

ICS 35.240.40

A 11

备案号:

JR

中华人民共和国金融行业标准

JR/T 0025.8—2013

代替JR/T 0025.8—2010

中国金融集成电路（IC）卡规范 第8部分：与应用无关的非接触式规范

China financial integrated circuit card specifications—
Part 8: Contactless specification independent of application

(ISO 14443:2001, Identification cards—Contactless integrated
circuit(s) cards—Proximity cards, Part 1~4, NEQ)

2013-02-05 发布

2013-02-05 实施

中国人民银行 发布

目 次

前言.....	III
引言.....	V
1 范围.....	1
2 规范性引用文件.....	1
3 术语和定义.....	2
4 符号和缩略语.....	3
5 物理特性.....	6
5.1 一般特性.....	6
5.2 尺寸.....	6
5.3 附加特性.....	6
6 射频功率和信号接口.....	7
6.1 PICC 的初始对话.....	7
6.2 功率传送.....	7
6.3 信号接口.....	7
6.4 Type A 通信信号接口.....	8
6.5 Type B 通信信号接口.....	11
6.6 PICC 最小耦合区.....	13
7 初始化和防冲突.....	13
7.1 轮询.....	13
7.2 Type A 的初始化和防冲突.....	13
7.3 Type B 的初始化和防冲突.....	27
8 传输协议.....	39
8.1 Type A PICC 的协议激活.....	39
8.2 Type B PICC 的协议激活.....	47
8.3 半双工块传输协议.....	48
8.4 Type A 和 Type B PICC 的协议停活.....	54
9 数据元和命令.....	54
9.1 命令.....	54
9.2 关闭非接触通道命令.....	55
9.3 激活非接触通道命令.....	56
附录 A (资料性附录) 标准兼容性和表面质量.....	57
附录 B (资料性附录) Type A 的通信举例.....	58
附录 C (规范性附录) CRC_A 和 CRC_B 的编码.....	60
附录 D (资料性附录) Type A 时间槽——初始化和防冲突.....	64
附录 E (资料性附录) Type B——防冲突序列举例.....	67
附录 F (资料性附录) 使用多激活的举例.....	69
附录 G (资料性附录) 协议说明书.....	70
附录 H (资料性附录) 块和帧编码概览.....	77
附录 I (规范性附录) 安全报文.....	78

参考文献 81

前 言

JR/T 0025《中国金融集成电路（IC）卡规范》分为以下部分：

- 第1部分：电子钱包/电子存折应用卡片规范（废止）；
- 第2部分：电子钱包/电子存折应用规范（废止）；
- 第3部分：与应用无关的IC卡与终端接口规范；
- 第4部分：借记/贷记应用规范；
- 第5部分：借记/贷记应用卡片规范；
- 第6部分：借记/贷记应用终端规范；
- 第7部分：借记/贷记应用安全规范；
- 第8部分：与应用无关的非接触式规范；
- 第9部分：电子钱包扩展应用指南（废止）；
- 第10部分：借记/贷记应用个人化指南；
- 第11部分：非接触式IC卡通讯规范；
- 第12部分：非接触式IC卡支付规范；
- 第13部分：基于借记/贷记应用的小额支付规范；
- 第14部分：非接触式IC卡小额支付扩展应用规范；
- 第15部分：电子现金双币支付应用规范；
- 第16部分：IC卡互联网终端规范；
- 第17部分：借记/贷记应用安全增强规范。

本部分为JR/T 0025的第8部分。

本部分按照GB/T 1.1-2009给出的规则起草。

本部分代替JR/T 0025.8-2010《中国金融集成电路（IC）卡规范 第8部分：与应用无关的非接触式规范》。

本部分与JR/T 0025.8-2010相比主要变化如下：

- 修订了标准的前言；
- 删除了对JR/T0025已废止部分的引用。

本部分使用重新起草法参考ISO 14443:2001 Identification cards-Contactless integrated circuit(s) cards-Proximity cards, Part 1~4，与ISO 14443:2001的一致性程度为非等效，主要区别是将ISO 14443的四部分合并为一部分，并增加了关闭和激活非接触式通道指令。

本部分由中国人民银行提出。

本部分由全国金融标准化技术委员会（SAC/TC180）归口。

本部分主要起草单位：中国人民银行、中国工商银行、中国银行、中国建设银行、中国农业银行、交通银行、中国邮政储蓄银行、中国银联股份有限公司、中国金融电子化公司、银行卡检测中心、中钞信用卡产业发展有限公司、捷德（中国）信息科技有限公司、惠尔丰（中国）信息系统有限公司、福建联迪商用设备有限公司。

本部分主要起草人：王永红、李晓枫、陆书春、潘润红、杜宁、陈则栋、吴晓光、李春欢、刘志刚、张永峰、汤沁莹、李新、张栋、王红剑、李一凡、余沁、周新衡、张步、冯珂、李建峰、向前、涂晓军、齐大鹏、陈震宇、郑元龙、聂舒、丁吉、白雪晶、李子达、沈卓群、刘世英、于海涛、翁秀诚。

本部分所代替标准的历次版本发布情况为：

JR/T 0025.8—2013

——JR/T 0025.8—2005;

——JR/T 0025.8—2010。

引 言

与应用无关的非接触式规范是与应用无关的接口规范,发卡机构可以根据实际需求将非接触式接口与借记/贷记应用相结合,形成非接触式的借记/贷记应用;还可以与未来出现的新支付应用结合,具有较高的灵活性。

中国金融集成电路（IC）卡规范

第8部分：与应用无关的非接触式规范

1 范围

JR/T 0025的本部分包括以下主要内容：

- 物理特性：规定了接近式 IC 卡（PICC）的物理特性。本部分等同采用 ISO/IEC 14443-1 内容；
- 射频功率和信号接口：规定了在接近式耦合设备（PCD）和接近式 IC 卡（PICC）之间提供功率和双向通信的场的性质与特征。本部分没有规定产生耦合场的方法，也没有规定遵循电磁场辐射和人体辐射安全的规章。本部分等同采用 ISO/IEC 14443-2 内容；
- 初始化和防冲突：描述了 PICC 进入 PCD 工作场的轮询，在 PCD 和 PICC 之间通信的初始阶段期间所使用的字节格式、帧和时序，初始 REQ 和 ATQ 命令内容，探测方法和与几个卡（防冲突）中的某一个通信的方法，初始化 PICC 和 PCD 之间的通信所需要的其它参数，容易和加速选择在应用准则基础上的几个卡中的一个（即最需要处理的一个）的任选方法。本部分等同采用 ISO/IEC 14443-3 内容；
- 传输协议：规定了以无触点环境中的特殊需要为特色的半双工传输协议，并定义了协议的激活和停活序列。这一部分适用于 Type A 和 Type B 的 PICC。本部分等同采用 ISO/IEC 14443-4 内容；
- 数据元和命令集：定义了金融应用中关闭和激活非接触式通道所使用的一般数据元、命令集和对终端响应的基本要求。

本部分适用于由银行发行或接受的非接触式金融 IC 卡，其使用对象主要是与非接触式金融 IC 卡应用相关的卡片设计、制造、管理、发行、受理以及应用系统的研制、开发、集成和维护等相关部门（单位）。

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。

- GB/T 7496 信息处理系统 数据通信 高级数据链路控制规程 帧结构（GB/T 7496—1987，ISO/IEC 3309:1984，IDT）
- GB/T 14916 识别卡 物理特性（GB/T 14916—2006，ISO/IEC 7810:2003，IDT）
- GB/T 16649.2 识别卡 带触点的集成电路卡 第2部分：触点的尺寸和位置（GB/T 16649.2—2006，ISO/IEC 7816-2:1999，IDT）
- GB/T 16649.3 识别卡 带触点的集成电路卡 第3部分：电信号和传输协议（GB/T 16649.3—2006，ISO/IEC 7816-3:1997，IDT）
- GB/T 16649.4 识别卡 带触点的集成电路卡 第4部分：用于交换的结构、安全和命令（GB/T 16649.4—2010，ISO/IEC 7816-4:2005，IDT）
- GB/T 16649.5 识别卡 带触点的集成电路卡 第5部分：应用标识符的编号系统和注册程序（GB/T 16649.5—2002，ISO/IEC 7816-5:1994，NEQ）
- GB/T 16649.6 识别卡 带触点的集成电路卡 第6部分：行业间数据元（GB/T 16649.6—2001，ISO/IEC 7816-6:1996，IDT）

GB/T 17554.1 识别卡 测试方法 第1部分:一般特性测试 (GB/T 17554.1—2006, ISO/IEC 10373-1:1998, MOD)

JR/T 0025.7 中国金融集成电路 (IC) 卡规范 第7部分:借记/贷记应用安全规范

JR/T 0025.17 中国金融集成电路 (IC) 卡规范 第17部分:借记/贷记应用安全增强规范

ISO/IEC 13239 信息技术 系统间远程通信和信息交换 高级数据链路控制 (HDLC) 规程

ISO/IEC 14443.1~14443.4 识别卡 非接触式集成电路卡 接近式卡

CCITT X.25 数据网络分组交换通信协议

CCITT V.42 数据机标准

3 术语和定义

下列术语和定义适用于本文件。

3.1

集成电路 (IC) integrated circuit (IC)

具有处理和/或存储功能的电子器件。

3.2

无触点的 contactless

完成与卡交换信号和给卡供应能量,而无需使用通电流元件(即不存在从外部接口设备到卡内所包含集成电路的直接通路)。

3.3

无触点集成电路卡 contactless integrated circuit(s) card

一种ID-1型卡(如GB/T 14916中所规定),在它上面已装入集成电路,并且与集成电路的通信是用无触点的方式完成的。

3.4

接近式 IC 卡 (PICC) proximity card (PICC)

一种ID-1型卡,在它上面已装入集成电路和耦合电路,并且与集成电路的通信是通过与接近式耦合设备的电感耦合完成的。

3.5

接近式耦合设备 (PCD) proximity coupling device (PCD)

用电感耦合给PICC提供能量并控制与PICC交换数据的读/写设备。

3.6

位持续时间 bit duration

确定一逻辑状态的时间,在这段时间结束时,一个新的位将开始。

3.7

二进制移相键控 binary phase shift keying

移相为180°的移相键控,从而导致两个可能的相位状态。

3.8

调制指数 modulation index

定义为 $[a-b]/[a+b]$,其中a, b分别是信号幅度的峰值和最小值。

3.9

不归零电平 (NRZ-L) non-return to zero (NRZ-L)

位编码的方式,位持续期间的逻辑状态可以借此通过通信媒介的两个已定义的物理状态之一来表示。

3.10

副载波 subcarrier

以频率 f_s 调制载波频率 f_c 而产生的RF信号。

3.11

防冲突环 anticollision loop

在PCD激励场中，PCD准备和几个PICC中的一张或多张之间的对话所使用的算法。

3.12

位冲突检测协议 bit collision detection protocol

在帧内比特级使用冲突检测的防冲突方法。冲突出现在至少两个PICC把互补位模式发送给PCD时。在这种情况下，位模式被合并，在整个（100%）位持续时间内载波以副载波来调制。

PCD检测出冲突位并按串联次序识别所有PICC ID。

3.13

字节 byte

由指明的8位数据b1到b8组成，从最高有效位（MSB，b8）到最低有效位（LSB，b1）。

3.14

冲突 collision

在同一时间周期内，在同一PCD的工作场中，有两张或两张以上的PICC进行数据传输，使得PCD不能辨别数据是从哪一张PICC发出的。

3.15

基本时间单元 (etu) elementary time unit (etu)

对于本部分，基本时间单元 (etu) 定义为： $1\text{etu}=128/f_c$ 。

3.16

帧 frame

帧是一序列数据位和任选差错检测位，它在开始和结束处有定界符。

注：Type A PICC 使用为 Type A 定义的标准帧，Type B PICC 使用为 Type B 定义的标准帧。

3.17

上层 higher layer

属于应用或上层协议，它不在本部分描述。

3.18

时间槽协议 time slot protocol

PCD与一个或多个PICC建立逻辑通道的方法，该方法对于PICC响应使用时间槽定位，类似于 slotted-Aloha 方法。

3.19

唯一识别符 (UID) unique identifier (UID)

Type A防冲突算法所需的一个编号。

3.20

块 block

帧的一种特殊类型，它包含有效协议数据格式。

注：有效协议数据格式包括 I-块、R-块或 S-块。

3.21

无效块 invalid block

帧的一种类型，它包含无效协议格式。

注：没有接收到帧的超时不被解释为一无效块。

4 符号和缩略语

ADC Type B 的应用数据编码 (Application Data Coding, Type B)

ACK	肯定确认(Positive ACKnowledgement)
AFI	Type B 的应用族识别符 (Application Family Identifier, Type B)
Apf	在 REQB/WUPB 中使用的防冲突前缀 f (Type B) (Anticollision Prefix f, used in REQB/WUPB, Type B)
Apn	在 Slot-MARKER 命令中使用的防冲突前缀 n (Type B) (Anticollision Prefix n, used in Slot-MARKER Command, Type B)
ASK	移幅键控(Amplitude Shift Keying)
ATQ	请求应答(Answer To Request)
ATQA	Type A 的请求应答(Answer To reQuest, Type A)
ATQB	Type B 的请求应答(Answer To reQuest, Type B)
ATS	选择应答(Answer To Select)
ATTRIB	Type B 的 PICC 选择命令(PICC selection command, Type B)
BCC	UID CLn 校验字节,4 个先前字节的“异或”值(Type A)(UID CLn check byte, calculated as exclusive-or over the 4 previous bytes, Type A)
BPSK	二进制移相键控(Binary Phase Shift Keying)
CID	卡标识符(Card IDentifier)
CLn	Type A 的串联级 n, $3 \geq n \geq 1$ (Cascade Level n, Type A)
CRC	循环冗余校验(Cyclic Redundancy Check)
CRC_A	Type A 的循环冗余校验差错检测码(Cyclic Redundancy Check error detection code A)
CRC_B	Type B 的循环冗余校验差错检测码(Cyclic Redundancy Check error detection code B)
CT	Type A 的串联标记(Cascade Tag, Type A)
D	除数(Divisor)
DR	接收的除数 (PCD 到 PICC) (Divisor Receive (PCD to PICC))
DRI	接收的除数整数 (PCD 到 PICC) (Divisor Receive Integer (PCD to PICC))
DS	发送的除数 (PICC 到 PCD) (Divisor Send (PICC to PCD))
DSI	发送的除数整数 (PICC 到 PCD) (Divisor Send Integer (PICC to PCD))
E	Type A 的通信结束(End of communication , Type A)
EDC	差错检测码(Error Detection Code)
EGT	Type B 的额外保护时间(Extra Guard Time, Type B)
EOF	帧结束(End Of Frame)
etu	基本时间单元(Elementary time unit)
f_c	载波频率 (作场的频率, 13.56MHz) (Frequency of operating field(carrier frequency))
FDT	帧延迟时间(Frame Delay Time)
f_s	副载波调制频率(Frequency of subcarrier modulation)
FSC	接近式 IC 卡帧长度(Frame Size for proximity Card)
FSCI	接近式 IC 卡帧长度整数(Frame Size for proximity Card Integer)
FSD	接近式耦合设备帧长度(Frame Size for proximity coupling Device)
FSDI	接近式耦合设备帧长度整数(Frame Size for proximity coupling Device Integer)
FWI	帧等待时间整数(Frame Waiting time Integer)
FWT	帧等待时间(帧等待时间) (Frame Waiting Time)
FWT _{TEMP}	临时帧等待时间(temporary Frame Waiting Time)
HLTA	Type A PICC 暂停命令(Halt Command, Type A)
HLTB	Type B PICC 暂停命令(Halt Command, Type B)

ID	标识号(Identification number)
INF	信息域(INformation field)
LSB	最低有效位(Least Significant Bit)
max	最大值(Index to define a maximum value)
min	最小值(Index to define a minimum value)
MSB	最高有效位(Most Significant Bit)
N	Type B 防冲突槽的数目或每个槽内 PICC 响应的概率(Number of anticollision slots or PICC response probability in each slot, Type B)
NAD	结点地址(Node Address)
NAK	否定确认(Negative Acknowledgement)
NRZ-L	不归零电平(L为电平)(Non-Return to Zero, (L for level))
NVB	Type A 的有效位的数目(Number of Valid Bits, Type A)
OOK	开/关键控(On/Off Keying)
OSI	开放系统互连(Open System Interconnection)
P	Type A 的奇校验位(Odd Parity Bit, Type A)
PARAM	属性格式中的参数(PARAMeter)
PCB	协议控制字节(Protocol Control Byte)
PCD	接近式耦合设备(读写器)(Proximity Coupling Device)
PICC	接近式 IC 卡(Proximity Card)
PPS	协议和参数选择(Protocol and Parameter Selection)
PPS0	协议和参数选择参数 0(Protocol and Parameter Selection parameter 0)
PPS1	协议和参数选择参数 1(Protocol and Parameter Selection parameter 1)
PPSS	协议和参数选择开始(Protocol and Parameter Selection Start)
PUPI	Type B 的伪唯一 PICC 标识符(Pseudo-Unique PICC Identifier, Type B)
R	Type B 的防冲突序列期间 PICC 所选定的槽号(Slot number chosen by the PICC during the anticollision sequence, Type B)
R(ACK)	包含肯定确认的 R-块(R-block containing a positive acknowledge)
R(NAK)	包含否定确认的 R-块(R-block containing a negative acknowledge)
RATS	Type A 的选择应答请求(Request for Answer To Select, Type A)
REQA	Type A 的请求命令(Request Command, Type A)
REQB	Type B 的请求命令(Request Command, Type B)
RF	射频(Radio Frequency)
RFU	预留(Reserved for Future Use)
S	Type A 的通信开始(Start of communication, Type A)
SAK	Type A 的选择确认(Select Acknowledge, Type A)
SEL	Type A 的选择码(SElect code, Type A)
SFGI	启动帧保护时间整数(Start-up Frame Guard time Integer)
SFGT	启动帧保护时间(Start-up Frame Guard Time)
SOF	帧开始(Start Of Frame)
TRO	Type B 的 PCD off 和 PICC on 之间静默的最小延迟(Guard Time, Type B)
TR1	Type B 的 PICC 数据传输之前最小副载波的持续期(Synchronization Time, Type B)
UID	Type A 的唯一标识符(Unique Identifier, Type A)
uid _n	Type A 的唯一标识符的字节数目 n, n ≥ 0(Byte number n of unique identifier, Type A)

- WTX 等待时间延迟 (Waiting Time eXtension)
- WTXM 等待时间延迟乘数 (Waiting Time eXtension Multiplier)
- WUPA Type A 的 PICC 唤醒命令 (Wake-UP Command, Type A)
- WUPB Type B 的 PICC 唤醒命令 (Wake-UP Command, Type B)

5 物理特性

5.1 一般特性

PICC应具有与GB/T 14916中规定的ID-1型卡的要求相应的物理特性。标准兼容性和表面质量参见附录A。

5.2 尺寸

PICC的额定尺寸应是GB/T 14916中规定的ID-1型卡的尺寸。

5.3 附加特性

5.3.1 紫外线

本部分不包括保护PICC不受到超出正常水平剂量紫外线的影响。需要加强防护的部分应是卡制造商的责任并应注明可以承受紫外线的程度。

5.3.2 X-射线

卡的任何一面暴露于70keV到140keV的中等能量X-射线（每年0.1Gy的累积剂量）后，应不引起该卡的失效。

注：这相当于人暴露其中能接受的最大值的年累积剂量的近似两倍。

5.3.3 动态弯曲应力

按照GB/T 17554.1中描述的测试方法（其中短边和长边的最大偏移为 $h_wA=20\text{mm}$ ， $h_wB=10\text{mm}$ ）测试后，PICC应能继续正常工作。

5.3.4 动态扭曲应力

按照GB/T 17554.1中描述的测试方法（其中最大旋转角度 α 等于 15° ）测试后，PICC应能继续正常工作。

5.3.5 交变磁场

在表1给出平均磁场强度的磁场内，在任意方向上暴露后，PICC应能继续正常工作。平均时间为6分钟，磁场的最大rms值被限制在平均值的33倍以内。

表1 磁场强度与频率

频率范围 (MHz)	平均磁场强度 (A/m)	平均时间 (min)
0.3~3.0	1.63	6
3.0~30	4.89/f	6
30~300	0.163	6

另外，在平均值为10A/m rms、13.56MHz频率的磁场中持续暴露后，PICC应能继续正常工作。平均时间为30秒，磁场的最大值被限制在12A/m rms。

5.3.6 交变电场

在表2给出平均电场强度的电场内，在任意方向上暴露后，PICC应能继续正常工作。平均时间为6分钟，电场的最大rms值被限制在平均值的33倍以内。

表2 电场强度与频率

频率范围 (MHz)	平均电场强度 (V/m)	平均时间 (min)
0.3~3.0	614	6
3.0~30	1842/f	6
30~300	61.4	6

表2中 f 为电场频率。

5.3.7 静电

按照GB/T 17554.1中描述的测试方法（其中测试电压为6kV）测试后，PICC应能继续正常工作。

5.3.8 静态磁场

在640kA/m的静态磁场内暴露后，PICC应能继续正常工作。

警告：磁条上的数据内容可能被这样的磁场擦去。

5.3.9 工作温度

在0℃到50℃的环境温度范围内，PICC应能正常工作。

6 射频功率和信号接口

6.1 PICC的初始对话

PCD和PICC之间的初始对话通过下列连续操作进行：

- PCD的RF工作场激活PICC；
- PICC静待来自PCD的命令；
- PCD传输命令；
- PICC传输响应。

这些操作使用下列条款中规定的射频功率和信号接口。

6.2 功率传送

PCD应产生给予能量的RF场，为传送功率，该RF场与PICC进行耦合，为了通信，该RF场应被调制。

6.2.1 频率

RF工作场频率(f_c)应为13.56MHz±7kHz。

6.2.2 工作场

最小未调制工作场为 H_{min} ，其值为1.5A/m (rms)。

最大未调制工作场为 H_{max} ，其值为7.5A/m (rms)。

PICC应按预期在 H_{min} 和 H_{max} 之间持续工作。

PCD应在制造商规定的位置（工作空间）处产生一个最小为 H_{min} ，但不超过 H_{max} 的场。

另外，在制造商规定的位置（工作空间），PCD应能将功率提供给任意的单个参考PICC（在GB/T 17554.1中定义）。

在PICC的任何可能位置内，PCD应不产生高于5.3.5中规定的值的交变磁场。

PCD工作场的测试方法在GB/T 17554.1中规定。

6.3 信号接口

两种通信信号接口Type A和Type B在下列各条中予以描述。

在检测到Type A或Type B的PICC存在之前，PCD应选择两种调制方法之一。

在通信期间，直到PCD停止通信或PICC移走，只有一个通信信号接口可以是有效的。然后，后续序列可以使用任一调制方法。

图1是下面几个部分描述概念的示意图。

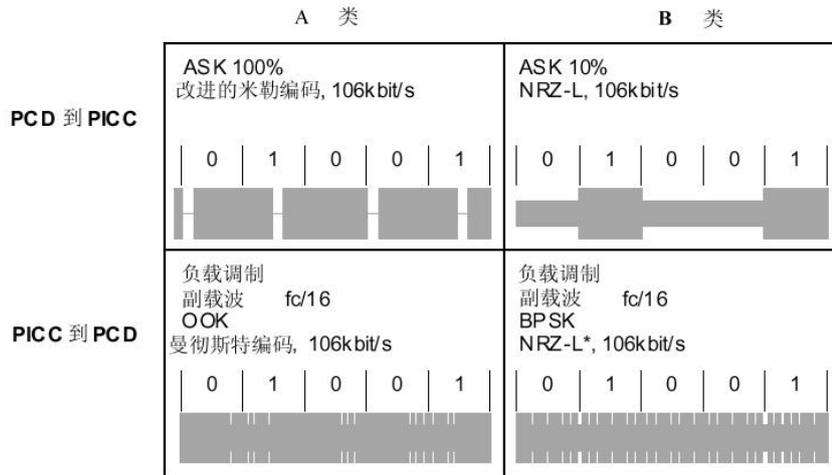


图1 Type A、Type B 接口的通信信号举例

注：*也可能数据反相。

6.4 Type A 通信信号接口

6.4.1 PCD 到 PICC 的通信

6.4.1.1 数据速率

在初始化和防冲突期间，传输的数据位速率应为 $f_c/128$ (~106kbps)。

6.4.1.2 调制

使用RF工作场的ASK100%调制原理来产生一个如图2所示的“暂停 (pause)”状态来进行PCD和PICC间的通信。

PCD场的包络线应单调递减到小于其初始值 $H_{INITIAL}$ 的5%，并至少在 t_2 时间内保持小于5%。该包络线应符合图2。

如果PCD场的包络线不单调递减，则当前最大值和在当前最大值前通过相同值的时间之间的时间应不超过 $0.5\mu s$ 。如果当前最大值大于 $H_{INITIAL}$ 的5%，这种情况才适用。

