基于PKI和CPK的RFID系统混合密钥管理机制研究

张 兵[1]，秦志光[1]，万国根[2]

(1. 电子科技大学计算机科学与工程学院 成都 611731；2. 成都大学信息科学与技术学院 成都 610106)

【摘要】现有的RFID系统密钥管理通常基于RFID系统某一层设计，缺乏一种通用的架构和统一的密钥管理机制。该文基于RFID系统架构和组成元素，提出基于PKI和CPK的混合密钥管理方案。该方案对RFID设备与实体进行统一标识，建立统一的标识空间和统一的密钥空间，同时，将PKI密钥管理技术应用于RFID系统的后端系统，解决传统互联网身份认证和RFID后端现有安全方案的兼容问题；将CPK密钥管理技术应用于RFID系统的前端系统，实现前端系统密钥的“集中生成和分散存储”，解决RFID系统处理对象多、单个对象资源少，对象之间可以直接证明标识的真伪而无需第三方参与的安全需求问题。提出的密钥管理架构和密钥管理机制可以应用于设备大规模部署、需要设备直接认证和离线认证的RFID系统中。

关 键 词 CPK；密钥管理；PKI；RFID

中图分类号 TP301 文献标志码 A doi:10.3969/j.issn.1001-0548.2015.03.017

Study on Hybrid Key Management Mechanisms of RFID System Based on PKI and CPK

ZHANG Bing[1], QIN Zhi-guang[1], and WAN Guo-gen[2]

(1. School of Computer Science and Engineering, University of Electronic Science and Technology of China Chengdu 611731;
2. College of Information Science and Technology, Chengdu University Chengdu 610106)

Abstract The previous key management mechanisms in RFID systems are usually based on a certain layer, and lack of a common framework and a unified key management mechanism. In this article, a unified hybrid key management mechanism of RFID systems based on PKI and CPK is proposed. In the mechanism, the terminal nodes are identified according its tag, a unified identity space is established, and a unified key space is established. At the same time, PKI key management technology is used for the back-end devices of RFID systems to solve the compatibility problem of traditional Internet authentication and the existing security solutions; CPK key management technology is used for the front-end devices of RFID systems to implement the "centralized generation and distributed storage" management of the front-end key, and the security issues are solved because there are more processing objects in the RFID system, less resource in a single device, and need more direct proof of identification of the authenticity of the device without the third party. The presented techniques can be used in the RFID applications that require large-scale deployment of equipment, equipment direct certification and offline certification requirements.

Key words CPK; key management; PKI; RFID

随着RFID技术的广泛应用，RFID系统安全问题也日益凸显[1]。RFID系统涉及服务器、读写器、标签、网络、数据库系统及业务系统等多种对象，其中，RFID标签资源较少，计算能力较低，存储空间较少，难以在其上采用一些目前在传统安全领域已被证明是成熟的安全性比较高的加密算法和安全技术，导致RFID标签易被假冒、篡改、泄漏；其次，RFID标签与读写器之间通信主要采用无线射频通信技术，因其无线通信信道的开放性，所以存在泄露标识对象隐私和数据的危险[2]。

密钥是安全的基础。大型RFID系统中设备种类多，数量庞大，设备的计算能力、存储能力也大不相同，设备之间存在直接认证、离线认证需求[3]。因此，研制恰当的密钥管理体系架构和管理机制，实现大规模环境下不同设备均有密钥，并根据密钥进行直接认证、离线认证，是确保RFID系统安全的重要内容。

本文基于RFID系统组成元素和网络体系架构，

收稿日期：2014－01－07； 修回日期：2014－09－13
基金项目：国家863项目(2008AA04A107)
作者简介：张兵(1973－)，男，博士生，主要从事信息和网络安全、RFID应用与安全方面的研究.

