控制权限设置实验

一、 实验编号及名称

编号：IES_ISO14443_06

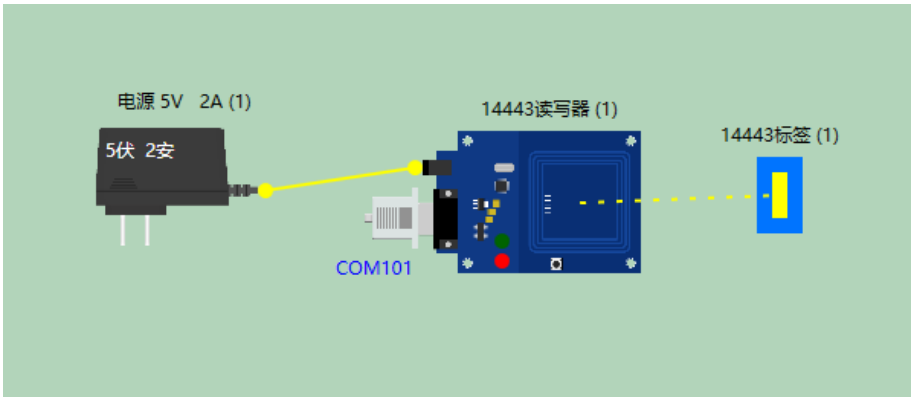
名称：控制权限设置实验

二、 实验目的

1、 掌握每个扇区的第 4 块的作用；
2、 掌握第 4 块的数据结构。

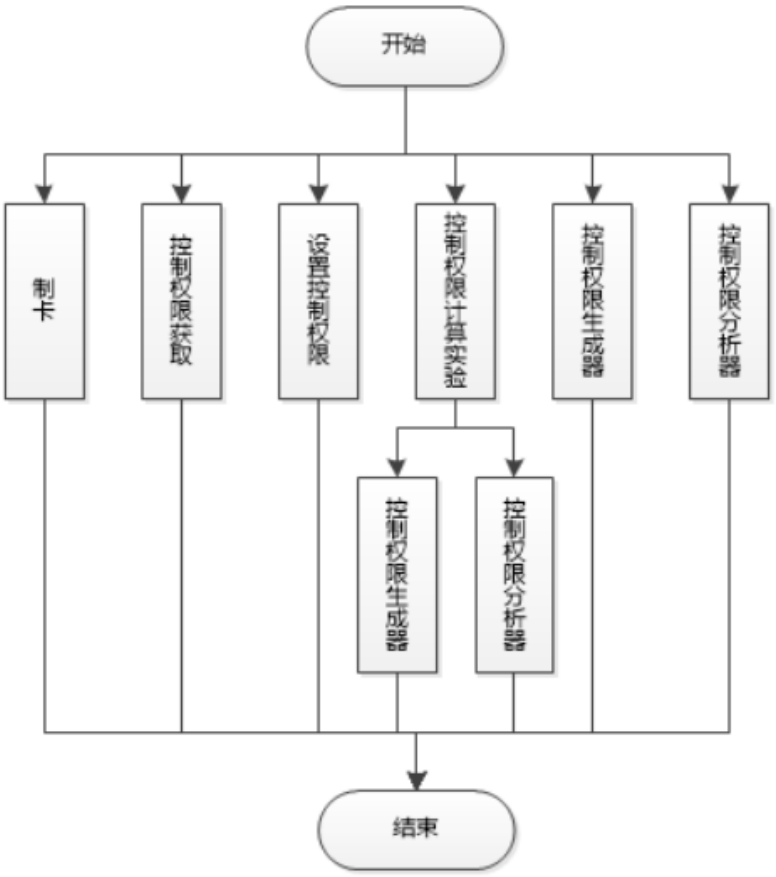
三、 实验设备

ISO14443 读写器、串口线、5V，2A 电源、ISO14443 卡片。在《物联网虚拟仿真实验平台》中按照下图所示进行设备的连接和串口的配置。



注：上图中 COM101 为读写器设备通过串口线与上位机连接的串口号

四、 实验内容说明



如上图所示，本实验分为六项内容，包括制卡、控制权限获取、设置控制权限、控制权限生成器、控制权限分析器。本实验的目的是为让学生了解利用控制位权限设置的规则，测试不同的权限，都有哪些变化；利用手动运算新权限设置规则；数据位的权限值表、控制位的权限值表。

五、 实验操作

1、 制卡

点击制卡后，出现制卡界面。

点击【打开】按钮，打开串口。然后点击【制卡】完成制卡实验。首先确立要进行操作的扇区和块区，算出操作块地址。本实验是对扇区 1，块 3 块地址为 7。块地址 7 是 1 扇区的控制块。

注： 一般一张空白的卡默认权限都是 “FF078069”,它是卡片中的最高权限，类似与管理员一样。FF078069 的块 0、块 1、块 2 中的权限都是 KeyA|B,意思就是验证 A 或者 B 密钥可读（Read）、可写（Write）、可加值（Inc）、可减值（Dec）。

注：如果用了使用过的卡片，更换卡片之后只需重新点击打开串口，系统会自动读取新卡片标签并显示到界面

控制块的权限表与数据块的权限表不同。数据块的权限表数据的读写权限和电子钱包的加减权限。但是控制块有密钥 A 的读写权限，密钥 B 的读写权

限，和控制权限的读写权限。比如:该控制权限没有读 A 密钥的权限，所以读取出来的 A 密钥全是 0。同理 B 密钥也是类似的，但是控制权限的读取权限都是可以读的。

单击制卡按钮，如提示成功，会弹出该制卡卡号的制卡信息，如密钥 A、密钥 B 还有块 3 的控制权限。如果提示失败，原因可能是验证 B 密钥失败，这时你要确定你制卡时是否是一张空白卡。如提示写入失败，则要保证你操作是否是一张空白卡。 。