上冲应保持在 $H_{INITIAL}$ 的 90%和 110%之内。

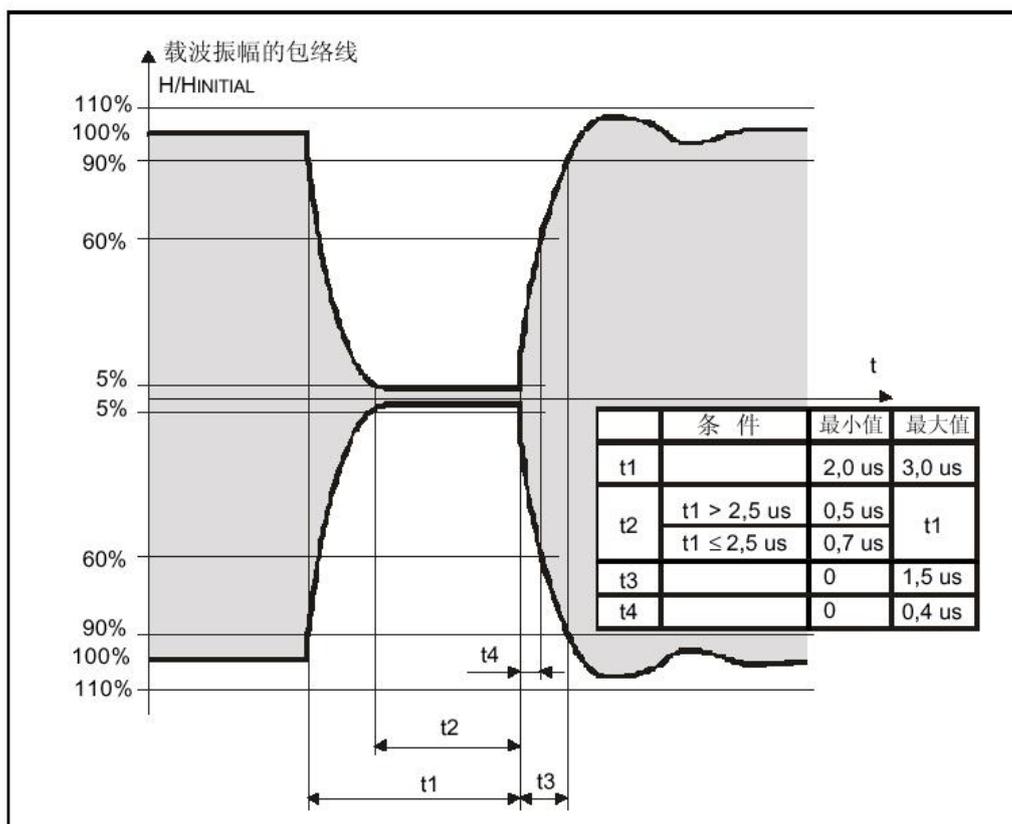
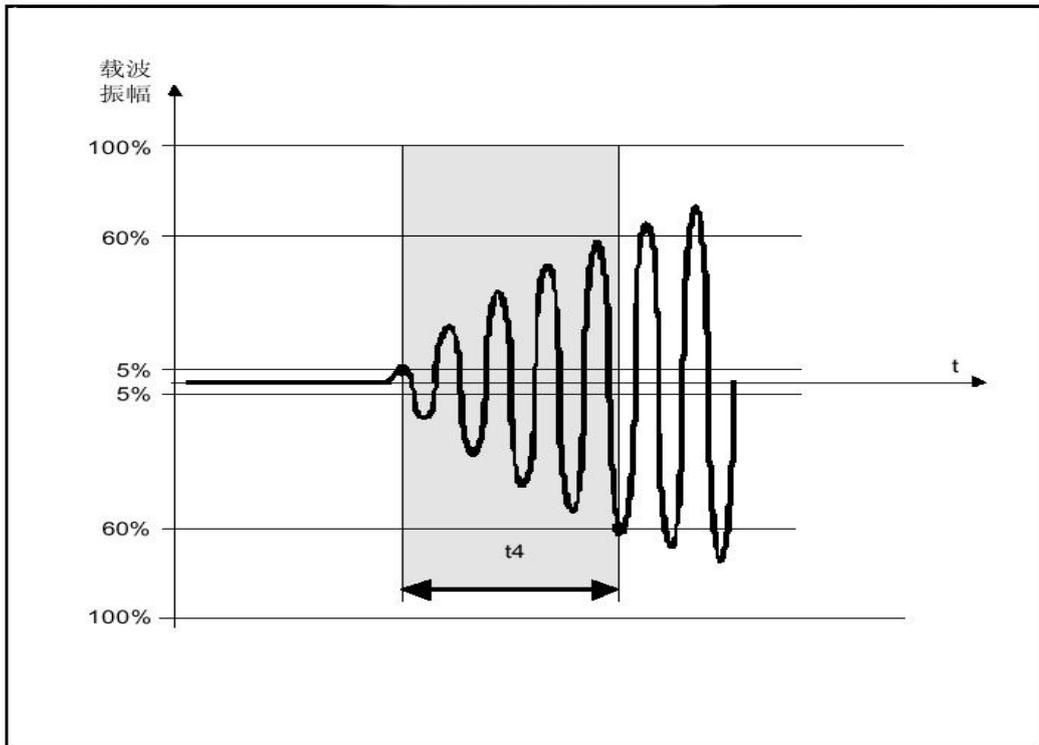


图2 暂停

在场超出 $H_{INITIAL}$ 的 5% 之后和超出 $H_{INITIAL}$ 的 60% 之前，PICC 应检测到“暂停 (pause) 结束”。图 3 给出了“暂停 (pause) 结束”的定义。该定义适用于所有调制包络定时。



注：在设计为一次仅处理一张卡的系统中，不需考虑 t_4 。

图3 暂停结束的定义

6.4.1.3 位的表示和编码

定义了下面的序列：

- 序列 X：在半个位持续时间之后，“暂停 (pause)”应出现；
- 序列 Y：在整个位持续时间，没有调制出现；
- 序列 Z：在位持续时间开始时，“暂停 (pause)”应出现。

上面的序列用于编码下面的信息：

- 逻辑“1”：序列 X；
- 逻辑“0”：序列 Y 带有下列两种异常情况：
 - 如果有两个或两个以上的连续“0”，则序列 Z 应从第二个“0”处开始被使用；
 - 如果在起始帧后的第一位是“0”，则序列 Z 应被用来表示它，并且以后直接紧跟着任何个“0”。
- 通信开始：序列 Z；
- 通信结束：逻辑“0”，后面跟随着序列 Y；
- 没有信息：至少两个序列 Y。

6.4.2 PICC 到 PCD 的通信

6.4.2.1 数据速率

在初始化和防冲突期间，传输的数据位速率应为 $f_c/128$ (~106kbps)。

6.4.2.2 负载调制

PICC 应能经由电感耦合区域与 PCD 通信，在该区域中，所加载的载波频率能产生频率为 f_s 的副载波。该副载波应能通过切换 PICC 中的负载来产生。

在以 GB/T 17554.1 描述的方法测试时，负载调制幅度应至少为 $30/H^{1.2}$ mV (峰值)，其中 H 是以 A/m

6.5.1.3 位的表示和编码

位编码格式是带有如下定义的逻辑电平的 NRZ-L:

- 逻辑“1”：载波场高幅度（没有使用调制）；
- 逻辑“0”：载波场低幅度。

6.5.2 PICC 到 PCD 的通信

6.5.2.1 数据速率

在初始化和防冲突期间，传输的数据位速率应为 $f_c/128$ (~106kbps)。

6.5.2.2 负载调制

PICC 应能经由电感耦合区域与 PCD 通信，在该区域中，所加载的载波频率能产生频率为 f_s 的副载波。该副载波应能通过切换 PICC 中的负载来产生。

在以 GB/T 17554.1 描述的方法测试时，负载调制幅度应至少为 $30/H^{1.2}$ mV（峰值），其中 H 是以 A/m 为单位的磁场强度的有效值（rms）。

6.5.2.3 副载波

副载波负载调制的频率 f_s 应为 $f_c/16$ （约 847KHz），因此，在初始化和防冲突期间，一个位持续时间等于 8 个副载波周期。

PICC 仅当数据被发送时才产生一副载波。

6.5.2.4 副载波调制

副载波应按图 5 中所描述的进行 BPSK 调制。移相应仅在副载波的上升或下降沿的标称位置发生。

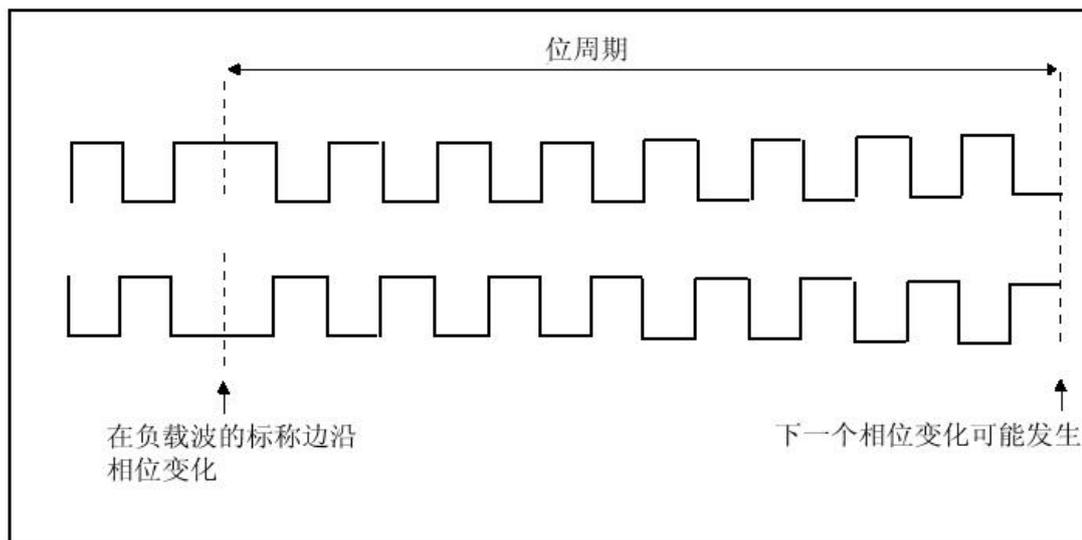


图5 允许的移相（PICC 内部副载波负载切换）

6.5.2.5 位的表示和编码

位编码应是 NRZ-L，其中，逻辑状态的改变应通过副载波的移相（180°）来表示。

在 PICC 帧的开始处，NRZ-L 的初始逻辑电平是通过下面的序列建立的：

- 在来自 PCD 的任何命令之后，在保护时间 $TR0$ 内，PICC 应不生成副载波。 $TR0$ 应大于 $64/f_s$ ；
- 然后，在延迟 $TR1$ 之前，PICC 应生成没有相位跃变的副载波，建立了副载波相位基准 Φ_0 ， $TR1$ 应大于 $80/f_s$ ；
- 副载波的初始相位状态 Φ_0 应定义为逻辑“1”，从而第一个相位跃变表示从逻辑“1”到逻辑“0”的跃变；
- 随后逻辑状态根据副载波相位基准来定义：
 - Φ_0 ：表示逻辑状态 1；
 - Φ_0+180° 表示逻辑状态 0。

6.6 PICC 最小耦合区

PICC 耦合天线可以有任何形状和位置，但应如图 6 所示围绕区域。上边界和左边界在 GB/T 16649.2 中定义。阴影部分是直径为 5.0mm 的区域。

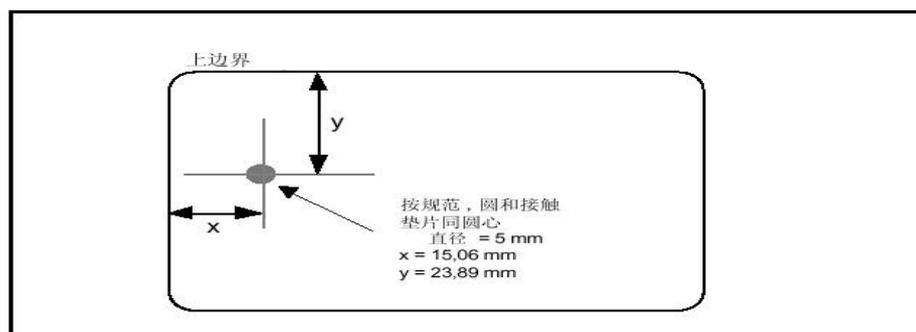


图6 PICC 最小耦合区

7 初始化和防冲突

7.1 轮询

为了检测到工作场内的PICC，PCD发送重复的请求命令。PCD应以任意序列发送在此描述的REQA和REQB，另外，也可以发送附录E中描述的其他命令。

当PICC暴露于未调制的工作场内（见6.2.2），它能在5ms内接受一个请求。

- 1: 当 Type A PICC 接收到任何 Type B 命令时，它应能在 5ms 内接受一个未调制工作场的 REQA。
- 2: 当 Type B PICC 接收到任何 Type A 命令时，它应能在 5ms 内接受一个未调制工作场的 REQB。

7.2 Type A 的初始化和防冲突

本条描述了适用于Type A PICC的初始化和位冲突检测协议。

至少两张以上的Type A PICC同时在一个或多个比特位置上传送互补的位模式时，PCD会检测到冲突。在这种情况下，位模式合并，并且在整个（100%）位持续时间内载波以负载波进行调制（见6.4和6.5）。

7.2.1 帧格式和时序

本条定义了通信初始化和防冲突期间使用的帧格式和时序。关于位表示和编码，见6.4和6.5。

帧应成对传送，PCD到PICC后随PICC到PCD，使用下列的序列：

——PCD 帧：

- PCD 通信开始；
- 信息和根据需要 PCD 传送的差错检测位；
- PCD 通信结束。

——PCD 到 PICC 的帧延迟时间；

——PICC 帧：

- PICC 通信开始；
- 信息和根据需要 PICC 传送的差错检测位；
- PICC 通信结束。

——PICC 到 PCD 的帧延迟时间。

PCD到PICC的帧延迟时间（FDT）与PCD通信结束重迭。

7.2.1.1 帧延迟时间

帧延迟时间（FDT）定义为在相反方向上所发送的两个帧之间的时间。

7.2.1.2 PCD 到 PICC 的帧延迟时间

PCD所发送的最后一个暂停的结束与PICC所发送的起始位范围内的第一个调制边沿之间的时间，它应遵守图7中定义的时序，此处n为一整数。

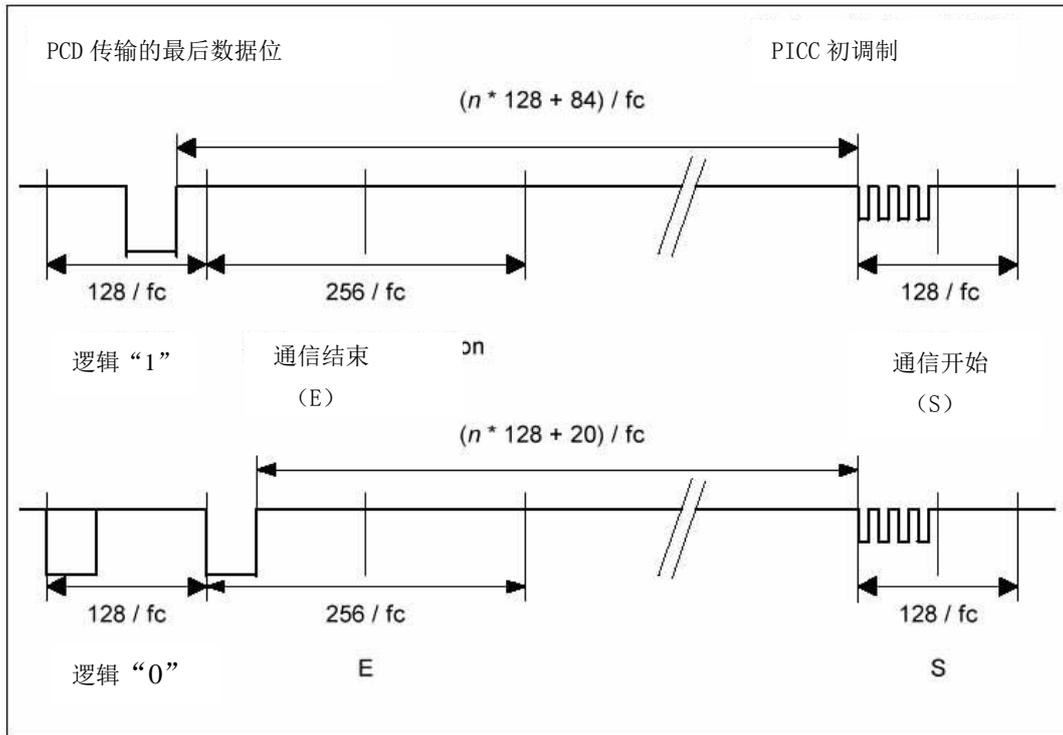


图7 PCD 到 PICC 的帧延迟时间

表3定义了n和依赖于命令类型的FDT的值以及这一命令中最后发送的数据位的逻辑状态。

表3 PCD 到 PICC 的帧延迟时间

命令类型	N (整数)	FDT	
		最后一位= (1) b	最后一位= (0) b
REQA 命令 WAKE-UP 命令 ANTICOLLISION 命令 SELECT 命令	9	1236/f _c	1172/f _c
所有其它命令	≥9	(n*128+84)/f _c	(n*128+20)/f _c

注：值 n=9 意味着场中的所有 PICC 应以防冲突所需的同步方式进行响应。

对于所有的其他命令，PICC应确保起始位范围内的第一个调制边沿与图7中定义的位格对齐。

7.2.1.3 PICC 到 PCD 的帧延迟时间

PICC 所发送的最后一个调制与 PCD 所发送的第一个暂停之间的时间，它应至少为 1172/f_c。

7.2.1.4 请求保护时间

请求保护时间定义为两个连续请求命令的起始位间的最小时间。它的值为 7000/f_c。

7.2.1.5 帧格式

定义了下列帧类型：

- 用于表 4 中定义命令的短帧；
- 用于普通命令的标准帧；
- 面向位的防冲突命令的防冲突帧。

7.2.1.6 短帧

短帧如图8所示，用于初始化通信，并按以下次序组成：

- 通信开始；

7.2.1.9 CRC_A

CRC_A帧是k数据位的一个函数，由帧内除奇偶校验位、S和E以及CRC_A本身外的所有数据位组成。由于数据以字节编码，因此位数k是8的倍数。对于差错检测，在标准帧中发送两个CRC_A字节，它在字节之后，E之前。CRC_A如ISO/IEC 13239中定义，但初始寄存器内容应为“6363”并且计算后寄存器内容应不取反。

举例见附录C。

7.2.2 PICC 状态

下列各部分提供了专门针对位冲突检测协议的Type A的PICC状态的描述。

下列状态图考虑了第7章中命令引起的所有可能的状态转换。

PICC重复使接收帧有效。当检测到传输差错时不发送响应。

下列符号用于图12示出的状态图：

AC	ANTICOLLISION Command (matched UID)
nAC	ANTICOLLISION Command (not matched UID)
SELECT	SELECT Command (matched UID)
nSELECT	SELECT Command (not matched UID)
DESELECT	DESELECT Command, 在附录G.2.3中定义
Error	transmission error detected

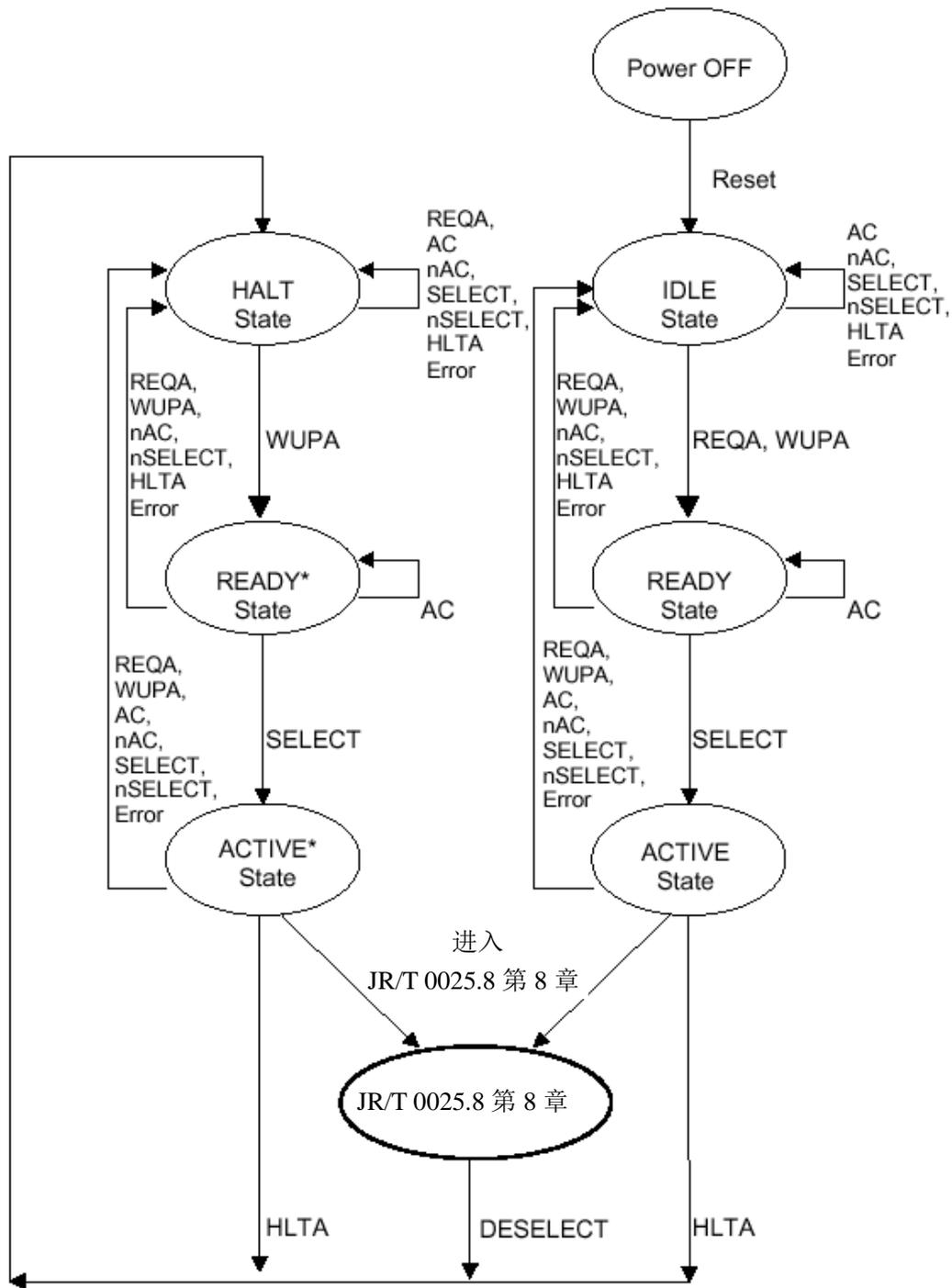


图12 Type A PICC 状态图

与JR/T 0025.8第7章兼容但不使用JR/T 0025.8第8章的PICC可以通过专有命令来设置ACTIVE或ACTIVE*状态。

7.2.2.1 POWER-OFF 状态

描述:

在POWER-OFF状态中，由于缺少载波能量，PICC不能被激励。

状态跳出条件和转换:

如果PICC处于大于 H_{min} （见6.2.2）的激活磁场中，它将在一个不大于延迟时间内进入IDLE状态。

7.2.2.2 IDLE 状态

描述:

在IDLE状态中, PICC被加电。它听从命令并能识别REQA和WUPA命令。

状态跳出条件和转换:

在接收到有效的REQA或WUPA命令后, PICC进入READY状态并发送其ATQA。

7.2.2.3 READY 状态

描述:

在READY状态, 位帧防冲突和专有的防冲突方法都可以应用。串联级别在这一状态内被处理以获取完整的UID。

状态跳出条件和转换:

当根据其完整UID选中它时, PICC进入ACTIVE状态。

7.2.2.4 ACTIVE 状态

——描述:

在ACTIVE状态, PICC听从任何上层报文。

——状态跳出条件和转换:

当接收到有效HLTA命令时, PICC进入HALT状态。

注: 在上层协议中, 可以定义特定命令以使 PICC 返回到 HALT 状态。

7.2.2.5 HALT 状态

——描述:

在HALT状态, PICC仅响应WUPA命令。

——状态跳出条件和转换:

在接收到有效的WUPA命令后, PICC进入READY*状态并发送其ATQA

7.2.2.6 READY*状态

——描述:

READY*状态类似于READY状态, 位帧防冲突和专有的防冲突方法都可以应用。串联级别在这一状态内被处理以获取完整的UID。

——状态跳出条件和转换:

当根据其完整UID选中它时, PICC进入ACTIVE*状态。

7.2.2.7 ACTIVE*状态

——描述:

ACTIVE*状态类似于ACTIVE状态, PICC被选中并听从任何上层报文。

——状态跳出条件和转换:

当接收到有效HLTA命令时, PICC进入HALT状态。

7.2.3 命令集

PCD用来管理与几个PICC通信的命令是:

——REQA;

——WUPA;

——ANTICOLLISION;

——SELECT;

——HALT。

这些命令使用上面描述的字节和帧格式。

7.2.3.1 REQA 和 WUPA 命令

REQA和WUPA命令由PCD发出, 以探测工作场中的Type A PICC。它们在一个短帧内传输。

从图12可以看出在这些情况下PICC实际上必须应答这些相关命令。

特殊地，WUPA命令由PCD发出，使已经进入HALT状态的PICC回到READY*状态。它们应当参与进一步的防冲突和选择规程。

使用短帧格式的REQA和WUPA命令的编码见表4。

表4 短帧格式

b7	b6	b5	b4	b3	b2	b1	含义
0	1	0	0	1	1	0	‘26’ = REQA
1	0	1	0	0	1	0	‘52’ = WUPA
0	1	1	0	1	0	1	‘35’ = 可选时间槽方法，见附录 D
1	0	0	x	x	x	x	‘40’ 至 ‘4F’ = 私有
1	1	1	1	x	x	x	‘78’ 至 ‘7F’ = 私有
所有其他值							预留

7.2.3.2 ANTICOLLISION 命令和 SELECT 命令

这些命令在防冲突环（见图10和11）期间使用。ANTICOLLISION和SELECT命令由下列内容组成：

- 选择代码 SEL（1 个字节）；
- 有效位的数目 NVB（1 个字节，编码见表 9）；
- 根据 NVB 的值，UID CL_n 的 0 到 40 个数据位。

