

# Enhancing Device Security by Using JTAGLOCK Feature

Vivek Singh

## ABSTRACT

The JTAGLOCK feature provides a means for the C2000 device to disable JTAG access to the device via debug tools like Code Composer Studio™ (CCS) IDE. This feature has been implemented in the C2000™ Microcontroller (MCU) devices starting with the TMS320F2838x product family. This application report provides details on how to leverage this feature.

## Contents

1	Security Feature on C2000 Device .....	1
2	JTAGLOCK Feature .....	2
3	Enabling JTAGLOCK .....	3
4	Disabling JTAGLOCK .....	5
5	Permanent JTAGLOCK .....	6
6	References .....	7

## List of Figures

1	Launching On-Chip Flash GUI .....	4
2	JTAGLOCK Configuration Fields in On-Chip Flash GUI .....	4
3	Updating ccxml File With JTAG Password .....	6

## List of Tables

1	JTAGLOCK Mode .....	2
2	Z1OTP_JLM_ENABLE .....	2
3	Z1OTP_JTAGPSWDHx .....	3
4	Z1OTP_JTAGPSWDLx .....	3
5	Security Configuration for Permanent JTAGLOCK.....	6

## Trademarks

Code Composer Studio, C2000 are trademarks of Texas Instruments.  
All other trademarks are the property of their respective owners.

## 1 Security Feature on C2000 Device

The Dual Code Security Module (DCSM) baseline architecture provides a barrier to someone trying to gain unauthorized access to important intellectual property in the form of firmware (FW). A resource like memory can be left unsecured or allocated to either of the two secure zones. Additionally, it can be marked as execute-only (EXEONLY) to raise the barrier even higher. Through special hardware features, firmware stored in EXEONLY flash can even be copied to and run from EXEONLY RAM. Each of the secure zone is protected by a 128-bit CSM password and security configurations are programmed into the one-time programmable (OTP) area of the Flash. The configuration governs, among other items, which flash sectors and RAM blocks (memory) are allocated to which zone. Security logic protects un-authorized access to each zone's secure resources. For detailed information about device security features, please refer to *Dual Code Security Module (DCSM)* section in the device-specific Technical Reference Manual (TRM).

## 2 JTAGLOCK Feature

All C2000 devices have a JTAG interface, which is used for debugging the device via debug tools like Code Composer Studio (CCS). The Dual Code Security Module (DCSM) on C2000 device provides a clean method to debug one secure zone while maintaining the security barrier around the other zone, as well as allowing a slight lowering of the barrier to debug the two zones together. However, there are times where the flexibility of debugging is not as important as strengthening the barrier around firmware. Hence user may want to disable any debug access to the device. In the security world, strengthening comes in the form of layering. The JTAGLOCK feature provides this additional layer by blocking JTAG (debugger) access to the device entirely. User can enable the JTAGLOCK feature by programming the USER OTP appropriately. In addition to 128-bit CSM password, another 128-bit JTAG password has been added to security configuration to enable/disable the JTAGLOCK feature. Thus, JTAGLOCK essentially puts another hedge around the device firmware, overlaying on top of the base DCSM architecture.

**Table 1. JTAGLOCK Mode**

JTAGLOCK Mode	Description
JTAGLOCK Enable	JTAG access to all the CPU is blocked. Debug tool like CCS cannot connect to device.
JTAGLOCK Disable	JTAG access to all the CPU is allowed. Debug tool like CCS can connect to any CPU based on other security configuration.

**NOTE:** Although JTAGLOCK is available without using the base DCSM security, for highest security it is recommended that both be enabled. To enable the base DCSM security and lock the zones, you must program a 128-bit CSM password along with other security configuration into the USER OTP as per the device-specific Technical Reference Manual.

### 2.1 Z1OTP\_JLM\_ENABLE

This is a 32-bit value in Zone1 USER OTP of CPU1 at address location 0x78006. The default value of this location is 0xffff000f. 4 bits (LSB) of this 32-bit value maps to JLM (JTAG LOCK Module) enable. To enable the JTAGLOCK feature, you must change this 4-bit value from 0xF (default value) to any other value.