2、 控制权限读取

（1） 寻卡

打开串口，点击【寻卡】按钮，自动获取卡片。

（2） 选卡

点击【选卡】，选择你读取到卡号的卡片。

（3） 验证

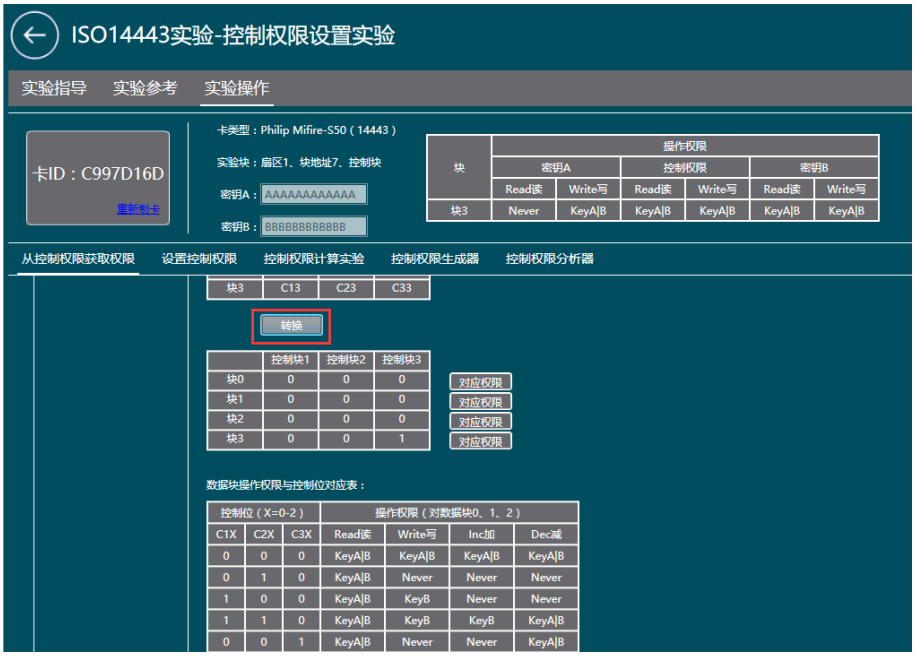
点击【验证】，验证 1 扇区的 A 密钥，如果提示验证成功，就可对这个扇区进行读取操作，否则无法进行读取操作。

（4） 读取

本实验读取的是块地址 7 的数据，读取出来的数据前 6 个字节是 A 密钥、中间 4 个字节是控制权限，后面 6 个字节是 B 密钥。具体结构在 IES_ISO14443_02 卡结构实验已经说明清楚了。

