|  |  |
| --- | --- |
| 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 |

|  |  |
| --- | --- |
| 3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. |

|  |  |
| --- | --- |
| 4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 | 1. UID（跟原来的GID没有什么区别） 2. 用一个List（）来控制被撤回的属性 3. 树形结构 |
| 创新点 | 属性可撤回 |

|  |  |
| --- | --- |
| 5题目 | Improving Privacy and Security in Multi-Authority Attribute-Based Encryption |
| 分类于endnote中 | Multi-authority |
| 文章目的： | 乱入，不是论文，是一个邀请函 |
| 主要方法 |  |
| 创新点 |  |

|  |  |
| --- | --- |
| 6题目 | Efficient Statically-Secure Large-Universe  Multi-Authority Attribute-Based Encryption |
| 分类于endnote中 | Multi-authority |
| 文章目的： | 1.任何字符串可以被当做属性  2.同一个属性可以被使用多次  3.提高效率和方案可行性 |
| 主要方法 | 1. 矩阵 2. 树形结构 3. 线性秘密分享方案   4.layering technique |
| 创新点 | 1. 取消了central authority 2. 用了program-and-cancel" techniques来证明安全性（没看懂） |

|  |  |
| --- | --- |
| 7题目 | A Framework of Multi-Authority Attribute-Based Encryption with Outsourcing and Revocation |
| 分类于endnote中 | Multi-authority |
| 文章目的： | 给出了一个具体可行的属性可撤回的和out-  Sourced（云计算）的multi-Abe架构 |
| 主要方法 |  |
| 创新点 | 1.在small-universe中可以撤回  2.通过outsource 提升效率 |

|  |  |
| --- | --- |
| 8题目 | Fully Secure Multi-authority Ciphertext-Policy  Attribute-Based Encryption without Random  Oracles |
| 分类于endnote中 | Multi-authority |
| 文章目的： | 1.阻止个人机构解密密文  2.非随机预言模型下的CP-ABE系统 |
| 主要方法 | multiple Central Authorities (CAs) and Attribute Authorities (AAs) |
| 创新点 | 1. 提高了效率 2. 非随机预言模型 |

|  |  |
| --- | --- |
| 9题目 | TR-MABE: White-Box Traceable and Revocable  Multi-authority Attribute-based Encryption and Its  Applications to Multi-level Privacy-preserving  e-Healthcare Cloud Computing Systems |
| 分类于endnote中 | Multi-authority |
| 文章目的： | 解决网络医疗数据的若干问题：   1. 负责病人的主治医生可以查看病患身体状况，还可以验证他的身份，其他医生只能查看身体状况，其他人则不能获得信息 2. 可追踪和可撤回的multi-Abe |
| 主要方法 | 1. 云计算 |
| 创新点 | 1. 减小了从机构可能的秘密泄露 2. 没有引入其他签名 |

|  |  |
| --- | --- |
| 10题目 | Provably secure unbounded multi-authority  ciphertext-policy attribute-based encryption |
| 分类于endnote中 | Multi-authority |
| 文章目的： | 解决属性规模受限的问题 |
| 主要方法 | 1. LSSS（linear secret sharing scheme） 2. Identity related和 linked attribute-related keys都会被用到 |
| 创新点 | 1.不受限制的方案  2任何参与者都可以成为AA |

|  |  |
| --- | --- |
| 11题目 | Free global ID against collusion attack on multi-authority attribute-based encryption |
| 分类于endnote中 | Multi-authority |
| 文章目的： | 1.解决Multi-authority中的合谋攻击  2.提出不适用GID的方案 |
| 主要方法 | 1. 建立Free-GID系统 |
| 创新点 | 1. formulize user action of making request for key into legality and collusion |