j后，进行秘密恢复，其中参与秘密恢复的设备数量至少为T，并且T个设备的子秘密分别为$\left(x_1, S_1\right), \left(x_2, S_2\right), \cdots, \left(x_T, S_T\right)$。按照式(8)进行秘密值恢复，即

$$E(x) = \sum_{i=1}^{T} S_i \prod_{\substack{j=1 \\ j \neq i}}^{T} \frac{x - x_j}{x_i - x_j} \tag{8}$$

当$x = 0$时，$E(0) = s$，即底层物联网设备的共享私钥$\mathrm{SK}_{\mathrm{IoT}} = s$。计算对应公钥$\mathrm{PK}_s = \varepsilon_2^s$后，将该公钥在安全通道中分发给所有物联网设备。

3.4 数据加密

1) 物联网设备选取$r_1, r_2 \in Z_\mu$，计算第i个数据类型的选择密钥$\mathrm{TS}_i = \{\mathrm{TS}_{i1}, \mathrm{TS}_{i2}, \mathrm{TS}_{i3}, \mathrm{TS}_{i4}, \mathrm{TS}_{i5}, \mathrm{TS}_{i6}\}$，其中$\mathrm{TS}_{i1} = \varepsilon_1^{r_1 + r_2} \cdot H\left(T_i \| \mathrm{ID}_i\right)^{r_2}$，$\mathrm{TS}_{i2} = \varepsilon_2^{r_2}$，$\mathrm{TS}_{i3} = \varepsilon^{f\left(m_2\right) \cdot r_1}$，$\mathrm{TS}_{i4} = \varepsilon^{r_1}, \mathrm{TS}_{i5} = \varepsilon_1^{r_2 \cdot a_3 \cdot \omega_i}, \mathrm{TS}_{i6} = \varepsilon_1^{r_2 \cdot \omega_i}$。

2) 物联网设备选择2个随机数$r_i', \hat{r}_i \in \left[1, \frac{N}{4}\right]$对数据$m_i$进行加密，表示为

$$c_i = \left(c_{i1}, c_{i2}\right) = \left(g^{r_i'}, \mathrm{PK}_R^{r_i'}\left(1 + m_i \cdot N\right) \bmod N^2\right) \tag{9}$$

$$\sigma_i = \left(\sigma_{i1}, \sigma_{i2}\right) = \left(H\left(\mathrm{TS}_p\right)^{\hat{r}_i} \cdot \varepsilon_1^{m_i \mathrm{SK}_{\mathrm{IoT}}}, \varepsilon_2^{\hat{r}_i}\right) \tag{10}$$

3) 物联网设备向边缘节点edge_i广播$(c_i, \mathrm{TS}_i, \sigma_i, \mathrm{TS}_p)$。

3.5 数据选择性聚合

1) 边缘节点edge_i需要区分接收到的数据类型T_i是否为预期数据类型，因此edge_i进行计算为

$$\begin{aligned} & e\left(\mathrm{TS}_{i1}, \mathrm{TV}_{i1}\right) = \\ & e\left(\varepsilon_1^{r_1 + r_2} \cdot H\left(T_i\right)^{r_2}, \varepsilon_2^{\omega_i}\right) = \\ & e\left(\varepsilon_1^{r_1}, \varepsilon_2^{\omega_i}\right) \cdot e\left(\varepsilon_1^{r_2}, \varepsilon_2^{\omega_i}\right) \cdot e\left(H\left(T_i\right)^{r_2}, \varepsilon_2^{\omega_i}\right) = \\ & e\left(\varepsilon_1, \varepsilon_2\right)^{r_1 \omega_i} \cdot e\left(\varepsilon_1, \varepsilon_2\right)^{r_2 \omega_i} \cdot e\left(H\left(T_i\right)^{r_2}, \varepsilon_2^{\omega_i}\right) \end{aligned} \tag{11}$$

$$e\left(\mathrm{TS}_{i2}, \mathrm{TV}_{i2}\right) = e\left(\varepsilon_2^{r_2}, H\left(T_i\right)^{\omega_i}\right) \tag{12}$$

$$e\left(\mathrm{TS}_{i3},\mathrm{TV}_{i3}\right)=e\left(\varepsilon^{f\left(m_2\right)\cdot r_1},\varepsilon_2^{e_2\cdot a_2\cdot\omega_i}\right)=$$
$$e\left(\varepsilon,\varepsilon_2\right)^{r_1\cdot\omega_i\cdot f\left(m_2\right)\cdot e_2\cdot a_2} \tag{13}$$

$$e\left(\mathrm{TS}_{i4},\mathrm{TV}_{i4}\right)=e\left(\varepsilon^{r_1},\varepsilon_2^{f\left(m_1\right)\cdot e_1\cdot a_1\cdot\omega_i}\right)=$$
$$e\left(\varepsilon,\varepsilon_2\right)^{r_1\cdot\omega_i\cdot f\left(m_1\right)\cdot e_1\cdot a_1} \tag{14}$$

$$e\left(\mathrm{TS}_{i5},\mathrm{TV}_{i5}\right)=e\left(\varepsilon_1^{r_2\cdot a_3\cdot\omega_i},\varepsilon^{f\left(m_3\right)\cdot e_3}\right)=$$
$$e\left(\varepsilon_1,\varepsilon\right)^{r_2\cdot\omega_i\cdot f\left(m_3\right)\cdot e_3\cdot a_3} \tag{15}$$

$$e\left(\mathrm{TS}_{i6},\mathrm{TV}_{i6}\right)=e\left(\varepsilon_1^{r_2\cdot\omega_i},\varepsilon^{f\left(m_4\right)\cdot e_4\cdot a_4}\right)=$$
$$e\left(\varepsilon_1,\varepsilon\right)^{r_2\cdot\omega_i\cdot f\left(m_4\right)\cdot e_4\cdot a_4} \tag{16}$$

2) 边缘节点 edge_i 需要验证等式

$$e\left(\mathrm{TS}_{i1},\mathrm{TV}_{i1}\right)=e\left(\mathrm{TS}_{i2},\mathrm{TV}_{i2}\right)\cdot e\left(\mathrm{TS}_{i3},\mathrm{TV}_{i3}\right)\cdot e\left(\mathrm{TS}_{i4},\mathrm{TV}_{i4}\right)\cdot e\left(\mathrm{TS}_{i5},\mathrm{TV}_{i5}\right)\cdot e\left(\mathrm{TS}_{i6},\mathrm{TV}_{i6}\right) \tag{17}$$

