



复旦微电子

FM11NT0X1TT ***NFC Forum Type2 Tag 芯片***

技术手册

2018. 7



本资料是为了让用户根据用途选择合适的上海复旦微电子集团股份有限公司（以下简称复旦微电子）的产品而提供的参考资料，不转让属于复旦微电子或者第三者所有的知识产权以及其他权利的许可。

在使用本资料所记载的信息最终做出有关信息和产品是否适用的判断前，请您务必将所有信息作为一个整体系统来进行评价。

采购方对于选择与使用本文描述的复旦微电子的产品和服务全权负责，复旦微电子不承担采购方选择与使用本文描述的产品和服务的责任。除非以书面形式明确地认可，复旦微电子的产品不推荐、不授权、不担保用于包括军事、航空、航天、救生及生命维持系统在内的，由于失效或故障可能导致人身伤亡、严重的财产或环境损失的产品或系统中。

未经复旦微电子的许可，不得翻印或者复制全部或部分本资料的内容。

今后日常的产品更新会在适当的时候发布，恕不另行通知。在购买本资料所记载的产品时，请预先向复旦微电子在当地的销售办事处确认最新信息，并请您通过各种方式关注复旦微电子公布的信息，包括复旦微电子的网站(<http://www.fmsh.com/>)。

如果您需要了解有关本资料所记载的信息或产品的详情，请与上海复旦微电子集团股份有限公司在当地的销售办事处联系。

商 标

上海复旦微电子集团股份有限公司的公司名称、徽标以及“复旦”徽标均为上海复旦微电子集团股份有限公司及其分公司在中国的商标或注册商标。

上海复旦微电子集团股份有限公司在中国发布，版权所有。

目 录

目 录.....	3
1 说明.....	4
2 产品综述.....	5
2.1 产品简介	5
2.2 产品特点	5
2.2.1 EEPROM 存储器.....	5
2.2.2 NFC Forum Type2 Tag 兼容性.....	5
2.2.3 防拆功能.....	6
2.2.4 安全特性.....	6
2.3 结构框图	7
2.4 引脚说明	7
3 功能描述.....	8
3.1 总体描述	8
3.2 存储器	8
3.2.1 概述.....	8
3.2.2 EEPROM 存储空间定义.....	8
3.2.3 UID/Serial Number.....	12
3.2.4 Static Lock Bytes.....	12
3.2.5 Dynamic Lock Bytes.....	12
3.2.6 Capability Container (CC bytes)	14
3.2.7 存储器初始化.....	14
3.2.8 配置信息块.....	15
3.3 通信原理	17
3.4 附加功能	18
3.4.1 Counter	18
3.4.2 ASCII 映射功能.....	18
3.4.3 密码保护.....	22
3.5 指令系统	23
3.5.1 概述.....	23
3.5.2 部分指令详细说明.....	24
4 电气参数.....	30
4.1 极限额定参数	30
4.2 推荐工作条件	30
4.3 电参数	30
4.4 存储器参数	31
5 订货信息.....	32
6 封装信息.....	33
6.1 TSOT 封装	33
版本信息.....	34
上海复旦微电子集团股份有限公司销售及服务中心	35



1 说明

本文档为 FM11NT0X1TT 芯片技术手册。FM11NT0X1TT 是复旦微电子有限公司开发的第二代符合 ISO/IEC14443-A 协议和 NFC Forum Type2 Tag 标准的、具备防拆功能的芯片。FM11NT0X1TT 分为三种子类型：FM11NT021TT、FM11NT041TT 和 FM11NT081TT。请联系复旦微电子有限公司提供更多相关文档支持详细设计开发。

2 产品综述

2.1 产品简介

FM11NT0X1TT 是复旦微电子公司开发的符合 ISO/IEC14443-A 协议和 NFC Forum Type2 Tag 标准的、具备防拆功能的标签芯片。FM11NT0X1TT 分为 3 种子类型：FM11NT021TT、FM11NT041TT 和 FM11NT081TT，对应三种不同大小的存储器用户区。可广泛应用于智能包装、物品防伪等领域。

2.2 产品特点

- 通讯协议：ISO/IEC 14443-A
- 工作频率：13.56MHz
- 具有防冲突功能
- 最远操作距离：10cm（与天线设计和读卡器功率有关）
- 数据传输速率：106 kbit/s
- 高数据完整性：16bit CRC，奇偶校验
- 7 bytes UID，两重防冲突
- 支持 UID ASCII 映射功能，可自动序列化为 NDEF 信息
- 自动计数器，每次上电后第一次执行读或快速读指令触发计数一次
- 支持计数器计数值的 ASCII 映射功能，可自动映射为 NDEF 信息
- 支持快速读取指令
- 50pF 谐振电容
- 利用 DP 和 GND 管脚可支持防拆功能

2.2.1 EEPROM 存储器

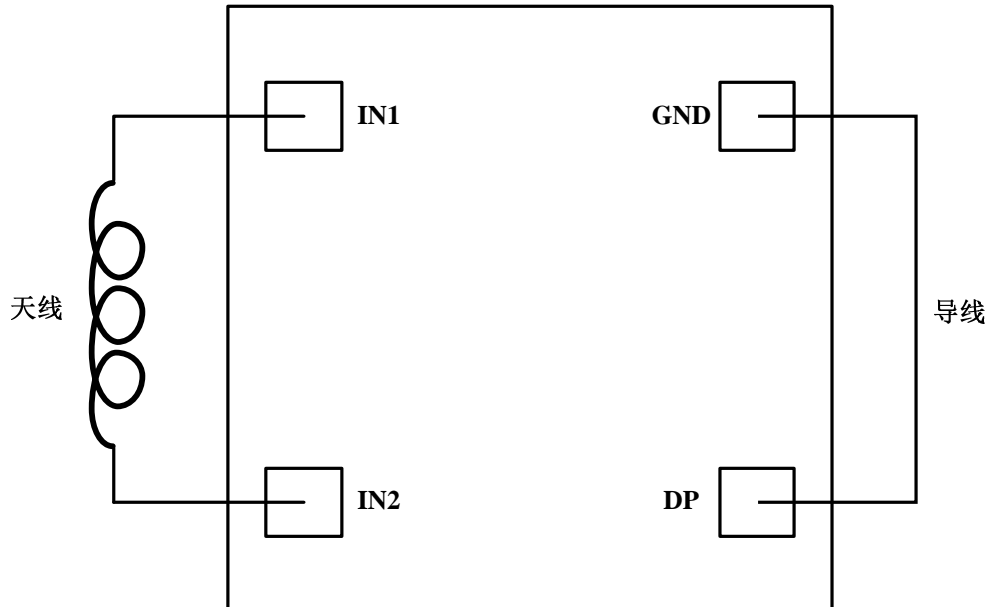
- 三种产品的 EEPROM 总容量分别为 180, 540 或 924 bytes, 分为 45, 135, 或 231 页(Page), 每页 4 bytes
- 三种产品的 EEPROM 用户区容量分别为 144, 504, 或 888 bytes, 分为 36, 126 或 222 页 (Page), 每页 4 bytes
- 三种产品的前 16 页均可单页锁定（一页对应一位锁定位），对于 FM11NT021TT, 16 页以后的存储区间可双页锁定（两页对应一位锁定位）；对于 FM11NT041TT 和 FM11NT081TT, 16 页以后的存储区间按每 16 页进行锁定（16 个连续页对应一位锁定位）。
- 数据保存时间：大于 10 年
- 擦写次数：大于 100 万次

2.2.2 NFC Forum Type2 Tag 兼容性

FM11NT0X1TT 芯片功能完全兼容 NFC Forum Type2 Tag 的技术要求，芯片出厂时已做好 NDEF 格式数据的初始化。

2.2.3 防拆功能

FM11NT0X1TT 具备 Tag Temper 防拆功能。在芯片外部将 DP 和 GND 管脚短接在一起。如下图所示。导线的状态有两种：闭合、断开。标签收到 PCD 的特定指令时，标签会将导线的状态回发给 PCD。PCD 由此可获悉标签在附着物上的状态是否发生改变。



PCD 若要获取 Detection 线路的状态，需进行如下配置：

- Mirror_Conf = 2'b11，即同时启用 UID Mirror 和 NFC CNT Mirror 功能；
- 使用 Read Block 命令读取 Mirror 地址数据，并将 UID Mirror 和 NFC CNT Mirror 数据的分隔符读出。

PCD 可通过判断标签返回的 Mirror 分隔符的值来确定连接状态：若分隔符为 79H，则处于断开状态；若分隔符为 78H，则处于闭合状态。

2.2.4 安全特性

- 每颗芯片拥有独立 7 byte UID，UID 不可改写
- CC 区有 OTP 功能，具有抗撕裂能力，防止恶意解锁。
- 存储区具有只读锁定功能
- 具有可选择使能的密码保护存储区功能，密码尝试的最大次数可配置。
- 基于算法的原厂数字签名

2.3 结构框图

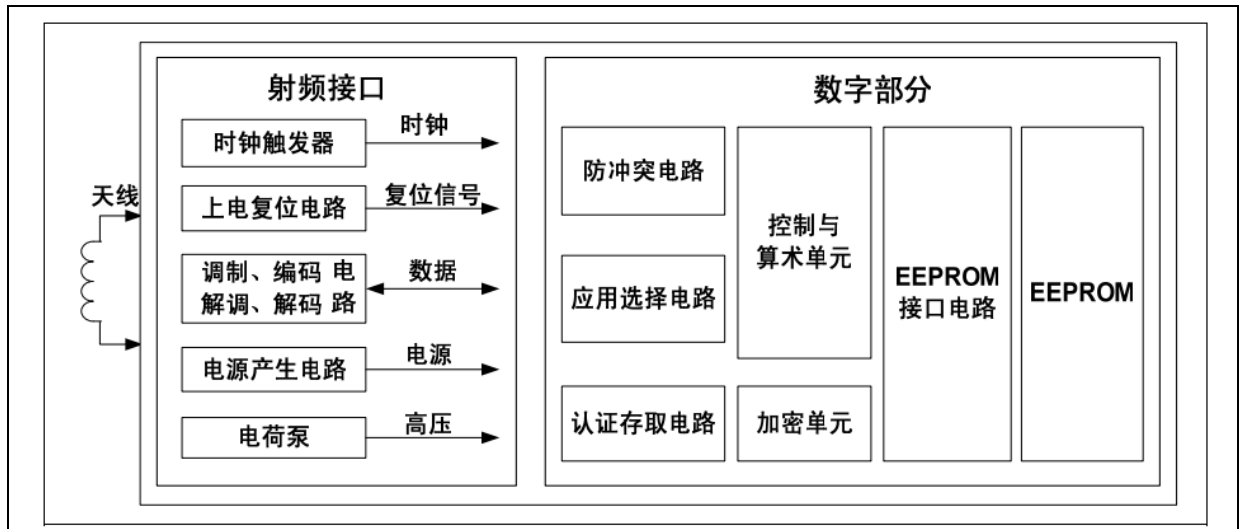


图 2-1 FM11NT0X1TT 结构框图

2.4 引脚说明

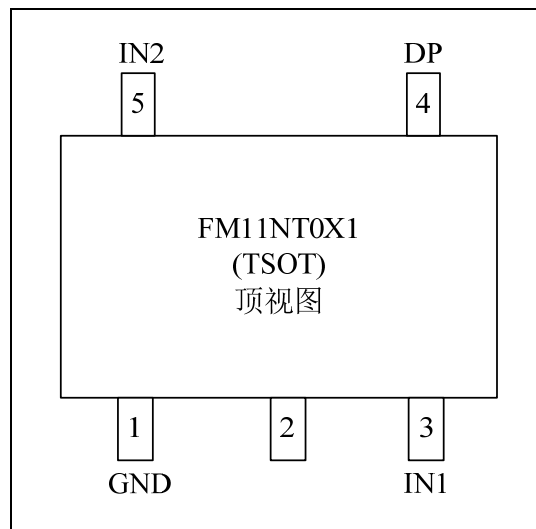


图 2-2 TSOT23-5L 封装引脚示意图

编号	管脚名称	说明
1	GND	芯片地
2		悬空
3	IN1	天线射频输入端
4	DP	与 GND 互连，具备防拆功能
5	IN2	天线射频输入端

表 2-1 TSOT23-5L 封装引脚列表

3 功能描述

3.1 总体描述

FM11NT0X1TT 芯片由三部分构成：

- 射频模拟电路
- 数字逻辑电路
- 非易失性存储器（EEPROM）

射频模拟电路完成数据的解调和回发，为整个芯片提供稳定的电源和时钟。

数字逻辑电路完成协议的处理，并控制 EEPROM 的读写操作。

EEPROM 提供高可靠的数据存储。

3.2 存储器

3.2.1 概述

FM11NT0X1TT 的 EEPROM 以 4 字节为一页进行组织，不同产品型号的用户存储区容量参见下表：

型号	用户存储器字节数	用户存储器块地址范围
FM11NT021TT	144	04h~27h
FM11NT041TT	504	04h~81h
FM11NT081TT	888	04h~E1h

