

EFM32 加密/解锁流程

Energy Micro MCU

AN01010101 V1.00 Date: 2011/11/18

产品应用笔记

类别	内容
关键词	EFM32 芯片加密/解锁 Debug Lock Jlink STK
摘要	本文主要阐述 EFM32 芯片加密与解锁流程

修订历史

版本	日期	原因
V1.00	2011/11/18	创建文档

目 录

1. 概述.....	1
2. EFM32 加密/解锁工具	1
2.1 硬件工具.....	1
2.2 软件工具.....	2
3. 使用 STK 加密/解锁.....	3
3.1 硬件连接.....	3
3.1.1 STK 板载 MCU 芯片	3
3.1.2 外部 MCU 芯片.....	4
3.2 操作步骤.....	5
4. 使用 Jlink 加密/解锁.....	7
4.1 硬件连接.....	7
4.2 操作步骤.....	7
4.2.1 加密.....	7
4.2.2 解锁.....	9

1. 概述

EFM32 可以通过 SWD 调试口上锁达到禁止外部访问片内 Flash 的目的，使得芯片内的执行代码得到保护，不被非法访问者窃取。同时，也可以通过清除调试上锁字（Debug Lock Word, DLW），解锁调试口访问 Cortex-M3 内核的功能且片内 Flash 的代码将被擦除。

当调试访问被上锁，调试接口仍然保持可访问，但是连接到 Cortex-M3 内核的访问将被阻止。该访问机制将由 Authentication Access Port（AAP）控制，如图 1.1 所示。

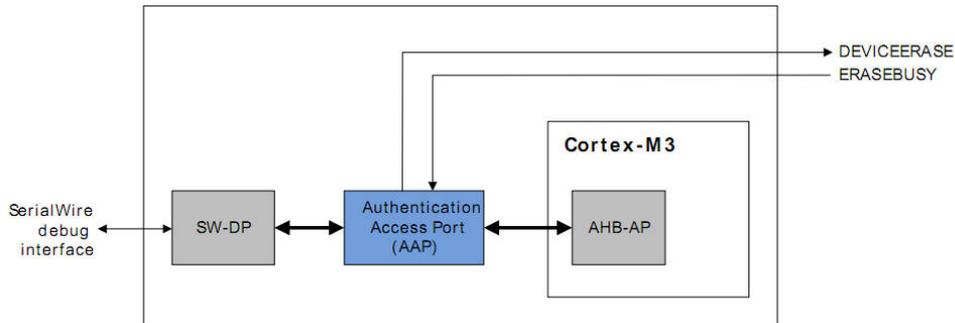


图 1.1 认证访问接口

设备解锁是通过写入 AAP_CMDKEY 寄存器，然后通过调试口将 AAP_CMD 寄存器标志位 DEVI CEERASE 位置 1 实现。该擦除操作擦除 Flash（main block），所有锁住位被复位且通过 AHB-AP 的调试口被使能。该操作在 40ms 内完成。需要注意在设备擦除操作中 SRAM 内容也将被删除。

调试器可以读取 AAP_STATUS 寄存器的状态。当在 AAP_CMD 寄存器的 DEVI CEERASE 被置 1 之后，ERASEBUSY 被置 1，调试器可以置 1 AAP_CMD 寄存器的 SYSRESETREQ 位。在复位之后，调试器恢复通过 AHB-AP 的正常调试会话。

注意：

如果调试引脚被重新配置为 I/O 功能而不是调试功能时，设备擦除将不再被执行。引脚在复位状态下被配置为调试功能。

2. EFM32 加密/解锁工具

EFM32 的加密/解锁可以通过带 SWD 接口且支持 EFM32 Flash 编程操作的仿真器或编程器执行。常见的使用工具有 EFM32 TinyGecko/Gecko STK 开发板和通用 Jlink 仿真器。下面将分别以 STK 板载 Jlink 仿真器和通用 Jlink 仿真器进行说明 EFM32 的加密和解锁步骤。

2.1 硬件工具

图 2.1 所示为带有板载 Jlink 仿真器的 EFM32 Tiny Gecko STK 开发板。图 2.2 所示为带板载仿真器的 EFM32 Gecko STK 开发板。图 2.3 所示为通用的 Jlink 仿真器。

