超高频 RFID 协议介绍

协议介绍

射频识别空中接口协议规定了相关频段射频识别系统空中接口的物理层和没提访问控制层参数以及协议工作方式。

适用于对应频段射频识别系统标签和读写器的设计、生产、测试和使用。

目前，中国主要的超高频 RFID 协议有 EPC、GB、GJB 三种。

EPC 协议

由 GS1（Globe standard 1）的附属组织 EPCglobal 发布。

EPC 是电子产品代码（Electronic Product Code）的简称。超高频 RFID 空中接口协议主要经历如下变化：

- 2004 年 EPCglobal 提出初版 EPC Gen2 协议标准
- 2005 年 EPC 协议被收入 ISO/IEC 18000-6C 标准
- 2008 年 EPCglobal 发布 EPC Gen2 v1.2.0 版
- 2013 年 Gen2v2 协议签订
- 2014 年 Gen2v2 协议收入 ISO/IEC 18000-63 标准

考虑到协议存在继承关系，而且目前大量标签并未采用最新标准。故本文用 EPC 指代 EPCglobal 组织提出的空中接口协议。

GJB 协议

由中国人民解放军总装备部批准。

GJB 是国家军用标准简称。军用超高频射频识别空中接口标准为 GJB 7377.1-2011。2011 年 9 月 6 日发布，2011 年 10 月 1 日实施。

本文用 GJB 指代 GJB 7377.1-2011。

GB 协议

由中国国家标准化管理委员会发布。

GB 是国家标准简称。超高频射频识别空中接口标准为 GB/T 29768-2013。2013 年 9 月 18 日发布，2014 年 5 月 1 日实施。

本文用 GB 指代 GB/T 29768-2013。

协议异同

下表简单列举了三种不同协议的主要异同。

表 1　　协议的主要异同

项目	EPC	GJB	GB
通信相关			

调制方式	SSB-ASK / DSB-ASK / PR-ASK	SSB-ASK / DSB-ASK	SSB-ASK / DSB-ASK
R-T 编码[1]	PIE（脉冲宽度编码）	TPP（截断式脉冲位置编码）	TPP（截断式脉冲位置编码）
T-R 编码[2]	FM0 / MILLER	FM0 / MILLER	FM0 / MILLER
T-R 前导[3]	1010V1（FM0） 010111（MILLER）	1110V00V（FM0） 00111101（MILLER）	1110V00V（FM0） 00111101（MILLER）
下行速率	40kHz - 160kHz	40kHz - 80kHz	40kHz - 80kHz
上行速率	40kHz - 640kHz （和下行速率有关）	80kHz - 640kHz （和下行速率有关）	64kHz - 640kHz （和下行速率无关）
应用相关			
会话标识	4 个	1 个	4 个
用户区	0 或 1 个	0-1 个（可自定义扩展）	0-15 个子区
访问口令	32bits	读取、写入各 32bits	每个子区独立读取、写入各 32bits
锁定口令	和访问口令相同	32bits	32bits
灭活口令	32bits	32bits	32bits
安全通信	不支持	支持	支持
句柄	RN16	RN11+CRC5	RN11+CRC5