表 3-1 用户存储空间与型号的对应关系

3.2.2 EEPROM 存储空间定义

3.2.2.1 FM11NT021TT



图 3-1 FM11NT021TT 存储空间分配

上图中各区域的详细访问权限和说明参见下表:

存储区域	地址范围 (Byte)	用户访问	功能说明
UID	0000h~0008h	R	ISO14443A UID + BCC
Static Lock	000Ah~000Bh	OTP	静态锁定位
CC	000Ch~000Fh	RWL	Capability Container
User Data	0010h~009Fh	RWL	用户数据
Dynamic Lock	00A0h~00A3h	OTP	动态锁定位
Configuration	00A4h~00B3h	RWL	用户配置区

说明:

F – Forbidden

R – Read

W – Write

L – Writing can be Locked

3.2.2.2 FM11NT041TT



图 3-2 FM11NT041TT 存储空间分配

上图中各区域的详细访问权限和说明参见下表：

存储区域	地址范围 (Byte)	用户访问	功能说明
UID	0000h~0008h	R	ISO14443A UID + BCC
Static Lock	000Ah~000Bh	OTP	静态锁定位
CC	000Ch~000Fh	RWL	Capability Container
User Data	0010h~0207h	RWL	用户数据
Dynamic Lock	0208h~020Bh	OTP	动态锁定位
Configuration	020Ch~021Bh	RWL	用户配置区

说明：

F – Forbidden

R – Read

W – Write

L – Writing can be Locked

3.2.2.3 FM11NT081TT

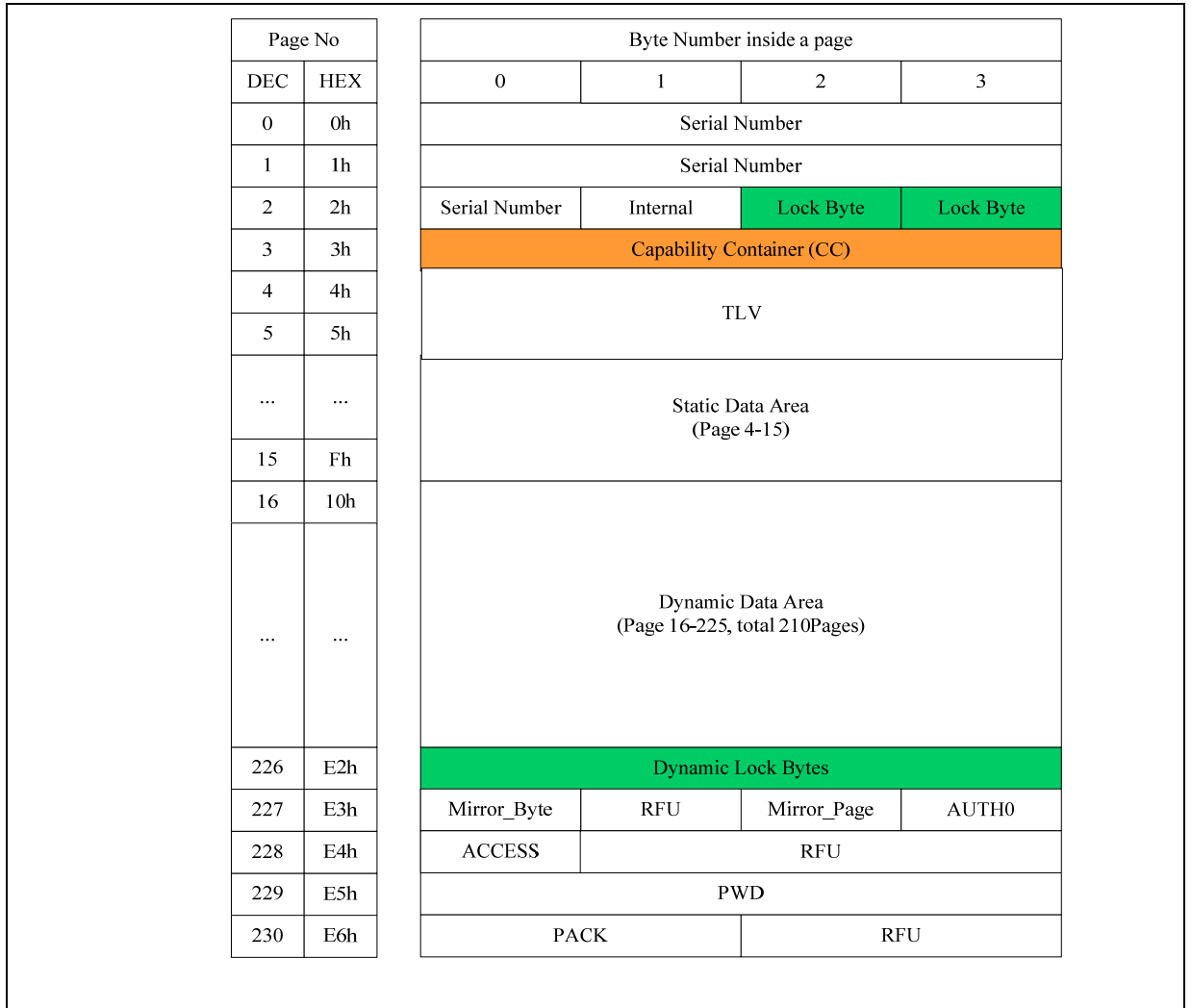


图 3-3 FM11NT081TT 存储空间分配

上图中各区域的详细访问权限和说明参见下表：

存储区域	地址范围 (Byte)	用户访问	功能说明
UID	0000h~0008h	R	ISO14443A UID + BCC
Static Lock	000Ah~000Bh	OTP	静态锁定位
CC	000Ch~000Fh	RWL	Capability Container
User Data	0010h~0387h	RWL	用户数据
Dynamic Lock	0388h~038Bh	OTP	动态锁定位
Configuration	038Ch~039Bh	RWL	用户配置区

说明：

F – Forbidden

R – Read

W – Write

L – Writing can be Locked

3.2.3 UID/Serial Number

每颗芯片独有的 7 字节序列号 (UID) 及其 2 字节校验码存放在 EE 的最低地址, 包括 Page0、Page1 和 Page2 的第一字节。UID 在出厂时写入, 用户不能改写。

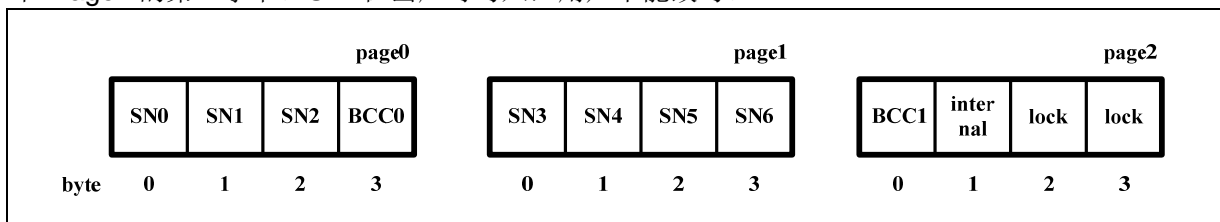


图 3-4 UID/Serial Number

根据 ISO14443-3 校验字节 BCC0 定义为 $CT \oplus SN0 \oplus SN1 \oplus SN2$, 而 BCC1 定义为 $SN3 \oplus SN4 \oplus SN5 \oplus SN6$ 。

SN0 保存复旦微电子公司的制造商代码。

3.2.4 Static Lock Bytes

Page2 的 byte2 和 byte3 为 static lock bytes, 可用于锁定 static data area 中的 12 页和 CC 页的写权限。Static lock bits 为 OTP 属性, 用户一旦将其改写为 1, 便无法再改写为 0, 同时对应锁定的页变为只读属性, 无法改写。

Lock byte0 的 Bit7~Bit4 和 lock byte1 的 Bit7~Bit0 分别对应锁定 12 个 static data page, lock byte0 的 Bit3 对应锁定 CC 页, lock byte0 的 Bit2~Bit0 则为 Block-Locking Bits (BL), BL 位一旦置为 1, 则对应的 lock 位不能再被改写。

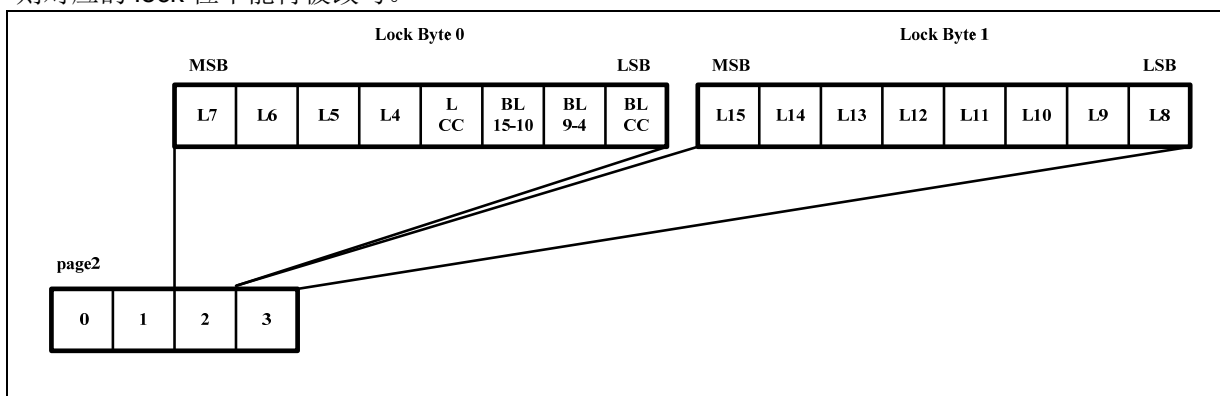


图 3-5 UID/Serial Number

上图中, L_x 表示用于锁定 Page x 的写权限, BL_x 表示阻止改写 memory area x 的 BL 位。

比如, 若 BL_{15-10} 被置为 1, 则 $L_{15} \sim L_{10}$ (lock byte1 的 Bit[7:2]) 将不能再被改写。所有的 L_x 和 BL_x 都是 OTP 的, 用户可以用 WRITE 或 COMPATIBILITY_WRITE 命令进行改写, 一旦写为 1, 不能再改写为 0, 且具有抗撕裂能力。出厂时, Static Lock bytes 的默认值为 00 00h。

