应用笔记

Application Note

AN1172

G32A1085 A1065 A1045 系列信息安全应用笔记

版本：**V1.1**

1 引言

本应用笔记提供在 G32A1085 A1065 A1045 关于信息安全的介绍。

目录

2 信息安全模块

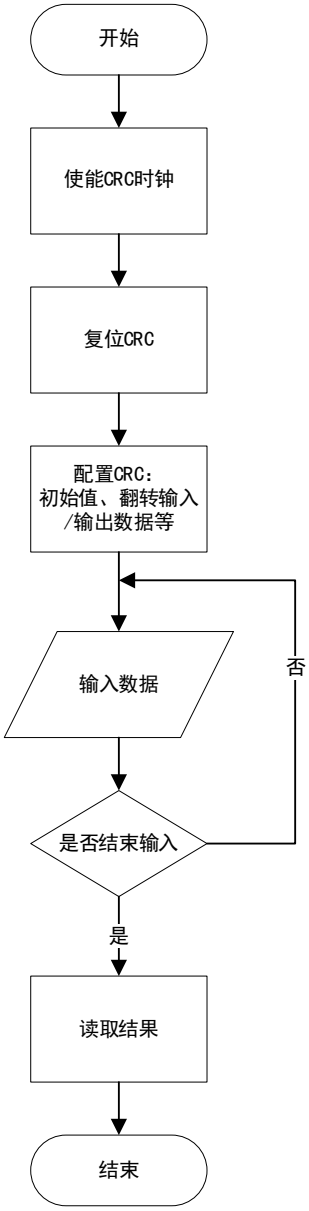
2.1 CRC 计算单元

2.1.1 简介

循环冗余校验（CRC）计算单元可将输入数据经过固定的生成多项式计算得到 8/16/32 位的 CRC 计算结果，主要用来检测或校验数据传输或者保存后的正确性与完整性。

