山东大学

毕 业 论 文(设 计)

论文（设计）题目:

密文策略-基于属性加密的研究与实现

姓　　名 王军委

学　　号 200800300237

学　　院 山东大学软件学院

专　　业 软件工程

年　　级 2008 级

指导教师 胡程瑜

2012 年 5 月 13 日

山东大学毕业设计（论文）成绩评定表

学院：　　专业：　　年级：

<table>
<tr><td>学 号</td><td></td><td>姓 名</td><td></td><td>设计（论文）成绩</td><td></td></tr>
<tr><td colspan="2">设计（论文）题目</td><td colspan="4"></td></tr>
<tr><td rowspan="2">指导教师评语</td><td colspan="5"></td></tr>
<tr><td colspan="5">评定成绩：　　签名：　　年　月　日</td></tr>
<tr><td rowspan="2">评阅人评语</td><td colspan="5"></td></tr>
<tr><td colspan="5">评定成绩：　　签名：　　年　月　日</td></tr>
<tr><td rowspan="2">答辩小组评语</td><td colspan="5"></td></tr>
<tr><td colspan="5">答辩成绩：　　组长签名：　　年　月　日</td></tr>
</table>

注：设计（论文）成绩=指导教师评定成绩（30%）＋评阅人评定成绩（30%）＋答辩成绩（40%）

目录

密文策略-基于属性的加密的研究与实现

摘　要

在分布式系统中，只有当用户拥有某些凭据或者属性才能够访问数据。目前，执行这种策略的唯一方式是采用一个可信的服务器来存储数据并进行访问控制。然而，如果任意一个存储数据的服务器被攻破，那么数据的保密性就会大打折扣。在本文中，我们提供一个称之为密文策略－基于属性的加密的技术来实现对加密数据的复杂的访问控制。通过我们的技术，加密数据甚至可以存储在不可信的存储服务器上，而且我们的技术可以抵制合谋攻击。先前的基于属性的加密方案用属性来描述被加密的数据，而将策略写入用户的密钥里；然而在我们的系统中属性用来描述用户的凭据，加密数据的一方来决定谁可以解密的策略。因此，我们的加密方案在概念上更接近与传统的访问控制方法。除此之外，我们提供了我们系统的 Java 实现。

关键词： 访问控制；密文策略；基于属性加密；合谋攻击

ABSTRACT

Only when the user has some credentials or attributes, can he be able to access the data in a distributed system. At present, the only way for the implementation of this strategy is making use of a trusted server to store data and implement access control. But if any server that stored data is compromised, then the confidentiality of the data is compromised. In this article, we provide a technology called Ciphertext-Policy Attribute-Based Encryption to implement complex access control on encrypted data. Through our technology, encrypted data can even be stored in the untrusted storage server. In addition, our technology can resist the collusion attacks. In previous Attribute-Based encryption scheme, properties are used to describe the data to be encrypted, the policy is written to the user's keys; however, in our system properties are used to describe the user's credentials, the party who encrypting make the policy for who can decrypt. Therefore, our encryption scheme is closer in concept to traditional access control methods. Besides, we provide our system a Java implementation of our system.

Keywords: Access Control; Collusion Attacks; Ciphertext-Policy; Attribute-Based Encryption

第1章 绪论

1.1 基于属性加密的研究背景

在许多情况下，当用户对敏感数据进行加密时，这时他迫切需要建立特定的访问控制策略决定谁可以解密数据。例如，假设 FBI 在 Knoxville 和 San Francisco 的公共反腐办公室调查涉及 San Francisco 说客行贿 Tennessee 国会议员的指控。上级 FBI 特工可能想加密一份敏感的备忘录以便只有拥有特定凭据和属性的特工可以查看。例如，上级特工可能指定下述访问结构来访问此信息：

((“Public Corruption Office” **AND** (“Knoxville”
OR “San Francisco”)) **OR** “Name: Charlie Eppes”)[1]

通过这个访问结构，意味着上级特工可能只允许备忘录被工作在 Knoxville 或者 San Francisco 公共反腐办公室的或者名字叫做 Charlie Eppes 的特工查看。

就像上例中所解释的，秘密数据拥有者能够根据特定的知识选择访问策略。除了这些特定的知识，这个人甚至可能不知道能够访问被加密数据人员的精确身份，但他有以属性或者凭据的方式描述这些可以解密数据人员的方法。

传统方案中，这种表达式形式的访问控制必须采用在可信服务器上存储数据的方式。服务器作为一种工具而被信任，这种工具通过检查用户是否拥有某种凭据来控制访问数据。然而，随着数据的增长，数据会被存储到分布式环境中，且服务器的数目越来越多。在分布式环境中复制数据具有高性能和高可靠性的优势，但是随着数据的增长，保证数据安全性越来越难；当数据存储在多个服务器上，这些服务器中任意一个被攻破的可能性大幅攀升。基于这些原因我们需要敏感数据以加密的方式存储，以便数据在服务器被攻破的情况下仍然保密。

公钥加密是一个保障存储和传输敏感数据的强有力机制。传统上，加密被看作是用户向目标用户或者设备分享数据的一种方法，但是这种方法仅适用于数据提供方确切的知道要跟谁分享数据，更多的应用中数据提供者想要根据接受者的凭据来制定分享机制。也就是说，大多数现存的公钥加密方案允许一方给另一方加密数据，但是不能够高效的处理像上述例子中更复杂的表达式形式的访问控制。

1.2 国内外研究现状

Sahai 和 Waters[2]提出了加密算法本身决定谁可以解密被加密的加密新思路。数据提供者用谓词$f(\cdot)$描述他想他想如何分享数据，用户被赋予与他们的凭据X关联的密钥；当$f(X)=1$时，拥有凭据X的用户可以解密拥有谓词$f(\cdot)$的密文。

Sahai 和 Waters[2]提出了这种问题的正式描述，他们称之为基于属性的加密[1]。在 ABE 中，用户的凭据用被称为“属性”的字符串集合表示，谓词用基于这些属性上的公式表示。SW[2]的技术受到基于身份的加密[3]上一些工作[3-5,6,7]的启发。SW 方法的一个缺点是他们最初的构造受限于处理由门限组成的公式。

在随后的工作中，Goyal, Pandey, Sahai 和 Waters[8]进一步阐明了 ABE 的概念。尤其是，他们提出了两种互补形式的 ABE。其一是密钥策略-基于属性的加密[4]，属性用来描述密文，对属性的公式用来描述用户的私钥；其二是与 KP-ABE 互补的密文策略-基于属性的加密[5]，属性用来描述用户的凭据即私钥，公式则被加密放附加到密文。除此之外，Goyal 等人[8]提供了 KP-ABE 的一种构造。由于它允许被加密数据的密钥能够被任意单调访问公式描述，所以该构造的代价较高。这个系统被证明在双线型 Diffie-Hellman 假设下选择性安全。然而他们把 CP-ABE 描述性的构造留做了一个开放性问题。

第一次明确解决 CP-ABE 问题的是 Bethencourt，Sahai 和 Waters[1]。他们描述了一个高效的可以描述的系统，这个系统允许加密者以任意单调访问公式来表达访问谓词f，并取得了 Goyal 等人[8]系统的类似表现和效率。

1.3 本文的主要工作

本文主要描述 BSW 的工作[1]并给出了他们工作的一个 Java 实现。在 BSW 的系统中用户的私钥与任意数目的字符串形式的属性相关联，当一方要要加密数据时，他们明确相关的属性上的访问结构，仅当用户的属性可以通过密文的访问结构，他才能解密密文。从数学角度讲，访问结构被描述为单调“访问树”，访问结构的节点由门限组成，叶子节点描述了属性。我们用 AND 来构造$n\text{-}of\text{-}n$门，用 OR 表示1-of-n门。

1.4 本文的主要技术

从较高的水平上讲，BSW 的主要工作与最近 Sahai 和 Waters[2], Goyal 等人[8]的工作相似，但是 BSW 却大量采用了新的技术。KP-ABE 中，密文与描述性的属性关联，用户的私钥与策略关联（与 BSW 的情况恰好相反）。我们强调

[1] Attribute-Based Encryption，简称 ABE
[2] Amit Sahai 和 Brent Waters[2]，简称 SW
[3] Identity-Based Encryption，简称 IBE
[4] Key-Policy ABE，简称 KP-ABE
[5] Ciphertext-Policy ABE，简称 CP-ABE