提出RFID系统密钥管理架构和基于PKI和CPK的混合密钥管理机制。

1 RFID密钥管理的相关研究

密钥管理包括密钥的产生、装入、存储、备份、分配、更新、吊销和销毁等环节[4]。目前，针对RFID系统的密钥管理通常有两种不同的方式[5]：1) 集中式管理模式。由特定组织(密钥管理中心)对密钥进行生成、分发、吊销与更新；2) 分布式管理模式。建立区域管理中心，通过分簇分层次方式对密钥进行管理。集中式管理模式实现较为容易，但对密钥管理中心的处理能力和安全性要求高，而分布式方式较适用于设备地域分布广，具有区域聚集特征的RFID系统，但对汇聚节点或网关的要求比较高，存在成本和开销问题。在实现方法上，RFID系统的密钥管理通常采用固定的方式，例如，采用基于对称密钥的方法或者采用非对称密钥方法[6]。采用对称密钥方法主要有SPINS协议[7]、基于密钥池预分配的E-G方法、单密钥和多密钥空间随机密钥预分配方法等；采用非对称密钥方法的密钥管理主要有MICA2[8]。

近几年来，PKI[9](public key infrastructure)和CPK[10-11](combined public key)技术逐步应用到RFID系统中。文献[12]提出一种基于PKI的物联网安全模型，该模型在EPC网络的传输层和应用层引入一个经过简化的PKI模块，实现通信过程中的身份认证和加密传输服务；文献[13]提出采用CPK技术和对称加密算法，并基于芯片级操作的方案来构建身份认证系统，实现了感知层设备的身份认证和数据加密；文献[14]基于PKI和IBE提出一种物联网安全传输机制，实现了物联网后端系统的安全数据传输。以上方法的缺陷是只能应用于RFID系统的某一层次，缺乏一种通用的架构。

在RFID系统中，设备数量庞大，而且系统资源和处理能力又大不相同，特别是前端系统和后端系统，常常采用不同的通信机制和设备管理方式。因此，在RFID系统中，很难采用单纯一种方式来管理密钥。然而，如果由于安全机制不同造成系统联通性差，则必定会影响系统使用。因此，需要在系统建设中实现前端系统和后端系统在密钥管理中的有效集成，和速度、能耗、处理能力以及安全性的整体优化。

2 RFID系统密钥管理架构

2.1 RFID系统基本结构

RFID系统包括前端系统和后端系统[15]，其基本结构如图1所示。

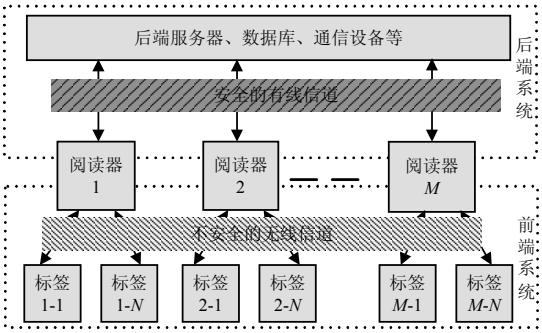

图1 RFID系统基本结构

前端系统包括RFID读写器、RFID标签等设备，后端系统包括RFID中间件、服务器、系统软件、数据、网络用户等设备。前端系统的标签存在资源限制，难以在其上采用传统的安全加密算法；读写器实际工作在后端系统和前端系统之间，相比于前端的标签，拥有更多的CPU、内存资源；后端系统服务器、数据库通信设备等通常具有较多的处理资源。因此，RFID系统密钥管理应考虑这些不同实体设备的需求，从提高整个系统的安全性能和适应性出发，采用不同的方法。

2.2 RFID系统密钥管理架构

本文提出RFID系统密钥管理方案由安全中心(security center, SC)、安全网络通信中间件(middle communication component, MCC)、安全读写器(reader, R)和安全标签(tag, T)组成，如图2所示。

1) 安全中心。主要任务完成密钥的生成、分发、存储、恢复、更新、销毁等，以及对整个RFID系统进行安全监控、身份认证等。安全中心包括密钥管理中心、标识管理中心等设备，如图3所示。为了提升系统处理能力，安全中心可实行分级管理，例如在分中心部署认证服务器，实现设备接入与认证，会话密钥生成等操作。

2) 标识管理中心。对整个RFID系统的标识进行管理。RFID系统的标识包括系统中所有的服务器、读写器、用卡设备、RFID标签等。标识管理中心主要包括标签管理服务器、发卡终端等。

