| 1.A Ciphertext-Policy Attribute-Based Encryption Scheme with Constant Ciphertext Length | |
| --- | --- |
| 分类于ednote中 | constant ciphertext |
| 文章目的 | 提出基于属性加密方案中固定密文长度的加密方案 |
| 主要方法 | 使用双线性对将多个属性映射到有限域下的乘法子群中以固定密文长度 |
| 创新点 | 使用多值与门构造CP-ABE方案中访问结构并完成固定密文长度 |

| 2.Constant Size Ciphertexts in Threshold Attribute-Based Encryption | |
| --- | --- |
| 分类于ednote中 | constant ciphertext |
| 文章目的 | 提出基于属性加密方案中固定密文长度的加密方案 |
| 主要方法 | 使用动态阈值公钥加密算法计算所需的值，并构造方案结构 |
| 创新点 | 提出能抵抗共谋攻击和能够承认合理解密策略的固定密文长度ABE方案 |

| 3.Attribute-based encryption schemes with constant-size ciphertexts | |
| --- | --- |
| 分类于ednote中 | constant ciphertext |
| 文章目的 | 提出了允许真实表现访问结构和固定密文长度的ABE加密方案 |
| 主要方法 | 对于每个访问结构定义普通和首要两个属性，并使这两个属性在不同的集合中，以此来构造方案 |
| 创新点 | 具有紧凑密文特征的ABE方案中，可以不管底层属性的个数 |

| 4.CP-ABE with constant-size keys for lightweight | |
| --- | --- |
| 分类于ednote中 | constant ciphertext |
| 文章目的 | 提出新的安全的CP-ABE固定密文方案让此能够广泛应用于轻量级设备中 |
| 主要方法 | 在加密过程中使用HASH函数与加密函数共同生成密文 |
| 创新点 | 使得CP-ABE方案能够广泛用于轻量级设备中 |

| 5.Computationally Efficient Expressive Key-Policy Attribute Based Encryption Schemes with Constant-Size Ciphertext | |
| --- | --- |
| 分类于ednote中 | constant ciphertext |
| 文章目的 | 构建高效的KP-ABE下的秘密共享（LSSS）方案 |
| 主要方法 |  |
| 创新点 | 在CCA和CPA标准安全下，构建高效的KP-ABE下的秘密共享方案可实现MAS（单调访问结构） |

| 6.Fully secure ciphertext policy attribute-based encryption with constant length ciphertext and faster decryption | |
| --- | --- |
| 分类于ednote中 | constant ciphertext |
| 文章目的 | 提出了具有完全安全并且能够更快解密的具有恒定密文长度的CP-ABE方案 |
| 主要方法 | 在算法构造中使用双索引，一个索引指向属性另一个指向现实中具有更好可读性的可能值 |
| 创新点 | 提出在多点传输设备中完全安全的恒定密文长度的CP-ABE方案 |

| 7.Attribute based proxy re-encryption with delegating capabilities | |
| --- | --- |
| 分类于ednote中 | delegation |
| 文章目的 | 提出了基于属性的代理重加密方案中并讨论了方案中委托性能 |
| 主要方法 | 将密钥共享技术与CP-ABE的构建相结合构造代理重加密方案 |
| 创新点 | 提出了基于属性的代理重加密 |

| 8.Circuit ciphertext-policy attribute-based hybrid encryption with verifiable delegation in cloud computing | |
| --- | --- |
| 分类于ednote中 | delegation |
| 文章目的 | 提出了在云服务器上可验证授权的基于电路密文策略的混合加密方案 |
| 主要方法 | 使用多线性映射和电路策略来构造混合加密方案 |
| 创新点 | 基于电路密文策略的混合加密 |

| 9.Traceable CP-ABE: how to trace decryption devices found in the wild | |
| --- | --- |
| 分类于ednote中 | traceable |
| 文章目的 | 提出了可追踪解密设备的CP-ABE方案 |
| 主要方法 | 给每一个用户定义一个唯一的身份索引，并且构造了两个黑盒，一个是密钥匹配黑盒一个是访问结构匹配黑盒，以此来构造我们的可追溯CP-ABE方案 |
| 创新点 | 可追踪解密设备 |

