NFC ISO14443-TypeA

什么是NFC

NFC（Near Field Communication）的工作原理基于射频识别（RFID）技术，它利用电磁感应来实现设备之间的近场通信。

NFC设备一般由两个主要部分组成：读取器（读写器）和标签（被动设备）。当两个支持NFC的设备靠近时，它们之间会建立一个无线连接。这需要设备之间的天线相互靠近，并且处于接近距离（通常在10厘米范围内），以便进行高效的通信。

NFC使用13.56 MHz的频率进行通信。当设备与标签靠近时，读取器会发送一个电磁场到标签。标签中的天线接收到这个电磁场后，产生电流并回传给读取器。这种方法被称为感应耦合。

NFC的模式

1. **读取器/写入器模式（Reader/Writer Mode）**：在这种模式下，一个设备作为读取器或写入器，可以与被动设备（例如智能卡、标签等）进行通信。读取器/写入器设备可以向被动设备发送指令或数据，以读取信息或写入数据到被动设备中。
2. **卡模拟模式（Card Emulation Mode）**：在这种模式下，一个设备模拟成一个被动设备，例如智能卡或标签。其他读取器/写入器设备可以通过NFC与该设备进行通信，并像与实际智能卡进行交互一样读取或写入数据。在这种模式下，设备可以用作门禁卡、公交卡或银行卡的替代品。
3. **点对点模式（Peer-to-Peer Mode）**：在这种模式下，两个NFC设备可以直接进行通信，彼此之间没有读取器或写入器的角色限制。这种模式可用于快速传输文件、交换联系人信息、启动应用程序等。在点对点模式下，每个设备都可以同时扮演读取器和标签的角色。

NFC的协议

1. **ISO 14443 A/B：**
   - ISO 14443A：该协议使用13.56 MHz 高频范围内的载波调制技术，支持防冲突算法、命令传输、数据加密等功能。ISO 14443A 是最广泛应用的 NFC 协议之一，但通信距离较短，一般为几厘米。

- ISO 14443B：该协议也使用13.56 MHz 高频范围，但采用幅度调制技术。相比于 ISO 14443A，ISO 14443B 具有更高的通信速率和更大的通信距离，最高可达到十几厘米。

2. **ISO 18092：**

   ISO 18092 支持点对点模式和读写器/写入器模式，使得两个 NFC 设备可以直接交换数据并共享资源。广泛应用于移动支付、联系人信息交换、文件传输等需要设备直接通信的场景。

3. **FeliCa：**

   FeliCa 是由索尼公司开发的一种非接触式 IC 卡技术，也是 NFC 中的一种协议。FeliCa 在 13.56 MHz 高频范围内进行通信，具有较快的数据传输速度和较大的存储容量。主要在日本广泛应用于移动支付、公共交通卡等领域。

4. **ISO 15693：**

   ISO 15693 是一种非接触式射频识别（RFID）协议，也被广泛应用于 NFC 技术中。它定义了在 13.56 MHz 高频范围内的通信规范。ISO 15693 支持读写器与标签之间的双向通信，标签可以主动响应读取器的请求，并提供数据或执行特定操作。ISO 15693 标签允许比其他 NFC 标准更大的通信距离，最高可达到 1-1.5 米。ISO 15693 支持较快的数据传输速度，通常为 26 kbps 或更高。

符号缩略语

符号	缩略语
ACK	肯定确认
NAK	否定确认
ATQA	请求应答，类型A
REQA	请求命令，类型A
HALT	PICC暂停命令，类型A
WUPA	PICC唤醒命令，类型A
PCD	接近式耦合设备（读写器）
PICC	接近式卡
SEL	选择命令
UID	唯一标识符
NVB	有效位的数目

名词解释

UID唯一标识符

NFC的UID是一个由制造商分配给每个NFC设备的独特编号。它类似于设备的序列号，用于区分不同的NFC设备。UID通常是一个16进制数字，长度可以根据设备类型和制造商的规范而异。当进行NFC通信时，读取器或其他NFC设备可以通过读取目标设备的UID来确定其身份。这样可以实现诸如数据交换、支付、门禁控制等功能。例如，当将两个支持NFC的智能手机靠近时，它们可以通过互相交换UID来建立通信连接。需要注意的是，NFC的UID并不是可编程或可更改的。它由设备制造商在生产过程中写入设备的芯片中，并且在设备的整个生命周期中保持不变。

