密码算法库使用指南

V1.1.0

国民技术股份有限公司 NSING TECHNOLOGIES INC.
地址：深圳市南山区高新北区宝深路109号国民技术大厦
电话：+86-755-86309900 传真：+86-755-86169100
网址：https://www.nsingtech.com 邮编：518057

声明

国民技术股份有限公司（下称“国民技术”）对此文档拥有专属产权。依据中华人民共和国的法律、条约以及世界其他法域相适用的管辖，此文档及其中描述的国民技术产品（下称“产品”）为公司所有。

国民技术在此并未授予专利权、著作权、商标权或其他任何知识产权许可。所提到或引用的第三方名称或品牌（如有）仅用作区别之目的。

国民技术保留随时变更、订正、增强、修改和改良此文档的权利，恕不另行通知。请使用人在下单购买前联系国民技术获取此文档的最新版本。

国民技术竭力提供准确可信的资讯，但即便如此，并不推定国民技术对此文档准确性和可靠性承担责任。

使用此文档信息以及生成产品时，使用者应当进行合理的设计、编程并测试其功能性和安全性，国民技术不对任何因使用此文档或本产品而产生的任何直接、间接、意外、特殊、惩罚性或衍生性损害结果承担责任。

国民技术对于产品在系统或设备中的应用效果没有任何故意或保证，如有任何应用在其发生操作不当或故障情况下，有可能致使人员伤亡、人身伤害或严重财产损失，则此类应用被视为“不安全使用”。

不安全使用包括但不限于：外科手术设备、原子能控制仪器、飞机或宇宙飞船仪器、所有类型的安全装置以及其他旨在支持或维持生命的应用。

所有不安全使用的风险应由使用人承担，同时使用人应使国民技术免于因为这类不安全使用而导致被诉、支付费用、发生损害或承担责任时的赔偿。

对于此文档和产品的任何明示、默示之保证，包括但不限于适销性、特定用途适用性和不侵权的保证责任，国民技术可在法律允许范围内进行免责。

未经明确许可，任何人不得以任何理由对此文档的全部或部分进行使用、复制、修改、抄录和传播。

国民技术股份有限公司 NSING TECHNOLOGIES INC.
地址：深圳市南山区高新北区宝深路109号国民技术大厦
电话：+86-755-86309900 传真：+86-755-86169100
网址：https://www.nsingtech.com 邮编：518057

注 意

这是国民技术不便于披露的文件，它包含一些保密的信息。在没有签订任何保密协议前或者在国民技术单方面要求的情况下请归还于国民技术。任何非国民技术委托人不得使用或者参考该文件。

如果你得到了这份文件，请注意：

- 不得公开文档内容
- 不得转载全部或部分文档内容
- 不得修改全部或部分文档内容

在以下情况这份文件必须销毁

- 国民技术已经提供更新的版本
- 未签订保密协议或者保密协议已经过期
- 受委托人离职

给我们的客户

我们一直在不断的改进我们的产品及说明文档的品质。我们努力保证这份文档的说明是准确的，但也可能存在一些我们未曾发现的失误。如果您发现了文档中有任何疑问或错失的地方请及时联系我们。您的理解及支持将使得这份文档更加完善。

国民技术股份有限公司 NSING TECHNOLOGIES INC.
地址：深圳市南山区高新北区宝深路109号国民技术大厦
电话：+86-755-86309900 传真：+86-755-86169100
网址：https://www.nsingtech.com 邮编：518057

版本历史

版本	日期	备注
V1.0.0	2025.04.28	新建文档
V1.0.1	2025.08.21	1，修改页眉的 logo
V1.1.0	2026.1.15	1，文件重命名

国民技术股份有限公司 NSING TECHNOLOGIES INC.
地址：深圳市南山区高新北区宝深路109号国民技术大厦
电话：+86-755-86309900 传真：+86-755-86169100
网址：https://www.nsingtech.com 邮编：518057

术语及缩略语

缩写	全拼
AES	Advance Encryption Standard
DES	Data Encryption standard
TDES	Triple Data Encryption standard
RNG	Random Number Generator
SHA	Secure Hashing Algorithm are required for digital signature applications

国民技术股份有限公司 NSING TECHNOLOGIES INC.
地址：深圳市南山区高新北区宝深路109号国民技术大厦
电话：+86-755-86309900 传真：+86-755-86169100
网址：https://www.nsingtech.com 邮编：518057

目 录

目 录 ..... - 6 -

1. 概述 ..... - 9 -

1.1. 支持的算法 ..... - 9 -

1.2. 基本数据类型 ..... - 9 -

2. DES/TDES 算法 API 说明 ..... - 10 -

2.1. 算法库使用方法 ..... - 10 -

2.2. 数据类型定义 ..... - 10 -

2.3. 函数接口说明 ..... - 11 -

2.3.1. DES/TDES 算法初始化函数 ..... - 11 -

2.3.2. DES/TDES 算法加解密函数 ..... - 12 -

2.3.3. DES/TDES 关闭函数 ..... - 12 -

2.3.4. DES/TDES 库获取版本信息函数 ..... - 13 -

3. AES 算法 API 说明 ..... - 14 -

3.1. 算法库使用方法 ..... - 14 -

3.2. 数据类型定义 ..... - 14 -

3.3. 函数接口说明 ..... - 15 -

3.3.1. AES 算法初始化函数 ..... - 15 -

3.3.2. AES 算法加解密函数 ..... - 15 -

3.3.3. AES 关闭函数 ..... - 16 -

3.3.4. AES 库获取版本信息函数 ..... - 16 -

4. HASH 算法 API 说明 ..... - 18 -

4.1. 算法库使用方法 ..... - 18 -

4.2. 数据类型定义 ..... - 18 -

4.3. 函数接口说明 ..... - 20 -

4.3.1. HASH 初始化函数 ..... - 20 -

国民技术股份有限公司 NSING TECHNOLOGIES INC.
地址：深圳市南山区高新北区宝深路109号国民技术大厦
电话：+86-755-86309900 传真：+86-755-86169100
网址：https://www.nsingtech.com 邮编：518057

4.3.2. HASH 分步开始运算函数 - 21 -

4.3.3. HASH 分步处理函数 - 21 -

4.3.4. HASH 分步完成函数 - 22 -

4.3.5. HASH 单次杂凑函数 - 22 -

4.3.6. HASH 关闭函数 - 23 -

4.3.7. HASH 库获取版本信息函数 - 23 -

5. RNG 算法 API 说明 - 25 -

5.1. 算法库使用方法 - 25 -

5.2. 数据类型定义 - 25 -

5.3. 函数接口说明 - 25 -

5.3.1. 伪随机数初始化函数 - 26 -

5.3.2. 伪随机数种子更新函数 - 26 -

5.3.3. 伪随机生成函数 - 26 -

5.3.4. 真随机数按字生成函数 - 27 -

5.3.5. 真随机数按字节生成函数 - 27 -

5.3.6. 获取 RNG 库版本信息 - 27 -

6. SM4 算法 API 说明 - 29 -

6.1. 算法库使用方法 - 29 -

6.2. 数据类型定义 - 29 -

6.3. 函数接口说明 - 30 -

6.3.1. SM4 模块初始化 - 30 -

6.3.2. SM4 模块加解密 - 31 -

6.3.3. SM4 关闭 - 31 -

6.3.4. 获取 SM4 库版本信息 - 32 -

I. 法库函数调用例程 - 33 -

II. 附录二 AES 算法库函数调用例程 - 41 -

国民技术股份有限公司 NSING TECHNOLOGIES INC.
地址：深圳市南山区高新北区宝深路109号国民技术大厦
电话：+86-755-86309900 传真：+86-755-86169100
网址：https://www.nsingtech.com 邮编：518057

III. 附录三 HASH 算法库函数调用例程 ..... - 53 -

III.1 HASH_TEST ..... - 53 -

III.2 HASH_SINGLE_TEST ..... - 57 -

III.3 HASH_SUBSTEP_TEST ..... - 58 -

IV. 附录四 RNG 算法库调用例程 ..... - 61 -

IV.1 伪随机 ..... - 61 -

IV.2 真随机 ..... - 61 -

V. 附录五 SM4 算法库函数调用例程 ..... - 63 -

国民技术股份有限公司 NSING TECHNOLOGIES INC.
地址：深圳市南山区高新北区宝深路109号国民技术大厦
电话：+86-755-86309900 传真：+86-755-86169100
网址：https://www.nsingtech.com 邮编：518057

1. 概述

本文档适用于已下载相关算法的 N32H7xx 芯片，主要说明该类芯片中算法接口和使用方法。

1.1. 支持的算法

N32H7xx 芯片提供的算法如下：

- DES: ECB/CBC 加密/解密
- TDES: ECB/CBC 加密/解密
- AES: ECB/CBC/CTR 加密/解密（AES-128/192/256）
- HASH: 获取摘要，支持（SHA1/224/256/384/512）
- SM4: ECB/CBC 加密解密
- RNG: 随机数生成

1.2. 基本数据类型

```
typedef    unsigned          char uint8_t;
typedef    unsigned short    int uint16_t;
typedef    unsigned          int uint32_t;
typedef    unsigned          __INT64 uint64_t;
typedef    signed            char int8_t;
typedef    signed short      int int16_t;
typedef    signed            int int32_t;
typedef    signed            __INT64 int64_t;
```


国民技术股份有限公司 NSING TECHNOLOGIES INC.
地址：深圳市南山区高新北区宝深路109号国民技术大厦
电话：+86-755-86309900 传真：+86-755-86169100
网址：https://www.nsingtech.com 邮编：518057

2. DES/TDES算法API说明

2.1. 算法库使用方法

算法库使用方法如下：

1. 将 DES.h、Common.h 加入头文件夹中；将 Common.lib、DES.lib 添加到工程中；
2. 按 2.3 节函数说明调用函数，例程见附录一提供的 demo。

2.2. 数据类型定义

```
enum DES
{
    DES_Init_OK = 0x2a2a7a7a,          //DES opreation success
    DES_Crypto_OK = 0x2a2a7a7a,        //DES opreation success
    DES_ModeErr = 0x5a5a5a5a,          //Working mode error(Neither ECB nor CBC)
    DES_EnDeErr,                       //En&De error(Neither encryption nor decryption)
    DES_ParaNull,                      // the part of input(output/iv) Null
    DES_KeyLenErr,
    DES_LengthErr,
    DES_ATTACKED,                       //DES subjected to attack
};
typedef struct
{
        uint8_t *in;              // the part of input to be encrypted or decrypted
        uint8_t *iv;              // the part of initial vector
        uint8_t *out;             // the part of out
        uint8_t *key;             // the part of key
        uint32_t inByteLen;       // the length(by byte) of plaintext or cipher
```


国民技术股份有限公司 NSING TECHNOLOGIES INC.
地址：深圳市南山区高新北区宝深路109号国民技术大厦
电话：+86-755-86309900 传真：+86-755-86169100
网址：https://www.nsingtech.com 邮编：518057

```
    uint32_t En_De;          // 0x33333333- encrypt, 0x44444444 - decrypt
    uint32_t Mode;           // 0x11111111 - ECB, 0x22222222 - CBC
    uint32_t keyByteLen;     //the length(by byte) of key
}DES_PARM;

typedef  DES_PARM  TDES_PARM;
```

