电子汽车衡作弊形态探究和反作弊分析

□陆海兵[1]　马丙辉[2,3]　李金扬[2,3]　张子超[2,3]　边浩阳[2,3]

（1. 启东市综合检验中心　2. 浙江省质量科学研究院　3. 浙江省工程测力质量检验中心）

【摘　要】电子汽车衡作为大宗物品贸易结算的称重设备，其称重结果的准确性直接关系到双方的经济利益。但作弊技术的存在和发展，对计量公平产生了巨大的威胁，不仅破坏了计量器具的准确度等级，还直接摧毁了计量检定/校准活动的价值。本文简要梳理了电子汽车衡遥控作弊形态的发展脉络，希望与计量同仁加强该领域的研究，保障计量活动的公正公平。

【关键词】电子汽车衡；遥控作弊；滚动码；LoRa；反作弊技术

文献标识码：A　　文章编号：1003-1870（2026）01-0018-03

Exploration of Cheating Forms and Anti-Cheating Analysis for Electronic Truck Scales

【Abstract】Electronic truck scales serve as weighing equipment for the trade settlement of bulk goods, and the accuracy of their weighing results is directly related to the economic interests of both parties. However, the existence and development of cheating techniques pose a huge threat to metrological fairness, not only undermining the accuracy level of measuring instruments, but also directly destroying the value of metrological verification/calibration activities. This paper briefly reviews the development context of remote control cheating forms of electronic truck scales, aiming to strengthen research in this field with metrology colleagues and ensure the fairness and impartiality of metrology activities.

【Keywords】electronic truck scale; remote control cheating; rolling code; loRa; anti-cheating technology

引言

电子汽车衡是非自动衡器的一种型式，广泛应用于码头港口、矿山、冶金、化工、粮食、物资、交通等领域，称量范围一般是几十吨，即一辆货车及其上物品的总质量。由于其称重数据是双方货款支付的直接依据，因此对其要求很高，计量准确是根本。也是基于重大利益的原因，针对电子汽车衡的作弊行为，特别是技术含量高、隐蔽性强的遥控作弊，长期以来屡禁不止。这种违法犯罪行为不仅给企业带来巨额经济损失，且严重破坏了市场经济的诚信交易基本原则。

随着电子和信息化技术的不断发展、不断演化，电子汽车衡遥控作弊技术形成了一场持续改进的攻防对抗。本文旨在深入剖析这一对抗历程，从技术原理层面揭示作弊手段的升级路径，并系统总结与之对应的防护策略，以期为计量监管、设备制造和使用单位提供全面思考。

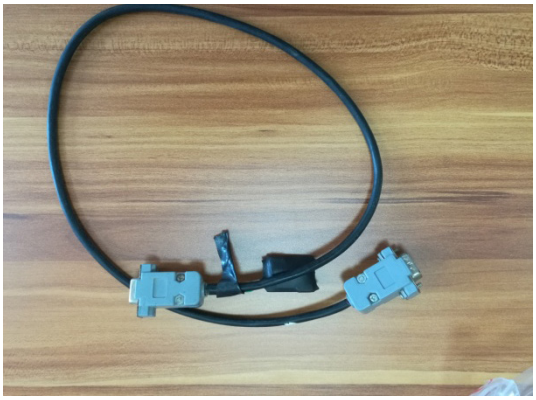
1　遥控作弊的技术特征和演变

1.1　遥控作弊原理与技术特征

早期及当前大部分简易遥控作弊装置。主要利用公共的ISM（工业、科学和医疗）频段，其中以315MHz 和433MHz 最为典型作为信号传输的方式。

通常汽车衡的关键部位安装接收电路装置，如称重传感器、或隐藏在传感器电缆接线盒内、或导线、或接线插头、或仪表内部。在电子汽车衡外部，操作者手持遥控器，在车辆行驶至承载器称重时，通过无线信号向接收装置发送指令。该指令通常直接作用于称重传感器的模拟信号或称重仪表的总信号线上，通过改变一个微小的、可控制的直流电压偏移，来改变最终的称重结果显示，如图1 所示。

（1）称重传感器加装接受电路形态



（2）仪表接口另增加导线形态

图1　电子汽车衡作弊形态

早期信号编码方式简单固定。多为PT2262/2272等通用编解码芯片，无任何加密措施。按下遥控器，重量立即增加或减少一定数值，操作简单直接。由于信号协议公开，使用廉价的无线信号分析仪即可轻松捕获、复制并重放攻击信号。

1.2　作弊形态的演变

从作弊形态看，电子汽车衡遥控作弊可分为三个阶段：

（1）固定频率模拟阶段。大致在2000–2010年，主要以315MHz、433MHz、418 MHz 等民用免授权频段为主，作弊设备通过复制称重传感器信号频率与编码，直接向称重仪表发射伪造数据，技术门槛低、成本低廉。

（2）编码加密破解阶段。大致在2010–2020年，随着称重仪表厂商引入简单加密机制，作弊者通过破解固定编码规则，开发匹配加密算法的遥控设备，实现对加密信号的伪造，典型代表为对跳频技术的初级破解。

（3）新型无线技术滥用阶段。2020 年以来，以滚动码、LoRa 等抗干扰能力强，传输距离远的无线技术被用于作弊，通过动态编码规避静态防御，利用低功耗广域网（LPWAN）特性扩大作弊范围，作弊隐蔽性与成功率显著提升。

