# Application Note

## Document No.: AN1172

## G32A1085 A1065 A1045

## Information Security Application Notes

**Version: V1.1**

# 1 Introduction

This application note introduces the information security features of the G32A1085 A1065 A1045 series.

# Content

# 2 Information Security Modules

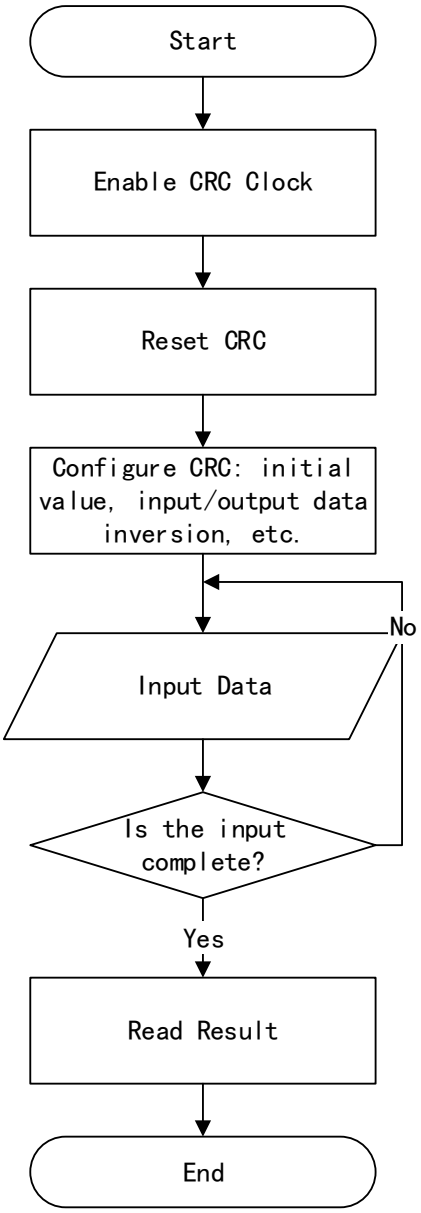
## 2.1 CRC Calculation Unit

### 2.1.1 Overview

The Cyclic Redundancy Check (CRC) calculation unit uses a fixed generator polynomial to process input data and generate 8-bit, 16-bit, or 32-bit CRC results. It is mainly used to check data correctness and integrity after transmission or storage.