说明：

[1] 读写器到标签的编码方式

[2] 标签应答读写器的编码方式

[3] 标签应答读写器的固定前导符号，“V”表示不符合 FM0 编码规则的符号

物理层介绍

下行编码

下行编码指读写器发送给标签的空中接口命令编码。EPC 协议为 PIE 编码（脉冲宽度编码），GB 和 GJB 协议为 TPP 编码（截断式脉冲位置编码）。

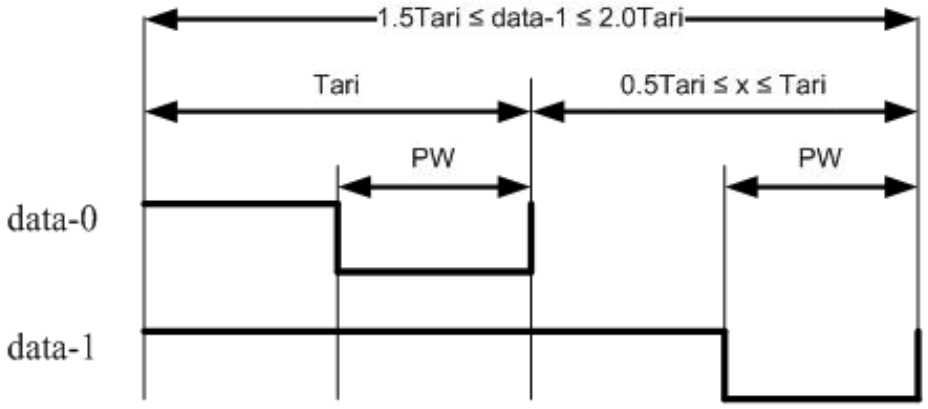


图 1　　PIE 编码

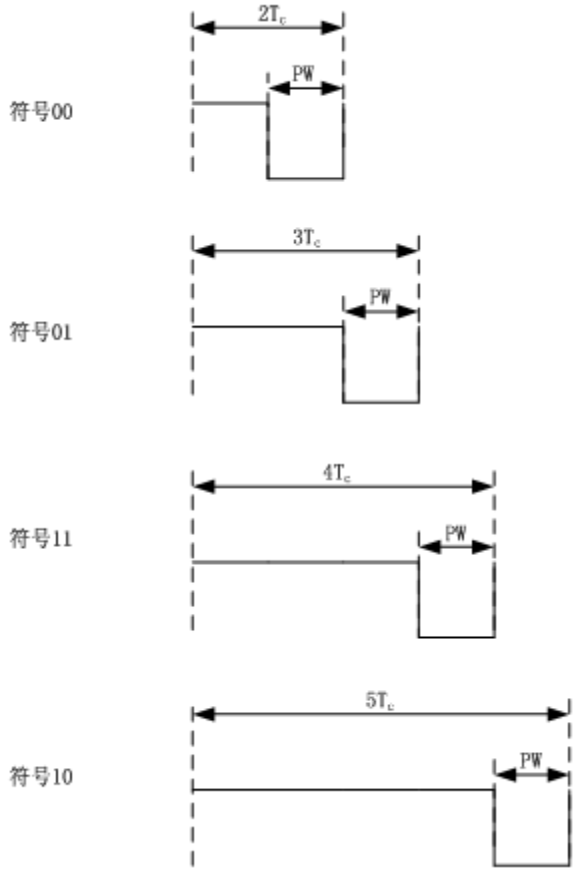


图 2　　TPP 编码

从上图可以发现两种编码方式的不同，PIE 编码一个符号表示 1 个比特数据，TPP 编码一个符号表示 2 个比特数据。

下行编码方式的不同是 EPC 协议和 GJB、GB 协议的重大区别之一。许多支持 EPC 协议的读写器方案，都是基于 PIE 编码设计和实现的，难以快速切换到 TPP 编码，这也是目前支持 GJB 和 GB 协议读写器不多的原因之一。

