



写博客



发布Chat (http://gitbook.cn/new/gitchat/activity?utm_source=csdnblog1)

登录 (https://passport.csdn.net/account/login?ref=toolbar)

ref=toolbar)

注册 (http://passport.csdn.net/account/mobile/register?ref=toolbar&action=mobileRegister)



1



MSP430熔丝及加密总结

原创

2016年10月23日 15:58:27

1262

MSP430熔丝及加密总结

MSP430是使用熔丝或者电子熔丝去做内部代码的保护，如果熔丝烧断，那么将不能使用JTAG或者BSL去非法访问内部代码。MSP430F1/F2/F4系列是采用物理熔丝的方式，使用编程器在TEST引脚或者TDI引脚上加6.5V±0.5V的电压，采取这种方式，JTAG接口被禁止而且是不可恢复的，只能通过BSL去访问。MSP430F5/F6/FR2/FR4/FR5/FR系列都是采用e-Fuse电子熔丝的方式去做加密，一般是在Flash/FRAM中的2个字的位置（签名）内写入一定的内容去实现加锁或者加密码。器件只能通过密码保护的BSL去访问。通过BSL去访问器件，去清除JTAG签名区，那么是可以重新恢复并且访问MCU的。

Table 1. JTAG Locking Features Across MSP Families

Device Family	Physical Fuse	Boot Override	Electronic Fuse	JTAG Signatures	Reversible	JTAG Access With Password
MSP430F1xx/F2xx/F4xx	✓					
MSP430F5xx/F6xx			✓	0x17FC–0x17FF	✓ with bootloader	
MSP430FR5xx/FR6xx			✓	0xFF80–0xFF83	✓ with bootloader	✓
MSP430FR2xx/FR4xx			✓	0xFF80–0xFF83	✓ with bootloader	
MSP430i2xx			✓	0xFFDC–0xFFDF	No factory bootloader available	
MSP432Pxx		✓			✓ with boot override factory reset	

F5x/F6x eFuse:



鸵鸟蛭蛭 (http://blog.cs...

+ 关注

(http://blog.csdn.net/sphinz1)

码云

未开通

原创

6

粉丝

0

喜欢

0

(https://gi
utm_sourc

他的最新文章

更多文章 (http://blog.csdn.net/sphinz1)

TMS320F28335: Possible Incorrect
Operation of XINTF Module After
Power Up
(/sphinz1/article/details/75043835)

C2000 进入低功耗所需的配置
(/sphinz1/article/details/75043764)

limp mode下对芯片进行恢复
(/sphinz1/article/details/74930370)

.out文件转bin文件
(/sphinz1/article/details/73718043)

JTAG签名在17FCh~17FFh地址内，写入全0或者全F以外的值会将JTAG/BSL接口锁住。要对这些地址编程，那么首先要清除SYSBSLC寄存器中的SYSBSLPE位，用于解锁BSL Flash被保护的区域。

Table 2. JTAG Locking on F5xx/F6xx

Name	Addresses	Value	Device Security
JTAG/SBW Signature	17FCh~17FFh ⁽¹⁾	FFFF_FFFFh	JTAG/SBW is unlocked.
		0000_0000h	
		Any other value	JTAG/SBW is locked.

如果要清除JTAG/SBW保护，可以使用BSL去对JTAG签名写入全0，BSL也是通过中断向量表中的FFE0h~FFFFh中的至少32bytes的密码去做保护。因为JTAG签名是位于被保护的BSL区域，BSL首先回清除SYSBSLC寄存器中的SYSBSLPE位，随后对JTAG签名写入全0。

FR5xx/FR6xxeFuse：

JTAG签名在FRAM的FF80~FF83h范围内，写入55555555h到JTAG签名中，JTAG/BSL接口被无密码的锁住。如果想要解除JTAG/SBW保护，bootloader可以使用5555或AAAA以外的值去清除JTAG签名。或者执行BSL整体擦除指令。

Table 3. JTAG Locking on FR5xx/FR6xx

Name	Addresses	Value	Device Security
JTAG/SBW Signatures	FF80h~FF83h	5555h_5555h	JTAG/SBW is locked without password.
		@FF80h = AAAAh	JTAG/SBW is locked with password. ⁽¹⁾
		@FF82h = password length in words	
		Any other value	JTAG/SBW is unlocked.

