

电子计价秤防作弊技术研究与应用

□李远斌

惠州市惠阳区质量技术监督检测所

【摘要】针对市场上电子计价秤作弊现象频发的问题，本文分析了作弊秤的生产特征与密码破解逻辑，提出基于硬件芯片读取与软件数据库协同的防作弊解决方案。通过研发快速读取密码的硬件装置，并配套开发生产企业-密码映射软件系统，实现基层计量技术机构检定人员和相关执法人员高效识别作弊秤的目标。

【关键词】电子计价秤；作弊密码；密码；硬件读取；软件数据库

文献标识码：A 文章编号：1003-1870（2025）09-0024-03

Research and Application of Anti-Cheating Technology for Electronic Pricing Scales

【Abstract】 In response to the frequent problem of cheating in electronic pricing scales on the market, this paper analyzes the production characteristics and password cracking logic of cheating scales, and proposes an anti-cheating solution based on the collaboration of hardware chip reader and software database. Through the research and development of hardware devices that can quickly read passwords and the development of manufacturer-password mapping software systems, the verification personnel and relevant law enforcement personnel of grass-roots metrological technical institutions can efficiently identify cheating scales.

【Keywords】 electronic pricing scale; cheating password; password; hardware reader; software database

引言

电子计价秤作为贸易结算的核心计量器具，其计量准确性直接关系到消费者权益与市场公平。然而，部分生产企业通过在单片机中嵌入作弊程序，利用密码切换正常/作弊模式，严重扰乱市场秩序。当前，基层执法主要依赖人工经验与逐次尝试密码，效率低下且覆盖面有限。因此，亟需探索智能化、系统化的防作弊技术路径，以应对日益隐蔽的作弊手段。

1 典型特征

当前市场上的作弊秤已呈现出以下典型特征：

（1）生产源头高度集中化

具有作弊功能的电子计价秤生产呈现显著的“窝点化”特征。据作者工作经验总结，约80%的作弊秤源自少数几家具备电子衡器生产资质的企业。这些企业虽持有合法营业执照与计量器具型式评价证书，但在利益驱动下，通过技术手段在生产环节预留作弊程序植入端口，给下游销售商或品牌代理商提供了正常电子计价秤变为作弊电子计价秤的可能性。为规避监管，多数企业常采用“一证多牌”策略：同一铭牌标识下，通过更换商标（如将正规品牌标识替换为无知名度的小众商标）、调整外观设计

(如改变秤体颜色、外壳材质)等方式,衍生出数十种“变脸”产品。这种“同一生产源头、多样产品形态”的模式,使得基层计量技术机构或执法人员难以通过铭牌或外观直接锁定问题企业。

(2) 密码体系复杂化与动态化

作弊秤的密码设置已从早期的固定模式演变为“企业差异化+地域动态化”的双重复杂体系:

企业间密码差异:不同生产企业采用独立的密码生成逻辑,部分企业甚至引入简单加密算法(如异或运算、字符位移)对密码进行二次处理。例如,某企业将基础密码“123456”与生产批次号后两位进行异或运算,生成最终密码“135789”。

地域性密码适配:同一企业针对不同销售区域(如华东、华南、华北)设置差异化密码。这种策略既便于企业控制作弊范围(如仅对特定地区经销商开放作弊功能),又增加了跨区域执法的破解难度。例如,某企业销往华东地区的秤体密码为“1234”,而销往华南地区的同一型号秤体密码则变为“5678”。

当前基层执法主要依赖人工经验与逐次尝试密码:执法人员需根据铭牌信息推测可能的生产企业,再通过“尝试该企业已知密码库”的方式解锁作弊程序。此方法存在三大痛点——效率低下,覆盖面有限(仅能识别已掌握密码的企业型号),这种被动应对模式已无法适应日益复杂的作弊手段,亟需探索智能化、系统化的技术解决方案。

2 破解电子计价秤作弊技术路径

针对上述问题,作者提出“硬件芯片读取+软件数据库协同”的智能化防作弊方案,从生产源头逆向破解密码,构建覆盖全行业的动态防控体系。

2.1 硬件层:芯片级密码读取装置研发

(1) 技术原理与实现路径

传统试密码方法依赖外部输入,效率低且依赖已知密码库。本研究提出通过硬件直连秤体芯片,直接读取存储密码的存储器数据,从根本上绕过密码试探环节。具体实现分为三个关键步骤:

物理接口适配:通过拆解典型作弊秤电路板,

定位存储密码的核心芯片(多为Flash存储器或EEPROM芯片)。利用微控制器(如STM32系列)设计专用接口电路,匹配芯片的通信协议(如I²C、SPI或UART)。例如,某品牌作弊秤的密码存储于型号为AT24C02的EEPROM芯片中,通过I²C总线与主控芯片通信,读取电压范围为1.7~5.5V,支持标准模式(100kbps)与快速模式(400kbps)。

