

# RFID 系统下基于组合公钥的密钥管理应用研究

黄 灿, 刘 丹, 彭春林

(电子科技大学 电子科学技术研究院, 四川 成都 611731)

**摘 要:** 由于 RFID 系统的特殊性, 传统的密钥管理方法已不适用. 针对 RFID 系统, 从系统初始化、密钥生成、密钥分配和数据安全传输四个方面提出了一种结合组合公钥算法的密钥管理应用方案. 该方案解决了低成本的限制下标签存储量小、计算能力弱问题, 与 RFID 系统终端设备处理能力相匹配. 分析表明, 此方案具有存储量小、安全性和运行效率较高的特点, 为 RFID 系统的密钥管理体制提供了新的手段.

**关键词:** 射频识别技术; 组合公钥; 密钥管理; ECC 复合定理; 种子矩阵

**中图分类号:** TP309.2

**文献标识码:** A

**文章编号:** 1000-7180(2013)12-0104-04

## Application Research on Key Management for RFID Based on CPK

HUANG Can, LIU Dan, PENG Chun-lin

(Research Institute Electronic Science and Technology, UESTC, Chengdu 611731, China)

**Abstract:** Now, however, traditional teaching methods fail to satisfy the particularity of the RFID system. In this paper, a key management scheme for RFID is proposed, which combines CPK (Combined Public Key) cryptography. The detailed contents, including initializing system, producing key, distributing key, and transmitting data securely, are described. This solution solves small storage and weak compute capability problems. It is matched to the processing power of terminal equipment of RFID. The study shows that the approach has some important features, such as small storage, high security and high running efficiency. And it provides new means for key management of RFID.

**Key words:** radio frequency identification; combined public key; key management; ECC composed principle; seed matrix

### 1 引言

在 RFID 广泛应用的同时, 安全问题成了制约 RFID 系统发展的核心问题之一, 而密钥管理又是诸多安全问题中最核心、最难以解决的问题. 人们在密钥的管理方面进行了广泛的研究, 特别是在密钥的生成、密钥分配和数据加密方面进行了探索.

在传统的加密算法中, 通常采用证书机制解决公钥的认证问题, 例如 PKI (Public Key Infrastructure) 基于普通公钥体制下密钥管理系统<sup>[1]</sup>, 还有基于身份的密钥管理系统 IBE (Identity Based Encryption)<sup>[2]</sup>, 最近几年出现的 CPK (Combined Pub-

lic Key) 基于组合公钥体制下密钥管理系统, 是我国南湘浩研究员提出的. CPK 算法利用标识映射算法实现标识与公钥的绑定, 以很小的密钥因子矩阵, 根据用户标识组合生成大量的用户密钥, 具有认证简单, 密钥管理规模大等优点<sup>[3]</sup>, 非常适用于海量密钥管理问题.

由于 CPK 具有大规模密钥管理及公钥不需要第三方认证的特点, 与 PKI、IBE 相比具有优势, 得到了广泛的研究, 人们已经研究设计了基于 CPK 算法的安全电子邮件系统, 并将 CPK 算法应用到了网格计算、ADHOC 网络、移动 IPv6 (MIPv6) 网络等方面. 本文的目的就是研究 RFID 系统下, 基于组

收稿日期: 2013-03-18; 修回日期: 2013-05-22

基金项目: 成都市高校院所应用成果转化项目 (12DXYB195JH-002)

合公钥算法的密钥管理方案应用。

## 2 RFID 系统的安全性和局限性

RFID 的安全问题超出了原有计算机信息系统的安全边界,引入了新的安全和隐私风险。RFID 安全问题会出现在 RFID 标签、读写器、传输网络和数据存储等各个环节。现有的大部分 RFID 系统采用的是简单的对称加密和弱认证,使之存在信道易破解,身份不匿名易追溯使用者,敏感数据易泄露等缺陷<sup>[4]</sup>。

解决以上问题的关键即是密钥管理,隐私数据防泄漏的强度取决于密钥的安全性。但在 RFID 系统中实现传统加密方法的难点在于 RFID 系统的自身的异构特点,体现在以下三个方面:

(1)由于 RFID 系统标签本身计算能力弱、存储量小、可编程性和电池电源等局限性,限制了其上可支持的加密机制<sup>[5]</sup>。

(2)加密硬件模块功耗太高,不适合只有少数逻辑处理单元和存储器的 RFID 读写器<sup>[5]</sup>。

(3)在增强设备安全性的同时存储、成本、能源消耗也会增加。

因此低成本的 RFID 系统采用的密钥管理方法必须与设备的处理能力相匹配。

## 3 RFID 系统下基于组和公钥的密钥管理方案

RFID 系统由 CPK 密钥管理中心(T),读写器和标签组成,系统架构如图 1 所示。CPK 密钥管理中心运行在网络层及应用层。读写器、标签运行在感知层。读写器是可接入网络的,直接可与中心进行认证的,数量级达十万级别以上,读写器部署时物理安全性较高。标签为有源标签,数量级为千万级以上。

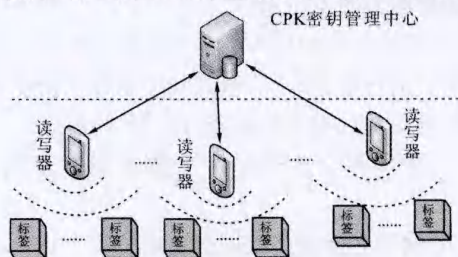


图 1 RFID 系统架构图

系统的业务流程包括以下步骤:

(1)建立并初始化 CPK 密钥管理中心,安装 CPK 密钥管理软件并进行系统初始化。

(2)终端设备提交 CPK 密钥注册申请。在进行

安全通信之前,设备必须向中心提交 CPK 密钥注册申请,申请时需提交有效标识 ID。

(3)CPK 密钥管理中心将公钥因子矩阵和映射组合算法内置于设备芯片中,并分配私钥。

(4)终端设备通过公钥因子矩阵计算出交互设备公钥,使用密钥安全通信。

### 3.1 系统初始化

CPK 密钥管理中心 T,以有限域  $F_p$  上的椭圆曲线构建组合公钥方案,中心完成方案参数的初始化,选取高安全性的椭圆曲线参数建立椭圆曲线密钥系统,从中选取公私密钥对构建公钥因子矩阵和私钥因子矩阵。并为 RFID 系统中每个可信节点,分配公钥因子矩阵;以及根据节点的身份信息、可信状态信息和私钥因子矩阵,计算节点私钥并分配。

#### 3.1.1 系统参数生成和公私钥因子矩阵构建

(1)CPK 密钥管理中心 T 在有限域  $F_p$  上,选取一条足够安全的椭圆曲线,即要选取阶为大素数或含大素数因子的椭圆曲线。假设椭圆曲线  $y^2 \equiv (x^3 + ax + b) \bmod p$ ,将此曲线记为  $E_p(a, b)$ ,其中  $p$  是一个整数, $a, b$  是  $F_p$  上满足条件  $4a^3 + 27b^2 \neq 0$  的两个小于  $p$  的非负整数。设  $G$  是椭圆曲线  $E_p(a, b)$  上的基点,用  $G = (x, y)$  标记,由基点  $G$  的所有倍点构成  $E_p(a, b)$  的子群  $S$ ,  $n$  为大素数,是基点  $G$  的阶。假定私钥为整数  $v$ ,则对应的公钥为  $R = vG$ ,  $param = \{a, b, G, n, p\}$  为确定椭圆曲线密码的参数<sup>[6]</sup>。