如果是5555_5555h到JTAG签名区中，那么JTAG会被直接锁死，只能通过BSL命令去解锁。
如果写入AAAA_xxxxh到JTAG签名区中，那么JTAG被密码锁死，可以通过密码去让仿真器访问MCU。
如果JTAG签名中写入其它值，那么JTAG/SBW没有被锁住。

FR4xx/FR2xxeFuse：

JTAG签名在FF80~FF83h范围内，对JTAG签名中写入00000000h或FFFFFFFFh以外的值可以将JTAG进行无密码解锁的锁住。可以使用Bootloader对签名去写入全0或者全1去解锁JTAG/BSL保护。BSL也是密码保护的，在中断向量表中的至少32个字节做BSL的密码，也可以通过BSL的整体擦除命令去解锁。



种植头发的价格



在线课程



【免费】搜狗机器翻译技术分享
http://edu.csdn.net/course/detail/590?
utm_source=blog9)
http://edu.csdn.net/hu
iyiCourse/detail/590?
blog9)



深度学习在推荐领域的应用和实践
http://edu.csdn.net/course/series_detail/68?
utm_source=blog9)
http://edu.csdn.net/hu
iyiCourse/series_detail/
68?utm_source=blog9)

热门文章

MSP430熔丝及加密总结 (/sphinzi1/articl
e/details/52902284)

1261

Table 4. JTAG Locking on FR2xx/FR4xx

Name	Addresses	Value	Device Security
JTAG/SBW Signature	FF80h–FF83h	FFFF_FFFFh	JTAG/SBW is unlocked.
		0000_0000h	
		Any other value	JTAG/SBW is locked.

所以，如果JTAG/SBW被锁住，那么仿真器不能通过密码去访问器件，只能采用BSL按照一定的密码匹配去解锁器件。



1



FR5/FR6xx加密例程分析

```
#pragma RETAIN(JTAG_signatures)
#pragma DATA_SECTION(JTAG_signatures, ".jtagsignature")
const uint16_t JTAG_signatures[] = {0xAAAA, 0x0002};

...

#pragma RETAIN(JTAG_password)
#pragma DATA_SECTION(JTAG_password, ".jtagpassword")
const uint8_t JTAG_password[] = {0x12, 0x34, 0x56, 0x78};
```

在linker文件中将.jtagsignature分配到JTAG签名区去，0xFF80中写入0xAAAA，那么是采用密码的方式加锁eFuse，0xFF82中写入0x0002，那么密码的长度为2个字节。jtagpassword被分配到0xFF88起始的区域中，写入相应的密码。

器件加密后，再进行一次BOR复位，那么JTAG被锁住了。可以再CCS中对.ccxml文件进行配置然后再次让仿真器访问器件。如下图所示。

全新TMS320F28377S没法连接仿真器，解决办法 (/sphinz1/article/details/56482452)

332

.out文件转bin文件 (/sphinz1/article/details/73718043)

328

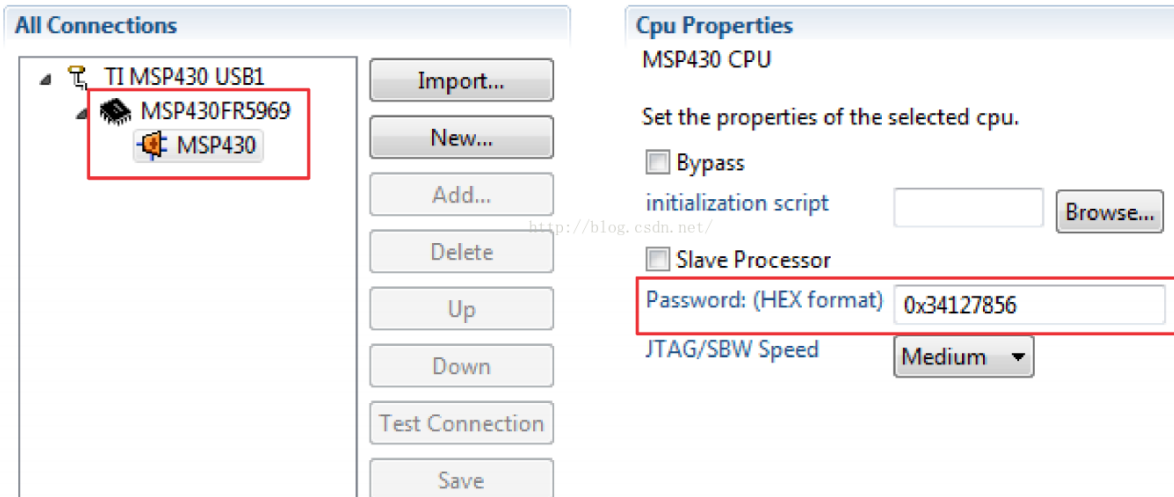
limp mode下对芯片进行恢复 (/sphinz1/article/details/74930370)