2.3. 函数接口说明

DES/TDES 算法库包含的函数列表如下：

表 2-1 DES/TDES 算法库函数表

函数	描述
uint32_t DES_Init(DES_PARM *parm) #define TDES_Init DES_Init	DES/TDES 初始化函数
uint32_t DES_Crypto1(DES_PARM *parm) #define TDES_Crypto1 DES_Crypto1	DES/TDES 加解密函数
Void DES_Close(void) #define TDES_Close DES_Close	DES/TDES 关闭函数
void DES_Version(uint8_t *type, uint8_t *customer, uint8_t date[3], uint8_t *version) #define TDES_Version DES_Version	DES//TDES 版本获取函数

2.3.1. DES/TDES算法初始化函数

DES_Init DES/TDES 算法初始化

函数原型 uint32_t DES_Init(DES_PARM *parm)

参数说明 DES_Parm 输入，指向 DES_PARM 结构体的指针

返回值 DES_Init_OK：初始化成功 其他：初始化错误

注意事项 1. 若是 ECB 模式，则参数 iv1、iv2 可直接用 NULL 替换。

国民技术股份有限公司 NSING TECHNOLOGIES INC.
地址：深圳市南山区高新北区宝深路109号国民技术大厦
电话：+86-755-86309900 传真：+86-755-86169100
网址：https://www.nsingtech.com 邮编：518057

2. 用户使用 TDES 时，可以把 TDES_Init、*TDES_PARM 分别*替换 DES_Init、*DES_PARM*，变成 TDES_Init (*TDES_PARM* *parm)使用。

2.3.2. DES/TDES算法加解密函数

DES_Crypto	DES/TDES 算法加解密
函数原型	uint32_t DES_Crypto1(DES_PARM *parm)
参数说明	DES_Parm　　输入，指向 DES_PARM 结构体的指针
返回值	DES_Crypto_OK：运算正确　　其他：运算错误
注意事项	

1. 若是 ECB 模式，则参数 iv1、iv2 可直接用 NULL 替换。
2. 用户使用 TDES 时，可以把 TDES_Crypto、*TDES_PARM 分别*替换 DES_Crypto、*DES_PARM*，变成 TDES_Crypto (*TDES_PARM* *parm)使用。
3. 大量数据作为一整体但分多块进行 CBC 加密时，需注意：

第 X 块数据（X>1）调用本函数进行加密，使用的初始向量 IV（IV = iv1）一定要更新为第 X-1 块数据调用本函数进行加密得到的密文的最后一个分组（8 字节）。

4. 大量数据作为一整体但分多块进行 CBC 解密时，需注意：

第 X 块数据（X>1）调用本函数进行解密，使用的初始向量 IV（IV = iv1）一定要更新为第 X-1 块数据的最后一个分组（8 字节）。

5.调用方式请参考附录一。

2.3.3. DES/TDES关闭函数

DES_Close	关闭 DES/TDES 算法时钟和系统时钟
函数原型	void DES_Close(void)
参数说明	无
返回值	无

国民技术股份有限公司 NSING TECHNOLOGIES INC.
地址：深圳市南山区高新北区宝深路109号国民技术大厦
电话：+86-755-86309900　　传真：+86-755-86169100
网址：https://www.nsingtech.com 邮编：518057

注意事项	1. 用户使用 TDES 时，可以把 TDES_ Close 替换 DES_Close，变成 TDES_ Close (void)使用。

2.3.4. DES/TDES库获取版本信息函数

DES_Version	DES/TDES 库获取版本信息
函数原型	void DES_Version(uint8_t *type, uint8_t *customer, uint8_t date[3], uint8_t *version)
参数说明	type 商业或安全版本 customer 标准或定制版本 date 年，月，日 version 版本 x.x
返回值	

注意事项	*type = 0x03; // 商业和安全版
	*customer = 0x00; // 标准版本
	date[0] = 25; // Year()
	date[1] = 04; // Month()
	date[2] = 27; // Day ()
	*version = 0x10; // 表示版本 1.0

1.	用户使用 TDES 时，可以把 TDES_Version 替换 DES_Version，变成 TDES_Version (uint8_t *type, uint8_t *customer, uint8_t date[3], uint8_t *version) 使用。

国民技术股份有限公司 NSING TECHNOLOGIES INC.
地址：深圳市南山区高新北区宝深路109号国民技术大厦
电话：+86-755-86309900 传真：+86-755-86169100
网址：https://www.nsingtech.com 邮编：518057

3. AES算法API说明

3.1. 算法库使用方法

算法库使用方法如下：

1. 将 AES.h、Common.h 加入头文件夹中；将 Common.lib、AES.lib 添加到工程中；
2. 按 3.3 节函数说明调用函数，例程见附录二提供的 demo

3.2. 数据类型定义

```
enum{
        AES_Init_OK = 0x3a3a5a5a,       //AES opreation success
        AES_Crypto_OK=0x3a3aa5a5,       //AES opreation success
        AES_ModeErr= 0x5a5a5a5a,        //Working mode error(Neither ECB nor CBC,CTR)
        AES_EnDeErr,                    // En&De error(Neither encryption nor decryption)
        AES_ParaNull,                   // the part of input(output/iv) Null
        AES_LengthErr,
        AES_KeyLengthError,
        AES_ATTACKED,                   //AES subjected to attack
};
typedef struct
{
    uint8_t *in;            // the part of input to be encrypted or decrypted
    uint8_t *iv;            // the part of initial vector
    uint8_t *out;           // the part of out
    uint8_t *key;           // the part of key
    uint32_t keyBytelen;    // the length(by byte) of key
    uint32_t inBytelen;     // the length(by byte) of plaintext or cipher
```


国民技术股份有限公司 NSING TECHNOLOGIES INC.
地址：深圳市南山区高新北区宝深路109号国民技术大厦
电话：+86-755-86309900 传真：+86-755-86169100
网址：https://www.nsingtech.com 邮编：518057

```
    uint32_t En_De;      // 0x44444444- encrypt, 0x55555555 - decrypt
    uint32_t Mode;       // 0x11111111 - ECB, 0x22222222 - CBC,0x33333333-AES_CTR
}AES_PARM;
```

3.3. 函数接口说明

AES 算法库包含的函数列表如下：

表 3-1　AES 算法库函数表

函数	描述
uint32_t　AES_Init(AES_PARM *parm)	AES 初始化函数
uint32_t AES_Crypto(AES_PARM *parm)	AES 加解密函数
void AES_Close(void)	AES 关闭函数
void AES_Version(uint8_t *type, uint8_t *customer, uint8_t date[3], uint8_t *version)	AES 版本获取函数

3.3.1. AES算法初始化函数

AES_Init　　AES 算法初始化

函数原型　　uint32_t　AES_Init(AES_PARM *parm)

参数说明　　AES _Parm　　输入，指向 AES _PARM 结构体的指针

返回值　　AES_Init_OK：初始化成功　　其他：初始化错误

注意事项　　1. 若是 ECB 模式，则参数 iv 可直接用 NULL 替换。

3.3.2. AES算法加解密函数

AES_Crypto　　AES 算法加解密

函数原型　　uint32_t AES_Crypto(AES_PARM *parm)

参数说明　　AES _Parm　　输入，指向 AES _PARM 结构体的指针

国民技术股份有限公司 NSING TECHNOLOGIES INC.
地址：深圳市南山区高新北区宝深路109号国民技术大厦
电话：+86-755-86309900　　传真：+86-755-86169100
网址：https://www.nsingtech.com 邮编：518057

返回值 AES_Crypto_OK：运算正确 其他：运算错误

注意事项 1. 若是 ECB 模式，则参数 iv 可直接用 NULL 替换。

2. 大量数据作为一整体但分多块进行 CBC 或者 CTR 加密时，需注意：

第 X 块数据（X>1）调用本函数进行加密，使用的初始向量 iv

一定要更新为第 X-1 块数据调用本函数进行加密得到的密文的最后一个分组（16 字节）。

4. 大量数据作为一整体但分多块进行 CBC 解密时，需注意：

第 X 块数据（X>1）调用本函数进行解密，使用的初始向量 iv

一定要更新为第 X-1 块数据的最后一个分组（16 字节）。

3.3.3. AES关闭函数

AES_Close 关闭 AES 算法时钟和系统时钟

函数原型 void AES_Close(void)

参数说明 无

返回值 无

注意事项

3.3.4. AES库获取版本信息函数

AES_Version 获取 AES 库版本信息

函数原型 void AES_Version(uint8_t *type, uint8_t *customer, uint8_t date[3], uint8_t *version)

参数说明

type	商业或安全版本
customer	标准或定制版本
date	年，月，日
version	版本 x.x

国民技术股份有限公司 NSING TECHNOLOGIES INC.
地址：深圳市南山区高新北区宝深路109号国民技术大厦
电话：+86-755-86309900 传真：+86-755-86169100
网址：https://www.nsingtech.com 邮编：518057

返回值

注意事项

*type = 0x03;　　// 商业和安全版

*customer = 0x00; // 标准版本

date[0] = 25; //Year()

date[1] = 04; //Month()

date[2] = 27 //Day ()

*version = 0x10;　//表示版本 1.0

国民技术股份有限公司 NSING TECHNOLOGIES INC.
地址：深圳市南山区高新北区宝深路109号国民技术大厦
电话：+86-755-86309900　　传真：+86-755-86169100
网址：https://www.nsingtech.com 邮编：518057

4. HASH算法API说明

包括 SHA256 算法库。

4.1. 算法库使用方法

数据输入及输出均采用字节大端顺序。算法库使用方法如下：

1. 将 HASH.h、Common_lib.h 加入头文件夹中，将、Common.lib、HASH.lib 添加到工程中；
2. 按 4.3 节函数说明调用函数，例程见附录三提供的 demo

4.2. 数据类型定义

```
enum
{
    HASH_SEQUENCE_TRUE = 0x0105A5A5,     //save IV
    HASH_SEQUENCE_FALSE = 0x010A5A5A,    //not save IV
    HASH_Init_OK = 0x5a5a5a5a,           //hash init success
    HASH_Start_OK = 0x5a5a5a5a,          //hash update success
    HASH_Update_OK = 0x5a5a5a5a,         //hash update success
    HASH_Complete_OK = 0x5a5a5a5a,       //hash complete success
    HASH_Close_OK = 0x5a5a5a5a,          //hash close success
    HASH_ByteLenPlus_OK = 0x5a5a5a5a,    //byte length plus success
    HASH_PadMsg_OK = 0x5a5a5a5a,         //message padding success
    HASH_ProcMsgBuf_OK = 0x5a5a5a5a,     //message processing success
    SM3_Hash_OK = 0x5a5a5a5a,            //sm3 operation success
    SHA256_Hash_OK = 0x5a5a5a5a,         //sha256 operation success
    SHA1_Hash_OK = 0,                    //sha1 operation success
    SHA224_Hash_OK = 0,                  //sha224 operation success
    SHA384_Hash_OK = 0,                  //sha384 operation success
```