下行前导码

在读写器给标签发送实际命令之前，需要先发送前导码。

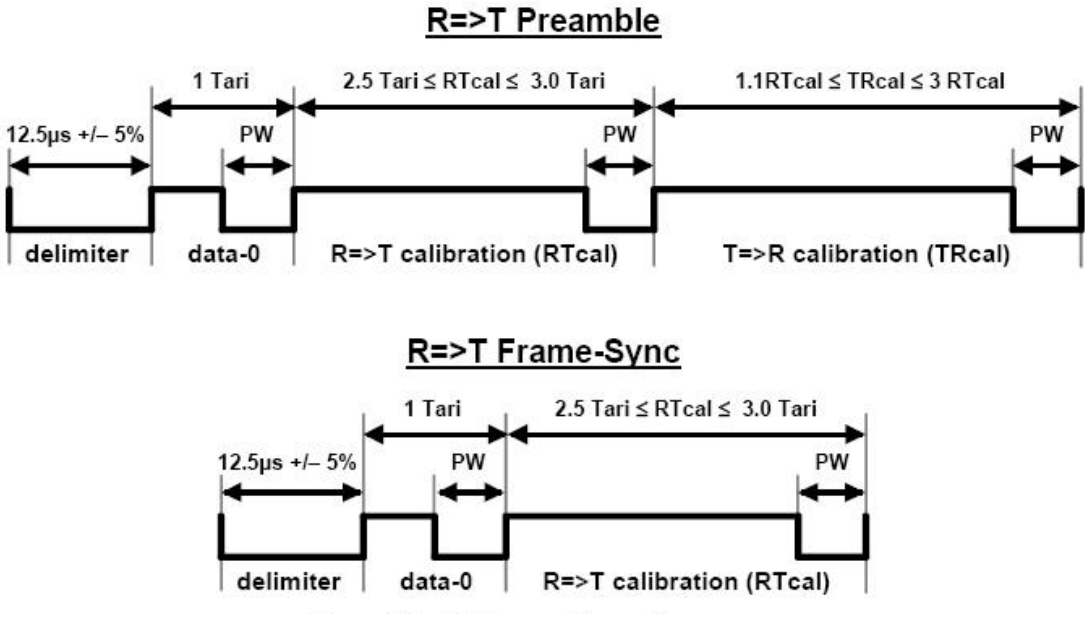


图 3　　EPC 协议下行前导码

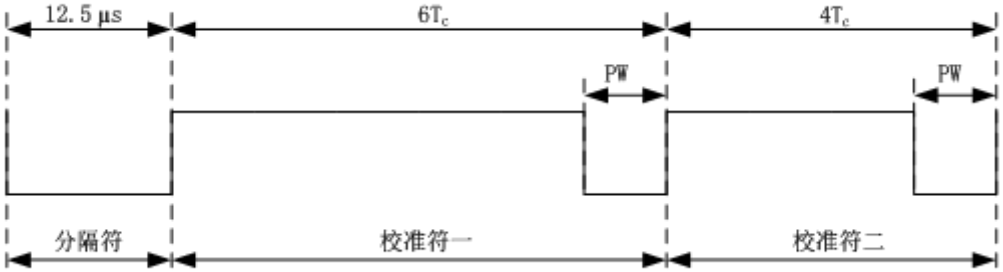


图 4　　GJB 协议下行前导码

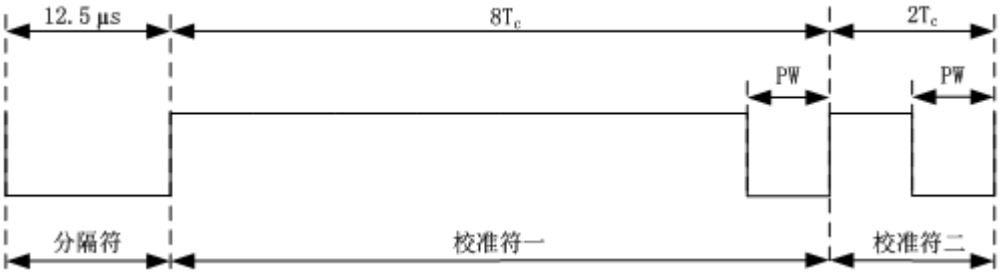


