SM3密码杂凑算法

1 符号

∧:32比特与运算

∨:32比特或运算

⊕:32比特异或运算

¬:32比特非运算

<<<k:32比特循环左移k比特运算

⟵:左移赋值运算符

2 常数与函数

2.1 初始值

IV = 7380166f 4914b2b9 172442d7 da8a0600 a96f30bc 163138aa e38dee4d b0fb0e4e

2.2 常量

$$T_j = \begin{cases} 79cc4519 & 0 \le j \le 15 \\ 7a879d8a & 16 \le j \le 63 \end{cases}$$

2.3 布尔函数

$$FF_j(X,Y,Z) = \begin{cases} X \oplus Y \oplus Z & 0 \le j \le 15 \\ (X \wedge Y) \vee (X \wedge Z) \vee (Y \wedge Z) & 16 \le j \le 63 \end{cases}$$

$$GG_j(X,Y,Z) = \begin{cases} X \oplus Y \oplus Z & 0 \le j \le 15 \\ (X \wedge Y) \vee (\neg X \wedge Z) & 16 \le j \le 63 \end{cases}$$

其中 X，Y，Z为字

2.4 置换函数

$$P_0(X) = X \oplus (X <<< 9) \oplus (X <<< 17)$$
$$P_1(X) = X \oplus (X <<< 15) \oplus (X <<< 23)$$

3 算法描述

3.1 概述

SM3密码杂凑算法的输入为长度为 l ($l < 2^{64}$)比特的消息m，经过填充、迭代压缩，生成杂凑值，杂凑值输出长度为256比特。

3.2 填充

假设消息m的长度为 l 比特，首先将比特"1"添加到消息的末尾，再添加 k 个"0"，k 是满足 $l+k\equiv 448(mod512)$的最小的非负整数。然后再添加一个64位比特串，该比特串是长度 l 的二进制表示。填充后的消息m'的比特长度为512的倍数。

3.3 迭代压缩

3.3.1 迭代过程

将填充后的消息m'按照512比特进行分组：$m'=B^{(0)}B^{(1)}\cdots B^{(n-1)}$，其中$n=(l+k+65)/512$。对$m'$按照下列方式迭代：

$$
\begin{aligned}
&FOR\quad i=0\quad TO\quad n-1\\
&V^{(i+1)}=CF(V^{(i)},B^{(i)})\\
&ENDFOR
\end{aligned}
$$

其中CF为压缩函数，$V^{(0)}$为256比特初始值IV，$B^{(i)}$为填充后的消息分组，迭代压缩结果为$V^{(n)}$

3.3.2 消息扩展

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

$$
\begin{aligned}
&a)\text{将消息分组}B^{(i)}\text{划分为}16\text{个字}W_0,W_1,\dots,W_{15}\\
&b)FOR\quad j=16\quad TO\quad 67\\
&W_j\leftarrow P(W_{j-16}\oplus W_{j-9}\oplus(W_{j-3}<<<15))\oplus(W_{j-13}<<<7)\oplus W_{j-6}\\
&c)FOR\quad j=0\quad TO\quad 63\\
&W'_j=W_j\oplus W_{j+4}
\end{aligned}
$$

3.3.3 压缩函数

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 $V^{i+1}=CF(V^{(i)},B^{(i)}),0\le i\le n-1$。计算描述过程如下：

$$
\begin{aligned}
&FOR\quad j=0\quad TO\quad 63\\
&SS1\leftarrow((A<<<12)+E+(T_i<<<(j\ mod\ 32)))<<<7\\
&SS2\leftarrow SS1\oplus(A<<<12)\\
&TT1\leftarrow FF_i(A,B,C)+D+SS2+W'_i\\
&TT2\leftarrow GG_i(E,F,G)+H+SS1+W'_i\\
&D\leftarrow C\\
&C\leftarrow B<<<9\\
&B\leftarrow A\\
&A\leftarrow TT1\\
&H\leftarrow G\\
&G\leftarrow F<<<19\\
&F\leftarrow E\\
&E\leftarrow P_0(TT2)\\
&ENDFOR\\
&V^{(i+1)}\leftarrow ABCDEFGH\oplus V^{(i)}
\end{aligned}
$$

3.3.4 输出杂凑值

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

输出256比特的杂凑值$y = ABCDEFGH$