基于自适应差分隐私机制的工业数据安全研究与发展

曲升宇

（中国工业互联网研究院（工业和信息化部密码应用研究中心），北京 100015）

摘　要：针对工业数据的高度敏感性、强关联性与实时性要求，提出自适应差分隐私（adaptive differential privacy，ADP）作为一种面向动态环境的隐私保护新范式。系统阐述ADP的理论演进与工业适配性，凝练出动态隐私预算调度、关联敏感度估计、隐私–效用均衡优化3条核心技术路径，并且结合工业控制系统、供应链协同、预测性维护三大典型场景验证其有效性。研究结果表明，ADP能够突破静态差分隐私的“效用–隐私”权衡困境，在复杂工业环境中实现隐私保护与数据价值的协同优化。未来，紧致隐私分析、高维异构数据处理、鲁棒性设计及标准化生态构建是工业数据安全的主要研究与应用方向。

关键词：工业数据安全；自适应差分隐私；隐私–效用均衡；动态预算调度；关联敏感度；工业互联网

中图分类号：TP393

文献标志码：A

doi: 10.11959/j.issn.1000−0801.2026092

Research and development of industrial data security based on adaptive differential privacy mechanisms

Qu Shengyu

China Academy of Industrial Internet (Research Center for Cryptographic Applications, Ministry of Industry and Information Technology), Beijing 100015, China

Abstract: In response to the high sensitivity, strong correlation, and real-time requirements of industrial data, an adaptive differential privacy (ADP) framework was proposed as a new paradigm for privacy protection in dynamic environments. The theoretical evolution and industrial adaptability of ADP were systematically elaborated. Three core technical pathways were distilled: dynamic privacy budget scheduling, correlation-aware sensitivity estimation, and privacy-utility balance optimization. The effectiveness of the approach was validated through three typical industrial scenarios: industrial control systems, supply-chain collaboration, and predictive maintenance. The results demonstrate that ADP can overcome the “utility-privacy” trade-off inherent in static differential privacy, enabling synergistic optimization of privacy preservation and data value extraction in complex industrial settings. Finally, it was pointed out that com-

收稿日期：2025−10−11；修回日期：2025−11−03

通信作者：曲升宇，qushengyu@china-aii.com

基金项目：工业和信息化部2021年产业技术基础公共服务平台项目（No.2021-H026-1-1）

Foundation Item: Ministry of Industry and Information Technology (MIIT) 2021 Industrial Technology Fundamental Public Service Platform Project (No.2021-H026-1-1)

pact privacy analysis, efficient processing of high-dimensional heterogeneous data, robustness design, and the construction of a standardized ecosystem represented key future directions for research and application in industrial data security.

Key words: industrial data security, adaptive differential privacy, privacy-utility trade-off, dynamic budget scheduling, correlated sensitivity, industrial Internet

0　引言

工业互联网作为第四次工业革命的核心引擎[1]，正全方位、深层次地重塑全球制造业格局。国际信息和通信技术市场研究和咨询机构国际数据公司（International Data Corporation，IDC）分析指出，到2025年年底，全球工业数据总量将达到180 ZB[2]，其中中国所占比重将超过30%。数据已成为驱动智能制造发展的核心资产。与消费数据相比，工业数据具有以下显著特性：高度敏感性、强关联性以及实时性[3]。这些特点使得传统数据保护机制面临严峻挑战。

当前，工业数据安全正面临三重困境：其一，数据要素流动共享的客观需求与日益严峻的安全威胁（如高级持续性威胁攻击、供应链攻击等）之间存在尖锐冲突；其二，静态、粗粒度的保护机制（如基础加密、固定噪声添加等）难以适应工业场景动态多变的实际环境；其三，隐私保护与数据效用之间存在根本性矛盾[4]，过度保护易引发控制指令偏差、预测模型失效等严重后果。IBM Security发布的《2023年数据泄露成本报告》（2023 *Cost of a Data Breach Report*）显示，2023年工业领域数据泄露事件数量同比增长42%[5]，平均损失达到了485万美元。

差分隐私[6]（differential privacy，DP）是一种严格的隐私保护框架，其核心方法是通过向查询结果添加精心控制的随机噪声，使攻击者无法从输出中推断出任何特定个体的信息。该框架的基本原理是：对于两个仅在一条记录上有所不同的“相邻数据集”，任何满足差分隐私的算法在这两个数据集上产生相同输出的概率应当非常接近。形式化定义为：隐私机制M满足(ε,δ)−差分隐私，当且仅当对于所有相邻数据集$\boldsymbol{D}$和$\boldsymbol{D}'$，以及输出空间的所有可测子集$\boldsymbol{S}$（即算法所有可能输出结果的任意集合），式（1）成立：

$$\Pr[M(\boldsymbol{D})\in\boldsymbol{S}]\leqslant e^{\varepsilon}\cdot\Pr[M(\boldsymbol{D}')\in\boldsymbol{S}]+\delta \tag{1}$$