3.2.5 Dynamic Lock Bytes

根据 NFC T2TOP 规范, Dynamic Lock bytes 用来锁定从 Page 10h 开始的用户存储器区域。Dynamic Lock bytes 所在地址根据产品型号不同而不同。

型号	Dynamic Lock Bytes 页地址	页锁定范围
FM11NT021TT	28h	16~39
FM11NT041TT	82h	16~129
FM11NT081TT	E2h	16~225

表 3-2 Dynamic Lock Bytes 块地址

Dynamic Lock bytes 同样具有 OTP 属性，一旦被置为 1，不能再被改写为 0。

FM11NT021TT Dynamic Lock bytes 定义：

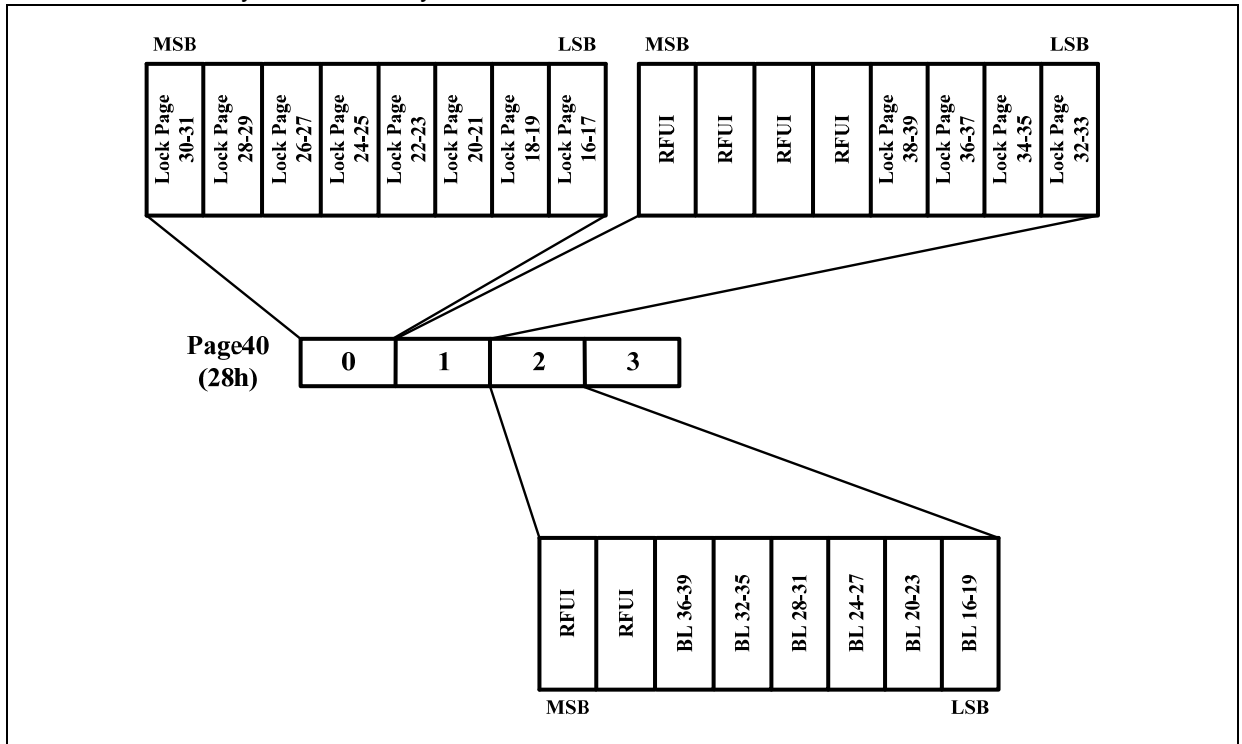


图 3-6 FM11NT021TT Dynamic Lock Bytes

FM11NT041TT Dynamic Lock bytes 定义：

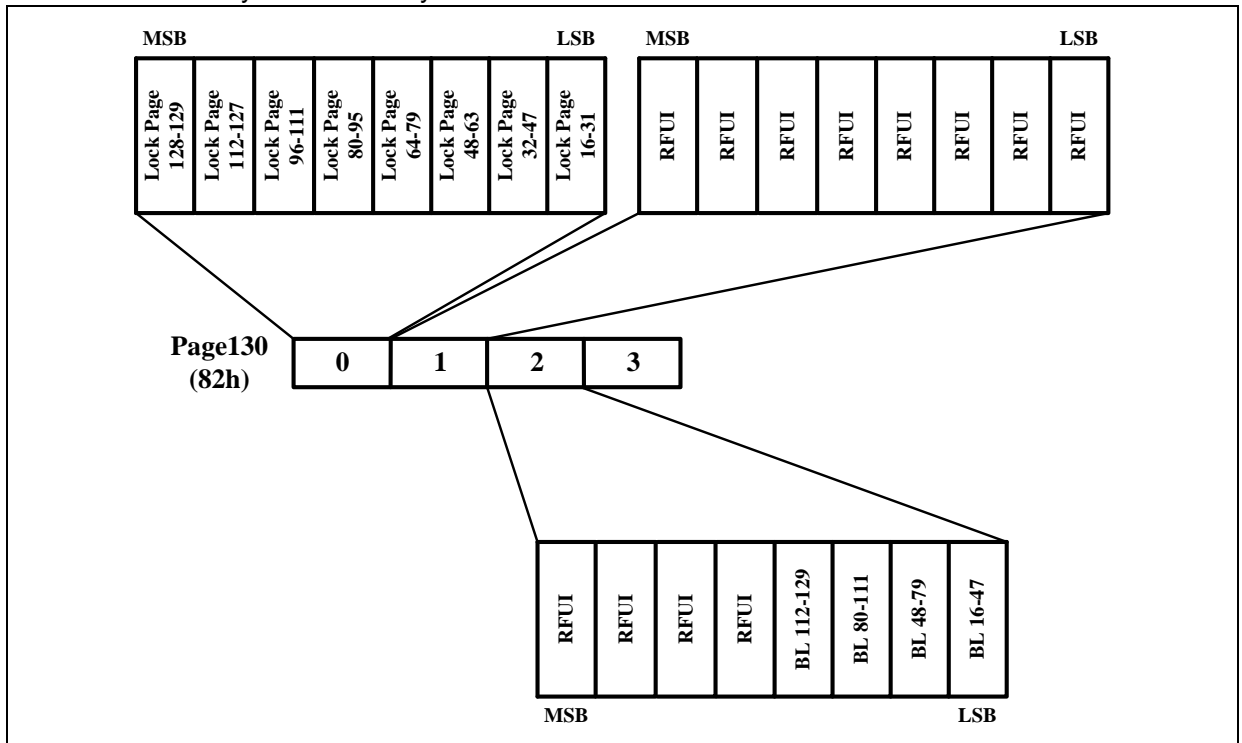


图 3-7 FM11NT041TT Dynamic Lock Bytes

FM11NT081TT Dynamic Lock bytes 定义:

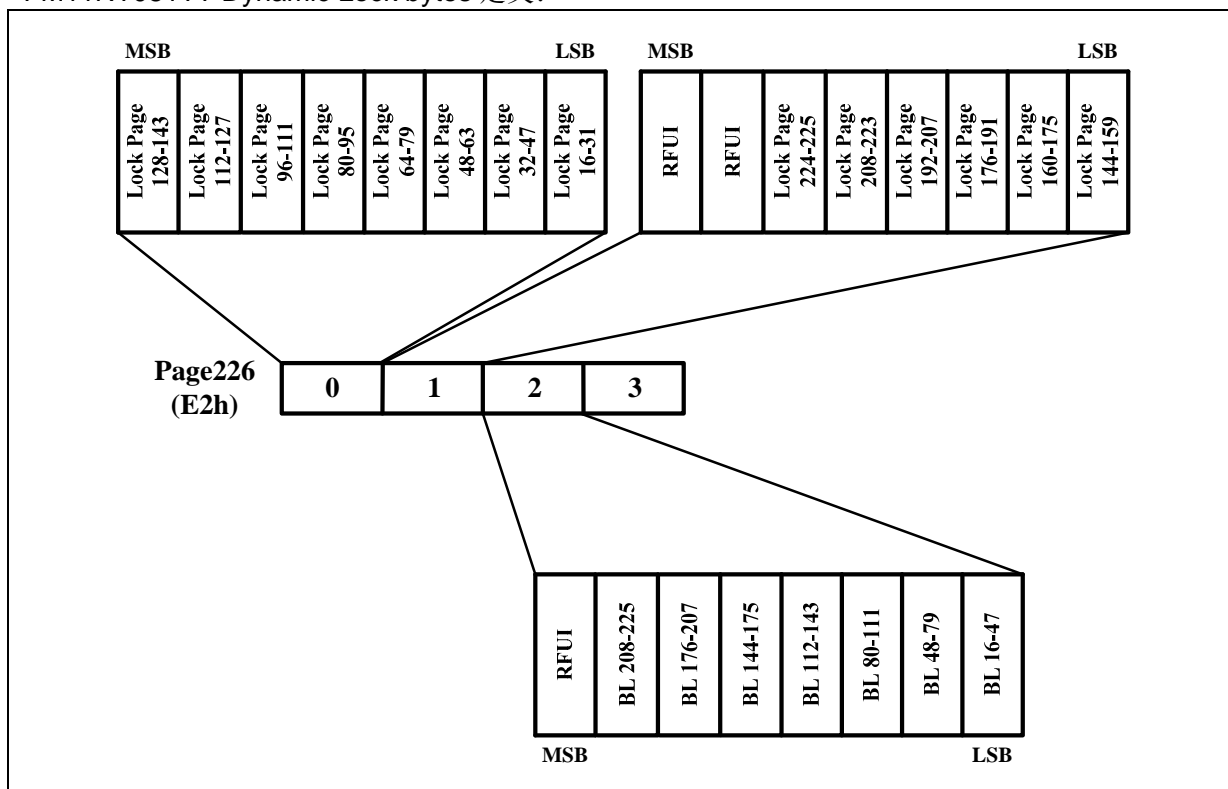


图 3-8 FM11NT081TT Dynamic Lock Bytes

3.2.6 Capability Container (CC bytes)

Capability Container 根据 NFC Forum Type2 Tag 规范生成。CC 页内容的详细定义可参考协议 NFC Forum T2TOP1.1。CC 页的内容可以通过 WRITE 或者 COMPATIBILITY_WRITE 指令改写，CC 页具有 OTP 属性，一旦置为 1，不能再改写为 0。

为了保证对 NFC T2TOP 的兼容性，不建议用户修改 CC 页的内容。

CC 的详细定义如下：

- Byte0: 必须为 E1h 以符合 NFC Forum 要求
- Byte1: 代表芯片支持的 NFCT2T OP 版本号，比如 10h 表示 version1.0
- Byte2: 此字节×8 代表 data area 大小，比如 06h 表示 Tag 数据区为 48 字节
- Byte3: 高 4bit 表示 CC 和 data area 的读权限，默认 0h，8h-Eh 为私有化数据，1h-7h 和 Fh 为 RFUI；低 4bit 表示 CC 和 data area 的写权限，默认 0h，Fh 表示禁止写权限

3.2.7 存储器初始化

FM11NT0X1TT 的 CC 页 (03h) 以及数据页 04h、05h 在芯片出厂时已经根据 NFC Forum T2TOP 规范预先进行了数据初始化。以下三个表格分别表明了 FM11NT021TT、FM11NT041TT、FM11NT081TT 出厂后的初始化内容。05h 以后的用户区初始化数据为全“00h”。

