doi:10.1631/FITEE.1601530

题目：云存储环境下一种基于身份的公开审计协议安全性分析

概要：数据完整性公开验证对提高云存储系统的适用性、可服务性至关重要。最近，Tan 和 Jia（2014）提出了一种基于身份的云数据完整性公开验证（NaEPASC）协议，以简化用户密钥管理和减轻完整性验证负担。NaEPASC 可以使第三方审计人员（third-party auditor, TPA）能够在云计算环境中高效和安全地验证外包数据的完整性。然而，本文指出 NaEPASC 在数据签名阶段容易遭受签名伪造攻击，即恶意云服务器可以通过使用两个正确的签名来伪造任意数据块的有效签名。此外，证明了 NaEPASC 在挑战阶段受到数据隐私威胁，即 TPA 或冒充 TPA 的外部攻击者可以分析出外包数据的内容。本文分析表明 NaEPASC 在数据验证过程中不安全。本文的工作有助于密码学家和工程师设计、实施更安全高效的基于身份的云存储数据完整性公开审计方案。

关键词：云数据；公开审计；数据完整性；数据隐私