如果等式不成立，则加密数据被丢弃。等式验证过程如下。

$$e\left(\mathrm{TS}_{i2},\mathrm{TV}_{i2}\right)\cdot e\left(\mathrm{TS}_{i3},\mathrm{TV}_{i3}\right)\cdot e\left(\mathrm{TS}_{i4},\mathrm{TV}_{i4}\right)\cdot e\left(\mathrm{TS}_{i5},\mathrm{TV}_{i5}\right)\cdot e\left(\mathrm{TS}_{i6},\mathrm{TV}_{i6}\right)=$$
$$e\left(\varepsilon_2^{r_2},H\left(T_i\right)^{\omega_i}\right)\cdot e\left(\varepsilon,\varepsilon_2\right)^{r_1\omega_i f\left(m_2\right)\cdot e_2\cdot a_2}\cdot e\left(\varepsilon,\varepsilon_2\right)^{r_1\omega_i f\left(m_1\right)\cdot e_1\cdot a_1}\cdot e\left(\varepsilon_1,\varepsilon\right)^{r_2\omega_i f\left(m_3\right)\cdot e_3\cdot a_3}\cdot e\left(\varepsilon_1,\varepsilon\right)^{r_2\omega_i f\left(m_4\right)\cdot e_4\cdot a_4}=$$
$$e\left(\varepsilon_2^{r_2},H\left(T_i\right)^{\omega_i}\right)\cdot e\left(\varepsilon,\varepsilon_2\right)^{r_1\omega_i\left(f\left(m_2\right)\cdot e_2\cdot a_2+f\left(m_1\right)\cdot e_1\cdot a_1\right)}\cdot e\left(\varepsilon_1,\varepsilon\right)^{r_2\omega_i\left(f\left(m_3\right)\cdot e_3\cdot a_3+f\left(m_4\right)\cdot e_4\cdot a_4\right)}=$$
$$e\left(\varepsilon_2^{r_2},H\left(T_i\right)^{\omega_i}\right)\cdot e\left(\varepsilon,\varepsilon_2\right)^{k_1r_1\omega_i}\cdot e\left(\varepsilon_1,\varepsilon\right)^{k_2r_2\omega_i}=$$
$$e\left(\varepsilon_2^{r_2},H\left(T_i\right)^{\omega_i}\right)\cdot e\left(\varepsilon^{k_1},\varepsilon_2\right)^{r_1\omega_i}\cdot e\left(\varepsilon_1,\varepsilon^{k_2}\right)^{r_2\omega_i}=$$
$$e\left(\varepsilon_2^{r_2},H\left(T_i\right)^{\omega_i}\right)\cdot e\left(\varepsilon_1,\varepsilon_2\right)^{\left(r_1+r_2\right)\omega_i}=$$
$$e\left(TS_{i1},TV_{i1}\right) \tag{18}$$

如 3.1 节所述，由于 ξ 满足 $M|\xi-1$，根据有限群理论，对于群 $\mathbb{G}$ 中的任意元素 h，有 $h^M=1$，因此可确保由中国剩余定理求解产生的任意整数倍 M 在群指数运算中等于单位元，以此保证式(18)的正确性。

详细的数据类型选择算法如算法 1 所示。利用边缘层的验证密钥对接收到的数据进行快速类型过滤，并仅聚合所需类型。

算法 1　数据类型选择算法

输入　$\left(\mathrm{TV}_{i1},\mathrm{TV}_{i2},\mathrm{TV}_{i3},\mathrm{TV}_{i4},\mathrm{TV}_{i5},\mathrm{TV}_{i6}\right)$ 且 $i>0$，选择密钥 $\left(\mathrm{TS}_{i1},\mathrm{TS}_{i2},\mathrm{TS}_{i3},\mathrm{TS}_{i4},\mathrm{TS}_{i5},\mathrm{TS}_{i6}\right)$，且 $i=1,\cdots,\pi$

输出　$c_i,i>0$

① for i=1 to k do
② $c_i=\left(c_{i1}=0,c_{i2}=0\right)$
③ $\sigma_i=\left(\sigma_{i1}=0,\sigma_{i2}=0\right)$
④ for j=1 to π do
⑤ $\mathrm{label}_1=e\left(\mathrm{TS}_{j1},\mathrm{TV}_{i1}\right)$
⑥ $\mathrm{label}_2=e\left(\mathrm{TS}_{j2},\mathrm{TV}_{i2}\right)\cdot e\left(\mathrm{TS}_{j3},\mathrm{TV}_{i3}\right)$
⑦ $\mathrm{label}_3=e\left(\mathrm{TS}_{j4},\mathrm{TV}_{i4}\right)\cdot e\left(\mathrm{TS}_{j5},\mathrm{TV}_{i5}\right)\cdot e\left(\mathrm{TS}_{j6},\mathrm{TV}_{i6}\right)$
⑧ if $\mathrm{label}_1==\mathrm{label}_2\cdot\mathrm{label}_3$ then
⑨ $c_i=\left(c_{i1}\cdot c_{j1},c_{i2}.c_{j2}\right)$
⑩ $\sigma_i=\left(\sigma_{i1}\cdot\sigma_{j1},\sigma_{i2}.\sigma_{j2}\right)$
⑪ end if
⑫ end for
⑬ end for
⑭ return $c_i,i>0$

3) 边缘节点 edge_i 将来自多个物联网设备的相同类型的所有加密传感消息 c_i 聚合，详细过程如算法 2 所示。利用同态加密性质对密文和签名通过模乘操作聚合，最终分别输出密文聚合结果和签名聚合结果。

$$(c,\sigma)=\left(c_i,\sigma_i\right)_{i=1}^{k} \tag{19}$$

算法 2　数据聚合算法

输入　选定密文集合 $\left(c_i\right),i=1,\cdots,\pi$ 和签名集合 $\sigma_i=\left(\sigma_{i1},\sigma_{i2}\right),i=1,\cdots,\pi$

输出　$\left(c_i,\sigma_i\right)$

① for i=1 to size$\left(c_i\right)$ do
② $c_i=0,\sigma_i=0$
③ for j=1 to π do
④ $c_{ij}=\left(c_{ij1},c_{ij2}\right)$
⑤ $c_i=c_i\cdot c_{ij}$
⑥ $\sigma_{ij}=\left(\sigma_{ij1},\sigma_{ij2}\right)$

⑦ $\sigma_i = \sigma_i \cdot \sigma_{ij}$

⑧ end for

⑨ end for

⑩ return $\left(c_i,\sigma_i\right)$

4) 边缘节点 edge_i 利用超递增序列 S 聚合所有的加密消息 c_i: $c_{\text{aggr}} = \left(c_{\text{aggr}_1},c_{\text{aggr}_2}\right) = \left(\prod c_{i1}^{S^i},\prod c_{i2}^{S^i}\right)$。由于物联网设备通过秘密共享方案获得秘密值即公共私钥 SK_{IoT}, 因此签名可以聚合为 $\sigma_{\text{aggr}} = \left(\sigma_{\text{aggr}_1},\sigma_{\text{aggr}_2}\right) = \left(\prod\sigma_{i1},\prod\sigma_{i2}\right)$。

5) 边缘节点向中心服务器发送 c_{aggr} 和 σ_{aggr}。

3.6 数据解密

1) 中心服务器在接收到时段 T 内的聚合结果 c_{aggr} 和 σ_{aggr} 后，首先使用私钥 τ 解密数据类型为 T_i 的聚合结果为

$$\frac{c_{\text{aggr}_2}}{c_{\text{aggr}_1}^{\tau_i}} = 1 + \left(\sum m_i S^i\right) N \bmod N^2 \tag{20}$$