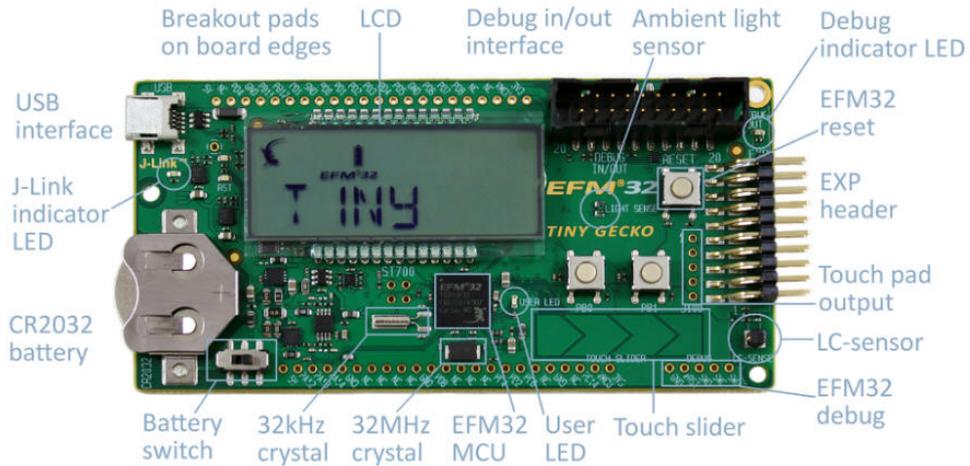


图 2.1 Tiny Gecko STK 开发板

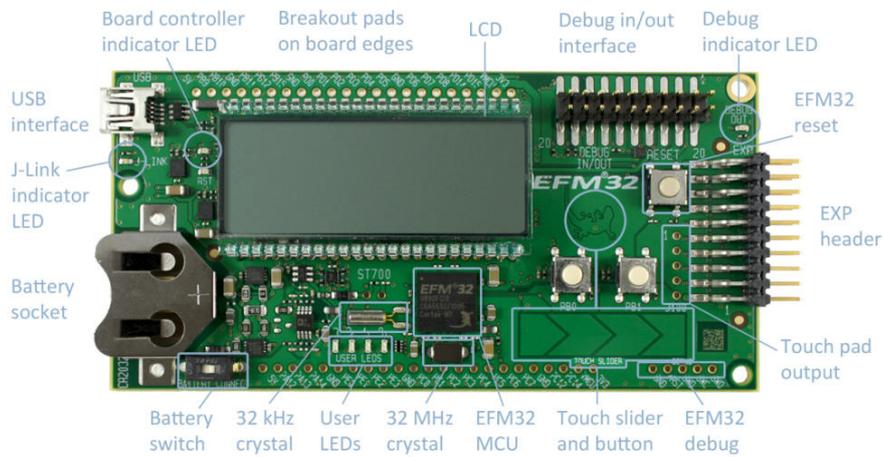


图 2.2 Gecko STK 开发板



图 2.3 通用 Jlink 仿真器

2.2 软件工具

使用 STK 开发板上的板载仿真器进行加密/解锁的用户可以使用 Simplicity Studio 软件上自带的 energyAware Commander 软件进行芯片的加密/解锁，如图 2.4 所示。使用通用 Jlink

仿真器的用户可以使用 Seeger JLink-ARM 驱动软件包中自带的 Jlink Commander 软件, 如图 2.5 所示。为了支持 EFM32 以下操作, 请安装 JLink-ARM 4.36e 版本或以上版本。

