Cryptographic Algorithm Library User Guide

V1.0.0

国民技术股份有限公司 Nations 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
邮箱：info@nationz.com.cn 邮编：518057

Disclaimer

This document is the exclusive property of NSING TECHNOLOGIES PTE. LTD. (Hereinafter referred to as NSING). This document, and the product of NSING described herein (Hereinafter referred to as the Product) are owned by NSING under the laws and treaties of Republic of Singapore and other applicable jurisdictions worldwide. The intellectual properties of the product belong to NSING Technologies Inc. and NSING Technologies Inc. does not grant any third party any license under its patents, copyrights, trademarks, or other intellectual property rights. Names and brands of third party may be mentioned or referred thereto (if any) for identification purposes only. NSING reserves the right to make changes, corrections. enhancements, modifications, and improvements to this document at any time without notice. Please contact NSING and obtain the latest version of this document before placing orders. Although NSING has attempted to provide accurate and reliable information, NSING assumes no responsibility for the accuracy and reliability of this document. It is the responsibility of the user of this document to properly design, program, and test the functionality and safety of any application made of this information and any resulting product. In no event shall NSING be liable for any direct, indirect, incidental, special, exemplary, or consequential damages arising in any way out of the use of this document or the Product. NSING Products are neither intended nor warranted for usage in systems or equipment, any malfunction or failure of which may cause loss of human life, bodily injury or severe property damage. Such applications are deemed, Insecure Usage'. Insecure usage includes, but is not limited to: equipment for surgical implementation, atomic energy control instruments, airplane or spaceship instruments, all types of safety devices, and other applications intended to supporter sustain life. All Insecure Usage shall be made at user's risk. User shall indemnify NSING and hold NSING harmless from and against all claims, costs, damages, and other liabilities, arising from or related to any customer's Insecure Usage Any express or implied warranty with regard to this document or the Product, including, but not limited to. The warranties of merchantability, fitness for a particular purpose and non-infringement are disclaimed to the fullest extent permitted by law. Unless otherwise explicitly permitted by NSING, anyone may not use, duplicate, modify, transcribe or otherwise distribute this document for any purposes, in whole or in part.

To our customers:

国民技术股份有限公司 Nations 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
邮箱：info@nationz.com.cn 邮编：518057

We are constantly improving the quality of our products and documentation. We strive to ensure that the instructions in this document are accurate, but there may also be some errors that we have not discovered. If you find any questions or omissions in the document, please contact us promptly. Your understanding and support will make this document more comprehensive.

版本历史

Version	Date	Comments
V1.1.0	2026.01.15	Create file

国民技术股份有限公司 Nations 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
邮箱：info@nationz.com.cn 邮编：518057

Terms and Abbreviations

Abbreviations	Full Forms
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 Nations 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
邮箱：info@nationz.com.cn 邮编：518057

Contents

国民技术股份有限公司 Nations 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
邮箱：info@nationz.com.cn 邮编：518057

国民技术股份有限公司 Nations 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
邮箱：info@nationz.com.cn 邮编：518057

国民技术股份有限公司 Nations 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
邮箱：info@nationz.com.cn 邮编：518057

1. Overview

This document is applicable to N32H7xx chips that have downloaded relevant algorithms, mainly explaining the algorithm interfaces and usage methods in this type of chip.

1.1. Supported Algorithm

The algorithm provided by the N32H7xx chip is as follows：

- DES: encrypt/decrypt(ECB/CBC)
- TDES: encrypt/decrypt(ECB/CBC)
- AES: (ECB/CBC/CTR) encrypt/decrypt（AES-128/192/256）
- HASH: get digest，support（SHA-1/SHA-224/SHA-256/SHA-384/ SHA-512）
- SM4: encrypt/decrypt(ECB/CBC)
- RNG: generation of random number

1.2. Basic Data Types

```
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 Nations 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
邮箱：info@nationz.com.cn 邮编：518057

2. DES/TDES algorithm API specification

2.1. Usage of algorithm library

The usage method of the algorithm library is as follows:

1. Add DES. h, Common.h to the header folder; Add,Common.lib, DES.lib to the project
2. Call the function according to the function description in section 2.3

2.2. Data type define

