物联网中基于属性加密与相等性测试

姚莉沙 1 ，王尚平 1,2

(1 西安理工大学 理学院，西安 710054；2 陕西省网络计算与安全技术重点实验室，陕西 西安 710048)

摘 要：为保护资源受限的物联网设备间数据交换的安全与隐私，采用外包技术，把密文策略基于属性加密与相等性测试结合，针对物联网设备，提出一种简洁的加解密算法，并在不解密的情况下建立由授权云服务器执行的密文检测机制，从而减轻本地计算负担和实现精确解密.基于判定性 q －1 假设，证明提出的方案抗选择明文攻击，是不可区分安全的.最后，实验分析表明方案实用且有效.

关键词：物联网；基于属性加密；相等性测试；选择明文攻击

Attribute-based encryption with equality test in the internet of things

YAO Li-sha 1 ，WANG Shang-ping 1,2

(1 School of Science，Xi′an University of Technology ，Xi′an 710054，China；2 Key Laboratory of Network

Computing and Security Technology of Shaanxi Province，Xi′an 710048，China)

Abstract：In order to protect the security and privacy of data exchange between the resource-constrained Internet of Things (IoT) devices，the outsourcing technology is adopted to combine the ciphertext policy attribute-based encryption and equality test. For IoT devices，a concise encryption and decryption algorithm is proposed，as well as the ciphertext detection mechanism performed by the authorized cloud server is established without decryption, thereby alleviating the local computing burden and achieving accurate decryption. Based on the decisional q－1 assumption，it is proved that the proposed scheme resists chosen plaintext attacks and enjoys indistinguishable security. Finally，the experimental analysis shows that the scheme is practical and effective.

Key words：Internet of Things；attribute-based encryption；equality test；chosen plaintext attacks

作者简介：

姚莉沙 女，（1993-），硕士研究生.研究方向为密码理论与网络安全.E-mail:yaolishaqh@163.com.

王尚平 男，（1963-），教授，博士生导师.研究方向为数字签名与网络身份认证、密码理论与网络安全等.