在密码学和计算机安全中，长度扩展攻击（Length extension attacks）是指针对某些允许包含额外信息的加密散列函数的攻击手段。该攻击适用于在消息与密钥的长度已知的情形下，所有采取了 H(key||message) 此类构造的散列函数。MD5 和 SHA-1 等基于 Merkle–Damgård 构造的算法均对此类攻击显示出脆弱性。

攻击的要点在于：

攻击者可以控制 message

攻击者需要知道 key 的长度，如不知道可以考虑暴力破解

攻击已经知道了包含 key 的一个消息的 hash 值

SM3 的消息长度是 64 字节或者它的倍数，如果消息的长度不足则需要填充，之后对消息进行分组，每组 64 字节，每一次加密一组，并更新 8 个初始向量，并继续用新向量去加密下一组，以此类推。可以利用这一特性去实现攻击，当我们得到第一次加密后的向量值时，再人为构造一组消息用于下一次加密，就可以在不知道 secret 的情况下得到合法的 hash 值，这是因为 8 个向量中的值便能表示第一轮的加密结果。

攻击可以达到的效果在于，如果知道一个原消息哈希值 H(key||M1) 及其 key||M1 长度，对于任意的字符串 M2，攻击者可以计算出 H(pad(key||M1) + M2) 的值，而不需要知道是 key 及 M1 是多少。