SEL规定了串联级别CL_n。

ANTICOLLISION命令在面向位的防冲突帧中传输。

SELECT命令在标准帧中传输。

由于NVB没有规定40个有效位，因此若PICC保持在READY状态或READY*状态中，命令就被称为ANTICOLLISION命令。

如果NVB规定了UID CL_n的40个数据位（NVB= ‘70’ ），则应添加CRC_A。该命令被称为SELECT命令。

如果PICC已发送了完整的UID，则它从READY状态转换到ACTIVE状态或从READY*状态转换到ACTIVE*状态并在其SAK响应中指出UID完整。

否则，PICC保持在READY状态或READY*状态中并且该PCD应以递增串联级别启动一个新的防冲突环。

7.2.3.3 HALT 命令

HALT命令由四个字节组成并应使用标准帧来发送，如图13所示。

发送的第一个位



图13 HALT 命令帧

如果PICC在HALT帧结束后1ms周期期间以任何调制表示响应，则该响应应解释为“不确认”。

7.2.4 选择序列

选择序列的目的是获得来自PICC的UID以及选择该PICC以便进一步通信。

7.2.4.1 选择序列流程表

PCD的初始化和防冲突流程见图14。

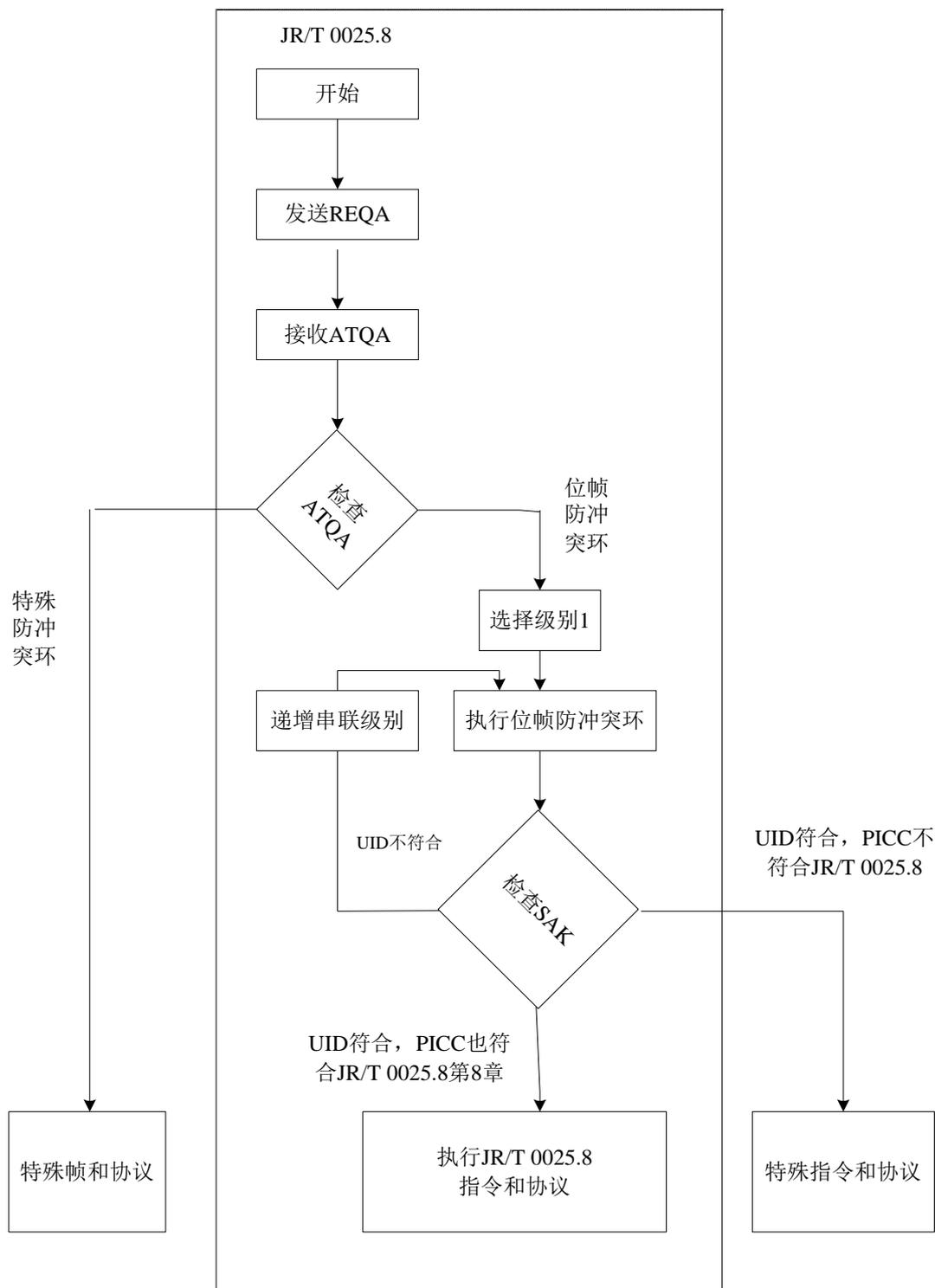


图14 PCD的初始化和防冲突流程图

7.2.4.2 ATQA—请求应答

在PCD发送REQA命令之后，所有IDLE状态的PICC应同步与ATQA命令同步响应。

在PCD发送WUPA命令之后，所有IDLE状态或HALT状态的PICC应同步与ATQA命令同步响应。

当多个PICC响应发生时，PCD应能检测到任何冲突。

有关例子在附录B中给出。

7.2.4.2.1 ATQA 的编码

ATQA的编码规则见表5。

表5 ATQA 的编码

MSB											LSB				
b16	b15	b14	b13	b12	b11	b10	b9	b8	b7	b6	b5	b4	b3	b2	b1
RFU				专有				UID 长度位帧		RFU	位帧防冲突				

7.2.4.2.2 位帧防冲突的编码规则

- 规则 1: 位 b7 和 b8 编码了 UID 长度（单个、两个或三个，见表 6）；
 - 规则 2: b1、b2、b3、b4 或 b5 中的一个位置为 (1) b 以指出位帧防冲突（见表 7）。
- 注：位 9 到 12 指出了附加的和专有的方法。

表6 位帧防冲突用的 b7 和 b8 的编码

b8	b7	含义
0	0	UID 长度：单个
0	1	UID 长度：两个
1	0	UID 长度：三个
1	1	RFU

表7 位帧防冲突用的 b1~b5 的编码

b5	b4	b3	b2	b1	含义
1	0	0	0	0	位帧防冲突
0	1	0	0	0	位帧防冲突
0	0	1	0	0	位帧防冲突
0	0	0	1	0	位帧防冲突
0	0	0	0	1	位帧防冲突
所有其它					RFU

7.2.4.3 防冲突和选择

7.2.4.3.1 每个串联级别范围内的防冲突环

下面算法应适用于防冲突环：

- 步骤 1: PCD 为选择的防冲突类型和串联级别分配了带有编码的 SEL；
- 步骤 2: PCD 分配了带有值为 ‘20’ 的 NVB；

注：该值定义了该 PCD 将不发送 UID CLn 的任何部分。因此该命令迫使工作场内的所有 PICC 以其完整的 UID CLn 表示响应。

- 步骤 3: PCD 发送 SEL 和 NVB；
- 步骤 4: 工作场内的所有 PICC 应使用它们的完整的 UID CLn 响应；
- 步骤 5: 假设场内的 PICC 拥有唯一序列号，那么，如果一个以上的 PICC 响应，则冲突发生。如果没有冲突发生，则步骤 6 到步骤 10 可被跳过；
- 步骤 6: PCD 应识别出第一个冲突的位置；
- 步骤 7: PCD 分配了带有值的 NVB，该值规定了 UID CLn 有效位数。这些有效位应是 PCD 所决定的冲突发生之前被接收到的 UID CLn 的一部分再加上 (0) b 或 (1) b。典型的实现是增加 (1) b；
- 步骤 8: PCD 发送 SEL 和 NVB，后随有效位本身；
- 步骤 9: 只有 PICC 的 UID CLn 中的一部分等于 PCD 所发送的有效位时，PICC 才应发送其 UID CLn 的其余部分；

- 步骤 10: 如果出现进一步的冲突, 则重复步骤 6~9。最大的环数目是 32;
- 步骤 11: 如果不出现进一步的冲突, 则 PCD 分配带有值为 ‘70’ 的 NVB;
注: 该值定义了 PCD 将发送完整的 UID CL_n。
- 步骤 12: PCD 发送 SEL 和 NVB, 后随 UID CL_n 的所有 40 个位, 后面又紧跟 CRC_A 校验和;
- 步骤 13: 它的 UID CL_n 与 40 个位匹配, 则该 PICC 以其 SAK 表示响应;
- 步骤 14: 如果 UID 完整, 则 PICC 应发送带有清空的串联级别位的 SAK, 并从 READY 状态转换到 ACTIVE 状态, 或从 READY*状态转换到 ACTIVE*状态;
- 步骤 15: PCD 应检验 SAK 的串联位是否被设置, 以决定带有递增串联级别的进一步防冲突环是否应继续进行。

如果PICC的UID是已知的, 则PCD可以跳过步骤2~10来选择该PICC, 而无需执行防冲突环。

PCD防冲突环流程见图15。

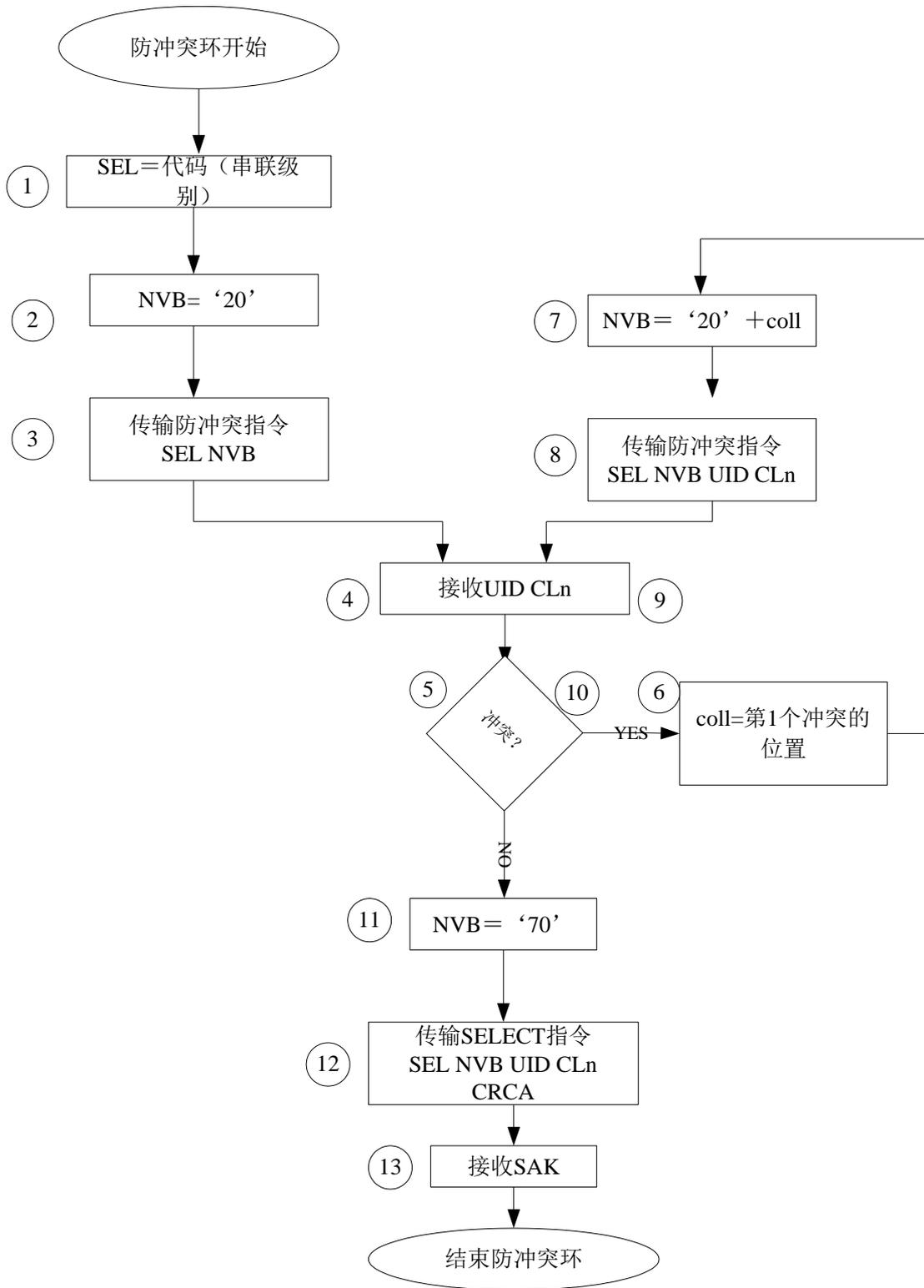


图15 PCD 防冲突环流程图

注：循环编号对应算法步骤。

7.2.4.3.2 SEL 的编码（选择代码）

SEL的编码规则见表8。

长度：1字节

可能值：‘93’，‘95’，‘97’

表8 SEL 的编码

b8	b7	b6	b5	b4	b3	b2	b1	含义
1	0	0	1	0	0	1	1	‘93’：选择串联级别 1
1	0	0	1	0	1	0	1	‘95’：选择串联级别 2
1	0	0	1	0	1	1	1	‘97’：选择串联级别 3
1	0	0	1	所有其他				RFU

7.2.4.3.3 NVB 的编码（有效位的数）

NVB的编码规则见表9。

长度：1字节

较高4位称为字节计数，规定所有被8分开的有效数据位的数，包括被PCD发送的NVB和SEL。这样，字节计数的最小值是2而最大值是7。

较低4位称为位计数，规定由PCD发送的模8所有有效数据位的数。

表9 NVB 的编码

b8	b7	b6	b5	b4	b3	b2	b1	含义
0	0	1	0	x	x	x	X	字节计数=2
0	0	1	1	x	x	x	X	字节计数=3
0	1	0	0	x	x	x	X	字节计数=4
0	1	0	1	x	x	x	X	字节计数=5
0	1	1	0	x	x	x	x	字节计数=6
0	1	1	1	x	x	x	x	字节计数=7
x	x	X	x	0	0	0	0	位计数=0
x	x	X	x	0	0	0	1	位计数=1
x	x	X	x	0	0	1	0	位计数=2
x	x	X	x	0	0	1	1	位计数=3
x	x	X	x	0	1	0	0	位计数=4
x	x	X	x	0	1	0	1	位计数=5
x	x	X	x	0	1	1	0	位计数=6
x	x	X	x	0	1	1	1	位计数=7

7.2.4.3.4 SAK 的编码（选择确认）

当NVB规定40个有效位并且当所有这些数据位与UID CLn相配时，SAK由PICC来发送。SAK的编码规则见图16。



图16 选择确认（SAK）

位b3（串联位）和b6的编码在表10中给出。

表10 SAK 的编码

b8	b7	b6	b5	b4	b3	b2	b1	含义
x	x	x	x	x	1	x	x	串联位设置：UID 不完整

x	x	1	x	x	0	x	x	UID 完整, PICC 遵循 JR/T 0025 的本部分
x	x	0	x	x	0	x	x	UID 完整, PICC 不遵循 JR/T 0025 的本部分

7.2.4.4 UID 内容和串联级别

UID由4、7或10个UID字节组成。因此, PICC最多处理3个串联级别, 以得到所有UID字节。在每个串联级别内, 由5个数据字节组成的UID的一部分应被发送到PCD。根据最大串联级别, 定义了UID长度的三个类型。该UID长度应与表11一致。

表11 UID 长度

最大串联级别	UID 长度	字节数
1	单个	4
2	两个	7
3	三个	10

UID 是一固定的唯一数或由 PICC 动态生成的随机数。UID 的第一个字节 (uid₀) 分配后随 UID 字节的内容。单个长度的 UID 编码规则见表 12。

表12 单个长度的 UID

uid ₀	描述
'08'	uid ₁ 到 uid ₃ 是动态生成的随机数
'x0' — 'x7' 'x9' — 'xE'	专有的固定数
'18' — 'F8' 'xF'	RFU

串联标记 CT 的值 '88' 应不用于单个长度 UID 中的 uid₀。多个长度的 UID 编码规则见表 13 和图 17。

表13 两个和三个长度的 UID

uid ₀	描述
制造商 ID 根据 GB/T 16649.6*	每一制造商对唯一编号的其他字节的值的唯一性负责
*值 '81' 到 'FE' 在 GB/T 16649.6 中标注为 '私有', 在本上下文中应不予允许。	

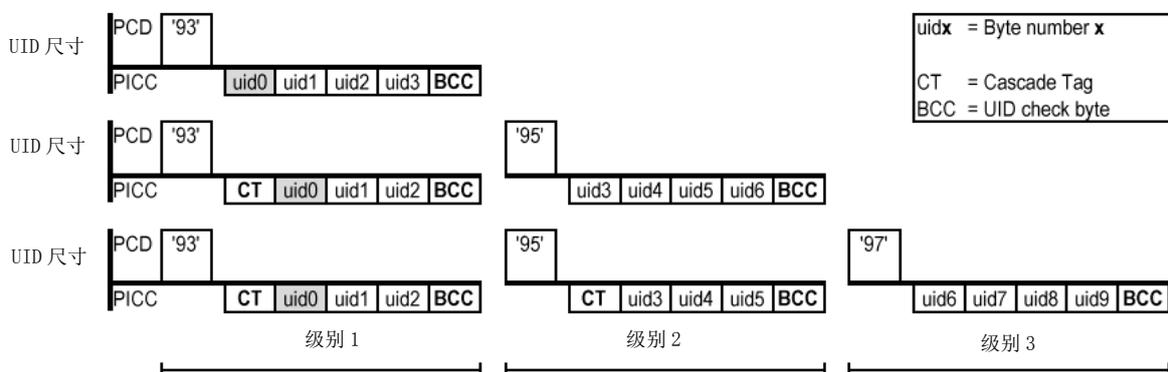


图17 串联级别的使用

注: 串联标记的用途是迫使造成与具有较小 UID 长度的 PICC 冲突。

下列算法应适用于PCD以获得完整UID:

——步骤 1: PCD 选择串联级别 1;

- 步骤 2: 应执行防冲突环;
- 步骤 3: PCD 应检验 SAK 的串联位;
- 步骤 4: 如果设置了串联位, PCD 应增加串联级别并初始化一个新的防冲突环。

7.3 Type B 的初始化和防冲突

本条描述了类型 Type B PICC 的初始化和冲突检测协议。

7.3.1 位、字节和帧的时序

本条定义了 Type B PICC 防冲突和通信初始化期间使用的字节、帧和命令的时序。关于位表示和编码见本部分第 6 章。

7.3.1.1 字符传输格式

PICC 和 PCD 之间的字节通过字符来发送和接收, 在防冲突序列期间, 字符的格式如下:

- 1 个逻辑“0”起始位;
- 8 个数据位发送, 首先发送 LSB;
- 1 个逻辑“1”停止位。

用一个字符执行一个字节的发送需要 10 etu, 如图 18 所示。

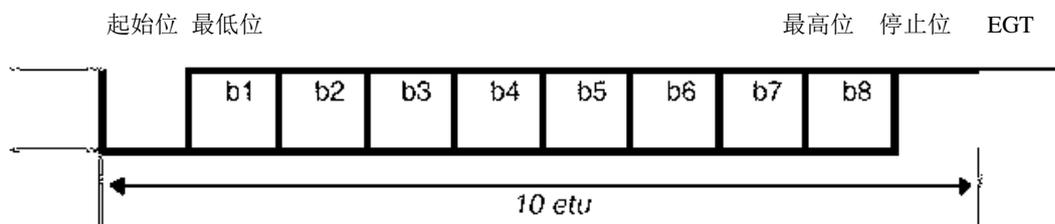


图 18 字符格式

一个字符范围内的位边界应出现在 $(n-0.125)$ etu 和 $(n+0.125)$ etu 之间, 其中 n 是起始位的下降沿之后的位边界数 ($1 \leq n \leq 9$)。

7.3.1.2 字符间距

一个字符与下一个发送的字符利用额外的保护时间 (EGT) 来隔开。

由 PCD 发送给 PICC 的两个连续字符之间的 EGT 应为 0 到 57 μs 之间的任何值。

由 PICC 发送给 PCD 的两个连续字符之间的 EGT 应具有 0 到 19 μs 之间的任何值。

7.3.1.3 帧格式

PCD 和 PICC 按帧发送字符, 帧格式见图 19。帧通常用 SOF (帧的起始) 和 EOF (帧的结束) 定界。关于异常情况见 7.3.10.3。



图 19 帧格式

7.3.1.4 SOF

SOF 如图 20 所示, 包括:

- 一个下降沿;
- 后面紧跟 10 个 etu 的逻辑 0;
- 后面紧跟位于下一个 etu 内任何地方的一个下降沿;
- 后面紧跟至少为 2 个 etu (但不超过 3 个 etu) 的逻辑 1。

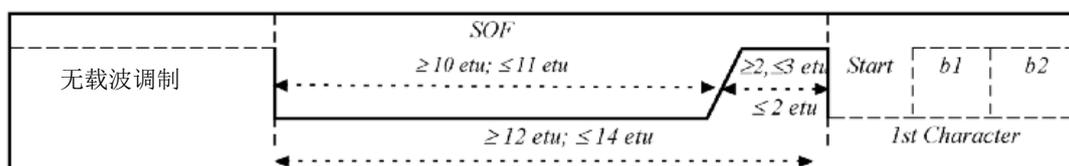


图20 SOF

7.3.1.5 EOF

EOF如图21所示，包括：

- 一个下降沿；
- 后面紧跟 10 个 etu 的逻辑 0；
- 后面紧跟位于下一个 etu 内任何地方的一个下降沿。

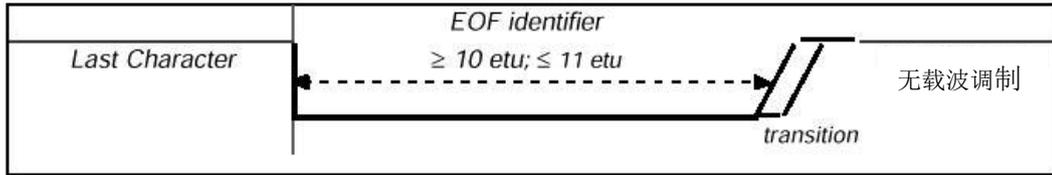


图21 EOF 标识符

注：收到假 EOF 的概率很低，并且对应于在错误收到停止位的情况下传输的 ‘00’ 字符。

7.3.1.6 PICC SOF 前的时序

在PCD数据传输之后，PICC开始的通信应遵守图22中定义的时序。

缺省的TR0和TR1最小值在6.5.2.5中定义，并且可以被PCD减小，见7.3.10.3。

TR0 的最大值为 $256/f_s$ （仅对 ATQB）和 $(256/f_s) * 2^{FWI}$ （对所有其他帧）（见 7.3.9.4.3）。

TR1 的最大值为 $200/f_s$ 。

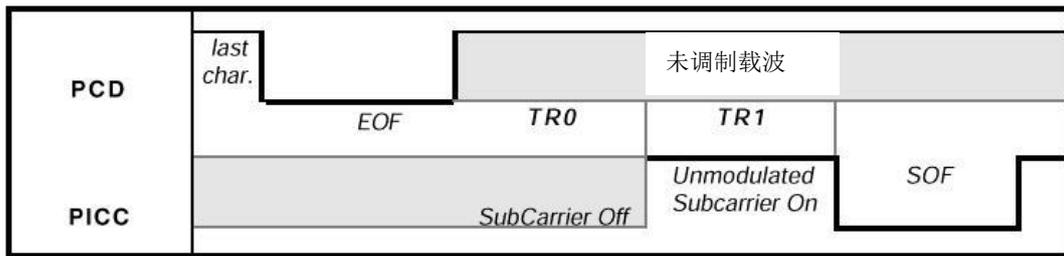


图22 PICC 副载波 SOF

仅当PICC打算开始发送信息时，它才可以接通副载波。

7.3.1.7 PCD SOF 前的时序

在PICC数据传输和EOF之后，PCD开始的通信应遵守图23中的时序。

在EOF传输之后，PICC应断开它的副载波。副载波信号应：

- 在 EOF 结束之前不能停止；
- 在 EOF 结束之后的 2 个 etu 内被停止。

PICC EOF 开始（下降沿）和 PCD SOF 开始（下降沿）之间的最小延迟为 $10\text{etu} + 32/f_s$ 。

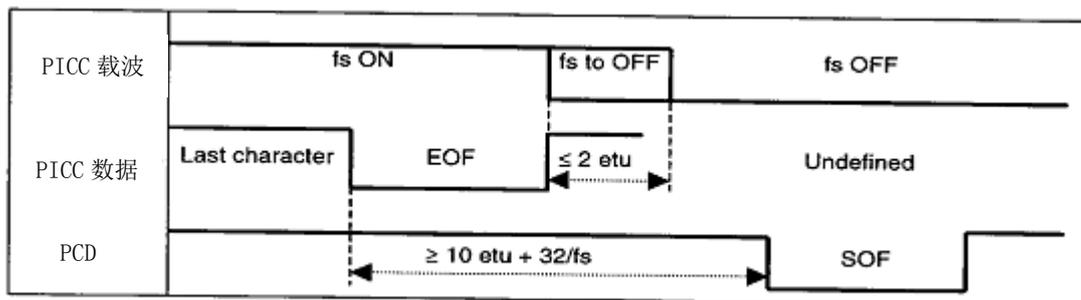


图23 PICC 到 PCD 的 SOF

7.3.2 CRC_B

1 st ,字节	
Data 字节 (N 字节)	CRC_B (2 字节)

图24 帧范围内 CRC_B 的位置

如果接收到的帧带有一个有效的CRC_B值，该帧才应被认为是正确的。帧范围内的CRC_B的位置见图24。

帧CRC_B是k个数据位的函数，该k个数据位由帧中的所有数据位组成，但不包括起始位、停止位、字节间的延迟、SOF和EOF以及CRC_B本身。由于数据按字节编码，因此位数k是8的倍数。

对于差错校验，帧包括了两个CRC_B字节，在数据字节之后，EOF之前。CRC_B在GB/T 7496中定义。寄存器初始内容为全1：“FFFF”。这两个CRC_B字节出现在k/8个数据字节之后和在EOF之前。

举例见附录C。

7.3.3 防冲突序列

PCD通过在本章中详述的命令集对防冲突序列进行管理。

PCD是与一个或多个PICC通信时的主控方，它通过发出REQB命令来启动卡的通信活动，以便提示PICC进行响应。

在防冲突序列期间，可能发生两个或两个以上的PICC同时响应：这就是冲突。命令集和允许PCD处理冲突序列以便及时分离PICC传输。

在完成防冲突序列后，PICC通信将完全处于PCD的控制之下，每次只允许一个PICC通信。

防冲突方案以时间槽的定义为基础，要求PICC在时间槽内用最小标识数据进行应答。时间槽数被参数化，范围从1到某一整数。在每一个时间槽内，PICC响应的概率也是可控制的。在防冲突序列中，PICC仅被允许应答一次。从而，即便在PCD场中有多个卡，在一个时间槽内也仅有一个卡应答，并且PCD在这个时间槽内能捕获标识数据。根据标识数据，PCD能够与被标识的卡建立一个通信信道。

防冲突序列允许选择一个或多个PICC以便在任何时候进行进一步的通信。

命令集允许在PCD级实现不同的防冲突管理策略。这个策略处在应用设计者的控制下，并且可包括：

- 概率的（响应概率小于或等于1的重复性单个时间槽提示）；
- 伪确定性的（扫描所有多个时间槽，以便在防冲突序列期间使所有在场的卡应答的概率最大）；
- 可动态进行的这些方法的组合。

