|  |  |
| --- | --- |
| 1题目 | Efficient and Provable Secure Ciphertext-Policy  Attribute-Based Encryption Schemes |
| 分类于endnote中 | Efficient |
| 文章目的： | 提出了一个高效的访问策略为“∧”、“∨”的CP-ABE方案，并进一步提出了高效的访问策略为“of”、“∧”、“∨”三种操作符的CP-ABE方案。 |
| 主要方法 | 在“∧”、“∨”方案中采用Unanimous Consent Control by Modular Addition Scheme（模块化加法方案的一致同意控制）；将树结构中所以叶子节点统一按升序编号j，加密时对应叶节点（为属性值，为shamir秘密分享的部分值），解密时密钥，这样就可以直接双线性配（使用一次）对来计算shamir秘密分享的秘密值，不用再像BSW的CP-ABE中两次配对然后相除。 |
| 创新点 | 第一个方案比Cheung, L., Newport, C.的Provably secure ciphertext policy ABE方案具有更高的效率，第二个方案比Bethencourt, J., Sahai, A., Waters, B.的Ciphertext-Policy Attribute-Based Encryption方案具有更高的效率。 |

|  |  |
| --- | --- |
| 2题目 | Generic and Efficient Constructions of Attribute-Based Encryption with Verifiable Outsourced Decryption |
| 分类于endnote中 | Efficient |
| 文章目的： | 提出了CPA安全和RCCA安全的可验证外包解密的ABE系统的通用结构，并实现了一个在标准模型下CPA安全的具体实例。 |
| 主要方法 | 在CPA安全的可验证外包解密的ABE系统的通用结构中，采用一个commitment方案来验证外包解密的正确性；在RCCA安全的通用结构中，在commitment方案的基础上，采用一个 encapsulation （封装）方案和一个massage authentication code来实现。 |
| 创新点 | 与现有的方案相比，文中的CPA安全结构中密文更加简短，计算消耗更低；此外，RCCA安全结构中的技术可以被用在实现通用的CCA安全的ABE中。 |

|  |  |
| --- | --- |
| 3题目 | Attribute Based Encryption with Direct Efficiency Tradeoff |
| 分类于endnote中 | Efficient |
| 文章目的： | 提出了第一个fully secure unbounded ABE（完全安全的无限制ABE）方案，在这个方案中，密文大小和密钥大小可以直接进行Tradeoff（权衡）。 |
| 主要方法 | 在Attrapadung, N.: Dual system encryption via doubly selective security中提到的Doubly Spatial Encryption (KP-DSE) scheme基础上，将对应于密文中的t个属性划分为t/d个不相交的子集，然后将每个子集编码到KP-DSE中的仿射子空间中，利用KP-DSE实现密文大小为O(t/d)，通过调整d实现Tradeoff。 |
| 创新点 | 实现密文大小和密钥大小之间的Tradeoff |

|  |  |
| --- | --- |
| 4题目 | Turing Machines with Shortcuts: Efficient Attribute-Based Encryption for Bounded Functions |
| 分类于endnote中 | Efficient |
| 文章目的： | 为有界多栈的deterministic pushdown automata (DPDAs)和Turing machines提出了一个ABE方案的直接构造。 |
| 主要方法 | 主要方法源自Boyen, X., Li, Q.: Attribute-based encryption for finite automata from LWE中的LWE-based ABE方案。 |
| 创新点 | 文中的方案具有“input-specific” decryption runtime的特点，即解密时间由属性内容决定；如果一个机器在某个特定输入时过早停止时，它的执行可以中断。 |

|  |  |
| --- | --- |
| 5题目 | Generic Constructions for Chosen-Ciphertext Secure Attribute Based Encryption |
| 分类于endnote中 | Generic |
| 文章目的： | 提出了将CPA安全的ABE转换为标准模型下CCA安全ABE的通用转换。 |
| 主要方法 | 通用转换包括三个部分的结合：1、CP-ABE或者KP-ABE；2、最初的ABE方案中处理小属性域或者大属性域；3、采用已有的delegatability（代理）方法还是新的可验证性方法。 |
| 创新点 | 更加通用的将CPA安全的ABE方案转换为CCA安全方案。 |

