密码运算实验手册

版本1.0



华为技术有限公司

目录

[1 课程介绍 2](#_Toc55554824)

[1.1 简介 2](#_Toc55554825)

[1.2 内容描述 2](#_Toc55554826)

[1.3 读者知识背景 2](#_Toc55554827)

[1.4 实验环境说明 2](#_Toc55554828)

[2 密码运算实验 3](#_Toc55554829)

[2.1 实验介绍 3](#_Toc55554830)

[2.1.1 关于本实验 3](#_Toc55554831)

[2.1.2 内容介绍 3](#_Toc55554832)

[2.1.3 密码运算指令集 3](#_Toc55554833)

[2.1.4 SHA256算法概述 6](#_Toc55554834)

[2.1.5 算法伪代码 9](#_Toc55554835)

[2.2 实验任务操作指导 11](#_Toc55554836)

[2.2.1 创建程序源码 11](#_Toc55554837)

[2.2.2 进行编译运行 21](#_Toc55554838)

[2.3 思考题及答案 22](#_Toc55554839)

# 课程介绍

## 简介

本书适用于学习ARM平台汇编课程的学生进行实验练习，完成本实验手册后，您将能更加充分理解ARM汇编代码运行环境的搭建、配置及编译运行，掌握如何在华为鲲鹏云服务器上完成环境配置，完成GNU ARM中的简单密码运算。

## 内容描述

本实验指导书通过在华为鲲鹏云服务器上，用加密指令实现SHA256算法的汇编代码。完成实验操作后，读者会掌握基本的汇编程序编写，对开发编译环境的配置、GNU ARM中的简单密码运算，以及加深对ARM平台的了解。

## 读者知识背景

本课程为ARM平台汇编基础扩展课程，为了更好地掌握本书内容，阅读本书的读者应首先具备以下基本条件：

* 具备基本的Linux命令能力；
* 基本的密码学知识；
* 基本的汇编代码和C语言代码的能力。

## 实验环境说明

* 华为鲲鹏云主机、openEuler20.03操作系统；
* 安装gcc7.3+版本；
* 每套实验环境可供1名学员上机操作。

# 密码运算实验

## 实验介绍

### 关于本实验

本实验将通过GNU标准的C语言和ARM汇编代码，在ARM平台上用加密指令实现SHA256算法。

### 教学目标

掌握GNU ARM平台汇编代码的编写以及编译运⾏方式。

### 内容介绍

本实验会先简单介绍一下密码运算的专用汇编指令集以及SHA256的算法，然后通过编写伪代码的方式，更好的理解算法的原理。最后完成在ARM平台上用C语言和汇编代码加密指令实现SHA256算法的实验。

### 密码运算指令集

基于32个128bit FP/SIMD寄存器v0-v31，ArmV8-A提供AES类、哈希类、SM类等常见密码运算的专用汇编指令。关于这些指令的具体格式和例子，可以参考文档Arm公司官方文档“Arm® Architecture Reference Manual --Armv8, for Armv8-A architecture profile”。

哈希运算指令集：

[SHA1C](https://developer.arm.com/docs/100069/0604/a64-simd-vector-instructions/sha1c): SHA1 hash update (choose).

[SHA1H](https://developer.arm.com/docs/100069/0604/a64-simd-vector-instructions/sha1h): SHA1 fixed rotate.

[SHA1M](https://developer.arm.com/docs/100069/0604/a64-simd-vector-instructions/sha1m): SHA1 hash update (majority).

[SHA1P](https://developer.arm.com/docs/100069/0604/a64-simd-vector-instructions/sha1p): SHA1 hash update (parity).

[SHA1SU0](https://developer.arm.com/docs/100069/0604/a64-simd-vector-instructions/sha1su0): SHA1 schedule update 0.

[SHA1SU1](https://developer.arm.com/docs/100069/0604/a64-simd-vector-instructions/sha1su1): SHA1 schedule update 1.

[SHA256H](https://developer.arm.com/docs/100069/0604/a64-simd-vector-instructions/sha256h): SHA256 hash update (part 1).

[SHA256H2](https://developer.arm.com/docs/100069/0604/a64-simd-vector-instructions/sha256h2): SHA256 hash update (part 2).

[SHA256SU0](https://developer.arm.com/docs/100069/0604/a64-simd-vector-instructions/sha256su0): SHA256 schedule update 0.

[SHA256SU1](https://developer.arm.com/docs/100069/0604/a64-simd-vector-instructions/sha256su1): SHA256 schedule update 1.

[SHA512H](https://developer.arm.com/docs/100069/0604/a64-simd-vector-instructions/sha512h): SHA512 Hash update part 1.

[SHA512H2](https://developer.arm.com/docs/100069/0604/a64-simd-vector-instructions/sha512h2): SHA512 Hash update part 2.

[SHA512SU0](https://developer.arm.com/docs/100069/0604/a64-simd-vector-instructions/sha512su0): SHA512 Schedule Update 0.