### 2.1.2 Programming Guide

Figure 1 CRC Calculation Unit Program Flowchart



## 2.2 AES256 Encryption/Decryption Module

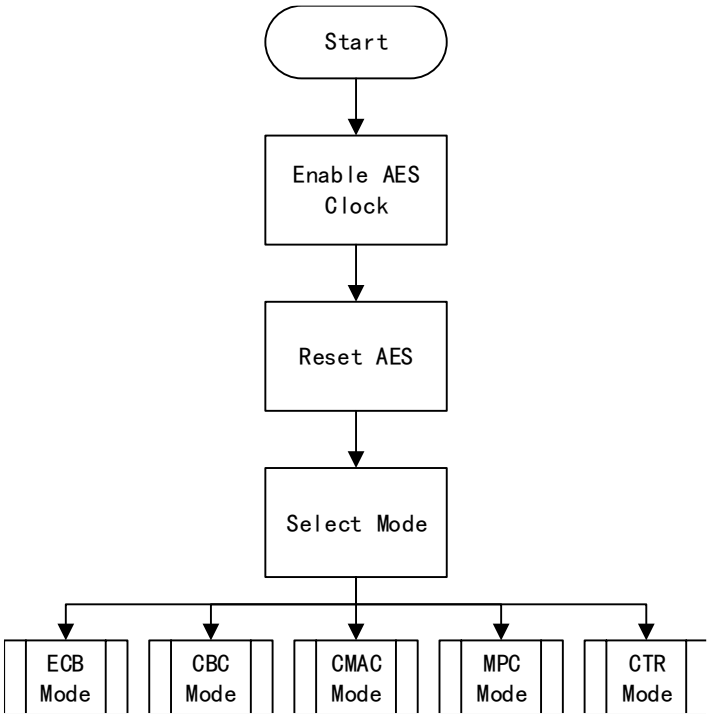
### 2.2.1 Overview

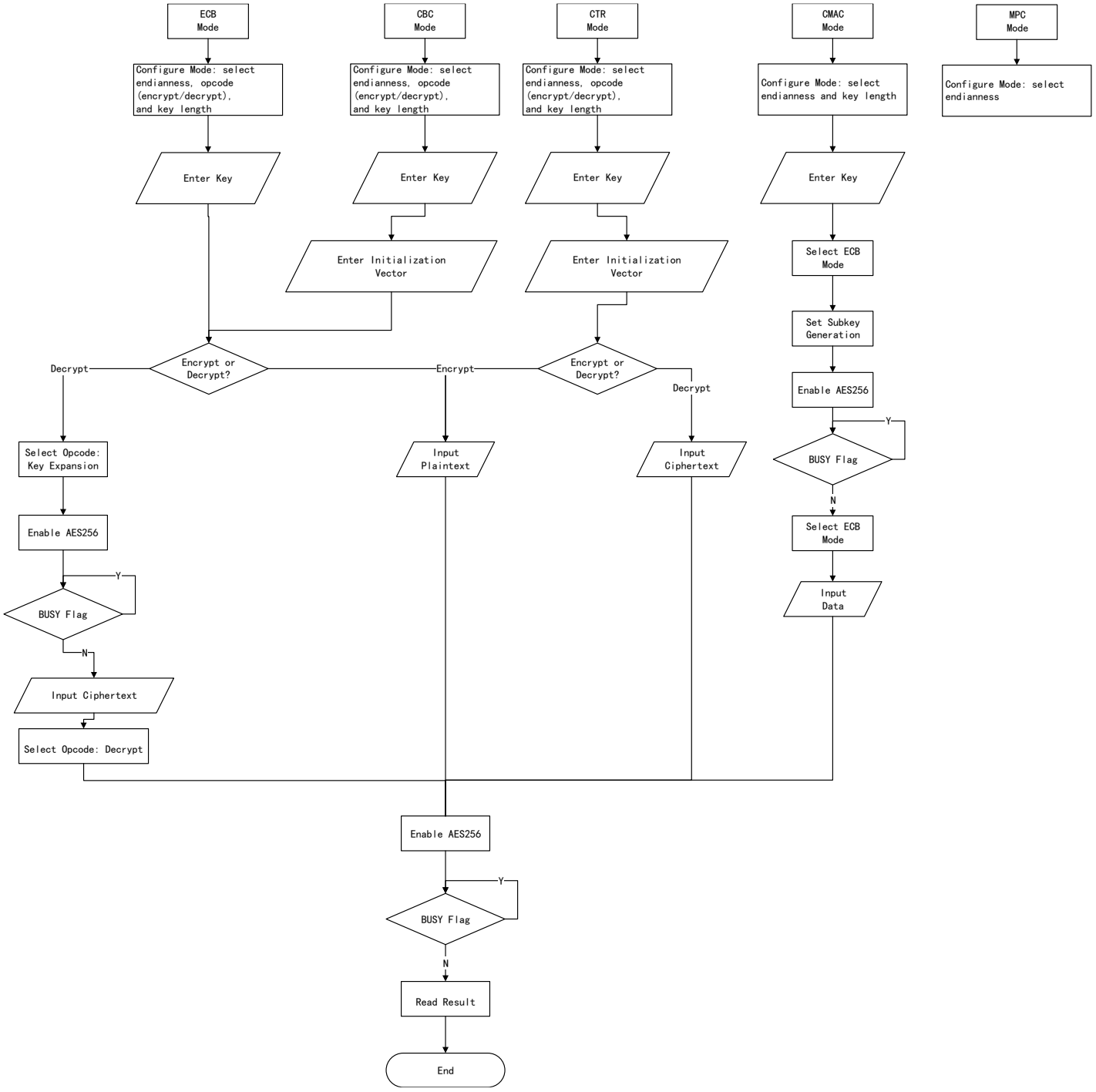
The AES256 module implements the AES (Advanced Encryption Standard) algorithm, also known as the Rijndael algorithm.