(2)CPK 密钥管理中心 T 在给定椭圆曲线密码参数  $param = \{a, b, G, n, p\}$  的基础上,构建公钥因子矩阵和私钥因子矩阵。选一点  $G(x_G, y_G) \in E(F_p)$ ,如果  $n$  是满足  $n \times G = 0$  的最小整数,则由  $G$  的倍点  $\{G, 2G, 3G, \dots, nG\}$  构成一个子群,在子群中取出  $s \times t$  个等式  $R_{ij} = r_{ij}G (1 \leq i \leq s, 1 \leq j \leq t)$ ,将每个等式中的  $R_{ij}, r_{ij}$  放在两个矩阵中相应的位置,构成公钥因子矩阵 PSK 和私钥因子矩阵 SSK<sup>[7]</sup>:

$$PSK = \begin{bmatrix} R_{11} & R_{12} & \dots & R_{1t} \\ R_{21} & \dots & \dots & R_{2t} \\ \vdots & \vdots & \vdots & \vdots \\ R_{s1} & R_{s2} & \dots & R_{st} \end{bmatrix}$$

$$SSK = \begin{bmatrix} r_{11} & r_{12} & \dots & r_{1t} \\ r_{21} & \dots & \dots & r_{2t} \\ \vdots & \vdots & \vdots & \vdots \\ r_{s1} & r_{s2} & \dots & r_{st} \end{bmatrix}$$

(3)选择映射函数  $H: \{0, 1\}^* \rightarrow \{0, 1\}^{k \times t} (s = 2^k)$ ,公开系统参数  $param = \{a, b, G, n, p, PSK, H\}$ 。

### 3.1.2 预分配节点私钥

在 RFID 系统中,CPK 密钥管理中心 T 加密存储私钥因子矩阵,通过设备的标识 ID 进行特定的映射组合算法从私钥因子矩阵中计算出设备(读写器或标签)私钥,密钥生成算法如图 2 所示.并分配给设备(读写器和标签),具体过程如下.

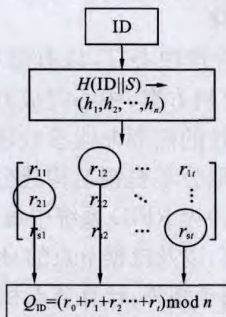


图2 公私密钥对生成算法

(1) 终端设备节点具有唯一的标识信息  $I_i$  和时间信息  $T_i$ , 两者构成节点身份信息  $ID_i = (I_i \parallel T_i)$ . 则每个终端节点具有身份信息  $ID_i (ID_i \in ID)$  和可信状态信息  $S_i (S_i \in S)$ .

(2) 中心 T 盘存所有终端设备节点的身份信息  $ID = \{ID_1, ID_2, \dots, ID_n\}$  和可信状态信息  $S = \{S_1, S_2, \dots, S_n\}$ .

(3) CPK 密钥管理中心通过映射算法计算  $ID_i$  和  $S_i$  的散列值  $H(ID_i \parallel S_i) = (h_1, h_2, \dots, h_n)$ , 其中  $h_i (1 \leq i \leq n)$  是长度为  $k$  的二进制串.

(4) 二进制串  $h_i$  对应一个十进制数  $i_j$ , 从 SSK 中选择第  $j$  列的第  $i_j + 1$  个值  $r_{i_j}$ . 依次从密钥因子矩阵中选取密钥因子, 对所有密钥因子进行组合运算. 私钥:  $SK = (r_0 + r_1 + \dots + r_t) \bmod n$ . 将 SK 存储到节点设备安全区.

### 3.2 系统运行阶段

在系统运行阶段,源节点根据密钥生成算法计算出目标节点的公钥.根据计算出的公钥和存储在目标节点安全区中的私钥运用 ECDSA 算法进行数字签名,根据鉴定过程中协商出的会话密钥运用 AES 对称加密算法加密所需传送的明文,以保障进行安全的数据通信.

#### 3.2.1 目标节点公钥生成

在系统运行阶段,源终端设备节点根据目标终端设备节点身份信息 ID 向目标确认其可信状态信息后,根据公钥因子矩阵和内置于设备芯片中的映射组合算法,通过  $ID_i$  和  $S_i$  进行特定的映射组合算法从公钥因子矩阵中计算出交互设备(读写器或标

签)公钥,具体过程如下.