[SHA512SU1](https://developer.arm.com/docs/100069/0604/a64-simd-vector-instructions/sha512su1): SHA512 Schedule Update 1.

例如，SHA512H指令的格式为：SHA512H Q7,Q8,V9.2D。使用SHA512H指令来计算一个80轮迭代的SHA512哈希运算的例子如下：

// X0 contains the pointer to the bottom of the (padded) 16\*64 bytes of message to be

// hashed, with space above the that message to hold a further 64 \* 64 bytes of working

// data

// X1 contains the pointer to the 0th element of 80 64-bit constants (in ascending addresses) defined in the SHA2 specification

// X2 contains a loop variable

// V4,V5,V6, V7 hold VS0 to VS3 respectively

// V8 holds running hash V1

// V9 holds running hash V0

MOV X2, #0

loop1:

LD1 {V0.2D}, [X0] // Data

LD1 {V1.2D}, [X1] // K values

ADD X1, X1, #16

ADD X0, X0, #16

ADD X2, X2, #16

ADD V2.2D, V0.2D, V1.2D

EXT V2.16B, V2.16B, V2.16B, #8

EXT V8.16B, V6.16B, V7.16B, #8

EXT V9.16B, V5.16B, V6.16B, #8

ADD V7.2D, V7.2D, V2.2D

SHA512H Q7, Q8, V9.2D

ADD V10.2D, V5.2D, V7.2D

SHA512H2 Q7, Q5, V4.2D

MOV V5.16B, V4.16B

MOV V4.16B, V7.16B

MOV V7.16B, V6.16B

MOV V6.16B, V10.16B

CMP X2, #128

BLT loop1

// work out pointers to previous words in the data

SUB X3, X0, #128

SUB X4, X0, #112

SUB X5, X0, #16

SUB X6, X0, #56

loop2:

LD1 {V11.2D}, [X3]

LD1 {V12.2D}, [X4]

LD1 {V13.2D}, [X5]

LD1 {V14.2D}, [X6]

SHA512SU0 V11.2D, V12.2D

SHA512SU1 V11.2D, V13.2D, V14.2D

ST1 {V11.2D}, [X0]

LD1 {V1.2D}, [X1] // K values

ADD X0, X0, #16

ADD X1, X1, #16

ADD X3, X3, #16

ADD X4, X4, #16

ADD X5, X5, #16

ADD X6, X6, #16

ADD X2, X2, #16

ADD V2.2D, V11.2D, V1.2D

EXT V2.16B, V2.16B, V2.16B, #8

EXT V8.16B, V6.16B, V7.16B, #8

EXT V9.16B, V5.16B, V6.16B, #8

ADD V7.2D, V7.2D, V2.2D

SHA512H Q7, Q8, V9.2D

ADD V10.2D, V5.2D, V7.2D

SHA512H2 Q7, Q5, V4.2D

MOV V5.16B, V4.16B

MOV V4.16B, V7.16B

MOV V7.16B, V6.16B

MOV V6.16B, V10.16B

CMP X2, #320

BLT loop2

AES运算相关指令集：

[AESD](https://developer.arm.com/docs/100069/0604/a64-simd-vector-instructions/aesd): AES single round decryption.

[AESE](https://developer.arm.com/docs/100069/0604/a64-simd-vector-instructions/aese): AES single round encryption.

[AESIMC](https://developer.arm.com/docs/100069/0604/a64-simd-vector-instructions/aesimc): AES inverse mix columns.

[AESMC](https://developer.arm.com/docs/100069/0604/a64-simd-vector-instructions/aesmc): AES mix columns.

例如，AESD指令的格式为： AESD.<dt> <Qd>, <Qm>。

SM算法相关指令集：

[SM3PARTW1](https://developer.arm.com/docs/100069/0604/a64-simd-vector-instructions/sm3partw1): SM3PARTW1.

[SM3PARTW2](https://developer.arm.com/docs/100069/0604/a64-simd-vector-instructions/sm3partw2): SM3PARTW2.

[SM3SS1](https://developer.arm.com/docs/100069/0604/a64-simd-vector-instructions/sm3ss1): SM3SS1.

[SM3TT1A](https://developer.arm.com/docs/100069/0604/a64-simd-vector-instructions/sm3tt1a): SM3TT1A.

[SM3TT1B](https://developer.arm.com/docs/100069/0604/a64-simd-vector-instructions/sm3tt1b): SM3TT1B.

[SM3TT2A](https://developer.arm.com/docs/100069/0604/a64-simd-vector-instructions/sm3tt2a): SM3TT2A.

[SM3TT2B](https://developer.arm.com/docs/100069/0604/a64-simd-vector-instructions/sm3tt2b): SM3TT2B.

[SM4E](https://developer.arm.com/docs/100069/0604/a64-simd-vector-instructions/sm4e): SM4 Encode.

[SM4EKEY](https://developer.arm.com/docs/100069/0604/a64-simd-vector-instructions/sm4ekey): SM4 Key.

