说明文档

1. 协议目标

Google Password Checkup 协议旨在在保护用户隐私的前提下，检测用户密码是否出现在已知泄露密码库中。协议要求用户密码不被泄露给服务器，同时服务器无法推断用户的真实密码，而客户端能够安全得到检测结果。协议核心思想包括哈希前缀匹配、私有集合成员资格（PSM）和k-匿名性，并通过同态加密保证查询安全。

2. 协议流程概述

当用户在客户端输入密码后，客户端首先通过 `Client.hash_password` 将密码做 SHA-1 哈希，并使用 `Client.get_prefix` 提取哈希的高位前缀作为查询标识。客户端随后使用 Paillier 公钥对前缀加密，并通过 `Client.check_password` 将加密前缀发送给服务器。

服务器在 `Server.homomorphic_check` 中接收加密前缀后，对泄露密码库中的哈希进行匹配，并返回加密后的匹配结果。整个匹配过程在加密域进行，服务器无法获取用户真实密码。客户端收到结果后使用私钥解密，判断密码是否出现在泄露库中，从而完成安全验证。

3. 协议特点

该协议保证用户密码在传输过程中不以明文形式发送给服务器，服务器仅能操作加密数据，无法得知真实密码或前缀。客户端在本地解密得到最终判断结果，确保安全性和准确性。