7.3.4 PICC 状态描述

在防冲突序列期间，PICC具体的行为是根据不同的状态及状态间的转换条件确定的。

7.3.4.1 状态转换图

PICC状态转换流程的示例如图25所示。

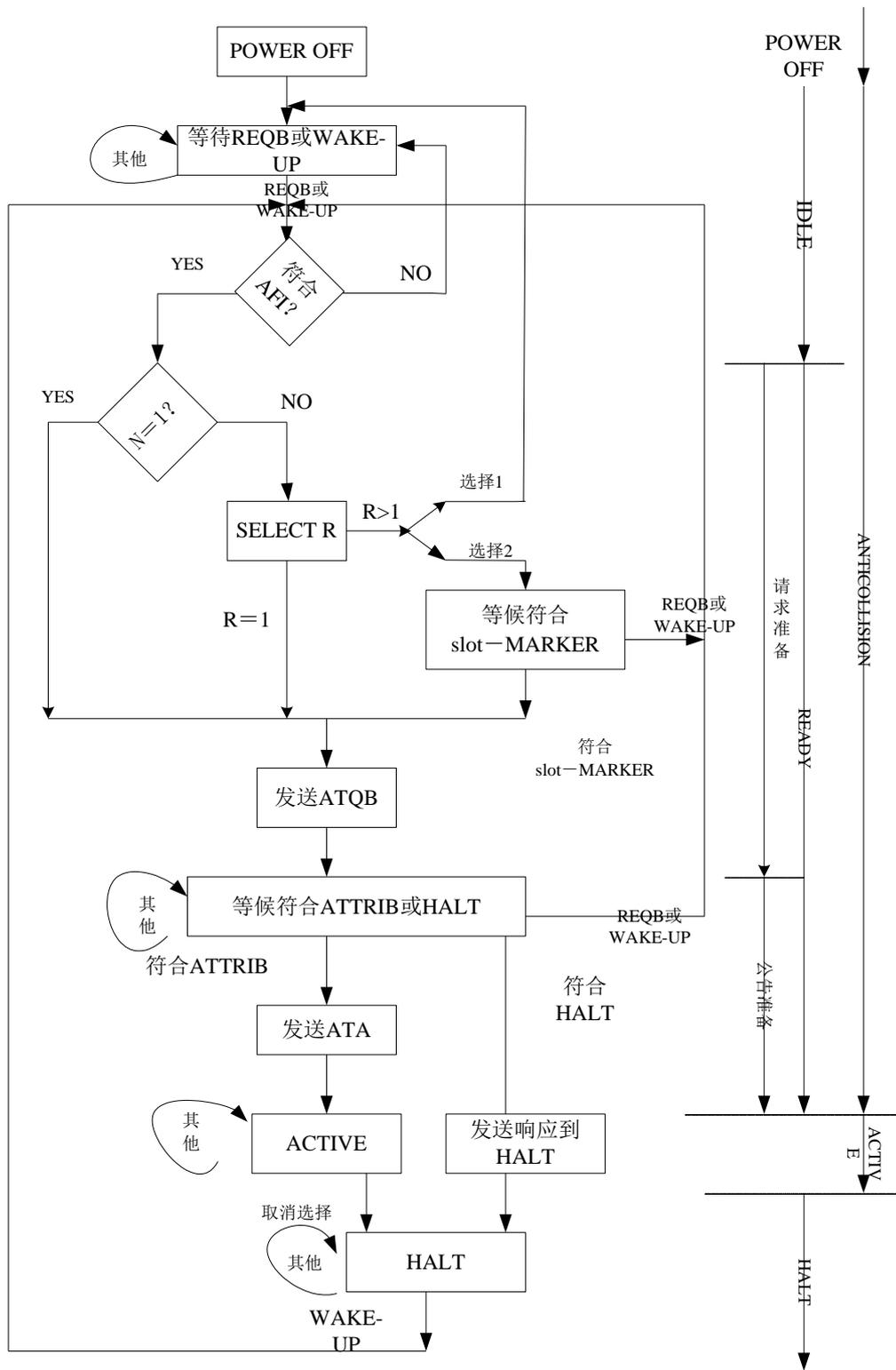


图25 PICC 状态转换流程图举例（提示的）

注 1: R 是 PICC 在 1 到 N (N 的编码见 7.3.7.4) 范围内选择的一个数。

注 2: 选项 1-对于 PICC 不支持 Slot-MARKER 命令 (概率方法)。

选项 2-对于 PICC 支持 Slot-MARKER 命令 (时间槽方法)。

7.3.4.2 状态描述和转换的概述

下述退出条件和转换适用于任何状态: 如果RF场消失, 则PICC返回到POWER-OFF状态。

下列备注适用于专门针对防冲突序列的任何状态（除ACTIVE状态外）：

- 使用前几条中定义的缺省通信参数；
- 除发送前几条中规定的响应帧，PICC 应不发射副载波；
- 当 PICC 加电并正确复位时，它收听从 PCD 收到的任何命令帧；
- 若来自 PCD 的帧是有效的（正确的 CRC_B），则 PICC 执行要求的动作和/或根据其状态进行响应；

注：在防冲突命令中，帧中数据的前三位是 (101) b（防冲突前缀字节的前三位）。

- PICC 不应答任何不以 (101) b（防冲突前缀字节的前三个位）开始的命令帧；
- PICC 仅对收到的有效帧进行反应（当检测到传输差错时不发送响应）。

7.3.4.3 POWER-OFF 状态

描述：

在POWER-OFF状态下，PICC因缺乏载波能量而不加电。

状态退出条件和转换：

如果 PICC 处于一个能量大于 H_{min} （见第 6 章）的激励磁场，则它应在不大于 t_{ORB} 的延迟范围内进入其 IDLE 状态。

7.3.4.4 IDLE 状态

描述：

在IDLE状态下，PICC是加电的，它收听帧并应识别REQB信息。

状态退出条件和转换：

一旦收到一个有效的REQB或WUPB命令帧，PICC就进入READY-REQUESTED状态。（有效的REQB或WUPB命令指具有REQB/WUPB命令并匹配AFI的有效帧。详见REQB/WUPB命令规范）。

7.3.4.5 READY-REQUESTED 状态

描述：

在READY-REQUESTED状态下，PICC是加电的，并且定义了一个唯一的时间槽用来发送其ATQB（如果有）。

它收听帧并应识别REQB和Slot-MARKER报文。

状态退出条件和转换：

见7.3.6。

7.3.4.6 READY-DECLARED 状态

描述：

在READY-DECLARED状态下，PICC是加电的，并且发送了与收到的最后一个有效REQB报文相对应的其ATQB。

它收听帧并应识别REQB和ATTRIB报文。

状态退出条件和转换：

一旦收到带有ATTRIB命令的有效帧，当且仅当ATTRIB命令中的PUPI与PICC的PUPI匹配时，PICC才应进入ACTIVE状态。

若ATTRIB命令中的PUPI与PICC的PUPI不匹配，则PICC仍保持在READY-DECLARED状态。

一旦收到有效REQB命令帧，状态退出条件和转换按在IDLE状态下接收到有效REQB命令帧。

一旦收到匹配的HALT命令，PICC应进入HALT状态。

7.3.4.7 ACTIVE 状态

描述：

PICC是加电的，并且自从信道号（CID）已经通过ATTRIB命令已分配给该PICC以来，PICC便进入上层模式。

它收听正确格式化（正确的CID和有效的CRC_B）的任何上层报文。

PICC应不在任何带有无效CRC_B或带有另一个CID（不是所分配的那个CID）的帧以后发射副载波。

状态退出条件和转换：

当收到有效的HALT命令帧时，PICC进入HALT状态。

特定备注：

应该不应答有效REQB或Slot-MARKER帧。

应该不应答带有ATTRIB命令的有效帧。

在上层协议中，可以定义特定的命令用来把PICC返回到其他状态（IDLE或HALT）。只有在收到这样的命令以后，PICC才可以返回到这些状态。

7.3.4.8 HALT 状态

描述：

PICC仅响应使它回到IDLE状态的WAKE-UP命令。

状态退出条件和转换：

如果RF场消失，则PICC返回到POWER-OFF状态。

7.3.5 命令集合

四个基本的命令可用来管理多结点通信信道：

- REQB/WUPB；
- Slot-MARKER；
- ATTRIB；
- HALT。

所有这四个命令都使用了上面详述的字节、帧格式和时序。

这些命令以及PICC对这些命令的响应在下列各条中描述。

所收到的带有错误格式的帧（错误的帧标识符或无效的CRC_B）应忽略。

7.3.6 防冲突响应规则

在READY-REQUESTED子状态中的PICC，在接收到有效的REQB/WUPB命令（要求AFI=0或AFI与内部请求匹配）后，应根据下列规则响应：（其中参数N在REQB/WUPB命令中给出）

- 若 N=1，则 PICC 将发送一 ATQB 并进入 READY-DECLARED 子状态；
- 若 N>1，则 PICC 将内部产生一在 1 到 N 之间均匀分布的随机数 R；
- 若 R=1，则 PICC 将发送一 ATQB 并进入 READY-DECLARED 子状态；
- 若 R>1：
 - 采用概率路径（参考选项 1）的 PICC 将返回到 IDLE 状态；
 - 在发送 ATQB 并进入 READY-DECLARED 子状态前，采用时间槽路径（参考选项 2）的 PICC 将等待至收到一带有匹配时间槽号（槽号=R）的 Slot-MARKER 命令。

7.3.7 REQB/WUPB 命令

由PCD所发出的REQB命令用来探测Type B PICC的场。

时间槽编号（或每个时间槽内的响应概率）N作为一个参数包含在REQB命令中，以优化给定应用的防冲突算法。每个不处于ACTIVE或HALT状态（即处于IDLE或READY状态）的PICC应处理该报文，并选择它将在哪个时间槽（每个时间槽被选中的概率都为1/N）内返回它的ATQB响应信息。

7.3.7.1 REQB/WUPB 命令格式

REQB/WUPB命令由PCD发出，长度为5个字节，格式见图26。

1 st 字节	2 nd 字节	3 rd 字节	4 th 、5 th 字节
Apf (1 字节)	AFI (1 字节)	PARAM (1 字节)	CRC_B (2 字节)
MSB LSB	MSB LSB	MSB LSB	MSB LSB

图26 REQB/WUPB 命令格式

7.3.7.2 防冲突前缀字节 APf 的编码

防冲突前缀字节 APf = '05' = (0000 0101) b。

7.3.7.3 AFI 的编码

AFI (应用族标识符) 代表由PCD所瞄准的应用类型, 编码规则见表14。AFI可用来在ATQB之前预先选择PICC: 只有那些具有由AFI所指出的类型的应用的PICC才可以应答AFI不等于'00'的REQB命令。

当AFI等于'00', 所有PICC应处理REQB。

AFI的最高有效半字节可用来编码按表14定义的某个特定的应用族或所有应用族。

AFI的最低有效半字节可用来编码某个特定应用子族或所有应用子族。不同于0的子族代码是专有的。

表14 AFI 的编码

AFI 最高有效半字节	AFI 最低有效半字节	含义-PICC 响应来自	举例/注释
'0'	'0'	所有族和子族	没有应用预选
'X'	'0'	族 X 的所有子族	广泛的应用预选
'X'	'Y'	仅族 X 的第 Y 个子族	
'0'	'Y'	仅专有的子族 Y	
'1'	'0', 'Y'	运输	集团运输、汽车、航空公司……
'2'	'0', 'Y'	金融	IEP、银行、零售……
'3'	'0', 'Y'	标识	门禁控制……
'4'	'0', 'Y'	电信	公用电话、GSM……
'5'	'0', 'Y'	医学	
'6'	'0', 'Y'	多媒体	因特网服务……
'7'	'0', 'Y'	博彩	
'8'	'0', 'Y'	数据存储	可移植文件……
'9' — 'F'	'0', 'Y'	RFU	

注: X = '1' 到 'F', Y = '1' 到 'F'。

7.3.7.4 PARAM 的编码

PARAM的编码规则见图27。

RFU				REQB/WUPB	N (时间槽的数)		
b8=0	b7=0	b6=0	b5=0	b4	b3	b2	b1

图27 PARAM 的编码

b4=0: “正常请求” (PICC在Idle状态或Ready状态下处理该请求)

b4=1: “请求所有” (PICC在Idle状态或Ready状态或HALT状态下处理该请求)

b1到b3用来编码对应表15的时间槽N的数。

表15 N 的编码

b3b2b1	N
000	1=2 ⁰
001	2=2 ¹
010	4=2 ²
011	8=2 ³
100	16=2 ⁴
101	RFU
11x	RFU

注：对于每个 PICC，在第一个时间槽内响应（ATQB）的概率应为 1/N。因此，如果 PCD 中使用了概率的方法，则 N 不可用来调整时间槽的编号，而是在这个唯一的时间槽内 PICC 返回它的 ATQB 的概率。

7.3.8 Slot-MARKER 命令

在REQB/WUPB命令之后，PCD可发送至多（N-1）个时间槽标记来定义每个时间槽的开始。

时间槽标记可以：

——在 PCD 收到的 ATQB 报文结束之后被发送，以便标记下一个时间槽的开始；

——如果没有收到 ATQB（如果已知该时间槽为空，则不必等到该时间槽结束），则较早地被发送。

不强制PICC支持该命令。在这种情况下，PICC应忽略任何Slot-MARKER命令。在概率方法中，在REQB（在第一个时间槽里）后，PICC仅可在第一个时间槽内发送其ATQB。

7.3.8.1 Slot-MARKER 命令格式

该命令由PCD发送，大小为3字节，格式见图28。

1 st 字节		2 nd , 3 rd 字节	
APn (1 字节)		CRC_B (2 字节)	
MSB	LSB	MSB	LSB

图28 Slot-MARKER 命令格式

7.3.8.2 防冲突前缀字节 APn 的编码

APn = (nnnn 0101) b, 其中nnnn是时间槽标记的编号，编码规则见表16。

表16 时间槽编号的编码

nnnn	时间槽编号
0001	2
0010	3
0011	4
.....
1110	15
1111	16

注：不强制时间槽标记按递增的时间槽编号顺序来发送。

7.3.9 ATQB (Type B 的请求应答) 响应

对REQB和Slot-MARKER命令的响应都被称作ATQB（请求应答）。

ATQB有固定长度（14个字节）和限定的持续时间。

仅对于 ATQB，第 6 章中定义的 TR0 应不大于 256/f_s。

7.3.9.1 ATQB 响应格式

ATQB 的格式见图 29。

1 st 字节	2 nd , 3 rd , 4 th , 5 th 字节	6 th , 7 th , 8 th , 9 th 字节	10 th , 11 th , 12 th 字节	13 th , 14 th 字节
'50' (1 字节)	PUPI (4 字节)	应用数据 (4 字节)	协议信息 (3 字节)	CRC_B (2 字节)
MSB	LSB	MSB	LSB	MSB
	MSB	LSB	MSB	LSB

图29 ATQB 格式

7.3.9.2 PUPI (伪唯一 PICC 标识符)

伪唯一PICC标识符（PUPI）可用来区分防冲突期间的不同PICC。这4字节数可以是PICC动态产生的一个数或一个多样化的固定数。

7.3.9.3 应用数据

应用数据字段用来通知PCD在PICC上当前安装了哪些应用。这个信息使得在有多个PICC存在时，PCD能选择想要的PICC。

应用数据字段根据协议信息（见7.3.9.4）中的ADC（应用数据编码）定义，该协议信息定义了用下面描述的CRC_B压缩方法还是用专有编码。

当使用CRC_B压缩方法时，应用数据字段包含见图30。

1 st 字节	2 nd , 3 rd 字节	4 th 字节
AFI (1 字节)	CRC_B (AID) (2 字节)	应用的编号 (1 字节)
MSB	LSB MSB	LSB MSB LSB

图30 应用数据格式

7.3.9.3.1 AFI

对单应用PICC，AFI给出了应用族（见表14 AFI的编码）。

对多应用PICC，AFI给出了CRC_B (AID) 中描述的应用族。

7.3.9.3.2 CRC_B (AID)

CRC_B (AID) 是PICC中应用的AID（如GB/T 16649.5中定义）的CRC_B计算的结果，PICC与REQB/WUPB命令中给出的AFI匹配。

7.3.9.3.3 应用的编号

指出了PICC中的其他应用。

最高有效半字节值给出应用的编号，与应用数据中给出的AFI相一致，‘0’意味着没有应用，‘F’意味着15个应用或更多。

最低有效半字节值给出PICC中应用的所有编号，‘0’意味着没有应用，‘F’意味着15个应用或更多。

7.3.9.4 协议信息

该字段指示了卡所支持的参数。协议信息的具体格式见图31。

1 st 字节	2 nd 字节	3 rd 字节
位速率能力 (8 位)	最大帧长度 (4 位)	协议类型 (4 位)
MSB	LSB MSB	LSB MSB LSB
		FWI (4 位)
		ADC (2 位)
		F0 (2 位)

图31 协议信息格式

7.3.9.4.1 FO

PICC支持的帧选项定义见表17。

表17 PICC 支持的帧选项

b2	b1	含义
1	x	PICC 支持的 NAD
x	1	PICC 支持的 CID

7.3.9.4.2 ADC

PICC支持的应用数据编码定义见表18。

表18 PICC 支持的应用数据编码

b4	b3	含义
0	0	应用是专有的
0	1	应用如 7.3.9.3 中编码
其他值为 RFU		

7.3.9.4.3 FWI

帧等待时间整数（4位）：

FWI编码—整数数值用来定义FWT。

FWT定义了PCD帧结束后PICC开始响应的最大时间。

FWT根据下面的公式计算：

$$FWT = (256 \times 16 / f_c) \times 2^{FWI}$$

其中FWI的值在0到14之间，值15为RFU。

对于FWI=0，FWT为最小（~302μ s）；

对于FWI=14，FWT为最大（~4949ms）。

7.3.9.4.4 协议类型

PICC支持的协议类型见表19。

表19 PICC 支持的协议类型

b4	b3	b2	b1	含义
0	0	0	1	PICC 支持 JR/T 0025 的本部分
0	0	0	0	PICC 不支持 JR/T 0025 的本部分
其他值是 RFU				

7.3.9.4.5 最大帧长度

最大帧长度对照关系见表20。

表20 最大帧长度

ATQB 中的最大帧长度代码	0	1	2	3	4	5	6	7	8	9—F
最大帧长度（字节）	16	24	32	40	48	64	96	128	256	RFU>256

7.3.9.4.6 位速率能力

PICC支持的位速率见表21。

表21 PICC 支持的位速率

b8	b7	b6	b5	b4	b3	b2	b1	含义
0	0	0	0	0	0	0	0	在两个方向上 PICC 仅支持 106kbits/s
1	x	x	x	0	x	x	x	从 PCD 到 PICC 和从 PICC 到 PCD 强制相同的位速率
x	x	x	1	0	x	x	x	PICC 到 PCD, 1etu=64/f _c , 支持的位速率为 212kbit/s
x	x	1	x	0	x	x	x	PICC 到 PCD, 1etu=32/f _c , 支持的位速率为 424kbit/s
x	1	x	x	0	x	x	x	PICC 到 PCD, 1etu=16/f _c , 支持的位速率为 847kbit/s
x	x	x	x	0	x	x	1	PCD 到 PICC, 1etu=64/f _c , 支持的位速率为 212kbit/s
x	x	x	x	0	x	1	x	PCD 到 PICC, 1etu=32/f _c , 支持的位速率为 424kbit/s
x	x	x	x	0	1	x	x	PCD 到 PICC, 1etu=16/f _c , 支持的位速率为 847kbit/s
其他值（b4=1）为 RFU								

7.3.10 ATTRIB 命令

PCD发送的ATTRIB命令应包括选择单个PICC所要求的信息。

收到一个带有其标识符的ATTRIB命令的PICC就成为选中的，并分配到一个专用信道。在选中之后，该PICC仅响应第8章中定义的包括其唯一CID的命令。

7.3.10.1 ATTRIB 命令格式

TTRIB命令的格式见图32。

1 st 字节	2 nd , 3 rd , 4 th , 5 th 字节	6 th 字节	7 th 字节	8 th 字节	9 th 字节	10 th , ……字 节	
--------------------	---	--------------------	--------------------	--------------------	--------------------	-----------------------------	--

'1D' (1 字节)	标识符 (4 字节)	参数 1 (1 字节)	参数 2 (1 字节)	参数 3 (1 字节)	参数 4 (1 字节)	上层 INF (可选-0 或 多个字节)	CRC_B (2 字节)
MSB LSB	MSB LSB	MSB LSB	MSB LSB	MSB LSB	MSB LSB	MSB LSB	MSB LSB

图32 ATTRIB 格式

7.3.10.2 标识符

该标识符是PICC发送的ATQB中的PUPI的值。

7.3.10.3 参数 1 的编码

参数1的编码格式见图33。

b8	B7	b6	b5	b4	b3	b2	b1
最小 TR0		最小 TR1		EOF	SOF	RFU	
若无其他规定，所有 RFU 位应置为 0							

图33 PARAM 1 的编码

7.3.10.3.1 最小 TR0

最小TR0向PICC指示在PCD发送的命令结束之后，进行响应之前的最小延迟。6.5.2.5规定了TR0的缺省值。TR0编码格式见表22。

表22 TR0 编码

b8	b7	最小 TR0
0	0	缺省值
0	1	$48/f_s$
1	0	$16/f_s$
1	1	RFU

注：当从传输转换到接收时，最小 TR0 由 PCD 要求，并且其值依赖于 PCD 的执行。

7.3.10.3.2 最小 TR1

最小TR1向PICC指示副载波调制开始和数据传输开始之间的最小延迟。6.5.2.5规定了TR1的缺省值。TR1编码格式见表23。

表23 TR1 编码

b6	b5	最小 TR1
0	0	缺省值
0	1	$64/f_s$
1	0	$16/f_s$
1	1	RFU

注：最小 TR1 是 PCD 为与 PICC 同步所要求的，并且其值依赖于 PCD 的执行。

7.3.10.3.3 EOF/SOF

b3和b4指示PCD有能力抑制从PICC到PCD的EOF或SOF中断，该能力可以减少通信开销。对PICC，抑制EOF和/或SOF是任选的。b3和b4的编码分别见表24和表25。

表24 SOF 处理

b3	SOF 要求
0	是
1	否

表25 EOF 处理

b4	EOF 要求
----	--------

0	是
1	否

7.3.10.4 参数 2 的编码

最低有效半字节 (b4到b1) 可用来编码表23中规定的可被PCD接收到的最大帧长度。参数2的编码格式见表26。

表26 参数 2 的 b4 到 b1 的编码

ATQB 中最大帧长度代 码	0	1	2	3	4	5	6	7	8	9—F
最大帧长度 (字节)	RFU	RFU	32	40	48	64	96	128	256	RFU>256

最高有效半字节b8到b5用于位速率选择, 如表27和表28所规定。

表27 参数 2 的 b6&b5 的编码

b6	b5	含义
0	0	PCD 到 PICC, letu=128/f _c , 位速率为 106kbit/s
0	1	PCD 到 PICC, letu=64/f _c , 位速率为 212kbit/s
1	0	PCD 到 PICC, letu=32/f _c , 位速率为 424kbit/s
1	1	PCD 到 PICC, letu=16/f _c , 位速率为 847kbit/s

表28 参数 2 的 b8&b7 的编码

b8	b7	含义
0	0	PICC 到 PCD, letu=128/f _c , 位速率为 106kbit/s
0	1	PICC 到 PCD, letu=64/f _c , 位速率为 212kbit/s
1	0	PICC 到 PCD, letu=32/f _c , 位速率为 424kbit/s
1	1	PICC 到 PCD, letu=16/f _c , 位速率为 847kbit/s

7.3.10.5 参数 3 的编码

b4 b3 b2 b1=0001

b8 b7 b6 b5=RFU=0000

7.3.10.6 参数 4 的编码

参数4包含下列两部分:

——最低有效半字节 (b4 到 b1) 被称为卡标识符 (CID), 并定义了 在 0 到 14 范围内寻址 PICC 的逻辑号。值 15 为 RFU。CID 由 PCD 规定并对所有在同一时刻处于 ACTIVE 状态的 PICC 是唯一的。如果 PICC 不支持 CID, 应使用编码值 (0000) b;

——最高有效半字节 (b8 到 b5) 被置为 (0000) b, 所有其他值为 RFU。

7.3.10.7 上层 INF

任何上层命令都可以包括在内。

不强制PICC成功地处理在上下文中的任何命令。

但是如果不包含任何应用命令, PICC仍应成功地处理这种报文。

7.3.11 对 ATTRIB 命令的应答

PICC应使用下面描述的格式对任何有效的ATTRIB命令 (正确的PUPI和有效的CRC_B) 进行应答。对ATTRIB命令的应答格式见图34。

1 st 字节		2 nd , 字节	
MBLI	CID	上层响应	CRC_B
(1 字节)		(可选 0 或多个字节)	(2 字节)
MSB	LSB	MSB	LSB

图34 对 ATTRIB 命令的应答格式

第一个字节由两部分组成：

- 最低有效半字节（b4 到 b1）包含返回的 CID。如果 PICC 不支持 CID，将返回编码值（0000）b；
- 最高有效半字节（b8 到 b5）称为最大缓冲区长度索引（MBLI）。它由 PICC 使用以使 PCD 知道接收链帧的内部缓冲区的限制。

MBLI 的编码如下：

- MBLI=0 意味着 PICC 不提供内部缓冲区大小的信息；
- MBLI>0 用于根据下面的公式计算实际内部最大缓冲区长度（MBL）：

$$MBL = (\text{PICC 最大帧长度}) * 2^{(MBLI-1)},$$

其中 PICC 最大帧长度由 PICC 在其 ATQB 中返回。当 PCD 返回链帧给 PICC 时，它将确保计算出来的长度不大于 MBL。

其余字节是可选和用于上层响应的。

如图35所示，PICC应使用一个空的上层响应来应答空（没有上层INF字段）ATTRIB命令。

1 st 字节		2 nd , 3 rd 位	
MBLI	CID	CRC_B	
(1 字节)		(2 字节)	
MSB	LSB	MSB	LSB

图35 PICC 对 ATTRIB 的应答

注 1：对 ATTRIB 命令（如图 34 和 35 所定义）的有效应答（相同 CID 和有效的 CRC_B）是 PCD 检测 PICC 选择已成功的手段。

注 2：只要 PICC 响应满足上面描述的格式，就可以指示允许在本上下文中 PICC 不支持上层命令的上层响应。

7.3.12 HLTB 命令及应答

HALT命令用于将PICC置为HALT状态，因而对正常REQB没有更多的响应。

对该命令应答后，PICC仅对WUPB命令应答。

HALT命令的格式见图36。

1 st 字节		2 nd , 3 rd , 4 th , 5 th 字节		6 th , 7 th 字节	
'50'		识别符		CRC_B	
(1 字节)		(4 字节)		(2 字节)	
MSB	LSB	MSB	LSB	MSB	LSB

图36 HLTB 命令格式

4字节标识符为PICC发送的ATQB中PUPI的值。

对来自PICC的HLT命令的应答的格式见图37。

1st 字节		2nd, 3rd 字节	
'00'		CRC_B	
(1 字节)		(2 字节)	
MSB	LSB	MSB	LSB

图37 PICC 对 HLTB 命令应答的格式

8 传输协议

8.1 Type A PICC 的协议激活

应使用下列激活序列：

- 如第 7 章中所定义的 PICC 激活序列（请求、防冲突环和选择）；
- 为获得 ATS，在开始应校验到 SAK 字节。SAK 在第 7 章中定义；

- 如果没有获得 ATS，使用第 7 章中定义的 HALT 命令，PICC 可被置为 HALT 状态；
- 如果获得了 ATS，在接收到 SAK 后，PCD 可发送 RATS 作为下一条命令；
- PICC 应发送其 ATS 作为对 RATS 的应答。如果在选择后直接接收到 RATS，则 PICC 应仅应答 RATS；
- 如果 PICC 在 ATS 中支持任何变化的参数，PCD 可使用 PPS 请求作为接收到 ATS 后的下一条命令，并用其来改变参数；
- PICC 应发送 PPS 响应作为对 PPS 请求的应答。