- Supports three key lengths: AES-128, AES-192, and AES-256
- Supports three modes: ECB (Electronic Codebook), CBC (Cipher Block Chaining), and CTR (Counter)
- Supports two algorithms: CMAC and MP-compress

### 2.2.2 Programming Guide

Figure 2 AES256 Encryption/Decryption Module Program Flowchart






## 2.3 SHA256 Cryptographic Hash Function

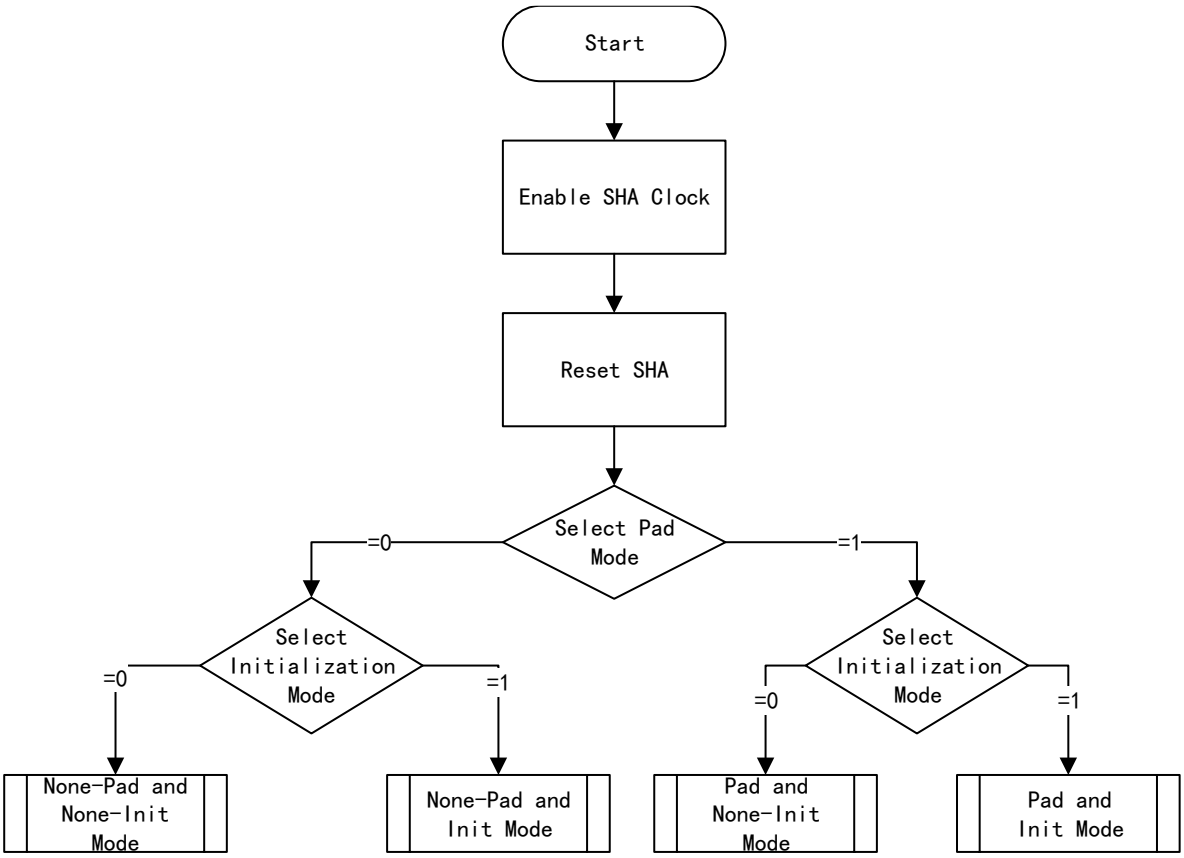
### 2.3.1 Overview

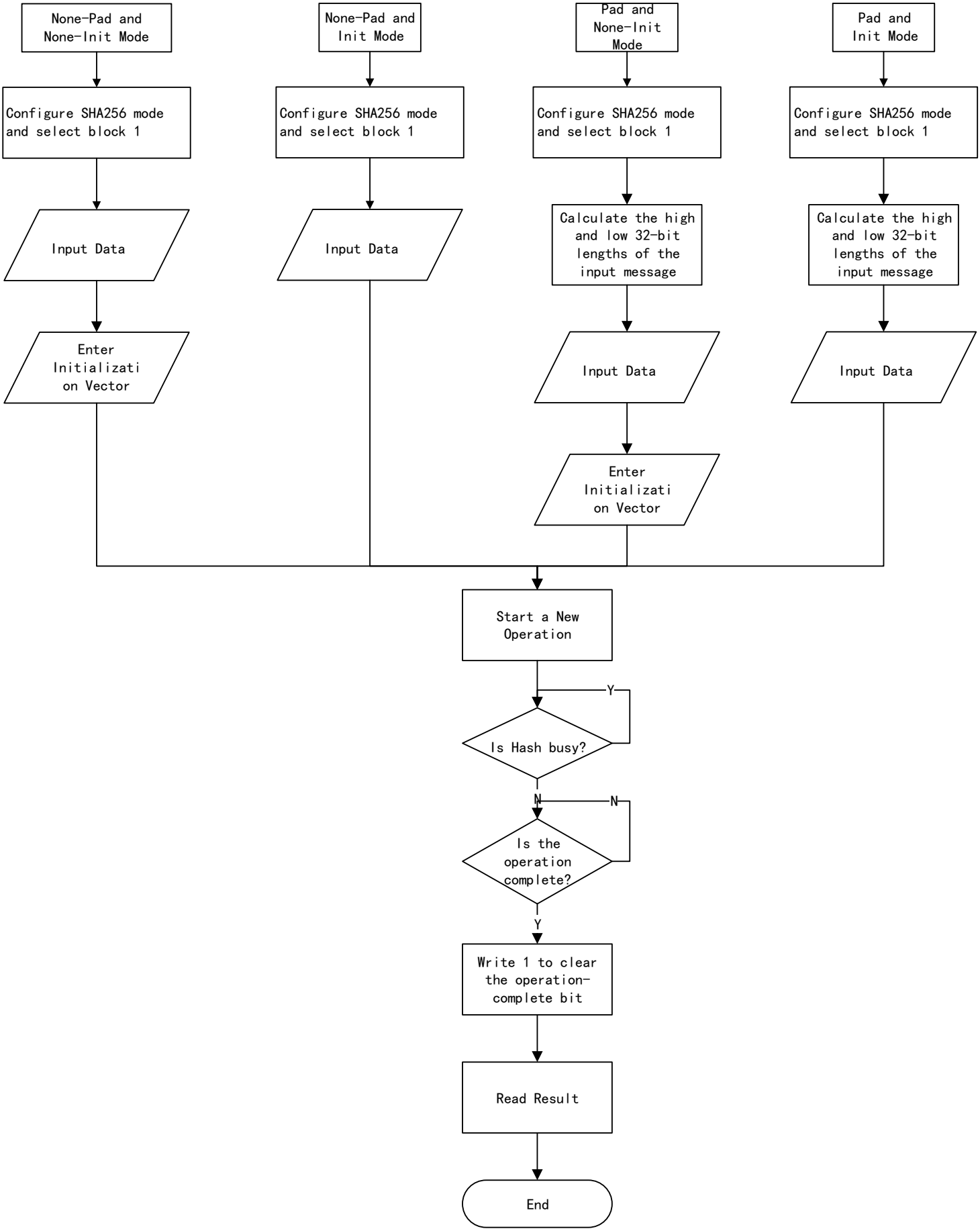
SHA256 (Secure Hash Algorithm 256-bit) is a cryptographic hash function in the SHA-2 family. The MCU SHA256 module provides fast and secure hash calculation for data integrity checks, digital signatures, password storage, and other security applications. Compared with software implementation, the hardware SHA256 module improves calculation speed and reduces CPU

load. The maximum message length is 63×256, and each message block is 512 bits.

### 2.3.2 Programming Guide

Figure 3 SHA256 Cryptographic Hash Function Program Flowchart




None-Pad and None-Init Mode
None-Pad and Init Mode
Pad and None-Init Mode
Pad and Init Mode
Configure SHA256 mode and select block 1
Configure SHA256 mode and select block 1
Configure SHA256 mode and select block 1
Configure SHA256 mode and select block 1
Input Data
Input Data
Calculate the high and low 32-bit lengths of the input message
Calculate the high and low 32-bit lengths of the input message
Enter Initializati on Vector
Input Data
Input Data
Enter Initializati on Vector
Start a New Operation
Y
Is Hash busy?
N
N
Is the operation complete?
Y
Write 1 to clear the operation-complete bit
Read Result
End

## 2.4 TRNG True Random Number Generator

### 2.4.1 Overview

The TRNG is a true random number generator based on continuous analog noise. It provides a 32-bit random number to the host when read.

