MEGAHUNT

AN2x0005

应用手册

MH2457

固件安全功能说明

引言

本文档是对 MH2457 固件安全功能的简介、设置、说明和使用场景介绍。

目录

1. 固件安全 2
1.1. 安全功能简介 2
1.2. 安全功能设置 2
1.3. 安全功能说明 2
1.3.1. 安全 Boot 3
1.3.2. Flash 固件数据 3
1.3.3. Flash 信息数据 3
1.4. 应用场景 3
2. 修订记录 4

1. 固件安全

1.1. 安全功能简介

芯片内置安全 Boot 程序，支持固件安全下载、启动验签和信息数据加密保存等安全功能。芯片支持自定义设备信息写入和保存，结合相应密钥，可实现身份认证和数字签名等安全应用场景。这些措施有效地防止未授权生产、数据窃取和篡改，确保芯片设备在整个生命周期内的安全性。

芯片内置丰富的外设资源和硬件安全加密模块，支持 DES、TDES、AES、RSA、ECC、SHA 等主流加密算法。

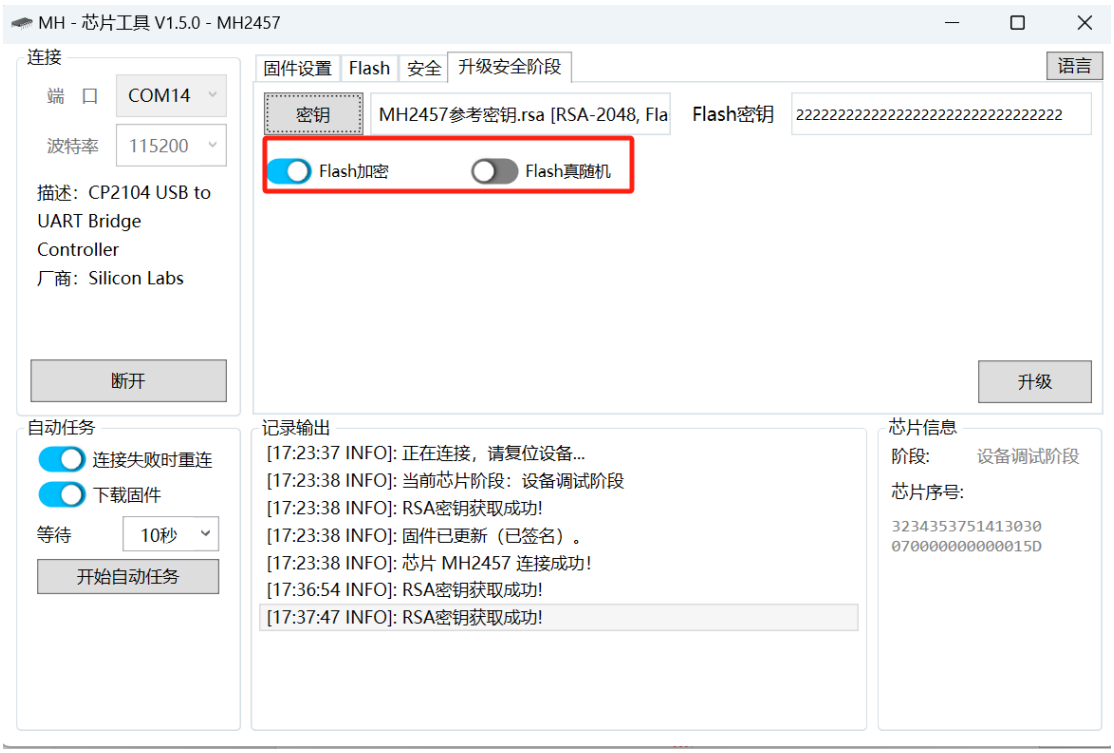
该防护方案无需额外的安全芯片。在安全、成本、功耗、性能等方面，设备优势更加明显，提升市场竞争力。

1.2. 安全功能设置

客户将自有私钥对应的公钥数据注入芯片，并选择是否开启 Flash 加密功能。升级成功后，芯片进入安全阶段，操作如下图所示。

Flash 加密功能是可选的，建议启用 Flash 加密功能，并同时选择“Flash 真随机”选项。启用后存储在 Flash 中的数据将被加密。

注意：芯片的公钥等参数仅可注入一次，升级到安全阶段后无法回退，且 JTAG 功能将自动禁用。



1.3. 安全功能说明

芯片在安全阶段可以通过安全 Boot 启动、Flash 加密等多个方面实现芯片安全防护等功能。

1.3.1. 安全 Boot

在安全阶段，芯片仅允许下载由预先注入的公钥对应私钥签名后的固件。芯片上电启动时，会使用注入的公钥验证固件合法性，同时校验固件完整性，防止未经授权的固件更新或恶意固件加载，从而保障敏感数据的安全。