3) 密钥管理中心。主要由密钥管理服务器、密钥发布服务器、身份管理服务器、管理终端等部分组成，用于实现设备密钥、公私钥因子矩阵、密钥库以及身份库的生成、存储与分发等。

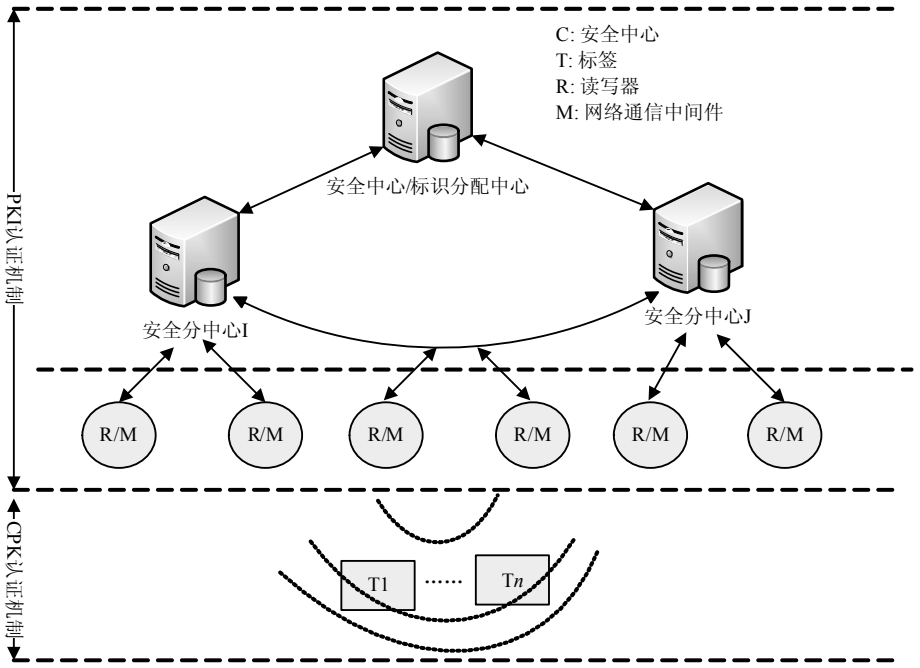

图2　基于PKI和CPK的混合密钥管理方案架构

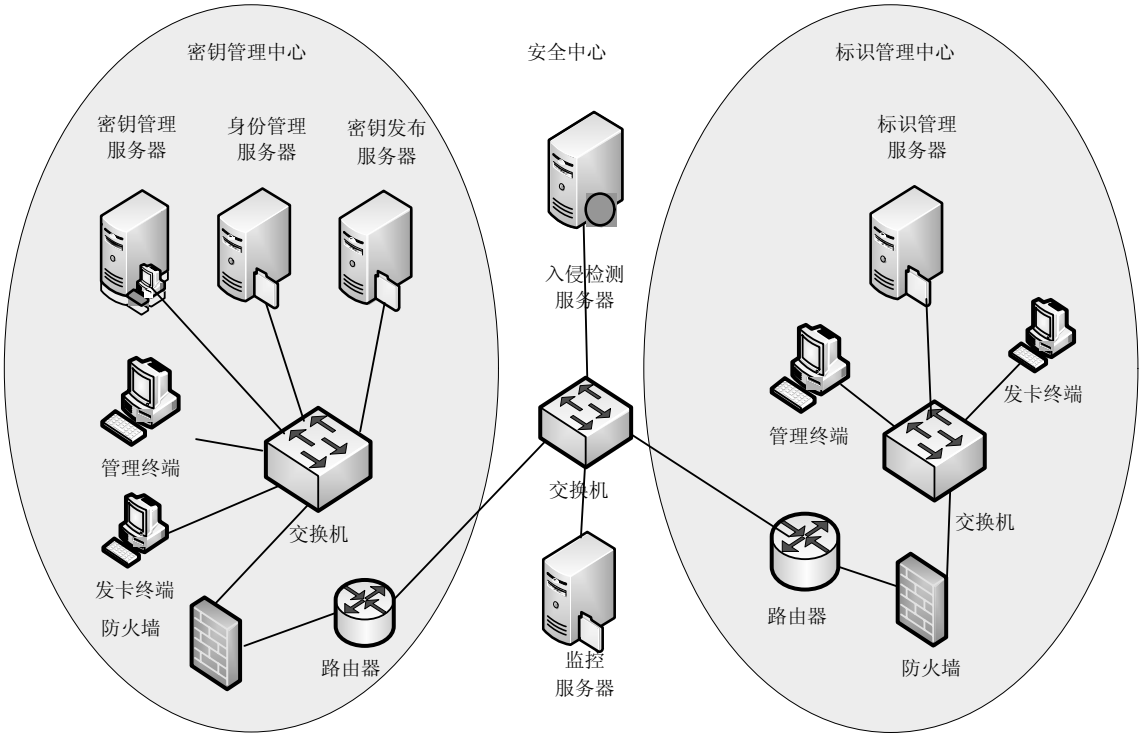

图3　安全中心组成

4) 安全读写器。主要任务是实现标签的安全接入以及数据转换。读写器使用安全协议，通过有线/无线/接触等方式将命令、业务数据等发给RFID标签(或其他含有标签的智能密码卡)，对标签进行验证处理，验证完成后传至后端管理系统。读写器中被保护的数据包括3种类型：与后端系统进行相互认证的密钥、与标签进行相互认证的密钥，与标签相关的数据、自身的数据和执行代码。

5) 安全网络通信中间件。主要任务是对送往后端系统的数据进行校对，进行读写器协调、数据传送、数据存储等操作。中间件存在两种形态：一种为一个物理实体，其与安全读写器共用标识密钥；

另一种是单独的一台 PC，具有单独的标识密钥，其与安全中心之间的身份验证方式与各个安全中心之间的身份验证方式类似。

