# SHA256 软件实现说明

**注：**

**本文<章节 2>SHA-256 算法描述，摘录于《NIST.FIPS.180-4-2015》标准，如有疑问请参考源文献，欢迎指正勘误；**

**本文为 ECC 模块使用辅助文档，仅供参考。**

| 版本记录 | 版本修改说明 |
| --- | --- |
| V0.1 | 1. 初始版本 @20170207 |
| V0.2 | 1. 概述描述勘误 @20170829 |

# 1 1.概述

SHA 算法包括 SHA-1，SHA-256，SHA-224，SHA-512，SHA-384，SHA-512/224，SHA-512/256 这些分类；常用算法为 SHA-1 和 SHA-256，常作为 ECDSA 签名的 HASH 运算；

# 2 SHA-256 算法

现介绍 SHA-256 算法，以下算法来自**美国标准 NIST<FIPS.180-4-2015>;**

## 2.1 SHA-256 算法主体结构

$M^{(i)}$为消息块，长度 512-bit，超过 512bits 的消息，需要分段，不足 512 bits 需要补零操作；
$H^{(0)}$和 $K_t^{(256)}$为固定常量，长度分别 8*32-bit 和 64*32-bit
For i=1~N
{
1）准备消息调度表

$$W_t = \begin{cases} M_t^{(i)} & 0 \le t \le 15 \\ \sigma_1^{\{256\}}(W_{t-2}) + W_{t-7} + \sigma_0^{\{256\}}(W_{t-15}) + W_{t-16} & 16 \le t \le 63 \end{cases}$$

2）初始化工作变量 a，b，c，d，e，f，g，h

$$a = H_0^{(i-1)}$$
$$b = H_1^{(i-1)}$$
$$c = H_2^{(i-1)}$$
$$d = H_3^{(i-1)}$$
$$e = H_4^{(i-1)}$$
$$f = H_5^{(i-1)}$$
$$g = H_6^{(i-1)}$$
$$h = H_7^{(i-1)}$$

3）64 次迭代运算
For t=0~63
{

$$T_1 = h + \sum_1^{\{256\}}(e) + Ch(e,f,g) + K_t^{\{256\}} + W_t$$
$$T_2 = \sum_0^{\{256\}}(a) + Maj(a,b,c)$$
$$h = g$$
$$g = f$$
$$f = e$$
$$e = d + T_1$$
$$d = c$$
$$c = b$$
$$b = a$$
$$a = T_1 + T_2$$

}

4）计算中间 hash 值 $H^{(i)}$

$$H_0^{(i)} = a + H_0^{(i-1)}$$
$$H_1^{(i)} = b + H_1^{(i-1)}$$
$$H_2^{(i)} = c + H_2^{(i-1)}$$
$$H_3^{(i)} = d + H_3^{(i-1)}$$
$$H_4^{(i)} = e + H_4^{(i-1)}$$
$$H_5^{(i)} = f + H_5^{(i-1)}$$
$$H_6^{(i)} = g + H_6^{(i-1)}$$
$$H_7^{(i)} = h + H_7^{(i-1)}$$

}

经过 i=1~N，循环运算上面 1）~4），最后得到 256-bit 的消息摘要

$$H_0^{(N)} \| H_1^{(N)} \| H_2^{(N)} \| H_3^{(N)} \| H_4^{(N)} \| H_5^{(N)} \| H_6^{(N)} \| H_7^{(N)}$$

由于 SHA-224 除了 hash 初始值不同及 hash 结果 224-bit 外，算法与 SHA-256 相同。

## 2.2 SHA-256 引用逻辑函数

$$Ch(x,y,z) = (x \wedge y) \oplus (\neg x \wedge z)$$
$$Maj(x,y,z) = (x \wedge y) \oplus (x \wedge z) \oplus (y \wedge z)$$

$$\sum_0^{\{256\}}(x) = ROTR^2(x) \oplus ROTR^{13}(x) \oplus ROTR^{22}(x)$$
$$\sum_1^{\{256\}}(x) = ROTR^6(x) \oplus ROTR^{11}(x) \oplus ROTR^{25}(x)$$
$$\sigma_0^{\{256\}}(x) = ROTR^7(x) \oplus ROTR^{18}(x) \oplus SHR^3(x)$$
$$\sigma_1^{\{256\}}(x) = ROTR^{17}(x) \oplus ROTR^{19}(x) \oplus SHR^{10}(x)$$

