ICS 35.040
L 80
备案号:44641—2014

GM

中华人民共和国密码行业标准

GM/T 0036—2014

采用非接触卡的门禁系统密码应用技术指南

Technical guidance of cryptographic application for access control systems based on contactless smart card

2014-02-13 发布　　2014-02-13 实施

国家密码管理局　　发布

目　　次

前　言

本标准按照 GB/T 1.1—2009 给出的规则起草。

本标准由密码行业标准化技术委员会提出并归口。

本标准起草单位：上海复旦微电子集团股份有限公司，上海华虹集成电路有限责任公司，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，上海华申智能卡应用系统有限公司，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，复旦大学。

本标准主要起草人：俞军、董浩然、梁少峰、吴行军、周建锁、王俊峰、谢文录、柳逊、陈跃、顾震、王云松、徐树民、王俊宇。

采用非接触卡的门禁系统密码应用技术指南

1 范围

本标准规定了针对采用非接触式卡的门禁系统，采用密码安全技术时，系统中使用的密码设备、密码算法、密码协议和密钥管理的相关要求。

本标准适用于指导采用非接触卡的门禁系统相关产品的研制、使用和管理。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本(包括所有的修改单)适用于本文件。

GM/T 0002—2012 SM4 分组密码算法

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

3 术语和定义

下列术语和定义适用于本文件。

3.1

安全存取模块 secure access module

嵌入在读写器内的密码模块，为读写器提供安全服务。

3.2

电子标签 RFID tag

一种用于射频识别，载有与预期应用相关的电子识别信息的载体，每个标签具有唯一的电子编码。通常由耦合元件及芯片组成，包括非接触 CPU 卡和非接触存储卡。

3.3

读写器 reader

与电子标签进行数据通信并对标签进行读、写操作的设备。

3.4

对称密码算法 symmetric cryptographic algorithm

加解密使用相同密钥的密码算法。

3.5

分散密钥 derived key

由根密钥和非保密可变数据生成的对称密钥。

3.6

根密钥 derivation key

用来生成分散密钥的密钥。

3.7

机密性 confidentiality

保证信息不被泄露给非授权的个人、进程等实体的性质。

3.8

加密　encipherment/encryption

对数据进行密码变换以产生密文的过程。

3.9

鉴别　authentication

确认一个实体所声称的身份或信息的真实性。

3.10

解密　decipherment/decryption

加密过程对应的逆过程。

3.11

密码模块　cryptographic module

实现密码运算功能的，相对独立的软件、硬件、固件或其组合。

3.12

密码算法　cryptographic algorithm

描述密码处理过程的运算规则。

3.13

密码协议　cryptography protocol

两个或两个以上参与者使用密码算法，按照约定的规则，为达到某种特定目的而采取的一系列步骤。

3.14

密钥管理　key management

根据安全策略，对密钥的产生、分发、存储、更新、归档、撤销、备份、恢复和销毁等密钥全生命周期的管理。

3.15

射频识别　radio frequency identification

利用射频信号通过空间耦合(交变磁场或电磁场)实现信息的无接触传递，并通过所传递的信息达到识别目的。

3.16

审计　audit

对信息系统记录与活动进行的独立观察和考核。

3.17

数据完整性　data integrity

数据没有遭受以非授权方式所作的篡改或破坏的性质。

3.18

SM1 算法　SM1 algorithm

一种分组密码算法，分组长度为 128 比特，密钥长度为 128 比特。

3.19

SM4 算法　SM4 algorithm

一种分组密码算法，分组长度为 128 比特，密钥长度为 128 比特。

3.20

SM7 算法　SM7 algorithm

一种分组密码算法，分组长度为 64 比特，密钥长度为 128 比特。

3.21

随机数　random number

一种数据序列，其产生不可预测，其序列没有周期性。

3.22

消息鉴别码　message authentication code

又称消息认证码，是消息鉴别算法的输出。

3.23

唯一标识符　unique identifier

由电子标签芯片制造商固化在电子标签芯片内的唯一标识符，包含芯片生产序列号、经注册的厂商代码等唯一性信息。

3.24

主体　subject

引起信息在客体之间流动的人、进程或设备等。

4　符号和缩略语

4.1　符号

下列符号适用于本文件。

‖：数据连接符，将信息串联，表示左侧和右侧数据拼接在一起形成一个新的数据

Enc(X,K)：加密运算符，用密钥 K 对 X 进行加密运算

Dec(X,K)：解密运算符，用密钥 K 对 X 进行解密运算

⊕：比特异或

4.2　缩略语

下列缩略语适用于本文件。

IC：集成电路(Integrated Circuit)

MCU：微控制单元(Micro Controller Unit)

RFID：射频识别(Radio Frequency IDentification)

SAM：安全存取模块(Secure Access Module)

UID：唯一标识符(Unique IDentifier)

