云加密在衡器中的应用

□上海耀华称重系统有限公司　乔星南

【摘　要】在衡器行业的发展历程中，防作弊一直是衡器厂家重点关注的对象，而随着作弊水平的不断提高，一些防作弊技术已经被破解。主要原因是传统的防作弊技术密钥的获取、验证是在本地进行的。不同以往，云加密防作弊技术借助云物联平台，密钥的获取、验证是在云服务器上进行的，作弊无从下手，真正做到了防作弊。

本文阐述了云加密技术的概念，通过与传统防作弊技术的对比，展示了云加密技术的防作弊效果，介绍了云加密系统的组成及应用，以方便理解。

【关键词】衡器；防作弊；云物联；云加密

引言

衡器行业是我国重要的基础行业之一，它的发展史是比较漫长的。改革开放以来，我国的衡器行业取得了长足发展，伴随着科技的高速发展以及应用水平的不断提高，特别是云物联（基于云计算的物联网）的快速发展，衡器行业，也迎来了新的发展方向。

目前，衡器行业推出了各种基于云物联的衡器，它们带有如远程安全报警、远程健康监测及诊断和远程重量显示等功能。用户可仅凭一部手机，便能了解到仪表的各种信息，此类物联网产品的应用，提升了用户的使用体验，为用户的使用带来了许多的便捷。

然而，在物联网衡器繁荣发展的背后也应该有新的思考，在提升用户体验的同时，怎么提升物联网衡器的防作弊效果?

纵观衡器行业的发展，作弊和防作弊一直是老生常谈的话题。究其原因不难发现，称量的结果和金钱挂钩，一些不法人员在利益的驱使下在衡器上动起了手脚。而衡器厂为了防止作弊或修复已被破解的系统，也需要对防作弊系统进行升级。两者的相互较量，使目前市面上作弊手段和作弊设备层出不穷。

1　非云加密防作弊技术

非云加密防作弊系统，如协议加密防作弊系统（图1），密钥存储在加密器的存储器中。使用时，先通过加密器把密钥分别写入到仪表和数字传感器的存储器中，再把仪表和传感器连接，进行密钥验证。

此类的防作弊技术，由于密钥的获取和验证是在本地（无网络环境下）进行的，仪表和传感器通信的过程中，加密和解密过程无法被监控到。因此，破解者可以通过反向工程等技术手段窃取密钥。

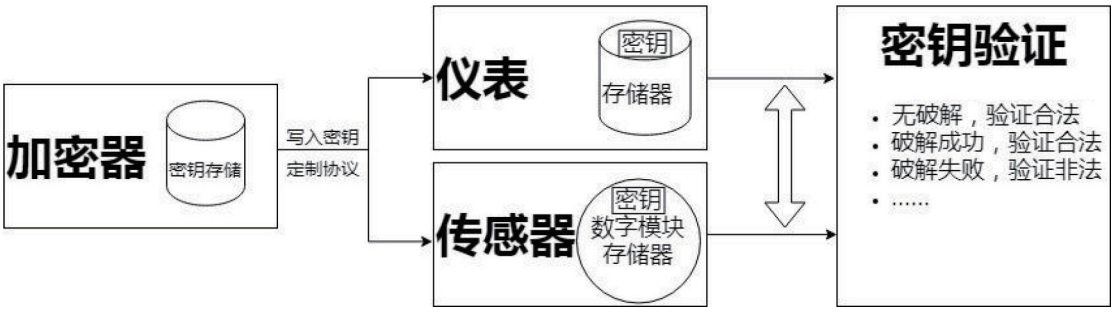

图1　协议加密防作弊系统

如图1 所示，被破解成功的仪表和传感器本身是无法感知的，而用户在可以正常使用和操作的情况下亦无法感知自己的设备已经被作弊，这种情况下会对用户造成严重的经济损失。如果作弊失败，仪表一般可以获取到作弊的信息并展示给用户，若是物联网仪表，则可以推送报警信息给用户。推送速度的快慢，分别由物联网仪表和用户接受设备的网络状况决定，防作弊功能比较被动。由此可见，此类防作弊技术无法真正做到防作弊。