其中，m_i 表示数据类型为 T_i 的所有传输数据的汇总结果。

2) 通过执行 $L(x)$ 函数恢复结果为

$$L\left(\frac{c_{\text{aggr}_2}}{c_{\text{aggr}_1}^{\tau_i}}\right) = \sum m_i S^i \tag{21}$$

其中，$L(x) = \dfrac{x-1}{N}$，对于 $m = \sum m_i S^i$。恢复每种数据类型聚合结果的详细过程如算法 3 所示。通过利用超递增序列和模幂运算的性质，使用递归算法，将解密的明文聚合结果分解为单维数据明文聚合结果。

算法 3 恢复各数据类型的聚合结果算法

输入 $m = m_1 S + m_2 S^2 + \cdots + m_i S^i$ 和超递增序列 $\left(1,S,S^2,\cdots,S^i\right), m_i < S - 1$

输出 $\left(m_1,m_2,\cdots,m_i\right)$

① for i to 0 do

② $m_{i-1} = m \bmod S^i$

③ $m_i = \dfrac{m - m_{i-1}}{S^i}$

④ end for

⑤ return $\left(m_1,m_2,\cdots,m_i\right)$

4 正确性和安全性分析

4.1 正确性分析

1) 密文加解密的正确性证明过程如下。

$$\frac{c_{\text{aggr}_2}}{c_{\text{aggr}_1}^{\tau_i}} = \frac{\text{PK}_{R_i}^{\sum r_i'}\left(1 + \left(\sum m_i S^i\right) N \bmod N^2\right)}{g^{\tau_i \sum r_i'}} = \frac{g^{\tau_i \sum r_i'}\left(1 + \left(\sum m_i S^i\right) N \bmod N^2\right)}{g^{\tau_i \sum r_i'}} = 1 + \left(\sum m_i S^i\right) N \bmod N^2 \tag{22}$$

其中，m_i 表示数据类型为 T_i 的所有传输数据聚合值。通过执行 $L(x)$ 函数即可获取明文聚合结果为

$$L\left(\frac{c_{\text{aggr}_2}}{c_{\text{aggr}_1}^{\tau_i}}\right) = L\left(\left(1 + \left(\sum m_i S^i\right) N\right) \bmod N^2\right) = \frac{\left(1 + \left(\sum m_i S^i\right) N\right) - 1 \bmod N^2}{N} = \sum m_i S^i \tag{23}$$

2) 聚合签名验证的正确性证明过程如下。

$$\begin{aligned}
&e\left(\sigma_{\text{aggr}_1},\varepsilon_2\right) = \\
&e\left(\prod H\left(\text{TS}_p\right)^{\hat{r}_i} \cdot \varepsilon_1^{m_i \text{SK}_{\text{IoT}}},\varepsilon_2\right) = \\
&e\left(\prod H\left(\text{TS}_p\right)^{\hat{r}_i},\varepsilon_2\right) \cdot e\left(\varepsilon_1^{\sum m_i \text{SK}_{\text{IoT}}},\varepsilon_2\right) = \\
&e\left(\prod H\left(\text{TS}_p\right)^{\hat{r}_i},\varepsilon_2\right) \cdot e\left(\varepsilon_1^{\sum m_i s},\varepsilon_2\right) = \\
&e\left(\prod H\left(\text{TS}_p\right)^{\hat{r}_i},\varepsilon_2\right) \cdot e\left(\varepsilon_1^{\sum m_i},\varepsilon_2^s\right) = \\
&e\left(H\left(\text{TS}_p\right),\prod \varepsilon_2^{\hat{r}_i}\right) \cdot e\left(\varepsilon_1^{\sum m_i},\varepsilon_2^s\right) = \\
&e\left(H\left(\text{TS}_p\right),\sigma_{\text{aggr}_2}\right) \cdot e\left(\varepsilon_1^{\sum m_i},\varepsilon_2^s\right)
\end{aligned} \tag{24}$$

4.2 安全性定义

本文方案旨在半诚实敌手模型下实现以下安全属性。

1) 密文不可区分性：当加密数据从物联网设备上传到边缘服务器时，要求加密数据不应泄露任何关于其底层原始数据的信息。即使边缘服务器可以选择并聚合多个密文，最终的聚合结果也只能由中心服务器访问。

2) 签名隐私：当物联网设备向边缘服务器传输加密数据时，相应的签名也会附加。因此，要求签名不应泄露任何关于底层数据的信息。此外，即使边缘服务器可以选取并聚合多个签名，最终的聚合结果也不能泄露任何关于底层数据内容的信息。

3) 类型隐私：在设备数据传输过程中，加密类型不应泄露任何关于数据类型的敏感信息。类型隐私的定义与签名隐私相似。

方案采用基于模拟的安全范式来形式化上述安

全目标。通过比较真实协议执行视图与理想模拟视图的不可区分性来定义安全。

为形式化表述半诚实敌手模型下的安全性，引入一个在半诚实非勾结的对手存在时的基于模拟的安全模型如下。

假设D_a表示方案中的发送端物联网设备，E_a表示边缘服务器，$P\left(D_a,E_a\right)$表示协议执行期间的所有参与者，$\mathcal{A}_{D_a}$和$\mathcal{A}_{E_a}$分别表示为对D_a和E_a进行破坏的两类敌手。在真实环境中，参与实体D_a以x,y,z作为输入（w_x,w_y,w_z作为额外的辅助输入），E_a以接收到的w_1,w_2,w_3作为辅助输入。如果$\mathcal{H}\subset\mathcal{P}$是诚实实体的集合，当$P$是诚实的，即$P\in\mathcal{H}$，$\text{out}_P$表示实体$P$在协议执行期间的实际输出，当$P$被破坏成为敌手，即$P\in\mathcal{P}\backslash\mathcal{H}$，$\text{out}_{P^*}$表示$P$在协议执行期间的输出视图。

对每个参与实体$P^*\in\mathcal{P}$执行协议，当存在实体$\mathcal{P}=\!=\left(D_a,E_a\right)$和敌手$\mathcal{A}=\left(\mathcal{A}_{D_a},\mathcal{A}_{E_a}\right)$，协议输出$P^*$的部分视图为

$$\text{REAL}_{\Pi,\mathcal{A},\mathcal{P},w}^{P^*}\left(x,y,z\right)=\left\{\text{out}_P\right\}\cup\left\{\text{out}_P^*:P\in\mathcal{P}\backslash\mathcal{H}\right\}\quad(25)$$

在模拟环境中，假设一个理想函数f是负责与其他实体交互的受信实体。如果拥有者D_a向f提交x,y,z，当x,y,z其中一个为$\perp$时，f返回$\perp$；否则f返回$f\left(x,y,z\right)$到D_a。假设$\mathcal{H}\subset\mathcal{P}$为诚实实体的集合，如果$P$是诚实的，即$P\in\mathcal{H}$，$\text{out}_P$表示$f$返回给实体$P$的输出。当$P$被损坏时，即$P\in\mathcal{P}\backslash\mathcal{H}$，$\text{out}_{P^*}$表示$P$返回某个随机值的响应。对每个参与实体$P^*\in\mathcal{P}$执行基于$f$模拟的协议，当实体$\mathcal{P}=\!=\left(D_a,E_a\right)$和对应模拟器$\mathcal{S}\left(\mathcal{S}_{D_a},\mathcal{S}_{E_a}\right)$存在，协议输出$P^*$的部分视图如下。

$$\text{IDEAL}_{f,\mathcal{S},\mathcal{P},w}^{P^*}\left(x,y,z\right)=\left\{\text{out}_P\right\}\cup\left\{\text{out}_P^*:P\in\mathcal{P}\backslash\mathcal{H}\right\}\quad(26)$$