5　密码系统概述

5.1　系统构成

基于非接触式 IC 卡的门禁系统的密码应用涉及应用系统、密钥管理及发卡系统，如图 1 所示。

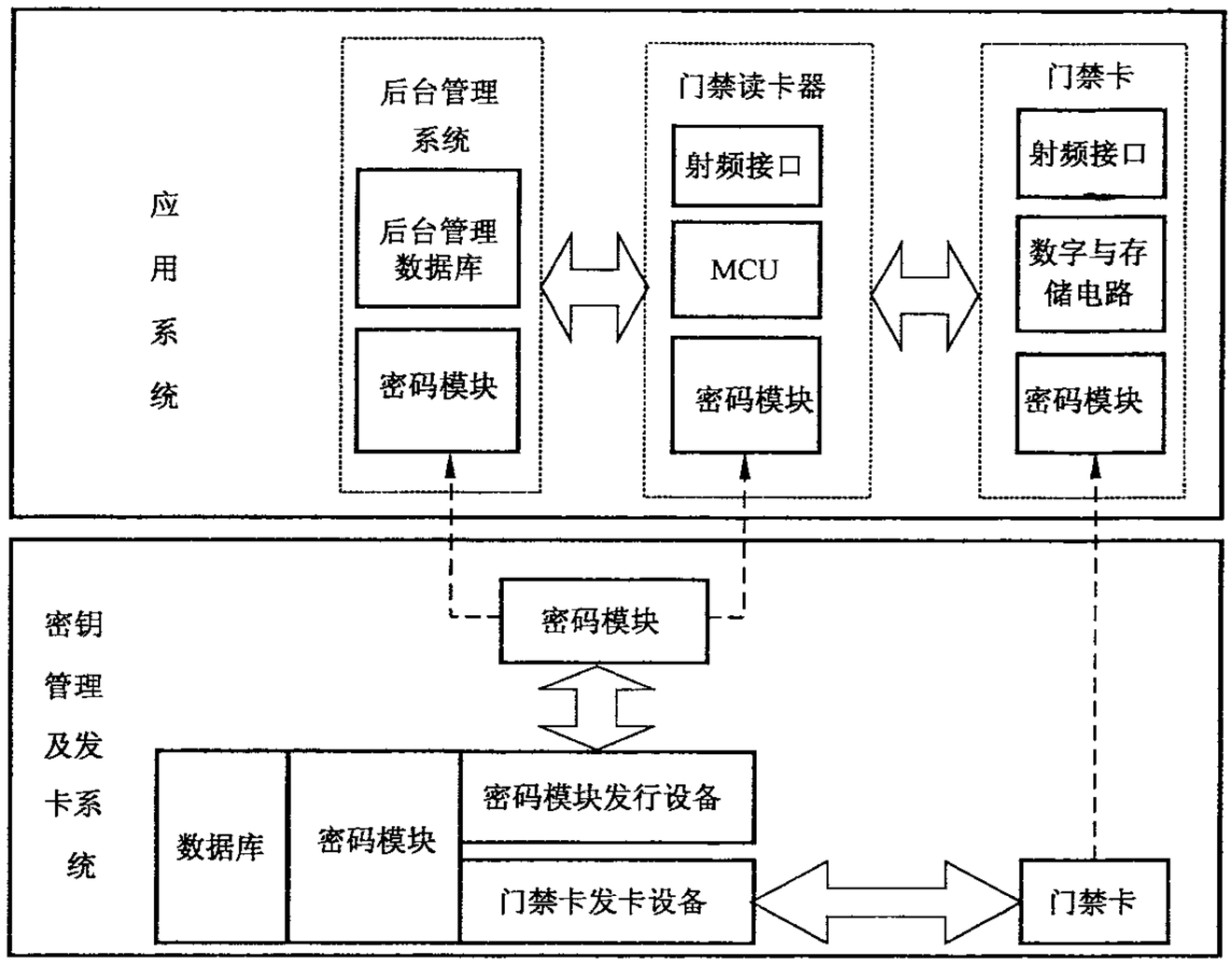

图 1　门禁系统中密码应用结构图

5.2　应用系统

在应用系统中，一般由门禁卡、门禁读卡器和后台管理系统构成，通过各设备内的密码模块对系统提供密码安全保护。其中：

a) 门禁卡内的密码模块：用于门禁读卡器或后台管理系统对门禁卡进行身份鉴别时（鉴别门禁卡是否合法）提供密码服务（如计算鉴别码）；

b) 门禁读卡器/后台管理系统内的密码模块：用于对门禁卡进行身份鉴别时提供密码服务（如密钥分散、验证鉴别码等）。在门禁系统的具体方案设计时，可选择在门禁读卡器或后台管理系统内配用密码模块。

5.3　密钥管理及发卡系统

密钥管理及发卡系统分为密钥管理子系统和发卡子系统。密钥管理子系统的功能是为门禁系统的密码应用生成密钥，并通过密码模块发行设备发行（初始化和注入密钥）密码模块，发卡子系统的功能是通过发卡设备对门禁卡发卡（初始化、注入密钥和写入应用信息）。

