doi:10.1631/FITEE.1500219

题目：标准模型下基于高效分级身份的格上加密方案

概要：本文在标准模型下，利用固定维数的格基代理算法提出了一种高效的格基分级身份加密方案。其公钥尺寸仅为$(dm^2+mn)\log q$比特，而消息-密文扩展因子仅为$\log q$，其中d为最大分级深度，(n, m, q)为公开参数。本文构造了一种新的公钥赋值算法，将 1 个随机、公开的矩阵平均赋值为两个身份比特，从而仅仅需要d个公开矩阵来构造标准模型下的 HIBE 方案；与之相比，Crypto 2010 所提出的 HIBE 方案中需要$2d$个同样尺寸的矩阵，公钥尺寸达到$(2dm^2+mn+m)\log q$。为了将该方案的消息-密文扩展因子压缩到$\log q$，本文基于 Gentry 的加密方案建立了一种基础加密算法，一次加密操作中能够加密m^2比特明文并得到$m^2\log q$比特密文。因此，文中所提方案在公钥尺寸、消息-密文扩展因子等方面具有一定的优势。基于差错学习问题的困难性，我们证明该方案在选择身份、选择明文攻击下是安全的。

关键词：分级身份加密；格密码；标准模型；差错学习问题；高斯