KP-ABE 中，加密者对谁可以访问他所加密的数据不具有控制权，除非他选择对数据的描述性数据。然而，他必须保证提供给用户适当的私钥以授权或者阻止用户解密密文。换言之，在[2, 8]中，“情报”掌握在私钥询问者手中，而不是加密者手中。在我们的构造里，加密者决定了其他人能否访问他所加密的数据。因此，在[2,8]中的技术不适合我们，我们必须采用新的技术。

从技术的水平上讲，BSW 必须达到的主要目标是可抵抗合谋攻击: 如果多个用户合谋，他们只能解密至少他们中的一个用户可以独立解密的密文。特别提到绪论一开始提到的例子[1]，假设工作在 San Francisco 反恐局的 FBI 特工与他工作在 New York 公共反腐局的朋友合谋。我们不希望合谋者能够解密由他们共同属性加密的备忘录。在我们的构造中，这种安全是先决条件。

在[2,8]的工作中，通过利用秘密分享方案[9, 10]6和独立地选择私密份额嵌入到每一个人的私钥中来保证可抵制合谋攻击。因为秘密分享方案的每次调用中随机数是独立的，所以可抵制合谋攻击。在我们的情况中，用户的私钥与属性集而不是属性集上的访问结构关联，因此秘密分享方案不适用。

相反，BSW 设计了一种采用两级随机掩蔽技术的新的私钥随机技术。这项技术利用了高效可计算的双线性映射群。

最后，我们提供了 BSW 构造的一个实现来展示实践中系统表现是良好的。

1.5 本文的组织结构

本文的余下部分组织结构如下。在第二章我们将给出相关背景知识的定义以及高效可计算双线性映射群的相关概念，第三章我们将讨论 BSW 的 CP-ABE 构造，第四章我们会提供一个 CP-ABE 的 Java 实现，第五章将是本文的总结。

6 Secret-Sharing Scheme

第2章 基础知识

我们首先给出 CP-ABE 安全性的正式定义，然后我们给出双线性映射的背景信息。如同 Goyal 等人[8]所做，我们定义访问结构并在我们的安全性定义中使用；不同的是，在我们的定义中属性将用来描述用户，访问结构用来标记被加密的数据。

2.1 定义

定义1（访问结构[1]） 令$\{P_1, P_2, \dots, P_n\}$是所有的参与方集合。集合$A \subseteq 2^{\{P_1,P_2,\dots,P_n\}}$是单调的是指：对于任意$B, C$，如果$B \in A$且$B \subseteq C$，则$C \subseteq A$。访问结构（特别的，单调访问结构）是$\{P_1, P_2, \dots, P_n\}$的非空子集$A$（特别的，单调集合），例如，$A \subseteq 2^{\{P_1,P_2,\dots,P_n\}} \setminus \{\emptyset\}$，集合$A$中的集合元素被称为授权集，不在集合$A$中的集合被称为未授权集。

在我们的论述中，参与方被属性所代替，因此，访问结构A 包含了授权属性集。本文中我们只注意单调访问结构，但是，以BSW 的技术实现通用的访问结构是可能的。从现在开始，除非特别强调，访问结构是指单调访问结构。

2.1.1 通用 CP-ABE 方案

一个CP-ABE 机制包含四个基本的算法：Setup，Encrypt，KeyGen 和 Decrypt。

Setup Setup 算法的输入只有隐含的安全参数，输出公共参数PK和主密钥MK。

Encrypt(PK, M, $\mathbb{A}$**)**加密算法的输入是公共参数PK，明文M和属性全集上的访问结构$\mathbb{A}$。算法加密明文M，产生密文CT，只有用户持有满足访问结构的属性集合才能解密消息。我们假定密文隐含访问结构$\mathbb{A}$。

KeyGen (MK, S**)** 密钥生成算法的输入是主密钥MK和描述私钥的属性集合S，输出是私钥SK。

Decrypt(PK, **CT**, **SK)** 解密算法的输入是公共参数PK，包含访问策略$\mathbb{A}$的密文CT和属性集合S生成的私钥SK。如果集合S满足访问结构$\mathbb{A}$，那么算法会解密密文CT 返回消息M。

现在我们将描述CP-ABE 方案的安全模型。如同IBE 方案[4,5,7]的安全模型，

CP-ABE 方案的安全模型允许敌手询问任何不能解密密文的私钥，即在我们的安全定义中敌手挑战访问结构$\mathbb{A}^*$的解密，并且可以询问任意不满足S^* 的私钥S。

2.1.2 CP-ABE 安全模型

现在我们给出正式的安全游戏。

Setup 挑战者运行Setup 算法并将得到的公共参数PK 交给敌手。

阶段1 敌手反复生成对应于属性集$S_1, \dots, S_{q_1}$的私钥。

Challenge 敌手提供两个等长的信息M_0和M_1。除此之外，敌手提供一个阶段1中所有属性集合$S_1, \dots, S_{q_1}$都不满足的挑战访问结构$\mathbb{A}^*$。挑战者随机选取$b \in \{0,1\}$，在访问结构$\mathbb{A}^*$下加密M_b，并将密文CT*交给敌手。

阶段2 敌手提供属性集合$S_{q_1+1}, \dots, S_q$，并且该属性集合不满足对应的挑战访问结构，重复阶段1。

Guess 敌手输出对b的猜测b'。

在上述游戏中敌手$\mathcal{A}$的优势被定义为$\Pr[b' = b] - 1/2$。我们注意到这个模型可以通过在阶段1 和阶段2 中允许解密敌手询问的明文扩展为可以处理选择明文攻击的情形。

定义2 *在上述游戏中，如果多项式时间内敌手最多有可以忽略的优势，那么CP-ABE方案是安全的。*

2.2 双线性映射

我们给出一些与高效可计算双线型映射群相关的事实。

设$\mathbb{G}_0$和$\mathbb{G}_1$是阶为素数p的两个乘法循环群，g是$\mathbb{G}_0$的生成元，$e: \mathbb{G}_0 \times \mathbb{G}_0 \to \mathbb{G}_1$。双线性映射$e$具有以下性质：

a) 双线性：对于任意$u, v \in \mathbb{G}_0$和任意$a, b \in Z_p$，我们有$e(u^a, v^b) = e(u, v)^{ab}$；

b) 非退化性：$e(g, g) \neq 1$。

如果$\mathbb{G}_0$中的群操作和双线性映射$e: \mathbb{G}_0 \times \mathbb{G}_0 \to \mathbb{G}_1$都是高效可计算的，我们称$\mathbb{G}_0$为双线性群。请注意由于$e(g^a, g^b) = e(g, g)^{ab} = e(g^b, g^a)$，双线性映射$e$具有

对称性。

第3章 BSW 的 CP-ABE 构造

本章中我们提供了BSW 方案的构造。我们首先介绍描述密文的访问树和描述私钥的属性的模型，其次我们给出BSW 方案的描述，最后我们给出安全性，高效性的讨论。

3.1 模型

在BSW的构造中私钥被描述性的属性集合S所确定。一方想解密数据必须拥有满足访问树结构的私钥。

访问树中的每个内部节点是一个门，叶子节点与属性关联。（请注意，这样的描述是非常具有表达力的。例如，我们分别用$2\text{-}of\text{-}2$ 和$1\text{-}of\text{-}2$ 的门来表达树中“AND”门和“OR”门。）当且仅当私钥的属性分配到树的节点并使树能满足，持有私钥的用户将能够解密密文。尽管在我们的方案里，属性用来标记私钥，我们还是用与[8]相同的概念来描述访问树。

访问树$\mathcal{T}$ 用$\mathcal{T}$代表访问结构，通过他的孩子和门限值描述的门限来代表树的每个非叶子节点。设节点x 的孩子数目为num_x，门限值为k_x，那么$0 < k_x \leq num_x$。当$k_x = 1$，门限是或门；当$k_x = num_x$，门限是与门。树的每个叶子节点x用一个属性和门限值$k_x = 1$描述。为了方便的使用访问树，我们定义了一些函数。函数$\mathbf{parent}(x)$表示节点x的父节点, 仅当x是叶子节点时，函数$\mathbf{att}(x)$被定义为x所描述的属性。访问树$\mathcal{T}$同时定义了每个节点的子节点的被标记为从1到num_x的顺序索引值，函数$\mathbf{index}(x)$定义为与节点x关联的这样一个索引值，且对一个给定的密钥，索引值以任意的方式唯一的赋值给访问结构中的节点。