1.3　相应防护技术与策略

针对此阶段的作弊手段，防护策略相对直接，核心在于“阻断”和“监测”。

（1）物理屏蔽与频率监测

金属屏蔽：对接线盒、称重仪表进行严格的金属密封和保护，避免非法识别的物理破坏和侵入。

频率干扰/ 监测：在汽车衡关键区域安装针对遥控信号多频主动式信号干扰器，或部署无线信号监测仪，实时监听该频段内的非法信号发射并报警。

（2）称重传感器与线路防护

称重传感器直接数字传输：采用数字化智能传感器。称重传感器内部直接将模拟信号转换为数字信号，并通过总线（如RS485）进行传输。外部注入的模拟电压干扰在数字域无法起作用。

电缆防护：使用带钢带铠装或金属导管的防护电缆，并尽可能埋地铺设，增加窃听和接入的难度。

2　滚动码技术与加密对抗

2.1　作弊原理与技术特征

为了规避固定编码易被侦测和复制的缺陷，作弊技术开始引入滚动码（Rolling Code）技术。滚动码技术的核心是“同步”与“变化”。

遥控器（发射端）和接收器内部预存一个相同的伪随机数序列和同步计数器。每次按下按键，遥控器不仅发送指令，还发送一个根据特定算法生成的、每次都不相同的滚动码。接收器接收到信号后，会验证该滚动码是否在预期的序列窗口内，如果是则执行指令，并同步更新自身的计数器。

采用滚动码的作弊装置使得每次攻击的信号内容都不同。即使监管部门捕获了一次攻击信号，也无法通过简单的重放（Replay Attack）来再次触发作弊，因为该码已被接收器视为“过期”。

2.2 相应防护技术与策略

对抗滚动码作弊，防护重心必须从“信号层面”提升至“协议与身份认证层面”。在称重仪表与称重传感器之间，乃至与远程监控系统之间采用双向身份认证机制。例如，在每次通信前，双方通过非对称加密算法（如RSA）或预共享密钥的挑战– 应答机制验证对方身份。

（1）双向认证与高级加密。对传输的所有指令和数据进行高强度加密（如AES 算法），即使信号被截获，攻击者也无法解密和伪造有效的作弊指令。

（2）设备数字指纹与可信度计算。为每一台合法的称重仪表和称重传感器赋予唯一的数字身份证（如基于硬件的安全芯片），所有关键操作（如修改标定参数）都需要通过数字签名验证。非法的接收装置无法通过身份认证，无法接入系统。

（3）行为审计与日志分析。称重仪表具备完善的安全事件日志功能，记录所有关键操作（如标定、按键、通信中断等）的时间戳和操作源。定期审计日志，可发现异常操作模式。

3 新的作弊形态：LoRa 等LPWAN 技术

3.1 作弊原理和技术特征

随着物联网（IoT）的兴起，LoRa（Long Range）等低功耗广域网（LPWAN）技术因其超远距离（数公里）、低功耗和强穿透性，开始进入作弊者的视野。

作弊者无须亲临现场，可在数公里外通过LoRa网络向预先植入的作弊模块发送指令，极大地降低了被抓现行的风险。LoRa 信号采用扩频技术，功率谱密度低，淹没在背景噪声中，传统的频段扫描仪难以有效侦测和识别。理论上，作弊者可以构建一个LoRa 网络，同时控制分布在不同地点的多个汽车衡上的作弊终端，实现规模化、有组织的犯罪。

3.2 相应防护技术和策略

面对此类基于先进通信技术的潜在威胁，反作弊防护体系必须走向智能化、网络化和一体化。

（1）终端加固。推行基于安全芯片的硬件安全模块（HSM），确保密钥存储和加密运算在物理上不可被读取和篡改。设备固件具备安全启动和远程安全升级能力，以修复潜在漏洞。

（2）通信安全。即使攻击者使用LoRa，防护的核心依然是加密和认证。在仪表与传感器、仪表与云平台之间的所有通信，必须强制使用基于TLS/DTLS 的加密通道和双向证书认证。

（3）智能监测。通过大数据分析与AI 构建称重数据云平台，利用大数据和人工智能算法对历史称重数据进行建模分析。系统可以自动学习特定车辆、特定线路的正常称重模式，一旦发现重量异常波动，皮重/ 毛重逻辑不合理，称重曲线异常等情况，立即触发预警。

（4）多源信息融合。将称重数据与视频监控（AI 行为分析）、车辆GPS 数据、货单信息等进行交叉验证，形成完整的证据链。

4 结论与展望

电子汽车衡的作弊形态与防护技术正经历了一条从“模拟信号对抗”到“数字加密对抗”，并正向“智能安全博弈”演进的清晰路径。未来的电子汽车衡，不应再被视为一个单独的计量器具，而应成为一个接入工业互联网的安全节点。通过技术、管理和法制的多重结合，持续迭代防护手段，才能在这场持续的技术博弈中占据主动。

构建多维度、多技术融合的反作弊体系，是应对汽车衡遥控作弊的关键。技术层面需强化动态加密与智能监测，监管层面需实现全流程数据管控，标准层面需明确技术禁区与协作机制。只有通过“技术+ 管理+ 标准”的协同发力，才能有效遏制遥控作弊行为，保障计量公平，维护市场良好秩序环境，为贸易计量最坚实的保障。

参考文献

[1] 孙梦翔. 计量作弊与预防初探[J]. 中国计量, 2009,2.

[2] 乔星南. 云加密在衡器中的应用[J]. 衡器. 2022,12.

[3] 马丙辉. 衡器的作弊特征及其对策研究[J]. 衡器. 2018,12.

作者简介

陆海兵，任职于启东市综合检验检测中心，主要研究方向是衡器计量及衡器安全防护等，具有较强的一线工作经验和反作弊技能。