(1) 终端设备节点具有唯一的标识信息  $I_i$  和时间信息  $T_i$ , 两者构成节点身份信息  $ID_i = (I_i \parallel T_i)$ . 源节点根据终端节点的身份信息  $ID_i$  和可信状态信息  $S_i$  计算散列值  $H(ID_i \parallel S_i) = (h_1, h_2, \dots, h_n)$ .

(2) 每个散列值  $h_i$  对应一个十进制数  $i_j$ , 从 PSK 中选择第  $j$  列的第  $i_j + 1$  个值  $R_{i_j}$ . 依次从密钥因子矩阵中选取密钥因子, 对所有密钥因子进行组合运算, 公钥:

$$PK = R_0 + R_1 + \dots + R_t \\ = (x_0, y_0) + (x_1, y_1) + \dots + (x_t, y_t) \bmod p$$

如上则实现了节点公私密钥对的生成, 系统整体实现流程如图 3 所示.

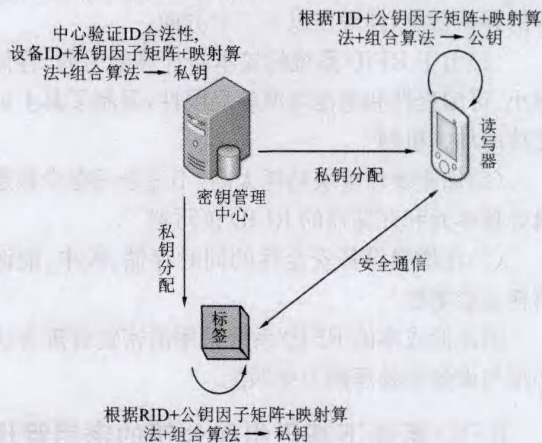


图3 公私密钥生成流程图

#### 3.2.2 数据安全通信

在通过了身份认证,鉴别出合法设备后,进行安全的数据通信.在读写器与标签相互认证的过程中,已经协商出了会话密钥.在系统的设计中,用 ECDSA 算法进行数字签名,用 AES 算法加密所需传送的明文.设计出的合法标签向合法读写器发送数据的结构模型如图 4 所示.

(1) 标签从公钥矩阵中计算出读写器的公钥,对数据明文进行哈希运算,得到明文的数据摘要,用读写器的公钥对数据进行加密,得到数字签名.

(2) 标签用会话密钥加密数据明文得到数据密文.

(3) 读写器接收到数据密文.

(4) 读写器还原出数据明文以及数字签名,通过对明文哈希运算得到一个数据摘要,同时通过数字签名,得到另一个数据摘要,对它们进行比较,若是一致,则数据完整性得到保障,接收到的数据信息有效.

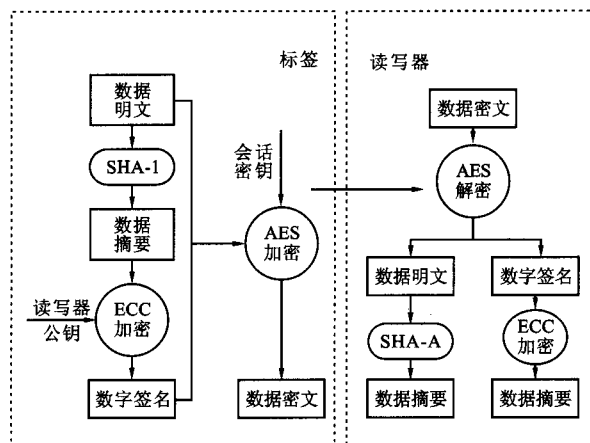


图4 标签向读写器发送数据结构模型图

## 4 方案分析

### 4.1 特点分析

(1)本方案针对 RFID 标签存储量小,提出了解决办法.标签中不需要再盘存大量交互节点的公钥列表,只需要存储“小”的公钥因子矩阵(例如  $32 \times 32$  的矩阵约占用 67 kB 的存储空间)即可通过映射和组合算法计算出公钥,实现了较小的开销,较高的安全性.

(2)本方案针对 RFID 标签计算量小,提出通过映射、椭圆曲线上的点加法、取模运算计算得私钥.

