格上基于身份的门限代理重加密方案及应用

吴立强[1]，韩益亮[1]，杨晓元[1,2]，张敏情[1]
[1]中国人民武装警察部队工程大学网络和信息安全重点实验室，中国西安市，710086
[2]西安电子科技大学计算机网络与信息安全教育部重点实验室，中国西安市，710071

摘要：门限代理重加密通过设置多个代理者，不仅能有效防止单个代理者和被授权者合谋，从而违背授权者的意愿随意转化任意文件，而且能在某些代理者瘫痪或者损毁的情况下仍然提供正常服务。本文提出一个格上非交互的基于身份门限代理重加密方案，无需公钥证书。在设计方案过程中，采用了两次Shamir的秘密共享方法，一方面有效隐藏了授权者的私钥信息，另一方面通过分割代理重加密密钥，实现了代理权限的去中心化。鲁棒性是指某个代理者如果提交了非法的密文转化密文份额，那么组合者会立刻识别出这个恶意的代理者。本文方案通过格上全同态签名实现了这一属性。因此，即使未来量子攻击变得可行，我们整个方案也能完全抵抗量子攻击。本文方案的安全性在标准模型下规约为判定性差错学习困难假设。最后，给出本文方案的两个典型应用场景，包括基于区块链的文件共享系统和基于门限密码学的鲁棒密钥托管系统。

关键词：后量子密码；门限代理重加密；格；鲁棒性；去中心化
https://doi.org/10.1631/FITEE.2000366