满足访问树 令$\mathcal{T}$是根为r 的访问树，$\mathcal{T}_x$表示以x为根的$\mathcal{T}$的子树，因此$\mathcal{T}$等同于$\mathcal{T}_r$。如果属性集合γ满足访问树$\mathcal{T}_x$，我们表示为$\mathcal{T}_x(\gamma) = 1$。我们用如下递归的方式计算$\mathcal{T}_x(\gamma)$：如果$x$是非叶子节点，对于$x$的所有孩子，计算$\mathcal{T}_{x'}(\gamma)$，当且仅当至少$k_x$个孩子返回1，$\mathcal{T}_x(\gamma)$返回1；如果$x$是叶子节点，那么当且仅当$\mathbf{att}(x) \in \gamma$时，$\mathcal{T}_x(\gamma)$返回1。

3.2 BSW 的 CP-ABE 构造

设$\mathbb{G}_0$是阶为素数p的双线性映射群，g是$\mathbb{G}_0$的生成元，$e: \mathbb{G}_0 \times \mathbb{G}_0 \to \mathbb{G}_1$是双

线性映射。安全参数κ决定群的规模。同时，我们定义了拉格朗日系数$\Delta_{i,S}$，i $\in \mathbb{Z}_p$，S是集合$\mathbb{Z}_p$中的元素：$\Delta_{i,S}(x) = \prod_{j\in S, j\neq i} \frac{x-j}{i-j}$。哈希函数$H: \{0,1\}^* \to \mathbb{G}_0$是random oracle，这个函数可以把任意用二进制串描述的属性映射到随机的群元素。BSW的构造如下。

Setup Setup 算法选择生成元为g，阶为素数p的双线性映射$\mathbb{G}_0$，指数$\alpha, \beta \in \mathbb{Z}_p$。生成公钥

$$\mathrm{PK} = \mathbb{G}_0, g, h = g^{\beta}, e(g,g)^{\alpha}$$

和主密钥$\mathrm{MK} = \beta, g^{\alpha}$。

Encrypt(PK, M, $\mathcal{T}$**)** 加密算法在树访问结构$\mathcal{T}$下加密消息M。算法首先为$\mathcal{T}$每个节点x（包括叶子节点）选择一个多项式q_x。从树的根节点 R 开始，自上而下选择多项式。节点x的多项式q_x的度d_x比该节点的门限值k_x少 1，即$d_x = k_x - 1$。

算法从根节点 R 开始选择随机数$s \in \mathbb{Z}_p$，并设置$q_R(0) = s$。然后，算法随机选择多项式q_R 上的d_R个点来完全定义q_R。对于其他的顶点x，令$q_x(0) = q_{\mathbf{parent}(x)}(\mathbf{index}(x))$，随机选择其它$d_x$个顶点来完全定义$q_x$。

设$\mathcal{T}$中所有叶子节点的集合为 Y ，那么在给定的树形访问结构$\mathcal{T}$下计算密文

$$\mathrm{CT} = (\mathcal{T}, \tilde{C} = Me(g,g)^{\alpha s}, C = h^s,$$
$$\forall y \in Y:\ C_y = g^{q_y(0)}, C_y' = H(\mathbf{att}(y))^{q_y(0)}) \ 。$$

KeyGen (MK, S**)** 密钥生成算法的输入是属性集合S，输出为被S所标记的密钥。算法首先选择随机数$r \in \mathbb{Z}_p$，然后对每一个$j \in S$选择随机数$r_j \in \mathbb{Z}_p$。最后计算出私钥

$$\mathrm{SK} = (D = g^{(\alpha+r)/\beta},$$
$$\forall j \in S:\ D_j = g^r \cdot H(j)^{r_j}, D_j' = g^{r_j}) \ 。$$

Decrypt(PK, **CT**, **SK)** 我们的解密算法是一个递归算法。为了便于讨论，我们提出了解密算法的最简单形式，并在下一小节中提出了潜在的性能改进。

我们首先定义递归算法 Decrypt(PK, CT, x)，它用密文$\mathrm{CT} = (\mathcal{T}, \tilde{C}, C, \forall y \in Y: C_y, C_y')$，与属性集合$S$关联的私钥 SK，$\mathcal{T}$中的节点$x$作为输入。

当节点x 是叶子节点，令$i = \mathbf{att}(x)$，如果$i \in S$，那么

$$\text{DecryptNode}(\text{CT}, \text{SK}, x) = \frac{e(D_i, C_x)}{e(D_i', C_x')}$$

$$= \frac{e\left(g^r \cdot \text{H(i)}^{r_i}, g^{q_x(0)}\right)}{e(g^{r_i}, H(i)^{q_x(0)})}$$

$$= e(g, g)^{r q_x(0)} \text{ 。}$$

如果$i \notin S$，那么$\text{DecryptNode}(\text{CT}, \text{SK}, x) = \perp$。

现在我们考虑x是非叶子节点时的递归情况。算法 Decrypt(PK, CT, x)工作方式如下：对于x 的所有子节点 z，计算$F_z = \text{DecryptNode}(\text{CT}, \text{SK}, z)$。令$S_x$为$k_x$大小的满足$F_z \neq \perp$的子节点$z$的集合。如果不存在这样的集合，那么这个节点不满足，且函数返回$\perp$。

否则，我们计算

$$\text{F}_x = \prod_{z \in S(x)} F_z^{\Delta_{i,S_x'}(0)}, \text{其中}, i = \textbf{index}(z), S_x' = \{\textbf{index}(z) : z \in S_x\}$$

$$= \prod_{z \in S(x)} \left(e(g, g)^{r \cdot q_z(0)}\right)^{\Delta_{i,S_x'}(0)}$$

$$= \prod_{z \in S(x)} \left(e(g, g)^{r \cdot q_{\textbf{parent}(z)}(\textbf{index}(z))}\right)^{\Delta_{i,S_x'}(0)}$$

$$= \prod_{z \in S(x)} e(g, g)^{r \cdot q_x(i) \cdot \Delta_{i,S_x'}(0)}$$

$$= e(g, g)^{r \cdot q_x(0)} \quad \text{(使用多项式插值)}$$

并返回结果。

在定义了 DecryptNode 函数之后，我们定义解密算法。算法首先调用 DecryptNode(CT, SK, R)，R 是树$\mathcal{T}$的根节点。如果树满足S，我们令

$$A = \text{DecryptNode}(\text{CT}, \text{SK}, R) = e(g, g)^{r q_R(0)} = e(g, g)^{rs} \text{ 。}$$

现在算法通过下面计算解密

$$\tilde{C} / \left(\frac{e(C, D)}{A}\right) = \tilde{C} / \left(\frac{e\left(h^s, g^{(\alpha + r)/\beta}\right)}{e(g, g)^{rs}}\right) = M \text{ 。}$$

3.3 直觉安全和效率

现在我们将提出我们方案的直觉安全性和我们方案的效率的讨论。

3.3.1直觉安全

如同之前的 ABE 方案，在设计我们的方案时面临的最大挑战是如何抵制合谋攻击。我们采用了 Sahai 和 Waters 方案[2]中的通过随机化用户私钥的方案来组织合谋；所不同的是，我们把秘密分享的思想嵌入到密文而不是私钥中。攻击者必须恢复$e(g,g)^{\alpha s}$才能够解密。为了做到这一点，攻击者必须从用户的私钥中配对 C, D 两部分，这会得到想要的值$e(g,g)^{\alpha s}$，但是被某些值$e(g,g)^{rs}$所蒙蔽。当且仅当某用户拥有密钥的部分满足嵌入到密文中的秘密分享，这个值才不会被蒙蔽。合谋攻击不会在上述过程中起到任何作用，因为用户私钥的随机性随机化了盲值。

3.3.2效率

密钥生成算法和加密算法的效率都非常容易计算。加密算法对密文访问树的每个叶子节点需要两次指数运算，密文的规模中包括每个树叶子节点的两个群元素。密钥生成算法对用户的每个属性需要两次指数运算，私钥包含对每个属性的两个群元素。最简单的形式，解密算法需要对与私钥属性匹配的访问树叶子节点两次配对，对沿着上述叶子到根节点的路径节点的（至多[7]) 一次指数运算。然而，可能存在着不止一种满足策略的方式，一个更加智能的算法可能会沿着这条线路优化，我们会在第四章中介绍多种提升性能的方法。

