文档信息

信息	内容
关键字	隐私模式　密钥　安全 ISO/IEC 15693
摘要	本文旨在阐述 ICODE SLI-S 的安全特性及使用方法。

1. 介绍

I•CODE SLI-S/I•CODE SLI-S HC为ICODE产品系列中第二颗符合ISO/IEC15693和标准的芯片，主要面向需要较高安全特性、大容量存储器的应用，以满足日益增长的数据安全和隐私需求。此外，I•CODE SLI-S/I•CODE SLI-S HC还符合HF EPC标准。

1.1 范围

本文旨在介绍I•CODE SLI-S/I•CODE SLI-S HC的新增特性，主要集中于安全特性。此外，将简单与I•CODE SLI作一比较。

1.2 如何使用本文档

本文只介绍 I•CODE SLI-S/I•CODE SLI-S HC 的特性，所包含的任何信息并不取代相关的数据手册或应用指南。

I•CODE SLI-S/I•CODE SLI-S HC 两者的区别仅在于芯片本身所带的电容，在硬件功能上完全相同，因此，在后续章节中，I•CODE SLI-S 将用来表示 I•CODE SLI-S 和 I•CODE SLI-S HC。

1.3 参考文档

1. [SL113720] I•CODE SLI-S/SLI-S HC SL2 ICS53/SL2 ICS54 Functional Specification.
2. [SL058030] I•CODE SLI Smart Label IC SL2 ICS20 Functional Specification.

2. I•CODE SLI-S 安全特性和工作模式

I•CODE SLI-S提供灵活的方式保护用户数据，以满足日益增长的数据安全需求。

I•CODE SLI-S 提供多达五组的密码：

- 32 bits 读密码
- 32 bits 写密码
- 32 bit EAS 密码
- 32 bit 隐私密码
- 32 bit 灭活密码

根据以上密码， ICODE SLI-S可以被分别设置为下述工作方式：

- 由用户读密码和/或写密码保护的用户数据保护模式
- 由隐私密码保护的隐私模式
- EAS 密码保护的 EAS 保护模式
- 由灭活密码保护的灭活模式

2.1 用户数据保护模式

读密码和写密码可以用来保护用户数据。根据不同的配置，I•CODE SLI-S 可以工作于以下模式：

2.1.1 32bits 密码保护模式

在该模式下，存储器的保护由一组密码实现。

2.1.1.1 公开模式

在该模式中，所有的用户数据没有保护，可以任意读取。

2.1.1.2 读密码保护模式

在该模式中，读操作和写操作均由读密码保护。在对存储器进行任何读写操作之前，必须首先发送读密码。

2.1.1.3 写密码保护模式

在该模式中，写操作由写密码保护。在对存储器进行任何写操作之前，必须首先发送写密码。

注意：

在写密码保护模式中，读操作不受保护，即可以任意读取。

2.1.1.4 读写保护模式

在该模式中，读操作由读密码保护，写操作由写密码保护。在对存储器进行任何读操作之前，必须首先发送读密码；在对存储器进行任何写操作之前，必须首先发送写密码。

2.1.2 64 bits 保护模式

在该模式下，存储器的保护由读密码**和**写密码两组密码实现。在对存储器进行任何操作之前，必须首先发送读密码**和**写密码。

注意：

64bit 保护模式为不可逆操作，即设置为 64bit 保护模式后，无法再更改回公开模式或 32bit 保护模式。

2.2 隐私模式

可以通过 32bit 的隐私密码将 I•CODE SLI-S 设置为隐私模式。一旦标签进入该模式，则标签除了对指令 Get Random Number 和 Set Password 响应外，不对其他任何指令响应。

隐私模式主要用于满足客户日益增长的隐私需求。

2.3 EAS 保护模式

指令 Set EAS, Reset EAS, EAS Alarm 和 EAS Lock 与 I•CODE SLI 兼容。I•CODE SLI-S 主要在如下两个方面扩展 EAS 功能：

- 可以对 Set EAS, Reset EAS 和 EAS Lock 使用 32bit 密码保护
- 智能 EAS 功能：添加了 EAS 标志，以区别不同的应用。该 EAS 标志通过选项标志（option flag）来标识。

2.4 标签灭活

通过 32bit 的灭活密码验证后，标签可以被永久灭活，此后标签将不再对任何指令响应。

注意：

1．灭活为不可逆过程

2．I•CODE SLI-S 符合 ISO15693 标准和 HF EPC 标准，在 HF EPC 标准中，标签亦有 24bit 的灭活密码，但此 24bit 密码仅灭活 EPC 功能。而此处所指的灭活为整个标签的灭活。