6) 安全标签。安全标签是嵌入有密钥和安全协议的标签。安全标签的标识由标识管理中心统一管理，密钥信息由密钥管理中心管理。安全标签中的数据包括:标签标识、标签私钥、读写器密钥矩阵、业务数据和执行代码等。本方案的安全标签主要是指具有较多的计算资源和存储资源的有源标签，需要嵌入密钥和 CPK 密钥矩阵，并具备安装认证加密协议条件，以实现与读写器进行实体认证与通信。

3 PKI与CPK混合密钥管理机制

3.1 统一的密钥空间

本方案为RFID系统中的每个实体赋予一个加密密钥，因此，需要建立全系统统一的密钥空间，并对系统中所有实体的密钥进行统一管理。

每个实体都需要建立标识。标识可以是标签的ID、服务器的MAC地址，管理人员的EMAIL，对于没有物理标识的设备(如读写器、中间件)，可以为其赋予一个临时值TRID。所有实体的标识统一编码，形成RFID系统的实体标识空间，并通过转换，建立RFID系统的密钥空间。标识空间与密钥空间的映射关系如图4所示。

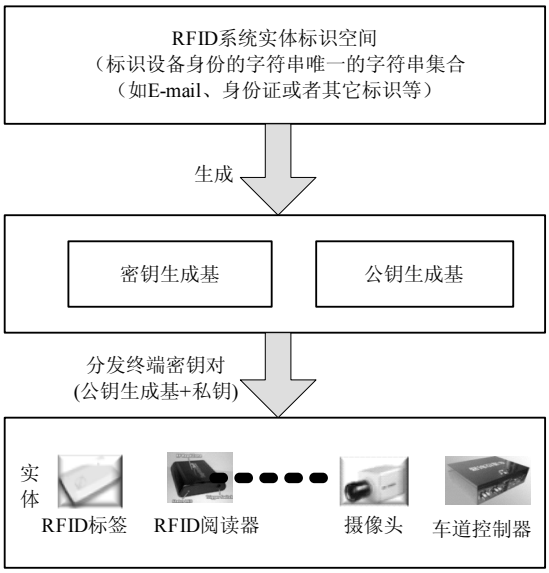

图4 基于标识的密钥生成

所有参与实体，包括前端的读写器、标签，后端的服务器、中间件、网关设备、交换设备，甚至软件系统、使用人员等均赋予一个唯一标识，然后由所有标识建立标识空间。密钥管理中心根据实体设备的标识生成密钥生成基和公钥生成基，生成私钥，并通过安全信道将私钥写入RFID标签、读写器等设备中。