图 5　　GB 协议下行前导码

上行编码

上行编码指标签发送给读写器的空中接口命令应答编码，有两种编码格式，FM0 和 MILLER 编码。

FM0 编码如下图所示。而且每个符号之间有相位翻转，这样的编码方式可以减少直流分量。

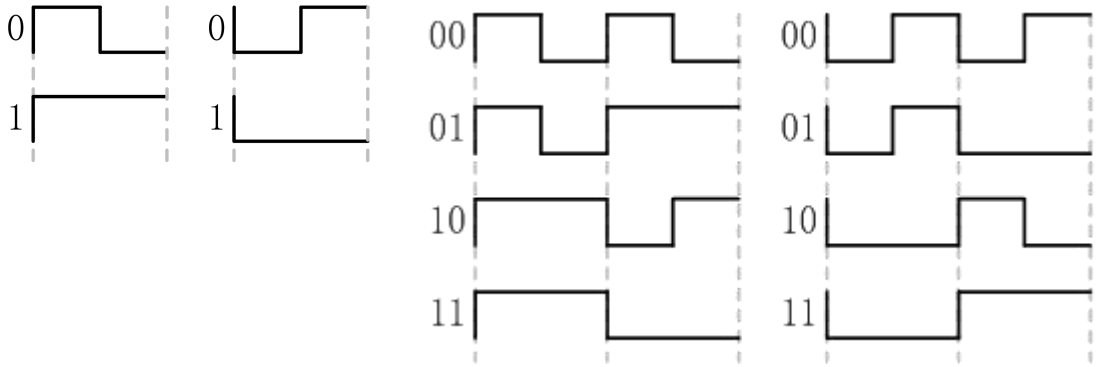
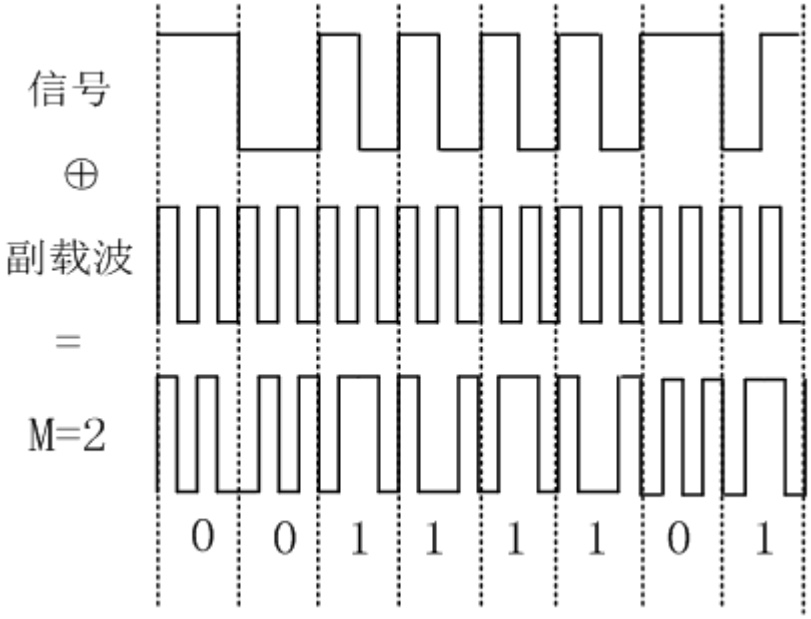