2　云加密防作弊技术

物联网衡器带来的不仅是使用上的便捷，还带来了防作弊技术的新方向，即云加密防作弊。下面通过对比的方式来介绍云加密防作弊技术。

2.1　网络要求

云加密系统中，“云”字表明它需要网络。依托于云物联的云加密防作弊技术，应用时需要物联网仪表或加密器设备可以连接网络，非云加密系统没有网络要求。

2.2　密钥获取和验证

云加密系统中，使用加密器对仪表加密操作的密钥叫作“公钥”（图3），仪表首先在云服务器验证“公钥”的合法性，验证通过可以获得“私钥”，再使用“私钥”和传感器进行通信。不管是仪表“私钥”的获取，还是传感器“私钥”的生产，每个环节都需要云服务器验证，后面详述。非云加密系统则如图1 所示，获取和验证都是在本地进行的，这也是为什么非云加密系统无法真正防作弊。

总结以上，云加密防作弊技术是通过云服务器来获取和验证密钥的防作弊技术。

通过表1 回顾防作弊的发展，来更好地理解云加密的作用。

表1　不同的加密系统

加密方式	特点
早期数字系统	传感器和仪表之间通讯采用协议加密，容易加装作弊装置
动态加密系统	传感器和仪表之间通讯采用动态加密，不容易加装作弊装置
AES 动态加密系统	传感器和仪表之间通讯采用动态加密，配合阻抗匹配专利技术，很难加装作弊装置
云加密系统	传感器和仪表之间通讯采用云加密，无法加装作弊装置

3　云加密系统概述

如表1 所示，非“云加密”系统中，虽然AES 动态加密系统的防作弊等级最高，但只是很难加装作弊装置，并不是无法被破解的，而“云加密”系统却可以做到无法加装作弊装置。该系统之所以有极强的防作弊效果，下面从传感器的生产、密钥的存储和密钥的获取进行阐述。

3.1　传感器生产方式

在传感器的生产检测中，支持“云加密”通信协议的传感器会进行联网验证云密钥，只有验证合法的传感器，才被允许使用“云加密”的通信协议以及与计量相关的操作（图2），其目的是要从源头上杜绝非法的传感器流出。

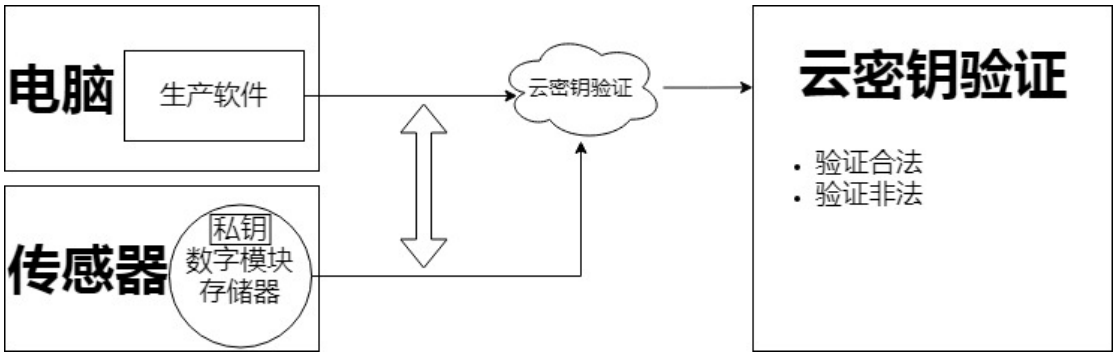

图2　传感器生产

3.2　密钥的存储位置

传统的协议加密系统密钥是存储在加密器的存储器中。不同以往，“云加密”系统需要有两个密钥来进行加密和解密，一个是公开的密钥（简称公钥），另一个是私有的密钥（简称私钥）。其中公钥储存在加密器中，私钥储存在云端服务器中（图3）。

3.3　密钥的获取方式

基于云物联的“云加密”系统，密钥的获取离不了网络的参与。用加密器给传感器和仪表使用“云加密”的通信方式后，“云加密”系统首先到云端服务器验证公钥的合法性，验证成功则可以获取到私钥，验证失败则无法获取到私钥（图3），然后用私钥进行验证通信。