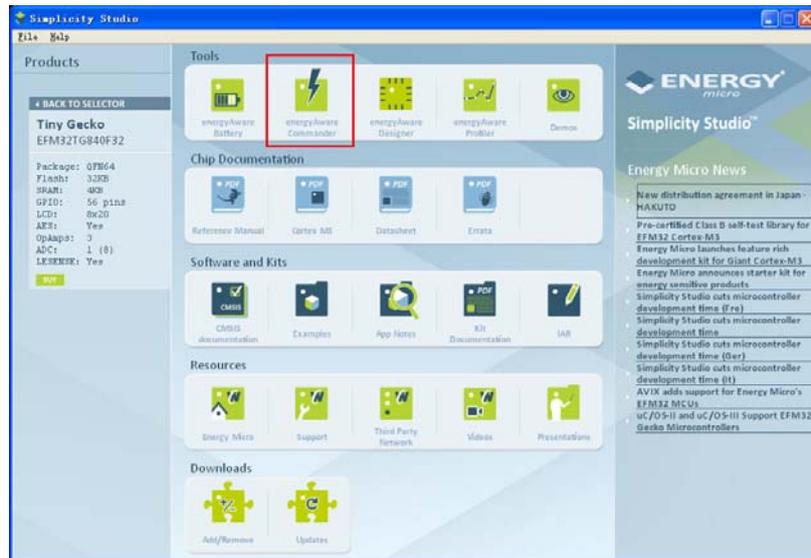


图 2.4 Simplicity Studio 软件

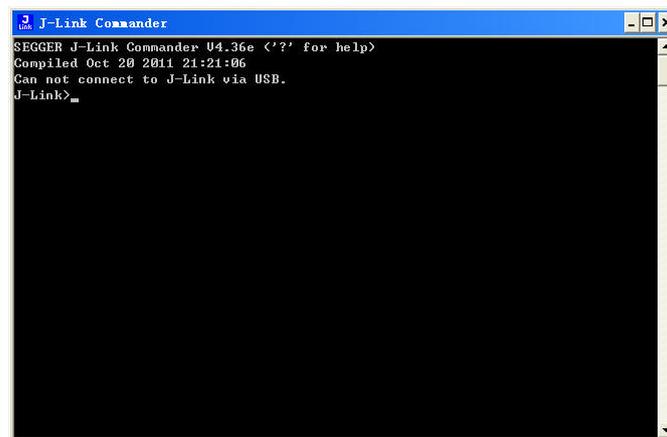


图 2.5 J-Link Commander 软件

3. 使用 STK 加密/解锁

下面将以 EFM32 Gecko STK 开发板为例阐述 STK 加密、解锁的详细步骤。

3.1 硬件连接

根据硬件连接方式的不同可以分为两种情况: STK 板载仿真器仿真板载 MCU; STK 板载仿真器仿真 STK 外部 MCU。

3.1.1 STK 板载 MCU 芯片

EFM32 Gecko STK 开发板板载仿真器与板载 MCU 连接已内部连接, 因此用户只需将开发板与电脑通过 miniUSB 口的进行连接, 并将供电选择开关 (电池座旁边) 拨向 MCU 方向即可。当连接正确且开发板供电正常时, 在电脑的设备管理器端可以看到 JLink 仿真器被正确识别出来。

在 energyAware Commder 软件的【Debug Mode】配置时，将选项配置为【MCU】模式，以便用户可以使用板载 Jlink 仿真器对 STK 开发板上的 MCU 进行所需的仿真调试操作。

3.1.2 外部 MCU 芯片

用户需要使用 STK 仿真开发板外部的 EFM32 芯片，需要进行硬件连接和软件配置。操作步骤如下：

(1)使用导线将STK 开发板上或下方的 VMCU 引脚连接到 20pin 引脚的 Debug In/Out 插座的第 1 脚，使得 STK 开发板为外部系统提供 3.3V 电源；图 3.1 所示为 STK 开发板上 20pin Debug In/Out 插座与外部 EFM32 芯片的连接示意图。用户可使用杜邦线将其中的 6 个引脚相连，也可以通过 20Pin 的排线将 STK 开发板与外部 MCU 系统进行连接。

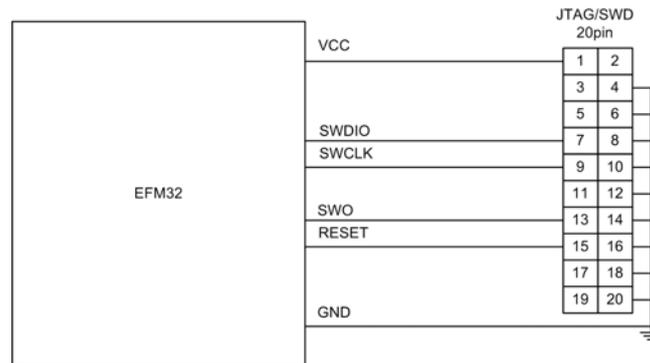


图 3.1 JTAG/SWD 接口连接示意图

(2) 打开 energyAware Commder 软件时，在配置仿真器【Debug mode】时，在下拉列表中选择【Out】模式，如图 3.2 所示。STK 开发板上 Debug 接口旁边的 DEBUG OUT LED 指示灯将点亮。

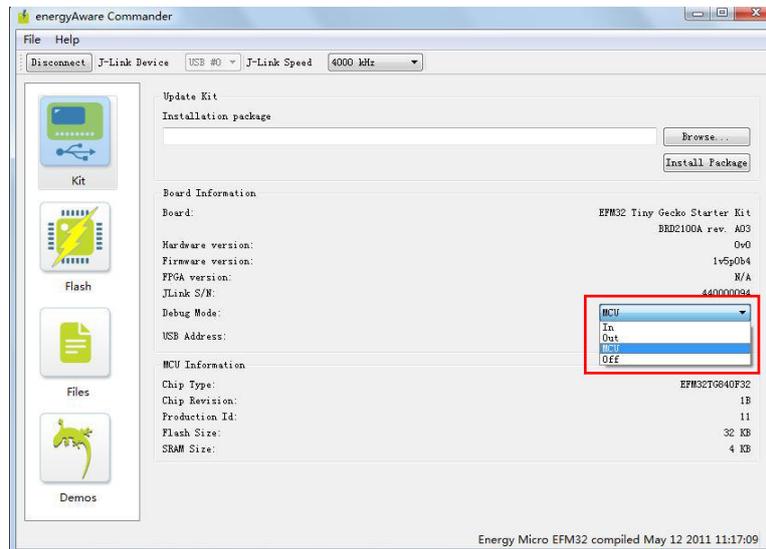


图 3.2 配置板载 Jlink 仿真器为 Debug Out 模式

注意：对于 STK 开发板板载仿真器的【Debug Mode】配置为软件配置，STK 开发板掉电后会丢失，因此再次使用时需要重复执行相同的软件配置步骤。

3.2 操作步骤

下面以 EFM32 Gecko 开发板的加密/解锁流程为例，进行详细阐述。

- (1) 按照前文描述的硬件连接步骤，将仿真器与 MCU 的调试接口进行正确连接。
- (2) 将 STK 开发板的 USB 接口连接到 PC 端，运行 energyAware Commander 软件，并点击【Connect】按钮，如图 3.3 所示。

