



应用笔记

ACM32H5 系列芯片
算法库使用说明

版本: V1.0

日期: 2025-3-10

上海航芯电子科技股份有限公司

1. 算法库数据类型

算法库中的数据类型定义如下：

```
typedef unsigned char uint8_t;
```

```
typedef unsigned int uint32_t;
```

即 uint8_t 表示 8 位无符号数，uint32_t 表示 32 位无符号数。

2. HRNG

2.1. 主要特性

内含可靠噪声振荡器；
符合国际 FIPS-140-2 和 NIST SP800-22 测试标准；
符合国密局《随机数检测规范》测试标准；

2.2. 库文件说明

HRNG 模块需要的库及头文件如下：

hal_hrng.lib	实现取随机数操作
hal_hrng.h	hal_hrng.lib 对应的头文件

2.3. 函数说明

图表 2.3-1 HRNG 驱动函数说明

(函数内均有开关时钟操作)

函数名	功能描述	参数	
HAL_HRNG_Init	初始化函数用于启动随机数模块	输入	无
		输出	无
		返回值	无
HAL_HRNG_DeInit	关闭随机数模块	输入	无
		输出	无
		返回值	无
HAL_HRNG_GetHrng	取多个字节随机数	输入	uint32_t byte_len: 取随机数的字节长度
		输出	uint8_t *hdata: 存放随机数的起始地址
		返回值	0: 表示取随机数成功; 1: 表示失败

2.4. 注意事项

随机数库函数内均有开关时钟操作。

3. AES

3.1. 主要特性

- 支持 AES 加密和解密运算
- 支持 ECB/CBC/CTR 模式
- 数据输入和输出支持 SWAP 模式，即大小端可配置
- 支持 128/192/256 bit 密钥长度

3.2. 库文件说明

AES 模块需要的库及头文件如下：

hal_aes.lib	实现 AES 加解密运算
hal_aes.h	hal_aes 库对应的头文件

3.3. 函数说明

表 3.3-1 AES 驱动函数说明

(函数内均有开关时钟操作)

函数名	功能描述	参数	
HAL_AES_SetKey	配置 AES 密钥及对调模式	输入	uint32_t *keyin: 存放密钥的起始地址
			uint8_t key_len: 密钥长度(128/192/256)
			uint8_t swap_en: 输入输出大小端对调使能 0: 输入输出数据大小端对调禁止 1: 输入输出数据大小端对调使能
		输出	无
		返回值	无
HAL_AES_Crypt	AES 加解密函数	输入	uint32_t *indata: 存放输入数据的起始地址
			uint32_t block_len: 加解密的块(128 bit)个数
			uint8_t operation:加解密操作选择 0: 解密 1: 加密
			uint8_t mode: 加解密模式选择 0: ECB 模式 1: CBC 模式 2: CTR 模式
			uint32_t *iv: 存放 CBC/CTR 模式初始向量的起始地址 Note: CTR 模式时, iv[3]被用作计数器 cnt 值, 该值最大只能自加到 0xffffffff, 超过这个值 cnt 将回到 0 重新开始自加, iv[2]值始终不变。
			uint32_t security_mode: 安全模式选择 0x12345678: 普通模式 0: 安全模式

		输出	uint32_t *outdata: 存放输出结果的起始地址
		返回值	uint32_t 加解密运行结果 0: 运行失败 0xa59ada68: 运行成功

3.4. 注意事项

如果输入 AES 模块进行加解密运算的数据为 32bit 数组，高 32 位字数据存储 在数组的低位元素中，每个字以大端方式存放，举例如下：

设待加密数据为：0x112233445566778899aabbccddeeff00

则输入 AES 模块进行运算的数组为：

```
uint32_t plain_text[4] = {0x11223344, 0x55667788, 0x99aabbcc, 0xddeeff00};
```

如果使能 SWAP 模式，则输入 AES 模块进行运算的数组为：

```
uint32_t plain_text [4]= {0x44332211, 0x88776655, 0xccbbaa99, 0x00feedd};
```

输出数据格式与输入相同。

如果输入 AES 模块进行加解密运算的数据为 8bit 数组，举例如下：

设待加密数据为：0x112233445566778899aabbccddeeff00

则输入 AES 模块进行运算的数组为：

```
uint8_t plain_text[16] = {0x11,0x22,0x33,0x44,0x55,0x66,0x77,0x88,0x99,0xaa,0xbb,  
0xcc,0x dd,0xee,0xff,0x00};
```