密钥管理及发卡系统中的密码设备提供密钥生成、密钥分散以及对门禁卡发卡时的身份鉴别等密码服务。

6　与密码相关的安全技术要求

6.1　密码应用安全技术要求

基于非接触式 IC 卡的门禁系统中的密码应用方案应遵循相应密码算法使用标准，如GM/T 0002—2012。

6.2　密码设备安全技术要求

基于非接触式 IC 卡的门禁系统中的密码设备包括：应用系统密码模块、密钥管理及发卡系统密码

模块，具体密码设备的配用见图 1。

在门禁系统中使用的所有密码设备应遵循相应密码算法使用标准。

在门禁系统中使用的所有密码设备应具有必要的物理防护措施，以保证密码安全。

6.3 密码算法安全技术要求

在门禁系统中所配用的密码算法必须符合国家密码管理主管部门的要求，密码算法应用方案应遵循相应密码算法使用标准。

6.4 密码协议安全技术要求

在门禁系统中，须实现门禁读卡器或后台管理设备对门禁卡的身份鉴别，在身份鉴别过程中所使用的认证协议应遵循 GM/T 0035.4—2014。

6.5 密钥管理安全技术要求

6.5.1 密钥生成

密钥应由符合国家密码管理要求的随机数产生，应保证所生成密钥的机密性和随机性。确保密钥生成过程不可预测，确保在密钥空间内所生成的任意两个密钥具有相同的概率。

6.5.2 密钥注入

门禁卡发卡和密码模块发行时的密钥注入应注意以下两点：

a) 密钥注入过程中不得泄露明文密钥的任何组成部分；

b) 在密码设备、接口和传输信道未受到任何可能导致密钥或敏感数据泄露、篡改的状况下，才可以将密钥加载到密码设备中。

6.5.3 其他要求

在密钥生成、注入、更新及存储等的整个使用过程中，应保证密钥不被泄漏。

7 密码应用参考方案

本标准给出了以下密码应用方案作为参考：

a) 基于国产密码算法 SM7 的非接触逻辑加密卡方案，参见附录 A；