国民技术股份有限公司 NSING TECHNOLOGIES INC.
地址：深圳市南山区高新北区宝深路109号国民技术大厦
电话：+86-755-86309900 传真：+86-755-86169100
网址：https://www.nsingtech.com 邮编：518057

```
    SHA512_Hash_OK = 0,                 //sha512 operation success
    HASH_Init_ERROR = 0x01044400,       //hash init error
    HASH_Start_ERROR,                   //hash start error
    HASH_Update_ERROR,                  //hash update error
    HASH_Complete_ERROR,                //hash complete error
    HASH_ByteLenPlus_ERROR,             //hash byte plus error
    HASH_ATTACK,                        //hash operation subject to attack
};

typedef struct _HASH_CTX_ HASH_CTX;

typedef struct
{
    const uint16_t HashAlgID;           //choice hash algorithm
    //const uint32_t * const K, KLen;   //K and byte length of K
    const uint32_t * const IV, IVLen;   //IV and byte length of IV
    const uint32_t HASH_ALGCR, HASH_SACCR, HASH_HASHCTRL;   //relate registers
    const uint32_t BlockByteLen, BlockWordLen;      //byte length of block, word length of block
    const uint32_t DigestByteLen, DigestWordLen;    //byte length of digest,word length of digest
    const uint32_t Cycle;               //interation times
    uint32_t (* const ByteLenPlus)(uint32_t *, uint32_t);   //function pointer
    uint32_t (* const PadMsg)(HASH_CTX *);          //function pointer
}HASH_ALG;


typedef struct _HASH_CTX_
{
    const HASH_ALG      *hashAlg;   //pointer to HASH_ALG
```


国民技术股份有限公司 NSING TECHNOLOGIES INC.
地址：深圳市南山区高新北区宝深路109号国民技术大厦
电话：+86-755-86309900 传真：+86-755-86169100
网址：https://www.nsingtech.com 邮编：518057

```
    uint32_t    sequence;           // TRUE if the IV should be saved
    uint32_t    IV[16];
    uint32_t    msgByteLen[4];
    uint8_t     msgBuf[132];
    uint32_t    msgIdx;
}HASH_CTX;
```

4.3. 函数接口说明

HASH 算法库包含的函数列表如下：

表 4-1 HASH 算法库函数表

函数	描述
uint32_t HASH_Init(HASH_CTX *ctx)	HASH 初始化函数
uint32_t HASH_Start(HASH_CTX *ctx)	HASH 分步杂凑开始运算函数
uint32_t HASH_Update(HASH_CTX *ctx, uint8_t *in, uint32_t byteLen);	HASH 分步杂凑处理函数
uint32_t HASH_Complete(HASH_CTX *ctx, uint8_t *out)	HASH 分步杂凑完成函数
uint32_t SHA256_Hash(uint8_t* in,uint32_t byteLen, uint8_t* out);	HASH 单次杂凑函数
uint32_t HASH_Close(void)	HASH 关闭函数
void HASH_Version(uint8_t *type, uint8_t *customer, uint8_t date[3], uint8_t *version)	HASH 获取算法库版本函数

4.3.1. HASH初始化函数

HASH_Init	HASH 初始化
函数原型	uint32_t HASH_Init(HASH_CTX *ctx)
参数说明	ctx 输入，指向 HASH_CTX 结构体的指针

国民技术股份有限公司 NSING TECHNOLOGIES INC.
地址：深圳市南山区高新北区宝深路109号国民技术大厦
电话：+86-755-86309900 传真：+86-755-86169100
网址：https://www.nsingtech.com 邮编：518057

返回值	HASH_Init_OK：初始化成功　　其他：初始化错误
注意事项	1. ctx 必须指向 RAM 区，且指向的内容不可更改(为杂凑计算的中间状态和临时内容存储)，下同 2. 分步计算一段消息的杂凑值时，必须先调用本函数

4.3.2. HASH分步开始运算函数

HASH_Start	HASH 启动运算
函数原型	uint32_t　HASH_Start(HASH_CTX *ctx)
参数说明	ctx　　输入，指向 HASH_CTX 结构体的指针
返回值	HASH_Start_OK：运算正确　　其他：运算错误
注意事项	1. 若需要 HASH 运算过程中支持中断，将 ctx->sequence 置为 *HASH_SEQUENCE_TRUE，在中断结束后需要重新调用* HASH_Init 函数，然后再调用 HASH_Update 函数；否则，置为 *HASH_SEQUENCE*_FALSE。 **2.调用方式请参考附录四。**

4.3.3. HASH分步处理函数

HASH_Update	HASH 分步处理数据
函数原型	uint32_t HASH_Update(HASH_CTX *ctx, uint8_t *in, uint32_t byteLen)
参数说明	ctx　　输入，指向 HASH_CTX 结构体的指针 in　　输入，指要杂凑的信息 byteLen　　输入，指杂凑信息的字节长度
返回值	HASH_Update_OK：运算正确　　其他：运算错误
注意事项	1. 调用此函数前必须先调用初始化函数 HASH_Init 和 HASH_Start 2. ctx 必须指向 RAM 区，且指向的内容不可更改(为杂凑计算的中间状态和临时内容存储)。 3. in 内容可指向 RAM 或 Flash 区。

国民技术股份有限公司 NSING TECHNOLOGIES INC.
地址：深圳市南山区高新北区宝深路109号国民技术大厦
电话：+86-755-86309900　　传真：+86-755-86169100
网址：https://www.nsingtech.com 邮编：518057

4. byteLen 可以是 0，即调用此函数没有任何效果。

5. 初始化后，对一整块消息可任意分割成多小块，对每一小块消息可依次调用此函数，最后调用 HASH_Complete 函数，即可得到这一整块消息的杂凑结果。

6.若需要级联应用，需要将 *ctx->sequence = HASH_SEQUENCE_TRUE*，把外部的 IV 拷贝到 ctx->IV，并且把已 Update 的数据长度 len 用 ctx->hashAlg->ByteLenPlus(ctx->msgByteLen,len)加到 ctx->msgByteLen，然后调用 HASH_Update 函数，才能级联成功。

7. 调用方式请参考附录四。

4.3.4. HASH分步完成函数

HASH_Complete	HASH 完成并取结果
函数原型	uint32_t HASH_Complete(HASH_CTX *ctx, uint8_t *out)
参数说明	ctx　　输入，指向 HASH_CTX 结构体的指针 out　　输出，指向 HASH 结果的指针
返回值	HASH_Complete_OK：运算正确　　其他：运算错误
注意事项	1. 消息输入完毕，调用此函数才能获得最终结果， 2. ctx 必须指向 RAM 区，且指向的内容不可更改(为杂凑计算的中间状态和临时内容存储)。 3.调用方式请参考附录四。

4.3.5. HASH单次杂凑函数

XXX_HASH	HASH 单次杂凑并取结果
函数原型	uint32_t XXX_Hash(uint8_t* in,uint32_t byteLen, uint8_t* out)
参数说明	XXX_Hash 可选：SM3_Hash、SHA1_Hash、SHA224_Hash、SHA256_Hash、SHA384_Hash、SHA512_Hash

国民技术股份有限公司 NSING TECHNOLOGIES INC.
地址：深圳市南山区高新北区宝深路109号国民技术大厦
电话：+86-755-86309900　　传真：+86-755-86169100
网址：https://www.nsingtech.com 邮编：518057

	in 输入，指向消息的指针
	byteLen 输入，消息的字节长度
	out 输出，指向 HASH 结果的指针
返回值	XXX_Hash_OK：运算正确 其他：运算错误
注意事项	1. 此函数适用短消息单次杂凑运算。
	2. 可单独调用此函数，无需调用初始化函数。
	3.调用方式请参考附录四。

4.3.6. HASH关闭函数

HASH_Close	HASH 运算关闭
函数原型	uint32_t HASH_Close(void)
参数说明	
返回值	HASH_Close_OK：关闭成功 其他：关闭错误
注意事项	

4.3.7. HASH库获取版本信息函数

HASH_Version	获取 HASH 库版本信息
函数原型	void HASH_Version(uint8_t *type, uint8_t *customer, uint8_t date[3], uint8_t *version)
参数说明	type 商业或安全版本
	customer 标准或定制版本
	date 年，月，日
	version //版本 x.x
返回值	
注意事项	*type = 0x03; // 商业和安全版

国民技术股份有限公司 NSING TECHNOLOGIES INC.
地址：深圳市南山区高新北区宝深路109号国民技术大厦
电话：+86-755-86309900 传真：+86-755-86169100
网址：https://www.nsingtech.com 邮编：518057

```
*customer = 0x00;    // 标准版本
date[0] = 18;        //Year()
date[1] = 12;        //Month()
date[2] = 28;        //Day ()
*version = 0x10;     //表示版本 1.0
```


国民技术股份有限公司 NSING TECHNOLOGIES INC.
地址：深圳市南山区高新北区宝深路109号国民技术大厦
电话：+86-755-86309900 传真：+86-755-86169100
网址：https://www.nsingtech.com 邮编：518057

5. RNG算法API说明

5.1. 算法库使用方法

算法库使用方法如下：

1、将 RNG.h、Common.h 加入头文件夹中，将 RNG.lib 、Common.lib 添加到工程中；

2、按 5.3 节函数说明调用函数，例程见附录四提供的 demo。

5.2. 数据类型定义

```
enum{
    RNG_OK = 0x5a5a5a5a,          //RNG generation process is ok
    RNG_LENError = 0x311ECF50,    //RNG generation of key length error
    RNG_ADDRError = 0x63BB4C39,   //This return value is not used
    RNG_ADDRNULL = 0x7A9DB86C,    // This address is empty
    RNG_Attack = 0x4794674F,      //The RNG generation process is attacked
    RNG_ModeError=0x479467aa,     //RNG choose mode is fail
    RNG_TESTFAIL=0x479467bb,      //RNG test is fail
    RNG_SEEDNULL=0x479467cc,      //RNG seed is NULL
};
```

5.3. 函数接口说明

RNG 算法库包含的函数列表如下：

表 5-1　RNG 算法库函数表

函数	描述
uint32_t GetTrueRand_U32(uint32_t *rand, uint32_t wordLen)	真随机数按字生成函数
uint32_t GetTrueRand_U8(uint8_t *rand, uint32_t bytelen)	真随机数按字节生成函数

国民技术股份有限公司 NSING TECHNOLOGIES INC.
地址：深圳市南山区高新北区宝深路109号国民技术大厦
电话：+86-755-86309900　　传真：+86-755-86169100
网址：https://www.nsingtech.com 邮编：518057

uint32_t PseudoRandNumInit(uint32_t seed[5])	伪随机数初始化函数
uint32_t PseudoRandNumReseed(uint32_t seed[5])	伪随机数种子更新函数
uint32_t GetPseudoRand_U32(uint32_t *rand, uint32_t wordLen)	伪随机数按字生成函数
void RNG_Version(uint8_t *type, uint8_t *customer, uint8_t date[3], uint8_t *version)	获取 RNG 库版本信息

5.3.1. 伪随机数初始化函数

PseudoRandNumInit 伪随机数模块初始化

函数原型 uint32_t PseudoRandNumInit(uint32_t seed[5])

参数说明 seed 输入，伪随机种子变量数组，可以为 NULL，当为 NULL 时，内部取真随机数为种子

返回值 RNG_OK 成功 ；其他 初始化出错

5.3.2. 伪随机数种子更新函数

PseudoRandNumReseed 伪随机数种子更新

函数原型 uint32_t PseudoRandNumReseed (uint32_t seed[5])

