GigaDevice Semiconductor Inc.

GD32H7 系列 MCU OSPI Flash 执行环境
用户指南

应用笔记

AN122

1.1 版本

（2024 年 3 月）

目录

图索引

表索引

1. 前言

OSPI 是可以用来连接外部存储器，支持单线，双线，四线和八线 SPI 存储器，可工作在三种模式：间接模式，状态轮询模式，内存映射模式。

本文档用于介绍 OSPI 使用的有关方法，以及有关的工具软件和注意事项。

2. 硬件资源

2.1. OSPI

GD32H7xx 系列 MCU 最多提供了 OSPI0 和 OSPI1 两个 OSPI 接口。

当 OSPI 工作在间接模式下，使用 OSPI 的寄存器执行所有的操作。在状态轮询模式下，MCU 周期性读取并检测外部存储器的状态寄存器值。

在内存映射模式下，外部存储器被映射到 MCU 的地址空间（OSPI0 的映射地址为 0x9000 0000，OSPI1 的映射地址为 0x7000 0000），MCU 可以和访问内部存储器一样访问 SPI 存储器。

2.2. 实时解密（RTDEC）模块

GD32H7xx 系列 MCU 最多提供了 RTDEC0 和 RTDEC1 两个 RTDEC，每个 RTDEC 可以配置四个独立、不同的加密区域。每个 OSPI 接口可以对应一个 RTDEC，在 OSPI 存储器映射模式下，读取 OSPI Flash 数据时，使用 AES-128 CTR 模式实时解密。

3. IDE 下载算法

Gigadevice 官方 pack 包提供了在 keil 和 IAR 中向 OSPI Flash 下载数据的算法，安装 pack 可通过 keil 和 IAR 向 OSPI Flash 下载数据。

4. BootLoader 支持

GD32H7xx MCU 内置的 Bootloader 支持往 OSPI Flash 中烧录数据，具体参考 ***AN126_GD32H7xx_BootLoader 操作注意事项***。

5. 从 OSPI Flash 启动

5.1. OSPI Flash 支持

OSPI 支持 SDR（单倍数据速率）和 DTR（双倍传输速率）两种模式。

5.1.1. SDR 模式

单线模式：支持 GD 系列 SPI flash，例如 GD25Q127C，GD25Q16E，GD25Q32E，GD25Q64F，GD25F64F。

四线模式：支持 GD 系列 SPI flash，例如 GD25Q127C，GD25Q16E，GD25Q32E，GD25Q64F，GD25F64F。

八线模式：支持 GD 系列八线 SPI flash，例如 GD25X，GD25LX。

5.1.2. DTR 模式

八线模式：支持 GD 系列八线 SPI flash，例如 GD25X，GD25LX。

5.2. OSPI 启动配置

5.2.1. OSPI 引导模式选择

GD32 MCU 提供不同的引导源，可通过 BOOT 管脚电平和 FMC_BTADDR_MDF 寄存器的 BOOT_ADDR0/1[15:0]进行选择。详情见***表 5-1. 引导模式选择***和***表 5-2. 引导模式详细描述***。BOOT 引脚的电平状态会在复位后的第四个 CK_SYS(系统时钟)的上升沿进行锁存。用户可自行选择所需要的引导源，通过设置上电复位和系统复位后的 BOOT 的引脚电平。一旦这个引脚电平被采样，它们可以被释放并用于其他用途。

在 BOOT 引脚电平确定的情况下，从 OSPI 启动需要将 BOOT_ADDRx[15:0]配置为 0x7000

或 0x9000。

表 5-1. 引导模式选择

引导源地址	启动模式选择引脚
	BOOT
引导地址高位：由BOOT_ADDR0[15:0]定义 引导地址低位：0x0000	0
引导地址高位：由BOOT_ADDR1[15:0]定义 引导地址低位：0x0000	1