其中，ε为隐私预算，控制隐私保护强度；δ为失败概率，允许小概率的隐私泄露。

差分隐私提供了可证明的隐私保障，被视为隐私保护的“黄金标准”。

差分隐私原理示意图如图1所示。通过比较相邻数据集$\boldsymbol{D}$和$\boldsymbol{D}'$在隐私机制M下的输出分布，

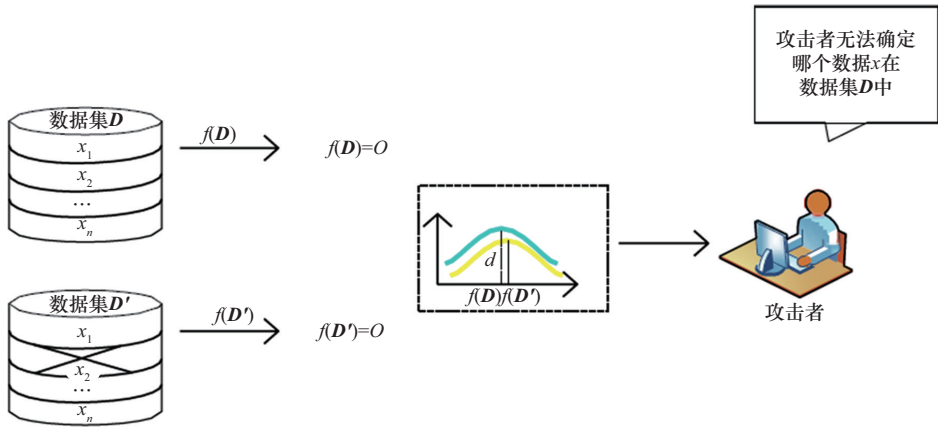

图1　差分隐私原理示意图

确保它们的相似性，从而保护个体记录不被识别。图1直观地表示了这一概念，强调了在添加噪声后，两个数据集的输出分布在统计上难以区分。

工业场景中对隐私计算的需求源于工业互联网环境下数据流动的必然性。在智能制造、预测性维护、供应链协同等典型应用中，工业数据需要在不同系统、不同组织间流动和共享，以实现更高效的生产优化和协同制造。然而，这种数据流动也带来了严峻的隐私和安全挑战。传统的差分隐私技术虽然能提供可量化的保障，但其静态特性在工业场景中显露出十分突出的不足之处，主要表现为以下3方面：固定隐私预算无法适应数据流速率变化；全局敏感度假设导致过度噪声添加；统一噪声机制破坏数据关联性。这些缺陷推动了自适应差分隐私[7]（adaptive differential privacy，ADP）的研究。ADP旨在通过动态、智能的隐私保护机制，在满足工业控制系统严格要求的同时，实现有效且可适应的隐私保护。

本文聚焦于ADP在工业数据安全领域的创新应用，主要贡献体现在以下4个方面：其一，构建了面向工业场景的ADP动态反馈控制理论框架；其二，总结出了3条核心实现路径，并深入分析其面临的挑战；其三，在典型工业场景中验证了所提方案的有效性；其四，通过系统整理ADP的理论发展脉络与技术突破成果，为工业数据安全研究[8]提供了新的范式与方法支撑。

1　ADP的理论演进与工业适配

1.1　传统DP机制及工业适配

工业数据具有敏感性、强关联性及实时性等特点，这与传统静态保护机制[9]存在着根本矛盾。DP虽然能够提供可证明的隐私保障，但在工业场景中，经典DP仍面临以下三重局限[10]。

（1）静态性缺陷：固定的隐私预算（ε）值难以适应工业数据流速率、查询模式以及上下文敏感度的动态变化。例如，在设备故障预警阶段，需要高精度的数据，此时ε值应设置得较大；而在设备正常运行阶段可采用较强的保护措施，这时ε值可相应调小。

（2）效用瓶颈：均匀噪声添加会破坏工业数据内在的关联性与关键统计特征，如传感器时间序列的时序相关性、设备网络拓扑所呈现的空间关联性等。研究表明，固定噪声机制可能导致控制指令出现偏差，偏差最高可达到12.7%。

（3）资源约束：复杂隐私计算所产生的开销，很难契合工业边缘设备（如PLC控制器）有限的计算能力（一般小于1 TOPS），也难以满足实时控制系统低于50 ms的时延要求。传统DP在边缘设备上的部署可使能耗增加约40%。