参数说明 seed 输入，伪随机种子变量数组，可以为 NULL，当为 NULL 时，内部取真随机数为种子

返回值 RNG_OK 成功 ；其他 初始化出错

注意事项 首次调用次函数时，必须先调用 PseudoRandNumInit 初始化函数

5.3.3. 伪随机生成函数

GetPseudoRand_U32 伪随机数按 word 生成函数

函数原型 uint32_t GetPseudoRand_U32(uint32_t *rand, uint32_t wordLen)

参数说明 rand 指针，指向生成的随机数

wordlen: 拟获取伪随机数word长

国民技术股份有限公司 NSING TECHNOLOGIES INC.
地址：深圳市南山区高新北区宝深路109号国民技术大厦
电话：+86-755-86309900 传真：+86-755-86169100
网址：https://www.nsingtech.com 邮编：518057

返回值	RNG_OK 成功 ； 其他 生成伪随机数出错
说明	按word生成伪随机数
注意事项	首次调用伪随机生成时，必须先调用PseudoRandNumInit初始化函数和PseudoRandNumReseed更新种子函数，用户可输入种子数组，如果用户输入seed为NULL，则内部自动生成种子；
例程	

5.3.4. 真随机数按字生成函数

GetTrueRand_U32真随机数按字生成函数

函数原型	uint32_t GetTrueRand_U32(uint32_t *rand, uint32_t wordLen)
参数说明	rand: 指针，指向生成的随机数某内存地址 wordLen: 拟获取真随机数的字长度
返回值	RNG_OK 成功； 其他：生成真随机数出错，详见枚举类型值定义

5.3.5. 真随机数按字节生成函数

GetTrueRand_U32真随机数按字节生成函数

函数原型	uint32_t GetTrueRand_U8(uint8_t *rand, uint32_t bytelen)
参数说明	rand: 指针，指向生成的随机数某内存地址 bytelen: 拟获取真随机数的字节长度
返回值	RNG_OK 成功； 其他：生成真随机数出错，详见枚举类型值定义

5.3.6. 获取RNG库版本信息

RNG_Version 获取 RNG 库版本信息

函数原型	void RNG_Version(uint8_t *type, uint8_t *customer, uint8_t date[3], uint8_t *version)
参数说明	type 商业或安全版本 customer 标准或定制版本

国民技术股份有限公司 NSING TECHNOLOGIES INC.
地址：深圳市南山区高新北区宝深路109号国民技术大厦
电话：+86-755-86309900 传真：+86-755-86169100
网址：https://www.nsingtech.com 邮编：518057

date 年，月，日

version //版本 x.x

返回值

注意事项

```
*type = 0x03;        // 商业和安全版
*customer = 0x00;    // 标准版本
date[0] = 25;        //Year()
date[1] = 04;        //Month()
date[2] = 27;        //Day ()
*version = 0x10;     //表示版本 1.0
```


国民技术股份有限公司 NSING TECHNOLOGIES INC.
地址：深圳市南山区高新北区宝深路109号国民技术大厦
电话：+86-755-86309900 传真：+86-755-86169100
网址：https://www.nsingtech.com 邮编：518057

6. SM4算法API说明

6.1. 算法库使用方法

算法库使用方法如下：

1. 将 SM4.h、Common.h 加入头文件夹中，将 Common.lib、SM4.lib 添加到工程中，建议时钟加扰配置为关闭；
2. 按 6.3 节函数说明调用函数，例程见附录五提供的 demo

6.2. 数据类型定义

```
enum SM4_ENUM
{
    SM4_Init_OK = 0x5a5a5a5a,       //SM4 opreation success
    SM4_Crypto_OK=0x5a5a5a5a,       //SM4 opreation success
    SM4_ParaNull =0x27A90E35,       //the address    of input is NULL
    SM4_ModeErr,                    //working mode error(Neither ECB nor CBC)
    SM4_EnDeErr,                    // En&De error(Neither encryption nor decryption)
    SM4_LengthErr,                  //the byte length of input error
    SM4_ATTACKED,                   //SM4 subjected to attack
};


typedef struct{
    uint8_t *in;            // the part of input to be encrypted or decrypted
    uint8_t *iv;            // the part of initial vector
    uint8_t *out;           // the part of out
    uint8_t *key;           // the part of key
    uint32_t inBytelen;     //the word length of input or output
```


国民技术股份有限公司 NSING TECHNOLOGIES INC.
地址：深圳市南山区高新北区宝深路109号国民技术大厦
电话：+86-755-86309900 传真：+86-755-86169100
网址：https://www.nsingtech.com 邮编：518057

```
    uint32_t En_De;      //encrypt/decrypt
    uint32_t Mode;       // ECB/CBC
}SM4_PARM;
```

6.3. 函数接口说明

SM4 算法库包含的函数列表如下：

表 6-1　SM4 算法库函数表

函数	描述
uint32_t SM4_Init(SM4_PARM *parm)	SM4 算法初始化
uint32_t SM4_Crypto1(SM4_PARM *parm)	SM4 算法加密/解密
void SM4_Close(void)	SM4 算法关闭
void SM4_Version(uint8_t *type, uint8_t *customer, uint8_t date[3], uint8_t *version)	获取 SM4 库版本信息

6.3.1. SM4模块初始化

SM4_Init　初始化 SM4 模块

函数原型　uint32_t SM4_Init(SM4_PARM *parm)

参数说明　parm　输入，指向 SM4_PARM 结构体的指针

返回值　SM4_ *Init* _OK：初始化成功　其他值：计算错误，详见枚举类型值定义

注意事项

1. 结构体 SM4_PARM 参考 9.2 节 *SM4_PARM 的定义*。

2.若是 ECB 模式，则参数 iv1、iv2 可直接用 NULL 替换

3. 大量数据作为一整体但分多块进行 CBC 加密时，需注意：

第 X 块数据（X>1）调用本函数进行加密，使用的初始向量 IV（IV = iv1）一定要更新为第 X-1 块数据调用本函数进行加密得到的密文的最后一个分组（16 字节）。

国民技术股份有限公司 NSING TECHNOLOGIES INC.
地址：深圳市南山区高新北区宝深路109号国民技术大厦
电话：+86-755-86309900　传真：+86-755-86169100
网址：https://www.nsingtech.com 邮编：518057

4. 大量数据作为一整体但分多块进行 CBC 解密时，需注意：

第 X 块数据（X>1）调用本函数进行解密，使用的初始向量 IV（IV = iv1）一定要更新为第 X-1 块数据的最后一个分组（16 字节）

6.3.2. SM4模块加解密

SM4_Crypto	SM4 模块加解密
函数原型	uint32_t SM4_Crypto1(SM4_PARM *parm)
参数说明	parm　输入，指向 SM4_PARM 结构体的指针
返回值	SM4_Crypto_OK：运算正确　其他值：计算错误，详见枚举类型值定义
注意事项	

1. 结构体 SM4_PARM 参考 9.2 节 *SM4_PARM 的定义*。

2.若是 ECB 模式，则参数 iv1、iv2 可直接用 NULL 替换

3. 大量数据作为一整体但分多块进行 CBC 加密时，需注意：

第 X 块数据（X>1）调用本函数进行加密，使用的初始向量 IV（IV = iv1）一定要更新为第 X-1 块数据调用本函数进行加密得到的密文的最后一个分组（16 字节）。

4. 大量数据作为一整体但分多块进行 CBC 解密时，需注意：

第 X 块数据（X>1）调用本函数进行解密，使用的初始向量 IV（IV = iv1）一定要更新为第 X-1 块数据的最后一个分组（16 字节）

6.3.3. SM4关闭

SM4_Close	关闭 SM4 算法时钟
函数原型	void SM4_Close(void)
参数说明	
返回值	
注意事项	

国民技术股份有限公司 NSING TECHNOLOGIES INC.
地址：深圳市南山区高新北区宝深路109号国民技术大厦
电话：+86-755-86309900　传真：+86-755-86169100
网址：https://www.nsingtech.com 邮编：518057

6.3.4. 获取SM4库版本信息

SM4_Version	获取 SM4 库版本信息
函数原型	void SM4_Version(uint8_t *type, uint8_t *customer, uint8_t date[3], uint8_t *version)
参数说明	type 商业或安全版本 customer 标准或定制版本 date 年，月，日 version //版本 x.x
返回值	

注意事项	*type = 0x03; // 商业和安全版
	*customer = 0x00; // 标准版本
	date[0] = 25; //Year()
	date[1] = 04; //Month()
	date[2] = 27; //Day ()
	*version = 0x10; //表示版本 1.0

国民技术股份有限公司 NSING TECHNOLOGIES INC.
地址：深圳市南山区高新北区宝深路109号国民技术大厦
电话：+86-755-86309900 传真：+86-755-86169100
网址：https://www.nsingtech.com 邮编：518057

i. 法库函数调用例程

```
//所有数据都是字节大端，自然顺序
uint32_t DES_test()
{
    uint8_t
in_2[16]={0x81,0xc2,0xe1,0x52,0x47,0x80,0xba,0xcb,0x81,0xc2,0xe1,0x52,0x47,0x80,0xba,0xcb};
    uint8_t iV[8] = {0x11,0x50,0x37,0x58,0x1C,0x80,0xD5,0xF3};
    uint8_t key_8[8]={0x4c,0xfd,0x58,0x76,0x3b,0x79,0x51,0x86};
    uint8_t
key_16[16]={0x4c,0xfd,0x58,0x76,0x3b,0x79,0x51,0x86,0x61,0xf7,0x7c,0xc4,0x46,0xe9,0xf8,0x9d};
    uint8_t
key_24[24]={0x4c,0xfd,0x58,0x76,0x3b,0x79,0x51,0x86,0x61,0xf7,0x7c,0xc4,0x46,0xe9,0xf8,0x9d,0x1
1,0x50,0x37,0x58,0x1C,0x80,0xD5,0xF3};

    uint8_t
DES_ECB_ENC[16]={0x0B,0x09,0x3E,0x89,0x14,0xD6,0xE0,0xDA,0x0B,0x09,0x3E,0x89,0x14,0xD6
,0xE0,0xDA};
    uint8_t
T2DES_ECB_ENC[16]={0x0C,0x46,0x15,0x56,0x19,0x8D,0x09,0xA9,0x0C,0x46,0x15,0x56,0x19,0x8
D,0x09,0xA9};
    uint8_t
T3DES_ECB_ENC[16]={0x15,0xA2,0xB8,0xBA,0x3A,0xCA,0xEF,0x04,0x15,0xA2,0xB8,0xBA,0x3A,
0xCA,0xEF,0x04};
    uint8_t
DES_CBC_ENC[16]={0x15,0x95,0xB5,0xAC,0xC1,0x5A,0xFC,0x62,0x62,0xD0,0xF8,0xEE,0xB1,0xF
C,0x1B,0xA8};
```