3.2 混合密钥管理机制

RFID前端系统和后端系统分别采用不同的密钥管理机制。前端系统采用CPK的密钥管理机制，后端系统采用PKI机制，如图5所示。

图5 混合密钥管理机制

3.3 密钥存储方式

前端系统和后端系统的密钥存储方式如图6所示。

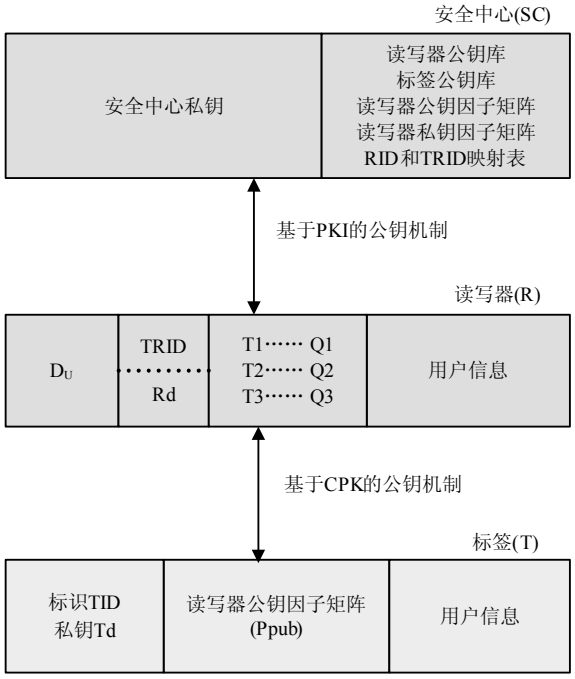

图6 密钥分配存储位置

1) 安全中心。安全中心存放了安全中心的私钥，读写器、标签的公钥库和公私钥因子矩阵，建立身份ID与读写器和标签密钥的映射关系。

2) 读写器。读写器工作在后端系统和前端系统

之间，因此，需要与后端的中心设备和前端的标签分别进行双向身份验证。读写器需要存储向上私钥(读写器与中心进行身份认证的读写器私钥)和向下私钥(读写器与标签进行身份认证的读写器私钥)、TRID、安全中心公钥、所属的标签公钥以及这些密钥与身份ID的映射关系。

由于读写器没有自身的唯一标识，因此由安全中心随机生成TRID作为其标识，然后使用TRID根据映射矩阵从私钥因子矩阵中取出相应私钥(读写器向下私钥)写入读写器。

在图6中，TRID为读写器标识，Q_i为其范围内的标识为T_i的标签的公钥，D_u为向上私钥(读写器与安全中心进行身份认证的读写器私钥)，D_d为向下私钥(读写器与标签进行身份认证的读写器私钥)。

3) 标签。标签需要存储自己的标识私钥和读写器的CPK公钥因子矩阵。标识私钥存放到安全区，公钥因子矩阵存放到用户区。公钥因子矩阵在安全中心一次性生成，在制卡过程中，写入标签。

3.4 密钥生成方式

密钥由两种密钥生成方案生成。方案*A*：PKI体制的密钥生成；方案*B*：CPK体制的密钥生成。如表1所示。

表1 密钥生成方案

设备密钥	密钥生成方案
安全中心密钥	方案*A*
中间件密钥	方案*A*
读写器向上密钥	方案*A*
读写器向下私钥/公钥因子矩阵	方案*B*
标签私钥/标签公钥因子矩	方案*B*

安全中心所需的密钥及网络通信中间件所需的密钥都通过方案*A*产生。读写器使用两套不同的密钥，与上层交互时使用sw的密钥(向上密钥)对，使用方案*A*产生，与标签交互时使用的密钥(向下密钥)，通过方案*B*产生。读写器公私钥因子矩阵、标签公私钥因子矩阵由方案*B*产生。

