GigaDevice Semiconductor Inc.

GD32H7xx 系列安全存储管理

应用笔记

AN113

目录

图索引

表索引

1. 简介

GD32H7xx 系列除安全保护（SPC），扇区擦除/编程保护（WP）和仅执行的专用代码读保护区域（DCRP）外，也提供了闪存加解密方案和安全模式用以保护数据及代码。安全模式可以支持预授权固件安装（LFI）、安全启动和预授权固件更新（LFU），也可以支持用户自定义的安全应用开发。

2. 闪存加解密方案

GD32H7xx 系列为片上 flash 和外部 OSPI flash 提供了 AES（128）算法加解密的方案。

片上 flash 和外部 OSPI flash 有着类似的保护机制，加密都由软件工具实现，解密都由硬件实现。加密时，都需要用户使用 Gigadevice 提供的软件工具在写入代码或数据前完成外部加密。

默认状态下解密功能都是未使能的。

对于片上 flash，用户可以通过使能 efuse 用户控制段中的 AESEN 位来打开 AES 解密功能，并通过 FMC_AESIVx_MDF 寄存器来设置初始向量中的高 96 位，而 AES 秘钥也由 efuse 设置。配置完成后，读取代码或数据时硬件会自动解密，用户不用参与解密过程。

注意：通过配置 FMC_NODEC 寄存器可以划分一块非解密区，当该区域有效时，即便 AESEN 位为 1，该区域也不进行解密操作。

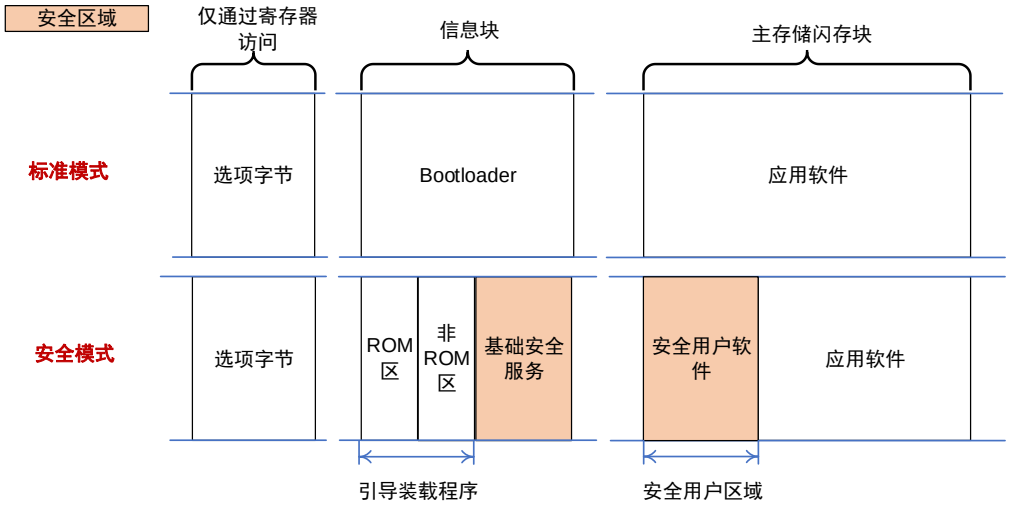
对于外部 OSPI flash，用户可以通过 RTDEC 模块来进行解密。配置完成后，读取代码或数据时硬件会自动解密，用户不用参与解密过程。更多有关 OSPI 解密的内容，请参考 ***AN122 GD32H7xx 系列 MCU OSPI flash 执行环境用户指南***。

3. 安全模式

对某些敏感程序设置安全保护是有必要的，以避免潜在的恶意软件攻击。例如，预授权固件更新软件需要高度的保护，因为它处理其他进程无法检索的机密数据（如加密秘钥）。

MCU 提供了具有限制访问特性的安全存储区。在该区域里能够构建，可以在任何用户应用程序之前执行的安全服务。只有在设备配置为安全模式时，才能访问这些安全区域及其包含的软件。*图 3-1. 标准模式和安全模式内部存储架构*显示了该区域的详细信息。

图 3-1. 标准模式和安全模式内部存储架构



其中，安全用户区域在复位后被访问一次，且区域内代码执行完成后将被隐藏。基础安全服务是配置安全服务的 Gigadevice 软件。安全用户软件位于安全用户区域，复位后执行一次。安全用户软件可以实现安全启动和预授权固件更新。