2.1.2 编程指南

图 1 CRC 计算单元程序流程图



2.2 AES256 加解密模块

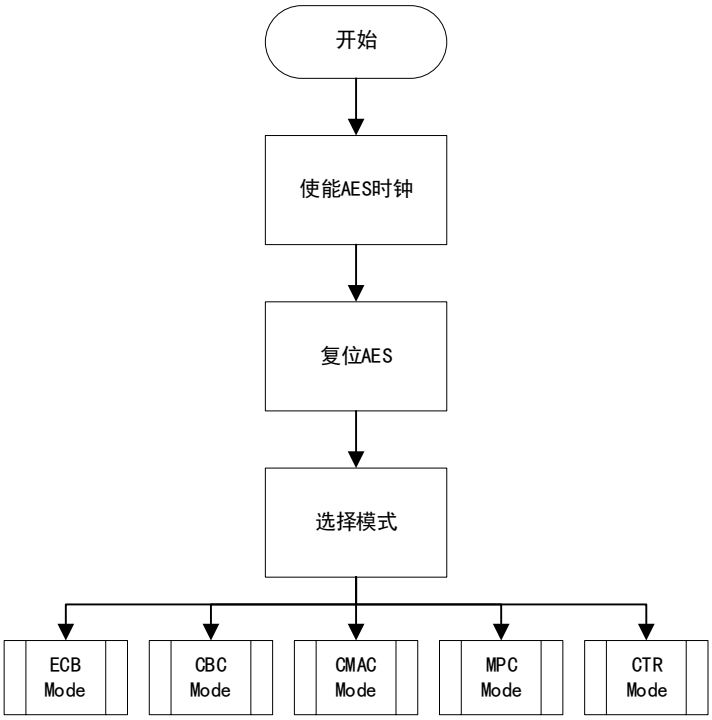
2.2.1 简介

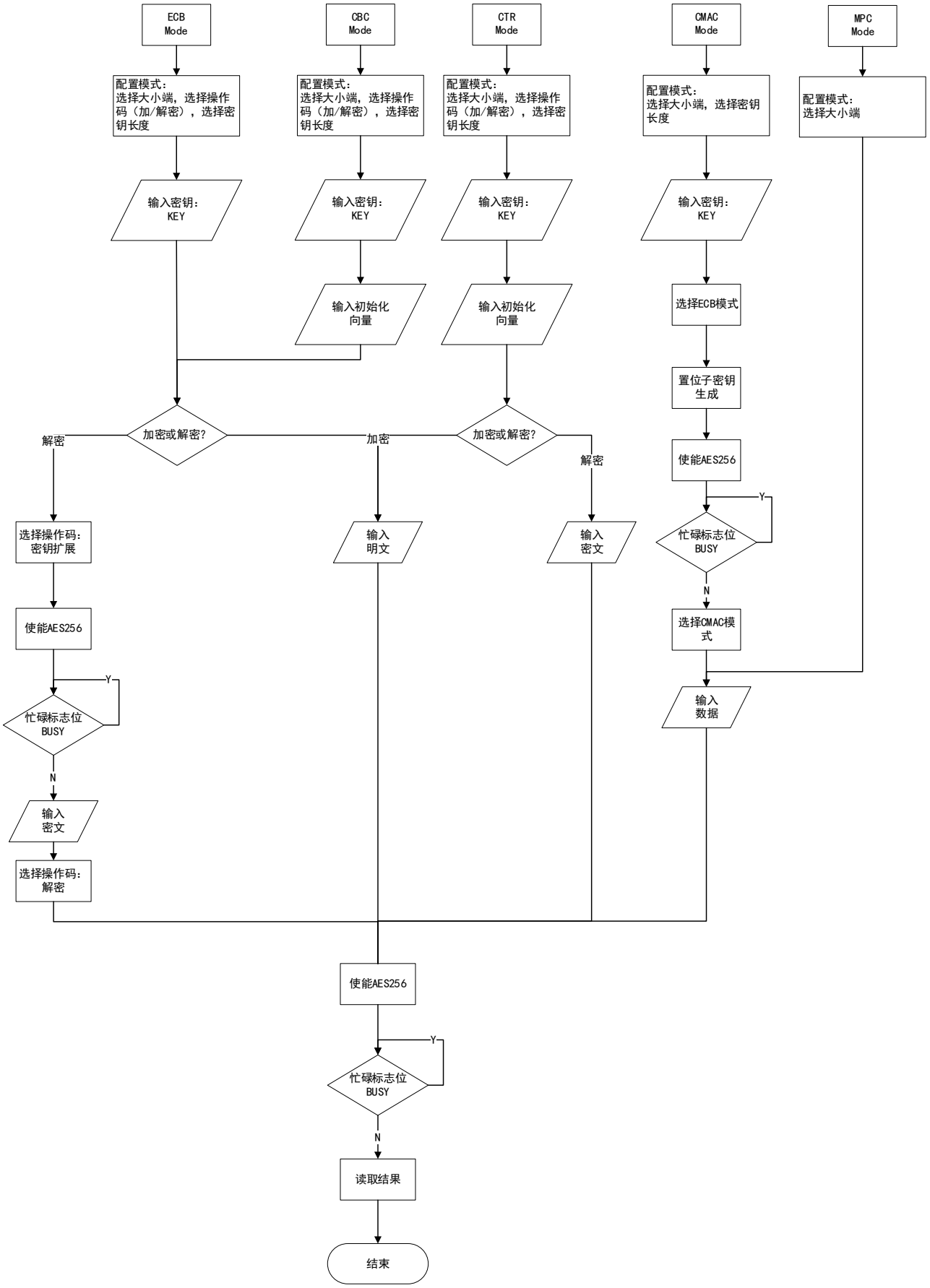
AES256 可实现 AES256（高级加密标准）编码算法，也被称为 Rijndael 算法。

- 支持三种不同长度的密钥：AES-128、AES-192、AES-256
- 支持三种模式：ECB（电子密码本）、CBC（密码分组链接）、CTR（计数器）
- 支持两种算法：CMAC 算法、MP-compress 算法