SELECT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。

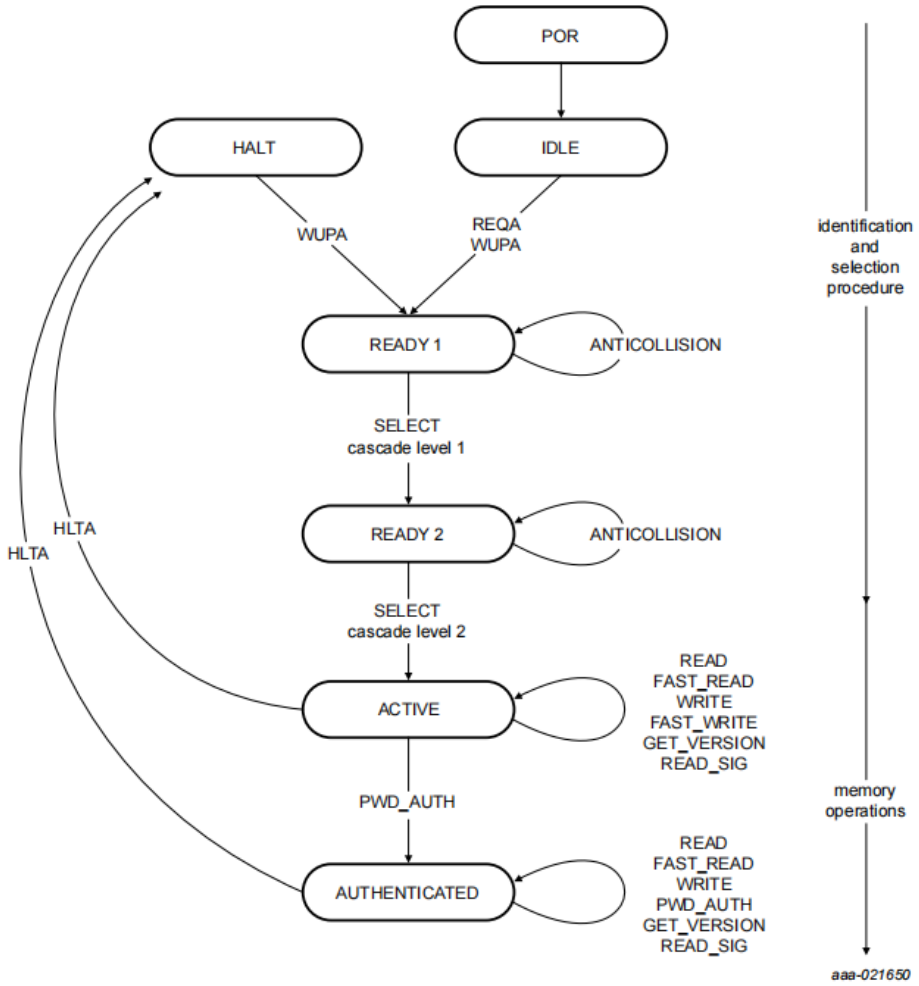
ANTICOLLISION防冲突

ANTICOLLISION（防冲突）是一种在RFID（Radio Frequency Identification，射频识别）系统中使用的技术，用于解决多个标签同时被读取时可能发生的冲突问题。在RFID系统中，当多个标签处于读取范围内时，它们可能会同时响应读取器的指令，导致数据混乱或无法准确识别每个标签。

AUTH认证

NFC认证（Near Field Communication Authentication）是指通过近场通信技术对NFC设备或实体的身份或真实性进行验证的过程。它确保只有授权的设备才能交换敏感信息或执行特定操作。NFC认证在安全的非接触式交易、移动支付、门禁系统和其他涉及敏感数据交换的应用中起着至关重要的作用。实施适当的认证措施有助于防止未经授权的访问、保护用户隐私，并确保NFC交易的完整性。

PICC状态机-基于NT3H(ISOTypeA)



- **POWER-OFF状态**

  在POWER-OFF状态中，由于缺少载波能量，PICC不能被激励并且应不发射副载波。

- **IDLE状态**

  最大延迟内激活工作场后，PICC应进入其IDLE状态。在这种状态中，PICC被加电，并且能够解调和识别从PCD来的有效REQA和WUPA命令。

- **READY状态**

一旦收到有效REQA或WUPA报文则立即进入该状态，用其UID选择了PICC时则退出该状态并直接进入ACTIVE状态。在这种状态中，比特帧防冲突或其他任选的防冲突方法都可以使用。所有串联级别都在这一状态内处理以取得所有UID CLn。

- **ACTIVE状态**

  通过使用其完整UID选择PICC来进入该状态。

- **AUTHENTICATED状态**

  在ACTIVE状态下，PICC接收到AUTH命令且校验密钥成功后，进入AUTH状态，此时PCD设备可访问加密区域并且修改现有密钥。

- **HALT状态**

  使用HALT命令来进入HALT状态。在这种状态中，PICC应仅响应使PICC转换为READY状态的WUPA命令。处于HALT状态的PICC将不参与任何进一步的通信，除非使用了WUPA命令。