| 10.Traceable CP-ABE on prime order groups: Fully secure and fully collusion-resistant blackbox traceable | |
| --- | --- |
| 分类于ednote中 | traceable |
| 文章目的 | 提出了一个在标准模型下完全安全，完全抗共谋的可追溯的黑盒并且支持单调访问结构的CP-ABE方案 |
| 主要方法 | 在构造中使用双配对向量空间这个工具和LSSS进行密钥构造 |
| 创新点 | 这个方案是构造在素数群上的，所以它的效率更加高方案开销是O( √N） |

| 11.White-box traceable ciphertext-policy attribute-based encryption supporting flexible attributes | |
| --- | --- |
| 分类于ednote中 | traceable |
| 文章目的 | 提出了两个实用的大型CP-ABE系统中构造可追溯泄密者的白盒方案 |
| 主要方法 | 在T-LU-CPABE 方案中，在方案构造中添加用户的身份的标示，并在算法构造中增加了密钥检查步骤。而在eT-LU-CPABE这个方案中， 除了用了上面方案的构造思想外还，利用Shamir的门限方案优化追溯属性这样使得我们在step中存储的值为常数级。 |
| 创新点 | 在大型的CP-ABE系统中，白盒开销仍为常数，能够适用于多数商业设备中 |

| 12.Accountable Authority Ciphertext-Policy Attribute-Based Encryption with White-Box Traceability and Public Auditing in the Cloud | |
| --- | --- |
| 分类于ednote中 | traceable |
| 文章目的 | 通过构造一个具有白盒可追溯性和能进行公共审计的负责的权威的CP-ABE方案来解决在云服务器上CP-ABE密钥的滥用和审计的问题 |
| 主要方法 | 让用户和权威机构共同确定解密密钥，用户通过他的身份和属性获取密钥而权威机构无法得知用户获取的是哪一个密钥。 |
| 创新点 | 这个方案拥有审计的功能，并且审计性是公开的，任何人可以使用审计算法判断用户是否泄漏秘密，同时因为使用pailliar加密所以不需要存储追溯用户列表，不用额外的开销来存储维护用户列表。 |

| 13.Ciphertext-policy attribute-based encryption | |
| --- | --- |
| 分类于ednote中 | CP-ABE |
| 文章目的 | 提出了一个基于密文策略属性的加密的方案，允许一种新类型的加密访问控制，其中用户的私钥由一组属性指定，并且加密方加密数据可以对这些属性指定策略，指定哪些用户能够解密，方案允许策略表示为任何单调的树访问结构，并且抵抗共谋攻击。 |
| 主要方法 | 使用树的结构来构造相对对应的访问结构，其中树的每个叶子节点表示对应的属性 |
| 创新点 | 构造访问结构来限制能够进行解密的用户 |

| 14.Provably secure ciphertext policy ABE | |
| --- | --- |
| 分类于ednote中 | CP-ABE |
| 文章目的 | 提出了一个可靠安全的CP-ABE方案 |
| 主要方法 | 将正负属性的AND门作为方案中的访问结构，在这个更简单的设置中可以获得在标准复杂性假设下非常安全的高效方案，应用Canetti-Halevi-Katz技术，使用一次性签名获得选择的密文（CCA）安全扩展。 |
| 创新点 | 这是CP-ABE的第一个正式的CCA安全证明。 |

| 15.Bounded ciphertext policy attribute based encryption | |
| --- | --- |
| 分类于ednote中 | CP-ABE |
| 文章目的 | 提出了可以构造支持由具有阈值门作为其节点的有界大小访问树表示的访问结构的基于属性加密方案。 |
| 主要方法 | 访问树的大小的界限在系统建立时被选择并且由元组（d，num）表示，其中d表示访问树的最大深度，num表示每个非最大访问树的最大数目。任何满足这些大小上限的访问树都由加密器动态地选择。同时这个方案为访问结构树中可能出现的每个位置引入每个属性的多个“副本”。 |
| 创新点 | 这个方案中对于非单调访问策略，方案设计的结构可以支持具有有界多项式大小的任何访问公式。 |