安全模式和安全用户区域可以通过选项字节或 efuse 配置。用户可以通过基础安全服务去设置选项字节中的安全用户区域，从而把安全代码和数据配置在安全用户区域。

3.1. 安全启动流程

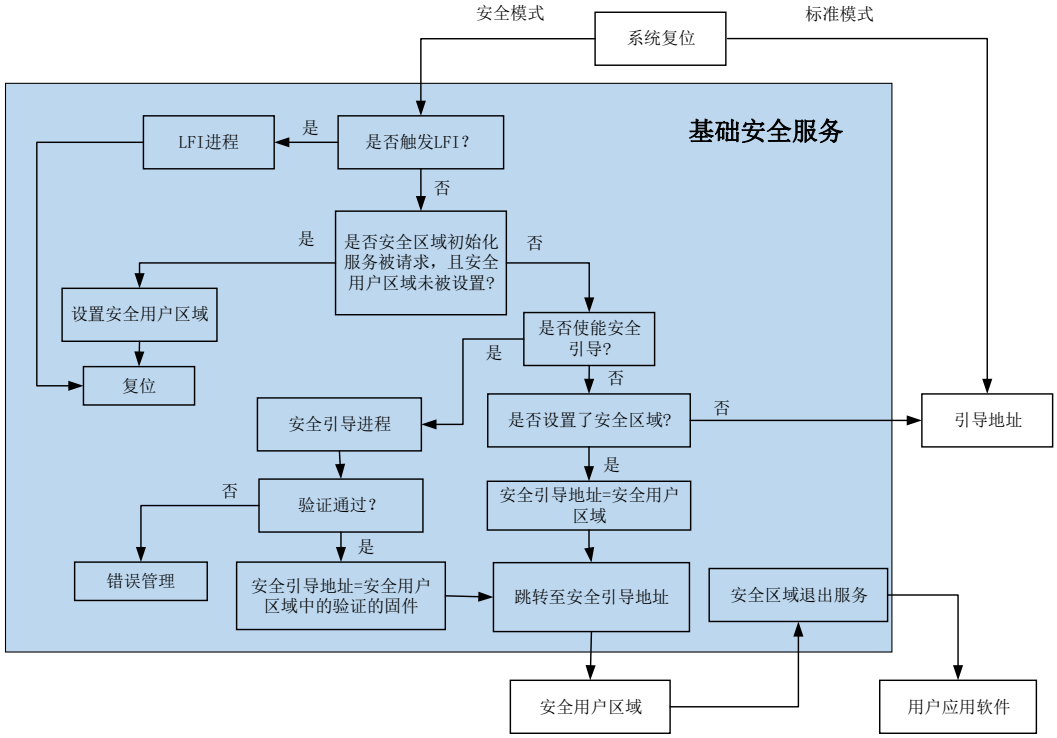
在安全模式下，安全固件存储在信息块中，以支持引导。安全用户软件是存储在主存储闪存块中的安全应用代码、数据或算法。

如果没有配置安全用户区域，则安全引导装载程序将跳转至由 FMC_BTADDR_EFT 寄存器中的 BOOT_ADDR0[15:0]选项字节决定的引导地址。

在安全模式下，MCU 无论引导配置如何（BOOT 引脚及 BOOT 地址），都会强制从安全 ROM 区启动。

具体启动流程如*图 3-2. 安全启动流程*所示。

图 3-2. 安全启动流程



更多有关预授权固件安装的内容，请参考 ***AN118 GD32H7xx 系列预授权固件安装概述***。

更多有关预授权固件更新的内容，请参考 ***AN119 GD32H7xx 系列预授权固件更新概述***。

更多有关安全启动的内容，请参考 ***AN120 GD32H7xx 系列安全启动概述***。

3.2. 安全服务配置

只要选项字节或 efuse 中的 SCR 位有一个位被置为了 1，安全模式都将被启用，此时 FMC_OBSTAT0_EFT 寄存器的 SCR 位为 1。且启用后需要系统复位来激活安全模式。

与 efuse 配置不同，选项字节中的 SCR 位可以修改，如果不存在有效的 DCRP 区域或安全用户区域，选项字节中的 SCR 位可以自由清 0。否则，选项字节中的 SCR 清 0 的唯一方式是：在 DCRP_EREN 位（FMC_DCRPADDR_EFT 或 FMC_DCRPADDR_MDF 寄存器中）为 1，且 SCR_EREN 位（FMC_SCRADDR_EFT 或 FMC_SCRADDR_MDF 寄存器中）为 1 时，去执行 SPC 降级。否则，将会产生选项字节修改错误（OBMERR）。