b) 基于国产密码算法 SM1/SM4 的非接触 CPU 卡方案(包括方式 1 和方式 2 两种实现方式)，参见附录 B。

8 其他应考虑的安全因素

在本标准中只强调了对密码应用的安全要求，从系统整体的安全性出发，以下因素在具体系统实现时应加以考虑：

a) 后台管理系统的管理要求；

b) 门禁读卡器与后台管理系统的安全保障；

c) 其他与密码安全机制无关的管理及技术措施，如口令识别、生物特征识别、人员值守等。

在系统方案设计及应用时，需针对具体应用情况在密码安全保障的基础上采取其他适当的管理和技术措施，以增强门禁系统的安全性。

附 录 A
（资料性附录）
基于 SM7 算法的非接触式逻辑加密卡方案

A.1 系统构成

本方案采用基于 SM7 算法的非接触逻辑加密卡作为门禁卡。系统构成示意图如图 A.1 所示。

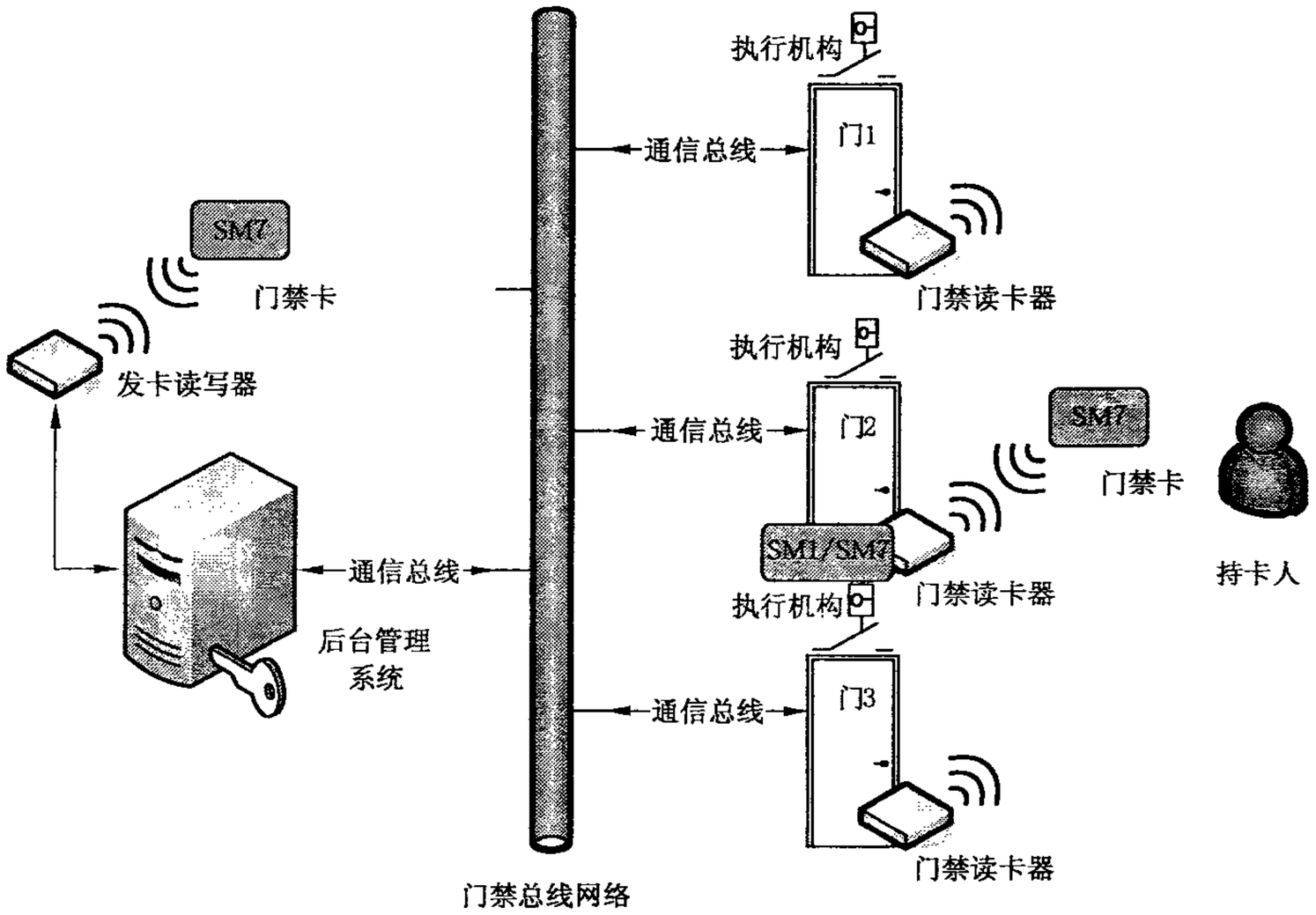

图 A.1 采用基于 SM7 算法的非接触逻辑加密卡作为门禁卡的系统示意图

A.2 方案原理

本方案采用国家密码管理主管部门指定的 SM1 分组加密算法进行密钥分散，实现一卡一密；采用国家密码管理主管部门指定的 SM7 分组加密算法进行门禁卡与门禁读卡器之间的身份鉴别。本方案原理框图如图 A.2 所示。

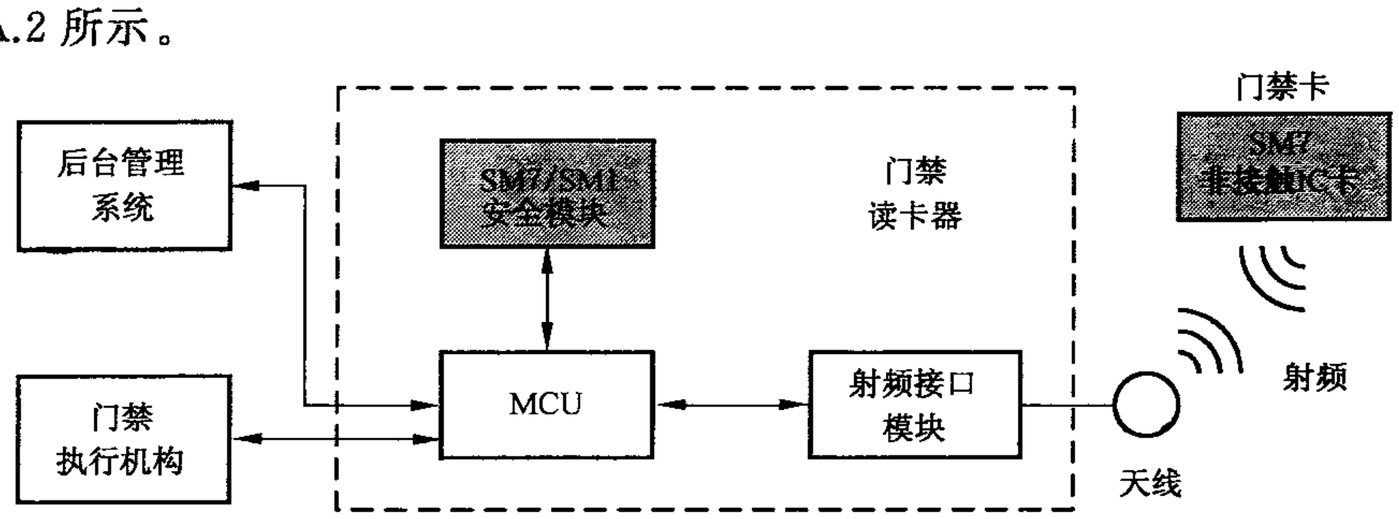

图 A.2 基于 SM7 的非接触逻辑加密卡门禁系统原理框图

门禁卡采用 SM7 分组密码算法，卡内存放发行信息及卡片密钥。

在门禁读卡器中，射频接口模块负责读卡器与门禁卡间的射频通信；MCU 负责读卡器内部的数据交换，与后台管理系统及门禁执行机构的数据通信。SM7/SM1 安全存取模块负责读卡器中的安全密码运算，鉴别门禁卡的合法性，存放系统根密钥。

