doi:10.1631/FITEE.1800518

题目：高效可验证的雾辅助私有集合交集计算

概要：私有集合交集计算允许两方实体在不泄露除交集结果以外其他信息的前提下计算出两方实体的集合交集。随着雾计算的发展，将集合交集外包至雾的需求应运而生。然而，目前私有集合交集计算都是基于全同态加密和配对操作，所需代价较高且不支持移动，难以在雾计算中应用。提出一种高效可验证的雾辅助私有集合交集计算方案。在该方案中，实体将私有集合交集计算外包至雾，雾在没有解密能力的前提下计算集合交集。该方案不依赖全同态加密和配对操作，极大提高了计算效率。此外，构建并证明了该方案的安全性。最后，对比分析本方案与其他方案的通信复杂度和计算复杂度。分析结果表明，该方案更高效，更具现实意义。

关键词：私有集合交集计算；雾计算；可验证；数据隐私