（5） 转换

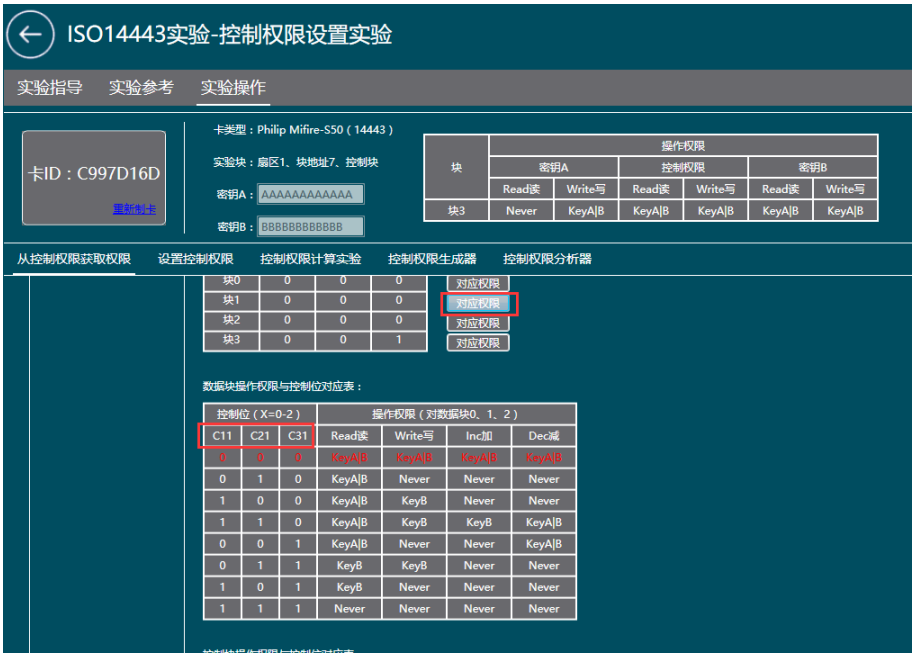
将读取到的控制权限转换为二进制，然后显示在表格中

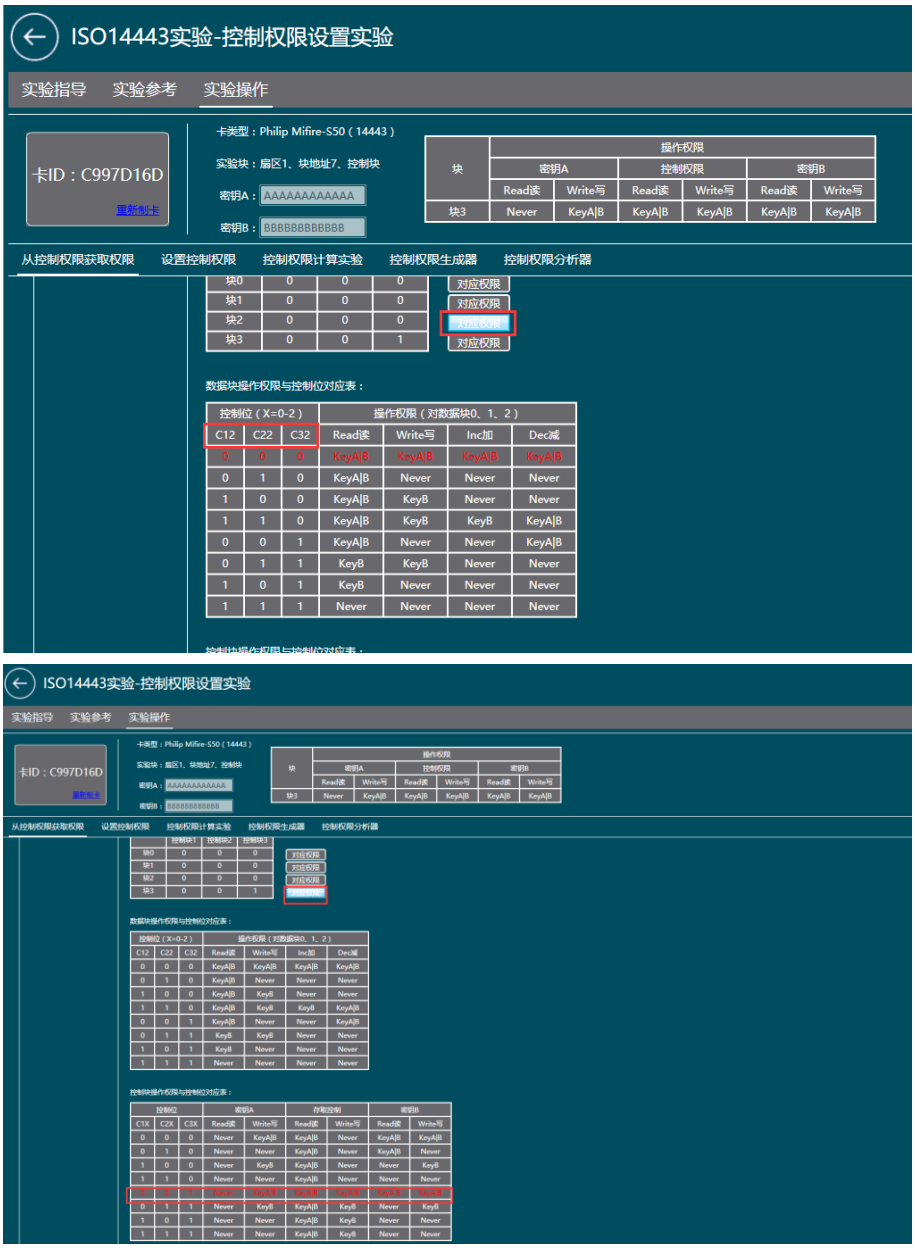


根据控制权限二进制表和控制权限与控制位对应表获取到每个块区的指令

（6） 对应权限


ISO14443实验-控制权限设置实验
实验指导
实验参考
实验操作
卡ID：C997D16D
重新制卡
卡类型：Philip Mifire-S50（14443）
实验块：扇区1、块地址7、控制块
密钥A：AAAAAAAAAAAA
密钥B：BBBBBBBBBBBB
块
操作权限
密钥A
控制权限
密钥B
Read读
Write写
Read读
Write写
Read读
Write写
块3
Never
KeyA|B
KeyA|B
KeyA|B
KeyA|B
KeyA|B
从控制权限获取权限
设置控制权限
控制权限计算实验
控制权限生成器
控制权限分析器
转换
控制块1
控制块2
控制块3
块0 0 0 0
块1 0 0 0
块2 0 0 0
块3 0 0 1
对应权限
对应权限
对应权限
对应权限
数据块操作权限与控制位对应表：
控制位（X=0-2）
操作权限（对数据块0、1、2）
C10
C20
C30
Read读
Write写
Inc加
Dec减
0 0 0 KeyA|B KeyA|B KeyA|B KeyA|B
0 1 0 KeyA|B Never Never Never
1 0 0 KeyA|B KeyB Never Never
1 1 0 KeyA|B KeyB KeyB KeyA|B
0 0 1 KeyA|B Never Never KeyA|B

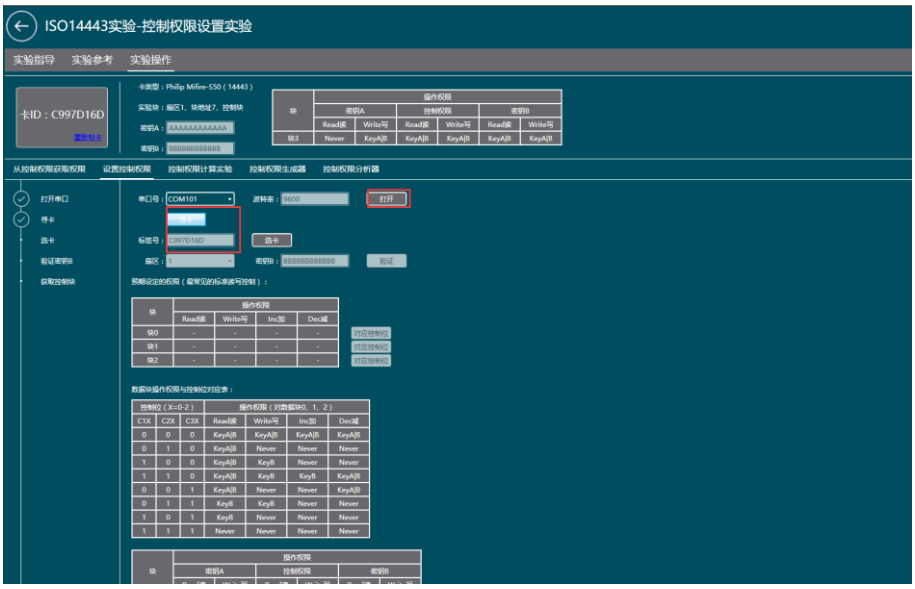

ISO14443实验-控制权限设置实验
实验指导
实验参考
实验操作
卡ID：C997D16D
重新制卡
卡类型：Philip Mifire-S50（14443）
实验块：扇区1、块地址7、控制块
密钥A：AAAAAAAAAAAA
密钥B：BBBBBBBBBBBB
块
操作权限
密钥A
控制权限
密钥B
Read读
Write写
Read读
Write写
Read读
Write写
块3
Never
KeyA|B
KeyA|B
KeyA|B
KeyA|B
KeyA|B
从控制权限获取权限
设置控制权限
控制权限计算实验
控制权限生成器
控制权限分析器
块0 0 0 0
块1 0 0 0
块2 0 0 0
块3 0 0 1
对应权限
对应权限
对应权限
对应权限
数据块操作权限与控制位对应表：
控制位（X=0-2）
操作权限（对数据块0、1、2）
C11
C21
C31
Read读
Write写
Inc加
Dec减
0 0 0 KeyA|B KeyA|B KeyA|B KeyA|B
0 1 0 KeyA|B Never Never Never
1 0 0 KeyA|B KeyB Never Never
1 1 0 KeyA|B KeyB KeyB KeyA|B
0 0 1 KeyA|B Never Never KeyA|B
0 1 1 KeyB KeyB Never Never
1 0 1 KeyB Never Never Never
1 1 1 Never Never Never Never