|  |  |
| --- | --- |
| 6题目 | Accountable authority key policy attribute-based encryption |
| 分类于endnote中 | KP-ABE |
| 文章目的： | 提出了一个accountable authority（负责任的授权中心）的KP-ABE方案 |
| 主要方法 | 用一个(id*,* *T* )配对来确定一个用户，*T*是访问树，id是用户身份，然后将一个秘密值分成两个部分，一个用来产生与身份相关的部分密钥，另一个用来产生与访问树相关的部分密钥，其解密能力与id不相关（一个额外的元素引入密文中来实现），将Libert B, Vergnaud D. Towards black-box accountable authority IBE with short ciphertexts and private keys中的弱黑箱跟踪机制扩展到本文中的方案里。 |
| 创新点 | 与Li J, Ren K, Kim K. A2BE: accountable attribute-based encryption for abuse free access control.相比，本文的方案不需要一个高层次的秘密，同时也非常高效；在标准模型下安全，基于modified bilinear decisional Diffie-Hellman (mBDDH) assumption。 |

|  |  |
| --- | --- |
| 7题目 | A general transformation from KP-ABE to searchable encryption |
| 分类于endnote中 | KP-ABE |
| 文章目的： | 提出了将ABE转换成Attribute Based Encryption with Keyword Search (ABEKS)方案的通用方式，并给出了一个具体的attribute private的KP-ABE方案以及基于这个方案实现ABEKS方案。 |
| 主要方法 | 引入A. De Caro, V. Iovino, G. Persiano, Fully secure anonymous HIBE and secret-key anonymous IBE with short ciphertexts的技术来实现弱的的匿名特性，即attribute private ABE方案。  首先将加密数据文件作为ABEKS的明文，加密者用数据文件的关键字进行加密，搜索者会构建一个与搜索策略相关的密钥，第三方服务器用这个密钥进行解密得到匹配搜索策略的原密文。 |
| 创新点 | 允许多用户针对远程数据执行一个灵活的搜索 |

|  |  |
| --- | --- |
| 8题目 | Practical Direct Chosen Ciphertext Secure Key-Policy Attribute-Based Encryption  with Public Ciphertext Test |
| 分类于endnote中 | KP-ABE |
| 文章目的： | 提出了一个在标准模型下实现CCA2语义安全的直接KP-ABE方案 |
| 主要方法 | 本文中的方案结构是基于Rouselakis, Y., Waters, B.: Practical constructions and new proof methods for large universe attribute-based encryption中的KP-ABE系统，该KP-ABE系统包含了一个Decision Diffie-Hellman (DDH) ciphertext tuple，并允许使用任意属性。  本文中的方案还添加了一个on-the-fly dummy attribute用于解密过程中的密文验证。此外，还利用Chameleon hash解决安全性证明过程中的不能提前知道挑战on-the-fly dummy attribute的问题。 |
| 创新点 | 与文中方案里的基础CPA安全的KP-ABE方案相比，仅仅引入了一个Chameleon hash的代价；并允许进行公共密文有效性测试；与现有的将Chameleon hash运用于签名不同，本文举例说明了Chameleon hash在加密方案中的结构和安全性证明过程中的应用。 |

|  |  |
| --- | --- |
| 9题目 | Key-Policy Weighted Attribute Based Encryption for Fine-Grained Access Control |
| 分类于endnote中 | KP-ABE |
| 文章目的： | 提出了一个Key-Policy Weighted Attribute based Encryption (KP-WABE)，该方案中属性都有一个权值，对应于该属性在系统中的重要性。 |
| 主要方法 | 在这个结构中，属性被假定分成n个链，每一个链中代表着对应于一个属性的不同权值属性。  要成功解密密文，需要密文中包含的加权属性集满足密钥中包含的加权访问树。 |
| 创新点 | 文中的KP-WABE方案可以简单的转成传统的KP-ABE方案，当所有的属性拥有相同的权值。  使用l-th bilinear Diffie-Hellman inversion assumption给出了安全性证明；比传统的ABE方案相比，在实用性方面有了显著的改进。 |