```
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 Nations 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
邮箱：info@nationz.com.cn 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. Function interface description

The DES /TDES algorithm library contains the following list of functions:

Table 2-1 DES/TDES algorithm library function table

Function	description
uint32_t DES_Init(DES_PARM *parm) #define TDES_Init DES_Init	DES/TDES initialization
uint32_t DES_Crypto1(DES_PARM *parm) #define TDES_Crypto1 DES_Crypto1	DES/TDES encryption and decryption
Void DES_Close(void) #define TDES_Close DES_Close	DES/TDES close
void DES_Version(uint8_t *type, uint8_t *customer, uint8_t date[3], uint8_t *version) #define TDES_Version DES_Version	DES//TDES version retrieval function

2.3.1. DES/TDES initialization

DES_Init DES/TDES initialzation

Function uint32_t DES_Init(DES_PARM *parm)

Parameter DES_Parm input，point to DES_PARM

Return DES_Init_OK：success other：fail

Notice 1. In ECB mode, parameters iv can be directly replaced with NULL。

国民技术股份有限公司 Nations 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
邮箱：info@nationz.com.cn 邮编：518057

2. When using TDES, users can replace TDES_Init and TDES_PARM with DES_Init and DES_PARM respectively, and use it as TDES_Init (TDES_PARM *parm).

2.3.2. DES/TDES encryption and decryption

DES_Crypto	DES/TDES encryption and decryption
Function	uint32_t DES_Crypto1(DES_PARM *parm)
Parameter	DES_Parm input，point to DES_PARM
Return	DES_Crypto_OK：success other：fail
Notice	

1. In ECB mode, parameters iv can be directly replaced with NULL
2. When using TDES, users can replace TDES_Init and TDES_PARM with DES_Init and DES_PARM respectively, and use it as TDES_Init (TDES_PARM *parm).
3. When encrypting a large amount of data as a whole but in multiple blocks using ECB mode, note the following:The initial vector IV (IV = iv1) used when calling this function to encrypt the X-th block of data (X>1) must be updated to the last block (8 bytes) of the ciphertext obtained by calling this function to encrypt the (X-1)-th block of data.
4. When encrypting a large amount of data as a whole but in multiple blocks using ECB mode, note the following:The initial vector IV (IV = iv1) used when calling this function to encrypt the X-th block of data (X>1) must be updated to the last block (8 bytes) of the ciphertext obtained by calling this function to encrypt the (X-1)-th block of data.
5. Please refer to Appendix 1 for the calling method。

国民技术股份有限公司 Nations 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
邮箱：info@nationz.com.cn 邮编：518057

2.3.3. DES/TDES close

DES_Close	close DES/TDES algorithm clock and system clcok
Function	void DES_Close(void)
Parameter	none
Return	**none**
Notice	1. When users use TDES, they can replace TDES_Close with DES_Close and use it as TDES_Close (void).

2.3.4. DES/TDES get library version information

DES_Version	DES/TDES get library version information
Function	void DES_Version(uint8_t *type, uint8_t *customer, uint8_t date[3], uint8_t *version)
Parameter	type Business or Security version customer Standard or customized version date year，data，day version version x.x
Return	

Notice	*type = 0x03; // Security version
	*customer = 0x00; // Standard
	date[0] = 25; // Year()
	date[1] = 04; // Month()
	date[2] = 27; // Day ()
	*version = 0x10; // 1.0
	1. When users use TDES, they can replace TDES_Version with DES_Version and use it as TDES_Version (uint8_t *type, uint8_t *customer, uint8_t date[3], uint8_t *version).