根据获取到的每个块区的指令，得到每个块区的控制权限情况

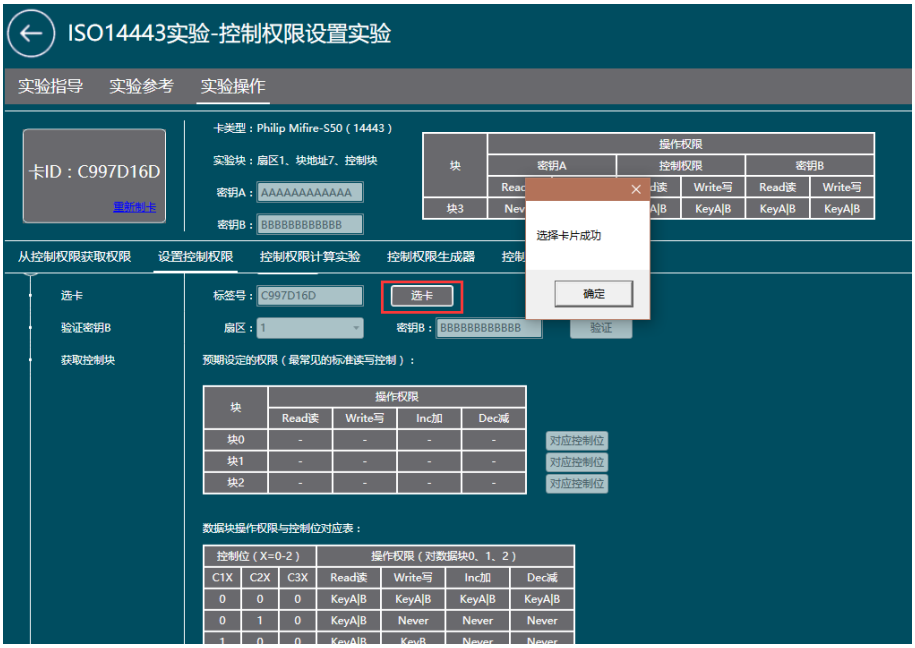
3、 设置控制权限

（1） 寻卡



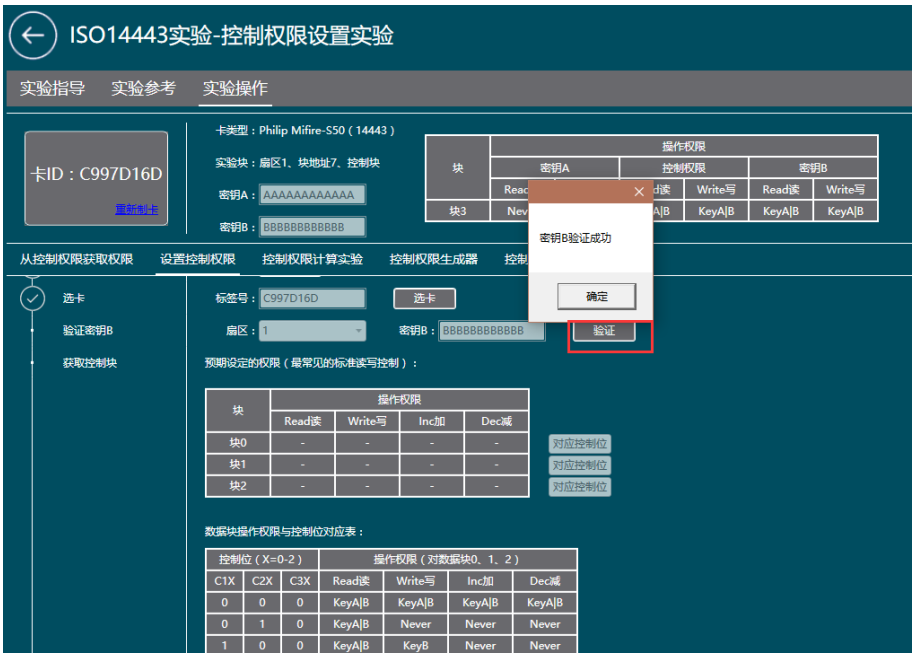
打开串口，点击【寻卡】按钮。

（2） 选卡



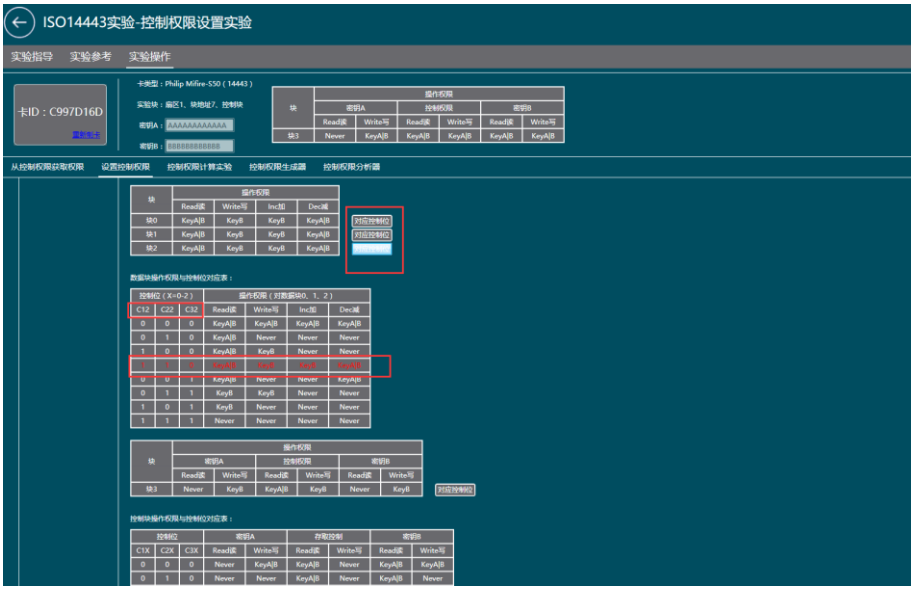
选择你读取到卡号的卡片，点击【选卡】按钮。

（3） 验证



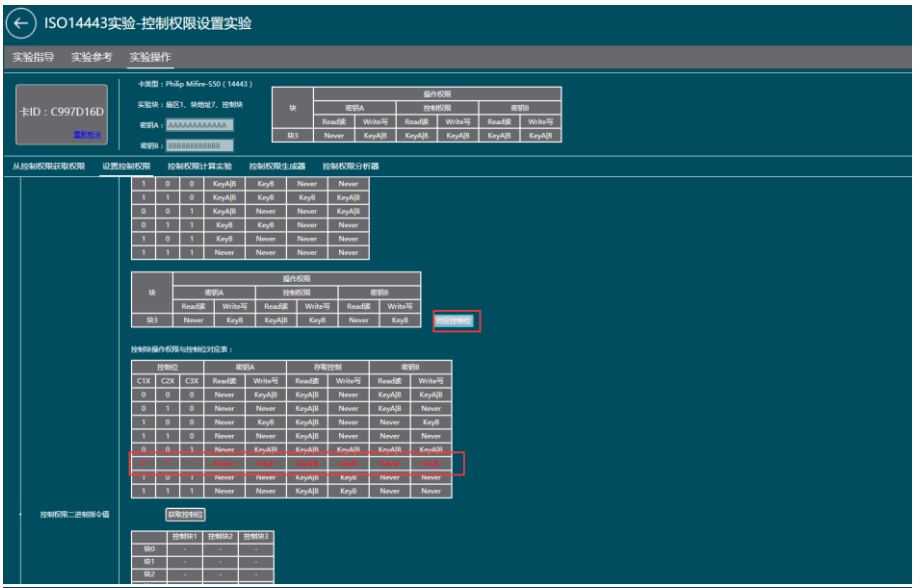
验证 1 扇区的 B 密钥，如果提示验证成功，就可对这个扇区进行写入操作。

（4） 获取控制块



获取到每个块区的指令，然后显示在表格中

（5） 获取控制位



卡类型：Philip Mifire-S50（14443）

实验块：扇区1、块地址7、控制块

密钥A：AAAAAAAAAAAA

密钥B：BBBBBBBBBBBB

块	操作权限					
	密钥A		控制权限		密钥B	
	Read读	Write写	Read读	Write写	Read读	Write写
块3	Never	KeyA|B	KeyA|B	KeyA|B	KeyA|B	KeyA|B

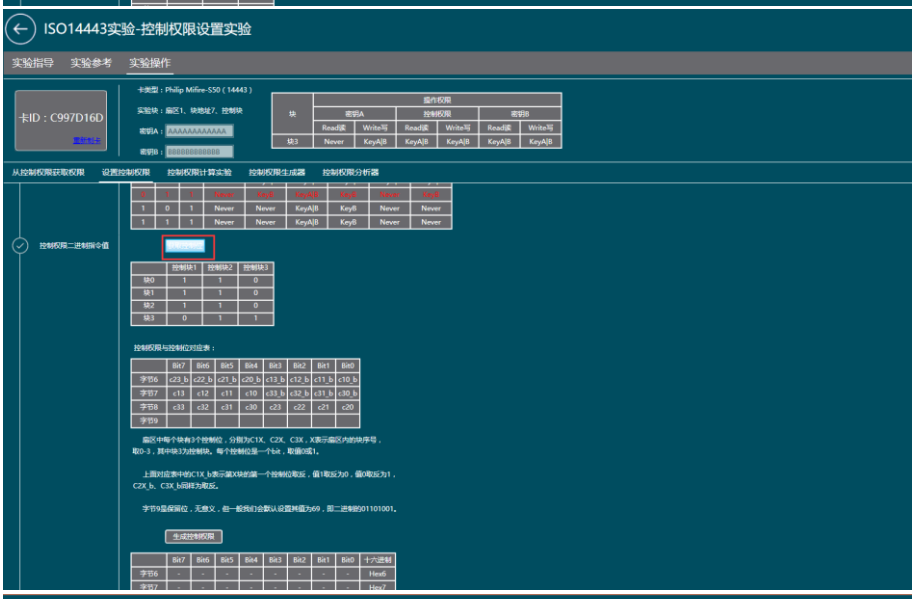
1	0	0	KeyA|B	KeyB	Never	Never
1	1	0	KeyA|B	KeyB	KeyB	KeyA|B
0	0	1	KeyA|B	Never	Never	KeyA|B
0	1	1	KeyB	KeyB	Never	Never
1	0	1	KeyB	Never	Never	Never
1	1	1	Never	Never	Never	Never

块	操作权限					
	密钥A		控制权限		密钥B	
	Read读	Write写	Read读	Write写	Read读	Write写
块3	Never	KeyB	KeyA|B	KeyB	Never	KeyB

控制块操作权限与控制位对应表：

控制位			密钥A		存取控制		密钥B	
C1X	C2X	C3X	Read读	Write写	Read读	Write写	Read读	Write写