[7] 如果路径中存在不满足的节点，幂运算会减少

第4章 实现

在本章中我们将要讨论实现第三章构造的一些实际问题，包括一些优化，我们所开发的工具包的描述。

4.1 解密算法的效率改进

尽管没有必要减少 Setup、Keygen 和 Encrypt 算法的群运算，但是却通过新的技术可以大幅提升解密算法的性能，我们将在此介绍这些改进。

优化解密策略 第 3 章出的递归算法中，被对私钥属性匹配的叶子节点进行两次配对，对沿着节点到根的每个内部节点（不包括根节点）至多一次指数运算。递归部分的最后一步会有一次额外的配对。当然，每个门限值为 k 的内部节点，只保留他的 k 个孩子。考虑到在提前叶节点满足和选择可以满足整个访问树的自己的时间，我们可能避免估计 DecryptNode，因为结果最终不被使用。

更精确的讲，设M是访问树$\mathcal{T}$的节点的子集。我们定义函数 **restrict**$(\mathcal{T}, M)$是从$\mathcal{T}$删除以下节点（同时保持门限值不变）形成的访问树。首先，我们删除所有不在M中的节点，下一步我们删除沿着孩子数小于门限值k_x的内部节点 x 一直到$\mathcal{T}$的根节点的所有节点。重复上述步骤直至没有节点可以删除，这时候得到的就是 **restrict**$(\mathcal{T}, M)$。因此给定访问树$\mathcal{T}$和满足访问树的属性集γ，自然的问题是选择集合 M 使得γ满足 **restrict**$(\mathcal{T}, M)$并且M中的叶子数目是最少的（考虑到配对操作的代价是最昂贵的）。这可以通过对树的一次遍历的递归算法很容易的实现。算法 DecryptNode 在 **restrict**$(\mathcal{T}, M)$上会取得与原来相同的结构。

直接计算 进一步性能改进，可以放弃DecryptNode 函数并采取更直接的计算。直观的讲，我们想象展平树上对DecryptNode 的递归调用，然后合并指数运算到每一个（用过的）叶子节点上。更精确的讲，令$\mathcal{T}$ 是根为r的访问树，γ是属性集合，$M \subseteq \mathcal{T}$使得满足**restrict**$(\mathcal{T}, M)$。同时假设 M是最小的，即没有内部节点的孩子数比门限值大。设$L \subseteq M$是M中的叶子节点。那么对于每一个$\ell \in L$，ℓ到r的路径表示为

$$\rho(\ell) = \left(\ell, \mathbf{parent}(\ell), \mathbf{parent}\left(\mathbf{parent}(\ell)\right), \dots, r\right) \text{ 。}$$

同时，节点x的兄弟节点（包括x）表示为

$$\mathbf{sibs}(x) = \{y | \mathbf{parent}(x) = \mathbf{parent}(y)\} \text{ 。}$$

在上述概念的基础上，我们可以继续计算DecryptNode(CT, SK, r)。首先，对每一个$\ell \in L$计算

$$\mathrm{z}_\ell = \prod_{\substack{x \in \rho(\ell) \\ x \neq r}} \Delta_{i,S}(0), \text{ 其中} i = \mathbf{index}(x), S = \{\mathbf{index}(y) | y \in \mathbf{sibs}(x)\} \ ,$$

然后计算

$$\mathrm{DecryptNode}(\mathrm{CT}, \mathrm{SK}, r) = \prod_{\substack{\ell \in L \\ i = \mathbf{att}(\ell)}} \left(\frac{e(D_i, C_\ell)}{e(D_i', C_\ell')} \right)^{\mathrm{z}_\ell} \quad 。$$

用这种方法，整个解密算法中指数运算的次数从$M-1$（例如，除去根节点以外的每个节点一次）减少为$|L|$，配对的次数为$2|L|$。

合并配对　合并具有相同属性的叶子可能进一步较少配对的数目。如果对于L中的某些ℓ_1, ℓ_2，有$\mathbf{att}(\ell_1) = \mathbf{att}(\ell_2) = i$，那么

$$\left(\frac{e(D_i, C_{\ell_1})}{e(D_i', C_{\ell_1}')} \right)^{z_{\ell_1}} \cdot \left(\frac{e(D_i, C_{\ell_2})}{e(D_i', C_{\ell_2}')} \right)^{z_{\ell_2}}$$

$$= \frac{e\left(D_i, C_{\ell_1}^{z_{\ell_1}}\right)}{e\left(D_i', C_{\ell_1}'^{z_{\ell_1}}\right)} \cdot \frac{e\left(D_i, C_{\ell_2}^{z_{\ell_2}}\right)}{e\left(D_i', C_{\ell_2}'^{z_{\ell_2}}\right)}$$

$$= \frac{e\left(D_i, C_{\ell_1}^{z_{\ell_1}} \cdot C_{\ell_2}^{z_{\ell_2}}\right)}{e\left(D_i', C_{\ell_1}'^{z_{\ell_1}} \cdot C_{\ell_2}'^{z_{\ell_2}}\right)} \quad 。$$

利用这个事实，我们合并L中所有互相不同的属性的配对，配对总数减少至$2m$，m是出现在L 中不同的属性的个数。但是请注意，幂运算的次数增加了，且某些幂运算现在执行在$\mathbb{G}_0$上而不是$\mathbb{G}_1$上。具体来讲，如果m‘是至少与其他叶子节点分享属性的叶子节点的数目，那么我们在$\mathbb{G}_0$和$\mathbb{G}_1$上分别执行$2m$次，$|L| - m$’次指数运算，而不是分别为0 次，$|L|$次。如果椭圆曲线群$\mathbb{G}_0$上的幂运算比与其阶相同的有限域$\mathbb{G}_1$慢，那么这个技术将潜在的增加解密的时间。

4.2　CP-ABE 的 Java 实现、安装以及 API 简介

4.2.1CP-ABE 的 Java 实现

我们给出了第三章构造的实现，称之为 cpabe 包[12]，并在 GPL 协议[13]下发布。

开发平台：Linux kernel 3.3.4-2-ARCH

硬件环境：Intel(R) Core(TM) 2 Duo CPU T5800 @ 2.00GHz

软件环境：Eclipse 3.7.2-2 extra, openjdk6 6.b24_1.11.1-3

外部依赖：jPBC 1.2.0

我们的实现使用了 jPBC 库[14][8]，是由萨勒诺大学计算机科学与应用系的 GAS 实验室主导开发的。jPBC 的开发这给 jPBC 的定义是：

a) 实现了 Ben Lynn 开发的 PBC 库[15]接口

b) 对 PBC 库的封装

代码测试：cpabe 包经过了严格的单元测试和系统测试后发布。

4.2.2CPABE 包的安装

首先去 jPBC 的官方网站下载最新的 jPBC 库。下载完成后解压得到 jpbc-api-version.jar, jpbc-plaf-version.jar（其中 version>=1.2.0），并将这两个 jar 包作为 cpabe 的外部引用包。

使用编译打包工具将源代码打包成 jar 包，或者直接作为应用的源代码应用的新的系统中去。

4.2.3API 简介

cpabe 包的可以使用 cpabe 类的成员函数的方式直接被其它大型的系统调用。

Setup 初始化接口，生成公共参数 PK 和主密钥 MK，并分别存储到 pubfile 和 mskfile 对应的文件路径中去。

代码 **4.1:** **setup**

```
/*
 * Generate a public key and corresponding master secret key.
 */
public void setup(String pubfile, String mskfile)
```

KeyGen 私钥生成算法接口，从 pubfile 和 mskfile 指定的文件中分别读取公共参数 PK 和主密钥 MK，根据用户的属性串 attr_str，生成用户的私钥 SK 并存储到

[8] jPBC 遵循 LGPL 协议

prvfile 指定的文件中。

用户的每个属性是由字符串表示的，将这些字符串用空格分割连接成一个长的字符串 *S*，称 *S* 为用户的属性串（子串的先后顺序无关）。比如说学生甲拥有的属性分别用字符串描述为：“*sid_2008001*”（表示学号是 2008001）、“*birthdate_19900101*”（生日是 19900101）、“*sname_jia*”（表示名字叫“甲”），则学生甲的属性串 *S* 为：

“*sid_2008001　birthdate_19900101　sname_jia*”

代码 4.2:　keygen

```
/*
 * Generate a private key with the given set of attributes.
 */
public void keygen(String pubfile, String prvfile,
                   String mskfile, String attr_str)
```