表 5-2. 引导模式详细描述

SCR	SPC[7:0]	BOOT_ADDRESS（在BOOT_ADDRx(x = 0,1)配置）	BOOT_MODE	启动地址
1	x	XXXX	SECURITY BOOT	ROM
0	安全保护等级高	0x9000_0000	USER BOOT	OSPI0
		0x7000_0000	USER BOOT	OSPI1
		0x0800_0000~max user flash	USER BOOT	BOOT_ADDRESS
		其他地址	USER BOOT	0x0800_0000
	无保护状态/安全保护等级低	0x9000_0000	USER BOOT	OSPI0
		0x7000_0000	USER BOOT	OSPI1
		0x2408_000 max RAM shared(ITCM/DTCM/AXI)	SRAM BOOT(RAM shared)	BOOT_ADDRESS
		0x2400_0000~ max AXI SRAM	SRAM BOOT(AXI SRAM)	BOOT_ADDRESS
		0x2000_0000	SRAM BOOT(DTCM)	0x2000_0000
		0x0800_0000~max user flash	USER BOOT	BOOT_ADDRESS
		0x0000_0000	SRAM BOOT(ITCM)	0x0000_0000
		0x1FF0_0000	SYSTEM BOOT	BootLoader
		其他地址	USER BOOT	0x0800_0000(BOOT Pin = 0)
			SYSTEM BOOT	BootLoader(BOOT Pin = 1)

5.2.2. OSPI 启动 GPIO 映射

从 OSPI 启动使用到的 OSPI Flash GPIO 如*表 5-3. OSPI GPIO 引脚*所示，暂不支持使用其它引脚。

表 5-3. OSPI GPIO 引脚

OSPI0	GPIO 引脚	OSPI1	GPIO
OSPI0_IO0	PD11	OSPI1_IO0	PF0
OSPI0_IO1	PD12	OSPI1_IO1	PF1
OSPI0_IO2	PA3	OSPI1_IO2	PF2
OSPI0_IO3	PD13	OSPI1_IO3	PF3
OSPI0_IO4	PD4	OSPI1_IO4	PG0
OSPI0_IO5	PD5	OSPI1_IO5	PG1
OSPI0_IO6	PD6	OSPI1_IO6	PG10
OSPI0_IO7	PD7	OSPI1_IO7	PG11
OSPI0_CLK	PB2	OSPI1_CLK	PF4
OSPI0_NCS	PB6	OSPI1_NCS	PG12

5.2.3. OSPI 启动参数

OSPI Flash 启动时，可以从 OSPI 中读取相关参数：

1. OSPI 通讯模式选择：1 线，2 线，4 线或者 8 线 OSPI；
2. 通讯速率；
3. OSPI 使用 STR 或者 DTR 模式；
4. OSPI 对应的 RTDEC 相关配置；
5. 是否开 cache；
6. 选项字节的配置。

5.3. OSPI 启动模式的安全支持

为了数据安全，从 OSPI 启动时，OSPI Flash 中的文件受保护，并且可以将 MCU 与 OSPI Flash 绑定。

5.3.1. OSPI Flash 中的文件受保护

OSPI Flash 中的文件由系统区和数据区组成，由 Gigadevice 支持的软件工具将用户的原始文件生成。

系统区

系统区是一个 4K 字节的空间，在 OSPI 闪存的第一个扇区中进行编程。该区域始终加密，有 2 种加密模式，公共模式和用户模式。

- 公共模式：该模式采用 AES-256 方式对 OSPI 引导系统区进行加密。采用 Gigadevice 自由加密模式和秘钥，对所有用户开放。
- 用户模式：该模式采用 AES-128 方式对 OSPI 引导系统文件进行加密。KEY/IV 由用户自定义，KEY 设置在 EFUSE_AES_KEYX，IV 设置在 FMC_AESIVX_MDF。

数据区

数据区是一个自由空间，用户可以选择加密或不加密。以及一些加密区域和一些非加密区域的组合。

每个 OSPI 接口对应一个 RTDEC 模块用于解密数据，每个 RTDEC 模块可以支持最多 4 个区域，每个区域可以使用由用户定制的 KEY 和 IV。

5.3.2. OSPI Flash 与 MCU 的绑定

GD32H7xx 系列允许将 OSPI Flash 与 MCU 绑定，以防止客户的产品被抄袭和程序被篡改。如果开启此功能，第一次启动时 MCU 会自动完成绑定，后续每次启动都会识别 MCU ID，如果不匹配则无法工作。因此，即使是同一类型的产品，OSPI Flash 也无法在任何其他产品中工作，且加密区不能被篡改。如果想要更换 MCU，但仍然使用该 OSPI Flash 芯片，用户需要重新初始化 OSPI Flash 中的文件。

