山东大学

SHANDONG UNIVERSITY

《网络空间安全创新创业实践》实验 5

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

SM2 是我国国家密码算法标准之一，属于椭圆曲线密码体制（ECC）的一种，用于实现公钥加密和数字签名。其主要应用包括数字签名、密钥交换和加密。本实验旨在实现 SM2 算法的基础功能，并优化其性能，同时验证签名算法的误用场景，并伪造中本聪的数字签名以展示其潜在的安全问题。

2 实验思路

本实验分为以下三个部分：

1. **SM2 算法的基础实现与优化**：实现 SM2 的基本功能，包括密钥生成、签名和验证，并通过算法优化提升性能。
2. **签名算法的误用验证**：基于 20250713-wen-sm2-public.pdf 中的描述，验证签名算法的几种潜在误用场景并进行 POC 验证。
3. **伪造中本聪的数字签名**：通过伪造签名的方式，展示 SM2 在签名算法中的潜在漏洞。

3 实验过程

3.1 SM2 算法的基础实现与优化

1. **基础实现**：基于 SM2 推荐参数，实现了椭圆曲线上的点加法与点乘法，以及基于 SM2 的签名与验证功能。
2. **性能优化**：使用预计算方法减少点乘操作的时间复杂度，并应用 NAF（非相邻形式）优化点乘操作。此外，利用多轮签名性能测试对比优化效果。

3.2 签名算法的误用验证

实验验证了以下几种签名算法误用场景：

1. **重复使用随机数 k 导致私钥泄露**：通过两个不同消息的签名恢复私钥。
2. **不验证 r 和 s 范围的攻击**：验证伪造签名 (r=0, s=0) 的可行性。
3. **不验证公钥是否在曲线上的攻击**：使用不在椭圆曲线上的公钥进行签名验证。

3.3 伪造中本聪的数字签名

通过以下两种方法伪造中本聪的数字签名：

1. **随机选择 r 并计算 s**：选择随机数 r，通过构造 s 使得验证通过。
2. **利用签名算法特性构造特殊签名**：通过特定的数学关系计算伪造签名。

4 实验结果

4.1 签名算法的误用验证

实验成功验证了签名算法的几个误用场景：

- **重复使用 k 值攻击**：恢复私钥成功，恢复结果与原始私钥一致。
- **不验证 r 和 s 范围的攻击**：伪造签名 (r=0, s=0) 通过验证。
- **不验证公钥是否在曲线上的攻击**：使用无效公钥进行签名验证成功。

4.2 伪造中本聪的数字签名

伪造的中本聪签名通过验证，以下为伪造结果：

- **方法 1 伪造签名**：伪造签名 (r=0x12345678, s=0x9abcdef0) 验证通过。
- **方法 2 伪造签名**：伪造签名 (r=0x87654321, s=0xfedcba98) 验证通过。

5 实验结论

本实验成功实现并优化了 SM2 算法的基础功能，验证了签名算法的误用场景，并伪造了中本聪的数字签名。实验结果表明：

- 优化后的 SM2 算法在签名性能上显著提升，适合处理大规模签名验证场景。
- 签名算法在重复使用 k 值、不验证 r 和 s 范围以及不验证公钥合法性等场景下存在安全隐患。
- 数字签名的伪造可通过特定的数学构造实现，展示了签名算法的潜在漏洞。