Encrypt 加密算法从pubfile中读取公共参数，在访问策略policy下将inputfile指定的文件加密为路径为encfile的文件。其中访问策略是用后序遍历门限编码的字符串。比如访问策略“*foo bar fim 2of3 baf 1of2*”指定了含有两个门限四个叶子节点的访问策略，并且拥有属性“*baf*”或者“*foo*”、“*bar*”、“*fim*”中的至少两个的属性集合满足该访问策略。

代码 4.3:　enc

```
/*
 * The policy is specified as a simple string which encodes a
 * post order traversal of threshold tree defining the access
 * policy. As an example,
 *
 * "foo bar fim 2of3 baf 1of2"
 *
 * specifies a policy with two threshold gates and four leaves.
 * It is not possible to specify an attribute with whitespace in
 * it (although "_" is allowed).
 *
 * Numerical attributes and any other fancy stuff are not
 * supported.
 *
 */
public void enc(String pubfile, String policy,
                String inputfile, String encfile)
```

Decrypt 解密算法从 pubfile 指定的文件中读入公共参数，从 prvfile 中读入用户私钥，将加密文件 encfile 解密为 decfile。

代码 **4.4:** **dec**

```
/*
 * Decrypt the specified ciphertext using the given private key.
 */
public void dec(String pubfile, String prvfile,
                String encfile, String decfile)
```

附录 A 包含一个具体的完整调用实例。

第5章 总结

5.1 本文工作的总结

本文通过对以往属性加密方案的研究，以及大量文献的学习，决定选择概念上更接近于传统访问控制的密文策略-基于属性加密作为研究重点。

首先，本文叙述了基于属性加密的提出和研究背景、发展现状，分析了基于属性加密的两个主要研究方向，密钥策略-基于属性加密和密文策略-基于属性加密在概念和技术实现上的异同。

之后，本文给出密文策略-基于属性加密的通用方案，在通用方案的基础上定义了密文策略-基于属性加密的安全模型和安全性定义。同时，本文还提供了（单调）访问结构，授权集以及双线性映射等基础知识。

本文还提供了 BSW 的基于属性加密构造方案，给出直觉上的安全性分析和效率分析，并从优化解密策略、采用更直接计算、合并相同属性的叶子等多角度分析了解密算法的效率改进。

最后本文给出了 BSW 构造的 Java 实现 cpabe 包，并对 cpabe 的安装和 API 接口进行了简单的介绍。

总之，密文策略-基于属性的加密削弱传统海量数据管理中复杂的访问控制带来的效率损失和不安全因素，并能够比传统公钥密码表达更复杂的访问控制，同时可以抵制合谋攻击，是现代密码体系研究的一个新的重要领域。

5.2 BSW 构造的缺陷

尽管 BSW 的构造很好的实现了复杂的访问控制和抵制合谋攻击，但是构造方案的复杂性不可避免的延续了属性加密和基于属性加密的一些缺陷，苏金树等[16]详细讨论这些问题，包括一下这些方面：

a) 策略灵活性不足：密文策略-基于属性密码方案中的加密者决定访问策略，因此公钥的复杂度与访问策略复杂度相关，限制了访问结构的设计；
b) 密钥管理困难：密文策略-基于属性加密方案中用户密钥与属性关联，属性动态变化，导致了密钥的撤销和重新生成，增加了密钥管理的难度；
c) 密钥泄露责任划分困难：基于属性机制中用户私钥由授权者生成，且用户私钥与用户的隐私信息无关，因此当密钥泄露时无法区分是授权者还是用户的责任。

5.3 发展趋势与应用展望

根据 5.2 中阐述的密文策略-基于属性的加密存在的策略灵活性不足、密钥管理困难、密钥泄漏等多方面缺陷，近来不少学者在研究，并在密码和安全协议领域的期刊和学术会议上发布了不少好的研究成果，针对苏金树等[16]具体阐述的这些成果，我们认为基于属性的加密仍需要在这些方面做更深入的研究。

根据摘　要所述，密文策略-基于属性加密在分布式系统（云系统）的访问控制中的应用前景非常广阔。随着云计算平台的成熟，效率和可靠性日益提高，暴露出来的安全问题也越来越多。密文策略-基于属性加密可以在提供访问控制的前提下，提高了安全性，因此 CP-ABE 在云计算中的应用前景广阔。

致　谢

从近代密码学基础知识的学习[17]，到代码实现，再到论文撰写，我的本科毕业设计前后经过近了三个月。这段时间内，在老师和同学们的指导和帮助下，我参阅了基于属性加密的相关论文、著作以及网上信息，在此向这些论著作者、老师以及同学们表示由衷的感谢和深深的敬意。

首先，我要感谢山东大学计算机学院信息安全实验室胡程瑜老师，感谢胡老师在本课题的开题、设计和撰写论文期间，给予我的宝贵意见和指导，以及为我提供的良好的实践机器及环境。

同时，我要感谢萨勒诺大学计算机科学与应用系的Angelo De Caro 博士和瑞士洛桑联邦理工学院的Julien Perrochet 硕士。Angelo De Caro 博士提供的jPBC工具包，为我的代码实现提供了极大的便利，同时Angelo De Caro 博士总是不厌其烦的回答我在使用jPBC 工具包时所遇到的问题。在Julien Perrochet硕士的鼓励及督促下，我完善了本文中用Java 实现的CP-ABE 项目的主页和文档[12]，并给了我长期将该项目维护下去的信心。

其次，我要感谢山东大学计算机学院信息安全实验室徐秋亮教授，王皓博士，赵川硕士，李贵莹硕士，王克瑞硕士等，他们在百忙之中抽出时间给我分配毕业设计任务，对我遇到的难题进行细致的分析与指导，加深了我对基于属性加密这个课题的理解。

除此之外，我还要感谢我的同学，在我阅读著作过程中，遇到不少难题，是他们不厌其烦地为我解答，给我提供帮助，在我心情低落的时候，也是他们给我的最好的鼓励和支持。

最后，再次感谢所有指导、帮助我完成毕业设计的教授、老师、研究生和同学，他们的帮助，使我的毕业设计得以顺利完成。

参考文献

[1] Amit Sahai John Bethencourt and Brent Waters. Ciphertex-policy attribute based encryption. In IEEE Symposium on Security and Privacy, pages 223 – 238, 2007.

[2] Amit Sahai and Brent Waters. Fuzzy identity-based encryption. In EUROCRYPT, pages 457 – 473, 2005.

[3] Dan Boneh and Xavier Boyen. Efficient selective-id secure identity-base encryption based encryption without random oracles. In EUROCRYPT, pages 223 – 238, 2004.

[4] Dan Boneh and Matthew K. Franklin. Identity-based encryption from weil pairing. In Advances in Crptology - CRYPTO, pages 213 – 229, 2001.

[5] Clifford Cocks. An identity based encryption scheme based on quadratioc residues. In IMA Int. Conf., pages 360 – 363, 2001.

[6] Shai Halevi Ran Canetti and Jonathan Katz. A forward-secure public-key encryption scheme. In EUROCRYPT, pages 255 – 271, 2004.

[7] Adi Shamir. Identity-based cryptosystems and signature schemes. In CRYPTO, pages 47 – 53, 1984.

[8] Amit Sahai Vipul Goyal, Omkant Pandey and Brent Waters. Attributebased encryption for fine-grained access control of encrypted data. In ACM Conference on Computer and Communications Security, pages 89 – 98, 2006.

[9] George Robert Blakley. Safeguarding cryptographic keys. In National Computer Conference, pages 313 – 317. American Federation of Information Processing Societies Proceedings, 1979.

[10] Adi Shamir. How to share a secret. Commun. ACM, 22(11):612 – 613, 1979.

[11] E. Fujisaki and T. Okamoto. Secure integration of asymmetric and symmetric encryption schemes. In CRYPTO, pages 537 – 554, 1999.

[12] Junwei Wang. cpabe.http:/wakemecn.github.com/cpabe/.

[13] GNU General Public License Version 2. http://www.gnu.org/licenses/ gpl-2.0.html , 1991.

[14] GAS lab. Java Pairing Based Cryptography Library. http://gas.dia.unisa.it/ projects/ jpbc/contact.html

[15] Ben Lynn, Pairing-Based Cryptography Library (PBC Library), GAS Laboratory, http:/crypto.stanford.edu/pbc

[16] 苏金树， 曹 丹， 王小峰， 孙一品， 胡乔林, 属性基加密机制，软件学报，

1301-1305，2011

[17] Jonathan Katz and Yehuda Lindell. Introduction to Modern Cryptography. CRC PRESS, 2007.