方案中，门禁读卡器上传鉴别结果给后台管理系统，后台管理系统进行实时或非实时门禁权限及审计管理，门禁执行机构具体执行完成门禁操作。

A.3 密码安全应用流程

A.3.1 密钥管理及发卡系统

a） 安全模块发行

后台管理系统使用密钥管理子系统密码设备生成门禁系统根密钥。门禁系统根密钥必须被安全地导入安全模块。

b） 门禁卡发卡

进行门禁卡发卡时，后台管理系统使用 SM1 算法对系统根密钥进行密钥分散，实现一卡一密；通过发卡读写器对卡片进行数据结构的初始化、卡片密钥的下载、发行信息的写入；发卡过程使用 SM7 算法保证数据交换的机密性。

A.3.2 门禁控制

门禁读卡器上传门禁卡身份鉴别的结果给后台管理系统，用于控制门禁功能的执行。在该过程中，门禁读卡器使用安全存取模块的 SM1 算法对安全存取模块内预存的系统根密钥进行分散，得到与当前门禁卡对应的卡片密钥，然后使用安全模块的 SM7 算法和该卡片密钥对门禁卡进行身份鉴别。

附 录 B
（资料性附录）
基于 SM1/SM4 算法的非接触式 CPU 卡方案

B.1 系统构成

本方案采用基于 SM1/SM4 算法的非接触 CPU 卡，可采用两种方式实现，即方式 1 和方式 2。系统构成示意图如 B.1 所示。

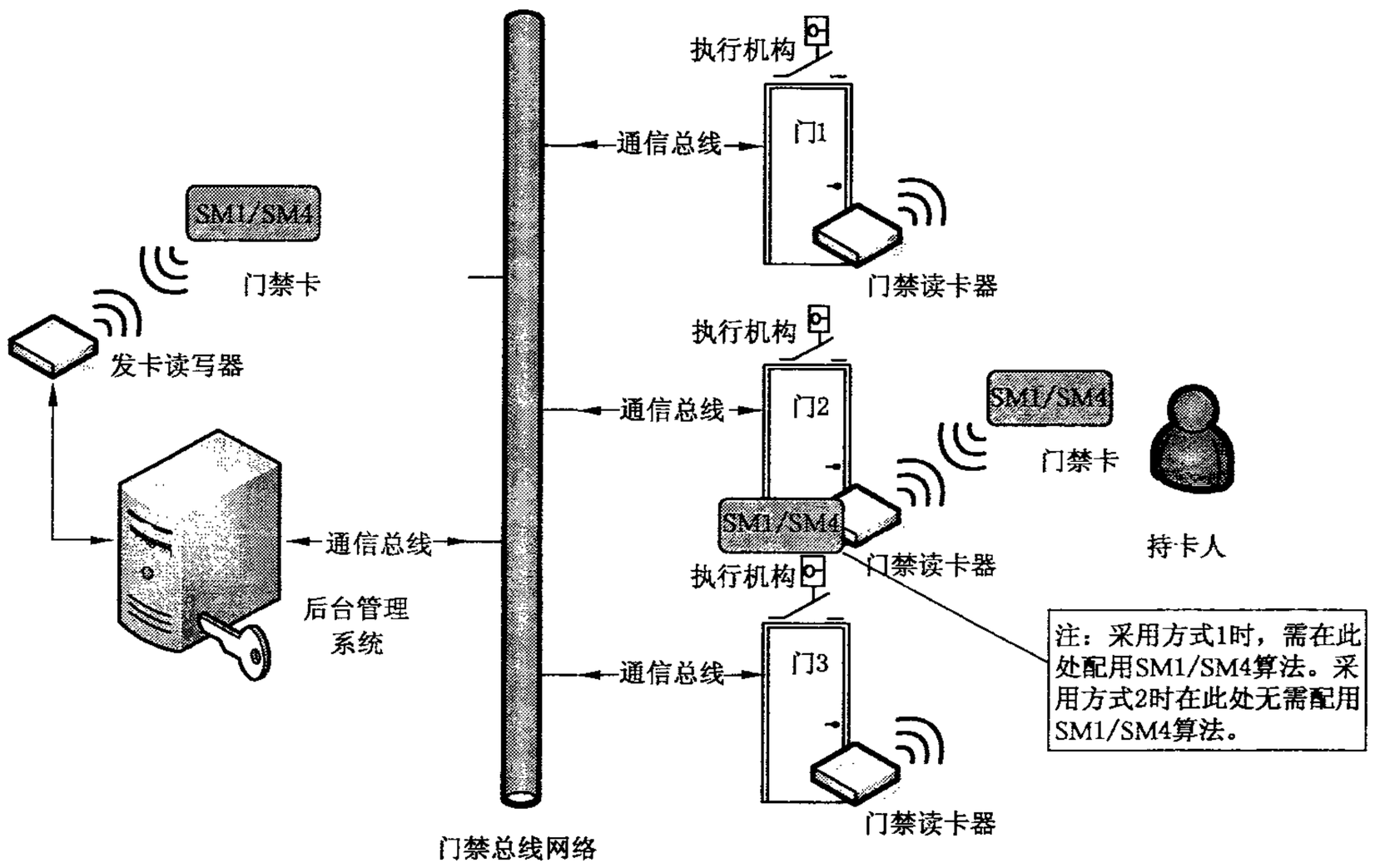

图 B.1 采用基于 SM1/SM4 算法的非接触 CPU 卡作为门禁卡的系统示意图