## 2.5 96-Bit Unique ID

### 2.5.1 Overview

Primary uses of the 96-bit chip ID:

- Used as a serial number
- Used as a key when writing to Flash; the code and key are combined through an algorithm to improve the security of code stored in Flash
- Used for boot configuration
- The identity tag provides a unique reference number for each MCU. This unique identity cannot be changed by the user. Depending on the use case, the user can read the identity in bytes, half-words, or full words.

## 2.6 Supported Software Algorithms

- SM3 and SM4 encryption/decryption
- RSA2048/3072/4096 asymmetric encryption/decryption and digital signature verification

Table 1 Supported Software Algorithm Timing Statistics

| Test Item | Description | Time (G32A1085 RUN) Unit: ms |
|---|---|---|
| SM3 (software) | SM3+1KB Data | 2.990115 |
| | SM3+256KB Data | 712.01714 |
| SM4 Encryption (software) | SM4+16byte Data | 0.106235 |
| SM4 Decryption (software) | SM4+16byte Data | 0.106825 |
| RSA Signing (software) | RSA2048 | 14656.3482 |
| | RSA3072 | 41779.8112 |
| | RSA4096 | 88937.2924 |
| RSA Verification (software) | RSA2048 | 309.45358 |
| | RSA3072 | 640.32805 |
| | RSA4096 | 1059.66028 |
| RSA Encryption (software) | RSA2048 | 309.16726 |
| | RSA3072 | 640.32224 |
| | RSA4096 | 1060.06744 |

| Test Item | Description | Time (G32A1085 RUN) Unit: ms |
|---|---|---|
| RSA Decryption (software) | RSA2048 | 14657.6365 |
| | RSA3072 | 41780.1378 |
| | RSA4096 | 88939.8017 |
| AES256-ECB mode (hardware) | Encryption+1KB Data | 0.267108 |
| | Decryption+1KB Data | 0.267858 |
| AES256-CBC mode (hardware) | Encryption+1KB Data | 0.267874 |
| | Decryption+1KB Data | 0.268656 |
| AES256-CTR mode (hardware) | Encryption+1KB Data | 0.267874 |
| | Decryption+1KB Data | 0.268124 |
| AES256-CMAC mode (hardware) | 1KB Data | 0.262686 |
| AES256-MPC mode (hardware) | 1KB Data | 0.265326 |
| SHA256-Pad_Init mode (hardware) | 1KB Data | 0.361282 |
| SHA256-Pad_NoneInit mode (hardware) | 1KB Data | 0.366766 |
| SHA256-NonePad_Init mode (hardware) | 1KB Data | 0.360064 |
| SHA256-NonePad_NoneInit mode (hardware) | 1KB Data | 0.36564 |