在真实环境中的协议Π可以被模拟环境中的理想函数f部分模拟时，协议Π被认为在非勾结的半诚实敌手模型中是安全的。

定义 1　假设f表示实体$\mathcal{P}=\!=\left(D_a,E_a\right)$之间交互的确定性函数，$\Pi$表示实体$\mathcal{P}=\!=\left(D_a,E_a\right)$之间执行的协议。$\mathcal{H}\subset\mathcal{P}$表示诚实实体的子集，如果$\mathcal{H}=\varnothing$，即每个实体$P\in\mathcal{P}$都是半诚实非勾结的实体。对于所有半诚实非勾结的实体$P\in\mathcal{P}$，协议Π可以被函数f安全地模拟，当且仅当对于所有的半诚实的非勾结敌手$\mathcal{A}=\left(\mathcal{A}_{D_a},\mathcal{A}_{E_a}\right)$，存在一个多项式时间转换的模拟器集合$S'=\left(S'_{D_a},S'_{E_a}\right)$，其中$S_{D_a}=S'_{D_a}\left(\mathcal{A}_{D_a}\right)$。对于所有的输入$x,y\in\mathbb{Z}_N$，辅助输入$z\in\mathbb{Z}_N$，式(27)成立，其中$\overset{c}{\approx}$表示计算不可区分性。

$$\text{REAL}_{\Pi,\mathcal{A},\mathcal{P},w}^{P^*}\left(x,y,z\right)\overset{c}{\approx}\text{IDEAL}_{f,\mathcal{S},\mathcal{P},w}^{P^*}\left(x,y,z\right)\quad(27)$$

4.3　安全性分析

定理 1　在半诚实非勾结的参与实体$\mathcal{A}=\left(\mathcal{A}_{D_a},\mathcal{A}_{E_a}\right)$存在的情况下，协议可以基于定义1安全地实现方案框架。

证明　假设$\mathcal{A}_{D_a}$是由S'_{D_a}模拟的，S'_{D_a}接收(x)作为输入，然后构造$(c)\leftarrow\text{DataEnc}(x)$，采用一个Paillier加密系统，将密文$(c)$返回给$\mathcal{A}_{D_a}$，并将$\mathcal{A}_{D_a}$的视图输出为$(c)$。由于$\mathcal{A}_{D_a}$不知道用于解密的相应私钥，因此无法恢复$(c)$，并且由于Paillier加密系统的语义安全性，真实环境中$\mathcal{A}_{D_a}$的视图和模拟环境中的输出是无法区分的。即使$\mathcal{A}_{D_a}$可以得到密文$\left(c=\left(g^{r'_i},\text{PK}_R^{r'_i}\left(1+m_i\cdot N\right)\bmod N^2\right)\right),\text{PK}_R=g^{\tau}$，但由于$\mathcal{A}_{D_a}$不知道$\text{PK}_R^{r'_i}$，因此无法从$(c)$中解密出$x$。根据$\left(g^{r'_i},\text{PK}_R=g^{\tau}\right)$计算出$\text{PK}_R^{r'_i}$类似于解决计算性CDH问题，而解决CDH假设在计算上是不可行的，因此保证了加密数据的隐私性。

S'_{D_a}接收(T)作为输入并模拟$\mathcal{A}_{D_a}$，然后构造$(\text{TS})\leftarrow\text{DataEnc}(T)$，将密文$(\text{TS})$返回给$\mathcal{A}_{D_a}$，并将$\mathcal{A}_{D_a}$的视图输出为$(\text{TS})$，对于某种数据类型密文$(\text{TS})$，其中，$\text{TS}_{i1}=\varepsilon_1^{r_1+r_2}\cdot H\left(T_i\right)^{r_2},\text{TS}_{i2}=\varepsilon_2^{r_2}$，$\text{TS}_{i3}=\varepsilon^{f\left(m_2\right)\cdot r_1},\text{TS}_{i4}=\varepsilon^{r_1},\text{TS}_{i5}=\varepsilon_1^{r_2\cdot a_3\cdot\omega_i},\text{TS}_{i6}=\varepsilon_1^{r_2\cdot\omega_i}$，$r_1,r_2$是随机数。在数据类型选择阶段，$\mathcal{A}_{D_a}$不知道$\varepsilon_1^{r_1}$，因此无法从$\left(\text{TS}_{i1},\text{TS}_{i2},\text{TS}_{i3},\text{TS}_{i4},\text{TS}_{i5},\text{TS}_{i6}\right)$中获取任何关于数据类型$(T)$的信息。真实环境中$\mathcal{A}_{D_a}$的视图和模拟环境中的输出是无法区分的。为了区分真实环境和模拟环境中的数据类型，$\mathcal{A}_{D_a}$可以随机构造一个密文(TS')，并检验式(28)是否成立，即

$$e\left(\frac{\text{TS}}{\frac{\text{TS}'}{\varepsilon_1^{r_1-r'_1}}},\varepsilon_2\right)=e\left(H\left(T\right),\varepsilon_2^{r_2-r'_2}\right)\quad(28)$$

从等式$\left(\varepsilon,\varepsilon_1=\varepsilon^{k_1},\varepsilon^{r_2-r_2'}\right)$中获得$\varepsilon_2^{r_2-r_2'}$等同于解决CDH问题。解决CDH假设在计算上是不可行的，因此保证了加密数据的隐私性。

S_{D_a}'接收(x,T)作为输入并模拟$\mathcal{A}_{D_a}$，然后构造$(\sigma)\leftarrow\mathrm{DataEnc}(x,T)$，将密文$(\sigma)$返回给$\mathcal{A}_{D_a}$，并将$\mathcal{A}_{D_a}$的视图输出为$(\sigma)$。通过以上证明，加密数据和数据类型的隐私得到保护，因此真实环境中$\mathcal{A}_{D_a}$的视图和模拟环境中的输出是无法区分的。

通过证明，很明显本文方案满足密文不可区分性、签名隐私性和类型隐私。

5　性能分析

本节将本文方案与其他4种安全数据聚合方案（即LVPDA[25]、VMEMDA[26]、PFDAM[27]和EEPPDA[28]）在通信和计算成本方面进行对比。

对于计算成本评估，首先计算每个阶段的加密操作数量，然后计算比较的总体成本。由于加法的计算成本小于双线性配对和其他操作，在这里省略其计算。实验环境是一台安装Windows 10操作系统的笔记本计算机，配有Intel(R) Core(TM) i5-8265U CPU (1.60 GHz)和8 GB RAM。评估过程基于JPBC库、JDK 1.8以及JNA等，基于Java代码验证所设计的算法。测量结果主要考虑一些代价昂贵的操作，包括模幂计算、双线性配对运算以及哈希操作运算等。

