doi:10.1631/FITEE.1800066

题目：一种基于 Chaum-Pedersen 协议的欺骗可检测云存储数据共享协议

概要：随着云计算技术的发展，数据可外包给云，方便用户共享。然而，用户常常担心其数据在云端的可靠性和完整性。因此，在云端提供安全的数据共享服务至关重要。本文将门限秘密共享技术和Chaum-Pedersen零知识证明相结合，提出一种可靠、安全的云数据共享方案。该方案不仅有效、灵活、语义安全，还能有效识别行为不诚实的欺骗者身份，确保合法用户解密密钥的安全。相比而言，该方案计算性能较好，尤其适合云端用户医疗保险数据保护。

关键词：数据分享；Chaum-Pedersen 证明；欺骗可检测；云储存