所有的 LOCK 位在出厂时为“0”状态，意味着所有的页都处于未锁定状态。

页地址	Byte0	Byte1	Byte2	Byte3
03h	E1h	10h	12h	00h
04h	01h	03h	A0h	0Ch
05h	34h	03h	00h	FEh

表 3-3 FM11NT021TT 初始化内容



页地址	Byte0	Byte1	Byte2	Byte3
03h	E1h	10h	3Eh	00h
04h	03h	00h	FEh	00h
05h	00h	00h	00h	00h

表 3-4 FM11NT041TT 初始化内容

页地址	Byte0	Byte1	Byte2	Byte3
03h	E1h	10h	6Dh	00h
04h	03h	00h	FEh	00h
05h	00h	00h	00h	00h

表 3-5 FM11NT081TT 初始化内容

3.2.8 配置信息块

3.2.8.1 概述

FM11NT021TT 的 29h~2Ch 页、FM11NT041TT 的 83h~86h 页和 FM11NT081TT 的 E3h~E6h 页是芯片的用户配置信息区，其内容定义如下：

页地址	Byte0	Byte1	Byte2	Byte3
29h/83h/E3h	Mapping	RFUI	Mapping Page	AUTH0
2Ah/84h/E4h	ACCESS	RFUI	RFUI	RFUI
2Bh/85h/E5h	PWD			
2Ch/86h/E6h	PACK		RFUI	RFUI

表 3-6 FM11NT0X1TT 配置信息区

3.2.8.2 ACCESS

Name: ACCESS			
Field	Description	Reset	Access
7	PROT 定义密码保护程度 0: 写 EE 需要密码验证 1: 读写 EE 都需要密码验证	0	RW
6	CFGLOCK 配置区锁定位（只锁定最低 2 页） 0: 配置区可以改写 1: 配置信息永久不可写	0	RW
5	RFU		
4	NFC_CNT_EN 0: Counter 禁止 1: Counter 使能 如果 Counter 使能，Counter 会在每次进场后收到的第一个 READ 或 FAST_READ 时递增	0	RW



Name: ACCESS			
Field	Description	Reset	Access
3	NFC_CNT_PWD_PROT 0: Counter 不受密码保护 1: Counter 密码保护使能 如果 Counter 密码保护使能, FM11NT0X1TT 只会在经过密码认证之后响应 READ_CNT 命令并回发 Counter 值, 否则回发错误代码	0	RW
2:0	AUTHLIM 密码验证错误次数上限 000: 无上限 001-111: 指定密码错误最大次数 一旦密码验证错误超过 AUTHLIM, 后续 PWD_AUTH 命令不论密码正确与否全部响应 NAK	3'b000	RW

表 3-7 ACCESS byte 功能描述

3.2.8.3 Mapping

Name: Mapping Byte			
Field	Description	Reset	Access
7:6	Mapping CONF 定义使用哪种 ASCII 映射 00: 无 ASCII 映射 01: 使用 UID 映射 10: 使用 Counter 映射 11: 同时使用 UID 和 Counter 映射	2'b00	RW
5:4	Mapping Byte ASCII 映射目标起始字节地址	2'b00	RW
3:0	RFU		

表 3-8 Mapping byte 功能描述

3.2.8.4 Mapping Page

Name: Mapping Page			
Field	Description	Reset	Access
7:0	Mapping Page ASCII 映射目标起始页地址。 Mapping Page > 03h 时使能 ASCII 映射, 长度 14 字节。	8'h0	RW

表 3-9 Mapping Block byte 功能描述

3.2.8.5 AUTH0

Name: AUTH0			
Field	Description	Reset	Access
7:0	AUTH0	8'hFF	RW



定义需要密码保护的起始页地址。		
-----------------	--	--

表 3-10 AUTH0 byte 功能描述

3.2.8.6 PWD

Name: PWD			
Field	Description	Reset	Access
31:0	PWD 32bit 密码，用户模式下不可读 不被 AUTH0 保护时用户可写，建议将 PWD 置于 AUTH0 保护范围内，经过 PWD_AUTH 之后才可以改写。	32'hFFFFFFFF	RW

表 3-11 PWD byte 功能描述

3.2.8.7 PACK

Name: PACK			
Field	Description	Reset	Access
15:0	PACK 16bit 密码认证回发 PWD_AUTH 命令下发的密码与 FM11NT0X1TT 本地 PWD 相符时回发 PACK，否则回发 NAK。 不被 AUTH0 保护时用户可写，建议将 PACK 置于 AUTH0 保护范围内，经过 PWD_AUTH 之后才可以改写。	16'h0000	RW

表 3-12 PACK byte 功能描述

3.3 通信原理

具体通信协议和时序定义等请用户自行参考 ISO/IEC 14443-A 协议。

芯片工作流程符合 ISO14443A-3 协议，如下图所示：

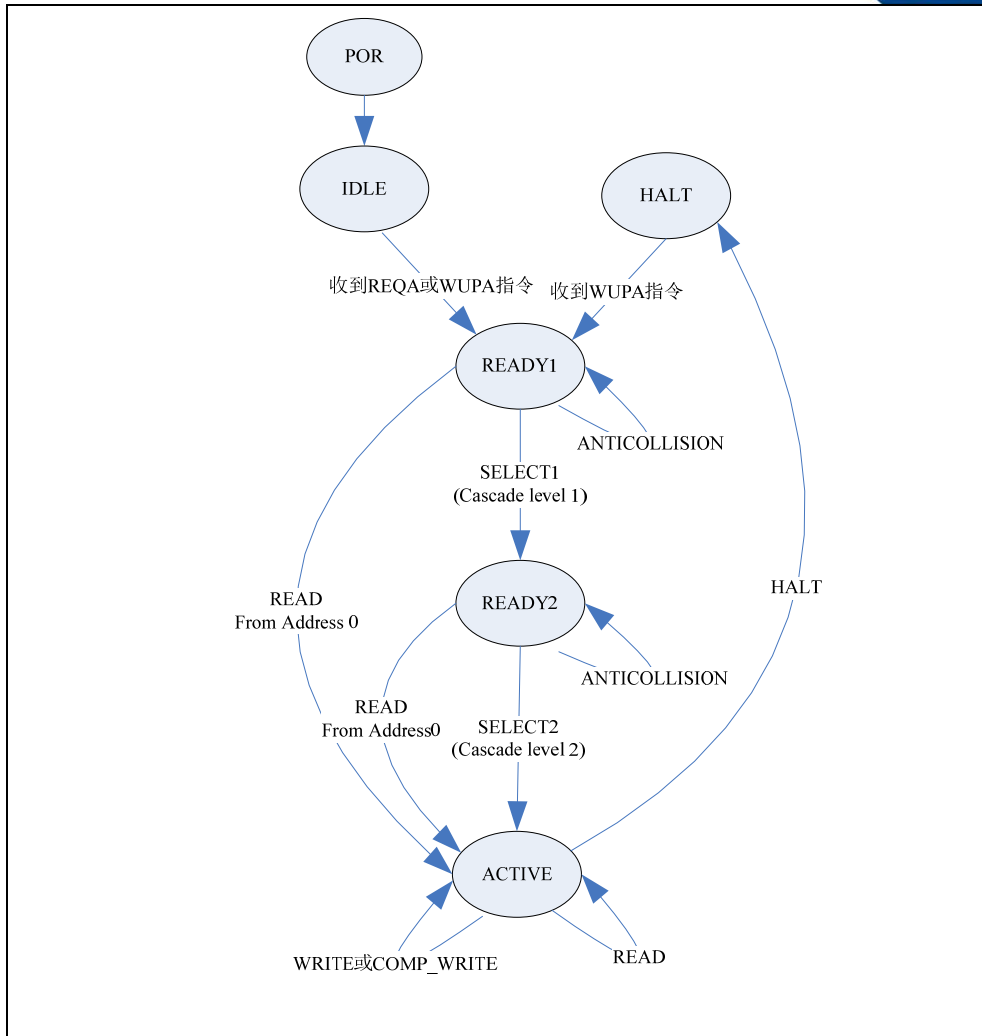


图 3-9 工作流程

3.4 附加功能

FM11NT0X1TT 除符合 NFC FORUM T2T 规范规定功能以外，还有以下附加功能。

3.4.1 Counter

FM11NT0X1TT 内建一个 24bit 非挥发计数器，在每次进场后收到第一条 READ 或 FAST_READ 命令时，自动触发计数器递增。

Counter 功能可以用 NFC_CNT_EN 位来使能或者禁止（参见章节 3.2.8.2）。

Counter 的值可以使用 READ_CNT 命令或者 Counter Mapping 功能读出。读取计数值也可以被密码保护，使能或禁止密码保护由 NFC_CNT_PWD_PROT（参见章节 3.2.8.2）控制。

3.4.2 ASCII 映射功能

3.4.2.1 概述

FM11NT0X1TT 支持将 7 字节 UID 或 3 字节 Counter 的 ASCII 码映射到用户数据区的某处空间中。当 READ 或者 FAST_READ 指令读取的 EE 空间中包含此 Mapping 空间，则 FM11NT0X1TT 回发 UID 或 Counter 的 ASCII 码，而非此物理空间中的实际存储数据。



根据 EE 中的 MAPPING_CONF（参见章节 3.2.8.4）配置，用户可以选择单独映射 UID、Counter 或者同时映射 UID+Counter。

映射的起始地址由 MAPPING_PAGE（参见章节 3.2.8.5）和 MAPPING_BYTE（参见章节 3.2.8.4）信息共同定义。

如果同时映射 UID 和 Counter，则 UID 和 Counter 字节之间自动插入“x”字符（ASCII 码 78h）进行分割。

ASCII Mapping	存储器中需要占据的空间
UID	14 bytes
Counter	6 bytes
UID + Counter	14 bytes UID + 1 byte 分隔符 + 6 bytes Counter = 21 bytes

表 3-13 映射所需空间大小

3.4.2.2 UID 映射

此功能可以将 7 字节 UID 的 ASCII 码映射到芯片的物理存储空间中的特定地址，映射后需要占据 14 字节。当 READ 或者 FAST_READ 指令涉及到被映射的地址，FM11NT0X1TT 将回发 UID 的 ASCII 码，而不是实际物理空间中的数据。

物理存储空间中被映射的目标地址可以通过 MAPPING_PAGE 和 MAPPING_BYTE 指定。其中 MAPPING_PAGE 指定了映射起始的页地址，MAPPING_BYTE 指定了映射起始页中开始映射的字节地址。

用户通过将 MAPPING_PAGE 写成 >03h 的值，以及 MAPPING_CONF 写为 01b，来使能 UID 映射功能。用户必须注意 14 字节的 UID 映射不能超出用户存储空间的上限，否则映射功能无效。

取值	MAPPING_PAGE	MAPPING_BYTE
最小值	04h	00b
最大值	最大用户块-3	10b

表 3-14 UID 映射地址范围

下面的例子中，MAPPING_PAGE=0Ch，MAPPING_BYTE=01b，物理存储内容如下表：

页地址	Byte0	Byte1	Byte2	Byte3	ASCII
00h	1D	A2	30	56	
01h	11	09	67	EC	
02h	B6	internal	lock bytes		
03h					
04h					
...	...				
0Ch	3D	30	30	30	=000
0Dh	30	30	30	30	0000
0Eh	30	30	30	30	0000
0Fh	30	30	30	FE	000.
10h	00	00	00	00	...
...	...				