例如，SM4EKEY指令的格式为：SM4EKEY V8.4S, V8.4S, V16.4S。

### SHA256算法概述

SHA256是一个哈希函数。哈希函数，又称散列算法，是一种从任何一种数据中创建小的数字“指纹”的方法。散列函数把消息或数据压缩成摘要，使得数据量变小，将数据的格式固定下来。该函数将数据打乱混合，重新创建一个叫做散列值（或哈希值）的指纹。散列值通常用一个短的随机字母和数字组成的字符串来代表。对于任意长度的消息，SHA256都会产生一个256bit长的哈希值，称作消息摘要。SHA256用一个64位的数据来表示原始消息的长度。因此，通过SHA256计算的消息长度必须要小于2^64。长度信息的编码方式为64-bit的大尾端整数。关于大尾端的含义，可以自行查询。

SHA256算法的主要过程如下。

#### 常量初始化

SHA256算法中用到了8个哈希初值以及64个哈希常量。其中，SHA256算法的8个哈希初值如下：

h0 := 0x6a09e667

h1 := 0xbb67ae85

h2 := 0x3c6ef372

h3 := 0xa54ff53a

h4 := 0x510e527f

h5 := 0x9b05688c

h6 := 0x1f83d9ab

h7 := 0x5be0cd19

 这些初值是对自然数中前8个质数（2,3,5,7,11,13,17,19）的平方根的小数部分取前32bit而来。在SHA256算法中，用到的64个常量如下：

428a2f98 71374491 b5c0fbcf e9b5dba5

3956c25b 59f111f1 923f82a4 ab1c5ed5

d807aa98 12835b01 243185be 550c7dc3

72be5d74 80deb1fe 9bdc06a7 c19bf174

e49b69c1 efbe4786 0fc19dc6 240ca1cc

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

和8个哈希初值类似，这些常量是对自然数中前64个质数

(2,3,5,7,11,13,17,19,23,29,31,37,41,43,47,53,59,61,67,71,73,79,83,89,97…)的立方根的小数部分取前32bit而来。

#### 信息预处理（pre-processing）

SHA256算法中的预处理就是在想要Hash的报文后面补充需要的信息，使整个消息的长度满足指定的结构。该指定的结构由三个部分组成：基本报文、填充比特和附加的64位基本报文长度值。

信息预处理分为两个步骤：附加填充比特和附加长度。

附加填充比特

在报文末尾进行填充，使报文长度在对512取模以后的余数是448。填充是这样进行的：先补第一个比特为1，然后都补0，直到长度满足对512取模后余数是448。需要注意的是，信息必须进行填充，也就是说，即使长度已经满足对512取模后余数是448，补位也必须要进行，这时要填充512个比特。因此，填充是至少补一位，最多补512位。

例：以信息“abc”为例显示补位的过程。

a,b,c对应的16进制数分别是61,62,63，于是原始信息的二进制编码为：01100001 01100010 01100011。

补位第一步，首先补一个“1” ：0110000101100010 011000111。

补位第二步,补423个“0”：01100001 01100010 01100011 10000000 00000000 … 00000000。

补位完成后的数据如下（为了简介用16进制表示）：

61626380 00000000 00000000 00000000

00000000 00000000 00000000 00000000

00000000 00000000 00000000 00000000

00000000 00000000

为什么是448? 因为在第一步的预处理后，第二步会再附加上一个64bit的数据，用来表示原始报文的长度信息。而448+64=512，正好拼成了一个完整的结构。

附加长度值

附加长度值就是将原始数据（第一步填充前的消息）的长度信息补到已经进行了填充操作的消息后面。由于消息“abc”是3个字符，占用24个bit。因此，在进行了补长度的操作以后，整个消息就变成下面这样了（16进制格式）。

61626380 00000000 00000000 00000000

00000000 00000000 00000000 00000000

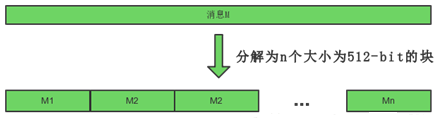
00000000 00000000 00000000 00000000

00000000 00000000 00000000 00000018

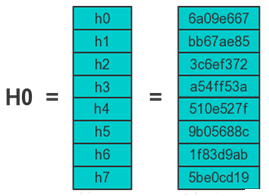
#### 计算消息摘要

现在来介绍SHA256算法的主体部分，即消息摘要是如何计算的。

首先：将消息分解成512-bit大小的块。



假设消息M可以被分解为n个块，于是整个算法需要做的就是完成n次迭代，n次迭代的结果就是最终的哈希值，即256bit的数字摘要。一个256-bit的摘要的初始值H0，经过第一个数据块进行运算，得到H1，即完成了第一次迭代。H1经过第二个数据块得到H2，……，依次处理，最后得到Hn，Hn即为最终的256-bit消息摘要。图中256-bit的Hi被描述8个小块，这是因为SHA256算法中的最小运算单元称为“字”（Word），一个字是32位。此外，第一次迭代中，映射的初值设置为前面介绍的8个哈希初值，如下图所示：



