| 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 |

| 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 |

| 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 |

| 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 |

| 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） |

| 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 |

| 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 |

| 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 |

| 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 |

| 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 |  |
| 主要方法 |  |
| 创新点 |  |

|  | |
| --- | --- |
| 分类于ednote中 |  |
| 文章目的 |  |
| 主要方法 |  |
| 创新点 |  |

|  | |
| --- | --- |
| 分类于ednote中 |  |
| 文章目的 |  |
| 主要方法 |  |
| 创新点 |  |

|  | |
| --- | --- |
| 分类于ednote中 |  |
| 文章目的 |  |
| 主要方法 |  |
| 创新点 |  |

|  | |
| --- | --- |
| 分类于ednote中 |  |
| 文章目的 |  |
| 主要方法 |  |
| 创新点 |  |

|  | |
| --- | --- |
| 分类于ednote中 |  |
| 文章目的 |  |
| 主要方法 |  |
| 创新点 |  |

|  | |
| --- | --- |
| 分类于ednote中 |  |
| 文章目的 |  |
| 主要方法 |  |
| 创新点 |  |

|  | |
| --- | --- |
| 分类于ednote中 |  |
| 文章目的 |  |
| 主要方法 |  |
| 创新点 |  |

|  | |
| --- | --- |
| 分类于ednote中 |  |
| 文章目的 |  |
| 主要方法 |  |
| 创新点 |  |

|  | |
| --- | --- |
| 分类于ednote中 |  |
| 文章目的 |  |
| 主要方法 |  |
| 创新点 |  |

|  | |
| --- | --- |
| 分类于ednote中 |  |
| 文章目的 |  |
| 主要方法 |  |
| 创新点 |  |