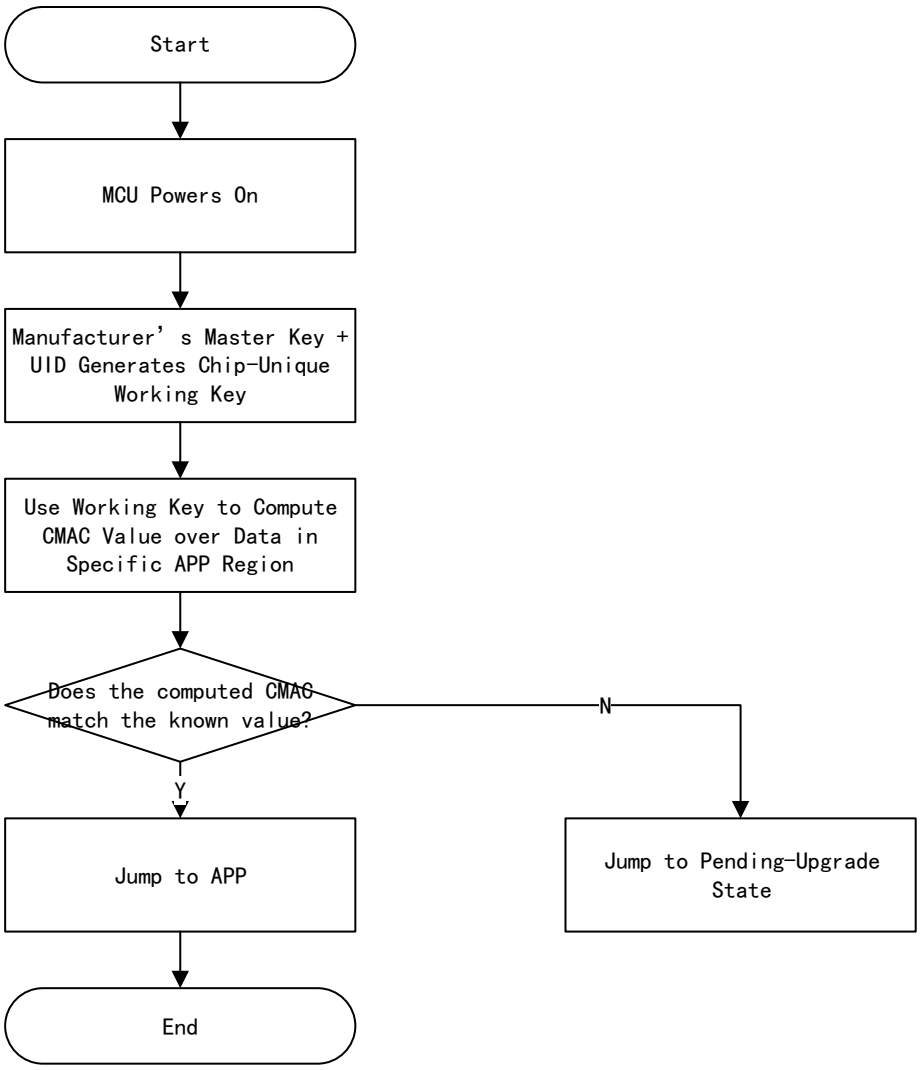
# 3 Secure Boot Process

## 3.1 Overview

PFlash divides the program into two main parts: the Bootloader and the App SW. After the MCU powers on, the Bootloader runs first. It uses the manufacturer's master key and the 96-bit UID to generate a chip-unique working key. This working key is then used as the AES256 key to calculate the CMAC value of the data in a specified APP region. The calculated CMAC value is compared with the CMAC value stored at a designated address. If the values match, execution jumps to the App SW region. If they do not match, the device enters the pending-upgrade state.

