GRPLT Lite配置工具自定义固件加密及应用介绍

版本： **1.2**

发布日期： **2022-06-27**

深圳市汇顶科技股份有限公司

商标声明

GOODiX 和其他汇顶商标均为深圳市汇顶科技股份有限公司的商标。本文档提及的其他所有商标或注册商标，由各自的所有人持有。

免责声明

本文档中所述的器件应用信息及其他类似内容仅为您提供便利，它们可能由更新之信息所替代。确保应用符合技术规范，是您自身应负的责任。

深圳市汇顶科技股份有限公司（以下简称“GOODIX”）对这些信息不作任何明示或暗示、书面或口头、法定或其他形式的声明或担保，包括但不限于针对其使用情况、质量、性能、适销性或特定用途的适用性的声明或担保。GOODIX对因这些信息及使用这些信息而引起的后果不承担任何责任。

未经GOODIX书面批准，不得将GOODIX的产品用作生命维持系统中的关键组件。在GOODIX知识产权保护下，不得暗中或以其他方式转让任何许可证。

深圳市汇顶科技股份有限公司

总部地址：深圳市福田保税区腾飞工业大厦B座2层、13层

电话：+86-755-33338828　　传真：+86-755-33338099

网址：www.goodix.com

前言

编写目的

本文档介绍如何通过GR551x SDK包中提供的固件加密示例工程修改自定义加密算法，实现自定义固件加密，并启动对应加密流程，以便客户深入了解GRPLT Lite配置工具自定义固件加密应用及其流程。

读者对象

本文适用于以下读者：

- GR551x用户
- GR551x开发人员
- GR551x测试人员
- 文档工程师

版本说明

本文档为第3次发布，对应的产品系列为GR551x。

修订记录

版本	日期	修订内容
1.0	2021-06-28	首次发布
1.1	2022-02-20	更新软件界面截图
1.2	2022-06-27	更新软件名称

目录

1 简介

GRPLT Lite配置工具自定义加密固件相较于Goodix加密方式，用户能够采用自定义加密算法，并将该算法生成的密钥写入芯片，实现加密逻辑的独立控制；应用时用户可根据加密算法反推密钥正确性，推动加密固件的顺利运行，为用户产品提供安全保障。

在进行操作前，可参考以下文档。

表 1-1 文档参考

名称	描述
GRPLT Lite配置工具用户手册	介绍GRPLT Lite配置工具的安装和使用方法
GR551x固件升级指南	介绍GR551x的固件升级原理和应用

2 应用自定义加密固件

GR551x SDK包中提供加密示例工程ble_enc_app_template，其中加密指令响应及GU串口交互逻辑均已实现。用户只需简单操作，便可实现自定义固件加密。

说明:

- GRPLT Lite配置工具自定义加密功能暂只支持特定的1.6.02 SDK版本，如为其他SDK版本，因与烧录配置不匹配，可能造成自定义加密失败。
- GU（Golden Unit）是指已经校准过的BLE模块。

---

1. 生成用户自定义加密固件。具体操作，详见2.1 修改加密算法和2.2 编译自定义加密示例工程。
2. 启用自定义固件加密流程。具体操作，详见2.3 启动自定义加密流程。

2.1 修改加密算法

加密示例工程中的custom_enc_info()函数传入16字节chip_uid，通过自定义加密算法生成32字节加密信息，从而将enc_key写入User Region区域。用户需要根据加密信息待写入区域，修改加密示例工程ble_enc_app_template中的对应算法函数：

- 若加密信息需写入eFuse的User Region区域（前32字节）：修改*enc_key.c*文件中自定义加密方式相关的加密算法custom_enc_info()函数。
- 若加密信息需写入NVDS或其他Flash区域：修改*enc_key.c*文件中的custom_enc_info()函数和*custom_enc.c*文件中的custom_enc_process()函数。

2.2 编译自定义加密示例工程

修改加密算法后，用户可直接编译工程；编译完成后，`SDK_Folder\projects\peripheral_app\ble_enc_app_template\project\Keil_5\build`目录下将生成自定义加密固件*ble_enc_app_template_fw.bin*。

说明:

SDK_Folder为GR551x SDK的根目录。

2.3 启动自定义加密流程

1. 下载自定义加密固件。
   (1) 将编译生成的加密固件*ble_enc_app_template_fw.bin*拷贝至GRPLT Lite配置工具软件包中的对应文件夹。

说明:

加密固件需放入的文件夹，请参考《GRPLT Lite配置工具用户手册》。

---

(2) 运行*GRPLT Lite Config Tool.exe*，进入“可选功能配置 > 加密算法配置”面板，勾选“用户自定义加密方式”后，点击“导入bin文件”，导入拷贝至软件包中的自定义加密固件*ble_enc_app_template_fw.bin*。