表 3-15 UID 映射前的物理存储空间

UID 映射后的虚拟存储空间如下表:

页地址	Byte0	Byte1	Byte2	Byte3	ASCII
00h	1D	A2	30	56	
01h	11	09	67	EC	
02h	B6	internal	lock bytes		
03h					
04h					
...	...				
0Ch	3D	31	44	41	=1DA
0Dh	32	33	30	31	2301
0Eh	31	30	39	36	1096
0Fh	37	45	43	FE	7EC.
10h	00	00	00	00	...
...	...				

表 3-16 UID 映射后的虚拟存储空间

3.4.2.3 Counter 映射

此功能可以将 3 字节 Counter 的 ASCII 码映射到芯片的物理存储空间中的特定地址，映射后需要占据 6 字节。当 READ 或者 FAST_READ 指令涉及到被映射的地址，FM11NT0X1TT 将回发 Counter 的 ASCII 码，而不是物理空间中的实际数据。

物理存储空间中被映射的目标地址可以通过 MAPPING_PAGE 和 MAPPING_BYTE 指定。其中 MAPPING_PAGE 指定了映射起始的页地址，MAPPING_BYTE 指定了映射起始页中开始映射的字节地址。

用户通过将 MAPPING_PAGE 写成 >03h 的值，以及 MAPPING_CONF 写为 10b，来使能 Counter 映射功能。用户必须注意 6 字节的 Counter 映射不能超出用户存储空间的上限，否则映射功能无效。

如果 NFC_CNT_PWD_PROT 被置位为 1，则 Counter 值处于密码保护状态下，只有进行了成功的 PWD_AUTH 操作之后，FM11NT0X1TT 才会执行 Counter 映射，否则映射功能无效。

取值	MAPPING_PAGE	MAPPING_BYTE
最小值	04h	00b
最大值	最大用户块-1	10b

表 3-17 Counter 映射地址范围

下面的例子中，MAPPING_PAGE=0Ch，MAPPING_BYTE=01b，Counter 的计数值为 00-10-2F，物理存储内容如下表:

页地址	Byte0	Byte1	Byte2	Byte3	ASCII
00h	1D	A2	30	56	
01h	11	09	67	EC	
02h	B6	internal	lock bytes		
03h					
04h					
...	...				
0Ch	3D	30	30	30	=000



页地址	Byte0	Byte1	Byte2	Byte3	ASCII
0Dh	30	30	30	FE	000.
0Eh	00	00	00	00	...
0Fh	00	00	00	00	...
10h	00	00	00	00	...
...	...				

表 3-18 Counter 映射前的物理存储空间

Counter 映射后的虚拟存储空间如下表:

页地址	Byte0	Byte1	Byte2	Byte3	ASCII
00h	1D	A2	30	56	
01h	11	09	67	EC	
02h	B6	internal	lock bytes		
03h					
04h					
...	...				
0Ch	3D	30	30	31	=001
0Dh	30	32	46	FE	02F.
0Eh	00	00	00	00	...
0Fh	00	00	00	00	...
10h	00	00	00	00	...
...	...				

表 3-19 Counter 映射后的虚拟存储空间

3.4.2.4 UID + Counter 映射

此功能可以将 7 字节 UID 和 3 字节 Counter 的 ASCII 码一同映射到芯片的物理存储空间中的特定地址，两者之间用 1 字节分隔符（“x”字符，ASCII 码 78h）分隔，因此映射后需要占据 21 字节。当 READ 或者 FAST_READ 指令涉及到被映射的地址，FM11NT0X1TT 将回发 Counter 的 ASCII 码，而不是物理空间中的实际数据。

物理存储空间中被映射的目标地址可以通过 MAPPING_PAGE 和 MAPPING_BYTE 指定。其中 MAPPING_PAGE 指定了映射起始的页地址，MAPPING_BYTE 指定了映射起始页中开始映射的字节地址。

用户通过将 MAPPING_PAGE 写成 >03h 的值，以及 MAPPING_CONF 写为 11b，来使能 Counter 映射功能。用户必须注意 21 字节的映射值不能超出用户存储空间的上限，否则映射功能无效。

如果 NFC_CNT_PWD_PROT 被置位为 1，则 Counter 值处于密码保护状态下，只有在事先进行了成功的 PWD_AUTH 操作之后，FM11NT0X1TT 才会执行 Counter 映射，否则映射功能无效。

取值	MAPPING_PAGE	MAPPING_BYTE
最小值	04h	00b
最大值	最大用户块-5	11b

表 3-20 UID + Counter 映射地址范围

下面的例子中，MAPPING_PAGE=0Ch，MAPPING_BYTE=01b，Counter 的计数值为 00-10-2F，物

理存储内容如下表:

页地址	Byte0	Byte1	Byte2	Byte3	ASCII
00h	1D	A2	30	56	
01h	11	09	67	EC	
02h	B6	internal	lock bytes		
03h					
04h					
...	...				
0Ch	3D	30	30	30	=000
0Dh	30	30	30	30	0000
0Eh	30	30	30	30	0000
0Fh	30	30	30	78	000x
10h	30	30	30	30	0000
11h	30	30	FE	00	00..
...	...				

表 3-21 映射前的物理存储空间

UID 映射后的虚拟存储空间如下表:

页地址	Byte0	Byte1	Byte2	Byte3	ASCII
00h	1D	A2	30	56	
01h	11	09	67	EC	
02h	B6	internal	lock bytes		
03h					
04h					
...	...				
0Ch	3D	31	44	41	=1DA
0Dh	32	33	30	31	2301
0Eh	31	30	39	36	1096
0Fh	37	45	43	78	7ECx
10h	30	30	31	30	0010
11h	32	46	FE	00	2F..
...	...				

表 3-22 映射后的虚拟存储空间

3.4.3 密码保护

用户可以通过使能密码保护功能来限制对特定存储器地址范围的读写访问权限。EEPROM 中保存 4 字节的密码 (PWD) 和 2 字节的密码认证响应 (PACK)，由用户自行定义并写入。

AUTHLIM 参数 (参见章节 3.2.8.2) 用于定义允许的密码尝试次数上限，芯片会自动记录 NFC 设备发起的错误密码认证次数，当错误次数超过 AUTHLIM 规定的上限后，即使 NFC 设备发送了正确的密码，也不被 FM11NT0X1TT 所接受。如果 NFC 设备在达到错误上限之前 (含错误次数等于错误上限) 发送了正确的密码，则 FM11NT0X1TT 自动清零记录的出错次数。注意密码错误次数是保存在 EEPROM 中的，并不会因为下电而清除。

在 FM11NT0X1TT 的出厂状态下，AUTH0 初始化为 FFh，即默认关闭了密码保护功能，此时用户



可以任意改写 PWD 和 PACK 的内容。当用户写入配置信息、PWD 和 PACK 之后，可以根据需要设置 AUTH0。芯片重新上电后将 EEPROM 存储区从 AUTH0 指向的页地址开始设为密码保护。用户可以通过这种方法保护配置信息、PWD、PACK 和敏感数据不被非法改写。

3.5 指令系统

3.5.1 概述

FM11NT0X1TT 支持的指令集如下表所示。

Command	ISO14443	Code
Request	REQA	26h
WakeUp	WUPA	52h
Anticollision CL1	Anticollision CL1	93h 20h
Select CL1	Select CL1	93h 70h
Anticollision CL2	Anticollision CL2	95h 20h
Select CL2	Select CL2	95h 70h
Halt	HLTA	50h 00h
GET_VERSION	-	60h
READ	-	30h
FAST_READ	-	3Ah
WRITE	-	A2h
READ_CNT	-	39h
COMP_WRITE	-	A0h
PWD_AUTH	-	1Bh
READ_SIG	-	3Ch

表 3-23 FM11NT0X1TT 指令集

FM11NT0X1TT 定义了 4bit 的 ACK 和 NAK，其编码和含义如下：

Code	ACK/NAK
4'hA	Acknowledge
4'h0	NAK, 命令参数错误
4'h1	NAK, 校验位或 CRC 错
4'h4	NAK, 非法密码认证或内部计数器溢出
4'h5	NAK, EE 写错误

表 3-24 FM11NT0X1TT ACK 和 NAK 编码

FM11NT0X1TT 定义的 ATQA 和 SAK 如下：

Response	Hex	Bit
ATQA	00 44	0000_0000_0100_0100
SAK	00	0000_0000

表 3-25 FM11NT0X1TT ATQA 和 SAK 编码

3.5.2 部分指令详细说明

3.5.2.1 READ

READ 命令只有一个字节的参数——读地址(Page Address)，最多寻址 256 页，每页占 4 字节，共计 1KB 正好占据一个 Sector。

FM11NT0X1TT 在收到 READ 命令后，在规定时间内回发页地址参数指定页开始的 16 个字节（固定回发 4 页），或者回发 NAK 响应。

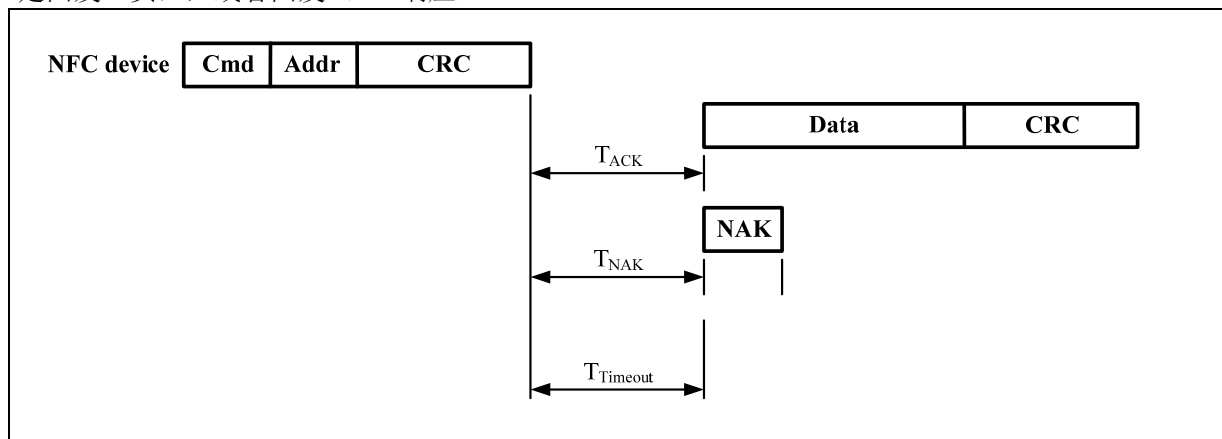


图 3-10 READ 命令

内容	编码	描述	长度
Cmd	30h	READ 命令编码	1byte
Addr	-	读取页起始地址	1byte
CRC	-	CRC 校验码	2bytes
Data	-	FM11NT0X1TT 回发的数据	16bytes
NAK	参见表 3-24	参见表 3-24	4bits

表 3-26 READ 命令

比如 Addr=03h，则 FM11NT0X1TT 回发 Page03、04、05、06 的数据。如果 Addr 位于 EE 可访问空间之外，FM11NT0X1TT 回发 NAK。如果 Addr 临近可访问 EE 的边界，则 FM11NT0X1TT 采用 roll-over 策略。比如对于 8K EE，有效地址范围是 00-E6h，若 Addr=E4h，则 FM11NT0X1TT 回发 PageE4、E5、E6、00 的数据；若 Addr>E6h，FM11NT0X1TT 回发 NAK。

出厂状态下，FM11NT0X1TT READ 命令地址有效范围如下：

FM11NT021TT: 00h~2Ch;

FM11NT041TT: 00h~86h;

FM11NT081TT: 00h~E6h;