**Table 2. Z1OTP\_JLM\_ENABLE**

Z1OTP_JLM_ENABLE	JTAGLOCK Feature
0xffff000f (default)	JTAGLOCK Disable
0xffff000e	JTAGLOCK Enable
0xffff000d	JTAGLOCK Enable
-----	JTAGLOCK Enable
0xffff0000	JTAGLOCK Enable
0x00000000	JTAGLOCK Enable

## 2.2 JTAG Password

The JTAGLOCK feature is protected by a 128-bit JTAG password. This 128-bit JTAG password is split into two 64-bit passwords: JTAGPSWDHx and JTAGPSWDLx. Like all other security configuration, these are also part of Zone1 USER OTP of CPU1.

### 2.2.1 Z1OTP\_JTAGPSWDHx

JTAGPSWDHx (JTAGPSWDH0 and JTAGPSWDH1) is the upper half of 128-bit JTAG password located in the header section of Zone1 USER OTP of CPU1. Since this is a part of the header, once these values are programmed, it can never be changed again.

**Table 3. Z1OTP\_JTAGPSWDHx**

JTAGPSWDHx	USER OTP Address
JTAGPSWDH0	0x78014
JTAGPSWDH1	0x78016

### 2.2.2 Z1OTP\_JTAGPSWDLx

JTAGPSWDLx (JTAGPSWDL0 and JTAGPSWDL1) is the lower half of 128-bit JTAG password located in each of the Zone Select Block (ZSB) of Zone1 USER OTP of CPU1. You can change these 64-bit values by selecting a new Zone Select Block (ZSB), if needed. For detailed information about the Zone Select Block (ZSB), see the *Dual Code Security Module* section in device-specific Technical Reference Manual.

**Table 4. Z1OTP\_JTAGPSWDLx**

JTAGPSWDLx	USER OTP Address
JTAGPSWDL0	Zone_Select_Block address + 0x1C
JTAGPSWDL1	Zone_Select_Block address + 0x1E

Basically, you can initially choose a 128-bit password to protect the JTAG interface, but only the lower 64-bit can be modified later and the upper 64-bit remains same.

## 3 Enabling JTAGLOCK

Enabling the JTAGLOCK feature is a two step process:

1. Program a 128-bit JTAG password (Z1OTP\_JTAGPSWDHx/Z1OTP\_JTAGPSWDLx).
2. Enable the JTAGLOCK module (JLM) by programming Z1OTP\_JLM\_ENABLE.

**NOTE:** When you want to change the Z1OTP\_JTAGPSWDLx value, select a new Zone Select Block by changing the Z1OTP\_LINKPOINTERx value and programming a new value for Z1OTP\_JTAGPSWDLx.

Just like the programming of any other security configuration, the JTAGLOCK settings can be programmed by the CCS flash plug-in GUI or by incorporating these values in the .out file itself.

### 3.1 CCS Flash Plug-in GUI

The CCS Flash plug-in has a graphical user interface (GUI) which enables you to program the security configuration. It has GUI fields for every configuration so that you can choose to program different settings at different times. This method is more useful for initial development when you want to try different options to learn about security feature on the device.

Follow these steps to bring-up the Flash plug-in GUI in CCS:

1. Launch CCS Target configuration.
2. Connect to **CPU1**.
3. Click on **Tool** and then select **On-Chip Flash**.

This will bring-up the GUI which has all the security configuration fields as shown in Figure 2. As mentioned earlier, it is advisable to program the JTAGLOCK password first and then program the JTAGLOCK (JLM) field, because once the JTAGLOCK (JLM) field is programmed and a CPU reset is performed, the JTAG interface will get disabled and CCS connection will be terminated until the 128-bit JTAG password is scanned in.