国民技术股份有限公司 Nations 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
邮箱：info@nationz.com.cn 邮编：518057

3. AES algorithm API specification

3.1. Usage of algorithm library

The usage method of the algorithm library is as follows:

1. Add AES.h, Common.h to the header folder; Add,Common.lib, AES.lib.lib to the project
2. Call the function according to the function description in section 3.3 . See the demo in Appendix 2 for test cases

3.2. Data type define

```
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
```


国民技术股份有限公司 Nations 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
邮箱：info@nationz.com.cn 邮编：518057

```
    uint32_t inBytelen;    // the length(by byte) of plaintext or cipher
    uint32_t En_De;        // 0x44444444- encrypt, 0x55555555 - decrypt
    uint32_t Mode;         // 0x11111111 - ECB, 0x22222222 - CBC,0x33333333-AES_CTR
}AES_PARM;
```

3.3. Function interface description

The AES algorithm library contains the following list of functions：

Table 3-1 AES algorithm library function table

Function	description
uint32_t AES_Init(AES_PARM *parm)	AES initialization
uint32_t AES_Crypto(AES_PARM *parm)	AES encryption/ decryption
void AES_Close(void)	AES close
void AES_Version(uint8_t *type, uint8_t *customer, uint8_t date[3], uint8_t *version)	AES version retrieval function

3.3.1. AES initialization

AES_Init AES initialization

Function uint32_t AES_Init(AES_PARM *parm)

Parameter AES _Parm input，point to AES _PARM

Return AES_Init_OK：success other：fail

Notice 1. In ECB mode, parameters iv can be directly replaced with NULL。

3.3.2. AES encryption/decryption

AES_Crypto AES encryption/decryption

Function uint32_t AES_Crypto(AES_PARM *parm)

国民技术股份有限公司 Nations 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
邮箱：info@nationz.com.cn 邮编：518057

Parameter AES _Parm input，point to AES _PARM

Return AES_Crypto_OK：success other：fail

Notice

1. In ECB mode, parameters iv can be directly replaced with NULL。
2. when encrypting a large amount of data as a whole but in multiple blocks using CBC or CTR mode, note the following:The initial vector iv used when calling this function to encrypt the X-th block of data (X>1) must be updated to the last block (16 bytes) of the ciphertext obtained by calling this function to encrypt the (X-1)-th block of data.
3. When decrypting a large amount of data as a whole but in multiple blocks using CBC mode, note the following:The initial vector iv used when calling this function to decrypt the X-th block of data (X>1) must be updated to the last block (16 bytes) of the (X-1)-th block of data

3.3.3. AES close

AES_Close **close** AES algorithm clock and system clock

Function void AES_Close(void)

Parameter

Return

Notice

3.3.4. AES get library version information

AES_Version get AES library version information

Function void AES_Version(uint8_t *type, uint8_t *customer, uint8_t date[3], uint8_t *version)

Parameter

type	Business or Security version
customer	Standard or customized version
date	year，data，day

国民技术股份有限公司 Nations 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
邮箱：info@nationz.com.cn 邮编：518057

version vesion x.x

Return

Notice *type = 0x03; // Security version

*customer = 0x00; // Standard

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

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

date[2] = 27 //Day ()

*version = 0x10; //vesion 1.0

国民技术股份有限公司 Nations 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
邮箱：info@nationz.com.cn 邮编：518057

4. HASH algorithm API specification

4.1. Usage of algorithm library

The usage method of the algorithm library is as follows:

1. Add HASH.h, Common.h to the header folder; Add Common.lib, HASH.lib to the project
2. Call the function according to the function description in section 4.3 . See the demo in Appendix 3 for test cases

4.2. Data type define

```
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
    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
    SHA512_Hash_OK = 0,                  //sha512 operation success
```


国民技术股份有限公司 Nations 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
邮箱：info@nationz.com.cn 邮编：518057

```
    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
    uint32_t      sequence;        // TRUE if the IV should be saved
```


国民技术股份有限公司 Nations 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
邮箱：info@nationz.com.cn 邮编：518057

```
    uint32_t    IV[16];
    uint32_t    msgByteLen[4];
    uint8_t     msgBuf[132];
    uint32_t    msgIdx;
}HASH_CTX;
```

