**doi:**10.1631/FITEE.1700534

**题目：**不依赖双线性对的带关键字搜索的无证书公钥加密方案构造

**概要：**可搜索公钥加密使存储服务器在未知数据内容时能对其存储的加密数据进行搜索，这为加密数据存储系统检索密文提供一种非常理想的解决方法。无证书公钥密码体制是一种具有许多优点的新型密码学原语，它不仅克服了基于身份密码体制中的密钥托管问题，而且避免了传统公钥密码体制中复杂的证书管理问题。目前文献中已有3个带关键字搜索的无证书公钥加密方案。然而，这些方案的构造都需要使用耗时的双线性对运算，因此不适用于计算资源受限或电量受限的设备。针对这一问题，我们设计了一个不依赖双线性对的带关键字搜索的无证书公钥加密方案。基于计算性Diffie-Hellman问题的困难性假设，我们证明所提出方案在随机预言模型中满足适应性选择关键字攻击下的密文不可区分安全性。效率对比和仿真实验表明，该方案具有更好性能。此外，我们还给出3个拓展方案。

**关键词：**可搜索公钥加密；带关键字搜索的无证书公钥加密；双线性对；计算性Diffie-Hellman问题