0	0	0	Never	KeyA|B	KeyA|B	Never	KeyA|B	KeyA|B
0	1	0	Never	Never	KeyA|B	Never	KeyA|B	Never
1	0	0	Never	KeyB	KeyA|B	Never	Never	KeyB
1	1	0	Never	Never	KeyA|B	Never	Never	Never
0	0	1	Never	KeyA|B	KeyA|B	KeyA|B	KeyA|B	KeyA|B
0	1	1	Never	KeyB	KeyA|B	KeyB	Never	KeyB
1	0	1	Never	Never	KeyA|B	KeyB	Never	Never
1	1	1	Never	Never	KeyA|B	KeyB	Never	Never

	控制块1	控制块2	控制块3
块0	-	-	-
块1	-	-	-
块2	-	-	-



卡类型：Philip Mifire-S50（14443）

实验块：扇区1、块地址7、控制块

密钥A：AAAAAAAAAAAA

密钥B：BBBBBBBBBBBB

块	操作权限					
	密钥A		控制权限		密钥B	
	Read读	Write写	Read读	Write写	Read读	Write写
块3	Never	KeyA|B	KeyA|B	KeyA|B	KeyA|B	KeyA|B

0	1	1	Never	KeyB	KeyA|B	KeyB	Never	KeyB
1	0	1	Never	Never	KeyA|B	KeyB	Never	Never
1	1	1	Never	Never	KeyA|B	KeyB	Never	Never

	控制块1	控制块2	控制块3
块0	1	1	0
块1	1	1	0
块2	1	1	0
块3	0	1	1

控制权限与控制位对应表：

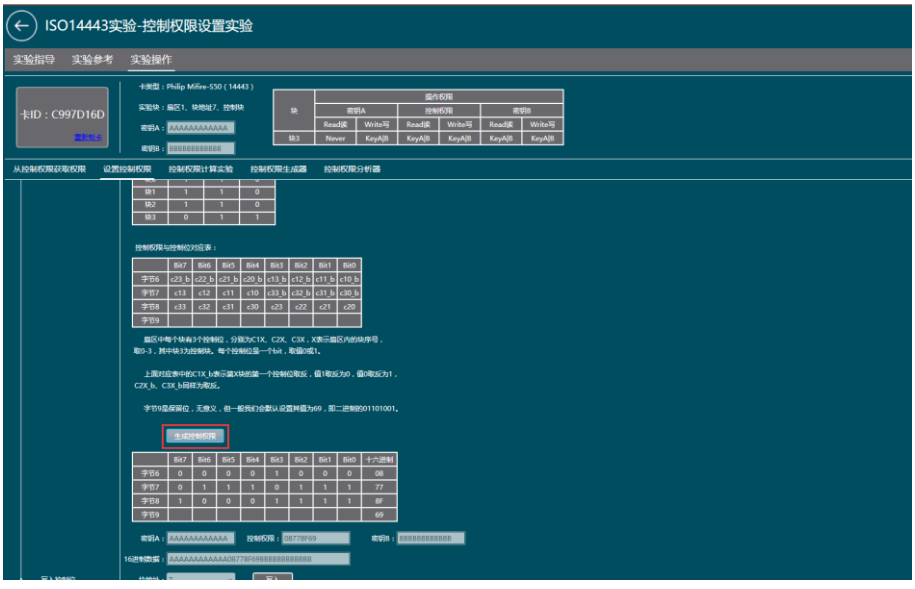
	Bit7	Bit6	Bit5	Bit4	Bit3	Bit2	Bit1	Bit0
字节6	c23_b	c22_b	c21_b	c20_b	c13_b	c12_b	c11_b	c10_b
字节7	c13	c12	c11	c10	c33_b	c32_b	c31_b	c30_b
字节8	c33	c32	c31	c30	c23	c22	c21	c20
字节9								