4.3. Function interface description

The HASH algorithm library contains the following list of functions：

Table 4-1 HASH algorithm library function table

Function	description
uint32_t HASH_Init(HASH_CTX *ctx)	HASH initialization
uint32_t HASH_Start(HASH_CTX *ctx)	HASH Start operation
uint32_t HASH_Update(HASH_CTX *ctx, uint8_t *in, uint32_t byteLen);	HASH update operation
uint32_t HASH_Complete(HASH_CTX *ctx, uint8_t *out)	HASH completion
uint32_t HASH_Close(void)	HASH close
void HASH_Version(uint8_t *type, uint8_t *customer, uint8_t date[3], uint8_t *version)	HASH version retrieval function

4.3.1. HASH initialization

HASH_Init	HASH initialization
Function	uint32_t HASH_Init(HASH_CTX *ctx)
Parameter	ctx input，point to HASH_CTX
Return	HASH_Init_OK：success other：fail
Notice	1. The ctx must point to the RAM area and the content it points to cannot be changed (as an intermediate state for hash calculations and temporary content storage), the same applies below 2. When calculating the hash value of a message step by step, this function must be called first

国民技术股份有限公司 Nations 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
邮箱：info@nationz.com.cn 邮编：518057

4.3.2. HASH start

HASH_Start	HASH start
Function	uint32_t HASH_Start(HASH_CTX *ctx)
Parameter	ctx **input**，point to HASH_CTX
Return	HASH_Start_OK：success other：fail
Notice	1. If support for interruption during the HASH operation is required, set ctx->sequence to HASH_SEQUENCE_TRUE; after the interruption ends, it is necessary to call the HASH_Init function again, followed by the HASH_Update function; otherwise, set it to HASH_SEQUENCE_FALSE 2. Please refer to Appendix 4 for the calling method

4.3.3. HASH update

HASH_Update	HASH update
Function	uint32_t HASH_Update(HASH_CTX *ctx, uint8_t *in, uint32_t byteLen)
Parameter	ctx **input**，point to HASH_CTX in **input**，point to message byteLen **input**，point to length of message
Return	HASH_Update_OK：success other：fail
Notice	1. Before calling this function, you must first call the initialization functions HASH_Init and HASH_Start 2. ctx must point to the RAM area, and the content it points to must not be modified (it serves as storage for the intermediate state and temporary content of the hash calculation). 3. The content of in can point to the RAM or Flash area. 4. byteLen can be 0。

国民技术股份有限公司 Nations 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
邮箱：info@nationz.com.cn 邮编：518057

5. After initialization, a single entire message can be arbitrarily divided into multiple small blocks; this function can be called sequentially for each small block of the message, and finally the HASH_Complete function is called to obtain the hash result of the entire message

6. If cascaded application is required, you need to set ctx->sequence = HASH_SEQUENCE_TRUE, copy the external IV to ctx->IV, add the length len of the updated data to ctx->msgByteLen using ctx->hashAlg->ByteLenPlus(ctx->msgByteLen, len), and then call the HASH_Update function to achieve successful cascading.

7. Please refer to Appendix 4 for the calling method

4.3.4. HASH completion

HASH_Complete	HASH completion
Function	uint32_t HASH_Complete(HASH_CTX *ctx, uint8_t *out)
Parameter	ctx input，point to HASH_CTX out output，point to HASH result
Return	HASH_Complete_OK：success other：fail
Notice	1. After the message input is completed, only by calling this function can you obtain the final result 2. ctx must point to the RAM area, and the content it points to must not be modified (it serves as storage for the intermediate state and temporary content of the hash calculation)。 3. Please refer to Appendix 4 for the calling method。

4.3.5. One-shot Hash Function

XXX_HASH	One-shot Hash Function

国民技术股份有限公司 Nations 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
邮箱：info@nationz.com.cn 邮编：518057

Function uint32_t XXX_Hash(uint8_t* in,uint32_t byteLen, uint8_t* out)

Parameter XXX_Hash ： SHA1_Hash、SHA224_Hash、SHA256_Hash、 SHA384_Hash、SHA512_Hash

in input，point to message

byteLen input，the length of message

out output，point to hash result

Return XXX_Hash_OK：success other：fail

Notice 1. This function is applicable to single-pass hash operations for short messages.