6. GD32H7xx LFIx 简介

LFIx（Licensed Firmware Install X）有关资源用于支持 GD32H7xx 系列 OSPI Flash 固件安装，分为公共加密模式和客户加密模式。无论哪种模式，OSPI Flash 中除了客户指定的区域外，数据始终处于加密状态。

公共加密模式简洁，高效，采用 Gigadevice 自有加密模式和秘钥，对所有用户开放。

用户加密模式在 HSM（Hardware Secure Module）的支持下，全过程完全使用用户自定义的密码和参数完成加密。

Gigadevice 为了支持客户开发和量产，准备了相应的工具，可以实现在线和离线量产。具体软件操作参考 ***AN133_GD32H7 系列 MCU 安全固件生成器使用指南***文档。

6.1. OSPI Flash 文件结构

将 OSPI Flash 分为系统区和数据区，其中数据区又可以划分成 9 个可选的用户区，并且大小由用户自定义，但要符合对齐要求，如***表 6-1. OSPI Flash 中文件结构***所示：

表 6-1. OSPI Flash 中文件结构

序号	名称	描述
0	系统区	4KB，地址固定为 0x90000000（OSPI0）或 0x70000000（OSPI1）。
1	用户区 1	可选，非加密数据区。
2	用户区 2	可选，加密数据区。基于 AES-128 CTR 模式加密，由 RTDECx 区域 y 实时解密。
3	用户区 3	可选，非加密数据区。
4	用户区 4	可选，加密数据区。基于 AES-128 CTR 模式加密，由 RTDECx 区域 y 实时解密。
5	用户区 5	可选，非加密数据区。
6	用户区 6	可选，加密数据区。基于 AES-128 CTR 模式加密，由 RTDECx 区域 y 实时解密。
7	用户区 7	可选，非加密数据区。
8	用户区 8	可选，加密数据区。基于 AES-128 CTR 模式加密，由 RTDECx 区域 y 实时解密。
9	用户区 9	可选，非加密数据区。

6.2. 公共加密模式

公共加密模式中，所有使用 GD32H7xx 的产品全部采用 Gigadevice 私有的加密解决方案。Gigadevice 私有的加密解决方案基于 AES 256/128 加密，客户程序和数据根据 LFIx 不同阶段采用独立的加密参数，加盐后再加密，对于重要参数采用多层加密，实现相对安全的快速开发和低成本生产。

