RFID 系统混合密钥管理机制的若干研究

赵 斌
（成都信息工程大学 通信工程学院，四川 成都 610225）

摘要：由于 RFID 系统标签资源少、计算能力不理想、存储空间可用率低，传统的加密算法和安全技术并不能够与其相结合，致使 RFID 标签被篡改、假冒等恶劣现象频发，使标识对象的权益很难得到保障，为有效解决 RFID 安全问题，人们将 RFID 与密钥相结合，提出 RFID 系统混合密钥，文章结合 RFID 系统混合密钥管理机制的分析，对 RFID 系统混合密钥管理机制若干问题展开研究，为 RFID 系统安全性的提升作出努力。

关键词：RFID 系统；混合密钥；管理机制
中图分类号：TP391.44；TN918.4 **文献标识码**：A **文章编号**：1673-1131（2015）08-0218-01

0 引言

RFID 系统即射频识别系统，其可以通过射频信号对目标对象自动识别，使物品跟踪、数据交换等突破人工限制及时快速地完成，所以其对环境的适应性非常强，属于非接触式自动识别技术，所以又被称之为“电子标签”，由于其操作简单、准确性有保证，所以近年来得到广泛应用，但与此同时其安全性的缺陷日渐显露，混合密钥管理机制的深化迫在眉睫。

1 RFID 系统混合密钥管理机制

所谓混合密钥管理机制即针对 RFID 系统的前端系统和后端系统使用不同的密钥管理机制，RFID 系统的前端系统主要包括安全中心的各类服务器、接入网关、系统软件、网络用户数据等[1]。

2 RFID 系统混合密钥管理机制分析

2.1 RFID 系统混合密钥管理机制具有统一的密钥空间

在密钥管理机制中 RFID 系统中每个设备结构都有一个加密密钥，为避免设备之间建立联系需要认证，RFID 系统混合密钥管理机制需要建立统一的密钥空间，对所有设备结构进行管理，首先 RFID 系统内所有设备结构都建立标识，如标签 ID、服务器 MAC 地址等，对于像读写器这种没有物理标识的可以随机赋予 TRID 值，然后对所有建立的标识进行统一编码，在合理的转换后形成 RFID 系统密钥空间，混合密钥管理机制会针对密钥空间中的密钥标识生成密钥和公钥生成基，通过安全信道私钥会进入 RFID 系统，使之形成统一的密钥空间，如图 1 所示[2]。

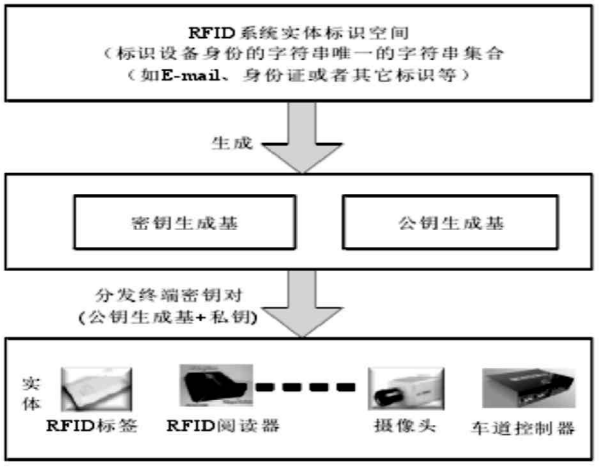

图 1 统一空间的形成过程

2.2 RFID 系统混合密钥管理机制中的密钥存储方式

RFID 系统混合密钥管理机制中的密钥主要存储于安全中心、读写器和标签三个部分，在安全中心主要存储安全中心私钥、读写器及标签的公钥库、读写器自身的公钥和私钥因子矩阵以及 RID 和 TRID 的映射表四大主体；读写器由于其处于 RFID 系统前后端系统的连接位置，所以其主要作用是进行前后端建立联系时的身份认证，所以其主要存储向上和向下的私钥、安全中心与标签的公钥、及 ID 与密钥的映射表等，但在此过程中应注意读写器自身并没有唯一标识；标签主要是将自身私钥存储于安全区，将公钥因子矩阵存储于用户区[3]。

2.3 RFID 系统混合密钥管理机制中的密钥生成方式

RFID 系统混合密钥管理机制中的密钥生成有 CPK 和 PKI 两种方案，通常情况下安全中心及中间件密钥生成需要采用 PKI 方案，标签公钥及私钥因子矩阵需要 CPK 方案，而读写器由于处于前后端系统之间所以向上通常选用 PKI 方案，向下通常选用 CPK 方案，读写器公私钥因子矩阵是由安全中心统一生成的，所以其接受实体申请并能够直接对身份进行检测，在检测的过程中就可以自动生成密钥，并通过实体分发使系统密钥不断得到完善，而读写器由于其不具有物理标识，其 TRID 是临时赋予的，所以安全中心在赋予其 TRID 的同时需要形成其密钥和私钥。

2.4 RFID 系统混合密钥管理机制中的密钥更新方式

在 RFID 系统混合密钥管理机制中标识密钥是一成不变的，所以不需要更新，而读写器的 TRID 是临时赋予的，所以其有一定的时长限制，当密钥使用超出时长就需要对其进行更新，当读写器进行工作被提醒密钥过期时，其会主动向安全中心提出重新申请密钥的请求，安全中心在接到请求后对其进行重新生成，完成更新，或读写器工作的 IP 地址与原地址存在不符时，安全中心也会自动对读写器密钥进行更新，并在安全中心数据库进行状态更新。

3 结语

通过上述分析可以发现，传统密钥管理机制虽在一定程度上能够起到保护 RFID 系统安全的作用，但 RFID 系统内部设备之间需要进行直接或离线的认证，操作程序复杂，而混合密钥管理机制对 RFID 系统进行统一识别，特别是将混合密钥管理机制应用于 RFID 系统后端，舍去了系统内设备相互认证的环节，使其内部所有安全方案实现了兼容，所以混合密钥管理机制对 RFID 系统安全性具有非常好的效果，应在深化的过程中积极推广。

参考文献：

[1] 张兵，秦志光，万国根．基于 PKI 和 CPK 的 RFID 系统混合密钥管理机制研究[J]．电子科技大学学报，2015,5(3):415-421
[2] 陈浩，徐燕．基于 Android 水电信息采集系统的构建策略[J]．南方农机，2015 (5):60-61