下面开始介绍每一次迭代的内容：

先构造64个字（word），对于每一块，将块分解为16个32-bit的big-endian的字，记为w[0], …, w[15]，也就是说，前16个字直接由消息的第i个块分解得到。其余的字由如下迭代公式得到：

https://img2018.cnblogs.com/blog/1488104/201909/1488104-20190911152042421-1781681943.png

 最后进行64次循环。

### 算法伪代码

在简单了解密码运算指令集和SHA256算法后，为了更好的理解算法的原理。本实验通过伪代码的形式，来展示如何实现一个简单的SHA256算法。

伪代码如下：

Note: All variables are unsigned 32 bits and wrap modulo 232 when calculating

Initialize variables

(first 32 bits of the fractional parts of the square roots of the first 8 primes 2..19):

h0 := 0x6a09e667

h1 := 0xbb67ae85

h2 := 0x3c6ef372

h3 := 0xa54ff53a

h4 := 0x510e527f

h5 := 0x9b05688c

h6 := 0x1f83d9ab

h7 := 0x5be0cd19

Initialize table of round constants

(first 32 bits of the fractional parts of the cube roots of the first 64 primes 2..311):

k[0..63] :=

0x428a2f98, 0x71374491, 0xb5c0fbcf, 0xe9b5dba5, 0x3956c25b, 0x59f111f1, 0x923f82a4, 0xab1c5ed5,

0xd807aa98, 0x12835b01, 0x243185be, 0x550c7dc3, 0x72be5d74, 0x80deb1fe, 0x9bdc06a7, 0xc19bf174,

0xe49b69c1, 0xefbe4786, 0x0fc19dc6, 0x240ca1cc, 0x2de92c6f, 0x4a7484aa, 0x5cb0a9dc, 0x76f988da,

0x983e5152, 0xa831c66d, 0xb00327c8, 0xbf597fc7, 0xc6e00bf3, 0xd5a79147, 0x06ca6351, 0x14292967,

0x27b70a85, 0x2e1b2138, 0x4d2c6dfc, 0x53380d13, 0x650a7354, 0x766a0abb, 0x81c2c92e, 0x92722c85,

0xa2bfe8a1, 0xa81a664b, 0xc24b8b70, 0xc76c51a3, 0xd192e819, 0xd6990624, 0xf40e3585, 0x106aa070,

0x19a4c116, 0x1e376c08, 0x2748774c, 0x34b0bcb5, 0x391c0cb3, 0x4ed8aa4a, 0x5b9cca4f, 0x682e6ff3,

0x748f82ee, 0x78a5636f, 0x84c87814, 0x8cc70208, 0x90befffa, 0xa4506ceb, 0xbef9a3f7, 0xc67178f2

Pre-processing:

append the bit '1' to the message

append k bits '0', where k is the minimum number >= 0 such that the resulting message

length (in bits) is congruent to 448(mod 512)

append length of message (before pre-processing), in bits, as 64-bit big-endian integer

Process the message in successive 512-bit chunks:

break message into 512-bit chunks

for each chunk

break chunk into sixteen 32-bit big-endian words w[0..15]

Extend the sixteen 32-bit words into sixty-four 32-bit words:

for i from 16 to 63

s0 := (w[i-15] rightrotate 7) xor (w[i-15] rightrotate 18) xor(w[i-15] rightshift 3)

s1 := (w[i-2] rightrotate 17) xor (w[i-2] rightrotate 19) xor(w[i-2] rightshift 10)

w[i] := w[i-16] + s0 + w[i-7] + s1

Initialize hash value for this chunk:

a := h0

b := h1

c := h2

d := h3

e := h4

f := h5

g := h6

h := h7

Main loop:

for i from 0 to 63

s0 := (a rightrotate 2) xor (a rightrotate 13) xor(a rightrotate 22)

maj := (a and b) xor (a and c) xor(b and c)

t2 := s0 + maj

s1 := (e rightrotate 6) xor (e rightrotate 11) xor(e rightrotate 25)

ch := (e and f) xor ((not e) and g)

t1 := h + s1 + ch + k[i] + w[i]

h := g

g := f

f := e

e := d + t1

d := c

c := b

b := a

a := t1 + t2

Add this chunk's hash to result so far:

h0 := h0 + a

h1 := h1 + b

h2 := h2 + c

h3 := h3 + d

h4 := h4 + e

h5 := h5 + f

h6 := h6 + g

h7 := h7 + h

Produce the final hash value (big-endian):

digest = hash = h0 append h1 append h2 append h3 append h4 append h5 append h6 append h7

## 实验任务操作指导

### 创建程序源码

实验说明：本实验通过GNU标准的C语言和汇编代码，使用加密指令来实现SHA256算法。通过对README.md文件的加密，验证了加密算法的作用。

以下步骤以在华为鲲鹏云服务器上执行为例。

创建目录

执行以下命令，创建sha256-armv8目录存放该程序的所有文件, 并进入sha256-armv8目录。

mkdir sha256-armv8

cd sha256-armv8

创建sha256算法源代码

执行以下命令，创建用加密指令实现SHA256算法的C源码sha256.c。

vim sha256.c

代码内容如下：

/\* sha256.c\*/

#include <stdio.h>

#include <string.h>

#include <stdint.h>

#include <stdbool.h>

void sha256\_block\_data\_order (uint32\_t \*ctx, const void \*in, size\_t num);