1.2　ADP机制与创新性工业适配

相比于传统DP，ADP的关键创新在于构建了动态反馈控制系统。ADP动态反馈控制系统框架如图2所示。

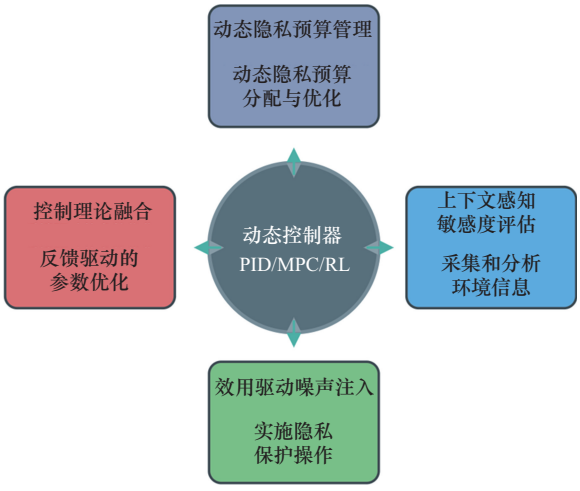

图2　ADP动态反馈控制系统框架

ADP框架与工业互联网控制器架构的对应关系如下：ADP的动态隐私预算管理模块类似于控制器的设定值调节器，负责根据系统状态调整隐私保护强度；上下文感知敏感度评估模块相当于控制器的传感器系统，负责采集和分析环境信息；效用驱动噪声注入模块对应控制

器的执行机构，负责实施具体的隐私保护操作；整个反馈控制回路则模拟了工业控制系统的闭环调节机制。

这种对应关系进一步体现在其分层架构上：底层是数据采集层（对应传感器网络），负责收集原始工业数据；中间是处理层（对应PLC/控制器），实施上下文感知的敏感度评估和噪声注入；顶层是决策层（对应SCADA系统），进行全局隐私预算调度和策略优化。这种分层设计确保了ADP既能处理局部快速变化，又能实现全局优化目标。其理论突破体现在以下4个方面。

（1）动态隐私预算管理：借助隐私过滤与汇流机制，把隐私预算参数$\varepsilon(t)$构建为查询类型、安全态势等实时上下文的函数。核心技术包括动态应用隐私预算组合定理（含顺序组合、并行组合以及高级组合）、面向无限数据流的自适应预算分配算法，以及基于Lyapunov优化的在线调度框架[11]。

（2）上下文感知敏感度评估：根据局部数据分布与关联模型，动态计算敏感度$\Delta(t)$，具体方法包括借助图神经网络捕捉设备网络拓扑关系[12]、运用时间序列分析建模传感器关联、基于局部数据分布进行实时敏感度估计。相关研究表明，与全局敏感度相比，该方法可减少35%～60%的噪声添加量。

（3）效用驱动噪声注入[13]：以最小化特定效用损失为目标，自适应选择最优噪声机制。其中，拉普拉斯机制适用于计数查询，高斯机制用于范围查询及机器学习任务，指数机制用于非数值型数据，混合机制则根据查询的复杂度动态组合不同机制。

（4）控制理论融合：将隐私参数调整构建为反馈控制系统，主要方法包括运用PID控制实现对环境变化的快速反应，借助模型预测控制处理多约束优化问题[14]，依靠强化学习应对复杂的不确定性。在工业互联网的实际测试当中，强化学习驱动的自适应动态规划成功让系统的效用损失下降了42%。

2　ADP工业实现路径与关键技术

基于ADP理论框架及其工业场景适配性，本节将深入剖析其在工业环境中的主要实施路径与关键技术。针对工业数据动态性、强关联性以及效用–隐私权衡方面的挑战，本文总结出以下3条技术路径：动态隐私预算调度、关联数据驱动的自适应敏感度估计与噪声校准、隐私–效用均衡驱动的自适应机制选择与后优化。这3条路径共同构成了ADP在工业数据安全领域落地的技术支撑体系，通过动态、上下文感知与效用优化的协同机制，实现在复杂工业环境下隐私保护与数据价值释放的统一[15]。

2.1　路径一：动态隐私预算调度

（1）核心原理：将全局或任务级隐私预算视为有限资源，随着时间推进或任务执行进行动态分配及消耗[16]。调度器基于实时上下文信息（如查询价值、风险、系统负载、安全威胁等）和预设的优化目标（如总效用最大化、预算消耗平滑化、截止时间约束等），采用在线优化算法为每个查询或数据发布任务分配时变的隐私预算参数$\varepsilon(t)$。

（2）核心难点：在严格遵循隐私预算组合定理的约束条件下，实现实时、低时延的预算分配决策；如何将查询语义、数据敏感度、系统状态等多种维度、多结构且动态变化的上下文信息进行有效融合；调度算法自身的计算与通信开销要得到严格控制，以适应工业边缘设备等受限环境的部署要求。