2.2.2 编程指南

图 2 AES256 加解密模块程序流程图




ECB Mode
CBC Mode
CTR Mode
CMAC Mode
MPC Mode
配置模式：选择大小端，选择操作码（加/解密），选择密钥长度
配置模式：选择大小端，选择操作码（加/解密），选择密钥长度
配置模式：选择大小端，选择操作码（加/解密），选择密钥长度
配置模式：选择大小端，选择密钥长度
配置模式：选择大小端
输入密钥：KEY
输入密钥：KEY
输入密钥：KEY
输入密钥：KEY
输入初始化向量
输入初始化向量
选择ECB模式
置位子密钥生成
使能AES256
忙碌标志位BUSY
选择CMAC模式
输入数据
加密或解密?
加密或解密?
解密
加密
解密
选择操作码：密钥扩展
输入明文
输入密文
使能AES256
忙碌标志位BUSY
输入密文
选择操作码：解密
使能AES256
忙碌标志位BUSY
读取结果
结束
Y
N
Y
N

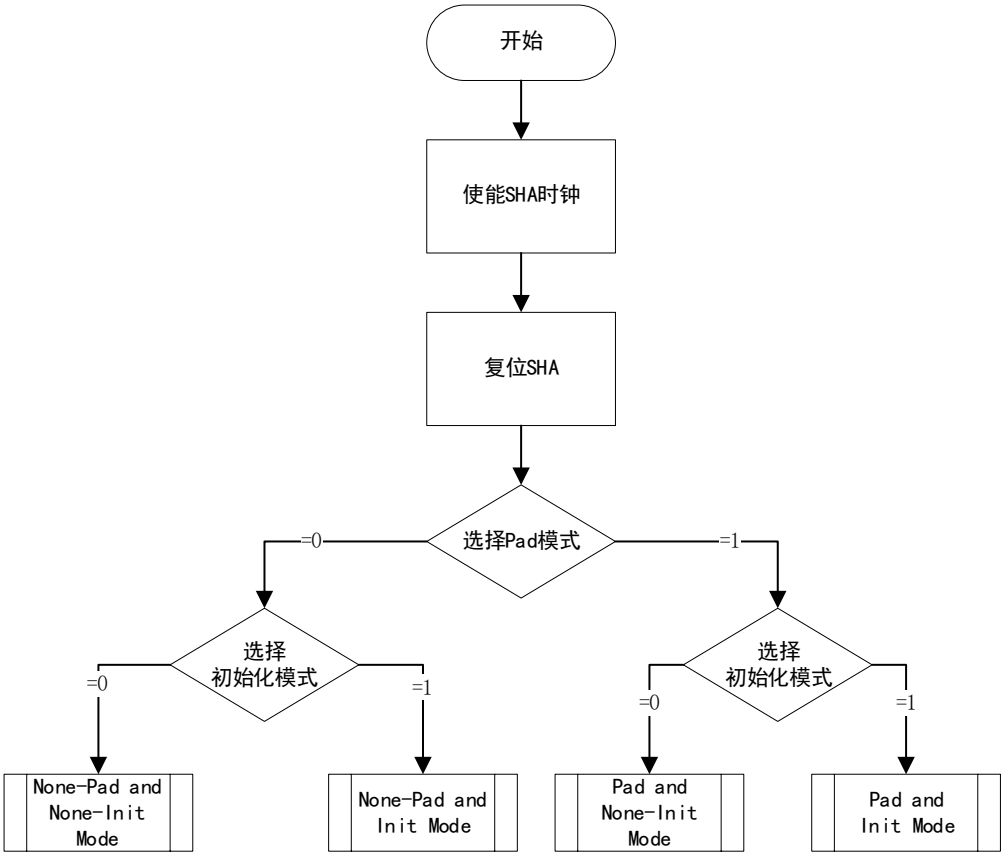
2.3 SHA256 密码学哈希函数

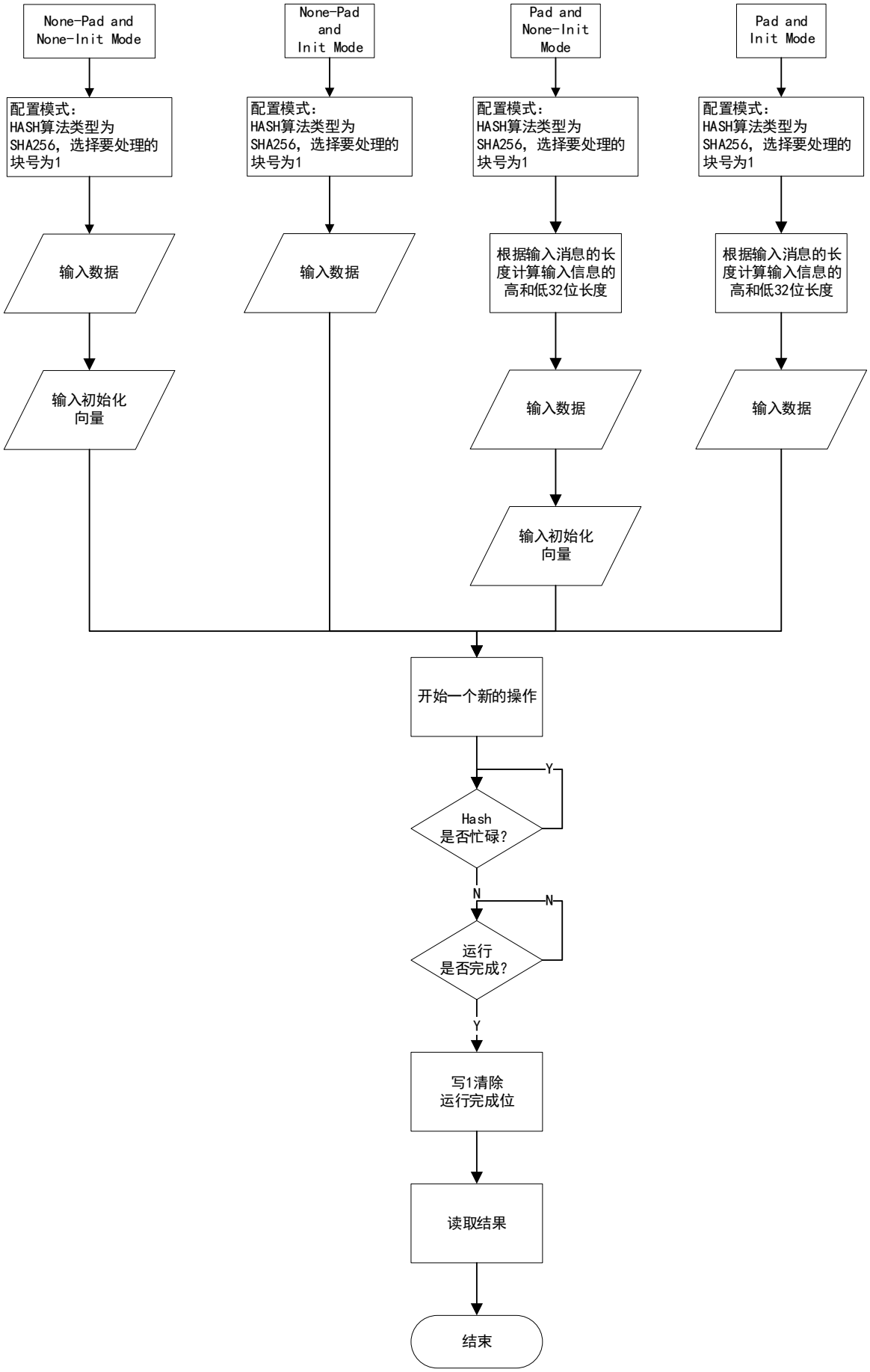
2.3.1 简介

SHA256（Secure Hash Algorithm 256-bit）是一种密码学哈希函数，属于 SHA-2 系列的一部分。在 MCU 中集成 SHA256 模块，能够为系统提供高效安全的哈希计算能力，可应用于数据完整性验证、数字签名、密码存储等安全相关的应用场景。通过硬件实现 SHA256 算法，相较于软件实现，能显著提高计算速度，同时降低 CPU 的负载。最大长度 63*256，每个消息块的长度为 512 位。