## 2.3 Hash 初值

SHA-224 **Hash 初值：**

$$H_0^{(0)} = \texttt{c1059ed8}$$
$$H_1^{(0)} = \texttt{367cd507}$$
$$H_2^{(0)} = \texttt{3070dd17}$$
$$H_3^{(0)} = \texttt{f70e5939}$$
$$H_4^{(0)} = \texttt{ffc00b31}$$
$$H_5^{(0)} = \texttt{68581511}$$
$$H_6^{(0)} = \texttt{64f98fa7}$$

SHA-256 **Hash 初值：**

$$H_0^{(0)} = \texttt{6a09e667}$$
$$H_1^{(0)} = \texttt{bb67ae85}$$
$$H_2^{(0)} = \texttt{3c6ef372}$$
$$H_3^{(0)} = \texttt{a54ff53a}$$
$$H_4^{(0)} = \texttt{510e527f}$$
$$H_5^{(0)} = \texttt{9b05688c}$$
$$H_6^{(0)} = \texttt{1f83d9ab}$$
$$H_7^{(0)} = \texttt{5be0cd19}$$

## 2.4 固定常量 K

```
428a2f98 71374491 b5c0fbcf e9b5dba5 3956c25b 59f111f1 923f82a4 ab1c5ed5
d807aa98 12835b01 243185be 550c7dc3 72be5d74 80deb1fe 9bdc06a7 c19bf174
e49b69c1 efbe4786 0fc19dc6 240calcc 2de92c6f 4a7484aa 5cb0a9dc 76f988da
983e5152 a831c66d b00327c8 bf597fc7 c6e00bf3 d5a79147 06ca6351 14292967
27b70a85 2e1b2138 4d2c6dfc 53380d13 650a7354 766a0abb 81c2c92e 92722c85
a2bfe8a1 a81a664b c24b8b70 c76c51a3 d192e819 d6990624 f40e3585 106aa070
19a4c116 1e376c08 2748774c 34b0bcb5 391c0cb3 4ed8aa4a 5b9cca4f 682e6ff3
748f82ee 78a5636f 84c87814 8cc70208 90befffa a4506ceb bef9a3f7 c67178f2
```

# 3 软件实现

## 3.1 SHA256 库函数

函数声明：

void SHA256(SHA256_InputTypedef* SHA256_InputStruct, uint8_t *pHashAddr);

入口参数:

SHA256_InputTypedef　　SHA256 运算初始化变量结构体指针，主要包含 5 个参数:

1) pMtestAddr　　uint8_t *型变量，其指向对象待运算消息 m

2) LenMtest　　uint64_t 型变量，待运算的消息长度（byte）

pHashAddr　　uint8_t *型变量，其指向对象计算后的 HASH 结果

返回参数: 无

# 4 TESTCASE

| SHA256 TESTCASE |
| --- |
| Testcase0<br>消息(字符串）896bit<br>"qwertyuiopasdfghjklsdfhjknbsdjkfhwyer97234725wjnrlkjy879qwertyuiopasdfghjklsdfhjknbsdjkfhwyer97234725wjnrlkjy879"<br>摘要(hex)256bit<br>0x99bf8093cd9c98db84fe52e83ebe9a3ca959180f2cc966630ea3ca5e65d55e52 |
| Testcase1<br>消息(字符串）512bit<br>"qwertyuiopasdfghjklsdfhjknbsdjkfhwyer97234725wjnrlkjy87923523bjk"<br>摘要(hex)256bit<br>0xb98b0260087cab2f0c04042874323779942fdbbc878ec7a25e463312fefd726 |
| Testcase2<br>消息(字符串）448bit<br>"qwertyuiopasdfghjklsdfhjknbsdjkfhwyer97234725wjnrlkjy879"<br>摘要(hex)256bit<br>0x98c65f99b6613bc4a76a82abe6756b87bf8f4fcd00fabeba8173a25d7264e783 |

# 5 时间及资源消耗

**1）H1409 上软件实现 SHA-256 速度为:**

**1.38ms @PLL22MHz**

**2.76ms @PLL11MHz**

**5.52ms @PLL5.5MHz**

**以上结果是以消息长度 512-bit 评估，超过 512-bit 消息，以 512-bit 分段补零，时间按分段数线性增加。**

**2）软件实现 SHA-256 过程，ram 占有量约 4k，flash 数据存储 2k；**