当选项字节的 SCR 位为 1 而 efuse 中的 SCR 位不为 1 时，可以返回标准模式，若要返回标准模式，在清除 SCR 选项位之前或在清除 SCR 选项位的同时，需要移除安全用户区域和 DCRP 区域。具体操作详见相关选项字节的修改规则。

4. 安全用户软件

4.1. 访问权限

安全用户软件存储在安全用户区域中，只能在安全模式下访问。安全用户软件是会在复位后由安全引导装载程序调用执行的安全代码，在系统复位后，安全用户软件将构建用户安全启动、软件许可检查、安全固件更新和安全初始化等内容。

安全用户软件执行后，若代码跳转到了用户的主（非安全）应用程序中，安全用户区域的内容将会被禁止访问。退出安全区域前必须通过调用 exitSecureAreas 安全函数来实现跳转，其中一个输入参数是退出后要跳转的主应用程序的地址。

一旦进入应用程序代码，尝试对一个安全用户区域进行读操作时，读保护错误(RSERR)将会置位，且中止当前的读操作。

4.2. 安全用户区域配置

可以通过设置粒度为 4KB 字节的 SCR_AREA_END[10:0]和 SCR_AREA_START[10:0]选项字节来定义一个安全用户区域。实际安全用户区域大小由以下公式定义：

安全用户区域大小 = [(SCR_AREA_END[10:0] - SCR_AREA_START[10:0]) + 1] x 4Kbytes.

如果 SCR_AREA_END[10:0]等于 SCR_AREA_START[10:0]，整个主存储闪存块都是安全用户区域。

如果 SCR_AREA_END[10:0]小于 SCR_AREA_START[10:0]，安全用户区域为空。

除选项字节外，也可以通过修改 efuse 中的用户控制段对安全用户区域进行配置，其粒度为 32KB 字节。

注意：efuse 的安全配置优先级高于闪存的选项字节，所以在产品中，如果采用选项字节配置安全用户区域时，应该保持 efuse 中的安全用户区域的起始/结束地址都设置为 0，并将 efuse 中 SCRLK 位置 1，否则可能会导致安全区域有漏洞。

当通过选项字节配置安全用户区域，并且区域地址有效时，安全用户区域的代码可以更新安全用户区域的大小。

5. 基础安全服务

基础安全服务提供了安全区域设置函数和安全区域退出函数。

5.1. 安全区域设置函数

安全区域设置函数是由 Gigadevice 提供用来执行安全区域初始化的函数，在标准模式下运行时，可以通过直接调用函数（resetAndInitializeSecureAreas）来设置安全用户区域，而其他基础安全服务不允许访问。

表 5-1. 函数 resetAndInitializeSecureAreas 见下表：

表 5-1. 函数 resetAndInitializeSecureAreas

函数名称	resetAndInitializeSecureAreas
函数原型	void resetAndInitializeSecureAreas(BSS_secure_area_struct area);
功能描述	根据SCR_AREA_START和SCR_AREA_END选项字节来配置安全用户区域范围。
先决条件	-
被调用函数	-
输入参数{in}	
area	安全用户区域起始及结束地址
输出参数{out}	
-	-
返回值	
-	-

注意：在函数完成后,将产生系统复位。此函数仅在首次设置安全用户区域时才可使用。用户应该保证目标安全区域内有正确的安全程序，使其能够退出到标准程序，否则会造成芯片报废。

5.2. 安全区域退出函数

Gigadevice提供了一个跳转到用户应用程序的函数（exitSecureArea）。它允许安全地关闭安全用户区域，以保证安全区域的内容不再被访问。

*表5-2. 函数exitSecureArea*见下表:

表 5-2. 函数 exitSecureArea

函数名称	exitSecureArea
函数原型	void exitSecureArea(unsigned int vectors, unsigned int jtagState);
功能描述	从安全用户区域退出并跳转到主用户应用程序
先决条件	-
被调用函数	-
输入参数{in}	

vectors	退出后要跳转的应用程序向量的地址
输入参数{in}	
jtag_state	退出安全用户区域后的JTAG的状态
BSS_EXIT_SCR_JTAG_ENABLE	退出安全用户区域后使能JTAG
BSS_EXIT_SCR_JTAG_DISABLE	退出安全用户区域后失能JTAG
输出参数{out}	
-	-
返回值	
-	-

