论文引用格式：邓劼，戴文飞，陈伟业．基于标识密码技术的物联网安全解决方案[J].现代电信科技，2017,47(4)：46-50.
DENG Jie, DAI Wenfei, CHEN Weiye. Internet security solution based on identity cryptography [J].Modern Science & Technology of Telecommunications,2017,47(4):46-50.

基于标识密码技术的物联网安全解决方案

邓劼[1]，戴文飞[1]，陈伟业[2]
（1.中移铁通有限公司政企客户中心，北京 100033；2.工业和信息化部应急通信保障中心，北京100804）

摘要：对目前物联网安全现状和风险进行了分析，介绍了一种全新的基于标识密码技术的物联网安全解决方案，并详细阐述业务的具体技术实现方式和实施部署的策略。通过同现有物联网的对比分析，就基于标识密码技术安全方案的技术原理、特点和优势作出重点的说明，并介绍了将该方案扩展到智能家居和工业控制等领域的应用。

关键词：物联网；安全；标识密码技术
中图分类号：TN915.08　　**文献标识码**：A

Internet security solution based on identity cryptography

DENG Jie[1], DAI Wenfei[1], CHEN Weiye[2]
（1.Client Center of Government and Enterprises of China Mobile Tietong Co., Ltd., Beijing 100033;
2.Emergency Communication Security Center of MIIT, Beijing 100804）

Abstract: This paper analyzes the present situation and risk of the Internet of Things security, introduces a new security solution of Internet of Things based on the Identity-Based Cryptograph technology, and elaborates the concrete technology realization mode and the implementation strategy of the business. Through the comparative analysis of identity authentication, data security, management control etc. and based on the technical principle, characteristics and advantages of the cryptographic technology security scheme, it introduces the scheme to the intelligent home and industrial control and other fields of application.

Keywords: Internet of Things; security; Identity-Based Cryptograph

1 物联网安全背景分析

物联网在蓬勃发展的同时，其背后隐藏的安全问题也逐渐凸显出来。物联网的应用在某种程度上需要依赖互联网或者 TCP/IP 网络，物联网环境中从硬件层到软件应用层均可能存在安全隐患。就目前人们普遍使用的智能家居设备来看，其安全控制单纯使用物联网芯片的加密技术，难以实现完整的解决方案，存在安全的短板。而随着信息化系统的复杂程度越来越高，系统脆弱点和漏洞越来越多，单一的安全技术已不能保障系统的安全性。近几年许多影响巨大的信息安全事故充分说明，系统越复杂存在安全漏洞的风险也就越高。密码技术来作为信息安全的最关键防线，可以快速、经济地解决敏感数据保护的问题。

在传统的安全解决方案中，用户的身份认证常采用用户名密码认证或采用PKI/CA 技术实现，此

方式难以实现对海量用户的支持，同时难以在一些低端的智能设备里面实现，所以很难在物联网安全中得到广泛的应用。因为 PKI/CA 系统中需要为每一个设备、智能终端都要颁发数字证书，在使用过程中还需要交换对方的证书，在物联网这种用户数巨大、点对交互频繁而随机的使用场景下，需要维护管理大量证书、进行在线交换，整体建设和维护成本非常之高，难以普及。

本文提出的方案是基于标识密码技术构建，使用标识密码算法（国家 SM9 算法），结合一系列软硬件产品，形成物联网安全整体解决方案，可快速实现安全通道、安全存储、数据加密、身份认证、数字签名等功能。

2 物联网现存的安全问题分析

2.1 身份认证存在弊端

在物联网系统中，身份认证包括设备之间的认证、设备与用户之间的认证。在传统的身份认证方式中，普通的用户名和密码认证方式，无法避免弱口令、撞库攻击、字典攻击等问题，大多数用户也没有定期更改密码的习惯；而采用数字证书认证虽然安全，但使用繁琐，在终端设备上安装控件或 KEY 驱动和管理程序等，使用极其不便。表 1 是现行的各种身份认证方式存在的弊端分析。

综上，要解决这些问题，需要一种兼顾易用性、安全性与兼容性的身份认证技术。

2.2 数据传输安全风险

物联网系统中数据传输方式有两种，明文传输和通道加密，其安全风险分析如下。

（1）数据明文传输

大量摄像头、智能家居等物联网系统中，数据明文传输，一旦网络被监听，数据即被窃取。

（2）SSL 通道传输

表 1 现行身份认证方式弊端分析

身份认证方式	弊端
普通口令认证	弱口令、口令截获、字典攻击、撞库、拖库
手机短信认证	认证费用高、伪基站、短信劫持、手机病毒
数字证书认证	部署成本高、必须安装插件、易用性不高
动态令牌	成本高、用户认证依赖独立设备、易用性不高、服务端密钥存在安全风险
指纹、虹膜等生物识别认证	部署成本高、终端适配要求高、实现难度大、易用性不高