图 6　　FM0 编码

而 MILLER 编码的规则和 FM0 的编码规则稍有不同，具体示意如下图所示，可以选用副载波系数 M 为 2、4 或者 8。



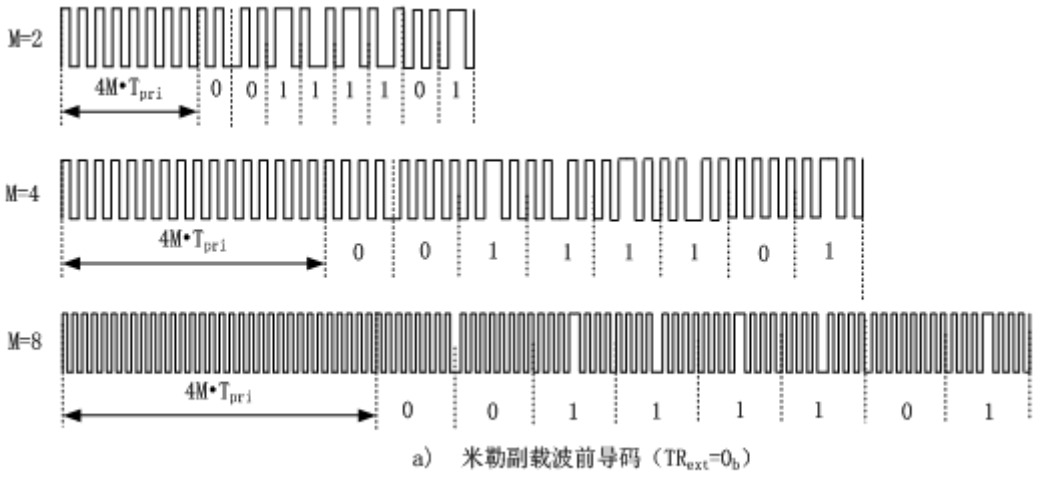


图 7　　MILLER 编码示意

上行前导码

在标签给读写器发送应答之前，需要先发送前导码。

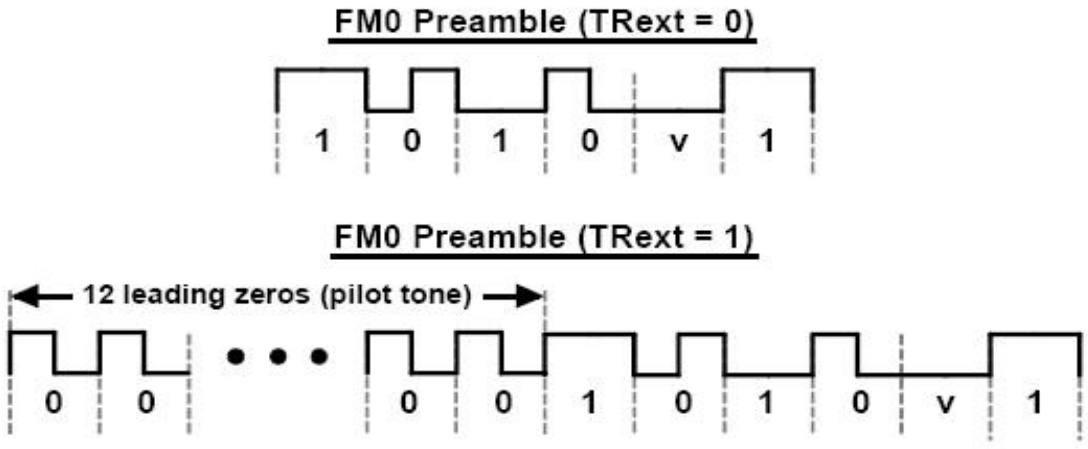


图 8　　EPC 协议上行前导码

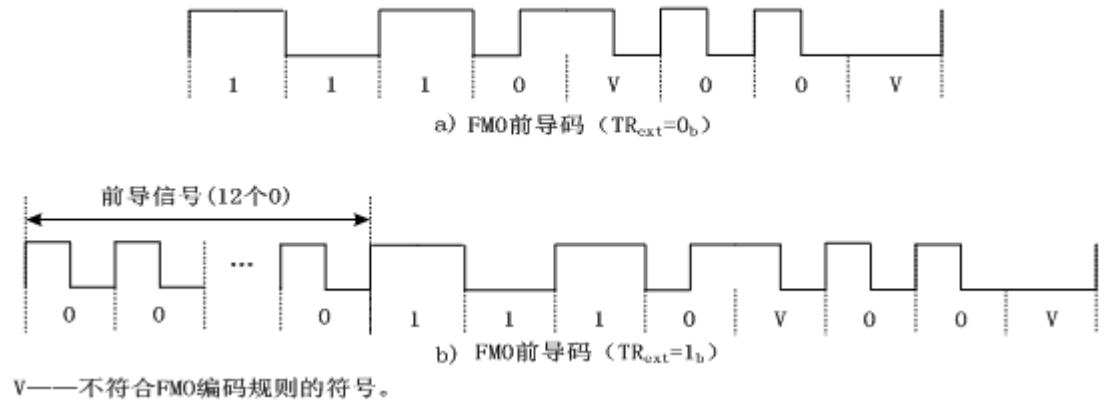


图 9　　GJB 和 GB 协议上行前导码

从上图可以发现 GJB 和 GB 协议的上行前导码相同，但和 EPC 协议在长度和内容上均不同。这也是 EPC 协议和 GJB、GB 协议的重大区别之一。

存储区介绍

逻辑存储区存放数据的最小单位为 1 个字，即 16 比特。

电子标签的逻辑存储区均为四种，协议要求和访问情况*，如下表所示。

表 2　　存储区说明

存储区	EPC	GJB	GB	备注
RESERVED / 安全区	必选	必选	必选	存放标签口令等安全数据
	可读可写	永远不可读	永远不可读	
EPC / 编码区	必选	必选	必选	存放标签电子产品编码（EPC）
	可读可写	永远可读	永远可读	
TID / 标签信息区	必选	必选	必选	存放标签唯一标示码
	永远不可写	永远不可写	永远不可写	
USER / 用户区	*可选*	*可选*	*可选*	GB 标签可有最多 16 个用户子区
	可读可写	可读可写	可读可写	

说明：

*访问情况可能随锁定命令配置变化，这里列出默认情况。

另外，GB 协议中，每个用户子区起始的 4 个字存放读写口令，永远不可读。

命令介绍

命令集分为两组，即盘点组命令和访问组命令。不同协议的命令见下表。

命令分为必选命令和可选命令两种，可选命令为读写器和标签可支持的命令，下表中用灰色斜体标出。

除必选命令和可选命令外，可以根据需要对命令集进行扩展，从而实现特定的功能。扩展敏两个分为专用命令和定制命令。专用命令是以生产制造为目的的，不能在射频识别应用系统中被使用。定制命令可以在和标准兼容的前提下被激