6.2.1. 公共加密程序文件结构

公共加密模式下，文件结构如*表 6-2. 公共加密程序文件结构*所示：

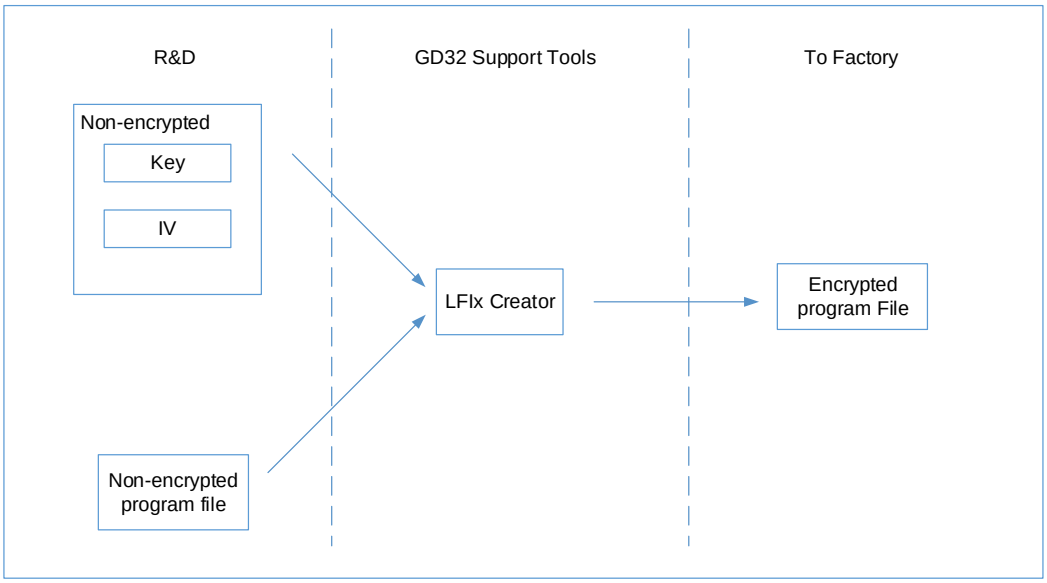
表 6-2. 公共加密程序文件结构

序号	名称	R&D 数据	到工厂数据
0	系统区	4KB	基于 AES 256 的 Gigadevice 私有的加密解决方案。
1	用户区 1	可选，非加密数据区。	不处理
2	用户区 2	可选，加密数据区。	不处理
3	用户区 3	可选，非加密数据区。	不处理
4	用户区 4	可选，加密数据区。	不处理
5	用户区 5	可选，非加密数据区。	不处理
6	用户区 6	可选，加密数据区。	不处理
7	用户区 7	可选，非加密数据区。	不处理
8	用户区 8	可选，加密数据区。	不处理
9	用户区 9	可选，非加密数据区。	不处理

