|  |  |
| --- | --- |
| 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。 |