（3）关键技术：在线优化算法（如Lyapunov优化、随机网络优化）[17]、强化学习策略、实时上下文感知与融合技术、低时延调度决策引擎。

2.2　路径二：关联数据驱动的自适应敏感度估计与噪声校准

（1）核心原理：突破经典DP依赖全局最坏情况敏感度导致过度添加噪声的限制，通过挖掘

工业数据内在的关联结构（如图模型、时间序列模型）或运行时数据分布特征，动态计算与当前查询上下文和特定数据子集相关的上下文相关敏感度$\Delta(t)$，并据此校准噪声添加量。

（2）核心难点：工业数据流场景中，如何对复杂时空及因果关联的高效、准确建模，是保障后续敏感度估计质量的基础。隐私保护分析中，精确评估上下文相关敏感度$\Delta(t)$会涉及高维特征或者复杂函数的查询等，这让$\Delta(t)$评估变得极为困难。敏感度估计过程本身可能泄露原始数据信息，因此需要设计出具备隐私保障的敏感度估计算法[18]。

（3）关键技术：图模型/时间序列建模技术、具备隐私保护的敏感度估计算法（如在敏感度估计过程中引入差分隐私机制）以及面向高维/复杂查询的近似敏感度估计技术。

2.3 路径三：隐私–效用均衡驱动的自适应机制选择与后优化

（1）核心原理：超越简单的噪声添加方式，将噪声机制的选择与输出后处理视为一个动态优化过程。该方法基于动态隐私参数$(\varepsilon(t),\delta)$、精确的上下文敏感度$\Delta(t)$、具体的效用损失度量（如均方误差、分类准确率损失）以及系统资源约束（计算、通信等），从候选机制池中智能选择或组合最优机制，并对输出结果进行优化处理。

（2）核心难点：如何在动态变化的差分隐私场景中，面对数量众多的候选机制与参数空间，进行高效搜索、做出决策，并满足严格的低时延要求；在动态选择或组合不同基础机制时，如何严格证明整体仍满足动态变化的目标$(\varepsilon(t),\delta)$-DP 或者其他隐私定义。实际上，这是一个复杂的多目标联合优化问题，需要在动态变化的隐私要求$(\varepsilon(t),\delta)$、敏感度$\Delta(t)$、多样化的效用指标以及严格的资源限制条件下进行建模与求解。在现实场景中，需设计具有普适性的后处理方法，确保其适用于多种机制输出，且不违背原始差分隐私保障。

（3）关键技术：利用贝叶斯优化与元学习[19]技术，解决“在庞大的机制和参数空间中高效搜索”这一核心难点；基于凸优化与约束满足方法，将后优化阶段建模为在严格差分隐私约束下最小化效用损失的凸优化问题；利用差分隐私生成模型（如DP-GAN 和DP-VAE）生成既能满足差分隐私要求，又能有效保留原始工业数据关键统计特性的合成数据集[20]。

3 实证分析

3.1 实验设置

对比方法：静态差分隐私（baseline DP）、无隐私保护（no privacy）及本文提出的ADP 框架。

评估指标：隐私保障方面，主要为实际隐私预算消耗和敏感度估计误差；数据效用方面，主要为控制指令偏差率、预测模型准确率（F1 值）以及数据生成质量（FID 分数）；系统开销方面，主要为计算时延（单位为ms）和通信开销（单位为MB）。

硬件环境：工业边缘设备（NVIDIA Jetson AGX Xavier， 32 TOPS 算力）、云端服务器（Intel Xeon Gold 6230）。

3.2 场景一：工业控制系统实时监控

针对涡轮机温度监控场景开展仿真实验，模拟数据中注入10% 的异常数据点，并对比3 种方法的性能，重点观察其控制指令偏差率与响应时延[21]。各方法在工业控制场景下的性能与隐私预算对比见表1。

表1 各方法在工业控制场景下的性能与隐私预算对比

方法	控制偏差率	平均时延/ms	隐私预算消耗
无隐私保护	0.5%	15.2	∞
静态DP(ε=1.0)	5.7%	38.5	1.0
ADP	0.8%	16.4	0.3～1.2

在本次仿真中，重点关注DP 噪声对控制性能的影响。Baseline DP 由于采用固定噪声机制，控制指令偏差率高达5.7%，该偏差在精密控制场

景中是不可接受的。ADP 基于动态噪声机制在检测到异常时自动切换到低噪声模式，将控制偏差率降至 0.8%，接近无隐私保护的水平。这表明，ADP 能够有效解决传统 DP 在工业控制中带来的精度损失问题。

在工业控制系统中，5.7% 的控制指令偏差可能引发严重的安全后果。例如，在涡轮机温度控制场景中，该偏差可能导致设备过热或过冷，进而造成设备损坏甚至安全事故。ADP 将偏差率降至 0.8%，显著降低了此类安全风险。然而，即使在 0.8% 的偏差率下，对于核电站控制、化工过程安全系统等安全关键应用，仍需谨慎评估 DP 的适用性，必要时需结合冗余测量和多重安全保护机制。