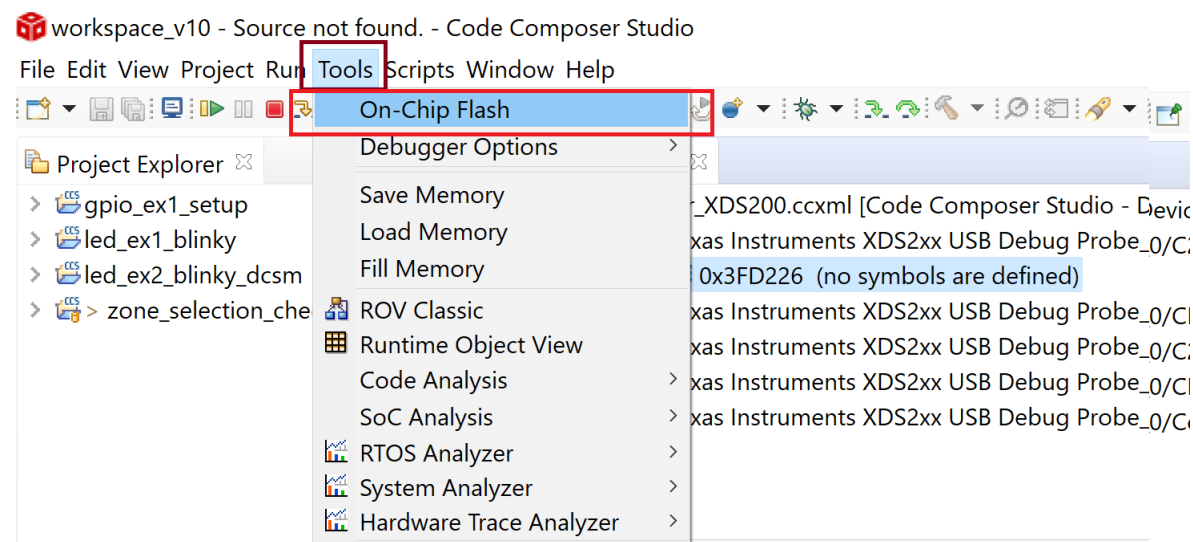


Figure 1. Launching On-Chip Flash GUI

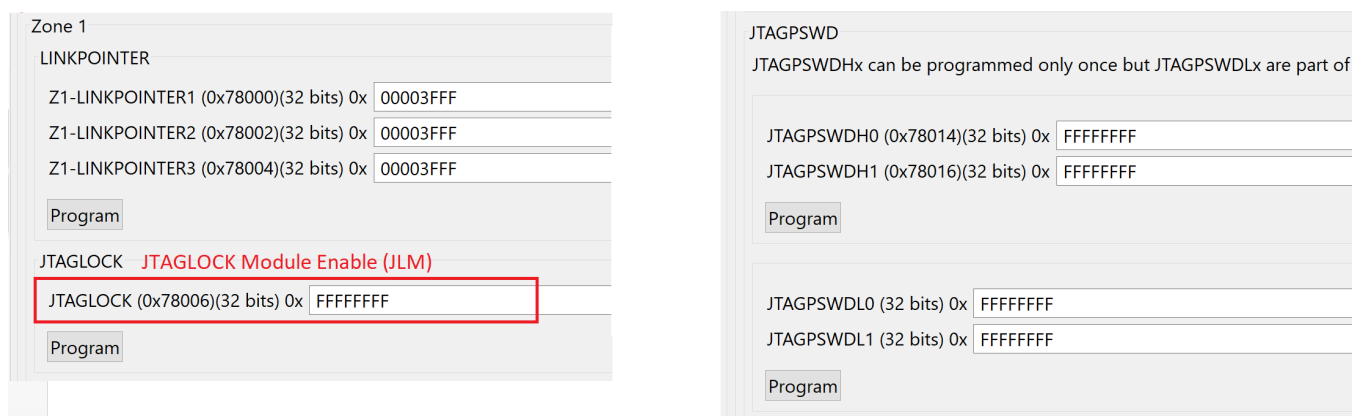


Figure 2. JTAGLOCK Configuration Fields in On-Chip Flash GUI

### 3.2 Security Configuration Embedded in .out File

You can include security configuration as part of the C code itself so that it is embedded in the .out file and gets programmed when programming the .out file. This method is useful when the security configuration values are almost finalized or for production programming. In this case, all the security settings get programmed at once. Hence, if the JTAGLOCK (JLM) has been enabled, then CCS connection will be terminated after the .out file has been programmed and the CPU has been reset.