附录A　capbe 包使用演示

代码 1.1:　DemoForCpabe.java

```
import cpabe.Cpabe;

public class DemoForCpabe {
   final static boolean DEBUG = true;

   static String pubfile = "file_path/pub_key";
   static String mskfile = "file_path/master_key";
   static String prvfile = "file_path/prv_key";

   static String inputfile = "file_path/input.pdf";
   static String encfile = "file_path/input.pdf.cpabe";
   static String decfile = "file_path/input.pdf.new";

   static String[] attr = { "baf", "fim1", "foo" };
   static String[] another_attr = { "baf1", "fim1", "foo" };
   static String policy = "foo bar fim 2of3 baf 1of2";

   public static void main(String[] args) throws Exception{
      String attr_str;

      attr_str = student_attr;
      policy = student_policy;

      Cpabe test = new Cpabe();
      println("//start to setup");
      test.setup(pubfile, mskfile);
      println("//end to setup");

      println("//start to keygen");
      test.keygen(pubfile, prvfile, mskfile, attr_str);
      println("//end to keygen");

      println("//start to enc");
      test.enc(pubfile, policy, inputfile, encfile);
      println("//end to enc");

      println("//start to dec");
      test.dec(pubfile, prvfile, encfile, decfile);
      println("//end to dec");
   }
```

```
    /* connect element of array with blank space*/
    public static String array2Str(String[] arr) {
        int len = arr.length;
        String str = arr[0];

        for (int i = 1; i < len; i++) {
            str += " ";
            str += arr[i];
        }

        return str;
    }

    /* print Object o */
    private static void println(Object obj) {
        if (DEBUG)
            System.out.println(obj);
    }
}
```

附录B　外文文献原文

Fuzzy Identity-Based Encryption (Excerpts)

Amit Sahai　　Brent Waters
sahai@cs.ucla.edu　　bwaters@cs.stanford.edu

Abstract

We introduce a new type of Identity-Based Encryption (IBE) scheme that we call Fuzzy Identity-Based Encryption. In Fuzzy IBE we view an identity as set of descriptive attributes. A Fuzzy IBE scheme allows for a private key for an identity, ω, to decrypt a ciphertext encrypted with an identity, ω', if and only if the identities ω and ω' are close to each other as measured by the "set overlap" distance metric. A Fuzzy IBE scheme can be applied to enable encryption using biometric inputs as identities; the error-tolerance property of a Fuzzy IBE scheme is precisely what allows for the use of biometric identities, which inherently will have some noise each time they are sampled. Additionally, we show that Fuzzy-IBE can be used for a type of application that we term "attribute-based encryption".

In this paper we present two constructions of Fuzzy IBE schemes. Our constructions can be viewed as an Identity-Based Encryption of a message under several attributes that compose a (fuzzy) identity. Our IBE schemes are both error-tolerant and secure against collusion attacks. Additionally, our basic construction does not use random oracles. We prove the security of our schemes under the Selective-ID security model.

1 Introduction

Identity-Based Encryption [15] (IBE) allows for a sender to encrypt a message to an identity without access to a public key certificate. The ability to do public key encryption without certificates has many practical applications. For example, a user can send an encrypted mail to a recipient, e.g. bobsmith@gmail.com, without the requiring either the existence of a Public-Key Infrastructure or that the recipient be on-line at the time of creation.

One common feature of all previous Identity-Based Encryption systems is that they view identities as a string of characters. In this paper we propose a new type of Identity-Based Encryption that we call *Fuzzy Identity-Based Encryption* in which we view identities as a set of descriptive attributes. In a Fuzzy Identity-Based Encryption scheme, a user with the secret key for the identity ω is able to decrypt a ciphertext encrypted with the public key ω' if and only if ω and ω' are within a certain distance of each other as judged by some metric. Therefore, our system allows for a certain amount of error-tolerance in the identities.

Fuzzy-IBE gives rise to two interesting new applications. The first is an Identity-Based Encryption system that uses biometric identities. That is we can view a user's biometric, for example an iris scan, as that user's identity described by several

attributes and then encrypt to the user using their biometric identity. Since biometric measurements are noisy, we cannot use existing IBE systems. However, the error-tolerance property of Fuzzy-IBE allows for a private key (derived from a measurement of a biometric) to decrypt a ciphertext encrypted with a slightly different measurement of the same biometric.

Secondly, Fuzzy IBE can be used for an application that we call "attribute-based encryption". In this application a party will wish to encrypt a document to all users that have a certain set of attributes. For example, in a computer science department, the chairperson might want to encrypt a document to all of its systems faculty on a hiring committee. In this case it would encrypt to the identity {"hiring-committee", "faculty", "systems"}. Any user who has an identity that contains all of these attributes could decrypt the document. The advantage to using Fuzzy IBE is that the document can be stored on an simple untrusted storage server instead of relying on trusted server to perform authentication checks before delivering a document.

We further discuss the usefulness of using biometrics in Identity-Based and then discuss our contributions.

Using biometrics in Identity-Based Encryption In many situations, using biometric-based identity in an IBE system has a number of important advantages over "standard" IBE. We argue that the use of biometric identities fits the framework of Identity-Based Encryption very well and is a very valuable application of it.

First, the process of obtaining a secret key from an authority is very natural and straightforward. In standard Identity-Based Encryption schemes a user with a certain identity, for example, "Bob Smith", will need to go to an authority to obtain the private key corresponding to the identity. In this process the user will need to "prove" to the authority that he is indeed entitled to this identity. This will typically involve presenting supplementary documents or credentials. The type of authentication that is necessary is not always clear and robustness of this process is questionable (the supplementary documents themselves could be subject to forgery). Typically, there will exist a tradeoff between a system that is expensive in this step and one that is less reliable.

In contrast, if a biometric is used as an identity then the verification process for an identity is very clear. The user must demonstrate ownership of the biometric under the supervision of a well trained operator. If the operator is able to detect imitation attacks, for example playing the recording of a voice, then the security of this phase is only limited by the quality of the biometric technique itself. We emphasize that the biometric measurement for an individual need not be kept secret. Indeed, it is not if it is used as a public key. We must only guarantee that an attacker cannot fool the key authority into believing that an attacker owns a biometric identity that he does not.

Also, a biometric identity is an inherent trait and will always with a person. Using biometrics in Identity-Based Encryption will mean that the person will always have their public key handy. In several situations a user will want to present an encryption key to someone when they are physically present. For example, consider the case when a user is traveling and another party encrypts an ad-hoc meeting between them.

Finally, using a biometric as an identity has the advantage that identities are

unique if the underlying biometric is of a good quality. Some types of standard identities, such as the name “Bob Smith” will clearly not be unique or change owners over time.

Security Against Collusion Attacks In addition to providing error-tolerance in the set of attributes composing the identity any IBE scheme that encrypts to multiple attributes must provide security against collusion attacks. In particular, no group of users should be able to combine their keys in such a way that they can decrypt a ciphertext that none of them alone could. This property is important for security in both biometric applications and “attribute-based encryption”.

Our Contributions We formalize the notion of Fuzzy Identity-Based Encryption and provide a construction for a Fuzzy Identity-Based Encryption scheme. Our construction uses groups for which an efficient bilinear map exists, but for which the Computational Diffie-Hellman problem is assumed to be hard.

Our primary technique is that we construct a user’s private key as a set of private key components, one for each attribute in the user’s identity. We share use Shamir’s method of secret sharing [14] to distribute shares of a master secret in the exponents of the user’s private key components. Shamir’s secret sharing within the exponent gives our scheme the crucial property of being error-tolerant since only a subset of the private key components are needed to decrypt a message. Additionally, our scheme is resistant to collusion attacks. Different users have their private key components generated with different random polynomials. If multiple users collude they will be unable to combine their private key components in any useful way.

In the first version of our scheme, the public key size grows linearly with the number of potential attributes in the universe. The public parameter growth is manageable for a biometric system where all the possible attributes are defined at the system creation time. However, this becomes a limitation in a more general system where we might like an attribute to be defined by an arbitrary string. To accommodate these more general requirements we additionally provide a Fuzzy-IBE system for large universes, where attributes are defined by arbitrary strings.

We prove our scheme secure under an adapted version of the Selective-ID security model first proposed by Canetti et al. [5]. Additionally, our construction does not use random oracles. We reduce the security of our scheme to an assumption that is similar to the Decisional Bilinear Diffie-Hellman assumption.