国民技术股份有限公司 NSING TECHNOLOGIES INC.
地址：深圳市南山区高新北区宝深路109号国民技术大厦
电话：+86-755-86309900 传真：+86-755-86169100
网址：https://www.nsingtech.com 邮编：518057

```
    uint8_t
T2DES_CBC_ENC[16]={0x7E,0xE9,0xF8,0x19,0xBC,0x4D,0x1E,0xED,0xCD,0x0D,0x38,0x93,0xE5,0
x80,0x3A,0xD6};
    uint8_t
T3DES_CBC_ENC[16]={0xC4,0x2D,0x00,0x22,0x71,0x58,0x5F,0x91,0x3F,0x08,0x75,0xC4,0x18,0x9
3,0xF3,0xA7};
    uint8_t out1[18],out2[18];

    DES_PARM des_Parm={0};
    des_Parm.Mode = DES_ECB;
    des_Parm.En_De = DES_ENCRYPT;
    des_Parm.in=in_2;
    des_Parm.inByteLen=16;
    des_Parm.key=key_8;
    des_Parm.keyByteLen=8;
    des_Parm.out=out1+2;
    DES_Init(&des_Parm);
    DES_Crypto1(&des_Parm);
    if(memcmp(out1+2, DES_ECB_ENC, 16))
    {
        return 0x5A5A5A5A;
    }
    des_Parm.Mode = DES_ECB;
    des_Parm.En_De = DES_DECRYPT;
    des_Parm.in=out1+2;
    des_Parm.inByteLen=16;
    des_Parm.key=key_8;
    des_Parm.keyByteLen=8;
```


国民技术股份有限公司 NSING TECHNOLOGIES INC.
地址：深圳市南山区高新北区宝深路109号国民技术大厦
电话：+86-755-86309900 传真：+86-755-86169100
网址：https://www.nsingtech.com 邮编：518057

```
des_Parm.out=out2;
DES_Init(&des_Parm);
DES_Crypto1(&des_Parm);
if(memcmp(out2, in_2, 16))
{
    return 0x5A5A5A5A;
}

des_Parm.Mode = DES_ECB;
des_Parm.En_De = DES_ENCRYPT;
des_Parm.in=in_2;
des_Parm.inByteLen=16;
des_Parm.key=key_16;
des_Parm.keyByteLen=16;
des_Parm.out=out1+2;
DES_Init(&des_Parm);
DES_Crypto1(&des_Parm);
if(memcmp(out1+2, T2DES_ECB_ENC, 16))
{
    return 0x5A5A5A5A;
}
des_Parm.Mode = DES_ECB;
des_Parm.En_De = DES_DECRYPT;
des_Parm.in=out1+2;
des_Parm.inByteLen=16;
des_Parm.key=key_16;
des_Parm.keyByteLen=16;
des_Parm.out=out2;
```


国民技术股份有限公司 NSING TECHNOLOGIES INC.
地址：深圳市南山区高新北区宝深路109号国民技术大厦
电话：+86-755-86309900 传真：+86-755-86169100
网址：https://www.nsingtech.com 邮编：518057

```
DES_Init(&des_Parm);
DES_Crypto1(&des_Parm);
if(memcmp(out2, in_2, 16))
{
    return 0x5A5A5A5A;
}

des_Parm.Mode = DES_ECB;
des_Parm.En_De = DES_ENCRYPT;
des_Parm.in=in_2;
des_Parm.inByteLen=16;
des_Parm.key=key_24;
des_Parm.keyByteLen=24;
des_Parm.out=out1+2;
DES_Init(&des_Parm);
DES_Crypto1(&des_Parm);
if(memcmp(out1+2, T3DES_ECB_ENC, 16))
{
    return 0x5A5A5A5A;
}
des_Parm.Mode = DES_ECB;
des_Parm.En_De = DES_DECRYPT;
des_Parm.in=out1+2;
des_Parm.inByteLen=16;
des_Parm.key=key_24;
des_Parm.keyByteLen=24;
des_Parm.out=out2;
DES_Init(&des_Parm);
```


国民技术股份有限公司 NSING TECHNOLOGIES INC.
地址：深圳市南山区高新北区宝深路109号国民技术大厦
电话：+86-755-86309900 传真：+86-755-86169100
网址：https://www.nsingtech.com 邮编：518057

```
DES_Crypto1(&des_Parm);
if(memcmp(out2, in_2, 16))
{
    return 0x5A5A5A5A;
}

des_Parm.Mode = DES_CBC;
des_Parm.En_De = DES_ENCRYPT;
des_Parm.in=in_2;
des_Parm.inByteLen=16;
des_Parm.key=key_8;
des_Parm.keyByteLen=8;
des_Parm.iv=iV;
des_Parm.out=out1+2;
DES_Init(&des_Parm);
DES_Crypto1(&des_Parm);
if(memcmp(out1+2, DES_CBC_ENC, 16))
{
    return 0x5A5A5A5A;
}
des_Parm.Mode = DES_CBC;
des_Parm.En_De = DES_DECRYPT;
des_Parm.in=out1+2;
des_Parm.inByteLen=16;
des_Parm.key=key_8;
des_Parm.keyByteLen=8;
des_Parm.iv=iV;
des_Parm.out=out2;
```


国民技术股份有限公司 NSING TECHNOLOGIES INC.
地址：深圳市南山区高新北区宝深路109号国民技术大厦
电话：+86-755-86309900 传真：+86-755-86169100
网址：https://www.nsingtech.com 邮编：518057

```
DES_Init(&des_Parm);
DES_Crypto1(&des_Parm);
if(memcmp(out2, in_2, 16))
{
    return 0x5A5A5A5A;
}

des_Parm.Mode = DES_CBC;
des_Parm.En_De = DES_ENCRYPT;
des_Parm.in=in_2;
des_Parm.inByteLen=16;
des_Parm.key=key_16;
des_Parm.keyByteLen=16;
des_Parm.iv=iV;
des_Parm.out=out1+2;
DES_Init(&des_Parm);
DES_Crypto1(&des_Parm);
if(memcmp(out1+2, T2DES_CBC_ENC, 16))
{
    return 0x5A5A5A5A;
}
des_Parm.Mode = DES_CBC;
des_Parm.En_De = DES_DECRYPT;
des_Parm.in=out1+2;
des_Parm.inByteLen=16;
des_Parm.key=key_16;
des_Parm.keyByteLen=16;
des_Parm.iv=iV;
```


国民技术股份有限公司 NSING TECHNOLOGIES INC.
地址：深圳市南山区高新北区宝深路109号国民技术大厦
电话：+86-755-86309900 传真：+86-755-86169100
网址：https://www.nsingtech.com 邮编：518057

```
des_Parm.out=out2;
DES_Init(&des_Parm);
DES_Crypto1(&des_Parm);
if(memcmp(out2, in_2, 16))
{
    return 0x5A5A5A5A;
}

des_Parm.Mode = DES_CBC;
des_Parm.En_De = DES_ENCRYPT;
des_Parm.in=in_2;
des_Parm.inByteLen=16;
des_Parm.key=key_24;
des_Parm.keyByteLen=24;
des_Parm.iv=iV;
des_Parm.out=out1+2;
DES_Init(&des_Parm);
DES_Crypto1(&des_Parm);
DES_Init(&des_Parm);
DES_Crypto1(&des_Parm);
if(memcmp(out1+2, T3DES_CBC_ENC, 16))
{
    return 0x5A5A5A5A;
}
des_Parm.Mode = DES_CBC;
des_Parm.En_De = DES_DECRYPT;
des_Parm.in=out1+2;
des_Parm.inByteLen=16;
```


国民技术股份有限公司 NSING TECHNOLOGIES INC.
地址：深圳市南山区高新北区宝深路109号国民技术大厦
电话：+86-755-86309900 传真：+86-755-86169100
网址：https://www.nsingtech.com 邮编：518057

```
    des_Parm.key=key_24;
    des_Parm.keyByteLen=24;
    des_Parm.iv=iV;
    des_Parm.out=out2;
    DES_Init(&des_Parm);
    DES_Crypto1(&des_Parm);
    if(memcmp(out2, in_2, 16))
    {
        return 0x5A5A5A5A;
    }

    printf("DES_test is successed!\r\n");
}
```


国民技术股份有限公司 NSING TECHNOLOGIES INC.
地址：深圳市南山区高新北区宝深路109号国民技术大厦
电话：+86-755-86309900 传真：+86-755-86169100
网址：https://www.nsingtech.com 邮编：518057

ii.附录二 AES算法库函数调用例程

```
//所有数据都是字节大端，自然顺序

uint32_t aes_test()
{
    uint8_t
in[16]={0xFF,0xFF,0xFF,0xFF,0xFF,0xFF,0xFF,0xFF,0xFF,0xFF,0xFF,0xFF,0xFF,0xFF,0xFF,0xFF};
  uint8_t
iv[16]={0xA2,0x10,0x3F,0x84,0xA4,0x2E,0xDB,0x8A,0x0C,0xA0,0x97,0x70,0x4E,0x34,0x39,0x33};//
A2103F84A42EDB8A0CA097704E343933
    uint8_t
key128[16]={0xFE,0x7C,0x24,0x38,0x83,0xFA,0xBB,0x78,0xF4,0x59,0xCF,0xEB,0xCF,0x67,0x02,0x
79};//FE7C243883FABB78F459CFEBCF670279
    uint8_t
key192[24]={0x67,0x69,0x7E,0xDE,0x12,0xE8,0xC5,0x04,0xF5,0x88,0x4A,0x7E,0xA4,0x5B,0x6F,0x7
B,0xAB,0x92,0x2B,0x64,0xDA,0x88,0x00,0x04};

    uint8_t
key256[32]={0x89,0x02,0xF5,0xF3,0xA6,0xF5,0x84,0x50,0xB0,0xB9,0xD3,0xCF,0x30,0x82,
    0xD9,0xDA,0xF9,0xAA,0x18,0x3C,0xB9,0xF6,0xCF,0x86,0xCF,0x1B,0x70,0xB1,0x5C,0x81,0x54,
0x06};//8902F5F3A6F58450B0B9D3CF3082D9DAF9AA183CB9F6CF86CF1B70B15C815406
    uint8_t
ECB128_en[16]={0x4E,0xE6,0xF9,0x56,0xBF,0x80,0x04,0xF4,0x61,0x23,0xD4,0x26,0x24,0x47,0x03,
0x2A};
    uint8_t
CBC128_en[16]={0xFC,0x15,0x9F,0x65,0x7E,0x02,0xF7,0xEB,0x3A,0x5D,0xF0,0x8E,0x79,0x51,0xC
0,0x12};
```


国民技术股份有限公司 NSING TECHNOLOGIES INC.
地址：深圳市南山区高新北区宝深路109号国民技术大厦
电话：+86-755-86309900 传真：+86-755-86169100
网址：https://www.nsingtech.com 邮编：518057

```
    uint8_t
CTR128_en[16]={0x3B,0x7C,0xDB,0xED,0x8F,0xAD,0xEE,0x7C,0xA5,0x52,0x95,0x6D,0x7D,0x86,0
xCE,0xD5};
    uint8_t
ECB192_en[16]={0x1D,0x58,0x54,0x75,0x87,0xDA,0x23,0xBF,0xF4,0xD0,0xA6,0x33,0x4B,0x98,0x2
9,0xB6};
    uint8_t
CBC192_en[16]={0x9F,0x8C,0x2A,0x1C,0x9A,0x4F,0xE7,0x01,0xC6,0xF5,0x05,0x8F,0xD1,0x6A,0x1
1,0x89};
    uint8_t
CTR192_en[16]={0x64,0xFA,0x50,0x31,0xB8,0x46,0xD2,0xCD,0xBC,0x38,0x11,0x62,0xB5,0x9A,0x
C4,0x4C};
    uint8_t
ECB256_en[16]={0xF4,0xD2,0xC6,0xD4,0xD1,0x64,0x6B,0xBD,0xB3,0x66,0x80,0x94,0x9A,0xBD,0x
0A,0xF4};
    uint8_t
CBC256_en[16]={0x65,0x05,0xE9,0x66,0x5D,0x47,0x6A,0x33,0xB0,0xDB,0x2A,0x94,0xE6,0x1E,0x3
F,0xC5};
    uint8_t
CTR256_en[16]={0x75,0xC9,0x8F,0xF7,0x62,0x64,0x97,0x08,0xB3,0xE9,0xD0,0xC6,0x73,0x77,0x54,
0x69};


    uint8_t out1[19], out2[19];
    AES_PARM AES_Parm={0};
    AES_Parm.Mode = AES_CTR;
    AES_Parm.En_De = AES_ENCRYPT;
    AES_Parm.in=in;
```