对于启动了密码保护的情况，如果没有经过密码校验，Addr 处于被保护区域（AUTH0 设定地址之后），则 FM11NT0X1TT 回发 NAK。如果 Addr 在被保护区域边界处，FM11NT0X1TT 同样使用 roll-over 策略。比如 AUTH0==60h，Addr=59h，未过密码校验，则 FM11NT0X1TT 回发 Page59、00、01、02。一旦通过了密码校验，READ 指令行为与无密码保护情况完全一致。

出于安全考虑，无法读出 PWD 和 PACK 的真实数据。当 READ 命令的返回数据包含这两页时，PWD 和 PACK 的返回数据将会是 00h。

通信的时序特征符合 ISO14443-3 标准。

3.5.2.2 WRITE

WRITE 命令有 2 个参数：写地址（Page Address）和写入数据，写地址与 READ 命令相同，写入数据固定为 4 字节（一页），LSB 在先。FM11NT0X1TT 擦写 EE 成功后回发 ACK，否则回发 NAK。

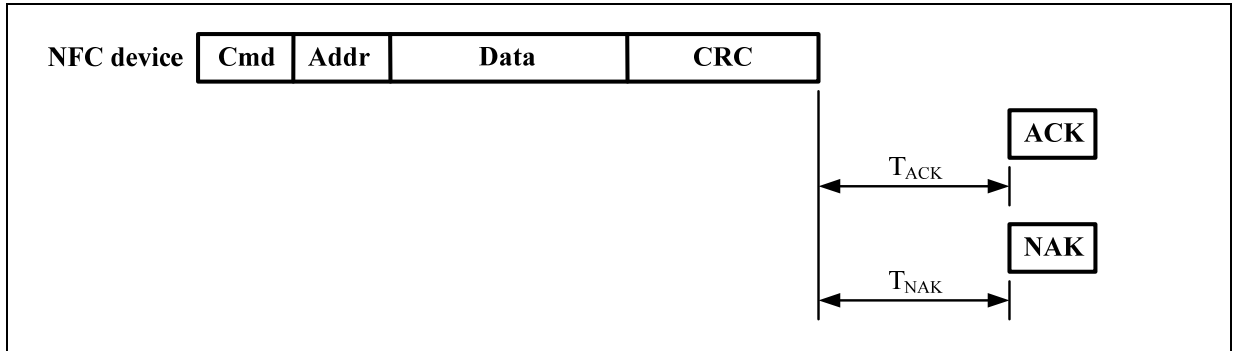


图 3-11 WRITE 命令

内容	编码	描述	长度
Cmd	A2h	WRITE 命令编码	1byte
Addr	-	写入页地址	1byte
CRC	-	CRC 校验码	2bytes
Data	-	FM11NT0X1TT 收到的数据	4bytes
ACK/NAK	参见表 3-24	参见表 3-24	4bits

表 3-27 WRITE 命令

FM11NT0X1TT WRITE 命令地址有效范围如下，写地址超出地址有效范围将回发 NAK：

FM11NT021TT: 00h~2Ch;

FM11NT041TT: 00h~86h;

FM11NT081TT: 00h~E6h;

3.5.2.3 GET_VERSION

GET_VERSION 指令用于获得芯片的详细型号和版本信息。

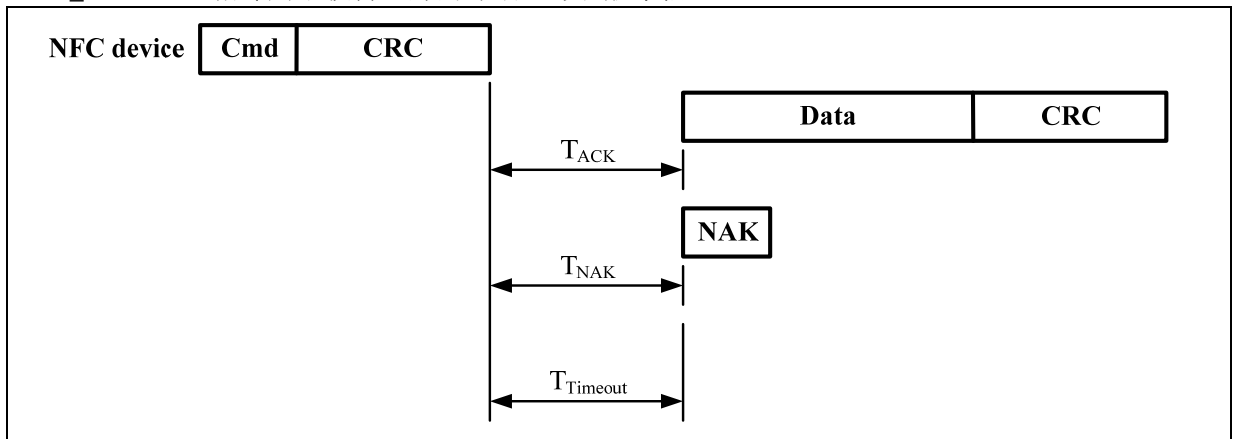


图 3-12 GET_VERSION 命令

内容	编码	描述	长度
Cmd	60h	GET_VERSION 命令编码	1byte
CRC	-	CRC 校验码	2bytes
Data	-	FM11NT0X1TT 回发的数据	8bytes

内容	编码	描述	长度
NAK	参见表 3-24	参见表 3-24	4bits

表 3-28 GET_VERSION 命令

GET_VERSION 回发信息说明:

Byte No.	描述	FM11NT021T T	FM11NT041 TT	FM11NT081 TT	含义
0	Header	00h	00h	00h	固定
1	Vendor ID	1Dh	1Dh	1Dh	FMSH
2	Product Type	04h	04h	04h	NTAG
3	Product Subtype	01h	01h	01h	50pF
4	Major Version	01h	01h	01h	1
5	Minor Version	00h	00h	00h	V0
6	Storage Size	0Fh	11h	13h	存储容量
7	Protocol Type	03h	03h	03h	支持 ISO14443-3

表 3-29 GET_VERSION 回发信息

存储容量 (Storage Size) 数据长 1 个字节, 该字节定义了可用数据存储区的大小。Storage Size 的 Bit7~Bit1 表示一个无符号整数 n , FM11NT0X1TT 用户数据存储区的大小至少为 2^n 个字节。如果 Bit0 为 0, 那么 FM11NT0X1TT 可用数据存储区的大小就为 2^n 个字节。如果 Bit0 为 1, 那么 FM11NT0X1TT 可用数据存储区的大小在 2^n 和 2^{n+1} 个字节之间。

比如, 对于 FM11NT021TT, 可用数据存储区为 144 字节, 介于 128 字节和 256 字节之间。因此 Storage Size 的 Bit7~Bit1 为 07h, Bit0 为 1。这样 FM11NT021TT 的 Storage Size 字节就为 0Fh。FM11NT041TT 和 FM11NT081TT 的 Storage Size 数据也是同样的含义。

3.5.2.4 FAST_READ

FAST_READ 命令可以用来从 FM11NT0X1TT 连续读取 N 个 Page 的数据, 命令参数包含起始页地址和结束页地址, 不限制回发数据长度。

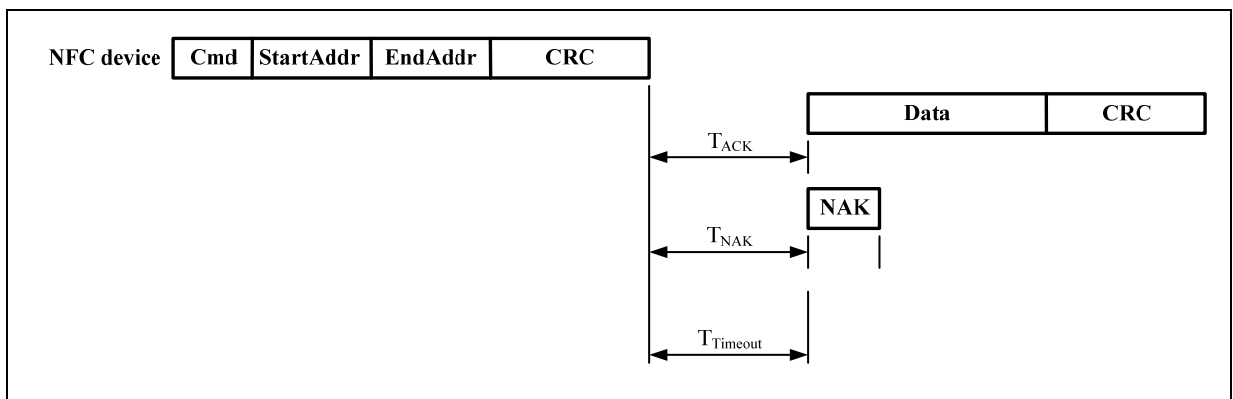


图 3-13 FAST_READ 命令

内容	编码	描述	长度
Cmd	3Ah	FAST_READ 命令编码	1byte
StartAddr	-	起始页地址	1byte
EndAddr	-	结束页地址	1byte
CRC	-	CRC 校验码	2bytes

内容	编码	描述	长度
Data	-	FM11NT0X1TT 收到的数据	n*4bytes
NAK	参见表 3-24	参见表 3-24	4bits

表 3-30 FAST_READ 命令

假设 StartAddr==03h, EndAddr==07h, 则 FM11NT0X1TT 回发 Page03、04、05、06、07 的数据。EndAddr 必须大于或等于 StartAddr。如果 EndAddr 小于 StartAddr, 则 FM11NT0X1TT 回发 NAK。如果 EndAddr 等于 StartAddr, 则 FAST_READ 命令等同于 READ 命令。如果被寻址的页超出了 EE 物理配置空间, 则 FM11NT0X1TT 回发 NAK。在没有通过密码校验的情况下, 如果读取区域包含被密码保护的区域, FM11NT0X1TT 回发 NAK。

3.5.2.5 COMPATIBILITY_WRITE

COMPATIBILITY_WRITE 命令分 2 部分, 第一部分先给出写地址, 第二部分给出 16 字节写数据, 但是只有最低 4 字节数据会被写入, 由于数据传输时 LSB 在先, 所以是先发的 4 字节被写入目标块, 后续 12 字节数据忽略。

