|  |  |
| --- | --- |
| 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）。 |

|  |  |
| --- | --- |
| 10题目 | Attribute-Based Encryption with Break-Glass |
| 分类/出处 | Others |
| 文章目的： | 在分布式ABE方案的基础上增加一个break-glass功能：即在紧急情况下通过改变访问控制策略来访问数据。 |
| 主要方法 | 不是直接把break-glass嵌入到ABE方案中，而是通过权威对申请者的身份验证来实现。 |
| 创新点 | 增添新的功能（break-glass）。且有如下特性：   1. 多层次break-glass。 2. 生成记录使用break-glass的日志。 |

|  |  |
| --- | --- |
| 10题目 | Fully Secure Functional Encryption: Attribute-Based Encryption and (Hierarchical) Inner Product Encryption |
| 分类/出处 | Others |
| 文章目的： | 建立一个full安全的ABE方案；建立一个full安全的谓词加密方案 |
| 主要方法 | 1. 兼容多个属性。每个属性最多重复使用k次，每个实际属性转换为k个方案中的属性。 2. 全安全性。群选用N=p1p2p3合数群；引入半功能密文秘钥；挑战游戏从真实方案逐步过渡到全半功能秘钥方案，使得敌手无法得到有用的信息。 3. 利用正交空间的向量正交特性，构造PE方案。 |
| 创新点 | 1. 为了兼容多次出现同一属性，该文进行了相应的转换。 2. 第一次构造了全安全性的加密方案。 3. Full安全的谓词加密方案构造。 |

|  |  |
| --- | --- |
| 11题目 | Implementing Attribute-Based Encryption in Web Services |
| 分类/出处 | Others |
| 文章目的： | 把CP-ABE方案应用到网页服务器中。 |
| 主要方法 | 用代码实现CP-ABE方案的嵌入，并计算时间表征方案性能，并与传统的保密方案进行对比。 |
| 创新点 | ABE应用 |

|  |  |
| --- | --- |
| 12题目 | Efficient and Secure Group Key Management Based on EBS and Attribute Encryption |
| 分类/出处 | Others |
| 文章目的： | 把CP-ABE方案应用到EBS系统，使EBS系统具有抗碰撞性，并使其比传统EBS系统性能更好。 |
| 主要方法 | 把EBS系统的administrative key作为属性，访问结构为tree，叶子节点为属性，叶子节点的父节点为用户ID。并讨论系统建立，用户撤销等情况在此方案ABE层次下的操作。 |
| 创新点 | ABE应用 |

|  |  |
| --- | --- |
| 13题目 | Enhancing Attribute-Based Encryption with Attribute Hierarchy |
| 分类/出处 | Others |
| 文章目的： | 1、形式化提出HABE  2、证明了树形分层ABE的安全性。  3、验证了提出的HABE的高效。 |
| 主要方法 | 1. 定义树形HABE，与fuzz-ABE不同的是每个节点均代表一个属性。n个树形结构代表n个分层。每个树形结构中距离根节点的远近代表优先级的高低，若低优先级树形能符合解密条件，则高优先级树形也符合解密条件。当用户属性在n个结构中持有不少于d（门限值）个时，才能解密。      1. 构造私钥时，选定一个优先级属性，高于该优先级且从根节点来的路径经过该节点的属性，均作处理，成为私钥的一部分。 2. 树形结构之间采用门限共享方式，通过门限值d连接起来。 |
| 创新点 | 形式化提出HABE并证明了其安全性；效率相比原ABE方案有所提高 |

|  |  |
| --- | --- |
| 14题目 | 属性基加密机制 |
| 分类/出处 | Others |
| 文章目的： | 对ABE加密体制研究，做一个综述。 |
| 主要方法 | C:\Users\xulei\Desktop\IMG_20161023_231409.jpg |

