ICS 35.040
L 80
备案号:44636—2014

GM

中华人民共和国密码行业标准

GM/T 0035.1—2014

射频识别系统密码应用技术要求
第1部分:密码安全保护框架及安全级别

Specifications of cryptographic application for RFID systems—Part 1: Cryptographic protection framework and security levels

2014-02-13 发布　　2014-02-13 实施

国家密码管理局　发布

GM/T 0035.1—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1部分:密码安全保护框架及安全级别
GM/T 0035.1—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 1.5　字数 38 千字
2014年5月第一版　2014年5月第一次印刷
*
书号:155066·2-27016　定价 27.00 元

GM/T 0035.1-2014

A.5 密码算法及密钥管理

A.5.1 密钥管理系统

密钥管理系统的作用是规划、产生、保管、分散、传递、管理以及销毁应用系统的密钥，保证应用系统的安全运行。密钥管理系统采用国家指定的密码算法，原则上采用硬件设备产生各级根密钥，并通过采用国家密码管理主管部门指定的密码算法按应用环节的需要将所需密钥下载或分散至安全存储模块中(SAM 卡)。在各个应用环节，安全存储模块完成密钥分散、密钥认证、传输数据的 MAC 计算以及应用数据的加密等功能。同时，各个应用的安全存储模块所装载的密钥根据应用需要而有所不同，保证各个应用的安全独立性。

A.5.2 对称密码算法 SM7 及密钥管理

该算法用于防伪标签与读写器间数据传输加密和完整性校验，由电子标签芯片和读写器的硬件实现，电子标签内的密钥保存在电子标签芯片中密钥存储区的相应位置；读写器所需的密钥以根密钥的形式保存在安全存取模块(SAM)的安全文件中，在读写器获得电子标签应用标识、UID 等分散因子后，由 SAM 卡将根密钥用标签分散因子进行分散，获得对应的标签密钥。

A.5.3 对称密码算法 SM1/SM4 及密钥管理

A.5.3.1 功能描述

该算法用于防伪标签、读写器和中间件数据存储加密，标签与读写器、读写器与中间件间的传输加密，由读写器及应用系统硬件实现。该算法加解密双方使用同一个密钥，密钥的产生、保管和分发过程必须在受控的安全环境下进行，使用环节的算法和密钥必须保存在通过安全认证的硬件设备(如标签芯片和 SAM 卡)中，加解密运算同样也在此硬件设备中进行，以保证运算过程和中间结果不被泄露，运算结果只能在需要时传输到设备以外。SAM 卡所需的密钥以根密钥的形式保存在 SAM 卡的安全文件中，在读写器获得标签应用标识、UID 等分散因子后，由 SAM 卡将根密钥对标签分散因子进行分散，获得对应的标签密钥保存在 SAM 卡内的临时密钥区，进行后续的加密、解密和鉴别运算。

A.5.3.2 根密钥产生

用于对称密钥体系某一应用的根密钥，必须使用硬件随机数发生器产生。

A.5.3.3 子密钥分散

子密钥分散方法如图 A.5 所示，密钥长度及密钥分散因子长度均为 16 字节。将密钥分散因子作为输入数据，采用国家密码管理主管部门指定的算法进行加密计算，产生的 16 字节的结果作为子密钥。

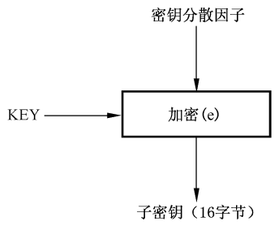

图 A.5 密钥分散计算方法

目 次

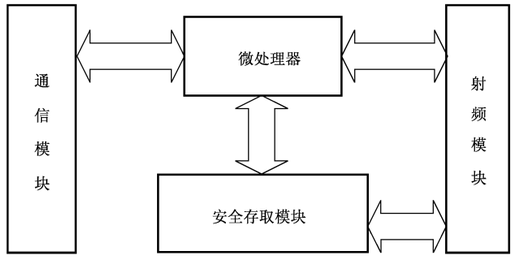

图 A.3　读写器基本结构图

通信模块负责读写器与系统之间的物理层接口；射频模块负责读写器与标签之间的物理层接口；安全存取模块负责读写器与标签之间通信链路的加/解密和指令的编/解码；微处理器负责对来自于标签或系统的指令解析、处理和数据转发功能。

A.3.7.2　安全存取模块

读写器中的安全存取模块包括：随机数发生器、存储器、对称算法处理单元和数据编/解码单元。

随机数发生器用于产生在密钥分散和流加密过程中使用的随机数；存储器用于保存在加密过程中使用的过程密钥、随机数、数据流等；对称算法处理单元用于产生在流加密过程中所要使用的密钥；数据编码单元用于产生对二进制位流进行编码后供射频模块调制发送的数字基带；数据解码单元用于产生对射频模块解调后的数字基带进行解码后供流加密运算的二进制位流。

A.3.7.3　访问流程

读写器对电子标签的访问流程如图 A.4 所示。

A.4　电子标签与读写器通信安全技术

A.4.1　电子标签与读写器通信安全需求

电子标签与读写器通信主要面对安全威胁有：对标签、读写器的非法访问、伪造、跟踪、窃听、数据篡改等，其安全需求有：电子标签与读写器之间的双向身份鉴别、电子标签与读写器之间数据双向传输加密、数据传输安全鉴别等。

A.4.2　电子标签与读写器之间的双向身份鉴别

读写器与标签间的双向身份鉴别采用对称密码算法 SM7 加密的三重身份鉴别机制，以保证标签与读写器在面临非法访问、伪造、跟踪等安全威胁时，攻击者无法通过身份鉴别，从而保证标签与读写器身份的合法性。

具体密钥设置参见 A.5.2。

A.4.3　电子标签与读写器之间数据双向传输加密

电子标签与读写器之间数据双向传输信息采用对称密码算法 SM1/SM4 进行链路加密，以保证传输信息面临窃听等安全威胁时，攻击者得不到明文数据，从而保证信息传输安全。

具体密钥设置参见 A.5.3。

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 1 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。

本部分起草单位：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、兴唐通信科技有限公司、北京同方微电子有限公司、航天信息股份有限公司、北京华大智宝电子系统有限公司。

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