山东大学

SHANDONG UNIVERSITY

《网络空间安全创新创业实践》实验 6

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

Google Password Checkup 协议是一种隐私保护的密码泄露检查协议，旨在帮助用户验证其密码是否出现在泄露的数据库中，同时保证用户的隐私。该协议基于密码哈希、同态加密和椭圆曲线加密技术，可以在不泄露用户密码的情况下进行泄露检测。本实验基于刘巍然老师的报告《Google Password Checkup》和论文 2019-723.pdf 中的 Figure 2 协议，使用 Python 实现该协议并验证其功能。

2 实验思路

本实验的目标是实现 Google Password Checkup 协议，具体分为以下步骤：

1. **客户端数据处理**：将客户端密码哈希到椭圆曲线上的点，并进行指数运算以保护用户隐私。
2. **服务器数据处理**：服务器对密码进行双重哈希，并加密关联的泄露次数信息。
3. **交集计算与同态加法求和**：客户端和服务器协同计算密码交集，并使用同态加密技术对泄露次数求和。
4. **服务器解密求和结果**：服务器解密最终的泄露次数总和，验证协议的正确性。

3 实验过程

3.1 协议的实现

本实验基于椭圆曲线密码学和 Paillier 同态加密技术，具体包括以下步骤：

1. **客户端第一轮**：客户端将密码哈希到椭圆曲线上的点，并使用随机指数进行加密以保护隐私。
2. **服务器第二轮**：服务器对密码进行双重哈希，加密泄露次数，并返回双重哈希的密码和加密值。
3. **客户端第三轮**：客户端计算交集，并对交集中泄露次数进行同态加法求和。
4. **服务器解密结果**：服务器解密最终的求和结果，并验证协议正确性。

3.2 实现细节

- 使用 HKDF 对密码进行哈希，并映射到椭圆曲线上的点。
- 使用 Paillier 加密对泄露次数进行加密，并支持同态加法操作。
- 使用随机数和指数运算保护客户端和服务器密码隐私。

4 实验结果

4.1 交集和计算验证

实验结果表明，协议可以正确计算密码交集，并对泄露次数进行同态加法求和。以下为实验结果：

- 客户端密码：`password123`, `securePass`, `admin123`, `qwerty`
- 服务器密码：`password123`, `qwerty`, `admin`, `123456`
- 交集：`password123`, `qwerty`
- 泄露次数总和：265000

4.2 协议正确性验证

实验验证了协议的正确性，解密后的求和结果与实际交集的泄露次数总和一致。

5 实验结论

本实验成功实现了 Google Password Checkup 协议，并验证了其功能。实验结果表明：

- 协议能够在保护用户密码隐私的同时，正确计算密码交集并进行泄露次数求和。
- 使用椭圆曲线密码学和 Paillier 同态加密技术可以有效保护隐私并支持同态操作。