为保证实验结果的可重复性与统计显著性，每个实验配置均进行了30次独立运行，且每次运行的随机种子不同。主要操作时间开销如表2所示，列出了30次实验的平均时间开销、标准差与95%置信区间（基于t分布计算）。

表2　主要操作时间开销

操作类型	平均时间开销/ms	标准差	95%置信区间
$T_{\mathrm{EXP}_{\mathbb{Z}}}$	1.394	0.016	(1.389, 1.400)
$T_{\mathrm{EXP}_{\mathbb{G}}}$	0.041	0.015	(0.035, 0.047)
T_{BP}	0.033	0.020	(0.026, 0.041)
$T_{\mathrm{MUL}_{\mathbb{Z}}}$	0.218	0.076	(0.190, 0.247)
$T_{\mathrm{MUL}_{\mathbb{G}}}$	0.094	0.032	(0.082, 0.106)
T_H	0.249	0.404	(0.099, 0.400)

5.1　计算成本分析

由于系统密钥生成和分发只执行一次，因此仅从以下3个阶段对方案进行计算复杂度理论分析：主要考虑设备层数据加密、边缘层数据选择性聚合以及中心服务器数据解密和签名验证的计算成本。在设备层数据加密阶段，本文方案首先需要运行$6T_{\mathrm{EXP}_{\mathbb{G}}}$、$2T_{\mathrm{MUL}_{\mathbb{Z}}}$、$T_H$和$T_{\mathrm{EXP}_{\mathbb{Z}}}$生成数据类型密文即数据类型选择密钥$\mathrm{TS}_i=\{\mathrm{TS}_{i1},\mathrm{TS}_{i2},\mathrm{TS}_{i3},\mathrm{TS}_{i4},\mathrm{TS}_{i5},\mathrm{TS}_{i6}\}$。然后为数据密文和签名生成消耗$4T_{\mathrm{EXP}_{\mathbb{G}}}$、$3T_{\mathrm{MUL}_{\mathbb{Z}}}$、$T_H$和$T_{\mathrm{EXP}_{\mathbb{Z}}}$。因此，设备层数据加密的总计算成本为$10T_{\mathrm{EXP}_{\mathbb{G}}}+5T_{\mathrm{MUL}_{\mathbb{Z}}}+2T_H+2T_{\mathrm{EXP}_{\mathbb{Z}}}$。在边缘层数据选择性聚合阶段，本文方案需要执行$6nT_{\mathrm{BP}}$，计算出6个相对应的数据类型验证值$e(\mathrm{TS}_{i1},\mathrm{TV}_{i1})$，$e(\mathrm{TS}_{i2},\mathrm{TV}_{i2})$，$e(\mathrm{TS}_{i3},\mathrm{TV}_{i3})$，$e(\mathrm{TS}_{i4},\mathrm{TV}_{i4})$，$e(\mathrm{TS}_{i5},\mathrm{TV}_{i5})$，$e(\mathrm{TS}_{i6},\mathrm{TV}_{i6})$。然后，数据类型验证消耗$4nT_{\mathrm{MUL}_{\mathbb{G}}}$，密文聚合和签名聚合共消耗了$2nT_{\mathrm{EXP}_{\mathbb{G}}}$和$(4n-2)T_{\mathrm{MUL}_{\mathbb{G}}}$。在数据选择性聚合阶段的总计算成本为$2nT_{\mathrm{EXP}_{\mathbb{G}}}+(8n-2)T_{\mathrm{MUL}_{\mathbb{G}}}+6nT_{\mathrm{BP}}$。在中心服务器数据解密和签名验证阶段，本文方案需消耗$2T_{\mathrm{EXP}_{\mathbb{G}}}+2T_{\mathrm{MUL}_{\mathbb{G}}}+3T_{\mathrm{BP}}+T_{\mathrm{MUL}_{\mathbb{Z}}}+T_H$进行数据解密和签名验证。因此方案最终的总体计算成本为$(2n+12)T_{\mathrm{EXP}_{\mathbb{G}}}+6T_{\mathrm{MUL}_{\mathbb{Z}}}+8nT_{\mathrm{MUL}_{\mathbb{G}}}+2T_{\mathrm{EXP}_{\mathbb{Z}}}+(6n+3)T_{\mathrm{BP}}+3T_H$。本文方案以及LVPDA[25]、VME-MDA[26]、PFDAM[27]与EEPPDA[28]的计算成本对比如表3所示，方案功能对比如表4所示。

根据表2中提供的每个密码原语时间开销的测量结果，对本文方案以及LVPDA[25]、VME-MDA[26]、PFDAM[27]及EEPPDA[28]进行计算成本对比分析。5种方案在设备层加密阶段的设备层计算成本对比如图2所示。可以看出，与VMEMDA[26]方案相比，本文方案在数据加密过程中将1 000个物联网设备并发计算成本至少降低50%，较EEPPDA[28]方案降低约67%，虽然较LVPDA[25]和PFDAM[27]方案需要更多的计算成本，但本文方案支持更加复杂的不同类型数据加密。5种方案在边缘层数据聚合阶段的边缘层计算成本对比如图3所示。

本文方案在该过程中实现了最低的计算成本，其中，假设PFDAM[27]方案的最大聚合量$l=5$。5种方案在中心服务器数据解密和签名验证阶段的中心服务器计算成本对比如图4所示。由于边缘服务器分担了部分数据验证工作，因此在该阶段的计算成本也最小。