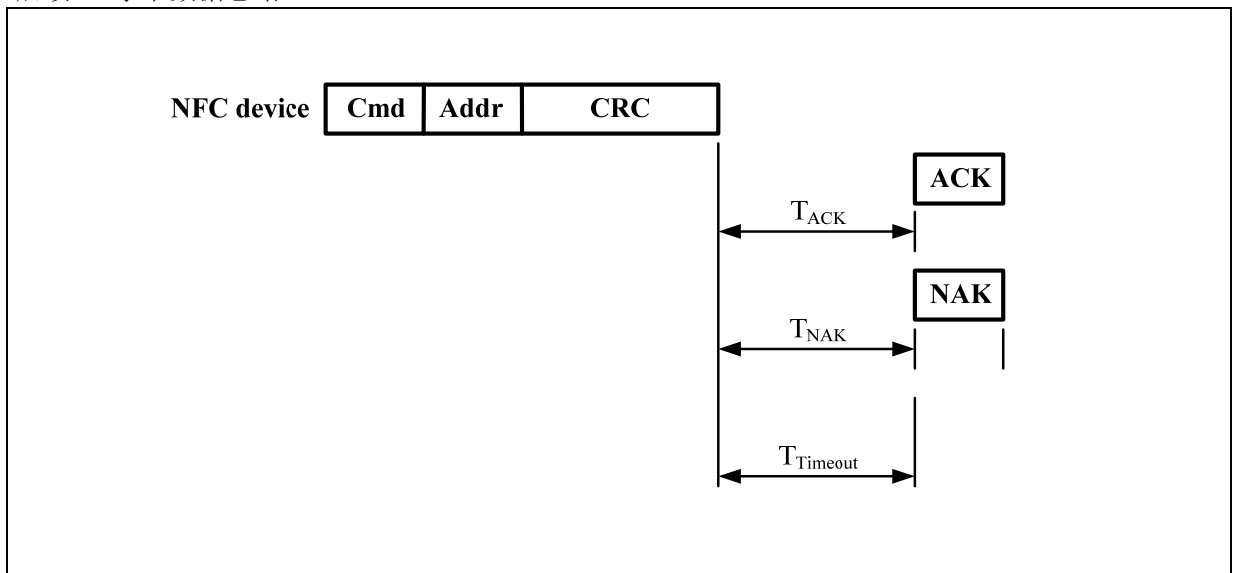


图 3-14 COMPATIBILITY_WRITE 命令第一部分

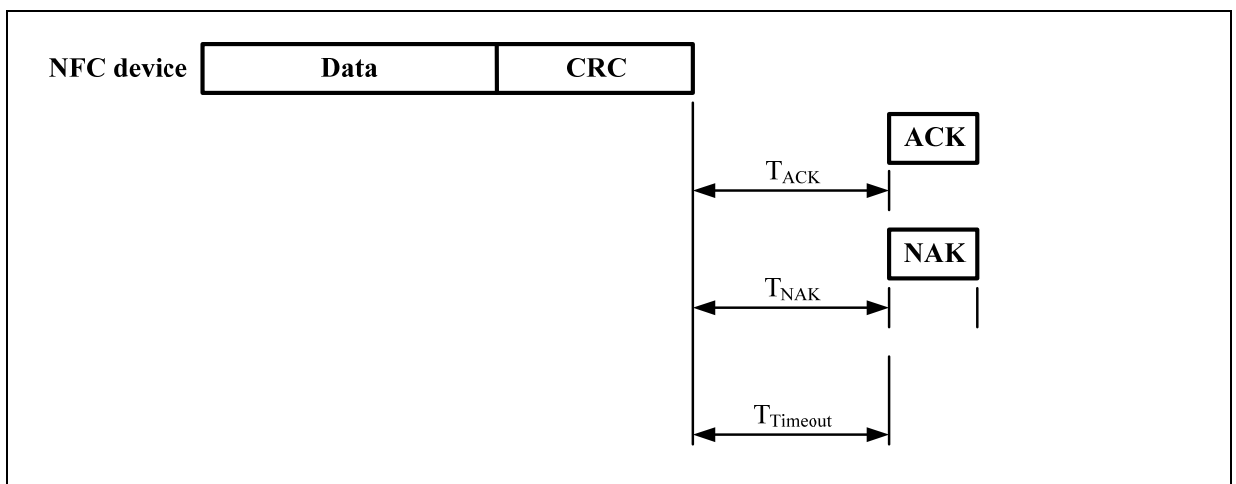


图 3-15 COMPATIBILITY_WRITE 命令第二部分

内容	编码	描述	长度
Cmd	A2h	COMPATIBILITY_WRITE 命令编码	1byte
Addr	-	起始页地址	1byte
CRC	-	CRC 校验码	2bytes
Data	-	FM11NT0X1TT 收到的数据	4bytes
ACK/NAK	参见表 3-24	参见表 3-24	4bits

表 3-31 COMPATIBILITY_WRITE 命令

COMPATIBILITY_WRITE 命令合法地址范围:

- FM11NT021TT: 块地址 00h-2Ch
- FM11NT041TT: 块地址 00h-86h
- FM11NT081TT: 块地址 00h-E6h

当命令地址超出以上范围时, 芯片回发 NAK。

3.5.2.6 PWD_AUTH

PWD_AUTH 命令用于密码验证, 当 NFC 设备试图访问被密码保护的区域(页地址大于等于 AUTH0) 时, 必须首先使用 PWD_AUTH 命令发送正确的密码。密码由用户预先写入 EEPROM。如果密码匹配成功, FM11NT0X1TT 会回发密码认证响应 PACK, 否则回发 NAK。为了防止暴力破解, 用户可以设置 AUTHLIM 来限制错误密码认证的次数上限, 当 NFC 设备发送错误密码次数超过 AUTHLIM 规定的上限之后, FM11NT0X1TT 受密码保护的区域将永远无法访问(根据密码访问配置), 后续发送的任何 PWD_AUTH 命令, 即使密码正确, FM11NT0X1TT 也会回发 NAK。

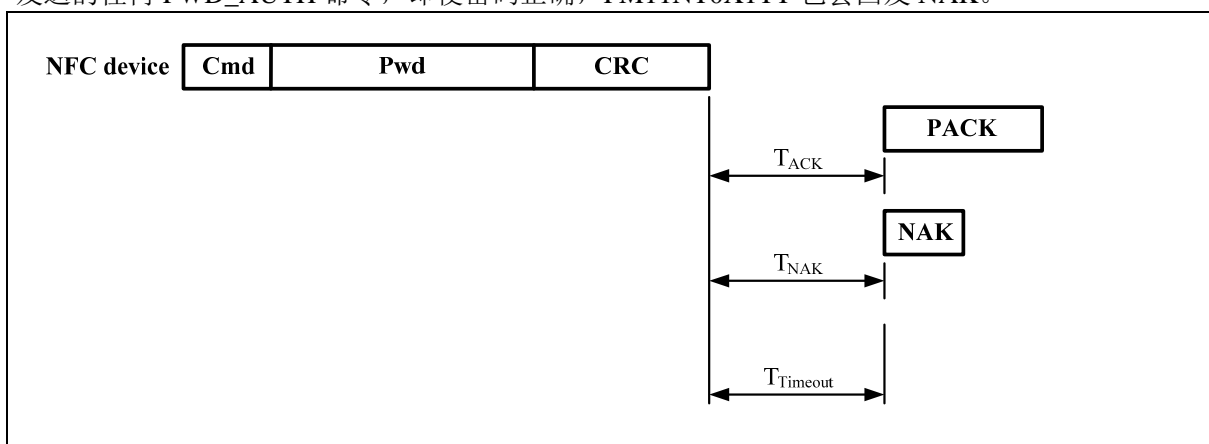


图 3-16 PWD_AUTH 命令

内容	编码	描述	长度
Cmd	1Bh	PWD_AUTH 命令编码	1byte
Pwd	-	密码	4bytes
CRC	-	CRC 校验码	2bytes
PACK	-	密码认证响应	2bytes
NAK	参见表 3-24	参见表 3-24	4bits

表 3-32 PWD_AUTH 命令

3.5.2.7 READ_SIG

READ_SIG 为原厂验签命令, FM11NT0X1TT 收到 READ_SIG 后自动回发 32 字节原厂签名数据, 此签名在出厂时写入 EEPROM, 用户不可改写。签名根据加密算法生成, 每颗芯片都有唯一的签名,

用户可通过此命令来实现简单的防伪功能。

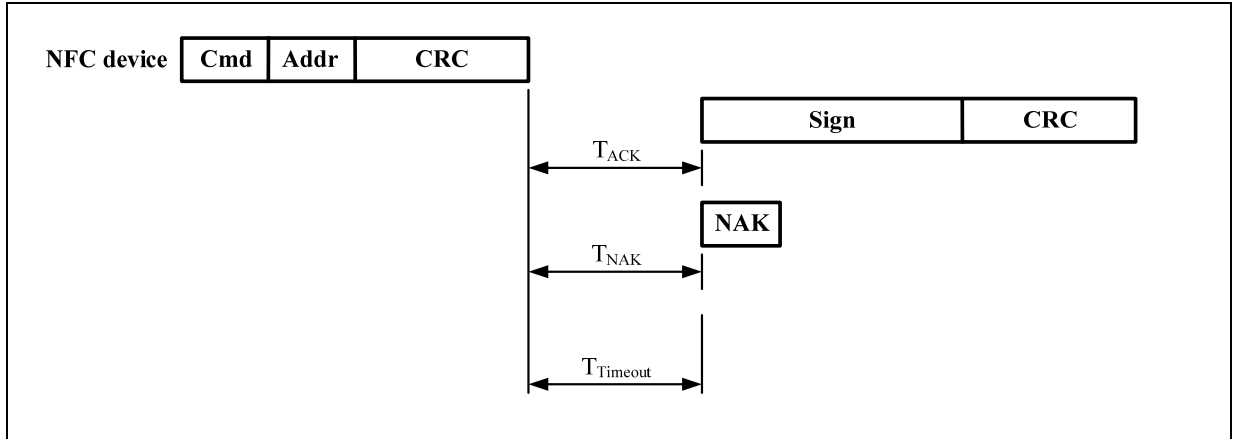


图 3-17 READ_SIG 命令

内容	编码	描述	长度
Cmd	3Ch	READ_SIG 命令编码	1byte
Addr	00h	RFU, 固定为 00h	1byte
CRC	-	CRC 校验码	2bytes
Sign	-	签名数据	32bytes
NAK	参见表 3-24	参见表 3-24	4bits

表 3-33 READ_SIG 命令

3.5.2.8 READ_CNT

READ_CNT 命令用于读出 FM11NT0X1TT 内建的 Counter 计数器的值。READ_CNT 命令包含一个固定的地址参数 02h (Addr)。如果 Counter 启用了密码保护 (NFC_CNT_PWD_PROT 设置为 1)，那么只有当密码校验通过后，READ_CNT 命令才能正确返回 Counter 的值。

FM11NT0X1TT 在收到 READ_CNT 命令后，在规定时间内回发 3 字节 Counter 计数器的值，或者回发 NAK 响应。如果 READ_CNT 命令的地址参数不是 02h，那么 FM11NT0X1TT 在收到 READ_CNT 命令后回发 NAK。如果 Counter 启用了密码保护，但是未经过密码校验认证，那么 FM11NT0X1TT 在收到 READ_CNT 命令后回发 NAK。

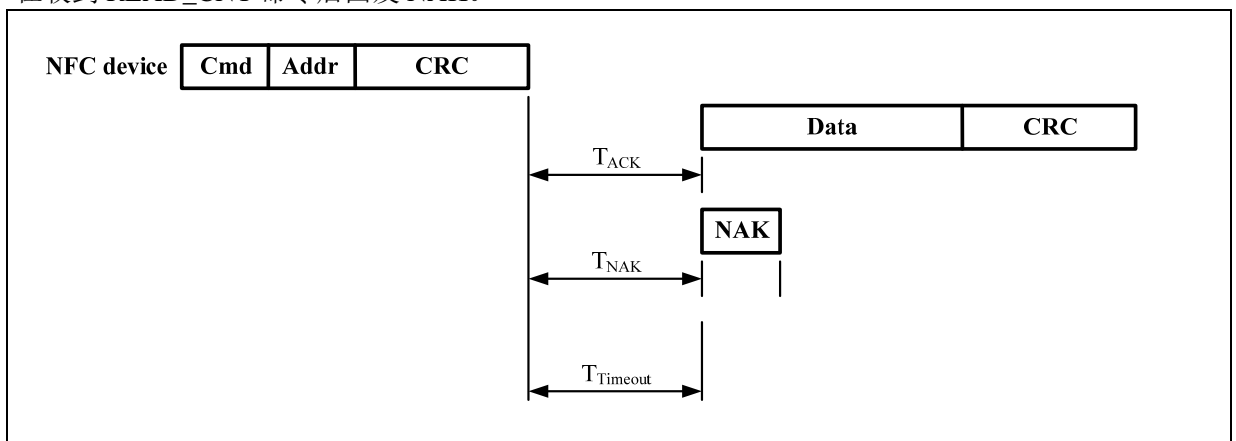


图 3-18 READ_CNT 命令

内容	编码	描述	长度
Cmd	39h	READ_CNT 命令编码	1byte

内容	编码	描述	长度
Addr	02h	Counter 地址	1byte
CRC	-	CRC 校验码	2bytes
Data	-	Counter 计数值	3bytes
NAK	参见表 3-24	参见表 3-24	4bits