3. 基于 RC632/RC400 的读写器升级的简单说明

在基于 RC632/RC400 的读写器中，固件程序主要以两种形式实现。

- 基于 NXP 的基本函数库（BFL，Basic Function Library）
- 用户自己开发函数原型

无论对于上述任何一种方式，开发工程师均需要了解三个方面：

- ICODE SLI-S 的安全机制
- 发送指令的正确顺序
- 新增指令的参数

3.1 基于 NXP 的 BFL

对此类读写器，请从 NXP 网站下载最新的 BFL，或与 NXP 上海的 FAE 联系。

开发工程根据安全机制的特点按照正确的顺序调用函数并设定正确的参数即可。

3.2 用户自己开发函数原型

对此类读写器，开发工程师可以参考本文档，阅读 SLI-S 的 datasheet，按照 datasheet 提供的完整指令格式，合理的调用自己开发的函数原型、正确设定参数即可。

4. 安全机制的实现

4.1 密码初始化和修改

在出厂默认条件下 ，所有的初始密码为全零，所有存储器为公开模式，即在该默认状态下，访问存储器时不需要验证密码。

只要知道当前密码，则密码的初始化可以在任何场合下进行。但是，由于 Write Password 指令中的密码为明文，因此我们强烈建议在安全的环境中初始化或者更改密码，以保证密码的安全性。

指令 Write Password 用来更改密码，在使用 Write Password 指令时，会有两种情况：

- 当前密码为全零
- 当前密码不为全零

但两种情况均要求在发送 Write Password 之前先通过指令 Set Password 发送当前密码，即使当前密码为默认的全零。

注意：

- *更改密码后，新密码即刻生效，即如果要访问响应的存储单元，则必须首先通过 Set Password 指令发送新的密码，即使新密码与旧密码相同。*
  - *例如，假设按照以下顺序发送指令：：*
    - *通过 Set Password 指令发送当前密码；*
    - *发送 Protect Page 指令将 Page0 设置为读写均由读密码保护模式；*
    - *发送 Write Password 指令，更改读密码，使新密码与旧密码相同；*
    - *发送 Read Single Block 指令，则将有错误码返回，指示需要密码验证。*
- *Write Password 指令只能在寻址模式或选择模式下发送*
- *密码更改只能在已知当前密码的情况下发生*

4.2 密码传送

指令 Set Password 用来传送密码，以获得存储器的存取权限。

Set Password 指令在标签上电后只需发送一次，除非更改过密码。

Set Password 指令中，密码不是明文发送，而是通过与随机数的抑或（XOR）来保护。即在发送 Set Password 密码之前， 需要先发送 Get Random Number 指令，此时标签将返回一个 16bit 的随机数，将该随机数分别与密码的高 16bit 和低 16bit 分别进行抑或操作，即可得到要发送的受保护的密码。

发送密码[31:0]=密码[31:0] XOR {随机数[15:0]，随机数[15:0]}

如果多次发送 Get Random Number 指令，则只有最后一次收到的随机数有效。

注意：

- *Set Password 指令只能在 addressed 或 selected 下执行，隐私密码除外*
- *如果 SLI-S 接收到错误的密码，则其将不再执行后续任何指令，直到重新上电*

4.3 用户数据保护

4.3.1 设置保护

设置用户数据保护主要涉及到以下指令。

表 1 用户数据保护指令

指令	描述
Protect Page	使能某个存储单元的保护功能
Lock Page Protection Condition	锁定某个存储单元的保护状态
Get Multiple Block Protection Status	查询存储单元的保护信息
64 bit Password Protection	使能 64bit 密码保护功能

读密码和写密码可以用来保护存储单元。密码保护功能可以通过指令 Protect Page 或者 64bit Password Protection 来使能。同样，保护状态可以通过 Protect Page 来改变，比如将由读写由读密码保护模式改为公开模式等。

注意：

- *保护模式的更改只能在保护状态未锁定的情况下*
- *如果设置了 64bit 保护模式，则状态不可再更改*

通过 Protect Page 指令，存储单元可以配置成如下保护状态：

表 2 保护状态配置

Protection Status	32 bit Password Protection	64 bit Password Protection
00h	Public	Public
01h	Read and Write protected by the Read password	Read and Write protected by the Read plus Write password
10h	Write protected by the Write password	Write protected by the Read plus Write password
11h	Read protected by the Read password **and** Write protected by the Write password	Read and Write protected by the Read plus Write password

指令 Lock page Protection Condition 可以用来永久地锁定存储单元的保护状态。

指令 Get Multiple Block Protection Status 可以用来查询存储单元的保护状态信息。

4.3.2 保护状态对 Inventory Page Read 的影响

如果要读取的存储单元由读密码保护，则在 Inventory Read 指令之前，必须发送密码，否则将无法内容。

由于 Inventory Read 主要用作发送的第一条指令，即读取相关的存储单元内容以代替唯一序列号，而且 Set Password 只能在 Selected 和 Addressed 模式下使用，故 Inventory Page Read 在实际中只适用于读取 Public 状态的存储单元。