2.3.2 编程指南

图 3 SHA256 密码学哈希函数程序流程图




None-Pad and None-Init Mode
None-Pad and Init Mode
Pad and None-Init Mode
Pad and Init Mode
配置模式：HASH算法类型为SHA256，选择要处理的块号为1
配置模式：HASH算法类型为SHA256，选择要处理的块号为1
配置模式：HASH算法类型为SHA256，选择要处理的块号为1
配置模式：HASH算法类型为SHA256，选择要处理的块号为1
输入数据
输入数据
根据输入消息的长度计算输入信息的高和低32位长度
根据输入消息的长度计算输入信息的高和低32位长度
输入初始化向量
输入数据
输入数据
输入初始化向量
开始一个新的操作
Hash是否忙碌?
Y
N
运行是否完成?
N
Y
写1清除运行完成位
读取结果
结束

2.4 TRNG 真随机数生成器

2.4.1 简介

TRNG 是一个真随机数发生器，以连续模拟噪声为基础，在主机读数为其提供一个 32 位的随机数。

2.5 96 位唯一 ID

2.5.1 简介

96 位芯片的 ID 主要用处：

- 作为序列号
- 作为密码，在编写闪存时，代码和密码通过算法结合，可以提高代码在 Flash 内的安全性
- 用于启动配置
- 身份标识所提供的参考号码对任一 MCU 微控制器系列都是唯一的，无论在什么情况下，用户都不能改变这唯一的身份标识。根据不同用法，用户可以选择以字节、半字或全字为单位读取身份标识。

2.6 支持的软件算法

- SM3、SM4 加解密
- RSA2048/3072/4096 非对称加解密以及数字签名验签

表格 1 支持的软件算法耗时统计表

测试项	描述	耗时 G32A1085 RUN 64MHz 单位：ms
SM3（软件）	SM3+1KB Data	2.990115
	SM3+256KB Data	712.01714
SM4 加密（软件）	SM4+16byte Data	0.106235
SM4 解密（软件）	SM4+16byte Data	0.106825
RSA 签名（软件）	RSA2048	14656.3482
	RSA3072	41779.8112

测试项	描述	耗时 G32A1085 RUN 64MHz 单位：ms
	RSA4096	88937.2924
RSA 验签（软件）	RSA2048	309.45358
	RSA3072	640.32805
	RSA4096	1059.66028
RSA 加密（软件）	RSA2048	309.16726
	RSA3072	640.32224
	RSA4096	1060.06744
RSA 解密（软件）	RSA2048	14657.6365
	RSA3072	41780.1378
	RSA4096	88939.8017
AES256-ECB 模式（硬件）	加密+1KB Data	0.267108
	解密+1KB Data	0.267858
AES256-CBC 模式（硬件）	加密+1KB Data	0.267874
	解密+1KB Data	0.268656
AES256-CTR 模式（硬件）	加密+1KB Data	0.267874
	解密+1KB Data	0.268124
AES256-CMAC 模式（硬件）	1KB Data	0.262686
AES256-MPC 模式（硬件）	1KB Data	0.265326
SHA256-Pad_Init 模式（硬件）	1KB Data	0.361282
SHA256-Pad_NoneInit 模式（硬件）	1KB Data	0.366766
SHA256-NonePad_Init 模式（硬件）	1KB Data	0.360064
SHA256-NonePad_NoneInit 模式（硬件）	1KB Data	0.36564

