|  |  |
| --- | --- |
| 1题目 | Multi-authority Attribute Based Encryption |
| 分类于endnote中 | Multi-authority |
| 文章目的： | 第一次提出一种解决multi-authority的分享方案 |
| 主要方法 | 1. 提出 global identifier (GID)，防止合谋攻击 2. 提出the central authority，来解决其他authority被收买的情况 |
| 创新点 | 1. 针对多个authority； 2. 任意个机构authority可以被收买 3. 减小authority对监管秘钥和属性的管理负担 |

|  |  |
| --- | --- |
| 2题目 | Secure threshold multi authority attribute based encryption without a central authority |
| 分类于endnote中 | Multi-authority |
| 文章目的： | 改善了multi-authority的方法，不在使用central authority.第一次提出了一个multi-authority的基于模糊身份加密，并且进一步提出基于属性的模糊加密。 |
| 主要方法 | Distributed key generation protocol (DKG) 和 joint zero secret sharing protocol (JZSS) |
| 创新点 | 1. 取消了central authority； 2. 部分机构authority可以被收买 |

|  |  |
| --- | --- |
| 2题目 | 多授权中心可验证的基于属性的加密方案 |
| 分类于endnote中 | Multi-authority |
| 文章目的： | 1. 将可验证的属性加密方案由单个授权中心推广到多个授权中心,  2. 检验出是哪个授权中心部分的密钥出错,  3. 各个授权中心在被检查出错时, 也只需要重发对应部分的信息 |
| 主要方法 | 树形结构 |
| 创新点 | 1. 方便管理秘钥. |

|  |  |
| --- | --- |
| 2题目 | Multi-authority Attribute Based Encryption Scheme with Revocation |
| 分类于endnote中 | Multi-authority |
| 文章目的： | 1. 属性可撤回 |
| 主要方法 | （还没有看完） |
| 创新点 |  |