扇区中每个块有3个控制位，分别为C1X、C2X、C3X，X表示扇区内的块序号，取0-3，其中块3为控制块。每个控制位是一个bit，取值0或1。

上面对应表中的C1X_b表示第X块的第一个控制位取反，值1取反为0，值0取反为1，C2X_b、C3X_b同样为取反。

字节9是保留位，无意义，但一般我们会默认设置其值为69，即二进制的01101001。

	Bit7	Bit6	Bit5	Bit4	Bit3	Bit2	Bit1	Bit0	十六进制
字节6	-	-	-	-	-	-	-	-	Hex6
字节7	-	-	-	-	-	-	-	-	Hex7



卡类型：Philip Mifire-S50（14443）

实验块：扇区1、块地址7、控制块

密钥A：AAAAAAAAAAAA

密钥B：BBBBBBBBBBBB

块	操作权限					
	密钥A		控制权限		密钥B	
	Read读	Write写	Read读	Write写	Read读	Write写
块3	Never	KeyA|B	KeyA|B	KeyA|B	KeyA|B	KeyA|B

块1	1	1	0
块2	1	1	0
块3	0	1	1

控制权限与控制位对应表：

	Bit7	Bit6	Bit5	Bit4	Bit3	Bit2	Bit1	Bit0
字节6	c23_b	c22_b	c21_b	c20_b	c13_b	c12_b	c11_b	c10_b
字节7	c13	c12	c11	c10	c33_b	c32_b	c31_b	c30_b
字节8	c33	c32	c31	c30	c23	c22	c21	c20
字节9								

扇区中每个块有3个控制位，分别为C1X、C2X、C3X，X表示扇区内的块序号，取0-3，其中块3为控制块。每个控制位是一个bit，取值0或1。

上面对应表中的C1X_b表示第X块的第一个控制位取反，值1取反为0，值0取反为1，C2X_b、C3X_b同样为取反。

字节9是保留位，无意义，但一般我们会默认设置其值为69，即二进制的01101001。

	Bit7	Bit6	Bit5	Bit4	Bit3	Bit2	Bit1	Bit0	十六进制
字节6	0	0	0	0	1	0	0	0	08
字节7	0	1	1	1	0	1	1	1	77
字节8	1	0	0	0	1	1	1	1	8F
字节9									69

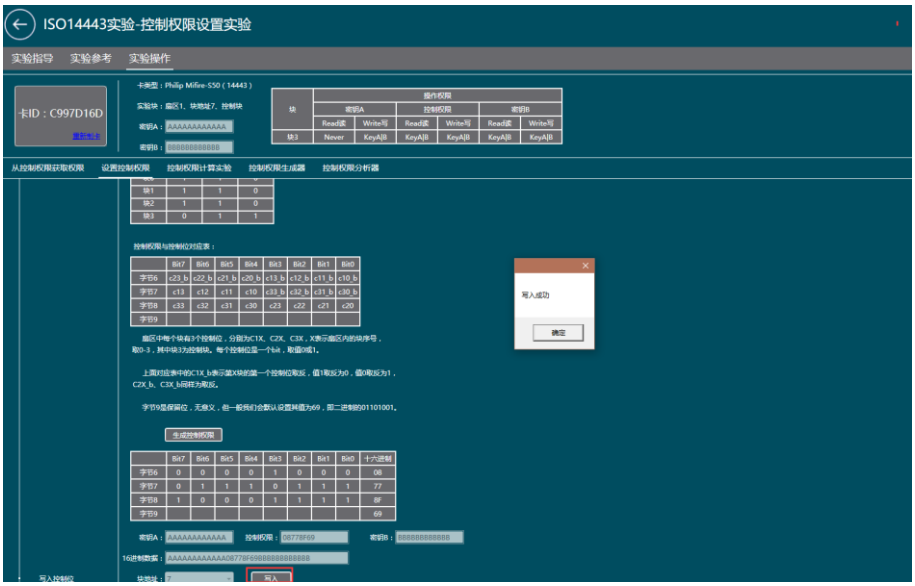
密钥A：AAAAAAAAAAAA　控制权限：08778F69　密钥B：BBBBBBBBBBBB

16进制数据：AAAAAAAAAAAA08778F69BBBBBBBBBBBB

根据《控制权限与控制位对应表》和当前块区的指令情况，生成新的控

制权限

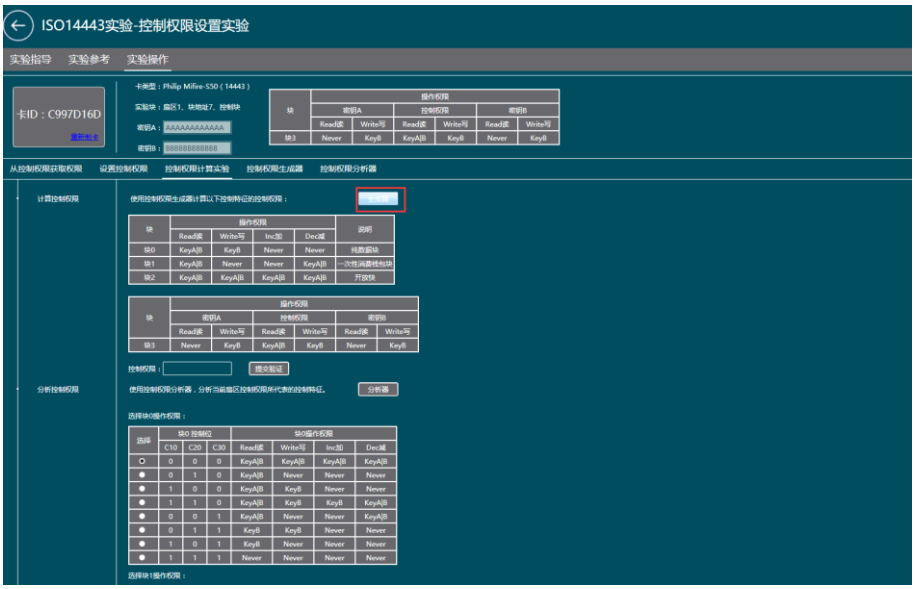
（6） 写入



将获取到的新权限与 A 密钥、B 密钥组合成新的十六进制字符串，然后写入到块地址 7 中。提示写入成功，说明新的权限已经写入成功，提示失败，可能原因是你没有写入权限或者字符串错误。