表3　　计算成本对比

方案	设备层	边缘层	中心服务器	总体计算成本
本文方案	$10T_{\mathrm{EXP_G}}+5T_{\mathrm{MUL_Z}}+2T_H+2T_{\mathrm{EXP_Z}}$	$2nT_{\mathrm{EXP_G}}+(8n-2)T_{\mathrm{MUL_G}}+6nT_{\mathrm{BP}}$	$2T_{\mathrm{EXP_G}}+2T_{\mathrm{MUL_G}}+3T_{\mathrm{BP}}+T_{\mathrm{MUL_Z}}+T_H$	$(2n+12)T_{\mathrm{EXP_G}}+6T_{\mathrm{MUL_Z}}+3T_H+8nT_{\mathrm{MUL_G}}+2T_{\mathrm{EXP_Z}}+(6l+3)T_{\mathrm{BP}}$
VMEMDA	$(3l+3)T_{\mathrm{MUL_Z}}+T_{\mathrm{MUL_G}}+3T_H+2T_{\mathrm{HH}}+2T_{\mathrm{EXP_Z}}+3T_{\mathrm{EXP_G}}$	$(3n-2)T_{MUL_Z}+(6n-4)T_{MUL_G}+T_{EXP_Z}+(2n+1)T_{EXP_G}+(n+1)T_H+(2n+1)T_{HH}+3T_{BP}$	$nT_{\mathrm{MUL_G}}+4T_{\mathrm{MUL_Z}}+nT_{\mathrm{EXP_G}}+4T_{\mathrm{EXP_Z}}+3T_H+3T_{\mathrm{BP}}+2T_{\mathrm{HH}}$	$(3n+3l+5)T_{\mathrm{MUL_Z}}+(7n-3)T_{\mathrm{MUL_G}}+7T_{\mathrm{EXP_Z}}+(3n+4)T_{\mathrm{EXP_G}}+(n+7)T_H+(2n+5)T_{\mathrm{HH}}+6T_{\mathrm{BP}}$
PFDAM	$T_{\mathrm{MUL_Z}}+T_{\mathrm{MUL_G}}+2T_H+2T_{\mathrm{HMAC}}+4T_{\mathrm{EXP_G}}$	$nT_{\mathrm{MUL_Z}}+n(l+2)T_{\mathrm{MUL_G}}+(n+1)T_{\mathrm{EXP_G}}+(n+1)T_H+nT_{\mathrm{HMAC}}+n(l+1)T_{\mathrm{BP}}$	$T_{\mathrm{MUL_Z}}+T_{\mathrm{EXP_G}}+2T_{\mathrm{BP}}$	$(n+2)T_{\mathrm{MUL_Z}}+n(l+3)T_{\mathrm{MUL_G}}+(n+6)T_{\mathrm{EXP_G}}+(n+3)T_H+(n+2)T_{\mathrm{HMAC}}+n(l+3)T_{\mathrm{BP}}$
LVPDA	$8T_{\mathrm{EXP_G}}+3T_{\mathrm{EXP_Z}}+4T_H+5T_{\mathrm{MUL_Z}}+2T_{\mathrm{MUL_G}}$	$(n+1)T_{\mathrm{MUL_G}}+(3n+1)T_H+(2n+2)T_{\mathrm{BP}}+T_{\mathrm{EXP_Z}}$	$2T_{\mathrm{EXP_G}}+T_{\mathrm{MUL_G}}+2T_{\mathrm{BP}}+2T_{\mathrm{MUL_Z}}+2T_H$	$10T_{\mathrm{EXP_G}}+7T_{\mathrm{MUL_Z}}+(n+2)T_{\mathrm{MUL_G}}+2nT_{\mathrm{BP}}+4T_{\mathrm{EXP_Z}}+(3n+7)T_H$
EEPPDA	$T_{\mathrm{EXP_G}}+2T_{\mathrm{EXP_Z}}+T_H+T_{\mathrm{MUL_G}}+T_{\mathrm{BP}}$	$(Z-1)T_{\mathrm{BP}}+2(Z+1)T_{\mathrm{MUL_G}}+ZT_{\mathrm{EXP_Z}}+T_{\mathrm{EXP_G}}$	$(n-1)T_{\mathrm{BP}}+2(n+1)T_{\mathrm{MUL_G}}+nT_{\mathrm{MUL_Z}}+2T_{\mathrm{EXP_G}}$	$(n+Z-1)T_{\mathrm{BP}}+(2n+2Z+5)T_{\mathrm{MUL_G}}+nT_{\mathrm{MUL_Z}}+4T_{\mathrm{EXP_G}}+(Z+2)T_{\mathrm{EXP_Z}}+T_H$

表4　　方案功能对比

方案	类型过滤	支持多维数据聚合	聚合签名/验证
本文方案	√	√	√
VMEMDA	×	√	√
PFDAM	√	√	√
LVPDA	×	×	√
EEPPDA	×	×	√

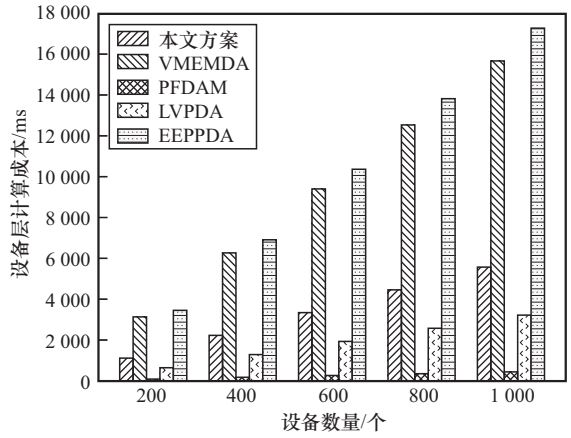

图2　设备层计算成本

上述3个阶段的总体计算成本对比如图5所示，随着物联网设备数量的增加，本文方案可保持最低的计算成本。

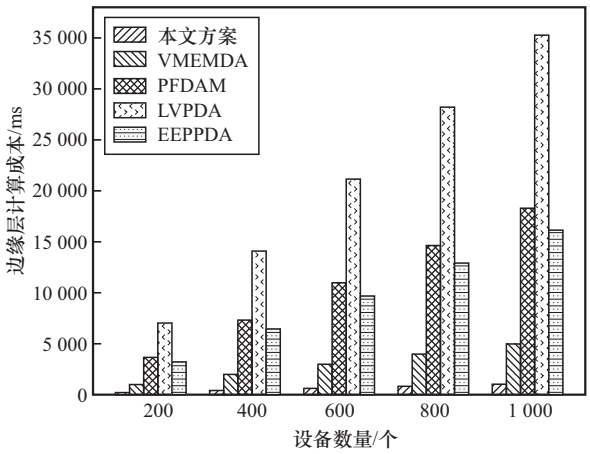

图3　边缘层计算成本

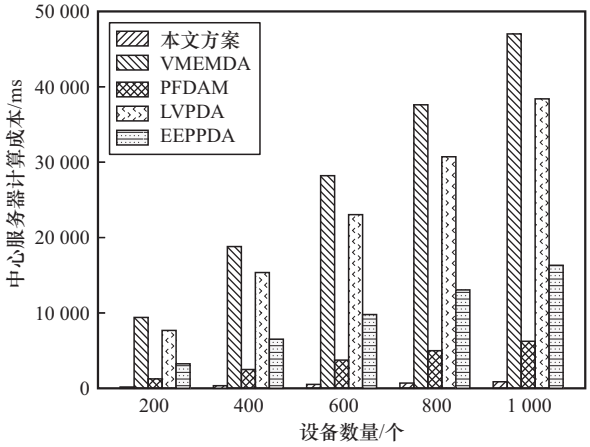

图4　中心服务器计算成本

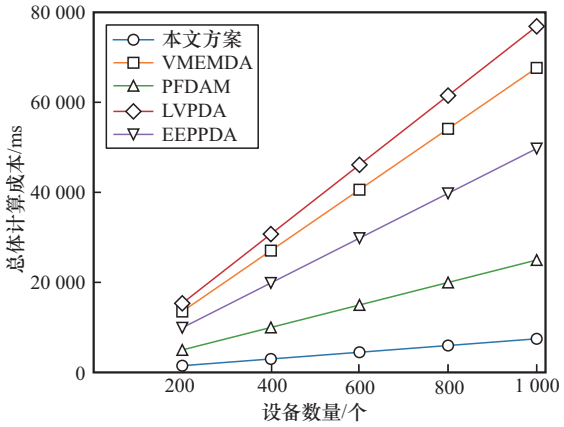

图5　总体计算成本

为更公平地体现不同方案的效率，排除因功能细节差异带来的影响，进一步引入“单位维度–设备聚合计算成本”这一归一化指标进行分析，其计算公式为 $\frac{\text{总计算时间}}{\text{数据维度} \times \text{设备数量}}$。单设备–单维度时间开销对比如图6所示，分别展示了所有方案的归一化结果。结果表明，即便在本文方案承担了更复杂的类型过滤功能的前提下，其处理单设备的效率依然显著优于LVPDA[25]、VMEMDA[26]方案及EEPPDA[27]方案；PFDAM[27]的单设备–单维度时间开销更低，但其物联网设备超过200个后，PFDAM[27]的时间开销将远超本文方案。由此证明本文方案的高效性与可扩展性。

