实验结果：

已知secret（未知）长度为3位，对应的sm3摘要为

66c7f0f462eeedd9d1f2d46bdc10e4e24167c4875cf2f7a2297da02b8f4ba8e0



已知Secret+补充部分+str2(已知)所对应的sm3摘要为

accf73ffc14f32535d8814377cf8cad2238c905fbdb50528036f5bef72052639



利用长度扩展攻击，任意输入长度为3的str代替secret,也能获得同样的sm3摘要。

如图，对于任意输入的长度为3的“fsw”,产生了相同的sm3摘要