4、 控制权限计算实验、控制权限生成器、控制权限分析器

（1） 计算控制权限

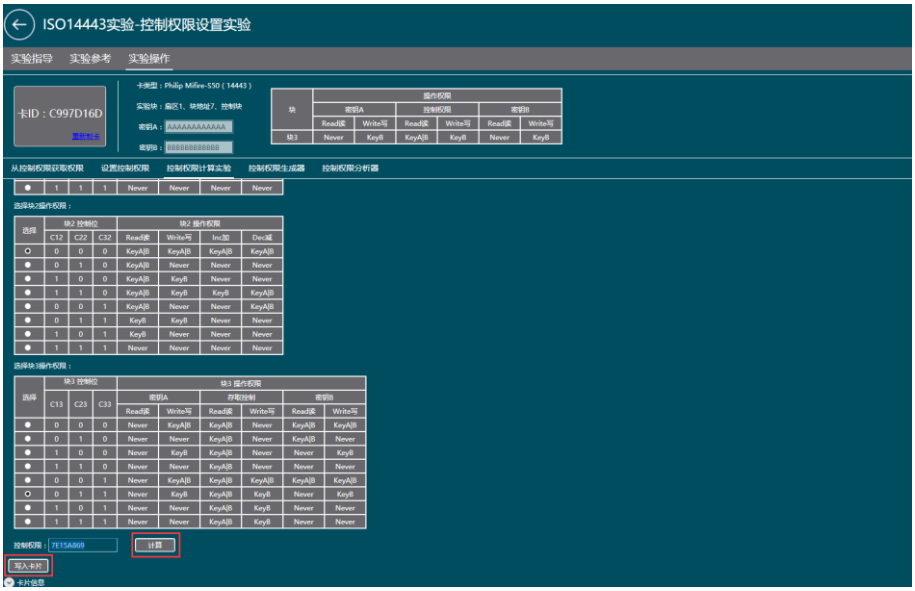


点击【生成器】按钮，打开控制权限生成器。

注：查看要用生成器生成权限的表，最好将这个权限表截个图。然后点击生成器，调转到控制权限生成器中，根据您要设置的权限表的块区权限情况，选择每个块区的权限，然后进行计算，将计算好的权限写入到卡片中。点击确定，确定成功后会自动调转到该界面。也可以参考实验参考 6-1、6-2 表进行相关操

作

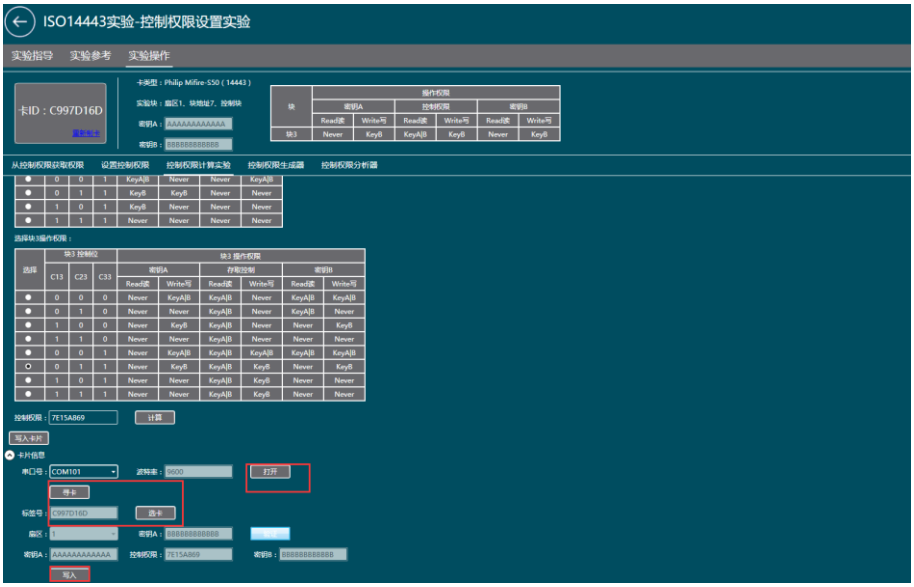
（2） 控制权限计算



按照权限表选择，点击【计算】按钮，获取控制权限。

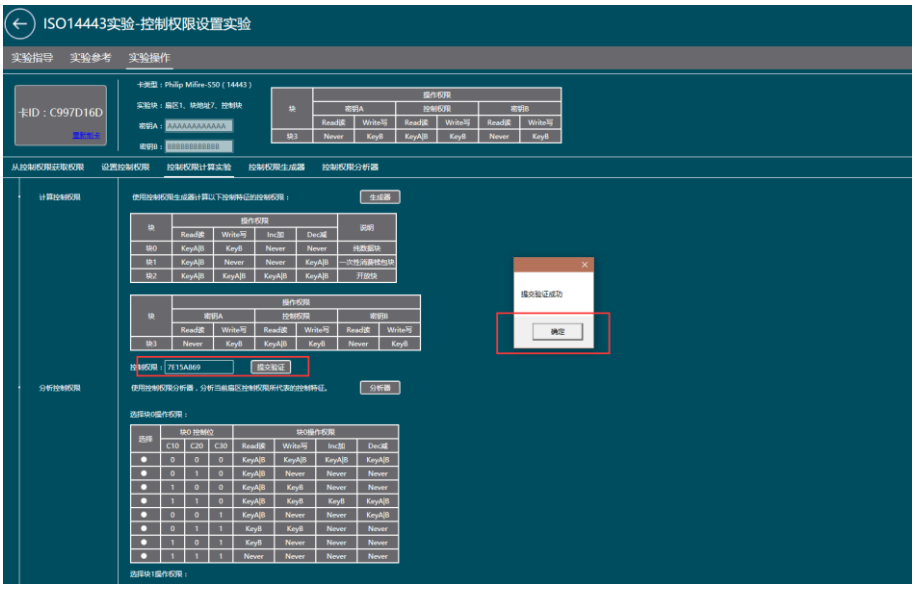
注：计算的控制权限需要复制，在控制权限计算实验界面中会验证计算出来的控制权限是否跟指定的控制权限值相同