To see how to include security configurations in C code, see the DCSM example (<C2000Ware>\driverlib\2838x\examples\c28x\dcsm ) in C2000Ware.

## 4 Disabling JTAGLOCK

Occasionally, a need may arise to debug the device in which JTAGLOCK is enabled (JTAG interface disabled). For example, a device may be returned to Texas Instruments for failure analysis (FA). Code Composer Studio (CCS) is the most convenient tool to debug the C2000 device and for that, the JTAG interface need to be accessible. For this reason, a hardware mechanism has been provided to disable the JTAGLOCK by providing 128-bit JTAG password. This hardware mechanism uses the JTAG pin to enter the password, therefore, access to JTAG pins on the circuit board must be available for this.

[Section 4.1](#) explains how to disable the JTAGLOCK using 128-bit JTAG password.

### 4.1 Target Configuration (.ccxml) File

In this method, the 128-bit JTAG password can be entered in the device ccxml file (Target Configuration file) and the CCS will use this password to unlock the JTAG before connecting to the target. Follow these steps:

1. Double click on the device target configuration file (.ccxml file).
2. Click on the **Advanced** tab of the Target Configuration window.
3. Click on the **JLM** subpath.
4. Enter the 128-bit JTAG password in the **Unlock Key** fields.
5. Click on the **Save** icon.

When you try to connect to the target (CPU1), the CCS will use the 128-bit JTAG password to unlock the JTAG password. If the password is correct, then the JTAG interface will get enabled and the target will get connected. If the password is not correct, then the target connection will fail.