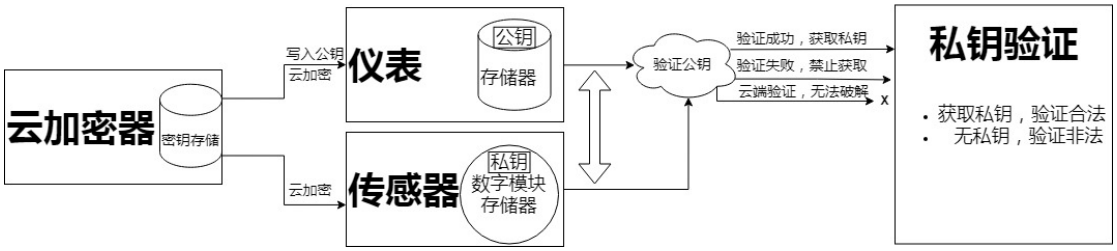

图3　云加密系统

“云加密”系统可以细分为在线“云加密”系统和离线“云加密”系统两种。所谓在线“云加密”系统，是指该系统中的仪表本身可以连接网络，具有物联网的功能，可以通过仪表的网络验证、获取云密钥。离线“云加密”系统，是指该系统中的仪表本身不可以连接网络，不具备物联网的功能，只能通过借用加密器的网络来验证、获取云密钥。

之所以有这种区分，是从用户的角度出发，让

用户在可以使用到“云加密”系统的前提下，根据自身的需求来选择使用在线“云加密”系统还是离线“云加密”系统。比如需要物联网功能的用户，可以使用在线“云加密”系统，而现场网络不好并且不要物联网功能的，可以使用离线“云加密”系统。

下表2 列出了“云加密”系统的硬件组成。

表2　云加密系统的硬件

	在线“云加密”	离线“云加密”
支持的仪表	 DS10  DS12	 DS17
支持的加密器	 TS3  TS4	 TS4（需联网）
支持的传感器	 V5版  V6版	 V6版

4　云加密应用

以DS10 仪表、DS17 仪表、TS4 加密器和V6 版数字传感器（以下简称V6 传感器）为例，分别介绍在线“云加密”、离线“云加密”的应用。其中，DS10 仪表具有物联网功能，应用于在线“云加密”场景。DS17 仪表不具有物联网功能，应用于离线“云加密”场景。

4.1　在线“云加密”应用

需注意，加密使用时，TS4 加密器要在可用状态。基于安全和管理考虑，TS4 加密器如果网络离线并且剩余天数或次数为0，不允许进行加密操作。另外，DS10 仪表因为要联网验证获取云密钥，所以要保证DS10 仪表网络在线，即仪表的指示云灯显示绿色。

使用TS4 加密器分别对仪表和传感器加“云加密”通信协议，仪表会自动采样，到云端认证并获取云密钥（私钥），获取成功后进行“云加密”协议的通信，完成在线“云加密”的操作。

4.2　离线“云加密”应用

需注意，由于DS17 仪表不具备联网功能，因此要保证TS4 加密器处于网络在线的状态，以使DS17 仪表通过使用TS4 加密器的网络去获取云密钥。

使用TS4 加密器为传感器加“离线云加密”通信协议，把传感器和仪表连接，使用TS4 加密器为仪表加“离线云加密”通信协议。仪表会自动采样，然后到云端认证并获取云密钥（私钥），获取成功后进行“离线云加密”协议的通信，完成离线“云加密”的操作。

虽然“云加密”系统的逻辑复杂，但“云加密”系统的操作和传统防作弊系统的操作方法类似，只需要使用加密器进行加密操作即可。“云加密”系统使用简单，对用户来说无学习成本。

5　云加密的意义

任何防作弊系统的初衷都是为了维护用户的利益。但随着破解手段的不断升级，传统意义的防作弊系统正在或者已经被攻破，此时，迫切需要一种新的，真正行之有效的技术来解决作弊问题。

“云加密”系统有重重的密钥和验证。不仅传感器的生产需要在云端进行验证，而且加密后系统还需要在云端验证获取密钥。这种加密机制让破解者无从下手，进而杜绝了作弊的可能。

因此，做到真正的防破解、防作弊便是“云加密”系统存在的意义。

作者简介：乔星南，男，汉族，河南省商丘市人，2017 年毕业于安阳工学院，学士，主要从事嵌入式研发。