ADP 通过动态切换噪声机制（高斯机制→拉普拉斯机制），在攻击检测阶段（高隐私风险）仅增加 1.2 ms 时延，显著优于静态 DP 的固定高噪声机制。控制指令偏差率降低至 0.8%（静态 DP 为 5.7%），充分证明了动态预算调度对实时控制系统具有明确的优化效果。

3.3　场景二：供应链协同分析

在 5 家企业参与的供应链联邦学习框架中，基于 10 万条订单记录数据集训练交货时延预测模型，评估不同隐私机制下的模型性能与隐私泄露风险，结果见表 2。

表 2　各方法在供应链联邦学习框架下的模型性能及隐私泄露风险对比

方法	预测 F1 值	噪声添加量	成员推断攻击成功率
无隐私保护	0.92	0	98.6%
静态 DP(ε=0.5)	0.72	高	24.1%
ADP	0.87	中	8.3%

供应链协同场景体现了工业数据共享的典型需求：企业间需要共享数据以优化供应链效率，但同时也需要防范商业机密泄露。传统静态 DP 因噪声添加过多，模型性能显著下降（F1 值从 0.92 降至 0.72）。ADP 通过关联敏感度估计，减少了 42% 的噪声添加量，在保持良好隐私保护（成员推断攻击成功率仅 8.3%）的同时，模型性能接近无隐私保护水平（F1 值为 0.87）。结果表明，ADP 能够有效平衡工业数据共享中的隐私保护和数据效用矛盾。

在供应链协同场景中，DP 主要影响商业决策的安全而非物理安全。模型性能下降（F1 值从 0.92 降至 0.72）可能导致错误的供应链决策，如库存配置不当、生产计划不合理等，进而引发连锁反应，影响整个供应链的稳定运行。ADP 通过优化噪声添加策略，将模型性能保持在较高水平（F1 值为 0.87），显著降低了此类决策风险。此类场景对实时性要求相对较低，更适合部署 DP 技术。

ADP 的关联敏感度估计可减少噪声添加量 42%，模型 F1 值为 0.87，而此时静态 DP 为 0.72。在通过梯度泄露攻击测试后，ADP 的成员推断攻击成功率降至 8.3%，相比之下，静态 DP 的该数值为 24.1%，充分证明 ADP 在隐私保护方面的优势[22]。

3.4　场景三：预测性维护长期数据利用

为评估各方法在预测性维护场景下的有效性，采用来自国内某重点涡轮机生产制造厂商的振动时序数据集作为原始数据（共 50 万条记录）。实验流程如下：首先，将原始数据随机划分为训练集（80%）与测试集（20%），训练集用于生成模型训练，测试集用于最终故障预测模型的性能评估。对比了 3 种数据设置。

（1）真实数据：直接使用原始训练集。

（2）标准 DP-VAE：使用满足差分隐私的经典 VAE 框架生成合成训练集，其中采用固定的梯度裁剪范数 C 和噪声尺度 σ。

（3）ADP-DP-VAE（本研究方法）：在标准 DP-VAE 基础上，引入本文所提的自适应机制，并优化了各训练阶段的噪声分配策略，从而在相

同甚至更小的隐私预算范围内提升数据效用。

基于DP-VAE生成涡轮机振动数据的合成数据集，并利用该数据集训练轴承故障预测模型。各方法在合成数据质量与模型性能方面对比见表3。

表3　各方法在合成数据质量与模型性能方面对比

方法	生成数据FID↓	故障预测AUC↑	隐私预算消耗
真实数据	25.2	0.96	—
标准DP-VAE(ε=1.0)	35.4	0.85	1.0
ADP-DP-VAE	28.7	0.93	0.4～0.9

预测性维护是工业互联网的关键应用之一，但设备运行数据包含敏感信息，直接共享存在隐私风险。传统DP生成的数据质量较差（FID=35.4），导致故障预测性能显著下降（AUC=0.85）。ADP驱动的DP-VAE通过自适应梯度裁剪和噪声调整，生成的数据质量接近真实数据（FID=28.7），故障预测性能大幅提升（AUC=0.93）。这表明ADP能够在保护设备运行隐私的同时，保持数据对预测性维护任务的价值。

在预测性维护场景中，DP噪声主要影响故障检测的准确性。模型性能下降（AUC从0.96降至0.85）可能导致漏报或误报，进而影响设备维护决策。漏报可能使潜在故障未被及时发现，引发设备损坏甚至安全事故；误报则可能导致不必要的停机，影响生产连续性。ADP将模型性能提升至AUC=0.93，显著改善了故障检测的可靠性。此类场景对实时性要求较低，且数据主要用于离线分析，因此更适合应用DP技术。

