doi:10.1631/FITEE.1800405

题目：云存储中基于属性加密的通用型用户撤销系统

概要：云存储是面向企业和个人用户的服务模型，包括付费和免费两种方式。基于云存储服务模型，用户通过互联网随时随地享受云存储提供的存储服务和管理功能。由于大多数云存储由第三方服务商提供，因此在数据保护和访问控制方面，云存储提供商和共享多租户环境下可信任性面临极大挑战。基于属性加密（attribute-based encryption，ABE）不仅保护数据的机密性，而且其中的密文或解密密钥与相关细粒度访问策略有关，这些策略在解密过程中被自动执行，使每个数据级别的数据访问处于控制之下。但是，在实际动态用户撤销应用中该方案有一定局限性。提出两种具有隐私保护功能的基于属性加密的通用型用户撤销系统：通过密文重加密（user revocation via ciphertext re-encryption，UR-CRE）实现的用户撤销系统和通过云存储提供商（user revocation via cloud storage providers，UR-CSP）实现的用户撤销系统。这两种系统可以与任意类型基于属性加密的方案协作，实现动态撤销用户。

关键词：基于属性的加密；通用型用户撤销；用户隐私；云存储；访问控制