B.2 方案原理

本方案中门禁卡采用由国家密码管理主管部门指定的 SM1/SM4 算法的 CPU 卡，卡内存放发行信息和卡片密钥，并具有符合相关标准的片上操作系统(COS)；门禁卡与非接读卡器之间采用 SM1/SM4 算法进行身份鉴别和数据加密通讯；在发卡系统中和读写器中的安全模块中同样采用 SM1/SM4 算法进行门禁卡的密钥分散，实现一卡一密。

a) 方式 1，与基于 SM7 算法的非接触式逻辑加密卡所采用的方案类似，主要不同点在于安全模块只需支持 SM1/SM4 算法。

其原理框图如图 B.2 所示。

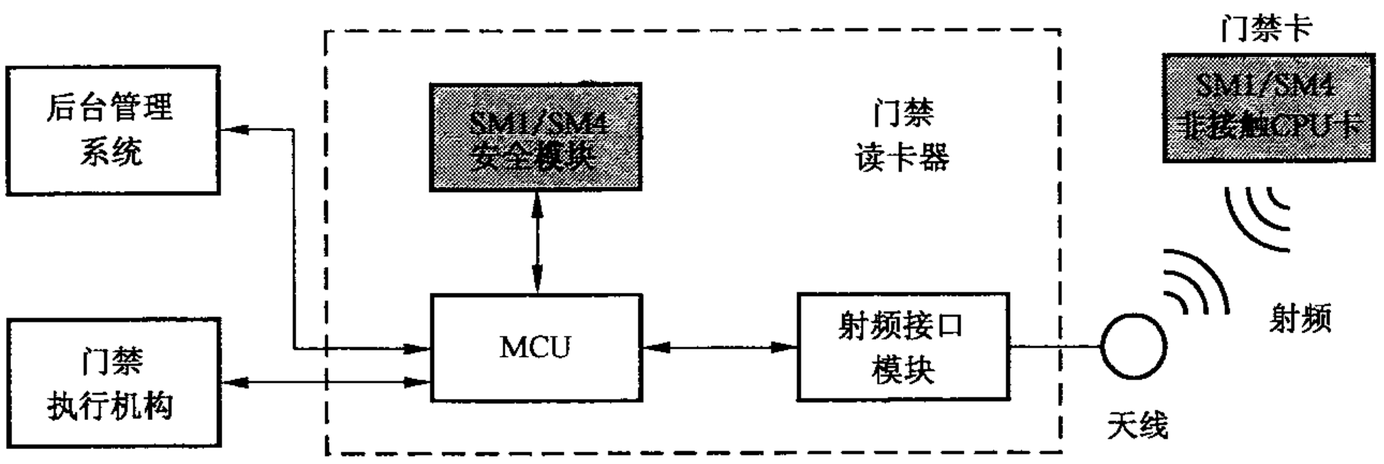

图 B.2　基于 SM1/SM4 的非接触 CPU 卡系统方式 1 原理框图

b)　方式 2,适用于门禁读卡器实时在线操作的情况,门禁读卡器中不需包含带有 SM1/SM4 算法的安全模块,其原理框图如图 B.3 所示。

本方案中,读卡器不负责鉴别门禁卡的合法性,而是在获得门禁卡产生的身份鉴别信息后,将该需要鉴别的信息反馈给门禁控制后台管理系统。并由后台管理系统(如带有 SM1/SM4 算法的安全模块)或与其联网的后台管理系统(带有 SM1/SM4 算法的安全模块)鉴别门禁读卡器上传的鉴别信息,判断产生该鉴别信息的门禁卡是否合法,并控制门禁执行机构完成门禁操作,同时后台管理系统还负责门禁读卡器的管理工作。