135

TMS320F28377S的BSL密码 (/sphinz1/article/details/75043835)

93

Target Configuration



这时候MCU是已经被加密了，如果执行芯片擦除操作，或者在代码中将JTAG签名区写入FFFF_FFFFh(5555或者AAAAh之外的值)，那么芯片也能解密。

另外，BSL也是可以禁止使用的。

版权声明：本文为博主原创文章，未经博主允许不得转载。



相关文章推荐

msp430 学习经验总结 (/ming1006/article/details/7626165)

最近学习MSP430，把自己的一些经验分享下，这是我在网上发现的一篇很不错的文章，归纳得很好，简洁明了。 1.MSP430 开发环境建立 1.安装IAR for msp430 软件，软件带US...

 ming1006 (<http://blog.csdn.net/ming1006>) 2012-06-02 16:33  4522



1



msp430加密解密 (<http://download.csdn.net/detail/liulongxiang/1485128>)

2009-07-13 11:59 6KB [下载](#)



太任性！学AI的应届学弟怒拒20K Offer，他想要多少钱？

AI改变命运呀！！前段时间在我司联合举办的秋季招聘会上，一名刚刚毕业的学弟陆续拒绝2份Offer，企业给出18K、23K高薪，学弟拒绝后直接来了一句...

(http://edu.csdn.net/topic/ai1?utm_source=blog10)

个人总结之MSP430F5510串口通讯 (485) (/black_yu/article/details/51873276)

1.首先先介绍一下USCI模块 通用串行通信接口 (USCI) 模块支持多种异步通信模式。不同的 USCI 模块支持不同的模式。每一个 USCI 模块以不同的字母命名。例如，USCI_A 不同于...

 black_yu (http://blog.csdn.net/black_yu) 2016-07-10 20:49  1168

个人总结之基于MSP430F5510的TMP275驱动 (/black_yu/article/details/51873322)

1.TMP275是什么？TMP275是一款精度为 $\pm 0.5^{\circ}\text{C}$ 且具有 12 位模数转换器 (ADC) 的集成数字温度传感器，可在低至 2.7V 的电源供电下运行，并且与德州仪器 (TI) 的...

 black_yu (http://blog.csdn.net/black_yu) 2016-07-10 20:57  356

个人总结之基于MSP430F5510的X9331驱动 (/black_yu/article/details/51873298)

1.X9331是什么？X9331是一款数字带电位器，有32个电阻值，电阻值可通过外部信号进行控制，选择好的电阻值被保存在非挥发存储器中，可重复调用。2.X9331有什么用？我们拿来干嘛？X...

 black_yu (http://blog.csdn.net/black_yu) 2016-07-10 20:53  174



1



msp430g2553内部资源总结 (http://download.csdn.net/detail/qq_17315333/8351445)

(http://download.csdn.net/detail/qq_17315333/8351445)

2015-01-11 21:24 3.96MB 



MSP430时钟设置及应用总结 (<http://download.csdn.net/detail/mcgradyc/3545316>)

(<http://download.csdn.net/detail/mcgradyc/3545316>)

2011-08-24 16:35 40KB 

蓝牙连接MSP430F1232单片机之后，不传输数据 (/jingjbuer/article/details/50551788)

通过安卓手机端的软件来接受蓝牙数据，蓝牙连接单片机，通过单片机的串口将数据给蓝牙，然后蓝牙再发送给手机，现在手机端通过Eclipse调试，发现应该是卡在了输入流的read上，因为read方法是阻塞式的...

