|  |  |
| --- | --- |
| 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； |

|  |  |
| --- | --- |
| 2题目 | How to Delegate and Verify in Public: Verifiable Computation from Attribute-based Encryption |
| 分类于endnote中 | Verify |
| 文章目的： | 建立一种ABE和可验证性计算之间的联系。提出了一个协议（public verifiable computation protocol）包含Public Delegatability和Public Verifiability两个properties。 |
| 主要方法 | 调查可验证性计算，和基于delegation的ABE方案的研究现状，找到尚未未解决的问题，分析并得出一些成果，总结两个方向，建立起一个理论(即提出一种协议) |
| 创新点 | 协议免疫“rejection problem”；delegation的预处理采用分摊外包；解耦evaluation function以提高验证计算效率。 |