6.2.2. 公共加密量产资源准备

所有使用 GD32H7xx 的产品使用相同的加密解决方案，需要使用到 gigadevice 支持的工具，如*图 6-1. 公共加密结构图*所示：

图 6-1. 公共加密结构图



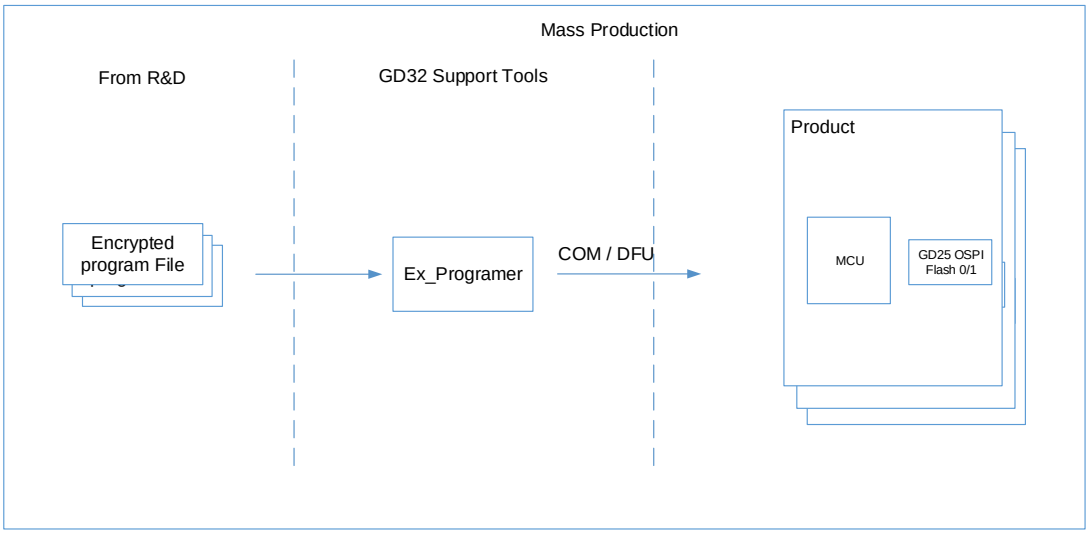
6.2.3. 量产支持

为了支持客户开发和量产，准备了相应的工具，可以实现在线和离线量产。

在线量产

公共加密模式下，在线量产如*图 6-2. 公共加密在线量产结构图*所示：

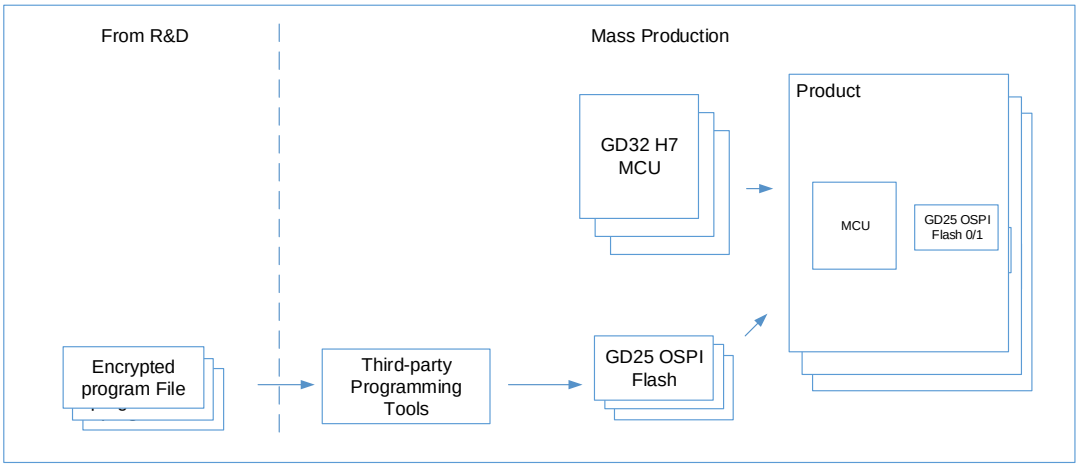
图 6-2. 公共加密在线量产结构图



离线量产

公共加密模式下，离线量产如*图 6-3. 公共加密离线量产结构图*所示：

图 6-3. 公共加密离线量产结构图



6.3. 用户加密模式

此模式需要签署有关协议以后才能查看所有资料，请与 Gigadevice 联系。

6.3.1. 用户加密程序文件结构

用户加密模式下，文件结构如*表 6-3. 用户加密加密程序文件结构*所示：

表 6-3. 用户加密加密程序文件结构

序号	名称	R&D 数据	到工厂数据
0	系统区	4KB	采用用户自定义秘钥进行加密，该秘钥被编程到目标 MCU 的 EFUSE
1	用户区 1	可选，非加密数据区。	不处理
2	用户区 2	可选，加密数据区。	不处理
3	用户区 3	可选，非加密数据区。	不处理
4	用户区 4	可选，加密数据区。	不处理
5	用户区 5	可选，非加密数据区。	不处理
6	用户区 6	可选，加密数据区。	不处理
7	用户区 7	可选，非加密数据区。	不处理
8	用户区 8	可选，加密数据区。	不处理
9	用户区 9	可选，非加密数据区。	不处理

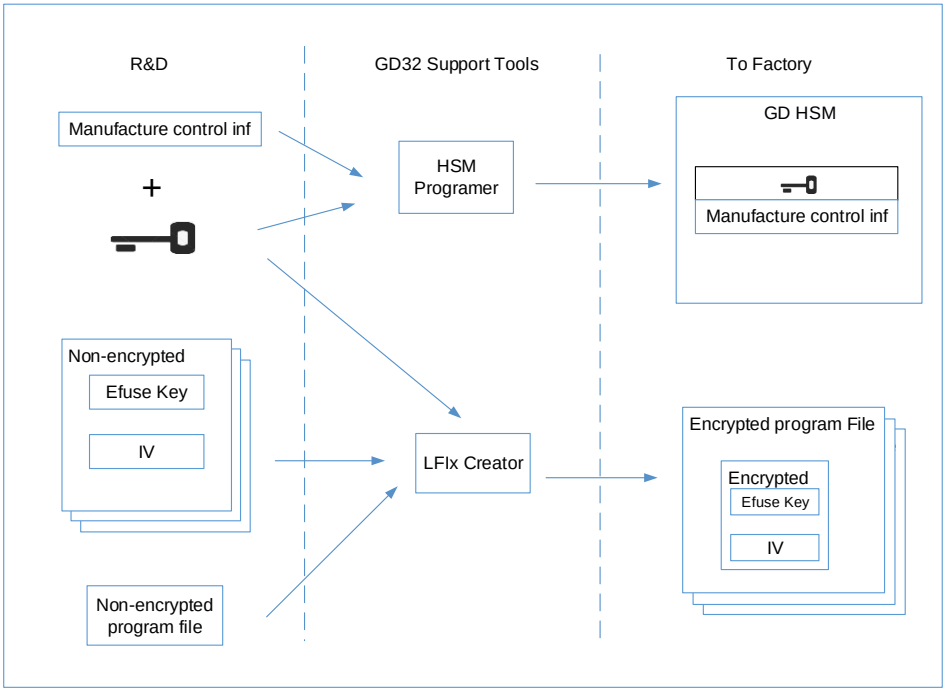
6.3.2. 用户加密量产资源准备

所有使用 GD32H7xx 的产品使用客户自定义的加密解决方案，需要使用到 HSM 和 LFIx Creater 工具，用户加密模式可以对每个产品使用独立加密参数或根据产品类型加密。可以同时提供产品生产数量控制。