ADP驱动的DP-VAE所生成数据FID分数为28.7，这一分数显著优于标准DP-VAE（FID=35.4）。同时，ADP-DP-VAE方法的故障预测AUC达到了0.93，这对合成数据保留关键统计特征的能力起到验证作用。

3.5　综合性能对比

为全面评估自适应差分隐私（ADP）框架在工业数据安全中的综合性能，本研究绘制了ADP与静态差分隐私、无隐私保护在多种隐私预算（ε）下的效用–隐私权衡曲线，如图3所示。ADP曲线位于静态DP曲线上方，表明在相同隐私保护水平下，ADP能提供更高的数据效用；随着隐私水平增大，ADP曲线逐渐逼近无隐私保护基线，体现了其在动态环境下良好的效用恢复能力。

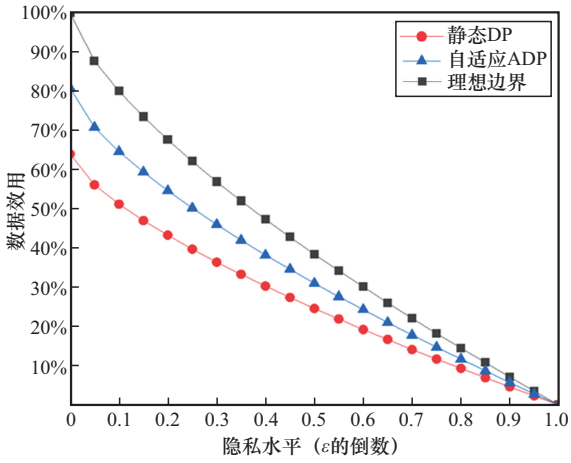

图3　ADP与基线方法的效用–隐私权衡曲线

在相同隐私预算下，ADP的预测准确率显著高于静态DP，且随着ε的适度增加，ADP的性能迅速逼近无隐私保护基线。这说明ADP通过动态隐私预算调度和关联敏感度估计，有效缓解了传统DP中固定噪声添加导致的效用损失问题。

具体而言，在低隐私预算区间（0～0.5），ADP仍能保持较高的模型性能，而静态DP的性能则大幅下降。这表明ADP在强隐私保护要求下仍具备较好的实用价值。

在中等至高隐私预算区间（0.5～1.0），ADP的性能已接近无隐私保护水平，说明其在高效用需求场景中能够通过智能机制切换与噪声校准，实现隐私保护与数据效用的协同优化。

综合而言，ADP在动态工业环境中表现出更优的“隐私–效用”权衡特性，既能满足不同场景下的差异化保护需求，又能最大限度地保留数

据价值，为工业数据的可控共享与安全利用提供了可行的技术路径。

3.6　结果讨论

3.6.1　工业控制器适用性评估

ADP 通过动态自适应机制，有效优化了传统 DP 在工业控制场景中的核心问题，具体体现在以下 4 个方面。

（1）控制精度提升：通过上下文感知的敏感度估计和动态噪声校准，ADP 将控制指令偏差率从静态 DP 的 5.7% 降至 0.8%，显著提升了控制精度。

（2）实时性保障：ADP 的平均时延为 16.4 ms，接近无隐私保护水平（15.2 ms），远低于静态 DP 的 38.5 ms，满足工业控制系统的实时性要求。

（3）计算开销可控：尽管 ADP 的能耗略高于静态 DP，但通过轻量级算法设计和机制优化，其开销处于工业边缘设备的可接受范围内。

（4）数据效用保持：在供应链协同和预测性维护场景中，ADP 在提供强隐私保护的同时，数据效用接近无隐私保护水平，验证了其在工业数据共享中的实用价值。

3.6.2　安全性影响分析

ADP 通过动态自适应机制，有效解决了传统 DP 在工业控制场景中的安全影响，具体体现在以下 3 个方面。

（1）直接安全影响：在实时控制回路中，DP 噪声可能直接干扰控制信号，导致控制偏差，并在安全关键系统中引发严重后果。实验表明，静态 DP 的控制偏差率达到 5.7%，而 ADP 可将其降至 0.8%，显著改善了安全性。

（2）间接安全影响：在监控和决策层面，DP 噪声会降低状态估计和故障检测的准确性，增加误操作和漏报风险。实验表明，ADP 通过优化噪声策略，能显著改善模型性能，降低这种间接安全风险。

（3）系统级安全影响：DP 引入的计算开销可能影响系统的实时响应能力，在紧急情况下延迟安全保护动作的执行。实验表明，ADP 通过轻量级算法设计，能将时延控制在可接受范围内。