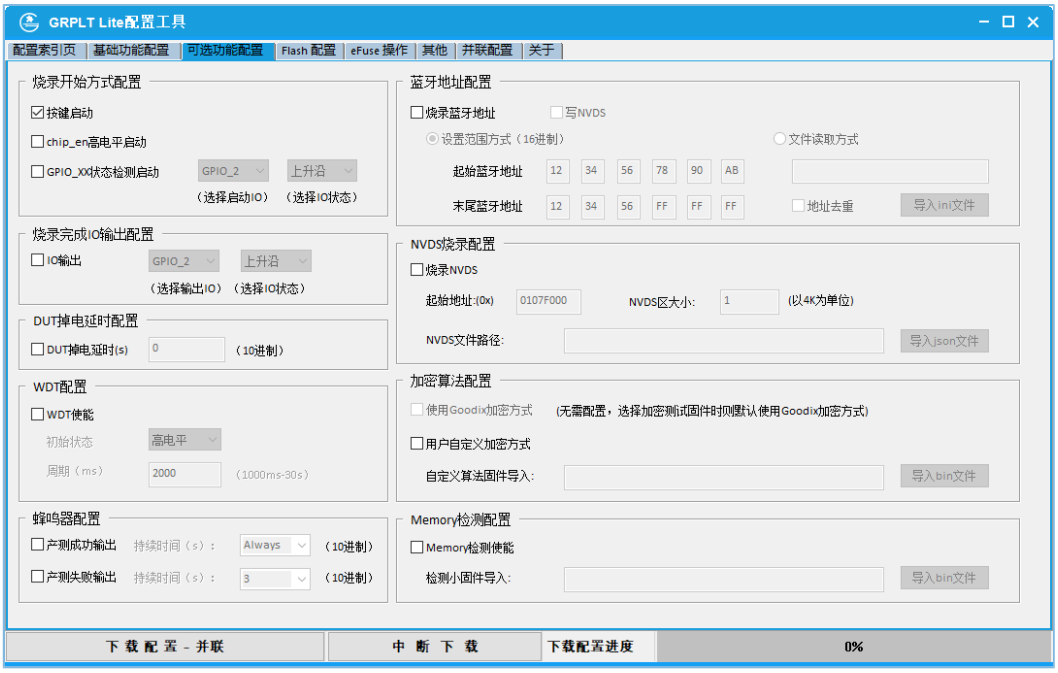

图 2-1 导入自定义加密固件

(3) 点击GRPLT Lite配置工具左下角的“下载配置-并联”按钮，启动配置下载。

配置下载完成后，关闭GRPLT Lite配置工具。

2. 运行加密固件，启动离线烧录。

连接离线板和DUT，并单击离线板下方的K2或K5按键，开始自定义加密固件的离线烧录流程。关于K2和K5按键的区别，请参考《GRPLT Lite配置工具用户手册》。

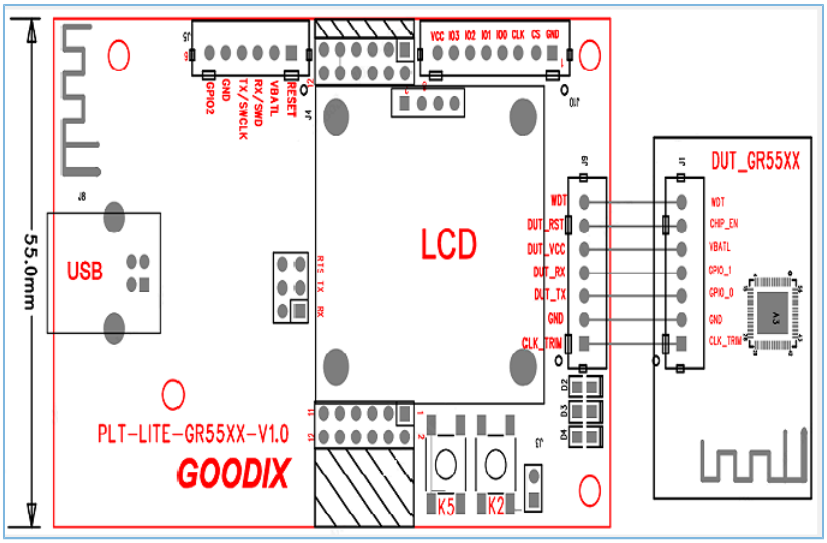

图 2-2 ISP硬件连接示意图

GU检测自定义加密固件正常运行后，将发送指令ENC_DEAL（0x0401）操作固件对DUT进行加密并写入加密密钥。

说明:

- 整机应用时，可根据加密方式反推密钥是否正确。例如加密示例工程ble_enc_app_template的加密方式为：将chip_uid拷贝2份写入eFuse的User Region区域。整机应用时，可先读取芯片的chip_uid和User Region区域，判断User Region区域内容是否为拷贝的2份chip_uid。
- ENC_DEAL加密指令介绍，详见4 自定义加密指令ENC_DEAL。
- DUT （Device Under Test，待测模组），本文特指焊接了GR551x芯片的PCB。

  - 写入成功且回读正确：DUT通过串口发送成功状态给GU。
  - 写入失败：返回失败状态。

自定义加密具体流程及相关错误信息，请参考3 自定义加密烧录流程及相关错误信息。

3 自定义加密烧录流程及相关错误信息

选用自定义加密方式，并启动离线烧录后，自定义加密流程将对应开启。自定义加密流程执行成功，则自动执行后续流程，反之则会在离线板显示屏上显示对应错误信息并停止量产烧录。

在离线量产烧录流程中，自定义加密环节的具体执行流程如下：

1. GU通过串口将自定义加密固件下载至DUT。此时离线板将显示“StartDown ENC FW”。

   GU下载自定义加密固件的流程如下：

   (1) GU检查加密固件格式。

   若检测到img_info的pattern有误或boot_info的load_addr未对齐，离线板将显示“Down ENC FW Img Check Fail”，提示加密固件格式错误。

   (2) 基于DFU协议，GU将加密固件写入DUT。

说明:

下文DFU指令（PROGRAM_START、PROGRAM_FLASH、 PROGRAM_END、 OPERATE_REG ）的详细介绍，可参考《GR551x固件升级指南》。

   GU发送PROGRAM_START（0x23）指令，写入固件。如果DUT应答失败，离线板会显示“Down ENC FW Start Error”，提示加密固件启动信息写入失败。

   (3) GU发送PROGRAM_FLASH（0x24）指令，写入固件数据的头信息。如果DUT应答失败，离线板会显示“Down ENC FW Program Error”，提示加密固件编程失败。

   (4) GU发送PROGRAM_END（0x25）指令，完成固件的写入。如果DUT应答失败，离线板会显示“Down ENC FW End Fail”，提示加密固件校验失败。

说明:

如果在自定义加密固件下载的整个流程中，操作Flash、操作寄存器复位、更新img_info、加密回应或擦除Flash等指令超时无响应，则会报错“Down ENC Info Timeout”，提示写入用户加密信息超时。

---

2. 加密固件成功下载后，GU会发送OPERATE_REG（0x2C）指令操作DUT寄存器，进行加密前的芯片复位，确保加密固件成功运行。

   若DUT应答失败，则会报错“Down ENC Info Fail”，提示写入用户加密信息失败。

3. 加密固件下载完成并成功运行后，GU将发送ENC_DEAL（0x0401）指令写入用户自定义加密信息。此时，DUT将判断加密流程是否成功执行。

   - 未成功执行：DUT将回应写入失败（0x02），并报错“DownENC Info Error”，提示写入用户加密信息错误。
   - 成功执行：继续执行后续的烧录流程。

4 自定义加密指令ENC_DEAL

GU通过发送自定义加密ENC_DEAL指令启动写入用户自定义加密信息，DUT在收到此命令后启动加密流程，并判断是否执行成功，对应响应DUT。

4.1 GU发送数据

表 4-1 GU端发送的数据

字节序号	描述	有效值	说明
0 - 1	帧头	0x4744	以字符‘G’和‘D’的ASCII码值0x47和0x44表示
2 - 3	帧类型	0x0401	下载用户自定义加密固件，启动对应加密流程
4 - 5	数据长度	0x0000	
6 - 7	和校验	0x0000 - 0xFFFF	帧类型和数据长度的16位和校验

4.2 DUT回应数据

表 4-2 DUT端回应的数据

字节序号	描述		有效值	说明
0 - 1	帧头		0x4744	以字符‘G’和‘D’的ASCII码值0x47和0x44表示
2 - 3	帧类型		0x0401	启用自定义加密固件，并执行对应加密流程
4 - 5	数据长度		0x0002	
6	数据内容	应答	0x03	0x03：DUT回应0x0401
7		执行结果	0x01或0x02	0x01：成功 0x02：失败
8 - 9	和校验		0x0000 - 0xFFFF	帧类型、数据长度、数据内容（应答及执行结果）的16位和校验