|  |  |
| --- | --- |
| 1题目 | Cryptanalysis of a CP-ABE scheme with policy in normal forms |
| 分类于endnote中 | survey |
| 文章目的： | 驳倒《Efficient attribute based access control mechanism for vehicular ad hoc network》中加密方案（DNF,CDF结构的CP-ABE）在标准模型下的安全性，证明其DNF不具有CPA安全性。得出目前这类方案都只能在CNF上具有选择明文安全，而在DNF上不具备。 |
| 主要方法 | 利用选择明文攻击者的秘钥提取谕言机，提取一个sk，作为中间变量，结合已给密文的乘除操作，恢复出明文。 |
| 创新点 | 驳论； |