我们按照要求分三部分实现：SM3基础实现与优化、长度扩展攻击验证、Merkle树构建及证明。

第一部分：SM3基础实现与优化

我们将从基础实现开始，然后逐步优化。

第二部分：长度扩展攻击验证

基于SM3的实现，演示长度扩展攻击。

第三部分：Merkle树构建（10w叶子节点）及存在性证明和不存在性证明

按照RFC6962构建Merkle树，并实现证明。

结果如下：