国民技术股份有限公司 NSING TECHNOLOGIES INC.
地址：深圳市南山区高新北区宝深路109号国民技术大厦
电话：+86-755-86309900 传真：+86-755-86169100
网址：https://www.nsingtech.com 邮编：518057

```
AES_Parm.inBytelen=16;
AES_Parm.key=key128;
AES_Parm.keyBytelen=16;
AES_Parm.iv=iv;
AES_Parm.out=out1+1;

AES_Init(&AES_Parm);
AES_Crypto(&AES_Parm);
if(memcmp(out1+1,CTR128_en,16))
{
    return 0x6D;
}
AES_Parm.Mode = AES_CTR;
AES_Parm.En_De = AES_DECRYPT;
AES_Parm.in=out1+1;
AES_Parm.inBytelen=16;
AES_Parm.key=key128;
AES_Parm.keyBytelen=16;
AES_Parm.iv=iv;
AES_Parm.out=out2;
AES_Init(&AES_Parm);
AES_Crypto(&AES_Parm);
if(memcmp(out2,in,16))
{
    return 0x6D;
}

AES_Parm.Mode = AES_ECB;
```


国民技术股份有限公司 NSING TECHNOLOGIES INC.
地址：深圳市南山区高新北区宝深路109号国民技术大厦
电话：+86-755-86309900 传真：+86-755-86169100
网址：https://www.nsingtech.com 邮编：518057

```
AES_Parm.En_De = AES_ENCRYPT;
AES_Parm.in=in;
AES_Parm.inBytelen=16;
AES_Parm.key=key128;
AES_Parm.keyBytelen=16;
AES_Parm.iv=iv;
AES_Parm.out=out1+1;
AES_Init(&AES_Parm);
AES_Crypto(&AES_Parm);
if(memcmp(out1+1,ECB128_en,16))
{
    return 0x6D;
}
AES_Parm.Mode = AES_ECB;
AES_Parm.En_De = AES_DECRYPT;
AES_Parm.in=out1+1;
AES_Parm.inBytelen=16;
AES_Parm.key=key128;
AES_Parm.keyBytelen=16;
AES_Parm.iv=iv;
AES_Parm.out=out2;
AES_Init(&AES_Parm);
AES_Crypto(&AES_Parm);
if(memcmp(out2,in,16))
{
    return 0x6D;
}
```


国民技术股份有限公司 NSING TECHNOLOGIES INC.
地址：深圳市南山区高新北区宝深路109号国民技术大厦
电话：+86-755-86309900 传真：+86-755-86169100
网址：https://www.nsingtech.com 邮编：518057

```
AES_Parm.Mode = AES_CBC;
AES_Parm.En_De = AES_ENCRYPT;
AES_Parm.in=in;
AES_Parm.inBytelen=16;
AES_Parm.key=key128;
AES_Parm.keyBytelen=16;
AES_Parm.iv=iv;
AES_Parm.out=out1+1;
AES_Init(&AES_Parm);
AES_Crypto(&AES_Parm);
if(memcmp(out1+1,CBC128_en,16))
{
    return 0x6D;
}
AES_Parm.Mode = AES_CBC;
AES_Parm.En_De = AES_DECRYPT;
AES_Parm.in=out1+1;
AES_Parm.inBytelen=16;
AES_Parm.key=key128;
AES_Parm.keyBytelen=16;
AES_Parm.iv=iv;
AES_Parm.out=out2;
AES_Init(&AES_Parm);
AES_Crypto(&AES_Parm);
if(memcmp(out2,in,16))
{
    return 0x6D;
}
```


国民技术股份有限公司 NSING TECHNOLOGIES INC.
地址：深圳市南山区高新北区宝深路109号国民技术大厦
电话：+86-755-86309900 传真：+86-755-86169100
网址：https://www.nsingtech.com 邮编：518057

```
AES_Parm.Mode = AES_CTR;
AES_Parm.En_De = AES_ENCRYPT;
AES_Parm.in=in;
AES_Parm.inBytelen=16;
AES_Parm.key=key192;
AES_Parm.keyBytelen=24;
AES_Parm.iv=iv;
AES_Parm.out=out1+1;
AES_Init(&AES_Parm);
AES_Crypto(&AES_Parm);
if(memcmp(out1+1,CTR192_en,16))
{
    return 0x6D;
}
AES_Parm.Mode = AES_CTR;
AES_Parm.En_De = AES_DECRYPT;
AES_Parm.in=out1+1;
AES_Parm.inBytelen=16;
AES_Parm.key=key192;
AES_Parm.keyBytelen=24;
AES_Parm.iv=iv;
AES_Parm.out=out2;
AES_Init(&AES_Parm);
AES_Crypto(&AES_Parm);
if(memcmp(out2,in,16))
{
    return 0x6D;
```


国民技术股份有限公司 NSING TECHNOLOGIES INC.
地址：深圳市南山区高新北区宝深路109号国民技术大厦
电话：+86-755-86309900 传真：+86-755-86169100
网址：https://www.nsingtech.com 邮编：518057

```
}

AES_Parm.Mode = AES_ECB;
AES_Parm.En_De = AES_ENCRYPT;
AES_Parm.in=in;
AES_Parm.inBytelen=16;
AES_Parm.key=key192;
AES_Parm.keyBytelen=24;
AES_Parm.iv=iv;
AES_Parm.out=out1+1;
AES_Init(&AES_Parm);
AES_Crypto(&AES_Parm);
if(memcmp(out1+1,ECB192_en,16))
{
    return 0x6D;
}
AES_Parm.Mode = AES_ECB;
AES_Parm.En_De = AES_DECRYPT;
AES_Parm.in=out1+1;
AES_Parm.inBytelen=16;
AES_Parm.key=key192;
AES_Parm.keyBytelen=24;
AES_Parm.iv=iv;
AES_Parm.out=out2;
AES_Init(&AES_Parm);
AES_Crypto(&AES_Parm);
if(memcmp(out2,in,16))
{
```


国民技术股份有限公司 NSING TECHNOLOGIES INC.
地址：深圳市南山区高新北区宝深路109号国民技术大厦
电话：+86-755-86309900 传真：+86-755-86169100
网址：https://www.nsingtech.com 邮编：518057

```
    return 0x6D;
}

AES_Parm.Mode = AES_CBC;
AES_Parm.En_De = AES_ENCRYPT;
AES_Parm.in=in;
AES_Parm.inBytelen=16;
AES_Parm.key=key192;
AES_Parm.keyBytelen=24;
AES_Parm.iv=iv;
AES_Parm.out=out1+1;
AES_Init(&AES_Parm);
AES_Crypto(&AES_Parm);
if(memcmp(out1+1,CBC192_en,16))
{
    return 0x6D;
}
AES_Parm.Mode = AES_CBC;
AES_Parm.En_De = AES_DECRYPT;
AES_Parm.in=out1+1;
AES_Parm.inBytelen=16;
AES_Parm.key=key192;
AES_Parm.keyBytelen=24;
AES_Parm.iv=iv;
AES_Parm.out=out2;
AES_Init(&AES_Parm);
AES_Crypto(&AES_Parm);
if(memcmp(out2,in,16))
```


国民技术股份有限公司 NSING TECHNOLOGIES INC.
地址：深圳市南山区高新北区宝深路109号国民技术大厦
电话：+86-755-86309900 传真：+86-755-86169100
网址：https://www.nsingtech.com 邮编：518057

```
{
    return 0x6D;
}

AES_Parm.Mode = AES_CTR;
AES_Parm.En_De = AES_ENCRYPT;
AES_Parm.in=in;
AES_Parm.inBytelen=16;
AES_Parm.key=key256;
AES_Parm.keyBytelen=32;
AES_Parm.iv=iv;
AES_Parm.out=out1+1;
AES_Init(&AES_Parm);
AES_Crypto(&AES_Parm);
if(memcmp(out1+1,CTR256_en,16))
{
    return 0x6D;
}
AES_Parm.Mode = AES_CTR;
AES_Parm.En_De = AES_DECRYPT;
AES_Parm.in=out1+1;
AES_Parm.inBytelen=16;
AES_Parm.key=key256;
AES_Parm.keyBytelen=32;
AES_Parm.iv=iv;
AES_Parm.out=out2;
AES_Init(&AES_Parm);
AES_Crypto(&AES_Parm);
```


国民技术股份有限公司 NSING TECHNOLOGIES INC.
地址：深圳市南山区高新北区宝深路109号国民技术大厦
电话：+86-755-86309900 传真：+86-755-86169100
网址：https://www.nsingtech.com 邮编：518057

```
if(memcmp(out2,in,16))
{
    return 0x6D;
}

AES_Parm.Mode = AES_ECB;
AES_Parm.En_De = AES_ENCRYPT;
AES_Parm.in=in;
AES_Parm.inBytelen=16;
AES_Parm.key=key256;
AES_Parm.keyBytelen=32;
AES_Parm.iv=iv;
AES_Parm.out=out1+1;
AES_Init(&AES_Parm);
AES_Crypto(&AES_Parm);
if(memcmp(out1+1,ECB256_en,16))
{
    return 0x6D;
}
AES_Parm.Mode = AES_ECB;
AES_Parm.En_De = AES_DECRYPT;
AES_Parm.in=out1+1;
AES_Parm.inBytelen=16;
AES_Parm.key=key256;
AES_Parm.keyBytelen=32;
AES_Parm.iv=iv;
AES_Parm.out=out2;
AES_Init(&AES_Parm);
```


国民技术股份有限公司 NSING TECHNOLOGIES INC.
地址：深圳市南山区高新北区宝深路109号国民技术大厦
电话：+86-755-86309900 传真：+86-755-86169100
网址：https://www.nsingtech.com 邮编：518057

```
AES_Crypto(&AES_Parm);
if(memcmp(out2,in,16))
{
    return 0x6D;
}

AES_Parm.Mode = AES_CBC;
AES_Parm.En_De = AES_ENCRYPT;
AES_Parm.in=in;
AES_Parm.inBytelen=16;
AES_Parm.key=key256;
AES_Parm.keyBytelen=32;
AES_Parm.iv=iv;
AES_Parm.out=out1+1;
AES_Init(&AES_Parm);
AES_Crypto(&AES_Parm);
if(memcmp(out1+1,CBC256_en,16))
{
    return 0x6D;
}
AES_Parm.Mode = AES_CBC;
AES_Parm.En_De = AES_DECRYPT;
AES_Parm.in=out1+1;
AES_Parm.inBytelen=16;
AES_Parm.key=key256;
AES_Parm.keyBytelen=32;
AES_Parm.iv=iv;
AES_Parm.out=out2;
```