// SHA-256 initial hash value

const uint32\_t H\_0[8] = {

0x6a09e667,

0xbb67ae85,

0x3c6ef372,

0xa54ff53a,

0x510e527f,

0x9b05688c,

0x1f83d9ab,

0x5be0cd19,

};

void sha256\_print\_hash(uint32\_t \*H, const char \*title) {

printf("-----------------------------------------------------------------------------------------\n");

printf("| %-85s |\n", title);

printf("-----------------------------------------------------------------------------------------\n");

printf("| H[0] | H[1] | H[2] | H[3] | H[4] | H[5] | H[6] | H[7] |\n");

printf("| %08x | %08x | %08x | %08x | %08x | %08x | %08x | %08x |\n", H[0], H[1], H[2], H[3], H[4], H[5], H[6], H[7]);

printf("-----------------------------------------------------------------------------------------\n");

}

// initialize hash value

void sha256\_init(uint32\_t \*H) {

H[0] = 0x6a09e667;

H[1] = 0xbb67ae85;

H[2] = 0x3c6ef372;

H[3] = 0xa54ff53a;

H[4] = 0x510e527f;

H[5] = 0x9b05688c;

H[6] = 0x1f83d9ab;

H[7] = 0x5be0cd19;

}

int main(int argc, char \*\*argv) {

unsigned int i;

// check arguments

if (argc != 2) {

printf("Usage: %s <input file>\n", argv[0]);

return -1;

}

// open input file

FILE \*fp = fopen(argv[1], "r");

if (!fp) {

printf("Error opening file '%s' for reading.\n", argv[1]);

return -1;

}

// initialize hash value

uint32\_t H[8];

memcpy(H, H\_0, 8\*4);

// read file and calculate hash

uint64\_t bits = 0;

unsigned char buffer[64];

size\_t len;

while (len = fread(buffer, 1, sizeof(buffer), fp)) {

bits += len \* 8;

// preserve value of len by breaking on end of file (or error)

if (len < 64) {

break;

}

sha256\_block\_data\_order(H, buffer,1);

}

// add padding

if (len < 56) {

// padd current block to 56 byte

buffer[len] = 0x80;

i = len + 1;

} else {

// fill up current block and update hash

buffer[len] = 0x80;

for (i = len + 1; i < 64; i++) {

buffer[i] = 0x00;

}

sha256\_block\_data\_order(H, buffer,1);

// add (almost) one block of zero bytes

i = 0;

}

for (; i < 56; i++) {

buffer[i] = 0x00;

}

// add message length in bits in big endian

for (i = 0; i < 8; i++) {

buffer[63 - i] = bits >> (i \* 8);

}

sha256\_block\_data\_order(H, buffer,1);

// print hash

sha256\_print\_hash(H, "Final Hash");

// convert hash to char array (in correct order)

for (i = 0; i < 8; i++) {

buffer[i\*4 + 0] = H[i] >> 24;

buffer[i\*4 + 1] = H[i] >> 16;

buffer[i\*4 + 2] = H[i] >> 8;

buffer[i\*4 + 3] = H[i];

}

// print hash

printf("Hash:\t");

for (i = 0; i < 32; i++) {

printf("%02x", buffer[i]);

}

printf("\n");

return 0;

}

创建sha256-armv8-aarch32.S源代码

执行以下命令，创建sha256-armv8-aarch32.S源代码。

vim sha256-armv8-aarch32.S

代码内容如下：

/\* sha256-armv8-aarch32.S \*/

.text

.code 32

# SHA256 assembly implementation for ARMv8 AArch32

.global sha256\_block\_data\_order

.type sha256\_block\_data\_order,%function

.align 2

sha256\_block\_data\_order:

.Lsha256prolog:

vpush {q4}

vldmia r0, {s0, s1, s2, s3, s4, s5, s6, s7}

add r2, r1, r2, lsl #6

.Lsha256loop:

vld1.32 {d16-d19}, [r1]!

adr r3, .LKConstant256

vmov q2, q0

vmov q3, q1

vld1.32 {d20-d23}, [r1]!

