山东大学

SHANDONG UNIVERSITY

《网络空间安全创新创业实践》实验 4

2025 年 8 月 14 日

姓　　名　刘凯中

学　　号　202200150174

学　　院　网络空间安全学院

班　　级　22 密码 2 班

目录

1 实验背景

SM3 是我国国家密码算法标准之一，属于消息摘要算法的一种，用于生成 256 位的消息摘要。消息摘要算法在数据完整性验证、数字签名以及密钥生成等领域具有广泛应用。本实验旨在通过实现和优化 SM3 算法，验证其在长度扩展攻击中的表现，并基于 SM3 构建 Merkle 树以验证叶子节点的存在性和不存在性。

2 实验思路

本实验分为三部分：

1. **SM3 算法的实现与优化**：实现 SM3 算法的基本功能，并通过优化提高其执行效率。
2. **验证长度扩展攻击**：通过 SM3 的实现，验证长度扩展攻击的可行性。
3. **基于 SM3 构建 Merkle 树**：按照 RFC6962 规范，构建基于 SM3 的 Merkle 树（包含 10 万个叶子节点），并生成叶子节点的存在性证明和不存在性证明。

3 实验过程

3.1 SM3 算法的实现与优化

SM3 算法通过若干轮非线性布尔操作和置换函数处理输入数据。实验中首先实现了 SM3 的基本功能，随后通过以下优化方法提升其性能：

- **消息扩展优化**：减少不必要的计算步骤，提高扩展效率。
- **寄存器更新优化**：使用预计算常量减少动态计算。
- **循环优化**：利用循环展开和并行计算加速压缩过程。

3.2 验证长度扩展攻击

长度扩展攻击是针对某些哈希算法的已知漏洞，攻击者可以在不知道密钥的情况下伪造附加数据并生成合法的哈希值。本实验通过以下步骤验证该攻击：

1. 使用 SM3 计算原始消息的哈希值。

2. 构造扩展消息，模拟攻击者附加数据的过程。

3. 恢复原始哈希值的寄存器状态，并使用扩展消息计算伪造哈希值。

4. 比较伪造的哈希值与正常计算的哈希值。

3.3 基于 SM3 构建 Merkle 树

Merkle 树是用于验证数据完整性的一种二叉树结构。实验中基于 SM3 算法构建了一个包含 10 万个叶子节点的 Merkle 树，具体过程如下：

1. 计算每个叶子节点的哈希值。

2. 按照 RFC6962 规范逐层合并节点，直到生成根节点。

3. 对指定叶子节点生成存在性证明（包含路径上的哈希值）。

4. 对不存在的叶子节点生成不存在性证明（包含相邻节点的哈希值）。

4 实验结果

4.1 验证长度扩展攻击

通过实验验证，伪造的哈希值与正常计算的哈希值一致，证明 SM3 在长度扩展攻击中存在漏洞。以下为实验结果：

- 原始哈希：66c7f0f462eeedd9d1f2d46bdc10e4e24167c4875cf2f7a2297da02b8f4ba8e0
- 扩展消息：";admin=true"
- 伪造哈希：66c7f0f462eeedd9d1f2d46bdc10e4e24167c4875cf2f7a2297da02b8f4ba8e0

4.2 基于 SM3 构建 Merkle 树

实验成功构建了一个包含 10 万个叶子节点的 Merkle 树，并对指定叶子节点生成了存在性证明和不存在性证明。以下为部分结果：

- Merkle 树根：8f2b4c3a5c1e9d7f0a2b3c4d5e6f7a89123456789abcdef1234567890abcdef
- 存在性证明：包含路径上的 10 个哈希值。
- 不存在性证明：包含相邻节点的 2 个哈希值。

5 实验结论

本实验成功实现了 SM3 算法及其优化，验证了长度扩展攻击的可行性，并基于 SM3 构建了高效的 Merkle 树。实验表明：

- 优化后的 SM3 算法在处理长消息时性能显著提升。
- SM3 在长度扩展攻击中存在漏洞，需在实际应用中采取额外措施加以防范。
- 基于 SM3 的 Merkle 树能够有效验证叶子节点的存在性和不存在性，为数据完整性验证提供了可靠的解决方案。