## 3.2 Process

Figure 4 Secure Boot Flowchart



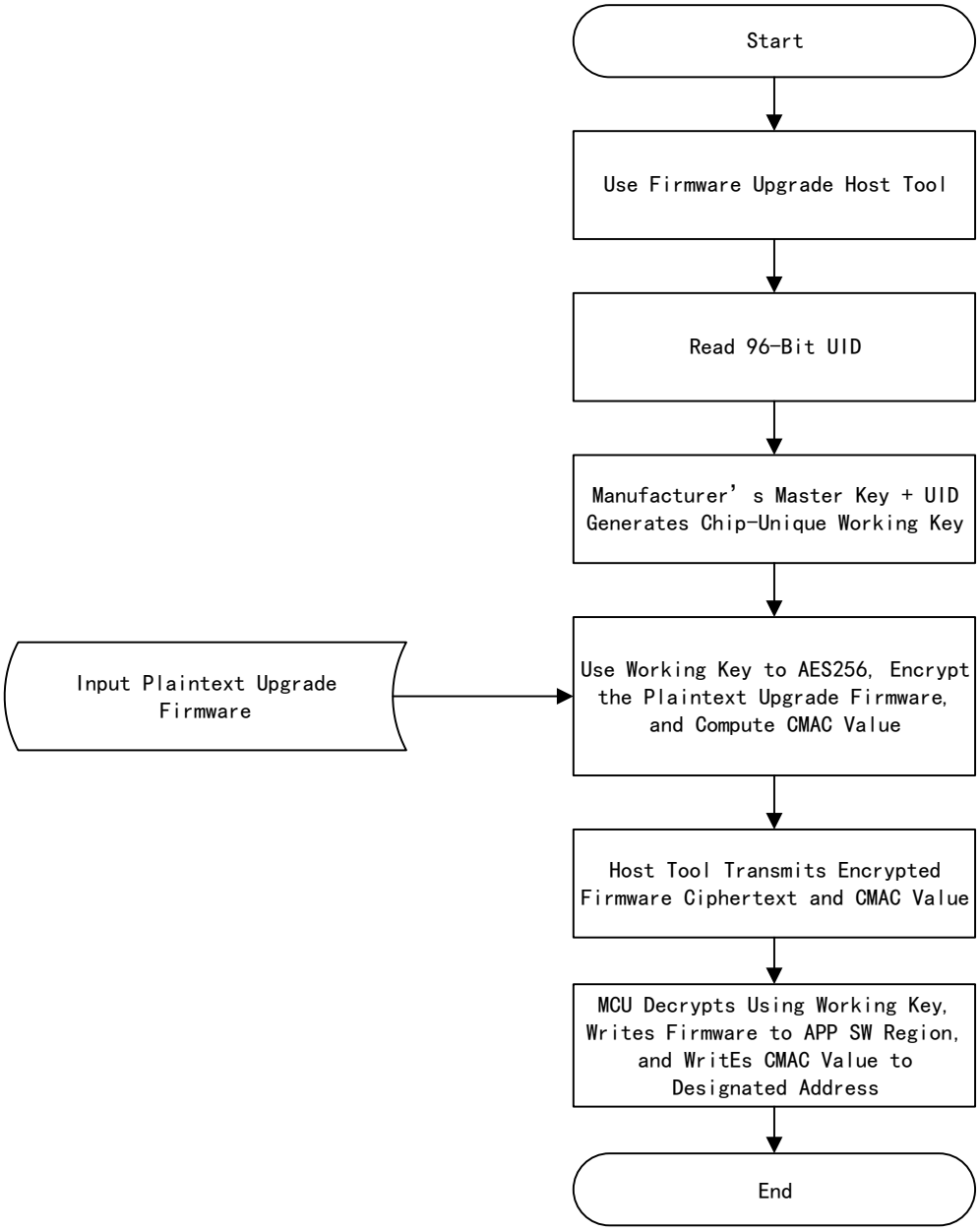
# 4 Secure Upgrade Process

## 4.1 Overview

The firmware upgrade host tool first reads the 96-bit UID and uses it with the manufacturer's master key to derive a unique working key. This working key is used to AES256-encrypt the plaintext upgrade firmware and calculate its CMAC value. The host tool then sends the encrypted firmware ciphertext and CMAC value to the MCU. After receiving the ciphertext, the MCU decrypts it, writes the firmware to the App SW region, and writes the CMAC value to a designated address.

## 4.2 Process

Figure 5 Secure Upgrade Flowchart



# 5 Revision History

Table 2 Document Revision History

| Date | Version | Revision History |
|---|---|---|
| May, 2025 | 1.0 | ● Initial release |
| June, 2025 | 1.1 | ● Updated the software timing data and added hardware timing in Section 2.6. |

# Statement

This document is formulated and published by Geehy Semiconductor Co., Ltd. (hereinafter referred to as “Geehy”). The contents in this document are protected by laws and regulations of trademark, copyright and software copyright. Geehy reserves the right to make corrections and modifications to this document at any time. Read this document carefully before using Geehy products. Once you use the Geehy product, it means that you (hereinafter referred to as the “users”) have known and accepted all the contents of this document. Users shall use the Geehy product in accordance with relevant laws and regulations and the requirements of this document.

1. Ownership

This document can only be used in connection with the corresponding chip products or software products provided by Geehy. Without the prior permission of Geehy, no unit or individual may copy, transcribe, modify, edit or disseminate all or part of the contents of this document for any reason or in any form.

The “极海” or “Geehy” words or graphics with “®” or “™” in this document are trademarks of Geehy. Other product or service names displayed on Geehy products are the property of their respective owners.

2. No Intellectual Property License

Geehy owns all rights, ownership and intellectual property rights involved in this document.

Geehy shall not be deemed to grant the license or right of any intellectual property to users explicitly or implicitly due to the sale or distribution of Geehy products or this document.

If any third party’s products, services or intellectual property are involved in this document, it shall not be deemed that Geehy authorizes users to use the aforesaid third party’s products, services or intellectual property. Any information regarding the application of the product, Geehy hereby disclaims any and all warranties and liabilities of any kind, including without limitation warranties of non-infringement of intellectual property rights of any third party, unless otherwise agreed in sales order or sales contract.