|  |  |
| --- | --- |
| 15题目 | Flexible Attribute-Based Encryption |
| 分类/出处 | Others |
| 文章目的： | 1、为了实现ABE的灵活性，本文在原有CP-ABE方案基础上，增加一个“loose”功能：把一个策略下的加密信息（密文）转移到另一个策略下加密。且满足：转移过程不知道明文；转移过程不需要原策略对应的秘钥且（区别于代理重加密）且与策略和密文无关；转移后密文仅当属性满足转移后策略方可解密。  2、实现和原ABE方案相同的安全性。 |
| 主要方法 | 1. 在setup阶段额外生成了一个陷门信息，用来重加密密文。 2. 安全性证明时，引入loose key 不可区分，保证了在转移时不知道明文；引入loose operation 不可区分，保证了在转移后的密文和转移前不可区分（即不知道让敌手不知道是否进行了loose操作） |
| 创新点 | 相较于代理重加密，该文重加密的方式比较特别：不用原加密的私钥，而是在系统建立时生成陷门信息来完成重加密。这样的设计使之在效用上与代理重加密区分开来。 |

|  |  |
| --- | --- |
| 16题目 | An Attribute-Based Encryption Scheme Secure Against Malicious KGC |
| 分类/出处 | Others |
| 文章目的： | 建立一个ABE方案能够抵御恶意KGC(解决秘钥托管问题)，同时使其公钥、密文长度和原ABE方案相当。 |
| 主要方法 | 1. 引入新的第三方dealer参与到秘钥生成中来。 2. 具体来讲，同KGC生成秘钥方式类似，引入多项式隐藏秘密x，把KGC秘密y和dealer秘密y嵌入到密文中。 |
| 创新点 | 解决秘钥托管问题，且使方案公钥、密文长度和原ABE方案相当。相较于多权威，优于效率（通信花销）。 |

|  |  |
| --- | --- |
| 17题目 | Multi-user Attribute Based Searchable Encryption |
| 分类/出处 | Others |
| 文章目的： | 把ABE和可搜索加密方案结合起来，实现可搜索加密方案的细粒度访问 |
| 18题目 | Scalable and Secure Sharing of Personal Health Records in Cloud Computing Using Attribute-Based Encryption |
| 分类/出处 | Others  EEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS |
| 文章目的： | 利用ABE加密体制建立一套灵活、安全的个人健康记录系统。ABE方案需实现便捷的秘钥管理、灵活的访问控制、高效的秘钥撤销 |
| 主要方法 | 根据实际应用需要，把对象分为两部分。一部分是私人user，另一部分是public user。对加密信息的权限分别为：有限制的读；有限制的写和无限制的读（已授权）。分别对应KP-ABE和CP-ABE(外加基于时间间隔写权限的签名)。具体   1. 秘钥管理。私人user数量少，一般不存在秘钥管理的问题；Public user采用多权威属   性加密（门限方案）。   1. 访问控制。对于私人user，KP-ABE,其私钥的访问结构由数据拥有者生成，因此可以访   问加密数据的类型（属性）；对于public users，CP-ABE，user的属性由多个  权威机构生成，结合起来的属性集合用来满足加密数据的数据结构，因此  可以读到加密数据全部信息。此外，为了实现写操作，权威机构发布基于  时间间隔的签名。接着，利用修正的代理重加密实现访问策略更新。最后，方案引入紧急秘钥，供可行第三方紧急解密。   1. 秘钥撤销。立即撤销。重加密密文，更新秘钥。对于私人user，由数据拥有者操作。   对于public user，由权威机构操作，且可以实现public user的属性撤销（public user 的属性对于每一个权威机构来说，可以看做IBE方案中的身份） |
| 创新点 | 把ABE方案恰如其分、满足需求地融入个人健康记录系统中，使其具有灵活、安全、实用的特性；从问题着手构建ABE方案的写作思路。在更新访问策略中，利用系统建立的随机种子s’，生成随机数，减少计算开销；在实现写操作时，非常应景地采用时间间隔签名，实用性高。 |

|  |  |
| --- | --- |
| 19题目 | NEON Implementation of an Attribute-Based Encryption Scheme |
| 分类/出处 | Others |
| 文章目的： | 把经典CP-ABE方案在实际移动端平台进行仿真。 |
| 主要方法 | 搭建一套ARM处理器，支持NEON指令系统的硬件；创建一个软件库用来支持ABE方案中的双线性映射运算。 |
| 创新点 | ABE仿真 |