SSL 通道传输使用协商密钥来加密传输的数据。首先，SSL 协议本身被曝光很多漏洞，如握手进程缓冲区溢出漏洞、心血漏洞等，协议本身就不能保证安全；其次，SSL 通道建立过程未进行双向认证，即存在中间人攻击（黑客拦截 SSL 建立过程，伪造服务端与用户端的身份）的风险；此外，SSL 还存在管理配置不当、SSL 可降级明文访问等问题。因此，需要一种更安全的传输协议，来保证数据传输过程安全可靠。

2.3 缺少严格的访问控制与授权管理

通过逆向分析、网络活动分析等手段可以判断出控制设备的标识和指令，这些指令如果没有防重放的参数是可以直接使用的，剩下的就是看能否越权控制该设备。整个控制过程中如果没有绑定关系、或者设备标识有规律可寻，此时根据一个或者多个设备控制标识就可以预测出其他设备控制标识（如将 mac 地址作为设备控制标识符），从而横向控制大量的智能设备。其实，在强身份认证的前提下，配合基于用户名、设备 ID、组织、IP、端口的访问控制，这些问题是可以得到解决的。

2.4 数据安全问题

物联网系统中数据本身的安全也存在问题，机密性、完整性不够，不支持抗抵赖。如果数据本身未

加密，那么服务端存储的数据、中间传输的数据、用户端存储的数据，都可能会被盗走。此外存在数据篡改、伪造等问题，因此需要密码技术来实现数据本身加密，及数据哈希验证、签名抗抵赖等安全防护。

3 基于标识密码技术的解决方案

3.1 方案概述

本方案基于IBC标识密码技术，综合使用国密SM3/SM4/SM9系列算法，结合CHAP挑战应答、NTLS安全传输协议等安全机制，可以快速实现安全通道、安全存储、数据加密、身份认证、数字签名等功能，解决物联网系统中身份认证、数据安全、传输安全、访问控制等安全问题，形成完善的解决方案。

SM9标识密码算法以物联网设备ID、用户手机号等一切唯一的标识作为公钥，无需数字证书，安全分发专属私钥。SM9标识密码算法与SM4对称密码算法相结合，实现数据加密保护；SM9标识密码算法与SM3摘要密码算法相结合，实现数据完整性验证与抗抵赖。真正做到以密码技术为核心，从根本上解决物联网的安全问题。

3.2 方案架构

图1是基于标识密码技术的解决方案的架构图。

（1）密钥管理基础设施

密钥管理基础设施包括标识密码机和管理平台，可提供SM3/SM4/SM9算法运算与密钥生成的功能。密码机采用具备国密型号的专用硬件设备，管理平台采用具备国密型号的专用密码管理软件系统。

（2）安全运营平台

安全运营平台是一个提供多种功能的云端运营管理平台，可实现用户的身份认证、基于用户标识的授权管理、用户远程接入的P2P安全加密传输、用户与设备的监控审计等功能。

（3）终端APP

终端APP集成安全中间件，具备私钥下载与存储、安全认证、安全接入等功能。用户可以使用终端APP远程安全控制物联网设备。

（4）物联网设备

包括摄像头等物联网设备集成安全中间件，下发设备私钥，认证设备身份，并在原有功能的基础上新增安全接入与数据加密等安全功能。

（5）中间件

安全中间件（SDK）分为服务端、终端、设备端三种，均包含有多种安全接口，与物联网系统中的APP、设备系统结合后，可提供基于IBC技术身份认证、数据加密、数字签名、NTSL安全通道等功能，可支持Android、iOS、Wndows、Linux系统，也可以支持X86、MIPS、ARM的各种智能硬件。安全中间具有很强的灵活性，还能支持嵌入式系统及芯片实现安全应用。由于安全中间已经封装好了很多不同功能的接口，软件系统可直接调用，调试简单。