2. You can call this function independently without needing to call the initialization function

3. Please refer to Appendix 4 for the calling method。

4.3.6. HASH close

HASH_Close HASH close

Function uint32_t HASH_Close(void)

Parameter

Return HASH_Close_OK：success other：fail

Notice

4.3.7. HASH get library version information

HASH_Version get HASH library version information

Function void HASH_Version(uint8_t *type, uint8_t *customer, uint8_t date[3], uint8_t *version)

Parameter type Business or Security version

customer Standard or customized version

国民技术股份有限公司 Nations 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
邮箱：info@nationz.com.cn 邮编：518057

date year，data，day

version //version x.x

Return

Notice

```
*type = 0x03;          // Security
*customer = 0x00;      // Standard
date[0] = 18;          //Year()
date[1] = 12;          //Month()
date[2] = 28;          //Day ()
*version = 0x10;       //version 1.0
```


国民技术股份有限公司 Nations 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
邮箱：info@nationz.com.cn 邮编：518057

5. RNG algorithm API specification

5.1. Usage of algorithm library

The usage method of the algorithm library is as follows:

1. Add RNG.h, Common.h to the header folder; Add Common.lib, RNG.lib to the project

2. Call the function according to the function description in section 5.3 . See the demo in Appendix 4 for test cases

5.2. Data type define

```
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. Function interface description

The RNG algorithm library contains the following list of functions：

Table 5-1 RNG algorithm library function table

Function	description
uint32_t GetTrueRand_U32(uint32_t *rand, uint32_t wordLen)	True random number

国民技术股份有限公司 Nations 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
邮箱：info@nationz.com.cn 邮编：518057

	generation function by word
uint32_t GetTrueRand_U8(uint8_t *rand, uint32_t bytelen)	True random number generation function by byte
uint32_t PseudoRandNumInit(uint32_t seed[5])	Pseudo random number initialization function
uint32_t PseudoRandNumReseed(uint32_t seed[5])	Pseudo random number seed update function
uint32_t GetPseudoRand_U32(uint32_t *rand, uint32_t wordLen)	Pseudo random number word-based generation function
void RNG_Version(uint8_t *type, uint8_t *customer, uint8_t date[3], uint8_t *version)	Obtain RNG library version Information

5.3.1. Pseudo random number initialization function

PseudoRandNumInit Pseudo random number initialization function

Function uint32_t PseudoRandNumInit(uint32_t seed[5])

Parameter seed input，The pseudo-random seed variable array can be NULL; when it is NULL, the internal true random number is used as the seed.

Return RNG_OK success ； other fail

5.3.2. Pseudo random number seed update function

PseudoRandNumReseed Pseudo random number seed update function

Function uint32_t PseudoRandNumReseed (uint32_t seed[5])

Parameter seed input，The pseudo-random seed variable array can be NULL; when it is NULL, the internal true random number is used as the seed.

Return RNG_OK success ； other fail

国民技术股份有限公司 Nations 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
邮箱：info@nationz.com.cn 邮编：518057

Notice When calling this function for the first time, you must first call the PseudoRandNumInit initialization function

5.3.3. Pseudo random number word-based generation function

GetPseudoRand_U32	Pseudo random number word-based generation function
Function	uint32_t GetPseudoRand_U32(uint32_t *rand, uint32_t wordLen)
Parameter	rand： point to rand number wordlen: Word length of the pseudo-random number to be obtained
Return	RNG_OK success； other fail
description	Generate pseudo-random numbers by word
Notice	When calling pseudo-random generation for the first time, you must first call the PseudoRandNumInit initialization function and the PseudoRandNumReseed seed update function. The user can input a seed array; if the user inputs seed as NULL, the seed will be automatically generated internally

5.3.4. True random number generation function by word

GetTrueRand_U32	True random number generation function by word
Function	uint32_t GetTrueRand_U32(uint32_t *rand, uint32_t wordLen)
Parameter	rand: point to rand number wordLen: Word length of the random number to be obtained
Return	RNG_OK success； other：fail

5.3.5. True random number generation function by byte

GetTrueRand_U8	True random number generation function by byte
函数原型	uint32_t GetTrueRand_U8(uint8_t *rand, uint32_t bytelen)
参数说明	rand: point to rand number

国民技术股份有限公司 Nations 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
邮箱：info@nationz.com.cn 邮编：518057

bytelen: Byte length of the random number to be obtained

返回值 RNG_OK success； other：fail

5.3.6. Obtain RNG library version Information

RNG_Version	Obtain RNG library version Information
Function	void RNG_Version(uint8_t *type, uint8_t *customer, uint8_t date[3], uint8_t *version)
Parameter	type Business or Security version customer Standard or customized version date year，data，day version //version x.x
Return	

Notice	*type = 0x03; // Security
	*customer = 0x00; // Standard
	date[0] = 18; //Year()
	date[1] = 12; //Month()
	date[2] = 28; //Day ()
	*version = 0x10; //version 1.0

国民技术股份有限公司 Nations 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
邮箱：info@nationz.com.cn 邮编：518057

6. SM4 lgorithm API specification

6.1. Usage of algorithm library

The usage method of the algorithm library is as follows:

1. Add SM4.h, Common.h to the header folder; Add Common.lib, SM4.lib to the project
2. Call the function according to the function description in section 6.3 . See the demo in Appendix 5 for test cases

6.2. Data type define