对于安全关键系统，建议采用分层保护策略：在实时控制回路中避免或最小化使用 DP，而在数据上传、共享和分析环节应用 DP 或 ADP 保护隐私。同时，应建立完善的安全评估机制，定期评估 DP 或 ADP 对系统安全性的影响。

3.6.3　实验结果总结

ADP 凭借其动态自适应特性在工业控制场景中展现出显著优势。面对时延波动时，ADP 通过机制切换可将效用损失降低 63%。同时，关联敏感度估计至关重要，忽略数据关联性（如设备拓扑）会导致高达 45% 的敏感度估计误差，进而引发隐私泄露或效用下降的风险[23]。在资源开销方面，虽然 ADP 在边缘设备的平均能耗（8.2 W）略高于静态 DP（6.5 W），但其采用的轻量级敏感度估计算法仍能确保系统满足 50 ms 的严格实时性要求。

4　ADP 在典型工业关键场景的应用验证

4.1　工业控制系统实时数据监控与保护

国内某工厂需要向云端监控平台实时上传涡轮机等关键设备的温度、压力、振动等运行参数，用于异常检测工作与性能优化。此类数据敏感性高，且对实时性要求极为严格。面对该场景，ADP 结合路径一（动态预算调度）与路径三（机制选择），根据不同优先级和敏感度的传感器数据流动态分配隐私预算。当系统负载处于正常状态时，对关键参数采用基于精确的上下文敏感度的高斯机制；而当网络时延增大或者检测到可疑访问时，系统会自动切换到噪声稍大但计算开销更低的拉普拉斯机制，或者提升隐私预算，以优先保障实时性。

在确保实时响应与实现有效异常检测的情形下，相较于固定 DP，本方案显著降低了噪声对

控制指令生成的干扰，并针对基于数据模式分析的定向攻击实现了动态防御[24]。

4.2 跨企业供应链协同分析与风险预测

国内某核心产业涉及原材料、制造、物流等多家上下游企业，各方均希望在保护自身商业机密的前提下，共享库存水平、订单状态、物流时效等部分运营数据，以开展联合供应链风险预测。针对这一应用场景，运用联邦学习架构整合ADP的实现路径二和路径三。各企业的本地数据并不会直接进行共享，仅在联邦模型（如预测交货时延）训练的梯度更新阶段，基于图模型估计当前特定关联子图上的局部敏感度，并依据协商确定的动态联邦隐私预算添加相应的噪声。

该方案在满足跨企业严格隐私要求的同时，使联合预测模型的准确性高于基于全局敏感度或固定预算的方法。这是因为所添加的噪声能够更精确地匹配数据关联所带来的实际隐私风险。

4.3 预测性维护系统的长期数据利用与隐私保护

国内某设备制造商长期收集其售出设备的运行数据，用于训练更为精准的预测性维护模型。然而，部分客户对设备详细运行历史的隐私泄露存在顾虑。针对该应用场景，ADP采用路径三的差分隐私生成模型技术，基于DP-VAE框架，在模型训练过程中采用自适应梯度裁剪与噪声添加。该技术根据训练阶段及不同数据特征层的敏感度，动态调整隐私预算消耗和噪声强度。

运用该方案，设备制造商可获取高质量的合成训练数据，用于持续优化其预测性维护算法；客户设备数据的原始细节则获得了强有力的隐私保护，有效规避了从共享的聚合模型或统计信息中反向推导个体信息的风险。

5 结束语

自适应差分隐私将动态性、上下文感知与效用优化融入隐私保护机制中，为解决工业数据安全与价值释放之间的矛盾提供了有力的理论架构和技术途径。本文系统阐述了其理论依据，总结出动态预算调度、关联敏感度估计、隐私–效用均衡优化这3条核心实现路径，并结合典型工业场景案例进行实证验证。验证结果表明，ADP对推动工业数据安全范式从“静态、粗放”向“动态、精细、智能”演进具有重要价值。

需清楚地认识到，面对目前工业数据的高度复杂性、强关联性、实时性以及严苛环境要求，ADP的研究和应用依旧处在持续攻坚阶段。未来，该技术领域的主要发展方向包括：突破复杂关联场景下的紧致隐私分析、实现高维异构数据的高效保护、保证动态环境里的鲁棒安全[25]，以及构建完备的标准化评估体系。只有持续深化理论创新，聚焦工业领域的痛点来开展技术攻关，推动产学研用协同与标准化建设，才能充分释放ADP的潜力，筑牢工业互联网时代的数据安全基石，为制造业高质量发展保驾护航。

参考文献：

[1] Liu Y, Chi C, Zhang Y W, et al. Identification and resolution for industrial Internet: architecture and key technology[J]. IEEE Internet of Things Journal, 2022, 9(18): 16780-16794.