此外，固件代码可增加对芯片注入公钥数据值的校验等，严防终端的未授权生产或过度生产。

1.3.2. Flash 固件数据

芯片启用 Flash 加密后，固件数据将加密存储于芯片的 Flash 中，运行时，芯片会自动解密并加载相关数据或代码，防止芯片固件数据被窃取或篡改。

开启 Flash 真随机加密，每个芯片会生成不同的真随机数作为加密密钥，确保“一芯一密”，从而提升安全性。这种加密方式不会影响授权固件的正常下载或更新过程。

1.3.3. Flash 信息数据

芯片固件代码需要在空闲 Flash 区域保存信息数据时，可调用 Flash 加密编程接口，将信息数据加密写入指定区域，这样即使在启用 Flash 加密的情况下，信息数据也能够被正确读取，确保数据的机密性和完整性。

Flash 加密编程接口实现参考下图：

```
//使用的ROM接口定义在mhscpu_qspi.h文件中
#define ROM_QSPI_ProgramCrypt            (*((uint8_t (*)(uint8_t *, uint32_t, uint32_t))(*(uint32_t *)0x001C)))

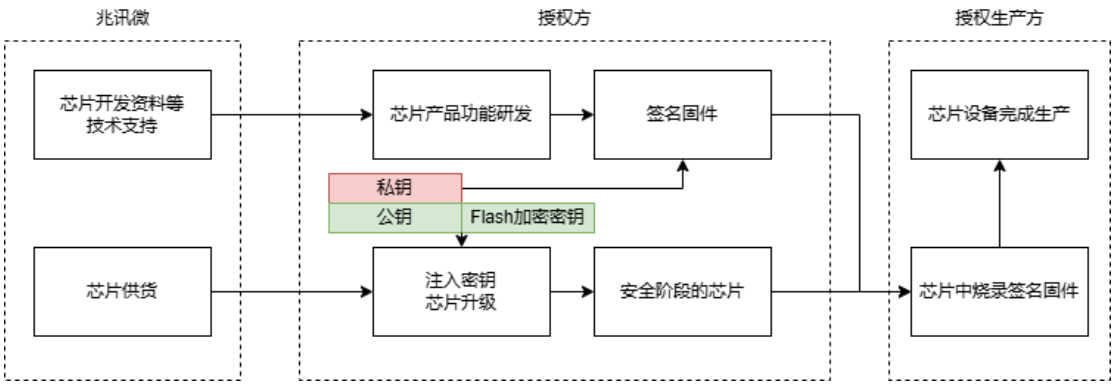

//Flash加密编程接口实现在mhscpu_qspi.c文件中
uint8_t FLASH_ProgramCrypt(uint32_t addr,uint32_t size,uint8_t *buffer)
{
    uint8_t ret;

    __disable_irq();
    __disable_fault_irq();
    /*need to use DMA2_Stream4*/
    ret = ROM_QSPI_ProgramCrypt(buffer, addr, size);
    __enable_fault_irq();
    __enable_irq();

    return ret;
}
```

1.4. 应用场景

芯片实现安全防护功能的应用场景，如下图：



2. 修订记录

表 2-1 修订记录

日期	修订版本	描述
2025-01-06	1.0	1. 初稿完成
2025-05-28	1.1	1. 更新模板

DISCLAIMER

The information in this document is current as of the published date. The information is subject to change without notice. For actual design-in, refer to the latest publications of MEGAHUNT Datasheets, and other official documents, for the most up-to-date specifications of MEGAHUNT products. Not all products and/or types are available in every country. Please contact a MEGAHUNT sales representative for availability and additional information.

No part of this document may be copied or reproduced in any form or by any means without the prior written consent of MEGAHUNT. MEGAHUNT assumes no responsibility for any errors or inaccuracies that may appear in this document.

MEGAHUNT disclaims any liability for patent, copyright or other intellectual property rights infringements of third parties by or arising from the use of MEGAHUNT products listed in this document or any other liability arising from the use of such products. No license, express, implied or otherwise, is granted under any patents, copyrights or other intellectual property rights of MEGAHUNT or others. Descriptions of circuits, software and other related information in this document are provided for illustrative purposes in semiconductor product operation and application examples. The incorporation of these circuits, software and information in the design of a customer's equipment shall be done under the full responsibility of the customer. MEGAHUNT assumes no responsibility for any losses incurred by customers or third parties arising from the use of these circuits, software and information.

The fonts, images, and other logos used by our company are legally authorized or legally used free of charge without infringing any third-party's rights.

Our company reserves the right to modify or revoke this disclaimer.

If you have any doubts, please contact us promptly and we will actively resolve them.

For more information about MEGAHUNT products and solutions, visit our website at www.megahuntmicro.com