```
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 Nations 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
邮箱：info@nationz.com.cn 邮编：518057

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

6.3. Function interface description

The SM4 algorithm library contains the following list of functions：

Table 6-1 SM4 algorithm library function table

Function	description
uint32_t SM4_Init(SM4_PARM *parm)	SM4 initialization
uint32_t SM4_Crypto1(SM4_PARM *parm)	SM4 encryption/decryption
void SM4_Close(void)	SM4 close
void SM4_Version(uint8_t *type, uint8_t *customer, uint8_t date[3], uint8_t *version)	Obtain SM4 library version Information

6.3.1. SM4 initialization

SM4_Init SM4 initialization

Function uint32_t SM4_Init(SM4_PARM *parm)

Parameter parm input，point to SM4_PARM

Return SM4_ *Init* _OK：success other：fail

Notice

1. If it is ECB mode, the parameters iv can be directly replaced with NULL.
2. When encrypting a large amount of data as a whole but in multiple blocks using CBC mode, note the following:For the X-th block of data (X>1) encrypted by calling this function, the initialization vector IV used (IV = iv) must be updated to

国民技术股份有限公司 Nations 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
邮箱：info@nationz.com.cn 邮编：518057

the last block (16 bytes) of the ciphertext obtained by encrypting the (X-1)-th block of data with this function.

3. When decrypting a large amount of data as a whole but in multiple blocks using CBC mode, note the following:For the X-th block of data (X>1) decrypted by calling this function, the initialization vector IV used (IV = iv) must be updated to the last block (16 bytes) of the (X-1)-th block of data.

6.3.2. SM4 encryption/decryption

SM4_Crypto	SM4 encryption/decryption
Function	uint32_t SM4_Crypto1(SM4_PARM *parm)
Parameter	parm input，point to SM4_PARM
Return	SM4_Crypto_OK：success other：fail
Notice	

1. If it is ECB mode, the parameters iv can be directly replaced with NULL.

2.When encrypting a large amount of data as a whole but in multiple blocks using CBC mode, note the following:For the X-th block of data (X>1) encrypted by calling this function, the initialization vector IV used (IV = iv) must be updated to the last block (16 bytes) of the ciphertext obtained by encrypting the (X-1)-th block of data with this function.

