从258中了解到，Google Password Checkup依赖于一种称为隐私集合交集（Private Set Intersection，PSI）的加密协议。更具体地说，它使用了一种增强版的PSI协议，称为"隐私加入和计算"（Private Join and Compute）。该协议结合了两种基本的加密技术：隐私集合交集和同态加密。隐私集合交集允许双方私下加入他们的集合并发现他们共有的标识符，而同态加密允许直接对加密数据执行某些计算，而不必先解密5。

25还提到，该协议确保所有输入（标识符及其相关数据）在整个过程中保持完全加密且不可读，任何一方都没有透露他们的原始数据，最终结果是以聚合统计信息的形式解密和共享的唯一结果。

协议的核心步骤包括：客户端对用户名和密码进行加盐哈希处理，使用盲签名技术向服务器请求凭证加密密钥，生成凭证加密哈希值，然后与服务器端的泄露凭证数据库进行隐私集合交集查询，最后客户端可以确定自己的凭证是否已泄露，而服务器不会得知用户的凭证信息。

实验结果：