表 3-34 READ_CNT 命令

4 电气参数

4.1 极限额定参数

参数	最小值	最大值	单位
存储温度	-55	+125	°C
最大输入电流 (IN1 对 IN2; 峰值)	-	±30	mA
ESD (HBM) 【2】	-	±4	KV

表 4-1 FM11NT0X1TT 极限额定参数【1】

*注【1】：如果外加条件超过“极限额定参数”的额定值，将会对芯片造成永久性的破坏。

*注【2】：ESD 测试用 CDIP8 封装完成。

4.2 推荐工作条件

符号	参数	条件	最小值	典型值	最大值	单位
T _A	工作温度		-40	+25	+85	°C
H _A	天线场强		1.5		7.5	A/M

表 4-2 FM11NT0X1TT 推荐工作条件

4.3 电参数

符号	参数	条件	最小值	典型值	最大值	单位
f _i	输入频率	【1】	13.553	13.56	13.567	MHz
C _i	输入谐振电容【2】	IN1 和 IN2 之间		50		pF

表 4-3 电参数

注【1】：频宽依据 ISM 频段规定

注【2】：用 Agilent E5061B 在 13.56MHz 和 0.707V RMS 电压下测得



4.4 存储器参数

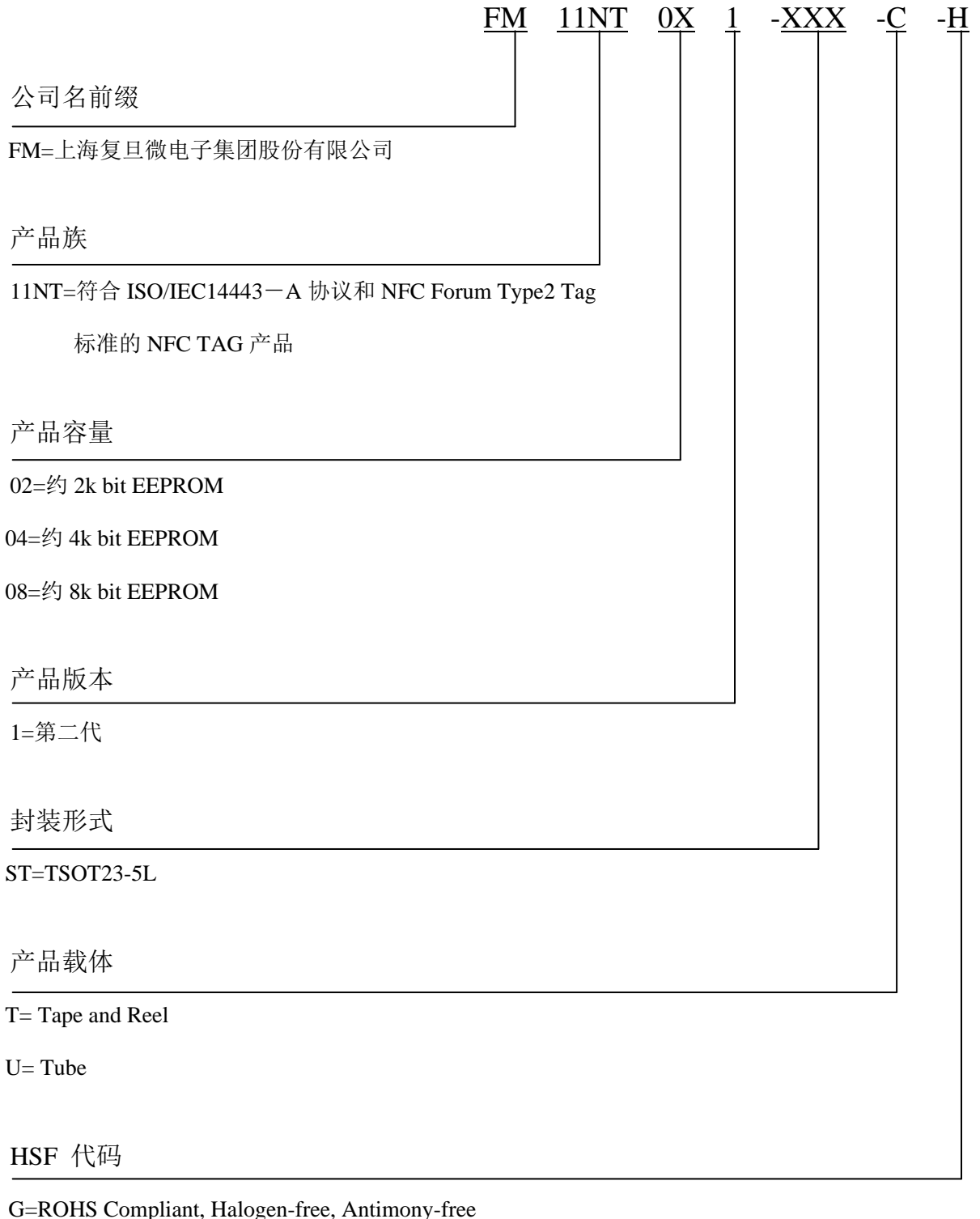
符号	参数	条件	最小值	典型值	最大值	单位
t_{ret}	数据保存时间	环境温度 55°C	10			年
$N_{endu(W)}$	擦写次数	环境温度 25°C	100			万次

表 4-4 存储器参数



5 订货信息

器件代号	封装形式	包装方式
FM11NT0X1TT-ST-T-G	TSOT23-5 塑封	卷带包装
FM11NT0X1TT-WIB2	凸点晶圆	8 英寸凸点晶圆 (120um 芯片厚度)
FM11NT0X1TT-WIS2	减划晶圆	8 英寸减薄划片晶圆 (120um 芯片厚度)



6 封装信息

6.1 TSOT 封装

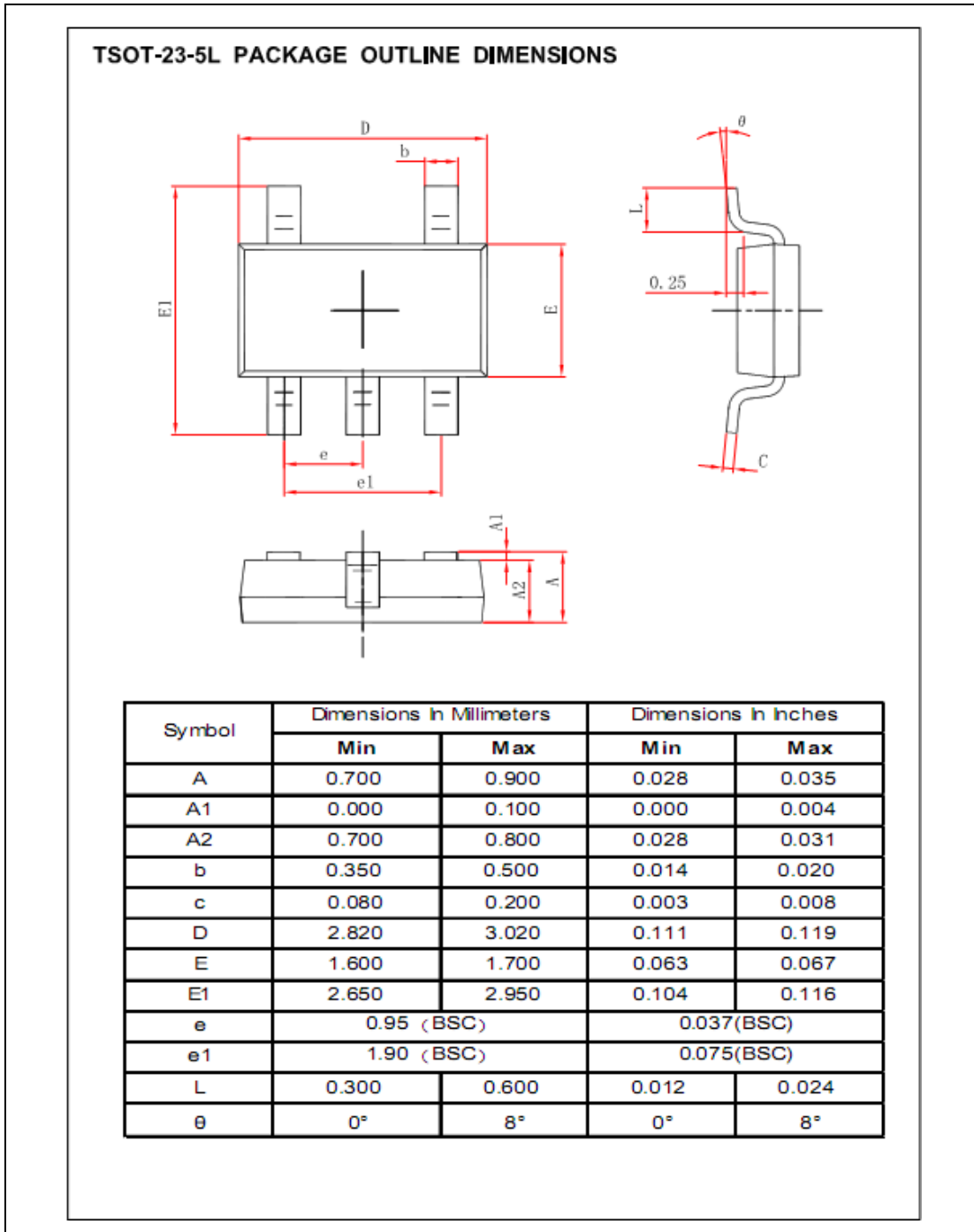


图 6-1 TSOT23-5L 封装尺寸图



版本信息

版本号	发布日期	页数	章节或图表	更改说明
0.1	2018.7	35		初始版本，未来一些具体参数可能会有更新。



上海复旦微电子集团股份有限公司销售及服 务网 点

上海复旦微电子集团股份有限公司

地址：上海市国泰路 127 号 4 号楼

邮编：200433

电话：(86-021) 6565 5050

传真：(86-021) 6565 9115

上海复旦微电子（香港）股份有限公司

地址：香港九龙尖沙咀东嘉连威老道 98 号东海商业中心 5 楼 506 室

电话：(852) 2116 3288 2116 3338

传真：(852) 2116 0882

北京办事处

地址：北京市东城区东直门北小街青龙胡同 1 号歌华大厦 B 座 423 室

邮编：100007

电话：(86-10) 8418 6608

传真：(86-10) 8418 6211

深圳办事处

地址：深圳市华强北路 4002 号圣廷苑酒店世纪楼 1301 室

邮编：518028

电话：(86-0755) 8335 0911 8335 1011 8335 2011 8335 0611

传真：(86-0755) 8335 9011

台湾办事处

地址：台北市 114 内湖区内湖路一段 252 号 12 楼 1225 室

电话：(886-2) 7721 1889

传真：(886-2) 7722 3888

新加坡办事处

地址：237, Alexandra Road, #07-01, The Alexcier, Singapore 159929

电话：(65) 6472 3688

传真：(65) 6472 3669

北美办事处

地址：2490 W. Ray Road Suite#2 Chandler, AZ 85224 USA

电话：(480) 857-6500 ext 18

公司网址：<http://www.fmsk.com/>