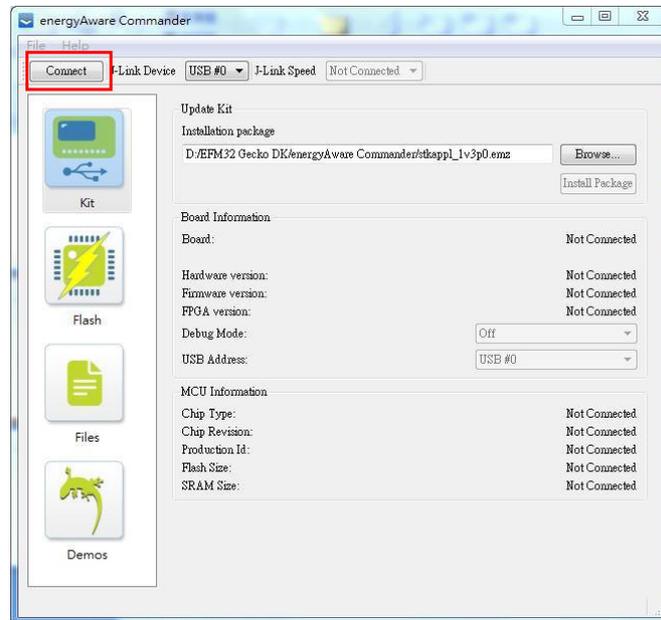


图 3.3 连接板载仿真器

- (3) 当 STK 开发板与被仿真调试的 MCU 进行正确连接时，可以在【Board Information】和【MCU Information】栏看到仿真器和 MCU 的信息，如图 3.4 所示。

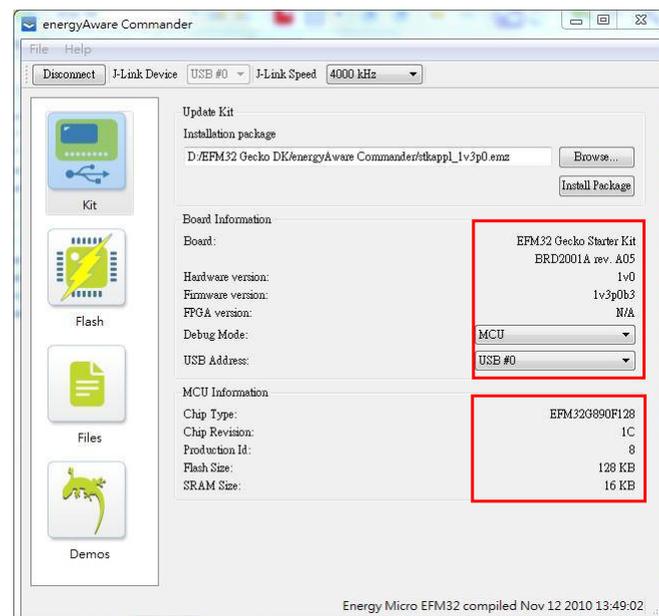


图 3.4 仿真器与 MCU 信息

- (4) 根据硬件连接所描述，按需求选择仿真器的【Debug Mode】，仿真 STK 开发板上

的 MCU 选择【MCU】选项；仿真 STK 开发板外部的 MCU 可选择【Out】选项，如图 3.5 所示。

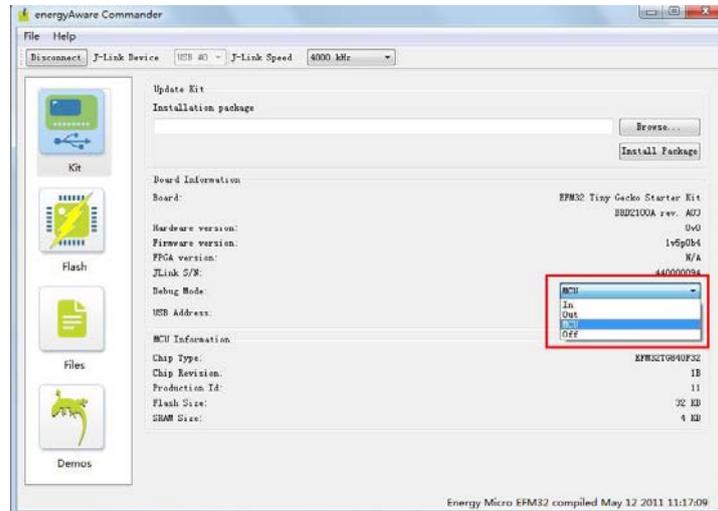


图 3.5 配置仿真器 Debug Mode

(4) 点击窗口左边的【Flash】选项页，切换的 Flash 操作界面。在【Debug Lock Tools】栏中，可以点击【Lock debug access】按钮，将目标 MCU 的 SWD 接口上锁，禁止外部访问片内的 Flash，如图 3.6 所示。需要注意的是，当芯片的调试口被上锁后，芯片不能够再进行仿真和调试操作，必须执行解锁擦除操作。

