

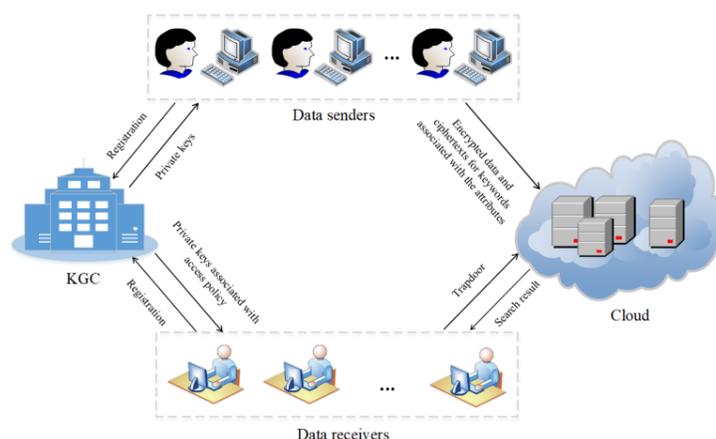


## 网络与信息安全科研团队论文被计算机网络信息安全领域顶级期刊IEEE TIFS录用

发布日期: 2023-10-13, 周五 发布人: 吴琢宇

近日, 我院网络与信息安全科研团队在网络信息安全领域研究最新研究成果被计算机网络信息安全领域顶级期刊IEEE TIFS录用。研究成果: ABAEKS: Attribute-Based Authenticated Encryption With Keyword Search Over Outsourced Encrypted data。该论文主要由罗富财副研究员, 王海燕助理研究员, 林昌露教授, 闫幸福研究员共同完成。

云计算的广泛采用和数据的指数级增长凸显了对安全数据共享的需求和查询。基于属性的关键字搜索 (ABKS) 已经成为一种针对存储在云中的加密数据的有效搜索手段。然而, 现有的ABKS方案很容易受到量子计算机的攻击, (内部) 关键字猜测攻击 (KGA), 或需要高的端到端延迟。为了解决这些问题, 罗富财等人引入了一个新的概念, 称为关键字可搜索的基于属性认证加密 (ABAEKS), 并提出了一种高效的ABAEKS方案。该ABAEKS 方案需要的端到端延迟低, 并且能够抵抗量子计算机攻击和 (内部) KGA。通过大量实验表明, 该ABAEKS方案在计算上是高效的, 并优于当前最先进的ABKS方案。



IEEE TIFS, 英文全称IEEE Transactions on Information Forensics and Security, 这个期刊是中国计算机学会推荐国际学术会议和期刊列表的A类期刊, 影响因子 6.8, 在网络与信息安全领域具有极高的评价。

**分类:** 学院新闻 (/zh-hans/taxonomy/term/56)

科研动态 (/zh-hans/taxonomy/term/29)

### 专题栏目

- > 毕业设计 (<http://bysj.zjgsu.edu.cn>)
- > 实验管理 (<http://scielab.zjgsu.edu.cn>)
- > 学生科技 (<http://acm.zjgsu.edu.cn>)

### 平台建设

- > 国家及省级平台 (/index.php/zh-hans/%E5%B9%B3%E5%8F%B0%E5%BB%BA%E8%AE%BE)
- > 软件项目管理平台 (<http://zjgsu.5upm.com>)

### 快速链接

- > 人才引进 (/index.php/zh-hans/%E4%BA%BA%E6%89%8D%E5%BC%95%E8%BF%9B)
- > 内部办公 (<http://10.21.11.14/cieservice/>)
- > 办事指南 (/index.php/zh-hans/%E5%8A%9E%E4%BA%8B%E6%8C%87%E5%8D%97)
- > 文件下载 (/index.php/zh-hans/%E6%96%87%E4%BB%B6%E4%B8%8B%E8%BD%BD)

### 联系方式

地址: 浙江杭州下沙高教园区学正街18号

电话: (86)0571-28008316

邮箱: [scie@zjgsu.edu.cn](mailto:scie@zjgsu.edu.cn) (<mailto:scie@zjgsu.edu.cn>)

Copyright © 1997-2021 浙江工商大学

浙公网安备 33011802000512号 (<http://www.beian.gov.cn/portal/registerSystemInfo?recordcode=33011802000512>)

登录 (/user/login)