国民技术股份有限公司 NSING TECHNOLOGIES INC.
地址：深圳市南山区高新北区宝深路109号国民技术大厦
电话：+86-755-86309900 传真：+86-755-86169100
网址：https://www.nsingtech.com 邮编：518057

```
    AES_Init(&AES_Parm);
    AES_Crypto(&AES_Parm);
    if(memcmp(out2,in,16))
    {
        return 0x6D;
    }
    printf("aes_test is succsed!\r\n");

}
```


国民技术股份有限公司 NSING TECHNOLOGIES INC.
地址：深圳市南山区高新北区宝深路109号国民技术大厦
电话：+86-755-86309900 传真：+86-755-86169100
网址：https://www.nsingtech.com 邮编：518057

iii.附录三 HASH算法库函数调用例程

所有数据都是字节大端，自然顺序

iii.1 HASH_test

```
uint32_t SHA_test()
{
    uint8_t
in[16]={0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00};
    uint8_t
sha1_out[20]={0xE1,0x29,0xF2,0x7C,0x51,0x03,0xBC,0x5C,0xC4,0x4B,0xCD,0xF0,0xA1,0x5E,0x16,
0x0D,0x44,0x50,0x66,0xFF};
    uint8_t sha224_out[28]=
    {

0xF1,0x85,0xBD,0x39,0x9E,0x1B,0x65,0x96,0x42,0x86,0x2C,0xE0,0x59,0xE2,0x02,0xA1,0x9A,0xA8,
0x73,0xA1,0x02,0x94,0xCF,0x30,0xCA,0x5F,0x90,0xEB
    };
    uint8_t sha256_out[32]=
    {
0x37,0x47,0x08,0xFF,0xF7,0x71,0x9D,0xD5,0x97,0x9E,0xC8,0x75,0xD5,0x6C,0xD2,0x28,0x6F,0x6D,
0x3C,0xF7,0xEC,0x31,0x7A,0x3B,0x25,0x63,0x2A,0xAB,0x28,0xEC,0x37,0xBB    };
    uint8_t sha384_out[48]=
    {
0xAE,0x40,0x65,0x9D,0xA1,0x19,0x3C,0xDE,0xC8,0xDF,0x47,0x4B,0x5E,0x36,0x41,0x6A,0x82,0x47
,0x3B,0x83,0xD3,0x2D,0xBB,0xE1,0xDD,0x6D,0xF8,0xEC,0x94,0x99,0xD2,0x49,0x02,0xCA,0x08,0x
C3,0x34,0x87,0x6B,0xC8,0xE6,0x9E,0x81,0x8B,0xEE,0xCC,0x04,0x6A };
```


国民技术股份有限公司 NSING TECHNOLOGIES INC.
地址：深圳市南山区高新北区宝深路109号国民技术大厦
电话：+86-755-86309900 传真：+86-755-86169100
网址：https://www.nsingtech.com 邮编：518057

```
    uint8_t sha512_out[64]=
    {
0x0B,0x6C,0xBA,0xC8,0x38,0xDF,0xE7,0xF4,0x7E,0xA1,0xBD,0x0D,0xF0,0x0E,0xC2,0x82,0xFD,0x
F4,0x55,0x10,0xC9,0x21,0x61,0x07,0x2C,0xCF,0xB8,0x40,0x35,0x39,0x0C,0x4D,0xA7,0x43,0xD9,0x
C3,0xB9,0x54,0xEA,0xA1,0xB0,0xF8,0x6F,0xC9,0x86,0x1B,0x23,0xCC,0x6C,0x86,0x67,0xAB,0x23,0
x2C,0x11,0xC6,0x86,0x43,0x2E,0xBB,0x5C,0x8C,0x3F,0x27    };
    uint8_t out[69];
    uint8_t ret;
    HASH_CTX ctx[1];
    ctx->hashAlg = HASH_ALG_SHA1;
    ctx->sequence = HASH_SEQUENCE_FALSE;

    HASH_Init(ctx);
    HASH_Start(ctx);
    HASH_Update(ctx, in, 16);
    HASH_Complete(ctx, out+1);
    HASH_Close();
    if (memcmp(out+1,sha1_out,20))
    {
        return 0x5a5a5a5a;
    }
    else
    {
      printf("SHA1-Test success\r\n");
    }
    ctx->hashAlg = HASH_ALG_SHA224;
    ctx->sequence = HASH_SEQUENCE_FALSE;
```


国民技术股份有限公司 NSING TECHNOLOGIES INC.
地址：深圳市南山区高新北区宝深路109号国民技术大厦
电话：+86-755-86309900 传真：+86-755-86169100
网址：https://www.nsingtech.com 邮编：518057

```
HASH_Init(ctx);
HASH_Start(ctx);
HASH_Update(ctx, in, 16);
ret=HASH_Complete(ctx, out+1);
HASH_Close();
if (memcmp(out+1,sha224_out,28))
{
    return 0x5a5a5a5a;
}
else
{
  printf("SHA224-Test success\r\n");
}

ctx->hashAlg = HASH_ALG_SHA256;
ctx->sequence = HASH_SEQUENCE_FALSE;
HASH_Init(ctx);
HASH_Start(ctx);
HASH_Update(ctx, in, 16);
ret=HASH_Complete(ctx, out+1);
HASH_Close();
if(memcmp(out+1,sha256_out,32))
{
    return 0x5a5a5a5a;
}
else
{
     printf("SHA256-Test success\r\n");
```


国民技术股份有限公司 NSING TECHNOLOGIES INC.
地址：深圳市南山区高新北区宝深路109号国民技术大厦
电话：+86-755-86309900 传真：+86-755-86169100
网址：https://www.nsingtech.com 邮编：518057

```
}
ctx->hashAlg = HASH_ALG_SHA384;
ctx->sequence = HASH_SEQUENCE_FALSE;

    HASH_Init(ctx);
    HASH_Start(ctx);
    HASH_Update(ctx, in, 16);
    ret=HASH_Complete(ctx, out+1);
    HASH_Close();
    if(memcmp(out+1,sha384_out,48))
    {
        return 0x5a5a5a5a;
    }
    else
    {
      printf("SHA384-Test success\r\n");
    }

    ctx->hashAlg = HASH_ALG_SHA512;
    ctx->sequence = HASH_SEQUENCE_FALSE;

    HASH_Init(ctx);
    HASH_Start(ctx);
    HASH_Update(ctx, in, 16);
    ret=HASH_Complete(ctx, out+1);
    HASH_Close();
    if(memcmp(out+1,sha512_out,64))
    {
```


国民技术股份有限公司 NSING TECHNOLOGIES INC.
地址：深圳市南山区高新北区宝深路109号国民技术大厦
电话：+86-755-86309900 传真：+86-755-86169100
网址：https://www.nsingtech.com 邮编：518057

```
            return 0x5a5a5a5a;
        }
        else
        {
          printf("SHA512-Test success\r\n");
        }
    }
```

iii.2 HASH_single_test

```
//sha256 单次哈希测试用例
uint32_t HASH_single_test(void)
{
    uint32_t ret;
    //消息：
    uint8_t in[48]=
    {
0x1C,0xBB,0x9F,0x4A,0x43,0x6A,0xAD,0x81,0xFE,0x4F,0x52,0x4A,0x0A,0x76,0x22,0xC8,0x4F,0x90,0x18,0x30,0xA4,0xD2,0x8C, 0x6A,0xC3,0x40,0xA0,0xBD,0x0A,0x6A,0x37,0x18,0x8D,0x19, 0x9D, 0xE5, 0xCB,0x84,0xA3,0xFC,0x39,0xDE,0x8C,0xD6,0xFC,0x2F, 0xC8,0x88};//字节大端
    //消息摘要输出：
    uint8_t out[32];
    //单次 sha256 的正确消息摘要：
    uint8_t sha256_out[32]=
    {
0xE2,0xE4,0x2C,0x8A,0x01,0x1A,0xE7,0x98,0x67,0x74,0x93,0xAF,0x9D,0x65,0x99,0xB3,0xA1,0x68, 0x8B,0x5A,0xF1,0x32, 0x3D,0x5B,0xFF,0xFB,0x12,0x30,0x94,0xE4,0x81,0xDD};//字节大端
  //sha256 的单次杂凑
  ret=SHA256_Hash(in,48,out);
```


国民技术股份有限公司 NSING TECHNOLOGIES INC.
地址：深圳市南山区高新北区宝深路109号国民技术大厦
电话：+86-755-86309900 传真：+86-755-86169100
网址：https://www.nsingtech.com 邮编：518057

```
    if(ret!=SHA256_Hash_OK)return 0x5A5A5A5A;
    if(memcmp(out,sha256_out,32))
    {
            return 0x5a5a5a5a;
    }
      else
      {
          printf("SHA256-Test success\r\n");
      }
      return 0;
}
```

iii.3 Hash_substep_test

```
//SHA256 固定分布测试
uint32_t Hash_substep_test(void)
{
//输入消息 字节大端
      uint8_t hash256_fixin[48*3]=
      {
          0x56,0x9F,0x3E,0x6A,0x8A,0x28,0x10,0x1D,0xE0,
          0x67,0xD9,0x15,0x27,0xB7,0xE1,0x89,0x7D,0x35,
          0x1D,0xDE,0xF2,0x1F,0x12,0x60,0x4B,0x8E,0x23,
          0x82,0x57,0x0B,0x54,0x59,0xFB,0xE7,0xE9,0x41,
          0xD3,0x93,0x7B,0x68,0xCA,0x04,0xD6,0x16,0x54,
          0x88,0xBE,0xC5,0x4C,0x61,0x14,0x35,0xA1,0x80,
          0x58,0xBE,0x48,0x1A,0x97,0x8D,0xA9,0x67,0x04,
          0xE8,0x89,0x00,0xE7,0x3E,0x6E,0xAA,0x2B,0x7A,
          0x94,0x86,0x21,0x19,0x00,0xF0,0xA9,0x95,0xE5,
```


国民技术股份有限公司 NSING TECHNOLOGIES INC.
地址：深圳市南山区高新北区宝深路109号国民技术大厦
电话：+86-755-86309900 传真：+86-755-86169100
网址：https://www.nsingtech.com 邮编：518057

```
    0x08,0x62,0xC4,0xB6,0xF3,0x37,0x71,0xD4,0x66,
    0x38,0x6F,0x7D,0x4C,0xE5,0x84,0xE3,0x10,0x61,
    0x88,0x6D,0x56,0x2F,0x1A,0x14,0x52,0x11,0x4E,
    0x59,0x7A,0xF6,0xEB,0x05,0xD1,0x59,0x85,0xA7,
    0x0A,0x2C,0x1F,0x97,0xB4,0xA9,0xD8,0xF7,0xBC,
    0x2D,0xE8,0x4F,0xC1,0xE6,0x4C,0x18,0x5F,0xF6,
    0x1F,0x71,0x3C,0xBF,0xD2,0x42,0x1A,0x16,0xBB
};
uint8_t out[32];
//输出消息 字节大端
uint8_t hash256_fixout[32]=
{
   0xFA,0xE9,0x77,0xDB,0x34,0x0F,0x40,0x2A,0xE3,0x38,0x5A,0x54,0xB5,0x9F,0x39,0xDF,0x49,0x7
   7,0x59,0x4E,0xEB,0x4F,0x02,0xBD,0x36,0xED,0xA2,0xDF,0x35,0x4A,0xB0,0x76
 };
uint32_t i,byteLen=48;
HASH_CTX ctx[1];
ctx->hashAlg = HASH_ALG_SHA256;
ctx->sequence = HASH_SEQUENCE_TRUE;
HASH_Init(ctx);
HASH_Start(ctx);

for(i=0;i<3;i++)
{
    HASH_Update(ctx,hash256_fixin+i*byteLen,byteLen);
 }
HASH_Complete(ctx, out);
HASH_Close();
```