(5) 图 3.6 所示，点击【Debug Lock Tools】栏中的【Unlock debug access】按钮即可将芯片的 SWD 接口解锁，同时，芯片片内的 Flash 代码将被擦除且 RAM 上数据也会丢失。

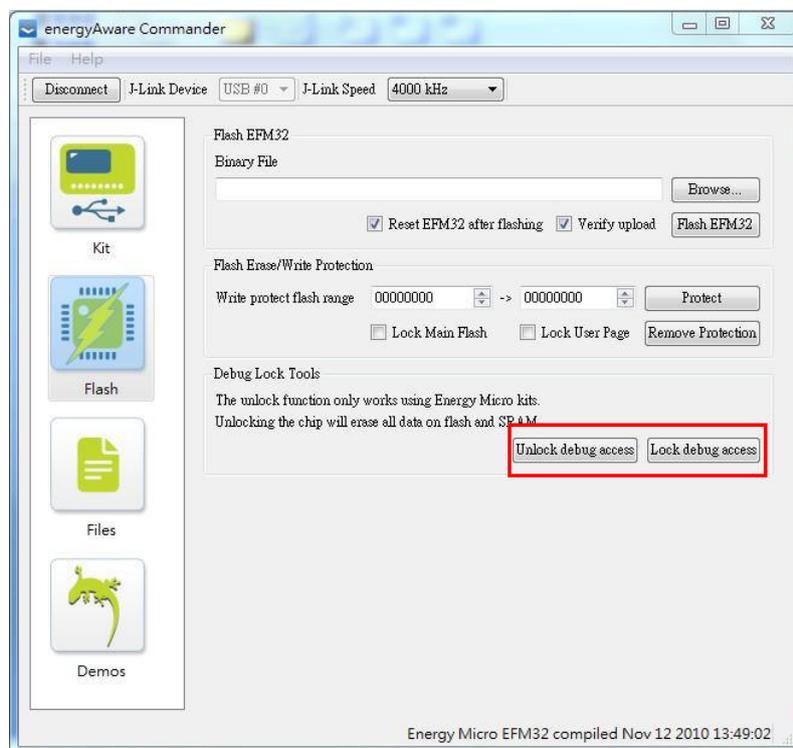


图 3.6 Debug Lock/unlok 操作

按照以上步骤操作即可将目标 MCU 的 SWD 调试接口进行上锁或解锁，从而达到保护芯片内 Flash 不被非法用户窃取。

4. 使用 Jlink 加密/解锁

下面将以通用仿真器 JLink 加密和解锁 EFM32 TG840F32 芯片为例，阐述详细的操作步骤。

4.1 硬件连接

用户使用导线或连接座将 JLink 仿真器的 20pin 调试仿真接口与 EFM32 的系统进行连接，如图 4.1 所示。

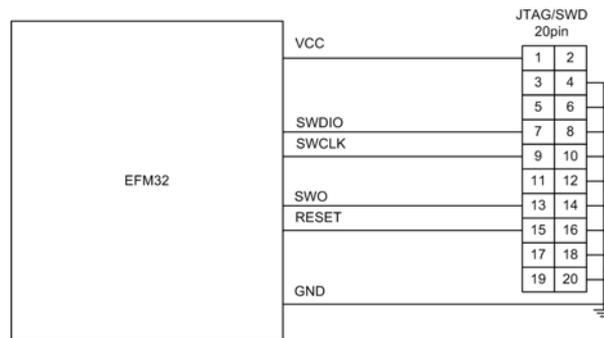


图 4.1 JLink 仿真器 JTAG/SWD 接口与 MCU 连接

技巧提示:

如果 EFM32 STK 开发板上的板载仿真器出现故障，无法正常对 MCU 进行加密/解锁操作，也可以按照本小节描述的步骤执行加密/解锁操作。其中，必须将 STK 开发板的板载仿真器与 STK 板载 MCU 连接断开，又或将板载仿真器通过 energyAware Commder 软件，将其【Debug Mode】软件设置为【In】模式。

4.2 操作步骤

通用 JLink 仿真器与 energyAware Commder 软件配套使用时，只能对芯片 SWD 调试接口进行上锁加密，不能进行解锁操作。下面将分两部分分别描述：

4.2.1 加密

(1)按照前文硬件连接要求将 JLink 仿真器的调试接口与 MCU 系统调试接口进行连接。然后将仿真器连接到电脑的 USB 端口上，并将 EFM32TG840 系统上电。

(2)运行 Simplicity Studio 软件中的 energyAware Commder 软件，点击界面左上方的【Connect】按钮，将仿真器与开发板连接上。在【Board Information】栏将没有 JLink 仿真器的信息，在【MCU Information】栏可以看到芯片的型号和序列号等信息，如图 4.5 所示。