安全中心的设备和标签的公私钥及相应的读写器公私钥因子矩阵、公私钥矩阵由安全中心集中生成，接受实体的申请，对身份进行核查，生产基于标识的密钥，并向实体分发。读写器的TRID由安全中心生成，并可进行更新，在生成TRID时，同时生成读写器的私钥和公钥，分配相应的标签的公钥，然后写入读写器中。

3.5 密钥分发方式

读写器和中间件的密钥分发方式有两种，一种是读写器通过网络向安全中心请求所需的标签的标识公钥，另一种是将所需的标识公钥存储在TF卡中，读写器通过插入TF卡获取其中的标签的标识公钥，这种情况一般用于用户已有读写器的情况。用户通过购买TF卡和与TF卡内容相对应的标签，与前一种按需获取，TF卡可批量获取标签标识公钥。密钥分发策略是按需分发，即读写器查询到射频范围内有新加入的标签时，向安全中心提出请求。

标签密钥的分发是在制卡过程中自动产生的，并直接写入到标签的存储区中。

3.6 密钥更新方式

需要更新的密钥是安全中心的公私钥、读写器的TRID、向上标识公私钥对、向下标识私钥。标签的标识密钥是永久性的，不进行更新。而读写器TRID及向下私钥设置一个有效期，超过有效期后，产生新的密钥。

密钥更新采用时间触发更新和位置变化触发更新机制。时间触发更新机制是安全中心等待读写器发起请求，读写器用旧密钥和安全中心通讯时，会被安全中心告知密钥已过期，进而进行密钥更新操作。位置变化触发设置为通过检查读写器发送包中的IP地址和所属区域IP地址不相符时触发。更新完成后，安全中心设置数据库记录的相应更新字段为已更新，否则保存为待更新。

3.7 密钥销毁方式

密钥销毁由管理员执行。管理员向制卡中心提交需要销毁设备TID，制卡中心检查请求合法性，如果合法，则把TID发送给安全中心。安全中心检查请求合法性，如果合法，则通知密钥托管中心，把TID、TID对应的私钥加入回收列表，并更改其状态；安全中心将数据库中TID、TID对应的公钥加入到回收列表，并修改其状态。安全中心在相关读写器下一次主动连接的时候，通知读写器销毁TID的公钥。同时，制卡中心销毁此设备的私钥；制卡中心把最终处理结果发回给管理员。

4 方案分析

4.1 方案对比分析

本方案与其他方案的比较如表2所示。

本方案的特色是对RFID系统的每个实体的标识、密钥进行统一管理，建立了统一的标识空间和密钥空间。在实现上，在读写器使用两套密钥，从

而保障了PKI机制与CPK机制在一个RFID系统的统一运行。

表2 RFID系统不同密钥管理方案比较

方案	密钥机制	使用场合
SPINS协议	对称密钥	RFID前端系统
MICA2	非对称密钥	RFID前端系统
文献[12]	简化的PKI	RFID后端系统
文献[13]	CPK	RFID前端系统
文献[14]	PKI与IBE	IBE用于RFID前端系统 PKI用于RFID后端系统 (前端和后端分开管理)
本方案	PKI与CPK	CPK用于RFID前端系统 PKI用于RFID后端系统 (前端和后端统一管理)

使用本方案，具有以下优点。

1) 支持后端系统与其他系统兼容

RFID系统的后端系统通常是传统的网络系统，这些系统大部分都建立有基于PKI的安全基础设施。本方案可以将PKI和CPK二者结合使用，因此，本方案可以使RFID系统兼容以前的设备，减少投资。

2) 支持前端系统设备直接认证、离线认证

在RFID前端系统，由于标签的计算能力和存储能力有限，且数量多，分散度较高，联网条件较差，经常需要在移动中进行设备验证，难以保障第三方在场，经常出现的情况是要求读写器与标签直接认证、离线认证。本方案采用CPK机制，设备认证时不用交换公钥，不需要第三方在场，大大减少了网络带宽，同时减少了公钥管理的复杂度。