3. When decrypting a large amount of data as a whole but in multiple blocks using CBC mode, note the following:For the X-th block of data (X>1) decrypted by calling this function, the initialization vector IV used (IV = iv) must be updated to the last block (16 bytes) of the (X-1)-th block of data.

6.3.3. SM4 close

SM4_Close	close SM4 algorithm and system clock
Function	void SM4_Close(void)

国民技术股份有限公司 Nations 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
邮箱：info@nationz.com.cn 邮编：518057

Parameter

Return

Notice

6.3.4. Obtain SM4 version information

SM4_Version	get SM4 version
Function	void SM4_Version(uint8_t *type, uint8_t *customer, uint8_t date[3], uint8_t *version)
Parameter	type Business or Security version customer Standard or customized version date year，data，day version //version x.x
Return	

Notice	*type = 0x03; // Security
	*customer = 0x00; // Standard
	date[0] = 18; //Year()
	date[1] = 12; //Month()
	date[2] = 28; //Day ()
	*version = 0x10; //version 1.0

国民技术股份有限公司 Nations 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
邮箱：info@nationz.com.cn 邮编：518057

i. Appendix Ⅰ DES algorithm library function call routine

```
//All data is in big-endian byte order
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};
```


国民技术股份有限公司 Nations 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
邮箱：info@nationz.com.cn 邮编：518057

```
    uint8_t
DES_CBC_ENC[16]={0x15,0x95,0xB5,0xAC,0xC1,0x5A,0xFC,0x62,0x62,0xD0,0xF8,0xEE,0xB1,0xF
C,0x1B,0xA8};
    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;
```


国民技术股份有限公司 Nations 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
邮箱：info@nationz.com.cn 邮编：518057

```
des_Parm.inByteLen=16;
des_Parm.key=key_8;
des_Parm.keyByteLen=8;
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;
```


国民技术股份有限公司 Nations 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
邮箱：info@nationz.com.cn 邮编：518057

```
des_Parm.key=key_16;
des_Parm.keyByteLen=16;
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_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;
```


国民技术股份有限公司 Nations 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
邮箱：info@nationz.com.cn 邮编：518057

```
des_Parm.keyByteLen=24;
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_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;
```


国民技术股份有限公司 Nations 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
邮箱：info@nationz.com.cn 邮编：518057

```
des_Parm.keyByteLen=8;
des_Parm.iv=iV;
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_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;
```


国民技术股份有限公司 Nations 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
邮箱：info@nationz.com.cn 邮编：518057

```
des_Parm.key=key_16;
des_Parm.keyByteLen=16;
des_Parm.iv=iV;
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;
```


国民技术股份有限公司 Nations 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
邮箱：info@nationz.com.cn 邮编：518057

```
    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.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 Nations 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
邮箱：info@nationz.com.cn 邮编：518057

ii. Appendix 2 AES algorithm lib function call routine

//All data is in big-endian byte order, natural sequence

```
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};
```


国民技术股份有限公司 Nations 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
邮箱：info@nationz.com.cn 邮编：518057

```
    uint8_t
CBC128_en[16]={0xFC,0x15,0x9F,0x65,0x7E,0x02,0xF7,0xEB,0x3A,0x5D,0xF0,0x8E,0x79,0x51,0xC
0,0x12};
    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};
```


国民技术股份有限公司 Nations 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
邮箱：info@nationz.com.cn 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=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;
```


国民技术股份有限公司 Nations 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
邮箱：info@nationz.com.cn 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=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))
{
```


国民技术股份有限公司 Nations 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
邮箱：info@nationz.com.cn 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=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))
```


国民技术股份有限公司 Nations 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
邮箱：info@nationz.com.cn 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=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);
```


国民技术股份有限公司 Nations 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
邮箱：info@nationz.com.cn 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=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);
```


国民技术股份有限公司 Nations 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
邮箱：info@nationz.com.cn 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=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;
```


国民技术股份有限公司 Nations 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
邮箱：info@nationz.com.cn 邮编：518057