(3)点击界面中左边的【Flash】选项页，在【Debug Lock Tools】栏中【unlock Debug Access】按钮将是灰色无效状态，【Lock Debug Access】为有效状态。点击【Lock Debug Access】按钮即可将目标 MCU 的 SWD 接口进行上锁，如图 4.3 所示。

(4)若芯片 Debug 接口上锁成功，那么界面中将弹出如图 4.4 所示对话框。

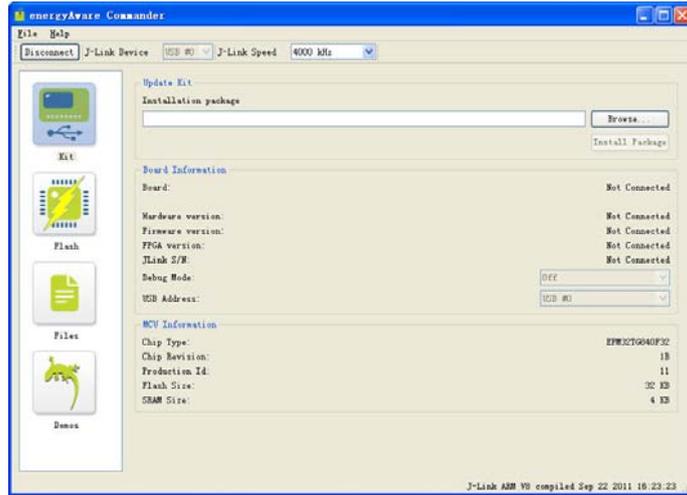


图 4.2 连接仿真器与 energyAware Commdr 软件

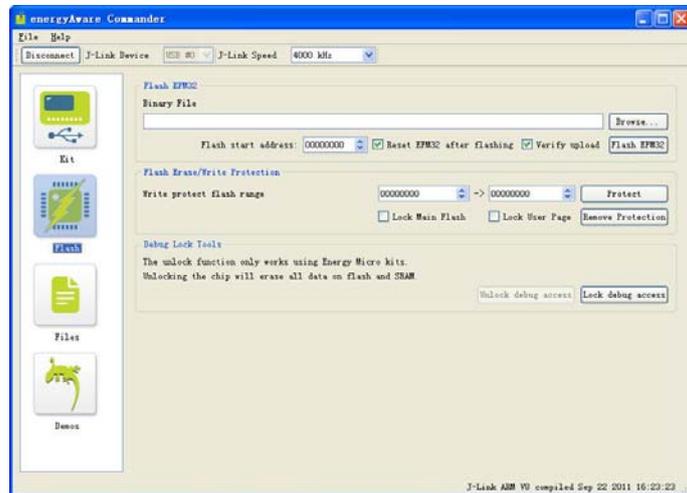


图 4.3 Lock Debug Access 操作

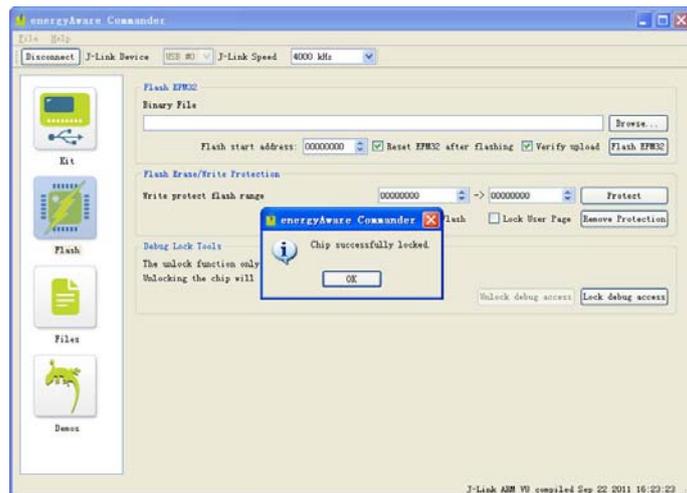


图 4.4 Debug Lock 成功

芯片 SWD 接口上锁后，使得片内的 Flash 被保护，外部仿真器或编程器无法访问到片内 Flash 的内容。

4.2.2 解锁

(1)按照前文硬件连接要求将 JLink 仿真器的调试接口与 MCU 系统调试接口进行连接。然后将仿真器连接到电脑 USB 端口上，并将 EFM32TG840 系统上电；