|  |  |
| --- | --- |
| 10题目 | Adaptable key-policy attribute-based encryption with time interval |
| 分类于endnote中 | KP-ABE |
| 文章目的： | 介绍了一个扩展KP-ABE概念：adaptable key-policy attribute-based encryption with time  interval (KP-TIABE)；并展示了一个具体的方案。 |
| 主要方法 | 方案的实现是基于一个代数组合：Goyal et al. (2006)的KP-ABE方案、Lai et al.(2014)的自适应CP-ABE方案和Paterson and Quaglia (2010)的TSE方案。在adaptable KP-TIABE中，用户从密钥生成中心接收一个带访问策略的私钥；一个非完全信任的时间服务器广播全部系统公共参数以及每一个时间间隔广播一个时刻密钥；另一个非完全信任的自适应服务器可以将一个在特定解密时间间隔的密文转为在另一个特定时间间隔下的密文，这两个密文对应于同一明文，同时这个自适应服务器不会得到明文的任何信息。 |
| 创新点 | 更加实用；可以调整对应于密文中的解密时间间隔，在动态系统环境下更具有吸引力。 |

|  |  |
| --- | --- |
| 11题目 | Collaborative KP-ABE for Cloud-Based Internet of Things Applications |
| 分类于endnote中 | KP-ABE |
| 文章目的： | 提出了一种方法将KP-ABE应用到基于云计算的物联网应用中。 |
| 主要方法 | 这篇文章主要关注加密原语，它通常被资源受限的节点最频繁的调用。主要思路是利用云服务器的计算能力和存储能力以及物联网的异构性将高昂代价的操作代理给资源受限低的邻近节点（加密机的邻近节点）。 |
| 创新点 | 利用云服务器的能力执行KP-ABE中的繁重操作 |

|  |  |
| --- | --- |
| 12题目 | An Efficient KP-ABE Scheme for Content Protection in Information-Centric Networking |
| 分类于endnote中 | KP-ABE |
| 文章目的： | 提出了一个高效的key-policy ABE with fast key generation and decryption (FKP-ABE)。 |
| 主要方法 | 在密钥产生阶段，FKP-ABE避免了指数运算，仅仅需要对访问策略中的每个属性进行乘法/除法运算。在解密阶段,通过将配对操作转换为指数运算操作，实现了配对操作次数减少至一次。此外，展示了一个视频点播系统框架，在这个框架中，将FKP-ABE合成到了 Information-Centric Networking（信息中心网络）结构中，对多媒体内容实现了独立保护，终端用户可以通过其轻量级设备获取或者访问其请求的内容。 |
| 创新点 | 提高了应用在Information-Centric Networking中的ABE的效率，综合效率比现有的KP-ABE方案都要高。基于DBDH假设证明了方案的CPA安全性。 |

|  |  |
| --- | --- |
| 13题目 | Dual-Policy Attribute Based Encryption |
| 分类于endnote中 | policy or access |
| 文章目的： | 提出了一个新的ABE变种：Dual-Policy ABE。即一种将KP-ABE和CP-ABE结合起来的方案。 |
| 主要方法 | 文中的方案是基于Waters, B.: Ciphertext-Policy Attribute-Based Encryption中的CP-ABE方案和Goyal, V., Pandey, O., Sahai, A., Waters, B.: Attribute-based encryption for finegrained access control of encrypted data中的KP-ABE方案的一个代数组合。加密者可以将代表数据本身的属性和指定哪些人能解密的访问策略结合到密文中，用户的私钥中也同时包含代表用户认证信息的属性以及指定用户可以解密哪些密文的访问策略。 |
| 创新点 | 1. 一个结合KP-ABE和CP-ABE新的ABE方案；（2）密钥代理：允许将上面提到的KP-ABE中的密钥或者CP-ABE中的密钥代理到本文中DP-ABE方案；（3）单一策略模式的特点：   允许用户使用DP-ABE的密钥就像在动态的使用普通KP-ABE方案和CP-ABE方案。 |

