ICS 35.040
L 80
备案号:44639—2014

GM

中华人民共和国密码行业标准

GM/T 0035.4—2014

射频识别系统密码应用技术要求
第4部分:电子标签与读写器通信密码应用技术要求

Specifications of cryptographic application for RFID systems—Part 4:Specification of cryptographic application for communication between RFID tag and reader

2014-02-13 发布　　2014-02-13 实施

国家密码管理局　　发布

GM/T 0035.4—2014

中华人民共和国密码
行业标准
射频识别系统密码应用技术要求
第4部分:电子标签与读写器通信密码
应用技术要求
GM/T 0035.4—2014
*
中国标准出版社出版发行
北京市朝阳区和平里西街甲2号(100029)
北京市西城区三里河北街16号(100045)
网址 www.spc.net.cn
总编室:(010)64275323　发行中心:(010)51780235
读者服务部:(010)68523946
中国标准出版社秦皇岛印刷厂印刷
各地新华书店经销
*
开本 880×1230　1/16　印张 1　字数 20 千字
2014年4月第一版　2014年4月第一次印刷
*
书号:155066·2-27014　定价 18.00 元

GM/T 0035.4-2014

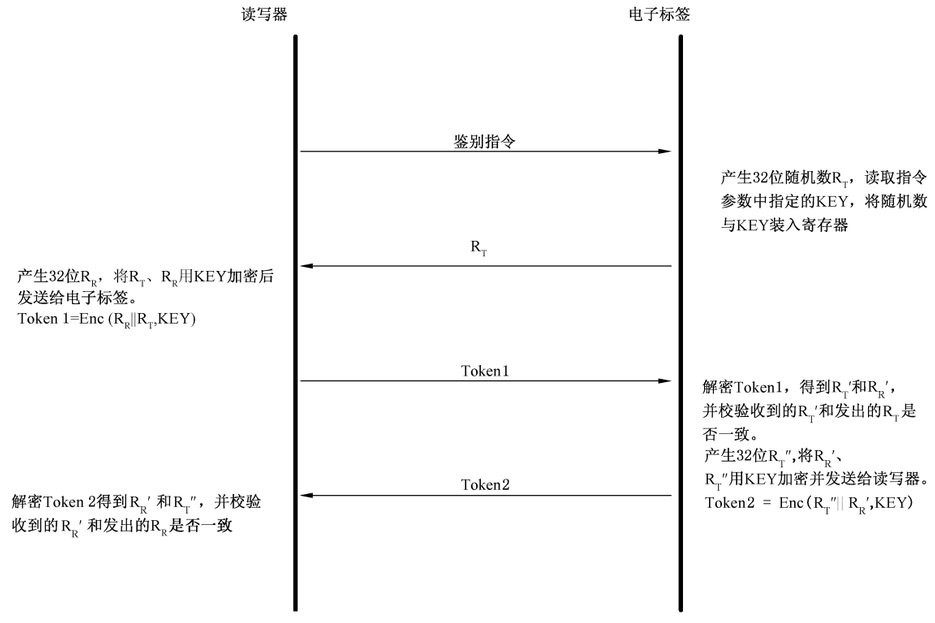

图 A.1　基于 SM7 对称密码算法的双向身份鉴别

A.3　流加密应用

对通信数据的加密采用基于 SM7 算法的流加密方式，数据发送端通过 OFB 模式循环产生密码流，并将通信明文数据与密码流异或后发出；数据接收端通过相同方法产生相同的密码流，将接收到的加密数据与密码流异或后得到数据明文。

在图 A.1 描述的双向身份鉴别过程结束后，电子标签与读写器都继续使用当次身份鉴别过程所使用的密钥 KEY，将身份鉴别过程中产生的 Token2 作为初始向量，通过 SM7 算法的 OFB 模式运算，所产生的加密结果用作流加密的密码流，与通信数据明文（密文）异或后得到通信数据密文（明文）。

目　　次

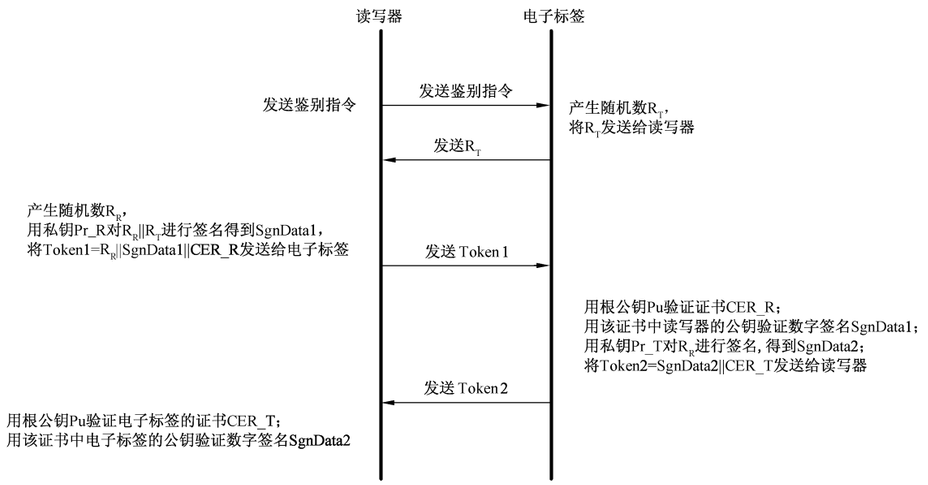

图 2　采用非对称算法的双向鉴别流程图

描述如下：

a)　读写器向电子标签发送鉴别请求命令。

b)　电子标签产生随机数 R_T，发送给读写器。

c)　读写器产生随机数 R_R，用自己的私钥 Pr_R 对 $R_R \| R_T$ 直接进行签名得到 SgnData1，并将数据块 Token1＝$R_R \| SgnData1 \| CER\_R$ 发送给电子标签。

d)　电子标签用根公钥 Pu 验证证书 CER_R。如验证通过，用该证书中读写器的公钥验证数字签名 SgnData1。如果验证通过，则完成对读写器的身份鉴别。

e)　电子标签用自己的私钥 Pr_T 对 R_R 直接进行签名得到 SgnData2，并将 Token2＝SgnData2 ‖ CER_T 发送给读写器。

f)　读写器用根公钥 Pu 验证电子标签的证书 CER_T。如果验证通过，用该证书中电子标签的公钥验证数字签名 SgnData2，如果验证通过，则完成对电子标签的身份鉴别，双向鉴别通过。

也可对上述鉴别过程进行适当变化，如附录 B 所示。

前　言

GM/T 0035《射频识别系统密码应用技术要求》分为五个部分：

——第 1 部分：密码安全保护框架及安全级别；

——第 2 部分：电子标签芯片密码应用技术要求；

——第 3 部分：读写器密码应用技术要求；

——第 4 部分：电子标签与读写器通信密码应用技术要求；

——第 5 部分：密钥管理技术要求。

本部分为 GM/T 0035 的第 4 部分。

本部分按照 GB/T 1.1—2009 给出的规则起草。

本部分由密码行业标准化技术委员会提出并归口。

本部分主要起草单位：北京同方微电子有限公司、兴唐通信科技有限公司、北京中电华大电子设计有限责任公司、上海复旦微电子集团股份有限公司、航天信息股份有限公司、上海华申智能卡应用系统有限公司、复旦大学、上海华虹集成电路有限责任公司、北京华大智宝电子系统有限公司。

本部分主要起草人：吴行军、董浩然、王俊峰、周建锁、陈跃、俞军、梁少峰、谢文录、王云松、徐树民、顾震、王俊宇、柳逊、王会波。