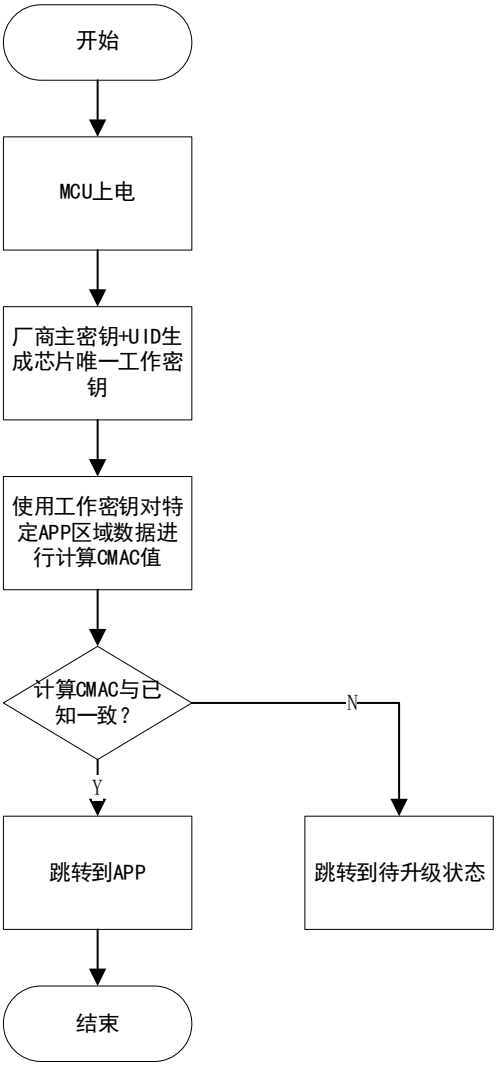
3 安全启动流程

3.1 简介

PFlash 将程序分为两大部分：一是 Bootloader，二是 App SW。MCU 上电后，执行 Bootloader 程序：Bootloader 使用厂商主密钥+UID（96 位唯一 ID）生成芯片唯一工作密钥，然后该工作密钥作为 AES256 的密钥对特定 APP 区数据进行计算 CMAC 值，最后比较计算出来的 CMAC 值和保存在指定地址的 CMAC 值，一致则跳转到 App SW 区，不一致则跳转到待升级状态。

3.2 流程

图 4 安全启动流程图



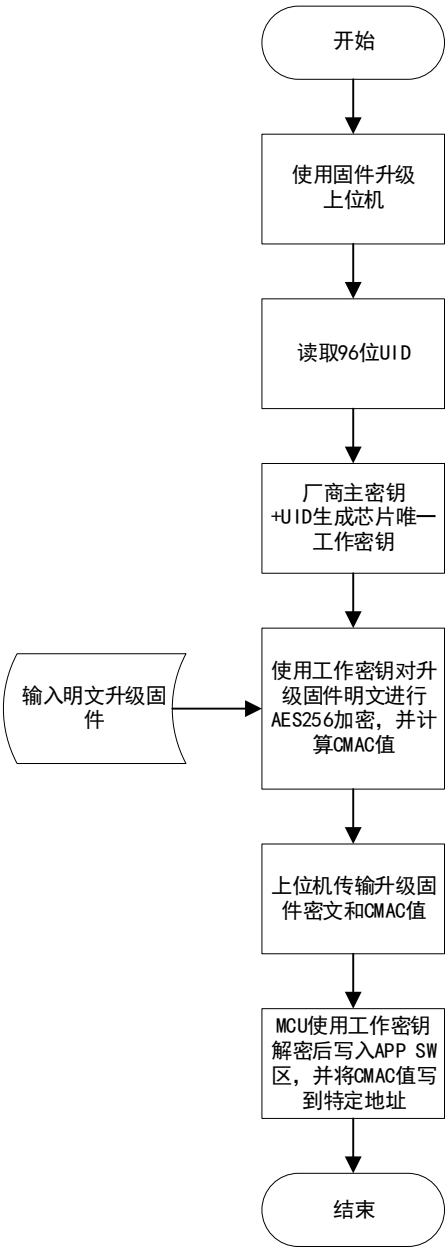
4 安全升级流程

4.1 简介

首先使用固件升级上位机读取 96 位唯一芯片 IID+厂商主密钥作为唯一工作密钥，然后使用该工作密钥对升级固件明文进行 AES256 加密，并计算 CMAC 值，最后上位机传输升级固件密文和 CMAC 值，MCU 收到密文后解密写到 App SW 区，并将 CMAC 值写到特定地址。