vrev32.8 q8, q8

vldmia r3!, {d24, d25}

vrev32.8 q9, q9

vrev32.8 q10, q10

vldmia r3!, {d26, d27}

vadd.i32 q12, q8, q12

sha256su0.32 q8, q9

vrev32.8 q11, q11

vldmia r3!, {d28, d29}

vadd.i32 q13, q9, q13

vmov q4, q2

sha256h.32 q2, q3, q12

sha256h2.32 q3, q4, q12

sha256su0.32 q9, q10

sha256su1.32 q8, q10, q11

vldmia r3!, {d30, d31}

vadd.i32 q14, q10, q14

vmov q4, q2

sha256h.32 q2, q3, q13

sha256h2.32 q3, q4, q13

sha256su0.32 q10, q11

sha256su1.32 q9, q11, q8

vldmia r3!, {d24, d25}

vadd.i32 q15, q11, q15

vmov q4, q2

sha256h.32 q2, q3, q14

sha256h2.32 q3, q4, q14

sha256su0.32 q11, q8

sha256su1.32 q10, q8, q9

vldmia r3!, {d26, d27}

vadd.i32 q12, q8, q12

vmov q4, q2

sha256h.32 q2, q3, q15

sha256h2.32 q3, q4, q15

sha256su0.32 q8, q9

sha256su1.32 q11, q9, q10

vldmia r3!, {d28, d29}

vadd.i32 q13, q9, q13

vmov q4, q2

sha256h.32 q2, q3, q12

sha256h2.32 q3, q4, q12

sha256su0.32 q9, q10

sha256su1.32 q8, q10, q11

vldmia r3!, {d30, d31}

vadd.i32 q14, q10, q14

vmov q4, q2

sha256h.32 q2, q3, q13

sha256h2.32 q3, q4, q13

sha256su0.32 q10, q11

sha256su1.32 q9, q11, q8

vldmia r3!, {d24, d25}

vadd.i32 q15, q11, q15

vmov q4, q2

sha256h.32 q2, q3, q14

sha256h2.32 q3, q4, q14

sha256su0.32 q11, q8

sha256su1.32 q10, q8, q9

vldmia r3!, {d26, d27}

vadd.i32 q12, q8, q12

vmov q4, q2

sha256h.32 q2, q3, q15

sha256h2.32 q3, q4, q15

sha256su0.32 q8, q9

sha256su1.32 q11, q9, q10

vldmia r3!, {d28, d29}

vadd.i32 q13, q9, q13

vmov q4, q2

sha256h.32 q2, q3, q12

sha256h2.32 q3, q4, q12

sha256su0.32 q9, q10

sha256su1.32 q8, q10, q11

vldmia r3!, {d30, d31}

vadd.i32 q14, q10, q14

vmov q4, q2

sha256h.32 q2, q3, q13

sha256h2.32 q3, q4, q13

sha256su0.32 q10, q11

sha256su1.32 q9, q11, q8

vldmia r3!, {d24, d25}

vadd.i32 q15, q11, q15

vmov q4, q2

sha256h.32 q2, q3, q14

sha256h2.32 q3, q4, q14

sha256su0.32 q11, q8

sha256su1.32 q10, q8, q9

vldmia r3!, {d26, d27}

vadd.i32 q12, q8, q12

vmov q4, q2

sha256h.32 q2, q3, q15

sha256h2.32 q3, q4, q15

sha256su1.32 q11, q9, q10

vldmia r3!, {d28, d29}

vadd.i32 q13, q9, q13

vmov q4, q2

sha256h.32 q2, q3, q12

sha256h2.32 q3, q4, q12

vldmia r3!, {d30, d31}

vadd.i32 q14, q10, q14

vmov q4, q2

sha256h.32 q2, q3, q13

sha256h2.32 q3, q4, q13

vadd.i32 q15, q11, q15

vmov q4, q2

sha256h.32 q2, q3, q14

sha256h2.32 q3, q4, q14

vmov q4, q2

sha256h.32 q2, q3, q15

sha256h2.32 q3, q4, q15

teq r1, r2

vadd.i32 q0, q0, q2

vadd.i32 q1, q1, q3

bne .Lsha256loop

.Lsha256epilog:

vstmia r0, {s0, s1, s2, s3, s4, s5, s6, s7}

vpop {q4}

bx lr

.align 5

.LKConstant256:

.word 0x428a2f98,0x71374491,0xb5c0fbcf,0xe9b5dba5

.word 0x3956c25b,0x59f111f1,0x923f82a4,0xab1c5ed5

.word 0xd807aa98,0x12835b01,0x243185be,0x550c7dc3

.word 0x72be5d74,0x80deb1fe,0x9bdc06a7,0xc19bf174

.word 0xe49b69c1,0xefbe4786,0x0fc19dc6,0x240ca1cc

.word 0x2de92c6f,0x4a7484aa,0x5cb0a9dc,0x76f988da

.word 0x983e5152,0xa831c66d,0xb00327c8,0xbf597fc7

.word 0xc6e00bf3,0xd5a79147,0x06ca6351,0x14292967

.word 0x27b70a85,0x2e1b2138,0x4d2c6dfc,0x53380d13

.word 0x650a7354,0x766a0abb,0x81c2c92e,0x92722c85

.word 0xa2bfe8a1,0xa81a664b,0xc24b8b70,0xc76c51a3

.word 0xd192e819,0xd6990624,0xf40e3585,0x106aa070

.word 0x19a4c116,0x1e376c08,0x2748774c,0x34b0bcb5

.word 0x391c0cb3,0x4ed8aa4a,0x5b9cca4f,0x682e6ff3

.word 0x748f82ee,0x78a5636f,0x84c87814,0x8cc70208

.word 0x90befffa,0xa4506ceb,0xbef9a3f7,0xc67178f2

.size sha256\_block\_data\_order,.-sha256\_block\_data\_order

.align 2

创建sha256-armv8-aarch64.S源代码

执行以下命令，创建sha256-armv8-aarch64.S源代码。

vim sha256-armv8-aarch64.S

代码内容如下：

/\* sha256-armv8-aarch64.S \*/

.text

.arch armv8-a+crypto

# SHA256 assembly implementation for ARMv8 AArch64

.global sha256\_block\_data\_order

.type sha256\_block\_data\_order,%function

.align 2

sha256\_block\_data\_order:

.Lsha256prolog:

stp x29, x30, [sp,#-64]!

mov x29, sp

adr x3, .LKConstant256

str q8, [sp, #16]

ld1 {v16.4s-v19.4s}, [x3], #64

ld1 {v0.4s}, [x0], #16

ld1 {v20.4s-v23.4s}, [x3], #64

add x2, x1, x2, lsl #6

ld1 {v1.4s}, [x0]

ld1 {v24.4s-v27.4s}, [x3], #64

sub x0, x0, #16

str q9, [sp, #32]

str q10, [sp, #48]

ld1 {v28.4s-v31.4s}, [x3], #64

.Lsha256loop:

ld1 {v5.16b-v8.16b}, [x1], #64

mov v2.16b, v0.16b

mov v3.16b, v1.16b

rev32 v5.16b, v5.16b

rev32 v6.16b, v6.16b

add v9.4s, v5.4s, v16.4s

rev32 v7.16b, v7.16b

add v10.4s, v6.4s, v17.4s

mov v4.16b, v2.16b

sha256h q2, q3, v9.4s

sha256h2 q3, q4, v9.4s

sha256su0 v5.4s, v6.4s

rev32 v8.16b, v8.16b

add v9.4s, v7.4s, v18.4s

mov v4.16b, v2.16b

sha256h q2, q3, v10.4s

sha256h2 q3, q4, v10.4s

sha256su0 v6.4s, v7.4s

sha256su1 v5.4s, v7.4s, v8.4s

add v10.4s, v8.4s, v19.4s

mov v4.16b, v2.16b

sha256h q2, q3, v9.4s

sha256h2 q3, q4, v9.4s

sha256su0 v7.4s, v8.4s

sha256su1 v6.4s, v8.4s, v5.4s

add v9.4s, v5.4s, v20.4s

mov v4.16b, v2.16b

sha256h q2, q3, v10.4s

sha256h2 q3, q4, v10.4s

sha256su0 v8.4s, v5.4s

sha256su1 v7.4s, v5.4s, v6.4s

add v10.4s, v6.4s, v21.4s

mov v4.16b, v2.16b

sha256h q2, q3, v9.4s

sha256h2 q3, q4, v9.4s

sha256su0 v5.4s, v6.4s

sha256su1 v8.4s, v6.4s, v7.4s

add v9.4s, v7.4s, v22.4s

mov v4.16b, v2.16b

sha256h q2, q3, v10.4s

sha256h2 q3, q4, v10.4s

sha256su0 v6.4s, v7.4s

sha256su1 v5.4s, v7.4s, v8.4s

add v10.4s, v8.4s, v23.4s

mov v4.16b, v2.16b

sha256h q2, q3, v9.4s

sha256h2 q3, q4, v9.4s

sha256su0 v7.4s, v8.4s

sha256su1 v6.4s, v8.4s, v5.4s

add v9.4s, v5.4s, v24.4s

mov v4.16b, v2.16b

sha256h q2, q3, v10.4s

sha256h2 q3, q4, v10.4s

sha256su0 v8.4s, v5.4s

sha256su1 v7.4s, v5.4s, v6.4s

add v10.4s, v6.4s, v25.4s

mov v4.16b, v2.16b

sha256h q2, q3, v9.4s

sha256h2 q3, q4, v9.4s

sha256su0 v5.4s, v6.4s

sha256su1 v8.4s, v6.4s, v7.4s

add v9.4s, v7.4s, v26.4s

mov v4.16b, v2.16b

sha256h q2, q3, v10.4s

sha256h2 q3, q4, v10.4s

sha256su0 v6.4s, v7.4s

sha256su1 v5.4s, v7.4s, v8.4s

add v10.4s, v8.4s, v27.4s

mov v4.16b, v2.16b

sha256h q2, q3, v9.4s

sha256h2 q3, q4, v9.4s

sha256su0 v7.4s, v8.4s

sha256su1 v6.4s, v8.4s, v5.4s

add v9.4s, v5.4s, v28.4s

mov v4.16b, v2.16b

sha256h q2, q3, v10.4s

sha256h2 q3, q4, v10.4s

sha256su0 v8.4s, v5.4s

sha256su1 v7.4s, v5.4s, v6.4s

add v10.4s, v6.4s, v29.4s

mov v4.16b, v2.16b

sha256h q2, q3, v9.4s

sha256h2 q3, q4, v9.4s

sha256su1 v8.4s, v6.4s, v7.4s

add v9.4s, v7.4s, v30.4s

mov v4.16b, v2.16b

sha256h q2, q3, v10.4s

sha256h2 q3, q4, v10.4s

add v10.4s, v8.4s, v31.4s

mov v4.16b, v2.16b

sha256h q2, q3, v9.4s

sha256h2 q3, q4, v9.4s

mov v4.16b, v2.16b

sha256h q2, q3, v10.4s

sha256h2 q3, q4, v10.4s

cmp x1, x2

add v1.4s, v1.4s, v3.4s

add v0.4s, v0.4s, v2.4s

b.ne .Lsha256loop

.Lsha256epilog:

st1 {v0.4s,v1.4s}, [x0]

ldr q10, [sp, #48]

ldr q9, [sp, #32]

ldr q8, [sp, #16]

ldr x29, [sp], #64

ret

.align 5

.LKConstant256:

.word 0x428a2f98,0x71374491,0xb5c0fbcf,0xe9b5dba5

.word 0x3956c25b,0x59f111f1,0x923f82a4,0xab1c5ed5

.word 0xd807aa98,0x12835b01,0x243185be,0x550c7dc3

.word 0x72be5d74,0x80deb1fe,0x9bdc06a7,0xc19bf174

.word 0xe49b69c1,0xefbe4786,0x0fc19dc6,0x240ca1cc

.word 0x2de92c6f,0x4a7484aa,0x5cb0a9dc,0x76f988da

.word 0x983e5152,0xa831c66d,0xb00327c8,0xbf597fc7

.word 0xc6e00bf3,0xd5a79147,0x06ca6351,0x14292967

.word 0x27b70a85,0x2e1b2138,0x4d2c6dfc,0x53380d13

.word 0x650a7354,0x766a0abb,0x81c2c92e,0x92722c85

.word 0xa2bfe8a1,0xa81a664b,0xc24b8b70,0xc76c51a3

.word 0xd192e819,0xd6990624,0xf40e3585,0x106aa070

.word 0x19a4c116,0x1e376c08,0x2748774c,0x34b0bcb5

.word 0x391c0cb3,0x4ed8aa4a,0x5b9cca4f,0x682e6ff3

.word 0x748f82ee,0x78a5636f,0x84c87814,0x8cc70208

.word 0x90befffa,0xa4506ceb,0xbef9a3f7,0xc67178f2

.size sha256\_block\_data\_order,.-sha256\_block\_data\_order

.align 2

### 进行编译运行

创建makefile

执行以下命令，创建Makefile。

vim Makefile

代码内容如下：

CC = gcc

CFLAGS = -O3 -mcpu=generic+crypto

sha256:sha256.c

$(CC) $(CFLAGS) sha256.c sha256-armv8-aarch64.S -o sha256

创建README.md

执行以下命令，创建README.md。

vim README.md

代码内容如下：

# SHA-256

This is a very basic implementation of a SHA-256 hash according to the [FIPS

180-4 standard](http://csrc.nist.gov/publications/fips/fips180-4/fips-180-4.pdf)

in C. I did it for educational purposes, the code is not optimized at all, but

(almost) corresponds line by line to the standard.

The algorithm to process a small block of data is quite simple and very well

described in the standard. I found that correctly implementing the padding is

much harder.

It does not have any dependencies (except for the C standard library of course)

and can be compiled with `make`. When `sha256sum` is installed, a short test can

be run with `make test`.

Usage:

./main <input file>

```

编译

执行以下命令，进行编译。

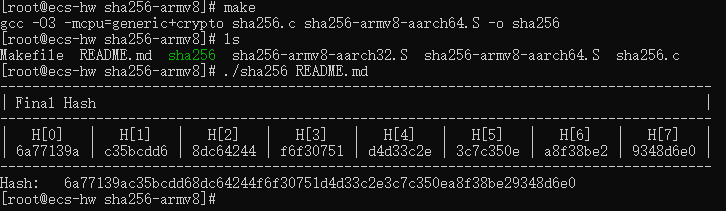
make

运行程序

执行以下命令，运行可执行文件sha256，并查看结果。

./sha256 README.md

命令和生成的结果如下：



可以看到通过SHA256加密后，README.md文件的Hash值为：

6a77139ac35bcdd68dc64244f6f30751d4d33c2e3c7c350ea8f38be29348d6e0。

## 思考题及答案

* 除了SHA256还有哪些常见的加密算法？

参考答案：

DES加密算法、AES加密算法、RSA加密算法、Base64加密算法、MD5加密算法、SHA1加密算法、XXXTEA加密算法。

说明：《汇编与接口技术》课程配套实验手册中的实验内容由北京交通大学计算机与信息技术学院赵宏智老师提供，华为公司负责实验手册文档的编写。