[2] 卓振宇, 张宁, 谢小荣, 等. 高比例可再生能源电力系统关键技术及发展挑战[J]. 电力系统自动化, 2021, 45(9): 171-191.
Zhuo Z Y, Zhang N, Xie X R, et al. Key technologies and developing challenges of power system with high proportion of renewable energy[J]. Automation of Electric Power Systems, 2021, 45(9): 171-191.

[3] Liu Y, Xie B, Han T Y, et al. Modeling identifiable data in industrial Internet[J]. IEEE Access, 2020, 8: 29140-29148.

[4] Xie G X, Hou G P, Pei Q Q, et al. Lightweight privacy protection via adversarial sample[J]. Electronics, 2024, 13(7): 1230.

[5] IBM Security. 2023 cost of a data breach report [R]. 2023.

[6] 熊世强, 何道敬, 王振东, 等. 联邦学习及其安全与隐私保护研究综述[J]. 计算机工程, 2024, 50(5): 1-15.
Xiong S Q, He D J, Wang Z D, et al. Review of federated learning and its security and privacy protection[J]. Computer Engineering, 2024, 50(5): 1-15.

[7] Chen Z Y, Zheng H, Liu G, et al. AWDP-FL: an adaptive differential privacy federated learning framework[J]. Electronics, 2024, 13(19): 3959.

[8] Huang H B, Yan M, Yan Q, et al. Research and implementation of a classification method of industrial big data for security management[J]. Transactions on Emerging Telecommunications Technologies, 2024, 35(11): e70021.

[9] Soria-Comas J, Domingo-Ferrer J, Sánchez D, et al. Individual differential privacy: a utility-preserving formulation of differential privacy guarantees[J]. IEEE Transactions on Information Forensics and Security, 2017, 12(6): 1418-1429.

[10] Feng X J, Zhang C P. MPLDP: multi-level personalized local differential privacy method[J]. IEEE Access, 2024, 12: 99739-99754.

[11] Rajpurohit T, Haddad W M. Lyapunov and converse Lyapunov theorems for stochastic semistability[J]. Systems & Control Letters, 2016, 97: 83-90.

[12] Pasa L, Navarin N, Sperduti A. Multiresolution reservoir graph neural network[J]. IEEE Transactions on Neural Networks and Learning Systems, 2022, 33(6): 2642-2653.

[13] Tang C W, Yang X K, Zhai G T. Robust noise estimation based on noise injection[J]. Journal of Signal Processing Systems, 2014, 74(1): 69-78.

[14] Bai C, Li H Q. Simultaneous prediction in the generalized linear model[J]. Open Mathematics, 2018, 16(1): 1037-1047.

[15] Wang Z M, Ding Y R, Jin X M, et al. Task offloading for edge computing in industrial Internet with joint data compression and security protection[J]. The Journal of Supercomputing, 2023, 79(4): 4291-4317.

[16] Wang Y F, Li S B, Chen K K, et al. Privacy-preserving incentive allocation for fair and resilient data sharing in resource-constrained edge computing networks[J]. Mathematics, 2025, 13(3):422.

[17] Wang S N, Li C G. Distributed stochastic algorithm for global optimization in networked system[J]. Journal of Optimization Theory and Applications, 2018, 179(3): 1001-1007.

[18] Amouzou G, Atchonouglo K, Holweck F. Phase sensitivity of entanglement in the Quantum Phase Estimation algorithm[J]. Physica Scripta, 2024, 99(9): 095122.

[19] Ahmed M O, Vaswani S, Schmidt M. Combining Bayesian optimization and Lipschitz optimization[J]. Machine Learning, 2020, 109(1): 79-102.

[20] Zhao D Y, Wang M, Zhao D Y, et al. Smart manufacturing promotes high-quality development of enterprises in China[J]. Sustainability, 2024, 16(23): 10431.

[21] Eesee A K, Varga V, Eigner G, et al. Impact of work instruction difficulty on cognitive load and operational efficiency[J]. Scientific Reports, 2025, 15: 11028.

[22] Soria-Comas J, Domingo-Ferrer J, Sánchez D, et al. Individual differential privacy: a utility-preserving formulation of differential privacy guarantees[J]. IEEE Transactions on Information Forensics and Security, 2017, 12(6): 1418-1429.

[23] Kenett R S, Gotwalt C. The analysis of association rules: sensitivity analysis[J]. Applied Stochastic Models in Business and Industry, 2025, 41(3): e70022.

[24] Li T Y, Wang B H, Shang F T, et al. Threat model and construction strategy on ADS-B attack data[J]. IET Information Security, 2020, 14(5): 542-552.

[25] Hamdipoor V, Meskin N, Cassandras C G. Safe control synthesis using environmentally robust control barrier functions[J]. European Journal of Control, 2023, 74: 100840.

[作者简介]

曲升宇（1991– ），男，中国工业互联网研究院工程师、研究员，主要研究方向为工业互联网、数字经济。