3. Version Update

Users can obtain the latest document of the corresponding models when ordering Geehy products.

If the contents in this document are inconsistent with Geehy products, the agreement in the sales order or the sales contract shall prevail.

4. Information Reliability

The relevant data in this document are obtained from batch test by Geehy Laboratory or cooperative third-party testing organization. However, clerical errors in correction or errors caused by differences in testing environment may occur inevitably. Therefore, users should understand that Geehy does not bear any responsibility for such errors that may occur in this document. The relevant data in this document are only used to guide users as performance parameter reference and do not constitute Geehy's guarantee for any product performance.

Users shall select appropriate Geehy products according to their own needs, and effectively verify and test the applicability of Geehy products to confirm that Geehy products meet their own needs, corresponding standards, safety or other reliability requirements. If losses are caused to users due to user's failure to fully verify and test Geehy products, Geehy will not bear any responsibility.

5. Legality

USERS SHALL ABIDE BY ALL APPLICABLE LOCAL LAWS AND REGULATIONS WHEN USING THIS DOCUMENT AND THE MATCHING GEEHY PRODUCTS. USERS SHALL UNDERSTAND THAT THE PRODUCTS MAY BE RESTRICTED BY THE EXPORT, RE-EXPORT OR OTHER LAWS OF THE COUNTRIES OF THE PRODUCTS SUPPLIERS, GEEHY, GEEHY DISTRIBUTORS AND USERS. USERS (ON BEHALF OR ITSELF, SUBSIDIARIES AND AFFILIATED ENTERPRISES) SHALL AGREE AND PROMISE TO ABIDE BY ALL APPLICABLE LAWS AND REGULATIONS ON THE EXPORT AND RE-EXPORT OF GEEHY PRODUCTS AND/OR TECHNOLOGIES AND DIRECT PRODUCTS.

6. Disclaimer of Warranty

THIS DOCUMENT IS PROVIDED BY GEEHY "AS IS" AND THERE IS NO WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, TO THE EXTENT PERMITTED BY APPLICABLE LAW.

GEEHY'S PRODUCTS ARE NOT DESIGNED, AUTHORIZED, OR WARRANTED FOR USE AS CRITICAL COMPONENTS IN MILITARY, LIFE-SUPPORT, POLLUTION CONTROL, OR HAZARDOUS SUBSTANCES MANAGEMENT SYSTEMS, NOR WHERE FAILURE COULD RESULT IN INJURY, DEATH, PROPERTY OR ENVIRONMENTAL DAMAGE.

IF THE PRODUCT IS NOT LABELED AS "AUTOMOTIVE GRADE," IT SHOULD NOT BE CONSIDERED SUITABLE FOR AUTOMOTIVE APPLICATIONS. GEEHY ASSUMES NO LIABILITY FOR THE USE BEYOND ITS SPECIFICATIONS OR GUIDELINES.

THE USER SHOULD ENSURE THAT THE APPLICATION OF THE PRODUCTS COMPLIES WITH ALL RELEVANT STANDARDS, INCLUDING BUT NOT LIMITED TO SAFETY, INFORMATION SECURITY, AND ENVIRONMENTAL REQUIREMENTS. THE USER ASSUMES FULL RESPONSIBILITY FOR THE SELECTION AND USE OF GEEHY PRODUCTS. GEEHY WILL BEAR NO RESPONSIBILITY FOR ANY DISPUTES ARISING FROM THE SUBSEQUENT DESIGN OR USE BY USERS.

7. Limitation of Liability

IN NO EVENT, UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL GEEHY OR ANY OTHER PARTY WHO PROVIDES THE DOCUMENT AND PRODUCTS "AS IS", BE LIABLE FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, DIRECT, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE DOCUMENT AND PRODUCTS (INCLUDING BUT NOT LIMITED TO LOSSES OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY USERS OR THIRD PARTIES). THIS COVERS POTENTIAL DAMAGES TO PERSONAL SAFETY, PROPERTY, OR THE ENVIRONMENT, FOR WHICH GEEHY WILL NOT BE RESPONSIBLE.

8. Scope of Application

The information in this document replaces the information provided in all previous versions of the document.