(3)为 RFID 系统提供了一个可靠的、最大限度降低其面临的安全风险的安全机制,同时在系统存储、计算、能量消耗、成本上寻找到一个平衡点.

### 4.2 安全性分析

方案安全性的关键在于椭圆曲线参数的选择、私钥因子矩阵保密、密钥因子矩阵的大小.在构建椭圆曲线密码系统时,本方案避免使用弱安全性的曲线参数,只将几种得到权威组织认可的高安全强度曲线参数作为备选项,保证了椭圆曲线密码系统的安全性.另外,严格保证了私钥因子矩阵的安全性.

由于基于 CPK 算法生成的私钥存储在标签或读写器中,每个私钥都包含了私钥因子矩阵的部分信息.而根据每对  $(ID_i, d_{ID_i})$  可列出一个线性同余方程:

$$\begin{cases} \alpha_{11}d_{s11} + \alpha_{12}d_{s12} + \cdots + \alpha_{1h}d_{s1h} \equiv d_{ID_1} \pmod{q} \\ \alpha_{21}d_{s21} + \alpha_{22}d_{s22} + \cdots + \alpha_{2h}d_{s2h} \equiv d_{ID_2} \pmod{q} \\ \vdots \\ \alpha_{m1}d_{sm1} + \alpha_{m2}d_{sm2} + \cdots + \alpha_{mh}d_{smh} \equiv d_{ID_m} \pmod{q} \end{cases}$$

当攻击者收集到足够多私钥时,就可通过解线

性同余方程组求解出私钥因子矩阵,攻破 CPK 的密码体制.

但要求解  $n$  个变元的线性方程组必须能够列出  $n$  个线性无关的方程组.在实际 RFID 系统中只需要数量级为千万的密钥空间  $8^8$ ,方案中扩大密钥因子矩阵采用  $32^{32}$  密钥空间大小,则设备节点规模  $8^8 \ll 32^{32}$ ,即使所以设备节点都参与共谋,仍不能建立求解线性无关的方程.

## 5 结束语

本文给出了 RFID 系统下基于组合公钥的密钥管理方案.该方案中不仅摆脱了传统密钥管理的局限性,减少了系统的消耗,提高了系统的实用性,而且由少量的种子矩阵通过组合的方法产生大量的密钥,具有节省存储空间和方便生成密钥对的优越性,对于拥有千万级别标签和读写器的大规模的 RFID 系统来说,有着应用的现实意义.本方案是通过扩大密钥矩阵的规模来抵抗的共谋攻击,用户数大于系统中实际的用户数,只能抵抗线性分析共谋攻击,下一步则需要在共谋攻击的问题上进一步的探索.

### 参考文献:

- [1] 张庆胜,叶震,周兵斌,等.椭圆曲线加密算法在 PKI 中的应用[J].计算机工程与设计,2004,25(7):1229-1231.
- [2] 曾兵,杨宇,曹云飞,等.基于身份加密(IBE)技术研究[J].信息安全与通信保密,2011(4):64-66.
- [3] 南湘浩.CPK 组合公钥体制(v7.0)[J].计算机安全,2012(5):2-4.
- [4] 王连强,吕述望,韩小西,等.RFID 系统中安全和隐私问题的研究[J].计算机应用研究,2006,23(6):16-18.
- [5] 王小妮,魏桂英.物联网 RFID 系统数据传输中密码算法的研究[J].北京信息科技大学学报:自然科学版,2009,24(4):75-78.
- [6] 龙弟强,王亚弟,韩继红,等.一种基于双矩阵组合公钥算法的密钥生成方案[J].计算机应用研究,2011,28(8):3058-3060.
- [7] 基于 ECC 设计的 CPK 实现[J].焦作师范高等专科学校学报,2009,25(3):74-76.

### 作者简介:

黄灿 女,(1989—),硕士研究生.研究方向为网络安全.  
 刘丹 男,(1969—),博士,副教授.研究方向为网络安全.  
 彭春林 男,(1975—),硕士,高工.研究方向为网络安全.