如果 PICC 在 ATS 中不支持任何变化的参数，则它无需执行 PPS。

图 38 示出了从 PCD 角度来看的 Type A PICC 激活序列。

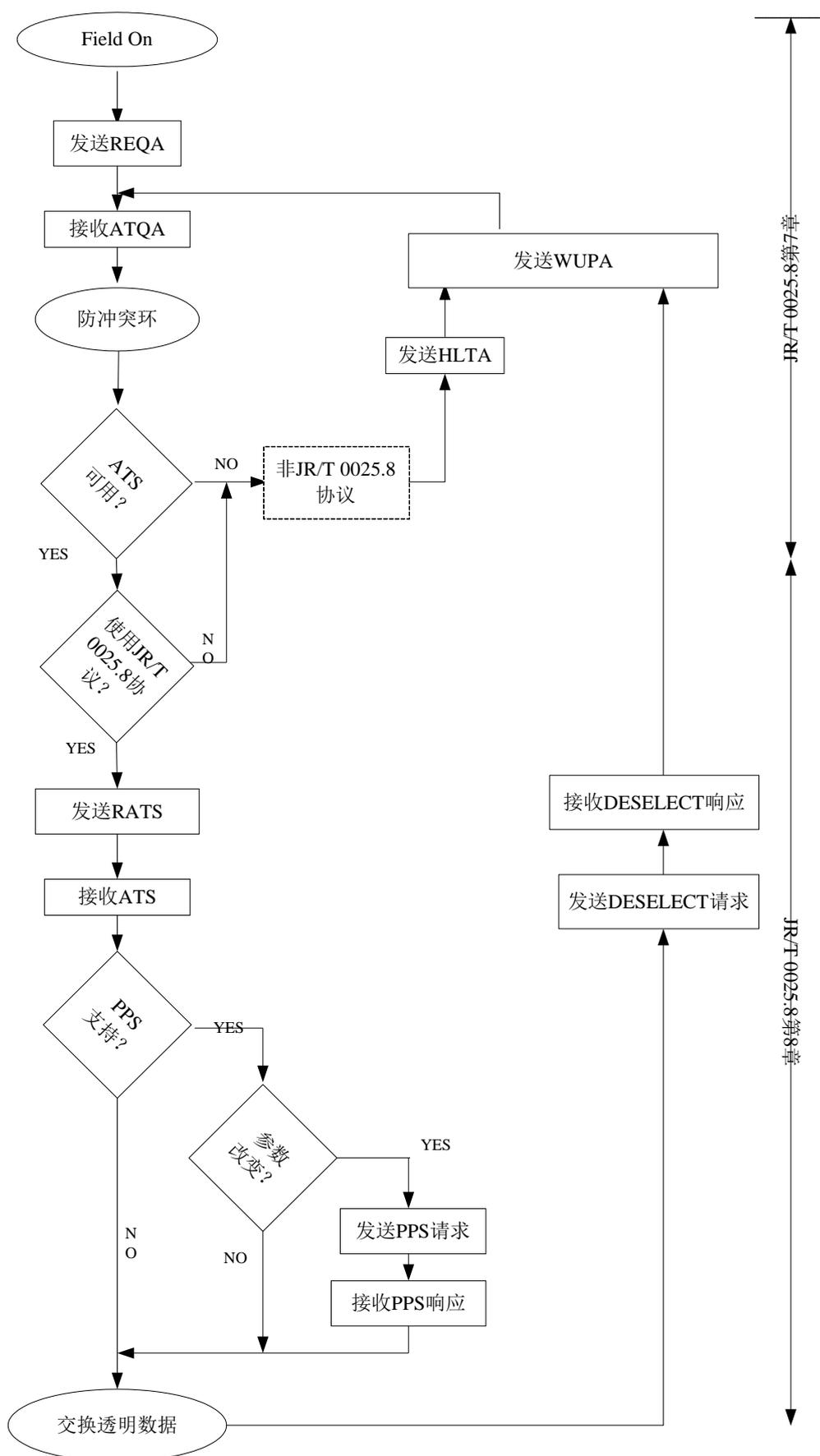


图38 从 PCD 角度来看的 Type A PICC 激活

8.1.1 选择应答请求

本条定义了带有所有字段的RATS（见图39）。

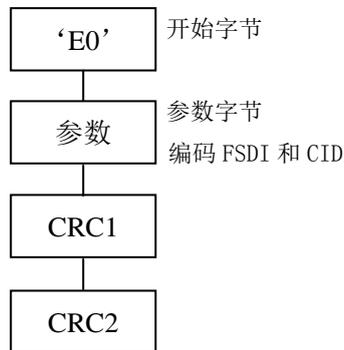


图39 选择应答请求

参数字节由两部分组成（见图40）：

- 最高有效半字节 b8 到 b5 称为 FSDI，它用于编码 FSD。FSD 定义了 PCD 能收到的帧的最大长度。FSD 的编码在表 29 中给出；
- 最低有效半字节 b4 到 b1 命名为 CID，它定义编址了的 PICC 的逻辑号在 0 到 14 范围内。值 15 为 RFU。CID 由 PCD 规定，并且对同一时刻处在 ACTIVE 状态中的所有 PICC，它应是唯一的。CID 在 PICC 被激活期间是固定的，并且 PICC 应使用 CID 作为其逻辑标识符，它包含在接收到的第一个无差错的 RATS。

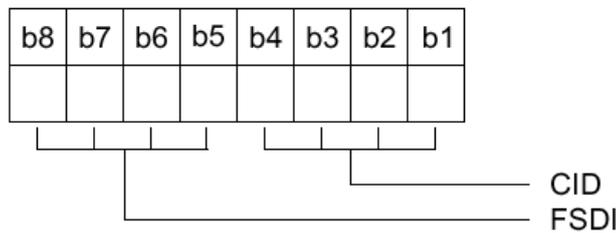


图40 RATS 参数字节的编码

表29 FSD 到 FSDI 的转换

FSDI	'0'	'1'	'2'	'3'	'4'	'5'	'6'	'7'	'8'	'9'—'F'
FSD (字节)	16	24	32	40	48	64	96	128	256	RFU >256

8.1.2 选择应答

本章定义了带有所所有可用字段的ATS（见图41）。

在已定义字段中的一个没有在PICC发送的ATS中出现的情况下，应应用该字段的缺省值。

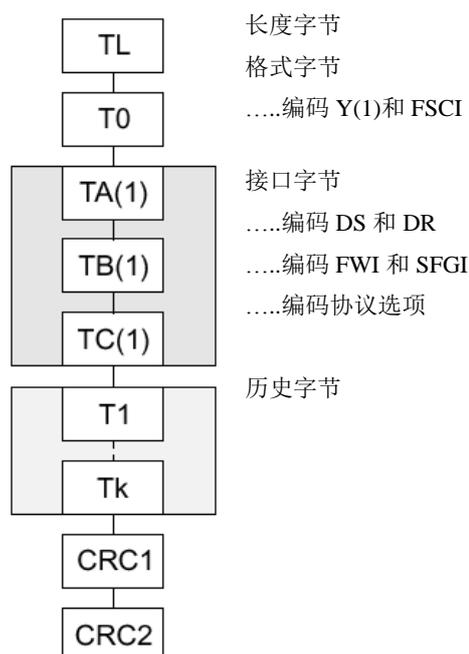


图41 ATS 的结构

8.1.2.1 字节结构

长度字节TL以下面的顺序跟随着可选后续字节的可变号码：

- 格式字节 T0；
- 接口字节 TA (1) ， TB (1) ， TC (1) ；
- 应用信息字节 T1 到 TK。

8.1.2.2 长度字节

长度字节TL是强制的，它规定了传送的ATS（包括其本身）的长度。两个CRC字节并不包括在TL中。ATS的最大长度应不超出指示的FSD。因此TL的最大值应不超过FSD-2。

8.1.2.3 格式字节

格式字节T0是强制的，并且当长度大于1，它便出现。当该格式字节出现时，ATS能仅包含下列可选字节。

T0由三部分组成（见图42）：

- 最高有效位 b8 应置为 0，其他值为 RFU；
- 包含 Y (1) 的位 b7 到 b5 指示接口字节 TC (1) ， TB (1) 和 TA (1) 的出现；
- 最低有效半字节 b4 到 b1 称为 FSCI，它用于编码 FSC。FSC 定义了 PICC 能接收的帧的最大长度。FSCI 的缺省值为 2，这导致了一 32 字节的 FSC。FSC 的编码等于 FSD 的编码（见表 29）。

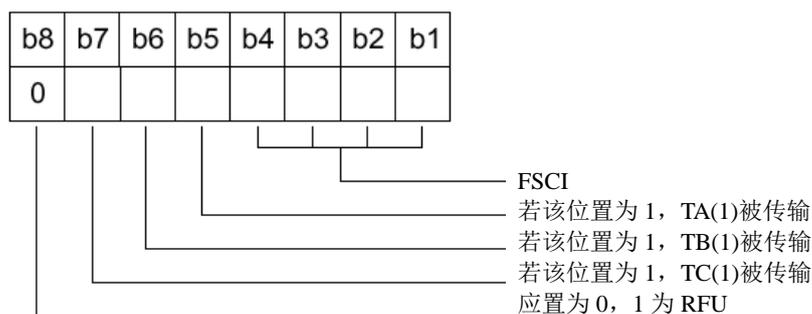


图42 格式字节的编码

8.1.2.4 接口字节 TA (1)

接口字节TA (1) 由四部分组成 (见图43) :

- 最高有效位 b8 编码了为每个方向处理不同除数的可能性。当该位被置为 1 时, PICC 不能为每个方向处理不同除数;
- 位 b7 到 b5 为 PICC 到 PCD 方向编码了 PICC 的位速率能力, 称为 DS。其缺省值应为 (000) b;
- 位 b4 被置为 (0) b, 其他值为 RFU;
- 位 b3 到 b1 为 PCD 到 PICC 方向编码了 PICC 的位速率能力, 称为 DR。其缺省值应为 (000) b。

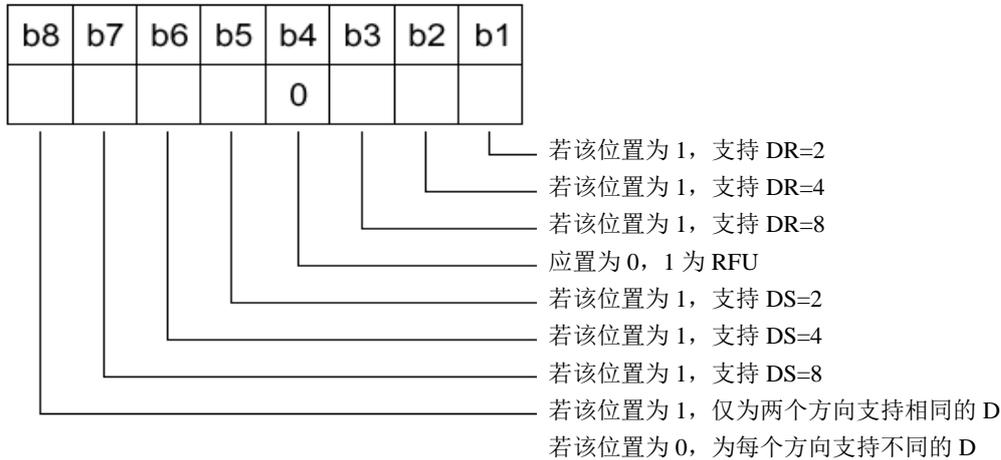


图43 接口字节 TA (1) 的编码

为每个方向选择特定除数可以使用PPS由PCD来完成。

8.1.2.5 接口字节 TB (1)

接口字节TB (1) 运送信息以定义帧等待时间和启动帧保护时间。

接口字节TB (1) 由两部分组成 (见图44) :

- 最高有效半字节 b8 到 b5 称为 FWI, 它编码 FWT (见 8.3.2) ;
- 最低有效半字节 b4 到 b1 称为 SFGI, 它编码了一乘数值用于定义 SFGT。SFGT 定义了发送了 ATS 之后, 准备接收下一个帧之前 PICC 所需的特定保护时间。SFGI 在 0 到 14 范围内编码。值 15 为 RFU。值 0 指示无需 SFGT, 在 1 到 14 范围内的值用于用下面给出的公式计算 SFGT。SFGI 的缺省值为 0。

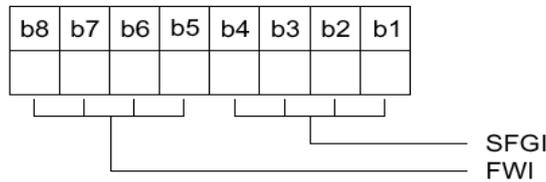


图44 接口字节 TB (1) 的编码

SFGT 用下面的公式计算:

$$SFGT = (256 \times 16 / f_c) \times 2^{SFGI}$$

SFGT_{MIN} = 第 7 章定义的帧延迟时间最小值

SFGT_{DEFAULT} = 第 7 章定义的帧延迟时间最小值

SFGT_{MAX} ≈ 4949ms

8.1.2.6 接口字节 TC (1)

接口字节TC (1) 规定了协议的参数。

特定接口字节TC (1) 由两部分组成 (见图45) :

- 最高有效位 b8 到 b3 为 000000b, 所有其他值为 RFU;
- 位 b2 和 b1 定义了 PICC 支持的开端字段中的可选字段。允许 PCD 跳过已被指出被 PICC 支持的字段, 但 PICC 不支持的字段应不被 PCD 传输。缺省值应为 (10) b, 它指出支持 CID 和不支持 NAD。

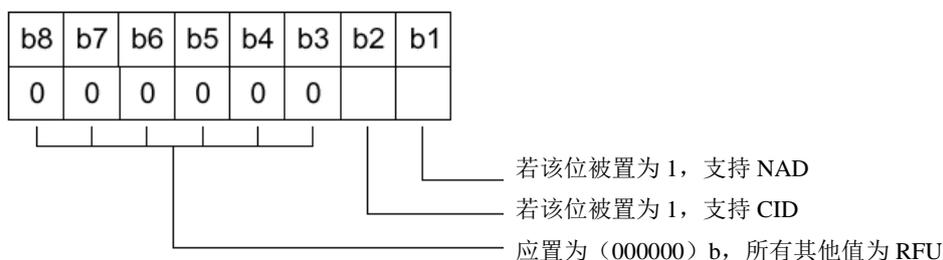


图45 接口字节 TC (1)

8.1.2.7 历史字节

历史字节T1到Tk是可选的并包含了通用信息。ATS的最大长度给出了历史字节的最大可能数目。ISO/IEC 7816-4规定了历史字节的内容。

8.1.3 协议和参数选择请求

PPS请求包含着被格式字节和一参数字节跟随的开始字节 (见图46)。

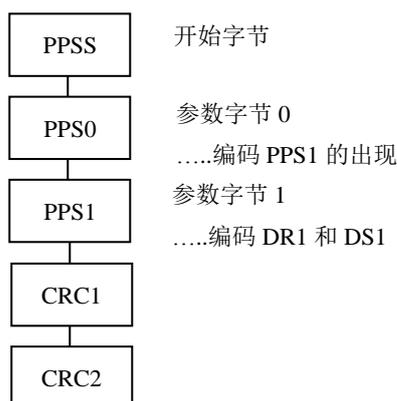


图46 协议和参数选择请求

8.1.3.1 开始字节

PPSS包含两部分 (见图47) :

- 最高有效半字节 b8 到 b5 应置为 'D' 并标识了 PPS;
- 最低有效半字节 b4 到 b1 称为 CID, 它定义了已编址的 PICC 的逻辑号。

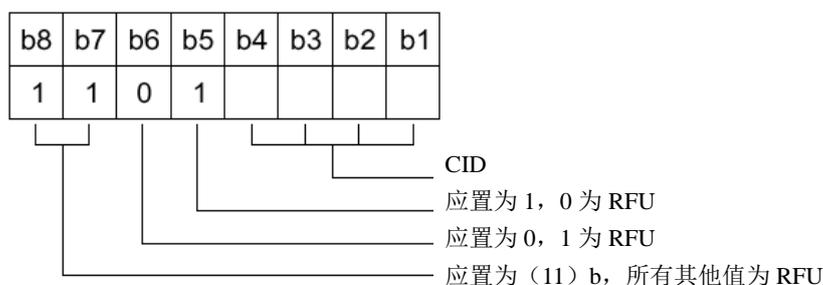


图47 PPSS 的编码

8.1.3.2 参数字节 0

PPS0指示可选字节PPS1的出现 (见图48)。

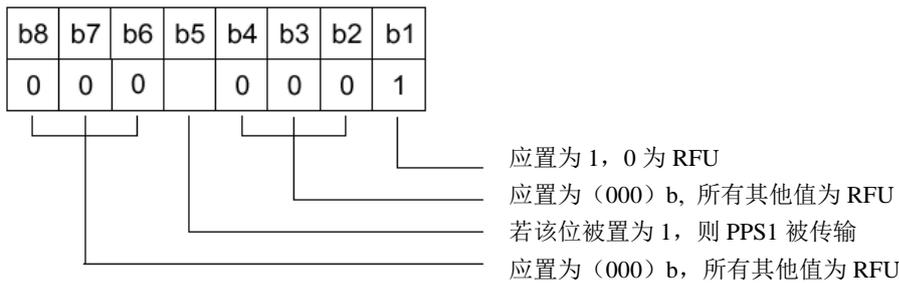


图48 PPS0 的编码

8.1.3.3 参数字节 1

PPS1由三部分组成（见图49）：

- 最高有效半字节 b8 到 b5 为 (0000) b，所有其他值为 RFU；
- 位 b4, b3 称为 DSI，它编码了已选择的从 PICC 到 PCD 的除数整数；
- 位 b2, b1 称为 DRI，它编码了已选择的从 PCD 到 PICC 的除数整数。

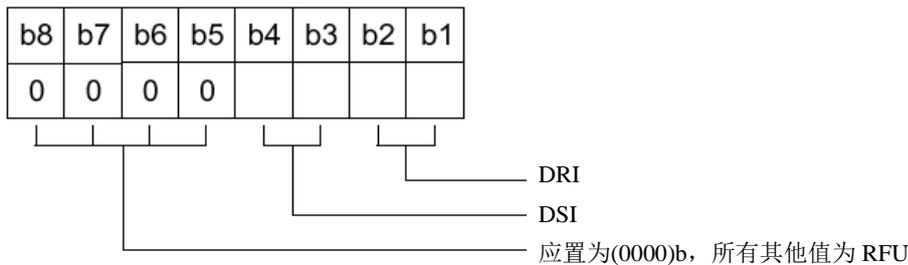


图49 PPS1 的编码

对于可能的DS和DR的定义，见8.1.2.4。

D的编码在表30中给出。

表30 DRI, DSI 到 D 的转换

DRI, DSI	(00) b	(01) b	(10) b	(11) b
D	1	2	4	8

8.1.4 协议和参数选择响应

PPS响应确认接收到的PPS请求（见图50），并仅包开始字节（见8.1.3.1）。

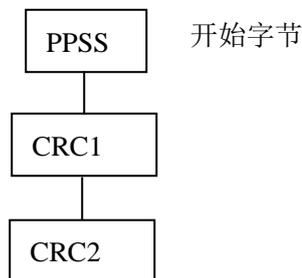


图50 协议和参数选择响应

8.1.5 激活帧等待时间

激活帧等待时间为 PICC 在接收到的来自 PCD 的帧的结尾之后开始发送其响应帧定义了最大时间，其值为 $65536/f_c$ ($\sim 4833\mu s$)。

注：在任何方向上两个帧之间的最小时间在第 7 章中定义。

8.1.6 差错检测和恢复

8.1.6.1 RATS 和 ATS 的处理

8.1.6.1.1 PCD 规则

当PCD发送了RATS并接收到有效ATS，PCD应继续工作。

在任何其他情况下，在它应使用如8.4中定义的停活序列前，PCD可以重新传输RATS。在停活序列失败的情况下，它可以使用第7章中定义的HLTA命令。

8.1.6.1.2 PICC 规则

当PICC被最后一条命令选择，并且收到有效RATS，PICC应：

- 发送回其 ATS；
- 使 RATS 失效（停止响应接收到的 RATS）。

收到除了HALT命令的任何块（有效或无效），PICC应：

- 忽略该块；
- 保持在接收模式。

8.1.6.2 PPS 请求和 PPS 响应的处理

8.1.6.2.1 PCD 规则

当PCD发送了PPS并接收到有效PPS响应，PCD应激活选择的参数并继续工作。

在任何其他情况下，PCD可以重新传输PPS请求并继续工作。

8.1.6.2.2 PICC 规则

当PICC接收到RATS，发送了其ATS，并且：

- a) 接收到有效 PPS 请求，PICC 应：
 - 发送 PPS 响应；
 - 使 PPS 请求失效（停止响应接收到的 PPS 请求）；
 - 激活接收到的参数。
- b) 接收到无效块，PICC 应：
 - 使 PPS 请求失效（停止响应接收到的 PPS 请求）；
 - 保持在接收模式。
- c) 接收到除了 PPS 请求的有效块，PICC 应：
 - 使 PPS 请求失效（停止响应接收到的 PPS 请求）；
 - 继续工作。

8.1.6.3 激活期间 CID 的处理

当PCD发送了包含CID=n不等于0的RATS，并且：

- a) 接收到指示CID被支持的ATS，PCD应：
 - 发送包含CID =n的块给该PICC；
 - 当该PICC处于ACTIVE状态时，对于进一步的RATS，不使用CID=n。
- b) 接收到指示CID不被支持的ATS，PCD应：
 - 发送不包含CID的块给该PICC；
 - 当该PICC处于ACTIVE状态时，不激活任何其他PICC。

当PCD发送了包含CID等于0的RATS，并且：

- a) 接收到指示CID被支持的ATS，PCD应：
 - 发送包含CID等于0的块给该PICC；
 - 当该PICC处于ACTIVE状态时，不激活任何其他PICC。
- b) 接收到指示CID不被支持的ATS，PCD应：
 - 发送不包含CID的块给该PICC；
 - 当该PICC处于ACTIVE状态时，不激活任何其他PICC。

8.2 Type B PICC 的协议激活

Type B PICC 的激活序列在第 7 章中描述。

8.3 半双工块传输协议

半双工块传输协议符合无触点卡环境的特殊需要，并使用第 7 章中定义的帧格式。

帧格式的其他相关元素有：

- 块格式；
- 最大帧等待时间；
- 功率指示；
- 协议操作。

本协议根据 OSI 参考模型的原理压条法设计，需特别注意穿越边界的交互作用的最小限度。四层定义如下：

- 根据第 7 章交换字节的物理层；
- 按本章中定义进行交换块的数据链路层；
- 为使系统开销最小而与数据链路层结合的会话层；
- 处理命令的应用层，它涉及在两个方向上至少一个块或块链的交换。

注：应用选择的使用如 GB/T 16649.5 中所定义。不推荐在多应用的 PICC 中使用隐含的应用选择。

8.3.1 块格式

块格式（见图 51）由一个头域（必备）、一个信息域（可选）和一个尾域（必备）组成。

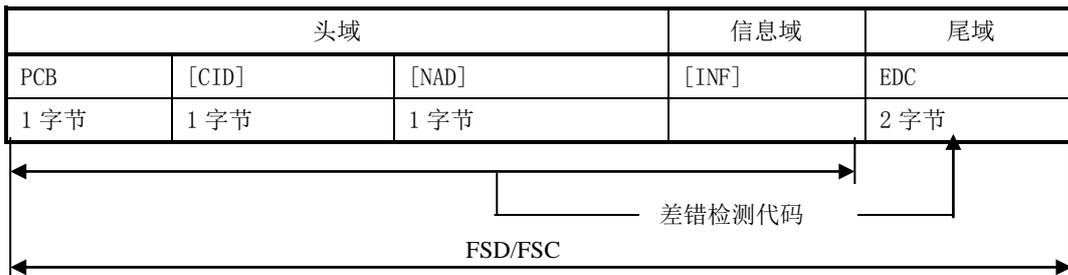


图51 块格式

8.3.1.1 头域

头域是必备的，最多由三个字节构成：

- 协议控制字节（必备）；
- 卡标识符（可选）；
- 结点地址（可选）。

8.3.1.1.1 协议控制字节域

PCB 用于传送控制数据传输所需要的信息。

协议定义了块的三种基本类型：

- 用于为应用层的使用传送信息的信息块（I-块）；
- 用于传送确认或不确认的接收准备块（R-块）。R-块不包含 INF 域。确认涉及最后接收到的块；
- 用于在 PCD 和 PICC 间交换控制信息的管理块（S-块）。两种不同类型的 S-块定义如下：
 - 包含 1 字节长 INF 域的等待时间延迟，和
 - 不包含 INF 域的 DESELECT。

PCB 的编码依赖于它的类型，如图 52 所定义。此处没有定义的 PCB 编码在第 5、6、7 章的其他章节使用或为 RFU。I-块、R-块和 S-块的编码在图 50、图 51、图 52 中给出。