 jingjbuer (<http://blog.csdn.net/jingjbuer>) 2016-01-22 09:12  816



msp430相关模块学习总结 (http://download.csdn.net/detail/sinat_29971733/8916183)

(http://download.csdn.net/detail/sinat_29971733/8916183)

2015-07-20 14:58 1004KB 



MSP430时钟设置及应用总结 (http://download.csdn.net/detail/qq_17208267/8921833)

(http://download.csdn.net/detail/qq_17208267/8921833)

2015-07-22 10:31 97KB 

nRF24L01 MSP430 发送接收驱动程序 (/nmzqdsg/article/details/6750904)

nrf24l01.c #include "nrf24l01.h" unsigned char flag=0;//状态寄存器 (STATUS) 标志 unsigned char success=0;...



nmzqdsq (<http://blog.csdn.net/nmzqdsq>) 2011-09-05 20:10 1340



msp430g2553内部资源总结 (http://download.csdn.net/detail/qq_20645075/8910657)

(http://download.csdn.net/detail/qq_20645075/8910657)

2015-07-18 00:50 59KB

下载



msp430总结 (<http://download.csdn.net/detail/yuxinshu1989/3854437>)

(<http://download.csdn.net/detail/yuxinshu1989/3854437>)

2011-11-28 22:13 96KB

下载

TinyOS在MSP430F2618上移植 (三) 之LCD (/hwwr112100/article/details/6628504)

本节记录串口TFT LCD在TinyOS上的移植。1.8寸LCD显示屏采用ST7735控制器，使用SPI接口实现控制、显示数据的传输。

总体架构：分为3层结构，最底层位于相应的pl...



hwwr112100 (<http://blog.csdn.net/hwwr112100>) 2011-07-24 04:19 1801

两种方式实现TinyOS对MSP430F26&54系列的支持 (/hwwr112100/article/details/6569306)

第一种方式在Ubuntu 下TinyOS msp430 Toolchain mspgcc升级一文中已经作了详细分析，下面说说另一种方式实现TinyOS对MSP430高端系列单片机的支持。我们...



hwwr112100 (<http://blog.csdn.net/hwwr112100>) 2011-06-26 23:39 1981

MSP430 串口初始化，及串口操作 (/jxm_csdn/article/details/45218423)

关于UART0串口的初始化，及操作函数说明 关于UART1串口的初始化，及操作函数说明



jxm_csdn (http://blog.csdn.net/jxm_csdn) 2015-04-23 10:38 698

MSP430 SPI驱动 代码设计流程 (/dannielyoung/article/details/72903956)

MSP430 SPI驱动 代码设计流程平常工作中，如果使用MSP430作为主控芯片，经常会遇到需要编写SPI 或 I2C 驱动，来读取和控制外设（比如LCD屏幕，一些传感器）的情况。为了减少重复性工作...



Dannielyoung (<http://blog.csdn.net/Dannielyoung>) 2017-06-07 21:07 535



1



IAR for MSP430 和 AVR 单片机, 数据类型和指针大小(编译器手册) (/kissmonx/article/details/7980836)

=====
=====...



KISSMonX (<http://blog.csdn.net/KISSMonX>) 2012-09-14 22:36 1989



51 , AVR,PIC,MSP430,STM32单片机比较 (/cfxzy/article/details/18908667)

这里是几款单片机的对比的一个帖子，转过来和大家分享，如果有不同意见，请多多指教~ 如果只是用来进行简单的机电控制，那就用51单片机 如果牵涉到低功耗设计，那用MSP430单片机 如果既要综合考虑价格...



cfxzy (<http://blog.csdn.net/cfxzy>) 2014-02-03 10:35 5393

MSP430-----2 (/wangjinzhouqw/article/details/7855309)

这里首先补充下IO口的中断，中断是通过PxIE,PxIES，PxIFG决定的，配置中断仍然要设置方向寄存器，上拉下拉使能寄存器，上拉下拉极性寄存器。在这块芯片中有个COMPARE模块，这个...



wangjinzhouqw (<http://blog.csdn.net/wangjinzhouqw>) 2012-08-11 20:45 836