注意：在函数完成后,将不会产生系统复位。出于安全考虑，用户在安全用户区域调用此函数前应禁用缓存。

6. 存储保护总结

*图 6-1. 闪存保护区域*为各保护区域之间的关系。

图 6-1. 闪存保护区域

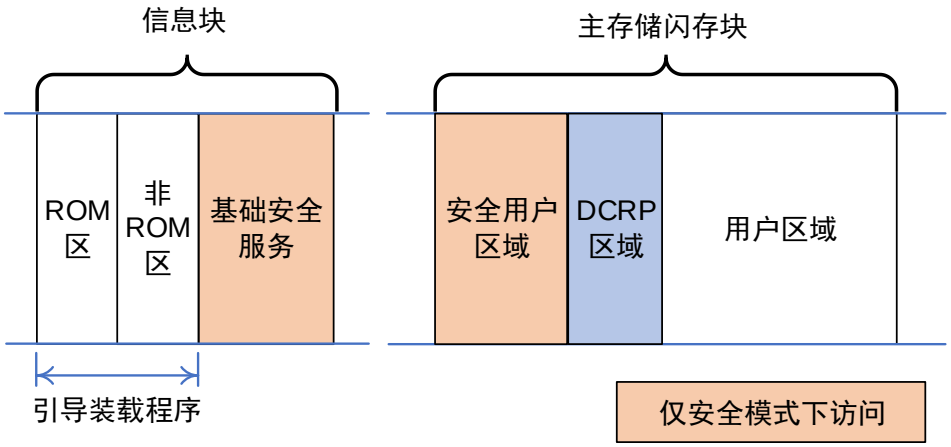


*表 6-1. 安全存储保护访问权限*总结了各保护区域的访问权限。

表 6-1. 安全存储保护访问权限

区域	模式	操作	访问权限
DCRP	标准或安全模式	执行	有
		读	无
		调试	无
安全用户区域	安全模式	执行	复位后代码执行完之前有权限
		读	复位后代码执行完之前有权限
		调试	无
基础安全服务	安全模式	执行	复位后代码执行完之前有权限
		读	复位后代码执行完之前有权限
		调试	无

7. 版本历史

表 7-1. 版本历史

版本号.	说明	日期
1.0	首次发布	2023 年 04 月 18 日

Important Notice

This document is the property of GigaDevice Semiconductor Inc. and its subsidiaries (the "Company"). This document, including any product of the Company described in this document (the "Product"), is owned by the Company under the intellectual property laws and treaties of the People's Republic of China and other jurisdictions worldwide. The Company reserves all rights under such laws and treaties and does not grant any license under its patents, copyrights, trademarks, or other intellectual property rights. The names and brands of third party referred thereto (if any) are the property of their respective owner and referred to for identification purposes only.

The Company makes no warranty of any kind, express or implied, with regard to this document or any Product, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. The Company does not assume any liability arising out of the application or use of any Product described in this document. Any information provided in this document is provided only for reference purposes. It is the responsibility of the user of this document to properly design, program, and test the functionality and safety of any application made of this information and any resulting product. Except for customized products which has been expressly identified in the applicable agreement, the Products are designed, developed, and/or manufactured for ordinary business, industrial, personal, and/or household applications only. The Products are not designed, intended, or authorized for use as components in systems designed or intended for the operation of weapons, weapons systems, nuclear installations, atomic energy control instruments, combustion control instruments, airplane or spaceship instruments, transportation instruments, traffic signal instruments, life-support devices or systems, other medical devices or systems (including resuscitation equipment and surgical implants), pollution control or hazardous substances management, or other uses where the failure of the device or Product could cause personal injury, death, property or environmental damage ("Unintended Uses"). Customers shall take any and all actions to ensure using and selling the Products in accordance with the applicable laws and regulations. The Company is not liable, in whole or in part, and customers shall and hereby do release the Company as well as it's suppliers and/or distributors from any claim, damage, or other liability arising from or related to all Unintended Uses of the Products. Customers shall indemnify and hold the Company as well as it's suppliers and/or distributors harmless from and against all claims, costs, damages, and other liabilities, including claims for personal injury or death, arising from or related to any Unintended Uses of the Products.

Information in this document is provided solely in connection with the Products. The Company reserves the right to make changes, corrections, modifications or improvements to this document and Products and services described herein at any time, without notice.