独立加密

独立加密模式下，可以实现客户每个产品 ID 使用不同的加密参数，如*图 6-4. 独立加密结构图*所示：

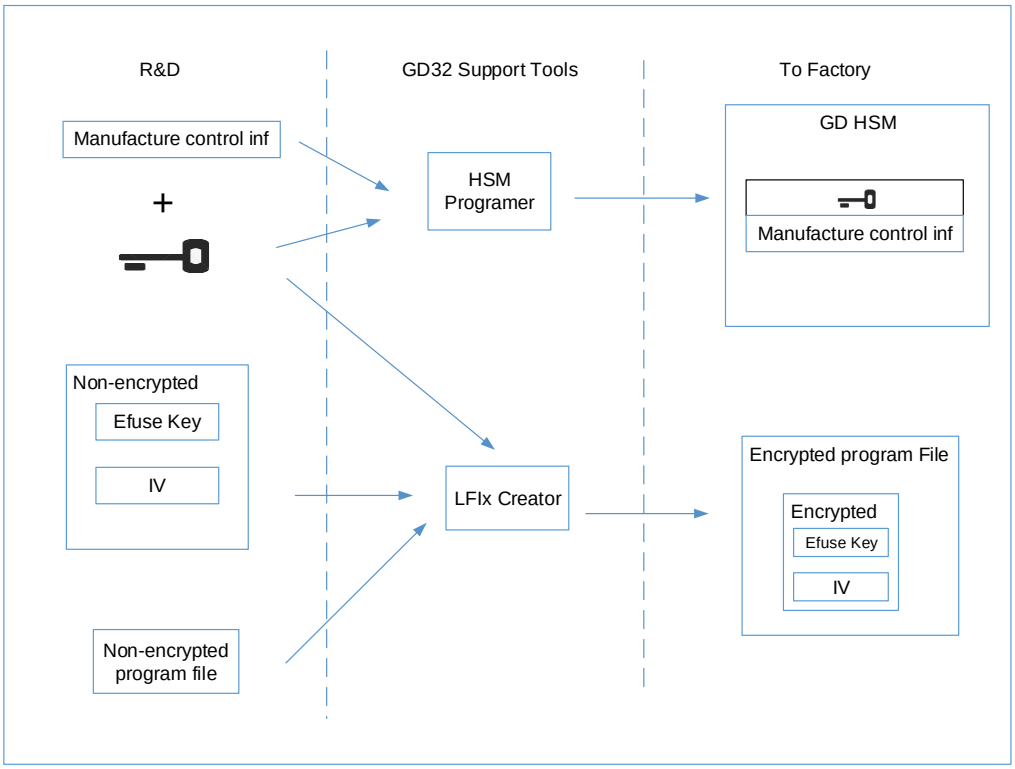
图 6-4. 独立加密结构图



基于产品类型加密

该加密模式下，可以实现客户每个产品类型使用相同的加密参数，如*图 6-5. 根据产品类型加密结构图*所示：

图 6-5. 根据产品类型加密结构图

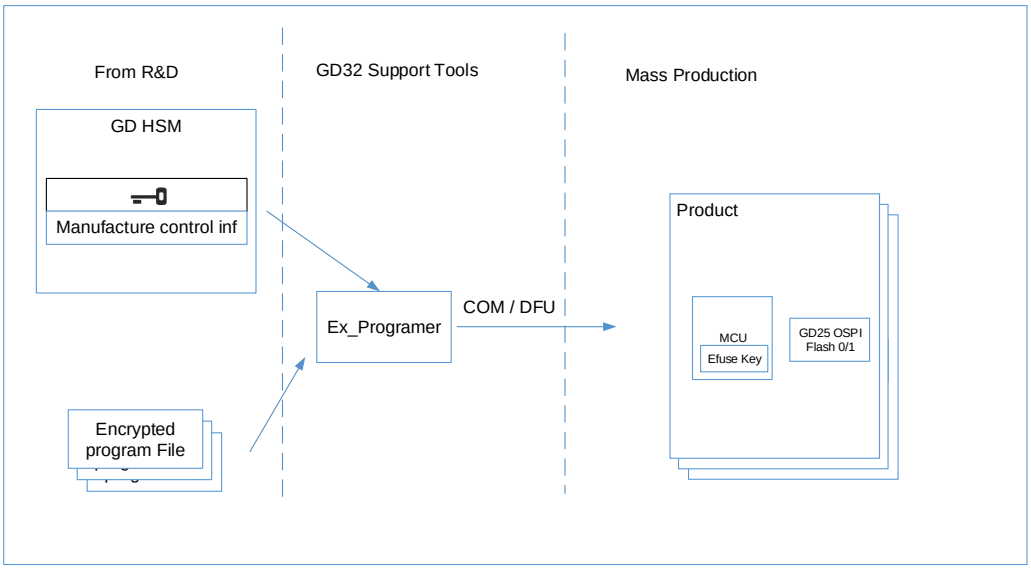


6.3.3. 量产支持

在线量产

用户加密模式下，在线量产如*图 6-6. 用户加密在线量产结构图*所示：