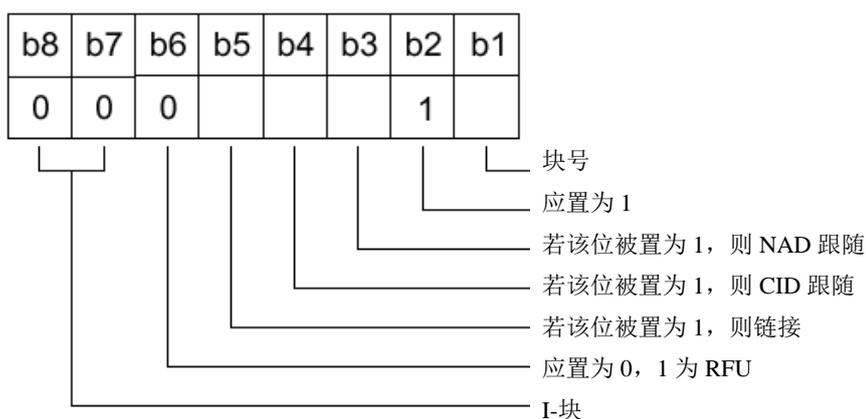


图52 I-块 PCB 的编码

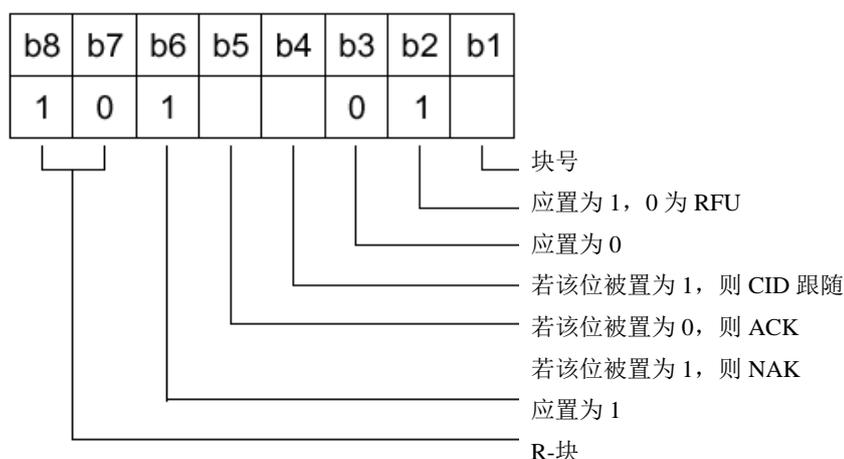


图53 R-块 PCB 的编码

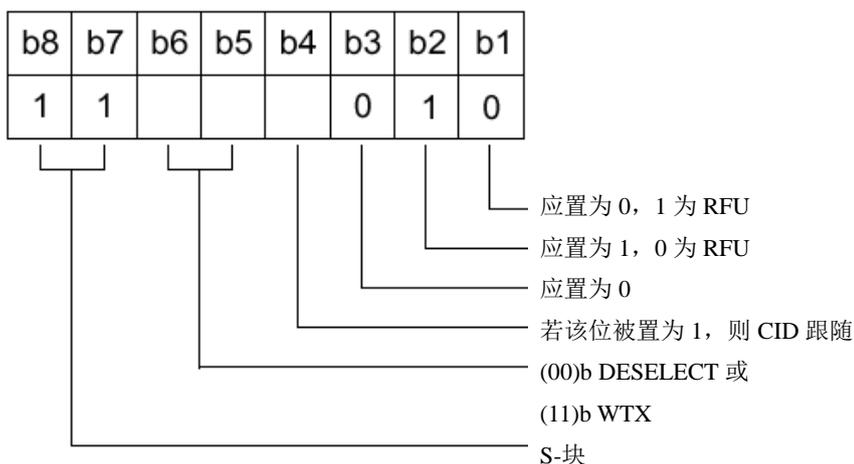


图54 S-块 PCB 的编码

8.3.1.1.2 卡标识符域

CID 域用于识别特定的 PICC, 它由三部分组成 (见图 55):

- 最高有效位 b8, b7 用于从 PICC 到 PCD 的功率水平指示。对于 PCD 到 PICC 的通信, 这两位应被置为 0。功率水平指示的定义见 8.3.4;
- 位 b6 和 b5 用于传送附加信息, 它没有被定义并应置为 (00) b, 所有其他值为 RFU;
- 位 b4 到 b1 编码 CID。

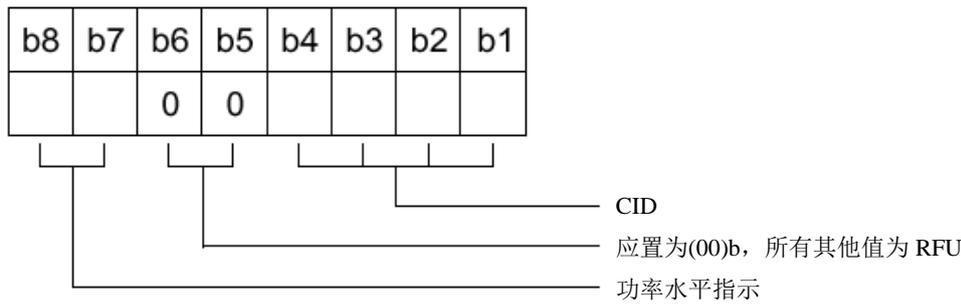


图55 卡标识符的编码

Type A CID 的编码在 8.1.1 中给出, Type B 的在第 7 章中给出。

PICC 对 CID 的处理描述如下:

- 不支持 CID 的 PICC 应忽略任何包含 CID 的块。
- 支持 CID 的 PICC 应:
 - 通过使用其 CID 响应包含其 CID 的块;
 - 忽略包含其他 CID 的块;
 - 假若其 CID 为 0, 亦通过不使用 CID 响应不包含 CID 的块。

8.3.1.1.3 结点地址域

在头域里的 NAD 被保存用于建立和编址不同的逻辑连接。当位 b8 和 b4 被置为 0 时, NAD 的用途应为适应来自 GB/T 16649.3 的定义。所有其他值为 RFU。

下列定义应适用 NAD 的用途:

- NAD 域应仅用于 I-块;
- 当 PCD 使用 NAD 时, PICC 也应使用 NAD;
- 在链接期间, NAD 仅在链的第一个块内传输;
- PCD 应不使用 NAD 编址不同的 PICC (CID 应被用于编址不同的 PICC);
- 当 PCD 不支持 NAD 时, 应忽略任何包含 NAD 的块。

8.3.1.2 信息域 (INF)

INF 于是可选的。当它存在时, INF 域传送 I-块中的应用数据或非应用数据和 S-块中的状态信息。信息域的长度通过计算整个块的字节数减去头域和尾域得出。

8.3.1.3 尾域

该域包含传输块的 EDC。EDC 为第 7 章中定义 CRC。

8.3.2 帧等待时间 (FWT)

FWT 给 PICC 定义了 PCD 帧结束后开始其响应帧的最大时间 (见图 56)。

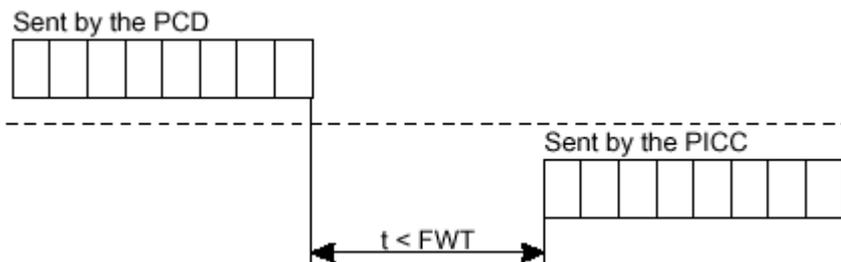


图56 帧等待时间

注: 在任何方向上两个帧之间的最小时间在第 7 章中定义。

FWT 通过下面的公式计算:

$$FWT = (256 \times 16 / f_c) \times 2^{FWI}$$

其中 FWI 的值在 0 到 14 之间, 15 为 RFU。对于 Type A, 若 TB (1) 被省略, 则 FWI 的缺省值为 4,

给出的 FWT 值约为 4.8ms。

对于 FWI=0, $FWT = FWT_{\min}$ ($\sim 302\mu s$)

对于 FWI=14, $FWT = FWT_{\max}$ ($\sim 4949\mu s$)

FWT 应用于检测传输差错或无响应的 PICC。如果来自 PICC 的响应的开始没有在 FWT 内被接收到, 则 PCD 收回发送的权利。

Type B FWI 域的值在 ATQB 中的设置如第 7 章中所定义。Type A FWI 域的值在 ATS 中设置 (见 8.1.2.5)。

8.3.3 帧等待时间扩展

当 PICC 需要比定义的 FWT 更多的时间用于处理接收到的块时, 应使用 S(WTX) 请求等待时间扩展。S(WTX) 请求包含 1 字节长 INF 域, 它由两部分组成 (见图 57):

- 最高有效位 b8, b7 编码功率水平指示 (见 8.3.4);
- 最低有效位 b6 到 b1 编码 WTXM。WTXM 在 1 到 59 范围内编码。值 0 和 60 到 63 为 RFU。

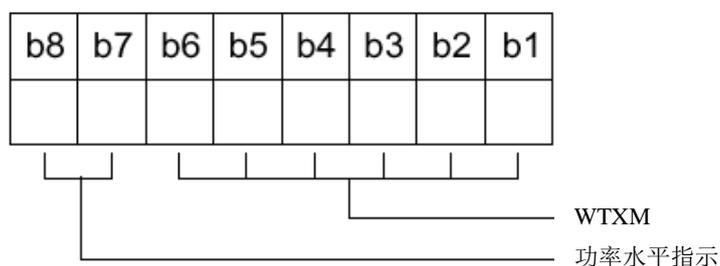


图57 S(WTX) 请求的 INF 域编码

PCD 应通过发送包含 1 字节长 INF 域的 S(WTX) 来确认, 该 INF 域由两部分组成 (见图 58) 并包含了与在请求中接收到的相同的 WTXM:

- 最高有效位 b8, b7 为 (00) b, 所有其他值为 RFU;
- 最低有效位 b6 到 b1 编码了用于定义临时 FWT 的确认的 WTXM 值。

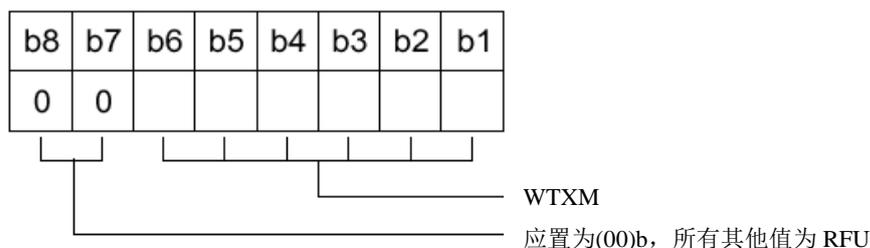


图58 S(WTX) 响应的 INF 域编码

FWT 的响应的临时值通过下面的公式计算:

$$FWT_{\text{TEMP}} = FWT \times WTXM$$

PICC 需要的时间 FWT_{TEMP} 在 PCD 发送了 S(WTX) 响应之后开始。

当公式得出的结果大于 FWT_{\max} 时, 应该使用 FWT_{\max} 。

临时 FWT 仅在下一个块被 PCD 接收到时才应用。

8.3.4 功率水平指示

功率水平指示通过使用插入在 CID (当存在时) 中的两位来编码, 并在 S-块中被 PICC 发送 (见 8.3.1.1.2 和 8.3.3)。

表31 功率水平指示的编码

(00) b	PICC 不支持功率水平指示
(01) b	对于完整功能性, 功率不充分

(10) b	对于完整功能性, 功率充分
(11) b	对于完整功能性, 功率超出

注: 由 PCD 进行的功率水平指示的解释是可选的。

8.3.5 协议操作

在激活序列后, PICC应等待一仅PCD才有权力发送的命令。在发送了块之后, PCD应转换到接收模式并在转换回传输模式之前等待块。PICC可以传输块仅响应接收到的块(对时间延迟是察觉不到的)。在响应后, PICC应返回到接收模式。

在当前命令/响应对没有完成或帧等待时间超出而没有响应时, PCD不应初始化一新的命令/响应对。

8.3.5.1 多激活

多激活特征允许PCD保持几个PICC同时在ACTIVE状态。对于停活PICC和激活另一张PICC, 这允许几个PICC间直接转换而无须另外的时间。

多激活的举例见附录G。

注: 对每个已激活的 PICC, PCD 需要处理分离的块号。

8.3.5.2 链接

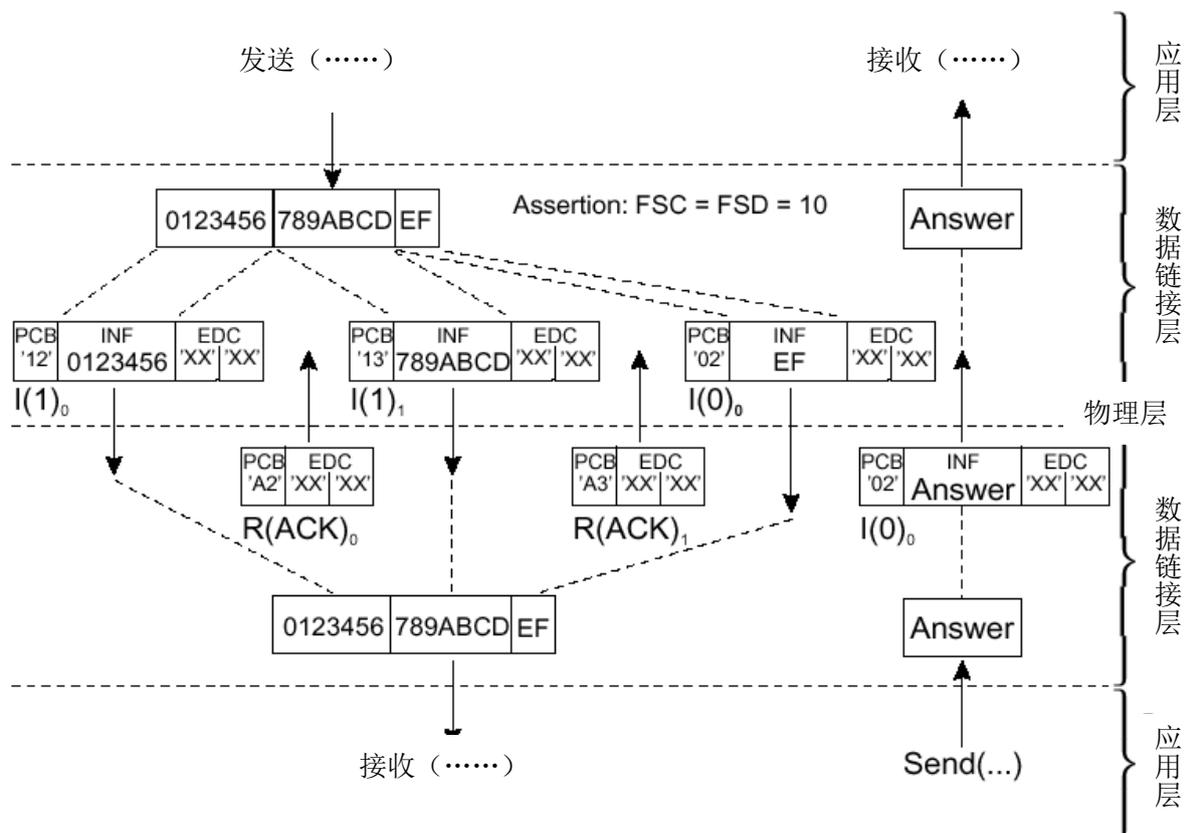
链接过程允许PCD或PICC通过把信息划分成若干块来传输不符合分别由FSC或FSD定义的单块的信息。每一块的长度应分别小于或等于FSC或FSD。

块的链接通过链接I-块中PCB的位(M)来控制。每一个带链接位集的I-块应被R-块确认。

链接的特性在图59中给出, 16字节长字符串分成三块来传输。

记号:

I (1) x	带链接位设置和块号 x 的 I-块
I (0) x	链接位未设置的带块号 x 的 I-块
R (ACK) x	指示确认的 R-块



注: 本例没有使用可选字段 NAD 和 CID。

图59 链接

8.3.5.3 块编号规则

8.3.5.3.1 PCD 规则

规则A: 对每一张激活的PICC, PCD块号应被初始化为0。

规则B: 当带有的块号等于当前块号的I-块或R(ACK)块被接收到时, PCD在可选地发送块前为该PICC锁定当前块号。

8.3.5.3.2 PICC 规则

规则C: 在激活时, PICC块号应被初始化为1。

规则D: 当I-块被接收到(独立于其块号), PICC在发送块前锁定其块号。

规则E: 当带有块号不等于当前PICC的块号的R(ACK)块被接收到时, PICC在发送块前锁定其块号。

8.3.5.4 块处理规则

8.3.5.4.1 一般规则

规则1: 首块应由PCD来发送。

规则2: 当I-块指示链接已被接收到时, 块应由R(ACK)块来确认。

规则3: S-块仅成对使用。S(...)请求块总是跟随着S(...)响应块(见8.3.3和8.4)。

8.3.5.4.2 PCD 规则

规则4: 当接收到无效块或FWT超时, 则R(NAK)块被发送(PCD链接或S(DESELECT)情况除外)。

规则5: 在PICC链接的情况下, 当接收到无效块或FWT超时, R(ACK)块被发送。

规则6: 当接收到R(ACK)块, 如果其块号不等于PICC的当前块号, 则最后的I-块被重新传送。

规则7: 当接收到R(ACK)块, 如果其块号等于PCD的当前块号, 则继续链接。

规则8: 如果S(DESELECT)请求没有被无差错S(DESELECT)响应进行回答, 则S(DESELECT)请求可以被重新传送或PICC可以被忽视。

8.3.5.4.3 PICC 规则

规则9: 允许PICC发送S(WTX)块而不发送I-块或R(ACK)块。

规则10: 当I-块没有指示链接已被接收到时, 块应由I-块来确认。

规则11: 当接收到R(ACK)块或R(NAK)块, 如果其块号等于PICC的当前块号, 则最后的块被重新传送。

规则12: 当接收到R(NAK)块, 如果其块号不等于PICC的当前块号, 则R(ACK)块被发送。

规则13: 当接收到R(ACK)块, 如果其块号不等于PICC的当前块号, 则继续链接。

8.3.5.5 差错检测和恢复

当检测到差错时, 应试图使用下列恢复规则。本章中的定义支配块处理规则(见8.3.5.3)。

下列差错应被PCD检测到:

a) 传输差错(帧差错或EDC差错)或FWT超时

PCD应试图通过以下顺序示出的技术进行差错恢复:

——块的重新传输(可选);

——S(DESELECT)请求的使用;

——忽视PICC。

b) 协议差错(违反了PCB编码或违反了协议规则)

PCD应试图通过以下顺序示出的技术进行差错恢复:

——S(DESELECT)请求的使用;

——忽视PICC。

下列差错应被PICC检测到:

a) 传输差错(帧差错或EDC差错);

b) 协议差错(违反了协议规则)。

PICC应尽量没有差错恢复。当传输差错或协议差错发生时，PICC始终应返回接收模式，在任何时候它都应接收S（DESELECT）请求。

注：R（NAK）块不由PICC发送。

8.4 Type A 和 Type B PICC 的协议停活

PCD和PICC间的交易完成之后，PICC应被置为HALT状态。

PICC的停活通过使用DESELECT命令来完成。

DESELECT命令象协议的S-块那样编码，并由PCD发送的S（DESELECT）请求块和PICC作为确认发送的S（DESELECT）响应组成。

8.4.1 停活帧等待时间

停活帧等待时间给PICC定义了接收到来自PCD的S（DESELECT）请求帧的末端后开始发送其S（DESELECT）响应的最短时间，其值为 $65536/f_c$ （ $\sim 4833\mu s$ ）。

注：在任何方向上帧之间的最短时间在第7章中定义。

8.4.2 差错检测和恢复

当PCD发送了S（DESELECT）请求并接收到了S（DESELECT）响应，则PICC已被成功地置为了HALT状态并且分配给它的CID也被释放。

当PCD没有接收到S（DESELECT）响应，则PCD可以重新进行停活序列。

9 数据元和命令

9.1 命令

9.1.1 C-APDU 格式

C-APDU由4字节长的必备头后跟一个可变长的条件体组成，见图60。

CLA	INS	P1	P2	Lc	Data	Le
←必备头→				←条件体→		

图60 C-APDU 格式

C-APDU中发送的数据字节数用Lc（命令数据域的长度）表示。

R-APDU中期望返回的数据字节数用Le（期望数据长度）表示。当Le存在且值为0时，表示需要最大字节数（256字节）。在命令报文需要时，Le可始终被设为'00'。

C-APDU报文的内容见表32。

表32 C-APDU 的内容

代码	描述	长度
CLA	命令类别	1
INS	指令字节	1
P1	指令参数 1	1
P2	指令参数 2	1
Lc	命令数据域中存在的字节数	0 或 1
Data	命令发送的数据位串（=Lc）	可变
Le	响应数据域中期望的最大数据字节数	0 或 1

9.1.2 R-APDU 格式

R-APDU格式由一个变长的条件体和后随两字节长的必备尾组成，见图61。

Data	SW1	SW2
条件体	←必备尾→	

图61 R-APDU 的结构

R-APDU的内容见表33。

表33 R-APDU 的内容

代码	描述	长度
Data	响应中接收的数据位串 (=Lr)	变长
SW1	命令处理状态	1
SW2	命令处理限定	1

当使用T=1协议时，对于所有Le='00'的命令，状态字SW1 SW2="90 00"或"61 La"均表示命令的成功执行。但由于可读性的需要，这两种应答码只用了"90 00"作为参考。

本条描述以下的C/R-APDU：

- 关闭非接触通道；
- 激活非接触通道。

9.2 关闭非接触通道命令

9.2.1 定义和范围

此命令的目的是将卡片的非接触方式暂时关闭。此时，卡片如果有接触接口，则接触接口的操作应该不受任何影响。当卡片的非接触通道被关闭以后，除了激活非接触通道指令和取随机数指令，其它任何指令以非接触方式送入卡片后，卡片都响应6D00。

此命令使用应用维护密钥保护。

9.2.2 命令报文

关闭非接触通道命令报文编码见表34。

表34 关闭非接触通道命令报文

代码	值
CLA	'84'
INS	'70'
P1	'80'
P2	'04'
Lc	'04'
Data	报文鉴别码 (MAC) 数据元；根据附录 I 中的规定编码
Le	不存在

9.2.3 命令报文数据域

命令报文数据域包括根据附录I中的规定进行编码的报文鉴别码 (MAC) 数据元。

9.2.4 响应报文数据域

响应报文数据域不存在。

9.2.5 响应报文状态字

此命令执行成功的状态字是“9000”。

IC卡可能回送的警告状态字如表35所示。

表35 关闭非接触通道警告状态

SW1	SW2	含义
62	00	无信息提供
62	81	写 EEPROM 错误

IC卡可能回送的错误状态字如表36所示。

表36 关闭非接触通道错误状态

SW1	SW2	含义
-----	-----	----

64	00	状态标志未变
65	81	内存失败
69	82	不满足安全状态
69	87	安全报文数据项丢失
69	88	安全报文数据项不正确
6A	88	P1, P2 不正确
6A	81	卡片锁定

9.3 激活非接触通道命令

9.3.1 定义和范围

此指令的目的是将关闭的非接触方式激活。此指令允许以接触和非接触两种方式发到卡片中。当卡片收到此指令，并且卡片的当前状态符合执行此指令的安全要求，卡片将激活非接触通道。

此命令使用应用维护密钥保护。

9.3.2 命令报文

激活非接触通道命令报文编码见表37。

表37 激活非接触通道命令报文

代码	值
CLA	'84'
INS	'70'
P1	'00'
P2	'04'
Lc	'04'
Data	报文鉴别码 (MAC) 数据元; 根据附录 I 中的规定编码
Le	不存在

9.3.3 命令报文数据域

命令报文数据域包括根据附录I中的规定进行编码的报文鉴别码 (MAC) 数据元。

9.3.4 响应报文数据域

响应报文数据域不存在。

9.3.5 响应报文状态字

此命令执行成功的状态字是“9000”。

在非接触通道工作正常的情况下，卡片收到此指令，卡片返回9000。

IC卡可能回送的错误状态字如表38所示。

表38 激活非接触通道错误状态

SW1	SW2	含义
64	00	状态标志未变
65	81	内存失败
69	82	不满足安全状态
69	87	安全报文数据项丢失
69	88	安全报文数据项不正确
6A	88	P1、P2 不正确
6A	81	卡锁定

附 录 A
(资料性附录)
标准兼容性和表面质量

A.1 标准兼容性

本部分并不排斥把其它现有标准附加到PICC，一些限制可以适用于PICC的凸印。

A.2 印刷的表面质量

在制造过程通过附加印刷之后，要求按规格定制PICC，应注意确保用于印刷的区域具有适合于印刷技术或所使用印刷机的足够质量。

附录 B
 (资料性附录)
 Type A 的通信举例

本例示出了在下列假设基础上该场内两个PICC的选择序列：
 ——PICC#1 带有 UID 长度：单个，uid₀的值为 '10'；
 ——PICC#2 带有 UID 长度：两个。