1.1 Related Work

Identity-Based Encryption Shamir [15] first proposed the concept of Identity-Based Encryption. However, it wasn’t until much later that Boneh and Franklin [3] presented the first Identity-Based Encryption scheme that was both practical and secure. Their solution made novel use of groups for which there was an efficiently computable bilinear map.

Canetti et al. [5] proposed the first construction for IBE that was provably secure outside the random oracle model. To prove security they described a slightly weaker

model of security known as the Selective-ID model, in which the adversary declares which identity he will attack before the global public parameters are generated. Boneh and Boyen [2] give two schemes with improved efficiency and prove security in the Selective-ID model without random oracles.

Biometrics Other work in applying biometrics to cryptography has focused on the derivation of a secret from a biometric [12, 11, 10, 6, 9, 7, 4]. This secret can be then used for operations such as symmetric encryption or UNIX style password authentication.

The distinguishing feature of our work from the above related work on biometrics above is that we view the biometric input as potentially public information instead of a secret. Our only physical requirement is that the biometric cannot be imitated such that a trained human operator would be fooled. We stress the importance of this, since it is much easier to capture a digital reading of someone's biometric, than to fool someone into believing that someone else's biometric is one's own. Simply capturing a digital reading of someone's biometric would (forever) invalidate approaches where symmetric keys are systematically derived from biometric readings.

Attribute-based encryption Yao et al. [17] show how an IBE system that encrypts to multiple hierarchical-identities in a collusion-resistant manner implies a forward secure Hierarchical IBE scheme. They also note how their techniques for resisting collusion attacks are useful in attributebased encryption. However, the cost of their scheme in terms of computation, private key size, and ciphertext size increases exponentially with the number of attributes.

References

[1] Mihir Bellare, Alexandra Boldyreva, Anand Desai, and D. Pointcheval. Key-privacy in publickey encryption. Lecture Notes in Computer Science, 2248, 2001.

[2] Dan Boneh and Xavier Boyen. Efficient selective-id secure identity based encryption without random oracles. In Proceedings of the International Conference on Advances in Cryptology (EUROCRYPT '04), Lecture Notes in Computer Science. Springer Verlag, 2004.

[3] Dan Boneh and Matthew K. Franklin. Identity-based encryption from the Weil pairing. In Proceedings of the 21st Annual International Cryptology Conference on Advances in Cryptology, pages 213–229. Springer-Verlag, 2001.

[4] Xavier Boyen. Reusable cryptographic fuzzy extractors. In ACM Conference on Computer and Communications Security—CCS 2004, 2004.

[5] Ran Canetti, Shai Halevi, and Jonathan Katz. A forward-secure public-key encryption scheme. In Proceedings of Eurocrypt 2003. Springer-Verlag, 2003.

[6] G.I. Davida, Y. Frankel, and B.J. Matt. On enabling secure applications through off-line biometric identification. In IEEE Symposium on Privacy and Security,

1998.

[7] Yevgeniy Dodis, Leonid Reyzin, and Adam Smith. Fuzzy extractors: How to generate string keys from biometrics and other noisy data. In Proceedings of the International Conference on Advances in Cryptology (EUROCRYPT ’04), Lecture Notes in Computer Science. Springer Verlag, 2004.

[8] Eiichiro Fujisaki and Tatsuaki Okamoto. Secure integration of asymmetric and symmetric encryption schemes. In Proceedings of the 19th Annual International Cryptology Conference on Advances in Cryptology, pages 537–554. Springer-Verlag, 1999.

[9] Ari Juels and Martin Wattenberg. A fuzzy commitment scheme. In Proceedings of the 6th ACM conference on Computer and communications security, pages 28–36. ACM Press, 1999.

[10] Fabian Monrose, Michael K. Reiter, Q. (Peter) Li, Daniel Lopresti, and Chilin Shih. Towards voice generated cryptographic keys on resource constrained devices. In Proceedings of the 11th USENIX Security Symposium, 2002.

[11] Fabian Monrose, Michael K. Reiter, Q. (Peter) Li, and Susanne Wetzel. Cryptographic key generation from voice. In Proceedings of the IEEE Conference on Security and Privacy, 2001.

[12] Fabian Monrose, Michael K. Reiter, and Susanne Wetzel. Password hardening based on keystroke dynamics. In Proceedings of the 6th ACM conference on Computer and communications security, pages 73–82. ACM Press, 1999.

[13] Amit Sahai. Non-malleable non-interactive zero knowledge and adaptive chosen-ciphertext security. In In Proceedings of 40 IEEE Symp. on Foundations of Computer Science, 1999.

[14] Adi Shamir. How to share a secret. Communications. ACM, 22(11):612–613, 1979.

[15] Adi Shamir. Identity-based cryptosystems and signature schemes. In Proceedings of CRYPTO 84 on Advances in cryptology, pages 47–53. Springer-Verlag New York, Inc., 1985.

[16] Brent Waters. Efficient identity based encryption without random oracles. In To Appear in Proceedings Eurocrypt 2005, 2005.

[17] Danfeng Yao, Nelly Fazio, Yevgeniy Dodis, and Anna Lysyanskaya. Id-based encryption for complex hierarchies with applications to forward security and broadcast encryption. In ACM Conference on Computer and Communications Security—CCS 2004, 2004.

附录C　外文文献译文

模糊的基于身份加密（节选）

Amit Sahai　　Brent Waters
sahai@cs.ucla.edu　　bwaters@cs.stanford.edu

摘要

我们引入一种新的基于身份加密[9]方案叫做模糊的基于身份加密[10]。在Fuzzy IBE中我们将身份特性看作描述性的属性集合。假设私钥代表身份特性ω，密文代表身份特性ω‘，那么当且仅当ω与ω’按照“设置重叠”度量足够接近时，私钥才能够解密密文。Fuzzy IBE方案可以适用于以生物特性作为输入的解密中；生物特性的每次采样都会有噪声，因此Fuzzy IBE的错误容忍正适用于生物识别身份。除此之外，我们表明Fuzzy IBE能够被应用于我们称为“基于属性加密[11]”的应用中。

本文中我们提供了Fuzzy IBE的两种构造方案。我们的构造被看作是拥有多个属性符合成的（模糊）身份的消息的加密。我们的IBE方案既可以容错，又可以安全的抵制合谋攻击。除此之外，我们的基础构造没有使用随机预言模型，我们在选择ID安全模型下证明我们方案的安全性。

1 绪论

基于身份加密 [15] (IBE) 允许发送者在不能获取公钥证书的条件下向某个身份特性加密消息。这种不使用证书的公钥加密能力具有很多实际的应用。例如，一个用户在公钥基础设施不存在，或者接受者在加密时并不在线的前提下，可以发送加密邮件给向接受者（如bobsmith@gmail.com）。

之前的IBE方案的一个共同特性是他们将属性看作是字符串。本文中我们提供了一种醒的IBE叫做*模糊的基于身份加密*，在Fuzzy IBE中我们讲属性看作是描述性的属性集合。在Fuzzy IBE方案中，用户拥有身份特性ω的密钥，密文用公钥ω’加密，当且仅当用些指标来判断ω和ω‘彼此在一定的距离内。因此，我们的系统允许身份特性中有一定的量的容错。

Fuzzy-IBE提出了两个新的有趣应用。一个是使用生物特性的IBE系统，这个应用可以将用户的生物识别，例如，虹膜扫描，看作用一些属性描述的用户身份

[9] Identity-Based Encryption, 简称 IBE
[10] Fuzzy Identity-Based Encryption,简称 Fuzzy IBE
[11] attribute-based encryption,简称 ABE

特性，然后用用户的身份特性给用户加密。由于生物识别存在噪声，我们不能使用已经存在的IBE方案。然而，Fuzzy-IBE的容错特性允许私钥（来自一个生物测量）解密用另一个稍微不同的相同生物测量加密的密文。

Fuzzy IBE的第二个应用被我们称作“基于属性的加密”。在这个应用中，一方可能想将文件对给拥有某些特定属性集合的所有用户。例如，在计算机科学系，系主任可能想将文件加密给招聘委员会的所有系统部教师。在这种情况下，他可能加密文件给身份属性{“招聘委员会”, “教室”, “系统部”}。任何拥有上述三个属性的用户可以解密文件。使用Fuzzy IBE的优势是文件可以存储在一个简单的不可信存储服务器，而不是依赖于可信服务器在提供文件之前执行验证检查。

我们进一步讨论在IBE中使用生物识别的意义，并讨论我们的贡献。

在IBE中使用生物识别技术 许多情况下，在IBE方案中使用基于生物识别的身份比“标准”的IBE有许多重要的优势。我们认为，生物识别身份非常适合IBE的框架，是IBE非常有价值的应用。