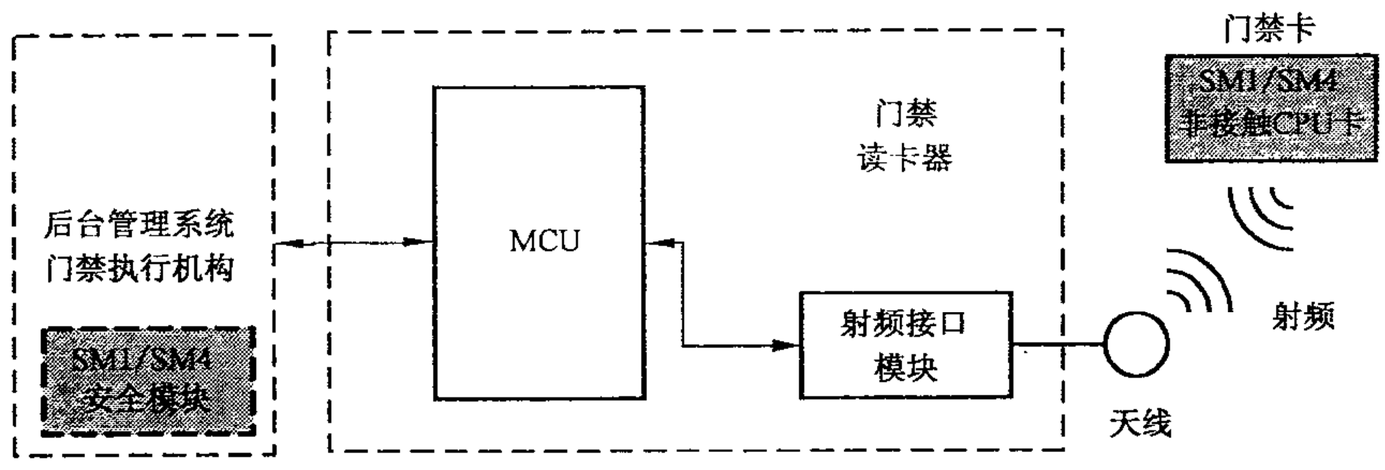

图 B.3　基于 SM1/SM4 的非接触 CPU 卡系统方式 2 原理框图

在本方案中,射频接口模块负责读卡器与门禁卡间的射频通信;MCU 控制射频接口模块与门禁卡的通讯,负责实现读卡器内部的数据传送及与后台管理系统的通信功能。

B.3　密码安全应用流程

B.3.1　密钥管理及发卡系统

a)　安全模块发行

门禁后台管理系统使用密钥管理子系统密码设备生成门禁系统根密钥,安全导入安全模块。

b)　门禁卡发卡

后台管理系统使用 SM1/SM4 算法对系统根密钥进行密钥分散,实现一卡一密;通过发卡读写器对卡片利用过程密钥采用 SM1/SM4 算法进行卡片身份鉴别,应用目录,文件系统等数据结构初始化并完成卡片密钥 Keyc 的下载,以及对卡片进行持卡人信息与签发单位信息的写入,该过程使用 CPU 卡的发卡流程保证信息写入的安全性、数据的机密性。

B.3.2　门禁卡控制

针对 B.2 描述的两种实现方式,分别论述如下。

a） 方式 1 实现方法

方式 1 中，门禁读卡器直接对门禁卡作身份鉴别，并根据结果来控制门禁功能的执行。在该过程与采用 SM7 算法的逻辑加密卡类似，在此不作论述。不同的是身份鉴别时，采用 CPU 卡的内部认证命令完成对 CPU 门禁卡的身份鉴别而不是逻辑加密卡的专用命令。

b） 方式 2 实现方法

方式 2 中，门禁读卡器不直接对门禁卡作身份鉴别，而是由后台管理系统（通过支持 SM1/SM4 算法的安全存取模块）对卡片进行身份鉴别，并根据鉴别结果来控制门禁功能的执行。

身份鉴别的具体方法如下：

——门禁读卡器读取门禁卡的卡片唯一识别号（UID），用于卡片一卡一密密码分散用的特定发行信息 Ci（如有）；

——门禁读卡器发送一个内部认证命令给门禁卡，即发送随机数 R_a（随机数的产生由下文论述）给门禁卡，门禁卡内部用存在卡片中的一卡一密密码 Keyc 对该随机数用 SM1/SM4 算法做加密运算，得到 $R'_a=Enc(Keyc,R_a)$ 并回发给门禁读卡器；

——门禁读卡器传送该 R_a（也可以不上传），R'_a，UID，Ci（如有）到后台管理系统；

——后台管理系统在得到第 3 步上传得信息后，即可以进行门禁卡的身份鉴别工作，首先利用门禁卡的 UID，Ci（如有）等分散因子，利用保存在安全模块中的系统根密钥 Keyr，用 SM1/SM4 算法分散得到门禁卡的一卡一密密钥 Keyc，即 Keyc=Enc(Keyr，UID，Ci) 再用此一卡一密密钥对 R_a（记录在后台管理系统中或由读卡器上传）采用 SM1/SM4 算法做加密运算，即 $R''_a=Enc(Keyc,R_a)$，如果 $R'_a=R''_a$，则卡片的身份鉴别正确，否则鉴别不通过；

——后台管理系统对比卡片唯一性识别号是否为黑名单，如不是，则卡片为系统内合法门禁卡，发出开门信息到门禁执行机构开门。同时使用安全模块产生下一次读写器用于身份鉴别的随机数 R_{a+1}，并同本次鉴别结果（无论本次身份鉴别结果是否合法）发送至门禁读卡器。门禁读卡器接收并存储该随机数用于下一次门禁的内部认证命令的身份鉴别过程。