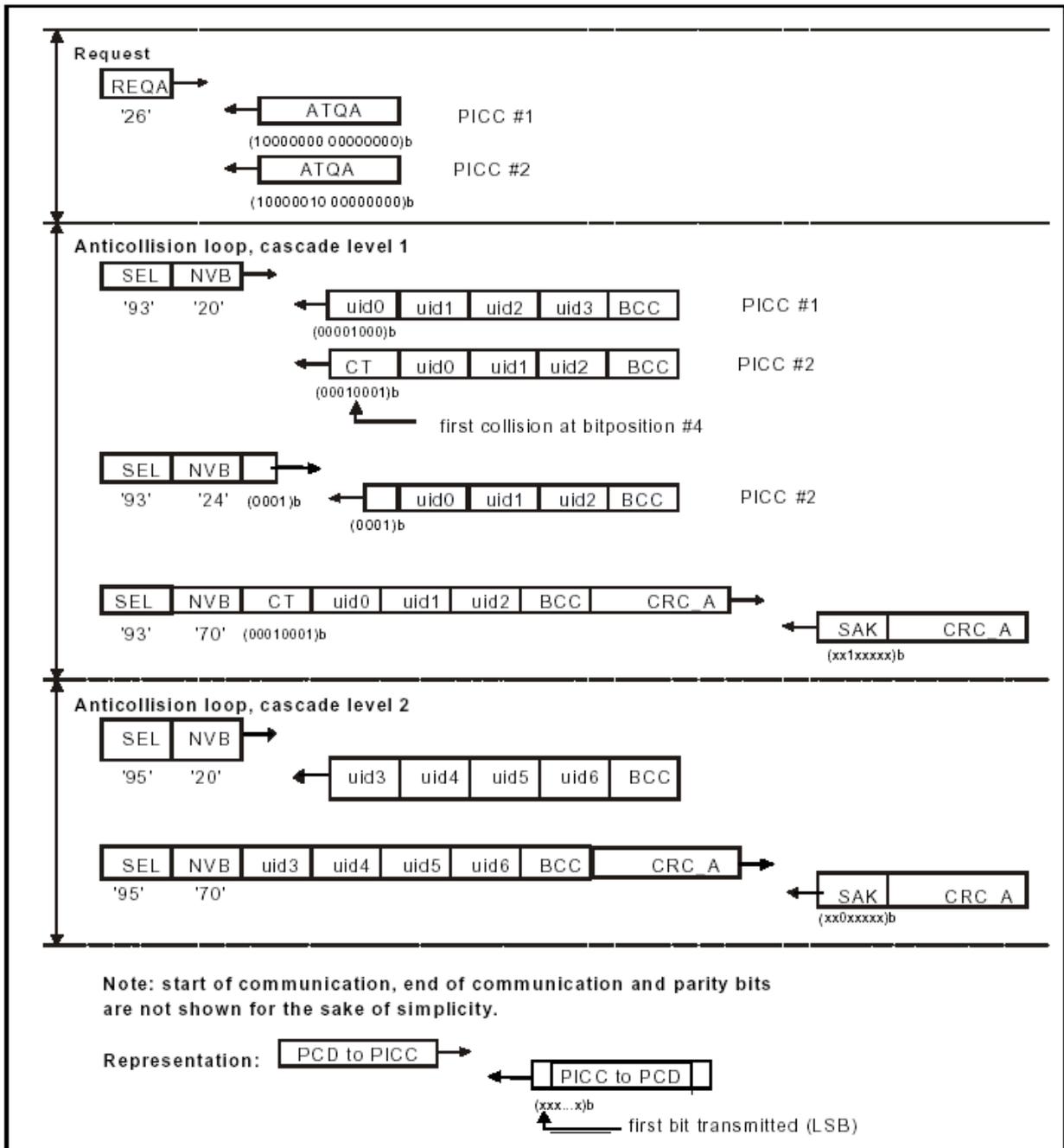


图 B.1 位帧防冲突的选择序列

位帧防冲突的选择序列说明见表B.1。

表 B.1 位帧防冲突的选择序列说明

请求	<p>PCD 发送 REQUEST 命令</p> <p>所有的 PICC 以它们的 ATQA 进行响应:</p> <p>PICC#1 指示位帧防冲突, UID 长度: 单个</p> <p>PICC#2 指示位帧防冲突, UID 长度: 两个</p>
防冲突循环	<p>PCD 发送 ANTICOLLISION 命令:</p>
串联级别 1	<p>SEL 规定了位帧防冲突和串联级别 1</p> <p>NVB 的值 '20' 规定 PCD 不会发送 UID CL1</p> <p>因此, 场内所有的 PICC 都会以它们的 UID CL1 进行响应</p> <p>由于串联标记的值 '88' 引起第一次冲突发生在比特位置# 4</p> <p>PCD 发送另一个包括 UID CL1 的前三位的 ANTICOLLISION 命令, 该 UID CL1 是冲突发生前收到的, UID CL1 后面紧跟一个 (1) b。</p> <p>从而, PCD 将值 '24' 赋给 NVB</p> <p>这 4 位对应于 PICC#2 的 UID CL1 的前 4 位</p> <p>PICC#2 以它的 UID CL1 的其余 36 位进行响应。由于 PICC#1 不响应, 因此没有冲突发生</p> <p>由于 PCD “知道” PICC#2 的 UID CL1 的所有位, 因此它对 PICC#2 发送 SELECT 命令</p> <p>PICC#2 以 SAK 进行响应, 指出 UID 是不完整的</p> <p>因此, PCD 增加串联级别</p>
防冲突循环	<p>PCD 发送另一个 ANTICOLLISION 命令:</p>
串联级别 2	<p>SEL 规定了位帧防冲突和串联级别 2</p> <p>NVB 复位到 '20' 以迫使 PICC#2 以它的完整的 UID 进行响应</p> <p>PICC#2 以它的 UID CL2 的全部 40 位进行响应</p> <p>PCD 对串联级别 2 的 PICC#2 发送 SELECT 命令,</p> <p>PICC#2 以 SAK 进行响应, 指出 UID 是完整的, 并且从 READY 状态转换到 ACTIVE 状态</p>

附 录 C
(规范性附录)
CRC_A 和 CRC_B 的编码

C.1 CRC_A编码

本附录用于解释说明，同时表示了存在于物理层的位模式。之所以包括本附录，是为了检验第7章中Type A的CRC_A编码的实现情况。

编码和解码的过程可由带有合适的反馈门的16级循环移位寄存器方便地完成。根据ITU-T的建议，附件1、图I-1/V.41和图I-2/V.41，寄存器的触发器应编号为FF0至FF15。FF0是最左边的触发器，数据从FF0移入。FF15是最右边的触发器，数据从FF15移出。

表C.1定义了寄存器的初始内容。

表 C.1 初始值为“6363”的16位移位寄存器的初始内容

FF0	FF1	FF2	FF3	FF4	FF5	FF6	FF7	FF8	FF9	FF10	FF11	FF12	FF13	FF14	FF15
0	1	1	0	0	0	1	1	0	1	1	0	0	0	1	1

因此，FF0对应于最高有效位，FF15对应于最低有效位。

C.2 通过标准帧发送的位模式举例

例1：数据的传输，第1个字节=‘00’，第2个字节=‘00’，附加的CRC_A，如图C.1所示。计算出的CRC_A=“1EA0”，16位移位寄存器的内容如表C.2所示。

第1个发送的位

S	0000 0000	1	0000 0000	1	0000 0101	1	01111 1000	1	E
	‘00’	P	‘00’	P	‘A0’	P	‘1E’	P	

图 C.1 CRC_A 编码举例 1

表 C.2 值为“1EA0”的16位移位寄存器的内容

FF0	FF1	FF2	FF3	FF4	FF5	FF6	FF7	FF8	FF9	FF10	FF11	FF12	FF13	FF14	FF15
0	0	0	1	1	1	1	0	1	0	1	0	0	0	0	0

例2：数据块的传输，第1个字节=‘12’，第2个字节=‘34’，附加的CRC_A，如图C.2所示。计算出的CRC_A=“CF26”，16位移位寄存器的内容如表C.3所示。

第1个发送的位

S	0100 1000	1	0010 1100	0	0110 0100	0	11111 0011	1	E
	‘12’	P	‘34’	P	‘26’	P	‘CF’	P	

图 C.2 CRC_A 编码举例 2

表 C.3 值为“CF26”的16位移位寄存器的内容

FF0	FF1	FF2	FF3	FF4	FF5	FF6	FF7	FF8	FF9	FF10	FF11	FF12	FF13	FF14	FF15
1	1	0	0	1	1	1	1	0	0	1	0	0	1	1	0

C.3 CRC_B编码

本附录用于解释说明，同时表示了存在于物理层的位模式。之所以包括本附录，是为了检验第7章中Type B的CRC_B编码的实现情况。更详细的内容参考GB/T 7496、CCITT X.25和V.42#8.1.1.6.1。

初始值=“FFFF”。

C.4 通过标准帧传送的位模式实例

例 1: 数据的传输, 第 1 个数据字节= ‘00’, 第 2 个数据字节= ‘00’, 第 3 个数据字节= ‘00’, 附加的 CRC_B, 如图 C.3 所示。。

计算出的CRC_B= “C6CC”

		第 1 个数据字节	第 2 个数据字节	第 3 个数据字节	CRC_B		
帧=	SOF	‘00’	‘00’	‘00’	‘CC’	‘C6’	EOF

图 C.3 CRC_B 编码举例 1

例 2: 数据的传输, 第 1 个数据字节= ‘0F’, 第 2 个数据字节= ‘AA’, 第 3 个数据字节= ‘FF’, 附加的 CRC_B, 如图 C.4 所示。。

计算出的CRC_B= “D1FC”

		第 1 个数据字节	第 2 个数据字节	第 3 个数据字节	CRC_B		
帧=	SOF	‘0F’	‘AA’	‘FF’	‘FC’	‘D1’	EOF

图 C.4 CRC_B 编码举例 2

例 3: 数据的传输, 第 1 个数据字节= ‘0A’, 第 2 个数据字节= ‘12’, 第 3 个数据字节= ‘34’, 第 4 个数据字节= ‘56’, 附加的 CRC_B, 如图 C.5 所示。。

计算出的CRC_B= “F62C”

		第 1 个数据字节	第 2 个数据字节	第 3 个数据字节	第 4 个数据字节	CRC_B		
帧=	SOF	‘0A’	‘12’	‘34’	‘56’	‘2C’	‘F6’	EOF

图 C.5 CRC_B 编码举例 3

C.5 用C语言写的CRC计算的代码例子

```
#include <stdio.h>
#include <stdlib.h>
#include <string.h>
#include <ctype.h>

#define CRC_A 1
#define CRC_B 2
#define BYTE unsigned char

unsigned short UpdateCrc(unsigned char ch, unsigned short *lpwCrc)
{
    ch = (ch^(unsigned char)((*lpwCrc) & 0x00FF));
    ch = (ch^(ch<<4));

    *lpwCrc = (*lpwCrc >> 8)^(unsigned short)ch << 8)^(unsigned short)ch<<3)^(unsigned short)ch>>4);
    return(*lpwCrc);
}

void ComputeCrc(int CRCType, char *Data, int Length,
BYTE *TransmitFirst, BYTE *TransmitSecond)
```

```

{
unsigned char chBlock;
unsigned short wCrc;

switch(CRCType) {
case CRC_A:
wCrc = 0x6363; // ITU-V.41
break;
case CRC_B:
wCrc = 0xFFFF; // GB/T 7496
break;
default:
return;
}
do {
chBlock = *Data++;
UpdateCrc(chBlock, &wCrc);
} while (--Length);
if (CRCType == CRC_B)
wCrc = ~wCrc; // GB/T 7496
*TransmitFirst = (BYTE) (wCrc & 0xFF);
*TransmitSecond = (BYTE) ((wCrc >> 8) & 0xFF);

return;
}

BYTE BuffCRC_A[10] = {0x12, 0x34};
BYTE BuffCRC_B[10] = {0x0A, 0x12, 0x34, 0x56};
unsigned short Crc;
BYTE First, Second;
FILE *OutFd;
int i;

int main(void)
{
printf("CRC-16 reference results 3-Jun-1999\n");

printf("by Mickey Cohen - mickey@softchip.com\n\n");
printf("Crc-16 G(x) = x^16 + x^12 + x^5 + 1\n\n");

printf("CRC_A of [ ");
for(i=0; i<2; i++) printf("%02X ", BuffCRC_A[i]);
ComputeCrc(CRC_A, BuffCRC_A, 2, &First, &Second);
printf("] Transmitted: %02X then %02X.\n", First, Second);

```

```
printf("CRC_B of [ ");  
for(i=0; i<4; i++) printf("%02X ", BuffCRC_B[i]);  
ComputeCrc(CRC_B, BuffCRC_B, 4, &First, &Second);  
printf("] Transmitted: %02X then %02X.\n", First, Second);  
  
return(0);  
}
```

附录 D
(资料性附录)

Type A 时间槽——初始化和防冲突

本附录描述了应用于Type A PICC的时间槽检测协议。不要求支持Type A和Type B的轮询的PCD支持该检测协议以作为强制性防冲突协议，见6.4条。

D.1 术语和缩略语

ATQA_t	对Type A时间槽请求的应答
ATQ-ID	对REQ-ID的应答
CID_t	Type A时间槽的卡标识符
HALT_t	Type A时间槽的HALT命令
REQA_t	Type A时间槽的REQuest命令
REQ-ID	REQuest-ID命令
SAK_t	Type A时间槽的选择确认
SEL_t	Type A时间槽的SElect命令

D.2 位、字节和帧格式

D.2.1 时序定义

轮询复位时间

Type A时间槽轮询复位时间等于Type A轮询复位时间。

从 REQA_t 到 ATQA_t 的时间间隔

一旦收到REQA_t，等待 32 ± 2 etu后，PICC返回ATQA_t。PCD可能识别不出ATQA_t的编码。

请求保护时间

请求保护时间定义为两个连续请求命令的起始位之间的最短时间，其值应为0.5ms。

帧保护时间

帧保护时间定义为在相反方向上两个连续帧的最后一位的上升沿和起始位的下降沿之间的最短时间。其值应为10etu。

时间槽长度

第一个时间槽开始于REQ-ID后的32etu内。每个时间槽长度为104etu，包括94etu的ATQ-ID接收和其后的10etu的帧保护时间。

D.2.2 帧格式

REQA_t 帧

见7.1.2.6和表4。REQA_t的数据内容为‘35’。

标准帧

如图D.1所示，每个数据字节的LSB首先被发送。每个数据字节没有奇偶校验位。CRC_B在7.2中定义。

S	数据：n*（8 数据位+没有奇偶校验位）				CRC_B 2 字节	E
	1 字节 命令或响应	（0 或 1 字节） （参数 1）	（0 或 1 字节） （参数 2）	（0 或 8 字节） （UID）		

图 D.1 CRC_B 编码举例 3

D.3 PICC状态

下面条款提供了Type A_时间槽PICC的状态。

POWER-OFF 状态

在POWER-OFF状态下，由于缺少载波，PICC不被激活并且不发副载波。

IDLE 状态

该状态在场被激活5ms延迟后进入。

READY 状态

该状态通过REQA_t进入。

ACTIVE 状态

该状态通过带有完整UID和CID_t的SEL_t进入。PCD从PICC获得SAK_t信息。

HALT 状态

这一状态通过HALT_t从ACTIVE状态进入。在这一状态下，PICC是静默的。

D.4 命令/响应集合

用到了4对命令和响应的集，见表D.1。

表 D.1 命令/响应集合

类型	名称	编码 (b8-b1)	含义
命令	REQA_t	(b7-b1) (0110101) b (= '35')	请求 PICC Type A 时间槽来应答 ATQA_t。REQA_t 伴随着两个参数。
响应	ATQA_t	'00' 到 'FF' 的任何一个字节内容	对 REQA_t 的应答。PCD 能识别出 Type A 时间槽 PICC 的存在。然而，不要求 PCD 识别出 ATQA_t 的编码。
命令	REQ-ID	(00001000) b (= '08')	请求 PICC 向若干时间槽中的某一个应答它的 UID。
响应	ATQ-ID	(00000110) b (= '06')	向 4 个时间槽中的某一个应答 8 字节 UID。ATQ-ID 伴随着 8 字节 UID。
命令	SEL_t	(01000NNN) b, (NNN=CID_t No. (0-7)) (01100NNN) b, (NNN+8=CID_t No. (8-15))	选择带有其 UID 的 PICC 并设置 CID_t。SEL_t 伴随着 8 字节 UID。
响应	SAK_t	(1000XXX) b (= '8X', 除非另有规定, 否则 'X' = '0')	确认 SEL_t
命令	HALT_t	(00011NNN) b, (NNN=CID_t No. (0-7)) (00111NNN) b, (NNN+8=CID_t No. (8-15))	暂停带有其 CID_t 的 PICC 并释放其 CID_t。
响应	对 HALT_t 的响应	(00000110) b (= '06')	确认 HALT_t

REQ_ID 命令的参数见表 D.2。

表 D.2 REQ_ID 命令的参数

参数	含义	
P1	b8-b7	时间槽长度, b7=1: 对于 8 字节 UID, b8=0
	b6-b1	时间槽的数目, b3=1: 对于 4 个时间槽, 其他的=0
P2	'00'	

D.5 时间槽防冲突序列

序列流程图由图D. 2示出。

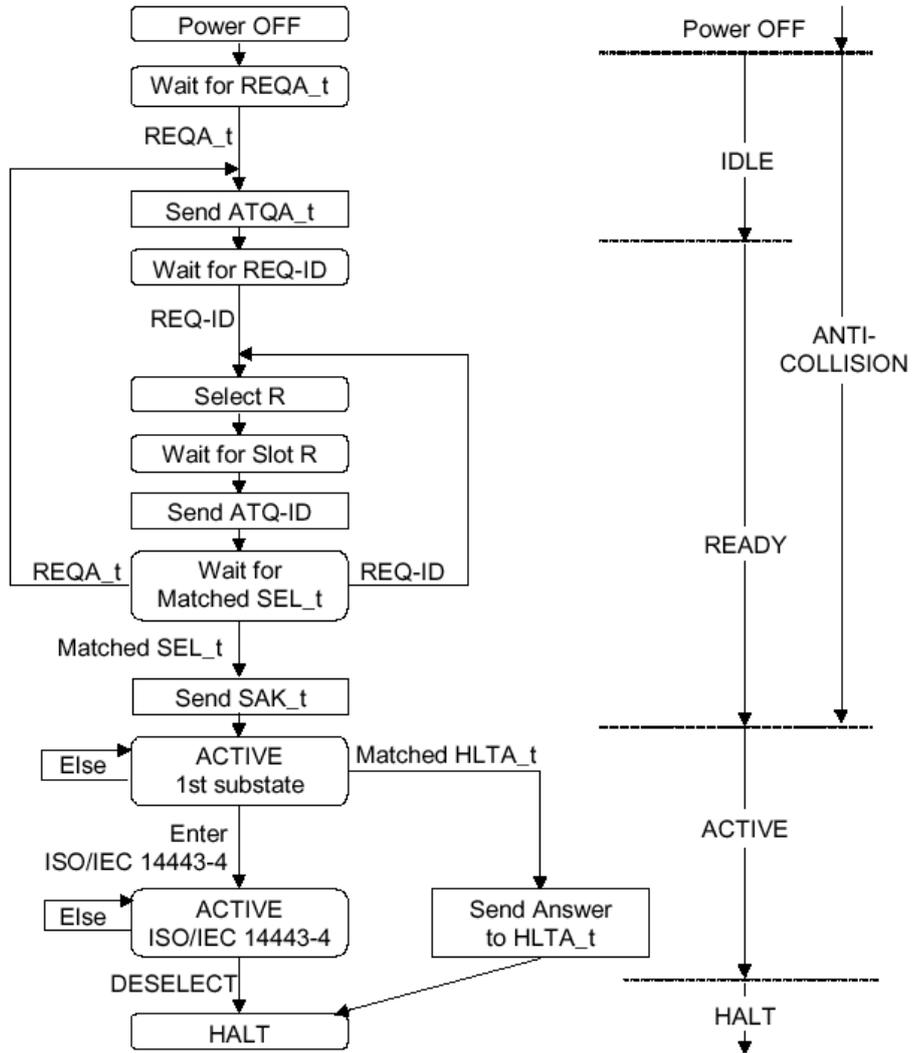
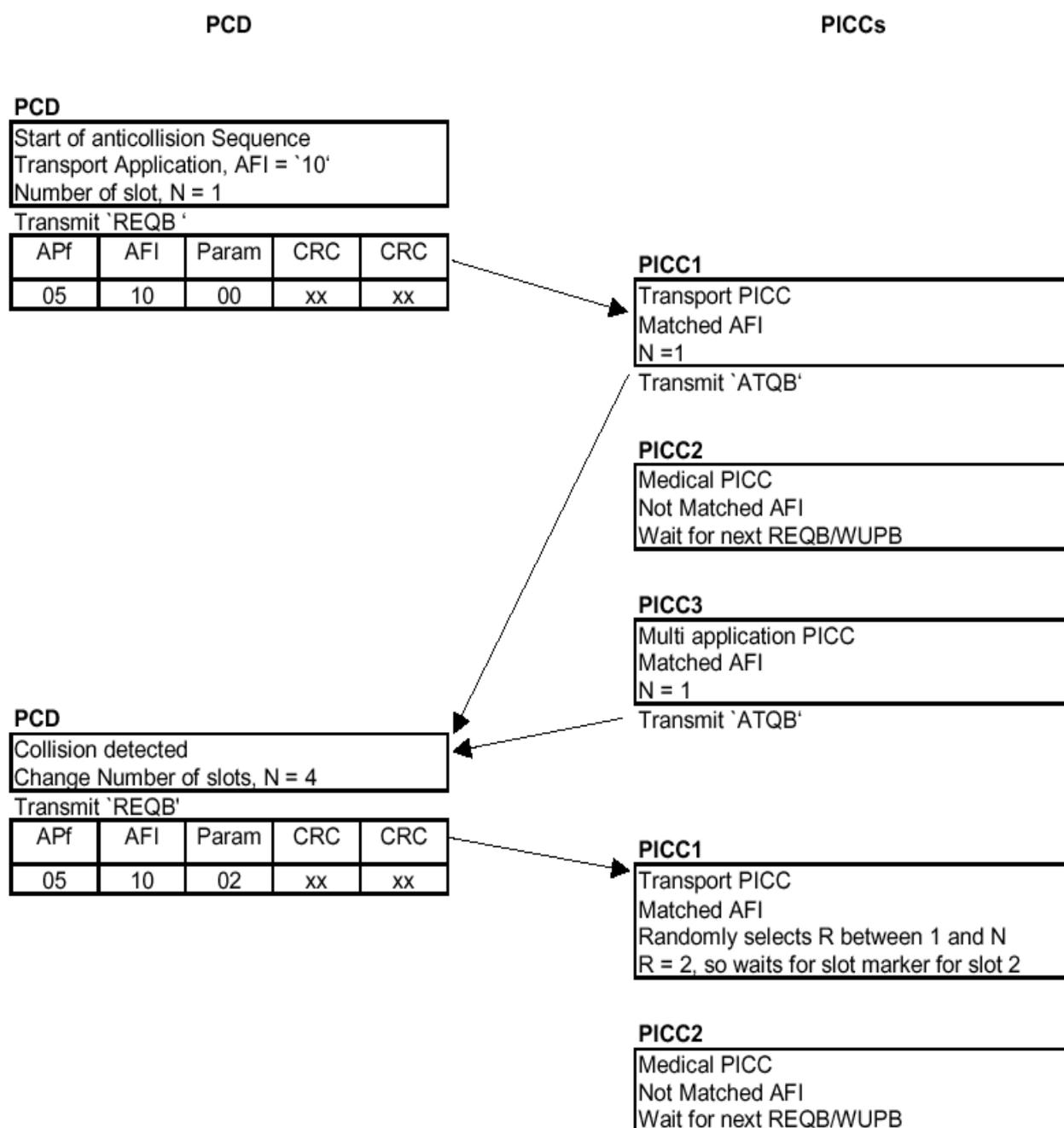


图 D. 2 时间槽-Type A 防冲突流程图

附 录 E
(资料性附录)
Type B——防冲突序列举例

Type B防冲突是命令的变形集，以使应用可以改进防冲突策略。

Type B 防冲突序列举例见图 E. 1。



续下页

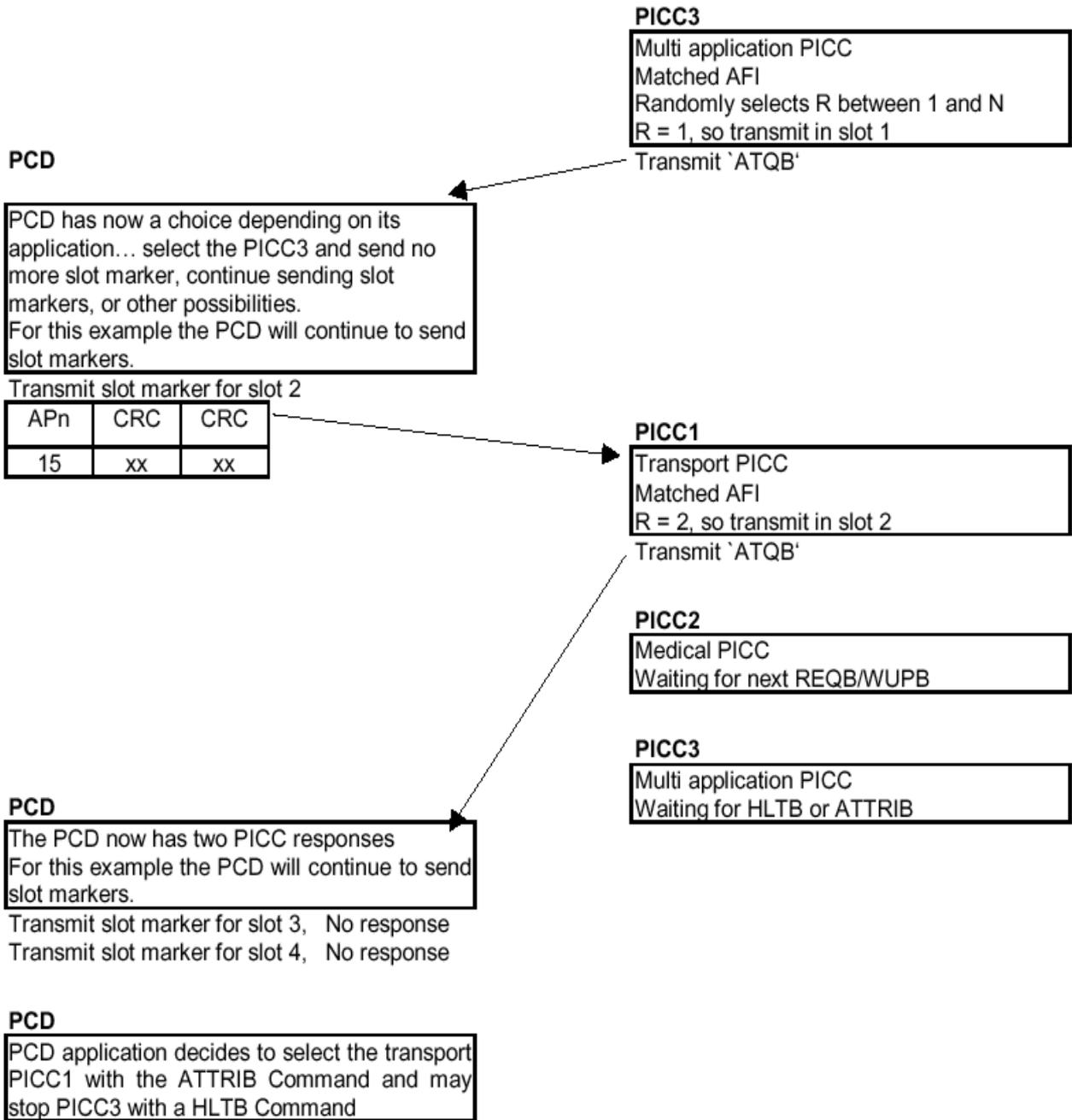


图 E.1 Type B 防冲突序列举例 1

附 录 F
(资料性附录)
使用多激活的举例

表F.1描述了对三张PICC使用多激活的例子。

表 F.1 多激活

PCD 动作	PICC1 状态	PICC2 状态	PICC3 状态
给场提供功率			
三张 PICC 进入该场	IDLE	IDLE	IDLE
激活带 CID=1 的 PICC	ACTIVE (1)	IDLE	IDLE
带 CID=1 的任何数据传输	ACTIVE (1)	IDLE	IDLE
.....			
激活带 CID=2 的 PICC	ACTIVE (1)	ACTIVE (2)	IDLE
带 CID=1, 2 的任何数据传输	ACTIVE (1)	ACTIVE (2)	IDLE
.....			
激活带 CID=3 的 PICC	ACTIVE (1)	ACTIVE (2)	ACTIVE (3)
带 CID=1, 2, 3 的任何数据传输	ACTIVE (1)	ACTIVE (2)	ACTIVE (3)
.....			
带 CID=3 的 S (DESELECT) 命令	ACTIVE (1)	ACTIVE (2)	HALT
带 CID=2 的 S (DESELECT) 命令	ACTIVE (1)	HALT	HALT
带 CID=1 的 S (DESELECT) 命令	HALT	HALT	HALT
.....			