3.3 安全功能

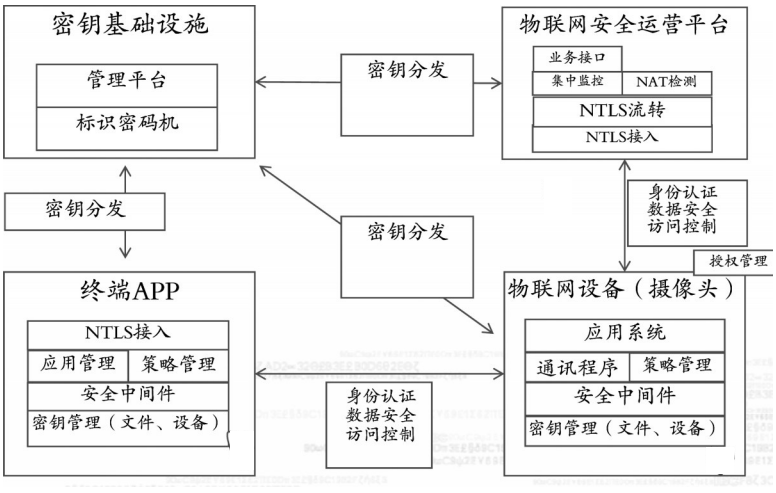

图1 解决方案架构图

基于标识密码技术的解决方案具有多重安全防护功能。

(1)强身份认证

以设备ID或者用户手机号为标识公钥,分发专属私钥,无需证书认证等繁琐的过程,使用私钥签名、公钥验签的方式,再结合CHAP挑战应答机制,实现强身份认证。此外,认证过程无用户名密码传递,杜绝了弱口令、暴力破解、撞库攻击等安全问题,并且因为标识即是公钥,无需证书交换认证过程,在安全的前提下,又兼顾的易用性。认证SDK适用于Linux、Windows和iOS等多种系统,开发要求不高,兼容性高。认证过程如图2所示,适用于用户、设备、云端平台之间多种身份认证过程。

(2)加密传输

此方案在标准安全传输协议TLS的基础上,优化握手过程,结合SM9国密算法,形成了NTLS下一代安全传输协议。该协议传输效率高、支持海量并发;并且因为使用了SM9算法实现双向认证,并且加密了密钥协商过程中的交换密钥,杜绝了中间人攻击等安全风险。此外,云端平台支持握手过程的转发,当物联网设备不具备公网IP等情况下,支持数据转发或者NAT穿墙,在用户与设备之间建立P2P(点对点)加密通道。

(3)访问控制与授权

由于SM9算法中标识即是公钥,代表了用户、设备的身份,因此,基于标识可以方便的实现访问控制。NTLS安全传输协议支持基于IP地址、TCP、UDP、端口来设置访问权限,建立通道后,客户端只能访问服务端指定的内容,其他拒绝访问。适用于设备接入云端平台、设备之间互相访问、用户与设备之间的访问等多种过程,避免了越权访问、横向控制等多种问题。

(4)数据安全保护

支持基于数据本身的加密、签名,从根本上实现安全防护,即使数据被监听、窃取,因为数据加密,也不会导致泄密。同时,数据电子签名验签保证数据在传输、存储过程中不会被篡改,也认证了数据发送方的真实身份,实现抗抵赖。

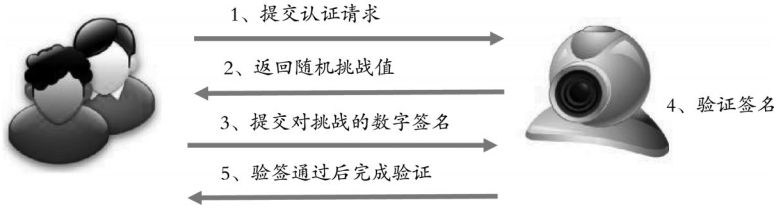

图2 强身份认证流程

3.4 方案部署(功能实现)

图3是基于标识密码技术的解决方案具体部署的拓扑图,各部分功能如下。

(1)密钥基础设施:国密型号的标识密码机与标识管理系统,提供密钥生成与算法运算等服务。

(2)运营管理平台:在原摄像头云端平台的基础上,增加安全接入、身份认证、授权管理、集中监控等多种功能。提供用户身份认证、设备在线状态查询、加密通道建立等多种安全服务。

(3)摄像头:在原摄像头基础上,集成IBC SDK开发包,支持私钥认证、通道建立、数据加解密、签名验签等多种功能。

(4)终端(手机、电脑)应用:用户远程连接、查看、控制摄像头的应用程序,同样支持私钥认证、通道建立、数据加解密、签名验签等多种功能。

3.5 方案优势

本方案在实现强身份认证、数据安全保护等安全性前提下,兼顾系统的易用性、兼容性、可靠性与扩展性。(1)安全性:身份认证、数据传输、数据存储全方位安全保护,综合使用过密SM系列算法;(2)兼容性:SM9算法标识即是公钥,无需数字证书,硬件性能