防冲突-选择级联流程

当PICC处于READY状态时，需要执行以下步骤，使PICC正常进入ACTIVE状态，每执行一次防冲突流程可读取4字节数据，NT3H2211的UID为7字节，需执行两次

1. 读取器发送一个命令给附近的所有标签。
2. 所有标签接收到命令后，生成一个随机数，用作其UID。
3. 标签按照一定顺序（通常是随机选择）将其UID发送回读取器。
4. 读取器接收到标签的UID后，会进行校验和比较。
5. 如果读取器检测到冲突（即两个或多个标签的标识符相同），它将发送一个冲突解决命令给所有冲突的标签。
6. 冲突的标签会再次生成新的UID，并将其发送回读取器。
7. 这个过程不断重复，直到所有标签都被成功识别并没有冲突。

访问加密区域

当PICC处于ACTIVE状态时，PCD可以发送AUTH命令，获取访问加密区域的权限

以NT3H2211的卡模式为例：

由PICC设备定义的加密区域为(AUTH0)---(E1)，访问前需发送AUTH命令，命令中携带4字节密钥，在获取权限后，可通过访问区域(E5)读取或修改现有密钥

Table 40. Illustration of the SRAM memory addressing via the NFC interface in pass-through mode (PTHRU_ON_OFF set to 1b) for the NTAG I²C *plus* 2k

Sector address	Page address		Byte number within a page				Access cond. ACTIVE state	Access cond. AUTH. state
	Dec.	Hex.	0	1	2	3		
0	0	00h	Serial number (UID)				READ	
	1	01h	Serial number (UID)			Internal	READ	
	2	02h	Internal		Static lock bytes		READ/R&W	
	3	03h	Capability Container (CC)				READ&WRITE	
	4	04h	Unprotected user memory				READ&WRITE	
	...	...						
	AUTH0	AUTH0	Protected user memory				READ	READ&WRITE
	...	...						
	225	E1h						
	226	E2h	Dynamic lock bytes			00h	R&W/READ	
	227	E3h	RFU	RFU	RFU	AUTH0	READ	READ&WRITE
	228	E4h	ACCESS	RFU	RFU	RFU	READ	READ&WRITE
	229	E5h	PWD				READ	READ&WRITE

P2P读写

当PICC处于ACTIVE状态时，PCD可以发送W/R命令，访问指定区域

以NT3H2211的透传模式为例：

由硬件设备定义的透传区域为(F0)---(FF)，每个区域大小为4字节，PCD设备与PICC设备每次可透传64字节的数据，且必须透传64字节。

在发送方填满SRAM区域之后，NT3H会产生信号，接收方需将SRAM中的数据取走后，才能继续透传写入SRAM，否则将被视为错误命令。

Table 40. Illustration of the SRAM memory addressing via the NFC interface in pass-through mode (PTHRU_ON_OFF set to 1b) for the NTAG I²C *plus* 2k...*continued*

Sector address	Page address		Byte number within a page				Access cond. ACTIVE state	Access cond. AUTH. state
	Dec.	Hex.	0	1	2	3		
	230	E6h	PACK		RFU	RFU	READ	READ&WRITE
	231	E7h	PT_I2C	RFU	RFU	RFU	READ	READ&WRITE
	232	E8h	Configuration registers				see Table 11	
	233	E9h						
	234	EAh	Invalid access - returns NAK				n.a.	
	235	EBh						
	236	ECh	Session registers				see Table 12	
	237	EDh						
	238	EEh	Invalid access - returns NAK				n.a.	
	239	EFh						
	240	F0h	SRAM				READ&WRITE	
	...	...						
	255	FFh						
1	0	00h	(Un-)protected user memory				READ&WRITE	
	...	...						
	255	FFh						
2	...	...	Invalid access - returns NAK				n.a.	
3	0	00h	Invalid access - returns NAK				n.a.	
	...	...						
	248	F8h	Session registers				see Table 12	
	249	F9h						
	...	...	Invalid access - returns NAK				n.a.	
	255	FFh						

防错误机制

当PCD发送至PICC的某个命令存在错误，例如AUTH校验失败、写失败等，或接收到未知命令，PICC会立即回到HALT或IDLE状态。PCD设备要继续访问PICC，必须重新执行防冲突-选择级联流程，使PICC正常进入ACTIVE状态。

参考文章

【IoT】NFC ISO14443A 协议解析_nfc fdt帧延时时间-CSDN博客