3) 设备管理量大

在大规模RFID系统中，前端系统的标签数量通常很大。本方案基于实体标识，建立标识空间，并基于标识空间，建立实体的公私钥矩阵，生成实体的公私钥。公私钥矩阵占用空间比较小，但是可以提供几乎无限个密钥量，用户可以利用标识计算公钥信息，不再需要第三方认证其公钥的正确性。这种优点有利于在物联网这种设备量大，需要离线认证、交叉认证、直接认证的场合中使用。本章提出的方案具备对多达10^{32}规模设备的密钥量的生成能力，可支持巨大数量的用户群。

4.2 安全性分析

本方案的安全性，取决于采用的PKI和CPK机制。针对CPK机制的抗共谋安全问题，本方案在读写器对TRID采用动态更新机制，确保了在标签丢失或被攻破的情况下，仍然具有较高的安全性。

4.3 性能分析

系统性能主要体现在RFID前端系统，本方案与其他方案前端系统在性能方面的比较如表3所示。

表3 RFID系统不同密钥管理方案性能比较

方案	前端密钥机制	带宽	时延	空间
SPINS	对称密钥	小	小	大
MICA2	非对称密钥	大	大	大
文献[13]	CPK	小	小	较大
文献[14]	IBE	小	小	较大
本方案	CPK,ECC	小	小	小

本方案前端系统利用CPK算法依据双方的身份标识，计算出所需的公钥，省去了公钥证书的传输及验证，节省了带宽和证书验证时延。

在存储方面，本方案只需在标签侧存储CPK矩阵，读写器侧按实际区域的标签个数占用存储空间，占用空间大小和读写器管理的标签个数相关，因此，比SPINS、MICA2、文献[13]、文献[14]方案占据的空间都小。一条TID与其标识公钥对的大小为1K，如果一个读写器需要管理的标签的个数为10 000～1 000 000个，则其需要的存储量大概为10 M～1 G。由于读写器通常都具有较大的存储空间，本方案不会对读写器的性能产生影响；标签侧若采用ECC192算法，其标签本身标识私钥约占97字节(776 bit)，安全区鉴别密钥大小为1 024位；假设公钥因子矩阵为10×10的矩阵，则可以产生10的10次方个公钥，约占4.6 KB的存储空间，不会对标签的应用存储产生明显影响。

5 方案验证

本方案已应用到国家发改委2011年信息安全专项“基于物联网应用的安全控制平台系统的产业化”项目，该项目基于针对应急物资保障领域建立安全的RFID应用建设安全控制平台。系统后端采用简化的PKI模块(证书加ECDH实现)，前端采用CPK密钥管理机制。经验证，本方案实现了以下安全功能：

1) 建立了统一的物联网设备标识空间，对标识进行维护、存储和管理。按安全中心服务器能力，系统标识管理能力可达1亿个物联网设备。2) 根据物联网设备标识生成密钥生成基、公钥生成基，根据用户合法身份生成用户密钥。公钥空间10^{48}个，制卡(带有公钥生成基和用户密钥的标签)能力400万张。3) 定时发布当前和历史公钥因子矩阵，生成物联网设备黑名单，并提供查询和下载服务。4) 对接入网络设备(标签、读写设备)进行认证，有效防止了

克隆、欺骗、非授权访问、拒绝服务、假冒、隐私破坏、重放、篡改等各种攻击手段5) 对传输的信息进行了加密处理。在接入系统和安全管理中心之间、读卡设备和安全标签之间，进行数据保密传输，保证了信息传递过程中数据的机密性、完整性、真实性和可用性。

6 结　论

大型RFID系统设备多、类型多，部署范围广，设备之间存在直接认证、离线认证需求，完全依靠PKI体系管理认证和密钥管理，难以满足安全要求。本文基于RFID系统组成元素和网络体系架构，提出基于PKI和CPK的混合密钥管理机制。该机制通过对RFID系统设备进行统一标识，建立统一的标识空间，进而建立统一的密钥空间。同时，将PKI密钥管理技术应用于RFID系统的后端系统，解决了传统互联网身份认证和现有安全方案的兼容问题；采用CPK密钥管理机制，实现了感知层密钥的“集中生成和分散存储”管理方式，解决了RFID系统处理对象多、单个对象资源少，更多需求对象之间直接证明标识的真伪而无需第三方参与的安全需求问题。本文提出的方案可用于物联网安全体系架构的建立和设备之间的密钥管理。

参 考 文 献

[1] NING H, LIU H. Cyber-physical-social based security architecture for future internet of things[J]. Advances in Internet of Things, 2012, 2(1): 34-39.