活，但协议不做定义。

表 3　　协议命令列表

命令	EPC	GJB	GB	说明
盘点组				
分类	Select	Sort	Sort	指定规则分类
启动查询	Query	Query	Query	启动盘点周期
调整查询	QueryAdjust			调整计数器
重复查询	QueryRep	QueryRep	QueryRep	调整计数器
分裂		Divide	Divide	调整计数器
分散		Disperse	Disperse	调整计数器
收缩		Shrink	Shrink	调整计数器
编码获取	ACK	ACK	ACK	获取编码区
应答错误	NAK	NAK	NAK	调整标签状态
访问组				
句柄更新		RefreshRN	RefreshRN	句柄更新
随机数获取	Req_RN	Get_RN	Get_RN	获取随机数
访问	*Access*	Access	Access	开启权限
读取	Read	Read	Read	读取数据
写入	Write	Write	Write	写入数据
块写入	*BlockWrite*			整块写入数据
擦除		Erase	Erase	擦除数据
块擦除	*BlockErase*			整块擦除数据
锁定	Lock	Lock	Lock	锁定存储区
块永久锁定	*BlockPermalock*			整块永久锁定
灭活	Kill	Kill	Kill	灭活标签
安全参数获取		*Get_SecPara*	*Get_SecPara*	获取安全参数
请求异或鉴别			*Req_XAuth*	请求异或鉴别
异或鉴别			*XAuth*	异或鉴别
单向异或鉴别			*Get_XAuth*	单向异或鉴别
双向异或鉴别			*Req_XAuth_Ex*	双向异或鉴别
请求鉴别		*Req_SAuth*	*Req_SAuth*	请求鉴别
鉴别		*SAuth*	*SAuth*	鉴别
单向鉴别		*Get_SAuth*	*Get_SAuth*	单向鉴别
双向鉴别		*Mul_SAuth*	*Mul_SAuth*	双向鉴别
安全通信		*Sec_Com*	*Sec_Com*	安全通信

句柄

EPC 协议句柄为 16bits 随机数 RN16，而 GJB 和 GB 协议中的句柄则是 RN11+CRC5。

读取

如果读取内容超出逻辑存储区的范围，则标签返回存储区溢出的错误代码。

在 GJB 协议中，如果读取长度为 0，标签不响应。

在 EPC 和 GB 协议中，如果读取长度为 0，访问存储区为标签信息区和用户区时，标签返回从起始地址开始到存储区结尾的所有数据；访问编码区时返回从起始地址开始到编码长度指示的数据。

写入/擦除

部分标签限制写入的最大长度，比如每次只能写入 1 个字。在应用中可以拆分成多次写入。

擦除可以理解为写入指定长度的 0。擦除和写入使用同样的访问口令。

锁定

锁定命令用于锁定标签逻辑存储区或配置标签的安全模式。

只有当标签有锁定口令时，锁定命令才有效。

EPC 锁定

EPC 标签可以对灭活口令、访问口令、EPC 区、TID 区、USER 区分别锁定，锁定分为永久和非永久两种。参数如下：

表 4　　EPC 锁定参数

	Kill pwd		Access pwd		EPC memory		TID memory		User memory	
	19	18	17	16	15	14	13	12	11	10
掩码	skip/ write	skip/ write	skip/ write	skip/ write	skip/ write	skip/ write	skip/ write	skip/ write	skip/ write	skip/ write
	9	8	7	6	5	4	3	2	1	0
动作	pwd read/ write	perma lock	pwd read/ write	perma lock	pwd write	perma lock	pwd write	perma lock	pwd write	perma lock

锁定参数中，掩码如果置为 0，则对应动作不生效。动作组合效果如下：

表 5　　EPC 锁定动作组合

存储区	pwd write	permalock	说明
EPC TID User	0	0	可以无需认证口令进行写入
	0	1	永久无需认证口令进行写入
	1	0	需要认证口令进行写入
	1	1	永久不可写入
存储区	**pwd read/write**	**permalock**	**说明**
Kill pwd Access pwd	0	0	可以无需认证口令进行读取和写入
	0	1	永久无需认证口令进行读取和写入
	1	0	需要认证口令进行读取和写入
	1	1	永久不可读取和不可写入

GJB 和 GB 锁定

GJB 和 GB 协议可以设置存储区锁定的状态为可读可写、可读不可写、不可读可写、不可读不可写。

只有当标签有锁定口令时，锁定命令才有效。

不同的存储区的读写权限有限制，在配置时需要特别注意。相关说明如下：

表 6　　GJB 和 GB 锁定动作

存储区	读取	写入	备注
安全区	不可读	可配置	永远不可读，写入权限可配置
编码区	可读	可配置	永远可读，写入权限可配置
标签信息区	可配置	不可写	永远不可写，读取权限可配置
用户区	可配置	可配置	每个子区可单独锁定，每个子区前 4 个字存放口令，永远不可读

灭活

灭活后的标签不再响应读写器的任何命令。