```
AES_Init(&AES_Parm);
AES_Crypto(&AES_Parm);
if(memcmp(out2,in,16))
{
    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;
```


国民技术股份有限公司 Nations 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
邮箱：info@nationz.com.cn 邮编：518057

```
AES_Parm.out=out2;
AES_Init(&AES_Parm);
AES_Crypto(&AES_Parm);
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;
```


国民技术股份有限公司 Nations 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
邮箱：info@nationz.com.cn 邮编：518057

```
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_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;
```


国民技术股份有限公司 Nations 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
邮箱：info@nationz.com.cn 邮编：518057

```
    AES_Parm.keyBytelen=32;
    AES_Parm.iv=iv;
    AES_Parm.out=out2;
    AES_Init(&AES_Parm);
    AES_Crypto(&AES_Parm);
    if(memcmp(out2,in,16))
    {
        return 0x6D;
    }
    printf("aes_test is succsed!\r\n");

}
```

iii. Appendix 3 HASH algorithm lib function call routine

//All data is in big-endian byte order, natural sequence

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};
```


国民技术股份有限公司 Nations 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
邮箱：info@nationz.com.cn 邮编：518057

```
    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};
    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);
```


国民技术股份有限公司 Nations 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
邮箱：info@nationz.com.cn 邮编：518057

```
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;

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");
}
```


国民技术股份有限公司 Nations 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
邮箱：info@nationz.com.cn 邮编：518057

```
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");
}
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;
     }
```


国民技术股份有限公司 Nations 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
邮箱：info@nationz.com.cn 邮编：518057

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

iii.2 HASH_single_test

```
uint32_t HASH_single_test(void)
{
    uint32_t ret;
```


国民技术股份有限公司 Nations 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
邮箱：info@nationz.com.cn 邮编：518057

```
    uint8_t in[48]=
    {
0x1C,0xBB,0x9F,0x4A,0x43,0x6A,0xAD,0x81,0xFE,0x4F,0x52,0x4A,0x0A,0x76,0x22,0xC8,0x4F,0x9
0,0x18,0x30,0xA4,0xD2,0x8C, 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
    :
    uint8_t out[32];

    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};

  ret=SHA256_Hash(in,48,out);
  if(ret!=SHA256_Hash_OK)return 0x5A5A5A5A;
  if(memcmp(out,sha256_out,32))
  {
          return 0x5a5a5a5a;
  }
    else
    {
        printf("SHA256-Test success\r\n");
    }
    return 0;
}
```


国民技术股份有限公司 Nations 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
邮箱：info@nationz.com.cn 邮编：518057

iii.3 Hash_substep_test

```
uint32_t Hash_substep_test(void)
{
    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,
        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];
        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
```


国民技术股份有限公司 Nations 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
邮箱：info@nationz.com.cn 邮编：518057

```
    };
    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();
    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 Nations 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
邮箱：info@nationz.com.cn 邮编：518057

iv. Appendix 4 RNG algorithm lib function Call Routine

iv.1 Prng

```
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 Trng

```
uint32_t TRNG()
```


国民技术股份有限公司 Nations 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
邮箱：info@nationz.com.cn 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 Nations 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
邮箱：info@nationz.com.cn 邮编：518057

v.Appendix SM4 algorithm lib function call routine

```
//All data is in big-endian byte order, natural sequence
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
```


国民技术股份有限公司 Nations 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
邮箱：info@nationz.com.cn 邮编：518057

```
x02,0x69,0x86,0x3C,0x8F,0xA5,0x3A,0xAA,0xA9,0x60,0x11,0x15,0x25,0x15,0x56,0x23,0x12,0xE3,0x
B4,0x4B,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;
```


国民技术股份有限公司 Nations 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
邮箱：info@nationz.com.cn 邮编：518057

```
SM4_Parm.inBytelen=128;
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;
```


国民技术股份有限公司 Nations 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
邮箱：info@nationz.com.cn 邮编：518057

```
    SM4_Parm.out=out2;
    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 Nations 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
邮箱：info@nationz.com.cn 邮编：518057