附 录 G
(资料性附录)
协议说明书

本附录给出了一些无差错操作和差错处理的设定。

G.1 记法

任何块	===>	正确接收到
任何块	=≠=>	错误接收到
任何块	= =>	没有接收到 (FWT超时)
分界线	——	最小协议操作的结束
I(1) _x		带链接位设置和块号x的I-块
I(0) _x		链接位未设置的带块号x的I-块
R(ACK) _x		指示确认的R-块
R(NAK) _x		指示不确认的R-块
S(...)		S-块

对目标PICC, 设定中的块编号都以PCD的当前块号开始。为便于表述, PICC激活序列后设定才开始, 因此当前块号对PCD来说以0开始, 对PICC来说以1开始。

G.2 无差错操作

G.2.1 块的交换

设定1 I-块交换, 见表G.1。

表G.1 无差错操作的块交换

注释	块号 (0)	PCD		PICC	块号 (1)	注释
1. 规则 1		I (0) 0	===>		0	规则 D
2. 规则 B	1		<===	I (0) 0		规则 10
3.		I (0) 1	===>		1	规则 D
4. 规则 B	0		<===	I (0) 1		规则 10

G.2.2 等待时间扩展请求

设定2 等待时间扩展, 见表G.2。

表G.2 无差错操作的等待时间扩展

注释	块号 (0)	PCD		PICC	块号 (1)	注释
1. 规则 1		I (0) 0	===>		0	规则 D
2.			<===	S (WTX) 请求		规则 9
3. 规则 3		S (WTX) 响应	===>			
4. 规则 B	1		<===	I (0) 0		规则 10
5.		I (0) 1	===>		1	规则 D
6. 规则 B	0		<===	I (0) 1		规则 10

G.2.3 DESELECT

设定3 DESELECT, 见表G.3。

表G.3 无差错操作的DESELECT

注释	块号 (0)	PCD		PICC	块号 (1)	注释
----	--------	-----	--	------	--------	----

1. 规则 1		I (0) 0	====>		0	规则 D
2. 规则 B	1		<====	I (0) 0		规则 10
3.		S (DESELECT) 请求	====>			
4.			<====	S (DESELECT) 响应		规则 3

G. 2.4 链接

设定4 PCD使用链接, 见表G. 4。

表G. 4 无差错操作的PCD使用链接

注释	块号 (0)	PCD		PICC	块号 (1)	注释
1. 规则 1		I (1) 0	====>		0	规则 D
2. 规则 B	1	I (0) 1	<====	R (ACK) 0		规则 2
3. 规则 7			====>		1	规则 D
4. 规则 B	0		<====	I (0) 1		规则 10
5.		I (0) 0	====>		0	规则 D
6. 规则 B	1		<====	I (0) 0		规则 10

设定5 PICC使用链接, 见表G. 5。

表G. 5 无差错操作的PICC使用链接

注释	块号 (0)	PCD		PICC	块号 (1)	注释
1. 规则 1		I (0) 0	====>		0	规则 D
2. 规则 B	1		<====	I (1) 0		规则 10
3. 规则 2		R (ACK) 1	====>		1	规则 E
4. 规则 B	0		<====	I (0) 1		规则 13
5.		I (0) 0	====>		0	规则 D
6. 规则 B	1		<====	I (0) 0		规则 10

G. 3 差错处理

G. 3.1 块的交换

设定6 协议开始, 见表G. 6。

表G. 6 差错处理的协议开始

注释	块号 (0)	PCD		PICC	块号 (1)	注释
1. 规则 1		I (0) 0	====>		0	
2. 超时			<==	-		
3. 规则 4		R (NAK) 0	====>			
4.	无变化		<====	R (ACK) 1		规则 12
5. 规则 6		I (0) 0	====>		0	规则 D
6. 规则 B	1		<====	I (0) 0		规则 10
7.		I (0) 1	====>		1	规则 D
8. 规则 B	0		<====	I (0) 1		规则 10

设定7 I-块交换, 见表G. 7。

表G. 7 差错处理的块交换

注释	块号 (0)	PCD		PICC	块号 (1)	注释
----	--------	-----	--	------	--------	----

1. 规则 1		I (0) 0	====>		0	规则 D
2. 规则 B	1		<===>	I (0) 0		规则 10
3.		I (0) 1	==>			
4. 超时			<==>	-		
5. 规则 4		R (NAK) 1	====>			
6.	无变化		<===>	R (ACK) 0		规则 12
7. 规则 6		I (0) 1	====>		1	规则 D
8. 规则 B	0		<===>	I (0) 1		规则 10
9.		I (0) 0	====>		0	规则 D
10. 规则 B	1		<===>	I (0) 0		规则 10

设定8 I-块交换, 见表G.8。

表G.8 差错处理的块交换

注释	块号 (0)	PCD		PICC	块号 (1)	注释
1. 规则 1		I (0) 0	====>		0	规则 D
2.			<==>	I (0) 0		规则 10
3. 规则 4		R (NAK) 0	====>			
4. 规则 B	1		<===>	I (0) 0-		规则 11
5.		I (0) 1	====>		1	规则 D
6. 规则 B	0		<===>	I (0) 1		规则 10

设定9 I-块交换, 见表G.9。

表G.9 差错处理的块交换

注释	块号 (0)	PCD		PICC	块号 (1)	注释
1. 规则 1		I (0) 0	====>		0	规则 D
2.			<==>	I (0) 0		规则 10
3. 规则 4		R (NAK) 0	==>			
4. 超时			<==>	-		
5. 规则 4		R (NAK) 0	====>			
6. 规则 B	1		<===>	I (0) 0		规则 11
7.		I (0) 1	====>		1	规则 D
8. 规则 B	0		<===>	I (0) 1		规则 10

G.3.2 等待时间扩展请求

设定10 等待时间扩展请求, 见表G.10。

表G.10 差错处理的等待时间扩展请求

注释	块号 (0)	PCD		PICC	块号 (1)	注释
1. 规则 1		I (0) 0	====>		0	规则 D
2.			<==>	S (WTX) 请求		规则 9
3. 规则 4		R (NAK) 0	====>			
4.			<===>	S (WTX) 请求		规则 11
5. 规则 3		S (WTX) 响应	====>			
6. 规则 B	1		<===>	I (0) 0		规则 10
7.		I (0) 1	====>		1	规则 D
8. 规则 B	0		<===>	I (0) 1		规则 10

设定11 等待时间扩展请求，见表G. 11。

表G. 11 差错处理的等待时间扩展请求

注释	块号 (0)	PCD		PICC	块号 (1)	注释
1. 规则 1		I (0) 0	====>		0	规则 D
2.			<===>	S (WTX) 请求		规则 9
3. 规则 4		R (NAK) 0	===>			
4. 超时			<= =	-		
5. 规则 4		R (NAK) 0	====>			
6.			<====	S (WTX) 请求		规则 11
7. 规则 3		S (WTX) 响应	====>			
8. 规则 B	1		<====	I (0) 0		规则 10
9.		I (0) 1	====>		1	规则 D
10. 规则 B	0		<====	I (0) 1		规则 10

设定12 等待时间扩展请求，见表G. 12。

表G. 12 差错处理的等待时间扩展请求

注释	块号 (0)	PCD		PICC	块号 (1)	注释
1. 规则 1		I (0) 0	====>		0	规则 D
2.			<====	S (WTX) 请求		规则 9
3. 规则 3		S (WTX) 响应	===>			
4. 超时			<= =	-		
5. 规则 4		R (NAK) 0	====>			
6.			<====	S (WTX) 请求		规则 11
7. 规则 3		S (WTX) 响应	====>			
8. 规则 B	1		<====	I (0) 0		规则 10
9.		I (0) 1	====>		1	规则 D
10. 规则 B	0		<====	I (0) 1		规则 10

设定13 等待时间扩展请求，见表G. 13。

表G. 13 差错处理的等待时间扩展请求

注释	块号 (0)	PCD		PICC	块号 (1)	注释
1. 规则 1		I (0) 0	====>		0	规则 D
2.			<====	S (WTX) 请求		规则 9
3. 规则 3		S (WTX) 响应	====>			
4.			<===>	I (0) 0		规则 10
5. 规则 4		R (NAK) 0	====>			
6. 规则 B	1		<====	I (0) 0		规则 11
7.		I (0) 1	====>		1	规则 D
8. 规则 B	0		<====	I (0) 1		规则 10

设定14 等待时间扩展请求，见表G. 14。

表G. 14 差错处理的等待时间扩展请求

注释	块号 (0)	PCD		PICC	块号 (1)	注释
1. 规则 1		I (0) 0	====>		0	规则 D
2.			<====	S (WTX) 请求		规则 9

3. 规则 3		S (WTX) 响应	====>			
4.			<=≠=	I (0) 0		规则 10
5. 规则 4		R (NAK) 0	=≠=>			
6. 超时			<= =	-		
7. 规则 4		R (NAK) 0	====>			
8. 规则 B	1		<====	I (0) 0		规则 11
9.		I (0) 1	====>		1	规则 D
10. 规则 B	0		<====	I (0) 1		规则 10

G.3.3 DESELECT

设定15 DESELECT, 见表G.15。

表G.15 差错处理的DESELECT

注释	块号 (0)	PCD		PICC	块号 (1)	注释
1. 规则 1		I (0) 0	====>	I (0) 0	0	规则 D
2. 规则 B			<====			规则 10
3.		S (DESELECT) 请求	=≠=>			
4. 超时			<= =	-		
5. 规则 8		S (DESELECT) 请求	====>			
6.			<====	S (DESELECT) 响应		规则 3

G.3.4 链接

设定16 PCD使用链接, 见表G.16。

表G.16 差错处理的PCD使用链接

注释	块号 (0)	PCD		PICC	块号 (1)	注释
1. 规则 1		I (1) 0	====>		0	规则 D
2.			<=≠=	R (ACK) 0		规则 2
3. 规则 4		R (NAK) 0	====>			
4. 规则 B	1		<====	R (ACK) 0		规则 11
5. 规则 7		I (1) 1	====>		1	规则 D
6. 规则 B	0		<====	R (ACK) 1		规则 2
7. 规则 7		I (0) 0	====>		0	规则 D
8. 规则 B	1		<====	I (0) 0		规则 10
9.		I (0) 1	====>		1	规则 D
10. 规则 B	0		<====	I (0) 1		规则 10

设定17 PCD使用链接, 见表G.17。

表G.17 差错处理的PCD使用链接

注释	块号 (0)	PCD		PICC	块号 (1)	注释
1. 规则 1		I (1) 0	====>		0	规则 D
2. 规则 B	1		<====	R (ACK) 0		规则 2
3. 规则 7		I (1) 1	=≠=>			
4. 超时			<= =	-		
5. 规则 4		R (NAK) 0	====>			
6.	无变化		<====	R (ACK) 0		规则 12
7. 规则 6		I (1) 1	====>		1	规则 D

8. 规则 B	0		<====	R (ACK) 1		规则 2
9. 规则 7		I (0) 0	====>		0	规则 D
10. 规则 B	1		<====	I (0) 0		规则 10
11.		I (0) 1	====>		1	规则 D
12. 规则 B	0		<====	I (0) 1		规则 10

设定18 PCD使用链接，见表G. 18。

表G. 18 差错处理的PCD使用链接

注释	块号 (0)	PCD		PICC	块号 (1)	注释
1. 规则 1		I (1) 0	====>		0	规则 D
2.			<=≠=	R (ACK) 0		规则 2
3. 规则 4		R (NAK) 0	≠=>			
4. 超时			<= =	-		
5. 规则 4		R (NAK) 0	====>			
6. 规则 B	1		<====	R (ACK) 0		规则 11
7. 规则 7		I (1) 1	====>		1	规则 D
8. 规则 B	0		<====	R (ACK) 1		规则 2
9. 规则 7		I (0) 0	====>		0	规则 D
10. 规则 B	1		<====	I (0) 0		规则 10
11.		I (0) 1	====>		1	规则 D
12. 规则 B	0		<====	I (0) 1		规则 10

设定19 PICC使用链接，见表G. 19。

表G. 19 差错处理的PICC使用链接

注释	块号 (0)	PCD		PICC	块号 (1)	注释
1. 规则 1		I (0) 0	====>		0	规则 D
2. 规则 B	1		<====	I (1) 0		规则 10
3. 规则 2		R (ACK) 1	≠=>			
4. 超时			<= =	-		
5. 规则 5		R (ACK) 1	====>		1	规则 E
6. 规则 B	0		<====	I (1) 1		规则 13
7. 规则 2		R (ACK) 0	====>		0	规则 E
8. 规则 B	1		<====	I (0) 0		规则 13
9.		I (0) 1	====>		1	规则 D
10. 规则 B	0		<====	I (0) 1		规则 10

设定20 PICC使用链接，见表G. 20。

表G. 20 差错处理的PICC使用链接

注释	块号 (0)	PCD		PICC	块号 (1)	注释
1. 规则 1		I (0) 0	====>		0	规则 D
2. 规则 B	1		<====	I (1) 0		规则 10
3. 规则 2		R (ACK) 1	====>		1	规则 E
4.			<=≠=	I (1) 1		规则 13
5. 规则 5		R (ACK) 1	====>		无变化	
6. 规则 B	0		<====	I (1) 1		规则 11

JR/T 0025.8—2013

7. 规则 2		R (ACK) 0	====>		0	规则 E
8. 规则 B	1		<====	I (0) 0		规则 13
9.		I (0) 1	====>		1	规则 D
10. 规则 B	0		<====	I (0) 1		规则 10

附 录 H
(资料性附录)
块和帧编码概览

本附录给出了由PCD发送的不同的块和帧编码的概览。块的类型在各个帧的第一个字节指出。
第7章中的定义：

REQA	(0100110)b (7 位)
WUPA	(1010010)b (7 位)
REQB/WUPB	(00000101)b
Slot-MARKER (仅 Type B)	(xxxx0101)b
SELECT (仅 Type A)	(1001xxxx)b
ATTRIB (仅 Type B)	(00011101)b
HLTA	(01010000)b
HLTB	(01010000)b

本附录中的定义：

RATS	(11100000)b
PPS	(1101xxxx)b
I-块	(00xxxxxx)b (除了(00xxx101)b)
R-块	(10xxxxxx)b (除了(1001xxxx)b)
S-块	(11xxxxxx)b (除了(1110xxxx)b 和(1101xxxx)b)

表H. 1描述了已定义的块和帧编码的第一个字节。

表 H. 1 块和帧编码

位	I-块 PCB	R-块 PCB	DESELECT	S-块 PCB	WTX	REQB/WUPB	Slot-MARKER	SELECT	ATTRIB	HLTA	HLTB	RATS	PPS
b8	0	1	1			0	x	1	0	0	0	1	1
b7	0	0	1			0	x	0	0	1	1	1	1
b6	0 (RFU)	1	0	1		x	x	0	0	0	0	1	0
b5	链接	ACK/NAK	0	1		x	x	1	1	1	1	0	1
b4	CID	CID	CID			0	0	x	1	0	0	0	x
b3	NAD	0 (无 NAD)	0 (无 NAD)			1	1	x	1	0	0	0	x
b2	1	1 (RFU)	1 (RFU)			0	0	x	0	0	0	0	x
b1	块号	块号	0 (RFU)			1	1	x	1	0	0	0	x

附 录 I
(规范性附录)
安全报文

安全报文传送的目的是保证数据的可靠性、完整性和对发送方的认证。数据完整性和对发送方的认证通过使用MAC来实现。数据的可靠性通过对数据域的加密来得到保证。

1.1 安全报文传送格式

本部分中定义的安全报文传送格式应符合GB/T 16649.4的规定。当CLA字节的第二个半字节等于十六进制数字'4'时,表明对发送方命令数据要采用安全报文传送。卡中的FCI表明某个命令的数据域的数据是否需要加密传输,是否应该以加密的方式处理。安全报文传送格式见表I.1。

表 I.1 安全报文传送格式

b4	b3	b2	b1	说 明
0	0	x	x	不需要安全报文
0	1	x	x	需要安全报文

1.2 报文完整性和验证

MAC是使用命令的所有元素(包括命令头)产生的。一条命令的完整性,包括命令数据域(如果存在的话)中的数据元,通过安全报文传送得以保证。

1.2.1 MAC的位置

MAC是命令数据域中最后一个数据元。

1.2.2 MAC的长度

本部分中MAC的长度规定为4个字节。

1.2.3 MAC密钥的产生

在安全信息处理过程中用到的MAC过程密钥是按照I.3中描述的过程密钥的产生过程产生的。MAC密钥的原始密钥用于产生MAC过程密钥。

1.2.4 MAC的计算

如果用双长度DES密钥计算MAC,步骤如下:

步骤 1: 初始值为 8 字节全零(此步骤可省略);

步骤 2: 下列数据按顺序排列得到一个数据块 D:

——CLA、INS、P1、P2 和 Lc (Lc 的长度包括 MAC 的长度);

——ATC (对于发卡行脚本处理,此 ATC 在请求报文中上送);

——应用密文(对于发卡行脚本处理,此应用密文通常是 ARQC,或 AAC,在请求报文中上送);

——命令数据域中的明文或密文数据(如果存在);

步骤 3: 将上述数据块 D 分成 8 字节长的数据块 D1、D2、D3...最后一块数据块的字节长度为 1 到 8;

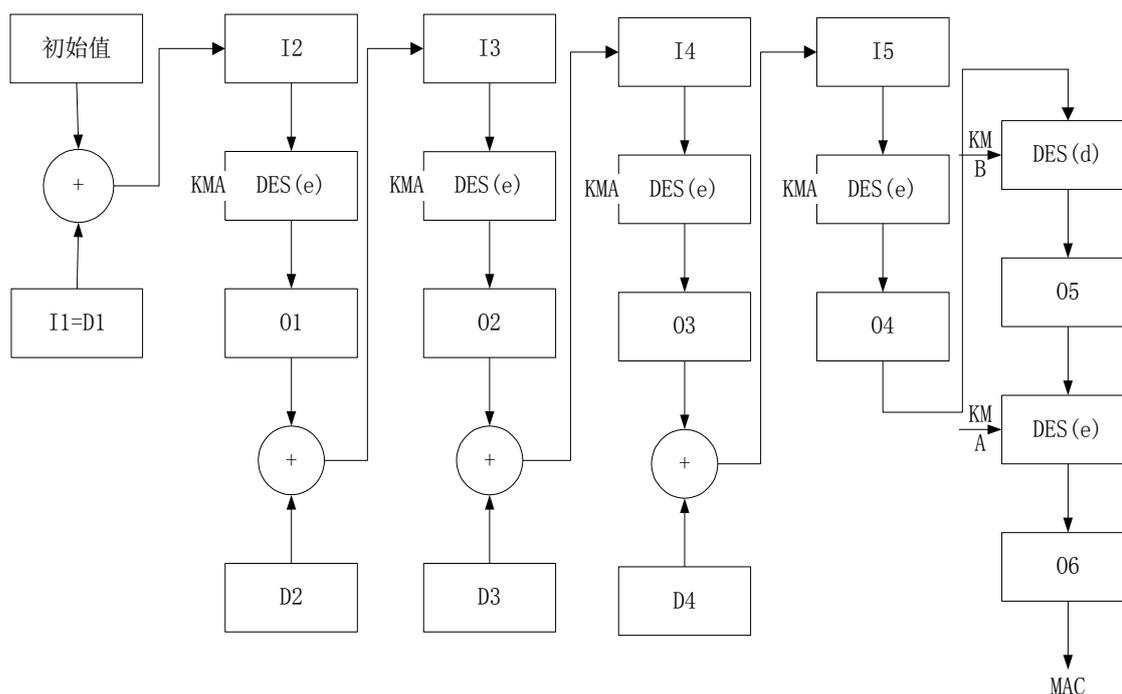
步骤 4: 如果最后一块数据块的长度为 8 字节,后面补 8 字节数据块: 80 00 00 00 00 00 00 00, 执行步骤 5;

如果最后一块数据块的长度小于 8 字节,后面补一个字节 80,如果长度到 8 字节,执行步骤 5。如果仍然不够 8 字节,补 00 直到 8 字节;

步骤 5: 用 MAC 过程密钥对数据块进行加密。MAC 过程密钥的生成见 1.3;

图 1.1 是使用 MAC 过程密钥 A 和 B 生成 MAC 的流程图;

步骤 6: MAC 的计算结果为 8 字节,从最左边的字节开始取 4 字节。



说明:

I = 输入	D = 数据块
DES(e) = DES算法 (加密模式)	KMA = MAC过程密钥A
DES(d) = DES算法 (解密模式)	KMB = MAC过程密钥B
O = 输出	+ = 异或

图 1.1 使用双长度 DES 密钥计算 MAC

如果用 SM4 算法计算 MAC，步骤如下：

步骤 1：初始值为 16 字节全零（此步骤可省略）；

步骤 2：下列数据按顺序排列得到一个数据块 D：

——CLA、INS、P1、P2 和 Lc（Lc 的长度包括 MAC 的长度）；

——ATC（对于发卡行脚本处理，此 ATC 在请求申报文中上送）；

——应用密文（对于发卡行脚本处理，此应用密文通常是 ARQC，或 AAC，在请求报文中上送）；

——命令数据域中的明文或密文数据（如果存在）。

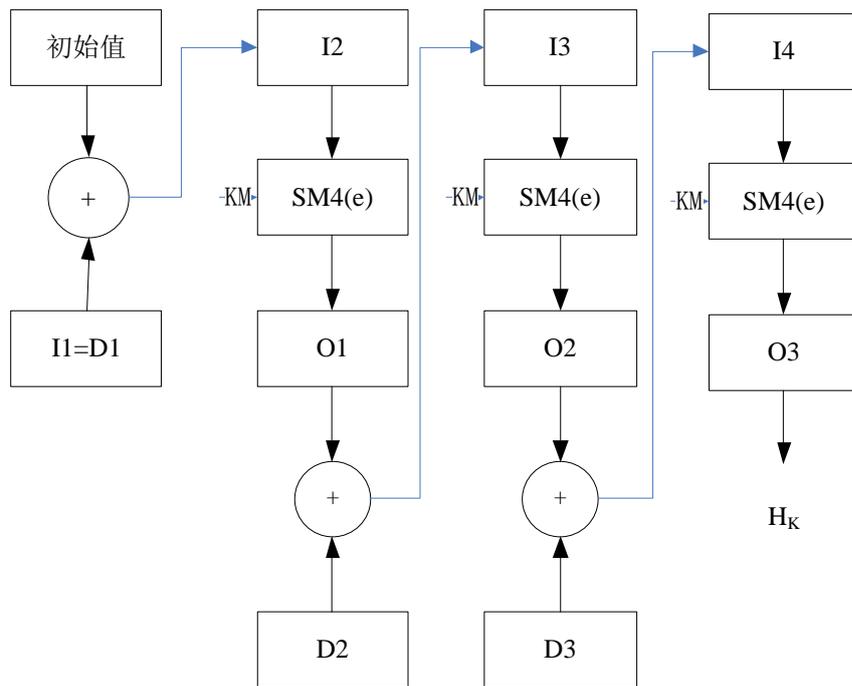
步骤 3：将上述数据块 D 分成 16 字节长的数据块 D1、D2、D3...最后一块数据块的字节长度为 1 到 16；

步骤 4：如果最后一块数据块的长度为 16 字节，后面补 16 字节数据块：80 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00，执行步骤 5；

如果最后一块数据块的长度小于 16 字节，后面补一个字节 80，如果长度到 16 字节，执行步骤 5。如果仍然不够 16 字节，补 00 直到 16 字节；

步骤 5：用 MAC 过程密钥对数据块进行加密，MAC 过程密钥的生成见 1.3。

图 1.2 是使用 MAC 过程密钥生成 MAC 的流程图，取计算结果 H_k 的前 4 字节作为 MAC 值。



说明：

I = 输入	D = X = 数据块
SM4(e) = SM4算法（加密模式）	KM = MAC过程密钥
O = 输出	+ = 异或

图 1.2 使用 SM4 算法计算 MAC

1.3 过程密钥的产生

本部分描述了过程密钥的生成方法。

如果用双长度DES密钥生成，步骤如下：

步骤 1：生成过程密钥的卡片密钥是：MAC DES 密钥 A 和 B（MAC UDK），数据加密 DES 密钥 A 和 B（ENC UDK）；

步骤 2：将两字节的 ATC 右对齐，前面补 6 个字节 00.....（见 JR/T 0025.7）；

步骤 3：将两字节的 ATC 取反后右对齐，前面补 6 个字节 00.....（见 JR/T 0025.7）。

如果用 SM4 算法生成，步骤如下：

步骤 1：生成过程密钥的卡片密钥是：MAC SM4 密钥（MAC UDK），数据加密 SM4 密钥（ENC UDK）；

步骤 2：将两字节的 ATC 右对齐，前面补 14 个字节 00.....（见 JR/T 0025.17）；

步骤 3：将两字节的 ATC 取反后右对齐，前面补 14 个字节 00.....（见 JR/T 0025.17）。

参考文献

- [1] GB/T 15120.1—1994 识别卡 记录技术 第1部分：凸印（ISO 7811-1:1985, IDT）
- [2] GB/T 15120.2—1994 识别卡 记录技术 第2部分：磁条（ISO 7811-2:1985, IDT）
- [3] GB/T 15120.3—1994 识别卡 记录技术 第3部分：ID-1型卡上凸印字符的位（ISO 7811-3:1985, IDT）
- [4] GB/T 15120.4—1994 识别卡 记录技术 第4部分：ID-1型卡上只读磁道 磁道1和2的位置（ISO 7811-4:1985, IDT）
- [5] GB/T 15694.1—1995 识别卡 发卡者的标识 第1部分：编码体系（ISO/IEC 7812-1:1993, IDT）
- [6] GB/T 15694.2—2002 识别卡 发卡者的标识 第2部分：应用和注册规程（ISO/IEC 7812-2:2000, IDT）
- [7] GB/T 16649.1—2006 识别卡 带触点的集成电路卡 第1部分：物理特性（ISO/IEC 7816-1:1998, MOD）
- [8] GB/T 17552—2008 识别卡 金融交易卡（ISO/IEC 7813:2006, IDT）
- [9] ISO/IEC 7811-5:1995 识别卡 记录技术 第5部分：ID-1型卡上读写磁道 磁道3的位置
- [10] ISO/IEC 7811-6:1995 识别卡 记录技术 第6部分：磁条 高矫顽磁性
- [11] ISO/IEC 10536-1:1992 识别卡 无触点集成电路卡 第1部分：物理特性
- [12] ISO/IEC 10536-2:1995 识别卡 无触点集成电路卡 第2部分：耦合区域的尺寸和位置
- [13] ISO/IEC 10536-3:1992 识别卡 无触点集成电路卡 第3部分：电信号和重设置过程
-