医疗区块链环境下基于身份的格上可搜索属性签密方案

俞惠芳 [1,2]，白小平 [1]
[1] 西安邮电大学网络空间安全学院，中国西安市，710121
[2] 青海交通职业技术学院信息工程学院，中国西宁市，810003

摘要：电子医疗系统在给人们提供便利的同时，面临数据伪造和信息泄露的风险。为解决这些问题，提出一种适用于医疗区块链的基于身份的格上可搜索属性签密（BCMS-LIDSASC）方案。BCMS-LIDSASC 实现了区块链环境下去中心化和抗量子安全，可提供细粒度访问控制，同时具有可搜索性；此外，利用智能合约替代传统的可信第三方，用星际文件系统（IPFS）存储密文，缓解区块链的存储压力。相比而言，BCMS-LIDSASC 拥有更短密钥、更小存储需求和更低计算成本，有助于安全高效地管理医疗数据，可保护患者的隐私信息和确保电子医疗系统的完整性。

关键词：区块链；基于身份的可搜索属性签密；分布式存储；NTRU 格
https://doi.org/10.1631/FITEE.2300248