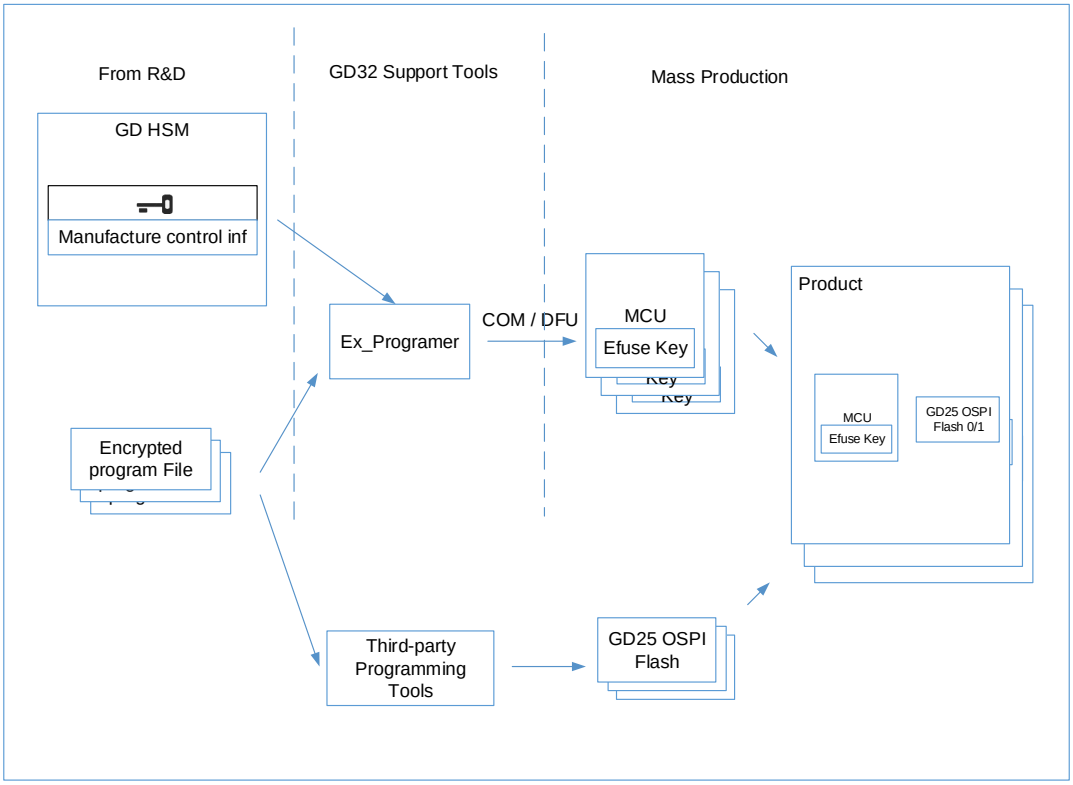
图 6-6. 用户加密在线量产结构图



离线量产

用户加密模式下，离线量产如*图 6-7. 用户加密离线量产结构图*所示，MCU 和 Flash 在烧写完成后需要保证一一对应。

图 6-7. 用户加密离线量产结构图



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 4 月 20 日
1.1	1. 更新***表 5-3. OSPI GPIO 引脚*** OSPI0_IO2 为 PA3。	2024 年 3 月 8 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.