|  |  |
| --- | --- |
| 14题目 | Mediated Ciphertext-Policy Attribute-Based Encryption and Its Application |
| 分类于endnote中 | policy or access |
| 文章目的： | 提出了一个mediated Ciphertext-Policy Attribute-Based Encryption（mCP-ABE），即扩展普通CP-ABE让其能够进行即时的属性撤销。并展示了如何采用这个方案安全地管理个人健康记录。 |
| 主要方法 | 在mCP-ABE方案中，私钥被划分成两个分享部分，一部分分享给mediator，另一部分分享给用户。当用户想解密数据时，需要先联系mediator取得一个解密令牌。mediator中存有一个属性撤销列表，并且拒绝给撤销的属性分配解密令牌。没有这个解密令牌用户则无法完成解密，所以属性撤销也就隐含地完成了。 |
| 创新点 | 即时的属性撤销并给出了现实中具体应用 |

|  |  |
| --- | --- |
| 15题目 | Duality in ABE: Converting Attribute Based Encryption for Dual Predicate and Dual Policy  via Computational Encodings |
| 分类于endnote中 | policy or access |
| 文章目的： | 提出了一个通用的转换，可以将具有任意判定的ABE方案转换成其对偶判定的ABE方案。  此外还提出了将ABE方案转换成Dual-policy ABE的通用方法。 |
| 主要方法 | 本文回顾了Attrapadung, N.: Dual system encryption via doubly selective security[1]，并且证明了[1]中的转换保留了编码的计算安全性。因此将[1]中转换应用到  [1]中的KP-DSE马上就获得了第一个完全安全的CP-DSE。 |
| 创新点 | 为ABE方案构建了其对偶判定的完全安全的ABE方案。提出了一个通用转化：将普通ABE方案转换成Dual-policy ABE（双重策略ABE）。 |

|  |  |
| --- | --- |
| 16题目 | An effective ECC-based user access control scheme with attribute-based encryption for wireless  sensor networks |
| 分类于endnote中 | policy or access |
| 文章目的： | 在hierarchical wireless sensor network（HWSN）中，利用ABE提出了一个新的基于password的用户访问控制方案。 |
| 主要方法 | 在这个方案中，一个外部用户由HWSN中的Base Station（BS）和集群的群主在特定的访问权限下进行认证。在认证成功之后，集群的群主按照用户的请求使用ABE的方法发送加密的实时数据。只有被认证的用户并拥有正确的访问权限才能恢复出明文。 |
| 创新点 | 一个合法的用户可以在任何时间改变password而不需要与BS联系；与现有方案相比，新节点的动态加入更有效率；支持匿名用户属性；在通信和计算方面，本方案更有效率。 |

|  |  |
| --- | --- |
| 17题目 | Scalable Access Policy for Attribute Based Encryption in Cloud Storage |
| 分类于endnote中 | policy or access |
| 文章目的： | 提出了一个叫做block Linear Secret Sharing Scheme (LSSS) 矩阵的访问策略。 |
| 主要方法 | 节点矩阵是一个特殊的LSSS矩阵，Nikov, V., Nikova, S.: New monotone span programs from old.中的定理提供了一个有效的方式来建立block LSSS矩阵（节点矩阵集合的复合矩阵）。 |
| 创新点 | 提供了一个通用的方法来描述作为访问策略的block LSSS矩阵，能实现高扩展性；  引入mask matrix的概念来提高block LSSS矩阵的灵活性和安全性（隐藏策略结构）；  为block LSSS矩阵提供四种管理功能，能够处理任何类型的策略更新。 |

|  |  |
| --- | --- |
| 18题目 | Rebuttal to “Comments on ‘Control Cloud Data Access Privilege and  Anonymity With Fully Anonymous Attribute-Based Encryption”’ |
| 分类于endnote中 | policy or access |
| 文章目的： | 处理Comments on ‘Control Cloud Data Access Privilege and Anonymity With Fully Anonymous Attribute-Based Encryption’中提到的一个缺陷。 |
| 主要方法 | 首先汇总Control Cloud Data Access Privilege and Anonymity With Fully Anonymous Attribute-Based Encryption中发现的缺陷，这个缺陷导致系统主密钥的泄露，然后通过阻止权威机构发送所有的单个给密钥请求者。 |
| 创新点 | 对之前的文章中出现的缺陷进行改进 |