山东大学
SHANDONG UNIVERSITY

Project4 SM3 实现和优化

学院 网络空间安全

专业 网络空间安全

学号 202200460149

班级姓名 网安 22.1 班张弛

2025 年 7 月 14 日

目录

1 实验任务

实现 SM3 的实现和优化

2 SM3 实现

2.1 SM3 概述

SM3 密码杂凑算法是中国国家密码管理局 2010 年公布的中国商用密码杂凑算法标准。该算法于 2012 年发布为密码行业标准 (GM/T 0004-2012)，2016 年发布为国家密码杂凑算法标准 (GB/T 32905-2016)。

SM3 采用 Merkle-Damgard 结构。消息分组长度为 512 位，摘要值长度为 256 位。

整个算法的执行过程可以概括成四个步骤：消息填充、消息扩展、迭代压缩、输出结果。

2.2 消息填充

SM3 的消息扩展步骤是以 512 位的数据分组作为输入的。因此，我们需要在一开始就把数据长度填充至 512 位的倍数。数据填充规则和 MD5 一样，具体步骤如下：

1、先填充一个 “1”，后面加上 k 个 “0”。其中 k 是满足 (n+1+k) mod 512 = 448 的最小正整数。

2、追加 64 位的数据长度（bit 为单位，大端序存放 1。）

一个例子如下所示：

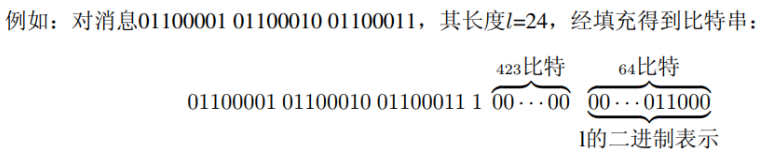

图 1 消息填充

代码实现如下所示：

2.3 消息扩展

SM3 这一步骤产生 132 个消息字。（一个消息字的长度为 32 位，4 个字节，8 个 16 进制数字）概括来说，先将一个 512 位数据分组划分为 16 个消息字，并

且作为生成的 132 个消息字的前 16 个。再用这 16 个消息字递推生成剩余的 116 个消息字。

在最终得到的 132 个消息字中，前 68 个消息字构成数列 $\{W_j\}$，后 64 个消息字构成数列 $\{W'_j\}$，其中下标 j 从 0 开始计数。

5.3.2 消息扩展

将消息分组$B^{(i)}$按以下方法扩展生成132个字$W_0, W_1, \cdots, W_{67}, W'_0, W'_1, \cdots, W'_{63}$，用于压缩函数$CF$：

a)将消息分组$B^{(i)}$划分为16个字$W_0, W_1, \cdots, W_{15}$。

b)FOR j=16 TO 67

$W_j \leftarrow P_1(W_{j-16} \oplus W_{j-9} \oplus (W_{j-3} \lll 15)) \oplus (W_{j-13} \lll 7) \oplus W_{j-6}$

ENDFOR

c)FOR j=0 TO 63

$W'_j = W_j \oplus W_{j+4}$

ENDFOR

图 2 消息扩展

2.4 迭代压缩

SM3 使用消息扩展得到的消息字进行迭代压缩运算：

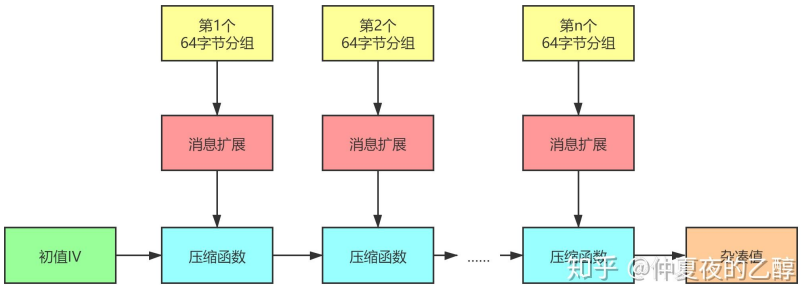

图 3 迭代压缩

初值 IV 被放在 A、B、C、D、E、F、G、H 八个 32 位变量中。整个算法中最核心、也最复杂的地方就在于压缩函数。压缩函数将这八个变量进行 64 轮相同的计算，64 轮的计算过程如下图所示：

2.5 输出结果

将得到的 A、B、C、D、E、F、G、H 八个变量拼接输出，就是 SM3 算法的输出，一共 256bit。

令A,B,C,D,E,F,G,H为字寄存器,$SS1,SS2,TT1,TT2$为中间变量,压缩函数$V^{i+1} = CF(V^{(i)}, B^{(i)}), 0 \leq i \leq n-1$。计算过程描述如下：

$ABCDEFGH \leftarrow V^{(i)}$

FOR j=0 TO 63

$SS1 \leftarrow ((A \lll 12) + E + (T_j \lll j)) \lll 7$

$SS2 \leftarrow SS1 \oplus (A \lll 12)$

$TT1 \leftarrow FF_j(A,B,C) + D + SS2 + W'_j$

$TT2 \leftarrow GG_j(E,F,G) + H + SS1 + W_j$

$D \leftarrow C$

$C \leftarrow B \lll 9$

$B \leftarrow A$

$A \leftarrow TT1$

$H \leftarrow G$

$G \leftarrow F \lll 19$

$F \leftarrow E$

$E \leftarrow P_0(TT2)$

ENDFOR

$V^{(i+1)} \leftarrow ABCDEFGH \oplus V^{(i)}$

其中，字的存储为大端(big-endian)格式。

图 4 轮操作

3　SM3 优化

3.1　优化 1：SIMD 优化

3.2　优化 2：

3.3　优化 3

4　参考链接

1、https://blog.csdn.net/qq_40662424/article/details/121637732