4.2 流程

图 5 安全升级流程图



5 版本历史

表格 2 文件版本历史

日期	版本	变更历史
2026.5	1.0	● 初始版本
2026.6	1.1	● 更新 2.6 章节的软件算法耗时统计时间和增加硬件算法时间

声明

本手册由珠海极海半导体有限公司（以下简称“极海”）制订并发布，所列内容均受商标、著作权、软件著作权相关法律法规保护，极海保留随时更正、修改本手册的权利。使用极海产品前请仔细阅读本手册，一旦使用产品则表明您（以下称“用户”）已知悉并接受本手册的所有内容。用户必须按照相关法律法规和本手册的要求使用极海产品。

1、权利所有

本手册仅应当被用于与极海所提供的对应型号的芯片产品、软件产品搭配使用，未经极海许可，任何单位或个人均不得以任何理由或方式对本手册的全部或部分内容进行复制、抄录、修改、编辑或传播。

本手册中所列带有“®”或“™”的“极海”或“Geehy”字样或图形均为极海的商标，其他在极海产品上显示的产品或服务名称均为其各自所有者的财产。

2、无知识产权许可

极海拥有本手册所涉及的全部权利、所有权及知识产权。

极海不应因销售、分发极海产品及本手册而被视为将任何知识产权的许可或权利明示或默示地授予用户。

如果本手册中涉及任何第三方的产品、服务或知识产权，不应被视为极海授权用户使用前述第三方产品、服务或知识产权，也不应被视为极海对第三方产品、服务或知识产权提供任何形式的保证，包括但不限于任何第三方知识产权的非侵权保证，除非极海在销售订单或销售合同中另有约定。

3、版本更新

用户在下单购买极海产品时可获取相应产品的最新版的手册。

如果本手册中所述的内容与极海产品不一致的，应以极海销售订单或销售合同中的约定为准。

4、信息可靠性

本手册相关数据经极海实验室或合作的第三方测试机构批量测试获得，但本手册相关数据难免会出现校正笔误或因测试环境差异所导致的误差，因此用户应当理解，极海对本手册中可能出现的该等错误无需承担任何责任。本手册相关数据仅用于指导用户作为性能参数参照，不构成极海对任何产品性能方面的保证。

用户应根据自身需求选择合适的极海产品，并对极海产品的应用适用性进行有效验证和测试，以确认极海产品满足用户自身的需求、相应标准、安全或其它可靠性要求；若因用户未充分对极海产品进行有效验证和测试而致使用户损失的，极海不承担任何责任。

5、合规要求

用户在使用本手册及所搭配的极海产品时，应遵守当地所适用的所有法律法规。用户应了解产品可能受到产品供应商、极海、极海经销商及用户所在地等各国有关出口、再出口或其它法律的限制，用户（代表其本身、子公司及关联企业）应同意并保证遵守所有关于取得极海产品及/或技术与直接产品的出口和再出口适用法律与法规。

6、免责声明

本手册由极海“按原样”（as is）提供，在适用法律所允许的范围内，极海不提供任何形式的明示或暗示担保，包括但不限于对产品适销性和特定用途适用性的担保。

极海产品并非设计、授权或担保适合用于军事、生命保障系统、污染控制或有害物质管理系统中的关键部件，亦非设计、授权或担保适合用于在产品失效或故障时可导致人员受伤、死亡、财产或环境损害的应用。

如果产品未标明“汽车级”，则表示不适用于汽车应用。如果用户对产品的应用超出极海提供的规格、应用领域、规范，极海不承担任何责任。

用户应该确保对产品的应用符合相应标准以及功能安全、信息安全、环境标准等要求。用户对极海产品的选择和使用负全部的责任。对于用户后续在针对极海产品进行设计、使用的过程中所引起的任何纠纷，极海概不承担责任。

7、责任限制

在任何情况下，除非适用法律要求或书面同意，否则极海和/或以“按原样”形式提供本手册

及产品的任何第三方均不承担损害赔偿责任，包括任何一般、特殊因使用或无法使用本手册及产品而产生的直接、间接或附带损害（包括但不限于数据丢失或数据不准确，或用户或第三方遭受的损失），这涵盖了可能导致的人身安全、财产或环境损害等情况，对于这些损害极海概不承担责任。

8、适用范围

本手册的信息用以取代本手册所有早期版本所提供的信息。