4.3.3 指令顺序举例

将 Page5 的读写权限分别设置为由 read password 和 write password 保护。

(1)Inventory： 得到 UID

(2)Select： 选择该标签，可选指令

(3)Set password： 设置 read password

(4)Set password： 设置 write password

(5)Protect page： protection status = 11

(6)其他指令。 如果需要对 block 进行读写，则不需要重新发送密钥（除非更改了密钥）。

4.3.4 与 ICODE SLI 的命令比较

由于 ICODE SLI-S 对存储器是按照 Page 进行密码保护，故 ICODE SLI-S 将对指令做相应的修改。

4.3.4.1 Read Multiple Blocks

在 ISO15693 中，Read Multiple blocks 指令用于读取多个存储单元（SLI 以 4 个字节为一单元）。但是在 SLI-S 中采用的是按 page 管理 EEPROM（每个 page 包含 4 个 block，每个 block 包含 4 个字节），故 SLI-S 不再支持 Read multiple blocks。

4.3.4.2 Get Multiple Blocks Security Status

基于同样的道理，SLI-S 不支持 Get Multiple Blocks Security Status，而是由 Get multiple block protection status 指令取代。由于所有的 page 可能被读密码或者写密码保护，且其保护状态可能被锁定，故该指令扩展为如表 3 所示形式：

表 3 Block 的状态

Bit	Name	Value	Description
b1 (LSB)	Lock bit (WAC)	0	Block is not locked
		1	Block is locked (Lock Block command)
b2	Read password protected	0	disabled
		1	enabled
b3	Write password protected	0	disabled
		1	enabled
b4	Page protection lock	0	not locked
		1	locked
b5 to b8 (MSB)	-	0	

4.3.4.3 Inventory Read 和 Fast Inventory Read

SLI-S 同样不支持 Inventory Read 和 Fast Inventory Read 指令，而是由 Inventory Page Read 和 Fast Inventory Page Read 取代。

注意：

如果所读单元由读密码保护，则在指令之前需先发送密码。

4.4 设置隐私模式

隐私模式只有在知道隐私密码的情况下才能进入或离开。

以下指令如隐私模式相关：

表 4 与隐私模式相关的指令

指令	描述
Enable Privacy	使能隐私模式
Get Random Number	获取一个随机数，用于保护密码发送
Set password	发送密码/退出隐私模式

4.4.1 进入模式

Enable Privacy 指令用来使标签进入隐私模式，在此指令之前必须由 Set password 指令发送隐私秘密。

4.4.1.1 指令顺序举例

(1) Inventory： 得到 UID

(2) Select： 选择该标签，可选指令

(3) Set password： 设置 privacy password

(4) Enable privacy： 使能隐私模式

4.4.2 退出模式

在隐私模式下，标签只对 Get Random Number 和 Set Password 指令做响应。在 Get Random Number 指令后，标签将返回一个 16bit 的随机数。将密码与该 16bit 随机数异或后，通过 Set Password 指令发送。如果标签验证通过该密码，则其将离开隐私模式。

注意:

- *当需要退出隐私模式时，set password 指令不用 addressed mode 或 selected mode*
- *当多个标签在天线场时，如果有且仅有一个标签处于隐私模式，则当发送非 addressed 模式或 selected 模式的 set password 指令时，该隐私模式的标签仍可退出隐私模式*

4.4.2.1 指令顺序举例

(1) Get Random Number： 得到 16bit 随机数

(2) Set password： 设置 privacy password，此后将推出 Privacy 模式

4.5 EAS 保护模式

以下指令与 EAS 保护模式相关。

表 5 EAS 保护模式相关指令

指令	描述
Set EAS	使能 EAS 功能（如果 EAS 状态未被锁定）
Reset EAS	复位 EAS 功能（如果 EAS 状态未被锁定）
Lock EAS	锁定 EAS 状态
Password Protect EAS	使能 EAS 密码保护功能

EAS 保护功能将影响 Set EAS, Reset EAS 和 Lock EAS 指令，即在更改 EAS 状态之前，需要先发送 EAS 密码。在该密码保护下，只有已知密码的读写器才能设置或取消 EAS 功能或锁定状态，极大的增强了 EAS 的保护功能。

注意:

- *EAS Alarm 指令不受密码保护的影响*
- *EAS 保护为非可逆过程*

4.5.1 指令顺序举例

(1) Inventory： 得到 UID

(2) Select：　　选择该标签，可选指令

(3) Set password：　　设置 EAS password

(4) Password Protect EAS：　　使能 EAS 保护功能

(5) Set EAS：　　使能 EAS

4.6 灭活模式

以下指令与灭活有关.

表 6 灭活模式指令

指令	描述
Destroy SLI-S	通过此指令后，SLI-S 将不再对任何指令反应

灭活模式由灭活密码保护，即在该指令之前需先发送灭活密码。

注意:

- *灭活指令只能在 Addressed 或 Selected 模式下执行*
- *灭活为非可逆过程*

4.6.1 指令顺序举例

(1) Inventory：　　得到 UID

(2) Select：　　选择该标签，可选指令

(3) Set password：　　设置 Destroy password

(4)Destroy SLI-S