（3） 写入卡片



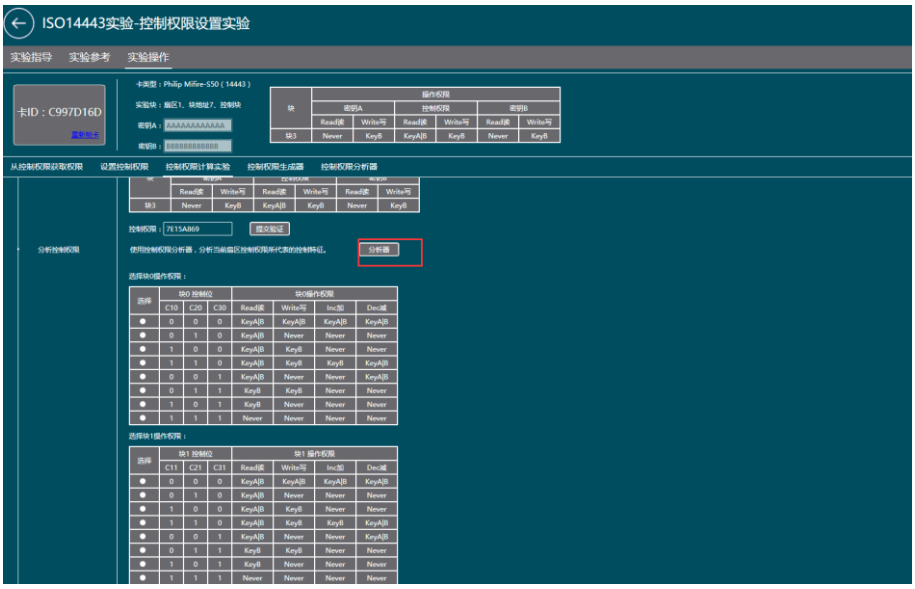
打开串口，寻卡、选卡、验证一次完成后，点击【写入】按钮，完成写入卡片。

（4） 控制权限



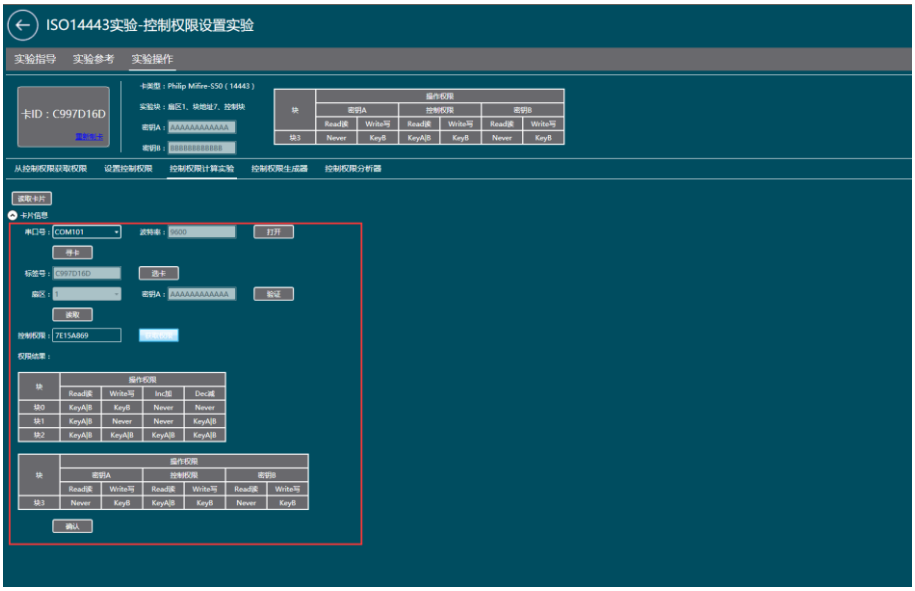
填写用生成器计算的控制权限。如果提示验证成功，则该步骤成功，如果失败原因是计算出来的控制权限与表中的不符。

（5） 分析器



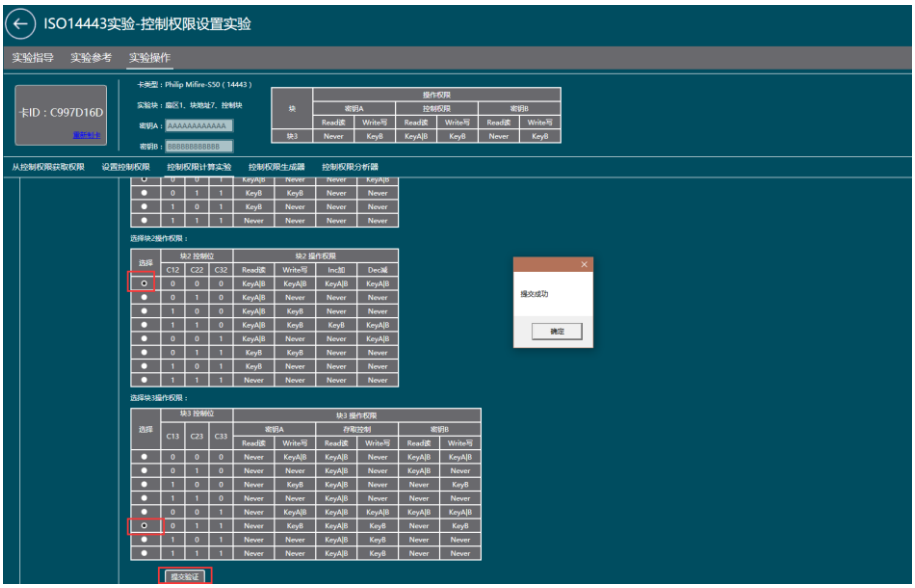
点击【分析器】按钮，打开控制权限分析器界面。

（6） 控制权限分析器



打开串口，寻卡、选卡、验证、读取、获取权限依次完成，显示权限结果，点击【确认】按钮，返回控制权限计算实验界面。

（7） 分析控制权限



按照权限表选择，点击【提交验证】按钮，提示提交成功，完成本实验。

六、 实验思考

1、 设置权限的指令有什么规律，每个指令之间他们的权限值又有什么不同？指令之间的权限值是随便设置的呢？还是按照了怎样的排列设置的？

2、 脱离实验的步骤，自己又是否可独立完成新权限值的设置呢？

3、 联系现实一些场景的应用，猜想它们又用了高频 14443 的那些权限呢？