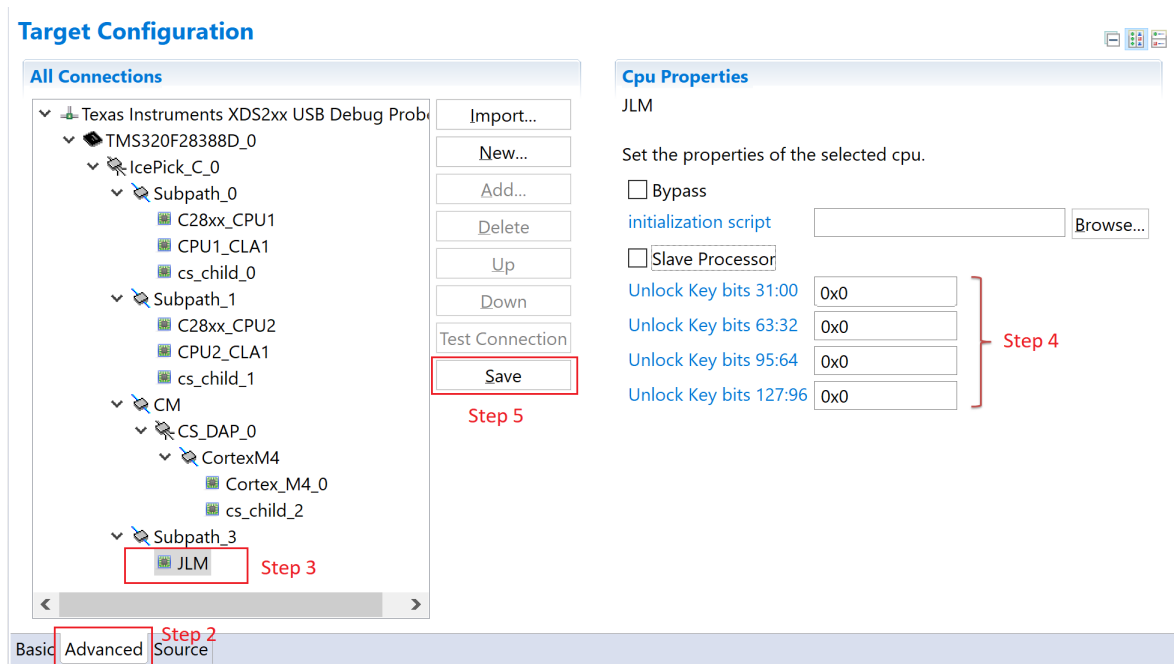


Figure 3. Updating cxmml File With JTAG Password

## 5 Permanent JTAGLOCK

Sometimes, you may want to permanently disable the JTAG interface on the device in the field. This can be achieved by programming the 128-bit JTAG password value as ALL\_0 and enabling the JTAGLOCK module (JLM). Once this is done, JTAGLOCK can not be disabled again hence you cannot connect to the target via CCS for any further debug on that device. Table 5 provides the required security configuration to permanently enable JTAGLOCK feature.

Table 5. Security Configuration for Permanent JTAGLOCK

Security Configuration	Value
Z1OTP_LINKPOINTER1	0x0000_0000
Z1OTP_LINKPOINTER2	0x0000_0000
Z1OTP_LINKPOINTER3	0x0000_0000
Z1OTP_JLM_ENABLE	0x0000_0000 (Enable JTAGLOCK)
Z1OTP_JTAGPSWDH1	0x0000_0000
Z1OTP_JTAGPSWDH0	0x0000_0000
Z1OTP_JTAGPSWDL1	0x0000_0000
Z1OTP_JTAGPSWDL0	0x0000_0000

**NOTE:** Devices with JTAGLOCK will limit TI's ability to perform a complete analysis for customer returns in the event of a device failure. You need to provide the JTAGLOCK password to TI along with the unit for analysis. If the permanent JTAGLOCK is used, TI will not be able to perform failure analysis.

**NOTE:** In this case LINKPOINTERS are also programmed with ALL\_0 values. This means last Zone Select Block (ZSB) has been used and security configurations cannot be changed any more on this device.

## 6 References

- Texas Instruments: [TMS320F2838x Microcontrollers Technical Reference Manual](#)

## IMPORTANT NOTICE AND DISCLAIMER

TI PROVIDES TECHNICAL AND RELIABILITY DATA (INCLUDING DATA SHEETS), DESIGN RESOURCES (INCLUDING REFERENCE DESIGNS), APPLICATION OR OTHER DESIGN ADVICE, WEB TOOLS, SAFETY INFORMATION, AND OTHER RESOURCES "AS IS" AND WITH ALL FAULTS, AND DISCLAIMS ALL WARRANTIES, EXPRESS AND IMPLIED, INCLUDING WITHOUT LIMITATION ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT OF THIRD PARTY INTELLECTUAL PROPERTY RIGHTS.

These resources are intended for skilled developers designing with TI products. You are solely responsible for (1) selecting the appropriate TI products for your application, (2) designing, validating and testing your application, and (3) ensuring your application meets applicable standards, and any other safety, security, regulatory or other requirements.

These resources are subject to change without notice. TI grants you permission to use these resources only for development of an application that uses the TI products described in the resource. Other reproduction and display of these resources is prohibited. No license is granted to any other TI intellectual property right or to any third party intellectual property right. TI disclaims responsibility for, and you will fully indemnify TI and its representatives against, any claims, damages, costs, losses, and liabilities arising out of your use of these resources.

TI's products are provided subject to [TI's Terms of Sale](#) or other applicable terms available either on [ti.com](#) or provided in conjunction with such TI products. TI's provision of these resources does not expand or otherwise alter TI's applicable warranties or warranty disclaimers for TI products.

TI objects to and rejects any additional or different terms you may have proposed.

Mailing Address: Texas Instruments, Post Office Box 655303, Dallas, Texas 75265  
Copyright © 2022, Texas Instruments Incorporated