身份鉴别过程如图 B.4 所示。

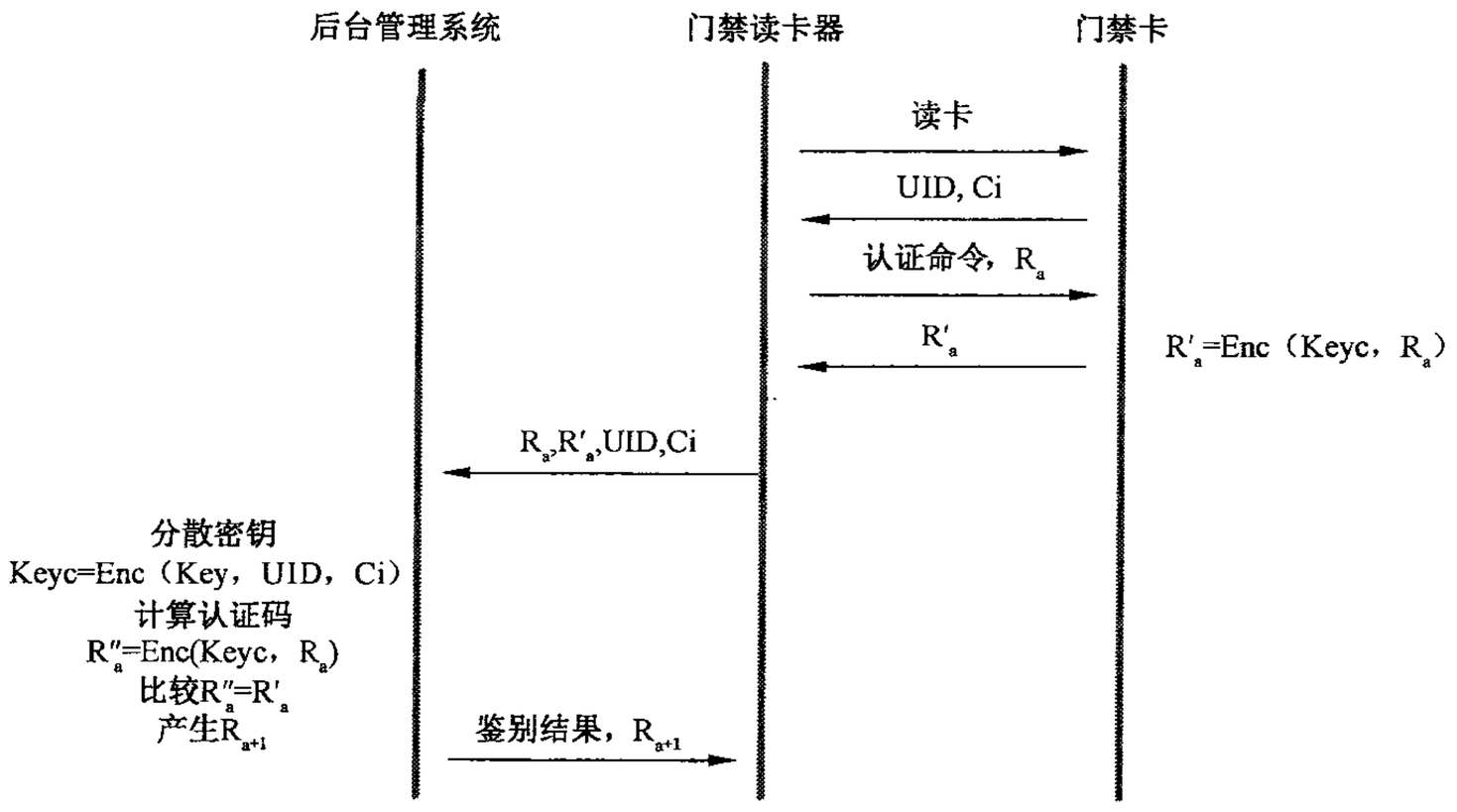

图 B.4 基于后台管理系统 SAM 的身份鉴别过程

由上述过程可以看到，门禁读卡器在身份鉴别中使用的随机数对安全性的影响很大，为了保证该随机数发生器的真随机性，其随机数产生需要由具有真随机数发生器的安全模块产生，而本方案中推荐由 SM1/SM4 安全模块产生该随机数，MCU 利用该随机数进行门禁的身份鉴别过程。门禁读卡器在每次上电后（或规定一定时间）必须在门禁后台管理系统做一个在线注册的工作，表明其上线，与此同

时，具有 SM1/SM4 算法安全模块后台管理系统利用 SM1/SM4 算法安全模块产生一个真随机数并传送给门禁读卡器，门禁读卡器收到该真随机数后存储，以此用于下一次门禁卡的身份鉴别。在一次完整地身份鉴别后，无论鉴别结果如何，后台管理系统均会利用安全模块产生新的随机数，并同鉴别结果一起发送给读写器，读写器存储该新的随机数用于下一次的门禁卡的身份鉴别。

中华人民共和国密码
行业标准
采用非接触卡的门禁系统密码应用技术指南
GM/T 0036—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 22 千字
2014年4月第一版 2014年4月第一次印刷
*
书号:155066·2-27008

GM/T 0036-2014