(2) 运行 JLink ARM 软件中的 JLink Commdr 软件，如图 4.5 所示。

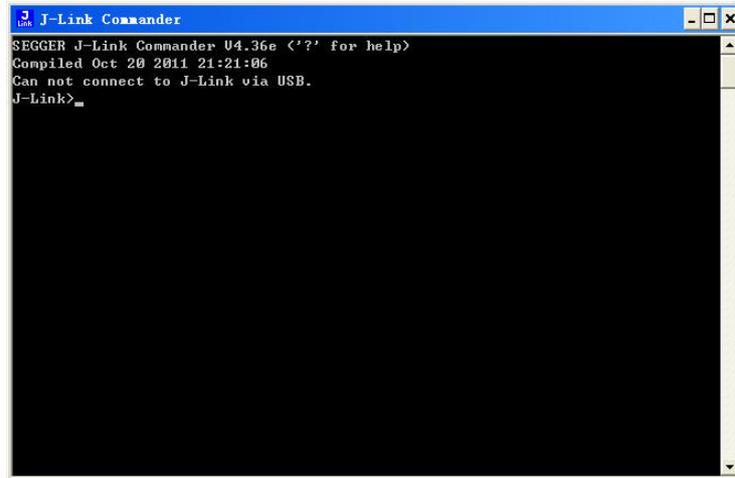


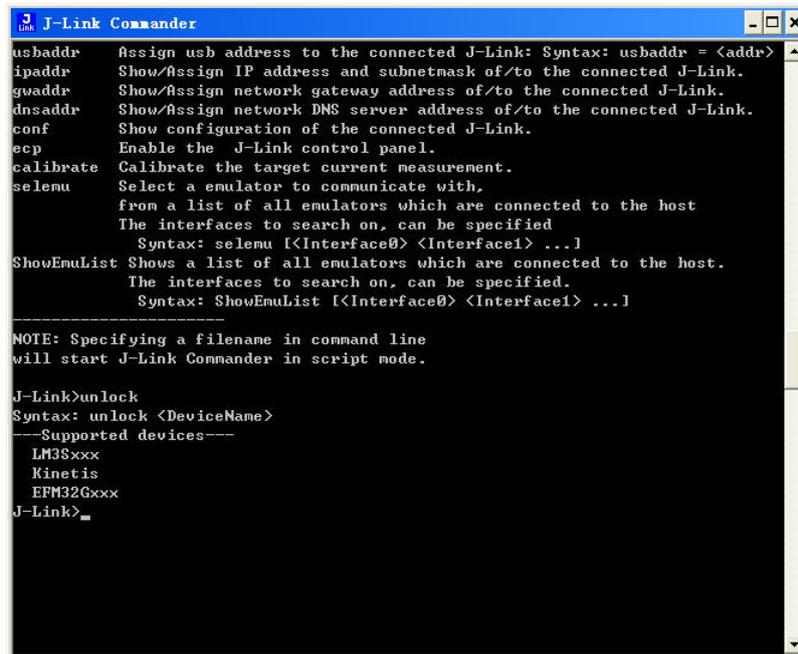
图 4.5 JLink Commdr 软件

(3) 在 Dos 命令行界面中输入“?”(问号)，界面中将显示相关命令行操作帮助。其中，Unlock 命令为对芯片执行解锁操作的命令，如图 4.6 所示。



图 4.6 JLink Commdr 命令

(4) 在命令行中输入: unlock, 输入回车键, 界面将提示支持解锁的器件类型, 如图 4.7 所示。



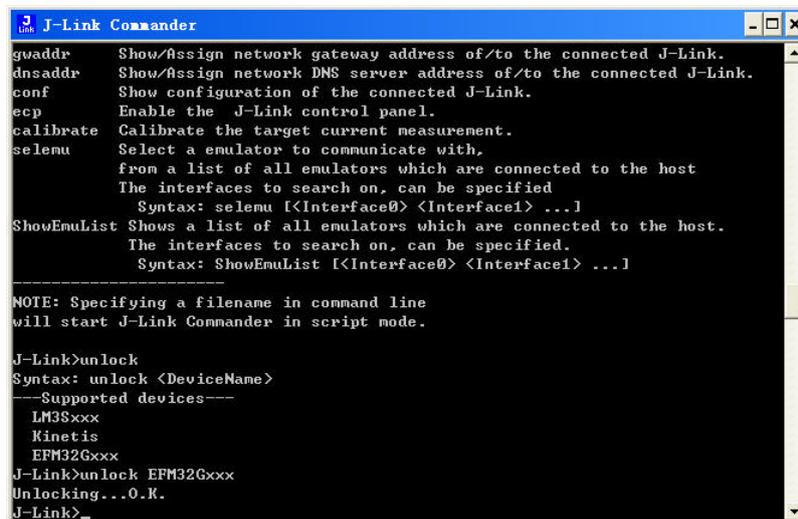
```
J-Link Commander
usbaddr  Assign usb address to the connected J-Link: Syntax: usbaddr = <addr>
ipaddr   Show/Assign IP address and subnetmask of/to the connected J-Link.
gwaddr   Show/Assign network gateway address of/to the connected J-Link.
dnsaddr  Show/Assign network DNS server address of/to the connected J-Link.
conf     Show configuration of the connected J-Link.
ecp      Enable the J-Link control panel.
calibrate Calibrate the target current measurement.
selemu   Select a emulator to communicate with,
          from a list of all emulators which are connected to the host
          The interfaces to search on, can be specified
          Syntax: selemu [<Interface0> <Interface1> ...]
ShowEmuList Shows a list of all emulators which are connected to the host.
          The interfaces to search on, can be specified.
          Syntax: ShowEmuList [<Interface0> <Interface1> ...]

NOTE: Specifying a filename in command line
will start J-Link Commander in script mode.

J-Link>unlock
Syntax: unlock <DeviceName>
---Supported devices---
LM3Sxxx
Kinetis
EFM32Gxxx
J-Link>
```