[2] ZHAO K, GE L. A survey on the internet of things security[C]//2013 9th International Conference on Computational Intelligence and Security (CIS). [S.l.]: IEEE, 2013: 663-667.

[3] SARMA A, GIRAO J. Identities in the future internet of things[J]. Wireless Peers Communication，2009，49(3): 353-363.

[4] JIANG Ji-ya, LIU Tong, SHI Yan-qing, et al. The research on mutual authentication protocol for RFID system based on combined symmetric key[C]//International Conference on Information, Business and Education Technology. Beijing: [s.n.], 2013: 136-137.

[5] 闫韬. 物联网隐私保护及密钥管理机制中若干关键技术研究[D]. 北京: 北京邮电大学, 2012.
YAN Tao. Research on the key problems of privacy protection and key management in the internet of things[D]. Beijing: Beijing University of Posts&telecommunications, 2012.

[6] LIU Y, ZHOU G. Key technologies and applications of internet of things[C]//2012 Fifth International Conference on Intelligent Computation Technology and Automation (ICICTA). [S.l.]: IEEE, 2012: 197-200.

[7] PERRIG A, SZEWCZYK R, TYGAR J D, et al. SPINS: Security protocols for sensor networks[J]. Wireless Networks, 2002, 8(5): 521-534.

[8] GORLATOVA M, SHARMA T, SHRESTHA D, et al. Prototyping energy harvesting active networked tags (EnHANTs) with MICA2 Motes[C]//2010 7th Annual IEEE Communications Society Conference on Sensor Mesh and Ad Hoc Communications and Networks (SECON). [S.l.]: IEEE, 2010: 1-3.

[9] VEGENDLA A, SEO H, LEE D, et al. Implementation of an RFID key management system for DASH7[J]. Journal of Information and Communication Convergence Engineering, 2014, 12(1): 19-25.

[10] 南相浩. CPK算法与标识认证[J]. 信息安全与通信保密, 2006(9): 51-54.
NAN Xiang-hao. CPK algorithm and identity authenrication[J]. Information Security and Communications Privacy, 2006(9): 51-54.

[11] 王嘉林. 基于PKI和CPK的大规模网络认证方案的对比分析[J]. 保密科学技术, 2012(6): 44-46.
WANG Jia-lin. Comparative analysis of large scale network authentication scheme based on CPK and PKI[J]. Security Science and Technology, 2012(6): 44-46.

[12] 曾会, 蒋兴浩, 孙锬锋. 一种基于PKI的物联网安全模型研究[J]. 计算机应用与软件, 2012, 29(6): 271-274.
ZENG Hui, JIANG Xing-hao, SUN Tan-feng. Research on a PKI-based IoT securiry model[J]. Computer Applications and Software , 2012, 29(6): 271-274.

[13] 冯福伟, 李瑛, 徐冠宁, 等. 基于集群架构的物联网身份认证系统[J]. 计算机应用, 2013, 33(A01): 126-129.
FENG Fu-wei, LI Ying，XU Guan-ning, et al. IoT authentication system based on cluster architecture[J]. Journal of Computer Applications, 2013, 33(A01): 126-129.

[14] YANG L, YU P, BAILING W, et al. IOT secure transmission based on integration of IBE and PKI/CA[J]. International Journal of Control & Automation, 2013, 6(2): 50-61.

[15] 张文奇. 基于RFID的物联网安全接入机制研究[D]. 北京: 北京交通大学, 2013.
ZHANG Wen-qi. Research on network security access mechanism based on RFID[D]. Beijing: Beijing Jiaotong University, 2013.

编　辑　蒋　晓