基于属性的加密中的若干关键技术研究

作者：张星

随着云计算的广泛应用，越来越多的用户和机构选择将数据存储在云存储系统中，但是这些数据中不乏一些敏感数据，为保证它们的安全，需要对其进行加密存储。基于属性的加密（attribute-based encryption, ABE）实现了对于存储在第三方的加密数据的细粒度共享。但是，基于属性的加密中仍有很多问题没有得到很好的解决，例如分层、可追责性、密钥托管等问题，需要更深一步的研究和探索，否则将大大阻碍基于属性的加密的进一步应用。为了解决这些问题，对基于属性的加密中的一些关键技术进行研究，包括：

针对支持分层的基于属性的加密（hierarchical attribute-based encryption, HABE）表达能力受限的情况，提出了一种支持分层的基于属性的加密方案，该方案基于支持单调访问结构的 ABE 方案，借鉴 HIBE 的分层策略组织多个 KGC，从而实现了一个支持单调访问结构的 HABE 方案，论文在标准模型下证明了给出的 HABE 方案是选择安全的。针对 HABE 方案中线上加密开销大的问题，论文采取线下加密与线上加密相结合的方法，较好解决了该问题，并通过了实验验证。

针对 ABE 对用户和机构同时进行追责支持不足的情况，提出了一种支持追责的基于属性的加密方案，该方案通过在用户密钥中加入用户身份信息和 KGC 无法获知的秘密信息，从而实现在白盒模型下既支持用户追责又支持机构追责。论文在标准模型下证明了给出的方案是选择安全的。针对移动设备的计算能力和电池续航能力不足的问题，论文采取支持密文的外包解密方法，较好解决了该问题。

针对 ABE 中存在的密钥托管问题，提出了一种面向密钥托管的基于属性的加密方案，该方案通过 KGC 和 OAA 两个机构联合生成用户密钥，从而可以抵抗用户与单个机构的合谋攻击。论文在标准模型下证明了给出的方案是选择安全的，且通过实验验证，该方案与基于单机构的加密方案相比，用户加密和解密阶段的开销没有明显增加，其增加的开销主要在密钥生成阶段。

研究成果可以应用在社交网络、付费电视、审计日志、个人电子病历等需要加密共享的领域。此外，本文对于信息安全的多个研究方向，如细粒度访问控制、广播加密、可搜索加密、组密钥管理、隐私保护等也有很好地推动作用。