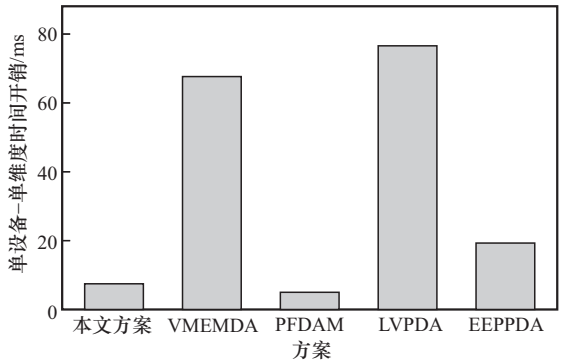

图6　单设备–单维度时间开销对比

本文方案的计算成本与设备数量n呈近似线性关系，从图5和图6可以看出，本文方案具有良好的可扩展性。基于已有的实验数据（$n \leqslant 1\,000$）对算法复杂度进行外推。根据其线性增长趋势，可以预测当设备数量增长至n=10 000时，总计算时间约为74 670 ms，这一性能在基于边缘计算的实际部署中是可接受的，如在智能电网或环境监测中，数据上报周期通常为15 min或更长。本文方案的计算成本仅占一个采集周期的8.3%，留有充足的时间进行数据传输、存储和后续分析。

为验证本文方案在多类型数据传输的物联网环境下的性能与可扩展性，在设备数量n=500时，令数据类型从l=2种增加至l=20种，测试总体时间开销。数据类型数量–总体时间开销如图7所示。

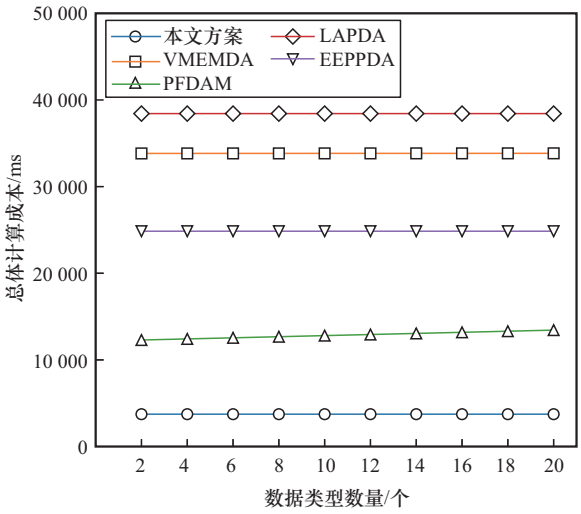

图7　数据类型数量–总体时间开销

随着数据类型数量的增加，总体时间开销仅呈现缓慢的线性增长且本文方案总体时间开销始终处于最低状态。表明了本文方案所设计类型验证密钥机制的高效性，且引入类型过滤功能所带来的额外开销是可接受的。

5.2　通信成本分析

通信成本计算主要考虑设备发送数据至边缘服务器和边缘服务器发送数据至中心服务器的阶段，第一个阶段需要$8|\mathbb{G}|+|\mathrm{ID}_i|$ bit，第二个阶段需要$4|\mathbb{G}|$ bit，因此通信总成本为$12|\mathbb{G}|+|\mathrm{ID}_i|$ bit。4个方案具体的通信成本对比如表5所示。

通信成本参数定义如下：Paillier密码系统参数N为1 024 bit，各设备ID位长32 bit，时间戳TS_p为64 bit，素数p位长320 bit，群$\mathbb{G}$元素位长为512 bit。本文方案与LVPDA[25]、VMEMDA[26]、PFDAM[27]及EEPPDA[28]总体通信成本对比如图8所示。

本文方案的总体通信成本为6176 bit，VMEMDA、PFDAM[27]和LVPDA[25]与EEPPDA[28]的总体通信成本分别为6 368 bit、8 736 bit、4 608 bit、4 288 bit，

表5　通信成本对比

方案	设备层/bit	边缘层/bit	总体通信成本/bit
本文方案	$8\|\mathbb{G}\|+\|\mathrm{ID}_i\|$	$4\|\mathbb{G}\|$	$12\|\mathbb{G}\|+\|\mathrm{ID}_i\|$
VMEMDA	$2\|\mathbb{G}\|+\|\mathrm{TS}_p\|+\|N\|$	$2\|\mathbb{G}\|+\|p\|+\|N\|$	$4\|\mathbb{G}\|+\|\mathrm{TS}_p\|+2\|N\|+\|p\|$
PFDAM	$\|\mathbb{G}_T\|+l\|\mathbb{G}_1\|+\|H\|+\|N\|$	$\|\mathbb{G}_1\|+2\|N\|$	$\|\mathbb{G}_T\|+(l+1)\|\mathbb{G}_1\|+\|H\|+3\|N\|$
LVPDA	$\|\mathrm{ID}_i\|+\|\mathrm{TS}_p\|+2\|N\|+\|p_1\|$	$\|\mathrm{ID}_j\|+\|\mathrm{TS}_p\|+2\|N\|+\|p_1\|$	$\|\mathrm{ID}_j\|+\|\mathrm{TS}_p\|+2\|N\|+\|p_1\|$
EEPPDA	$2\|\mathbb{G}\|+\|\mathrm{ID}_{P_{XY}}\|+\|\tau_{XY}\|$	$2\|\mathbb{G}\|+\|\mathrm{ID}_{\mathrm{ES}_x}\|+\|\tau_X\|$	$4\|\mathbb{G}\|+\|\mathrm{ID}_{\mathrm{ES}_x}\|+\|\tau_X\|+\|\mathrm{ID}_{P_{XY}}\|+\|\tau_{XY}\|$

其中PFDAM方案在通信成本分析过程中的最大聚合维度l假设为5。相较于VMEMDA和PFDAM的通信成本，本文方案实现了更低的通信成本，分别降低了约3%以及29.3%。