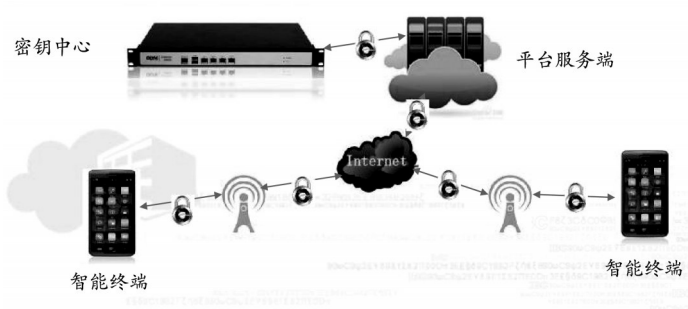

图3 方案部署拓扑图

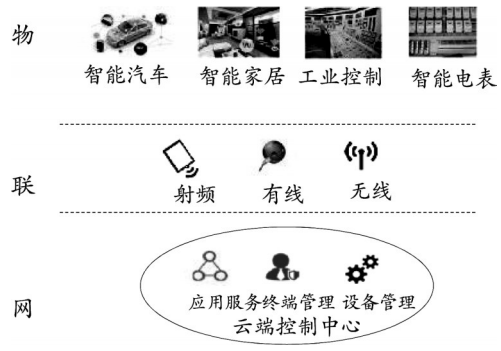

图4 物联网综合场景示意图

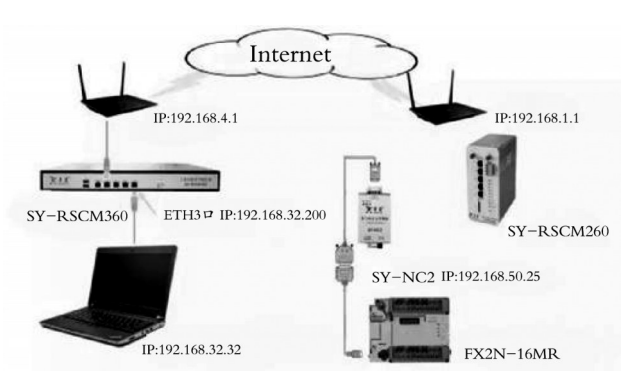

图5 基于标识的密码技术在工业控制场景应用示意图

要求低，支持各类架构的芯片，如 MIPS、ARM、X86；(3)高性能：标识密码算法相对于传统非对称算法在加解密、签名验签速率方面明显提升；(4)扩展性：支持冗余、扩展、备份等功能，可实现无限扩展升级运营级的管理架构，易于构建运营服务模式。

4 方案拓展

由于标识密码技术轻管理、易加密等特点，再加上技术成熟、接口丰富，方案支持智能家居、工业控制、车联网、智能电表等多种物联网场景的拓展。具体见图4。

4.1 智能家居

在智能家居场景中，家庭路由器升级为智能安全网关，实现用户强身份认证、安全接入、访问控制等安全功能。用户通过客户端应用程序，认证身份后，建立加密传输通道，可以访问指定的家庭网络中的其他家具设备，包括IP-TV、摄像头、空调、冰箱等一系列基于网络访问的设备(如图5所示)。

4.2 工业控制

在工业控制元件中集成本方案软件开发包，以设备ID为标识公钥，写入设备私钥，基于标识实现设备识别与访问控制，结合安全传输协议，可以实现远程访问，数据全程加密(如图5所示)。

参考文献

[1] 李向军. 物联网安全及解决措施[J]. 农业网络信息, 2010(12):5-7.
[2] 黄华. 基于Web应用的统一身份认证系统设计与实现[D]. 电子科技大学, 2012.
[3] 朱波, 张琳. 物联网环境下的控制安全技术探讨[J]. 消费电子, 2014(24).
[4] 刘旭. 基于Portal协议的安全认证接入的设计与实现[D]. 西安电子科技大学, 2013.
[5] 丁士杰, 谢军, 木薇. PKI在企业电子商务中的应用研究[J]. 电子测试, 2016(1):127-128.

作者简介

邓　劼：中移铁通有限公司政企客户中心业务经理，高级工程师，主要从事物联网产品的研发和推广。
戴文飞：中移铁通有限公司市场经营部业务经理，高级经济师，主要从事产品和渠道分析，智能家居产品研究。
陈伟业：工业和信息化部应急通信保障中心助理工程师，多年从事应急通信指挥调度系统运行维护管理相关工作，对通信技术业务发展、应急通信系统建设与运行维护等有比较深入的研究。