附件 1：最佳论文评选申请表

<table>
<tr><td>论文题目</td><td colspan="3">Revisiting Attribute-Based Encryption With Verifiable Outsourced Decryption</td></tr>
<tr><td>申请人</td><td colspan="3">林素青</td></tr>
<tr><td rowspan="3">论文作者</td><td rowspan="3">（请全体作者签名）
林素青，张锐，马晖，王明生</td><td rowspan="3">索引机构</td><td>√ SCI</td></tr>
<tr><td>☐ EI</td></tr>
<tr><td>☐ ISTP</td></tr>
<tr><td>期刊/
会议信息</td><td colspan="3">（请给出刊文的期刊或会议的名称，卷、期、页等信息）
IEEE Transactions on Information Forensics and Security (CCF 网络与信息安全，A 类期刊(排名第二)，中科院 SCI 分区为 2 区)，第 10 卷，第 10 期，第 2119-2130 页.</td></tr>
<tr><td>申请人自述</td><td colspan="3">（请简述论文的目的和意义，解决了什么问题，有何贡献或影响。总字数不超过 500 字）
基于属性密码学的访问控制技术，能同时实现对存储数据的隐私保护和细粒度访问控制。由于传统的属性加密方案，其解密计算量使得资源有限的弱终端用户难以承受,Green 等人提出具有外包解密功能的属性加密方案。为确保第三方服务器诚实可靠地执行外包解密运算，Lai 等人在外包解密中引入验证机制，提出具有外包解密可验证功能的属性加密方案，发表于 IEEE Transactions on Information Forensics and Security (2013)。
本论文改进并推广了 Lai 等人的方案，提出通用的构造方法，构造具有外包解密可验证功能的属性加密系统，为设计面向弱终端用户的访问控制机制提供一种系统可行的方法。理论分析可知，我们的方案在保证存储数据安全性的同时，能实现对外包解密的可靠性验证，且密文长度仅是同类方案的一半；实验验证，我们的方案，与同类方案相比，在计算效率和通信效率两方面均提高 50%。总之，我们的设计方法推进了基于属性密码学的访问控制技术从理论层面向实际应用的转化。</td></tr>
</table>