图 4.7 Unlock 命令操作

(5) 按 unlock 命令提示输入: unlock EFM32Gxxx, 然后输入回车键, 命令行界面中将返回 unlock OK 的指示, 如图 4.8 所示。



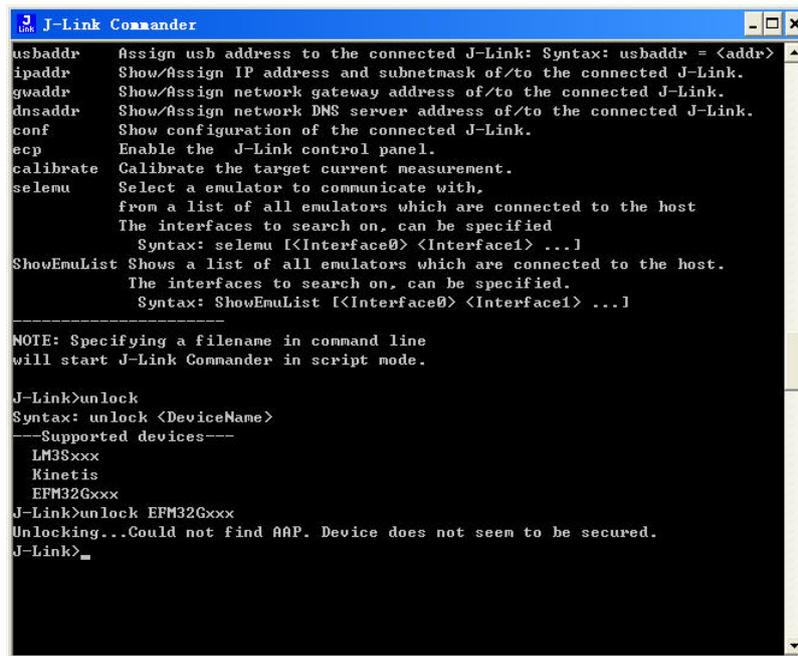
```
J-Link Commander
gwaddr   Show/Assign network gateway address of/to the connected J-Link.
dnsaddr  Show/Assign network DNS server address of/to the connected J-Link.
conf     Show configuration of the connected J-Link.
ecp      Enable the J-Link control panel.
calibrate Calibrate the target current measurement.
selemu   Select a emulator to communicate with,
          from a list of all emulators which are connected to the host
          The interfaces to search on, can be specified
          Syntax: selemu [<Interface0> <Interface1> ...]
ShowEmuList Shows a list of all emulators which are connected to the host.
          The interfaces to search on, can be specified.
          Syntax: ShowEmuList [<Interface0> <Interface1> ...]

NOTE: Specifying a filename in command line
will start J-Link Commander in script mode.

J-Link>unlock
Syntax: unlock <DeviceName>
---Supported devices---
LM3Sxxx
Kinetis
EFM32Gxxx
J-Link>unlock EFM32Gxxx
Unlocking...OK.
J-Link>
```

图 4.8 解锁成功

至此, 目标 EFM32 MCU 解锁成功, 芯片的 SWD 调试接口已被解锁且片内 Flash、RAM 代码将被擦除。芯片恢复 SWD 接口调试仿真功能。在解锁过程中, 若出现如图 4.9 所示的情况, 请重复执行以上解锁步骤。



```
J-Link Commander
usbaddr  Assign usb address to the connected J-Link: Syntax: usbaddr = <addr>
ipaddr   Show/Assign IP address and subnetmask of/to the connected J-Link.
gwaddr   Show/Assign network gateway address of/to the connected J-Link.
dnsaddr  Show/Assign network DNS server address of/to the connected J-Link.
conf     Show configuration of the connected J-Link.
ecp      Enable the J-Link control panel.
calibrate Calibrate the target current measurement.
selemu   Select a emulator to communicate with,
          from a list of all emulators which are connected to the host
          The interfaces to search on, can be specified
          Syntax: selemu [<Interface0> <Interface1> ...]
ShowEmuList Shows a list of all emulators which are connected to the host.
          The interfaces to search on, can be specified.
          Syntax: ShowEmuList [<Interface0> <Interface1> ...]

NOTE: Specifying a filename in command line
will start J-Link Commander in script mode.

J-Link>unlock
Syntax: unlock <DeviceName>
---Supported devices---
  LM3Sxxx
  Kinetis
  EFM32Gxxx
J-Link>unlock EFM32Gxxx
Unlocking...Could not find AAP. Device does not seem to be secured.
J-Link>_
```

图 4.9 AAP 访问失败