数据协议解析:密码通常以加密形式存储于芯片特定地址空间(如0x0000-0x00FF)。需逆向分析秤体主控程序,确定密码存储的起始地址、数据长度及加密方式。常见加密包括简单异或运算(如密码“123456”与固定密钥“ABCDEF”逐字节异或)、字符位移(如ASCII码值+3)等。通过编写解密算法(如Python脚本或嵌入式C程序),可实现明文密码的实时转换。

抗干扰设计:为避免读取过程中因电磁干扰或电压波动导致数据错误,硬件装置需集成稳压模块(如TPS7A4700低压差线性稳压器)与信号滤波电路(如RC低通滤波器),确保通信稳定性。

(2) 技术优势

效率飞跃:相较逐次试密码,芯片读取可在(10~30)秒内直接获取密码,效率提升90%以上。

覆盖全面:通过适配主流芯片型号(如AT24C系列、W25Q系列),可覆盖约90%的作弊秤电路板设计。

技术难点:需逆向工程破解不同企业的硬件通信接口与加密算法,研发难度大且周期较长。秤体所用单片机采用动态加密或硬件级防护,需进一步攻关。

2.2 软件层:生产企业-密码映射数据库系统开发

(1) 系统架构与核心功能

为实现破解成果的快速应用与共享,配套开发云端管理平台,构建“生产企业特征库+密码库”的动态数据库系统。其核心架构包括:

1) 生产企业视觉特征库:通过图像采集设备(如高清摄像头)录入已破解秤体的铭牌、商标、键盘

分布等特征，利用卷积神经网络（CNN）训练视觉识别模型。例如，某企业铭牌字体为黑体、字号12pt、间距2mm，商标为圆形logo含“竹”图案，键盘布局为4×6矩阵且“去皮”键位于右下角——这些特征可转化为图像特征向量，输入模型实现95%以上的生产企业识别准确率。

2) 密码关联库：将生产企业信息（如名称、商标、生产批次）与对应的密码、使用说明（如“输入密码后按‘设置’键确认”）、破解案例（如“该企业2021年款秤体密码为年份后两位+销售区域代码”）关联存储。数据库支持模糊查询（如输入“竹牌”或上传铭牌照片），自动匹配最相似的生产企业及对应密码。

3) 用户交互与数据共享模块：基层执法人员注册账号后，可通过手机APP或网页端上传铭牌照片、手动输入企业名称或选择视觉识别结果，系统实时返回密码及操作指南（如“长按‘单价1’键3秒进入作弊模式”）。对于未破解的秤体，支持一键上传硬件读取数据（如芯片地址、加密密码），供技术团队协同分析。

（2）动态更新与协同机制

实时推送更新：定期（如每周）向用户推送新破解案例与密码更新包，确保数据库覆盖最新作弊型号。

同行协作网络：建立跨区域执法部门协作机制，对无法破解的秤体，由平台自动分配至技术团队或已掌握相关技术的单位进行联合攻关，破解成果实时共享至全网。

3 实施效果与社会价值

本方案通过“技术+数据”双轮驱动，构建了从生产源头到流通环节的全链条防控体系。硬件装置的便携性与软件平台的易用性，使基层执法人员能够快速掌握破解技能，摆脱对经验依赖。数据库的动态更新机制，实现了“发现一台、破解一类”的规模化防控效果。

4 结语

本研究提出的“硬件芯片读取+软件数据库协

同”方案，从技术根源上破解了电子计价秤密码的获取难题，构建了智能化、系统化的防作弊体系。其核心价值在于将被动应对转化为主动防控，为市场监管提供了高效、精准的技术工具。未来需进一步深化产学研合作，推动技术标准化与规模化应用，切实守护市场公平与消费者权益。

参考文献

- [1] 王建军, 李伟. 电子计价秤作弊手段分析与监管对策[J]. 计量技术, 2020(5):45-49.
- [2] 无锡市计量测试院. 基于机器视觉的电子秤作弊识别系统研究[R]. 无锡: 无锡市计量测试院, 2021.
- [3] 张敏. 嵌入式系统数据加密与解密技术[M]. 北京: 电子工业出版社, 2019.
- [4] 国家市场监督管理总局. 电子计价秤产品质量监督抽查实施规范[S]. 2022版.
- [5] Goodfellow I, Bengio Y, Courville A. Deep Learning[M]. MIT Press, 2016. (卷积神经网络基础理论)
- [6] Texas Instruments. I²C Bus Specification and User Manual[EB/OL]. 2020. (通信协议技术文档)

作者简介

李远斌，男，惠州市惠阳区质量技术监督检测所。