国民技术股份有限公司 NSING TECHNOLOGIES INC.
地址：深圳市南山区高新北区宝深路109号国民技术大厦
电话：+86-755-86309900 传真：+86-755-86169100
网址：https://www.nsingtech.com 邮编：518057

```
    if (memcmp(out,hash256_fixout,32))
    {
        printf("hash256-FIX-Test fail\r\n");
        return 0x5A5A5A5A;
    }
    else
    {
        printf("hash256-FIX-Test success\r\n");
    }
    return 0;
}
```


国民技术股份有限公司 NSING TECHNOLOGIES INC.
地址：深圳市南山区高新北区宝深路109号国民技术大厦
电话：+86-755-86309900 传真：+86-755-86169100
网址：https://www.nsingtech.com 邮编：518057

iv.附录四 RNG算法库调用例程

iv.1 伪随机

```
uint32_t Prng_test(void)
{
    uint32_t seed1[5]={0x00000001,0x08704706,0xb89a7076,0xe54189fe,0x97720802};
    uint32_t rand1[9]={0x6E8A2B4E,0xE8A8883B,0x05377FDE,0x74A971A9,0xEAD3443A,
   0x272DD5BA ,0xDF08142A ,0x54003866 ,0x069DEA21 };
    uint32_t result[9];
    PseudoRandNumInit(seed1);
    GetPseudoRand_U32(result,9);

    if(Cmp_U32(result,9,rand1,9)!=Cmp_EQUAL)
    {
        return 0x5a5a5a5a;
    }
    else
    {
        printf("seed1 success\r\n");
    }
    return 0;
}
```

iv.2 真随机

```
uint32_t TRNG()
{
```


国民技术股份有限公司 NSING TECHNOLOGIES INC.
地址：深圳市南山区高新北区宝深路109号国民技术大厦
电话：+86-755-86309900 传真：+86-755-86169100
网址：https://www.nsingtech.com 邮编：518057

```
    uint32_t rand[32]={0},rand1[32]={0},rand2[32]={0};
    GetTrueRand_U32(rand,32);
    GetTrueRand_U32(rand1,32);
    GetTrueRand_U32(rand2,32);
    if(Cmp_U32(rand1,32,rand2,32)!=Cmp_EQUAL &&Cmp_U32(rand,32,rand2,32)!=Cmp_EQUAL
        &&Cmp_U32(rand,32,rand2,32)!=Cmp_EQUAL)
    printf("Rand successd!");
    GetTrueRand_U8((uint8_t*)rand,32);
    printf("Rand1 successd!");
}
```


国民技术股份有限公司 NSING TECHNOLOGIES INC.
地址：深圳市南山区高新北区宝深路109号国民技术大厦
电话：+86-755-86309900 传真：+86-755-86169100
网址：https://www.nsingtech.com 邮编：518057

v.附录五 SM4算法库函数调用例程

所有数据都是字节大端，自然顺序

```
uint32_t SM4_test()
{
    uint8_t
in[128]={0xD5,0xF4,0x34,0x4D,0x6A,0x09,0xBB,0xA6,0xCE,0xCD,0xDD,0x36,0x80,0xD4,0xB0,0x4
6,0xF1,0xDC,0xC7,0xB0,0xE6,0xA6,0xB4,0x4F,0x1D,0x04,0xCA,0xB4,0x33,0x34,0x28,0x1A,0xC5,0x
6C,0xF3,0x9C,0xD6,0xB6,0xE2,0xA6,0x70,0xFE,0x00,0xAA,0x8E,0x69,0xAD,0x14,0x3A,0xE9,0xE6,
0x7F,0xF3,0x0F,0xC7,0x29,0x51,0x20,0x4E,0xA4,0xEC,0x6A,0x62,0xCF,0x79,0xD8,0x14,0x05,0x36,
0xC5,0x24,0x94,0x89,0x0E,0xC7,0x71,0xE3,0x6B,0xA7,0x2A,0xEB,0xFF,0x2C,0x1B,0xD9,0x2D,0xF
A,0xE5,0x1F,0xAE,0xBB,0x1C,0x4F,0xE0,0x1E,0x40,0x39,0x61,0x1F,0xEF,0x53,0xDD,0x8A,0x58,0x
5F,0x24,0xBA,0xF3,0x47,0x80,0xA7,0x70,0x4C,0x45,0x20,0xED,0x5F,0xA9,0x54,0x6B,0xCF,0xD6,0
x97,0x83,0x25,0x3E,0x63,0x55};
    uint8_t
key[16]={0x4D,0x2F,0x9D,0xC2,0xF6,0xA7,0x1A,0xDB,0x3A,0x69,0x62,0x98,0x82,0x50,0xB4,0xCE
};
    uint8_t
iv[16]={0x0D,0xF5,0x99,0x42,0xF8,0xB4,0x97,0x51,0x0D,0xF5,0x99,0x42,0xF8,0xB4,0x97,0x51};

    uint8_t
ECB_ENC[128]={0x4E,0xE1,0x96,0x3B,0x70,0x9A,0xED,0x7B,0x57,0x9B,0xDC,0x2E,0xDA,0xBB,0
xC7,0xF7,0x38,0x59,0xB5,0xF2,0xED,0x6B,0x44,0x03,0x24,0x95,0x2B,0x1C,0xD9,0x24,0xAF,0xEE,0
x63,0x2F,0x99,0x1E,0x1B,0xF4,0x82,0xDF,0x5A,0x66,0xA5,0x43,0x9C,0xE6,0x92,0xEC,0x66,0xDB,
0xC1,0x88,0xAF,0xC0,0xB9,0xEB,0x8D,0xBB,0xEF,0x06,0x09,0x7E,0xDD,0x7A,0x3F,0xDA,0xFE,0x
0A,0x30,0x8C,0xA8,0x56,0x6E,0x0C,0xEF,0x6A,0x16,0x85,0x46,0x9B,0x13,0x7C,0xC8,0xA7,0x39,0x
AE,0xE3,0x60,0x4F,0x58,0x20,0x6D,0x76,0x5A,0xDA,0x13,0x4E,0xFA,0x28,0xF0,0xE1,0xD1,0x92,0
x02,0x69,0x86,0x3C,0x8F,0xA5,0x3A,0xAA,0xA9,0x60,0x1
```


国民技术股份有限公司 NSING TECHNOLOGIES INC.
地址：深圳市南山区高新北区宝深路109号国民技术大厦
电话：+86-755-86309900 传真：+86-755-86169100
网址：https://www.nsingtech.com 邮编：518057

```
1,0x15,0x25,0x15,0x56,0x23,0x12,0xE3,0xB4,0x4B,0x36,0x2D,0xD5,0xAA,0x9A};
    uint8_t
CBC_ENC[128]={0xC3,0xA6,0xC7,0x61,0x88,0x79,0xE6,0x7F,0x47,0xB5,0xEC,0x1E,0xB0,0x4E,0x1
A,0x45,0x8E,0x05,0x53,0x30,0xFA,0x73,0x81,0x16,0x38,0x1A,0x74,0x04,0x61,0x61,0xFA,0x41,0x4D
,0x48,0xCD,0xD4,0x73,0xE0,0x72,0x41,0xD0,0x2A,0x19,0x89,0x34,0xE8,0x64,0x81,0xB0,0xA4,0x98,
0x6F,0x27,0x94,0x0A,0xBA,0x8F,0x2B,0x54,0x9F,0xDB,0x50,0xAB,0x3A,0x87,0xFC,0x27,0x88,0xB
2,0x3F,0x6D,0x0E,0xA4,0xD9,0x20,0xF7,0x22,0xF6,0x4E,0x83,0x21,0x45,0x42,0x21,0x74,0xAD,0xF
4,0xA3,0x6B,0x55,0x0D,0xFF,0xF1,0xC5,0x20,0x69,0x44,0x6C,0x99,0x99,0xDB,0x79,0xE2,0x44,0x4
E,0xF5,0x2E,0x8B,0xC1,0xF2,0x88,0xA5,0xE9,0xBD,0x2B,0x1A,0xF1,0xB0,0xE6,0x2E,0x73,0xFC,0x
B4,0x38,0xF2,0x5D,0x3E,0x57};
    uint8_t out1[130],out2[130];
    SM4_PARM SM4_Parm={0};
    SM4_Parm.Mode = SM4_ECB;
    SM4_Parm.En_De = SM4_ENCRYPT;
    SM4_Parm.in=in;
    SM4_Parm.inBytelen=128;
    SM4_Parm.key=key;
    SM4_Parm.out=out1+2;
    SM4_Init(&SM4_Parm);
    SM4_Crypto1(&SM4_Parm);
    if(memcmp(out1+2,ECB_ENC,128))
    {
        return 0x6D;
    }
    SM4_Parm.Mode = SM4_ECB;
    SM4_Parm.En_De = SM4_DECRYPT;
    SM4_Parm.in=out1+2;
    SM4_Parm.inBytelen=128;
```


国民技术股份有限公司 NSING TECHNOLOGIES INC.
地址：深圳市南山区高新北区宝深路109号国民技术大厦
电话：+86-755-86309900 传真：+86-755-86169100
网址：https://www.nsingtech.com 邮编：518057

```
SM4_Parm.key=key;
SM4_Parm.out=out2;
SM4_Init(&SM4_Parm);
SM4_Crypto1(&SM4_Parm);
if(memcmp(out2,in,128))
{
    return 0x6D;
}

SM4_Parm.Mode = SM4_CBC;
SM4_Parm.En_De = SM4_ENCRYPT;
SM4_Parm.in=in;
SM4_Parm.inBytelen=128;
SM4_Parm.key=key;
SM4_Parm.out=out1+2;
SM4_Parm.iv=iv;
SM4_Init(&SM4_Parm);
SM4_Crypto1(&SM4_Parm);
if(memcmp(out1+2,CBC_ENC,128))
{
    return 0x6D;
}
SM4_Parm.Mode = SM4_CBC;
SM4_Parm.En_De = SM4_DECRYPT;
SM4_Parm.in=out1+2;
SM4_Parm.inBytelen=128;
SM4_Parm.key=key;
SM4_Parm.out=out2;
```


国民技术股份有限公司 NSING TECHNOLOGIES INC.
地址：深圳市南山区高新北区宝深路109号国民技术大厦
电话：+86-755-86309900 传真：+86-755-86169100
网址：https://www.nsingtech.com 邮编：518057

```
    SM4_Parm.iv=iv;
    SM4_Init(&SM4_Parm);
    SM4_Crypto1(&SM4_Parm);
    if(memcmp(out2,in,128))
    {
        return 0x6D;
    }
    printf("SM4_test is successed! \r\n");
}
```


国民技术股份有限公司 NSING TECHNOLOGIES INC.
地址：深圳市南山区高新北区宝深路109号国民技术大厦
电话：+86-755-86309900 传真：+86-755-86169100
网址：https://www.nsingtech.com 邮编：518057