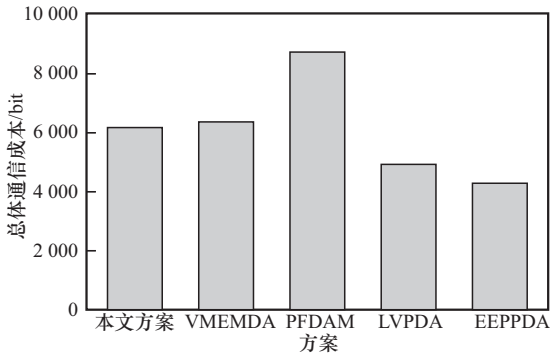

图8　总体通信成本对比

6　结束语

本文方案提出了一种隐私保护数据聚合方案，通过改进的Paillier加密算法实现数据加密，并结合双线性对、秘密共享等技术构建了完整的加密传输框架。首先对采集数据进行加密和签名，边缘服务器根据预设的数据类型验证密钥对密文进行过滤并聚合，然后由中心服务器完成聚合结果的解密和验证。此外，设计了基于数据类型的验证机制，支持对不同类型数据筛选聚合，同时将计算任务移至边缘节点，降低终端设备的计算成本。安全性分析表明，本文方案在保证数据机密性和完整性的同时，能够有效抵抗窃听、伪造等攻击。实验结果表明，相较于现有方案，本文方案在计算效率和通信成本方面均具有一定优势。

参考文献：

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

[2] GENTRY C. Fully homomorphic encryption using ideal lattices[C]//Proceedings of the Forty-First Annual ACM Symposium on Theory of Computing. New York: ACM Press, 2009: 169-178.

[3] 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.

[4] LYU L J, NANDAKUMAR K, RUBINSTEIN B, et al. PPFA: privacy preserving fog-enabled aggregation in smart grid[J]. IEEE Transactions on Industrial Informatics, 2018, 14(8): 3733-3744.

[5] 张晓均, 张经伟, 黄超, 等. 可验证医疗密态数据聚合与统计分析方案[J]. 软件学报, 2022, 33(11): 4285-4304.
ZHANG X J, ZHANG J W, HUANG C, et al. Verifiable medical con fidential data aggregation and statistical analysis scheme[J]. Journal of Software, 2022, 33(11): 4285-4304.

[6] SHANG S, LI X, GU K, et al. A robust privacy-preserving data aggregation scheme for edge-supported IIoT[J]. IEEE Transactions on Industrial Informatics, 2024, 20(3): 4305-4316.

[7] GHEISARI M, JAVADPOUR A, GAO J C, et al. PPDMIT: a lightweight architecture for privacy-preserving data aggregation in the Internet of things[J]. Journal of Ambient Intelligence and Humanized Computing, 2023, 14(5): 5211-5223.

[8] ZHANG L, WU Q H, DOMINGO-FERRER J, et al. Distributed aggregate privacy-preserving authentication in VANETs[J]. IEEE Transactions on Intelligent Transportation Systems, 2016, 18(3): 516-526.

[9] 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.

[10] LI S H, XUE K P, YANG Q Y, et al. PPMA: privacy-preserving multi-subset data aggregation in smart grid[J]. IEEE Transactions on Industrial Informatics, 2018, 14(2): 462-471.

[11] KONG Q L, LU R X, MA M D, et al. A privacy-preserving sensory data sharing scheme in Internet of Vehicles[J]. Future Generation Computer Systems, 2019, 92: 644-655.

[12] HU P, WANG Y L, GONG B, et al. A secure and lightweight privacy-preserving data aggregation scheme for Internet of vehicles[J]. Peer-to-Peer Networking and Applications, 2020, 13(3): 1002-1013.

[13] MERAD-BOUDIA O R, SENOUCI S M. An efficient and secure mul-

tidimensional data aggregation for fog-computing-based smart grid[J]. IEEE Internet of Things Journal, 2021, 8(8): 6143-6153.

[14] ZHANG X J, HUANG C, ZHANG Y, et al. Enabling verifiable privacy-preserving multi-type data aggregation in smart grids[J]. IEEE Transactions on Dependable and Secure Computing, 2022, 19(6): 4225-4239.

[15] SHI H, ZHAO J, GU C L, et al. Enabling efficient multidimensional encrypted data aggregation for fog-cloud-based smart grid[C]//Proceedings of the 2023 IEEE 16th International Conference on Cloud Computing (CLOUD). Piscataway: IEEE Press, 2023: 557-559.

[16] LIU H D, GU T L, SHOJAFAR M, et al. OPERA: optional dimensional privacy-preserving data aggregation for smart healthcare systems[J]. IEEE Transactions on Industrial Informatics, 2023, 19(1): 857-866.

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

[18] SINGH V P, KUMAR A, DUBEY A, et al. Privacy-preserving data aggregation in smart cities: secure and efficient techniques for urban data management[C]//Proceedings of the 2025 International Conference on Networks and Cryptology (NETCRYPT). Piscataway: IEEE Press, 2025: 1-5.

[19] ZHU B Y, LI Y M, HU G X, et al. A privacy-preserving data aggregation scheme based on Chinese remainder theorem in mobile crowdsensing system[J]. IEEE Systems Journal, 2023, 17(3): 4257-4266.

[20] SRIDOKMAI T, PRAKANCHAROEN S. The homomorphic other property of Paillier cryptosystem[C]//Proceedings of the 2015 International Conference on Science and Technology (TICST). Piscataway: IEEE Press, 2015: 356-359.

[21] BONEH D, FRANKLIN M. Identity-based encryption from the Weil pairing[C]//Advances in Cryptology — CRYPTO 2001. Berlin: Springer, 2001: 213-229.

[22] DIFFIE W, HELLMAN M E. New directions in cryptography[M]//Democratizing cryptography: the work of Whitfield Diffie and Martin Hellman. New York：Association for Computing Machinery. 2022: 365-390.

[23] GAUSS C F. Disquisitiones arithmeticae[M]. New Hawen: Yale University Press, 1966.

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

[25] ZHANG J L, ZHAO Y C, WU J, et al. LVPDA: a lightweight and verifiable privacy-preserving data aggregation scheme for edge-enabled IoT[J]. IEEE Internet of Things Journal, 2020, 7(5): 4016-4027.

[26] ZHAO J, HUANG H J, ZHANG X J, et al. VMEMDA: verifiable multidimensional encrypted medical data aggregation scheme for cloud-based wireless body area networks[J]. IEEE Internet of Things Journal, 2024, 11(10): 18647-18662.

[27] ZHANG J H, WEI J. PFDAM: privacy-preserving fine-grained data aggregation scheme supporting multifunctionality in smart grid[J]. IEEE Internet of Things Journal, 2024, 11(15): 25520-25533.

[28] BHOWMIK T, BANERJEE I. EEPPDA: Edge-enabled efficient privacy-preserving data aggregation in smart healthcare Internet of things network[J]. International Journal of Network Management, 2023, 33: e2216.

[作者简介]

牛坤（1985– ），女，山西长治人，博士，贵州大学副教授、硕士生导师，主要研究方向为信息安全、密码学等。

石淼（2001– ），女，吉林舒兰人，贵州大学硕士生，主要研究方向为数据安全、密码学等。

彭长根（1963– ），男，贵州黔东南人，博士，贵州大学教授、博士生导师，主要研究方向为密码学与信息安全、大数据与隐私保护等。

许德权（1989– ），男，贵州安顺人，博士，贵阳学院讲师，主要研究方向为密码学。

蔡斐（1988– ），男，江苏海门人，贵州轻工职业技术学院讲师，主要研究方向为云计算。