首先，从授权者手中获取私钥是非常自然和直接的。在标准的IBE方案中，一个用户拥有一个身份，比如说“Bob Smith”，需要去授权者手中获取对应于该身份的私钥。这个过程中，他必须向授权者“证明”他确实与这种身份挂钩，这通常会涉及到提交补充文件或者凭据。这种必要的验证通常是不清晰，这个过程是有待商榷的（补充文件本身可能是伪造的）。通常情况下，系统会有一个在昂贵和不可靠之间的权衡。

相反，如果生物特性作为身份的验证过程是很清楚的，用户必须在一个训练有素的操作员的监督下证明拥有这些生物特征。如果操作员能够检测模仿攻击，例如播放录音，那么安全性就仅仅局限在生物识别技术本身。我们强调个人的生物特征测量不需要保密，事实上，如果不是作为公钥使用的话还是要保密的。我们要保证密钥授权者不能认为攻击者拥有他不具有的生物身份。

除此之外，生物特性是一个人固有的特性。在IBE中使用生物识别意味着用户可以随手拿出自己的公钥。在许多情况下，用户想给其他人提供加密密钥，这个密钥是在物理上真是存在的。例如，考虑一方在旅行，并与另一方加密他们之间的私密会议。

最后，用生物特征作为身份还有一个优势，如果生物特征的质量非常好的话，该身份是独一无二的。一个标准的属性，例如名字“Bob Smith”，显然不是独一无二的或者是随着时间变化的。

抵制合谋攻击的安全性 由属性集合组成身份的IBE方案中除了提供容错外，还

要提供抵制合谋的安全性。特别是，没有这样的用户组，他们能够组合他们以某种方式组合他们的密钥解密密文，但是他们单独不能解密。这个特性对生物识别的应用和ABE的安全性都非常重要。

我们的贡献 我们正式的给出了Fuzzy IBE的概念，并给出了一个构造方案。我们的构造使用。因为高效的双线性映射存在，且计算Diffie-Hellman问题假定是困难的，所以我们的构造中使用了群。

我们的主要方法是，我们用代表用户身份特征的属性代表每一个私钥组件，这些组件的集合构成了用户的私钥。我们使用Shamir的秘密分享[14]方法来分配一个主密钥在用户私钥组件中的指数值。带有指数的Shamir秘密分享给我们的方案提供了容错的重要特性，因为只要用户所有私钥组件集合的子集就能解密消息。此外，我们的方案可以抵制合谋攻击。不同的用户使用不同随机多项式生成他们的私钥组组件。如果多个用户合谋，他们不能找到任何有用的方式组合他们的私钥组件。

在我们方案的第一个版本中，公钥大小随着全集中潜在的属性的数目而线性增长。公共参数的增长在创建初期定义了可能的属性的生物识别系统中是可测量的，然而，在属性被定义为任意的字符串的更通用的系统中，这却变成了限制。为了适应更通用的需求，我们额外的提供了Fuzzy IBE方案一个属性被定义为任意字符串的属性全集。

我们在选择ID安全模型的适应版本中证明我们的方案是安全的，这个模型最初是由Canetti等[5]人提出来的。此外，我们的系统并未使用随机预言模型。我们将我们方案的安全性削减为类似决策双线性Diffie-Hellman假设。

1.1 相关工作

基于身份加密 Shamir[15]首先提出了IBE的概念，然而直到Boneh和Franklin[3]才提出了第一个既实用又安全的IBE方案。他们的解决方案新颖的使用了高效可计算双线性群。

Canetti等人[15]首先在随机预言模型外提出了可证安全的IBE构造。为了证明安全性，他们描述了比被成为选择ID模型的稍微弱的模型，在这个模型中敌手在公共参数生成前宣称他要攻击的身份。Boneh和Boyen[2]在随机预言之外的选择ID模型下提出了两个改进效率的可证安全方案。

生物识别技术 将生物识别技术应用到加密的其他工作集中在从秘密推导出生物特征上[12, 11, 10, 6, 9, 7, 4]，这个秘密可以应用到如对称密码方案和UNIX风格的密码验证上。

与上述工作相比，我们的工作特点是，我们将生物输入特性看作潜在的公共信息而不是秘密，我们唯一的物理要求是无法模仿生物识别，如训练有素的操作人员不会被愚弄。我们强调这一点的重要性是，相比于让操作员相信另一个人的生物特征是某个人的，捕捉一个人的生物特征的数位阅读更容易。简单的捕捉生物识别的数位阅读对对称密钥体系是（永远）无效的。

基于属性加密 Yao等人 [17] 提出了合谋攻击方式的基于分层身份的IBE方案，意味着前向安全的分层IBE方案。他们还指出如何在ABE中使用他们的技术抵制合谋攻击。然而，在他们的方案中，计算的成本，私钥大小，密文大小随着属性数目的增加而呈指数增长。

参考文献

[1] Mihir Bellare, Alexandra Boldyreva, Anand Desai, and D. Pointcheval. Key-privacy in publickey encryption. Lecture Notes in Computer Science, 2248, 2001.

[2] Dan Boneh and Xavier Boyen. Efficient selective-id secure identity based encryption without random oracles. In Proceedings of the International Conference on Advances in Cryptology (EUROCRYPT ’04), Lecture Notes in Computer Science. Springer Verlag, 2004.

[3] Dan Boneh and Matthew K. Franklin. Identity-based encryption from the Weil pairing. In Proceedings of the 21st Annual International Cryptology Conference on Advances in Cryptology, pages 213–229. Springer-Verlag, 2001.

[4] Xavier Boyen. Reusable cryptographic fuzzy extractors. In ACM Conference on Computer and Communications Security—CCS 2004, 2004.

[5] Ran Canetti, Shai Halevi, and Jonathan Katz. A forward-secure public-key encryption scheme. In Proceedings of Eurocrypt 2003. Springer-Verlag, 2003.

[6] G.I. Davida, Y. Frankel, and B.J. Matt. On enabling secure applications through off-line biometric identification. In IEEE Symposium on Privacy and Security, 1998.

[7] Yevgeniy Dodis, Leonid Reyzin, and Adam Smith. Fuzzy extractors: How to generate string keys from biometrics and other noisy data. In Proceedings of the International Conference on Advances in Cryptology (EUROCRYPT ’04), Lecture Notes in Computer Science. Springer Verlag, 2004.

[8] Eiichiro Fujisaki and Tatsuaki Okamoto. Secure integration of asymmetric and symmetric encryption schemes. In Proceedings of the 19th Annual International Cryptology Conference on Advances in Cryptology, pages 537–554. Springer-Verlag, 1999.

[9] Ari Juels and Martin Wattenberg. A fuzzy commitment scheme. In Proceedings of the 6th ACM conference on Computer and communications security, pages

28–36. ACM Press, 1999.

[10] Fabian Monrose, Michael K. Reiter, Q. (Peter) Li, Daniel Lopresti, and Chilin Shih. Towards voice generated cryptographic keys on resource constrained devices. In Proceedings of the 11th USENIX Security Symposium, 2002.

[11] Fabian Monrose, Michael K. Reiter, Q. (Peter) Li, and Susanne Wetzel. Cryptographic key generation from voice. In Proceedings of the IEEE Conference on Security and Privacy, 2001.

[12] Fabian Monrose, Michael K. Reiter, and Susanne Wetzel. Password hardening based on keystroke dynamics. In Proceedings of the 6th ACM conference on Computer and communications security, pages 73–82. ACM Press, 1999.

[13] Amit Sahai. Non-malleable non-interactive zero knowledge and adaptive chosen-ciphertext security. In In Proceedings of 40 IEEE Symp. on Foundations of Computer Science, 1999.

[14] Adi Shamir. How to share a secret. Communications. ACM, 22(11):612–613, 1979.

[15] Adi Shamir. Identity-based cryptosystems and signature schemes. In Proceedings of CRYPTO 84 on Advances in cryptology, pages 47–53. Springer-Verlag New York, Inc., 1985.

[16] Brent Waters. Efficient identity based encryption without random oracles. In To Appear in Proceedings Eurocrypt 2005, 2005.

[17] Danfeng Yao, Nelly Fazio, Yevgeniy Dodis, and Anna Lysyanskaya. Id-based encryption for complex hierarchies with applications to forward security and broadcast encryption. In ACM Conference on Computer and Communications Security—CCS 2004, 2004.