如果使能 SWAP 模式，则输入 AES 模块进行运算的数组为：

```
uint8_t plain_text [16]={0x44,0x33,0x22,0x11,0x88,0x77,0x66,0x55,0xcc,0xbb,  
0xaa,0x99,0x00,0xff,0xee,0xdd};
```

输出数据格式与输入相同。

SWAP 模式对密钥、初始向量、输入数据、输出数据同时有效。

CTR 模式时，iv[3]被用作计数器 cnt 值，该值最大只能自加到 0xffffffff，超过这个值 cnt 将回到 0 重新开始自加，iv[0-2]值始终不变。

4. HASH

4.1. 主要特性

支持 SHA1/SHA256 算法

4.2. 库文件说明

HASH 模块需要的库及头文件如下：

hal_sha1.lib	实现 SHA1 运算
hal_sha1.h	hal_sha1.lib 对应的头文件
hal_256.lib	实现 SHA224/SHA256 运算
hal_256.h	hal_sha224_256.lib 对应的头文件

4.3. 函数说明

表 4.3-1 HASH 驱动函数说明

(函数内均有开关时钟操作)

函数名	功能描述	参数	
HAL_SHA1_Hash	SHA1 运算	输入	uint8_t *pDataIn: 待压缩数据的起始地址
			uint32_t DataLen: 待压缩数据的字节长度
		输出	uint8_t *pDigest: 摘要值的起始地址
		返回值	无
HAL_SHA256_Hash	SHA256 运算	输入	uint8_t *pDataIn: 待压缩数据的起始地址
			uint32_t DataLen: 待压缩数据的字节长度
		输出	uint8_t *pDigest: 摘要值的起始地址
		返回值	无

4.4. 注意事项

涉及到 HASH 运算的数据格式都是 big endian;

若：A = 0x11223344556677889900;

则：A[0] = 0x11;

A[1] = 0x22;

A[2] = 0x33;

A[3] = 0x44;

A[4] = 0x55;

A[5] = 0x66;

A[6] = 0x77;

```
A[7] = 0x88;  
A[9] = 0x99;  
A[10] = 0x00;
```

5. CRC

5.1. 主要特性

支持设置 7/8/16/32 位多项式及其正反向设置;

支持 8/16/32 位数据输入输出及其正反向设置;

支持 8/16/32 位数据输入输出及其正反向设置;

5.2. 库文件说明

CRC 模块提供源码，需要文件如下：

hal_crc.lib	实现 CRC 运算
hal_crc.h	hal_crc.c 对应的头文件

5.3. 函数说明

图表 5.3-1 CRC 驱动函数说明

(函数内均有开关时钟操作)

函数名	功能描述	参数	
HAL_CRC_Init	初始化 CRC 运算	输入	CRC_HandleTypeDef *hcrc: CRC 句柄指针
		输出	无
		返回值	无
HAL_CRC_Calculate	CRC 运算函数	输入	CRC_HandleTypeDef *hcrc: CRC 句柄指针
		输出	无
		返回值	uint32_t: CRC 结算结果

5.4. 注意事项

HAL_CRC_Calculate 函数内有开关时钟操作。

6. CORDIC

6.1. 主要特性

24 位 CORDIC 旋转引擎;
支持 sin/cos/atan2/sinh/cosh/atanh/sqrt/ln 等函数;

6.2. 库文件说明

HRNG 模块需要的库及头文件如下:

hal_cordic.lib	实现 cordic 各函数运算
hal_cordic.h	hal_cordic.lib 对应的头文件

6.3. 函数说明

图表 6.3-1 CORDIC 驱动函数说明

函数名	功能描述	参数	
HAL_CORDIC_CosSin_x x 为计算精度, 范围(1~8)	cos/sin 运算	输入	int angle_para: 以弧度为单位的角度值(除以 π ,范围[-1,1],Q31 格式)
		输出	int* cos_data:输入角度的 cos 值(范围[-1,1],Q31 格式)
			int* sin_data: 输入角度的 sin 值(范围[-1,1],Q31 格式)
		返回值	无
HAL_CORDIC_AtanSqrt_x x 为计算精度, 范围(1~8) atan 与 sqrt 值在精度 1 时误差非常大, 不建议使用	atan/sqrt 运算	输入	int x: x 方向坐标值(如果 $ x >1$,那么必须对其进行缩放以使其范围在[-1,1], Q31 格式)
			int y: y 方向坐标值(如果 $ y >1$,那么必须对其进行缩放以使其范围在[-1,1], Q31 格式)
		输出	int* sqrt_data: xy 代表向量的长度(Q31 格式) 需要除以(CORDIC_F_31>>4)得到 float 格式值
			int* atan_data: xy 代表向量的角度(Q31 格式) 需要乘以 PI 得到以弧度为单位的角度值
		返回值	无
HAL_CORDIC_CoshSinh_x x 为计算精度, 范围(1~8)	cosh/sinh 运算	输入	int angle_para: 双曲线角度值(范围[-0.559 ~0. 559] ,Q31 格式)
		输出	int* cosh_data:输入角度的 cosh 值(范围[0.5 0.846],Q31 格式)
			int* sinh_data: 输入角度的 sinh 值(范围[-0.683 0.683],Q31 格式)
		返回值	无

HAL_CORDIC_Atanh_x x 为计算精度，范围(1~8)	atanh 运算	输入	int angle_para: 双曲线角度值(范围[-0.403 0.403], Q31 格式)	
		输出	int* atanh_value: 输入角度的 atanh 值(Q31 格式)，需要乘 2 得到正确的 atanh 值	
		返回值	无	
HAL_CORDIC_Ln_x x 为计算精度，范围(1~8)	ln 运算	输入	int arg:输入参数(范围[0.054 0.875], Q31 格式)	
			int scale:缩放因子 需要根据原始数据 x 范围进行缩放: 原始数据范围 缩放因子 arg 范围 0.107 ≤ x < 1 1 0.0535 ≤ arg < 0.5 1 ≤ x < 3 2 0.25 ≤ ARG1 < 0.75 3 ≤ x < 7 3 0.375 ≤ ARG1 < 0.875 7 ≤ x ≤ 9.35 4 0.4375 ≤ ARG1 < 0.584	
			输出	int* ln_value: 输入参数的 ln 值(Q31 格式)，需要乘以 4 得到正确的 ln 值
			返回值	无
HAL_CORDIC_Sqrt_x x 为计算精度，范围(1~8)	sqrt 运算	输入	int arg: 输入参数(范围[0.027 0.875], Q31 格式)	
			int scale:缩放因子 需要根据原始数据 x 范围进行缩放: 原始数据范围 缩放因子 arg 范围 0.027 ≤ x < 0.75 0 0.027 ≤ ARG1 < 0.75 0.75 ≤ x < 1.75 1 0.375 ≤ ARG1 < 0.875 1.75 ≤ x ≤ 2.341 2 0.4375 ≤ ARG1 ≤ 0.585	
			输出	int* sqrt_value: 输入参数的 sqrt 值(Q31 格式)，需要乘以 2^scale/W_INV_Q31 得到正确的 sqrt 值
			返回值	无

6.4. 注意事项

Q31 格式中, 数字由 1 个符号位和 31 个二进制小数位表示, 因此数字范围是 -1(0x80000000)到 1-231(0x7FFFFFFF);

例如 0.5 转换成 Q31 格式为: $0.5 * 2^{31} = 1073741824 = 0x40000000$

6.5. 注意事项

Cordic 函数内没有开关时钟操作, 需在调用函数前外部打开时钟。

7. 版本历史

版本	日期	作者	描述
V1.0	2025-03-10	Hangxin	初始版

8. 版权声明

本文档的所有部分，其著作权归上海航芯电子科技股份有限公司（简称航芯科技）所有，未经航芯科技授权许可，任何个人及组织不得复制、转载、仿制本文档的全部或部分组件。本文档没有任何形式的担保、立场表达或其他暗示，若有任何因本文档或其中提及的产品所有资讯所引起的直接或间接损失，航芯科技及所属员工恕不为其担保任何责任。除此以外，本文档所提到的产品规格及资讯仅供参考，内容亦会随时更新，恕不另行通知。

联系我们

公司：上海航芯电子科技股份有限公司

地址：上海市闵行区合川路 2570 号科技绿洲三期 2 号楼 702 室

邮编：200241

电话：+86-21-6125 9080

传真：+86-21-6125 9080-830

Email: service@HangChip.com

Website: www.hangChip.com