|  |  |
| --- | --- |
| 1题目 | Cryptanalysis of a CP-ABE scheme with policy in normal forms |
| 分类于endnote中 | survey |
| 文章目的： | 驳倒《Efficient attribute based access control mechanism for vehicular ad hoc network》中加密方案（DNF,CDF结构的CP-ABE）在标准模型下的安全性，证明其DNF不具有CPA安全性。得出目前这类方案都只能在CNF上具有选择明文安全，而在DNF上不具备。 |
| 主要方法 | 利用选择明文攻击者的秘钥提取谕言机，提取一个sk，作为中间变量，结合已给密文的乘除操作，恢复出明文。 |
| 创新点 | 驳论； |

|  |  |
| --- | --- |
| 2题目 | How to Delegate and Verify in Public: Verifiable Computation from Attribute-based Encryption |
| 分类于endnote中 | Verify |
| 文章目的： | 建立一种ABE和可验证性计算之间的联系。提出了一个协议（public verifiable computation protocol）包含Public Delegatability和Public Verifiability两个properties。 |
| 主要方法 | 调查可验证性计算，和基于delegation的ABE方案的研究现状，找到尚未解决的问题，分析并得出一些成果，总结两个方向，建立起一个理论(即提出一种协议) |
| 创新点 | 协议免疫“rejection problem”；delegation的预处理采用分摊外包；解耦evaluation function以提高验证计算效率。 |

|  |  |
| --- | --- |
| 3题目 | Comparative Study of Attribute Based Encryption  Techniques in Cloud Computing |
| 分类于endnote中 | Survey |
| 文章目的： | 对比各种属性基加密方案的各种实际性能（如Rejection Rate） |
| 主要方法 | 在网站上搭建基于美国国家标准与技术研究院标准的测试平台 |
| 创新点 | 做了一个用于实际的实验 |

|  |  |
| --- | --- |
| 4题目 | Directly revocable key-policy attribute-based encryption  with verifiable ciphertext delegation |
| 分类于endnote中 | Verify |
| 文章目的： | 建立一个KP-ABE变种加密体制，这种体制具有直接撤销授权和代理撤销的可验证性功能 |
| 主要方法 | ABE用于数据加密，IDE用于撤销授权，密文分割成数据部分和授权（身份）部分，解除数据和授权的耦合 |
| 创新点 | 把IDE泛ABE化，使对ABE的访问控制的操作（加密解密）能够用于IDE,并实现撤销。  把密文分割成数据部分和授权部分，分开处理，使得撤销后，不影响未撤销的用户。  利用二元树的特征完成了针对代理撤销第三方的可验证的设计 |
| 5题目 | Defending Against Key Abuse Attacks in  KP-ABE Enabled Broadcast Systems |
| 分类于endnote中 | Secure function |
| 文章目的： | 建立一个能够追踪秘钥滥用源的KP-ABE方案 |
| 主要方法 | 利用*V. Goyal, O. Pandey,* *A. Sahai, and B. Waters, “Attribute-based encryption forfine-grained access control of encrypted data,” in CCS ’06, 2006* 中的KP-ABE加密体制和*D. Boneh, A. Sahai, and BrentWaters, “Fully collusion resistant traitor tracingwith short ciphertexts and private keys,” in* *EUROCRYPT’06. London, UK:Springer-Verlag, 2006*中的隐藏策略加密体制，把其分别作为该方案的主干部分和追踪部分，结合在一起，实现追踪秘钥滥用源的KP-ABE方案，继承了源方案对应的DBDH,DL安全性 |
| 创新点 | 把IDE泛ABE化，即：使“身份”扮演访问结构中“属性”的角色。 |
| 效率 | 密文、秘钥长度和身份空间n呈线性关系。 |

|  |  |
| --- | --- |
| 6题目 | Attribute-Sets: A Practically Motivated Enhancement to  Attribute-Based Encryption |
| 分类于endnote中 | others |
| 文章目的： | 建立一个支持属性用集合来表示的CP-ABE方案，并实现了用户有限制的结合自己的属性进行解密的功能。 |
| 主要方法 | 把*Bethencourt, J., Sahai, A., Waters, B.: Ciphertext-Policy Attribute-Based Encryption. In: IEEE Symposium on Security and Privacy (2007)*中用一个值表示属性推广到用集合来表示属性。在抗碰撞性上，模仿上述文献，在属性上添加一个随机值，此外在用户身份上也添加一个随机值，实现用户有限制的结合自己的属性进行解密，且可以抵抗不同用户结合各自的属性解密。 |
| 创新点 | 实现了新的功能，相较于传统CP-ABE，有更多的灵活性和实用性。 |

|  |  |
| --- | --- |
| 7题目 | Arbitrary-State Attribute-Based Encryption with Dynamic Membership |
| 分类/出处 | Others  IEEE TRANSACTIONS ON COMPUTERS |
| 文章目的： | 建立一个支持任意属性状态（属性不仅只有两个状态—有或者无—）和关系动态管理的ABE方案 |
| 主要方法 | 1. 属性值之间，属性内容之间的抗碰撞性，通过引入对应个数的随机数来实现。 2. 用户加入、用户撤销、属性更新是通过更新公钥来实现，具体来讲：加入、撤销属性内容和属性值以及加入、撤销用户身份，会引入或生成对应数量的随机值，对这些随机值的处理使之能够对属性内容、属性值添加或剔除，最终提现到公钥上（所有操作）、私钥上（用户加入、属性更新）。 |
| 创新点 | 1、属性集合设置。类似于文章6。即把属性划分成内容和值。一个内容可以有多个值，一个用户又可以有多个内容。  2、引入登记、离开、更新步骤。实现用户加入、用户撤销、属性更新（关系动态管理）功能。  3、基于DBDH的CCA安全。 |

|  |  |
| --- | --- |
| 8题目 | Privacy-Aware Attribute-Based Encryption with User Accountability |
| 分类/出处 | Others |
| 文章目的： | 建立一个具有黑盒追踪、隐藏策略功能的CP-ABE方案 |
| 主要方法 | 1、策略隐藏。在特定访问结构下，把属性通过H函数隐藏。（策略隐藏和密文不可验证是等价的）  2、黑盒追踪。在隐藏策略方案基础上增加了身份加密机制。 |
| 创新点 | 1. 公钥为常数。 2. 密文长度为0（logN）。   3、第一个实现秘钥滥用追责的。 |

|  |  |
| --- | --- |
| 9题目 | Extended Attribute Based Encryption for Private  Information Retrieval |
| 分类/出处 | Others |
| 文章目的： | 基于Layouni,M.: Acredited symmetrically private information retrieval. In Miyaji, A., Kikuchi, H., Rannenberg, K., eds.: IWSEC. Volume 4752 of Lecture Notes in Computer Science., Springer (2007) 262-277 中的ASPIR方案，建立一个多权威属性基加密方案。方案能够限制授权机构，使其只能发送能够让接收者解密的指定加密数据。 |
| 主要方法 | 1、把授权者对接收者的签名作为方案的属性。仅当接受者获得满足访问结构的来自授权者的签名，才能解密。从而限制和控制了授权者。  2、利用ASPIR方案。接收者访问指定数据时，发送ASPIR请求到授权者，授权者发送带有标志的接收者能够解密（授权签名满足访问结构）的密文给接收者。没有带有标志的签名无效，所以授权者无法发送可被接收者解密的其他密文。 |
| 创新点 | 不用在方案建立时分配一个永久私钥给接收者，便于撤销和实现实时性（原因是属性集合不是设置在私钥上，而是设在授权者的签名上）。 |