| 16.Provably secure and efficient bounded ciphertext policy attribute based encryption | |
| --- | --- |
| 分类于ednote中 | CP-ABE |
| 文章目的 | 提供更快的加密/解密算法和缩短的密文大小来改进Goyal等人（GJPS）设计的CP-ABE的方案 |
| 主要方法 | 访问树转换为规范形式，并且直接将由发送方选择的（d，c）边界访问树映射到（d，c），消除了通过添加非叶节点将所有叶节点拉到最深级别的冗余步骤，从而降低计算成本，增加运算效率 |
| 创新点 | 与前面的CP-ABE方案比较在安全性不变的条件下效率更高效了 |

| 17.Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization | |
| --- | --- |
| 分类于ednote中 | CP-ABE |
| 文章目的 | 文章提出了一种新的方法，用于在具体和非交互式假设的标准模型中从一组通用的访问结构中实现CP-ABE系统。密文开销和加密时间都是O（n），同时方案中解密时间随节点数量而变化。 |
| 主要方法 | 密文根据访问控制LSSS矩阵M在不同属性之间分配密文加密指数的分享密钥。  用户的私钥与属性集合S相关联，用新选择的指数t随机化每个密钥，在解密期间，每个分享的密钥将乘以指数中的因子t |
| 创新点 | 与其他的CP-ABE方案相比较而言在效率上有所提升 |

| 18.A ciphertext policy attribute-based encryption scheme without pairings | |
| --- | --- |
| 分类于ednote中 | CP-ABE |
| 文章目的 | 提出了一种没有配对的选择性安全密文策略的CP-ABE方案 |
| 主要方法 | 将每个（正或负）属性与矩阵相关联，实际上矩阵通过网格加密中唯一的定义格子。因此，用户的“身份”唯一地定义一组网格。为具有属性集合S的用户生成秘密密钥时，使用由S确定的网格集合通过利用这些网格的陷门（即，短基）来共享用于加密的公共向量，并且秘密S中的每个属性的密钥是由该属性确定的网格（由网格定义的陪集）中的短向量，以此来作为方案的构造思想 |
| 创新点 | 第一个提出没有配对的选择性安全密文策略的CP-ABE方案 |

| 19.Extending the ciphertext-policy attribute based encryption scheme for supporting flexible access control | |
| --- | --- |
| 分类于ednote中 | CP-ABE |
| 文章目的 | 提出基于现有CP-ABE方案的扩展CP-ABE（ECP-ABE）方案。 ECP-ABE方案可以表示由除了AND，OR和阈值运算符之外的如NOT，<，≤，>，≥运算符的算术比较和逻辑表达式所表示的任何访问策略 |
| 主要方法 | 在ITHJ09方案的基础上通过引入扩展叶节点，增强了CP-ABE的访问树以支持所有种类的逻辑和算术比较运算符。用运算符节点替换原始叶节点，并给它两个孩子，称其为属性名节点和属性值节点。通过移除属性名称/值节点，将扩展树转换为等效标准树，将运算符节点转换为标准叶子节点然后将由扩展叶节点描述的属性表达式作为扩展属性分配给标准叶节点。 |
| 创新点 | 在原有的CP-ABE方案上扩展了其访问策略，使其能够更加灵活的使用实际生活中 |

| 20.Poster: Efficient ciphertext policy attribute based encryption under decisional linear assumption | |
| --- | --- |
| 分类于ednote中 | CP-ABE |
| 文章目的 | 提出一种新的基于密文策略属性的加密方案，其中访问结构由具有通配符的AND门限定。这个方案中使用单个元素来表示一个属性，同时该方案也实现恒定大小的密文和恒定数量的解密操作 |
| 主要方法 | 使用属性的“位置”做匹配。将访问结构中定义的所有正，负和通配符属性的索引设置为三组。通过使用Vietet的公式，解密者可以删除所有通配符位置，并且解密成功 |
| 创新点 | 提出一种仅使用一个元素来表示一个属性的新颖构造。 |